



**IMRAN KHAN(1802035)**  
**LAB#2**  
**Computer Networks**

## **1. Capture Traffic:**

## **2. Ping the 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

Io.	Time	Source	Destination	Protocol	Length	Info
965	22.871759	204.79.197.222	172.16.13.116	TLSv1.2	123	Application Data
966	22.871823	172.16.13.116	204.79.197.222	TCP	54	65340 → 443 [ACK] Seq=1406 Ack=6745 Win=261632 Len=0
967	22.872636	172.16.13.116	204.79.197.222	TLSv1.2	92	Application Data
968	22.872775	204.79.197.222	172.16.13.116	TLSv1.2	268	Application Data, Application Data
969	22.872775	204.79.197.222	172.16.13.116	TLSv1.2	92	Application Data
970	22.872833	172.16.13.116	204.79.197.222	TCP	54	65340 → 443 [ACK] Seq=1444 Ack=6997 Win=261376 Len=0
973	22.895305	172.67.141.50	172.16.13.116	TCP	66	[TCP Keep-Alive ACK] 443 → 65294 [ACK] Seq=1 Ack=2 Win=69 Len=0 SRE=1 SRE=2
975	22.929222	204.79.197.200	172.16.13.116	TCP	60	443 → 65335 [ACK] Seq=90330 Ack=26101 Win=525312 Len=0
976	22.931891	204.79.197.200	172.16.13.116	TCP	60	443 → 65335 [ACK] Seq=90330 Ack=28981 Win=525568 Len=0
977	22.931891	204.79.197.200	172.16.13.116	TCP	60	443 → 65335 [ACK] Seq=90330 Ack=29260 Win=525312 Len=0
978	22.934784	204.79.197.222	172.16.13.116	TCP	60	443 → 65340 [ACK] Seq=6997 Ack=1444 Win=524032 Len=0
980	23.043292	204.79.197.200	172.16.13.116	TLSv1.2	197	Application Data
981	23.043371	172.16.13.116	204.79.197.200	TCP	54	65335 → 443 [ACK] Seq=29260 Ack=90473 Win=261632 Len=0
1270	33.582454	172.16.13.116	185.199.108.133	TLSv1.2	78	Tensored Unknown Record

> Frame 978: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface '\Device\NPF\_{0BBB83689-C3E6-4851-B154-FF5B3D0AEB8C}', id 0  
> Ethernet II, Src: Cisco\_b3:id:d6 (00:aa:77:b3:id:d6), Dst: HonHaiP\_R\_62:23:b9 (a8:6b:ad:62:23:b9)  
> Internet Protocol Version 4, Src: 204.79.197.222, Dst: 172.16.13.116  
> Transmission Control Protocol, Src Port: 443, Dst Port: 65340, Seq: 6997, Ack: 1444, Len: 0

## 2. UDP

udp						
No.	Time	Source	Destination	Protocol	Length	Info
994	23.259307	fe80::b8e5:1f89:7b4... ff02::fb		MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
996	23.456352	172.16.11.34	224.0.0.251	MDNS	152	Standard query 0x0064 PTR %9E5E7C8F47989526C9BCD95D24
998	23.748084	172.16.11.143	172.16.255.255	NBNS	92	Name query NB WPAD<0>
1812	24.186474	172.16.13.81	255.255.255.255	UDP	150	1025 + 25860 Len=108
1819	24.550390	172.16.11.52	224.0.0.251	MDNS	290	Standard query response 0x0000 PTR, cache flush Android
1820	24.560957	fe80::gae7:c2ff:fe2... ff02::fb		MDNS	310	Standard query response 0x0000 PTR, cache flush Android
1821	24.702524	172.16.11.23	224.0.0.251	MDNS	152	Standard query 0x002e PTR %9E5E7C8F47989526C9BCD95D24
1096	27.107411	172.16.13.81	255.255.255.255	UDP	150	1025 + 25860 Len=108
1101	27.307393	172.16.12.249	224.0.0.251	MDNS	136	Standard query 0x001a PTR %9E5E7C8F47989526C9BCD95D24
1104	27.718784	172.16.12.204	224.0.0.251	MDNS	152	Standard query 0x0004 PTR %9E5E7C8F47989526C9BCD95D24
1121	28.303686	172.16.11.42	224.0.0.251	MDNS	136	Standard query 0x0049 PTR %9E5E7C8F47989526C9BCD95D24
1130	28.851317	172.16.13.116	8.8.8.8	DNS	76	Standard query 0xe5cc A www.facebook.com
1135	29.000246	8.8.8.8	172.16.13.116	DNS	121	Standard query response 0xe5cc A www.facebook.com CNAME
1141	29.205080	172.16.13.142	224.0.0.251	MDNS	136	Standard query 0x001a PTR %9E5E7C8F47989526C9BCD95D24

```

> Frame 1096: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF_{0BB83689-C3E6-4851-B154-FF5B3D
> Ethernet II, Src: 00:e1:25:01:4a:1c (00:e1:25:01:4a:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.16.13.81, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 1025, Dst Port: 25860
> Data (108 bytes)

```

## 3. ICMP

No.	Time	Source	Destination	Protocol	Length	Info
1136	29.018982	172.16.13.116	157.240.227.35	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 1137)
1137	29.067890	157.240.227.35	172.16.13.116	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl=247 (request in 1136)
1161	30.027323	172.16.13.116	157.240.227.35	ICMP	74	Echo (ping) request id=0x0001, seq=42/10752, ttl=128 (reply in 1162)
1162	30.076784	157.240.227.35	172.16.13.116	ICMP	74	Echo (ping) reply id=0x0001, seq=42/10752, ttl=247 (request in 1161)
1195	31.036614	172.16.13.116	157.240.227.35	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 1196)
1196	31.084235	157.240.227.35	172.16.13.116	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=247 (request in 1195)
1227	32.043915	172.16.13.116	157.240.227.35	ICMP	74	Echo (ping) request id=0x0001, seq=44/11264, ttl=128 (reply in 1228)
1228	32.099357	157.240.227.35	172.16.13.116	ICMP	74	Echo (ping) reply id=0x0001, seq=44/11264, ttl=247 (request in 1227)
2070	63.110341	172.16.13.116	172.16.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 2072)
2072	63.115024	172.16.0.1	172.16.13.116	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=128 (request in 2070)
2112	64.115145	172.16.13.116	172.16.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 2113)
2113	64.120854	172.16.0.1	172.16.13.116	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=128 (request in 2112)
2127	65.126061	172.16.13.116	172.16.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 2128)
2128	65.131166	172.16.0.1	172.16.13.116	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=128 (request in 2127)

```

> Frame 1136: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0BB83689-C3E6-4851-B154-FF5B3DAAEB8C}, 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: 157.240.227.35
> Internet Control Message Protocol

```

- 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_{0B883689-C3E6-4851-B154-FF583DDAE8C}, id 0
> Ethernet II, Src: HonHaiP_r_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@ .. ..t1..
0020	77 c6 ff 45 01 bb 4e bb 7e 53 00 00 00 80 02	w..E..N..~S.....
0030	fa f8 08 14 00 00 02 04 05 b4 01 03 03 08 01 01	.....
0040	04 02	..