COMPUTER NETWORKS

ASSIGNMENT # 1

SUBMITTED TO: Dr. Umar Farooq

SUBMITTED BY: M. Wajih Haider

ROLL NO: 280818

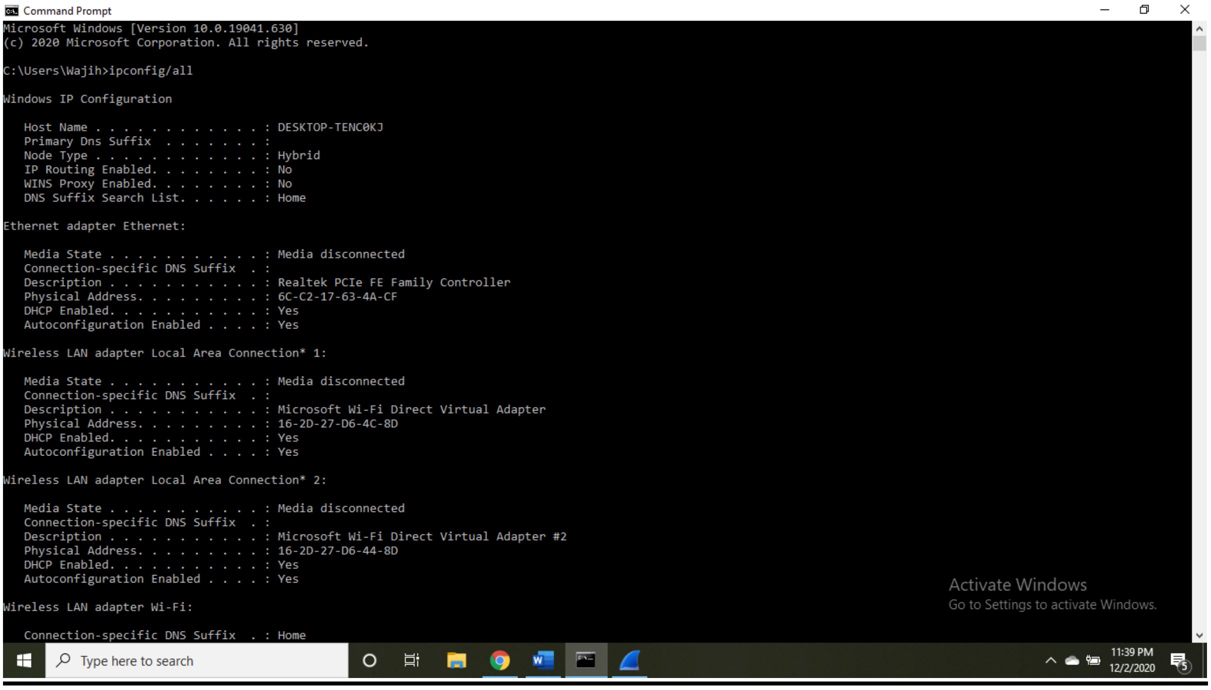
CE-40

SYNDICATE - B

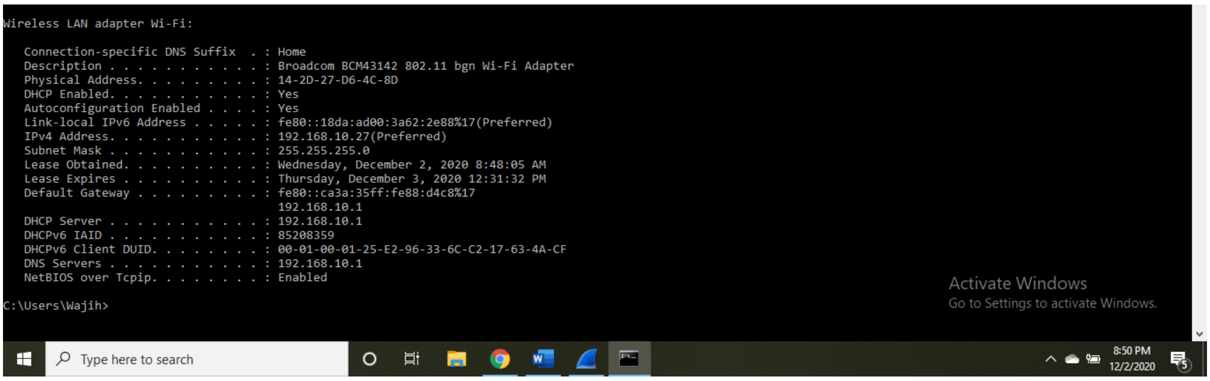
DATE: 2nd Dec 2020

DEPARTMENT OF COMPUTER AND SOFTWARE ENGINEERING

Output from ipconfig/all command

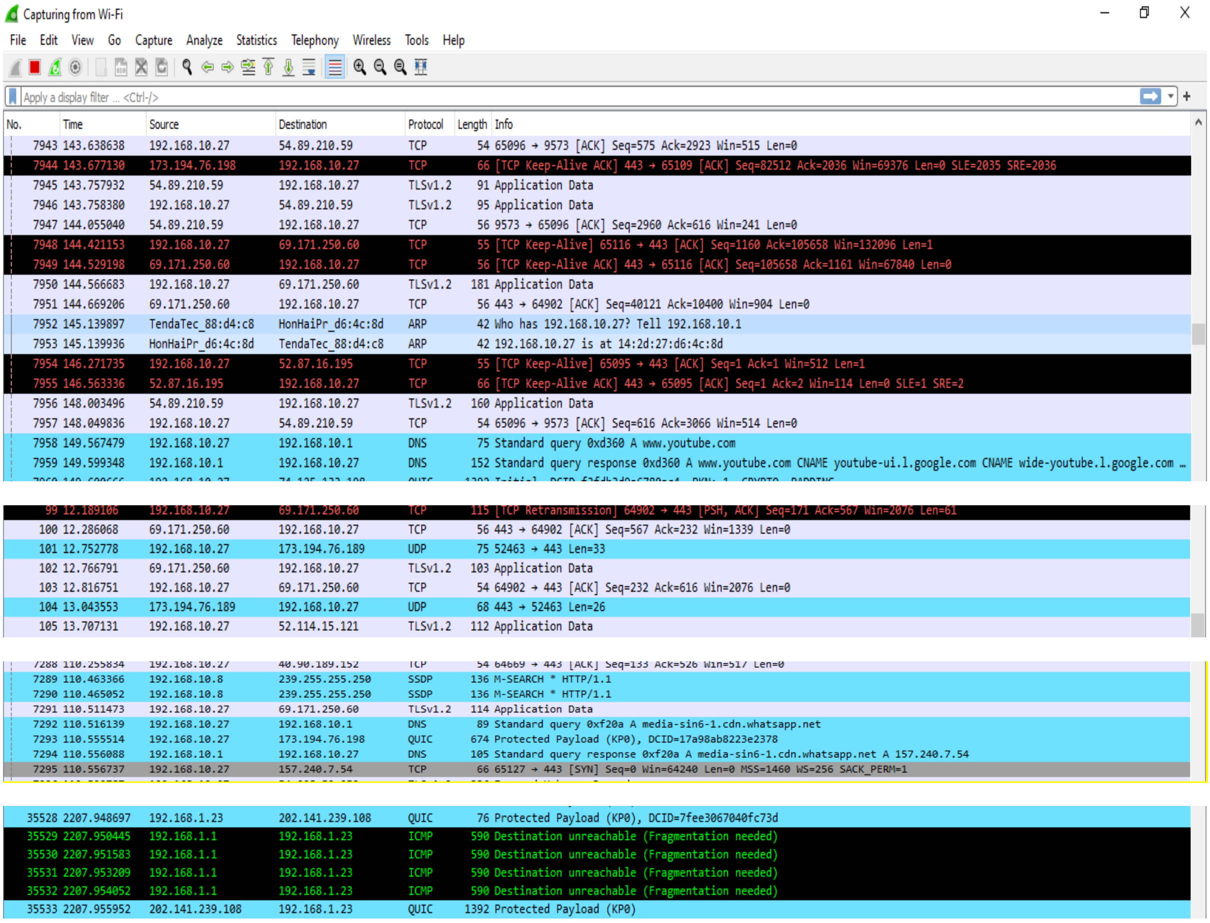


```
Microsoft Windows [Version 10.0.19041.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Wajih>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-TENC0KJ
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : Home

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 6C-C2-17-63-4A-CF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 16-2D-27-D6-4C-8D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 16-2D-27-D6-44-8D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Home
```



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Home
   Description . . . . . . . . . . . : Broadcom BCM43142 802.11 bgn Wi-Fi Adapter
   Physical Address. . . . . . . . . : 14-2D-27-D6-4C-8D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::18da:ad00:3a62:2e88%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.27(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, December 2, 2020 8:48:05 AM
   Lease Expires . . . . . . . . . . : Thursday, December 3, 2020 12:31:32 PM
   Default Gateway . . . . . . . . . : fe80::ca3a:35ff:fe88:d4c8%17
                                       192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 85208359
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-E2-96-33-6C-C2-17-63-4A-CF
   DNS Servers . . . . . . . . . . . : 192.168.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Wajih>
```

<u>TASK # 1:</u>


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

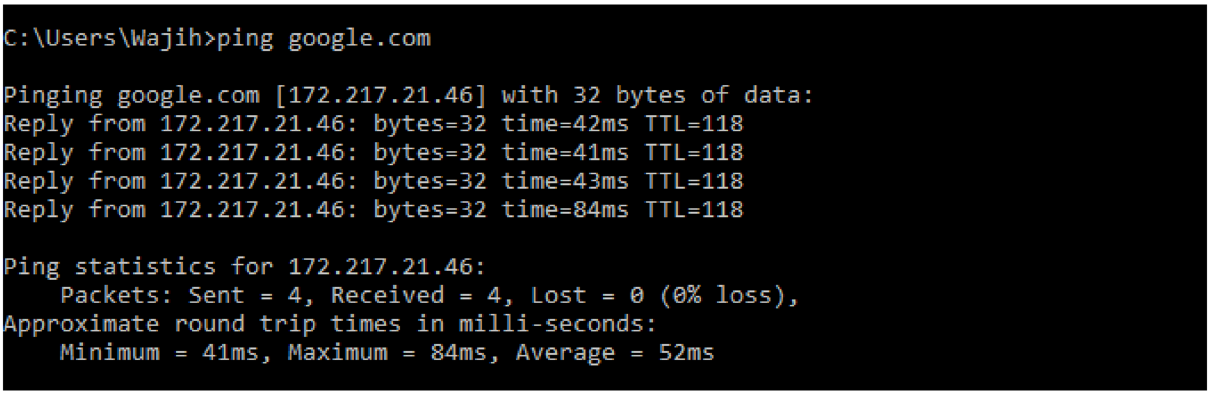
```
No.   Time        Source            Destination      Protocol Length Info
 7943 143.638638  192.168.10.27     54.89.210.59     TCP        54 65096 → 9573 [ACK] Seq=575 Ack=2923 Win=515 Len=0
 7944 143.677130  173.194.76.198    192.168.10.27    TCP        66 [TCP Keep-Alive ACK] 443 → 65109 [ACK] Seq=82512 Ack=2036 Win=69376 Len=0 SLE=2035 SRE=2036
 7945 143.757932  54.89.210.59      192.168.10.27    TLSv1.2    91 Application Data
 7946 143.758380  192.168.10.27     54.89.210.59     TLSv1.2    95 Application Data
 7947 144.055040  54.89.210.59      192.168.10.27    TCP        56 9573 → 65096 [ACK] Seq=2960 Ack=616 Win=241 Len=0
 7948 144.421153  192.168.10.27     69.171.250.60    TCP        55 [TCP Keep-Alive] 65116 → 443 [ACK] Seq=1160 Ack=105658 Win=132096 Len=1
 7949 144.529198  69.171.250.60     192.168.10.27    TCP        56 [TCP Keep-Alive ACK] 443 → 65116 [ACK] Seq=105658 Ack=1161 Win=67840 Len=0
 7950 144.566683  192.168.10.27     69.171.250.60    TLSv1.2   181 Application Data
 7951 144.669206  69.171.250.60     192.168.10.27    TCP        56 443 → 64902 [ACK] Seq=40121 Ack=10400 Win=904 Len=0
 7952 145.139897  TendaTec_88:d4:c8 HonHaiPr_d6:4c:8d ARP       42 Who has 192.168.10.27? Tell 192.168.10.1
 7953 145.139936  HonHaiPr_d6:4c:8d TendaTec_88:d4:c8 ARP       42 192.168.10.27 is at 14:2d:27:d6:4c:8d
 7954 146.271735  192.168.10.27     52.87.16.195     TCP        55 [TCP Keep-Alive] 65095 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
 7955 146.563336  52.87.16.195      192.168.10.27    TCP        66 [TCP Keep-Alive ACK] 443 → 65095 [ACK] Seq=1 Ack=2 Win=114 Len=0 SLE=1 SRE=2
 7956 148.003496  54.89.210.59      192.168.10.27    TLSv1.2   160 Application Data
 7957 148.049836  192.168.10.27     54.89.210.59     TCP        54 65096 → 9573 [ACK] Seq=616 Ack=3066 Win=514 Len=0
 7958 149.567479  192.168.10.27     192.168.10.1     DNS        75 Standard query 0xd360 A www.youtube.com
 7959 149.599348  192.168.10.1      192.168.10.27    DNS       152 Standard query response 0xd360 A www.youtube.com CNAME youtube-ui.l.google.com CNAME wide-youtube.l.google.com …

   99 12.189106   192.168.10.27     69.171.250.60    TCP       115 [TCP Retransmission] 64902 → 443 [PSH, ACK] Seq=171 Ack=567 Win=2076 Len=61
  100 12.286068   69.171.250.60     192.168.10.27    TCP        56 443 → 64902 [ACK] Seq=567 Ack=232 Win=1339 Len=0
  101 12.752778   192.168.10.27     173.194.76.189   UDP        75 52463 → 443 Len=33
  102 12.766791   69.171.250.60     192.168.10.27    TLSv1.2   103 Application Data
  103 12.816751   192.168.10.27     69.171.250.60    TCP        54 64902 → 443 [ACK] Seq=232 Ack=616 Win=2076 Len=0
  104 13.043553   173.194.76.189    192.168.10.27    UDP        68 443 → 52463 Len=26
  105 13.707131   192.168.10.27     52.114.15.121    TLSv1.2   112 Application Data

 7288 110.255834  192.168.10.27     40.90.189.152    TCP        54 64669 → 443 [ACK] Seq=133 Ack=526 Win=517 Len=0
 7289 110.463366  192.168.10.8      239.255.255.250  SSDP      136 M-SEARCH * HTTP/1.1
 7290 110.465052  192.168.10.8      239.255.255.250  SSDP      136 M-SEARCH * HTTP/1.1
 7291 110.511473  192.168.10.27     69.171.250.60    TLSv1.2   114 Application Data
 7292 110.516139  192.168.10.27     192.168.10.1     DNS        89 Standard query 0xf20a A media-sin6-1.cdn.whatsapp.net
 7293 110.555514  192.168.10.27     173.194.76.198   QUIC      674 Protected Payload (KP0), DCID=17a98ab8223e2378
 7294 110.556088  192.168.10.1      192.168.10.27    DNS       105 Standard query response 0xf20a A media-sin6-1.cdn.whatsapp.net A 157.240.7.54
 7295 110.556737  192.168.10.27     157.240.7.54     TCP        66 65127 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

35528 2207.948697 192.168.1.23      202.141.239.108  QUIC       76 Protected Payload (KP0), DCID=7fee3067040fc73d
35529 2207.950445 192.168.1.1       192.168.1.23     ICMP      590 Destination unreachable (Fragmentation needed)
35530 2207.951583 192.168.1.1       192.168.1.23     ICMP      590 Destination unreachable (Fragmentation needed)
35531 2207.953209 192.168.1.1       192.168.1.23     ICMP      590 Destination unreachable (Fragmentation needed)
35532 2207.954052 192.168.1.1       192.168.1.23     ICMP      590 Destination unreachable (Fragmentation needed)
35533 2207.955952 202.141.239.108   192.168.1.23     QUIC     1392 Protected Payload (KP0)
```

In this we can see various protocol headers, every header is either transport or application or network layer.

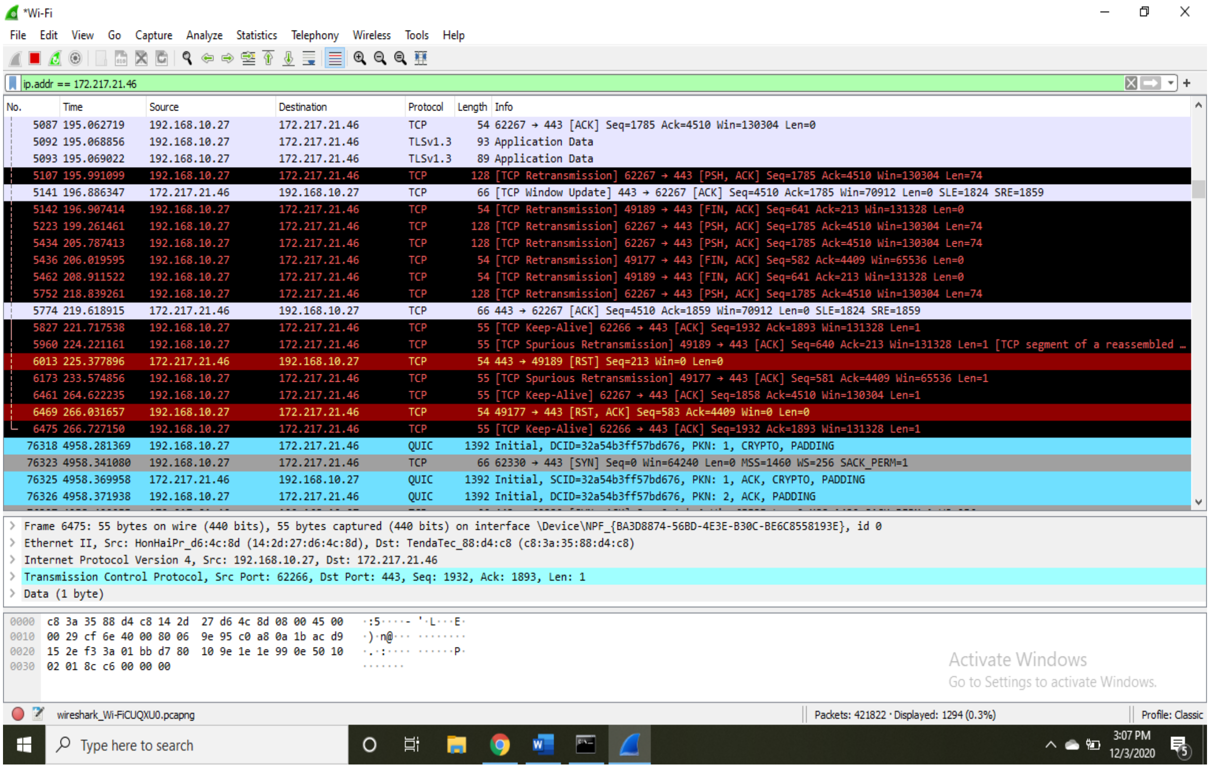
If we go through the screenshots above, we can see that we have UDP and TCP protocols these are the protocols of Transport Layer which is also the middle layer which helps application and network layer communicate. Moreover, if we look further, we can see ARP and ICMP Protocol headers in the above screenshots these are the protocols of Network Layer. QUIC, SSDP, and DNS are few protocols which can be seen above in the screenshots are those which work on Application layer.

Hence, we can see that the protocols of each of the Application, Transport and Network layer has been identified.

TASK # 2:



```
C:\Users\Wajih>ping google.com

Pinging google.com [172.217.21.46] with 32 bytes of data:
Reply from 172.217.21.46: bytes=32 time=42ms TTL=118
Reply from 172.217.21.46: bytes=32 time=41ms TTL=118
Reply from 172.217.21.46: bytes=32 time=43ms TTL=118
Reply from 172.217.21.46: bytes=32 time=84ms TTL=118

Ping statistics for 172.217.21.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 41ms, Maximum = 84ms, Average = 52ms
```



```
ip.addr == 172.217.21.46
```

```
No.    Time         Source          Destination     Protocol Length Info
  5087 195.062719   192.168.10.27   172.217.21.46   TCP        54 62267 → 443 [ACK] Seq=1785 Ack=4510 Win=130304 Len=0
  5092 195.068856   192.168.10.27   172.217.21.46   TLSv1.3    93 Application Data
  5093 195.069022   192.168.10.27   172.217.21.46   TLSv1.3    89 Application Data
  5107 195.991099   192.168.10.27   172.217.21.46   TCP       128 [TCP Retransmission] 62267 → 443 [PSH, ACK] Seq=1785 Ack=4510 Win=130304 Len=74
  5141 196.886347   172.217.21.46   192.168.10.27   TCP        66 [TCP Window Update] 443 → 62267 [ACK] Seq=4510 Ack=1785 Win=70912 Len=0 SLE=1824 SRE=1859
  5142 196.907414   192.168.10.27   172.217.21.46   TCP        54 [TCP Retransmission] 49189 → 443 [FIN, ACK] Seq=641 Ack=213 Win=131328 Len=0
  5223 199.261461   192.168.10.27   172.217.21.46   TCP       128 [TCP Retransmission] 62267 → 443 [PSH, ACK] Seq=1785 Ack=4510 Win=130304 Len=74
  5434 205.787413   192.168.10.27   172.217.21.46   TCP       128 [TCP Retransmission] 62267 → 443 [PSH, ACK] Seq=1785 Ack=4510 Win=130304 Len=74
  5436 206.019595   192.168.10.27   172.217.21.46   TCP        54 [TCP Retransmission] 49177 → 443 [FIN, ACK] Seq=582 Ack=4409 Win=65536 Len=0
  5462 208.911522   192.168.10.27   172.217.21.46   TCP        54 [TCP Retransmission] 49189 → 443 [FIN, ACK] Seq=641 Ack=213 Win=131328 Len=0
  5752 218.839261   192.168.10.27   172.217.21.46   TCP       128 [TCP Retransmission] 62267 → 443 [PSH, ACK] Seq=1785 Ack=4510 Win=130304 Len=74
  5774 219.618915   172.217.21.46   192.168.10.27   TCP        66 443 → 62267 [ACK] Seq=4510 Ack=1859 Win=70912 Len=0 SLE=1824 SRE=1859
  5827 221.717538   192.168.10.27   172.217.21.46   TCP        55 [TCP Keep-Alive] 62266 → 443 [ACK] Seq=1932 Ack=1893 Win=131328 Len=1
  5960 224.221161   192.168.10.27   172.217.21.46   TCP        55 [TCP Spurious Retransmission] 49189 → 443 [ACK] Seq=640 Ack=213 Win=131328 Len=1 [TCP segment of a reassembled …
  6013 225.377896   172.217.21.46   192.168.10.27   TCP        54 443 → 49189 [RST] Seq=213 Win=0 Len=0
  6173 233.574856   192.168.10.27   172.217.21.46   TCP        55 [TCP Spurious Retransmission] 49177 → 443 [ACK] Seq=581 Ack=4409 Win=65536 Len=1
  6461 264.622235   192.168.10.27   172.217.21.46   TCP        55 [TCP Keep-Alive] 62267 → 443 [ACK] Seq=1858 Ack=4510 Win=130304 Len=1
  6469 266.031657   192.168.10.27   172.217.21.46   TCP        54 49177 → 443 [RST, ACK] Seq=583 Ack=4409 Win=0 Len=0
  6475 266.727150   192.168.10.27   172.217.21.46   TCP        55 [TCP Keep-Alive] 62266 → 443 [ACK] Seq=1932 Ack=1893 Win=131328 Len=1
 76318 4958.281369  192.168.10.27   172.217.21.46   QUIC     1392 Initial, DCID=32a54b3ff57bd676, PKN: 1, CRYPTO, PADDING
 76323 4958.341080  192.168.10.27   172.217.21.46   TCP        66 62330 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 76325 4958.369958  172.217.21.46   192.168.10.27   QUIC     1392 Initial, SCID=32a54b3ff57bd676, PKN: 1, ACK, CRYPTO, PADDING
 76326 4958.371938  192.168.10.27   172.217.21.46   QUIC     1392 Initial, DCID=32a54b3ff57bd676, PKN: 2, ACK, PADDING
```

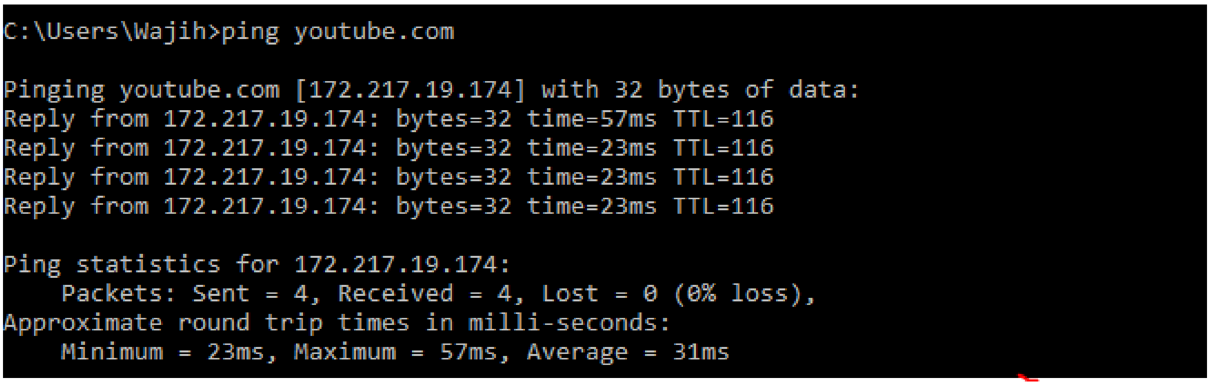
```
> Frame 6475: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{BA3D8874-56BD-4E3E-B30C-BE6C8558193E}, id 0
> Ethernet II, Src: HonHaiPr_d6:4c:8d (14:2d:27:d6:4c:8d), Dst: TendaTec_88:d4:c8 (c8:3a:35:88:d4:c8)
> Internet Protocol Version 4, Src: 192.168.10.27, Dst: 172.217.21.46
> Transmission Control Protocol, Src Port: 62266, Dst Port: 443, Seq: 1932, Ack: 1893, Len: 1
> Data (1 byte)
```

```
0000  c8 3a 35 88 d4 c8 14 2d  27 d6 4c 8d 08 00 45 00   ·:5····- '·L···E·
0010  00 29 cf 6e 40 00 80 06  9e 95 c0 a8 0a 1b ac d9   ·)·n@··· ········
0020  15 2e f3 3a 01 bb d7 80  10 9e 1e 1e 99 0e 50 10   ·.·:···· ······P·
0030  02 01 8c c6 00 00 00                               ·······
```

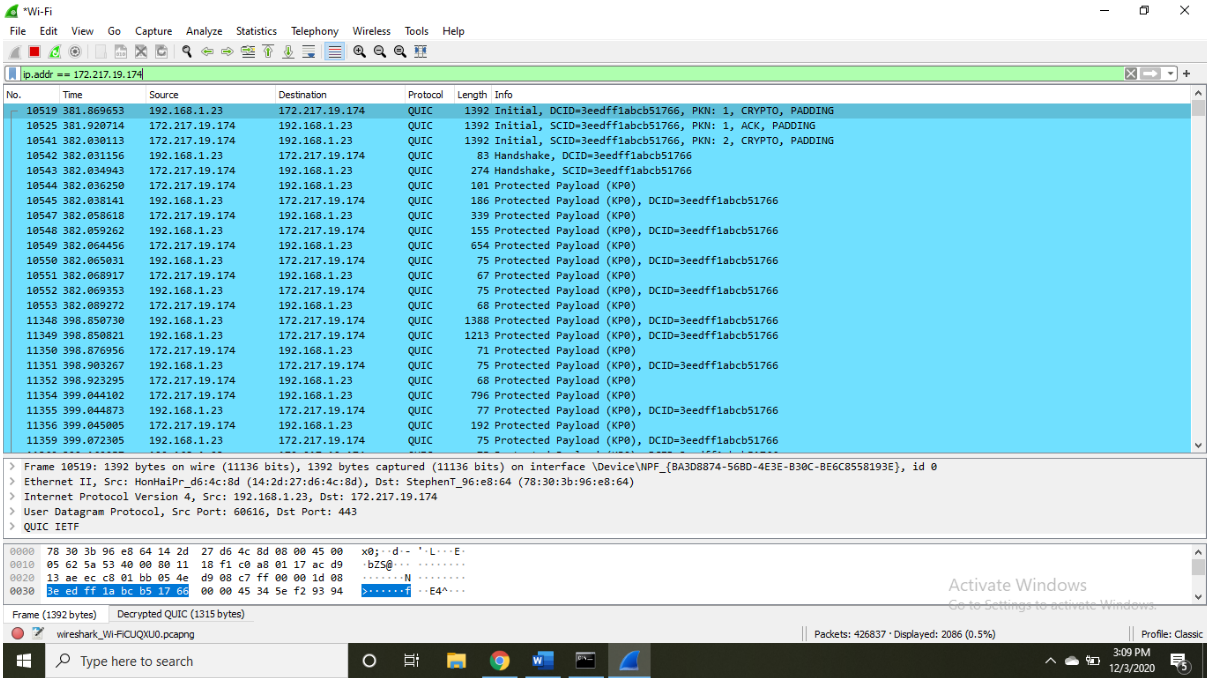
Activate Windows
Go to Settings to activate Windows.

wireshark_Wi-FiCUQXU0.pcapng | Packets: 421822 · Displayed: 1294 (0.3%) | Profile: Classic

Firstly, we pinged google.com through command prompt to get its IP Address which is 172.217.21.46, then we put up the filter as it can be seen in the screenshots too. This screenshot shows the traffic between our PC and google.com. We can also see that in some of the packets/messages our PC is the destination as it is coming from google, in others google is the destination as out PC is sending the packets/messages



```
C:\Users\Wajih>ping youtube.com

Pinging youtube.com [172.217.19.174] with 32 bytes of data:
Reply from 172.217.19.174: bytes=32 time=57ms TTL=116
Reply from 172.217.19.174: bytes=32 time=23ms TTL=116
Reply from 172.217.19.174: bytes=32 time=23ms TTL=116
Reply from 172.217.19.174: bytes=32 time=23ms TTL=116

Ping statistics for 172.217.19.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 57ms, Average = 31ms
```

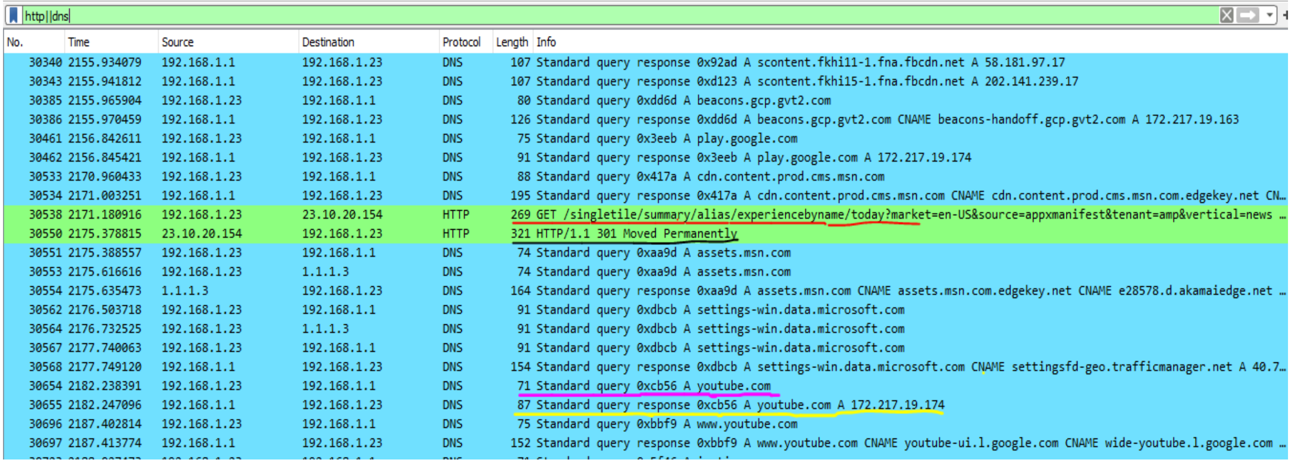


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 172.217.19.174

No.   Time        Source          Destination     Protocol Length Info
10519 381.869653  192.168.1.23    172.217.19.174  QUIC     1392 Initial, DCID=3eedff1abcb51766, PKN: 1, CRYPTO, PADDING
10525 381.920714  172.217.19.174  192.168.1.23    QUIC     1392 Initial, SCID=3eedff1abcb51766, PKN: 1, ACK, PADDING
10541 382.030113  172.217.19.174  192.168.1.23    QUIC     1392 Initial, SCID=3eedff1abcb51766, PKN: 2, CRYPTO, PADDING
10542 382.031156  192.168.1.23    172.217.19.174  QUIC       83 Handshake, DCID=3eedff1abcb51766
10543 382.034943  172.217.19.174  192.168.1.23    QUIC      274 Handshake, SCID=3eedff1abcb51766
10544 382.036250  172.217.19.174  192.168.1.23    QUIC      101 Protected Payload (KP0)
10545 382.038141  192.168.1.23    172.217.19.174  QUIC      186 Protected Payload (KP0), DCID=3eedff1abcb51766
10547 382.058618  172.217.19.174  192.168.1.23    QUIC      339 Protected Payload (KP0)
10548 382.059262  192.168.1.23    172.217.19.174  QUIC      155 Protected Payload (KP0), DCID=3eedff1abcb51766
10549 382.064456  172.217.19.174  192.168.1.23    QUIC      654 Protected Payload (KP0)
10550 382.065031  192.168.1.23    172.217.19.174  QUIC       75 Protected Payload (KP0), DCID=3eedff1abcb51766
10551 382.068917  172.217.19.174  192.168.1.23    QUIC       67 Protected Payload (KP0)
10552 382.069353  192.168.1.23    172.217.19.174  QUIC       75 Protected Payload (KP0), DCID=3eedff1abcb51766
10553 382.089272  172.217.19.174  192.168.1.23    QUIC       68 Protected Payload (KP0)
11348 398.850730  192.168.1.23    172.217.19.174  QUIC     1388 Protected Payload (KP0), DCID=3eedff1abcb51766
11349 398.850821  192.168.1.23    172.217.19.174  QUIC     1213 Protected Payload (KP0), DCID=3eedff1abcb51766
11350 398.876956  172.217.19.174  192.168.1.23    QUIC       71 Protected Payload (KP0)
11351 398.903267  192.168.1.23    172.217.19.174  QUIC       75 Protected Payload (KP0), DCID=3eedff1abcb51766
11352 398.923295  172.217.19.174  192.168.1.23    QUIC       68 Protected Payload (KP0)
11354 399.044102  172.217.19.174  192.168.1.23    QUIC      796 Protected Payload (KP0)
11355 399.044873  192.168.1.23    172.217.19.174  QUIC       77 Protected Payload (KP0), DCID=3eedff1abcb51766
11356 399.045005  172.217.19.174  192.168.1.23    QUIC      192 Protected Payload (KP0)
11359 399.072305  192.168.1.23    172.217.19.174  QUIC       75 Protected Payload (KP0), DCID=3eedff1abcb51766

> Frame 10519: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface \Device\NPF_{BA3D8874-56BD-4E3E-B30C-BE6C8558193E}, id 0
> Ethernet II, Src: HonHaiPr_d6:4c:8d (14:2d:27:d6:4c:8d), Dst: StephenT_96:e8:64 (78:30:3b:96:e8:64)
> Internet Protocol Version 4, Src: 192.168.1.23, Dst: 172.217.19.174
> User Datagram Protocol, Src Port: 60616, Dst Port: 443
> QUIC IETF

0000  78 30 3b 96 e8 64 14 2d  27 d6 4c 8d 08 00 45 00   x0;··d·- '·L···E·
0010  05 62 5a 53 40 00 80 11  18 f1 c0 a8 01 17 ac d9   ·bZS@··· ········
0020  13 ae ec c8 01 bb 05 4e  d9 08 c7 ff 00 00 1d 08   ·······N ········
0030  3e ed ff 1a bc b5 17 66  00 00 45 34 5e f2 93 94   >······f ··E4^···

Frame (1392 bytes)   Decrypted QUIC (1315 bytes)
wireshark_Wi-FiCUQXU0.pcapng        Packets: 426837 · Displayed: 2086 (0.5%)        Profile: Classic
```

For filtering the traffic to and from youtube.com, we once again pinged youtube.com through command prompt to get its IP Address which is 172.217.19.174, then we put up the filter as it can be seen in the screenshot too. This screenshot of wireshark shows the traffic between our PC and youtube.com. We can also see that in some of the packets/messages our PC is the destination as they are coming from youtube, in others youtube is the destination as out PC is sending the packets/messages.

TASK # 3:



http||dns

No.	Time	Source	Destination	Protocol	Length	Info
30340	2155.934079	192.168.1.1	192.168.1.23	DNS	107	Standard query response 0x92ad A scontent.fkhi11-1.fna.fbcdn.net A 58.181.97.17
30343	2155.941812	192.168.1.1	192.168.1.23	DNS	107	Standard query response 0xd123 A scontent.fkhi15-1.fna.fbcdn.net A 202.141.239.17
30385	2155.965904	192.168.1.23	192.168.1.1	DNS	80	Standard query 0xdd6d A beacons.gcp.gvt2.com
30386	2155.970459	192.168.1.1	192.168.1.23	DNS	126	Standard query response 0xdd6d A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 172.217.19.163
30461	2156.842611	192.168.1.23	192.168.1.1	DNS	75	Standard query 0x3eeb A play.google.com
30462	2156.845421	192.168.1.1	192.168.1.23	DNS	91	Standard query response 0x3eeb A play.google.com A 172.217.19.174
30533	2170.960433	192.168.1.23	192.168.1.1	DNS	88	Standard query 0x417a A cdn.content.prod.cms.msn.com
30534	2171.003251	192.168.1.1	192.168.1.23	DNS	195	Standard query response 0x417a A cdn.content.prod.cms.msn.com CNAME cdn.content.prod.cms.msn.com.edgekey.net CN…
30538	2171.180916	192.168.1.23	23.10.20.154	HTTP	269	GET /singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news …
30550	2175.378815	23.10.20.154	192.168.1.23	HTTP	321	HTTP/1.1 301 Moved Permanently
30551	2175.388557	192.168.1.23	192.168.1.1	DNS	74	Standard query 0xaa9d A assets.msn.com
30553	2175.616616	192.168.1.23	1.1.1.3	DNS	74	Standard query 0xaa9d A assets.msn.com
30554	2175.635473	1.1.1.3	192.168.1.23	DNS	164	Standard query response 0xaa9d A assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net …
30562	2176.503718	192.168.1.23	192.168.1.1	DNS	91	Standard query 0xdbcb A settings-win.data.microsoft.com
30564	2176.732525	192.168.1.23	1.1.1.3	DNS	91	Standard query 0xdbcb A settings-win.data.microsoft.com
30567	2177.740063	192.168.1.23	192.168.1.1	DNS	91	Standard query 0xdbcb A settings-win.data.microsoft.com
30568	2177.749120	192.168.1.1	192.168.1.23	DNS	154	Standard query response 0xdbcb A settings-win.data.microsoft.com CNAME settingsfd-geo.trafficmanager.net A 40.7…
30654	2182.238391	192.168.1.23	192.168.1.1	DNS	71	Standard query 0xcb56 A youtube.com
30655	2182.247096	192.168.1.1	192.168.1.23	DNS	87	Standard query response 0xcb56 A youtube.com A 172.217.19.174
30696	2187.402814	192.168.1.23	192.168.1.1	DNS	75	Standard query 0xbbf9 A www.youtube.com
30697	2187.413774	192.168.1.1	192.168.1.23	DNS	152	Standard query response 0xbbf9 A www.youtube.com CNAME youtube-ui.l.google.com CNAME wide-youtube.l.google.com …

Application layer protocols has two types of messages one of them is Request Message other is Response Message.

To identify and label them as required by the task, first of all, we put a filter to get the packets/messages only to and from DNS and HTTP which are application layer protocols. Now we can see the red underlined packet of HTTP no. 30538 is **request type** message, which is requesting for something, same way no.30550 a packet of HTTP which is underlined by black line is **response type** message. For DNS protocol we can see the pink underlined packet no. 30654 a **request type** message is requesting something from google.com server. If we look just below it, we can see a DNS **response message** which is underlined by yellow line, it is a response to the request which was made sometimes earlier from youtube.com server.