

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:

```
C:\WINDOWS\system32\cmd.  ×  +  v

C:\Users\Manoj>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=179ms TTL=113
Reply from 8.8.8.8: bytes=32 time=53ms TTL=113
Reply from 8.8.8.8: bytes=32 time=47ms TTL=113
Reply from 8.8.8.8: bytes=32 time=317ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 47ms, Maximum = 317ms, Average = 149ms

C:\Users\Manoj>|
```

Filtering ICMP packets via wireshark:

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
9	20.956103	192.168.76.151	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 10)
10	21.007338	8.8.8.8	192.168.76.151	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=55 (request in 9)
11	21.967332	192.168.76.151	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 12)
12	22.024893	8.8.8.8	192.168.76.151	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=55 (request in 11)
13	22.979358	192.168.76.151	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 14)
14	23.036577	8.8.8.8	192.168.76.151	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=55 (request in 13)
42	23.991596	192.168.76.151	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 43)
43	24.047033	8.8.8.8	192.168.76.151	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=55 (request in 42)

TCP-dump in linux:

sudo tcpdump -i enp0s3

```
manoj@MyLinuxVM: ~  
manoj@MyLinuxVM:~$ 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  
22:22:56.869251 IP6 fe80::71b9:429:dd22:4e79.dhcpv6-client > ff02::1:2.dhcpv6-server: dhcp6 inf-req  
22:22:56.952046 IP MyLinuxVM.34935 > _gateway.domain: 35605+ [1au] PTR? 2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (101)  
22:22:58.157592 IP _gateway.domain > MyLinuxVM.34935: 35605 NXDomain 0/1/1 (165)  
22:22:58.165369 IP MyLinuxVM.38648 > _gateway.domain: 23411+ [1au] PTR? 173.76.168.192.in-addr.arpa. (56)  
22:22:58.202506 IP _gateway.domain > MyLinuxVM.38648: 23411 NXDomain* 0/1/1 (115)  
22:22:58.203994 IP MyLinuxVM.47157 > _gateway.domain: 56111+ [1au] PTR? 43.76.168.192.in-addr.arpa. (55)  
22:22:58.206550 IP _gateway.domain > MyLinuxVM.47157: 56111 NXDomain 0/0/0 (44)  
22:22:58.206998 IP MyLinuxVM.47157 > _gateway.domain: 21088+ PTR? 43.76.168.192.in-addr.arpa. (44)  
22:22:58.209016 IP _gateway.domain > MyLinuxVM.47157: 21088 NXDomain 0/0/0 (44)  
22:23:00.560730 IP MyLinuxVM.45828 > _gateway.domain: 46779+ A? connectivity-check.ubuntu.com. (47)  
22:23:00.602559 IP _gateway.domain > MyLinuxVM.45828: 46779 12/0/0 A 185.125.190.17, A 91.189.91.49, A 185.125.190.96, A 185.125.190.49, A 91.189.91.96, A 185.125.190.97, A 185.125.190.98, A 91.189.91.98, A 185.125.190.48, A 185.125.190.18, A 91.189.91.97, A 91.189.91.48 (239)  
22:23:00.605528 IP MyLinuxVM.40430 > is-content-cache-1.ps5.canonical.com.http: Flags [S], seq 3168824872, win 64240, options [mss 1460,sackOK,TS val 1151953425 ecr 0,nop,wscale 7], length 0  
22:23:00.690251 IP MyLinuxVM.46428 > _gateway.domain: 41678+ PTR? 17.190.125.185.in-addr.arpa. (45)  
22:23:00.824560 IP is-content-cache-1.ps5.canonical.com.http > MyLinuxVM.40430: Flags [S.], seq 2932310768, ack 3168824873, win 65160, options [mss 1370,sackOK,TS val 3158983848 ecr 1151953425,nop,wscale 14], length 0  
22:23:00.824656 IP MyLinuxVM.40430 > is-content-cache-1.ps5.canonical.com.http: Flags [.], ack 1, win 502, options [nop,nop,TS val 1151953644 ecr 3158983848], length 0  
22:23:00.825252 IP MyLinuxVM.40430 > is-content-cache-1.ps5.canonical.com.http: Flags [P.], seq 1:89, ack 1, win 502, options [nop,nop,TS val 1151953644 ecr 3158983848], length 88: HTTP: GET / HTTP/1.1  
22:23:01.436882 IP is-content-cache-1.ps5.canonical.com.http > MyLinuxVM.40430: Flags [P.], seq 1:190, ack 89, win 4, options [nop,nop,TS val 3158984089 ecr 1151953644], length 189: HTTP: HTTP/1.1 204 No Content  
22:23:01.436944 IP MyLinuxVM.40430 > is-content-cache-1.ps5.canonical.com.http: Flags [.], ack 190, win 501, options [nop,nop,TS val 1151954256 ecr 3158984089], length 0  
22:23:01.440144 IP is-content-cache-1.ps5.canonical.com.http > MyLinuxVM.40430: Flags [F.], seq 190, ack 89, win 4, options [nop,nop,TS val 3158984089 ecr 1151953644], length 0  
22:23:01.454146 IP MyLinuxVM.40430 > is-content-cache-1.ps5.canonical.com.http: Flags [F.], seq 89, ack 191, win 501, options [nop,nop,TS val 1151954273 ecr 3158984089], length 0  
22:23:01.545204 IP is-content-cache-1.ps5.canonical.com.http > MyLinuxVM.40430: Flags [F.], seq 190, ack 89, win 4, options [nop,nop,TS val 3158984571 ecr 1151953644], length 0  
22:23:01.545248 IP MyLinuxVM.40430 > is-content-cache-1.ps5.canonical.com.http: Flags [.], ack 191, win 501, options [nop,nop,TS val 1151954364 ecr 3158984571,nop,nop,sack 1 {190:191}], length 0  
22:23:01.740745 IP is-content-cache-1.ps5.canonical.com.http > MyLinuxVM.40430: Flags [.], ack 90, win 4, options [nop,nop,TS val 3158984708 ecr 1151954273], length 0  
22:23:01.742894 IP _gateway.domain > MyLinuxVM.46428: 41678 1/0/0 PTR is-content-cache-1.ps5.canonical.com. (95)  
22:23:03.276944 ARP, Request who-has MyLinuxVM tell _gateway, length 46  
22:23:03.276966 ARP, Reply MyLinuxVM is-at 08:00:27:fb:5a:a7 (oui Unknown), length 28  
22:23:04.304272 ARP, Request who-has 192.168.76.151 tell _gateway, length 46  
22:23:04.329189 IP MyLinuxVM.58432 > _gateway.domain: 50175+ PTR? 151.76.168.192.in-addr.arpa. (45)  
22:23:04.708067 IP _gateway.domain > MyLinuxVM.58432: 50175 NXDomain* 0/1/0 (104)  
^C
```