COMPUTER NETWORKS LAB

NAME:	ARITRA DATTA
ROLL NO:	002010501054
CLASS:	BCSE – III
GROUP:	A2
ASSIGNMENT:	5
DEADLINE:	13th October, 2022

Problem Statement: Install Wireshark in the local machine and capture and analyse various packets according to the given questions.

Date of Submission: 10th November, 2022

QUESTION 1

Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighbouring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.

We first get the IP Address of neighbouring router using the **ipconfig** command.

```
C:\Users\Aritra Datta>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:1c01:745c:2e0d:2f8f:ad9d:74bd
   Temporary IPv6 Address. . . . . . : 2401:4900:1c01:745c:bdf6:337b:89de:dff9
   Link-local IPv6 Address . . . . . : fe80::83a1:64fe:ccd0:133b%14
   IPv4 Address. . . . . . . . . . . : 192.168.1.7
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%14
                                       192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

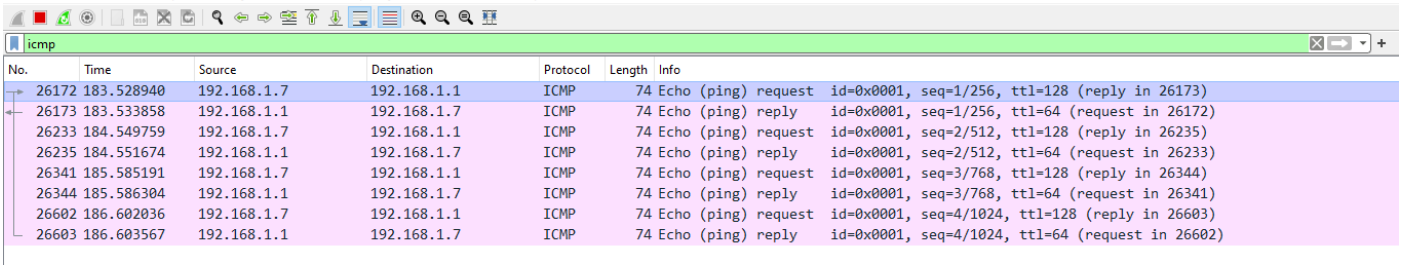
The router is then pinged using the **ping** command

```
C:\Users\Aritra Datta>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Aritra Datta>
```



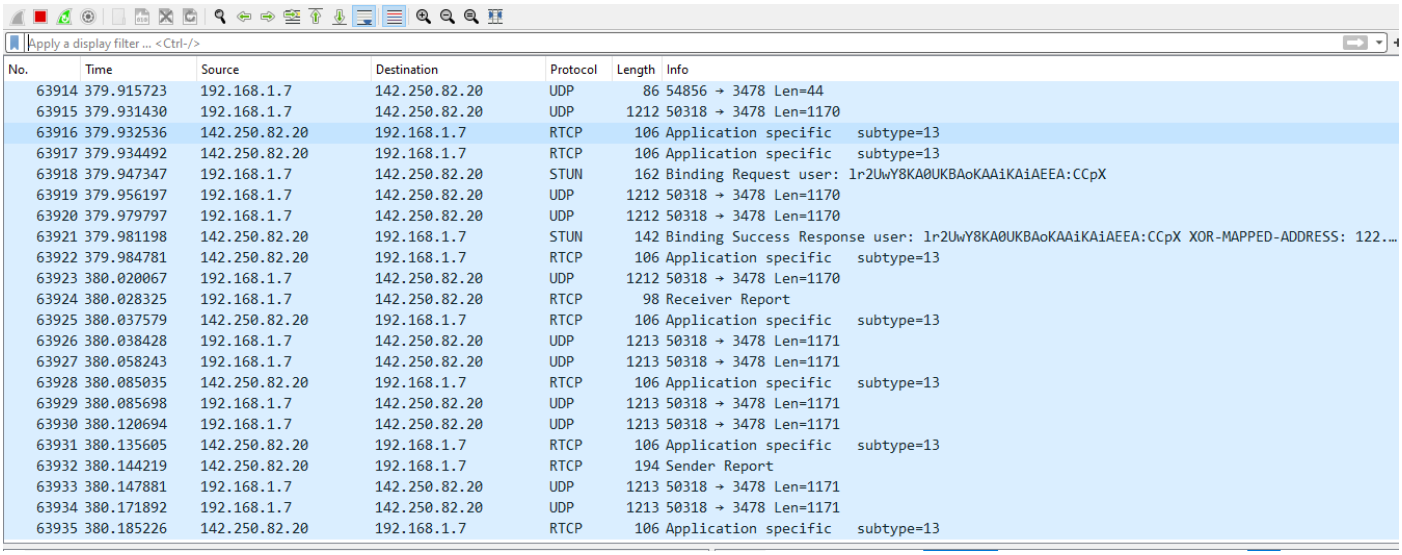
icmp

No.	Time	Source	Destination	Protocol	Length	Info
26172	183.528940	192.168.1.7	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 26173)
26173	183.533858	192.168.1.1	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 26172)
26233	184.549759	192.168.1.7	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 26235)
26235	184.551674	192.168.1.1	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 26233)
26341	185.585191	192.168.1.7	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 26344)
26344	185.586304	192.168.1.1	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 26341)
26602	186.602036	192.168.1.7	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 26603)
26603	186.603567	192.168.1.1	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 26602)

QUESTION 2

Generate some web traffic and

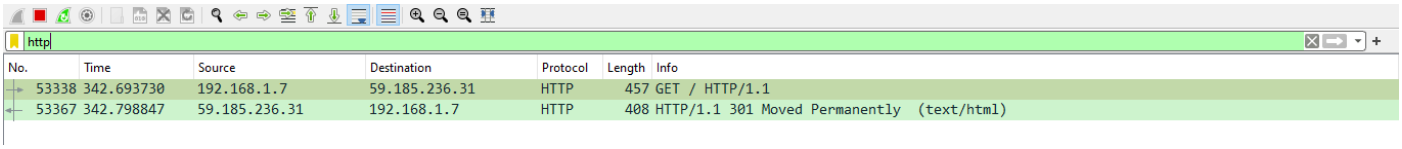
a) find the list the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
63914	379.915723	192.168.1.7	142.250.82.20	UDP	86	54856 → 3478 Len=44
63915	379.931430	192.168.1.7	142.250.82.20	UDP	1212	50318 → 3478 Len=1170
63916	379.932536	142.250.82.20	192.168.1.7	RTCP	106	Application specific subtype=13
63917	379.934492	142.250.82.20	192.168.1.7	RTCP	106	Application specific subtype=13
63918	379.947347	192.168.1.7	142.250.82.20	STUN	162	Binding Request user: lr2UwY8KA0UKBAoKAAiKAiAEEA:CCpX
63919	379.956197	192.168.1.7	142.250.82.20	UDP	1212	50318 → 3478 Len=1170
63920	379.979797	192.168.1.7	142.250.82.20	UDP	1212	50318 → 3478 Len=1170
63921	379.981198	142.250.82.20	192.168.1.7	STUN	142	Binding Success Response user: lr2UwY8KA0UKBAoKAAiKAiAEEA:CCpX XOR-MAPPED-ADDRESS: 122.…
63922	379.984781	142.250.82.20	192.168.1.7	RTCP	106	Application specific subtype=13
63923	380.020067	192.168.1.7	142.250.82.20	UDP	1212	50318 → 3478 Len=1170
63924	380.028325	192.168.1.7	142.250.82.20	RTCP	98	Receiver Report
63925	380.037579	142.250.82.20	192.168.1.7	RTCP	106	Application specific subtype=13
63926	380.038428	192.168.1.7	142.250.82.20	UDP	1213	50318 → 3478 Len=1171
63927	380.058243	192.168.1.7	142.250.82.20	UDP	1213	50318 → 3478 Len=1171
63928	380.085035	142.250.82.20	192.168.1.7	RTCP	106	Application specific subtype=13
63929	380.085698	192.168.1.7	142.250.82.20	UDP	1213	50318 → 3478 Len=1171
63930	380.120694	192.168.1.7	142.250.82.20	UDP	1213	50318 → 3478 Len=1171
63931	380.135605	142.250.82.20	192.168.1.7	RTCP	106	Application specific subtype=13
63932	380.144219	142.250.82.20	192.168.1.7	RTCP	194	Sender Report
63933	380.147881	192.168.1.7	142.250.82.20	UDP	1213	50318 → 3478 Len=1171
63934	380.171892	192.168.1.7	142.250.82.20	UDP	1213	50318 → 3478 Len=1171
63935	380.185226	142.250.82.20	192.168.1.7	RTCP	106	Application specific subtype=13

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



http

No.	Time	Source	Destination	Protocol	Length	Info
53338	342.693730	192.168.1.7	59.185.236.31	HTTP	457	GET / HTTP/1.1
53367	342.798847	59.185.236.31	192.168.1.7	HTTP	408	HTTP/1.1 301 Moved Permanently (text/html)

The HTTP GET / request was sent at 342.693730 seconds and the HTTP OK message was received at 342.798847 seconds. Time taken = **105.110 ms**.

c) What is the Internet address of the website? What is the Internet address of your computer?

As seen in the above screenshot, the address of the website is **59.185.236.31** and the address of my computer is **192.168.1.7**.

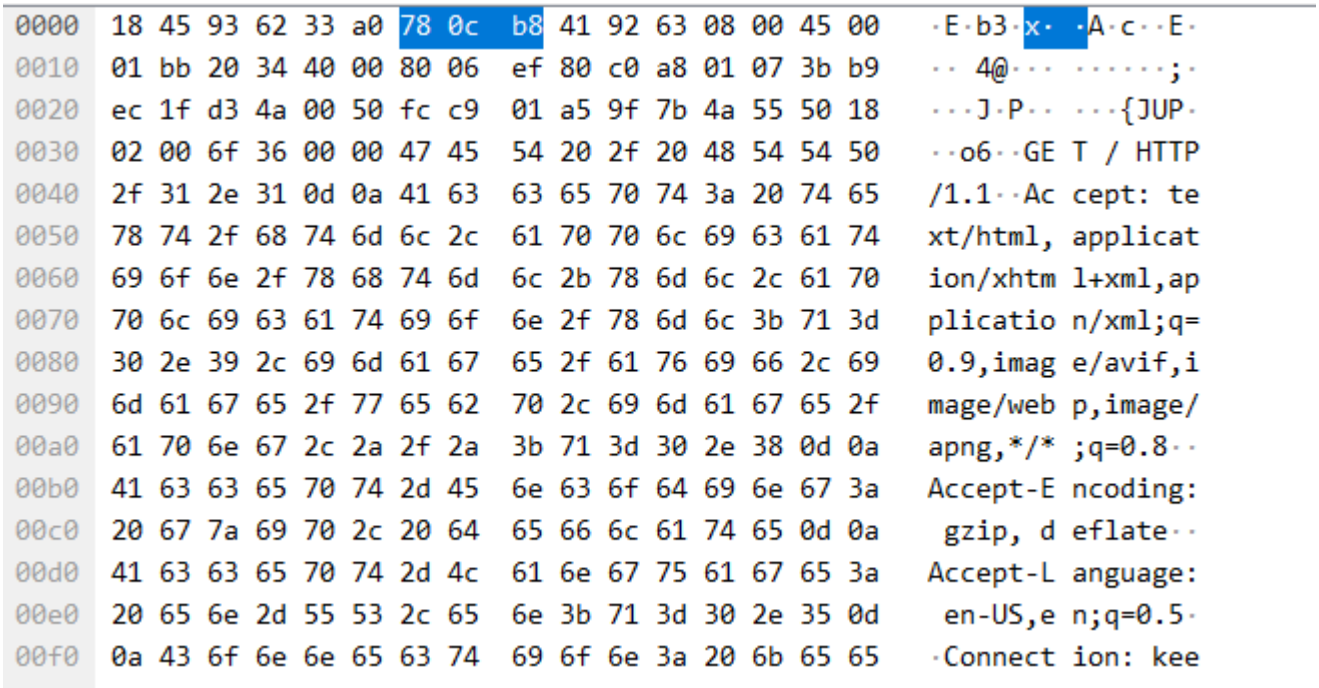
d) Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.

e) Find out the value of the Host from the Packet Details Panel, within the GET command.

As can be seen in the above screenshot, the host is **www.barc.gov.in\r\n**.

QUESTION 3

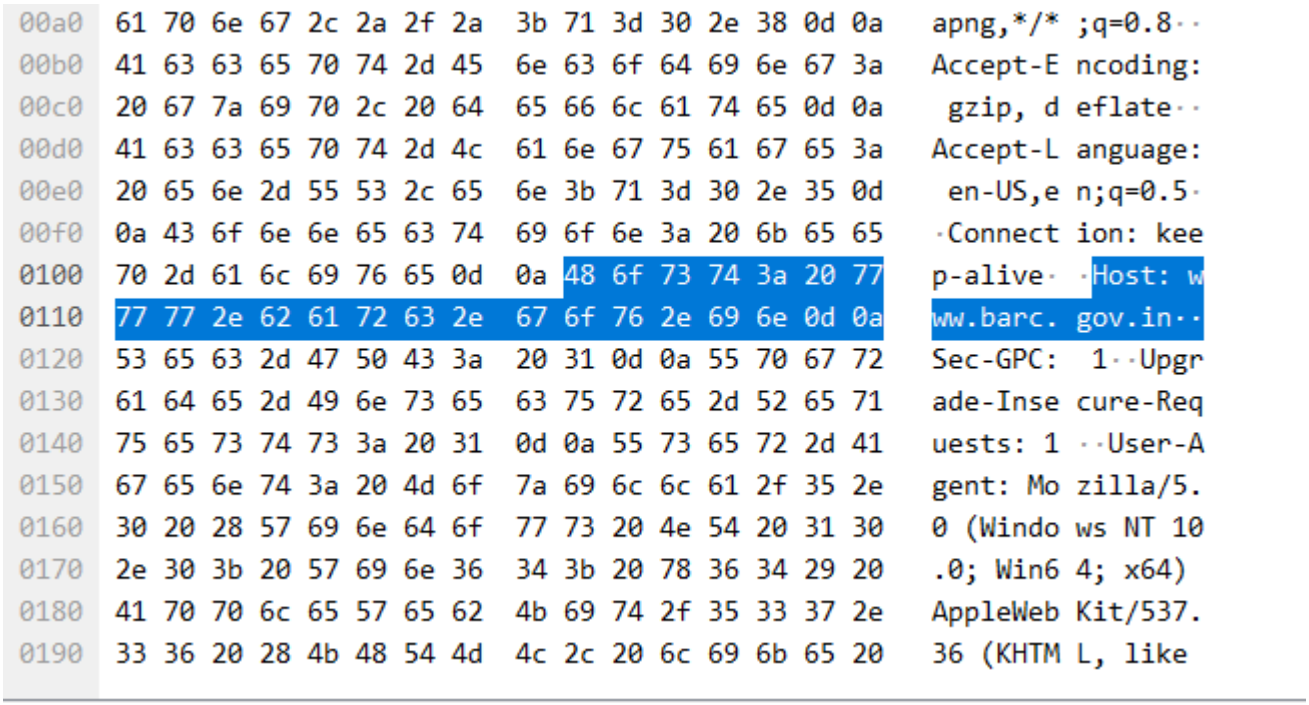
Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.



The left part is the hexadecimal representation of the packet, while the right side is the ASCII representation.

QUESTION 4

Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.



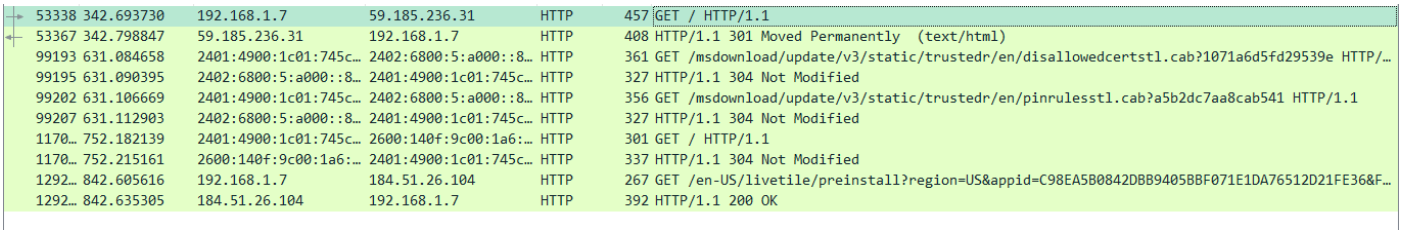
```
00a0  61 70 6e 67 2c 2a 2f 2a  3b 71 3d 30 2e 38 0d 0a   apng,*/* ;q=0.8··
00b0  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 3a   Accept-E ncoding:
00c0  20 67 7a 69 70 2c 20 64  65 66 6c 61 74 65 0d 0a    gzip, d eflate··
00d0  41 63 63 65 70 74 2d 4c  61 6e 67 75 61 67 65 3a   Accept-L anguage:
00e0  20 65 6e 2d 55 53 2c 65  6e 3b 71 3d 30 2e 35 0d    en-US,e n;q=0.5·
00f0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65   ·Connect ion: kee
0100  70 2d 61 6c 69 76 65 0d  0a 48 6f 73 74 3a 20 77   p-alive· ·Host: w
0110  77 77 2e 62 61 72 63 2e  67 6f 76 2e 69 6e 0d 0a   ww.barc. gov.in··
0120  53 65 63 2d 47 50 43 3a  20 31 0d 0a 55 70 67 72   Sec-GPC:  1··Upgr
0130  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse cure-Req
0140  75 65 73 74 73 3a 20 31  0d 0a 55 73 65 72 2d 41   uests: 1 ··User-A
0150  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
0160  30 20 28 57 69 6e 64 6f  77 73 20 4e 54 20 31 30   0 (Windo ws NT 10
0170  2e 30 3b 20 57 69 6e 36  34 3b 20 78 36 34 29 20   .0; Win6 4; x64)
0180  41 70 70 6c 65 57 65 62  4b 69 74 2f 35 33 37 2e   AppleWeb Kit/537.
0190  33 36 20 28 4b 48 54 4d  4c 2c 20 6c 69 6b 65 20   36 (KHTM L, like
```

The first 4 bytes (in hexadecimal) are **48 6f 73 74**.

QUESTION 5

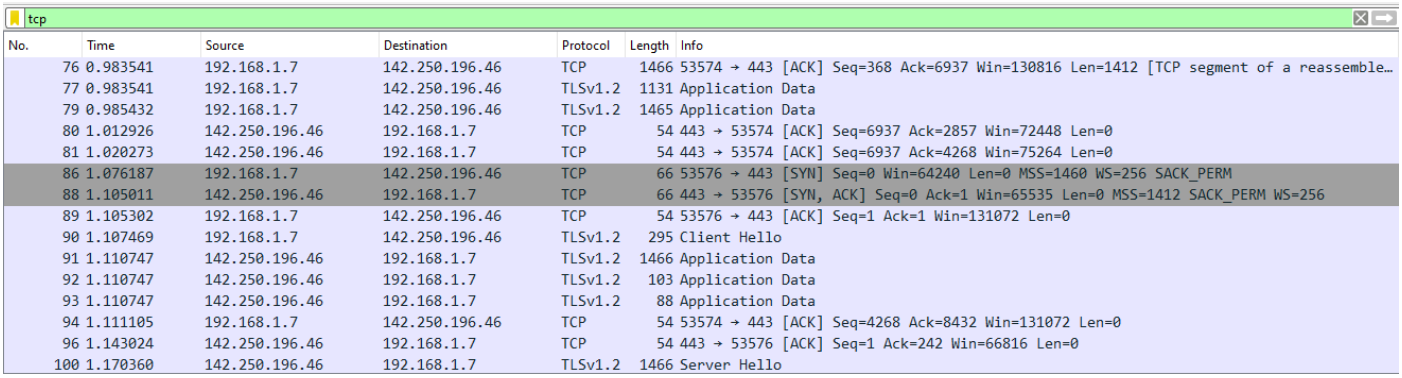
Filter packets with http, TCP, DNS and other protocols. Find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button click on follow.

HTTP



→	53338	342.693730	192.168.1.7	59.185.236.31	HTTP	457 GET / HTTP/1.1
←	53367	342.798847	59.185.236.31	192.168.1.7	HTTP	408 HTTP/1.1 301 Moved Permanently (text/html)
	99193	631.084658	2401:4900:1c01:745c…	2402:6800:5:a000::8…	HTTP	361 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1071a6d5fd29539e HTTP/…
	99195	631.090395	2402:6800:5:a000::8…	2401:4900:1c01:745c…	HTTP	327 HTTP/1.1 304 Not Modified
	99202	631.106669	2401:4900:1c01:745c…	2402:6800:5:a000::8…	HTTP	356 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?a5b2dc7aa8cab541 HTTP/1.1
	99207	631.112903	2402:6800:5:a000::8…	2401:4900:1c01:745c…	HTTP	327 HTTP/1.1 304 Not Modified
	1170…	752.182139	2401:4900:1c01:745c…	2600:140f:9c00:1a6:…	HTTP	301 GET / HTTP/1.1
	1170…	752.215161	2600:140f:9c00:1a6:…	2401:4900:1c01:745c…	HTTP	337 HTTP/1.1 304 Not Modified
	1292…	842.605616	192.168.1.7	184.51.26.104	HTTP	267 GET /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&F…
	1292…	842.635305	184.51.26.104	192.168.1.7	HTTP	392 HTTP/1.1 200 OK

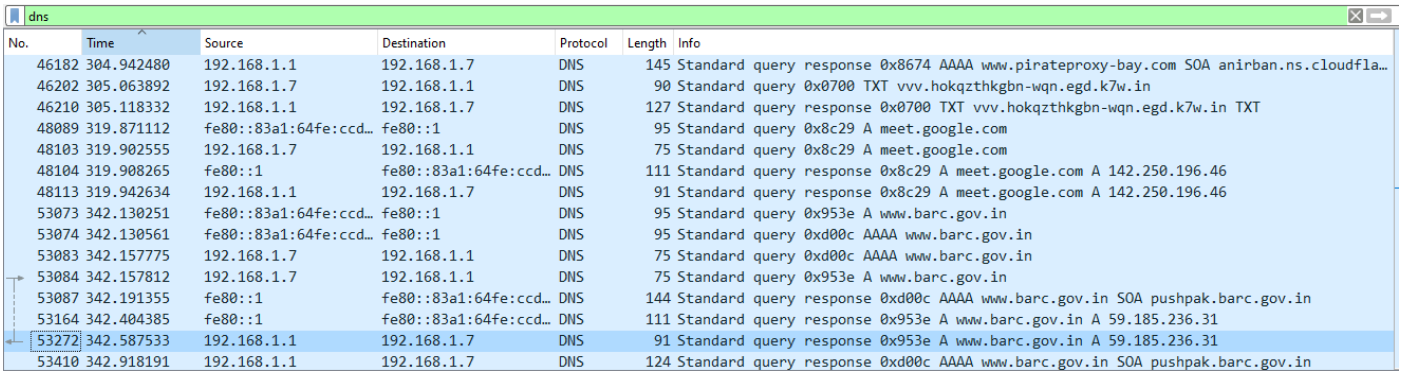
TCP



tcp

No.	Time	Source	Destination	Protocol	Length	Info
76	0.983541	192.168.1.7	142.250.196.46	TCP	1466	53574 → 443 [ACK] Seq=368 Ack=6937 Win=130816 Len=1412 [TCP segment of a reassemble…
77	0.983541	192.168.1.7	142.250.196.46	TLSv1.2	1131	Application Data
79	0.985432	192.168.1.7	142.250.196.46	TLSv1.2	1465	Application Data
80	1.012926	142.250.196.46	192.168.1.7	TCP	54	443 → 53574 [ACK] Seq=6937 Ack=2857 Win=72448 Len=0
81	1.020273	142.250.196.46	192.168.1.7	TCP	54	443 → 53574 [ACK] Seq=6937 Ack=4268 Win=75264 Len=0
86	1.076187	192.168.1.7	142.250.196.46	TCP	66	53576 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
88	1.105011	142.250.196.46	192.168.1.7	TCP	66	443 → 53576 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
89	1.105302	192.168.1.7	142.250.196.46	TCP	54	53576 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
90	1.107469	192.168.1.7	142.250.196.46	TLSv1.2	295	Client Hello
91	1.110747	142.250.196.46	192.168.1.7	TLSv1.2	1466	Application Data
92	1.110747	142.250.196.46	192.168.1.7	TLSv1.2	103	Application Data
93	1.110747	142.250.196.46	192.168.1.7	TLSv1.2	88	Application Data
94	1.111105	192.168.1.7	142.250.196.46	TCP	54	53574 → 443 [ACK] Seq=4268 Ack=8432 Win=131072 Len=0
96	1.143024	142.250.196.46	192.168.1.7	TCP	54	443 → 53576 [ACK] Seq=1 Ack=242 Win=66816 Len=0
100	1.170360	142.250.196.46	192.168.1.7	TLSv1.2	1466	Server Hello

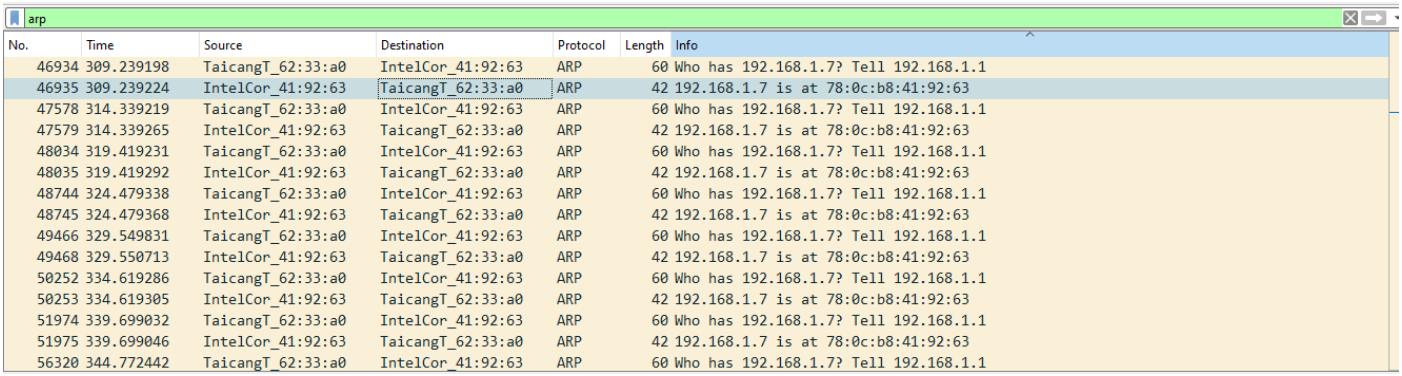
DNS



dns

No.	Time	Source	Destination	Protocol	Length	Info
46182	304.942480	192.168.1.1	192.168.1.7	DNS	145	Standard query response 0x8674 AAAA www.pirateproxy-bay.com SOA anirban.ns.cloudfla…
46202	305.063892	192.168.1.7	192.168.1.1	DNS	90	Standard query 0x0700 TXT vvv.hokqzthkgbn-wqn.egd.k7w.in
46210	305.118332	192.168.1.1	192.168.1.7	DNS	127	Standard query response 0x0700 TXT vvv.hokqzthkgbn-wqn.egd.k7w.in TXT
48089	319.871112	fe80::83a1:64fe:ccd…	fe80::1	DNS	95	Standard query 0x8c29 A meet.google.com
48103	319.902555	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x8c29 A meet.google.com
48104	319.908265	fe80::1	fe80::83a1:64fe:ccd…	DNS	111	Standard query response 0x8c29 A meet.google.com A 142.250.196.46
48113	319.942634	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0x8c29 A meet.google.com A 142.250.196.46
53073	342.130251	fe80::83a1:64fe:ccd…	fe80::1	DNS	95	Standard query 0x953e A www.barc.gov.in
53074	342.130561	fe80::83a1:64fe:ccd…	fe80::1	DNS	95	Standard query 0xd00c AAAA www.barc.gov.in
53083	342.157775	192.168.1.7	192.168.1.1	DNS	75	Standard query 0xd00c AAAA www.barc.gov.in
53084	342.157812	192.168.1.7	192.168.1.1	DNS	75	Standard query 0x953e A www.barc.gov.in
53087	342.191355	fe80::1	fe80::83a1:64fe:ccd…	DNS	144	Standard query response 0xd00c AAAA www.barc.gov.in SOA pushpak.barc.gov.in
53164	342.404385	fe80::1	fe80::83a1:64fe:ccd…	DNS	111	Standard query response 0x953e A www.barc.gov.in A 59.185.236.31
53272	342.587533	192.168.1.1	192.168.1.7	DNS	91	Standard query response 0x953e A www.barc.gov.in A 59.185.236.31
53410	342.918191	192.168.1.1	192.168.1.7	DNS	124	Standard query response 0xd00c AAAA www.barc.gov.in SOA pushpak.barc.gov.in

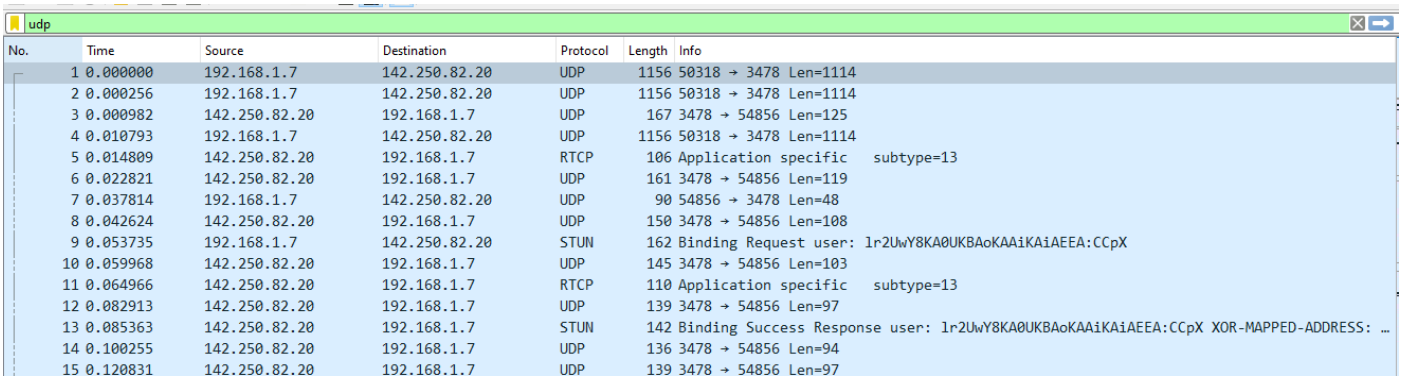
ARP



arp

No.	Time	Source	Destination	Protocol	Length	Info
46934	309.239198	TaicangT_62:33:a0	IntelCor_41:92:63	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1
46935	309.239224	IntelCor_41:92:63	TaicangT_62:33:a0	ARP	42	192.168.1.7 is at 78:0c:b8:41:92:63
47578	314.339219	TaicangT_62:33:a0	IntelCor_41:92:63	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1
47579	314.339265	IntelCor_41:92:63	TaicangT_62:33:a0	ARP	42	192.168.1.7 is at 78:0c:b8:41:92:63
48034	319.419231	TaicangT_62:33:a0	IntelCor_41:92:63	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1
48035	319.419292	IntelCor_41:92:63	TaicangT_62:33:a0	ARP	42	192.168.1.7 is at 78:0c:b8:41:92:63
48744	324.479338	TaicangT_62:33:a0	IntelCor_41:92:63	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1
48745	324.479368	IntelCor_41:92:63	TaicangT_62:33:a0	ARP	42	192.168.1.7 is at 78:0c:b8:41:92:63
49466	329.549831	TaicangT_62:33:a0	IntelCor_41:92:63	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1
49468	329.550713	IntelCor_41:92:63	TaicangT_62:33:a0	ARP	42	192.168.1.7 is at 78:0c:b8:41:92:63
50252	334.619286	TaicangT_62:33:a0	IntelCor_41:92:63	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1
50253	334.619305	IntelCor_41:92:63	TaicangT_62:33:a0	ARP	42	192.168.1.7 is at 78:0c:b8:41:92:63
51974	339.699032	TaicangT_62:33:a0	IntelCor_41:92:63	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1
51975	339.699046	IntelCor_41:92:63	TaicangT_62:33:a0	ARP	42	192.168.1.7 is at 78:0c:b8:41:92:63
56320	344.772442	TaicangT_62:33:a0	IntelCor_41:92:63	ARP	60	Who has 192.168.1.7? Tell 192.168.1.1

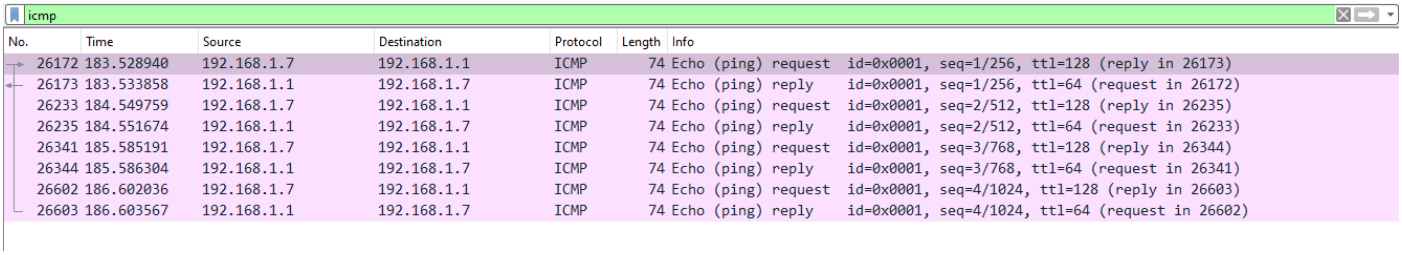
UDP



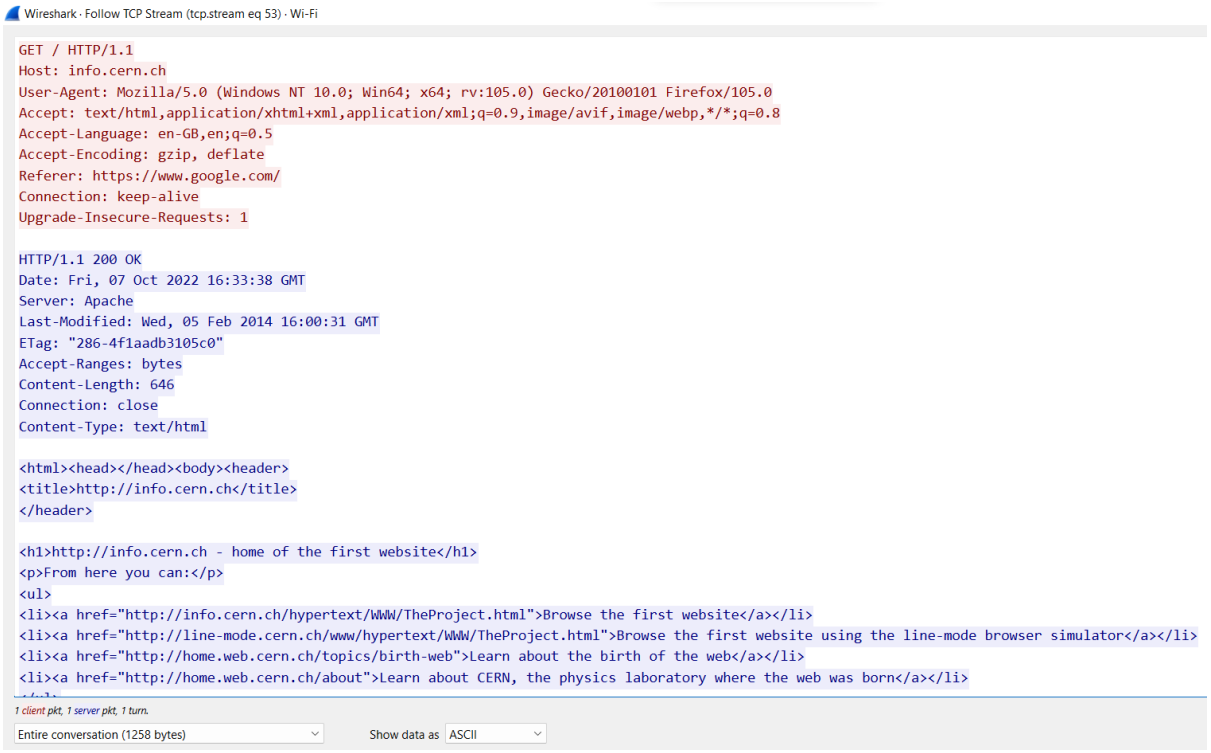
udp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.7	142.250.82.20	UDP	1156	50318 → 3478 Len=1114
2	0.000256	192.168.1.7	142.250.82.20	UDP	1156	50318 → 3478 Len=1114
3	0.000982	142.250.82.20	192.168.1.7	UDP	167	3478 → 54856 Len=125
4	0.010793	192.168.1.7	142.250.82.20	UDP	1156	50318 → 3478 Len=1114
5	0.014809	142.250.82.20	192.168.1.7	RTCP	106	Application specific subtype=13
6	0.022821	142.250.82.20	192.168.1.7	UDP	161	3478 → 54856 Len=119
7	0.037814	192.168.1.7	142.250.82.20	UDP	90	54856 → 3478 Len=48
8	0.042624	142.250.82.20	192.168.1.7	UDP	150	3478 → 54856 Len=108
9	0.053735	192.168.1.7	142.250.82.20	STUN	162	Binding Request user: lr2UwY8KA0UKBAoKAAiKAiAEEA:CCpX
10	0.059968	142.250.82.20	192.168.1.7	UDP	145	3478 → 54856 Len=103
11	0.064966	142.250.82.20	192.168.1.7	RTCP	110	Application specific subtype=13
12	0.082913	142.250.82.20	192.168.1.7	UDP	139	3478 → 54856 Len=97
13	0.085363	142.250.82.20	192.168.1.7	STUN	142	Binding Success Response user: lr2UwY8KA0UKBAoKAAiKAiAEEA:CCpX XOR-MAPPED-ADDRESS: …
14	0.100255	142.250.82.20	192.168.1.7	UDP	136	3478 → 54856 Len=94
15	0.120831	142.250.82.20	192.168.1.7	UDP	139	3478 → 54856 Len=97

ICMP



On selecting a packet of HTTP protocol, and on selecting Follow TCP Stream for this packet, the following result was obtained:



QUESTION 6

Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.

```
Ethernet II, Src: TaicangT_62:33:a0 (18:45:93:62:33:a0), Dst: IntelCor_41:92:63 (78:0c:b8:41:92:63)
  Destination: IntelCor_41:92:63 (78:0c:b8:41:92:63)
      Address: IntelCor_41:92:63 (78:0c:b8:41:92:63)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: TaicangT_62:33:a0 (18:45:93:62:33:a0)
      Address: TaicangT_62:33:a0 (18:45:93:62:33:a0)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

QUESTION 7

What are the manufacturers of your PC's Network Interface Card (NIC), and the servers NIC?

As can be seen in the above screenshot, the manufacturer of my computer's NIC is **TaicangT_62:33:a0.** The manufacturer of the server's NIC is **IntelCor_41:92:63.**

QUESTION 8

What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?

For my computer's manufacturer **(18:45:93:62:33:a0)**.

For the server's manufacturer **(78:0c:b8:41:92:63)**.

QUESTION 9

Find the following statistics:

- What percentage of packets in your capture are TCP, and give an example of the higher-level protocol which uses TCP?
- What percentage of packets in your capture are UDP, and give an example of the higher-level protocol which uses UDP?

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	195785	100.0	101014876	626 k	0	0	0	195785
Ethernet	100.0	195785	2.7	2746043	17 k	0	0	0	195785
Internet Protocol Version 6	1.3	2460	0.1	98400	610	0	0	0	2460
User Datagram Protocol	0.1	237	0.0	1896	11	0	0	0	237
Transmission Control Protocol	0.3	552	0.3	282378	1751	376	168190	1043	552
Internet Control Message Protocol v6	0.9	1671	0.1	53068	329	1671	53068	329	1671
Internet Protocol Version 4	98.5	192807	3.8	3856140	23 k	0	0	0	192807
User Datagram Protocol	83.6	163658	1.3	1309264	8121	0	0	0	163658
Transmission Control Protocol	14.9	29141	18.6	18744369	116 k	19546	10465321	64 k	29141
Internet Control Message Protocol	0.0	8	0.0	320	1	8	320	1	8
Address Resolution Protocol	0.3	518	0.0	19148	118	518	19148	118	518

15.2% of the packets follow TCP protocol**. 0.3%** are of IPv6 and **14.9%** are of IPv4. **SMTP** (Simple Mail Transfer Protocol Secure) and **FTP** (File Transfer Protocol) use TCP.

83.7% of the packets follow UDP protocol**. 0.1%** are of IPv6 and **83.6%** are of IPv4. **DNS** (Domain Name Service) and **RIP** (Routing Information Protocol) use UDP

QUESTION 10

Find the traffic flow Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.