Experiment-9

Q. Capturing & Analyzing network packets using Wireshark

Student Name: Parikshit Sharma
UID:19BCS4520
Branch: CSE
Section/Group IOT/A
Semester: 4
Date of Performance:03/05/2021
Subject Name: CN-LAB
Subject Code: CSP-293

1. Aim/Overview of the practical:

Capturing & Analyzing network packets using Wireshark

2. Task to be done:

A. Capturing
B. Analyzing network packets using Wireshark

3. Apparatus(For applied/experimental sciences/materials based labs):

Wireshark

3. Algorithm/Flowchart (For programming based labs):

Step1: Open the Wireshark and connect with any available network
Step2: Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface.
Step3: Filtering packets for any protocol like HTTP.
Step4: Just below the log entries, there is a panel with a summary of captured data.
Step5: Stop

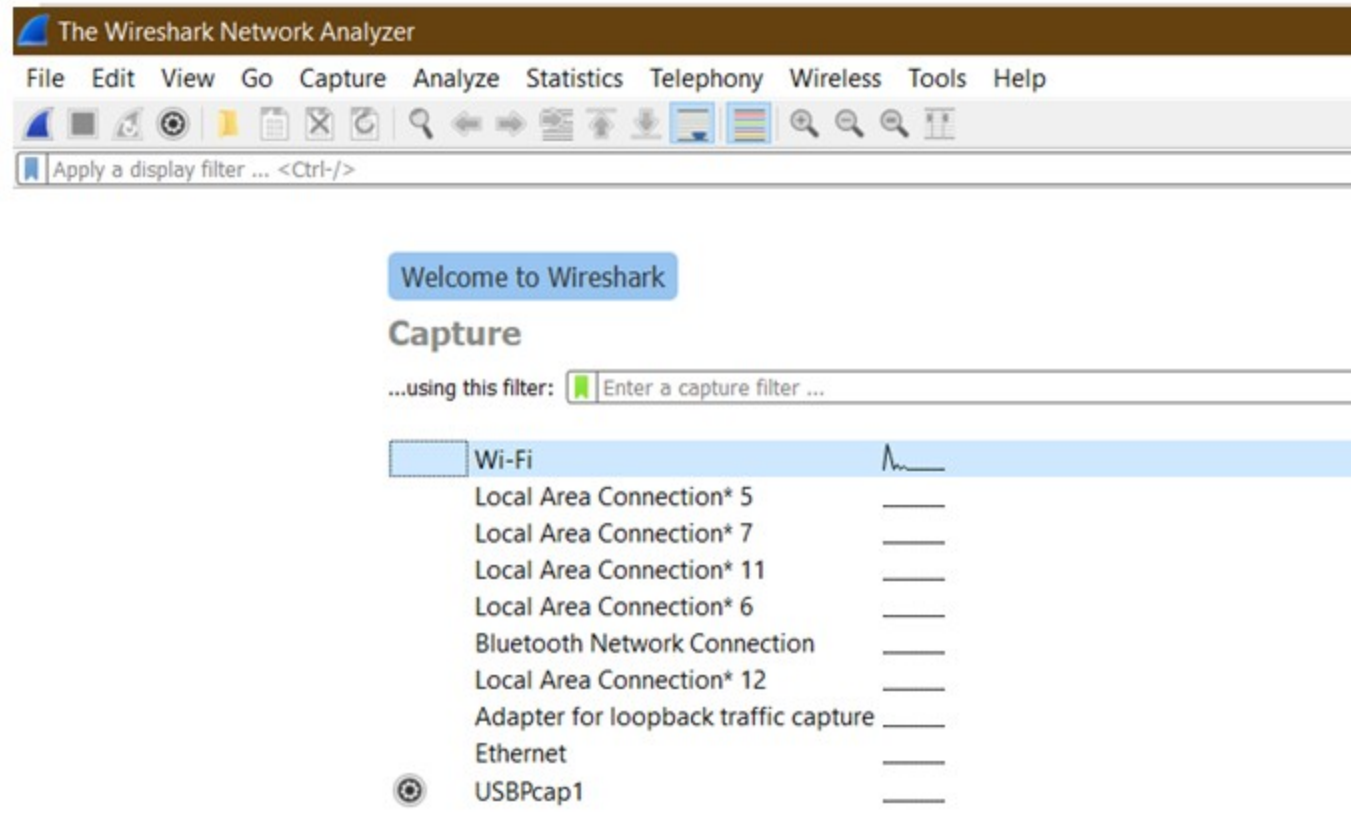
5. Theme/Interests definition(For creative domains):

Network packet: A network packet is a formatted unit of data carried by a packet-switched network. A packet consists of control information and user data .the latter is also known as the payload.

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

6. Steps for experiment/practical:

Step1: Open the Wireshark and connect with any available network



Wireshark Interface Diagram

Step2:Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface.

1 Packet information: You can easily find packets once you have captured some packets or have read in a previously saved capture file. Simply select Edit → Find Packet… in the main menu. Wireshark will open a toolbar between the main toolbar and the packet list

2 activity status: Status about frame, Ethernet, Internet protocol, user Datagram protocol and data.

3 Byte information: how many Byte are used.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
12931	44.518559	13.107.136.9	172.20.10.2	TLSv1.2	1354	Ignored Unknown Record
12932	44.518559	13.107.136.9	172.20.10.2	TLSv1.2	1354	Ignored Unknown Record
12933	44.518559	13.107.136.9	172.20.10.2	TLSv1.2	1354	Ignored Unknown Record
12934	44.518559	13.107.136.9	172.20.10.2	TLSv1.2	1354	Ignored Unknown Record
12935	44.518605	172.20.10.2	13.107.136.9	TCP	54	57509 → 443 [ACK] Seq=874 Ack=12785340 Win=4113
12936	44.519096	13.107.136.9	172.20.10.2	TLSv1.2	1354	Ignored Unknown Record
12937	44.519096	13.107.136.9	172.20.10.2	TLSv1.2	1354	Ignored Unknown Record
12938	44.519125	172.20.10.2	13.107.136.9	TCP	54	57509 → 443 [ACK] Seq=874 Ack=12787940 Win=4113
12939	44.519625	13.107.136.9	172.20.10.2	TLSv1.2	1354	Ignored Unknown Record
12940	44.519625	13.107.136.9	172.20.10.2	TCP	1354	443 → 57509 [ACK] Seq=12789240 Ack=874 Win=1022
12941	44.519625	13.107.136.9	172.20.10.2	TLSv1.2	1354	Ignored Unknown Record
12942	44.519657	172.20.10.2	13.107.136.9	TCP	54	57509 → 443 [ACK] Seq=874 Ack=12791840 Win=4113

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{F1013930-369D-456D-9FF2-BBF3DF57
> Ethernet II, Src: HonHaiPr_68:0a:ad (90:32:4b:68:0a:ad), Dst: 62:7e:c9:0a:39:64 (62:7e:c9:0a:39:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 52.202.62.250
> Transmission Control Protocol, Src Port: 57607, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

```
0000  62 7e c9 0a 39 64 90 32  4b 68 0a ad 08 00 45 00   b~··9d·2 Kh····E·
0010  00 29 28 48 40 00 80 06  a8 ac ac 14 0a 02 34 ca   ·)(H@··· ------4·
0020  3e fa e1 07 01 bb 5b 19  d4 3b 55 aa 37 3b 50 10   >·····[· ·;U·7;P·
0030  02 00 e4 fb 00 00 00                              -------
```

Wi-Fi: <live capture in progress>

Type here to search

Step3: Filtering packets for any protocol like HTTP.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
32242	218.793758	172.20.10.2	23.55.106.41	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/dis
32244	218.836234	23.55.106.41	172.20.10.2	HTTP	321	HTTP/1.1 304 Not Modified
32251	218.949658	172.20.10.2	23.55.106.80	HTTP	307	GET /DSTROOTCAX3CRL.crl HTTP/1.1
32253	218.994179	23.55.106.80	172.20.10.2	HTTP	322	HTTP/1.1 304 Not Modified
32254	219.001000	172.20.10.2	23.55.106.41	HTTP	334	GET /msdownload/update/v3/static/trustedr/en/aut
32256	219.041320	23.55.106.41	172.20.10.2	HTTP	320	HTTP/1.1 304 Not Modified

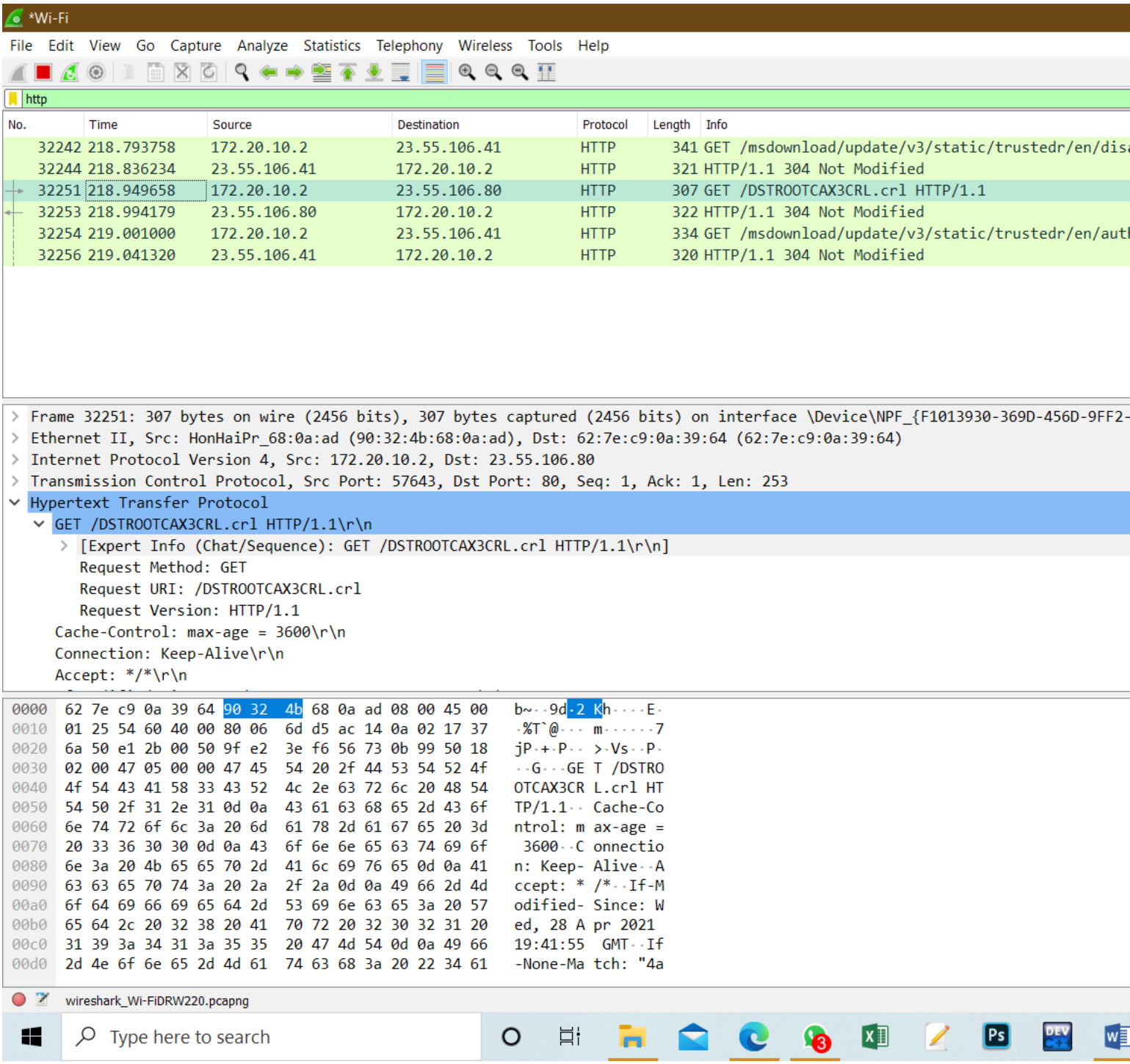
```
> Frame 32242: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface \Device\NPF_{F1013930-369D-456D-9FF2-
> Ethernet II, Src: HonHaiPr_68:0a:ad (90:32:4b:68:0a:ad), Dst: 62:7e:c9:0a:39:64 (62:7e:c9:0a:39:64)
> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 23.55.106.41
> Transmission Control Protocol, Src Port: 57642, Dst Port: 80, Seq: 1, Ack: 1, Len: 287
> Hypertext Transfer Protocol
```

```
0000  62 7e c9 0a 39 64 90 32  4b 68 0a ad 08 00 45 00   b~··9d·2 Kh····E·
0010  01 47 12 b4 40 00 80 06  af 86 ac 14 0a 02 17 37   ·G··@··· ·******7
0020  6a 29 e1 2a 00 50 81 ea  44 b9 4d 0a 86 a1 50 18   j)·*·P·· D·M···P·
0030  02 00 b8 62 00 00 47 45  54 20 2f 6d 73 64 6f 77   ···b··GE T /msdow
0040  6e 6c 6f 61 64 2f 75 70  64 61 74 65 2f 76 33 2f   nload/up date/v3/
0050  73 74 61 74 69 63 2f 74  72 75 73 74 65 64 72 2f   static/t rustedr/
0060  65 6e 2f 64 69 73 61 6c  6c 6f 77 65 64 63 65 72   en/disal lowedcer
0070  74 73 74 6c 2e 63 61 62  3f 66 32 34 33 39 65 64   tstl.cab ?f2439ed
0080  65 31 62 37 35 35 32 66  62 20 48 54 54 50 2f 31   e1b7552f b HTTP/1
0090  2e 31 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   .1··Conn ection:
00a0  4b 65 65 70 2d 41 6c 69  76 65 0d 0a 41 63 63 65   Keep-Ali ve··Acce
00b0  70 74 3a 20 2a 2f 2a 0d  0a 49 66 2d 4d 6f 64 69   pt: */*· ·If-Modi
00c0  66 69 65 64 2d 53 69 6e  63 65 3a 20 54 75 65 2c   fied-Sin ce: Tue,
00d0  20 31 36 20 4d 61 72 20  32 30 32 31 20 30 37 3a    16 Mar  2021 07:
```

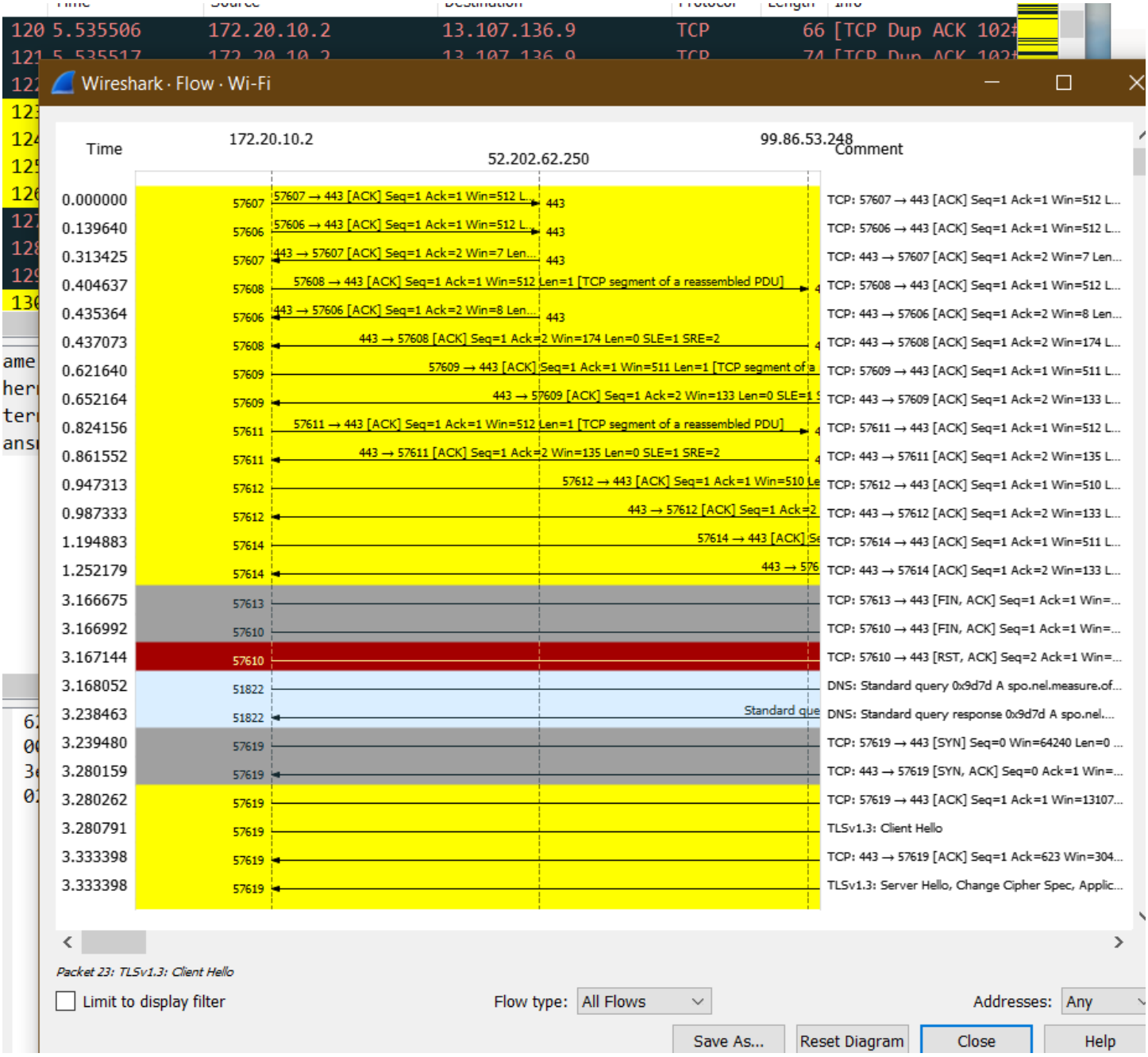
wireshark_Wi-FiDRW220.pcapng

Type here to search

Step4: Just below the log entries, there is a panel with a summary of captured data.

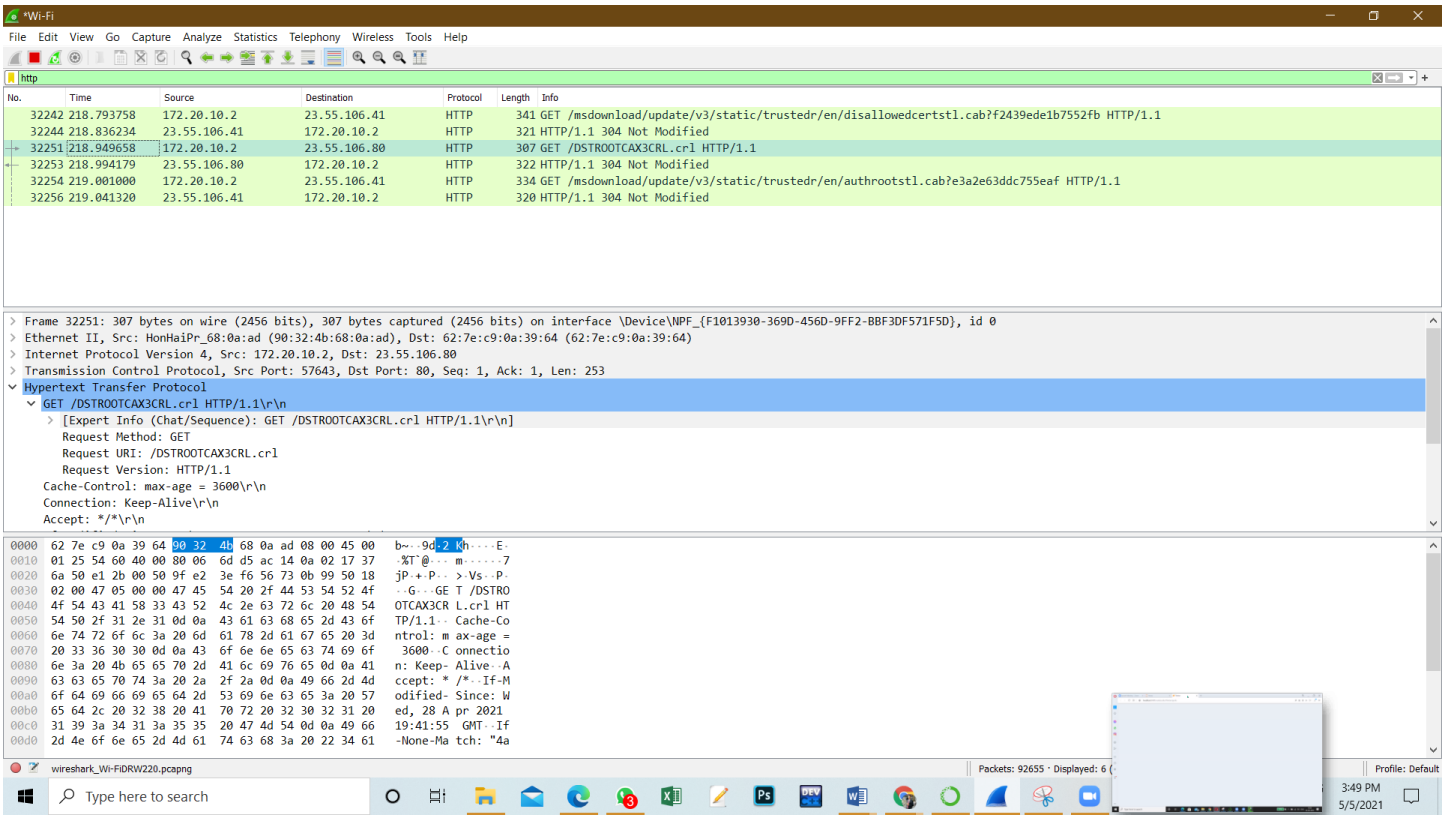


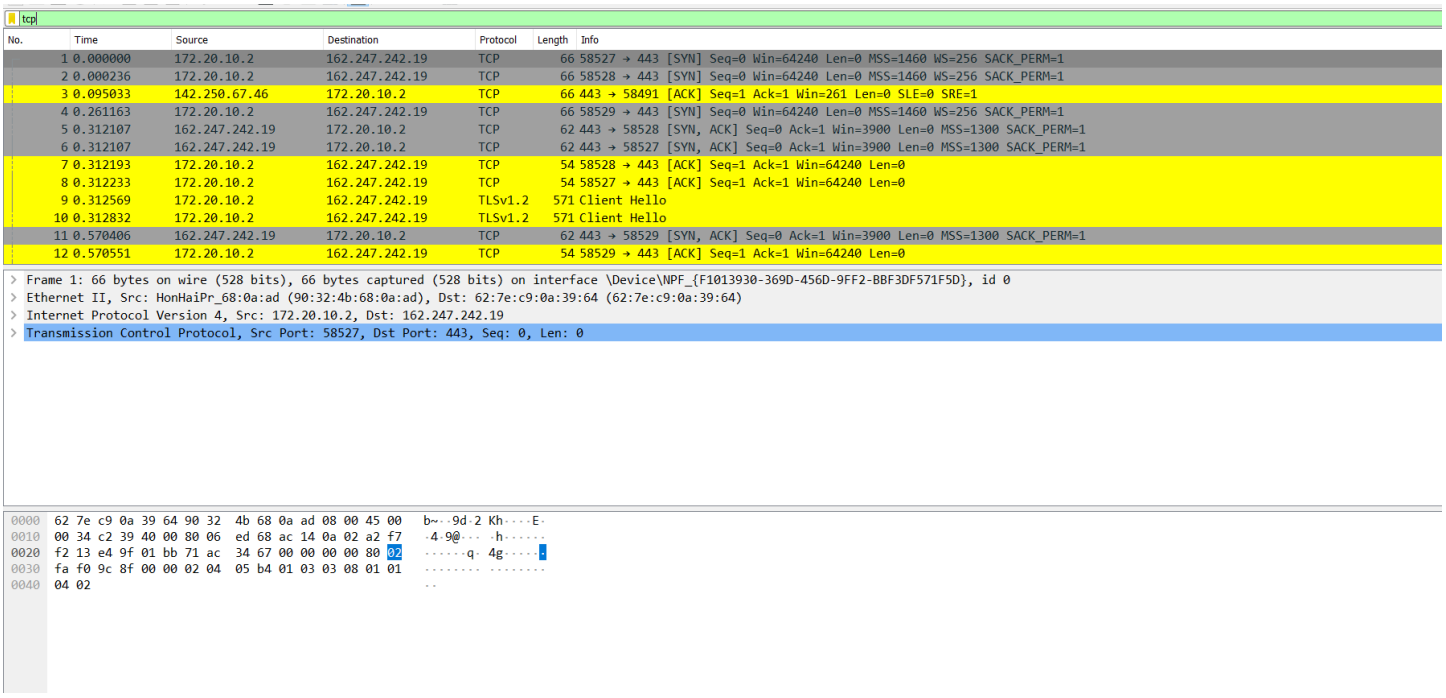
Colour coding rules



7. Observations/Discussions(For

applied/experimental sciences/materials based labs):





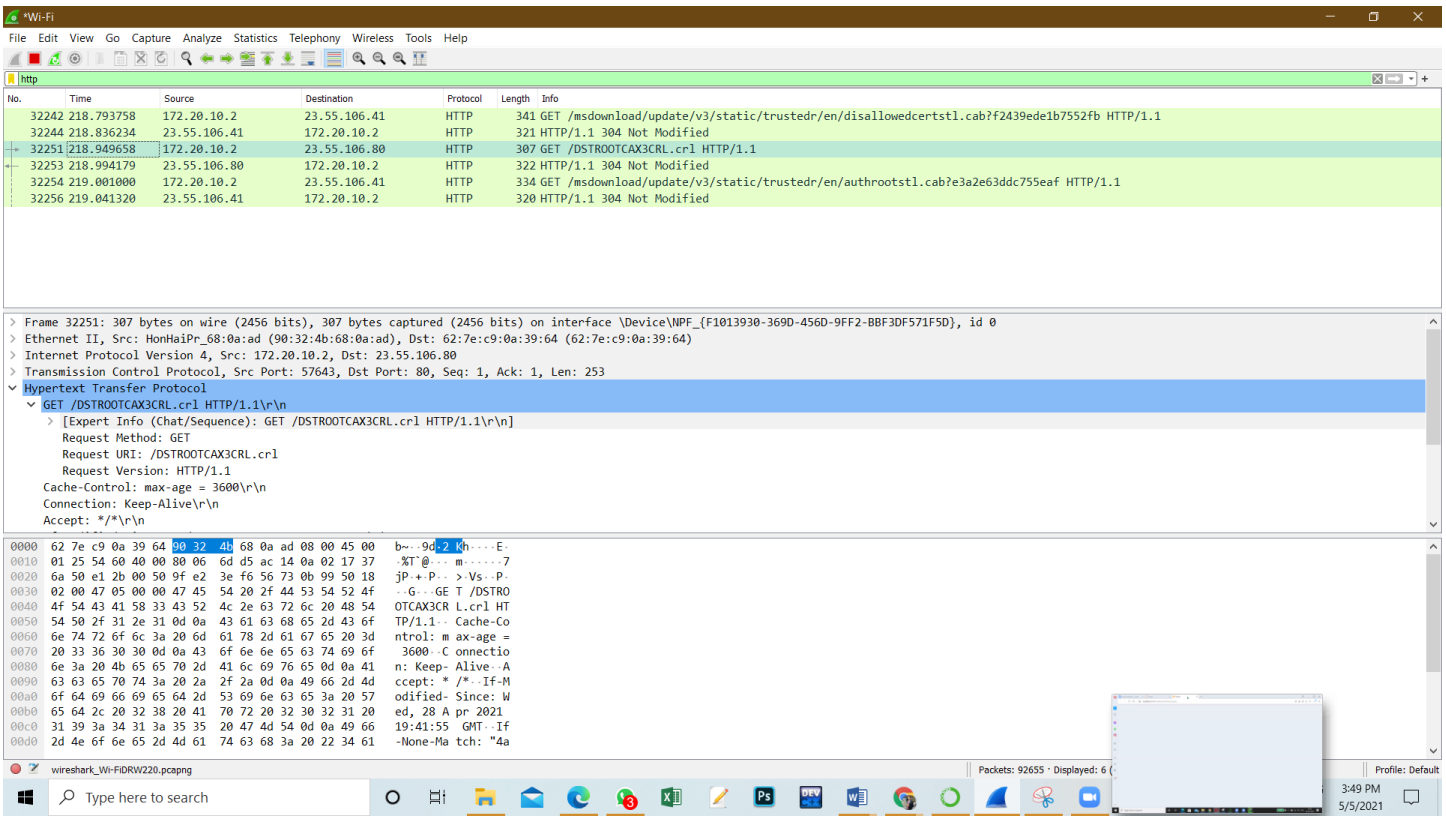
8. Percentage error (if any or applicable):

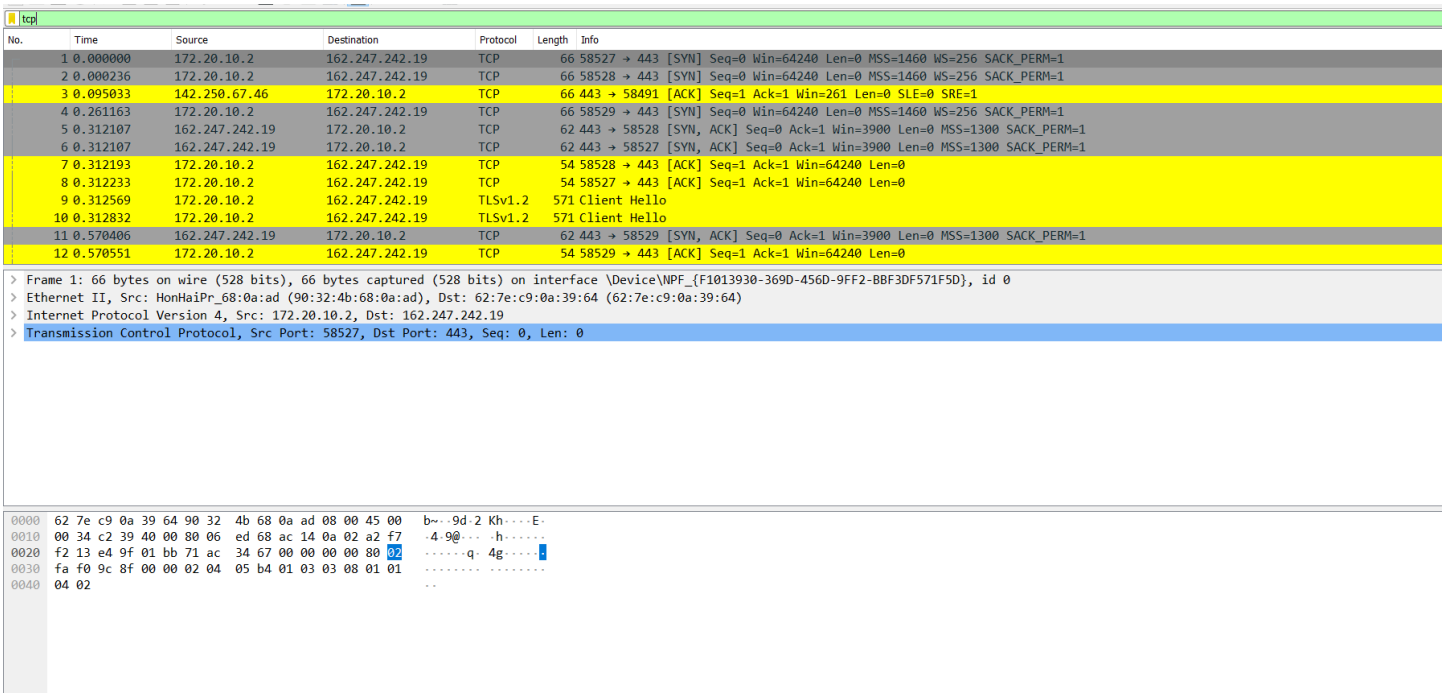
no

9. Calculations/ Chemical Reactions / Theorems /Formulas used etc :

no

10. Result/Output/Writing Summary:





11. Graphs (If Any): Image /Soft copy of graph paper to be attached here

no

Learning outcomes (What I have learnt):

1. I have learnt about http protocol.
2. I have learnt about Wireshark Network Analyzer.

3.I have learnt about sniffing.

4. I have learnt about https protocol.

Evaluation Grid (To be created as per the SOP and Assessment guidelines by the faculty):

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.			
2.			
3.			