

CSCI-651 ASSIGNMENT-1 REPORT

Vibudh Bhardwaj

INTRODUCTION

This report provides a comparison of packet data by the packet sniffer python program and Wireshark. It also shows the effectiveness of filtering commands in isolating specific packet types and traffic conditions.

COMPARISON

Below are screenshots comparing the first and last few packets from Wireshark and packet sniffer python program output.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.50.142	3.128.195.20	TLSv1.2	122	Application Data
2	0.069779	3.128.195.20	192.168.50.142	TCP	66	443 → 54497 [ACK] Seq=1 Ack=57 Win=9 Len=0 TSval=2709848943 TSecr=3358048821
3	0.504830	192.168.50.142	35.223.238.178	TCP	78	56636 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2538614080 TSecr=0 SA..
4	0.550368	35.223.238.178	192.168.50.142	TCP	74	443 → 56636 [SYN, ACK] Seq=0 Ack=1 Win=21120 Len=0 MSS=1420 SACK_PERM TSval=184884..
5	0.550546	192.168.50.142	35.223.238.178	TCP	66	56636 → 443 [ACK] Seq=1 Ack=1 Win=2816 Len=0 TSval=2538614126 TSecr=1848842650
6	0.552509	192.168.50.142	35.223.238.178	TLSv1.3	629	Client Hello (SNI=unleash.codeium.com)
7	0.594983	35.223.238.178	192.168.50.142	TCP	66	443 → 56636 [ACK] Seq=1 Ack=564 Win=20608 Len=0 TSval=1848842694 TSecr=2538614128
8	0.596730	35.223.238.178	192.168.50.142	TLSv1.3	1474	Server Hello, Change Cipher Spec, Application Data

Screenshot-1: First few packets captured by Wireshark

Packet #1 (Wireshark Packet Number)	Packet #3 (Wireshark Packet Number)
Packet size: 122 bytes Ethernet Header: Source MAC: 3e:93:5c:f0:d8:8e Destination MAC: d4:5d:64:dd:4f:e0 EtherType: 0x800	Packet size: 78 bytes Ethernet Header: Source MAC: 3e:93:5c:f0:d8:8e Destination MAC: d4:5d:64:dd:4f:e0 EtherType: 0x800
IP Header: Version: 4 Header Length: 5 Type of Service: 0 Total Length: 108 ID: 0 Flags: DF Fragment Offset: 0 Time to Live: 64 Protocol: 6 Checksum: 32961 Source IP: 192.168.50.142 Destination IP: 3.128.195.20 TCP Header: Source Port: 54497 Destination Port: 443 Sequence Number: 576954588 Acknowledgment Number: 3130253942 Flags: PA	IP Header: Version: 4 Header Length: 5 Type of Service: 0 Total Length: 64 ID: 5 Flags: DF Fragment Offset: 0 Time to Live: 64 Protocol: 6 Checksum: 13552 Source IP: 192.168.50.142 Destination IP: 35.223.238.178 TCP Header: Source Port: 56636 Destination Port: 443 Sequence Number: 853207011 Acknowledgment Number: 0 Flags: S
Packet #2 (Wireshark Packet Number)	Packet #4 (Wireshark Packet Number)
Packet size: 66 bytes Ethernet Header: Source MAC: d4:5d:64:dd:4f:e0 Destination MAC: 3e:93:5c:f0:d8:8e EtherType: 0x800	Packet size: 74 bytes Ethernet Header: Source MAC: d4:5d:64:dd:4f:e0 Destination MAC: 3e:93:5c:f0:d8:8e EtherType: 0x800
IP Header: Version: 4 Header Length: 5 Type of Service: 0 Total Length: 52 ID: 48671 Flags: DF Fragment Offset: 0 Time to Live: 52 Protocol: 6 Checksum: 52953 Source IP: 3.128.195.20 Destination IP: 192.168.50.142 TCP Header: Source Port: 443 Destination Port: 54497 Sequence Number: 3130253942 Acknowledgment Number: 576954644 Flags: A	IP Header: Version: 4 Header Length: 5 Type of Service: 0 Total Length: 60 ID: 0 Flags: DF Fragment Offset: 0 Time to Live: 53 Protocol: 6 Checksum: 16372 Source IP: 35.223.238.178 Destination IP: 192.168.50.142 TCP Header: Source Port: 443 Destination Port: 56636 Sequence Number: 3340113551 Acknowledgment Number: 853207012 Flags: SA

Screenshot-2: First few packets printed by pktsniffer.py

18982	24.291018	132.145.172.253	192.168.50.142	TLSv1.3	125 Application Data
18983	24.291242	192.168.50.142	132.145.172.253	TCP	66 50550 → 443 [ACK] Seq=114599 Ack=8805 Win=131008 Len=0 TSval=2739596547 TSecr=1009..
18984	24.303605	192.168.50.142	17.248.168.195	UDP	87 52734 → 443 Len=45
18985	24.342504	192.168.50.142	132.145.172.253	TLSv1.3	264 Application Data
18986	24.371297	132.145.172.253	192.168.50.142	TLSv1.3	125 Application Data
18987	24.371599	192.168.50.142	132.145.172.253	TCP	66 50550 → 443 [ACK] Seq=114797 Ack=8864 Win=131008 Len=0 TSval=2739596628 TSecr=1009..

Screenshot-3: Last few packets captured by Wireshark

```
Packet #18984 (Wireshark Packet Number)
-----
Packet size: 87 bytes
Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
-----
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 73
ID: 0
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 17
Checksum: 36018
Source IP: 192.168.50.142
Destination IP: 17.248.168.195
UDP Header:
Source Port: 52734
Destination Port: 443
Length: 53
Checksum: 30637

Packet #18985 (Wireshark Packet Number)
-----
Packet size: 264 bytes
Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
-----
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 250
ID: 0
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 6
Checksum: 5433
Source IP: 192.168.50.142
Destination IP: 132.145.172.253
TCP Header:
Source Port: 50550
Destination Port: 443
Sequence Number: 931679229
Acknowledgment Number: 1752454338
Flags: PA

Packet #18986 (Wireshark Packet Number)
-----
Packet size: 125 bytes
Ethernet Header:
Source MAC: d4:5d:64:dd:4f:e0
Destination MAC: 3e:93:5c:f0:d8:8e
EtherType: 0x800
-----
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 111
ID: 45659
Flags: DF
Fragment Offset: 0
Time to Live: 60
Protocol: 6
Checksum: 29832
Source IP: 132.145.172.253
Destination IP: 192.168.50.142
TCP Header:
Source Port: 443
Destination Port: 50550
Sequence Number: 1752454338
Acknowledgment Number: 931679427
Flags: PA

Packet #18987 (Wireshark Packet Number)
-----
Packet size: 66 bytes
Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
-----
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 52
ID: 0
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 6
Checksum: 5631
Source IP: 192.168.50.142
Destination IP: 132.145.172.253
TCP Header:
Source Port: 50550
Destination Port: 443
Sequence Number: 931679427
Acknowledgment Number: 1752454397
Flags: A
```

Screenshot-4: Last few packets printed by pktsniffer.py

FILTER FUNCTIONALITIES DEMONSTRATION

Screenshots below show how filtering commands work. They demonstrate how specific packets are excluded or included when certain flags are used.

HOST FILTERING (-host)

Shows packets filtered by a specific host.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.504830	192.168.50.142	35.223.238.178	TCP	78	56636 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TStamp=2538614080 TSecr=0 SA...
4	0.550368	35.223.238.178	192.168.50.142	TCP	74	443 → 56636 [SYN, ACK] Seq=0 Ack=1 Win=21120 Len=0 MSS=1420 SACK_PERM TStamp=184884...
5	0.550546	192.168.50.142	35.223.238.178	TCP	66	56636 → 443 [ACK] Seq=1 Ack=1 Win=2816 Len=0 TStamp=2538614126 TSecr=1848842650
6	0.552509	192.168.50.142	35.223.238.178	TLSv1.3	629	Client Hello (SNI=unleash.codeium.com)

Screenshot-5: Few Filtered packets sent from or to a specific host using wireshark (35.223.238.178)

Packet #3 (Wireshark Packet Number) Packet size: 78 bytes Ethernet Header: Source MAC: 3e:93:5c:f0:d8:8e Destination MAC: d4:5d:64:dd:4f:e0 EtherType: 0x800 IP Header: Version: 4 Header Length: 5 Type of Service: 0 Total Length: 64 ID: 0 Flags: DF Fragment Offset: 0 Time to Live: 64 Protocol: 6 Checksum: 13852 Source IP: 192.168.50.142 Destination IP: 35.223.238.178 TCP Header: Source Port: 56636 Destination Port: 443 Sequence Number: 853207011 Acknowledgment Number: 0 Flags: S	Packet #5 (Wireshark Packet Number) Packet size: 66 bytes Ethernet Header: Source MAC: 3e:93:5c:f0:d8:8e Destination MAC: d4:5d:64:dd:4f:e0 EtherType: 0x800 IP Header: Version: 4 Header Length: 5 Type of Service: 0 Total Length: 52 ID: 0 Flags: DF Fragment Offset: 0 Time to Live: 64 Protocol: 6 Checksum: 13544 Source IP: 192.168.0.142 Destination IP: 35.223.238.178 TCP Header: Source Port: 56636 Destination Port: 443 Sequence Number: 853207012 Acknowledgment Number: 3340113552 Flags: A
Packet #4 (Wireshark Packet Number) Packet size: 74 bytes Ethernet Header: Source MAC: d4:5d:64:dd:4f:e0 Destination MAC: 3e:93:5c:f0:d8:8e EtherType: 0x800 IP Header: Version: 4 Header Length: 5 Type of Service: 0 Total Length: 60 ID: 0 Flags: DF Fragment Offset: 0 Time to Live: 64 Protocol: 6 Checksum: 16372 Source IP: 35.223.238.178 Destination IP: 192.168.50.142 TCP Header: Source Port: 443 Destination Port: 56636 Sequence Number: 3340113551 Acknowledgment Number: 853207012 Flags: SA	Packet #6 (Wireshark Packet Number) Packet size: 629 bytes Ethernet Header: Source MAC: 3e:93:5c:f0:d8:8e Destination MAC: d4:5d:64:dd:4f:e0 EtherType: 0x800 IP Header: Version: 4 Header Length: 5 Type of Service: 0 Total Length: 615 ID: 0 Flags: DF Fragment Offset: 0 Time to Live: 64 Protocol: 6 Checksum: 13001 Source IP: 192.168.50.142 Destination IP: 35.223.238.178 TCP Header: Source Port: 56636 Destination Port: 443 Sequence Number: 853207012 Acknowledgment Number: 3340113552 Flags: PA

Screenshot-6: Few of the Packets filtered using pktsniffer.py using -host 35.223.238.178 argument

PORT FILTERING (-port)

Shows packets filtered by a specific port number.

No.	Time	Source	Destination	Protocol	Length	Info
3533	4.749654	192.168.50.142	35.223.238.178	TLSv1.2	382	Application Data
3534	4.750297	192.168.50.142	35.223.238.178	TCP	1474	56135 → 443 [ACK] Seq=317 Ack=1 Win=2048 Len=1408 TStamp=144895786 TSecr=438819702 [TCP P...
3535	4.750309	192.168.50.142	35.223.238.178	TLSv1.2	113	Application Data
3555	4.790215	35.223.238.178	192.168.50.142	TCP	66	443 → 56135 [ACK] Seq=1 Ack=1725 Win=163 Len=0 TStamp=438826650 TSecr=144895786

Screenshot-7: Few filtered packets with port number 56135 using Wireshark

```

Packet #3533 (Wireshark Packet Number)
Packet size: 382 bytes
Ethernet Header
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 368
ID: 0
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 6
Checksum: 13248
Source IP: 192.168.50.142
Destination IP: 35.223.238.178
TCP Header:
Source Port: 56136
Destination Port: 443
Sequence Number: 672812594
Acknowledgment Number: 769111095
Flags: PA

Packet #3534 (Wireshark Packet Number)
Packet size: 1474 bytes
Ethernet Header
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 1460
ID: 0
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 6
Checksum: 12156
Source IP: 192.168.50.142
Destination IP: 35.223.238.178
TCP Header:
Source Port: 56136
Destination Port: 443
Sequence Number: 672812910
Acknowledgment Number: 769111095
Flags: A

Packet #3535 (Wireshark Packet Number)
Packet size: 113 bytes
Ethernet Header
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 99
ID: 0
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 6
Checksum: 13517
Source IP: 192.168.50.142
Destination IP: 35.223.238.178
TCP Header:
Source Port: 56136
Destination Port: 443
Sequence Number: 672814318
Acknowledgment Number: 769111095
Flags: PA

Packet #3536 (Wireshark Packet Number)
Packet size: 66 bytes
Ethernet Header
Source MAC: d4:5d:64:dd:4f:e0
Destination MAC: 3e:93:5c:f0:d8:8e
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 52
ID: 6197
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 6
Checksum: 9987
Source IP: 35.223.238.178
Destination IP: 192.168.50.142
TCP Header:
Source Port: 443
Destination Port: 56136
Sequence Number: 769111095
Acknowledgment Number: 672814318
Flags: A

```

Screenshot-8: Few of the Packets filtered using pktsniffer.py using -port 56135 argument

IP-PACKET FILTERING (-ip)

Filters out non-IP packets, leaving only IP traffic

14086	8.490135	23.196.48.62	192.168.50.142	TLSv1.3	97 Application Data
14087	8.490631	192.168.50.142	23.196.48.62	TCP	66 50490 → 443 [ACK] Seq=393805 Ack=4946299 Win=3067584 Len=0 TSval=2248782014 TSecr=...
14088	8.600966	192.168.50.142	35.223.238.178	TCP	54 56558 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
14090	8.624494	192.168.50.142	17.248.168.195	UDP	154 52734 → 443 Len=112

Screenshot-9: Few filtered packets showing IP-traffic using Wireshark (#14089 filtered out)

```

Packet #14086 (Wireshark Packet Number)
Packet size: 97 bytes
Ethernet Header
Source MAC: d4:5d:64:dd:4f:e0
Destination MAC: 3e:93:5c:f0:d8:8e
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 83
ID: 51512
Flags: DF
Fragment Offset: 0
Time to Live: 51
Protocol: 6
Checksum: 17204
Source IP: 23.196.48.62
Destination IP: 192.168.50.142
TCP Header:
Source Port: 443
Destination Port: 50490
Sequence Number: 574874995
Acknowledgment Number: 1134880620
Flags: PA

Packet #14087 (Wireshark Packet Number)
Packet size: 66 bytes
Ethernet Header
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 52
ID: 0
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 6
Checksum: 05439
Source IP: 192.168.50.142
Destination IP: 23.196.48.62
TCP Header:
Source Port: 50490
Destination Port: 443
Sequence Number: 1134880620
Acknowledgment Number: 574875026
Flags: A

Packet #14088 (Wireshark Packet Number)
Packet size: 54 bytes
Ethernet Header
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 40
ID: 9859
Flags:
Fragment Offset: 0
Time to Live: 64
Protocol: 6
Checksum: 20101
Source IP: 192.168.50.142
Destination IP: 35.223.238.178
TCP Header:
Source Port: 56558
Destination Port: 443
Sequence Number: 1798528676
Acknowledgment Number: 2556195458
Flags: A

Packet #14089 (Wireshark Packet Number)
Packet size: 454 bytes
Ethernet Header
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 140
ID: 0
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 17
Checksum: 35951
Source IP: 192.168.50.142
Destination IP: 17.248.168.195
TCP Header:
Source Port: 52734
Destination Port: 443
Length: 120
Checksum: 43820

```

Screenshot-10: Few of the Packets filtered using pktsniffer.py using -ip argument (#14089 filtered out)

TCP PACKET FILTERING (-tcp)

Filters to display only TCP packets.

32 1.065642	192.168.50.142	142.250.190.35	TCP	66 50295 → 443 [ACK] Seq=83 Ack=210 Win=2044 Len=0 TStamp=1474470715 TSecr=3181286566
33 1.065864	192.168.50.142	142.250.190.35	TLSv1.2	105 Application Data
34 1.089179	142.250.190.35	192.168.50.142	TCP	66 443 → 50295 [ACK] Seq=210 Ack=122 Win=1050 Len=0 TStamp=3181286591 TSecr=1474470715
39 1.766684	192.168.50.142	3.130.116.206	TCP	78 50488 → 443 [SYN] Seq=0 Win=65535 Len=64 MSS=1460 WS=64 TStamp=2697664598 TSecr=0 SA...

Screenshot-11: Few filtered packets using TCP as viewed on Wireshark (#35-#38 filtered out)

Packet #32 (Wireshark Packet Number)	Packet #34 (Wireshark Packet Number)
Packet size: 66 bytes	Packet size: 66 bytes
Ethernet Header:	Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e	Source MAC: d4:5d:64:dd:4f:e0
Destination MAC: 3e:93:5c:f0:d8:8e	Destination MAC: 3e:93:5c:f0:d8:8e
EtherType: 0x8000	EtherType: 0x8000
IP Header:	IP Header:
Version: 4	Version: 4
Header Length: 5	Header Length: 5
Type of Service: 0	Type of Service: 0
Total Length: 52	Total Length: 52
ID: 0	ID: 15462
Flags:	Flags:
Fragment Offset: 0	Fragment Offset: 0
Time To Live: 64	Time To Live: 64
Protocol: 6	Protocol: 6
Checksum: 64111	Checksum: 29858
Source IP: 192.168.50.142	Source IP: 142.250.190.35
Destination IP: 142.250.190.35	Destination IP: 192.168.50.142
TCP Header:	TCP Header:
Source Port: 50295	Source Port: 443
Destination Port: 443	Destination Port: 50295
Sequence Number: 1441739231	Sequence Number: 1341634983
Acknowledgment Number: 1441739270	Acknowledgment Number: 1441739270
Flags: A	Flags: A
Packet #33 (Wireshark Packet Number)	Packet #39 (Wireshark Packet Number)
Packet size: 105 bytes	Packet size: 78 bytes
Ethernet Header:	Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e	Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0	Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x8000	EtherType: 0x8000
IP Header:	IP Header:
Version: 4	Version: 4
Header Length: 5	Header Length: 5
Type of Service: 0	Type of Service: 0
Total Length: 91	Total Length: 64
ID: 0	ID: 0
Flags:	Flags:
Fragment Offset: 0	Fragment Offset: 0
Time To Live: 64	Time To Live: 64
Protocol: 6	Protocol: 6
Checksum: 64092	Checksum: 53043
Source IP: 192.168.50.142	Source IP: 192.168.50.142
Destination IP: 142.250.190.35	Destination IP: 3.130.116.206
TCP Header:	TCP Header:
Source Port: 50295	Source Port: 50295
Destination Port: 443	Destination Port: 443
Sequence Number: 1441739231	Sequence Number: 2891508343
Acknowledgment Number: 1441634983	Acknowledgment Number: 0
Flags: PA	Flags: S

Screenshot-12: Few of the Packets filtered using pktsniffer.py using -tcp argument (#35-#38 filtered out)

UDP PACKET FILTERING (-udp)

Filters to display only UDP packets.

No.	Time	Source	Destination	Protocol	Length/Info
35 1.743154	192.168.50.142	192.168.50.1		DNS	95 Standard query 0xd2a1 HTTPS smoot-searchv2-ause2c.v.aaplimg.com
36 1.743219	192.168.50.142	192.168.50.1		DNS	95 Standard query 0x3abd A smoot-searchv2-ause2c.v.aaplimg.com
37 1.763195	192.168.50.1	192.168.50.142		DNS	111 Standard query response 0x3abd A smoot-searchv2-ause2c.v.aaplimg.com A 3.130.116.2...
38 1.763975	192.168.50.1	192.168.50.142		DNS	155 Standard query response 0xd2a1 HTTPS smoot-searchv2-ause2c.v.aaplimg.com SOA a.gsl...

Screenshot-13: Few filtered packets using UDP as viewed on Wireshark

Continued....

```

Packet #35 (Wireshark Packet Number)
-----
Packet size: 95 bytes
Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 81
ID: 46684
Flags:
Fragment Offset: 0
Time to Live: 64
Protocol: 17
Checksum: 62927
Source IP: 192.168.50.142
Destination IP: 192.168.50.1
UDP Header:
Source Port: 56636
Destination Port: 53
Length: 61
Checksum: 54821

Packet #36 (Wireshark Packet Number)
-----
Packet size: 95 bytes
Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 81
ID: 46117
Flags:
Fragment Offset: 0
Time to Live: 64
Protocol: 17
Checksum: 43494
Source IP: 192.168.50.142
Destination IP: 192.168.50.1
UDP Header:
Source Port: 62626
Destination Port: 53
Length: 61
Checksum: 38564

Packet #37 (Wireshark Packet Number)
-----
Packet size: 111 bytes
Ethernet Header:
Source MAC: d4:5d:64:dd:4f:e0
Destination MAC: 3e:93:5c:f0:d8:8e
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 97
ID: 46900
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 17
Checksum: 40311
Source IP: 192.168.50.1
Destination IP: 192.168.50.142
UDP Header:
Source Port: 53
Destination Port: 62626
Length: 77
Checksum: 4298

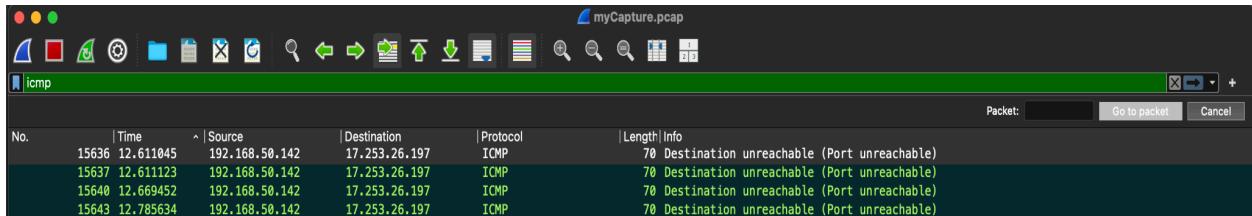
Packet #38 (Wireshark Packet Number)
-----
Packet size: 155 bytes
Ethernet Header:
Source MAC: d4:5d:64:dd:4f:e0
Destination MAC: 3e:93:5c:f0:d8:8e
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 141
ID: 46266
Flags: DF
Fragment Offset: 0
Time to Live: 64
Protocol: 17
Checksum: 40266
Source IP: 192.168.50.1
Destination IP: 192.168.50.142
UDP Header:
Source Port: 53
Destination Port: 56636
Length: 121
Checksum: 16881

```

Screenshot-14: Few of the Packets filtered using pktsniffer.py using `-udp` argument

ICMP PACKET FILTERING (-icmp)

Filters to display on ICMP packets.



Screenshot-15: Few filtered packets using ICMP as viewed on Wireshark

```

Packet #15636 (Wireshark Packet Number)
-----
Packet size: 70 bytes
Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 56
ID: 11887
Flags:
Fragment Offset: 0
Time to Live: 64
Protocol: 1
Checksum: 11358
Source IP: 192.168.50.142
Destination IP: 17.253.26.197
ICMP Header:
Type: 3
Code: 3
Checksum: 11711

Packet #15637 (Wireshark Packet Number)
-----
Packet size: 70 bytes
Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 56
ID: 64330
Flags:
Fragment Offset: 0
Time to Live: 64
Protocol: 1
Checksum: 24450
Source IP: 192.168.50.142
Destination IP: 17.253.26.197
ICMP Header:
Type: 3
Code: 3
Checksum: 11776

Packet #15640 (Wireshark Packet Number)
-----
Packet size: 70 bytes
Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 56
ID: 50777
Flags:
Fragment Offset: 0
Time to Live: 64
Protocol: 1
Checksum: 38003
Source IP: 192.168.50.142
Destination IP: 17.253.26.197
ICMP Header:
Type: 3
Code: 3
Checksum: 11700

Packet #15643 (Wireshark Packet Number)
-----
Packet size: 70 bytes
Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800
IP Header:
Version: 4
Header Length: 5
Type of Service: 0
Total Length: 56
ID: 12735
Flags:
Fragment Offset: 0
Time to Live: 64
Protocol: 1
Checksum: 10810
Source IP: 192.168.50.142
Destination IP: 17.253.26.197
ICMP Header:
Type: 3
Code: 3
Checksum: 11700

```

Screenshot-16: Few of the Packets filtered using pktsniffer.py using `-icmp` argument

NETWORK FILTERING (-net)

Filters packet belonging to a specific subnet.

37	1.763195	192.168.50.1	192.168.50.142	DNS	111 Standard query response 0x3abd A smoot-searchv2-ause2c.v.aaplimg.com A 3.130.116.2...
38	1.763975	192.168.50.1	192.168.50.142	DNS	155 Standard query response 0xd2a1 HTTPS smoot-searchv2-ause2c.v.aaplimg.com SOA a.gsl...
39	1.766684	192.168.50.142	3.130.116.206	TCP	78 50488 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2697664598 TSecr=0 SA...
40	1.792171	3.130.116.206	192.168.50.142	TCP	74 443 → 50488 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM TSval=273780...

Screenshot-17: Few filtered packets to a specific subnet (*ip.addr == 192.168.50.0/24*) as viewed on Wireshark

Packet #37 (Wireshark Packet Number)	Packet #39 (Wireshark Packet Number)
Packet size: 111 bytes	Packet size: 78 bytes
Ethernet Header:	Ethernet Header:
Source MAC: 3e:93:5c:f0:d8:8e	Source MAC: 3e:93:5c:f0:d8:8e
Destination MAC: d4:5d:64:dd:4f:e0	Destination MAC: d4:5d:64:dd:4f:e0
EtherType: 0x800	EtherType: 0x800
IP Header:	IP Header:
Version: 4	Version: 4
Header Length: 5	Header Length: 5
Type of Service: 0	Type of Service: 0
Total Length: 97	Total Length: 64
ID: 46900	ID: 0
Flags: DF	Flags: DF
Fragment Offset: 0	Fragment Offset: 0
Time to Live: 64	Time to Live: 64
Protocol: 17	Protocol: 6
Checksum: 40311	Checksum: 53041
Source IP: 192.168.50.1	Source IP: 192.168.50.142
Destination IP: 192.168.50.142	Destination IP: 3.130.116.206
UDP Header:	TCP Header:
Source Port: 53	Source Port: 50488
Destination Port: 62626	Destination Port: 443
Length: 77	Sequence Number: 2891508343
Checksum: 4298	Acknowledgment Number: 0
Flags: S	Flags: S
Packet #38 (Wireshark Packet Number)	Packet #40 (Wireshark Packet Number)
Packet size: 158 bytes	Packet size: 74 bytes
Ethernet Header:	Ethernet Header:
Source MAC: d4:5d:64:dd:4f:e0	Source MAC: d4:5d:64:dd:4f:e0
Destination MAC: 3e:93:5c:f0:d8:8e	Destination MAC: 3e:93:5c:f0:d8:8e
EtherType: 0x800	EtherType: 0x800
IP Header:	IP Header:
Version: 4	Version: 4
Header Length: 5	Header Length: 5
Type of Service: 0	Type of Service: 0
Total Length: 141	Total Length: 60
ID: 46901	ID: 0
Flags: DF	Flags: DF
Fragment Offset: 0	Fragment Offset: 0
Time to Live: 64	Time to Live: 243
Protocol: 17	Protocol: 6
Checksum: 40266	Checksum: 7224
Source IP: 192.168.50.1	Source IP: 3.130.116.206
Destination IP: 192.168.50.142	Destination IP: 192.168.50.142
UDP Header:	TCP Header:
Source Port: 53	Source Port: 443
Destination Port: 56636	Destination Port: 50488
Length: 121	Sequence Number: 3800904226
Checksum: 16881	Acknowledgment Number: 2891508344
Flags: SA	Flags: SA

Screenshot-18: Few of the Packets filtered using `pktsniffer.py` using `-net 192.168.50.0` argument

CONCLUSION

This report demonstrates that the packet sniffer program correctly captures and filters packets in a manner consistent with Wireshark. The filtering commands effectively isolate specific types of traffic, showing the program's correctness and usability.