

# **Assignment 3**

## Using a Packet Sniffer

## Part 1: Basics

### Answer 1:

1. ARP
2. UDP
3. LLMNR
4. TCP
5. STP
6. SSDP
7. DHCPv6
8. DNS
9. HTTP
10. TLSv1

### Answer 2:

When we look at the frame section of the GET request we see that the time the packet arrived is 08:04:59.937502000.

The same section for the HTTP OK shows an arrival time is 08:05:00.264414000  
Therefore, time difference = 0.326912 sec

### Answer 3:

- Because, we are behind a proxy address, therefore the ip address of [www.google.com](http://www.google.com) cannot be traced using wireshark as the DNS fails and request is sent to the proxy server which is 202.141.80.22
- The ip address of my computer is 172.16.27.66 which can be seen in the IP header field.

## Part 2: Ethernet

No.	Time	Source	Destination	Protocol	Length	Info
289	10.609042	Pegatron_b3:08:13	Pegatron_b3:06:13	ARP	42	172.16.27.66 is at 38:60:77:b3:08:13
290	10.655474	Pegatron_b3:05:18	Pegatron_b3:08:13	ARP	60	Who has 172.16.27.66? Tell 172.16.27.34
291	10.655484	Pegatron_b3:08:13	Pegatron_b3:05:18	ARP	42	172.16.27.66 is at 38:60:77:b3:08:13
292	10.683312	AsustekC_a8:7e:f0	Pegatron_b3:08:13	ARP	60	Who has 172.16.27.66? Tell 172.16.26.108
293	10.683326	Pegatron_b3:08:13	AsustekC_a8:7e:f0	ARP	42	172.16.27.66 is at 38:60:77:b3:08:13
294	10.683726	Hewlett-ee:22:fa	Broadcast	0x0800	60	IP
295	10.713352	Pegatron_b3:08:13	Cisco_9d:70:00	0x0800	460	IP
296	10.713684	Pegatron_b3:06:24	Pegatron_b3:08:13	ARP	60	Who has 172.16.27.66? Tell 172.16.27.24
297	10.713692	Pegatron_b3:08:13	Pegatron_b3:06:24	ARP	42	172.16.27.66 is at 38:60:77:b3:08:13
298	10.732156	Pegatron_c3:3a:11	Pegatron_b3:08:13	ARP	60	Who has 172.16.27.66? Tell 172.16.27.25
299	10.732168	Pegatron_b3:08:13	Pegatron_c3:3a:11	ARP	42	172.16.27.66 is at 38:60:77:b3:08:13
300	10.739419	Pegatron_b3:05:28	Pegatron_b3:08:13	ARP	60	Who has 172.16.27.66? Tell 172.16.27.7
301	10.739432	Pegatron_b3:08:13	Pegatron_b3:05:28	ARP	42	172.16.27.66 is at 38:60:77:b3:08:13

▶ Frame 295: 460 bytes on wire (3680 bits), 460 bytes captured (3680 bits)  
 ▼ Ethernet II, Src: Pegatron\_b3:08:13 (38:60:77:b3:08:13), Dst: Cisco\_9d:70:00 (00:24:f9:9d:70:00)  
   ▼ Destination: Cisco\_9d:70:00 (00:24:f9:9d:70:00)  
     Address: Cisco\_9d:70:00 (00:24:f9:9d:70:00)  
       ... ..0 ... = IG bit: Individual address (unicast)  
       ... ..0. ... = LG bit: Globally unique address (factory default)  
   ▼ Source: Pegatron\_b3:08:13 (38:60:77:b3:08:13)  
     Address: Pegatron\_b3:08:13 (38:60:77:b3:08:13)  
       ... ..0 ... = IG bit: Individual address (unicast)  
       ... ..0. ... = LG bit: Globally unique address (factory default)  
   Type: IP (0x0800)  
 ▼ Data (446 bytes)  
   Data: 450001bee0b840004006768bac101b42ca8d5016a0ce0c38...  
   [Length: 446]

```

0040 36 e0 47 45 54 20 68 74 74 70 3a 2f 2f 77 77 77 6. GET ht tp://www
0050 2e 66 61 71 73 2e 6f 72 67 2f 72 66 63 73 2f 72 .faqs.or g/rfcs/r
0060 66 63 38 32 36 2e 68 74 6d 6c 20 48 54 54 50 2f fc826.ht m1 HTTP/
0070 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 66 1.1..Hos t: www.f
0080 61 71 73 2e 6f 72 67 0d 0a 55 73 65 72 2d 41 67 aqs.org. .User-Ag
0090 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0
00a0 20 28 58 31 31 3b 20 55 62 75 6e 74 75 3b 20 4c (X11; U buntu; L
00b0 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 76 3a inux x86 _64; rv:
00c0 31 35 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 15.0) Ge cko/2010
00d0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 35 2e 0101 Fir efox/15.
  
```

Answer 1: 48-bit Ethernet address of your computer is 38:60:77:b3:08:13.

Answer 2: The destination address is 00:24:f9:9d:70:00. It is not the Ethernet address of the website with the RFC. This is not the address of the server, but rather, the address of the router or switch that this computer is connected to.

Answer 3: The hex value for the Frame type field is 0x0800. It identifies an upper layer protocol encapsulating the frame data which in this case is Internet Protocol version 4.

Answer 4: GET is at 67 bytes away from the start of the header frame.

No.	Time	Source	Destination	Protocol	Length	Info
319	11.062600	Pegatron_b3:08:13	AsustekC_a8:7e:91	ARP	42	172.16.27.66 is at 38:60:77:b3:08:13
320	11.413335	Cisco_9d:70:00	PVST+	STP	64	Conf. Root = 32768/0/00:24:f9:9d:70:04 Cost = 0 Port = 0x8305
321	11.439668	Cisco_9d:70:00	Pegatron_b3:08:13	0x0800	4209	IP
322	11.439702	Pegatron_b3:08:13	Cisco_9d:70:00	0x0800	66	IP
323	11.439864	Cisco_9d:70:00	Pegatron_b3:08:13	0x0800	314	IP
324	11.439880	Pegatron_b3:08:13	Cisco_9d:70:00	0x0800	66	IP
325	11.485636	Pegatron_b3:08:79	IPv6mcast_00:01:00:03	0x86dd	84	IPv6
326	11.485777	Pegatron_b3:08:79	IPv4mcast_00:00:fc	0x0800	64	IP
327	11.521754	Pegatron_b3:08:13	Cisco_9d:70:00	0x0800	460	IP

  

Frame 321: 4209 bytes on wire (33672 bits), 4209 bytes captured (33672 bits)

Ethernet II, Src: Cisco\_9d:70:00 (00:24:f9:9d:70:00), Dst: Pegatron\_b3:08:13 (38:60:77:b3:08:13)

Destination: Pegatron\_b3:08:13 (38:60:77:b3:08:13)

Address: Pegatron\_b3:08:13 (38:60:77:b3:08:13)

.....0..... = IG bit: Individual address (unicast)

.....0..... = LG bit: Globally unique address (factory default)

Source: Cisco\_9d:70:00 (00:24:f9:9d:70:00)

Address: Cisco\_9d:70:00 (00:24:f9:9d:70:00)

.....0..... = IG bit: Individual address (unicast)

.....0..... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Data (4195 bytes)

Data: 45001063076e40003f064231ca8d5016ac101b420c38a0ce...

[Length: 4195]

  

0000	38 60 77 b3 08 13 00 24 f9 9d 70 00 08 00 15 00	8'w....\$ ..p...E..
0010	10 63 07 6e 40 00 3f 06 42 31 ca 8d 50 16 ac 10	.c.nē.?. B1..P...
0020	1b 42 0c 38 a0 ce 44 4c f3 ec f1 d9 9b 2b 80 18	.B.8..DL .....+...
0030	00 a1 f2 4b 00 00 01 01 08 0a 2e 64 53 a2 00 0a	...K.... ..05...
0040	8d 7b 4b 54 54 50 2f 31 2e 30 20 32 30 30 20 4f	..(HTTP/1.0 200 O
0050	4b 0d 0a 44 61 74 65 3a 20 57 65 64 2c 20 32 30	K..Date: Wed, 20
0060	20 4d 61 72 20 32 30 31 33 20 30 37 3a 32 36 3a	Mar 201 3 07:26:
0070	31 37 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20	17 GMT.. Server:
0080	41 70 61 63 68 65 0d 0a 56 61 72 79 3a 20 41 63	Apache.. Vary: Ac
0090	63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 2c 65 73	cept-Enc oding:Us
00a0	65 72 2d 41 67 65 6e 74 0d 0a 43 6f 6e 74 65 6e	er-Agent ..Conten
00b0	74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70	t-Encodi ng: gzip
00c0	0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68	..Conten t-Length
00d0	8a 20 31 32 33 36 30 0d 0a 43 6f 6e 74 65 6e 74	: 12350 ..Content

Answer 5: The source address is 00:24:f9:9d:70:00 which is the address of the router or switch that the local computer is connected to. No, it is not the address of my computer nor the address of the website server.

Answer 6: The destination address of the Ethernet frame is 38:60:77:b3:08:13 which is the address of my computer.

Answer 7: The hex value for the Frame type field is 0x0800. It identifies an upper layer protocol encapsulating the frame data which in this case is Internet Protocol version 4.

## Part 3: IP

No.	Time	Source	Destination	Protocol	Length	Info
175	5.275314	202.141.80.9	172.16.27.66	DNS	129	Standard query response
176	5.275330	202.141.81.2	172.16.27.66	DNS	129	Standard query response
177	5.275558	172.16.27.66	202.141.80.9	DNS	80	Standard query AAAA jampui.iitg.ernet.in
178	5.276157	202.141.80.9	172.16.27.66	DNS	129	Standard query response
179	5.276416	172.16.27.66	202.141.80.9	DNS	80	Standard query A jampui.iitg.ernet.in
180	5.276875	202.141.80.9	172.16.27.66	DNS	171	Standard query response A 202.141.80.21
181	5.277119	172.16.27.66	202.141.80.21	UDP	70	Source port: 33028 Destination port: traceroute
182	5.277138	172.16.27.66	202.141.80.21	UDP	70	Source port: 33253 Destination port: 33435
183	5.277152	172.16.27.66	202.141.80.21	UDP	70	Source port: 57588 Destination port: 33436
184	5.277164	172.16.27.66	202.141.80.21	UDP	70	Source port: 59514 Destination port: 33437

  

Internet Protocol Version 4, Src: 172.16.27.66 (172.16.27.66), Dst: 202.141.80.21 (202.141.80.21)

Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))  
Total Length: 56  
Identification: 0x3026 (12326)  
Flags: 0x00  
Fragment offset: 0  
Time to live: 1  
Protocol: UDP (17)  
Header checksum: 0xa79a [correct]  
Source: 172.16.27.66 (172.16.27.66)  
Destination: 202.141.80.21 (202.141.80.21)  
User Datagram Protocol, Src Port: 33028 (33028), Dst Port: traceroute (33434)
Data (28 bytes)
Data: 404142434445464748494a4b4c4d4e4f5051525354555657...  
[Length: 28]

```

0000  00 24 f9 9d 70 00 38 60 77 b3 08 13 08 00 45 00  .$.p.8' w....E.
0010  00 38 30 26 00 00 01 11 a7 9a ac 10 1b 42 ca 8d  ,808... ..B..
0020  50 15 81 04 82 9a 00 24 df c9 40 41 42 43 44 45  P.....$ .@ABCDE
0030  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHJKLM NOPQRSTU
0040  56 57 58 59 5a 5b                                VWXYZ[

```

Answer 1: Ip address of computer is 172.16.27.66

Answer 2: Upper Layer Protocol field is UDP(17).

Answer 3:

IPHeader Length = 20 bytes

Total Length = 56 bytes

Thus there are 36 bytes in the payload of the IP datagram.

Answer 4: The more fragments bit = 0, so the data is not fragmented.

Answer 5: Header Checksum and Identification always change and Time to live may remain same in some packets.

Answer 6:

The fields **that stay constant** across the IP datagrams are:

- Version --Using IPv4 for all packets
- Header Length --These are ICMP packet
- Source IP -- Sending from the same source
- Destination IP -- Sending to the same destination
- Differentiated Services --All packets are ICMP they use the same type of Service class
- Upper Layer Protocol -- These are ICMP packets

The fields **that must stay** constant are:

- Version --Using IPv4 for all packets
- Header Length --These are ICMP packet
- Source IP -- Sending from the same source
- Destination IP -- Sending to the same destination
- Differentiated Services --All packets are ICMP they use the same type of Service class
- Upper Layer Protocol -- These are ICMP packets

The fields that **must change** are:

- Identification --IP packets must have different ids
- Time to live --Traceroute increments each subsequent packet
- Header checksum --Header changes, so must checksum

No.	Time	Source	Destination	Protocol	Length	Info
84	2.095017	172.16.24.254	172.16.27.66	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
85	2.095094	172.16.24.254	172.16.27.66	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
86	2.095161	172.16.24.254	172.16.27.66	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
645	18.399282	172.16.24.254	172.16.27.66	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
646	18.399311	172.16.24.254	172.16.27.66	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
▶ Frame 645: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)						
▶ Ethernet II, Src: Cisco_9d:70:00 (00:24:f9:9d:70:00), Dst: Pegatron_b3:08:13 (38:60:77:b3:08:13)						
▼ Internet Protocol Version 4, Src: 172.16.24.254 (172.16.24.254), Dst: 172.16.27.66 (172.16.27.66)						
Version: 4						
Header length: 20 bytes						
▶ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))						
Total Length: 56						
Identification: 0x04ad (1197)						
▶ Flags: 0x00						
Fragment offset: 0						
Time to live: 255						
Protocol: ICMP (1)						
▶ Header checksum: 0x29f7 [correct]						
Source: 172.16.24.254 (172.16.24.254)						
Destination: 172.16.27.66 (172.16.27.66)						
▶ Internet Control Message Protocol						
0000	38 60 77 b3 08 13 00 24	f9 9d 70 00 08 00 45 c0	8`w....\$w.p...E.			
0010	00 38 04 ad 00 00 ff 01	29 f7 ac 10 18 fe ac 10	.8.....)......			
0020	1b 42 0b 00 11 73 00 00	00 00 45 00 00 38 2d a2	.B...S...E..8-			
0030	00 00 01 11 aa 1e ac 10	1b 42 ca 8d 50 15 b5 3e	.....B..P..>			
0040	82 9a 00 24 ab 8f		...\$..			

## Answer 7:

The identification field is 0x04ad(1197) and TTL is 255. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram. The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value but the TTL field remains unchanged because the TTL for the first hop router is always the same.

## Part 4: UDP

No.	Time	Source	Destination	Protocol	Length	Info
94	3.353370	172.16.27.66	202.141.81.2	DNS	80	Standard query A jampui.iitg.ernet.in
95	3.353387	172.16.27.66	202.141.80.9	DNS	80	Standard query A jampui.iitg.ernet.in
96	3.353799	202.141.80.9	172.16.27.66	DNS	171	Standard query response A 202.141.80.21
97	3.353817	202.141.81.2	172.16.27.66	DNS	171	Standard query response A 202.141.80.21

▶ Frame 95: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)

▶ Ethernet II, Src: Pegatron\_b3:08:13 (38:60:77:b3:08:13), Dst: Cisco\_9d:70:00 (00:24:f9:9d:70:00)

▼ Internet Protocol Version 4, Src: 172.16.27.66 (172.16.27.66), Dst: 202.141.80.9 (202.141.80.9)

Version: 4

Header length: 20 bytes

▶ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

Total Length: 66

Identification: 0x0000 (0)

▶ Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

▶ Header checksum: 0x58c2 [correct]

Source: 172.16.27.66 (172.16.27.66)

Destination: 202.141.80.9 (202.141.80.9)

▼ User Datagram Protocol, Src Port: 16849 (16849), Dst Port: domain (53)

Source port: 16849 (16849)

Destination port: domain (53)

Length: 46

▼ Checksum: 0x372a [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

▶ Domain Name System (query)

0000 00 24 f9 9d 70 00 38 60 77 b3 08 13 08 00 45 00 .\$.p.8`w....E.

0010 00 42 00 00 40 00 40 11 58 c2 ac 10 1b 42 ca 8d .B..@. X....B..

0020 50 09 41 d1 00 35 00 2e 37 2a 36 a2 01 00 00 01 P.A..5.. 7\*6....

0030 00 00 00 00 00 00 06 6a 61 6d 70 75 69 04 69 69 .....j ampui.ii

0040 74 67 05 65 72 6e 65 74 02 69 6e 00 00 01 00 01 tg.ernet .in....

File: "/tmp/wireshark\_eth0\_20130..." Packets: 157 Displayed: 4 Marked: 0 Dropped: 0

No.	Time	Source	Destination	Protocol	Length	Info
94	3.353370	172.16.27.66	202.141.81.2	DNS	80	Standard query A jampui.iitg.ernet.in
95	3.353387	172.16.27.66	202.141.80.9	DNS	80	Standard query A jampui.iitg.ernet.in
96	3.353799	202.141.80.9	172.16.27.66	DNS	171	Standard query response A 202.141.80.21
97	3.353817	202.141.81.2	172.16.27.66	DNS	171	Standard query response A 202.141.80.21

▶ Frame 96: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits)

▶ Ethernet II, Src: Cisco\_9d:70:00 (00:24:f9:9d:70:00), Dst: Pegatron\_b3:08:13 (38:60:77:b3:08:13)

▼ Internet Protocol Version 4, Src: 202.141.80.9 (202.141.80.9), Dst: 172.16.27.66 (172.16.27.66)

Version: 4

Header length: 20 bytes

▶ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

Total Length: 157

Identification: 0xba2b (47659)

▶ Flags: 0x00

Fragment offset: 0

Time to live: 63

Protocol: UDP (17)

▶ Header checksum: 0xdf3b [correct]

Source: 202.141.80.9 (202.141.80.9)

Destination: 172.16.27.66 (172.16.27.66)

▼ User Datagram Protocol, Src Port: domain (53), Dst Port: 16849 (16849)

Source port: domain (53)

Destination port: 16849 (16849)

Length: 137

▼ Checksum: 0x2dd4 [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

▶ Domain Name System (response)

0000 38 60 77 b3 08 13 00 24 f9 9d 70 00 08 00 45 00 8`w...\$. .p...E.

0010 00 9d ba 2b 00 00 3f 11 df 3b ca 8d 50 09 ac 10 ...+..?. .;..P...

0020 1b 42 00 35 41 d1 00 89 2d d4 36 a2 85 00 00 01 .B.5A... -.6....

0030 00 01 00 02 00 02 06 6a 61 6d 70 75 69 04 69 69 .....j ampui.ii

0040 74 67 05 65 72 6e 65 74 02 69 6e 00 00 01 00 01 tg.ernet .in....

0050 c0 c0 0c 00 01 00 01 00 01 51 80 00 04 ca 8d 50 15 ..... Q....P.

0060 c0 13 00 02 00 01 00 01 51 80 00 0a 07 6e 61 61 ..... Q....naa

0070 6d 62 6f 72 c0 13 c0 13 00 02 00 01 00 01 51 80 mbor.....Q.

0080 00 09 06 6b 61 6d 72 75 70 c0 13 c0 58 00 01 00 ...kamru p...X...

File: "/tmp/wireshark\_eth0\_20130..." Packets: 157 Displayed: 4 Marked: 0 Dropped: 0

Answer 1: This contains 4 fields: Source Port, destination port, length, and checksum.

Answer 2:

The UDP has four fields of two bytes each so in total it is 8 bytes

Source Port = 2 bytes

Destination port = 2 bytes

Length = 2 bytes

Checksum = 2 bytes

Answer 3: Length of the UDP datagram = UDP header + The data length.

Answer 4: UDP protocol number in hex = 11 and in decimal = 17

Answer 5:

```
▼ User Datagram Protocol, Src Port: 16849 (16849), Dst Port: domain (53)
  Source port: 16849 (16849)
  Destination port: domain (53)
  Length: 46
▼ User Datagram Protocol, Src Port: domain (53), Dst Port: 16849 (16849)
  Source port: domain (53)
  Destination port: 16849 (16849)
  Length: 137
```

The source port number of the query packet is the destination port number of the response packet and the destination port number of the query packet is the source port number of the response packet.