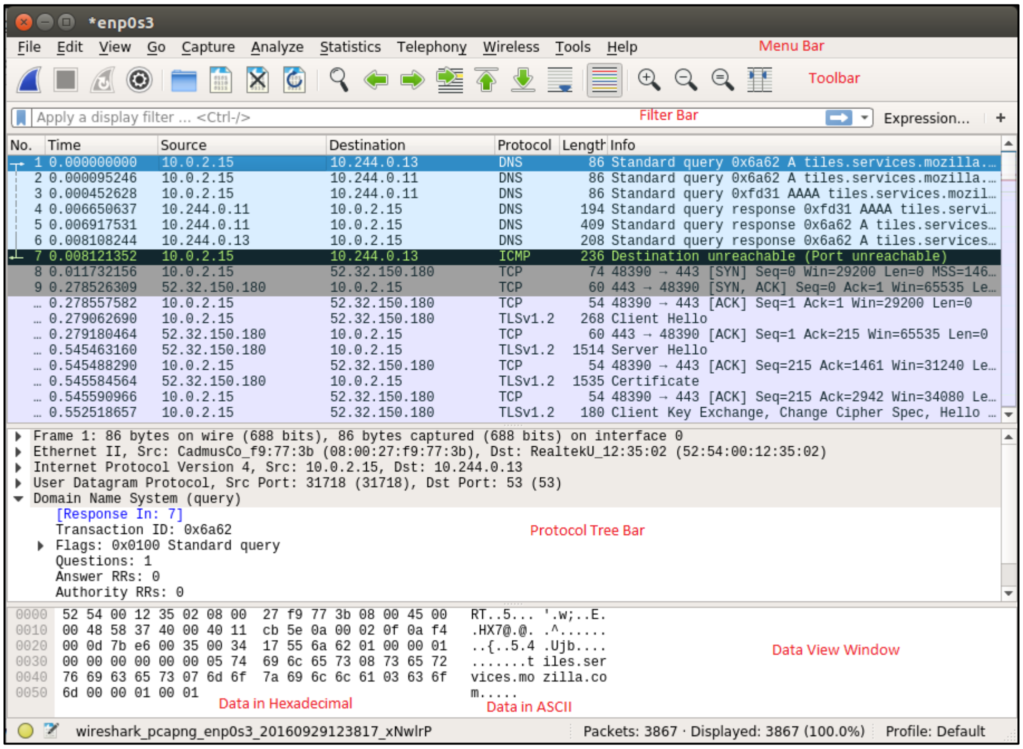
Contents

Using Wireshark

Start the Wireshark by executing `sudo wireshark` command in terminal in Linux or by clicking on start | programs| wireshark | wireshark in Windows. You will be able to see the GUI of the Wireshark as shown below:



```
No. Time        Source         Destination    Protocol Length Info
  1 0.000000000 10.0.2.15      10.244.0.13    DNS        86 Standard query 0x6a62 A tiles.services.mozilla…
  2 0.000095246 10.0.2.15      10.244.0.11    DNS        86 Standard query 0x6a62 A tiles.services.mozilla…
  3 0.000452628 10.0.2.15      10.244.0.11    DNS        86 Standard query 0xfd31 AAAA tiles.services.mozil…
  4 0.006650637 10.244.0.11    10.0.2.15      DNS       194 Standard query response 0xfd31 AAAA tiles.servi…
  5 0.006917531 10.244.0.11    10.0.2.15      DNS       409 Standard query response 0x6a62 A tiles.services…
  6 0.008108244 10.244.0.13    10.0.2.15      DNS       208 Standard query response 0x6a62 A tiles.services…
  7 0.008121352 10.0.2.15      10.244.0.13    ICMP      236 Destination unreachable (Port unreachable)
  8 0.011732156 10.0.2.15      52.32.150.180  TCP        74 48390 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=146…
  9 0.278526309 52.32.150.180  10.0.2.15      TCP        60 443 → 48390 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le…
  … 0.278557582 10.0.2.15      52.32.150.180  TCP        54 48390 → 443 [ACK] Seq=1 Ack=1 Win=29200 Len=0
  … 0.279062690 10.0.2.15      52.32.150.180  TLSv1.2   268 Client Hello
  … 0.279180464 52.32.150.180  10.0.2.15      TCP        60 443 → 48390 [ACK] Seq=1 Ack=215 Win=65535 Len=0
  … 0.545463160 52.32.150.180  10.0.2.15      TLSv1.2  1514 Server Hello
  … 0.545488290 10.0.2.15      52.32.150.180  TCP        54 48390 → 443 [ACK] Seq=215 Ack=1461 Win=31240 Le…
  … 0.545584564 52.32.150.180  10.0.2.15      TLSv1.2  1535 Certificate
  … 0.545590966 10.0.2.15      52.32.150.180  TCP        54 48390 → 443 [ACK] Seq=215 Ack=2942 Win=34080 Le…
  … 0.552518657 10.0.2.15      52.32.150.180  TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Hello …
```

```
▸ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▸ Ethernet II, Src: CadmusCo_f9:77:3b (08:00:27:f9:77:3b), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.244.0.13
▸ User Datagram Protocol, Src Port: 31718 (31718), Dst Port: 53 (53)
▾ Domain Name System (query)
    [Response In: 7]
    Transaction ID: 0x6a62
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

```
0000  52 54 00 12 35 02 08 00  27 f9 77 3b 08 00 45 00   RT..5... '.w;..E.
0010  00 48 58 37 40 00 40 11  cb 5e 0a 00 02 0f 0a f4   .HX7@.@. .^......
0020  00 0d 7b e6 00 35 00 34  17 55 6a 62 01 00 00 01   ..{..5.4 .Ujb....
0030  00 00 00 00 00 00 05 74  69 6c 65 73 08 73 65 72   .......t iles.ser
0040  76 69 63 65 73 07 6d 6f  7a 69 6c 6c 61 03 63 6f   vices.mo zilla.co
0050  6d 00 00 01 00 01                                  m.....
```

```
wireshark_pcapng_enp0s3_20160929123817_xNwlrP     Packets: 3867 · Displayed: 3867 (100.0%)     Profile: Default
```

Capturing the packets

1. To start capturing the packets, click on the Capture menu ->options or press CTRL+K.
2. Select the Interface, enable Packet Capture in Promiscuous mode, enable Update the Packets in Real Time, and check the Automatic Scrolling in Live Capture
3. Click the start button available in the Dialog Box.

Display Filter String

By using this, only packets matching the display filter string will be displayed in the Summary Window

1. By clicking the Filter button in the Filter Bar, will display the Display Filter dialog box, where a filter string (Conditions) can be provided.
2. Conditional expressions can be provided directly by typing in the Text Box next to the Filter Button in the Filter Bar. For Example: ip.addr==192.168.52.53 && telnet
3. Click on the expression in the Filter Bar to add the conditions by using the Filter Expression Dialog Box, which displays list of protocol decoders and their headers.

Saving the Captured Traffic

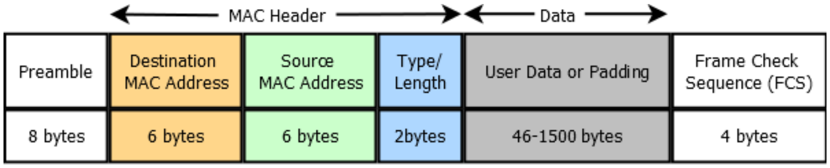
You can save the captured traffic which can also be used as Network-Based Evidence. To save the Captured packet press Ctrl+S, and you will get the dialog-box as shown below. You can save the captured packets and/or the Displayed Packets. Press 'Save' button. You can later open the same captured packets for analysis.

Viewing Statistics

You can view the various statistics by using the statistics menu in the Wireshark.

Answer the questions in the following sections.

Ethernet Header



	MAC Header			Data	
Preamble	Destination MAC Address	Source MAC Address	Type/ Length	User Data or Padding	Frame Check Sequence (FCS)
8 bytes	6 bytes	6 bytes	2bytes	46-1500 bytes	4 bytes

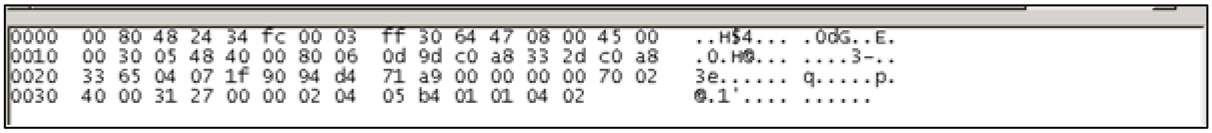
Ethernet Type 2 Frame

As the Ethernet hardware filters the preamble, it is not given to Wireshark or any other application. Most Ethernet interfaces also either don't supply the FCS to Wireshark or other applications, or aren't configured by their driver to do so; therefore, Wireshark will typically only be given the green shaded fields. Ethernet packets with less than the minimum 64 bytes for an Ethernet packet (header + user data + FCS) are padded to 64 bytes, which means that if there's less than 64-(14+4) = 46 bytes of user data, extra padding data is added to the packet. Beware: the minimum Ethernet packet size is commonly mentioned at 64 bytes, which is including the FCS. This can be confusing as the FCS is often not shown by Wireshark, simply because the underlying mechanisms simply don't supply it.

Exercise

1. Fill the answers in the table below by referring to the given packet data:

Worksheet: **Ethernet Frame**

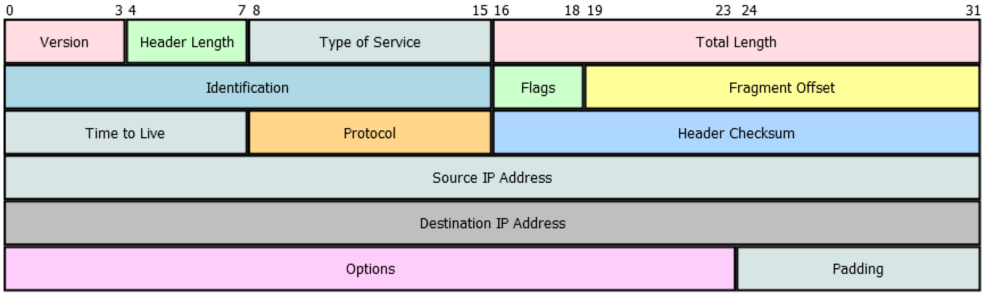


```
0000  00 80 48 24 34 fc 00 03  ff 30 64 47 08 00 45 00   ..H$4... .0dG..E.
0010  00 30 05 48 40 00 80 06  0d 9d c0 a8 33 2d c0 a8   .0.H@... ....3-..
0020  33 65 04 07 1f 90 94 d4  71 a9 00 00 00 00 70 02   3e...... q.....p.
0030  40 00 31 27 00 00 02 04  05 b4 01 01 04 02         @.1'.... ......
```

Fields	Values (Hex/Decimal)
Destination MAC Address	
Source MAC Address	
Ethernet Type	

2. Capture the network traffic in your LAN and write the following:
   a. Write the Destination MAC Address when the frames are broadcasted: ________________
   b. Write the Ethernet Type for the following
      i. IP Packet : ______________
      ii. ARP Request : ______________
      iii. ARP Reply : ______________

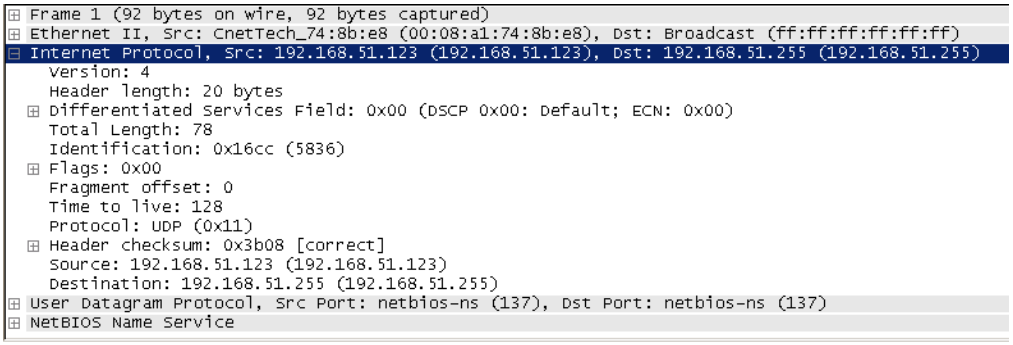
IPv4 Header



IPv4 Datagram Header

Using Wireshark:

1. Generate the IP traffic by pinging some **other** machine or by accessing/logging in to the FTP or TELNET server etc. [For ping type the following in your command shell. `ping 192.168.1.199` (192.168.1.199 is taken as an example here)]
2. To check the IP header in the Captured Packet, click and expand the "Internet protocol" on the protocol tree window in Wireshark.



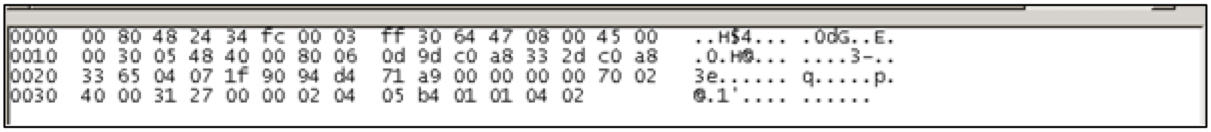
```
⊞ Frame 1 (92 bytes on wire, 92 bytes captured)
⊞ Ethernet II, Src: CnetTech_74:8b:e8 (00:08:a1:74:8b:e8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Internet Protocol, Src: 192.168.51.123 (192.168.51.123), Dst: 192.168.51.255 (192.168.51.255)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 78
    Identification: 0x16cc (5836)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0x3b08 [correct]
    Source: 192.168.51.123 (192.168.51.123)
    Destination: 192.168.51.255 (192.168.51.255)
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
⊞ NetBIOS Name Service
```

3. You can type IP in the Filter Bar and press Apply to view only IP packets rather than ARP packets.

Exercise:

1. Fill the answers in the table below referring to the packet data given in the table:

Worksheet: **IP Datagram**



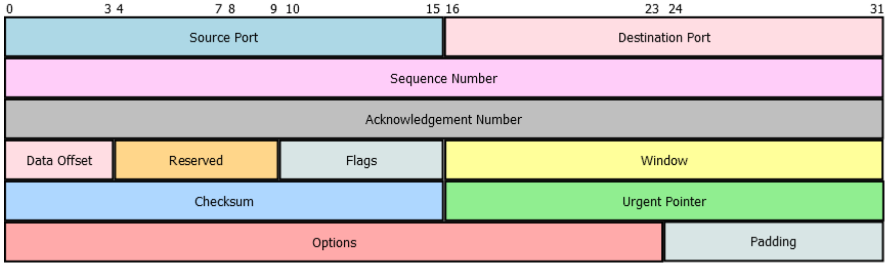
```
0000   00 80 48 24 34 fc 00 03  ff 30 64 47 08 00 45 00   ..H$4... .0dG..E.
0010   00 30 05 48 40 00 80 06  0d 9d c0 a8 33 2d c0 a8   .0.H@... ....3-..
0020   33 65 04 07 1f 90 94 d4  71 a9 00 00 00 00 70 02   3e...... q.....p.
0030   40 00 31 27 00 00 02 04  05 b4 01 01 04 02         @.1'.... ......
```

Fields	Values (Hex/Decimal)
Version	
Internet Header Length	
Total Length	
Identification	
Flags	
Fragment Offset	
Time to Live	
Protocol	
Header Checksum	

Source IP Address	
Destination IP Address	
Padding	

2. Observe the fragmentation of the IP Packets by sending the packets of size greater than MTU to some other system in the network. For e.g., this can be done by `ping –l 4000 <Some ip_addr>` on Windows and/or `ping –c 5 –s 4000 <Some ip_addr>` on Linux.
   [Fragmentation occurs when an IP datagram traveling on a network with a Maximum Transmission Unit (MTU) that is smaller than the size of the datagram. For Ethernet MTU for 'Ethernet v2' is 1500 bytes.]
   a. List which of the 'FLAGS' in IP Header, for each of the THREE (3) packets generated by the above ping command, are set to ONE (1)
      i. FLAGS set in **first** packet : _________________
      ii. FLAGS set in **second** packet : _________________
      iii. FLAGS set in **third** packet : _________________
   b. List the 'Fragment Offset' value (in decimal format) in the IP Header for each of the 3 packets (as in the above question)
      i. First packet : _________________
      ii. Second packet : _________________
      iii. Third packet : _________________
3. Capture the network traffic in your LAN and check the Protocol numbers in the IP Header for the following type of packets
   c. ICMP : ____________
   d. TCP : ____________
   e. UDP : ____________
4. List out the IP Header size in bytes (in decimal format). Note that the IHL (Internet Header Length) filed specifies the header length in 32-bit words : _____________
5. Calculate the data size in bytes in decimal format (Total IP packet length – IP Header size = IP payload size): _______________

TCP Header



TCP Header Format

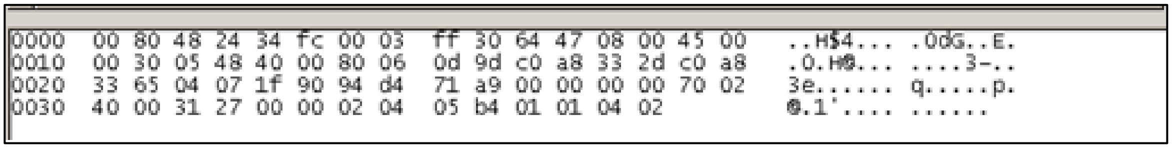
Using Wireshark:

1. Generate the IP traffic by accessing the Web/FTP/TELNET server by typing the URL in the browser/executing FTP command/executing TELNET command.
2. To check the TCP header, apply the '`tcp`' filter in the filter bar and click Transmission Control Protocol on protocol tree window in Wireshark.

Exercise:

1. Fill the answers in the table below referring to the packet data given in the table:

Worksheet: **TCP Segments**



```
0000   00 80 48 24 34 fc 00 03  ff 30 64 47 08 00 45 00   ..H$4... .0dG..E.
0010   00 30 05 48 40 00 80 06  0d 9d c0 a8 33 2d c0 a8   .0.H@... ....3-..
0020   33 65 04 07 1f 90 94 d4  71 a9 00 00 00 00 70 02   3e...... q.....p.
0030   40 00 31 27 00 00 02 04  05 b4 01 01 04 02         @.1'.... ......
```

<table>
<tr><th>Fields</th><th>Values (Hex/Decimal)</th></tr>
<tr><td>Source Port</td><td></td></tr>
<tr><td>Destination Port</td><td></td></tr>
<tr><td>Sequence Number</td><td></td></tr>
<tr><td>Acknowledgment Number</td><td></td></tr>
<tr><td>Header Length</td><td></td></tr>
<tr><td>Flags (Indicate which is set)
  2   1 | | 8   4   2   1
+-+-+-+-+ +-+-+-+-+-+-+-+-+
| U | A | | P | R | S | F |
+-+-+-+-+ +-+-+-+-+-+-+-+-+</td><td></td></tr>
<tr><td>Windows Size</td><td></td></tr>
<tr><td>Checksum</td><td></td></tr>
</table>

2. Capture the network traffic in the LAN when making and closing connection with FTP or TELNET server in the LAN and answer the following.
   a. Observe the TCP 3-way handshake during connection establishment and draw the packets exchanged mentioning sequence no. and acknowledgement no.

      ---------->

      <----------

      ---------->

   b. Observe the TCP connection termination and check for the FIN and ACK flag when the connection close is initiated by the client. Draw the packets exchanged.

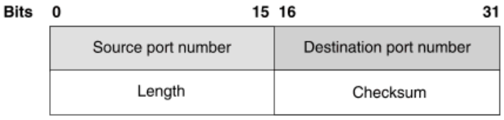
      ---------->

      <----------

      <----------

      ---------->

UDP Header



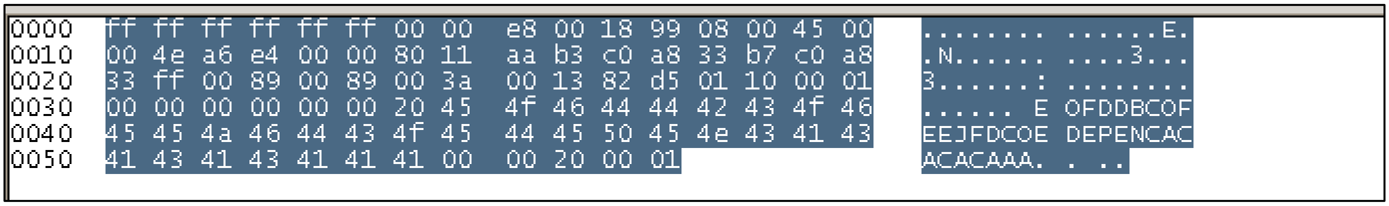
Using Wireshark:

1. To check the UDP header, type the 'udp' in the filter bar and click User Datagram Protocol on the protocol tree window in Wireshark.

Exercise:

1. Fill the answers in the table below referring to the packet data given in the table:

Worksheet: **UDP Datagram**



```
0000  ff ff ff ff ff ff 00 00  e8 00 18 99 08 00 45 00   ........ ......E.
0010  00 4e a6 e4 00 00 80 11  aa b3 c0 a8 33 b7 c0 a8   .N...... ....3...
0020  33 ff 00 89 00 89 00 3a  00 13 82 d5 01 10 00 01   3......: ........
0030  00 00 00 00 00 00 20 45  4f 46 44 44 42 43 4f 46   ...... E OFDDBCOF
0040  45 45 4a 46 44 43 4f 45  44 45 50 45 4e 43 41 43   EEJFDCOE DEPENCAC
0050  41 43 41 43 41 41 41 00  00 20 00 01               ACACAAA. . ..
```

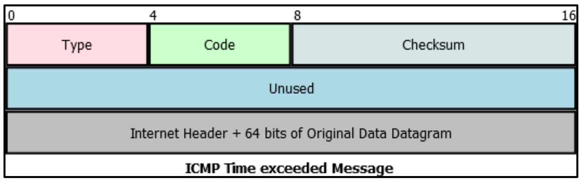
Fields	**Values (Hex/Decimal)**
Source Port	
Destination Port	
UDP Length	
Checksum	

2. Generate at least 3 different types/kinds of network traffic by execution various commands (e.g., connecting to FTP, TELNET, and web server).
    a. List out at least 3 application layer protocols using the UDP Protocol
        i. ___________
        ii. ___________
        iii. ___________

ICMP Header

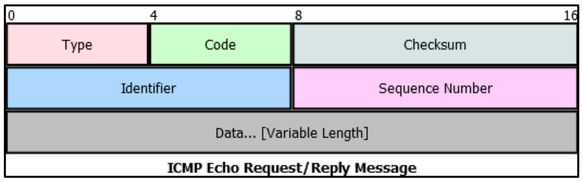
ICMP messages are used for a basic kind of error reporting between host to host, or host to gateway. ICMP, uses the basic support of IP as if it were a higher-level protocol, however, ICMP is actually an integral part of IP. ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable. There are still no guarantees that a datagram will be delivered or a control message will be returned. Some datagrams may still be undelivered without any report of their loss. The ICMP messages typically report errors in the processing of datagrams. ICMP messages are only sent about errors in handling fragment zero of fragmented datagrams. (Fragment zero has the fragment offset equal zero). ICMP messages are sent using the basic IP header.

Time Exceeded



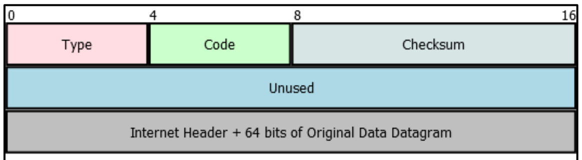
ICMP Time exceeded Message

Echo Request/Reply



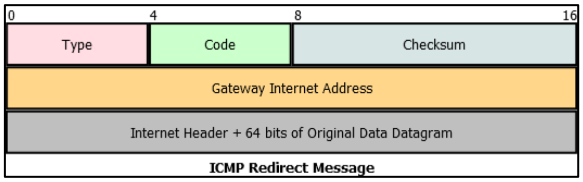
ICMP Echo Request/Reply Message

Destination Unreachable



ICMP Destination Unreachable Message

Redirect

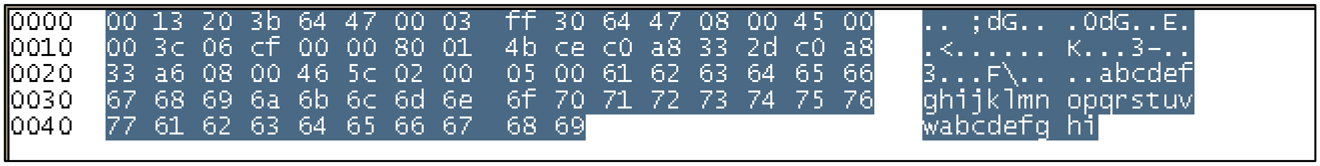


ICMP Redirect Message

Exercise:

1. Fill the answers in the table below referring to the packet data given in the table:

Worksheet: **ICMP**



```
0000  00 13 20 3b 64 47 00 03  ff 30 64 47 08 00 45 00   .. ;dG.. .0dG..E.
0010  00 3c 06 cf 00 00 80 01  4b ce c0 a8 33 2d c0 a8   .<...... K...3-..
0020  33 a6 08 00 46 5c 02 00  05 00 61 62 63 64 65 66   3...F\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Fields	**Values (Hex/Decimal)**
Type	
Code	
Identifier	
Sequence	
Data	

2. Generate the network traffic by executing ‘`ping`’ command in the terminal/command prompt.
   a. Identify the ‘sequence number’ and ‘identifier’ in ping **request** and **response** packets.
      i. Ping/Echo request: Sequence No.: __________ Identifier: _________
      ii. Ping/Echo response: Sequence No.: __________ Identifier: _________
   b. Filter the ICMP packets, locate the Destination Unreachable message and then list the following for ICMP header (If you are unable to capture Destination Unreachable ping packets with Wireshark, refer to Table1 below):
      i. Type : ___________
      ii. Code : ___________

For the list of Types and Codes in the ICMP, see the ICMP Codes table below.

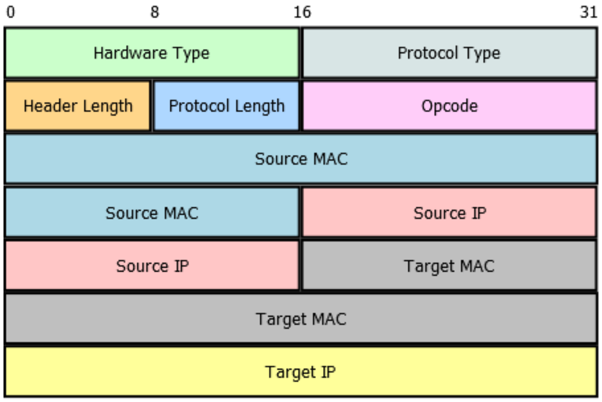
Table 1: ICMP Codes Table

Type	Code	Description	Query	Error
0	0	**Echo reply** (Ping reply)	*	
3		**Destination unreachable**:		
	0	Network unreachable		*
	1	Host unreachable		*
	2	protocol unreachable		*
	3	port unreachable		*
	4	fragmentation needed but don't-fragment bit set		*
	5	Source route failed		*
	6	destination network unknown		*
	7	destination host unknown		*
	8	source host isolated (obsolete)		*
	9	destination network administratively prohibited		*
	10	destination host administratively prohibited		*
	11	network unreachable for TOS		*
	12	host unreachable for TOS		*
	13	communication administratively prohibited by filtering		*
	14	host precedence violation		*
	15	precedence cut-off in effect		*
4	0	**Source quench** (elementary flow control)		*
5		**Redirect message**:		
	0	redirect for network		*

	1	redirect for host		*
	2	redirect for type-of-service and network		*
	3	redirect for type-of-service and host		*
8	0	**Echo request** (Ping request)	*	
9	0	router advertisement	*	
10	0	router solicitation	*	
11		**Time exceeded**:		
	0	time-to-live equals 0 during transit (Traceroute,)		*
	1	time-to-live equals 0 during reassembly ()		*
12		**Parameter problem**:		
	0	IP header bad (catchall error)		*
	1	required option missing		*
13	0	timestamp request	*	
14	0	timestamp reply	*	
15	0	information request	*	
16	0	information reply (obsolete)	*	
17	0	address mask request	*	
18	0	address mask reply	*	

ARP Header

The Address Resolution Protocol is used to dynamically discover the mapping between a layer 3 (protocol) and a layer 2 (hardware) address. A typical use is the mapping of an IP address (e.g., 192.168.0.10) to the underlying Ethernet address (e.g., 01:02:03:04:05:06). Sometimes a host sends out ARP packets NOT in order to discover a mapping but to use ARP for preloading of the ARP table of a different host with an entry. These special ARP packets are referred to as Gratuitous ARPs.

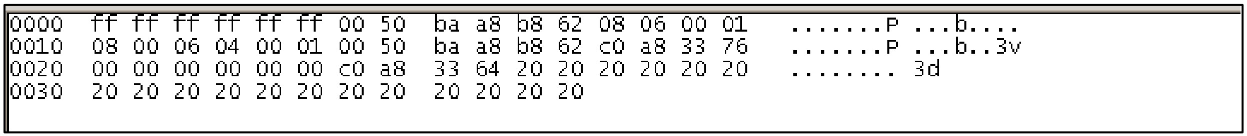


ARP Header

Exercise:

1. Fill the answers in the table below referring to the packet data given in the table:

Worksheet: **ARP Packets**



```
0000   ff ff ff ff ff ff 00 50  ba a8 b8 62 08 06 00 01   .......P ...b....
0010   08 00 06 04 00 01 00 50  ba a8 b8 62 c0 a8 33 76   .......P ...b..3v
0020   00 00 00 00 00 00 c0 a8  33 64 20 20 20 20 20 20   ........ 3d
0030   20 20 20 20 20 20 20 20  20 20 20 20
```

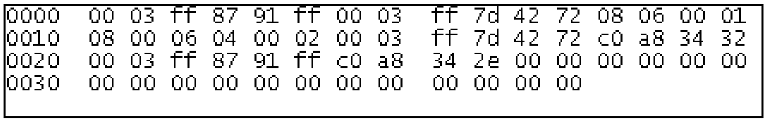
Fields	**Values (Hex/Decimal)**
Hardware Type	
Protocol Type	
Hardware Size	
Protocol Size	
Opcode	
Sender MAC Address	
Sender IP Address	
Destination MAC Address	
Destination IP Address	

2. Capture the packets in the LAN and answer the following for ARP packets: (**Hint:** Observe the Info Columns of the Summary Window in Wireshark for ARP packets. e.g., 'who has 192.168.51.166? Tell 192.168.51.169' and '192.168.51.166 is at 00:50:8d:2d:ac:6c')
   a. Write the Destination MAC Address when the ARP Request is sent: _______________
   b. View the ARP Cache of your system, by executing `arp –a` and/or `arp –v` on linux and `arp –a` on Windows. List the content of ARP cache for the interface which is active (i.e., connected to the LAN):

      ____
      ____
      ____

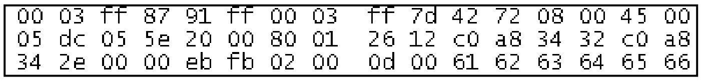
Mixed Assignments

Answer the following questions referring to the packet data given in the table(s):



```
0000   00 03 ff 87 91 ff 00 03  ff 7d 42 72 08 06 00 01
0010   08 00 06 04 00 02 00 03  ff 7d 42 72 c0 a8 34 32
0020   00 03 ff 87 91 ff c0 a8  34 2e 00 00 00 00 00 00
0030   00 00 00 00 00 00 00 00  00 00 00 00
```

1. Identify the following fields in the above shown packet
   a. Ethernet Type: ______________
2. Within ARP packet (for the above shown packet) list the following
   a. Source IP Address: ______________
   b. Destination IP Address: ______________



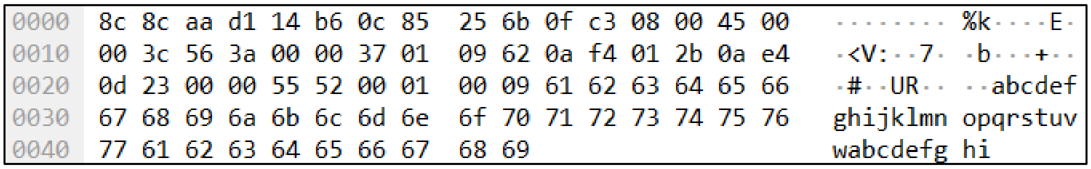
```
 00 03 ff 87 91 ff 00 03  ff 7d 42 72 08 00 45 00
 05 dc 05 5e 20 00 80 01  26 12 c0 a8 34 32 c0 a8
 34 2e 00 00 eb fb 02 00  0d 00 61 62 63 64 65 66
```

3. Identify the following field in the above shown packet:
   a. Ethernet Type: _____________
4. Within IP Datagram list the following:
   a. Source IP Address: _____________

b. Destination IP Address: _____________

c. Protocol: _____________

d. Status of More Fragment Flag: _____________



```
0000  8c 8c aa d1 14 b6 0c 85  25 6b 0f c3 08 00 45 00   ········ %k····E·
0010  00 3c 56 3a 00 00 37 01  09 62 0a f4 01 2b 0a e4   ·<V:··7· ·b···+··
0020  0d 23 00 00 55 52 00 01  00 09 61 62 63 64 65 66   ·#··UR·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

5. Above given is an ICMP packet.
   a. Identify whether it’s an echo request or reply packet: _____________

Notes

1. Download link for Wireshark: https://www.wireshark.org/download.html
2. Sample PCAP file are available at: https://wiki.wireshark.org/SampleCaptures
3. Other packet analysis software:
   - Network Packet Analyzer
   - Network Monitor
   - NetFlow Analyzer
   - Omnipeek
   - tcpdump