电子科技大学信息与软件工程学院

**实 验 报 告**

学 号 2021090912006

姓 名 杨俊贤

（实验） 课程名称 网络攻防技术

理论教师 罗绪成

实验教师 罗绪成

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：杨俊贤 学号：2021090912006 指导教师：罗绪成**

**实验地点：信软楼西305 实验时间：2023.11.17**

**一、实验名称：**WPA-PSK 口令破解实验

**二、实验学时：**4学时

**三、实验目的：**

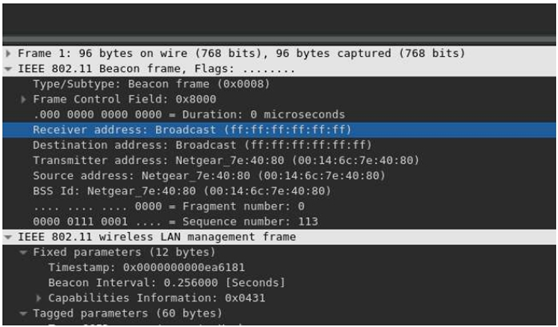
1） 理解 WLAN 的工作原理

2） 理解 RSN 的密钥层次

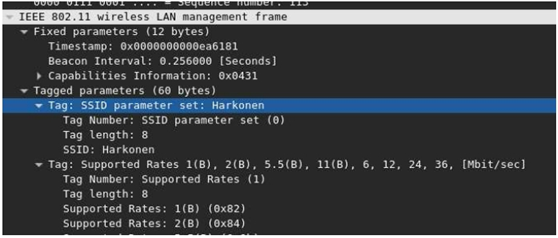
3） 掌握 4 次握手原理

**四、实验原理：**

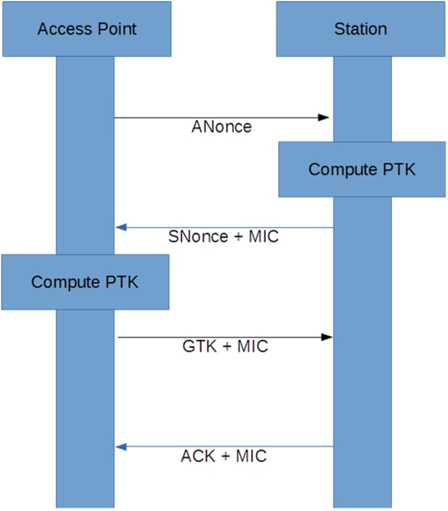
本实验主要用到 4-way 握手的原理。在 4-way 握手之前，STA 应该收到 AP 广播的 beacon 帧。AP 通过广播 beacon 帧来表示其无线网络的存在。如下图所示：



通过 beacon 帧，我们能够找到 SSID，如下图：

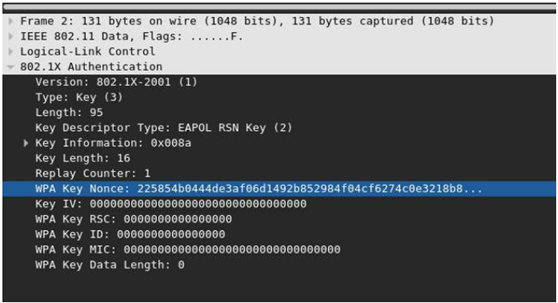


接下来是 4-way 握手过程，大致流程为：

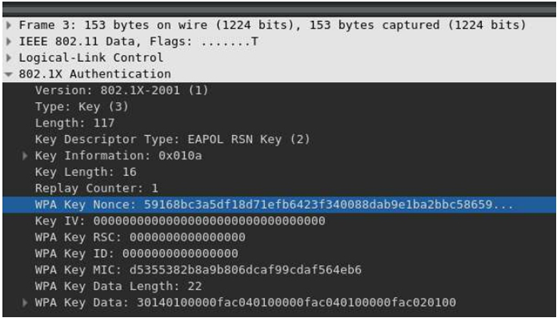


MSG-1

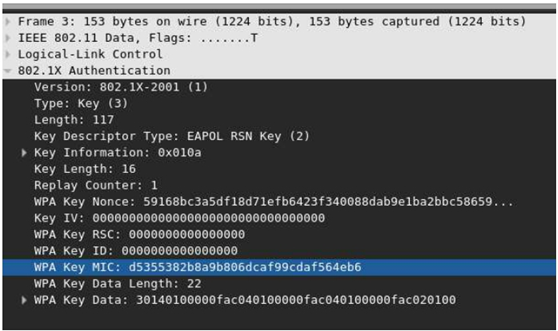
4-way 握手的第一条消息如下所示：



其中传递的关键信息就是 AP 生成 Nonce，称为 ANonce，长度为 256 比特。ANonce 作为产生 PTK 的输入之一。 MSG-2 STA 接收到第一个握手包后，就获得了 ANonce。STA 也生成一个 Nonce，称为 SNonce。通过设置无线网络时的配置，STA 和 AP 已经知道共同的 PMK，因此具备了 生成 PTK 的所需输入。则 STA 生成 PTK。生成 PTK 后，STA 发送第二个握手包给 AP， 其中包含两个重要的信息。其一是 STA 生成的 256 比特 SNonce；其二是 128 比特 MIC。 AP 需要 SNonce 来生成 PTK。ANonce 和 SNonce 用于防止重放攻击。SNonce 如下图：



MIC 用于验证 STA 知道 PTK，进而需要知道 PMK，从而验证了 STA 是合法的。 MIC 字段如下图所示。



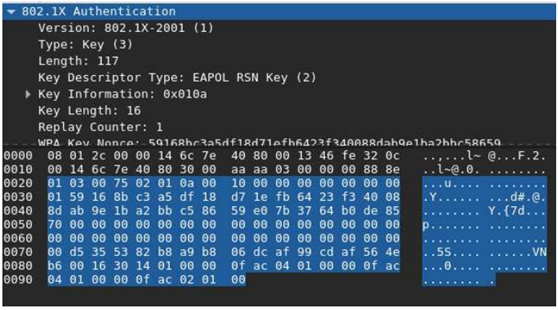
MIC 的计算方法为：

输入：802.1x 的所有字段，包括 MIC 字段，只是在计算的时候该字段设置为全 0。

对 WPA 来说，计算函数是 HMAC-MD5

对 WPA2 来说，计算函数是 HMAC-SHA1

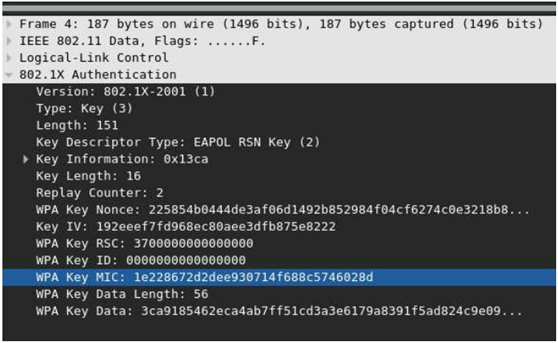
下图显示了 802.1x 的所有字段值。



要通过验证，也就是 STA 和 AP 计算出来的 MIC 相同，STA 必须有正确的 PTK， 进而正确的 PMK，因为计算的 PTK 的输入之一为 PMK。如果通过验证，则证明 STA 具有合法的 PMK，但是 PMK 没有在网上上传输，确保了 PTK 的保密性。第三方即使 观察到了这些流量，也无法推断出 PTK 或者 PMK。上述过程完成了 AP 对 STA 的认证。

MSG-3

在第三个握手包中，传输的重要信息包括 MIC 字段和 WPA key data 字段。通过 MIC 字段，AP 可以向 STA 认证自己。如果通过验证，这表明 AP 知道 PTK，进而知道 PMK。 这里计算 MIC 的方法和前面相同。如下图所示：



第三个握手包中也包含了 GTK，用于加解密 AP 和所有 STA 之间的广播数据，GTK 以密文形式包含在 WPA key data 字段。

MSG-4:

STA 发送第四个握手包，用于向 AP 确认它收到了正确的密钥，加密通信即将开始。 第四个握手包也包含 MIC 字段，计算方法同前。

通过上面的原理，我们就可以通过穷举法来找到正确的 PSK。实际攻击中，我们会 从字典中选择 PASSPHRASE，然后计算 PMK，然后 PTK，然后 MIC，直至找到的 PASSPHRASE 所计算出的 MIC 和握手包里面的 MIC 匹配，从而找到了正确的 PASSPHRASE。这种攻击称为离线字典攻击，其成功的关键在于用户使用了弱口令。

**五、实验内容：**

1） 配置无线网络攻击环境；

2） 抓取无线网络握手包；

3） 编写程序破解 WPA-PSK 的口令。

**六、实验器材（设备、元器件）：**

1） 一台PC电脑，Windows系统，配置有Kali Linux虚拟机。

**七、实验步骤：**

步骤一、环境搭建 配置无线网络抓包环境。

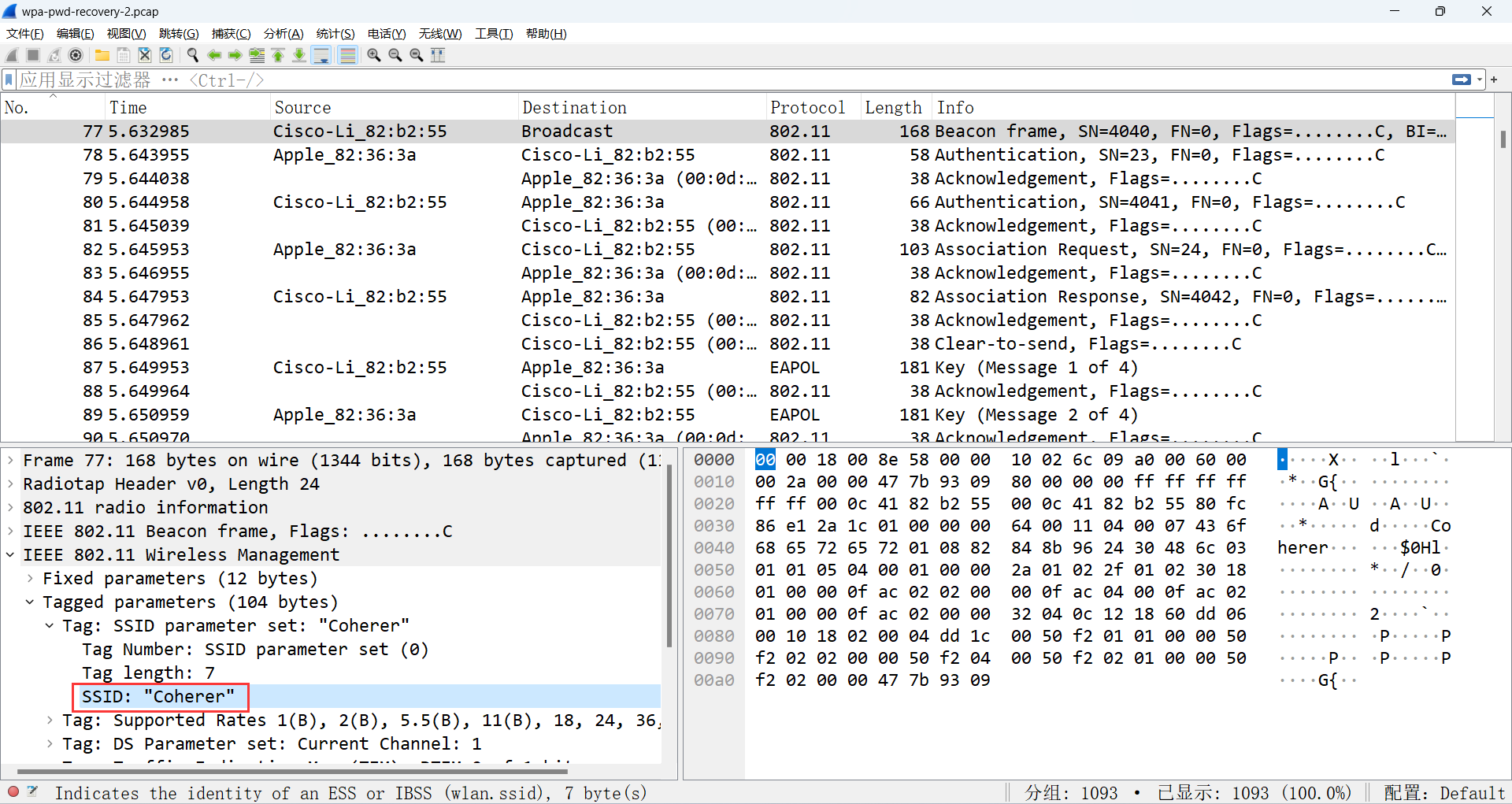
步骤二、抓取无线网络握手包 测试简单无线网络攻击如 deauth 等，抓取 WPA-PSK 握手包

步骤三、编写程序破解 WPA-PSK 的口令

步骤四、验证口令

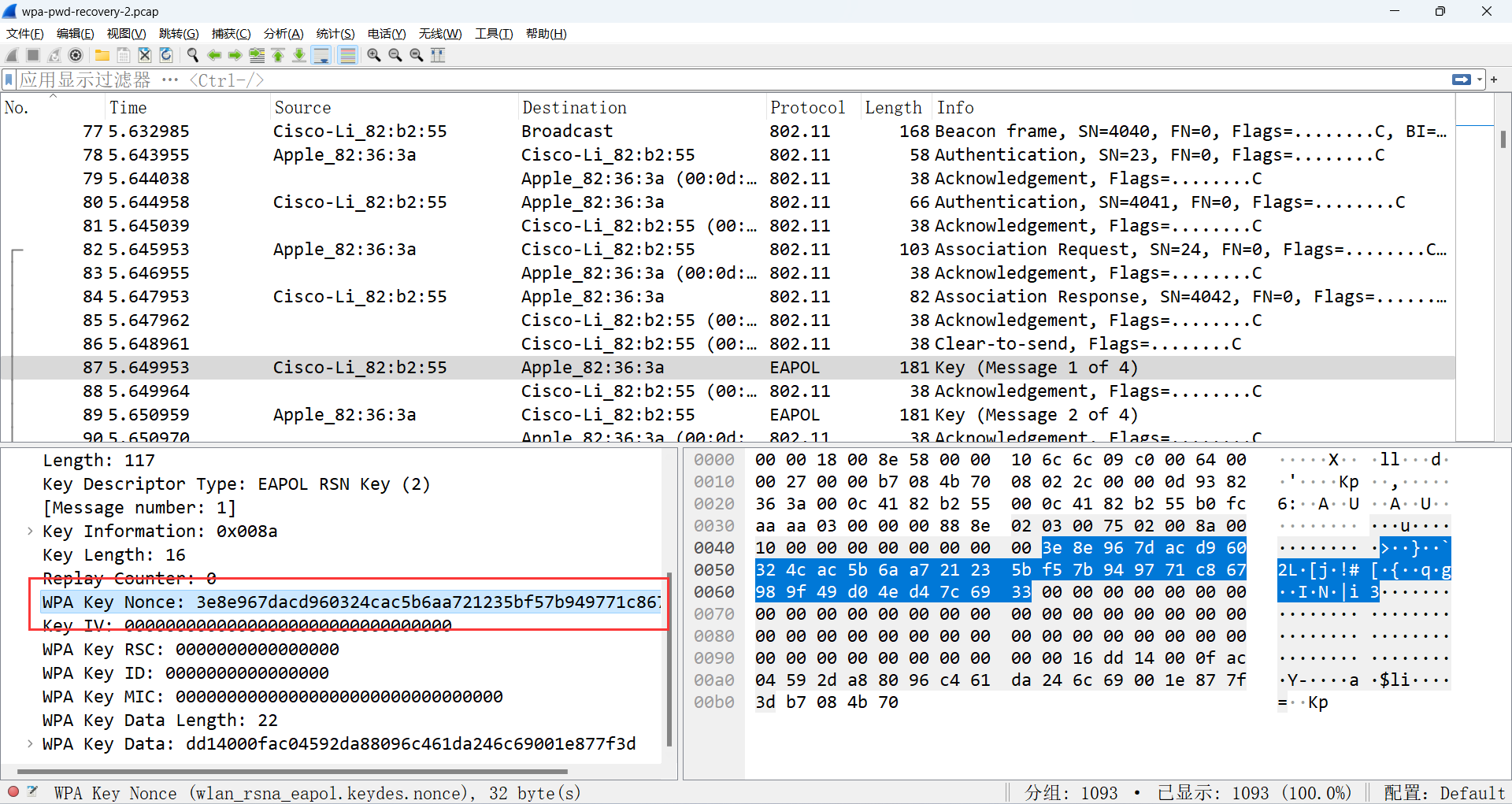
**八、实验结果与分析（含重要数据结果分析或核心代码流程分析）**

首先，根据beacon帧获取到相应的SSID：



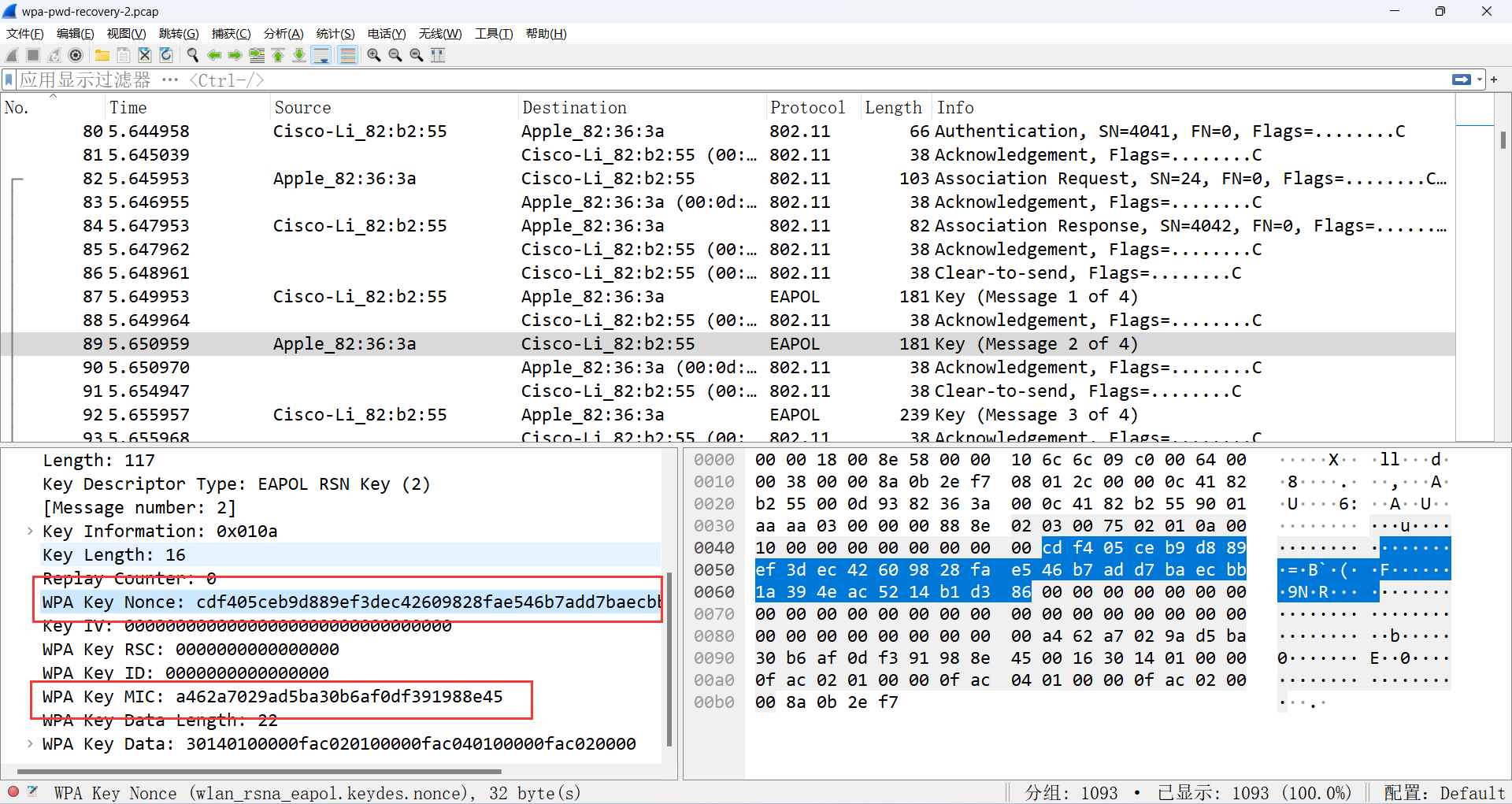
接下来，处理四次握手的过程：

MSG-1：



根据MSG-1，可以得到AP生成的ANonce。

MSG-2:



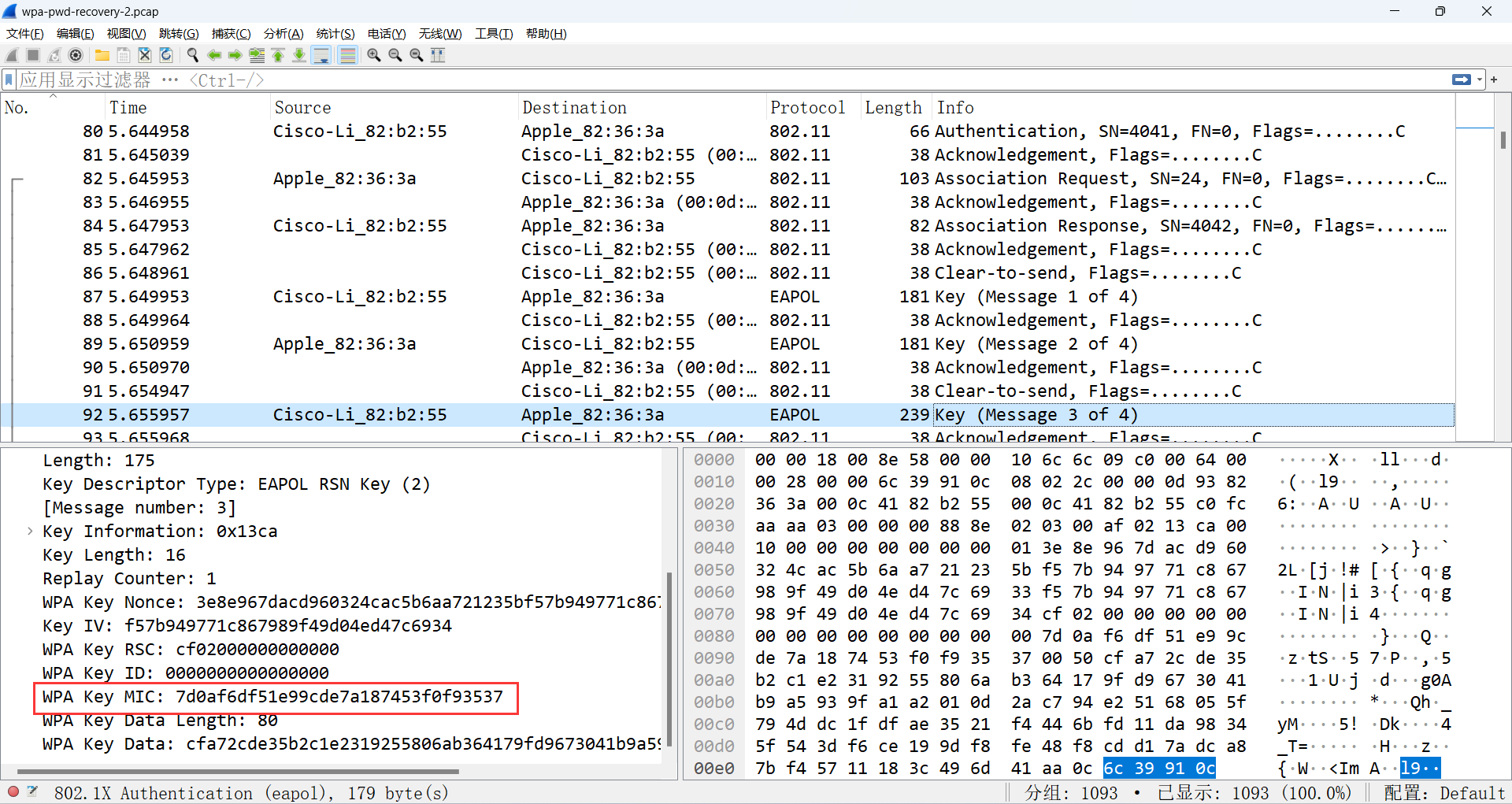
通过第二个握手包，可以获取我们需要的SNonce和MIC字段。

MIC 的计算方法为： 输入：802.1x 的所有字段，包括 MIC 字段，只是在计算的时候该字段设置为全 0。

对 WPA 来说，计算函数是 HMAC-MD5

对 WPA2 来说，计算函数是 HMAC-SHA1

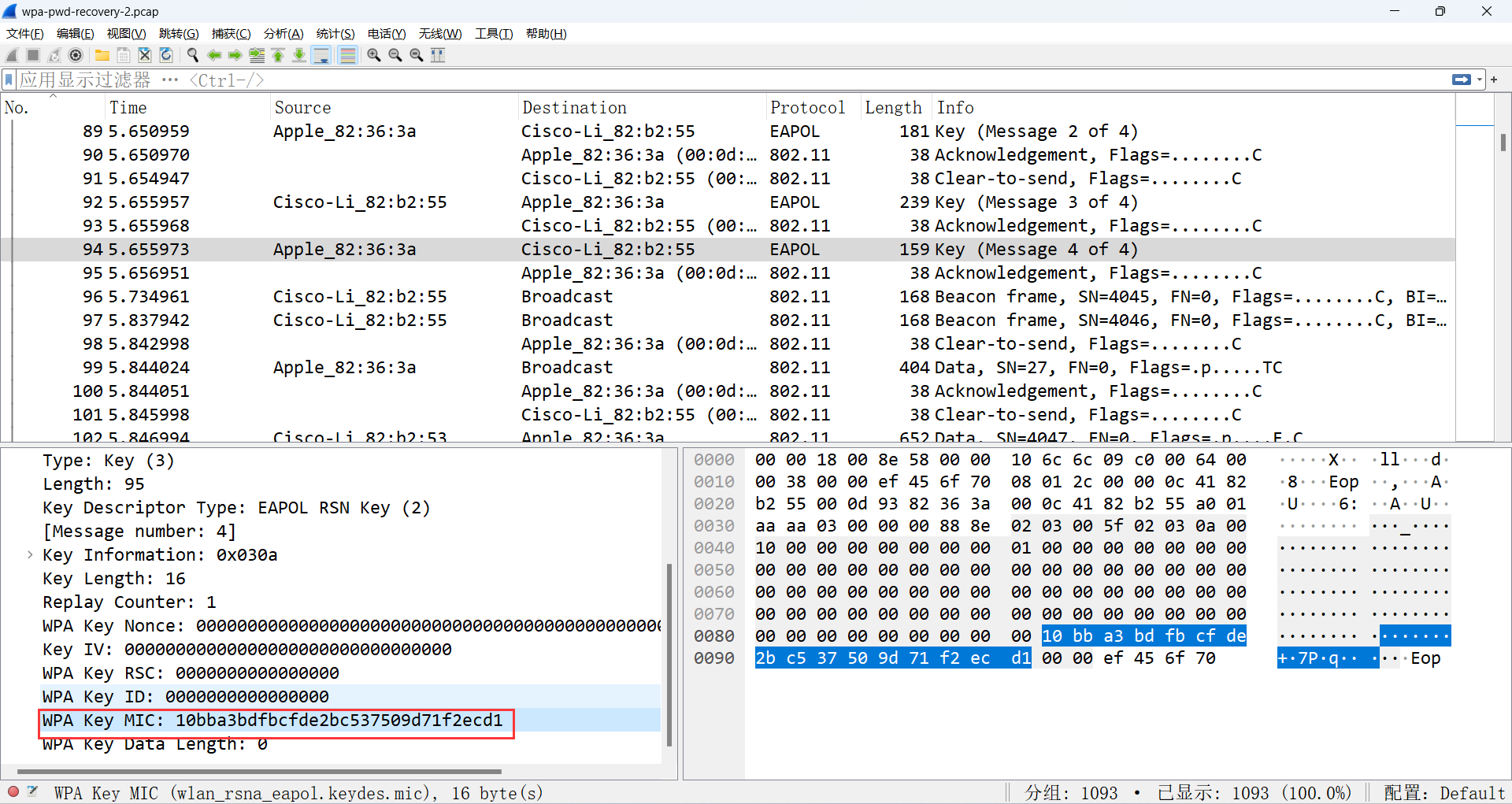
MSG-3:



在第三个握手包中，传输的重要信息包括 MIC 字段和 WPA key data 字段。通过 MIC 字段，AP 可以向 STA 认证自己。

同样的，获取需要的MIC字段，同时计算MIC的方法和之前相同。

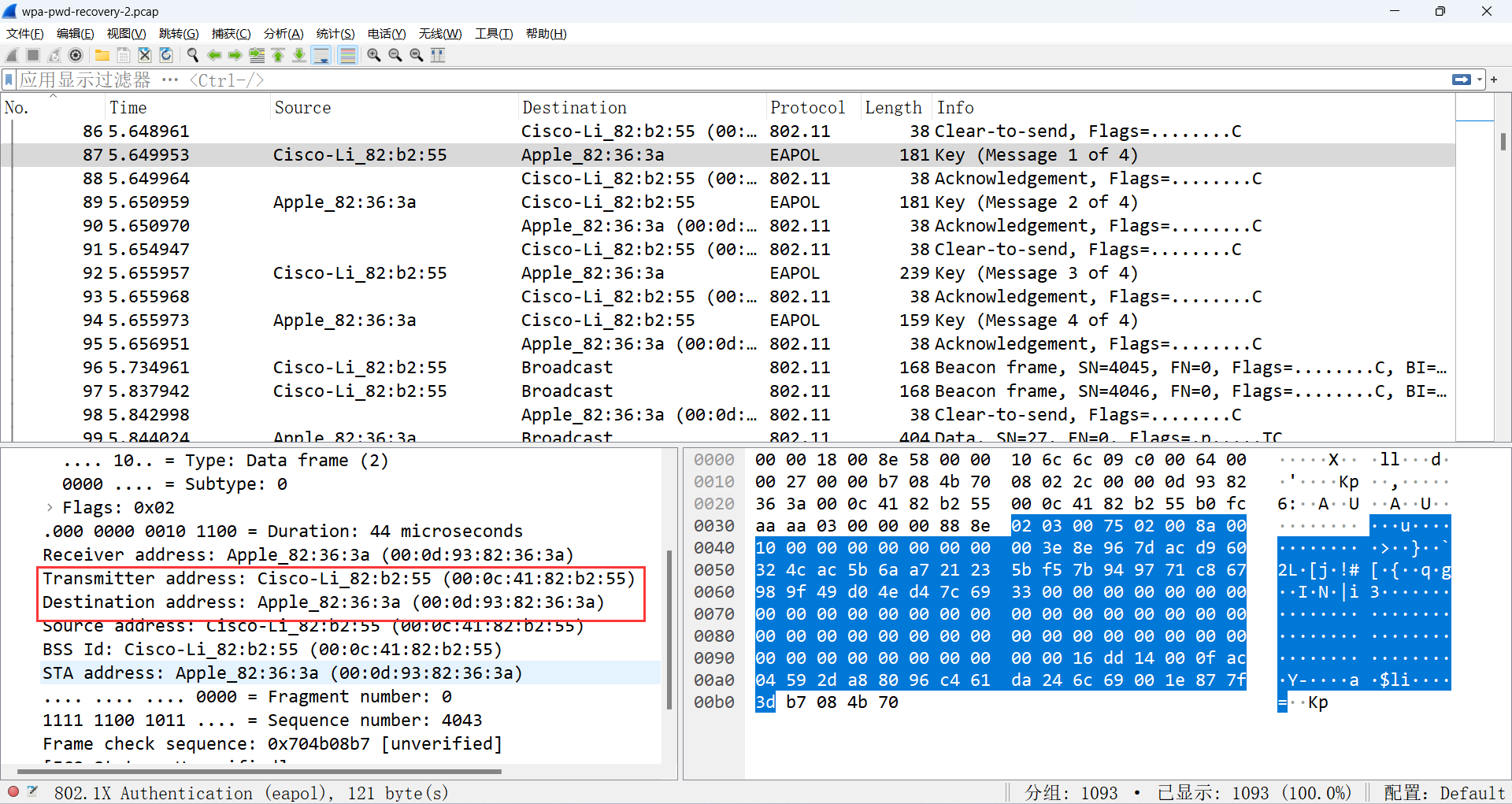
MSG-4:



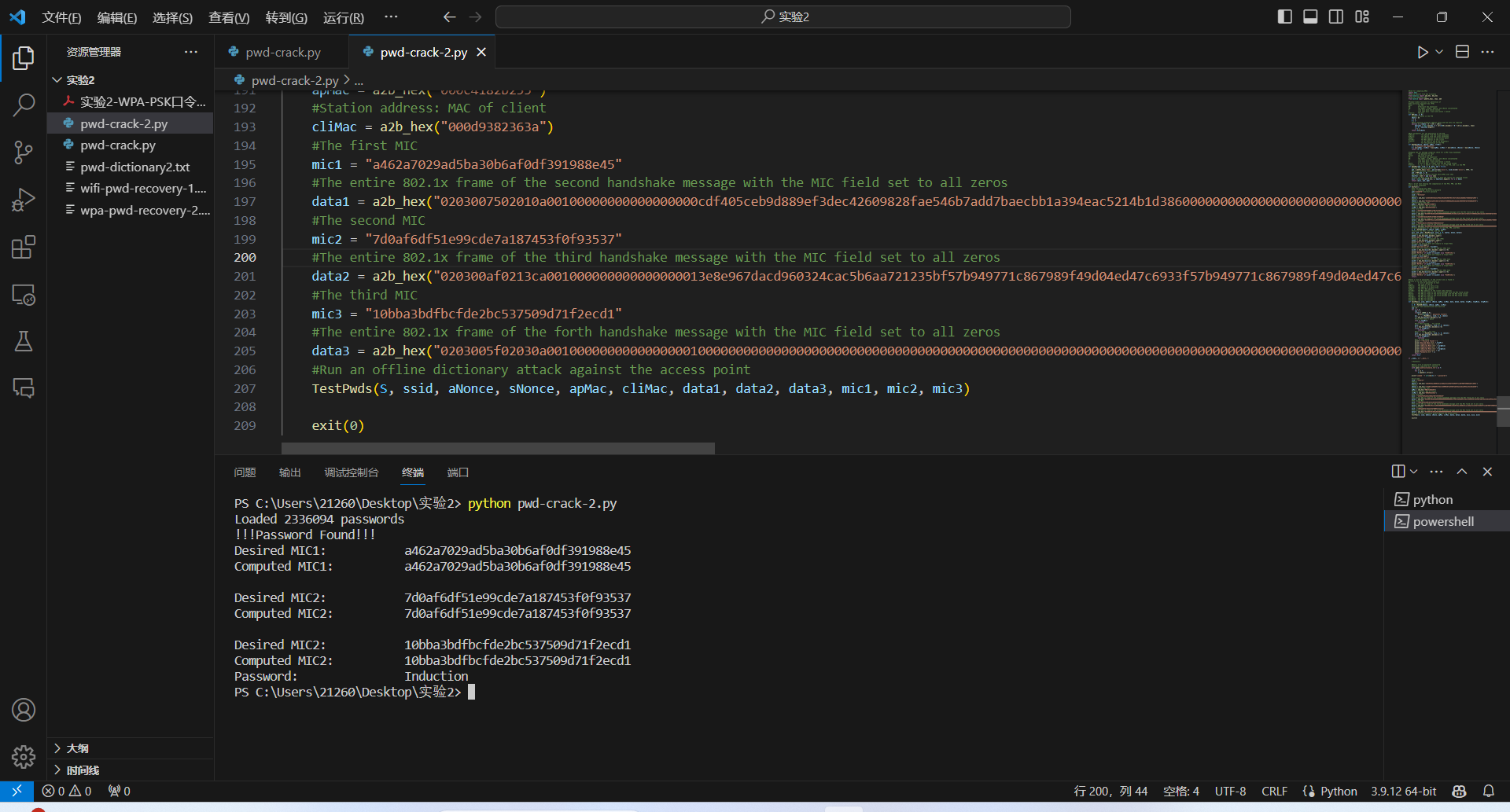
STA 发送第四个握手包，用于向 AP 确认它收到了正确的密钥，加密通信即将开始。

第四个握手包也包含 MIC 字段，计算方法同前。

同时根据上述的握手阶段，获取需要的AP地址和STA地址。

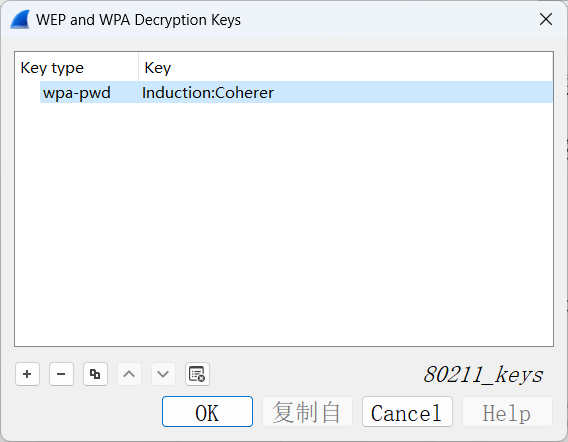


编写代码，同时利用提供的离线字典集合进行暴力破解：

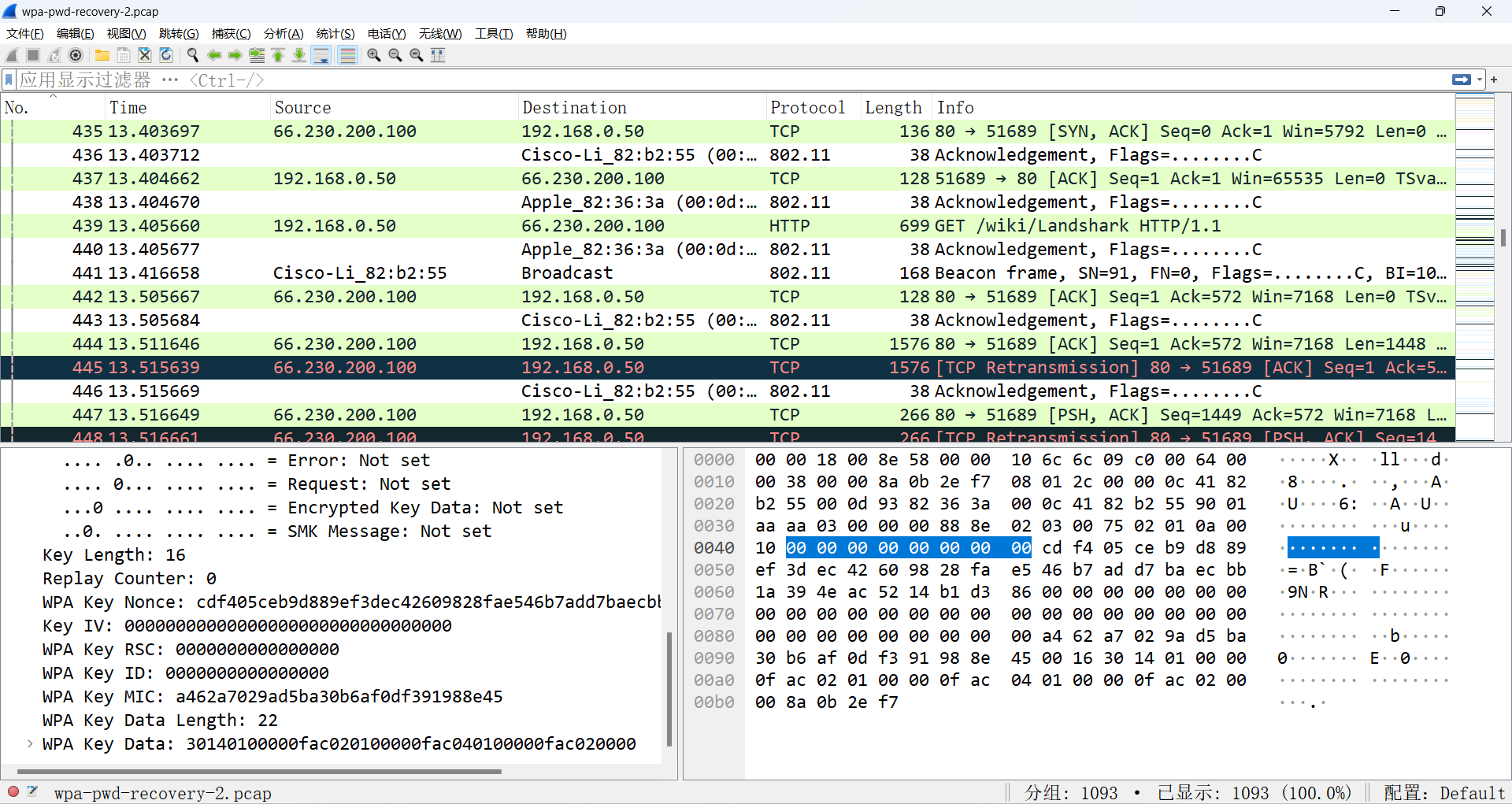


得到我们**wpa-pwd-recovery-2.pcap**这个包的密码是**Induction**。

接下来进行验证，我们得到的口令到底是否正确。

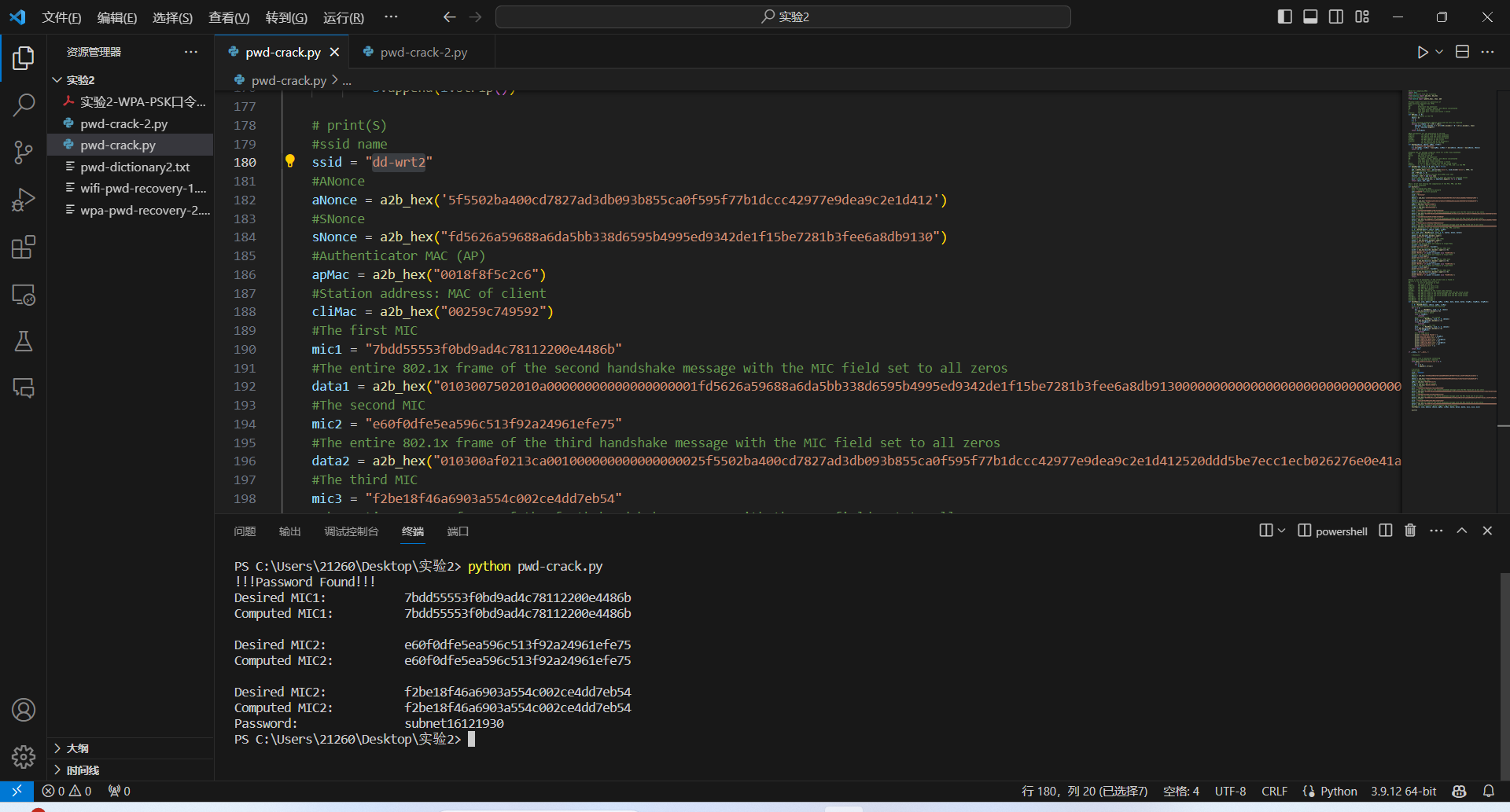


在wireshark里面配置一下我们这个包的wpa-pwd，然后返回查看结果：



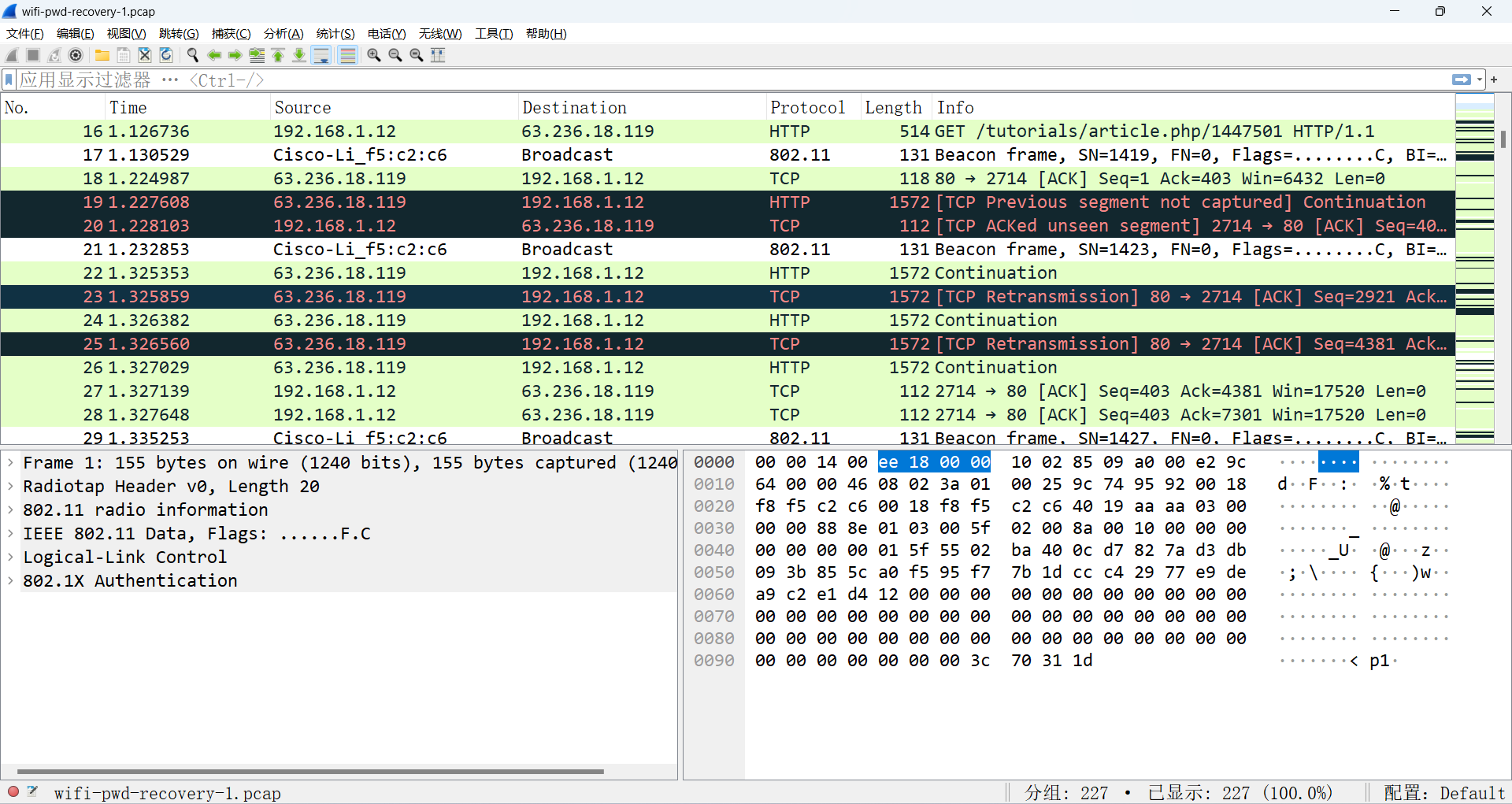
从这里可以看到，上层协议可以解析了，比如 DNS 协议里面的域名，http 协议里面 GET 命令的内容等，表明**已经解密数据帧**。

同理，我们能够暴力破解一下数据包：wifi-pwd-recovery-1.pcap：



得到我们**wifi-pwd-recovery-1.pcap**这个包的密码是**subnet16121930**。

同样的，我们进入wireshark进行验证：



可以看见，同样**破解成功**了。

**九、总结及心得体会：**

通过完成WPA-PSK口令破解实验，我在无线局域网络（WLAN）的工作原理、RSN的密钥层次以及四次握手原理等方面取得了一些新的认识和经验。首先，在实验中，我深入理解了WLAN的工作原理。无线局域网络采用了一种无线传输数据的方式，通过基站和终端之间的无线信号传输实现网络连接。在WPA-PSK的口令破解实验中，我了解到WLAN的数据传输中存在加密和认证的过程，这有助于提高无线网络的安全性。其次，我对RSN的密钥层次有了更深入的了解。RSN是为了加强WLAN的安全性而设计的一种协议，它采用了更为复杂的密钥层次结构，包括PTK和GTK等。最后，通过实验，我掌握了四次握手的原理。四次握手是WPA-PSK协议中建立安全连接的过程，其中包括AP和客户端之间的密钥协商。在破解实验中，我深入了解了这一过程，并通过分析捕获到的握手包来获取关键的信息，进而实现对口令的破解。

**十、对本实验过程及方法、手段的改进建议：**

本实验设计合理，流程循序渐进，难度由浅入深，暂无其他建议。

**报告评分：**

**指导教师签字：**