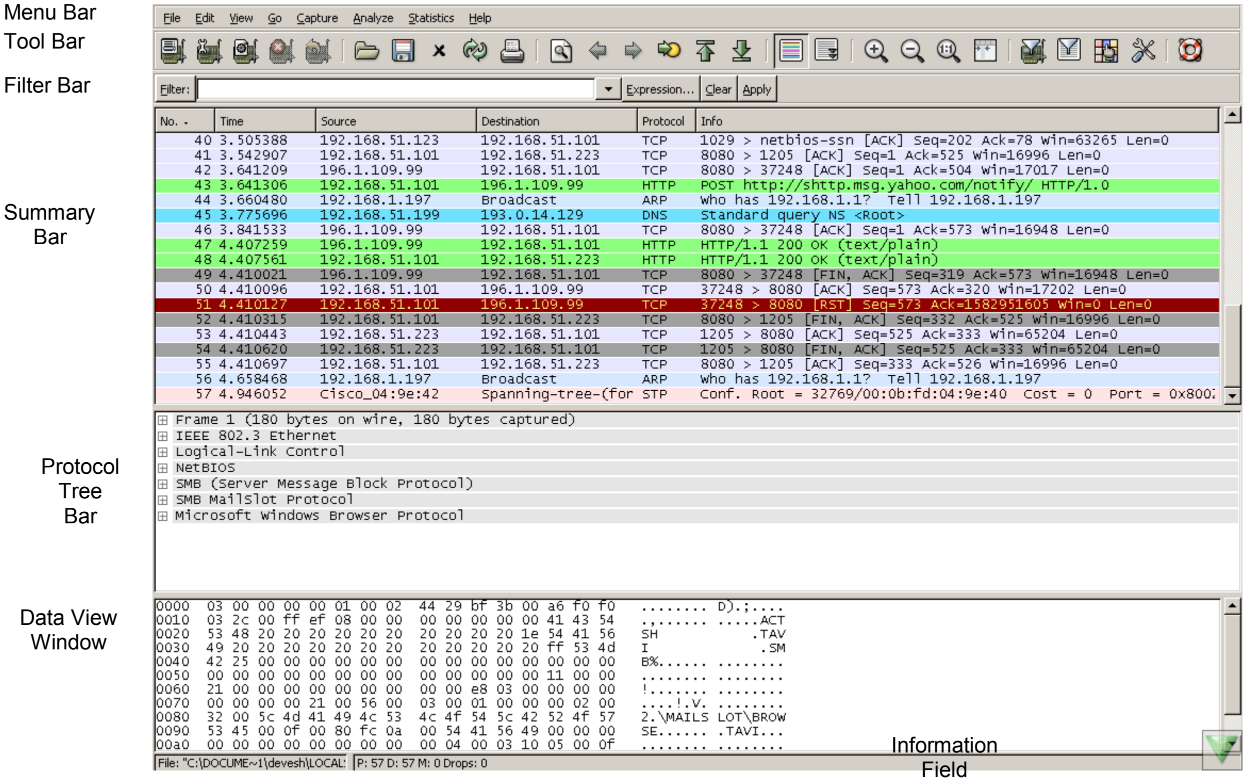
TCP/IP Packet Analysis using Wireshark

Using Wireshark

Start the wireshark by clicking on start | programs| wireshark | wireshark. You will be able to see the GUI of the wireshark as shown below:



No.	Time	Source	Destination	Protocol	Info
40	3.505388	192.168.51.123	192.168.51.101	TCP	1029 > netbios-ssn [ACK] Seq=202 Ack=78 Win=63265 Len=0
41	3.542907	192.168.51.101	192.168.51.223	TCP	8080 > 1205 [ACK] Seq=1 Ack=525 Win=16996 Len=0
42	3.641209	196.1.109.99	192.168.51.101	TCP	8080 > 37248 [ACK] Seq=1 Ack=504 Win=17017 Len=0
43	3.641306	192.168.51.101	196.1.109.99	HTTP	POST http://shttp.msg.yahoo.com/notify/ HTTP/1.0
44	3.660480	192.168.1.197	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.197
45	3.775696	192.168.51.199	193.0.14.129	DNS	Standard query NS <Root>
46	3.841533	196.1.109.99	192.168.51.101	TCP	8080 > 37248 [ACK] Seq=1 Ack=573 Win=16948 Len=0
47	4.407259	196.1.109.99	192.168.51.101	HTTP	HTTP/1.1 200 OK (text/plain)
48	4.407561	192.168.51.101	192.168.51.223	HTTP	HTTP/1.1 200 OK (text/plain)
49	4.410021	196.1.109.99	192.168.51.101	TCP	8080 > 37248 [FIN, ACK] Seq=319 Ack=573 Win=16948 Len=0
50	4.410096	192.168.51.101	196.1.109.99	TCP	37248 > 8080 [ACK] Seq=573 Ack=320 Win=17202 Len=0
51	4.410127	192.168.51.101	196.1.109.99	TCP	37248 > 8080 [RST] Seq=573 Ack=1582951605 Win=0 Len=0
52	4.410315	192.168.51.101	192.168.51.223	TCP	8080 > 1205 [FIN, ACK] Seq=332 Ack=525 Win=16996 Len=0
53	4.410443	192.168.51.223	192.168.51.101	TCP	1205 > 8080 [ACK] Seq=525 Ack=333 Win=65204 Len=0
54	4.410620	192.168.51.223	192.168.51.101	TCP	1205 > 8080 [FIN, ACK] Seq=525 Ack=333 Win=65204 Len=0
55	4.410697	192.168.51.101	192.168.51.223	TCP	8080 > 1205 [ACK] Seq=333 Ack=526 Win=16996 Len=0
56	4.658468	192.168.1.197	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.197
57	4.946052	Cisco_04:9e:42	Spanning-tree-(for	STP	Conf. Root = 32769/00:0b:fd:04:9e:40 Cost = 0 Port = 0x800:

```
⊞ Frame 1 (180 bytes on wire, 180 bytes captured)
⊞ IEEE 802.3 Ethernet
⊞ Logical-Link Control
⊞ NetBIOS
⊞ SMB (Server Message Block Protocol)
⊞ SMB MailSlot Protocol
⊞ Microsoft Windows Browser Protocol
```

```
0000  03 00 00 00 00 01 00 02  44 29 bf 3b 00 a6 f0 f0   ........ D).;....
0010  03 2c 00 ff ef 08 00 00  00 00 00 00 00 41 43 54   .,...... .....ACT
0020  53 48 20 20 20 20 20 20  20 20 20 20 1e 54 41 56   SH           .TAV
0030  49 20 20 20 20 20 20 20  20 20 20 20 20 ff 53 4d   I             .SM
0040  42 25 00 00 00 00 00 00  00 00 00 00 00 00 00 00   B%...... ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 11 00 00   ........ ........
0060  21 00 00 00 00 00 00 00  00 00 e8 03 00 00 00 00   !....... ........
0070  00 00 00 00 21 00 56 00  03 00 01 00 00 00 02 00   ....!.V. ........
0080  32 00 5c 4d 41 49 4c 53  4c 4f 54 5c 42 52 4f 57   2.\MAILS LOT\BROW
0090  53 45 00 0f 00 80 fc 0a  00 54 41 56 49 00 00 00   SE...... .TAVI...
00a0  00 00 00 00 00 00 00 00  00 04 00 03 10 05 00 0f   ........ ........
```

File: "C:\DOCUME~1\devesh\LOCAL: P: 57 D: 57 M: 0 Drops: 0

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

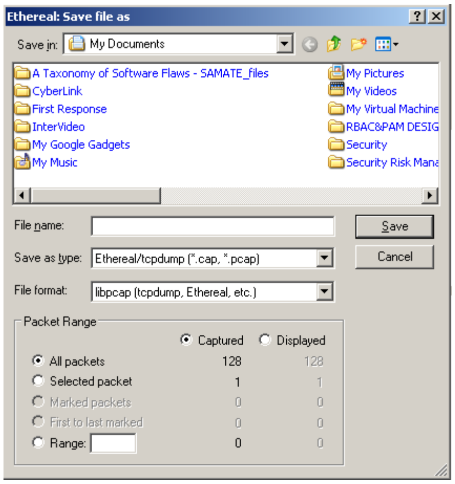
2) **Display Filter String**- By using this, only packets matching the display filter string will be displayed in the Summary Window
   a. By clicking the Filter button in the Filter Bar, will display the Display Filter dialog box, where a filter string (Conditions) can be provided.
   b. Conditional 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

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.

3) **Save 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.



File name:

Save as type: Ethereal/tcpdump (*.cap, *.pcap)

File format: libpcap (tcpdump, Ethereal, etc.)

Packet Range

	● Captured	○ Displayed
● All packets	128	128
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0

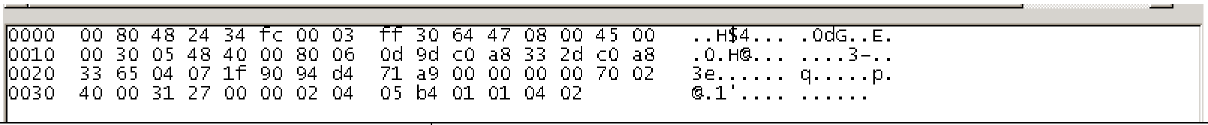
4) **You can view the various statistics by using the statistics menu in the wireshark**

5) **Generate the traffic and fill the tables in following sections**.

1) Ethernet Header Format

Destination MAC Address	Source MAC Address	Type

Worksheet: **Ethernet Frame**



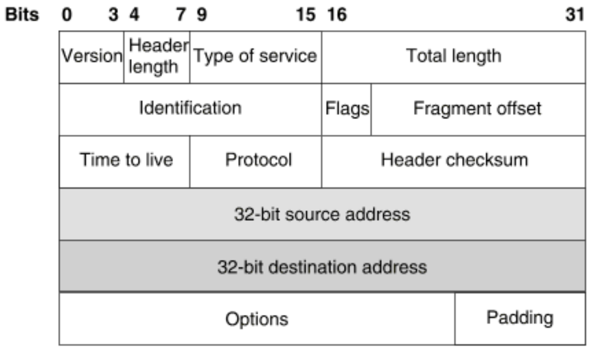
```
0000   00 80 48 24 34 fc 00 03  ff 30 64 47 08 00 45 00   ..H$4... .0dG..E.
0010   00 30 05 48 40 00 80 06  0d 9d c0 a8 33 2d c0 a8   .0.H@... ....3-..
0020   33 65 04 07 1f 90 94 d4  71 a9 00 00 00 00 70 02   3e...... q.....p.
0030   40 00 31 27 00 00 02 04  05 b4 01 01 04 02         @.1'.... ......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

Fields	**Values** **Hex/Decimal Code**
Destination MAC Address	
Source MAC Address	
Ethernet Type	

Exercise

1. Check the Destination MAC Address when the frames are broadcasted _________________.
2. Check the ARP and IP Datagram's Ethernet Type
   a. IP Datagram : _______________
   b. ARP request : _______________
   c. ARP reply : _______________

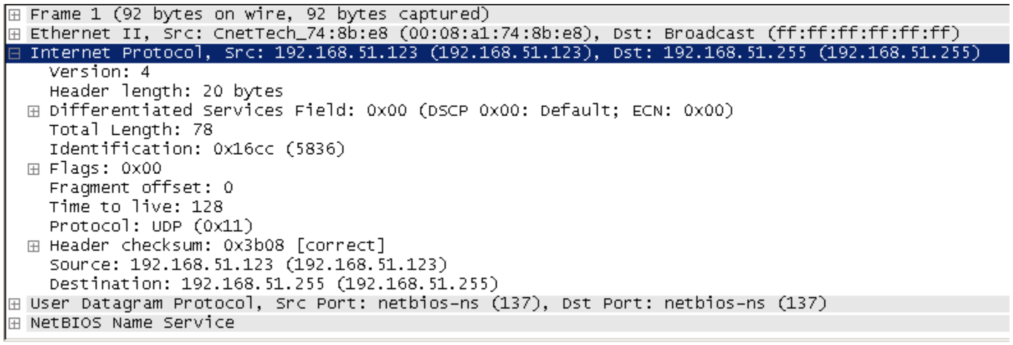
2) IPv4 header format



Using Wireshark:

1. Generate the IP traffic by pinging some other machine
   Type the following in your command shell.   Ping *192.168.1.199 .*
   (192.168.1.199 is taken as an example here)

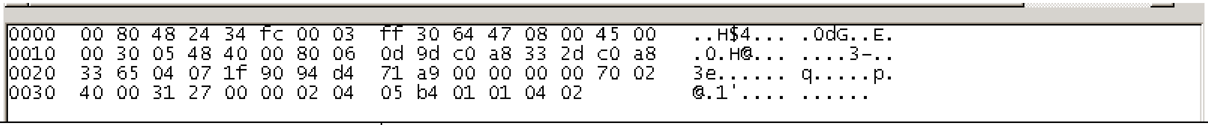
2. To check the IP header in the Captured Packet click **Internet protocol** on the protocol tree window in Wireshark.



```
⊞ 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.

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 Code
Version	
Internet Header Length	
Total Length	
Identification	
Flags	
Fragment Offset	
Time to Live	

Protocol	
Header Checksum	
Source Address	
Destination Address	
Padding	

Exercise:

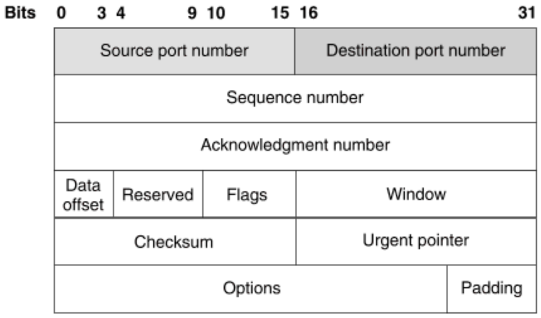
1. Generate the fragmentation of the packet, by using `ping –l 4000 <Some ip_addr>`. Fragmentation occurs when an IP datagram traveling on a network with a Maximum Transmission Unit (MTU) that is smaller than the size of the datagram. For Ethernet MTU for an IP datagram is 1500 bytes.
   a. Check the flags in IP header ________________
   b. Check the Fragment Offset value________________

2. Check the Protocol numbers of
   a. ICMP:___________
   b. TCP:___________
   c. UDP:___________

3. Calculate the header size by multiplying it by 4. ____________
4. The value found in IP header is not represented in bytes. This value is represented as 32-but words. So 5 32-bit words (or 4 Bytes) = ____________ ____bytes.

5. Calculate the data size: Total IP size – Header size. ______________

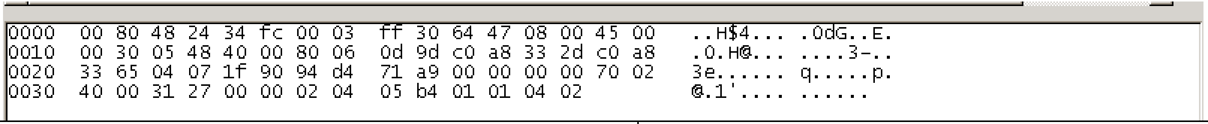
3) TCP header format



Using Wireshark:

1. Generate the IP traffic by accessing the Web Server by typing the URL in the browser
2. To check the TCP header, type the tcp in the filter bar and click Transmission Control Protocol on protocol tree window in Wireshark.

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'.... ......
```

Fields	**Values** **Hex/Decimal Code**

Source Port	
Destination Port	
Sequence Number	
Acknowledgment Number	
Header Length	

Flags
(Indicate which is set)
`  2   1 | | 8   4   2   1`
`+-+-+-+-+ +-+-+-+-+-+-+-+-+`
`| U | A | | P | R | S | F |`
`+-+-+-+-+ +-+-+-+-+-+-+-+-+`	

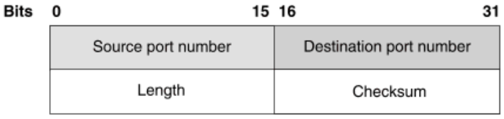
Windows Size	
Checksum	

Exercise:

1. Check the TCP 3 way handshake and draw the packets exchanged mentioning sequence no. and acknowledgement no.

2. Check for the FIN and ACK flag when the connection is closed and draw the packets exchanged. Check for both types of connection termination scenarios.

4) UDP header format

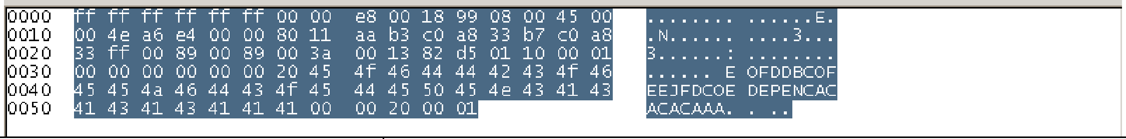


Bits 0 ... 15	16 ... 31
Source port number	Destination port number
Length	Checksum

Using Wireshark:

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

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. . ..
```

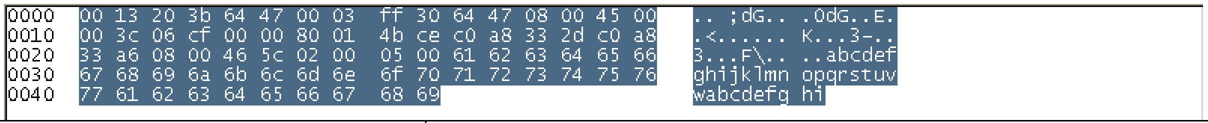
Fields	Values Hex/Decimal Code
Source Port	
Destination Port	
UDP Length	
Checksum	

Exercise:

1. List out the Application protocols using the UDP Protocol
   a. ___________
   b. ___________
   c. ___________

5) ICMP Header

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 Code
Type	
Code	
Identifier	
Sequence	
Data	

Generate the traffic by using ping command.

Exercise:

1. Identify the sequence number _____________ ___and Identifier ________________ in ping request and response packets.

2. Filter the ICMP packets and look at the Destination Unreachable message. List the following:
   a. Type : ____________
   b. Code : ____________

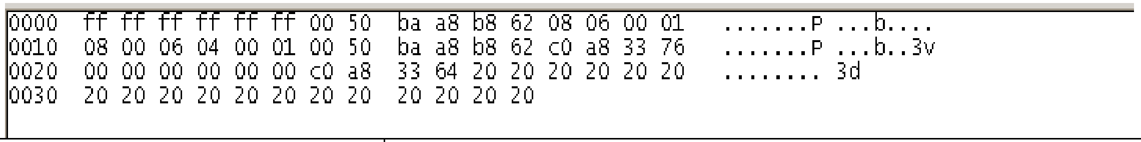
For Types and Codes, see the ICMP Codes table.

ICMP Codes

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 cutoff in effect		*
4	0	source quench (elementary flow control.)		*
5		redirect:		
	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	*	

6) ARP Packets

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 Code**
Hardware Type	
Protocol Type	
Hardware Size	
Protocol Size	
Opcode	

Sender MAC Address	
Sender IP Address	
Destination MAC Address	
Destination IP Address	

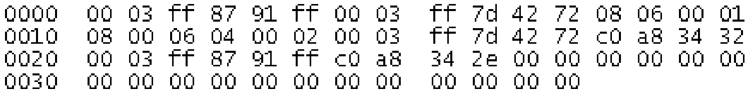
Exercise:

Check the Info Columns of the Summary Window in Wireshark.
Eg. Who has 192.168.51.166? Tell 192.168.51.169
!92.168.51.166 is at 00:50:8d:2d:ac:6c

1. Check the Destination address when the ARP Request is sent. ______________

2. To view the ARP Cache of your system, open the command prompt and type arp –a. List the content of ARP cache:
    a. __________
    b. __________
    c. __________

Mixed Assignments:



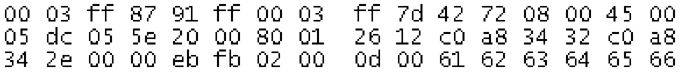
```
0000  00 03 ff 87 91 ff 00 03  ff 7d 42 72 08 06 00 01
0010  08 00 06 04 00 02 00 03  ff 7d 42 72 c0 a8 34 32
0020  00 03 ff 87 91 ff c0 a8  34 2e 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

Identify the following field in the above shown packet

1. Ethernet Type_____________

Within IP Datagram list

2. Source Address______________
3. Destination Address_____________



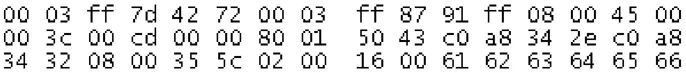
```
00 03 ff 87 91 ff 00 03  ff 7d 42 72 08 00 45 00
05 dc 05 5e 20 00 80 01  26 12 c0 a8 34 32 c0 a8
34 2e 00 00 eb fb 02 00  0d 00 61 62 63 64 65 66
```

Identify the following field in the above shown packet

1. Ethernet Type___________

Within IP Datagram

2. Source Address_____________
3. Destination Address____________
4. Protocol____________
5. Status of More Fragment Flag______________



```
00 03 ff 7d 42 72 00 03  ff 87 91 ff 08 00 45 00
00 3c 00 cd 00 00 80 01  50 43 c0 a8 34 2e c0 a8
34 32 08 00 35 5c 02 00  16 00 61 62 63 64 65 66
```

Identify the following field in the above shown packet

1. It’s an ICMP packet. Identify whether it’s a ping Request or Reply packet. ____________