

CS349 : Networks Lab

Report

Assignment 3: Wireshark

Anil Kag
10010111
a.kag@iitg.ernet.in

March 20, 2013

1 Basics

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Ans: Protocols which appear in the protocol column in the unfiltered packet-listing

- | | | |
|--------------|-----------|----------|
| (a) ARP | (e) ICMP | (i) SSDP |
| (b) DHCPv6 | (f) HTTP | (j) STP |
| (c) DNS | (g) LLC | (k) TCP |
| (d) Ethernet | (h) LLNMR | (l) UDP |

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

Ans: Packet details are as follows

no	time	source	destination	proto	len	info
310	17:00:18.753711	172.16.27.59	202.141.80.22	HTTP	867	GET http://www.google.co.in/ HTTP/1.1
391	17:00:18.903545	202.141.80.22	172.16.27.59	HTTP	66	HTTP/1.0 200 OK (text/html)

Time taken = $0.903545\text{sec} - 0.753711\text{sec} = 0.149834\text{sec}$

3. What is the Internet address of the www.google.com? What is the Internet address of your computer?

Ans: IP of google cannot be determined by looking at the above two packets because the proxy server(202.141.80.22) handles the connection part between my host & google.com. Firstly my machine tries to resolve the domain name “www.google.com” but the dns server fails in resolving the address & hence the packet is sent to the proxy server which then handles the connection for interacting with public addresses.

My host ip \Rightarrow 172.16.27.59 (can be seen in the src field in IP header in http get request)

2 Ethernet

Reference packets used for solving this part

no	time	source	destination	proto	len	info
113	17:47:02.684944	172.16.27.59	202.141.80.22	HTTP	668	GET http://www.faqs.org/rfcs/rfc826.html
391	17:47:03.771542	202.141.80.22	172.16.27.59	HTTP	3935	HTTP/1.1 HTTP/1.0 200 OK (text/html)

1. What is the 48-bit Ethernet address of your computer?

Ans: HTTP GET message's ethernet header

Ethernet II, Src: Pegatron_b3:05:c4 (38:60:77:b3:05:c4), Dst: Cisco_9d:70:00 (00:24:f9:9d:70:00)

Ethernet address of my computer Pegatron_b3:05:c4 (38:60:77:b3:05:c4) given by src field

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of the website with the RFC? What device has this as its Ethernet address?

Ans: Destination Ethernet address 00:24:f9:9d:70:00

It's not the ethernet address of the RFC website.

It's actually the ethernet address of the next hop for reaching the destination in my computer's routing table.

You can actually check the IP for the device having destination ethernet address as this by running 'arp -n' on your linux machine & check the IP corresponding to this ethernet address on my machine.

\$ arp -n

Address	HWtype	HWaddress	Flags	Mask	Iface
172.16.27.68	ether	f0:4d:a2:4f:15:6d	C		eth0
172.16.24.254	ether	00:24:f9:9d:70:00	C		eth0

⇒ it's ethernet address of 172.16.24.254

3. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

Ans: Type field value = 0x0800 ⇒ IP packet

There are no flags in the Ethernet II header.

4. How many bytes from the very start of the Ethernet frame does the ASCII G in GET appear in the Ethernet frame?

Ans: Ethernet Header Contents

```

0000  00 24 f9 9d 70 00 38 60 77 b3 05 c4 08 00 45 00  .$.p.8' w....E.
0010  02 8e 56 bd 40 00 40 06 ff bd ac 10 1b 3b ca 8d  ..V.@.@. ....;..
0020  50 16 c9 6a 0c 38 94 40 d2 f1 66 42 57 69 80 18  P..j.8.@ ..fBWi..
0030  00 e5 28 7f 00 00 01 01 08 0a 00 9e 84 4b 15 b1  ..(..... ....K..
0040  50 ee 47 45 54 20 68 74 74 70 3a 2f 2f 77 77 77  P.GET ht tp://www

```

ASCII letter 'G' starts on line 5 with base 0x0040 & offset 0x0003

Ethernet Header size = 14bytes & IP Header size = 20bytes & TCP Header Size = 32bytes (in my case 12bytes extra is covered by options field)

⇒ position (in bytes) from the start of Ethernet Frame = 4 * 16 + 3 = 67 (0x0010 = 16 in decimal)

i.e. G comes after 14 + 20 + 32 = 66 bytes in the packet

5. What is the value of the Ethernet source address? Is this the address of your computer, or of the destination website? What device has this as its Ethernet address?

Ans: HTTP Response

Ethernet II, Src: Cisco_9d:70:00 (00:24:f9:9d:70:00), Dst: Pegatron_b3:05:c4 (38:60:77:b3:05:c4)

src = 00:24:f9:9d:70:00 ⇒ hop just before my computer in the path from website to my computer

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Ans: dst = 38:60:77:b3:05:c4 \Rightarrow my computer (you can verify via ifconfig & look at the hwaddress for the eth0 interface)

```
$ ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 38:60:77:b3:05:c4
          inet addr:172.16.27.59  Bcast:172.16.27.255  Mask:255.255.252.0
          inet6 addr: fe80::3a60:77ff:feb3:5c4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8008125  errors:0  dropped:4342  overruns:0  frame:0
          TX packets:173669  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1129843477 (1.1 GB)  TX bytes:20988447 (20.9 MB)
          Interrupt:43 Base address:0xe000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:21789  errors:0  dropped:0  overruns:0  frame:0
          TX packets:21789  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1986523 (1.9 MB)  TX bytes:1986523 (1.9 MB)
```

7. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

Ans: Type field == 0x0800 \Rightarrow IP

There are no flags in the Ethernet II header.

3 IP

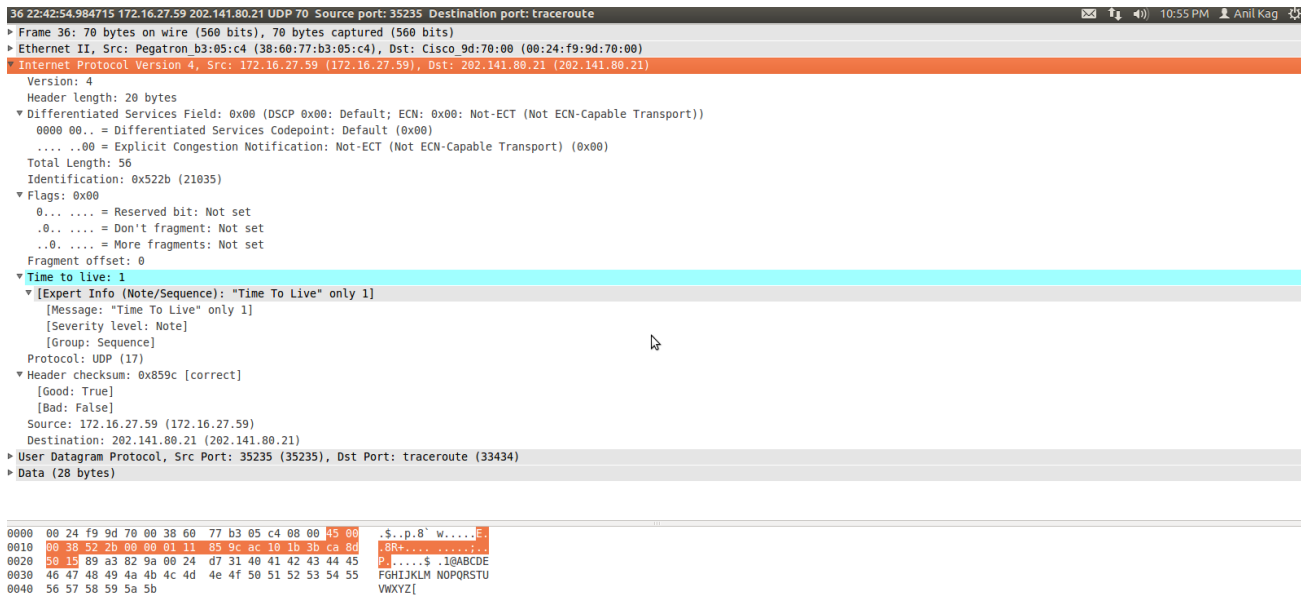


Figure 1: IP Header

1. What is the IP address of your computer?

Ans: Internet Protocol Version 4, Src: 172.16.27.59 (172.16.27.59), Dst: 202.141.80.21 (202.141.80.21)
⇒ IP of my computer = 172.16.27.59

2. Within the IP packet header, what is the value in the upper layer protocol field?

Ans: Protocol: UDP (17)

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Ans: Internet Header Length = 20bytes
(if only looking at packet, value given in IHLen is 5 ⇒ 5 * 32 bits = 5 * 4bytes = 20 bytes)

Total Length = 56bytes = Header Length + IP Payload Length
⇒ IP Payload Length = 56bytes - 20bytes = 36bytes
(as Header length = 20bytes)

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Ans: Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Since fragment offset is 0 & no more fragments are going to come (more bit not set)
⇒ no fragmentation

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

Ans: Identification & Checksum always change while going from one packet to other

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Ans: Fields which stay constant are Version, Header Length, Differentiated Services, Protocol, Src & Dest IP.

The field stated above must remain constant, because, version is 4 due to IPv4 & hence length also is fixed. Also the protocol field = UDP(17).

Field which must change are identification & checksum (these two may also change depending on certain conditions).

Identification field uniquely identifies a packet & hence should be unique except for the case of fragmentation.

7. What is the value in the Identification field and the TTL field? Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

Ans:

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
49	22:42:54.984856	172.16.27.59	202.141.80.21	UDP	70	Yes	Source port: 33110 Destination port: 33447
50	22:42:54.984866	172.16.27.59	202.141.80.21	UDP	70	Yes	Source port: 36381 Destination port: 33448
51	22:42:54.984876	172.16.27.59	202.141.80.21	UDP	70	Yes	Source port: 58136 Destination port: 33449
52	22:42:54.984941	202.141.80.21	172.16.27.59	ICMP	90	Yes	Destination unreachable (Host administratively prohibited)
53	22:42:54.984953	202.141.80.21	172.16.27.59	ICMP	90	Yes	Destination unreachable (Host administratively prohibited)
54	22:42:54.984957	202.141.80.21	172.16.27.59	ICMP	90	Yes	Destination unreachable (Host administratively prohibited)
55	22:42:54.984967	202.141.80.21	172.16.27.59	ICMP	90	Yes	Destination unreachable (Host administratively prohibited)
56	22:42:54.984970	202.141.80.21	172.16.27.59	ICMP	90	Yes	Destination unreachable (Host administratively prohibited)
57	22:42:54.984981	202.141.80.21	172.16.27.59	ICMP	90	Yes	Destination unreachable (Host administratively prohibited)
58	22:42:54.985012	172.16.24.254	172.16.27.59	ICMP	70	Yes	Time-to-live exceeded (Time to live exceeded in transit)
59	22:42:54.985085	172.16.24.254	172.16.27.59	ICMP	70	Yes	Time-to-live exceeded (Time to live exceeded in transit)
60	22:42:54.985152	172.16.24.254	172.16.27.59	ICMP	70	Yes	Time-to-live exceeded (Time to live exceeded in transit)
61	22:42:54.985165	172.16.27.59	202.141.81.2	DNS	86	Yes	Standard query PTR 254.24.16.172.in-addr.arpa

Frame 58: 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 b3:05:c4 (38:60:77:b3:05:c4)
 Internet Protocol Version 4, Src: 172.16.24.254 (172.16.24.254), Dst: 172.16.27.59 (172.16.27.59)
 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: 0x2fb0 (12208)
 Flags: 0x00
 Fragment offset: 0
 Time to live: 255
 Protocol: ICMP (1)
 Header checksum: 0xfefa [correct]
 Source: 172.16.24.254 (172.16.24.254)
 Destination: 172.16.27.59 (172.16.27.59)
 Internet Control Message Protocol

```

0000  38 60 77 b3 05 c4 00 24 f9 9d 70 00 00 45 c0  8'w...$ ..p...E.
0010  00 38 2f b0 00 00 ff 01 fe fa ac 10 1b fe ac 10  .8/.....
0020  1b 3b 0b 00 11 6c 00 00 00 00 45 00 00 38 52 2b  -?...L...E..BR+
0030  00 00 01 11 85 9c ac 10 1b 3b ca 8d 50 15 89 a3  .....;...P...
0040  82 9a 00 24 d7 31  ....$.1
  
```

Figure 2: TTL Value & Id Field

For the current packet (figure 2)

Identification: *0x2fb0*(12208)

Time to live: 255

Yes, the TTL values in all these messages remains the same but the identification value changes. Since the TTL-Exceeded replies are sent by the nearest router (first hop), the TTL values will be set to maximum of that field which means that it'll be 256 because the TTL field is 8bits long. No other router exists in between my computer & first hop router & hence no one can reduce the TTL value.

4 UDP

part4-total-capture [Wireshark 1.6.7]

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
39	23:43:44.573062	172.16.27.59	202.141.80.9	DNS	80	Yes	Standard query response, Server failure
40	23:43:44.573070	172.16.27.59	202.141.81.2	DNS	80	Yes	Standard query A jampui.iitg.ernet.in
41	23:43:44.573676	202.141.81.2	172.16.27.59	DNS	171	Yes	Standard query response A 202.141.80.21
42	23:43:44.573688	202.141.80.9	172.16.27.59	DNS	171	Yes	Standard query response A 202.141.80.21
16	23:43:43.976428	172.16.27.63	255.255.255.255	ICMP	60	Yes	Echo (ping) request id=0x0001, seq=21660/40020, ttl=255
6	23:43:43.278129	fe80::1c15:55fe:3af4::ff02::1:ff47:d0c6		ICMPv6	86	Yes	Neighbor Solicitation for fe80::b1de:d39:5447:d0c6 from e0:cb:4e:07:c8:29
4	23:43:43.219248	fe80::b485:1e60:c955::ff02::1:3		LLMNR	84	Yes	Standard query A wpad
5	23:43:43.219580	172.16.26.221	224.0.0.252	LLMNR	64	Yes	Standard query A wpad
7	23:43:43.319694	fe80::b485:1e60:c955::ff02::1:3		LLMNR	84	Yes	Standard query A wpad

Frame 39: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)

Ethernet II, Src: Pegatron b3:05:c4 (38:60:77:b3:05:c4), Dst: Cisco 9d:70:00 (00:24:f9:9d:70:00)

Internet Protocol Version 4, Src: 172.16.27.59 (172.16.27.59), 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: 0x58c9 [correct]

Source: 172.16.27.59 (172.16.27.59)

Destination: 202.141.80.9 (202.141.80.9)

User Datagram Protocol, Src Port: 56060 (56060), Dst Port: domain (53)

Source port: 56060 (56060)

Destination port: domain (53)

Length: 46

Checksum: 0xb86f [validation disabled]

Domain Name System (query)

0000 00 24 f9 9d 70 00 38 60 77 b3 05 c4 08 00 45 00 .\$.p.8`W....E.
0010 00 42 00 00 40 00 40 58 c9 ac 10 1b 3b ca 8d .B.@.X.....
0020 50 09 da fc 00 35 00 2e b8 6f 1c 38 01 00 00 01 P....5...o.8...
0030 00 00 00 00 00 00 06 6a 61 6d 70 75 69 04 69 69j ampui.i
0040 74 67 05 65 72 6e 65 74 02 69 6e 00 00 01 00 01 tg.ernet .in.....

Normal mode

Line: 406 Col: 4 INS LINE

Figure 3: UDP Header

part4-total-capture [Wireshark 1.6.7]

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
39	23:43:44.573062	172.16.27.59	202.141.80.9	DNS	80	Yes	Standard query response, Server failure
40	23:43:44.573070	172.16.27.59	202.141.81.2	DNS	80	Yes	Standard query A jampui.iitg.ernet.in
41	23:43:44.573676	202.141.81.2	172.16.27.59	DNS	171	Yes	Standard query response A 202.141.80.21
42	23:43:44.573688	202.141.80.9	172.16.27.59	DNS	171	Yes	Standard query response A 202.141.80.21
16	23:43:43.976428	172.16.27.63	255.255.255.255	ICMP	60	Yes	Echo (ping) request id=0x0001, seq=21660/40020, ttl=255
6	23:43:43.278129	fe80::1c15:55fe:3af4::ff02::1:ff47:d0c6		ICMPv6	86	Yes	Neighbor Solicitation for fe80::b1de:d39:5447:d0c6 from e0:cb:4e:07:c8:29
4	23:43:43.219248	fe80::b485:1e60:c955::ff02::1:3		LLMNR	84	Yes	Standard query A wpad
5	23:43:43.219580	172.16.26.221	224.0.0.252	LLMNR	64	Yes	Standard query A wpad
7	23:43:43.319694	fe80::b485:1e60:c955::ff02::1:3		LLMNR	84	Yes	Standard query A wpad

Frame 39: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)

Ethernet II, Src: Pegatron b3:05:c4 (38:60:77:b3:05:c4), Dst: Cisco 9d:70:00 (00:24:f9:9d:70:00)

Internet Protocol Version 4, Src: 172.16.27.59 (172.16.27.59), 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: 0x58c9 [correct]

Source: 172.16.27.59 (172.16.27.59)

Destination: 202.141.80.9 (202.141.80.9)

User Datagram Protocol, Src Port: 56060 (56060), Dst Port: domain (53)

Source port: 56060 (56060)

Destination port: domain (53)

Length: 46

Checksum: 0xb86f [validation disabled]

Domain Name System (query)

0000 00 24 f9 9d 70 00 38 60 77 b3 05 c4 08 00 45 00 .\$.p.8`W....E.
0010 00 42 00 00 40 00 40 58 c9 ac 10 1b 3b ca 8d .B.@.X.....
0020 50 09 da fc 00 35 00 2e b8 6f 1c 38 01 00 00 01 P....5...o.8...
0030 00 00 00 00 00 00 06 6a 61 6d 70 75 69 04 69 69j ampui.i
0040 74 67 05 65 72 6e 65 74 02 69 6e 00 00 01 00 01 tg.ernet .in.....

Normal mode

Line: 406 Col: 4 INS LINE

Figure 4: UDP+IP Header

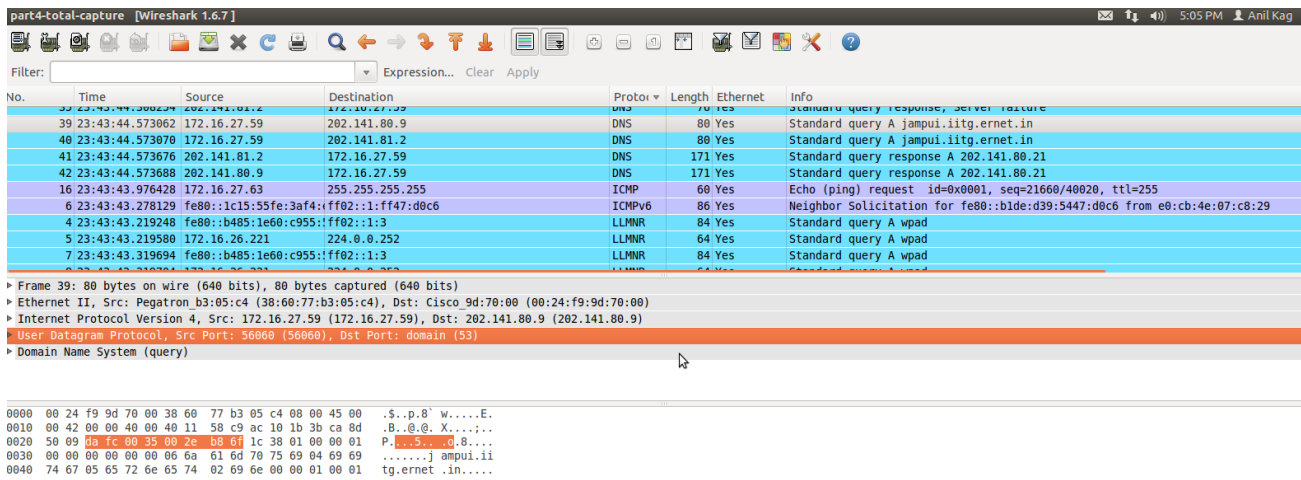


Figure 5: UDP Header marked

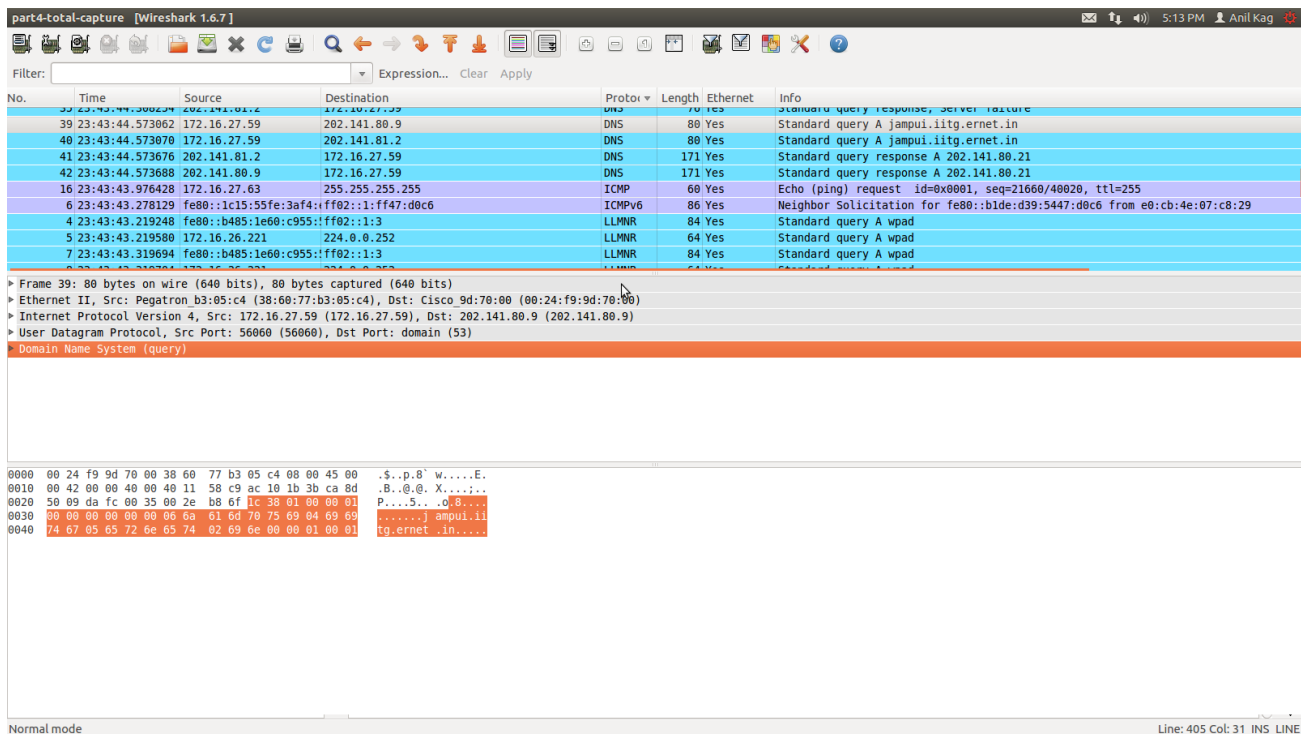


Figure 6: UDP Payload Marked

1. Select one packet. From this packet, determine how many fields there are in the UDP header. Name these fields.

Ans: Fields in the UDP header are as follows (can be seen in the UDP section of the packet):

- (a) source port
- (b) destination port
- (c) length
- (d) checksum

2. From the packet content field, determine the length (in bytes) of each of the UDP header fields.

Ans: Each Field in the UDP Header is 2bytes(16 bits) long \Rightarrow total udp header length = 8bytes

3. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

Ans: Select the DNS query portion & it expands over 46bytes which is equal to the length given in the UDP packet

⇒ length in UDP packet refers to the payload length along with the UDP header length.

UDP Header length 8bytes. *See figure 5*

Payload length is $2 * 16\text{bytes}$ (in last 2 rows) + 6bytes (in 3rd last row) = 38bytes . *See figure 6*

4. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.

Ans: Protocol Number = 17(decimal), 0x11(hexadecimal). *See figure 4*

5. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.

Ans: Packet details at UDP Header

Request	User Datagram Protocol, Src Port: 56060 (56060), Dst Port: domain (53)
Response	User Datagram Protocol, Src Port: domain (53), Dst Port: 56060 (56060)

Source port in one becomes the destination in other & vice-versa