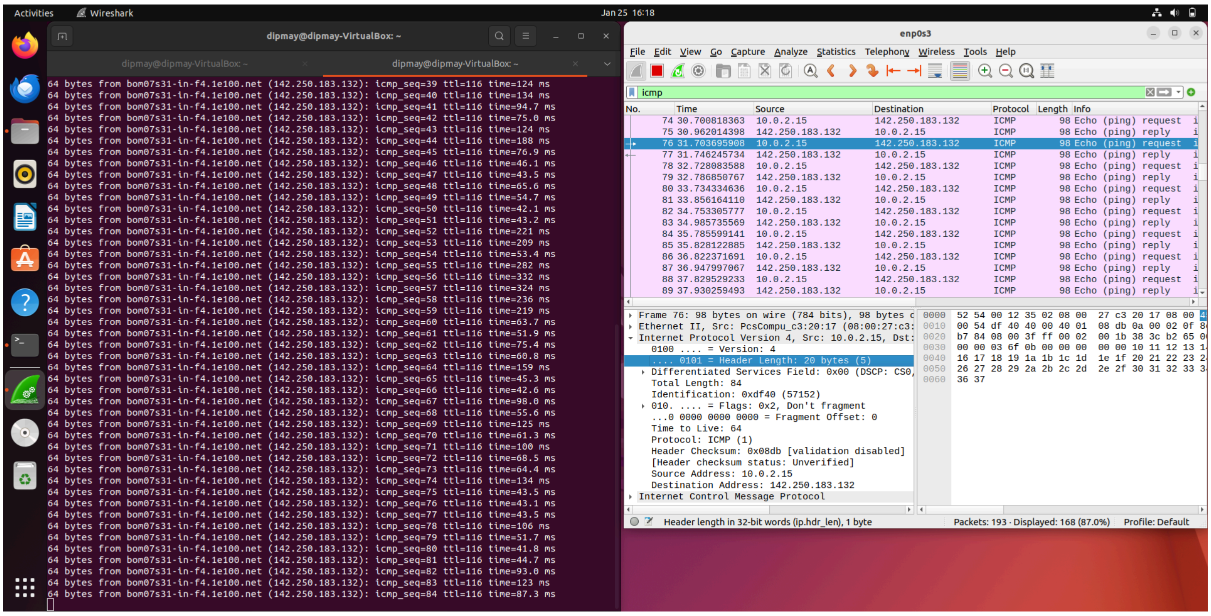
# *EXPLORING WIRESHARK TOOL*

**Dipmay Biswas (2021CSB043)**

Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands : (i) **ping**


Activities
Wireshark
Jan 25 16:18
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=39 ttl=116 time=124 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=40 ttl=116 time=134 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=41 ttl=116 time=94.7 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=42 ttl=116 time=75.0 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=43 ttl=116 time=124 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=44 ttl=116 time=188 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=45 ttl=116 time=76.9 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=46 ttl=116 time=46.1 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=47 ttl=116 time=43.5 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=48 ttl=116 time=65.6 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=49 ttl=116 time=54.7 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=50 ttl=116 time=42.1 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=51 ttl=116 time=43.2 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=52 ttl=116 time=221 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=53 ttl=116 time=209 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=54 ttl=116 time=53.4 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=55 ttl=116 time=282 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=56 ttl=116 time=332 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=57 ttl=116 time=324 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=58 ttl=116 time=236 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=59 ttl=116 time=219 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=60 ttl=116 time=63.7 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=61 ttl=116 time=51.9 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=62 ttl=116 time=75.4 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=63 ttl=116 time=60.8 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=64 ttl=116 time=159 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=65 ttl=116 time=45.3 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=66 ttl=116 time=42.6 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=67 ttl=116 time=98.0 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=68 ttl=116 time=55.6 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=69 ttl=116 time=125 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=70 ttl=116 time=61.3 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=71 ttl=116 time=100 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=72 ttl=116 time=68.5 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=73 ttl=116 time=64.4 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=74 ttl=116 time=134 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=75 ttl=116 time=43.5 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=76 ttl=116 time=43.1 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=77 ttl=116 time=43.5 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=78 ttl=116 time=106 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=79 ttl=116 time=51.7 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=80 ttl=116 time=41.8 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=81 ttl=116 time=44.7 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=82 ttl=116 time=93.0 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=83 ttl=116 time=123 ms
64 bytes from bom07s31-in-f4.1e100.net (142.250.183.132): icmp_seq=84 ttl=116 time=87.3 ms
```

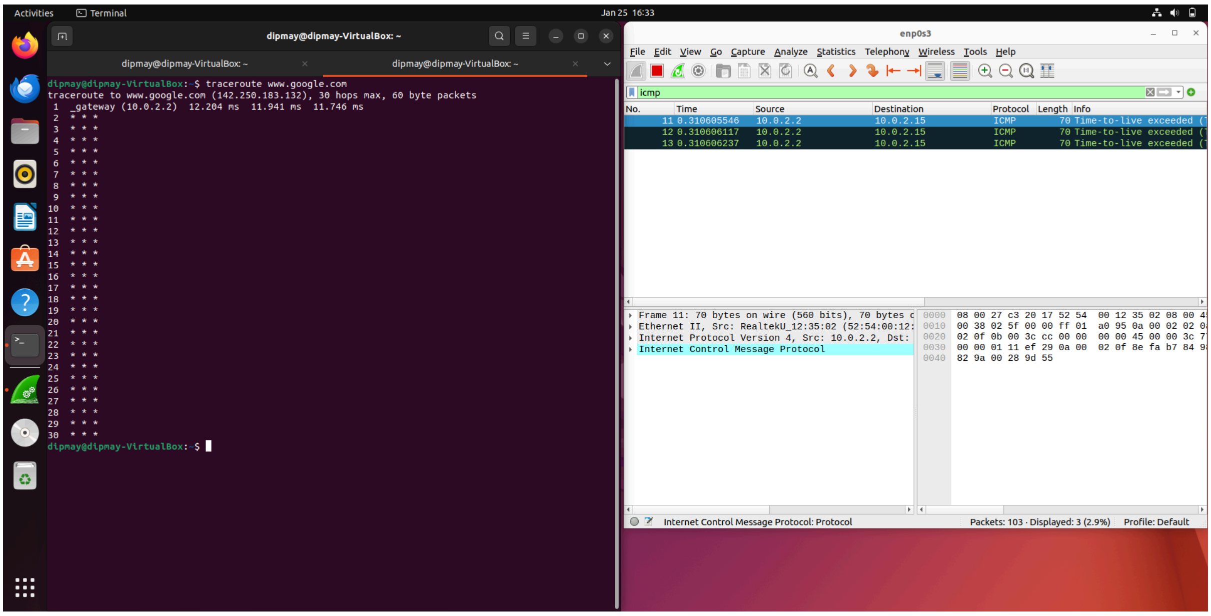
```
No.  Time          Source           Destination      Protocol Length Info
  74 30.700818363  10.0.2.15        142.250.183.132  ICMP       98 Echo (ping) request  i
  75 30.962014398  142.250.183.132  10.0.2.15        ICMP       98 Echo (ping) reply    i
  76 31.703695908  10.0.2.15        142.250.183.132  ICMP       98 Echo (ping) request  i
  77 31.746245734  142.250.183.132  10.0.2.15        ICMP       98 Echo (ping) reply    i
  78 32.728083588  10.0.2.15        142.250.183.132  ICMP       98 Echo (ping) request  i
  79 32.786850767  142.250.183.132  10.0.2.15        ICMP       98 Echo (ping) reply    i
  80 33.734334636  10.0.2.15        142.250.183.132  ICMP       98 Echo (ping) request  i
  81 33.856164110  142.250.183.132  10.0.2.15        ICMP       98 Echo (ping) reply    i
  82 34.753305777  10.0.2.15        142.250.183.132  ICMP       98 Echo (ping) request  i
  83 34.985735569  142.250.183.132  10.0.2.15        ICMP       98 Echo (ping) reply    i
  84 35.785599141  10.0.2.15        142.250.183.132  ICMP       98 Echo (ping) request  i
  85 35.828122885  142.250.183.132  10.0.2.15        ICMP       98 Echo (ping) reply    i
  86 36.822371691  10.0.2.15        142.250.183.132  ICMP       98 Echo (ping) request  i
  87 36.947997067  142.250.183.132  10.0.2.15        ICMP       98 Echo (ping) reply    i
  88 37.829529233  10.0.2.15        142.250.183.132  ICMP       98 Echo (ping) request  i
  89 37.930259493  142.250.183.132  10.0.2.15        ICMP       98 Echo (ping) reply    i
```

```
› Frame 76: 98 bytes on wire (784 bits), 98 bytes c
› Ethernet II, Src: PcsCompu_c3:20:17 (08:00:27:c3:
⌄ Internet Protocol Version 4, Src: 10.0.2.15, Dst:
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0,
    Total Length: 84
    Identification: 0xdf40 (57152)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x08db [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 142.250.183.132
› Internet Control Message Protocol
```

```
0000  52 54 00 12 35 02 08 00  27 c3 20 17 08 00 4
0010  00 54 df 40 40 00 40 01  08 db 0a 00 02 0f 8
0020  b7 84 08 00 3f ff 00 02  00 1b 38 3c b2 65 0
0030  00 00 03 6f 0b 00 00 00  00 00 10 11 12 13 1
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 2
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 3
0060  36 37
```

```
Header length in 32-bit words (ip.hdr_len), 1 byte    Packets: 193 · Displayed: 168 (87.0%)    Profile: Default
```

Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands : (ii) **traceroute**


Activities
Terminal
Jan 25 16:33
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
dipmay@dipmay-VirtualBox:~$ traceroute www.google.com
traceroute to www.google.com (142.250.183.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  12.204 ms  11.941 ms  11.746 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
dipmay@dipmay-VirtualBox:~$
```

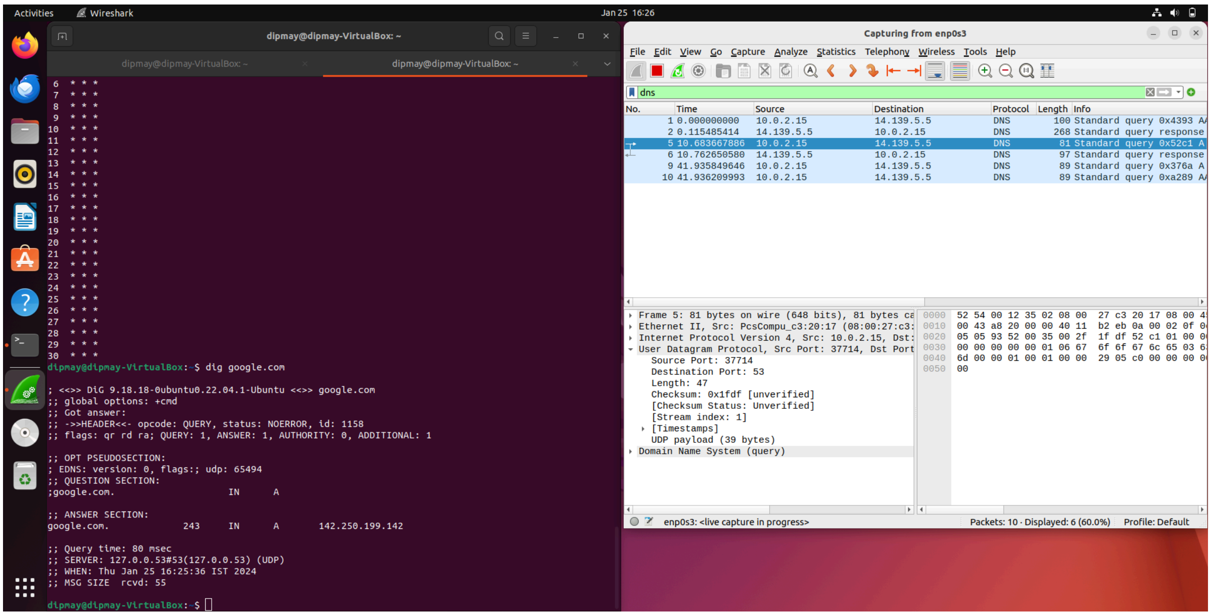
```
No.  Time         Source    Destination  Protocol Length Info
  11 0.310605546  10.0.2.2  10.0.2.15    ICMP       70 Time-to-live exceeded (
  12 0.310606117  10.0.2.2  10.0.2.15    ICMP       70 Time-to-live exceeded (
  13 0.310606237  10.0.2.2  10.0.2.15    ICMP       70 Time-to-live exceeded (
```

```
› Frame 11: 70 bytes on wire (560 bits), 70 bytes c
› Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:
› Internet Protocol Version 4, Src: 10.0.2.2, Dst:
› Internet Control Message Protocol
```

```
0000  08 00 27 c3 20 17 52 54  00 12 35 02 08 00 4
0010  00 38 02 5f 00 00 ff 01  a0 95 0a 00 02 02 0
0020  02 0f 0b 00 3c cc 00 00  00 00 45 00 00 3c 7
0030  00 00 01 11 ef 29 0a 00  02 0f 8e fa b7 84 9
0040  82 9a 00 28 9d 55
```

```
Internet Control Message Protocol: Protocol    Packets: 103 · Displayed: 3 (2.9%)    Profile: Default
```

Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands : (iii) **dig**


Activities
Wireshark
Jan 25 16:26
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
6  * * *
7  * * *
8  * * *
9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
dipmay@dipmay-VirtualBox:~$ dig google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1158
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             243     IN      A       142.250.199.142

;; Query time: 80 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Jan 25 16:25:36 IST 2024
;; MSG SIZE  rcvd: 55

dipmay@dipmay-VirtualBox:~$ 
```

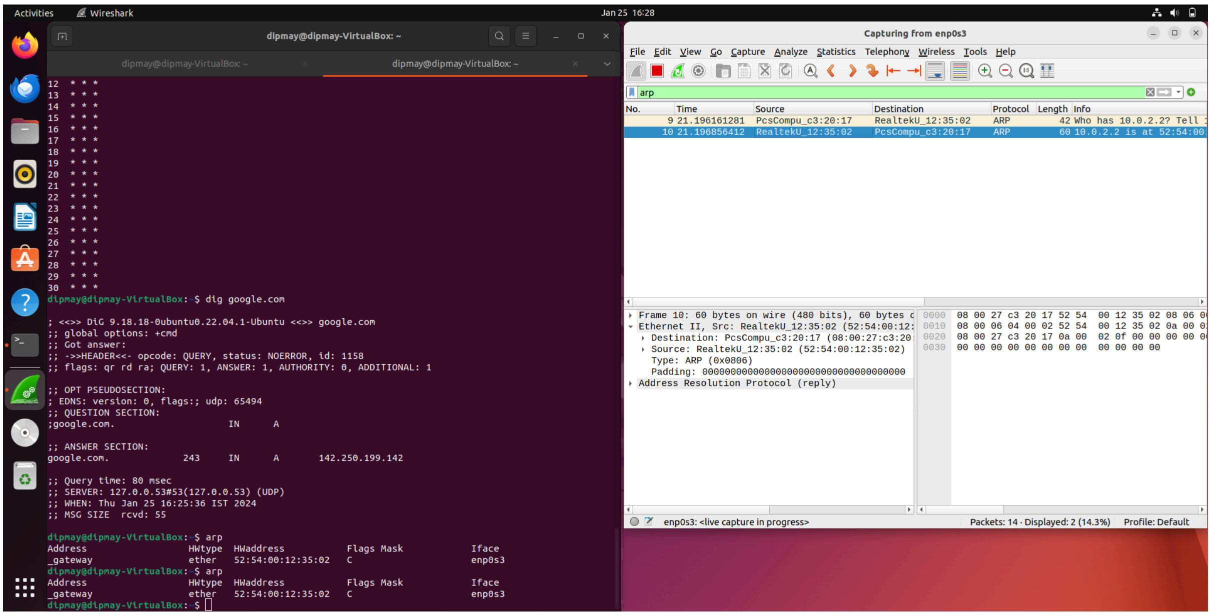
```
No.   Time          Source       Destination  Protocol Length Info
    1 0.000000000   10.0.2.15    14.139.5.5   DNS       100 Standard query 0x4393 AA
    2 0.115485414   14.139.5.5   10.0.2.15    DNS       268 Standard query response
    5 10.683667886  10.0.2.15    14.139.5.5   DNS        81 Standard query 0x52c1 A
    6 10.762650580  14.139.5.5   10.0.2.15    DNS        97 Standard query response
    9 41.935849646  10.0.2.15    14.139.5.5   DNS        89 Standard query 0x376a A
   10 41.936209993  10.0.2.15    14.139.5.5   DNS        89 Standard query 0xa289 AA
```

```
▸ Frame 5: 81 bytes on wire (648 bits), 81 bytes ca
▸ Ethernet II, Src: PcsCompu_c3:20:17 (08:00:27:c3:
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst:
▾ User Datagram Protocol, Src Port: 37714, Dst Port
    Source Port: 37714
    Destination Port: 53
    Length: 47
    Checksum: 0x1fdf [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  ▸ [Timestamps]
    UDP payload (39 bytes)
▸ Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 c3 20 17 08 00 4
0010  00 43 a8 20 00 00 40 11  b2 eb 0a 00 02 0f 0
0020  05 05 93 52 00 35 00 2f  1f df 52 c1 01 00 0
0030  00 00 00 00 00 01 06 67  6f 6f 67 6c 65 03 6
0040  6d 00 00 01 00 01 00 00  29 05 c0 00 00 00 0
0050  00
```

enp0s3: <live capture in progress>    Packets: 10 · Displayed: 6 (60.0%)    Profile: Default

Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands : (iv) **arp**


Activities
Wireshark
Jan 25 16:28
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
dipmay@dipmay-VirtualBox:~$ dig google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1158
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             243     IN      A       142.250.199.142

;; Query time: 80 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Jan 25 16:25:36 IST 2024
;; MSG SIZE  rcvd: 55

dipmay@dipmay-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:02   C                     enp0s3
dipmay@dipmay-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:02   C                     enp0s3
dipmay@dipmay-VirtualBox:~$ 
```

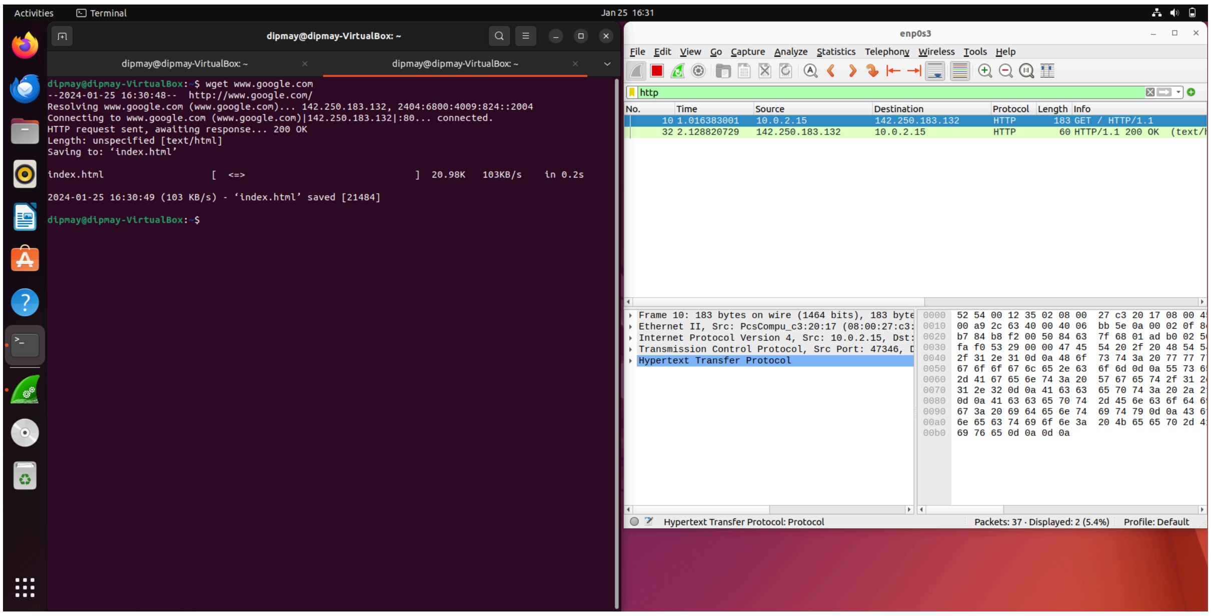
```
No.   Time          Source              Destination         Protocol Length Info
    9 21.196161281  PcsCompu_c3:20:17   RealtekU_12:35:02   ARP        42 Who has 10.0.2.2? Tell 1
   10 21.196856412  RealtekU_12:35:02   PcsCompu_c3:20:17   ARP        60 10.0.2.2 is at 52:54:00
```

```
▸ Frame 10: 60 bytes on wire (480 bits), 60 bytes c
▾ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:
  ▸ Destination: PcsCompu_c3:20:17 (08:00:27:c3:20
  ▸ Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▸ Address Resolution Protocol (reply)
```

```
0000  08 00 27 c3 20 17 52 54  00 12 35 02 08 06 0
0010  08 00 06 04 00 02 52 54  00 12 35 02 0a 00 0
0020  08 00 27 c3 20 17 0a 00  02 0f 00 00 00 00 0
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

enp0s3: <live capture in progress>    Packets: 14 · Displayed: 2 (14.3%)    Profile: Default

Q1) Analyse the packets (across all layers)exchanged with your computer while executing the following commands：(v) **wget**



```
dipmay@dipmay-VirtualBox:~$ wget www.google.com
--2024-01-25 16:30:48--  http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.183.132, 2404:6800:4009:824::2004
Connecting to www.google.com (www.google.com)|142.250.183.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html’

index.html                   [  <=>                              ]  20.98K   103KB/s    in 0.2s

2024-01-25 16:30:49 (103 KB/s) - ‘index.html’ saved [21484]

dipmay@dipmay-VirtualBox:~$
```

http

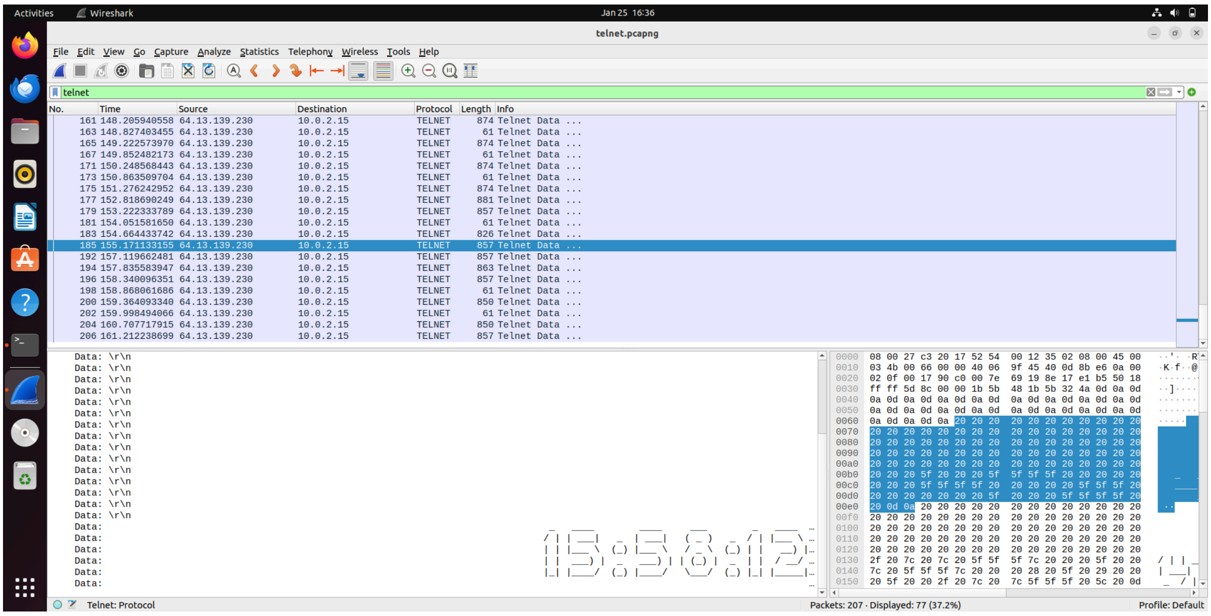
```
No.      Time         Source           Destination       Protocol  Length Info
      10 1.016383001  10.0.2.15        142.250.183.132   HTTP         183 GET / HTTP/1.1
      32 2.128820729  142.250.183.132  10.0.2.15         HTTP          60 HTTP/1.1 200 OK  (text/
```

```
▸ Frame 10: 183 bytes on wire (1464 bits), 183 byte
▸ Ethernet II, Src: PcsCompu_c3:20:17 (08:00:27:c3:
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst:
▸ Transmission Control Protocol, Src Port: 47346, D
▸ Hypertext Transfer Protocol
```

```
0000  52 54 00 12 35 02 08 00  27 c3 20 17 08 00
0010  00 a9 2c 63 40 00 40 06  bb 5e 0a 00 02 0f
0020  b7 84 b8 f2 00 50 84 63  7f 68 01 ad b0 02
0030  fa f0 53 29 00 00 47 45  54 20 2f 20 48 54
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73
0060  2d 41 67 65 6e 74 3a 20  57 67 65 74 2f 31
0070  31 2e 32 0d 0a 41 63 63  65 70 74 3a 20 2a
0080  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64
0090  67 3a 20 69 64 65 6e 74  69 74 79 0d 0a 43
00a0  6e 65 63 74 69 6f 6e 3a  20 4b 65 65 70 2d
00b0  69 76 65 0d 0a 0d 0a
```

Hypertext Transfer Protocol: Protocol    Packets: 37 · Displayed: 2 (5.4%)    Profile: Default

Q2) Capture the packets while sending/receiving telnet requests/responses between your computer and a custom server running the telnet daemon. What is your observation while analyzing the application layer data?



Activities
Wireshark
Jan 25 16:36
telnet.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

```
No.   Time          Source          Destination  Protocol Length Info
  161 148.205940558 64.13.139.230   10.0.2.15    TELNET    874 Telnet Data ...
  163 148.827403455 64.13.139.230   10.0.2.15    TELNET     61 Telnet Data ...
  165 149.222573970 64.13.139.230   10.0.2.15    TELNET    874 Telnet Data ...
  167 149.852482173 64.13.139.230   10.0.2.15    TELNET     61 Telnet Data ...
  171 150.248568443 64.13.139.230   10.0.2.15    TELNET    874 Telnet Data ...
  173 150.863509704 64.13.139.230   10.0.2.15    TELNET     61 Telnet Data ...
  175 151.276242952 64.13.139.230   10.0.2.15    TELNET    874 Telnet Data ...
  177 152.818690249 64.13.139.230   10.0.2.15    TELNET    881 Telnet Data ...
  179 153.222333789 64.13.139.230   10.0.2.15    TELNET    857 Telnet Data ...
  181 154.051581650 64.13.139.230   10.0.2.15    TELNET     61 Telnet Data ...
  183 154.664433742 64.13.139.230   10.0.2.15    TELNET    826 Telnet Data ...
  185 155.171133155 64.13.139.230   10.0.2.15    TELNET    857 Telnet Data ...
  192 157.119662481 64.13.139.230   10.0.2.15    TELNET    857 Telnet Data ...
  194 157.835583947 64.13.139.230   10.0.2.15    TELNET    863 Telnet Data ...
  196 158.340096351 64.13.139.230   10.0.2.15    TELNET    857 Telnet Data ...
  198 158.868061686 64.13.139.230   10.0.2.15    TELNET     61 Telnet Data ...
  200 159.364093340 64.13.139.230   10.0.2.15    TELNET    850 Telnet Data ...
  202 159.998494066 64.13.139.230   10.0.2.15    TELNET     61 Telnet Data ...
  204 160.707717915 64.13.139.230   10.0.2.15    TELNET    850 Telnet Data ...
  206 161.212238699 64.13.139.230   10.0.2.15    TELNET    857 Telnet Data ...
```

```
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data: \r\n
    Data:                      _  ____     ____    ___     _  ____  …
    Data:                     / | | ___|  _ | ___|  ( _ )  _ / | |___ \ …
    Data:                     | | |___ \ (_) |___ \  / _ \ (_) | |  __) |…
    Data:                     | |  ___) | _  ___) || (_) | _  | | / __/ …
    Data:                     |_| |____/ (_) |____/  \___/ (_) |_| |_____|…
    Data:                                                                …
```

```
0000  08 00 27 c3 20 17 52 54  00 12 35 02 08 00 45 00   ··'· ·RT
0010  03 4b 00 66 00 00 40 06  9f 45 40 0d 8b e6 0a 00   ·K·f··@·
0020  02 0f 00 17 90 c0 00 7e  69 19 8e 17 e1 b5 50 18   ········
0030  ff ff 5d 8c 00 00 1b 5b  48 1b 5b 32 4a 0d 0a 0d   ··]·····
0040  0a 0d 0a 0d 0a 0d 0a 0d  0a 0d 0a 0d 0a 0d 0a 0d   ········
0050  0a 0d 0a 0d 0a 0d 0a 0d  0a 0d 0a 0d 0a 0d 0a 0d   ········
0060  0a 0d 0a 0d 0a 20 20 20  20 20 20 20 20 20 20 20   ·····
0070  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0080  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0090  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00a0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00b0  20 20 20 5f 20 20 20 5f  5f 5f 5f 20 20 20 20 20      _   _
00c0  20 20 20 5f 5f 5f 5f 20  20 20 20 20 5f 5f 5f 20      ____
00d0  20 20 20 20 20 20 20 5f  20 20 20 5f 5f 5f 5f 20          _
00e0  20 0d 0a 20 20 20 20 20  20 20 20 20 20 20 20 20    ··
00f0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0100  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0110  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0120  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0130  2f 20 7c 20 7c 20 5f 5f  5f 7c 20 20 20 5f 20 20   / | | _
0140  7c 20 5f 5f 5f 7c 20 20  20 28 20 5f 20 29 20 20   | ___|
0150  20 5f 20 20 2f 20 7c 20  7c 5f 5f 5f 20 5c 20 0d    _  / |
```

Telnet: Protocol

Packets: 207 · Displayed: 77 (37.2%)

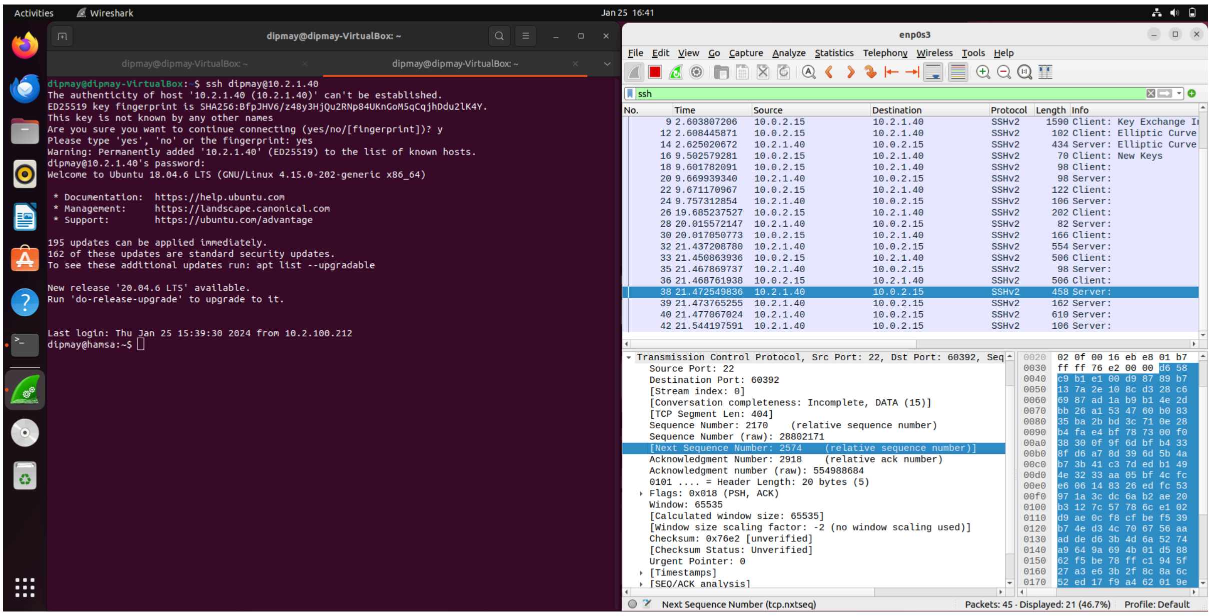
Profile: Default

TCP protocols follow 3-way handshaking.

Port Number for Telnet：23

The application layer is **unsecured** as no key exchange mechanism is present like ssh.

Q3) Capture the packets while sending/receiving ssh requests/responses between your computer and one of the department servers. What is your observation while analyzing the application layer data?



Activities
Wireshark
Jan 25 16:41
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
dipmay@dipmay-VirtualBox: ~
enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssh

```
dipmay@dipmay-VirtualBox:~$ ssh dipmay@10.2.1.40
The authenticity of host '10.2.1.40 (10.2.1.40)' can't be established.
ED25519 key fingerprint is SHA256:BfpJHV6/z48y3HjQu2RNp84UKnGoM5qCqjhDdu2lK4Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.2.1.40' (ED25519) to the list of known hosts.
dipmay@10.2.1.40's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-202-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

195 updates can be applied immediately.
162 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Thu Jan 25 15:39:30 2024 from 10.2.100.212
dipmay@hamsa:~$ 
```

```
No.   Time          Source      Destination  Protocol  Length Info
    9 2.603807206   10.0.2.15   10.2.1.40    SSHv2     1590 Client: Key Exchange In
   12 2.608445871   10.0.2.15   10.2.1.40    SSHv2      102 Client: Elliptic Curve
   14 2.625020672   10.2.1.40   10.0.2.15    SSHv2      434 Server: Elliptic Curve
   16 9.502579281   10.0.2.15   10.2.1.40    SSHv2       70 Client: New Keys
   18 9.601782091   10.0.2.15   10.2.1.40    SSHv2       98 Client:
   20 9.669939340   10.2.1.40   10.0.2.15    SSHv2       98 Server:
   22 9.671170967   10.0.2.15   10.2.1.40    SSHv2      122 Client:
   24 9.757312854   10.2.1.40   10.0.2.15    SSHv2      106 Server:
   26 19.685237527  10.0.2.15   10.2.1.40    SSHv2      202 Client:
   28 20.015572147  10.2.1.40   10.0.2.15    SSHv2       82 Server:
   30 20.017050773  10.0.2.15   10.2.1.40    SSHv2      166 Client:
   32 21.437208780  10.2.1.40   10.0.2.15    SSHv2      554 Server:
   33 21.450863936  10.0.2.15   10.2.1.40    SSHv2      506 Client:
   35 21.467869737  10.2.1.40   10.0.2.15    SSHv2       98 Server:
   36 21.468761938  10.0.2.15   10.2.1.40    SSHv2      506 Client:
   38 21.472549836  10.2.1.40   10.0.2.15    SSHv2      458 Server:
   39 21.473765255  10.2.1.40   10.0.2.15    SSHv2      162 Server:
   40 21.477067024  10.2.1.40   10.0.2.15    SSHv2      610 Server:
   42 21.544197591  10.2.1.40   10.0.2.15    SSHv2      106 Server:
```

```
Transmission Control Protocol, Src Port: 22, Dst Port: 60392, Seq
    Source Port: 22
    Destination Port: 60392
    [Stream index: 0]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 404]
    Sequence Number: 2170    (relative sequence number)
    Sequence Number (raw): 28802171
    [Next Sequence Number: 2574    (relative sequence number)]
    Acknowledgment Number: 2918    (relative ack number)
    Acknowledgment number (raw): 554988684
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x76e2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
```

```
0020  02 0f 00 16 eb e8 01 b7
0030  ff ff 76 e2 00 00 d6 58
0040  c9 b1 e1 00 d9 87 89 b7
0050  13 7a 2e 10 8c d3 28 c6
0060  69 87 ad 1a b9 b1 4e 2d
0070  bb 26 a1 53 47 60 b0 83
0080  35 ba 2b bd 3c 71 0e 28
0090  b4 fa e4 bf 78 73 00 f0
00a0  38 30 0f 9f 6d bf b4 33
00b0  8f d6 a7 8d 39 6d 5b 4a
00c0  b7 3b 41 c3 7d ed b1 49
00d0  4e 32 33 aa 05 bf 4c fc
00e0  e6 06 14 83 26 ed fc 53
00f0  97 1a 3c dc 6a b2 ae 20
0100  b3 12 7c 57 78 6c e1 02
0110  d9 ae 0c f8 cf be f5 39
0120  b7 4e d3 4c 70 67 56 aa
0130  ad de d6 3b 4d 6a 52 74
0140  a9 64 9a 69 4b 01 d5 88
0150  62 f5 be 78 ff c1 94 5f
0160  27 a3 e6 3b 2f 8c 8a 6c
0170  52 ed 17 f9 a4 62 01 9e
```

Next Sequence Number (tcp.nxtseq)    Packets: 45 · Displayed: 21 (46.7%)    Profile: Default

Port Number for ssh : 22

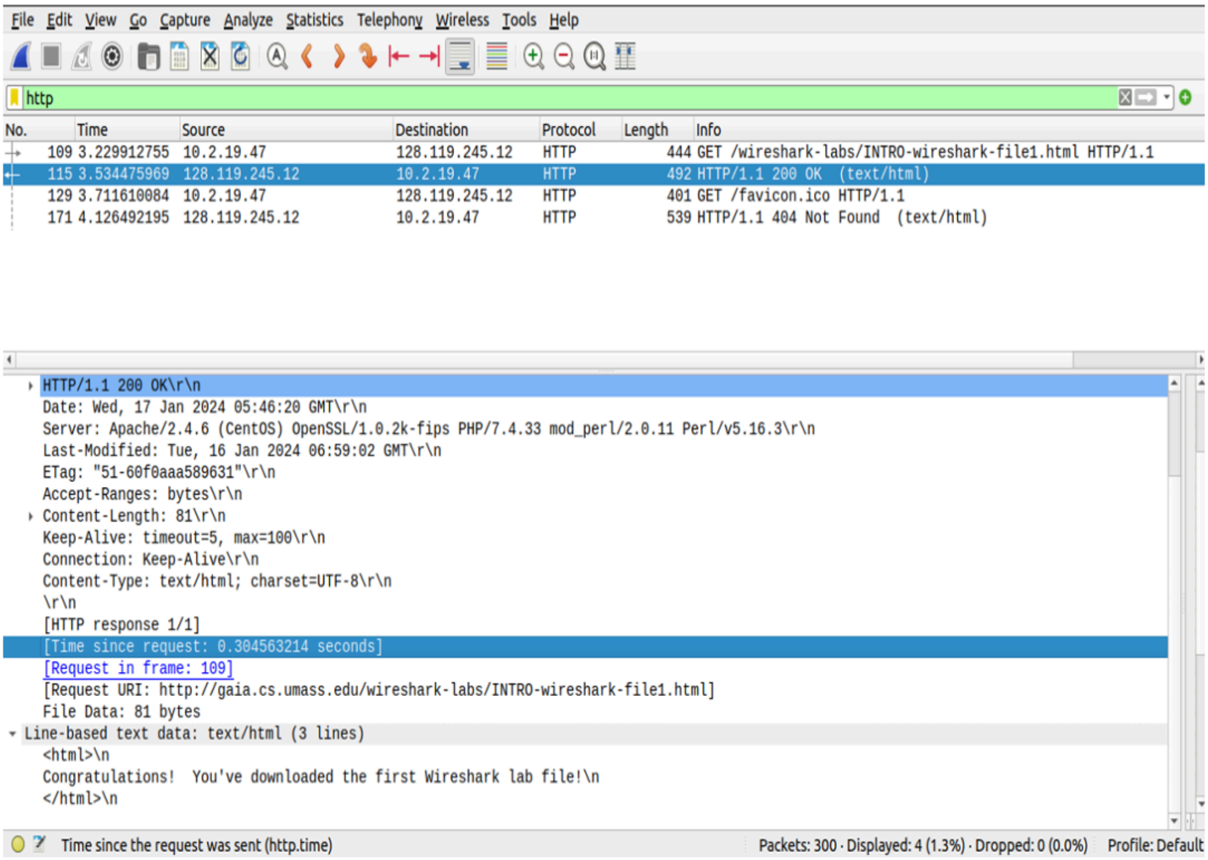
It is used for remote login.

It is much more **secure** in comparison to telnet.

Key exchange occurs and then proceeds.

Elliptic Curve Diffie − HellmanKey Exchange

.Q4) Enter the URL : *http://gaia.cs.umass.edu/wireshark − labs/INTRO − wireshark − file*1*.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.



http

```
No.  Time         Source          Destination     Protocol Length Info
 109 3.229912755  10.2.19.47      128.119.245.12  HTTP       444 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 115 3.534475969  128.119.245.12  10.2.19.47      HTTP       492 HTTP/1.1 200 OK  (text/html)
 129 3.711610084  10.2.19.47      128.119.245.12  HTTP       401 GET /favicon.ico HTTP/1.1
 171 4.126492195  128.119.245.12  10.2.19.47      HTTP       539 HTTP/1.1 404 Not Found  (text/html)
```

```
  ▸ HTTP/1.1 200 OK\r\n
    Date: Wed, 17 Jan 2024 05:46:20 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 16 Jan 2024 06:59:02 GMT\r\n
    ETag: "51-60f0aaa589631"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.304563214 seconds]
    [Request in frame: 109]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
▾ Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```

Time since the request was sent (http.time)    Packets: 300 · Displayed: 4 (1.3%) · Dropped: 0 (0.0%)    Profile: Default

Answer the following from the captured packets :
(a) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

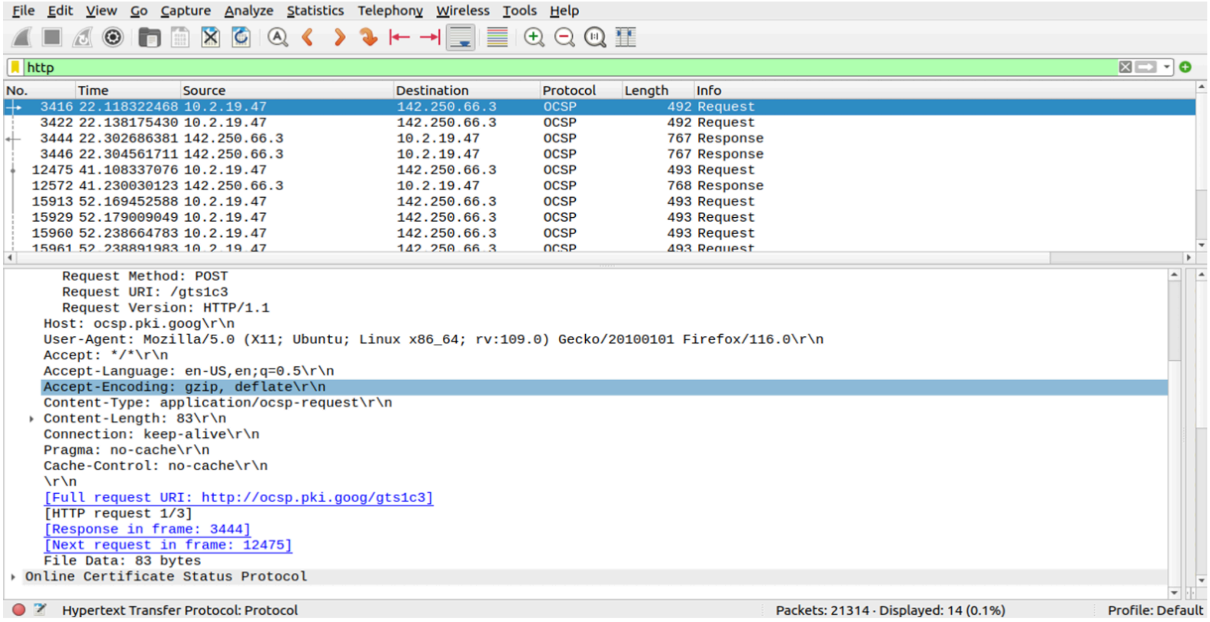
Ans) **0.304563214 sec.**

(b) 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.

Ans) **128.119.245.12** & **10.2.19.47**

Q5) Start the Wireshark packet capturing service. 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：


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time         Source         Destination    Protocol  Length Info
 3416 22.118322468 10.2.19.47     142.250.66.3   OCSP         492 Request
 3422 22.138175430 10.2.19.47     142.250.66.3   OCSP         492 Request
 3444 22.302686381 142.250.66.3   10.2.19.47     OCSP         767 Response
 3446 22.304561711 142.250.66.3   10.2.19.47     OCSP         767 Response
12475 41.108337076 10.2.19.47     142.250.66.3   OCSP         493 Request
12572 41.230030123 142.250.66.3   10.2.19.47     OCSP         768 Response
15913 52.169452588 10.2.19.47     142.250.66.3   OCSP         493 Request
15929 52.179009049 10.2.19.47     142.250.66.3   OCSP         493 Request
15960 52.238664783 10.2.19.47     142.250.66.3   OCSP         493 Request
15961 52.238891983 10.2.19.47     142.250.66.3   OCSP         493 Request
```

```
      Request Method: POST
      Request URI: /gts1c3
      Request Version: HTTP/1.1
   Host: ocsp.pki.goog\r\n
   User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0\r\n
   Accept: */*\r\n
   Accept-Language: en-US,en;q=0.5\r\n
   Accept-Encoding: gzip, deflate\r\n
   Content-Type: application/ocsp-request\r\n
 ▸ Content-Length: 83\r\n
   Connection: keep-alive\r\n
   Pragma: no-cache\r\n
   Cache-Control: no-cache\r\n
   \r\n
   [Full request URI: http://ocsp.pki.goog/gts1c3]
   [HTTP request 1/3]
   [Response in frame: 3444]
   [Next request in frame: 12475]
   File Data: 83 bytes
▸ Online Certificate Status Protocol
```

Hypertext Transfer Protocol: Protocol    Packets: 21314 · Displayed: 14 (0.1%)    Profile: Default

(a) Is there any difference in the application layer protocol?

Ans) **Yes!!**

(b) How is it different from the HTTP data you analyzed in the above problem?

Ans) **It is much more secure than HTTP protocol as it uses OCSP.**