13.9.1 成功的 WEP 认证

80211-WEPauth.pcap 文件包含了成功连接 WEP 无线网络的例子。这个网络使用 WEP 安全机制。你必须向 WAP 提供一个密码，以通过认证并解密它发来的数据。你可以把 WEP 密码当成无线网络密码。

如图 13-11 所示，这个捕获文件以数据包 4 所示的从 WAP（00:11:88:6b:68:30）发送到无线客户端（00:14:a5:30:b0:af）的质询开始❶。这个质询的目的是确认无线客户端是否有正确的 WEP 密码。展开 802.11 头部和 tagged parameters，你可以看到这个质询。

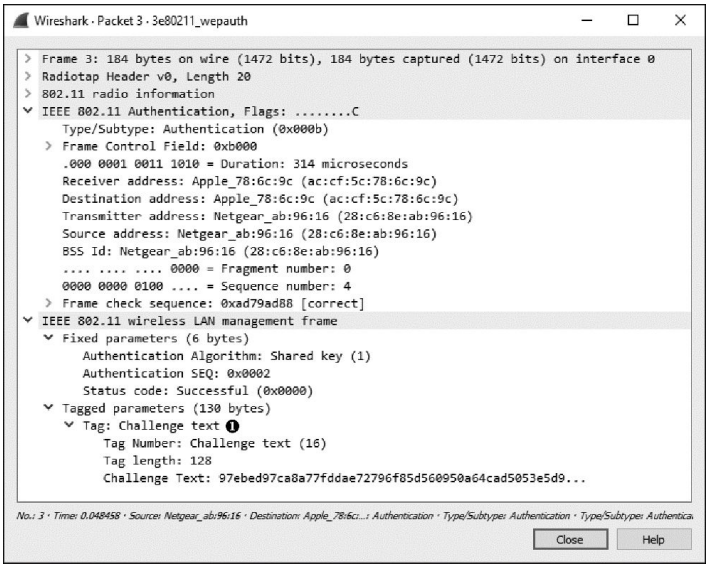


图 13-11　WAP 给无线客户端发送质询文本

在数据包 5 中，这个质询被确认。然后无线客户端将用 WEP 密码解密的质询文本返回给 WAP❶，如图 13-12 所示。

在数据包 7 中，这个数据包被再次确认，并且 WAP 在数据包 8 中响应了无线客户端，如图 13-13 所示。响应里包含了一个说明认证成功的通知❶。

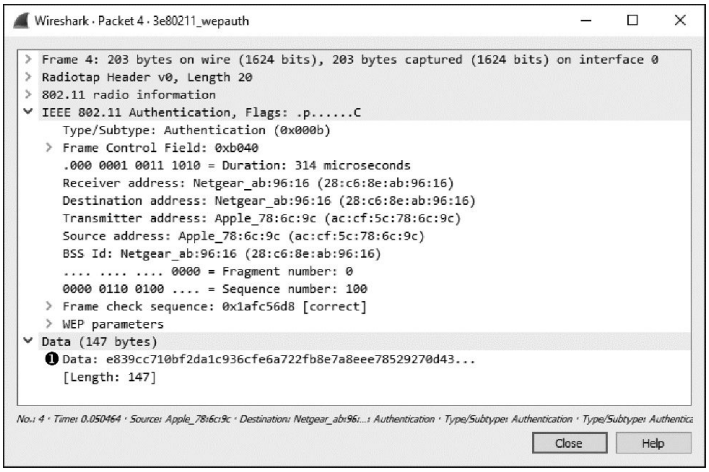


图 13-12　无线客户端向 WAP 发送已解密的质询文本

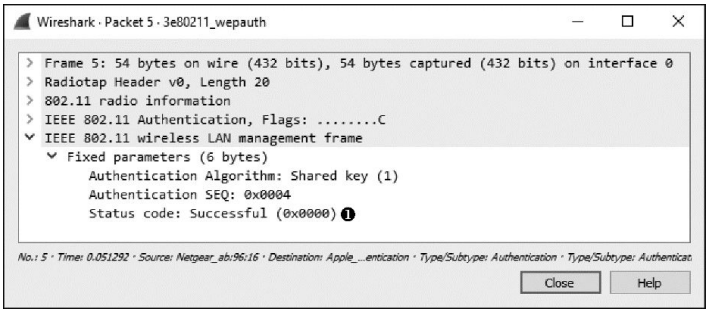
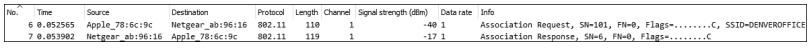


图 13-13　WAP 通知客户端认证成功了

成功认证后，客户端可以发送关联（association）请求、接收确认并完成连接过程，如图 13-14 所示。



No.	Time	Source	Destination	Protocol	Length	Channel	Signal strength (dBm)	Data rate	Info
6	0.052565	Apple_78:6c:9c	Netgear_ab:96:16	802.11	110	1	-40	1	Association Request, SN=101, FN=0, Flags=........C, SSID=DENVEROFFICE
7	0.053902	Netgear_ab:96:16	Apple_78:6c:9c	802.11	119	1	-17	1	Association Response, SN=6, FN=0, Flags=........C

图 13-14　认证过程后紧跟一个简单的双数据包关联请求和响应