

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

```
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
No filter provided. Please provide a filter (tcp, icmp, arp, udp) or press Enter to capture all packets: udp
Available interfaces: ['lo', 'enp0s3if6', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: udp

Captured Packet 1:
=====
01005e0000fb6a0265aad89080045000710f7a000ff11c0d30a0003e0000fb14e914e9005d29f3000000
00000400000000000000f5f636fd70616e696f6e2d6c696e6b045f746370056c6f63616c0000c0001075f7264
6c696e6bc01c000c0001055f72616f70c01c000c0001085f616972706c6179c01c000c0001
=====
Parsing Ethernet Header
-----
Ethernet Header:
Destination MAC: 01005e0000fb | 01:00:5e:00:00:fb
Source MAC: 6a0265aad89 | 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: 0
Protocol: 11 | 17
Source IP: 8a000033 | 10.0.0.51
Destination IP: e0000fb | 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-----
000000000004000000000000f5f636fd70616e696f6e2d6c696e6b045f746370056c6f63616c0000c000107
5f72646c696e6bc01c000c0001055f72616f70c01c000c0001085f616972706c6179c01c000c0001
=====
Packet capture completed on wlp2s0.
anmol@anmols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

Wireshark packet capture details for UDP 36.

No.	Time	Source	Destination
36	0.74189912	10.0.0.51	224.0.0.251
37	0.754189626	fe80::14b0:a203:8e70:279d	ff02::fb
32	0.754189654	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 36: 127 bytes on wire (1016 bits), 120 bytes captured (960 bits) on interface wlp2s0

Ethernet II, Src: 6a:02:65:aa:ad:89 (6a:02:65:aa:ad:89), Dst: 01:00:5e:00:00:fb (01:00:5e:00:00:fb)

Internet Protocol Version 4, Src: 10.0.0.51, Dst: 224.0.0.251

0100 ... = Version: 4

0101 ... = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP) = 0

Total Length: 113

Identification: 0xf7a (3962)

000 ... = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 255

Protocol: UDP (17)

Header Checksum: 0xc0d3 [validation disabled] [Header checksum status: Unverified]

Source Address: 10.0.0.51

Destination Address: 224.0.0.251

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Length: 93

Checksum: 0x29f3 [unverified] [Checksum status: Unverified] [Stream index: 0]

[Timestamp]

UDP payload (85 bytes)

Multicast Domain Name System (query)

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
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
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

The screenshot displays a terminal window on the left and a Wireshark packet analysis window on the right.

Terminal Window:

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

Wireshark Window:

The Wireshark window shows a packet capture on the 'icmp' filter. The packet list shows three packets:

No.	Time	Source	Destination
131	22.074353375	10.0.0.71	52.94.225.242
132	22.074353375	52.94.225.242	10.0.0.71
133	23.694317983	10.0.0.71	52.94.225.242

The packet details pane shows the following information for the selected packet (No. 131):

- Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:35:25:aa), Dst: Destination: VantivaConne_85:92:8f (c4:50:c8:59:28:f3c6aa73525aa) (3c:6a:a7:35:25:aa)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 10.0.0.71, Dst: 52.94.225.242
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP)
- Total Length: 84
- Identification: 0xaa55 (43685)
- 0100 = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 64
- Protocol: ICMP (1)
- Header Checksum: 0x0f6c [validation disabled] [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: 0x0d03 [correct]
- [Checksum Status: Good]
- Identifier (BE): 8971 (0x238b)
- Identifier (LE): 2851 (0x0b23)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Response frame: 132]
- Timestamp from icmp data: Feb 1, 2025 22:07:43.533750000
- [Timestamp from icmp data (relative): 0.000000000]
- Data (40 bytes)

Test 07

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

Test 08

```
anmol@annols-x1: ~/Documents/BCIT/comp-7003-a2/source
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 | 28004
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

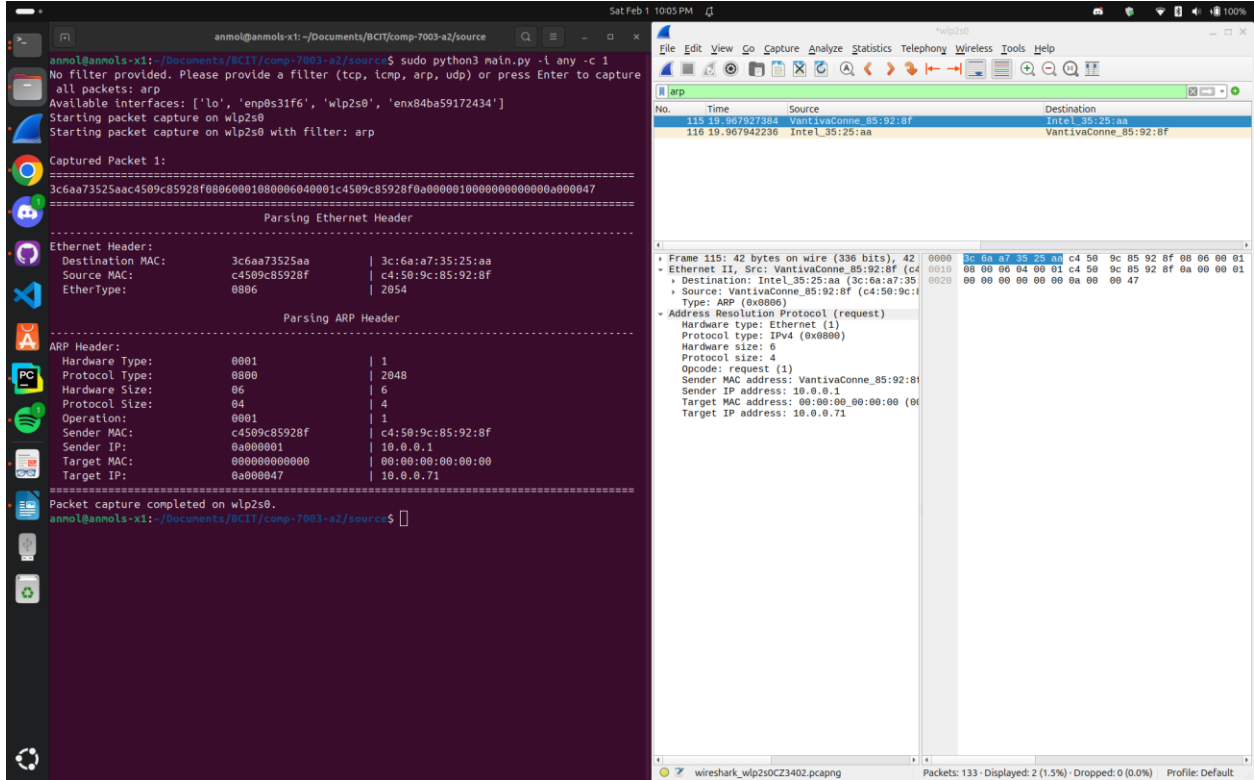
=====ICMP Payload=====
10112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
Packet capture completed on wlp2s0.
anmol@annols-x1:~/Documents/BCIT/comp-7003-a2/source$
```

Wireshark packet capture analysis of an ICMP Echo (ping) request.

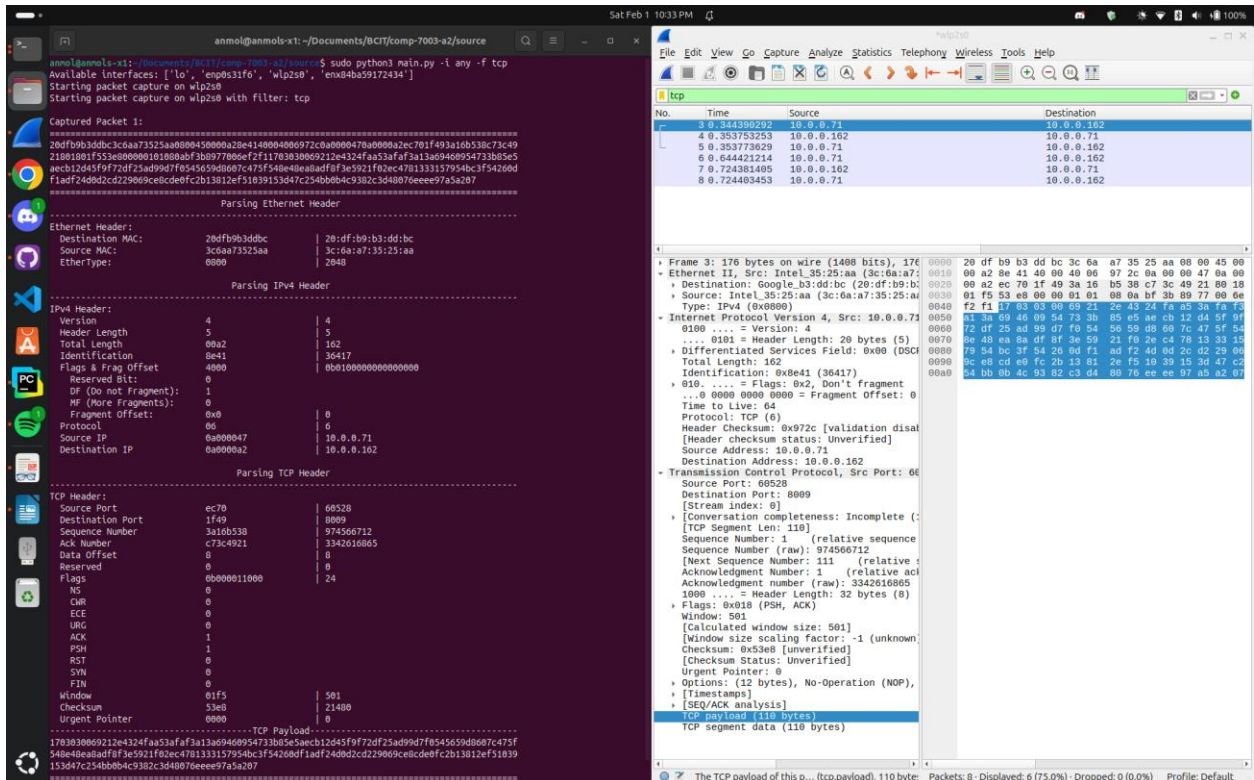
No.	Time	Source	Destination
148	14.273315613	10.0.0.71	10.0.0.1
149	14.280431210	10.0.0.1	10.0.0.71
150	15.274537127	10.0.0.71	10.0.0.1
153	15.279857140	10.0.0.1	10.0.0.71

Frame 148: 80 bytes on wire (784 bits), 90 captured (720 bits) on interface wlp2s0
Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:35:25:aa), Dst: Intel_85:92:8f (c4:50:9c:85:92:8f)
Internet Protocol Version 4, Src: 10.0.0.71, Dst: 10.0.0.1
ICMP Echo (ping) request, Sequence Number: 10674 (0x4122)
Checksum: 0xb5dd (validation disabled)
Header checksum status: Unverified
Source Address: 10.0.0.71
Destination Address: 10.0.0.1
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x7d58 [correct]
[Checksum Status: Good]
Identifier (BE): 8769 (0x2241)
Identifier (LE): 10674 (0x4122)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 250 (0x0100)
[Response Frame: 149]
Timestamp from icmp data: Feb 1, 2025 22:14:14.273315613
[Timestamp from icmp data (relative): 0.000000000]
Data (40 bytes)

Test 09



Test 10



Test 11

The terminal window shows the execution of a packet capture script on the `wlp2s0` interface. The script uses `python3 main.py -i any -f udp`. The captured packet is a UDP packet from `10.0.0.71` to `142.251.33.74` on port 55798. The packet is 29 bytes long and contains a single byte of data.

The Wireshark window displays the packet details and packet bytes. The packet is a UDP packet from `10.0.0.71` to `142.251.33.74` on port 55798. The packet is 29 bytes long and contains a single byte of data.

Test 12

The terminal window shows the execution of a packet capture script on the `wlp2s0` interface. The script uses `python3 main.py -i any -f icmp`. The captured packet is an ICMP packet from `10.0.0.71` to `10.0.0.1` on port 8072. The packet is 40 bytes long and contains a single byte of data.

The Wireshark window displays the packet details and packet bytes. The packet is an ICMP packet from `10.0.0.71` to `10.0.0.1` on port 8072. The packet is 40 bytes long and contains a single byte of data.

Test 13

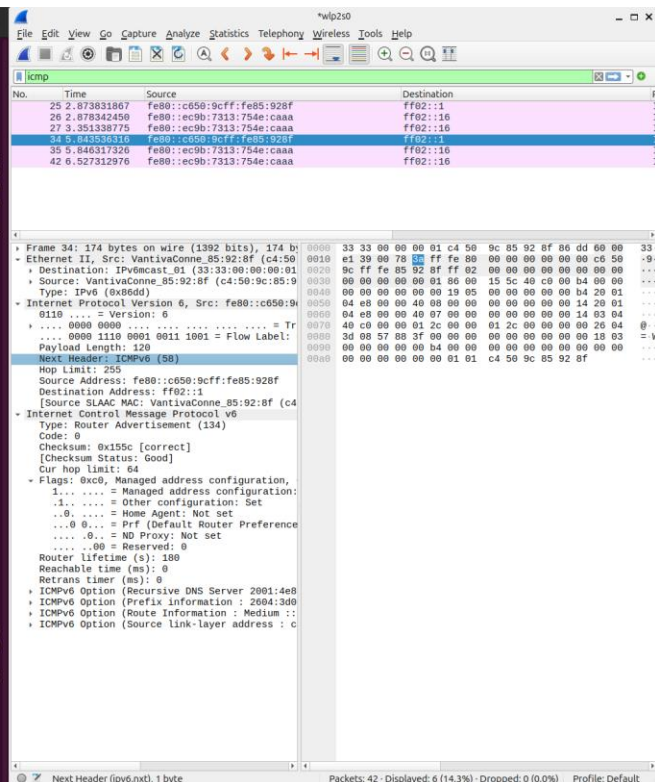
The terminal window shows the execution of a packet sniffer using Scapy with manual HEX parsing. The command is: `sudo python3 main.py -c 2 -f arp`. The output shows the capture of two ARP packets. The first packet is an ARP request from 10.0.0.1 to 10.0.0.1. The second packet is an ARP reply from 10.0.0.1 to 10.0.0.1.

The Wireshark window shows the captured packets. The first packet is an ARP request from 10.0.0.1 to 10.0.0.1. The second packet is an ARP reply from 10.0.0.1 to 10.0.0.1.

Test 14

The terminal window shows the execution of a packet sniffer using Scapy with manual HEX parsing. The command is: `sudo python3 main.py -h`. The output shows the help message for the script. The command is: `sudo python3 main.py -c 2 -f udp`. The output shows the capture of two UDP packets. The first packet is a UDP request from 10.0.0.1 to 10.0.0.1. The second packet is a UDP reply from 10.0.0.1 to 10.0.0.1.

The Wireshark window shows the captured packets. The first packet is a UDP request from 10.0.0.1 to 10.0.0.1. The second packet is a UDP reply from 10.0.0.1 to 10.0.0.1.

[illegible]

```

[~] anmol@anmolos-x1:~/Documents/anmolos-k1:~/Documents/icmp-7003-a2/source$ sudo python3 main.py -i any -c 1 -f ip6
Available interfaces: ['lo', 'enp0s3if0', 'wlp2s0', 'enx84ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: ip6

Captured Packet 1:

c4599c592df3c6aa73525aa8046d604a0be025114020443d0857803f0ec1023d3d75dc13a52607f0bb40ea00
0b0000000000000000200aac0201bb00259a056f7f06e28b0a4e8923ab03c1ea16d3f4ef7312dc14ac50e2f2724f1
45

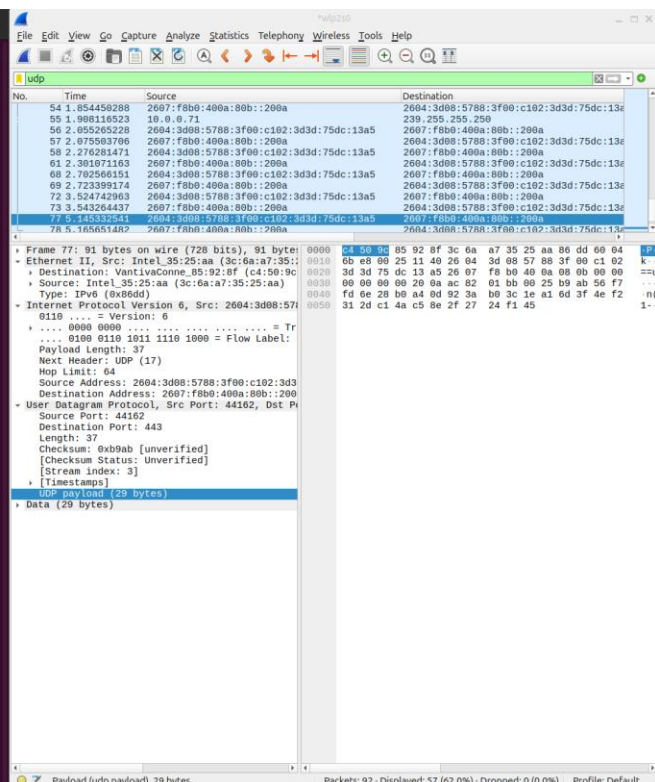
-----
Parsing Ethernet Header
-----
Ethernet Header:
Destination MAC: c4599c592df3c6aa73525aa      | c4:50:9c:85:92:bf
Source MAC: 3c6aa73525aa                        | 3c:6aa:07:35:25:aa
EtherType: 86dd                                  | 34525

-----
Parsing IPv6 Header
-----
IPv6 Header:
Version 6 | 6
Traffic Class 00 | 0
Flow Label 45be8 | 289768
Payload Length 0025 | 37
Next Header 11 | 17
Hop Limit 40 | 64
Source IP 2084:3d08:5780:3f0ec1023d3d75dc13a5 | 2084:3d08:5780:3f0ec102:3d3d:75dc:13a5
Destination IP 2007:f0b0:400a:0000:0000:0000:0000:200a | 2007:f0b0:400a:0000:0000:0000:0000:200a

-----
Parsing UDP Header
-----
UDP Header:
Source Port ac02 | 44102
Destination Port 01bb | 443
Length 0025 | 37
Checksum b9ab | 47531

-----
UDP Payload-----
50f7f06e28b0a4e8923ab03c1ea16d3f4ef7312dc14ac50e2f2724f145
-----
Packet capture completed on wlp2s0.
anmol@anmolos-x1:~/Documents/icmp-7003-a2/source$

```



Test 17

```
anmol@anmol:~$ cd /Documents/BCTI/comp-7003-a2/source
anmol@anmol:~/Documents/BCTI/comp-7003-a2/source$ sudo python3 main.py -l any -c 1 -f dns
Available interfaces: ['lo', 'enp8s31f6', 'wlp2s0', 'enx8ba59172434']
Starting packet capture on wlp2s0
Starting packet capture on wlp2s0 with filter: udp port 53 or tcp port 53

Captured Packet 1:
=====
c4509c8592f3c0aa73525aa00004a7277800040112d9a0a000047403b00109466003500367d817afba1
00000100000000000103777777896ad574627261696e73036f6d000001000100002905c0000000000000
=====

Parsing Ethernet Header
-----
Ethernet Header:
  Destination MAC: c4509c8592f3c0aa73525aa00004a7277800040112d9a0a000047403b00109466003500367d817afba1
  Source MAC: 3c6aa73525aa00004a7277800040112d9a0a000047403b00109466003500367d817afba1
  EtherType: 0800

Parsing IPv4 Header
-----
IPv4 Header:
  Version: 4
  Header Length: 5
  Total Length: 004a
  Identification: 7277
  Flags & frag offset: 0000
  Reserved bits: 0
  DF (Do not fragment): 0
  MF (More fragments): 0
  Fragment offset: 0x0
  Protocol: 11
  Source IP: 0a000047
  Destination IP: 403b9010

Parsing UDP Header
-----
UDP Header:
  Source Port: 9466
  Destination Port: 0035
  Length: 0036
  Checksum: 7d81

Parsing DNS Header
-----
DNS Header:
  Transaction ID: 7afb
  Flags: 0100
  Questions: 0001
  Answer RRs: 0000
  Authority RRs: 0000
  Additional RRs: 0001

Packet capture completed on wlp2s0.
anmol@anmol:~/Documents/BCTI/comp-7003-a2/source$
```

Wireshark packet capture analysis of a DNS query.

Packet 68: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface wlp2s0

Ethernet II, Src: Intel_35:25:aa (3c:6a:a7:35:25:aa), Dst: VantivaConne_85:92:bf (c4:50:9c:85:92:bf)

Internet Protocol Version 4, Src: 10.0.0.71, Destination: 10.0.0.71

User Datagram Protocol, Src Port: 37990, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x7afb
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries: 1
Additional records: 0

Response in: 70