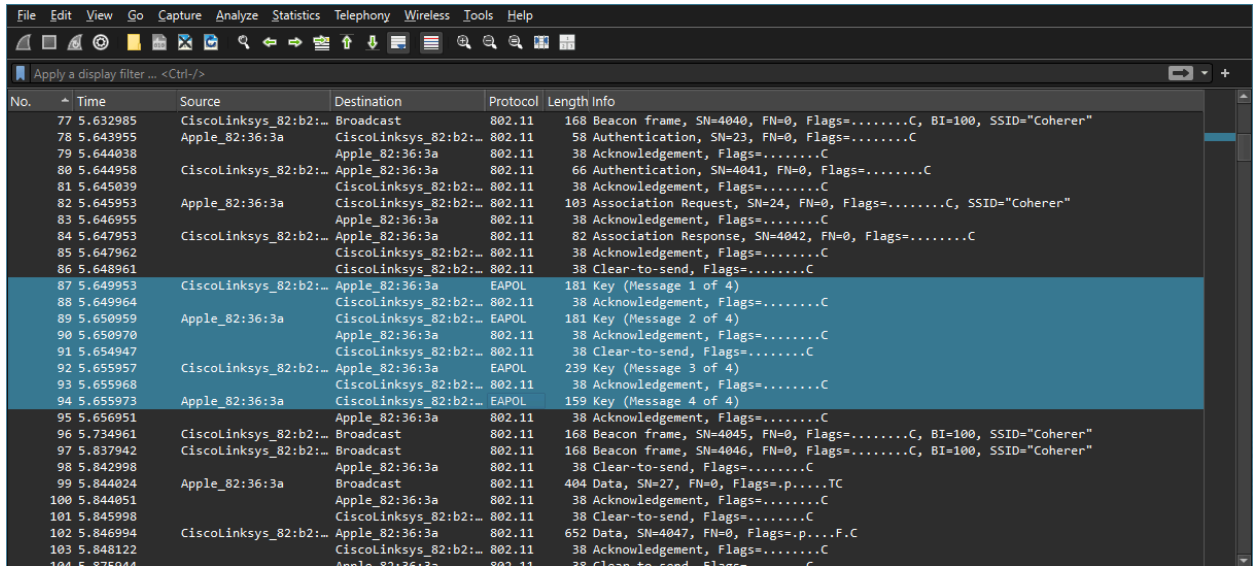


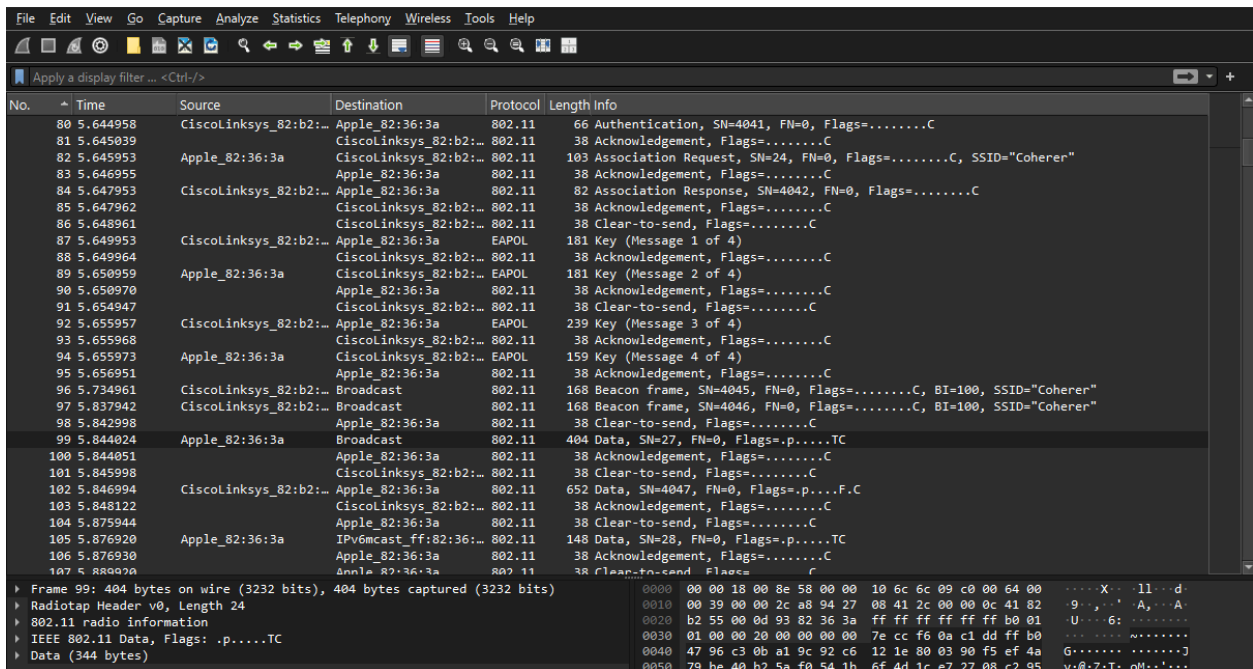
## Viewing the EAPOL Handshake protocol in Wireshark.



The screenshot shows a Wireshark packet capture of an EAPOL handshake. The packet list on the left shows packets 77 through 104. The selected packet 99 is highlighted in blue. The packet details pane on the right shows the structure of the EAPOL Key (Message 1 of 4) packet, including the Key (Message 1 of 4) field.

No.	Time	Source	Destination	Protocol	Length	Info
77	5.632985	CiscoLinksys_82:b2:1	Broadcast	802.11	168	Beacon frame, SN=4040, FN=0, Flags=.....C, BI=100, SSID="Coherer"
78	5.643955	Apple_82:36:3a	CiscoLinksys_82:b2:1	802.11	58	Authentication, SN=23, FN=0, Flags=.....C
79	5.644038		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
80	5.644958	CiscoLinksys_82:b2:1	Apple_82:36:3a	802.11	66	Authentication, SN=4041, FN=0, Flags=.....C
81	5.645039		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
82	5.645953	Apple_82:36:3a	CiscoLinksys_82:b2:1	802.11	103	Association Request, SN=24, FN=0, Flags=.....C, SSID="Coherer"
83	5.646955		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
84	5.647953	CiscoLinksys_82:b2:1	Apple_82:36:3a	802.11	82	Association Response, SN=4042, FN=0, Flags=.....C
85	5.647962		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
86	5.648961		CiscoLinksys_82:b2:1	802.11	38	Clear-to-send, Flags=.....C
87	5.649953	CiscoLinksys_82:b2:1	Apple_82:36:3a	EAPOL	181	Key (Message 1 of 4)
88	5.649964		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
89	5.650959	Apple_82:36:3a	CiscoLinksys_82:b2:1	EAPOL	181	Key (Message 2 of 4)
90	5.650970		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
91	5.654947		CiscoLinksys_82:b2:1	802.11	38	Clear-to-send, Flags=.....C
92	5.655957	CiscoLinksys_82:b2:1	Apple_82:36:3a	EAPOL	239	Key (Message 3 of 4)
93	5.655968		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
94	5.655973	Apple_82:36:3a	CiscoLinksys_82:b2:1	EAPOL	159	Key (Message 4 of 4)
95	5.656951		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
96	5.734961	CiscoLinksys_82:b2:1	Broadcast	802.11	168	Beacon frame, SN=4045, FN=0, Flags=.....C, BI=100, SSID="Coherer"
97	5.837942	CiscoLinksys_82:b2:1	Broadcast	802.11	168	Beacon frame, SN=4046, FN=0, Flags=.....C, BI=100, SSID="Coherer"
98	5.842998		Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
99	5.844024	Apple_82:36:3a	Broadcast	802.11	404	Data, SN=27, FN=0, Flags=p....TC
100	5.844051		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
101	5.845998		CiscoLinksys_82:b2:1	802.11	38	Clear-to-send, Flags=.....C
102	5.846994	CiscoLinksys_82:b2:1	Apple_82:36:3a	802.11	652	Data, SN=4047, FN=0, Flags=p....F.C
103	5.848122		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
104	5.875944		Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C

## Viewing No. 99 Data.



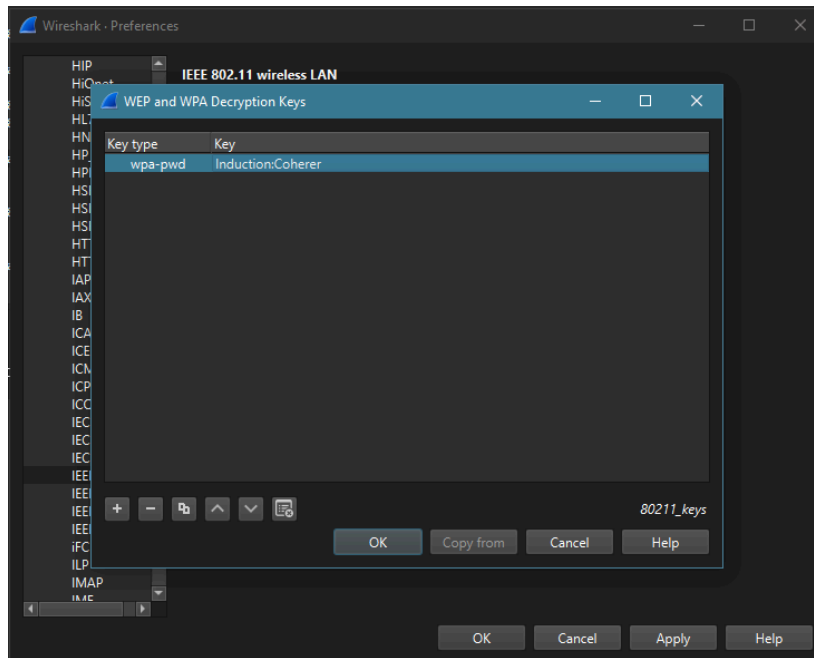
The screenshot shows the packet details pane for packet 99. The pane is expanded to show the IEEE 802.11 Data field, which has a length of 344 bytes. The raw bytes of the data field are displayed in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
80	5.644958	CiscoLinksys_82:b2:1	Apple_82:36:3a	802.11	66	Authentication, SN=4041, FN=0, Flags=.....C
81	5.645039		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
82	5.645953	Apple_82:36:3a	CiscoLinksys_82:b2:1	802.11	103	Association Request, SN=24, FN=0, Flags=.....C, SSID="Coherer"
83	5.646955		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
84	5.647953	CiscoLinksys_82:b2:1	Apple_82:36:3a	802.11	82	Association Response, SN=4042, FN=0, Flags=.....C
85	5.647962		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
86	5.648961		CiscoLinksys_82:b2:1	802.11	38	Clear-to-send, Flags=.....C
87	5.649953	CiscoLinksys_82:b2:1	Apple_82:36:3a	EAPOL	181	Key (Message 1 of 4)
88	5.649964		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
89	5.650959	Apple_82:36:3a	CiscoLinksys_82:b2:1	EAPOL	181	Key (Message 2 of 4)
90	5.650970		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
91	5.654947		CiscoLinksys_82:b2:1	802.11	38	Clear-to-send, Flags=.....C
92	5.655957	CiscoLinksys_82:b2:1	Apple_82:36:3a	EAPOL	239	Key (Message 3 of 4)
93	5.655968		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
94	5.655973	Apple_82:36:3a	CiscoLinksys_82:b2:1	EAPOL	159	Key (Message 4 of 4)
95	5.656951		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
96	5.734961	CiscoLinksys_82:b2:1	Broadcast	802.11	168	Beacon frame, SN=4045, FN=0, Flags=.....C, BI=100, SSID="Coherer"
97	5.837942	CiscoLinksys_82:b2:1	Broadcast	802.11	168	Beacon frame, SN=4046, FN=0, Flags=.....C, BI=100, SSID="Coherer"
98	5.842998		Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
99	5.844024	Apple_82:36:3a	Broadcast	802.11	404	Data, SN=27, FN=0, Flags=p....TC
100	5.844051		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
101	5.845998		CiscoLinksys_82:b2:1	802.11	38	Clear-to-send, Flags=.....C
102	5.846994	CiscoLinksys_82:b2:1	Apple_82:36:3a	802.11	652	Data, SN=4047, FN=0, Flags=p....F.C
103	5.848122		CiscoLinksys_82:b2:1	802.11	38	Acknowledgement, Flags=.....C
104	5.875944		Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
105	5.876920	Apple_82:36:3a	IPv6mcast::ff:82:36:1	802.11	148	Data, SN=28, FN=0, Flags=p....TC
106	5.876930		Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
107	5.880020		Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C

Frame 99: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits) on interface 0  
Radiotap Header v0, Length 24  
802.11 radio Information  
IEEE 802.11 Data, Flags: p....TC  
Data (344 bytes)

0000 00 00 18 00 8e 58 00 00 10 6c 6c 00 c0 00 64 00 ...X...ll...d  
0010 00 39 00 00 2c a8 94 27 08 41 2c 00 00 c1 82 ...9...A...A  
0020 b2 55 00 0d 93 82 36 3a ff ff ff ff ff b0 01 ...U...6: .....  
0030 01 00 00 20 00 00 00 00 7e cc f6 0a c1 dd ff b0 .....  
0040 47 96 c3 0b a1 9c 92 c6 12 1e 80 03 90 f5 ef 4a G.....J  
0050 79 be 40 b2 5a f0 54 1b 6f 4d 1c e7 27 08 c2 95 v@ZT: oM'....

## Entering the WPA Key and Decrypting



Frame 99 is decrypted and contains a DHCP packet

The image shows a Wireshark packet capture. The packet list on the left shows frame 99 selected, which is a DHCP Request (Transaction ID 0x3b0f7566) from 0.0.0.0 to 255.255.255.255. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Dynamic Host Configuration Protocol (Request). The packet bytes pane at the bottom shows the raw data of the packet, including the DHCP request structure.

No.	Time	Source	Destination	Protocol	Length	Info
86	5.648961		CiscoLinksys_82:b2:...	802.11	38	Clear-to-send, Flags=.....C
87	5.649953	CiscoLinksys_82:b2:...	Apple_82:36:3a	EAPOL	181	Key (Message 1 of 4)
88	5.649964	CiscoLinksys_82:b2:...	CiscoLinksys_82:b2:...	802.11	38	Acknowledgement, Flags=.....C
89	5.650959	Apple_82:36:3a	CiscoLinksys_82:b2:...	EAPOL	181	Key (Message 2 of 4)
90	5.650970	Apple_82:36:3a	CiscoLinksys_82:b2:...	802.11	38	Acknowledgement, Flags=.....C
91	5.654947	CiscoLinksys_82:b2:...	CiscoLinksys_82:b2:...	802.11	38	Clear-to-send, Flags=.....C
92	5.655957	Apple_82:36:3a	CiscoLinksys_82:b2:...	EAPOL	239	Key (Message 3 of 4)
93	5.655968	CiscoLinksys_82:b2:...	CiscoLinksys_82:b2:...	802.11	38	Acknowledgement, Flags=.....C
94	5.655973	Apple_82:36:3a	CiscoLinksys_82:b2:...	EAPOL	159	Key (Message 4 of 4)
95	5.656951	Apple_82:36:3a	CiscoLinksys_82:b2:...	802.11	38	Acknowledgement, Flags=.....C
96	5.734961	CiscoLinksys_82:b2:...	Broadcast	802.11	168	Beacon frame, SN=4045, FN=0, Flags=.....C, BI=100, SSID="Coherer"
97	5.837942	CiscoLinksys_82:b2:...	Broadcast	802.11	168	Beacon frame, SN=4046, FN=0, Flags=.....C, BI=100, SSID="Coherer"
98	5.842998	Apple_82:36:3a	CiscoLinksys_82:b2:...	802.11	38	Clear-to-send, Flags=.....C
99	5.844024	0.0.0.0	255.255.255.255	DHCP	404	DHCP Request - Transaction ID 0x3b0f7566
100	5.844051	Apple_82:36:3a	CiscoLinksys_82:b2:...	802.11	38	Acknowledgement, Flags=.....C
101	5.845998	CiscoLinksys_82:b2:...	Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
102	5.846994	192.168.0.1	192.168.0.50	DHCP	652	DHCP ACK - Transaction ID 0x3b0f7566
103	5.848122	CiscoLinksys_82:b2:...	Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
104	5.875944	Apple_82:36:3a	CiscoLinksys_82:b2:...	802.11	38	Clear-to-send, Flags=.....C
105	5.876920	fe80::20d:93ff:fe82...	ff02::1:ff82:363a	ICMPv6	148	Multicast Listener Report
106	5.876930	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
107	5.889920	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
108	5.890916	AppleTalk-broadcast...	AppleTalk-broadcast...	AARP	104	Is there a 65496.228
109	5.890924	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C
110	5.919930	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Clear-to-send, Flags=.....C
111	5.920914	AppleTalk-broadcast...	AppleTalk-broadcast...	AARP	104	Is there a 65496.228
112	5.920924	Apple_82:36:3a	Apple_82:36:3a	802.11	38	Acknowledgement, Flags=.....C

Frame 99: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits) on interface 0  
RadioTap Header v0, Length 24  
802.11 radio information  
IEEE 802.11 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)

I learned how to decrypt encrypted network traffic using Wireshark. I did this by editing the decryption keys in the IEEE 802.11 wireless LAN to view DHCP protocols. This allowed me to view the raw data in frame 99.