

# Software and Cybersecurity Lab

## CS445 Lab3

Name: Dipean Dasgupta

ID: 202151188

**Task: Explore Packet sniffing in wireshark and see how it captures and analyzes network traffic.**

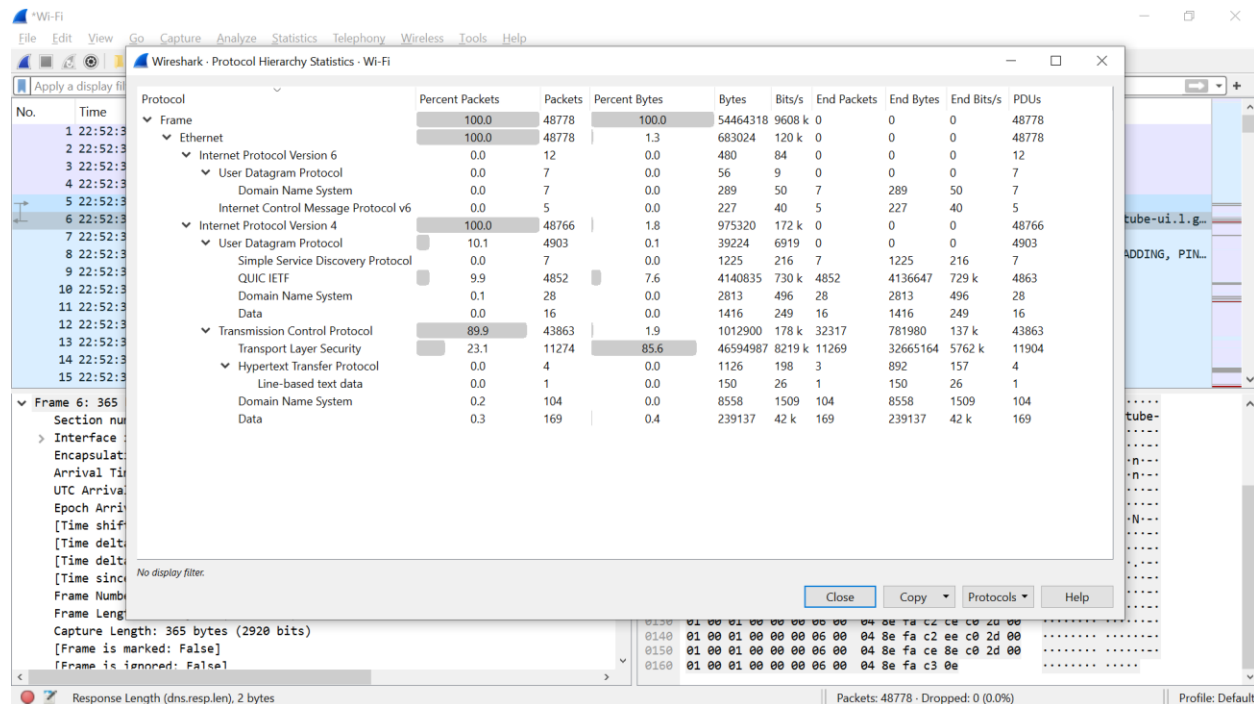
### Setup:

- OS: Windows 10
- Software: Wireshark

Firstly Wireshark software was start up. As Laptop was connected to wifi, so from the capture interfaces options WiFi was selected. On clicking the capture button, for test one website was visited and then capture was halted. In the meantime Wireshark software captured all the packets.

### Subtask1:

From the protocol hierarchy in statistics tab, information on the protocols that the packets were of were displayed. As per this particular capture the protocols are listed in the screenshot below:



The image depicts that multiple protocols have been captured. List of those protocols as per wireshark is listed below:

1. TCP(43863)    2. QUIC(4852)    3. DNS(140)    4. TLS
5. ICMP(5)    6. HTTP(4)    7. UDP    8.SSDP(7)

## Subtask 2:

Here, for a specific site request time elapsed from request to reply message is calculated.

The screenshot shows a Wireshark packet capture. The packet list on the left shows 15 packets. Packet 6 (No. 6, Time 22:52:35.814408, Source 192.168.1.1, Destination 192.168.1.26, Protocol DNS) is selected. The packet details pane on the right shows the frame structure for this packet, including the Ethernet II header, Internet Protocol Version 4 header, and the DNS query. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

From the screenshot we can see, when site of youtube was requested(5<sup>th</sup> one in list), query response was the 6<sup>th</sup> in the list.

Query Timestamp: 22 : 52 : 35.795419

Query Response Timestamp: 22 : 52 : 35.814408

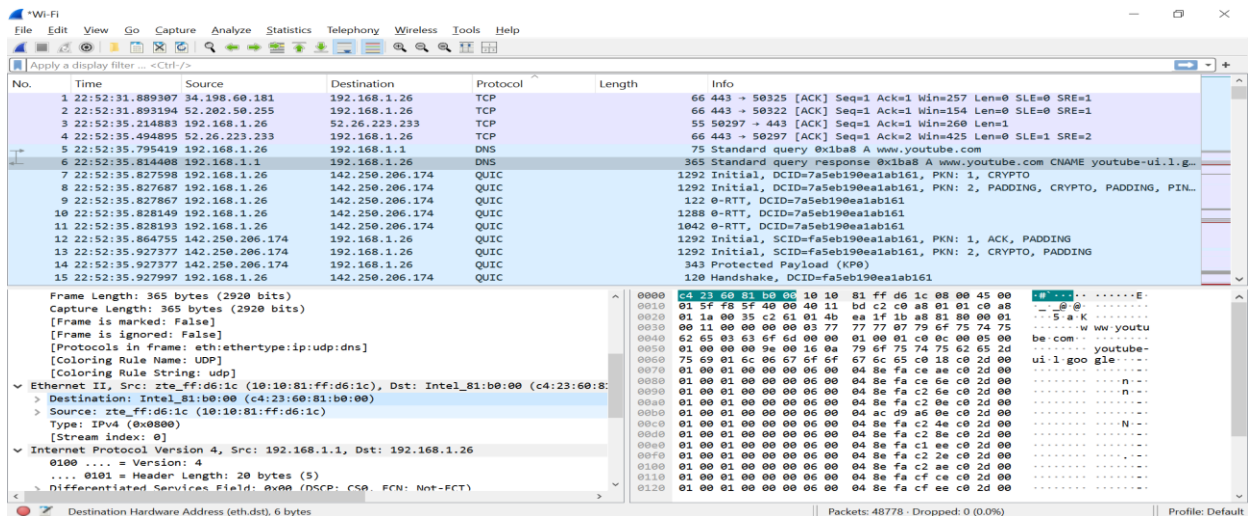
Time Elapsed: 0.018989000 seconds; this can be also verified from the Frame details ; given Time delta from previous captured frame is 0.018989000 seconds.

## Subtask 3:

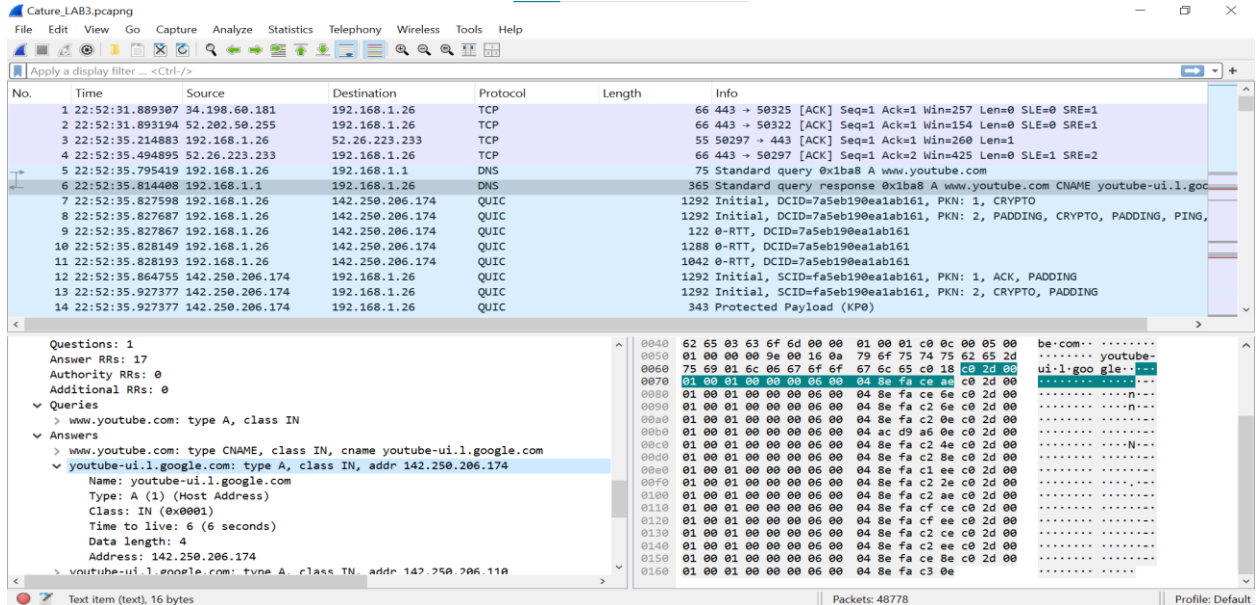
The screenshot shows the network configuration for a wireless LAN adapter. The configuration includes the following details:

- Connection-specific DNS Suffix : .
- Description : Intel(R) Wireless-AC 9462
- Physical Address : C4-23-60-81-B0-00
- DHCP Enabled : Yes
- Autoconfiguration Enabled : Yes
- Link-local IPv6 Address : fe80::5738:b414:ddb2:7509%5(Preferred)
- IPv4 Address : 192.168.1.26(Preferred)
- Subnet Mask : 255.255.255.0
- Lease Obtained : Thursday, September 12, 2024 10:17:17 PM
- Lease Expires : Friday, September 13, 2024 10:17:17 PM
- Default Gateway : 192.168.1.1
- DHCP Server : 192.168.1.1
- DHCPv6 IAID : 298866784
- DHCPv6 Client DUID : 00-01-00-01-2A-6C-23-91-C4-23-60-81-B0-00
- DNS Servers : 192.168.1.1
- NetBIOS over Tcpip : Enabled

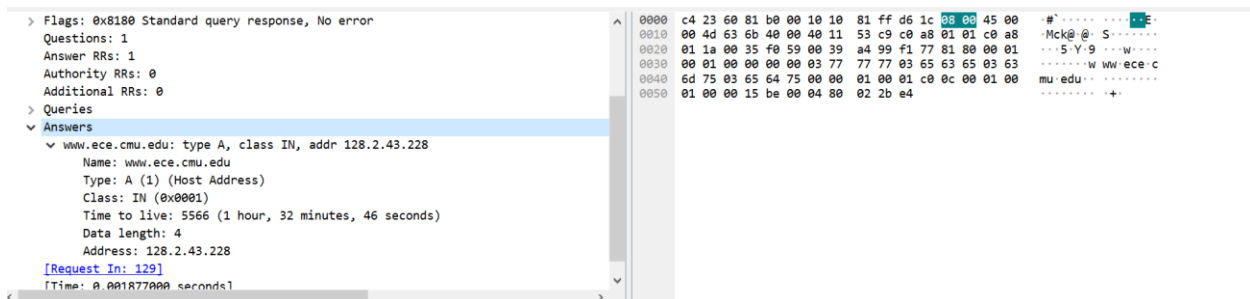
For my laptop, IPv4 Address: 192.168.1.26    MAC Address: C4-23-60-81-B0-00



From the screenshot, in the bottom left section under Ethernet II, Destination: C4:23:60:81:b0:00(mac address matched), 192.168.1.26(IP address matched)



Here, since site query was of youtube , from the screenshot shared below; the ip address for youtube is: 142.250.206.174



Ip address of [www.ece.cmu.edu](http://www.ece.cmu.edu): 128.2.43.228



## Subtask 4:

So, total number of packets captured by wireshark was 48778.

In order to find the packets out of these total packets contain IP address of my device, the filter was used below:

```
ip.addr == 192.168.1.26
```

Wireshark packet capture showing filtered results for IP address 192.168.1.26. The packet list shows various TCP and HTTP packets. The packet details pane shows the structure of a selected HTTP GET packet, including Ethernet II, Internet Protocol, and Hypertext Transfer Protocol layers.

Total 48743 out of 48778 contained IP address of my device.

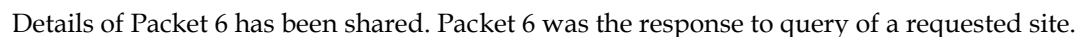
Now, for finding number of packets not having IP address of my device, the following filter was applied:

```
!(ip.addr == 192.168.1.26)
```

Wireshark packet capture showing filtered results for IP address 192.168.1.26. The packet list shows various DNS, ICMPv6, and SSDP packets. The packet details pane shows the structure of a selected ICMPv6 Neighbor Solicitation packet, including Ethernet II, Internet Protocol, and ICMPv6 layers.

So here:

- Below screenshot of details of a packet is shared below:



Wireshark packet capture showing an HTTP GET request and response. The packet list shows a GET request from 192.168.1.26 to 128.2.42.52. The packet details show the request line 'GET / HTTP/1.1' and the response line 'HTTP/1.0 301 Moved Permanently'. The packet bytes show the raw data of the request and response.

No.	Time	Source	Destination	Protocol	Length	Info
78	17:45:00.505735	192.168.1.26	128.2.42.52	HTTP		575 GET / HTTP/1.1
84	17:45:00.771944	128.2.42.52	192.168.1.26	HTTP		182 HTTP/1.0 301 Moved Permanently
1026	17:45:05.132797	192.168.1.26	18.67.196.194	OCSP		504 Request
1069	17:45:05.217863	18.67.196.194	192.168.1.26	OCSP		998 Response
2027	17:45:06.103273	192.168.1.26	18.67.196.194	OCSP		504 Request
2130	17:45:06.160805	18.67.196.194	192.168.1.26	OCSP		998 Response
2449	17:45:06.281131	192.168.1.26	18.67.196.194	OCSP		504 Request
2496	17:45:06.317968	18.67.196.194	192.168.1.26	OCSP		998 Response
2815	17:45:06.576555	192.168.1.26	18.67.196.194	OCSP		504 Request
2868	17:45:06.667657	18.67.196.194	192.168.1.26	OCSP		998 Response
6613	17:45:10.190470	192.168.1.26	152.195.38.76	OCSP		495 Request
6659	17:45:10.206928	152.195.38.76	192.168.1.26	OCSP		791 Response
6797	17:45:10.300634	192.168.1.26	152.195.38.76	OCSP		495 Request
6808	17:45:10.318279	152.195.38.76	192.168.1.26	OCSP		791 Response

Packet details for packet 78 (GET / HTTP/1.1):

- Calculated window size: 67072
- Window size scaling factor: 512
- Checksum: 0xd175 [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (944 bytes)
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
  - Content-Type: application/ocsp-response\r\n
  - Content-Length: 471\r\n
  - Connection: keep-alive\r\n
  - Accept-Ranges: bytes\r\n

Packet bytes for packet 78 (GET / HTTP/1.1):

```

0030 00 83 d1 75 00 00 48 54 54 50 2f 31 2e 31 20 32
0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 54
0050 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6d 6e
0060 2f 6f 63 73 70 2d 72 65 73 70 6f 6e 73 65 0d 0a
0070 43 6f 6e 74 65 6e 74 2d 43 65 6e 67 74 68 3a 20
0080 34 37 31 0d 0a 43 6f 6e 65 63 74 69 6f 6e 63 a
0090 20 6b 65 65 70 2d 61 6c 69 65 6b 0a 41 63 63
00a0 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65
00b0 73 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c
00c0 3a 20 61 67 78 2d 61 67 65 3d 37 32 30 30 0d 0a
00d0 44 61 74 65 3a 20 54 75 65 20 31 37 20 37 20 53 65
00e0 70 20 32 30 32 34 20 31 32 3a 31 35 3a 30 35 20
00f0 47 4d 54 0d 0a 41 61 73 74 2d 4d 6f 64 69 66 69
0100 65 64 3a 20 54 75 65 2c 20 31 37 20 53 65 70 20
0110 32 30 32 34 20 31 31 3a 34 3a 33 30 20 47 4d
0120 54 0d 0a 53 65 67 72 65 72 3a 20 45 43 41 63 63
0130 20 28 73 67 63 2f 35 36 41 35 20 0d 0a 58 2d 43

```

Ip address of [www.ini.cmu.edu](http://www.ini.cmu.edu): 128.2.42.52

1<sup>st</sup> packet : HTTP GET message

After that all the responses showed HTTP/1.1 200 OK message.

-----End of Assignment-----