NETWORK LAB REPORT

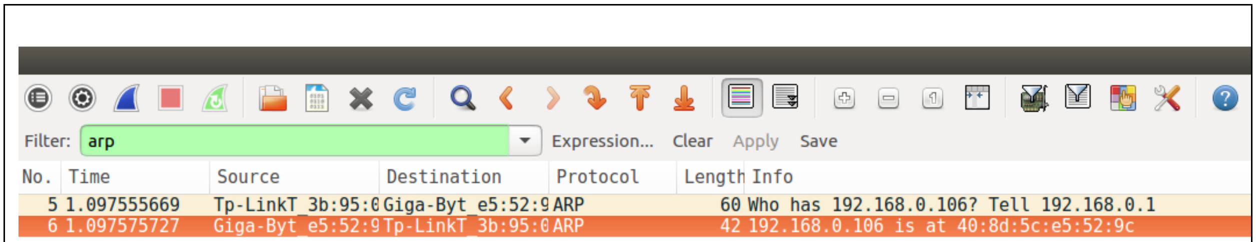
NAME: ANURAN CHAKRABORTY
ROLL NO.: 20
CLASS: BCSE-III
SECTION: A1

ASSIGNMENT NUMBER: 5

PROBLEM STATEMENT:
Packet tracer and traffic analysis with Wireshark.

DEADLINE: 4TH APRIL, 2019
SUBMITTED ON: 4TH APRIL, 2019
REPORT SUBMITTED ON: 11TH APRIL, 2019

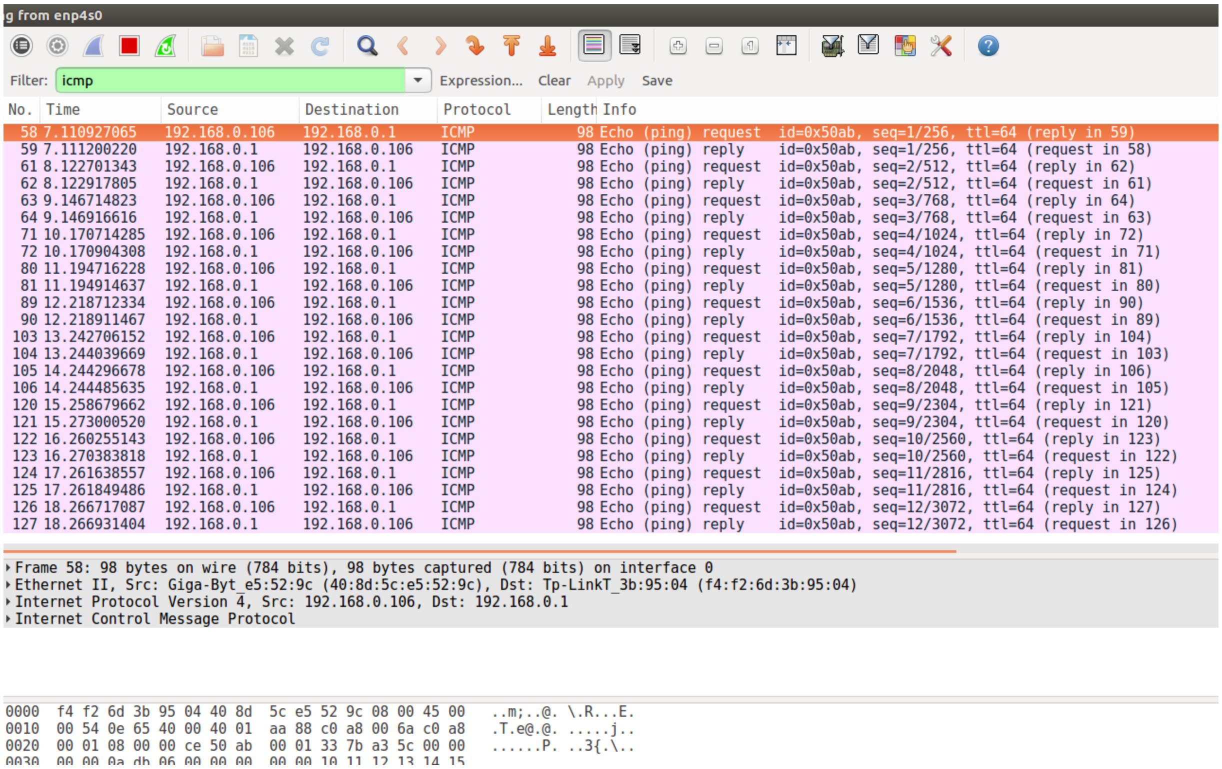
1. **Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the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



```
Filter: arp

No. Time          Source            Destination       Protocol    Length Info
  5 1.097555669   Tp-LinkT_3b:95:0 Giga-Byt_e5:52:9 ARP                60 Who has 192.168.0.106? Tell 192.168.0.1
  6 1.097575727   Giga-Byt_e5:52:9 Tp-LinkT_3b:95:0 ARP                42 192.168.0.106 is at 40:8d:5c:e5:52:9c
```

Fig 1. The ARP Requests can be seen asking for the physical address of the machine.



```
Filter: icmp

No. Time           Source          Destination     Protocol     Length Info
 58 7.110927065    192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=1/256, ttl=64 (reply in 59)
 59 7.111200220    192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=1/256, ttl=64 (request in 58)
 61 8.122701343    192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=2/512, ttl=64 (reply in 62)
 62 8.122917805    192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=2/512, ttl=64 (request in 61)
 63 9.146714823    192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=3/768, ttl=64 (reply in 64)
 64 9.146916616    192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=3/768, ttl=64 (request in 63)
 71 10.170714285   192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=4/1024, ttl=64 (reply in 72)
 72 10.170904308   192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=4/1024, ttl=64 (request in 71)
 80 11.194716228   192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=5/1280, ttl=64 (reply in 81)
 81 11.194914637   192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=5/1280, ttl=64 (request in 80)
 89 12.218712334   192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=6/1536, ttl=64 (reply in 90)
 90 12.218911467   192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=6/1536, ttl=64 (request in 89)
103 13.242706152   192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=7/1792, ttl=64 (reply in 104)
104 13.244039669   192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=7/1792, ttl=64 (request in 103)
105 14.244296678   192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=8/2048, ttl=64 (reply in 106)
106 14.244485635   192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=8/2048, ttl=64 (request in 105)
120 15.258679662   192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=9/2304, ttl=64 (reply in 121)
121 15.273000520   192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=9/2304, ttl=64 (request in 120)
122 16.260255143   192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=10/2560, ttl=64 (reply in 123)
123 16.270383818   192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=10/2560, ttl=64 (request in 122)
124 17.261638557   192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=11/2816, ttl=64 (reply in 125)
125 17.261849486   192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=11/2816, ttl=64 (request in 124)
126 18.266717087   192.168.0.106   192.168.0.1     ICMP             98 Echo (ping) request  id=0x50ab, seq=12/3072, ttl=64 (reply in 127)
127 18.266931404   192.168.0.1     192.168.0.106   ICMP             98 Echo (ping) reply    id=0x50ab, seq=12/3072, ttl=64 (request in 126)

▸Frame 58: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸Ethernet II, Src: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c), Dst: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04)
▸Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1
▸Internet Control Message Protocol

0000  f4 f2 6d 3b 95 04 40 8d  5c e5 52 9c 08 00 45 00   ..m;..@. \.R...E.
0010  00 54 0e 65 40 00 40 01  aa 88 c0 a8 00 6a c0 a8   .T.e@.@. .....j..
0020  00 01 08 00 00 ce 50 ab  00 01 33 7b a3 5c 00 00   ......P. ..3{.\..
0030  00 00 0a db 06 00 00 00  00 00 10 11 12 13 14 15
```

Fig 2. The ICMP packets which are sent

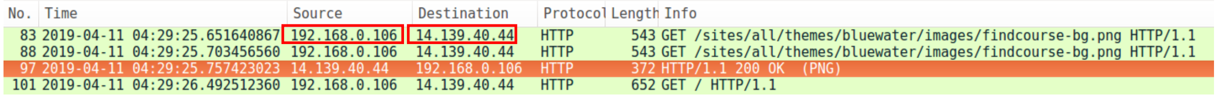
2. Generate some web traffic and

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

The different protocols that were found were:

- TCP
- TLSv1.2
- DNS
- GQUIC
- UDP
- SSDP
- MDNS

b. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)



No.	Time	Source	Destination	Protocol	Length	Info
83	2019-04-11 04:29:25.651640867	192.168.0.106	14.139.40.44	HTTP	543	GET /sites/all/themes/bluewater/images/findcourse-bg.png HTTP/1.1
88	2019-04-11 04:29:25.703456560	192.168.0.106	14.139.40.44	HTTP	543	GET /sites/all/themes/bluewater/images/findcourse-bg.png HTTP/1.1
97	2019-04-11 04:29:25.757423023	14.139.40.44	192.168.0.106	HTTP	372	HTTP/1.1 200 OK (PNG)
101	2019-04-11 04:29:26.492512360	192.168.0.106	14.139.40.44	HTTP	652	GET / HTTP/1.1

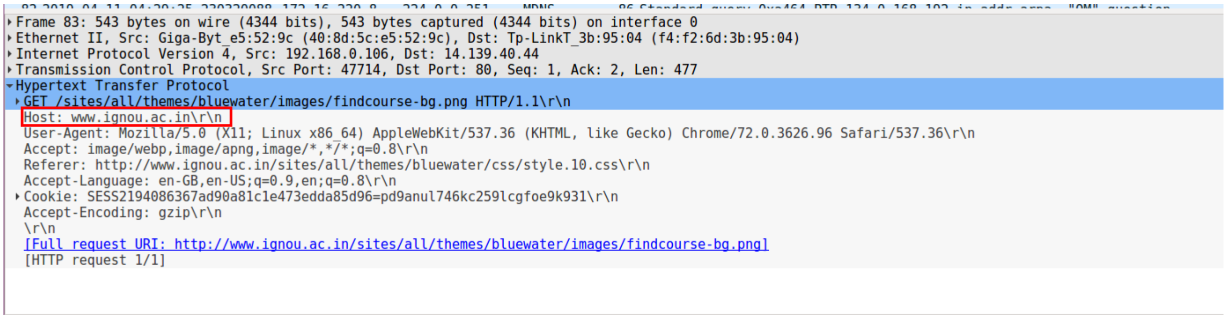
Fig 3. Showing the HTTP get and OK reply

It can be seen from fig 3. That it took approximately 0.054 seconds from the OF reply to be received after the last get has been dispatched.

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

From Fig. 3. It can be seen that for the HTTP get message the source is 192.168.0.106 and the destination address is 14.139.40.44. Thus, IP address of the website is: **14.139.40.44** and that of the computer is: **192.168.0.106.**

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.



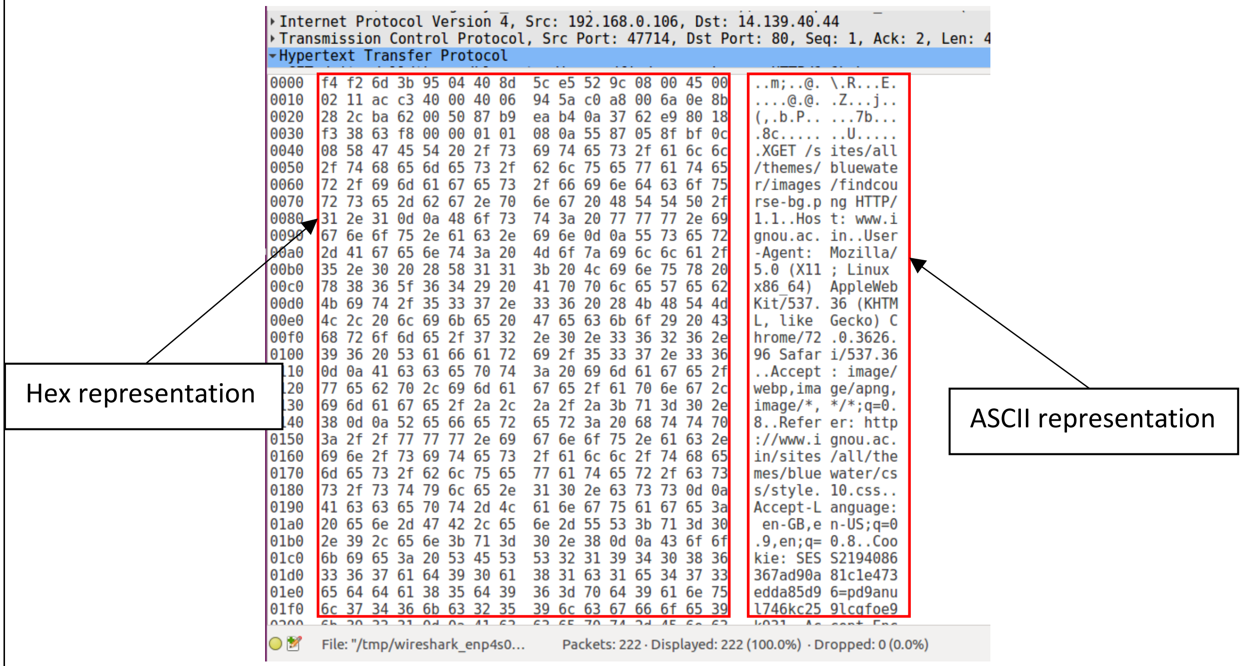
```
▸Frame 83: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface 0
▸Ethernet II, Src: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c), Dst: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04)
▸Internet Protocol Version 4, Src: 192.168.0.106, Dst: 14.139.40.44
▸Transmission Control Protocol, Src Port: 47714, Dst Port: 80, Seq: 1, Ack: 2, Len: 477
▾Hypertext Transfer Protocol
 ▸GET /sites/all/themes/bluewater/images/findcourse-bg.png HTTP/1.1\r\n
  Host: www.ignou.ac.in\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.96 Safari/537.36\r\n
  Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
  Referer: http://www.ignou.ac.in/sites/all/themes/bluewater/css/style.10.css\r\n
  Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
 ▸Cookie: SESS2194086367ad90a81c1e473edda85d96=pd9anul746kc259lcgfoe9k931\r\n
  Accept-Encoding: gzip\r\n
  \r\n
  [Full request URI: http://www.ignou.ac.in/sites/all/themes/bluewater/images/findcourse-bg.png]
  [HTTP request 1/1]
```

Fig 4. Packet details panel of HTTP get message.

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

From **Fig 4.** It can be seen that the Host is **www.ignou.ac.in.**

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

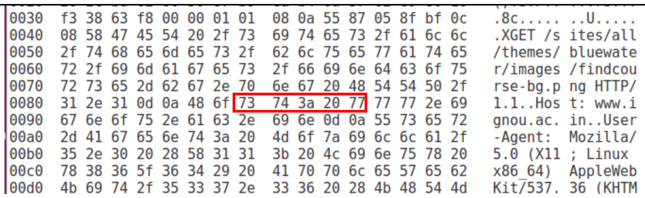


```
▸Internet Protocol Version 4, Src: 192.168.0.106, Dst: 14.139.40.44
▸Transmission Control Protocol, Src Port: 47714, Dst Port: 80, Seq: 1, Ack: 2, Len: 4
▾Hypertext Transfer Protocol
0000  f4 f2 6d 3b 95 04 40 8d  5c e5 52 9c 08 00 45 00   ..m;..@. \.R...E.
0010  02 11 ac c3 40 00 40 06  94 5a c0 a8 00 6a 0e 8b   ....@.@. .Z...j..
0020  28 2c ba 62 00 50 87 b9  ea b4 0a 37 62 e9 80 18   (,.b.P.. ...7b...
0030  f3 38 63 f8 00 00 01 01  08 0a 55 87 05 8f bf 0c   .8c..... ..U.....
0040  08 58 47 45 54 20 2f 73  69 74 65 73 2f 61 6c 6c   .XGET /s ites/all
0050  2f 74 68 65 6d 65 73 2f  62 6c 75 65 77 61 74 65   /themes/ bluewate
0060  72 2f 69 6d 61 67 65 73  2f 66 69 6e 64 63 6f 75   r/images /findcou
0070  72 73 65 2d 62 67 2e 70  6e 67 20 48 54 54 50 2f   rse-bg.p ng HTTP/
0080  31 2e 31 0d 0a 48 6f 73  74 3a 20 77 77 77 2e 69   1.1..Hos t: www.i
0090  67 6e 6f 75 2e 61 63 2e  69 6e 0d 0a 55 73 65 72   gnou.ac. in..User
00a0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00b0  35 2e 30 20 28 58 31 31  3b 20 4c 69 6e 75 78 20   5.0 (X11 ; Linux 
00c0  78 38 36 5f 36 34 29 20  41 70 70 6c 65 57 65 62   x86_64)  AppleWeb
00d0  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
00e0  4c 2c 20 6c 69 6b 65 20  47 65 63 6b 6f 29 20 43   L, like  Gecko) C
00f0  68 72 6f 6d 65 2f 37 32  2e 30 2e 33 36 32 36 2e   hrome/72 .0.3626.
0100  39 36 20 53 61 66 61 72  69 2f 35 33 37 2e 33 36   96 Safar i/537.36
 110  0d 0a 41 63 63 65 70 74  3a 20 69 6d 61 67 65 2f   ..Accept : image/
 120  77 65 62 70 2c 69 6d 61  67 65 2f 61 70 6e 67 2c   webp,ima ge/apng,
 130  69 6d 61 67 65 2f 2a 2c  2a 2f 2a 3b 71 3d 30 2e   image/*, */*;q=0.
 140  38 0d 0a 52 65 66 65 72  65 72 3a 20 68 74 74 70   8..Refer er: http
0150  3a 2f 2f 77 77 77 2e 69  67 6e 6f 75 2e 61 63 2e   ://www.i gnou.ac.
0160  69 6e 2f 73 69 74 65 73  2f 61 6c 6c 2f 74 68 65   in/sites /all/the
0170  6d 65 73 2f 62 6c 75 65  77 61 74 65 72 2f 63 73   mes/blue water/cs
0180  73 2f 73 74 79 6c 65 2e  31 30 2e 63 73 73 0d 0a   s/style. 10.css..
0190  41 63 63 65 70 74 2d 4c  61 6e 67 75 61 67 65 3a   Accept-L anguage:
01a0  20 65 6e 2d 47 42 2c 65  6e 2d 55 53 3b 71 3d 30    en-GB,e n-US;q=0
01b0  2e 39 2c 65 6e 3b 71 3d  30 2e 38 0d 0a 43 6f 6f   .9,en;q= 0.8..Coo
01c0  6b 69 65 3a 20 53 45 53  53 32 31 39 34 30 38 36   kie: SES S2194086
01d0  33 36 37 61 64 39 30 61  38 31 63 31 65 34 37 33   367ad90a 81c1e473
01e0  65 64 64 61 38 35 64 39  36 3d 70 64 39 61 6e 75   edda85d9 6=pd9anu
01f0  6c 37 34 36 6b 63 32 35  39 6c 63 67 66 6f 65 39   l746kc25 9lcgfoe9
```

File: "/tmp/wireshark_enp4s0... Packets: 222 · Displayed: 222 (100.0%) · Dropped: 0 (0.0%)

Fig 5. Hex and ASCII regions of packet.

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

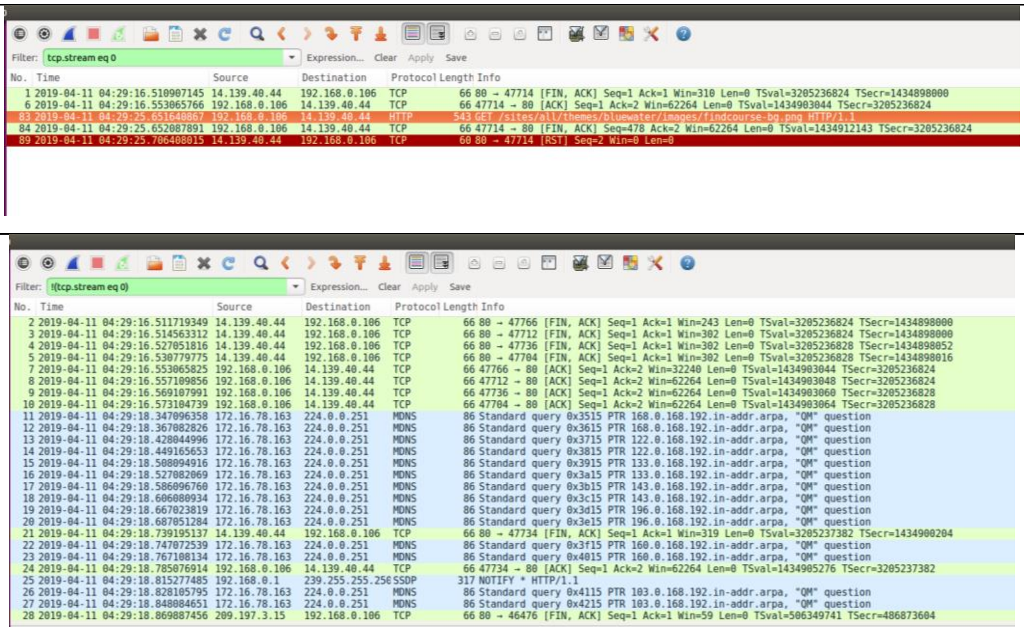


```
0030  f3 38 63 f8 00 00 01 01  08 0a 55 87 05 8f bf 0c   .8c..... ..U.....
0040  08 58 47 45 54 20 2f 73  69 74 65 73 2f 61 6c 6c   .XGET /s ites/all
0050  2f 74 68 65 6d 65 73 2f  62 6c 75 65 77 61 74 65   /themes/ bluewate
0060  72 2f 69 6d 61 67 65 73  2f 66 69 6e 64 63 6f 75   r/images /findcou
0070  72 73 65 2d 62 67 2e 70  6e 67 20 48 54 54 50 2f   rse-bg.p ng HTTP/
0080  31 2e 31 0d 0a 48 6f 73  74 3a 20 77 77 77 2e 69   1.1..Hos t: www.i
0090  67 6e 6f 75 2e 61 63 2e  69 6e 0d 0a 55 73 65 72   gnou.ac. in..User
00a0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00b0  35 2e 30 20 28 58 31 31  3b 20 4c 69 6e 75 78 20   5.0 (X11 ; Linux
00c0  78 38 36 5f 36 34 29 20  41 70 70 6c 65 57 65 62   x86_64)  AppleWeb
00d0  4b 69 74 2f 35 33 37 2e  33 36 20 28 4b 48 54 4d   Kit/537. 36 (KHTM
```

Fig 6. First 4 bytes of host

5. Filter packets with http, TCP, DNS and other protocols.

a. **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**.

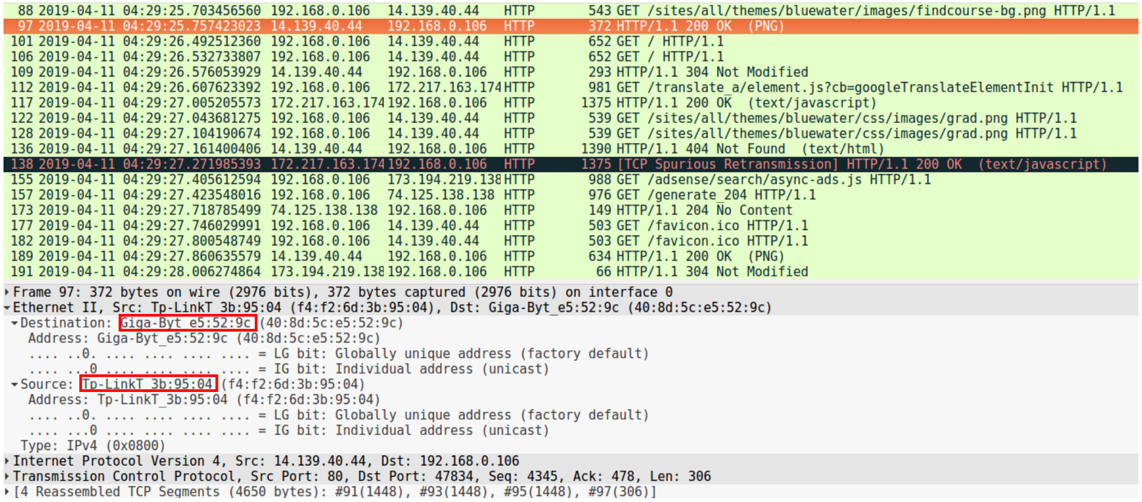


```
Filter: tcp.stream eq 0
No. Time                          Source          Destination     Protocol Length Info
  1 2019-04-11 04:29:16.510907145 14.139.40.44    192.168.0.106   TCP        66 80 → 47714 [FIN, ACK] Seq=1 Ack=1 Win=310 Len=0 TSval=3205236824 TSecr=1434898000
  6 2019-04-11 04:29:16.553065766 192.168.0.106   14.139.40.44    TCP        66 47714 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434903044 TSecr=3205236824
 83 2019-04-11 04:29:25.651640867 192.168.0.106   14.139.40.44    HTTP      543 GET /sites/all/themes/bluewater/images/findcourse-bg.png HTTP/1.1
 84 2019-04-11 04:29:25.652087891 192.168.0.106   14.139.40.44    TCP        66 47714 → 80 [FIN, ACK] Seq=478 Ack=2 Win=62264 Len=0 TSval=1434912143 TSecr=3205236824
 89 2019-04-11 04:29:25.706408015 14.139.40.44    192.168.0.106   TCP        60 80 → 47714 [RST] Seq=2 Win=0 Len=0
```

```
Filter: !(tcp.stream eq 0)
No. Time                          Source          Destination     Protocol Length Info
  2 2019-04-11 04:29:16.511719349 14.139.40.44    192.168.0.106   TCP        66 80 → 47766 [FIN, ACK] Seq=1 Ack=1 Win=243 Len=0 TSval=3205236824 TSecr=1434898000
  3 2019-04-11 04:29:16.514563312 14.139.40.44    192.168.0.106   TCP        66 80 → 47712 [FIN, ACK] Seq=1 Ack=1 Win=302 Len=0 TSval=3205236824 TSecr=1434898000
  4 2019-04-11 04:29:16.527051816 14.139.40.44    192.168.0.106   TCP        66 80 → 47736 [FIN, ACK] Seq=1 Ack=1 Win=302 Len=0 TSval=3205236828 TSecr=1434898052
  5 2019-04-11 04:29:16.530779775 14.139.40.44    192.168.0.106   TCP        66 80 → 47704 [FIN, ACK] Seq=1 Ack=1 Win=302 Len=0 TSval=3205236828 TSecr=1434898016
  7 2019-04-11 04:29:16.553065825 192.168.0.106   14.139.40.44    TCP        66 47766 → 80 [ACK] Seq=1 Ack=2 Win=32240 Len=0 TSval=1434903044 TSecr=3205236824
  8 2019-04-11 04:29:16.557109856 192.168.0.106   14.139.40.44    TCP        66 47712 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434903048 TSecr=3205236824
  9 2019-04-11 04:29:16.569107991 192.168.0.106   14.139.40.44    TCP        66 47736 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434903060 TSecr=3205236828
 10 2019-04-11 04:29:16.573104739 192.168.0.106   14.139.40.44    TCP        66 47704 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434903064 TSecr=3205236828
 11 2019-04-11 04:29:18.347096358 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3515 PTR 168.0.168.192.in-addr.arpa, "QM" question
 12 2019-04-11 04:29:18.367082826 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3615 PTR 168.0.168.192.in-addr.arpa, "QM" question
 13 2019-04-11 04:29:18.428044996 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3715 PTR 122.0.168.192.in-addr.arpa, "QM" question
 14 2019-04-11 04:29:18.449165653 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3815 PTR 122.0.168.192.in-addr.arpa, "QM" question
 15 2019-04-11 04:29:18.508094916 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3915 PTR 133.0.168.192.in-addr.arpa, "QM" question
 16 2019-04-11 04:29:18.527082069 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3a15 PTR 133.0.168.192.in-addr.arpa, "QM" question
 17 2019-04-11 04:29:18.586096760 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3b15 PTR 143.0.168.192.in-addr.arpa, "QM" question
 18 2019-04-11 04:29:18.606080934 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3c15 PTR 143.0.168.192.in-addr.arpa, "QM" question
 19 2019-04-11 04:29:18.667023819 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3d15 PTR 196.0.168.192.in-addr.arpa, "QM" question
 20 2019-04-11 04:29:18.687051284 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3e15 PTR 196.0.168.192.in-addr.arpa, "QM" question
 21 2019-04-11 04:29:18.739195137 14.139.40.44    192.168.0.106   TCP        66 80 → 47734 [FIN, ACK] Seq=1 Ack=1 Win=319 Len=0 TSval=3205237382 TSecr=1434900204
 22 2019-04-11 04:29:18.747072539 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x3f15 PTR 160.0.168.192.in-addr.arpa, "QM" question
 23 2019-04-11 04:29:18.767108134 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x4015 PTR 160.0.168.192.in-addr.arpa, "QM" question
 24 2019-04-11 04:29:18.785076914 192.168.0.106   14.139.40.44    TCP        66 47734 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434905276 TSecr=3205237382
 25 2019-04-11 04:29:18.815277485 192.168.0.1     239.255.255.250 SSDP      317 NOTIFY * HTTP/1.1
 26 2019-04-11 04:29:18.828105795 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x4115 PTR 103.0.168.192.in-addr.arpa, "QM" question
 27 2019-04-11 04:29:18.848084651 172.16.78.163   224.0.0.251     MDNS       86 Standard query 0x4215 PTR 103.0.168.192.in-addr.arpa, "QM" question
 28 2019-04-11 04:29:18.869887456 209.197.3.15    192.168.0.106   TCP        66 80 → 46476 [FIN, ACK] Seq=1 Ack=1 Win=59 Len=0 TSval=506349741 TSecr=486873604
```

Fig 7. Network flow

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.



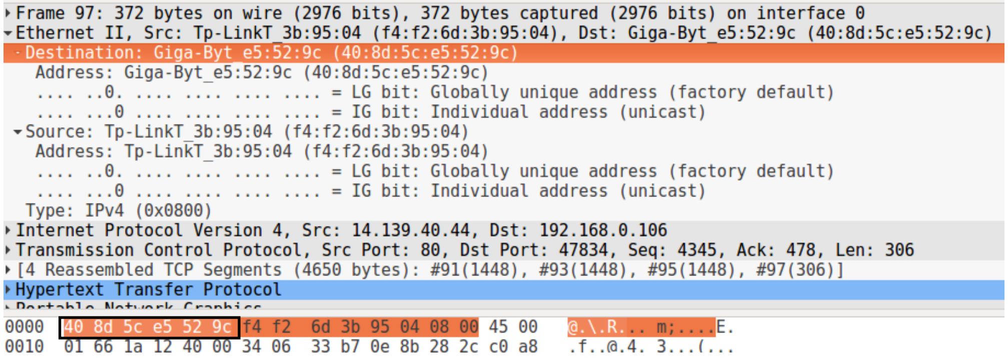
```
  88 2019-04-11 04:29:25.703456560 192.168.0.106   14.139.40.44    HTTP       543 GET /sites/all/themes/bluewater/images/findcourse-bg.png HTTP/1.1
  97 2019-04-11 04:29:25.757423023 14.139.40.44    192.168.0.106   HTTP       372 HTTP/1.1 200 OK  (PNG)
 101 2019-04-11 04:29:26.492512360 192.168.0.106   14.139.40.44    HTTP       652 GET / HTTP/1.1
 106 2019-04-11 04:29:26.532733807 192.168.0.106   14.139.40.44    HTTP       652 GET / HTTP/1.1
 109 2019-04-11 04:29:26.576053929 14.139.40.44    192.168.0.106   HTTP       293 HTTP/1.1 304 Not Modified
 112 2019-04-11 04:29:26.607623392 192.168.0.106   172.217.163.174 HTTP       981 GET /translate_a/element.js?cb=googleTranslateElementInit HTTP/1.1
 117 2019-04-11 04:29:27.005205573 172.217.163.174 192.168.0.106   HTTP      1375 HTTP/1.1 200 OK  (text/javascript)
 122 2019-04-11 04:29:27.043681275 192.168.0.106   14.139.40.44    HTTP       539 GET /sites/all/themes/bluewater/css/images/grad.png HTTP/1.1
 128 2019-04-11 04:29:27.104190674 192.168.0.106   14.139.40.44    HTTP       539 GET /sites/all/themes/bluewater/css/images/grad.png HTTP/1.1
 136 2019-04-11 04:29:27.161400406 14.139.40.44    192.168.0.106   HTTP      1390 HTTP/1.1 404 Not Found  (text/html)
 138 2019-04-11 04:29:27.271985393 172.217.163.174 192.168.0.106   HTTP      1375 [TCP Spurious Retransmission] HTTP/1.1 200 OK  (text/javascript)
 155 2019-04-11 04:29:27.405612594 192.168.0.106   173.194.219.138 HTTP       988 GET /adsense/search/async-ads.js HTTP/1.1
 157 2019-04-11 04:29:27.423548016 192.168.0.106   74.125.138.138  HTTP       976 GET /generate_204 HTTP/1.1
 173 2019-04-11 04:29:27.718785499 74.125.138.138  192.168.0.106   HTTP       149 HTTP/1.1 204 No Content
 177 2019-04-11 04:29:27.746029991 192.168.0.106   14.139.40.44    HTTP       503 GET /favicon.ico HTTP/1.1
 182 2019-04-11 04:29:27.800548749 192.168.0.106   14.139.40.44    HTTP       503 GET /favicon.ico HTTP/1.1
 189 2019-04-11 04:29:27.860635579 14.139.40.44    192.168.0.106   HTTP       634 HTTP/1.1 200 OK  (PNG)
 191 2019-04-11 04:29:28.006274864 173.194.219.138 192.168.0.106   HTTP        66 HTTP/1.1 304 Not Modified
▸Frame 97: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on interface 0
▾Ethernet II, Src: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04), Dst: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c)
 ▾Destination: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c)
    Address: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
 ▾Source: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04)
    Address: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: IPv4 (0x0800)
▸Internet Protocol Version 4, Src: 14.139.40.44, Dst: 192.168.0.106
▸Transmission Control Protocol, Src Port: 80, Dst Port: 47834, Seq: 4345, Ack: 478, Len: 306
▸[4 Reassembled TCP Segments (4650 bytes): #91(1448), #93(1448), #95(1448), #97(306)]
```

Fig 8. Ethernet details of packet coming from host

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

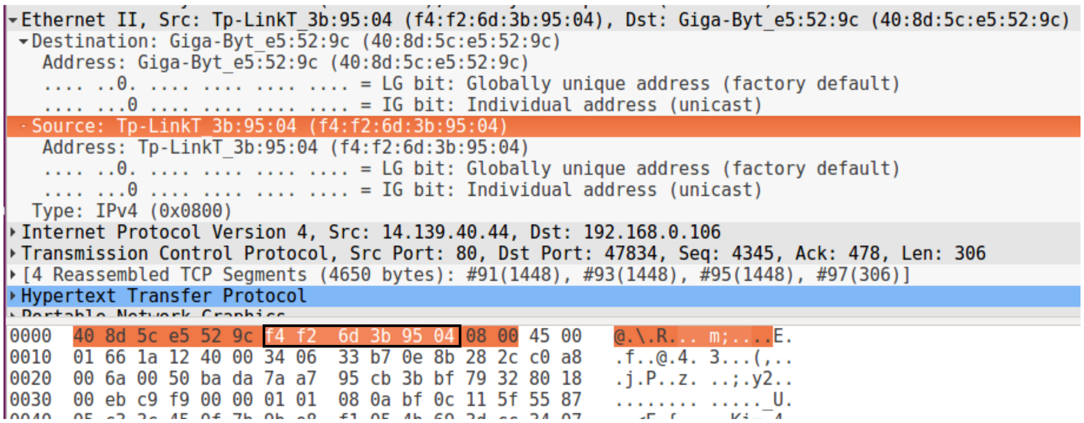
PC's Network Interface Card (NIC): **Gigabyte.**
Server's NIC: **TP-Link.**

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



```
▸Frame 97: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on interface 0
▾Ethernet II, Src: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04), Dst: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c)
 ▾Destination: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c)
    Address: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
 ▾Source: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04)
    Address: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: IPv4 (0x0800)
▸Internet Protocol Version 4, Src: 14.139.40.44, Dst: 192.168.0.106
▸Transmission Control Protocol, Src Port: 80, Dst Port: 47834, Seq: 4345, Ack: 478, Len: 306
▸[4 Reassembled TCP Segments (4650 bytes): #91(1448), #93(1448), #95(1448), #97(306)]
▸Hypertext Transfer Protocol
▸Portable Network Graphics
0000  40 8d 5c e5 52 9c f4 f2  6d 3b 95 04 08 00 45 00   @.\.R... m;....E.
0010  01 66 1a 12 40 00 34 06  33 b7 0e 8b 28 2c c0 a8   .f..@.4. 3...(...
```

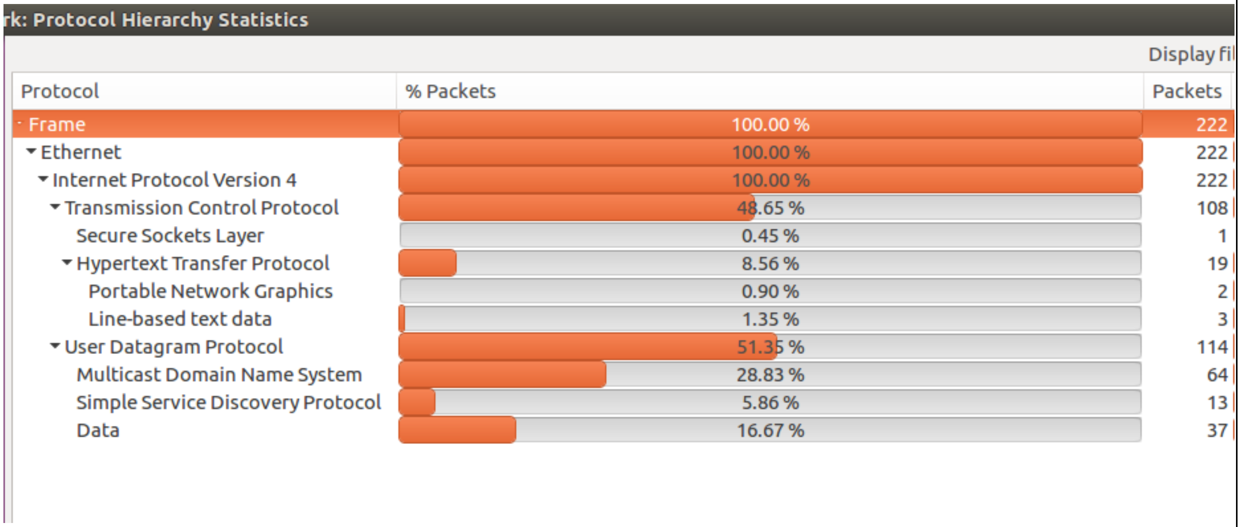
Fig 9. Hex value of Gigabyte NIC



```
▾Ethernet II, Src: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04), Dst: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c)
 ▾Destination: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c)
   Address: Giga-Byt_e5:52:9c (40:8d:5c:e5:52:9c)
   .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
 ▾Source: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04)
   Address: Tp-LinkT_3b:95:04 (f4:f2:6d:3b:95:04)
   .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▸Internet Protocol Version 4, Src: 14.139.40.44, Dst: 192.168.0.106
▸Transmission Control Protocol, Src Port: 80, Dst Port: 47834, Seq: 4345, Ack: 478, Len: 306
▸[4 Reassembled TCP Segments (4650 bytes): #91(1448), #93(1448), #95(1448), #97(306)]
▸Hypertext Transfer Protocol
▸Portable Network Graphics
0000  40 8d 5c e5 52 9c f4 f2  6d 3b 95 04 08 00 45 00   @.\.R... m;....E.
0010  01 66 1a 12 40 00 34 06  33 b7 0e 8b 28 2c c0 a8   .f..@.4. 3...(,..
0020  00 6a 00 50 ba da 7a a7  95 cb 3b bf 79 32 80 18   .j.P..z. ..;.y2..
0030  00 eb c9 f9 00 00 01 01  08 0a bf 0c 11 5f 55 87   ........ ....._U.
```

Fig 10. Hex value of TP-Link Router

9. Find the following statistics:



rk: Protocol Hierarchy Statistics

Display fil

Protocol	% Packets	Packets
Frame	100.00 %	222
▾Ethernet	100.00 %	222
▾Internet Protocol Version 4	100.00 %	222
▾Transmission Control Protocol	48.65 %	108
Secure Sockets Layer	0.45 %	1
▾Hypertext Transfer Protocol	8.56 %	19
Portable Network Graphics	0.90 %	2
Line-based text data	1.35 %	3
▾User Datagram Protocol	51.35 %	114
Multicast Domain Name System	28.83 %	64
Simple Service Discovery Protocol	5.86 %	13
Data	16.67 %	37

Fig 11. Statistics of packets

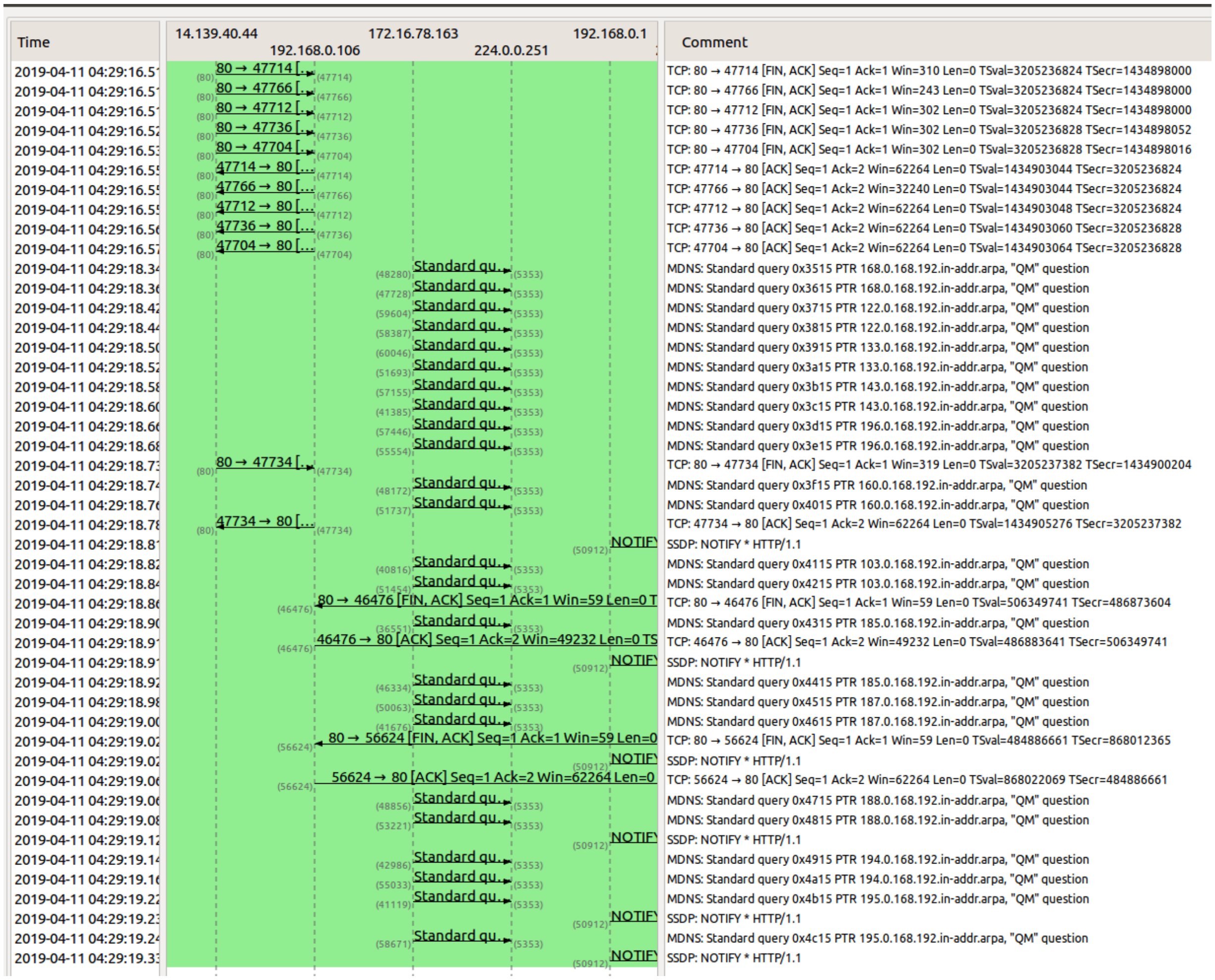
a. What percentage of packets in your capture are TCP, and give an example of the higher-level protocol which uses TCP?

48.65% of packets are TCP. **FTP** is a higher-level protocol that uses TCP.

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

51.35% of packets are TCP. **DNS** is a higher-level protocol that uses TCP.

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



Time	14.139.40.44 · 192.168.0.106 · 172.16.78.163 · 224.0.0.251 · 192.168.0.1	Comment
2019-04-11 04:29:16.51	(80) 80 → 47714 [... (47714)	TCP: 80 → 47714 [FIN, ACK] Seq=1 Ack=1 Win=310 Len=0 TSval=3205236824 TSecr=1434898000
2019-04-11 04:29:16.51	(80) 80 → 47766 [... (47766)	TCP: 80 → 47766 [FIN, ACK] Seq=1 Ack=1 Win=243 Len=0 TSval=3205236824 TSecr=1434898000
2019-04-11 04:29:16.51	(80) 80 → 47712 [... (47712)	TCP: 80 → 47712 [FIN, ACK] Seq=1 Ack=1 Win=302 Len=0 TSval=3205236824 TSecr=1434898000
2019-04-11 04:29:16.52	(80) 80 → 47736 [... (47736)	TCP: 80 → 47736 [FIN, ACK] Seq=1 Ack=1 Win=302 Len=0 TSval=3205236828 TSecr=1434898052
2019-04-11 04:29:16.53	(80) 80 → 47704 [... (47704)	TCP: 80 → 47704 [FIN, ACK] Seq=1 Ack=1 Win=302 Len=0 TSval=3205236828 TSecr=1434898016
2019-04-11 04:29:16.55	(80) 47714 → 80 [... (47714)	TCP: 47714 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434903044 TSecr=3205236824
2019-04-11 04:29:16.55	(80) 47766 → 80 [... (47766)	TCP: 47766 → 80 [ACK] Seq=1 Ack=2 Win=32240 Len=0 TSval=1434903044 TSecr=3205236824
2019-04-11 04:29:16.55	(80) 47712 → 80 [... (47712)	TCP: 47712 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434903048 TSecr=3205236824
2019-04-11 04:29:16.56	(80) 47736 → 80 [... (47736)	TCP: 47736 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434903060 TSecr=3205236828
2019-04-11 04:29:16.57	(80) 47704 → 80 [... (47704)	TCP: 47704 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434903064 TSecr=3205236828
2019-04-11 04:29:18.34	(48280) Standard qu... (5353)	MDNS: Standard query 0x3515 PTR 168.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.36	(47728) Standard qu... (5353)	MDNS: Standard query 0x3615 PTR 168.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.42	(59604) Standard qu... (5353)	MDNS: Standard query 0x3715 PTR 122.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.44	(58387) Standard qu... (5353)	MDNS: Standard query 0x3815 PTR 122.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.50	(60046) Standard qu... (5353)	MDNS: Standard query 0x3915 PTR 133.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.52	(51693) Standard qu... (5353)	MDNS: Standard query 0x3a15 PTR 133.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.58	(57155) Standard qu... (5353)	MDNS: Standard query 0x3b15 PTR 143.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.60	(41385) Standard qu... (5353)	MDNS: Standard query 0x3c15 PTR 143.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.66	(57446) Standard qu... (5353)	MDNS: Standard query 0x3d15 PTR 196.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.68	(55554) Standard qu... (5353)	MDNS: Standard query 0x3e15 PTR 196.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.73	(80) 80 → 47734 [... (47734)	TCP: 80 → 47734 [FIN, ACK] Seq=1 Ack=1 Win=319 Len=0 TSval=3205237382 TSecr=1434900204
2019-04-11 04:29:18.74	(48172) Standard qu... (5353)	MDNS: Standard query 0x3f15 PTR 160.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.76	(51737) Standard qu... (5353)	MDNS: Standard query 0x4015 PTR 160.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.78	(80) 47734 → 80 [... (47734)	TCP: 47734 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=1434905276 TSecr=3205237382
2019-04-11 04:29:18.81	(50912) NOTIFY	SSDP: NOTIFY * HTTP/1.1
2019-04-11 04:29:18.82	(40816) Standard qu... (5353)	MDNS: Standard query 0x4115 PTR 103.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.84	(51454) Standard qu... (5353)	MDNS: Standard query 0x4215 PTR 103.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.86	(46476) 80 → 46476 [FIN, ACK] Seq=1 Ack=1 Win=59 Len=0 T	TCP: 80 → 46476 [FIN, ACK] Seq=1 Ack=1 Win=59 Len=0 TSval=506349741 TSecr=486873604
2019-04-11 04:29:18.90	(36551) Standard qu... (5353)	MDNS: Standard query 0x4315 PTR 185.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.91	(46476) 46476 → 80 [ACK] Seq=1 Ack=2 Win=49232 Len=0 TS	TCP: 46476 → 80 [ACK] Seq=1 Ack=2 Win=49232 Len=0 TSval=486883641 TSecr=506349741
2019-04-11 04:29:18.91	(50912) NOTIFY	SSDP: NOTIFY * HTTP/1.1
2019-04-11 04:29:18.92	(46334) Standard qu... (5353)	MDNS: Standard query 0x4415 PTR 185.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:18.98	(50063) Standard qu... (5353)	MDNS: Standard query 0x4515 PTR 187.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:19.00	(41676) Standard qu... (5353)	MDNS: Standard query 0x4615 PTR 187.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:19.02	(56624) 80 → 56624 [FIN, ACK] Seq=1 Ack=1 Win=59 Len=0	TCP: 80 → 56624 [FIN, ACK] Seq=1 Ack=1 Win=59 Len=0 TSval=484886661 TSecr=868012365
2019-04-11 04:29:19.02	(50912) NOTIFY	SSDP: NOTIFY * HTTP/1.1
2019-04-11 04:29:19.06	(56624) 56624 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0	TCP: 56624 → 80 [ACK] Seq=1 Ack=2 Win=62264 Len=0 TSval=868022069 TSecr=484886661
2019-04-11 04:29:19.06	(48856) Standard qu... (5353)	MDNS: Standard query 0x4715 PTR 188.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:19.08	(53221) Standard qu... (5353)	MDNS: Standard query 0x4815 PTR 188.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:19.12	(50912) NOTIFY	SSDP: NOTIFY * HTTP/1.1
2019-04-11 04:29:19.14	(42986) Standard qu... (5353)	MDNS: Standard query 0x4915 PTR 194.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:19.16	(55033) Standard qu... (5353)	MDNS: Standard query 0x4a15 PTR 194.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:19.22	(41119) Standard qu... (5353)	MDNS: Standard query 0x4b15 PTR 195.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:19.23	(50912) NOTIFY	SSDP: NOTIFY * HTTP/1.1
2019-04-11 04:29:19.24	(58671) Standard qu... (5353)	MDNS: Standard query 0x4c15 PTR 195.0.168.192.in-addr.arpa, "QM" question
2019-04-11 04:29:19.33	(50912) NOTIFY	SSDP: NOTIFY * HTTP/1.1

Fig 12. Network flow graph