2024.9.13

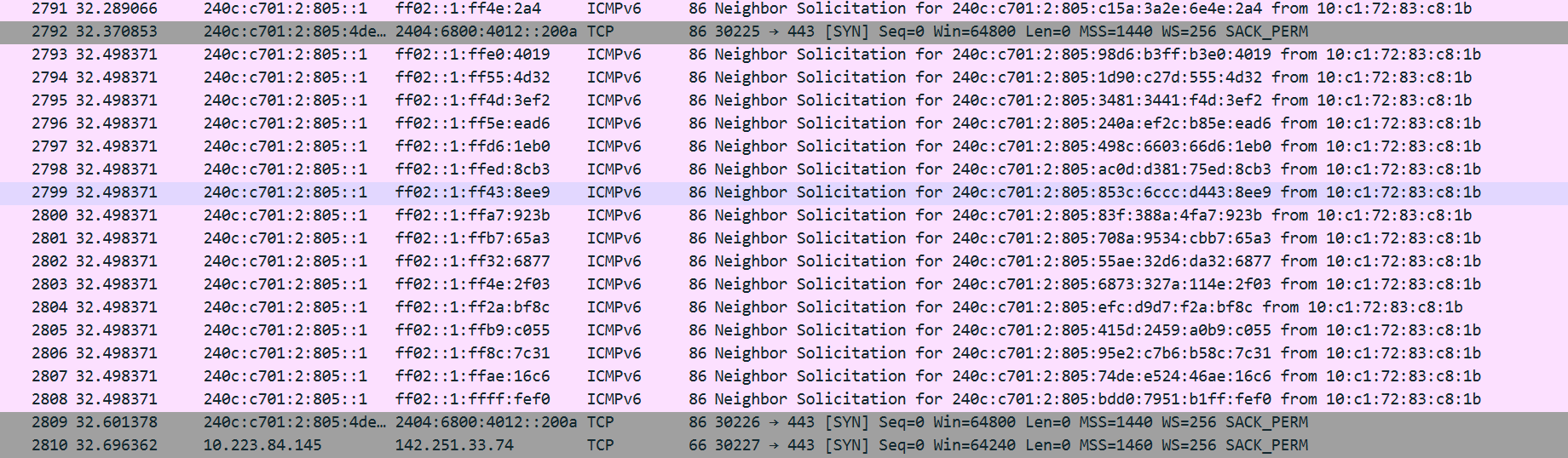
计算机网络（H） Lab1

实验人：谢志康

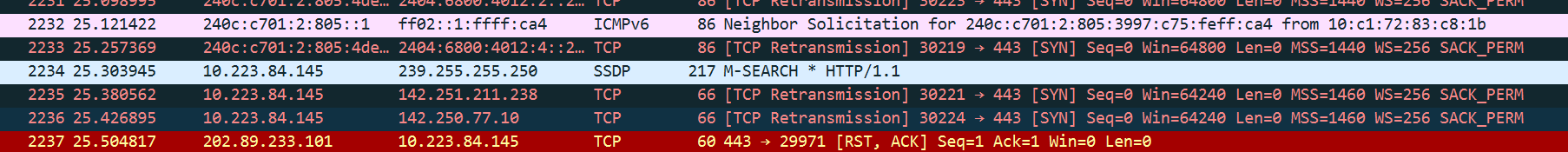
学号：22307110187

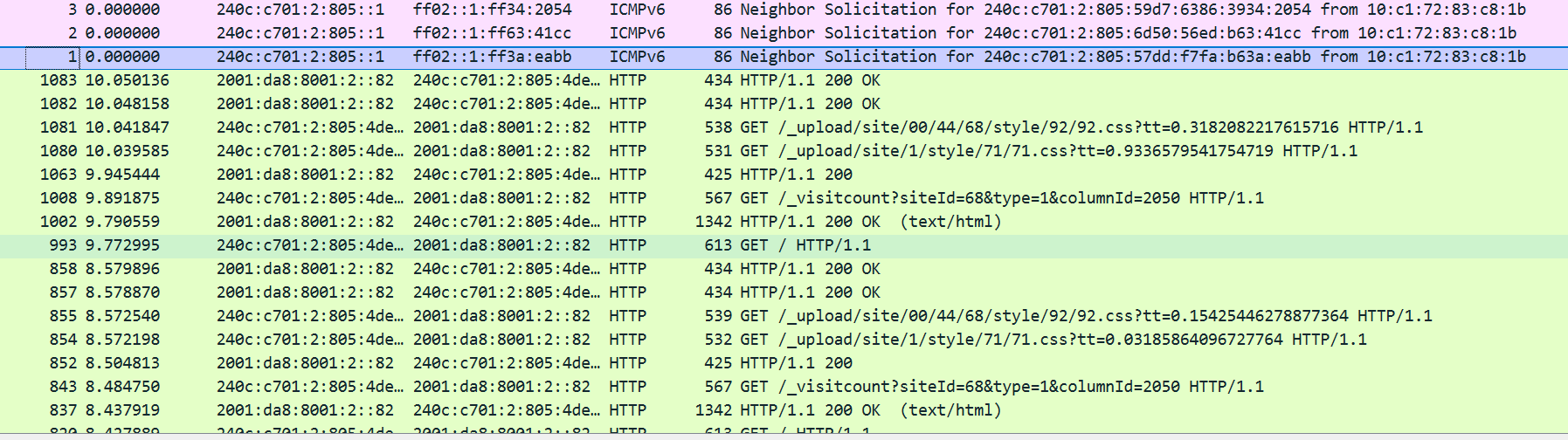
实验内容：

1. 请列出捕获到的5种不同类型的协议。



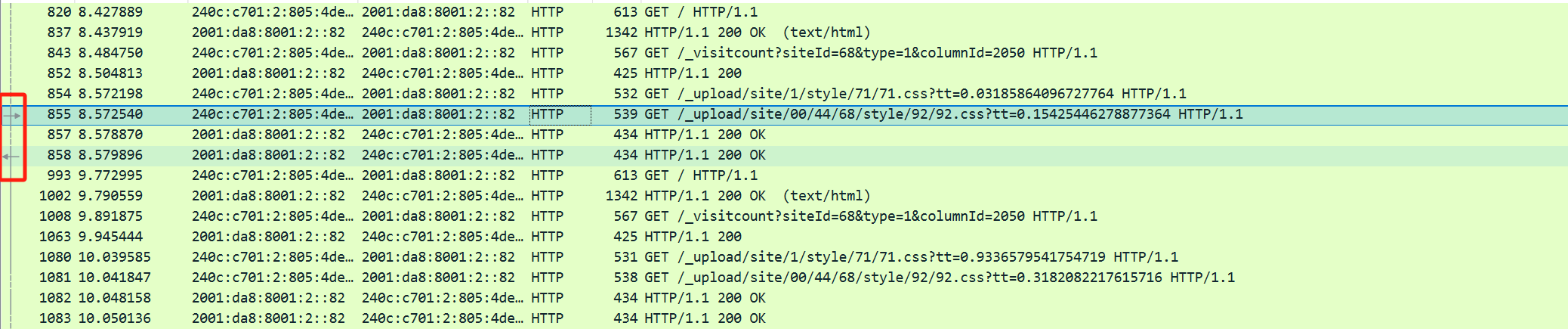




有TCP ICMPv6 ARP SSDP HTTP 协议。

1. 用显示过滤器过滤出所有http消息，从发送第一条 HTTP GET 请求到收到对应的 HTTP OK 回复用了多长时间？默认情况下，数据包列表窗口中 “Time”列的值是自 Wireshark 捕获开始经过的秒数，也可以点击菜单栏“视图-时间显示格式”切换到其他格式。

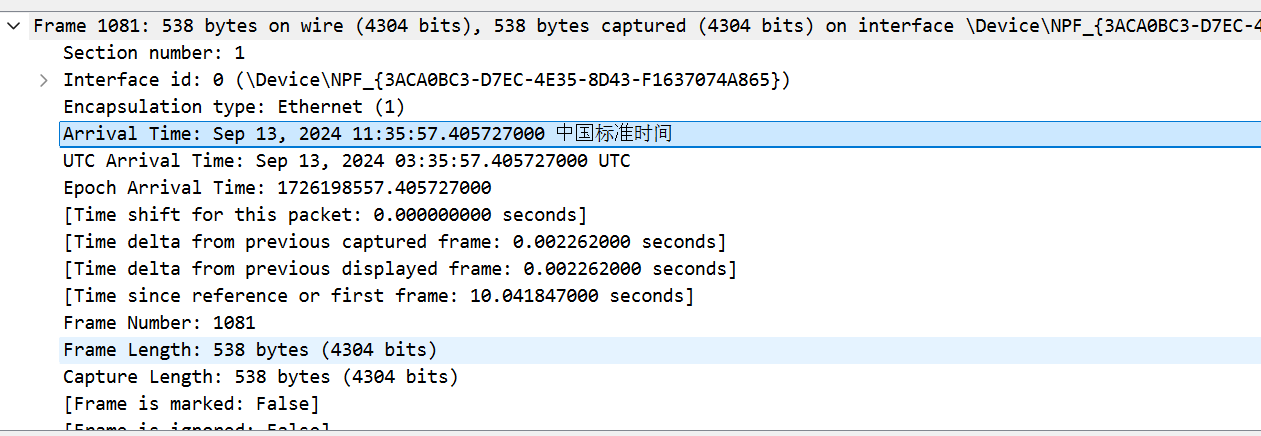
清除浏览器缓存，重新运行，过滤后——按照时间排序



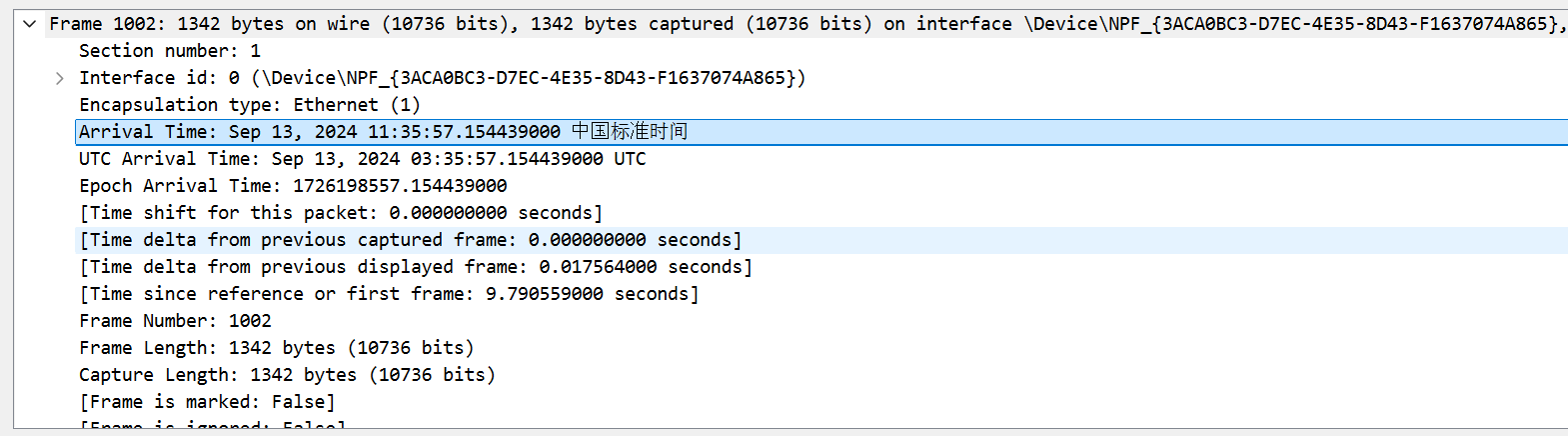
首先找到第一个确认确实是我们的目标网站（清除缓存且只打开该网页，这个应该不会出错）的HTTP GET信号，查看详细信息：



其次查看时间节点：11:35:57.405727000

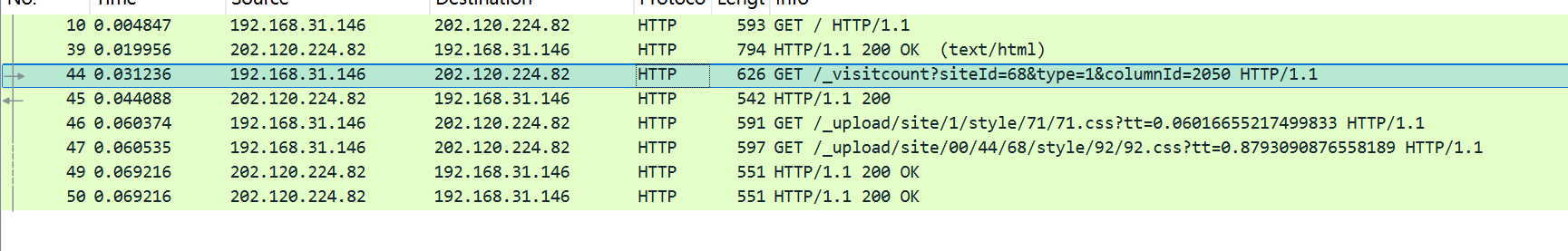


再看第一个OK信号：时间节点：11:35:57.154439000



所以，时间差为0.405727-0.154439 = 0.251288

1. 复旦信息办的 IP 地址是什么？你的计算机发送 HTTP GET 请求时的 IP 地址是什么？



GET情况下，本机发送，Source即为本机IPv4地址：192.168.31.146

复旦信息办的IPv4地址为：202.120.224.82

1. 找到任意一个 HTTP 包，发出 HTTP 请求的网络浏览器是什么？你可以在分组详细信息中 的 Hypertext Transfer Protocol（也即 HTTP ）部分，或者追踪流的页面中寻找“UserAgent"字段。

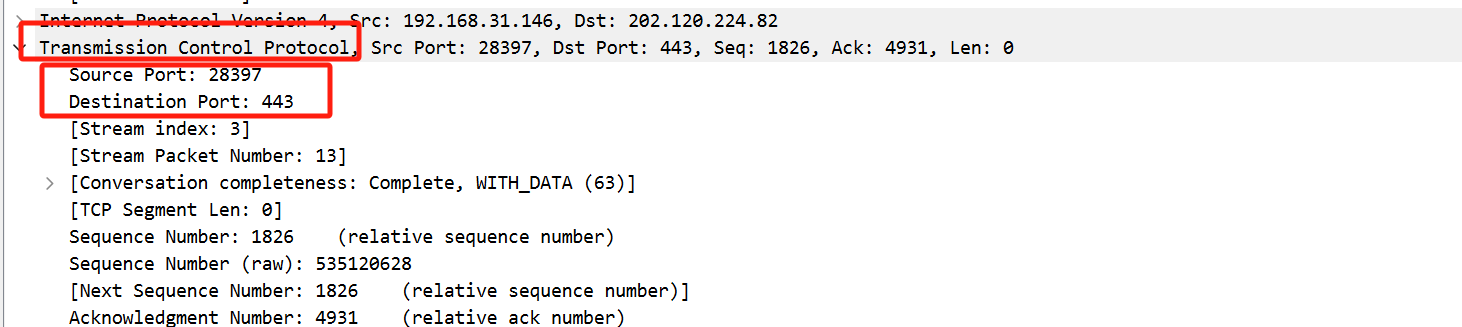
是Chrome浏览器



1. 找到任意一个 TCP 包，源端口号和目的端口号各自是什么？你可以发现，分组详细信息中的Transmission Control Protocol（也即 TCP）部分列出了 Src Port 和 Dst Port。

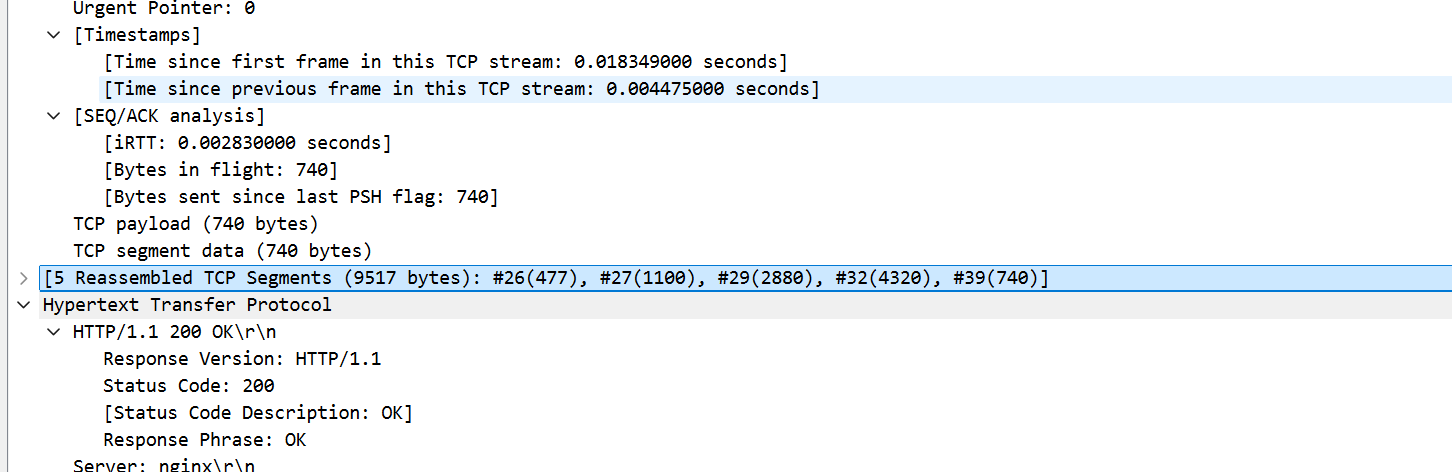
源端口号：28397

目的端口号：443



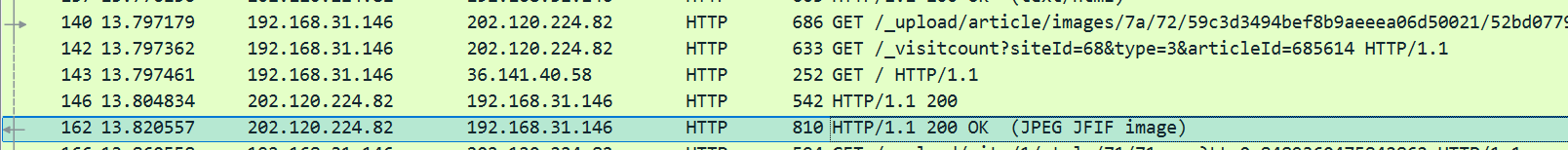
1. 找到一个由多个 TCP 报文段组合而成的 HTTP 响应分组，这个分组是由多少个 TCP 报文段组成的？在分组详细信息中，会有“[x Reassembled TCP Segments]”提示。

在详细信息的TCP下，有5个TCP报文段

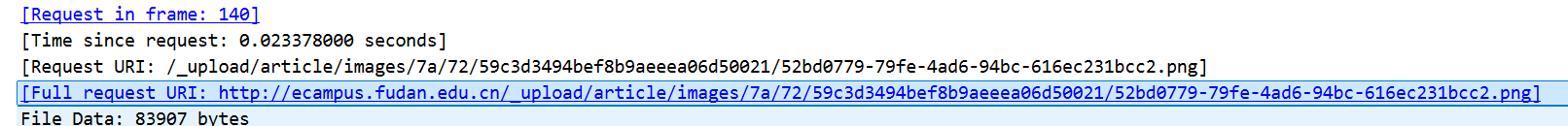


1. 找到一个带有明文图片的分组，通过“显示分组字节”在 wireshark中显示图片，并在浏览器中找到对应图片。

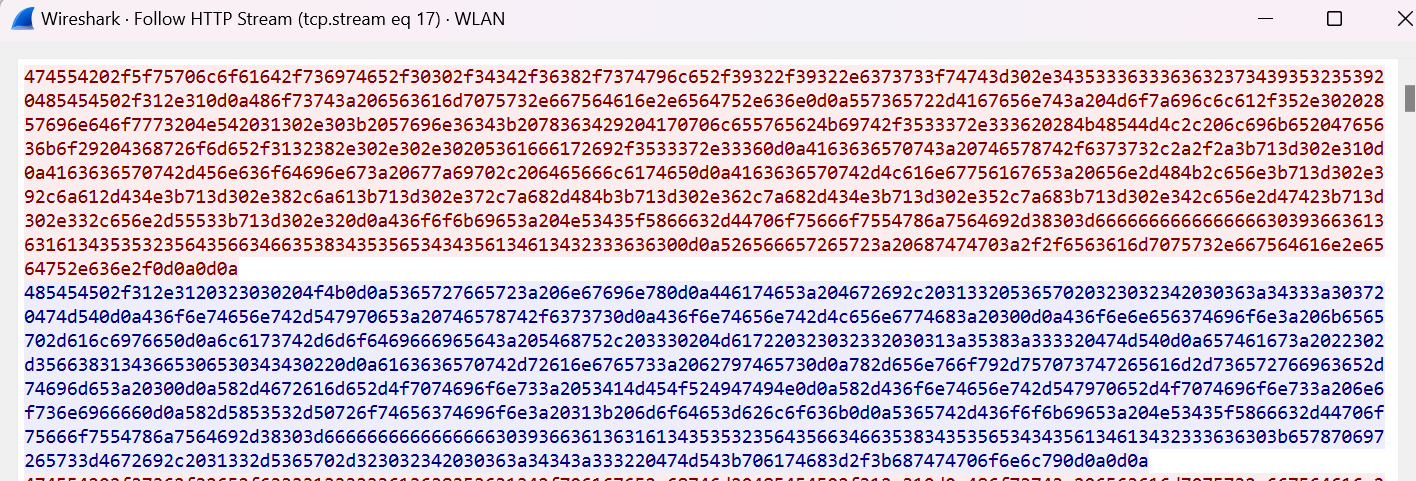
点击图片后可以抓到jpeg格式的请求和响应



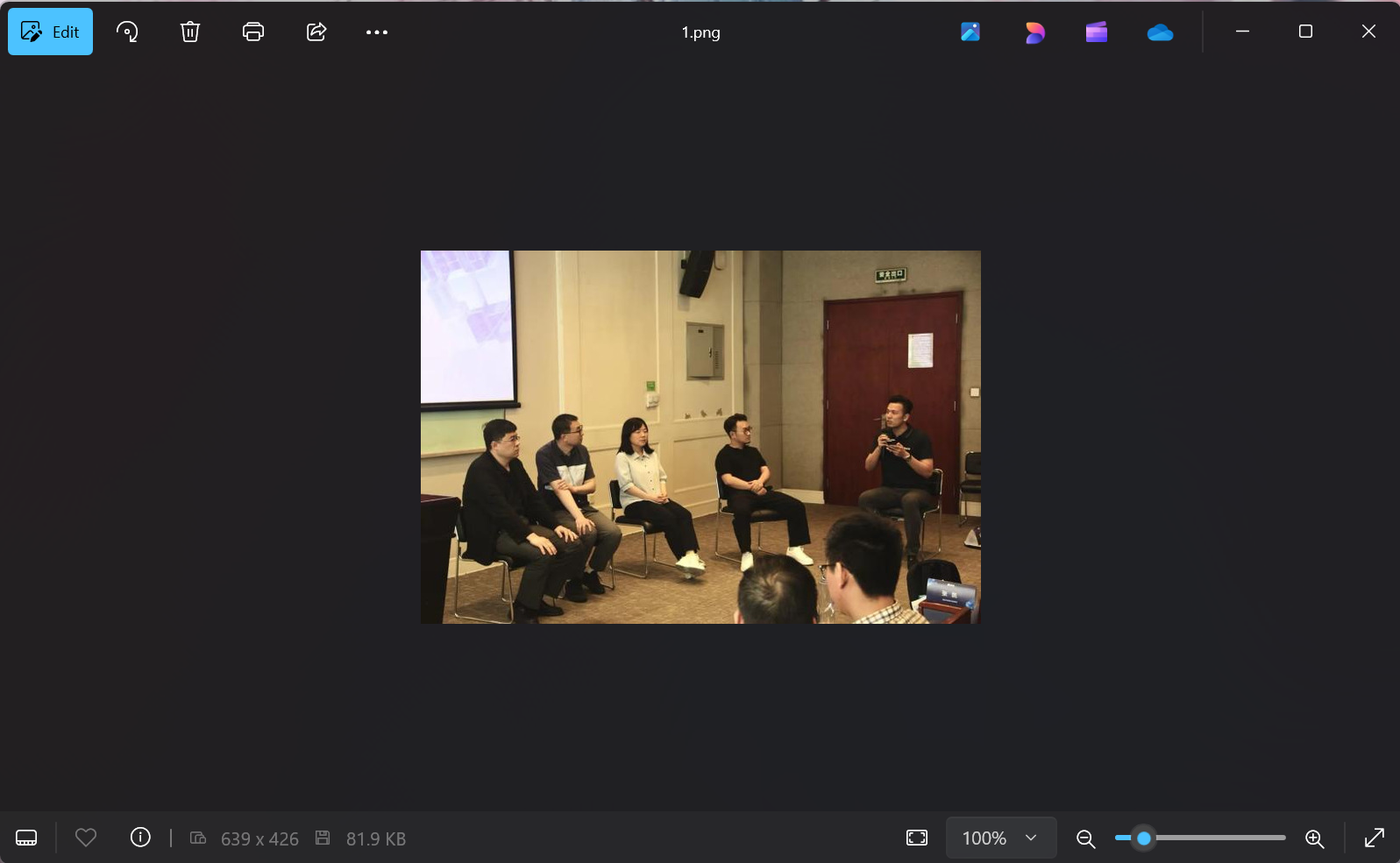
核查信息是一张完整的图片：



我以follow http stream的方法得到raw数据：



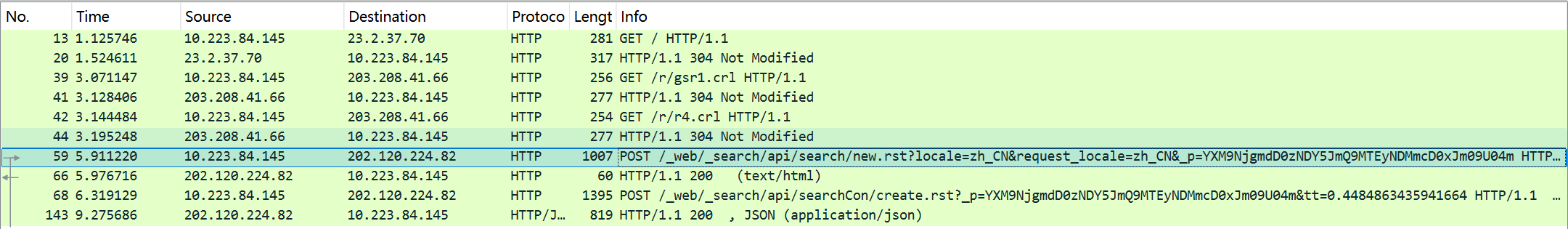
保存后即可打开：



在网站中也有这张图片：

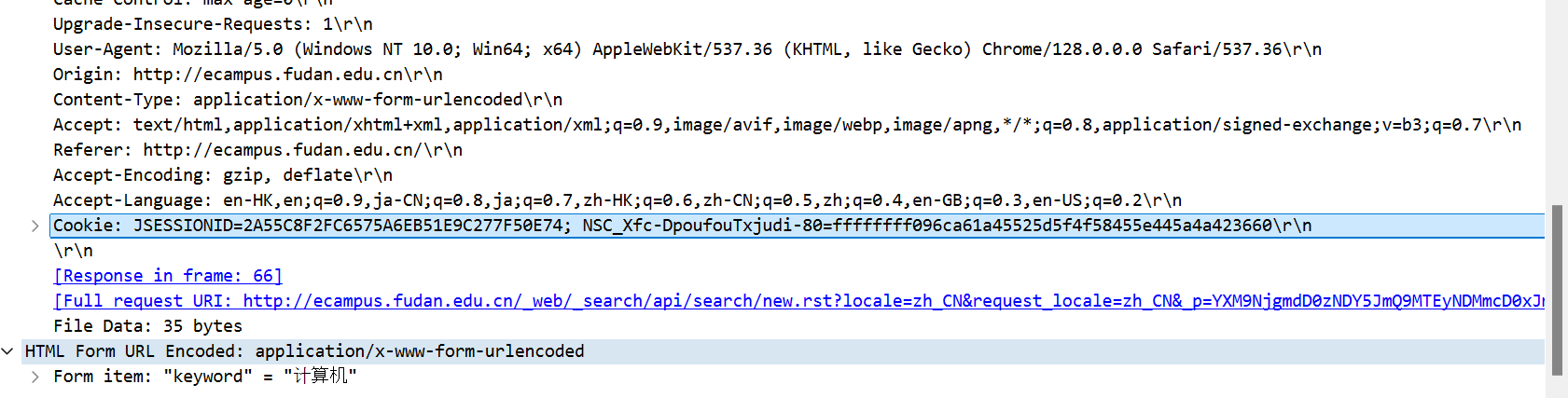


1. （确保你已经为以上问题保存了必要的截图后）重新开启分组捕获，在复旦信息办网站右上角的导航栏搜索任意内容，在捕获到的分组里寻找你输入的内容，观察 HTTP 如何通过 POST 方法发送数据。



有两个HTTP的POST方法显示：

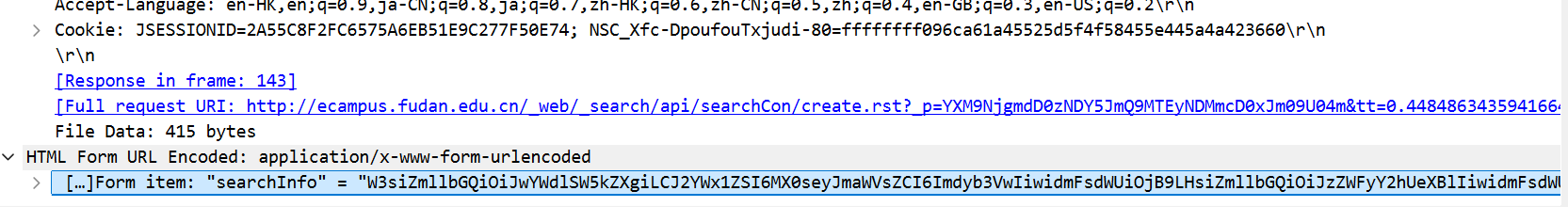
在分组详细信息中，可以在keyword那里找到自己输入的内容：



根据搜索资料，请求的内容通常会在application/x-www-form-urlencoded 格式中发送，可以看到上图确实：HTML Form URL Encoded: application/x-www-form-urlencoded。

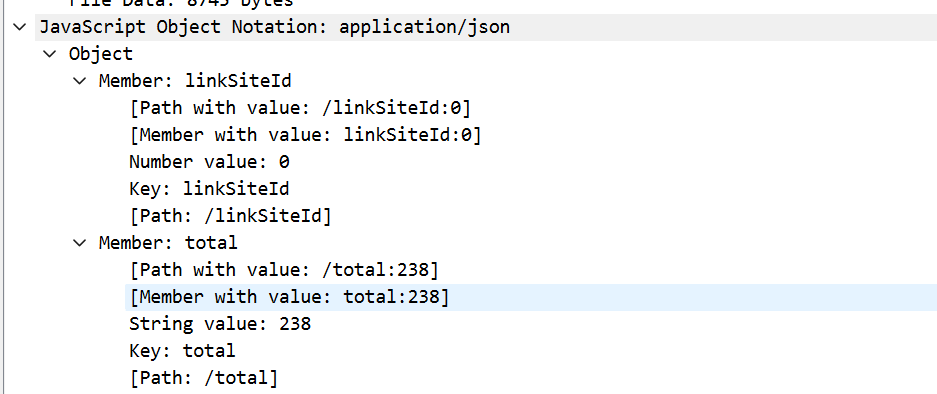
内容类型——Content-Type: application/x-www-form-urlencoded\r\n

在第二个POST中：SearchInfo是json字符串



同时，有encoded字样，应该是加密过后。

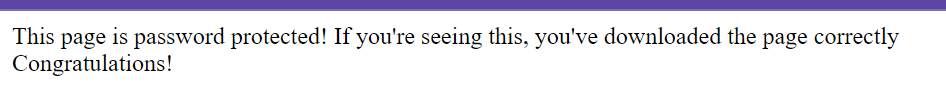
在响应的详细信息中，可以看到传回来多少检索结果：238



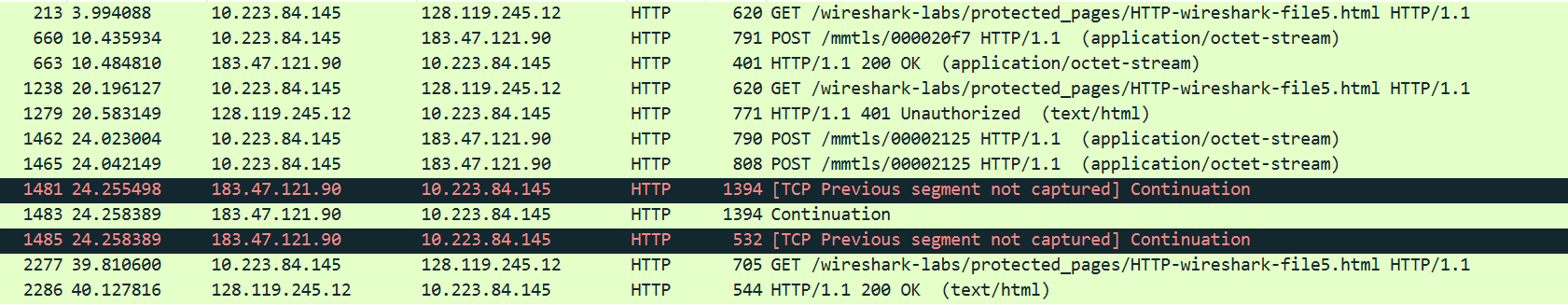
检查后发现确实：



以下问题的现象可能会受浏览器缓存影响，如果你第一次访问指定网页时操作失误，请关闭该网页、清除浏览器缓存后再重新操作。重新开启分组捕获，访问 http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html ，输入用户名 wireshark-students，密码 network



抓到的信息如下：



1. 在抓取的分组中找到输入的用户名和密码（提示：传输使用了base64编码）。将地址中

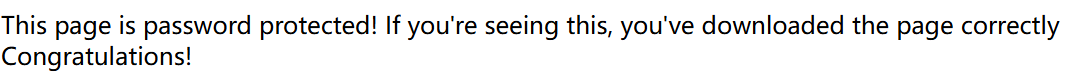
的http改为https（https://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTPwireshark-file5.html），还能否通过捕获分组获得密码？

在分组详细信息里面可以直接找到credential的信息：

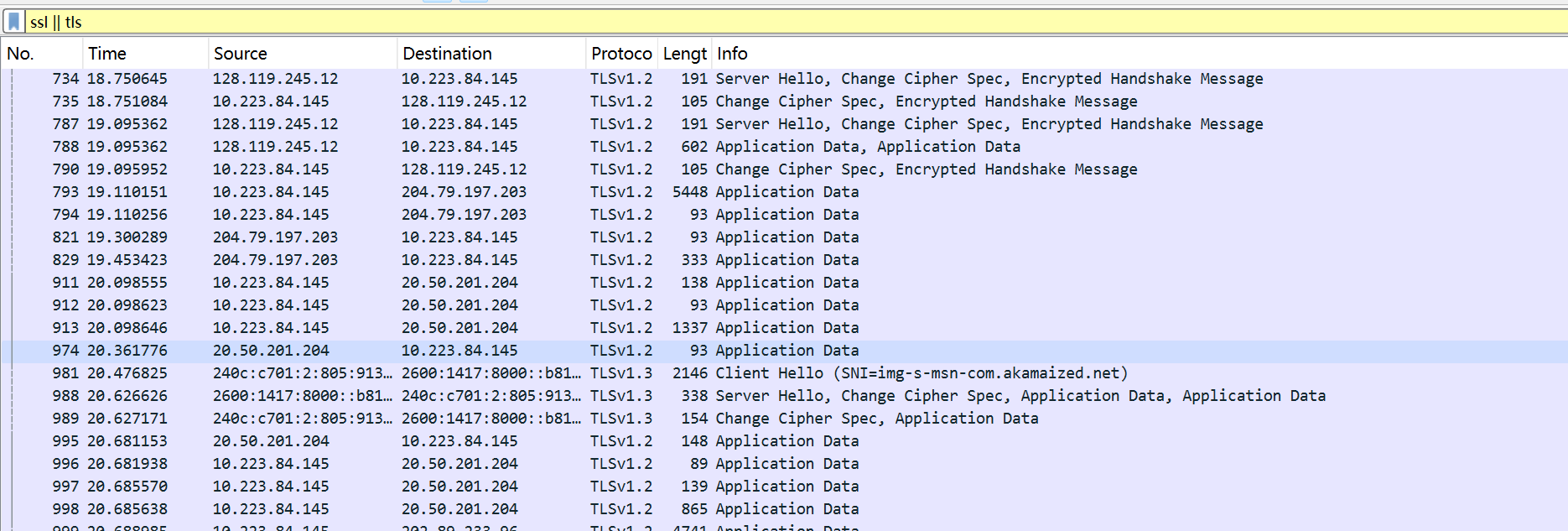


完全没有加密，wireshark-students : network 账号密码都直接显示了

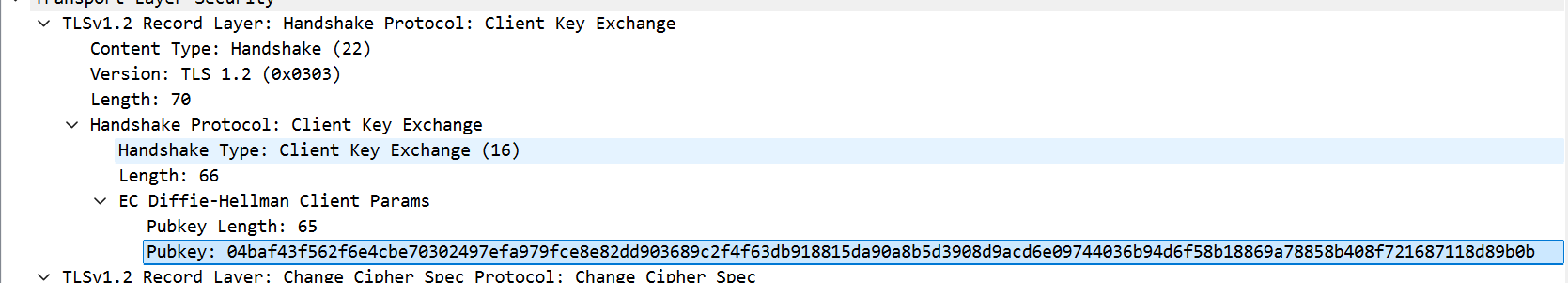
在使用https登录后：



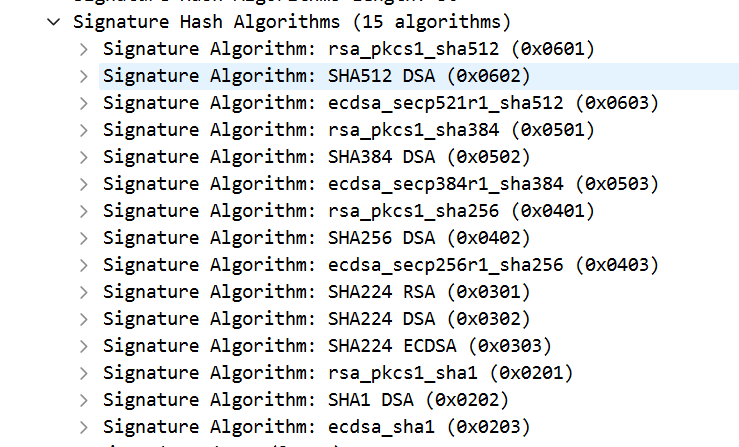
没有http的item。首先通过查询资料了解道https通常使用ssl或tls加密信息，因此应该无法直接获取账号密码，首先先找一下加密信息——



发现能获得加密的公钥：（在client key exchange中，在握手过程之后，即会话密钥协商阶段）



也可以看到加密算法：



在application data中，可以看到客户端和服务器之间传输的加密后的数据：例如：

