Varun Narravula
ID: 923-287-037

Prof. Qun Wang
CSC645 Computer Networks

Project 4

Approach

In order to do this assignment, I need to:

1. Install a Python environment with `scapy` included as a package.
2. Figure out how to capture packets and print their contents.
3. Isolate the contents of each packet received per directions.

As for isolation of packets, this can easily be done with `scapy.all.sniff()`. I will only sniff 15 packets from a specific interface that I'll pass through a command-line argument, to reduce noise, and pass each packet to a callback function.

From here, I can get the packet number using a counter. Then, I'll just isolate the Ethernet frame, get the destination MAC and source MAC addresses, and print them. Afterward, I'll just check if the payload is an IP packet, and isolate the destination and source from there. Lastly, I'll get the first 42 raw bytes by just using the `bytes()` function on the whole packet and slicing it as an array.

I faced no challenges with this assignment other than setting up the environment. I opted to do this with a Nix shell, as that is what I'm used to.

Frame Capture Output

```
Packet 1
Source MAC: 1c:bf:c0:d9:6d:39
Destination MAC: 01:00:5e:00:00:fb
IP Version: 4
Source IP: 192.168.1.68
Destination IP: 224.0.0.251
First 42 bytes (hex):
01 00 5e 00 00 fb 1c bf
c0 d9 6d 39 08 00 45 00
00 3d c9 78 00 00 01 11
4d 50 c0 a8 01 44 e0 00
00 fb 14 e9 14 e9 00 29
ae ec
------------------------------
Packet 2
Source MAC: 1c:bf:c0:d9:6d:39
Destination MAC: 33:33:00:00:00:fb
No IP layer found in this frame.
First 42 bytes (hex):
33 33 00 00 00 fb 1c bf
c0 d9 6d 39 86 dd 60 09
20 83 00 29 11 01 fe 80
00 00 00 00 00 00 79 34
04 08 5c ba b7 df ff 02
00 00
------------------------------
Packet 3
Source MAC: 1c:bf:c0:d9:6d:39
Destination MAC: 33:33:00:00:00:fb
No IP layer found in this frame.
```

```
First 42 bytes (hex):
33 33 00 00 00 fb 1c bf
c0 d9 6d 39 86 dd 60 09
20 83 00 2a 11 01 fe 80
00 00 00 00 00 00 79 34
04 08 5c ba b7 df ff 02
00 00
------------------------------
Packet 4
Source MAC: 1c:bf:c0:d9:6d:39
Destination MAC: 01:00:5e:00:00:fb
IP Version: 4
Source IP: 192.168.1.68
Destination IP: 224.0.0.251
First 42 bytes (hex):
01 00 5e 00 00 fb 1c bf
c0 d9 6d 39 08 00 45 00
00 3e c9 79 00 00 01 11
4d 4e c0 a8 01 44 e0 00
00 fb 14 e9 14 e9 00 2a
2e f6
------------------------------
Packet 5
Source MAC: c8:94:02:f7:52:7b
Destination MAC: ff:ff:ff:ff:ff:ff
No IP layer found in this frame.
First 42 bytes (hex):
ff ff ff ff ff ff c8 94
02 f7 52 7b 08 06 00 01
08 00 06 04 00 01 c8 94
02 f7 52 7b c0 a8 01 5e
00 00 00 00 00 00 c0 a8
01 6a
------------------------------
Packet 6
Source MAC: f8:18:97:b2:fa:97
Destination MAC: ff:ff:ff:ff:ff:ff
No IP layer found in this frame.
First 42 bytes (hex):
ff ff ff ff ff ff f8 18
97 b2 fa 97 73 73 12 11
00 00 00 43 67 9e 18 e7
e3 89 c7 73 68 a6 78 fd
48 c2 70 46 fa 6d 5d 95
12 9a
------------------------------
Packet 7
Source MAC: c8:58:c0:c5:7c:f9
Destination MAC: f8:18:97:b2:fa:8d
IP Version: 4
Source IP: 192.168.1.72
Destination IP: 162.254.195.69
First 42 bytes (hex):
f8 18 97 b2 fa 8d c8 58
c0 c5 7c f9 08 00 45 00
00 6a d8 64 40 00 40 06
```

```
39 f5 c0 a8 01 48 a2 fe
c3 45 cc 23 69 8a 4d 1c
72 7c
------------------------------
Packet 8
Source MAC: f8:18:97:b2:fa:8d
Destination MAC: c8:58:c0:c5:7c:f9
IP Version: 4
Source IP: 162.254.195.69
Destination IP: 192.168.1.72
First 42 bytes (hex):
c8 58 c0 c5 7c f9 f8 18
97 b2 fa 8d 08 00 45 00
00 34 95 7d 40 00 35 06
88 12 a2 fe c3 45 c0 a8
01 48 69 8a cc 23 76 c6
9e b9
------------------------------
Packet 9
Source MAC: c8:94:02:f7:52:7b
Destination MAC: ff:ff:ff:ff:ff:ff
No IP layer found in this frame.
First 42 bytes (hex):
ff ff ff ff ff ff c8 94
02 f7 52 7b 08 06 00 01
08 00 06 04 00 01 c8 94
02 f7 52 7b c0 a8 01 5e
00 00 00 00 00 00 c0 a8
01 6a
------------------------------
Packet 10
Source MAC: c8:58:c0:c5:7c:f9
Destination MAC: f8:18:97:b2:fa:8d
No IP layer found in this frame.
First 42 bytes (hex):
f8 18 97 b2 fa 8d c8 58
c0 c5 7c f9 86 dd 60 0e
5e fd 00 40 06 40 26 00
17 00 3b d0 67 d0 72 f5
dc 69 64 7e c7 17 2a 04
4e 42
------------------------------
Packet 11
Source MAC: f8:18:97:b2:fa:8d
Destination MAC: c8:58:c0:c5:7c:f9
No IP layer found in this frame.
First 42 bytes (hex):
c8 58 c0 c5 7c f9 f8 18
97 b2 fa 8d 86 dd 60 0f
7c 56 00 20 06 37 2a 04
4e 42 00 4c 00 00 00 00
00 00 00 00 03 47 26 00
17 00
------------------------------
Packet 12
Source MAC: f8:18:97:b2:fa:97
```

```
Destination MAC: ff:ff:ff:ff:ff:ff
No IP layer found in this frame.
First 42 bytes (hex):
ff ff ff ff ff ff f8 18
97 b2 fa 97 73 73 12 11
00 00 00 43 67 9e 18 e7
e3 89 c7 73 68 a6 78 fd
48 c2 70 46 fa 6d 5d 95
12 9a
------------------------------
Packet 13
Source MAC: c8:94:02:f7:52:7b
Destination MAC: ff:ff:ff:ff:ff:ff
No IP layer found in this frame.
First 42 bytes (hex):
ff ff ff ff ff ff c8 94
02 f7 52 7b 08 06 00 01
08 00 06 04 00 01 c8 94
02 f7 52 7b c0 a8 01 5e
00 00 00 00 00 00 c0 a8
01 6a
------------------------------
Packet 14
Source MAC: 1c:bf:c0:d9:6d:39
Destination MAC: 01:00:5e:00:00:fb
IP Version: 4
Source IP: 192.168.1.68
Destination IP: 224.0.0.251
First 42 bytes (hex):
01 00 5e 00 00 fb 1c bf
c0 d9 6d 39 08 00 45 00
00 3e c9 7a 00 00 01 11
4d 4d c0 a8 01 44 e0 00
00 fb 14 e9 14 e9 00 2a
ae f5
------------------------------
Packet 15
Source MAC: 1c:bf:c0:d9:6d:39
Destination MAC: 33:33:00:00:00:fb
No IP layer found in this frame.
First 42 bytes (hex):
33 33 00 00 00 fb 1c bf
c0 d9 6d 39 86 dd 60 09
20 83 00 2a 11 01 fe 80
00 00 00 00 00 00 79 34
04 08 5c ba b7 df ff 02
00 00
------------------------------
```

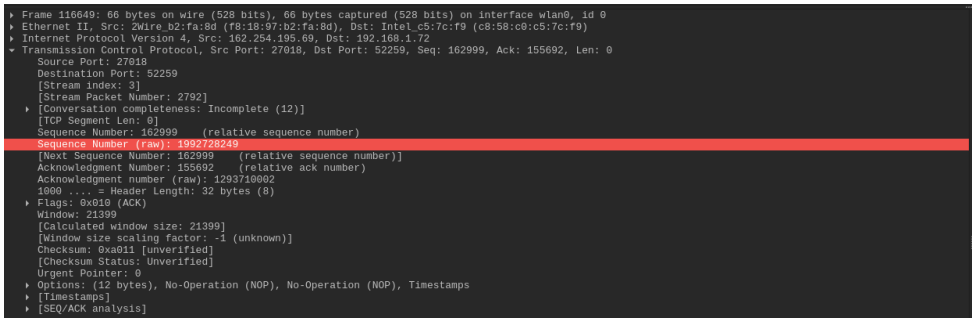
Wireshark Packet Comparison

Let's take a look at the bytes for Packet 8 again.

```
------------------------------
c8 58 c0 c5 7c f9 f8 18
97 b2 fa 8d 08 00 45 00
00 34 95 7d 40 00 35 06
88 12 a2 fe c3 45 c0 a8
```

```
01 48 69 8a cc 23 76 c6
9e b9
------------------------------
```

These are the first 42 bytes of the packet; when you convert the last 4 bytes of it `0x76c69eb9`, we get the number 1992728249, which corresponds to a TCP sequence number in this packet. Proof:



As you can see, the bytes for this sequence number are the exact same as Packet 8 in the above output.