Experiment 1.1

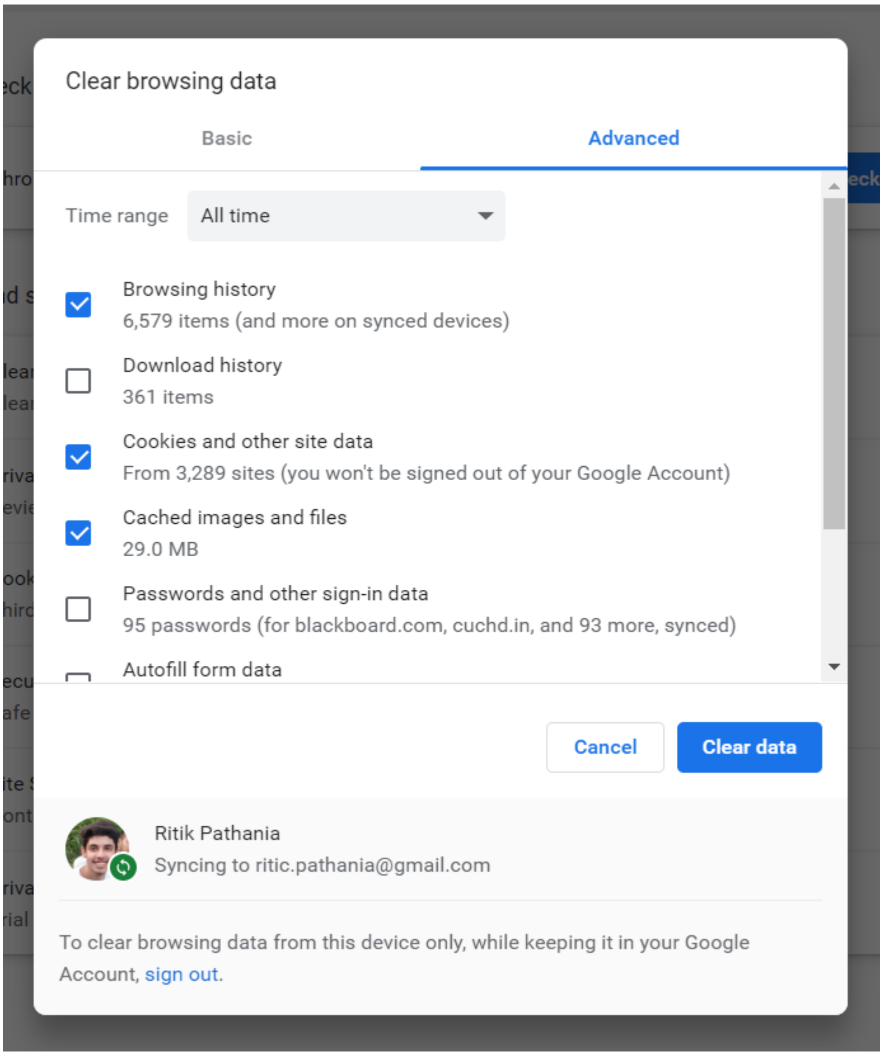
Student Name	: Ritik Pathania
UID	: 20BCS1743
Section	: 601 B
Subject Code	: 20CSP-338
Subject Name	: Web and Mobile Security Lab

Aim: Identity Http packet on Wireshark.

Requirements: To analyse HTTP traffic. We use Wireshark to analyse the HTTP traffic.

Steps for the experiment:

1. **Clearing browser cache memory:**



Clear browsing data

Time range: All time

☑ Browsing history
6,579 items (and more on synced devices)

☐ Download history
361 items

☑ Cookies and other site data
From 3,289 sites (you won't be signed out of your Google Account)

☑ Cached images and files
29.0 MB

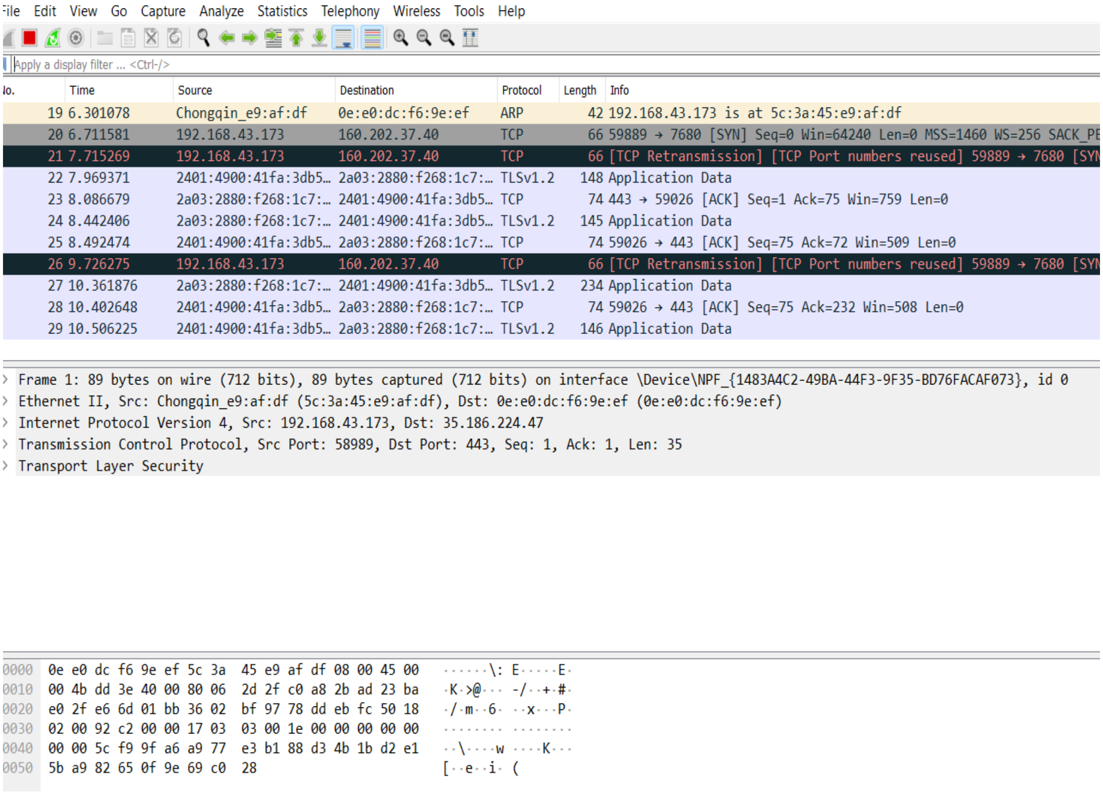
☐ Passwords and other sign-in data
95 passwords (for blackboard.com, cuchd.in, and 93 more, synced)

☐ Autofill form data

Ritik Pathania
Syncing to ritic.pathania@gmail.com

To clear browsing data from this device only, while keeping it in your Google Account, sign out.

2. Capturing the protocols:

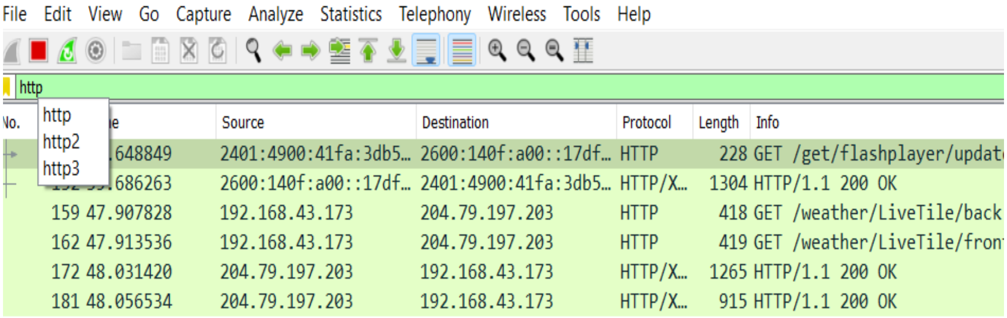

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time       Source               Destination          Protocol Length Info
  19 6.301078   Chongqin_e9:af:df    0e:e0:dc:f6:9e:ef    ARP      42 192.168.43.173 is at 5c:3a:45:e9:af:df
  20 6.711581   192.168.43.173       160.202.37.40        TCP      66 59889 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
  21 7.715269   192.168.43.173       160.202.37.40        TCP      66 [TCP Retransmission] [TCP Port numbers reused] 59889 → 7680 [SYN
  22 7.969371   2401:4900:41fa:3db5… 2a03:2880:f268:1c7:… TLSv1.2 148 Application Data
  23 8.086679   2a03:2880:f268:1c7:… 2401:4900:41fa:3db5… TCP      74 443 → 59026 [ACK] Seq=1 Ack=75 Win=759 Len=0
  24 8.442406   2a03:2880:f268:1c7:… 2401:4900:41fa:3db5… TLSv1.2 145 Application Data
  25 8.492474   2401:4900:41fa:3db5… 2a03:2880:f268:1c7:… TCP      74 59026 → 443 [ACK] Seq=75 Ack=72 Win=509 Len=0
  26 9.726275   192.168.43.173       160.202.37.40        TCP      66 [TCP Retransmission] [TCP Port numbers reused] 59889 → 7680 [SYN
  27 10.361876  2a03:2880:f268:1c7:… 2401:4900:41fa:3db5… TLSv1.2 234 Application Data
  28 10.402648  2401:4900:41fa:3db5… 2a03:2880:f268:1c7:… TCP      74 59026 → 443 [ACK] Seq=75 Ack=232 Win=508 Len=0
  29 10.506225  2401:4900:41fa:3db5… 2a03:2880:f268:1c7:… TLSv1.2 146 Application Data
```

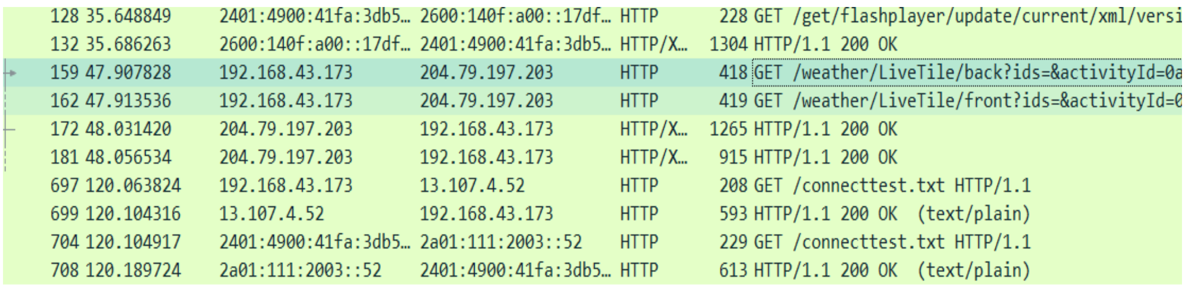
```
> Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{1483A4C2-49BA-44F3-9F35-BD76FACAF073}, id 0
> Ethernet II, Src: Chongqin_e9:af:df (5c:3a:45:e9:af:df), Dst: 0e:e0:dc:f6:9e:ef (0e:e0:dc:f6:9e:ef)
> Internet Protocol Version 4, Src: 192.168.43.173, Dst: 35.186.224.47
> Transmission Control Protocol, Src Port: 58989, Dst Port: 443, Seq: 1, Ack: 1, Len: 35
> Transport Layer Security
```

```
0000  0e e0 dc f6 9e ef 5c 3a  45 e9 af df 08 00 45 00   ······\: E·····E·
0010  00 4b dd 3e 40 00 80 06  2d 2f c0 a8 2b ad 23 ba   ·K·>@··· -/··+·#·
0020  e0 2f e6 6d 01 bb 36 02  bf 97 78 dd eb fc 50 18   ·/·m··6· ··x···P·
0030  02 00 92 c2 00 00 17 03  03 00 1e 00 00 00 00 00   ········ ········
0040  00 00 5c f9 9f a6 a9 77  e3 b1 88 d3 4b 1b d2 e1   ··\····w ····K···
0050  5b a9 82 65 0f 9e 69 c0  28                        [··e··i· (
```

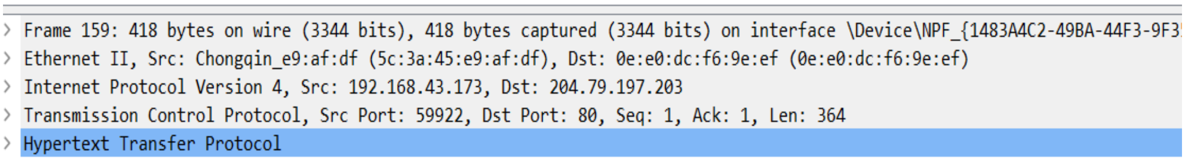
3. HTTP trafficking sites:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
http3

```
No.  Time         Source               Destination          Protocol Length Info
        648849    2401:4900:41fa:3db5… 2600:140f:a00::17df… HTTP     228 GET /get/flashplayer/updat
        686263    2600:140f:a00::17df… 2401:4900:41fa:3db5… HTTP/X…  1304 HTTP/1.1 200 OK
 159 47.907828    192.168.43.173       204.79.197.203       HTTP     418 GET /weather/LiveTile/back
 162 47.913536    192.168.43.173       204.79.197.203       HTTP     419 GET /weather/LiveTile/fron
 172 48.031420    204.79.197.203       192.168.43.173       HTTP/X…  1265 HTTP/1.1 200 OK
 181 48.056534    204.79.197.203       192.168.43.173       HTTP/X…  915 HTTP/1.1 200 OK
```



```
 128 35.648849    2401:4900:41fa:3db5… 2600:140f:a00::17df… HTTP     228 GET /get/flashplayer/update/current/xml/versi
 132 35.686263    2600:140f:a00::17df… 2401:4900:41fa:3db5… HTTP/X…  1304 HTTP/1.1 200 OK
 159 47.907828    192.168.43.173       204.79.197.203       HTTP     418 GET /weather/LiveTile/back?ids=&activityId=0a
 162 47.913536    192.168.43.173       204.79.197.203       HTTP     419 GET /weather/LiveTile/front?ids=&activityId=0
 172 48.031420    204.79.197.203       192.168.43.173       HTTP/X…  1265 HTTP/1.1 200 OK
 181 48.056534    204.79.197.203       192.168.43.173       HTTP/X…  915 HTTP/1.1 200 OK
 697 120.063824   192.168.43.173       13.107.4.52          HTTP     208 GET /connecttest.txt HTTP/1.1
 699 120.104316   13.107.4.52          192.168.43.173       HTTP     593 HTTP/1.1 200 OK  (text/plain)
 704 120.104917   2401:4900:41fa:3db5… 2a01:111:2003::52    HTTP     229 GET /connecttest.txt HTTP/1.1
 708 120.189724   2a01:111:2003::52    2401:4900:41fa:3db5… HTTP     613 HTTP/1.1 200 OK  (text/plain)
```



```
> Frame 159: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface \Device\NPF_{1483A4C2-49BA-44F3-9F3
> Ethernet II, Src: Chongqin_e9:af:df (5c:3a:45:e9:af:df), Dst: 0e:e0:dc:f6:9e:ef (0e:e0:dc:f6:9e:ef)
> Internet Protocol Version 4, Src: 192.168.43.173, Dst: 204.79.197.203
> Transmission Control Protocol, Src Port: 59922, Dst Port: 80, Seq: 1, Ack: 1, Len: 364
> Hypertext Transfer Protocol
```

Learning outcomes (What I have learnt):

Identify requests (from the client) and response packets. Find HTTP version, response code/phrase, requested file (including size). Observe a single small file (e.g., a simple HTML file) request/response behaviour and the request/response behaviour for a file that has already been received. Observe how a larger file is sent in multiple segments Observe multi-file (e.g., a web page with an image) request/response behaviour. Observe request/response behaviour for a page that needs authentication.

Evaluation Grid (To be created per the faculty's SOP and Assessment guidelines):

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Worksheet completion including writing learning objectives/Outcomes. (To be submitted at the end of the day).		
2.	Post-Lab Quiz Result.		
3.	Student Engagement in Simulation/Demonstration/Performance and Controls/Pre-Lab Questions.		
	Signature of Faculty (with Date):	Total Marks Obtained:	