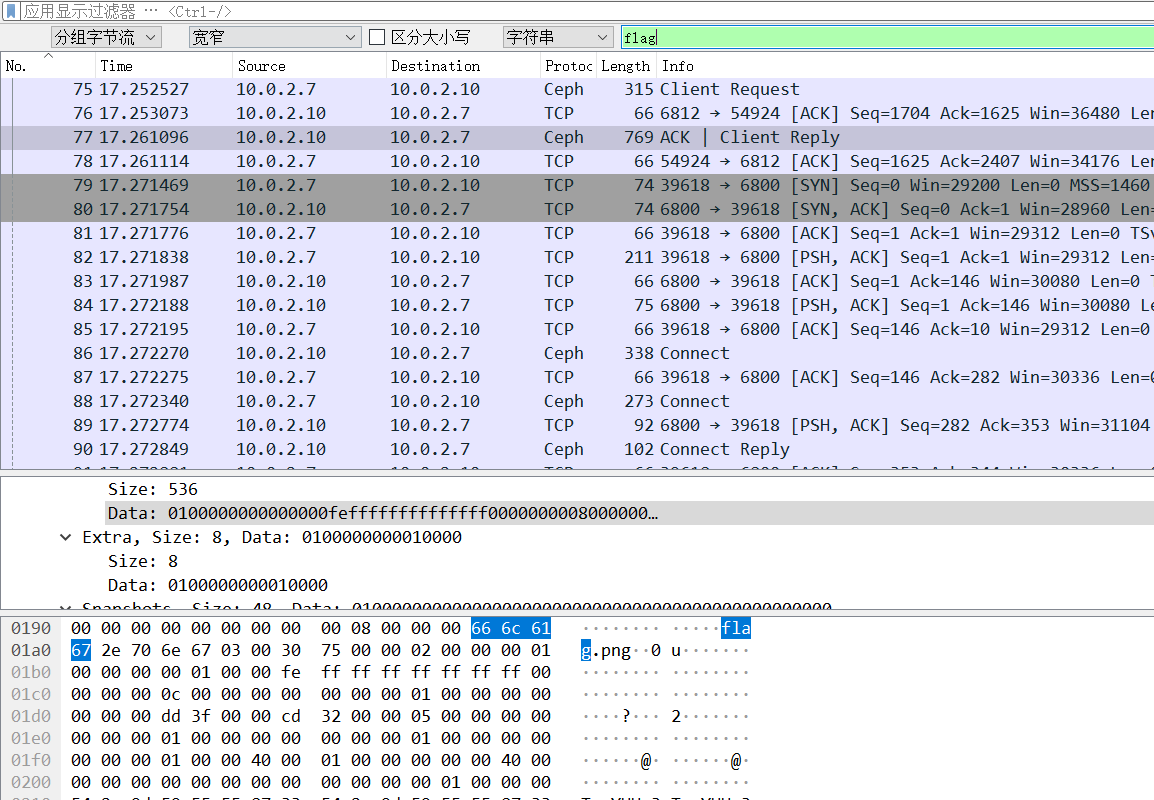
网络流量分析是指捕捉网络中流动的数据包，并通过查看包内部数据以及进行相关的协议、流量分析、统计等来发现网络运行过程中出现的问题。在应急响应中，流量分析作为重要的取证方法，在ctf题中尤为常见，此处通过分析几个ctf题目，利用wireshark对数据流量包进行分析。

一、Cephalopod(图片提取)

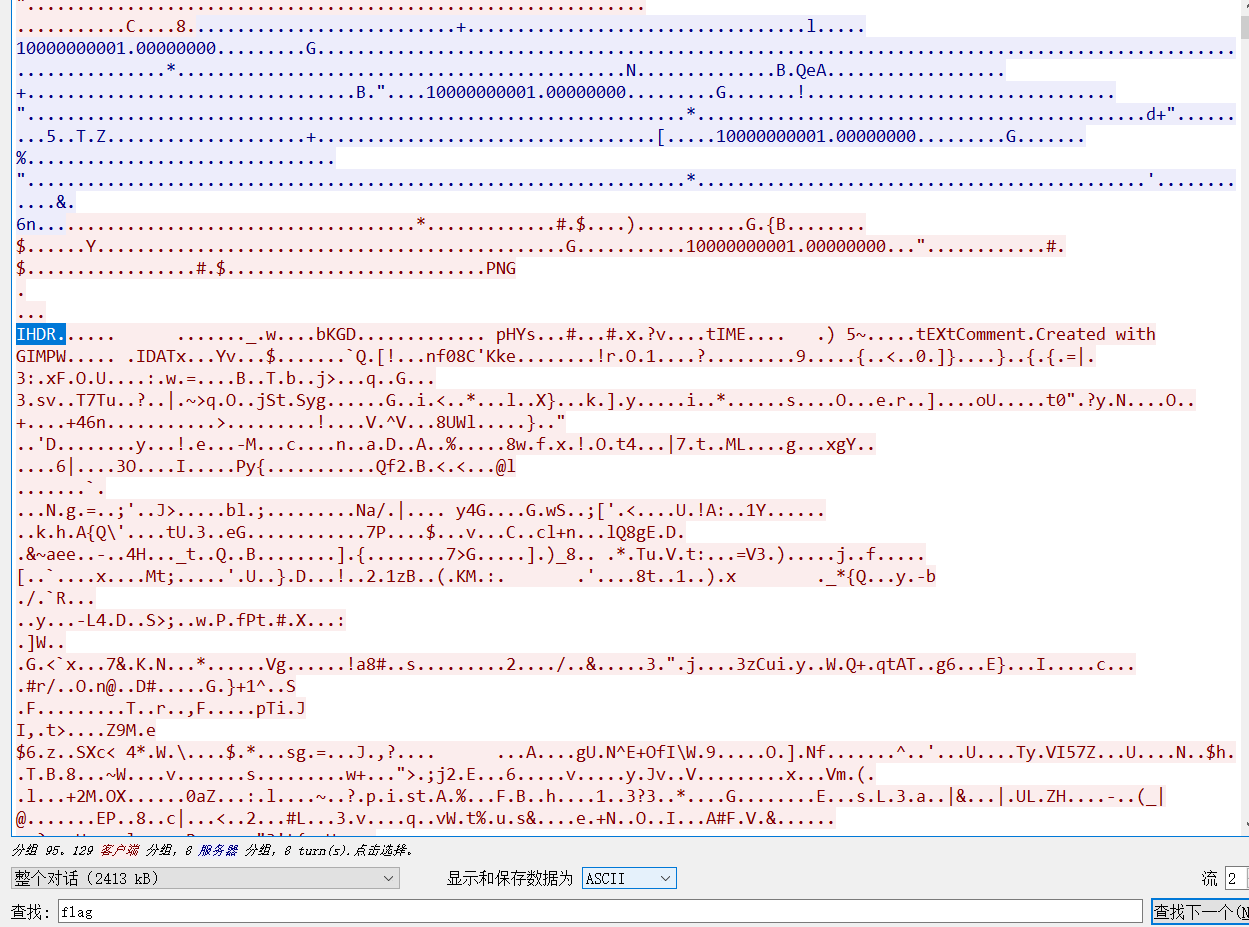
题目描述如下：



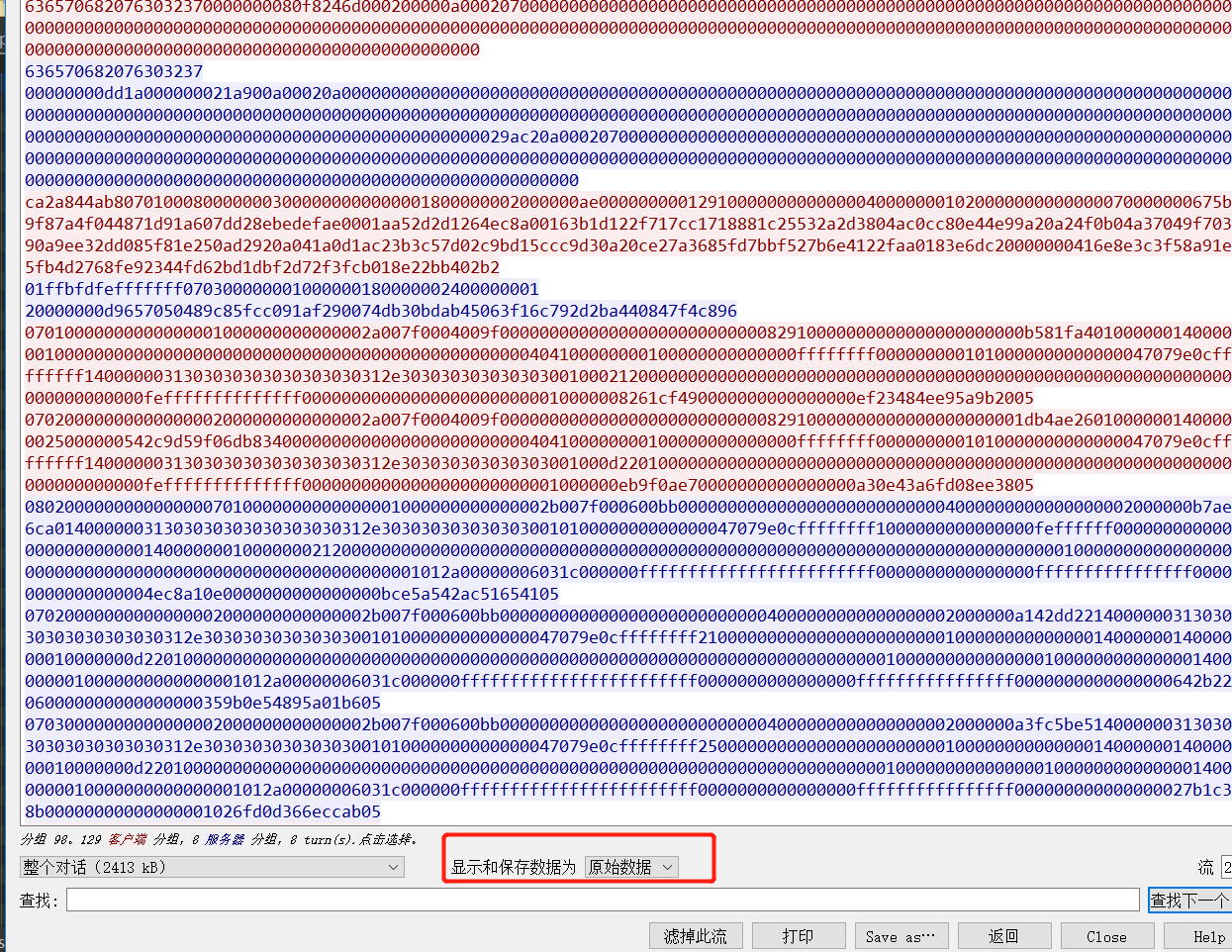
1、下载附件发现，为一个Cephalopod.pcap流量包，分组字节流模式下进行关键字搜索，可发现flag.png



2、通过右键追踪tcp数据流的方法，可发现图片信息



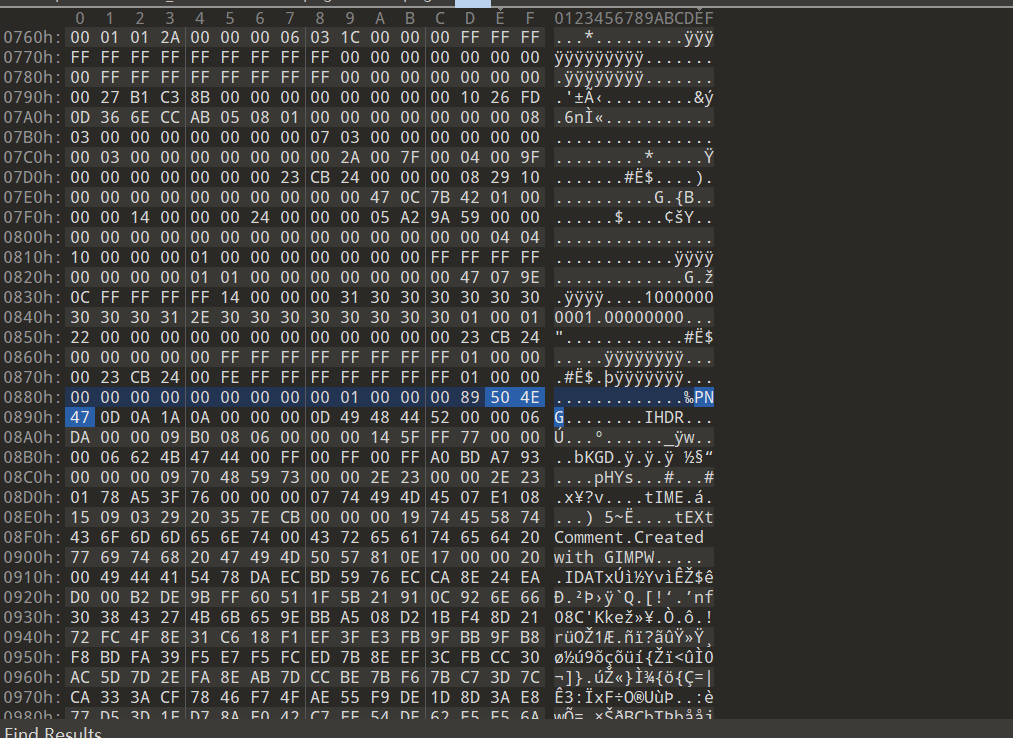
3、将此数据流保存为“原始数据”，保存即可



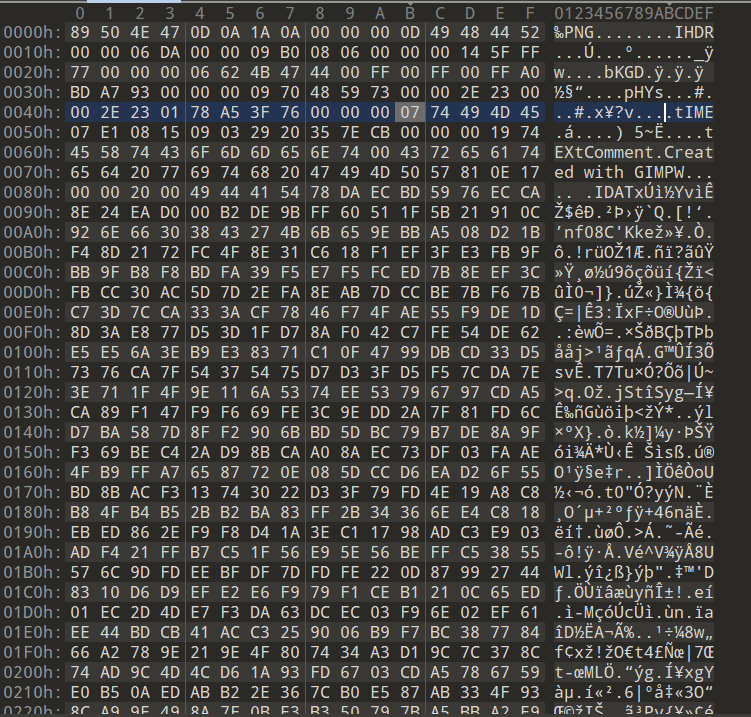
4、此时保存后的文件并不是一张png格式的图片，png图片的结构如下

PNG文件标志 PNG数据块 …… PNG数据块

PNG数据块：IHDR为文件头数据块的第一块，它包含有PNG文件中存储的图像数据的基本信息，并要作为第一个数据块出现在PNG数据流中，而且一个PNG数据流中只能有一个文件头数据块。所以需要将png文件标志位前面的数据进行删除



最终得到一张完整的png格式图片



5、打开该图片即可获得相关flag



二、信息提取

题目描述：数据库中的flag被偷走了，好在全过程我们都有记录

题目文件：sqlmap.pcap

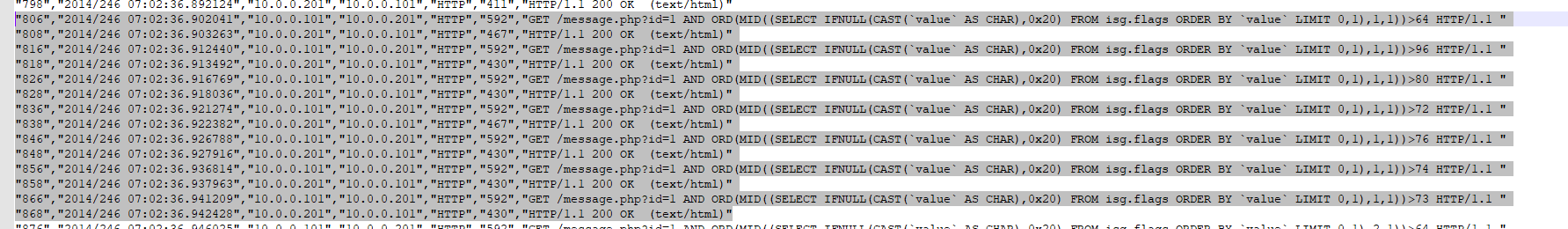
1、打开流量数据包，”导出对象“——”http“数据包，可显示所有的http流量，从中不难发现sql注入攻击流量



2、利用python脚本对文件提取数据并进行解码，如下图，从中可见系统存在sql盲注，先进行数据库猜解在进行表名猜解



3、将过滤后的数据包导出结果如下：



ascii有 128个所以从 64 开始判断，然后是96(64和128的中间值)，说明>64是正确的 ，才会取96，然后是 80，80小于96，说明>96是错误的，所以才会取 64和96 的中间值 80，然后是 72 ，说明>80是错误的，取80和64之间的中间值72，然后是76，说明>72是正确的，才会取 72 和80之间的中间值76，然后是 74，说明>76是错误的，才会取 72 和76的中间值 74，然后是73，说明>74是错误的，才会取 72 和 74的中间值 73，通过分析数据包发现，当返回值长度大于430即可判断正确，所以只需要获取最后一次正确的值，在将此值加1即为最终数据，可利用脚本解出获得最终的flag（）



小结：关于流量分析确实懂得不多，有待学习和提高，感谢互联网大牛的倾情奉献。

参考链接：<https://www.cxyzjd.com/article/vhkjhwbs/102612656#8%EF%BC%8C%E4%BF%A1%E6%81%AF%E6%8F%90%E5%8F%96%EF%BC%88%E8%B6%85%E8%AF%A6%E7%BB%86%EF%BC%89>