Name: Aswath S

Reg No: 21BEC2188

Networking Training Program

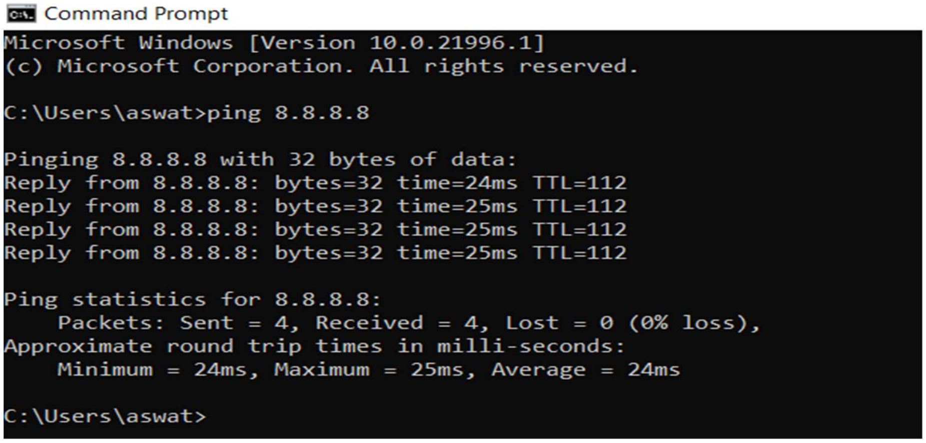
Question-3:

Explore packet filter using wireshark/tcp dump/cisco packet tracer

Using Wireshark :

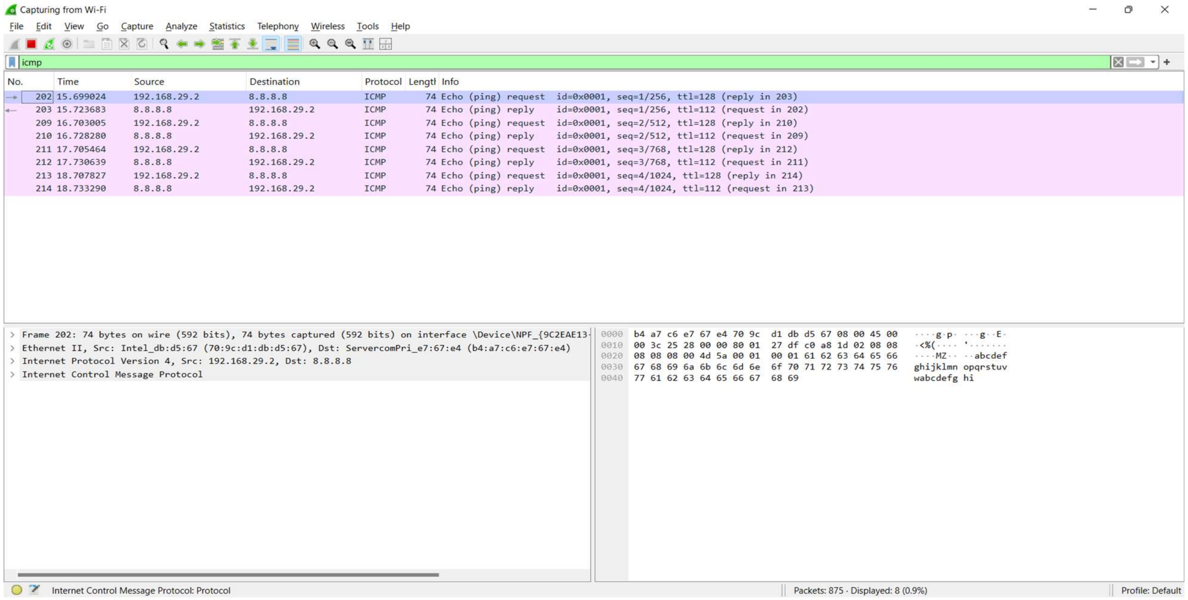
Lets ping a google server (8.8.8.8) ICMP packets in the cmd and in wireshark we can capture the icmp packets.

In cmd:



```
Microsoft Windows [Version 10.0.21996.1]
(c) Microsoft Corporation. All rights reserved.

C:\Users\aswat>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=24ms TTL=112
Reply from 8.8.8.8: bytes=32 time=25ms TTL=112
Reply from 8.8.8.8: bytes=32 time=25ms TTL=112
Reply from 8.8.8.8: bytes=32 time=25ms TTL=112

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 25ms, Average = 24ms

C:\Users\aswat>
```

In wire shark



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

icmp

No.	Time	Source	Destination	Protocol	Lengtl	Info
202	15.699024	192.168.29.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 203)
203	15.723683	8.8.8.8	192.168.29.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=112 (request in 202)
209	16.703005	192.168.29.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 210)
210	16.728280	8.8.8.8	192.168.29.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=112 (request in 209)
211	17.705464	192.168.29.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 212)
212	17.730639	8.8.8.8	192.168.29.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=112 (request in 211)
213	18.707827	192.168.29.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 214)
214	18.733290	8.8.8.8	192.168.29.2	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=112 (request in 213)

```
> Frame 202: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{9C2EAE13-
> Ethernet II, Src: Intel_db:d5:67 (70:9c:d1:db:d5:67), Dst: ServercomPri_e7:67:e4 (b4:a7:c6:e7:67:e4)
> Internet Protocol Version 4, Src: 192.168.29.2, Dst: 8.8.8.8
> Internet Control Message Protocol
```

```
0000  b4 a7 c6 e7 67 e4 70 9c  d1 db d5 67 08 00 45 00   ····g·p· ···g··E·
0010  00 3c 25 28 00 00 80 01  27 df c0 a8 1d 02 08 08   ·<%(···· '·······
0020  08 08 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ····MZ·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Control Message Protocol: Protocol | Packets: 875 · Displayed: 8 (0.9%) | Profile: Default

Using Tcpdump in linux:

```
aswath@aswath-VirtualBox:~$ sudo tcpdump -i enp0s3

tcpdump: verbose output suppressed, use -v[v]... for full protocol decode

listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes

23:14:02.015758 IP 192.168.29.2 > igmp.mcast.net: igmp v3 report, 1 group record(s)

23:14:02.062803 IP6 fe80::b6a7:c6ff:fee7:67e4 > ip6-allnodes: ICMP6, router advertisement,
length 88

23:14:02.063869 IP aswath-VirtualBox.43291 > reliance.reliance.domain: 29203+ PTR?
2.29.168.192.in-addr.arpa. (43)

23:14:02.083062 IP reliance.reliance.domain > aswath-VirtualBox.43291: 29203 NXDomain
0/0/0 (43)

23:14:02.147600 IP reliance.reliance.52535 > aswath-VirtualBox.netbios-ns: UDP, length 50

23:14:02.185107 IP aswath-VirtualBox.42995 > reliance.reliance.domain: 16127+ PTR?
1.29.168.192.in-addr.arpa. (43)

23:14:02.186976 IP reliance.reliance.domain > aswath-VirtualBox.42995: 16127* 1/0/0 PTR
reliance.reliance. (74)

23:14:02.187675 IP aswath-VirtualBox.57329 > reliance.reliance.domain: 14121+ PTR?
92.29.168.192.in-addr.arpa. (44)

23:14:02.189088 IP reliance.reliance.domain > aswath-VirtualBox.57329: 14121 NXDomain
0/0/0 (44)

23:14:02.515883 IP 192.168.29.2 > igmp.mcast.net: igmp v3 report, 1 group record(s)

^C

10 packets captured

10 packets received by filter

0 packets dropped by kernel
```