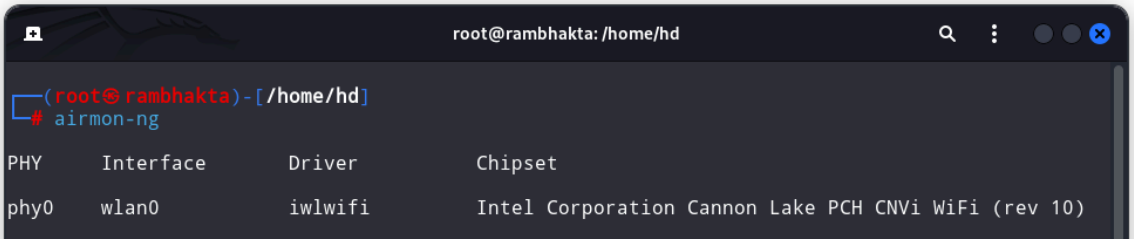
Hands-on Session: Simple Attacks on Wi-Fi Networks

Group Details :

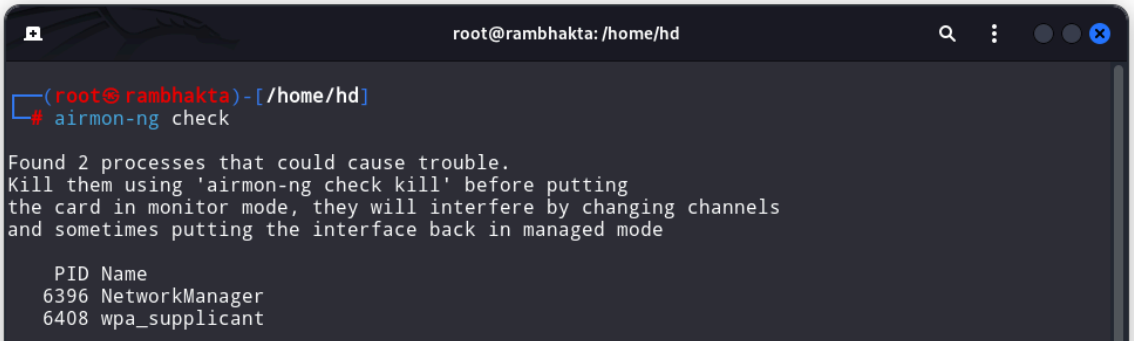
CS23MTECH11029	Patel Heetkumar Dilipbhai
CS23MTECH13001	Anil kumar Sharma
CS23MTECH13002	KR Anuraj

Task 1 : DoS attacks on a victim Wi-Fi STA

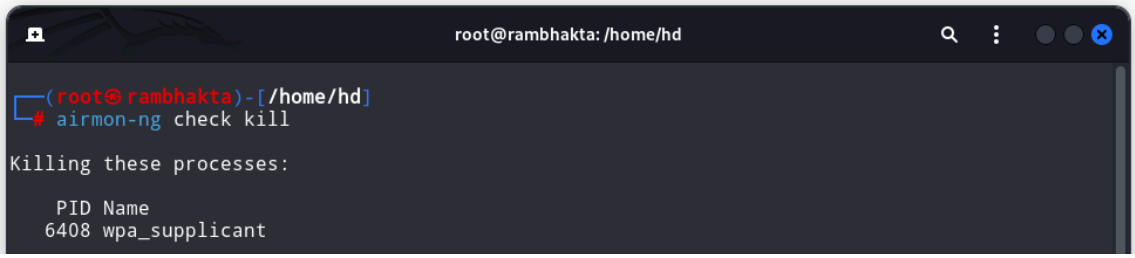
Checking the available interface using the "**airmon-ng**" command.



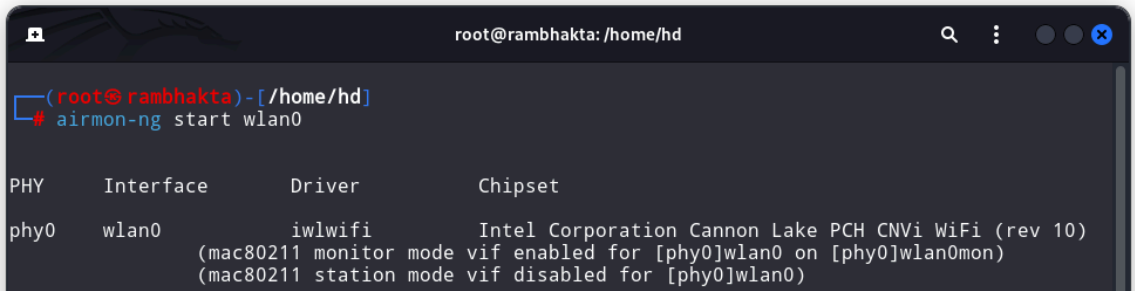
Checking any unnecessary network process going on using the "**airmon-ng check**" command.



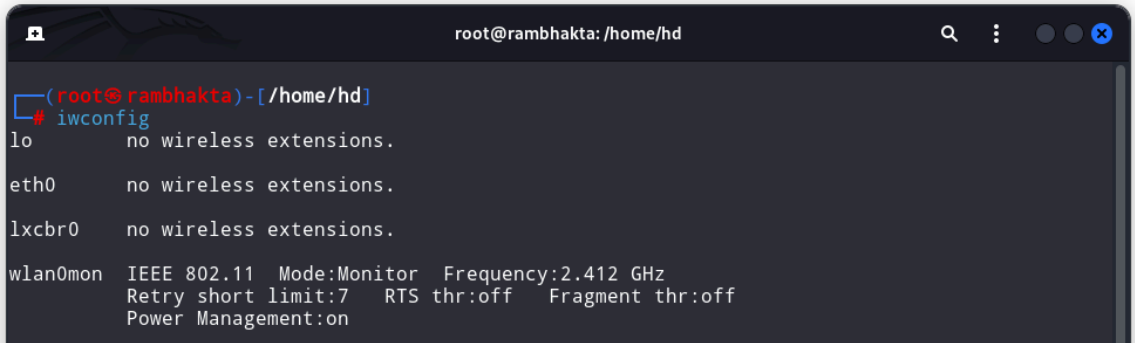
Killing unnecessary process using the "**airmon-ng check kill**" command.



Starting **monitor mode** using airmon-ng on the wlan0 interface using the "**airmon-ng start wlan0**" command.

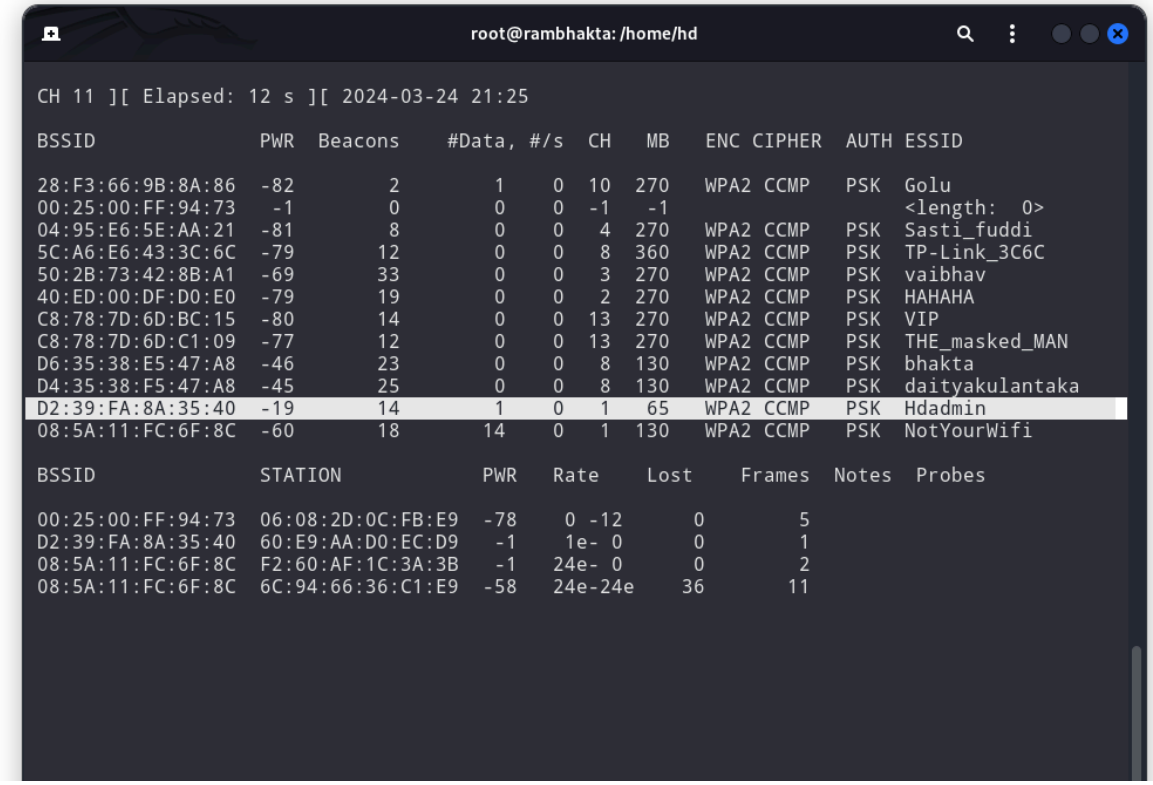


Checking whether monitor mode is enabled or not using the "**iwconfig**" command.

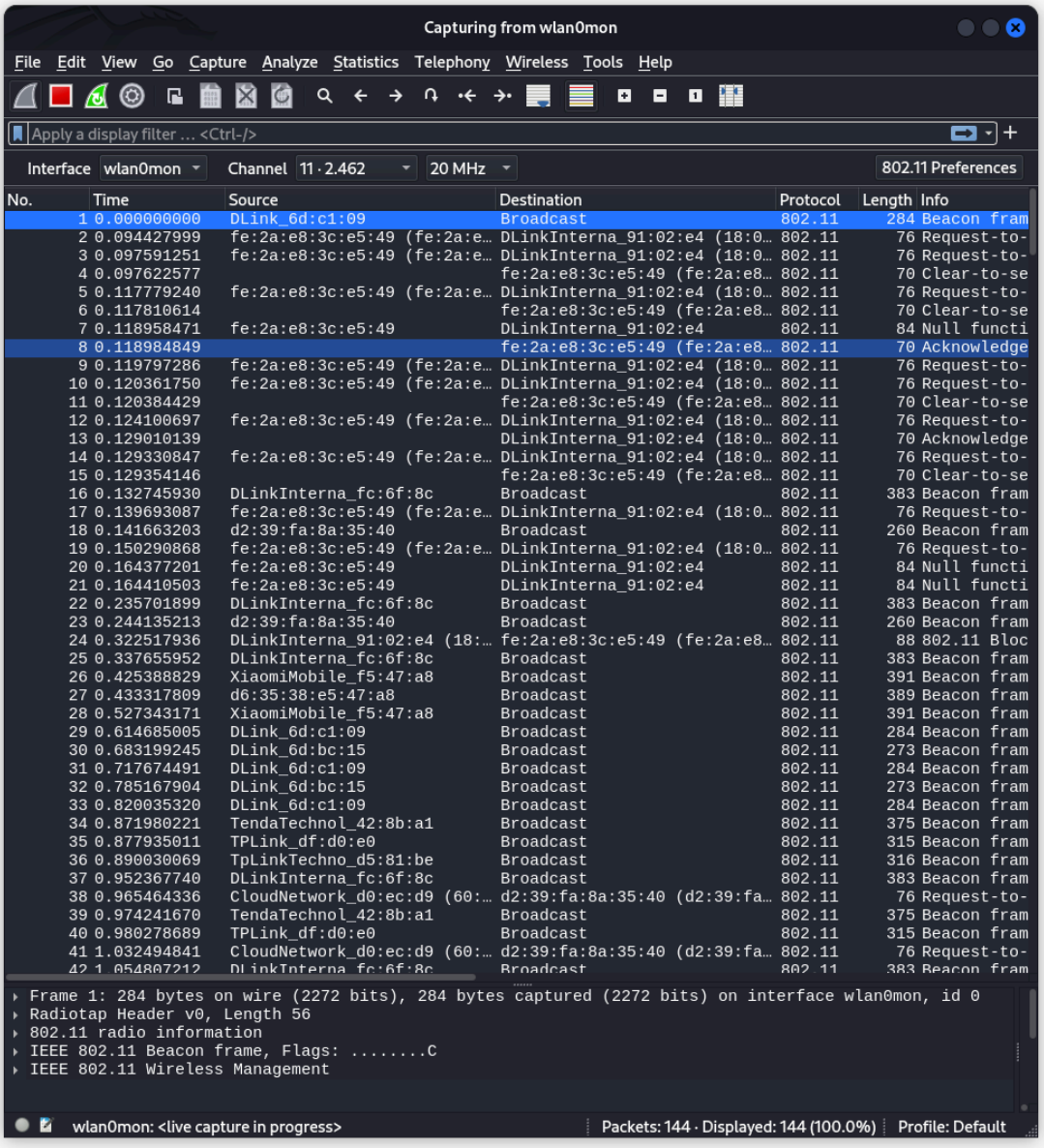


Hands-on Session: Simple Attacks on Wi-Fi Networks

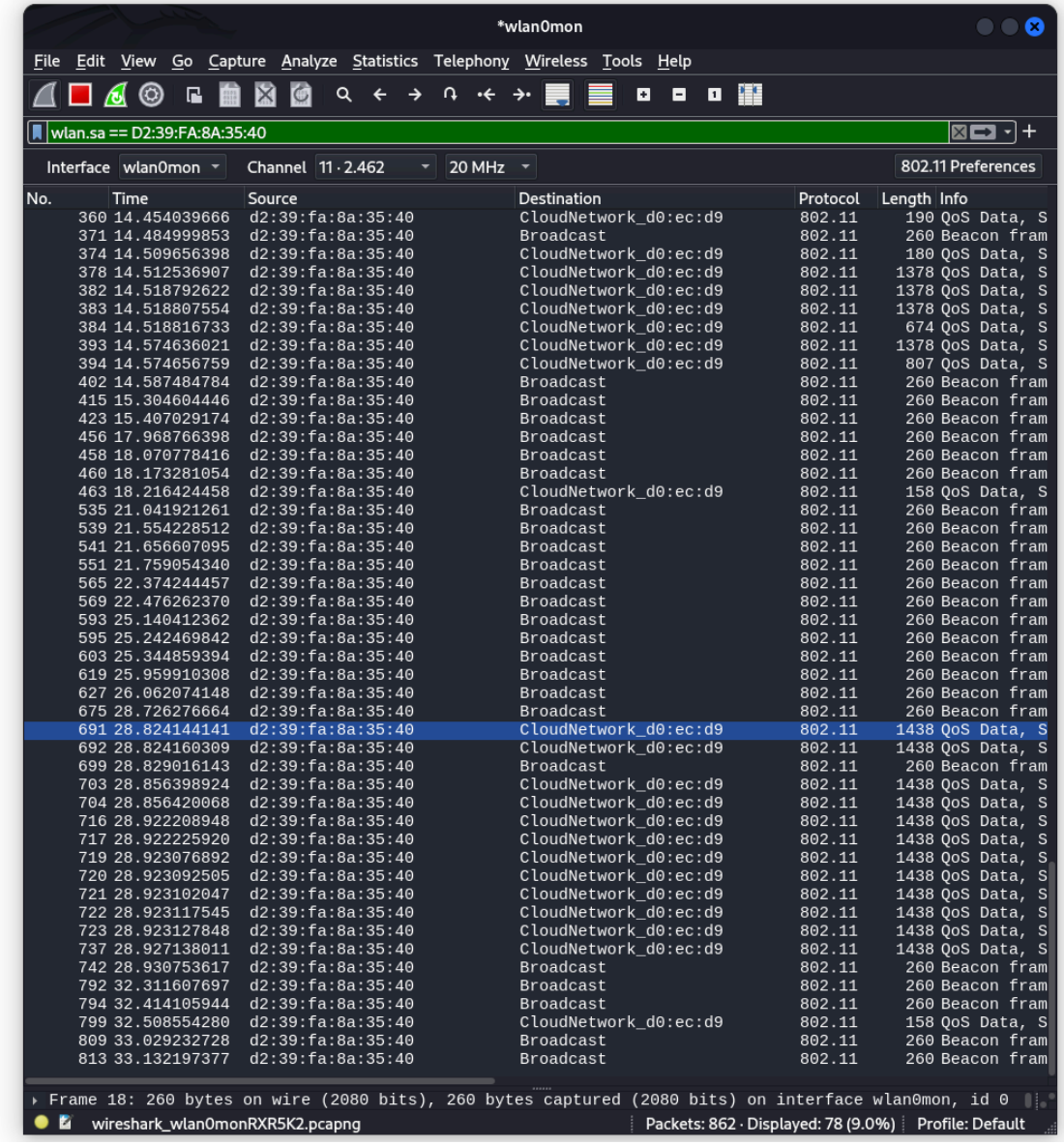
Checking the available access points on the monitor mode interface using “**airodump-ng wlan0mon**” command.



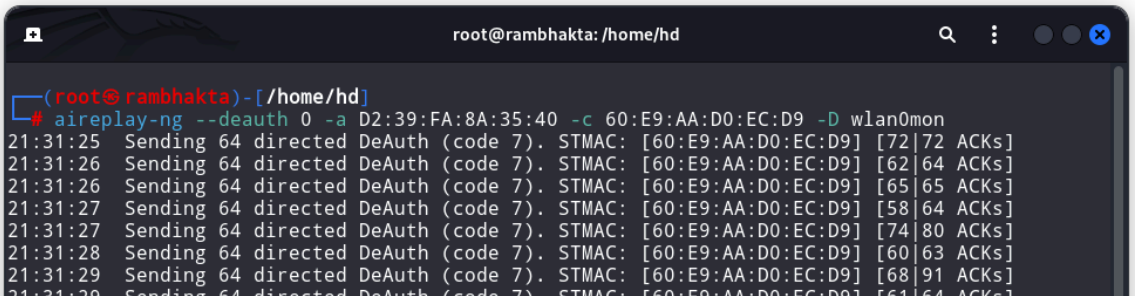
Now we can see traffic by turning wireshark on the wlan0mon monitor mode interface.



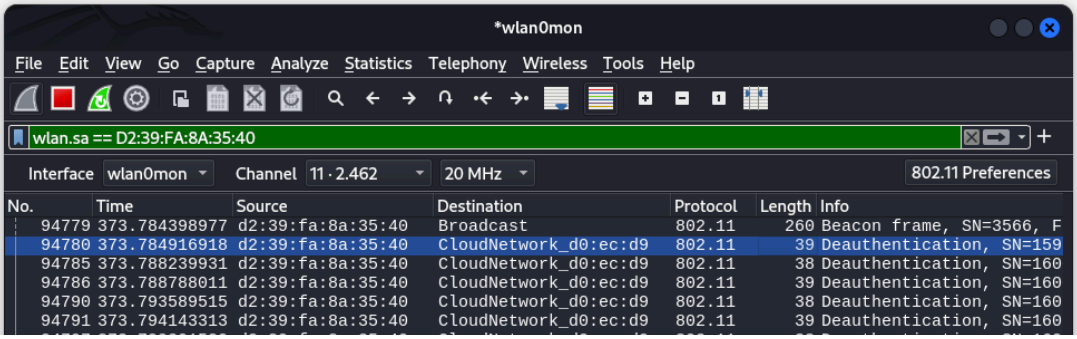
To filter out our target access point traffic we can filter traffic using its MAC address as below.



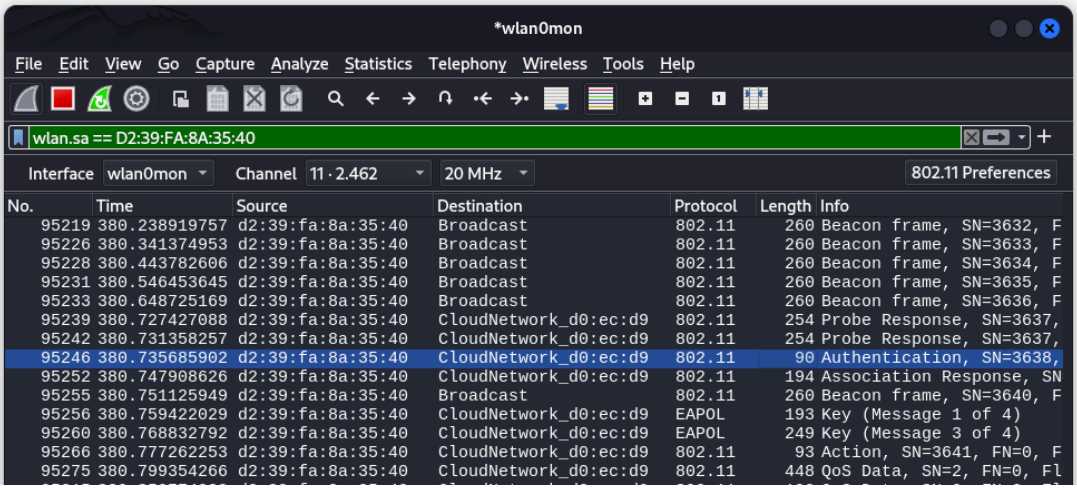
Sending deauth packet using aireplay-ng on victim's MAC using "**aireplay-ng –deauth 0 -a (Access point MAC addr) -c (Client's MAC addr) -D wlan0mon**" command.



We can see in wireshark below that deauth packets were sent to the victim's device.

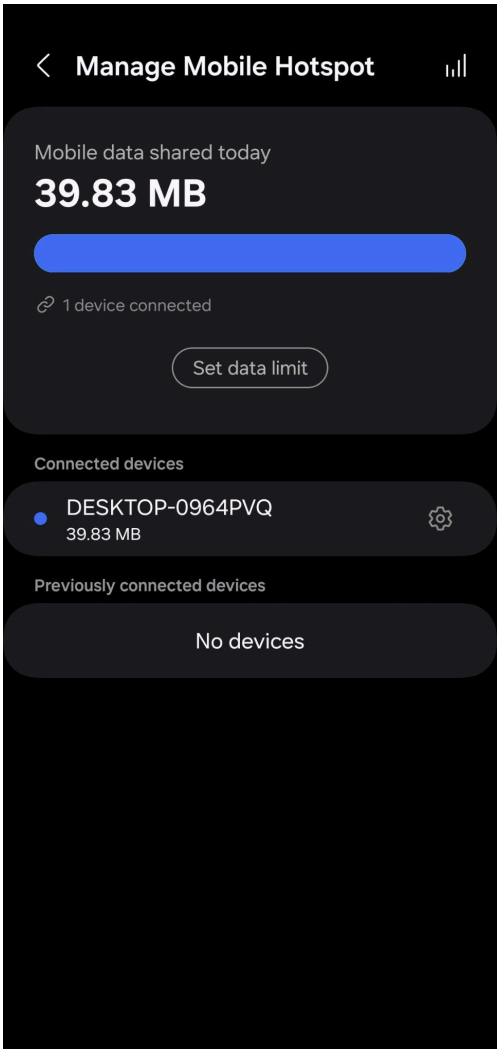


After deauth packet stops, the victim tries to reconnect as shown with the blue highlighted line in the below image.

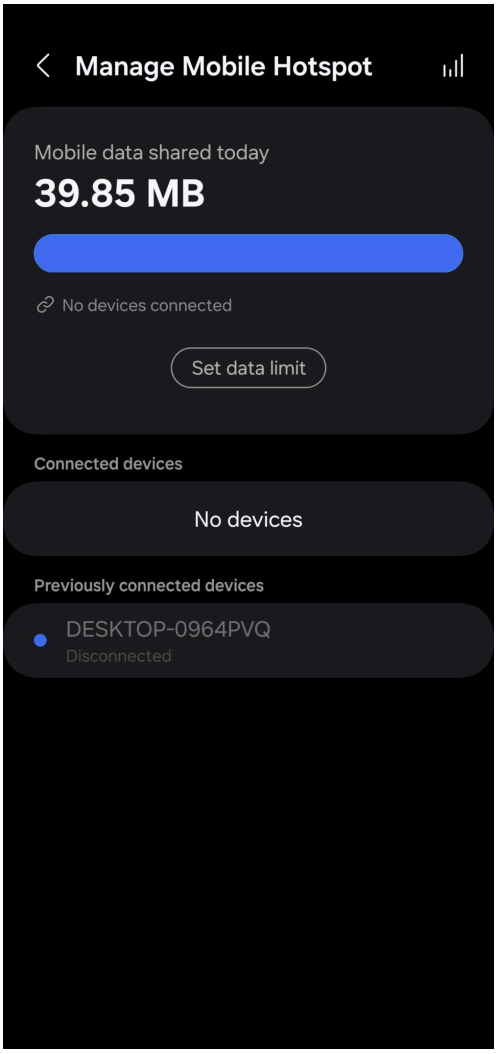


Hands-on Session: Simple Attacks on Wi-Fi Networks

Withouth Deauth

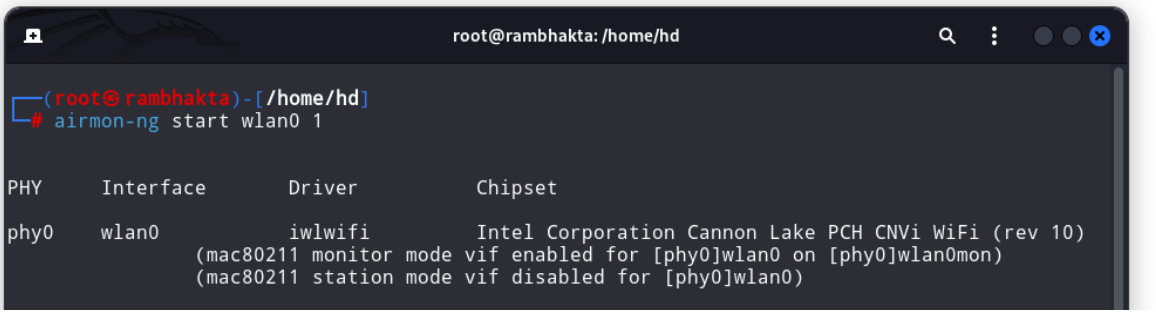


While Deauth

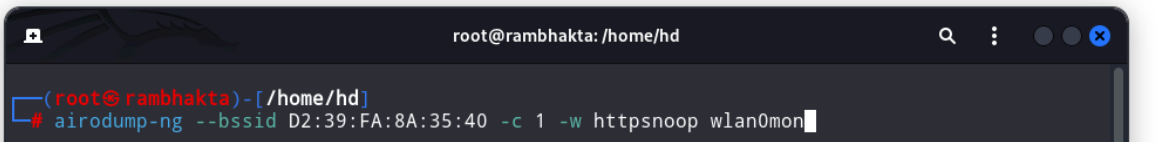


Task-2: Snoop into HTTP traffic of a victim Wi-Fi STA

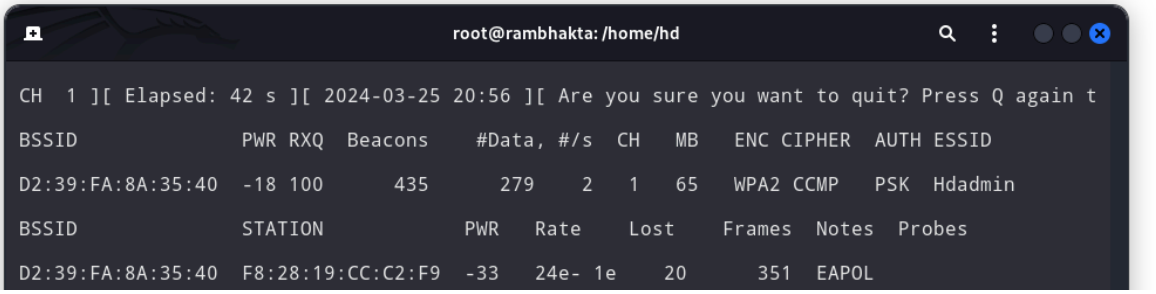
Turning the monitor mode using "**airmon-ng start wlan0**" command.



Starting packet capturing on access point's MAC address using "**airdump-ng –bssid (Access point MAC addr) -c 1 -w httpsnoop wlan0mon**" command, where c is channel no on which access point is enabled.

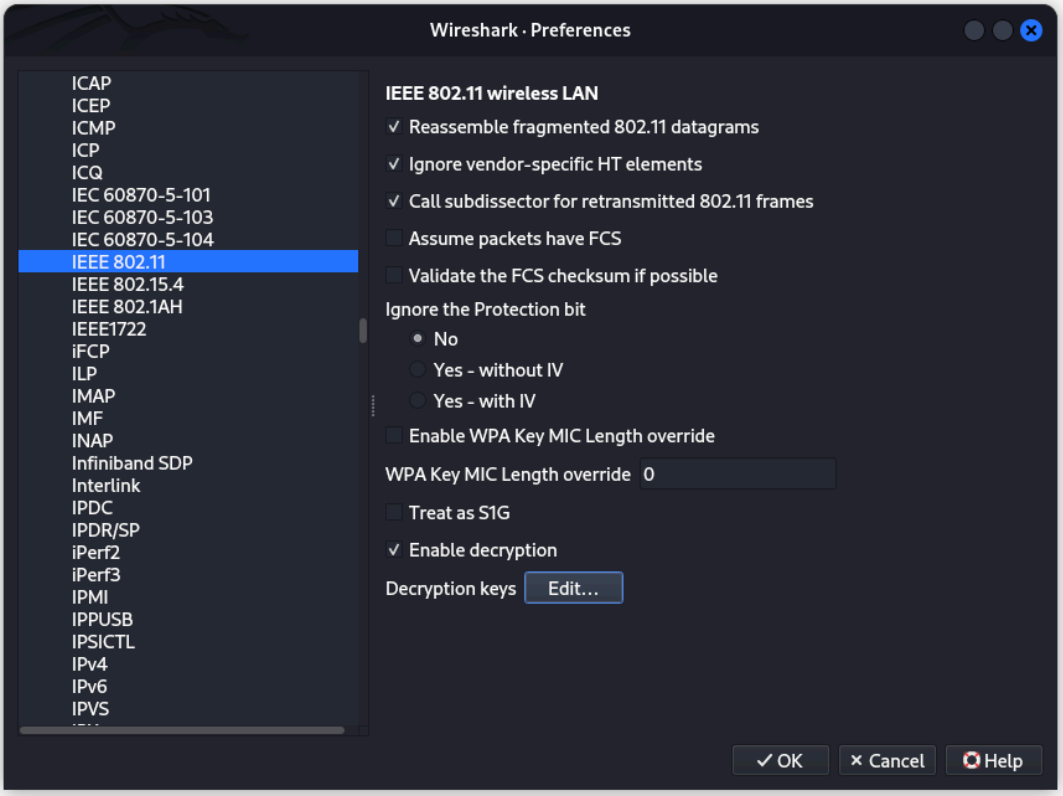


Now you can see in the image below the packet capture starts.

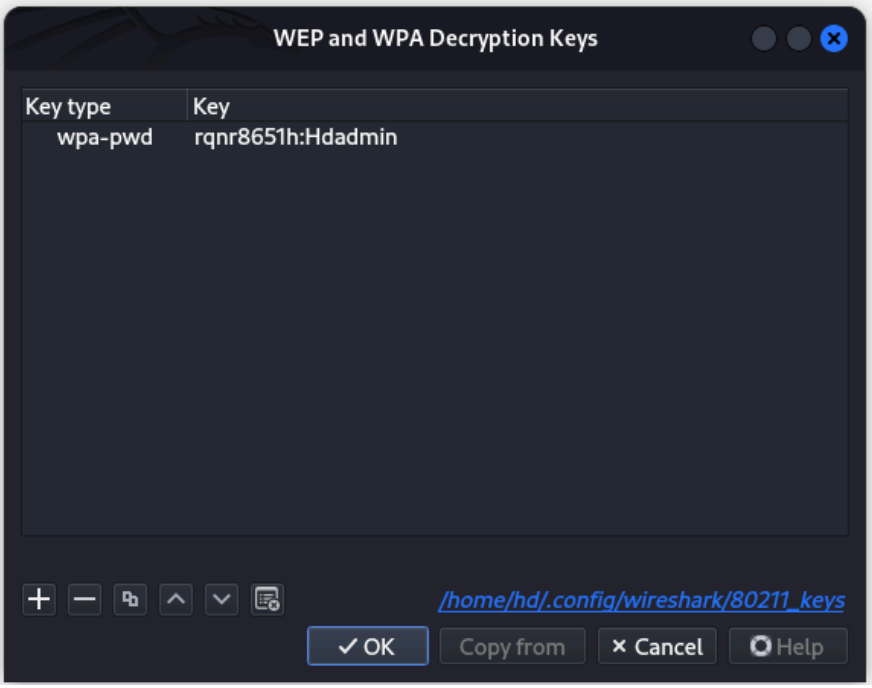


Now to decrypt the encryption at link layer go to **Edit -> Preference -> Protocols -> IEEE 802.11**

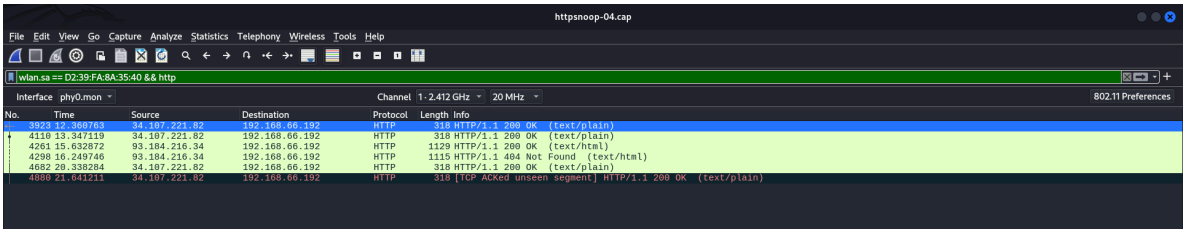
Enable the **Toggle button to enable decryption** (last second option in below image).



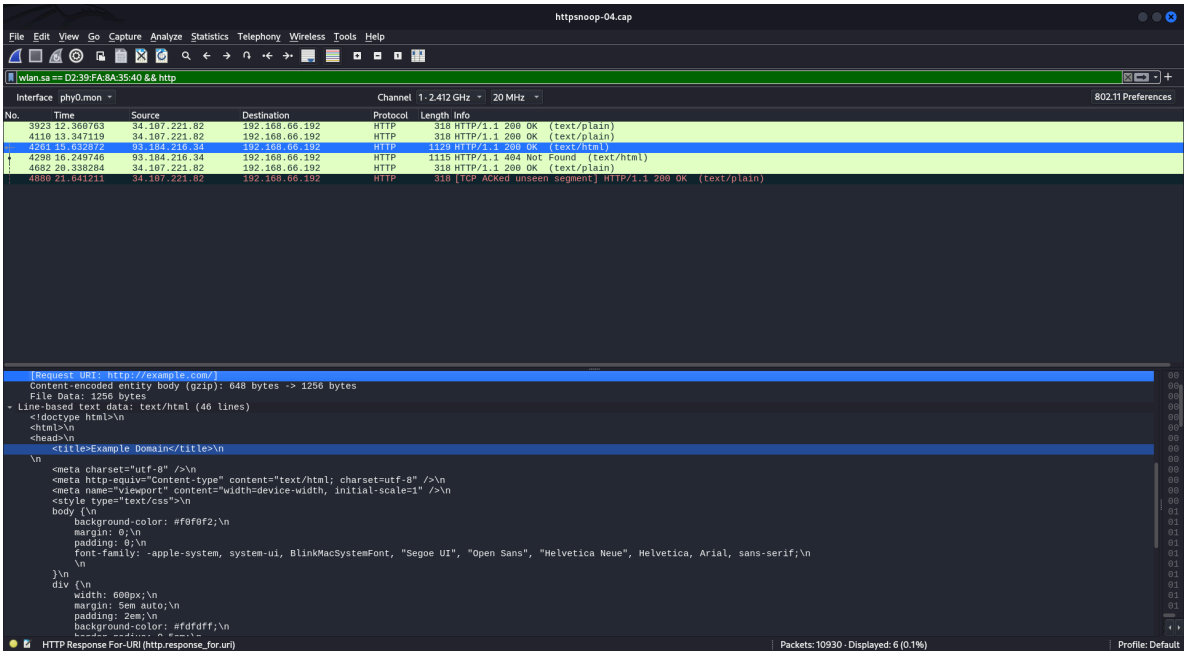
Setting the **wpa-pwd with [pwd]:[ssid]** as shown below.



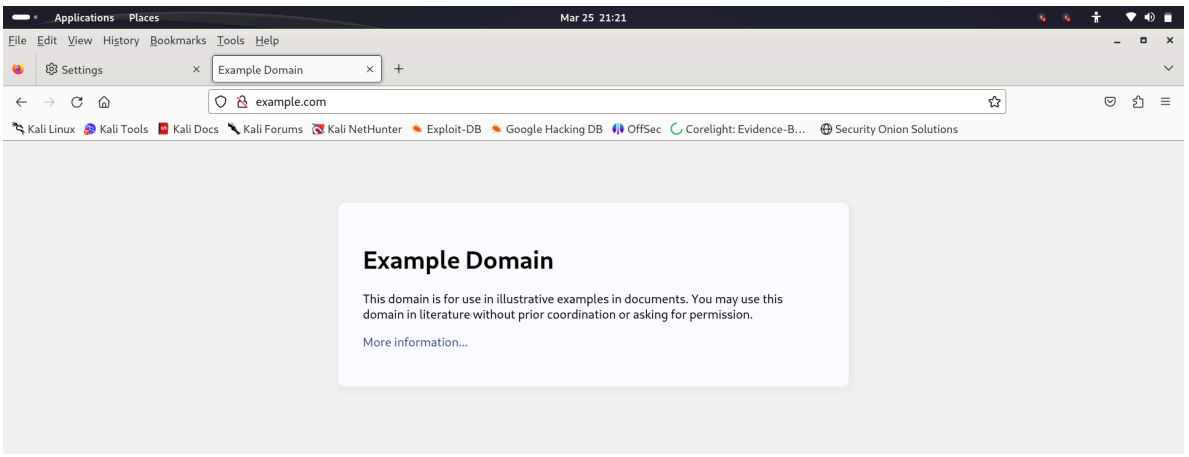
On filtering the http packets on our access point we can see some packets as shown in the image below.



Here client is accessing example.com on http whose html code is shown in one packet as you can see in the blue highlighted line below which shows successful snooping of http traffic.



Client's view.

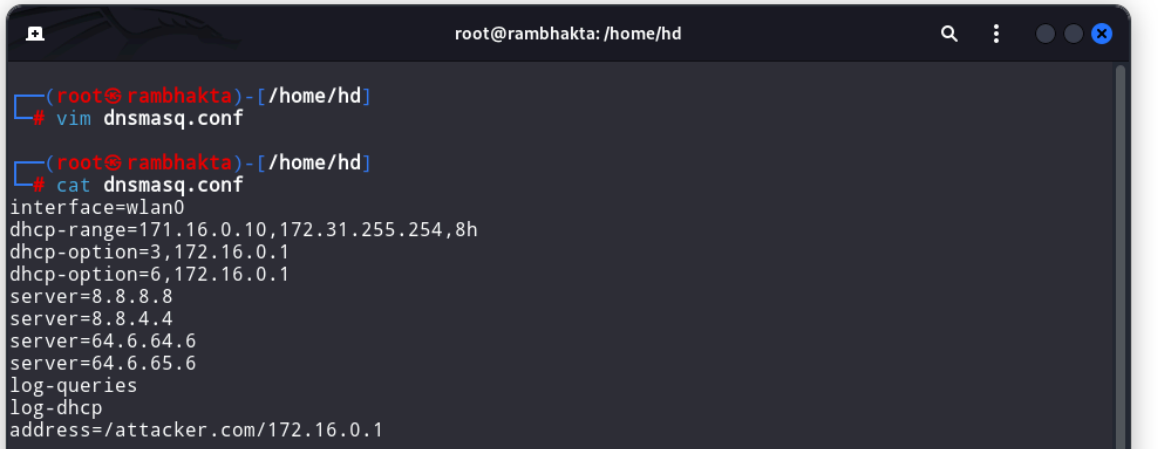


Task-3: MITM attacks on a Wi-Fi Network

We are attempting a **MITM attack by creating an evil twin hotspot (rogue AP)** on a genuine Wi-Fi network using **hostapd** and **dnsmasq** tools.

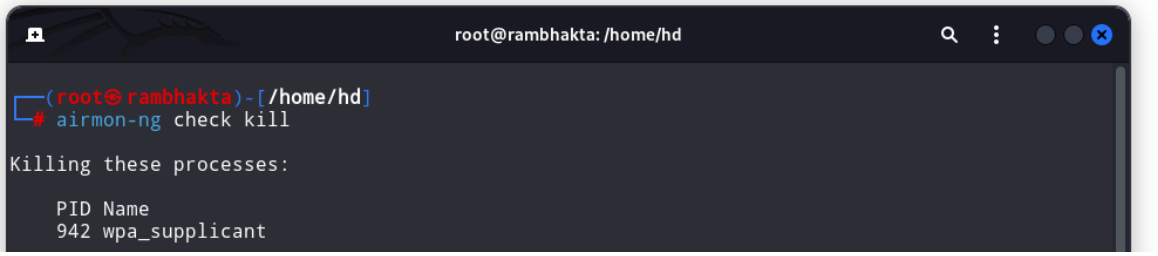
Now to create fake hotspot we are creating 2 config files, one for hostapd and one for dnsmasq.

dnsmasq.conf

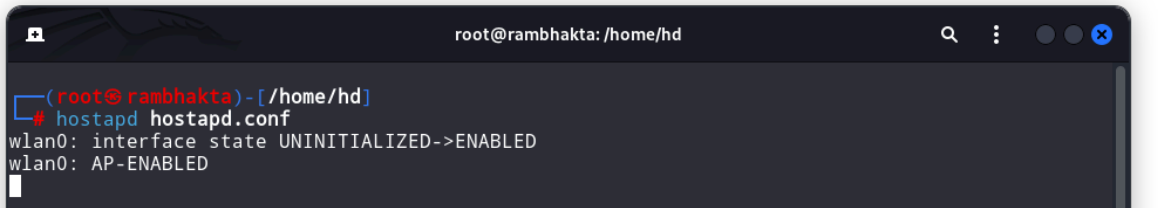


hostapd.conf

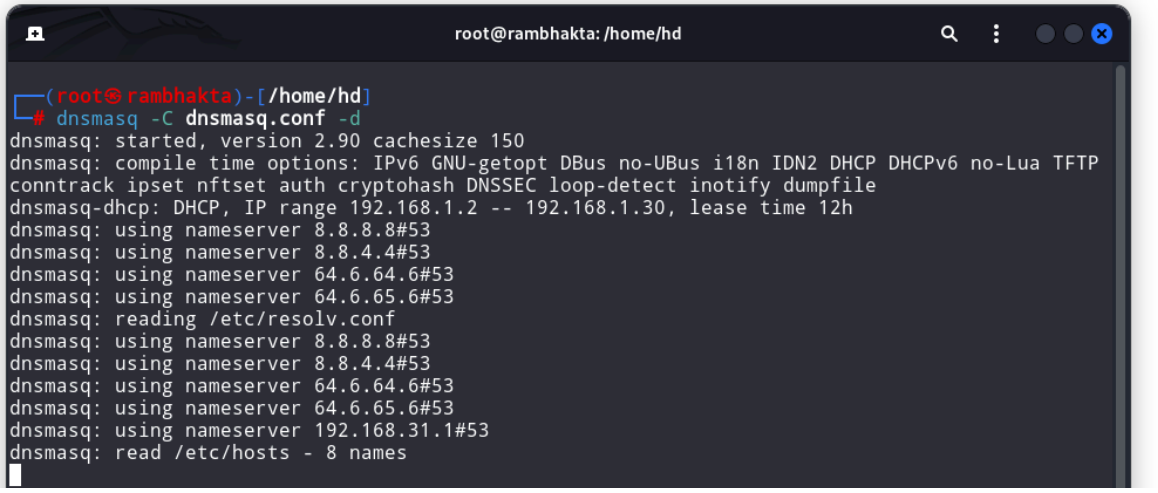
Before creating a hotspot we have to remove unnecessary network processes which can harm our process using the "**airmon-ng check kill**" command.



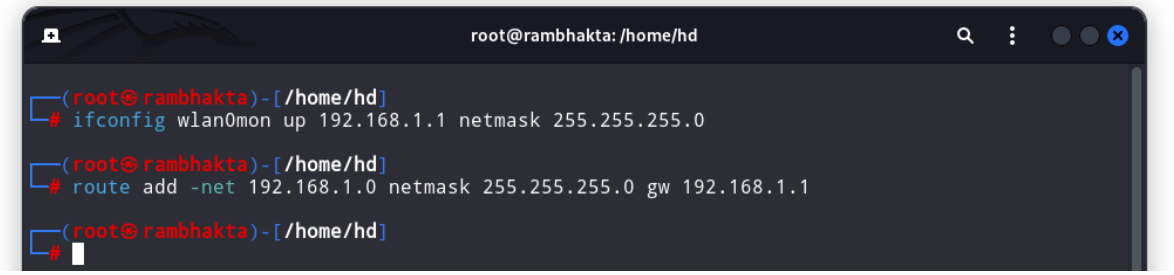
Now to **create a hotspot** using the **hostapd.conf** file, execute the "**hostapd hostapd.conf**" command.



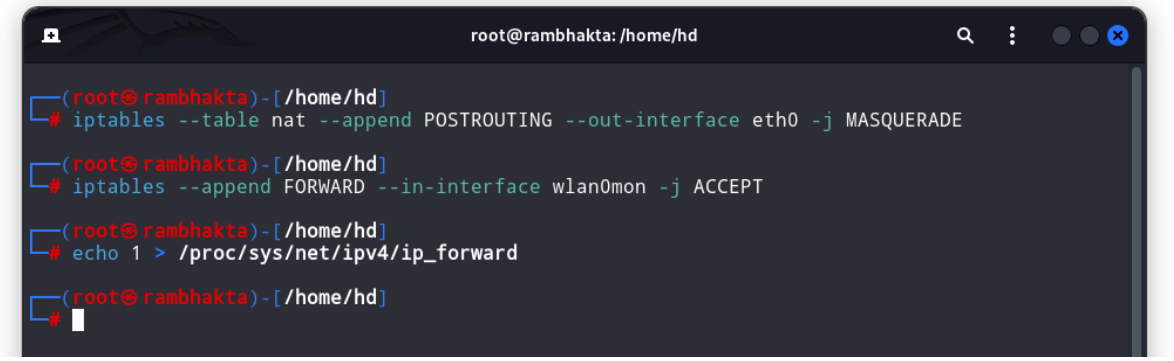
Creating dns for our hotspot so that newly connected devices can get an ip address to connect with the internet. For that we have to execute the "**dnsmasq -C dnsmasq.conf -d**" command.



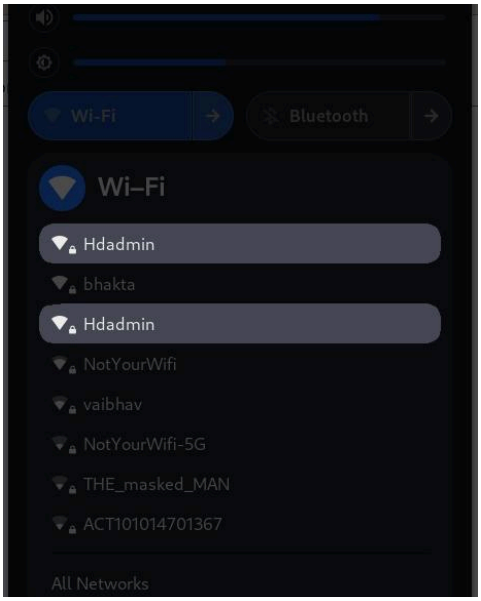
Assigning IP, gateway and netmask to access point.



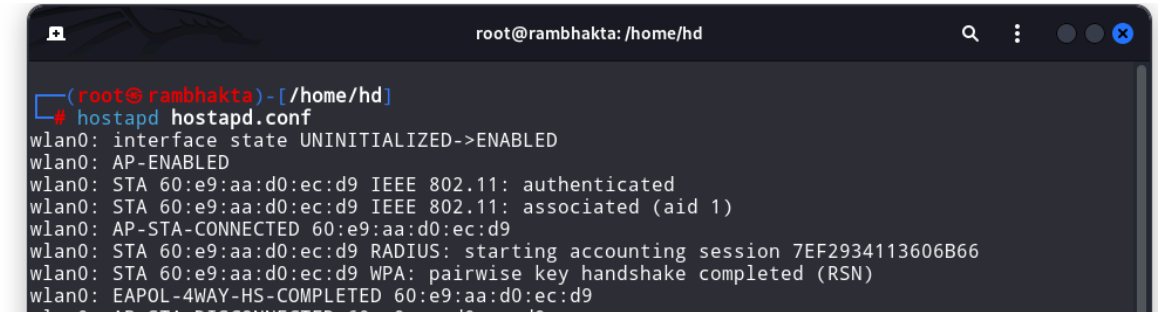
Adding forwarding properties so that traffic from client will be sent to some interface which is connected to the internet so that client can't be able to know that there is some issue with access point and he/she can be able to access the internet.



Now at this stage we have a fully functional fake hotspot ready with us as we can see two hotspots with the same SSID in the image below.

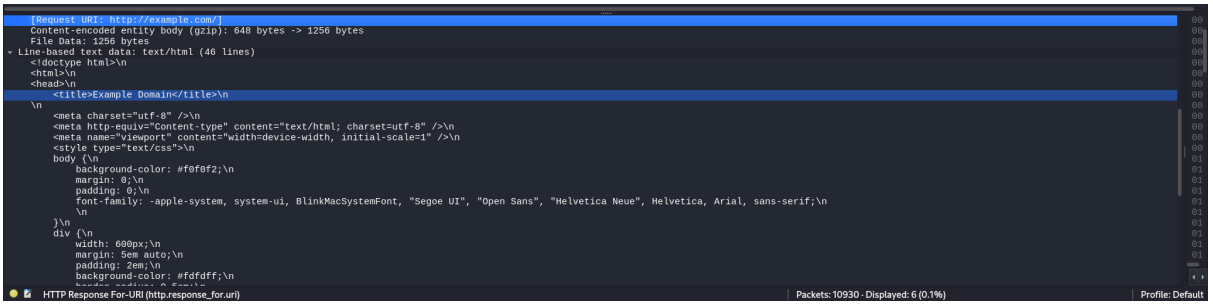


We can see in the image below the client is connected to our fake hotspot and the 4 way handshake is completed.

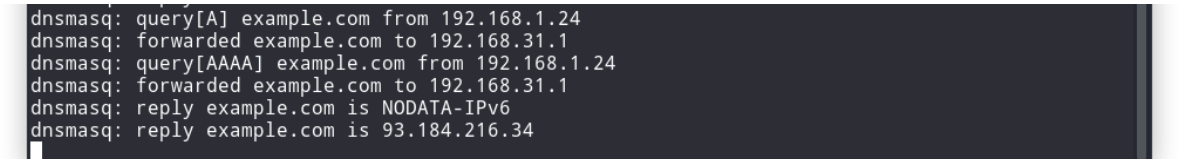


Step 2 : To perform a **passive attack** on this we can simply capture packets on this interface where the hotspot is running.

Here on capturing we can capture http traffic of the client on our fake wifi and we can see the code of **example.com** is sent as response from server to client on his/her request.

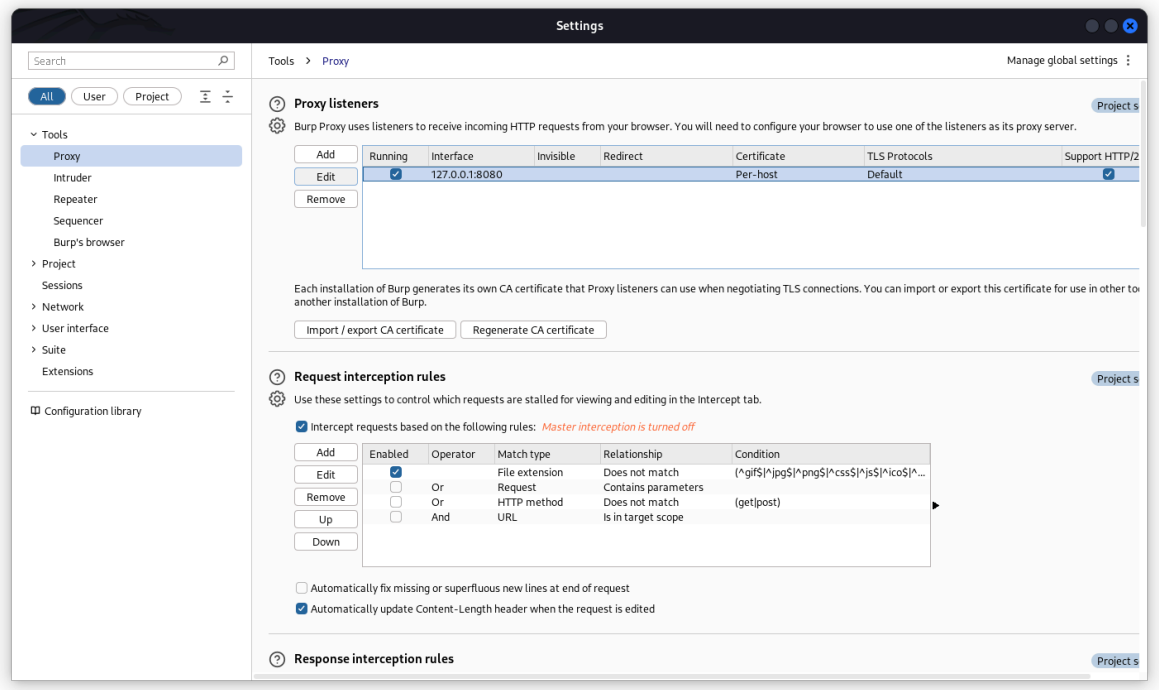


At the same time we can also see the DNS query of client requesting sites i.e. **example.com**.

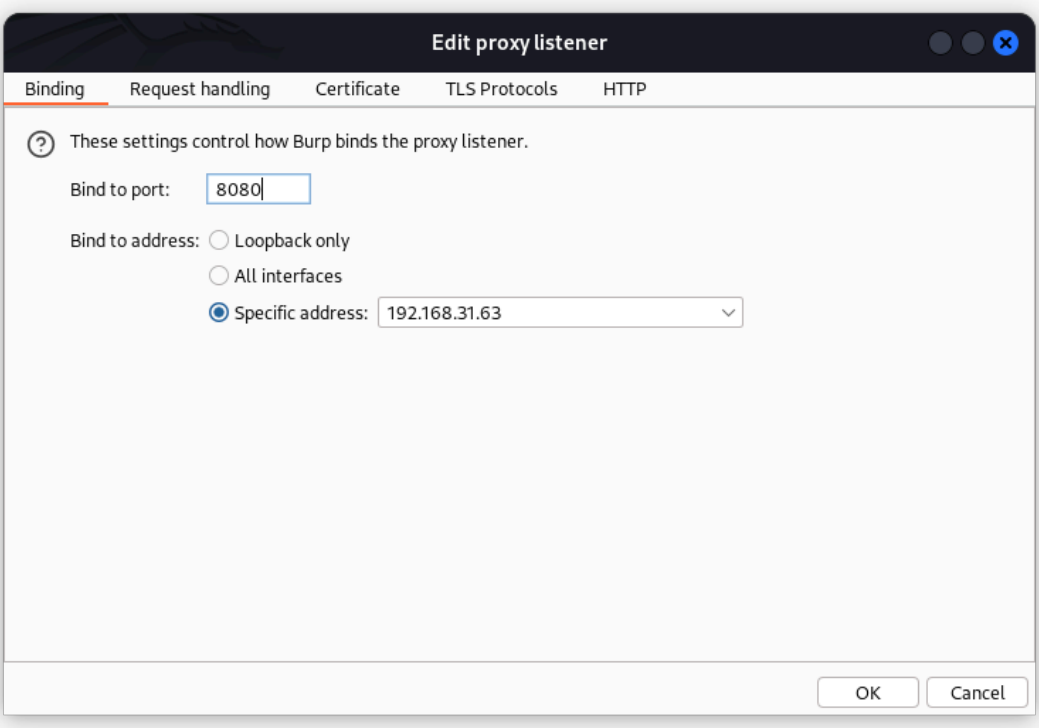


Step 3 : To perform an **active attack**, we are setting the **burpsuite as a transparent proxy** on the access point.

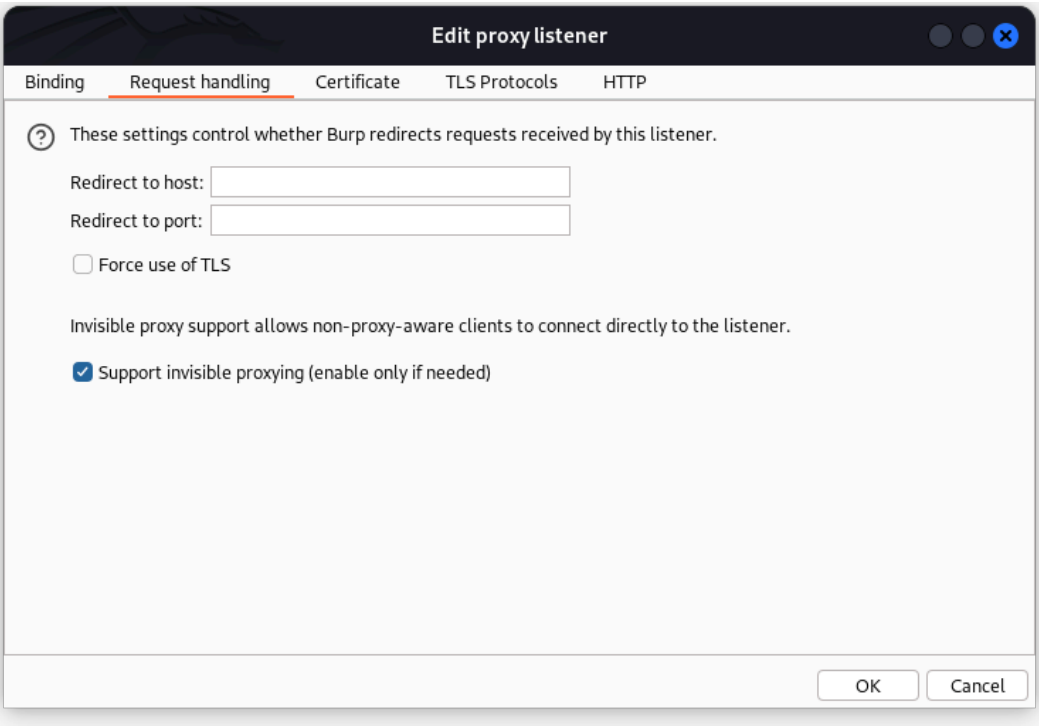
To setup proxy go to **Proxy tab -> Proxy setting -> Proxy listener** as shown in below image



Now **edit or add a new listener rule**, here we are using **8080 port with specific ip 192.168.31.63**.

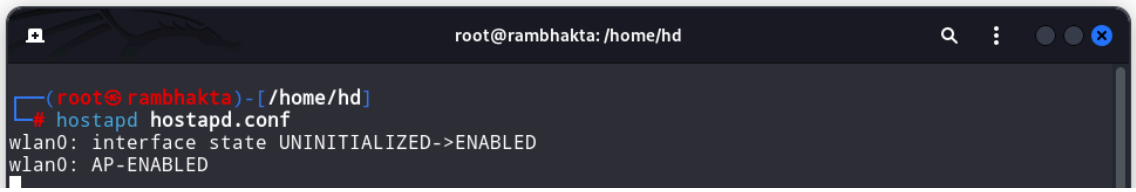


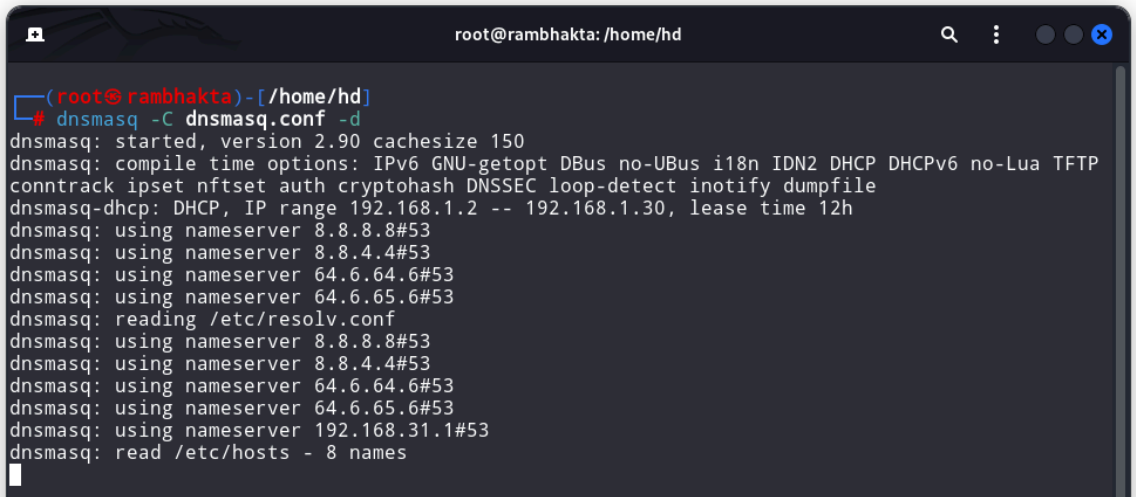
Toggle invisible proxy button to turn on transparent proxy.



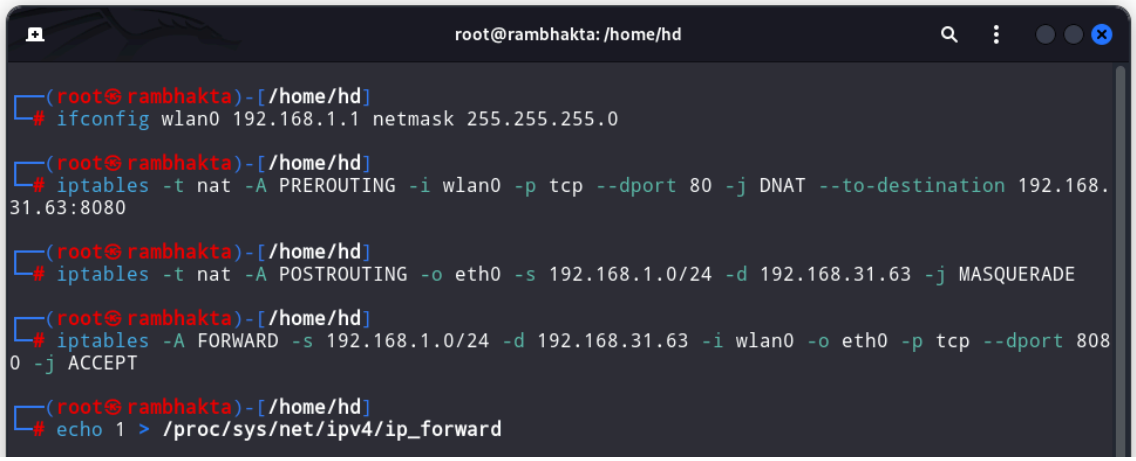
Now **turn on the Intercept on** in the proxy tab.

Turning hotspot and it dns as done before in step 2.

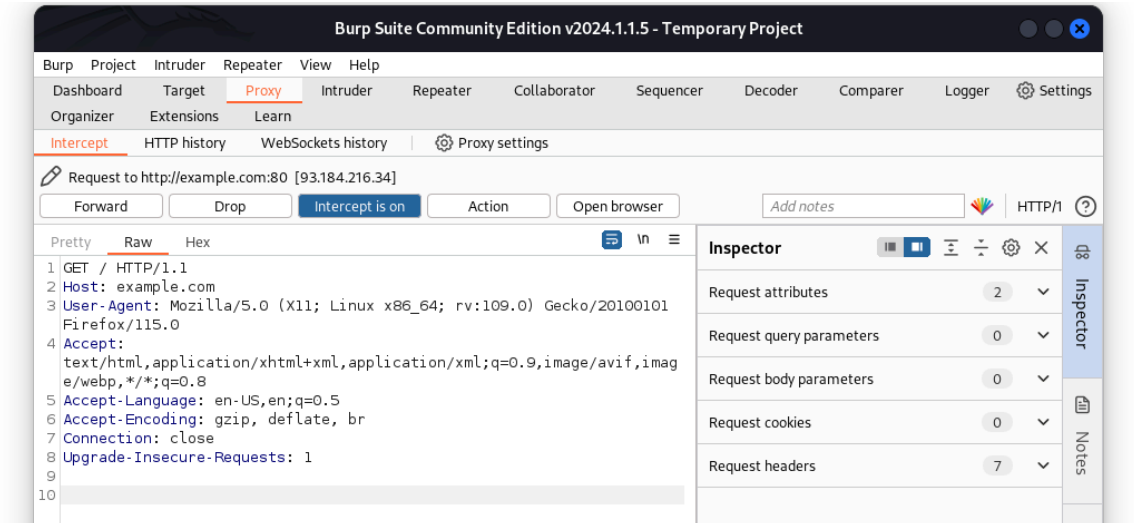




Adding forwarding rules, show that request from client goes to server via the burpsuite proxy and response from server goes to client via burpsuite proxy.

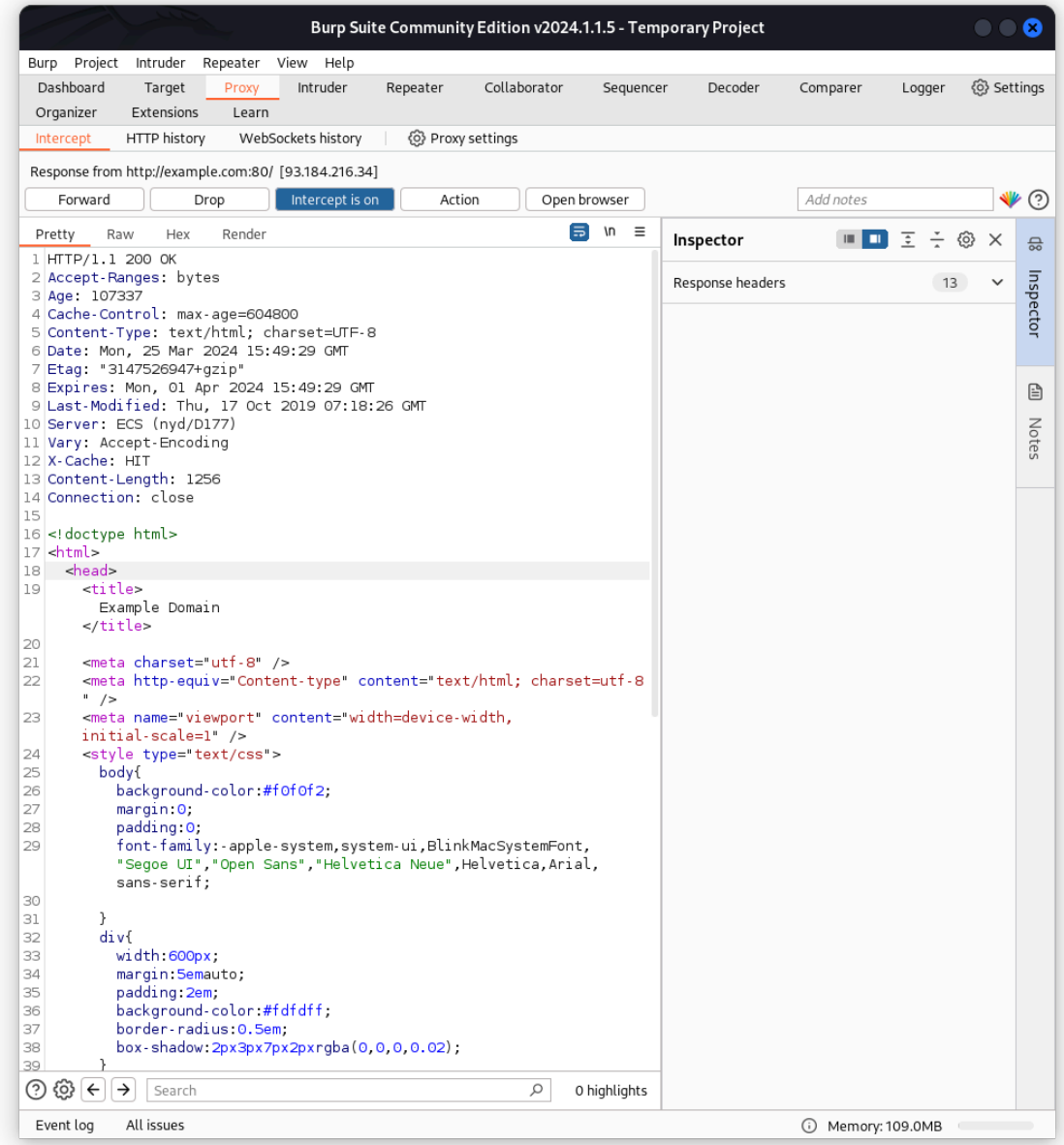


Now when client request some website like example.com here the request first come to buprsuite proxy as shown in below image.



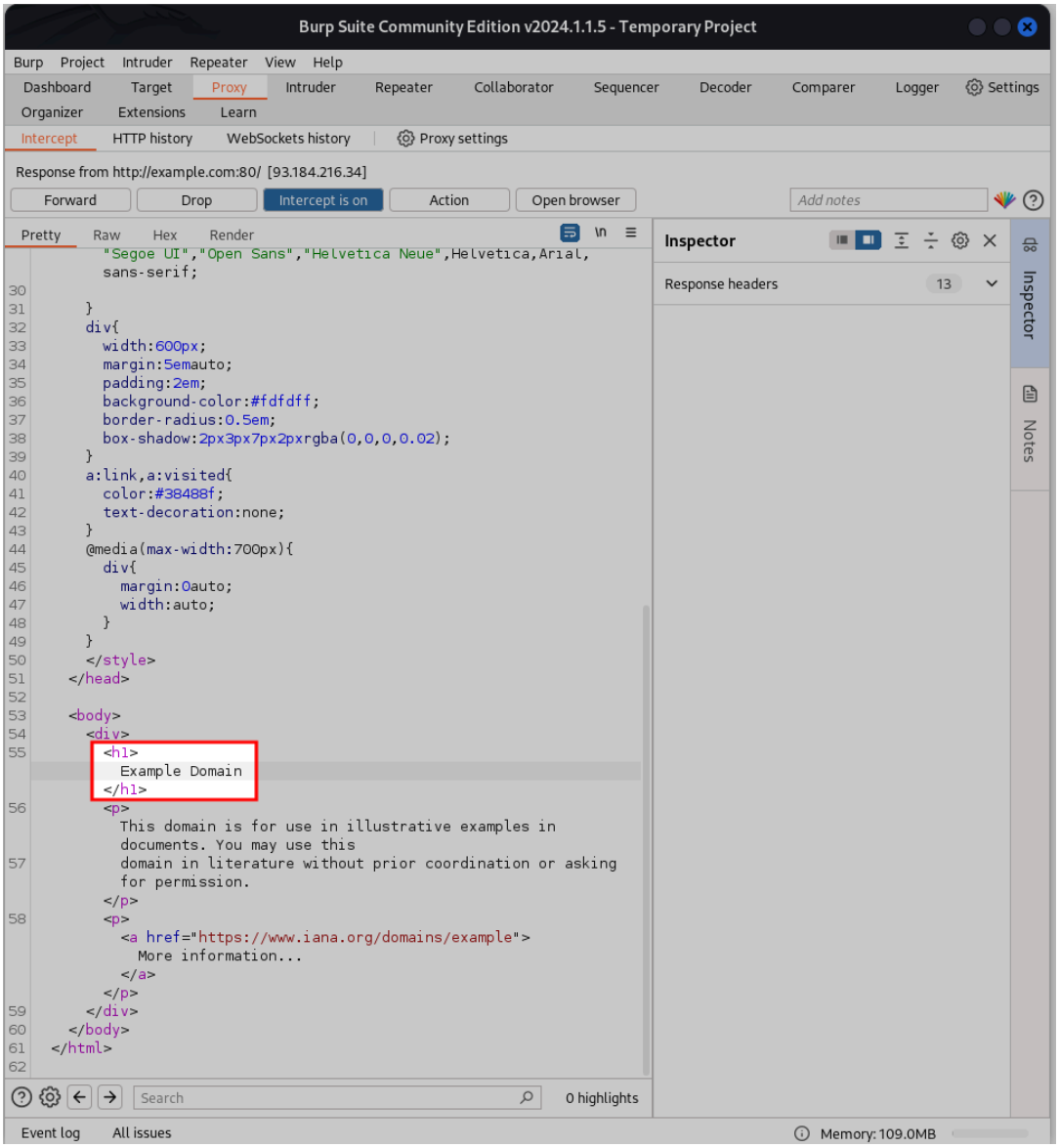
To entertain the response of this request, the attacker has to go to the **Action button -> Do interrupt -> Response to this request**.

Now we can see the response from the server first comes to the proxy as shown in the image below.

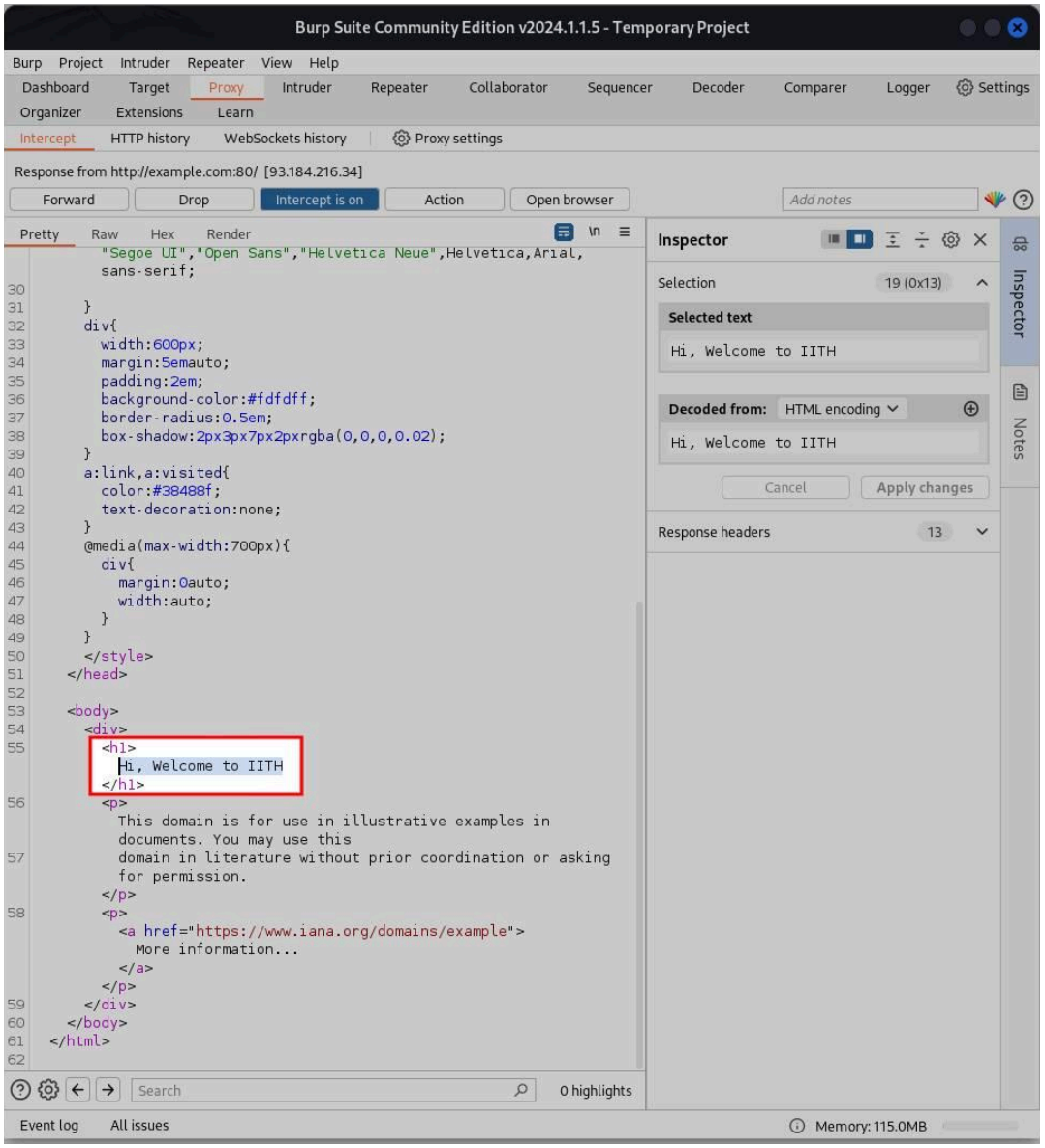


Hands-on Session: Simple Attacks on Wi-Fi Networks

As part of the **active attack**, we are **changing the part of html code Actual string is "Example Domain"** as shown in below image.



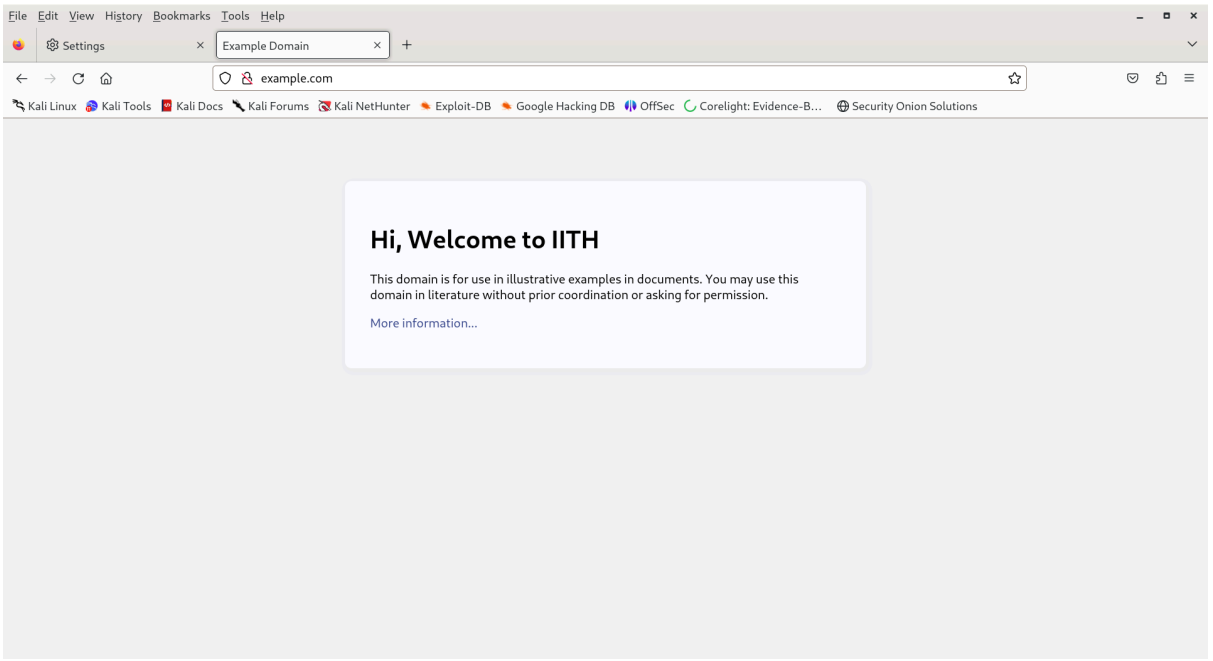
We are **modifying that string to "Hi, Welcome to IITH"**



Now on **pressing the forward button** at the interceptor proxy client receives the modified code.

Hands-on Session: Simple Attacks on Wi-Fi Networks

Client can see our modified website (or attacker's modified content)



Actual site content will look like below.