## 解题文档

### 关键技术

解题主要掌握HTTP流量分析和BLUETOOTH流量分析技术，难点是BLUETOOTH流量分析以及分析提取数据。

### 解题思路

第一步：获得flag.7z的解压密码

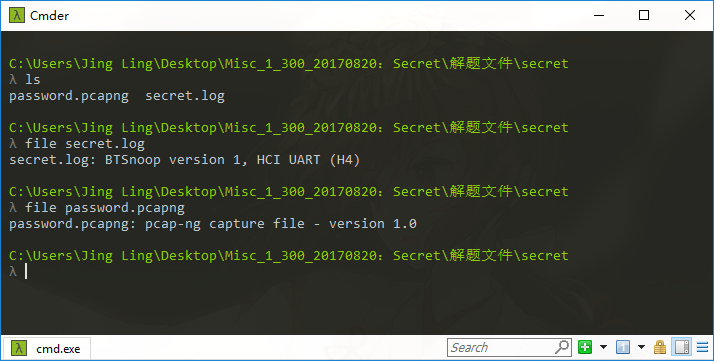
第二步：解密flag.enc内容

### 解题步骤

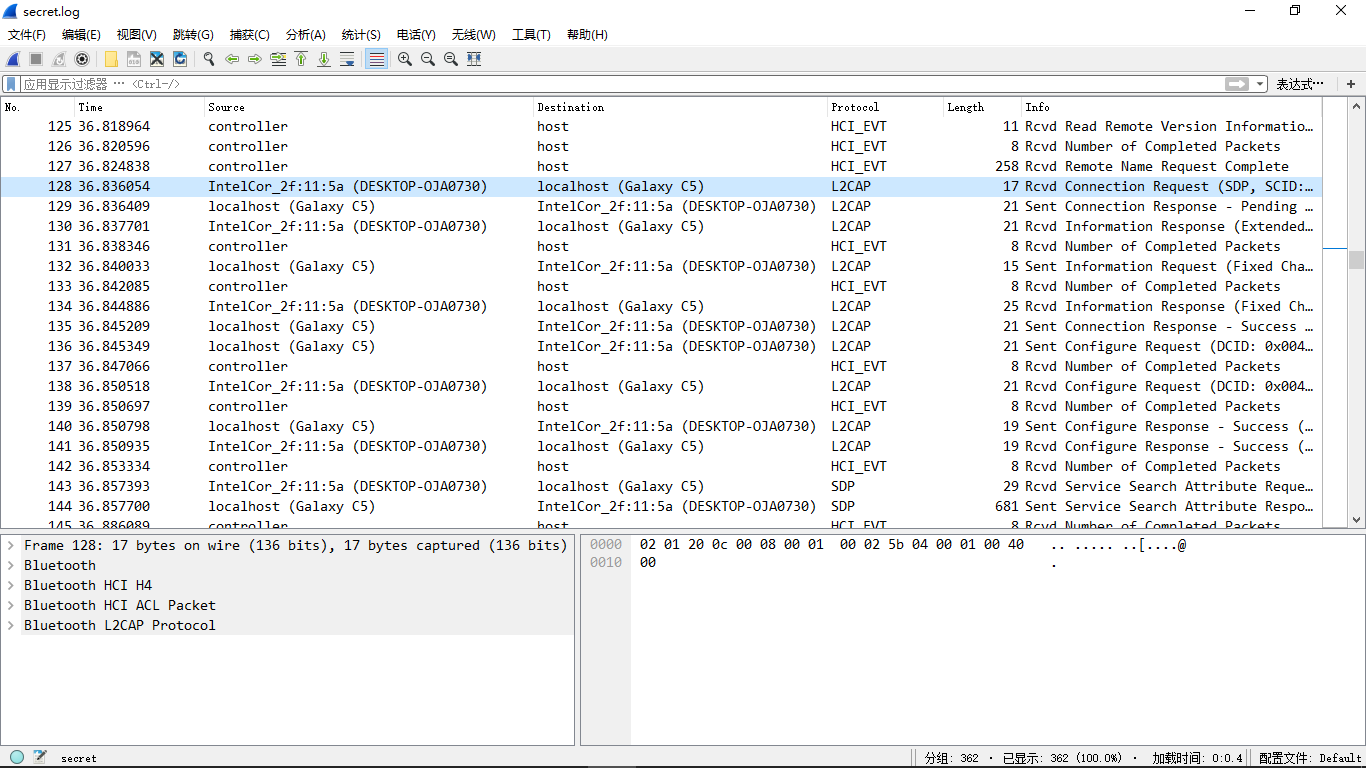
1. 提取Secret.rar

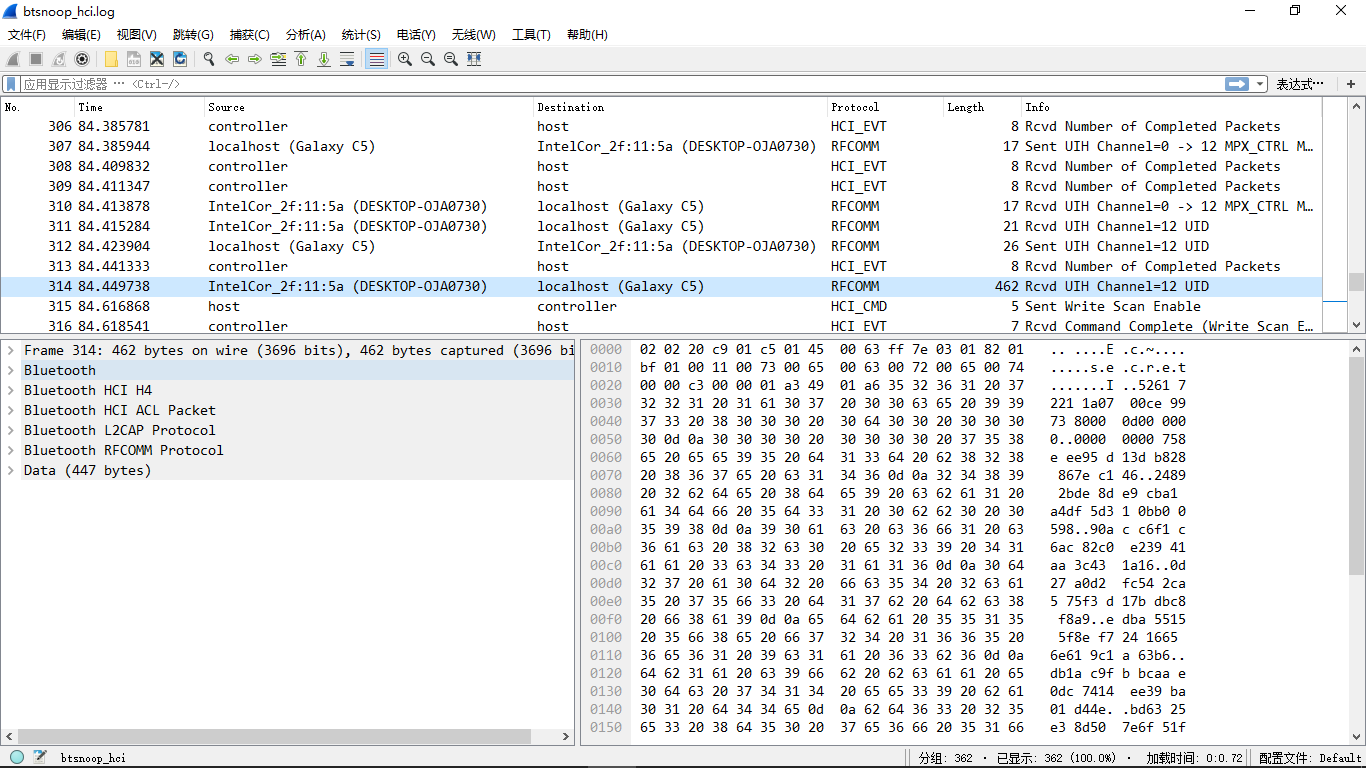
解压Secret.7z得到password.pcapng

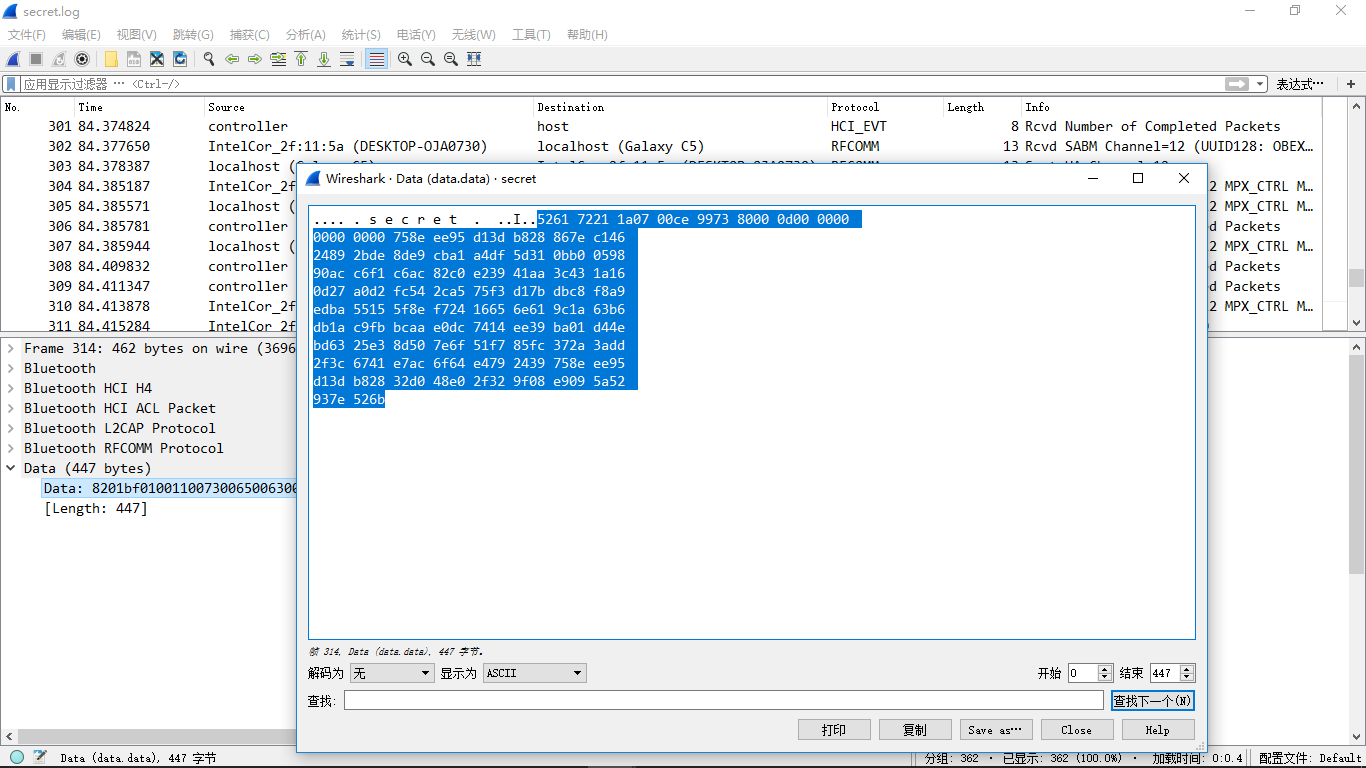
和secret.log两个文件，通过分析可知分别是pcap-ng捕获流量包和蓝牙捕获流量包。



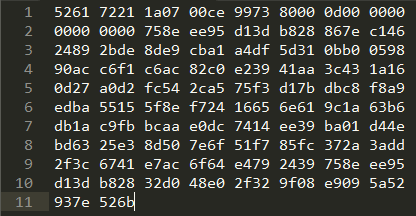
使用wireshark分析蓝牙流量：



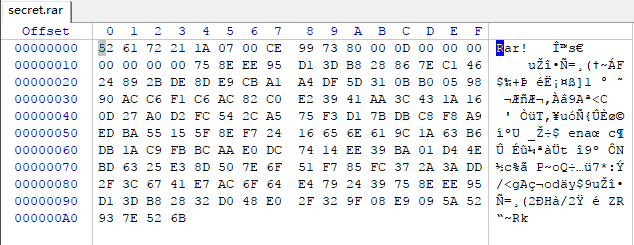




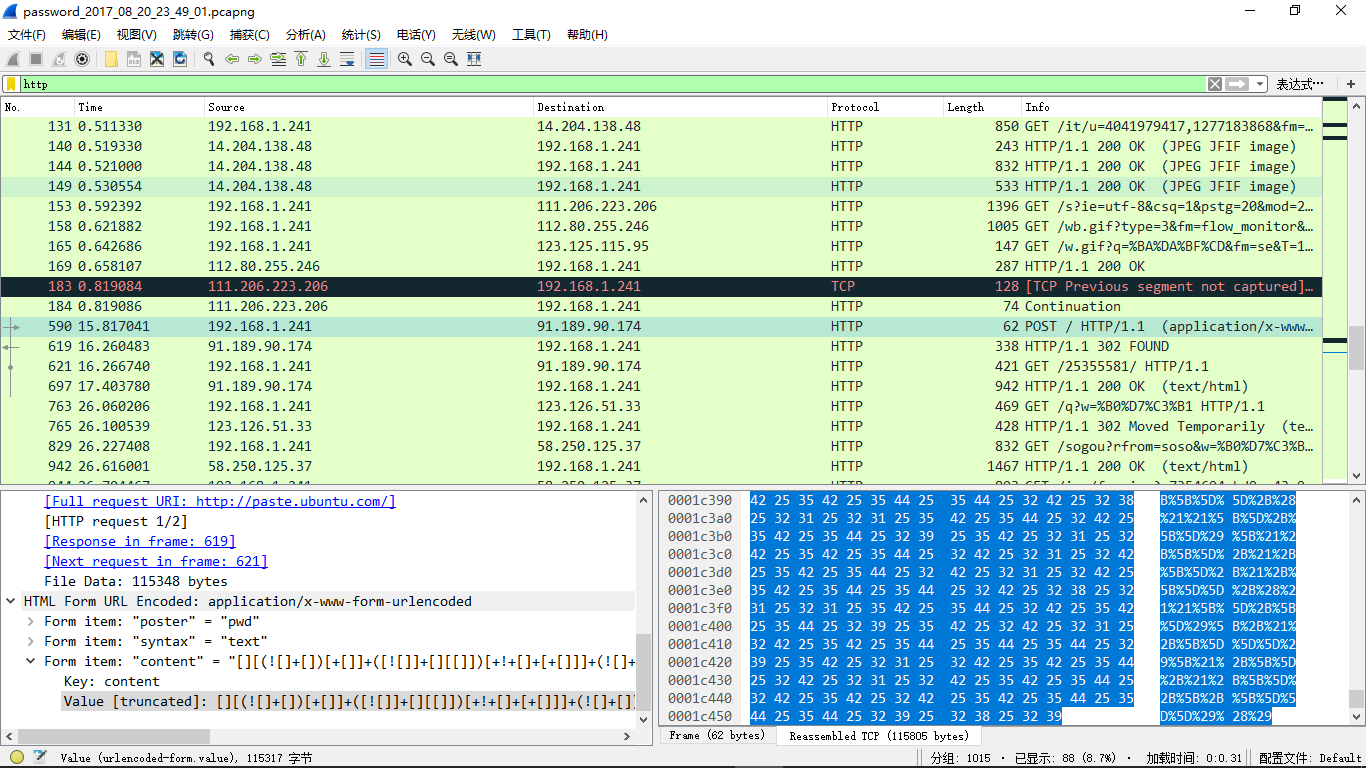
根据分析277号数据包是电脑DESKTOP-OJA0730开始向手机Galaxy C5发送secret，将data提取出来出去头标志得到data。



简单分析一下，5261开头，526b结尾应该是RAR文件，所以将16进制的ASCII转换为二进制文件得到secret.rar文件：



1. 尝试打开secret.rar提示输入密码，根据提示分析password.pcapng：



根据分析，过滤出HTTP流量，发现密码经过jsfuck编码，提取出代码在浏览器控制台运行得到密码：  


解压secret.rar，得到flag.txt。

