IMRAN KHAN(1802035)
LAB#2
Computer Networks

1. Capture Traffic:

2. Ping t he following hosts:

1. www.facebook.com

C:\Users\imran khan>ping www.facebook.com

Pinging star-mini.c10r.facebook.com [157.240.227.35] with 32 bytes of data:
Reply from 157.240.227.35: bytes=32 time=49ms TTL=247
Reply from 157.240.227.35: bytes=32 time=49ms TTL=247
Reply from 157.240.227.35: bytes=32 time=47ms TTL=247
Reply from 157.240.227.35: bytes=32 time=55ms TTL=247

Ping statistics for 157.240.227.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 55ms, Average = 50ms

2. 172.16.0.1

C:\Users\imran khan>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time=4ms TTL=128
Reply from 172.16.0.1: bytes=32 time=5ms TTL=128
Reply from 172.16.0.1: bytes=32 time=5ms TTL=128
Reply from 172.16.0.1: bytes=32 time=4ms TTL=128

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

3. Any other host of your choice.

C:\Users\imran khan>ping www.google.com

Pinging www.google.com [216.58.208.228] with 32 bytes of data:
Reply from 216.58.208.228: bytes=32 time=46ms TTL=247
Reply from 216.58.208.228: bytes=32 time=47ms TTL=247
Reply from 216.58.208.228: bytes=32 time=47ms TTL=247
Reply from 216.58.208.228: bytes=32 time=45ms TTL=247

Ping statistics for 216.58.208.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 47ms, Average = 46ms

    C:\Users\imran khan>ping 172.16.0.67

    Pinging 172.16.0.67 with 32 bytes of data:
    Reply from 172.16.13.116: Destination host unreachable.

Reply from 172.16.13.116: Destination host unreachable.
Reply from 172.16.13.116: Destination host unreachable.
Reply from 172.16.13.116: Destination host unreachable.

Ping statistics for 172.16.0.67:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

4. Capturing Analysis:

- **How many packets have you captured?**

Packets: 32660

- **What is the average packet size?**

Avg packet size :668

- **List down all protocol names that you get in the captured data. Try to figure out which protocol is working up to which layer.**

TCP:Transport Layer

ARP:Network Layer

UDP:Transport Layer

ICMP:Network Layer

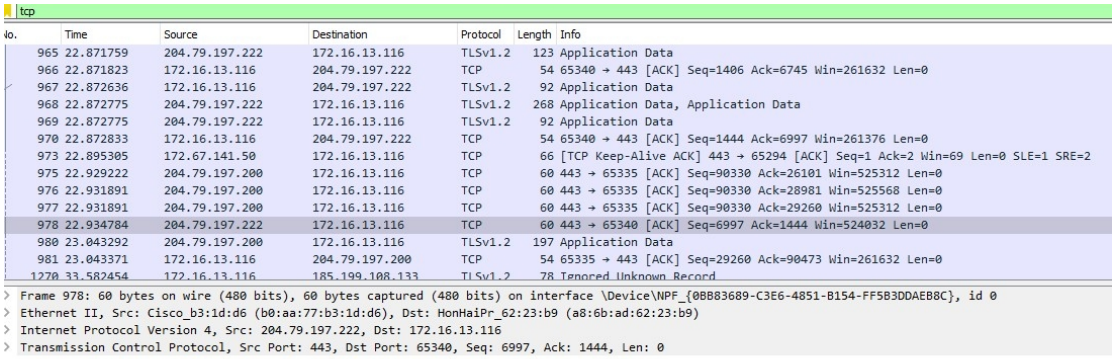
SSDP:Application Layer

DNS:Application layer

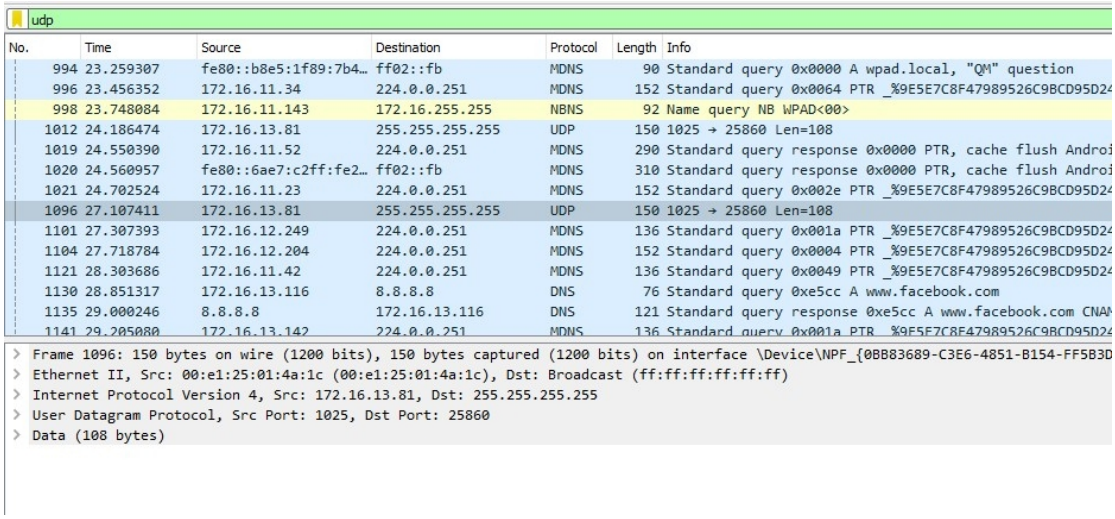
QUIC:Transport Layer

- ***Select any 3 packets with different protocol, and try to map each header section data to corresponding TCP/IP layer.***

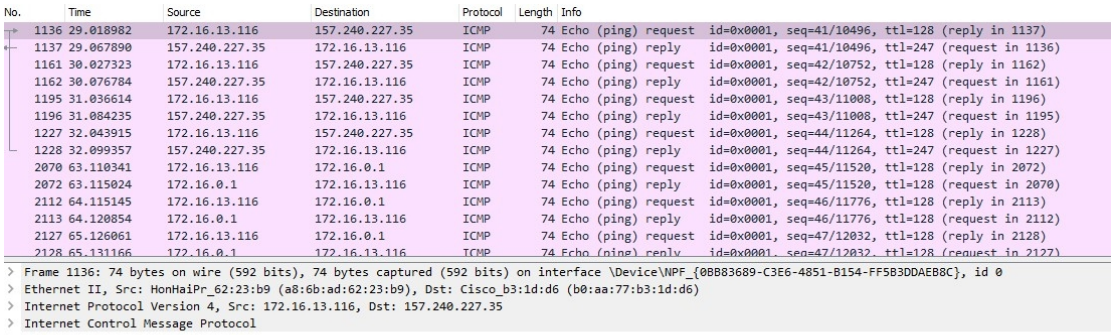
1. TCP



2. UDP



3.ICMP



• Search the ping packets you generated or received in task 2.3.2. Which protocol is being used in ping utility?

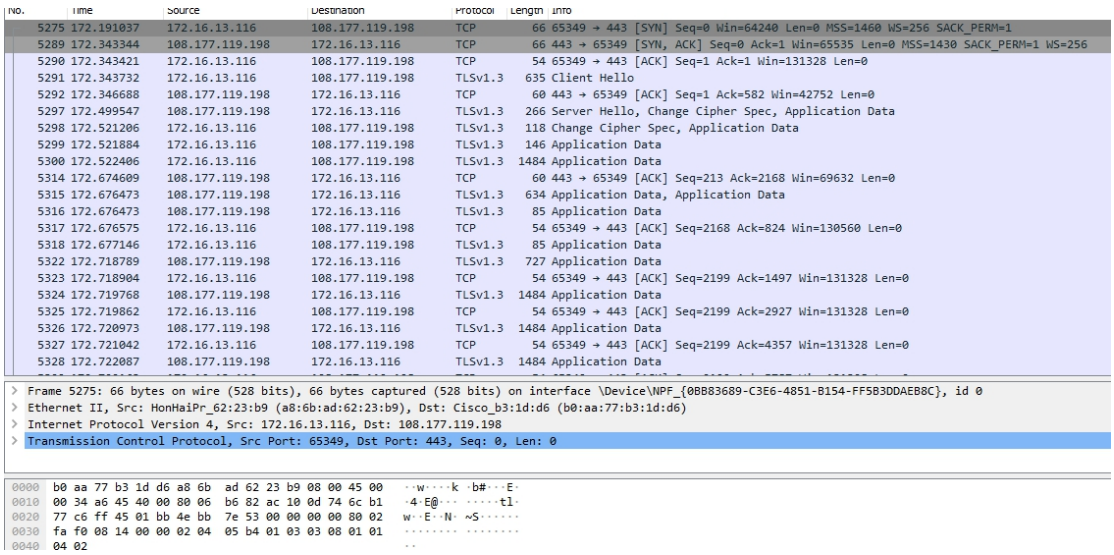
ICMP

• What is the ip addresses of face book and the other host of your choice. Provide only the ip address that you see in the captured packets.

- FACEBOOK:157.240.227.35
- 172.16.0.1:172.16.0.1
- Google:216.58.208.228

• Which protocol is being used by YouTube? And at which layer this protocol runs?

TCP was used by You tube. This protocol runs on transport layer.



No.	Time	Source	Destination	Protocol	Length	Info
5275	172.191037	172.16.13.116	108.177.119.198	TCP	66	65349 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5289	172.343344	108.177.119.198	172.16.13.116	TCP	66	443 → 65349 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
5290	172.343421	172.16.13.116	108.177.119.198	TCP	54	65349 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5291	172.343732	172.16.13.116	108.177.119.198	TLSv1.3	635	Client Hello
5292	172.346688	108.177.119.198	172.16.13.116	TCP	60	443 → 65349 [ACK] Seq=1 Ack=582 Win=42752 Len=0
5297	172.499547	108.177.119.198	172.16.13.116	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Data
5298	172.521206	172.16.13.116	108.177.119.198	TLSv1.3	118	Change Cipher Spec, Application Data
5299	172.521884	172.16.13.116	108.177.119.198	TLSv1.3	146	Application Data
5300	172.522406	172.16.13.116	108.177.119.198	TLSv1.3	1484	Application Data
5314	172.674609	108.177.119.198	172.16.13.116	TCP	60	443 → 65349 [ACK] Seq=213 Ack=2168 Win=69632 Len=0
5315	172.676473	108.177.119.198	172.16.13.116	TLSv1.3	634	Application Data, Application Data
5316	172.676473	108.177.119.198	172.16.13.116	TLSv1.3	85	Application Data
5317	172.676575	172.16.13.116	108.177.119.198	TCP	54	65349 → 443 [ACK] Seq=2168 Ack=824 Win=130560 Len=0
5318	172.677146	172.16.13.116	108.177.119.198	TLSv1.3	85	Application Data
5322	172.718789	108.177.119.198	172.16.13.116	TLSv1.3	727	Application Data
5323	172.718904	172.16.13.116	108.177.119.198	TCP	54	65349 → 443 [ACK] Seq=2199 Ack=1497 Win=131328 Len=0
5324	172.719768	108.177.119.198	172.16.13.116	TLSv1.3	1484	Application Data
5325	172.719862	172.16.13.116	108.177.119.198	TCP	54	65349 → 443 [ACK] Seq=2199 Ack=2927 Win=131328 Len=0
5326	172.720973	108.177.119.198	172.16.13.116	TLSv1.3	1484	Application Data
5327	172.721042	172.16.13.116	108.177.119.198	TCP	54	65349 → 443 [ACK] Seq=2199 Ack=4357 Win=131328 Len=0
5328	172.722087	108.177.119.198	172.16.13.116	TLSv1.3	1484	Application Data

```
> Frame 5275: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{0BB83689-C3E6-4851-B154-FF5B3DDAEB8C}, id 0
> Ethernet II, Src: HonHaiPr_62:23:b9 (a8:6b:ad:62:23:b9), Dst: Cisco_b3:1d:d6 (b0:aa:77:b3:1d:d6)
> Internet Protocol Version 4, Src: 172.16.13.116, Dst: 108.177.119.198
> Transmission Control Protocol, Src Port: 65349, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  b0 aa 77 b3 1d d6 a8 6b  ad 62 23 b9 08 00 45 00   ··w····k ·b#···E·
0010  00 34 a6 45 40 00 80 06  b6 82 ac 10 0d 74 6c b1   ·4·E@··· ·····tl·
0020  77 c6 ff 45 01 bb 4e bb  7e 53 00 00 00 00 80 02   w··E··N· ~S······
0030  fa f0 08 14 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                             ··
```