Computer Forensics
Computer Forensics

• Preservation, identification, extraction, documentation, and interpretation of computer media for evidence and/or root cause analysis

• Computer media include:
  – Computers, PDAs, Cellular Phones…

• Internet Forensics
  – http://berghel.net/home.php
Examples of Digital Forensics

• Computers increasingly involved in criminal and corporate investigations

• Email
  – Harassment or Threat
  – Blackmail
  – Illegal transmission of internal corporate documents

• Evidence of inappropriate use of computer resources or attacks
  – Use of a machine as a spam email generator
  – Use of a machine to distribute illegally copied software
Who needs it?

- Law enforcement
  - Prosecution of crimes which involve computers or other digital devices
  - Defend the innocent
  - Prosecute the guilty
  - Must follow the strict guidelines during entire forensics process to ensure evidence will be admissible in court
- Military
  - Prosecution of internal, computer-related crimes
- Security Agencies
  - Anti-terrorism efforts
  - Some provisions, e.g., Patriot Act, relax traditional privacy guards
Who needs it?

• General
  – Employee misconduct in corporate cases
  – What happened to this computer?
  – For accidental deletion or malicious deletion of data by a user, what can be recovered?

• Privacy advocates
  – What can be done to ensure privacy?
  – Premise: Individuals have a right to privacy. How can individuals ensure that their digital data is private?
  – Very difficult, unless strong encryption is needed, then storage of keys becomes the difficult issue.
Challenges

• Evidence collection done in adversarial environment
• Judge and Jury are not technical
• Commercial testing tools may not work
Basic Methodology

• Acquire the evidence without altering or damaging the original
  – Where might the evidence be? What devices did the suspect use?
  – Stabilize the evidence, prevent loss and contamination
  – If possible, make identical copies of evidence for examination
  – Preservation: Imaging
    • When making copies of media to be investigated, must prevent accidental modification or destruction of evidence
    • dd under unix
    • Dos boot floppies
  – Deleted files recoverable using forensics tools
    • “Deleted” files, on almost any kind of digital storage media, are almost never completely “gone”
Where is the evidence?

- Undeleted files
- Deleted files
- Windows registry
- Print spool files
- Hibernation files
- Temp files (all those .TMP files!)
- Slack space
- Swap files
- Browser caches
- A variety of removable media (floppies, ZIP, tapes…)

Sources of Information
“Deletion” / “Obfuscation” Fallacies

- I delete the file, it’s gone
  - Deleted files are recoverable using digital forensics tools
- I changed the name of the file, now no one can find it
  - Digital forensics tools immediately identify files based on content – names do not matter at all
- I formatted the drive
  - This destroys almost nothing
- I use only web-based email
  - Some email fragments are still present locally.
- I cut the floppy into little pieces
  - At this point, it is a question of how important it is to recover the data, because it is harder to recover the data
Basic Methodology – Con’t

• Authenticate the Evidence
  – Cryptographic hashing provides a mechanism for “fingerprinting” files
  – File contents are matched quickly, regardless of name
  – Hashes equivalent, file contents equivalent
  – Typical Algorithm: MD5, SHA-1
    • md5sum
Basic Methodology – Con’t

• Analysis – Most technical
  – Using copies of original digital evidence, recover as much evidence as possible
  – Discover of deleted files
  – Discovery of renamed files
  – Discover of encrypted materials
  – Check of unallocated and slack space
  – Application of password cracking techniques to open encrypted materials.