Packet Analyzer Report

Cedric Bone

Contents

1 Introduction

2 Description
- 2.1 Command-line Arguments . . . . .
- 2.2 Comparison with Wireshark . . . . .
- 2.3 Comparison Screenshots (First Few Packets) . . . . .
- 2.4 Comparison Screenshots (Last Few Packets) . . . . .

3 Filter Demonstrations
- 3.1 Host Filter . . . . .
- 3.2 Port Filter . . . . .
- 3.3 IP Filter . . . . .
- 3.4 TCP Filter . . . . .
- 3.5 UDP Filter . . . . .
- 3.6 ICMP Filter . . . . .
- 3.7 Network Filter . . . . .

4 Conclusion

1 Introduction

This report summarizes the functionality of pktsniffer.py. The goal was to capture network traffic using Wireshark, parse the captured packets, and then display a breakdown of the packet headers.

2 Description

pktsniffer.py reads packets from a specified .pcap file. It then processes each packet to retrieve Ethernet, IP, and TCP/UDP/ICMP headers.

2.1 Command-line Arguments

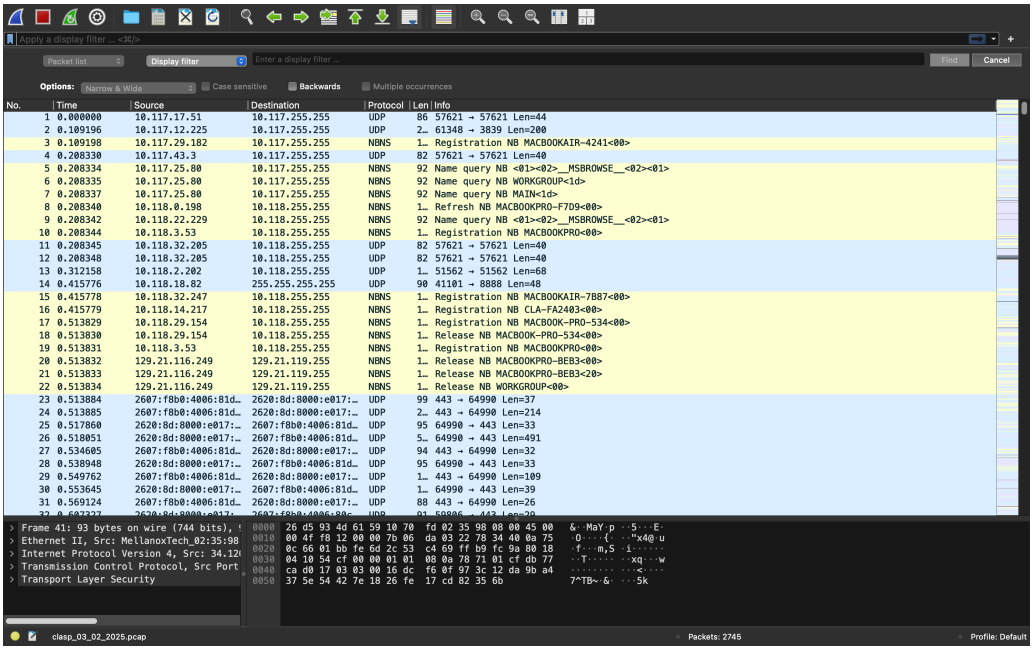
Below is a summary of the main command-line arguments:

- `-r` : Path to the pcap file (required).
- `-c` : Limit the number of packets analyzed (optional).
- `-host` : Filter by host (source IP).
- `-port` : Filter by source/destination port.
- `-ip` : Filter by IP address (source or destination).
- `-tcp` : Filter TCP packets.
- `-udp` : Filter UDP packets.
- `-icmp` : Filter ICMP packets.
- `-net` : Filter by a substring that matches a network prefix.

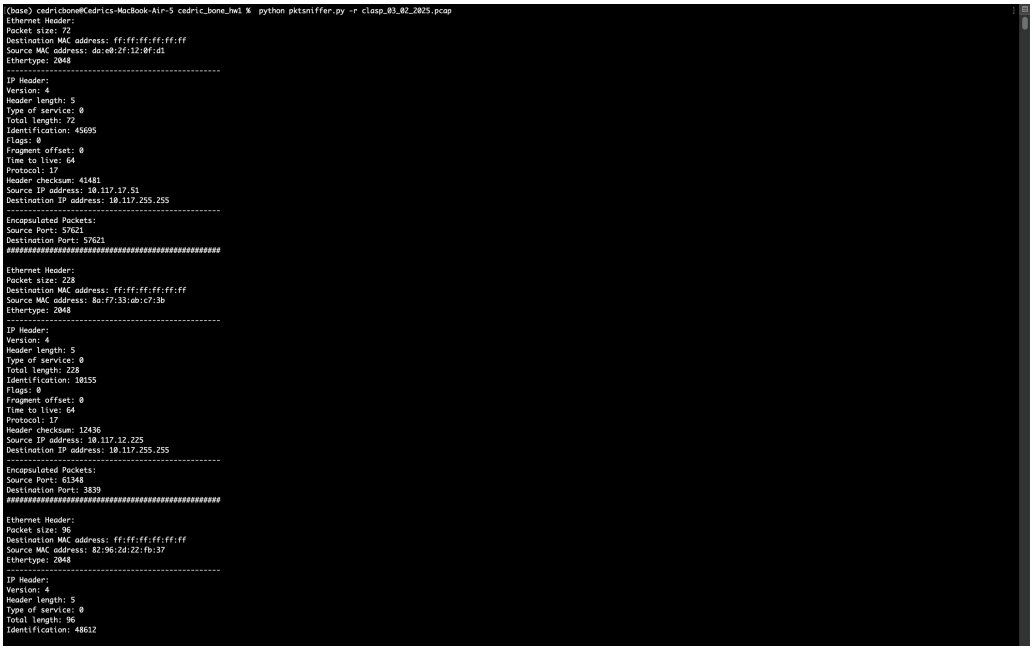
2.2 Comparison with Wireshark

Network traffic was captured using Wireshark and saved to clasp_03_02_2025.pcap. Below are screenshots comparing packets in Wireshark versus pktsniffer.py.

2.3 Comparison Screenshots (First Few Packets)



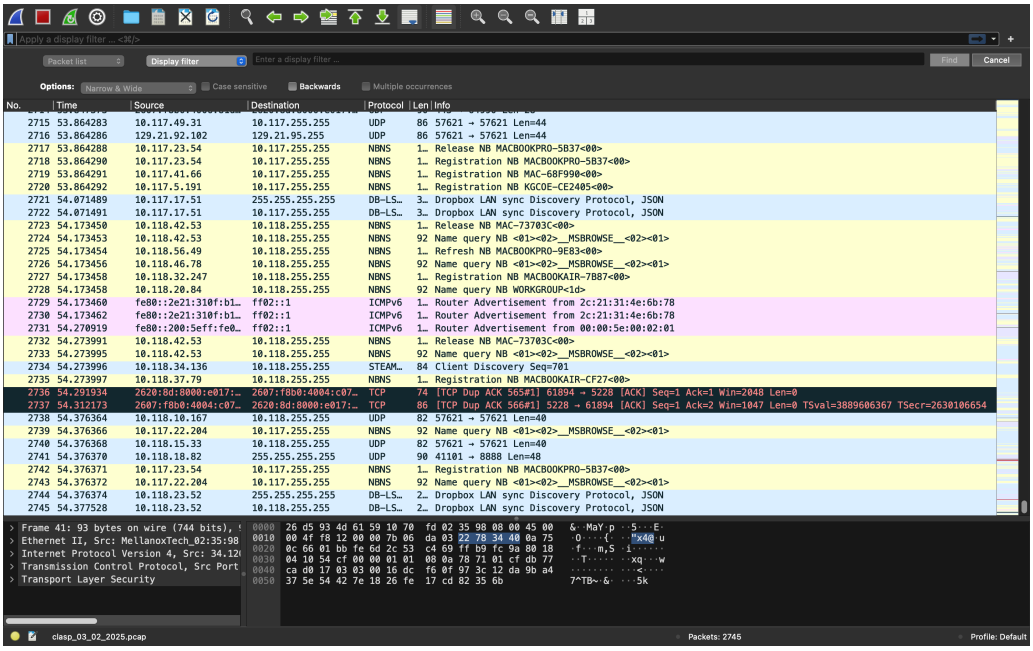
(a) Wireshark



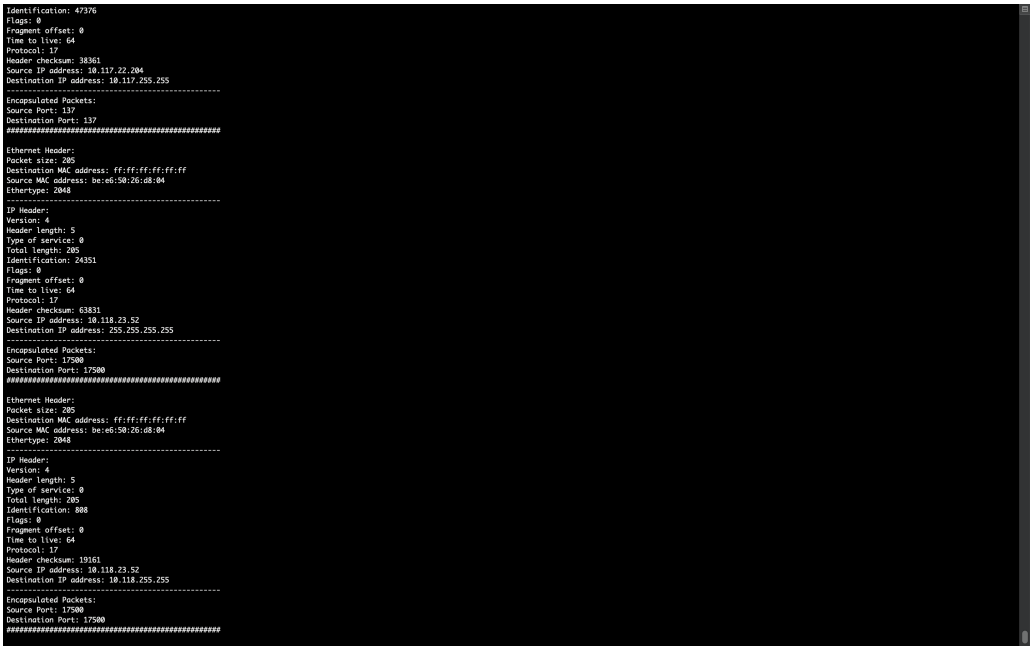
(b) pktsniffer

Figure 1: Wireshark vs. pktsniffer (first few packets).

2.4 Comparison Screenshots (Last Few Packets)



(a) Wireshark



(b) pktsniffer

Figure 2: Wireshark vs. pktsniffer (last few packets).

3 Filter Demonstrations

Tested filter flags to ensure correct functionality.

3.1 Host Filter

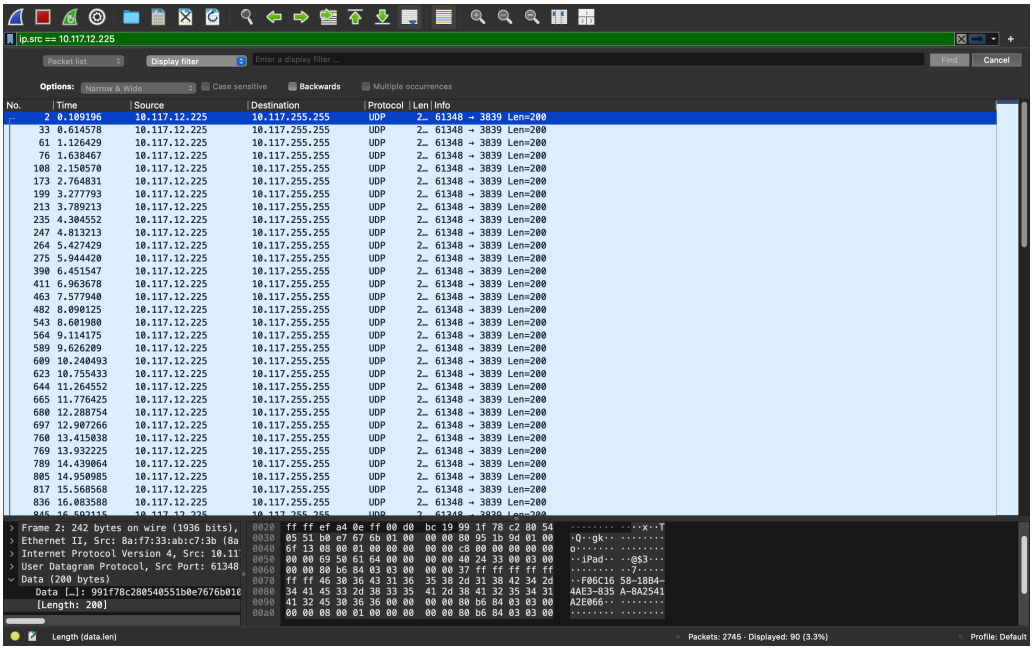
Only packets from 10.117.12.225 are shown.

pktsniffer command:

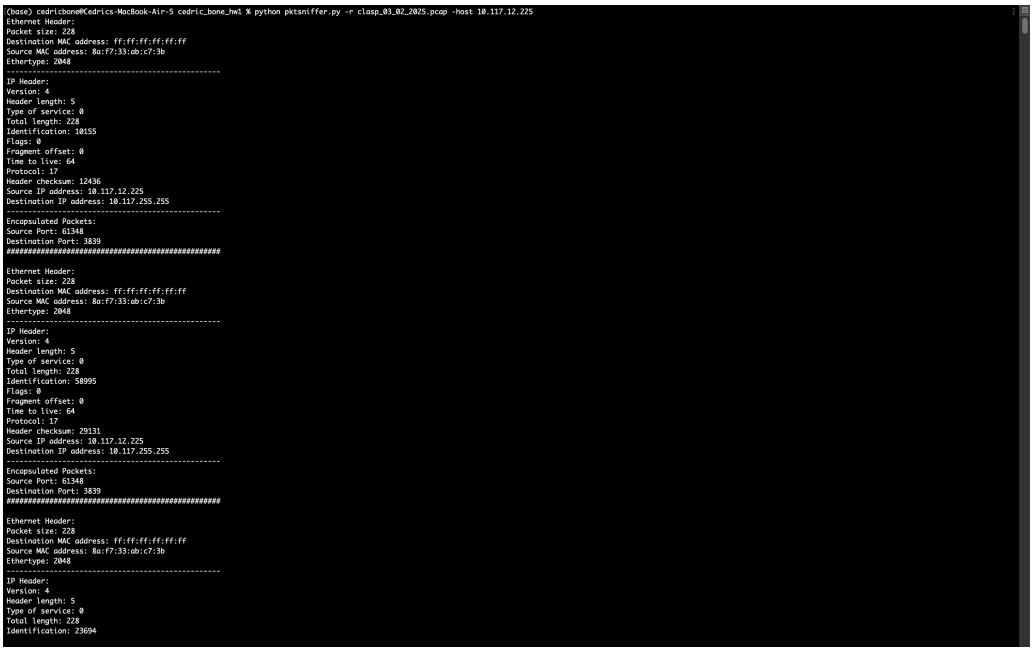
```
python pktsniffer.py -r clasp_03_02_2025.pcap -host 10.117.12.225
```

Wireshark filter:

```
ip.src == 10.117.12.225
```



(a) Wireshark Host Filter



(b) pktsniffer Host Filter

Figure 3: Host filter demonstration.

3.2 Port Filter

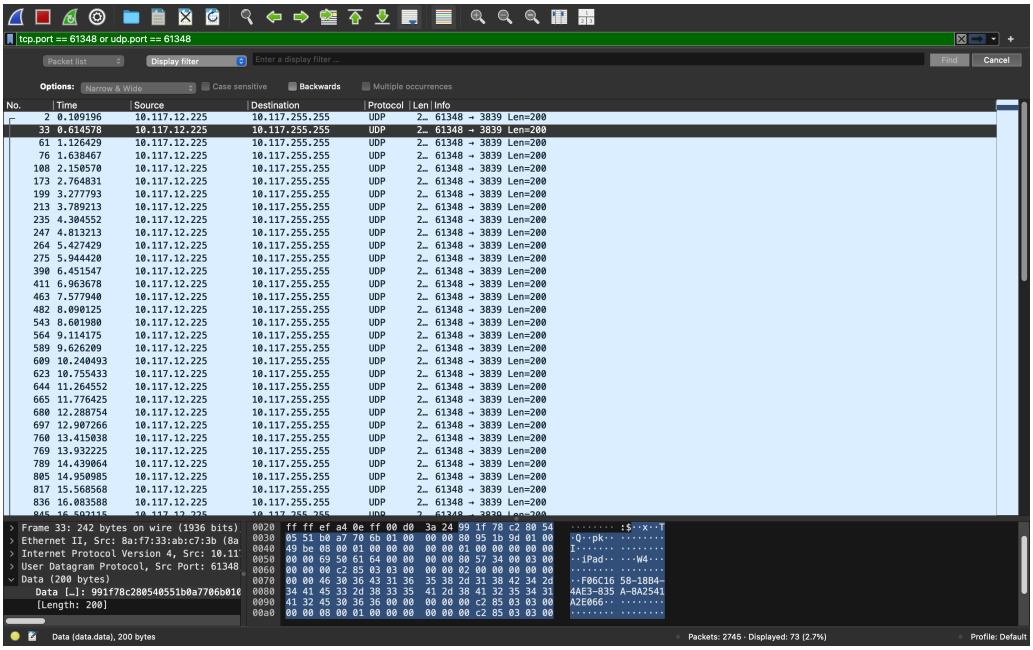
Only packets on port 61348 are shown.

pktsniffer command:

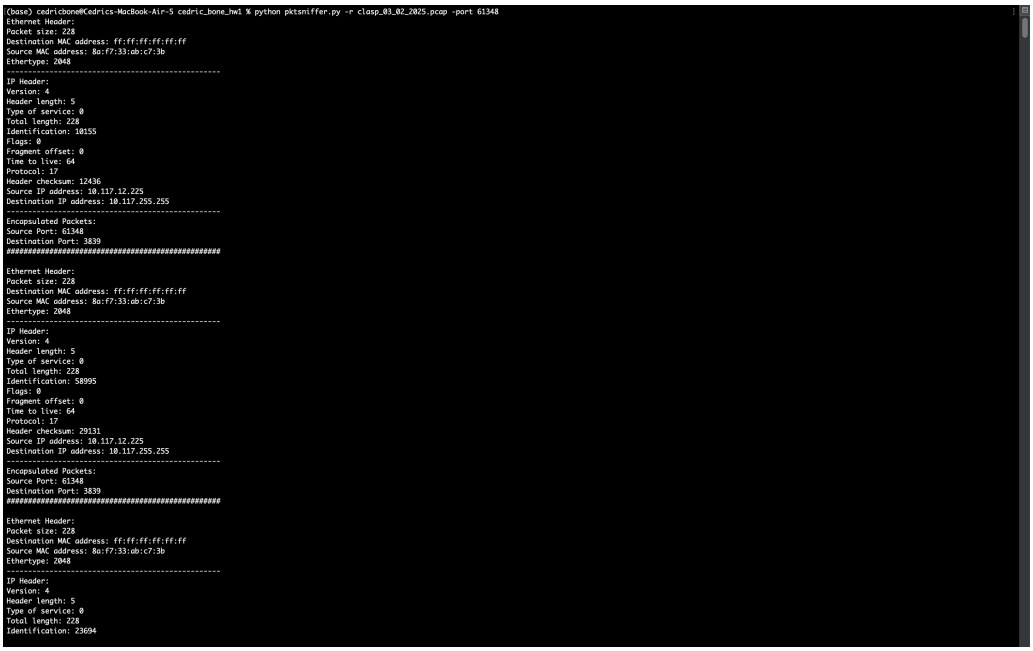
```
python pktsniffer.py -r clasp_03_02_2025.pcap -port 61348
```

Wireshark filter:

```
tcp.port == 61348 or udp.port == 61348
```



(a) Wireshark Port Filter



(b) pktsniffer Port Filter

Figure 4: Port filter demonstration.

3.3 IP Filter

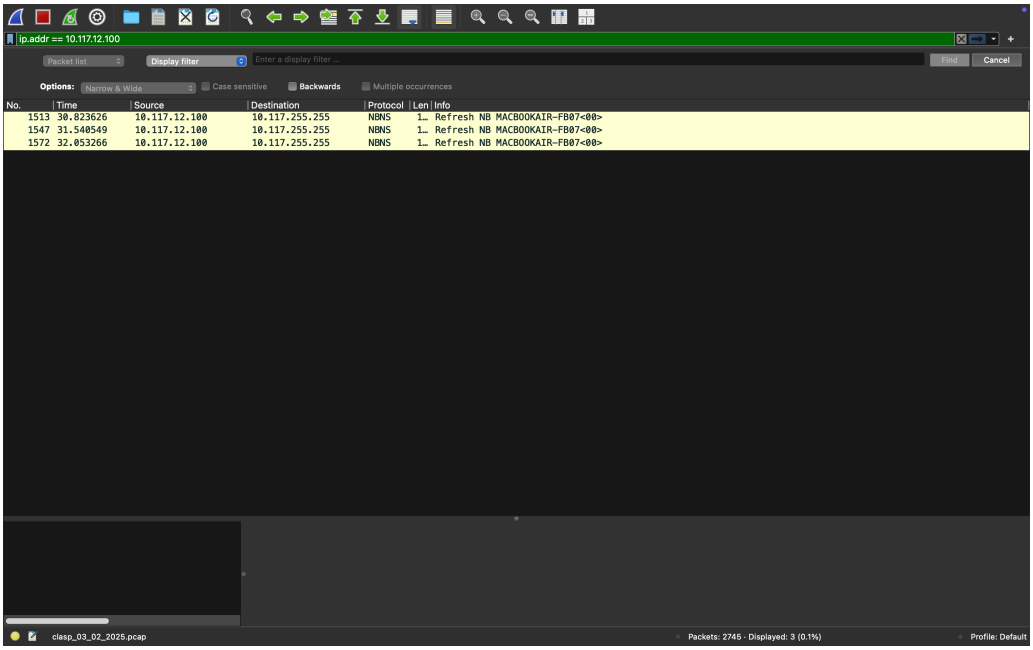
Shows all packets where the source or destination IP is 10.117.12.100.

pktsniffer command:

```
python pktsniffer.py -r clasp_03_02_2025.pcap -ip 10.117.12.100
```

Wireshark filter:

```
ip.addr == 10.117.12.100
```



(a) Wireshark IP Filter

(b) pktsniffer IP Filter

Figure 5: IP filter demonstration.

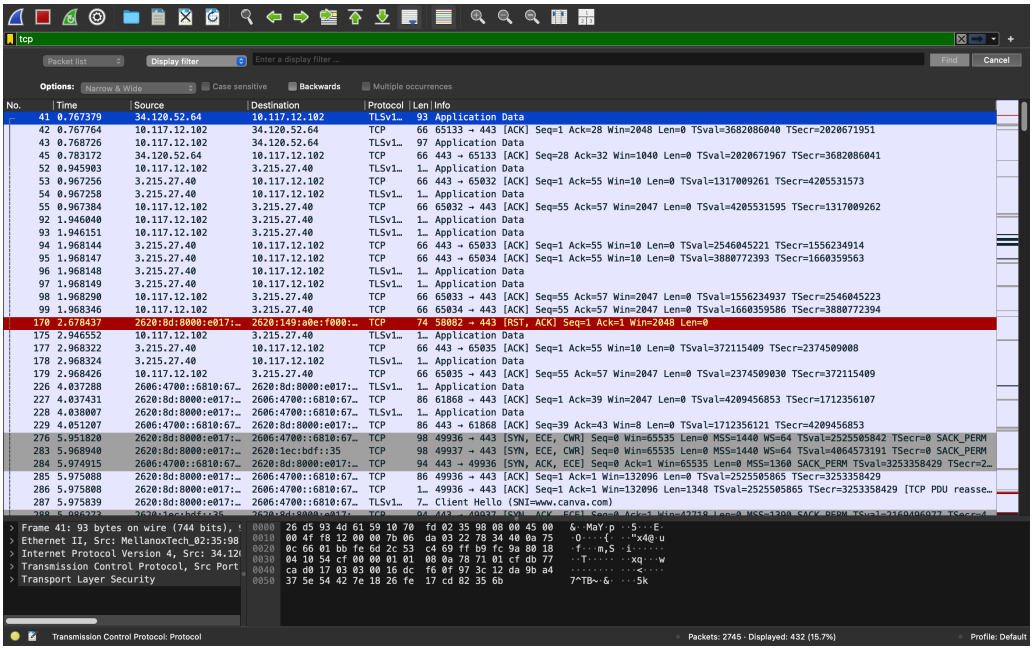
3.4 TCP Filter

Filter only TCP packets.

```
python pktsniffer.py -r clasp_03_02_2025.pcap -tcp
```

Wireshark filter:

```
tcp
```



(a) Wireshark TCP Filter

(b) pktsniffer TCP Filter

Figure 6: TCP filter demonstration.

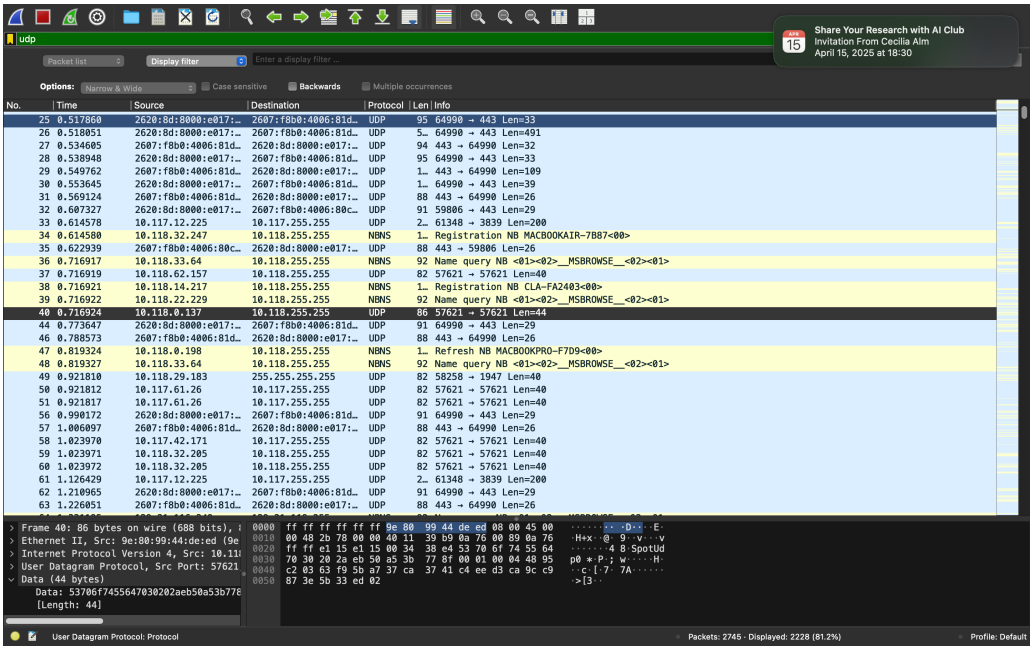
3.5 UDP Filter

Filter only UDP packets.

```
python pktsniffer.py -r clasp_03_02_2025.pcap -udp
```

Wireshark filter:

```
udp
```



(a) Wireshark UDP Filter

(b) pktsniffer UDP Filter

Figure 7: UDP filter demonstration.

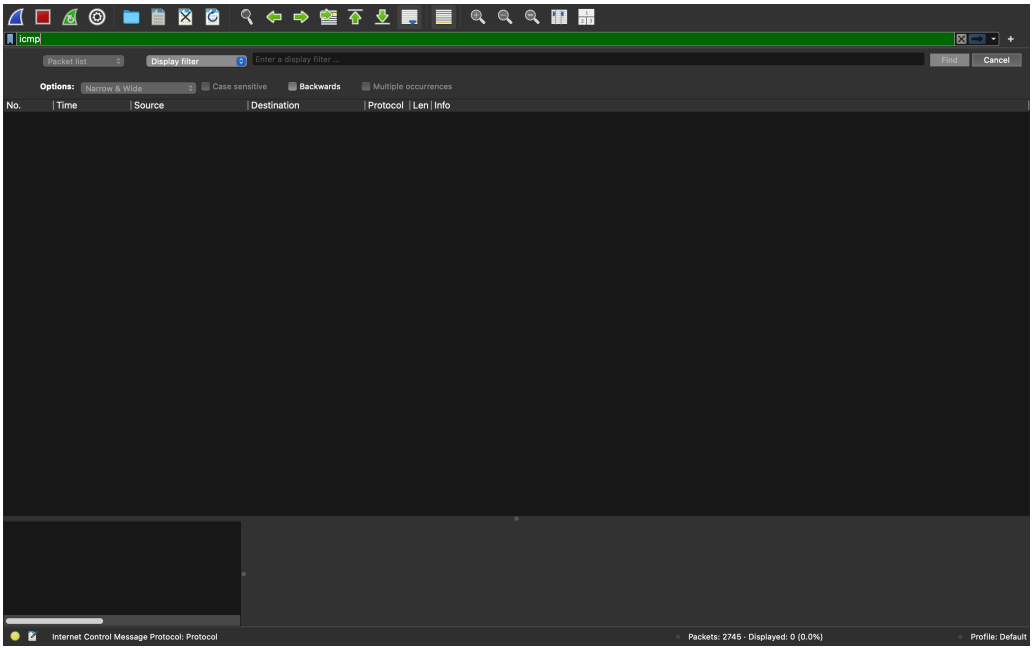
3.6 ICMP Filter

Filter only ICMP packets.

```
python pktsniffer.py -r clasp_03_02_2025.pcap -icmp
```

Wireshark filter:

```
icmp
```



(a) Wireshark ICMP Filter

(b) pktsniffer ICMP Filter

Figure 8: ICMP filter demonstration.

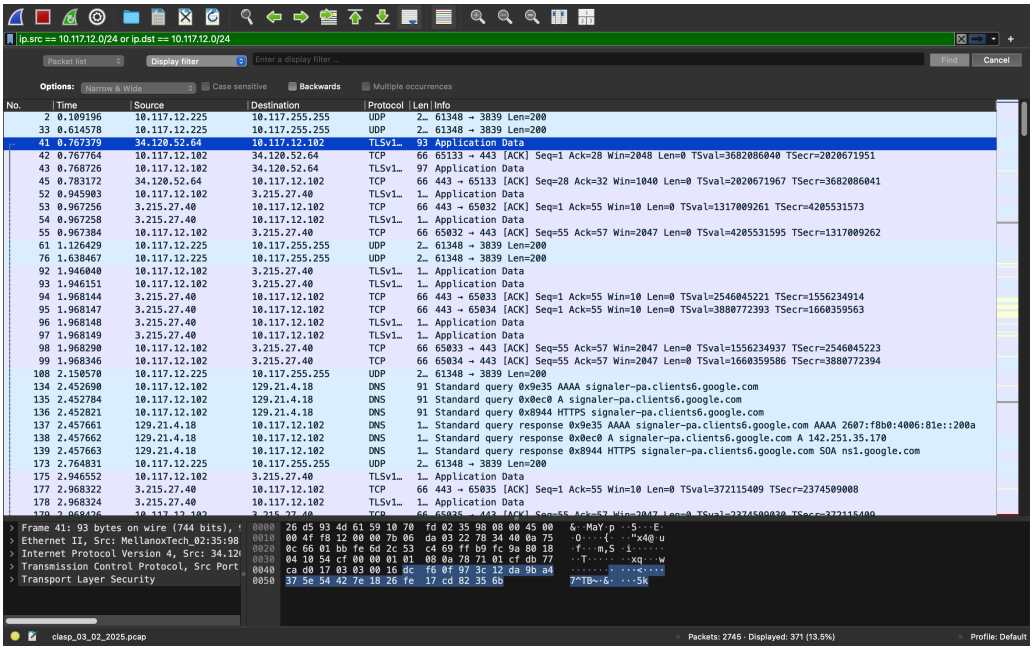
3.7 Network Filter

Packets where the source or destination IP contains 10.117.12.

```
python pktsniffer.py -r clasp_03_02_2025.pcap -net 10.117.12
```

Wireshark filter:

```
ip.src == 10.117.12.0/24 or ip.dst == 10.117.12.0/24
```



(a) Wireshark Net Filter

(b) pktsniffer Net Filter

Figure 9: Network filter demonstration.

4 Conclusion

pktsniffer.py reads from a .pcap file and provides a summary of each packet's Ethernet, IP, and TCP/UDP/ICMP headers. The filters allow subsets of the packets. Comparisons with Wireshark confirm that the program displays accurate header information.