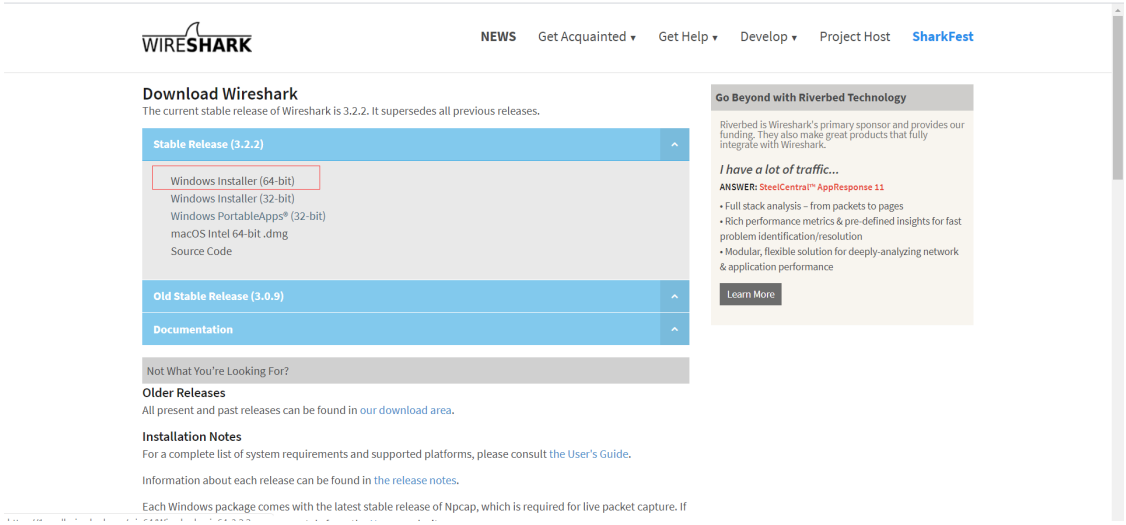
信息安全原理HW4

姓名：王祚滨　**学号**：3180104933

实验过程：

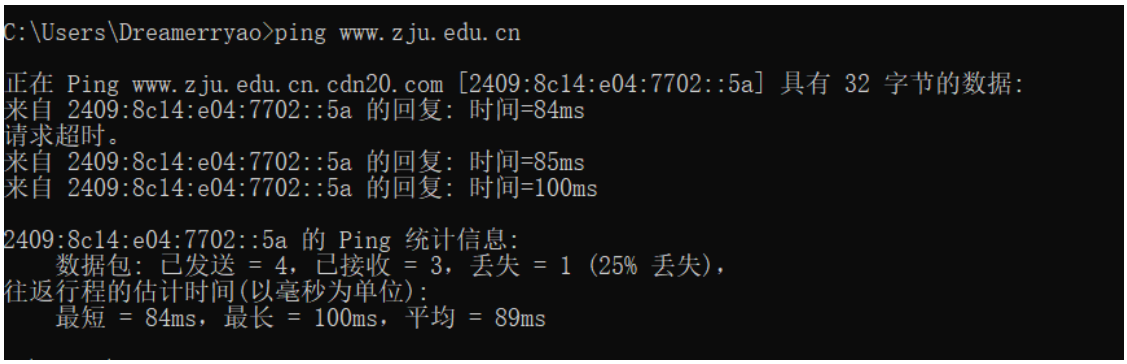
1. download **Wireshark**



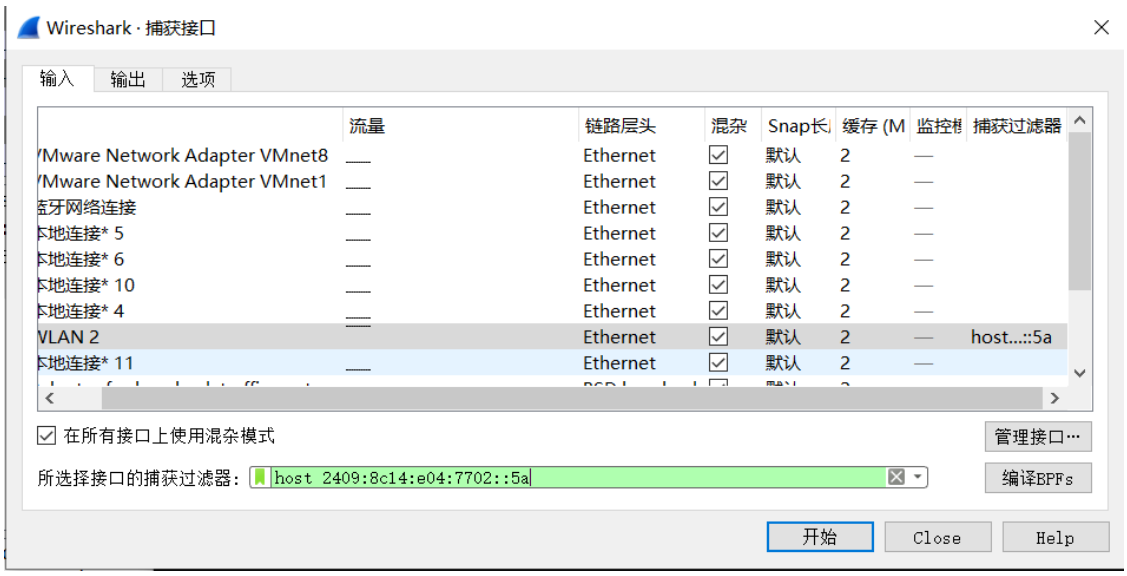
2. 重启网卡服务，防止其他因素干扰

   在cmd中键入命令 net start npf

3. 获取目标网站服务器

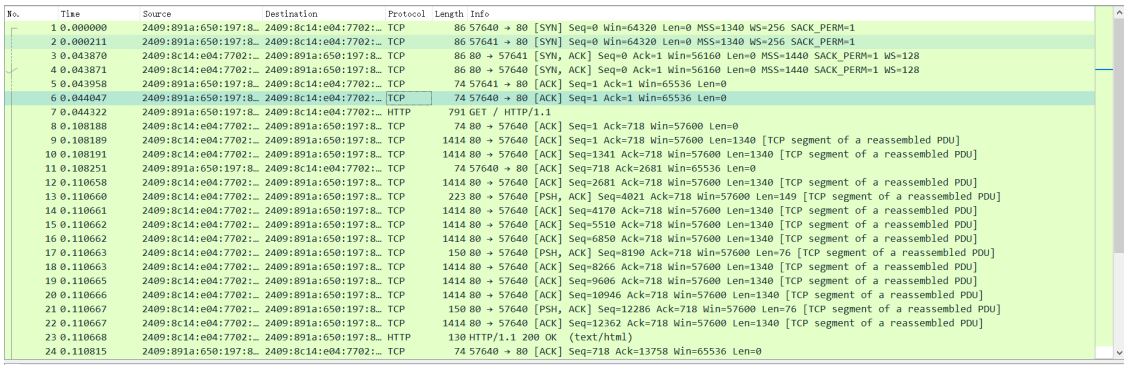


4. 配置wireshark，点击“捕获”，“选项”，设置filter为host 2409:8c14:e04:7702::5a



5. 点击“开始”，开始抓包。

6. 导出抓包的结果，其部分结果为

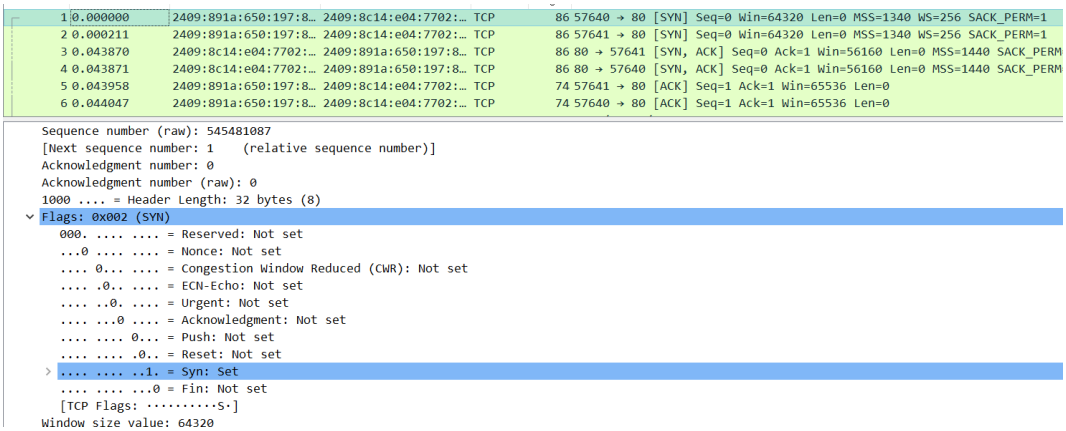


7. 对抓到的包进行分析

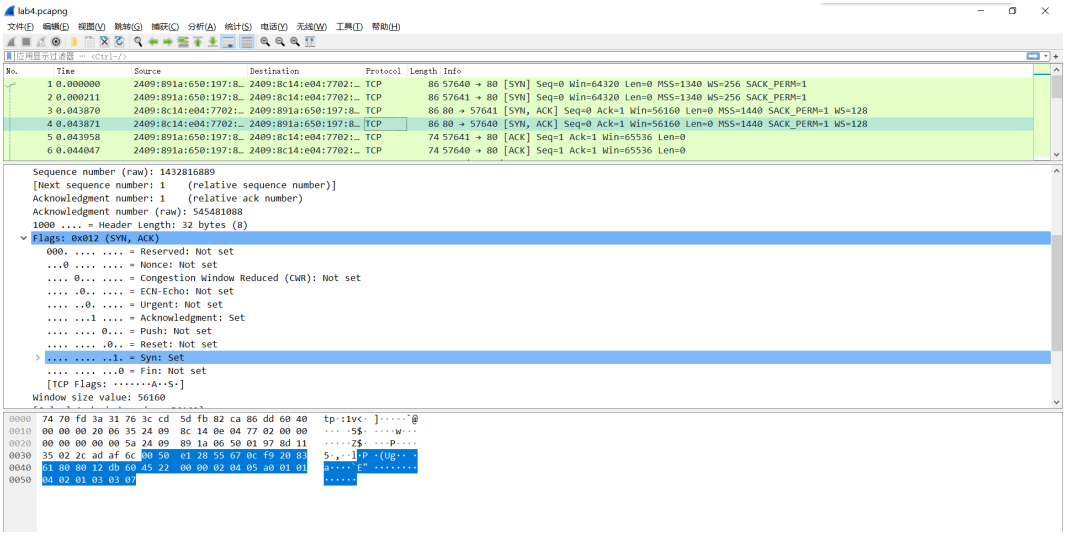
    1. 三次握手建立TCP

        可以看到，与本机57640端口和57641端口都建立了连接，以57640端口说明

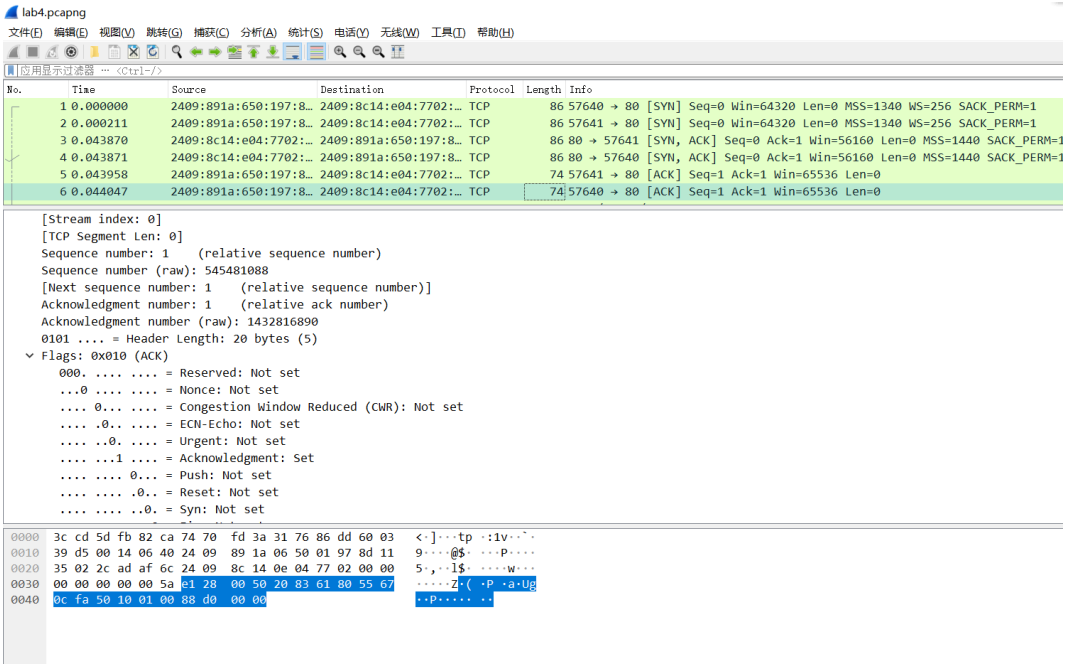
        首先， 本机向目标服务器发送同步请求,将获得包括 Src，Dst，Port 等信息， 并将其中 Flags 字段的 Syn 位置为 Set



        随后，目标服务器向本机回复一个 ACK 包，其中 Flag 字段的 Syn 和 Acknowledgment 字段置为 Set



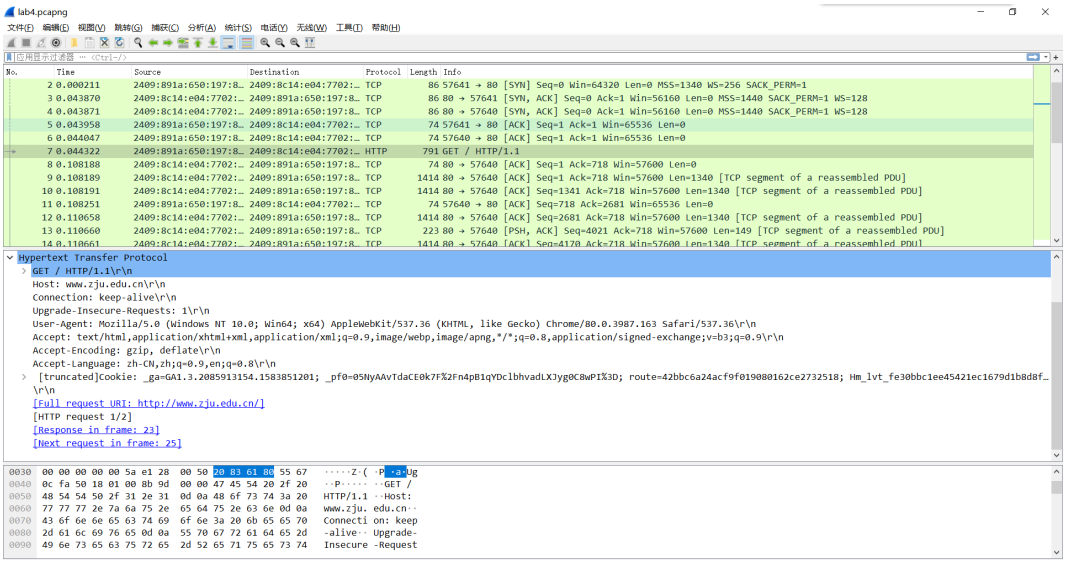
最后进行第三次握手，本机向目标服务器发送一个ACK 包，其中 Flag 字段的 Acknowledgment 字段置为 Set ，至此，成功连接



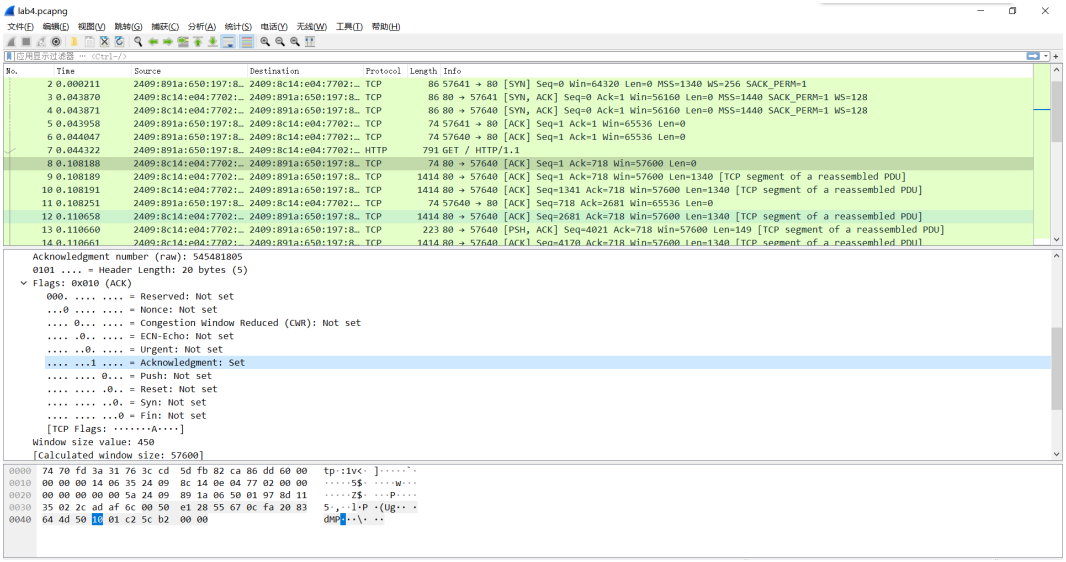
2. HTTP请求

本机发出 HTTP 请求之后，目标服务器收到请求发送 ACK

本机发出HTTP GET请求

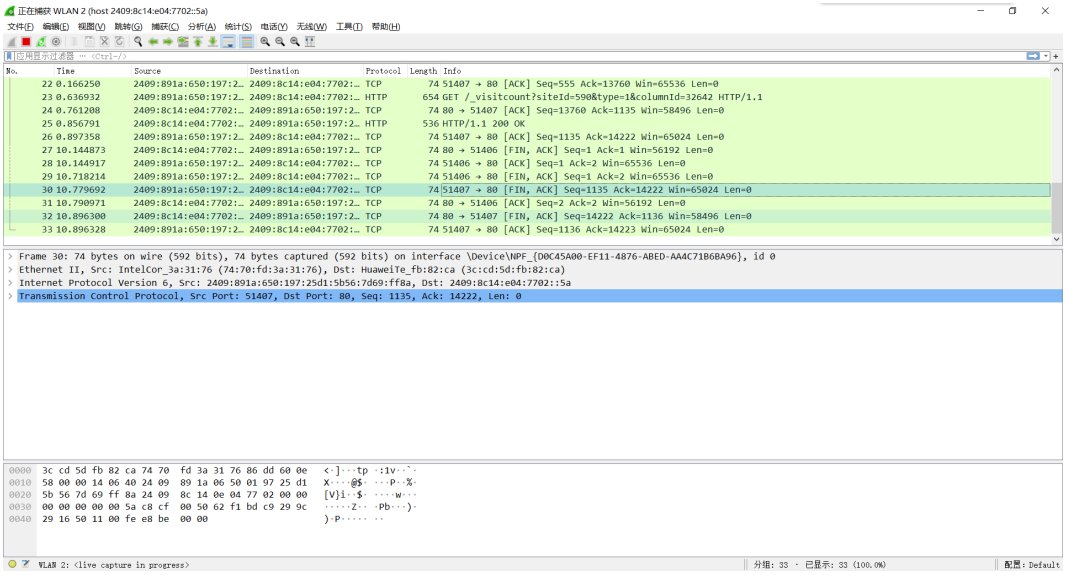


目标服务器收到请求，回ACK包

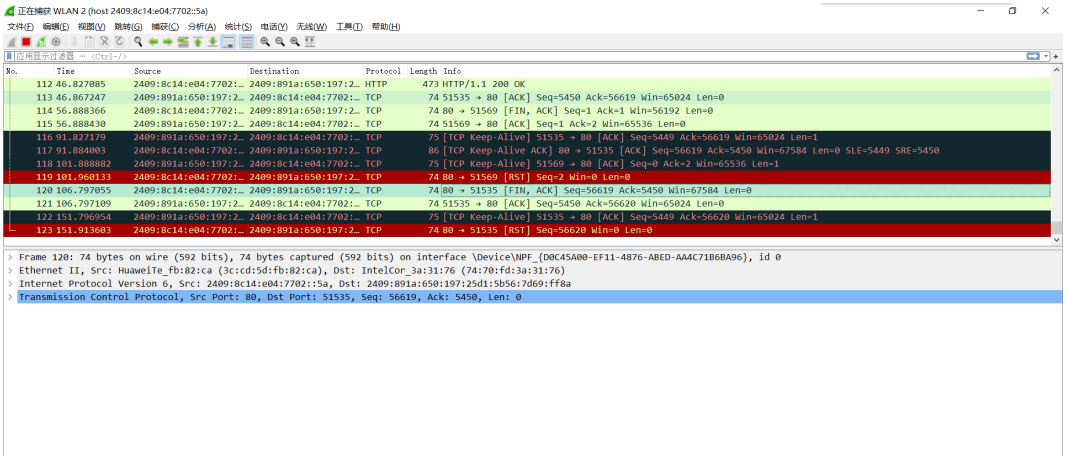


3. 完成HTTP过程，断开TCP连接

1.手动断开：可以看到27-33行，51407.51406两个端口断开连接



2.等待一段时间，可以发现目标服务器会发送RST包断开连接

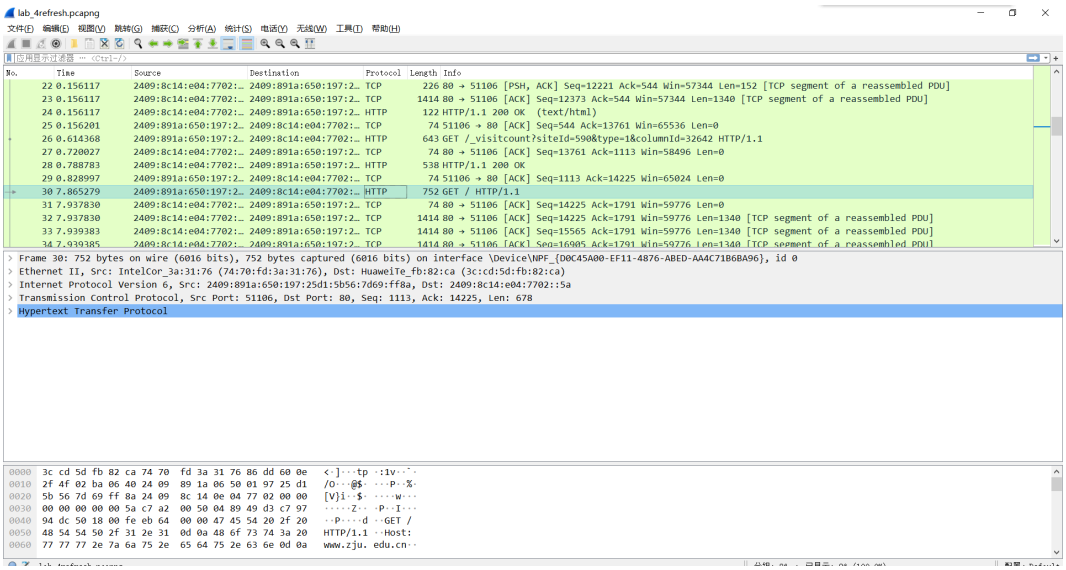


8. 附1：删除缓存重新渲染(对应pcapng为lab4_重新渲染.pcapng)

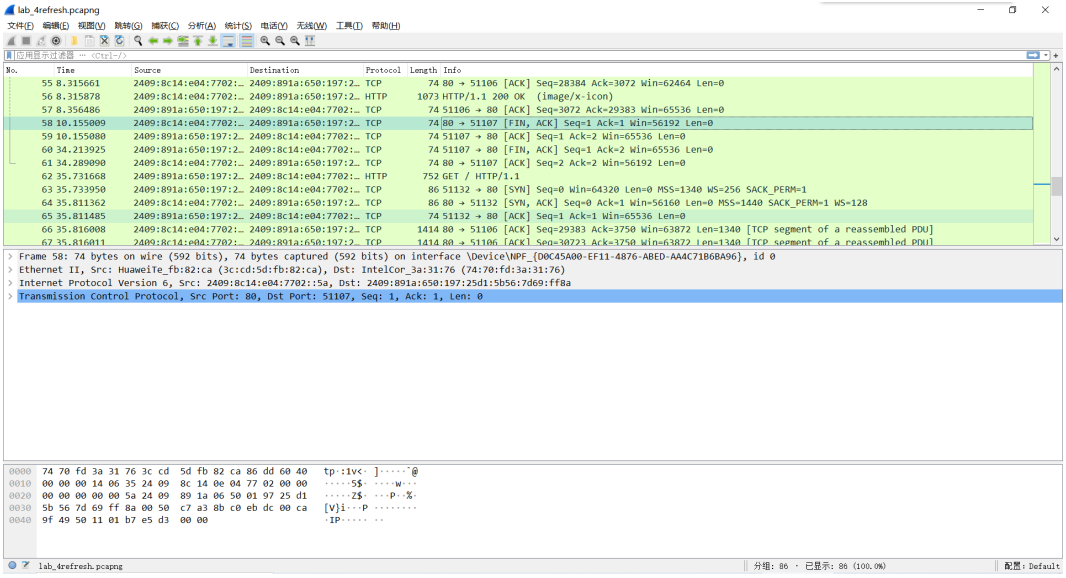
    1. 可以看到，包的数量显著增加，其中HTTP包数量明显增多，从目标服务器获取对应图片等信息，渲染整个界面

9. 附2：刷新界面以及重新输入网址(对应pcapng为lab_4refresh.pcapng)

1. 可以看到，点击刷新，并不会重新建立TCP，直接开始HTTP请求



2. 而输入网址重新渲染，则会将本机其中一个端口断开连接，下面例子为51107端口，并与一个新的端口建立连接，下面例子为51132端口



3. 如果在打开一个网址的时候新建一个页面进入相同网址，可以看到line48所示，没有预想中新端口的建立，而是直接从HTTP请求开始