

# 深圳大学实验报告

课程名称: 计算机网络

实验项目名称: 实验三 数据包抓取与分析

学院: 计算机与软件学院

专业: 计算机科学与技术

指导教师: 崔来中

报告人: 张博智 学号: 2023150159 班级: 计科 2 班

实验时间: 2025 年 4 月 1 日

实验报告提交时间: 2025 年 4 月 6 日

教务部制

### 实验目的：

学习安装、使用协议分析软件，掌握基本的数据报捕获、过滤和协议的分析技巧，能对抓取数据包进行分析。

### 实验内容：

协议分析软件的安装和使用、学会抓取数据包的方法并对抓取数据包进行分析

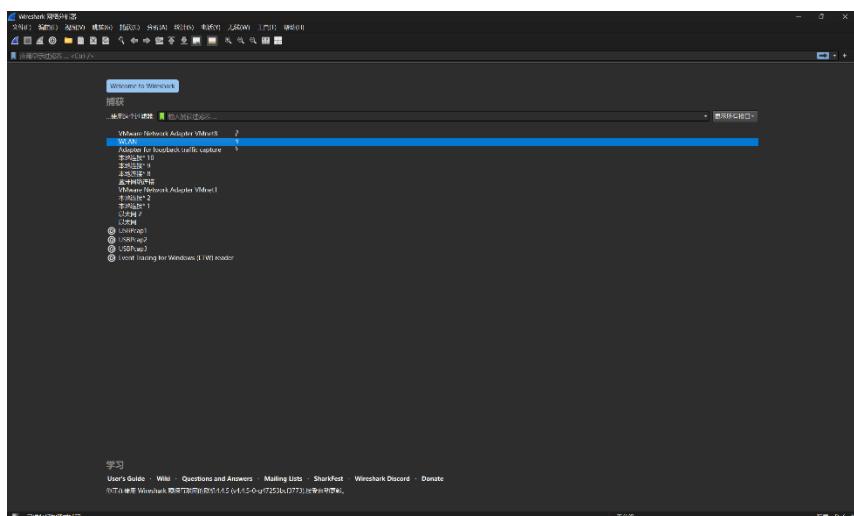
### 实验环境和要求：

使用 Windows 操作系统； Internet 连接

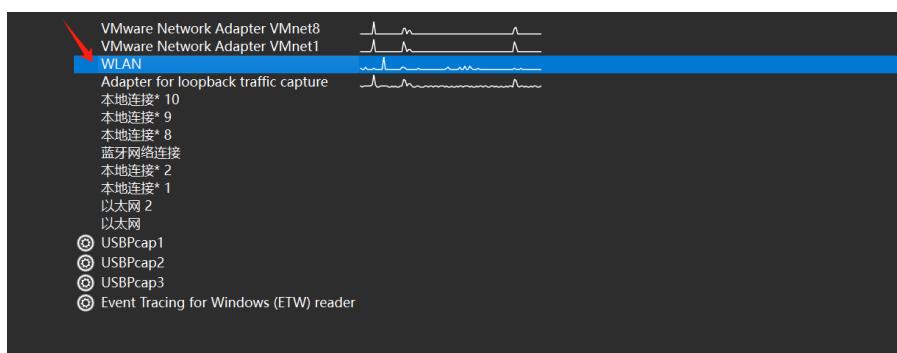
抓包软件 Wireshark。

### 方法、步骤：

1. 在网址 <http://wiki.wireshark.org/CaptureSetup/NetworkMedia> 处下载最新版的 wireshark 并安装：



2. wireshark 是捕获机器上的某一块网卡的网络包，当你的机器上有多块网卡的时候，你需要选择一个网卡。



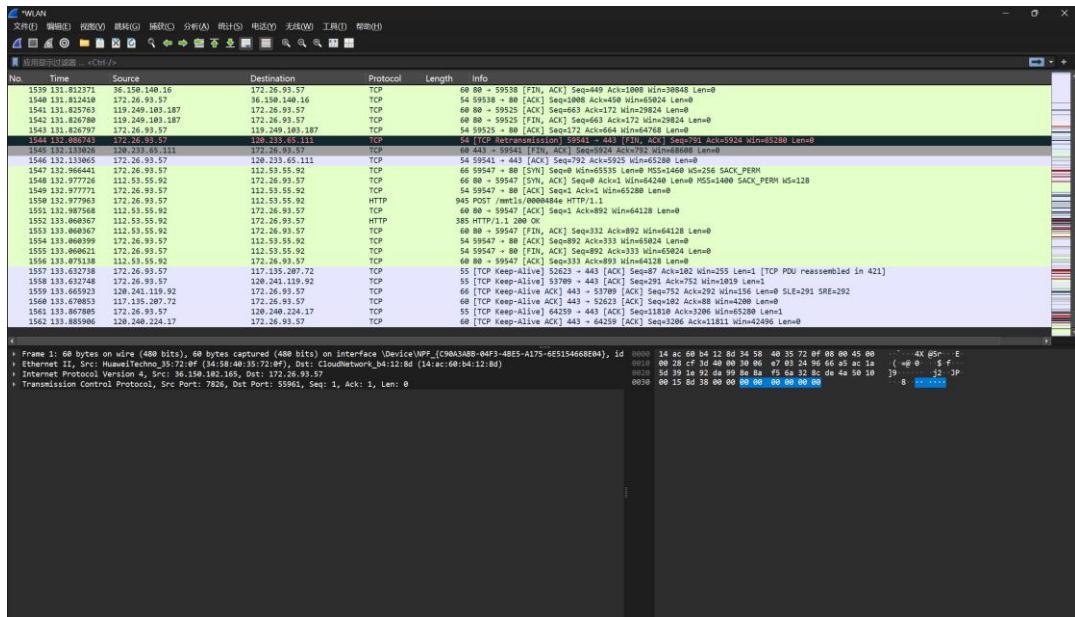
### 3. Wireshark 主要分为这几个界面：

Display Filter(显示过滤器), 用于过滤

Packet List Pane(封包列表), 显示捕获到的封包, 有源地址和目标地址, 端口号。颜色不同, 代表 3. Packet Details Pane(封包详细信息), 显示封包中的字段

Dissector Pane(16 进制数据)

Miscellaneous(地址栏, 杂项)



### 4. 过滤器会帮助我们在大量的数据中迅速找到我们需要的信息。

No.	Time	Source	Destination	Protocol	Length	Info
1539	131.812371	36.150.140.16	172.26.93.57	TCP	60 80	→ 59538 [FIN, ACK] Seq=449 Ack=1008 Win=30848 Len=0

### 5. 这个面板是我们最重要的, 用来查看协议中的每一个字段

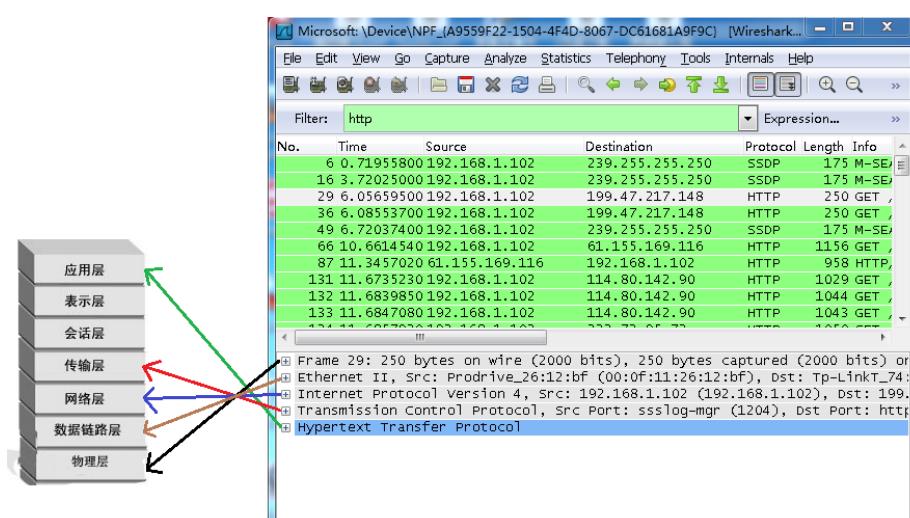
-Frame:物理层的数据帧概况

-Ethernet:数据链路层以太网帧头部信息

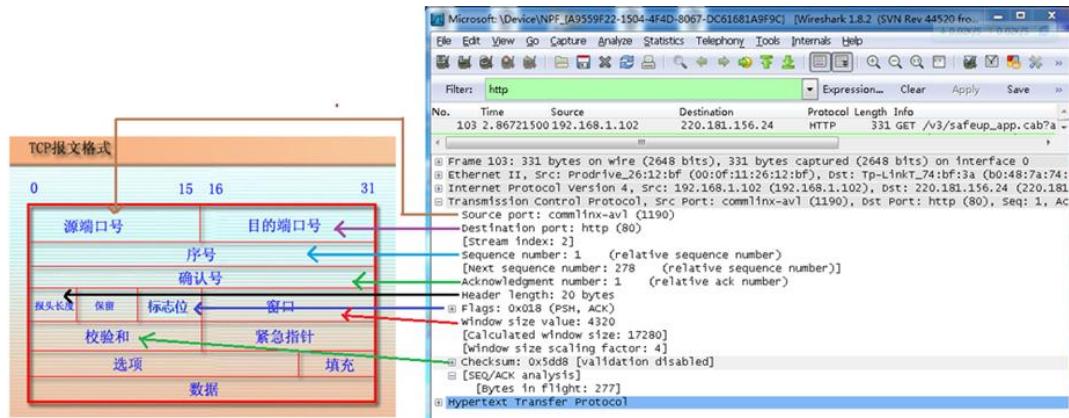
-Internet Protocol Version 4:互联网层|P 包头部信息

-Transmission Control Protocol:传输层 T 的数据段头部信息, 此处是 TCP- Hypertext

Transfer Protocol:应用层的信息, 此处是 HTTP 协议



## 6. 从下图可以看到 wireshark 捕获到的 TCP 包中的每个字段



实验过程及内容：

(ps:由于 ppt 提供的两个关于深大的网址无法打开，本实验用校园网网址进行代替)

### 一、tcp 分析

网址 1: www1.szu.edu.cn--三次握手

客户端发送连接请求

No.	Time	Source	Destination	Protocol	Length	Info
3279 30.235658	172.26.84.145	210.39.4.1		TCP	66	58781 + 43 (Syn) Seq=55335 Len=6 MSS=1460 Win=3280 SACK_PERM WS=512
3279 30.239587	210.39.4.1	172.26.84.145		TCP	66	58782 + 443 (Ack) Seq=1 Ack=1 Win=65280 Len=0 MSS=1460 SACK_PERM WS=512
3279 30.239663	172.26.84.145	210.39.4.1		TCP	54	58782 + 443 (ACK) Seq=1 Ack=1 Win=65280 Len=0
3279 30.239932	172.26.84.145	210.39.4.1		TCP	1514	58782 + 443 (ACK) Seq=1 Ack=1 Win=65280 Len=1460 [TCP PDU reassembled in 32880]
3280 30.239955	172.26.84.145	210.39.4.1		TLSv1.3	383	Cipher: Hello, Change Cipher Spec, Application Data
3280 30.239963	210.39.4.1	172.26.84.145		TCP	66	58783 + 50 (Syn) Seq=1 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=512
3280 30.231282	172.26.84.145	210.39.4.1		TCP	54	58783 + 88 (ACK) Seq=1 Ack=1 Win=5280 Len=0
3280 30.236333	210.39.4.1	172.26.84.145		TCP	60	58782 + 443 (ACK) Seq=1 Ack=1 Win=32256 Len=0
3287 30.236802	210.39.4.1	172.26.84.145		TCP	60	58782 + 443 (ACK) Seq=1 Ack=1 Win=35328 Len=0
3288 30.238444	210.39.4.1	172.26.84.145		TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
3289 30.239963	210.39.4.1	172.26.84.145		TCP	1514	58782 + 443 (ACK) Seq=29200 Ack=1799 Win=35328 Len=1460 [TCP PDU reassembled in 32880]
3290 30.239988	210.39.4.1	172.26.84.145		TLSv1.3	1239	Application Data
3291 30.239988	210.39.4.1	172.26.84.145		TLSv1.3	371	Application Data, Application Data
3292 30.239942	172.26.84.145	210.39.4.1		TCP	54	58782 + 443 (ACK) Seq=1798 Ack=4414 Win=65280 Len=0
3293 30.240495	210.39.4.1	172.26.84.145		TLSv1.3	134	Client Hello, Application Data
3296 30.240499	172.26.84.145	210.39.4.1		TLSv1.3	146	Application Data
3299 30.241928	172.26.84.145	210.39.4.1		TLSv1.3	578	Application Data
3300 30.246488	210.39.4.1	172.26.84.145		TLSv1.3	133	Application Data
3301 30.246974	210.39.4.1	172.26.84.145		TLSv1.3	133	Application Data
3302 30.247129	210.39.4.1	172.26.84.145		TLSv1.3	129	Application Data
3307 30.247921	172.26.84.145	210.39.4.1		TCP	54	58782 + 443 (ACK) Seq=2486 Ack=4643 Win=65280 Len=0
3309 30.247129	172.26.84.145	210.39.4.1		TLSv1.3	85	Application Data
3310 30.248529	210.39.4.1	172.26.84.145		TLSv1.3	365	Application Data
						0x0000 34 58 40 35 72 0f 14 ac 60 b4 12
						0x0010 00 34 5e e2 40 00 88 06 c5 d5 a6
						0x0020 04 01 c6 5f 00 50 ea 0d 55 de 06
						0x0030 ff ff 91 a0 00 00 02 04 95 54 02
						0x0040 04 02

**Ethernet II, Src: Cloudnetwork\_b4-11:8d (14:ac:68:b4:11:8d), Dst: HuaweiTechno\_35:72:0f (34:58:46:35:72:0f)**

**Internet Protocol Version 4, Src: 172.26.84.145, Dst: 210.39.4.1**

**Transmission Control Protocol, Src Port: 58783, Dst Port: 80, Seq: 0, Len: 0**

Source Port: 58783  
Destination Port: 80  
[Stream Index: 44]  
[Stream Packet Number: 1]  
[Conversation completeness: Complete, NO\_DATA (23)]  
[TCP Segment Len: 0]  
[Sequence Number (raw): 3992674244]  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 0  
Acknowledgment Number (raw): 0  
[Offset: 0, Length: 32 bytes (8)]  
Flags: 0x0002 (Syn)  
000..... = Reserved: Not set  
..0..... = Accurate ECN: Not set  
..0..... = Congestion Window Reduced: Not set  
..0..... = Don't Fragment: Not set  
..0..... = Urgent: Not set  
...0.... = Acknowledgment: Not set  
...0.... = Push: Not set  
...0.... = Reset: Not set  
...0.... = Syn: Set  
...0.... = Syn-ack: Not set  
...0.... = W-ack: Not set  
[TCP Flags: .....S]  
Window: 65535  
[Calculated window size: 65535]

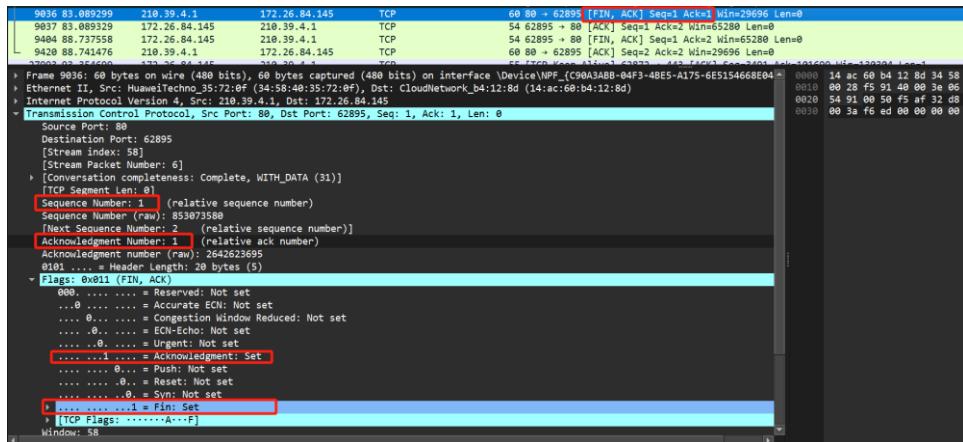
## 服务器端接收连接请求

No.	Time	Source	Destination	Protocol	Length	Info
3273	30.252618	172.26.84.145	219.39.4.1	TCP	66	56782 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3276	30.262848	172.26.84.145	219.39.4.1	TCP	66	56783 + 88 [SYN] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3278	30.230663	172.26.84.145	219.39.4.1	TCP	66	56784 + 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0 MSS=1460 Win=65280 SACK_PERM
3279	30.230932	172.26.84.145	219.39.4.1	TCP	1514	56782 + 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1460 [TCP PDU reassembled in 3280]
3280	30.230932	172.26.84.145	219.39.4.1	TLSv1.3	383	Client Hello (SNI=wvd.szu.edu.cn)
3281	30.231363	219.39.4.1	172.26.84.145	TCP	66	88 + 56783 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
3282	30.231363	172.26.84.145	219.39.4.1	TCP	66	56784 + 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0 MSS=1460 Win=65280 SACK_PERM
3286	30.236333	219.39.4.1	172.26.84.145	TCP	66	443 + 56782 [ACK] Seq=1 Ack=1461 Win=32256 Len=8
3287	30.236802	219.39.4.1	172.26.84.145	TCP	66	443 + 56782 [ACK] Seq=1 Ack=1798 Win=35328 Len=8
3288	30.238444	219.39.4.1	172.26.84.145	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
3289	30.239908	219.39.4.1	172.26.84.145	TCP	1514	443 + 56782 [ACK] Seq=1461 Ack=1798 Win=35328 Len=1460 [TCP PDU reassembled in 3290]
3290	30.239908	219.39.4.1	172.26.84.145	TLSv1.3	128	Application Data, Application Data
3291	30.239908	219.39.4.1	172.26.84.145	TLSv1.3	371	Application Data, Application Data
3292	30.239942	172.26.84.145	219.39.4.1	TCP	66	56782 + 443 [ACK] Seq=1798 Ack=4414 Win=65280 Len=0
3297	30.240847	219.26.84.145	219.39.4.1	TLSv1.3	134	Change Cipher Spec, Application Data
3298	30.240847	172.26.84.145	219.39.4.1	TLSv1.3	146	Application Data, Application Data
3299	30.240848	219.39.4.1	172.26.84.145	TLSv1.3	597	Application Data
3300	30.240848	219.39.4.1	172.26.84.145	TLSv1.3	133	Application Data
3306	30.240974	219.39.4.1	172.26.84.145	TLSv1.3	133	Application Data
3302	30.240974	219.39.4.1	172.26.84.145	TLSv1.3	125	Application Data
3307	30.240974	172.26.84.145	219.39.4.1	TCP	66	56783 + 443 [ACK] Seq=2486 Ack=4643 Win=65280 Len=0
3309	30.240974	219.39.4.1	172.26.84.145	TLSv1.3	85	Application Data
3310	30.240974	219.39.4.1	172.26.84.145	TLSv1.3	365	Application Data
3311	30.240974	219.39.4.1	172.26.84.145	TLSv1.3	82	Application Data
3312	30.240974	219.39.4.1	172.26.84.145	TLSv1.3	82	Application Data
3	Ethernet II, Src: HuaweiTechno_35-72-0F (34:58:45:35-72-0F), Dst: CloudNetwork_b4:12:8d (14:ac:68:b4:12:8d)					
4	Internet Control Message Protocol, Src Port: 50782, Dst Port: 50782, Seq: 0, Ack: 1, Len: 8					
5	Source Port: 443 Destination Port: 50782 [Stream index: 43] [Content type: payload [2]] [Content type completeness: Complete, WITH_DATA (31)] [TCP Segment Len: 0] Sequence Number: 0 (relative sequence number) Sequence Number (raw): 3726592863 Max Sequence Number: 0 (relative sequence number) Acknowledgment Number: 1 (relative ack number) Acknowledgment Number (raw): 1087317211 Header Length: 32 bytes (8) Flags: 0x012 (SYN, ACK) 0x00000000... Reserved: Not set 0x00000001... = Accurate ECN: Not set 0x00000002... = Congestion Window Reduced: Not set 0x00000004... = ECN-Echo: Not set 0x00000008... = Urgent: Not set 0x00000010... = Push: Not set 0x00000020... = Reset: Not set 0x00000040... = A..: Sym: Set 0x00000080... = P..: Fin: Not set [TCP Flags: 0x012 (SYN, ACK)] Window: 202980 [Calculated window size: 292801]					

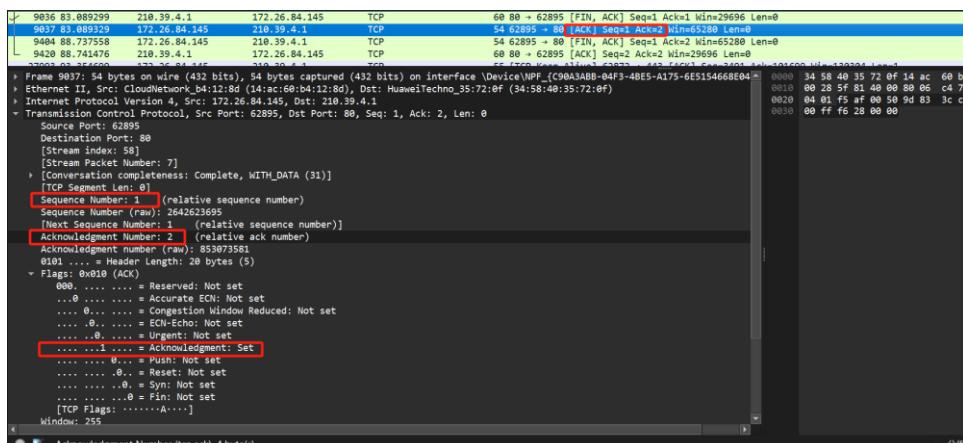
客户端确认

## 网址 1: www1.szu.edu.cn—四次挥手

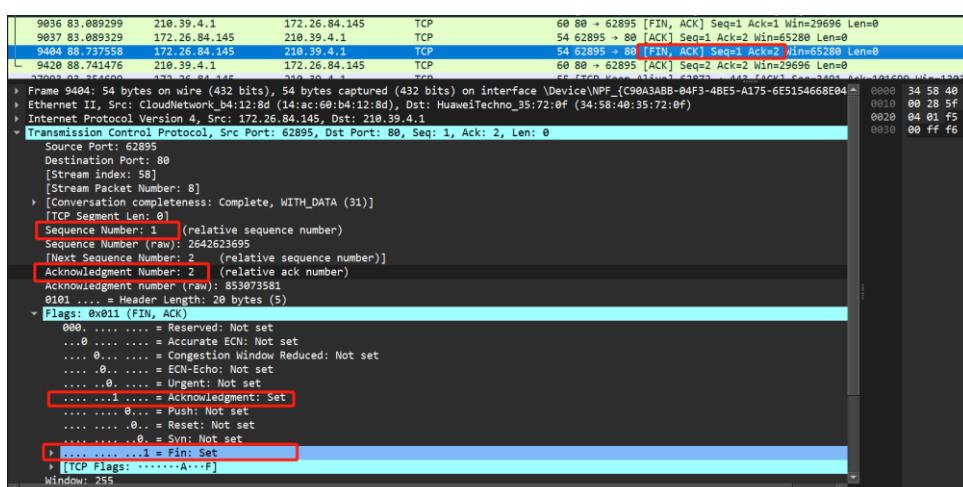
服务端确认断开连接（在网站静止足够长的时间，会发现服务器端会自动发送断开连接的请求）



客户端发送 ACK，已确认将要断开连接。但为了确定是否还有信息未发送，此时并未真正断开连接。



客户端已确认信息全部发送完毕，确认断开连接



服务器确认断开连接

```
9836 83.089299 210.39.4.1 172.26.84.145 TCP 60 88 → 62895 [FIN, ACK] Seq=1 Ack=1 Win=29696 Len=0
9837 83.089329 172.26.84.145 210.39.4.1 TCP 54 62895 → 88 [ACK] Seq=1 Ack=2 Win=65288 Len=0
9404 88.737558 172.26.84.145 210.39.4.1 TCP 54 62895 → 89 [FIN, ACK] Seq=1 Ack=2 Win=65288 Len=0
9420 88.741476 210.39.4.1 172.26.84.145 TCP 60 88 → 62895 [ACK] Seq=2 Ack=2 Win=29696 Len=0
0000 14 8c b4 12
Frame 9420: 68 bytes on wire (488 bits), 68 bytes captured (488 bits) on interface Device NPF ([09:3a:0b-04:f3-48e5-a175-6e515466fe84]
Ethernet II, Src: Huawei_Technology_35-72:0F (34:58:48:35-72:0F), Dst: CloudNetwork_b4:12:8D (14:ac:68:b4:12:8d)
Internet Protocol Version 4, Src: 210.39.4.1, Dst: 172.26.84.145
Transmission Control Protocol, Src Port: 88, Dst Port: 62895, Seq: 2, Ack: 2, Len: 0
Source IP: 210.39.4.1
Destination Port: 62895
[Stream index: 58]
[Stream Packet Number: 9]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 2 (relative sequence number)
Sequence Number (raw): 853073581
Next Sequence Number: 2 (relative sequence number)
Acknowledgment Number: 2 (relative ack number)
Acknowledgment Number (raw): 2642623696
0x01 = Header Length: 20 bytes (5)
Flags: 0x10 (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.... .... = Acknowledgment: Set
    0...0.... = Push: Not set
    ...0.... .... = Reset: Not set
    ...0.... .... = Syn: Not set
    ...0.... .... = Fin: Not set
    [TCP Flags: .....A....]
Window: 58
0000 14 8c b4 12
0001 00 28 5b d4
0002 00 91 00 59 ff
0003 00 3a f6 ec 00
Acknowledgment Number (tcp.ack), 4 byte(s)
```

网址 2: [www.youku.com](http://www.youku.com) --三次握手

客户端发送连接请求

服务器端接收连接请求

## 客户端确认

1729 8.683088	172.26.84.145	106.11.43.183	TCP	66 63338 -> 443 [SYN] Seq=0 Win=65536 Len=64 Win=256 SACK_PERM
1738 8.690213	172.26.84.145	106.11.43.183	TCP	66 63338 -> 443 [ACK] Seq=1 Win=73800 Len=65536 SACK_PERM Win=512
1740 8.690213	172.26.84.145	106.11.43.183	TCP	1454 443 -> 63338 [PSH, ACK] Seq=1 Win=73800 Len=6446 [TCP PDU reassembled in 1740]
1740 8.690436	172.26.84.145	106.11.43.183	TLSv1.2	476 Client Hello (SM4+PC,pay.youku.com)
1796 8.645276	106.11.43.183	172.26.84.145	TCP	68 443 -> 63338 [ACK] Seq=1480 Win=7168 Len=8
1797 8.645276	106.11.43.183	172.26.84.145	TCP	1454 443 -> 63338 [ACK] Seq=1481 Win=7168 Len=122 [TCP PDU reassembled in 1797]
2297 9.277814	106.11.43.183	172.26.84.145	TCP	68 443 -> 63338 [ACK] Seq=1481 Win=7168 Len=8
2298 9.277814	106.11.43.183	172.26.84.145	TLSv1.2	1454 Server Hello
2300 9.277814	106.11.43.183	172.26.84.145	TCP	1454 443 -> 63338 [PSH, ACK] Seq=1481 Win=7168 Len=6446 [TCP PDU reassembled in 2300]
2300 9.277814	106.11.43.183	172.26.84.145	TLSv1.2	1398 443 -> 63338 [PSH, ACK] Seq=1481 Win=7168 Len=1296 [TCP PDU reassembled in 2301]
2301 9.277814	106.11.43.183	172.26.84.145	TLSv1.2	1288 Certificate, Server Key Exchange, Server Name Done
2302 9.277814	106.11.43.183	172.26.84.145	TLSv1.2	54 63338 -> 443 [ACK] Seq=1482 Ack=1331 Win=6288 Len=8
2303 9.277814	106.11.43.183	172.26.84.145	TLSv1.2	1454 Client Hello, Change Cipher Spec, Encrypted Handshake Message
2304 9.277814	106.11.43.183	172.26.84.145	TLSv1.2	153 Application Data
2305 9.277814	106.11.43.183	172.26.84.145	TLSv1.2	1065 Application Data
2306 9.277814	106.11.43.183	172.26.84.145	TLSv1.2	59 63338 -> 443 [ACK] Seq=1483 Ack=1026 Win=7168 Len=8
2315 9.380157	106.11.43.183	172.26.84.145	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2316 9.380157	106.11.43.183	172.26.84.145	TLSv1.2	132 Application Data
2317 9.380157	106.11.43.183	172.26.84.145	TLSv1.2	54 63338 -> 443 [ACK] Seq=1484 Ack=5667 Win=68824 Len=8
2318 9.380157	106.11.43.183	172.26.84.145	TLSv1.2	92 Application Data
2319 9.398662	106.11.43.183	172.26.84.145	TLSv1.2	863 Application Data
2320 9.398662	106.11.43.183	172.26.84.145	TLSv1.2	92 Application Data
2321 9.398662	106.11.43.183	172.26.84.145	TCP	54 63338 -> 443 [ACK] Seq=1484 Ack=6514 Win=64256 Len=8

## 网址 2: www.youku.com –四次挥手（三次）

### 客户端确认断开连接

97333 69.658755	172.26.84.145	106.11.43.183	TCP	54 63338 -> 443 [FIN, ACK] Seq=20240 Ack=26070 Win=65280 Len=0
97434 69.111897	106.11.43.183	172.26.84.145	TCP	60 443 -> 63338 [FIN, ACK] Seq=26070 Ack=20241 Win=12800 Len=0
97443 69.112006	172.26.84.145	106.11.43.183	TCP	54 63338 -> 443 [ACK] Seq=20241 Ack=26071 Win=65280 Len=0
> Frame 97333: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 'Device\NPF_{C90A3ABB-04F3-4B55-A175-6E5154668E0' [0000: 34 58 40 35 72 0f 34 ac 69 b4 12 8d]				
> Ethernet II, Src: CloudNetwork_04:12:8d (14:ac:b4:12:8d), Dst: HuaweiTechno_30:72:0f (34:58:40:35:72:0f)				
> Internet Protocol Version 4, Src: 172.26.84.145, Dst: 106.11.43.183				
> Transmission Control Protocol, Src Port: 63338, Dst Port: 443, Seq: 20240, Ack: 26070, Len: 0				
Source Port: 63338 Destination Port: 443 [Stream index: 48] [Stream Packet Number: 124] > Conversation completeness: Complete, WITH_DATA (31) [TCP Segment Len: 0] Sequence Number: 20240 (relative sequence number) Sequence Number (raw): 620111391 [Next Sequence Number: 20241 (relative sequence number)] Acknowledgment Number: 26070 (relative ack number) Acknowledgment number (raw): 1137455612 0101 .... = Header Length: 20 bytes (5) + Flags: 0x011 (FIN, ACK) ....0..... = Reserved: Not set ....0..... = Accurate ECN: Not set ....0..... = Congestion Window Reduced: Not set ....0..... = ECN-Echo: Not set ....0..... = Urgent: Not set ....0..... = Acknowledgment: Set ....0..... = Push: Not set ....0..... = Reset: Not set ....0..... = Sync: Not set ....0..... = ACK: Set ....1.... = FIN: Set > ....0....0....1 = FIN: Set > [TCP Flags: .....A---F] Window: 255				

当被动关闭方（此处是优酷服务器服务器）在 tcp 挥手过程中，如果“没有数据要发送”，同时“没有开启 TCP\_QUICKACK”（默认没有开启，等于是在使用 tcp 延迟确认机制），那么第二次和第三次挥手就会合并传输，这样就出现了三次挥手。

97333 69.658755	172.26.84.145	106.11.43.183	TCP	54 63338 -> 443 [FIN, ACK] Seq=20240 Ack=26070 Win=65280 Len=0
97434 69.111897	106.11.43.183	172.26.84.145	TCP	60 443 -> 63338 [FIN, ACK] Seq=26070 Ack=20241 Win=12800 Len=0
97443 69.112006	172.26.84.145	106.11.43.183	TCP	54 63338 -> 443 [ACK] Seq=20241 Ack=26071 Win=65280 Len=0
> Frame 97333: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 'Device\NPF_{C90A3ABB-04F3-4B55-A175-6E5154668E0' [0000: 34 58 40 35 72 0f 34 ac 69 b4 12 8d]				
> Ethernet II, Src: CloudNetwork_04:12:8d (14:ac:b4:12:8d), Dst: CloudNetwork_04:12:8d (14:ac:b4:12:8d)				
> Internet Protocol Version 4, Src: 106.11.43.183, Dst: 172.26.84.145				
> Transmission Control Protocol, Src Port: 63338, Dst Port: 443, Seq: 26070, Ack: 20241, Len: 0				
Source Port: 63338 Destination Port: 443 [Stream index: 48] [Stream Packet Number: 125] > Conversation completeness: Complete, WITH_DATA (31) [TCP Segment Len: 0] Sequence Number: 26070 (relative sequence number) Sequence Number (raw): 1137455612 [Next Sequence Number: 26071 (relative sequence number)] Acknowledgment Number: 20241 (relative ack number) Acknowledgment number (raw): 620111392 0101 .... = Header Length: 20 bytes (5) + Flags: 0x011 (FIN, ACK) ....0..... = Reserved: Not set ....0..... = Accurate ECN: Not set ....0..... = Congestion Window Reduced: Not set ....0..... = ECN-Echo: Not set ....0..... = Urgent: Not set ....0..... = Acknowledgment: Set ....0..... = Push: Not set ....0..... = Reset: Not set ....0..... = Sync: Not set ....0..... = ACK: Set ....1.... = FIN: Set > ....0....0....1 = FIN: Set > [TCP Flags: .....A---F] Window: 255				

## 客户端确认断开连接

97333 69.058755 172.26.84.145 106.11.43.183 TCP 54 63338 + 443 [FIN, ACK] Seq=20240 Ack=26070 Win=65280 Len=0
97343 69.111897 106.11.43.183 172.26.84.145 TCP 60 443 + 63338 [FIN, ACK] Seq=26070 Ack=20241 Win=12800 Len=0
97443 69.112006 172.26.84.145 106.11.43.183 TCP 54 63338 + 443 [ACK] Seq=20241 Ack=26070 Win=65280 Len=0
> Frame 97443: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C90A3AB8-04F3-4BE5-A175-6E5154668EB~
> Ethernet II, Src: CloudNetwork_b4:12:8d (48:ac:60:b4:12:8d), Dst: HuaweiTechno_35:72:0f (34:58:40:35:72:0f)
> Internet Protocol Version 4, Src: 172.26.84.145, Dst: 106.11.43.183
> Transmission Control Protocol, Src Port: 63338, Dst Port: 443, Seq: 20241, Ack: 26071, Len: 0
Source Port: 63338 Destination Port: 443 [Stream index: 48] [Stream Packet Number: 126] > [Conversation completeness: Complete, WITH_DATA (31)] [TCP Segment Len: 0] Sequence Number: 20241 (relative sequence number) Sequence Number (raw): 63011594 (Next Sequence Number: 20241 (relative sequence number)) Acknowledgment Number: 26071 (relative ack number) Acknowledgment number (raw): 1137455613 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 .0 . . . . . = Acknowledgment: Set .0 . . . . . = Push: Not set .0 . . . . . = Reset: Not set .0 . . . . . = Sync: Not set .0 . . . . . = Fin: Not set [TCP Flags: .0101A...] Window: 255

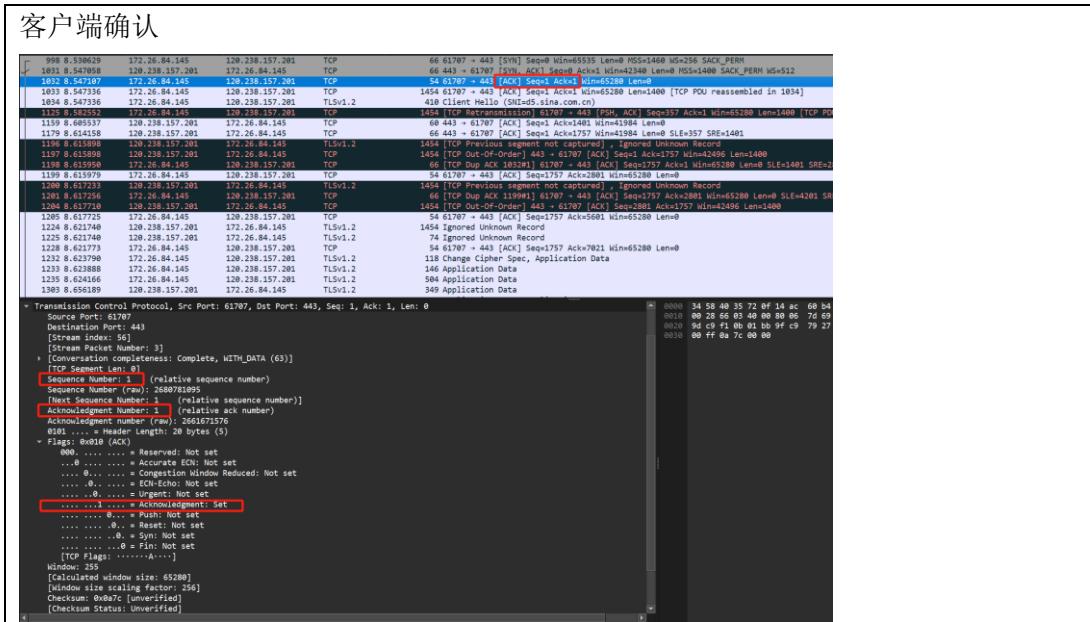
## 网址 3: www.sina.com.cn --三次握手

### 客户端发送连接请求

192.8.0.54:52 172.26.84.145 120.238.157.201 TCP 66 61707 - 443 [SYN, ACK] Seq=15373 Ack=14400 Win=256 SACK_PERM
1832 8.547088 120.238.157.201 172.26.84.145 TCP 54 61707 - 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1832 8.547107 172.26.84.145 120.238.157.201 TCP 1454 61707 + 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0 [TCP PDU reassembled in 1034]
1832 8.547136 172.26.84.145 120.238.157.201 TCP 1454 61707 + 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 1034]
1129 8.618352 172.26.84.145 120.238.157.201 TCP 1454 [TCP Retransmission] 61707 - 443 [PSH, ACK] Seq=357 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 1034]
1159 8.640537 120.238.157.201 172.26.84.145 TCP 68 443 - 61707 [ACK] Seq=14401 Win=1984 Len=0
1179 8.641518 120.238.157.201 172.26.84.145 TCP 68 443 - 61707 [ACK] Seq=14401 Win=1984 Len=0
1179 8.641535 120.238.157.201 172.26.84.145 TLSv1.2 1454 [TCP Out-Of-Order] 61707 - 443 [ACK] Seq=14401 Win=1984 Len=0
1179 8.641588 120.238.157.201 172.26.84.145 TCP 1454 [TCP Out-Of-Order] 61707 - 443 [ACK] Seq=14401 Win=1984 Len=0
1179 8.641598 120.238.157.201 172.26.84.145 TLSv1.2 66 [TCP Out-ACK 1832M] 61707 - 443 [ACK] Seq=357 Ack=1 Win=65280 Len=0 SLE=1401 SRE=2801
1220 8.617233 120.238.157.201 172.26.84.145 TLSv1.2 1454 [TCP Previous segment not captured] Ignored Unknown Record
1220 8.617256 120.238.157.201 172.26.84.145 TCP 66 [TCP Out ACK 1199M] 61707 - 443 [ACK] Seq=277 Ack=2801 Win=65280 Len=4201 SRE=600
1220 8.617257 120.238.157.201 172.26.84.145 TCP 66 443 - 61707 [ACK] Seq=277 Ack=2801 Win=65280 Len=4201 SRE=600
1220 8.617258 120.238.157.201 172.26.84.145 TLSv1.2 1454 Ignored Unknown Record
1220 8.617259 120.238.157.201 172.26.84.145 TCP 66 443 - 61707 [ACK] Seq=277 Ack=2801 Win=65280 Len=0
1220 8.617260 120.238.157.201 172.26.84.145 TLSv1.2 118 Change Cipher Spec, Application Data
1220 8.617261 120.238.157.201 172.26.84.145 TCP 146 Application Data
1220 8.617262 120.238.157.201 172.26.84.145 TLSv1.2 584 Application Data
1220 8.617263 120.238.157.201 172.26.84.145 TLSv1.2 349 Application Data
> Transmission Control Protocol, Src Port: 61707, Dst Port: 443, Seq: 0, Len: 0
Source Port: 61707 Destination Port: 443 [Stream index: 56] [Stream Packet Number: 1] > [Conversation completeness: Complete, WITH_DATA (63)] [TCP Segment Len: 0] Sequence Number: 15373 (relative sequence number) Sequence Number (raw): 268671594 (Next Sequence Number: 1 (relative sequence number)) Acknowledgment Number: 0 Acknowledgment number (raw): 0 1000 . . . = Header Length: 32 bytes (8) Flags: 0x0002 (SYN) 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 . . . . . = Acknowledgment: Not set .0 . . . . . = Push: Not set .0 . . . . . = Reset: Not set .0 . . . . . = Syn: Set [TCP Flags: .0002S...] Window: 255 [calculated window size: 65535] Checksum: 0xb4f6 [Unverified] [Checksum Status: Unverified] Urgent Pointer: 0

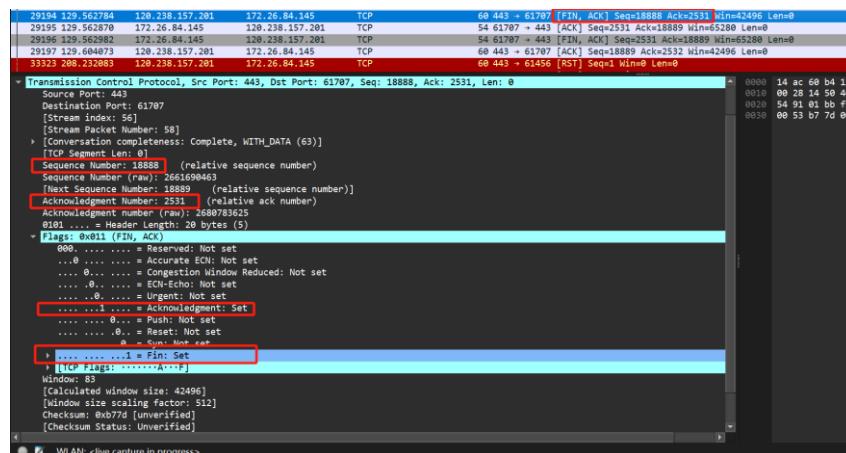
### 服务器端确认连接请求

192.8.0.54:52 172.26.84.145 120.238.157.201 TCP 66 61707 - 443 [SYN, ACK] Seq=15373 Ack=14400 Win=256 SACK_PERM
1832 8.547107 172.26.84.145 120.238.157.201 TCP 54 61707 - 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1832 8.547136 172.26.84.145 120.238.157.201 TCP 1454 61707 + 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 1034]
1129 8.618352 172.26.84.145 120.238.157.201 TCP 1454 [TCP Retransmission] 61707 - 443 [PSH, ACK] Seq=357 Ack=1 Win=65280 Len=1400 [TCP PDU reassembled in 1034]
1159 8.640537 120.238.157.201 172.26.84.145 TCP 68 443 - 61707 [ACK] Seq=14401 Win=1984 Len=0
1179 8.641518 120.238.157.201 172.26.84.145 TCP 68 443 - 61707 [ACK] Seq=14401 Win=1984 Len=0
1179 8.641535 120.238.157.201 172.26.84.145 TLSv1.2 1454 Ignored Unknown Record
1179 8.641588 120.238.157.201 172.26.84.145 TCP 66 [TCP Out-Of-Order] 61707 - 443 [ACK] Seq=14401 Win=1984 Len=0
1179 8.641598 120.238.157.201 172.26.84.145 TLSv1.2 66 [TCP Out-ACK 1832M] 61707 - 443 [ACK] Seq=357 Ack=1 Win=65280 Len=0 SLE=1401 SRE=2801
1220 8.617233 120.238.157.201 172.26.84.145 TLSv1.2 1454 [TCP Previous segment not captured] Ignored Unknown Record
1220 8.617256 120.238.157.201 172.26.84.145 TCP 66 [TCP Out ACK 1199M] 61707 - 443 [ACK] Seq=277 Ack=2801 Win=65280 Len=4201 SRE=600
1220 8.617257 120.238.157.201 172.26.84.145 TCP 66 443 - 61707 [ACK] Seq=277 Ack=2801 Win=65280 Len=0
1220 8.617258 120.238.157.201 172.26.84.145 TLSv1.2 1454 Ignored Unknown Record
1220 8.617259 120.238.157.201 172.26.84.145 TCP 66 443 - 61707 [ACK] Seq=277 Ack=2801 Win=65280 Len=0
1220 8.617260 120.238.157.201 172.26.84.145 TLSv1.2 118 Change Cipher Spec, Application Data
1220 8.617261 120.238.157.201 172.26.84.145 TCP 146 Application Data
1220 8.617262 120.238.157.201 172.26.84.145 TLSv1.2 584 Application Data
1220 8.617263 120.238.157.201 172.26.84.145 TLSv1.2 349 Application Data
> Transmission Control Protocol, Src Port: 61707, Dst Port: 443, Seq: 0, Ack: 1, Len: 0
Source Port: 61707 Destination Port: 443 [Stream index: 56] [Stream Packet Number: 2] > [Conversation completeness: Complete, WITH_DATA (63)] [TCP Segment Len: 0] Sequence Number: 15373 (relative sequence number) Sequence Number (raw): 268671595 (Next Sequence Number: 1 (relative sequence number)) Acknowledgment Number: 0 Acknowledgment number (raw): 0 1000 . . . = Header Length: 32 bytes (8) Flags: 0x0002 (SYN) 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 . . . . . = Acknowledgment: Set .0 . . . . . = Push: Not set .0 . . . . . = Reset: Not set .0 . . . . . = Syn: Set [TCP Flags: .0002S...] Window: 255 [calculated window size: 42348] Checksum: 0xc57f [Unverified] [Checksum Status: Unverified] Urgent Pointer: 0

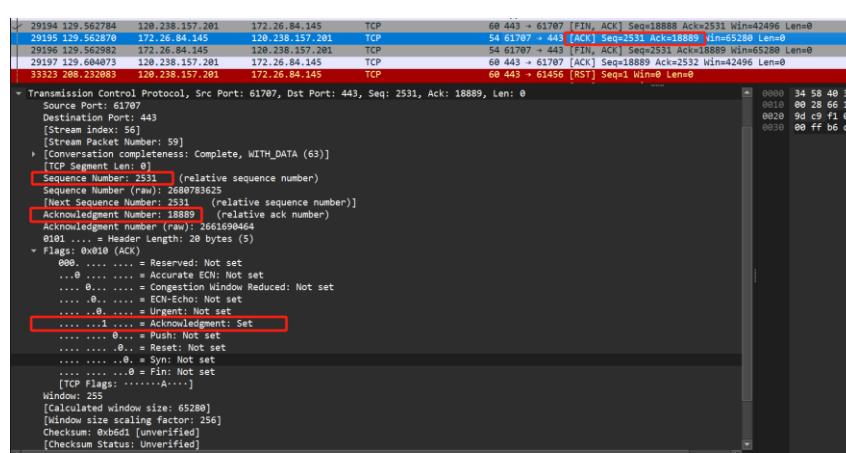


网址 3: [www.sina.com.cn](http://www.sina.com.cn) –四次挥手（在网站静止足够长的时间，会发现服务器端会自动发送断开连接的请求）

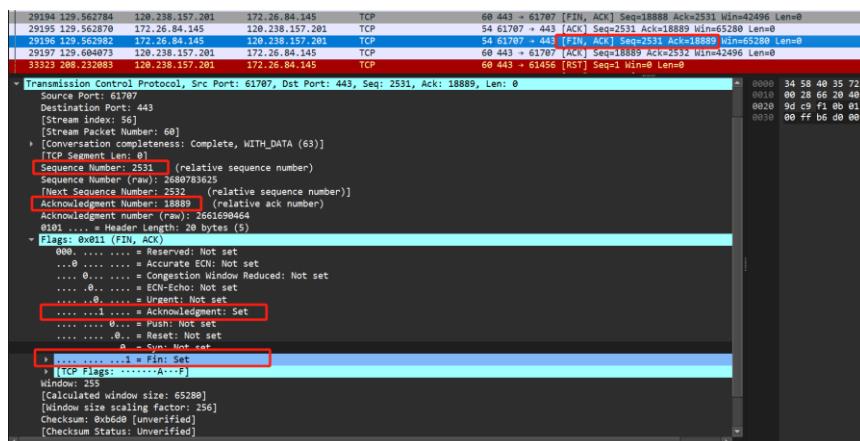
服务器端向客户端发送确认断开连接的请求



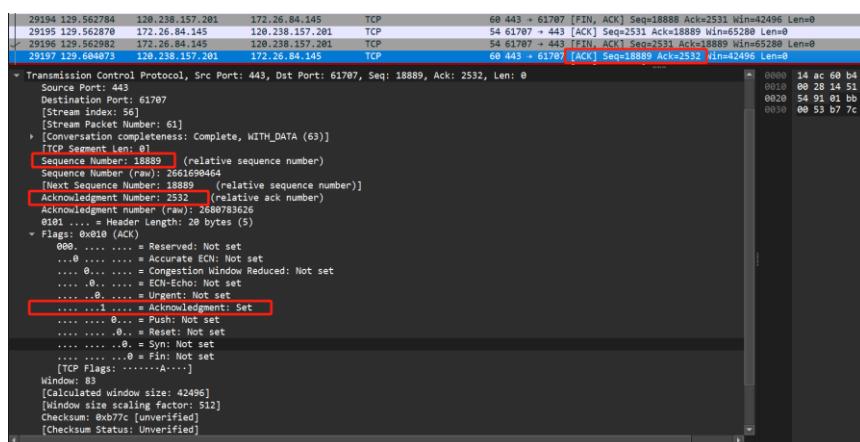
客户端发送 ACK，已确认将要断开连接。但为了确定是否还有信息未发送，此时并未真正断开连接。



客户端已确认信息全部发送完毕，确认断开连接

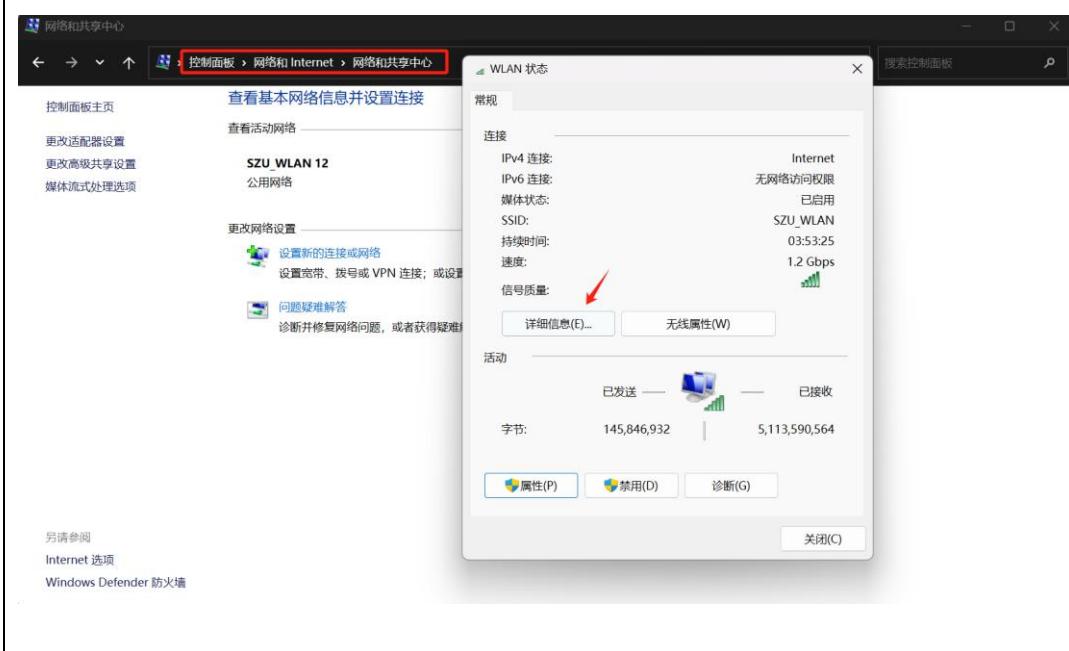


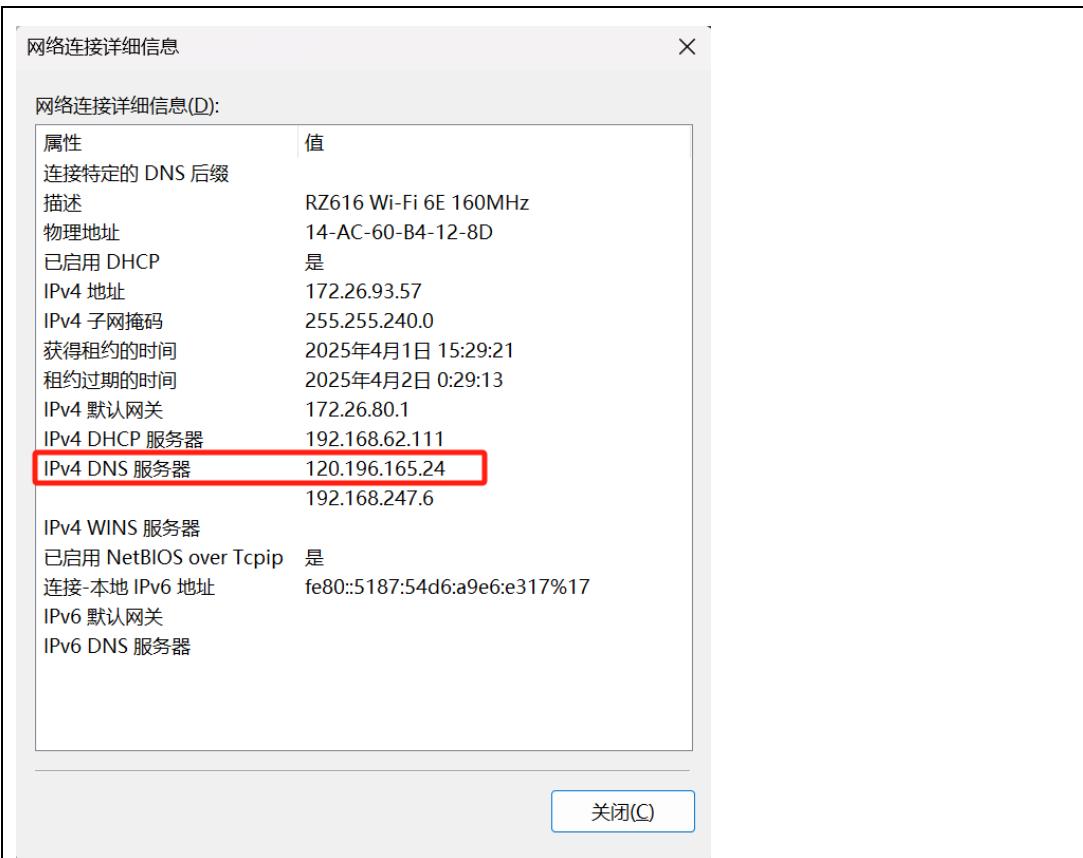
服务器确认断开连接



## 二、三个网址的 udp 和 dns 协议分析

在控制面板中可以找到自己当前网卡的 DNS 服务器的 IP 地址（在后续抓包过程可以发现确实是把域名发送到了该 IP 地址对应的 DNS 服务器）：





网址 1: www1.szu.edu.cn

由图可知：

该数据包的源端口=53， 目的端口=61380

长度=199, 校验码=0x676f

需要转换的网址是：[www1.szu.edu.cn](http://www1.szu.edu.cn)

IP 地址是: 210.30.4.1

网址 2: [www.youku.com](http://www.youku.com)

由图可知

该数据包的源端口（DNS 服务器）=53， 目的端口=61342

长度=492，校验码=0xd67

需要转换的网址是: [www.youku..com](http://www.youku.com)

IP 地址: 106.11.43.215

网址 3: [www.sina.com.cn](http://www.sina.com.cn)

```

3742 19.734517 128.196.165.24 DNS 226 Standard query response 0x2f91 A www.sina.com.cn CHNAME spool.grid.sinaedge.com CHNAME wsd.sinaling.cn.alikunlun.com SOA ns3.alikunlun.com
3743 19.734517 128.196.165.24 DNS 545 Standard query response 0x2f91 A www.sina.com.cn CHNAME spool.grid.sinaedge.com CHNAME wsd.sinaling.cn.alikunlun.com A 120.238.157.157.
3884 19.844147 172.26.93.57 DNS 77 Standard query response 0x2fcd A 1.sso.sina.com.cn
3885 19.844147 172.26.93.57 DNS 77 Standard query response 0x2fcd HTTPS 1.sso.sina.com.cn
3886 19.845201 128.196.165.24 DNS 76 Standard query response 0x2fcd A www.sina.com.cn
3887 19.845201 172.26.93.57 DNS 76 Standard query response 0x2fcd HTTPS news.sina.com.cn
3888 19.849015 128.196.165.24 DNS 547 Standard query response 0x2f6b A 1.sso.sina.com.cn CHNAME spool.grid.sinaedge.com CHNAME wsd.sinaling.cn.alikunlun.com A 120.238.157.157.
3889 19.849015 128.196.165.24 DNS 548 Standard query response 0x2f6b A 1.sso.sina.com.cn CHNAME spool.grid.sinaedge.com CHNAME wsd.sinaling.cn.alikunlun.com A 120.238.157.157.

* User Datagram Protocol, Src Port: 53, Dst Port: 40936
Source Port: 53
Destination Port: 40936
Length: 144
Checksum: 0x8d55 [unverified]
[checksum status: Unverified]
[Stream index: 48]
[Type/Protocol Number: 2]
[Timestamp: 1531144400.000000]
[UDP payload (598 bytes)]
Domain Name System (response)
Flags: 0x0000 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 3
Additional RRs: 4
+ Queries
- www.sina.com.cn: type A, class IN
+ www.sina.com.cn: type CNAME, class IN, cname spool.grid.sinaedge.com
+ www.sina.com.cn: type CNAME, class IN, cname wsd.sinaling.cn.w.alikunlun.com
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.157.212
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.157.188
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.157.188
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.157.212
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.157.208
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.157.208
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.157.217
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.158.233
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.158.237
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.158.237
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.157.178
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.241.119.92
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.241.119.99
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.158.238
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.241.119.91
+ www.sinaling.cn.alikunlun.com: type A, class IN, addr 128.238.157.281
+ Authoritative nameservers
+ Additional records

* Time: 0.000000000 seconds!
```

由图可知

该数据包的源端口（DNS 服务器）=53， 目的端口=49316

长度=511，校验码=0x5e55

需要转换的网址是: [www.sina.com.cn](http://www.sina.com.cn)

IP 地址有：

```

> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.157.212
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.157.207
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.157.188
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.158.218
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.241.119.90
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.158.236
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.157.208
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.158.217
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.158.233
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.158.237
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.157.178
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.241.119.92
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.241.119.89
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.158.238
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.241.119.91
> ww1.sinaimg.cn.w.alikunlun.com: type A, class IN, addr 120.238.157.201

```

DNS 系统还支持基于地理位置的域名解析，可以将域名解析成距离用户地理位置最近的服务器地址，加快用户访问速度。

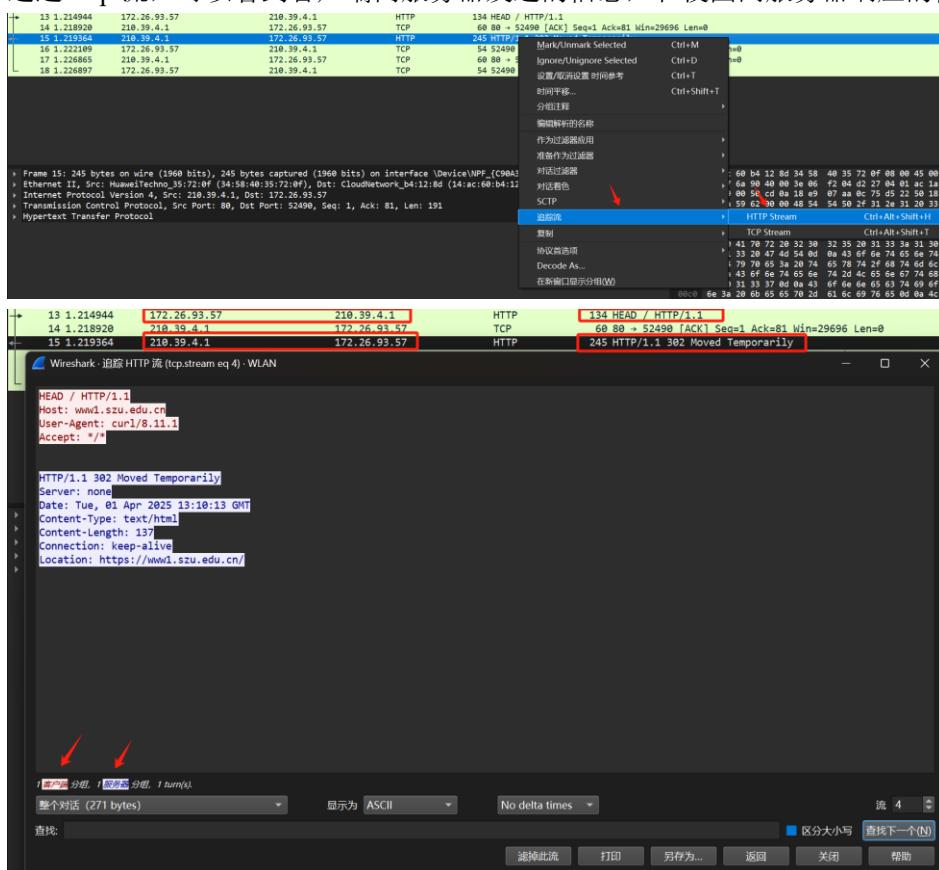
### 三、三个网站的 HTTP 协议分析

网址 1：www1.szu.edu.cn

首先通过控制台给对应网址发送数据包：

```
C:\Users\Burh233>curl -I www1.szu.edu.cn
HTTP/1.1 302 Moved Temporarily
Server: none
Date: Tue, 01 Apr 2025 13:10:13 GMT
Content-Type: text/html
Content-Length: 137
Connection: keep-alive
Location: https://www1.szu.edu.cn/
```

通过 http 流，可以看到客户端向服务器发送的信息，和校园网服务器响应的信息

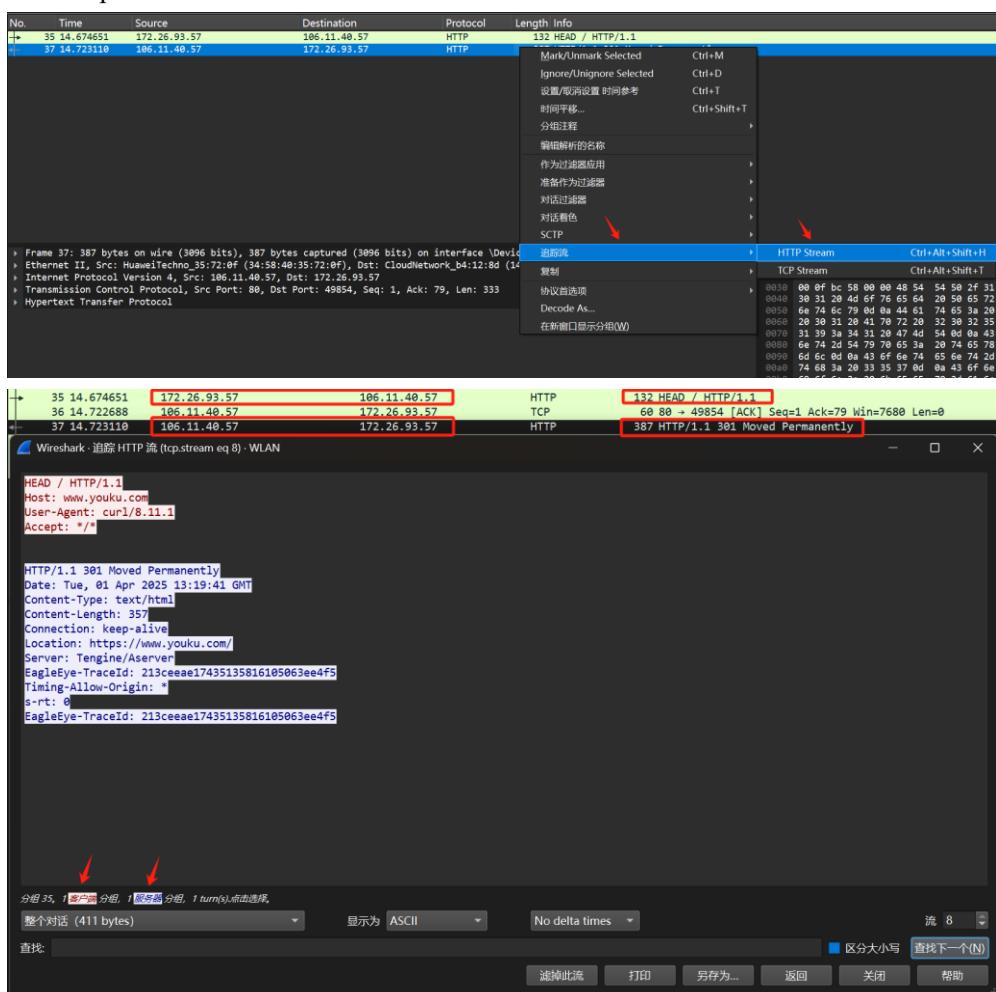


## 网址 2: www.youku.com

首先通过控制台给对应网址发送数据包:

```
C:\Users\Burh233>curl -I www.youku.com
HTTP/1.1 301 Moved Permanently
Date: Tue, 01 Apr 2025 13:19:02 GMT
Content-Type: text/html
Content-Length: 357
Connection: keep-alive
Location: https://www.youku.com/
Server: Tengine/Aserver
EagleEye-TraceId: 213e6d3d17435135426587328ec305
Timing-Allow-Origin: *
s-rt: 0
EagleEye-TraceId: 213e6d3d17435135426587328ec305
```

通过 http 流，可以看到客户端向服务器发送的信息，和优酷服务器响应的信息



### 网址 3: [www.sina.com.cn](http://www.sina.com.cn)

首先通过控制台给对应网址发送数据包:

```
C:\Users\Burh233>curl -I www.sina.com.cn
HTTP/1.1 302 Found
Server: Tengine
Date: Tue, 01 Apr 2025 13:24:24 GMT
Content-Type: text/html
Content-Length: 242
Connection: keep-alive
Location: https://www.sina.com.cn/
X-DSL-CHECK: 5
X-Via-CDN: f=aliyun,s=cache18.cn3102,c=183.238.144.48;
Via: cache18.cn3102[,0]
Timing-Allow-Origin: *
EagleId: 78ee9da617435138648408698e
```

通过 http 流，可以看到客户端向服务器发送的信息，和优酷服务器响应的信息

The screenshot shows the Wireshark interface. At the top, a context menu is open over the selected response frame (Frame 27). The 'Follow Stream' option is highlighted with a red arrow. Below the menu, the captured traffic is listed, and a separate window titled 'WireShark - 追踪 HTTP 流 (tcp.stream eq 5) - WLAN' displays the detailed HTTP stream for the selected response. Another red arrow points to this window.

No.	Time	Source	Destination	Protocol	Length	Info
+ 25	3.924192	172.26.93.57	120.238.157.211	HTTP	134	HEAD / HTTP/1.1
+ 26	3.945409	120.238.157.211	172.26.93.57	TCP	60	89 - 51937 [ACK] Seq=1 Ack=81 Win=42496 Len=0
+ 27	3.947305	120.238.157.211	172.26.93.57	HTTP	394	HTTP/1.1 302 Found

WireShark - 追踪 HTTP 流 (tcp.stream eq 5) - WLAN

```
HEAD / HTTP/1.1
Host: www.sina.com.cn
User-Agent: curl/8.11.1
Accept: */*

HTTP/1.1 302 Found
Server: Tengine
Date: Tue, 01 Apr 2025 13:24:24 GMT
Content-Type: text/html
Content-Length: 242
Connection: keep-alive
Location: https://www.sina.com.cn/
X-DSL-CHECK: 5
X-Via-CDN: f=aliyun,s=cache18.cn3102,c=183.238.144.48;
Via: cache18.cn3102[,0]
Timing-Allow-Origin: *
EagleId: 78ee9da617435138648408698e
```

搜索: 分组, 1 话单, 分组, 1 话单(s). 显示为: ASCII No delta times 流 5 区分大小写 查找下一个(N) 打印 另存为... 返回 关闭 帮助

实验分析：

### **TCP 连接管理**

三次握手：客户端发送 SYN，服务端响应 SYN+ACK，客户端确认 ACK，成功建立连接。

四次挥手：主动关闭方发送 FIN，接收方 ACK 确认；接收方发送 FIN，主动方 ACK 确认后释放连接。

观察到部分场景因延迟确认机制导致挥手步骤合并为三次(FIN+ACK 合并)。

### **DNS 协议分析**

响应中包含域名对应的 IP 地址（如 www1.szu.edu.cn 解析为 210.39.4.1）。

支持基于地理位置的解析，返回距离用户最近的服务器 IP。

### **HTTP 协议解析**

响应包含状态码（如 200 OK）、响应头和 HTML 内容。

观察到 HTTPS 流量因加密无法直接解析明文内容。

深圳大学学生实验报告用纸

**实验结论:**

**工具掌握:** 熟练使用 Wireshark 进行数据包捕获、过滤及分层解析，验证了网络协议的分层结构（物理层→应用层）。

**协议理解:**

TCP 通过三次握手确保可靠连接，四次挥手实现有序断开。

DNS 通过 UDP 实现高效域名解析，支持负载均衡与地理位置优化。

HTTP/HTTPS 协议在应用层实现客户端与服务器的请求-响应交互。

**指导教师批阅意见:**

**成绩评定:**

指导教师签字:

年   月   日

备注:

- 注: 1、报告内的项目或内容设置, 可根据实际情况加以调整和补充。  
2、教师批改学生实验报告时间应在学生提交实验报告时间后 10 日内。