

Guidance Software
215 north marengo avenue, 2nd floor
pasadena, california 91101
phone: 626.229.9191
fax: 626.229.9199
e-mail: documentation@guidancesoftware.com
www.guidancesoftware.com
EnCase Forensic v5.05 User Manual

ENCASE™ FORENSIC

USER MANUAL

VERSION 5

 **Guidance**[™]
SOFTWARE

TABLE OF CONTENTS

Legal Notice	1
EnCase® License Agreement	1
Copyright	1
Definitions	1
License and Certain Restrictions	1
Non-Exclusive License	1
Support	3
Support for the Law Enforcement/Government Edition of the PROGRAM	3
Support for the Corporate Edition of the PROGRAM	3
Support for the Corporate Deluxe Edition of the PROGRAM	3
Premium License Support Program, Annual Payment Option	4
Premium License Support Program, Three-Year Payment Option	4
EnScript® Macros WARNING	4
Disclaimer of Warranties	4
Limitation of Liability and Damages	5
Export Restrictions	6
U.S. Government End Users:	6
General Provisions	6
Preface	9
Manual Organization	9
Minimum Recommended Requirements	9
Help Resources	10
Technical Support	10
EnCase Message Boards	11
About Guidance Software	11
EnCase Forensic	11
EnCase Enterprise	12
Guidance Software's Professional Development and Training	12
Law Enforcement Courses	12
Computer Forensics and Incident Response Courses	12
Expert Courses	13
Guidance Software's Professional Services Division	13
Additional Corporate Services	13
What's New in EnCase Version 5	15
Enhanced User Interface	15
Home Subtab	17

Entries subtab	17
Secure Storage Subtab	17
Email Subtab	18
History and WebCache Subtabs	18
File Extents, Permissions and Bookmarks Subtabs	19
Sources Subtab and Table Column	20
Subjects Subtab	21
Local Keywords	21
EnCase LinEn Acquisition Utility	21
Additional File System Support	22
Symbolic Link Table Column	22
Ability to Create ENBCD From ISO Image	22
Go To Parent	22
Acquisition Options	23
Quick Reacquisition Option	23
Read Ahead	23
Granularity	23
Block Size	23
Restart Acquisition	23
Globally Unique Identifiers (GUIDs)	24
Evidence File Segment/Splitting File Size	24
CD/DVD Inspector File Support	24
Logon User Identification	25
EnCase Installation Files and Folders	25
Export and Import of Bookmarks	26
Flag Lost Files Option	26
Keyword Tester	27
Ability to Create a Logical Evidence File	27
Single Files Option	27
Filter Conditions	27
EnScripts Added to Filter Pane	28
PDF and Windows Help Files	28
Device Configuration Overlay (DCO) and Host Protected Area (HPA) Support	28
Virtual PC Images	29
Support for SlySoft CloneCD%00 Images	29
PC Guardian Access	29
Additional Servlet Support	29
CD/DVD Module	30
FastBloc SE Module	30
Improved Enterprise Snapshot Functionality	30
Enhanced EnScript Support	30

Installing EnCase	31
The EnCase Installation CD and Autorun	31
Disk 1 CD Installation Menu and Contents	31
Security Key Drivers Installation	31
Installing EnCase Version 5	32
Installing the Servlet	34
Software Updates	36
To Download the Latest EnCase Version 5 Update	36
Configuration Questions	37
Security Key Questions	38
Creating the EnCase Boot Disk	39
Windows Acquisition Issues	39
Creating the EnCase Boot Disk	39
Steps to Create the EnCase Barebones Boot Disk	40
Creating an EnCase Boot CD	42
Booting a Computer with the EnCase Boot Disk	44
EnCase Network Boot Disk	45
FAQs about EnCase Boot Disk	46
EnCase for DOS	47
Launching EnCase for DOS	47
EnCase for DOS Functions	47
Locking / Unlocking (L)	47
Acquiring	48
Hashing	48
Server	50
Mode	52
Quit	53
EnCase LinEn Utility	55
Description	55
LinEn Setup	57
For SuSE 9.1	57
For Red Hat	57
Drive-to-Drive Acquisition	58
Preview or Acquisition via Crossover	59
Previewing vs. Acquiring	63
Limitations of Previewing	63
Advantages of Previewing	64
Live Device and FastBloc Indicators	64
Preview Questions	64
Acquisition Questions	65

Parallel Port Cable Acquisition	67
Parallel Preview \ Acquisition Process	67
Network Cable Acquisition	73
Creating the EnCase Network Boot Disk (ENBD) or LinEn CD	73
EnCase Network Boot Disk (ENBD)	73
EnCase LinEn Utility	75
Using the ENBD	75
Using the EnCase LinEn Utility	77
Troubleshooting LinEn connectivity issues	77
Preview or Acquisition	78
Windows XP SP2	78
Windows 2000, XP, and 2003	79
Drive-to-Drive DOS Acquisition	81
Drive Geometry Problems	81
Benefits and Drawbacks	82
Steps to Follow	82
Acquiring Macintosh Devices	89
Acquiring Unix and Linux	89
After the Acquisition Is Complete	90
FastBloc Acquisitions	91
FastBloc Acquisition Process	91
Live Device and FastBloc Indicators	93
Acquiring in Windows Without FastBloc	100
Acquiring in Windows with a non-FastBloc Write-Blocker	101
After Acquisition Is Complete	101
Acquiring Disk Configurations	103
Software RAID	104
Windows NT: Software Disk Configurations	104
Dynamic Disk	105
Hardware Disk Configuration	106
Disk Configuration Set Acquired as One Drive	106
Disk Configurations Acquired as Separate Drives	106
Validating Parity on a RAID-5	108
RAID-10	108
SCSI Drives and DOS	108
Acquiring Palm PDAs	109
Palms Supported	109
Directions	109
Getting Out of Console Mode	116
One Final Note on Palms	117
Acquiring Removable Media	119

Zip / Jaz Disks	119
Floppy Disks	120
Write-Protecting a Floppy Disk	121
Superdisks (LS-120)	121
CD-ROM, CD-R, CD-RW	121
Flash media	122
Equipment needed to preview/acquire flash media	122
How to acquire flash media	122
Examining flash media	122
Acquiring Multiple Pieces of Media	123
First Steps	125
Connecting to Remote Media	125
SAFE Administration and User Accounts	125
Logging Into a SAFE Server	126
Creating a New Case	127
Connecting to Media	127
Remote Acquisition	129
Time Zone Settings	130
Recover Folders on FAT Volumes	133
Behind the Scenes with Recover Folders	133
Recovering NTFS Folders	134
Lost Files in UFS and EXT2/3 Partitions	136
Signature Analysis	136
File Signatures	136
Adding a New Signature	138
Starting a Signature Analysis	139
Viewing Results	140
Hash Analysis	141
File Hashing	141
Creating a Hash Set	141
Importing Hash Sets	143
HashKeeper	143
NSRL Hash Sets	145
Rebuilding the Hash Library	147
Benefits of a Hash Analysis	147
Starting a Hash Analysis	148
Analyzing the Hash Results	148
EnScripts	149
Initialize Case	149
FAT and NTFS Info Record Finder	149
File Finder	149

Link File Parser	150
Find Unique EMail Address List	150
Navigating EnCase	151
Creating a New Case	151
Case Management	153
Concurrent Case Management	153
The Options Dialog	154
Global Options	155
Colors	157
Fonts	158
EnScript	158
Storage Paths	159
Enterprise	160
Adding Evidence Files to a Case	164
Sessions Option	167
Error Messages	169
Verifying the Evidence	170
Adding Raw Image Files	171
SafeBack and VMware Images	173
Single Files	175
Logical Evidence Files	176
Interface	176
Docking and Undocking	177
Undocking	177
Docking	177
EnCase Views	178
The Set Include Option Button	178
The Cases Tab	178
File Types	183
File Signatures	184
File Viewers	184
Keywords	185
Security IDs	185
Text Styles	188
EnScripts	189
Hash Sets	190
EnScript Types	190
Table Pane \ View	191
Table View Columns Explained	192
Organizing Columns	200

Rearranging Columns	200
Hiding and Showing Columns	201
Sorting Files in Columns	201
EnCase Icon Descriptions	202
Gallery View	210
America Online .ART files	212
Timeline View	213
Report View	214
EnScript View	215
View (Bottom) Pane	215
Panes	219
Date and Time Questions	220
Viewing Files	221
Copy/UnErasing Files	221
Copying/UnErasing Bookmarks	223
Copying Entire Folders	224
Viewing Files Outside of EnCase	225
File Viewers	225
Setting up a File Viewer	225
File Types	226
File Viewing FAQs	226
E-Mail and Internet Artifacts	229
E-Mail	229
Using the Email Option	230
E-mail Attachments tab	233
Email Table Columns Explained	233
History	235
Finding Web Artifacts	235
Time interpretations formats:	236
History Table Columns Explained	237
Web Cache	238
Finding Web Cache data	239
WebCache Table Columns Explained	240
Keyword Searches	243
Creating Keyword Groups	243
Entering Keywords	244
Search Options	245
International Keywords	246
Keyword Tester Tab	247
Exporting/Importing Keywords	248
Exporting Keywords	248

Importing Keywords	250
Adding Keyword Lists	251
Starting a Search	251
Search Options	252
Viewing Search Hits	253
Bookmarking Search Hits	258
The Refresh Button	258
Canceling a Search	259
Viewing Compound Files	261
Registry Files	261
OLE Files	262
Compressed Files	264
Outlook Express E-Mail	264
Base64 and UUE Encoding	265
MS Outlook E-Mail	266
NTFS Compressed Files	267
Search Compressed NTFS Files and Folders	267
Thumbs.db	268
EnScript and Filters	269
EnScript Path	270
Include Folder	270
Running EnScripts	271
Editing EnScripts	271
Console	272
The EnScript Library	273
Filters	273
Editing Filters	274
Starting and Stopping Filters	274
Creating a Filter	275
Creating a Condition	275
Queries	275
Advanced Analysis	277
Recovering Partitions	277
Adding Partitions	277
Deleting Partitions	281
Recovering Folders from a Formatted Drive	282
Web Browsing History	282
Reading What the Subject Threw Away	284
Making Sense of a DriveSpace Volume	285
Cracking Encrypted or Password Protected Files	286
System Snapshot	286

Volatile Data Defined	286
Volatile Data Components	287
Volatile Data Capture Using Snapshot	287
Open Ports	288
Open Ports Table Columns	288
Active Processes	289
Processes Table Columns	290
Open Files	292
Network Interfaces and Users	292
Foreign Language Support (Unicode)	295
Viewing Unicode Files	297
Unicode Fonts	299
Changing Font Size	302
Font Recommendations	302
Viewing Non-Unicode Files	303
Right to Left (RTL) Languages	306
Foreign Language Keyword Searches	307
Copying and Pasting	307
Character Map	308
Regional Settings	310
Foreign Language Bookmarking	311
Rich Edit Control in Bookmarks	313
More Information	314
Restoring Evidence	315
Physical vs. Logical Restore	315
Preparing the Target Media	316
Physical Restore	316
Logical Restore	320
Bootting the Restored Hard Drive	320
Restoration FAQs	322
Archiving Evidence	323
What Should Be Archived	323
Verifying Evidence Files	324
Cleaning House	325
Bookmarks	329
Understanding Bookmarks	329
Highlighted Data Bookmark	330
Text	331
Picture	332
Integers	333

Dates	333
Windows	333
Styles	334
Notes Bookmark	335
Folder Information Bookmark	337
Notable File Bookmark	338
File Group Bookmark	340
Snapshot	343
Documentation Options for Threads	343
Bookmark Options	344
Move or Copy Bookmarks	348
Notable (Bookmarks table)	348
Exporting Bookmarks	348
The Report	351
Presenting the Findings	351
Reordering Bookmarks for Reports	354
Presenting Multiple Images	356
Exporting the Report	358
Documenting All Files and Folders Contained on Media	361
Presenting Search Results	362
Appendix A	367
Forensic Terminology	367
PC Hardware	367
Hard Drive Anatomy	368
Hard Drive Layout	370
File System Concepts	372
File Systems	374
Disk Configurations Explained	376
Evidence Storage	379
Evidence Files Explained	381
Appendix B	383
GREP	383
GREP Syntax	383
GREP Examples	384
Appendix C	389
Third Party Utilities	389
Quick View Plus	389
IrfanView	389
AC/DSee	389
DBXtract	389
MBXtract	390

Decode Shell Extension	390
Disk Compare	390
Mailbag Assistant	390
PST Cracker	390
OST2PST	390
Gpart	390
CD-R Diagnostic	391
Dir to HTML	391
Appendix D	393
The Forensic Lab	393
Field Acquisitions	393
Lab Analysis	394
Need Additional Information?	394
Index	395

LEGAL NOTICE

EnCase[®] License Agreement

Copyright

EnCase[®] version 5 is furnished under this license agreement (this “Agreement”) and may be used only in accordance with the terms of this Agreement. Copyright 1998-2006 Guidance Software, Inc. All Rights Reserved.

Definitions

PROGRAM is defined as the computer program “EnCase” including the software in executable form only and the single dongle hardware key with which this Agreement is included or remotely re-programmed by COMPANY, and any updates or maintenance releases thereto that COMPANY may provide to you. COMPANY is defined as Guidance Software, Inc., a California Corporation.

License and Certain Restrictions

This Agreement applies to both the trial and full versions of the PROGRAM. Do not use the PROGRAM until you have carefully read the following Agreement. This Agreement sets forth the terms and conditions for licensing of the PROGRAM from COMPANY to you, and installing the PROGRAM indicates that you have read and understand this Agreement and accept its terms and conditions. If you do not agree with this Agreement, promptly return the PROGRAM and accompanying items to COMPANY within ten (10) days of purchase for a full refund with receipt. Absent such return, the PROGRAM will be deemed accepted by you upon shipment.

Non-Exclusive License

Authorized Use. You are granted a limited non-exclusive license to use a copy of the enclosed PROGRAM on the computer(s) used by a single individual. By your use

of the PROGRAM pursuant to this Agreement, you recognize and acknowledge COMPANY's proprietary rights in the PROGRAM. You may not distribute the PROGRAM, including any demonstration version of the PROGRAM, to third parties without the written authorization from COMPANY. You may copy the "encase.exe", "en.exe", and "LinEn" executables to create and verify EnCase® evidence files, but you may not make or distribute copies of such executables, or copies, including demonstration versions, of the PROGRAM, for use in conjunction with any third party software. You may make additional backup copies of the PROGRAM for your own use, as long as only one copy may be used at any one time. No copies or duplicates of the dongle hardware key may be made.

Restrictions. You may not copy the printed materials, if any, accompanying the PROGRAM, or print multiple copies of any user documentation. Applicable copyright laws protect the PROGRAM in its entirety. The PROGRAM also contains COMPANY trade secrets, and thus you may not decompile, reverse engineer, disassemble, or otherwise reduce the PROGRAM to human-perceivable form or disable any functionality that limits the use of the PROGRAM. You may not modify, adapt, translate, rent, sublicense, assign, loan, resell for profit, distribute, or network the PROGRAM, disk, or related materials or create derivative works based upon the PROGRAM or any part thereof. You may not publicly display the PROGRAM or provide technical training or instruction for monetary compensation or other consideration in any form. Your license is automatically terminated if you take any of the actions prohibited by the paragraph.

Transfer. You may not transfer the PROGRAM to a third party, or sell the computer on which the PROGRAM is installed to a third party, without written consent from COMPANY and written acceptance of the terms of this Agreement by the transferee. If you transfer the PROGRAM with the written consent of COMPANY, you must transfer all computer programs and documentation and erase any copies residing on computer equipment. Your license is automatically terminated if you transfer the PROGRAM without the written consent of COMPANY. You are to ensure that the PROGRAM is not made available in any form to anyone not subject to this Agreement. A transfer fee of \$150 will be charged to transfer the PROGRAM (not applicable to transfers associated with orders from VARs, distributors, or resellers or intra-company transfers).

Title. At all times, full title and ownership of the PROGRAM shall remain with COMPANY. You are granted a non-exclusive license to utilize the PROGRAM subject to the terms of this Agreement.

Support

There are five separate levels of support available: (1) Support for the Law Enforcement/Government Edition of the PROGRAM, (2) Support for the Corporate Edition of the PROGRAM, (3) Support for the Corporate Deluxe Edition of the PROGRAM; (4) Premium License Support Program (“PLSP”), annual payment option, which is available to law enforcement and government only; and (5) PLSP, three-year payment option, which is available to law enforcement and government only. The five separate levels of support have the following terms:

Support for the Law Enforcement/Government Edition of the PROGRAM

As part of your license of the PROGRAM, you will receive one year of telephone and E-mail support only in accordance with COMPANY’s standard telephone and E-mail support policies, and you are entitled to receive updates (e.g., version 5.01 to version 5.05), if any, of version 5 of the PROGRAM only for one (1) year from the date of purchase. Support will begin upon the effective date of this Agreement, which is defined as the date the PROGRAM is licensed to you. After the initial year of support, you may elect to continue your support for additional periods of time for a separate fee. Such continued support will include during the applicable time period only: (i) telephone and E-mail support, and (ii) updates (e.g., version 5.01 to version 5.05), if any, of version 5 of the PROGRAM.

Support for the Corporate Edition of the PROGRAM

As part of your license of the PROGRAM, you purchased one, two, or three years of support. For the applicable time period purchased, you will receive: (i) telephone and E-mail support, (ii) updates (e.g., version 5.01 to version 5.05), if any, of version 5 of the PROGRAM, and (iii) any major releases of the PROGRAM (e.g., version 5 to version 6), and subsequent updates, if any, of such release, during such applicable time period. Support will begin upon the effective date of this Agreement, which is defined as the date the PROGRAM is licensed to you. After the initial period of support that you purchased, you may elect to continue your support for additional periods of time for a separate fee.

Support for the Corporate Deluxe Edition of the PROGRAM

As part of your license of the PROGRAM, you licensed EnCase® Virtual File System, EnCase® Physical Disk Emulator, and EnCase® Decryption Suite, and you purchased one, two, or three years of support. In addition, you will receive FastBloc® Software Edition upon public release of such product by COMPANY. For the applicable time period purchased, you will receive: (i) telephone and E-mail support, (ii) updates (e.g., version 5.01 to version 5.05), if any, of version 5 of the PROGRAM,

(iii) any updates to EnCase® Virtual File System, EnCase® Physical Disk Emulator, and/or EnCase® Decryption Suite, and (iv) any major releases of the PROGRAM (e.g., version 5 to version 6), and subsequent updates, if any, of such release, during such applicable time period. Support will begin upon the effective date of this Agreement, which is defined as the date the PROGRAM is licensed to you. After the initial period of support that you purchased, you may elect to continue your support for additional periods of time for a separate fee.

Premium License Support Program, Annual Payment Option

PLSP is available only to law enforcement and government agencies. If you purchased PLSP, annual payment option, you have agreed to pay for three years of PLSP with three annual payments: the first annual fee upon purchase, the second annual fee on the first anniversary of your purchase, and the third annual fee on the second anniversary of your purchase. PLSP includes, for the entire three-year term, the “Support for the Law Enforcement/Government Edition of the PROGRAM” described above, as well as (i) any major releases of the PROGRAM (e.g., version 5 to version 6), and subsequent updates, if any, of such release, (ii) FastBloc® Software Edition (upon public release of such product by COMPANY), and (iii) any updates to EnCase® Forensic Edition Modules (e.g., EnCase® Virtual File System, EnCase® Physical Disk Emulator, or EnCase® Decryption Suite).

Premium License Support Program, Three-Year Payment Option

PLSP is available only to law enforcement and government agencies. If you purchased PLSP, three-year payment option, you have agreed to pay for three years of PLSP with one annual payment upon purchase. The features of PLSP are as described above.

EnScript® Macros WARNING

EnScript® Macros are executable files and thus should be treated with the same caution as any other executable file received from a third party over the Internet or by other means. Like other executable files, it is possible to intentionally write EnScript® Macros with malicious code or to imbed viruses within the code of an EnScript® Macro. It is thus imperative that you identify and trust the source from which you receive an EnScript® Macro. As with any other file, EnScripts® Macros received from third parties should be screened for viruses.

Disclaimer of Warranties

EXCEPT AS PROVIDED ABOVE, THIS PROGRAM AND ANY RELATED SERVICES ARE PROVIDED AS-IS, AND TO THE MAXIMUM EXTENT

PERMITTED BY APPLICABLE LAW, COMPANY DISCLAIMS ALL OTHER REPRESENTATION AND WARRANTIES, EXPRESS OR IMPLIED, REGARDING THIS PROGRAM, DISKETTE, RELATED MATERIALS AND ANY SERVICES, INCLUDING THEIR FITNESS FOR A PARTICULAR PURPOSE, THEIR QUALITY, THEIR MERCHANTABILITY, TITLE OR THEIR NON-INFRINGEMENT. COMPANY DOES NOT WARRANT THAT THE PROGRAM IS FREE FROM BUGS, ERRORS, OR OTHER PROGRAM LIMITATIONS. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU. IN THAT EVENT, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF PURCHASE OF THE PROGRAM. HOWEVER, SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS AS WELL, WHICH VARY FROM STATE TO STATE.

Limitation of Liability and Damages

THE ENTIRE LIABILITY OF COMPANY AND ITS REPRESENTATIVES (AS DEFINED BELOW) FOR ANY REASON SHALL BE LIMITED TO THE AMOUNT PAID BY THE CUSTOMER FOR THE PROGRAM AND RELATED SERVICES PURCHASED FROM COMPANY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, COMPANY AND ITS SUBSIDIARIES, AFFILIATES, LICENSORS, PARTICIPATING FINANCIAL INSTITUTIONS, THIRD-PARTY CONTENT OR SERVICE PROVIDERS, DISTRIBUTORS, DEALERS OR SUPPLIERS (COLLECTIVELY, "REPRESENTATIVES") ARE NOT LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS OR INVESTMENT, OR THE LIKE), WHETHER BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF COMPANY OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. COMPANY WILL NOT BE SUBJECT TO LIABILITY FOR ANY BUGS OR DAMAGES CAUSED BY EnScript® MACROS, INCLUDING EnScript MACROS INTENTIONALLY WRITTEN BY THIRD PARTIES WITH MALICIOUS CODE AND/OR COMPUTER VIRUSES. SOME STATES DO NOT ALLOW THE LIMITATION AND/OR EXCLUSION OF

LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. THE LIMITATIONS OF DAMAGES SET FORTH ABOVE ARE FUNDAMENTAL ELEMENTS OF THE BASIS OF THE BARGAIN BETWEEN COMPANY AND YOU. COMPANY WOULD NOT BE ABLE TO HAVE PROVIDED THIS PROGRAM WITHOUT SUCH LIMITATIONS.

Export Restrictions

You acknowledge that the PROGRAM is subject to export and import control laws of the United States of America and other countries. You agree that PROGRAM will be exported, re-exported or resold only in compliance with such laws. You represent and warrant that the PROGRAM shall not be used for any nuclear, chemical/biological warfare, missile end-use or training related thereto. You also agree that it will not, without first procuring a BIS license or License Exception, (a) re-export or release the above PROGRAM to a national of a country in Country Code D:1 or E:2; nor (b) export to Country Groups D:1 or E:2 the direct product of the PROGRAM, if such foreign produced product is subject to national security controls as identified on the Commerce Control List (See General Prohibition Three Sec. 736.2(b)(3) of the Export Administration Regulations).

U.S. Government End Users:

The PROGRAM and software documentation are "Commercial Items" and "commercial software documentation," as such terms are used in 48 C.F.R. 12.212 (SEPT 1995) and are provided to the Government (i) for acquisition by or on behalf of civilian agencies, consistent with the policy set forth in 48 C.F.R. 12.212; or (ii) for acquisition by or on behalf of units of the Department of Defense, consistent with the policies set forth in 48 C.F.R. 227.7202-1 (JUN 1995) and 227.7203-3 (JUN 1995).

General Provisions

This Agreement sets forth COMPANY's and its Representatives' entire liability and your exclusive remedy with respect to the PROGRAM. You acknowledge that this Agreement is a complete statement of the agreement between you and COMPANY, and that there are no other prior or contemporaneous understandings, promises, representations, or descriptions regarding the PROGRAM or any related services. This Agreement does not limit any rights that COMPANY may have under trade secret, copyright, patent, or other laws. The Representatives of COMPANY are not authorized to make modifications to this Agreement, or to make any additional representations, commitments, or warranties binding on COMPANY, other than in

writing signed by an officer of COMPANY. Accordingly, such additional statements are not binding on COMPANY and you should not rely upon such statements. If any provision of this Agreement is invalid or unenforceable under applicable law, then it is, to that extent, deemed omitted and the remaining provisions will continue in full force and effect. The validity and performance of this Agreement shall be governed by California law (without reference to choice of law principles), except as to copyright and trademark matters, which are covered by federal laws. The parties specifically exclude the United Nations Convention on Contracts for the International Sale of Goods. This Agreement is deemed entered into at Los Angeles, California, and shall be construed as to its fair meaning and not strictly for or against either party.

© 2003-2006 Guidance Software, Inc. All rights reserved. EnCase is a registered trademark and EnScript is a trademark of Guidance Software, Inc.



215 North Marengo Avenue, Pasadena, CA 91101
Phone: 626.229.9191 Fax: 626.229.9199
<http://www.guidancesoftware.com>

PREFACE

Thank you for purchasing EnCase Forensic. You now have the world's leading technology for computer investigations. EnCase Forensic Version 5 (hereafter, "EnCase") is a court-validated solution used by law enforcement, and government and corporate investigators worldwide. At Guidance Software, we continually strive to improve our product and at the same time add more features to ensure that you have the best forensic software solution today and tomorrow.

Manual Organization

This manual is organized by chapters detailing the features of EnCase Version 5, media acquisition options, how to analyze and document acquired evidence and technical appendices (featuring forensic terminology, detailed technical information, EnScript syntax, third-party resources, and more).

This manual is not a substitute for the training classes. To fully learn the EnCase Methodology, and to earn the prestigious EnCE certification, we encourage all users to attend our licensed training classes.

Minimum Recommended Requirements

For best performance, it is recommended that examination machines using EnCase be configured, at a minimum, as described here:

- EnCase security key (Aladdin HASP HL dongle)
- Certificates for all purchased modules
- Current version of EnCase Forensic (updates are available for download from Guidance Software's web site at <http://www.guidancesoftware.com>)
- Pentium IV 1.4 GHz or faster processor
- 1 GB of RAM
- Windows 2000, XP Professional or 2003 Server
- At least 15 MB free hard drive space

Help Resources

GSI provides several different alternatives for users who need assistance. First and foremost is this manual. You should read this manual thoroughly to understand the product and its use. Before acquiring live evidence, be sure to run several “test” acquisitions and try different processes for examining the files.

GSI also provides assistance on our web site in the form of an on-line system, as well as a message board where forensic specialists post questions and answers in various aspects of forensic investigation.



It is imperative that you have your security key ID available when calling Guidance Software for Technical Support, Customer Support or Sales questions. Please use the area below to write down the dongle ID printed on your USB security key:

EnCase Forensic Dongle Serial Number

Technical Support

Guidance Software is committed to providing timely and effective technical support. Registered users receive free technical support, maintenance updates, and reduced pricing on updated versions. If you are unable to find an answer to your technical questions in this guide, please feel free to contact Technical Services using the following information:

North America	Asia/Pacific Rim	Europe
(626) 229-9191	(626) 229-9191	44 151 255 1700
support@EnCase.com	AsiaPacSupport@EnCase.com	Europe.support@EnCase.com
M-F 06:00 – 19:00 (PST)	S-Th 15:00 – 23:00 (PST)	M-F 08:00 – 16:00 (GMT)

When contacting Technical Services, please have the following information available:

- Your name, and the name of your organization
- Telephone number, fax number, and e-mail address

- The model of the computer, the operating system and version, the amount of memory, and the version of EnCase you are running
- Security key (dongle) ID number (available by selecting **About EnCase** from the **Help** menu)
- Detailed description of the problem. Describe any error messages exactly as they appear. Please list all of the steps and conditions that led to the problem. You may wish to create screen captures to e-mail to GSI

EnCase Message Boards

The EnCase message board (called the **Users Forum**), the EnScript™ board, the Enterprise Forum, and the Hardware Forum are resources for the computer forensics community to exchange ideas, ask questions, and give answers. Discussions range from basic acquisition techniques to in-depth analysis of encrypted files and more. Thousands of our experienced and skilled EnCase users are registered on the message boards, reviewing posts every day, and can offer their expertise on all functionality of EnCase. The message boards are an invaluable resource for the forensic investigator. Please visit our web site and look through the message boards for quick answers to your questions and tips from dedicated users.

You must register to access the message board. For message boards access, go to <http://www.guidancesoftware.com>. Once there, navigate to the message board. If you have any issues regarding the message board, please contact Tech Support.

About Guidance Software

Guidance Software is the leader in computer forensics and incident response solutions. Founded in 1997 and headquartered in Pasadena, CA, Guidance Software has offices and training facilities in California, Virginia and the United Kingdom. More than 15,000 corporate and government investigators depend on EnCase software, while more than 3,500 investigators attend Guidance Software's forensic methodology training annually. Accepted by numerous courts and honored with eWEEK's Excellence Award and SC Magazine's Annual Award, EnCase software is considered the standard forensic tool. For more information, visit Guidance Software's Web site at <http://www.guidancesoftware.com>.

EnCase Forensic

EnCase Forensic is recognized as the standard computer forensic software used by more than 15,000 investigators and 40 of the Fortune 50. EnCase Forensic provides

law enforcement, government and corporate investigators with dependable, court-validated technology relied upon by leading agencies worldwide since 1997.

EnCase Enterprise

EnCase Enterprise is for computer investigators and information security professionals who need to investigate computer breaches and other incidents throughout the enterprise. EnCase Enterprise is a powerful, network-enabled incident response and computer forensics system that provides immediate and thorough forensic analysis of compromised servers and workstations anywhere on the network without disrupting operations. Without EnCase Enterprise, organizations must resort to cumbersome and inefficient manual processes using stand-alone utilities that extend the response and investigation process by days if not weeks, and require subject systems to be taken out of service. This solution brings the highly successful and industry standard EnCase computer forensic technology to the enterprise for unprecedented incident response and investigation capability. EnCase Enterprise represents best practices for immediate incident response and investigation of perimeter breaches and internal threats.

Guidance Software's Professional Development and Training

Law Enforcement Courses

Designed for Federal, State and Local Law Enforcement Investigators

Guidance Software has trained thousands of law enforcement officers from more than 50 countries. As the world's the largest computer forensics trainer, Guidance Software's courses feature master instructors from federal, state and local law enforcement agencies. Many instructors remain full-time investigators with world-renowned computer crime units, bringing real-life, first-hand investigation experience to every class.

The five law enforcement courses train students how to recover digital evidence using Guidance Software's court-accepted EnCase Forensic software. Often ending up in front of a judge and jury, students are taught not only how to gather, locate and analyze evidence, but also how to properly explain the results of the investigation in a thorough, professional manner. Courses incorporate these sound forensic practices with the award-winning capabilities of EnCase Forensic.

Computer Forensics and Incident Response Courses

Designed for the IT Security Professional, Litigation Support Personnel, Legal Professionals and Forensic Investigators

Computer forensic investigators, network security professionals and internal computer incident response teams are being relied upon to manage incidents and mitigate risks. The same EnCase technology relied upon by law enforcement for years now serves as a vital internal tool for thousands of companies. Proper computer forensics training is crucial for corporate investigators.

Guidance Software offers three Computer Forensics and Incident Response courses specifically designed for security consultants, investigators and auditors in large enterprise networks. These courses train investigators and auditors how to use EnCase Enterprise and EnCase Forensic to investigate and respond to several types of incidents within their enterprise.

Expert Courses

Designed for Experienced Computer Forensic Investigators

Guidance Software's expert-level courses are designed for law enforcement and corporate investigators with significant computer forensics experience. Offering investigators an in-depth focus on file systems and advanced and advanced system artifacts recovery techniques, the expert-level courses utilize the vast capabilities of both the EnCase Forensic and EnCase Enterprise software solutions.

Guidance Software's Professional Services Division

Guidance Software's Professional Services Division (PSD) provides unparalleled computer investigation support to clients and partners. This support enables immediate response to any scale of investigation or proactive audit. PSD's services leverage unrivaled computer investigation professionals, including talent drawn from leading law enforcement agencies and Fortune 500 companies.

Additional Corporate Services

GSI is continuously working to provide you with state-of-the-art cutting-edge computer forensic solutions. GSI offers the following services:

- Technical support available via E-mail and telephone
- Forensic script macro tools
- Message Board / Users Group
- EnCase Legal Journal
- Legal resources pertaining to digital evidence

These services allow you to communicate with GSI and other users about the various capabilities of Guidance Software products.

WHAT'S NEW IN ENCASE VERSION 5

Enhanced User Interface

The Version 5 GUI is designed to better organize new and existing EnCase functionality. Windows, available from the **View** pull-down menu in Version 4 are now accessible via submenus named for the pane in which they appear, as illustrated in Figure 1-1.

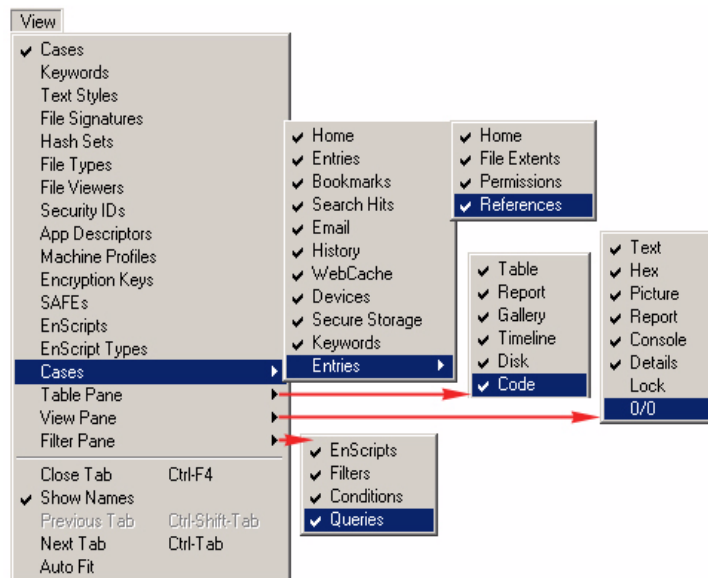


Figure 1-1: Expanded View Menu

Each submenu in turn, relates to a display GUI on the main page. For example, the Table Pane submenu contains six selections, including **Table**, **Report**, **Gallery** and

so forth. Each of these selections appears as a selectable button in the main display's Table Pane. Figure 1-2 shows the entire screen, while Figure 1-3 shows the **Table Pane** menu item and its associated Table Pane buttons.

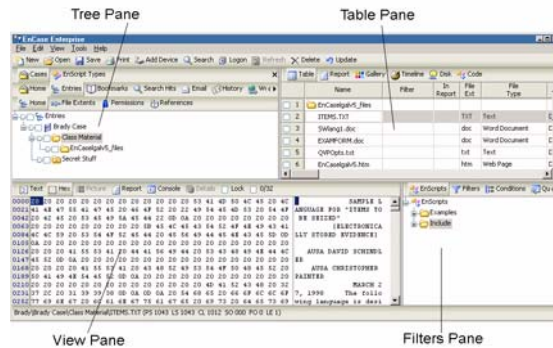


Figure 1-2: EnCase Window Showing Pane Location



Figure 1-3: Table Pane Menu and Table Buttons

The **Cases** tab is displayed in the Tree Pane by default when a new case is created or a saved case is opened. Several new tabs appear under the **Cases** tab in the Tree Pane that provide additional functionality in the ability to search, display, sort and bookmark specific data. An example of some displayed tabs appears below:



Figure 1-4: Cases Subtabs

Home Subtab

When **Cases** and **Home** are selected, open cases appear in the Table Pane when the **Table** tab is selected (Figure 1-5).

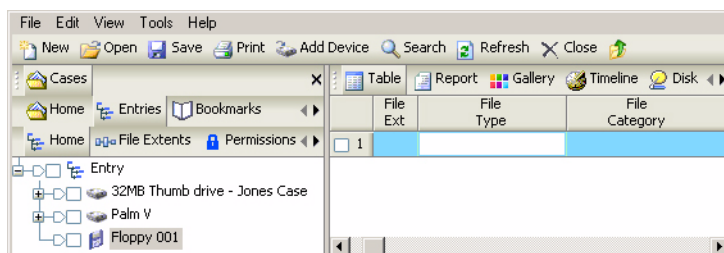


Figure 1-5: Open Cases Showing in Home Tab

Entries subtab

The **Entries** Subtab shows the contents of a selected case. The tab displays all file and folder entries in the selected case. Selecting **Entries** displays its associated **Home** (which shows the devices and volumes in the case), **File Extents**, **Permissions** and **Bookmarks** Subtabs (Figure 1-6). These tabs and subtabs, and their uses, are discussed in depth later in this manual.



Figure 1-6: Entries Subtabs

Secure Storage Subtab

Files and security data encrypted via EFS can be unencrypted using passwords and keys parsed from the system files and registry. This requires using the EnCase Decryption Suite Module (the EDS Cert must be present in the C:\Program Files\EnCase5\Certs directory).

Data from the **Secure Storage** table obtained by right-clicking on a device and selecting **Analyze EFS...**, or opening the **Secure Storage**, right-clicking the **Secure Storage** root folder and selecting **Analyze EFS...**

All devices in the case are scanned. Passwords, keys, syskeys, etc., appear listed in plain text in the Table frame. Refer to the *EnCase Decryption Suite Manual* for additional information.

Email Subtab

EnCase Version 5 includes the ability to parse, analyze and display various types of E-mail formats such as MS Outlook®, Outlook Express®, and web-based E-mail accounts, and to display them in a separate **Email** tab. Version 5.05 provides Outlook 2003 support, in addition to the ability to recovery deleted e-mails stored in .PST files. Examiners can also now copy and unerase e-mail in message format. E-mails can now be stored in Logical Evidence Files.

E-mail files are displayed in their normal file structure under the **Entries** tab and in restructured format in the **Email** tab. The **Email** tab has two associated sub-tabs:

- Home
- Attachments

Clicking the **Home** tab displays all case-related E-mail entries. Selecting the **Attachments** Subtab displays attachments associated with the selected E-mail entry.

In addition to MS Outlook and Outlook Express, EnCase now locates additional E-mail file types, including:

- MSN Hotmail®
- Yahoo!®
- AOL® 6, 7, 8 and 9
- Netscape®
- mBox (Unix)

History and WebCache Subtabs

Users can parse, analyze and display various types of Internet and Windows history artifacts logged when web sites or file directories are accessed through supported Internet Explorer, Mozilla, Opera, and Safari. Version 5.05 also supports Mozilla and Internet Explorer for the Macintosh and the latest version of Safari.

The **History** tab allows users to search various history attributes and organize them into one table. Find artifacts by right-clicking the **History** icon in the Tree Pane of the **History** Subtab (Figure 1-7) or the **WebCache** icon in the root of the **WebCache**

(Figure 1-8) Subtab and selecting **Email/Internet Search** from the submenu that appears (Figure 1-9).

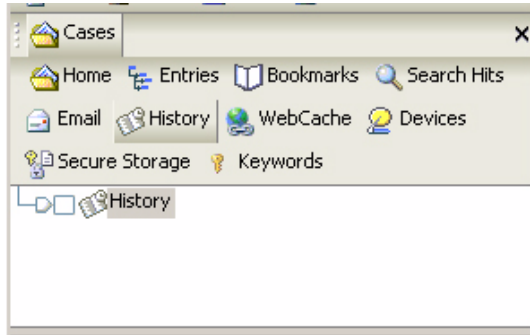


Figure 1-7: History Tree Pane Display



Figure 1-8: Web Cache Tree Pane Display

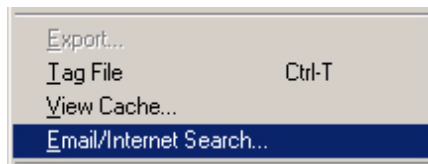


Figure 1-9: Email/Internet Search Submenu

File Extents, Permissions and Bookmarks Subtabs

Three new subtabs below **Entries** (**File Extents**, **Permissions** and **Bookmarks**) appear when files selected in the table pane have these attributes.

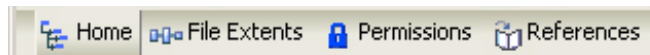


Figure 1-10: Entries Subtabs

To show this information (when it exists), select one of the tabs in Figure 1-10 and the **Details** tab in the displays pane. The data is parsed for these subtabs whether or not a particular column is selected.

The **File Extents** Subtab contains file extent data like start byte, total bytes, start sector, total sectors, start cluster and total clusters).

Permissions data includes security information (permissions) associated with the file, such as SID, property and permissions, while selecting **Bookmarks** indicates the selected file is book marked and shows the bookmark entry.

Figure 1-11 shows a typical file extents report. Notice that some of the same information appears in the Table Pane and the View Pane.

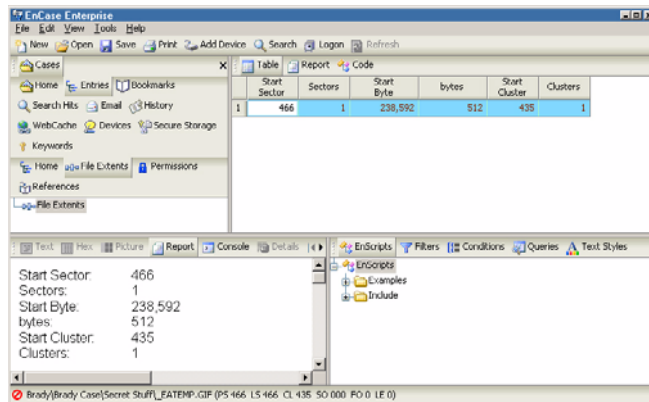


Figure 1-11: File Extents Data

Sources Subtab and Table Column

When a case contains a logical evidence file, the source of the file's contents is listed in the **Sources** Subtab under **Devices** in the **Cases** tab.

With the **Home** Subtab selected under **Devices**, the logical evidence file in the Table pane display a TRUE boolean value in the **Sources** column. Clicking on the column for the file activates the **Details** tab in the View pane, displaying the file name, evidence number, total bytes, physical offset, logical offset, hash value, GUID, and

acquisition date (where the data is available). This same data is available whether selecting the **Sources** Subtab, or the **Sources** table column in **Home**.

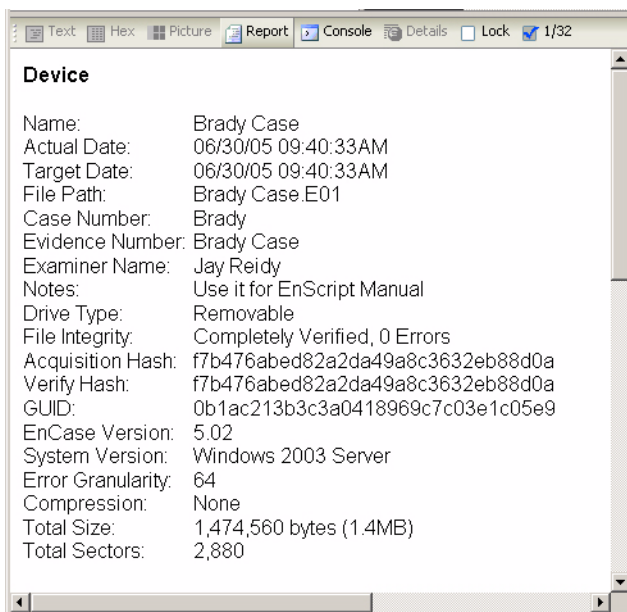


Figure 1-12: Logical Device Report

Subjects Subtab



The **Subjects** Subtab beneath **Devices** allows the examiner to create defined subjects (or users). These subjects allow the examiner to keep track of elements within logical evidence files by associating them with the created name. The full functionality of this feature is not activated, but its use will be particularly useful in EnCase Enterprise examinations on live machines.

Local Keywords



A separate **Keywords** Subtab appears under **Cases** that allows keywords to be created and saved for a specific case. The functionality is similar to that of the global **Keyword** tab, except that the keywords are stored in the Case file rather than in **keywords.ini**.

EnCase LinEn Acquisition Utility

The EnCase LinEn utility allows you to acquire any device from a Linux-based forensic computer. The LinEn utility provides an alternate method of acquiring a device via FastBloc in Windows, or **EN.EXE** in DOS. This method also allows users

to hash any device present on the Linux operating system it is running on. With the introduction of LinEn, users are now able to acquire Linux machines via a crossover cable from the Windows EnCase client by putting it into Server Mode. LinEn is dependent on the distribution of Linux it is installed on. In Version 5.05, ATA support has been added to LinEn functionality, working similarly as to the way it does in the DOS version of EnCase (EN . EXE). See the section of this document titled, “EnCase Linen Utility” for more detailed information.

Additional File System Support

EnCase Version 5 supports TiVo® 1 and TiVo 2 file systems, as well as AIX Journaling File System (JFS1 and JFS2) and LVM8. For JFS file systems, you will need to run the **Scan for LVM** option on the device to see the file structure.

Symbolic Link Table Column

In Unix-based file systems (including AIX), symbolic, or soft links are files, similar to Windows .LNK shortcut files, that point to other files. Symbolic links do not contain the data found in the target file, but can provide links to directories, or files on remote devices. A column has been added to the Table view that indicates the path indicated in the symbolic link.

Ability to Create ENBCD From ISO Image

Using the **Create Boot Disk...** option in the **Tools** menu, you can select an ISO image to add EN.EXE or the LinEn executable to, creating an image that can be burned to an EnCase Boot CD.

Go To Parent

Version 5 contains a feature that allows the user to go upward in the folder structure to the parent folder in four different ways:

- Right click the selected folder then select **Go To Parent**.
- Hitting the [**Backspace**] key.
- Selecting **Go To Parent** from the **Edit** menu.
- Clicking on the icon on the top toolbar with the folder and green arrow.

Acquisition Options

Quick Reacquisition Option

Reacquiring an evidence file to resize file segments is much faster if the **Quick Reacquisition** box is checked. Using this option, a user can reacquire a file while changing segment size. Other acquisition options, such as compression, block size, granularity, assigning name or evidence number are grayed out and unavailable.

Read Ahead

The **Read Ahead** feature is available for EnCase Enterprise users only. It is grayed out and unavailable in EnCase Forensic.

Granularity

Historically during an acquisition, if a read error is found on a hard disk, the entire data block containing the read error is zeroed out by EnCase. Using granularity, the investigator has the flexibility of specifying the number of sectors within the corrupted data block to be zeroed out. This means that instead of all the sectors being zeroed out whenever there are read errors, the user can now specify the degree to which the analysis is refined by setting the granularity from the default 64 sectors for hard drives (16 sectors for CDs and DVDs), down to 1. Using a finer setting will decrease the acquisition speed of the evidence file. The settings and subsequent number of sectors zeroed out are described in the table below:

Granularity setting	64	32	16	8	4	2	1
Sectors zeroed per block	64	32	16	8	4	4	1

Block Size

The block size used to calculate the CRC value can be increased from the default of 64 by using the Block Size option in the acquisition options window. Granularity should always be a value less than the selected block size. Additional information is available in the Acquisition sections of this document.

Restart Acquisition

The **Restart Acquisition** option allows a user to continue a Windows-based acquisition from the exact point where it was terminated. It is designed so if an investigator *manually* terminates the acquisition in EnCase, the acquisition can be restarted by pointing the acquisition to the location where the already acquired evidence files reside. This option is available in EnCase Forensic as well as EnCase Enterprise.

When the option box is checked, the user is prompted for the **Acquisition File Path** (the location where the segments of the failed acquisition are stored) and the **Maximum File Segment Size (MB)**, which should be set to what the original acquisition was set to (640 MB by default, but changeable up to 2,000,000 MB). Bear in mind when setting this value that if you are writing files to a FAT file system, the maximum allowable size is 2,000 (2 gigabytes); setting the value higher will result in write errors.

Globally Unique Identifiers (GUIDs)

GUIDs are 128-bit numbers created by an operating system or application to uniquely identify a particular object (such as a file). EnCase utilizes an API to allow a GUID to be assigned to evidence files acquired in Versions 5.01 and higher. GUIDs can be generated for files created in previous versions by re-acquiring the evidence file. GUIDs appear in the top-level Entries Report, and in the table when selecting the **Devices** Subtab below **Cases**. Clicking on the **Home** Subtab will show any GUID assigned to devices in the case; the **Sources** Subtab will show GUIDs of the source evidence files from which a logical evidence file is created.

Evidence File Segment/Splitting File Size

The input values for splitting files being copied out and segment size of evidence files being acquired have been increased to 2,000,000 MB (2 terabytes). This is to take advantage of the ability to write larger files in an NTFS file system. The default value for each of these is still 640 MB (so that the file segments can be written to CD). Bear in mind when setting this value that if you are writing files to a FAT file system, the maximum allowable size is 2,000 (2 gigabytes); setting the value higher will result in write errors.

CD/DVD Inspector File Support

EnCase now has support for viewing files created using CD/DVD Inspector. To view these, drag the modified zip files from Windows explorer onto the EnCase application window to create a Single File. In the table pane, right-click on the file (which will have a .zip extension) and select View File Structure. If you receive a message stating "This file has a "Zip" signature. Continue parsing?," click **[OK]**. The mounted volume should display all the files that were visible using CD/DVD creator. Note that files in the table are automatically populated with hash values and extra date and time attributes extracted through **CD/DVD Inspector** not normally associated with Zip files.

Logon User Identification

A new **Mark Logon Users** option in the Scan Local Machine EnScript dialog box allows the investigator to identify the user currently logged on to the forensic machine with a double asterisk. After the script is run, accessing the **Network** Subtab below the **Snapshot** tab in **Bookmarks** will show the network users in the table, with the double asterisks following the name of the currently logged on user.

EnCase Installation Files and Folders

When EnCase is installed, a copy of the installer (**Setup 5.05.exe**) is automatically placed in the root of the application directory (typically **C:\Program Files\EnCase5**). The **Scripts** foldername has been changed to **EnScripts**.

As of Version 5.05, there are twelve folders created in the root installation directory, depending on which modules are installed:

- **Backup**

With AutoSave turned on in Global Options, the backup case file (*.CBAK) will be automatically saved to this folder.

- **Cache**

The **Cache** folder holds temporary ISO images when using the CD/DVD Module

- **Certs**

The **Certs** folder is the repository for certificates for all modules such as FastBloc SE, VFS, PDE, EDS, and the `encase.Pcert` file used for security authentication.

- **Config**

The **Config** folder contains all the .INI files that maintain the EnCase configuration settings.

- **EnScripts**

EnScripts that are shipped with EnCase are stored in this folder by default.

- **Export**

The **Export** folder is the **Default Export Folder** for any files marked for export through an EnScript, or for table data, keywords, etc. exported from EnCase. It can be changed through the **Case Options** menu when opening a new case, or in the **Case Options** tab when selecting **Options** from the **Tools** menu.

- **Hash Sets**

The **Hash Sets** folder is the default storage area for Hash Sets imported into or created in EnCase.

- **Help**

This folder contains the WinHelp files accessed by selecting **Help** from the **Help** pull-down menu. This folder must reside in this location for the Help files to be accessed by EnCase.

- **Keys**

Module cert files and encryption keys are stored in this folder.

- **License**

The License folder is used for storage of licenses used to define permissions for Packages.

- **Storage**

This folder is used as a temporary repository of data related to certain EnScript functions. It is empty at the time of installation, and is purged automatically by EnCase. There is no need to place anything in or remove anything from this folder.

- **Temp**

The **Temp** folder is the default **Temporary Folder** for files sent through EnCase to a viewer, where they are copied out and stored until closed from the viewer. It can be changed through the **Case Options** menu when opening a new case, or in the **Case Options** tab when selecting **Options** from the **Tools** menu.

Export and Import of Bookmarks

EnCase has introduced a new feature in the Bookmarks tab that allows the user to import and export bookmarks. This feature allows the user to submit bookmarks to another investigator for review without the cumbersome task of including keywords, search hits, etc. Multiple investigators can also use this to access bookmarks when examining different aspects of an evidence file without having to create multiple case files. See the "Bookmarks", on Page 329 of this document for additional information.

Flag Lost Files Option

When an acquired drive contains many lost clusters, the time it takes to open the evidence file is significantly longer because EnCase marks and attempts to resolve these lost files. Version 5 provides a **Flag Lost Files** checkbox in the **Global** tab of

the **Tools Options** menu. By default, this option is unchecked which means lost clusters are treated as unallocated space, drastically decreasing the amount of time required to process the volume. If this option is checked, EnCase will tag all lost clusters in **Disk** view (indicated by yellow blocks with a question mark). This option must be set before an evidence file is added to the case.

Keyword Tester

When creating a keyword, the user can test a search string against a known file by clicking the **Keyword Tester** tab. This is also useful for testing the ability to search GREP expressions or foreign languages. More information is available in "Bookmarks", on Page 329 of this document.

Ability to Create a Logical Evidence File

Users can now isolate files from inside an evidence file and access them through a logical evidence file. When the desired files are blue-checked in the table, right clicking anywhere in the Tree Pane will show the option to **Create Logical Evidence File....** Logical Evidence Files can contain Single Files, files from a previewed device, files from evidence files, or a combination of these.

In Version 5.05, Logical Evidence File support is upgraded to provide users with options for retaining file content. This includes folder content and hash value omission, as well as making them accessible through EnScript.

For more information, refer to the *Navigating EnCase* section of this document.

Single Files Option

The Single Files option allows the creation of a logical evidence file containing a number of external files. When active, an icon will appear in the Tree Pane, called "**Single Files**". The user can add files to the folder, and then save the file by blue-checking files within the Single Files, right-clicking and selecting **Acquire Logical Evidence File**.

Filter Conditions

A new tab, **Conditions**, has been added to the Filters Pane. Conditions allow the user to specify parameters for filtering the files viewable in the table. Where Filters require the user to enter code for the filter conditions, the new tab allows the user to create filters based on pre-set conditions, selectable from a menu. As with Filters, Conditions can be combined using the **Queries** tab in the Filter Pane. See "EnScript and Filters", on Page 269 for more information.

EnScripts Added to Filter Pane

An **EnScripts** tab has been added to the Filter Pane which allows immediate access to the EnScripts regardless of what is selected in the Tree Pane.

PDF and Windows Help Files

When EnCase Version 5 is installed from the CD, a PDF version of the manual and Windows help files are installed. These can be accessed from the EnCase **Help** pull-down menu. Users can now search or follow hypertext links to the HTML help files through the **Help** menu for topics pertaining to EnCase, or open the PDF version of the manual, provided Adobe Acrobat Reader is installed on the forensic machine. Updated Help files and the PDF manual are available from Guidance Software's web site on the Downloads page.

In Version 5.05, EnCase Help supports the .CHM file format. A .CHM file increases functionality by incorporating a set of web pages written in a subset of HTML and a hyperlinked table of contents. Files in .CHM format are optimized for reading and the files are heavily indexed.



NOTE: When upgrading from an earlier version of EnCase to Version 5.05, delete the existing .hlp file located in the ...\\EnCase5\\Help directory and replace it with the latest version of the file. The file can be found at <http://www.guidancesoftware.com/support/downloads.asp> to find the most up to date file.

Device Configuration Overlay (DCO) and Host Protected Area (HPA) Support

Version 5.05 has the ability for users to detect and image DCO and/or HPA areas on any ATA-6 or higher-level disk drive. These areas are detected using EN . EXE (DOS), LinEn (Linux), or the FastBloc SE module; they are not detected using EnCase in Windows with a hardware write-block device.

EnCase now shows if a **DCO** area exists in addition to the **HPA** area on a target drive. **HPA** is a special area located at the end of a disk. It is usually configured so the casual observer cannot see it, and can only be accessed by reconfiguring the disk. **HPA** and **DCO** are extremely similar; the difference is the SET_MAX_ADDRESS bit setting that allows recovery of a removed HPA at reboot. EnCase sees both areas if they co-exist on a hard drive. For more information, see the *EnCase Modules Manual* or the chapters in this document on *EnCase for DOS* and *EnCase Linen Utility*.

Virtual PC Images

Microsoft Virtual PC 2004 permits a user to run multiple PC-based operating systems simultaneously on one workstation. Users can save images of these virtual PCs in a fashion similar to VMware. EnCase treats Microsoft Virtual PC 2004 images as devices that can be added, parsed and submitted to the same investigation as physical devices.

Virtual PC is capable of creating flat files and sparse files, both of which are supported transparently by EnCase.

Virtual PC files are added via the **Add Devices** dialog box. From the dialog, navigate to the folder containing the primary Virtual PC files (*.vhd) and add them as an EnCase evidence file. See the *Navigating EnCase* chapter of this document for additional information.

Support for SlySoft CloneCD™ Images

Version 5.05 allows users to add raw images of Raw CD-ROM images created using SlySoft CloneCD. When adding these images, users can specify the Pre-Sector Bytes, Post-Sector Bytes and Start Byte of the image.

PC Guardian Access

PC Guardian software provides users with full-volume encryption. The software controls access to the operating system and encrypts every sector of a computer hard drive including temp files, system files and unused disk space.

EnCase Enterprise can see a PC Guardian drive decrypted since the drive has already been booted and the server is deployed to it, but in version 5.05, evidence files of hard drives encrypted with PC Guardian can be decrypted in EnCase Forensic using the new PC Guardian Access tool. This tool provides the ability to decrypt a physical hard drive that has been encrypted with PC Guardian software by detecting that it is protected and providing for input of the decryption key user name and password combination to decrypt the data.

Additional Servlet Support

EnCase Enterprise and FIM Version 5.05 now support servlets for AIX operating system version 4.3, 5.1, 5.2 and 5.3. The new servlets have the same functionality as previous *nix servlets, and provide system-level file system access and the ability to conduct remediation.

This software automatically determines which drivers and servlets to install. If the machine has a 64-bit processor, the process installs two servlets and two drivers.

Also new to Version 5.05 is support for an Apple OSX servlet. The servlet can be deployed to Apple computers on a LAN running version OSX.2 and higher.

For information on deploying the AIX or OSX servlet, refer to the *Servlet Deployment Guide* section of the *EnCase Enterprise* or *EnCase FIM Administrator Manual*

CD/DVD Module

This EnCase cert-based module provides the user with the ability to select entries, reports and other selected data and writes to a CD or DVD. This includes the ability to select and burn EnCase Evidence files (.E01) and Logical Evidence Files (.L01), or to write them to media at acquisition. For more information, see the *EnCase Modules Manual*.

FastBloc SE Module

The new **FastBloc SE** module provides a collection of disk controller utilities such as the same safe subject media preview and acquisition in Windows to an EnCase evidence file currently available from **FastBloc** hardware, and wiping and restoring of drives attached to the PCI controller card. IDE, SCSI, USB and FireWire drives attached to supported PCI controller cards are write-blocked when configured as such by the module. Wiping and restoring of drives attached to the controller is also possible, with the logical restore retaining the same hash value as the original drive. FastBloc SE also allows access to HPA and DCO areas of a suspect drive in Windows (this functionality is not available using a hardware write-blocker with EnCase in Windows). For detail, refer to the *EnCase Modules Manual*.

Improved Enterprise Snapshot Functionality

The Enterprise **Snapshot** function has been updated to provide improved root kit detection support, improved .dll analysis, the ability to detect other communication protocols and hidden port detection.

Enhanced EnScript Support

Newly added EnScript support gives user the ability to scan a directory listing of mounted shared files. In addition to a new EnScript interface to the Email view, there is also EnScript support for sockets in EnCase Enterprise. Users can now use EnScripts to recover folders, as well as for searching and hashing.

INSTALLING ENCASE

Two CDs ship with EnCase Enterprise, Examiner and SAFE Software. Updates are available at <http://www.guidancesoftware.com>. A security key ID and e-mail address is required to download. Instructions for installing the SAFE are in the *EnCase Enterprise Administrator Manual*.



If the Examiner or SAFE is running Windows XP SP2, configure Windows Firewall for proper operation of EnCase. Refer to the whitepaper, *Enabling EE SAFE and Servlet Traffic on Windows XP SP2*, at <http://www.guidancesoftware.com>.

The EnCase Installation CD and Autorun

The EnCase Installation CD is set to start when placed in the drive. If Autorun is turned off, start Windows Explorer, go to the CD-ROM icon and double-click **SETUP . EXE**.

Disk 1 CD Installation Menu and Contents

Install Examiner Software	Installs EnCase Version 5 Examiner
Security Key Drivers	Installs the latest Aladdin Security Key drivers
View Manual (PDF)	The User Manual in Adobe Acrobat PDF format
View White Papers	Guidance Software's white papers
View Help File	The WinHelp file for EnCase
Visit Guidance Software	Direct link to Guidance Software's web site
Install Adobe Acrobat	Installs Acrobat Reader 5.0 to read PDF documents

Security Key Drivers Installation

- Ensure that the dongle is not attached to the machine. Insert the EnCase CD-ROM into the CD-ROM drive.
- If Autorun is enabled, the EnCase splash screen automatically appears.

- Click on the link for **Security Key Drivers** that appears in the splash screen



Figure 2-1: EnCase CD Autorun Window

- Click [**Next >**] when presented with the HASP installation screen. The necessary files will be copied to the hard drive.
- Click [**Next >**] at the summary screen.
- When the screen indicates that the installation is complete, click [**Finish**].
- Power down the computer, insert the security key and boot up the system.



If the security key is inserted before clicking [**Finish**], EnCase will launch in Acquisition Mode, disabling the ability to preview and see file structure but allowing evidence acquisition. Reinstall the driver with the dongle removed to resolve this issue.

If there are problems with the installation, go to the troubleshooting page on our web site at <http://www.guidancesoftware.com>. Once there, navigate to the message board. If you have any issues regarding the message board, please contact Tech Support.

Installing EnCase Version 5

- Insert the EnCase CD into your CD-ROM drive.
- If Autorun is enabled, the EnCase splash screen automatically appears.
- Click on the **Install EnCase** button.
- At the EnCase screen that reports the version being installed, click [**Next >**].

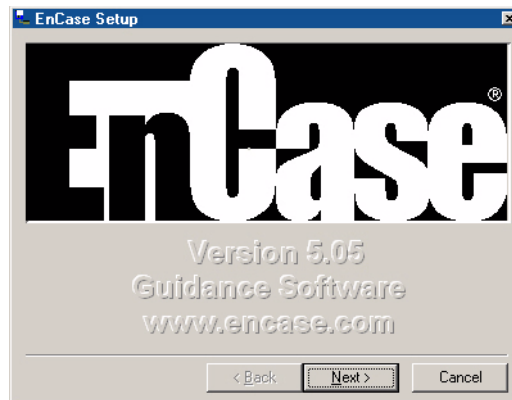


Figure 2-2: EnCase version window

- You will see a License Agreement screen. You must agree to the terms of the license agreement to proceed with the installation. Please read the license agreement, click on the **I Agree** radio button, then click [**Next >**].

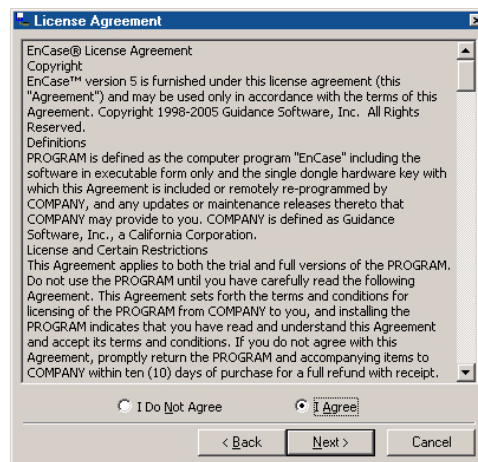


Figure 2-3: EnCase license agreement

- The install dialogue box will appear. You can change the directory into which EnCase installs by clicking on the ellipsis box to the right of the Install To field, but it is recommended that you use the default directory (C:\Program Files\EnCase5).
- If the **View ReadMe** check box is clicked, the EnCase installer will display a text file containing important information about the installation once it is complete. Click [**Finish**] to install EnCase.

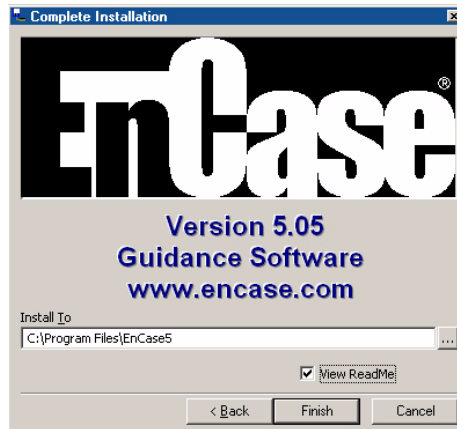


Figure 2-4: EnCase install dialog box

- The EnCase installation will create a program icon on your desktop.



Figure 2-5: EnCase program icon

- If prompted, reboot the computer.
- To run EnCase, double-click on the desktop icon or from the **Start** menu and select **EnCase** under **Programs**.

Installing the Servlet

The method of installing applications on workstations (network devices) will most likely vary by organization. As discussed in the Administrator's manual, the Servlet can be pushed out to network devices across the network in a variety of ways. In this section, we will discuss how the Servlet is created and some basic commands associated with **enstart.exe**.

enstart.exe is created in **C:\Program Files\EnCase SAFE** when the SAFE setup routine is completed. This file is an executable program with the SAFE public key embedded in it. This key is generated during the SAFE setup routine and is automatically included into the Servlet.

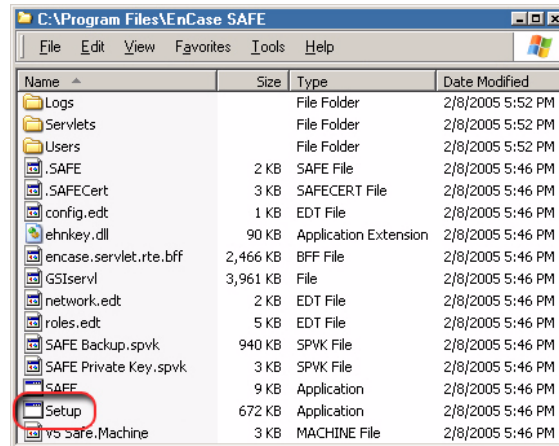


Figure 2-6: setup.exe in EnCase SAFE directory

Starting and stopping **enstart.exe** is a simple process. From the command prompt in the directory where **setup.exe** resides, type, “**setup**”. This starts the service and adds it to the Windows list of services to be started automatically upon boot. To stop the service, type, “**net stop enstart**” from a command prompt.

There are two ways to determine whether the **enstart** service is running; the best is to use the [Ctrl][Alt][Del] key sequence to enter **Windows Task Manager**. If **enstart.exe** is listed as a process, then the Servlet is running.

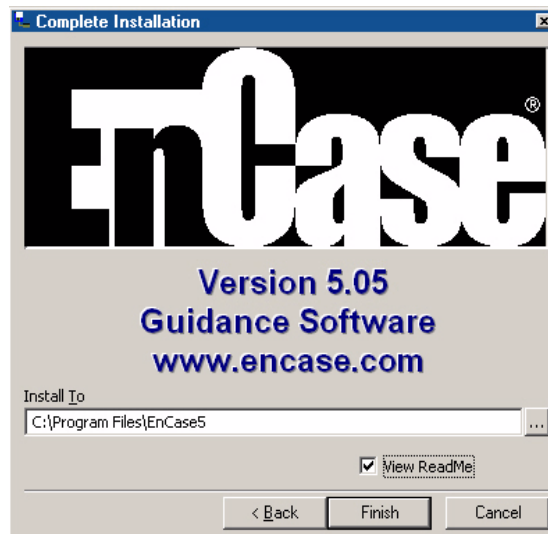


Figure 2-7: enstart.exe service in Task Manager

Another way of determining whether or not the service is running is by using **netstat -an** from the command line. Running **netstat** on the network device should indicate the port designated is in listening status (by default 4445). This is the EE current standard port for the **enstart.exe** Servlet.

```
C:\>netstat -an
Active Connections
Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0              LISTENING
TCP   0.0.0.0:445              0.0.0.0:0              LISTENING
TCP   0.0.0.0:3389            0.0.0.0:0              LISTENING
TCP   0.0.0.0:4445            0.0.0.0:0              LISTENING
TCP   0.0.0.0:5800            0.0.0.0:0              LISTENING
TCP   0.0.0.0:5900            0.0.0.0:0              LISTENING
TCP   10.0.35.18:139          0.0.0.0:0              LISTENING
TCP   127.0.0.1:1027          0.0.0.0:0              LISTENING
UDP   0.0.0.0:445             *:*
UDP   0.0.0.0:500             *:*
```

Figure 2-8: netstat -an on a network device

Software Updates

EnCase is continually being refined and updated in response to user requests. Minor updates and fixes are available on our web site.

To Download the Latest EnCase Version 5 Update

- Open Internet Explorer (or your favorite browser) and navigate to <http://www.guidancesoftware.com>. Once there, navigate to the message board. If you have any issues regarding the message board, please contact Tech Support. Be sure cookies are enabled.
- Click on the download link for the appropriate upgrade. Take care to get the correct language version, and edition (Enterprise and Forensic are available from the same download page, but require a different user name and password).
- Enter the required Security Key Serial Number and E-mail Address (used to register the software), and then click the **Send** link.
- Click on the appropriate download link; when the **File Download** pop-up window appears, click on the **[Save]** button.
- Note the executable directory, and click the **[Save]** button.
- When the executable has finished downloading, you can click on the **[Open]** button, or find the executable and double-click on it to install it, using the *Installation Instructions* above.

All evidence files, as well as case files from versions 4.18a and above are supported by the upgrade, however, Version 3 .CAS files will not open in Version 4 or 5 and

vice versa. Evidence files will open in any version of EnCase regardless of the version used to acquire them.



If the security key is inserted before clicking [Finish], EnCase will launch in Acquisition Mode, disabling the ability to preview and see file structure but allowing evidence acquisition. Reinstall the driver with the dongle removed to resolve this issue.

Configuration Questions

- **What systems will EnCase run on?**

You can acquire evidence with any PC that can run DOS, Linux or Windows versions Windows 2000, XP or 2003 Server; evidence files can only be examined on Windows 2000, NT, XP or 2003 Server PCs.

- **What systems will the EnCase servlet run on?**

The EnCase servlet `enstart.exe` can be installed on Windows operating systems from Windows 95 to Windows 2003 Server, with the `setup.exe` installer. The EnCase servlet `enlinuxpc` can be installed on Linux operating systems based on kernel 2.4 and above; and it was designed for the Red Hat, Mandrake, and SuSE distributions.

- **What is the optimal PC configuration to run EnCase for Windows on?**

See *Appendix D: The Forensic Lab*.

- **What file systems does EnCase Version 5 support?**

EnCase can interpret FAT12, FAT16, FAT32, NTFS, and EXT2/3, HFS and HFS+, FFS (BSD), UFS (Unix), Reiser, JFS and JFS2 (AIX), Palm and all CD and DVD file systems. EnCase Version 5 will also allow preview and acquisition of TiVo Series 1 and 2 hard drives.

If EnCase does not recognize the file system on the drive (HPFS for example), it will show unrecognized file system as an “unallocated cluster” file. Keyword and file-header searches are still possible, as is the ability to create bookmarks, but file names or folder structures will not be available. EnScripts can be executed against these file-systems as well.

Security Key Questions

- **When I run EnCase for Windows, I cannot see file structure, and the title bar reads “EnCase Acquisition”, yet my security key is plugged into the USB port / parallel port of my PC.**
- Make sure the drivers for the security key are installed, following the directions for proper installation; you cannot use a parallel port security key with EnCase V5.
- For EnCase Version 5, make sure your security key is an Aladdin HASP HL USB security key.
- In some cases, USB security keys fail for no apparent reason. This can often be traced to a hardware conflict between a SCSI card and the second IDE channel. Try removing devices or the SCSI card.
- Do not connect the security key into a USB hub.
- Ensure that your forensic machine is set to the correct date and time.
- Make sure that you do not have another Aladdin dongle inserted into the machine.
- The **C:\Program Files\EnCase5\Certs\encase.PCert** file may have become corrupted; delete this file and re-install EnCase.
- The security key could be defective. To determine if this is the case, please call our Technical Services department at 626-229-9191 or send e-mail to support@guidancesoftware.com.
- **If I purchased a parallel-port security key, can I exchange it for a USB security key (or vice-versa)?**

Version 5 works only with new HASP HL USB dongles. Dongles distributed for version 4 (parallel or USB) do not work with EnCase 5. Contact Guidance Software Customer Service department to replacing the dongle.

CREATING THE ENCASE BOOT DISK

Before starting a DOS acquisition, you should first create an EnCase Boot Disk. The EnCase Boot Disk is used to safely acquire digital media in DOS when a forensically sound acquisition in Windows is not possible.

Windows Acquisition Issues

Windows will write to any local hard drive it detects, sharing such files as the Recycle Bin and `desktop.ini`. Last Accessed dates and times will be changed, thus tainting the evidentiary integrity of the subject drive. Forensically sound acquisitions in Windows are not possible unless special write blocking, such as FastBloc, is used.

The 16-bit DOS operating system allows forensically sound acquisitions (write blocking) without taking special precautions. For that reason, whether acquiring via the bare bones boot disk or previewing via the EnCase Network Boot Disk (ENBD), examiners will need an EnCase (“bare bones”) Boot Disk which uses DOS rather than Windows.

Creating the EnCase Boot Disk

An EnCase Boot diskette is used to boot the computer to DOS. The support files on these disks have been modified to allow the diskette to boot to a non-writable state. The diskettes are used throughout the forensics process and are referred to throughout this manual. Follow the steps below to create this diskette.



There are two types of EnCase Boot Disk: the barebones boot disk (described here), and the EnCase Network Boot Disk (ENBD), detailed later in this chapter. The ENBD has the features of the barebones boot disk, but also allows for crossover cable previews \ acquisitions.

Steps to Create the EnCase Barebones Boot Disk

- Open an Internet browser and download the barebones boot disk image from Guidance Software's web site at <http://www.guidancesoftware.com> saving the bootfloppy.E01 file to the root EnCase directory (typically C:\Program Files\EnCase5)
- Launch EnCase for Windows.
- From the **Tools...** menu, select **Create Boot Disk...**

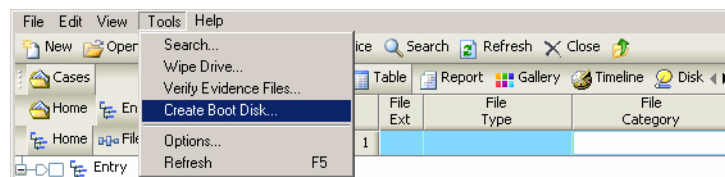


Figure 3-1: Create Boot Disk option

- Put a diskette in the drive (all data on the diskette are overwritten). Select the appropriate radio button (in most cases, **A:**) and click [**Next >**].

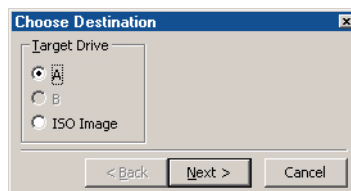


Figure 3-2: Select floppy drive

- The next screen provides several formatting options via radio buttons:
 - **Update existing boot floppy** - This option allows upgrading an EnCase boot disk from an earlier to a current EnCase version.
 - **Overwrite diskette with a boot floppy base image** - This option takes the EnCase boot disk image (**bootfloppy.E01**) and creates a boot disk from it. If a boot disk image of a different name is used, or is located somewhere besides the default location (**C:\Program Files\EnCase5**), you can specify the correct path or name by clicking on the ellipsis box to the right of the **Image path** field and browsing to the appropriate file and location. Select this option to create the boot disk as described in these steps, and then click [**Next >**].
 - **Change from a system diskette to a boot floppy** - This option allows **io.sys** and **command.com** on a boot floppy to be altered so that the hard drive's **io.sys** and **command.com** are not accessed at boot. Use this option only if a Windows 98 version of DOS is used.

- Select the appropriate option (typically **Overwrite diskette with a boot floppy base image**) and click [**Next >**]. A progress meter will appear in the **Copying Boot Image** field.

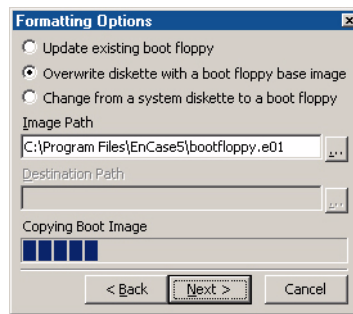


Figure 3-3: Select format option

- The **Copy Files** screen provides the capability of copying specific files (such as the EnCase DOS executable file, EN . EXE) to the floppy during the build process. This can also be done manually by clicking [**Finish**] and doing a copy via Windows Explorer or through the DOS COPY command. To add the file during the boot disk creation process, right click in the **Update Files** window and select **New**.



If this file has been copied using the menu option previously, the path will appear in the Update Files window. If this is the case, select the file and click [**Finish**].

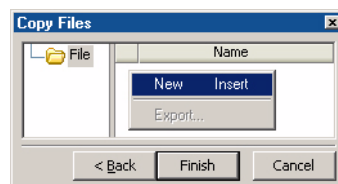


Figure 3-4: Specify files to copy

- Browse to and select the current EN . EXE, and then click [**Open**].

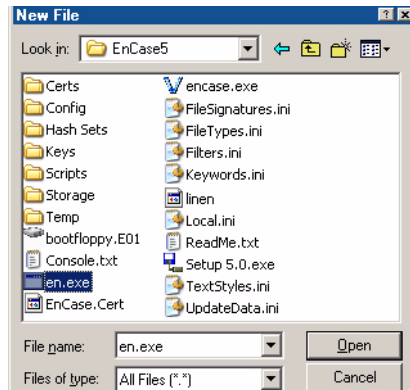


Figure 3-5: Find and select EN.EXE

- The path with the EN . EXE file will populate the window and be highlighted in blue. Click [**Finish**] to complete the disk creation process.

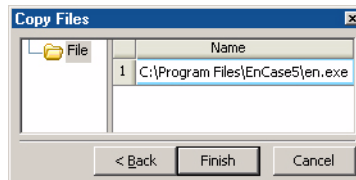


Figure 3-6: Copying files

- A progress meter will indicate that files are being copied to the floppy. When prompted that the disk was successfully created, click [**OK**].

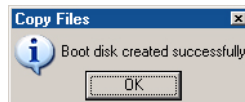


Figure 3-7: Successful disk creation

- Eject the EnCase Boot Disk and label it accurately.
- Be sure to test the new disk on a machine without drives that will be used as evidence, going by the guidelines set in the chapter on *EnCase for DOS*.

Creating an EnCase Boot CD

It is also possible to create a bootable CD to run EnCase for DOS. As with the diskette version, support files are modified to allow the diskette to boot to a non-writable state.

Keep a floppy and CD boot version in the forensic toolkit in case machines are encountered in the field without one. Create the CD as follows:

- Open an Internet browser and download the self-extracting executable for the ISO image at <http://www.guidancesoftware.com>.
- From the folder where the file was downloaded, double-click on the downloaded file to unzip the files into the directory where the file resides.
- Launch EnCase, and from the **Tools** menu, select **Create Boot Disk....**
- Click the **ISO Image** radio button and click [**Next >**] in the **Choose Destination** window.

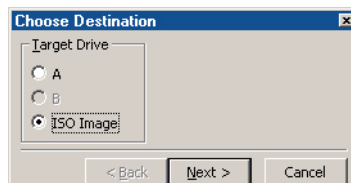


Figure 3-8: Choose ISO image as destination

- Change the **Image Path** to reflect the full path of the downloaded ISO image (e.g., **C:\Program Files\EnCase5\ENBCD420.iso**).
- Change the **Destination Path** to the path and filename of the new ISO image (e.g., **C:\Program Files\EnCase5\ENBCD50.iso**). Click [**Next >**].

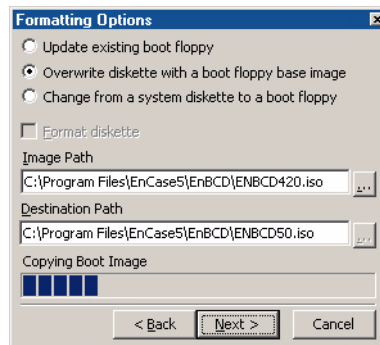


Figure 3-9: Setting paths for EnBCD

- The **Copy Files** screen provides the capability of copying specific files (such as the EnCase DOS executable file, **EN . EXE** or the EnCase **l i n e n** utility for Linux) to the floppy during the build process. This can also be done manually by clicking [**Finish**] and doing a copy via Windows Explorer or through the

DOS COPY command. To add the file during the boot disk creation process, right click in the **Update Files** window and select **New**.



If this file has been copied using the menu option previously, the path will appear in the Update Files window. If this is the case, select the file and click [Finish].

- Browse to and select the current EN . EXE, and then click [**Open**].
- The path with the EN . EXE file will populate the window and be highlighted in blue. Click [**Finish**] to complete the disk creation process.
- Refer to the documentation of the software manufacturer of the CD burning software you are using for instructions on creating a CD using the newly updated ISO image.
- Remove the EnCase Boot CD and label it accurately.

Be sure to test the new disk on a machine without drives that will be used as evidence, going by the guidelines set in the chapter on *EnCase for DOS*. Also note that if you are using the CD for doing a network crossover cable or parallel cable acquisition, you will need to make sure the EnCase Examiner software is running the same version of EnCase as the **EN . EXE** you updated to the CD.



The ISO image for creating the EnCase Boot CD (EnBCD) is provided as a courtesy of the Ontario Provincial Police, Electronic Crime Section.

Booting a Computer with the EnCase Boot Disk

Because of the uncertainty of a suspect machine's configuration, the process of booting the machine can be the riskiest part of the investigation. One mistake can lead to the accidental booting of the hard drive, which may alter or destroy evidence. A complete description of the boot process is beyond the scope of this manual, but the following guidelines will help aid the investigator to safely boot most PCs.



Follow your established procedure, usually dependant on Operating Systems, when shutting down a system.

- Confirm that the subject computer is powered off.
- Open the computer and inspect the inside for unusual connections or configurations. It is not unheard of for a computer to house a disconnected hard drive.
- Disconnect the power cables to all the resident hard drives.
- Insert the EnCase Boot Disk or EnCase Boot CD and turn on the computer. You can open the CD drive by pushing a paper clip into the small hole on the face of the drive while power is off.
- Run the CMOS (BIOS) setup routine to ensure that the computer is set to boot from the floppy drive (or CD ROM, if EnBCD used). Most systems display the correct setup key on the screen as the system boots. If not, the following is a list of common setup keys:
 - **Compaq Computers:**[F10]
 - **IBM Computers:**[F1]
 - **IBM clones:**[Del], [F2], [Ctrl][Alt][Esc] or [Ctrl][Alt][Enter]
- Verify that the computer is set to boot from the appropriate drive by reviewing the boot order settings, and note any changes made.
- Exit the BIOS setup and save changes.
- Allow the computer to continue to boot from the selected device. Confirm that a boot from the floppy or CD is possible. You may wish to attach a storage drive at this time to see if the system tries to boot from the hard drive.
- Power off the computer and reconnect the disk drive power cables.
- Confirm that the EnCase Boot Disk is still in the drive and turn on the computer, allowing the computer to boot from the floppy disk or CD.

EnCase Network Boot Disk

One way to preview and acquire media when hardware write blocking is unavailable is using the crossover or parallel cable acquisition method (detailed in the chapter titled *Network Cable Acquisitions*.) In order to perform this type of acquisition, you will need to create an EnCase Network Boot Disk (ENBD) or EnCase Network Boot CD. The various ENBD creation utilities are available from links in an article downloadable from Guidance Software's web site at <http://www.guidancesoftware.com>. Detailed instructions, including which ENBD utility to download and how to do a network crossover preview/acquisition, are included.

The ENBD is capable of auto-detecting network interface cards, as well as allowing the user to specify which network card to load drivers for. If the user allows the ENBD to auto-detect the card, the appropriate DOS driver should be loaded and EnCase for DOS is launched into server mode. If the user selects the manual method, the user must specify the network card in the subject's machine. ENBD then loads the appropriate DOS driver and launches EnCase for DOS. (additional information can be found in the chapter titled *EnCase for DOS*)

FAQs about EnCase Boot Disk

- **How do I make sure the computer does not boot to the hard drive on startup?**
- Physically unplug the hard drives before turning on the computer. Power on and run the BIOS setup routine to ensure that the computer is set to boot from the floppy drive (drive A:), or the CD if the EnCase Boot CD is used.
- To access the BIOS setup, you will need to press a specific key sequence repeatedly as soon as the power comes on. On most IBM compatible PCs, the key is [F1] or [Delete]. Compaq computers often use the [F10] key. If possible, check the computer's documentation. There is usually a message flashed on the power splash-screen indicating which key to press to access the BIOS setup.
- Once in the BIOS, look for the boot order section. After setting the BIOS to boot from the floppy disk, reboot the computer to confirm that it does. After confirmation, turn off the computer, reconnect the hard drives, and reboot the computer with the EnCase Boot Disk inserted in the floppy drive.
- **Does the EnCase Boot Disk prevent writing to the hard drive on boot up?**

Yes. When you create an EnCase Boot Disk, all references to C:\ are changed to A:\ in COMMAND.COM and IO.SYS to prevent files from being accessed on the C drive on boot up. By starting EnCase for DOS immediately, you will prevent any accidental access to the hard drive from that point.

ENCASE FOR DOS

EnCase for DOS is used primarily for performing acquisitions. The executable (EN.EXE), located in the EnCase installation folder (typically C:\Program Files\EnCase5), is copied to the EnCase Boot Disk during the creation process.

Launching EnCase for DOS

After creating the EnCase Boot Disk (see the ENBD section in the chapter on *Network Cable Acquisition*) and booting up the Subject system with the ENBD, type EN . EXE at the A:\> DOS prompt to launch EnCase for DOS.

EnCase for DOS Functions

While EnCase for DOS is used to put a subject computer into server mode so that it can be acquired, EnCase for DOS has other useful functions as well. All of these will be detailed in this chapter.

Locking / Unlocking (L)

The **Lock** command prevents the DOS operating system from inadvertently writing to a local hard drive. To successfully use this feature, the forensic investigator must know which hard drive to lock and unlock.



Figure 4-1: Unlocking a physical device



Drives can only be locked and unlocked when booted to DOS. Opening a DOS (Command prompt) window from within Windows does not give EnCase for DOS the access it needs to the hardware layers, nor is it forensically sound.

Acquiring

For more information, please see the chapter on *Drive to Drive Acquisition*.

Hashing

EnCase for DOS can generate a hash value for a drive. This can be used to compare the hash value EnCase for Windows reports for media acquisition to the hash value of the original media. To hash, press **[H]** for Hash.

Use the arrow keys to select the drive or volume and hit **[Enter]**.

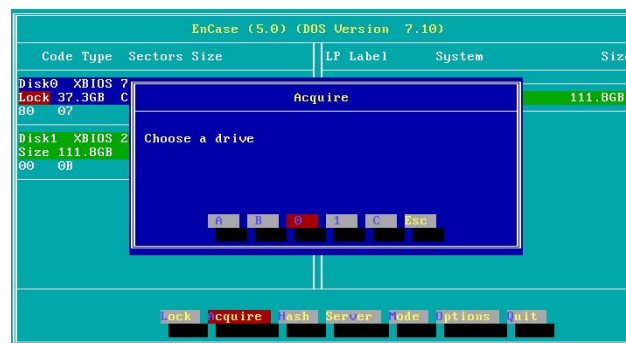


Figure 4-2: Choose a device or volume to hash

When prompted for a start sector, hit **[Enter]** to accept the default of 0. This will almost always be the value used.



Figure 4-3: Select hash Start Sector

Take the default value for stop sector unless you are hashing a SafeBack image. Hashing SafeBack images requires knowing the specific start and stop sectors of the image. Change the stop sector or accept the by hitting the **[Enter]** key.



You do not have to hash SafeBack images in EnCase for DOS, since in EnCase for Windows (version 4.19 and higher), SafeBack images can be brought directly into EnCase in the same manner as EnCase evidence files

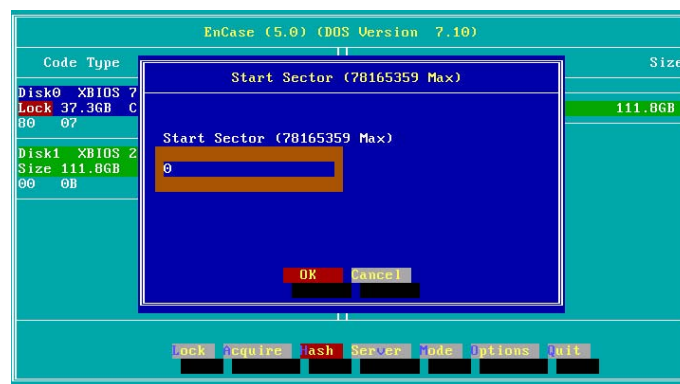


Figure 4-4: Select hash Stop Sector (SafeBack example)

When EnCase starts the hash, the option buttons at the bottom disappear, replaced by a hashing progress meter.

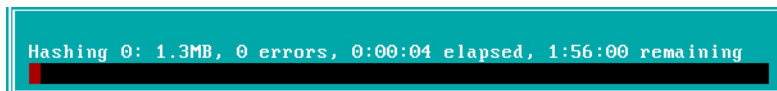


Figure 4-5: Hashing progress meter

When the device has been hashed, a status screen will appear with the hash value and the option to write the value to a file. The hash value can be written out to a text file on the floppy or an unlocked storage device with a FAT file system (the volume letter will appear in the right pane). To store this information, make sure the **[Yes]** button is highlighted in red (or press the **[Y]** key), then press **[Enter]**.

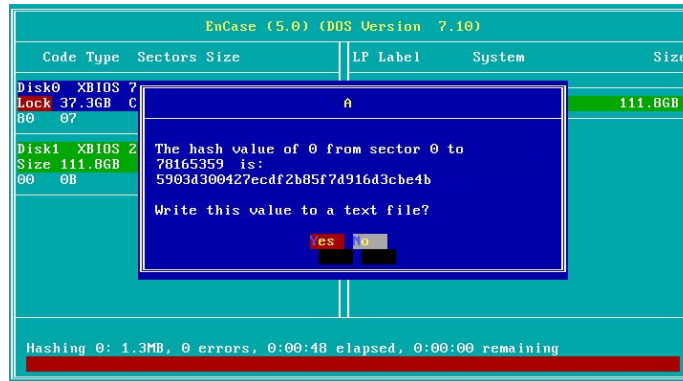


Figure 4-6: Hash status screen

Enter the complete path, including directory and filename, where you wish to store the hash value. You can store this on the A : \ drive, or on the unlocked storage drive, but make sure you have a valid path before entering the information. When the path has been entered, hit the **[Enter]** key. The hash value will be stored in a text file and you will be returned to the main EN . EXE menu.

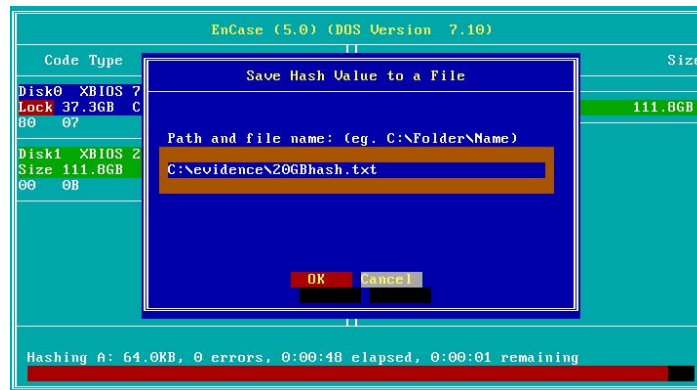


Figure 4-7: Saving hash value

Server

The subject computer must be placed in Server mode to acquire and preview subject media safely using the crossover or parallel port cable methods of acquisition. Before previewing or acquiring media on a subject machine, it is necessary to *prepare* the computer so that it can be previewed or acquired. The subject computer will have to be put in Server mode when performing either parallel port lap-link cable or crossover network cable preview and/or acquisition. When using the crossover cable,

put the subject machine in Server mode first; with a parallel cable preview, launch EnCase on the storage computer, open a case and click on the **[Add Device]** button before placing the subject computer in Server mode.

To put a computer into Server mode:

- Make sure the subject machine is configured to boot from the floppy as described in the *FAQs about EnCase Boot Disk* section in the chapter on *Creating the EnCase Boot Disk*.
- Insert the ENBD in the subject machine floppy drive and power it on.

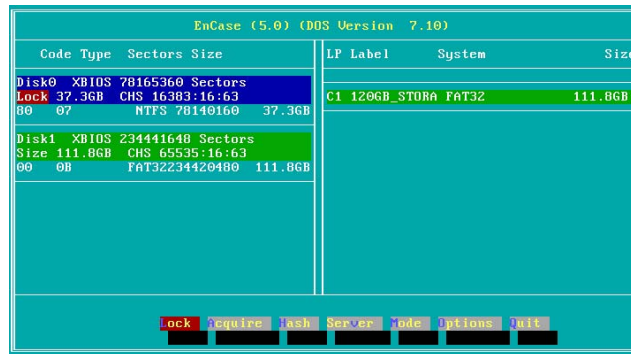


Figure 4-8: EnCase for DOS

- Physical disks are displayed on the left; FAT logical volumes (partitions) are displayed on the right. In the image above, the subject computer has two physical disks (**Disk0** and **Disk1**), with a single FAT32 logical volume (**C:**) on **Disk1**



Remember, the DOS operating system can only recognize volumes/partitions on FAT file systems. If an NTFS or EXT2 physical disk is listed on the left, no volumes will be displayed on the right.

- **Server Mode** must be set to allow for parallel port or network cable previews/acquisitions. To set the Server mode, press the **[V]** key.

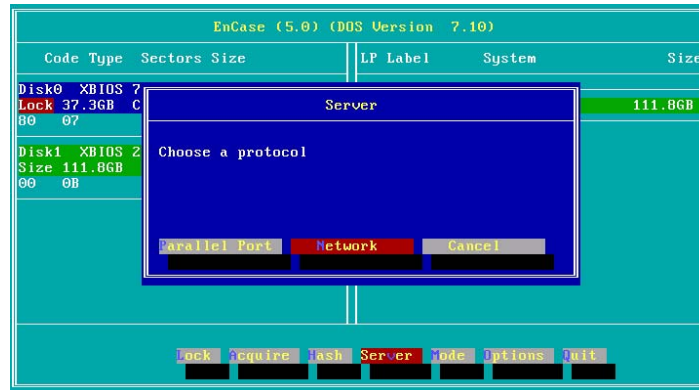


Figure 4-9: Choosing the protocol

- Choose the desired server protocol ([P] for Parallel and [N] for Network crossover cable), and then hit [Enter] to put the Subject computer in Parallel server mode.

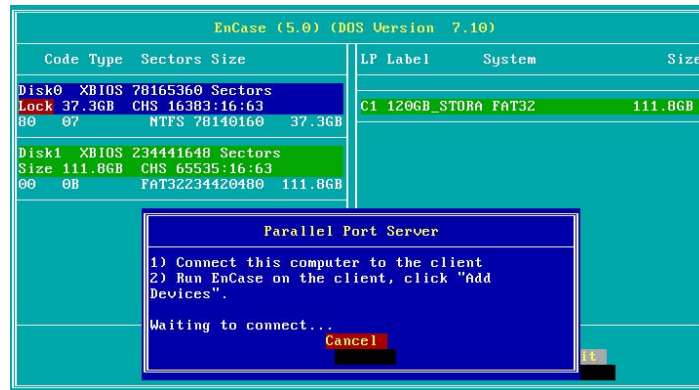


Figure 4-10: Parallel server mode



For an Examiner computer and a subject computer to successfully communicate through a parallel port cable or crossover network cable, the versions of EnCase (for both Windows and DOS) must match.

Mode

The Mode button is extremely useful when working with older computers that use legacy BIOS codes that underreport the number of cylinders on the hard drive. There

may be a small area of sectors at the end of the drive not accessed by the BIOS, and therefore not seen by EnCase for DOS.

EnCase addresses this limitation with the implementation of Direct Disk Access through the ATAPI interface. Select the **[Mode]** button by pressing the **[M]** key (or using the right arrow until the **[Mode]** button is highlighted in red), then press **[Enter]**. Use the right arrow until **ATA** is highlighted in red, then press **[Enter]**. EnCase will now access the drives via Direct ATA, providing accessibility to every sector of the hard drive.

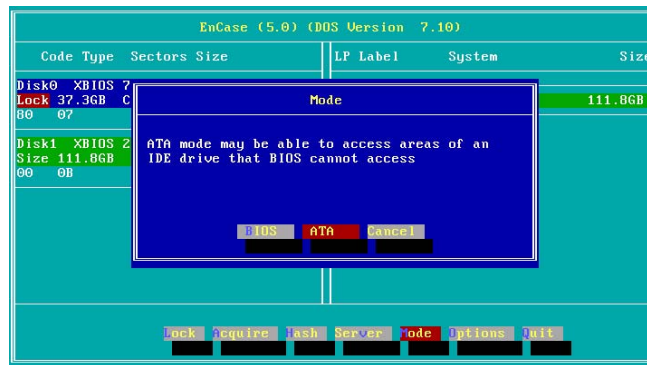


Figure 4-11: Direct ATA Mode

Quit

Select this option to quit EnCase for DOS. Quitting EnCase for DOS will return the machine to the DOS prompt.



Once EnCase for DOS has been closed, EnCase's software write-block on the local hard drives is no longer active. At this point, shut down the computer.

ENCASE LINEN UTILITY

The LinEn utility provides an alternate method of acquiring a device from using a FastBloc in Windows, or **EN.EXE** in DOS. This method allows you to acquire hard drives, USB and FireWire drives, and to apply a granularity which refines the number of sectors EnCase looks at one time. It also allows users to hash any device present on the Linux operating system it is running on. With the introduction of LinEn users are now able to acquire Linux machines via a crossover cable from the Windows EnCase client similar to the method used with EnCase for DOS. LinEn is dependent on the distribution of Linux it is installed on; for that reason there will be some variation in the setup in each distribution.

Description

The LinEn product is similar to EnCase for DOS (**EN.EXE**) in terms of the hashing and acquisition functionality. Among other benefits of using LinEn is its performance in hashing and acquisition. As with EnCase for DOS, LinEn also allows users to acquire a drive with greater precision around sectors with read errors through granularity settings. Features of LinEn include the following:

- **Drive-to-drive acquisition capability (logical partition to FAT32 partition)**

LinEn provides the ability to acquire a single partition, no matter what the format of that partition is. Partitions are acquired from the device where they reside in their native environment, requiring only a FAT32 storage drive to place the evidence on.

- **Drive-to-drive acquisition capability (physical device to FAT32 partition)**

Entire physical devices can be acquired, and the evidence files stored on a FAT32 storage partition. As with logical acquisitions, devices can be acquired

in their native environment, requiring only a FAT32 storage drive to place the evidence on.

- **Crossover cable acquisition capability**

Through a crossover connection, the user can preview or acquire a machine by putting the computer into “server mode” without having to open up the computer and physically remove any drives. This method can be used for acquiring RAID arrays on a server, or in the event that a field acquisition is only permitted after evidence is found via previewing the volume or device. As is the case with Drive-to-Drive acquisitions, a FAT32 storage drive is required to place the evidence on. The crossover method allows preview and/or acquisition of a device on a Linux-based machine, provided it has a properly installed NIC. You may need to specify an IP address when performing a crossover preview or acquisition. To determine the name of the network interface card, type “**ifconfig**” in the Console. Typically a compatible network card would show up as “**eth0**.” If this is the case, you need to specify an IP address by typing “**ifconfig eth0 10.0.0.1 netmask 255.0.0.0**” at the Console. A crossover acquisition will take longer than an acquisition via FastBloc.

- **Acquisition of and storage to FireWire and USB devices**

- With LinEn, you can acquire USB and FireWire devices. This feature can be useful for acquiring thumb drives, or hard drives within enclosures.
- As with any storage device in Linux, to store evidence to a FireWire or USB device, the device must first be mounted first; refer to your Linux manual for more information.

- **Hash analysis**

An MD5 hash can be run against an entire drive or an individual partition to generate a 128-bit MD5 checksum. The command can be used to compare the hash value that EnCase for Windows reports on an acquisition of media to the hash value for the original media.

- **Acquisition granularity for increasing the amount of data retained when bad sectors are encountered**

Historically, when a read error is found after an acquisition, the 64-sector block of data that contains the read error is “zeroed out” by EnCase (all of the data within the bad block is replaced with a 0). Through the use of granularity, the investigator has the flexibility to specify the number of sectors to zero out within a block of data generating a read error. What this means is that instead of all 64 sectors in a bad block being replaced by zeros, the user can narrow

down the number of sectors replaced by setting the granularity incrementally from 64 (the default value) to 1 in factors of two as shown below:

Granularity setting	64	32	16	8	4	2	1
Sectors zeroed per block	64	32	16	8	4	4	1



The lower the granularity (fewer sectors per block), the slower the acquisition will be.

LinEn Setup

Some configuration is needed before LinEn is able to run on a Linux distribution. Due to the nature of Linux and the number of distributions, only certain versions are listed here. We have enumerated the ideal methods of setup in order to effectively run the LinEn application in a forensically sound environment.

- Copy the LinEn file to the Linux system and note the folder where it resides.
- Disable the Automount File System setting to ensure the following:
 - the suspect drive is not accidentally accessed
 - an evidence file is not written to the subject drive

For SuSE 9.1

- Run **Yast**, located in **Main Menu / System / Configuration**.
- Open the **Runlevel Editor**.
- Make sure that the **autofs** feature is disabled.

For Red Hat

- Run **Services**, located in **Main Menu / System Settings / Server Settings**.
- Make sure that the **autofs** feature is unchecked.
- Start up Linux in console mode (LinEn will run from the GUI but for maximum performance we suggest running it from the Console.)
 - Edit the boot runlevel by modifying the **inittab** file residing in the **/etc** folder.
 - Find the line, "**id:5:initdefault:**" and change the '5' to a '3'. This changes the boot option so that Linux starts in console mode instead of the GUI interface.
 - Reboot the machine. Once the machine is restarted, it should start up in console mode. If it does not, re-check the **inittab** file.

- Navigate to the folder where the LinEn file resides and type “`./linen`” in the console to run it.

The screenshot shows the main LinEn screen with a teal background. It displays disk information for three disks: Disk0, Disk5, and Disk9. Each disk's details are shown in a table with columns for Code, Type, Sectors, Size, LP, Label, System, and Size. At the bottom, there is a terminal prompt with the text 'require ash Ser er uit]'.

Code	Type	Sectors	Size	LP	Label	System	Size
Disk0 /dev/hda Linux 78165360 Sectors							
Size 37.3GB							
00	B2	Linux Swap	1020096		hda1	/dev/hda1	Linux 498.1MB
00	B3	Linux EXT2	20972448		hda2	/dev/hda2	Linux 10.0GB
00	B3	Linux EXT2	9766512		hda3	/dev/hda3	Linux 4.7GB
00	0C	FAT32K	46406304		hda4	/dev/hda4	Linux 22.1GB
Disk5 /dev/hdd Linux 234375120 Sectors							
Size 111.8GB							
00	0C	FAT32K	40965750		hdd1	/dev/hdd1	Linux 19.5GB
00	0C	FAT32K	61432560		hdd2	/dev/hdd2	Linux 29.3GB
00	0C	FAT32K	65529135		hdd3	/dev/hdd3	Linux 31.2GB
Disk9 /dev/sda Linux 64000 Sectors							
Size 31.2MB							
80	01	FAT16	64448		sda1	/dev/sda1	Linux 31.4MB

Figure 5-1: Main LinEn screen

Drive-to-Drive Acquisition

Before performing a drive-to-drive acquisition, the investigator must be able to identify which device is the storage drive and which is the suspect drive. Type “`fdisk -l`” in the console to list all the devices. On typical desktop machines, the Operating System assigns the device name(s) as follows:

hdaPrimary master

hdbPrimary slave

hdcSecondary master

hddSecondary slave

SCSI, USB, and FireWire devices are typically labeled **sda**, **sdb**, **sdc**, etc...

- Start Linux in console mode using the modification described in setup.
- Mount a FAT32 storage partition.
 - Create a directory mounting for the partition (e.g. `/mnt/FAT32`) by typing in “`mkdir /mnt/FAT32`”
 - Mount the storage partition to the mount path using the command “`mount /dev/hda3 /mnt/FAT32`” - where “`hda3`” is the drive and partition.
- Navigate to the folder where LinEn resides and type “`./linen`” in the console to run LinEn.
- Choose the physical drive or logical partition you wish to acquire.



If a message is encountered stating “Permission denied”, type “`chmod 777 linen`” and re-attempt.

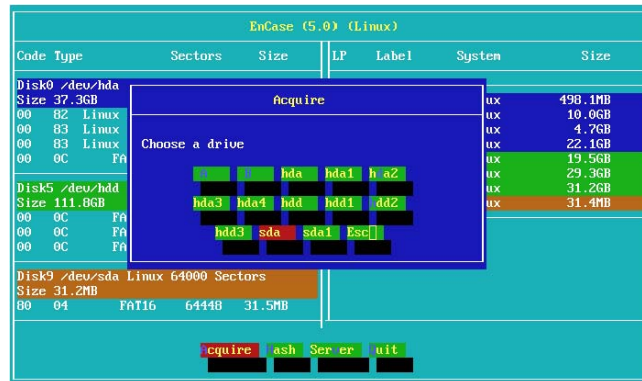


Figure 5-2: Choosing a drive to acquire

- Choose a storage path in which to place the evidence.
When specifying the storage path, you must input the mounting point of the partition (e.g. `/mnt/FAT32`). The example shows that the evidence file named `tdrive.E01` will be placed in the `/mnt/FAT32` folder.

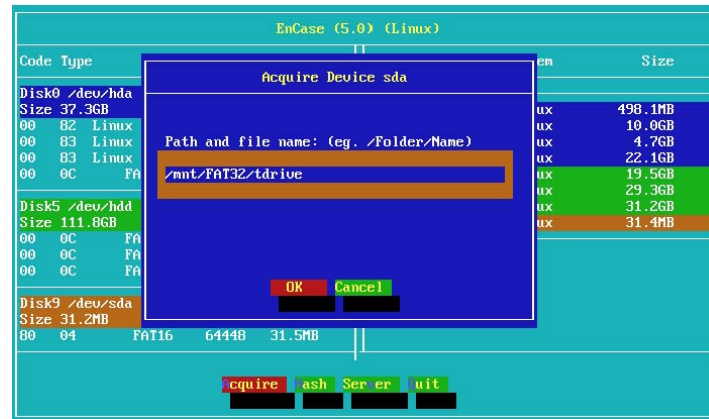


Figure 5-3: Specifying a storage path

Preview or Acquisition via Crossover

- Connect forensic machine to suspect machine using a crossover cable.

- Navigate to the folder where LinEn resides and type “`./linen`” in the console to run LinEn.
- Place machine in Server Mode by pressing [v] at the main screen, or using the right and left arrows until the **Server** option is highlighted and then pressing [Enter]. The subject machine should now be running in Server mode, displaying “**Waiting to connect...**”
- If nothing occurs when attempting to enable Server mode, ensure that an IP Address is assigned to the system and that the NIC is loaded as follows:
 - Exit LinEn
 - From the command line type: “`ifconfig eth0`”
 - Check to see if an IP address is listed for that device; if no IP address is listed then specify one by typing “`ifconfig eth0 10.0.0.1 netmask 255.0.0.0`”
 - Repeat the previous step once an IP address has been established.

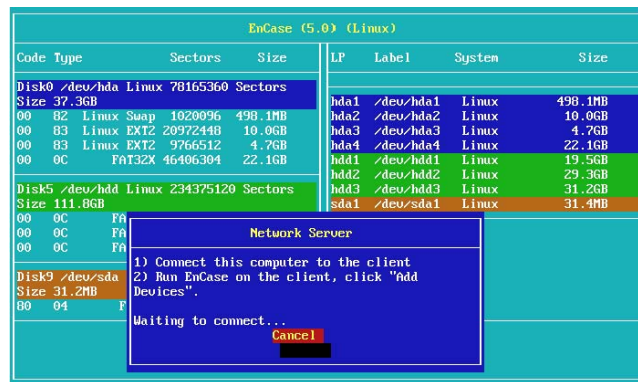


Figure 5-4: Putting LinEn in Server Mode

- Specify an IP address on the forensic machine (e.g., `10.0.0.50`).
- Launch EnCase on the forensic machine.
- Create a new case.
- Click on the [Add device] button.
- Blue-check **Network Crossover** and click [Next >].

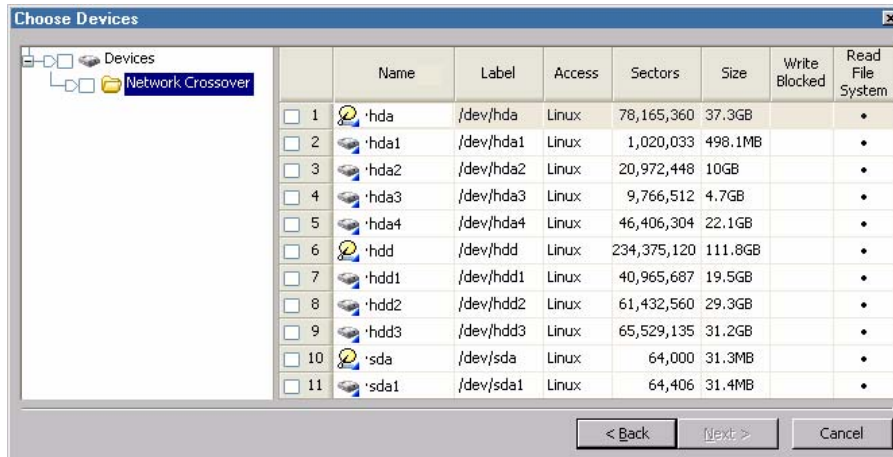


Figure 5-5: Available devices from Network Crossover

- Blue-check the physical disk or logical partition and click [**Next >**].
- Click the [**Finish**] button.

PREVIEWING VS. ACQUIRING

In EnCase for Windows, investigators preview a device before starting an acquisition. Preview can be saved in a case file without acquiring, however, if the device is accessed by another investigator or user before being acquired, contents of the device may have changed.

When running EnCase in **Acquisition** mode without a dongle inserted, you must preview a device prior to imaging it, but the preview does not show file structure. This does not prevent acquisition however.

Limitations of Previewing

Previewing media allows the investigator to view the media as if it has been acquired. An investigator previews media first in order to determine if a full investigation (acquisition and analysis) of the media must be performed. Previewing media is only available in EnCase for Windows.

Attaching a hard drive to the forensic machine and booting to Windows without write blocking in place will alter data on that drive. Unless a write-blocking device is used, changes to this drive will occur regardless of the precautions that EnCase makes, because of swap file activity.



It is possible to preview a local hard drive safely (without changing the media) if write-blocking, such as a FastBloc, is used. If write-blocking is not available, previews should be conducted through the parallel-port cable or crossover network cable with DOS disk on target machine.

The preview feature is so easy to use that many investigators mistake the preview for the actual acquisition. Be aware that although it is a quick way to find evidence, and it is still possible to save evidence results, the preview feature will only allow you to view case results while physically connected to the subject media.

Advantages of Previewing

By previewing a drive, the investigator does not have to wait to finish an acquisition before doing a preliminary examination. While previewing, you can run keyword searches and create bookmarks. Search results and bookmarks can be saved into a case file; however, each time the case is opened, the subject media must be physically connected to the Examiner machine and ready to be previewed.

Live Device and FastBloc Indicators

EnCase overlays a blue triangle in the lower right corner of the device icon to indicate a live (previewed) device. Logical volumes and physical drives write blocked by FastBloc are indicated by a blue square around the icon. The icon makes it easy to identify the devices which are protected and which are live. For steps on previewing and acquiring with FastBloc in Windows, please refer to the chapter on FastBloc Acquisitions.

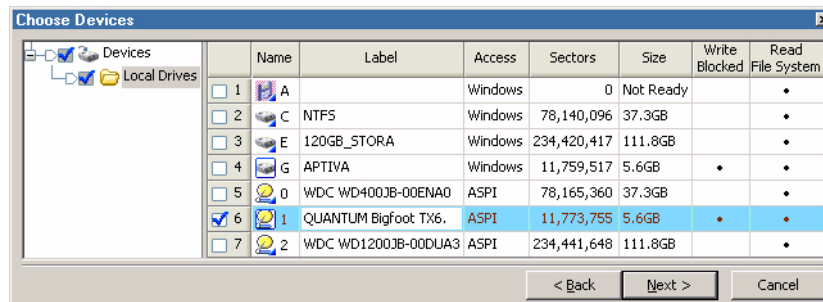


Figure 6-1: Devices with live preview and FastBloc indicators

Preview Questions

- **Can I Copy/UnErase files when I am previewing a Subject computer?**

Yes. Most EnCase functions are available while previewing a drive.

- **Can I preview Linux and Unix computers?**

Yes. The Linux or Unix drive must be attached to a computer booted with an EnCase Network Boot Disk (or LinEn) and running in Server Mode. The investigator would then preview via the parallel port or crossover network cable with his lab computer.

- **Why does my laptop computer shut down when I am trying to preview the Subject computer?**

Laptop computers, and many desktops, have power-saving features in the BIOS. These features will shut down ports or hard drives down to save energy after a given time. Disable this feature during setup on both subject and storage computers.

Acquisition Questions

- **How can I verify an evidence file to see if it is still intact?**

Select it from within the **Cases** tab, right-click, and choose **Verify Evidence Files....**

- **I am acquiring a huge drive. My evidence files are up to .E99. Can I still create more evidence file chunks?**

Yes, EnCase will keep creating them, beginning at **.A01**.

- **If my data drive fills with evidence files, do I have to stop the acquisition and start over with a larger drive>**

No. Attach another hard drive, or point to another hard drive that you have already attached and continue acquisition.

PARALLEL PORT CABLE ACQUISITION

Use the parallel port method of acquisition only when no other method of acquisition or preview is viable because of the slow speed of the process. This may include:

- When acquiring a laptop computer hard drive that cannot easily be removed and with no DOS-supported PCMCIA or on-board network interface card
- When acquiring a computer hard drive when no write-blocking device is available and there is no DOS-supported network interface card
- When acquiring a hardware RAID that is in a computer that does not have an on-board IDE channel

When acquiring using the parallel port and lap-link (null modem) parallel cable, the subject computer must be booted to DOS using the EnCase Network Boot Disk.

Parallel Preview \ Acquisition Process



It is imperative that the following steps be performed in the order shown to ensure a proper connection.

- Ensure EnCase on DOS and Windows machines match prior to acquisition.
- Make sure the subject machine is configured to boot from the floppy as described in the *FAQs about EnCase Boot Disk* section of this manual.
- Connect the two computers with the parallel port lap-link (null-modem) cable.
- Boot the storage computer into Windows.
- Launch EnCase and open a new case by clicking on the [**New**] button.
- Click the [**Add Device**] button or select **Add Device** from the **File** menu.

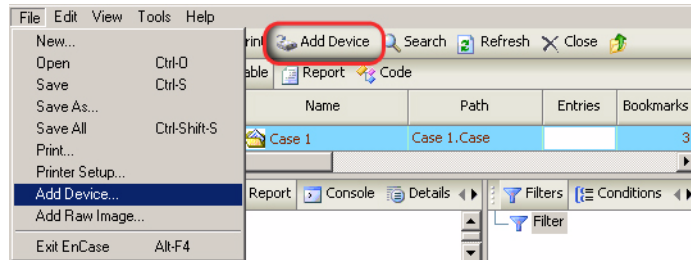


Figure 7-1: Adding a device

- Boot the subject computer with an EnCase Boot Disk (see the chapter on *Creating the EnCase Boot Disk*).
- Put the subject computer in Parallel server mode (see *EnCase for DOS*).
- In the **Add Device** wizard, blue check **Parallel Port** and click [**Next >**].

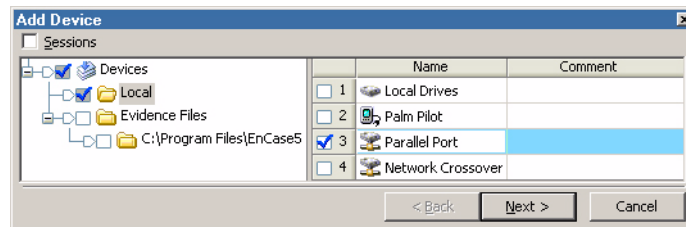


Figure 7-2: Selecting parallel port device

- Blue check a device or volume, then click [**Next >**]. Only the remote drives will be shown if the parallel port has been selected as the source.

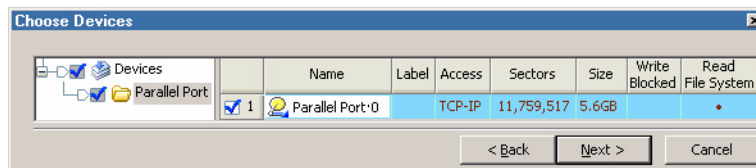


Figure 7-3: Drives available through the parallel port



If the Storage computer does not see the subject computer through the parallel port, try setting the parallel port in the BIOS of both machines to either ECP or EPP or ECP+EPP. Alternately, you can try rebooting one or both computers.

- At this point, double-clicking the media will allow the properties of the media to be edited, such as device name, case number, and more. Confirm the drive to add, and click [**Finish**].

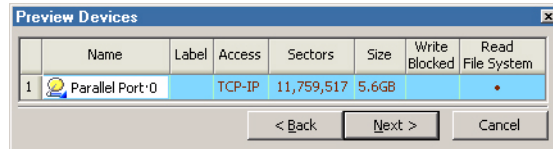


Figure 7-4: Confirming the drive to preview

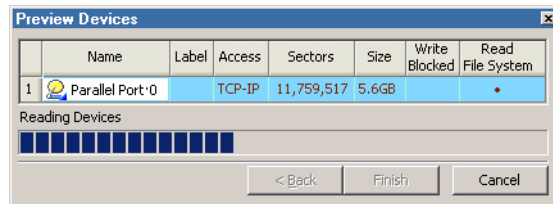


Figure 7-5: Adding preview via Add Device wizard

- Once the drive is previewed, right-click on the physical icon under the Cases tab and select **Acquire**, or click on the [Acquire] button at the top tool bar.

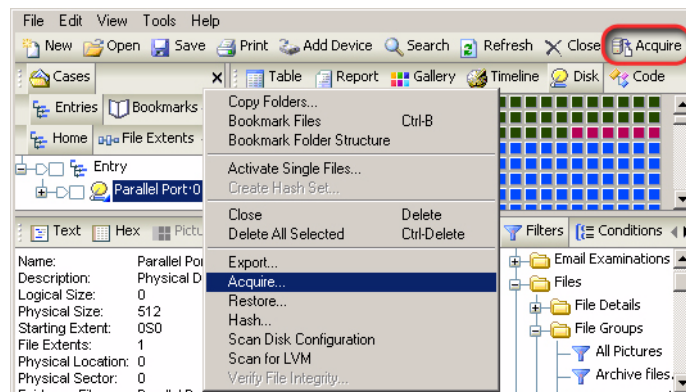


Figure 7-6: Acquiring previewed media

- A screen appears providing options for tasks to perform after the acquisition. The **New Image File** section provides three options:
 - **Do not add** – saves the device as an EnCase evidence file, but does not add it to the open case. This option leaves the preview intact.
 - **Add to Case** – saves the device as an EnCase evidence file, and adds it to the open case. This option also leaves the preview intact.
 - **Replace source device** (recommended) – Saves the device as an EnCase evidence file, adds it to the open case and removes the preview. This option does not alter the source device being acquired, and allows maintaining any bookmarks

set in preview mode. The other options in this window are for **Search, Hash and Signature Analysis** and **Restart Acquisition**. Checking the **Search, Hash and Signature Analysis** option will start the process automatically after the acquisition.

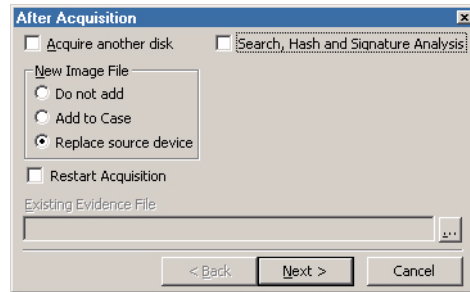


Figure 7-7: Acquisition options

- If the **Search, Hash and Signature Analysis** option is checked, a screen will appear to allow you to set the parameters for those tasks.

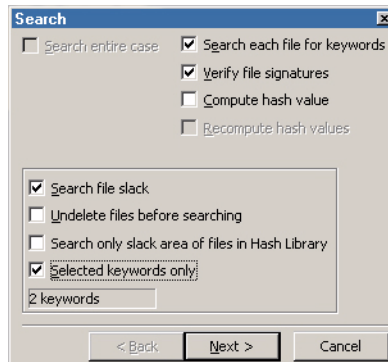


Figure 7-8: Search, Hash and Signature Analysis options

- Define the evidence file settings. Generally, **Best** compression can be used with parallel acquisitions as evidence can usually be compressed faster than it is transferred over the cable. Click [**Finish**] to begin the acquisition.

The screenshot shows the 'Options' dialog box with the following details:

- Name:** Quantum 5.25 GB HDD
- Evidence Number:** 001
- Notes:** Quantum 5.25 GB HDD from Jones machine
- File Segment Size (MB):** 640
- Start Sector:** 0
- Stop Sector:** 78165359
- Compression:** Good (Slower, Smaller) (selected)
- Generate image hash:**
- Block size (Sectors):** 64
- Error granularity (Sectors):** 64
- Output Path:** E:\Evidence\Jones Case\Quantum 5.25 GB HDD.E01

Figure 7-9: Acquisition options



Archive with the default 640MB “chunk” file size for easy CD-R archiving. Even if using a DVD-R burner, seven 640MB “chunks” fit comfortably onto a DVD-R.

If the Storage drive fills up during an acquisition, EnCase will prompt the user to redirect the data to a user-defined location. Unless the storage computer contains hard drives that are hot-swappable, EnCase must be directed to another form of media in your computer that already has a drive letter—for example, a second storage hard drive or mapped networked drive. If acquiring to Zip or Jaz disks, eject the full disk and insert another.

If the acquisition is terminated by the user prior to completion, the user can start the acquisition again and check the previously mentioned **Restart Acquisition** box. The grayed out **Acquisition File Path** field will become active, allowing the user to input or browse to the path (including first evidence file segment name) where the acquisition was saving the evidence file, as shown below:

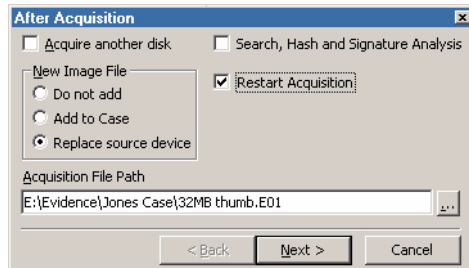


Figure 7-10: Restarting an acquisition

The **Options** window will appear again, although only the **File Segment Size** can be changed.

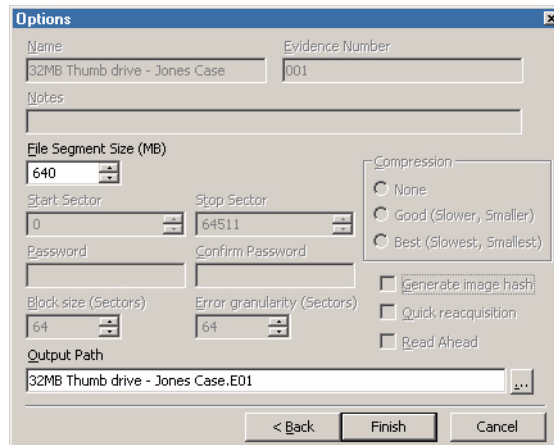


Figure 7-11: Acquisition restart options

After an acquisition has completed successfully:

- Power down both computers.
- Disconnect the parallel port cable
- Place the subject hard drive in a safe location
- Remove the boot floppy from the floppy drive
- Boot to Windows on the lab system

NETWORK CABLE ACQUISITION

EnCase allows users to preview and acquire data via the crossover network cable.



Previewing and acquiring with this method only works with a crossover cable. A yellow crossover cable was shipped with your EnCase software. Crossover cables are Ethernet cables using RJ-45 connectors, where one end of the cable is wired so that the Receive signal pins on one connector are connected to the Transmit signal pins on the other side. They are designed for direct workstation-to-workstation connectivity. A common CAT5 “straight-through” Ethernet cable will not work, nor will previews \ acquisitions across a LAN, unless using EnCase Enterprise.

Creating the EnCase Network Boot Disk (ENBD) or LinEn CD

Making a crossover network cable acquisition work requires loading a DOS packet driver so that EnCase for DOS can communicate with the installed PCI or PCMCIA network interface card (NIC), or loading the drivers through Linux via the EnCase LinEn CD.

EnCase Network Boot Disk (ENBD)

Guidance Software provides investigators with a downloadable creation utility for the EnCase Network Boot Disk (ENBD, created by the Ontario Provincial Police e-crime section) to facilitate the detection and loading of the correct DOS packet driver. The boot disk has the ability to manually or automatically detect NICs and load the drivers, giving the examiner maximum convenience and flexibility when acquiring or previewing media.

- Auto-detect automatically attempts detection of the NIC in the subject and forensic computers.
- Manual functionality allows the investigator to specify the NIC driver to load from a list of supported cards.

There are multiple ENBDs available for download, depending on the type of NIC in the subject computer. To create an ENBD:

- Go to <http://www.guidancesoftware.com>, select the support then downloads buttons and scroll down the page to download the appropriate ENBD.
- Place a blank, formatted floppy diskette in your floppy drive.
- Double-click on the downloaded ENBD file and proceed through the creation wizard until it is complete.
- The ENBD can detect and load SCSI device drivers for different SCSI controller cards as well as network cards. Refer to the table below for all cards currently supported:

<p>PCI cards supported for auto and manual loading:</p> <ul style="list-style-type: none"> • 3COM 10/100 V.90 Mini-PCI Combo Card • 3COM EtherLink III Series • 3COM EtherLink XL Series • 3COM EtherLink 10/100 with 3XP (3C990) • ACCTON EN1207D-TX/EN2242A Series • ACCTON EN5251 Series • ADMTEK PCI 10/100 Series • AMD PCNet Series • COMPAQ 10/100 and Gigabit • COMPAQ NetFlex-3 • DAVICOM PCI-Based Series • DIGITAL 2104x/2114x 10/100 Series • D-LINK DFE-530TX+ 10/100 Series • D-LINK DFE-550TX 10/100 Series • HP 10/100VG NDIS 2.01 Driver • INTEL PRO Series • INTEL PRO/1000 Server Series • LITE-ON PNIC-10/100 Series • MACRONIX MX987xx Series • NATIONAL DP83815 10/100 MacPhyter Series • NETGEAR FA310TX Adapter • REALTEK RTL8029 Series • REALTEK RTL8139/810X Series • SIS 900/7016 SIS900 10/100 Series • SMC Fast Ethernet 10/100 (1211TX) • SMC EtherPower II 10/100 (9432TX) • VIA PCI 10/100Mb Series • WINBOND W89C940F 10 PCI Adapter 	<p>PCMCIA cards supported for manual loading only:</p> <ul style="list-style-type: none"> • 3COM 3CCFE574 Family • 3COM 3CCFE575 Family • INTEL 16-BIT Series • INTEL 32-BIT Series • XIRCOM CE3B-100BTX (non-CardBus) • XIRCOM RealPort / Realport2 R2BEM56G-100 <p>SCSI controller cards supported for auto and manual loading:</p> <ul style="list-style-type: none"> • AIC-78XX/AIC-75XX • AIC-7890/91 • AMD PCscsi • BusLogic MultiMaster • IBM ServeRAID • Initio INI-9XXXU/UW • Initio INI-A100U2W • Symbios 53C8xx
---	--

- Copy C:\Program Files\EnCase5\en.exe to the ENBD. The same version of EnCase must exist on both the ENBD and the forensic machine.

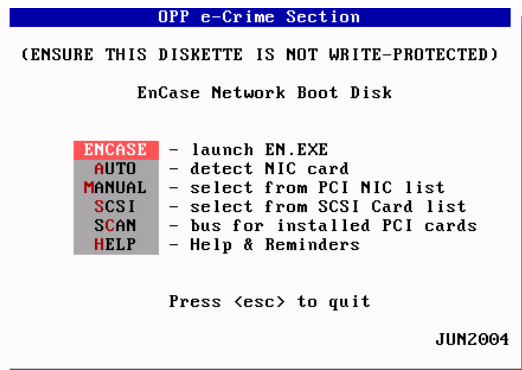


Figure 8-1: The EnCase Network Boot Disk menu

EnCase LinEn Utility

The LinEn utility discussed previously in the EnCase LinEn Utility chapter provides an alternate method of previewing or acquiring a device via crossover cable using EnCase for Windows. The distribution of Linux will determine the support for network interface cards, SCSI and USB devices. Refer to the *EnCase LinEn Utility* chapter of this document for information on creating the EnCase LinEn Utility CD.

Using the ENBD

- Make sure the subject machine is configured to boot from the ENBD floppy as follows:
 - Physically unplug all the hard drives before turning on the computer.
 - Power on and run the BIOS setup routine to ensure that the computer is set to boot from the floppy drive (drive A:) if the ENBD is used, or the CD ROM drive if the EnCase Boot CD is used. To access the BIOS setup, you will need to press a specific key sequence repeatedly as soon as the power comes on. On most IBM compatible PCs, the key is [F1] or [Delete]. Compaq computers often use the [F10] key. If possible, check the computer's documentation. There is usually a message flashed on the power splash-screen indicating which key to press to access the BIOS setup.
 - In the BIOS, look for the boot order section. After setting the BIOS to boot from the appropriate device with the boot diskette or CD in the drive and the hard drives still disconnected, reboot the computer to confirm that it does.
 - After confirming that the computer boots from the correct device, turn off the computer.

- Reconnect the hard drives and reboot the computer with the media still in the drive.
- Connect the subject computer to the storage computer via crossover cable.
- On the subject machine, the current ENBD displays the following menu options on startup:
 - **Network Support** - Loads appropriate menus for crossover acquisition
 - **USB – Acquisition (no drive letter assigned)** - Loads DOS USB drivers to allow the acquisition of a USB-connected device
 - **USB – Destination (drive letter assigned)** - Loads DOS USB drivers to allow storage to a USB-connected device
 - **Clean boot** - Loads similar to the barebones boot disk to do a direct DOS acquisition
- As shown in the figure at the top of the previous page, select **AUTO** from the menu to allow the ENBD to detect the NIC, or select **MANUAL** to load the packet driver manually. If **AUTO** is selected, the prompt allows the user to press any key to accept the drivers, at which point EnCase launches and automatically runs in Network Server mode



Be sure to observe that the NIC was detected without errors on both sides before proceeding with the preview/acquisition.

- If the driver is loaded manually, choose **ENCASE** from the menu to launch EnCase. You can also run EnCase to do a direct DOS acquisition by typing **EN . EXE** at the command prompt.

```

EnCase (5.0) (DOS Version 7.10)

Code Type Sectors Size LP Label System Size
-----
Disk0 XBIOS 78165360 Sectors
Lock 37.3GB CHS 16383:16:63 C1 120GB_STORAGE FAT32 111.8GB
80 07 NTFS 78140160 37.3GB

Disk1 XBIOS 234441648 Sectors
Size 111.8GB CHS 65535:16:63
00 0B FAT32234420480 111.8GB

Lock Require Hash Server Mode Options Quit
  
```

Figure 8-2: EnCase for DOS user screen

- Put EnCase for DOS in Server mode by using the arrow keys to select the **[Server]** button and clicking **[Enter]**.
- Choose **Network**. The subject machine should now be running in Server mode, displaying a message stating **Waiting to connect...**
- Connect from the Windows forensic machine as described in the *Preview or Acquisition* section of this chapter.

Using the EnCase LinEn Utility

- Make sure the subject machine is configured to boot from the EnCase LinEn Utility CD as follows:
 - Physically unplug all the hard drives before turning on the computer.
 - Power on and run the BIOS setup routine to ensure that the computer is set to boot from the CD ROM drive. To access the BIOS setup, you will need to press a specific key sequence repeatedly as soon as the power comes on. On most IBM compatible PCs, the key is **[F1]** or **[Delete]**. Compaq computers often use the **[F10]** key. If possible, check the computer's documentation. There is usually a message flashed on the power splash-screen indicating which key to press to access the BIOS setup.
 - In the BIOS, look for the boot order section. After setting the BIOS to boot from the CD ROM, with the LinEn CD in the drive and the hard drives still disconnected, reboot the computer to confirm that it does.
 - After confirming that the computer boots from the correct device, turn it off.
 - Reconnect hard drives and reboot with the media still in the CD ROM drive.
- Connect the subject computer to the storage computer via the crossover cable.
- Navigate to the folder where LinEn resides and type “**./linen**” in the console to run LinEn.
- Place machine in Server Mode by pressing **[v]** at the main screen, or using the right and left arrows until the **Server** option is highlighted and then pressing **[Enter]**. The subject machine should now be running in Server mode, displaying “**Waiting to connect...**”

Troubleshooting LinEn connectivity issues

If nothing occurs when attempting to enable Server mode, ensure that an IP Address is assigned to the system and that the NIC is loaded as follows:

- Exit LinEn
- From the command line type: “**ifconfig eth0**”
- Check to see if an IP address is listed for that device; if no IP address is listed then specify one by typing “**ifconfig eth0 10.0.0.1 netmask 255.0.0.0**”

Once an IP address is established, repeat the previously mentioned steps to connect.

Preview or Acquisition

LinEn can be run off a Linux boot CD with LinEn on it or from a standard Linux distribution installation. For instructions on preparing LinEn to run from either, see the chapter of this document on the *EnCase LinEn Utility*.

- Boot the forensic PC into Windows.
- Assign a fixed IP address to the storage computer, as follows:

Windows XP SP2

When the Examiner's operating system is Windows XP Service Pack 2, Windows Firewall may be running; if so, you will need to configure Windows Firewall to allow EnCase traffic for the crossover cable acquisition to work properly as follows:

- From the Windows [**Start**] button, select **Settings**, then choose **Windows Firewall** in the Control Panel

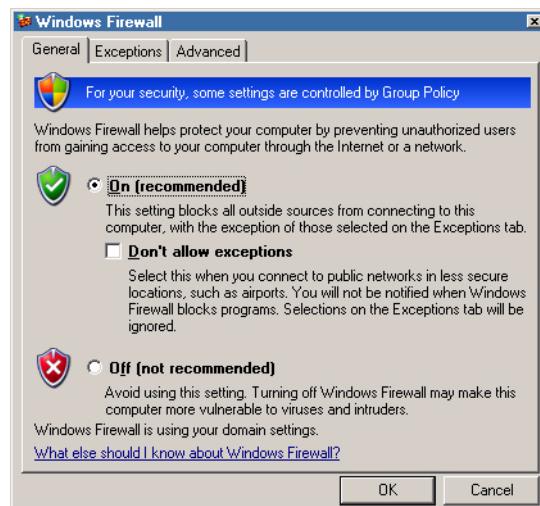


Figure 8-3: Windows Firewall control panel

- By default, the Firewall is set to **[On]**; the **Don't allow exceptions** box should be unchecked. If it is set to **[Off]**, Windows Firewall has been turned off and will not interfere with any functionality, and you can skip this process. If the Firewall is on, click on the **Exceptions** tab at the top of the window.

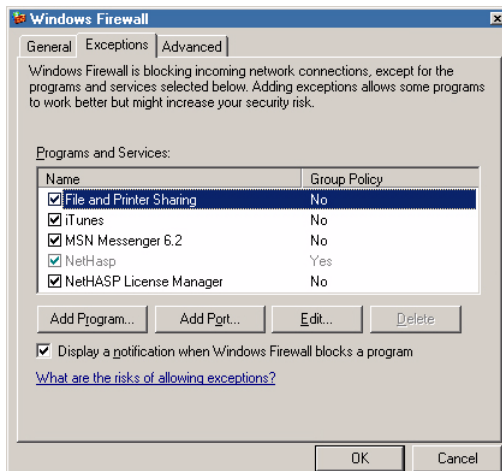


Figure 8-4: Windows Firewall Exceptions tab

- Click on the **[Add Program...]** button.

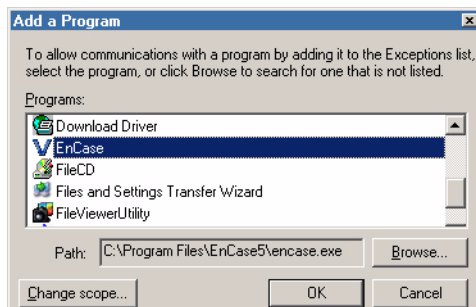


Figure 8-5: Adding an exception

- Find EnCase in the list in the **Programs** window and select it, or click the **[Browse...]** button to find the EnCase executable (by default, C:\Program Files\EnCase5\encase.exe) so that it shows in the **Path:** field.
- Click the **[OK]** button.
- Click **[OK]** in the main Windows Firewall to allow crossover preview\acquisition.
- Continue to configure the Examiner's machine as described in the following section

Windows 2000, XP, and 2003

- Right-click on **My Network Places** and select **Properties**.
- Right-click on **Local Area Connection** and select **Properties**.
- Double-click the TCP/IP protocol.

- Enter a fixed IP address (e.g., 10 . 0 . 0 . 50) in the **IP Address** tab.
- Enter a sub-net mask of 255 . 255 . 255 . 0.
- Click on the **[OK]** button.
- The **WINS** and **DNS** settings must be removed. Those will prevent the connection from taking place over the crossover network cable.
- Launch EnCase for Windows.
- Click the **[ADD DEVICE]** button on the top tool bar.
- Place a blue check in the box to the left of **Network Crossover**. EnCase will connect to the subject computer running in server mode. You can then preview/ acquire as outlined in the previous chapter.

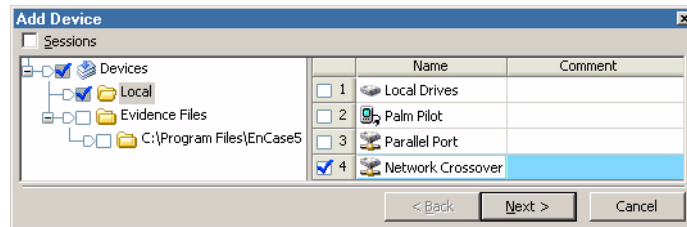


Figure 8-6: Network crossover acquisition

EnCase overlays a blue triangle in the lower right corner of the device icon to indicate that the device is live.



Figure 8-7: Blue triangle indicator for live devices

DRIVE-TO-DRIVE DOS ACQUISITION

One method of acquisition takes place entirely within EnCase for DOS. Typically, the Subject IDE hard drive will be placed in the Storage computer so that both the Subject and Storage IDE drives are on the same motherboard, hence the term “drive-to-drive”. There is no server mode in a drive-to-drive acquisition.

Drive Geometry Problems

Performing a drive-to-drive acquisition in the Subject computer’s environment might be necessary in certain situations. This method avoids any drive geometry problems that might result if the Subject hard drive is removed from its native environment.

As an example to illustrate this issue, assume a 20GB hard drive in the subject computer has a Phoenix BIOS from 1997. With the drive in a top-of-the-line computer with an Award BIOS from 2002, it is entirely likely that the BIOS in each are set to auto detect hard drives. Since they are different, they will likely also auto detect the same hard drive at a slightly different cylinders-heads-sectors setting. If you acquire drive-to-drive in the storage (forensic) system, you *might* encounter sporadic error messages or not see every sector that the Subject computer used. The solution would be to reacquire the original media in the media’s original (native) environment.

The caveat is that you must be certain the subject computer is set to boot from a diskette and not the hard drive. This can be checked in the BIOS. Ensure all hard drives are disconnected when booting the first time via diskette to ensure the subject computer will boot from the EnCase Boot Disk, *not* the subject media. If you are uncertain, it may be better to acquire the subject media in the forensic computer, although as previously mentioned, you may encounter drive geometry problems.

Benefits and Drawbacks

If a FastBloc is not available, the drive-to-drive acquisition is the fastest way to perform an acquisition without compromising the data. Data is transferred over an IDE ribbon cable, a much faster pipeline than a parallel port lap-link cable or crossover network cable.

There is a risk to the drive-to-drive acquisition: if both drives are the same make and model, and the storage partition is not labeled “**STORAGE**” (or something similar), it can be difficult to determine which drive to acquire *to* and which drive to acquire *from*. In that situation, it would be easy to acquire the *Storage* hard drive to the *Subject* hard drive, which could overwrite the unallocated space on the subject drive, thus altering it.

Steps to Follow

- Attach the subject hard drive to an IDE ribbon cable on the storage computer (or visa-versa to avoid drive geometry problems). Note that EnCase for DOS can only store evidence on a device formatted FAT32.
- Boot the storage computer with an EnCase Boot Disk.
- Launch EnCase for DOS (type EN at the a : \> prompt).
- All drives are locked by default, preventing the computer from writing to any drive by accident. Click [L] for LOCKING and specify the storage drive to unlock it.
- Click the [A] key to acquire.
- Choose the subject drive to acquire.

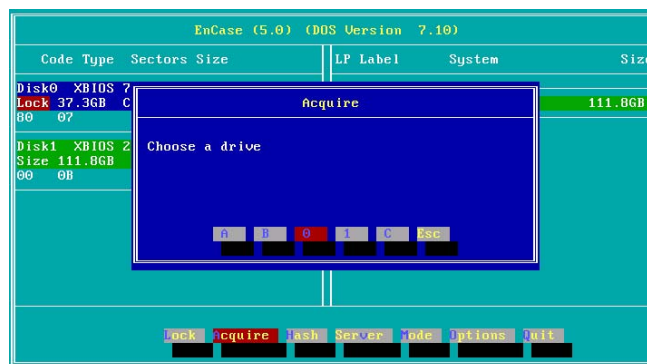


Figure 9-1: Starting acquisitions in EnCase for DOS

- EnCase prompts for the path to store the evidence file. Enter an unused file name on the storage drive attached to the subject computer (e.g., D:\DISK1) and then press **[Enter]**. It is a good idea to always create a uniquely named folder to hold evidence files. Avoid using the root directory, as the possibility exists that you could write to the wrong drive.

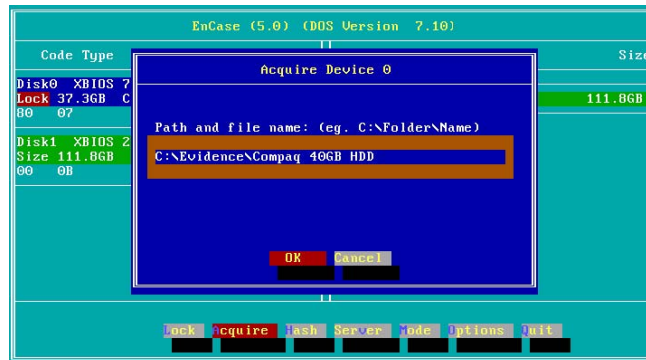


Figure 9-2: Input path for evidence file



The file path specified must already exist on the Storage computer. If it does not, exit EnCase for DOS, create that path (MD for “make directory”) then go back into EnCase for DOS.

- EnCase prompts you for the case number to which the evidence belongs. Enter the case number (if one has been assigned) and press **[Enter]**



Figure 9-3: Input for case number

- Enter the name of the examiner or investigator who is conducting the investigation and press **[Enter]**.

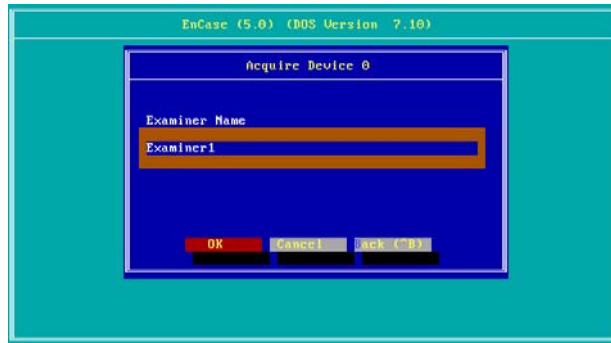


Figure 9-4: Input for examiner name

- Enter a numeric code to identify the specific evidence and press [**Enter**].



Figure 9-5: Input for evidence number

- Enter a short descriptive name such as **Laptop1**. This name will be used to describe the device in the Windows version of EnCase. When you have entered the name, press [**Enter**]

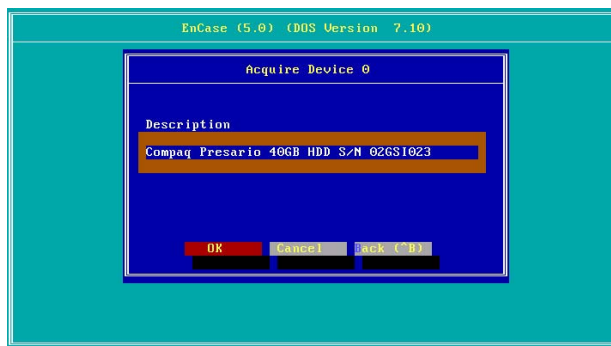


Figure 9-6: Input for unique description

- If the date and time displayed are correct, press **[Enter]**. If not, type in the correct date and time and press **[Enter]**.

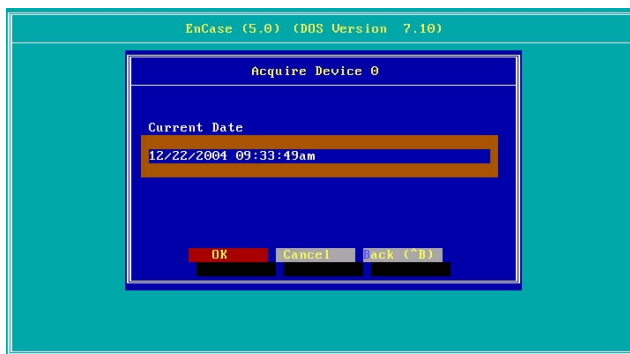


Figure 9-7: Date of acquisition computer



Entering the correct time and date **DOES NOT** change the system time; it simply notes in the acquisition information what the *Reported Time* and *Actual Time* were.

- Enter any notes or relevant information given to this piece of evidence (such as its location or condition), and then press **[Enter]**.



Figure 9-8: Input for notes

- Select **[Yes]** to compress the evidence file. The resulting files, in turn, will generally be two to three times smaller than if acquired with no compression. Using compression may take up to five times longer to create the file.



Figure 9-9: Select [Yes] to compress

- Choose whether or not to create an MD5 hash value. Choose [**Yes**] to generate an MD5 hash of the evidence at the time of acquisition (recommended).



Figure 9-10: Select [Yes] to obtain MD5 hash

- To add a password to an evidence file, type in the password and click [**OK**]. If the password is lost or forgotten, the evidence file is inaccessible.
- Enter the maximum size of the resulting file segments (chunks). The default is 640MB for CD-R archival, but this may be increased up to 2000MB or as small as 1MB.



Figure 9-11: Input for password

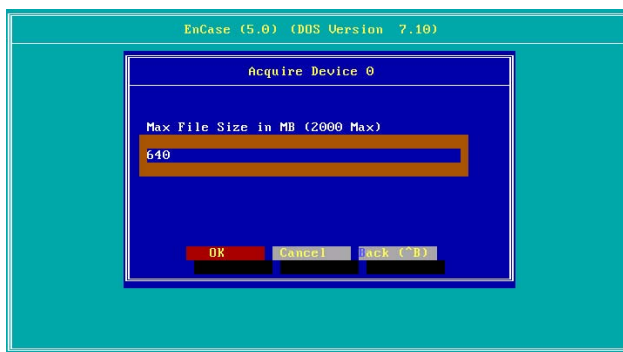


Figure 9-12: Input for evidence file segment size



Guidance Software recommends archiving with 640MB “chunk” file sizes. Even if archiving to DVD-R, seven 640MB “chunks” fit comfortably onto a DVD-R.

- EnCase allows the investigator to specify the number of sectors to acquire. While most of the time the default is correct, the exception is when dealing with a SafeBackclone of a drive. For example, SafeBack clones a 7GB drive to a 10GB drive. The extra 3GB are completely unnecessary to acquire. Simply type in the number of sectors that SafeBack reported cloning.

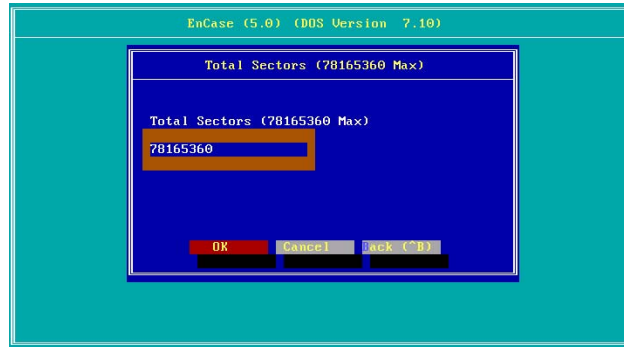


Figure 9-13: Specifying sectors for SafeBack-cloned drives

- The user is prompted to specify the granularity of the acquisition. This value specifies how many blocks to zero out if a read error is encountered while acquiring that block. The granularity can be changed from the default of 64, incrementally down to 1. The acquisition speed will increase as the granularity is set to a coarser setting (more sectors zeroed out per block). The settings and subsequent number of sectors zeroed out are described in the table below:

Granularity setting	64	32	16	8	4	2	1
Sectors zeroed per block	64	32	16	8	4	4	1

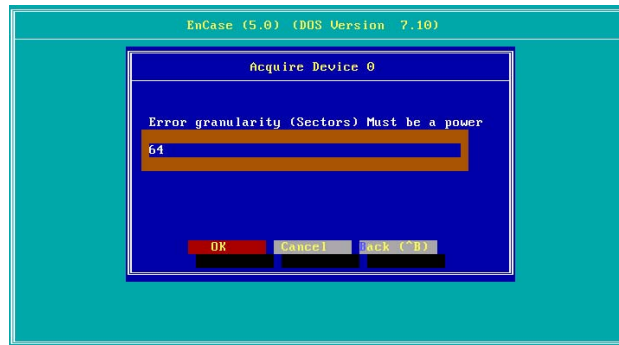


Figure 9-14: Granularity

- EnCase will now begin the disk acquisition process. This can take several hours, so ensure that the computer has a stable position and power supply. The time elapsed and estimated time remaining is displayed

```
EnCase (5.0) (DOS Version 7.10)

Input
-----
Drive           A
CaseNumber      001
Examiner        Examiner1
EvidenceNumber  001001
Alias           Compaq Presario 406B HDD SN0248GSI0121
Notes          For Jones counterfeit case
OutputPath      C:\evidence
Compression     N
ZeroPadding     1
Granularity     1

Acquiring Compaq Presario 406B HDD SN0248GSI0121, 0:00:00 elapsed
```

Figure 9-15: Acquisition

If the evidence drive fills up, EnCase for DOS will prompt you to switch to another storage location. Be sure to note the label or name of the media where the first section of evidence chunks are stored.

The file extension .E01 is always assigned to the first chunk of an evidence file set. Thereafter, the number in the extension is increased sequentially. An evidence set entitled “hard disk,” gets a name of `harddisk.E01` for the first output file, `harddisk.E02` to the next chunk, and so on.

Acquiring Macintosh Devices

EnCase can acquire and interpret the Macintosh and Power Mac file systems (HFS and HFS+). Acquiring a Macintosh hard drive is similar to acquiring a PC’s in a drive-to-drive acquisition. Macintosh computers cannot be booted with an EnCase boot disk. The hard drive must be removed and acquired onto a PC that can be booted with an ENBD or LinEn boot disk. If the media are an IDE hard drive, put it on the IDE ribbon cable. If the medium is a SCSI hard drive, attach it to the SCSI controller card in the storage computer and subsequently acquire it through DOS.

If the Macintosh HD is an IDE hard drive and a FastBloc unit is available, acquisition of the Macintosh hard drive is possible that way as well. See *FastBloc Acquisitions* for details.

Acquiring Unix and Linux

EnCase can acquire and interpret the EXT2/3, Reiser, FFS, JFS1, JFS2 and UFS file systems. To acquire a Unix, Linux, or BSD hard drive, handle it much like you would a PC hard drive. The caveat with Unix and BSD is the same as for Macintosh. Macintosh computers cannot be booted with an EnCase boot disk. The hard drive must be removed and acquired onto a PC that can be booted with an ENBD or LinEn boot

disk. If it is an IDE hard drive, put it on the IDE ribbon cable. If the subject media is SCSI, attach it to the SCSI controller card. Acquire through DOS using EnCase boot disk.

With an IDE hard drive, a FastBloc unit can provide an alternate means of acquisition of the UFS hard drive. Please see the chapter in this document on *FastBloc Acquisitions* for details.

After the Acquisition Is Complete

After the acquisition is complete, boot the storage computer into Windows to analyze the just-created evidence file. Remember to remove any connections to the subject hard drive before booting to Windows.

If completing a drive-to-drive (same IDE ribbon cable) acquisition in the Storage computer, follow these steps:

- Power down the computer.
- Disconnect the subject hard drive from the ribbon cable and power cable.
- Replace the cover on the storage computer.
- Place the subject hard drive in a safe, static-free location for safety.
- Remove the boot floppy from the floppy drive.
- Boot the storage computer and launch EnCase for Windows.
- If you performed an acquisition of another type, disconnect the cable connecting the subject media to the storage computer.

FASTBLOC ACQUISITIONS

Computer investigations require a fast, reliable means to acquire digital evidence. FastBloc Lab Edition (LE) and FastBloc Field Edition (FE) (hereafter referred to as FastBloc) are hardware write-blocking devices that enable the safe acquisition of subject media in Windows to an EnCase evidence file. Before FastBloc was developed, noninvasive acquisitions were exclusively conducted in cumbersome command-line environments.

The hardware versions of FastBloc are not stand-alone products. When attached to a computer and a subject hard drive, it provides investigators with the ability to quickly and safely preview or acquire data in a Windows environment. The unit is lightweight, self-contained, and portable for easy field acquisitions, with on-site verification immediately following the acquisition.

FastBloc SE is a software version of this product. More information on this product is available in the **V5.05 Modules Manual**.

FastBloc Acquisition Process



Figure 10-1: FastBloc LE



Figure 10-2: FastBloc FE



Figure 10-3: FastBloc 2 FE



Figure 10-4: FastBloc 2 LE

- Attach Subject IDE hard drive to FastBloc unit.
- Make sure IDE connection from FastBloc to the storage computer is snug.
- Power FastBloc on.
- Power the storage computer on.
- Launch EnCase for Windows on the storage machine.
- Click the [**Add device**] button.
- Blue-check **Local Devices** in **Add Devices** and click [**Next >**].

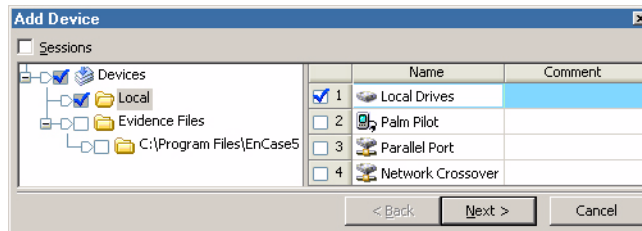


Figure 10-5: Adding write-blocked device

- Choose a physical drive protected by FastBloc (indicated by a blue border around the icon), and then click the [**Next >**] button.

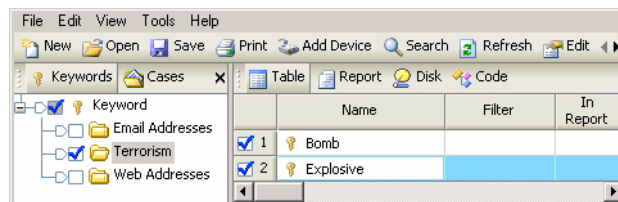


Figure 10-6: FastBloc-protected devices with blue border

- With the selected device showing in the **Preview Devices** window, click on the [**Finish**] button to confirm the selection. To edit device properties, such as the device name, device notes, etc., double-click the device name before clicking the [**Finish**] button.

Live Device and FastBloc Indicators

In EnCase, live devices (previews) are identified in Case view by a blue triangle overlay in the lower right of the icon. A blue square (without the triangle) is overlaid on volumes and devices write-blocked by FastBloc when previewed. Occasionally, improperly jumpered drives or cable issues may prevent the blue square overlay and the TRUE boolean Write Blocked value from appearing in EnCase, but since hardware write blocking is taking place, it is impossible for the device to be written to.

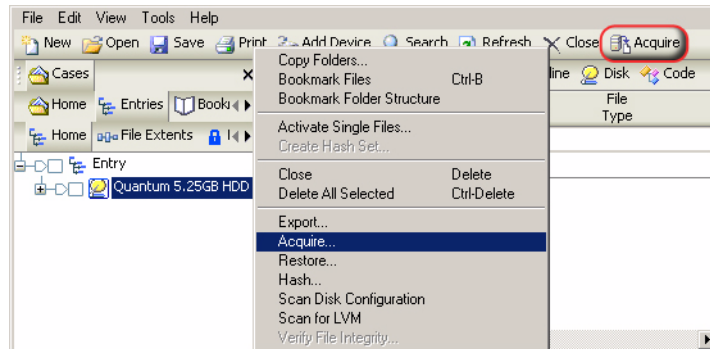


Figure 10-7: FastBloc-protected hard drive preview and acquisition

Acquiring via FastBloc provides access to the automated acquisition and analysis features such as verification, searching, hashing, and verification of the file signatures of very large hard drives overnight or a weekend at the time of acquisition. Prior to using these features, ensure you have added and selected the desired keywords in the **Keyword** view.

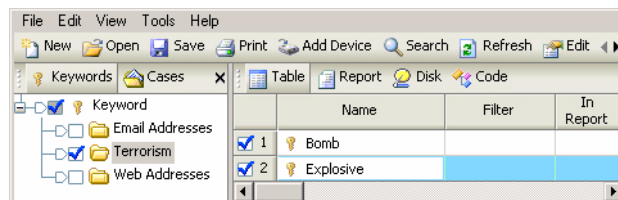


Figure 10-8: Creating keywords for acquisition options

Once the keywords have been created and selected, return to the Case view, right-click on the previewed device and select **Acquire...** Alternately, you can click on the [**Acquire**] button on the top tool bar.

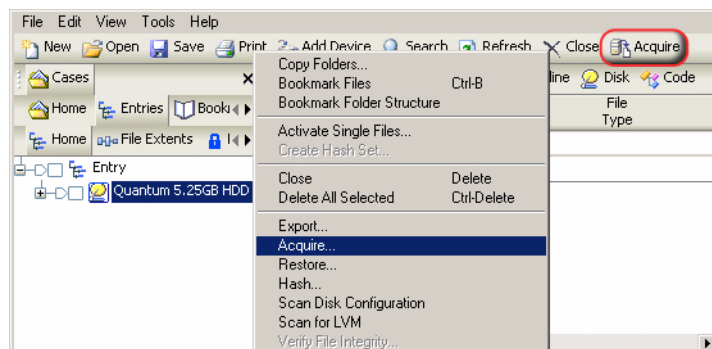


Figure 10-9: Acquiring a live write-blocked device

Several options are available in the **After Acquisition** screen that appears. Selecting **Acquire another disk** will allow the examiner to acquire several devices one after another, such as floppy disks or CDs. The examiner will not need to preview each new device before acquisition.

The examiner has three options for the evidence file once it is created.

- **Do not add** – this option will leave the evidence file in the saved location upon completion of the acquisition, but will not add it to the open Case. This is used for acquiring images to a central server or acquiring images that will not be examined immediately.
- **Add to Case** – this option will add the new evidence file to the case, but will not replace the live device (preview). This is used for adding acquired images to the case, but leaving the live access to the drive available to image other devices. It is important to note that if the case is saved with a live preview in it, when the case is reopened, it will look for the device to be physically attached.
- **Replace source device** – this option is used for hard drive acquisition or for acquiring a single piece of removable media. This option adds the new evidence file to the case, replacing the live preview. Any search hits, hashing, bookmarks, etc., of the live device during triage will be resolved to the newly added evidence file. This option is not available if you want to acquire another disk.

When acquiring a hard drive you should select **Replace source drive** to add the new evidence file to the case, replacing the live preview. EnCase now gives the examiner the option of searching, hashing, and running the file signature analysis

on the newly added evidence file. For these options, select **Search, Hash, and Signature Analysis**.

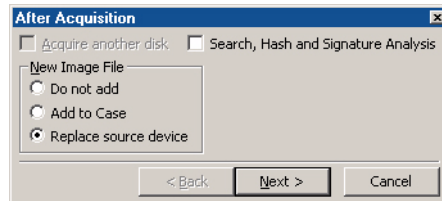


Figure 10-10: Post acquisition options

You will now have the **Search** options available. You should select the desired keyword(s) to search before starting the acquisition process, unless you wish to search all of the available keywords. If the desired keywords are not already selected in the **Keyword** view, select **Cancel**, go to the **Keyword** view, select or enter in the desired keywords, return to the **Case** view and start the acquisition process again. The **Search** window gives examiners the option of search and analyzing all of the devices in the case by selecting **Search entire case**. If the option is not selected, EnCase will only search and analyze the new evidence file after its creation.

The examiner has several analysis options available:

- **Search each file for keywords** – this option will search each file for the desired keywords, in the entire case or just new evidence file as selected by the examiner.
- **Verify files signatures** – this option will compare the file extensions and file header/signature of each file, in the entire case or just new evidence file as selected by the examiner.
- **Compute hash values** – this option will compute the hash value of the logical file area of each file and compare the value to the hash library, in the entire case or just new evidence file as selected by the examiner.
- **Recompute hash values** – this option will recompute all previously computed hash values generated for the files of the replaced live device. This is most often used for acquisitions over the enterprise network, to recompute the values of the files on the live machine if a hash analysis was conducted previously. This option is not necessary for local acquisitions.

There are four options for the searching if it is selected:

- **Search file slack** – this option will include searching the file slack (area between the logical and physical areas of the file) of each file, in the entire case or just new evidence file as selected by the examiner.
- **Undelete files before searching** – this option will logically “undelete” deleted files prior to searching. If a file is deleted, EnCase and other tools can determine if the assigned starting cluster is not assigned to another file (if it is assigned, then the file is Deleted/Overwritten). The unallocated clusters after the starting cluster may or may not belong to the deleted file. Choosing this option assumes the unallocated clusters after the starting cluster do belong to the deleted file. This is the same assumption made when copying out a deleted file. This option finds keyword fragmented between the starting cluster and the subsequent unallocated cluster. If determining the presence of a keyword on the media is critical to an investigation, the examiner should also search for portions of the keyword, including GREP expressions of fragments of the keyword.
- **Search only slack area of the files in the Hash Library** – this option will exclude the logical area of files for which their hash values matches that of a file in the Hash Library. The slack area of the physical file is still searched, in the entire case or just new evidence file as selected by the examiner.
- **Selected keywords only** – this option will have EnCase search only the keywords selected in the Keywords view rather than all available keywords, in the entire case or just new evidence file as selected by the examiner.

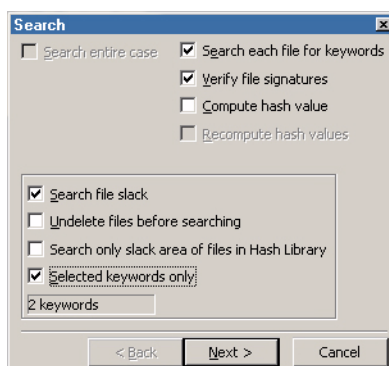


Figure 10-11: Search and analysis options

Choose [**Next >**] after selecting options. The last window will be the acquisition options. These are the standard options for the generation of an evidence file.

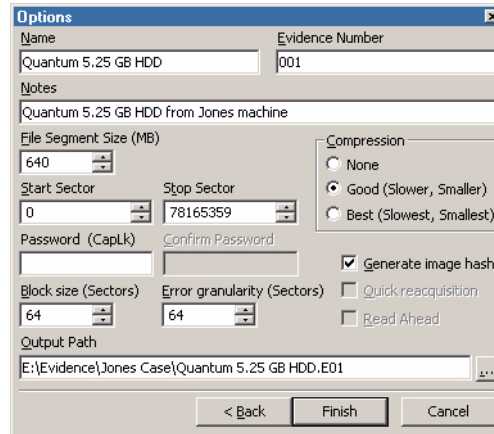


Figure 10-12: Evidence file options

After selecting [**Finish**] EnCase will begin the acquisition process. The progress bar indicates the status in the lower right hand corner.

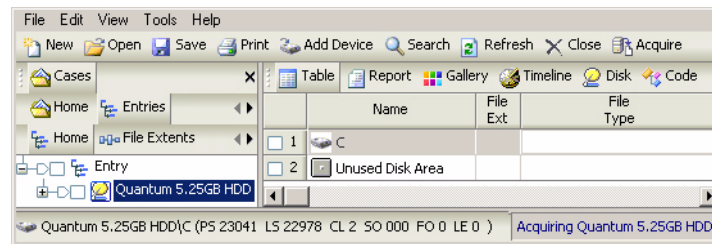


Figure 10-13: Acquisition status

When the acquisition is complete, EnCase will replace the live previewed device with the new evidence file and begin the verification of the evidence file.

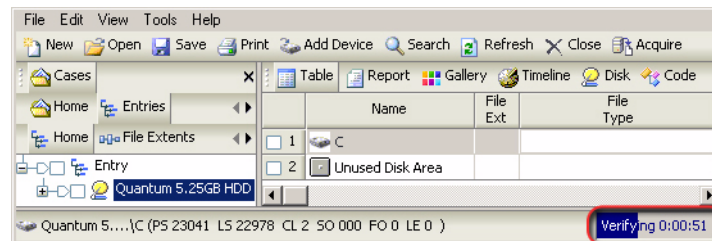


Figure 10-14: Verifying acquired evidence

When the verification is complete, EnCase will begin the searching and other analysis of the evidence file.



Figure 10-15: Searching after acquisition and verification

When all processes are complete, EnCase will present a dialogue box of the search results for when you return to the office. You have the option to write the results to the **Console** view and/or place in a bookmark note.

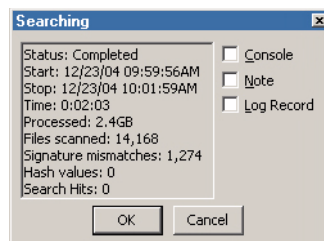


Figure 10-16: Search results

If a user wishes to re-acquire an evidence file, this can be done at a much faster rate than previously if the Quick Reacquisition check box is activated. With this option selected, the user can reacquire the file while changing the start or stop sector, password or the segment size and specify whether or not to generate an image hash. All other acquisition options, such as compression, block size, granularity, assigning name or evidence number are grayed out and unavailable.

If the acquisition is terminated by the user prior to completion, the user can start the acquisition again and check the **Restart Acquisition** box. The grayed out **Acquisition File Path** field will become active, allowing the user to input or browse to the path (including first evidence file segment name) where the acquisition was saving the evidence file, as shown below:

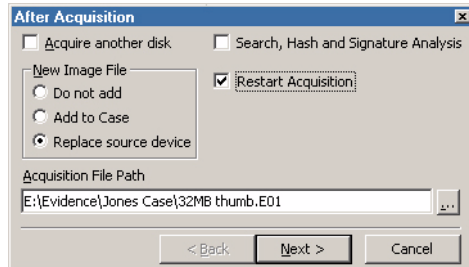


Figure 10-17: Restarting an acquisition

The **Options** window will appear again, although only the **File Segment Size** can be changed.

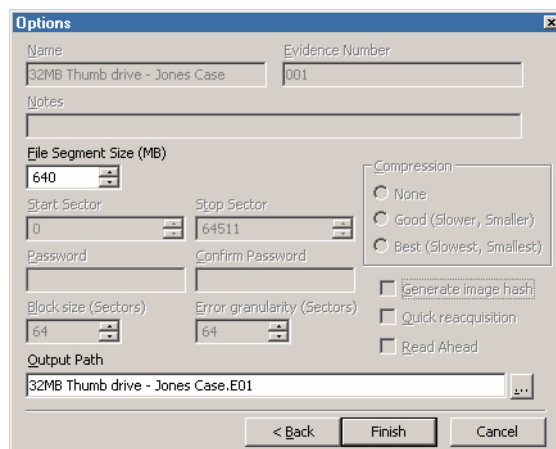


Figure 10-18: Acquisition restart options

Acquiring in Windows *Without* FastBloc

Never acquire hard drives in Windows without FastBloc because Windows writes to any local hard drive visible to it. Windows will, for example, put a Recycle Bin file on every hard drive that it detects and will also change Last Accessed date and time stamps for those drives.

Media that Windows *cannot* write to is safe to acquire from within Windows such as CD-ROMs, write-protected floppy diskettes, and write-protected USB thumb drives.

Acquiring in Windows *with* a non-FastBloc Write-Blocker

EnCase cannot recognize the presence of any hard drive write-blocker, other than FastBloc. For that reason, EnCase will report that the subject hard drive is NOT protected, when it very well could be. Users of non-FastBloc write-blockers are encouraged to test their equipment and become familiar with their capabilities.

After Acquisition Is Complete

Power down the computer, power down FastBloc, disconnect the subject media and store it in a safe location, and boot your computer back into Windows. Launch EnCase and prepare to analyze the evidence.

ACQUIRING DISK CONFIGURATIONS

Please see the *Forensic Terminology* appendix for definitions and detailed explanations of the types of Disk Configurations available. Guidance Software uses the term “disk configuration” instead of RAID. A software disk configuration is controlled by the operating system software whereas a controller card controls a hardware disk configuration. In a software disk configuration, the information pertinent to the layout of the partitions across the disks is located in the registry or at the end of the disk, depending on the operating system used to build the set; in a hardware disk configuration, it is stored in the BIOS of the controller card. With each of these methods, 6 disk configuration types can be created: spanned, mirrored, striped, RAID-5, RAID-10 and basic.

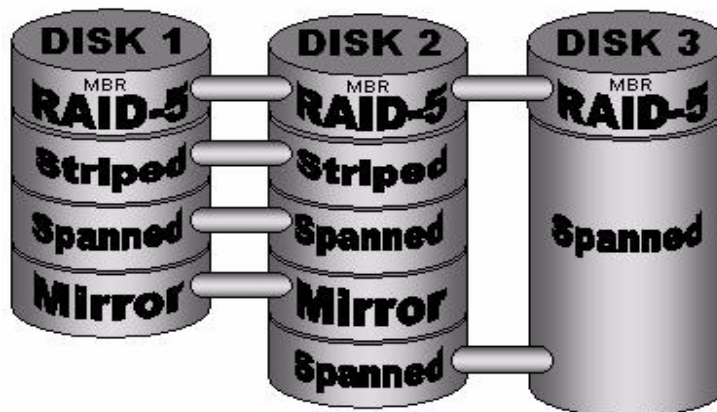


Figure 11-1: Possible setup for disk configuration

Software RAID

Windows NT: Software Disk Configurations

In a Windows NT file system it is possible to use the operating system to create different types of disk configurations across multiple drives. The disk configurations possible are spanned, mirrored, striped, RAID 5, and basic. The information detailing the types of partitions and the specific layout across multiple disks is contained in the registry of the operating system used to create the disk configuration. EnCase can read this registry information and resolve the configuration based on the key. EnCase can then virtually mount the software disk configuration within the EnCase case.

There are two ways to obtain the registry key.

- Acquire the drive with the operating system on it. It is likely that this drive will be part of the disk configuration set, but in the event it is not—such as the disk configuration being used for storage purposes only—acquire the OS drive and add it to the case along with the disk configuration set drives.
- On the Subject PC, go to the **Windows Disk Manager** and make a backup disk by selecting **Backup** from the **Partition** option. This will create a backup disk of the disk configuration information, placing the backup on a floppy disk. You can then copy the file into EnCase using the **Single Files** option, or acquire the floppy disk and add it to the case. The case must have the disk configuration set drives added to it as well. This situation would only work if working with a restored clone of a subject computer. It is also possible a registry backup disk may be found at the location.

Right-click on the evidence file that contains the key and select **Scan Disk Configuration**. At this point, EnCase will attempt to build the virtual devices using the information from the registry key.

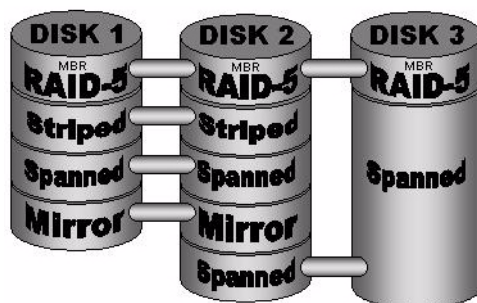


Figure 11-2: Rebuilding disk configuration with key



It is entirely possible that the investigator will not have access to the registry key to automatically rebuild the disk configuration set. In that event, the investigator will have to manually “edit” the devices, as described in the Hardware Disk Configuration section below.

Dynamic Disk

Dynamic Disk is a disk configuration available in Windows 2000, Windows XP and Windows 2003 Server. The information pertinent to building the configuration resides at the end of the disk rather than in a registry key. Therefore, each physical disk in this configuration contains the information necessary to reconstruct the original setup. EnCase reads the Dynamic Disk partition structure and resolves the configurations based on the information extracted.

To rebuild a Dynamic Disk configuration, add the physical devices involved in the set to the case and, from the Cases tab, right-click on any one of the devices and choose **Scan Disk Configuration**.

If the resulting disk configurations seem incorrect, they can be manually edited via the **Edit** command in the **Devices** tab.

Hardware Disk Configuration

Disk Configuration Set Acquired as One Drive

Unlike software disk configurations, those controlled by hardware contain the necessary configuration information in the card's BIOS. Since the disk configuration is controlled by hardware, EnCase cannot reconstruct the configurations from the physical disks. However, since the pertinent information to rebuild the set is contained within the controller, the computer (with the controller card) will actually see a hardware disk configuration as one (virtual) drive, regardless if the set is on two or more drives. If the investigator acquires the set in its native environment, the disk configuration can be acquired as one drive—by far the easiest option. The best method for performing such an acquisition would be to conduct a crossover network cable acquisition. (The EnCase Network Boot Disk for the Subject computer will have to have DOS drivers for that particular RAID controller card.) To acquire the set:

- Keep the disk configuration intact in its native environment.
- Boot the subject computer with an EnCase Network Boot Disk.
- Launch EnCase for DOS (remember, the BIOS interprets the disk configuration as one drive, so EnCase will too. The investigator will see the disk configuration as one drive).
- Acquire the disk configuration as you would normally acquire a single hard drive depending on the means of acquisition. Parallel port, crossover network cable, or “drive to drive,” acquisition of a hardware disk configuration set is straightforward, as long as the set is acquired as one drive.

If the physical drives were acquired separately, or could not be acquired in the native environment, EnCase has the ability to edit the hardware set manually (see below).

Disk Configurations Acquired as Separate Drives

Sometimes acquiring the hardware disk configuration as one drive is not possible, or the method of assembly of a software disk configuration seems incorrect. To edit a disk configuration, several items of information are required: the stripe-size, start sector and length per physical disk as well as if the striping is right handed or not. This data can be collected from the BIOS of the controller card, for a hardware set, or from the registry for software sets. To build the disk configuration:

- Add the evidence files to one case.
- Select **Devices** from the **View** menu.
- Right-click on any of the evidence file rows and select **Edit Disk Configuration...**

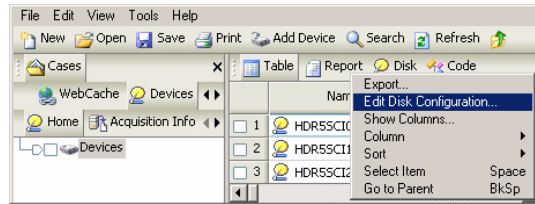


Figure 11-3: Edit Disk Configuration Command

- The **Disk Configuration** dialog box will appear. Right-click the **Component Devices** field on the right, and select **New**.

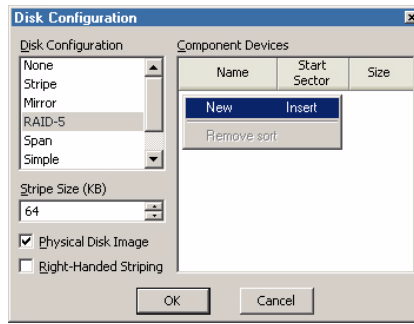


Figure 11-4: Disk Configuration settings

- For every component device involved in the set, right-click in the component devices window and select **New...** Assign the start sector and size that the disk configuration uses on each disk.

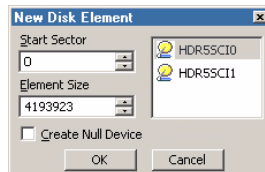


Figure 11-5: Adding devices manually

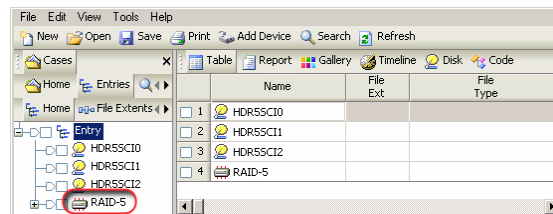


Figure 11-6: The rebuilt RAID

RAID-5 is composed of three or more disks. If one disk was missing or bad, EnCase can still rebuild the virtual disk using the parity information from the other disks in the configuration, which will be detected and done automatically during the reconstruction of hardware disk configurations using the **Scan Disk Configuration** command.

When rebuilding the RAID from the first two disks, the results of running **Validate parity** will be meaningless as you created the parity to build the missing disk.

Validating Parity on a RAID-5

The **Validate Parity** command checks the parity of the physical disks used to assemble the RAID-5. Thus, if the RAID-5 was rebuilt with a missing disk, this feature will not work. To check the parity from the Cases tab, right-click on the RAID 5 volume icon, and choose **Validate Parity** from the contextual menu. The process will run in the lower right hand corner of the screen as a background thread.

RAID-10

RAID-10 arrays require at least 4 drives, implemented as a striped array of RAID-1 arrays. This type of RAID is also supported by EnCase Version 5.

SCSI Drives and DOS

Most hardware disk configurations are SCSI. Whether acquiring the set's drives individually or as one drive, you will probably have to acquire these SCSI drives in DOS.

If you were to attempt a DOS acquisition of a SCSI drive *without* loading any device drivers, the acquisition might work. However, the computer's BIOS would not be seeing the SCSI drive accurately. To see the SCSI drive correctly, load DOS SCSI drivers when booting the computer. The EnCase Network Boot Disk has an auto-detection and auto-loading of drivers for SCSI cards (see the chapter on *Creating the EnCase Boot Disk* for the list of SCSI cards supported.)

ACQUIRING PALM PDAs

EnCase has the ability to preview and acquire some Palm PDAs. To successfully do so, you must disable any and all HotSync software from the Examiner machine.

Palms Supported

- IIIx, IIIxe
- V series
- VII series
- M series

Directions



Before connecting a USB Palm, make sure the Palm drivers are installed first.

- Put the Palm PDA (Pilot or Handspring) in its cradle.
- Attach the cradle cable to an available USB or serial port on the computer.
- Boot the computer into Windows.
- Launch EnCase and open a new case.
- Turn the PDA on.
- Put the PDA in Console mode as follows:
 - Using the stylus, write a lower-case cursive L on the left side of the “graffiti” area, as shown in Figure 12-2.
 - Place a double-dot on the left side of the “graffiti” area.

- Write a number two (2) on the right-side of the “graffiti” area



Figure 12-1: Palm “graffiti” area

l. .2

Figure 12-2: Input for Console mode



The Palm is in Console mode when a slightly longer beep than normal is heard. If you are acquiring a USB Palm device, the device should appear in the Windows Device Manager once it's in console mode. To get out of Console mode, you must reset the Palm as described in this chapter.

- Click the [**Add Device**] button in EnCase.
- Select **Local** and **Palm Pilot**, and then click [**Next >**].

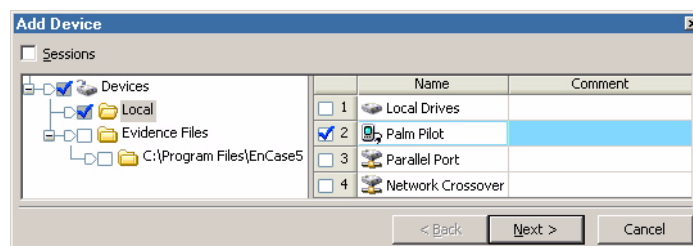


Figure 12-3: Previewing a Palm

- You will see all serial devices attached to the computer. Blue-check the Palm attached to COM2 (the serial port) and click [**Next >**].

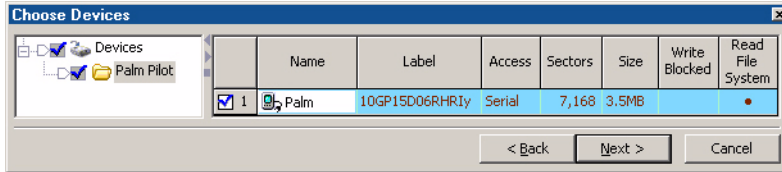


Figure 12-4: : Selecting the Palm as device

- Blue check the Palm to select it, and then click [**Finish**] to preview.

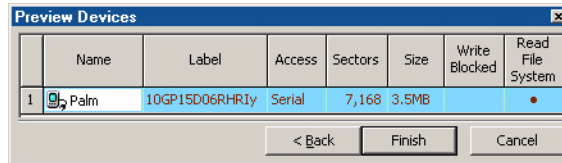


Figure 12-5: Selecting the Palm as device

You may double-click on the Palm if you wish to change the name or evidence number, add notes or uncheck **Read File System**. Click on the [**OK**] button to save changes.

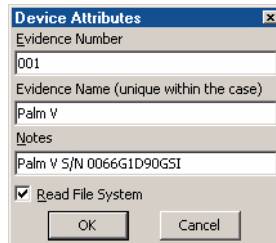


Figure 12-6: Editing device properties

The Palm should now appear as a device under the Cases tab.

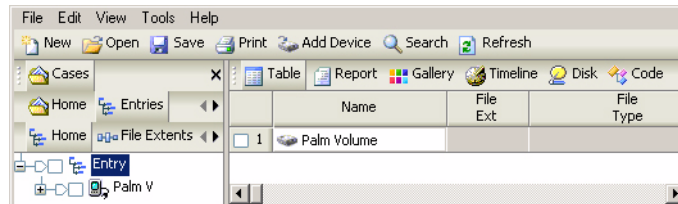


Figure 12-7: A previewed Palm

- Right-click on the Palm icon under the **Cases** tab and select **Acquire...**, or click on the [**Acquire**] button on the top toolbar. Several options are available in the **After Acquisition** screen that appears. **Acquire another disk** is grayed out since you will not be able to acquire subsequent Palms without previewing them first.

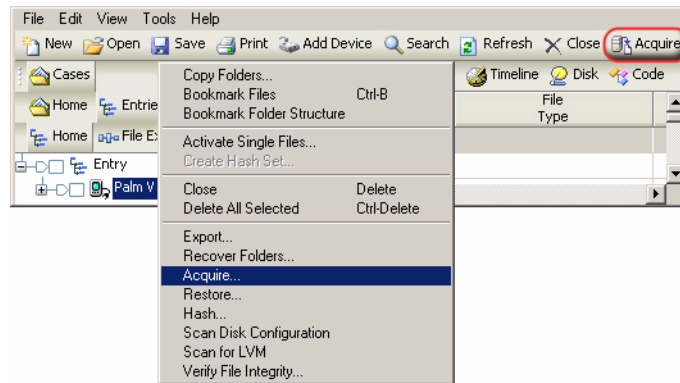


Figure 12-8: Acquiring a previewed Palm

- The examiner has three options under New Image File for the evidence file once it is created:
 - **Do not add** – this option will leave the evidence file in the saved location upon completion of the acquisition, but will not add it to the open case. This is used for acquiring images to a central server or acquiring images that will not be examined immediately.
 - **Add to Case** – this option will add the new evidence file to the case, but will not replace the live device (preview). This is used for adding acquired images to the case, but leaving the live access to the drive available to image other devices. It is important to note that if the case is saved with a live preview in it, when the case is reopened, it will look for the device to be physically attached.
 - **Replace source device** – this option is used for hard drive acquisition or for acquiring a single piece of removable media. This option adds the new evidence file to the case, replacing the live preview. Any search hits, hashing, bookmarks, etc, of the live device during triage will be resolved to the newly added evidence file. This option is not available if you want to acquire another disk.

When acquiring a Palm, it is best to select **Replace source drive**.

- EnCase gives the examiner the option of searching, hashing, and running the file signature analysis on the newly added evidence file. For these options, select **Search, Hash, and Signature Analysis**.

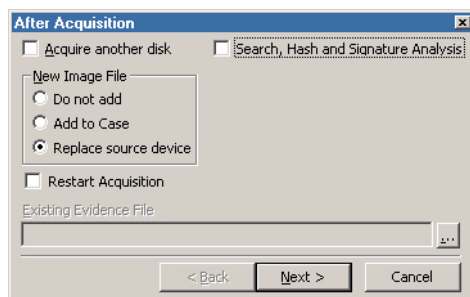


Figure 12-9: Post acquisition options

- You will now have the Search options available. You should select the desired keyword(s) to search before starting the acquisition process, unless you wish to search all of the available keywords. If the desired keywords are not already selected in the **Keyword** view, select **Cancel**, go to the **Keyword** view, select or enter in the desired keywords, return to the **Case** view and start the acquisition process again. The **Search** window gives examiners the option of search and analyzing all of the devices in the case by selecting **Search entire case**. If the option is not selected, EnCase will only search and analyze the new evidence file after its creation. The examiner has several analysis options available:
 - **Search each file for keywords** – this option will search each file for the desired keywords, in the entire case or just new evidence file as selected by the examiner.
 - **Verify files signatures** – this option will compare the file extensions and file header/signature of each file, in the entire case or just new evidence file as selected by the examiner.
 - **Compute hash values** – this option will compute the hash value of the logical file area of each file and compare the value to the hash library, in the entire case or just new evidence file as selected by the examiner.
 - **Recompute hash values** – this option will recompute all previously computed hash values generated for the files of the replaced live device. This is most often used for acquisitions over the enterprise network, to recompute the values of the files on the live machine if a hash analysis was conducted previously. This option is not necessary for local acquisitions.

There are four options for the searching if it is selected:

- **Search file slack** – this option will include searching the file slack (area between the logical and physical areas of the file) of each file, in the entire case or just new evidence file as selected by the examiner.
- **Undelete files before searching** – this option will logically “undelete” deleted files prior to searching. If a file is deleted, EnCase and other tools can determine if the assigned starting cluster is not assigned to another file (if it is assigned, then the file is Deleted/Overwritten). The unallocated clusters after the starting cluster may or may not belong to the deleted file. Choosing this option assumes the unallocated clusters after the starting cluster do belong to the deleted file. This is the same assumption made when copying out a deleted file. This option finds keyword fragmented between the starting cluster and the subsequent unallocated cluster. If determining the presence of a keyword on the media is critical to an investigation, the examiner should also search for portions of the keyword, including GREP expressions of fragments of the keyword.
- **Search only slack area of the files in the Hash Library** – this option will exclude the logical area of files for which their hash values matches that of a file in the Hash Library. The slack area of the physical file is still searched, in the entire case or just new evidence file as selected by the examiner.
- **Selected keywords only** – this option will have EnCase search only the keywords selected in the **Keywords** view rather than all available keywords, in the entire case or just new evidence file as selected by the examiner.

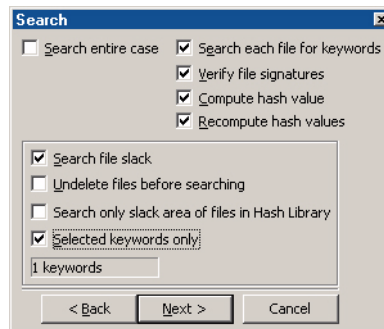


Figure 12-10: Search and analysis options

- Choose [**Next >**] after selecting options. The last window will provide acquisition options for the generation of an evidence file.

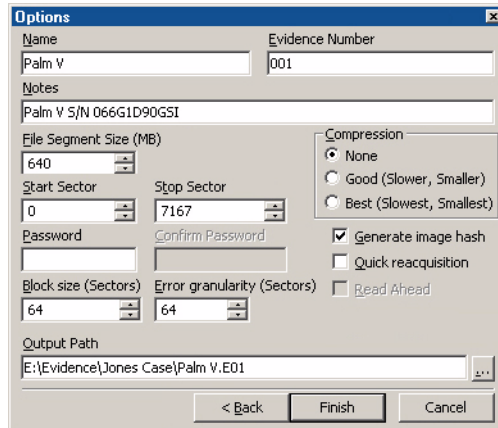


Figure 12-11: Evidence file options

- After selecting [**Finish**] EnCase will begin the acquisition process. The progress bar indicates the status in the lower right hand corner. The acquisition may occur quickly since it is acquiring directly from RAM.

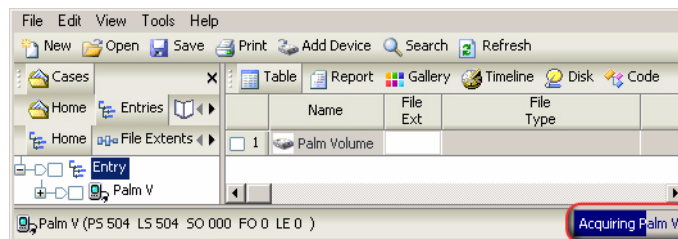


Figure 12-12: Acquisition status

- When the acquisition is done, EnCase replaces the live previewed device with the new evidence file and begin the verification of the evidence file.

- When the verification is complete, EnCase will begin the searching and other analysis of the evidence file.

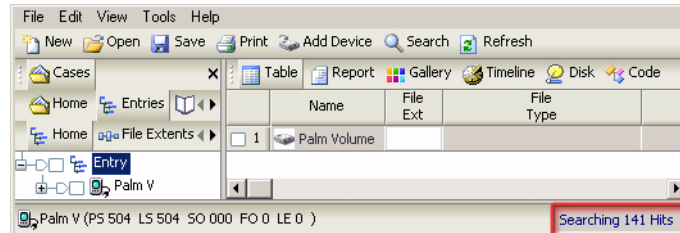


Figure 12-13: Searching after acquisition and verification

- When all processes are complete, EnCase will present a dialogue box of the search results for when you return to the office. You have the option to write the results to the Console view and/or place in a bookmark note.

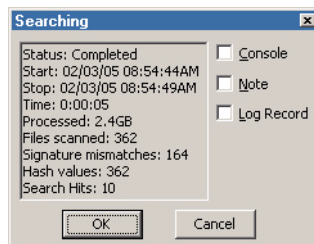


Figure 12-14: Search results

If a user wishes to re-acquire an evidence file, this can be done at a much faster rate than previously if the Quick Reacquisition check box is activated. With this option selected, the user can reacquire the file while changing the start or stop sector, password or the segment size and specify whether or not to generate an image hash. All other acquisition options, such as compression, block size, granularity, assigning name or evidence number are grayed out and unavailable.

Getting Out of Console Mode

To get a Palm out of “console mode,” you must do a soft reset on the Palm. Turning the Palm off and back on again does not take it out of console mode, and leaving it in console mode will cause the battery to drain faster than usual.

- Locate the small hole on the back of the Palm labeled “**RESET.**”
- Press the tip of a pen into the hole.

One Final Note on Palms

Initially previewing a serial Palm PDA may be slow because standard serial ports transfer data at a max of 115kbps. The preview and acquisition of a Palm Vx, for example, takes between 30 and 40 minutes. USB Palms will be faster; in acquisition tests, a 12MB m500 took four minutes to preview and 16 minutes to acquire. However, after the first keyword search on a previewed device, all other processes accessing the evidence file will be fast, as the entire evidence file has been cached in memory.

ACQUIRING REMOVABLE MEDIA

Zip and Jaz disks, flash media, and floppy disks are among the many other forms of media besides hard drives that the forensic investigator must be able to acquire. EnCase supports the acquisition of many forms of removable media.

Zip / Jaz Disks

Since the physical hardware on a Zip or Jaz drive does not allow for hardware write blocking, they should be acquired in DOS. Be sure you are running the latest version of EnCase on the forensic machine (downloadable by navigating to **Support and Downloads** at <http://www.guidancesoftware.com>). Perform the acquisition as follows:

- Download the EnCase Barebones Boot Floppy Image from <http://www.guidancesoftware.com> then **Support and Downloads** and save the file to C:\Program Files\EnCase5.
- Open EnCase and from the **Tools** menu, select **Create Boot Disk...**
- With a blank floppy in the drive, leave **A** selected as **Target Drive** and click on the [**Next >**] button.
- Select **Overwrite diskette with a boot floppy base image**, then click on the ellipsis box next to **Image Path** to set the path to C:\Program Files\EnCase5\bootfloppy.e01, if not set by default.
- At the **Copy Files** window, right click in the window and select **New**.
- Select C:\Program Files\EnCase5\EN.EXE and click [**Open**], then click [**Finish**].

- Click [**OK**] to close the boot disk creation session.
- Click on the [**Next >**] button.
- Create a temporary directory (such as C:\IOMEGA\TEMP), download the executable to create GUEST.EXE from Iomega's web site (<ftp://download.iomega.com/english/iodrv-dos-x86-10.exe>), saving it to the newly created folder.
- Go to the temporary folder and double-click on IODRV-DOS-X86-10.EXE to extract the files.
- Copy all the expanded files in that directory (except IODRV-DOS-X86-10.EXE and AUTORUN.EXE) to the floppy (A:).
- Shut down the forensic or suspect machine with a storage drive and Zip drive, removing the cables to all drives, including the Zip or Jaz drive.
- Boot the machine ensuring that the BIOS is configured to boot from floppy only.
- Shut the machine down, connect the cables to the storage drive and Zip or Jaz drive, and put the boot floppy in the diskette drive.
- Boot the machine.
- At the A:\> prompt, type GUEST.EXE.
- Run EnCase by typing EN.EXE, adding the /B switch if you get "divide by" errors.

The Zip or Jaz drive may be viewed as both a physical disk and a logical volume. Acquire in DOS as you would normally acquire a hard drive.

Floppy Disks

Floppy disks can be acquired safely in either DOS or Windows. Write-protect the disk and insert it into the floppy drive. Launch EnCase and acquire the floppy.

Write-Protecting a Floppy Disk

Floppy disks have a sliding tab that allows a disk to be write-protected, preventing any writes from taking place on the diskette. A write-protected (“locked”) floppy disk has a hole in the upper-right corner.

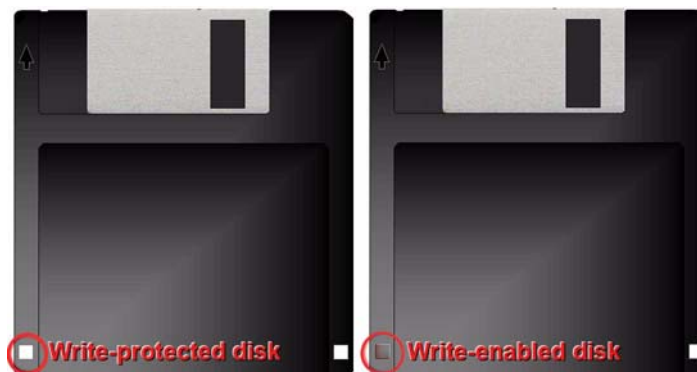


Figure 13-1: Write protecting a floppy disk

Superdisks (LS-120)

To acquire an Imation Superdisk, the investigator needs a drive that can load and recognize them. Superdisks have a physical write-protect tab on them, much like floppies do, and can be acquired in Windows in the same manner as a floppy disk.

CD-ROM, CD-R, CD-RW

CD-ROM, CD-R, and CD-RW disks can be acquired safely in Windows by EnCase. Place the CD into the drive and attempt to acquire with EnCase.

There are several issues that should be reviewed when a CD cannot be acquired. If the CD is formatted using UDF, this may cause CD-burning applications to take hold of the CD and prevent EnCase from recognizing it. To remedy this, you may need to disable or uninstall the CD burning application. For example, Roxio Easy CD Creator also loads an application (Direct CD) that launches at startup and runs in the background in Windows to recognize open session CDs.

Some types of CDs are viewable or recognized properly only if viewed using the correct hardware (e.g., CD reader, CD reader and writer, DVD-R, DVD+R, etc.) Other issues specific to CD-R, CD-RW, and CD-R/RW drives may contribute to EnCase being unable to acquire or even preview a CD-R or CD-RW; for a discussion on this issue, please review our message board.

If a CD cannot be acquired, wipe and format a small hard drive and copy the active files from the CD to this drive. Acquire the drive with EnCase. All file date and time stamps will have to be documented in other ways (such as looking at the CD-R in Windows and noting the file date/time stamps there).

Flash media

Flash media are memory storage cards for a portable devices such as PDAs, cell phones, and digital cameras. These are small matchbox-sized cards that can store data, music, applications etc. They are most commonly used in digital cameras to store images and transfer data from one portable device to another.

These cards come in different sizes and have different storage capacities. For example, Compact Flash cards can be found in digital cameras and pocket PCs and can store from 8MB of data up to 1GB. Common flash media devices are Compact Flash, Smart Media, and Memory Stick.

Equipment needed to preview/acquire flash media

Flash Card reader/writers are relatively inexpensive. Use a flash card reader to confirm that the process of examining this media is forensically sound. Most flash card readers connect via USB so ensure that a USB port is available. Ensure the flash card reader is compatible with the operating system running.

It is recommended using a 5-in-1 flash card reader that can read data from different size cards, such as Compact Flash, Smart Media, and Memory Sticks.

How to acquire flash media

- Place the flash card into the reading device and confirm all necessary device drivers are loaded.
- EnCase will recognize the flash card reader as a local device with a logical drive letter. It can be previewed or acquired as you would a local hard drive.
- If acquiring in Windows, EnCase cannot put a write-lock on the device. If either the memory card itself or the flash card reader has a write-lock facility, make sure this is set to the “lock” position.
- Most flash media use the FAT file system. Examining data on them is much like examining your average hard drive. It is possible to search both allocated and unallocated space.

Examining flash media

Images taken using a digital camera generally have unique image headers, specific to the camera manufacturer. The File Finder EnScript has a tab (**Custom File Type**)

that allows you to search for files with a specific header, footer and extension. Examine live image files in text view to determine the header and footer information, and run a search for them across unallocated space.

When examining images from digital cameras, Exif Reader can be used to analyze additional information that can be embedded within digital camera images and may show what make/model camera the image came from, time and date stamps, and other exposure/resolution/shutter speed information. The application can be downloaded at www.takenet.or.jp/~ryuuj/minisoft/exifread/english/.

Acquiring Multiple Pieces of Media

When acquiring multiple pieces of removable media, put a check box next to the **Acquire another disk** option in the **After Acquisition** screen.



Figure 13-2: Post acquisition options

The **Options** window will appear for the examiner to enter the case information and other evidence file options.

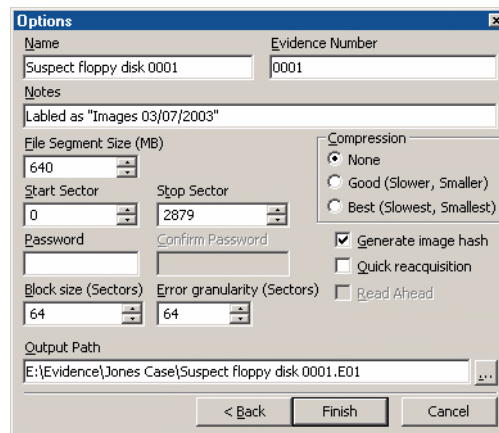


Figure 13-3: Acquisition Options window

At the conclusion of the acquisition, a dialogue box will appear with the option to save the results in a bookmark note, log record and/or write to the **Console**.

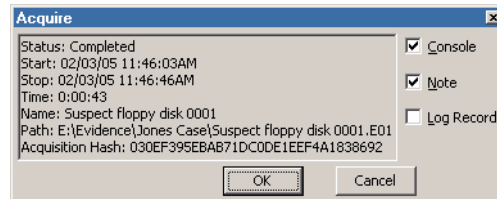


Figure 13-4: Acquisition status

If you wish to acquire another piece of media in the same drive, eject the current device and insert the next piece of media. Choose **[Next Disk]** to acquire the next piece of media, or **[Close]** to finish. If you choose **[Next Disk]**, EnCase will read the device without requiring you to preview using the **[Add Device]** function.

After the last piece of media is acquired, choose **[Close]**. In the Case view, right-click the live device with the blue triangle and choose **Close**, removing it from the case.

If a user wishes to re-acquire an evidence file, this can be done at a much faster rate than previously if the **Quick Reacquisition** check box is activated. With this option selected, the user can reacquire the file while changing the start or stop sector, password or the segment size and specify whether or not to generate an image hash. All other acquisition options, such as compression, block size, granularity, assigning name or evidence number are grayed out and unavailable.

FIRST STEPS

This chapter describes several features of EnCase that should be used at the start of any investigation. Whether responding to an incident, conducting an electronic discovery request, or auditing workstations, these steps are designed to save time and help ensure an accurate display of all data pertaining to the case.

Connecting to Remote Media

The enterprise functionality of EnCase allows the investigator to conduct forensically sound, remote previews over the Enterprise network without the Subject even being aware of the connection. For this reason, the security necessary to conduct such investigations is rigorous. The first step in initiating a remote preview or acquisition is to log onto a SAFE server, the machine that contains all administration rules and rights, and keeps logs of all transactions.



Figure 14-1: EnCase version 5 desktop icon

SAFE Administration and User Accounts

The keymaster must logon to the SAFE in order to create initial users or to create one user to perform the administration tasks associated with adding, editing, and deleting users and roles. Information on SAFE administration, user accounts, and roles is contained in the *EnCase Enterprise Administrator Manual*.

Logging Into a SAFE Server

Examiners log on using the account created for them by the keymaster. To log into a SAFE, [Logon] button on the top tool bar, or select **Logon...** from the **Tools** pull-down menu.

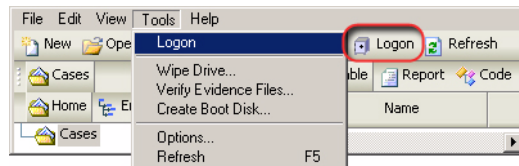


Figure 14-2: EnCase Examiner logon

At the **Logon** screen, select the name of the Examiner logging in. **Users** will appear based on their security keys residing in the **C:\Program Files\EnCase5\Keys** folder. Click on the username assigned by the account creator, typing in the **Password** (the pass phrase associated with the user's private key). When complete, click [Next >].

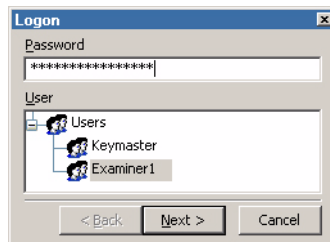


Figure 14-3: EnCase Examiner logon

Select the SAFE server to be connected (the name given to the SAFE upon initial installation) in the **SAFE** field. In the **Machine Name** field, type the IP address of the SAFE. When complete, click on [Finish].

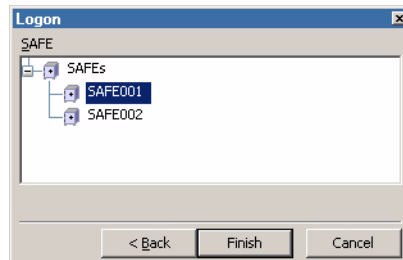


Figure 14-4: Selecting a SAFE

Upon a successful logon, a [**Logoff**] button (safe with a red minus sign) appears on the top tool bar beside the [**Logon**] button. You can logon to multiple SAFEs simultaneously using the [**Logon**] button again. The Tree Pane is populated by the SAFEs tab (which can also be accessed through the View pull-down menu). The table shows each SAFE attached to and the details about each (including the name of the user logged on).

Creating a New Case

Before connecting to a remote node, a new case must be opened. Click the [**New**] button on the tool bar, or select **New...** from the **File** pull-down menu. The Role window will open to allow the user to select a role. These roles are assigned by the keymaster to specific user accounts. Some have limited investigative functions and active time periods. Consult with the keymaster or delegate to determine the limits of the assigned roles.

Select the appropriate role and hit [**Next >**].

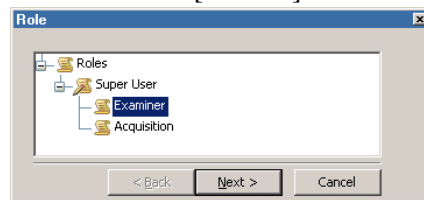


Figure 14-5: Selecting a Role

You are prompted to input information for the case options. These are described in the following chapter.

Connecting to Media

To preview computer media on the network via the Examiner, click the [**Add device**] button, or select **Add Device...** from the **File** pull-down menu.

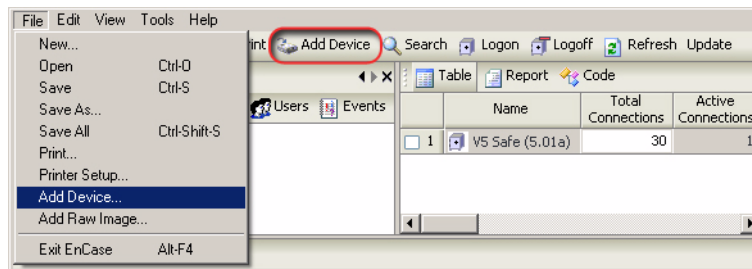


Figure 14-6: Adding a device to a new case

The user is prompted to select the type of media (the computer to preview or the preexisting evidence files) to add to the new Case. To find devices running the EnCase servlet on the enterprise network, click on the **Enterprise** folder and find the desired device in the table on the right. Blue check to select the desired machine(s) to preview, then click [**Next >**].

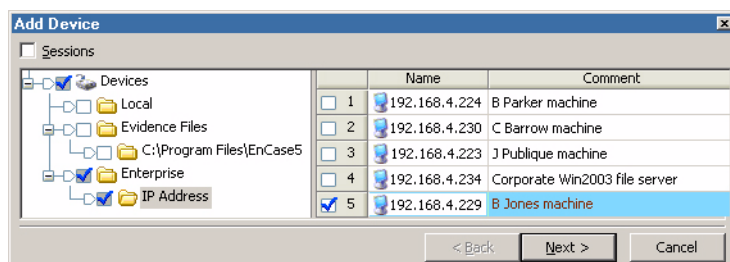


Figure 14-7: Selecting a machine

Select either the physical disk, logical volume or removable media (floppy disks can only be previewed on the local machine, not remotely). Blue check the desired media and click [**Next >**] to preview the device.

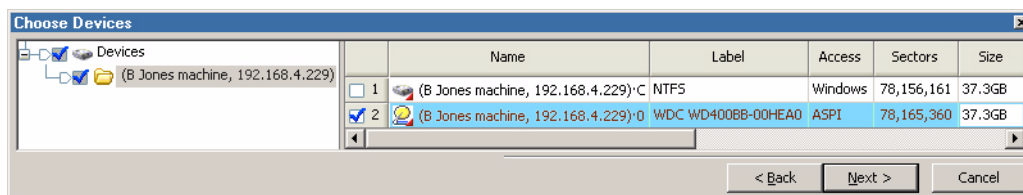


Figure 14-8: Selecting the appropriate media

Refer to the following chapter for instructions on how to change the device name, functionality of the available options, etc. Once the desired options have been selected, click [**Finish**] on the last screen to add the device(s) to the Case.

The hard drive of the machine is being previewed over a TCP/IP network. The red triangle in the bottom right corner of the device icon indicates that this is a live network connection. If the connection is lost, the icon will be covered with a pink square overlay; however, all of the information in the table (file names, dates, file sizes, etc.) will remain, and can be exported out as a report. You can also save your work as a Case file, reconnect to the machine, and resume the examination.

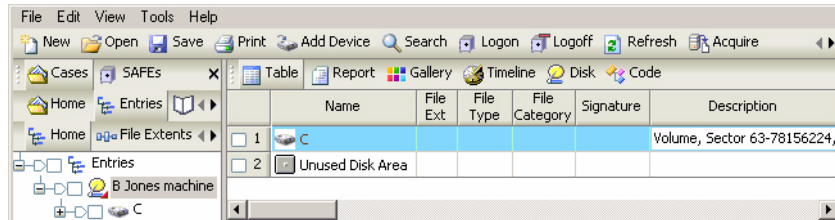


Figure 14-9: Previewed hard drive

Remote Acquisition

EnCase provides the automated acquisition and analysis features that allow the examiner to set EnCase to acquire, add, verify, search, hash, and verify the file signatures of large hard drives in a batch process, overnight or a weekend. For more detail on these functions, please refer to the following chapter. Before doing the acquisition, ensure that the desired keywords have been entered and selected in **Keyword** view. Detailed information regarding use of keywords can be found in the *Keyword Searches* chapter of this manual.

In Case view, select the previewed device to acquire. Right click on the device and select **Acquire...**, or click on the [**Acquire**] button on the top tool bar.

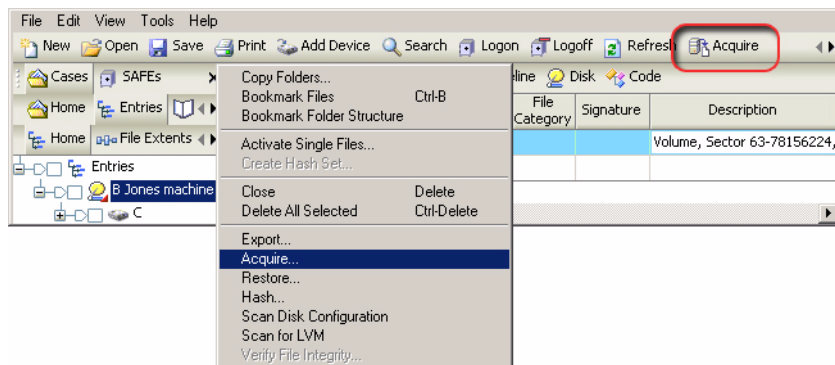


Figure 14-10: Acquiring previewed devices

Several options are available in the **After Acquisition** screen that appears. These are described in detail in the *FastBloc Acquisitions* chapter of this manual. After selecting [**Next>**], a screen with acquisition options appears. The **Read Ahead** option (checked by default), allows EnCase to cache blocks of data ahead of time so that they are available for commands in the process, decreasing acquisition time. The size

of the block is dependent on the value of the **Block size (Sectors)** option. There is a minimal risk of time-out, only present if unusually high block sizes are set.

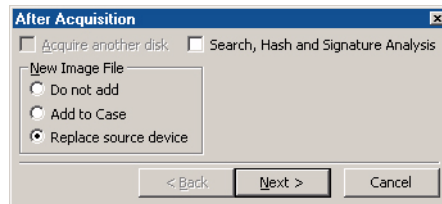


Figure 14-11: Acquisition options

After selecting [**Finish**] EnCase will begin the acquisition process. The progress bar indicates the status in the lower right hand corner.

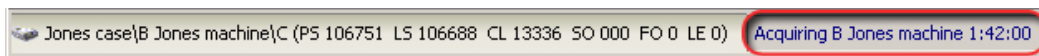


Figure 14-12: Acquisition status

When the acquisition is complete, EnCase replaces the live previewed device with the new evidence file and begin the verification of the evidence file if **Replace Source Device** is selected. Once verified, the selected post-acquisition processes are run. EnCase will present a dialogue box of the search results when this is complete, which can be written to the **Console**, a bookmark **Note** or a **Log Record**.

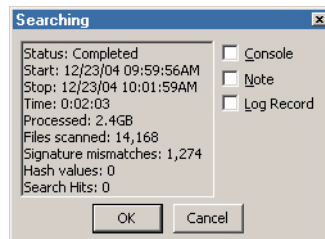


Figure 14-13: Post-acquisition results

Time Zone Settings

Often media in the same case originates from different time zones, which makes comparing the times of different events difficult. EnCase Version 5 allows, but does not require, the investigator to set the time-zone setting for each piece of media in the case independent of the system time zone, and independent of the other pieces of media in the case. The user can also view all dates relative to one consistent time zone, if desired.

When a new time zone is assigned, dates and times in GMT-based file systems such as NTFS will be adjusted accordingly. File systems, such as FAT16 and FAT32, which save dates and times in local time, will not display adjusted times when a new time zone is assigned. However, setting the time zone on a local-time system is important when dealing with case-level time settings; it lets EnCase know what time zone the system was originally in.

With regard to Daylight Saving Time, EnCase checks the date portion of an entry, determines if it falls within standard or daylight time (if applicable), and displays the adjusted time. To disregard seasonal settings, uncheck **Account for seasonal Daylight Saving Time adjustment** in the **Case Time Settings** dialog box. To modify a time zone setting for a piece of media, right-click on the media and select **Modify Time Zone Settings...** from the contextual menu.

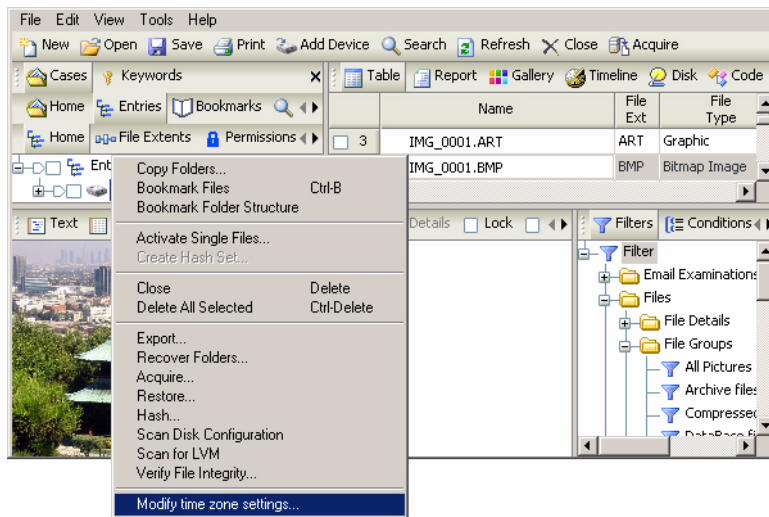


Figure 14-14: Time zone settings

Select the time zone for the piece of media. The default settings are read from the investigating computer's registry and displayed at right. If time zone settings are not specified, EnCase will default to deriving the date and time stamps from the current Windows registry settings on the investigating computer.

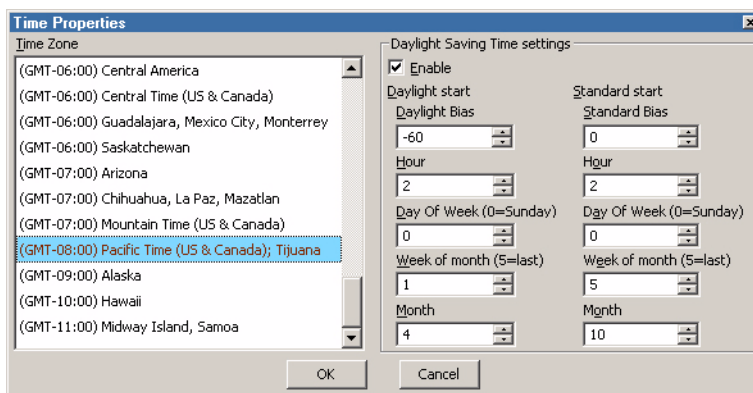


Figure 14-15: Time zone settings

EnCase also enables the user to show all dates in a case relative to the same time zone. For example, if the investigator is interested in comparing the times of activities that occurred across multiple machines, it may be advantageous to view them in one time zone. Activity which occurred at 5 pm Eastern time and 5 pm Pacific time did not occur at the same time relative to each other, so the investigator can choose to view the case in Pacific time; then, the time on Disk 1 (Pacific) will display as 5 pm, and the time on Disk 2 will display as 8 pm (5 pm Eastern).

To modify the case-level time zone settings, right-click on the **Case** folder under the **Home** subtab (below **Cases**) and select **Modify Time Settings...** from the contextual menu.

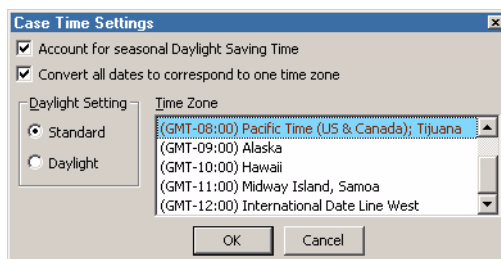


Figure 14-16: Choose desired time zone and daylight offset

By default, the checkbox to convert all dates to correspond to one time zone is not selected. To enable this feature, select the checkbox and the desired Time Zone to apply. Because this feature adjusts the times to a standard offset, you must choose whether to adjust for standard or daylight time as well.

Recover Folders on FAT Volumes

After adding an evidence file to a case, run **Recover Folders** on all FAT partitions by right clicking on each device and selecting **Recover Folders**. Folder recovery on NTFS and other partition types are covered in following sections. This command searches through the unallocated clusters of a specific FAT partition for the “dot, double-dot” signature of a deleted folder; when the signature matches, EnCase can rebuild the files and folders that were *within* that deleted folder.

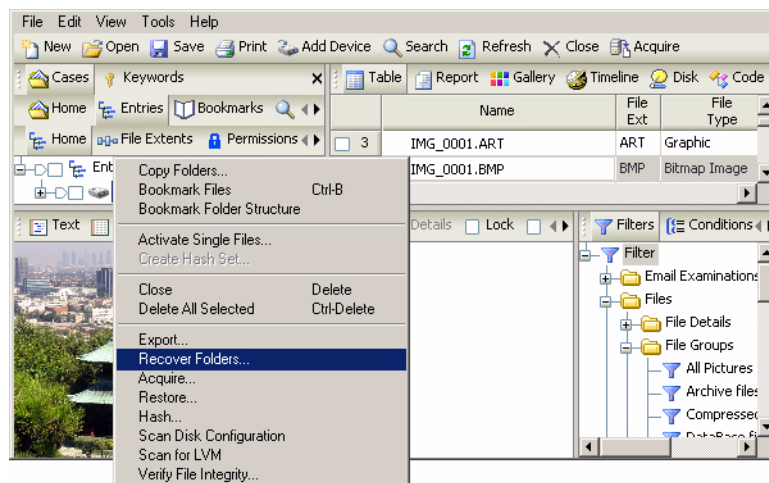


Figure 14-17: Recover folders

Behind the Scenes with Recover Folders

Typing **DIR** at a DOS command prompt will show two directories under every folder on that partition (including the root directory) - one folder with a dot (.) and another with a dot\double-dot (..). Every folder/directory in a FAT partition has dot\double-dot entries. These directories tell the file system where the directory entries for it and the parent reside. EnCase searches through the unallocated clusters for this signature and recovers folders that have been deleted with their directory entries overwritten in the parent directory. The contents of the directory, however, have not necessarily been overwritten. Though EnCase will not recover the names of these deleted folders (because the name was overwritten in the parent directory), it will attempt to recover everything that is within these folders (files and sub-folders), filenames included.

This is an important command to run, especially on formatted drives. This command can quickly and easily recover most of a formatted drive's information.

This command is available only when an evidence file *volume* is highlighted. Right-click on a volume under the **Entry** subtab under **Home** in the **Cases** tab and select **Recover Folders**. You will be prompted to scan the volume for lost folders; click [OK]. After the process executes, a gray **Recovered Folders** folder appears in the Case view. The folder will not appear until EnCase has searched the entire volume for deleted folders. If folders are recovered, you will be prompted to view the results.

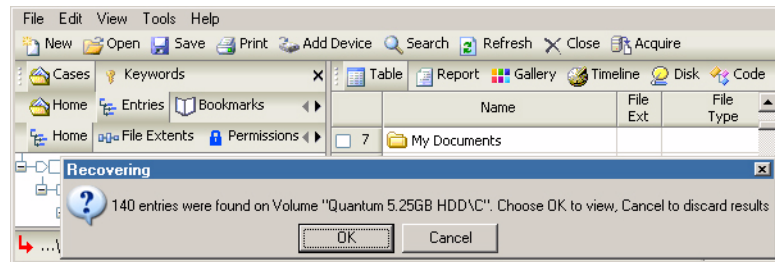


Figure 14-18: Recover Folders results



NOTE: Let Recover Folders finish before running any further analysis on the drive. Other EnCase functions, such as keyword searches, will prompt you to terminate the Recover Folders command. If you do so, you will lose any folders recovered to that point.

Recovering NTFS Folders

EnCase can recover NTFS files and folders from Unallocated Clusters and continue to parse through the current Master File Table (MFT) records for files without parent folders. This is particularly useful when a drive has been reformatted or the MFT is corrupted. Lost files that are recovered are placed in the gray **Recovered Folders** virtual folder in the root of the NTFS partition. To recover folders on an NTFS partition, right-click on the volume and select **Recover Folders**.

EnCase will open a window to confirm the user wishes to scan the volume for folders. Choose [OK] to begin the search for NTFS folders, or [Cancel] to cancel the request.

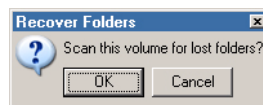


Figure 14-19: Begin scan for lost files

EnCase will begin searching for MFT records in the Unallocated Clusters. In the bottom right-hand corner a progress bar indicates the number of MFT records found and the approximate time required to complete the search.

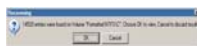


Figure 14-20: Progress bar for MFT record search

After EnCase locates the MFT records in the Unallocated Clusters, a prompt appears showing the number of entries found. Duplicate or false hits are parsed, so the number of entries that appears in the prompt may be lower than that reported during the recovery. If [OK] is pressed, EnCase will resolve the recovered MFT records to data on the volume, and attempt to rebuild the folder structure with children files and folders under parent folders. This process can take a long period of time, however, the results will greatly benefit examinations of NTFS volumes.

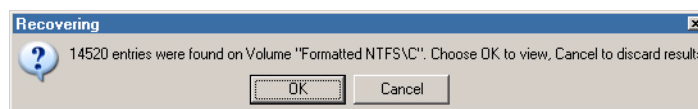


Figure 14-21: Viewing recovered MFT records

Since rebuilding the folder structure may take a long time, and users may opt to have faster access to the recovered files, if the recovered MFT entries in the unallocated space are NTFS4, the user will be given a choice to either have EnCase process the entries for parent/child relationships, or place all recovered entries into the Recovered Files folder immediately (with no folder structure). This dialog box includes the number of passes required to sort the entries. This number may be large; however, most passes will likely process instantly. The length of time required to process a given group depends only on the number of records within that group. This change does not affect NTFS5 recovered entries; these entries will be processed quickly as before. If the user chooses to process the entries for the folder structure, the progress bar will indicate which pass, of the total required, is currently running. The recovered folder structure is placed under the virtual Recovered Files folder.

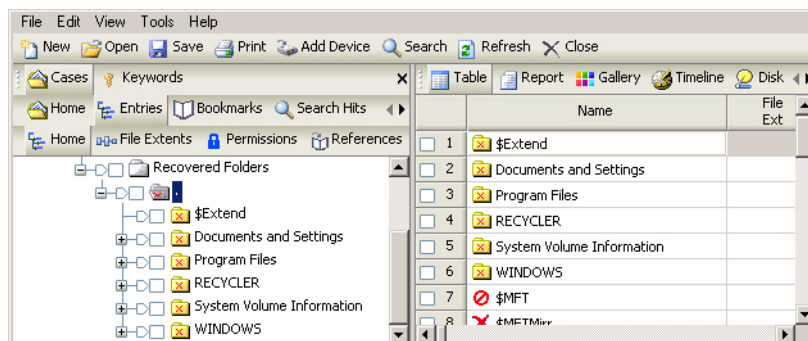


Figure 14-22: Recovered folder structure from a formatted NTFS drive

Lost Files in UFS and EXT2/3 Partitions

EnCase uses a different method for recovering deleted files and folders that have no parent in UFS and EXT2/3 partitions. When you preview a computer or add an evidence file that contains one of these partitions to EnCase, you will notice that a gray folder called **Lost Files** is automatically added to the tree in the **Entries** tab below each partition.

In the Master File Table (MFT) in NTFS, all files and folders are marked as a folder or file and as belonging to a parent. The files within a folder are that folder's children. If a user first deletes the files, then deletes the folder, and then creates a new folder, the originally deleted files can be lost. The new folder's entry in the MFT overwrites the deleted folder's entry. The original parent folder and its entry in the MFT are overwritten and gone. Its children, however, have not been overwritten and their entries are still in the MFT. As with NTFS, with UFS and EXT2/3 partitions, EnCase parses the MFT and finds those files that are still listed, but have no parent directory. All of these files are recovered and placed into the gray **Lost Files** folder.

Signature Analysis

File Signatures

There are thousands of file types, some of which have been standardized. The International Standards Organization (ISO) and the International Telecommunications Union, Telecommunication Standardization Sector (ITU-T) are working to standardize different types of electronic data. Typical graphic file formats such as JPEG (Joint Photographic Experts Group) have been standardized by both of these organizations. When file types are standardized, a signature—or

header—that programs can recognize usually precedes the data. File headers are associated with specific file extensions.

File extensions are the characters following the dot in a filename. They reveal the type of data that the file represents. For instance, if a filename contains a .TXT extension, it would be expected that the file type would be “**text**”. Many programs rely specifically on the extension to reflect the proper data type. Windows, for example, associates file types with their corresponding applications by use of file extensions.

One tactic to try to hide the true nature of a file is to rename the file and extension. A JPEG (image file) that has an incorrect extension such as “.dll” will not be recognized by most programs as a picture. It is therefore essential to compare each file’s signature with its extension to identify any files whose extensions have been deliberately changed. EnCase performs the Signature Analysis function in the background. Before running a signature analysis, familiarize yourself with how EnCase accesses and classifies file signatures. Select **File Signatures** from the **View** pull-down menu.

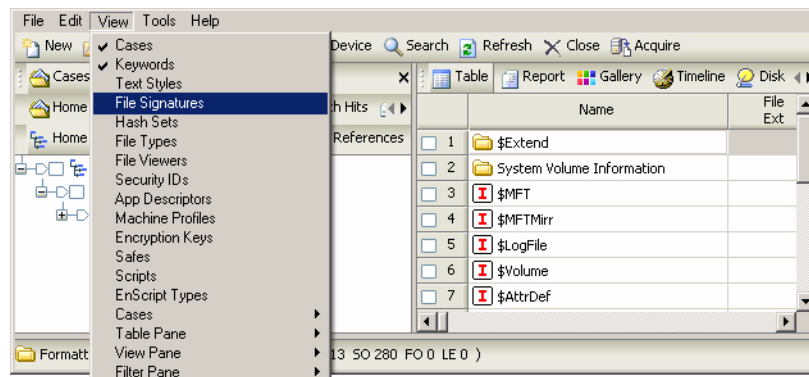


Figure 14-23: File Signatures option

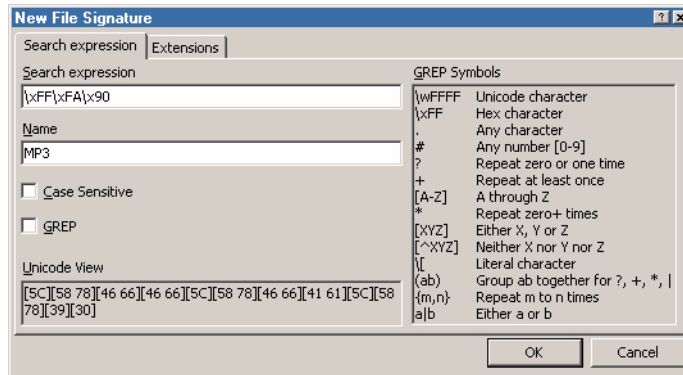


Figure 14-26: Adding an MP3 signature

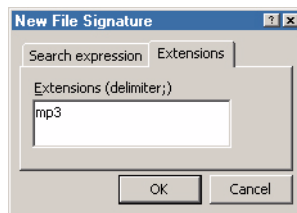


Figure 14-27: Adding an MP3 signature

Starting a Signature Analysis

To begin a Signature Analysis, click on the **Search** button on the top tool bar.

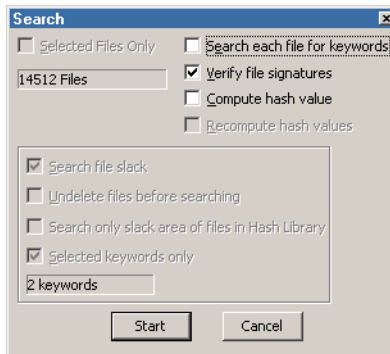



Figure 14-28: Running a signature analysis

In the dialogue box, check *only* **Verify file signatures**, and then click [**Start**]. The signature analysis will run in the background until complete. When the process completes, save the case.

Viewing Results

 In the **Cases** tab, display all files in the **Entries** subtab by clicking the **Set Include** button (“home plate”) so it turns green.

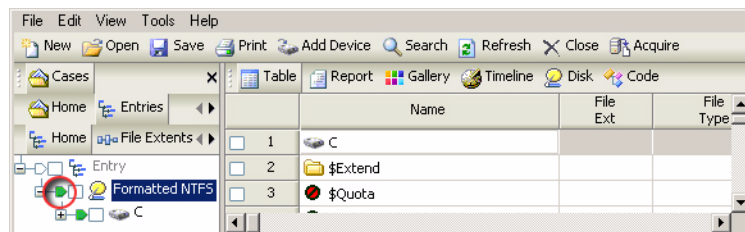


Figure 14-29: “Set Include Option

Click and drag the columns in the Table view so that the **File Name**, **File Ext**, and **Signature** column are next to each other. Once the column order is set, sort the columns with **Signature** at first level, **File Ext** at second level and **Name** at third level. To sub sort, hold the [**Shift**] key while double-clicking on the column header.

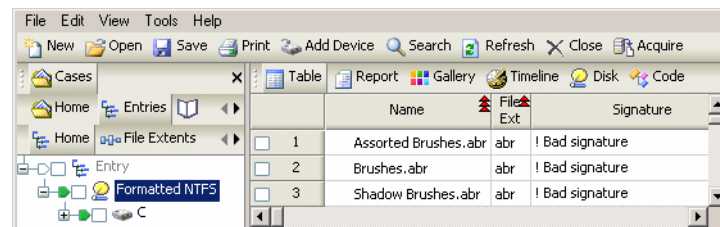


Figure 14-30: Signature analysis results with column changes and sorts in place

To examine the signatures, scroll up or down while viewing the signatures column. The results are described below:

- **! Bad signature**

A file extension has a header listed for it in the File Signature table, but the header of the file found in the case does not match the one in the File Signature table for that extension. The header is incorrect. This could indicate that the header is not known and should be added in the File Signature table.

- * **alias**

The header is in the File Signature table and the extension of the file in question is incorrect. This indicates a file with a renamed extension.

- **Match**

The header matches the extension. If the extension has no header in the File Signature table, EnCase will return a match as long as the header of the file does not match any header in the File Signature table.

- **Unknown**

Neither the header nor the file extension is in the File Signature table.

Hash Analysis

File Hashing

The **Hash** feature of EnCase allows the investigator to create a *hash value*—a “digital fingerprint”—for any file. The hash value for each file is unique, for all practical purposes. Only a copy of a particular file will yield the same hash value. The difficulty of coming up with two messages having the same message digest is on the order of 2^{64} operations, and that the difficulty of coming up with any message having a given message digest is on the order of 2^{128} operations. By building a library of hash values, EnCase is used to check for the presence of data with a hash value contained in the hash library. The hash value is determined by the file’s contents. It is independent of the file’s name, so the file’s hash value will be calculated by EnCase, and identified as matching a value in the hash library even if the file’s name has been changed.

The hash feature can be used to identify files whose contents are known *not* to be of interest to the examiner, such as operating system files and common application programs, as well as to identify files of interest, such as known Trojans, Root Kits, and unauthorized applications.

Hash sets are collections of hash values (representing unique files) that belong to the same group. For example, a hash set of all Windows 98 operating system files could be created and named “**Windows System Files**.” When a hash analysis is run on an evidence file, EnCase will identify all files included in that hash set. Those (logical) files can then be excluded from searches and examinations, speeding up keyword searches and other analysis functions.

Creating a Hash Set

Hash Sets can be created with any category name, although most filters in EnCase are designed for use with either “**Known**” or “**Notable**” category names. Known files

are benign or innocuous files that have little bearing on a case, such as Windows operating system files or Microsoft Office 2000 application files.

Notable files, on the other hand, would be files that might indicate criminal activity, such as hacker tool files, or child pornography sets.

To create a hash set, preview a machine or open an evidence file that contains the files that are going to be in the new hash set. You will need to make sure that EnCase recognizes the hash value of the files. Create the set as follows:

- Blue-check the files to be added into the new hash set.
- Click on the **Search** button on the top tool bar and check only the **Compute hash value** option. If the file already has a hash value listed in the Hash Value column of the Table in *Cases* view, and you wish to have EnCase recompute it to ensure you are using the correct hash value, you can also check the **Recompute hash values** option. After selecting these items, click [**Start**].

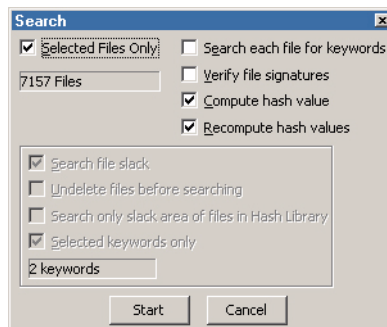


Figure 14-31: Computing hash values

- A status window will report the number of hash values generated. Click [**OK**] to close the window, and then verify that the values appear in the **Hash Value** column of the Table in *Cases* view.

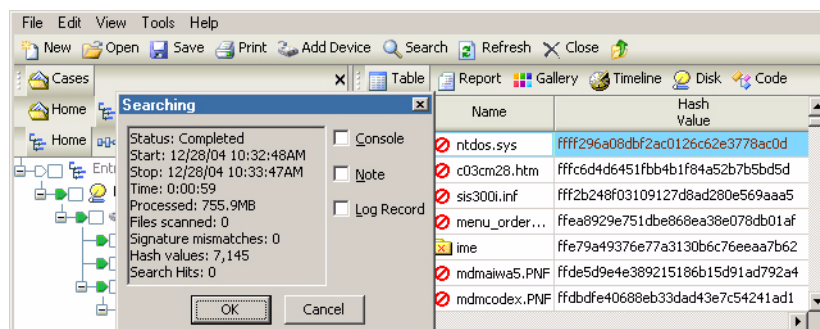


Figure 14-32: Generating hash values for selected files

- Blue check the files to include the values of in the hash set.
- Right-click in the Table Pane and select **Create Hash Set...**

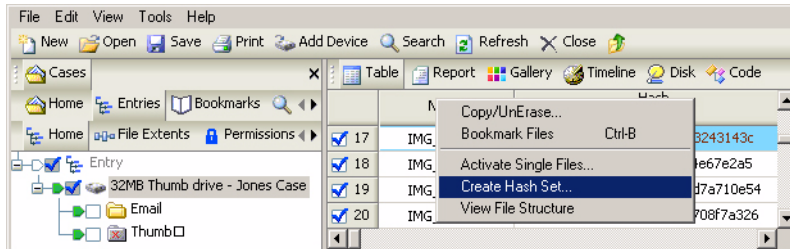


Figure 14-33: Creating hash set

- Enter the *Name* and *Category*, and then click [OK].



Figure 14-34: Hash Set Name and Category

You can blue-check, create, and add as many hash sets as desired.

Importing Hash Sets

EnCase supports importing hash sets from the HashKeeper and the National Software Reference Library (NSRL) CDs.

HashKeeper

HashKeeper, a program maintained by Heather Strong of the National Drug Intelligence Center, is an exhaustive library of hash sets for almost every operating system and application. This is a valuable resource for law enforcement. The HashKeeper CD is available exclusively through Heather Strong (heather.strong@usdoj.go) to members of the law enforcement community. To import HashKeeper sets:

- Copy hash sets from the HashKeeper CD to the **C:\Program Files\EnCase5\Hash Sets** folder. These files should have .HKE and .HSH extensions. These may be compressed using WinZip, or renamed with a .TXT extension. If the files have a .TXT extension, change them to .HKE.

- From the **View** menu, select **Hash Sets**.

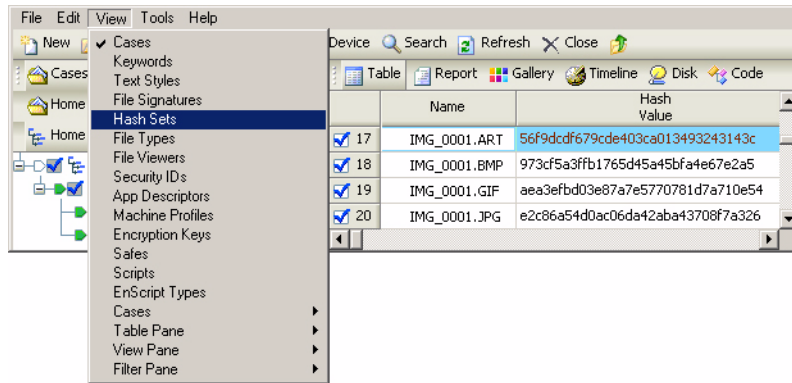


Figure 14-35: Hash Sets

- Right-click and select **Import HashKeeper...**

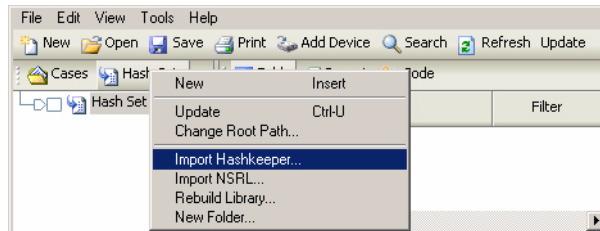


Figure 14-36: Import HashKeeper option

- A dialogue box will prompt for files with an .HKE extension. Navigate to the folder you copied the .HKE files to and select the ones you wish to import. You can import multiple files by holding down the **[Ctrl]** button and clicking on each of the desired files. Click **[Open]** to import the files.

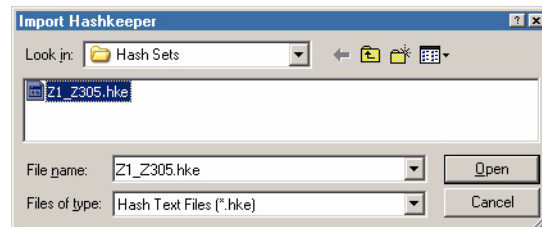


Figure 14-37: Browsing for .HKE files

Right click in the table and select **Update** to view the new hash sets.

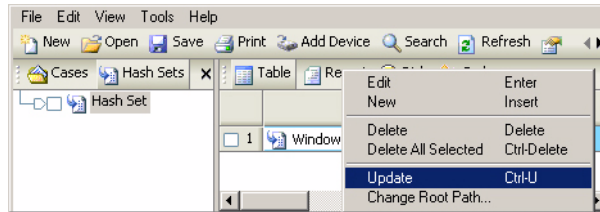


Figure 14-38: Update hash sets

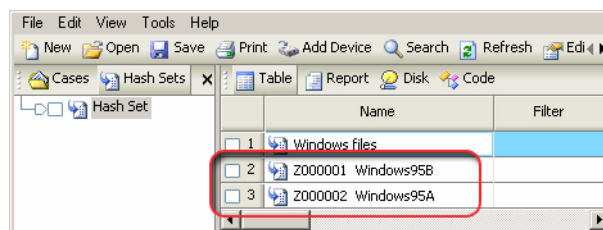


Figure 14-39: Imported hash sets

NSRL Hash Sets

The National Software Reference Library (NSRL) compiles a Reference Data Set CD, available at <http://www.nsrl.nist.gov>. The CD contains hundreds of hash sets of Known file types. These can be imported as follows:

- Extract the files from the .ZIP file on the NSRL CD to C:\Program Files\EnCase5\Hash Sets.
- Launch EnCase, and from the **View** menu, select **Hash Sets**.
- Right-click and select **Import NSRL...**

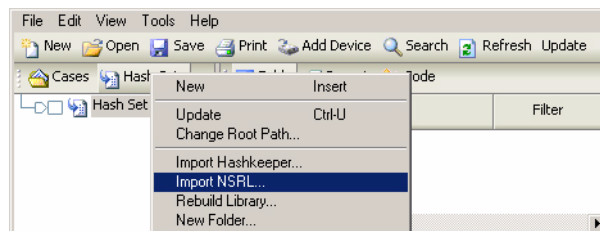


Figure 14-40: Importing NSRL hash sets

- Browse to the folder where you expanded the .ZIP file and select the NSRLFile.txt, then click [**Open**].

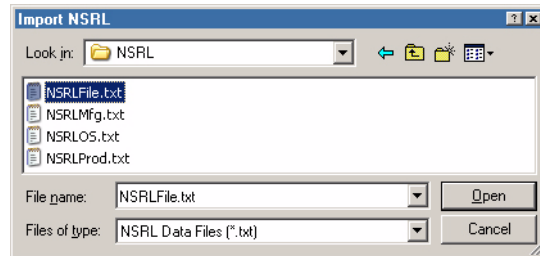


Figure 14-41: Selecting the NSRLFile.txt file

- The NSRL hash sets will start importing, indicated by the blue progress bar in the lower right corner of the EnCase window. When the files are imported, EnCase will read the hash values, displaying the status in the progress bar. Finally, EnCase will create the hash sets in the background. Depending on the number of files in the file, this may take some time.

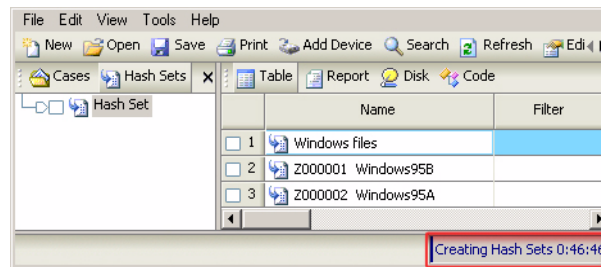


Figure 14-42: Creating NSRL Hash Sets

- Once the hash sets have been imported, right click on the root of the Hash Sets tab and select **Update**.

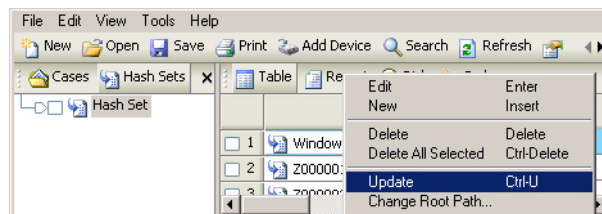


Figure 14-43: Updating Hash Sets

- Click on the **NSRL** folder in the left pane to view the hash sets. To add or change a **Category** to the files, double-click on the hash file in the table, then enter the category (**Known** or **Notable** is recommended) and click [OK]. You can change the hash file name at this time if you wish.

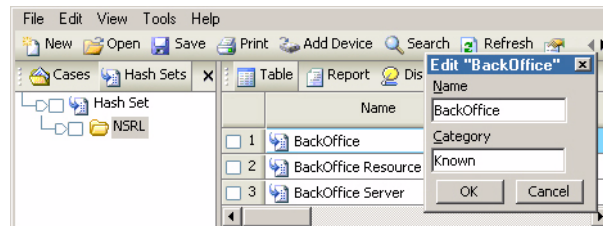


Figure 14-44: Changing Category

Rebuilding the Hash Library

The hash library contains the hash values to run against the data loaded into EnCase. The library is an accumulation of hash sets from chosen by the investigator, which can be rebuilt at any time, such as after adding new hash sets or deleting unwanted sets. Rebuild the library as follows:

- From the **View** menu, select **Hash Sets....**
- Blue-check the hash sets to be included in the library.
- Right-click on any hash set and select **Rebuild Library...**

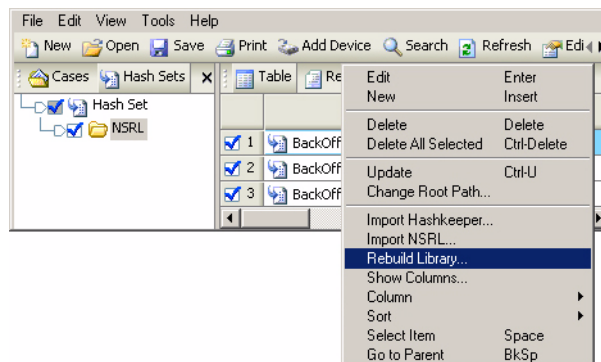


Figure 14-45: Rebuilding Hash Library

- A prompt will return and confirm the number of has sets that have been added to the library. Click [**OK**] to close the window.

Benefits of a Hash Analysis

Running a hash analysis will calculate MD5 hash values for all files that the user has specified (typically the entire case) and compare them with those stored in the hash library. Without generating this \value, it is not possible to benefit from using hash

sets in a hash library as no hash values are known. One of the first steps of any investigation is to run a hash analysis of all the evidence files within the case.

Starting a Hash Analysis

- Launch EnCase and open a case containing an acquired evidence file, or preview a machine.
- Click on the **Search** button on the top tool bar and check only **Compute hash value**. If the file already has a hash value listed in the Hash Value column of the Table, and you wish to have EnCase recompute it to ensure you are using the correct hash value, you can also check the **Recompute hash values** option. After selecting these items, click [**Start**].

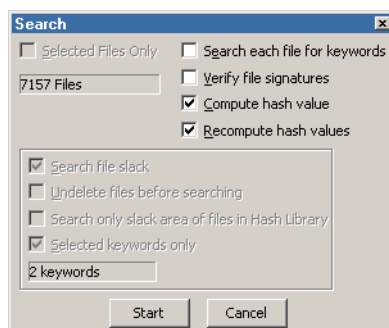


Figure 14-46: Computing hash values

- A status window reports the number of hash values generated; click [**OK**] to close the window.

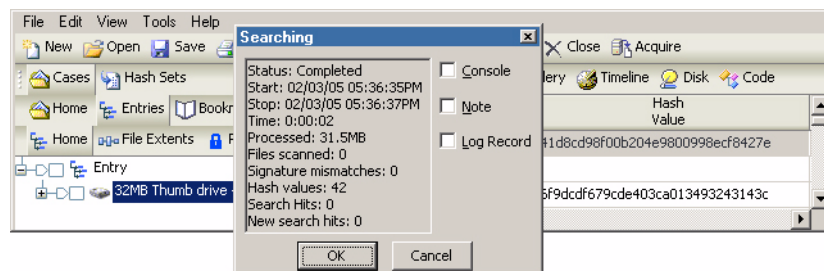


Figure 14-47: Confirmation of file hashing

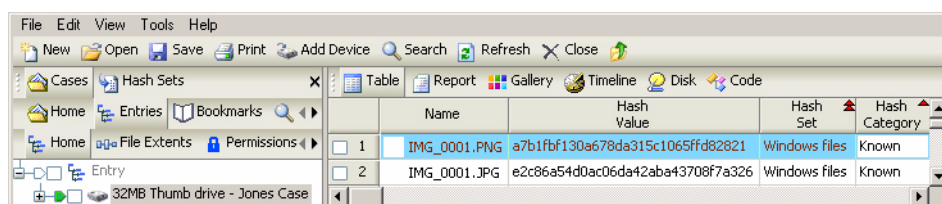
Analyzing the Hash Results



- Click on the green **Set Include Option** trigger (home plate) next to the evidence file in the Tree Pane under the **Entries** subtab (beneath **Cases**).

- Locate the three hash columns in the Table Pane (**Hash Value**, **Hash Set**, and **Hash Category**). You can put these together by clicking on the header and dragging the column where you want to put it.
- Sort on **Hash Category** by double-clicking on the column header, and then scroll to the top to view the results. You can sub-sort by holding down the [Shift] key and double clicking on the **Hash Set** column header.

The files that are in the hash sets are easily identified by entries in the hash columns. Knowing what files are in **Known** hash sets, for example, will allow the investigator to bypass files with known hash values in order to speed up keyword searches.



	Name	Hash Value	Hash Set	Hash Category
1	IMG_0001.PNG	a7b1fbf130a678da315c1065ffd82821	Windows files	Known
2	IMG_0001.JPG	e2c86a54d0ac06da42aba43708f7a326	Windows files	Known

Figure 14-48: Hash columns in Table view

EnScripts

There are a number of EnScripts that are installed with EnCase that provide useful functionality and save time and effort in the forensic examination of evidence files. The EnScripts are accessed by selecting **Scripts** from the **View** menu. Scripts created by parties other than Guidance Software are not available for download, but are frequently exchanged via the EnScript message board.

Initialize Case

The Initialize Case EnScript extracts useful information from Windows such as time zone settings, Windows version, shared folders, user info, and registration data, etc.

FAT and NTFS Info Record Finder

This script searches through unallocated space and slack space for FAT info file and NTFS Info2 records (database records of deleted files) and create a bookmark folder with the results.

File Finder

Recovers files from unallocated space, creating a Bookmark folder with the results, with an option to export the files to a specified directory. File types that can be selected include AOL ART, BMP, EMF, GIF, JPG, Photoshop (PSD), PNG, TIFF, Word, Excel,

Zip and GZip, with the ability to create a custom file type to search for based on header, footer and/or extension.

Link File Parser

The link file parser EnScript will extract information contained within Windows .LNK (shortcut) files. This information may include flags and attributes specific to the link file; the link type; creation, modification and last accessed dates; volume label; drive type; drive serial number; file length; icon file; link description; file link path; base path; application path; working directory; network share name, and command line.

Find Unique EMail Address List

This script searches through selected files for a “basic” e-mail signature. The “hit” is then confirmed using a built-in EnScript function. If the hit passes the confirmation test, it is added to an e-mail list, so that if the same address is found again later in the evidence file, it will not be added again to the list.

NAVIGATING ENCASE

This chapter describes how to create a new case, add evidence files and verify them using EnCase Version 5 and details the different tabs and views.



The interface for EnCase Version 5 has changed significantly from Version 4. Please read this chapter thoroughly, especially the section which explains the different “views” of EnCase.

Creating a New Case

Launch EnCase by double-clicking on the desktop icon, or launching the application from the **Program** menu on the [Start] button.



Figure 15-1: EnCase Version 5 desktop icon

Click the [**New**] button on the toolbar to create a case. You are prompted to input information for the case options:

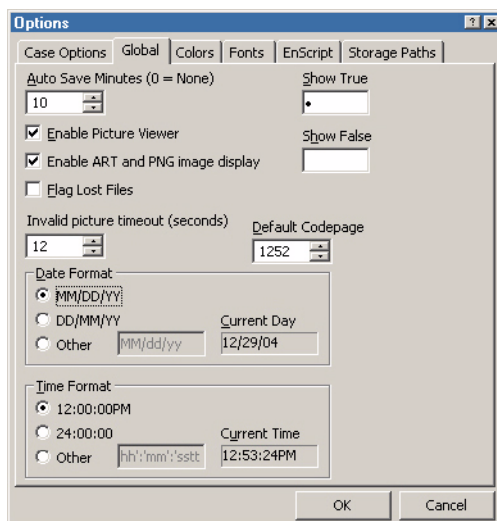


Figure 15-2: New case options

- **Name**

Enter a short description for the case. The text entered here will be the text displayed by the case folder under the Cases tab.

- **Examiner's Name**

Enter the lead investigator's name for this case.

- **Default Export Folder**

Files, by default, will be exported to this folder when the **Copy/UnErase** option is selected, or when an EnScript exports files to the hard drive.

- **Temporary Folder**

The temporary folder is where files are copied to when viewed with an external viewer. For example, if you set up QuickView Plus as a viewer in EnCase with which to view JPG and GIF files, and then double-clicked a .JPG file within an evidence file, the .JPG file would be extracted from the evidence file, copied

to the temporary folder, and then opened with QuickView Plus. When a case file is closed, EnCase automatically deletes the temporary folder's contents.



If the paths you enter for these folders do not already exist, EnCase creates them.

Click the [OK] button and the new (and empty) case is created.

Case Management

Before starting a case, it is important to create case organization guidelines. First, consider how case files and evidence files will be organized on the hard drive. Most investigators dedicate a high-capacity storage drive on the forensic machine to storage of evidence files, putting evidence files into appropriately named folders for each case they are working on. For example, if an investigator was working three cases, he might have a D:\Cases\Smith folder, a D:\Cases\Johnson folder, and a D:\Cases\Jones folder. With files for each case placed into a folder named after the Subject (such as D:\Cases\Jones), then your Default Export folder and Temporary folder might set to D:\Cases\Jones\export and D:\Cases\Jones\temp (respectively) for that case.

Concurrent Case Management

EnCase Version 5 has the ability to open more than one case at a time. Each case will appear in the Table Pane when the **Home** subfolder under **Cases** is selected. Each case has its own **Report** view, **Bookmark** folder, **Devices** folder, etc.

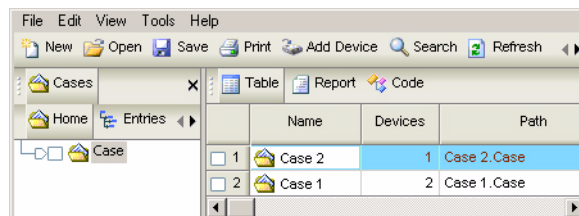


Figure 15-3: Multiple cases

Having multiple cases open simultaneously simplifies case comparison analysis functions, such as keyword searches, reviewing search hits, etc. Version 5 shows evidence files associated with each case differently than in Version 4. The **Devices** column of the table indicates how many devices are associated with the case in the

Name column. To look at the devices associated with a particular case, highlight the case in the Table Pane and then click on the **Entries** subtab below **Cases**.

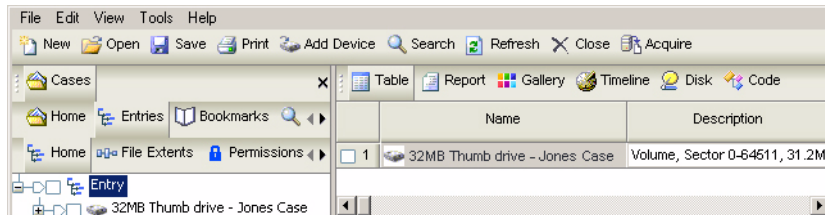


Figure 15-4: Devices associated with a case

The Options Dialog

The **Options** menu allows users to configure administrative functions of the software. To access the menu, select **Options...** from the **Tools** menu. Five tabs are available: **Global**, **Colors**, **Fonts**, **EnScript** and **Storage Paths**. When a case is open, a sixth tab (**Case Options**) appears that allows you to set default values for subsequent case name, Examiner name, and Export and Temporary folder location as described at the beginning of this chapter.

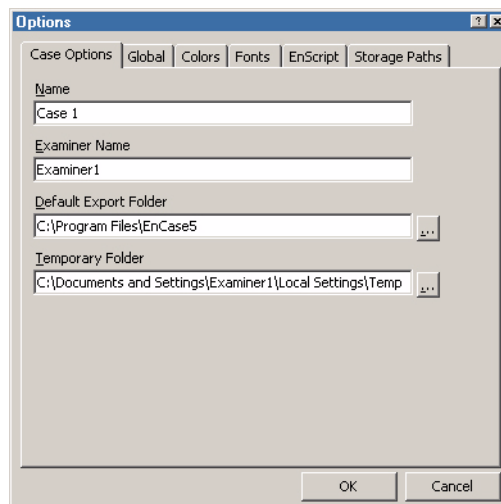


Figure 15-5: Case Options

Global Options

Global options, once set, are in effect when EnCase is open.

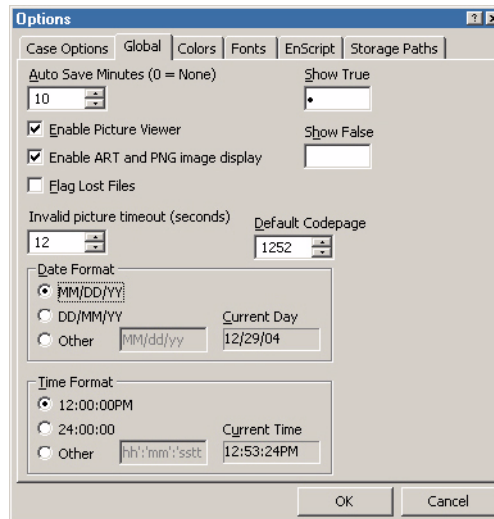


Figure 15-6: Global Options

Global options include:

- **Auto Save Minutes (0 = None)**

Auto Save records changes to the case and saves them to the .CBAK backup case file. This setting (10 minutes by default) determines the amount of time between saving the case. Setting this value to 0 disables **Auto Save**. With this set to a more frequent value, the examiner may see the performance slow down while performing other tasks.

- **Show True \ Show False**

Show True and **Show False** allow the user to define characters or strings that identify whether a condition in certain table columns is true or false. These appear various views such as **Show Picture, In Report, Is Deleted, Permissions, Excluded**, etc., and in wizards such as **Add Device (Write Blocked, Read File System)**.

By default, **Show True** is defined by a bullet (•), while **Show False** has no defined identifier. **Show True** is set to True and **Show False** to False, in the last two columns in this Add Device wizard:

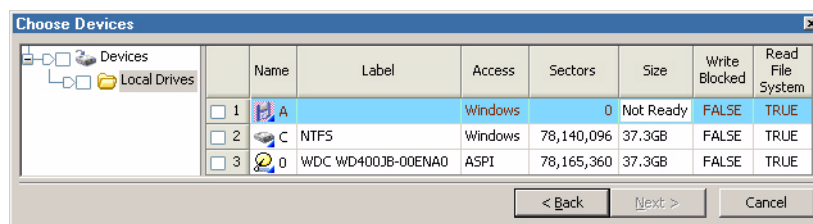


Figure 15-7: Add Device wizard showing True/False identifiers

- **Enable Picture Viewer**

This option, checked by default, allows EnCase to display pictures in Gallery view (right pane), Picture view (bottom pane) and in Report.

- **Enable ART and PNG image display**

Uncheck this option to disable displaying ART and PNG images in Gallery view (right pane), Picture view (bottom pane) and Report view, since these files appear to cause the bulk of the issues with corrupted images. Some ART and PNG images recovered in the unallocated clusters or otherwise corrupt logical files will crash the Internet Explorer .dlls used to display these images in EnCase. Guidance Software cannot prevent these corrupt images from crashing the .dlls nor the cascade effect of crashing EnCase. To alleviate this issue, the user can uncheck this option, allowing them to continue their work on a case while ignoring these corrupt image. Before viewing AOL ART and PNG files on the forensic machine, be sure to apply the libPNG library patch for Internet Explorer available at <http://www.libpng.org/pub/png/libpng.html>.

- **Invalid picture timeout (seconds)**

EnCase includes threaded crash protection for corrupt image files. The **Invalid picture timeout** sets the amount of time in seconds for a thread to try reading a corrupt image file. Once the timeout value has been exceeded, EnCase will cache the file to allow EnCase to take preventative measures ensuring the file does not crash EnCase when accessed later. By default, the value is set to 12 seconds.

- **Default Codepage**

This value, when set, is applied to any compound files mounted by right-clicking and selecting **View File Structure**. It is applied by default each time until changed.

- **Date Format**

This setting allows the user to change the way dates are displayed in EnCase. For example, Europeans typically display the date as **day/month/year** by selecting the **DD/MM/YY** radio button. You can also set a custom date display, substituting dashes for slashes or having the year display as 4 digits by typing **YYYY** for the year when selecting the **Other** radio button.

- **Time Format**

Time format can be changed to display military (24-hour) format, or a custom display specified after selecting the **Other** radio button.

- **Flag Lost Files**

By default, this option is unchecked which means lost clusters are treated as unallocated space, drastically decreasing the amount of time required to process the volume. If this option is checked, EnCase will tag all lost clusters in Disk view (indicated by yellow blocks with a question mark). This option must be set before an evidence file is added to the case

Colors

The investigator may change display colors for different elements of the EnCase interface. Bookmarked text by default is light blue, but can be changed by double-clicking the Bookmark entry and selecting a new color. Colors may be changed for representation of search hits, text selection (both focused and not focused), code comments, normal (logical) text, slack text, normal (logical) and slack text in reports, filter frames, and filter text (filter frames and filter text colors can be changed in **Queries** as well).

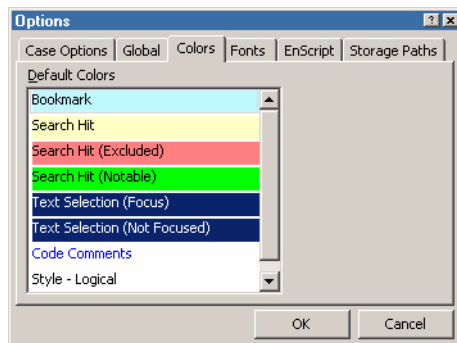


Figure 15-8: Colors Options

Fonts

A font, its size, style, and script can be changed for different areas of the EnCase interface. While any part of the EnCase interface can be customized (such as changing the font for Script code when scripting), the **Fonts** tab is useful when working with foreign languages that require a specific font to display correctly. To change a font, double-click on the area listed in the **Default Fonts** window. For more information, see the chapter in this document on *Foreign Language Support*.

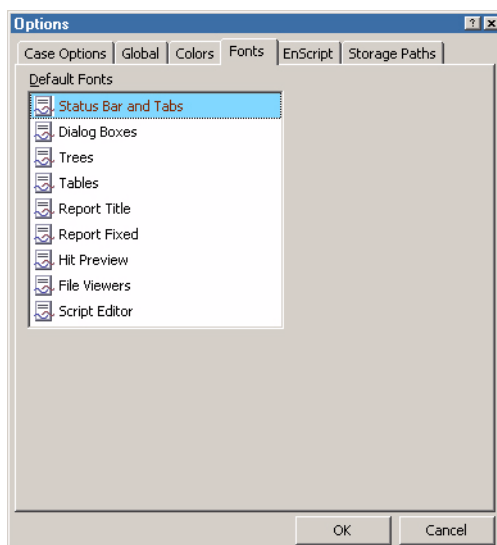


Figure 15-9: Fonts Options

EnScript

EnScripts are essentially small programs that allow EnCase to access data and extract and store that data for examination. The **Include Path** is the name of the EnScript libraries folder (this is typically located by default in **C:\Program**

Files\EnCase5\Scripts\Include); this should generally be left with the default path of **Include**.

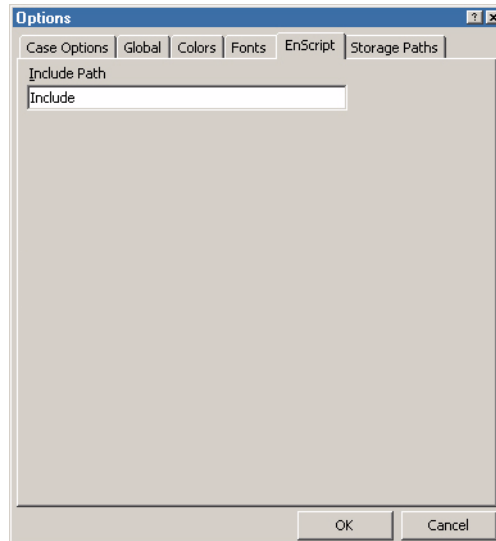


Figure 15-10: EnScript Options

Storage Paths

EnCase allows the user to set the paths to where the configuration files for global settings (.INI files) are stored using the **Storage Paths** tab. This feature allows an organization to have one set of EnCase .INI files on a networked drive that all examiners use. The administrator of the configuration files can change the .INI file attributes to be read-only for all examiners except the one who maintains the configuration file. The read-write attributes are displayed in the **Writable** column of the table. To change the path or read-write status, double click on the file, or highlight it and select **Edit** from the right click menu (or press [**Enter**]). The read-write status can also be changed by right clicking on the file in the **Writable** column and selecting **Writable**. Users can change the paths for the `SecurityIDs.ini`, `Viewers.ini`, `FileSignatures.ini`, `FileTypes.ini`,

Keywords.ini, AppDescriptors.ini, Profiles.ini, and TextStyles.ini.

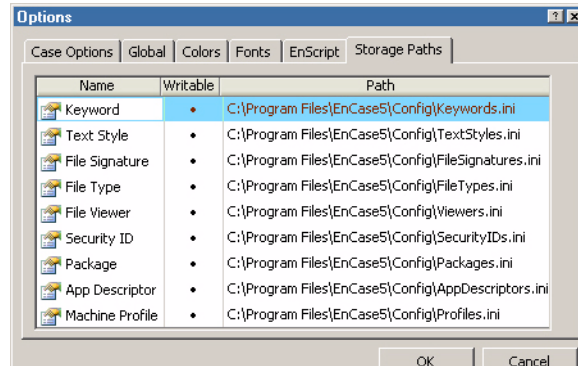


Figure 15-11: Storage Path Options

Enterprise

The **Enterprise** tab allows the user to set Enterprise-specific options. This tab does not appear in EnCase Forensic. Options in this window include:

- **Attempt Direct Connection**

EnCase now permits users to attempt connecting directly to a network node if there are communications issues with the SAFE. The different modes are as follows:

- **None**

If for some reason the target system cannot establish a connection with an EE client, then all traffic is redirected through the SAFE server. This can

increase communication times, however, it provides the investigator with the ability to obtain data that otherwise would not be available.

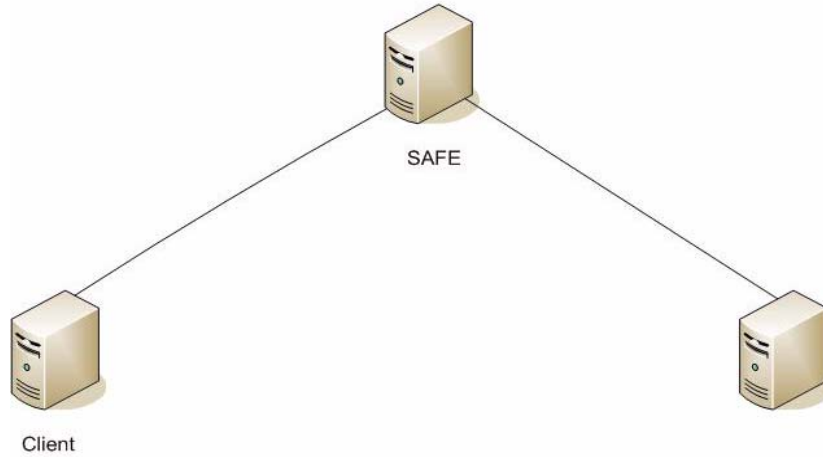


Figure 15-12: No Direct Connection attempt

- **Client to Node (Local)**

This option should be enabled when the client (Examiner) and the node (servlet) reside on the same network, and the SAFE resides on a different network. This allows data to transfer directly from the node to the client, after the client successfully authenticates through the SAFE. Also the client will use the IP address that the node believes it has, rather than the IP address the SAFE has for the node. In this configuration, the network should be designed so that all the company’s employees are located on the Corporate Desktop Network, and should employ routing/NATing.

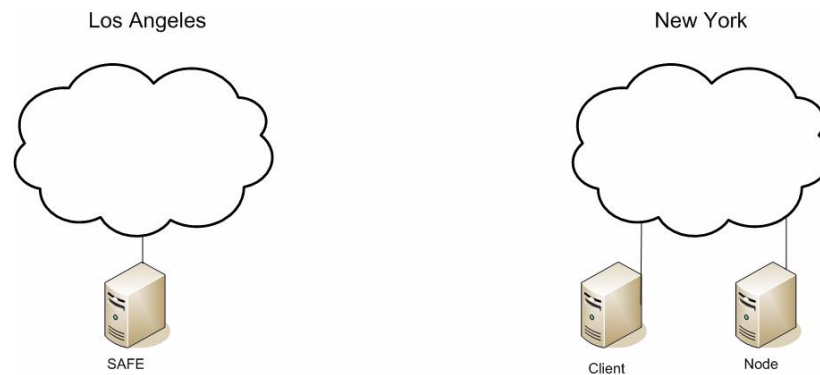


Figure 15-13: Client-to-Node (Local) Direct Connection attempt

- **Client to Node (SAFE)**

This mode is useful when an organization enables NAT (where a private IP address is mapped to a public IP address). Typically, the SAFE and node reside on the same subnet, and the client on another. This allows data to transfer directly from the node to the client, after the client successfully authenticates through the SAFE. The client also uses the IP address that the SAFE believes the node has, rather than the IP address the node reports it has to allow a direct connection between the client and node machine. This option is enabled by default.

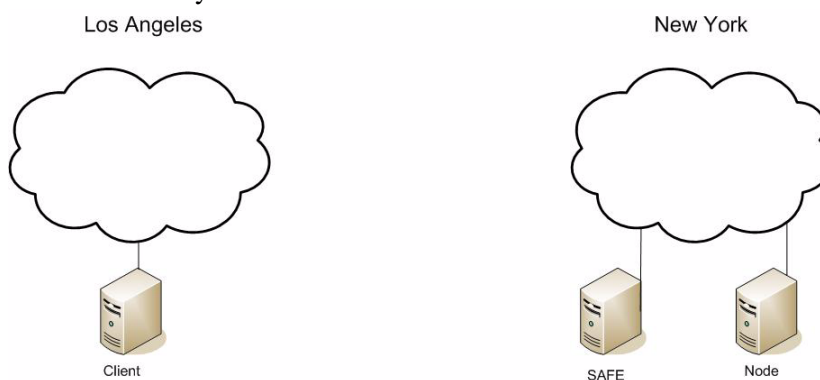


Figure 15-14: Client-to-Node (SAFE) Direct Connection attempt

- **Node to Client**

This functions similar to the **Client to Node (SAFE)** mode, except that the node will attempt the direction connection to client. It would be used where you desire direct data transfer between the node and the client, and there is NAT'ing or a firewall prohibiting the node from sending data directly to the local IP/default port of the client. Once you check the option, the **Client return address** configuration box will become available to enter the

NAT'ed IP address and custom port (e.g., **192.168.4.1:1545**). The **Client return address** box is grayed out unless this option is selected.

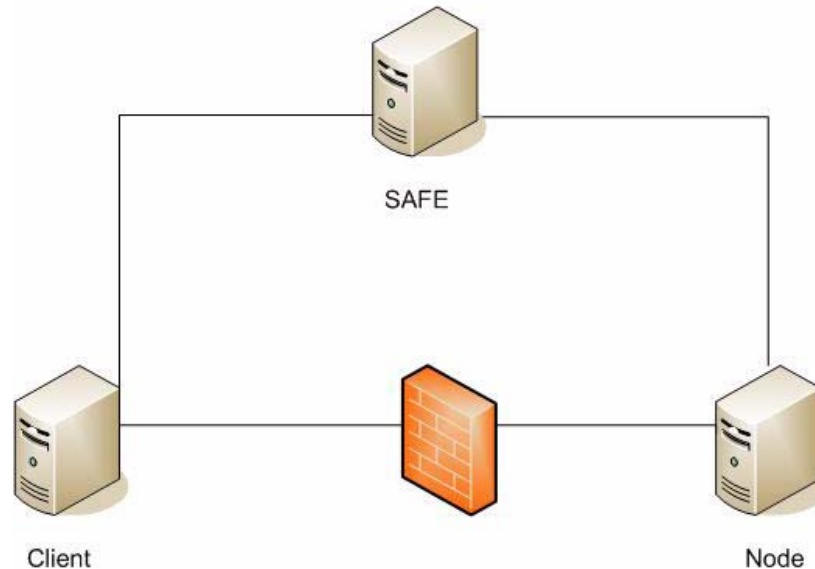


Figure 15-15: Node-to-Client Direct Connection attempt

- **Private Key Caching**

EnCase now caches users' private keys for a set period of time so that they can reconnect to the SAFE without having to re-enter their password. The value is set in minutes; a value of **0** denotes no caching taking place, while a value of **-1** allows for infinite key caching. This value is set to **60** by default.

- **Auto Reconnect**

EnCase Enterprise will attempt to reconnect to a node if the connection is lost during preview or acquisition. **The Auto Reconnect Attempts** feature allows the user to enter the number of times to try attempting re-establishing the

connection. **Auto Reconnect Intervals(secs)** specifies a value (in seconds) to allow between connection attempts.

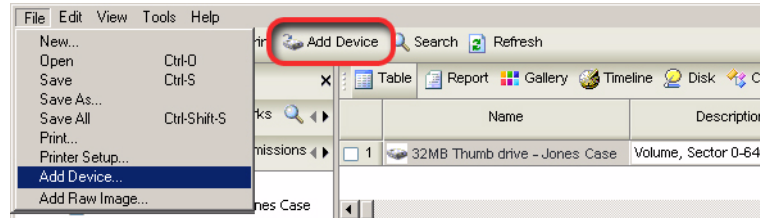


Figure 15-16: Enterprise Options

Adding Evidence Files to a Case

To add pre-existing evidence files to a case, the user must know the location of the evidence files, either locally or on the network. Add evidence as follows:

- Select **Add Device...** from the **File** menu, or click on the **[Add Device]** button on the top toolbar.

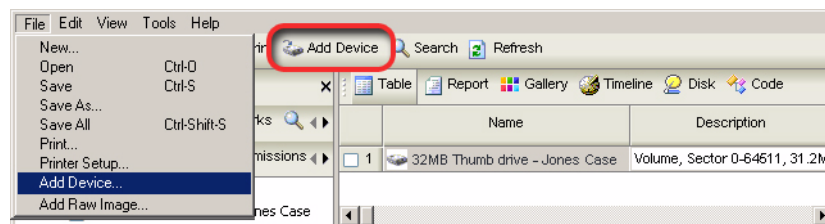


Figure 15-17: Adding a device

- Direct EnCase to the location of the saved evidence files by right clicking on the **Evidence Files** folder in the left pane and selecting **New**.

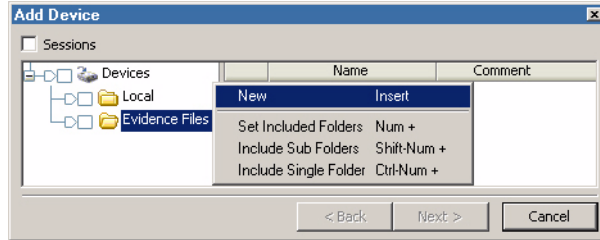


Figure 15-18: Defining new evidence file location

- Browse to the location of the evidence files and then click [OK].

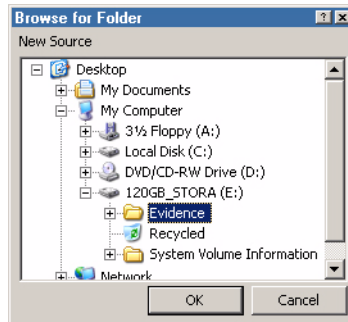


Figure 15-19: Selecting evidence file folder

- The new folder appears in the left pane below **Evidence Files**. Select the **Set Include Options** trigger (“home plate”) shown in Figure 15-20. All available evidence files in that folder and subfolders should appear in the right pane. Additional folders in other locations can be added in the same manner.

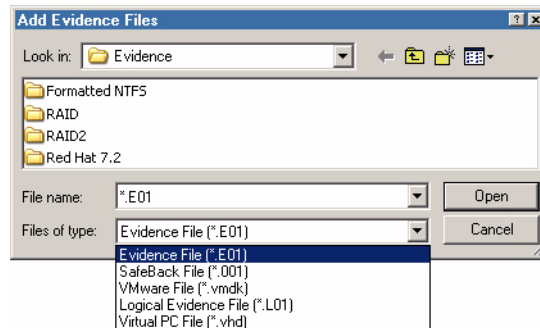


Figure 15-20: Adding evidence files

- Blue-check the desired evidence files (devices, volumes, floppy disks, removable media, or Palms) from the right pane and click the [**Next >**] button. A confirmation screen will show the evidence files you are adding.

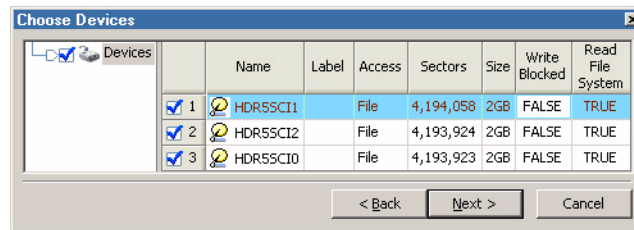


Figure 15-21: Confirming devices

- Double clicking on the selected item will allow you to select whether or not to have EnCase read the file system. If the **Read File System** check box is left blank, EnCase will not read or display filenames or a folder structure. After checking attributes, click [**OK**], then [**Next >**].

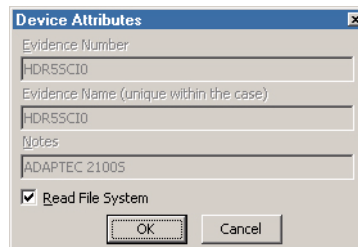


Figure 15-22: Device attributes

- You are prompted for a final confirmation before adding the selected items to the case. If all items are correct, click [**Finish**].

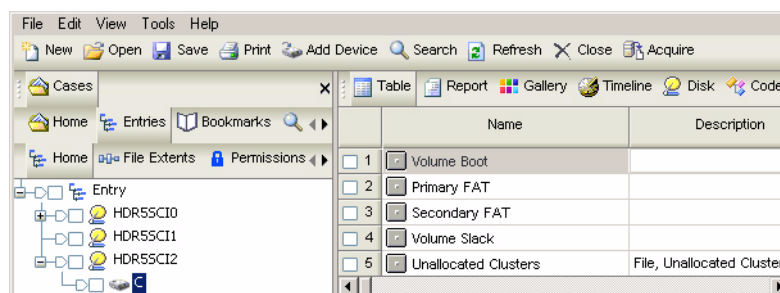


Figure 15-23: Case with three devices

Sessions Option

The **Sessions** option allows EnCase to remember previously previewed or audited devices. The session information is stored so that a new case can be opened but a device that is being actively audited can be retrieved for more efficient case management. To use the **Sessions** option:

- In a new or existing case, select **Add Device...** from the **File** menu, or click on the [**Add Device**] button on the top toolbar.
- Check the **Sessions** option in the upper left of the **Add Device** screen.

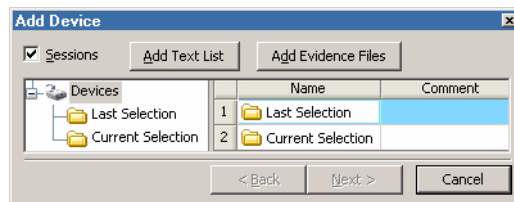


Figure 15-24: Sessions screen

- If the [**Add Text List**] button is selected, the examiner is prompted for a path to the evidence files. You can type a full local path (including a mapped drive letter), a network path (with domain access), or a combination. You may need to resolve network paths (`\\servername\foldername\evidence.E01`) by using the browser to find the evidence file. Complete the list with the [**OK**] button.

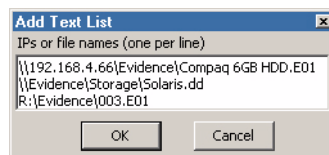


Figure 15-25: Text list for Sessions

- If [**Add Evidence Files**] is clicked, you can browse folders to find the evidence files, in the same manner as previous versions of EnCase. The drop-

down box for **Files of type:** allows users to search for an EnCase evidence file (.E01), SafeBack file (.001), or VMware file (.vmdk).

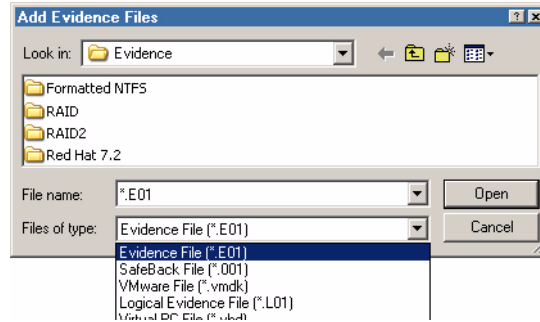


Figure 15-26: Adding evidence files

- Two folders appear in the left pane of the **Session** window. **Last Selection** contains the last evidence files added to, and saved in a case.

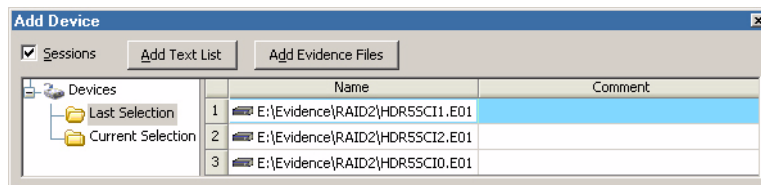


Figure 15-27: Last Selection folder

- **Current Selection** contains evidence files or devices currently selected (blue checked) in the **Add Device** wizard outside of sessions. Adding evidence via the **[Add Text List]** or **[Add Evidence Files]** buttons, or right clicking in the right pane, selecting **New** and adding a source path for evidence will also populate the **Current Selection** folder.

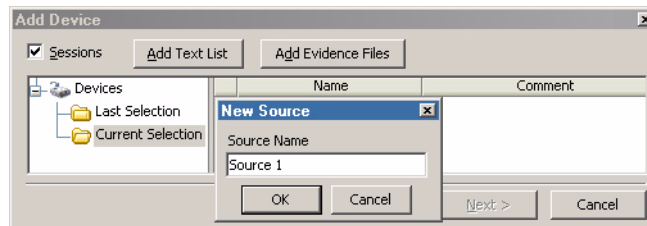


Figure 15-28: Current Selection folder

- You can also create new folders and subfolders to store links to evidence files the forensic machine has access to. Right click in the location where you wish to place the folder and select **New Folder**.

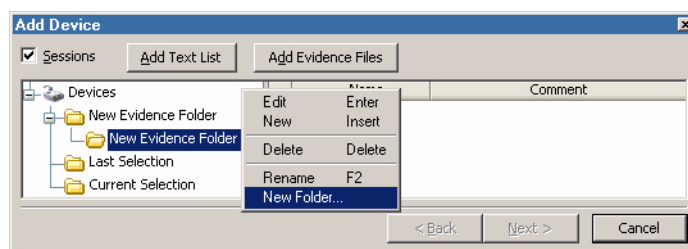


Figure 15-29: Creating a new Session folder

Error Messages

Below are typical error messages encountered when adding evidence.

- **“X:\PATH\EVIDENCE.Exx’ could not be found. Choose a new path for this file?”**

EnCase cannot add an evidence file unless all the segments (or “chunks”) are mounted at the same time. If possible, place all chunks of an evidence file in a single location on your hard drive. If storage space prevents this, select [**Yes**] to choose a new path and then browse to the location of the missing chunks. If the chunks in question are missing, you will be asked if you wish to zero out the sectors represented by the missing file.

- **“Error verifying checksum in the file [EVIDENCE.Exx]”**

The media on which the file is stored may have become corrupted. This error occurs when the evidence file header is corrupted to the point at which EnCase will no longer recognize it, rejecting it when adding it to a case. Try to re-acquire the original media to *different* media than before, or add a copy of the evidence (it is advisable to make multiple acquisitions for backup purposes).

- **“Unable to read 64 sectors starting at absolute sector nnnnnnnn”**

This message usually indicates that a file-pointer in the directory structure of the evidence file is pointing to an area of the disk EnCase did not acquire. This is the fault of the BIOS reporting the wrong size of the physical disk.

To determine if the BIOS has misreported the size of the disk, check the Drive Geometry section of the EnCase report for **Total Size in sectors**. The Partition Table section of the Report displays the sector size of each partition. The total

number of sectors, added up from each partition, should equal the *Total Size in sectors*. If it does not, the BIOS may have misread the geometry of the hard drive. You can try manually inputting the Cylinders-Heads-Sectors (CHS) information into the computer with the subject's hard drive, and then reacquiring the whole drive. Do not let the BIOS auto detect the CHS information.

The storage computer BIOS may not support more than 8 GB of drive space' also, the suspect machine BIOS may support the drive size but the storage computer BIOS may not.

Finally, if the CHS information is correct, but continue to encounter the error messages, data in the file may be corrupted, causing EnCase to interpret it as file-pointers to areas that do not exist. Click [OK] to bypass the error messages and continue inspecting the evidence file.

- **“Decompression error in file ' X:\PATH\EVIDENCE.Exx', file may be corrupted.”**

Reacquire the subject drive.

- EnCase locks up after adding the evidence file, and Task Manager reports that EnCase is ‘not responding.’

Adding evidence to a case rarely locks up EnCase. This condition may occur if evidence files are particularly large, if the file is in EXT2 format, if there are a large number of deleted files to be recovered, when adding SafeBack or dd images, or if the file is graphics intensive. EnCase is not frozen; it is performing multiple complex operations. This condition, sometimes accompanied by a “white screen”, usually disappears after the task is complete. Adding memory to the forensic machine sometimes alleviates this issue.

Verifying the Evidence

After adding an evidence file to a case, EnCase automatically starts verification of file integrity. EnCase reads the data in the evidence file and generates an MD5 (Message Digest 5 algorithm) hash value for the data, displaying the verification and acquisition MD5 hash values in the report. A flashing-blue bar will appear in the lower-right corner of the EnCase window indicating that verification is taking place, checking the hash value and CRC values of the saved file. To cancel verification, double-click the flashing verification bar.

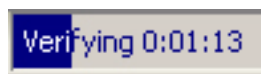


Figure 15-30: Evidence file verification

EnCase will save the evidence file verification only if you *save* the case *after* the verification process is finished. If the case is closed without saving, the verification process will begin each subsequent time the evidence file is loaded.

Adding Raw Image Files

EnCase can add raw image files (images of media in a flat-file format, such as Linux “dd”) to a case:

- Add the raw image by selecting **Add Raw Image...** from the **File** pull-down menu (a raw image cannot be added using the **Add Device** button.)

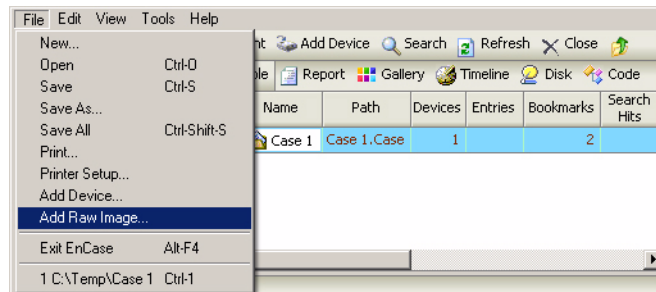


Figure 15-31: Add Raw Image

- At the top of the **Add Raw Image** screen is a **Name** field. Text entered here will be the name of the evidence file once it has been added to the case.
- Right click in the **Component Files** field and select **New**. If files were imported previously, they will show in this field.

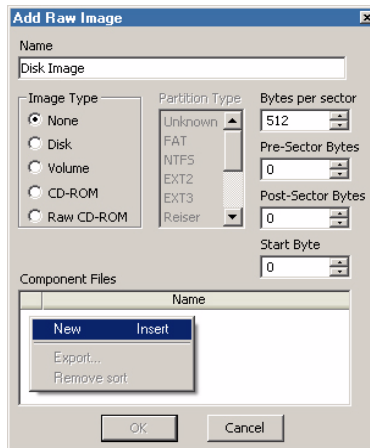


Figure 15-32: Add New Raw Image

- Add the raw image chunks in the order created. In the browser, select the last item, hold down the [**Shift**] key and using the “up arrow” key, select from the last item to the first (reverse order). You should see the correct sequence in the **File name:** field at the bottom of the browser. Click on [**Open**] to add the files.

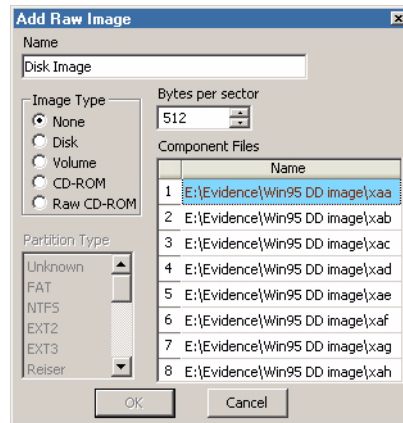


Figure 15-33: Selecting raw image segments in order

- The image chunks should show in the **Components Files** field in correct order. If they are out of order, click on the item in the wrong location and drag it to the proper location. You must specify the **Image Type** by selecting the appropriate radio button:
 - **None** – Selected by default; adds the entire image as Unallocated Clusters
 - **Disk** – Physical disk image
 - **Volume** – Locally mounted drive letters; includes floppies, removable media (except CD-ROM), logical volumes, etc. If known, the partition type should be specified by selecting the appropriate item in the **Partition Type** field.
 - **Raw CD-ROM** - Version 5.05 allows for the import of CD images made with SlySoft CloneCD™. When a **Raw CD-ROM** image is imported, **Pre-Sector Bytes**, **Post-Sector Bytes** and the **Start Byte** can be input in the corresponding text boxes.
- With the segments displaying in the correct order, and the appropriate **Image Type** and **Partition Type** selected, check the case name (in the **Name** field) and click [**OK**]. You should now see a complete volume or device with file structure visible.

SafeBack and VMware Images

SafeBack (.001) v2.x image files, VMware .vmdk images (versions 3 and 4) and Virtual PC files (.vhd) can be added to EnCase the same way as EnCase evidence files. The method for adding these files follows:

- Launch EnCase and open a new case.
- Click on the [**Add Device**] button on the toolbar, or select the option from the **File** drop-down menu.
- If the folder where the evidence is located exists in **Evidence Files**, click on the **Set Include Option** button. If it does not appear, right click on the **Evidence Files** folder, select **New**, browse to the directory where the files currently reside, highlight the folder and click [**OK**]. Blue check the appropriate EnCase evidence file (.E01), SafeBack image file (.001) or VMware image (.vmdk) or Virtual PC files (.vhd) and select [**Next >**].

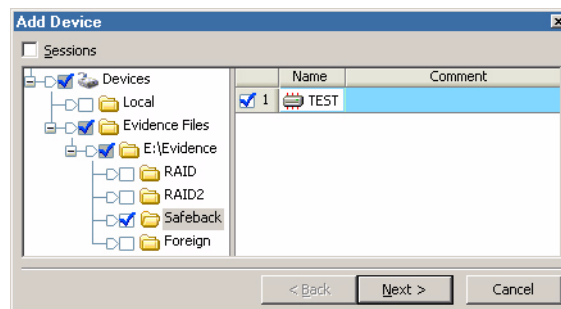


Figure 15-34: Adding a SafeBack image

- EnCase will parse the image file structure to determine the type of device contained within the image file. For large images, this may take longer; however, when the [**Add Device**] wizard is complete, the image file will be loaded immediately into the Case file since the file structure was already

parsed. This is different from EnCase evidence files, which are parsed after they are brought into the Case file.

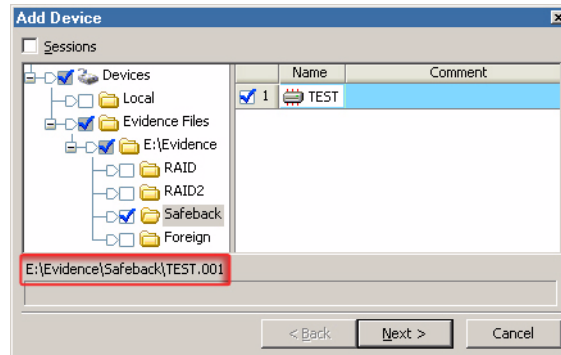


Figure 15-35: EnCase parsing a SafeBack image

- After EnCase parses the file structure, the information about the type and size of the device will be available in the **Choose Devices** window. Double-click on the device name to change the name in EnCase, or click **[Next >]** to continue. The **Preview Devices** window lists all devices selected for adding to the Case file.

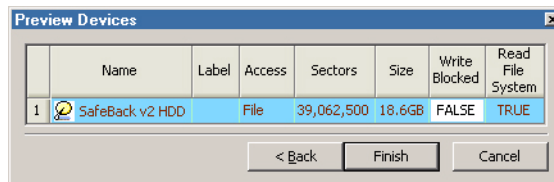


Figure 15-36: Preview Devices

- Click on **[Finish]**; the image file will be loaded into EnCase, and the CRCs will be verified. You will then be able to conduct an examination of the image

file as you would an EnCase evidence file or dd image. The results of the CRC verification will be reflected in the report of the device.

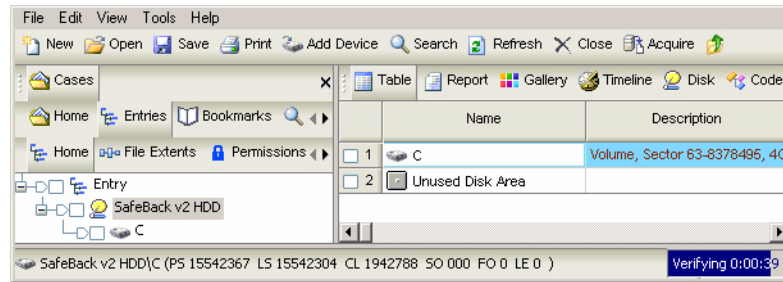


Figure 15-37: SafeBack image verifying in EnCase

You can also drag and drop a SafeBack .001 file into EnCase to parse, load, and verify the image file, or use the **Sessions** function in the **Add Device** wizard.

Single Files

The **Single Files** option allows the creation of a logical evidence file containing a number of external files. This option is disabled by default. To enable it, select the **Entries** subtab below **Cases**. You can right-click on the **Entry** root and select **Activate Single Files...**, or select the option from the **Edit** pull-down menu. A folder will appear in the Tree Pane called **Single Files**.

To add files to the folder, right click on the **Single Files** folder and select **New**, then navigate to the location of the files you wish to add. Files can only be added one at a time in this manner; once the file is selected, click on the **[Open]** button to add it to the folder. Alternately, you can drag-and-drop files from Windows Explorer to the open EnCase windows folder; allowing multiple files to be added simultaneously. This method does not require a case to be open or for the user to be in a specific tab.



You cannot drag-and-drop files from within an EnCase evidence file or preview to the Single Files folder.

Once the desired files have been added, the file can be saved as a logical evidence file by right-clicking on the **Single Files** folder and selecting **Acquire...**, or clicking on the **[Acquire]** button on the top toolbar.

Logical Evidence Files

Users can now isolate files from inside an evidence file and access them through a logical evidence file. When the desired files are blue checked in the table, right clicking anywhere in the Tree Pane will show the option to **Create Logical Evidence File....** An options screen appears, similar to that which appears when acquiring a device. You can add the files to a pre-existing logical evidence file by checking the box next to the **Add to existing Logical Evidence File** options and selecting the path and file name in the **Output Path** field. The **Lock file when completed** option allows the new logical evidence file to be locked so that it can not be appended.

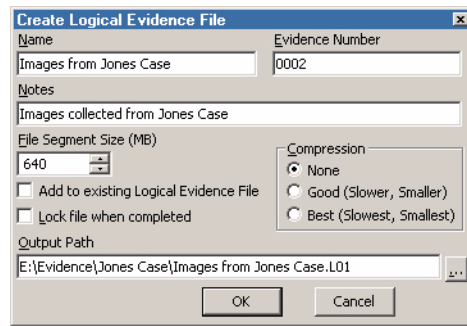


Figure 15-38: Creating a logical evidence file

Logical Evidence Files (.L01) can contain Single Files, files from a previewed device, files from evidence files, or a combination of these.

Interface

With the introduction of Version 5, the interface is more powerful and versatile than before. Tabs and menus that appeared in the separate panes previously are now categorized in the View menu by the pane in which they appear. These tabs also have subtabs to allow the user to see items specific to a case or device.

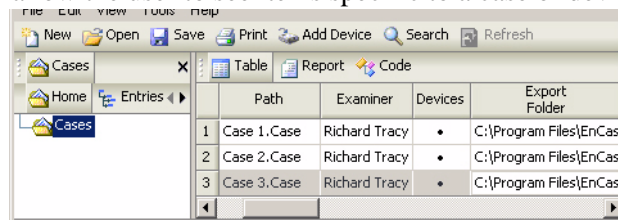


Figure 15-39: Cases tab with multiple cases

For a complete list of available tabs, click on the **View** pull-down menu (the *What's New* chapter of this manual shows all the **View** menu options). To close any of these tabs, click on the tab to select it and then click the [X] to the right, hit **[Ctrl] [F4]**, or right click on the tab and select **Close Tab**.

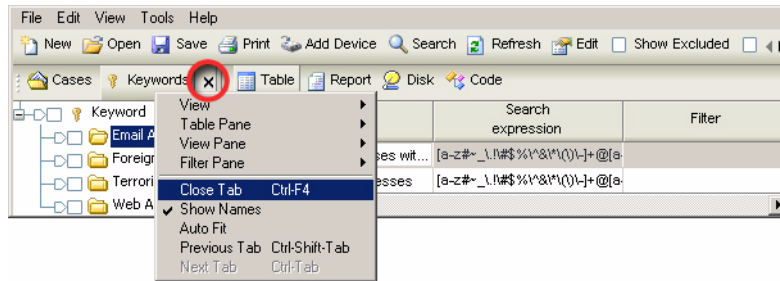


Figure 15-40: Closing a tab

Docking and Undocking

EnCase Version 5.05 allows the undocking and docking of the individual panes (Tree Pane, Text Pane, Table Pane and Filter Pane). Each of the four panes can be undocked and placed in different areas of a monitor. This feature may be particularly convenient when using running split monitors.

Undocking

In the figure below, note that there is a navigation box in the upper left corner of each pane. Take particular notice of the four vertical dots on the left side of each button.

- Click on a button. The associated pane is highlighted and becomes “disconnected” from the main display.

Figure 15-41: Tree Pane Selected for Moving

- You can reposition the undocked pane by left-clicking in the title bar of the pane, holding the mouse button down and dragging the pane to the desired location
- Each pane undocked is independent of the others and can be sized, moved, scrolled and manipulated individually.

Docking

Docking is accomplished as follows:

- Locate the original pane
- From the **View** pull-down menu, select **Reset View**, as shown below:

Figure 15-42: Docking Menu Selection

All undocked menus will be restored to their location when the case was initially opened.

EnCase Views

The Set Include Option Button



The **Set Include Option** (often called the “home plate”) is the polygon next to a tree that turns green when clicked. A representation of the option button appears at the top of this paragraph and in Figure 15-43. It displays, in the selected view on the right, *all* of the files within the parent and *all* subfolders of the selected media or folder from the left. The **Set Include** button can be activated in tabs (**Cases**, **Bookmarks**, **Devices**, etc.) and views (**Table**, **Gallery**, **Timeline** and **Report**).

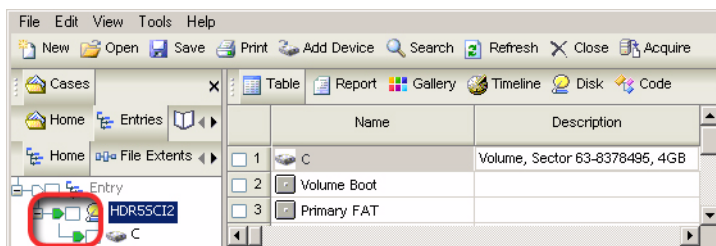


Figure 15-43: Set Option Button

A user can select the **Set Include** button at the parent folder level, then [Ctrl] click on a subfolder to deselect only that folder.

The Cases Tab

Cases is the default view in EnCase. If it is not visible, select it from the **View** pull-down menu. The data available in the **Cases** tab is accessed through the subtabs as follows

- **Home subtab**

Home displays all cases open within a single instance of EnCase. Table entries for this subtab include the case Name, Path, and the number of devices, entries,

bookmarks, search hits, secure storage items, and identified E-mail, History and Web Cache artifacts in the case.

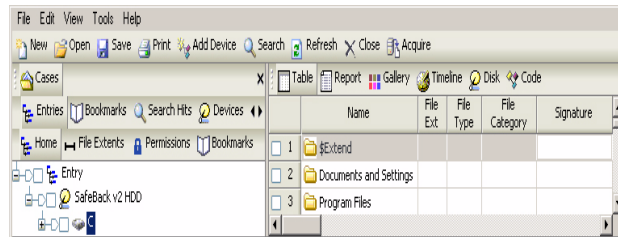


Figure 15-44: Home subtab (Cases)

• **Entries subtab**

The **Entries** subtab, new to version 5, displays (using an interface similar to Windows Explorer) all the evidence files, folders and files associated with the case highlighted in the Home subtab. In **Entries**, you can access **Table**, **Report**, **Gallery**, **Timeline**, **Disk** or **Code** views in the right pane (each described below). You can also Copy/Unerase highlighted files to your hard drive, bookmark highlighted files, or examine file with a specified viewer. As mentioned previously, if you click on the **Set Include** trigger for a folder, you will see *all* files in that folder and subfolders. Files highlighted in the right pane are represented in the bottom pane in the mode of the selected tab (**Text**, **Hex**, **Picture**, etc.). Table entries for this subtab include: **Name**; **File Extension**; **File Type**; **File Category**; **Signature**; **Description**; deletion status; **Last Accessed**, **File Created**, **Last Written**, **Last Modified**, **File Deleted** and **File Acquired** dates and times; logical and physical sizes; starting and file extents; **Permissions**; **References**; **Physical Location** and **Sector**; **Evidence File**; **File Identifier**; **Hash Value**, **Hash Set** and **Hash Category**; **Full Path**; **Short Name**; **Unique Name**; **Original Path**; and, **Symbolic Link**. The **Entries** subtab also has its' own subtabs to isolate entries into groups by **File Extents**, **Permissions** and **Bookmarks**.

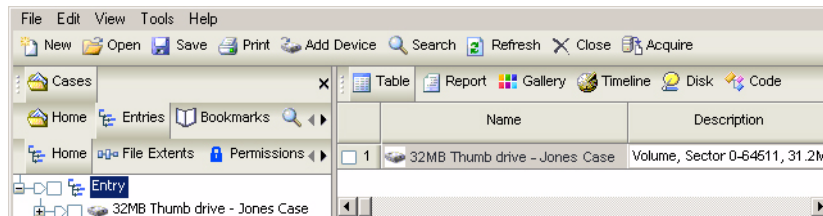


Figure 15-45: Entries subtab (Cases)

• Bookmarks subtab

Formerly a separate tab, **Bookmarks** is now a subtab under **Cases**. The **Bookmarks** subtab contains items that have been marked as files of interest. Bookmarks can be files, images, text fragments, and more (see the *Bookmarks* chapter of this document for further details.) Bookmarked items are placed within folders specified by the investigator. *Bookmarks* can display bookmarks in *Table*, *Report*, *Gallery* (for bookmarked images), *Disk* or *Timeline* views in the Table (right) pane. All bookmarks can be displayed by using the trigger.

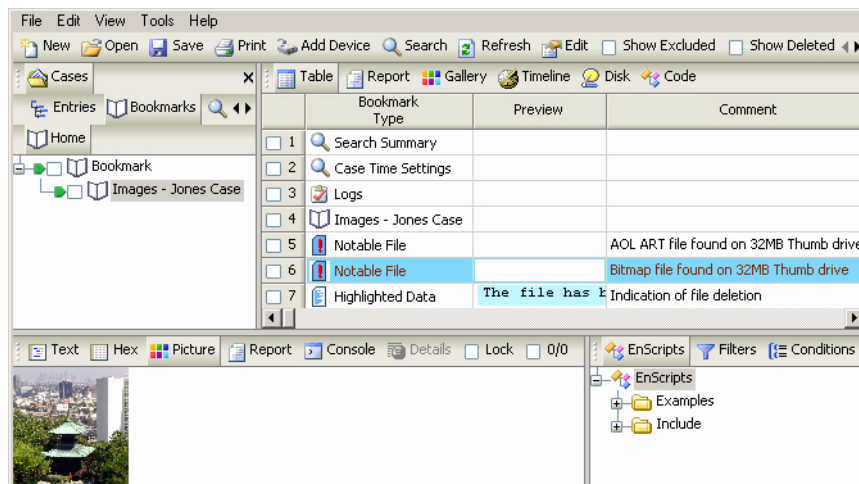


Figure 15-46: Bookmarks subtab (Cases)

• **Search Hits subtab**

Search hits generated from keyword searches are placed in the **Search Hits** subtab. Search Hits are covered in detail in the chapter of this document titled *Keyword Searches*.

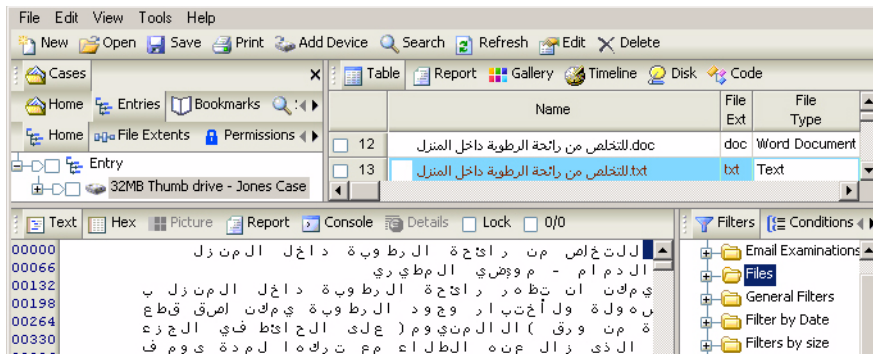


Figure 15-47: Search Hits subtab (Cases)

• **Devices subtab**

Devices is also now a **Cases** subtab, displaying information about the media in a case such as acquisitions notes, the examiner’s name, the acquisition, verification hash values, and more. Disk configurations can also be edited from this tab (see *Chapter 10* for details.)

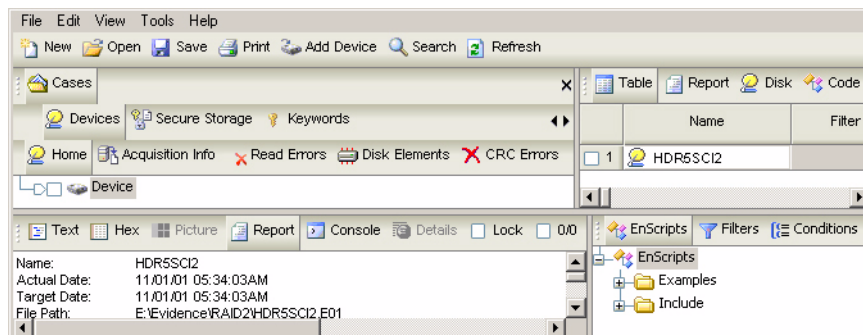


Figure 15-48: Devices subtab (Cases)

• **Secure Storage subtab**

Files and security data encrypted via EFS can be parsed from the registry; this requires the use of the EnCase Decryption Suite module (the EDS Cert must be present in the C:\Program Files\EnCase5\Certs directory). The Secure Storage tab, which appears whether or not the module is loaded, can

be populated by right-clicking on a device and selecting **Analyze EFS...**, or opening the Secure Storage subtab below Cases, right-clicking on the Secure Storage root folder and selecting **Analyze EFS...** (this will scan all devices in the case). Passwords, keys, etc. are then displayed in plain text in the table. Refer to the *EnCase Decryption Suite Manual* for additional information.

- **Email subtab**

The **Email** subtab allows the user to parse, analyze, and display various types of E-mail formats such as Outlook, Outlook Express, and web-based E-mail accounts. In addition to being displayed in normal file structure format in **Entries**, mounted E-mail files are displayed in restructured format in the **Email** tab. **Email** has its' own sub-tabs:

- **Home subtab**

Displays all E-mail entries

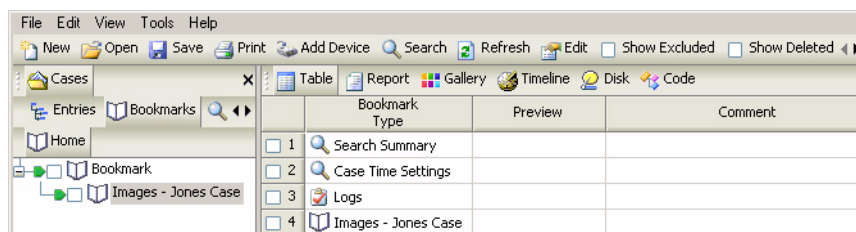


Figure 15-49: Home subtab under Email (Cases)

- **Attachments subtab**

Displays the attachments associated with the selected E-mail entry.

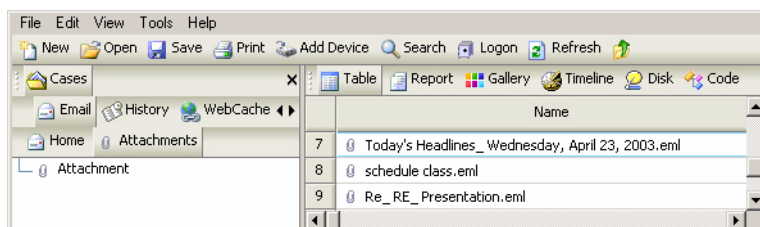


Figure 15-50: Attachments subtab under Email (Cases)

Email entries can be sorted by Device, Folder, or Email Type in a manner similar to that of Search Hits. See the *E-Mail and Internet Artifacts* chapter of this document for additional information.

• **History and WebCache subtabs**

Users can now parse, analyze, and display various types of Internet and Windows history artifacts logged when web sites or file directories are accessed through supported browsers, include; Internet Explorer, Mozilla, Opera, and Safari. The History tab allows users to search for various history attributes and organize them all in one table. See the *E-Mail and Internet Artifacts* chapter of this document for additional information.

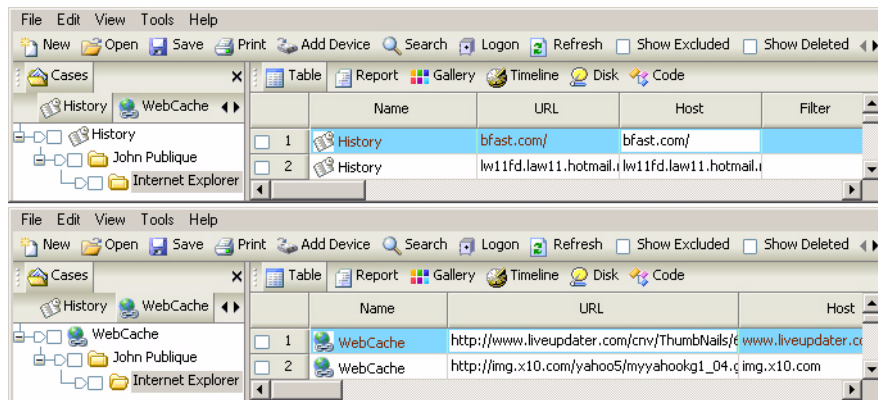


Figure 15-51: History and WebCache subtabs (Cases)

File Types

To access the **File Types** tab, select **File Types** from the **View** pull-down menu. This tab contains information on all file types and their associated viewers. EnCase allows the user to review, add, edit, or delete file types and to match file types to viewers. While EnCase has many file types already matched to specific applications for proper file access, it also provide a means to add viewers for file types that are

new or unrecognized by EnCase. **File Types** are covered in full in the chapter on *Viewing Files*.

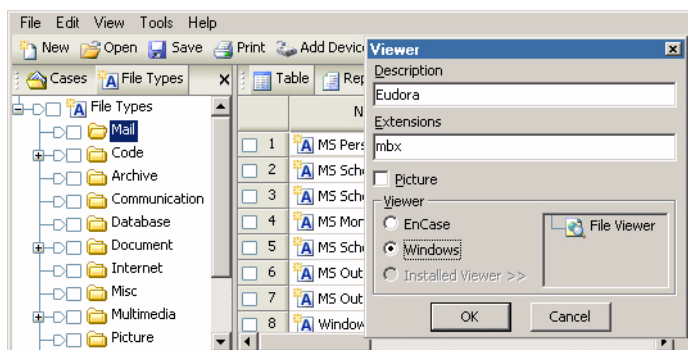


Figure 15-52: File Types tab

File Signatures

The *File Signatures* tab is accessed by selecting **File Signatures** from the **View** pull-down menu. File Signatures are the unique hex signature headers associated with specific file types. For example, an industry-standard JPG image must begin with the hex header signature `\xFF\xD8\xFF [\xFE\xE0] \x00`. From this tab, file signatures can be reviewed, added, edited, and deleted.

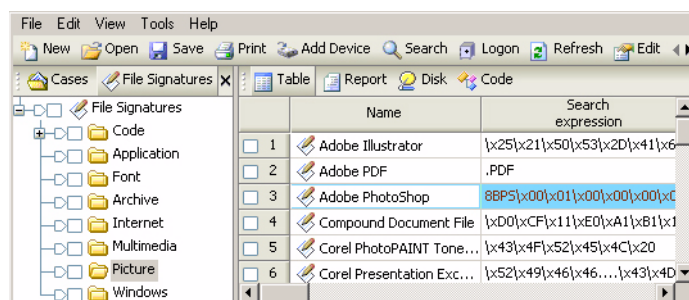


Figure 15-53: File Signatures tab

File Viewers

To access the *File Viewers* tab, select **File Viewers** from the **View** pull-down menu. File Viewers are applications that can be configured in EnCase in **File Types** to associate file types and viewers. By default, EnCase can view different file types, such as JPG or TXT, but some files types cannot be displayed natively by EnCase.

From this tab, file viewers are added, edited, and deleted. File Viewers are covered in full in the *Viewing Files* chapter of this document.

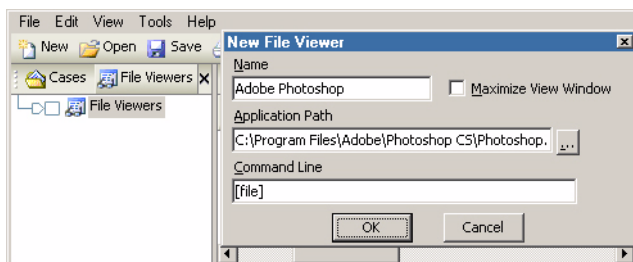


Figure 15-54: File Viewers tab

Keywords

The *Keywords* tab is accessed by selecting **Keywords** from the **View** pull-down menu. Keywords are terms used to search evidence files. They can be words, phrases, or hex strings. Keywords can be entered as case-sensitive, in GREP, in Unicode, UTF7 and UTF8, etc.

Keywords are saved in an initialization file (`keywords.ini`) in the `C:\Program Files\EnCase5\Config` directory. Keyword searches are performed at both a logical and physical level, meaning that EnCase can search for each term byte-by-byte from the beginning to the end of every medium, and also search every logical file for the term as well. Keywords are covered in detail in the *Keyword Searches* chapter of this document.

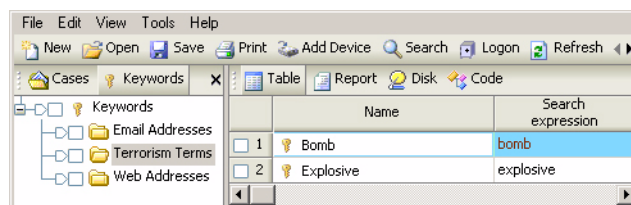


Figure 15-55: Keywords tab

Security IDs

Every file and folder on an NTFS file system has an owner, a group, and a set of permissions. While this information is stored differently in NTFS 4 and NTFS 5, EnCase extracts the security information for each file and folder. EnCase extracts the owner, group and permission settings (organized by owner or group) on Windows, Unix and Linux systems. The *Security IDs* tab allows the user to input Security IDs

for a particular piece of evidence to be used in examination. This tab is accessed by selecting **Security IDs** from the **View** pull-down menu.

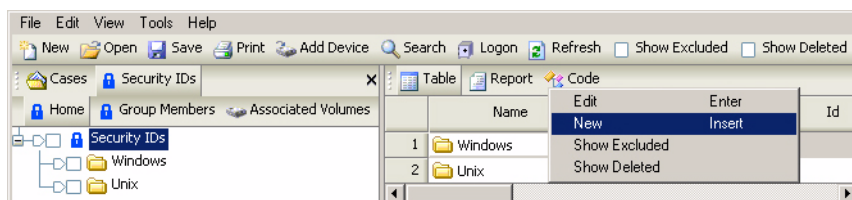


Figure 15-56: Security IDs tab

Below is a typical listing of NTFS file permissions, from the Administrator user folder C:\Documents and Settings\Administrator:

Permissions

NAME:BOB HUNTER

ID: S-1-5-21-1229272821-1580818891-854245398-1004

PROPERTY:ALLOW

PERMISSIONS:[FC] [M] [R&X] [R] [W] [SYNC]

ID:S-1-5-18

PROPERTY:ALLOW

PERMISSIONS:[FC] [M] [R&X] [R] [W] [SYNC]

NAME:ADMINISTRATORS

ID:S-1-5-32-544

PROPERTY:ALLOW

PERMISSIONS:[FC] [M] [R&X] [R] [W] [SYNC]

NAME:BOB HUNTER

ID: S-1-5-21-1229272821-1580818891-854245398-1004

PROPERTY:OWNER

Below is a typical listing of Unix file permissions, from the `.bash_profile` file under admin:

Permissions

Owner:500

Group:500

Permissions Allowed:Owner Read

Permissions Allowed:Owner Write

Permissions Allowed:Group Read

Permissions Allowed:Other Read

Notice that users and groups are displayed by a numbering system. The number is the Security Identifier, or SID. Every user, group, and machine has a unique SID in an NT network. For example, if Trevor Martin is a user on a Windows 2000 system, Trevor will have a Security ID number that matches to his name. Windows 2000 stores this information in the registry, and EnCase automatically displays his name in the Report tab in association with his SID.

However, if a new user, John Hopkins, logs onto the system who is *not* stored locally on the Windows 2000 system (but is on the network file-server, thus allowing him to log onto this client system), there will be no Security ID number correlated with John Hopkins. EnCase would be unable to associate John with a security ID number—John's Security ID number is on the network file-server, not the local machine. Unix User and Group IDs are not unique, and are not automatically associated with names either.

The solution is to preview or image the network file-server in addition to the client machine and retrieve all user Security IDs via the server. Those Security IDs can then be entered into EnCase under the Security IDs tab, and John's username would then be associated with his Security ID number. Windows 2000 SID information can be extracted and exported using EnScripts such as the **Active Directory Information Extractor** and the **Initialize Case** script.

Three folders are created by default in the Security IDs tab: **Windows**, **Nix** (for **Unix** and **Linux** IDs) and **Security IDs**. The folders are there to encourage organization, but each folder can contain any type of ID.

To create a new Security ID (SID), right click on the desired folder and select **New...** A dialog box will pop up with fields for **Name**, **Id**, **Group**, **Unix**, and **Group Members**.

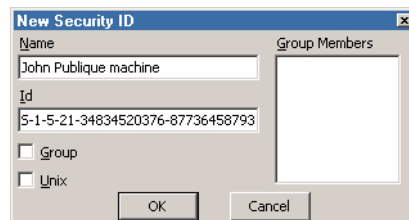


Figure 15-57: Creating a new Security ID

An explanation of the fields follows:

- **N**ame

The **N**ame field contains the name that will be resolved when the associated SID is found.

- **I**d

This field allows the entry of the Security ID (SID) that the user wishes to resolve. The Windows SID is in the form “S-x-x-x[-x-x-x-x]”. A Nix (Linux\Unix) SID is an integer such as 1000.

- **G**roup

The **G**roup checkbox must be selected if the SID pertains to Nix and represents a group. Nix IDs are not unique, and User IDs may overlap with Group IDs.

- **U**nix

This radio button must be selected if the SID being defined is for a Nix system.

- **G**roup Members

The **G**roup Members field is optional; it may be defined to aid in organization (mainly for Nix). Right-click and select **New...** in the **G**roup Members box to assign a member to the current Security ID.

It is recommended to create a new folder to contain the settings for each volume in a case, as SID settings are assigned to volumes at the folder level. Right-click on a folder in the Security IDs view and select **Associate Volumes...** to associate the Security IDs in the selected folder with currently open volumes. Select the volumes to which you wish to apply the settings, and click **[OK]**. The volumes that a particular folder is applied to are displayed in the **Associated Volumes** column of the **Security ID** table.



Figure 15-58: Associating Volumes

Text Styles

To access the **Text Styles** tab, select **Text Styles** from the **View** pull-down menu. Text Styles are used to view Code Pages correctly and with different settings, such as changes in color and text line length. EnCase has multiple default text styles, but styles can be added, edited, and deleted from this tab by either right-clicking and

selecting the command from the menu or clicking the second **New** button in the tool-bar. Text Styles are covered in full in the chapter on *Foreign Language Support*.

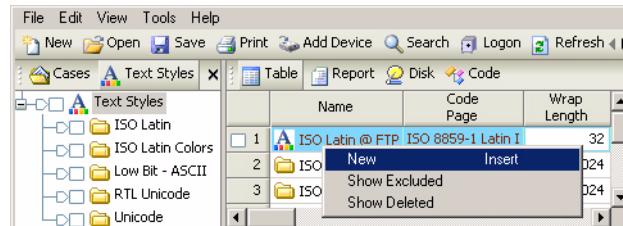


Figure 15-59: Viewing Text Style

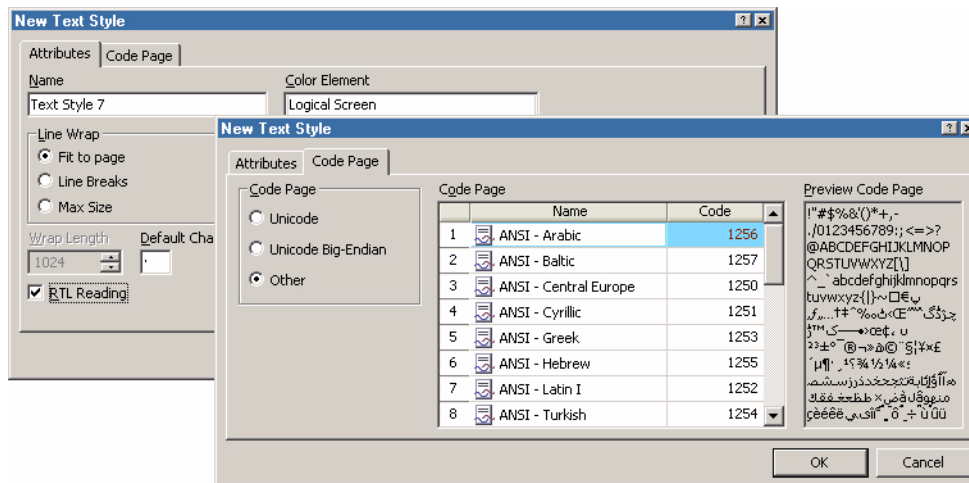


Figure 15-60: Adding new text style

EnScripts

The **EnScripts** tab is accessed by selecting **Scripts** from the **View** pull-down menu, as well as in the Filter Pane. The **EnScripts** tab is where EnScripts are reviewed and coded. EnScripts are small programs or macros that are designed to automate forensic procedures. EnScripts can access and manipulate many areas of the EnCase interface, from searching to creating bookmarks to putting information into the

report. EnScripts can be added, edited, and deleted from the Scripts tab. EnScripts are covered in detail in the chapter on *EnScript and Filters*.

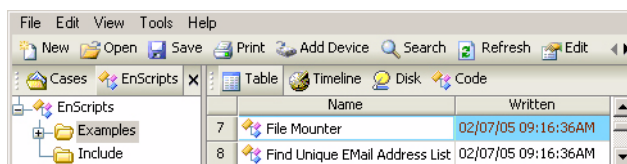


Figure 15-61: EnScripts tab

Hash Sets

To access the *Hash Sets* tab, select **Hash Sets** from the **View** pull-down menu. Hash Sets are a collection of hash values of files belonging to the same application. For example, if the `c:\Windows` folder is hashed on a clean system, the resulting collection of hash values could be labeled “Windows 98 Hash Set”. The Hash Sets tab is where Hash Sets can be edited, deleted, and imported.

A Hash Library is a collection of hash sets.

All hash functionality, editing, deleting, and importing, is accessible by right clicking and selecting the appropriate menu command. Hash Sets are explained in detail in the *First Steps* chapter of this document.

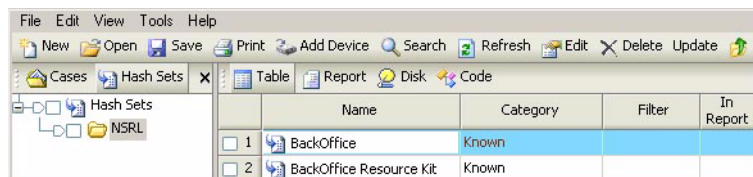


Figure 15-62: Hash Sets tab

EnScript Types

The *EnScript Types* tab is accessed by selecting **EnScript Types** from the **View** pull-down menu. The *EnScript Types* tab is a reference resource that contains the classes

of the EnScript language. The right-pane shows the parameter of each function in order.

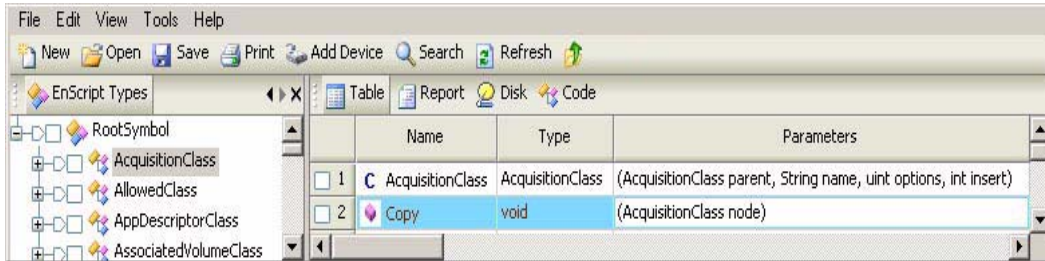


Figure 15-63: EnScript Types tab

Table Pane \ View

The Table view in the Table Pane (upper left) displays all objects in a selected container (folder, device, etc.) and their attributes. The investigator can sort the display by double clicking on the header bar over any of the columns in the table. To sort by up to five columns (sub-sort), hold down the **[Shift]** key and double-click another column header. The first sort is indicated by a red triangle in the header; each subsequent sort will have an additional triangle in the header. As described previously in this document, turning on the **Set Include** trigger (clicking on it until it turns green) will recursively show all objects in each subfolder.

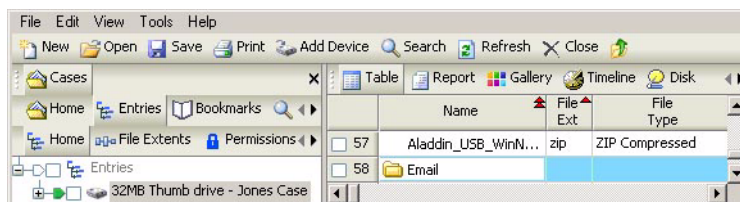


Figure 15-64: Table view with sort (File Ext) and Subsort (Name)

Common commands that can be executed in the **Table** view are Copying/UnErasing; bookmarking highlighted or selected (blue-checked) files; exporting the table;

viewing file structure of compound files; or sending a file to a specified viewer (see the chapter in this document on *Viewing Files*).

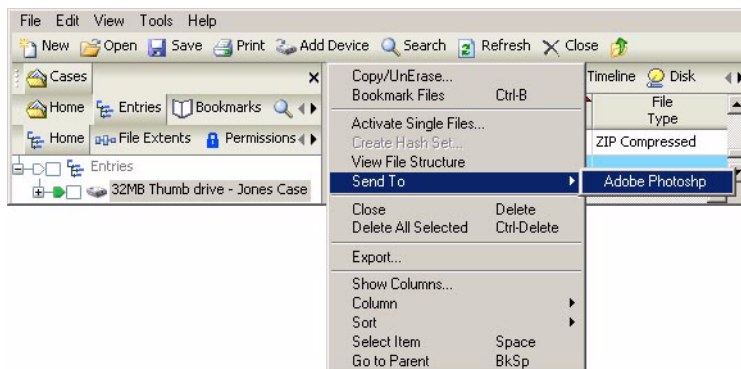


Figure 15-65: Table view commands

Table View Columns Explained

Table columns can be activated (shown) or deactivated (hidden) by right-clicking in the table, selecting **Show Columns...** and making sure the desired columns are blue checked. By default, the **Filter** and **In Report** columns are deactivated. The column descriptions follow:

- **Name**

Name identifies the file/folder/volume, etc. in the evidence file by name. Icons to the left of the filename indicate the status of the file (see the next section for an explanation of the icons).

- **Filter**

The **Filter** column displays the name of the saved filter options if the files meet the criteria set. For instance, if files are filtered using options saved with the name “**all JPG images**”, files in Table view matching the criteria would display [**all JPG images**] in this column.

- **In Report**

The **In Report** column indicates whether or not the item will appear in the report. By default, items in the table do not appear in the report, with the item having a **False** Boolean value (indicated, by default, as a blank entry). To change the value to **True**, blue check the item, click on the entry in the **In Report** column, and hit [Ctrl] [R], or right-click and select **In Report**. By default, a value of **True** is indicated by a bullet in the column, but both the **True** and **False** indicators can be changed from the **Global** tab in the **Options** settings

in the **Tools** pull-down menu. To have multiple files show in the report, blue-check all desired files, then right-click on the **In Report** header and select **In Report – Invert Selected Items** (in any of the selected files already have a *True* value, they will be set to *False*). To include selected files at all levels in the report, use the green **Set Include** button on a parent folder; all files in subfolders with the *True* In Report value will show in the report. This feature is used to assist in making quick reports without bookmarking, if desired.

- **File Ext**

The **File Ext** column displays the file's extension. Windows uses the file extension to determine which application opens the file. If a file has been renamed with a different extension type (for example, a JPEG image (.JPG) being renamed to look like an Excel spreadsheet (.XLS)), this column would report the extension given by the user, not the file type's true extension. The file header information is still intact; therefore, a signature mismatch will be reported if and when you ran a **Signature Analysis**.

- **File Type**

This column indicates type of file. EnCase generates this information from the **File Types** table (viewed by accessing the **File Types** option in the **View** pull-down menu) using the file's extension. After a **Signature Analysis** is run, the information will be generated from the file's signature.

- **File Category**

The **File Category** column indicates the category of the file assigned to the file type in the **File Types** EnCase window. For example, files with an **AI** extension would fall under the *Pictures* category, since the extension indicates an Adobe Illustrator file, found in the *Pictures* folder within the *File Types* table.

- **Signature**

The **Signature** column identifies the file by the header, not file extension. If the header and file extension do not match after a signature analysis is run, you will see a “*!Bad Signature*” message in this column. The **Signature** column is only be populated after a signature analysis is run. Signature Analysis results are explained in *Chapter 13*.

- **Description**

The **Description** column gives a short description or explanation of what the icon to the left of the file name is. For a full explanation of those icons, see the next section.

- **Is Deleted**

A TRUE Boolean value displays in this column if this file has been deleted and *not* emptied from the Recycle Bin.

- **Last Accessed**

Last Accessed column displays a date of the last access date of the file. A file does not have to be *altered* for the last accessed date to change—only accessed. Any activity (such as viewing, dragging, or even right-clicking) may change the last accessed date. The last accessed date may also change if the file is accessed by a program such as a virus checker.

- **File Created**

The **File Created** column is a record of when a particular file was created *at that location*. If a file is edited and changed on January 3rd, then *copied* to a floppy diskette on January 15th, and then that floppy diskette is acquired on January 28th, EnCase would show that the file (on the floppy) was created *after* it was last written or even accessed.

- **Last Written**

The **Last Written** column displays the last date and time that a file was actually opened, edited, and then saved. If a file is opened then closed, but not altered, the last written date and time do not change.

- **Entry Modified**

The **Entry Modified** column, pertinent to NTFS (Windows NT, Windows 2000, Windows XP, and Windows 2003 Server) and Linux file-system files, refers to the pointer for the file-entry and the information that the pointer contains, such as the size of the file. If a file was changed but its size not altered, then the **Entry Modified** column would NOT change. However, if the file *size* has changed (from eight sectors to ten sectors, for example), then this column would change.

- **File Deleted**

If an entry in an INFO2 file on an NTFS volume has a deleted date, the time and date of deletion will appear in this column. A TRUE Boolean value will also appear in the **Is Deleted** column.

- **File Acquired**

This field displays the date and time the evidence file the file resides in was acquired.

- **Logical Size**

The logical size of a file is how large the file is in terms of bytes, for example 7,551 bytes.

- **Physical Size**

Physical size is the cluster size of the file. Clusters in Windows 98 SE, for example, are 4096 bytes, so the physical size of any file with a logical size less than 4096 bytes will always have a physical size of 4096 bytes. Files are stored in increments of that unit. (For example, the 7,551 byte logical file occupies 8,192 bytes of physical disk space. The 641 byte difference is called *slack space*.)

- **Starting Extent**

The **Starting Extent** column contains the starting cluster of every file in the case. The format displayed is evidence file number, logical drive letter, followed by the cluster number. For example, a starting extent of 1D224803 means that the file is on the second evidence file (counting begins at zero, remember), on the logical D drive of the evidence file, at the 224,803rd cluster.

- **File Extents**

This column lists the number of extents (data runs) of the file that are fragmented on the drive. To view the extents, click on the column value for the file to be examined, and then select the **Details** tab in the bottom pane. Alternately, you can select the file in the **Entries** table, then select the **File Extents** subtab, which displays the file extent data in the table. When EnCase uncompresses a file, the uncompressed data is displayed in **Text** and **Hex** views, and the raw data is displayed in the **Disk** view. To reconcile the

difference between the physical location of the compressed and uncompressed data, EnCase will place *'Sparse'* entries in the File Extents column.

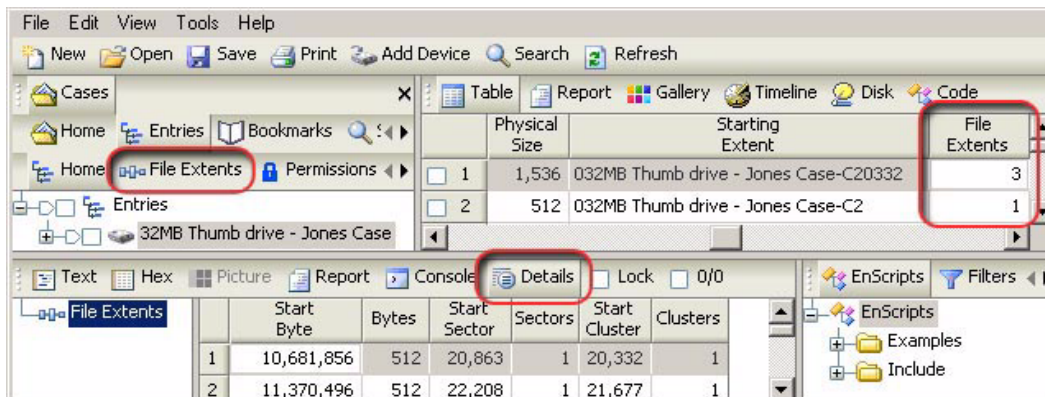


Figure 15-66: File Extents

• Permissions

The **Permissions** column displays security settings of a file or folder. A dot indicates that a security setting is applied. Security settings are viewed by selecting the entry and clicking on the **Details** tab in the lower pane. Alternately, you can select the file in the **Entries** table, then select the **Permissions** subtab, which displays the permissions in the table.

• Details Tab

Information displayed within this tab includes:

- **Name**

Displays names associated with the ID. **Permissions** is the default (no name is associated with the selection). Names are associated from within the evidence (local accounts and built-in) or by associating a volume with a set of ID/name pairs from the **Security ID** pane.

- **Filter**

Functions the same as the **Filter** column as described in Table view.

- **In Report**

Functions the same as the **In Report** column described in Table view

- **ID**

This column displays the ID related to the permission, either as a regular number (Unix), or in S-x-x... format (Windows). In Windows, each permission has an associated ID; in Unix, only rows that specify **Owner** and **Group** have an associated ID.

- **Property**

This column shows the significance of each particular row in the table (for instance, **Allow**, **Deny**, **Owner** or **Group**)

- **Permissions**

Extracted permissions specific to the highlighted item are listed here.

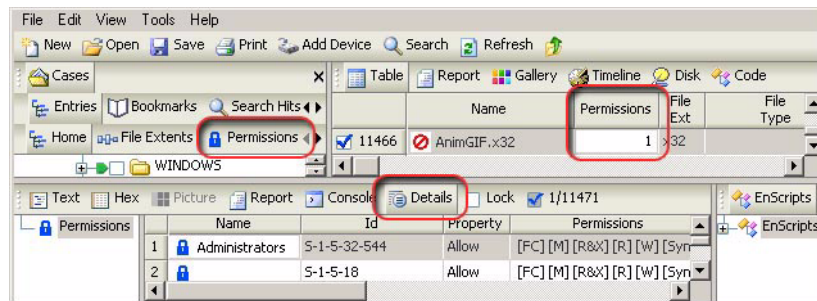


Figure 15-67: Permissions Column window

Each permission is enclosed in brackets (Ⓛ); a key to the permission definitions follows:

The permissions for the Unix environment are:

- G-R** Generic read
- G-W** Generic write
- G-X** Generic execute

The permissions for the Windows environment are:

- Obj In ACE** Object Inherit ACE
- Cont In ACE** Container Inherit ACE
- No Prop In ACE** No Propagate Inherit ACE
- In Only ACE** Inherit only ACE
- FC** Full Control
- M** Modify
- R&X** Read and Execute
- R** Read
- W** Write
- Delete** Delete
- R Attr** Read Attributes
- D Sbfl dr & FI** Delete Subfolders and Files
- Trav Fl dr/X FI** Traverse Folder/Execute File
- W EA** Write Extended Attributes

R EA	Read Extended Attributes
Crt Fldr/App Data	Create Folders/Append Data
Crt FI/W Data	Create Files/Write Data
Lst Fldr/Rd Data	List Folder/Read Data
W Attr	Write Attributes
Sync	Sync
Tk Own	Take Ownership
Chg Perm	Change Permissions
R Perm	Read Permissions
G-R	Generic R
G-W	Generic W
G-X	Generic X
G-All	Generic All
ACL Access	SACL Access

• References

The **References** column lists the number of times the selected file is referenced (such as being bookmarked). If a file has an entry in the **References** column, and the file is highlighted in that column, a **Details** tab appears in the bottom pane, where you can view the type of bookmark made, the folder location, bookmark comments, and a preview of the swept text in Highlighted Data bookmarks. Alternately, you can select the file in the **Entries** table, then select the **Bookmarks** subtab, which displays the file extent data in the **References** subtab table. Double-clicking on the bookmark in the **Details** view will take you to item in **Bookmarks** view.

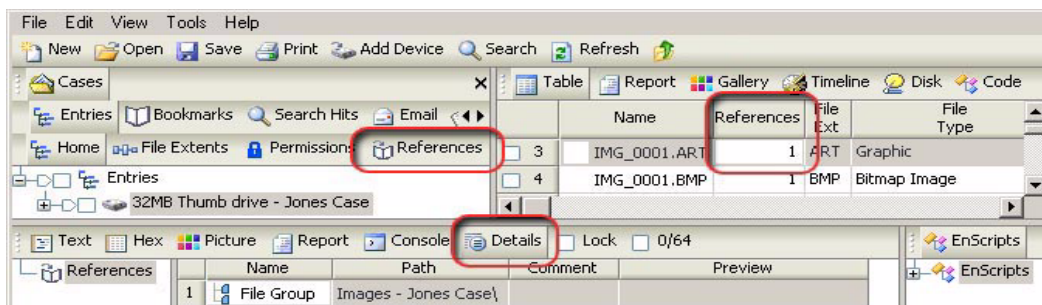


Figure 15-68: Bookmarks Column window

- **Physical Location**

EnCase organizes the Unallocated Clusters (UC) of a device into one virtual file. It reads the FAT (File Allocation Table) of the file system, or the \$Bitmap in NTFS to create this virtual file. This allows the examiner to examine all of the UC very efficiently with keyword searches and EnScripts. **Physical Location** is the number of bytes into the device at which that the UC begins.

- **Physical Sector**

The **Physical Sector** column lists the starting sector where the item resides in Unallocated Space, based on an algorithm applied to the data in the **Physical Location** column. This coincides with the Start Sector in the Details tab when viewing the File Extents in the table. This feature was added in version 4.20.

- **Evidence File**

The **Evidence File** column displays which evidence file the file resides in.

- **File Identifier**

The **File Identifier** is a file table index number, stored in the Master File Table. It is a unique number allocated to file/folders in an NTFS file system.

- **Hash Value**

The **Hash Value** column displays the hash value of every file in the case. The **Compute Hash Value** command must be run to generate this information.

- **Hash Set**

The **Hash Set** column displays the hash set to which a file belongs. If no hash sets have been created or imported, this column will be unpopulated.

- **Hash Category**

The **Hash Category** column displays the hash category to which a file belongs. If you have not created or imported any hash sets, then this column will either be unpopulated, or display both *Known* and *Notable*.

- **Full Path**

The **Full Path** column displays the location the file is located within the evidence file. It includes the evidence file name in the path.

- **Short Name**

The **Short Name** is name that Windows gives the file using the DOS “8.3” naming convention. For example, a file with the file name “onethousanddollarbill.jpg” would appear in this column as “onetho~1.jpg”.

- **Unique Name**

This column is used to display the name for files mounted with the EnCase Virtual File System (VFS) Module in Windows Explorer. For more information about the EnCase VFS Module, please refer to the VFS user manual available from www.guidancesoftware.com/support/downloads.asp.

- **Original Path**

The **Original Path** column displays information derived from the INFO2 file on deleted files sitting in the Recycle Bin; specifically, where the deleted file originally came from.

- For allocated (not deleted) files, the column is blank
- For files within the Recycle Bin, this column shows where they originated from before they were deleted
- For deleted/overwritten files, this column shows what file has overwritten the original

- **Symbolic Link**

In Unix-based file systems (including AIX), symbolic, or soft links are files, similar to Windows .LNK shortcut files, that point to other files. Symbolic links do not contain the data found in the target file, but can provide links to directories, or files on remote devices.

Organizing Columns

Rearranging Columns

Table columns can be arranged in any order. Use the horizontal scrollbar or the right arrow to maneuver to the desired column, left click on the header of the column and hold the button, and drag the column to the desired position. To reset the column

arrangement to the default setting, right click anywhere in the table, and select the **Reset** option under **Column**.

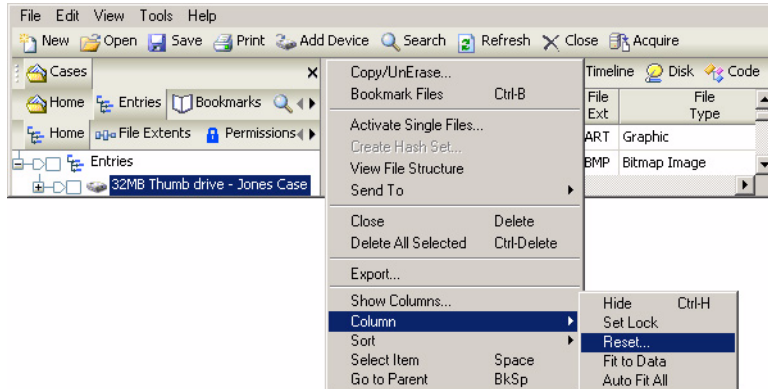


Figure 15-69: Resetting Columns

Hiding and Showing Columns

With over twenty columns in Table view, scrolling through unused columns may be time-consuming. You can select which columns you wish to display as follows:

- Right-click anywhere in the table and select **Show Columns...**
- Blue-check only the columns you wish to display, and then click [OK].

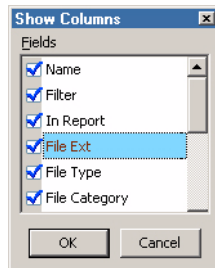


Figure 15-70: Setting columns

Sorting Files in Columns

Sorting files in columns quickly finds specific files or bookmarks. If, for example, an investigator wanted to view only JPEG files within a case, they can sort on the **File Ext** column then scroll to the JPG files section, as all JPEG files are sorted together. Alternatively, a JPG filter could also be used. EnCase employs “intellitype” functionality to allow you to click anywhere in a column, type the letters of the entry you wish to search for, and the cursor will jump to the desired entry. For instance,

if you are looking for JPEG files, click anywhere in the **File Ext** column and quickly type the letters J, P and G; you will be taken to the first entry with a .JPG extension. In version 4.18, typing [J] [P] would take you first to the first item beginning with “J”, then to the first item beginning with “P”. This was improved to allow multiple characters. The timeout is approximately 200 milliseconds between keystrokes, so an intentional pause in the keystrokes will take the selection to the beginning of the entries matching the last typed character.

Sorts and sub-sorts are possible up to five layers deep. Hold the [**Shift**] key and double-click the header of each column you want to sort by in the order of importance. To sort a column in the opposite order of the default, hold the [**Ctrl**] key while you click. Sorts and sub-sorts are also possible in the **Search Hits** and **Bookmarks** tables. For example, if a signature and hash analysis has been run, you can sort first by **File Ext**, then by **Hash Set**, and finally by **Name** in order to quickly find all the JPG files and compare them to Hash Sets in the library.

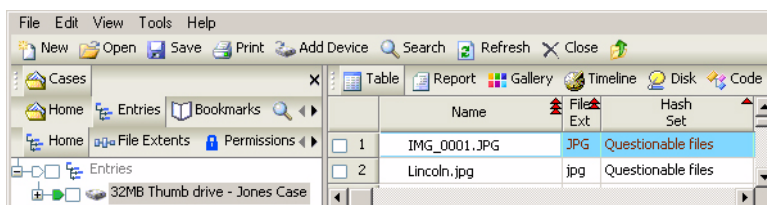


Figure 15-71: Sort by File Ext, Hash Set, then Name

EnCase Icon Descriptions

This section contains a detailed description of the icons used in EnCase. In Table view, the icon to the left of the file name typically describes the file’s status.



New: On the top toolbar, this icon opens a new case.

















Open: On the top toolbar, this icon opens an existing case.

















Save: On the top toolbar, this icon saves the open case.



Print: On the top toolbar, this icon prints the open EnCase window.

- 
Add Device: On the top toolbar, this icon allows live or saved evidence to be added to a case.
- 
Search: On the top toolbar, this icon starts a search.
- 
Refresh: On the top toolbar, this icon refreshes the EnCase window.
- 
View Cache, View Search Hits, etc.: On the top toolbar, this blue flag enables activities such as *Cache*, *Search Hits*, etc.
- 
Delete / Close: On the top toolbar, this icon allows for the deletion of selected items.
- 
Acquire: On the top toolbar, this icon appears after a device is previewed or an evidence file is opened, allowing acquisition.
- 
Cases (Cases\Home): This icon appears on the *Cases* tab, and in the *Cases/Home* subtab.
- 
Entries: This icon is displayed in the *Entries* subtab beneath *Cases* and in the *Home* subtab beneath *Entries*.
- 
Single Files: This icon appears when selecting the **Activate Single Files** option when right clicking on a device or volume in the *Entries* subtab
- 
Devices (Devices\Home): A physical hard drive icon. This icon does not represent a volume or logical device, such as a partition. A pink square overlay appears around the icon a preview network connection is dropped. It appears throughout EnCase, and in the *Devices* and *Devices/Home* subtab beneath *Cases*.
- 
Secure Storage: This subtab, beneath *Cases*, allows users to parse evidence files for EFS-encrypted items in conjunction with the EnCase EDS module
- 
Email: This subtab, beneath *Cases*, shows E-mail artifacts found in the case. The *Home* subtab, and *Email* folder in the Tree Pane also display the same icon.
- 
Back: This icon takes the user back up one level when drilling down to items in the table
- 
Show Excluded / Show Deleted: This box appears blank on the top tool bar in the tabs where items can be deleted or excluded (e.g., *Bookmarks*, *Keywords*, *Text Styles*, etc.) When selected, a check appears in the box, and deleted or excluded items appear in the table.

-  **Add Note:** Appears on the top toolbar while in the *Bookmarks* subtab beneath *Cases* to allow the user to add a note bookmark to appear in the report.
-  **Edit:** This icon appears on the top toolbar when the option is available (such as in the *Keywords* table)
-  **Attachments:** This subtab appears under the Email subtab and displays any attachments associated with recovered E-mail.
-  **History:** This subtab, beneath *Cases*, shows Web History artifacts found in the case. The *History* folder in the Tree Pane also display the same icon.
-  **File Extents:** This subtab, beneath *Entries*, shows file extent info when a file is selected with the information available.
-  **References / Bookmarks:** This subtab, beneath *Entries*, shows bookmark data when available on the selected file.
-  **WebCache:** This subtab, beneath *Cases*, shows Web artifacts found in the case. The *WebCache* folder in the Tree Pane also display the same icon.
-  **Network Share Device:** This icon appears when the VFS or PDE Module virtually mounts a case, device or folder.
-  **Volume / Logical Device:** Represents a volume, logical disk, and/or a partition, and appears in the left pane of the *Devices* subtab to indicate a device
-  **RAID, Dynamic Disk:** RAID disks and Dynamic Disks.
-  **Rebuilt RAID or Dynamic Disk:** RAID or Dynamic disk, successfully rebuilt within the EnCase environment. This icon also represents **Disk Elements** under the **Devices** tab.
-  **CD ROM:** Indicates a CD ROM.
-  **CD ROM session:** Indicates a session on a multi-session CD ROM.
-  **Folder:** An allocated folder (yellow).



Deleted folder: A folder that is deleted (yellow with a red X).



Deleted, Overwritten folder: A folder that is deleted and over-written by another file - gray with a red X (see Deleted, Overwritten file).



Folder, Invalid Cluster: A directory entry whose file type bit is set to “folder;” and whose starting cluster is set to zero. The icon is displayed as a pink folder.



Lost Files/Recovered Folders: Lost Files, Recovered Folders or indicates examining an NTFS or FAT drive (white folder).



Deleted file: A deleted file on the suspect’s computer that has been undefined by EnCase; nothing is changed in the evidence file.

Deleted and Overwritten file: EnCase determines that the starting cluster found in the directory entry for this file is occupied by another file and makes no further attempt to undelete this file. The name of the overwriting file is displayed in the status bar, and its contents (not that of the deleted file) displayed. Remnants of the original file may exist. Further examination should include checking the starting cluster, and the size of both files, to enable the examiner to determine if the data has been over-written. If it has not, the original file data may be on the hard drive in the slack space of the new file.



This icon also represents CRC Errors in the Devices tab.



Read Errors: Smaller than the above icon and lighter red, this icon represents Read Errors on the acquired device in the Devices tab.



Invalid Cluster: A filename entry that does not have a starting cluster number. EnCase cannot locate the file’s contents. Invalid cluster numbers are normally generated from system-deleted files, where the starting cluster number is changed to zero. This evidence indicates that the filename existed and the dates that it was created, modified, and accessed.



File, Hard Linked: A condition when multiple Names have a direct connection to the same Anode. EnCase splits the data into a file named “Hard Link Data #”. All corresponding Hard Links point to this file for the data. (for example: /bin/ls uses inode 64860; /var/ftp/bin/ls also uses inode 64860).



Internal File: A file created by file systems such as NTFS, HFS, Linux, EXT2.



Recycle Bin: The suspect’s recycle bin.



Unallocated space, MBR, unused disk area, FAT tables, VBR, Volume slack: A representation of these areas of the disk, showing that no files are currently allocated to these areas.



Text: A view of the selected file in ASCII.



Hex: A view of the selected file in Hexadecimal for each character displayed.



Picture/Gallery: Displays a picture if the selected file type is a graphic image.



Report: Displays the data that appears in the report for the selected item.



Table: When clicked in the Table pane, shows the table of items.



Timeline: When clicked in the Table Pane, displays a chart with blocks identifying times and dates associated with files



Code: When clicked in the Table Pane, displays the code for EnScripts and filters.



Console: Displays the console contents (C:\Program Files\EnCase5\console.txt); status information about the results of processes such as scripts, searches, and Recovered Folders, for example.



Filters: Displays the available filters for the current view.



Conditions: Displays the conditions to use for filtering.



Queries: Displays the available queries for the current view.



Disk: Displays the contents of the disk divided into individual sectors, which are represented as blocks.

Volume Boot	Bad Cluster	Wasted Area
FAT 1	Allocated	No Partition
FAT 2	Lost Cluster	Unknown
Root Folder	Deleted File	Volume Slack
Unallocated	Boot Sector	Disk Manager



Bookmarks: Icon for the **Bookmarks** tab and subtab.



Logs: Icon for a Log entry in **Bookmarks**.



Highlighted Data Bookmark: Created by sweeping data (clicking and dragging the mouse over data) in one of the sub-panes. This is a customizable bookmark.



Notes Bookmark: Allows the user to write additional comments into the report. It is not an evidence bookmark.



Folder Information Bookmark: Bookmarks the tree structure of a folder or device information of the selected media. The options include showing the device information, such as drive geometry, and the number of columns to use for the tree structure.



Notable File Bookmark: A file bookmarked by itself. This is a customizable bookmark.



File Group Bookmark: A bookmark that is part of a group of selected files. There is no comment on this bookmark.



Snapshot Bookmark: Contains the results of a system Snapshot of dynamic data for incident response and security auditing. This information is acquired running the *Scan Local Machine* EnScript against a preview of the local drive. This icon also appears on the *Home* subtab for *Snapshots*.



Open Files Bookmark: Subtab under *Snapshots* that contains the snapshot data on any open files on a target system.



Open Ports Bookmark: Subtab under *Snapshots* that contains the snapshot data for all open ports on a target system.



IDS Events Bookmark: Subtab under *Snapshots* that contains a snapshot of IDS events



Log Records Bookmark: Subtab under *Snapshots* that contains the results of the log parsing EnScript.



Processes Bookmark: Subtab under *Snapshots* that contains the snapshot data about all processes running on a target system.



Network Interfaces Bookmark: Subtab under *Snapshots* that contains the snapshot configuration of any of the network interfaces on a target system.



Network Users Bookmark / User: Icon appears in the subtab under *Snapshots* that contains the snapshot of the network users with system access, as well as anywhere EnCase Enterprise Users are shown.



Registry Values Bookmark: Subtab under *Snapshots* that contains the results of a Windows registry parsing EnScript (such as *Initialize Case*). This icon is also displayed in certain scripts when selecting the registry.



Drivers Bookmark: Subtab under *Snapshots* containing



File Types: Selecting this icon presents the File Types view.



File Signatures: Selecting this icon presents the File Signatures view



File Viewers: Selecting this icon presents the File Viewers view.



Global Keywords: This icon is displayed when selecting *Keywords* from the *View* pull-down menu.



Keywords: Selecting this icon presents the Keywords view.



Search Hits: This subtab under *Cases* presents the Search Hits view. The icon appears on the *Home* subtab beneath *Search Hits*, as well as the *Search Hit* root in the Tree Pane. It is also the icon used for *Search Summary* and *Case Time Settings* bookmarks.

Preview icon: When displayed as an overlay at the bottom right corner of any other icon, this blue triangular icon indicates that there is a live preview being performed on the selected device. A red icon indicates a preview of a network device in EnCase Enterprise.



Floppy disk \ Zip disk: Indicates a floppy disk or Zip disk preview/acquisition, and is also displayed in the Add Device window as a valid removable device.



Empty floppy disk: The floppy icon, surrounded by a pink overlay, indicates that no floppy media is available in the selected drive.



FastBloc protected device: A FastBloc write protected device available for preview or acquisition, indicated by a blue border overlay.



Palm: A Palm PDA device or evidence file is present.



Parallel Port \ Network Crossover: A device has been added using a parallel port or a network crossover cable.



Security IDs / Permissions (Entries subtab): Displays EnCase extracted file and folder security information (owner, group and permissions) for an NTFS file system as well as owner, group and permission settings for a Unix, or Linux system.



Text Styles: Selects the text style to view Code Pages in different settings, like variations in color and text line length. EnCase is configured with default text styles, but additional styles can be added, edited, and deleted from this tab by either right-clicking and selecting the command from the contextual menu or clicking the button in the toolbar



EnScripts / Code: Shows available EnScripts (small programs or macros designed to automate forensic procedures). When *Code* is selected in Table Pane, displays EnScript code in that window.



Run: The Run button appears on the top toolbar when code for an EnScript is selected and ready to run.



Hash Sets: A collection of hash values of files that belong to the same application.



App Descriptors: This view enables examiners to organize the hash values of live processes running on a system scanned by the Snapshot function.



Machine Profiles: This view enables examiners to create a custom profile of the authorized applications or processes that should be running on a target machine. The icon also appears on the *Home* subtab beneath *Machine Profiles*, and represents network nodes in the Network tabs. When a node is included, the icon has a green plus sign overlay in the upper right,



Allowed: Subtab beneath Machine Profiles that shows allowed permissions.



Encryption Keys: This view enables users to generate key pairs to be used with EnCase Enterprise.



EnScript Types: A reference resource containing the EnScript language classes. The right-pane displays each functions parameter.



Redirect: Indicates the file that overwrote a deleted file, displayed in the status bar. The contents being displayed are not the contents of the deleted file.



EnScript Member Functions: Functions that are defined within the Script or Class. This icon appears in the Tree Pane under *EnScript Types*.



Packages: The Packages icon appears when selecting Packages from the View pull-down menu. These are bundles EnScripts with permissions and properties applied.



SAFE: This icon appears in the SAFE tab, the *Logon* and *Logoff* button, and anywhere else a SAFE is represented. The *Logoff* button has a red minus sign overlay above the icon.



Role: Represents Roles where they appear in EnCase.



Events: This icon appears when events are captured by EnScripts, or logs are available (under the icon with the same image)



Permission: Indicates a permission name in the Role settings



Display (Query): Shows the Display characteristics for the selected Query when creating or editing a Query.



Condition (Query): Shows the Boolean condition for the selected Query when creating or editing a Query.

Gallery View

The Gallery view is a quick and easy way to view images that were stored on the Subject media. This includes all images purposely stored and all images inadvertently downloaded from the web.

It is possible to access all images within a highlighted folder, highlighted volume, or the entire case. If a folder is highlighted in the left pane of the *Cases* tab, EnCase

will display all contained files in the right pane. The **Set Include** trigger displays *all* images within the folder and any subfolders.

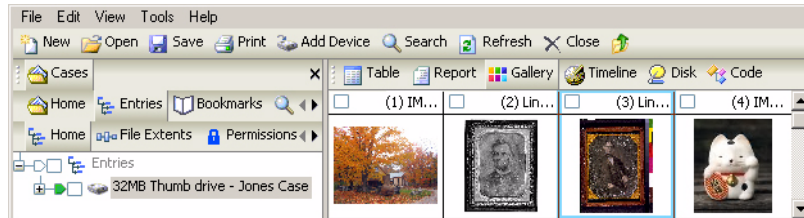


Figure 15-72: Gallery View

Within the Gallery view it is possible to bookmark images to display them in the report. Right-click on the image you wish to bookmark and choose **Bookmark Files**. Multiple images can be bookmarked simultaneously by blue-checking the box next to each file. When the **Bookmark Files** option is selected, a check box will appear in the **Bookmark Files** dialog box to **Bookmark Selected Items**; with a single file blue-checked, this option is grayed out. Toggling this check box will determine if the selected file or all blue checked files are bookmarked.

The Gallery view displays files based on their file extension by default. For example, if a .jpg file has been renamed to .dll, it *WILL NOT* be displayed in the Gallery view until a Signature Analysis has been run. Once the Signature Analysis has recognized that the file has been renamed and that the file is actually an image, it will be displayed in the Gallery view.

To reduce or increase the number of images displayed in the Gallery view at any one time, right click in the Gallery and select **Fewer Columns, More Columns, Fewer Rows** or **More Rows** from the menu.

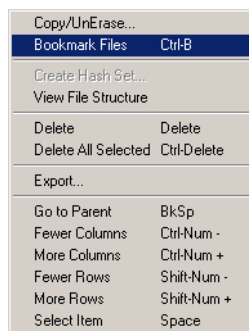


Figure 15-73: Gallery options

EnCase includes built-in crash protection, which prevents corrupted graphic images from appearing in Gallery or Picture view. The corrupt images are stored in cache so that EnCase recognizes them the next time they are accessed, and does not attempt to display them. These images are cached at the case level so that the images will not attempt to display in that case file again. The cache can be cleared by right clicking on the case in **Cases** view and selecting **Clear invalid image cache....** This option only appears after a corrupt image is encountered. The timeout (12 seconds by default) for the thread trying to read a corrupt image file can be set by clicking on the **Global** tab after selecting **Options** from the **Tools** pull-down menu.

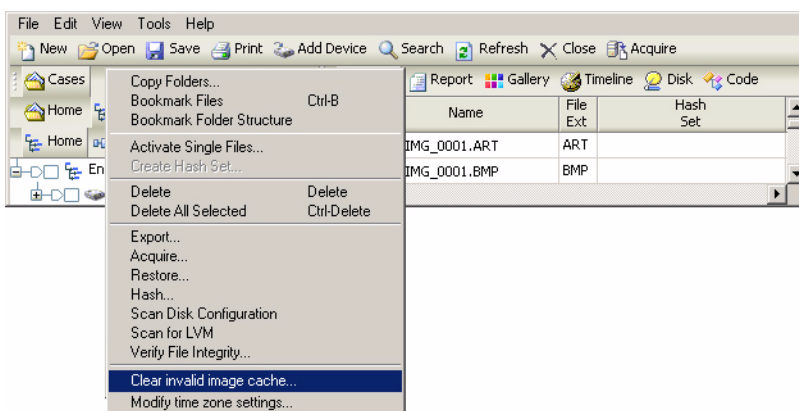


Figure 15-74: Clearing invalid image cache

America Online .ART files

EnCase has support for America Online .ART format images in the Picture and Gallery views. The .ART support requires the Internet Explorer AOL Support module be installed on the examination computer. The installer is available for download and installation from Microsoft's web site at <http://www.microsoft.com/windows2000/downloads/recommended/aolfix/default.asp>. This will install Jgaw400.dll, Jgdw400.dll, Jgmd400.dll, Jgpl400.dll, Jgsd400.dll, and

Jgsh400.dll. The installation does not require a reboot of the computer, nor closing and restarting of EnCase.

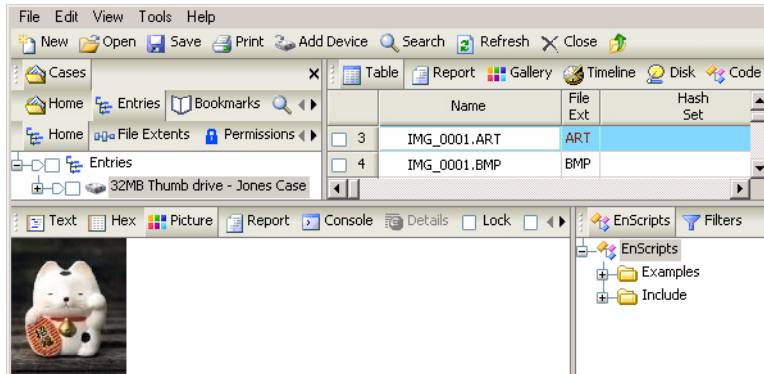


Figure 15-75: Viewing ART files

Timeline View

The Timeline view is a great resource for looking at *patterns* of file creation, editing, and last accessed times. You can zoom in (**Higher Resolution**) to a second-by-second timeline and zoom out (**Lower Resolution**) to a year-by-year timeline by right clicking and selecting the appropriate option.

Above the calendar view are five check boxes to quickly and easily filter which type of time stamp to display: **File Created, Last Written, Last Accessed, Last Modified and File Deleted.**

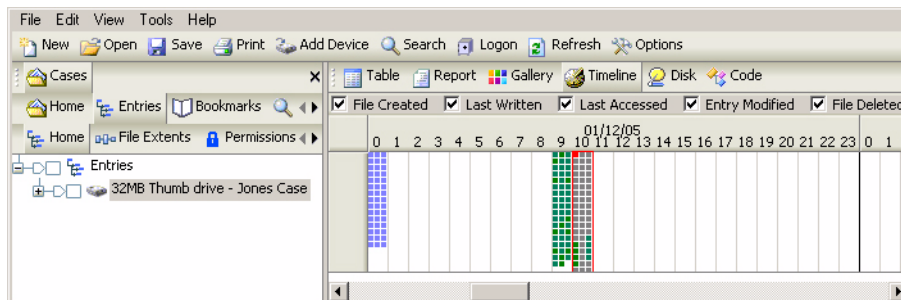










Figure 15-76: Timeline View

Times are represented by different color squares in Timeline view; the default colors are as follows:

	A file with a Created date / time stamp is represented by a green square (Red: 0, Green: 128, Blue: 92)
--	--

	A file with a Written date / time stamp is represented by a green square (Red: 0, Green: 128, Blue: 0)
	A file with a Accessed date / time stamp is represented by a light purple square (Red: 128, Green: 128, Blue: 255)
	A file with a Modified date / time stamp is represented by an aqua square (Red: 0, Green: 128, Blue: 128)
	A file with a Deleted date / time stamp is represented by a red square (Red: 255, Green: 0, Blue: 0)
	A file with a Logoff date / time stamp is represented by a black square (Red: 0, Green: 0, Blue: 0)
	A file with a File Acquired date / time stamp is represented by a gray square (Red: 128, Green: 128, Blue: 128)
	Dark blue squares indicate that file is blue checked in the table.
	Bright red borders around squares indicate that the file is highlighted.

A gray box with three dots in a row indicates that there are too many files to list in the space given. Double-click the box to zoom in for file details.

The **Logoff** option is only valid for EnCase Enterprise.

The color assignments for each box can be changed by right clicking in the timeline and selecting **Options...** Right click on each color to assign additional colors (**Transparent, Black, Light Red, Light Green** or **Light Blue**), or double click on them to assign a custom color. To change a box back to its' default color, right click on that box and select **Default**. You can also change the timeline start and stop dates in the **Options** window.

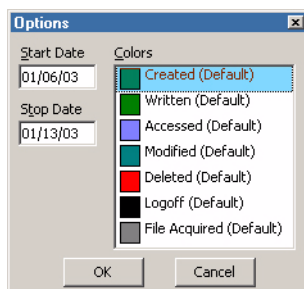


Figure 15-77: : Timeline Options

Report View

Report view displays information about the current folder/volume selected in the left pane, such as date and time stamps and file permissions. In the **Bookmark** subtab under Cases, Report view provides documentation for all of the evidence

bookmarked during the investigation. For additional information, see the chapter in this document on *The Report*.

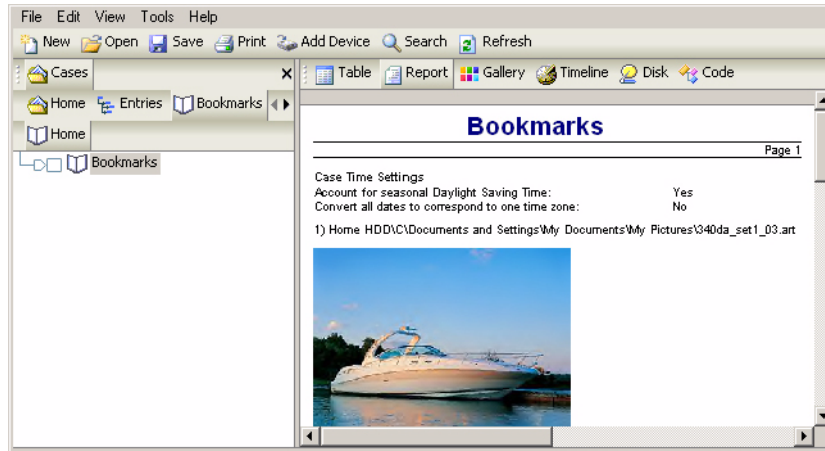


Figure 15-78: Report View

EnScript View

When the **EnScripts** view is selected, the right pane shows the code for the EnScript located in the folder selected in the left pane. To show the code for the script, with the script selected, click on the **[Code]** tab over the table pane. To compile the script then click on the **[Compile]** button on the top toolbar, press **[Ctrl]** and **[F9]** simultaneously, or right click in the code window and select **Compile**. To run the script, click on the **[Run]** button on the top toolbar, press **[F9]** simultaneously, or right click in the code window and select **Run**.

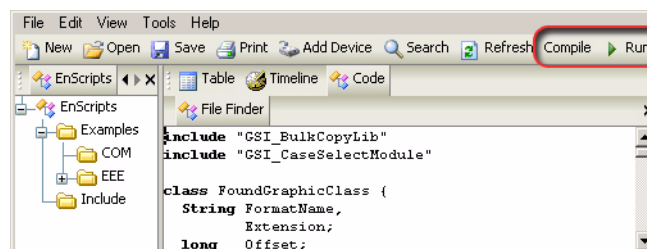


Figure 15-79: EnScript View

View (Bottom) Pane

The View Pane provides functionality specific to the view open and the item selected in the right pane. This includes feature tabs, a box to keep the tab constant, and a

navigation bar with numbers of files in the case and selected, and the precise location of the item selected.



Figure 15-80: Bottom Pane Tool Bar

- **Text**

The **Text** tab is for viewing text in the highlighted file above. It contains the output of the data in the selected Text Style for the currently selected file. Portions of the text can be “swept” by clicking and dragging, and then bookmarking, exporting or copying/pasting the highlighted data.

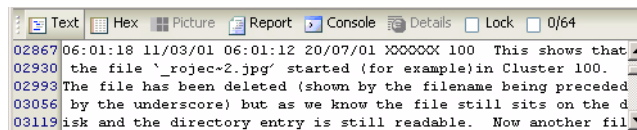


Figure 15-81: Text tab

- **Hex**

The **Hex** sub-tab contains the data, in hex format, of the currently selected file. The right-pane displays the text of the corresponding hex characters. EnCase 4.18 added the ability to sweep and copy data in the Hex view to the clipboard, and then paste the data as **Hex** in the desired application or within EnCase (similar to the method used for **Text**).

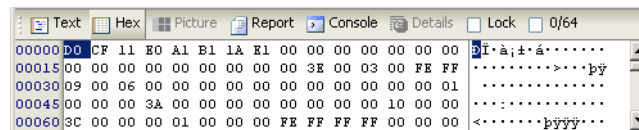


Figure 15-82: Hex tab

- **Picture**

The **Picture** tab displays the highlighted file/folder as an image. If the file is not an image, then the **Picture** tab will be grayed-out. EnCase can natively display GIF, JPEG, BMP, PNG, Photoshop PSD, AOL ART and TIFF files. Other image types require 3rd-party viewers.

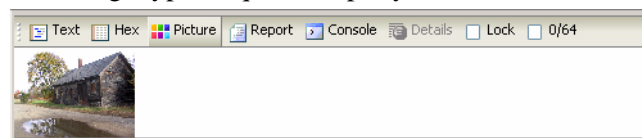


Figure 15-83: Picture tab

• **Report**

The **Report** tab displays the attributes of the currently selected file. The data shown is the same data as what is the Table view, but displayed in a report format in addition to the security attributes (if in NTFS).

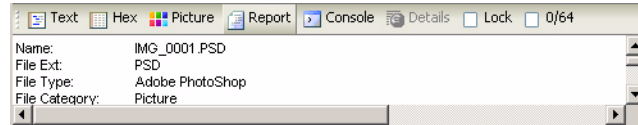


Figure 15-84: Report tab

• **Console**

The **Console** tab displays output from EnScripts, and functions such as Signature Analysis and searches that send output to the console upon execution. The console is located at C:\Program Files\EnCase4\console.txt.

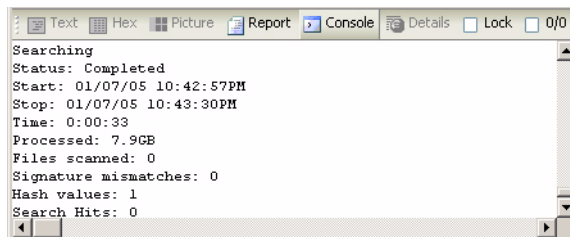


Figure 15-85: Console tab

• **Details**

The Details tab is used to show multi-dimension data referenced in a column of the Table view, such as File Extents or Bookmarks.

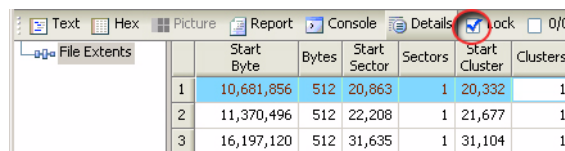


Figure 15-86: Details tab

• **Lock**

Checking **Lock** preserves the selected lower pane when scrolling through files. For example, if scrolling through the files in the table with the bottom pane locked in Hex mode, when an image is selected Hex view will be displayed for each file selected rather than returning to the default view (Picture, for images) for the file type (see figure above).

- **The “Dixon Box”**

The Dixon Box is at the top right of the View Pane. It is a check box with two numbers separated by a slash; the first number reflects the number of selected (blue-checked) files, while the second reflects the total number of files in the case. To quickly uncheck all files in a case, click in the box so that the first number is 0. Clicking again will select all files in a case.

- **Navigation data**

The navigation data, which appears at the bottom of the EnCase window (to the right of the filename) displays sector and cluster information. Every time the investigator clicks on new data (for example, clicking through sectors), the information displayed for that currently selected sector or cluster changes. The navigation bar contains the following information:

- **Evidence file name**

This is the name of the evidence file currently being accessed.

- **Physical sector number**

The number following the **PS** indicates the number of the physical sector currently accessed.

- **Logical sector number**

The logical sector, following the **LS**, is the Physical Sector minus 63.

- **Cluster number**

This indicates the location of the cluster being accessed (after the **CL**).

- **Sector offset**

Identified by the **SO**, this is the offset value within the *sector* of where the currently selected sector/cluster is.

- **File offset**

Identified by the **FO**, this is the offset value within the *currently highlighted file* of where the currently selected sector/cluster is.

- **Length**

The length, which follows the **LE**, indicates the number of bytes currently highlighted. Bytes can be “swept” (clicked and dragged to highlight) in the **Text** and **Hex** view, but *not* the **Disk** view.



NOTE: EnCase v5 uses the absolute byte offset for FO, as some devices (such as PDAs) do not use sectors or have sectors not equal to 512 bytes. This enables EnCase to give the examiner a more accurate and exact location of book marked evidence on the device. For example, the Physical Location of 3,688,448 is the number of bytes into the device at which a file, folder, bookmark or Unallocated Clusters start.

- **Find**

To search for specific text located in the lower pane in **Text** or **Hex** view, right-click and select **Find** or hit **[Ctrl][F]**. If text has been selected, the **Find** window will open with the selected text in the **Expression** field.

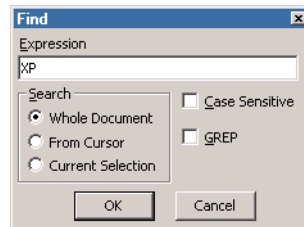


Figure 15-87: Find

Search options include:

- **Whole Document:** Searches the contents of the entire lower pane for the search string specified in the Expression field.
- **From Cursor:** Searches from the current cursor position to the end of the lower pane's text content for the search string specified in the Expression field.
- **Current Selection:** Searches for identical search strings specified in the Expression field.
- **Case Sensitive:** Searches for the specified string with regard to upper and lower case letters.
- **GREP:** Uses a specified GREP expression for the search string.



NOTE: Once the Find shows the first instance of the requested string (highlighted), you can press the F3 key to continue searching for similar strings.

EnCase, by default, displays characters in the **Text** and **Hex** tabs in 8-bit ANSI format. Unicode files view properly; however, modifications of both the format (encoding) and the font are required (see the chapter on *Foreign Language Support (Unicode)* for further details).

Panes

Whenever panes are split (right and left top panes, top from bottom, **Disk** view and **Text\Hex** view in the bottom pane), panes can be resized or restored by left clicking on the bars separating the panes and dragging the pane to the appropriate size.

Date and Time Questions

- **Is the Last Accessed Date the same as the deleted date?**

No. DOS does not store the deleted date of a file in the directory entry record. The only time that you can recover the deleted date and time is when the file is in the Recycle Bin. EnCase will recover these times when possible and display them in the **Deleted** column.

- **On some files, there are no time stamps in the Last Accessed column.**

If the file was created by a version of DOS prior to 7.0, the last access date will be blank.



NOTE: Let Recover Folders finish before running any further analysis on the drive. Other EnCase functions, such as keyword searches, will prompt you to terminate the Recover Folders command. If you do so, you will lose any folders recovered to that point.

VIEWING FILES

Some audio files, video files and certain graphic file formats are not immediately viewable within EnCase, however, examiners can utilize third-party viewers to examine the files properly.

Copy/UnErasing Files

EnCase has a feature to recover and unerase files byte-per-byte. Many operations in EnCase require selecting a list of files. To select a file or folder, click on the check box to the left of the number in the Table so that a blue check mark appears. You can also blue check folders in the Tree Pane. To select a range of files, blue-check the first file in the range, holding down the [**Shift**] key and blue check the last file in the range. Files blue-checked in a subfolder will display blue checks all the way up the tree to the root of **Entries**.

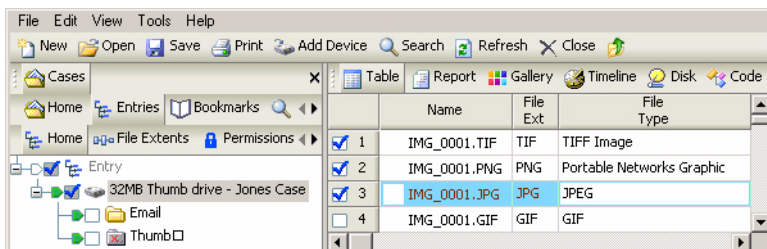


Figure 16-1: Selecting files and folders

To export a file from an evidence file in its native format, right-click on the desired file and select **Copy/UnErase...** To copy out a group of files, blue-check the desired files, right-click one of the files and select **Copy/UnErase....** You can specify whether to select only a single highlighted files, or all blue-checked files. When copying out multiple files, you can have these export as separate files or into a single concatenated file. Deleted files on a FAT volume have a hex `\xE5` character at the

beginning; EnCase allows you to replace this character with the character of choice (by default, this is an underscore (_)).

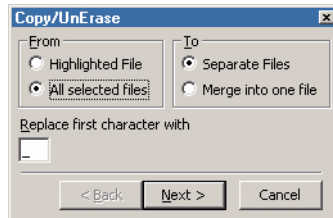


Figure 16-2: Copy/UnErase Options

After selecting the desired options, click [**Next >**] and select the radio button for the appropriate options as follows:

- **Logical File Only**

Copies out only the logical part of the file (file slack will not be copied).

- **Entire Physical File**

Copies out the entire file (logical file, as well as file slack).

- **RAM and Disk Slack**

RAM Slack (sector slack, the buffer between the logical area and the start of the File Slack) and Disk Slack the buffer between the end of the logical area and end of the physical area) are both copied out when this radio button is selected.

- **RAM Slack Only**

RAM Slack (sector slack) is copied out when the radio button is selected.

- **None**

Accepting the default **Character Mask** value of **None** copies the file out exactly as it is on the disk.

- **Do not Write Non-ASCII Characters**

Selecting this radio button copies out all characters EXCEPT non-ASCII characters.

- **Replace Non-ASCII Characters with DOT**

This option replaces all non-ASCII characters copied out with dots.

- **Show Errors**

Formerly, EnCase would pause on errors when copying out files. Version 5 provides the option of bypassing these so that large numbers of files can be copied out unattended. By default, this option is unchecked to skip errors.

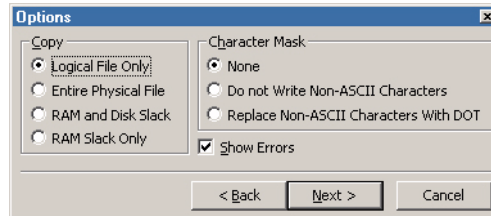


Figure 16-3: Copying options

Click [**Next >**] and choose a destination path in which to place the copied file(s). If multiple files are copied to a single file, the destination will be a file path. If separate files are being copied, the destination path will be a folder. You can accept the default, type in the path, or click on the ellipsis box on the right to browse to the desired location. By default, EnCase will split files over 640 MB in size; you can adjust this amount in the **Split files above (MB)** field. One useful purpose for this option is so that users can copy/unerase the entire Unallocated Cluster file and break it up into 640 MB chunks for burning to CD-R. The maximum value for this field is 2,000,000 MB (2 terabytes). Bear in mind when setting this value that if you are writing files to a FAT file system, the maximum allowable size is 2,000 (2 gigabytes); setting the value higher will result in write errors. Once the information is correct, press [**Finish**].

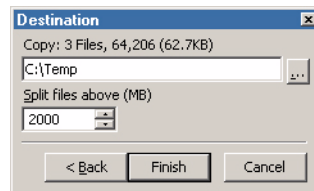


Figure 16-4: Copying options

When copying/unerasing a deleted file, EnCase will automatically unerase the file if possible.

Copying/UnErasing Bookmarks

It is possible to copy/unerase bookmarked files as well. The process is the same whether copying single or multiple bookmarks. Note that if the file has been deleted

and resides in Unallocated Space, **Copy/UnErase** will try to copy out the entire Unallocated Space, since the data pertaining to the file resides within.

- Click on the Dixon box or the root folder to blue-check all files, and then click again to remove all blue checks.
- Click on the **Bookmarks** tab under **Cases**.
- Blue-check the bookmarked file you wish to copy out. If you are copying multiple files, blue-check all files to be copied. To copy all files, or a range of files, you can blue check the first bookmark in the range, hold down the [**Shift**] key and then click on the check box of the last bookmark in the range. All bookmarks between the checked bookmarks will be checked.
- Right click anywhere in the Table view and select **Tag Selected Files**.
- Click on the **Entries** subtab and note that the files corresponding to the bookmarks you checked are now also all blue-checked.
- Right click on one of the blue-checked files and select **Copy/Unerase**.
- Make sure the radio buttons for **All selected files** and **Separate files** are selected and click [**Next >**]
- Select the appropriate **Copy** and **Character Mask** options (typically **Logical File Only** and **None**) and click [**Next >**]
- Set the appropriate path you wish to copy the files to and then click [**Finish**]

All tagged files (corresponding to the checked bookmarks) will be copied to the specified directory.

Copying Entire Folders

It is possible to copy out a folder and its' contents, including subfolders. To perform this task, do the following:

- In the **Entries** subtab, blue check the folder in the tree pane to copy
- Right click on the folder and select **Copy Folders....**
- In the field below **Copy:**, enter the destination path
- If you do not wish to copy all the files in the recursive folders, blue check the files you wish to be copied and place a check in the box labeled **Copy only selected files inside each folder**

- Click [OK].



If the *Copy Folders...* command is executed with an evidence file highlighted, the entire contents of the evidence file will be copied to the Storage hard drive!

Viewing Files Outside of EnCase

File Viewers

Frequently, an investigator will find file types that EnCase does not have the built-in capabilities to view (such as an MP3 or AVI file) or they might want to view a file type that EnCase does support with a third party tool or program. In either situation, it is necessary to set up a file viewer so that EnCase can associate the file type with the appropriate application.



To view a file outside of EnCase, a viewer capable of opening and interpreting that file type is required. For example, QuickView Plus (a popular image viewer) will not open an MP3 file.

Setting up a File Viewer

- From the **View** pull-down menu, select **File Viewers**
- Right-click on the root folder and select [**New**]

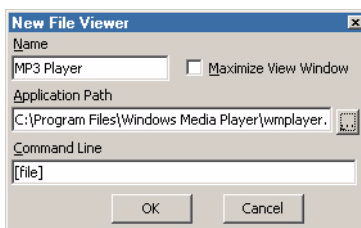


Figure 16-5: Setting up Windows Media Player as a Viewer

- In the **New File Viewer** window, enter a **Name** for the viewer and the application's executable path. The **Command Line** field is utilized in the event the external application needs additional commands or switches invoked in order to function properly, but in general it will be left with the default value of [**file**]
- Click [OK]

File Types

At installation, EnCase has a considerable amount of file signatures matched to their appropriate applications to properly access the file. However, files are constantly encountered from new applications, with different extensions and new access methods. EnCase allows the user to add file extensions and match them to the correct viewer. To configure File Types in EnCase, do the following:

- From the **View** pull-down menu, select **File Types**.
- Right-click on the **File Types** root folder and select **[New]**.
- Enter a **Description** (type of file), **Extensions** (file extensions to associate), and select a **Viewer** to use. If you choose EnCase, it will be opened within EnCase, but only if EnCase can view the file internally; selecting Windows uses the default viewer for the file type in Windows. If you have set up a Viewer in EnCase, you can select the **Installed Viewer >>** radio button and select the viewer from the window on the right. Non-native file viewers must be installed through EnCase prior to adding a new file type. When the options are complete, click **[OK]**.

After the file type has been associated with a viewer, whenever a file of that extension is double-clicked, the file will automatically be copy/unerased to the Storage hard drive and opened with the associated viewer.

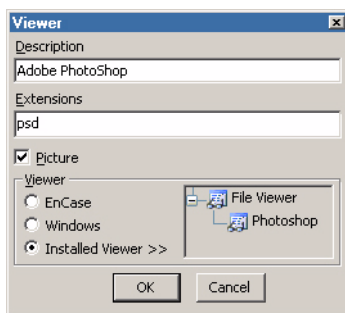


Figure 16-6: Associating a File Type with a Viewer

File Viewing FAQs

- Some deleted files have a '?' as the first character and some do not. Why?
If a file has a long name (any non uppercase 8.3 name), DOS stores two sets of entries for the file. One entry contains the 8.3 short equivalent (usually with

a ~ at the end) and the other set contains the long name. When a file is deleted, the first character of the 8.3 name is replaced with a hex E5 (set to '?' to make it readable) but the first character of the long name is preserved. EnCase replaces the '?' character in the short name entry with the first character of the long name if it exists.

- **When I copy an entire folder, do the deleted files get copied too?**

Yes. You can circumvent this by selecting the entire folder, then de-selecting the files that should not be copied. Then check **Copy only selected files** in the **Folder Copy** dialog.

- **Is it possible to recover a deleted file in its entirety?**

Not always. Some deleted files may not be recoverable at all or only partially recoverable. It is possible that the only remnant of a deleted file is its directory entry. Occasionally, some data may be recovered, but it is not necessarily the original contents of the file.

- **How do I select all files in the Case?**

In the **Entries** subtab below the **Cases** tab, checking any folder checks all the files and folders contained within. To check all the files and folders in the case, blue-check the root folder at the top of the tree. Checking it again will deselect all folders and files.

To select a range of items in the table view, blue-check the first item, hold the **[Shift]** key down and check the last item.

E-MAIL AND INTERNET ARTIFACTS

New to EnCase version 5 are several tabs that allow examination of evidence files and the ability to extract specific artifacts, including:

- **E-Mail**
- **History**
- **Web Cache**

These tabs allow the examiner to isolate the information in separate windows that can be searched, bookmarked, sorted, etc. Each tab is described in depth here.

E-Mail

When evidence is previewed in a case, EnCase can search for various types of E-mail and parse the contents. The results then become available in a user friendly format via the **Email** tab. This subtab resides below **Cases** and houses entry metadata such as **From**, **To**, **Subject**, **Created Date**, **Sent Date**, **Received Date**, **Header Information**, and **Attachments**. This feature can be run on the following email application types:

- **AOL 6.0, 7.0, 8.0, 9.0**
- **Outlook Express (.DBX)**
- **Outlook (.PST)**
- **Hotmail**
- **Yahoo!**

- **Netscape**
- **mbox**

Once the **Email\Internet Search** feature is run on evidence containing supported email applications, EnCase populates the contents into the **Home** and **Attachments** subtab, with the parsed contents gathered from the search.

The **Email** subtab also contains E-mail artifacts if a compound mail file is mounted manually from the **Entries** tab. For example, if a **.PST**, **.DBX**, or AOL **.PFC** file is mounted in the Entries tab, the E-mail entries will be automatically be displayed.

Along with the new **Email** tab, EnCase now supports additional E-mail file types, such as AOL 6, 7, 8 and 9, support for web-based E-mail such as Yahoo, Hotmail, and Netscape, MBox (Unix) support, and Outlook Newsgroups (.DBX) format support.

Webmail is populated from any relevant files in the WebCache tab. If you choose to search for any web mail types, the **History** and **WebCache** searches will be run automatically.

Using the Email Option

In order to use this feature, you must first add evidence that contains any or all of the above stated supported E-mail applications to a case. To view E-mail, do the following:

- Add evidence with supported E-mail entries
- Under the **Cases** tab, select **Email**
- Under the **Home** tab, right click on the root **Email** folder and select **Email\Internet Search**. Alternately, you can select **Email\Internet Search**

from the **Edit** pull-down menu, or click on the [Email/Internet Search] button on the top toolbar.

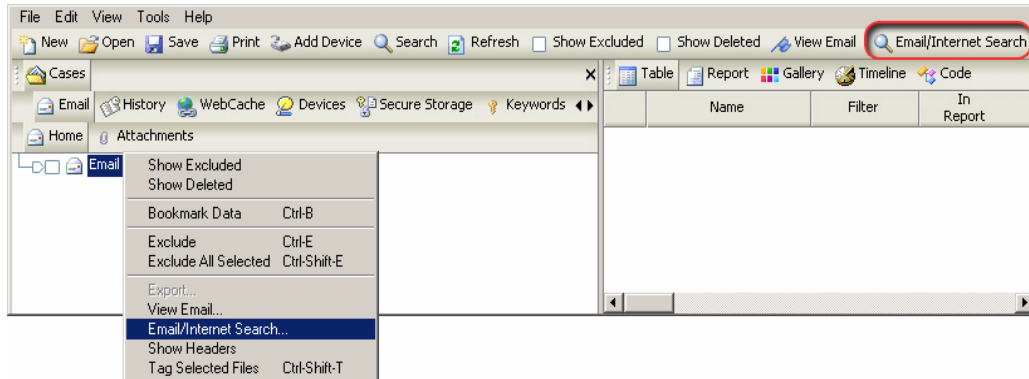


Figure 17-1: Searching for E-mail

- Select all or some of the supported E-mail types and apply the search to all evidence, or check the box for **Selected devices only** and click [OK]

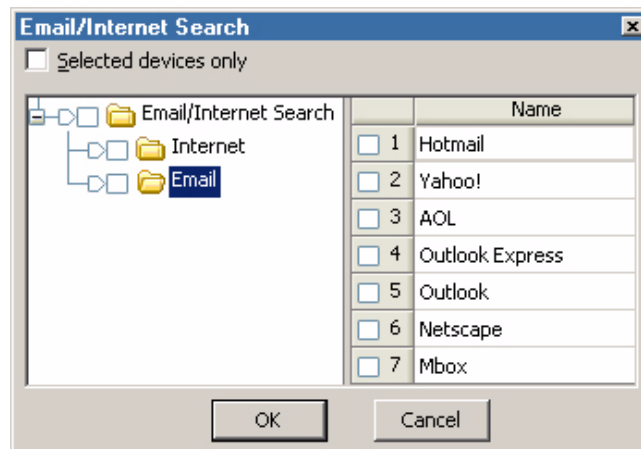


Figure 17-2: E-mail Search Parameters

- When the search is complete, messages should populate the Table Pane

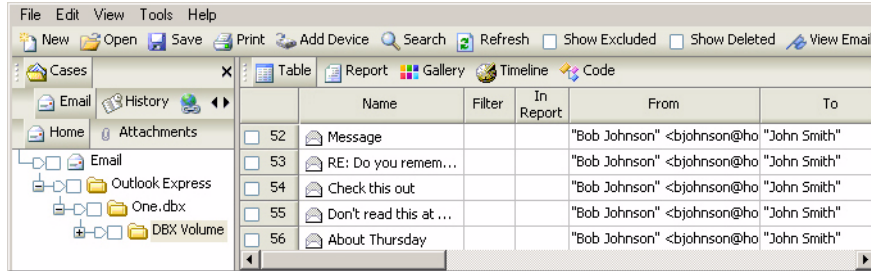


Figure 17-3: E-mail entries

An alternate method of viewing E-mail files is to mount a supported compound file as follows:

- Add evidence with supported E-mail entries
- Under the **Cases** tab, select **Entries**
- Select Table view in the right pane
- Right click on a compound file and select **View File Structure** (you will be given the option to Calculate unallocated space; check the box if you wish to do so)

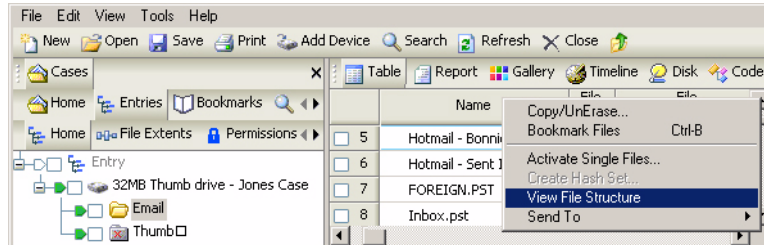


Figure 17-4: View File Structure of a DBX file

A dialog box appears that allows the calculation of unallocated space, as well as the ability to find deleted content within .PST files. check either of these boxes to enable those options when mounting the .PST.

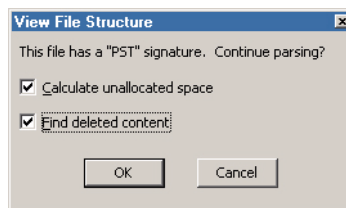


Figure 17-5: PST Mounting Options

- From the **Email** tab under **Cases**, select **Home**
- The E-mail contents of the mounted file should now appear in the Table Pane.



Mounting very large E-mail files will place an enormous strain on the forensic machine.

E-mail Attachments tab

If an E-mail message contains a number in the **Attachments** column, this indicates that the attachments can be retrieved by selecting the E-mail entry and clicking on the **Attachments** tab.

- Find an E-mail message that contains any number of attachments.

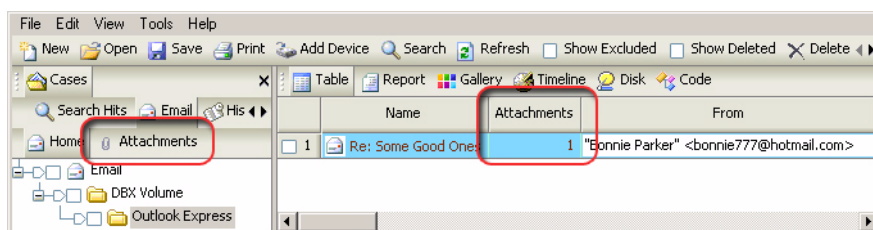


Figure 17-6: Attachments column

- Select that entry and then click on the **Attachments** tab.

Email Table Columns Explained

- **Name**
Subject of the E-mail message; varies between applications
- **Filter**
Narrows down E-mail entries by creating your custom filters
- **In Report**
The Boolean value indicating that the entry is included in the Report tab
- **From**
Sender of the E-mail. Drafts may not have an entry in the **From** column
- **To**
Recipient of the E-mail message. Drafts or E-mails that were BCC'ed may not have an entry in the **To** column

- **Subject**

Subject of the E-mail message. Not all E-mail messages require a subject; therefore this entry may not appear

- **Cc**

Party to whom E-mail message was Carbon Copied (cc). Since not all E-mail messages are copied to other parties this entry may not appear

- **Bcc**

Party to whom E-mail message was Blind Carbon Copied (bcc). Since not all E-mail messages are copied to other parties this entry may not appear. The difference between cc and bcc recipients is that bcc recipients are not seen by others receiving the message.

- **Created**

Date the E-mail message was created in Local Time format.

- **Sent**

Date the E-mail message was sent in Local Time format.

- **Received**

Date the E-mail message was received in Local Time format.

- **Header**

Header information of the message. Internal E-mail messages may not have header information available

- **Folder**

The location of the entry from within the compound file. Column information may vary for different E-mail types

- **EntryPath**

The location within the mounted volume of the E-mail artifact

- **Attachments**

The number of attachments for a particular E-mail message



All E-mail types do not follow a standardized format. The fields of the columns represented above may or may not be populated by data from retrieved E-mails. For example, some versions of AOL may or may not populate the header field.

History

When evidence is added to a case, EnCase has the ability to search through it for various types of web artifacts. The **Email\Internet Search** feature allows you to search for Internet usage via the following browsers:

- **Internet Explorer**
- **Mozilla (Firefox)**
- **Opera**
- **Safari**

Once the feature is run on evidence containing the supported browsers, EnCase will populate the **History** tab with the artifacts that were found. This option also populates the **WebCache** tab with the appropriate artifacts (see the section in this chapter on the **WebCache** tab). This data can also be extracted by opening the **History** tab, right-clicking on the **History** icon and selecting **Email\Internet Search**.

All the information found in the **History** tab is parsed from various files. The location of these files may vary from browser to browser. For example, Internet Explorer may use **INDEX.DAT** files that usually reside in **%root%\Documents and Settings\USERNAME\Local Settings\History\HistoryIE5** and its subfolders, while Firefox may store data in **HISTORY.DAT** residing in **%root%\Documents and Settings\USERNAME\Application Data\Mozilla\Firefox\Profiles*.default**. Depending on which files the history artifacts are parsed from, interpretations of the times listed under **First Date** and **Second Date** will vary.

To better understand the time stamps please see the *Time Interpretation Format* section below. Another method to better understand time interpretations is to clear the cache and history on your local machine, browse the Internet, and then preview the local machine. The *EnCase Internet and E-mail Examinations* training course is another useful resource for information on Web, E-mail, and P2P artifacts.

Finding Web Artifacts

To use the **Email\Internet Search** option to find web artifacts, you must first add evidence to a case that contains any or all of the above stated web artifacts entries. The option has the same functionality under either the **History** or **WebCache** tabs. You can also find this function on the toolbar when the **History** tab or **WebCache** tab is selected.

- Launch EnCase and open a new case.
- Add evidence containing supported web artifact entries.

- From the **Cases** tab, select **History**.
- Right-click on the root of the **History** folder and select **Email/Internet Search**.

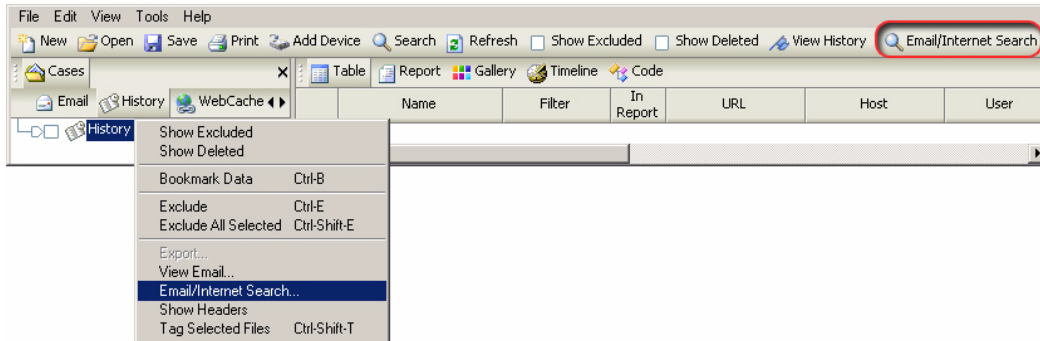


Figure 17-7: Finding Web Artifacts

- Check some or all of the supported browser types in the **Search for:** window and run the search on all evidence files, or check the box to search **Selected devices only**. When all selections have been made, click [OK].

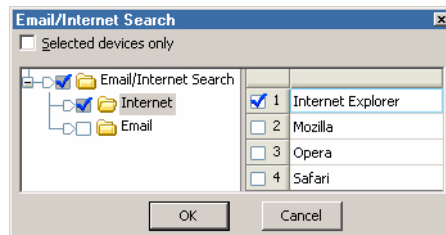


Figure 17-8: Select browser for search

- Artifacts should populate the **Table** pane.

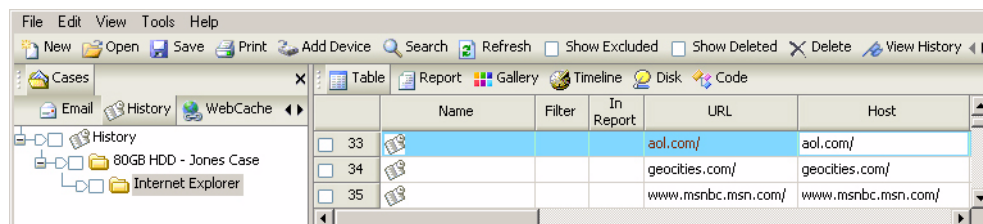


Figure 17-9: Web History artifacts

Time interpretations formats:

The name of an Internet Explorer history record will indicate the meanings of the associated times:

- **Cookies**

First Date: Cookie created

Second Date: Cookie last accessed

- **History**

First Date: Last accessed

Second Date: Last accessed

- **Content.IE5**

First Date: Server modified

Second Date: Last accessed

- **Daily**

First Date: Last accessed (Local Time)

Second Date: Last accessed

- **Weekly**

First Date: Last accessed (Local Time)

Second Date: File created



The timestamps of the Daily and Weekly Internet Explorer records warrant a special note. The Second Date is a normal Windows date which will display in the current Time Zone setting for the volume. However, the First Date is not a standard Windows timestamp. This timestamp is saved by Internet Explorer in the user's Local Time (rather than GMT). EnCase will adjust this time to display properly using the current time zone settings, however, if the First Date and Second date on a Daily history record do not match, it's an indication that the current time zone settings are not correct.

- **Time interpretation for other browsers (Safari, Mozilla and Opera):**

First Date: Last accessed

History Table Columns Explained

- **Name**

Will display the record name (**History, Daily, Weekly, etc.**) for an IE History record; **otherwise, it will be blank**

- **Filter**

Narrows down the History artifact entries by custom filters

- **In Report**

Contains a Boolean value to indicate entry is included in the report tab

- **URL**

Complete URL address of History entry

- **Host**
Domain Host of the URL
- **User**
Current user that was logged on at the time of visit
- **Title**
Title of web page (if available)
- **VisitCount**
Number of times site was visited by the user. A blank field indicates that no information about the number of times visited is available
- **First Date**
Date and time of last visit of user (may or may not be GMT offset)

- **Second Date**
See *Time Interpretations Formats* table. This only applies to IE.
- **Cached**
Contains a Boolean value to indicate if the entry also has an entry in the WebCache tab
- **HistoryPath**
Location of the **.DAT** file from where the entry was parsed

Web Cache

The **WebCache** tab under **Cases** allows the user to search evidence for various types of web artifacts. The **Email\Internet Search** feature allows you to search for the following types of Internet usage:

- **Internet Explorer**
- **Mozilla (Firefox)**
- **Opera**
- **Safari**

Once the **Email\Internet Search** is run on evidence containing the supported internet browsers, EnCase will populate the **WebCache** tab with the artifacts that were found. The **Email\Internet Search** feature is closely related to the functionality of the **History** tab previously discussed.

The function searches for artifacts located in cache folders. The locations of those cached archives depend on the Internet browser you are using (e.g., Opera stores cache files in **\Documents and Settings\UserName\Application**

`Data\Opera\Opera\profile\cache`, while Microsoft Internet Explorer stores cache data in the `\Documents and Settings\UserName\Local Settings\Temporary Internet Files\Content.IE5` and subfolders.

The *EnCase Internet and E-mail Examinations* training course also provides considerable useful information regarding Web, E-mail, and P2P artifacts.

Finding Web Cache data

To use the **Email\Internet Search** option, you must first add evidence to a case that uses any or all of the above stated web browsers. The option has the same functionality under either the **History** or **WebCache** tabs. You can also find this function on the toolbar when the **History** tab or **WebCache** tab is selected.

- Launch EnCase and open a new case.
- Add evidence that uses any of the following Internet browsers:
 - **Internet Explorer**
 - **Mozilla (Firefox)**
 - **Opera**
 - **Safari**
- From the **Cases** tab, select **WebCache**.
- Search for artifacts using one of the following methods:
 - Right-click on the root **WebCache** icon and select **Email\Internet Search**
 - From the **Edit** pull-down menu select **Email\Internet Search**
 - Click on the [**Email\Internet Search**] button on the top toolbar

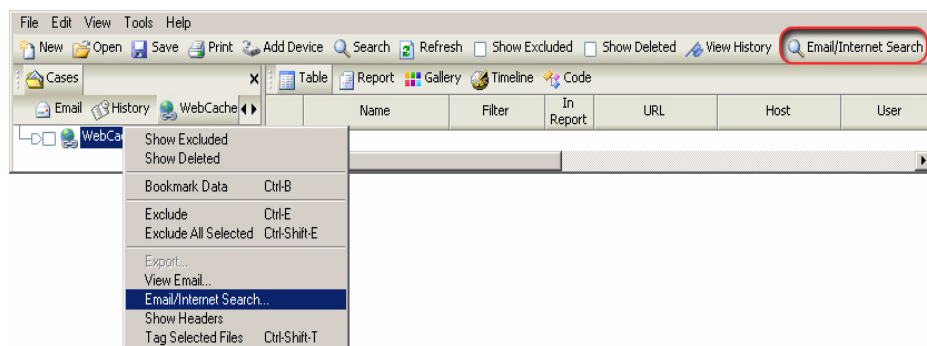


Figure 17-10: Find Web Artifacts

- Check some or all of the supported browser types in the **Search for:** window and run the search on all evidence files, or check the box to search **Selected devices only**. When all selections have been made, click [OK].

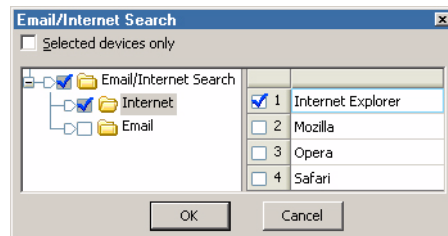


Figure 17-11: Artifact Search

- Artifacts should populate the Table pane

	Name	URL	Host
<input type="checkbox"/> 6	WebCache	http://i.cnn.net/cnn/element/ssi/css/1.1/main.css	i.cnn.net
<input type="checkbox"/> 7	WebCache	http://nowrunning.com/news/images/hrimages/hea	nowrunning.com
<input type="checkbox"/> 8	WebCache	http://gfx2.hotmail.com/i.p.fwd.gif	gfx2.hotmail.com

Figure 17-12: WebCache Artifacts

WebCache Table Columns Explained

- **Name**

Blank for standard cache records, **Redirect** for redirected records, **Deleted** for deleted records

- **Filter**

Narrows down the WebCache artifact entries by creating custom filters

- **User**

Current user that was logged on at time of visit

- **In Report**

The Boolean value indicating if the entry is included in the **Report** tab

- **URL**

The complete URL address of the WebCache entry

- **Host**

The Domain Host of the URL

- **InHistory**

The Boolean value indicating if the entry also has an entry in the **History** tab

- **CachedDate**

The date and time of when the artifact was cached on the local drive

- **CachePath**

The location in which the cached file is located (usually from the Temp folder of the Internet browser used)

KEYWORD SEARCHES

The search function of EnCase can locate information anywhere on the physical or logical media within current open cases. EnCase can search for each keyword byte-by-byte from the beginning to the end of every medium, and also search every logical file. Keywords can be either global or case specific.

Global keywords are saved in the **keywords.ini** initialization file within the EnCase directory. They are accessed by selecting the **Keywords** option from the **View** pull-down menu.

Case specific keywords are saved in the case file. They are managed from the **Keywords** subtab below **Cases**, which is enabled by checking the **Keywords** option under **Cases** in the **View** pull-down menu. The functionality of the local keyword tab is identical to that of the global tab.

Creating Keyword Groups

Global keywords may be accessed by any open case, therefore, it is important to group keywords properly so that they can be located easily when needed. To do this, folders can be created and moved around within the **Keywords** tab. This, and all functionality specific to keywords applies to keywords stored in either global or case-specific **Keyword** tabs.

To create a group, right-click where the folder is to be created, and select **New Folder**. To give that folder a specific name, hit the [**Backspace**] key after the folder is created until the name is blank, then type the name in. Alternately, once the folder is created,

you can right click on the folder and choose **Rename**, or highlight the folder and hit **[F2]**.

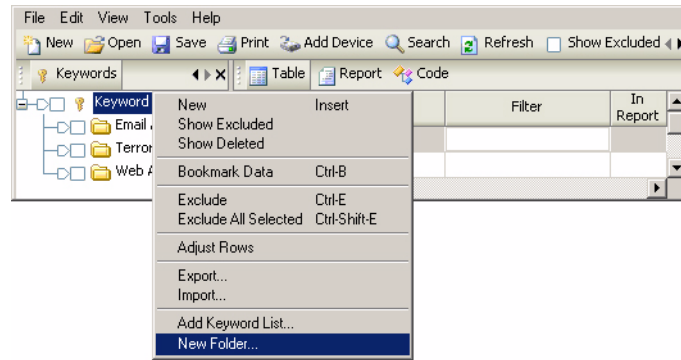


Figure 18-1: Creating a new Keyword folder

To delete a folder, right click on the folder and select **Delete** or press the **[Del]** hotkey. To move a folder, left click and hold on the number box associated with that folder in the right pane and then drag the folder to its new location.

Entering Keywords

Keywords can be added directly to a new folder, an existing folder, or to the root folder. To create a new keyword, right-click on the folder in which you wish to add a keyword and select **New** from the pop-up menu. The **New Keyword** dialog box will appear.

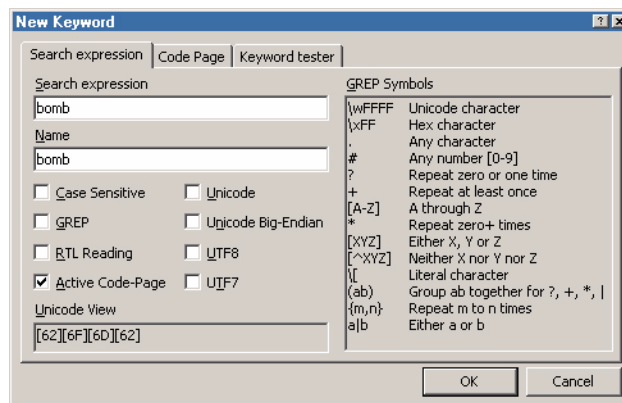


Figure 18-2: Keyword entry and options

Type the search string in the **Search expression** field and give the keyword a **Name** to identify it easily. Specify the parameters by checking the appropriate boxes

for **Case Sensitive**, **GREP**, etc. The section below describes each option and its' function. Once you have entered the search parameters, click [**OK**].



If a **GREP** keyword includes a slash (/), it must be escaped with another backslash to get the literal "\", since it is the escape character in **GREP**.

Search Options

- **Case Sensitive**

With this box checked, EnCase will search for the specified keyword only in the exact case specified.

- **GREP**

This option uses the input symbols and text to search using the **GREP** (Globally search for the Regular Expression and Print) advanced searching syntax (see the *GREP* appendix for token syntax and examples).

- **RTL Reading**

The **RTL Reading** option will search for the keyword in a right-to-left sequence. If, for example, a user enters “**Arabic keyword**,” and specifies the keyword as **RTL Reading**, EnCase would show hits on that expression, flush-right, in the reverse sequence as “**drowyek cibara**.”

- **Active Code-Page**

EnCase Version 5 has the ability to enter keywords in different languages. The **Active Code-Page** option must be checked to enter keywords in certain languages. English character searches use the **Latin I** code page.

- **Unicode**

The Unicode standard attempts to provide a unique encoding number for every character, regardless of platform, computer program, or language. Unicode uses 16-bits to represent each character, as opposed to ASCII (which uses 7-bits). Unicode on Intel-based PCs is referred to as Little Endian. The **Unicode** option will search for the keyword only in Unicode. For more details on Unicode, please see <http://www.unicode.org> and the chapter on *Foreign Language Support*.

- **Big-Endian Unicode**

Big-Endian Unicode uses the non-Intel PC data formatting scheme, in which the operating system addresses data by the most significant numbers first (the reverse of Little Endian).

- **UTF-8**

To meet the requirements of byte-oriented and ASCII-based systems, UTF-8 has been defined by the Unicode Standard. Each character is represented in UTF-8 as a sequence of up to 4 bytes, where the first byte indicates the number of bytes to follow in a multi-byte sequence, allowing for efficient string parsing. UTF-8 is commonly used in transmission via Internet protocols and in Web content.

- **UTF-7**

UTF-7 encodes the full BMP repertoire using only octets with the high-order bit clear (7 bit US-ASCII values, [US-ASCII]), and is thus deemed a mail-safe encoding. UTF-7 is mostly obsolete, to use when searching for older Internet content.

International Keywords

EnCase Version 5 can search for keywords with international language support. This allows the investigator to search, for example, for Arabic keywords using Arabic characters or Japanese keywords using Japanese characters. Keyword hits can be displayed in the desired language, as will the document in which the keyword was found.

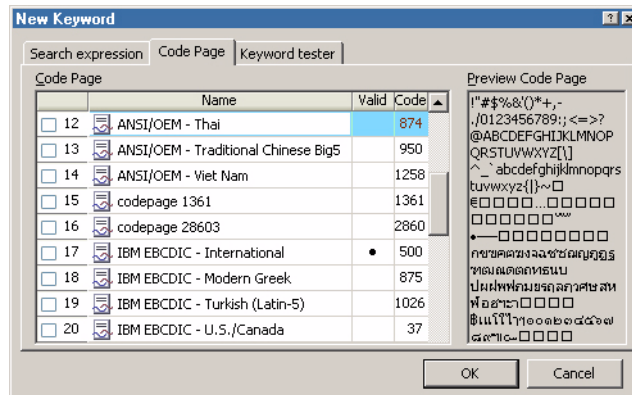


Figure 18-3: International keyword options

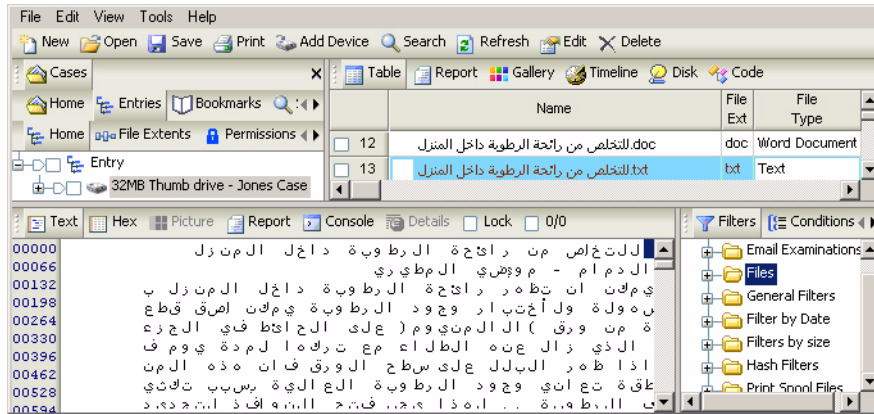


Figure 18-4: File displayed in Arabic, right to left

For languages other than English, see the chapter on *Foreign Language Support*.

Keyword Tester Tab

When creating a keyword, the user can test any search string against a known file by clicking on the **Keyword Tester** tab. Type the GREP expression in the **Search Expression** field and be sure to select the **GREP** check box.

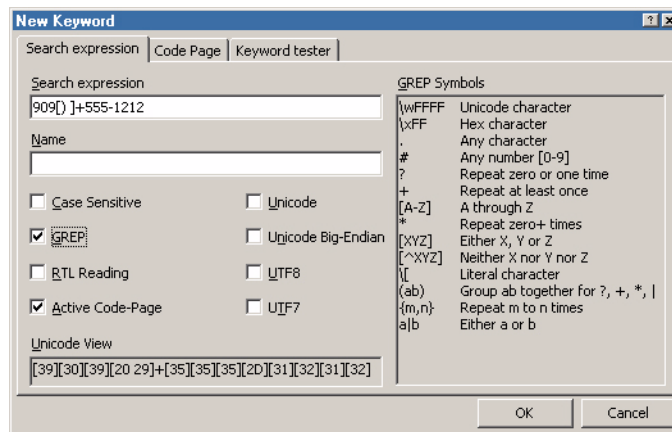


Figure 18-5: Creating the GREP expression

Click on the **Keyword tester** tab and in the **Test data** field, type the path to the file containing text that can be found using that string, or use the ellipsis box to locate

the file. Click on the **[Load]** button to test the string; the items found are highlighted in the window at the bottom, displayed in either **Text** or **Hex** views.

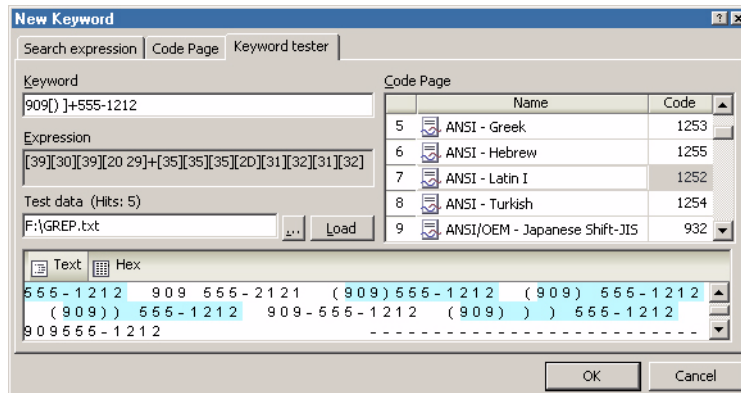


Figure 18-6: Testing the GREP expression

Exporting/Importing Keywords

Keywords and keyword lists can be exported to, and imported from other EnCase users. By exporting and importing keywords, it is possible to share keyword lists with other investigators.

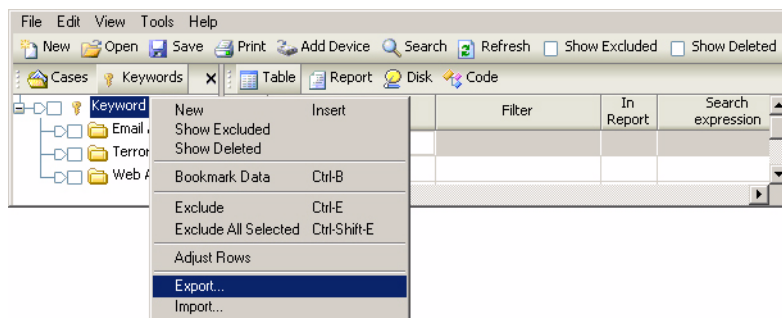


Figure 18-7: Export \ Import menu

Exporting Keywords

Keywords are exported in a TXT file format. You can export all keywords or export only blue-checked keywords. Keywords can be exported with their encoding information, including the following:

- Name
- Filter

- In Report
- Search Expression
- GREP
- Case Sensitive
- RTL Reading
- Active Code-Page
- Unicode
- Unicode Big-Endian
- UTF8
- UTF7
- Code Pages

Placing a check mark in front of each desired field exports it along with the keyword. Exported keywords can be manually added into the **Keyword** table. To export a keyword list for import, right click in the left pane and select the **Export** option. The **Export** options window will show **Export Tree (for Import)** checked, and any of the table columns that were blue checked on export from the table will be selected and grayed out. To export only the keywords in text format with specified fields, right click in the table and select **Export**. In this case, the **Export Tree (for Import)** option is unchecked and grayed out.

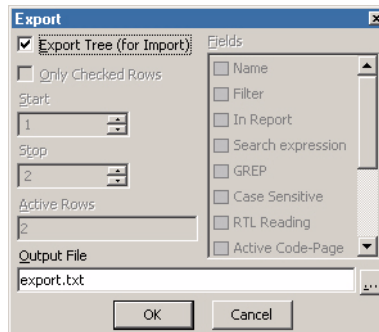


Figure 18-8: Exporting keyword list

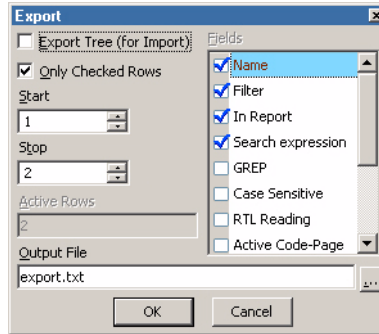


Figure 18-9: Exporting keywords

Exported keyword lists and keywords can be viewed by opening the .TXT file in WordPad or other text editor (control codes make the file unreadable in Notepad).

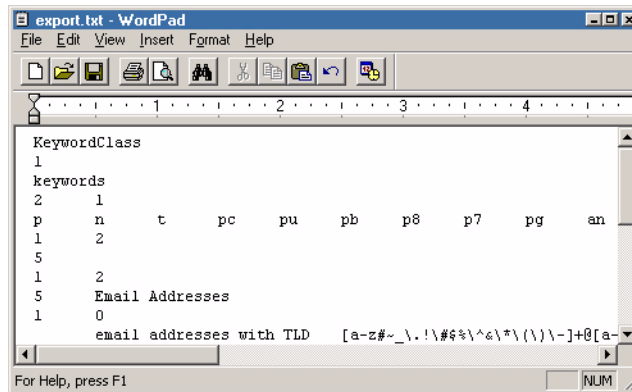


Figure 18-10: Viewing export.txt

Importing Keywords

Keywords are imported from a text file previously exported in EnCase. To import a keyword list into a particular folder, right click on the desired folder in the left pane and select **Import**. A subfolder, named Keyword, will be created and the folder structure from the imported keywords will appear beneath it.

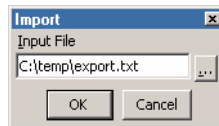


Figure 18-11: Importing exported keyword list

Adding Keyword Lists

To add keyword lists, right click in the right pane of the **Keywords** tab and select **Add Keyword List....** Keywords lists can either be typed directly into the **Keywords** field or they can be pasted from a keyword text document with one keyword and a line return per line. Select the appropriate keyword options (such as **GREP** or **Unicode**) by selecting the check box for that option, and click [**OK**]. The keywords will appear in the **Keywords** tab as separate entries.

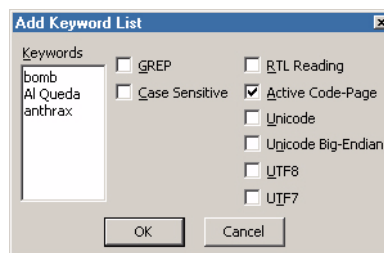


Figure 18-12: Adding keyword list

Starting a Search

To save time when beginning a search, decide whether to search an entire case, an entire device, or an individual file or folder. For example, when searching for information that may be in unallocated space, such as a file header, you can blue-check the Unallocated Clusters to avoid having to search the entire case.

To begin a search, click on the [**Search**] button on the top toolbar. There are several options that can be selected when running a search. Each option may generate significantly different results when the search is run.

The following image shows each search option, followed by descriptions:

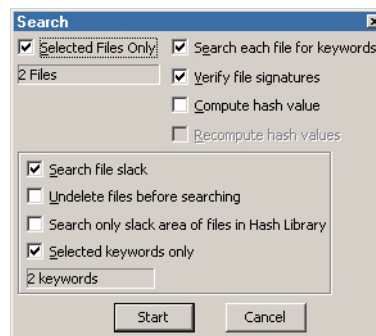


Figure 18-13: Search options

Search Options

- **Selected Files Only**

By default, EnCase will search every byte of the evidence file. A search for **Selected Files Only** looks at only files, folders or devices that have been blue-checked. The Dixon box below the option shows the number of files to be searched.

- **Search each file for keywords**

To run a signature analysis or a hash analysis without running a keyword search, uncheck this box and make sure the desired option is checked.

- **Verify file signatures**

This option will conduct a signature analysis on all files, or selected files with the **Selected Files Only** option enabled. Refer to the section on *Signature Analysis* for further information.

- **Compute hash value**

This option will conduct a hash analysis on all files, or selected files with the **Selected Files Only** option enabled. Refer to the *Hash Analysis* section for further information.

- **Recompute hash value**

If selected, EnCase will recompute all previously computed hash values generated for the files of the replaced live device. This is most often used for acquisitions over the enterprise network, to recompute the values of the files on the live machine if a hash analysis was conducted previously. This option is not necessary for local acquisitions.

- **Search file slack**

If selected, EnCase will search the slack area that exists between the end of the logical files and the end of their respective physical files.

- **Undelete files before searching**

If selected, this option will logically “undelete” deleted files prior to searching. If a file is deleted, EnCase and other tools can determine if the assigned starting cluster is not assigned to another file (if it is assigned, then the file is Deleted-overwritten). The unallocated clusters after the starting cluster may or may not belong to the deleted file. Choosing this option assumes the unallocated clusters after the starting cluster do belong to the deleted file. This is the same assumption made when copying out a deleted file. Choose this option will find a keyword fragmented between the starting cluster and the subsequent unallocated cluster. If determining the presence of a keyword on the media is

critical to an investigation, the examiner should also search for portions of the keyword, including GREP expressions of fragments of the keyword.

- **Search only slack area of files in Hash Library**

This option is used in conjunction with a hash analysis or on an evidence file that has already had a hash analysis performed. If a file is identified from the hash library, then it will not be searched. However, the slack area behind the file (as described above) will be searched. If this option is turned off, EnCase will ignore the hash analysis while running the search.

- **Selected keywords only**

This option allows the search to include all or just a selected number of keywords. The display box shows the number of keywords that will be used in the search. Keywords can be selected and deselected from the Keywords tab available under the View pull-down menu.

Click the [**Start**] button to begin the search.

Viewing Search Hits

As search hits accumulate, results can be viewed by selecting the **Search Hits** subtab under **Cases**. Each keyword triggers the creation of a folder of the same name in which keyword matches are placed. **Keyword** folders are recognized by the Key icon.

Many analysis functions can be performed in **Search Hits** view without having to change to **Cases** view. Search hits can be viewed while a search is still running by hitting the [**Refresh**] button on the top toolbar. Since EnCase is constantly updating the search hits window during the search, the table cannot be sorted until the search is complete.

In **Search Hits** view, you can select the [**View Search Hits**] button on the top toolbar, or right-click in the table and select **View Search Hits**, to change the way the search hits are displayed.

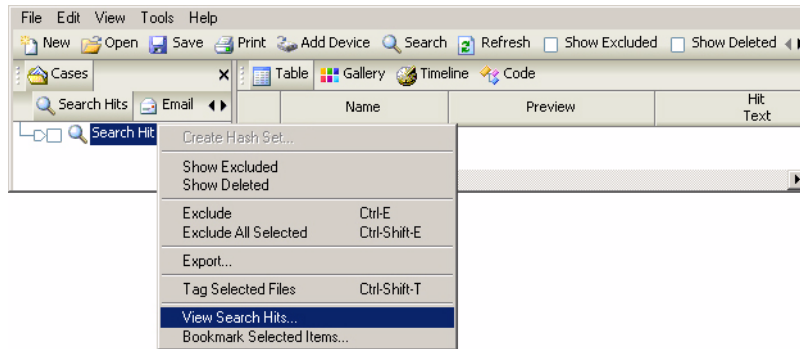


Figure 18-14: Viewing Search Hits

Search hits can be displayed and sorted by **Keyword** and/or **Device**. Blue check the option to display by. The **Arrangement** can be changed by left clicking on the desired icon and dragging it into place.

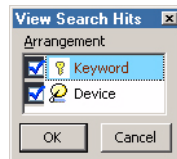


Figure 18-15: Organizing the Search Hits table

In the example below, the search results have been sorted by **Keyword**, with devices listed below the **Case**, and the keyword hits displayed under each device that has keyword search hits.

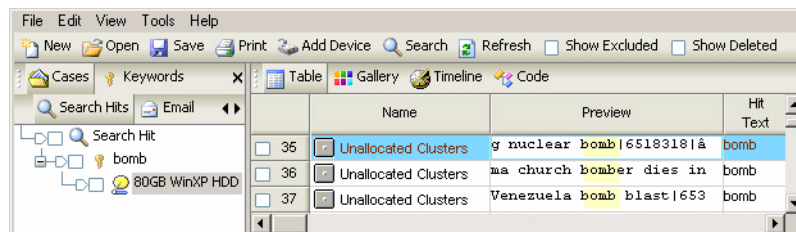


Figure 18-16: Keywords sorted by Keyword, then Device

Examiners can select search hits and perform a variety of tasks within **Search Hits** view. Right click in the table view in the **Entries** subtab to display the available options.

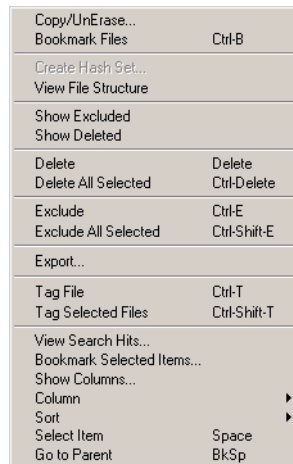


Figure 18-17: Search Hit options

- **Bookmark Files**

This option allows for bookmarking of one or more files found in the search. Bookmarking options appear once this option is selected - see the **Bookmarking** section later in this document for more information.

- **Create Hash Set**

By default, this option is grayed out unless Hash Analysis has been run through the **Search** feature. Refer to the chapter of this document on hash sets for more information.

- **View File Structure**

This option mounts the compound file containing the selected keyword.

- **Send To**

This option allows the Examiner to send the file containing the search hit to a file viewer configured through EnCase. This will only appear if a file viewer is configured.

- **Show Excluded**

This option (which also is featured on a button on the top toolbar) brings search hits that were previously excluded into view with the other search hits. By default, excluded search hits are displayed in red, although the color can be

changed in the **Colors** tab of the **Options** window, opened through the **Tools** pull-down menu.

- **Show Deleted**

This option (which also is featured on a button on the top toolbar) brings deleted search hits into view with the other search hits. If a parent folder is deleted, the children search hits below are all deleted, although they do not display the deleted icon overlay. See **Delete** below for more details.

- **Delete**

This option deletes the currently selected search hit. To undelete a deleted search hit, show all deleted files, right click on the deleted search hit and select **Delete**. This is a soft delete, and the user can undelete the search hit until the case is closed. If a keyword is deleted when the case is closed, the search hit is permanently deleted. Note that **Delete** does not delete the file from the evidence file, only from the case.

- **Delete All Selected**

This option deletes all selected search hits.

- **Exclude**

This option excludes the search hit from view, although the hit is not deleted from the case file. This feature replaces the Recycle Bin of EnCase Version 3, although it is superior in that it takes less resources from the examination computer and the search hits stay in the correct location, rather than being dumped into a central bin. To show the excluded search hit, see **Show Excluded**. Excluded search hits are indicated by a red **X** icon overlay and a red background on the search hit text in the table. Excluding the root keyword excludes all children search hits, although the children search hits do not receive the **X** icon overlay. Individual search hits can be excluded to help focus on relevant hits, without permanently deleting the “false” hits.

- **Exclude All Selected**

This option excludes all selected search hits from view.

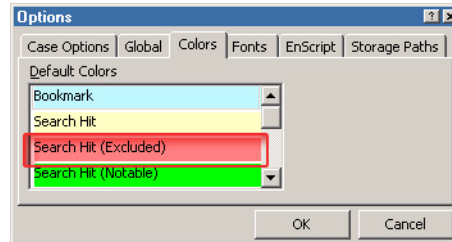


Figure 18-18: Excluded Search Hits default color

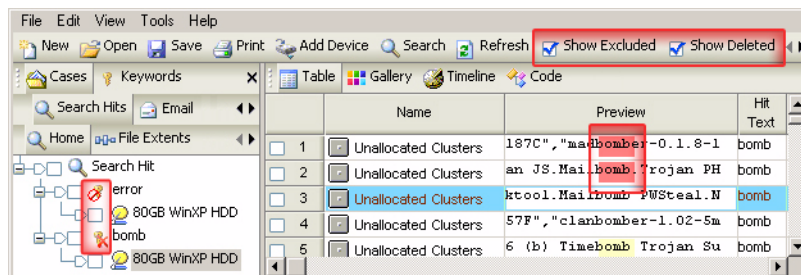


Figure 18-19: Deleted and Excluded search hits shown

- **Export**

This option allows the examiner to export out the data in the Table view into a tab-delimited text file, for import into Microsoft Excel or Access, or a similar program.

- **Tag File**

This option will blue check the file in the **Entries** subtab under **Cases**, in which the selected search hit is found. This allows the examiner to perform additional searches or run EnScripts just against those tagged files and the other previously blue checked files.

- **Tag Selected Files**

This option will blue-check selected files containing the search hits in the table when selecting the **Entries** subtab under **Cases**.

- **View Search Hits...**

This option (also a top toolbar button) will display the Arrangement window to allow for the rearrangement of the search hits displayed.

- **Bookmark Selected Items...**

This option will open a window to allow bookmarking of selected search hits.

- **Show Columns..., Column, and Sort**

These options allow the examiner to move, hide, or lock columns in the Table view, and sort the data in columns in ascending or descending order.

- **Select Item**

This option will blue check the selected search hit. Holding down the space bar will continue to select search hits entries until the space bar is released. When the case file is saved, the setting for selected search hits will be saved in the case file.

- **Go to Parent**

Selecting this option will move the selection in the Tree Pane up one level to the parent directory.



Be aware that any function performed on files in the Search Hits tab only affects the search hit itself; to perform a function on a file (such as creating hash sets, Copying\UnErasing, etc.), you will need to select the search hit, right-click and select Tag File. You can then perform the task on the files blue-checked in the Entries subtab.

Bookmarking Search Hits

To bookmark a file containing a search hit, right click on the filename and select **Tag File**. From the **Entries** subtab in **Cases** view, you can then right click on the blue-checked file and select **Bookmark Files**. You can also create a “sweeping text” bookmark of the search hit by selecting the appropriate text in the bottom pane, right clicking on the text and selecting **Bookmark Data**. Refer to the *Advanced Analysis* chapter for more information on creating bookmarks.

The Refresh Button

While a search is being run, although EnCase will report on the status bar in the lower right reports that it has found a number of search hits, they are not displayed when navigating to the Search Hits tab. This is because EnCase has not refreshed the display results. By pressing the [**Refresh**] button on the top toolbar, all search hits available at the time the button is pressed will be displayed in the table and the button will disappear. If additional search hits are discovered after the button is pressed, the button will reappear, to allow the table to be updated with the new search hits.

Canceling a Search

To cancel a keyword search, double-click the blue status bar in the lower-right corner of the screen. Click **[Yes]** in the dialog box that appears to cancel the search.

VIEWING COMPOUND FILES

A powerful feature of EnCase is the ability to view the individual components of compound files within an evidence file. Compound files are typically files that are comprised of multiple layers such as registry files, OLE files (such as Excel and Word), e-mail files (PST, DBX, etc.) and compressed WinZip. To view the structure of a compound file, right-click it and select **View File Structure**.

The **File Mounter** EnScript module allows the examiner to select a file type (DBX, GZip, PST, Tar, Thumbs.db or Zip) and have them mount automatically (provided they have valid signature matches).

Registry Files

The Windows registry contains valuable data that provides a great deal of information about the setup of the Subject computer. Registry files of Windows 95, 98, ME, NT 4.0, 2000, and XP computers can be mounted within EnCase by right clicking on the file and selecting **View File Structure**.

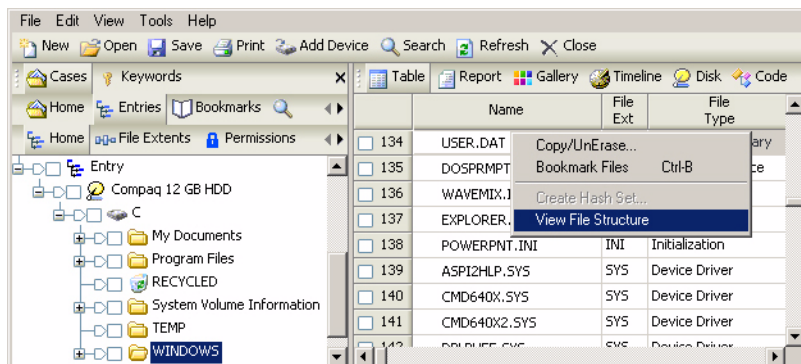


Figure 19-1: Mounting registry files

EnCase can calculate the unallocated space in the registry file by checking the appropriate box at the prompt, then clicking [OK] to continue parsing the file. The registry file will then be mounted in EnCase, and can be navigated in the same fashion as other folder structures. Keep in mind that this process can take a considerable amount of time

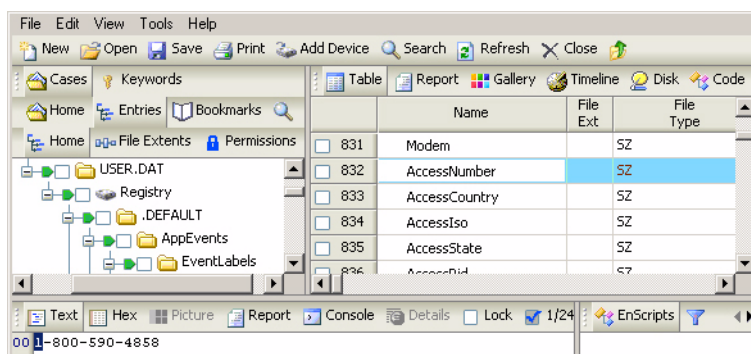


Figure 19-2: Viewing Registry File with EnCase

Windows 95, 98, and ME computers have two registry files. They are located in the system root folder, which is normally **C:\Windows**. The files are named **system.dat** and **user.dat**.

Windows NT 4.0, 2000, and XP divide the registry into four separate files. They are called **security**, **software**, **SAM**, and **system**. These files are stored in **C:\%SYSTEMROOT%\system32\config**.

OLE Files

OLE is Microsoft's Object Linked Embedded technology on which Microsoft's Office Suite of products is based. For example, it allows an Excel spreadsheet to be seamlessly embedded into a Word document. Microsoft Office documents that use this technology are layered compound files, which can be viewed at the layer level by right clicking on the file and selecting **View File Structure**.

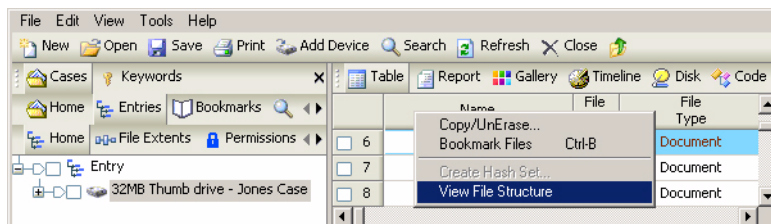


Figure 19-3: Mounting an OLE file

The file will be converted to a folder containing a file identified by a **Compound Volume** icon. Clicking on the icon displays the layers in the table. Information about the document, such as the created date and time, the version of the application that created it, any plain text within the document, and other metadata, is available further into the OLE directory structure. Highlight the data in **Text** tab of the bottom pane, right click and select **Bookmark Data**.

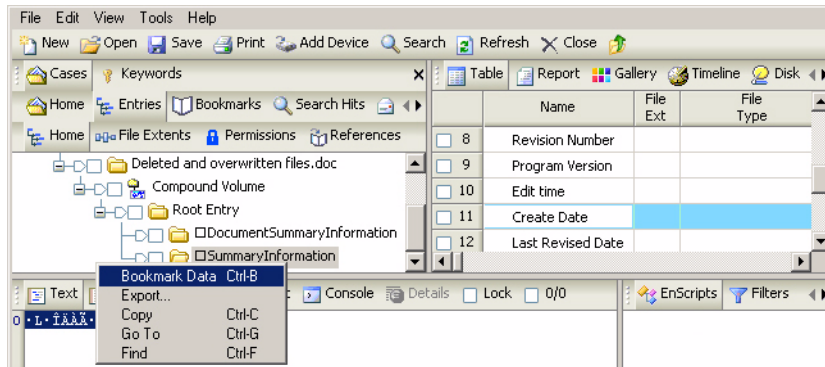


Figure 19-4: Extracting dates from an OLE file

In the **Bookmark Data** window that opens, select **Windows Date/Time** from the **Dates** folder in the **Data Type** window. The correct creation date should appear in the window at the bottom.

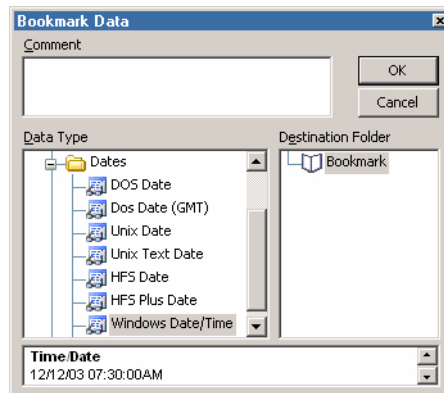


Figure 19-5: Extracting dates from an OLE file

Compressed Files

EnCase can mount compressed files in EnCase including WinZip (.zip) GZip (.gz) and Unix .tar files. To open a compressed file, right click on the file and select **View File Structure**. The contents are displayed as long as the container is not password-protected

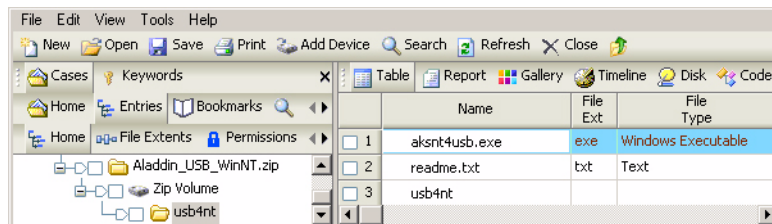


Figure 19-6: Mounted WinZip file



Only the modified date and times are shown on .gz and .tar files, as the compression processes do not store any other dates or times. GZip files are not labeled by name, only by their content file type and a .gz extension. For example, decompressing the file document.doc.gz displays the uncompressed document.doc file.

Outlook Express E-Mail

EnCase can read Outlook Express .DBX files folders by right clicking on the file and selecting **View File Structure**. The .DBX file is converted to a folder with the mounted DBX Volume beneath. The table in the right pane lists the individual e-mails by their subject line. The text of the selected e-mails is displayed in the bottom pane **Text** tab, and the e-mail is added to the **Email** tab.

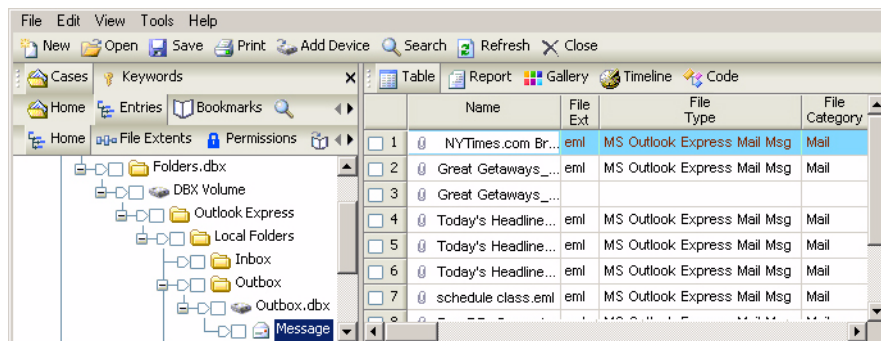


Figure 19-7: Viewing an Outlook Express .DBX file

Deleted e-mails and attachments can be retrieved from Unallocated Clusters. Alternately, you can view all Outlook Express E-mail automatically, using the **Search for Email...** option in the **Email** subtab below **Cases**, including deleted files and attachments. See the chapter on *E-Mail and Internet Artifacts* for additional information.

Base64 and UUE Encoding

EnCase will automatically display Base64 and UUE encoded attachments when the mail file is mounted. You can search for (and view) Base64 images as follows:

- In the **Entries** subtab below **Cases** view, blue check **Unallocated Clusters** in the table (normally located at the root of the volume).
- From the **View** pull-down menu, select **Keywords**. In the table (right pane), right click and select **New**.
- Enter **Base64** in the **Search expression** field, and then give the keyword a name. When you are finished, click **[OK]**.
- Blue check the new keyword in the table
- Click on the **[Search]** button on the top toolbar. Check **Selected Files Only**, **Search each file for keywords** and **Selected keywords only** (leave all other boxes unchecked), and then click **[Start]**
- From the **View** pull-down menu, select **Search Hits**.
- With the bottom pane in **Text** view, highlight the first character of the image, right click and select **Bookmark Data**.

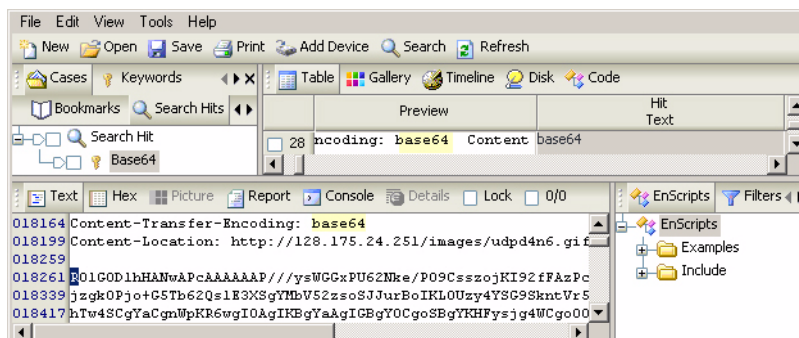


Figure 19-8: Book marking Base64 image

- In the **Data Type** window, select **Base64 Encoded Picture** (inside the **Picture** folder); the image should appear in the bottom pane.

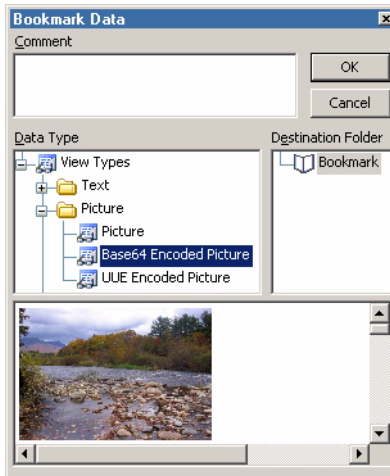


Figure 19-9: Book marking Base64 image

MS Outlook E-Mail

The process of mounting Outlook PST files is identical to that of Outlook Express as previously described. When EnCase mounts an Outlook PST file, messages are converted to an RTF (Rich Text Format) file (**message.rtf**.) The RTF file can be opened in word processing applications such as Microsoft Word. Foreign language messages can be displayed provided that the Microsoft Word Language Pack has been installed on the examiner's system.

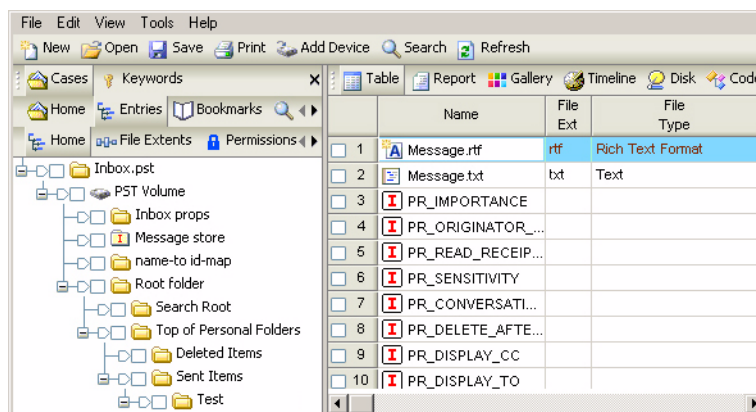


Figure 19-10: Mounted PST file

When expanded, the top level (or top root) of the .PST file directory contains multiple folders, including:

- Inbox props (properties)
- Message store (storage, containing the **PR_PST_PASSWORD** file and other IDs)
- Name-to-id-map
- Root folder, containing the following items:
 - **Search Root**: Reserved for future use
 - Top of **Personal Folders**, containing the **Inbox**, **Sent Items**, and **Deleted Items**

Each PST e-mail message file appears as a folder with all the message properties within the folder as well as any attachments associated with the e-mail message.



NOTES: Many of the fields within the .PST mail folder are duplicated, which is part of the .PST format. If a keyword is a match within a certain field, it will be duplicated in the secondary field as well. Created, written and modified dates are set by the e-mail messages. Outlook calendar entries (created, written and modified dates) are set by the calendar applications, but they do not reflect the actual date and time of the appointments, but when they were entered.

The message also appears in the **Email** subtab after mounting. Alternately, you can view all Outlook E-mail files automatically by using the **Search for Email...** option in the **Email** subtab below **Cases**, including deleted files and attachments. See the chapter on *E-Mail and Internet Artifacts* for additional information.

NTFS Compressed Files

EnCase mounts, views and searches NTFS compressed files in a plain-text format by detecting when a file has been compressed and automatically decompressing the file for easy analysis.

Search Compressed NTFS Files and Folders

The searching function within compressed files and folders has been greatly enhanced. The data within the files is displayed in the uncompressed format in the Text and Hex views of the bottom pane.

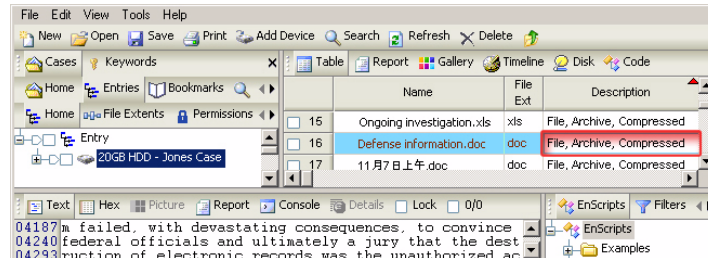


Figure 19-11: Uncompressed file with search hits

The examiner can view the uncompressed data of the file in the Disk view.

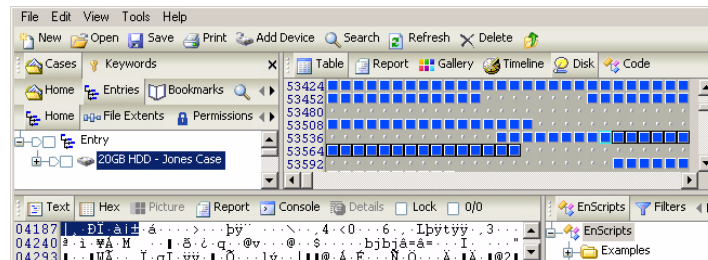


Figure 19-12: Uncompressed data in Disk view

Thumbs.db

EnCase supports parsing Windows' thumbs.db cache for images, web pages and other files. To mount **thumbs.db**, right-click **View File Structure**. The **Thumbnail Cache Volume** and the version appear. V2 thumbnails are in bitmap format, whereas later versions are in a modified .JPGs. The **Root Entry** folder contains the **Catalog** file of cached thumbnail names, their full path, and the cached images themselves. **Thumbs.db** also contains a record of the image's **Last Written** date.

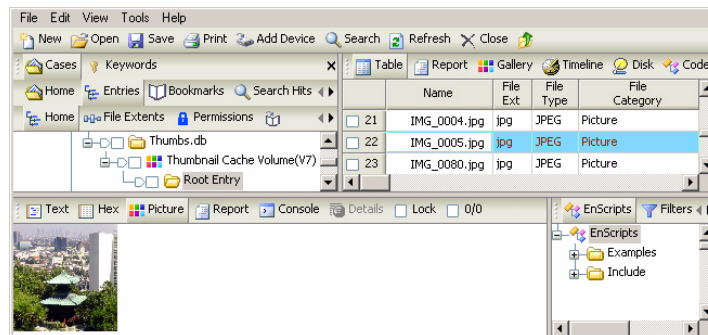


Figure 19-13: Cached thumbnails

ENSCRIPT AND FILTERS

EnScript is a programming language and Application Program Interface (API) that has been designed to operate within the EnCase environment. Although compatible with the ANSI C++ and Java standard for expression evaluation and operator meanings, EnCase contains only a small subset of C++ features. In other words, EnScript uses the same operators and general syntax as C++, though classes and functions are different. EnScript allows investigators / programmers to develop utilities to automate and/or facilitate forensic investigations. They can also be compiled and shared with other investigators. A programming background and an understanding of object-oriented programming are helpful to code in EnScript. An *EnScript User Manual* and *EnScript Programmer Reference* are available for download at <http://www.guidancesoftware.com>. In the Support section, select the Downloads page.

To access EnScripts, select **EnScripts** from the **View** pull-down menu,. When you select a folder in the Tree Pane, the available scripts appear in the Table Pane. EnScripts can also be run directly from the Filter Pane in the bottom right of the EnCase application window. Activating the **Set Include** trigger shows all scripts in subfolders in the table. An **EE** folder appears in the tree that contains scripts specific to EnCase Enterprise. By default, a **COM** folder is present, containing examples of script types and how they work. EnScript modules can be run by executing an EnScript such as Sweep Enterprise or Sweep Case.

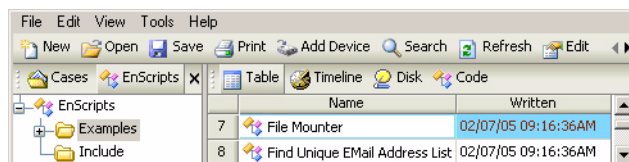


Figure 20-1: The EnScripts tab

EnScript Path

EnCase installs default EnScripts in **C:\Program Files \ EnCase5 \ Scripts \ Examples**. To set the path to access scripts from another location:

- Right-click on the root folder or one of the scripts in the left pane and select **Change Root Path....**

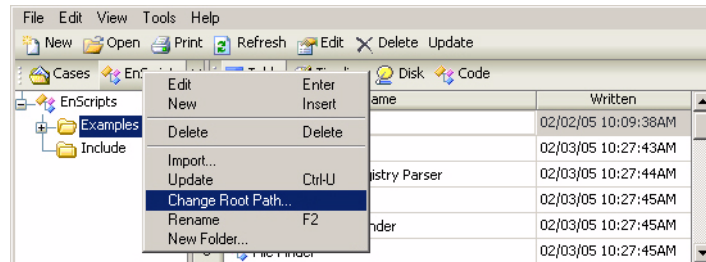


Figure 20-2: Changing the root path

- Browse to the correct folder for the EnScripts and click **[OK]**.

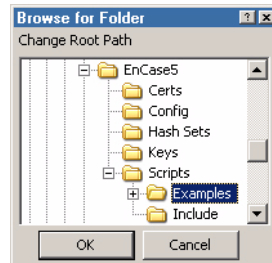


Figure 20-3: Setting the root path

Include Folder

Different scripts may have common functionality. Rather than have two scripts duplicate the same code, they often share code from a single file. By default, the code is placed in **C:\Program Files\EnCase5\Scripts\Include**.

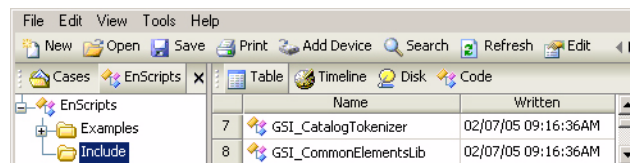


Figure 20-4: Common scripts

These scripts cannot be run like the ones in the **Examples** folder; they are only used for writing other scripts. If you move the **Include** folder, you will need to update the path by clicking on the **EnScript** tab after selecting **Options** from the **Tools** pull-down menu. Type the path, relative to the EnScript root path, in the **Include Path** field at the bottom. When writing scripts, you should put included files in the same folder as the main script or in a subfolder, since each time you upgrade EnCase, the EnCase installer will overwrite any custom scripts stored in the **Examples** or **Include** folder.

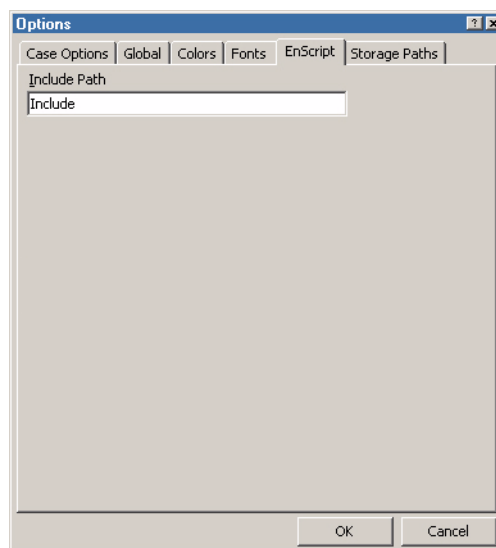


Figure 20-5: Changing Include path

Running EnScripts

To run an EnScript, double-click on the script name in either the table or the Filter Pane. Alternately, you can click on the [**Code**] button with the EnScript selected, then click the [**F9**] key or the [**Run**] button on the top toolbar.

Editing EnScripts

To edit an EnScript, right click on the script name in either the table or the Filter Pane and select **Edit Source** (a pencil overlay will be added to the middle of the EnScript icon). You can edit the source code in the right pane, if desired. If you have made any changes or created a new EnScript, it is a good idea to click on the [**Compile**] button on the top toolbar before running the script to verify that there are no errors. This option runs the code without executing the EnScript.

To close an EnScript, select the subtab under **Code** for the script you wish to close in the Table Pane, then click on the [X] to the right of the tab. Alternately, you can right click on the tab and select **Close Tab** or hit [Ctrl][F4].

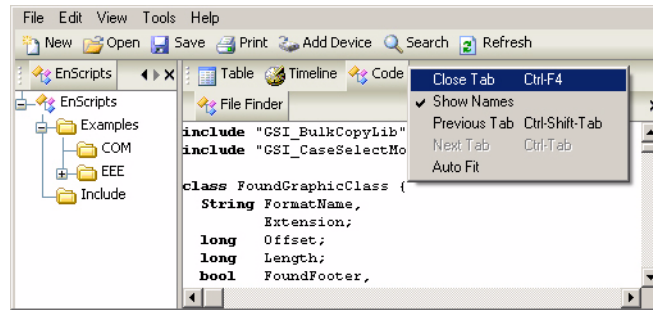


Figure 20-6: Closing an EnScript

To move or copy an EnScript to another (or the same) folder, hold the right mouse button down on the script, drag and drop it to the desired folder, then let go of the mouse button. You can then select **Move Here** or **Copy Here**. If the EnScript is being copied to the folder in which it already resides, it will be created with a number after the name (e.g., **File Finder1**).

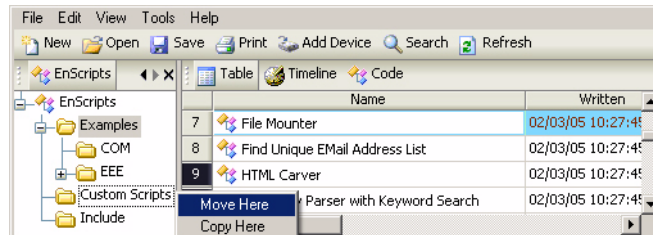


Figure 20-7: Moving or Copying an EnScript

Console

The **Console** tab in the bottom page displays the results of EnScripts that send output to the console. This information is also appended to **C:\Program**

`Files\EnCase5\console.txt`, which you can view by opening the file in WordPad or Notepad.

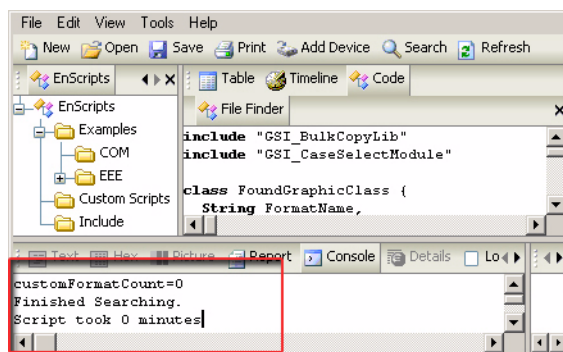


Figure 20-8: Viewing results in the console

The EnScript Library

To keep the EnScript library current, download the latest updates from <http://www.guidancesoftware.com> from the Downloads page in the Support section. Only EnScripts created by Guidance Software are available from this site. There is also useful information concerning EnScripts at the Guidance Software's EnScript Forum message board.



EnScript macros are executable files and should be treated with the same caution as any other executable file received from a third party. Like other executable files, it is possible to intentionally write EnScripts with malicious code or to imbed viruses within the code of an EnScript. It is imperative that you only obtain “free” EnScripts directly from Guidance Software or from a clearly identified source that you trust. EnScripts received from third parties should be screened for viruses. Guidance Software disclaims any representations, warranties, express or implied, regarding EnScripts provided on site including their fitness for a particular purpose, their quality, their merchantability, or their non-infringement. Guidance Software does not warrant that any EnScripts posted on this site are free from bugs, errors, or other program limitations. By utilizing any EnScripts provided on this site, you agree that Guidance Software will not be subject to liability for any bugs or damages caused by EnScript macros, including EnScripts intentionally written by third parties with malicious code and/or computer viruses. For full details on EnScript, please see the *EnScript Language Reference*, available from Guidance Software's web site at www.guidancesoftware.com

Filters

The Filter Pane allows investigators to run, create, edit or delete Filters, Conditions and Queries. The new **Conditions** tab allows the user to build filters by simply specifying parameters. Where filters require the user to enter code for the filter conditions, the new tab allows the user to create filters based on pre-set conditions,

selectable from a menu. Filters and Conditions can be combined into queries through the **Queries** tab.

Filters, including Conditions and Queries, determine the amount of information displayed in most areas of the EnCase interface. They are similar to EnScripts in that they use the EnScript syntax, though they typically are much shorter. All filters are stored in an initialization file (**C:\Program Files\EnCase5\Config\filters.ini**). This means that filters are saved globally within EnCase. To ensure that all copies of EnCase within a test environment have the same filters, copy **filters.ini** to all computers with EnCase installed. Any changes or additions to filters within EnCase automatically update **filters.ini**.

Editing Filters

Filters may be opened and edited even when EnCase does not have a case open. To edit a filter, right click on the filter name and select **Edit**.

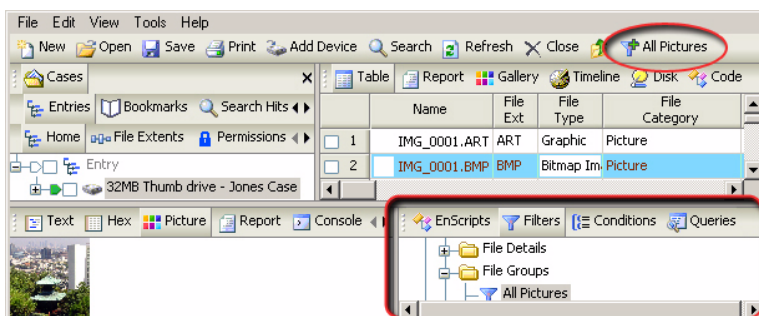


Figure 20-9: Filter Pane

Starting and Stopping Filters

To use the filter functionality, double-click on the appropriate item in the Filter Pane, or right click on the item and select **Run**. When the filter is activated, it appears on

the top toolbar with a green plus sign to indicate it is running. To stop a filter, click on the icon until the plus sign becomes a red minus sign.

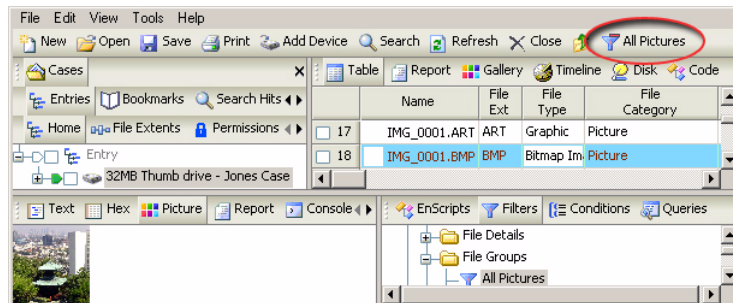


Figure 20-10: Stopping a filter

Creating a Filter

A new filter can be created by right clicking in the Filter Pane and selecting **New**. After naming the filter, you can edit it by right clicking and selecting **Edit Source**. Syntax for EnScript and Filters is covered in the *EnScript Language Reference*, available from Guidance Software's web site at <http://www.guidancesoftware.com> from the Downloads page in the Support section.

Creating a Condition

To create a condition, right-click on the root of the **Conditions** tab and select **New**. Enter the desired name in the **Name** field, then right click on the **Main** icon in the tree and select **New**. Assign a name in the **Function Name** field and then select a **Property** (which corresponds with a table column header). The available **Operators** for that property appear on the right. Values for the operator are entered in the provided field. If you wish to be prompted to input the value while running the filter, check the box labeled "**Prompt for value.**" You can also specify with a check box whether or not you wish to make the value case sensitive. Clicking on the **Edit Source Code** box allows the user to edit the code in the adjacent tab. Only examiners experienced with creating filter code should use this option. Once the condition is properly configured, click on the [OK] button.

As with filters, Conditions can be combined using the **Queries** tab in the Filter Pane.

Queries

Queries can be run, edited, added, renamed, and deleted in the same manner as Conditions.

ADVANCED ANALYSIS

Recovering Partitions

Occasionally a device has been formatted or even FDISKed in an attempt to destroy evidence. Formatting and FDISKing a hard drive does not actually delete data. Formatting deletes the structure indicating where the folders and files are on the disk. FDISKing a drive deletes a drive's partition information. EnCase can rebuild both partition information and directory and folder structure.

Adding Partitions

A formatted and/or FDISKed hard drive should be acquired using normal procedures. Add the evidence file to a new case within EnCase.

- A formatted drive will display logical volumes within EnCase, but each volume will have only an **Unallocated Clusters** entry in the table.
- An FDISKed drive will not show logical volume information. The entire drive will be displayed as **Unused Disk Area** in the table.

Restructure these portions of the disk as follows:

- Expand the **Examples** folder in the lower right pane in EnCase.

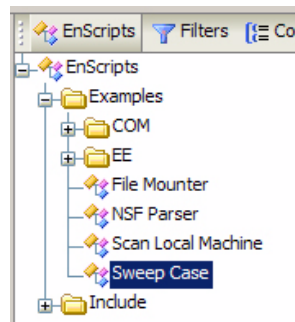


Figure 21-1: Expanding Examples

- Double-click the **Sweep Case EnScript**.
- Check the case you are working on and click **Next**.

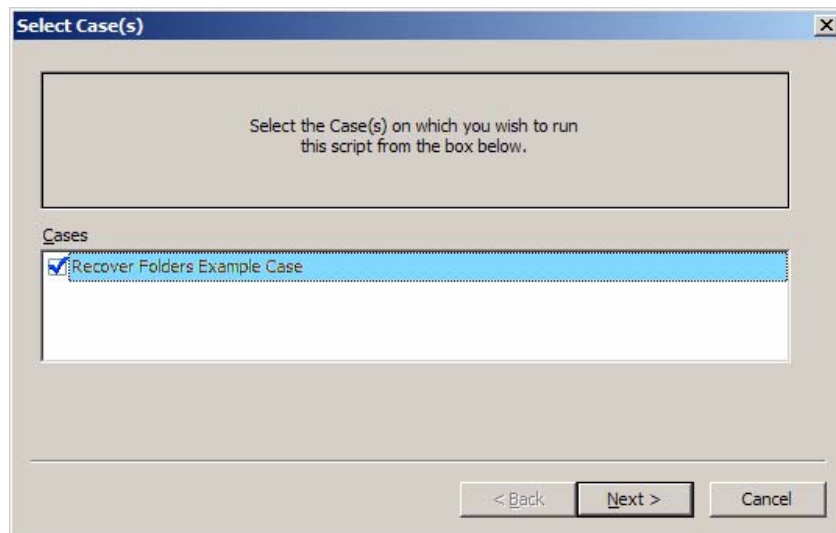


Figure 21-2: Sweep Case - Select Case

- Enter a Bookmark Folder name and optionally, a Folder Comment.

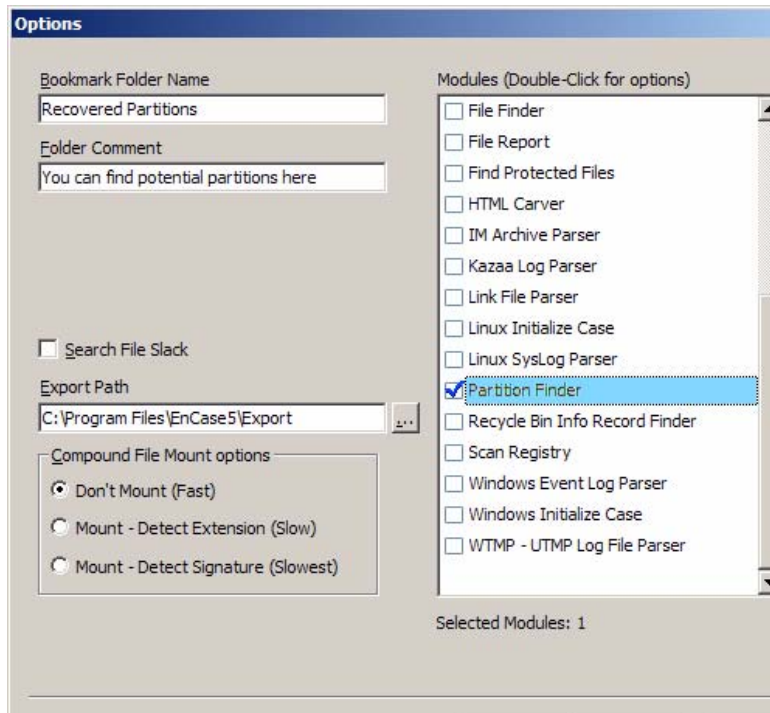


Figure 21-3: Sweep Case - Selecting Modules

- Find and check the **Partition Finder Module** in the right list.
- Click **Finish** to run the EnScript.
- When the Enscript has run, click the **Bookmarks** tab at the top of the upper left pane.

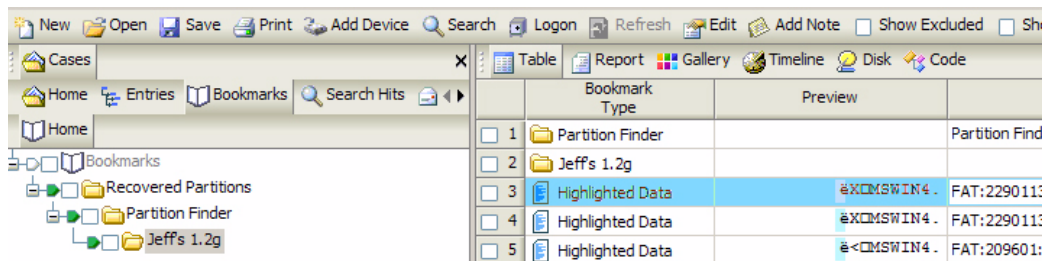


Figure 21-4: Bookmarks Results

- Click the Homeplate icon to show all the bookmarks the EnScript has found. Note the partition type and size in the comment, in this case a FAT partition of size 229 113 bytes.
- Highlight the entry in the right pane.
- Select **Disk View** in the right pane, where the sector with the found partition is outlined in aqua.

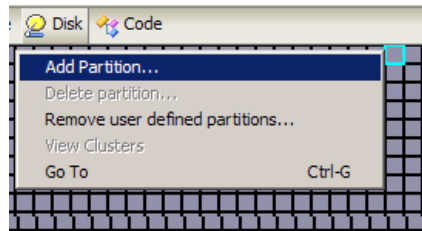


Figure 21-5: Disk View - Add Partition

- In that sector, right click and select **Add Partition**.

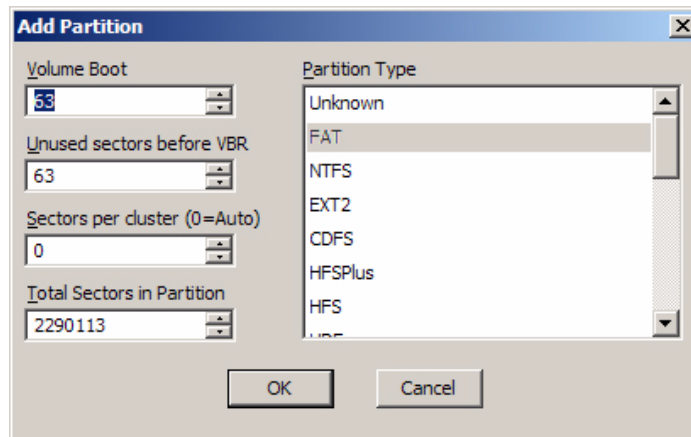


Figure 21-6: Add Partition Dialog

- The Add Partition screen detects the sectors and partition type automatically, populating the fields. Click [OK] to restore the partition.
- Select the **Entries** view in the left pane to see the contents of the partition you just added.

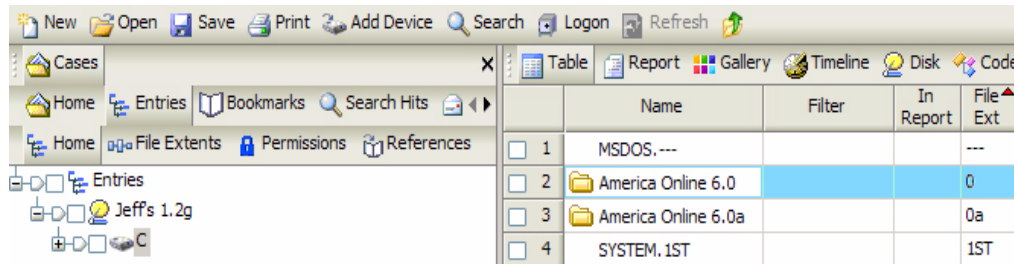


Figure 21-7: Partition added

- If the drive had multiple partitions, select **Bookmarks** in the left pane and **Table** view in the right pane. Select the next bookmarked partition, return to the **Disk** view window and repeat the above process.

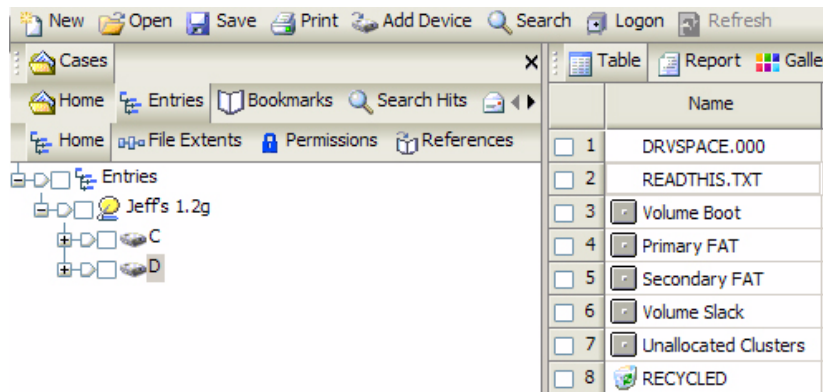


Figure 21-8: View both partitions

Deleting Partitions

To delete a partition (if, for example, a partition was created at the wrong sector), the entry must be deleted at the sector at which it was created on the evidence file image of the hard drive. Delete the partition as follows:

- In **Disk** view, navigate to the **Volume Boot** record entry (indicated by a pink block).
- Right click and select **Delete Partition....**
- Click [**Yes**] to confirm the removal of the partition.
- Return to Table view. The partition will be replaced in the table by **Unused Disk Space**.

Recovering Folders from a Formatted Drive

If the evidence file shows a logical volume but has no directory structure, the hard drive has probably been formatted. If this is a FAT-based system, EnCase can recover the original directory structure. Right-click on each logical volume and choose **Recover Folders**. This will search through the drive and recover folders, subfolders and files from within those folders if all that information is still available.

Occasionally, a device may be encountered containing a file system unsupported by EnCase. When this occurs, EnCase will display the device icon, but the table will only list Unallocated Clusters. Although there is no way to view file structure, it may be possible to run text searches through the Unallocated Clusters.

Web Browsing History

Often it is possible to recreate web pages that the subject visited. Refer to the *E-mail and Internet Artifacts* chapter of this manual for additional information on extracting Internet artifacts.



Warning! It is a good idea to disconnect the lab computer from the internet to avoid inadvertently downloading images and overwriting any content extracted from the evidence file.

To see the HTML pages still stored on the hard drive:

- Activate the **Set Include** trigger in the **Entries/Home** subtab under **Cases**.
- With the Table Pane in table view, double-click on the header for **File Ext** to sort by that column's entries.
- Click in the **File Ext** column and type "**HTM.**"
- Double-click an HTM or HTML file. The file will be copied to the storage hard drive and opened with the default browser. In most instances, the browser will

display a page with the HTML text intact, and the images replaced by white boxes with a red X.

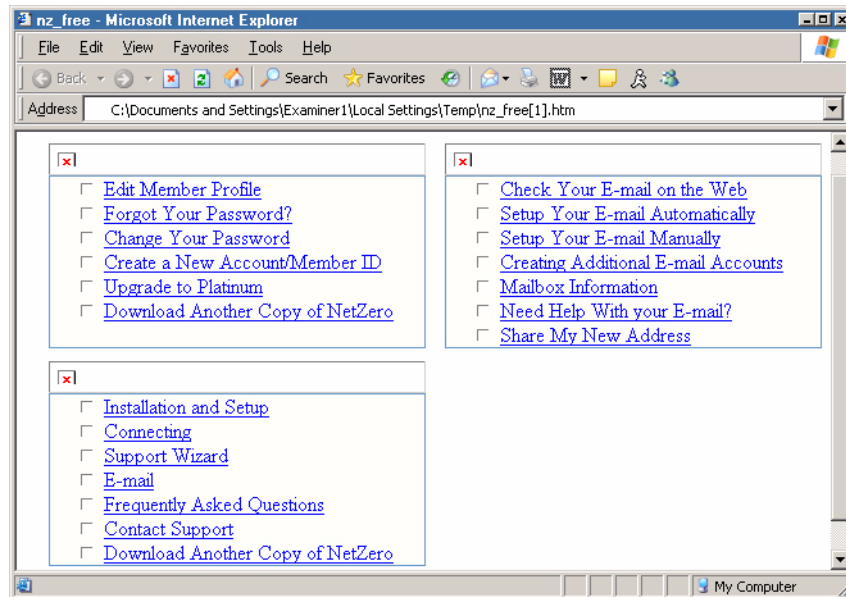


Figure 21-9: HTML document with missing images

Although the web page is open and being viewed from the investigating computer, the graphics for the web page are not yet available. To locate and match the missing images, the name of the file must be located.

- Right click on a white box and select **Properties**. Note the file name and file path.

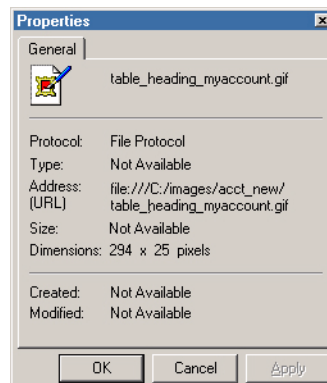


Figure 21-10: Properties of a missing web image

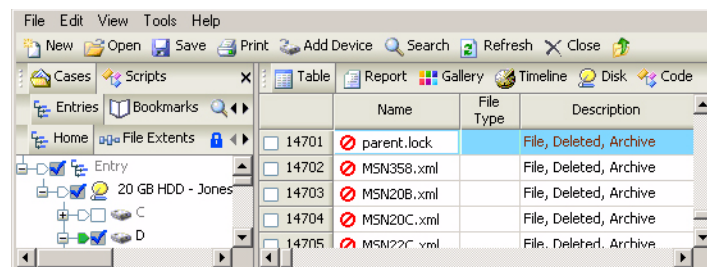
- In the table, find the image specified; you can sub-sort by **Name** to make it easier to locate.
- Right click on the image and select **Copy/UnErase...**, saving it to the local drive. Unless specified, EnCase will copy the file to the **Default Export** folder. To see the web page as it was originally laid out with the images, *the directory structure used to create the web page must be recreated*. Once the directory structure has been recreated, and the images moved to the appropriate directory, the web page is displayed as the subject originally saw it.

You can also use the History and WebCache features as described in the chapter on *E-Mail and Internet Artifacts*.

Reading What the Subject Threw Away

Computer users invariably delete data. However, when data is placed in the Recycle Bin, and the Recycle Bin is subsequently emptied, that data is not deleted. Rather, the pointers to the data are deleted; the data is still intact, but no longer allocated.

Because the data is not necessarily overwritten, EnCase can potentially recover deleted files (anything that was in the Recycle Bin at the time of acquisition, for example), and other files that might have pointers intact.



	Name	File Type	Description
<input type="checkbox"/>	14701	parent.lock	File, Deleted, Archive
<input type="checkbox"/>	14702	MSN358.xml	File, Deleted, Archive
<input type="checkbox"/>	14703	MSN20B.xml	File, Deleted, Archive
<input type="checkbox"/>	14704	MSN20C.xml	File, Deleted, Archive
<input type="checkbox"/>	14705	MSN22C.xml	File, Deleted, Archive

Figure 21-11: Recovered information

Even if files are emptied from the Recycle Bin and then deleted and overwritten, it is still possible to find records of those files within INFO2 files. The date/time stamp for when a file was deleted is recorded in the INFO2 file.

INFO2 files can be recovered from both allocated and unallocated clusters. Look for INFO2 files by sorting the table by file name.

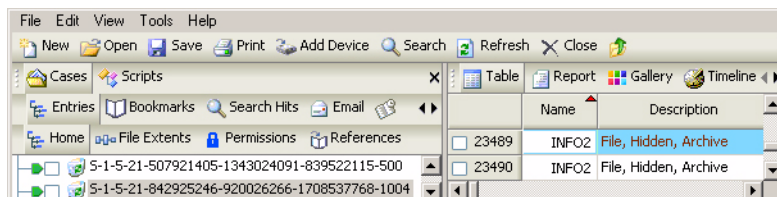


Figure 21-12: Locating INFO2 files

When a user empties a Recycle Bin, the INFO2 file is deleted as well. To recover deleted INFO2 files, run the **INFO2 Record Finder** EnScript, which searches unallocated clusters of the media and file slack to recover Recycle Bin records. Recovered records will then appear under **Bookmarks**, viewable in the proper format.

Making Sense of a DriveSpace Volume

DriveSpace volumes are only recognized as DriveSpace volumes after they have been acquired and mounted into EnCase. On the Storage computer, mount the DriveSpace file as a volume, and then acquire it again to see the directory structure and files. To do this, use the following procedure:

- A FAT16 partition must exist on the forensic PC to which you will copy / unerase the DriveSpace volume to. If one does not exist, create one. A FAT16 partition can only be created with a FAT16 OS (such as Windows 95). Create a Win95 or DOS 6.22 boot disk and use it to boot the storage computer.
- Run **FDISK** to create a partition, then exit, reboot, and format the FAT16 partition using format.exe.
- Image the DriveSpace volume.
- Add the evidence file to a new case in EnCase and search for a file named **DBLSPACE.000** or **DRVSPACE.000**.
- Right-click the file and copy/unerase it to the FAT16 partition on the storage computer.
- In Windows 98, go to the [Start] button and select **DriveSpace** from **System Tools** under the **Accessories** Program group.
- Launch DriveSpace.
- Select the FAT16 partition containing the compressed “.000” file.

- Select **Advance**, and then **Mount**.
- Select **DRVSPACE.000** and click **[OK]**, noting the drive letter assigned to it.
- In EnCase, the Compressed Volume File (**.000**) from the previous drive will now be seen as folders and files in a new logical volume. Acquire this new volume.
- Create the evidence file and add to your case. It is now possible to view the contents of the compressed drive.



An investigator may encounter this situation if the operating system of the evidence file is Windows 98.

Cracking Encrypted or Password Protected Files

If an encrypted or password-protected file is found, at the moment, a third-party utility must be used to crack the file. Copy / unerase the file to the storage hard drive and attempt to crack the file. Please see the appendix regarding *Third Party Utilities* for a list of different utilities helpful to the forensic examiner.

System Snapshot

The System Snapshot feature allow you to see all open files, processes and ports on the local system, effectively capturing volatile data. With EnCase Forensic, this can only be done with the local (forensic) machine using the **Scan Local Machine** EnScript; EnCase Enterprise or FIM allow the snapshot to be performed on a live preview of a remote machine using a different EnScript.

Volatile Data Defined

Volatile data exists in the main memory (RAM) of a server or workstation. If power is lost, or if a system fault occurs the data is lost. By contrast, static data is stored on hard drives, USB devices, CD's, etc., and is typically not lost when a loss of power or a system fault occurs.

A computer tracks numerous items that could be critical during incident response activities including; users on a system, TCP and UDP port information, open files, running processes and applications, and system resource utilization. Much of this information is contained within volatile data and is used by the system for administration and processing purposes. Snapshot captures this volatile data and provides information on what was occurring on a system at a given point in time.

During or after an incident, volatile data may reveal invaluable information. Are any ports open that should not be? Are unfamiliar services or machines accessing the system? Are unknown applications or processes executing? This information helps the examiner determine what is happening on the system at the current point in time, and if an attack is active.

The correlation of volatile data and static data is essential, but not exhaustive to the incident response process. Volatile data will help an examiner determine if suspicious activities or applications are active on a system, and help guide the examiner to search for backdoors or malicious code. Additionally, it may help the examiner determine who and what is accessing the system and its resources whether internal or externally. The most critical aspect of volatile data capture is it provides the examiner with the ability to quickly ascertain if unauthorized ports, processes or applications are active. This information is critical when deciding whether to continue system operation or take the system out of service. This is a crucial component of incident response triage; the ability to rapidly determine to what extent, if any, a system has been compromised.

Volatile Data Components

- **Open Ports**

Open ports are the active endpoints to a logical TCP connection on a system at a particular point in time.

- **Active Processes**

Active processes are the executables that are running on a computer at a particular point in time.

- **Open Files**

Open files are the files that are in use on a computer at a particular point in time.

- **Live Windows Registry**

Live Windows Registry keys are those that are active only during the logged on user's session.

Volatile Data Capture Using Snapshot

EnCase Forensic has the capability to capture volatile data from the local machine only. The examiner can view active processes, open ports and open files, and the live Windows Registry.

Organizations should have a thorough understanding of typical volatile data values for their environment including; authorized and utilized ports, authorized applications, and clearly documented file access privileges. Provided an organization has this understanding, it is easy to see how an examiner could quickly locate unauthorized sessions, services and applications by using Snapshot to acquire and analyze volatile data.

Running the Snapshot locally on the examiner machine provides the same type of information as is available when run across the network, but the data is limited to the examiners machine only.

	Name	Protocol	Local Address	Local Port	Remote Address
<input type="checkbox"/>	2	epmap	TCP		135
<input type="checkbox"/>	3	isakmp	UDP	500	
<input type="checkbox"/>	4	isakmp	UDP	500	
<input type="checkbox"/>	5	microsoft-ds	UDP	445	

Figure 21-13: Snapshot results on local machine

Open Ports

Open ports are ports that are currently in use or waiting for use by an application. As mentioned previously, organizations should have a thorough understanding of ports that are authorized and utilized within their organization on a per machine basis. Open port information will help the investigator understand who or what is communicating with a system at a particular point in time. Many times when a machine has been compromised, or is being compromised, there is communication occurring over open ports. Hackers and malicious employees often attempt to gain access to a computer by searching for open and vulnerable ports to exploit.

The examiner also has the ability to filter the results in the top right pane to meet certain specified criteria. The **Filter** and **Query** functionality in EnCase enables the examiner to target certain types of information and to narrow down the results shown in the top right pane. Numerous filters are provided with EnCase. New filters can be created and existing filters can be modified at any time by the examiner.

Open Ports Table Columns

- **Name**
Name of the service or port number.
- **Filter**
Visual indicator if the information viewed is the result of a running filter.

- **In Report**

Indicates whether or not the entry will appear in the **Report** view.

- **Protocol**

Indicates the protocol (OSI Layer 4) the port is using to communicate.

- **Local Address**

If the port is tied to a designated IP address, it will be indicated here.

- **Local Port**

This is the port the process is tied to.

- **Remote Address**

If there is a remote IP address connected to the indicated port, the IP will be visible here.

- **Remote Port**

If there is a remote machine connected to the port, the communication port on the remote machine will be present here.

- **State**

This indicates the status of the port. Options here are **Listening** (waiting for a connection), **Established** (an active connection to the port exists), **Time_Wait** (the process is waiting for additional information) and **Unknown** (UDP is stateless).

- **Process ID**

An integer used by the Operating System

Active Processes

Active processes are processes that are currently running on a system. This information is critical when trying to identify if rogue or unauthorized processes are active on a system. The Snapshot provides the ability to view active processes.

In the **Processes** tab, with the select all (**Set Include**) box (green home plate-like box) checked, all running processes on machine can be viewed in the right pane. The **App Comment** (Application Comment) field shows processes that are identified as authorized applications that are commonly used for malicious purposes.

EnCase is able to identify the malicious programs via a hash analysis, comparing the application's unique digital fingerprint (hash value) that had been pre-calculated and stored in EnCase by the examiner, with the hash value of that program that was calculated by EnCase and then captured during Snapshot. Since the hash value matches, EnCase returns the predefined Application Descriptor (**App Descriptor**) and Application Comment (**App Comment**) values, identifying the application on

the suspect computer. **Application Descriptor** provides categorization of executables via hash values, which enables the examiner to positively identify executables running on a system via a hash value match. **Application Descriptor** works in concert with Machine Profile, which contains an inventory of what should be running on a specific machine. Together the **Machine Profile** and the **Application Descriptor** let the examiner know what should be running on a specific computer and what is actually running on that machine. The examiner can identify directories, commands that were entered, times, and more.

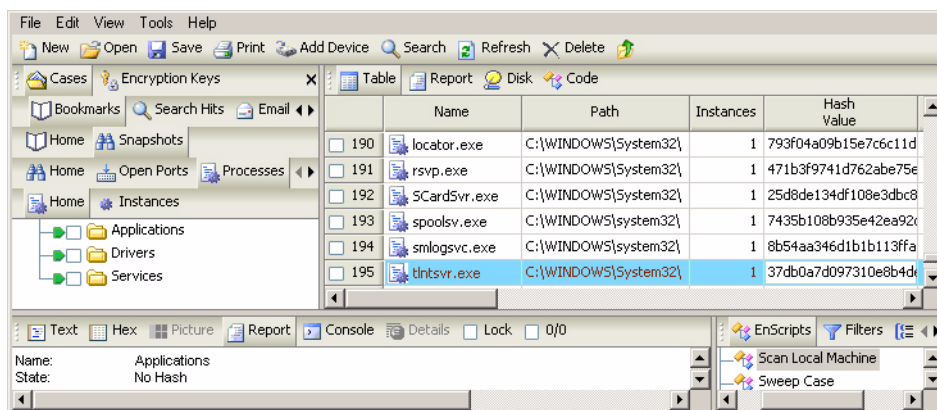


Figure 21-14: Active Processes

Processes Table Columns

- **Name**
Name of the process.
- **Filter**
Visual indicator if the information viewed is the result of a running filter.
- **In Report**
Indicates whether or not the entry will appear in the Report view.
- **ID**
This is the process ID (PID) assigned by the Operating System.
- **Parent ID**
This is the Parent Process ID (PPID) in the event that the viewed process was spawned by another process.
- **User ID**
In Linux and Windows this is the ID of the User who spawned the process.

- **Current Directory**

This is the current working directory.

- **Root Directory**

On a Linux system, this is the root directory for the machine.

- **Command Line**

These are the parameters that were passed when the process was started.

- **Executable**

This indicates the location of the binary executable, which spawned the process.

- **Start Time**

This is the date and time the process was started.

- **Hash Value**

MD5 Hash value for the process.

- **Hash Set**

If the hash value of the process is contained in the Hash Library, the hash set that includes the hash value will be listed here.

- **Hash Category**

If the hash value is included a hash set of the Hash Library, the category of the hash set will be listed here.

- **App Comment**

Comments that are associated with an **App Descriptor** (if applicable).

- **Profile**

This will list the Profile which includes the process (if applicable).

- **State**

This is the state of the process in regards to the App Descriptor. The 3 possible entries are:

- **No Profile**

The process hash is not assigned to a machine profile.

- **No Hash**

No hash value has been assigned to the process.

- **Approved**

The process has been assigned to an .app descriptor and included in the current profile.

- **Not Approved**

The process has been hashed, but is not included as part of the current machine profile.

Open Files

Open files are files currently in use on a system in relation to an active executable. This information is critical when trying to identify what person or process is accessing files on a system. Understanding what files are open provides an examiner with an understanding of what information a perpetrator or application is accessing. The Snapshot provides the ability to view and document open files.

In the following screen shot, the **Open Files** tab has been selected in the left pane. The right pane shows the open files that are in use by the process '.', sorted by file name.

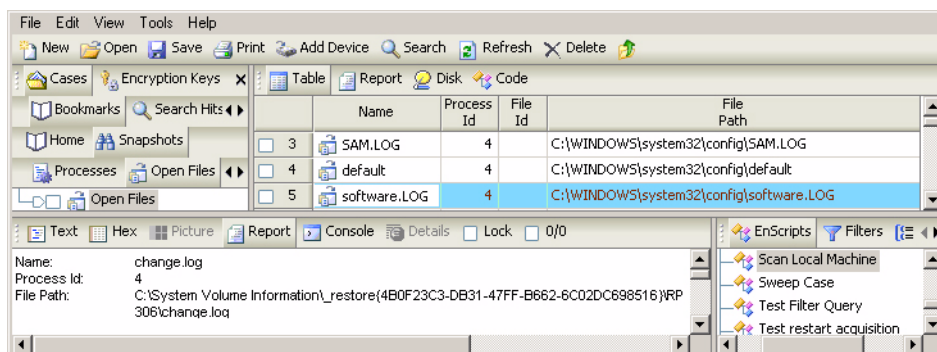


Figure 21-15: Open Files

At this point, the examiner has a lot of information regarding the rogue process running on the suspect computer. However, the examiner wishes to further investigate by examining data on the suspect computer's hard drive. To do so, the examiner 'Previews' the suspect computers drive contents with EE to analyze the contents of the computers drive media. Data that is actually stored on drive media (i.e. not in RAM) is considered static data.

Analysis of static data includes analyzing file systems, memory dumps, system logs, network data, operating system artifacts and much more, from drive media. EnCase provides robust functionality to examine the drive contents (static data) of suspect machines.

Network Interfaces and Users

Other data available in a Snapshot include the network card(s) in the machine and Windows users from the live registry.

The **Network Interfaces** tab includes information on the network interface card manufacturer, the assigned IP address, MAC address, and subnet mask.

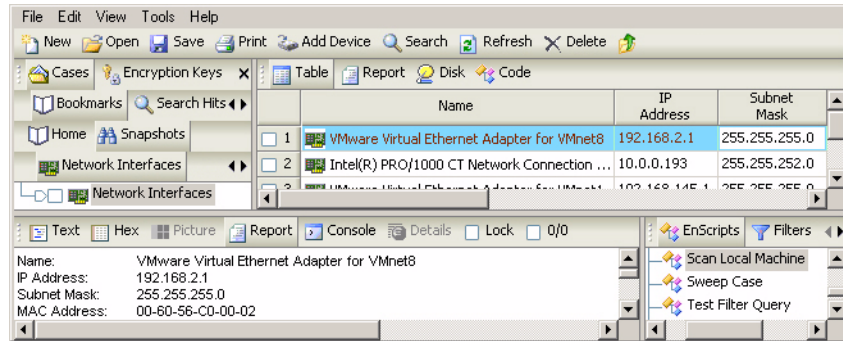


Figure 21-16: Network Interfaces

The **Network Users** tab has information about the all users who have logged onto a machine, including the user name, Security ID, and last date/time of login.

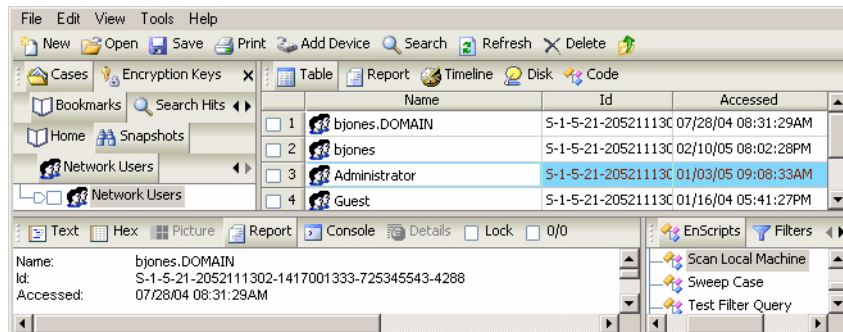


Figure 21-17: Network Users

This allows the examiner to create a Timeline of the login activity of Network Users.

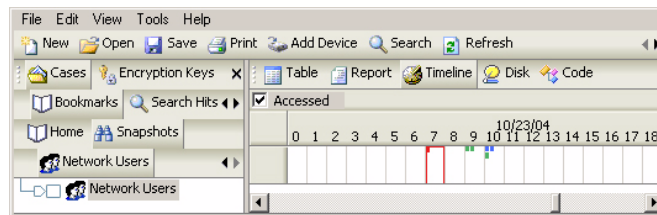


Figure 21-18: Timeline of Network Users

FOREIGN LANGUAGE SUPPORT (UNICODE)

This chapter covers a critical emerging area of investigations: working with languages other than English in forensic investigations. The matter is a complicated issue due to the many variables involved. Whether you are an investigator in the United States examining a system with foreign language documents on it, or an investigator working on a system with a non-English version of Windows examining media either in English or in a foreign language, these different variables determine the best way to approach analyzing the data.

The Unicode standard attempts to provide a unique encoding number for every character, regardless of platform, computer program, or language. Unicode uses 16-bits to represent each character, as opposed to ASCII (which uses 7-bits). For the complete Unicode code charts, please go to www.unicode.org/charts.















 Basic Latin	 Geometric Shapes
 Latin-1 Supplement	 Miscellaneous Symbols
 Latin Extended-A	 Dingbats
 Latin Extended-B	 Miscellaneous Mathematical Symbols-A
 IPA Extensions	 Supplemental Arrows-A
 Spacing Modifier Letters	 Braille Patterns
 Combining Diacritical Marks	 Supplemental Arrows-B

Figure 22-1: Unicode Code Charts (<http://www.unicode.org>)

EnCase supports Unicode, which means that investigators can search for and display Unicode characters, thus supporting more languages.

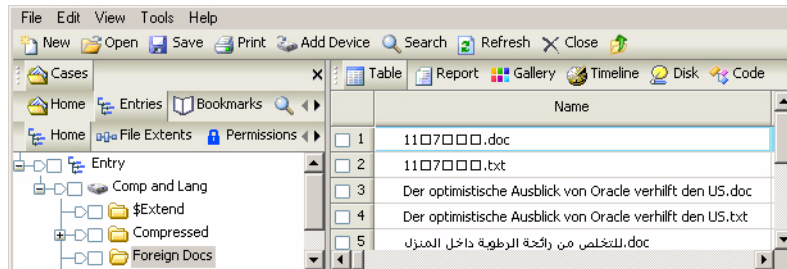


Figure 22-2: Foreign-language files in EnCase

Not all documents are entered in 16-bit Unicode, however, complicating the situation. This chapter will go over viewing Unicode documents, viewing non-Unicode, foreign-language documents, foreign language keyword searching, and bookmarking non-English text to display correctly in the report. The EnCase window by default does not recognize foreign characters in filenames; to configure EnCase to properly display these characters, select the **Options** feature from the **Tools** pull-down menu and click on the **Fonts** tab.

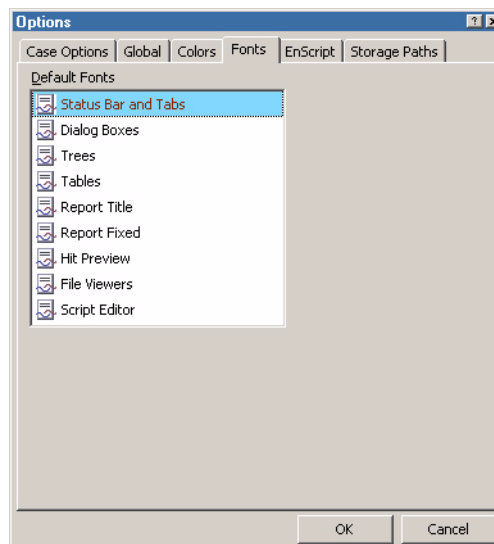


Figure 22-3: Fonts tab

Double-click on **Status Bar and Tabs** and then change the font to **Arial Unicode MS**.

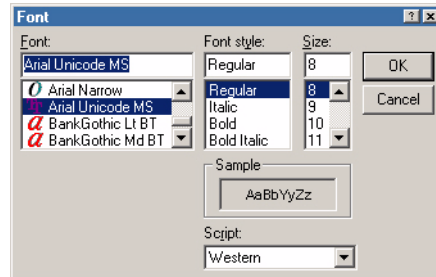


Figure 22-4: Font Selection

Click [OK] and view the EnCase frame; the filename is displayed correctly.

Figure 22-5: Foreign characters displayed

Viewing Unicode Files

EnCase, by default, displays **Text** and **Hex** tab characters in ANSI (8-bit) format with the *Courier New* font. To view Unicode files properly requires modifications of both the format (encoding) and the font. First, the Unicode file or document must be identified as Unicode. This is not always straightforward.

Text files (.TXT) containing Unicode begin with a Unicode hex signature `\xFF\xFE`. Word-processor documents written in Unicode, however, are not so easy. Typically, word-processor applications have signatures specific to the document, making identification of the file as Unicode more difficult.

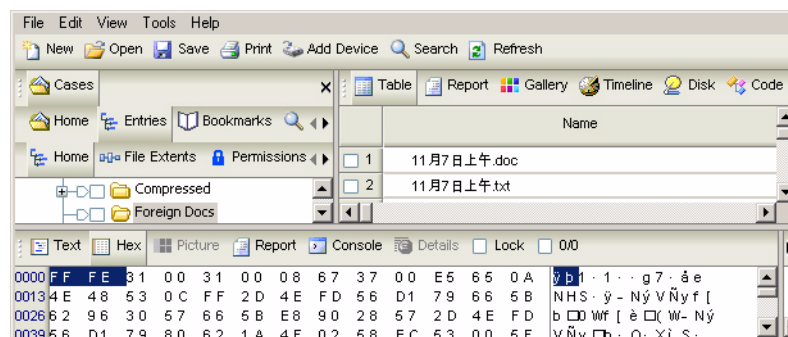


Figure 22-6: Unicode hex signature

To display the text in Unicode, select **Text Styles** from the **View** pull-down menu:

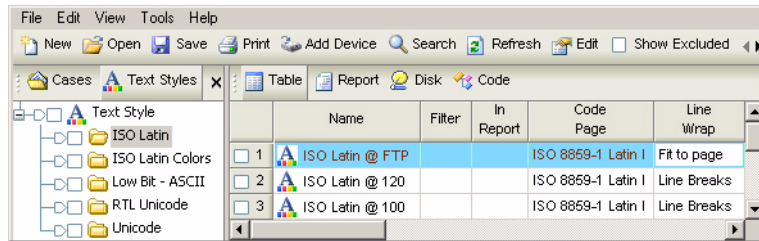


Figure 22-7: Text Styles view

- Right-click on the **Text Styles** selection on the left-hand side and select **New**.

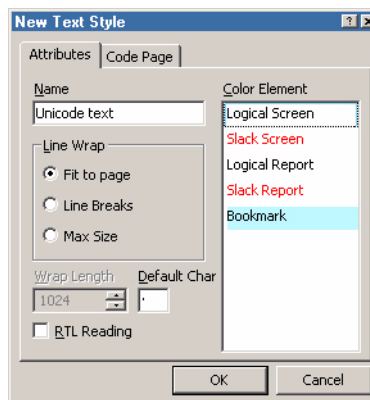


Figure 22-8: Creating a new Text Style

- In the **Attributes** tab, type in a name for the **Text Style**.
- Click on the **Code Page** tab. For a Unicode document, the **Unicode** radio-button must be checked. Notice when the **Unicode** radio-button is checked, all language code-pages are grayed-out.

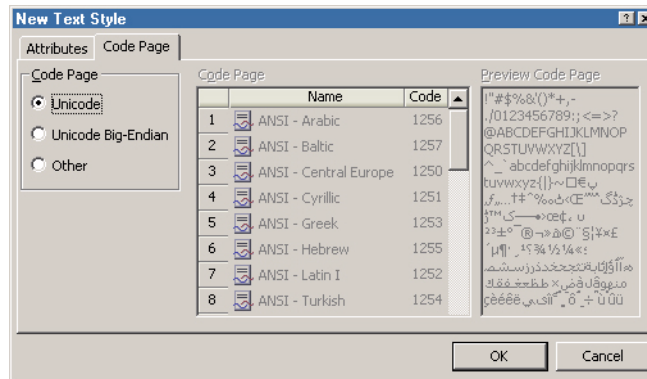


Figure 22-9: Code Page tab

- After clicking [OK], the Unicode text will be displayed properly.



Figure 22-10: Unicode text

Unicode Fonts

While Unicode is designed to be a universal character-encoding standard, correct display of Unicode characters relies heavily upon the font selected to display the characters. While one font might successfully display certain Unicode characters of a certain language, the same font might not display Unicode characters for another language. Characters that are not “translated” by the font are displayed as the “default” character, typically either a dot or a square.

The chart below illustrates how Unicode is a vast character-encoding scheme, with languages typically broken up into “sets.” A font can be thought of as the translator, which interprets the bytes and displays the character according to that number. However, if the font does not have enough information to translate all of the Unicode

character encoding, the application using that font will not display that character correctly. For character encoding that the font understands, those Unicode characters will be displayed correctly.

Unicode Characters	Font (translator)	Application
English subset	English subset understood	Correct display
Japanese subset	None	Default character
Chinese subset	None	Default character
Arabic subset	Arabic subset understood	Correct display

Figure 22-11: Unicode Characters

Switch to a Unicode font when a font is not displaying Unicode characters correctly. Unicode Arabic text is interpreted and displayed correctly by EnCase, even though the default font that EnCase uses to display text is Courier New (an 8-bit font). However, certain languages, such as Chinese and Japanese, cannot be viewed properly in this font. In order for characters to be displayed properly, the font, which is selected, must support that character set. The solution then is to switch the EnCase file-viewing font to a Unicode font (supporting all Unicode character sets).

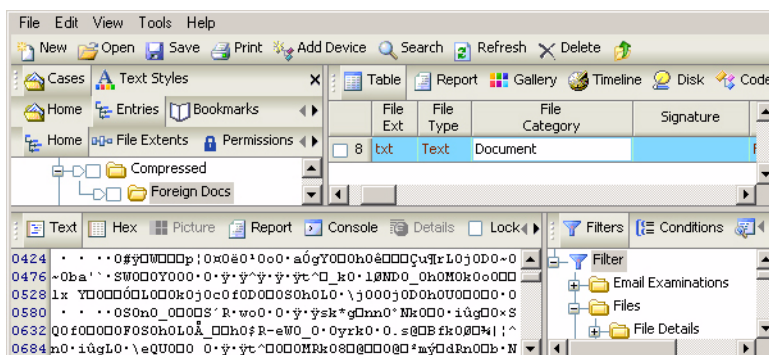


Figure 22-12: Unicode displayed improperly

To change the display font:

- From **Options** in the **Tools** pull-down, select **Fonts**, and double-click on **File Viewers**.

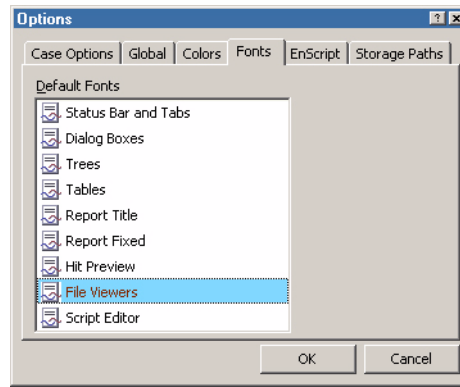


Figure 22-13: File Viewers

- Change the font from **Courier New** to **Arial Unicode MS** and click [OK].

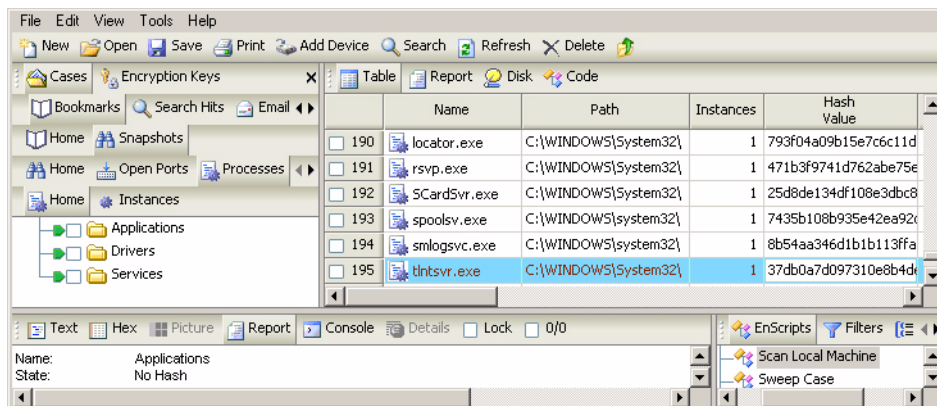


Figure 22-14: Configuring font

- Repeat the process for the default font for **Tables** and **Status Bar and Tabs**; the text file and labels should properly display Chinese text

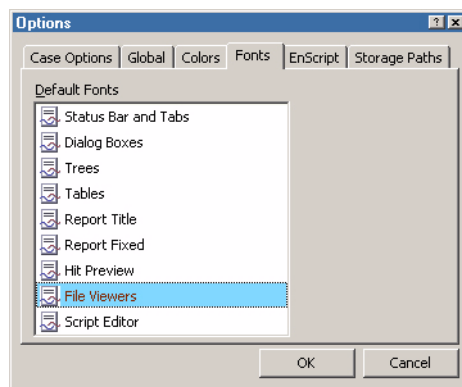


Figure 22-15: Viewing Unicode characters correctly

Changing Font Size

To increase or decrease the font size, follow these steps:

- From the **Tools** menu, navigate to **Options** and select **Fonts**.
- Double-click the **File Viewers** entry.
- Change the font size; the characters will appear larger.

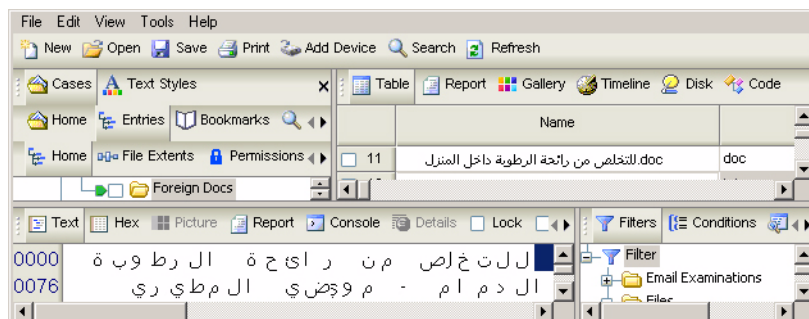


Figure 22-16: Larger font size

Font Recommendations

The Arial Unicode MS font contains most, if not all, of the Unicode characters, making it the ideal font to use for foreign-language investigations.

However, 8-bit characters will be interpreted as 16-bit pairs when this font is selected, so that 8-bit documents are not displayed correctly. The next image shows the **\$MFT** file displayed as a Unicode document with the Arial Unicode MS font selected for viewing. Chinese characters are displayed.

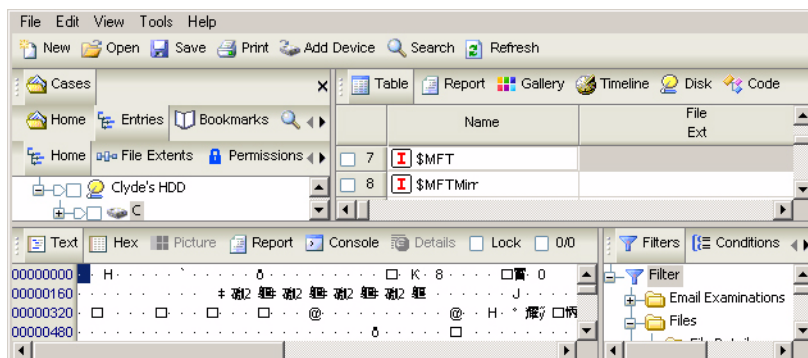


Figure 22-17: MFT displayed with Arial Unicode MS

For this reason, Guidance Software recommends using the **Courier New** font for English and all code page investigations and the **Arial Unicode MS** font for Unicode investigations.

Viewing Non-Unicode Files

Unicode is an attempt to display all characters from all languages in one standard. Before Unicode evolved to the point it has, separate character encoding schemes, called Code Pages, were created to display separate foreign languages. These Code Pages were excellent for displaying the language for which they were designed, but problematic in that they only displayed text in that language.

By including these Code Pages, EnCase allows the forensic investigator to view many foreign language documents correctly.

First, locate a non-Unicode, foreign-language document. In the example that follows, text of a Russian language document is displayed. EnCase uses the **ANSI - Latin I** Code Page by default, not **ANSI - Cyrillic**.

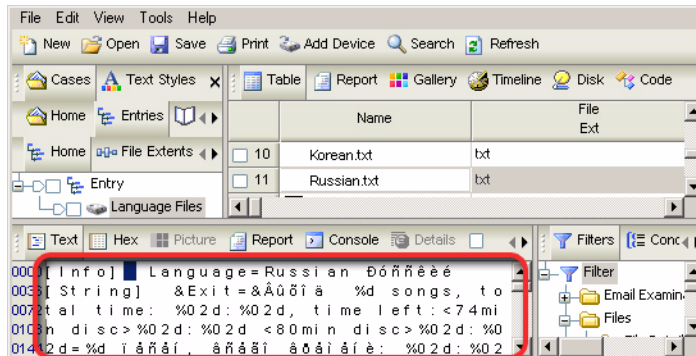


Figure 22-18: Russian text with ANSI Latin I Code Page

To display the text in the native language, create a new **Text Style** (navigate to the **View** pull-down menu from the menu bar and select **Text Styles**

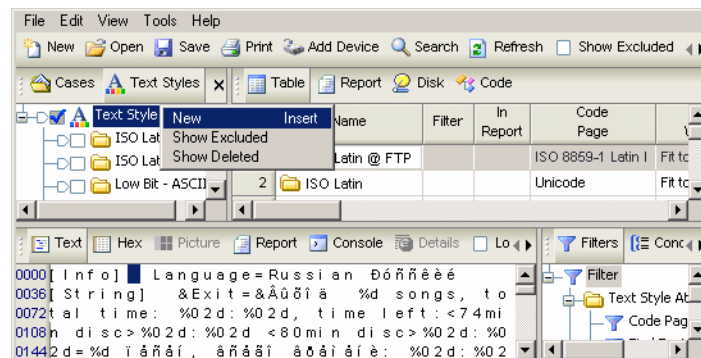


Figure 22-19: Text Styles tab

- Right-click on the **Text Styles** selection on the left-hand pane and choose **New**.
- Name the new Text Style the appropriate language (e.g., **Cyrillic ANSI**).
- Below the text formatting options is a box for **RTL Reading**, which means Right-to-Left reading. For languages that read right-to-left, such as Arabic or Hebrew, check the box. For Russian and other left-to-right languages, leave the check box empty.

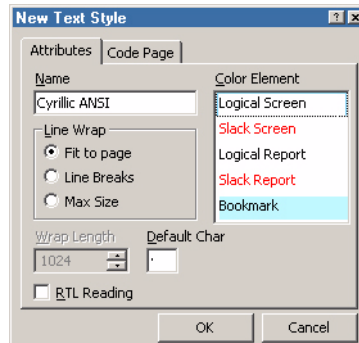


Figure 22-20: Text Style options

- The other tab, **Code Page**, presents several options for Code Pages. In this case, choose **ANSI - Cyrillic** to view the Russian document.
- Highlight the Code Page and click [OK].

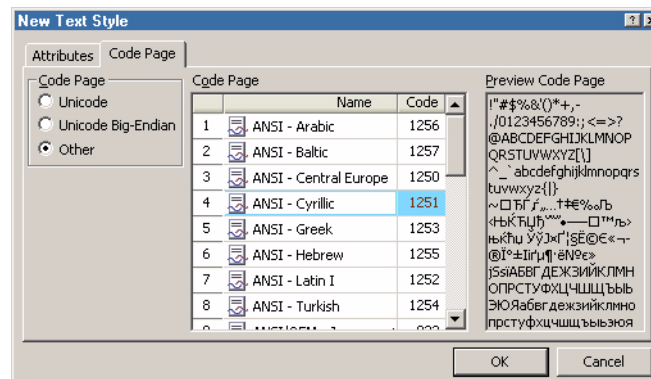


Figure 22-21: Assigning a Code Page to a Text Style

- Scroll through the list of Text Styles in the table and select the newly created Text Style.

The document should be properly displayed in EnCase. If not, you may need to go to the **Options** settings in the **Tools** pull-down menu and click on the **Fonts** tab. Double-click on **File Viewers** and ensure that a font is selected that has the characters in the language you are trying to view. Arial Unicode MS has a considerable amount of these characters.

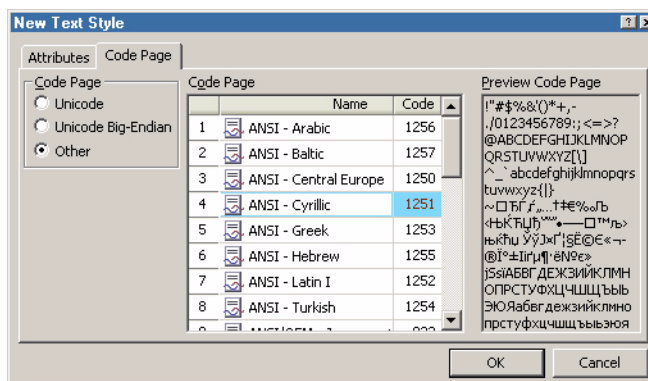


Figure 22-22: Non-Unicode Russian document

The differences are subtle, as the ANSI - Latin I code page uses many of the same characters as Cyrillic code page. Notice that the ANSI - Latin I code page is missing the Russian characters.

Text Styles can be created for every Code Page, so even if the Code Page used to create the document is unknown, viewing documents correctly becomes largely a matter of locating the correct Text Style (or switching to the Unicode text style and using a Unicode font).

Also, notice above that the first 95 characters of the ANSI - Central Europe Code Page are standard ASCII characters. If you click through all of the Code Pages, you will notice the first 95 characters of every ANSI Code Page do not change. This means that English characters and words, no matter the Code Page selected, will be displayed properly.

Right to Left (RTL) Languages

For languages that read right-to-left, such as Arabic and Hebrew, check the **RTL Reading** check box when creating the Text Style and click [OK]. This will work for 8-bit Code Pages with no complications, although it will not work with Arabic and Hebrew since they read right-to-left

For that reason, the investigator might need to create two Unicode Text Styles--one that displays left-to-right and one that displays right-to-left. Then, to view Arabic or Hebrew Unicode text, the RTL Unicode Text Style would be used.

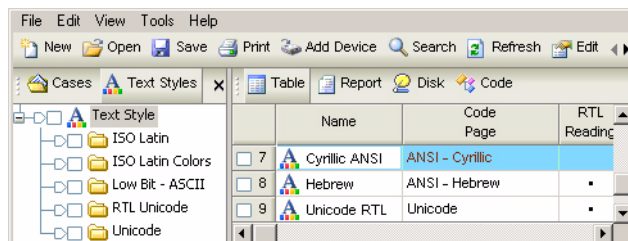


Figure 22-23: RTL and Left-to-Right reading Text Styles

Foreign Language Keyword Searches

Keyword searches are a critical function to quickly locate and bookmark key evidence. EnCase has the ability to search for foreign language keywords. Unfortunately, searching for foreign language keywords is not as easy as typing in the word in English, changing the Code Page to the language desired, and beginning the search. Typing in the word “fire,” for example, changing to the Central Europe Code Page (for German), and then beginning a search will not search for the German word for “fire.”

The first requirement is that the investigator must have knowledge of the desired word in the foreign language. For instance, in the example above, instead of “fire,” the investigator would have to type “feuer” (the German word for fire). Once the Central European Code Page is selected, the search can proceed.

Often, languages contain characters that are not readily typed in by an English-mapped, QWERTY keyboard: the French accent-grave, the German umlaut, or any character in Japanese, Chinese, Arabic, and many other languages. There are several solutions available to the investigator to enter keywords in a foreign language.

Copying and Pasting

Copying and pasting is the easiest method for entering keywords of a non-English language into the keyword field. Highlight the characters, copy them, and paste into the Search Expression field. If the pasted characters are displayed as boxes, the font being used to display those characters is the wrong font. The font must be changed by going to the **Tools** menu, navigating to **Options** and selecting **Fonts**, changing the font for **Dialog Boxes**.

The caveat with this method is that the desired keyword must be located in a document already before a search for the keyword can be executed.

Character Map

Another method for inputting keywords of a different language into EnCase is to select the characters from the Windows 2000 Character Map dialogue box. While this method can be used for all character maps, it is probably most useful when entering a keyword that mostly uses ASCII characters, but might contain one or two that are not standard. The French word “*garçon*” is a good example.

- Click on the **[Start]** button and from the **Programs** menu, navigate to **Accessories** and **System Tools**, selecting **Character Map**. Depending on the character needed from the Character Map, it might be necessary to change the font to a Unicode font. To change the font, go to the **Font** pull-down list and select a Unicode font, such as Arial Unicode MS.

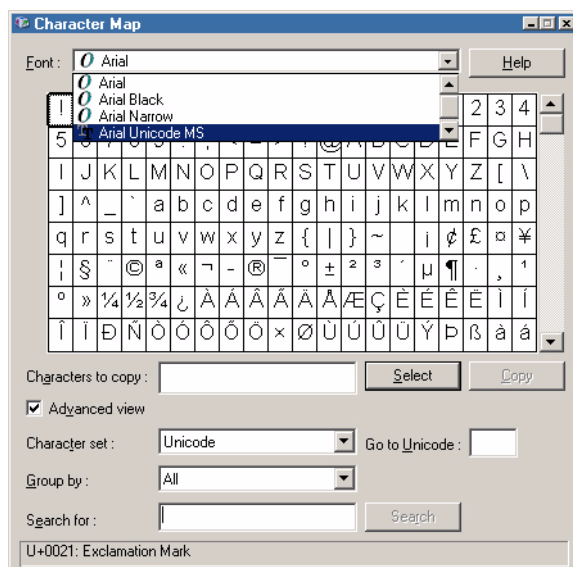


Figure 22-24: Selecting a font in Character Map

- Select the desired character from the Character Map and double-click it. It will appear in the **Characters to copy** field below.

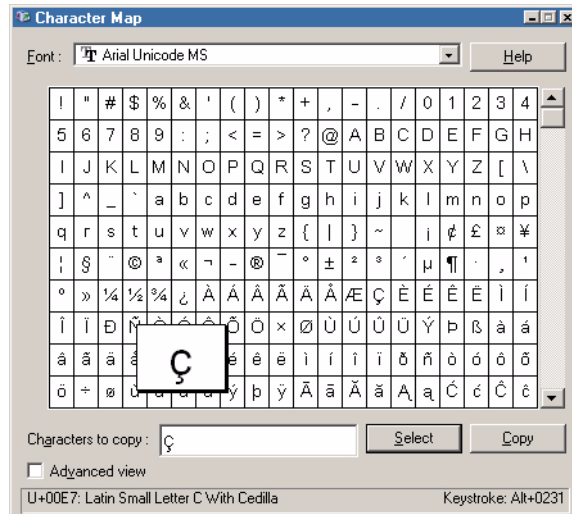


Figure 22-25: Selecting a character in Character Map

- Press the [**Copy**] button and switch back to EnCase.
- Navigate to the **Search Expression** field in the **New Keyword** dialogue and paste the character into the field.
- Enter the keyword info and check the **Active Code-Page** check box.

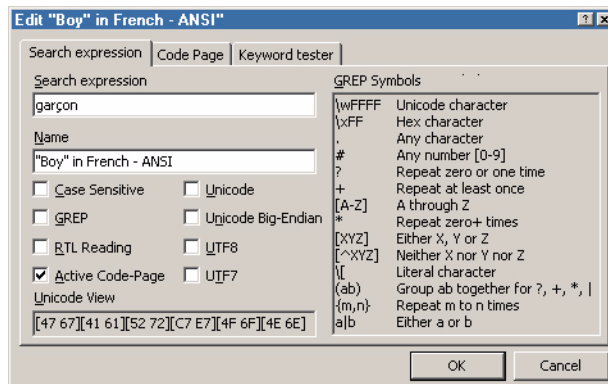


Figure 22-26: Creating keyword with ç character

- Select the appropriate Code Page (in this case, **ANSI - Latin I**).
- Blue check the Code Page, and then click [**OK**] to begin the search.

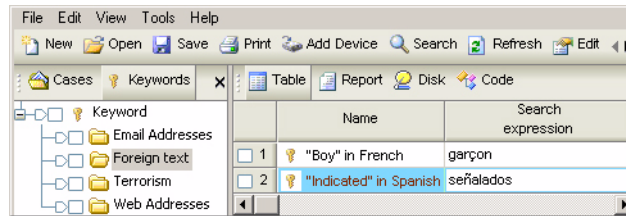


Figure 22-27: Foreign keywords

Regional Settings

The final method is to switch the storage computer's keyboard mapping to a different region, thus allowing input of a different language with the keyboard. Instead of manually selecting each character from the Character Map system tool (above), the foreign keyword can be typed into the **Search Expression** keyword field. The problem with remapping the keyboard is that the new mapping (the character each key inputs) is not displayed on the keys. Unless thoroughly familiar with the new keyboard mapping, or unless the keyboard map chart is available as a reference guide, this is not the recommended method for entering keywords in a foreign language. To remap the keyboard, open the **Regional Options** Control Panel from the **Settings** menu on the [Start] button.

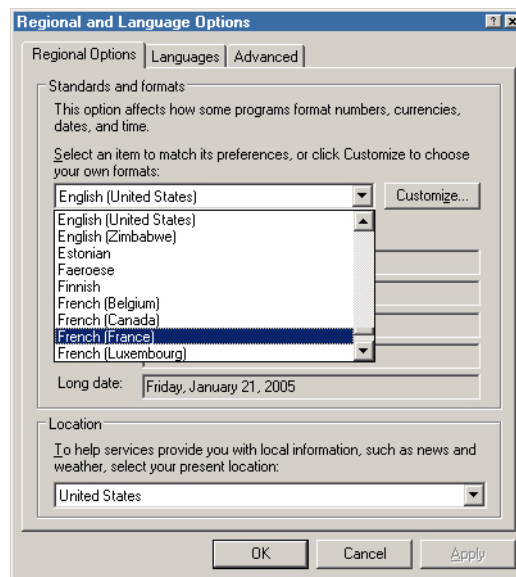


Figure 22-28: Selecting regional options

You will need to make the appropriate changes in the **Advanced** tab as well. When finished, click **[OK]** and switch to EnCase. You can now type the foreign keyword into the **Search Expression** field.

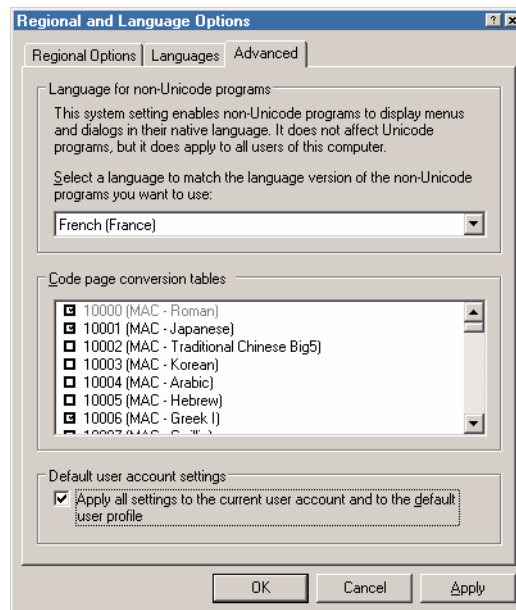


Figure 22-29: Advanced settings

Foreign Language Bookmarking

ASCII text can be bookmarked and displayed in the report, regardless of the language. Text is bookmarked and displayed with the available Text Styles. For a Unicode document, choose the standard Unicode view or the Unicode Text Style created under Text Styles.

- Click and highlight the desired text to appear in the report.
- Right-click and select **Bookmark Data** from the contextual menu.

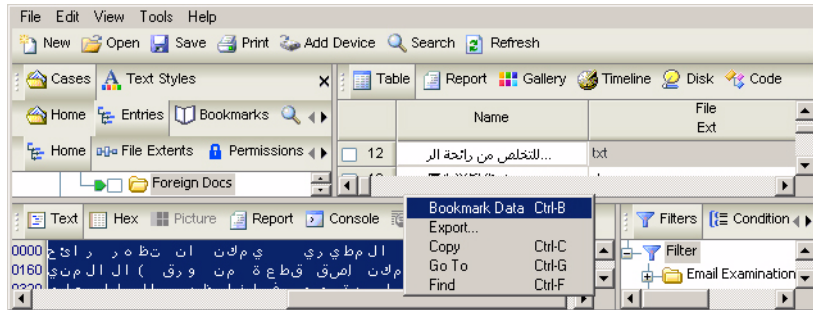


Figure 22-30: Bookmark the highlighted data

- Select the right Text Style. For Unicode Arabic, choose the **Unicode - Right-to-Left** Text Style from the **Styles** folder (Arabic text reads right-to-left).



Figure 22-31: Text formatted to flush-right

- Press [**OK**] and switch to the **Report** view. The bookmarked text will be displayed in the report, formatted in the desired text style.

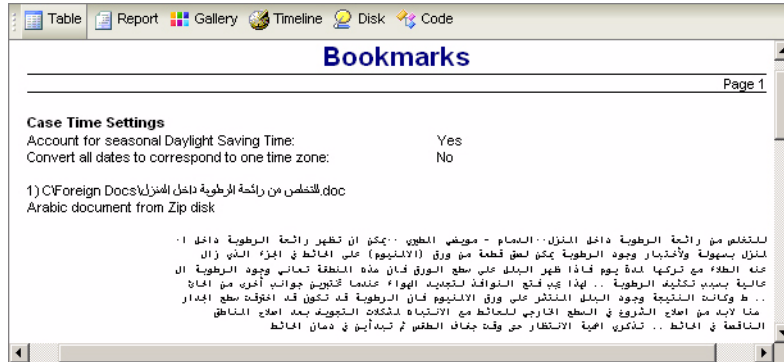


Figure 22-32: Arabic displayed in report

Rich Edit Control in Bookmarks

Guidance Software continues to improve the ability of EnCase to be used in international examinations with Rich Edit Control in the bookmark comments and bookmark notes. These comments and notes can now be written in languages other than English. In the example below, the comments of the examiner are entered in Arabic and English, and the swept data is displayed in the correct Arabic characters.

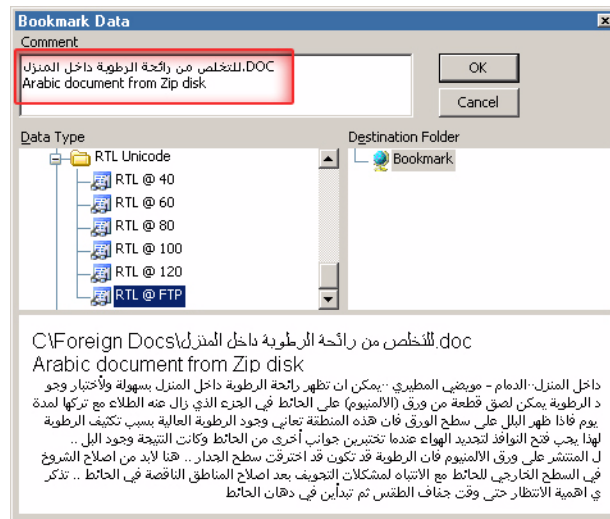


Figure 22-33: Rich Edit Control for book marking in desired language.

More Information

The implementation of foreign language support into EnCase is a substantial undertaking which allows forensic investigators to perform international investigations.

RESTORING EVIDENCE

EnCase allows an investigator to restore evidence files to prepared media. Restoring evidence files to media theoretically permits the investigator to boot the restored media and view the subject's computing environment without altering the original evidence. Restoring media, however, can be challenging. Read this chapter carefully before attempting a restore. **Additional information is also available in the *Validation Testing of the EnCase Restore Process in Windows* white paper, available on Guidance Software's web site at <http://www.guidancesoftware.com> in the Support section from the Downloads page.**



DO NOT boot up the Subject's drive. Do not boot up your forensic hard drive with the Subject drive attached. There is no need to touch the original media at all. Remember, it is still evidence.

Physical vs. Logical Restore

EnCase allows the investigator to restore either a logical volume or a physical drive.

- A logical volume is a volume that does not contain a Master Boot Record (MBR) or the Unused Disk Space.
- A physical volume contains the Master Boot Record and Unused Disk Space. Unused Disk Space, however, is typically not accessible to the user.

Most often, when complying with discovery issues, one must perform a physical restore, not a logical one. Logical restores are less desirable as they cannot be verified as an exact copy of the subject media. When a drive is restored for the purposes of booting the subject machine, a physical restore is the correct choice.

Whether restoring a drive physically or logically, restore the evidence files to a drive slightly larger in capacity than the original Subject hard drive. For example, if restoring a 2-gig hard drive image, restore the image to a 2 to 4-gig hard drive. Restoring media to a drive that is substantially bigger than the subject media can

prevent the restored clone from booting at all, possibly defeating the purpose of the restore.

Preparing the Target Media

Preparation of the target media (to which the image is going to be restored) is essential for a forensically sound restore.

- The target media must be wiped (see the chapter on *Advanced Analysis*).
- For logical restores, the target media must be FDISKed.
- For logical restores, the target media must be partitioned and formatted with the same file-type system as the volume to be restored (e.g., FAT32 to FAT32, NTFS to NTFS, etc.).
- For physical restores, do not FDISK, partition, or format the hard drive. Bring up EnCase and restore the image, physically, to the target media.

Physical Restore

Restoring a physical drive means that EnCase will copy everything, sector-by-sector, to the prepared target drive, thereby creating an exact copy of the subject drive. The target drive should be larger than the subject hard drive. When EnCase completes the restore it will provide the hash values verifying that the lab drive is an exact copy of the subject drive. If a separate, independent MD5 hash of the lab drive is run, be certain to choose to compute the hash over only the exact number of sectors included on the suspect's drive so that the MD5 hash will be accurate.

To restore a physical hard drive in EnCase:

- Install a sterile, unpartitioned, unformatted restoration drive to your forensic PC, using a connection other than IDE 0 (EnCase cannot restore a physical drive to IDE 0.) Ensure the intended restoration drive is at least as large as (but preferably larger than) the original from which the image was taken so that the restored data will never overwrite all sectors on the target hard drive. EnCase can wipe the remaining sectors of the target hard drive after the actual data from the evidence file is restored. Wiping remaining sectors is recommended.
- Using the EnCase, look at the acquired drive in Report view and note the precise physical drive geometry of the forensic image you are restoring from, including Cylinders, Heads and Sectors. Note the acquisition hash for later comparison on the restored drive.

- In the Tree Pane of the **Entries** subtab (below **Cases**), right click on the physical disk you wish to use as the source and select **Restore...**

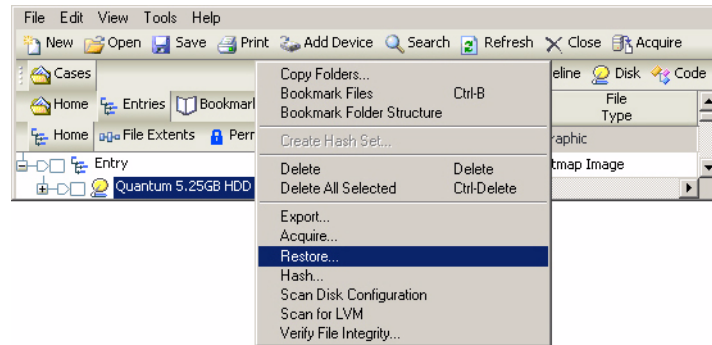


Figure 23-1: Restore command

- Select the destination drive from the list of possible destination devices to restore the physical disk to and click [**Next >**].

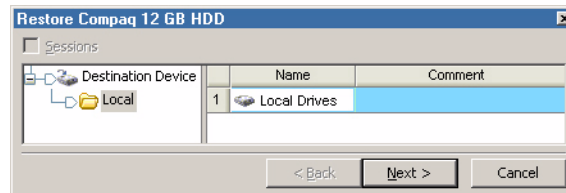


Figure 23-2: Local restore

- EnCase does not allow the investigator to restore to Drive 0 as this is typically the drive the operating system is installed on. If the operating system is running on a separate SCSI drive, EnCase will still not allow a restore to IDE 0. If the prepared target media is Drive 0, another drive will have to be added to the system (as a Master) to store the restored image. Select the drive to restore the image to and click [**Next >**].

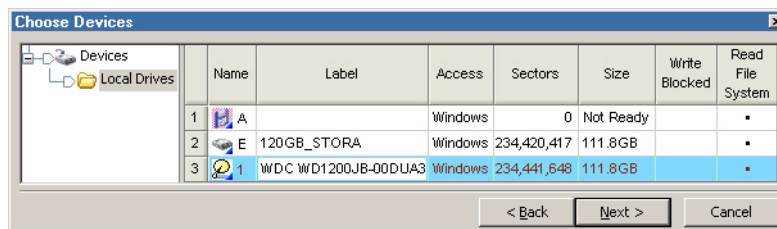


Figure 23-3: Selecting local media for restore

- EnCase can also verify the restored sectors to confirm that it is indeed a sector-by-sector copy of the original subject media.

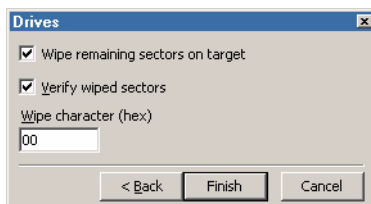


Figure 23-4: Restore options

Sometimes the **Convert Drive Geometry** option is available, other times not. This is entirely dependent on the drive geometry of the original drive in comparison to the restore drive. Drive geometries are of certain “types”. Every drive has a certain Cylinders-Heads-Sectors (CHS) drive geometry information. If the Heads and Sectors of the original drive imaged are identical to the target restore drive, then the drives are of the same type and the **Convert Drive Geometry** check box will not be available. If the drives are of different types (as in, the heads-sectors settings are different), then the **Convert Drive Geometry** check box will be available. For physical restores, check the **Convert Drive Geometry** check box if it is available. Click [**Finish**] when done.

- Confirm the restore to the designated drive. Type “**Yes**” in the field, and then click the [**Yes**] button to start the physical restore. When the restore is finished, a verification message displays such information as any read or write errors and the hash values for both the evidence file and the restored drive; these should match. If the hash values from the restore do not match, restore the evidence file again following the procedures above. It might be necessary to swap the target media for correct results.

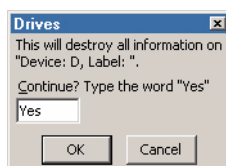


Figure 23-5: Starting restore

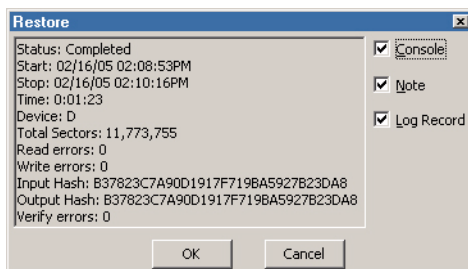


Figure 23-6: Restore confirmation

- Once the drive is restored, physically pull the power cord from the computer.
- Attach the restored drive in as near to the original configuration as possible (e.g., if the drive was originally on IDE channel 0 on the original computer, install it there.) This will help the computer to allocate the original drive letters, providing the proper mapping for .lnk files, etc.
- On older drives less than 8.4 GB, you may need to reboot using an EnCase Boot Diskette, and during the boot sequence set the CHS settings of the restoration drive in the CMOS to the physical geometry of the original drive, which you noted earlier (this will probably require overriding the auto-detected drive geometry.)
- Use EnCase for DOS to calculate the hash value of the restored drive, and compare it to the acquisition hash value to ensure its integrity.

If you wish to boot the drive, use an EnCase Boot Disk with **FDISK** copied to it. Run **FDISK /MBR**; the restored disk should now be bootable. Be aware that as soon as you boot it, the underlying data will be altered.

Note that differences may occur depending on whether you are restoring an NTFS or FAT32 file system, and whether the restored drive is being booted on the original hardware platform the drive was acquired from. If the drive was acquired via FastBloc, the subject drive is read through the ASPI layer, but Windows does allow writes through it. When EnCase in Windows is used to restore the drive, it is restoring through the BIOS. This usually results in a difference of one sector. Where Windows 98 physically goes through the BIOS, Windows 2000, XP and 2003 go through Windows protected mode drivers, resulting in issues when restoring to an identical drive. EnCase prompts the user to truncate the sectors that will not fit.

Windows 2000, XP and 2003 do not allow direct hardware access, so the writes need to be through the ASPI layer. ASPI has a problem with rounding off the last few sectors that do not fit on the last cylinder of a drive. This is the reason why all of the sectors

are visible when the drive is read, yet when writes are attempted a small number of sectors may be missing. This is a Windows/ASPI limitation and not one of EnCase. Although in an OS that allows direct hardware access (such as Windows 98) you should see the same number of sectors, both for reading and writing purposes, Windows 98 is not supported to run EnCase Version 5.

Drive manufacturers also state that even though drives may appear identical, once partitioned they may not have the same capacity. If possible, drives from the same batch should be used so that both will be read with the same capacity (check the date on the drive's label). Older hard drives may have 2 platters, while the newer version may only have one, with the single platter drive having a few less bytes available.

Logical Restore

Media have different types depending on the CHS (cylinders-heads-sectors) information. The same type might have different “cylinders” settings, but their heads and sectors information (the HS in CHS) will be the same. If the heads-sectors information is different, then the media type differs and another target restore hard drive should be used. A logical volume must be restored to a volume of the same size, or larger, and of the same type.

To prepare for a logical restore, the target media should be wiped, FDISKed, partitioned, and formatted prior to restore. Format the target drive with the same file-type system as the volume to be restored (e.g., FAT32 to FAT32, NTFS to NTFS, etc.).

The procedure for restoring a logical volume is identical to that of restoring a physical device. In the case of the logical volume, right click on the volume in **Case** view and select **Restore**.

When the logical restore is finished, a confirmation message will be displayed. The computer must be restarted to allow the restored volume to be recognized. Note that the restore volume contains only the information that was inside the selected partition.

Booting the Restored Hard Drive

After the restore operation has finished with no errors, remove the target hard drive from the storage system and place it into a test system. Switch the power on. Depending what operating system the subject ran, the test system should now be booting up exactly as the subject computer.

There are quite a few difficulties that can occur at this stage of the investigation. The most common is that the clone of the subject drive will not boot. Before trying anything else, check the restored disk using FDISK and verify it is set as an Active

drive. If not, set the drive as Active (using the FDISK utility) and this should enable it to boot.

Recommended steps for booting:

- Install a sterile restoration drive to your forensic PC, using a connection other than IDE 0 (EnCase cannot restore a physical drive to IDE 0). Ensure the intended restoration drive is at least as large as the original from which the image was taken.
- Create a single partition on the restoration drive, but do not format it
- Using the EnCase report view, note down the disk geometry of the forensic image of the drive you are restoring from (Cylinders, Heads, Sectors), taking care to get the physical geometry correct.
- Restore the forensic image of the *physical* drive to the restoration drive using the **Restore Drive** option in EnCase.
- Make the restored drive active if it is not already (in a Win2k/XP environment, right click on the desktop **My Computer** icon and select **Manage**, then select **Disk Management**. Right click on the restored drive and select **Make Active**).
- Shut down the computer and attach the restored drive in as near to the original configuration as possible (e.g., if the drive was attached to IDE 0 on the original computer, attach it to the same controller). This will help the computer to allocate the original drive letters, making .lnk files etc. work better.
- Reboot, and set the CHS settings of the restoration drive in the CMOS to the physical geometry of the original drive, which you noted earlier. (This may require overriding the auto-detected geometry).

The restored disk should now be bootable.



NTFS is a complicated file-structure and might not boot in any computer. If the Subject computer is still available, replace the Subject hard drive with the restored clone and try to boot the clone from this system.

For additional information pertaining to EnCase and the restore process, please refer to the whitepaper on Guidance Software's web site entitled, "*Validation Testing of the EnCase Restore Process in Windows*".

Restoration FAQs

- **I restored an image to a hard drive, and now, with that hard drive in a separate PC, it's not booting. Why not?**

The Cylinders-Heads-Sectors information (CHS) in the Master Boot Record (MBR) from the image does not match the CHS information of the actual hard drive. Reset the CHS information for the MBR. Boot with a DOS boot disk and, at the **A:\>** prompt, type "**FDISK /MBR**" (without the quotes) to reset the Master Boot Record.

Verify that the MBR has the correct **io.sys** file. "Re-SYS" the boot drive with the correct sys version. For example, if the subject had Windows 95B, then the hard drive should be sys'd from a Windows 95B-created boot disk. At the **A:\>** prompt, type "**SYS C:**".

ARCHIVING EVIDENCE

It is good forensic methodology to archive all evidence. Guidance Software recommends archiving evidence files as soon as they have been acquired. This way, should evidence files become corrupted during an investigation, the archived copies will still be available. Archive evidence files to either compact disc-recordable (CD-R) or digital versatile disc-recordable (DVD-R).

What Should Be Archived

Archiving EnCase evidence files is identical to archiving any other data. A device to archive the data and media to hold the data are necessary. CD-Rs are popular due to their ease, cost, speed, and endurance. Tape media can fail quite easily after years of storage in vaults, as can removable media like Jaz or Zip disks. Although CDs and DVDs are more stable than tape media, many investigators are moving to hard drive storage due to the recent decrease in cost and higher stability.

When acquiring media, the default evidence file segment size is 640MB, which is designed for CD archiving. The maximum value is 2,000,000 MB (2 terabytes). Bear in mind when setting this value that if you are writing files to a FAT file system, the maximum allowable size is 2,000 (2 gigabytes); setting the value higher will result in write errors.

Archiving to CD or DVD, requires the following:

- A CD-R or DVD-R burner
- CD-R burning software or similar product for DVD-R
- Multiple blank CD-R discs or DVD-R discs

Use the disc-burning software to archive the evidence file segments to the optical media. The last evidence file segment is usually smaller than 640MB, and the final CD-R or DVD-R disc frequently has free space. Therefore, in addition to the evidence file, add the following items:

- The version of EnCase used for the examination

- EnScripts used during the examination
- Hash sets used during the examination
- Keywords used during the examination
- The .CASE file for the examination. The CASE file should be burned to a separate CD-R, the two CD-Rs being kept together.
- Any other tools used for the examination

Verifying Evidence Files

After burning the discs, label the media accurately. Include the date, the related .CASE file, and which number in the sequence it is. Run **Verify Evidence Files** from the EnCase **Tools** menu on each disc to verify that the burn was thorough and that the evidence file segment is intact. The burning software will often report the disc burn was “OK” with no errors; however, one lost 0 or 1 can compromise the evidence. EnCase checks the 32-bit cyclical redundancy checksum (CRC) for each 64 sectors of data in the evidence file segment.

To verify several evidence files or evidence file segments:

- Insert the CD-R or DVD-R with the archived files into the CD-R drive or DVD-R drive.
- Launch EnCase
- From the **Tools** pull-down menu, select **Verify Evidence Files...**

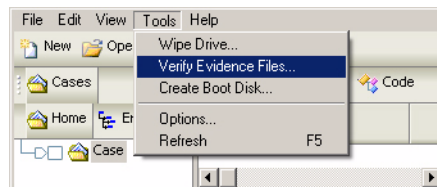


Figure 24-1: Verifying evidence files

- Browse to the archived evidence files or segments on the CD-R or DVD-R, highlight the desired files, and click **[Open]**. EnCase is capable of verifying more than one evidence file simultaneously.

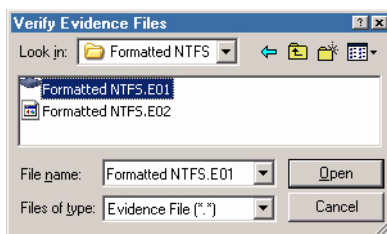


Figure 24-2: Selecting evidence files to verify

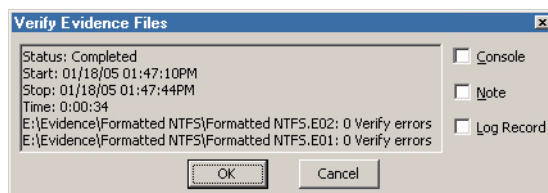


Figure 24-3: Console verification status

- After the archival process is complete and the disks labeled accurately, store the CD-Rs / DVD-Rs in a cool, dry place for safekeeping.

Cleaning House

To remove all trace of the evidence files from the storage hard drive, access the **Wipe Drive...** option from the **Tools** pull-down menu. If wiping the drive is not necessary,

it is nevertheless a good idea to archive the data and delete the material in preparation for another case.

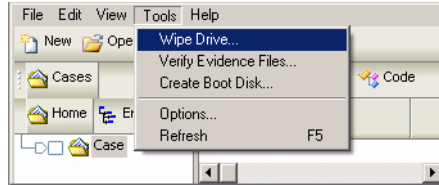


Figure 24-4: Wipe Drive option

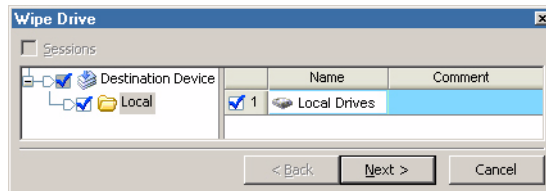


Figure 24-5: Choosing drive to wipe

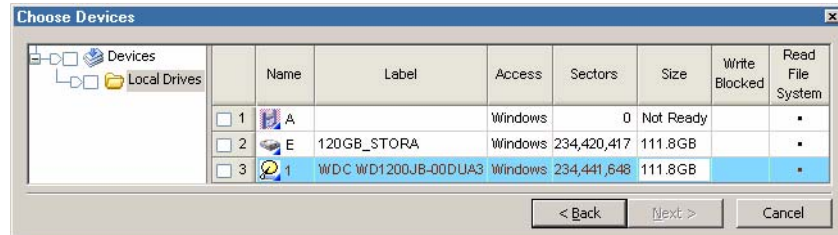


Figure 24-6: Selecting drive to wipe

The boot drive that EnCase resides on is not available to be wiped.

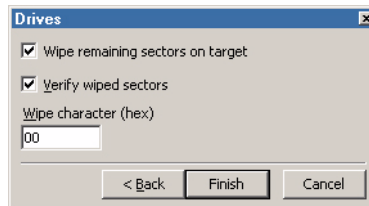


Figure 24-7: Wiping options

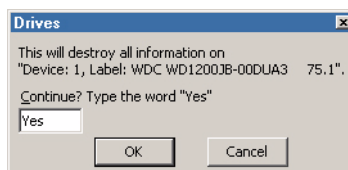


Figure 24-8: Wiping confirmation

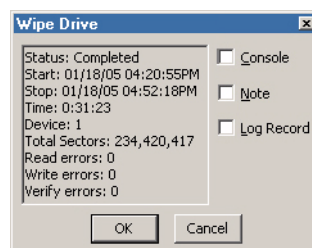


Figure 24-9: Wipe status



NOTE: The *Wipe Drive* feature can only wipe local devices.

BOOKMARKS

EnCase allows for files, folders, or sections of a file to be highlighted and saved for easy reference. These marks are called bookmarks. All bookmarks are saved in bookmark files, with each case having its own bookmark file. Bookmarks can be viewed at any time by selecting the **Bookmarks** subtab under **Cases**. Bookmarks can be made from anywhere data or folders exist.

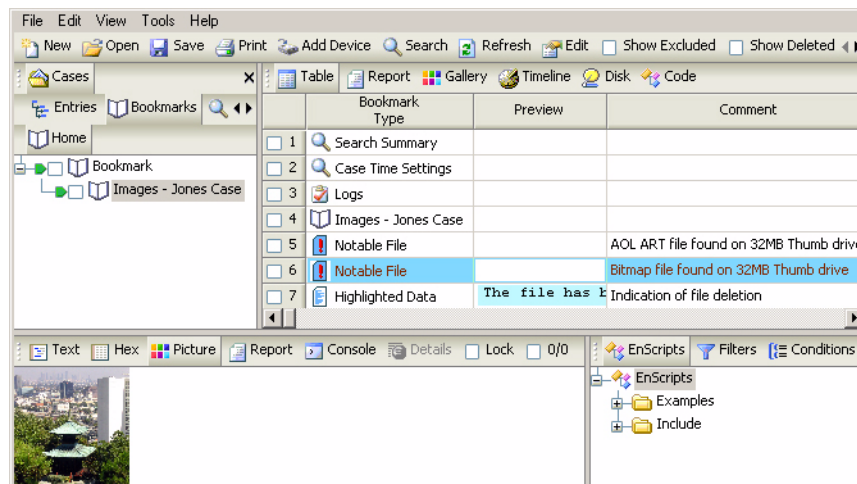


Figure 25-1: Bookmarks View

Understanding Bookmarks

There are different types of bookmarks; below is a list of these bookmarks and their descriptions:

- **Case Time Settings**

Shows whether Daylight Savings Time is being used on the evidence file and whether dates should be converted to a single time zone.

- **Search Summary**

Displays search results, times, keywords, etc. for a particular case

- **Highlighted Data Bookmark**

Created by clicking and dragging the mouse over data (“sweeping”) in one of the sub-panes. This is a fully customizable bookmark.

- **Notes Bookmark**

Used to allow the user to write additional comments into the report. It has a few formatting features. It is not a bookmark of evidence.

- **Folder Information Bookmark**

To bookmark the tree structure of a folder or device information of specific media. There is no comment on this bookmark. The options include showing the device information, such as drive geometry, and the number of columns to use for the tree structure.

- **Notable File Bookmark**

A file bookmarked by itself. This is a fully customizable bookmark.

- **File Group Bookmark**

Indicates that the bookmark was made as part of a group of selected files. There is no comment on this bookmark.

- **Snapshot Bookmark**

Bookmark containing the results of a System Snapshot of dynamic data for Incident Response and Security Auditing.

- **Log Record Bookmark**

Bookmark containing the results of log parsing EnScripts.

- **Registry Bookmark**

Bookmark containing the results of Windows registry parsing EnScripts.

Highlighted Data Bookmark

The **Highlighted Data** bookmark, also known as a sweeping bookmark or a text fragment bookmark, can be used to show a larger expanse of text. This type of bookmark is created by clicking and dragging-known as “sweeping” text or hex in the View Pane. To sweep an area of data, left-click on the first character and hold down the mouse button. Drag the mouse to the end of the data to be highlighted.

Complete the bookmark by right clicking in the highlighted area and selecting **Bookmark Data** from the contextual menu.

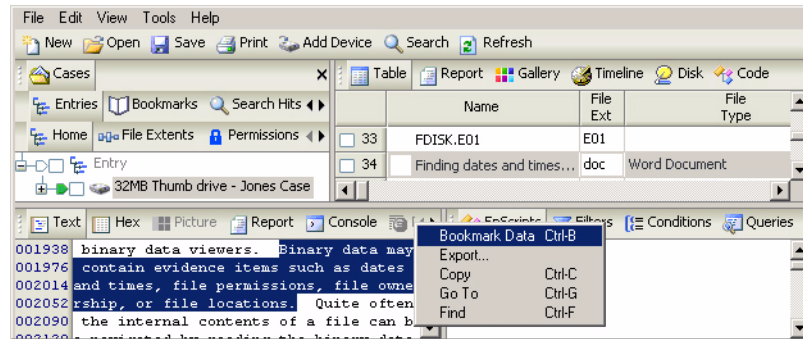


Figure 25-2: Swept text bookmark

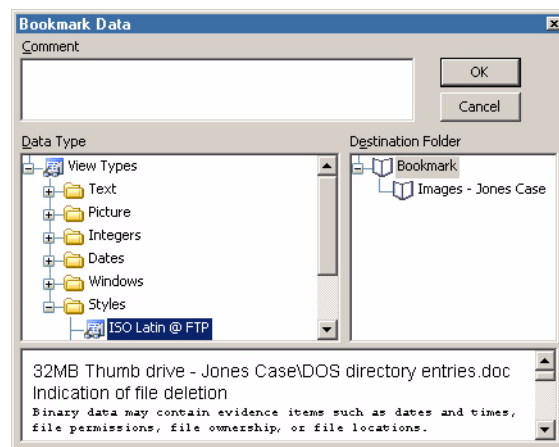


Figure 25-3: Preview of swept text bookmark

In the space provided, type a comment for this bookmark, up to one thousand characters. Select the **Data Type** of the bookmark. There are a variety of methods for displaying the bookmark:.

Text

- **Do not Show**

Hides text in the bookmark

- **High ASCII**

High ASCII includes additional ASCII characters (up to 256), which may include foreign language accents, math symbols, trademark and copyright symbols, etc. These characters are not the same on all computers.

- **Low ASCII**

ASCII defines code numbers for 128 characters, which are the alphabetic and numeric characters on a keyboard and some additional characters such as punctuation marks.

- **Hex**

Hexadecimal. The base 16 numbering system, sometimes used as a short way of representing binary numbers. The digits 0-9 are used, plus the letters A-F, which represent the numbers 10 to 15. The farthest-right digit is the ones place; the digit next to the left is the 16s place; the next place to the left is $16^2 = 256$, etc. Each place is 16 times the place immediately to the right of it.

- **Unicode**

A character set that uses 16 bits (two bytes) for each character, and therefore is able to include more characters than ASCII, which is based on 8-bit characters. Unicode can have 65,536 characters and therefore can be used to encode almost all the languages of the world. Unicode includes the ASCII character set within it.

- **ROT 13 Encoding**

ROT13 does simple text encoding by rotating the characters alphabetically by 13 characters, but does not encrypt it. Highlighted ROT13-encoded text will be converted when using this Data Type.

- **Reconstructed HTML**

Reconstructs HTML code into a bookmarked page when the code is highlighted and tagged

Picture

- **Picture**

EnCase can view natively JPG, GIF, EMF, TIFF, BMP, AOL ART and (occasionally) PSD file formats.

- **Base64 Encoded Picture**

Picture encoded for e-mail transport in Base64.

- **UUE Encoded Picture**

Picture encoded for e-mail transport with UUE.

Integers

- The selected data is displayed in the integer format. Options are 8-Bit Integer, 16-Bit Integer, 16-Bit Big-Endian, 32-Bit Integer and 32-Bit Big-Endian. Big Endian is an order in which the “big end” (most significant value in the sequence) is stored first (at the lowest storage address).

Dates

- **DOS Date**

Packed 16-bit value that specifies the month, day, year, and time of day an MS-DOS file was last written to

- **DOS Date (GMT)**

- **UNIX Date**

A Unix timestamp (in seconds) based on the standard Unix epoch of 01/01/1970 at 00:00:00 GMT

- **UNIX Text Date**

A Unix timestamp (in seconds) based on the standard Unix epoch of 01/01/1970 at 00:00:00 GMT, in text format

- **HFS Date**

A numeric value on a Macintosh that specifies the month, day, year, and time that a Macintosh file was last written to

- **HFS Plus Date**

A numeric value on a Power Macintosh that specifies the month, day, year, and time that the file was last written to

- **Windows Date/Time**

A numeric value on a Windows system that specifies the month, day, year, and time that a file was last written to

- **Lotus Date**

Date from a Lotus Notes database file

Windows

- **Partition Entry**

Characters indicating the beginning of a Windows partition entry

- **DOS Directory Entry**

MS-DOS uses one directory entry for each file and subdirectory. These characters can be interpreted by EnCase to view the DOS directory entry.

- **Win95 Info File Record and Win2000 Info File Record**

These are the structures that hold the paths and deleted dates for files in the recycle bin. These structures are found in a file called INFO or INFO2, thus the name.

Styles

- **Text Styles (ISO Latin @ FTP, ISO Latin, ISO Latin Colors, Low Bit - ASCII, etc.)** - see the chapter of this document on *Foreign Language Support* for directions on creating and editing **Text Styles**.

Select a destination folder to contain the bookmark. When finished, click [OK].

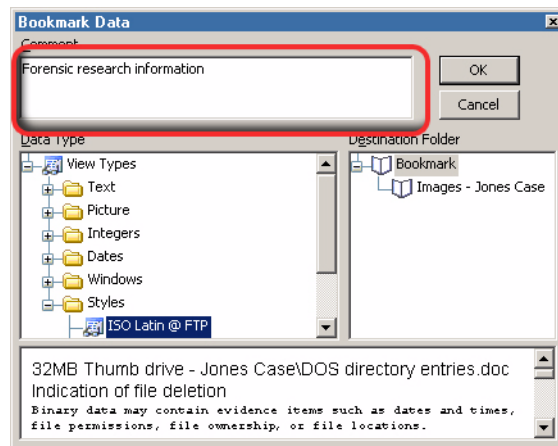


Figure 25-4: Adding a comment

View the bookmark in the **Bookmarks** table.

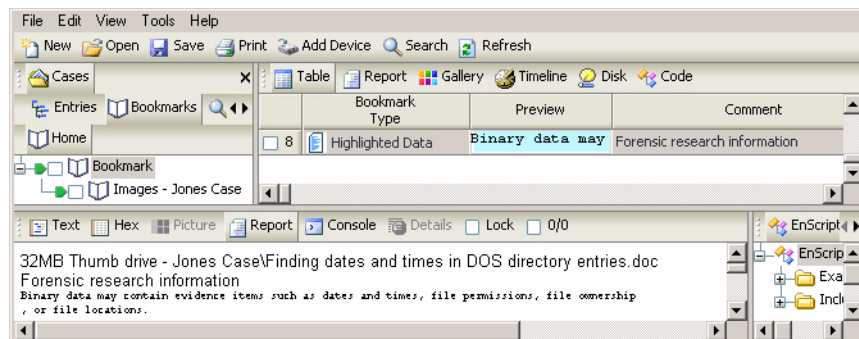


Figure 25-5: Comment / bookmark text, table view

Switch to **Report** view for the report display.

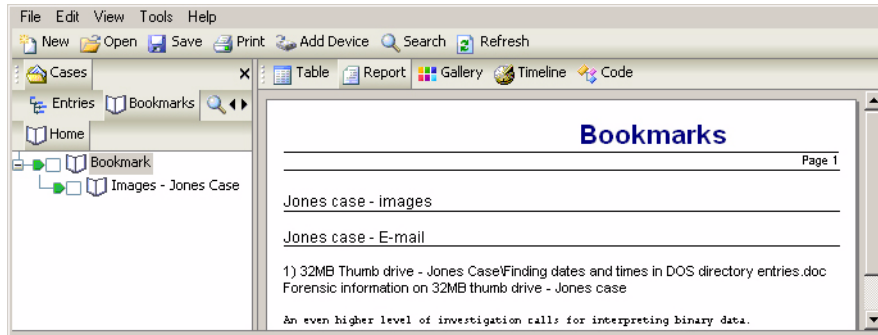


Figure 25-6: Comment / bookmark text, Report view

Text fragment bookmarks are one of the most common forms of bookmarking. They are extremely useful as they place evidentiary data directly into the report.

Notes Bookmark

The **Notes Bookmark** gives the investigator a great deal of flexibility when adding comments to the report. This bookmark has a field reserved only for comment text and can hold up to one thousand characters. It also contains formatting options including italics, bold, changing font size, and also changing the indent of the text. To add a note, right click the folder where the note is to be added in the left pane and select **Add Note...**

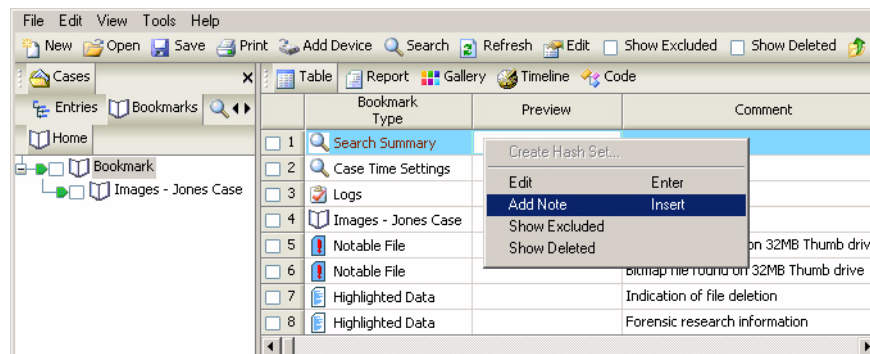


Figure 25-7: Adding a note

In the **Add Note Bookmark** window, type the text to be added into the note, apply formatting options and click [OK]. Check the **Show in report** box to have the note appear in **Report** view.

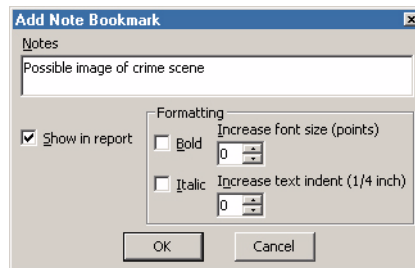


Figure 25-8: Adding new note text

View the bookmark in the table.

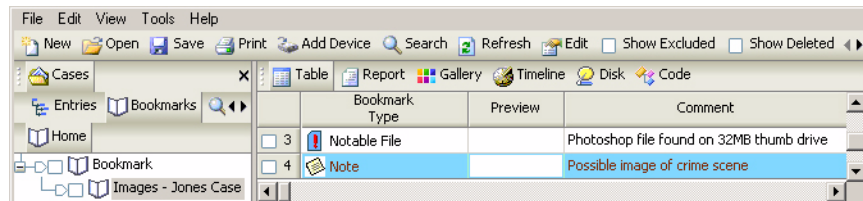


Figure 25-9: Note in Table view

Switch to **Report** view and review the results.

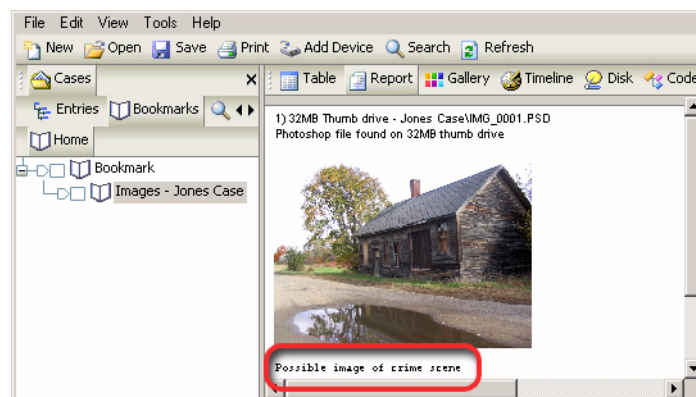


Figure 25-10: Note in Report view

Notes Bookmarks can be copied and placed anywhere within the report.

Folder Information Bookmark

The **Folder Information Bookmark** is used to bookmark folder structures or devices. By bookmarking a folder structure, the entire directory structure of that folder and its children can be shown within the report or bookmarked for later analysis. Individual devices, volumes, and physical disks can be bookmarked as well. This will show important device-specific information in the final report.

This type of bookmark is useful for marking directories that contain unauthorized documents, pictures, and applications. It is also a great way to show specific information about the type of media in the case.

To bookmark a folder, right-click on that folder in the right-hand pane of the **Case** view and select **Bookmark Folder Structure** from the context menu.

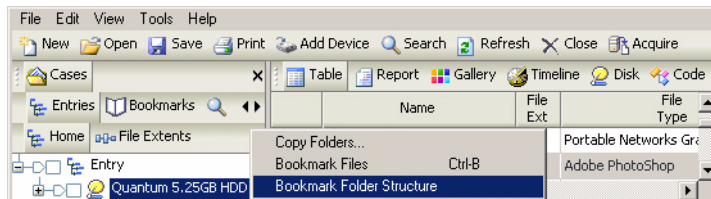


Figure 25-11: Book marking Folder Structure

In the **Add Folder Bookmark** window, select the **Include Device Information** check box. This will show details about the volume that the folder resides on in the report. **Columns** will split up the directory structure into what is specified here. If **[3]** is chosen, the directory structure will be shown in three columns down the page. Finally, choose where the bookmark will reside in the final report.

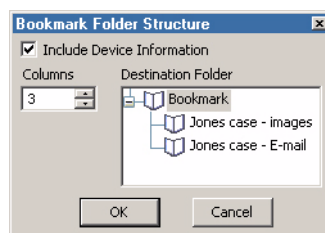


Figure 25-12: Book marking Folder Structure

View the bookmark in the Table view of the **Bookmarks** tab.

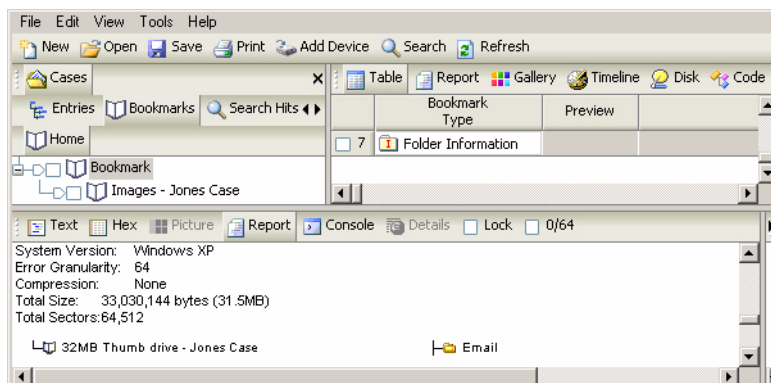


Figure 25-13: Folder information bookmark in Table

Switch to **Report** view and see the results in the report.

Notable File Bookmark

Notable File Bookmarks are used to identify individual files that contain important information to the current case. By bookmarking a file via this method, the contents of the file are not bookmarked. Only the details about the file (column headings in the table) are displayed in the report. To make a notable file bookmark in the table, highlight the file with one left-click, then right-click on the file and select **Bookmark File**.

Notable bookmarks are used for marking files that will be exported out of the case. It is also useful for showing specific fields such as dates and time stamps of important files while it also allows for a comment on the individual file itself.

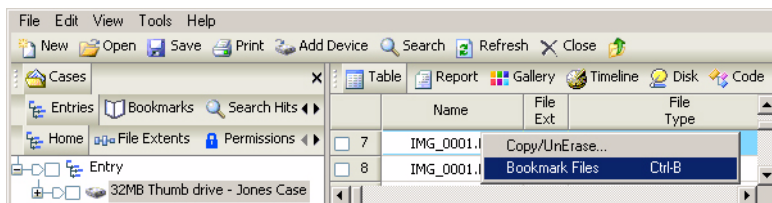


Figure 25-14: Book marking a file

In the **Bookmark File** window, type a comment for the file and select a bookmark location within the final report to store the file.

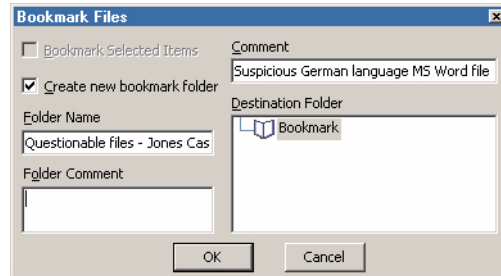


Figure 25-15: Adding Bookmark comment, choosing folder

Select the **Bookmarks** tab under **Cases** and view the bookmark in the table.

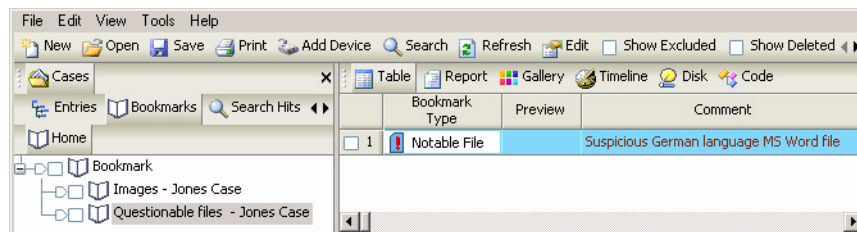


Figure 25-16: Notable File Bookmark

Switch to **Report** view and see the results in the report. Notice the default information shown for the bookmarked file, including the path of the file and the comment added when the bookmark was created. You can change the information that appears by right clicking on the folder that contains the notable file and selecting **Edit**.

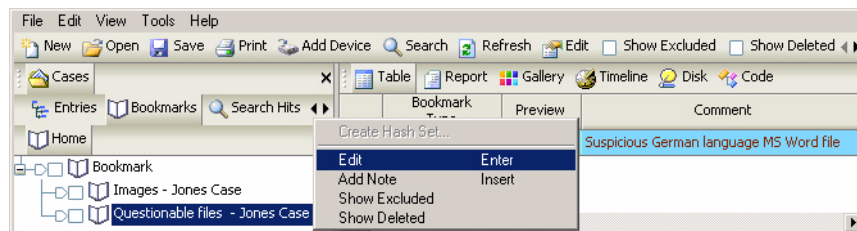


Figure 25-17: Editing the Bookmark folder

The **Edit Bookmark Folder** option will open. By editing this folder information, everything contained within the edited folder will assume the properties of that folder. A comment can be added to the folder. The format window is used to display which

fields will be shown for the files contained within the folder. Fields can be added from the **Fields** box on the right by double-clicking the desired field. You can also specify which tabs are available by blue-checking an item from the **Tables** column.

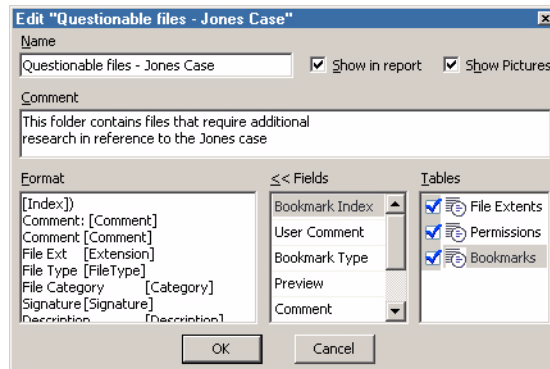


Figure 25-18: Selecting fields for the Report view

After the properties for the parent bookmark folder are changed, the report will reflect the changes that have been made. Notice below that all of the fields that were added in the above folder properties are now displayed for the notable file.

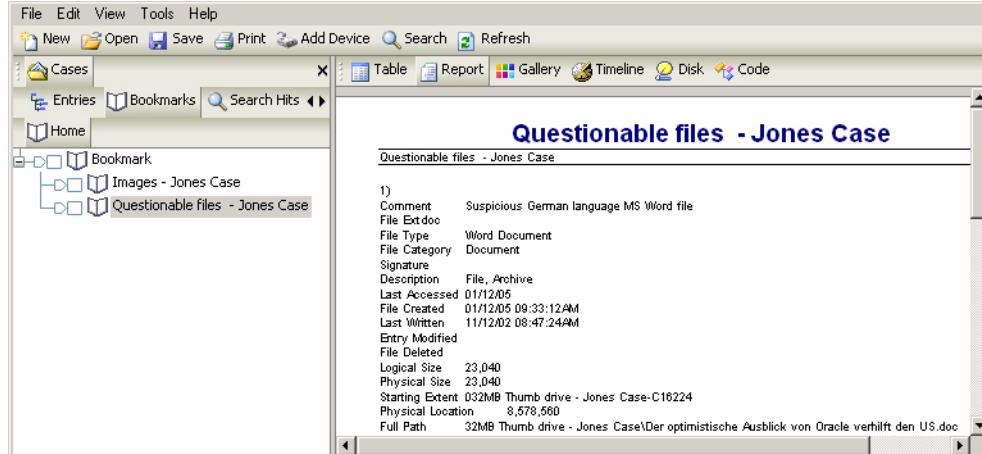


Figure 25-19: Report with additional fields

File Group Bookmark

File Group Bookmarks are similar to notable file bookmarks, except that they are used to bring attention to groups of files, not individual files. This type of bookmark is used to identify a group of files that contain important information to

the current case and are relevant to all other files within the group. By bookmarking a group of files, the contents of the files are not bookmarked; however, the details about the file (column headings in the **Cases** view) can be displayed in the report. To bookmark a group of files, blue-check the files in the table, right-click on one of the files and select **Bookmark Files**.

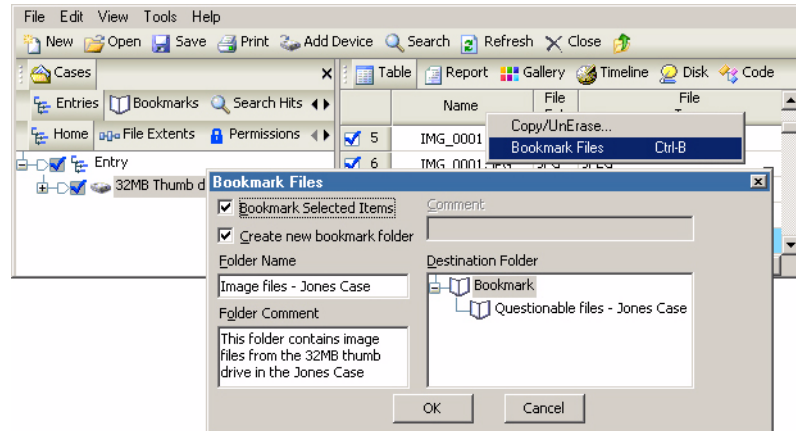


Figure 25-20: File Group bookmark

- In the **Bookmark Files** window, ensure the **Bookmark Selected Items** box is checked. The file group can be saved in an existing bookmark folder or in a new bookmark folder. If a new folder is created, a comment can be entered for that folder when it is created.
- Specify where to store the file group.
- View the bookmarks in the table view of the **Bookmarks** subtab.

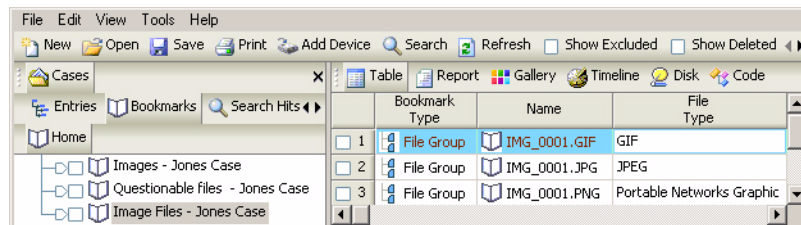


Figure 25-21: Viewing the bookmarks in the folder

Switch to **Report** view to observe the results. Notice that the default information shown for the files that were bookmarked is the full path of each file. Right click on the folder that contains the file group, and select **Edit** to change this information.

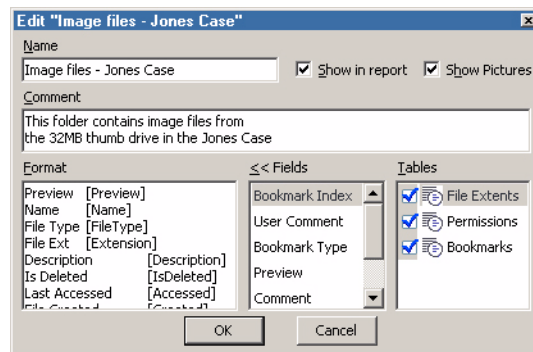


Figure 25-22: Editing Bookmark folder information

The **Edit Bookmark** folder will open. By editing this folder information, everything contained within the edited folder will assume the properties of that folder. A comment can be added to the folder. The format window is used to display which fields will be shown for the files contained within the folder. Fields can be added from the **Fields** box on the right by double-clicking on the desired field., and Tables can be displayed by blue checking them in the **Tables** field.

After the properties for the parent bookmark folder are changed, the report will reflect the changes that have been made. Notice in the figure below that all of the fields that were added in the above folder properties are displayed for the entire file group.

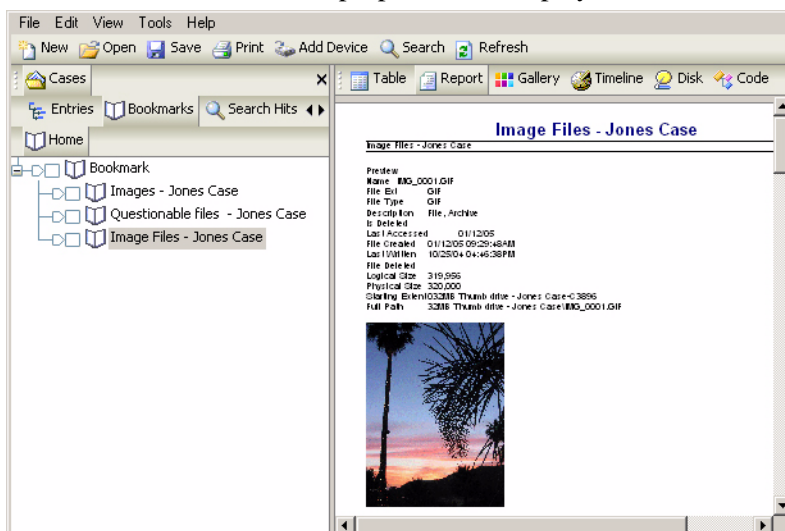


Figure 25-23: Viewing the fields in the report

This type of bookmark is used extensively for marking files that will be exported out of the case and for groups of files that contain similar information. File group bookmarks differ from notable file bookmarks in that a comment cannot be placed on individual files that have been bookmarked in this way. The only way to comment with this type of bookmark is by either making a folder comment on the containing folder or by placing a note in front of one of these files.

Snapshot

For more information on the Snapshot bookmark, please refer to the chapter on *Advanced Analysis*

Documentation Options for Threads

Examiners can bookmark the results of analysis threads into a note and/or write the results to the console. Examiners should be aware that some EnScripts clear the console and write their results to the console.

The following threads have the option to bookmark the results:

- **Acquire**

- **Verify Single Evidence File**
- Searching, Hashing and File Signature Analysis
- **Hash device**
- **Copy/Unerase** files and folders
- **Restore**
- **Recover Folders**
- **Power Indexing** (see section on *Xanalys*)

Bookmark Options

The **Bookmark** tab has many options that operate like the search hits.

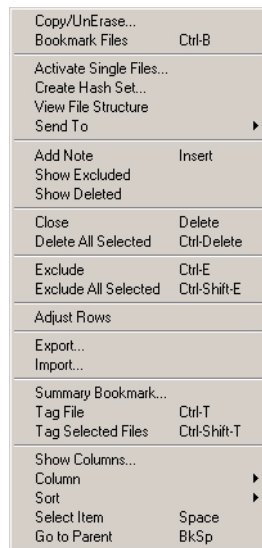


Figure 25-24: Bookmark options

The most significant options are the ability to exclude and delete bookmarks, the same way an examiner can control and display search hits. An examiner can delete or exclude individual or selected bookmarks, or a bookmark folder. Deleting or excluding the parent folder affects all children bookmarks. Bookmarks or bookmark folders that are deleted when the case file is closed are permanently deleted, just as search hits are controlled. An examiner can exclude bookmarks or bookmark folders

he or she does not want included in a report, but wants to retain in the case file for reference or research.

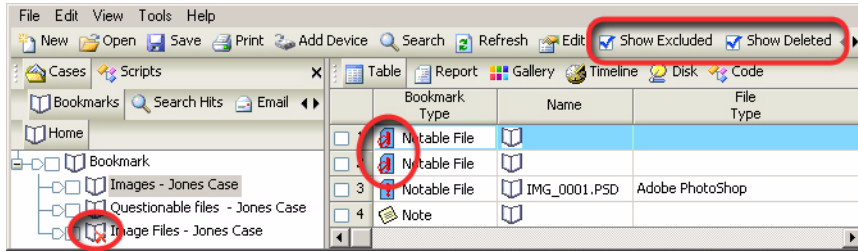


Figure 25-25: Deleted and excluded bookmark items shown

Case time zone settings can be bookmarked from the bookmark options window. Right-click on the Bookmark folder in the Tree Pane and choose **Summary Bookmark...**

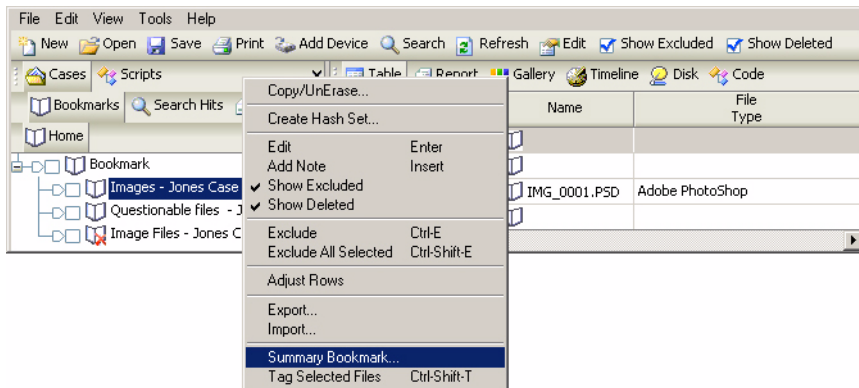


Figure 25-26: Choose Summary Bookmark

Select **Case Time Settings** to create a bookmark of the time zone settings.

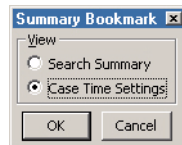


Figure 25-27: Choose Case Time Setting

The **Case Time Setting** bookmark is placed on the root of the bookmark tree, and can be moved to any location in the case bookmark structure.

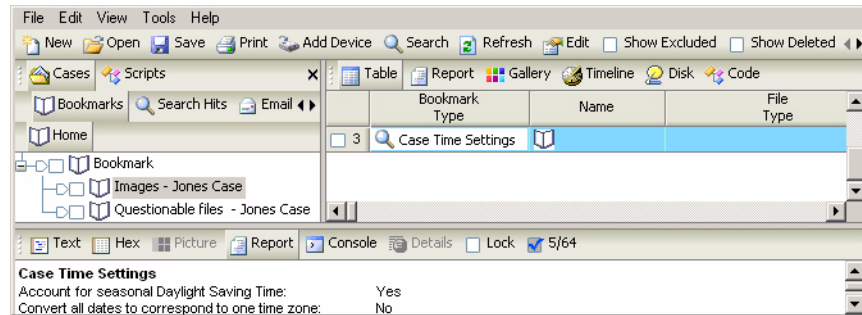


Figure 25-28: Case Time Settings bookmark

The Bookmark table contains encoding information about the bookmark. The columns contain the following information:

- Bookmark Type
- Preview
- Comment
- Page Break
- Show Picture
- Entry Selected
- File Offset
- Length
- Name
- Filter
- In Report
- File Ext
- File Type
- File category
- Signature
- Description
- Is Deleted
- Last Accessed
- File Created

- Last Written
- Entry Modified
- File Deleted
- File Acquired
- Logical Size
- Physical Size
- Starting Extent
- File Extents
- Permissions
- Bookmarks
- Physical Location
- Physical Sector
- Evidence File
- File Identifier
- Hash Value
- Hash Set
- Hash Category
- Full Path
- Short Name
- Unique name
- Original Path
- Symbolic Link
- Bookmark Path
- Bookmark Start
- Bookmark Sector
- Excluded
- Hit Deleted
- Notable

These items are described in the *Table View Columns Explained* section of the *Navigating EnCase* chapter.

Move or Copy Bookmarks

You can move or copy selected bookmarks from one folder to another. Blue-check the table entries to select the desired bookmarks. Right-click, hold, and drag the cursor to the new folder. Release the mouse to show the **Move Here**, **Copy Here**, or **Cancel** options. Left-click on the desired option to **Move (Cut & Paste)** or **Copy** the bookmarks to the new folder, or **Cancel** the action.



Be aware that any function performed on files in the Bookmarks tab only affects the bookmark itself; to perform a function on a file (such as creating hash sets, Copying/UnErasing, etc.), you will need to select the book marked file, right-click and select Tag File. You can then perform the task on the files blue-checked in the Entries subtab.

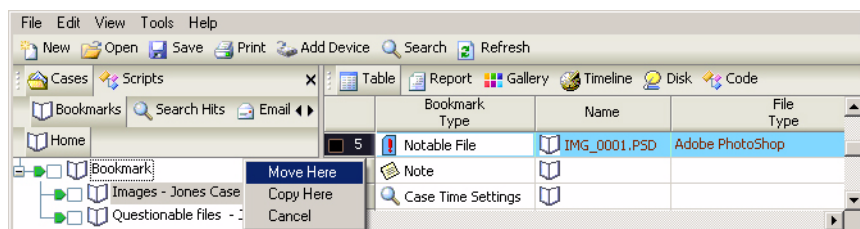


Figure 25-29: Move or Copy Bookmarks

Notable (Bookmarks table)

The **Notable** column is used to highlight and identify individual search hits or swept bookmarks in the right pane, in either the **Search Hits** or **Bookmarks** view, for inclusion in a report. The option can be turned on or off by selecting the target file, right-clicking the **Notable** column, and selecting **Notable** from the menu. You can also blue-check multiple files, right-click on one and select **Notable - Invert Selected Items** to make the selected items **Notable** or remove the classification, depending on the current status of that file

Exporting Bookmarks

Exporting Bookmarks

Bookmarks are exported in a TXT file format. You can export all bookmarks or export only blue-checked bookmarks. Bookmarks can be exported with their encoding information, including the categories described previously. Placing a check box in front of each desired field exports it along with the bookmark.

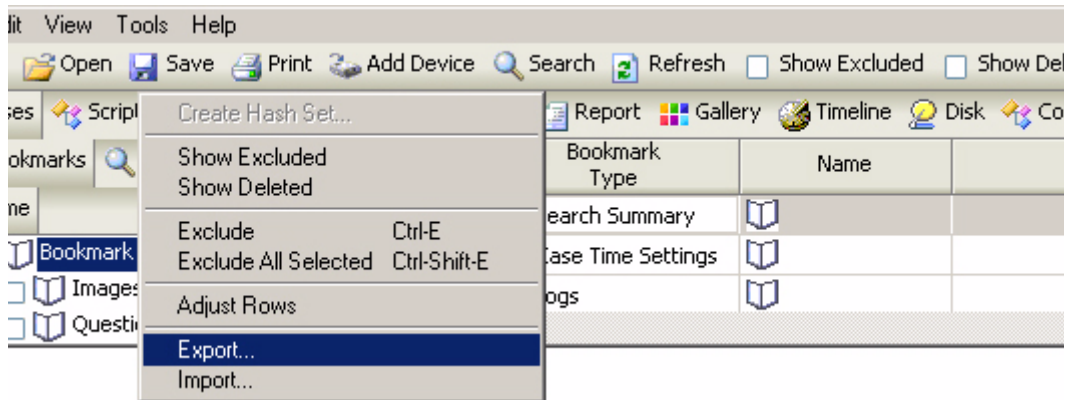


Figure 25-30: Export \ Import menu

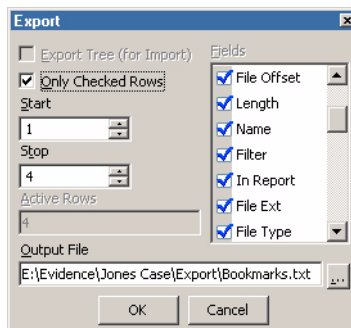
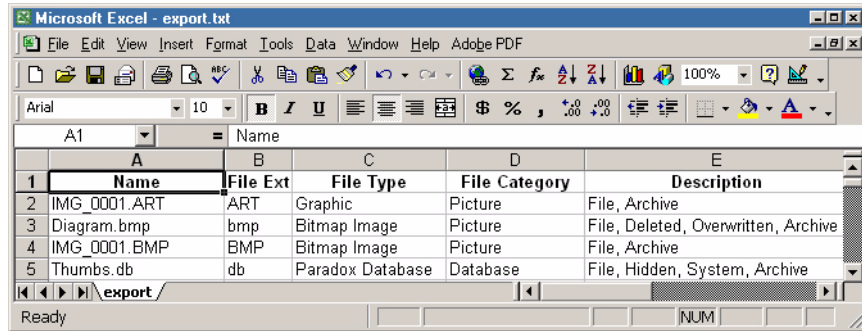


Figure 25-31: Exporting Bookmarks

Exported bookmarks can be viewed by opening the .TXT file using MS Excel or a text editor (the control codes may make the file unreadable in Notepad).



The screenshot shows a Microsoft Excel window titled "Microsoft Excel - export.txt". The spreadsheet contains a table with the following data:

	A	B	C	D	E
1	Name	File Ext	File Type	File Category	Description
2	IMG_0001.ART	ART	Graphic	Picture	File, Archive
3	Diagram.bmp	bmp	Bitmap Image	Picture	File, Deleted, Overwritten, Archive
4	IMG_0001.BMP	BMP	Bitmap Image	Picture	File, Archive
5	Thumbs.db	db	Paradox Database	Database	File, Hidden, System, Archive

Figure 25-32: Viewing Export.txt

THE REPORT

Presenting the Findings

The final phase of a forensic examination is reporting the findings. The report should be organized and presented in a readable format that the target audience will understand. The format and presentation of the report should be considered when the evidence is first received. EnCase is designed to help the investigator bookmark and export the findings in an organized manner so the final report can be generated quickly upon completion of the examination. EnCase provides several methods for generating the final report. Some investigators prefer to break up the final report into several sub-reports inside a word-processing program, with a summary report document directing the reader to their contents. Other investigators create paperless reports burned to compact disc, using a hyper linked summary of the sub-reports and supporting documentation and files. EnCase gives the investigator the flexibility to customize and organize the contents of the final report. The following sections outline the steps necessary to compile a clear, organized report of the findings that can be provided to management or judicial officials in an easily understood format.

The EnScript library contains an Initialize Case EnScript for creating a report with important drive geometry and acquisition information. This report is a single large report that could be several hundred pages in length when all book marked evidence in the case is included.

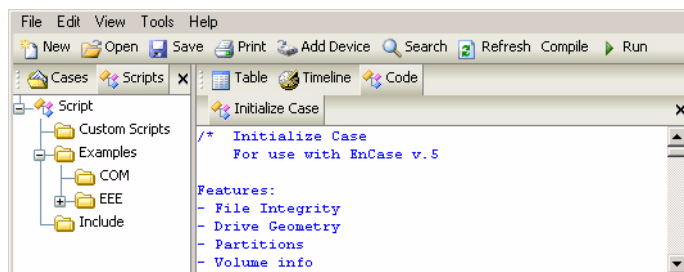


Figure 26-1: Initialize Case EnScript

Central to the final report is the information contained in the evidence file, documenting the chain of custody and characteristics of the physical media. To include this information in the final report, right-click on the physical disk and select **Bookmark Folder Structure**.

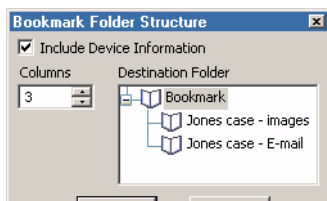


Figure 26-2: Bookmark the physical disk

In the **Bookmark Folder Structure** window, check the **Include Device Information** box. Type [0] in the **Columns** box to prevent the folder structure from being displayed. Click on the desired folder in the right pane in which to place the Folder Bookmark.

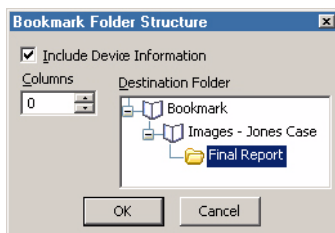


Figure 26-3: Adding the bookmark to the report

In the previous example, a **Folder Information** bookmark will be placed in the Final Report folder. Go to the **Bookmarks** tab; the new **Folder Information** bookmark, containing the case information and file integrity, is placed by default at the bottom of the Tree Pane. The order of the bookmarks can be arranged in any folder by selecting the bookmark's number in the far left column and dragging the bookmark into the desired location.



When using the drag and drop facility, ensure the green “Set Include” trigger is *NOT* on. Otherwise, dragging and dropping bookmarks does not work.

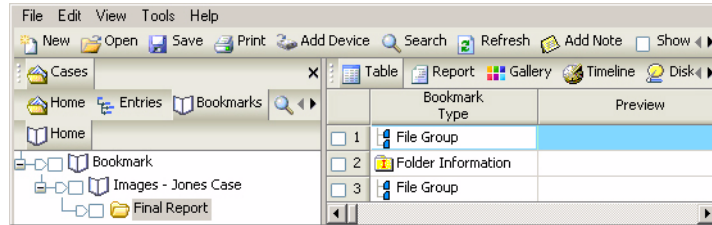


Figure 26-4: Reordering bookmark position

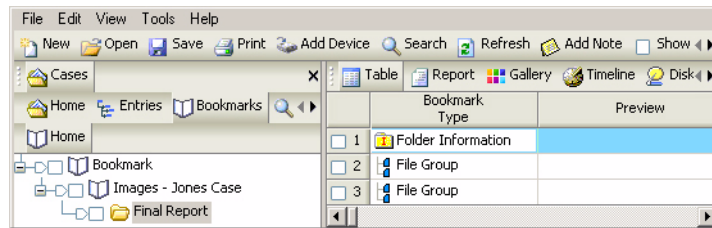


Figure 26-5: Reordered bookmark folder

To add the volume parameters of a partition to the final report, return to the **Entries** subtab under **Cases**. Right-click on the volume and select **Bookmark Folder Structure**.

Select the **Destination Folder** and check the **Include Device Information** box. Leave the **Columns** set at [3] to show the folder structure of the partition.

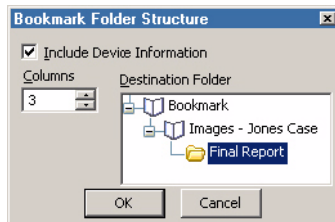


Figure 26-6: Adding the volume parameters to the report

To move the volume parameters report up to the second row, below the physical drive Folder Information bookmark, drag it to row 2.

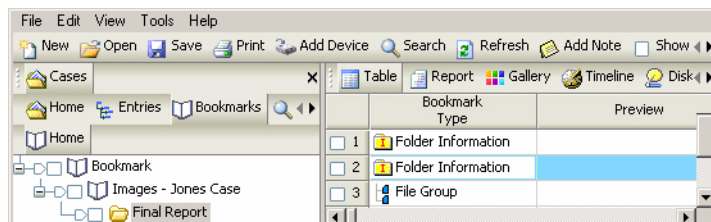


Figure 26-7: Reorder the bookmark

Click on the **Report** view tab in the Table Pane. The EnCase final report will be generated in the order listed within the bookmark folder. The bookmark sub-folders can also be reordered.

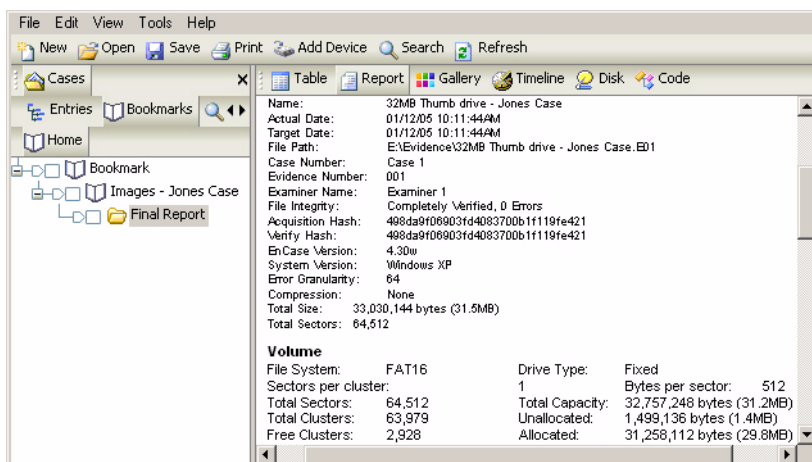


Figure 26-8: Final report

Reordering Bookmarks for Reports

Bookmarks can be sorted on any column, up to five sub-sorts. Some situations in which sorting is very helpful is illustrated by an EnCase examiner in Canada:

- Sort JPGs by file size in **Table** view and switch to **Gallery** view to examine them. The bigger images are then in one spot. The bigger is most often the unauthorized images.
- Sort images by file size in table and examine by file size. Identical looking images with different hash values may be indications of Steganography

- Sort images by creation date in table view and examine in the **Gallery** view. The images downloaded from the Internet can now be viewed in the chronological order that they were downloaded
- Bookmark the images downloaded from the Internet that are most relevant. Go to **Bookmarks**. Ensure sort by date created and go to **Report** view. The images are now in the report in the order they were downloaded.
- Keystroke loggers and stealth screen capture software can create .JPGs that are recoverable. These need to be added to a report in the order they were created to show a logical pattern.
- Word documents in table view of relevance are bookmarked. A report is created listing the documents in the chronological order they were created
- File Finder EnScript creates a bookmark folder of the recovered .JPGs and adds a comment field to each image. Sort by comment field and the recovered images can be grouped per the type of camera that took them.
- Surveillance cameras set up to take hidden cam shots every 10 seconds are sometimes identified in unallocated space and the only way to sort to prepare a logical sequence of images is to experiment with sorting by starting extent or physical location. A report prepared with images sorted in sequence makes the difference of what appears to be a movie, to a scrambled assortment of images with no cohesiveness.
- Text files are sometimes found containing chat sessions with individuals, often in the hundreds. These can be book marked and included in a report. These should be sorted chronologically in the report to give it any meaning.

After the columns are sorted in the desired order, right-click in the **Table** view and choose **Adjust Rows** to set the bookmark entries in the current sort order for the report. This prevents examiners from accidentally losing an import report created

by improperly clicking the mouse. The report stays in the last format, until the **Adjust Rows** function is set again for a new report.

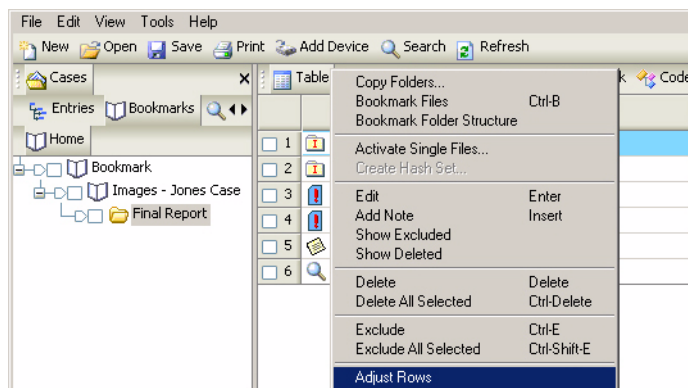


Figure 26-9: Using Adjust Rows

Presenting Multiple Images

Many forensic examinations recover multiple digital images. After bookmarking the images relevant to the investigation, the examiner can export custom reports containing these images from EnCase. The reports can be the standard rich text format (.RTF), viewable in Microsoft Word and printed in hard copy. Hypertext markup language (HTML) web pages can also be created when exporting for a paperless report on compact disc. The HTML format allows the reader to browse the recovered images as thumbnails and print out only the images required for a proceeding or in court.

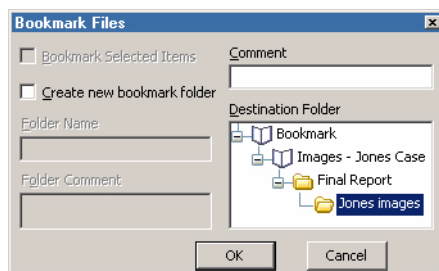


Figure 26-10: Book marking multiple images

After bookmarking the images inside EnCase, create a new folder on the examination hard drive to receive the report and copies of the evidence images.

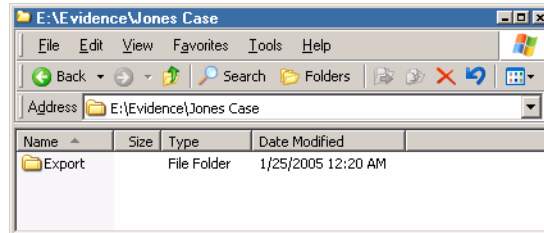


Figure 26-11: Folder for reports and images

In the **Bookmarks** subtab in the Tree Pane, select the bookmark folder containing the desired images. In the Table Pane, select the **Report** tab. Right-click on the **Bookmark** folder and select **Edit**. Customize the format of the report by inserting comments in the **Comment** box and adding data fields to the report. Double-click on the fields in the lower right **Fields** pane to move the field to the **Format** pane. This will show those properties in the report. If the examiner does not set the properties of a **Bookmark** folder, the folder will inherit the properties set for its parent folder.

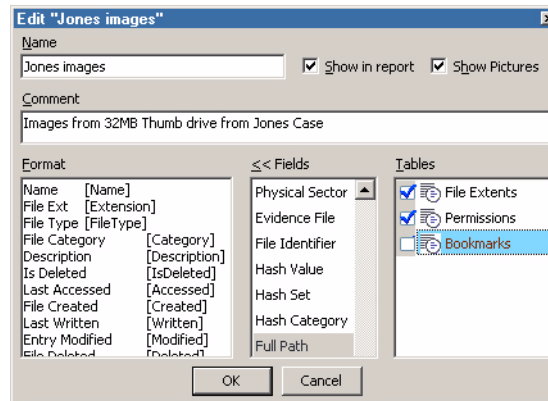


Figure 26-12: Customizing the format of the report

Exporting the Report

In the right pane, showing the **Report** view, right-click on the report and select **Export**.

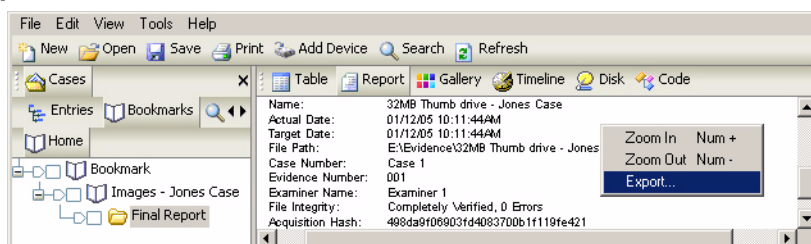


Figure 26-13: Exporting the report

It is possible to export the report in two different formats:

- **Rich Text Format (RTF)**

If the report is exported as a rich text format file, the file can then be easily edited with a word-processing application such as Microsoft Word. This is a good option for investigators who might need to customize their report.

- **Hyper Text Markup Language (HTML)**

If the report is exported as an HTML format file, hyperlinks for quick and easy navigation through the report can be created. The limitation is that editing the report in a WYSIWYG (What You See Is What You Get) environment requires an HTML editing program such as MS FrontPage.

Regardless of which format desired, browse to the folder to receive the report and select [OK].

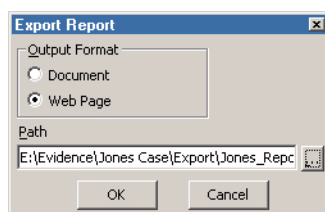


Figure 26-14: Exporting the report as an HTML file

Exporting the report as an HTML file will copy/unesave bookmarked images from the evidence file to the selected folder, as well as create four HTML files:

- Full HTML report with the name assigned by the examiner.
- **gallery.html**, which contains a thumbnail viewer for the exported files.

- **toc.html**, which contains a table of contents of hyperlinks to the full report created and named by the examiner, and to the gallery created by exporting in the **gallery.html** file.
- **Frame View.html**, which creates a frame view of the other three files, with the table of contents at the top and either the full report or the gallery displayed in the lower frame. The **Frame View.html** file is the one that should be opened to view the results. This is also the file to link to from text on a summary report file on the compact disc.

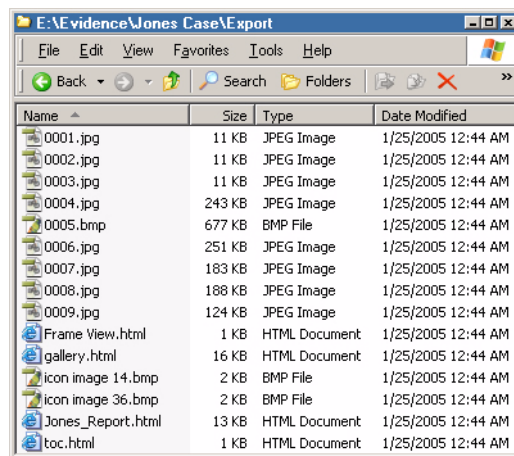


Figure 26-15: Files created by HTML report export

Double-clicking on the **Frame View.html** file will open the default browser. The full report, created and named by the examiner, is displayed by default. The table

of contents in the upper frame provides hyperlinks to browse to the **Gallery** view and to return to the report.

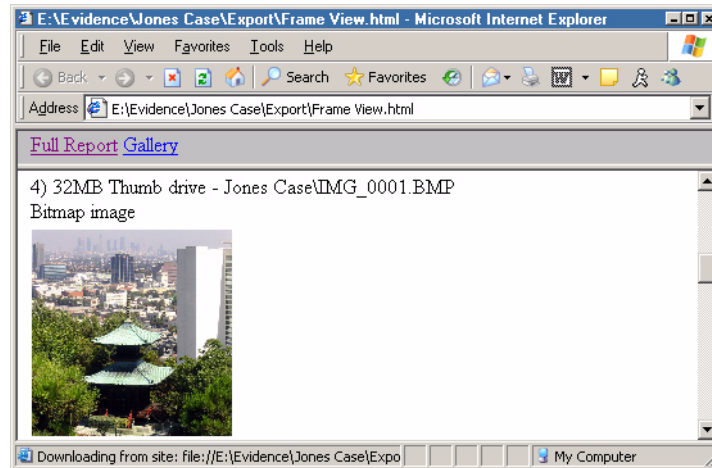


Figure 26-16: HTML report, full view

Clicking on the **Gallery** hyperlink will open **gallery.html** in the lower pane, and display thumbnails of the images copied/unerased out of the EnCase evidence file. The reader can use the **Gallery** to browse the exported files.

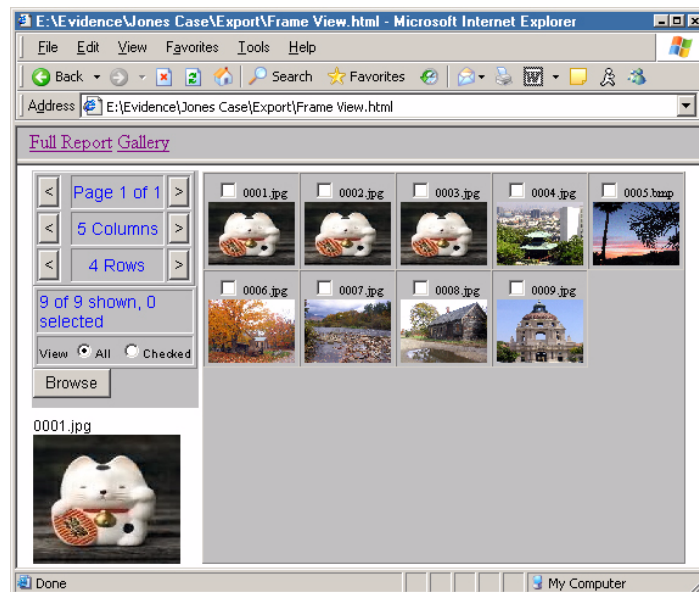


Figure 26-17: HTML report, gallery view

To view the image in full size, select the image thumbnail and it will be displayed in the bottom-left corner of the **Gallery** web page. Double-click on the image in the lower-left corner and Internet Explorer will open a new window containing the full-sized image.

Documenting All Files and Folders Contained on Media

To document all of the files and folders contained in a case, from the **Entries** subtab beneath **Cases**, click the **Set Include** trigger on the physical drive or media in the left pane. In the right pane, select **Table** view. Sort the rows by the **File Ext** column and sub-sort by the **Full Name** column. Right-click anywhere in the right pane and select **Export**.

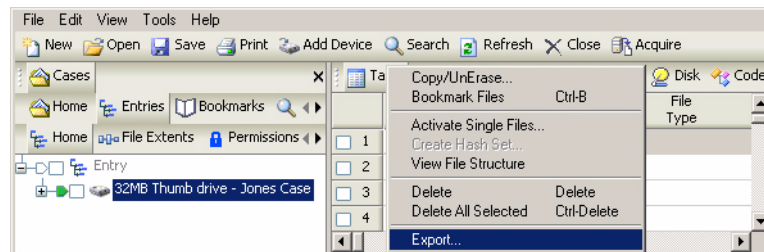


Figure 26-18: Export a spreadsheet index

In the **Export Table** window, check the columns to be included in the spreadsheet. To include all of the columns, check the first box, scroll down to the last box, hold down the **[Shift]** key, and check the last box. Leave the default to export all of the rows.

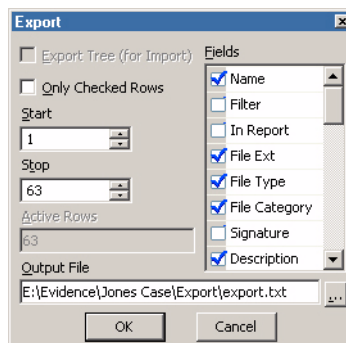


Figure 26-19: Setting export columns and rows

In the **Output File** field, entering a file name and changing the extension to **.xls** will automatically associate the file with Microsoft Excel without the extra steps of

importing a tab-delimited text file. The file can become quite large, especially when cataloging large-capacity hard drives.

Presenting Search Results

EnCase creates search hit folders under the **Search Hits** tab for each search session. A list of these search hits can be exported to a spreadsheet for inclusion in the report as follows:

- Select the **Set Include** button on the **Search Hit** folder in the **Search Hits** subtab; select **Table** view in the right pane.
- In the right pane, right-click and select **Export**.
- In the **Export** window, browse to the folder to receive the exported report.
- Name the report and change the extension to **.xls** for Microsoft Excel.
- Under the **Search Hits** tab, select the first keyword folder.
- In the Table Pane, right-click and select **Export** to send the search results to a spreadsheet.



Figure 26-20: Exporting search results

- In the **Export Table** window, select the rows and criteria to be exported.

- Name the export file with an **.xls** extension for Microsoft Excel.

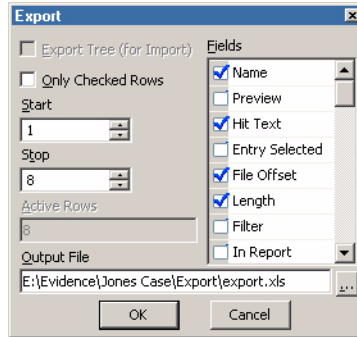


Figure 26-21: Selecting export criteria

- Export each of the **Search Hit Results** folders into separate Excel spreadsheets.

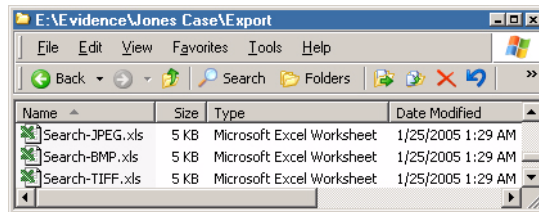


Figure 26-22: Search results as Excel spreadsheets

- Open the exported **Search Session** report with Microsoft Word. Microsoft Word 97 (and higher) features a competent HTML editor that can be used to customize exported EnCase reports and create paperless hyperlinked examination reports.
- Highlight text to be hyper linked. The Hyperlink window can be opened in three different ways:
 - Right-click on the highlighted text, and select **Hyperlink**
 - Use a hotkey sequence (**[Ctrl][K]**)

- Click on the hyperlink button on the tool bar

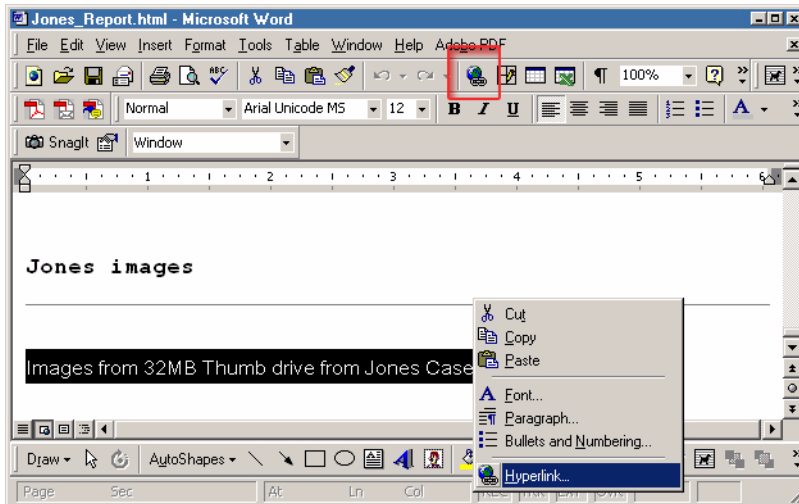


Figure 26-23: Creating a hyperlink in MS Word

- In the **Insert Hyperlink** window, type the name of the file to be linked or use the [**Browse**] button to find the file. Word will create a hyperlink in the report displaying the highlighted text to the linked file.

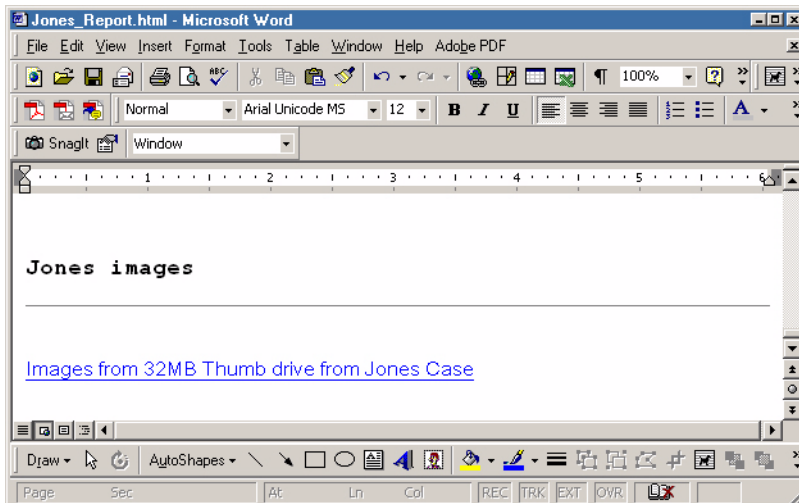


Figure 26-24: Hyperlinked text in report

- When the reader clicks on the hyperlink in the report, Windows will open the linked file and display the search results.

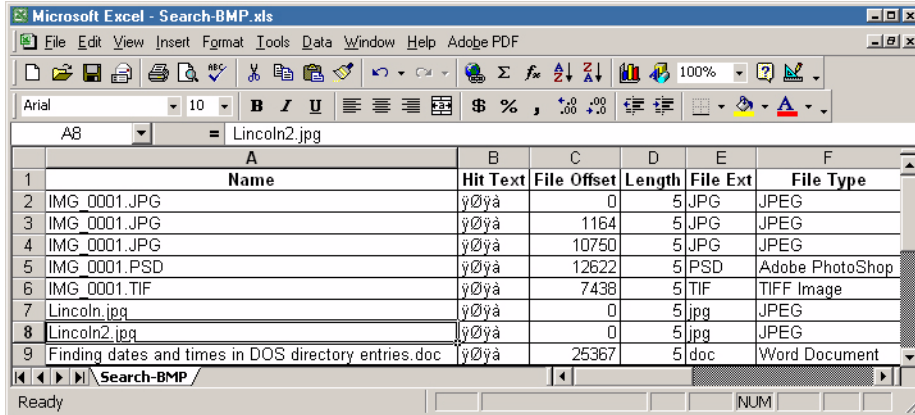


Figure 26-25: Opening hyperlinked text

This method of exporting customized sub-reports from EnCase and linking the reports from a summary examination report can be used to create paperless, courtroom-ready presentations. The reports will reflect the professional nature of the examination.

APPENDIX A

Forensic Terminology

Computer forensics, like most technical fields, has its share of jargon. Many of the terms in this guide have a precise meaning and should be understood thoroughly before attempting to use EnCase.

PC Hardware

- **Storage Computer/Media**

The Storage computer is the EnCase investigator's computer. The term Storage will loosely refer to either the examiner's hard drive or the examiner's computer.

- **Subject Computer/Media**

The Subject is the computer or media that is being examined. In the past this has been referred to as the *Target* or *Source*. However, those terms are vague and open to interpretation. Subject is the term that will be used from now on.

- **RAM**

Random Access Memory. Each computer has a certain amount of volatile read/write memory locations whose contents are lost when the power is turned off. The operating system, programs and drivers are all loaded into RAM at the same time.

- **ROM**

Read Only Memory. Chips that contain a permanent program that is “burned in” at the factory and maintained when the power to the computer is turned off. As its name implies, the information on the chips can only be read and not written to (i.e. your computer cannot store information in these chips). They usually contain small programs and data that are needed to boot the computer.

- **BIOS**

The Basic Input Output System of a PC. This is usually a number of machine code routines that are stored in ROM and available for execution at boot time. The “boot strap loader” is contained in ROM and is the first code to execute when the computer is turned on. The BIOS contains commands for reading the physical disks sector by sector.

Hard Drive Anatomy

- **Drive Geometry**

A physical drive is usually composed of any number of rapidly rotating platters with a set of read/write heads for each side of each platter. Each platter is divided into a series of concentric rings called tracks. Each track is further divided into sectors. Each sector is then divided into bytes. The number and position of these structures is referred to as the drive geometry.

- **Cylinder**

A cylinder, like a track, is a logical term and does not refer to a physical piece of hardware. In other words, you can't open a disk drive cover and see the “cylinders”. A cylinder refers to the set of tracks on every side of every platter that are at the same head position, as if an actual cylindrical cross-section had been taken out of the whole drive. If a drive contains 4 heads, a cylinder refers to all the information that is available to all the heads while on a single track.

- **Head**

There is one head for every side of every platter in a hard disk drive. They ride very close to the surface of the platter and allow information to be read from and written to the platter. The heads are attached to an arm, which is in turn attached to a head stack assembly. Normally, all heads move together and are positioned on the same logical track together. Heads are numbered sequentially from zero.

- **Sector**

A sector is a group of bytes within a track and is the smallest group of bytes that can be addressed on a drive. There are normally tens or hundreds of sectors within each track. The number of bytes in a sector can vary, but it is almost always 512. CD ROMs normally have 2048 bytes per sector (this does not include the hundreds of bytes per sector for error checking and correction). Sectors are numbered sequentially within a track, starting at 1. The numbering restarts on every track, so that “track 0, sector 1” and “track 5, sector 1” refer to different sectors.

- **Track**

Each platter on a disk is divided into thin concentric bands called Tracks. There is no physical structure associated with a track. Tracks are established when the disk is low level formatted. Tracks are numbered sequentially starting with track 0 on the outermost part of the platter, moving inwards.

- **Absolute Sectors**

Early disk drives contained a number of cylinders, heads and sectors and these numbers would refer to actual hardware present in the drive. The BIOS would address the disk controller directly and translate absolute sector numbers into C-H-S before writing to or reading from the disk. As disk capacities increased to unforeseen sizes, manufacturers and software developers were forced to change the stated number of cylinders, heads and sectors in order to trick the BIOS into addressing the additional space.

Today, the Cylinder, Head and Sector numbers are usually fictional and do not refer to actual disk structures or hardware. These numbers are first translated by the BIOS, and then translated by the low-level disk device driver, and then again by the drive hardware, into numbers that make sense for the actual media. You can run yourself ragged trying to figure out exactly where on the physical device the data is stored, and it rarely makes any difference.

Fortunately, there is always a well-defined order in which the sectors are addressed. They are numbered sequentially from 0 to N-1, N being the total number of software addressable sectors present on the drive.

Some disk utilities will report Cylinder-Head-Sector numbers, but the new BIOS extensions have made this convention obsolete. Also, as a practical matter, it is easier to refer to a sector by one number, rather than three.

EnCase follows the new convention and refers to sectors as if the entire drive were a large flat array of sectors, starting at sector 0. When viewing a location on a physical disk, EnCase will show the CHS numbers for compatibility with other disk utilities.

- **Platter**

A platter is a magnetized disk that the actual data of the hard drive is stored on. Modern hard drives typically have two platters, with heads reading and writing data to the platters simultaneously.

• Drives, Disks and Volumes

The terms “volume”, “drive” and “disk” are often used interchangeably in other literature. It is very important to understand the distinction between these terms as they are used with EnCase.

A “disk” is an actual piece of hardware that you can hold in your hand. It could be a floppy disk, hard disk, Zip Disk or any other piece of physical media.

A “volume” refers to a mounted partition. There may be only one “volume” on a “disk” as is the case on a floppy or Zip disk or there may be several volumes on a disk as on a partitioned hard drive.

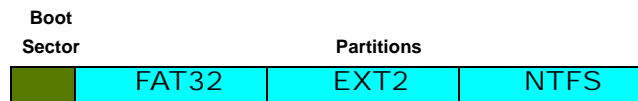
A volume is a concept, not a physical device. Early PC disks contained only one volume (e.g. “C”). As drives grew larger, it became convenient to partition a single physical disk into a set of logical volumes. There can be any number (up to 24, as in C, Z) of these logical volumes on a disk and they show up as drive “C”, “D” or “E” in DOS (when formatted FAT32.)



Figure 27-1: Multiple devices in case

Hard Drive Layout

• Master Boot Record



The very first sector of a physical disk (absolute sector 0) is called the master boot record (MBR). It contains machine code to enable the computer to find the partition table and the operating system. One of the first things a computer does when it starts up is to load this code into memory and execute it. This “boot code” has a very simple task. Its job is to read the partition table at the end of sector 0 and decide how the disk is laid out, and which partition contains the bootable operating system.

- **Partition Table**

The partition table describes the first four partitions, their location on the disk, and which partition is bootable. This is indicated by a single byte in the partition table. In fact, the entire logical layout of the disk is determined by 64 bytes of information. It is quite easy to hide or change information or even entire volumes from DOS by changing a single byte in the partition table.

- **Extended DOS Partitions**

Normally, each partition table entry describes a volume to be mounted by the file system. If more than four partitions are on the drive, a special partition type called an “Extended Partition” is created. In this configuration, the first sector of every extended partition is itself a boot sector with another partition table. This table has a duplicate copy of the partition entry for that volume that contains a sector offset into the current partition where the logical volume begins.

- **Volume Boot Sector**

Since every partition may contain a different file system, each partition contains a “volume boot sector” which is used to describe the type of file system on the partition and usually contains boot code necessary to mount a file system. This code is different from the master boot record code described earlier. The job of the volume boot code is to find a file in the root folder (io.sys in the case of DOS) that is then loaded and run to continue the boot process at a higher level. On Linux systems, the LILO boot loader serves the same purpose. It locates the Super Block that describes the rest of the file system.

- **Inter-Partition Space**

The sectors on the track between the start of the partition and the partition boot record are normally unused by any file system. This results in tens or even hundreds of sectors going to waste (not a big deal on a large drive). However, since this area is inaccessible to all but low-level disk viewers, it is theoretically possible to hide information there. EnCase labels these areas as “Unused Partition Area” and allows you to search and inspect their contents. These areas are also searched along with the rest of the disk, whenever a normal keyword search is done.

File System Concepts

- **Clusters**

A cluster is a group of sectors in a logical volume that is used to store files and folders. Clusters must contain a number of sectors that is a power of 2 (i.e. 2, 4, 8, 16, etc...). DOS maintains information about each cluster in the File Allocation Table. NTFS partitions store that same information in the file extents tables and the volume bitmap. EXT2 partitions store the information in the Inode Tables and Block Bitmaps. CD's usually have unfragmented file extents, so there is no need for a cluster bitmap or a FAT.

- **Cluster Bitmaps**

Each cluster on a file system is either used or available for allocation (free). In DOS, the state of the clusters is kept track of in the File Allocation Table. A "0" entry in the FAT indicates that the cluster is free, otherwise there are different codes to indicate which part of its file the cluster belongs to. NTFS keeps track of free clusters with a "bitmap". This is a file that contains 1 bit for every cluster on the volume. This file is put on the drive when it is formatted. EXT2 drives contain a block bitmap for every group, but the concept is the same.

- **Root Folder**

All file systems have a "tree" structure that supports files and folders within folders to an arbitrary depth. The "root" of this tree is always stored in a known location.

On FAT12 and FAT16 volumes, the root folder resides at a fixed location on the drive and contains a maximum number of entries that is determined when the volume is formatted. The number of files and folders in the root folder of such a volume is limited, but the number and size of the rest of the folders in the disk is essentially unlimited, because they are treated like normal files and can expand if space is available on the volume.

On FAT32 volumes, the root folder is also treated like a file and can contain any number of files or folders. Its location is stored in the volume boot record.

NTFS stores the root as a special file in the Master File Table. The name of the file is "." (dot).

EXT2 drives store the root as a special Inode in the first group.

CDFS give the location of the root folder in the boot sector.

- **File Entries**

A folder is treated just like a file on FAT and EXT2 volumes. Each folder contains a starting cluster and can be expanded or contracted as files are added or removed from the folder. Each file in the folder is represented by a 32-byte entry in a table. In other words, the content of a folder “file” is an array of records containing information about the files in the folder. Each entry in the folder can be either a file or another folder. In this way, a “tree” structure can be built. A 32-byte entry contains enough space for an 8.3 character file name. Windows 95 implements long file names by chaining together a number of entries and using the space to store the additional characters in the file name.

- **File Slack**

The space between the logical end and the physical end of a file is called the file slack. The diagram below shows a section of a disk that has 2 sectors per cluster. Since each cluster is 1024 bytes, the file takes up two clusters and has a physical size of 2048 bytes. The logical end of a file, in this example, comes before the physical end of the second cluster. The remaining bytes are remnants of previous files or folders. EnCase searches file slack by default.

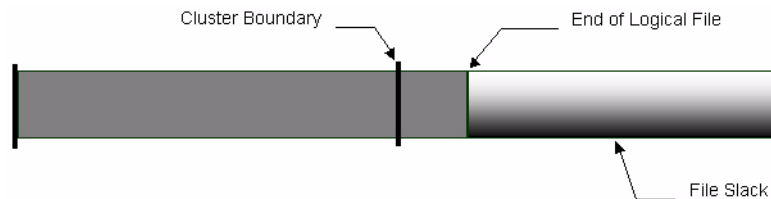


Figure 27-2: File Slack

- **Logical File Size**

All file systems keep track of the exact size of a file in bytes. This is the logical size of the file and is the number that you see in the properties for a file. This number is different from the physical file size.

- **Physical File Size**

The physical size of a file is the amount of space that the file occupies on the disk. A file or folder always occupies a whole number of clusters, even if it does not completely fill that space. A file always takes at least one cluster, even if it is empty. Therefore, even if a file has a logical size of only five bytes, its physical size is one cluster. EnCase displays both logical and physical size for every file.

- **RAM Slack**

The space from the end of the file to the end of the containing sector is called RAM slack. Before a sector is written to disk, it is stored in a buffer somewhere in RAM. If the buffer is only partially filled with information before being committed to disk, remnants from the end of the buffer will be written to disk. In this way, information that was never saved can be found in RAM slack on disk. EnCase searches all file slack by default.

- **Volume Slack**

On a formatted volume, there are a certain number of available sectors. These sectors are grouped together in clusters or blocks depending on the file system. If the number of possible clusters does not divide evenly into the number of available sectors, there will be some sectors left over at the end of the partition. These sectors are not used to store file/folder information by the file system. This wasted space is known as Volume Slack, and is usually less than the size of a cluster/block. Deleted files, hidden data and remnants of previous partitions could possibly be found in the volume slack

File Systems

- **File Allocation Table (FAT)**

The FAT is an array of numbers that sits near the beginning of a DOS volume. These numbers can be 1½ bytes (12 bits), 2 bytes (16 bits) or 4 bytes (32 bits) long depending on the size of the volume. This is why volumes are sometimes referred to as FAT12, FAT16 or FAT32.

Each entry in the FAT corresponds directly to one cluster and there is always one FAT entry for every cluster. Each entry is either a code indicating that the cluster is free, the cluster is bad or that this is the last cluster in a file. If it is not one of these codes, then the number refers to the next cluster in the chain belonging to a file. The first cluster in the chain for a file is recorded in the properties for that file, which are stored in its parent folder. The FAT is therefore a one way linked list of clusters for every file in a volume.

Folders on FAT drives are stored as special files. The content of these files are the records for each of its children. These “folder files” take up space on the volume along with the other normal files.

- **NTFS**

NTFS has an advanced structure that is designed to overcome the limitations of other file systems that have come before it. The file descriptors for every file on an NTFS volume are stored in the Master File Table (MFT), including

a reference to the MFT itself. Each file descriptor contains the name and other attributes of the file along with its extents list. This list contains the location of the file on the volume. Another file called the volume bitmap describes the free clusters on the volume. Folders are stored in a b-tree structure for quick disk access.

- **EXT2/3**

The EXT2 file system is the primary file system used on the Linux operating system. EXT2 partitions are divided into a series of Groups. Each Group contains a series of Inodes and Blocks. The Inode tables describe the files that are located within each group. As with the FAT file system, a folder is a file that contains descriptors for each of its children. EnCase can read and interpret the EXT2 file system and present its folder structure and files along side the rest of your evidence. EXT3 is EXT2 with journaling.

- **REISER**

The Reiser file-system is a “flavor” of EXT2. EnCase has the ability to mount and interpret the Reiser file system.

- **CDFS**

This ISO9660 standard is used to describe the files structure on a CD. There are many variations of the basic structure. The most notable is the Joliet standard that is used by Windows to allow for Unicode file names. EnCase can read and interpret the CDFS file system and present its folder structure and files along side the rest of your evidence.

- **HFS and HFS+**

This is the Macintosh and Power Macintosh file format. EnCase has also refined its support for other files systems. The Macintosh OS X Server operating system uses the Hierarchical Files System Plus (HFS+) without the wrapper of HFS. EnCase now supports this configuration.

- **Palm**

The PalmOS file system consists of databases with records, which store both executable applications and program data. Currently, the PalmOS is found on devices manufactured by Palm, Inc. (Palm), Handspring (Visor, Treo), Sony (Clie), some cell-phones (Kyocera pdQ and Samsung I-300) as well as a handful of other devices made by companies such as IBM, Handera, and Symbol.

- **UFS**

This is a common Unix file-system. However, Unix, like ice cream, has many flavors. Though EnCase can acquire all flavors, at this time, it can only interpret UFS.

Disk Configurations Explained

A Disk Configuration is a Redundant Array of Inexpensive Disks or RAID. There are commonly three types of RAID: **RAID 0**, **RAID 1**, and **RAID 5**.

- **RAID 0: Striping**

The first but not necessarily the most basic RAID type is RAID 0, or striping. The main purpose of RAID 0 is to provide speed. In fact, RAID 0 has no fault tolerance. If one drive in the array fails, the whole array is shot. There is no way to rebuild or repair the information stored on a RAID 0 array. This makes a RAID 0 setup the most susceptible to failure, a fact that usually keeps users with sensitive data from choosing RAID 0 as their RAID setup.

At the same time, however, RAID 0 is the fastest of all RAID setups. Since there is no overhead required to store extra information for fault tolerance, the speed of RAID 0 can theoretically perform 2 times the speed of a single drive when there are 2 drives in the array. Adding more drives only increases this theoretical performance amount a six-drive RAID 0 array's performance could be as fast as 6 times the performance of a single drive.

- **RAID 1: Mirroring**

Although speed can be an important aspect of computing, so can the safety and reliability that comes with fault tolerance. Speed is sacrificed, but RAID 1 provides users with a level of safety nonexistent in RAID 0.

RAID 1 works by writing identical sets of information to two drives in an array, otherwise known as mirroring. When the controller is sent a 64KB file to be written to a two disk RAID 1 array, the controller sends identical copies of this 64KB file to both disks in the array. Reads are the same as on a single drive the controller requests the file from one of the two drives.

The special feature of RAID 1 is its fault tolerance. If either of the two drives in the array fails, no data is lost. When a drive fails, the RAID controller uses the information off of the drive that is still available. When a new drive is added to the array to fix the failed one, a mirroring occurs in which the data from the good drive is written to the new drive to recreate the array again.

As one could suspect, RAID-1 offers very little in terms of performance. When requesting data from a drive, some RAID controllers take information from

the drive that is not busy or closer to the desired information, theoretically resulting in faster data access. When writing, on the other hand, there is some overhead when compared to a single drive as the controller must duplicate the file it is sent and then pass it along to the drives.

In a RAID-1 setup, identical drives are best in order to prevent lost space. Since the same data is being written to two drives, the size of the RAID-1 array is equal to the size of the smallest drive in the array. For example, if a 20GB drive and a 30GB drive are used in a RAID-1 setup, the array would only be 20GB with the 10 extra gigabytes on the 30GB drive going to waste. The performance difference between two drives is also an issue here, since a faster drive would have to wait for a slower drive before it could write more information.

RAID-1 is a good solution for those looking for security over speed. Although not the slowest of the common RAID types, RAID-1 can be slower than a single drive in some cases (more on that in the benchmarks). What RAID-1 does provide is a very safe environment, where failure of a single drive does not equate to any down time.

In addition, EnCase now supports the Mirror RAID (RAID-1) configuration of NTFS Dynamic Disks normally found on Compaq Windows's servers. If only one of the mirrored drives is present, the file structure is still available for examination.

• RAID 5

RAID 5 requires at least 3 drives and attempts to combine the speed of striping with the reliability of mirroring. This is done by striping the data across two drives in the array at a user defined stripe size. The third drive in the array, the one not getting striped data, is given a parity bit. A parity bit is generated from the original file using an algorithm to produce data that can recreate the information stored on both drives that received the striped data.

The two drives receiving the striped data and the one receiving the parity bit are constantly changing. For example, if drives 1 and 2 receive striped data on a write and drive 3 receives a parity bit, on the next write drives 2 and 3 will receive the striped data and drive 1 will receive the parity bit. The shifting continues and eliminates the random write performance hit that comes with a dedicated drive receiving the parity information.

The parity information is typically calculated on the RAID controller itself, and thus these types of controllers are called hardware RAID controllers since they require a special chip to make the parity information and decide what drive to send it to.

RAID 5 arrays provide a balance between RAID 0 and RAID 1 configurations. With RAID 5, some of the features of striping are in place as well as the features of mirroring. Thanks to the parity bit, if information is lost on one of the three drives in the array, it can be rebuilt. Thanks to the striping it uses to break up the data and send it to multiple drives, aspects of speed from RAID 0 are present. Recreation works in the following manner. Let's use a 3 drive RAID 5 array with a 64KB stripe size for an example with a 128KB file that needs to be written. First, a parity bit is created for the file that the controller card has received by performing an XOR calculation on the data. Next, the 128KB file is broken into two 64KB files, one of which is sent to drive 1 and the other to drive 2. Finally, the parity information calculated above is written to the third drive in the array.

Now, if one of the drives, or a portion of a drive, in the array goes bad and the 128KB file is lost, the data can be recreated via an xor operation between the remaining drives. It does not matter which drive fails all the data is still available. If the third drive in the above example, the one that received the parity information for this write, fails then the original data can be read off of drives 1 and 2 to recreate the parity information. If either drive 1 or drive 2 fails, then the parity information stored on drive 3 can be used to recreate the information lost on the original drive.

There is a significant overhead associated with RAID 5, however, due to the parity bit that must be calculated and written to on each drive. This is especially present when changing only one piece of information on one drive in the array. During this process, not only does the information that requires changing require writing but the parity bit must also be recreated. This means that once the data is written, both drives with the stripe blocks on them must be read, a new parity bit be calculated, and then the new parity bit has to be written to the third drive. This problem only increases as additional drives are added to the array.

For the same reasons mentioned in both the RAID 0 and RAID 1 discussions, it is best to use identical drives for a RAID 5 setup. Not only does this ensure speed, it also ensures that all of the array's storage capacity is utilized. The size of a RAID 5 array is equal to the size of the smallest drive times the number of drives in the array minus one (since one of the drives is always getting a parity bit).

RAID 5 does provide a good balance between speed and reliability and is a popular configuration for arrays in a variety of systems, from servers to workstations. The data security made possible with the parity bit as well as the

speed and space provided by RAID 5 have many high-end system builders turning to RAID 5.

Evidence Storage

- **Compression**

Compression technology allows EnCase to store a large disk in a relatively small file. EnCase uses an industry standard compression algorithm to achieve an average of 50% size reduction. If most of the disk is unused, the compression ratio can be much higher. This can result in great savings in disk storage space. Compressed Evidence Files take longer to generate because of the additional processing time required to compress information.

Compression **NEVER** has any effect on the final evidence, and compressed blocks are checked for validity in the same way as uncompressed ones.

- **MD5 Hash**

The MD5 hash is a 128-bit (16-byte) number that uniquely describes the contents of a file. The code to compute the MD5 was developed by RSA and is publicly available. For this reason, the MD5 hash is a standard in the forensics world.

Professor Ronald Rivest created the MD5 hash algorithm in 1991. It is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

The odds that two files with different contents have the same hash value is roughly 2^{128} or 3.4×10^{38} . If the hash values match, there is reasonable certainty that the file contents matches.

The purpose of the MD5 hash value within EnCase is two-fold. The first is to verify that the evidence file EnCase created is indeed the same in byte-structure as the original media; the second is for the creation of Hash Sets to add to your Hash Library.

EnCase calculates an MD5 Hash when it acquires a physical drive or logical volume. The hash value is written into the evidence file and becomes part of the documentation of the evidence. When an evidence file is added to a case, EnCase automatically verifies the CRC values, and re-computes the hash value for the evidence data within evidence file. The hash value that is stored in the evidence file, and the hash value that is computed when the evidence file is added to a case, appear in the Report for immediate confirmation that the

evidence file has not changed since it was acquired. At any time while using EnCase, you can select the case view, right-click on the physical drive or logical volume, and select Hash to re-compute the hash value of the drive or volume. The hash is generated as the data is read from the source device. The acquisition hash is the hash of the data that is acquired, and the verification hash is the confirmation of the acquired data. Both EnCase for DOS and EnCase for Windows give the examiner the option of hashing the source device itself before or after acquisition. This is not done by default due to the amount of time required, and is instead provided as an option to the user. In EnCase 4.13 and above, if you choose to hash a device separately from an acquisition in Windows, EnCase will automatically create a note of the date/time and results of hashing the device. This note is placed on the root folder of the device under the Bookmark view, for inclusion in your Final Report if you wish. Of course in EnCase for DOS, it still writes the results to a text file. You can bring the text file results into EnCase with Add Raw Image function under the File tab, for inclusion in your report.

One note on imaging devices with corrupted or damaged sectors. EnCase is building the hash value of the acquired device as it is reading the data from the sectors. If a sector is damaged or has corrupted data, the next time you make a hash of the device, the hash value may be different, as well as the next, and the next and so on.

- **CRC (Cyclical Redundancy Checksum)**

EnCase uses a CRC to verify the integrity of each block of data. The Cyclical Redundancy Checksum is a variation of the standard checksum, and works in much the same way. The advantage of the CRC is that it is order sensitive. The odds that two different data blocks produce the same CRC are roughly 1 in 4 billion.

Most hard drives store one CRC for every sector (512 bytes). When a read error is generated from a disk, this usually means that the CRC value of the sector on disk does not match the value that is recomputed by the drive hardware after the sector is read.

CRC values can be “reverse engineered” meaning that it is possible (though difficult) to force the CRC value of one document to match that of another by altering non-printing characters within the document. For this reason the method of choice for document verification is the MD5 hash. (See MD5 Hash)

- **File Signature**

Many (but certainly not all) file types contain a few bytes at the beginning that constitute a unique “signature” of that file type. Most graphic and document file types contain a signature. For example, the first 6 bytes at the beginning of a GIF file are either GIF89A or GIF87A. This allows EnCase and other applications to sense the true type of a file, regardless of the file's name extension.

Evidence Files Explained

The central component of the EnCase methodology is the Evidence File. This file contains four basic parts (the header, checksum and data blocks and the MD5 block) that work together to provide a secure and self-verifying description of the state of a computer disk at the time of analysis.

- **Evidence File Format**

The EnCase process begins with the creation of a complete physical bit-stream mirror image of a target drive in a completely non-invasive manner. The acquired bit-stream mirror image, called an Evidence File, is mounted as a read-only file or “virtual drive” from which EnCase proceeds to reconstruct the file structure utilizing the logical data in the bit-stream image. This allows the examiner to search and examine the contents of the drive in a Windows GUI in a completely non-invasive manner. Throughout this process, the bit-stream image is continually verified by both a CRC value for every 32K block as well as an MD5 hash calculated for all data contained in the Evidence File. Both the CRC and MD5 hash values are immediately assigned to the Evidence File upon acquisition.

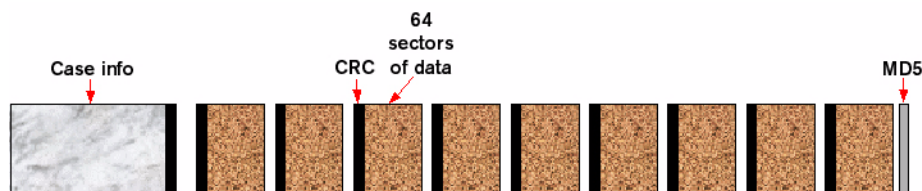


Figure 27-3: Evidence file composition

Each file contains an exact, sector-by-sector, copy of the disk. When the file is created the user gives information relevant to the investigation and EnCase archives this and other information inside the Evidence File along with the contents of the disk. This information in the header of the Evidence File is itself authenticated with a separate CRC.

Throughout the examination process, EnCase verifies the integrity of the evidence by recalculating the CRC and MD5 hash values and comparing them with the values recorded at the time of acquisition. This verification process is documented within the EnCase-generated report.

It is nearly impossible to tamper with the evidence once it has been acquired. This allows the investigators and legal team to confidently stand behind the evidence in court.

- **Image Verification**

In order to verify that the contents of an evidence file have not changed since the file was created, EnCase will read each sector block in the evidence file, re-compute the CRC for that block and compare it to the original. If the two do not match, the location of the mismatch is recorded in the Case File and shown in the report.

This process occurs automatically whenever a new Evidence File is added to the Case and is proceed in the background.

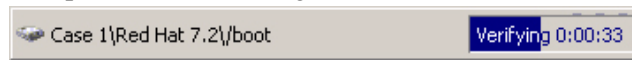


Figure 27-4: - Image verification

APPENDIX B

GREP

GREP Syntax

Symbol	Meaning
.	A period matches any single character.
\255	Decimal character (period)
\x	A character represented by its ASCII value in hex. For example, \x09 is a tab. \x0A is a line feed. Both hex digits should be present, even if they are 0.
?	A question mark after a character or set matches one or zero occurrences of that character or set. For example, "##?/##?/##" would match "1/1/98" or "01/01/89" but would NOT match "123/01/98."
*	An asterisk after a character matches any number of occurrences of that character, including zero time. For example, "john,*smith" would match "john,smith", "john,,smith", and "johnsmith".
+	A plus sign after a character matches any number of occurrences of that character except zero. For example, "john,+smith" would match "john,smith" or "john,,smith" but would NOT match "johnsmith".
#	A pound sign matches any numeric character [0-9]. For example, ### #### matches any number in the form 327-4323 (if looking for a phone number, for example).
[XYZ]	Characters in brackets match any one character that appears in the brackets. For example, "smit[hy]" would match "smith" and "smity".
[^XYZ]	A circumflex at the start of the string in brackets means NOT. Hence, [^hy] matches any characters except h and y.

[A-Z]	A dash within the brackets signifies a range of characters. For example, [a-e] matches any character from "a" through "e" (inclusive).
\[A backslash before a character indicates that the character is to be treated literally and not as a GREP character. For example, "one\+two" matches "one+two". A slash (\) must be placed in front of any GREP token (including a slash (\) itself) that you wish to be a literal part of the match.
{X,Y}	Repeat X-Y times. Example {3,7} would repeat three to seven times.
(ab)	Functions like a parenthesis in a mathematical expression. Groups ab together for +, *,
\wCDEF	Allows the investigator to enter Unicode code for a particular character; 4 integer code is required. See the Unicode chart for mapping.
a b	The 'pipe' acts as a logical OR. So it would read 'a or b'.

GREP Examples

The following examples show some of the power that GREP expressions deliver when looking for text. The first line is the example, followed by an explanation of the symbols used, followed by examples of text found using the expression.

- **john.smith**

The "." matches any single character. This expression finds "john" followed by any character followed by "smith".

```
john smith
john,smith
johnQsmith
NOT john@%smith
```

- **john[,;]smith**

The characters inside the brackets are called a set. The characters in a set are treated as a single character. This expression finds "john" followed by a space OR a comma OR a semicolon followed by "smith".

```
john smith
john,smith
john;smith
```

- **john[0-9a-z]smith**

The "-" indicates a range of characters when inside a set. This expression finds "john" followed by any character between ("0" and "9" or "a" and "z") followed by "smith".

```
john0smith
```

```
john1smith
```

```
johnzsmith
```

- **john[^#]smith**

The "^" at the start of a set indicates any character other than those in the set. This expression finds "john" followed by any character other than "0"- "9" followed by "smith".

```
john smith
```

```
johnQsmith
```

```
john,smith
```

- **john +smith**

The "+" means to repeat the preceding character (or set) any number of times, but at least once. This expression finds "john" followed by any number spaces followed by "smith".

```
john smith
```

```
john      smith
```

```
john                smith
```

- **john-*smith**

The "*" indicates to repeat the preceding character (or set) any number of times including zero times. This expression finds "john" followed by any number of dashes followed by "smith".

```
johnsmith
```

```
john-smith
```

```
john--smith
```

- **john smith\x0D\x0A**

The "\" followed by an "x" indicates a two-digit hex number representation for a character. This expression finds "john", followed by a space, followed by "smith", followed by a carriage return linefeed sequence.

john smith

NOT john smith.

NOT john,smith

- **it'?s**

The "?" repeats the preceding character (or set) one or zero times. This expression finds "it" followed by an apostrophe (or not) followed by "s".

its

it's

NOT it s

NOT it-s

- **c:\\images\\picture\\.gif**

The "\" preceding any character (including "\\") indicates that this is a literal character and not a GREP symbol. Be careful when expressing file names and paths in GREP. Slashes and dots should be preceded by a "\".

c:\images\picture.gif

- **chu[^a-z]**

This expression matches "chu" followed by any nonalphabetic or upper-case alpha character. This ensures that short names and words are not found inside other words. Capital characters, however, will be found.

chu

chuCK

NOT chuck

NOT chump

- **http://www\.[a-z]+\.**

This expression matches "http://www." followed by any lower-case alphabetic characters followed by ".com". This is a good way to look for web site references.

http://www.bozo.com

NOT http://www.to-wong-foo.com

NOT http://www.bozo.org

- **####-####-####-####**

The "#" character matches any number. This expression could match a credit card number where the numbers are separated by dashes.

1234-3623-3410-2232

4534-2123-9866-6512

NOT 1233456780007654

NOT 456

- **[456]###-?####-?####-?####[^\#]**

This expression could match a credit card number where the dashes between the numbers are optional and the first number being constrained to 4, 5, or 6.

6234-3623-3410-2232

4534212398666512

NOT 1233456780007654

NOT 323345680007654

- **\(?\###[\ \-]*###[\ \-]?####[^\#]**

This expression could match a U.S. phone number in one of several formats. The "\(?)" expression means that the open "(" character can be present or not. The "[\ \-]*" expression means that either a space or a close ")" or a dash can be repeated any number of times including zero.

(909) 875-4125

204-725-2436

103 875 4344

9098721344

- `###?#\.\##?#\.\##?#\.\##?#[^\.]`

This expression could match an IP number in regular form with 4 (up to 3 digit) numbers separated by periods.

123.235.23.1

255.255.255.255

0.0.0.0

NOT 234.1234.123.123

NOT 0.0.0.0.

APPENDIX C

Third Party Utilities

While EnCase has many capabilities, it does not and cannot do everything. Therefore we recommend certain third-party utilities that would be helpful to forensic investigators.

Guidance Software does not and cannot be responsible for the performance, availability, or reliability of any of these third-party utilities. We do not and cannot guarantee that we can help you set up, run, or troubleshoot any of these utilities either. We offer the following solely for your benefit and education.

Quick View Plus

For viewing files

<http://www.avantstar.com>

IrfanView

For viewing graphic files (free for home use)

<http://www.irfanview.com>

AC/DSee

For viewing graphic files (free trial version)

<http://www.acdsee.com>

DBXtract

To read Outlook Express 5.0 e-mails (free)

<http://chattanooga.net/~scochrn/DBXtract.htm>

MBXtract

To read Outlook Express 4.0 e-mails (free)

<http://chattanooga.net/~scochran/MBXtract.htm>

Decode Shell Extension

For decoding MIME or UUencoded e-mail attachments. Other potentially useful shareware utilities available at this site as well. (free)

<http://www.funduc.com>

Disk Compare

Compare two disks side-by-side (free)

<http://tp.lc.ehu.es/JMA/win95.html>

Mailbag Assistant

Mailbag Assistant supports several mailboxes, including Outlook Express, Eudora, Netscape Messenger, Pegasus, Forte Agent and The Bat! Support for additional mailers is planned in future versions (\$29.95).

www.fookes.com/mailbag

PST Cracker

Crack passwords in password-protected PST files (free)

<http://www.crak.com/downsoft.htm>

OST2PST

Converts .OST files to .PST files for easy viewing (free)

<http://www.pwdservice.com>

Gpart

A free tool which tries to guess the primary partition table of a PC-type hard disk in case the primary partition table in sector 0 is damaged, incorrect or deleted. The guessed table can be written to a file or device. Supported (guessable) file system or partition types:

- DOS/Windows FAT (FAT 12/16/32)
- Linux ext2

- Linux swap partitions versions 0 and 1 (Linux >= v2.2.X)
- OS/2 HPFS
- Windows NT/2000 FS
- *BSD disk labels
- Solaris/x86 disk labels
- Minix FS
- Reiser FS
- Linux LVM physical volume module (LVM by Heinz Mauelshagen)
- SGI XFS on Linux
- BeOS file system
- QNX 4.x fleshiest

<http://www.stud.uni-hannover.de/user/76201/gpart/>

CD-R Diagnostic

A CD-R diagnostic utility (\$50.00)

www.cdrom-prod.com

Dir to HTML

Free download version; **Dir to Html Pro** £ 4.99

http://www.silvermaine.co.uk/dir_to_html.asp

APPENDIX D

The Forensic Lab

Investigators use EnCase mainly for two different functions – acquisition and analysis. Forensic systems should be designed and built around those two functions. Two different computers might be the best solution.

Field Acquisitions

The most important feature to keep in mind for field acquisitions is *connectivity*. If you cannot bring the Subject's computer or hard drive back to the forensic lab with you, it is of the utmost importance that the correct tools are on-site so that the Subject media can be successfully and reliably imaged. Either a media device or a field computer that will attach to all types of hardware is required.

A *luggable* computer - a small desktop designed for field acquisitions - is an option. The advantage of these computers is that most, if not all, connectivity is on the *outside* of the case. Attaching an internal hard drive to the luggable without even opening the storage computer cover is possible. Many also come with drive drawers, where the subject hard drive can be placed to acquire its data.

Of course, options like that can get expensive. Cheaper alternatives are to bring an external FireWire hard drive into the field (as well as an EnCase Boot Disk with the appropriate DOS drivers for the drive) and attach that to the perpetrator's PC. This could also include external removable media such as external Jaz drives, external Zip drives, etc. With removable media, however, a large amount of media might be required. For a 20-gig hard drive, at least 20 Jaz cartridges would be needed. Furthermore, Jaz drives and other forms of removable media are not as reliable as hard drives. Guidance Software always recommends acquiring media to a hard drive.

Another option is to purchase a small desktop and stock it with a SCSI card (the Adaptec 29160 is recommended), a large hard drive, and at least 512 MB of RAM. A full-fledged field computer is much more versatile than a laptop.

Many investigators use laptop computers in the field for their portability, but laptops can be restrictive in terms of connectivity. The only ports available (that EnCase for DOS can take advantage of) are the parallel port (very slow) or the PCMCIA port for an external hard-drive. It seems almost easier to bring a small desktop. The difference in terms of acquisition time will more than make up for the transporting and setup time.

Regardless, remember to bring the EnCase Network Boot Disk and always perform acquisitions in EnCase for DOS, unless using a FastBloc.

Lab Analysis

The lab analysis machine (the Forensic PC) is the work-horse. Important features to keep in mind for the analysis machine are *speed* and *hard drive space*. A Pentium-IV running at 2 GHz or higher with 1 GB of RAM is a good start. One hard drive should be dedicated to the OS and applications (10 GB recommended) and a second FAT32-formatted hard drive dedicated to evidence file storage (80 GB recommended). Both hard drives should be 7200 RPM drives. A good lab analysis machine should also have a “computer forensic friendly” BIOS.

An excellent resource for computers built explicitly for computer forensics is Forensic-Computers.com, at www.forensic-computers.com.

Need Additional Information?

All questions about Storage computer or acquisition computer hardware configurations can be addressed to support@guidancesoftware.com.

INDEX

A

- Absolute Sectors 369
- AC/DSee 389
- Acquire 69
- Acquire Logical Evidence File 27
- Acquiring 63
- Acquiring drives in Windows without FastBloc 100
- Acquiring flash media 122
- Acquiring Macs 89
- Acquiring multiple pieces of removable media 123
- Acquiring Palm PDAs 109
- Acquiring Removable Media 119
- Acquiring UNIX 89
- Acquiring Unix and Linux 89
- Acquiring, DOS 48
- Acquisition File Path 24, 71, 99
- Acquisition Options 23
- Acquisition options 23
- Acquisition Restart 23
- Acquisition, Crossover Cable 73
- Acquisition, Parallel Port 67
- Active Code-Page 245
- Active Processes 287, 289
- Add Device 67
- Add to Case 69, 95, 112
- Adding a new signature 138
- Adding evidence files to a case 164
- Adding Keyword Lists 251
- Adding partitions 277
- Adding Raw Image files 171
- After Acquisition 95, 101, 112, 129
- After acquisition 90
- AIX Journaling File System 22
- Alias 141
- America Online .ART files 212
- Analyze EFS 17
- Analyzing hash results 148
- App Descriptor 289

- Archiving Evidence 323
- Attachments subtab 182
- Attempt Direct Connection 160
- Auto Reconnect 163
- Auto Save Minutes 155

B

- Backup 25
- Backup folder 25
- Bad signature 140
- Barebones Boot Disk 39, 40
- Base64 and UUE encoding 265
- Big-Endian Unicode 245
- BIOS 81, 368
- Block Size 23
- Bookmark Folder Structure 352
- Bookmark options 344
- Bookmarking Search Hits 258
- Bookmarks 19, 180, 329
- Bookmarks subtab 17, 19, 180
- Bookmarks tab 180
- Bookmarks, Copy/UnErase 223
- Bookmarks, Export and Import 26
- Bookmarks, exporting 26
- Boot Procedure 44
- bootfloppy.E01 40
- Booting the restored drive 320

C

- Canceling a search 259
- Case files compatibility 36
- Case Management 153
- Case management 153
- Case Options 154
- Case Time Settings 329
- Cases 178
- Cases tab 16, 178
- CD and DVD file systems 37
- CDFS 375
- CD-R 121
- CD-R Diagnostic 391
- CD-ROM 121
- CD-RW 121

Archiving Evidence 323
Attachments subtab 182
Attempt Direct Connection 160
Auto Reconnect 163
Auto Save Minutes 155

B

Backup 25
Backup folder 25
Bad signature 140
Barebones Boot Disk 39, 40
Base64 and UUE encoding 265
Big-Endian Unicode 245
BIOS 81, 368
Block Size 23
Bookmark Folder Structure 352
Bookmark options 344
Bookmarking Search Hits 258
Bookmarks 19, 180, 329
Bookmarks subtab 17, 19, 180
Bookmarks tab 180
Bookmarks, Copy/UnErase 223
Bookmarks, Export and Import 26
Bookmarks, exporting 26
Boot Procedure 44
bootfloppy.E01 40
Booting the restored drive 320

C

Canceling a search 259
Case files compatibility 36
Case Management 153
Case management 153
Case Options 154
Case Time Settings 329
Cases 178
Cases tab 16, 178
CD and DVD file systems 37
CDFS 375
CD-R 121
CD-R Diagnostic 391
CD-ROM 121
CD-RW 121

Certs 25
Change from a system diskette to a boot floppy 40
Changing font size 302
Character Map 308
Clean boot 76
Cleaning house 325
Client to Node (Local) 161
Client to Node (SAFE) 162
Cluster 20
Cluster Bitmaps 372
Cluster number 218
Clusters 372
Code Page tab 298
Colors Options 157
Compressed files 264
Compression 379
Compute hash values 96, 113
Concurrent case management 153
Conditions tab 27
Configuration Questions 37
Connecting to media 127
Connecting to remote media 125
Console 99, 217, 272
Convert Drive Geometry 318
Copy Folders 224
Copy/UnErase 64, 221
Cracking encrypted or password-protected files 286
CRC 23
CRC (Cyclical Redundancy Checksum) 380
Create Boot Disk 43
Creating a Hash Set 141
Creating a new case 151
Creating a new cCase 127
Creating Conditions 275
Creating Filters 275
Crossover preview / acquisition, LinEn 59
Cylinder 368

D

Date and time FAQs 220
Date Bookmark 333
Date Format 157
DBXtract 389

- Decode Shell Extension 390
- Default Export Folder 152
- Deleting partitions 281
- Details 217
- Devices 181
- Devices subtab 181
- Dir to Html 391
- Disk 1 31
- Disk 2 31
- Disk Compare 390
- Disk Configurations 103
- Dixon Box 218
- Do not add 69, 95, 112
- Do not Write Non-ASCII Characters 222
- Documenting files on media 361
- DOS 39
- DOS Directory Entry Bookmark 333
- Download 36
- Drive geometry 368
- Drive geometry problems 81
- Drives, disks and volumes 370
- DriveSpace volume 285
- Drive-to-Drive acquisition, LinEn 58
- Dynamic Disk 105
- E**
- Editing EnScripts 271
- Editing Filters 274
- E-Mail 229
- E-Mail and Internet artifacts 229
- Email subtab 18, 182
- EN.EXE 44, 75, 76
- Enable ART and PNG image display 156
- Enable Picture Viewer 156
- ENBCD 22
- EnCase Acquisition 38
- EnCase Boot CD (ENBCD) 42
- EnCase Boot Disk 39, 42
- EnCase Boot Disk (ENBD) 47
- EnCase Boot Disk FAQs 46
- EnCase Boot Disk, booting 44
- EnCase Enterprise 12
- EnCase for DOS 47
- EnCase Forensic 11
- EnCase icon descriptions 202
- EnCase Installation CD 31
- EnCase Network Boot CD (ENBCD) 45
- EnCase Network Boot Disk 45
- EnCase Network Boot Disk (ENBD) 39, 45, 73
- EnCase program icon 34
- EnCase Views 178
- enlinuxpc 37
- EnScript and Filters 269
- EnScript Options 159
- EnScript path 270
- EnScript Types 190
- EnScript Types tab 190
- EnScript View 215
- EnScripts 28, 149, 269
- EnScripts tab 189
- enstart.exe 34, 35, 36, 37
- Entering Keywords 244
- Enterprise Options 160
- Entire Physical File 222
- Entries subtab 17
- Error messages 169
- Evidence file format 381
- Evidence file name 218
- Evidence storage 379
- Examining flash media 122
- Export folder 25
- Exporting Keywords 248
- Exporting the Report 358
- Exporting/importing Bookmarks 348
- Exporting/importing Keywords 248
- EXT2/3 37, 375
- Extended DOS partition 371
- F**
- FastBloc 64, 91
- FastBloc Acquisitions 91
- FastBloc Field Edition (FE) 91
- FastBloc indicators 93
- FastBloc Lab Edition (LE) 91
- FAT and NTFS Info Record Finder 149
- FAT file systems 51

- FAT12 37
- FAT16 37
- FAT32 37
- FDISK 319
- FFS (BSD) 37
- Field acquisitions 393
- File Allocation Table (FAT) 374
- File entries 373
- File Extents subtab 17, 19
- File Finder 149
- File Group Bookmark 330, 340
- File Hashing 141
- File Mounter EnScript module 261
- File offset 218
- File Segment Size 100
- File Signature 381
- File Signatures 136, 184
- File Signatures tab 184
- File slack 373
- File system concepts 372
- File systems 37, 374
- file systems 22
- File Types 183, 226
- File Types tab 183
- File Viewers 184, 225
- File Viewers tab 184
- File Viewing FAQs 226
- Filter Conditions 27
- Filters 273
- Find 219
- Finding web artifacts 235
- Firewall 78
- FireWire / USB acquisitions 56
- First steps 125
- Flag Lost Files 26, 157
- Flash Card reader/writers 122
- Flash media 122
- Floppy Disks 120
- Folder Information Bookmark 330, 337
- Font recommendations 302
- Fonts Options 158
- Fonts tab 296
- Foreign language Bookmarking 311
- Foreign language Keyword searches 307
- Foreign language support 295
- Forensic Terminology 367
- G**
- Gallery View 202, 210
- Global Options 155
- Globally Unique Identifiers (GUIDs) 24
- Go To Parent 22
- Gpart 390
- Granularity 23, 56, 88
- GREP 245, 383
- GREP examples 384
- GUEST.EXE 120
- H**
- Hard drive anatomy 368
- Hard drive layout 370
- Hardware Disk Configuration 106
- Hash 141
- hash 48
- Hash Library 147
- Hash Sets 141
- Hash sets 141
- Hash Sets tab 190
- Hashing, DOS 48, 49
- Hashing, LinEn 56
- HashKeeper Hash Sets 143
- Head 368
- Help folder 26
- Help resources 10
- Hex 216
- HFS 37, 375
- HFS+ 37, 375
- Hiding and showing columns 201
- Highlighted Data Bookmark 330
- History 229, 235
- History subtab 18, 183
- Home Plate 178
- Home subtab 17, 178, 182
- Hyper Text Markup Language (HTML) 358

I

IE History time interpretation 236
ifconfig 56
Image verification 382
Importing Keywords 250
Include folder 270
INFO2 285
Initialize Case 149
installation files and folders 25
Installing EnCase 32
Installing the Servlet 34
Integers Bookmark 333
Interface 176
International Keywords 246
Inter-partition space 371
Invalid picture timeout 156
IrfanView 389

J

JFS 37
JFS1 22
JFS2 22
JFS2 (AIX 37

K

Keyword groups 243
Keyword searches 243
Keyword Tester 27, 247
Keywords 243
Keywords tab 185
keywords.ini 21
Known 141

L

Lab analysis 394
lap-link (null-modem) cable 67
Length 218
License Agreement 1, 33
LinEn 21, 55, 73, 75, 77
LinEn setup 57
LinEn, troubleshooting 77
Link File Parser 150
Live Device indicators 93
Live Windows Registry 287

Local Keywords 21

Lock 217

Lock Box 217

Locking / Unlocking 47

Log Record Bookmark 330

Logging Into a SAFE Server 126

Logical Evidence File 27

Logical Evidence Files 176

Logical File Only 222

Logical file size 373

Logical restore 320

Logical sector number 218

logon 125

Lost Files 136

Lost Files in UFS and EXT2/3 136

LVM8 22

M

Mailbag Assistant 390

Master Boot Record (MBR) 370

Master File Table 136

Match 141

Maximum File Segment Size 24

MBXtract 390

MD5 Hash 379

Message Boards 11

MFT 136

Mirrored 103

Mode, DOS 52

Move or Copy Bookmarks 348

MS Outlook E-Mail 266

N

Navigating EnCase 151

Navigation data 218

net stop 35

netstat 36

Network Interfaces and Users 292

Network Support 76

Node to Client 162

Non-FastBloc write-blockers 101

Notable 141

Notable File Bookmark 330, 338

Notes Bookmark 330, 335

NSRL Hash Sets 145

NTFS 37, 374

NTFS compressed files 267

O

OLE files 262

Open Files 287, 292

Open Ports 287, 288

Open Ports table columns 288

Options Dialog 154

Organizing columns 200

OST2PST 390

Outlook Express E-mail 264

Overwrite diskette with a boot floppy base image 40

P

Palm 37

PalmOS 375

Palms supported 109

pane locations 16

Panes 219

parallel port 67

Partition Entry Bookmark 333

Partition table 371

PC hardware 367

PCI cards supported 74

PCMCIA cards supported 74

PDA in Console mode 109

PDF manual 28

Permissions subtab 17, 19

Physical file size 373

Physical restore 316

Physical sector number 218

Physical vs. Logical restore 315

Picture 216

Platter 369

Presenting multiple images 356

Presenting Search Results 362

Presenting the findings 351

Preview, laptop computers 65

Preview, Linux and Unix 64

Previewing 63

Previewing advantages 64

Previewing Imitations 63

Private Key Caching 163

Processes table columns 290

Professional Services Division 13

PST Cracker 390

Q

Queries 275

Queries tab 27

Quick Reacquisition 23, 124

Quick View Plus 389

Quit, DOS 53

R

RAID 103

RAID 0

 Striping 376

RAID 1

 Mirroring 376

RAID 5 377

RAID, Software 104

RAID-10 103, 108

RAID-5 103, 108

RAID-5, validating parity 108

RAM 367

RAM and Disk Slack 222

RAM slack 374

RAM Slack Only 222

Raw Image 171

Read Ahead 23

ReadMe 33

Rearranging columns 200

Rebuilding the Hash Library 147

Recompute hash values 96, 113

Reconstructed HTML 332

Recover Folders 133

Recover Folders on FAT volumes 133

Recover NTFS Folders 134

Recovered information 284

Recovering Folders from a formatted drive 282

Recovering partitions 277

Recycle Bin 284

- Red Hat 57
- Refresh 258
- Regional settings 310
- Registry Bookmark 330
- Registry Files 261
- Registry files 261
- Reiser 37, 375
- Remote acquisition 129
- Reordering Bookmarks for Reports 354
- Replace Non-ASCII Characters with DOT 222
- Replace source device 69, 95, 112
- Replace source drive 95
- Report 217, 351
- Report View 214
- Requirements 9
- Restart Acquisition 23, 70, 71, 99
- Restoration FAQs 322
- Restoring evidence 315
- Rich Edit Control in Bookmarks 313
- Rich Text Format (RTF) 358
- Right-to-Left (RTL) languages 306
- ROM 367
- Root Folder 372
- ROT 13 Encoding 332
- RTL Reading 245
- Running EnScripts 271
- S**
- SAFE Administration 125
- SafeBack 87, 173
- SafeBack, DOS 87
- Scan for LVM 22
- Script Security 158, 159
- SCSI 108
- SCSI controller cards 74
- Search each file for keywords 96, 113
- Search file slack 97, 114
- Search Hits subtab 181
- Search only slack area of the files in the Hash Library 97, 114
- Search Options 252
- Search Summary 330
- Search, Hash and Signature Analysis 70
- Search, Hash, and Signature Analysis 96, 113
- Sector 368
- Sector offset 218
- Secure Storage subtab 17, 181
- Security IDs tab 185
- Security key
 - Drivers 31
- Security Key Drivers 32
- Security key IDs 10
- Selected keywords only 97, 114
- Server mode 50
- Server mode, DOS 50, 51
- Sessions Option 167
- SETUP.EXE 31
- setup.exe 35, 37
- Show Errors 223
- Show True Show False 155
- Signature Analysis 136
- Single Files 27, 175
- Snapshot 287, 343
- Snapshot Bookmark 330
- Sorting 201
- Sources subtab 20
- Sources table column 20
- Spanned 103
- Split files above (MB) 223
- Starting a search 251
- Starting a Signature Analysis 139
- Starting and stopping Filters 274
- Storage computer/media 367
- Storage folder 26
- Storage Paths Options 159
- Styles Bookmark 334
- Subject computer/media 367
- Subjects subtab 21
- Subtab, Attachments 233
- Superdisks 121
- SuSE 9.1 57
- Symbolic Link table column 22
- System Snapshot 286
- T**
- Table Columns, Email 233

Table columns, History 237
Table columns, WebCache 240
Table Pane 191
Table View 191
Table View columns 192
Technical Support 10
Temp folder 26
Temporary Folder 152
Text 216, 331
Text Styles tab 188
The Forensic Lab 393
Third-party utilities 389
Thumbs.db 268
Time Format 157
Time Zone settings 130
Timeline View 213
TiVo 22
TiVo Series 1 and 2 37
to Drive 81
Track 369
Training 12

U

UFS 376
UFS (Unix) 37
Undelete files before searching 97, 114
Unicode 245, 295
Unicode characters 300
Unicode fonts 299
Unique EMail Address List 150
Unknown 141
Update existing boot floppy 40
Updates 36
USB Acquisition 76
USB Destination 76
user interface 15
Users Forum 11
UTF-7 246
UTF-8 246

V

verify 170
Verify evidence files 65

Verify files signatures 96, 113
Verifying 170
Verifying evidence 170
Verifying evidence files 324
View File Structure 261
View Pane 215
Viewing Compound Files 261
Viewing Files 221
Viewing non-Unicode files 303
Viewing Search Hits 253
Viewing Unicode files 297
VMware 173
Volatile data components 287
Volatile data defined 286
Volume Boot Sector 371
Volume slack 374

W

Waiting to connect 77
Web browsing history 282
Web Cache 229, 238
WebCache subtab 18, 183
Win2000 Info File Record Bookmark 334
Win95 Info File Record Bookmark 334
Windows acquisition issues 39
Windows XP SP2 78
WinHelp 28
Wipe Drive 325
Write blocking 39
Write-protecting floppy disks 121

Z

Zip and Jaz disks 119
Zip Disks 119