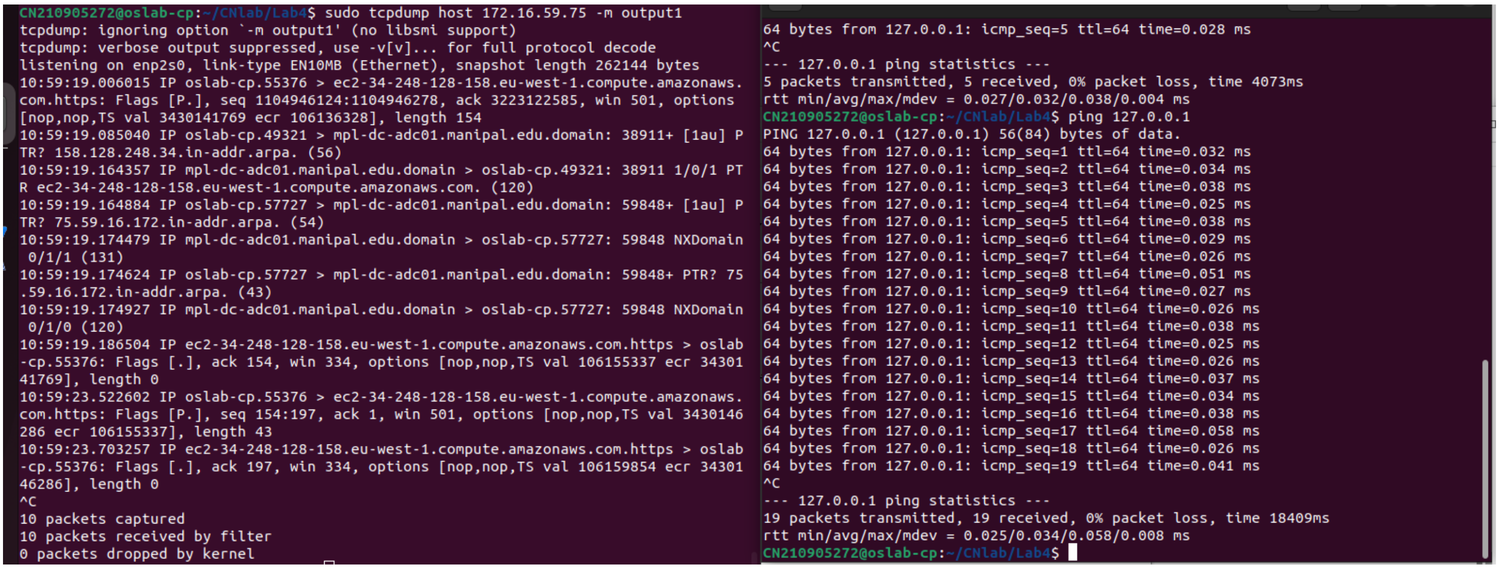
LAB-4>Network Data Analysis using tcpdump

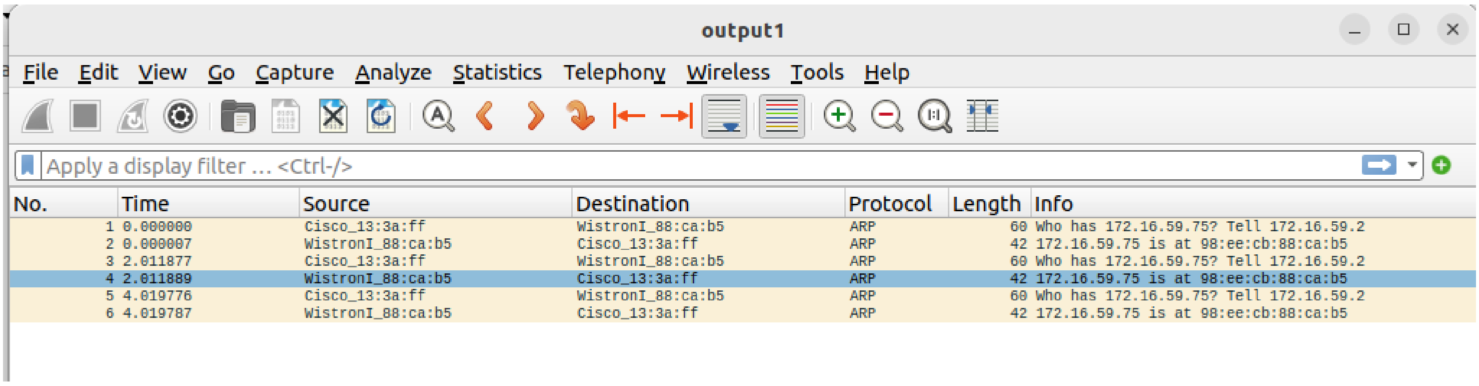
1. While tcpdump host your_host is running in one command window, run ping 127.0.0.1 from another command window. From the ping output, is the 127.0.0.1 interface on? Can you see any ICMP message sent from your host in the tcpdump output? Why?

-> Since, we use ping and it remains in the localhost, we cannot detect it in the tcmp output.



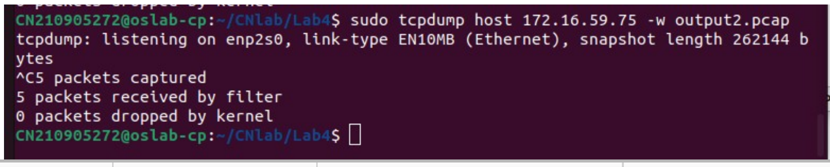
```
CN210905272@oslab-cp:~/CNlab/Lab4$ sudo tcpdump host 172.16.59.75 -m output1
tcpdump: ignoring option `-m output1' (no libsmi support)
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:59:19.006015 IP oslab-cp.55376 > ec2-34-248-128-158.eu-west-1.compute.amazonaws.
com.https: Flags [P.], seq 1104946124:1104946278, ack 3223122585, win 501, options
[nop,nop,TS val 3430141769 ecr 106136328], length 154
10:59:19.085040 IP oslab-cp.49321 > mpl-dc-adc01.manipal.edu.domain: 38911+ [1au] P
TR? 158.128.248.34.in-addr.arpa. (56)
10:59:19.164357 IP mpl-dc-adc01.manipal.edu.domain > oslab-cp.49321: 38911 1/0/1 PT
R ec2-34-248-128-158.eu-west-1.compute.amazonaws.com. (120)
10:59:19.164884 IP oslab-cp.57727 > mpl-dc-adc01.manipal.edu.domain: 59848+ [1au] P
TR? 75.59.16.172.in-addr.arpa. (54)
10:59:19.174479 IP mpl-dc-adc01.manipal.edu.domain > oslab-cp.57727: 59848 NXDomain
 0/1/1 (131)
10:59:19.174624 IP oslab-cp.57727 > mpl-dc-adc01.manipal.edu.domain: 59848+ PTR? 75
.59.16.172.in-addr.arpa. (43)
10:59:19.174927 IP mpl-dc-adc01.manipal.edu.domain > oslab-cp.57727: 59848 NXDomain
 0/1/0 (120)
10:59:19.186504 IP ec2-34-248-128-158.eu-west-1.compute.amazonaws.com.https > oslab
-cp.55376: Flags [.], ack 154, win 334, options [nop,nop,TS val 106155337 ecr 34301
41769], length 0
10:59:23.522602 IP oslab-cp.55376 > ec2-34-248-128-158.eu-west-1.compute.amazonaws.
com.https: Flags [P.], seq 154:197, ack 1, win 501, options [nop,nop,TS val 3430146
286 ecr 106155337], length 43
10:59:23.703257 IP ec2-34-248-128-158.eu-west-1.compute.amazonaws.com.https > oslab
-cp.55376: Flags [.], ack 197, win 334, options [nop,nop,TS val 106159854 ecr 34301
46286], length 0
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

```
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.028 ms
^C
--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4073ms
rtt min/avg/max/mdev = 0.027/0.032/0.038/0.004 ms
CN210905272@oslab-cp:~/CNlab/Lab4$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.034 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.025 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.027 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.025 ms
64 bytes from 127.0.0.1: icmp_seq=13 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=14 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=15 ttl=64 time=0.034 ms
64 bytes from 127.0.0.1: icmp_seq=16 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=17 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=18 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=19 ttl=64 time=0.041 ms
^C
--- 127.0.0.1 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18409ms
rtt min/avg/max/mdev = 0.025/0.034/0.058/0.008 ms
CN210905272@oslab-cp:~/CNlab/Lab4$
```

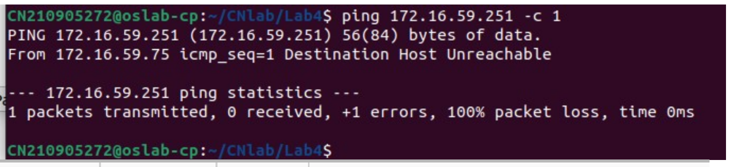

output1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_13:3a:ff	WistronI_88:ca:b5	ARP	60	Who has 172.16.59.75? Tell 172.16.59.2
2	0.000007	WistronI_88:ca:b5	Cisco_13:3a:ff	ARP	42	172.16.59.75 is at 98:ee:cb:88:ca:b5
3	2.011877	Cisco_13:3a:ff	WistronI_88:ca:b5	ARP	60	Who has 172.16.59.75? Tell 172.16.59.2
4	2.011889	WistronI_88:ca:b5	Cisco_13:3a:ff	ARP	42	172.16.59.75 is at 98:ee:cb:88:ca:b5
5	4.019776	Cisco_13:3a:ff	WistronI_88:ca:b5	ARP	60	Who has 172.16.59.75? Tell 172.16.59.2
6	4.019787	WistronI_88:ca:b5	Cisco_13:3a:ff	ARP	42	172.16.59.75 is at 98:ee:cb:88:ca:b5

2. While tcpdump host your_host is running to capture traffic from your machine, execute telnet 128.238.66.200. Note there is no host with this IP address in the current configuration of the lab network. Save the tcpdump output of the first few packets for the lab report. After getting the necessary output, terminate the telnet session. From the saved tcpdump output, describe how the ARP timeout and retransmission were performed. How many attempts were made to resolve a non-existing IP address?



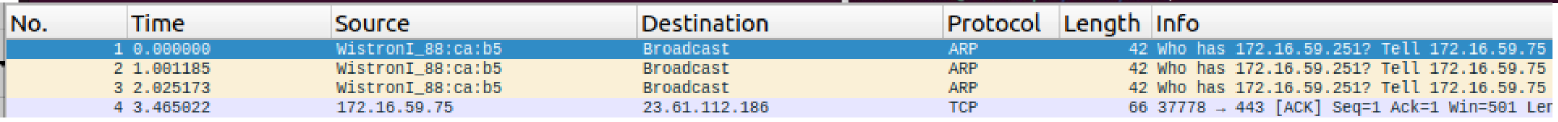
```
CN210905272@oslab-cp:~/CNlab/Lab4$ sudo tcpdump host 172.16.59.75 -w output2.pcap
tcpdump: listening on enp2s0, link-type EN10MB (Ethernet), snapshot length 262144 b
ytes
^C5 packets captured
5 packets received by filter
0 packets dropped by kernel
CN210905272@oslab-cp:~/CNlab/Lab4$ 
```



```
CN210905272@oslab-cp:~/CNlab/Lab4$ ping 172.16.59.251 -c 1
PING 172.16.59.251 (172.16.59.251) 56(84) bytes of data.
From 172.16.59.75 icmp_seq=1 Destination Host Unreachable

--- 172.16.59.251 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

CN210905272@oslab-cp:~/CNlab/Lab4$
```



```
No.    Time        Source              Destination      Protocol  Length Info
     1 0.000000    WistronI_88:ca:b5   Broadcast        ARP           42 Who has 172.16.59.251? Tell 172.16.59.75
     2 1.001185    WistronI_88:ca:b5   Broadcast        ARP           42 Who has 172.16.59.251? Tell 172.16.59.75
     3 2.025173    WistronI_88:ca:b5   Broadcast        ARP           42 Who has 172.16.59.251? Tell 172.16.59.75
     4 3.465022    172.16.59.75        23.61.112.186    TCP           66 37778 → 443 [ACK] Seq=1 Ack=1 Win=501 Ler
```

Ping to non existent ip address 172.16.59.69 . The source makes three attempts to get a response (mac address and other details) from the device at the address.

3. Briefly explain the purposes of the following tcpdump expressions.

a. tcpdump udp port 520

filters output for port 520

b. tcpdump -x -s 120 ip proto 89

c. tcpdump -x -s 70 host ip addr1 and (ip addr2 or ip addr3)

d. tcpdump -x -s 70 host ip addr1 and not ip addr2