信息安全原理 HW4

> 姓名：王晨雨
>
> 学号：3200102324

实验过程：

1. 清除浏览器缓存：

2. 重启网卡服务

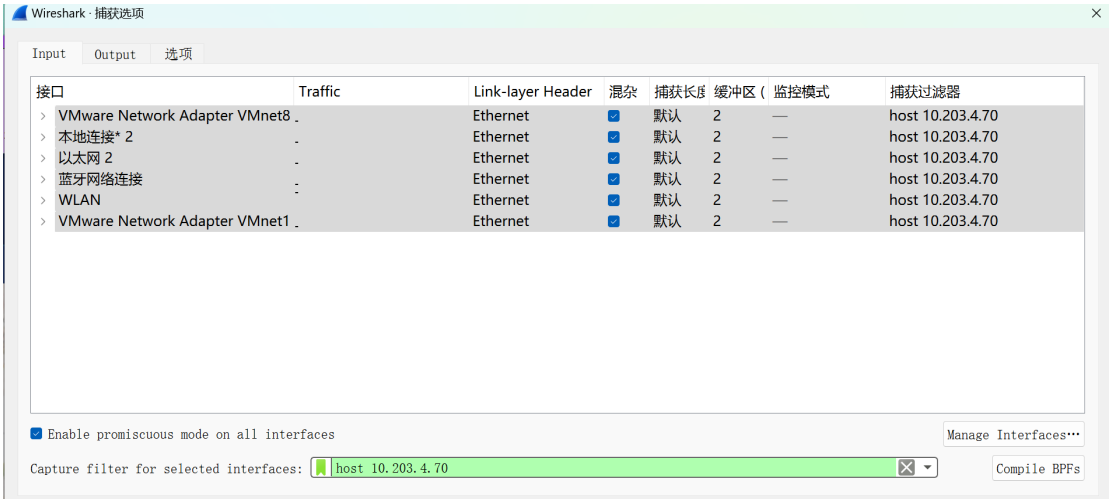
```
C:\Windows\System32>net start npf
请求的服务已经启动。

请键入 NET HELPMSG 2182 以获得更多的帮助。
```

3. 获取目标网站服务器

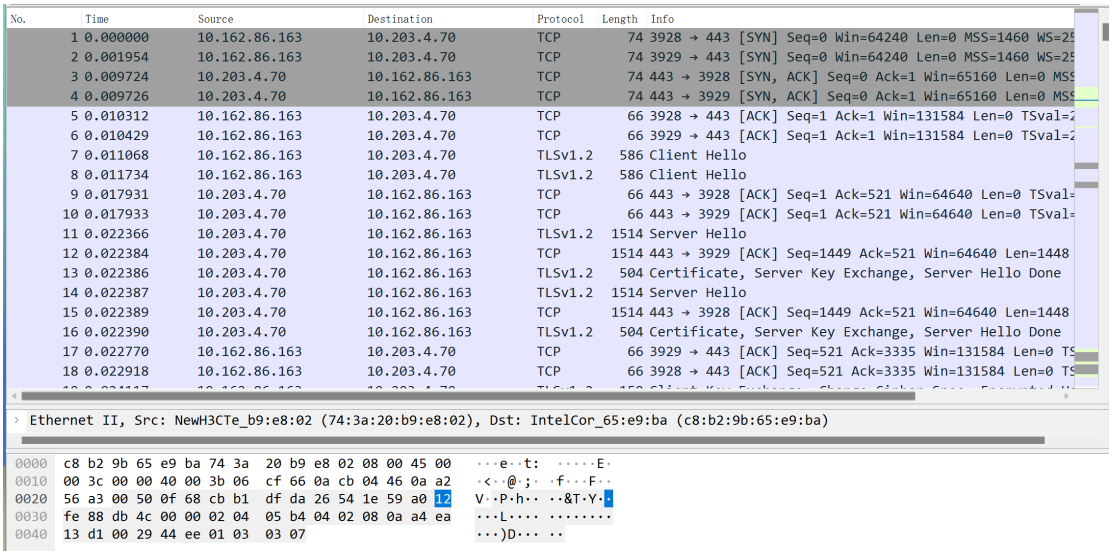
```
C:\Windows\System32>ping www.zju.edu.cn

正在 Ping www.zju.edu.cn [10.203.4.70] 具有 32 字节的数据:
来自 10.203.4.70 的回复: 字节=32 时间=22ms TTL=59
来自 10.203.4.70 的回复: 字节=32 时间=14ms TTL=59
来自 10.203.4.70 的回复: 字节=32 时间=16ms TTL=59
来自 10.203.4.70 的回复: 字节=32 时间=16ms TTL=59

10.203.4.70 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 14ms, 最长 = 22ms, 平均 = 17ms
```

4. 配置wireshark

   配置filter:



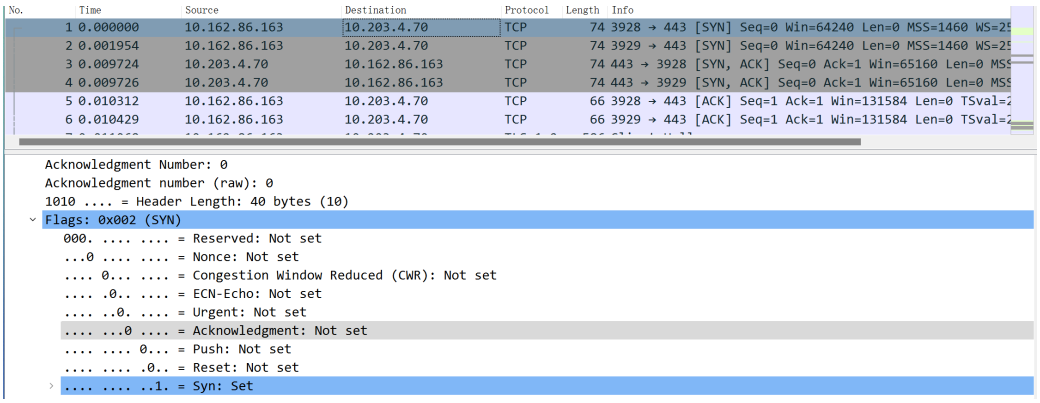
5. 开始抓包:



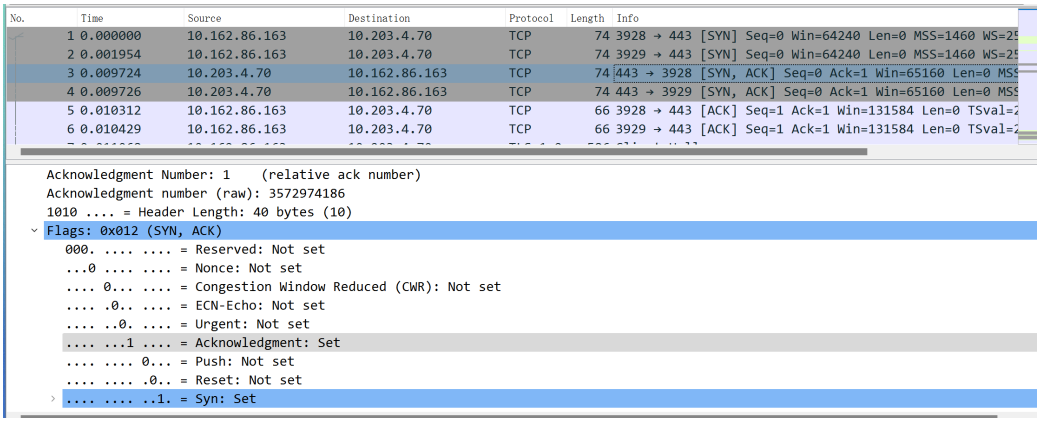
6. 分析抓包结果:

   1. TCP三次握手协议:

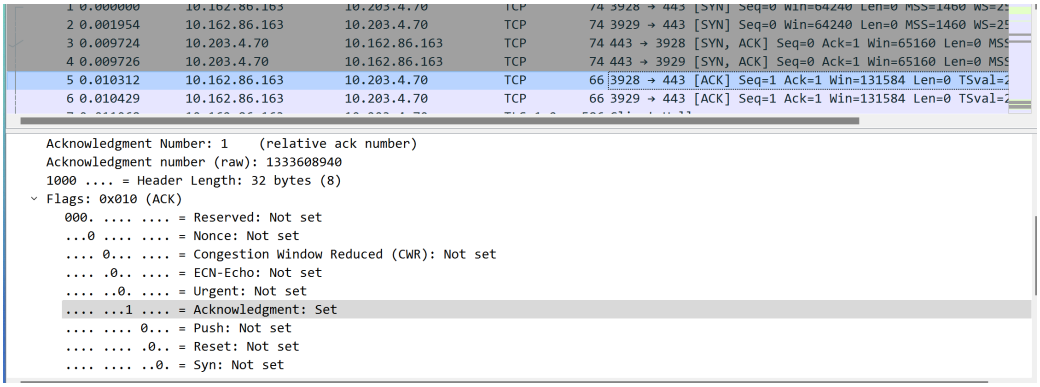
      本机向目标服务器发送同步请求，将Flags字段的Sym设置为Set



目标服务器向本机回复一个ACK包，其中Syn和Acknowledgment都为Set

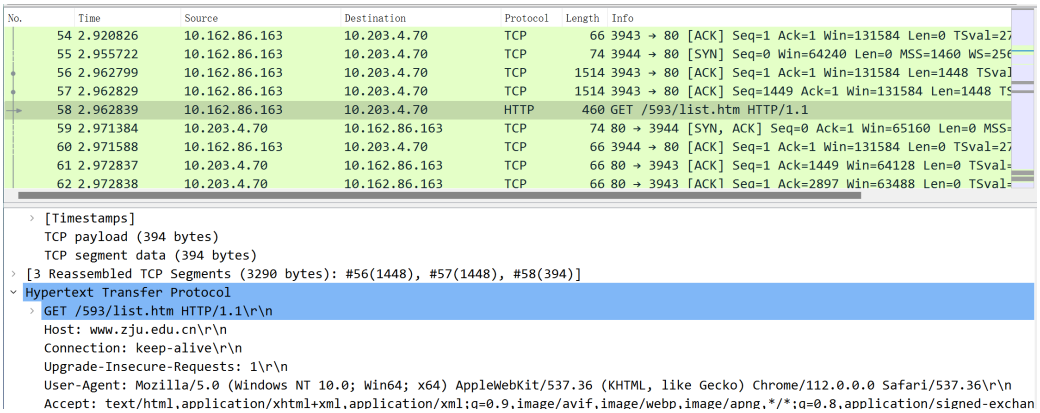


最后，本机向目标服务器发送一个ACK包，Flag和ACknowledgment设置为Set。成功连接。

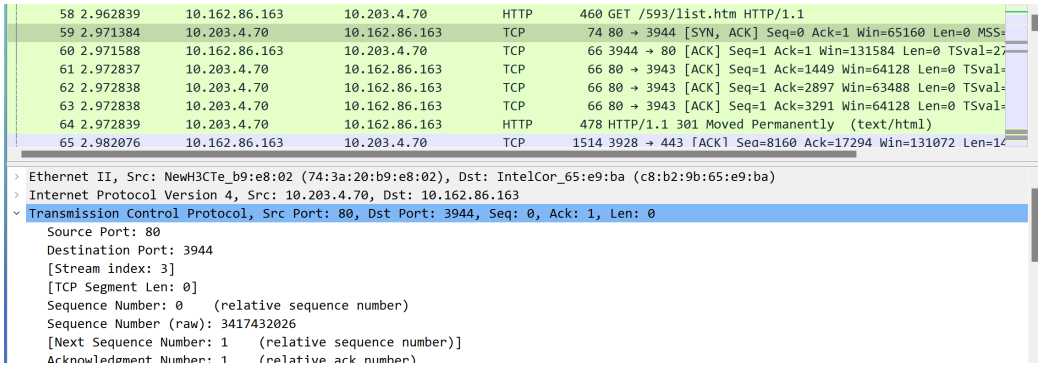


2. HTTP请求

`GET` 请求



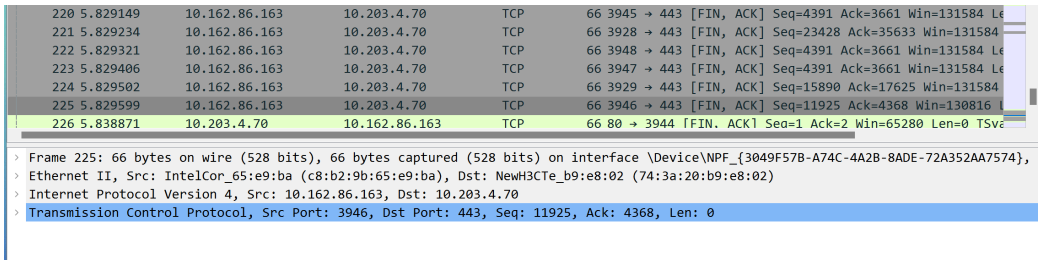
目标服务器返回ACK：



```
    58 2.962839    10.162.86.163    10.203.4.70      HTTP     460 GET /593/list.htm HTTP/1.1
    59 2.971384    10.203.4.70      10.162.86.163    TCP       74 80 → 3944 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
    60 2.971588    10.162.86.163    10.203.4.70      TCP       66 3944 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=27
    61 2.972837    10.203.4.70      10.162.86.163    TCP       66 80 → 3943 [ACK] Seq=1 Ack=1449 Win=64128 Len=0 TSval=
    62 2.972838    10.203.4.70      10.162.86.163    TCP       66 80 → 3943 [ACK] Seq=1 Ack=2897 Win=63488 Len=0 TSval=
    63 2.972838    10.203.4.70      10.162.86.163    TCP       66 80 → 3943 [ACK] Seq=1 Ack=3291 Win=64128 Len=0 TSval=
    64 2.972839    10.203.4.70      10.162.86.163    HTTP     478 HTTP/1.1 301 Moved Permanently  (text/html)
    65 2.982076    10.162.86.163    10.203.4.70      TCP     1514 3928 → 443 [ACK] Seq=8160 Ack=17294 Win=131072 Len=14
```

```
> Ethernet II, Src: NewH3CTe_b9:e8:02 (74:3a:20:b9:e8:02), Dst: IntelCor_65:e9:ba (c8:b2:9b:65:e9:ba)
> Internet Protocol Version 4, Src: 10.203.4.70, Dst: 10.162.86.163
v Transmission Control Protocol, Src Port: 80, Dst Port: 3944, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 3944
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3417432026
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
```

3. 断开TCP



```
   220 5.829149    10.162.86.163    10.203.4.70      TCP       66 3945 → 443 [FIN, ACK] Seq=4391 Ack=3661 Win=131584 Le
   221 5.829234    10.162.86.163    10.203.4.70      TCP       66 3928 → 443 [FIN, ACK] Seq=23428 Ack=35633 Win=131584
   222 5.829321    10.162.86.163    10.203.4.70      TCP       66 3948 → 443 [FIN, ACK] Seq=4391 Ack=3661 Win=131584 Le
   223 5.829406    10.162.86.163    10.203.4.70      TCP       66 3947 → 443 [FIN, ACK] Seq=4391 Ack=3661 Win=131584 Le
   224 5.829502    10.162.86.163    10.203.4.70      TCP       66 3929 → 443 [FIN, ACK] Seq=15890 Ack=17625 Win=131584
   225 5.829599    10.162.86.163    10.203.4.70      TCP       66 3946 → 443 [FIN, ACK] Seq=11925 Ack=4368 Win=130816 L
   226 5.838871    10.203.4.70      10.162.86.163    TCP       66 80 → 3944 [FIN, ACK] Seq=1 Ack=2 Win=65280 Len=0 TSva
```

```
> Frame 225: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{3049F57B-A74C-4A2B-8ADE-72A352AA7574},
> Ethernet II, Src: IntelCor_65:e9:ba (c8:b2:9b:65:e9:ba), Dst: NewH3CTe_b9:e8:02 (74:3a:20:b9:e8:02)
> Internet Protocol Version 4, Src: 10.162.86.163, Dst: 10.203.4.70
> Transmission Control Protocol, Src Port: 3946, Dst Port: 443, Seq: 11925, Ack: 4368, Len: 0
```