COMP 7003
Introduction to Information and Network Security

Assignment-02

Testing

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

Tests 4
Test 01 4
Test 02 4
Test 03 4
Test 04 5
Test 05 5
Test 06 5
Test 07 6
Test 08 6
Test 09 7
Test 10 7
Test 11 8
Test 12 8
Test 13 9
Test 14 9
Test 15 10
Test 16 10
Test 17 11

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	pass	pass	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

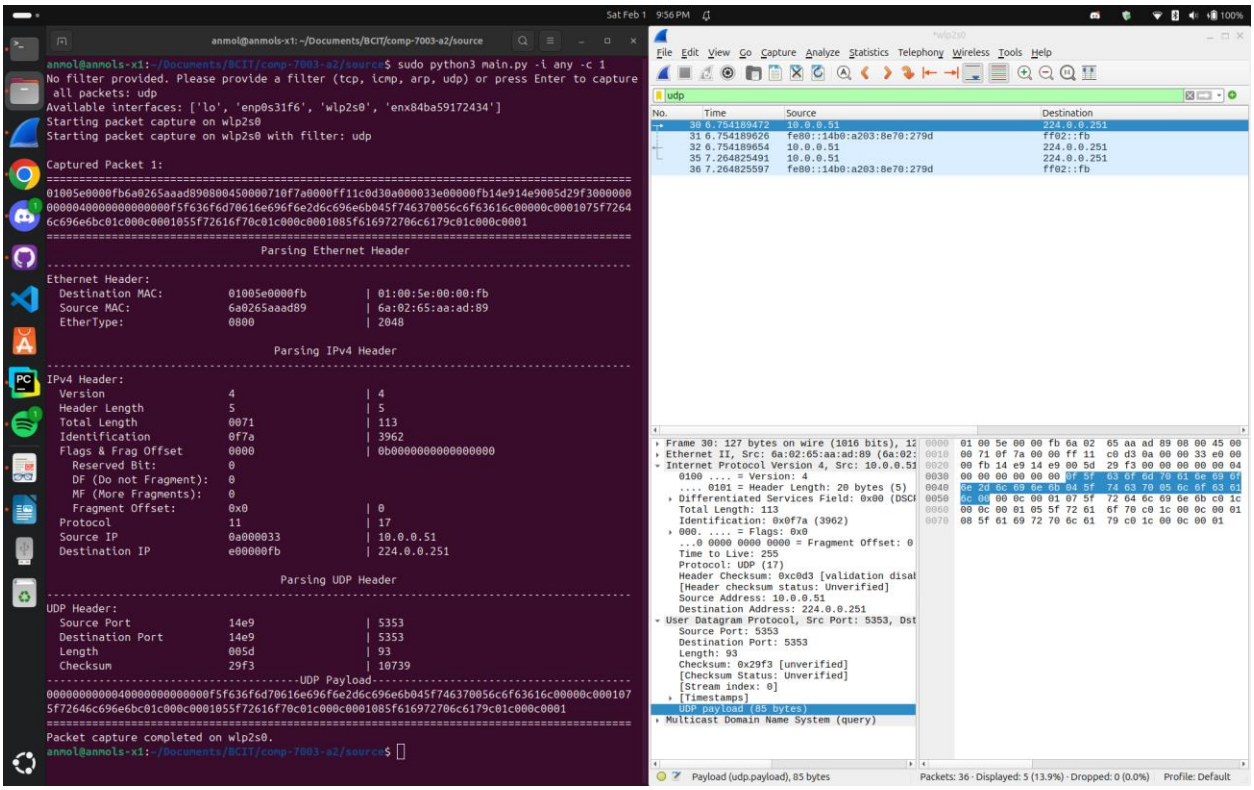
Test 01

```
anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
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$
```

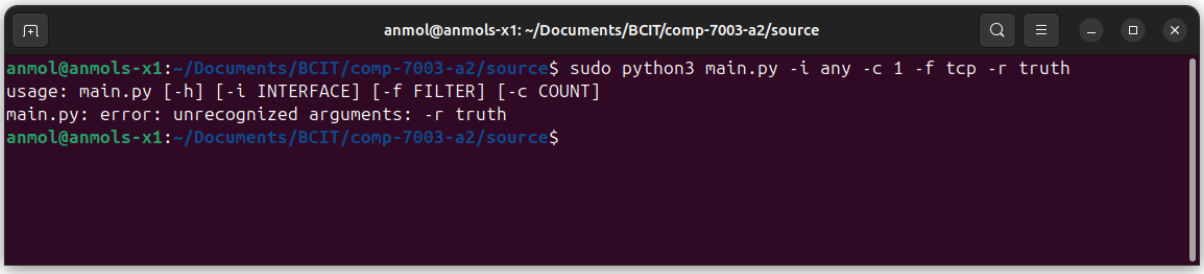
Test 02

```
anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
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$
```

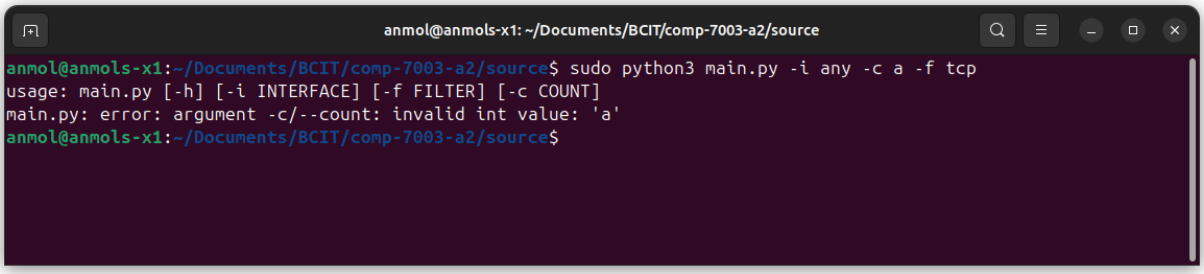
Test 03



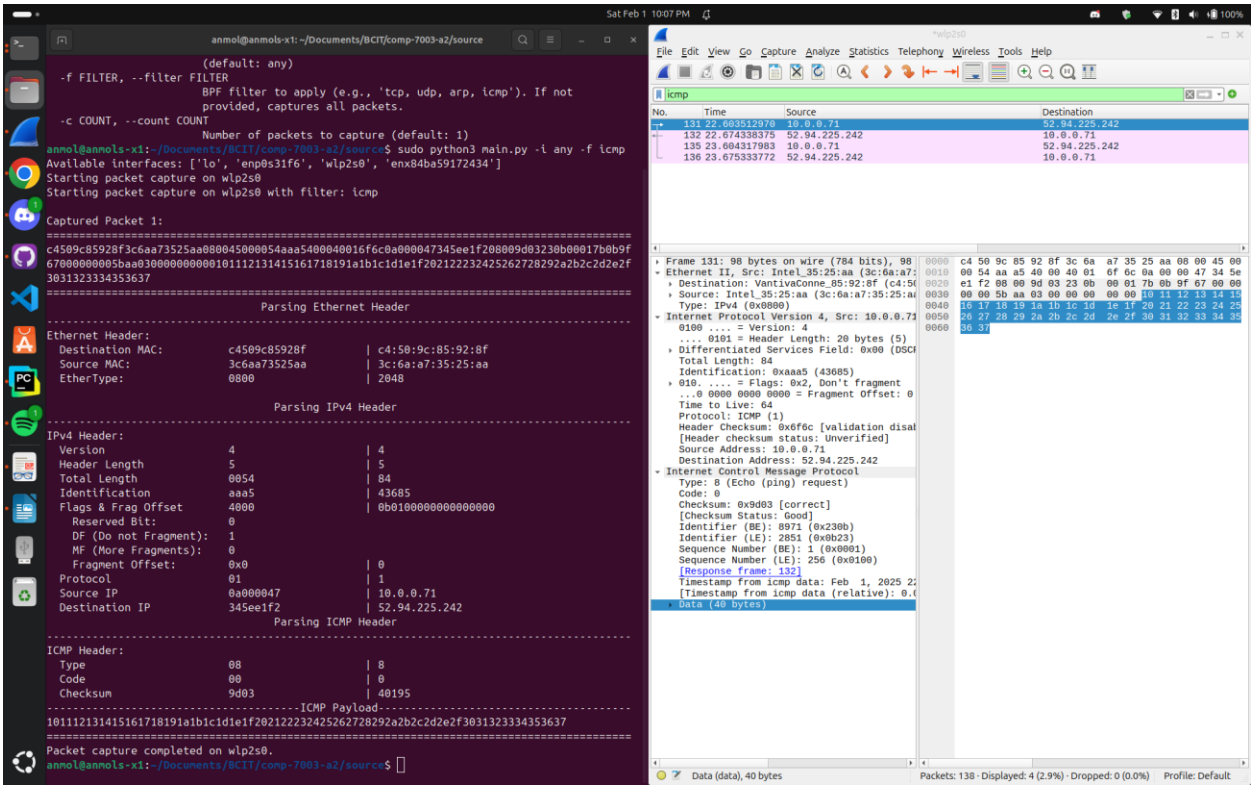
Test 04



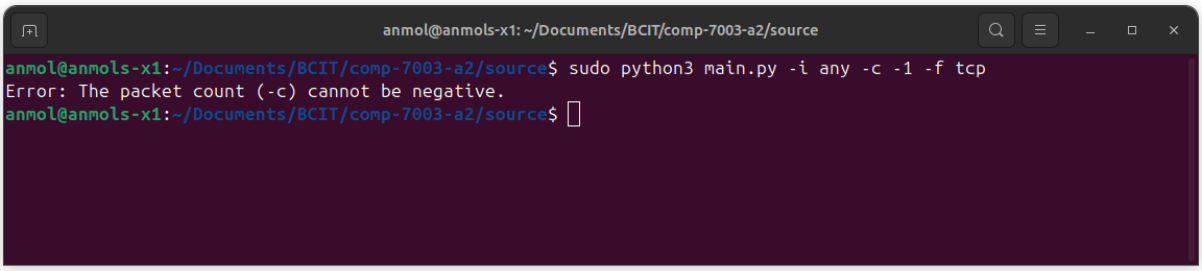
Test 05



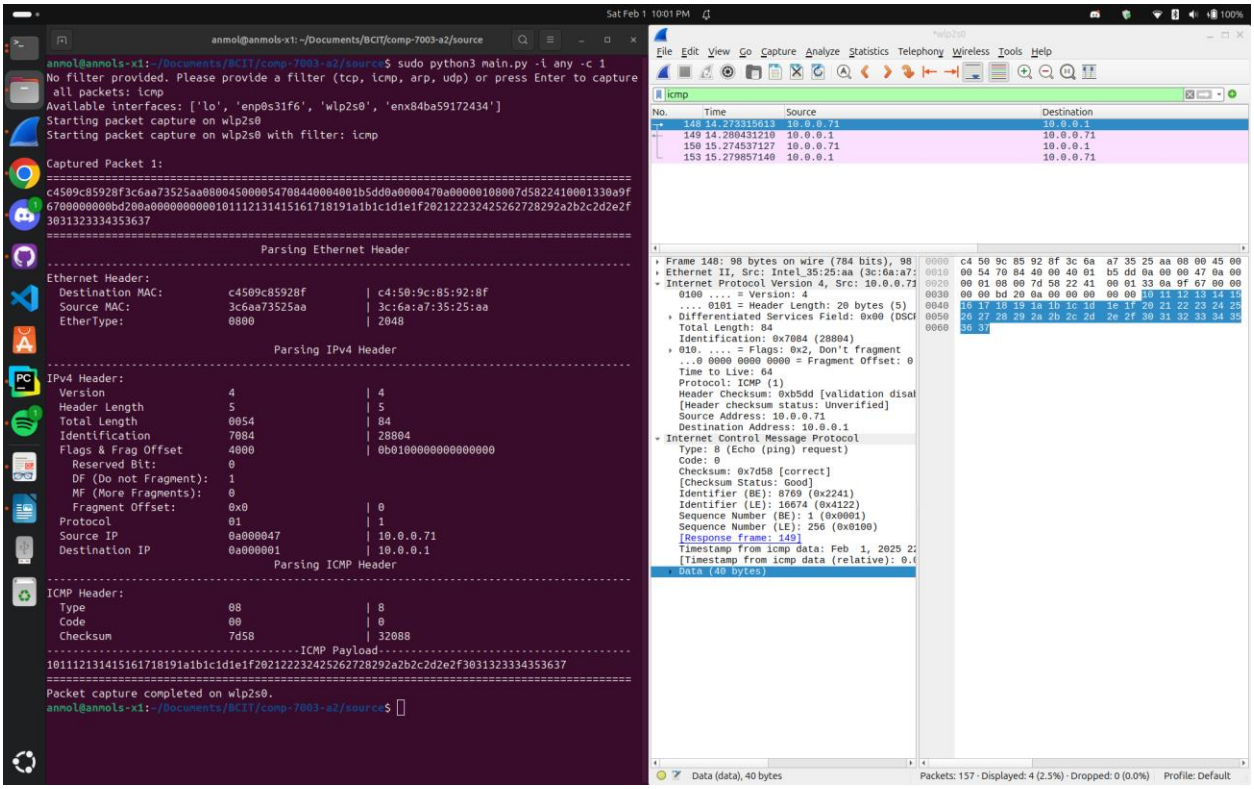
Test 06



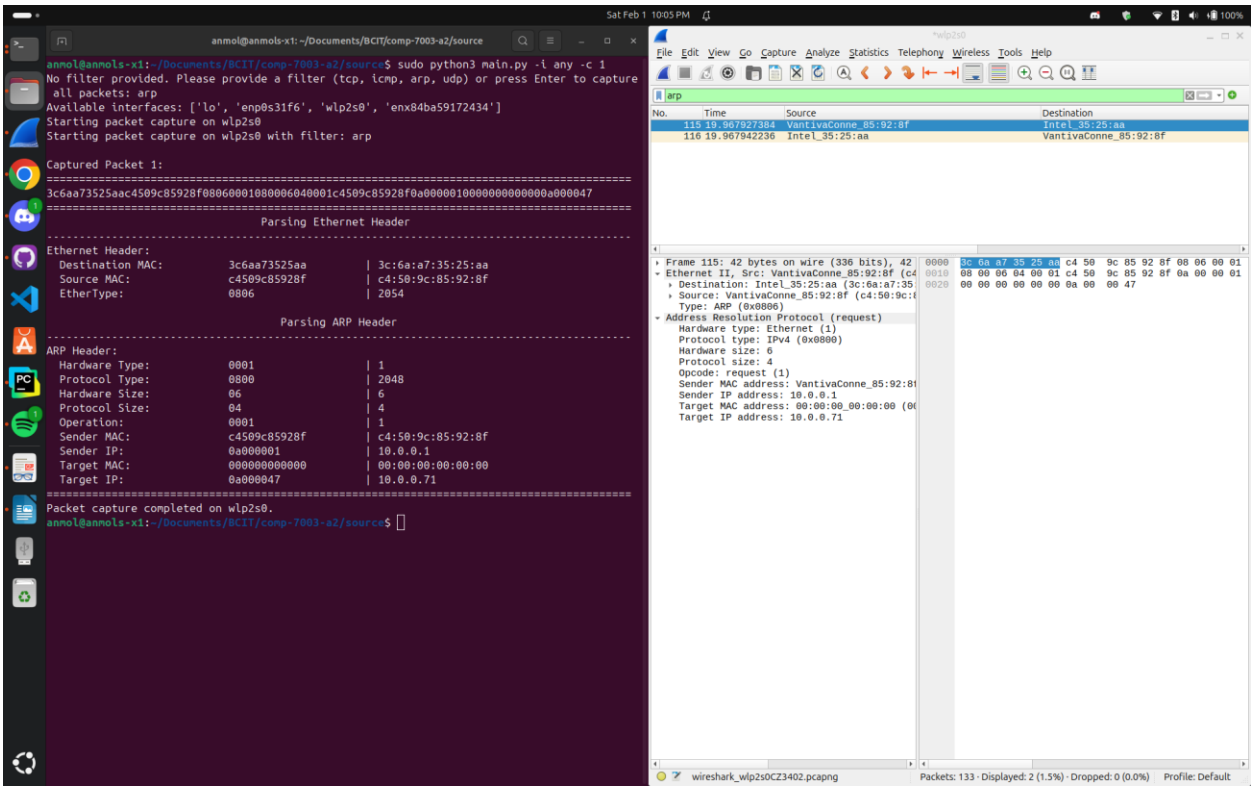
Test 07



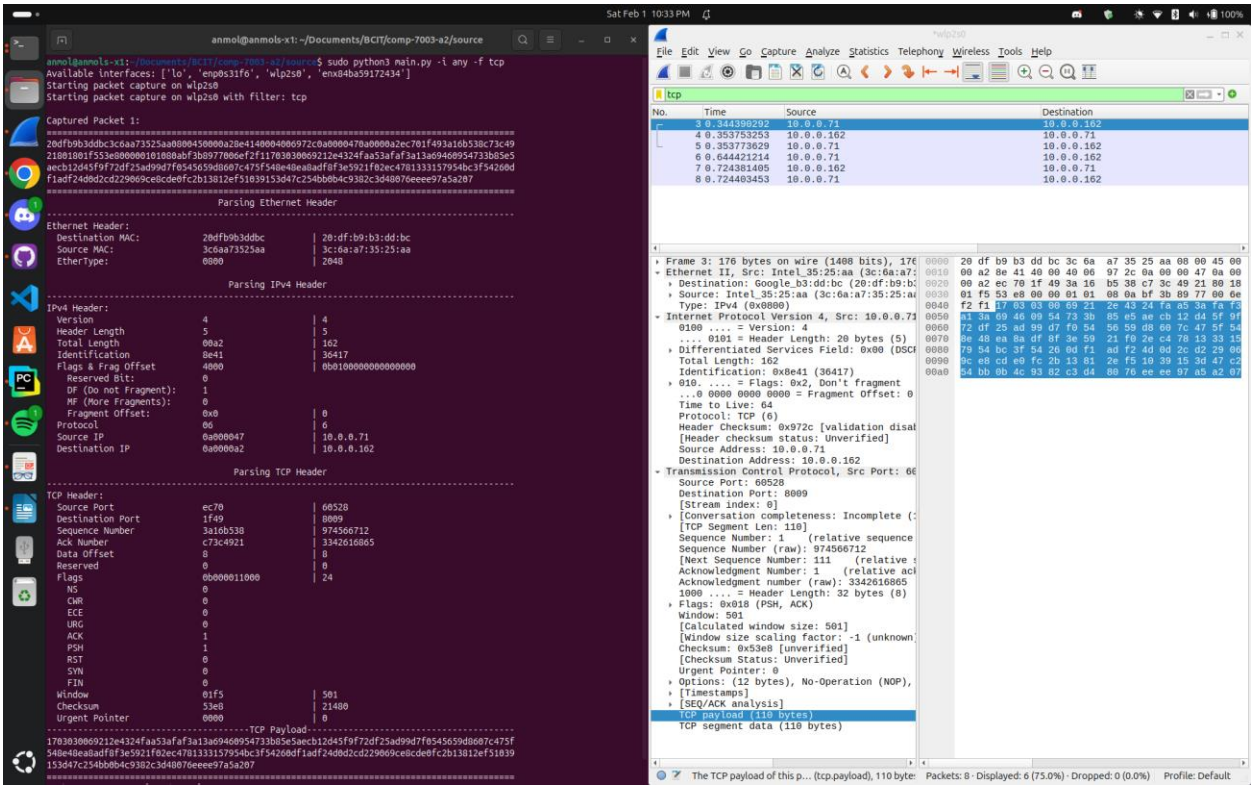
Test 08



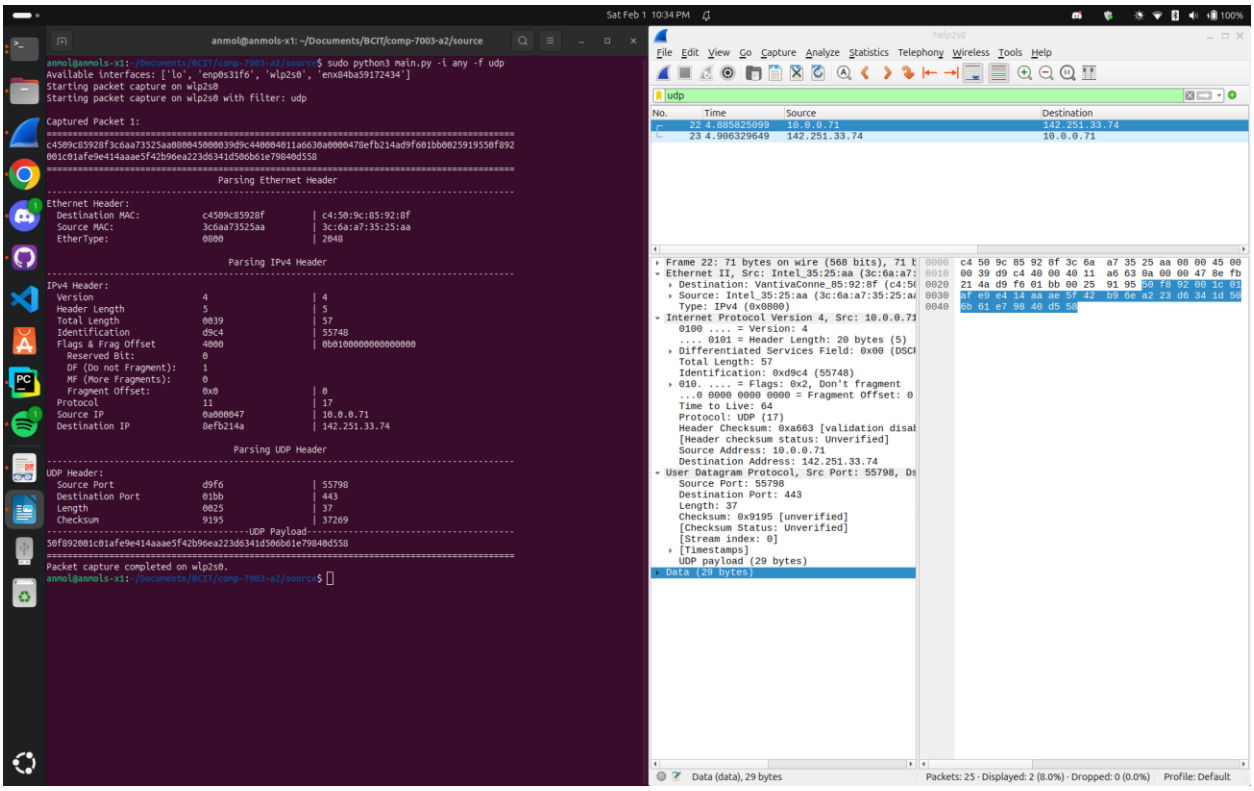
Test 09



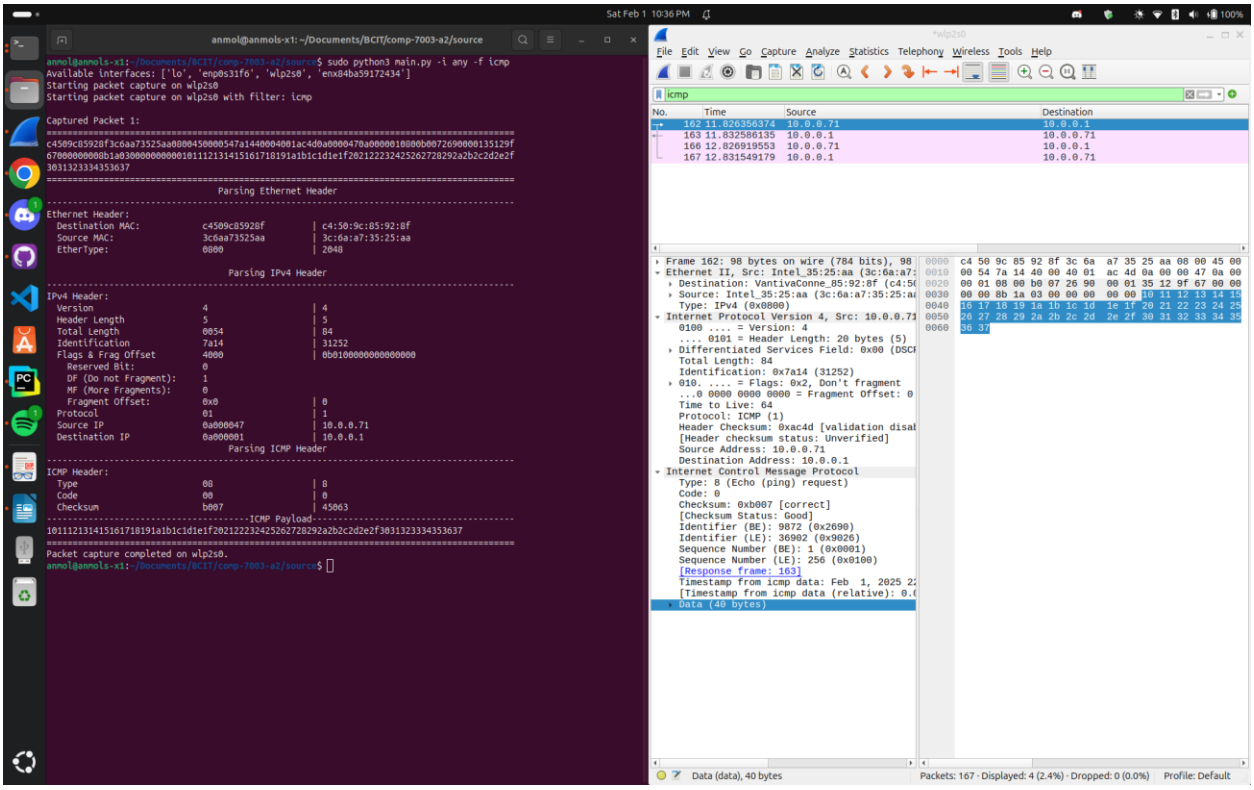
Test 10



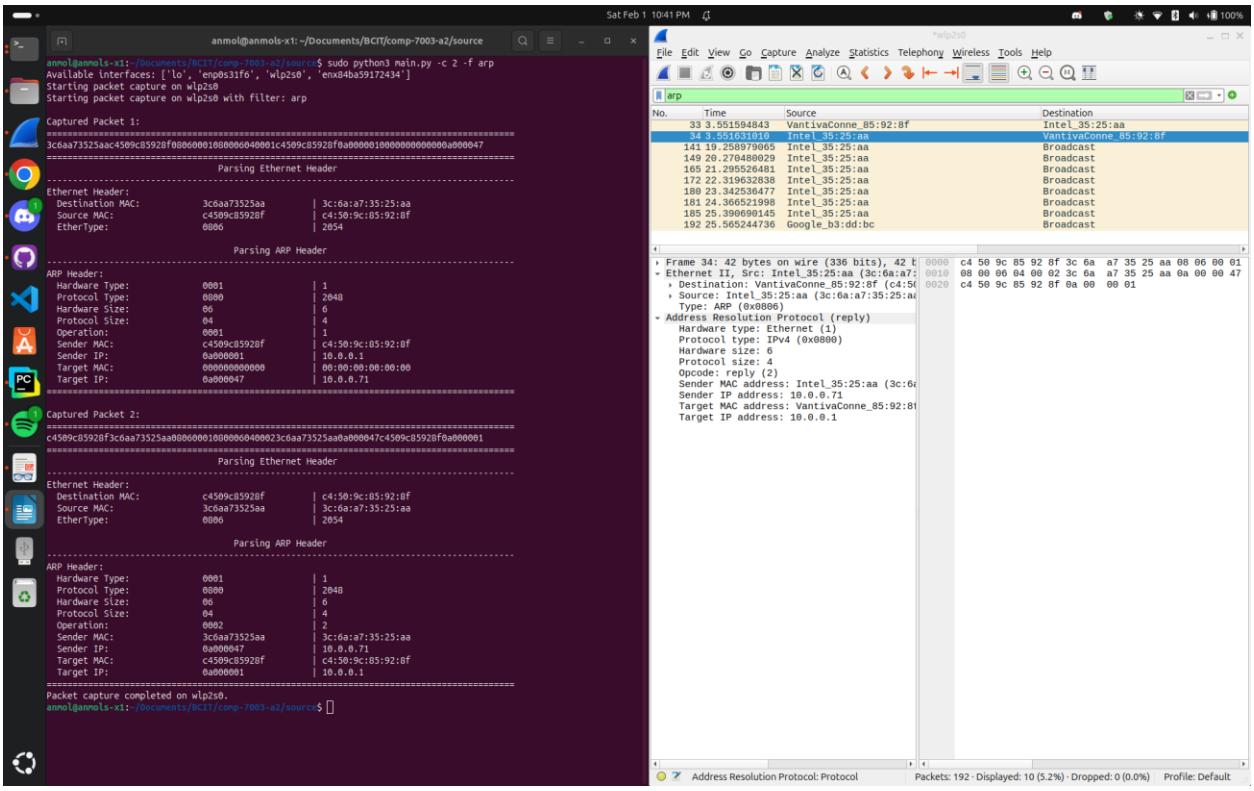
Test 11



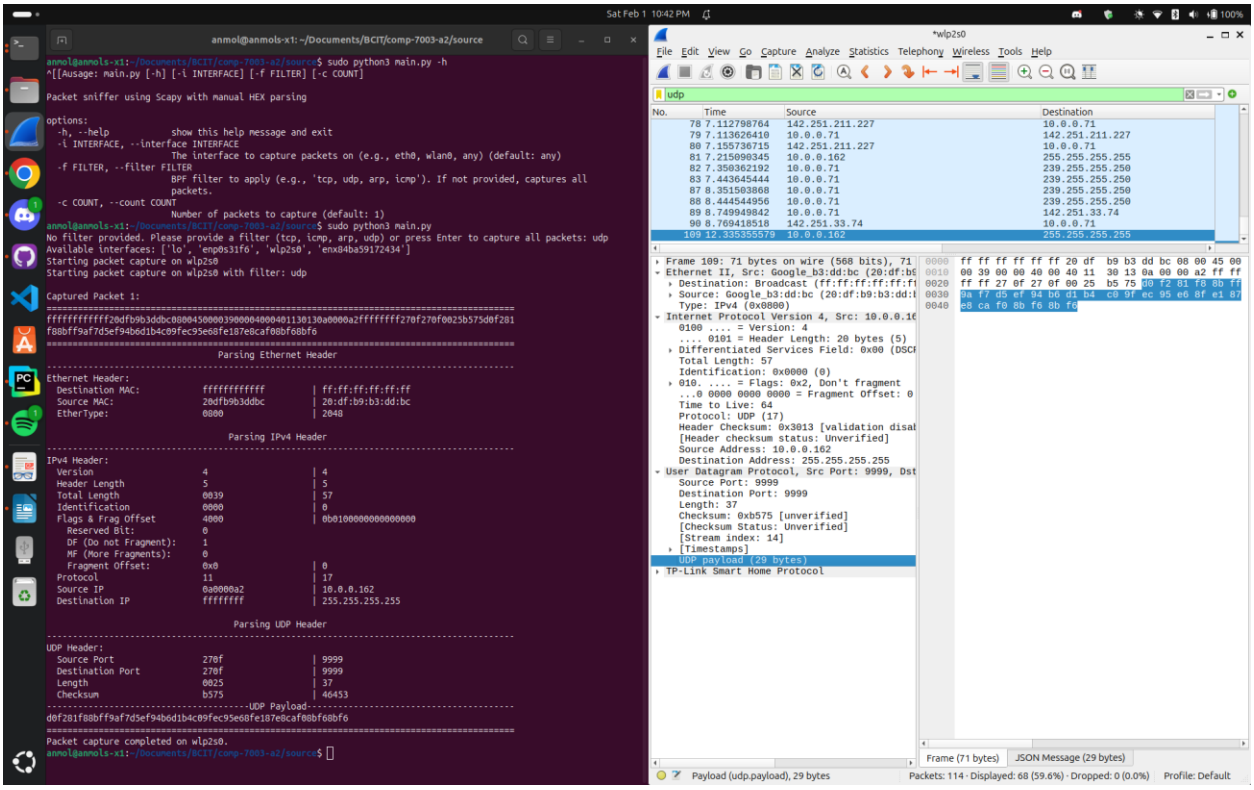
Test 12



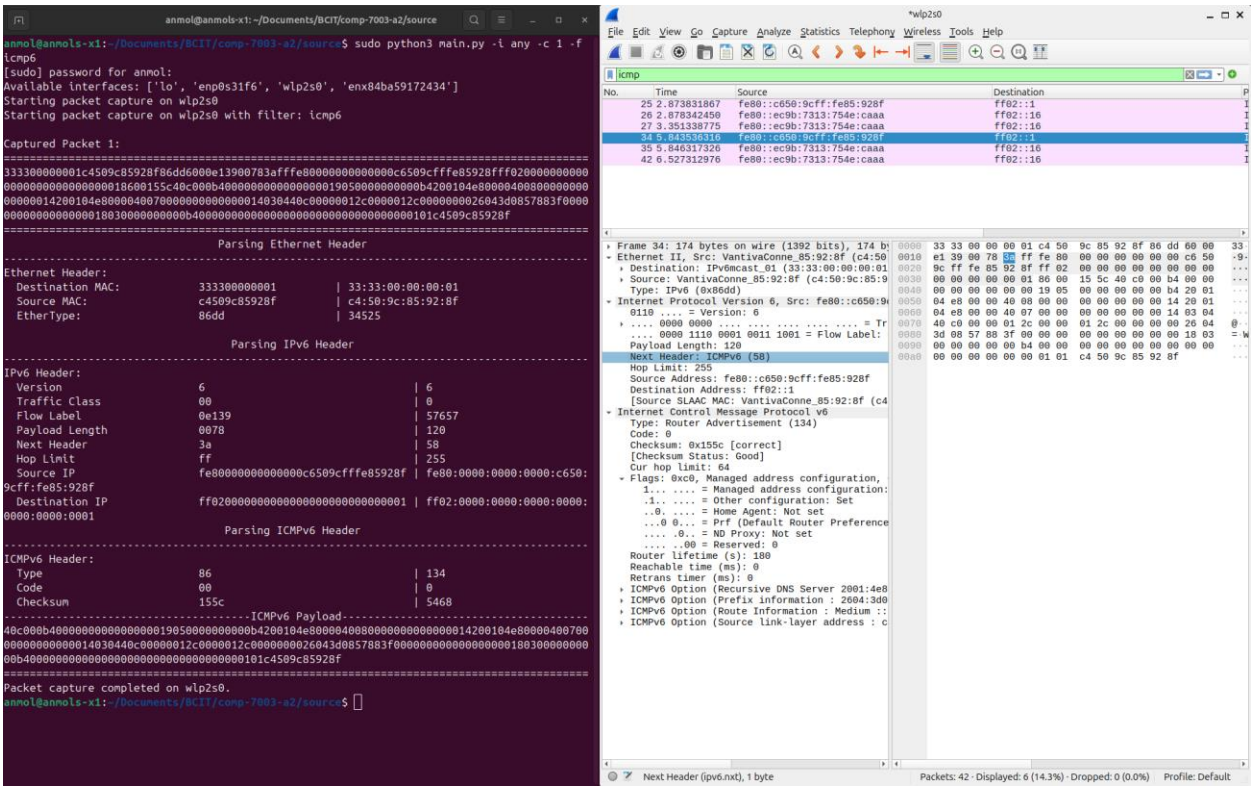
Test 13



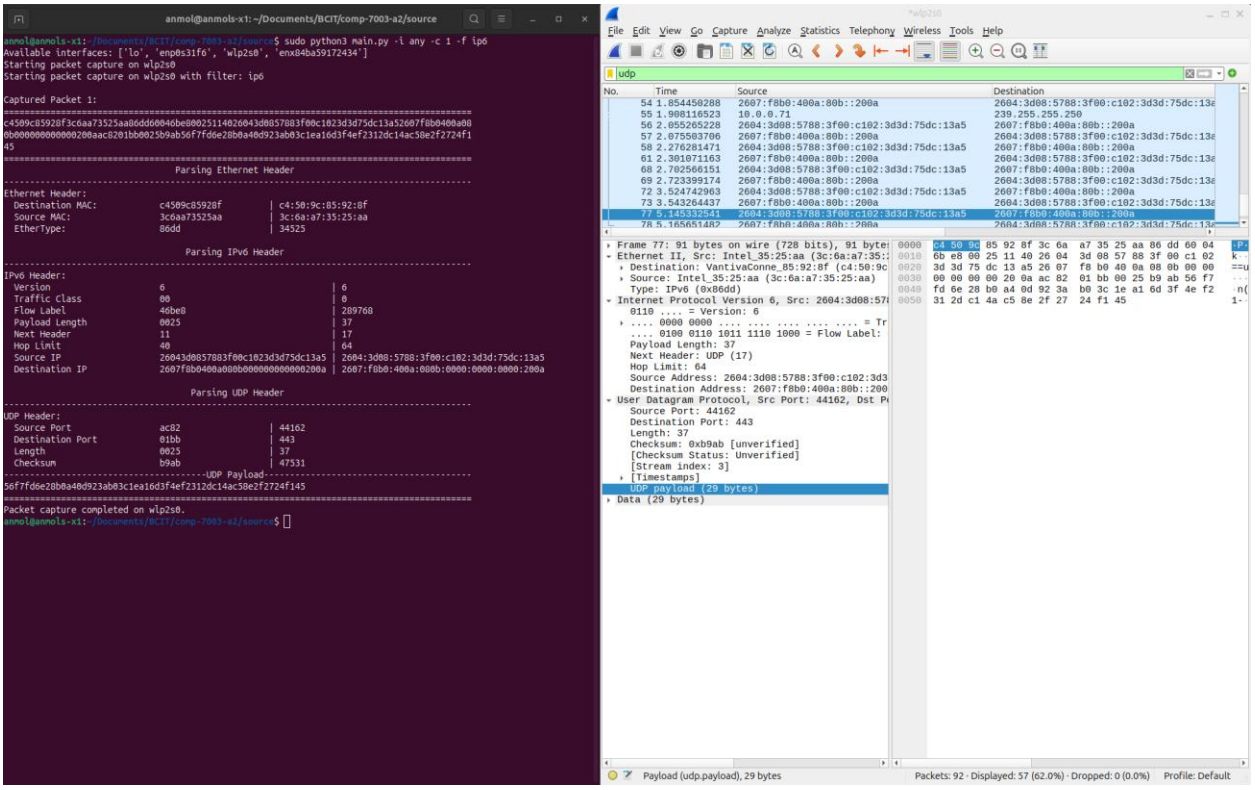
Test 14



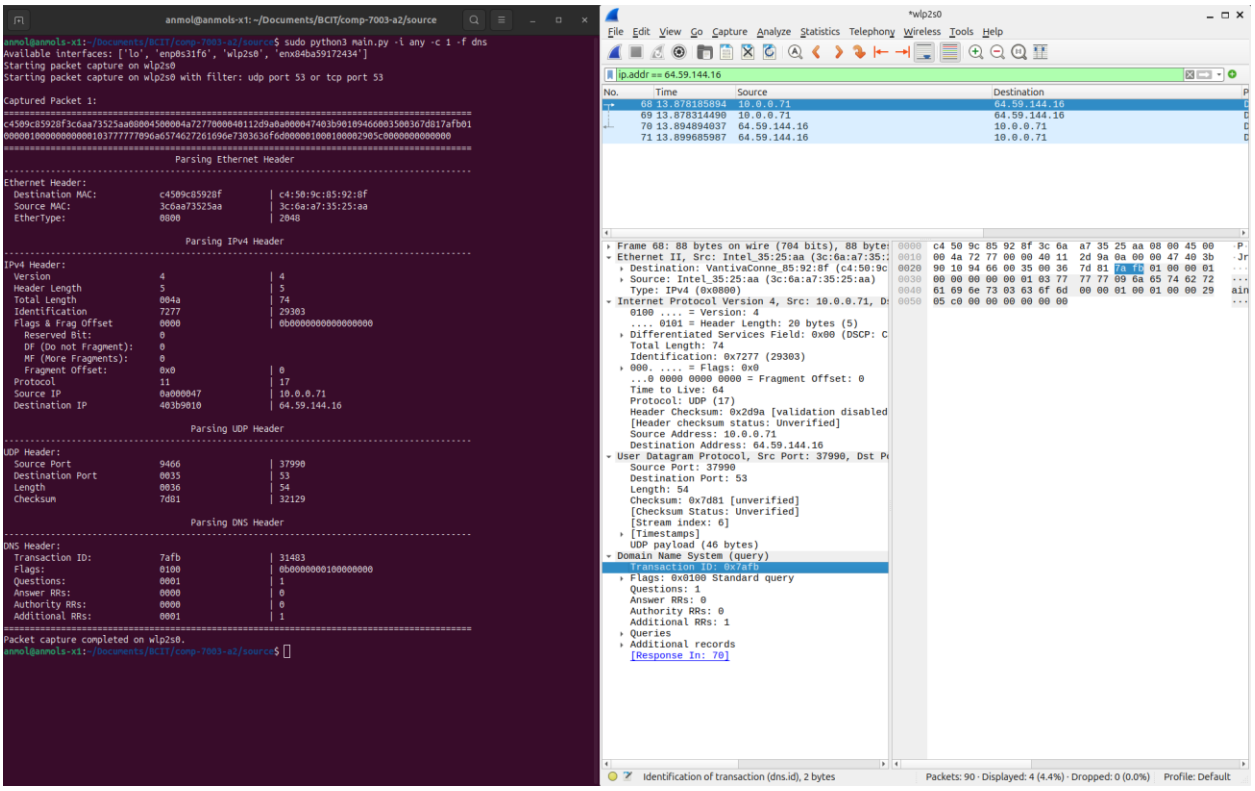
Test 15



Test 16



Test 17


anmol@anmols-x1: ~/Documents/BCIT/comp-7003-a2/source
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:
c4509c85928f3c6aa73525aa08004500004a72770000401120d9a0a000047403b9010946608350036 7d817afb01
0000010000000000010377777709696a657462726169 6e7303636f6d000001000100002905c000000000000
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 Po
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
0010 00 4a 72 77 00 00 40 11 2d 9a 0a 00 00 47 40 3b
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
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