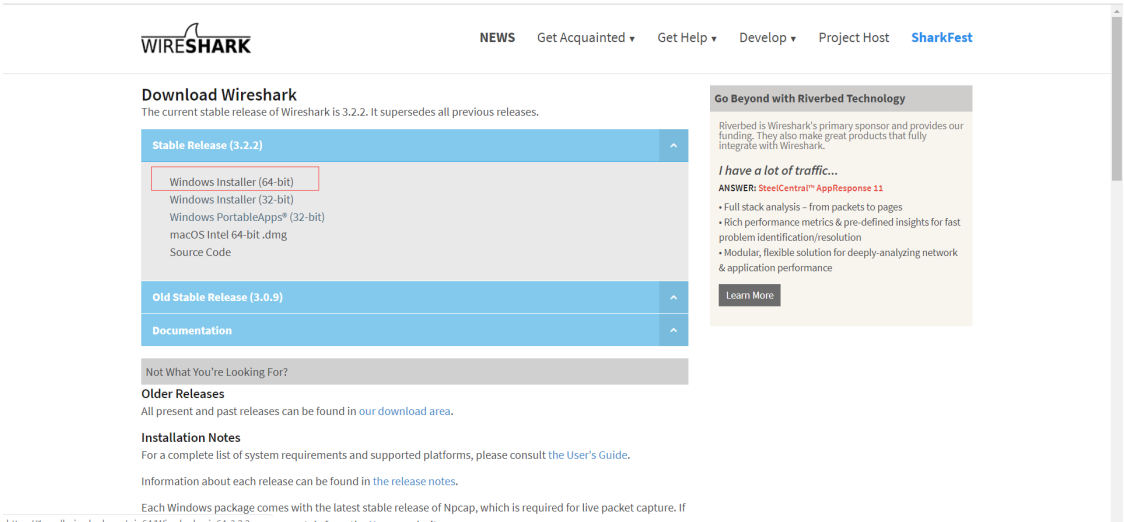


信息安全原理HW4

姓名：王祚滨 学号：3180104933

实验过程：

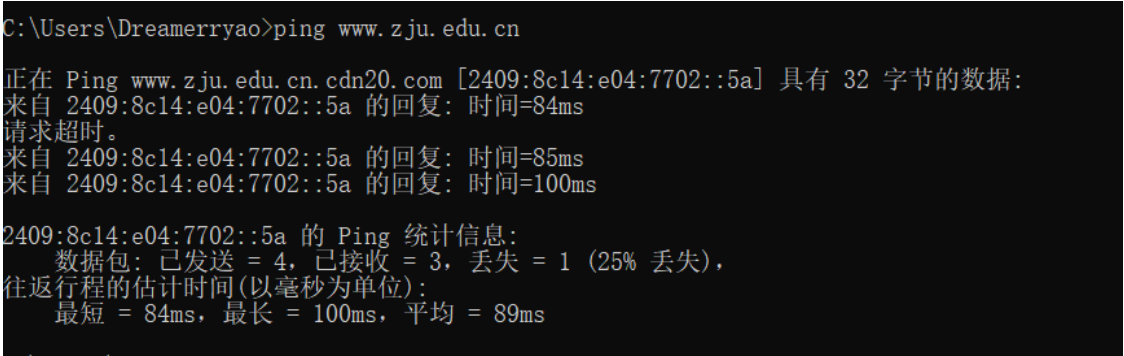
1. download Wireshark



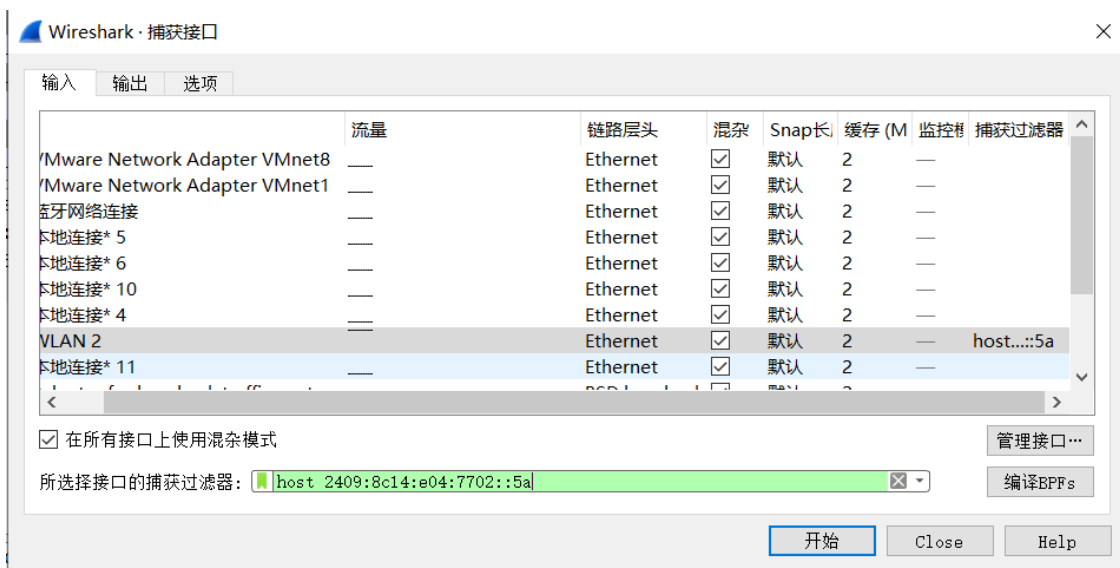
2. 重启网卡服务，防止其他因素干扰

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	86	57640 → 80 [SYN] Seq=0 Win=64320 Len=0 MSS=1340 WS=256 SACK_PERM=1
2	0.000211	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	86	57641 → 80 [SYN] Seq=0 Win=64320 Len=0 MSS=1340 WS=256 SACK_PERM=1
3	0.043870	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	86	80 → 57641 [SYN, ACK] Seq=0 Ack=1 Win=56160 Len=0 MSS=1440 SACK_PERM=1 WS=128
4	0.043871	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	86	80 → 57640 [SYN, ACK] Seq=0 Ack=1 Win=56160 Len=0 MSS=1440 SACK_PERM=1 WS=128
5	0.043958	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	74	57641 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.044047	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	74	57640 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
7	0.044322	2409:891a:650:197:8...	2409:8c14:e04:7702:...	HTTP	791	GET / HTTP/1.1
8	0.108188	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	74	80 → 57640 [ACK] Seq=1 Ack=718 Win=57600 Len=0
9	0.108189	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=1 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
10	0.108191	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=1341 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
11	0.108251	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	74	57640 → 80 [ACK] Seq=718 Ack=2681 Win=65536 Len=0
12	0.110658	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=2681 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
13	0.110660	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	223	80 → 57640 [PSH, ACK] Seq=4021 Ack=718 Win=57600 Len=149 [TCP segment of a reassembled PDU]
14	0.110661	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=4178 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
15	0.110662	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=5510 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
16	0.110662	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=6850 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
17	0.110663	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	150	80 → 57640 [PSH, ACK] Seq=8190 Ack=718 Win=57600 Len=76 [TCP segment of a reassembled PDU]
18	0.110663	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=8266 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
19	0.110665	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=9606 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
20	0.110666	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=10946 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
21	0.110667	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	150	80 → 57640 [PSH, ACK] Seq=12286 Ack=718 Win=57600 Len=76 [TCP segment of a reassembled PDU]
22	0.110667	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	1414	80 → 57640 [ACK] Seq=12362 Ack=718 Win=57600 Len=1340 [TCP segment of a reassembled PDU]
23	0.110668	2409:8c14:e04:7702:...	2409:891a:650:197:8...	HTTP	130	HTTP/1.1 200 OK (text/html)
24	0.110815	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	74	57640 → 80 [ACK] Seq=718 Ack=13758 Win=65536 Len=0

7. 对抓到的包进行分析

1. 三次握手建立TCP

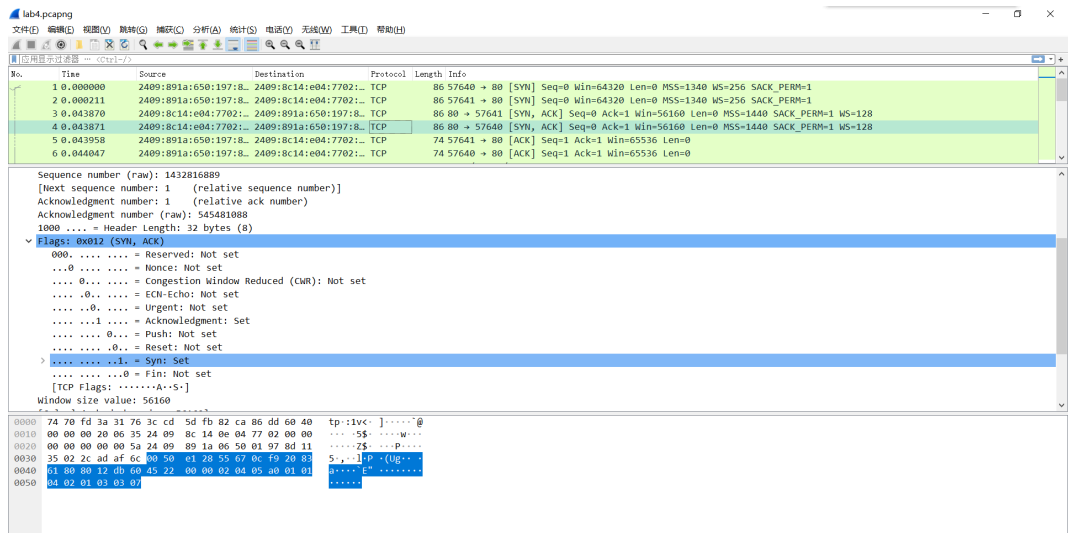
可以看到，与本机57640端口和57641端口都建立了连接，以57640端口说明

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

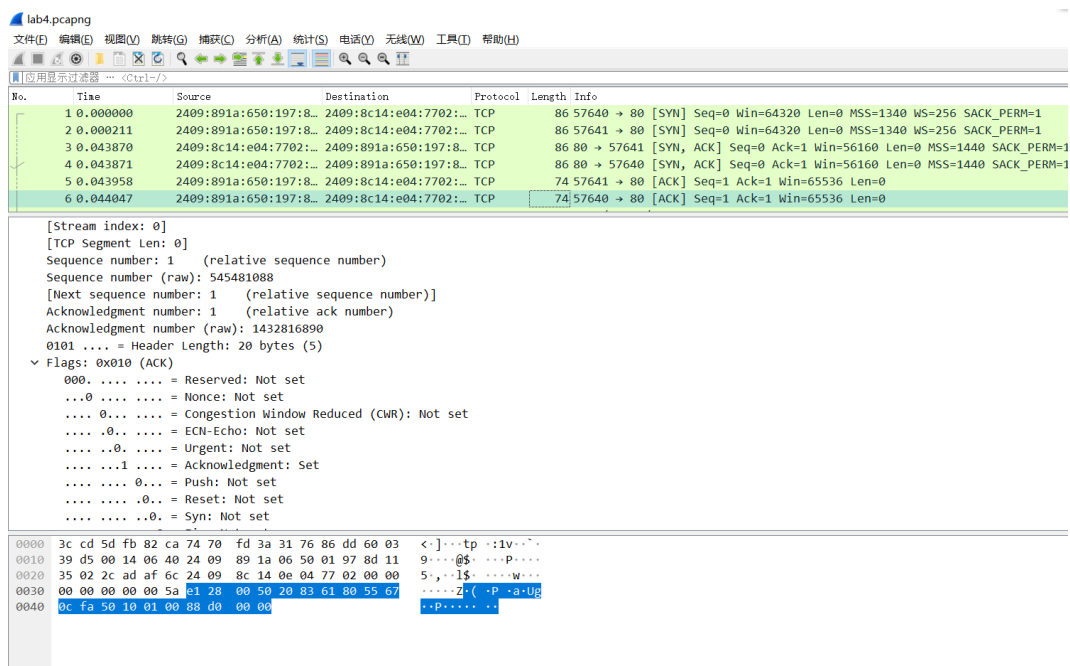
1	0.000000	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	86	57640 → 80 [SYN] Seq=0 Win=64320 Len=0 MSS=1340 WS=256 SACK_PERM=1
2	0.000211	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	86	57641 → 80 [SYN] Seq=0 Win=64320 Len=0 MSS=1340 WS=256 SACK_PERM=1
3	0.043870	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	86	80 → 57641 [SYN, ACK] Seq=0 Ack=1 Win=56160 Len=0 MSS=1440 SACK_PERM=1
4	0.043871	2409:8c14:e04:7702:...	2409:891a:650:197:8...	TCP	86	80 → 57640 [SYN, ACK] Seq=0 Ack=1 Win=56160 Len=0 MSS=1440 SACK_PERM=1
5	0.043958	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	74	57641 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.044047	2409:891a:650:197:8...	2409:8c14:e04:7702:...	TCP	74	57640 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0

Sequence number (raw): 545481087	
[Next sequence number: 1 (relative sequence number)]	
Acknowledgment number: 0	
Acknowledgment number (raw): 0	
1000 ... = Header Length: 32 bytes (8)	
Flags: 0x002 (SYN)	
000.	Reserved: Not set
...0.	Nonce: Not set
...0.	Congestion Window Reduced (CWR): Not set
...0.	ECN-Echo: Not set
...0.	Urgent: Not set
...0.	Acknowledgment: Not set
...0.	Push: Not set
...0.	Reset: Not set
>... ..1.	Syn: Set
... ..0.	Fin: Not set
[TCP Flags:S.]	
Window size value: 64320	

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



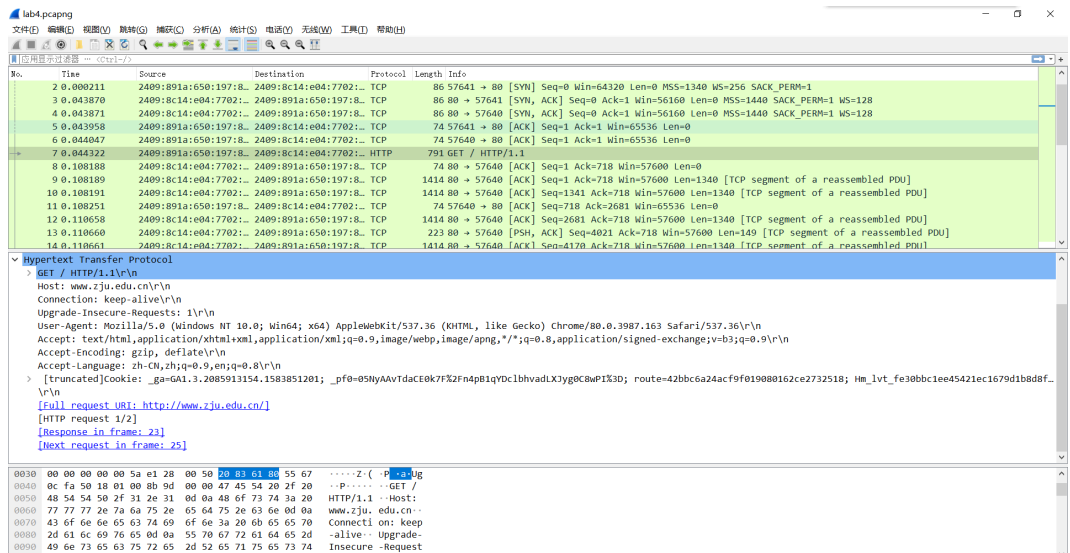
最后进行第三次握手，本机向目标服务器发送一个ACK包，其中 Flag 字段的 Acknowledgment 字段置为 Set，至此，成功连接



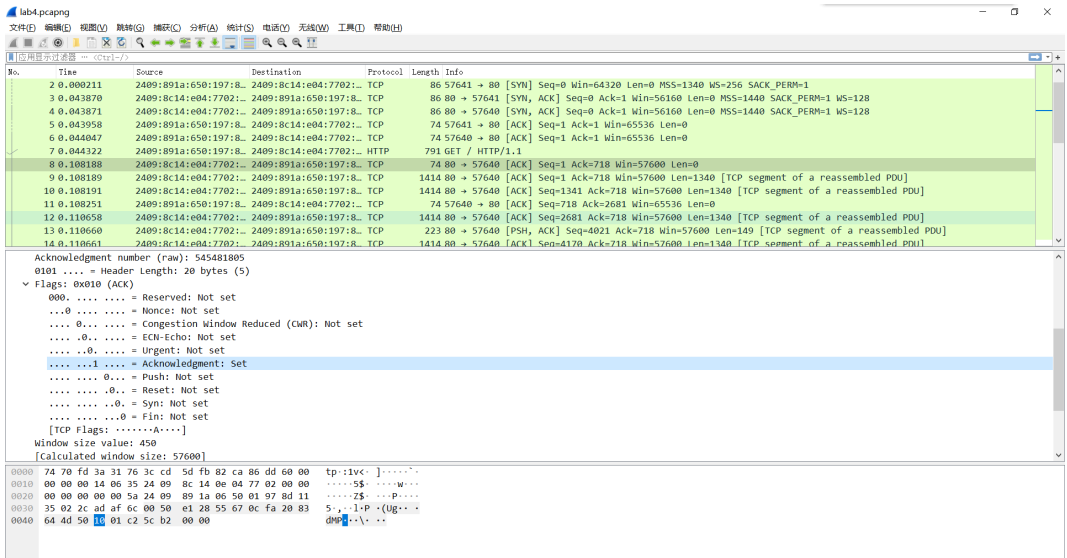
2. HTTP请求

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

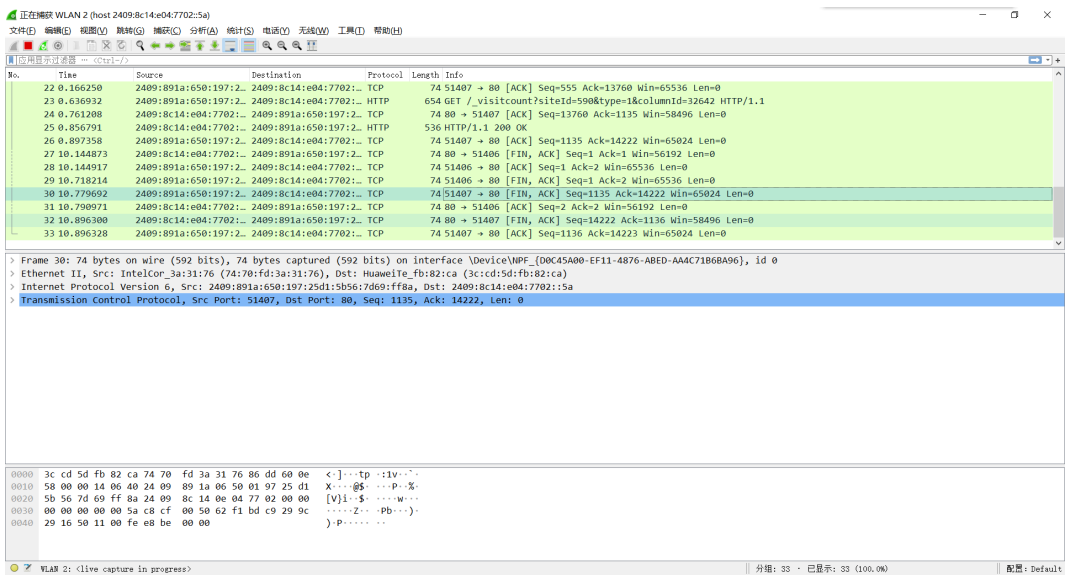


目标服务器收到请求，回ACK包

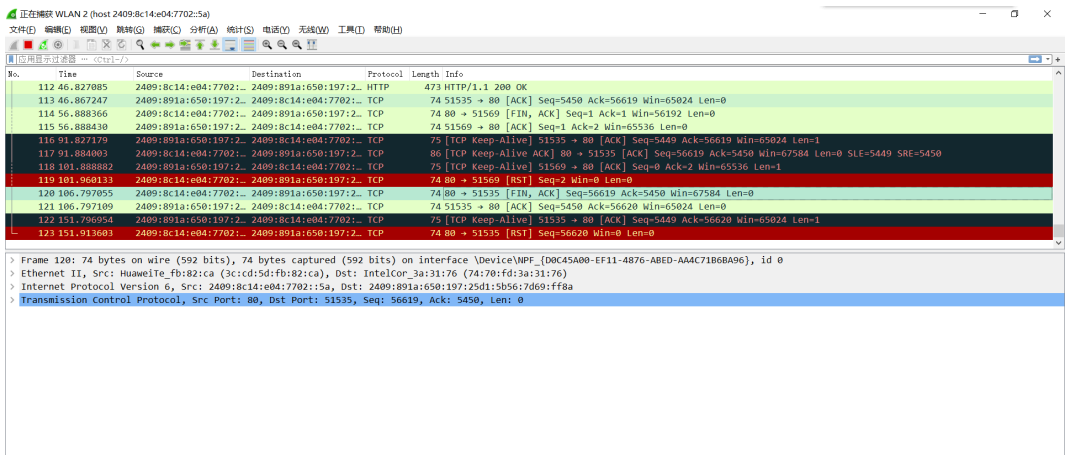


3. 完成HTTP过程，断开TCP连接

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

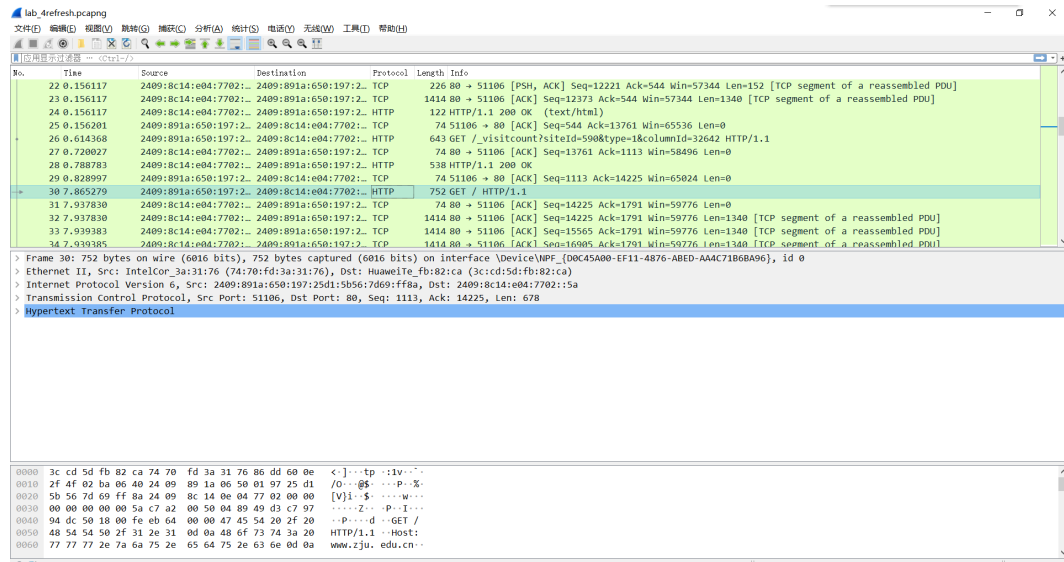


8. 附1：删除缓存重新渲染(对应pcapng为lab4_重新渲染.pcapng)

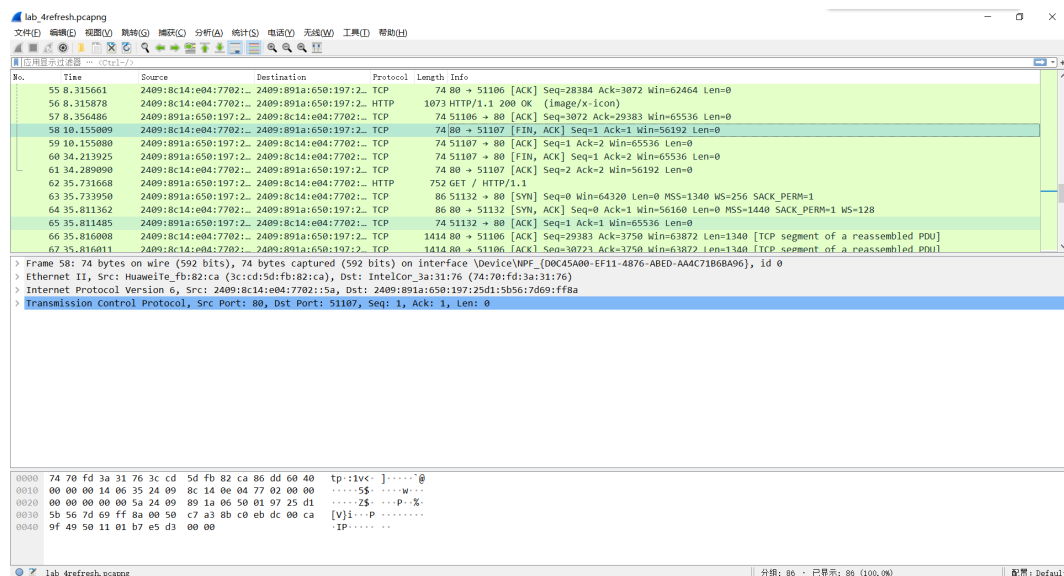
1. 可以看到，包的数量显著增加，其中HTTP包数量明显增多，从目标服务器获取对应图片等信息，渲染整个界面

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

