Computer Network Lab (CS 3272)
Assignment 2
Exploring Wireshark Tool

Name : Vinita Ramdular Yadav

Enrolment No: 2020CSB026

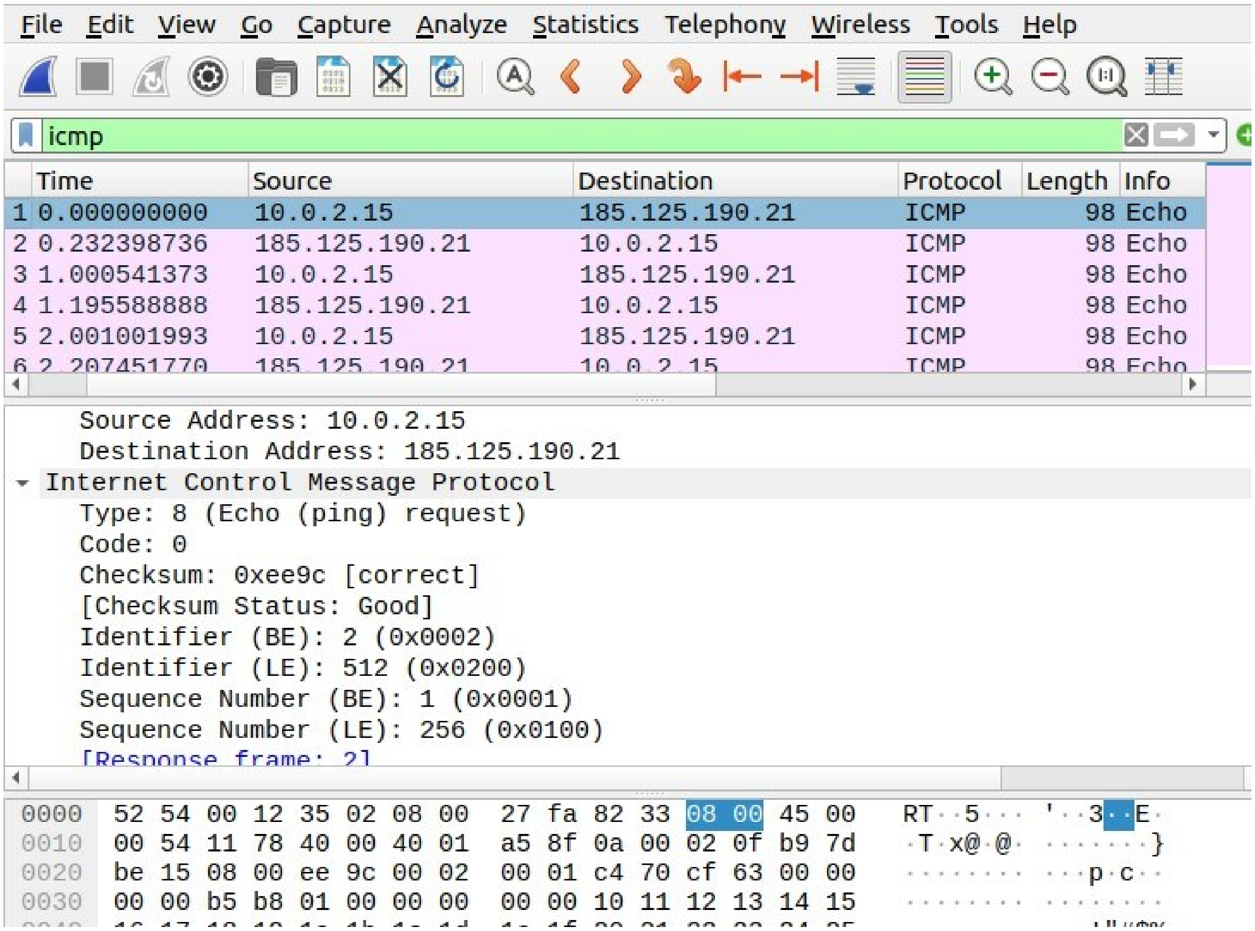
Semester : 6(Gx)

The aim of this assignment is to make you familiar with a GUI-based TCP/IP packet capturing (sniffing) tool called Wireshark.

1. Analyze 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:

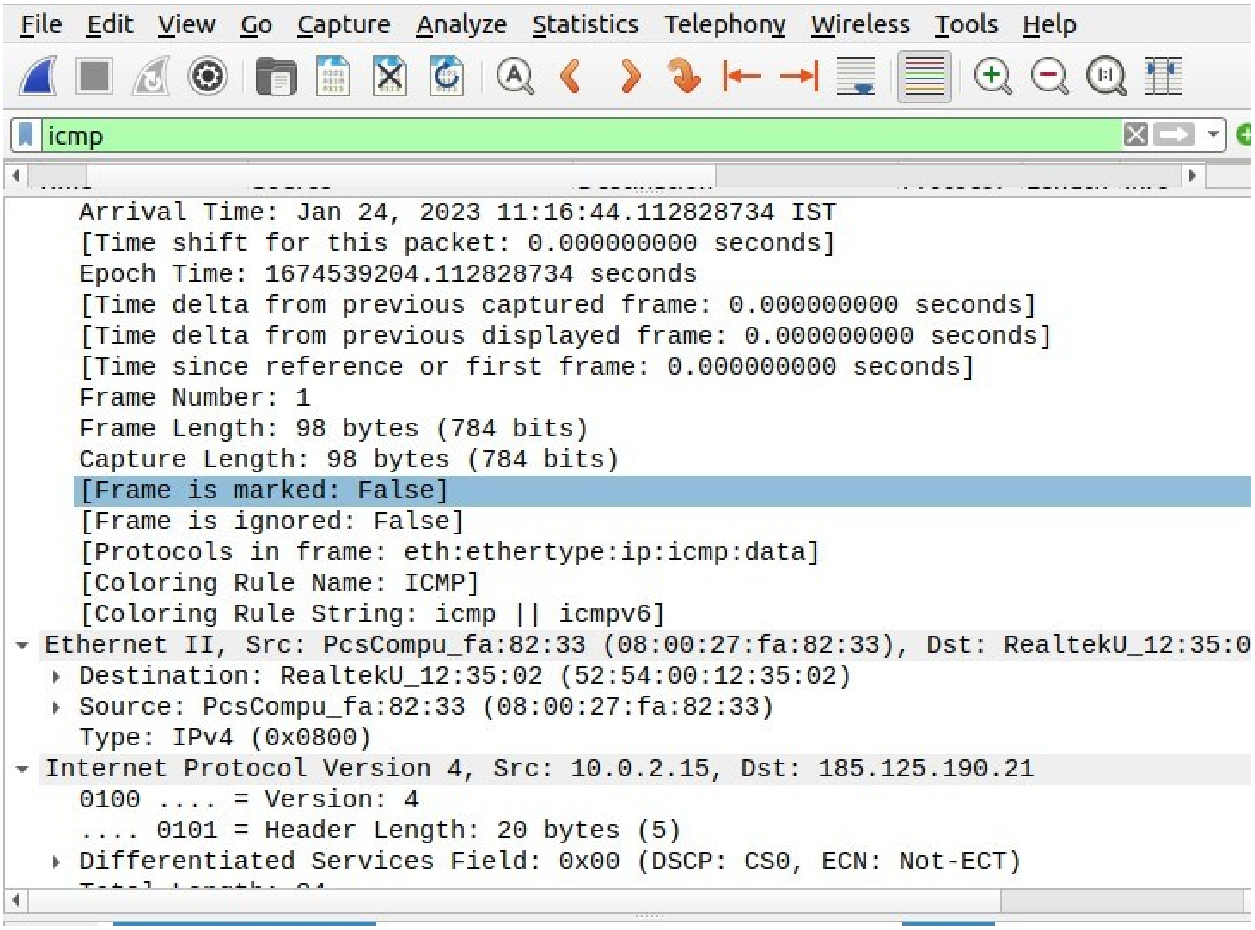


```
  Time          Source           Destination      Protocol  Length Info
1 0.000000000   10.0.2.15        185.125.190.21   ICMP          98 Echo
2 0.232398736   185.125.190.21   10.0.2.15        ICMP          98 Echo
3 1.000541373   10.0.2.15        185.125.190.21   ICMP          98 Echo
4 1.195588888   185.125.190.21   10.0.2.15        ICMP          98 Echo
5 2.001001993   10.0.2.15        185.125.190.21   ICMP          98 Echo
6 2.207451770   185.125.190.21   10.0.2.15        ICMP          98 Echo
```

```
    Source Address: 10.0.2.15
    Destination Address: 185.125.190.21
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xee9c [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 2]
```

```
0000  52 54 00 12 35 02 08 00  27 fa 82 33 08 00 45 00   RT··5···  '··3··E·
0010  00 54 11 78 40 00 40 01  a5 8f 0a 00 02 0f b9 7d   ·T·x@·@·  ·······}
0020  be 15 08 00 ee 9c 00 02  00 01 c4 70 cf 63 00 00   ········  ···p·c··
0030  00 00 b5 b8 01 00 00 00  00 00 10 11 12 13 14 15   ········  ········
```

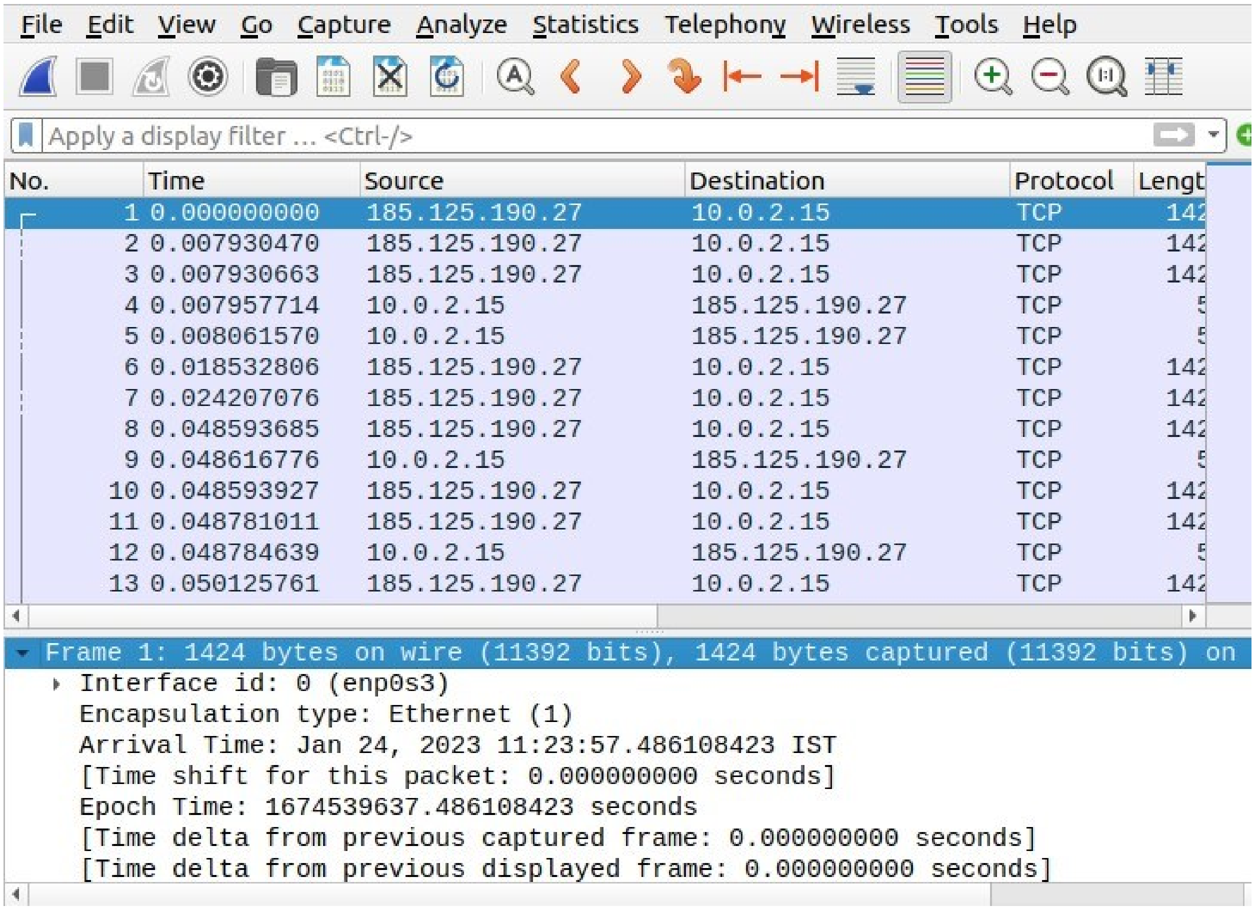
Analysis:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
    Arrival Time: Jan 24, 2023 11:16:44.112828734 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1674539204.112828734 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
▾ Ethernet II, Src: PcsCompu_fa:82:33 (08:00:27:fa:82:33), Dst: RealtekU_12:35:0
  ▸ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▸ Source: PcsCompu_fa:82:33 (08:00:27:fa:82:33)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 185.125.190.21
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

(ii)traceroute:

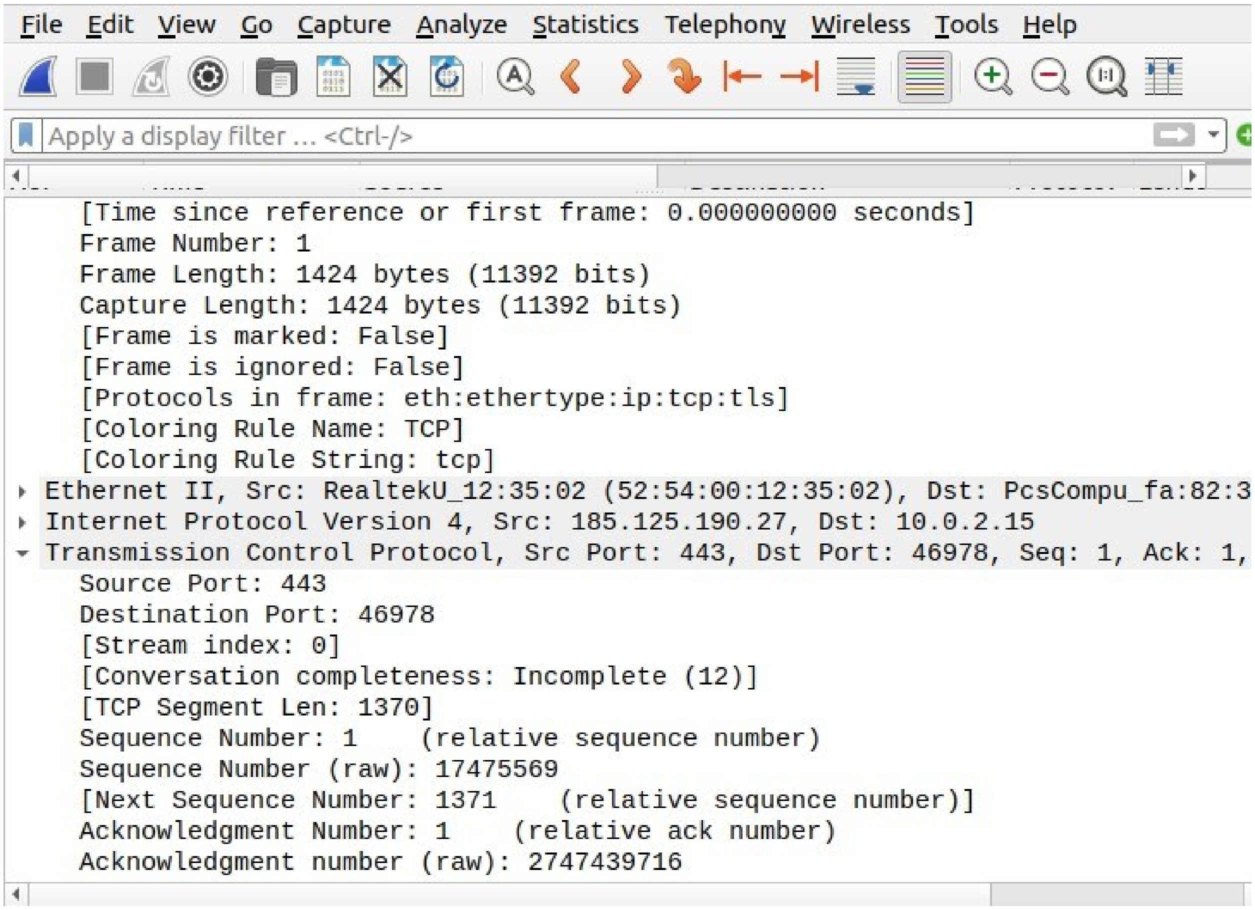
TCP - Transmission Control Protocol



```
No.    Time          Source            Destination       Protocol  Lengt
     1 0.000000000   185.125.190.27    10.0.2.15         TCP         142
     2 0.007930470   185.125.190.27    10.0.2.15         TCP         142
     3 0.007930663   185.125.190.27    10.0.2.15         TCP         142
     4 0.007957714   10.0.2.15         185.125.190.27    TCP           5
     5 0.008061570   10.0.2.15         185.125.190.27    TCP           5
     6 0.018532806   185.125.190.27    10.0.2.15         TCP         142
     7 0.024207076   185.125.190.27    10.0.2.15         TCP         142
     8 0.048593685   185.125.190.27    10.0.2.15         TCP         142
     9 0.048616776   10.0.2.15         185.125.190.27    TCP           5
    10 0.048593927   185.125.190.27    10.0.2.15         TCP         142
    11 0.048781011   185.125.190.27    10.0.2.15         TCP         142
    12 0.048784639   10.0.2.15         185.125.190.27    TCP           5
    13 0.050125761   185.125.190.27    10.0.2.15         TCP         142
```

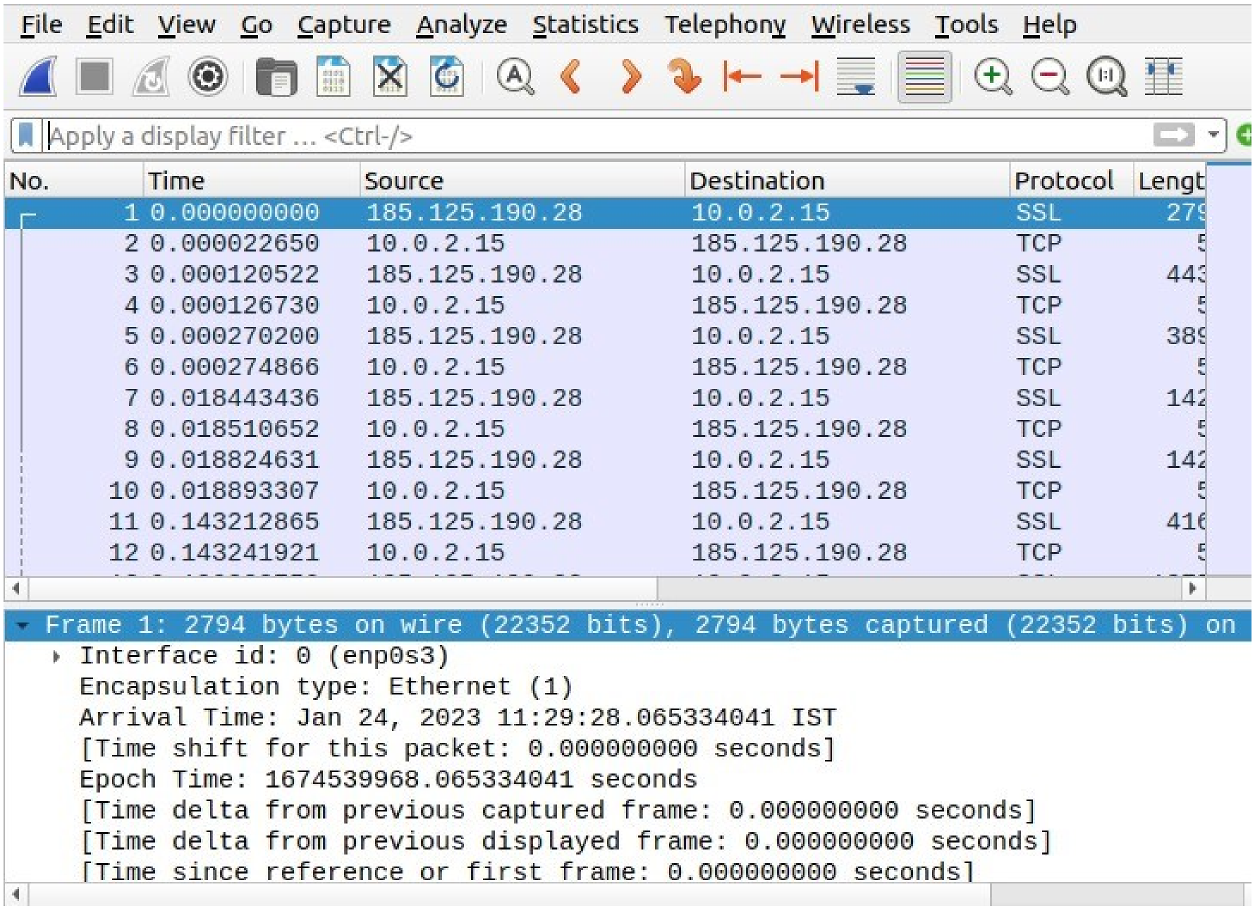
```
▾ Frame 1: 1424 bytes on wire (11392 bits), 1424 bytes captured (11392 bits) on
  ▸ Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2023 11:23:57.486108423 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1674539637.486108423 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
```

Analysis:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 1424 bytes (11392 bits)
    Capture Length: 1424 bytes (11392 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_fa:82:3
▸ Internet Protocol Version 4, Src: 185.125.190.27, Dst: 10.0.2.15
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 46978, Seq: 1, Ack: 1,
    Source Port: 443
    Destination Port: 46978
    [Stream index: 0]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 1370]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 17475569
    [Next Sequence Number: 1371    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2747439716
```

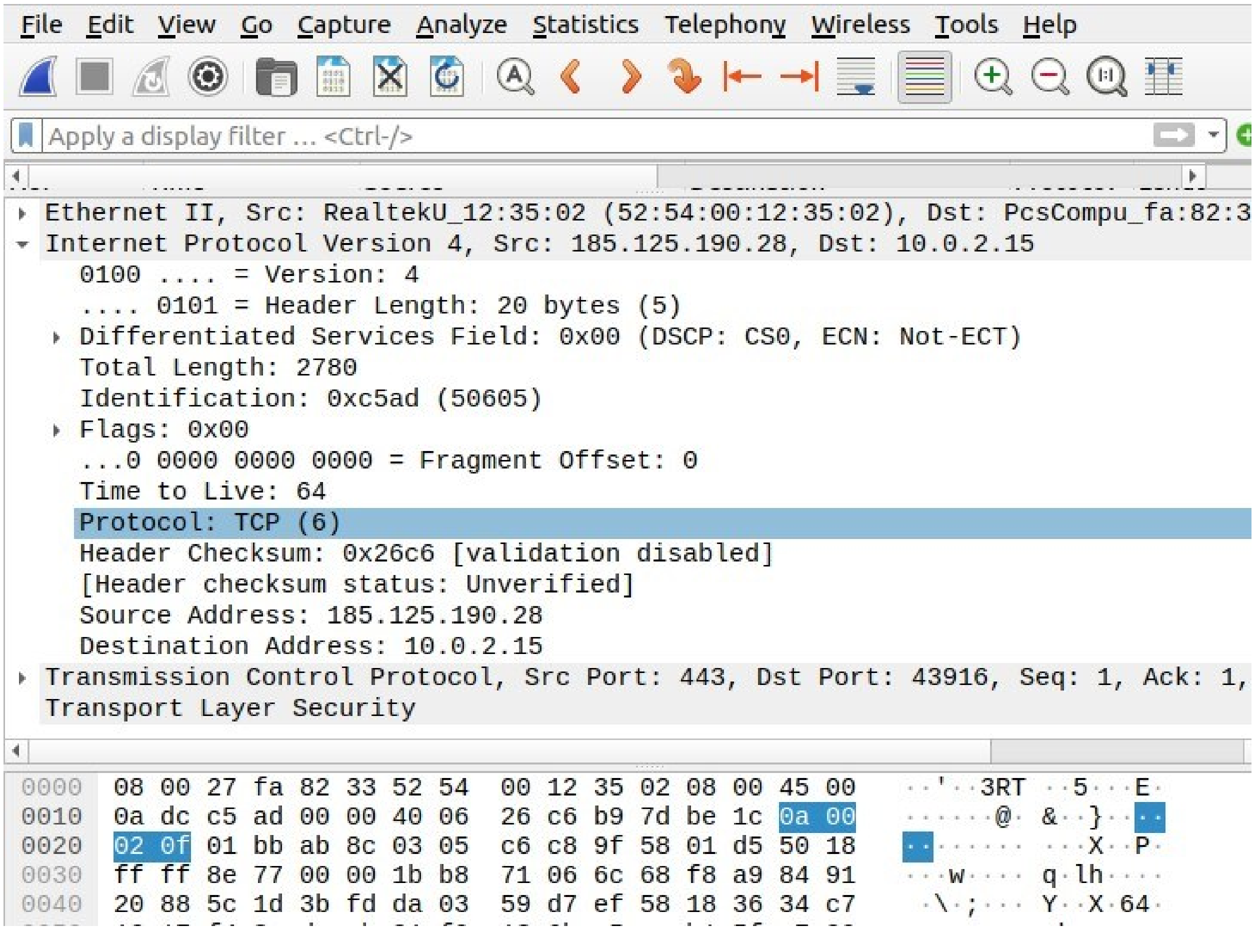
(iii)dig:



```
No.       Time          Source            Destination       Protocol  Lengt
        1 0.000000000   185.125.190.28    10.0.2.15         SSL        279
        2 0.000022650   10.0.2.15         185.125.190.28    TCP          5
        3 0.000120522   185.125.190.28    10.0.2.15         SSL        443
        4 0.000126730   10.0.2.15         185.125.190.28    TCP          5
        5 0.000270200   185.125.190.28    10.0.2.15         SSL        389
        6 0.000274866   10.0.2.15         185.125.190.28    TCP          5
        7 0.018443436   185.125.190.28    10.0.2.15         SSL        142
        8 0.018510652   10.0.2.15         185.125.190.28    TCP          5
        9 0.018824631   185.125.190.28    10.0.2.15         SSL        142
       10 0.018893307   10.0.2.15         185.125.190.28    TCP          5
       11 0.143212865   185.125.190.28    10.0.2.15         SSL        416
       12 0.143241921   10.0.2.15         185.125.190.28    TCP          5
```

```
▾ Frame 1: 2794 bytes on wire (22352 bits), 2794 bytes captured (22352 bits) on
    ▸ Interface id: 0 (enp0s3)
      Encapsulation type: Ethernet (1)
      Arrival Time: Jan 24, 2023 11:29:28.065334041 IST
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1674539968.065334041 seconds
      [Time delta from previous captured frame: 0.000000000 seconds]
      [Time delta from previous displayed frame: 0.000000000 seconds]
      [Time since reference or first frame: 0.000000000 seconds]
```

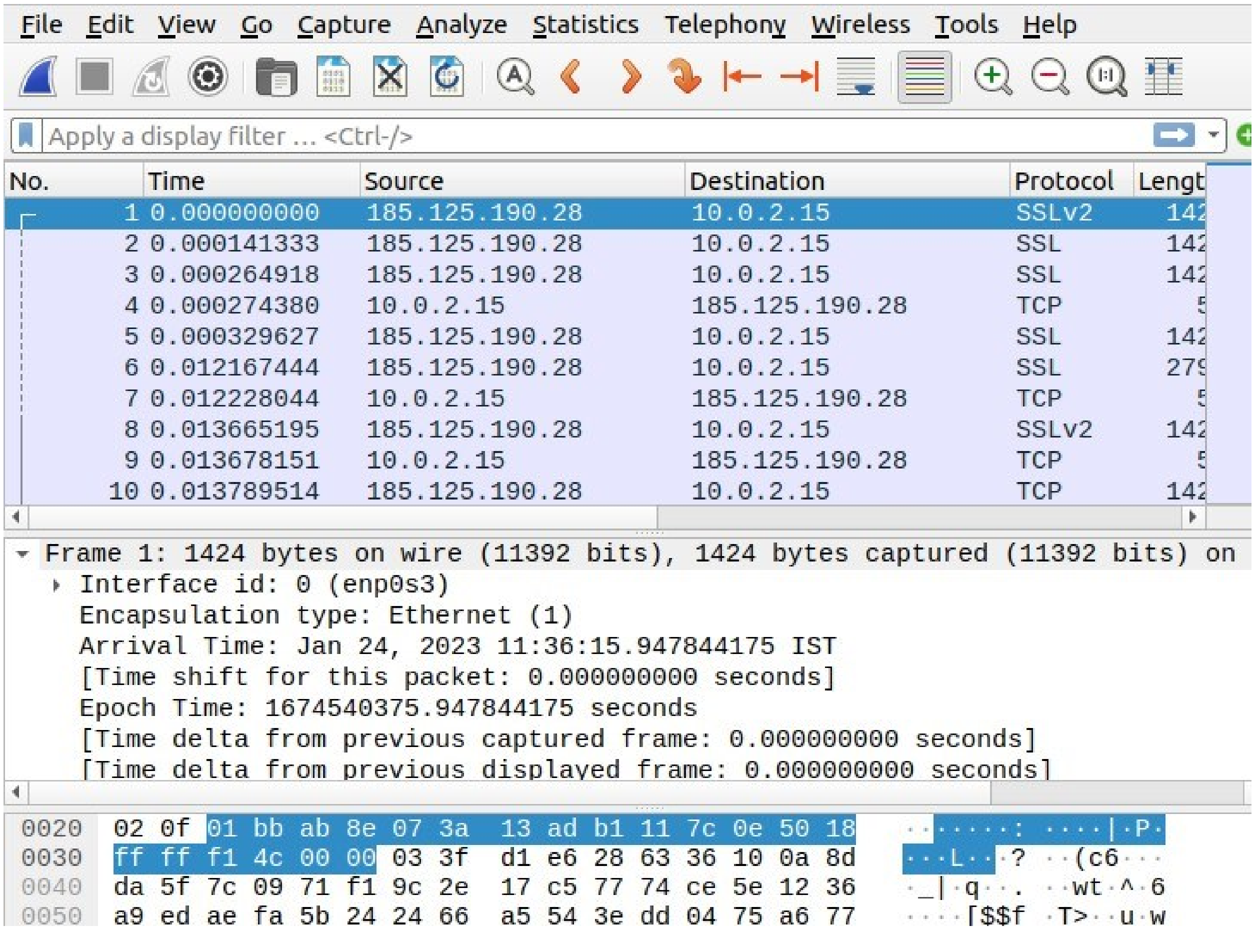
Analysis:



```
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_fa:82:3
▾ Internet Protocol Version 4, Src: 185.125.190.28, 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: 2780
     Identification: 0xc5ad (50605)
   ▸ Flags: 0x00
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 64
     Protocol: TCP (6)
     Header Checksum: 0x26c6 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 185.125.190.28
     Destination Address: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 43916, Seq: 1, Ack: 1,
  Transport Layer Security
```

```
0000  08 00 27 fa 82 33 52 54  00 12 35 02 08 00 45 00   ··'··3RT ··5···E·
0010  0a dc c5 ad 00 00 40 06  26 c6 b9 7d be 1c 0a 00   ······@· &··}····
0020  02 0f 01 bb ab 8c 03 05  c6 c8 9f 58 01 d5 50 18   ········ ···X··P·
0030  ff ff 8e 77 00 00 1b b8  71 06 6c 68 f8 a9 84 91   ···w···· q·lh····
0040  20 88 5c 1d 3b fd da 03  59 d7 ef 58 18 36 34 c7    ·\·;··· Y··X·64·
```

(iv)arp:

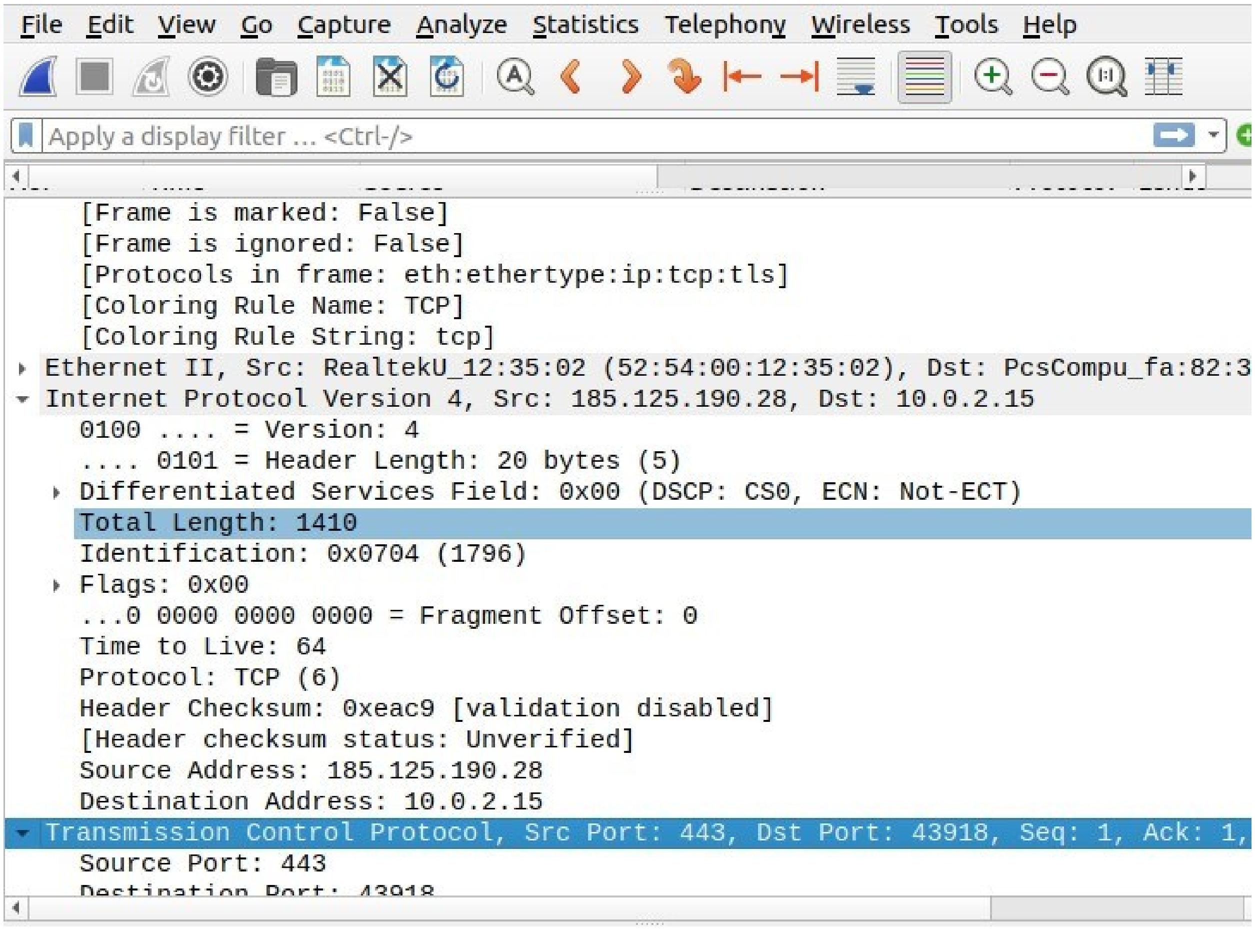

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.    Time         Source            Destination       Protocol  Lengt
     1 0.000000000  185.125.190.28    10.0.2.15         SSLv2      142
     2 0.000141333  185.125.190.28    10.0.2.15         SSL        142
     3 0.000264918  185.125.190.28    10.0.2.15         SSL        142
     4 0.000274380  10.0.2.15         185.125.190.28    TCP          5
     5 0.000329627  185.125.190.28    10.0.2.15         SSL        142
     6 0.012167444  185.125.190.28    10.0.2.15         SSL        279
     7 0.012228044  10.0.2.15         185.125.190.28    TCP          5
     8 0.013665195  185.125.190.28    10.0.2.15         SSLv2      142
     9 0.013678151  10.0.2.15         185.125.190.28    TCP          5
    10 0.013789514  185.125.190.28    10.0.2.15         TCP        142
```

```
▾ Frame 1: 1424 bytes on wire (11392 bits), 1424 bytes captured (11392 bits) on
  ▸ Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 24, 2023 11:36:15.947844175 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1674540375.947844175 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
```

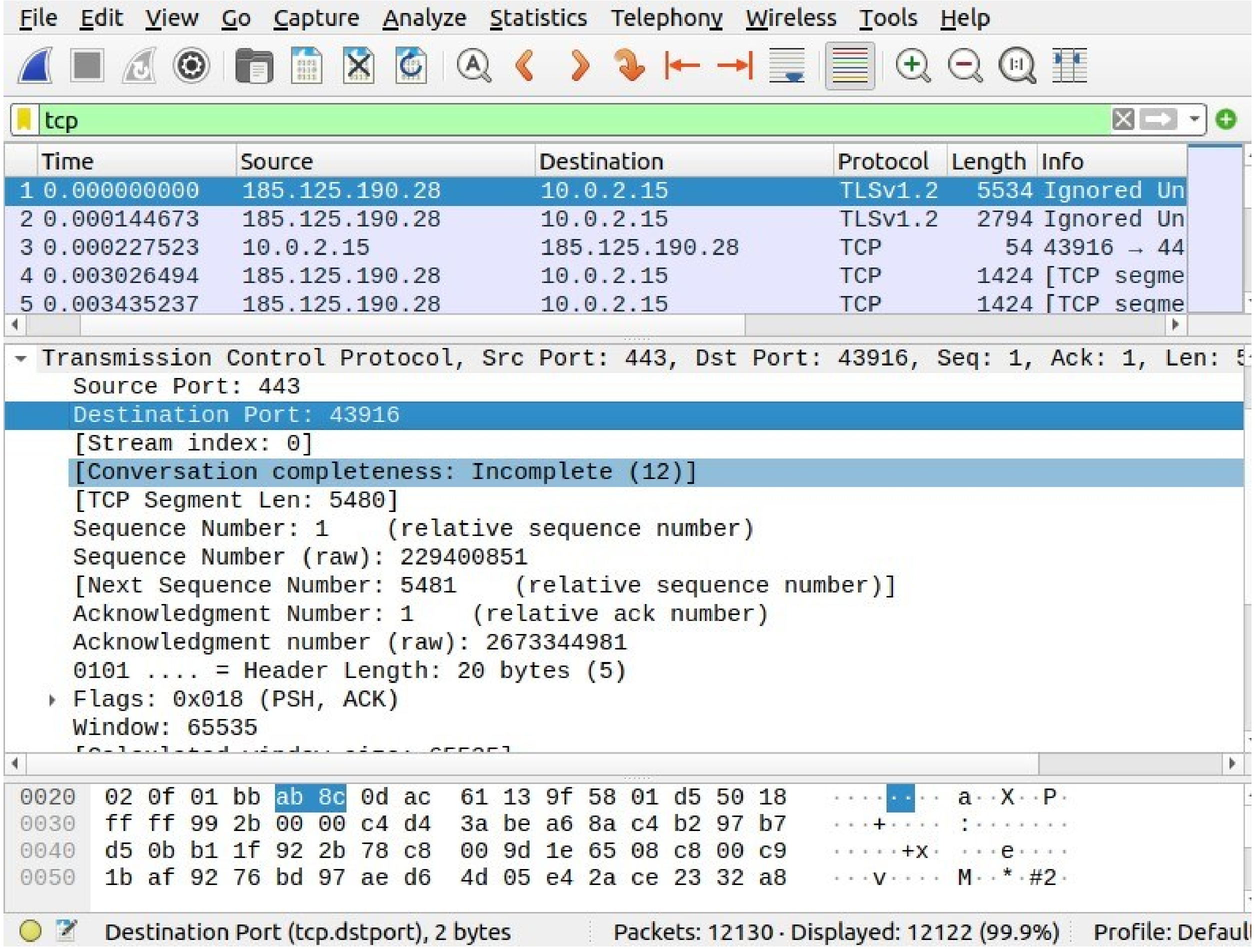
```
0020  02 0f 01 bb ab 8e 07 3a  13 ad b1 11 7c 0e 50 18   ········: ····|·P·
0030  ff ff f1 4c 00 00 03 3f  d1 e6 28 63 36 10 0a 8d   ···L···? ··(c6···
0040  da 5f 7c 09 71 f1 9c 2e  17 c5 77 74 ce 5e 12 36   ·_|·q··. ··wt·^·6
0050  a9 ed ae fa 5b 24 24 66  a5 54 3e dd 04 75 a6 77   ····[$$f ·T>··u·w
```

Analysis:



```
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_fa:82:3
▾ Internet Protocol Version 4, Src: 185.125.190.28, 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: 1410
    Identification: 0x0704 (1796)
  ▸ Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xeac9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 185.125.190.28
    Destination Address: 10.0.2.15
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 43918, Seq: 1, Ack: 1,
    Source Port: 443
    Destination Port: 43918
```

(v)wget:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

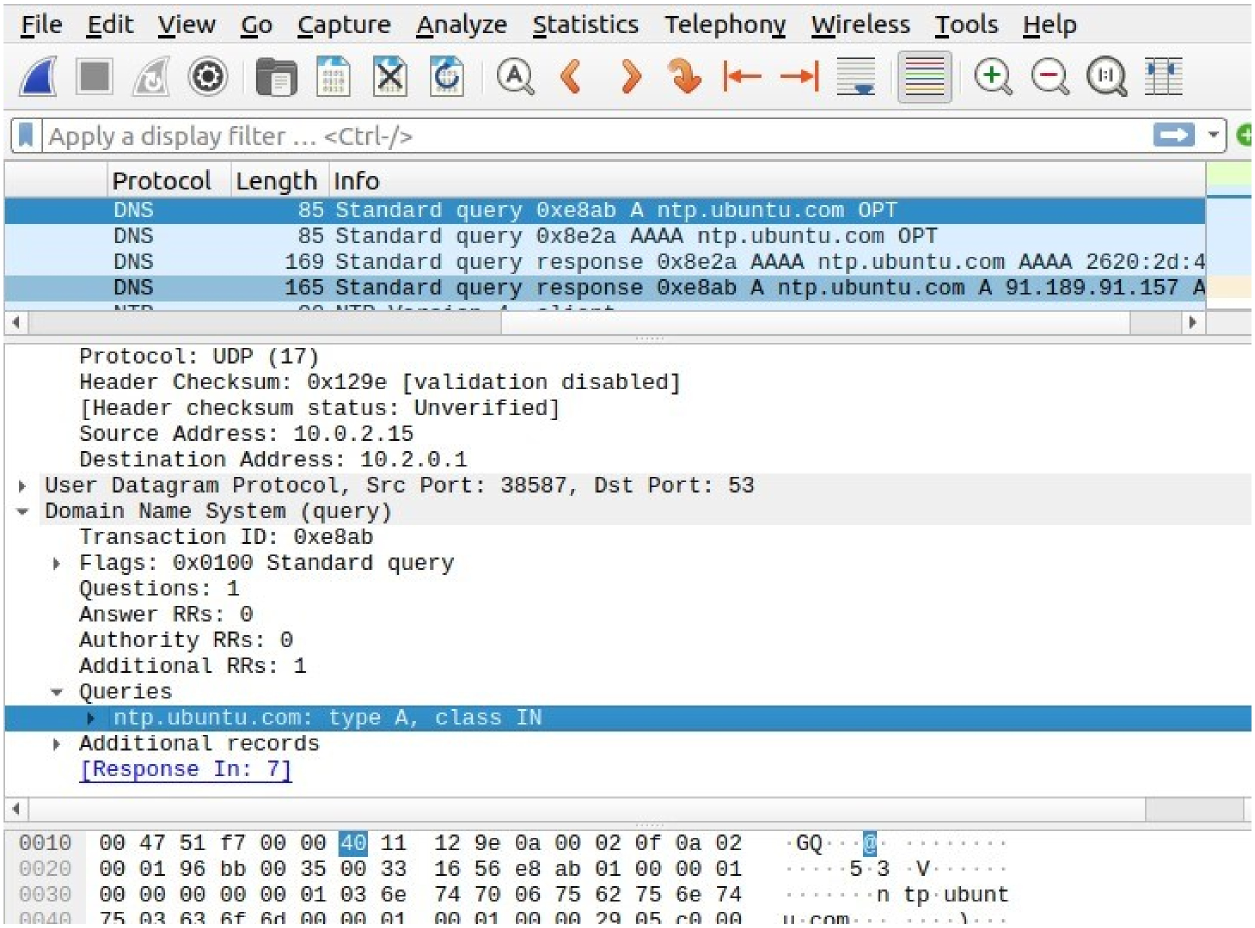
```
   Time          Source            Destination       Protocol  Length Info
 1 0.000000000   185.125.190.28    10.0.2.15         TLSv1.2     5534 Ignored Un
 2 0.000144673   185.125.190.28    10.0.2.15         TLSv1.2     2794 Ignored Un
 3 0.000227523   10.0.2.15         185.125.190.28    TCP           54 43916 → 44
 4 0.003026494   185.125.190.28    10.0.2.15         TCP         1424 [TCP segme
 5 0.003435237   185.125.190.28    10.0.2.15         TCP         1424 [TCP segme
```

```
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 43916, Seq: 1, Ack: 1, Len: 5
    Source Port: 443
    Destination Port: 43916
    [Stream index: 0]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 5480]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 229400851
    [Next Sequence Number: 5481    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2673344981
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 65535
    [Calculated window size: 65535]
```

```
0020  02 0f 01 bb ab 8c 0d ac  61 13 9f 58 01 d5 50 18   ········ a··X··P·
0030  ff ff 99 2b 00 00 c4 d4  3a be a6 8a c4 b2 97 b7   ···+···· :·······
0040  d5 0b b1 1f 92 2b 78 c8  00 9d 1e 65 08 c8 00 c9   ·····+x· ···e····
0050  1b af 92 76 bd 97 ae d6  4d 05 e4 2a ce 23 32 a8   ···v···· M··*·#2·
```

Destination Port (tcp.dstport), 2 bytes   Packets: 12130 · Displayed: 12122 (99.9%)   Profile: Defaul

2. Capture the packets whilesending/receiving telnet request/response between your computer and a custom server running the telnet daemon. What is your observation while analyzing the application layer data?

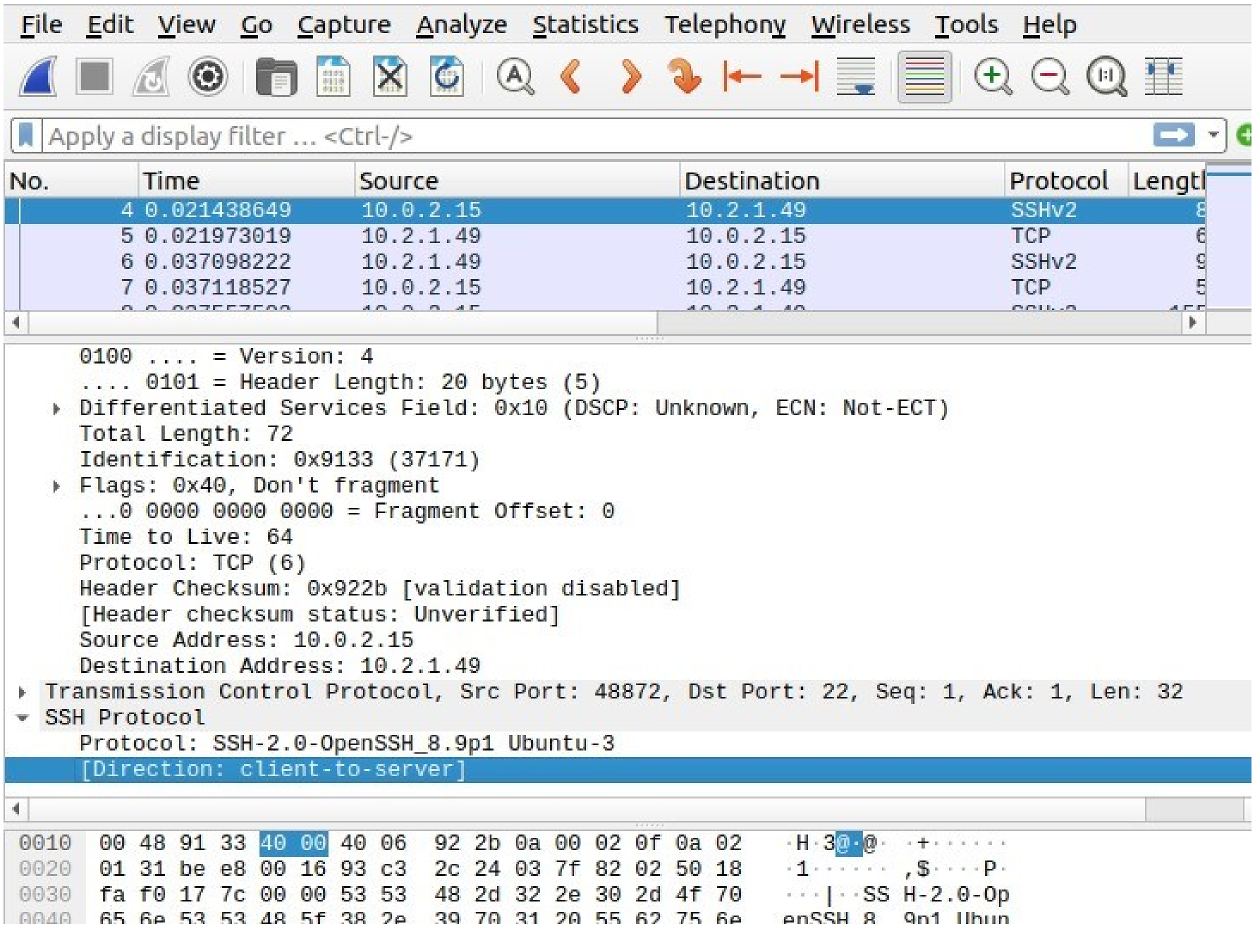

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
Protocol  Length  Info
DNS           85  Standard query 0xe8ab A ntp.ubuntu.com OPT
DNS           85  Standard query 0x8e2a AAAA ntp.ubuntu.com OPT
DNS          169  Standard query response 0x8e2a AAAA ntp.ubuntu.com AAAA 2620:2d:4
DNS          165  Standard query response 0xe8ab A ntp.ubuntu.com A 91.189.91.157 A
NTP           90  NTP Version 4, client
```

```
    Protocol: UDP (17)
    Header Checksum: 0x129e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 10.2.0.1
▸ User Datagram Protocol, Src Port: 38587, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xe8ab
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ ntp.ubuntu.com: type A, class IN
  ▸ Additional records
    [Response In: 7]
```

```
0010  00 47 51 f7 00 00 40 11  12 9e 0a 00 02 0f 0a 02   ·GQ···@· ········
0020  00 01 96 bb 00 35 00 33  16 56 e8 ab 01 00 00 01   ·····5·3 ·V······
0030  00 00 00 00 00 01 03 6e  74 70 06 75 62 75 6e 74   ·······n tp·ubunt
0040  75 03 63 6f 6d 00 00 01  00 01 00 00 29 05 c0 00   u·com··· ····)···
```

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


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.      Time          Source        Destination   Protocol  Lengtl
       4 0.021438649   10.0.2.15     10.2.1.49     SSHv2          8
       5 0.021973019   10.2.1.49     10.0.2.15     TCP            6
       6 0.037098222   10.2.1.49     10.0.2.15     SSHv2          9
       7 0.037118527   10.0.2.15     10.2.1.49     TCP            5
```

```
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▸ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
      Total Length: 72
      Identification: 0x9133 (37171)
    ▸ Flags: 0x40, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: TCP (6)
      Header Checksum: 0x922b [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 10.0.2.15
      Destination Address: 10.2.1.49
▸ Transmission Control Protocol, Src Port: 48872, Dst Port: 22, Seq: 1, Ack: 1, Len: 32
▾ SSH Protocol
      Protocol: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
      [Direction: client-to-server]
```

```
0010  00 48 91 33 40 00 40 06  92 2b 0a 00 02 0f 0a 02   ·H·3@·@· ·+······
0020  01 31 be e8 00 16 93 c3  2c 24 03 7f 82 02 50 18   ·1······ ,$····P·
0030  fa f0 17 7c 00 00 53 53  48 2d 32 2e 30 2d 4f 70   ···|··SS H-2.0-Op
0040  65 6e 53 53 48 5f 38 2e  39 70 31 20 55 62 75 6e   enSSH_8. 9p1 Ubun
```

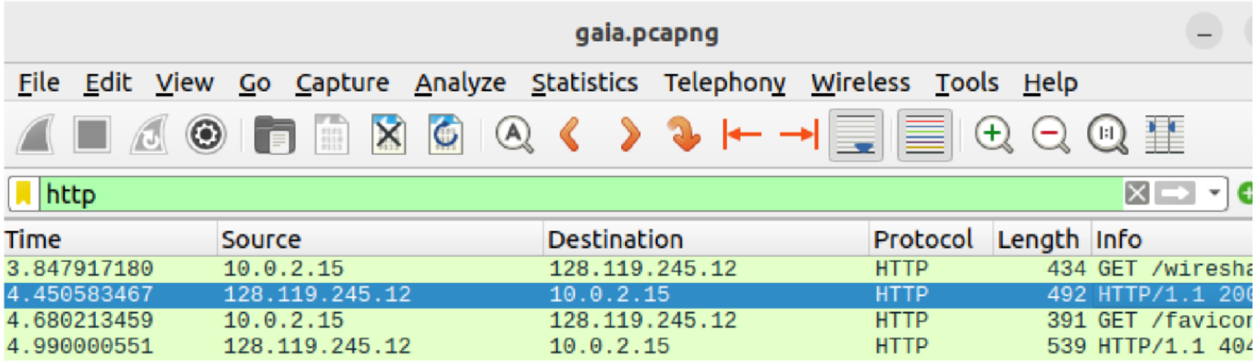
As we can see that the packet has given us the name of the protocol, i.e., SSH with version number and also, we got to know about what Operating System is running the device on both server and client end.

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 HTTPGET message was sent until the HTTP OK reply was received?



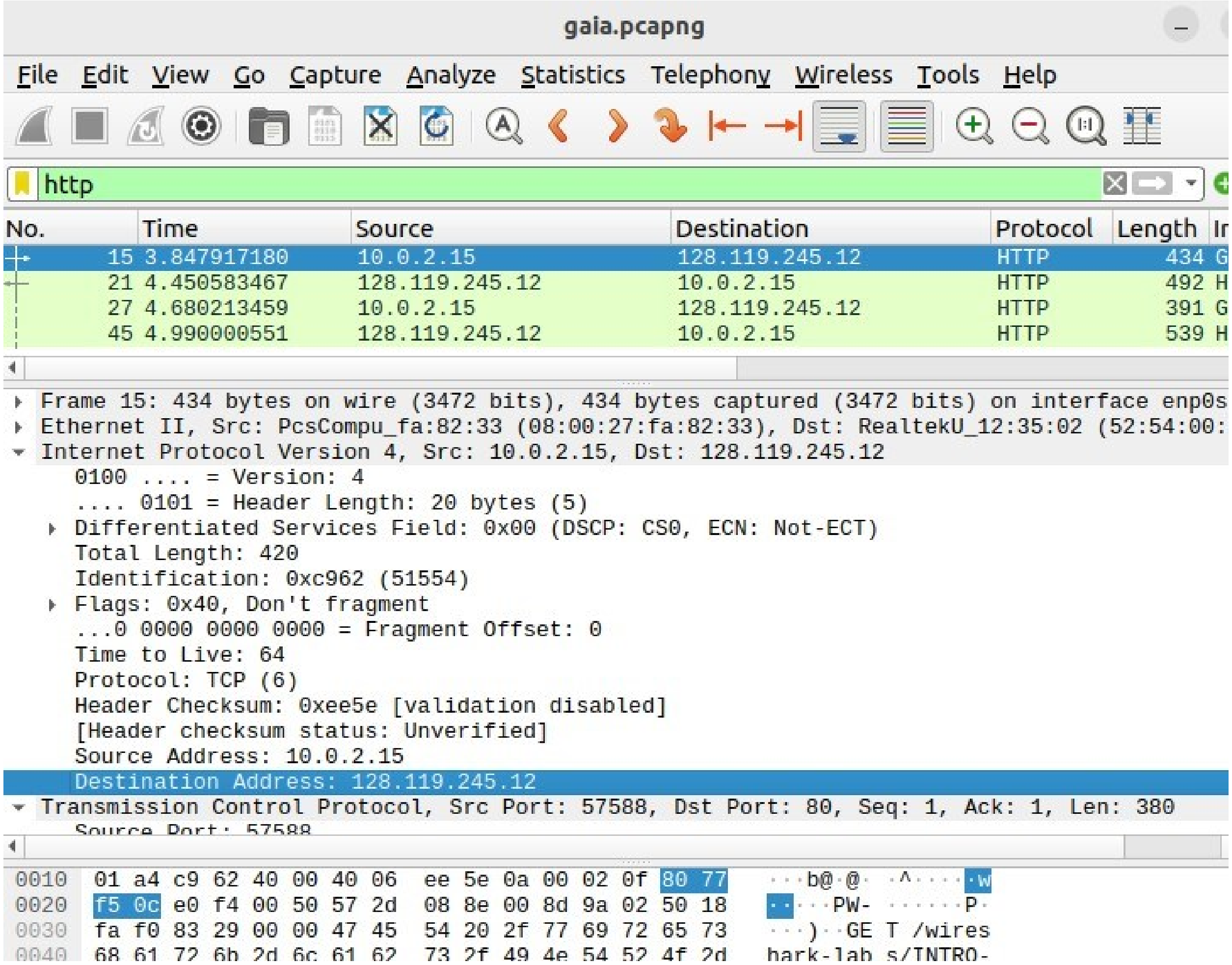
http

Time	Source	Destination	Protocol	Length	Info
3.847917180	10.0.2.15	128.119.245.12	HTTP	434	GET /wiresha
4.450583467	128.119.245.12	10.0.2.15	HTTP	492	HTTP/1.1 200
4.680213459	10.0.2.15	128.119.245.12	HTTP	391	GET /favicon
4.990000551	128.119.245.12	10.0.2.15	HTTP	539	HTTP/1.1 404

Time Difference: 4.450583467 - 3.847917180 = **0.602666287s**.

b. What is the Internet address of thegaia.cs.umass.edu? What is the Internet

address of your computer? Support your answer with an appropriate screenshot from your computer.


gaia.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

No.	Time	Source	Destination	Protocol	Length	I
15	3.847917180	10.0.2.15	128.119.245.12	HTTP	434	G
21	4.450583467	128.119.245.12	10.0.2.15	HTTP	492	H
27	4.680213459	10.0.2.15	128.119.245.12	HTTP	391	G
45	4.990000551	128.119.245.12	10.0.2.15	HTTP	539	H

```
▸ Frame 15: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface enp0s
▸ Ethernet II, Src: PcsCompu_fa:82:33 (08:00:27:fa:82:33), Dst: RealtekU_12:35:02 (52:54:00:
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 420
     Identification: 0xc962 (51554)
   ▸ Flags: 0x40, Don't fragment
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 64
     Protocol: TCP (6)
     Header Checksum: 0xee5e [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 10.0.2.15
     Destination Address: 128.119.245.12
▾ Transmission Control Protocol, Src Port: 57588, Dst Port: 80, Seq: 1, Ack: 1, Len: 380
     Source Port: 57588
```

```
0010  01 a4 c9 62 40 00 40 06  ee 5e 0a 00 02 0f 80 77   ···b@·@· ·^·····w
0020  f5 0c e0 f4 00 50 57 2d  08 8e 00 8d 9a 02 50 18   ····PW- ······P·
0030  fa f0 83 29 00 00 47 45  54 20 2f 77 69 72 65 73   ···)··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
```

Device IP: **10.0.2.15**

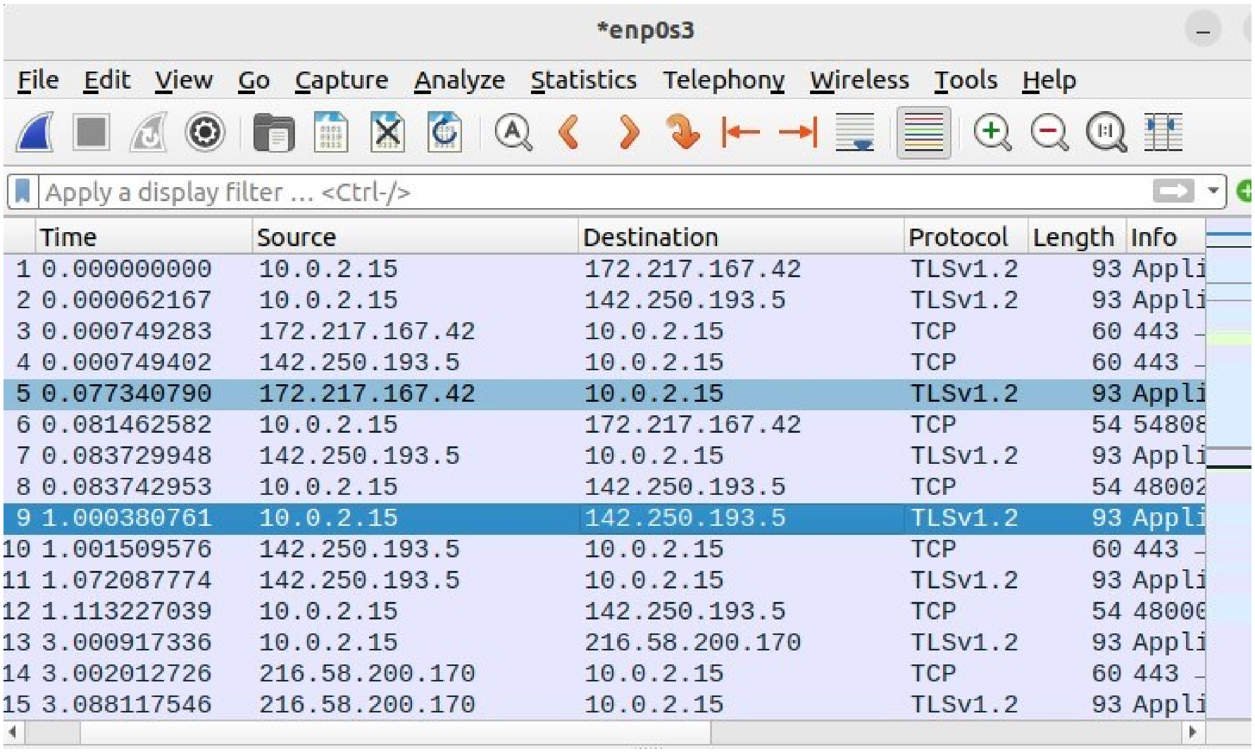
Website IP: **128.119.245.12**

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:

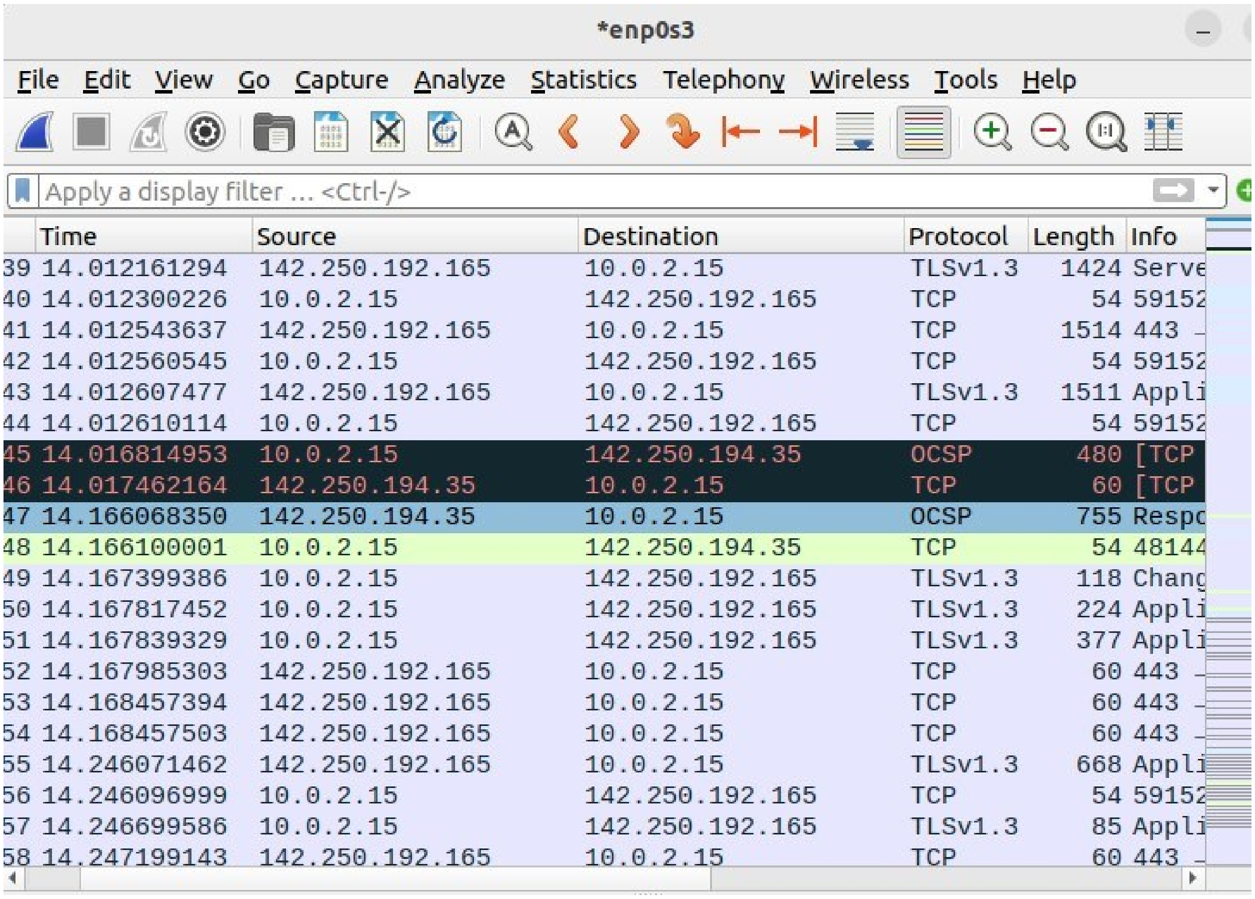
a. Is there any difference in the applicationlayer protocol?


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	172.217.167.42	TLSv1.2	93	Appli
2	0.000062167	10.0.2.15	142.250.193.5	TLSv1.2	93	Appli
3	0.000749283	172.217.167.42	10.0.2.15	TCP	60	443 –
4	0.000749402	142.250.193.5	10.0.2.15	TCP	60	443 –
5	0.077340790	172.217.167.42	10.0.2.15	TLSv1.2	93	Appli
6	0.081462582	10.0.2.15	172.217.167.42	TCP	54	54808
7	0.083729948	142.250.193.5	10.0.2.15	TLSv1.2	93	Appli
8	0.083742953	10.0.2.15	142.250.193.5	TCP	54	48002
9	1.000380761	10.0.2.15	142.250.193.5	TLSv1.2	93	Appli
10	1.001509576	142.250.193.5	10.0.2.15	TCP	60	443 –
11	1.072087774	142.250.193.5	10.0.2.15	TLSv1.2	93	Appli
12	1.113227039	10.0.2.15	142.250.193.5	TCP	54	48006
13	3.000917336	10.0.2.15	216.58.200.170	TLSv1.2	93	Appli
14	3.002012726	216.58.200.170	10.0.2.15	TCP	60	443 –
15	3.088117546	216.58.200.170	10.0.2.15	TLSv1.2	93	Appli

In the previous question, we have seen http but now TCP. This is the difference in Application layer protocol.

b. How is it different from the HTTP data youanalyzed in the above problem?


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

	Time	Source	Destination	Protocol	Length	Info
39	14.012161294	142.250.192.165	10.0.2.15	TLSv1.3	1424	Serve
40	14.012300226	10.0.2.15	142.250.192.165	TCP	54	59152
41	14.012543637	142.250.192.165	10.0.2.15	TCP	1514	443 -
42	14.012560545	10.0.2.15	142.250.192.165	TCP	54	59152
43	14.012607477	142.250.192.165	10.0.2.15	TLSv1.3	1511	Appli
44	14.012610114	10.0.2.15	142.250.192.165	TCP	54	59152
45	14.016814953	10.0.2.15	142.250.194.35	OCSP	480	[TCP
46	14.017462164	142.250.194.35	10.0.2.15	TCP	60	[TCP
47	14.166068350	142.250.194.35	10.0.2.15	OCSP	755	Respo
48	14.166100001	10.0.2.15	142.250.194.35	TCP	54	48144
49	14.167399386	10.0.2.15	142.250.192.165	TLSv1.3	118	Chang
50	14.167817452	10.0.2.15	142.250.192.165	TLSv1.3	224	Appli
51	14.167839329	10.0.2.15	142.250.192.165	TLSv1.3	377	Appli
52	14.167985303	142.250.192.165	10.0.2.15	TCP	60	443 -
53	14.168457394	142.250.192.165	10.0.2.15	TCP	60	443 -
54	14.168457503	142.250.192.165	10.0.2.15	TCP	60	443 -
55	14.246071462	142.250.192.165	10.0.2.15	TLSv1.3	668	Appli
56	14.246096999	10.0.2.15	142.250.192.165	TCP	54	59152
57	14.246699586	10.0.2.15	142.250.192.165	TLSv1.3	85	Appli
58	14.247199143	142.250.192.165	10.0.2.15	TCP	60	443 -

Here we can see GMAIL packets are OCSP certified (OSCP- Online Certificate Status Protocol) which is an Internet protocol. Here we used a password to login which is encrypted, so these packets are OCSP certified.HTTPS (HyperText Transfer Protocol Secure) is the secure version of HTTP where SSl/TLS encrypts communications. HTTPS uses TLS

(SSL) to encrypt normal HTTP requests and responses, making it safer and more secure.