

CSCI 4406 Computer Networks Lab2_60L

WiFi Traffic Analysis

Joshua Ludolf

Downloading the PCAP File

Right-click the link below and save the file somewhere you can find it, such as your desktop:

<https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=wpa-Induction.pcap>

Viewing the EAPOL Handshake

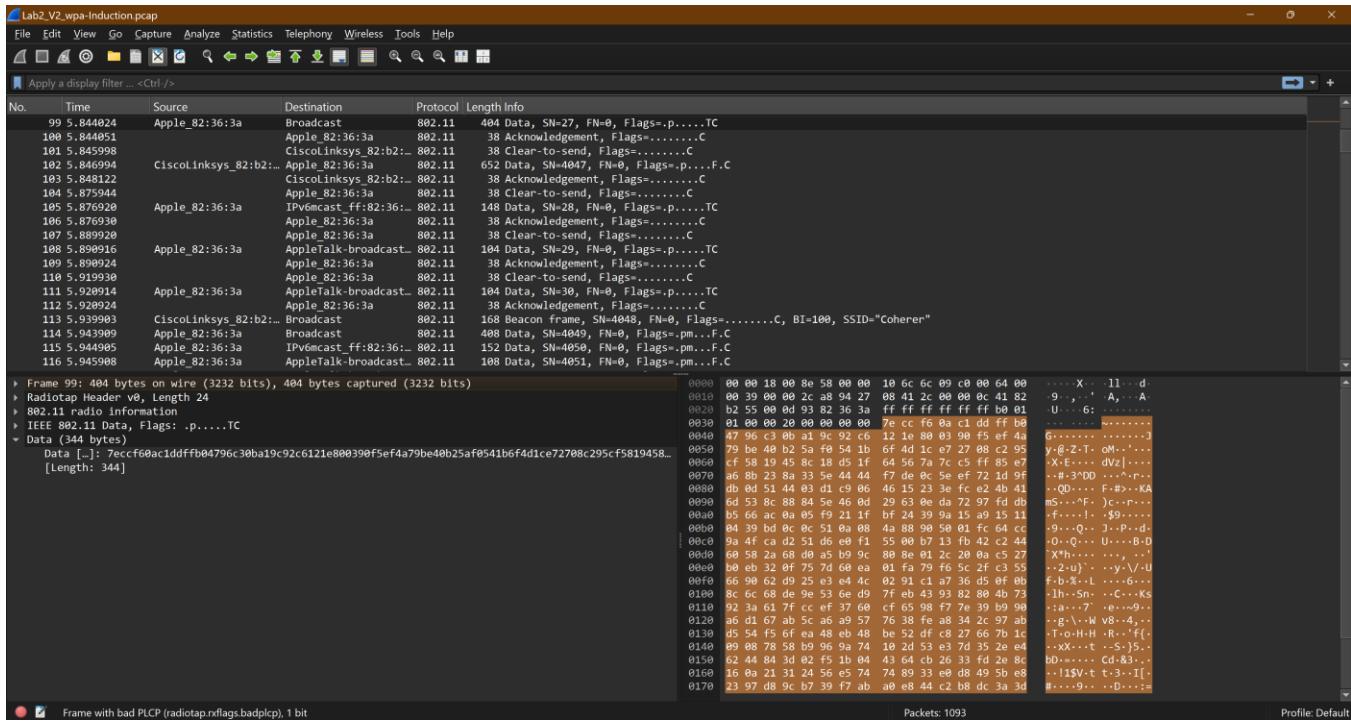
Double-click the **wpa-Induction.pcap** file. It opens in Wireshark.

Scroll down to find the four frames with a Protocol of "EAPOL", as shown below. Here an Apple device is joining a Cisco wireless network, and the four EAPOL packets are used to negotiate a private key for that user.

No.	Time	Source	Destination	Protocol	Length	Info
85	5.647962		Cisco-Li_82:b2:55 (00:0c:41:82:b2:55) (RA)	802.11	38	Acknowledgement, Flags=.....C
86	5.648961		Cisco-Li_82:b2:55 (00:0c:41:82:b2:55) (RA)	802.11	38	Clear-to-send, Flags=.....C
87	5.649953	Cisco-Li_82:b2:55	Apple_82:36:3a	EAPOL	181	Key (Message 1 of 4)
88	5.649964		Cisco-Li_82:b2:55 (00:0c:41:82:b2:55) (RA)	802.11	38	Acknowledgement, Flags=.....C
89	5.650959	Apple_82:36:3a	Cisco-Li_82:b2:55	EAPOL	181	Key (Message 2 of 4)
90	5.650970		Apple_82:36:3a (00:0d:93:82:36:3a) (RA)	802.11	38	Acknowledgement, Flags=.....C
91	5.654947		Cisco-Li_82:b2:55 (00:0c:41:82:b2:55) (RA)	802.11	38	Clear-to-send, Flags=.....C
92	5.655957	Cisco-Li_82:b2:55	Apple_82:36:3a	EAPOL	239	Key (Message 3 of 4)
93	5.655968		Cisco-Li_82:b2:55 (00:0c:41:82:b2:55) (RA)	802.11	38	Acknowledgement, Flags=.....C
94	5.655973	Apple_82:36:3a	Cisco-Li_82:b2:55	EAPOL	159	Key (Message 4 of 4)
95	5.656951		Apple_82:36:3a (00:0d:93:82:36:3a) (RA)	802.11	38	Acknowledgement, Flags=.....C

Viewing Encrypted Traffic

Scroll down to frame 99. Wireshark is unable to decrypt the contents of this frame--all it can say is that it contains "Data", as shown below.



No.	Time	Source	Destination	Protocol	Length	Info
85	5...		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
86	5...		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
87	5...	Cisco-Li_82:b2:55	Apple_82:36...	EAPOL	181	Key (Message 1 of 4)
88	5...		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
89	5...	Apple_82:36:3a	Cisco-Li_82...	EAPOL	181	Key (Message 2 of 4)
90	5...		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
91	5...		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
92	5...	Cisco-Li_82:b2:55	Apple_82:36...	EAPOL	239	Key (Message 3 of 4)
93	5...		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
94	5...	Apple_82:36:3a	Cisco-Li_82...	EAPOL	159	Key (Message 4 of 4)
95	5...		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
96	5...	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4045, FN=0, Flags=...
97	5...	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4046, FN=0, Flags=...
98	5...		Apple_82:36...	802.11	38	Clear-to-send, Flags=.....C
99	5...	Apple_82:36:3a	Broadcast	802.11	404	Data, SN=27, FN=0, Flags=.p.....TC
100	5...		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
101	5...		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C

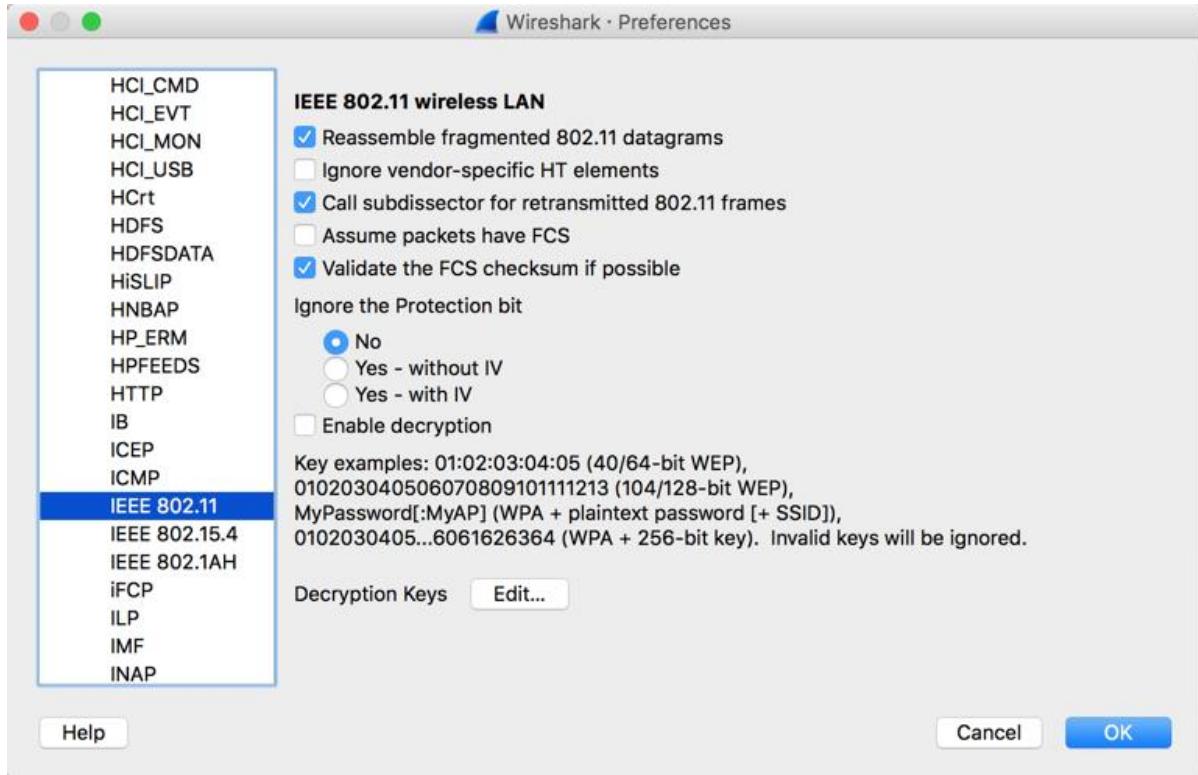
► Frame 99: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits)
 ► Radiotap Header v0, Length 24
 ► 802.11 radio information
 ► IEEE 802.11 Data, Flags: .p.....TC
 ▼ Data (344 bytes)
 Data: 7eccf60ac1ddfffb04796c30ba19c92c6121e800390f5ef4a...
 [Length: 344]

Entering the WPA Key

The precise steps vary, depending on which version of Wireshark you are using.

For Wireshark 2.0.0 on Mac OS X:

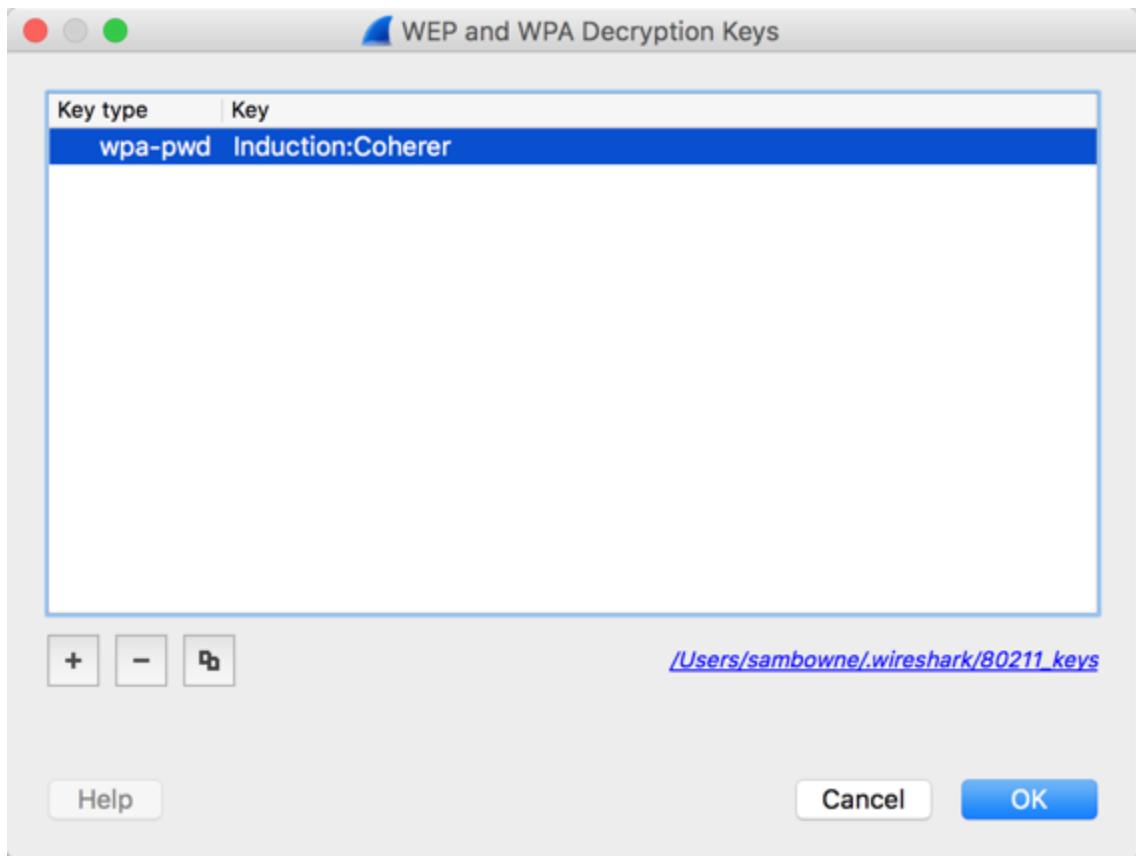
From the menu bar, click **Wireshark**, **Preferences**. In the left pane, expand **Protocols**. Scroll down and click "**IEEE 802.11**", as shown below.



In the "Decryption Keys" line, click the **Edit...** button.

Enter a key of type **wpa-pwd**, with the value **Induction:Coherer**, as shown below.

The key is "Induction" and the SSID of the network is "Coherer".



In the "WEP and WPA Decryption Keys" box, click the **OK** button.

In the "Wireshark Preferences" box, check the "**Enable decryption**" box. Click the **OK** button.

Frame 99 is now decrypted, revealing that it contains a **DHCP** packet, as shown below.

No.	Time	Source	Destination	Protocol	Length	Info
86	5...	Cisco-Li_82:...	Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
87	5...	Cisco-Li_82:...	Apple_82:36...	EAPOL	181	Key (Message 1 of 4)
88	5...		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
89	5...	Apple_82:36:...	Cisco-Li_82...	EAPOL	181	Key (Message 2 of 4)
90	5...		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
91	5...		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
92	5...	Cisco-Li_82:...	Apple_82:36...	EAPOL	239	Key (Message 3 of 4)
93	5...		Cisco-Li_82...	802.11	38	Acknowledgement, Flags=.....C
94	5...	Apple_82:36:...	Cisco-Li_82...	EAPOL	159	Key (Message 4 of 4)
95	5...		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
96	5...	Cisco-Li_82:...	Broadcast	802.11	168	Beacon frame, SN=4045, FN=0, Flags=.....C,
97	5...	Cisco-Li_82:...	Broadcast	802.11	168	Beacon frame, SN=4046, FN=0, Flags=.....C,
98	5...		Apple_82:36...	802.11	38	Clear-to-send, Flags=.....C
99	5...	0.0.0.0	255.255.255...	DHCP	404	DHCP Request - Transaction ID 0x3b0f7566
100	5...		Apple_82:36...	802.11	38	Acknowledgement, Flags=.....C
101	5...		Cisco-Li_82...	802.11	38	Clear-to-send, Flags=.....C
102	5...	192.168.0.1	192.168.0.50	DHCP	652	DHCP ACK - Transaction ID 0x3b0f7566



Saving the Screen Image

Make sure you can see the frame number of **99** and the Protocol of **DHCP**, as shown above.

The Wireshark interface displays the following details:

- File**: Lab2_V2_wpa-induction.pcap
- Edit**: None
- View**: None
- Capture**: mon0
- Analyze**: None
- Statistics**: None
- Telephone**: None
- Wireless**: None
- Tools**: None
- Help**: None

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
99	0.0.0.0			DHCP	404	DHCP Request - Transaction ID 0xb3b0f7566
100	0.0.0.0			DHCP	802.11	38 Acknowledgment, Flags=.....C
101	5.84598	CiscoLinksys_82:b2:..		DHCP	802.11	38 Clear-to-send, Flags=.....C
102	5.84694	192.168.0.1		DHCP	652	DHCP ACK - Transaction ID 0xb3b0f7566
103	5.848122	CiscoLinksys_82:b2:..		DHCP	802.11	38 Acknowledgment, Flags=.....C
104	5.847544	Apple_82:36:3a		DHCP	802.11	38 Clear-to-send, Flags=.....C
105	5.876928	fe80::20d:93ff:fe80::1	ff02::1:ff82:363a	TCPv6	148	Multicast Listener Report
106	5.876938	Apple_82:36:3a		DHCP	802.11	38 Acknowledgment, Flags=.....C
107	5.889920	Apple_82:36:3a		DHCP	802.11	38 Clear-to-send, Flags=.....C
108	5.890916	Apple_82:36:3a	AppleTalk:broadcast	AARP	104	Is there a 65496.228
109	5.890924	Apple_82:36:3a	Apple_82:36:3a	DHCP	802.11	38 Acknowledgment, Flags=.....C
110	5.919930	Apple_82:36:3a		DHCP	802.11	38 Clear-to-send, Flags=.....C
111	5.920914	Apple_82:36:3a	AppleTalk:broadcast	AARP	104	Is there a 65496.228
112	5.920924	Apple_82:36:3a		DHCP	802.11	38 Acknowledgment, Flags=.....C
113	5.939993	CiscoLinksys_82:b2:..	Broadcast	DHCP	802.11	168 Beacon frame, SN=4048, FN=0, Flags=.....C, BI=100, SSID="Coherer"
114	5.943989	Apple_82:36:3a	Broadcast	DHCP	802.11	408 Data, SN=4649, FN=0, Flags=.....C
115	5.944985	Apple_82:36:3a	IPV6multicast:ff:82:36:3a	DHCP	802.11	152 Data, SN=4650, FN=0, Flags=.....C

Frame 99: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits)

Frame details:

- Radiotap Header V0, Length 24
- 802.11 radio information
- IEEE 882.11 Data, Flags: .p....TC
- Logical-Link Control
- Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Request)
- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0xb3b0f7566
- Seconds elapsed: 0
- Boot flag: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 0.0.0.0
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: Apple_82:36:3a (00:0d:93:82:36:3a)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given

Frame 404 (bytes) Decrypted CCMP data (336 bytes)

Packets: 1093

Profile: Default

Things that I learned from this lab:

Wireshark is an application that can be used to decrypt a protocol and learned about “Packet Sniffing” which is to analyze network traffic. Wi-Fi Protected Access (WPA) is a security standard for wireless networks that uses encryption and authentication to safeguard data. Wired Equivalent Privacy (WEP) is meant to protect Wi-Fi transmissions by encrypting it from outsiders who are not inside the encrypted network.