

# CSG1105 Workshop Eight

## 1 INTRODUCTION

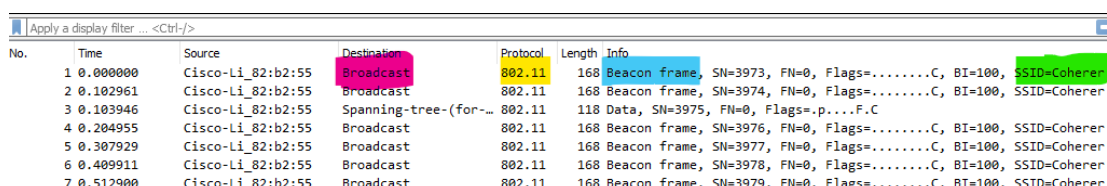
This week we are going to explore some basic aspects of capturing WiFi traffic and looking at encrypted and de-encrypted frames.

## 2 CAPTURING 802.11 IN WIRESHARK

Capturing 802.11 traffic is not as straight forward as capturing 802.3 Ethernet traffic. Many NICs and NIC drivers transform 802.11 frames into pseudo 802.3 frames before delivering them to the OS. This means the contents of 802.11 frames, including the radio headers are unavailable. In order to obtain the 802.11 information, Wireshark needs to use a special setting called **Monitor Mode** which may be set in the "Capture Options". Unfortunately, not all NICs are capable of being used in Monitor Mode. For this exercise, we will use a pre-prepared capture file called **wpa-induction.pcap**. This capture is one available from the Wireshark site at [https://wiki.wireshark.org/SampleCaptures#Sample\\_Captures](https://wiki.wireshark.org/SampleCaptures#Sample_Captures).

### 2.1 Examining a 802.11 Capture

1. Download `wpa-induction.pcap` from Blackboard
2. Load `wpa-induction.pcap` into Wireshark



The image shows a screenshot of the Wireshark packet capture list. The top bar says 'Apply a display filter ... <Ctrl-/>'. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The first seven packets are all 802.11 Beacon frames from Cisco-Li\_82:b2:55 to Broadcast. The first packet (No. 1) is highlighted with a blue background in the 'Info' column, and its details are expanded to show 'Beacon frame, SN=3973, FN=0, Flags=.....C, BI=100, SSID=Coherer'. The 'Destination' column for all packets is highlighted in pink, and the 'Protocol' column is highlighted in yellow.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=3973, FN=0, Flags=.....C, BI=100, SSID=Coherer
2	0.102961	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=3974, FN=0, Flags=.....C, BI=100, SSID=Coherer
3	0.103946	Cisco-Li_82:b2:55	Broadcast	802.11	118	Data, SN=3975, FN=0, Flags=p....F.C
4	0.204955	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=3976, FN=0, Flags=.....C, BI=100, SSID=Coherer
5	0.307929	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=3977, FN=0, Flags=.....C, BI=100, SSID=Coherer
6	0.409911	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=3978, FN=0, Flags=.....C, BI=100, SSID=Coherer
7	0.512900	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=3979, FN=0, Flags=.....C, BI=100, SSID=Coherer

3. Look at frame number 1.
4. Highlighted in yellow is the protocol (802.11)
5. Highlighted in pink is the destination, a broadcast
6. The blue highlight indicates this is a Beacon from form the Access Point (AP) with the **SSID** highlighted in green. Beacon frames are broadcast by AP's every few milliseconds to advertise their availability.
7. The beacon frame contains information about the AP including the address, available speeds and information about the encryption ciphers supported.

```

▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (12 bytes)
    Timestamp: 4761907593
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0411
  ▼ Tagged parameters (104 bytes)
    > Tag: SSID parameter set: Coherer
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 1
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    > Tag: ERP Information
    > Tag: ERP Information
    ▼ Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 24
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
      Pairwise Cipher Suite Count: 2
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) 00:0f:ac (Ieee 802.11) TKIP
        Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
      > RSN Capabilities: 0x0000
    ▼ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 4
      Extended Supported Rates: 6 (0x0c)
      Extended Supported Rates: 9 (0x12)
      Extended Supported Rates: 12 (0x18)
      Extended Supported Rates: 48 (0x60)
    > Tag: Vendor Specific: Broadcom
    ▼ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
      Tag Number: Vendor Specific (221)
      Tag length: 28
      OUI: 00:50:f2 (Microsoft Corp.)
      Vendor Specific OUI Type: 1
      Type: WPA Information Element (0x01)
      WPA Version: 1
      > Multicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
      Unicast Cipher Suite Count: 2
      ▼ Unicast Cipher Suite List 00:50:f2 (Microsoft Corp.) AES (CCM) 00:50:f2 (Microsoft Corp.) TKIP
        > Unicast Cipher Suite: 00:50:f2 (Microsoft Corp.) AES (CCM)
        > Unicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
        Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:50:f2 (Microsoft Corp.) PSK

```

8. Now look at frame 58.
9. This is a **Probe Request** from a station, an Apple device
10. The Yellow highlight shows the Probe Request frame type
11. The Pink highlight shows the four addresses
  - The Receiver address
  - the Destination address
  - the Transmitter address and the
  - the Source address
12. The Green highlight shows the target SSID

```

> Frame 58: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
▼ IEEE 802.11 Probe Request, Flags: .....C
    Type/Subtype: Probe Request (0x0004)
    > Frame Control Field: 0x4000
        .000 0000 0000 0000 = Duration: 0 microseconds
        Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
        Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
        Transmitter address: Apple_82:36:3a (00:0d:93:82:36:3a)
        Source address: Apple_82:36:3a (00:0d:93:82:36:3a)
        BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
        .... .... 0000 = Fragment number: 0
        0000 0000 0001 .... = Sequence number: 1
        Frame check sequence: 0x6d6689f7 [unverified]
        [FCS Status: Unverified]
▼ IEEE 802.11 Wireless Management
    ▼ Tagged parameters (25 bytes)
        ▼ Tag: SSID parameter set: Coherer
            Tag Number: SSID parameter set (0)
            Tag length: 7
            SSID: Coherer
        > Tag: Supported Rates 1, 2, 5.5, 11, 18, 24, 36, 54, [Mbit/sec]
        > Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]

```

13. Now examine frame 72

14. This the Probe Response from the AP

```

> Frame 72: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
▼ IEEE 802.11 Probe Response, Flags: ....R...C
    Type/Subtype: Probe Response (0x0005)
    > Frame Control Field: 0x5008
        .000 0001 0011 1010 = Duration: 314 microseconds
        Receiver address: Apple_82:36:3a (00:0d:93:82:36:3a)
        Destination address: Apple_82:36:3a (00:0d:93:82:36:3a)
        Transmitter address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
        Source address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
        BSS Id: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
        .... .... 0000 = Fragment number: 0
        1111 1100 0100 .... = Sequence number: 4036
        Frame check sequence: 0xe15eb4d3 [unverified]
        [FCS Status: Unverified]
▼ IEEE 802.11 Wireless Management
    ▼ Fixed parameters (12 bytes)
        Timestamp: 4767229254
        Beacon Interval: 0.102400 [Seconds]
        > Capabilities Information: 0x0411
    ▼ Tagged parameters (98 bytes)
        > Tag: SSID parameter set: Coherer
        > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
        > Tag: DS Parameter set: Current Channel: 1
        > Tag: ERP Information
        > Tag: ERP Information
        > Tag: RSN Information
        > Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
        > Tag: Vendor Specific: Broadcom
        > Tag: Vendor Specific: Microsoft Corp.: WPA Information Element

```

15. The previous example had the Receiver and Destination address as a broadcast. In this example, where the AP is communicating with the station, the Receiver and Destination is MAC address of the requesting station and the Transmitter and Source address is the MAC of the AP.
16. Examine Frames 78,80,82 and 84

No.	Time	Source	Destination	Protocol	Length	Info
76	5.530996	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4039, FN=0, Flags=.....C, BI=100, SSID=Coherer
77	5.632985	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4040, FN=0, Flags=.....C, BI=100, SSID=Coherer
78	5.643955	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	58	Authentication, SN=23, FN=0, Flags=.....C
79	5.644038		Apple_82:36:3a (00:...	802.11	38	Acknowledgement, Flags=.....C
80	5.644958	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	66	Authentication, SN=4041, FN=0, Flags=.....C
81	5.645039		Cisco-Li_82:b2:55 (...)	802.11	38	Acknowledgement, Flags=.....C
82	5.645953	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	103	Association Request, SN=24, FN=0, Flags=.....C, SSID=Coherer
83	5.646955		Apple_82:36:3a (00:...	802.11	38	Acknowledgement, Flags=.....C
84	5.647953	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	82	Association Response, SN=4042, FN=0, Flags=.....C

17. These frames are the Authentication Request & Response and the Association Request & Response
18. At this point in time, the Authentication is an "Open System" algorithm
19. Examine frames 87,89,92 and 94
20. These frames are the 802.1X EAPOL (Extensible Authentication Protocol over LAN) in which key information is exchanged to establish the WPA PSK session between the station and the AP
21. This performs a **Four Way Handshake** to establish the session. Details of this are beyond the scope of this unit.
22. **Note:** You will have also seen that each frame (other than broadcasts) has an Acknowledgement frame sent in return
23. Once the Four way handshake has been completed, the connection is established and is encrypted. Without the encryption key, we cannot see the contents of the frames.
24. Open Edit->Preferences->Protocols and locate IEEE802.11
25. Select "Enable decryption" and click "Edit"
26. Click "Key type" and choose "wpa-pwd"
27. Click Key field and enter "Induction" and click OK
28. You should be able now to see the contents of frames that contain packets and TCP streams as we have done in previous Wireshark exercises.
29. View an number of these frames to see that we can see the contents
30. If you reverse the "Enable decryption" these will no longer be visible
31. Examine frame 1050. This is "Disassociate" request which will result in the connection to the AP being terminated

### 3 SUMMARY

In this workshop, we have had a brief introduction to capturing and viewing IEEE802.11 frames. There is much more to the topic, but is beyond the scope of this unit.