Non-Malicious Traffic
## IPV4 Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version number</td>
</tr>
<tr>
<td>IHL</td>
<td>Internet Header Length</td>
</tr>
<tr>
<td>Type of service</td>
<td>Type of service</td>
</tr>
<tr>
<td>Total length</td>
<td>Total length of the packet</td>
</tr>
<tr>
<td>Identification</td>
<td>Identification of fragments</td>
</tr>
<tr>
<td>DF</td>
<td>Don't Fragment flag</td>
</tr>
<tr>
<td>MF</td>
<td>More Fragments flag</td>
</tr>
<tr>
<td>Fragment offset</td>
<td>Offset of fragment in packet</td>
</tr>
<tr>
<td>Time to live</td>
<td>Time to live for the packet</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol number</td>
</tr>
<tr>
<td>Header checksum</td>
<td>Header checksum</td>
</tr>
<tr>
<td>Source address</td>
<td>Source IP address</td>
</tr>
<tr>
<td>Destination address</td>
<td>Destination IP address</td>
</tr>
<tr>
<td>Options</td>
<td>Options (0 or more words)</td>
</tr>
</tbody>
</table>

- From Tanenbaum’s book
IP version field

Figure 5.2  IP version field.
IP header length

```
10:17:19.651646 207.172.110.197.1221 > 207.126.127.69.www:
  S 2149480675:2149480675 (0) win 16324 <mss
  1484, sackOK, timestamp 1343065 0, nop, wscale 0> (DF) (ttl 64,
  id 2662)
     4500 003c 0a66 4000 4006 a320 cfac 6ec5
     cf7e 7f45

Figure 5.3  IP Header Length fields.
```
IP Type of Service Fields

- 10 hex: minimize delay
- 08 hex: maximize throughput
- 04 hex: maximize reliability
- 02 hex: minimize monetary cost

Figure 5.4  IP Type of Service fields.
IP Total Length

10:17:19.651646 207.172.110.197.1221 > 207.126.127.69.www:
S 2149480675:2149480675 (0) win 16324 <mss
4500, sackOK, timestamp 1343065 0, nop, wscale 0> (DF) (ttl 64,
id 2662)

Figure 5.5 IP Total Length fields.
10:17:19.651646 207.172.110.197.1221 > 207.126.127.69.wwww:
  ⇨S 2149480675:2149480675 (0) win 16324 <mss
  ⇨1484,sackOK,timstamp 1343065 0,nop,wscale 0> (DF) (ttl 64,
  ⇨id 2662)

   4500 003c 0a66 4000 4006 a320 cfac 6ec5
   cf7e 7f45

*Figure 5.6* IP ID field.
## Fragments

<table>
<thead>
<tr>
<th>MF bit</th>
<th>Fragment Offset</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not set</td>
<td>Zero</td>
<td>Packet not fragmented</td>
</tr>
<tr>
<td>Set</td>
<td>Zero</td>
<td>First fragment</td>
</tr>
<tr>
<td>Set</td>
<td>Non-zero</td>
<td>Middle fragment</td>
</tr>
<tr>
<td>Not set</td>
<td>Non-zero</td>
<td>Last fragment</td>
</tr>
</tbody>
</table>
Fragments

10:17:19.651646 207.172.110.197.1221 > 207.126.127.69.www:
→S 2149480675:2149480675 (0) win 16324 <mss
→1484,sackOK,timestamp 1343065 0,nop,wscale 0> (DF) (ttl 64,
→id 2662)

Figure 5.8 IP Fragment Flags and Offset fields.
IP TTL and Protocol Fields

- 01 hex: ICMP
- 02 hex: IGMP
- 03 hex: GGP
- 04 hex: IP
- 06 hex: TCP
- 11 hex: UDP
IP Header Checksum

IP Header Checksum = 16-bit 1s complement of the 1s complement sum of all 16-bits words in the header
One Example

Checksum = 1s complement sum of the 1s complement of 4-bit quantities.

1s complement of 1111, 0000, 1100, 0101, 1000
is 0000, 1111, 0011, 1010, 0111.

1s complement sum: 0000 + 1111 = 1111.

\[1111 + 0011 = 0010 + 1 \text{ (carry)} = 0011\]
\[0011 + 1010 = 1101\]
\[1101 + 0111 = 0100 + 1 \text{ (carry)} = 0101\]

Ans: Checksum = 0101
IP Source Address and Destination Address

Figure 5.11  IP Source Address and Destination Address fields.
TCP Header

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Acknowledgment Number</td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td>URG</td>
</tr>
<tr>
<td>Data Offset</td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td></td>
</tr>
<tr>
<td>Padding</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>
TCP Source Port and Destination Port

Figure 5.13 TCP Source Port and Destination Port fields.
TCP Sequence Number

The offset into the data stream: \((SN – ISN - 1)\)
TCP Acknowledgement

The receiver has correctly received (AN-ISN-1) bytes data from the sender
TCP Data Offset and Control Bits

TCP Data Offset: the length of the TCP header in 32-bit words
A Partial list of normal control bit combinations

- SYN
- SYN-ACK
- ACK (within an established connection)
- RST
- RST-ACK
- FIN
- FIN-ACK
- FIN-PSH-ACK
- URG-ACK
- PSH-ACK
TCP Window Size

Figure 5.17  TCP Window Size field.
TCP Checksum and Urgent Pointer

Figure 5.18  TCP Checksum and Urgent Pointer fields.

TCP Three-Way Handshake

Figure 5.23  The first step of the three-way handshake.
TCP Three-Way Handshake

Figure 5.24 The second step of the three-way handshake.

Figure 5.25 The third step of the three-way handshake.