COMP 7003
Introduction to Information and Network Security

Assignment-02

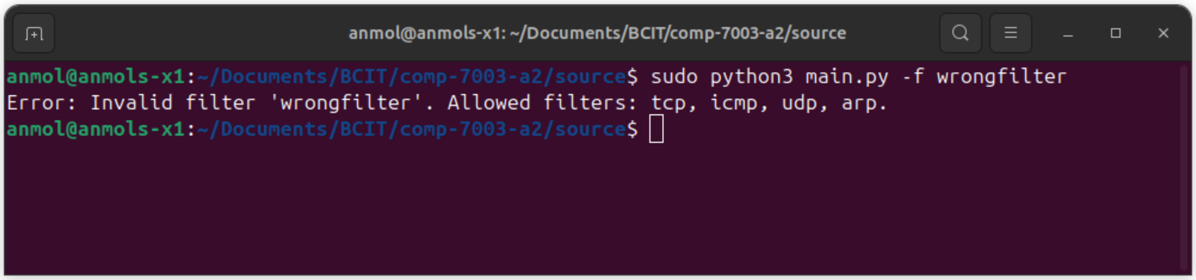
Testing

Anmol Mittal
A01397754
February 2nd, 2025
Course Reference Number (CRN): 91662

Test	Expected	Actual	Screenshot
Enter invalid BPF filter	fail	fail	Test 1
Too many arguments in the BPF Filter	fail	fail	Test 2
Enter no BPF filter	pass	pass	Test 3
Run the program with too many CLI arguments	fail	fail	Test 4
Enter non-number/integer in the number of packets to capture	fail	fail	Test 5
No number in the number of packets to capture prompt	pass	pass	Test 6
Negative number in the number of packets to capture	fail	fail	Test 7
Positive number in the number of packets to capture	pass	pass	Test 8
Valid BPF filter for ARP	pass	pass	Test 9
Valid BPF filter for TCP	pass	pass	Test 10
Valid BPF filter for UDP	pass	pass	Test 11
Valid BPF filter for ICMP	pass	pass	Test 12
No interface entered	pass	pass	Test 13
No arguments entered at all	pass	pass	Test 14
Valid BPF filter for ICMPv6	pass	pass	Test 15
Valid BPF filter for IPv6	pass	pass	Test 16
Valid BPF filter for DNS	pass	pass	Test 17

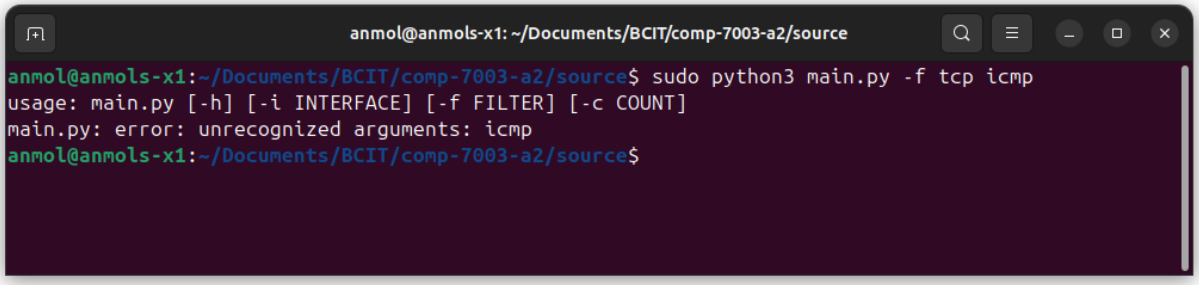
Tests

Test 01



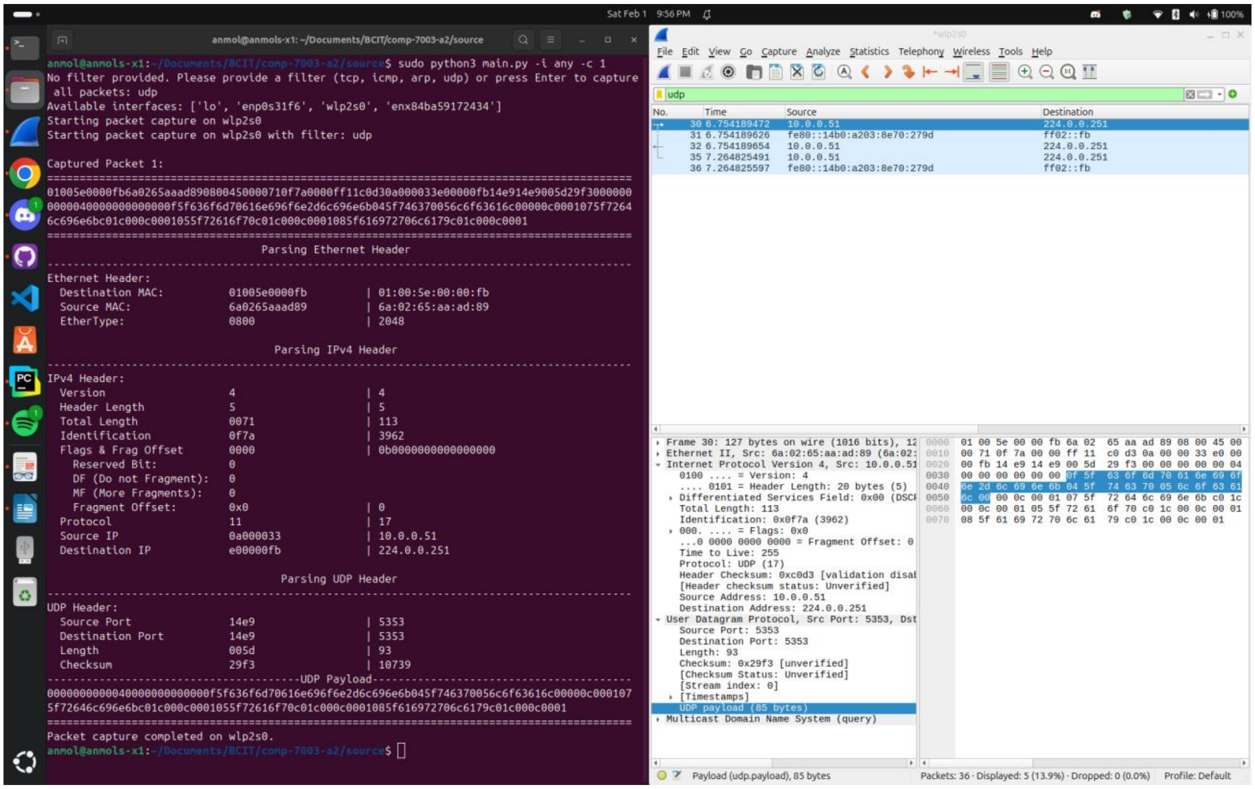
```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -f wrongfilter
Error: Invalid filter 'wrongfilter'. Allowed filters: tcp, icmp, udp, arp.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ 
```

Test 02



```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -f tcp icmp
usage: main.py [-h] [-i INTERFACE] [-f FILTER] [-c COUNT]
main.py: error: unrecognized arguments: icmp
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

Test 03


Sat Feb 1   9:56 PM
100%
anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -c 1
No filter provided. Please provide a filter (tcp, icmp, arp, udp) or press Enter to capture
 all packets: udp
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: udp

Captured Packet 1:
===========================================================================================
01005e0000fb6a0265aaad890800450000710f7a0000ff11c0d30a000033e00000fb14e914e9005d29f3000000
0000040000000000000000f5f636f6d70616e696f6e2d6c696e6b045f746370056c6f63616c00000c0001075f7264
6c696e6bc01c000c0001055f72616f70c01c000c0001085f616972706c6179c01c000c0001
===========================================================================================
                                   Parsing Ethernet Header
-------------------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:           01005e0000fb          | 01:00:5e:00:00:fb
  Source MAC:                6a0265aaad89          | 6a:02:65:aa:ad:89
  EtherType:                 0800                  | 2048

                                    Parsing IPv4 Header
-------------------------------------------------------------------------------------------
IPv4 Header:
  Version                    4                     | 4
  Header Length              5                     | 5
  Total Length               0071                  | 113
  Identification             0f7a                  | 3962
  Flags & Frag Offset        0000                  | 0b0000000000000000
    Reserved Bit:            0
    DF (Do not Fragment):    0
    MF (More Fragments):     0
    Fragment Offset:         0x0                   | 0
  Protocol                   11                    | 17
  Source IP                  0a000033              | 10.0.0.51
  Destination IP             e00000fb              | 224.0.0.251

                                    Parsing UDP Header
-------------------------------------------------------------------------------------------
UDP Header:
  Source Port                14e9                  | 5353
  Destination Port           14e9                  | 5353
  Length                     005d                  | 93
  Checksum                   29f3                  | 10739
-----------------------------------------UDP Payload---------------------------------------
000000000004000000000000000f5f636f6d70616e696f6e2d6c696e6b045f746370056c6f63616c00000c000107
5f72646c696e6bc01c000c0001055f72616f70c01c000c0001085f616972706c6179c01c000c0001
===========================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ 
```

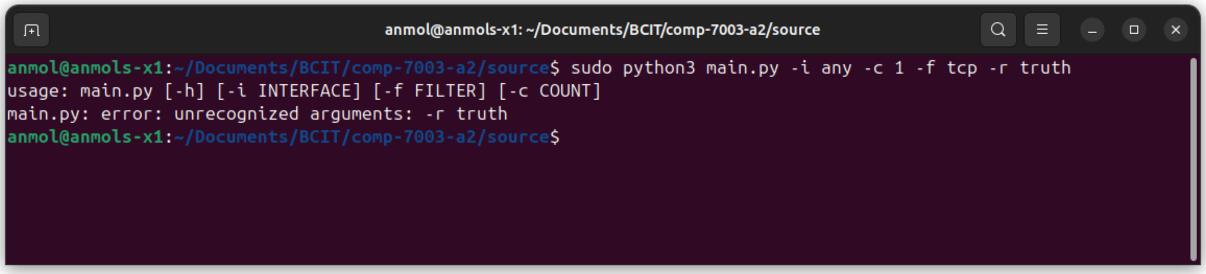
```
udp

No.    Time          Source                           Destination
    30 6.754189472   10.0.0.51                        224.0.0.251
    31 6.754189626   fe80::14b0:a203:8e70:279d        ff02::fb
    32 6.754189654   10.0.0.51                        224.0.0.251
    35 7.264825491   10.0.0.51                        224.0.0.251
    36 7.264825597   fe80::14b0:a203:8e70:279d        ff02::fb
```

```
▸ Frame 30: 127 bytes on wire (1016 bits), 12
▸ Ethernet II, Src: 6a:02:65:aa:ad:89 (6a:02:
▾ Internet Protocol Version 4, Src: 10.0.0.51
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCF
    Total Length: 113
    Identification: 0x0f7a (3962)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: UDP (17)
    Header Checksum: 0xc0d3 [validation disat
    [Header checksum status: Unverified]
    Source Address: 10.0.0.51
    Destination Address: 224.0.0.251
▾ User Datagram Protocol, Src Port: 5353, Dst
    Source Port: 5353
    Destination Port: 5353
    Length: 93
    Checksum: 0x29f3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  ▸ [Timestamps]
    UDP payload (85 bytes)
▸ Multicast Domain Name System (query)
```

```
0000  01 00 5e 00 00 fb 6a 02  65 aa ad 89 08 00 45 00
0010  00 71 0f 7a 00 00 ff 11  c0 d3 0a 00 00 33 e0 00
0020  00 fb 14 e9 14 e9 00 5d  29 f3 00 00 00 00 00 04
0030  00 00 00 00 00 00 0f 5f  63 6f 6d 70 61 6e 69 6f
0040  6e 2d 6c 69 6e 6b 04 5f  74 63 70 05 6c 6f 63 61
0050  6c 00 00 0c 00 01 07 5f  72 64 6c 69 6e 6b c0 1c
0060  00 0c 00 01 05 5f 72 61  6f 70 c0 1c 00 0c 00 01
0070  08 5f 61 69 72 70 6c 61  79 c0 1c 00 0c 00 01
```

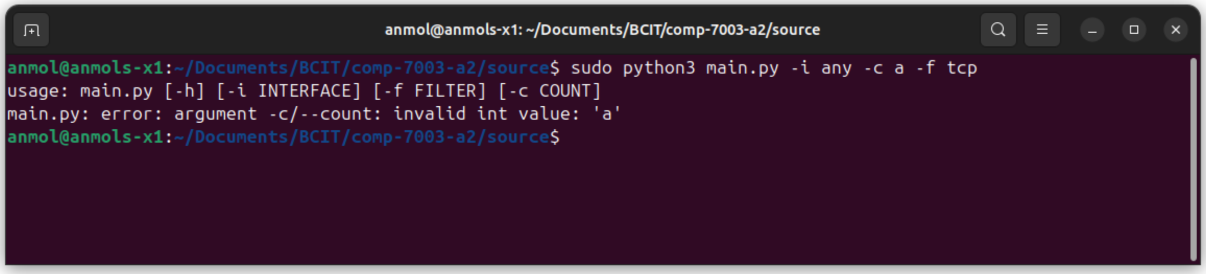
```
Payload (udp.payload), 85 bytes        Packets: 36 · Displayed: 5 (13.9%) · Dropped: 0 (0.0%)    Profile: Default
```

Test 04



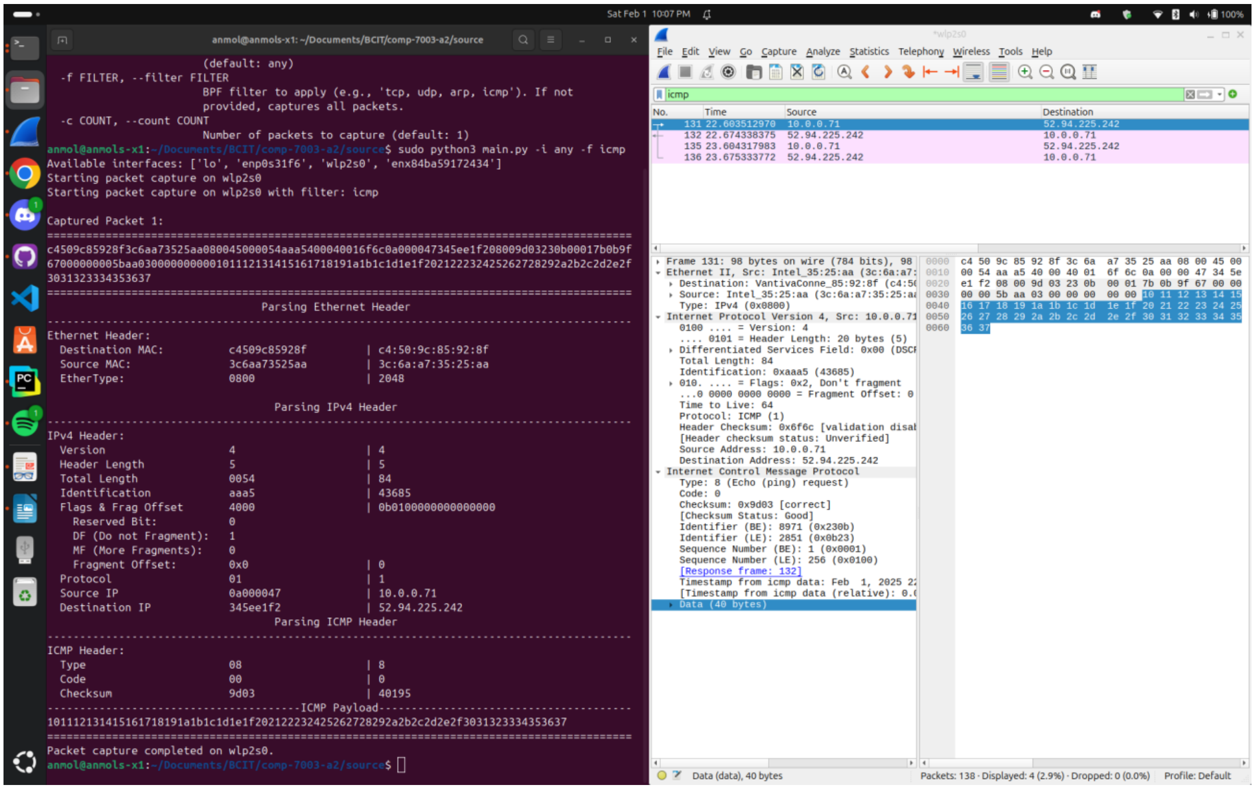
```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -c 1 -f tcp -r truth
usage: main.py [-h] [-i INTERFACE] [-f FILTER] [-c COUNT]
main.py: error: unrecognized arguments: -r truth
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

Test 05



```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -c a -f tcp
usage: main.py [-h] [-i INTERFACE] [-f FILTER] [-c COUNT]
main.py: error: argument -c/--count: invalid int value: 'a'
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

Test 06



```
                        (default: any)
  -f FILTER, --filter FILTER
                        BPF filter to apply (e.g., 'tcp, udp, arp, icmp'). If not
                        provided, captures all packets.
  -c COUNT, --count COUNT
                        Number of packets to capture (default: 1)
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -f icmp
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: icmp

Captured Packet 1:
==========================================================================================
c4509c85928f3c6aa73525aa080045000054aaa5400040016f6c0a000047345ee1f208009d03230b00017b0b9f
67000000005baa030000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f
3031323334353637
==========================================================================================
                                 Parsing Ethernet Header
------------------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:            c4509c85928f           | c4:50:9c:85:92:8f
  Source MAC:                 3c6aa73525aa           | 3c:6a:a7:35:25:aa
  EtherType:                  0800                   | 2048

                                  Parsing IPv4 Header
------------------------------------------------------------------------------------------
IPv4 Header:
  Version                     4                      | 4
  Header Length               5                      | 5
  Total Length                0054                   | 84
  Identification              aaa5                   | 43685
  Flags & Frag Offset         4000                   | 0b0100000000000000
    Reserved Bit:             0
    DF (Do not Fragment):     1
    MF (More Fragments):      0
    Fragment Offset:          0x0                    | 0
  Protocol                    01                     | 1
  Source IP                   0a000047               | 10.0.0.71
  Destination IP              345ee1f2               | 52.94.225.242
                                  Parsing ICMP Header
------------------------------------------------------------------------------------------
ICMP Header:
  Type                        08                     | 8
  Code                        00                     | 0
  Checksum                    9d03                   | 40195
---------------------------------------ICMP Payload---------------------------------------
101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
==========================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

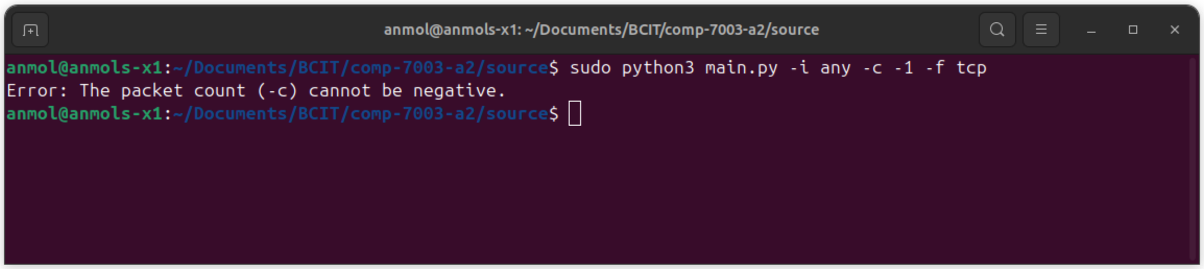
```
icmp

No.  Time           Source           Destination
131  22.603512970   10.0.0.71        52.94.225.242
132  22.674338375   52.94.225.242    10.0.0.71
135  23.604317983   10.0.0.71        52.94.225.242
136  23.675333772   52.94.225.242    10.0.0.71
```

```
Frame 131: 98 bytes on wire (784 bits), 98
Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:
  Destination: VantivaConne_85:92:8f (c4:5
  Source: Intel_35:25:aa (3c:6a:a7:35:25:a
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.71
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP
  Total Length: 84
  Identification: 0xaaa5 (43685)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0x6f6c [validation disab
  [Header checksum status: Unverified]
  Source Address: 10.0.0.71
  Destination Address: 52.94.225.242
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x9d03 [correct]
  [Checksum Status: Good]
  Identifier (BE): 8971 (0x230b)
  Identifier (LE): 2851 (0x0b23)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Response frame: 132]
  Timestamp from icmp data: Feb  1, 2025 22
  [Timestamp from icmp data (relative): 0.0
  Data (40 bytes)
```

```
0000  c4 50 9c 85 92 8f 3c 6a  a7 35 25 aa 08 00 45 00
0010  00 54 aa a5 40 00 40 01  6f 6c 0a 00 00 47 34 5e
0020  e1 f2 08 00 9d 03 23 0b  00 01 7b 0b 9f 67 00 00
0030  00 00 5b aa 03 00 00 00  00 00 10 11 12 13 14 15
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35
0060  36 37
```

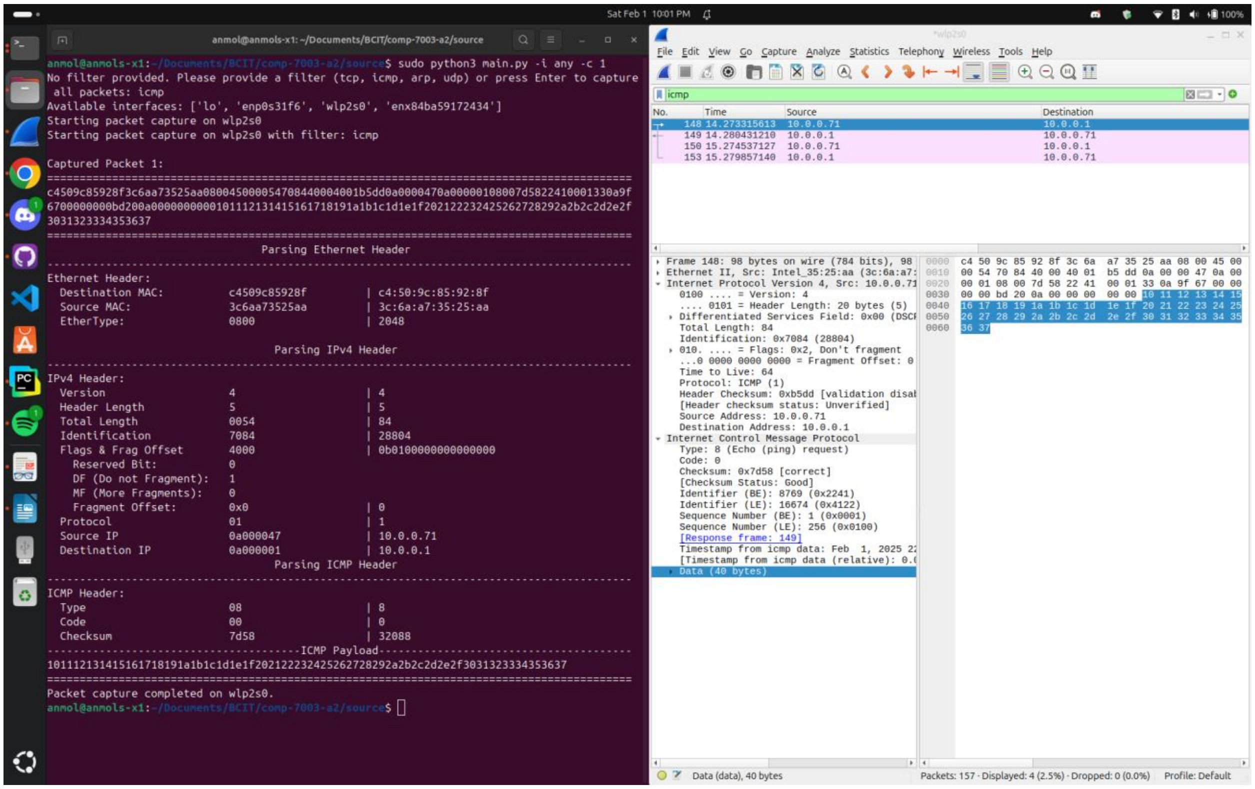
```
Data (data), 40 bytes        Packets: 138 · Displayed: 4 (2.9%) · Dropped: 0 (0.0%)    Profile: Default
```

Test 07



```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -c -1 -f tcp
Error: The packet count (-c) cannot be negative.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ 
```

Test 08



```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -c 1
No filter provided. Please provide a filter (tcp, icmp, arp, udp) or press Enter to capture
 all packets: icmp
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: icmp

Captured Packet 1:
==========================================================================================
c4509c85928f3c6aa73525aa080045000054708440004001b5dd0a0000470a00000108007d5822410001330a9f
6700000000bd200a00000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f
3031323334353637
==========================================================================================
                                 Parsing Ethernet Header
------------------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:             c4509c85928f           | c4:50:9c:85:92:8f
  Source MAC:                  3c6aa73525aa           | 3c:6a:a7:35:25:aa
  EtherType:                   0800                   | 2048

                                  Parsing IPv4 Header
------------------------------------------------------------------------------------------
IPv4 Header:
  Version                      4                      | 4
  Header Length                5                      | 5
  Total Length                 0054                   | 84
  Identification               7084                   | 28804
  Flags & Frag Offset          4000                   | 0b0100000000000000
    Reserved Bit:              0
    DF (Do not Fragment):      1
    MF (More Fragments):       0
    Fragment Offset:           0x0                    | 0
  Protocol                     01                     | 1
  Source IP                    0a000047               | 10.0.0.71
  Destination IP               0a000001               | 10.0.0.1
                                  Parsing ICMP Header
------------------------------------------------------------------------------------------
ICMP Header:
  Type                         08                     | 8
  Code                         00                     | 0
  Checksum                     7d58                   | 32088
------------------------------------ICMP Payload------------------------------------------
101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
==========================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ 
```

Sat Feb 1 10:01 PM
100%
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination
148	14.273315613	10.0.0.71	10.0.0.1
149	14.280431210	10.0.0.1	10.0.0.71
150	15.274537127	10.0.0.71	10.0.0.1
153	15.279857140	10.0.0.1	10.0.0.71

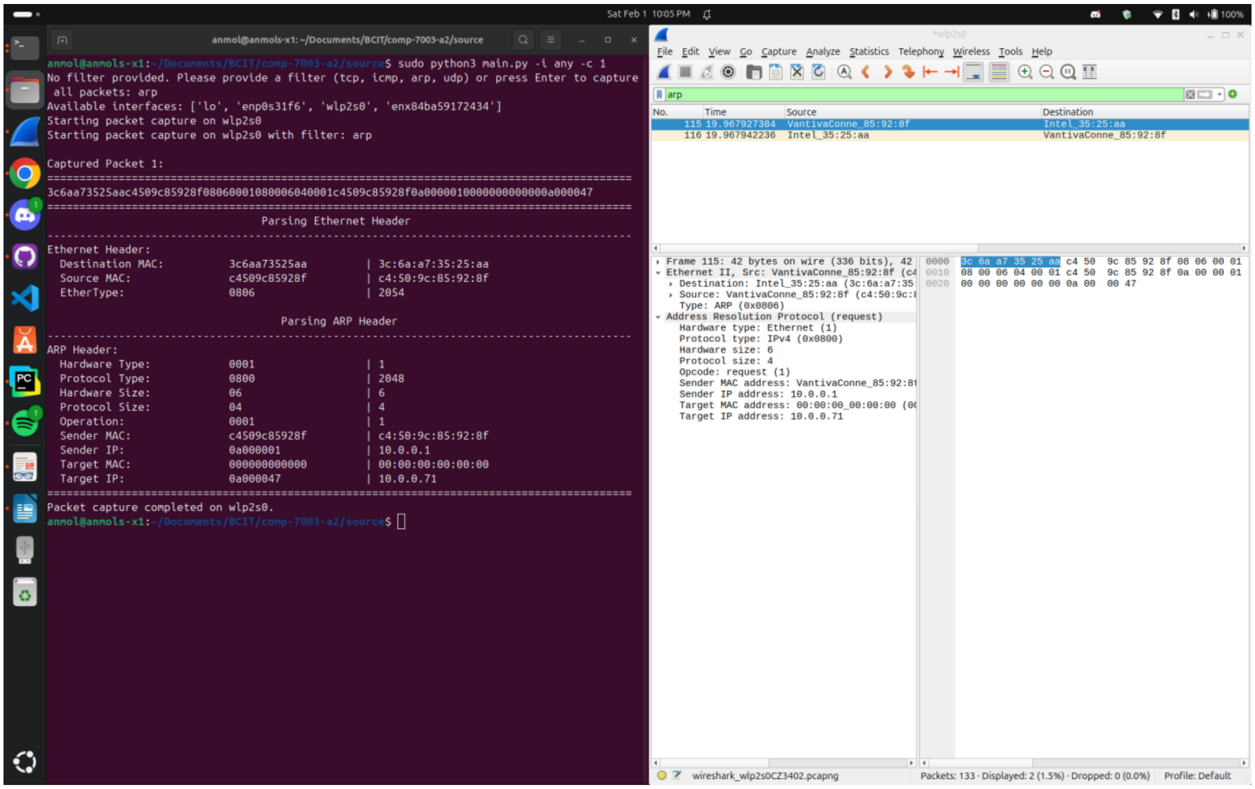
```
Frame 148: 98 bytes on wire (784 bits), 98
Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:
Internet Protocol Version 4, Src: 10.0.0.71
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP
    Total Length: 84
    Identification: 0x7084 (28804)
  010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xb5dd [validation disab
    [Header checksum status: Unverified]
    Source Address: 10.0.0.71
    Destination Address: 10.0.0.1
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x7d58 [correct]
    [Checksum Status: Good]
    Identifier (BE): 8769 (0x2241)
    Identifier (LE): 16674 (0x4122)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 149]
    Timestamp from icmp data: Feb  1, 2025 22
    [Timestamp from icmp data (relative): 0.0
  Data (40 bytes)
```

```
0000  c4 50 9c 85 92 8f 3c 6a  a7 35 25 aa 08 00 45 00
0010  00 54 70 84 40 00 40 01  b5 dd 0a 00 00 47 0a 00
0020  00 01 08 00 7d 58 22 41  00 01 33 0a 9f 67 00 00
0030  00 00 bd 20 0a 00 00 00  00 00 10 11 12 13 14 15
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35
0060  36 37
```

Data (data), 40 bytes

Packets: 157 · Displayed: 4 (2.5%) · Dropped: 0 (0.0%)   Profile: Default

Test 09


Sat Feb 1 10:05 PM
100%
anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -c 1
No filter provided. Please provide a filter (tcp, icmp, arp, udp) or press Enter to capture
 all packets: arp
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: arp

Captured Packet 1:
===========================================================================================
3c6aa73525aac4509c85928f08060001080006040001c4509c85928f0a000001000000000000000a000047
===========================================================================================
                                 Parsing Ethernet Header
-------------------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:            3c6aa73525aa          | 3c:6a:a7:35:25:aa
  Source MAC:                 c4509c85928f          | c4:50:9c:85:92:8f
  EtherType:                  0806                  | 2054

                                   Parsing ARP Header
-------------------------------------------------------------------------------------------
ARP Header:
  Hardware Type:              0001                  | 1
  Protocol Type:              0800                  | 2048
  Hardware Size:              06                    | 6
  Protocol Size:              04                    | 4
  Operation:                  0001                  | 1
  Sender MAC:                 c4509c85928f          | c4:50:9c:85:92:8f
  Sender IP:                  0a000001              | 10.0.0.1
  Target MAC:                 000000000000          | 00:00:00:00:00:00
  Target IP:                  0a000047              | 10.0.0.71
===========================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

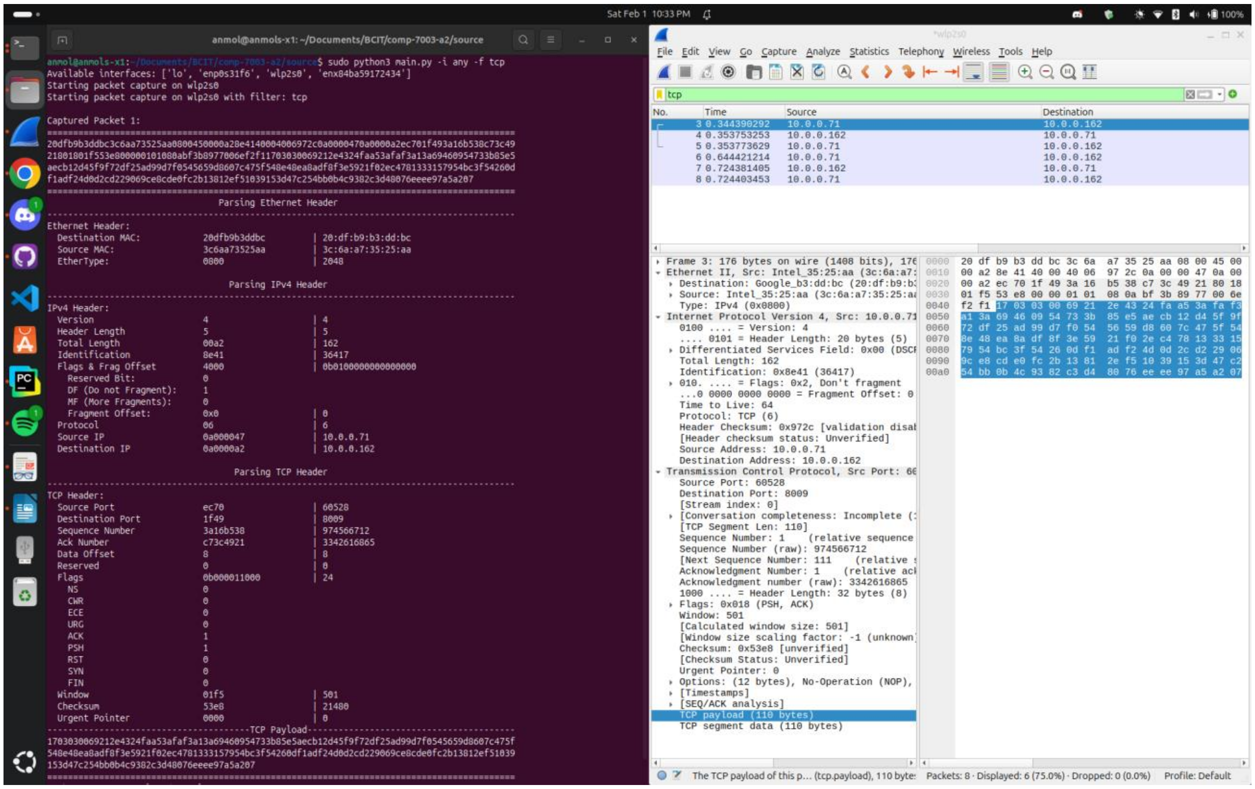
```
No.   Time           Source                     Destination
  115 19.967927384   VantivaConne_85:92:8f      Intel_35:25:aa
  116 19.967942236   Intel_35:25:aa             VantivaConne_85:92:8f
```

```
▸ Frame 115: 42 bytes on wire (336 bits), 42
▾ Ethernet II, Src: VantivaConne_85:92:8f (c4
  ▸ Destination: Intel_35:25:aa (3c:6a:a7:35
  ▸ Source: VantivaConne_85:92:8f (c4:50:9c:8
    Type: ARP (0x0806)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: VantivaConne_85:92:8f
    Sender IP address: 10.0.0.1
    Target MAC address: 00:00:00_00:00:00 (00
    Target IP address: 10.0.0.71
```

```
0000  3c 6a a7 35 25 aa c4 50  9c 85 92 8f 08 06 00 01
0010  08 00 06 04 00 01 c4 50  9c 85 92 8f 0a 00 00 01
0020  00 00 00 00 00 00 0a 00  00 47
```

wireshark_wlp2s0CZ3402.pcapng   Packets: 133 · Displayed: 2 (1.5%) · Dropped: 0 (0.0%)   Profile: Default

Test 10


Sat Feb 1 10:33 PM
100%
anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -f tcp
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: tcp

Captured Packet 1:
===========================================================================================
20dfb9b3ddbc3c6aa73525aa0800450000a28e4140004006972c0a0000470a0000a2ec701f493a16b538c73c49
21801801f553e800000101080abf3b8977006ef2f117030300069212e4324faa53afaf3a13a69460954733b85e5
aecb12d45f9f72df25ad99d7f0545659d8607c475f548e48ea8adf8f3e5921f02ec4781333157954bc3f54260d
f1adf24d0d2cd229069ce8cde0fc2b13812ef51039153d47c254bb0b4c9382c3d48076eeee97a5a207
===========================================================================================
                                 Parsing Ethernet Header
-------------------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:            20dfb9b3ddbc          | 20:df:b9:b3:dd:bc
  Source MAC:                 3c6aa73525aa          | 3c:6a:a7:35:25:aa
  EtherType:                  0800                  | 2048

                                   Parsing IPv4 Header
-------------------------------------------------------------------------------------------
IPv4 Header:
  Version                     4                     | 4
  Header Length               5                     | 5
  Total Length                00a2                  | 162
  Identification              8e41                  | 36417
  Flags & Frag Offset         4000                  | 0b0100000000000000
    Reserved Bit:             0
    DF (Do not Fragment):     1
    MF (More Fragments):      0
    Fragment Offset:          0x0                   | 0
  Protocol                    06                    | 6
  Source IP                   0a000047              | 10.0.0.71
  Destination IP              0a0000a2              | 10.0.0.162

                                   Parsing TCP Header
-------------------------------------------------------------------------------------------
TCP Header:
  Source Port                 ec70                  | 60528
  Destination Port            1f49                  | 8009
  Sequence Number             3a16b538              | 974566712
  Ack Number                  c73c4921              | 3342616865
  Data Offset                 8                     | 8
  Reserved                    0                     | 0
  Flags                       0b000011000           | 24
    NS                        0
    CWR                       0
    ECE                       0
    URG                       0
    ACK                       1
    PSH                       1
    RST                       0
    SYN                       0
    FIN                       0
  Window                      01f5                  | 501
  Checksum                    53e8                  | 21480
  Urgent Pointer              0000                  | 0
---------------------------------------TCP Payload-----------------------------------------
1703030069212e4324faa53afaf3a13a69460954733b85e5aecb12d45f9f72df25ad99d7f0545659d8607c475f
548e48ea8adf8f3e5921f02ec4781333157954bc3f54260df1adf24d0d2cd229069ce8cde0fc2b13812ef51039
153d47c254bb0b4c9382c3d48076eeee97a5a207
===========================================================================================
```

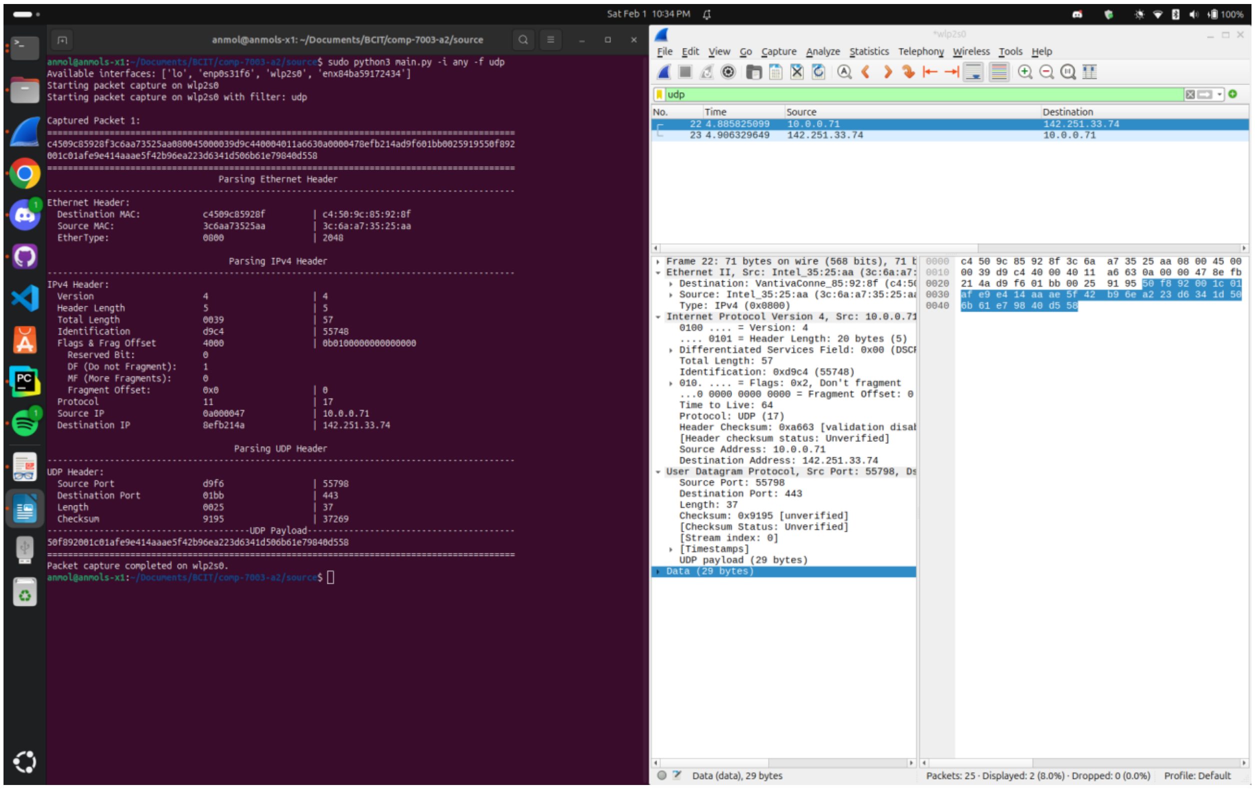
```
No.   Time           Source         Destination
    3 0.344390292    10.0.0.71      10.0.0.162
    4 0.353753253    10.0.0.162     10.0.0.71
    5 0.353773629    10.0.0.71      10.0.0.162
    6 0.644421214    10.0.0.71      10.0.0.162
    7 0.724381405    10.0.0.162     10.0.0.71
    8 0.724403453    10.0.0.71      10.0.0.162
```

```
▸ Frame 3: 176 bytes on wire (1408 bits), 176
▾ Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:
  ▸ Destination: Google_b3:dd:bc (20:df:b9:b3
  ▸ Source: Intel_35:25:aa (3c:6a:a7:35:25:aa
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.0.71
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP
    Total Length: 162
    Identification: 0x8e41 (36417)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x972c [validation disab
    [Header checksum status: Unverified]
    Source Address: 10.0.0.71
    Destination Address: 10.0.0.162
▾ Transmission Control Protocol, Src Port: 60
    Source Port: 60528
    Destination Port: 8009
    [Stream index: 0]
  ▸ [Conversation completeness: Incomplete (1
    [TCP Segment Len: 110]
    Sequence Number: 1    (relative sequence
    Sequence Number (raw): 974566712
    [Next Sequence Number: 111    (relative s
    Acknowledgment Number: 1    (relative ack
    Acknowledgment number (raw): 3342616865
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 501
    [Calculated window size: 501]
    [Window size scaling factor: -1 (unknown)
    Checksum: 0x53e8 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP),
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (110 bytes)
    TCP segment data (110 bytes)
```

```
0000  20 df b9 b3 dd bc 3c 6a  a7 35 25 aa 08 00 45 00
0010  00 a2 8e 41 40 00 40 06  97 2c 0a 00 00 47 0a 00
0020  00 a2 ec 70 1f 49 3a 16  b5 38 c7 3c 49 21 80 18
0030  01 f5 53 e8 00 00 01 01  08 0a bf 3b 89 77 00 6e
0040  f2 f1 17 03 03 00 69 21  2e 43 24 fa a5 3a fa f3
0050  a1 3a 69 46 09 54 73 3b  85 e5 ae cb 12 d4 5f 9f
0060  72 df 25 ad 99 d7 f0 54  56 59 d8 60 7c 47 5f 54
0070  8e 48 ea 8a df 8f 3e 59  21 f0 2e c4 78 13 33 15
0080  79 54 bc 3f 54 26 0d f1  ad f2 4d 0d 2c d2 29 06
0090  9c e8 cd e0 fc 2b 13 81  2e f5 10 39 15 3d 47 c2
00a0  54 bb 0b 4c 93 82 c3 d4  80 76 ee ee 97 a5 a2 07
```

The TCP payload of this p… (tcp.payload), 110 byte: Packets: 8 · Displayed: 6 (75.0%) · Dropped: 0 (0.0%)   Profile: Default

Test 11



Sat Feb 1 10:34 PM
100%
anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -f udp
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: udp

Captured Packet 1:
==========================================================================================
c4509c85928f3c6aa73525aa080045000039d9c440004011a6630a0000478efb214ad9f601bb0025919550f892
001c01afe9e414aaae5f42b96ea223d6341d506b61e79840d558
==========================================================================================
                                 Parsing Ethernet Header
------------------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:            c4509c85928f          | c4:50:9c:85:92:8f
  Source MAC:                 3c6aa73525aa          | 3c:6a:a7:35:25:aa
  EtherType:                  0800                  | 2048

                                   Parsing IPv4 Header
------------------------------------------------------------------------------------------
IPv4 Header:
  Version                     4                     | 4
  Header Length               5                     | 5
  Total Length                0039                  | 57
  Identification              d9c4                  | 55748
  Flags & Frag Offset         4000                  | 0b0100000000000000
    Reserved Bit:             0
    DF (Do not Fragment):     1
    MF (More Fragments):      0
    Fragment Offset:          0x0                   | 0
  Protocol                    11                    | 17
  Source IP                   0a000047              | 10.0.0.71
  Destination IP              8efb214a              | 142.251.33.74

                                    Parsing UDP Header
------------------------------------------------------------------------------------------
UDP Header:
  Source Port                 d9f6                  | 55798
  Destination Port            01bb                  | 443
  Length                      0025                  | 37
  Checksum                    9195                  | 37269
---------------------------------------UDP Payload----------------------------------------
50f892001c01afe9e414aaae5f42b96ea223d6341d506b61e79840d558
==========================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ 
```

```
No.   Time          Source          Destination
 22 4.885825099    10.0.0.71       142.251.33.74
 23 4.906329649    142.251.33.74   10.0.0.71
```

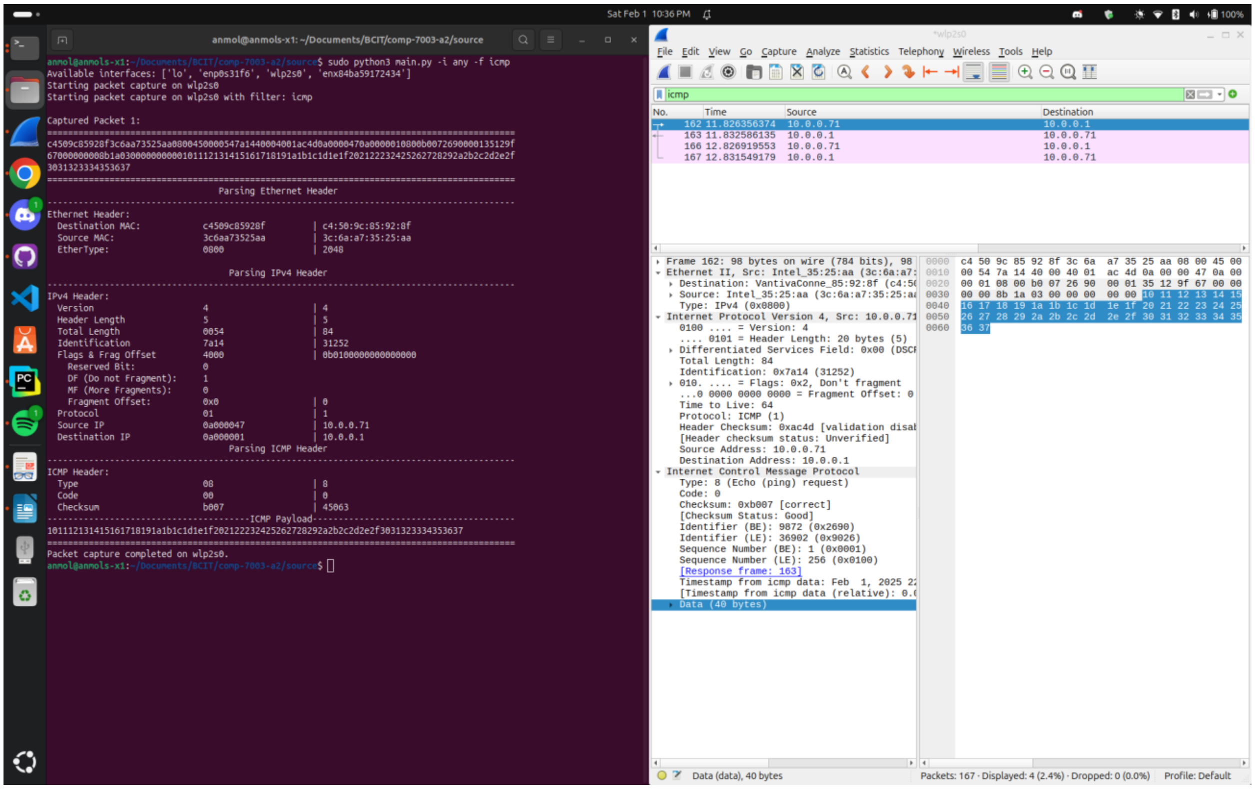
```
› Frame 22: 71 bytes on wire (568 bits), 71 b
⌄ Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:
  › Destination: VantivaConne_85:92:8f (c4:50
  › Source: Intel_35:25:aa (3c:6a:a7:35:25:aa
    Type: IPv4 (0x0800)
⌄ Internet Protocol Version 4, Src: 10.0.0.71
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP
    Total Length: 57
    Identification: 0xd9c4 (55748)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xa663 [validation disab
    [Header checksum status: Unverified]
    Source Address: 10.0.0.71
    Destination Address: 142.251.33.74
⌄ User Datagram Protocol, Src Port: 55798, Ds
    Source Port: 55798
    Destination Port: 443
    Length: 37
    Checksum: 0x9195 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  › [Timestamps]
    UDP payload (29 bytes)
› Data (29 bytes)
```

```
0000  c4 50 9c 85 92 8f 3c 6a  a7 35 25 aa 08 00 45 00
0010  00 39 d9 c4 40 00 40 11  a6 63 0a 00 00 47 8e fb
0020  21 4a d9 f6 01 bb 00 25  91 95 50 f8 92 00 1c 01
0030  af e9 e4 14 aa ae 5f 42  b9 6e a2 23 d6 34 1d 50
0040  6b 61 e7 98 40 d5 58
```

Data (data), 29 bytes

Packets: 25 · Displayed: 2 (8.0%) · Dropped: 0 (0.0%)   Profile: Default

Test 12



Sat Feb 1 10:36 PM
100%
anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -f icmp
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: icmp

Captured Packet 1:
==========================================================================================
c4509c85928f3c6aa73525aa08004500000547a1440004001ac4d0a0000470a0000010800b00726900001351 29f
67000000008b1a03000000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f
3031323334353637
==========================================================================================
                                 Parsing Ethernet Header
------------------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:            c4509c85928f          | c4:50:9c:85:92:8f
  Source MAC:                 3c6aa73525aa          | 3c:6a:a7:35:25:aa
  EtherType:                  0800                  | 2048

                                   Parsing IPv4 Header
------------------------------------------------------------------------------------------
IPv4 Header:
  Version                     4                     | 4
  Header Length               5                     | 5
  Total Length                0054                  | 84
  Identification              7a14                  | 31252
  Flags & Frag Offset         4000                  | 0b0100000000000000
    Reserved Bit:             0
    DF (Do not Fragment):     1
    MF (More Fragments):      0
    Fragment Offset:          0x0                   | 0
  Protocol                    01                    | 1
  Source IP                   0a000047              | 10.0.0.71
  Destination IP              0a000001              | 10.0.0.1
                                   Parsing ICMP Header
------------------------------------------------------------------------------------------
ICMP Header:
  Type                        08                    | 8
  Code                        00                    | 0
  Checksum                    b007                  | 45063
---------------------------------------ICMP Payload---------------------------------------
101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
==========================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ 
```

```
No.   Time           Source       Destination
 162 11.826356374   10.0.0.71    10.0.0.1
 163 11.832586135   10.0.0.1     10.0.0.71
 166 12.826919553   10.0.0.71    10.0.0.1
 167 12.831549179   10.0.0.1     10.0.0.71
```

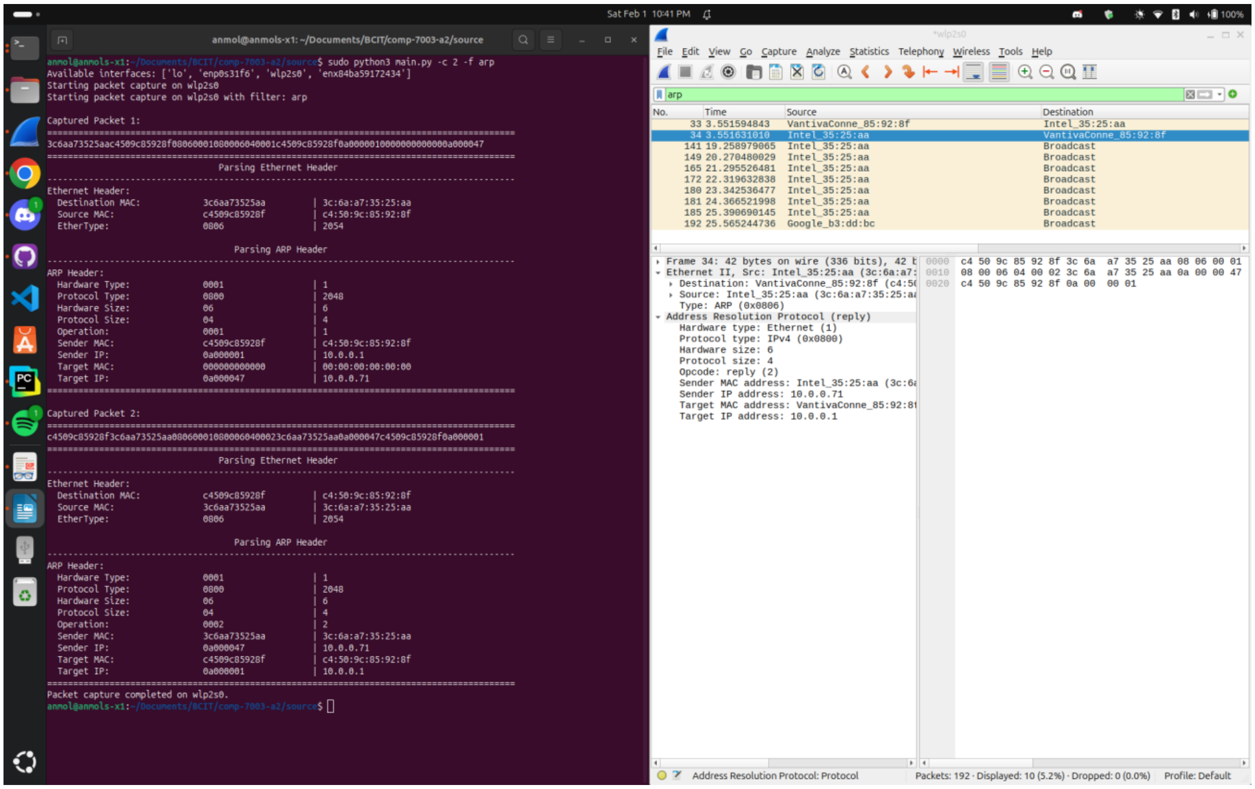
```
› Frame 162: 98 bytes on wire (784 bits), 98
⌄ Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:
  › Destination: VantivaConne_85:92:8f (c4:50
  › Source: Intel_35:25:aa (3c:6a:a7:35:25:aa
    Type: IPv4 (0x0800)
⌄ Internet Protocol Version 4, Src: 10.0.0.71
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP
    Total Length: 84
    Identification: 0x7a14 (31252)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xac4d [validation disab
    [Header checksum status: Unverified]
    Source Address: 10.0.0.71
    Destination Address: 10.0.0.1
⌄ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xb007 [correct]
    [Checksum Status: Good]
    Identifier (BE): 9872 (0x2690)
    Identifier (LE): 36902 (0x9026)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 163]
    Timestamp from icmp data: Feb  1, 2025 22
    [Timestamp from icmp data (relative): 0.0
  › Data (40 bytes)
```

```
0000  c4 50 9c 85 92 8f 3c 6a  a7 35 25 aa 08 00 45 00
0010  00 54 7a 14 40 00 40 01  ac 4d 0a 00 00 47 0a 00
0020  00 01 08 00 b0 07 26 90  00 01 35 12 9f 67 00 00
0030  00 00 8b 1a 03 00 00 00  00 00 10 11 12 13 14 15
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35
0060  36 37
```

Data (data), 40 bytes

Packets: 167 · Displayed: 4 (2.4%) · Dropped: 0 (0.0%)   Profile: Default

Test 13



```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -c 2 -f arp
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: arp

Captured Packet 1:
================================================================================
3c6aa73525aac4509c85928f08060001080006040001c4509c85928f0a0000010000000000000a000047
================================================================================
                          Parsing Ethernet Header
--------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:             3c6aa73525aa           | 3c:6a:a7:35:25:aa
  Source MAC:                  c4509c85928f           | c4:50:9c:85:92:8f
  EtherType:                   0806                   | 2054

                            Parsing ARP Header
--------------------------------------------------------------------------------
ARP Header:
  Hardware Type:               0001                   | 1
  Protocol Type:               0800                   | 2048
  Hardware Size:               06                     | 6
  Protocol Size:               04                     | 4
  Operation:                   0001                   | 1
  Sender MAC:                  c4509c85928f           | c4:50:9c:85:92:8f
  Sender IP:                   0a000001               | 10.0.0.1
  Target MAC:                  000000000000           | 00:00:00:00:00:00
  Target IP:                   0a000047               | 10.0.0.71
================================================================================

Captured Packet 2:
================================================================================
c4509c85928f3c6aa73525aa08060001080006040002 3c6aa73525aa0a000047c4509c85928f0a000001
================================================================================
                          Parsing Ethernet Header
--------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:             c4509c85928f           | c4:50:9c:85:92:8f
  Source MAC:                  3c6aa73525aa           | 3c:6a:a7:35:25:aa
  EtherType:                   0806                   | 2054

                            Parsing ARP Header
--------------------------------------------------------------------------------
ARP Header:
  Hardware Type:               0001                   | 1
  Protocol Type:               0800                   | 2048
  Hardware Size:               06                     | 6
  Protocol Size:               04                     | 4
  Operation:                   0002                   | 2
  Sender MAC:                  3c6aa73525aa           | 3c:6a:a7:35:25:aa
  Sender IP:                   0a000047               | 10.0.0.71
  Target MAC:                  c4509c85928f           | c4:50:9c:85:92:8f
  Target IP:                   0a000001               | 10.0.0.1
================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

```
No.  Time          Source                    Destination
 33 3.551594843   VantivaConne_85:92:8f     Intel_35:25:aa
 34 3.551631010   Intel_35:25:aa            VantivaConne_85:92:8f
141 19.258979065  Intel_35:25:aa            Broadcast
149 20.270480029  Intel_35:25:aa            Broadcast
165 21.295526481  Intel_35:25:aa            Broadcast
172 22.319632838  Intel_35:25:aa            Broadcast
180 23.342536477  Intel_35:25:aa            Broadcast
181 24.366521998  Intel_35:25:aa            Broadcast
185 25.390690145  Intel_35:25:aa            Broadcast
192 25.565244736  Google_b3:dd:bc           Broadcast
```

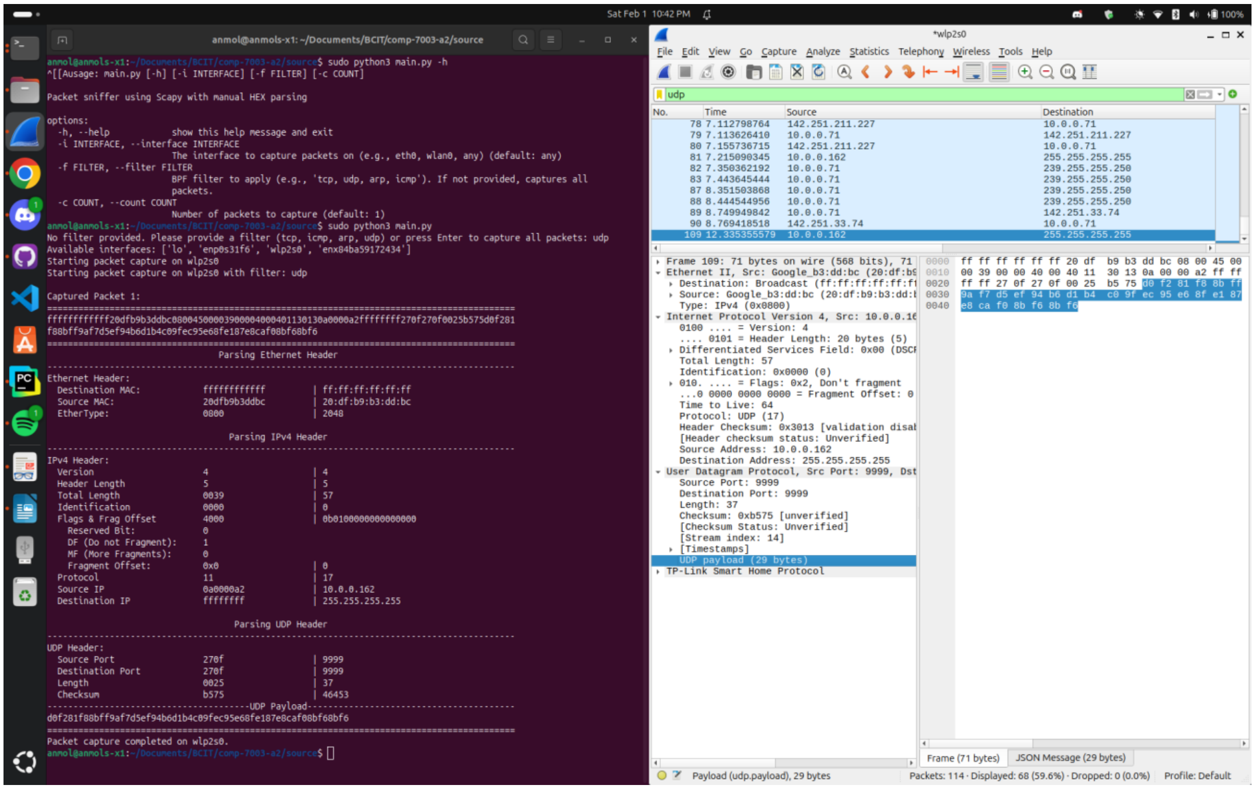
```
› Frame 34: 42 bytes on wire (336 bits), 42 b
⌄ Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:
  › Destination: VantivaConne_85:92:8f (c4:50
  › Source: Intel_35:25:aa (3c:6a:a7:35:25:aa
    Type: ARP (0x0806)
⌄ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Intel_35:25:aa (3c:6a
    Sender IP address: 10.0.0.71
    Target MAC address: VantivaConne_85:92:8f
    Target IP address: 10.0.0.1
```

```
0000  c4 50 9c 85 92 8f 3c 6a  a7 35 25 aa 08 06 00 01
0010  08 00 06 04 00 02 3c 6a  a7 35 25 aa 0a 00 00 47
0020  c4 50 9c 85 92 8f 0a 00  00 01
```

Address Resolution Protocol: Protocol   Packets: 192 · Displayed: 10 (5.2%) · Dropped: 0 (0.0%)   Profile: Default

Sat Feb 1 10:41 PM
100%
anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

Test 14



```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -h
^[[Ausage: main.py [-h] [-i INTERFACE] [-f FILTER] [-c COUNT]

Packet sniffer using Scapy with manual HEX parsing

options:
  -h, --help            show this help message and exit
  -i INTERFACE, --interface INTERFACE
                        The interface to capture packets on (e.g., eth0, wlan0, any) (default: any)
  -f FILTER, --filter FILTER
                        BPF filter to apply (e.g., 'tcp, udp, arp, icmp'). If not provided, captures all
                        packets.
  -c COUNT, --count COUNT
                        Number of packets to capture (default: 1)
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py
No filter provided. Please provide a filter (tcp, icmp, arp, udp) or press Enter to capture all packets: udp
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: udp

Captured Packet 1:
================================================================================
ffffffffffff20dfb9b3ddbc080045000039000040004011 30130a0000a2ffffffff270f270f0025b575d0f281
f88bff9af7d5ef94b6d1b4c09fec95e68fe187e8caf08bf68bf6
================================================================================
                          Parsing Ethernet Header
--------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:             ffffffffffff           | ff:ff:ff:ff:ff:ff
  Source MAC:                  20dfb9b3ddbc           | 20:df:b9:b3:dd:bc
  EtherType:                   0800                   | 2048

                            Parsing IPv4 Header
--------------------------------------------------------------------------------
IPv4 Header:
  Version                      4                      | 4
  Header Length                5                      | 5
  Total Length                 0039                   | 57
  Identification               0000                   | 0
  Flags & Frag Offset          4000                   | 0b0100000000000000
    Reserved Bit:              0
    DF (Do not Fragment):      1
    MF (More Fragments):       0
    Fragment Offset:           0x0                    | 0
  Protocol                     11                     | 17
  Source IP                    0a0000a2               | 10.0.0.162
  Destination IP               ffffffff               | 255.255.255.255

                            Parsing UDP Header
--------------------------------------------------------------------------------
UDP Header:
  Source Port                  270f                   | 9999
  Destination Port             270f                   | 9999
  Length                       0025                   | 37
  Checksum                     b575                   | 46453
-----------------------------------UDP Payload----------------------------------
d0f281f88bff9af7d5ef94b6d1b4c09fec95e68fe187e8caf08bf68bf6
================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

```
No.  Time          Source            Destination
 78 7.112798764   142.251.211.227   10.0.0.71
 79 7.113626410   10.0.0.71         142.251.211.227
 80 7.155736715   142.251.211.227   10.0.0.71
 81 7.215090345   10.0.0.162        255.255.255.255
 82 7.350362192   10.0.0.71         239.255.255.250
 83 7.443645444   10.0.0.71         239.255.255.250
 87 8.351503868   10.0.0.71         239.255.255.250
 88 8.444544956   10.0.0.71         239.255.255.250
 89 8.749949842   10.0.0.71         142.251.33.74
 90 8.769418518   142.251.33.74     10.0.0.71
109 12.335355579  10.0.0.162        255.255.255.255
```

```
› Frame 109: 71 bytes on wire (568 bits), 71
⌄ Ethernet II, Src: Google_b3:dd:bc (20:df:b9
  › Destination: Broadcast (ff:ff:ff:ff:ff:ff
  › Source: Google_b3:dd:bc (20:df:b9:b3:dd:b
    Type: IPv4 (0x0800)
⌄ Internet Protocol Version 4, Src: 10.0.0.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP
    Total Length: 57
    Identification: 0x0000 (0)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x3013 [validation disal
    [Header checksum status: Unverified]
    Source Address: 10.0.0.162
    Destination Address: 255.255.255.255
⌄ User Datagram Protocol, Src Port: 9999, Dst
    Source Port: 9999
    Destination Port: 9999
    Length: 37
    Checksum: 0xb575 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 14]
  › [Timestamps]
    UDP payload (29 bytes)
› TP-Link Smart Home Protocol
```

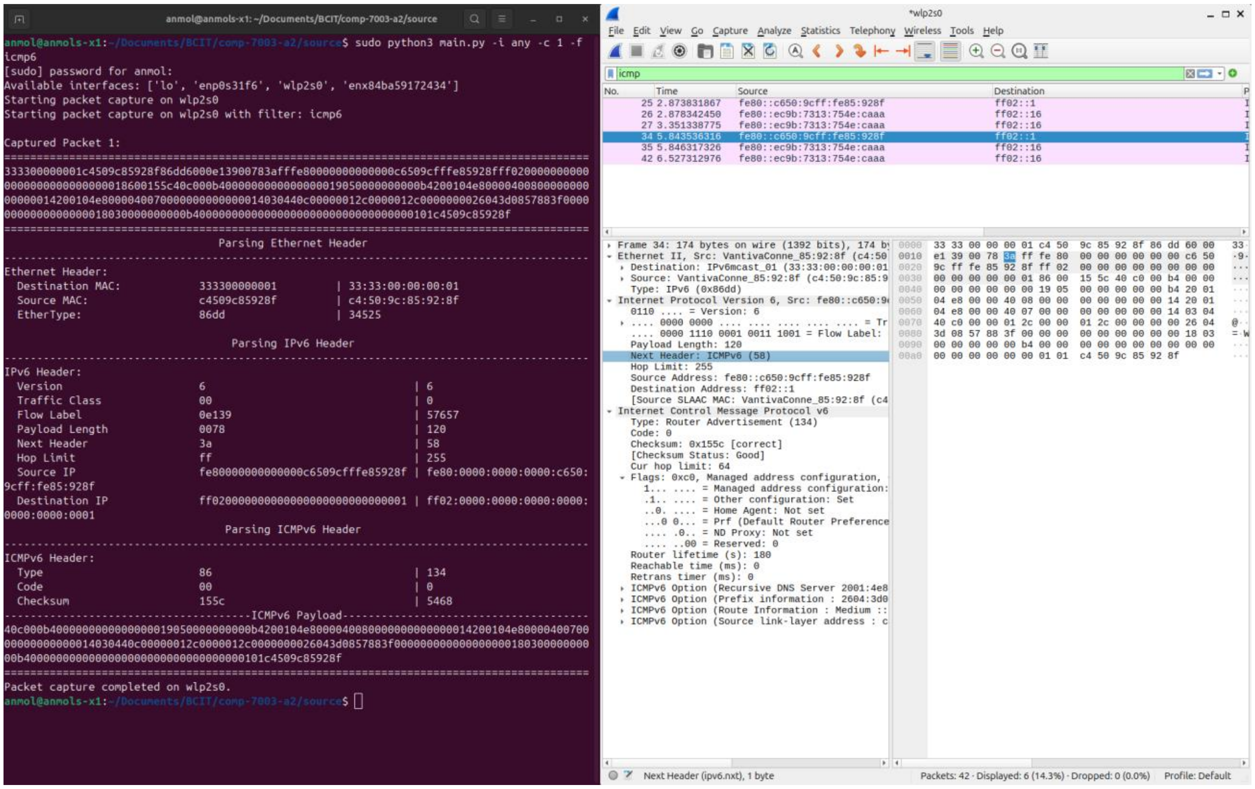
```
0000  ff ff ff ff ff ff 20 df  b9 b3 dd bc 08 00 45 00
0010  00 39 00 00 40 00 40 11  30 13 0a 00 00 a2 ff ff
0020  ff ff 27 0f 27 0f 00 25  b5 75 d0 f2 81 f8 8b ff
0030  9a f7 d5 ef 94 b6 d1 b4  c0 9f ec 95 e6 8f e1 87
0040  e8 ca f0 8b f6 8b f6
```

Frame (71 bytes)   JSON Message (29 bytes)

Payload (udp.payload), 29 bytes   Packets: 114 · Displayed: 68 (59.6%) · Dropped: 0 (0.0%)   Profile: Default

Sat Feb 1 10:42 PM
100%
anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp

Test 15


anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination

```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -c 1 -f
icmp6
[sudo] password for anmol:
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: icmp6

Captured Packet 1:
================================================================================
333300000001c4509c85928f86dd6000e13900783afffe80000000000000c6509cfffe85928fff020000000000
00000000000000000018600155c40c000b4000000000000000019050000000000b4200104e80000400800000000
0000014200104e8000040070000000000000014030440c00000012c0000012c0000000026043d0857883f0000
00000000000000180300000000b40000000000000000000000000000000000101c4509c85928f
================================================================================
                          Parsing Ethernet Header
--------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:            333300000001         | 33:33:00:00:00:01
  Source MAC:                 c4509c85928f         | c4:50:9c:85:92:8f
  EtherType:                  86dd                 | 34525

                            Parsing IPv6 Header
--------------------------------------------------------------------------------
IPv6 Header:
  Version                     6                                | 6
  Traffic Class               00                               | 0
  Flow Label                  0e139                            | 57657
  Payload Length              0078                             | 120
  Next Header                 3a                               | 58
  Hop Limit                   ff                               | 255
  Source IP                   fe80000000000000c6509cfffe85928f | fe80:0000:0000:0000:c650:
9cff:fe85:928f
  Destination IP              ff020000000000000000000000000001 | ff02:0000:0000:0000:0000:
0000:0000:0001
                            Parsing ICMPv6 Header
--------------------------------------------------------------------------------
ICMPv6 Header:
  Type                        86                               | 134
  Code                        00                               | 0
  Checksum                    155c                             | 5468
-----------------------------------ICMPv6 Payload-------------------------------------
40c000b4000000000000000019050000000000b4200104e800004008000000000000014200104e80000400700
000000000000014030440c00000012c0000012c0000000026043d0857883f00000000000000000180300000000
00b40000000000000000000000000000000000101c4509c85928f
================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

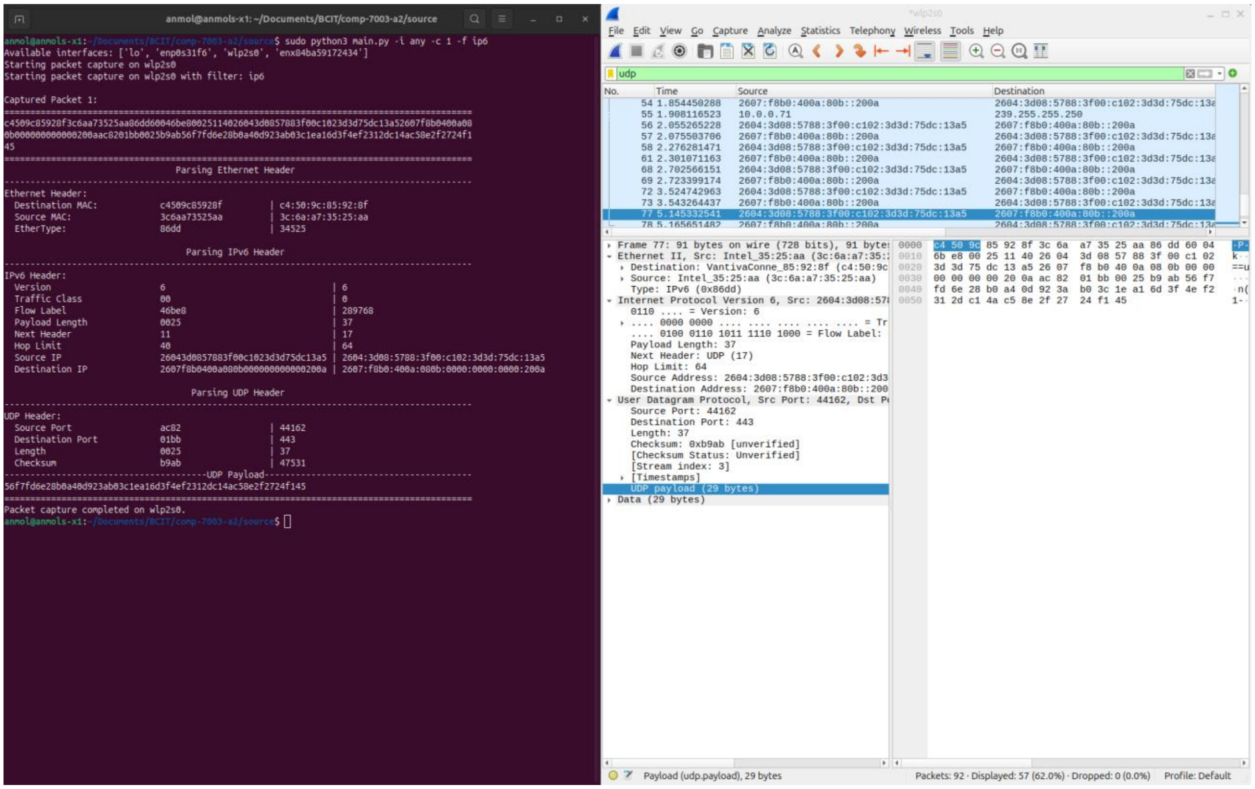
```
No.  Time          Source                       Destination
  25 2.873831867   fe80::c650:9cff:fe85:928f    ff02::1
  26 2.878342450   fe80::ec9b:7313:754e:caaa    ff02::16
  27 3.351338775   fe80::ec9b:7313:754e:caaa    ff02::16
  34 5.843536316   fe80::c650:9cff:fe85:928f    ff02::1
  35 5.846317326   fe80::ec9b:7313:754e:caaa    ff02::16
  42 6.527312976   fe80::ec9b:7313:754e:caaa    ff02::16
```

```
› Frame 34: 174 bytes on wire (1392 bits), 174 by
⌄ Ethernet II, Src: VantivaConne_85:92:8f (c4:50
  › Destination: IPv6mcast_01 (33:33:00:00:00:01
  › Source: VantivaConne_85:92:8f (c4:50:9c:85:9
    Type: IPv6 (0x86dd)
⌄ Internet Protocol Version 6, Src: fe80::c650:9
    0110 .... = Version: 6
  › .... 0000 0000 .... .... .... .... .... = Tr
    .... 0000 1110 0001 0011 1001 = Flow Label:
    Payload Length: 120
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: fe80::c650:9cff:fe85:928f
    Destination Address: ff02::1
    [Source SLAAC MAC: VantivaConne_85:92:8f (c4
⌄ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x155c [correct]
    [Checksum Status: Good]
    Cur hop limit: 64
  ⌄ Flags: 0xc0, Managed address configuration,
      1... .... = Managed address configuration:
      .1.. .... = Other configuration: Set
      ..0. .... = Home Agent: Not set
      ...0 0... = Prf (Default Router Preference
      .... .0.. = ND Proxy: Not set
      .... ..00 = Reserved: 0
    Router lifetime (s): 180
    Reachable time (ms): 0
    Retrans timer (ms): 0
  › ICMPv6 Option (Recursive DNS Server 2001:4e8
  › ICMPv6 Option (Prefix information : 2604:3d0
  › ICMPv6 Option (Route Information : Medium ::
  › ICMPv6 Option (Source link-layer address : c
```

```
0000  33 33 00 00 00 01 c4 50  9c 85 92 8f 86 dd 60 00
0010  e1 39 00 78 3a ff fe 80  00 00 00 00 00 00 c6 50
0020  9c ff fe 85 92 8f ff 02  00 00 00 00 00 00 00 00
0030  00 00 00 00 00 01 86 00  15 5c 40 c0 00 b4 00 00
0040  00 00 00 00 00 00 19 05  00 00 00 00 00 b4 20 01
0050  04 e8 00 00 40 08 00 00  00 00 00 00 00 14 20 01
0060  04 e8 00 00 40 07 00 00  00 00 00 00 00 14 03 04
0070  40 c0 00 00 01 2c 00 00  01 2c 00 00 00 00 26 04
0080  3d 08 57 88 3f 00 00 00  00 00 00 00 00 00 18 03
0090  00 00 00 00 00 b4 00 00  00 00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 01 01  c4 50 9c 85 92 8f
```

Next Header (ipv6.nxt), 1 byte   Packets: 42 · Displayed: 6 (14.3%) · Dropped: 0 (0.0%)   Profile: Default

Test 16


anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination

```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -c 1 -f ip6
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: ip6

Captured Packet 1:
================================================================================
c4509c85928f3c6aa73525aa86dd60046be80025114026043d0857883f00c1023d3d75dc13a52607f8b0400a08
0b000000000000200aac8201bb0025b9ab56f7fd6e28b0a40d923ab03c1ea16d3f4ef2312dc14ac58e2f2724f1
45
================================================================================
                          Parsing Ethernet Header
--------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:            c4509c85928f         | c4:50:9c:85:92:8f
  Source MAC:                 3c6aa73525aa         | 3c:6a:a7:35:25:aa
  EtherType:                  86dd                 | 34525

                            Parsing IPv6 Header
--------------------------------------------------------------------------------
IPv6 Header:
  Version                     6                                | 6
  Traffic Class               00                               | 0
  Flow Label                  46be8                            | 289768
  Payload Length              0025                             | 37
  Next Header                 11                               | 17
  Hop Limit                   40                               | 64
  Source IP                   26043d0857883f00c1023d3d75dc13a5 | 2604:3d08:5788:3f00:c102:3d3d:75dc:13a5
  Destination IP              2607f8b0400a080b000000000000200a | 2607:f8b0:400a:080b:0000:0000:0000:200a

                            Parsing UDP Header
--------------------------------------------------------------------------------
UDP Header:
  Source Port                 ac82                 | 44162
  Destination Port            01bb                 | 443
  Length                      0025                 | 37
  Checksum                    b9ab                 | 47531
-----------------------------------UDP Payload----------------------------------------
56f7fd6e28b0a40d923ab03c1ea16d3f4ef2312dc14ac58e2f2724f145
================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

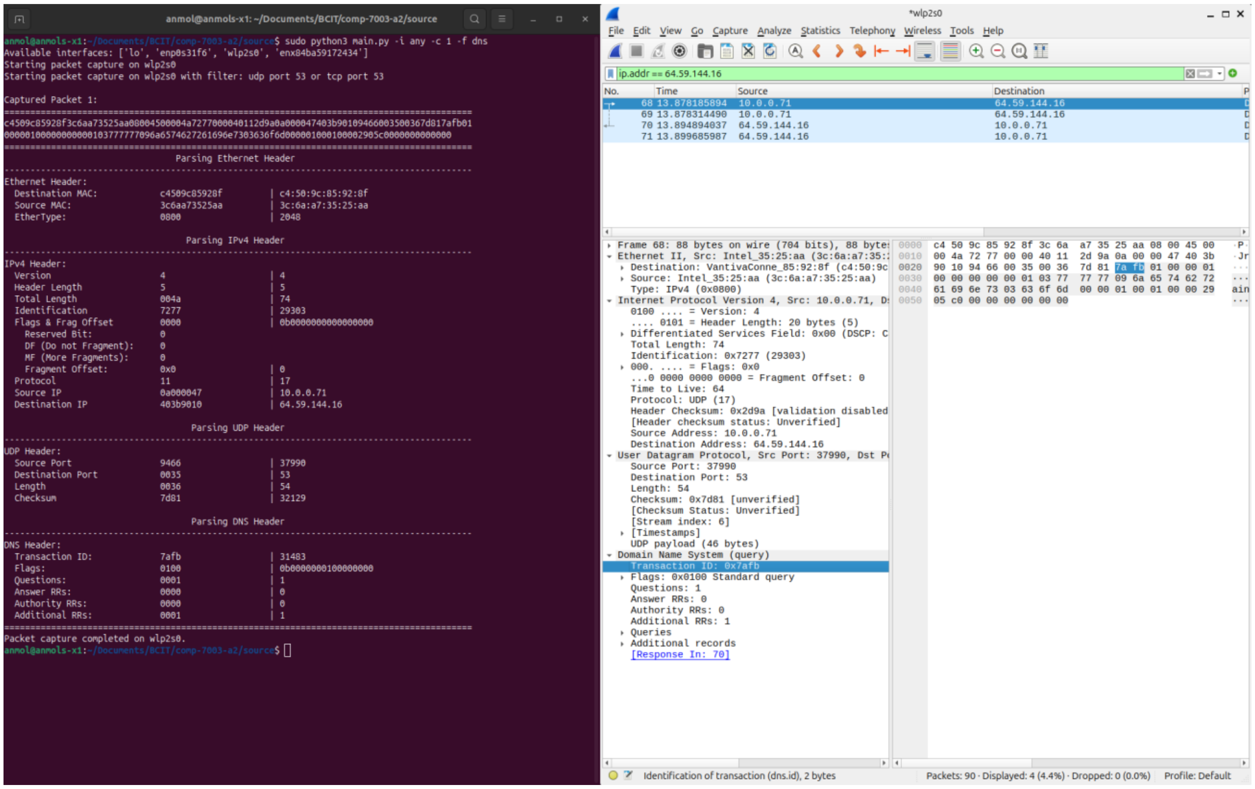
```
No.  Time          Source                                   Destination
  54 1.854450288   2607:f8b0:400a:80b::200a                 2604:3d08:5788:3f00:c102:3d3d:75dc:13a
  55 1.908116523   10.0.0.71                                239.255.255.250
  56 2.055265228   2604:3d08:5788:3f00:c102:3d3d:75dc:13a5  2607:f8b0:400a:80b::200a
  57 2.075503706   2607:f8b0:400a:80b::200a                 2604:3d08:5788:3f00:c102:3d3d:75dc:13a
  58 2.276281471   2604:3d08:5788:3f00:c102:3d3d:75dc:13a5  2607:f8b0:400a:80b::200a
  61 2.301071163   2607:f8b0:400a:80b::200a                 2604:3d08:5788:3f00:c102:3d3d:75dc:13a
  68 2.702566151   2604:3d08:5788:3f00:c102:3d3d:75dc:13a5  2607:f8b0:400a:80b::200a
  69 2.723399174   2607:f8b0:400a:80b::200a                 2604:3d08:5788:3f00:c102:3d3d:75dc:13a
  72 3.524742963   2604:3d08:5788:3f00:c102:3d3d:75dc:13a5  2607:f8b0:400a:80b::200a
  73 3.543264437   2607:f8b0:400a:80b::200a                 2604:3d08:5788:3f00:c102:3d3d:75dc:13a
  77 5.145332541   2604:3d08:5788:3f00:c102:3d3d:75dc:13a5  2607:f8b0:400a:80b::200a
  78 5.165651482   2607:f8b0:400a:80b::200a                 2604:3d08:5788:3f00:c102:3d3d:75dc:13a
```

```
› Frame 77: 91 bytes on wire (728 bits), 91 byte
⌄ Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:35::
  › Destination: VantivaConne_85:92:8f (c4:50:9c
  › Source: Intel_35:25:aa (3c:6a:a7:35:25:aa)
    Type: IPv6 (0x86dd)
⌄ Internet Protocol Version 6, Src: 2604:3d08:57
    0110 .... = Version: 6
  › .... 0000 0000 .... .... .... .... .... = Tr
    .... 0100 0110 1011 1110 1000 = Flow Label:
    Payload Length: 37
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2604:3d08:5788:3f00:c102:3d3
    Destination Address: 2607:f8b0:400a:80b::200
⌄ User Datagram Protocol, Src Port: 44162, Dst P
    Source Port: 44162
    Destination Port: 443
    Length: 37
    Checksum: 0xb9ab [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  › [Timestamps]
    UDP payload (29 bytes)
› Data (29 bytes)
```

```
0000  c4 50 9c 85 92 8f 3c 6a  a7 35 25 aa 86 dd 60 04
0010  6b e8 00 25 11 40 26 04  3d 08 57 88 3f 00 c1 02
0020  3d 3d 75 dc 13 a5 26 07  f8 b0 40 0a 08 0b 00 00
0030  00 00 00 00 20 0a ac 82  01 bb 00 25 b9 ab 56 f7
0040  fd 6e 28 b0 a4 0d 92 3a  b0 3c 1e a1 6d 3f 4e f2
0050  31 2d c1 4a c5 8e 2f 27  24 f1 45
```

Payload (udp.payload), 29 bytes   Packets: 92 · Displayed: 57 (62.0%) · Dropped: 0 (0.0%)   Profile: Default

Test 17



```
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ sudo python3 main.py -i any -c 1 -f dns
Available interfaces: ['lo', 'enp0s31f6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: udp port 53 or tcp port 53

Captured Packet 1:
==========================================================================================
c4509c85928f3c6aa73525aa08004500004a7277000040112d9a0a000047403b90109466003500367d817afb01
00000100000000000103777777096a6574627261696e7303636f6d000001000100002905c0000000000000
==========================================================================================
                                 Parsing Ethernet Header
------------------------------------------------------------------------------------------
Ethernet Header:
  Destination MAC:             c4509c85928f         | c4:50:9c:85:92:8f
  Source MAC:                  3c6aa73525aa         | 3c:6a:a7:35:25:aa
  EtherType:                   0800                 | 2048

                                   Parsing IPv4 Header
------------------------------------------------------------------------------------------
IPv4 Header:
  Version                      4                    | 4
  Header Length                5                    | 5
  Total Length                 004a                 | 74
  Identification               7277                 | 29303
  Flags & Frag Offset          0000                 | 0b0000000000000000
    Reserved Bit:              0
    DF (Do not Fragment):      0
    MF (More Fragments):       0
    Fragment Offset:           0x0                  | 0
  Protocol                     11                   | 17
  Source IP                    0a000047             | 10.0.0.71
  Destination IP               403b9010             | 64.59.144.16

                                    Parsing UDP Header
------------------------------------------------------------------------------------------
UDP Header:
  Source Port                  9466                 | 37990
  Destination Port             0035                 | 53
  Length                       0036                 | 54
  Checksum                     7d81                 | 32129

                                    Parsing DNS Header
------------------------------------------------------------------------------------------
DNS Header:
  Transaction ID:              7afb                 | 31483
  Flags:                       0100                 | 0b0000000100000000
  Questions:                   0001                 | 1
  Answer RRs:                  0000                 | 0
  Authority RRs:               0000                 | 0
  Additional RRs:              0001                 | 1
==========================================================================================
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$ 
```

*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 64.59.144.16

```
No.   Time          Source          Destination
   68 13.878185894  10.0.0.71       64.59.144.16
   69 13.878314490  10.0.0.71       64.59.144.16
   70 13.894894037  64.59.144.16    10.0.0.71
   71 13.899685987  64.59.144.16    10.0.0.71
```

```
▸ Frame 68: 88 bytes on wire (704 bits), 88 byte
▾ Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:35:
  ▸ Destination: VantivaConne_85:92:8f (c4:50:9c
  ▸ Source: Intel_35:25:aa (3c:6a:a7:35:25:aa)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.0.71, D
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: C
    Total Length: 74
    Identification: 0x7277 (29303)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x2d9a [validation disabled
    [Header checksum status: Unverified]
    Source Address: 10.0.0.71
    Destination Address: 64.59.144.16
▾ User Datagram Protocol, Src Port: 37990, Dst P
    Source Port: 37990
    Destination Port: 53
    Length: 54
    Checksum: 0x7d81 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
  ▸ [Timestamps]
    UDP payload (46 bytes)
▾ Domain Name System (query)
    Transaction ID: 0x7afb
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▸ Additional records
    [Response In: 70]
```

```
0000  c4 50 9c 85 92 8f 3c 6a  a7 35 25 aa 08 00 45 00   ·P·
0010  00 4a 72 77 00 00 40 11  2d 9a 0a 00 00 47 40 3b   ·Jr
0020  90 10 94 66 00 35 00 36  7d 81 7a fb 01 00 00 01   ···
0030  00 00 00 00 00 01 03 77  77 77 09 6a 65 74 62 72   ···
0040  61 69 6e 73 03 63 6f 6d  00 00 01 00 01 00 00 29   ain
0050  05 c0 00 00 00 00 00 00                            ···
```

Identification of transaction (dns.id), 2 bytes   Packets: 90 · Displayed: 4 (4.4%) · Dropped: 0 (0.0%)   Profile: Default