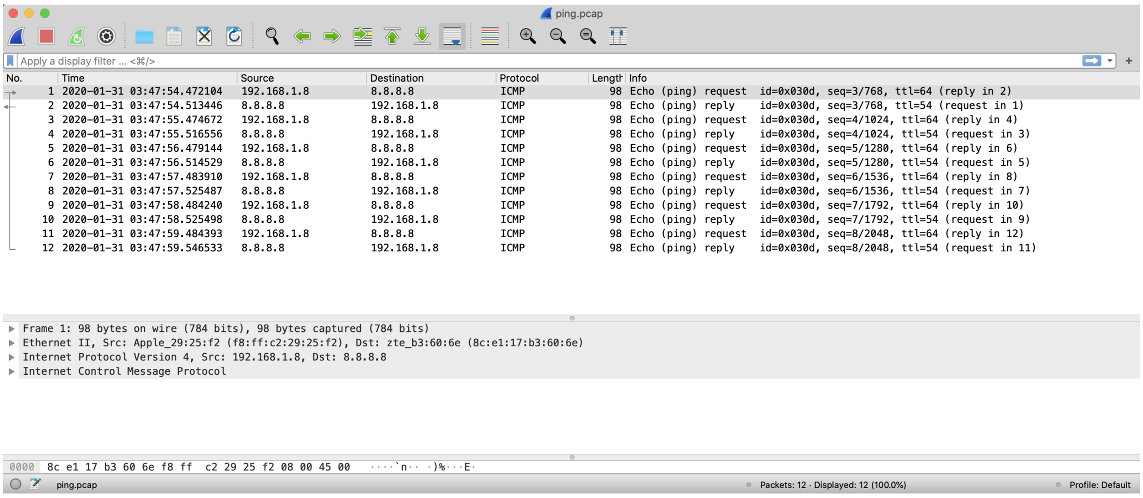
Assignment 3

Anjishnu Mukherjee B05-511017020 (510517086)

3a. Analyse the packets (across all layers) exchanged with your computer while executing the following commands: (i) ping, (ii) traceroute, (iii) dig, (iv) arp,(v) wget.

```
(i) ping :

    - We capture the relevant packets using the icmp filter.
    - There are 2 types of packets : Ping Request and Response
    - A request is made from my laptop's IP to the destination IP.
    - Corresponding response is present in the next packet.
```

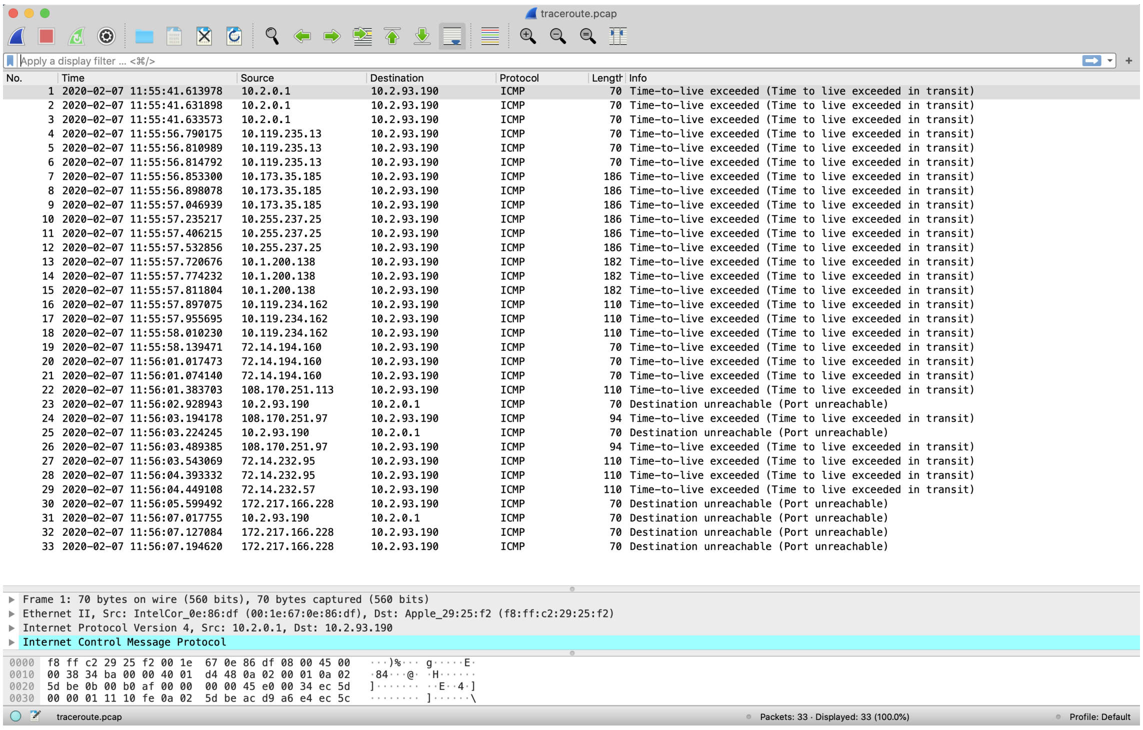


```
No.   Time                        Source         Destination    Protocol  Length Info
    1 2020-01-31 03:47:54.472104  192.168.1.8    8.8.8.8        ICMP      98 Echo (ping) request  id=0x030d, seq=3/768, ttl=64 (reply in 2)
    2 2020-01-31 03:47:54.513446  8.8.8.8        192.168.1.8    ICMP      98 Echo (ping) reply    id=0x030d, seq=3/768, ttl=54 (request in 1)
    3 2020-01-31 03:47:55.474672  192.168.1.8    8.8.8.8        ICMP      98 Echo (ping) request  id=0x030d, seq=4/1024, ttl=64 (reply in 4)
    4 2020-01-31 03:47:55.516556  8.8.8.8        192.168.1.8    ICMP      98 Echo (ping) reply    id=0x030d, seq=4/1024, ttl=54 (request in 3)
    5 2020-01-31 03:47:56.479144  192.168.1.8    8.8.8.8        ICMP      98 Echo (ping) request  id=0x030d, seq=5/1280, ttl=64 (reply in 6)
    6 2020-01-31 03:47:56.514529  8.8.8.8        192.168.1.8    ICMP      98 Echo (ping) reply    id=0x030d, seq=5/1280, ttl=54 (request in 5)
    7 2020-01-31 03:47:57.483910  192.168.1.8    8.8.8.8        ICMP      98 Echo (ping) request  id=0x030d, seq=6/1536, ttl=64 (reply in 8)
    8 2020-01-31 03:47:57.525487  8.8.8.8        192.168.1.8    ICMP      98 Echo (ping) reply    id=0x030d, seq=6/1536, ttl=54 (request in 7)
    9 2020-01-31 03:47:58.484240  192.168.1.8    8.8.8.8        ICMP      98 Echo (ping) request  id=0x030d, seq=7/1792, ttl=64 (reply in 10)
   10 2020-01-31 03:47:58.525498  8.8.8.8        192.168.1.8    ICMP      98 Echo (ping) reply    id=0x030d, seq=7/1792, ttl=54 (request in 9)
   11 2020-01-31 03:47:59.484393  192.168.1.8    8.8.8.8        ICMP      98 Echo (ping) request  id=0x030d, seq=8/2048, ttl=64 (reply in 12)
   12 2020-01-31 03:47:59.546533  8.8.8.8        192.168.1.8    ICMP      98 Echo (ping) reply    id=0x030d, seq=8/2048, ttl=54 (request in 11)
```

```
▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: Apple_29:25:f2 (f8:ff:c2:29:25:f2), Dst: zte_b3:60:6e (8c:e1:17:b3:60:6e)
▶ Internet Protocol Version 4, Src: 192.168.1.8, Dst: 8.8.8.8
▶ Internet Control Message Protocol
```

```
0000  8c e1 17 b3 60 6e f8 ff  c2 29 25 f2 08 00 45 00   ····`n·· ·)%···E·
```

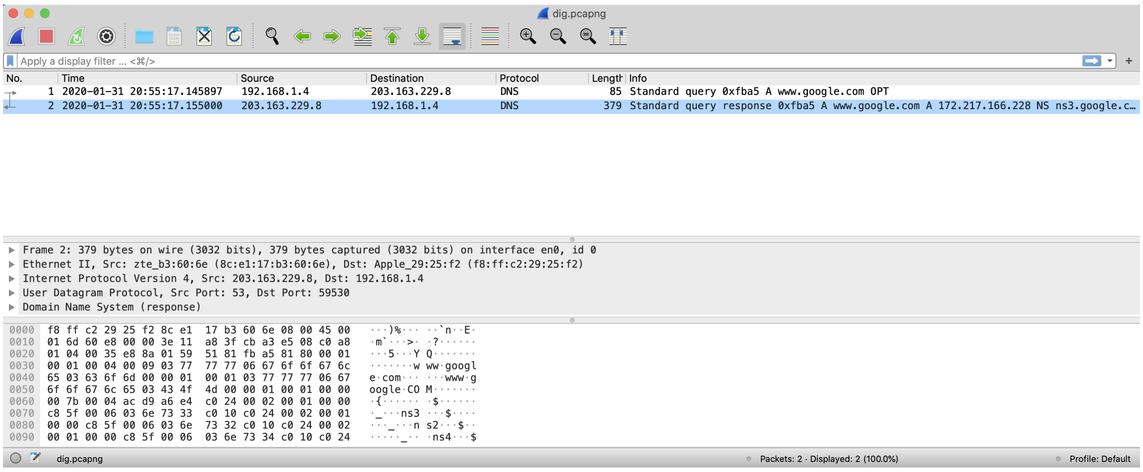
```
(ii) traceroute :

    - Makes use of TTL mechanism limiting the time to live for
      each packet to some value.
    - Devices send back an ICMP message when dropping the packet.
    - Thus we filter using ICMP filter.
    - The protocol used for the probes in a UNIX system is UDP and responses
      are send back using ICMP.
```



```
No.  Time                        Source            Destination    Protocol  Length Info
   1 2020-02-07 11:55:41.613978  10.2.0.1          10.2.93.190    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   2 2020-02-07 11:55:41.631898  10.2.0.1          10.2.93.190    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   3 2020-02-07 11:55:41.633573  10.2.0.1          10.2.93.190    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   4 2020-02-07 11:55:56.790175  10.119.235.13     10.2.93.190    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   5 2020-02-07 11:55:56.810989  10.119.235.13     10.2.93.190    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   6 2020-02-07 11:55:56.814792  10.119.235.13     10.2.93.190    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
   7 2020-02-07 11:55:56.853300  10.173.35.185     10.2.93.190    ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
   8 2020-02-07 11:55:56.898078  10.173.35.185     10.2.93.190    ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
   9 2020-02-07 11:55:57.046939  10.173.35.185     10.2.93.190    ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
  10 2020-02-07 11:55:57.235217  10.255.237.25     10.2.93.190    ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
  11 2020-02-07 11:55:57.406215  10.255.237.25     10.2.93.190    ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
  12 2020-02-07 11:55:57.532856  10.255.237.25     10.2.93.190    ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
  13 2020-02-07 11:55:57.720676  10.1.200.138      10.2.93.190    ICMP      182 Time-to-live exceeded (Time to live exceeded in transit)
  14 2020-02-07 11:55:57.774232  10.1.200.138      10.2.93.190    ICMP      182 Time-to-live exceeded (Time to live exceeded in transit)
  15 2020-02-07 11:55:57.811804  10.1.200.138      10.2.93.190    ICMP      182 Time-to-live exceeded (Time to live exceeded in transit)
  16 2020-02-07 11:55:57.897075  10.119.234.162    10.2.93.190    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  17 2020-02-07 11:55:57.955695  10.119.234.162    10.2.93.190    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  18 2020-02-07 11:55:58.010230  10.119.234.162    10.2.93.190    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  19 2020-02-07 11:55:58.139471  72.14.194.160     10.2.93.190    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  20 2020-02-07 11:56:01.017473  72.14.194.160     10.2.93.190    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  21 2020-02-07 11:56:01.074140  72.14.194.160     10.2.93.190    ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  22 2020-02-07 11:56:01.383703  108.170.251.113   10.2.93.190    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  23 2020-02-07 11:56:02.928943  10.2.93.190       10.2.0.1       ICMP       70 Destination unreachable (Port unreachable)
  24 2020-02-07 11:56:03.194178  108.170.251.97    10.2.93.190    ICMP       94 Time-to-live exceeded (Time to live exceeded in transit)
  25 2020-02-07 11:56:03.224245  10.2.93.190       10.2.0.1       ICMP       70 Destination unreachable (Port unreachable)
  26 2020-02-07 11:56:03.489385  108.170.251.97    10.2.93.190    ICMP       94 Time-to-live exceeded (Time to live exceeded in transit)
  27 2020-02-07 11:56:03.543069  72.14.232.95      10.2.93.190    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  28 2020-02-07 11:56:04.393332  72.14.232.95      10.2.93.190    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  29 2020-02-07 11:56:04.449108  72.14.232.57      10.2.93.190    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  30 2020-02-07 11:56:05.599492  172.217.166.228   10.2.93.190    ICMP       70 Destination unreachable (Port unreachable)
  31 2020-02-07 11:56:07.017755  10.2.93.190       10.2.0.1       ICMP       70 Destination unreachable (Port unreachable)
  32 2020-02-07 11:56:07.127084  172.217.166.228   10.2.93.190    ICMP       70 Destination unreachable (Port unreachable)
  33 2020-02-07 11:56:07.194620  172.217.166.228   10.2.93.190    ICMP       70 Destination unreachable (Port unreachable)

▶ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▶ Ethernet II, Src: IntelCor_0e:86:df (00:1e:67:0e:86:df), Dst: Apple_29:25:f2 (f8:ff:c2:29:25:f2)
▶ Internet Protocol Version 4, Src: 10.2.0.1, Dst: 10.2.93.190
▶ Internet Control Message Protocol

0000  f8 ff c2 29 25 f2 00 1e  67 0e 86 df 08 00 45 00   ···)%··· g·····E·
0010  00 38 34 ba 00 00 40 01  d4 48 0a 02 00 01 0a 02   ·84···@· ·H······
0020  5d be 0b 00 b0 af 00 00  00 00 45 e0 00 34 ec 5d   ]······· ··E··4·]
0030  00 00 01 11 10 fe 0a 02  5d be ac d9 a6 e4 ec 5c   ········ ]······\
```

(iii) dig :

- We filter using dns protocol.
- The info for the request packet shows 'A' because we are querying for a IP address.
- The DNS response packet shows the IP address corresponding to the name specified in the request.

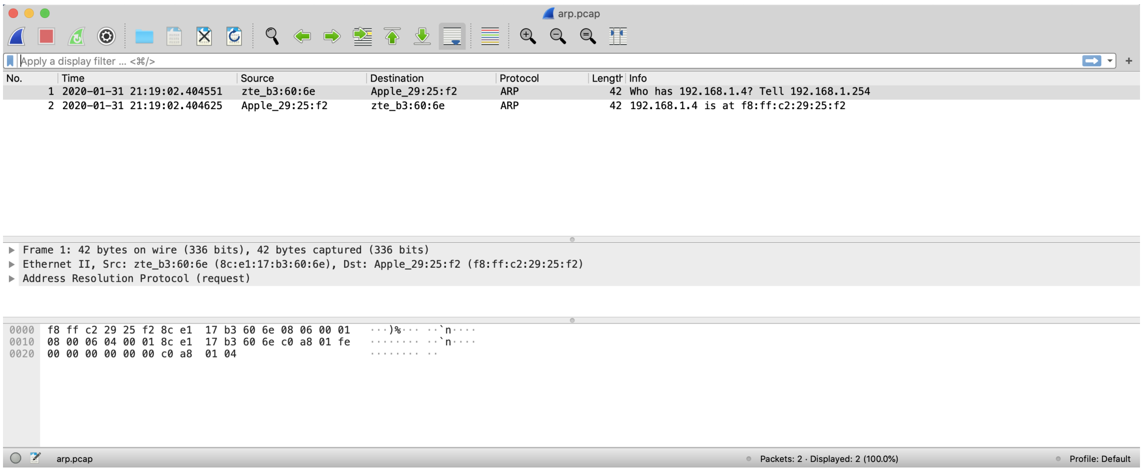


```
No.  Time                        Source          Destination     Protocol  Length Info
   1 2020-01-31 20:55:17.145897  192.168.1.4     203.163.229.8   DNS         85 Standard query 0xfba5 A www.google.com OPT
   2 2020-01-31 20:55:17.155000  203.163.229.8   192.168.1.4     DNS        379 Standard query response 0xfba5 A www.google.com A 172.217.166.228 NS ns3.google.c…

▶ Frame 2: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface en0, id 0
▶ Ethernet II, Src: zte_b3:60:6e (8c:e1:17:b3:60:6e), Dst: Apple_29:25:f2 (f8:ff:c2:29:25:f2)
▶ Internet Protocol Version 4, Src: 203.163.229.8, Dst: 192.168.1.4
▶ User Datagram Protocol, Src Port: 53, Dst Port: 59530
▶ Domain Name System (response)

0000  f8 ff c2 29 25 f2 8c e1  17 b3 60 6e 08 00 45 00   ···)%··· ··`n··E·
0010  01 6d 60 e8 00 00 3e 11  a8 3f cb a3 e5 08 c0 a8   ·m`···>· ·?······
0020  01 04 00 35 e8 8a 01 59  51 81 fb a5 81 80 00 01   ···5···Y Q·······
0030  00 01 00 04 00 09 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01 03 77 77 77 06 67   e·com··· ···www·g
0050  6f 6f 67 6c 65 03 43 4f  4d 00 00 01 00 01 00 00   oogle·CO M·······
0060  00 7b 00 04 ac d9 a6 e4  c0 24 00 02 00 01 00 00   ·{······ ·$······
0070  c8 5f 00 06 03 6e 73 33  c0 10 c0 24 00 02 00 01   ·_···ns3 ···$····
0080  00 00 c8 5f 00 06 03 6e  73 32 c0 10 c0 24 00 02   ···_···n s2···$··
0090  00 01 00 00 c8 5f 00 06  03 6e 73 34 c0 10 c0 24   ·····_·· ·ns4···$
```

(iv) arp :

- We filter using the ARP protocol.
- 2 packets are captured - ARP request and ARP reply.
- The request packet asks for the MAC address corresponding to the

```
     IP address of en0.
   - en0 is the active promiscuous mode interface I am using in wireshark.
   - The reply packet gives the MAC address.
```



arp.pcap

Apply a display filter ... <⌘/>

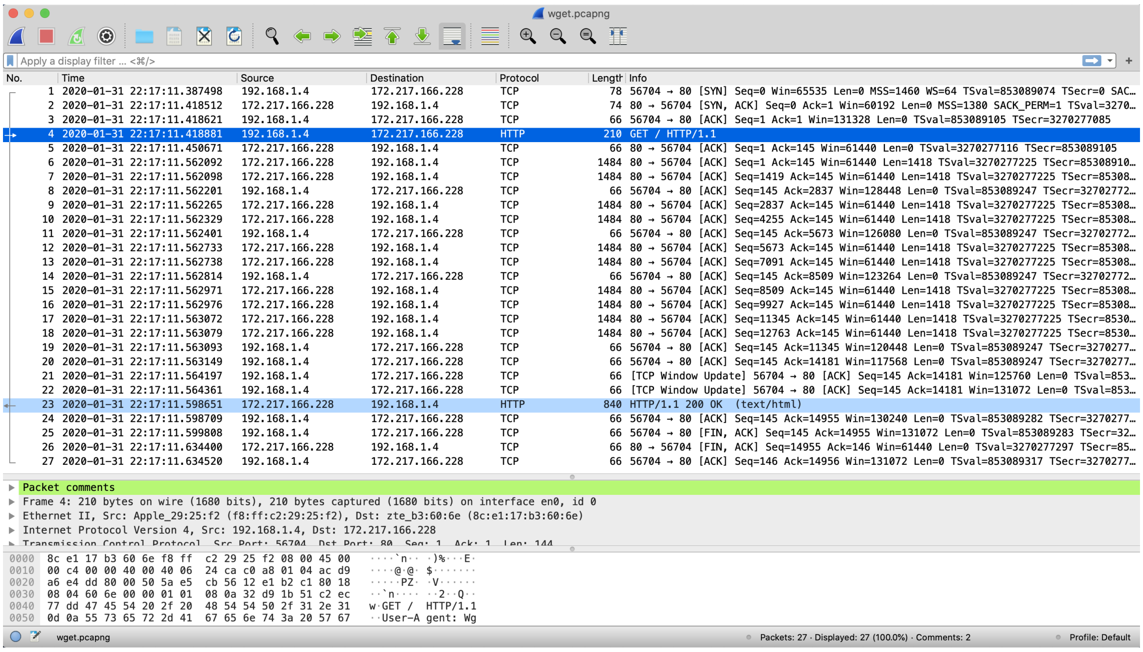
```
No.  Time                        Source          Destination     Protocol  Length Info
   1 2020-01-31 21:19:02.404551  zte_b3:60:6e    Apple_29:25:f2  ARP           42 Who has 192.168.1.4? Tell 192.168.1.254
   2 2020-01-31 21:19:02.404625  Apple_29:25:f2  zte_b3:60:6e    ARP           42 192.168.1.4 is at f8:ff:c2:29:25:f2
```

```
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▶ Ethernet II, Src: zte_b3:60:6e (8c:e1:17:b3:60:6e), Dst: Apple_29:25:f2 (f8:ff:c2:29:25:f2)
▶ Address Resolution Protocol (request)
```

```
0000  f8 ff c2 29 25 f2 8c e1  17 b3 60 6e 08 06 00 01   ···)%··· ··`n····
0010  08 00 06 04 00 01 8c e1  17 b3 60 6e c0 a8 01 fe   ········ ··`n····
0020  00 00 00 00 00 00 c0 a8  01 04                     ········ ··
```

arp.pcap · Packets: 2 · Displayed: 2 (100.0%) · Profile: Default

```
(v) wget :

   - We filter using tcp.port == 80 ( I am trying to get a http page using wget.)
   - Many packets get captured, but only 2 are of interest. (GET/HTTP and HTTP OK)
   - GET corresponds to sendig the request and OK is the response
     on successful completion.
```



wget.pcapng

Apply a display filter ... <⌘/>

```
No.  Time                        Source          Destination     Protocol  Length Info
   1 2020-01-31 22:17:11.387498  192.168.1.4     172.217.166.228 TCP           78 56704 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=853089074 TSecr=0 SAC…
   2 2020-01-31 22:17:11.418512  172.217.166.228 192.168.1.4     TCP           74 80 → 56704 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=3270…
   3 2020-01-31 22:17:11.418621  192.168.1.4     172.217.166.228 TCP           66 56704 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=853089105 TSecr=3270277085
   4 2020-01-31 22:17:11.418881  192.168.1.4     172.217.166.228 HTTP         210 GET / HTTP/1.1
   5 2020-01-31 22:17:11.450671  172.217.166.228 192.168.1.4     TCP           66 80 → 56704 [ACK] Seq=1 Ack=145 Win=61440 Len=0 TSval=3270277116 TSecr=853089105
   6 2020-01-31 22:17:11.562092  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=1 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=85308910…
   7 2020-01-31 22:17:11.562098  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=1419 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=85308…
   8 2020-01-31 22:17:11.562201  192.168.1.4     172.217.166.228 TCP           66 56704 → 80 [ACK] Seq=145 Ack=2837 Win=128448 Len=0 TSval=853089247 TSecr=32702772…
   9 2020-01-31 22:17:11.562265  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=2837 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=85308…
  10 2020-01-31 22:17:11.562329  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=4255 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=85308…
  11 2020-01-31 22:17:11.562401  192.168.1.4     172.217.166.228 TCP           66 56704 → 80 [ACK] Seq=145 Ack=5673 Win=126080 Len=0 TSval=853089247 TSecr=32702772…
  12 2020-01-31 22:17:11.562733  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=5673 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=85308…
  13 2020-01-31 22:17:11.562738  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=7091 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=85308…
  14 2020-01-31 22:17:11.562814  192.168.1.4     172.217.166.228 TCP           66 56704 → 80 [ACK] Seq=145 Ack=8509 Win=123264 Len=0 TSval=853089247 TSecr=32702772…
  15 2020-01-31 22:17:11.562971  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=8509 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=85308…
  16 2020-01-31 22:17:11.562976  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=9927 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=85308…
  17 2020-01-31 22:17:11.563072  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=11345 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=8530…
  18 2020-01-31 22:17:11.563079  172.217.166.228 192.168.1.4     TCP         1484 80 → 56704 [ACK] Seq=12763 Ack=145 Win=61440 Len=1418 TSval=3270277225 TSecr=8530…
  19 2020-01-31 22:17:11.563093  192.168.1.4     172.217.166.228 TCP           66 56704 → 80 [ACK] Seq=145 Ack=11345 Win=120448 Len=0 TSval=853089247 TSecr=3270277…
  20 2020-01-31 22:17:11.563149  192.168.1.4     172.217.166.228 TCP           66 56704 → 80 [ACK] Seq=145 Ack=14181 Win=117568 Len=0 TSval=853089247 TSecr=3270277…
  21 2020-01-31 22:17:11.564197  192.168.1.4     172.217.166.228 TCP           66 [TCP Window Update] 56704 → 80 [ACK] Seq=145 Ack=14181 Win=125760 Len=0 TSval=853…
  22 2020-01-31 22:17:11.564361  192.168.1.4     172.217.166.228 TCP           66 [TCP Window Update] 56704 → 80 [ACK] Seq=145 Ack=14181 Win=131072 Len=0 TSval=853…
  23 2020-01-31 22:17:11.598651  172.217.166.228 192.168.1.4     HTTP         840 HTTP/1.1 200 OK  (text/html)
  24 2020-01-31 22:17:11.598709  192.168.1.4     172.217.166.228 TCP           66 56704 → 80 [ACK] Seq=145 Ack=14955 Win=130240 Len=0 TSval=853089282 TSecr=3270277…
  25 2020-01-31 22:17:11.599808  192.168.1.4     172.217.166.228 TCP           66 56704 → 80 [FIN, ACK] Seq=145 Ack=14955 Win=131072 Len=0 TSval=853089283 TSecr=32…
  26 2020-01-31 22:17:11.634400  172.217.166.228 192.168.1.4     TCP           66 80 → 56704 [FIN, ACK] Seq=14955 Ack=146 Win=61440 Len=0 TSval=3270277297 TSecr=85…
  27 2020-01-31 22:17:11.634520  192.168.1.4     172.217.166.228 TCP           66 56704 → 80 [ACK] Seq=146 Ack=14956 Win=131072 Len=0 TSval=853089317 TSecr=3270277…
```

```
▶ Packet comments
▶ Frame 4: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_29:25:f2 (f8:ff:c2:29:25:f2), Dst: zte_b3:60:6e (8c:e1:17:b3:60:6e)
▶ Internet Protocol Version 4, Src: 192.168.1.4, Dst: 172.217.166.228
▶ Transmission Control Protocol, Src Port: 56704, Dst Port: 80, Seq: 1, Ack: 1, Len: 144
```

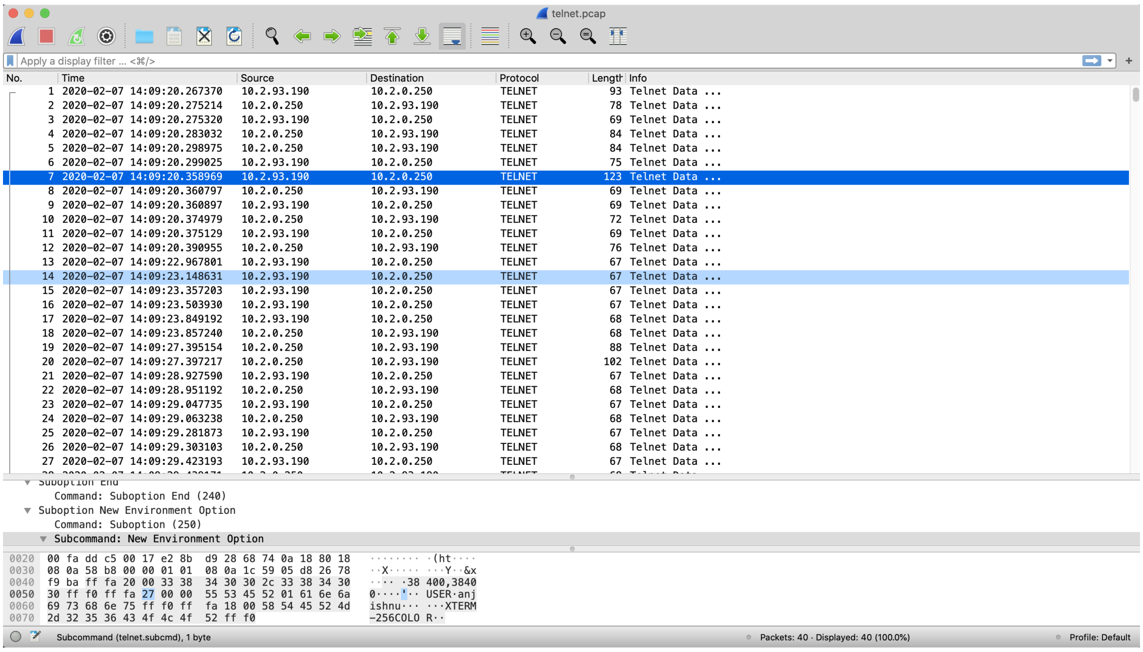
```
0000  8c e1 17 b3 60 6e f8 ff  c2 29 25 f2 08 00 45 00   ····`n·· ·)%···E·
0010  00 c4 00 00 40 00 40 06  24 ca c0 a8 01 04 ac d9   ····@·@· $·······
0020  a6 e4 dd 80 00 50 5a e5  cb 56 12 e1 b2 c1 80 18   ·····PZ· ·V······
0030  08 04 60 6e 00 00 01 01  08 0a 32 d9 1b 51 c2 ec   ··`n···· ··2··Q··
0040  77 dd 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   w·GET /  HTTP/1.1
0050  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 57 67   ··User-A gent: Wg
```

wget.pcapng · Packets: 27 · Displayed: 27 (100.0%) · Comments: 2 · Profile: Default

3b. Capture the packets while sending/receiving telnet request/response between your computer and a custom server running the telnet daemon. What is your observation while analysing the application layer data?

```
- telnet 10.2.0.250 (Username/Password : test/test)
- Packets between client and server are NOT encrypted using SSH
```

```
  or any other protocols.
- The only protocol being used is telnet which is not secured in any form.
```



telnet.pcap

Apply a display filter ... <⌘/>

```
No.   Time                        Source        Destination   Protocol  Length Info
    1 2020-02-07 14:09:20.267370  10.2.93.190   10.2.0.250    TELNET       93 Telnet Data ...
    2 2020-02-07 14:09:20.275214  10.2.0.250    10.2.93.190   TELNET       78 Telnet Data ...
    3 2020-02-07 14:09:20.275320  10.2.93.190   10.2.0.250    TELNET       69 Telnet Data ...
    4 2020-02-07 14:09:20.283032  10.2.0.250    10.2.93.190   TELNET       84 Telnet Data ...
    5 2020-02-07 14:09:20.298975  10.2.0.250    10.2.93.190   TELNET       84 Telnet Data ...
    6 2020-02-07 14:09:20.299025  10.2.93.190   10.2.0.250    TELNET       75 Telnet Data ...
    7 2020-02-07 14:09:20.358969  10.2.93.190   10.2.0.250    TELNET      123 Telnet Data ...
    8 2020-02-07 14:09:20.360797  10.2.0.250    10.2.93.190   TELNET       69 Telnet Data ...
    9 2020-02-07 14:09:20.360897  10.2.93.190   10.2.0.250    TELNET       69 Telnet Data ...
   10 2020-02-07 14:09:20.374979  10.2.0.250    10.2.93.190   TELNET       72 Telnet Data ...
   11 2020-02-07 14:09:20.375129  10.2.93.190   10.2.0.250    TELNET       69 Telnet Data ...
   12 2020-02-07 14:09:20.390955  10.2.0.250    10.2.93.190   TELNET       76 Telnet Data ...
   13 2020-02-07 14:09:22.967801  10.2.93.190   10.2.0.250    TELNET       67 Telnet Data ...
   14 2020-02-07 14:09:23.148631  10.2.93.190   10.2.0.250    TELNET       67 Telnet Data ...
   15 2020-02-07 14:09:23.357203  10.2.93.190   10.2.0.250    TELNET       67 Telnet Data ...
   16 2020-02-07 14:09:23.503930  10.2.93.190   10.2.0.250    TELNET       67 Telnet Data ...
   17 2020-02-07 14:09:23.849192  10.2.93.190   10.2.0.250    TELNET       68 Telnet Data ...
   18 2020-02-07 14:09:23.857240  10.2.0.250    10.2.93.190   TELNET       68 Telnet Data ...
   19 2020-02-07 14:09:27.395154  10.2.0.250    10.2.93.190   TELNET       88 Telnet Data ...
   20 2020-02-07 14:09:27.397217  10.2.0.250    10.2.93.190   TELNET      102 Telnet Data ...
   21 2020-02-07 14:09:28.927590  10.2.93.190   10.2.0.250    TELNET       67 Telnet Data ...
   22 2020-02-07 14:09:28.951192  10.2.0.250    10.2.93.190   TELNET       68 Telnet Data ...
   23 2020-02-07 14:09:29.047735  10.2.93.190   10.2.0.250    TELNET       67 Telnet Data ...
   24 2020-02-07 14:09:29.063238  10.2.0.250    10.2.93.190   TELNET       68 Telnet Data ...
   25 2020-02-07 14:09:29.281873  10.2.93.190   10.2.0.250    TELNET       67 Telnet Data ...
   26 2020-02-07 14:09:29.303103  10.2.0.250    10.2.93.190   TELNET       68 Telnet Data ...
   27 2020-02-07 14:09:29.423193  10.2.93.190   10.2.0.250    TELNET       67 Telnet Data ...
```

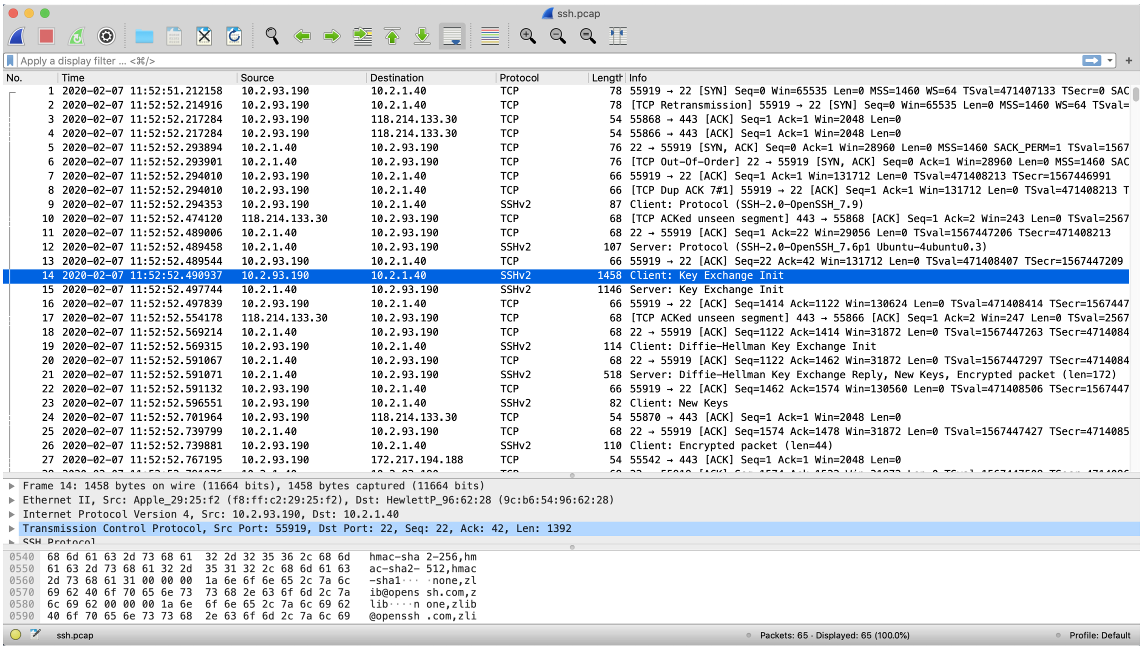
```
▼ Suboption End
      Command: Suboption End (240)
▼ Suboption New Environment Option
      Command: Suboption (250)
  ▼ Subcommand: New Environment Option
```

```
0020  00 fa dd c5 00 17 e2 8b  d9 28 68 74 0a 18 80 18   ········ ·(ht····
0030  08 0a 58 b8 00 00 01 01  08 0a 1c 59 05 d8 26 78   ··X····· ···Y··&x
0040  f9 ba ff fa 20 00 33 38  34 30 30 2c 33 38 34 30   ···· ·38 400,3840
0050  30 ff f0 ff fa 27 00 00  55 53 45 52 01 61 6e 6a   0····'·· USER·anj
0060  69 73 68 6e 75 ff f0 ff  fa 18 00 58 54 45 52 4d   ishnu··· ···XTERM
0070  2d 32 35 36 43 4f 4c 4f  52 ff f0                  -256COLO R··
```

Subcommand (telnet.subcmd), 1 byte   Packets: 40 · Displayed: 40 (100.0%)   Profile: Default

3c. Capture the packets while sending/receiving ssh request/response between your computer and one of the department servers. What is your observation while analysing the application layer data?

```
- Packets exchanged between the client and server are encrypted using SSHv2 based on
  OpenSSH 7.9
- The TLS protocol is used in the application layer.
```



ssh.pcap

Apply a display filter ... <⌘/>

```
No.   Time                        Source          Destination      Protocol  Length Info
    1 2020-02-07 11:52:51.212158  10.2.93.190     10.2.1.40        TCP          78 55919 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=471407133 TSecr=0 SAC
    2 2020-02-07 11:52:52.214916  10.2.93.190     10.2.1.40        TCP          78 [TCP Retransmission] 55919 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=
    3 2020-02-07 11:52:52.217284  10.2.93.190     118.214.133.30   TCP          54 55868 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
    4 2020-02-07 11:52:52.217284  10.2.93.190     118.214.133.30   TCP          54 55866 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
    5 2020-02-07 11:52:52.293894  10.2.1.40       10.2.93.190      TCP          76 22 → 55919 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1567
    6 2020-02-07 11:52:52.293901  10.2.1.40       10.2.93.190      TCP          76 [TCP Out-Of-Order] 22 → 55919 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SAC
    7 2020-02-07 11:52:52.294010  10.2.93.190     10.2.1.40        TCP          66 55919 → 22 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=471408213 TSecr=1567446991
    8 2020-02-07 11:52:52.294010  10.2.93.190     10.2.1.40        TCP          66 [TCP Dup ACK 7#1] 55919 → 22 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=471408213 T
    9 2020-02-07 11:52:52.294353  10.2.93.190     10.2.1.40        SSHv2        87 Client: Protocol (SSH-2.0-OpenSSH_7.9)
   10 2020-02-07 11:52:52.474120  118.214.133.30  10.2.93.190      TCP          68 [TCP ACKed unseen segment] 443 → 55868 [ACK] Seq=1 Ack=2 Win=243 Len=0 TSval=2567
   11 2020-02-07 11:52:52.489006  10.2.1.40       10.2.93.190      TCP          68 22 → 55919 [ACK] Seq=1 Ack=22 Win=29056 Len=0 TSval=1567447206 TSecr=471408213
   12 2020-02-07 11:52:52.489458  10.2.1.40       10.2.93.190      SSHv2       107 Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3)
   13 2020-02-07 11:52:52.489544  10.2.93.190     10.2.1.40        TCP          66 55919 → 22 [ACK] Seq=22 Ack=42 Win=131712 Len=0 TSval=471408407 TSecr=1567447209
   14 2020-02-07 11:52:52.490937  10.2.93.190     10.2.1.40        SSHv2      1458 Client: Key Exchange Init
   15 2020-02-07 11:52:52.497744  10.2.1.40       10.2.93.190      SSHv2      1146 Server: Key Exchange Init
   16 2020-02-07 11:52:52.497839  10.2.93.190     10.2.1.40        TCP          66 55919 → 22 [ACK] Seq=1414 Ack=1122 Win=130624 Len=0 TSval=471408414 TSecr=1567447
   17 2020-02-07 11:52:52.554178  118.214.133.30  10.2.93.190      TCP          68 [TCP ACKed unseen segment] 443 → 55866 [ACK] Seq=1 Ack=2 Win=247 Len=0 TSval=2567
   18 2020-02-07 11:52:52.569214  10.2.1.40       10.2.93.190      TCP          68 22 → 55919 [ACK] Seq=1122 Ack=1414 Win=31872 Len=0 TSval=1567447263 TSecr=4714084
   19 2020-02-07 11:52:52.569315  10.2.93.190     10.2.1.40        SSHv2       114 Client: Diffie-Hellman Key Exchange Init
   20 2020-02-07 11:52:52.591067  10.2.1.40       10.2.93.190      TCP          68 22 → 55919 [ACK] Seq=1122 Ack=1462 Win=31872 Len=0 TSval=1567447297 TSecr=4714084
   21 2020-02-07 11:52:52.591071  10.2.1.40       10.2.93.190      SSHv2       518 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)
   22 2020-02-07 11:52:52.591132  10.2.93.190     10.2.1.40        TCP          66 55919 → 22 [ACK] Seq=1462 Ack=1574 Win=130560 Len=0 TSval=471408506 TSecr=1567447
   23 2020-02-07 11:52:52.596551  10.2.93.190     10.2.1.40        SSHv2        82 Client: New Keys
   24 2020-02-07 11:52:52.701964  10.2.93.190     118.214.133.30   TCP          54 55870 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
   25 2020-02-07 11:52:52.739799  10.2.1.40       10.2.93.190      TCP          68 22 → 55919 [ACK] Seq=1574 Ack=1478 Win=31872 Len=0 TSval=1567447427 TSecr=4714085
   26 2020-02-07 11:52:52.739881  10.2.93.190     10.2.1.40        SSHv2       110 Client: Encrypted packet (len=44)
   27 2020-02-07 11:52:52.767195  10.2.93.190     172.217.194.188  TCP          54 55542 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
```

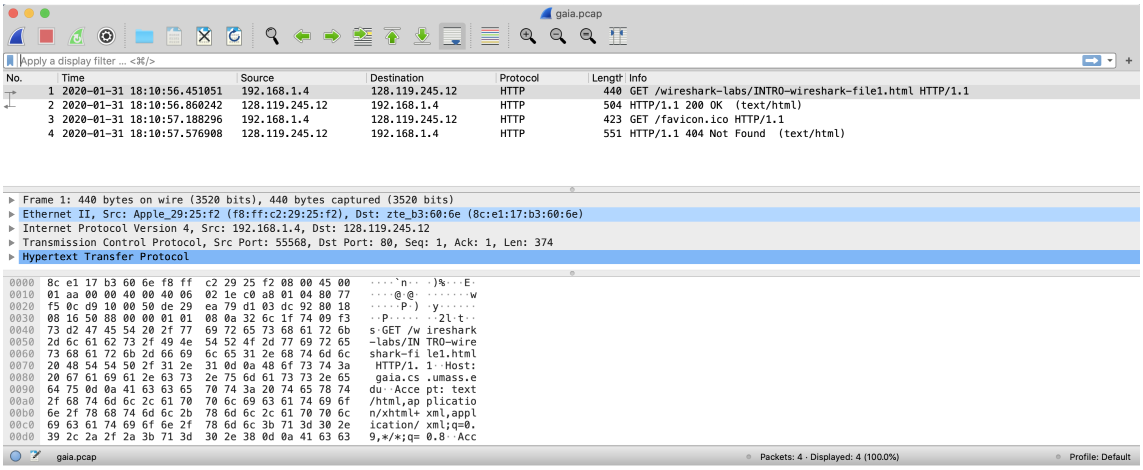
```
▶ Frame 14: 1458 bytes on wire (11664 bits), 1458 bytes captured (11664 bits)
▶ Ethernet II, Src: Apple_29:25:f2 (f8:ff:c2:29:25:f2), Dst: HewlettP_96:62:28 (9c:b6:54:96:62:28)
▶ Internet Protocol Version 4, Src: 10.2.93.190, Dst: 10.2.1.40
▶ Transmission Control Protocol, Src Port: 55919, Dst Port: 22, Seq: 22, Ack: 42, Len: 1392
▶ SSH Protocol
```

```
0540  68 6d 61 63 2d 73 68 61  32 2d 32 35 36 2c 68 6d   hmac-sha 2-256,hm
0550  61 63 2d 73 68 61 32 2d  35 31 32 2c 68 6d 61 63   ac-sha2- 512,hmac
0560  2d 73 68 61 31 00 00 00  1a 6e 6f 6e 65 2c 7a 6c   -sha1··· ·none,zl
0570  69 62 40 6f 70 65 6e 73  73 68 2e 63 6f 6d 2c 7a   ib@opens sh.com,z
0580  6c 69 62 00 00 00 1a 6e  6f 6e 65 2c 7a 6c 69 62   lib····n one,zlib
0590  40 6f 70 65 6e 73 73 68  2e 63 6f 6d 2c 7a 6c 69   @openssh .com,zli
```

ssh.pcap   Packets: 65 · Displayed: 65 (100.0%)   Profile: Default

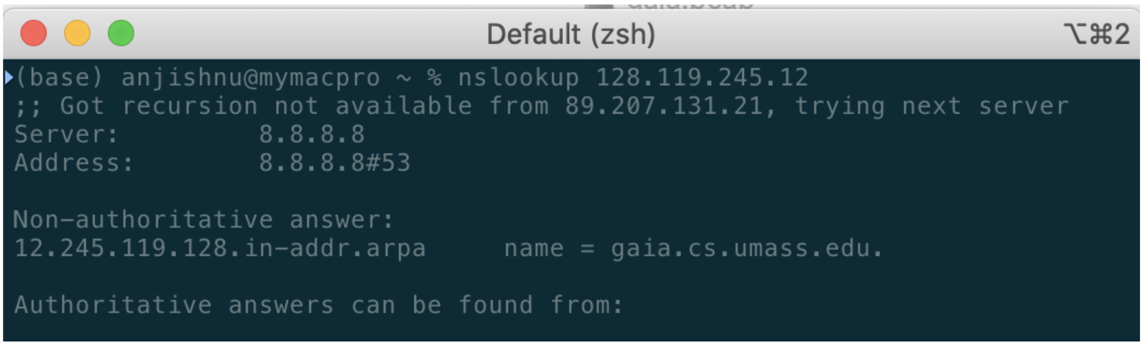
3d. Enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and capture packets using Wireshark. After your browser has displayed the INTRO-wireshark-file1.html page (it is a simple one line of congratulations), stop Wireshark packet capture. Answer the following from the packets captured:

```
- We use http filter for Wireshark capture.

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

    HTTP GET timestamp - Jan 31, 2020 18:10:56.451051000 IST
    HTTP OK timestamp - Jan 31, 2020 18:10:56.860242000 IST
    Time delta - 0.409191000 seconds
```



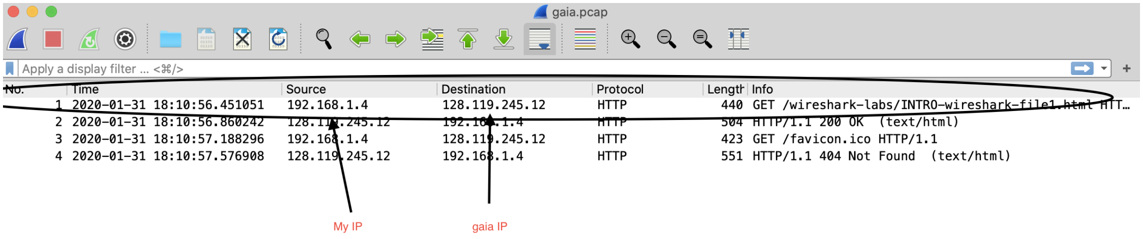
```
No.  Time                        Source          Destination     Protocol  Length Info
   1 2020-01-31 18:10:56.451051  192.168.1.4     128.119.245.12  HTTP         440 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   2 2020-01-31 18:10:56.860242  128.119.245.12  192.168.1.4     HTTP         504 HTTP/1.1 200 OK  (text/html)
   3 2020-01-31 18:10:57.188296  192.168.1.4     128.119.245.12  HTTP         423 GET /favicon.ico HTTP/1.1
   4 2020-01-31 18:10:57.576908  128.119.245.12  192.168.1.4     HTTP         551 HTTP/1.1 404 Not Found  (text/html)

▶ Frame 1: 440 bytes on wire (3520 bits), 440 bytes captured (3520 bits)
▶ Ethernet II, Src: Apple_29:25:f2 (f8:ff:c2:29:25:f2), Dst: zte_b3:60:6e (8c:e1:17:b3:60:6e)
▶ Internet Protocol Version 4, Src: 192.168.1.4, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 55568, Dst Port: 80, Seq: 1, Ack: 1, Len: 374
▶ Hypertext Transfer Protocol

0000  8c e1 17 b3 60 6e f8 ff  c2 29 25 f2 08 00 45 00   ····`n·· ·)%···E·
0010  01 aa 00 00 40 00 40 06  02 1e c0 a8 01 04 80 77   ····@·@· ·······w
0020  f5 0c d9 10 00 50 de 29  ea 79 d1 03 dc 92 80 18   ·····P·) ·y······
0030  08 16 50 88 00 00 01 01  08 0a 32 6c 1f 74 09 f3   ··P····· ··2l·t··
0040  73 d2 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   s·GET /w ireshark
0050  2d 6c 61 62 73 2f 49 4e  54 52 4f 2d 77 69 72 65   -labs/IN TRO-wire
0060  73 68 61 72 6b 2d 66 69  6c 65 31 2e 68 74 6d 6c   shark-fi le1.html
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0080  20 67 61 69 61 2e 63 73  2e 75 6d 61 73 73 2e 65    gaia.cs .umass.e
0090  64 75 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   du··Acce pt: text
00a0  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
00b0  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
00c0  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
00d0  39 2c 2a 2f 2a 3b 71 3d  30 2e 38 0d 0a 41 63 63   9,*/*;q= 0.8··Acc
```

```
(ii) What is the Internet address of the gaia.cs.umass.edu?
    What is the Internet address of your computer?
    Support your answer with an appropriate screenshot from your computer.

    IP of gaia.cs.umass.edu : 128.119.245.12
    Verfied further using nslookup.
    ---
    (base) anjishnu@mymacpro ~ % nslookup 128.119.245.12
    ;; Got recursion not available from 89.207.131.21, trying next server
    Server:   8.8.8.8
    Address: 8.8.8.8#53

    Non-authoritative answer:
    12.245.119.128.in-addr.arpa name = gaia.cs.umass.edu.
    ---
```



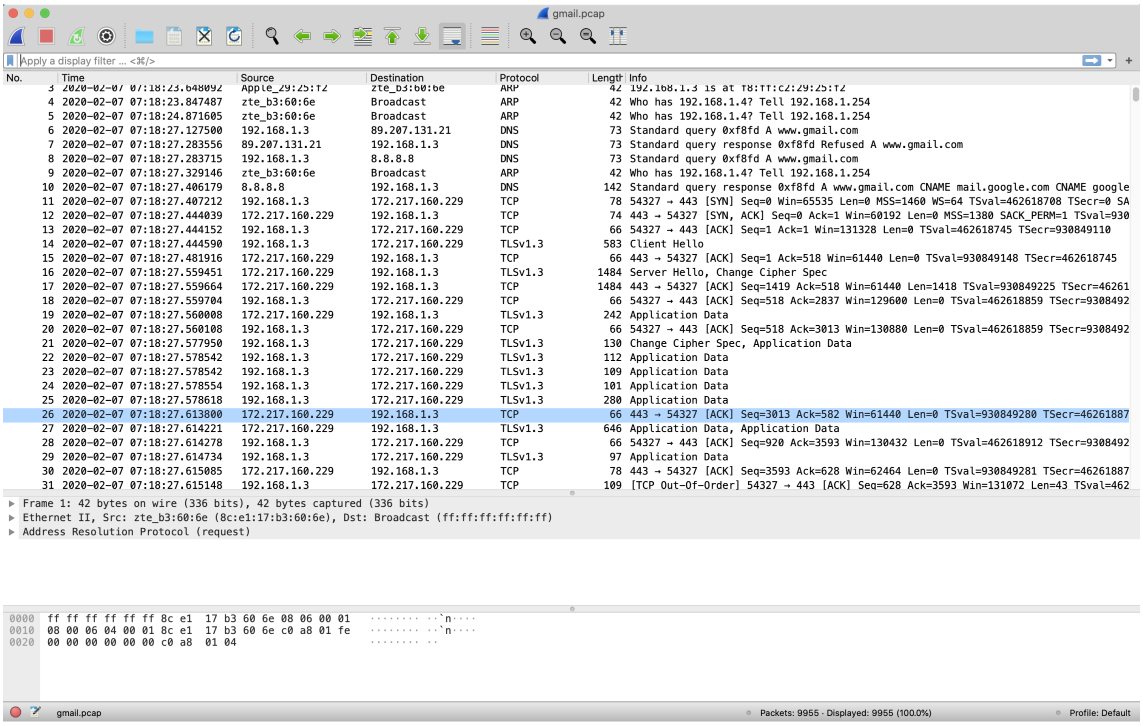
```
(base) anjishnu@mymacpro ~ % nslookup 128.119.245.12
;; Got recursion not available from 89.207.131.21, trying next server
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
12.245.119.128.in-addr.arpa     name = gaia.cs.umass.edu.

Authoritative answers can be found from:
```

```
IP of active promiscuous mode interface of my machine is 192.168.1.4

(Relevant screenshots attached with this document in submission email.)
```



```
No.  Time                        Source           Destination      Protocol  Length Info
  1  2020-01-31 18:10:56.451051  192.168.1.4      128.119.245.12   HTTP        440  GET /wireshark-labs/INTRO-wireshark-file1.html HTT…
  2  2020-01-31 18:10:56.860242  128.119.245.12   192.168.1.4      HTTP        504  HTTP/1.1 200 OK  (text/html)
  3  2020-01-31 18:10:57.188296  192.168.1.4      128.119.245.12   HTTP        423  GET /favicon.ico HTTP/1.1
  4  2020-01-31 18:10:57.576908  128.119.245.12   192.168.1.4      HTTP        551  HTTP/1.1 404 Not Found  (text/html)
```

3e. Start the Wireshark packet capturingservice. Enter the URL: https://www.gmail.com on your browser and sign-in to your gmail account by providing credentials (Username/Password). Answer the following from the captured packets:



```
No.  Time                        Source           Destination      Protocol  Length Info
  3  2020-02-07 07:18:23.648092  Apple_29:25:f2   zte_b3:60:6e     ARP         42  192.168.1.3 is at f8:ff:c2:29:25:f2
  4  2020-02-07 07:18:23.847487  zte_b3:60:6e     Broadcast        ARP         42  Who has 192.168.1.4? Tell 192.168.1.254
  5  2020-02-07 07:18:24.871605  zte_b3:60:6e     Broadcast        ARP         42  Who has 192.168.1.4? Tell 192.168.1.254
  6  2020-02-07 07:18:27.127500  192.168.1.3      89.207.131.21    DNS         73  Standard query 0xf8fd A www.gmail.com
  7  2020-02-07 07:18:27.283556  89.207.131.21    192.168.1.3      DNS         73  Standard query response 0xf8fd Refused A www.gmail.com
  8  2020-02-07 07:18:27.283715  192.168.1.3      8.8.8.8          DNS         73  Standard query 0xf8fd A www.gmail.com
  9  2020-02-07 07:18:27.329146  zte_b3:60:6e     Broadcast        ARP         42  Who has 192.168.1.4? Tell 192.168.1.254
 10  2020-02-07 07:18:27.406179  8.8.8.8          192.168.1.3      DNS        142  Standard query response 0xf8fd A www.gmail.com CNAME mail.google.com CNAME google
 11  2020-02-07 07:18:27.407212  192.168.1.3      172.217.160.229  TCP         78  54327 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=462618708 TSecr=0 SA
 12  2020-02-07 07:18:27.444039  172.217.160.229  192.168.1.3      TCP         74  443 → 54327 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=930
 13  2020-02-07 07:18:27.444152  192.168.1.3      172.217.160.229  TCP         66  54327 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=462618745 TSecr=930849110
 14  2020-02-07 07:18:27.444590  192.168.1.3      172.217.160.229  TLSv1.3    583  Client Hello
 15  2020-02-07 07:18:27.481916  172.217.160.229  192.168.1.3      TCP         66  443 → 54327 [ACK] Seq=1 Ack=518 Win=61440 Len=0 TSval=930849148 TSecr=462618745
 16  2020-02-07 07:18:27.559451  172.217.160.229  192.168.1.3      TLSv1.3   1484  Server Hello, Change Cipher Spec
 17  2020-02-07 07:18:27.559664  172.217.160.229  192.168.1.3      TCP       1484  443 → 54327 [ACK] Seq=1419 Ack=518 Win=61440 Len=1418 TSval=930849225 TSecr=46261
 18  2020-02-07 07:18:27.559704  192.168.1.3      172.217.160.229  TCP         66  54327 → 443 [ACK] Seq=518 Ack=2837 Win=129600 Len=0 TSval=462618859 TSecr=9308492
 19  2020-02-07 07:18:27.560008  172.217.160.229  192.168.1.3      TLSv1.3    242  Application Data
 20  2020-02-07 07:18:27.560108  192.168.1.3      172.217.160.229  TCP         66  54327 → 443 [ACK] Seq=518 Ack=3013 Win=130880 Len=0 TSval=462618859 TSecr=9308492
 21  2020-02-07 07:18:27.577950  192.168.1.3      172.217.160.229  TLSv1.3    130  Change Cipher Spec, Application Data
 22  2020-02-07 07:18:27.578542  192.168.1.3      172.217.160.229  TLSv1.3    112  Application Data
 23  2020-02-07 07:18:27.578542  192.168.1.3      172.217.160.229  TLSv1.3    109  Application Data
 24  2020-02-07 07:18:27.578554  192.168.1.3      172.217.160.229  TLSv1.3    101  Application Data
 25  2020-02-07 07:18:27.578618  192.168.1.3      172.217.160.229  TLSv1.3    280  Application Data
 26  2020-02-07 07:18:27.613800  172.217.160.229  192.168.1.3      TCP         66  443 → 54327 [ACK] Seq=3013 Ack=582 Win=61440 Len=0 TSval=930849280 TSecr=46261887
 27  2020-02-07 07:18:27.614221  172.217.160.229  192.168.1.3      TLSv1.3    646  Application Data, Application Data
 28  2020-02-07 07:18:27.614278  192.168.1.3      172.217.160.229  TCP         66  54327 → 443 [ACK] Seq=920 Ack=3593 Win=130432 Len=0 TSval=462618912 TSecr=9308492
 29  2020-02-07 07:18:27.614734  192.168.1.3      172.217.160.229  TLSv1.3     97  Application Data
 30  2020-02-07 07:18:27.615085  172.217.160.229  192.168.1.3      TCP         78  443 → 54327 [ACK] Seq=3593 Ack=628 Win=62464 Len=0 TSval=930849281 TSecr=46261887
 31  2020-02-07 07:18:27.615148  192.168.1.3      172.217.160.229  TCP        109  [TCP Out-Of-Order] 54327 → 443 [ACK] Seq=628 Ack=3593 Win=131072 Len=43 TSval=462

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▶ Ethernet II, Src: zte_b3:60:6e (8c:e1:17:b3:60:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 8c e1  17 b3 60 6e 08 06 00 01   ········ ··`n····
0010  08 00 06 04 00 01 8c e1  17 b3 60 6e c0 a8 01 fe   ········ ··`n····
0020  00 00 00 00 00 00 c0 a8  01 04                     ········ ··

gmail.pcap                                   Packets: 9955 · Displayed: 9955 (100.0%)      Profile: Default
```

```
i. Is there any difference in the application layer protocol?

   This URL uses HTTPS whereas for the previous question the URL used HTTP.
   Thus GMail application data is encrypted whereas for the previous question,
   we can directly see all the data captured from the packets as it was not secure.

ii. How it is different from the HTTP data you analysed in the above problem?

   The application data is encrypted using TLS protocol version 1.3 in this case.
   Whereas for the previous question, there was no encryption involved.
```