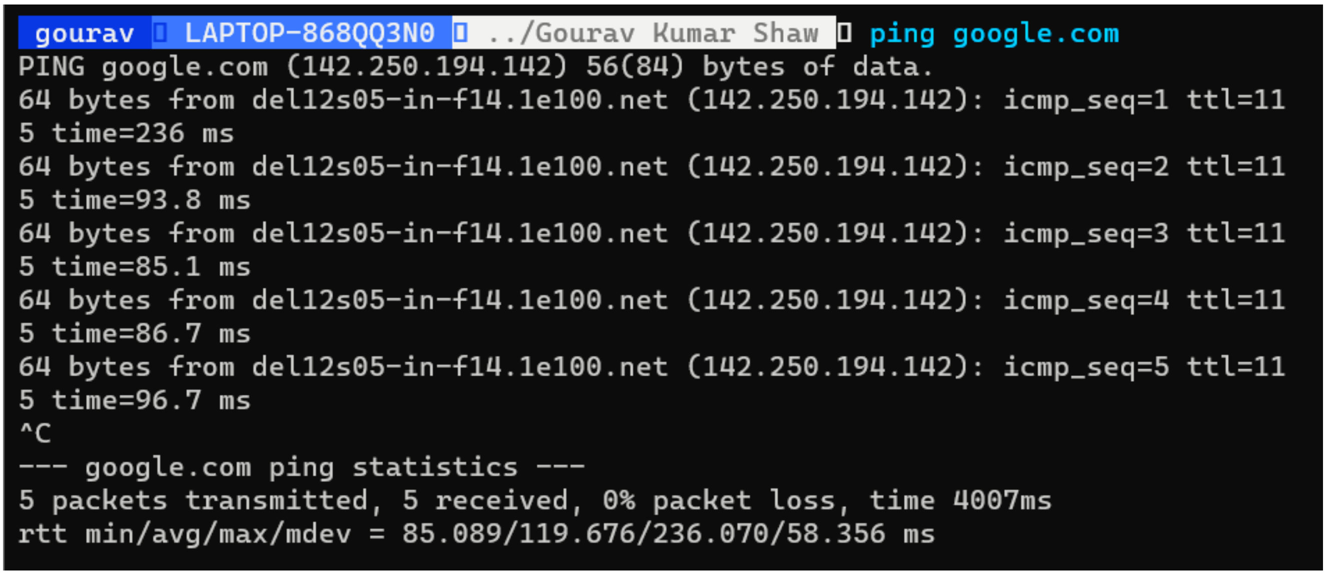
Name : Gourav Kumar Shaw
Enrollment Id. : 2020CSB010
Section: Gx
Subject : Computer Network Lab (CS 3272)

Assignment – 2

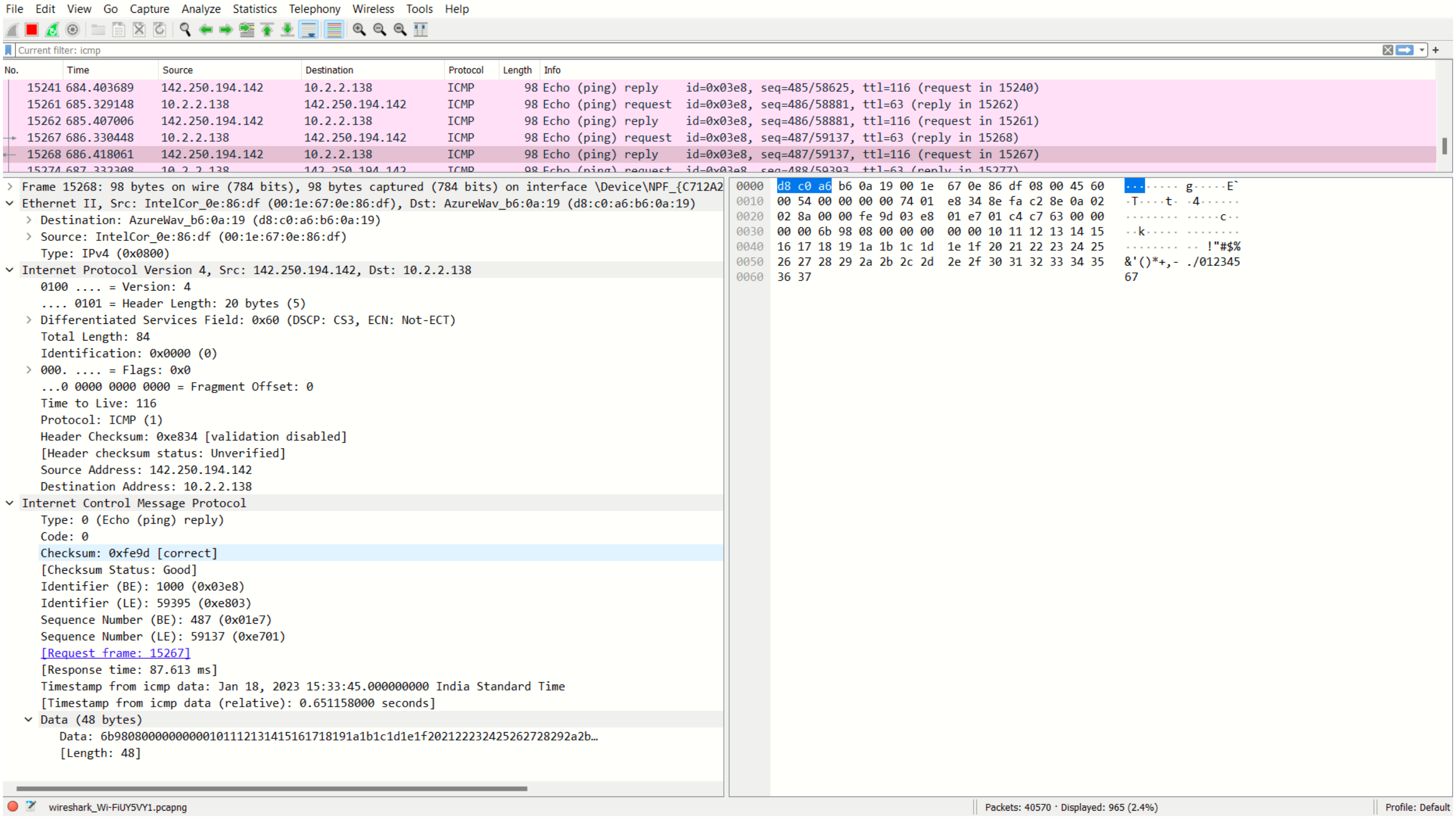
Q1. Analyse the packets (across all layers) exchanged with your computer while executing the following commands: (i) ping, (ii) traceroute, (iii) dig, (iv) arp,(v)wget.

Answer:

i)ping
→**Application layer:-** DNS, MDNS, TLS, HTTP
→**Transport layer:-** TCP
→**Network layer :-** ICMP



```
 gourav ▯ LAPTOP-868QQ3N0 ▯ ../Gourav Kumar Shaw ▯ ping google.com
PING google.com (142.250.194.142) 56(84) bytes of data.
64 bytes from del12s05-in-f14.1e100.net (142.250.194.142): icmp_seq=1 ttl=11
5 time=236 ms
64 bytes from del12s05-in-f14.1e100.net (142.250.194.142): icmp_seq=2 ttl=11
5 time=93.8 ms
64 bytes from del12s05-in-f14.1e100.net (142.250.194.142): icmp_seq=3 ttl=11
5 time=85.1 ms
64 bytes from del12s05-in-f14.1e100.net (142.250.194.142): icmp_seq=4 ttl=11
5 time=86.7 ms
64 bytes from del12s05-in-f14.1e100.net (142.250.194.142): icmp_seq=5 ttl=11
5 time=96.7 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 85.089/119.676/236.070/58.356 ms
```



```
No.   Time        Source           Destination      Protocol  Length Info
15241 684.403689  142.250.194.142  10.2.2.138       ICMP        98 Echo (ping) reply    id=0x03e8, seq=485/58625, ttl=116 (request in 15240)
15261 685.329148  10.2.2.138       142.250.194.142  ICMP        98 Echo (ping) request  id=0x03e8, seq=486/58881, ttl=63 (reply in 15262)
15262 685.407006  142.250.194.142  10.2.2.138       ICMP        98 Echo (ping) reply    id=0x03e8, seq=486/58881, ttl=116 (request in 15261)
15267 686.330448  10.2.2.138       142.250.194.142  ICMP        98 Echo (ping) request  id=0x03e8, seq=487/59137, ttl=63 (reply in 15268)
15268 686.418061  142.250.194.142  10.2.2.138       ICMP        98 Echo (ping) reply    id=0x03e8, seq=487/59137, ttl=116 (request in 15267)
15274 687.332308  10.2.2.138       142.250.194.142  ICMP        98 Echo (ping) request  id=0x03e8, seq=488/59393, ttl=63 (reply in 15277)
```

```
> Frame 15268: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{C712A2
v Ethernet II, Src: IntelCor_0e:86:df (00:1e:67:0e:86:df), Dst: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
  > Destination: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
  > Source: IntelCor_0e:86:df (00:1e:67:0e:86:df)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 142.250.194.142, Dst: 10.2.2.138
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x60 (DSCP: CS3, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 116
    Protocol: ICMP (1)
    Header Checksum: 0xe834 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 142.250.194.142
    Destination Address: 10.2.2.138
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xfe9d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1000 (0x03e8)
    Identifier (LE): 59395 (0xe803)
    Sequence Number (BE): 487 (0x01e7)
    Sequence Number (LE): 59137 (0xe701)
    [Request frame: 15267]
    [Response time: 87.613 ms]
    Timestamp from icmp data: Jan 18, 2023 15:33:45.000000000 India Standard Time
    [Timestamp from icmp data (relative): 0.651158000 seconds]
  v Data (48 bytes)
      Data: 6b98080000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
```

```
0000  d8 c0 a6 b6 0a 19 00 1e  67 0e 86 df 08 00 45 60   ········ g·····E`
0010  00 54 00 00 00 00 74 01  e8 34 8e fa c2 8e 0a 02   ·T····t· ·4······
0020  02 8a 00 00 fe 9d 03 e8  01 e7 01 c4 c7 63 00 00   ········ ·····c··
0030  00 00 6b 98 08 00 00 00  00 00 10 11 12 13 14 15   ··k····· ········
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   &'()*+,- ./012345
0060  36 37                                               67
```

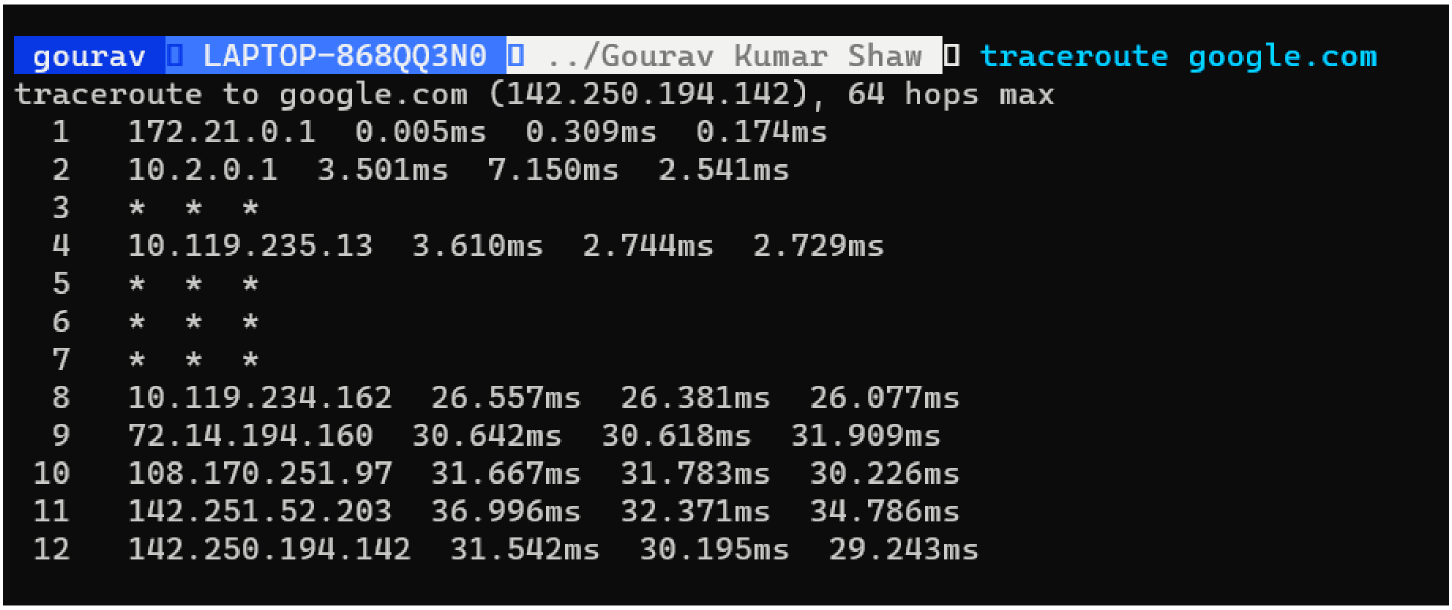
wireshark_Wi-FiUY5VY1.pcapng | Packets: 40570 · Displayed: 965 (2.4%) | Profile: Default

ii)traceroute

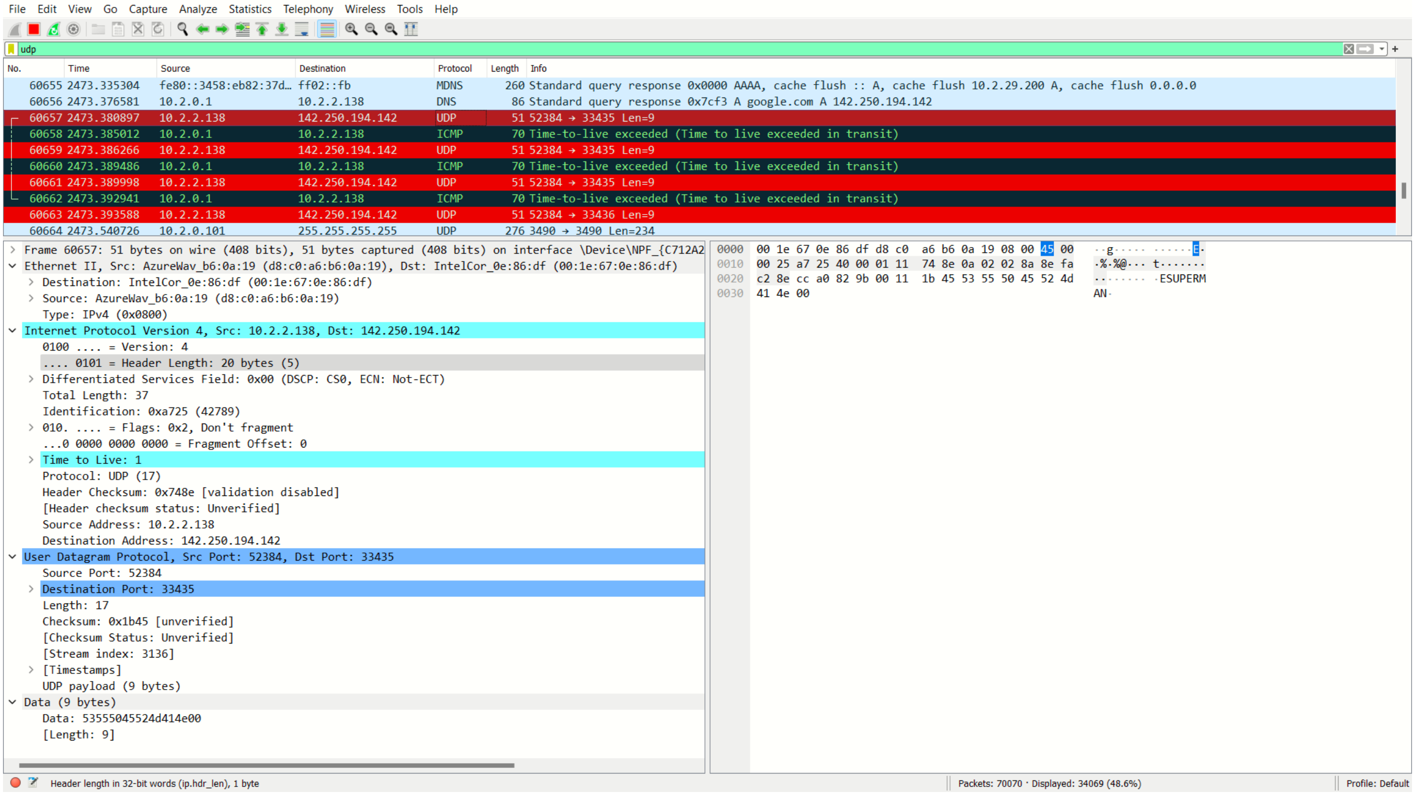
→**Application layer:-** DNS,TLS

→**Transport layer:-** TCP,UDP

→**Network layer :-** ICMP



```
 gourav ▯ LAPTOP-868QQ3N0 ▯ ../Gourav Kumar Shaw ▯ traceroute google.com
traceroute to google.com (142.250.194.142), 64 hops max
  1   172.21.0.1  0.005ms  0.309ms  0.174ms
  2   10.2.0.1  3.501ms  7.150ms  2.541ms
  3   *  *  *
  4   10.119.235.13  3.610ms  2.744ms  2.729ms
  5   *  *  *
  6   *  *  *
  7   *  *  *
  8   10.119.234.162  26.557ms  26.381ms  26.077ms
  9   72.14.194.160  30.642ms  30.618ms  31.909ms
 10   108.170.251.97  31.667ms  31.783ms  30.226ms
 11   142.251.52.203  36.996ms  32.371ms  34.786ms
 12   142.250.194.142  31.542ms  30.195ms  29.243ms
```



```
udp
```

```
No.   Time         Source              Destination      Protocol  Length Info
60655 2473.335304  fe80::3458:eb82:37d… ff02::fb        MDNS      260 Standard query response 0x0000 AAAA, cache flush :: A, cache flush 10.2.29.200 A, cache flush 0.0.0.0
60656 2473.376581  10.2.0.1            10.2.2.138       DNS        86 Standard query response 0x7cf3 A google.com A 142.250.194.142
60657 2473.380897  10.2.2.138          142.250.194.142  UDP        51 52384 → 33435 Len=9
60658 2473.385012  10.2.0.1            10.2.2.138       ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
60659 2473.386266  10.2.2.138          142.250.194.142  UDP        51 52384 → 33435 Len=9
60660 2473.389486  10.2.0.1            10.2.2.138       ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
60661 2473.389998  10.2.2.138          142.250.194.142  UDP        51 52384 → 33435 Len=9
60662 2473.392941  10.2.0.1            10.2.2.138       ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
60663 2473.393588  10.2.2.138          142.250.194.142  UDP        51 52384 → 33436 Len=9
60664 2473.540726  10.2.0.101          255.255.255.255  UDP       276 3490 → 3490 Len=234
```

```
> Frame 60657: 51 bytes on wire (408 bits), 51 bytes captured (408 bits) on interface \Device\NPF_{C712A2
v Ethernet II, Src: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19), Dst: IntelCor_0e:86:df (00:1e:67:0e:86:df)
  > Destination: IntelCor_0e:86:df (00:1e:67:0e:86:df)
  > Source: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.2.2.138, Dst: 142.250.194.142
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 37
    Identification: 0xa725 (42789)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x748e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.2.2.138
    Destination Address: 142.250.194.142
v User Datagram Protocol, Src Port: 52384, Dst Port: 33435
    Source Port: 52384
  > Destination Port: 33435
    Length: 17
    Checksum: 0x1b45 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3136]
  > [Timestamps]
    UDP payload (9 bytes)
v Data (9 bytes)
    Data: 53555045524d414e00
    [Length: 9]
```

```
0000  00 1e 67 0e 86 df d8 c0  a6 b6 0a 19 08 00 45 00   ··g····· ······E·
0010  00 25 a7 25 40 00 01 11  74 8e 0a 02 02 8a 8e fa   ·%·%@··· t·······
0020  c2 8e cc a0 82 9b 00 11  1b 45 53 55 50 45 52 4d   ········ ·ESUPERM
0030  41 4e 00                                           AN·
```

Header length in 32-bit words (ip.hdr_len), 1 byte

Packets: 70070 · Displayed: 34069 (48.6%)

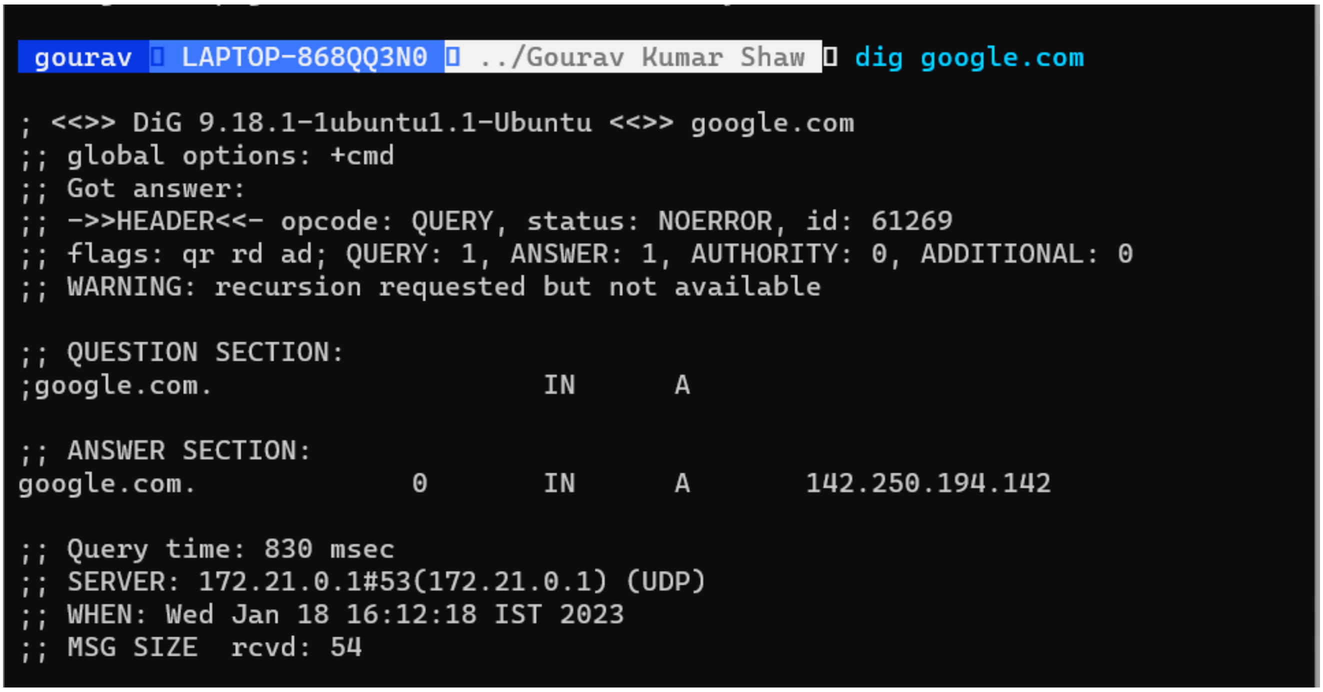
Profile: Default

iii)**dig**

→**Application layer:-** DNS,TLS

→**Transport layer:-** TCP

→**Network layer :-** ICMP



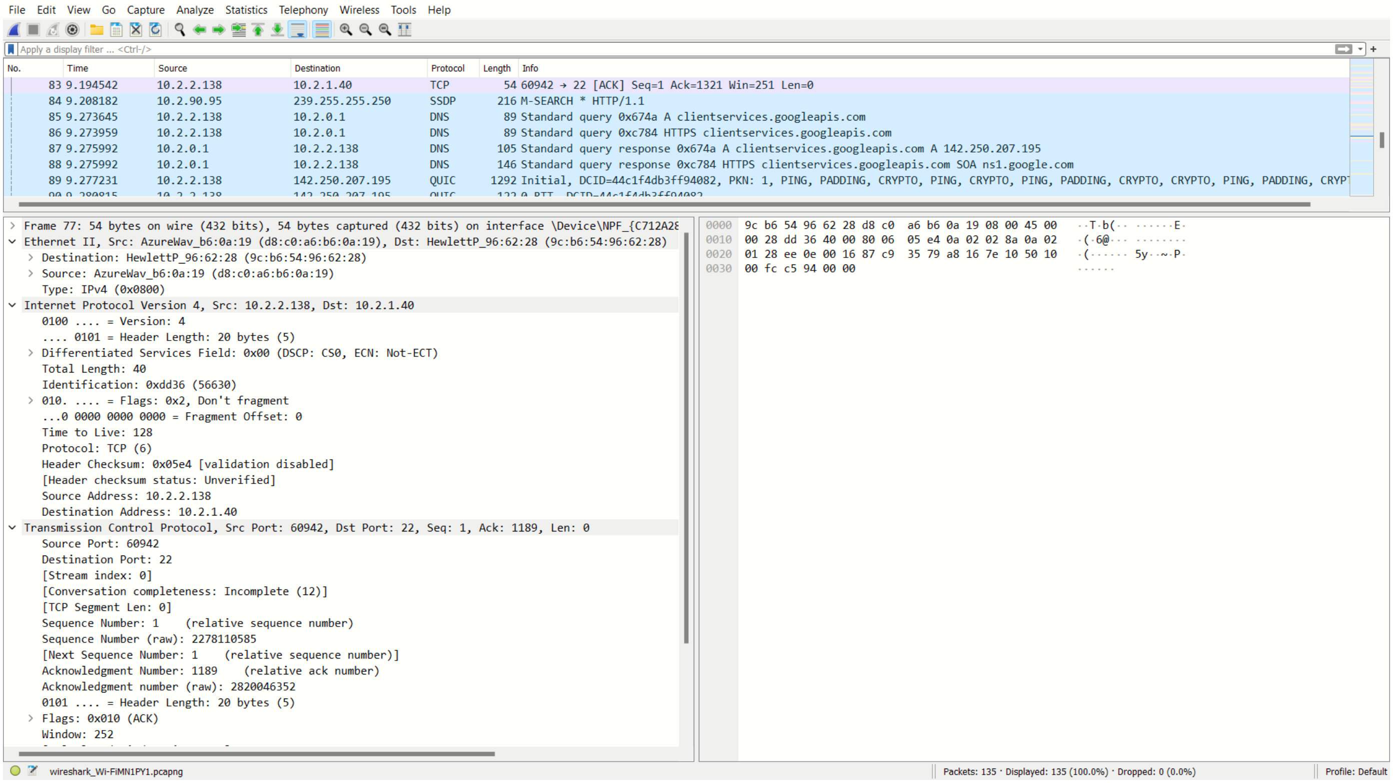
```
 gourav  LAPTOP-868QQ3N0  ../Gourav Kumar Shaw  dig google.com

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61269
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             0       IN      A       142.250.194.142

;; Query time: 830 msec
;; SERVER: 172.21.0.1#53(172.21.0.1) (UDP)
;; WHEN: Wed Jan 18 16:12:18 IST 2023
;; MSG SIZE  rcvd: 54
```


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

```
No.   Time       Source         Destination      Protocol Length Info
   83 9.194542   10.2.2.138     10.2.1.40        TCP        54 60942 → 22 [ACK] Seq=1 Ack=1321 Win=251 Len=0
   84 9.208182   10.2.90.95     239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
   85 9.273645   10.2.2.138     10.2.0.1         DNS        89 Standard query 0x674a A clientservices.googleapis.com
   86 9.273959   10.2.2.138     10.2.0.1         DNS        89 Standard query 0xc784 HTTPS clientservices.googleapis.com
   87 9.275992   10.2.0.1       10.2.2.138       DNS       105 Standard query response 0x674a A clientservices.googleapis.com A 142.250.207.195
   88 9.275992   10.2.0.1       10.2.2.138       DNS       146 Standard query response 0xc784 HTTPS clientservices.googleapis.com SOA ns1.google.com
   89 9.277231   10.2.2.138     142.250.207.195  QUIC     1292 Initial, DCID=44c1f4db3ff94082, PKN: 1, PING, PADDING, CRYPTO, PING, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, PING, PADDING, CRYPT
```

```
> Frame 77: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C712A28
v Ethernet II, Src: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19), Dst: HewlettP_96:62:28 (9c:b6:54:96:62:28)
  > Destination: HewlettP_96:62:28 (9c:b6:54:96:62:28)
  > Source: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.2.2.138, Dst: 10.2.1.40
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xdd36 (56630)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x05e4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.2.2.138
    Destination Address: 10.2.1.40
v Transmission Control Protocol, Src Port: 60942, Dst Port: 22, Seq: 1, Ack: 1189, Len: 0
    Source Port: 60942
    Destination Port: 22
    [Stream index: 0]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2278110585
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1189    (relative ack number)
    Acknowledgment number (raw): 2820046352
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 252
```

```
0000  9c b6 54 96 62 28 d8 c0  a6 b6 0a 19 08 00 45 00   ··T·b(·· ······E·
0010  00 28 dd 36 40 00 80 06  05 e4 0a 02 02 8a 0a 02   ·(·6@··· ········
0020  01 28 ee 0e 00 16 87 c9  35 79 a8 16 7e 10 50 10   ·(······ 5y··~·P·
0030  00 fc c5 94 00 00                                  ······
```

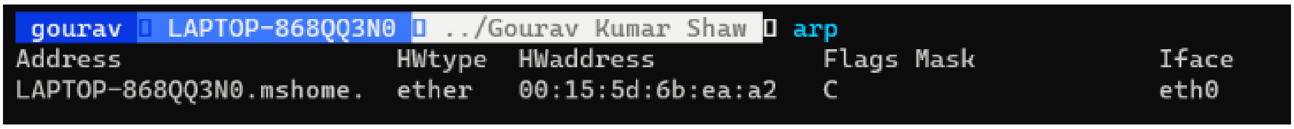
wireshark_Wi-FiMN1PY1.pcapng | Packets: 135 · Displayed: 135 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

iv)**arp**

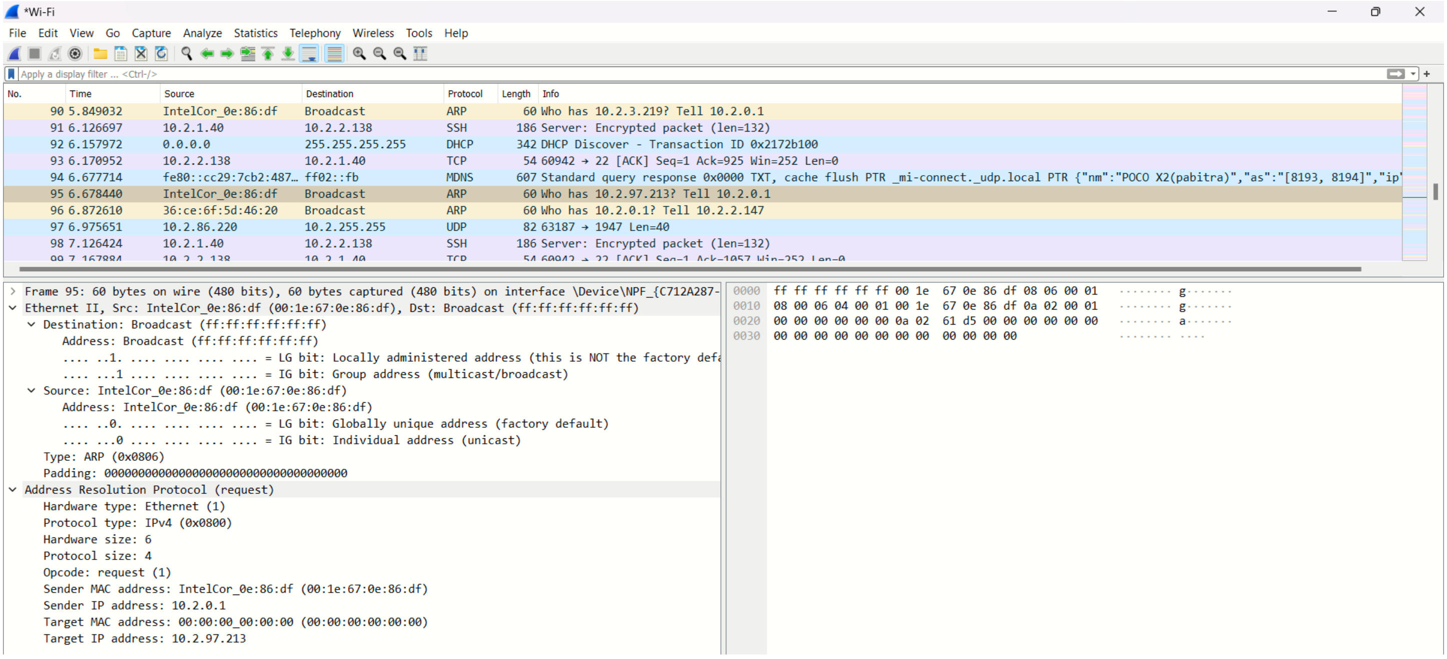
→**Application layer:-** LLMNR,MDNS,DNS

→**Transport layer:-** TCP

→**Network layer :-** ICMP



```
 gourav   LAPTOP-868QQ3N0   ../Gourav Kumar Shaw   arp
Address                  HWtype  HWaddress           Flags Mask            Iface
LAPTOP-868QQ3N0.mshome.  ether   00:15:5d:6b:ea:a2   C                     eth0
```


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

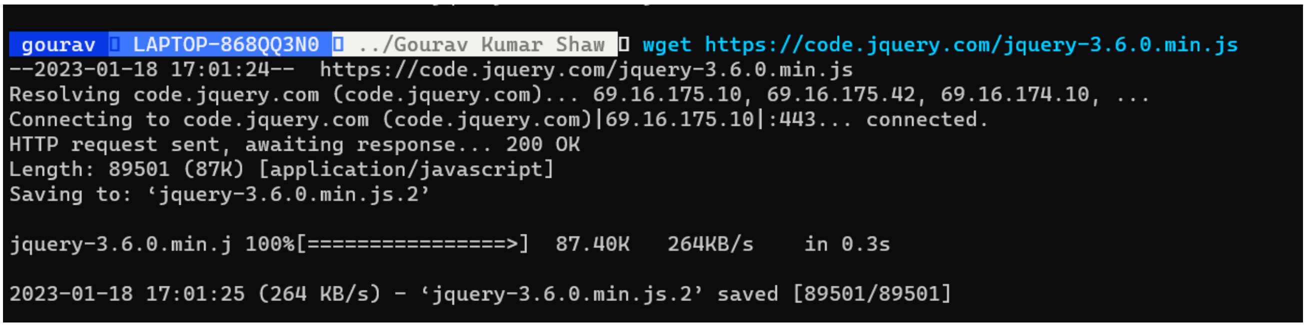
```
No.   Time       Source               Destination      Protocol Length Info
   90 5.849032   IntelCor_0e:86:df    Broadcast        ARP        60 Who has 10.2.3.219? Tell 10.2.0.1
   91 6.126697   10.2.1.40            10.2.2.138       SSH       186 Server: Encrypted packet (len=132)
   92 6.157972   0.0.0.0              255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x2172b100
   93 6.170952   10.2.2.138           10.2.1.40        TCP        54 60942 → 22 [ACK] Seq=1 Ack=925 Win=252 Len=0
   94 6.677714   fe80::cc29:7cb2:487… ff02::fb         MDNS      607 Standard query response 0x0000 TXT, cache flush PTR _mi-connect._udp.local PTR {"nm":"POCO X2(pabitra)","as":"[8193, 8194]","ip'
   95 6.678440   IntelCor_0e:86:df    Broadcast        ARP        60 Who has 10.2.97.213? Tell 10.2.0.1
   96 6.872610   36:ce:6f:5d:46:20    Broadcast        ARP        60 Who has 10.2.0.1? Tell 10.2.2.147
   97 6.975651   10.2.86.220          10.2.255.255     UDP        82 63187 → 1947 Len=40
   98 7.126424   10.2.1.40            10.2.2.138       SSH       186 Server: Encrypted packet (len=132)
```

```
> Frame 95: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{C712A287-
v Ethernet II, Src: IntelCor_0e:86:df (00:1e:67:0e:86:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory defa
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: IntelCor_0e:86:df (00:1e:67:0e:86:df)
      Address: IntelCor_0e:86:df (00:1e:67:0e:86:df)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_0e:86:df (00:1e:67:0e:86:df)
    Sender IP address: 10.2.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.2.97.213
```

```
0000  ff ff ff ff ff ff 00 1e  67 0e 86 df 08 06 00 01   ········ g·······
0010  08 00 06 04 00 01 00 1e  67 0e 86 df 0a 02 00 01   ········ g·······
0020  00 00 00 00 00 00 0a 02  61 d5 00 00 00 00 00 00   ········ a·······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

v)wget

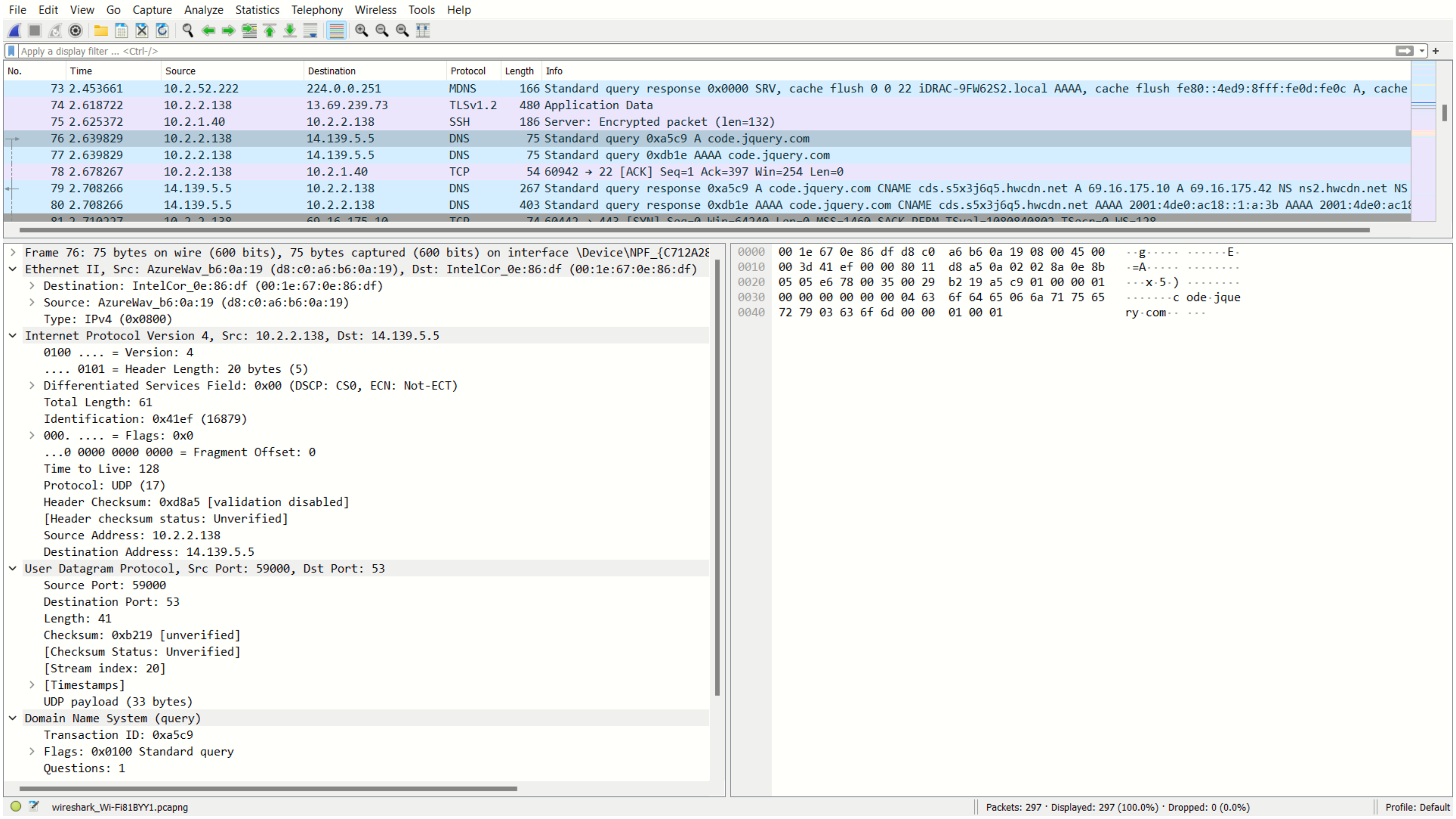
→**Application layer:-** DNS,TLS
→**Transport layer:-** TCP
→**Network layer:-** ICMP



```
gourav  LAPTOP-868QQ3N0  ../Gourav Kumar Shaw  wget https://code.jquery.com/jquery-3.6.0.min.js
--2023-01-18 17:01:24--  https://code.jquery.com/jquery-3.6.0.min.js
Resolving code.jquery.com (code.jquery.com)... 69.16.175.10, 69.16.175.42, 69.16.174.10, ...
Connecting to code.jquery.com (code.jquery.com)|69.16.175.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 89501 (87K) [application/javascript]
Saving to: ‘jquery-3.6.0.min.js.2’

jquery-3.6.0.min.j 100%[================>]  87.40K   264KB/s    in 0.3s

2023-01-18 17:01:25 (264 KB/s) - ‘jquery-3.6.0.min.js.2’ saved [89501/89501]
```



```
No.   Time       Source         Destination    Protocol Length Info
   73 2.453661   10.2.52.222    224.0.0.251    MDNS     166 Standard query response 0x0000 SRV, cache flush 0 0 22 iDRAC-9FW62S2.local AAAA, cache flush fe80::4ed9:8fff:fe0d:fe0c A, cache
   74 2.618722   10.2.2.138     13.69.239.73   TLSv1.2  480 Application Data
   75 2.625372   10.2.1.40      10.2.2.138     SSH      186 Server: Encrypted packet (len=132)
   76 2.639829   10.2.2.138     14.139.5.5     DNS       75 Standard query 0xa5c9 A code.jquery.com
   77 2.639829   10.2.2.138     14.139.5.5     DNS       75 Standard query 0xdb1e AAAA code.jquery.com
   78 2.678267   10.2.2.138     10.2.1.40      TCP       54 60942 → 22 [ACK] Seq=1 Ack=397 Win=254 Len=0
   79 2.708266   14.139.5.5     10.2.2.138     DNS      267 Standard query response 0xa5c9 A code.jquery.com CNAME cds.s5x3j6q5.hwcdn.net A 69.16.175.10 A 69.16.175.42 NS ns2.hwcdn.net NS
   80 2.708266   14.139.5.5     10.2.2.138     DNS      403 Standard query response 0xdb1e AAAA code.jquery.com CNAME cds.s5x3j6q5.hwcdn.net AAAA 2001:4de0:ac18::1:a:3b AAAA 2001:4de0:ac18
   81 2.710227   10.2.2.138     69.16.175.10   TCP       74 60442 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1080840802 TSecr=0 WS=128
```

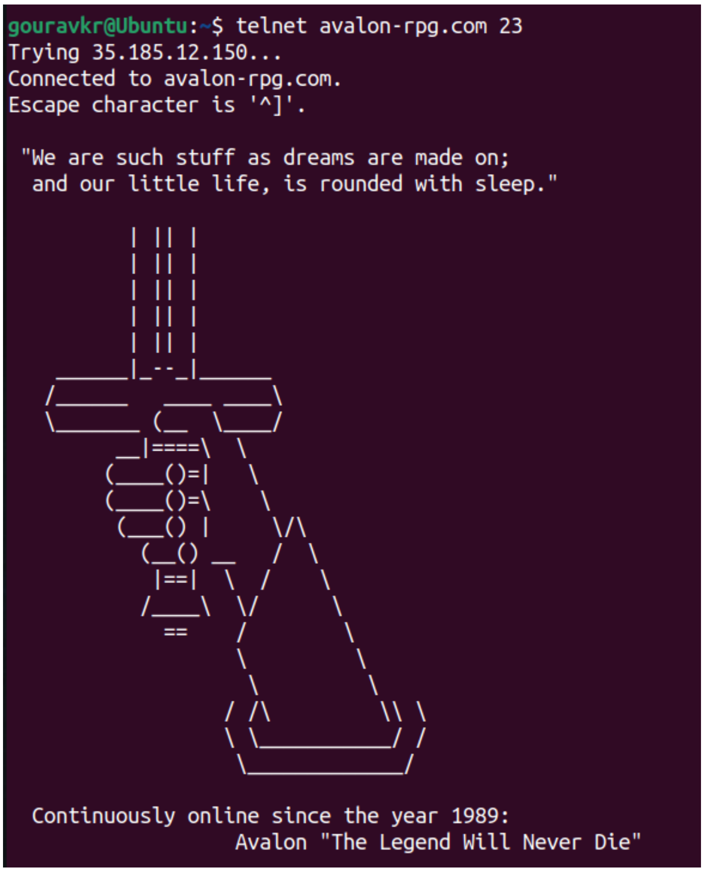
```
> Frame 76: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{C712A28
v Ethernet II, Src: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19), Dst: IntelCor_0e:86:df (00:1e:67:0e:86:df)
  > Destination: IntelCor_0e:86:df (00:1e:67:0e:86:df)
  > Source: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.2.2.138, Dst: 14.139.5.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 61
    Identification: 0x41ef (16879)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xd8a5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.2.2.138
    Destination Address: 14.139.5.5
v User Datagram Protocol, Src Port: 59000, Dst Port: 53
    Source Port: 59000
    Destination Port: 53
    Length: 41
    Checksum: 0xb219 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 20]
  > [Timestamps]
    UDP payload (33 bytes)
v Domain Name System (query)
    Transaction ID: 0xa5c9
  > Flags: 0x0100 Standard query
    Questions: 1
```

```
0000  00 1e 67 0e 86 df d8 c0  a6 b6 0a 19 08 00 45 00   ··g····· ······E·
0010  00 3d 41 ef 00 00 80 11  d8 a5 0a 02 02 8a 0e 8b   ·=A····· ········
0020  05 05 e6 78 00 35 00 29  b2 19 a5 c9 01 00 00 01   ···x·5·) ········
0030  00 00 00 00 00 00 04 63  6f 64 65 06 6a 71 75 65   ·······c ode·jque
0040  72 79 03 63 6f 6d 00 00  01 00 01                  ry·com·· ···
```

wireshark_Wi-Fi81BYY1.pcapng
Packets: 297 · Displayed: 297 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Q2. 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?

Answer:

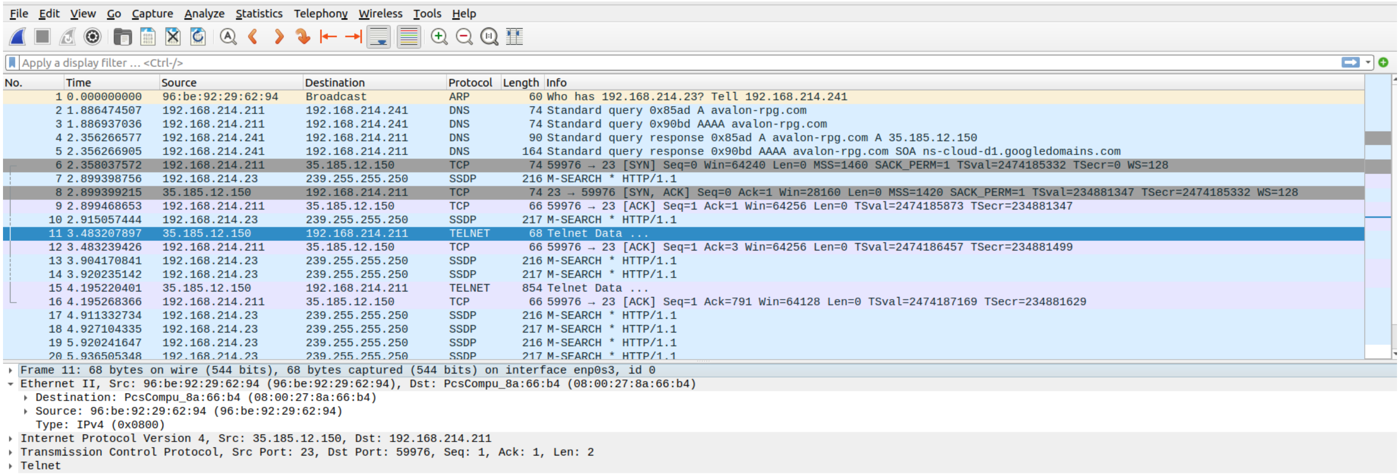


```
gouravkr@Ubuntu:~$ telnet avalon-rpg.com 23
Trying 35.185.12.150...
Connected to avalon-rpg.com.
Escape character is '^]'.

 "We are such stuff as dreams are made on;
  and our little life, is rounded with sleep."

          | || |
          | || |
          | || |
          | || |
          | || |
    ______|_--_|______
   /______   ____ ____\
   \_______ (__  \____/
         __|====\  \
        (____()=|   \
        (____()=\    \
         (___() |     \/\
           (__() __   /  \
            |==|  \  /    \
           /____\  \/      \
             ==    /        \
                   \         \
                    \         \
                  / /\         \\ \
                  \ \___________/ /
                   \_____________/

  Continuously online since the year 1989:
                   Avalon "The Legend Will Never Die"
```



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

```
No.  Time         Source             Destination        Protocol Length Info
   1 0.000000000  96:be:92:29:62:94  Broadcast          ARP        60 Who has 192.168.214.23? Tell 192.168.214.241
   2 1.886474507  192.168.214.211    192.168.214.241    DNS        74 Standard query 0x85ad A avalon-rpg.com
   3 1.886937036  192.168.214.211    192.168.214.241    DNS        74 Standard query 0x90bd AAAA avalon-rpg.com
   4 2.356266577  192.168.214.241    192.168.214.211    DNS        90 Standard query response 0x85ad A avalon-rpg.com A 35.185.12.150
   5 2.356266905  192.168.214.241    192.168.214.211    DNS       164 Standard query response 0x90bd AAAA avalon-rpg.com SOA ns-cloud-d1.googledomains.com
   6 2.358037572  192.168.214.211    35.185.12.150      TCP        74 59976 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2474185332 TSecr=0 WS=128
   7 2.899398756  192.168.214.23     239.255.255.250    SSDP      216 M-SEARCH * HTTP/1.1
   8 2.899399215  35.185.12.150      192.168.214.211    TCP        74 23 → 59976 [SYN, ACK] Seq=0 Ack=1 Win=28160 Len=0 MSS=1420 SACK_PERM=1 TSval=234881347 TSecr=2474185332 WS=128
   9 2.899468653  192.168.214.211    35.185.12.150      TCP        66 59976 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2474185873 TSecr=234881347
  10 2.915057444  192.168.214.23     239.255.255.250    SSDP      217 M-SEARCH * HTTP/1.1
  11 3.483207897  35.185.12.150      192.168.214.211    TELNET     68 Telnet Data ...
  12 3.483239426  192.168.214.211    35.185.12.150      TCP        66 59976 → 23 [ACK] Seq=1 Ack=3 Win=64256 Len=0 TSval=2474186457 TSecr=234881499
  13 3.904170841  192.168.214.23     239.255.255.250    SSDP      216 M-SEARCH * HTTP/1.1
  14 3.920235142  192.168.214.23     239.255.255.250    SSDP      217 M-SEARCH * HTTP/1.1
  15 4.195220401  35.185.12.150      192.168.214.211    TELNET    854 Telnet Data ...
  16 4.195268366  192.168.214.211    35.185.12.150      TCP        66 59976 → 23 [ACK] Seq=1 Ack=791 Win=64128 Len=0 TSval=2474187169 TSecr=234881629
  17 4.911332734  192.168.214.23     239.255.255.250    SSDP      216 M-SEARCH * HTTP/1.1
  18 4.927104335  192.168.214.23     239.255.255.250    SSDP      217 M-SEARCH * HTTP/1.1
  19 5.920241647  192.168.214.23     239.255.255.250    SSDP      216 M-SEARCH * HTTP/1.1
  20 5.936505348  192.168.214.23     239.255.255.250    SSDP      217 M-SEARCH * HTTP/1.1
```

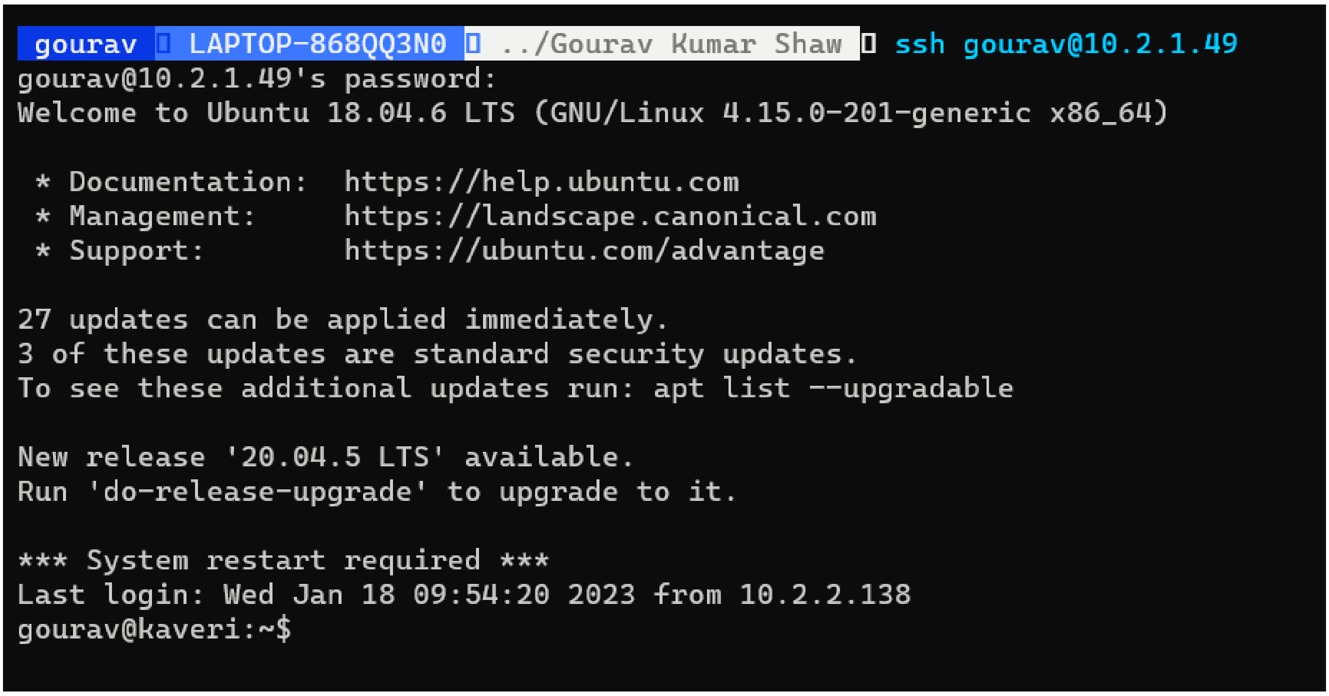
```
▸ Frame 11: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: 96:be:92:29:62:94 (96:be:92:29:62:94), Dst: PcsCompu_8a:66:b4 (08:00:27:8a:66:b4)
  ▸ Destination: PcsCompu_8a:66:b4 (08:00:27:8a:66:b4)
  ▸ Source: 96:be:92:29:62:94 (96:be:92:29:62:94)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 35.185.12.150, Dst: 192.168.214.211
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 59976, Seq: 1, Ack: 1, Len: 2
▸ Telnet
```

→**APPLICATION LAYER:-** TLS,DNS,TELNET

→Telnet is used to connect the server from remote location and it is not secure than the SSH. While using the telnet hackers may access the login credentials because the data is not encrypted but where as while using SSH the data is encrypted so it is secure.

Q3. 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?

Answer:



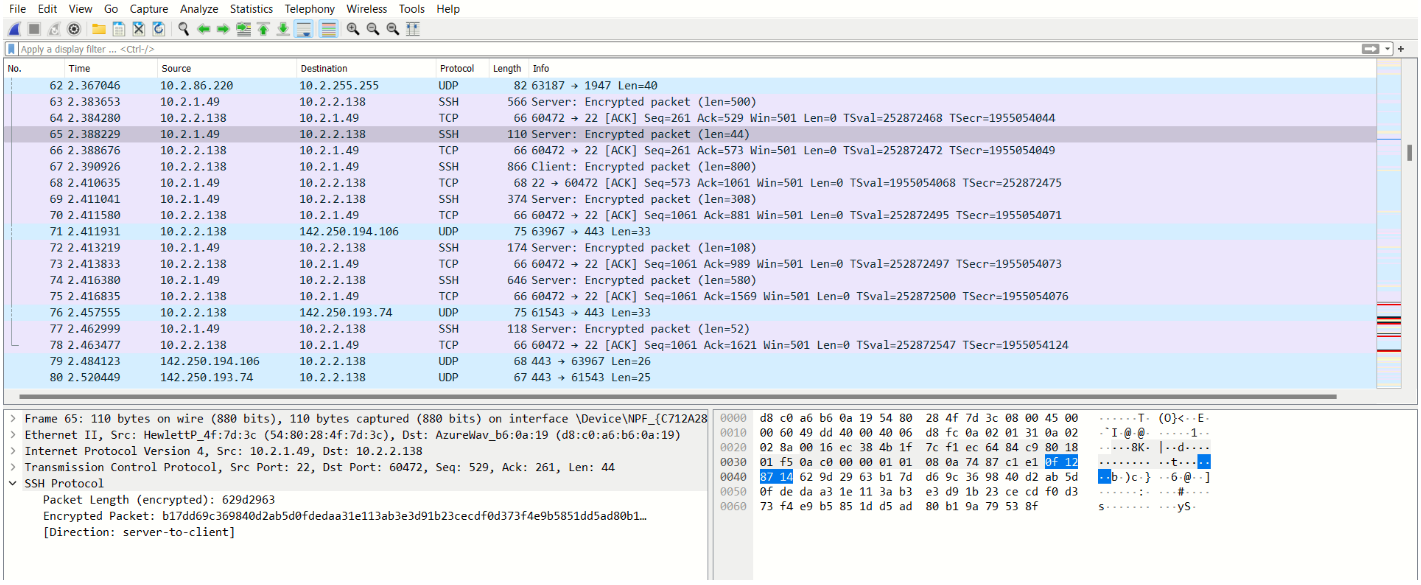
```
 gourav ▯ LAPTOP-868QQ3N0 ▯ ../Gourav Kumar Shaw ▯ ssh gourav@10.2.1.49
gourav@10.2.1.49's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-201-generic x86_64)

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

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

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Wed Jan 18 09:54:20 2023 from 10.2.2.138
gourav@kaveri:~$
```


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

```
No.   Time      Source           Destination      Protocol Length Info
   62 2.367046  10.2.86.220      10.2.255.255     UDP        82 63187 → 1947 Len=40
   63 2.383653  10.2.1.49        10.2.2.138       SSH       566 Server: Encrypted packet (len=500)
   64 2.384280  10.2.2.138       10.2.1.49        TCP        66 60472 → 22 [ACK] Seq=261 Ack=529 Win=501 Len=0 TSval=252872468 TSecr=1955054044
   65 2.388229  10.2.1.49        10.2.2.138       SSH       110 Server: Encrypted packet (len=44)
   66 2.388676  10.2.2.138       10.2.1.49        TCP        66 60472 → 22 [ACK] Seq=261 Ack=573 Win=501 Len=0 TSval=252872472 TSecr=1955054049
   67 2.390926  10.2.2.138       10.2.1.49        SSH       866 Client: Encrypted packet (len=800)
   68 2.410635  10.2.1.49        10.2.2.138       TCP        68 22 → 60472 [ACK] Seq=573 Ack=1061 Win=501 Len=0 TSval=1955054068 TSecr=252872475
   69 2.411041  10.2.1.49        10.2.2.138       SSH       374 Server: Encrypted packet (len=308)
   70 2.411580  10.2.2.138       10.2.1.49        TCP        66 60472 → 22 [ACK] Seq=1061 Ack=881 Win=501 Len=0 TSval=252872495 TSecr=1955054071
   71 2.411931  10.2.2.138       142.250.194.106  UDP        75 63967 → 443 Len=33
   72 2.413219  10.2.1.49        10.2.2.138       SSH       174 Server: Encrypted packet (len=108)
   73 2.413833  10.2.2.138       10.2.1.49        TCP        66 60472 → 22 [ACK] Seq=1061 Ack=989 Win=501 Len=0 TSval=252872497 TSecr=1955054073
   74 2.416380  10.2.1.49        10.2.2.138       SSH       646 Server: Encrypted packet (len=580)
   75 2.416835  10.2.2.138       10.2.1.49        TCP        66 60472 → 22 [ACK] Seq=1061 Ack=1569 Win=501 Len=0 TSval=252872500 TSecr=1955054076
   76 2.457555  10.2.2.138       142.250.193.74   UDP        75 61543 → 443 Len=33
   77 2.462999  10.2.1.49        10.2.2.138       SSH       118 Server: Encrypted packet (len=52)
   78 2.463477  10.2.2.138       10.2.1.49        TCP        66 60472 → 22 [ACK] Seq=1061 Ack=1621 Win=501 Len=0 TSval=252872547 TSecr=1955054124
   79 2.484123  142.250.194.106  10.2.2.138       UDP        68 443 → 63967 Len=26
   80 2.520449  142.250.193.74   10.2.2.138       UDP        67 443 → 61543 Len=25
```

```
> Frame 65: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{C712A28
> Ethernet II, Src: HewlettP_4f:7d:3c (54:80:28:4f:7d:3c), Dst: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
> Internet Protocol Version 4, Src: 10.2.1.49, Dst: 10.2.2.138
> Transmission Control Protocol, Src Port: 22, Dst Port: 60472, Seq: 529, Ack: 261, Len: 44
v SSH Protocol
    Packet Length (encrypted): 629d2963
    Encrypted Packet: b17dd69c369840d2ab5d0fdedaa31e113ab3e3d91b23cecdf0d373f4e9b5851dd5ad80b1…
    [Direction: server-to-client]
```

```
0000  d8 c0 a6 b6 0a 19 54 80  28 4f 7d 3c 08 00 45 00   ······T· (O}<··E·
0010  00 60 49 dd 40 00 40 06  d8 fc 0a 02 01 31 0a 02   ·`I·@·@· ·····1··
0020  02 8a 00 16 ec 38 4b 1f  7c f1 ec 64 84 c9 80 18   ·····8K· |··d····
0030  01 f5 0a c0 00 00 01 01  08 0a 74 87 c1 e1 0f 12   ········ ··t·····
0040  87 14 62 9d 29 63 b1 7d  d6 9c 36 98 40 d2 ab 5d   ··b·)c·} ··6·@··]
0050  0f de da a3 1e 11 3a b3  e3 d9 1b 23 ce cd f0 d3   ······:· ···#····
0060  73 f4 e9 b5 85 1d d5 ad  80 b1 9a 79 53 8f         s······· ···yS·
```

SSH(Secure Shell) is access credential that is used in the SSH Protocol. In other words, it is a cryptographic network protocol that is used for transferring encrypted data over network. The SSH protocol (also referred to as Secure Shell) is a method for secure remote login from one computer to another. It provides several alternative options for strong authentication.

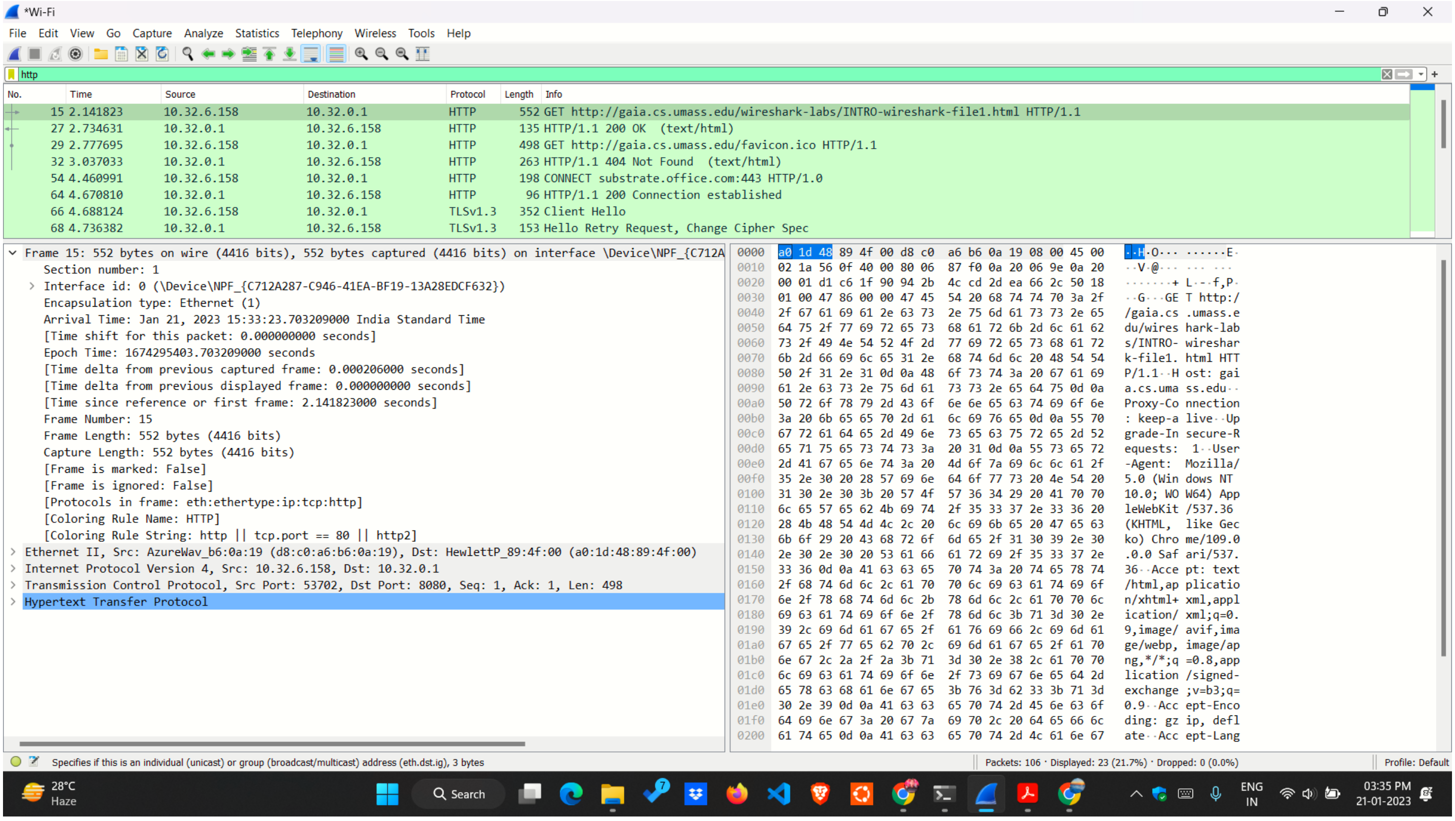
Q4. Enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and capture packets using Wireshark. After your browser has displayed the INTRO-wireshark-file1.html page (it is a simple one line of congratulations), stop Wireshark packet capture. Answer the following from the captured packets:

a. How long did it take from when the HTTP GET message was sent until the

HTTP OK reply was received?

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.

Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source         Destination    Protocol  Length  Info
   15 2.141823    10.32.6.158    10.32.0.1      HTTP       552 GET http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   27 2.734631    10.32.0.1      10.32.6.158    HTTP       135 HTTP/1.1 200 OK  (text/html)
   29 2.777695    10.32.6.158    10.32.0.1      HTTP       498 GET http://gaia.cs.umass.edu/favicon.ico HTTP/1.1
   32 3.037033    10.32.0.1      10.32.6.158    HTTP       263 HTTP/1.1 404 Not Found  (text/html)
   54 4.460991    10.32.6.158    10.32.0.1      HTTP       198 CONNECT substrate.office.com:443 HTTP/1.0
   64 4.670810    10.32.0.1      10.32.6.158    HTTP        96 HTTP/1.1 200 Connection established
   66 4.688124    10.32.6.158    10.32.0.1      TLSv1.3    352 Client Hello
   68 4.736382    10.32.0.1      10.32.6.158    TLSv1.3    153 Hello Retry Request, Change Cipher Spec
```

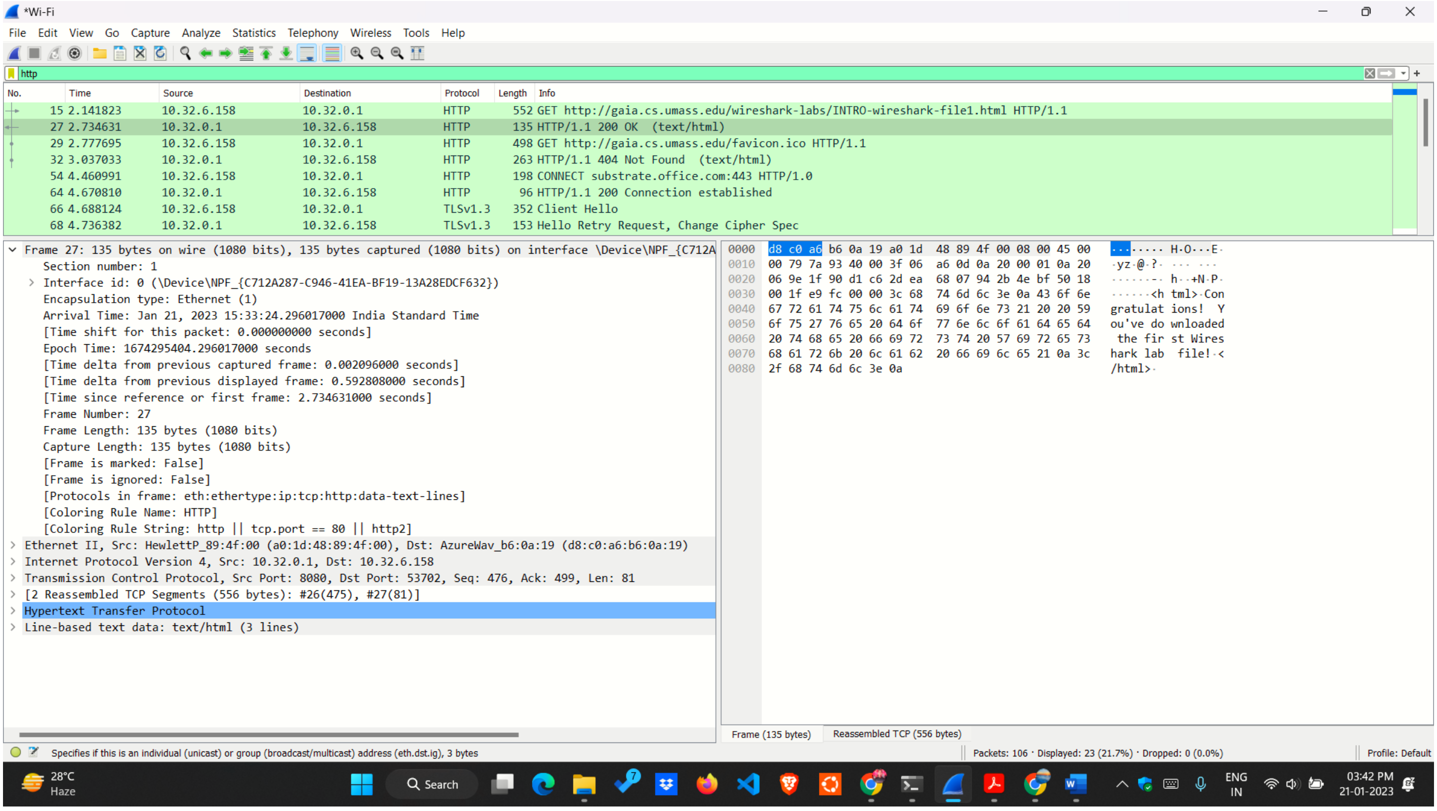
```
v Frame 15: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \Device\NPF_{C712A
    Section number: 1
  > Interface id: 0 (\Device\NPF_{C712A287-C946-41EA-BF19-13A28EDCF632})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 21, 2023 15:33:23.703209000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1674295403.703209000 seconds
    [Time delta from previous captured frame: 0.000206000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.141823000 seconds]
    Frame Number: 15
    Frame Length: 552 bytes (4416 bits)
    Capture Length: 552 bytes (4416 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19), Dst: HewlettP_89:4f:00 (a0:1d:48:89:4f:00)
> Internet Protocol Version 4, Src: 10.32.6.158, Dst: 10.32.0.1
> Transmission Control Protocol, Src Port: 53702, Dst Port: 8080, Seq: 1, Ack: 1, Len: 498
> Hypertext Transfer Protocol
```

```
0000  a0 1d 48 89 4f 00 d8 c0  a6 b6 0a 19 08 00 45 00   ··H·O··· ······E·
0010  02 1a 56 0f 40 00 80 06  87 f0 0a 20 06 9e 0a 20   ··V·@··· ··· ···
0020  00 01 d1 c6 1f 90 94 2b  4c cd 2d ea 66 2c 50 18   ·······+ L·-·f,P·
0030  01 00 47 86 00 00 47 45  54 20 68 74 74 70 3a 2f   ··G···GE T http:/
0040  2f 67 61 69 61 2e 63 73  2e 75 6d 61 73 73 2e 65   /gaia.cs .umass.e
0050  64 75 2f 77 69 72 65 73  68 61 72 6b 2d 6c 61 62   du/wires hark-lab
0060  73 2f 49 4e 54 52 4f 2d  77 69 72 65 73 68 61 72   s/INTRO- wireshar
0070  6b 2d 66 69 6c 65 31 2e  68 74 6d 6c 20 48 54 54   k-file1. html HTT
0080  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 67 61 69   P/1.1··H ost: gai
0090  61 2e 63 73 2e 75 6d 61  73 73 2e 65 64 75 0d 0a   a.cs.uma ss.edu··
00a0  50 72 6f 78 79 2d 43 6f  6e 6e 65 63 74 69 6f 6e   Proxy-Co nnection
00b0  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 55 70   : keep-a live··Up
00c0  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52   grade-In secure-R
00d0  65 71 75 65 73 74 73 3a  20 31 0d 0a 55 73 65 72   equests:  1··User
00e0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00f0  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT
0100  31 30 2e 30 3b 20 57 4f  57 36 34 29 20 41 70 70   10.0; WO W64) App
0110  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36
0120  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
0130  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 30 39 2e 30   ko) Chro me/109.0
0140  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
0150  33 36 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   36··Acce pt: text
0160  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
0170  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
0180  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
0190  39 2c 69 6d 61 67 65 2f  61 76 69 66 2c 69 6d 61   9,image/ avif,ima
01a0  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
01b0  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 2c 61 70 70   ng,*/*;q =0.8,app
01c0  6c 69 63 61 74 69 6f 6e  2f 73 69 67 6e 65 64 2d   lication /signed-
01d0  65 78 63 68 61 6e 67 65  3b 76 3d 62 33 3b 71 3d   exchange ;v=b3;q=
01e0  30 2e 39 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.9··Acc ept-Enco
01f0  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
0200  61 74 65 0d 0a 41 63 63  65 70 74 2d 4c 61 6e 67   ate··Acc ept-Lang
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes

Packets: 106 · Displayed: 23 (21.7%) · Dropped: 0 (0.0%)

Profile: Default



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.     Time        Source         Destination    Protocol  Length Info
     15 2.141823    10.32.6.158    10.32.0.1      HTTP      552 GET http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
     27 2.734631    10.32.0.1      10.32.6.158    HTTP      135 HTTP/1.1 200 OK  (text/html)
     29 2.777695    10.32.6.158    10.32.0.1      HTTP      498 GET http://gaia.cs.umass.edu/favicon.ico HTTP/1.1
     32 3.037033    10.32.0.1      10.32.6.158    HTTP      263 HTTP/1.1 404 Not Found  (text/html)
     54 4.460991    10.32.6.158    10.32.0.1      HTTP      198 CONNECT substrate.office.com:443 HTTP/1.0
     64 4.670810    10.32.0.1      10.32.6.158    HTTP       96 HTTP/1.1 200 Connection established
     66 4.688124    10.32.6.158    10.32.0.1      TLSv1.3   352 Client Hello
     68 4.736382    10.32.0.1      10.32.6.158    TLSv1.3   153 Hello Retry Request, Change Cipher Spec
```

```
Frame 27: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface \Device\NPF_{C712A
    Section number: 1
  > Interface id: 0 (\Device\NPF_{C712A287-C946-41EA-BF19-13A28EDCF632})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 21, 2023 15:33:24.296017000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1674295404.296017000 seconds
    [Time delta from previous captured frame: 0.002096000 seconds]
    [Time delta from previous displayed frame: 0.592808000 seconds]
    [Time since reference or first frame: 2.734631000 seconds]
    Frame Number: 27
    Frame Length: 135 bytes (1080 bits)
    Capture Length: 135 bytes (1080 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: HewlettP_89:4f:00 (a0:1d:48:89:4f:00), Dst: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
> Internet Protocol Version 4, Src: 10.32.0.1, Dst: 10.32.6.158
> Transmission Control Protocol, Src Port: 8080, Dst Port: 53702, Seq: 476, Ack: 499, Len: 81
> [2 Reassembled TCP Segments (556 bytes): #26(475), #27(81)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (3 lines)
```

```
0000  d8 c0 a6 b6 0a 19 a0 1d  48 89 4f 00 08 00 45 00   ········ H·O···E·
0010  00 79 7a 93 40 00 3f 06  a6 0d 0a 20 00 01 0a 20   ·yz·@·?· ··· ···
0020  06 9e 1f 90 d1 c6 2d ea  68 07 94 2b 4e bf 50 18   ······-· h··+N·P·
0030  00 1f e9 fc 00 00 3c 68  74 6d 6c 3e 0a 43 6f 6e   ······<h tml>·Con
0040  67 72 61 74 75 6c 61 74  69 6f 6e 73 21 20 20 59   gratulat ions!  Y
0050  6f 75 27 76 65 20 64 6f  77 6e 6c 6f 61 64 65 64   ou've do wnloaded
0060  20 74 68 65 20 66 69 72  73 74 20 57 69 72 65 73    the fir st Wires
0070  68 61 72 6b 20 6c 61 62  20 66 69 6c 65 21 0a 3c   hark lab  file!·<
0080  2f 68 74 6d 6c 3e 0a                               /html>·
```

```
Frame (135 bytes)   Reassembled TCP (556 bytes)
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes   Packets: 106 · Displayed: 23 (21.7%) · Dropped: 0 (0.0%)   Profile: Default
```

a. Time it take from when the HTTP GET message was sent until the HTTP OK reply was received is : 0.592808000 seconds

b. The Internet Address of the gaia.cs.umass.edu is :10.32.0.1

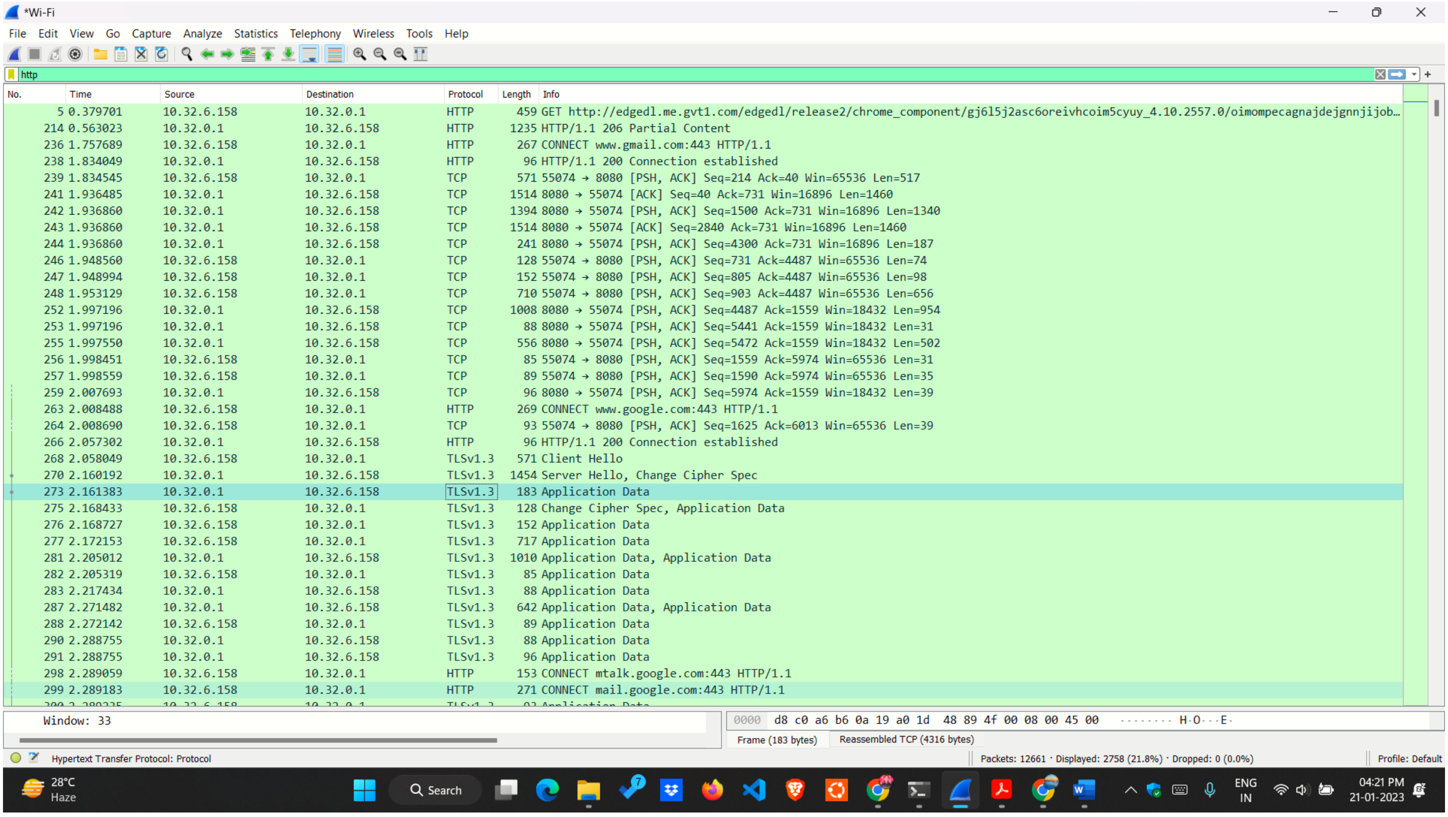
The Internet address of my computer is : 10.32.6.158

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:

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?

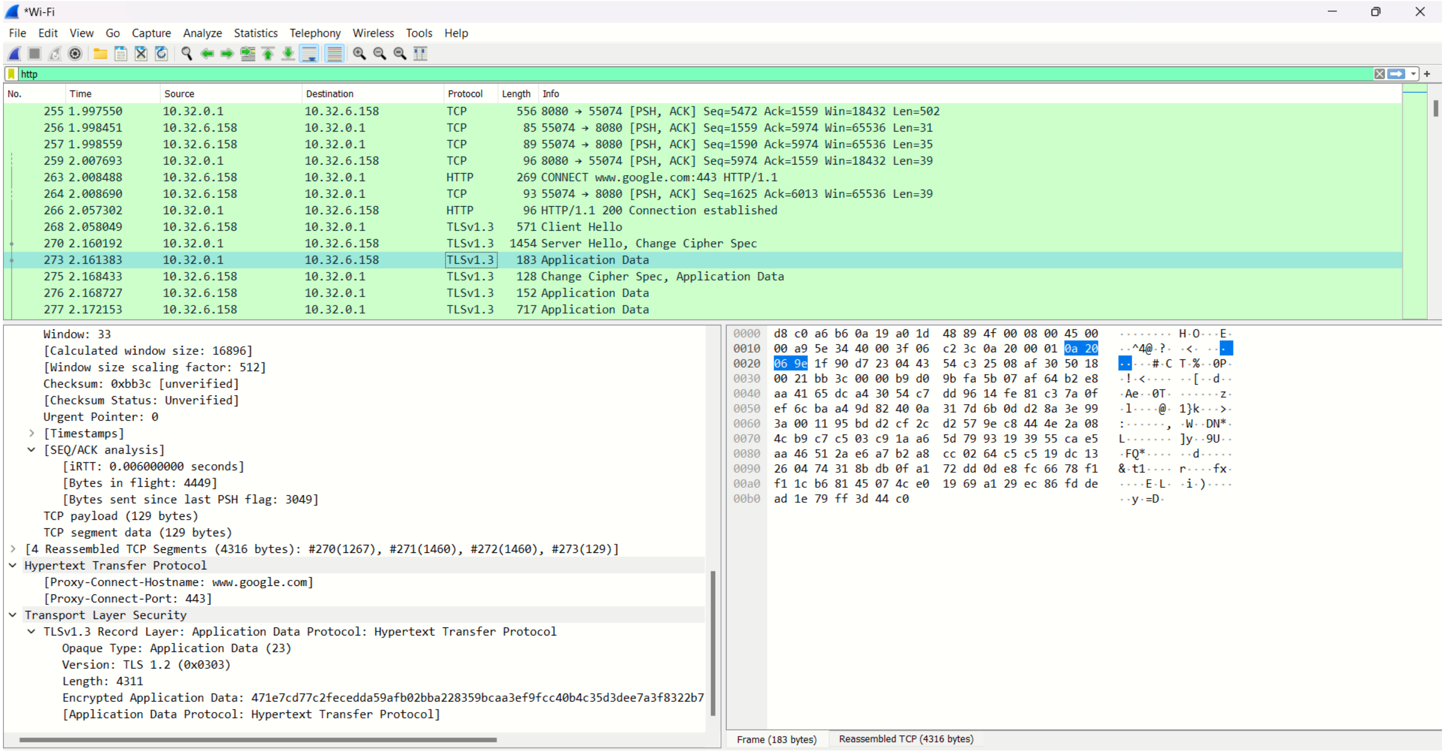
Answer:



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.   Time       Source         Destination    Protocol  Length Info
    5 0.379701   10.32.6.158    10.32.0.1      HTTP       459 GET http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/gj6l5j2asc6oreivhcoim5cyuy_4.10.2557.0/oimompecagnajdejgnnjijob…
  214 0.563023   10.32.0.1      10.32.6.158    HTTP      1235 HTTP/1.1 206 Partial Content
  236 1.757689   10.32.6.158    10.32.0.1      HTTP       267 CONNECT www.gmail.com:443 HTTP/1.1
  238 1.834049   10.32.0.1      10.32.6.158    HTTP        96 HTTP/1.1 200 Connection established
  239 1.834545   10.32.6.158    10.32.0.1      TCP        571 55074 → 8080 [PSH, ACK] Seq=214 Ack=40 Win=65536 Len=517
  241 1.936485   10.32.0.1      10.32.6.158    TCP       1514 8080 → 55074 [ACK] Seq=40 Ack=731 Win=16896 Len=1460
  242 1.936860   10.32.0.1      10.32.6.158    TCP       1394 8080 → 55074 [PSH, ACK] Seq=1500 Ack=731 Win=16896 Len=1340
  243 1.936860   10.32.0.1      10.32.6.158    TCP       1514 8080 → 55074 [ACK] Seq=2840 Ack=731 Win=16896 Len=1460
  244 1.936860   10.32.0.1      10.32.6.158    TCP        241 8080 → 55074 [PSH, ACK] Seq=4300 Ack=731 Win=16896 Len=187
  246 1.948560   10.32.6.158    10.32.0.1      TCP        128 55074 → 8080 [PSH, ACK] Seq=731 Ack=4487 Win=65536 Len=74
  247 1.948994   10.32.6.158    10.32.0.1      TCP        152 55074 → 8080 [PSH, ACK] Seq=805 Ack=4487 Win=65536 Len=98
  248 1.953129   10.32.6.158    10.32.0.1      TCP        710 55074 → 8080 [PSH, ACK] Seq=903 Ack=4487 Win=65536 Len=656
  252 1.997196   10.32.0.1      10.32.6.158    TCP       1008 8080 → 55074 [PSH, ACK] Seq=4487 Ack=1559 Win=18432 Len=954
  253 1.997196   10.32.0.1      10.32.6.158    TCP         88 8080 → 55074 [PSH, ACK] Seq=5441 Ack=1559 Win=18432 Len=31
  255 1.997550   10.32.0.1      10.32.6.158    TCP        556 8080 → 55074 [PSH, ACK] Seq=5472 Ack=1559 Win=18432 Len=502
  256 1.998451   10.32.6.158    10.32.0.1      TCP         85 55074 → 8080 [PSH, ACK] Seq=1559 Ack=5974 Win=65536 Len=31
  257 1.998559   10.32.6.158    10.32.0.1      TCP         89 55074 → 8080 [PSH, ACK] Seq=1590 Ack=5974 Win=65536 Len=35
  259 2.007693   10.32.0.1      10.32.6.158    TCP         96 8080 → 55074 [PSH, ACK] Seq=5974 Ack=1559 Win=18432 Len=39
  263 2.008488   10.32.6.158    10.32.0.1      HTTP       269 CONNECT www.google.com:443 HTTP/1.1
  264 2.008690   10.32.6.158    10.32.0.1      TCP         93 55074 → 8080 [PSH, ACK] Seq=1625 Ack=6013 Win=65536 Len=39
  266 2.057302   10.32.0.1      10.32.6.158    HTTP        96 HTTP/1.1 200 Connection established
  268 2.058049   10.32.6.158    10.32.0.1      TLSv1.3    571 Client Hello
  270 2.160192   10.32.0.1      10.32.6.158    TLSv1.3   1454 Server Hello, Change Cipher Spec
  273 2.161383   10.32.0.1      10.32.6.158    TLSv1.3    183 Application Data
  275 2.168433   10.32.6.158    10.32.0.1      TLSv1.3    128 Change Cipher Spec, Application Data
  276 2.168727   10.32.6.158    10.32.0.1      TLSv1.3    152 Application Data
  277 2.172153   10.32.6.158    10.32.0.1      TLSv1.3    717 Application Data
  281 2.205012   10.32.0.1      10.32.6.158    TLSv1.3   1010 Application Data, Application Data
  282 2.205319   10.32.6.158    10.32.0.1      TLSv1.3     85 Application Data
  283 2.217434   10.32.0.1      10.32.6.158    TLSv1.3     88 Application Data
  287 2.271482   10.32.0.1      10.32.6.158    TLSv1.3    642 Application Data, Application Data
  288 2.272142   10.32.6.158    10.32.0.1      TLSv1.3     89 Application Data
  290 2.288755   10.32.0.1      10.32.6.158    TLSv1.3     88 Application Data
  291 2.288755   10.32.0.1      10.32.6.158    TLSv1.3     96 Application Data
  298 2.289059   10.32.6.158    10.32.0.1      HTTP       153 CONNECT mtalk.google.com:443 HTTP/1.1
  299 2.289183   10.32.6.158    10.32.0.1      HTTP       271 CONNECT mail.google.com:443 HTTP/1.1
  300 2.289235   10.32.6.158    10.32.0.1      TLSv1.3     93 Application Data

    Window: 33
0000  d8 c0 a6 b6 0a 19 a0 1d  48 89 4f 00 08 00 45 00   ········ H·O···E·
Frame (183 bytes)   Reassembled TCP (4316 bytes)
Hypertext Transfer Protocol: Protocol    Packets: 12661 · Displayed: 2758 (21.8%) · Dropped: 0 (0.0%)    Profile: Default
```

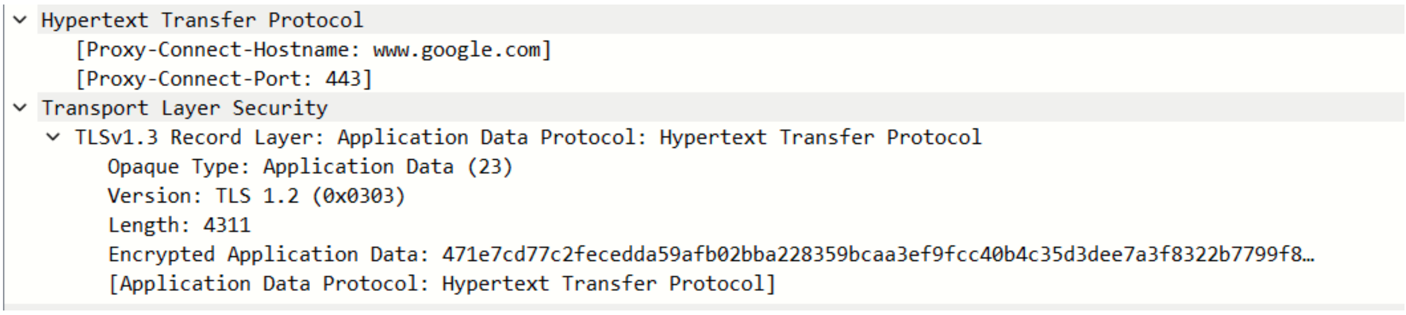

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time        Source        Destination   Protocol  Length Info
   255 1.997550    10.32.0.1     10.32.6.158   TCP        556 8080 → 55074 [PSH, ACK] Seq=5472 Ack=1559 Win=18432 Len=502
   256 1.998451    10.32.6.158   10.32.0.1     TCP         85 55074 → 8080 [PSH, ACK] Seq=1559 Ack=5974 Win=65536 Len=31
   257 1.998559    10.32.6.158   10.32.0.1     TCP         89 55074 → 8080 [PSH, ACK] Seq=1590 Ack=5974 Win=65536 Len=35
   259 2.007693    10.32.0.1     10.32.6.158   TCP         96 8080 → 55074 [PSH, ACK] Seq=5974 Ack=1559 Win=18432 Len=39
   263 2.008488    10.32.6.158   10.32.0.1     HTTP       269 CONNECT www.google.com:443 HTTP/1.1
   264 2.008690    10.32.6.158   10.32.0.1     TCP         93 55074 → 8080 [PSH, ACK] Seq=1625 Ack=6013 Win=65536 Len=39
   266 2.057302    10.32.0.1     10.32.6.158   HTTP        96 HTTP/1.1 200 Connection established
   268 2.058049    10.32.6.158   10.32.0.1     TLSv1.3    571 Client Hello
   270 2.160192    10.32.0.1     10.32.6.158   TLSv1.3   1454 Server Hello, Change Cipher Spec
   273 2.161383    10.32.0.1     10.32.6.158   TLSv1.3    183 Application Data
   275 2.168433    10.32.6.158   10.32.0.1     TLSv1.3    128 Change Cipher Spec, Application Data
   276 2.168727    10.32.6.158   10.32.0.1     TLSv1.3    152 Application Data
   277 2.172153    10.32.6.158   10.32.0.1     TLSv1.3    717 Application Data
```

```
    Window: 33
    [Calculated window size: 16896]
    [Window size scaling factor: 512]
    Checksum: 0xbb3c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  ∨ [SEQ/ACK analysis]
      [iRTT: 0.006000000 seconds]
      [Bytes in flight: 4449]
      [Bytes sent since last PSH flag: 3049]
    TCP payload (129 bytes)
    TCP segment data (129 bytes)
> [4 Reassembled TCP Segments (4316 bytes): #270(1267), #271(1460), #272(1460), #273(129)]
∨ Hypertext Transfer Protocol
    [Proxy-Connect-Hostname: www.google.com]
    [Proxy-Connect-Port: 443]
∨ Transport Layer Security
  ∨ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 4311
      Encrypted Application Data: 471e7cd77c2fecedda59afb02bba228359bcaa3ef9fcc40b4c35d3dee7a3f8322b7
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0000  d8 c0 a6 b6 0a 19 a0 1d  48 89 4f 00 08 00 45 00   ········ H·O···E·
0010  00 a9 5e 34 40 00 3f 06  c2 3c 0a 20 00 01 0a 20   ··^4@·?· ·<· ····
0020  06 9e 1f 90 d7 23 04 43  54 c3 25 08 af 30 50 18   ·····#·C T·%··0P·
0030  00 21 bb 3c 00 00 b9 d0  9b fa 5b 07 af 64 b2 e8   ·!·<···· ··[··d··
0040  aa 41 65 dc a4 30 54 c7  dd 96 14 fe 81 c3 7a 0f   ·Ae··0T· ······z·
0050  ef 6c ba a4 9d 82 40 0a  31 7d 6b 0d d2 8a 3e 99   ·l····@· 1}k···>·
0060  3a 00 11 95 bd d2 cf 2c  d2 57 9e c8 44 4e 2a 08   :······, ·W··DN*·
0070  4c b9 c7 c5 03 c9 1a a6  5d 79 93 19 39 55 ca e5   L······· ]y··9U··
0080  aa 46 51 2a e6 a7 b2 a8  cc 02 64 c5 c5 19 dc 13   ·FQ*···· ··d·····
0090  26 04 74 31 8b db 0f a1  72 dd 0d e8 fc 66 78 f1   &·t1···· r····fx·
00a0  f1 1c b6 81 45 07 4c e0  19 69 a1 29 ec 86 fd de   ····E·L· ·i·)····
00b0  ad 1e 79 ff 3d 44 c0                               ··y·=D·
```

Frame (183 bytes)   Reassembled TCP (4316 bytes)



```
∨ Hypertext Transfer Protocol
      [Proxy-Connect-Hostname: www.google.com]
      [Proxy-Connect-Port: 443]
∨ Transport Layer Security
  ∨ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
        Opaque Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 4311
        Encrypted Application Data: 471e7cd77c2fecedda59afb02bba228359bcaa3ef9fcc40b4c35d3dee7a3f8322b7799f8…
        [Application Data Protocol: Hypertext Transfer Protocol]
```

a. **Transport Layer Security** (**TLS**) is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains the most publicly visible.

b. The only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses, and to digitally sign those requests and responses.