Packet Sniffer Report

Name: Samyak Rajesh Shah
Email: ss4604@rit.edu

1. Introduction

The goal of this assignment was to implement a packet sniffer in Python that reads packets from a .pcap file and prints a human-readable summary. The program supports filtering packets by host IP, destination IP, network (CIDR), TCP/UDP/ICMP protocols, and ports. The captured packet information includes Ethernet, IP, and transport layer headers.

2. Environment and Setup

- **Python Version:** 3.7+
- **Dependencies:** PyShark (pyshark==0.6)
- **OS:** Windows 11

Installation:

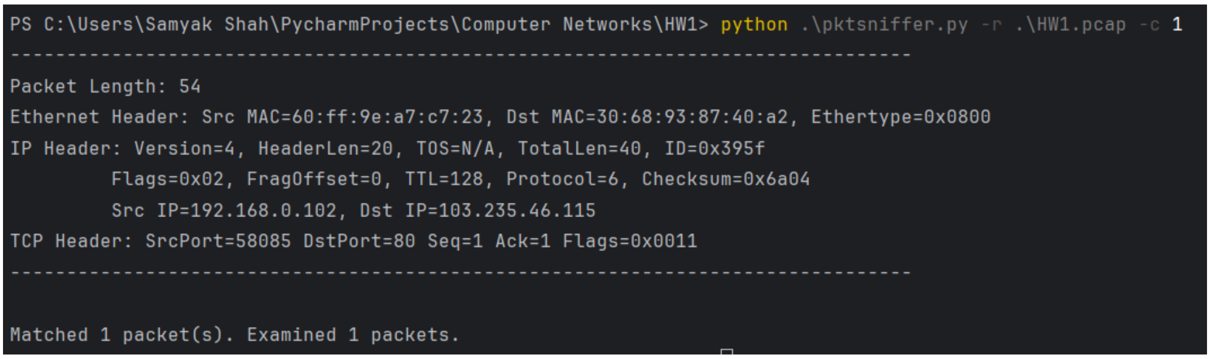
pip install -r requirements.txt

3. Packet Capture Output Comparison

3.1 First Few Packets

Description: Comparison between the first few packets from the program output and Wireshark.

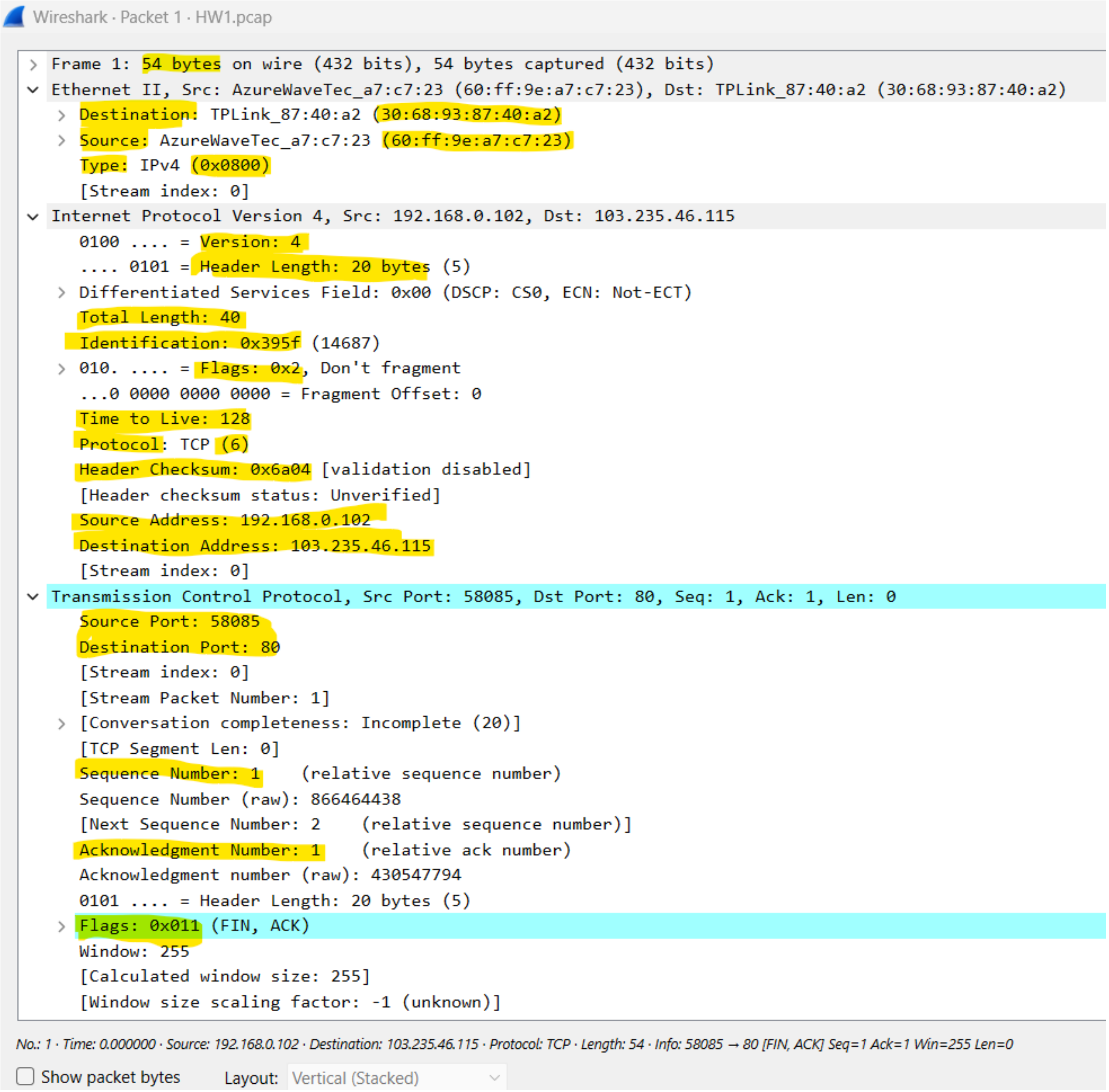
Program Output Screenshot:



```
PS C:\Users\Samyak Shah\PycharmProjects\Computer Networks\HW1> python .\pktsniffer.py -r .\HW1.pcap -c 1
--------------------------------------------------------------------------------
Packet Length: 54
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=40, ID=0x395f
         Flags=0x02, FragOffset=0, TTL=128, Protocol=6, Checksum=0x6a04
         Src IP=192.168.0.102, Dst IP=103.235.46.115
TCP Header: SrcPort=58085 DstPort=80 Seq=1 Ack=1 Flags=0x0011
--------------------------------------------------------------------------------


Matched 1 packet(s). Examined 1 packets.
```

Wireshark Screenshot:



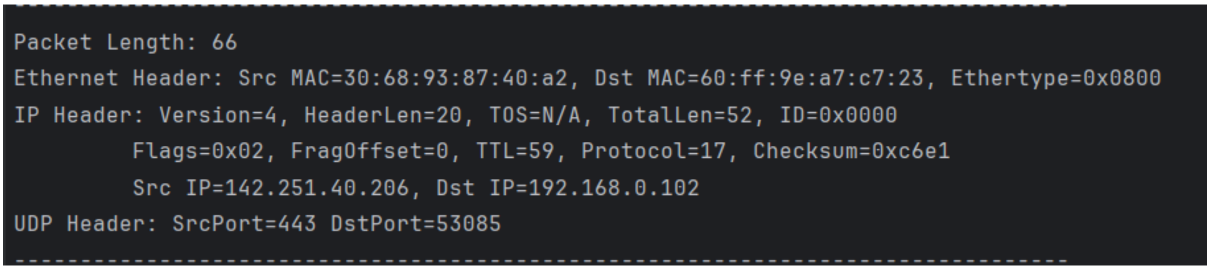
```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
v Ethernet II, Src: AzureWaveTec_a7:c7:23 (60:ff:9e:a7:c7:23), Dst: TPLink_87:40:a2 (30:68:93:87:40:a2)
  > Destination: TPLink_87:40:a2 (30:68:93:87:40:a2)
  > Source: AzureWaveTec_a7:c7:23 (60:ff:9e:a7:c7:23)
    Type: IPv4 (0x0800)
    [Stream index: 0]
v Internet Protocol Version 4, Src: 192.168.0.102, Dst: 103.235.46.115
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x395f (14687)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x6a04 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.102
    Destination Address: 103.235.46.115
    [Stream index: 0]
v Transmission Control Protocol, Src Port: 58085, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 58085
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 1]
  > [Conversation completeness: Incomplete (20)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 866464438
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 430547794
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x011 (FIN, ACK)
    Window: 255
    [Calculated window size: 255]
    [Window size scaling factor: -1 (unknown)]
```

No.: 1 · Time: 0.000000 · Source: 192.168.0.102 · Destination: 103.235.46.115 · Protocol: TCP · Length: 54 · Info: 58085 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0

3.2 Last Few Packets

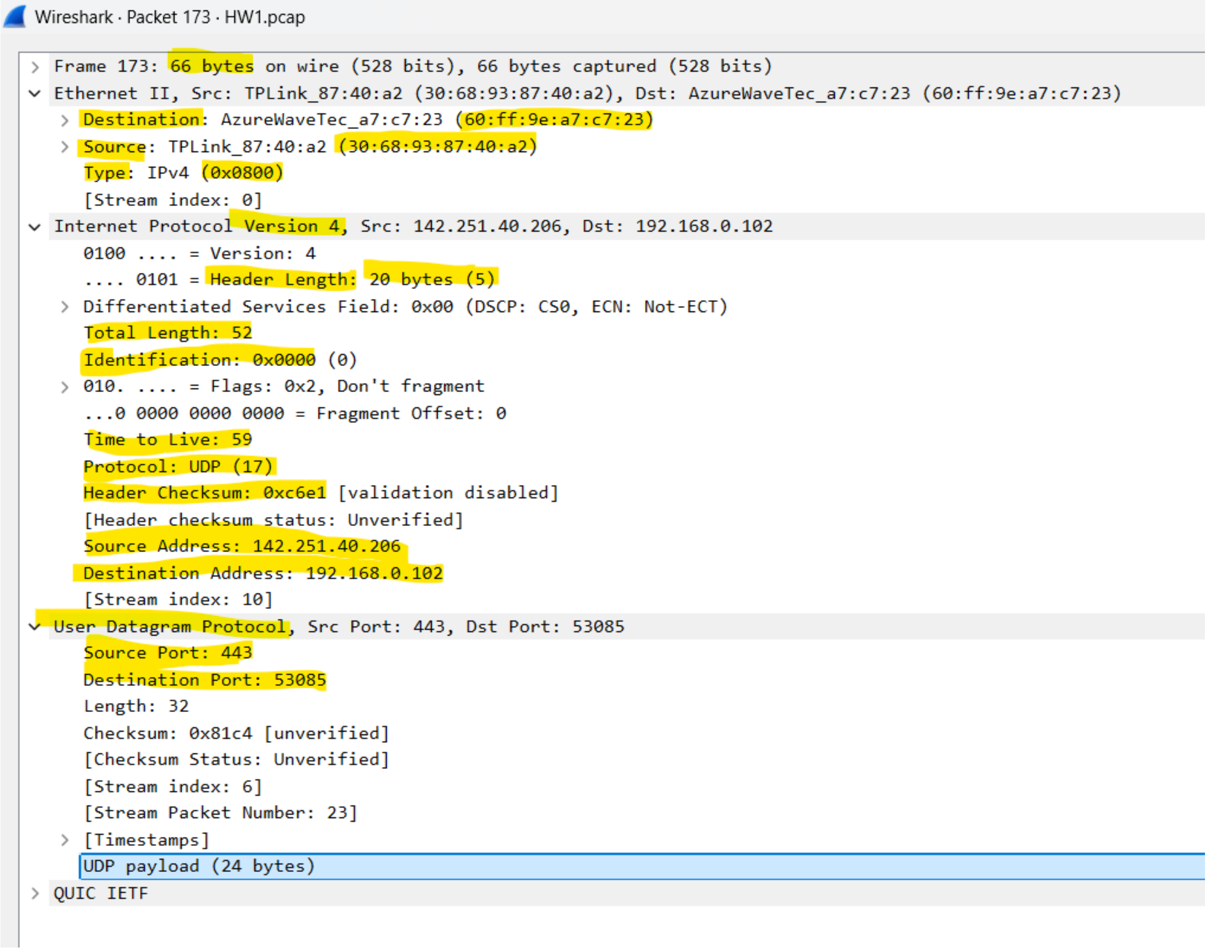
Description: Comparison between the last few packets from the program output and Wireshark.

Program Output Screenshot:



```
--------------------------------------------------------------------------------
Packet Length: 66
Ethernet Header: Src MAC=30:68:93:87:40:a2, Dst MAC=60:ff:9e:a7:c7:23, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=52, ID=0x0000
         Flags=0x02, FragOffset=0, TTL=59, Protocol=17, Checksum=0xc6e1
         Src IP=142.251.40.206, Dst IP=192.168.0.102
UDP Header: SrcPort=443 DstPort=53085
--------------------------------------------------------------------------------
```

Wireshark Screenshot:



```
> Frame 173: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
v Ethernet II, Src: TPLink_87:40:a2 (30:68:93:87:40:a2), Dst: AzureWaveTec_a7:c7:23 (60:ff:9e:a7:c7:23)
  > Destination: AzureWaveTec_a7:c7:23 (60:ff:9e:a7:c7:23)
  > Source: TPLink_87:40:a2 (30:68:93:87:40:a2)
    Type: IPv4 (0x0800)
    [Stream index: 0]
v Internet Protocol Version 4, Src: 142.251.40.206, Dst: 192.168.0.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 59
    Protocol: UDP (17)
    Header Checksum: 0xc6e1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 142.251.40.206
    Destination Address: 192.168.0.102
    [Stream index: 10]
v User Datagram Protocol, Src Port: 443, Dst Port: 53085
    Source Port: 443
    Destination Port: 53085
    Length: 32
    Checksum: 0x81c4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
    [Stream Packet Number: 23]
  > [Timestamps]
    UDP payload (24 bytes)
> QUIC IETF
```

4. Filtering Functionality

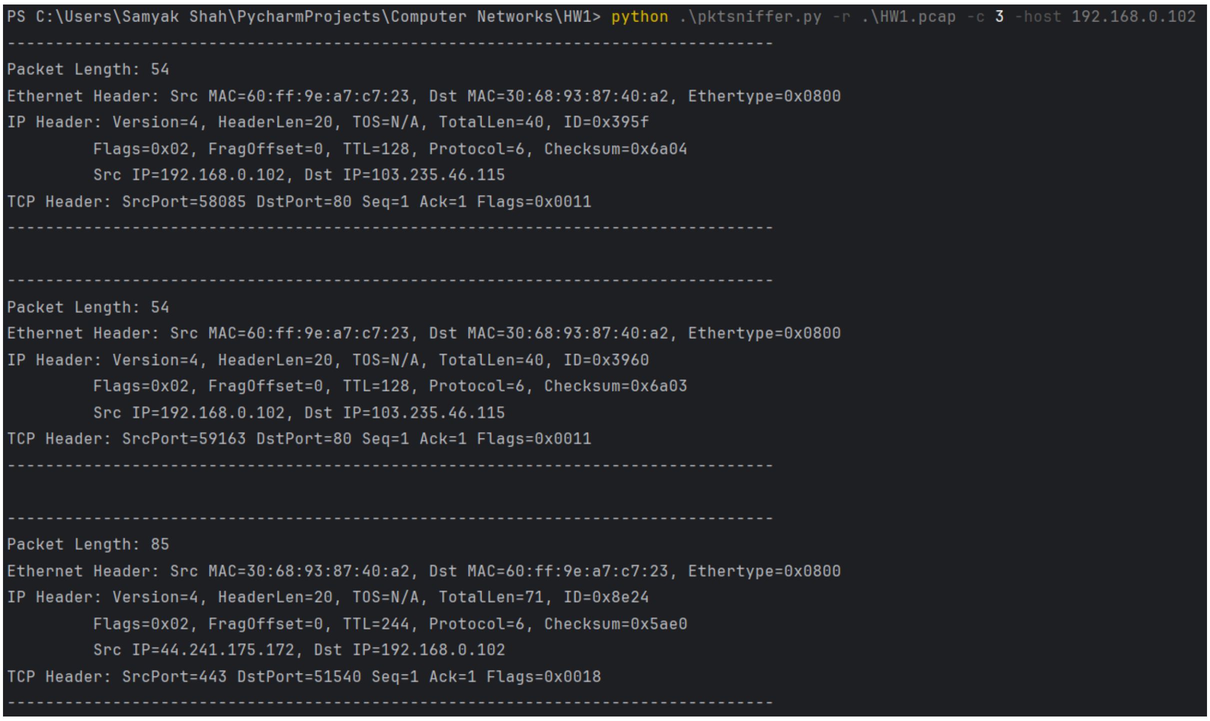
The program supports filtering packets using different flags. Screenshots below demonstrate the filtering capabilities.

4.1 Filter by Host

Command:

python packet_sniffer.py -r HW1.pcap -host 192.168.0.102

Program Output Screenshot:

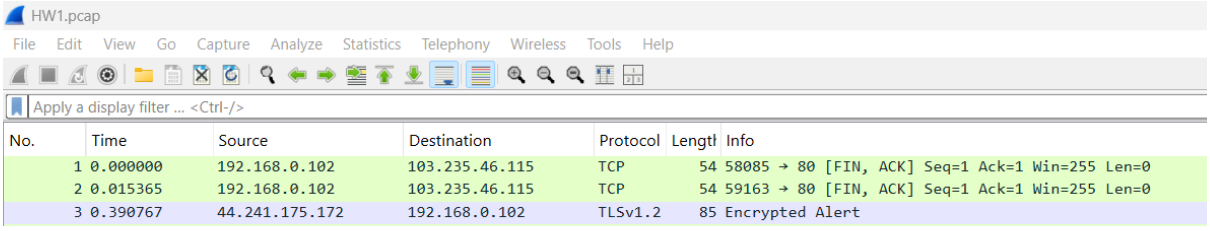


```
PS C:\Users\Samyak Shah\PycharmProjects\Computer Networks\HW1> python .\pktsniffer.py -r .\HW1.pcap -c 3 -host 192.168.0.102
--------------------------------------------------------------------------------
Packet Length: 54
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=40, ID=0x395f
         Flags=0x02, FragOffset=0, TTL=128, Protocol=6, Checksum=0x6a04
         Src IP=192.168.0.102, Dst IP=103.235.46.115
TCP Header: SrcPort=58085 DstPort=80 Seq=1 Ack=1 Flags=0x0011
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Packet Length: 54
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=40, ID=0x3960
         Flags=0x02, FragOffset=0, TTL=128, Protocol=6, Checksum=0x6a03
         Src IP=192.168.0.102, Dst IP=103.235.46.115
TCP Header: SrcPort=59163 DstPort=80 Seq=1 Ack=1 Flags=0x0011
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Packet Length: 85
Ethernet Header: Src MAC=30:68:93:87:40:a2, Dst MAC=60:ff:9e:a7:c7:23, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=71, ID=0x8e24
         Flags=0x02, FragOffset=0, TTL=244, Protocol=6, Checksum=0x5ae0
         Src IP=44.241.175.172, Dst IP=192.168.0.102
TCP Header: SrcPort=443 DstPort=51540 Seq=1 Ack=1 Flags=0x0018
--------------------------------------------------------------------------------
```

Wireshark Reference Screenshot:



HW1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

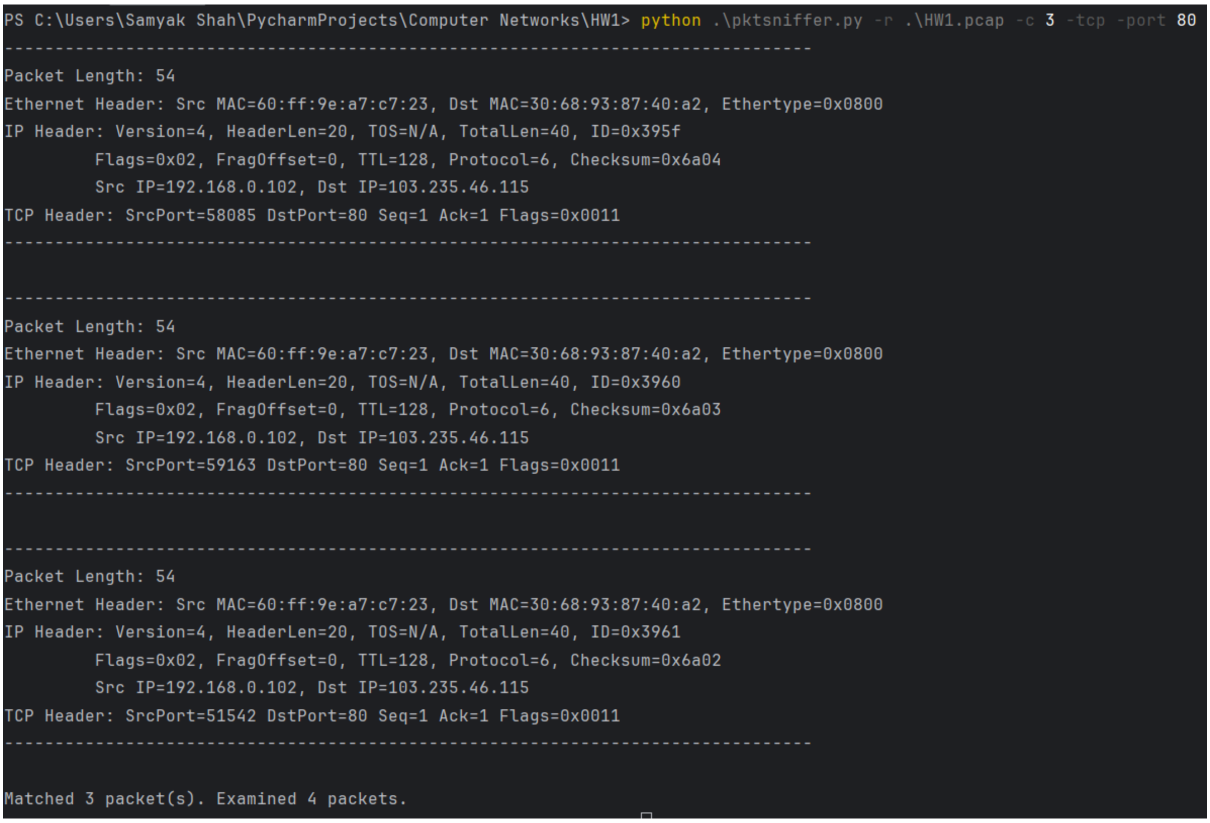
No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	192.168.0.102	103.235.46.115	TCP	54	58085 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
2	0.015365	192.168.0.102	103.235.46.115	TCP	54	59163 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
3	0.390767	44.241.175.172	192.168.0.102	TLSv1.2	85	Encrypted Alert

4.2 Filter by TCP/UDP Port

Command:

python packet_sniffer.py -r HW1.pcap -tcp -port 80

Program Output Screenshot:



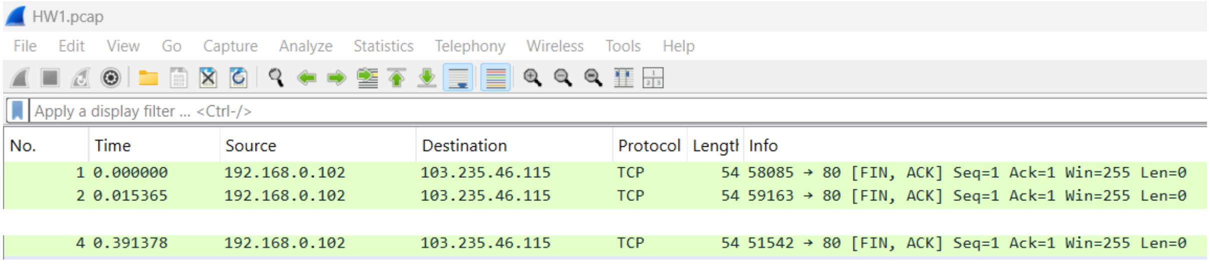
```
PS C:\Users\Samyak Shah\PycharmProjects\Computer Networks\HW1> python .\pktsniffer.py -r .\HW1.pcap -c 3 -tcp -port 80
--------------------------------------------------------------------------------
Packet Length: 54
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=40, ID=0x395f
         Flags=0x02, FragOffset=0, TTL=128, Protocol=6, Checksum=0x6a04
         Src IP=192.168.0.102, Dst IP=103.235.46.115
TCP Header: SrcPort=58085 DstPort=80 Seq=1 Ack=1 Flags=0x0011
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Packet Length: 54
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=40, ID=0x3960
         Flags=0x02, FragOffset=0, TTL=128, Protocol=6, Checksum=0x6a03
         Src IP=192.168.0.102, Dst IP=103.235.46.115
TCP Header: SrcPort=59163 DstPort=80 Seq=1 Ack=1 Flags=0x0011
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Packet Length: 54
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=40, ID=0x3961
         Flags=0x02, FragOffset=0, TTL=128, Protocol=6, Checksum=0x6a02
         Src IP=192.168.0.102, Dst IP=103.235.46.115
TCP Header: SrcPort=51542 DstPort=80 Seq=1 Ack=1 Flags=0x0011
--------------------------------------------------------------------------------

Matched 3 packet(s). Examined 4 packets.
```

Wireshark Reference Screenshot:



HW1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

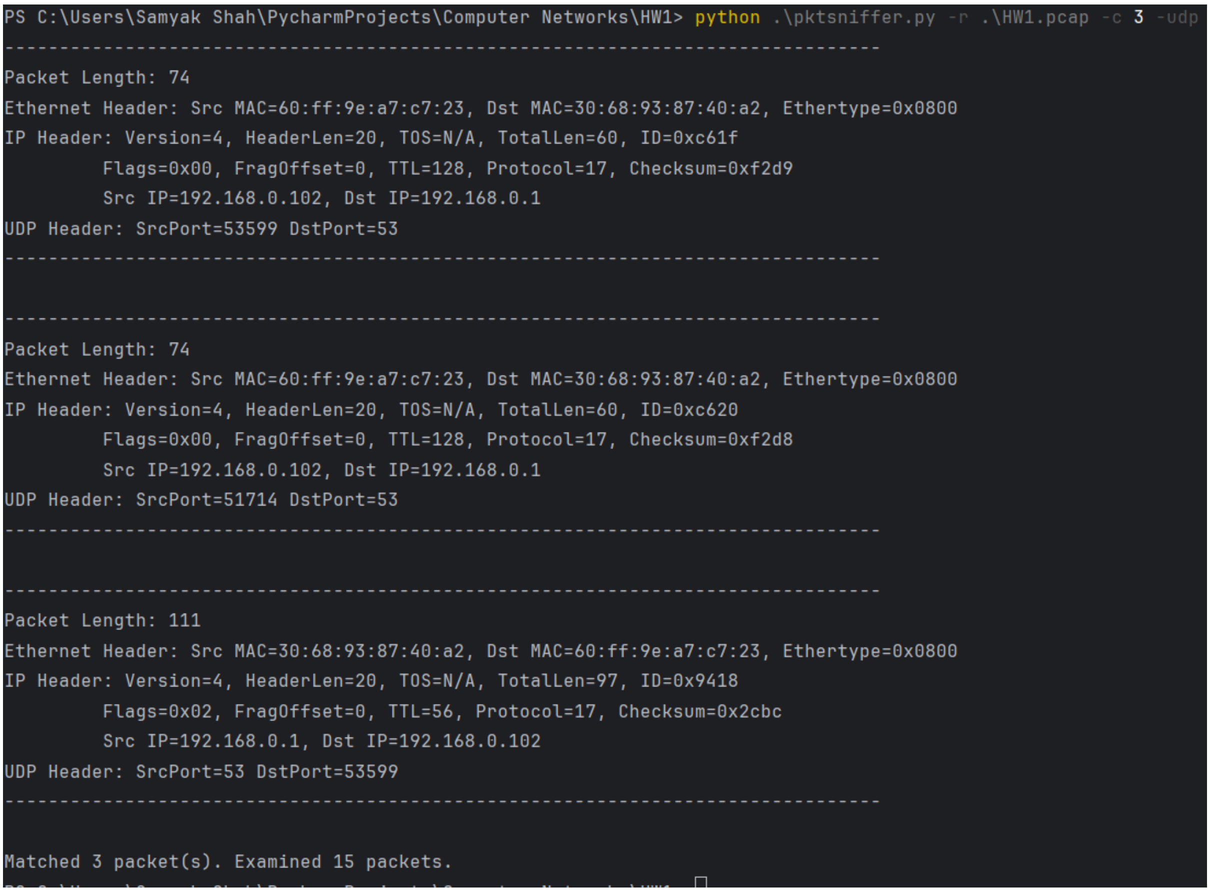
No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	192.168.0.102	103.235.46.115	TCP	54	58085 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
2	0.015365	192.168.0.102	103.235.46.115	TCP	54	59163 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
4	0.391378	192.168.0.102	103.235.46.115	TCP	54	51542 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0

4.3 Filter by Protocol

Command (UDP example):

python packet_sniffer.py -r sample.pcap -udp

Program Output Screenshot:



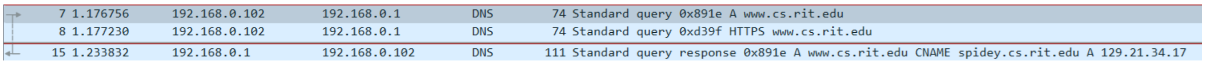
```
PS C:\Users\Samyak Shah\PycharmProjects\Computer Networks\HW1> python .\pktsniffer.py -r .\HW1.pcap -c 3 -udp
--------------------------------------------------------------------------------
Packet Length: 74
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=60, ID=0xc61f
         Flags=0x00, FragOffset=0, TTL=128, Protocol=17, Checksum=0xf2d9
         Src IP=192.168.0.102, Dst IP=192.168.0.1
UDP Header: SrcPort=53599 DstPort=53
--------------------------------------------------------------------------------


--------------------------------------------------------------------------------
Packet Length: 74
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=60, ID=0xc620
         Flags=0x00, FragOffset=0, TTL=128, Protocol=17, Checksum=0xf2d8
         Src IP=192.168.0.102, Dst IP=192.168.0.1
UDP Header: SrcPort=51714 DstPort=53
--------------------------------------------------------------------------------


--------------------------------------------------------------------------------
Packet Length: 111
Ethernet Header: Src MAC=30:68:93:87:40:a2, Dst MAC=60:ff:9e:a7:c7:23, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=97, ID=0x9418
         Flags=0x02, FragOffset=0, TTL=56, Protocol=17, Checksum=0x2cbc
         Src IP=192.168.0.1, Dst IP=192.168.0.102
UDP Header: SrcPort=53 DstPort=53599
--------------------------------------------------------------------------------


Matched 3 packet(s). Examined 15 packets.
```

Wireshark Reference Screenshot:



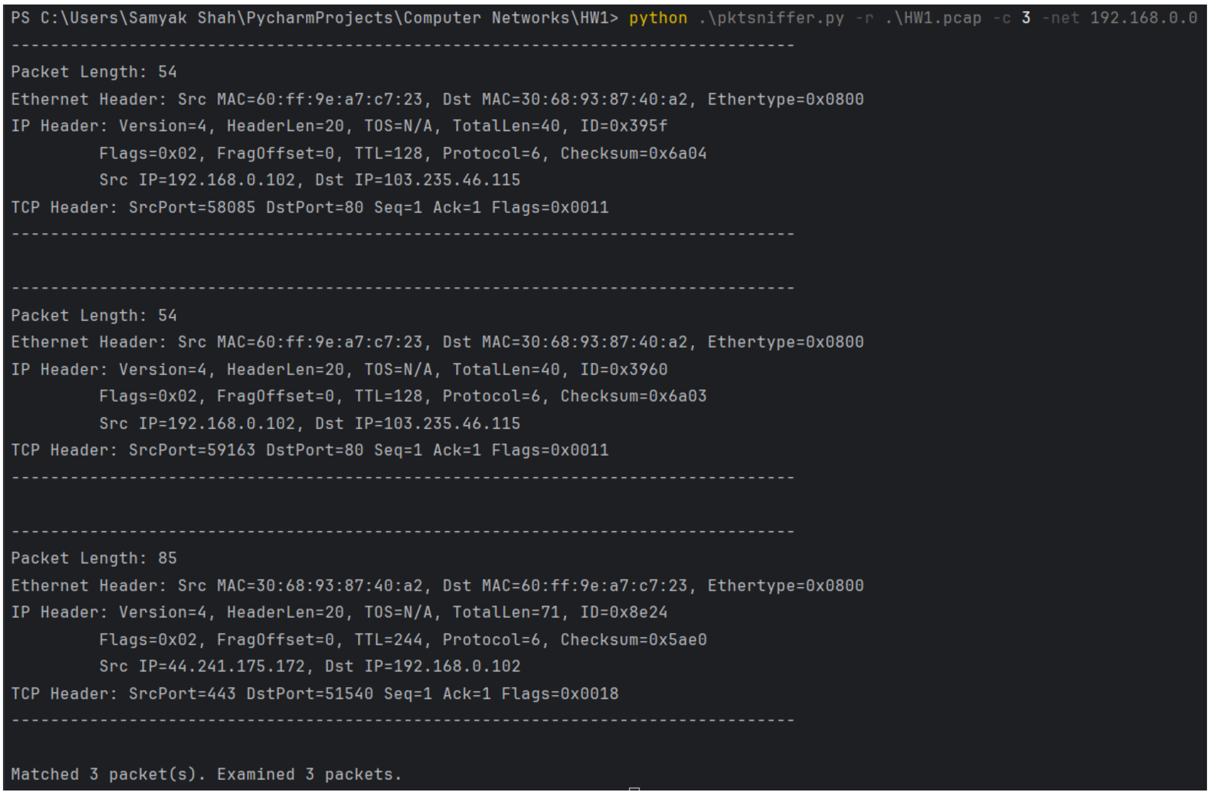
```
 7 1.176756   192.168.0.102   192.168.0.1     DNS    74 Standard query 0x891e A www.cs.rit.edu
 8 1.177230   192.168.0.102   192.168.0.1     DNS    74 Standard query 0xd39f HTTPS www.cs.rit.edu
15 1.233832   192.168.0.1     192.168.0.102   DNS   111 Standard query response 0x891e A www.cs.rit.edu CNAME spidey.cs.rit.edu A 129.21.34.17
```

4.4 Filter by Network (CIDR)

Command:

python packet_sniffer.py -r sample.pcap -net 192.168.0.0

Program Output Screenshot:



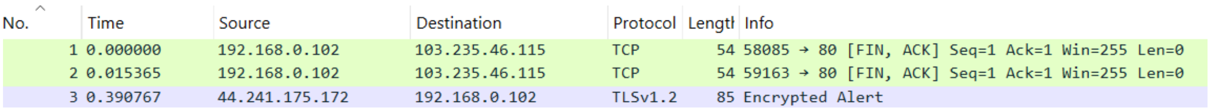
```
PS C:\Users\Samyak Shah\PycharmProjects\Computer Networks\HW1> python .\pktsniffer.py -r .\HW1.pcap -c 3 -net 192.168.0.0
--------------------------------------------------------------------------------
Packet Length: 54
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=40, ID=0x395f
         Flags=0x02, FragOffset=0, TTL=128, Protocol=6, Checksum=0x6a04
         Src IP=192.168.0.102, Dst IP=103.235.46.115
TCP Header: SrcPort=58085 DstPort=80 Seq=1 Ack=1 Flags=0x0011
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Packet Length: 54
Ethernet Header: Src MAC=60:ff:9e:a7:c7:23, Dst MAC=30:68:93:87:40:a2, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=40, ID=0x3960
         Flags=0x02, FragOffset=0, TTL=128, Protocol=6, Checksum=0x6a03
         Src IP=192.168.0.102, Dst IP=103.235.46.115
TCP Header: SrcPort=59163 DstPort=80 Seq=1 Ack=1 Flags=0x0011
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Packet Length: 85
Ethernet Header: Src MAC=30:68:93:87:40:a2, Dst MAC=60:ff:9e:a7:c7:23, Ethertype=0x0800
IP Header: Version=4, HeaderLen=20, TOS=N/A, TotalLen=71, ID=0x8e24
         Flags=0x02, FragOffset=0, TTL=244, Protocol=6, Checksum=0x5ae0
         Src IP=44.241.175.172, Dst IP=192.168.0.102
TCP Header: SrcPort=443 DstPort=51540 Seq=1 Ack=1 Flags=0x0018
--------------------------------------------------------------------------------

Matched 3 packet(s). Examined 3 packets.
```

Wireshark Reference Screenshot:



No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	192.168.0.102	103.235.46.115	TCP	54	58085 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
2	0.015365	192.168.0.102	103.235.46.115	TCP	54	59163 → 80 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
3	0.390767	44.241.175.172	192.168.0.102	TLSv1.2	85	Encrypted Alert

5. Conclusion

The packet sniffer successfully reads .pcap files and displays packet summaries. The filtering functions work correctly and are consistent with Wireshark output. This tool can be used for analyzing captured network traffic with custom filters.