



Project 1

Problem Statement :-

This is a very simple project with no deliverables. This project is to get familiar with the WLAN protocol and observe the management and data frames exchanges between stations and Aps in an 802.11 WLAN.

Abhishek Verma

1.To perform this exercise, you need to first download the Project1.PCAP file available on this page.

-> Downloaded

2. After the file is downloaded, you will need packet analysis software to open the file. If you do not already have a packet analyzer installed on your computer, you can download Wireshark from www.wireshark.org.

-> Wireshark is already installed

3. Using the packet analyzer, open the downloaded PCAP file. Most packet analyzers display a list of capture frames in the upper section of the screen, with each frame numbered sequentially in the first column.

->That is exactly the case in the capture.

4. Scroll down the list of frames and click frame #8, which is an unencrypted simple data frame. Look at the frame body and notice the upper-layer information, such as IP addresses and TCP ports. Make sure that the IP address you see is 192.168.100.51 and source IP and 192.168.100.52 as destination IP. The source TCP port is 20 and destination port is 1105. Note that this is an unencrypted data frame and even at the upper layer, the protocol is plain ftp with not application layer encryption.

-> Able to validate all the details on the pcap.

No.	Time	Source	Destination	Stream index	Protocol	Length Info
1	0.000000	Cisco_fa:7e:50	Broadcast	802.11		150 Beacon frame, SN=2741, FN=0, Flags=....., BI=100, SSID=airspy
2	0.000005	192.168.100.51	192.168.100.52	0	FTP-DATA	660 FTP Data: 588 bytes
3	0.000009		Cisco_fa:7e:50 (00:13:5f:f...	802.11		10 Acknowledgement, Flags=.....
4	0.000012	192.168.100.52	192.168.100.51	0	TCP	72 1105 → 20 [ACK] Seq=1 Ack=589 Win=17520 Len=0
5	0.000016		AskeyCom_bd:77:35 (00:90:9...	802.11		10 Acknowledgement, Flags=.....
6	0.000071	192.168.100.51	192.168.100.52	0	FTP-DATA	1532 FTP Data: 1460 bytes
7	0.000076		Cisco_fa:7e:50 (00:13:5f:f...	802.11		10 Acknowledgement, Flags=.....
8	0.000290	192.168.100.51	192.168.100.52	0	FTP-DATA	660 FTP Data: 588 bytes

```
> Frame 8: 660 bytes on wire (5280 bits), 660 bytes captured (5280 bits) on 0
> IEEE 802.11 Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.100.51 (192.168.100.51), Dst: 192.168.100.52 (192.168.100.52)
> Transmission Control Protocol, Src Port: 20, Dst Port: 1105, Seq: 2049, Ack: 1, Len: 588
  FTP Data (588 bytes data)
    [Setup frame: 2]
  Line-based text data (1 lines)
    [truncated]e times that try men's souls... These are the times that try men's souls... These are the times that try men's souls... These are the times that try men's souls... These are the times that try men's souls... These are the time
```

5. Click frame #136, which is an encrypted simple data frame. Look at the frame body and notice that WEP encryption is being used and that the upper-layer information cannot be seen. Make sure to note the WEP parameters – Initialization vector (IV) is 0x003a27 and the Integrity Code (ICV) is 0x7305864a. Note the position of these in the frame data.

136 -148.366693	AskeyCom_bd:77:35	GemtekTe_3d:67:3c	802.11	80 Data, SN=2601, FN=0, Flags=p....T
137 -148.366374		AskeyCom_bd:77:35 (00:90:96:bd:77:35)	802.11	10 Acknowledgement, Flags=.....
138 -148.366370	GemtekTe_3d:67:3c	AskeyCom_bd:77:35	802.11	668 Data, SN=3891, FN=0, Flags=p....F.
139 -148.366366		Cisco_fa:7e:50 (00:13:5f:f...	802.11	10 Acknowledgement, Flags=.....
140 -148.366032	GemtekTe_3d:67:3c	AskeyCom_bd:77:35	802.11	1104 Data, SN=3892, FN=0, Flags=p....F.
141 -148.366028		Cisco_fa:7e:50 (00:13:5f:f...	802.11	10 Acknowledgement, Flags=.....
142 -148.365916	AskeyCom_bd:77:35	GemtekTe_3d:67:3c	802.11	80 Data, SN=2602, FN=0, Flags=p....T
143 -148.365407		AskeyCom_bd:77:35 (00:90:96:bd:77:35)	802.11	10 Acknowledgement, Flags=.....
144 -148.365403	GemtekTe_3d:67:3c	AskeyCom_bd:77:35	802.11	1540 Data, SN=3893, FN=0, Flags=p....F.
145 -148.365399		Cisco_fa:7e:50 (00:13:5f:f...	802.11	10 Acknowledgement, Flags=.....
146 -148.365390	GemtekTe_3d:67:3c	AskeyCom_bd:77:35	802.11	668 Data, SN=3894, FN=0, Flags=p....F.

Transmitter address: AskeyCom_bd:77:35 (00:90:96:bd:77:35)	
Destination address: GemtekTe_3d:67:3c (00:1a:79:3d:67:3c)	
Source address: AskeyCom_bd:77:35 (00:90:96:bd:77:35)	
BSS Id: Cisco_fa:7e:50 (00:13:5f:f...	
STA address: AskeyCom_bd:77:35 (00:90:96:bd:77:35)	
.... 0000 = Fragment number: 0	
1010 0010 1001 = Sequence number: 2601	
WEP parameters	
Initialization Vector: 0x003a27	
Key Index: 0	
WEP ICV: 0x7305864a (not verified)	
Data (48 bytes)	
Data: 4d54698b0a76e142440c4f02df6c2448886015942f424867d2b7a855fd76f311e1f561aa...	
[Length: 48]	

6. Scroll down the list of frames and observe the EAP frame exchange from frame #209 to frame #246. Make sure to note that this sequence starts with an 802.1X authentication frame followed by acknowledgement. Note that the source MAC address in #209 is the receiver MAC address is #210. Note that the number of frame exchanges for the entire authentication process. Note that the Administrator is being authenticated. Note after being authenticated, EAP-PEAP over TLS is being requested. You can also see the content of the digital certificate and extract the information on the signing authority.

No.	Time	Source	Destination	Stream index	Protocol	Length	Info
208	-100399727.6..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
209	-100399724.4..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		EAPOL	78	Start
210	-100399724.4..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....
211	-100399724.4..	Cisco-Li_75:14:c1	Aironet_a2:e1:c2		EAP	41	Request, Identity
212	-100399724.4..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
213	-100399724.4..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		EAP	78	Response, Identity
214	-100399724.4..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....
215	-100399724.4..	Cisco-Li_75:14:c1	Aironet_a2:e1:c2		EAP	42	Request, Protected EAP (EAP-PEAP)
216	-100399724.4..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
217	-100399724.4..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		TLSv1	142	Client Hello
218	-100399724.4..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....
219	-100399724.4..	Cisco-Li_75:14:c1	Aironet_a2:e1:c2		EAP	1070	Request, Protected EAP (EAP-PEAP)
220	-100399724.4..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
221	-100399724.4..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		EAP	78	Response, Protected EAP (EAP-PEAP)
222	-100399724.4..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....
223	-100399724.3..	Cisco-Li_75:14:c1	Aironet_a2:e1:c2		TLSv1	416	Server Hello, Certificate, Server Hello Done
224	-100399724.3..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
225	-100399724.3..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		TLSv1	244	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
226	-100399724.3..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....
227	-100399724.3..	Cisco-Li_75:14:c1	Aironet_a2:e1:c2		TLSv1	101	Change Cipher Spec, Encrypted Handshake Message
228	-100399724.3..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
229	-100399724.3..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		EAP	78	Response, Protected EAP (EAP-PEAP)
230	-100399724.3..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....
231	-100399724.3..	Cisco-Li_75:14:c1	Aironet_a2:e1:c2		TLSv1	116	Application Data, Application Data
232	-100399724.3..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
233	-100399724.3..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		TLSv1	116	Application Data, Application Data
234	-100399724.3..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....
235	-100399724.3..	Cisco-Li_75:14:c1	Aironet_a2:e1:c2		TLSv1	148	Application Data, Application Data
236	-100399724.3..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
237	-100399724.3..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		TLSv1	180	Application Data, Application Data
238	-100399724.3..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....
239	-100399724.2..	Cisco-Li_75:14:c1	Aironet_a2:e1:c2		TLSv1	164	Application Data, Application Data
240	-100399724.2..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
241	-100399724.2..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		TLSv1	116	Application Data, Application Data
242	-100399724.2..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....
243	-100399724.2..	Cisco-Li_75:14:c1	Aironet_a2:e1:c2		TLSv1	116	Application Data, Application Data
244	-100399724.2..		Cisco-Li_75:14:c1 (00:0f:6..		802.11	10	Acknowledgement, Flags=.....
245	-100399724.2..	Aironet_a2:e1:c2	Cisco-Li_75:14:c1		TLSv1	116	Application Data, Application Data
246	-100399724.2..		Aironet_a2:e1:c2 (00:40:96..		802.11	10	Acknowledgement, Flags=.....

```

> Logical-Link Control
> 802.1X Authentication
✓ Extensible Authentication Protocol
  Code: Request (1)
  Id: 3
  Length: 380
  Type: Protected EAP (EAP-PEAP) (25)
  > EAP-TLS Flags: 0x00
  > [2 EAP-TLS Fragments (1398 bytes): #219(1024), #223(374)]
  ✓ Transport Layer Security
    > TLSv1 Record Layer: Handshake Protocol: Server Hello
    ✓ TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1305
      ✓ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1301
        Certificates Length: 1298
        > Certificates (1298 bytes)
    > TLSv1 Record Layer: Handshake Protocol: Server Hello Done

```

7. Scroll down the list of frames and observe the 4-Way Handshake from frame #247 to frame #254. Make sure to note all the 4 messages in the 4-way handshake and key exchange. Note that CCMP encryption is being used.

247	-100399724.2.. Cisco-Li_75:14:c1	Aironet_a2:e1:c2	EAPOL	131 Key (Message 1 of 4)
248	-100399724.2..	Cisco-Li_75:14:c1 (00:0f:6...	802.11	10 Acknowledgement, Flags=.....
249	-100399724.2.. Aironet_a2:e1:c2	Cisco-Li_75:14:c1	EAPOL	155 Key (Message 2 of 4)
250	-100399724.2..	Aironet_a2:e1:c2 (00:40:96...	802.11	10 Acknowledgement, Flags=.....
251	-100399724.2.. Cisco-Li_75:14:c1	Aironet_a2:e1:c2	EAPOL	155 Key (Message 3 of 4)
252	-100399724.2..	Cisco-Li_75:14:c1 (00:0f:6...	802.11	10 Acknowledgement, Flags=.....
253	-100399724.2.. Aironet_a2:e1:c2	Cisco-Li_75:14:c1	EAPOL	131 Key (Message 4 of 4)
254	-100399724.2..	Aironet_a2:e1:c2 (00:40:96...	802.11	10 Acknowledgement, Flags=.....
255	-100399724.2.. Cisco-Li_75:14:c1	Aironet_a2:e1:c2	802.11	171 Data, SN=2541, FN=0, Flags=.p....F.
256	-100399724.2..	Cisco-Li_75:14:c1 (00:0f:6...	802.11	10 Acknowledgement, Flags=.....

```

<
> DSAP: SNAP (0xaa)
> SSAP: SNAP (0xaa)
> Control field: U, func=UI (0x03)
  Organization Code: 00:00:00 (Officially Xerox, but
  Type: 802.1X Authentication (0x888e)
✓ 802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: Key (3)
  Length: 119
  Key Descriptor Type: EAPOL WPA Key (254)
  [Message number: 2]
  > Key Information: 0x010a
  Key Length: 16
  Replay Counter: 0
  WPA Key Nonce: 3d80b4ecd7b218c61f58912108d49fb625069860b7ec03b08086f123b0715ddb
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: cd5eaf88971a3b3592f8f3222203482d
  WPA Key Data Length: 24
  > WPA Key Data: dd160050f20101000050f20401000050f20401000050f201

```