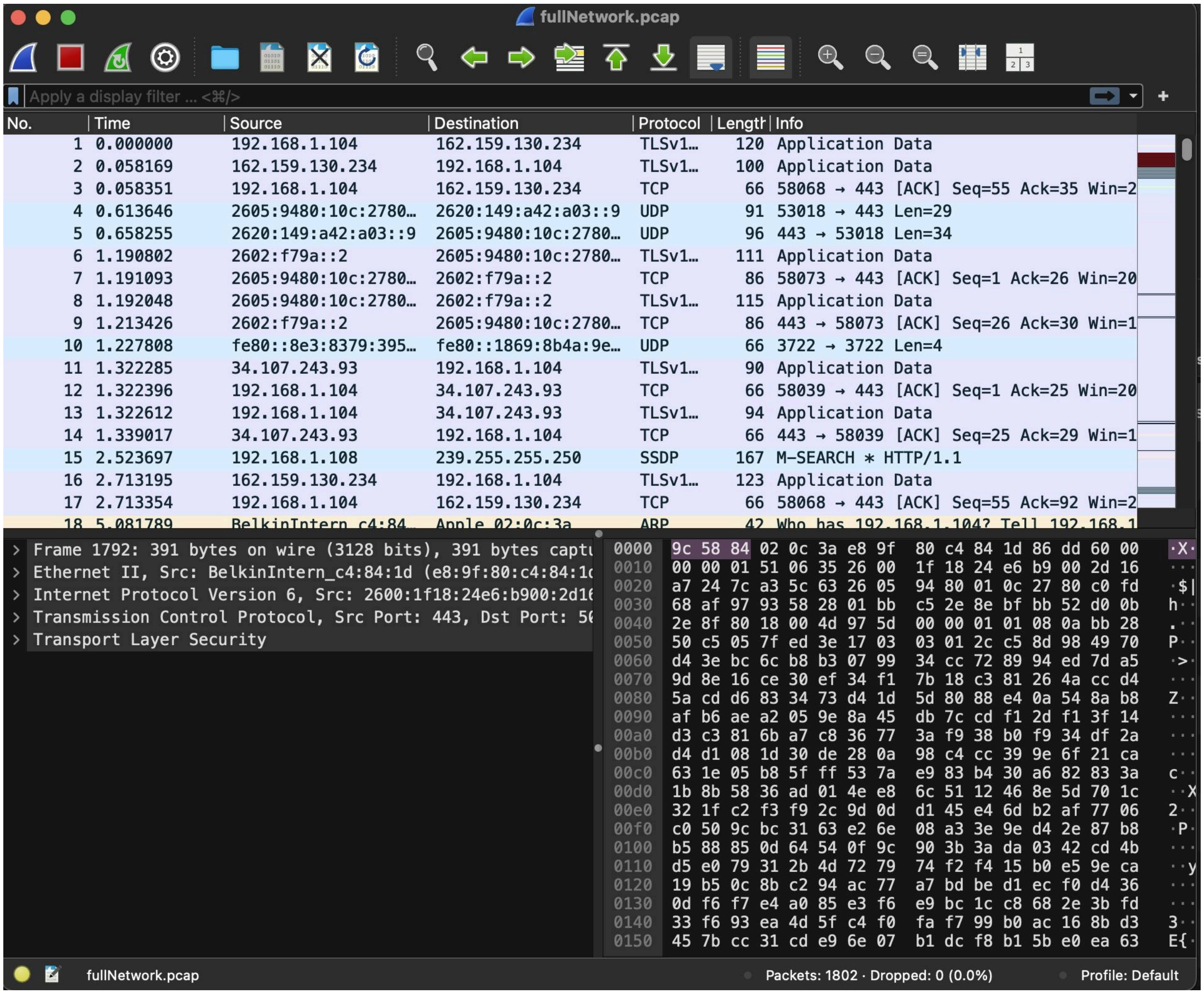
I.

This is the comparison between the packets captured from wireshark versus the first 5 packets printed out using the -c counter flag set to 5:

Start of file:

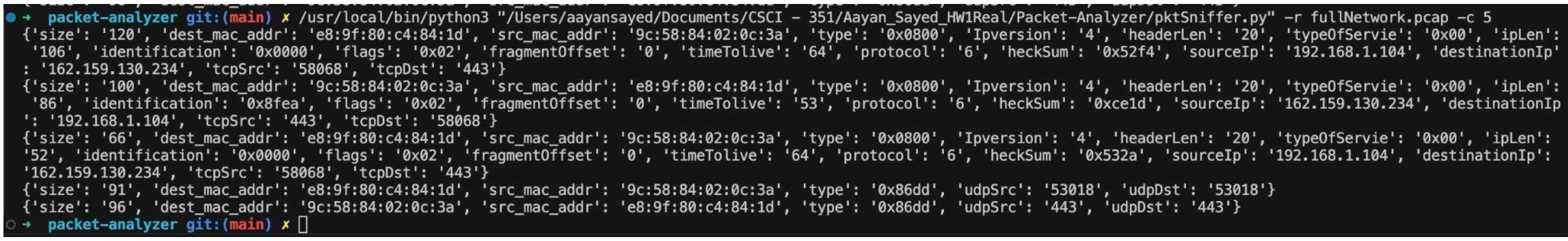


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.104	162.159.130.234	TLSv1…	120	Application Data
2	0.058169	162.159.130.234	192.168.1.104	TLSv1…	100	Application Data
3	0.058351	192.168.1.104	162.159.130.234	TCP	66	58068 → 443 [ACK] Seq=55 Ack=35 Win=2
4	0.613646	2605:9480:10c:2780…	2620:149:a42:a03::9	UDP	91	53018 → 443 Len=29
5	0.658255	2620:149:a42:a03::9	2605:9480:10c:2780…	UDP	96	443 → 53018 Len=34
6	1.190802	2602:f79a::2	2605:9480:10c:2780…	TLSv1…	111	Application Data
7	1.191093	2605:9480:10c:2780…	2602:f79a::2	TCP	86	58073 → 443 [ACK] Seq=1 Ack=26 Win=20
8	1.192048	2605:9480:10c:2780…	2602:f79a::2	TLSv1…	115	Application Data
9	1.213426	2602:f79a::2	2605:9480:10c:2780…	TCP	86	443 → 58073 [ACK] Seq=26 Ack=30 Win=1
10	1.227808	fe80::8e3:8379:395…	fe80::1869:8b4a:9e…	UDP	66	3722 → 3722 Len=4
11	1.322285	34.107.243.93	192.168.1.104	TLSv1…	90	Application Data
12	1.322396	192.168.1.104	34.107.243.93	TCP	66	58039 → 443 [ACK] Seq=1 Ack=25 Win=20
13	1.322612	192.168.1.104	34.107.243.93	TLSv1…	94	Application Data
14	1.339017	34.107.243.93	192.168.1.104	TCP	66	443 → 58039 [ACK] Seq=25 Ack=29 Win=1
15	2.523697	192.168.1.108	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
16	2.713195	162.159.130.234	192.168.1.104	TLSv1…	123	Application Data
17	2.713354	192.168.1.104	162.159.130.234	TCP	66	58068 → 443 [ACK] Seq=55 Ack=92 Win=2
18	5.081789	BelkinIntern_c4:84…	Apple_02:0c:3a	ARP	42	Who has 192.168.1.104? Tell 192.168.1

```
> Frame 1792: 391 bytes on wire (3128 bits), 391 bytes captu
> Ethernet II, Src: BelkinIntern_c4:84:1d (e8:9f:80:c4:84:1c
> Internet Protocol Version 6, Src: 2600:1f18:24e6:b900:2d16
> Transmission Control Protocol, Src Port: 443, Dst Port: 5(
> Transport Layer Security
```

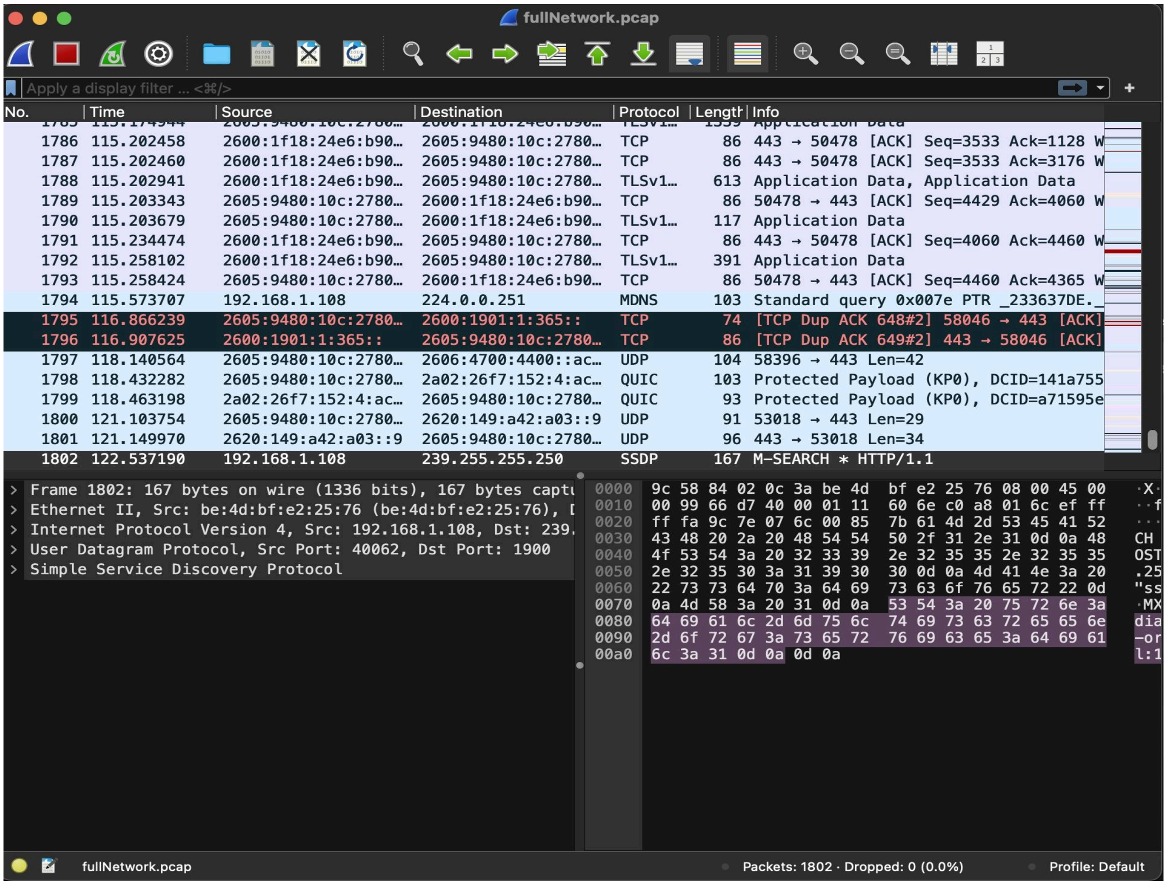
```
0000  9c 58 84 02 0c 3a e8 9f  80 c4 84 1d 86 dd 60 00   ·X·
0010  00 00 01 51 06 35 26 00  1f 18 24 e6 b9 00 2d 16   ···
0020  a7 24 7c a3 5c 63 26 05  94 80 01 0c 27 80 c0 fd   ·$|
0030  68 af 97 93 58 28 01 bb  c5 2e 8e bf bb 52 d0 0b   h··
0040  2e 8f 80 18 00 4d 97 5d  00 00 01 01 08 0a bb 28   .··
0050  50 c5 05 7f ed 3e 17 03  03 01 2c c5 8d 98 49 70   P··
0060  d4 3e bc 6c b8 b3 07 99  34 cc 72 89 94 ed 7d a5   ·>·
0070  9d 8e 16 ce 30 ef 34 f1  7b 18 c3 81 26 4a cc d4   ···
0080  5a cd d6 83 34 73 d4 1d  5d 80 88 e4 0a 54 8a b8   Z··
0090  af b6 ae a2 05 9e 8a 45  db 7c cd f1 2d f1 3f 14   ···
00a0  d3 c3 81 6b a7 c8 36 77  3a f9 38 b0 f9 34 df 2a   ···
00b0  d4 d1 08 1d 30 de 28 0a  98 c4 cc 39 9e 6f 21 ca   ···
00c0  63 1e 05 b8 5f ff 53 7a  e9 83 b4 30 a6 82 83 3a   c··
00d0  1b 8b 58 36 ad 01 4e e8  6c 51 12 46 8e 5d 70 1c   ··X
00e0  32 1f c2 f3 f9 2c 9d 0d  d1 45 e4 6d b2 af 77 06   2··
00f0  c0 50 9c bc 31 63 e2 6e  08 a3 3e 9e d4 2e 87 b8   ·P·
0100  b5 88 85 0d 64 54 0f 9c  90 3b 3a da 03 42 cd 4b   ···
0110  d5 e0 79 31 2b 4d 72 79  74 f2 f4 15 b0 e5 9e ca   ··y
0120  19 b5 0c 8b c2 94 ac 77  a7 bd be d1 ec f0 d4 36   ···
0130  0d f6 f7 e4 a0 85 e3 f6  e9 bc 1c c8 68 2e 3b fd   ···
0140  33 f6 93 ea 4d 5f c4 f0  fa f7 99 b0 ac 16 8b d3   3··
0150  45 7b cc 31 cd e9 6e 07  b1 dc f8 b1 5b e0 ea 63   E{·
```

I found the easiest indicator to look for is if the source address of the packet in wireshark is equal to the source address of the packet printed.



```
● → packet-analyzer git:(main) ✗ /usr/local/bin/python3 "/Users/aayansayed/Documents/CSCI - 351/Aayan_Sayed_HW1Real/Packet-Analyzer/pktSniffer.py" -r fullNetwork.pcap -c 5
  {'size': '120', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', 'typeOfServie': '0x00', 'ipLen':
   '106', 'identification': '0x0000', 'flags': '0x02', 'fragmentOffset': '0', 'timeTolive': '64', 'protocol': '6', 'heckSum': '0x52f4', 'sourceIp': '192.168.1.104', 'destinationIp'
  : '162.159.130.234', 'tcpSrc': '58068', 'tcpDst': '443'}
  {'size': '100', 'dest_mac_addr': '9c:58:84:02:0c:3a', 'src_mac_addr': 'e8:9f:80:c4:84:1d', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', 'typeOfServie': '0x00', 'ipLen':
   '86', 'identification': '0x8fea', 'flags': '0x02', 'fragmentOffset': '0', 'timeTolive': '53', 'protocol': '6', 'heckSum': '0xce1d', 'sourceIp': '162.159.130.234', 'destinationIp
  ': '192.168.1.104', 'tcpSrc': '443', 'tcpDst': '58068'}
  {'size': '66', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', 'typeOfServie': '0x00', 'ipLen':
  '52', 'identification': '0x0000', 'flags': '0x02', 'fragmentOffset': '0', 'timeTolive': '64', 'protocol': '6', 'heckSum': '0x532a', 'sourceIp': '192.168.1.104', 'destinationIp':
  '162.159.130.234', 'tcpSrc': '58068', 'tcpDst': '443'}
  {'size': '91', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x86dd', 'udpSrc': '53018', 'udpDst': '53018'}
  {'size': '96', 'dest_mac_addr': '9c:58:84:02:0c:3a', 'src_mac_addr': 'e8:9f:80:c4:84:1d', 'type': '0x86dd', 'udpSrc': '443', 'udpDst': '443'}
○ → packet-analyzer git:(main) ✗ 
```

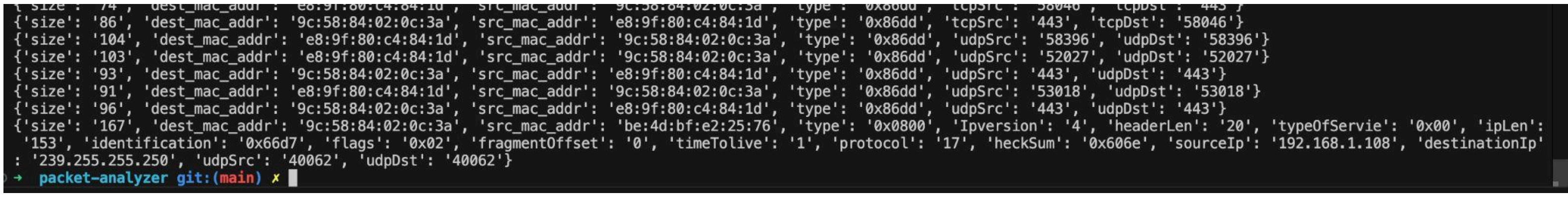
End of file:



No.	Time	Source	Destination	Protocol	Length	Info
1785	115.174944	2605:9480:10c:2780…	2600:1f18:24e6:b90…	TLSv1…	1339	Application Data
1786	115.202458	2600:1f18:24e6:b90…	2605:9480:10c:2780…	TCP	86	443 → 50478 [ACK] Seq=3533 Ack=1128 W
1787	115.202460	2600:1f18:24e6:b90…	2605:9480:10c:2780…	TCP	86	443 → 50478 [ACK] Seq=3533 Ack=3176 W
1788	115.202941	2600:1f18:24e6:b90…	2605:9480:10c:2780…	TLSv1…	613	Application Data, Application Data
1789	115.203343	2605:9480:10c:2780…	2600:1f18:24e6:b90…	TCP	86	50478 → 443 [ACK] Seq=4429 Ack=4060 W
1790	115.203679	2605:9480:10c:2780…	2600:1f18:24e6:b90…	TLSv1…	117	Application Data
1791	115.234474	2600:1f18:24e6:b90…	2605:9480:10c:2780…	TCP	86	443 → 50478 [ACK] Seq=4060 Ack=4460 W
1792	115.258102	2600:1f18:24e6:b90…	2605:9480:10c:2780…	TLSv1…	391	Application Data
1793	115.258424	2605:9480:10c:2780…	2600:1f18:24e6:b90…	TCP	86	50478 → 443 [ACK] Seq=4460 Ack=4365 W
1794	115.573707	192.168.1.108	224.0.0.251	MDNS	103	Standard query 0x007e PTR _233637DE._
1795	116.866239	2605:9480:10c:2780…	2600:1901:1:365::	TCP	74	[TCP Dup ACK 648#2] 58046 → 443 [ACK]
1796	116.907625	2600:1901:1:365::	2605:9480:10c:2780…	TCP	86	[TCP Dup ACK 649#2] 443 → 58046 [ACK]
1797	118.140564	2605:9480:10c:2780…	2606:4700:4400::ac…	UDP	104	58396 → 443 Len=42
1798	118.432282	2605:9480:10c:2780…	2a02:26f7:152:4:ac…	QUIC	103	Protected Payload (KP0), DCID=141a755
1799	118.463198	2a02:26f7:152:4:ac…	2605:9480:10c:2780…	QUIC	93	Protected Payload (KP0), DCID=a71595e
1800	121.103754	2605:9480:10c:2780…	2620:149:a42:a03::9	UDP	91	53018 → 443 Len=29
1801	121.149970	2620:149:a42:a03::9	2605:9480:10c:2780…	UDP	96	443 → 53018 Len=34
1802	122.537190	192.168.1.108	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1

```
> Frame 1802: 167 bytes on wire (1336 bits), 167 bytes captu
> Ethernet II, Src: be:4d:bf:e2:25:76 (be:4d:bf:e2:25:76), D
> Internet Protocol Version 4, Src: 192.168.1.108, Dst: 239.
> User Datagram Protocol, Src Port: 40062, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  9c 58 84 02 0c 3a be 4d  bf e2 25 76 08 00 45 00   ·X·
0010  00 99 66 d7 40 00 01 11  60 6e c0 a8 01 6c ef ff   ··f
0020  ff fa 9c 7e 07 6c 00 85  7b 61 4d 2d 53 45 41 52   ···
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH 
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .25
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ss
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dia
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -or
00a0  6c 3a 31 0d 0a 0d 0a                               l:1
```

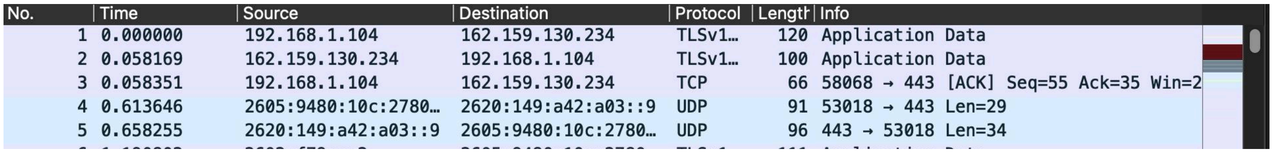


```
{'size': '74', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x86dd', 'tcpSrc': '58046', 'tcpDst': '443'}
{'size': '86', 'dest_mac_addr': '9c:58:84:02:0c:3a', 'src_mac_addr': 'e8:9f:80:c4:84:1d', 'type': '0x86dd', 'tcpSrc': '443', 'tcpDst': '58046'}
{'size': '104', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x86dd', 'udpSrc': '58396', 'udpDst': '58396'}
{'size': '103', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x86dd', 'udpSrc': '52027', 'udpDst': '52027'}
{'size': '93', 'dest_mac_addr': '9c:58:84:02:0c:3a', 'src_mac_addr': 'e8:9f:80:c4:84:1d', 'type': '0x86dd', 'udpSrc': '443', 'udpDst': '443'}
{'size': '91', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x86dd', 'udpSrc': '53018', 'udpDst': '53018'}
{'size': '96', 'dest_mac_addr': '9c:58:84:02:0c:3a', 'src_mac_addr': 'e8:9f:80:c4:84:1d', 'type': '0x86dd', 'udpSrc': '443', 'udpDst': '443'}
{'size': '167', 'dest_mac_addr': '9c:58:84:02:0c:3a', 'src_mac_addr': 'be:4d:bf:e2:25:76', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', 'typeOfServie': '0x00', 'ipLen':
 '153', 'identification': '0x66d7', 'flags': '0x02', 'fragmentOffset': '0', 'timeTolive': '1', 'protocol': '17', 'heckSum': '0x606e', 'sourceIp': '192.168.1.108', 'destinationIp'
: '239.255.255.250', 'udpSrc': '40062', 'udpDst': '40062'}
→ packet-analyzer git:(main) ✗ 
```

I only printed packets with either TCP, UDP or ICMP.

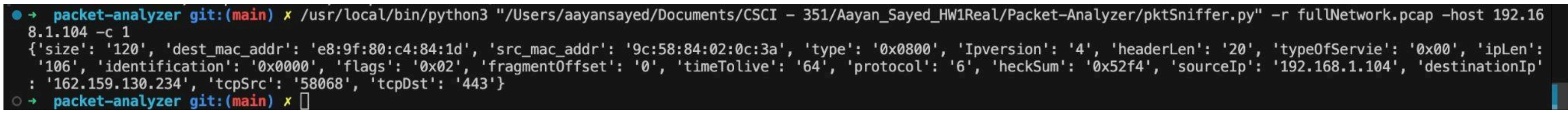
Command Line Filter tests:

For all of these tests (besides Icmp) I set counter to 5 and used the first 5 packets to filter.



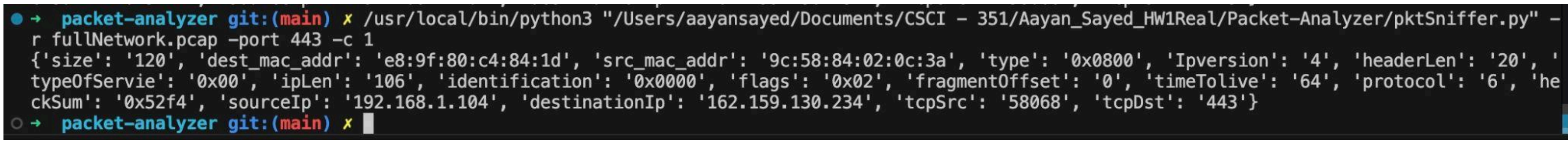
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.104	162.159.130.234	TLSv1…	120	Application Data
2	0.058169	162.159.130.234	192.168.1.104	TLSv1…	100	Application Data
3	0.058351	192.168.1.104	162.159.130.234	TCP	66	58068 → 443 [ACK] Seq=55 Ack=35 Win=2
4	0.613646	2605:9480:10c:2780…	2620:149:a42:a03::9	UDP	91	53018 → 443 Len=29
5	0.658255	2620:149:a42:a03::9	2605:9480:10c:2780…	UDP	96	443 → 53018 Len=34

Host:
Run with host - 192.168.1.104 - accurately gets the first packet



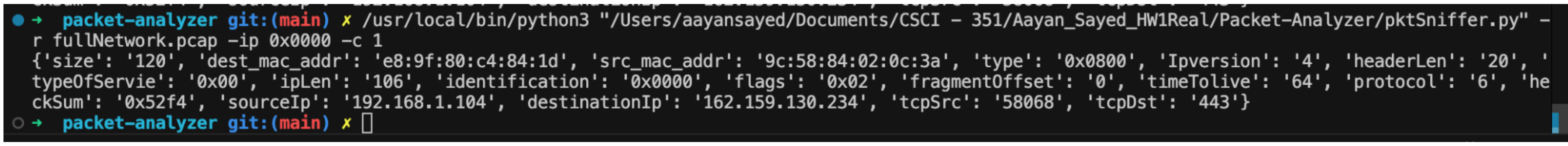
```
● → packet-analyzer git:(main) ✗ /usr/local/bin/python3 "/Users/aayansayed/Documents/CSCI - 351/Aayan_Sayed_HW1Real/Packet-Analyzer/pktSniffer.py" -r fullNetwork.pcap -host 192.16
  8.1.104 -c 1
  {'size': '120', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', 'typeOfServie': '0x00', 'ipLen':
   '106', 'identification': '0x0000', 'flags': '0x02', 'fragmentOffset': '0', 'timeTolive': '64', 'protocol': '6', 'heckSum': '0x52f4', 'sourceIp': '192.168.1.104', 'destinationIp'
  : '162.159.130.234', 'tcpSrc': '58068', 'tcpDst': '443'}
○ → packet-analyzer git:(main) ✗ ▯
```

Port:
Run with tcp destination port - 443 - accurately gets the first packet



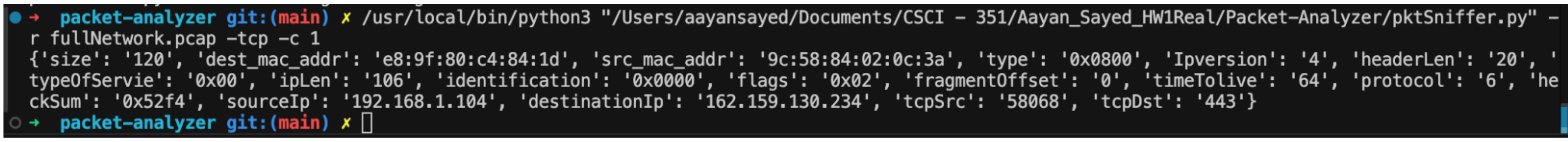
```
● → packet-analyzer git:(main) ✗ /usr/local/bin/python3 "/Users/aayansayed/Documents/CSCI - 351/Aayan_Sayed_HW1Real/Packet-Analyzer/pktSniffer.py" -
  r fullNetwork.pcap -port 443 -c 1
  {'size': '120', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', '
  typeOfServie': '0x00', 'ipLen': '106', 'identification': '0x0000', 'flags': '0x02', 'fragmentOffset': '0', 'timeTolive': '64', 'protocol': '6', 'he
  ckSum': '0x52f4', 'sourceIp': '192.168.1.104', 'destinationIp': '162.159.130.234', 'tcpSrc': '58068', 'tcpDst': '443'}
○ → packet-analyzer git:(main) ✗ █
```

IP:
Run with the IP.id of the first entry



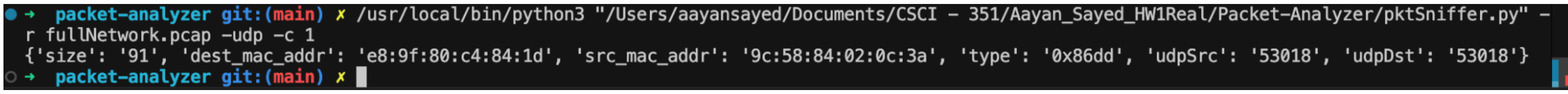
```
● → packet-analyzer git:(main) ✗ /usr/local/bin/python3 "/Users/aayansayed/Documents/CSCI - 351/Aayan_Sayed_HW1Real/Packet-Analyzer/pktSniffer.py" -
  r fullNetwork.pcap -ip 0x0000 -c 1
  {'size': '120', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', '
  typeOfServie': '0x00', 'ipLen': '106', 'identification': '0x0000', 'flags': '0x02', 'fragmentOffset': '0', 'timeTolive': '64', 'protocol': '6', 'he
  ckSum': '0x52f4', 'sourceIp': '192.168.1.104', 'destinationIp': '162.159.130.234', 'tcpSrc': '58068', 'tcpDst': '443'}
○ → packet-analyzer git:(main) ✗ ▯
```

TCP:
Run with counter set to 1 as to only display the first packet which was TCP



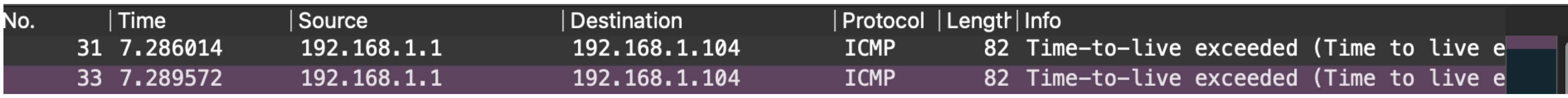
```
● → packet-analyzer git:(main) ✗ /usr/local/bin/python3 "/Users/aayansayed/Documents/CSCI - 351/Aayan_Sayed_HW1Real/Packet-Analyzer/pktSniffer.py" -
  r fullNetwork.pcap -tcp -c 1
  {'size': '120', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', '
  typeOfServie': '0x00', 'ipLen': '106', 'identification': '0x0000', 'flags': '0x02', 'fragmentOffset': '0', 'timeTolive': '64', 'protocol': '6', 'he
  ckSum': '0x52f4', 'sourceIp': '192.168.1.104', 'destinationIp': '162.159.130.234', 'tcpSrc': '58068', 'tcpDst': '443'}
○ → packet-analyzer git:(main) ✗ ▯
```

UDP:
Packet 4 was UDP so testing filtering for that packet - size and other attributes matched



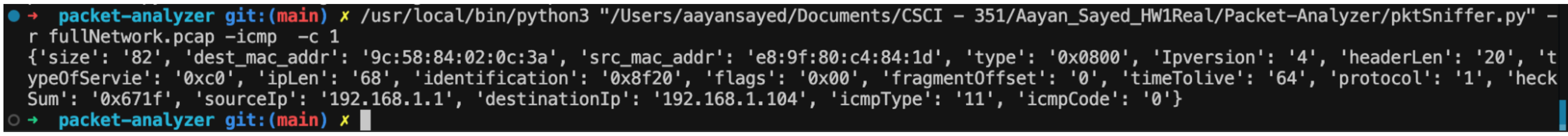
```
● → packet-analyzer git:(main) ✗ /usr/local/bin/python3 "/Users/aayansayed/Documents/CSCI - 351/Aayan_Sayed_HW1Real/Packet-Analyzer/pktSniffer.py" -
  r fullNetwork.pcap -udp -c 1
  {'size': '91', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x86dd', 'udpSrc': '53018', 'udpDst': '53018'}
○ → packet-analyzer git:(main) ✗ █
```

ICMP:
These were the first ICMP packets in the pcap file:



No.	Time	Source	Destination	Protocol	Length	Info
31	7.286014	192.168.1.1	192.168.1.104	ICMP	82	Time-to-live exceeded (Time to live e
33	7.289572	192.168.1.1	192.168.1.104	ICMP	82	Time-to-live exceeded (Time to live e

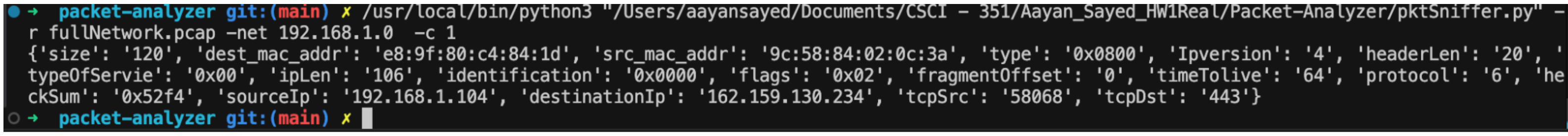
Result after running filter:



```
● → packet-analyzer git:(main) ✗ /usr/local/bin/python3 "/Users/aayansayed/Documents/CSCI - 351/Aayan_Sayed_HW1Real/Packet-Analyzer/pktSniffer.py" -
  r fullNetwork.pcap -icmp  -c 1
  {'size': '82', 'dest_mac_addr': '9c:58:84:02:0c:3a', 'src_mac_addr': 'e8:9f:80:c4:84:1d', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', 't
  ypeOfServie': '0xc0', 'ipLen': '68', 'identification': '0x8f20', 'flags': '0x00', 'fragmentOffset': '0', 'timeTolive': '64', 'protocol': '1', 'heck
  Sum': '0x671f', 'sourceIp': '192.168.1.1', 'destinationIp': '192.168.1.104', 'icmpType': '11', 'icmpCode': '0'}
○ → packet-analyzer git:(main) ✗ 
```

Net:

The first packet has a source IP of 192.168.1.104 but we will filter using 192.168.1.0



```
● → packet-analyzer git:(main) ✗ /usr/local/bin/python3 "/Users/aayansayed/Documents/CSCI - 351/Aayan_Sayed_HW1Real/Packet-Analyzer/pktSniffer.py" -
  r fullNetwork.pcap -net 192.168.1.0  -c 1
  {'size': '120', 'dest_mac_addr': 'e8:9f:80:c4:84:1d', 'src_mac_addr': '9c:58:84:02:0c:3a', 'type': '0x0800', 'Ipversion': '4', 'headerLen': '20', '
  typeOfServie': '0x00', 'ipLen': '106', 'identification': '0x0000', 'flags': '0x02', 'fragmentOffset': '0', 'timeTolive': '64', 'protocol': '6', 'he
  ckSum': '0x52f4', 'sourceIp': '192.168.1.104', 'destinationIp': '162.159.130.234', 'tcpSrc': '58068', 'tcpDst': '443'}
○ → packet-analyzer git:(main) ✗ 
```