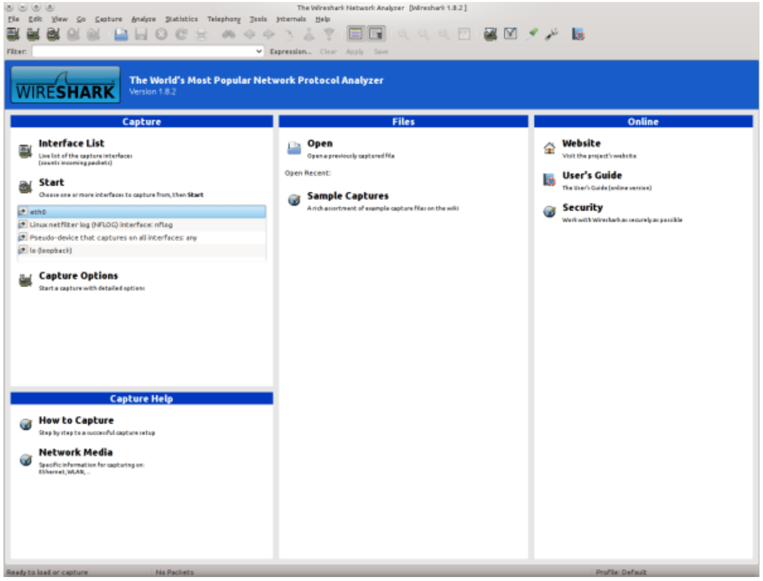
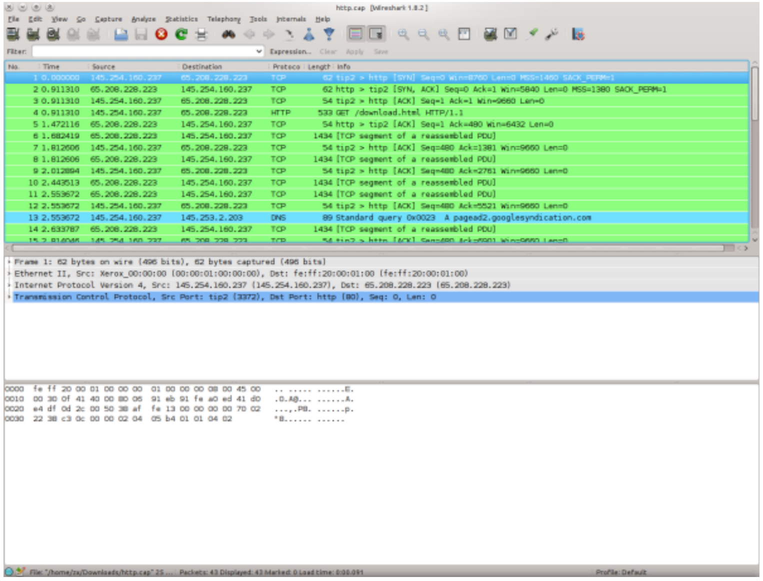
CENG334
COMPUTER NETWORKS
LABORATORY MANUAL VI

In this weeks laboratory manual, we will use Wireshark to study IPv4 headers. Wireshark is a powerful network analysis software. It can capture incoming/outgoing network packages to/from your computer and display the structure of these packets. It can also save captured packets to a file and load captured packets from it later.


The Wireshark Network Analyzer [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.8.2
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
eth0
Linux netfilter log (NFLOG) interface: nflog
Pseudo-device that captures on all interfaces: any
lo (loopback)
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default

Wireshark main window. Download sample capture file from course web page and load it via File -> Open.


http.cap [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

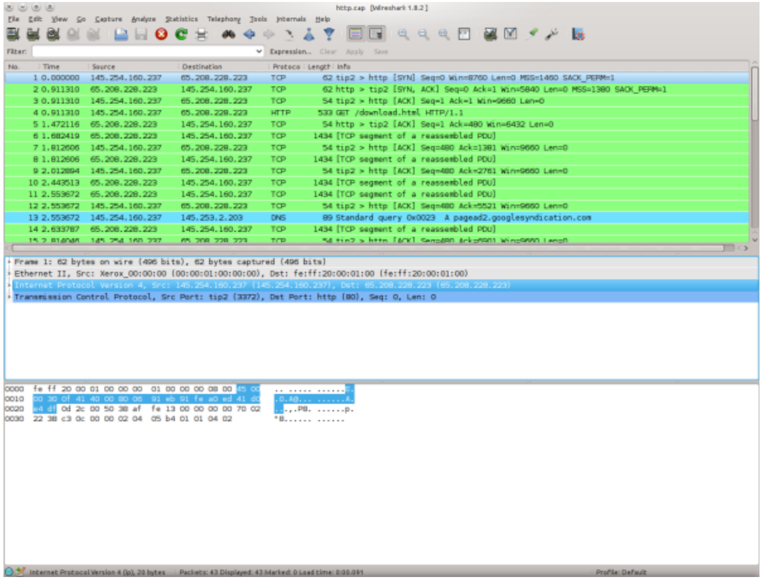
```
No.  Time      Source           Destination      Protoco Lengtl Info
  1 0.000000  145.254.160.237  65.208.228.223   TCP       62 tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
  2 0.911310  65.208.228.223   145.254.160.237  TCP       62 http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
  3 0.911310  145.254.160.237  65.208.228.223   TCP       54 tip2 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0
  4 0.911310  145.254.160.237  65.208.228.223   HTTP     533 GET /download.html HTTP/1.1
  5 1.472116  65.208.228.223   145.254.160.237  TCP       54 http > tip2 [ACK] Seq=1 Ack=480 Win=6432 Len=0
  6 1.682419  65.208.228.223   145.254.160.237  TCP     1434 [TCP segment of a reassembled PDU]
  7 1.812606  145.254.160.237  65.208.228.223   TCP       54 tip2 > http [ACK] Seq=480 Ack=1381 Win=9660 Len=0
  8 1.812606  65.208.228.223   145.254.160.237  TCP     1434 [TCP segment of a reassembled PDU]
  9 2.012894  145.254.160.237  65.208.228.223   TCP       54 tip2 > http [ACK] Seq=480 Ack=2761 Win=9660 Len=0
 10 2.443513  65.208.228.223   145.254.160.237  TCP     1434 [TCP segment of a reassembled PDU]
 11 2.553672  65.208.228.223   145.254.160.237  TCP     1434 [TCP segment of a reassembled PDU]
 12 2.553672  145.254.160.237  65.208.228.223   TCP       54 tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
 13 2.553672  145.254.160.237  145.253.2.203    DNS       89 Standard query 0x0023  A pagead2.googlesyndication.com
 14 2.633787  65.208.228.223   145.254.160.237  TCP     1434 [TCP segment of a reassembled PDU]
 15 2.814046  145.254.160.237  65.208.228.223   TCP       54 tip2 > http [ACK] Seq=480 Ack=6901 Win=9660 Len=0
```

```
▸ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▸ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
▸ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
▸ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   .. ..... ......E.
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   .0.A@... ......A.
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ...,.P8. ......p.
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8...... ......
```

File: "/home/za/Downloads/http.cap" 25 ... Packets: 43 Displayed: 43 Marked: 0 Load time: 0:00.091
Profile: Default

You can browse captured packages from the upper list.



http.cap [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

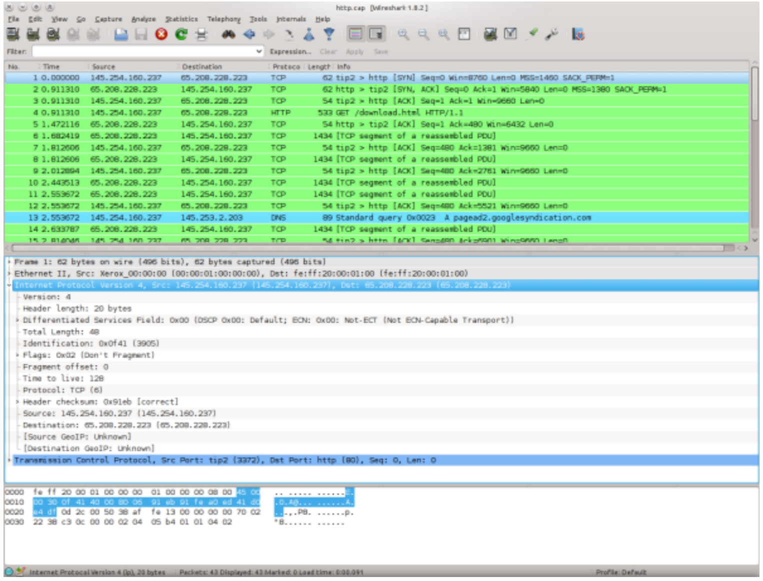
```
No.  Time        Source            Destination       Protoco Length Info
   1 0.000000    145.254.160.237   65.208.228.223    TCP       62 tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
   2 0.911310    65.208.228.223    145.254.160.237   TCP       62 http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
   3 0.911310    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0
   4 0.911310    145.254.160.237   65.208.228.223    HTTP     533 GET /download.html HTTP/1.1
   5 1.472116    65.208.228.223    145.254.160.237   TCP       54 http > tip2 [ACK] Seq=1 Ack=480 Win=6432 Len=0
   6 1.682419    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
   7 1.812606    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=1381 Win=9660 Len=0
   8 1.812606    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
   9 2.012894    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=2761 Win=9660 Len=0
  10 2.443513    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  11 2.553672    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  12 2.553672    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
  13 2.553672    145.254.160.237   145.253.2.203     DNS       89 Standard query 0x0023  A pagead2.googlesyndication.com
  14 2.633787    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  15 2.814046    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=6901 Win=9660 Len=0
```

```
▸ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▸ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
▸ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
▸ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   .. ..... ......E.
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   .0.A@... ......A.
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ...,.P8. ......p.
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8...... ......
```

Internet Protocol Version 4 (ip), 20 bytes
Packets: 43 Displayed: 43 Marked: 0 Load time: 0:00.091
Profile: Default

To select IPv4 headers of captured packages, select "Internet Protocol Version 4" part from the middle list. You can see the header at the lower part.



http.cap [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

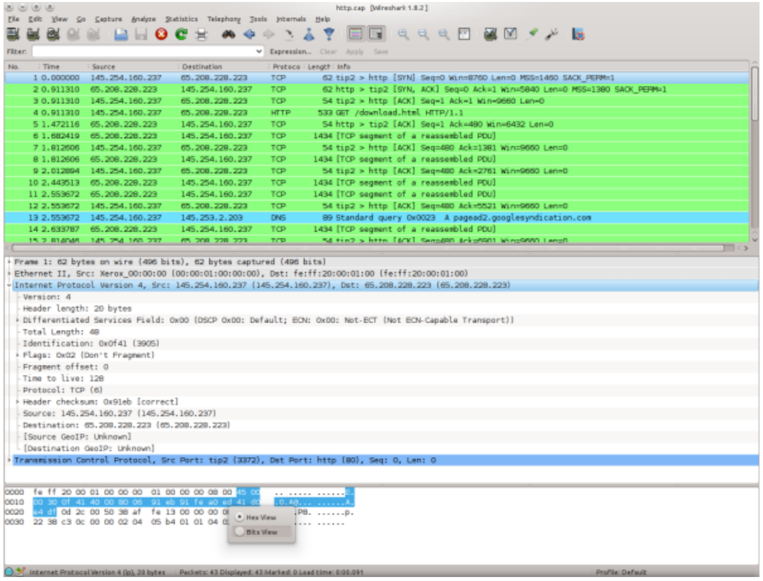
```
No.  Time        Source            Destination       Protoco Length Info
   1 0.000000    145.254.160.237   65.208.228.223    TCP       62 tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
   2 0.911310    65.208.228.223    145.254.160.237   TCP       62 http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
   3 0.911310    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0
   4 0.911310    145.254.160.237   65.208.228.223    HTTP     533 GET /download.html HTTP/1.1
   5 1.472116    65.208.228.223    145.254.160.237   TCP       54 http > tip2 [ACK] Seq=1 Ack=480 Win=6432 Len=0
   6 1.682419    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
   7 1.812606    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=1381 Win=9660 Len=0
   8 1.812606    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
   9 2.012894    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=2761 Win=9660 Len=0
  10 2.443513    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  11 2.553672    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  12 2.553672    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
  13 2.553672    145.254.160.237   145.253.2.203     DNS       89 Standard query 0x0023  A pagead2.googlesyndication.com
  14 2.633787    65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  15 2.814046    145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=6901 Win=9660 Len=0
```

```
▸ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▸ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
▾ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
    Version: 4
    Header length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 48
    Identification: 0x0f41 (3905)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ▸ Header checksum: 0x91eb [correct]
    Source: 145.254.160.237 (145.254.160.237)
    Destination: 65.208.228.223 (65.208.228.223)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▸ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   .. ..... ......E.
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   .0.A@... ......A.
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00 70 02   ...,.P8. ......p.
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02         "8...... ......
```

Internet Protocol Version 4 (ip), 20 bytes
Packets: 43 Displayed: 43 Marked: 0 Load time: 0:00.091
Profile: Default

Selecting different parts of the packet will highlight the associated bits in the lower section. Here we have selected and extended the header to show detailed information about the fields.



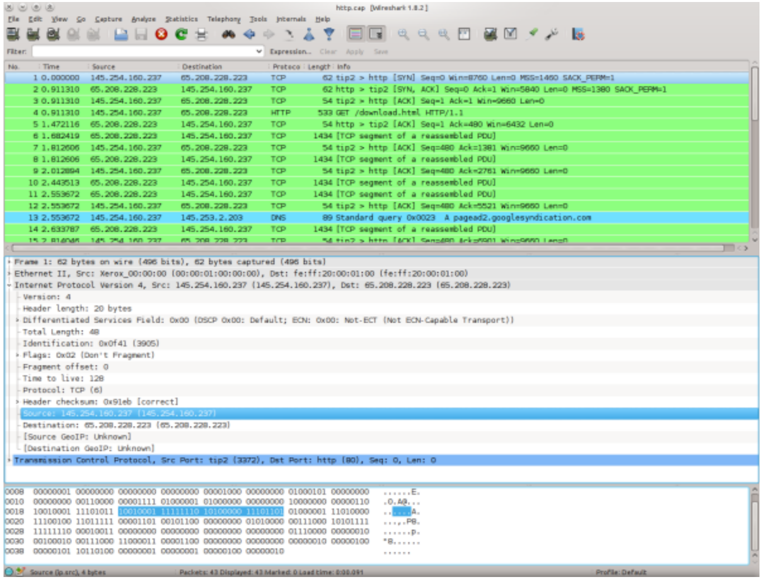
```
No.  Time       Source            Destination       Protoco Length Info
  1 0.000000   145.254.160.237   65.208.228.223    TCP       62 tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
  2 0.911310   65.208.228.223    145.254.160.237   TCP       62 http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
  3 0.911310   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0
  4 0.911310   145.254.160.237   65.208.228.223    HTTP     533 GET /download.html HTTP/1.1
  5 1.472116   65.208.228.223    145.254.160.237   TCP       54 http > tip2 [ACK] Seq=1 Ack=480 Win=6432 Len=0
  6 1.682419   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  7 1.812606   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=1381 Win=9660 Len=0
  8 1.812606   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  9 2.012894   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=2761 Win=9660 Len=0
 10 2.443513   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
 11 2.553672   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
 12 2.553672   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
 13 2.553672   145.254.160.237   145.253.2.203     DNS       89 Standard query 0x0023  A pagead2.googlesyndication.com
 14 2.633787   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
 15 2.814046   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=6901 Win=9660 Len=0
```

```
▸ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▸ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
▾ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
    Version: 4
    Header length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 48
    Identification: 0x0f41 (3905)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ▸ Header checksum: 0x91eb [correct]
    Source: 145.254.160.237 (145.254.160.237)
    Destination: 65.208.228.223 (65.208.228.223)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▸ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00   .. ...... ......E.
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed 41 d0   .0.A@... ......A.
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 0          .PB. ......p.
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 0          .... ......
```

● Hex View
○ Bits View
Internet Protocol Version 4 (ip), 20 bytes
Packets: 43 Displayed: 43 Marked: 0 Load time: 0:00.091
Profile: Default

You can switch between hexadecimal and binary views by right clicking on the lower part...



http.cap [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save

```
No.  Time       Source            Destination       Protoco Length Info
  1 0.000000   145.254.160.237   65.208.228.223    TCP       62 tip2 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
  2 0.911310   65.208.228.223    145.254.160.237   TCP       62 http > tip2 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
  3 0.911310   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0
  4 0.911310   145.254.160.237   65.208.228.223    HTTP     533 GET /download.html HTTP/1.1
  5 1.472116   65.208.228.223    145.254.160.237   TCP       54 http > tip2 [ACK] Seq=1 Ack=480 Win=6432 Len=0
  6 1.682419   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  7 1.812606   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=1381 Win=9660 Len=0
  8 1.812606   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
  9 2.012894   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=2761 Win=9660 Len=0
 10 2.443513   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
 11 2.553672   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
 12 2.553672   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0
 13 2.553672   145.254.160.237   145.253.2.203     DNS       89 Standard query 0x0023  A pagead2.googlesyndication.com
 14 2.633787   65.208.228.223    145.254.160.237   TCP     1434 [TCP segment of a reassembled PDU]
 15 2.814046   145.254.160.237   65.208.228.223    TCP       54 tip2 > http [ACK] Seq=480 Ack=6901 Win=9660 Len=0
```

```
▸ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▸ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
▾ Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
    Version: 4
    Header length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 48
    Identification: 0x0f41 (3905)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ▸ Header checksum: 0x91eb [correct]
    Source: 145.254.160.237 (145.254.160.237)
    Destination: 65.208.228.223 (65.208.228.223)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▸ Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 0, Len: 0
```

```
0008  00000001 00000000 00000000 00000000 00001000 00000000 01000101 00000000   ......E.
0010  00000000 00110000 00001111 01000001 01000000 00000000 10000000 00000110   .0.A@...
0018  10010001 11101011 10010001 11111110 10100000 11101101 01000001 11010000   ......A.
0020  11100100 11011111 00001101 00101100 00000000 01010000 00111000 10101111   ...,.P8.
0028  11111110 00010011 00000000 00000000 00000000 00000000 01110000 00000010   ......p.
0030  00100010 00111000 11000011 00001100 00000000 00000000 00000010 00000100   "8......
0038  00000101 10110100 00000001 00000001 00000100 00000010                     ......
```

... and see how the fields are represented in binary or hexadecimal.

Study the rest of the packets in the sample file and observe how each field is organized in each packet.

Calculating Checksum

You should follow three steps to calculate the checksum of an IPv4 header. As an example, the first packet in the sample capture file will be used. This header can be displayed as `45 00 00 30 0f 41 40 00 80 06 00 00 91 fe a0 ed 41 d0 e4 df` in hexadecimal form. Note that the checksum field is currently empty.

1. Calculate the sum of every 2 bytes.
   ```
   = 4500 + 0030 + 0f41 + 4000 + 8006 + 0000 + 91fe + a0ed + 41d0
     + e4df
   = 00036e11
   ```

2. The first 2 bytes are the carry, add them to the rest.
   ```
   = 0003 + 6e11
   = 6e14
   ```

3. Obtain 1's complement of this value.
   ```
   = ~6e14
   = 91eb
   ```

4. Write the result obtained in Step 3 to checksum field of header.
   ```
   45 00 00 30 0f 41 40 00 80 06 91 eb 91 fe a0 ed 41 d0 e4 df
   ```

Verifying Checksum

Verifying a checksum is almost similar to calculation, but now you must also add checksum to the sum operation in Step 1.

```
= 4500 + 0030 + 0f41 + 4000 + 8006 + 91eb + 91fe + a0ed + 41d0 + e4df
= 0003 fffc
```

```
= 0003 + fffc
= ffff
```

```
= ~ffff
= 0000
```

If you obtain 0000 in the final step, then that means the contents of the header has been correctly received. If not, it means there had been error(s) while receiving the package and it should either be repaired or received again.

Exercise

The C program below displays an IPv4 header which is defined in an array. Run it, then modify it to calculate the checksum of the header.

A reminder;

- char = 1 byte
- short int = 2 bytes
- int = 4 bytes
- long int = 8 bytes

```
#include <stdio.h>

int main()
{
        int i;
        unsigned short int byte_grp;
        unsigned char header[20] = { 0x45, 0x00, 0x00, 0x30, 0x0f, 0x41, 0x40, 0x00, 0x80, 0x06, 0x00,
0x00, 0x91, 0xfe, 0xa0, 0xed, 0x41, 0xd0, 0xe4, 0xdf };

        for (i = 0; i < 10; i++)
        {
                byte_grp = (header[2 * i] << 8) + header[2 * i + 1];
                printf("%04x ", byte_grp);
        }

        return 0;
}
```