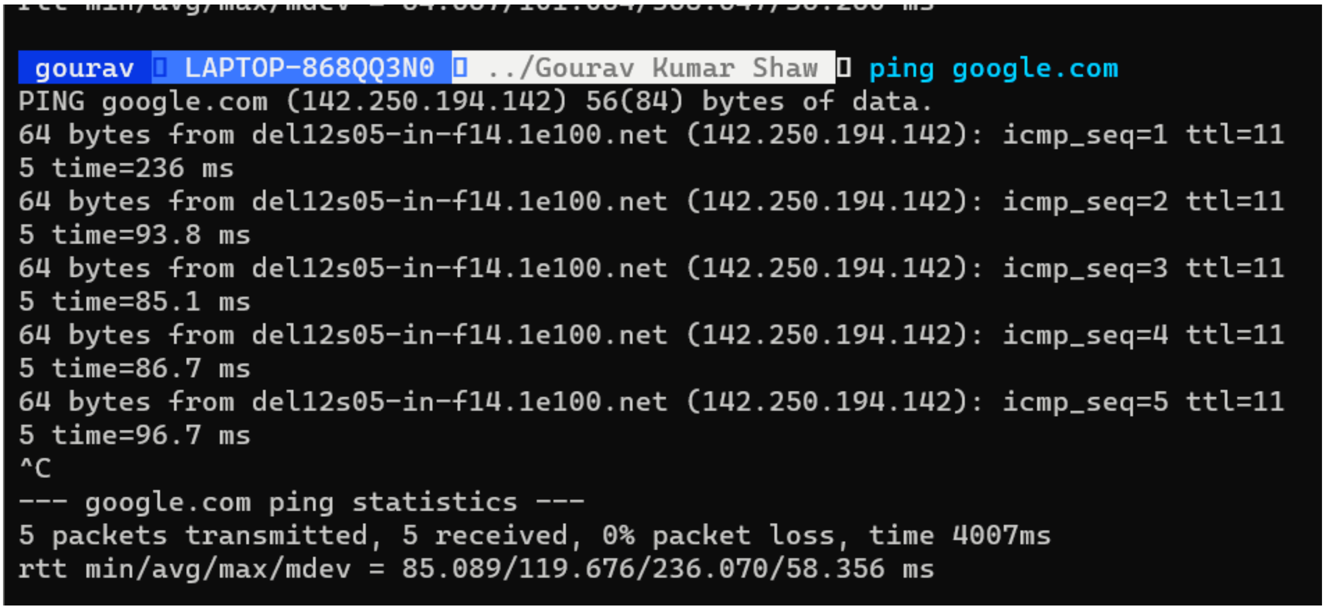
Name : Gourav Kumar Shaw
Enrollment Id. : 2020CSB010
Section: Gx
Subject : Computer Network lab

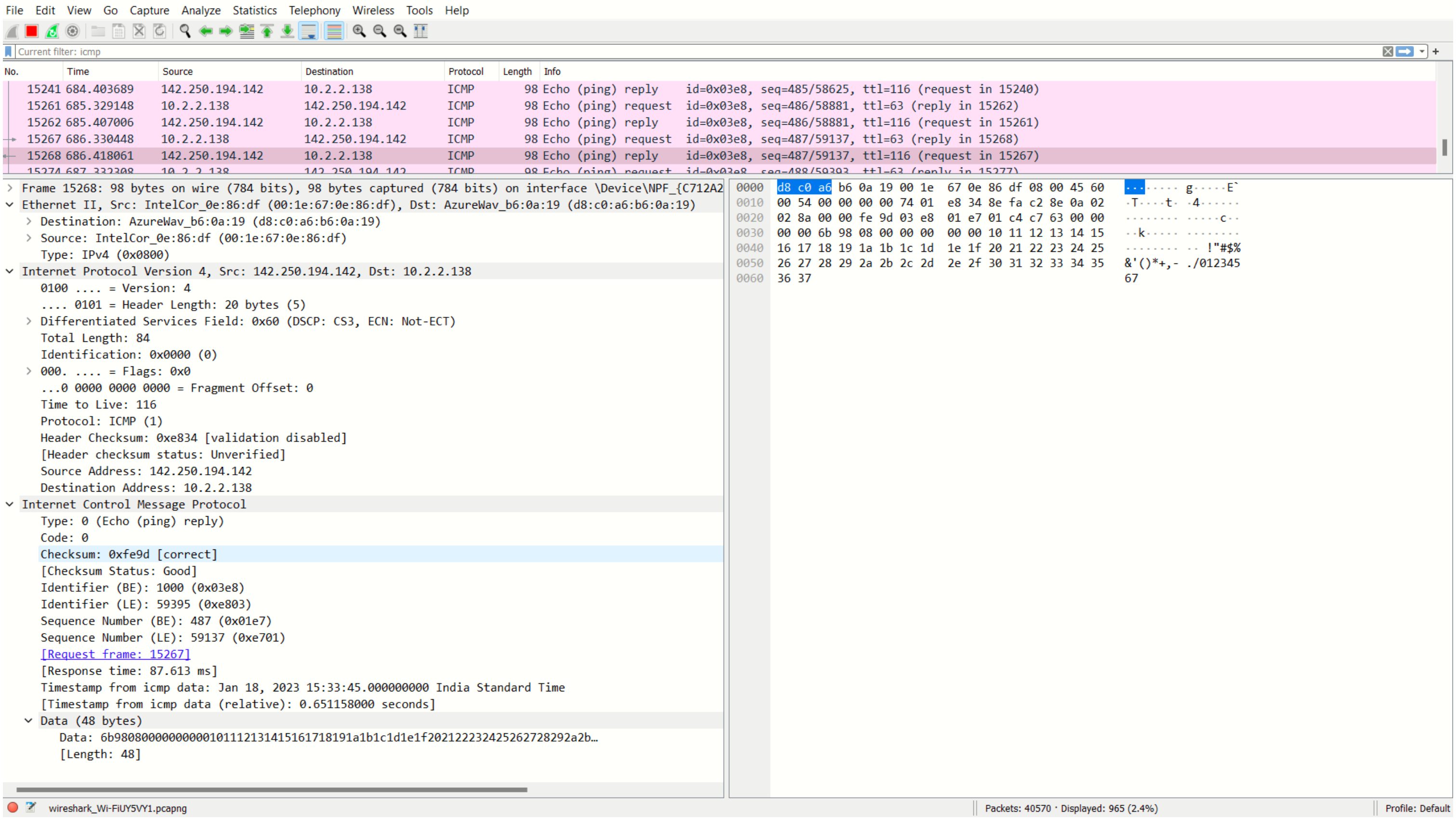
1. Analyse the packets (across all layers) exchanged with your computer while executing the

following commands: (i) ping, (ii) traceroute, (iii) dig, (iv) arp,(v)wget.

1. Ping



```
 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
```

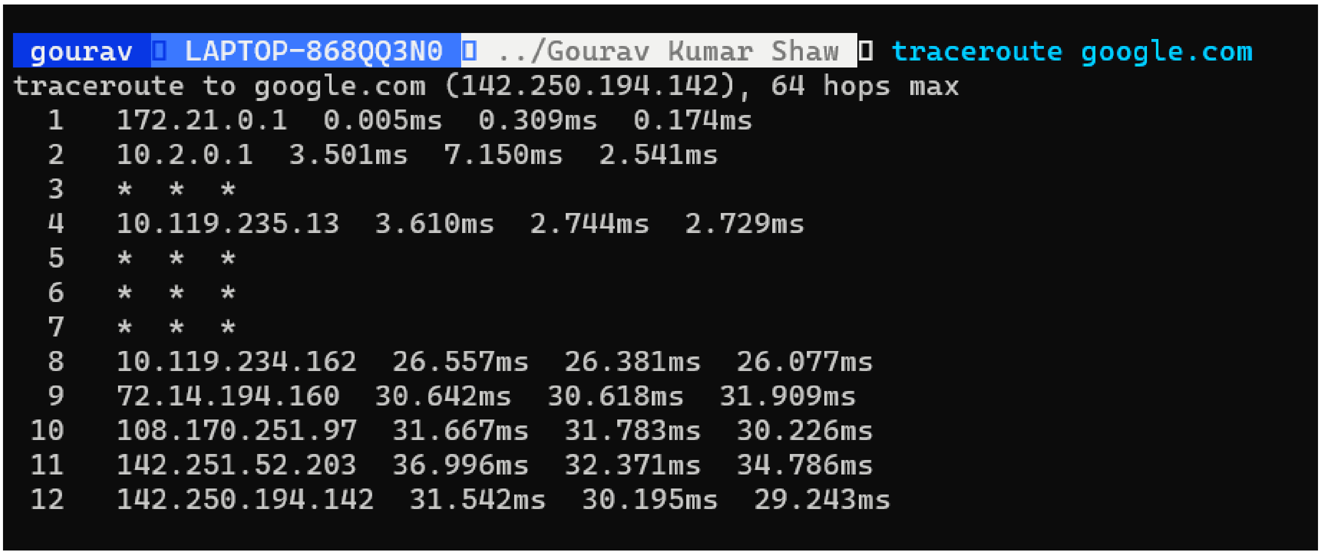

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: icmp
wireshark_Wi-FiUY5VY1.pcapng
Packets: 40570 · Displayed: 965 (2.4%)
Profile: Default

```
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)
```

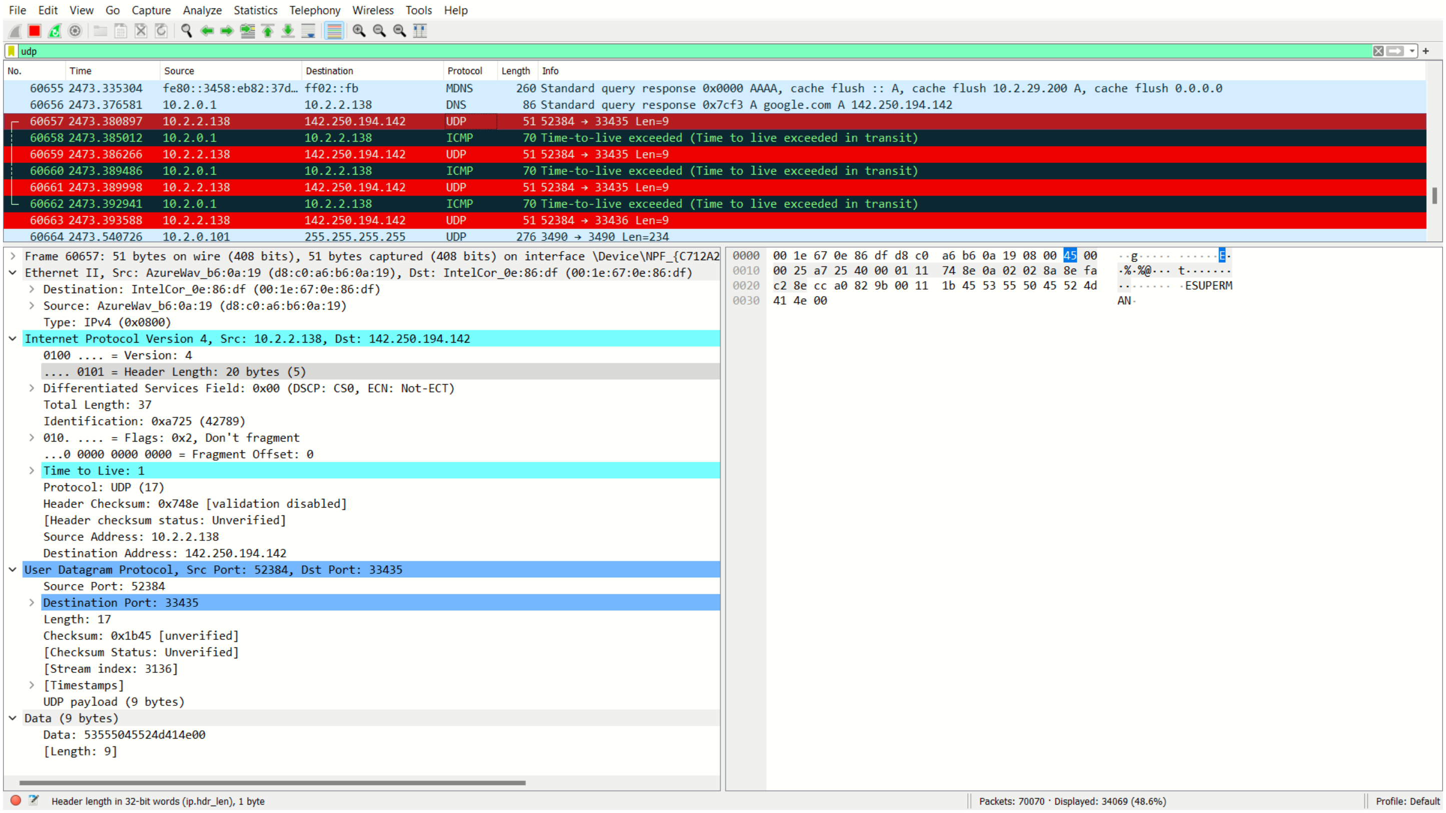
```
> Frame 15268: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{C712A2
v Ethernet II, Src: IntelCor_0e:86:df (00:1e:67:0e:86:df), Dst: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
  > Destination: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
  > Source: IntelCor_0e:86:df (00:1e:67:0e:86:df)
    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: 6b980800000000001011121314151617181 91a1b1c1d1e1f202122232425262728292a2b…
      [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
```

2.traceroute



```
 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

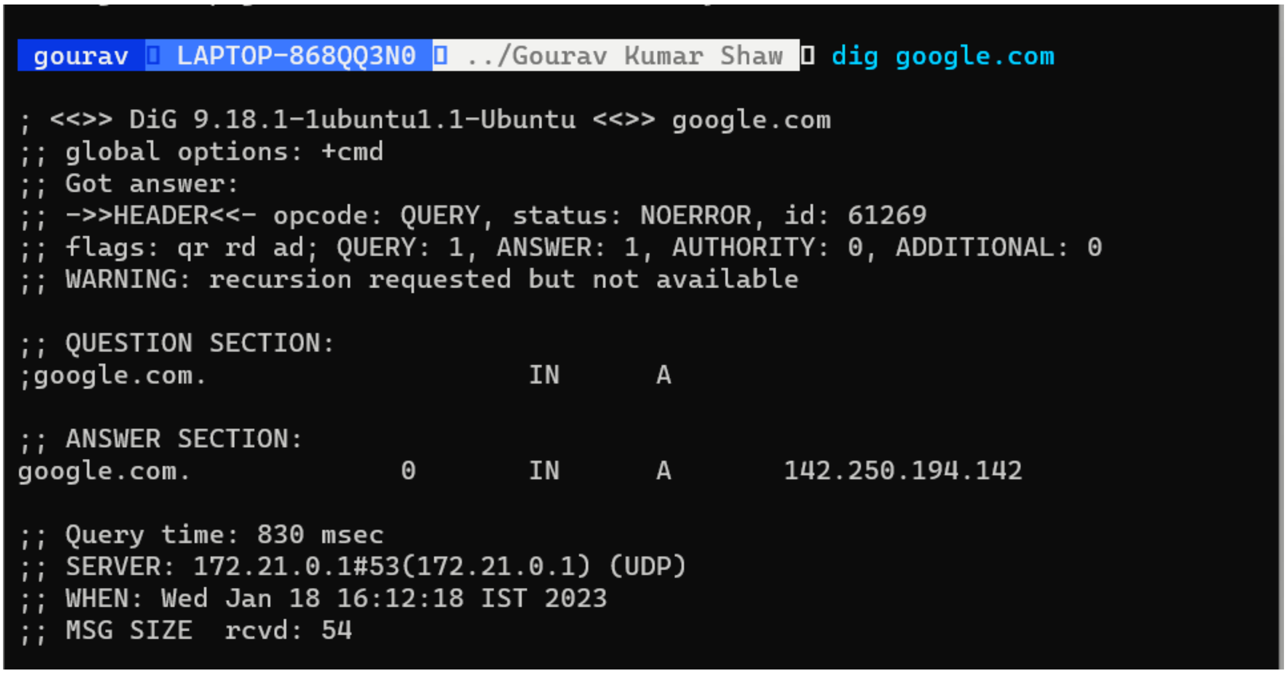
No.	Time	Source	Destination	Protocol	Length	Info
60655	2473.335304	fe80::3458:eb82:37d…	ff02::fb	MDNS	260	Standard query response 0x0000 AAAA, cache flush :: A, cache flush 10.2.29.200 A, cache flush 0.0.0.0
60656	2473.376581	10.2.0.1	10.2.2.138	DNS	86	Standard query response 0x7cf3 A google.com A 142.250.194.142
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

3.dig



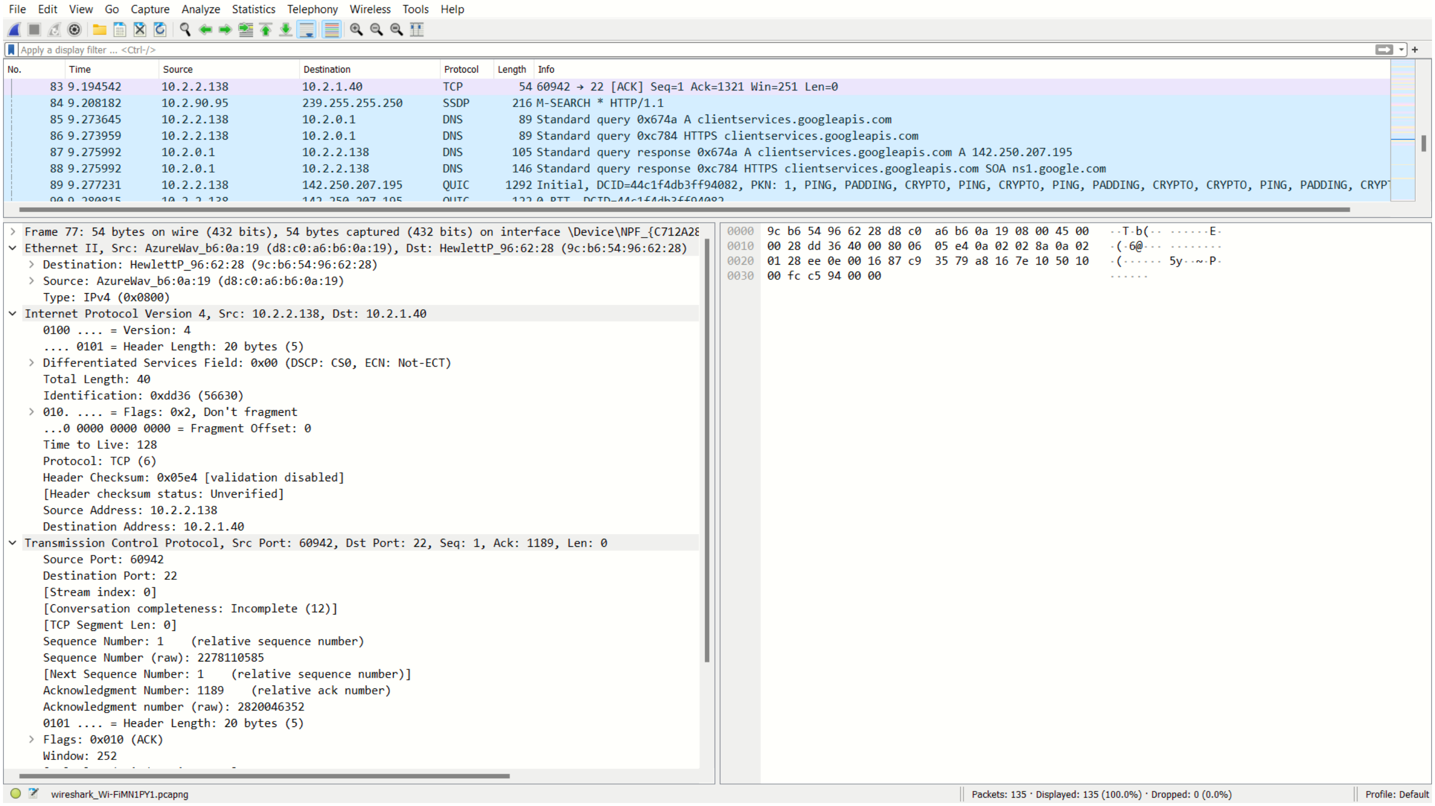
```
gourav  LAPTOP-868QQ3N0  ../Gourav Kumar Shaw  dig google.com

; <<>> 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-/>

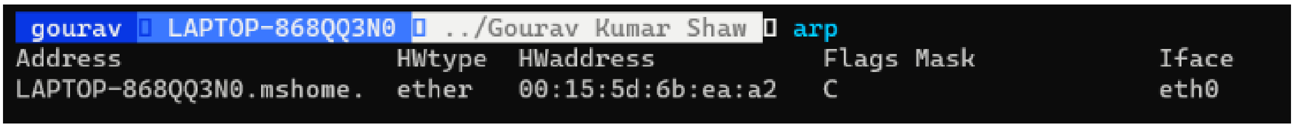
```
No.   Time        Source         Destination       Protocol  Length Info
   83 9.194542    10.2.2.138     10.2.1.40         TCP         54 60942 → 22 [ACK] Seq=1 Ack=1321 Win=251 Len=0
   84 9.208182    10.2.90.95     239.255.255.250   SSDP       216 M-SEARCH * HTTP/1.1
   85 9.273645    10.2.2.138     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
```

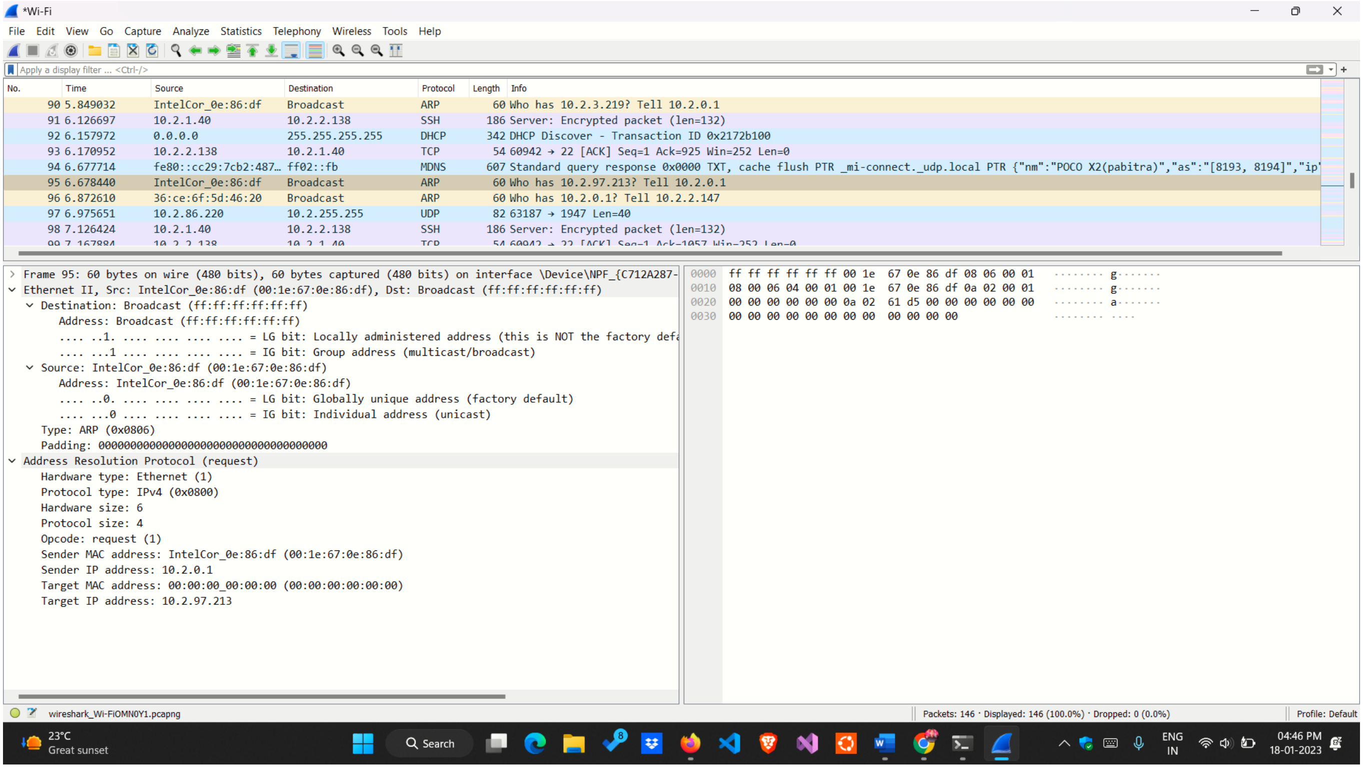
```
0000  9c b6 54 96 62 28 d8 c0  a6 b6 0a 19 08 00 45 00   ··T·b(·· ······E·
0010  00 28 dd 36 40 00 80 06  05 e4 0a 02 02 8a 0a 02   ·(·6@··· ········
0020  01 28 ee 0e 00 16 87 c9  35 79 a8 16 7e 10 50 10   ·(······ 5y··~·P·
0030  00 fc c5 94 00 00                                  ······
```

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

4. arp



```
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-/>
23°C
Great sunset
Search
ENG
IN
04:46 PM
18-01-2023

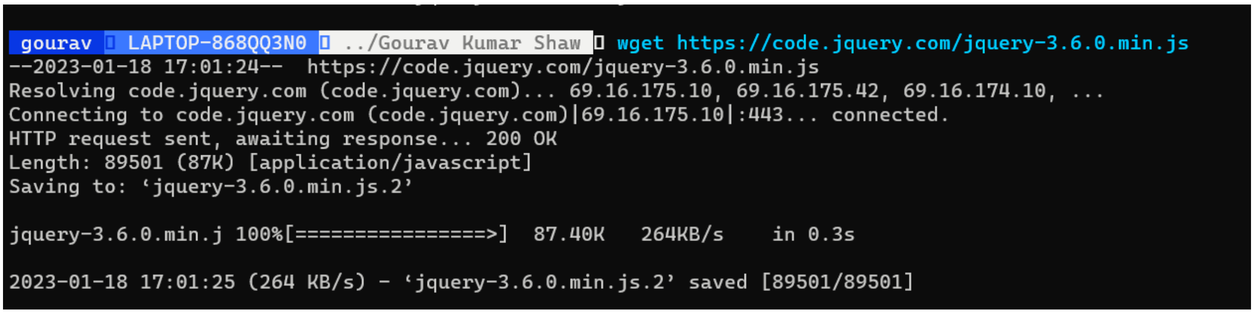
```
No.   Time      Source                  Destination      Protocol  Length Info
   90 5.849032  IntelCor_0e:86:df       Broadcast        ARP        60 Who has 10.2.3.219? Tell 10.2.0.1
   91 6.126697  10.2.1.40               10.2.2.138       SSH       186 Server: Encrypted packet (len=132)
   92 6.157972  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)
   99 7.167884  10.2.2.138              10.2.1.40        TCP        54 60942 → 22 [ACK] Seq=1 Ack=1057 Win=252 Len=0
```

```
> 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               ········ ····
```

```
wireshark_Wi-FiOMN0Y1.pcapng          Packets: 146 · Displayed: 146 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

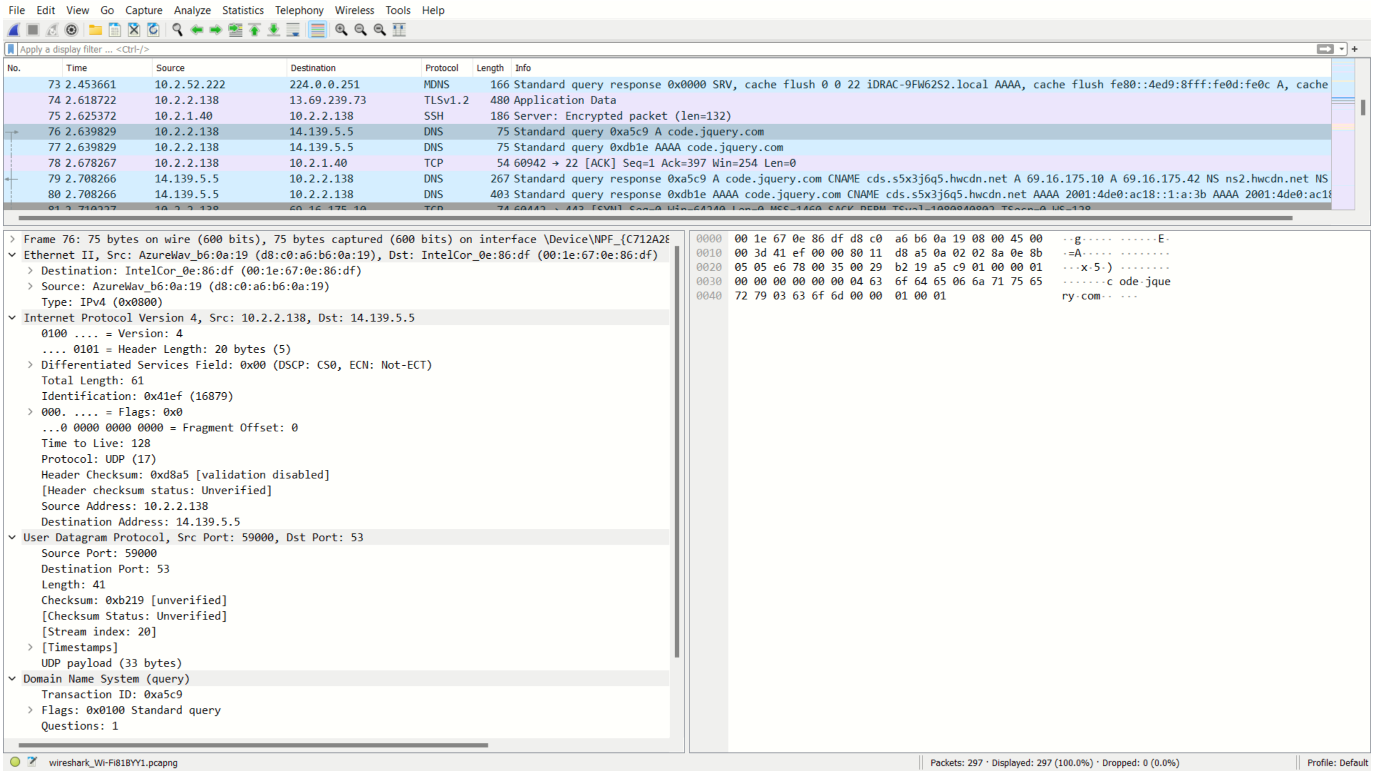
5. wget



```
 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]
```


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

```
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
```

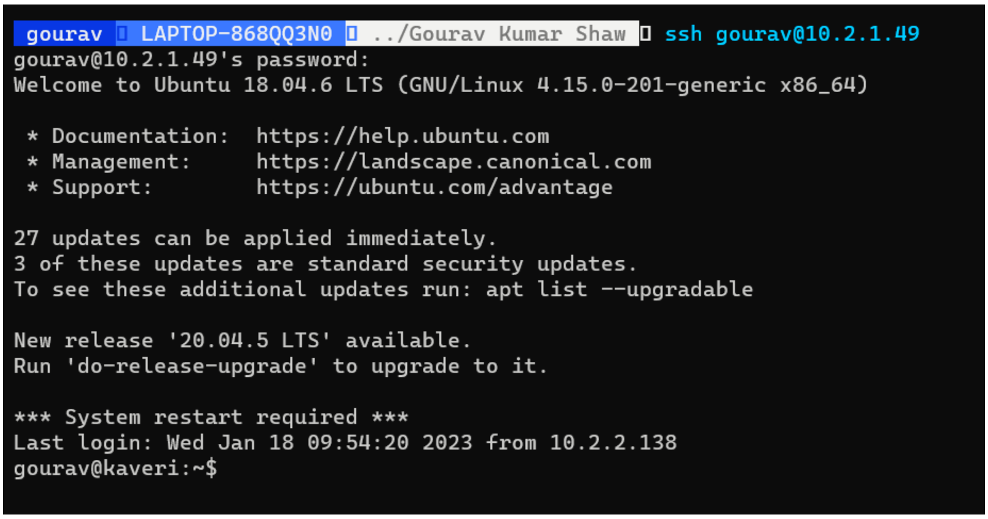
```
> Frame 76: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{C712A28
v Ethernet II, Src: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19), Dst: IntelCor_0e:86:df (00:1e:67:0e:86:df)
  > Destination: IntelCor_0e:86:df (00:1e:67:0e:86:df)
  > Source: AzureWav_b6:0a:19 (d8:c0:a6:b6:0a:19)
    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

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?

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?



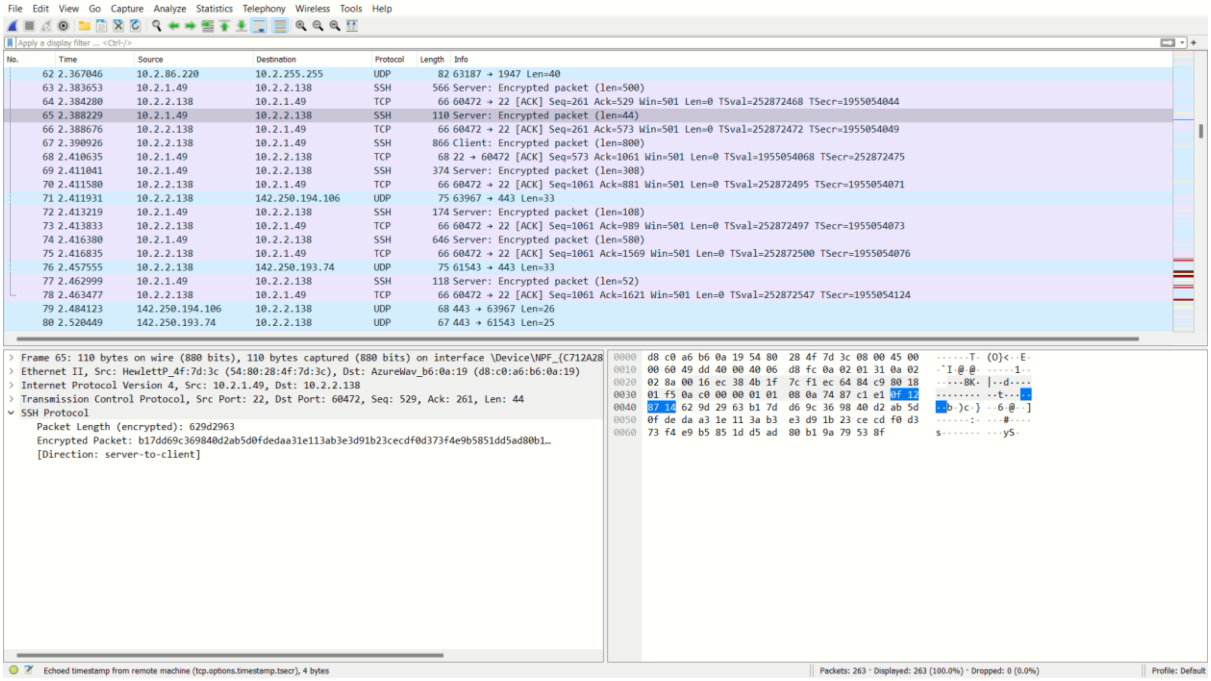
```
 gourav  LAPTOP-868QQ3N0  ../Gourav Kumar Shaw  ssh gourav@10.2.1.49
gourav@10.2.1.49's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-201-generic x86_64)

 * 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:~$
```



```
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·
```

Echoed timestamp from remote machine (tcp.options.timestamp.tsecr), 4 bytes
Packets: 263 · Displayed: 263 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

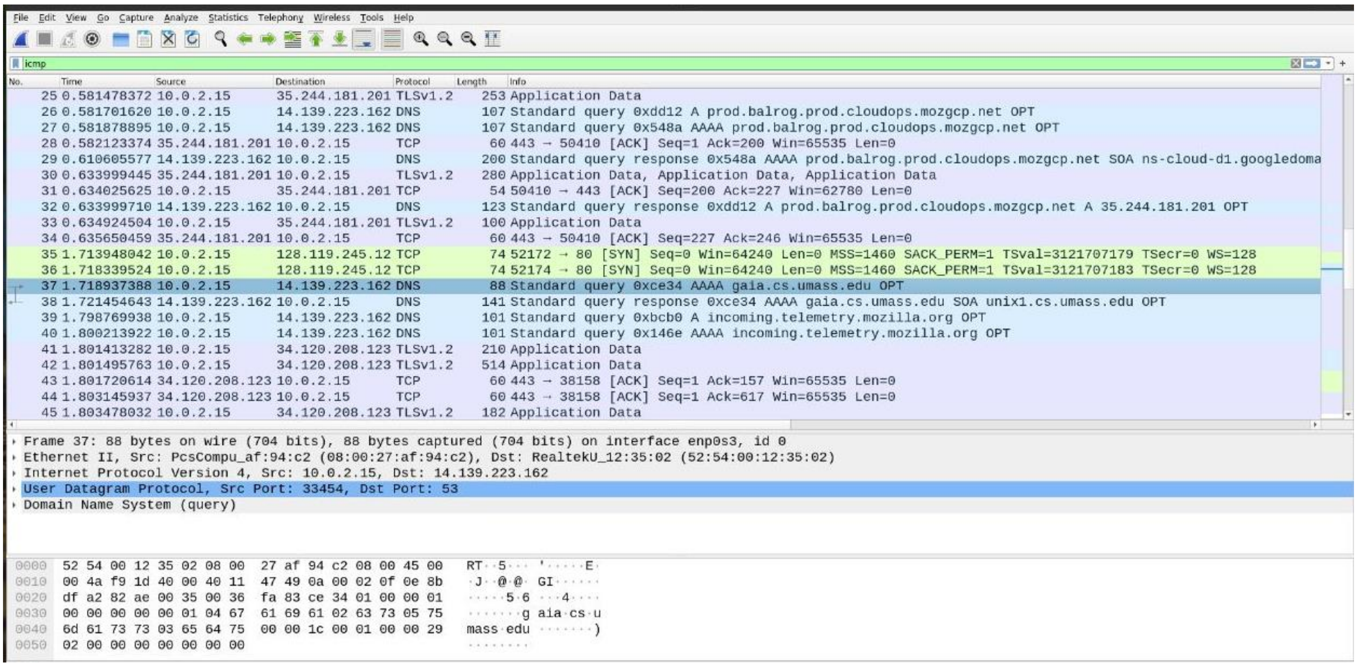
4. Enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and capture packets using Wireshark. After your

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?

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.



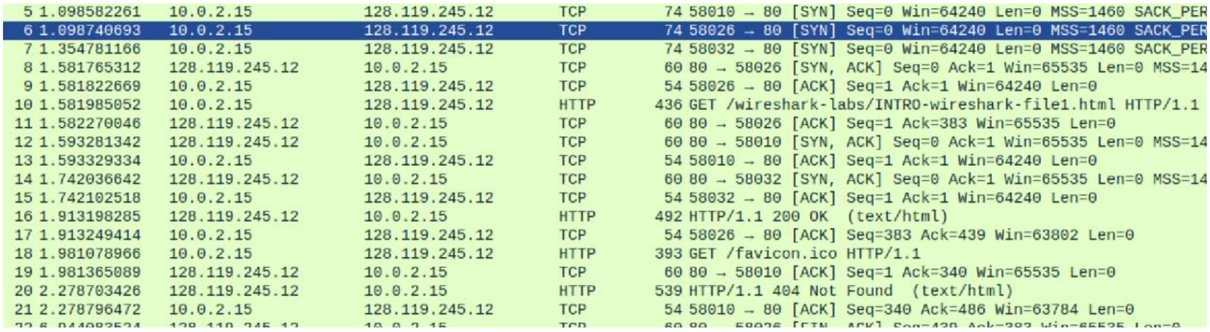
icmp

```
No.  Time        Source          Destination     Protocol Length Info
  25 0.581478372 10.0.2.15       35.244.181.201  TLSv1.2  253 Application Data
  26 0.581701620 10.0.2.15       14.139.223.162  DNS      107 Standard query 0xdd12 A prod.balrog.prod.cloudops.mozgcp.net OPT
  27 0.581878895 10.0.2.15       14.139.223.162  DNS      107 Standard query 0x548a AAAA prod.balrog.prod.cloudops.mozgcp.net OPT
  28 0.582123374 35.244.181.201  10.0.2.15       TCP       60 443 → 50410 [ACK] Seq=1 Ack=200 Win=65535 Len=0
  29 0.610605577 14.139.223.162  10.0.2.15       DNS      200 Standard query response 0x548a AAAA prod.balrog.prod.cloudops.mozgcp.net SOA ns-cloud-d1.googledoma
  30 0.633999445 35.244.181.201  10.0.2.15       TLSv1.2  280 Application Data, Application Data, Application Data
  31 0.634025625 10.0.2.15       35.244.181.201  TCP       54 50410 → 443 [ACK] Seq=200 Ack=227 Win=62780 Len=0
  32 0.633999710 14.139.223.162  10.0.2.15       DNS      123 Standard query response 0xdd12 A prod.balrog.prod.cloudops.mozgcp.net A 35.244.181.201 OPT
  33 0.634924504 10.0.2.15       35.244.181.201  TLSv1.2  100 Application Data
  34 0.635650459 35.244.181.201  10.0.2.15       TCP       60 443 → 50410 [ACK] Seq=227 Ack=246 Win=65535 Len=0
  35 1.713948042 10.0.2.15       128.119.245.12  TCP       74 52172 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3121707179 TSecr=0 WS=128
  36 1.718339524 10.0.2.15       128.119.245.12  TCP       74 52174 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3121707183 TSecr=0 WS=128
  37 1.718937388 10.0.2.15       14.139.223.162  DNS       88 Standard query 0xce34 AAAA gaia.cs.umass.edu OPT
  38 1.721454643 14.139.223.162  10.0.2.15       DNS      141 Standard query response 0xce34 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu OPT
  39 1.798769938 10.0.2.15       14.139.223.162  DNS      101 Standard query 0xbcb0 A incoming.telemetry.mozilla.org OPT
  40 1.800213922 10.0.2.15       14.139.223.162  DNS      101 Standard query 0x146e AAAA incoming.telemetry.mozilla.org OPT
  41 1.801413282 10.0.2.15       34.120.208.123  TLSv1.2  210 Application Data
  42 1.801495763 10.0.2.15       34.120.208.123  TLSv1.2  514 Application Data
  43 1.801720614 34.120.208.123  10.0.2.15       TCP       60 443 → 38158 [ACK] Seq=1 Ack=157 Win=65535 Len=0
  44 1.803145937 34.120.208.123  10.0.2.15       TCP       60 443 → 38158 [ACK] Seq=1 Ack=617 Win=65535 Len=0
  45 1.803478032 10.0.2.15       34.120.208.123  TLSv1.2  182 Application Data
```

```
› Frame 37: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_af:94:c2 (08:00:27:af:94:c2), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 14.139.223.162
› User Datagram Protocol, Src Port: 33454, Dst Port: 53
› Domain Name System (query)
```

```
0000  52 54 00 12 35 02 08 00  27 af 94 c2 08 00 45 00   RT··5···'·····E·
0010  00 4a f9 1d 40 00 40 11  47 49 0a 00 02 0f 0e 8b   ·J··@·@· GI······
0020  df a2 82 ae 00 35 00 36  fa 83 ce 34 01 00 00 01   ·····5·6 ···4····
0030  00 00 00 00 00 01 04 67  61 69 61 02 63 73 05 75   ·······g aia·cs·u
0040  6d 61 73 73 03 65 64 75  00 00 1c 00 01 00 00 29   mass·edu ·······)
0050  02 00 00 00 00 00 00 00                            ········
```

gaia.cs.umass.edu->14.139.223.162



```
 5 1.098582261   10.0.2.15        128.119.245.12   TCP    74 58010 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 6 1.098740693   10.0.2.15        128.119.245.12   TCP    74 58026 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 7 1.354781166   10.0.2.15        128.119.245.12   TCP    74 58032 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 8 1.581765312   128.119.245.12   10.0.2.15        TCP    60 80 → 58026 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
 9 1.581822669   10.0.2.15        128.119.245.12   TCP    54 58026 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10 1.581985052   10.0.2.15        128.119.245.12   HTTP  436 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
11 1.582270046   128.119.245.12   10.0.2.15        TCP    60 80 → 58026 [ACK] Seq=1 Ack=383 Win=65535 Len=0
12 1.593281342   128.119.245.12   10.0.2.15        TCP    60 80 → 58010 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
13 1.593329334   10.0.2.15        128.119.245.12   TCP    54 58010 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
14 1.742036642   128.119.245.12   10.0.2.15        TCP    60 80 → 58032 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
15 1.742102518   10.0.2.15        128.119.245.12   TCP    54 58032 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
16 1.913198285   128.119.245.12   10.0.2.15        HTTP  492 HTTP/1.1 200 OK  (text/html)
17 1.913249414   10.0.2.15        128.119.245.12   TCP    54 58026 → 80 [ACK] Seq=383 Ack=439 Win=63802 Len=0
18 1.981078966   10.0.2.15        128.119.245.12   HTTP  393 GET /favicon.ico HTTP/1.1
19 1.981365089   128.119.245.12   10.0.2.15        TCP    60 80 → 58010 [ACK] Seq=1 Ack=340 Win=65535 Len=0
20 2.278703426   128.119.245.12   10.0.2.15        HTTP  539 HTTP/1.1 404 Not Found  (text/html)
21 2.278796472   10.0.2.15        128.119.245.12   TCP    54 58010 → 80 [ACK] Seq=340 Ack=486 Win=63784 Len=0
```