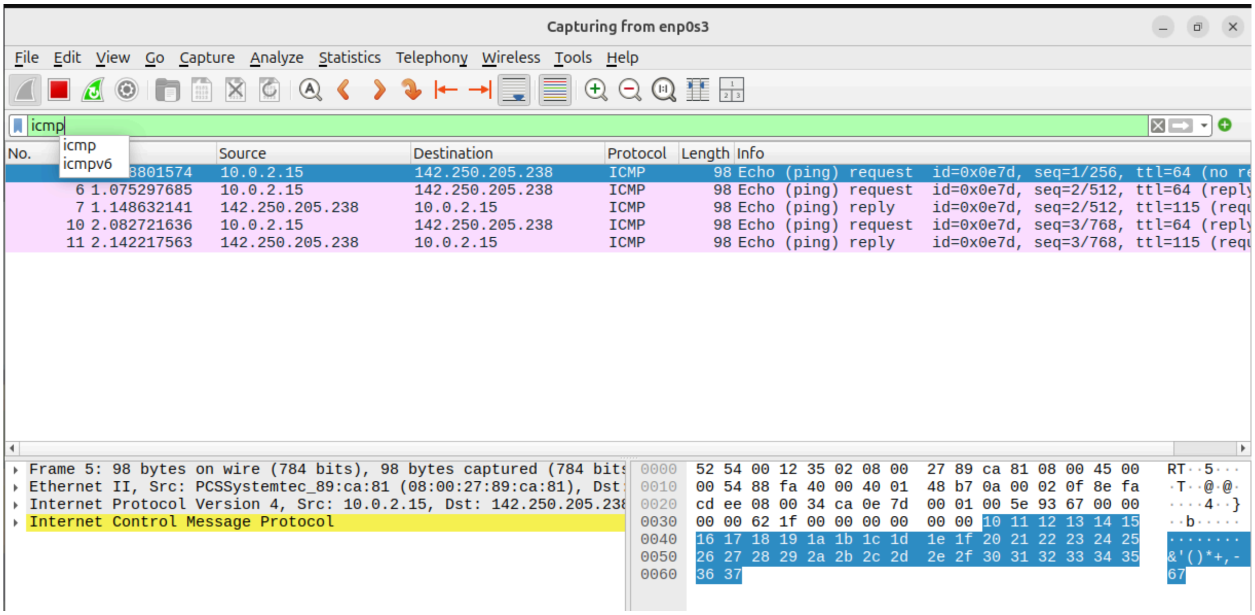
Assignment 2: Exploring Wireshark tool

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

Ping uses the ICMP protocol to send echo requests and receive echo replies to/from the target host to test connectivity between hosts.


Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmp
icmpv6

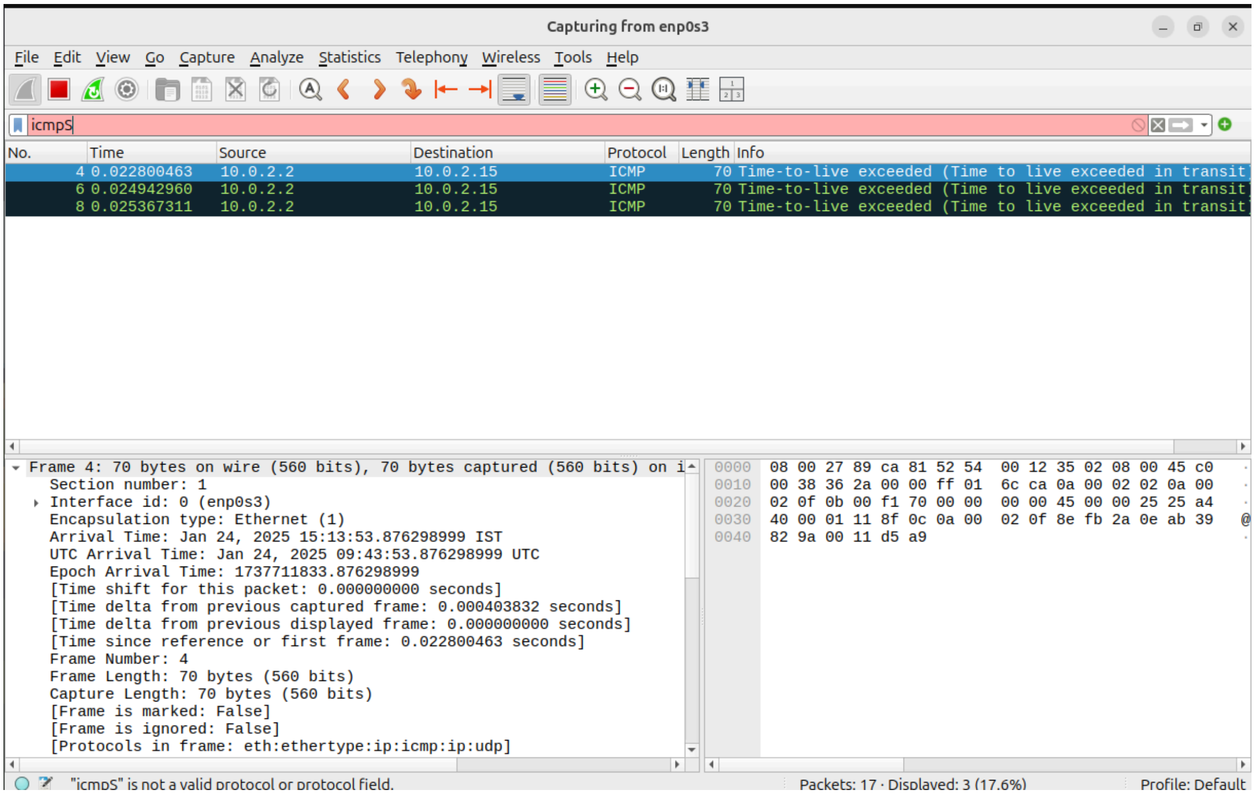
```
No.   Time          Source           Destination      Protocol Length Info
    5 ...3801574    10.0.2.15        142.250.205.238  ICMP       98 Echo (ping) request  id=0x0e7d, seq=1/256, ttl=64 (no re
    6 1.075297685   10.0.2.15        142.250.205.238  ICMP       98 Echo (ping) request  id=0x0e7d, seq=2/512, ttl=64 (reply
    7 1.148632141   142.250.205.238  10.0.2.15        ICMP       98 Echo (ping) reply    id=0x0e7d, seq=2/512, ttl=115 (requ
   10 2.082721636   10.0.2.15        142.250.205.238  ICMP       98 Echo (ping) request  id=0x0e7d, seq=3/768, ttl=64 (reply
   11 2.142217563   142.250.205.238  10.0.2.15        ICMP       98 Echo (ping) reply    id=0x0e7d, seq=3/768, ttl=115 (requ
```

```
› Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits
› Ethernet II, Src: PCSSystemtec_89:ca:81 (08:00:27:89:ca:81), Dst:
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.205.238
› Internet Control Message Protocol
```

```
0000  52 54 00 12 35 02 08 00  27 89 ca 81 08 00 45 00   RT··5···
0010  00 54 88 fa 40 00 40 01  48 b7 0a 00 02 0f 8e fa   ·T··@·@·
0020  cd ee 08 00 34 ca 0e 7d  00 01 00 5e 93 67 00 00   ····4··}
0030  00 00 62 1f 00 00 00 00  00 00 10 11 12 13 14 15   ··b·····
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-
0060  36 37                                              67
```

(ii) traceroute

Traceroute identifies the path packets take to reach the destination, using UDP or ICMP depending on the system configuration.The traceroute successfully mapped the routers between the local machine and the destination.


Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpS

```
No.     Time          Source        Destination   Protocol Length Info
      4 0.022800463   10.0.2.2      10.0.2.15     ICMP         70 Time-to-live exceeded (Time to live exceeded in transit
      6 0.024942960   10.0.2.2      10.0.2.15     ICMP         70 Time-to-live exceeded (Time to live exceeded in transit
      8 0.025367311   10.0.2.2      10.0.2.15     ICMP         70 Time-to-live exceeded (Time to live exceeded in transit
```

```
▾ Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on i
    Section number: 1
  ▸ Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2025 15:13:53.876298999 IST
    UTC Arrival Time: Jan 24, 2025 09:43:53.876298999 UTC
    Epoch Arrival Time: 1737711833.876298999
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000403832 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.022800463 seconds]
    Frame Number: 4
    Frame Length: 70 bytes (560 bits)
    Capture Length: 70 bytes (560 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:ip:udp]
```

```
0000  08 00 27 89 ca 81 52 54  00 12 35 02 08 00 45 c0   ·
0010  00 38 36 2a 00 00 ff 01  6c ca 0a 00 02 02 0a 00   ·
0020  02 0f 0b 00 f1 70 00 00  00 00 45 00 00 25 25 a4   ·
0030  40 00 01 11 8f 0c 0a 00  02 0f 8e fb 2a 0e ab 39   @
0040  82 9a 00 11 d5 a9                                  ·
```

"icmpS" is not a valid protocol or protocol field.

Packets: 17 · Displayed: 3 (17.6%)

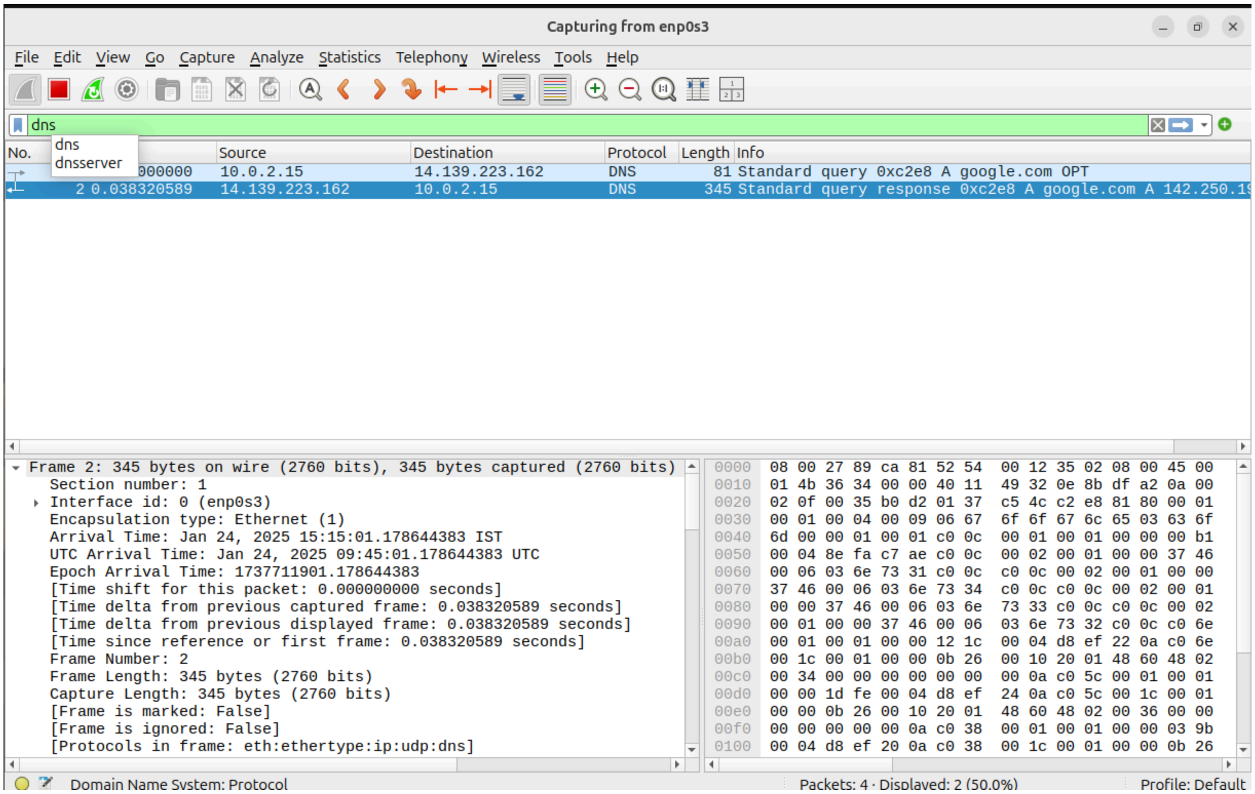
Profile: Default

(iii) dig

The dig command is used for querying dns records.

Query and Response Time: The delay between the query and response packets can be used to measure DNS resolution time.

Resolved IPs: The IP address(es) corresponding to google.com help understand the destination for subsequent connections.


Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
dns
dnsserver
No.            Source            Destination       Protocol Length Info
      000000   10.0.2.15         14.139.223.162    DNS          81 Standard query 0xc2e8 A google.com OPT
    2 0.038320589 14.139.223.162 10.0.2.15         DNS         345 Standard query response 0xc2e8 A google.com A 142.250.19
```

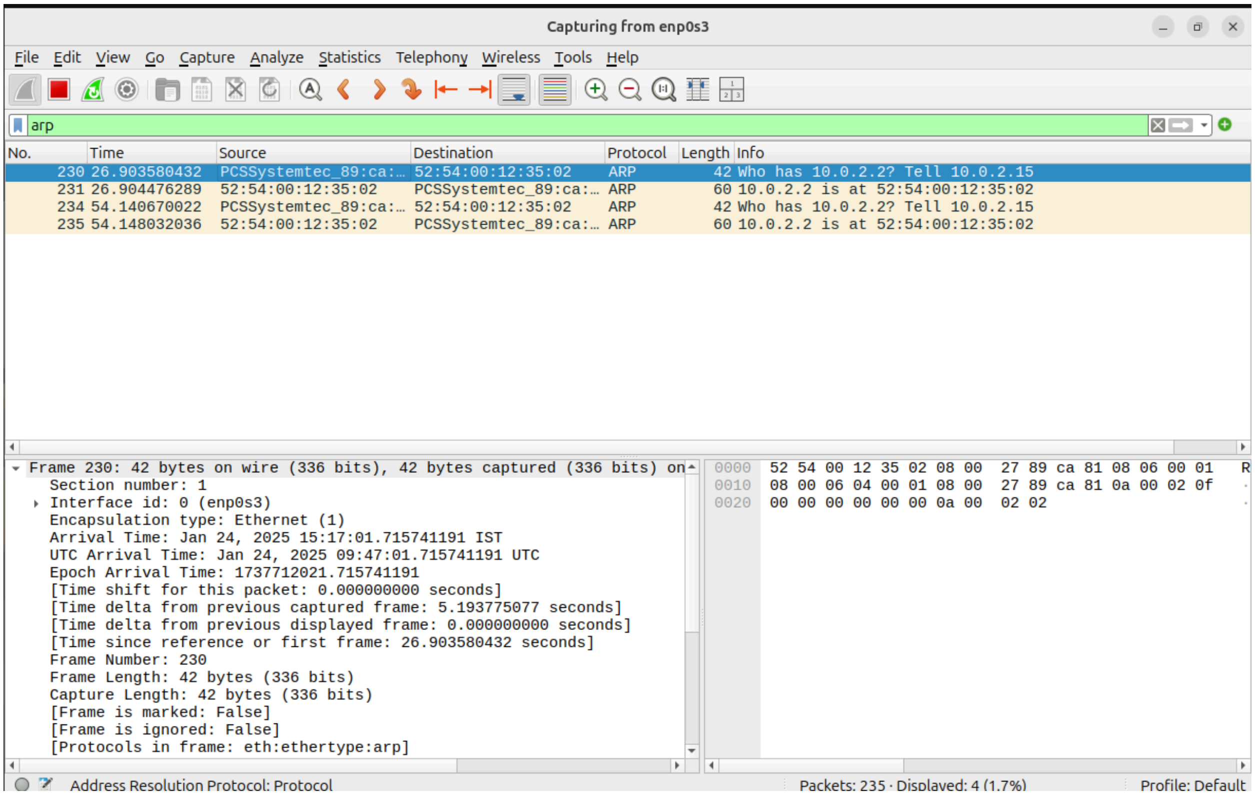
```
▾ Frame 2: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
    Section number: 1
  ▸ Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2025 15:15:01.178644383 IST
    UTC Arrival Time: Jan 24, 2025 09:45:01.178644383 UTC
    Epoch Arrival Time: 1737711901.178644383
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.038320589 seconds]
    [Time delta from previous displayed frame: 0.038320589 seconds]
    [Time since reference or first frame: 0.038320589 seconds]
    Frame Number: 2
    Frame Length: 345 bytes (2760 bits)
    Capture Length: 345 bytes (2760 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
```

```
0000  08 00 27 89 ca 81 52 54  00 12 35 02 08 00 45 00
0010  01 4b 36 34 00 00 40 11  49 32 0e 8b df a2 0a 00
0020  02 0f 00 35 b0 d2 01 37  c5 4c c2 e8 81 80 00 01
0030  00 01 00 04 00 09 06 67  6f 6f 67 6c 65 03 63 6f
0040  6d 00 00 01 00 01 c0 0c  00 01 00 01 00 00 00 b1
0050  00 04 8e fa c7 ae c0 0c  00 02 00 01 00 00 37 46
0060  00 06 03 6e 73 31 c0 0c  c0 0c 00 02 00 01 00 00
0070  37 46 00 06 03 6e 73 34  c0 0c c0 0c 00 02 00 01
0080  00 00 37 46 00 06 03 6e  73 33 c0 0c c0 0c 00 02
0090  00 01 00 00 37 46 00 06  03 6e 73 32 c0 0c c0 6e
00a0  00 01 00 01 00 00 12 1c  00 04 d8 ef 22 0a c0 6e
00b0  00 1c 00 01 00 00 0b 26  00 10 20 01 48 60 48 02
00c0  00 34 00 00 00 00 00 00  00 0a c0 5c 00 01 00 01
00d0  00 00 1d fe 00 04 d8 ef  24 0a c0 5c 00 1c 00 01
00e0  00 00 0b 26 00 10 20 01  48 60 48 02 00 36 00 00
00f0  00 00 00 00 00 0a c0 38  00 01 00 01 00 00 03 9b
0100  00 04 d8 ef 20 0a c0 38  00 1c 00 01 00 00 0b 26
```

```
Domain Name System: Protocol        Packets: 4 · Displayed: 2 (50.0%)        Profile: Default
```

(iv) arp

The `arp` command is a valuable tool for managing and inspecting the ARP cache. Wireshark captures reveal the broadcast-based nature of ARP requests and the direct unicast responses. These mechanisms highlight ARP's role in enabling seamless IP-to-MAC address resolution, ensuring proper communication in a local network.



arp

```
No.       Time          Source                 Destination            Protocol  Length Info
      230 26.903580432  PCSSystemtec_89:ca:…   52:54:00:12:35:02      ARP           42 Who has 10.0.2.2? Tell 10.0.2.15
      231 26.904476289  52:54:00:12:35:02      PCSSystemtec_89:ca:…   ARP           60 10.0.2.2 is at 52:54:00:12:35:02
      234 54.140670022  PCSSystemtec_89:ca:…   52:54:00:12:35:02      ARP           42 Who has 10.0.2.2? Tell 10.0.2.15
      235 54.148032036  52:54:00:12:35:02      PCSSystemtec_89:ca:…   ARP           60 10.0.2.2 is at 52:54:00:12:35:02
```

```
▾ Frame 230: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on
    Section number: 1
  ▸ Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2025 15:17:01.715741191 IST
    UTC Arrival Time: Jan 24, 2025 09:47:01.715741191 UTC
    Epoch Arrival Time: 1737712021.715741191
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 5.193775077 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 26.903580432 seconds]
    Frame Number: 230
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
```

```
0000  52 54 00 12 35 02 08 00  27 89 ca 81 08 06 00 01   R
0010  08 00 06 04 00 01 08 00  27 89 ca 81 0a 00 02 0f   ·
0020  00 00 00 00 00 00 0a 00  02 02                     ·
```

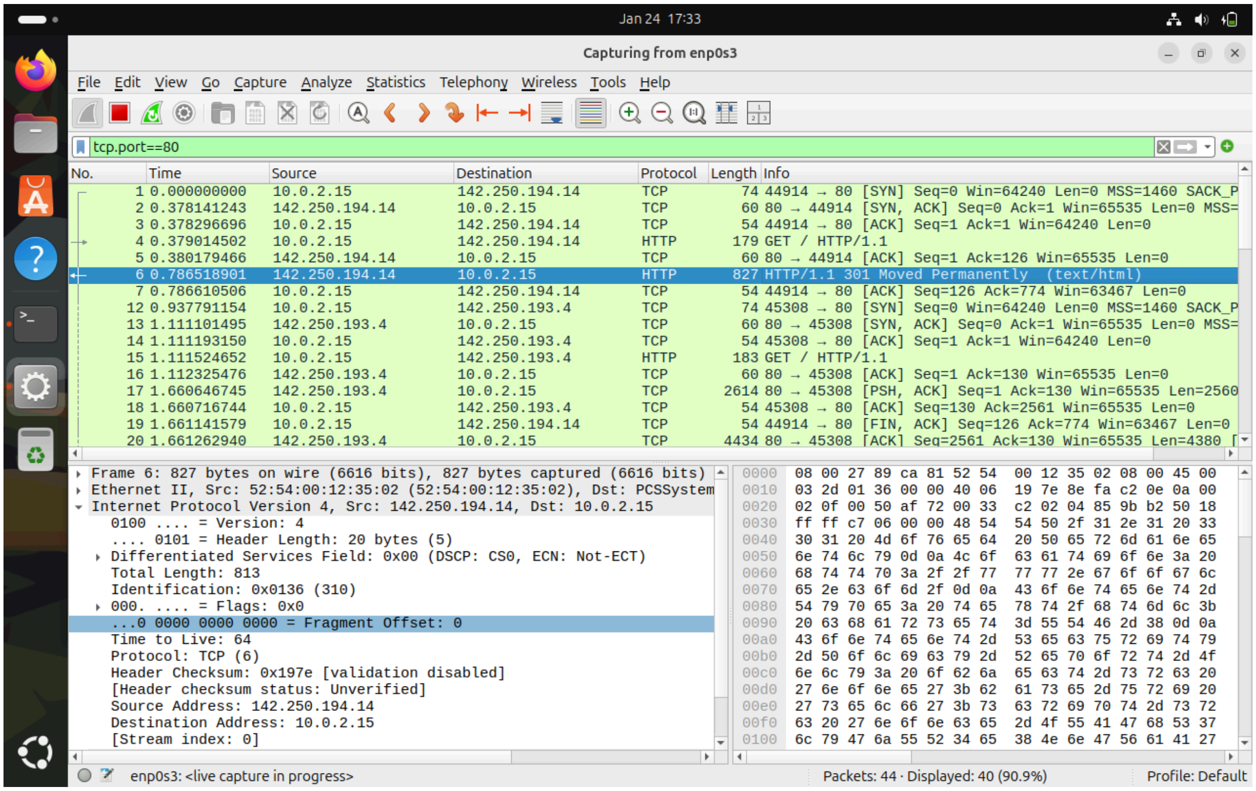
Address Resolution Protocol: Protocol

Packets: 235 · Displayed: 4 (1.7%)

Profile: Default

(v)wget.

The wget command fetches web pages or files over HTTP/HTTPS. Capturing HTTP requests and responses helps analyze this communication.


Jan 24 17:33
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==80

```
No.  Time         Source           Destination      Protocol Length Info
   1 0.000000000  10.0.2.15        142.250.194.14   TCP        74 44914 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
   2 0.378141243  142.250.194.14   10.0.2.15        TCP        60 80 → 44914 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
   3 0.378296696  10.0.2.15        142.250.194.14   TCP        54 44914 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   4 0.379014502  10.0.2.15        142.250.194.14   HTTP      179 GET / HTTP/1.1
   5 0.380179466  142.250.194.14   10.0.2.15        TCP        60 80 → 44914 [ACK] Seq=1 Ack=126 Win=65535 Len=0
   6 0.786518901  142.250.194.14   10.0.2.15        HTTP      827 HTTP/1.1 301 Moved Permanently  (text/html)
   7 0.786610506  10.0.2.15        142.250.194.14   TCP        54 44914 → 80 [ACK] Seq=126 Ack=774 Win=63467 Len=0
  12 0.937791154  10.0.2.15        142.250.193.4    TCP        74 45308 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
  13 1.111101495  142.250.193.4    10.0.2.15        TCP        60 80 → 45308 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
  14 1.111193150  10.0.2.15        142.250.193.4    TCP        54 45308 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  15 1.111524652  10.0.2.15        142.250.193.4    HTTP      183 GET / HTTP/1.1
  16 1.112325476  142.250.193.4    10.0.2.15        TCP        60 80 → 45308 [ACK] Seq=1 Ack=130 Win=65535 Len=0
  17 1.660646745  142.250.193.4    10.0.2.15        TCP      2614 80 → 45308 [PSH, ACK] Seq=1 Ack=130 Win=65535 Len=2560
  18 1.660716744  10.0.2.15        142.250.193.4    TCP        54 45308 → 80 [ACK] Seq=130 Ack=2561 Win=65535 Len=0
  19 1.661141579  10.0.2.15        142.250.194.14   TCP        54 44914 → 80 [FIN, ACK] Seq=126 Ack=774 Win=63467 Len=0
  20 1.661262940  142.250.193.4    10.0.2.15        TCP      4434 80 → 45308 [ACK] Seq=2561 Ack=130 Win=65535 Len=4380 [
```

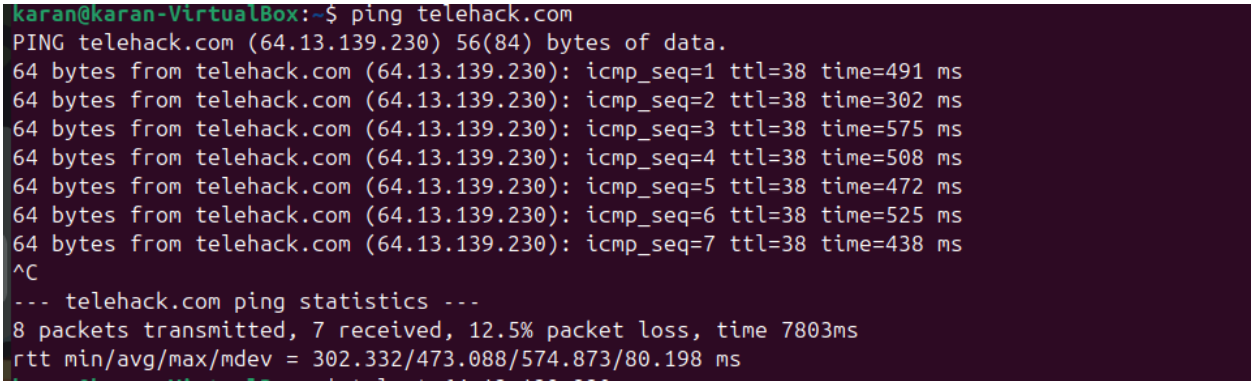
```
▸ Frame 6: 827 bytes on wire (6616 bits), 827 bytes captured (6616 bits)
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystem
▾ Internet Protocol Version 4, Src: 142.250.194.14, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 813
    Identification: 0x0136 (310)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x197e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 142.250.194.14
    Destination Address: 10.0.2.15
    [Stream index: 0]
```

```
0000  08 00 27 89 ca 81 52 54  00 12 35 02 08 00 45 00
0010  03 2d 01 36 00 00 40 06  19 7e 8e fa c2 0e 0a 00
0020  02 0f 00 50 af 72 00 33  c2 02 04 85 9b b2 50 18
0030  ff ff c7 06 00 00 48 54  54 50 2f 31 2e 31 20 33
0040  30 31 20 4d 6f 76 65 64  20 50 65 72 6d 61 6e 65
0050  6e 74 6c 79 0d 0a 4c 6f  63 61 74 69 6f 6e 3a 20
0060  68 74 74 70 3a 2f 2f 77  77 77 2e 67 6f 6f 67 6c
0070  65 2e 63 6f 6d 2f 0d 0a  43 6f 6e 74 65 6e 74 2d
0080  54 79 70 65 3a 20 74 65  78 74 2f 68 74 6d 6c 3b
0090  20 63 68 61 72 73 65 74  3d 55 54 46 2d 38 0d 0a
00a0  43 6f 6e 74 65 6e 74 2d  53 65 63 75 72 69 74 79
00b0  2d 50 6f 6c 69 63 79 2d  52 65 70 6f 72 74 2d 4f
00c0  6e 6c 79 3a 20 6f 62 6a  65 63 74 2d 73 72 63 20
00d0  27 6e 6f 6e 65 27 3b 62  61 73 65 2d 75 72 69 20
00e0  27 73 65 6c 66 27 3b 73  63 72 69 70 74 2d 73 72
00f0  63 20 27 6e 6f 6e 65 27  2d 4f 55 41 47 68 53 37
0100  6c 79 47 6a 55 52 34 65  38 4e 6e 47 56 61 41 27
```

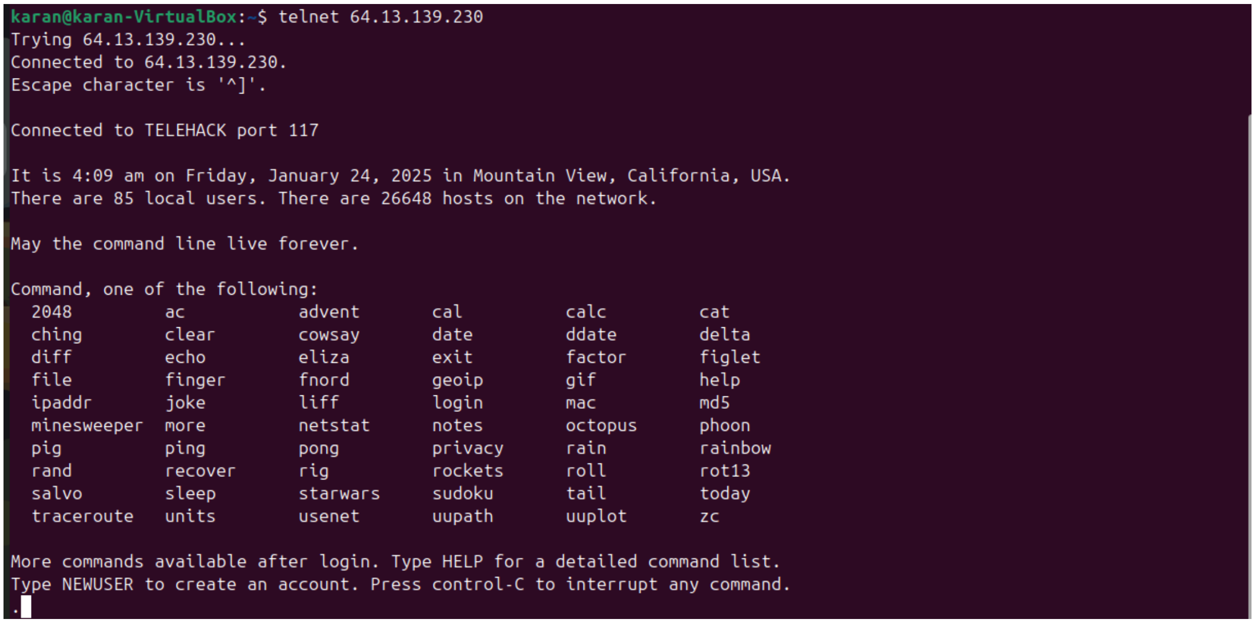
enp0s3: <live capture in progress>   Packets: 44 · Displayed: 40 (90.9%)   Profile: Default

2. 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?

I use “ping telehack.com” to get the IP address which accessible with telent which gives the IP address **64.13.139.230.** Then i use the command “telnet 64.13.139.230 to make the connection between my computer and the IP.

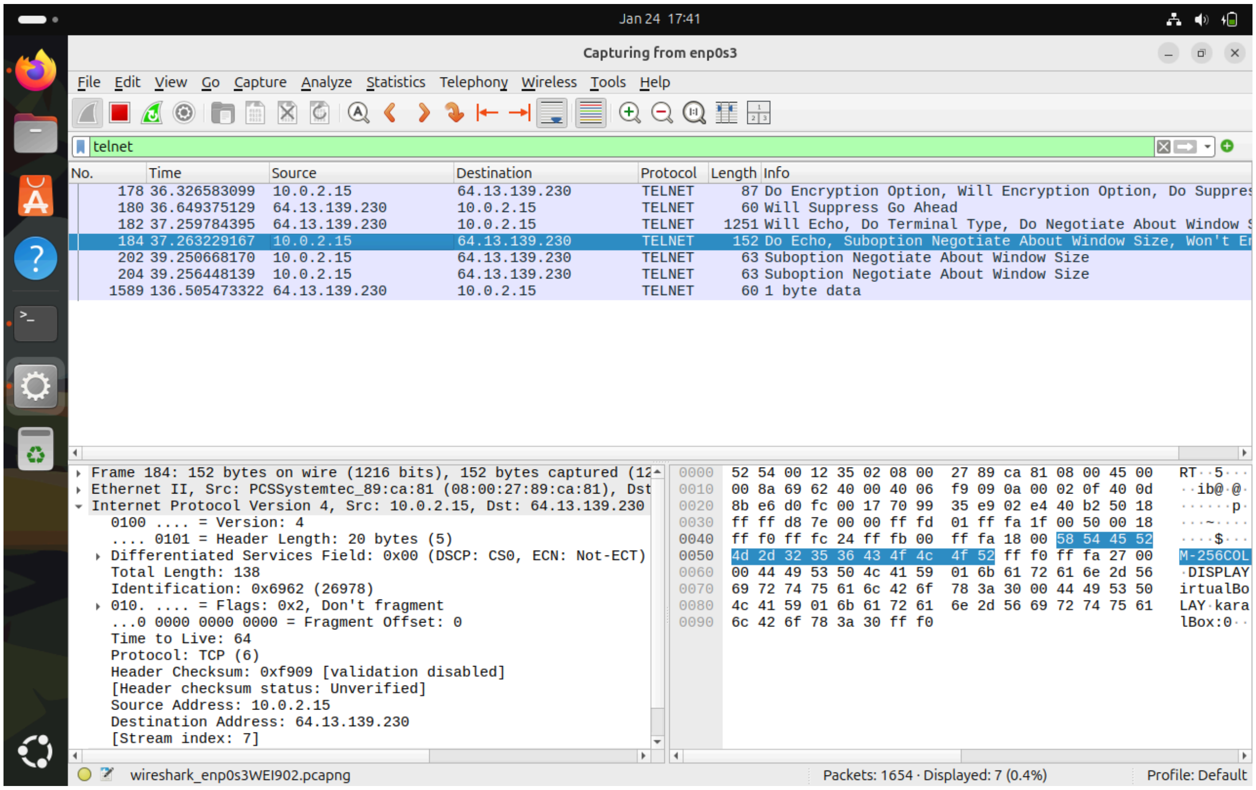


```
karan@karan-VirtualBox:~$ ping telehack.com
PING telehack.com (64.13.139.230) 56(84) bytes of data.
64 bytes from telehack.com (64.13.139.230): icmp_seq=1 ttl=38 time=491 ms
64 bytes from telehack.com (64.13.139.230): icmp_seq=2 ttl=38 time=302 ms
64 bytes from telehack.com (64.13.139.230): icmp_seq=3 ttl=38 time=575 ms
64 bytes from telehack.com (64.13.139.230): icmp_seq=4 ttl=38 time=508 ms
64 bytes from telehack.com (64.13.139.230): icmp_seq=5 ttl=38 time=472 ms
64 bytes from telehack.com (64.13.139.230): icmp_seq=6 ttl=38 time=525 ms
64 bytes from telehack.com (64.13.139.230): icmp_seq=7 ttl=38 time=438 ms
^C
--- telehack.com ping statistics ---
8 packets transmitted, 7 received, 12.5% packet loss, time 7803ms
rtt min/avg/max/mdev = 302.332/473.088/574.873/80.198 ms
```



```
karan@karan-VirtualBox:~$ telnet 64.13.139.230
Trying 64.13.139.230...
Connected to 64.13.139.230.
Escape character is '^]'.

Connected to TELEHACK port 117

It is 4:09 am on Friday, January 24, 2025 in Mountain View, California, USA.
There are 85 local users. There are 26648 hosts on the network.

May the command line live forever.

Command, one of the following:
  2048        ac          advent      cal         calc        cat
  ching       clear       cowsay      date        ddate       delta
  diff        echo        eliza       exit        factor      figlet
  file        finger      fnord       geoip       gif         help
  ipaddr      joke        liff        login       mac         md5
  minesweeper more        netstat     notes       octopus     phoon
  pig         ping        pong        privacy     rain        rainbow
  rand        recover     rig         rockets     roll        rot13
  salvo       sleep       starwars    sudoku      tail        today
  traceroute  units       usenet      uupath      uuplot      zc

More commands available after login. Type HELP for a detailed command list.
Type NEWUSER to create an account. Press control-C to interrupt any command.
.
```

In the picture we can see the Internet Protocol which tell us the Source and Destinations IP addresses.show the message that was sent by the local computer to the server. The data is sent as plaintext and is not encrypted.


Jan 24 17:41
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet

```
No.   Time           Source         Destination    Protocol Length Info
  178 36.326583099   10.0.2.15      64.13.139.230  TELNET     87 Do Encryption Option, Will Encryption Option, Do Suppres
  180 36.649375129   64.13.139.230  10.0.2.15      TELNET     60 Will Suppress Go Ahead
  182 37.259784395   64.13.139.230  10.0.2.15      TELNET   1251 Will Echo, Do Terminal Type, Do Negotiate About Window S
  184 37.263229167   10.0.2.15      64.13.139.230  TELNET    152 Do Echo, Suboption Negotiate About Window Size, Won't En
  202 39.250668170   10.0.2.15      64.13.139.230  TELNET     63 Suboption Negotiate About Window Size
  204 39.256448139   10.0.2.15      64.13.139.230  TELNET     63 Suboption Negotiate About Window Size
 1589 136.505473322  64.13.139.230  10.0.2.15      TELNET     60 1 byte data
```

```
▸ Frame 184: 152 bytes on wire (1216 bits), 152 bytes captured (12
▸ Ethernet II, Src: PCSSystemtec_89:ca:81 (08:00:27:89:ca:81), Dst
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 64.13.139.230
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 138
    Identification: 0x6962 (26978)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xf909 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 64.13.139.230
    [Stream index: 7]
```

```
0000  52 54 00 12 35 02 08 00  27 89 ca 81 08 00 45 00   RT··5···
0010  00 8a 69 62 40 00 40 06  f9 09 0a 00 02 0f 40 0d   ··ib@·@·
0020  8b e6 d0 fc 00 17 70 99  35 e9 02 e4 40 b2 50 18   ······p·
0030  ff ff d8 7e 00 00 ff fd  01 ff fa 1f 00 50 00 18   ···~····
0040  ff f0 ff fc 24 ff fb 00  ff fa 18 00 58 54 45 52   ····$···
0050  4d 2d 32 35 36 43 4f 4c  4f 52 ff f0 ff fa 27 00   M-256COL
0060  00 44 49 53 50 4c 41 59  01 6b 61 72 61 6e 2d 56   ·DISPLAY
0070  69 72 74 75 61 6c 42 6f  78 3a 30 00 44 49 53 50   irtualBo
0080  4c 41 59 01 6b 61 72 61  6e 2d 56 69 72 74 75 61   LAY·kara
0090  6c 42 6f 78 3a 30 ff f0                            lBox:0··
```

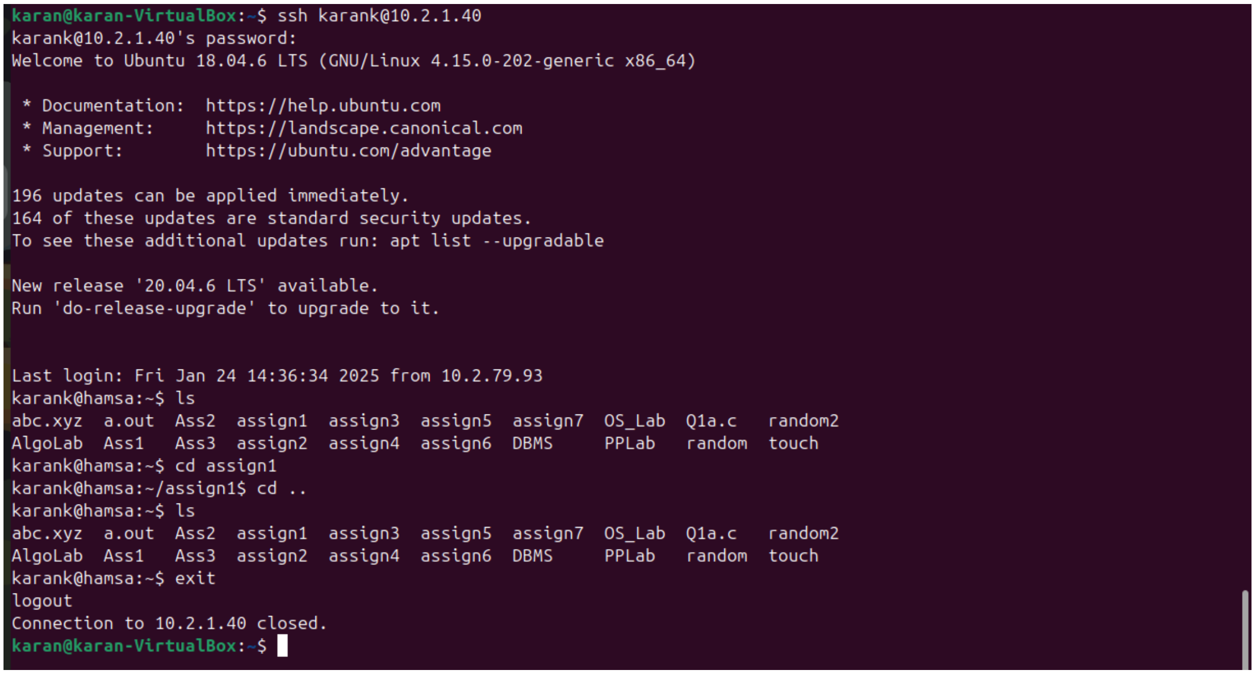
wireshark_enp0s3WEI902.pcapng

Packets: 1654 · Displayed: 7 (0.4%)

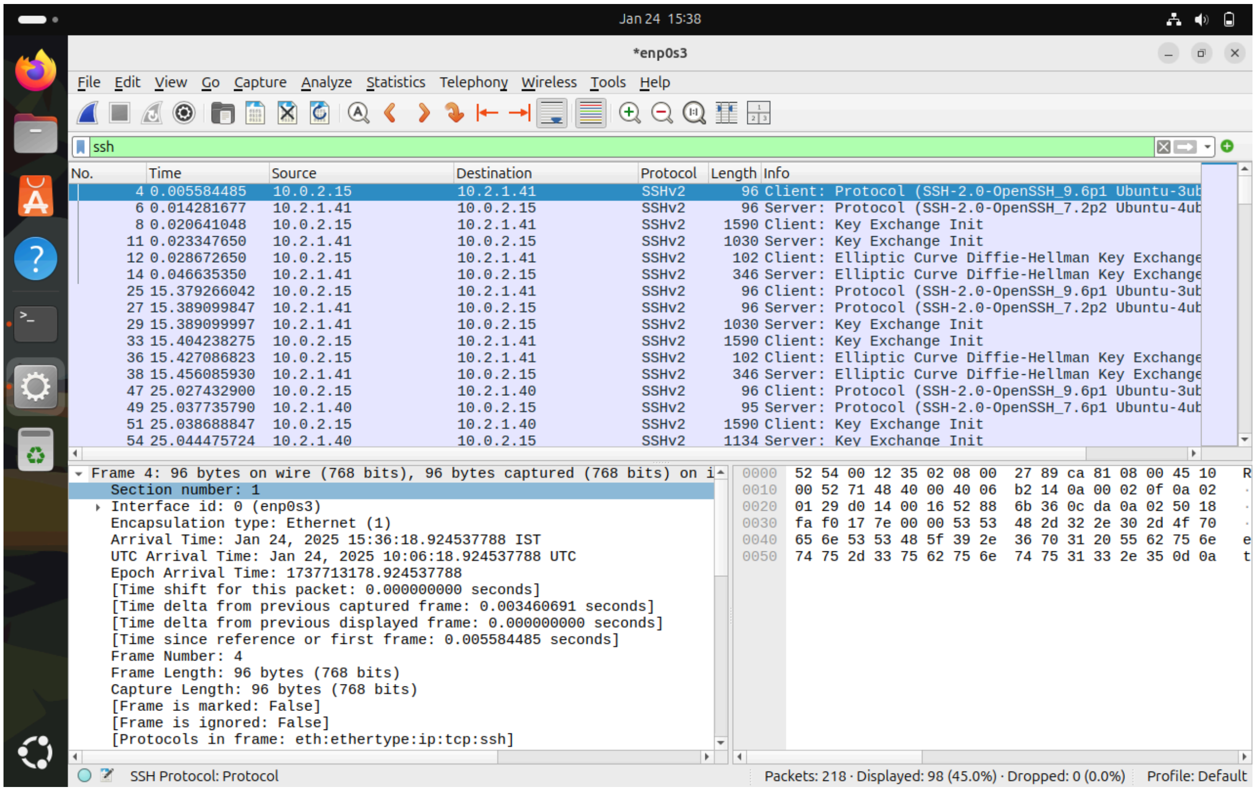
Profile: Default

3. 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?

Since ssh is secure protocol the information sent over the server connected via ssh, the data will be transmitted in a secure manner and the data packets captured by wireshark will have the data in an encrypted manner. Upon analyzing the captured packets in Wireshark, the application layer data appears encrypted. Instead of readable text or commands, the transmitted data is encapsulated within encrypted payloads, which are not visible in plain text. This encryption ensures that the communication is secure and cannot be interpreted by anyone monitoring the network traffic.



```
karan@karan-VirtualBox:~$ ssh karank@10.2.1.40
karank@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

196 updates can be applied immediately.
164 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: Fri Jan 24 14:36:34 2025 from 10.2.79.93
karank@hamsa:~$ ls
abc.xyz  a.out  Ass2  assign1  assign3  assign5  assign7  OS_Lab  Q1a.c   random2
AlgoLab  Ass1   Ass3  assign2  assign4  assign6  DBMS     PPLab   random  touch
karank@hamsa:~$ cd assign1
karank@hamsa:~/assign1$ cd ..
karank@hamsa:~$ ls
abc.xyz  a.out  Ass2  assign1  assign3  assign5  assign7  OS_Lab  Q1a.c   random2
AlgoLab  Ass1   Ass3  assign2  assign4  assign6  DBMS     PPLab   random  touch
karank@hamsa:~$ exit
logout
Connection to 10.2.1.40 closed.
karan@karan-VirtualBox:~$ 
```



Jan 24 15:38
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

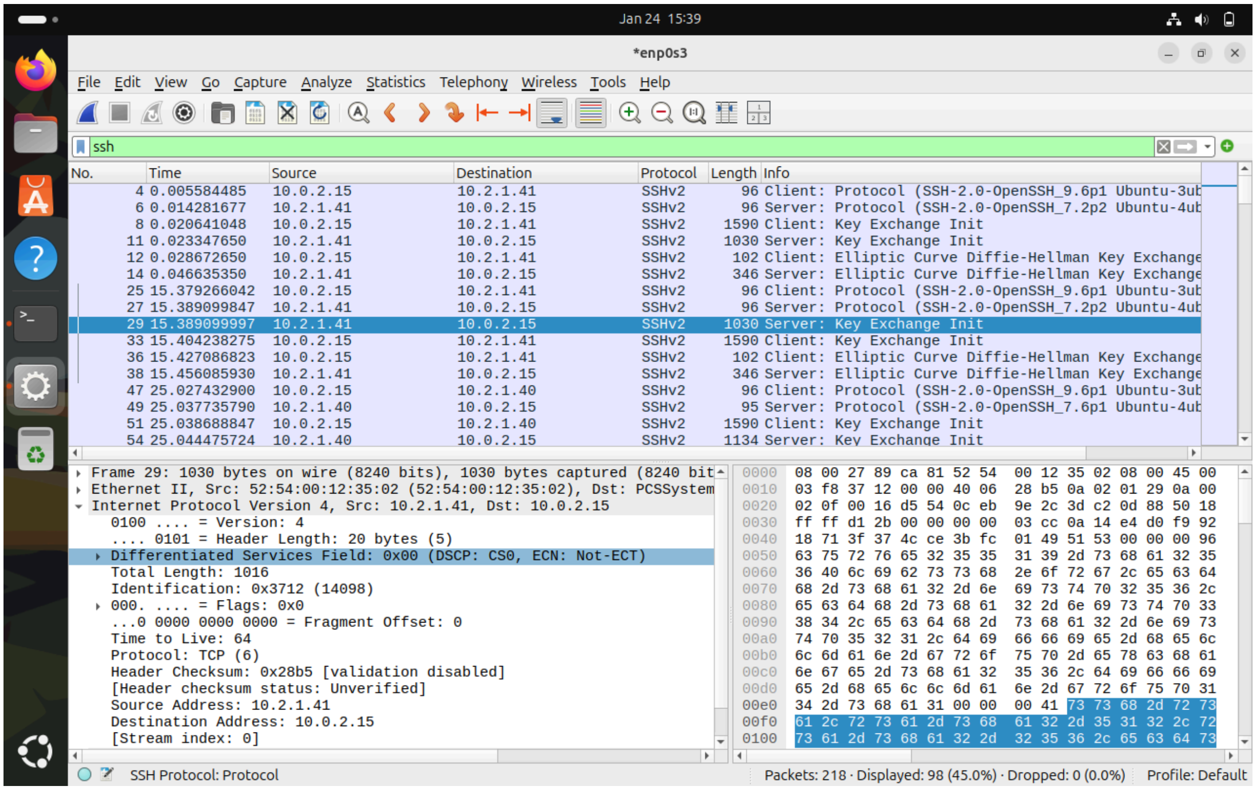
```
ssh
```

```
No.   Time          Source       Destination  Protocol Length Info
    4 0.005584485   10.0.2.15    10.2.1.41    SSHv2       96 Client: Protocol (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ub
    6 0.014281677   10.2.1.41    10.0.2.15    SSHv2       96 Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ub
    8 0.020641048   10.0.2.15    10.2.1.41    SSHv2     1590 Client: Key Exchange Init
   11 0.023347650   10.2.1.41    10.0.2.15    SSHv2     1030 Server: Key Exchange Init
   12 0.028672650   10.0.2.15    10.2.1.41    SSHv2      102 Client: Elliptic Curve Diffie-Hellman Key Exchange
   14 0.046635350   10.2.1.41    10.0.2.15    SSHv2      346 Server: Elliptic Curve Diffie-Hellman Key Exchange
   25 15.379266042  10.0.2.15    10.2.1.41    SSHv2       96 Client: Protocol (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ub
   27 15.389099847  10.2.1.41    10.0.2.15    SSHv2       96 Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ub
   29 15.389099997  10.2.1.41    10.0.2.15    SSHv2     1030 Server: Key Exchange Init
   33 15.404238275  10.0.2.15    10.2.1.41    SSHv2     1590 Client: Key Exchange Init
   36 15.427086823  10.0.2.15    10.2.1.41    SSHv2      102 Client: Elliptic Curve Diffie-Hellman Key Exchange
   38 15.456085930  10.2.1.41    10.0.2.15    SSHv2      346 Server: Elliptic Curve Diffie-Hellman Key Exchange
   47 25.027432900  10.0.2.15    10.2.1.40    SSHv2       96 Client: Protocol (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ub
   49 25.037735790  10.2.1.40    10.0.2.15    SSHv2       95 Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ub
   51 25.038688847  10.0.2.15    10.2.1.40    SSHv2     1590 Client: Key Exchange Init
   54 25.044475724  10.2.1.40    10.0.2.15    SSHv2     1134 Server: Key Exchange Init
```

```
▾ Frame 4: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on i
    Section number: 1
  ▸ Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2025 15:36:18.924537788 IST
    UTC Arrival Time: Jan 24, 2025 10:06:18.924537788 UTC
    Epoch Arrival Time: 1737713178.924537788
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.003460691 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.005584485 seconds]
    Frame Number: 4
    Frame Length: 96 bytes (768 bits)
    Capture Length: 96 bytes (768 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ssh]
```

```
0000  52 54 00 12 35 02 08 00  27 89 ca 81 08 00 45 10   R
0010  00 52 71 48 40 00 40 06  b2 14 0a 00 02 0f 0a 02   ·
0020  01 29 d0 14 00 16 52 88  6b 36 0c da 0a 02 50 18   ·
0030  fa f0 17 7e 00 00 53 53  48 2d 32 2e 30 2d 4f 70   ·
0040  65 6e 53 53 48 5f 39 2e  36 70 31 20 55 62 75 6e   e
0050  74 75 2d 33 75 62 75 6e  74 75 31 33 2e 35 0d 0a   t
```

SSH Protocol: Protocol Packets: 218 · Displayed: 98 (45.0%) · Dropped: 0 (0.0%) Profile: Default


Jan 24 15:39
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ssh
```

```
No.   Time          Source       Destination  Protocol Length Info
    4 0.005584485   10.0.2.15    10.2.1.41    SSHv2      96 Client: Protocol (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ub
    6 0.014281677   10.2.1.41    10.0.2.15    SSHv2      96 Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ub
    8 0.020641048   10.0.2.15    10.2.1.41    SSHv2    1590 Client: Key Exchange Init
   11 0.023347650   10.2.1.41    10.0.2.15    SSHv2    1030 Server: Key Exchange Init
   12 0.028672650   10.0.2.15    10.2.1.41    SSHv2     102 Client: Elliptic Curve Diffie-Hellman Key Exchange
   14 0.046635350   10.2.1.41    10.0.2.15    SSHv2     346 Server: Elliptic Curve Diffie-Hellman Key Exchange
   25 15.379266042  10.0.2.15    10.2.1.41    SSHv2      96 Client: Protocol (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ub
   27 15.389099847  10.2.1.41    10.0.2.15    SSHv2      96 Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ub
   29 15.389099997  10.2.1.41    10.0.2.15    SSHv2    1030 Server: Key Exchange Init
   33 15.404238275  10.0.2.15    10.2.1.41    SSHv2    1590 Client: Key Exchange Init
   36 15.427086823  10.0.2.15    10.2.1.41    SSHv2     102 Client: Elliptic Curve Diffie-Hellman Key Exchange
   38 15.456085930  10.2.1.41    10.0.2.15    SSHv2     346 Server: Elliptic Curve Diffie-Hellman Key Exchange
   47 25.027432900  10.0.2.15    10.2.1.40    SSHv2      96 Client: Protocol (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ub
   49 25.037735790  10.2.1.40    10.0.2.15    SSHv2      95 Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ub
   51 25.038688847  10.0.2.15    10.2.1.40    SSHv2    1590 Client: Key Exchange Init
   54 25.044475724  10.2.1.40    10.0.2.15    SSHv2    1134 Server: Key Exchange Init
```

```
▸ Frame 29: 1030 bytes on wire (8240 bits), 1030 bytes captured (8240 bit
▸ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystem
▾ Internet Protocol Version 4, Src: 10.2.1.41, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1016
    Identification: 0x3712 (14098)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x28b5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.2.1.41
    Destination Address: 10.0.2.15
    [Stream index: 0]
```

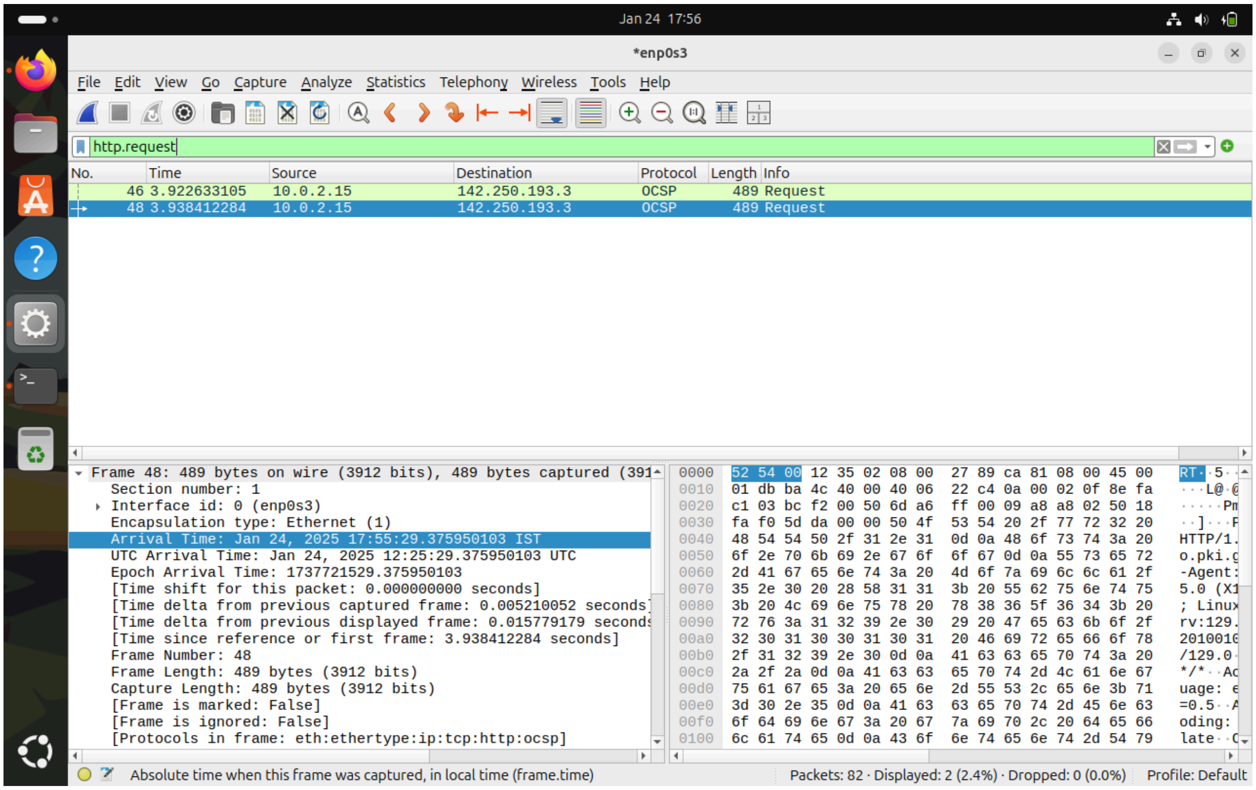
```
0000  08 00 27 89 ca 81 52 54  00 12 35 02 08 00 45 00
0010  03 f8 37 12 00 00 40 06  28 b5 0a 02 01 29 0a 00
0020  02 0f 00 16 d5 54 0c eb  9e 2c 3d c2 0d 88 50 18
0030  ff ff d1 2b 00 00 00 00  03 cc 0a 14 e4 d0 f9 92
0040  18 71 3f 37 4c ce 3b fc  01 49 51 53 00 00 00 96
0050  63 75 72 76 65 32 35 35  31 39 2d 73 68 61 32 35
0060  36 40 6c 69 62 73 73 68  2e 6f 72 67 2c 65 63 64
0070  68 2d 73 68 61 32 2d 6e  69 73 74 70 32 35 36 2c
0080  65 63 64 68 2d 73 68 61  32 2d 6e 69 73 74 70 33
0090  38 34 2c 65 63 64 68 2d  73 68 61 32 2d 6e 69 73
00a0  74 70 35 32 31 2c 64 69  66 66 69 65 2d 68 65 6c
00b0  6c 6d 61 6e 2d 67 72 6f  75 70 2d 65 78 63 68 61
00c0  6e 67 65 2d 73 68 61 32  35 36 2c 64 69 66 66 69
00d0  65 2d 68 65 6c 6c 6d 61  6e 2d 67 72 6f 75 70 31
00e0  34 2d 73 68 61 31 00 00  00 41 73 73 68 2d 72 73
00f0  61 2c 72 73 61 2d 73 68  61 32 2d 35 31 32 2c 72
0100  73 61 2d 73 68 61 32 2d  32 35 36 2c 65 63 64 73
```

```
SSH Protocol: Protocol          Packets: 218 · Displayed: 98 (45.0%) · Dropped: 0 (0.0%)   Profile: Default
```

4. 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 captured packets:
a. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

The HTTP GET request was sent at time 17:55:29.375950103 and the OK response was received at 17:55:29.568598741. The difference is 0.192648638.


Jan 24 17:56
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

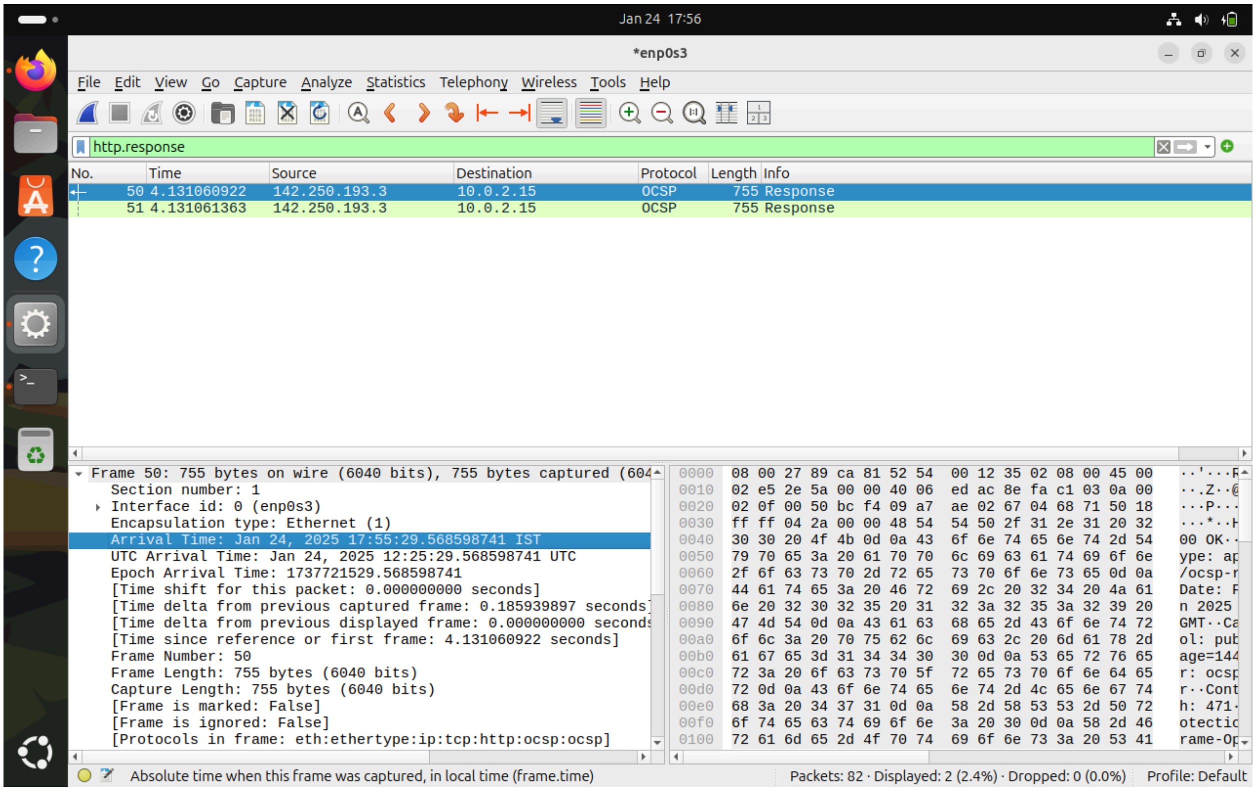
http.request

```
No.   Time         Source      Destination    Protocol Length Info
   46 3.922633105  10.0.2.15   142.250.193.3  OCSP        489 Request
   48 3.938412284  10.0.2.15   142.250.193.3  OCSP        489 Request
```

```
Frame 48: 489 bytes on wire (3912 bits), 489 bytes captured (391
    Section number: 1
  Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2025 17:55:29.375950103 IST
    UTC Arrival Time: Jan 24, 2025 12:25:29.375950103 UTC
    Epoch Arrival Time: 1737721529.375950103
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.005210052 seconds]
    [Time delta from previous displayed frame: 0.015779179 seconds
    [Time since reference or first frame: 3.938412284 seconds]
    Frame Number: 48
    Frame Length: 489 bytes (3912 bits)
    Capture Length: 489 bytes (3912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:ocsp]
```

```
0000  52 54 00 12 35 02 08 00  27 89 ca 81 08 00 45 00   RT··5··
0010  01 db ba 4c 40 00 40 06  22 c4 0a 00 02 0f 8e fa   ···L@·@
0020  c1 03 bc f2 00 50 6d a6  ff 00 09 a8 a8 02 50 18   ·····Pm
0030  fa f0 5d da 00 00 50 4f  53 54 20 2f 77 72 32 20   ··]···P
0040  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.
0050  6f 2e 70 6b 69 2e 67 6f  6f 67 0d 0a 55 73 65 72   o.pki.g
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:
0070  35 2e 30 20 28 58 31 31  3b 20 55 62 75 6e 74 75   5.0 (X1
0080  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux
0090  72 76 3a 31 32 39 2e 30  29 20 47 65 63 6b 6f 2f   rv:129.
00a0  32 30 31 30 30 31 30 31  20 46 69 72 65 66 6f 78   2010010
00b0  2f 31 32 39 2e 30 0d 0a  41 63 63 65 70 74 3a 20   /129.0·
00c0  2a 2f 2a 0d 0a 41 63 63  65 70 74 2d 4c 61 6e 67   */*··Ac
00d0  75 61 67 65 3a 20 65 6e  2d 55 53 2c 65 6e 3b 71   uage: e
00e0  3d 30 2e 35 0d 0a 41 63  63 65 70 74 2d 45 6e 63   =0.5··A
00f0  6f 64 69 6e 67 3a 20 67  7a 69 70 2c 20 64 65 66   oding:
0100  6c 61 74 65 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   late··C
```

Absolute time when this frame was captured, in local time (frame.time) | Packets: 82 · Displayed: 2 (2.4%) · Dropped: 0 (0.0%) | Profile: Default


Jan 24 17:56
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response

```
No.   Time         Source         Destination  Protocol Length Info
   50 4.131060922  142.250.193.3  10.0.2.15    OCSP        755 Response
   51 4.131061363  142.250.193.3  10.0.2.15    OCSP        755 Response
```

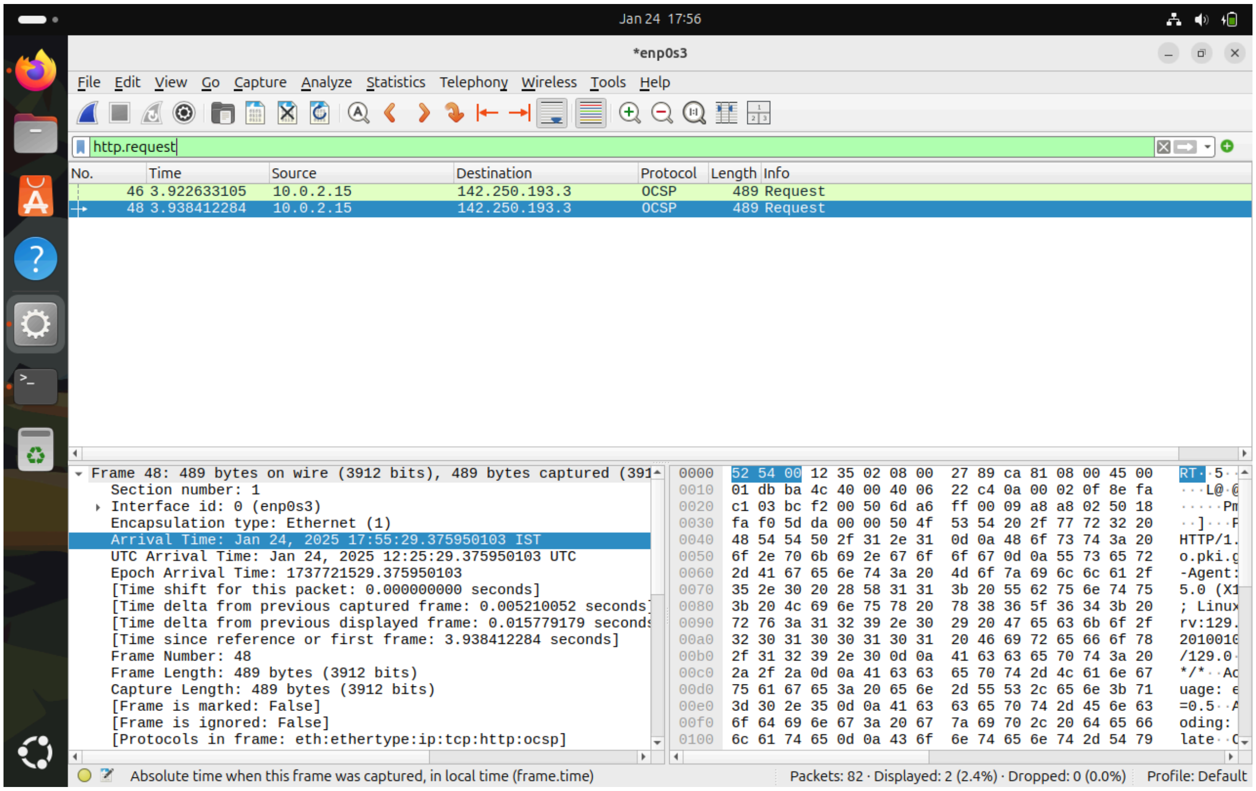
```
Frame 50: 755 bytes on wire (6040 bits), 755 bytes captured (604
    Section number: 1
  Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2025 17:55:29.568598741 IST
    UTC Arrival Time: Jan 24, 2025 12:25:29.568598741 UTC
    Epoch Arrival Time: 1737721529.568598741
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.185939897 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds
    [Time since reference or first frame: 4.131060922 seconds]
    Frame Number: 50
    Frame Length: 755 bytes (6040 bits)
    Capture Length: 755 bytes (6040 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:ocsp:ocsp]
```

```
0000  08 00 27 89 ca 81 52 54  00 12 35 02 08 00 45 00   ··'···R
0010  02 e5 2e 5a 00 00 40 06  ed ac 8e fa c1 03 0a 00   ···.Z··@
0020  02 0f 00 50 bc f4 09 a7  ae 02 67 04 68 71 50 18   ···P···
0030  ff ff 04 2a 00 00 48 54  54 50 2f 31 2e 31 20 32   ···*··H
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 54   00 OK··
0050  79 70 65 3a 20 61 70 70  6c 69 63 61 74 69 6f 6e   ype: ap
0060  2f 6f 63 73 70 2d 72 65  73 70 6f 6e 73 65 0d 0a   /ocsp-r
0070  44 61 74 65 3a 20 46 72  69 2c 20 32 34 20 4a 61   Date: F
0080  6e 20 32 30 32 35 20 31  32 3a 32 35 3a 32 39 20   n 2025
0090  47 4d 54 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72   GMT··Ca
00a0  6f 6c 3a 20 70 75 62 6c  69 63 2c 20 6d 61 78 2d   ol: pub
00b0  61 67 65 3d 31 34 34 30  30 0d 0a 53 65 72 76 65   age=144
00c0  72 3a 20 6f 63 73 70 5f  72 65 73 70 6f 6e 64 65   r: ocsp
00d0  72 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74   r··Cont
00e0  68 3a 20 34 37 31 0d 0a  58 2d 58 53 53 2d 50 72   h: 471·
00f0  6f 74 65 63 74 69 6f 6e  3a 20 30 0d 0a 58 2d 46   otectic
0100  72 61 6d 65 2d 4f 70 74  69 6f 6e 73 3a 20 53 41   rame-Op
```

Absolute time when this frame was captured, in local time (frame.time) | Packets: 82 · Displayed: 2 (2.4%) · Dropped: 0 (0.0%) | Profile: Default

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.

The internet address of gaia.cs.umass.edu has the internet address 142.250.193.3 and that of my computer is 10.0.2.15.



http.request

```
No.   Time          Source       Destination     Protocol  Length Info
   46 3.922633105   10.0.2.15    142.250.193.3   OCSP         489 Request
   48 3.938412284   10.0.2.15    142.250.193.3   OCSP         489 Request
```

```
▾ Frame 48: 489 bytes on wire (3912 bits), 489 bytes captured (391
    Section number: 1
  ▸ Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2025 17:55:29.375950103 IST
    UTC Arrival Time: Jan 24, 2025 12:25:29.375950103 UTC
    Epoch Arrival Time: 1737721529.375950103
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.005210052 seconds]
    [Time delta from previous displayed frame: 0.015779179 seconds
    [Time since reference or first frame: 3.938412284 seconds]
    Frame Number: 48
    Frame Length: 489 bytes (3912 bits)
    Capture Length: 489 bytes (3912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:ocsp]
```

```
0000  52 54 00 12 35 02 08 00  27 89 ca 81 08 00 45 00   RT··5··
0010  01 db ba 4c 40 00 40 06  22 c4 0a 00 02 0f 8e fa   ···L@·@
0020  c1 03 bc f2 00 50 6d a6  ff 00 09 a8 a8 02 50 18   ·····Pm
0030  fa f0 5d da 00 00 50 4f  53 54 20 2f 77 72 32 20   ··]···P
0040  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.
0050  6f 2e 70 6b 69 2e 67 6f  6f 67 0d 0a 55 73 65 72   o.pki.g
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:
0070  35 2e 30 20 28 58 31 31  3b 20 55 62 75 6e 74 75   5.0 (X1
0080  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux
0090  72 76 3a 31 32 39 2e 30  29 20 47 65 63 6b 6f 2f   rv:129.
00a0  32 30 31 30 30 31 30 31  20 46 69 72 65 66 6f 78   2010010
00b0  2f 31 32 39 2e 30 0d 0a  41 63 63 65 70 74 3a 20   /129.0·
00c0  2a 2f 2a 0d 0a 41 63 63  65 70 74 2d 4c 61 6e 67   */*··Ac
00d0  75 61 67 65 3a 20 65 6e  2d 55 53 2c 65 6e 3b 71   uage: e
00e0  3d 30 2e 35 0d 0a 41 63  63 65 70 74 2d 45 6e 63   =0.5··A
00f0  6f 64 69 6e 67 3a 20 67  7a 69 70 2c 20 64 65 66   oding:
0100  6c 61 74 65 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   late··C
```

Absolute time when this frame was captured, in local time (frame.time)

Packets: 82 · Displayed: 2 (2.4%) · Dropped: 0 (0.0%)

Profile: Default

5. 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:
a. Is there any difference in the application layer protocol?
b. How it is different from the HTTP data you analysed in the above problem?

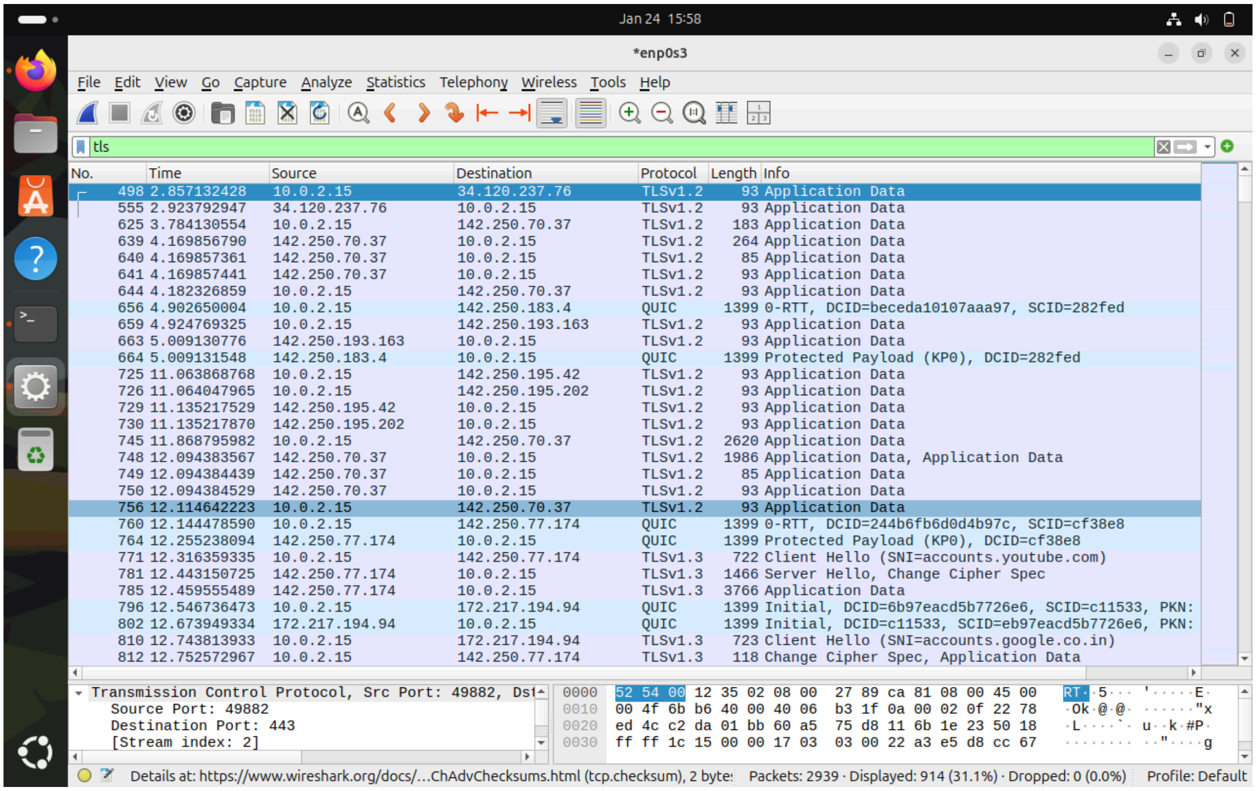
Analysis of the Captured Packets:

a. Difference in the Application Layer Protocol: The application layer protocol observed during the packet capture is HTTPS. Unlike HTTP, which transmits data in plain text, HTTPS ensures that all transmitted data is encrypted, providing a secure communication channel between the client and the server.

b. Differences Compared to HTTP Data: The primary difference between HTTPS and HTTP lies in the encryption and security protocols used. HTTPS utilizes Transport Layer Security (TLS) to encrypt the data being transmitted. During the initial connection, a handshake protocol is observed, which includes messages such as "Client Hello" and "Server Hello." These messages negotiate encryption parameters for the session.

Once the handshake is completed, all subsequent packets are encrypted and categorized as "Application Data" under the TLS protocol. Unlike HTTP, HTTPS traffic does not display unencrypted data such as "GET" requests or "OK" responses in the packet capture, that way sensitive information such as usernames and passwords will remain protected.

By applying the filter for the TLS protocol in Wireshark, only the encrypted application data and handshake messages are visible, safeguarding the contents of the communication.


Jan 24 15:58
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

```
No.   Time          Source            Destination       Protocol  Length Info
  498 2.857132428   10.0.2.15         34.120.237.76     TLSv1.2     93 Application Data
  555 2.923792947   34.120.237.76     10.0.2.15         TLSv1.2     93 Application Data
  625 3.784130554   10.0.2.15         142.250.70.37     TLSv1.2    183 Application Data
  639 4.169856790   142.250.70.37     10.0.2.15         TLSv1.2    264 Application Data
  640 4.169857361   142.250.70.37     10.0.2.15         TLSv1.2     85 Application Data
  641 4.169857441   142.250.70.37     10.0.2.15         TLSv1.2     93 Application Data
  644 4.182326859   10.0.2.15         142.250.70.37     TLSv1.2     93 Application Data
  656 4.902650004   10.0.2.15         142.250.183.4     QUIC      1399 0-RTT, DCID=beceda10107aaa97, SCID=282fed
  659 4.924769325   10.0.2.15         142.250.193.163   TLSv1.2     93 Application Data
  663 5.009130776   142.250.193.163   10.0.2.15         TLSv1.2     93 Application Data
  664 5.009131548   142.250.183.4     10.0.2.15         QUIC      1399 Protected Payload (KP0), DCID=282fed
  725 11.063868768  10.0.2.15         142.250.195.42    TLSv1.2     93 Application Data
  726 11.064047965  10.0.2.15         142.250.195.202   TLSv1.2     93 Application Data
  729 11.135217529  142.250.195.42    10.0.2.15         TLSv1.2     93 Application Data
  730 11.135217870  142.250.195.202   10.0.2.15         TLSv1.2     93 Application Data
  745 11.868795982  10.0.2.15         142.250.70.37     TLSv1.2   2620 Application Data
  748 12.094383567  142.250.70.37     10.0.2.15         TLSv1.2   1986 Application Data, Application Data
  749 12.094384439  142.250.70.37     10.0.2.15         TLSv1.2     85 Application Data
  750 12.094384529  142.250.70.37     10.0.2.15         TLSv1.2     93 Application Data
  756 12.114642223  10.0.2.15         142.250.70.37     TLSv1.2     93 Application Data
  760 12.144478590  10.0.2.15         142.250.77.174    QUIC      1399 0-RTT, DCID=244b6fb6d0d4b97c, SCID=cf38e8
  764 12.255238094  142.250.77.174    10.0.2.15         QUIC      1399 Protected Payload (KP0), DCID=cf38e8
  771 12.316359335  10.0.2.15         142.250.77.174    TLSv1.3    722 Client Hello (SNI=accounts.youtube.com)
  781 12.443150725  142.250.77.174    10.0.2.15         TLSv1.3   1466 Server Hello, Change Cipher Spec
  785 12.459555489  142.250.77.174    10.0.2.15         TLSv1.3   3766 Application Data
  796 12.546736473  10.0.2.15         172.217.194.94    QUIC      1399 Initial, DCID=6b97eacd5b7726e6, SCID=c11533, PKN:
  802 12.673949334  172.217.194.94    10.0.2.15         QUIC      1399 Initial, DCID=c11533, SCID=eb97eacd5b7726e6, PKN:
  810 12.743813933  10.0.2.15         172.217.194.94    TLSv1.3    723 Client Hello (SNI=accounts.google.co.in)
  812 12.752572967  10.0.2.15         142.250.77.174    TLSv1.3    118 Change Cipher Spec, Application Data
```

```
Transmission Control Protocol, Src Port: 49882, Dst
  Source Port: 49882
  Destination Port: 443
  [Stream index: 2]
```

```
0000  52 54 00 12 35 02 08 00  27 89 ca 81 08 00 45 00   RT··5···  '·····E·
0010  00 4f 6b b6 40 00 40 06  b3 1f 0a 00 02 0f 22 78   ·Ok·@·@·  ······"x
0020  ed 4c c2 da 01 bb 60 a5  75 d8 11 6b 1e 23 50 18   ·L····`·  u··k·#P·
0030  ff ff 1c 15 00 00 17 03  03 00 22 a3 e5 d8 cc 67   ········  ··"····g
```

Details at: https://www.wireshark.org/docs/…ChAdvChecksums.html (tcp.checksum), 2 byte: Packets: 2939 · Displayed: 914 (31.1%) · Dropped: 0 (0.0%) Profile: Default