

## HW4:Using Wireshark

### 一、获取抓包网站的 IP 地址

```
命令提示符
Microsoft Windows [版本 10.0.22000.1696]
(c) Microsoft Corporation。保留所有权利。

C:\Users\ll>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=7ms TTL=62
来自 10.203.4.70 的回复: 字节=32 时间=6ms TTL=62
来自 10.203.4.70 的回复: 字节=32 时间=8ms TTL=62
来自 10.203.4.70 的回复: 字节=32 时间=7ms TTL=62

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 = 6ms, 最长 = 8ms, 平均 = 7ms

C:\Users\ll>
```

### 二、清楚浏览器缓存

#### 清除浏览数据

时间范围

所有时间

#### ☒ 浏览历史记录

已同步设备上有 1 个及更多项目。请从已登录且正在同步的所有设备中清除历史记录。

#### ☒ 下载历史记录

无

#### ☒ Cookie 和其他站点数据

来自 11 个站点。使你从大多数站点退出登录。

#### ☒ 缓存的图像和文件

释放的空间小于 63.6 MB。你下次访问时，有些网站的加

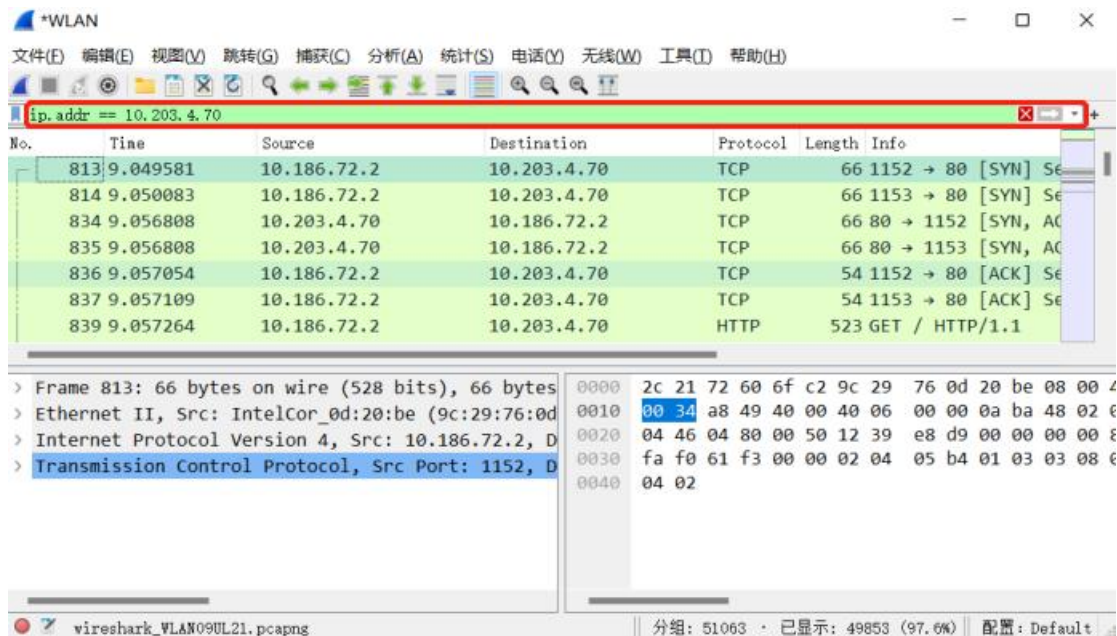
这将清除使用 2438452556@qq.com 登录到的所有同步设备上的数据。若仅希望清除此设备中的浏览数据，请 [先退出登录](#)。

立即清除

取消

### 三、设置显示过滤器

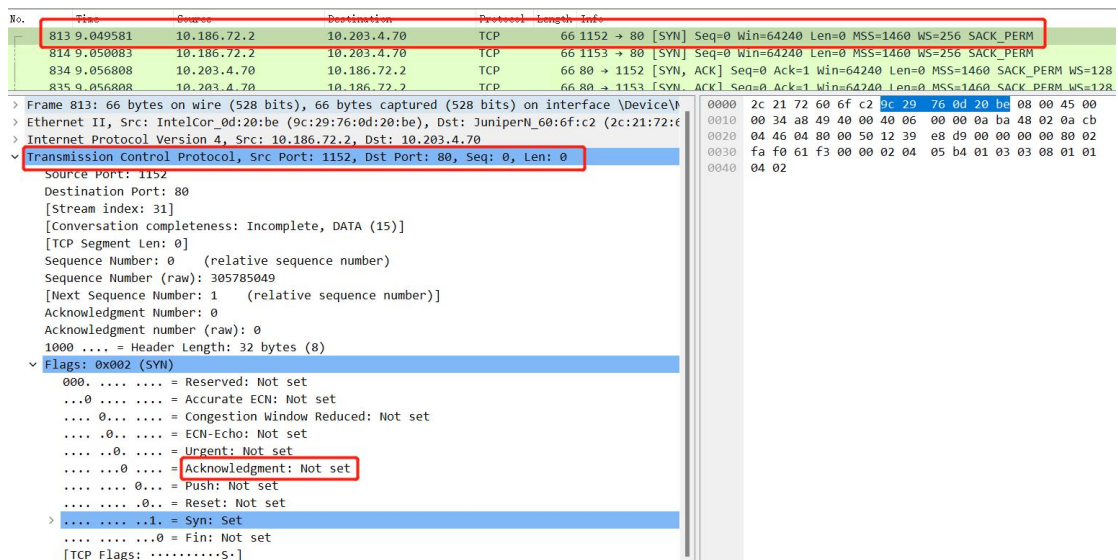
在红框内输入 `ip.addr == 10.203.4.70`，使抓取的包只和 `www.zju.edu.cn` 有关



### 四、数据分析

#### 1、TCP 的建立（三次握手协议）

**阶段一：**客户端给服务器发送一个 SYN 段(在 TCP 标头中 SYN 位字段为 1 的 TCP/IP 数据包), 该段中也包含客户端的初始序列号, 同时, 该阶段的 ACK 为 Not set 状态, SYN 为 set 状态。



The image shows a Wireshark packet capture of a SYN flood attack. The packet list on the left shows several SYN packets from 10.203.4.70 to 10.186.72.2. The packet details for packet 834 show a SYN flag and a sequence number of 0. The packet bytes show the raw data of the SYN packet.

No.	Time	Source	Destination	Protocol	Length	Info
813	9.049581	10.186.72.2	10.203.4.70	TCP	66	1152 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
814	9.050803	10.186.72.2	10.203.4.70	TCP	66	1153 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
834	9.056808	10.203.4.70	10.186.72.2	TCP	66	80 → 1152 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
835	9.056888	10.203.4.70	10.186.72.2	TCP	66	80 → 1153 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128

Packet 834 details:

- Frame 834: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF{...}
- Ethernet II, Src: JuniperN\_60:6f:c2 (2c:21:72:60:6f:c2), Dst: IntelCor\_0d:20:be (9c:29:76:c0:00:00)
- Internet Protocol Version 4, Src: 10.203.4.70, Dst: 10.186.72.2
- Transmission Control Protocol, Src Port: 80, Dst Port: 1152, Seq: 0, Ack: 1, Len: 0
  - Source Port: 80
  - Destination Port: 1152
  - [Stream index: 31]
  - [Conversation completeness: Incomplete, DATA (15)]
  - [TCP Segment Len: 0]
  - Sequence Number: 0 (relative sequence number)
  - Sequence Number (raw): 1343752443
  - [Next Sequence Number: 1 (relative sequence number)]
  - Acknowledgment Number: 1 (relative ack number)
  - Acknowledgment number (raw): 305785050
  - 1000 .... = Header Length: 32 bytes (8)
  - Flags: 0x012 (SYN, ACK)
    - 000. .... = Reserved: Not set
    - ...0 ..... = Accurate ECN: Not set
    - ....0..... = Congestion Window Reduced: Not set
    - ....0..... = ECN-Echo: Not set
    - ....0..... = Urgent: Not set
    - ....0.1.... = Acknowledgment: Set
    - ....0....0.. = Push: Not set
    - ....0....0.. = Reset: Not set
    - ....0....1.. = Syn: Set
    - ....0....0.. = Fin: Not set
    - [TCP Flags: .....A..S.]

Packet 834 bytes:

```

0000  9c 29 76 0d 20 be 2c 21 72 60 6f c2 08 00 45 00
0010  00 34 00 00 40 00 3e 06 da f7 0a cb 04 46 0a ba
0020  48 02 00 50 04 80 50 18 08 fb 12 39 e8 da 80 12
0030  fa f0 b9 c4 00 00 02 04 05 b4 01 01 04 02 01 03
0040  03 07
  
```

No.	Time	Source	Destination	Protocol	Length	Info
835	9.056808	10.203.4.70	10.186.72.2	TCP	66	80 → 1153 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
836	9.057054	10.186.72.2	10.203.4.70	TCP	54	1152 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
837	9.057109	10.186.72.2	10.203.4.70	TCP	54	1153 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
839	9.057264	10.186.72.2	10.203.4.70	HTTP	523	GET / HTTP/1.1

>	Frame 836: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF{...}	0000	2c 21 72 60 6f c2 9c 2
>	Ethernet II, Src: IntelCor_0d:20:be (9c:29:76:0d:20:be), Dst: JuniperN_00:6f:c2 (2c:21:72:f2:00:00)	0010	00 28 a8 4b 40 00 40 0
>	Internet Protocol Version 4, Src: 10.186.72.2, Dst: 10.203.4.70	0020	04 46 04 80 00 50 12 3
✓	Transmission Control Protocol, Src Port: 1152, Dst Port: 80, Seq: 1, Ack: 1, Len: 0	0030	02 01 61 e7 00 00

Source Port: 1152

Destination Port: 80

[Stream index: 31]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 305785050

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1343752444

0101 .... = Header Length: 20 bytes (5)

▼ Flags: 0x010 (ACK)

0000. .... = Reserved: Not set

...0 .... = Accurate ECN: Not set

.... 0... = Congestion Window Reduced: Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = **Acknowledgment: Set**

.... .... 0... = Push: Not set

.... ..0.. = Reset: Not set

.... .... 00. = Syn: Not set

.... .... ...0 = Fin: Not set

[TCP Flags: .....A....]

Window: 513



## 2、HTTP 请求

(1)客户发出 HTTP 请求之后，服务器收到请求发送 ACK

839	9.057264	10.186.72.2	10.203.4.70	HTTP	523 GET / HTTP/1.1
-----	----------	-------------	-------------	------	--------------------

```
> Frame 839: 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits) on interface \Device\NPF{...}
> Ethernet II, Src: IntelCor_0d:20:be (9c:29:76:0d:20:be), Dst: JuniperN_60:6f:c2 (2c:21:72:6f:c2:21:72:6f:c2)
> Internet Protocol Version 4, Src: 10.186.72.2, Dst: 10.203.4.70
v Transmission Control Protocol, Src Port: 1152, Dst Port: 80, Seq: 1, Ack: 1, Len: 469
  Source Port: 1152
  Destination Port: 80
  [Stream index: 31]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 469]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 305785050
  [Next Sequence Number: 470 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1343752444
  0101 .... = Header Length: 20 bytes (5)
v Flags: 0x018 (PSH, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  .... 0... = Congestion Window Reduced: Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 = Acknowledgment: Set
  .... .... 1... = Push: Set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....AP...]
  Window: 513
  [Calculated window size: 131328]
  [Window size scaling factor: 256]
```

```
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x63bc [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
  TCP payload (469 bytes)
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: www.zju.edu.cn\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
      \r\n
      [Full request URI: http://www.zju.edu.cn/]
      [HTTP request 1/1]
      [Response in frame: 842]
```

## (2) 服务器发送应答报文

ip.addr == 10.203.4.70						
No.	Time	Source	Destination	Protocol	Length	Info
839	9.057264	10.186.72.2	10.203.4.70	HTTP	523	GET / HTTP/1.1
841	9.060690	10.203.4.70	10.186.72.2	TCP	56	80 → 1152 [ACK] Seq=1 Ack=470 Win=64128 Len=0
842	9.060690	10.203.4.70	10.186.72.2	HTTP	454	HTTP/1.1 301 Moved Permanently (text/html)
850	9.073241	10.186.72.2	10.203.4.70	TCP	66	1157 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

> Frame 841: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF{...}

> Ethernet II, Src: JuniperN\_60:6f:c2 (2c:21:72:60:6f:c2), Dst: IntelCor\_0d:20:be (9c:29:76:cf:80:0d)

> Internet Protocol Version 4, Src: 10.203.4.70, Dst: 10.186.72.2

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1152, Seq: 1, Ack: 470, Len: 0

Source Port: 80

Destination Port: 1152

[Stream index: 31]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1343752444

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 470 (relative ack number)

Acknowledgment number (raw): 305785519

0101 .... = Header Length: 20 bytes (5)

▼ Flags: 0x010 (ACK)

000. .... = Reserved: Not set

...0 .... = Accurate ECN: Not set

.... 0... = Congestion Window Reduced: Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... ....0... = Push: Not set

.... .....0.. = Reset: Not set

.... .... .0. = Syn: Not set

.... .....0 = Fin: Not set

[TCP Flags: .....A....]

Window: 501

0000 9c 29 76 0d 20 be 2c 2

0010 00 28 a2 f7 40 00 3e 0

0020 48 02 00 50 04 80 50 1

0030 01 f5 f1 45 00 00 00 0