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

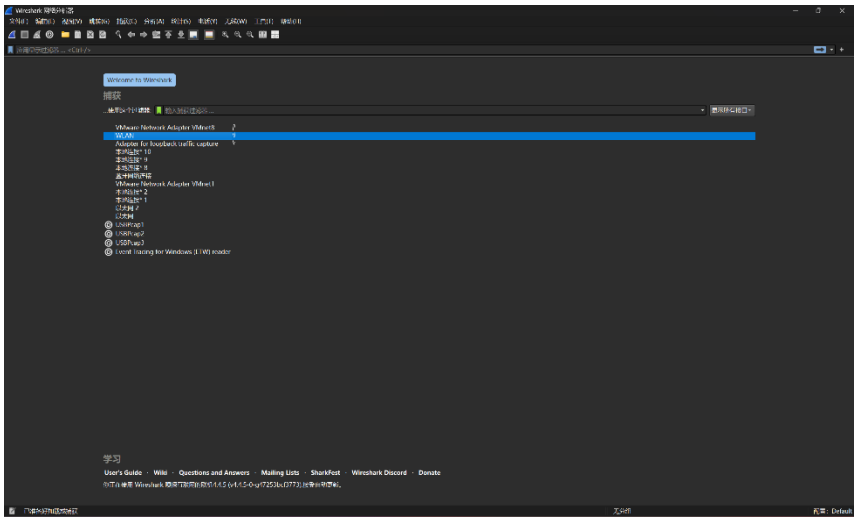
实验环境和要求：

使用 Windows 操作系统；Internet 连接

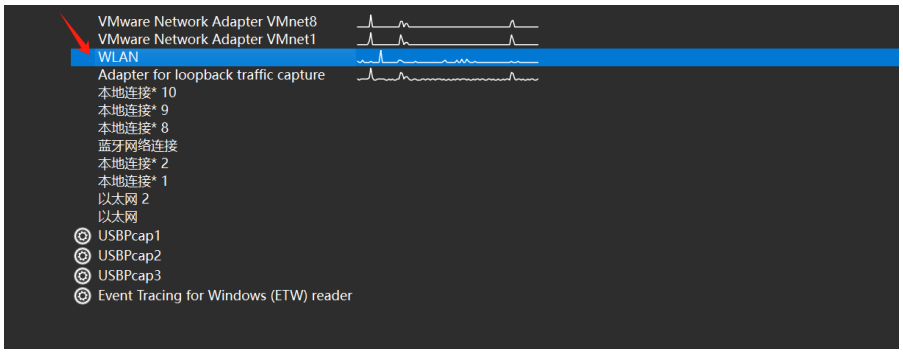
抓包软件 Wireshark。

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。



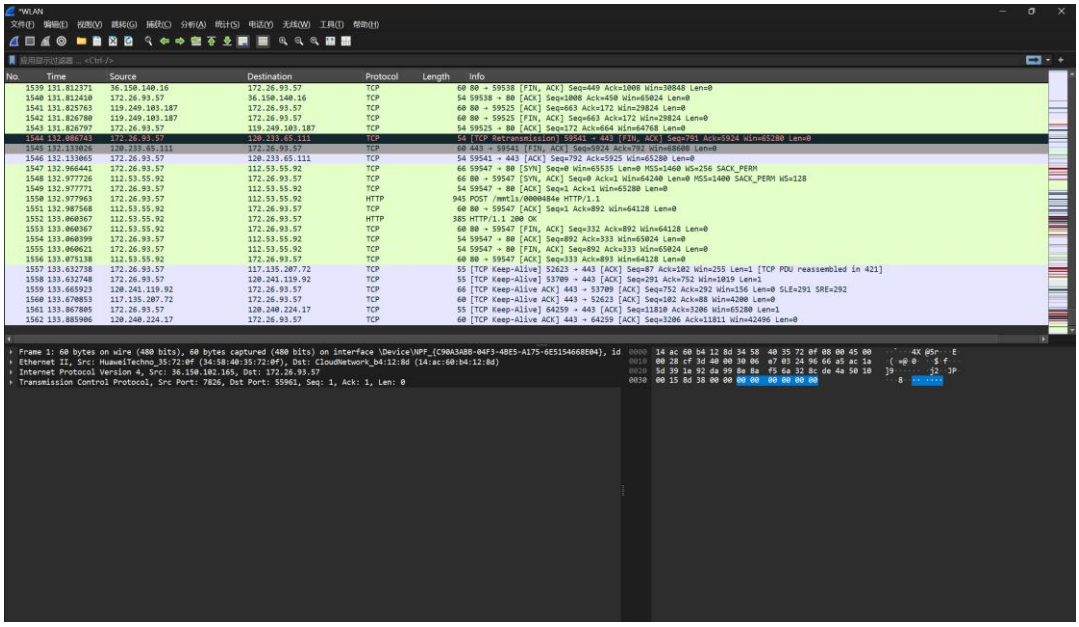
3. WireShark 主要分为这几个界面：

Display Filter(显示过滤器)，用于过滤

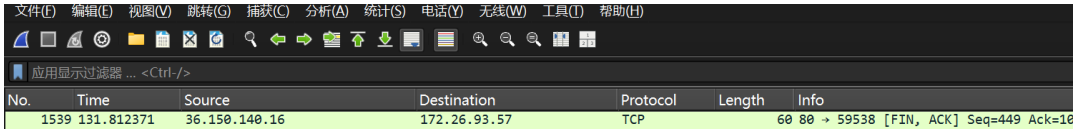
Packet List Pane(封包列表)，显示捕获到的封包，有源地址和目标地址，端口号。颜色不同，代表 3. Packet Details Pane(封包详细信息),显示封包中的字段

Dissector Pane(16 进制数据)

Miscellanous(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。



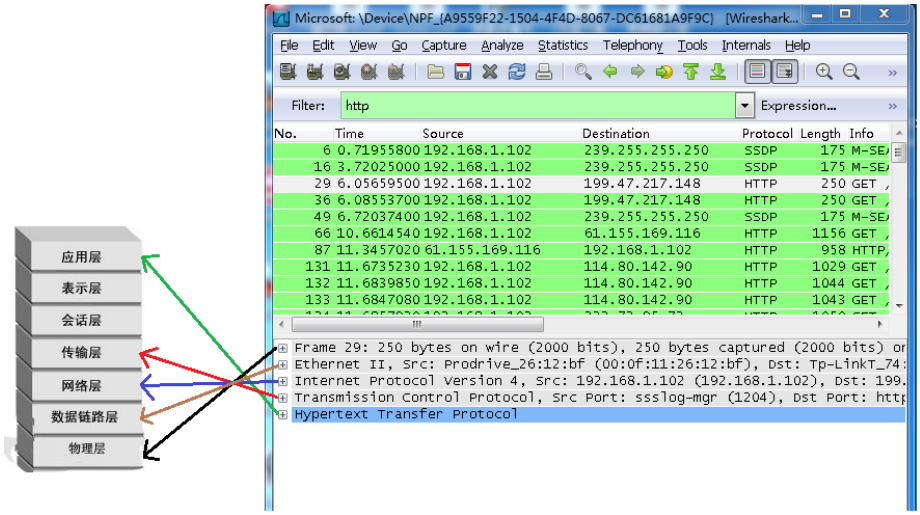
5. 这个面板是我们最重要的，用来查看协议中的每一个字段

-Frame:物理层的数据帧概况

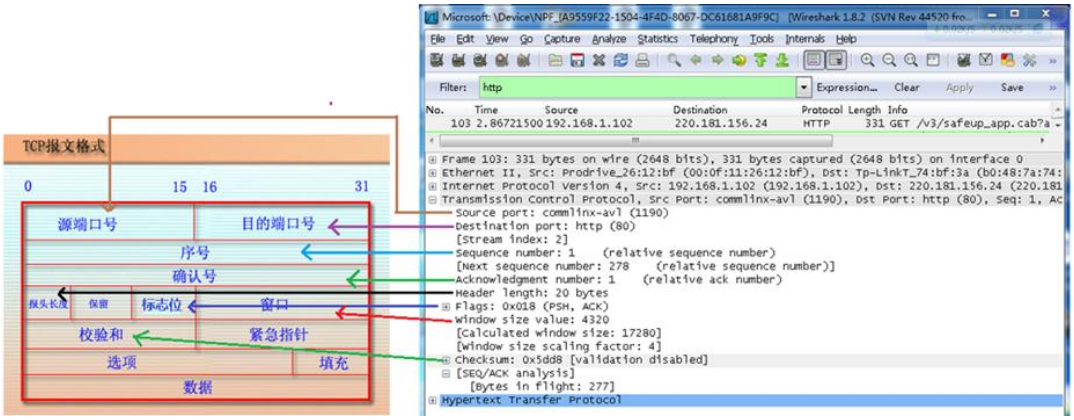
-Ethernetl:数据链路层以太网帧头部信息

-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



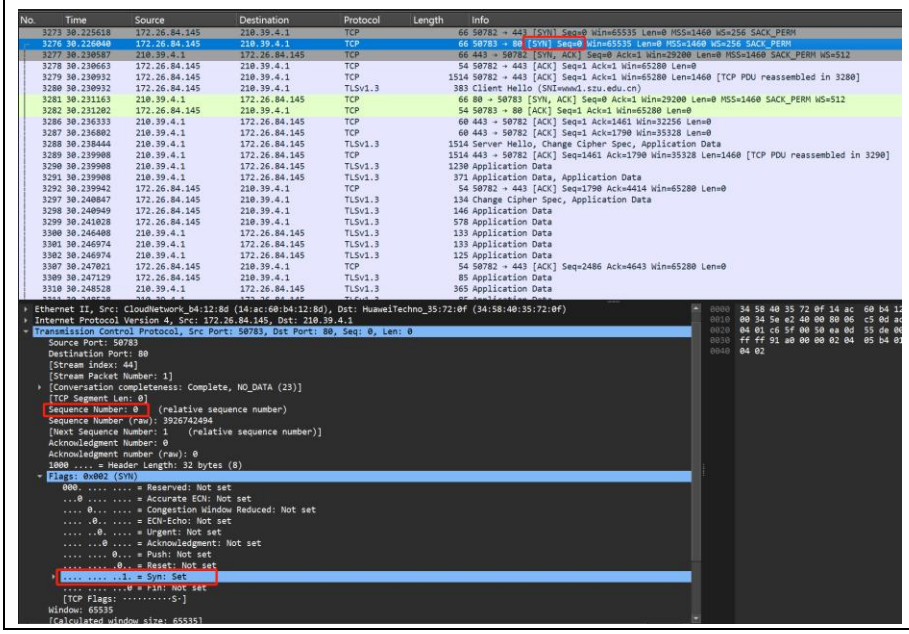
实验过程及内容：

（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）

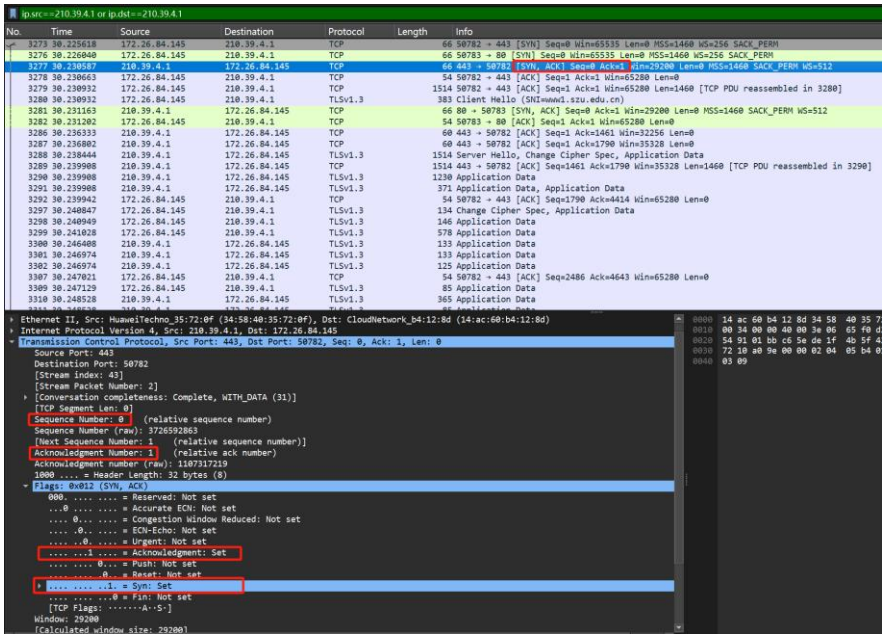
一、tcp 分析

网址 1：www1.szu.edu.cn--三次握手

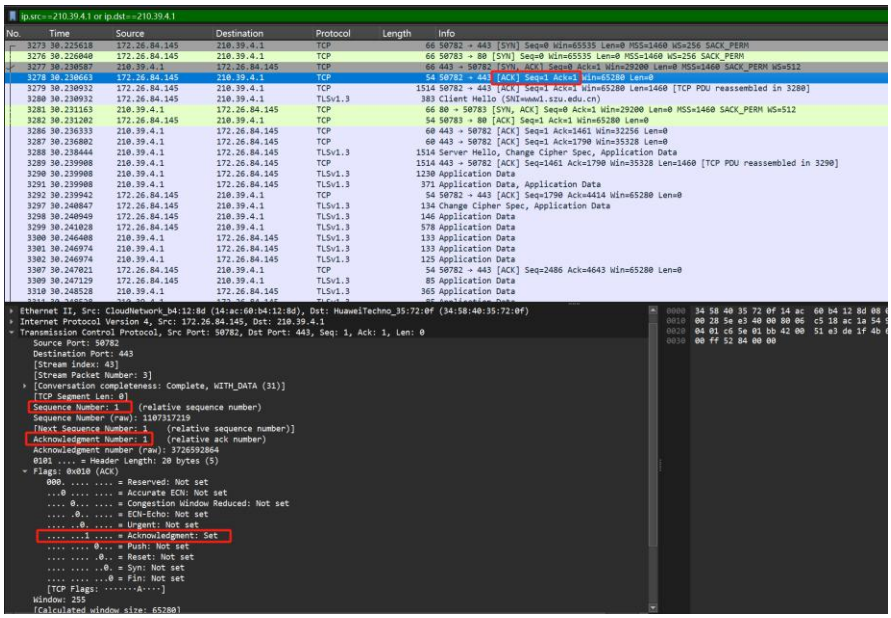
客户端发送连接请求



服务器端接收连接请求

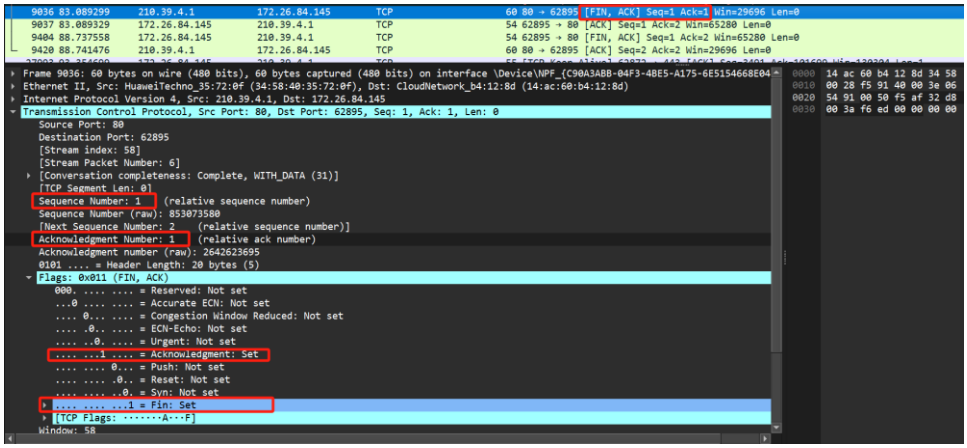


客户端确认

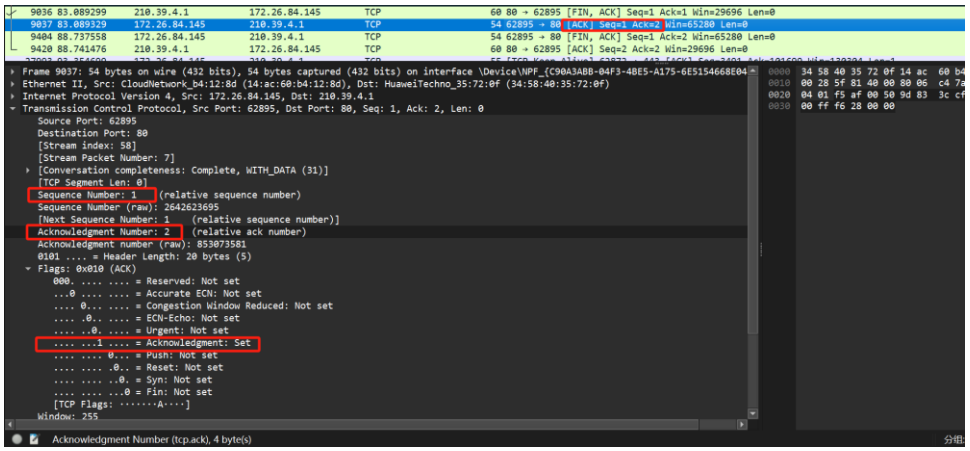


网址 1：www1.szu.edu.cn—四次挥手

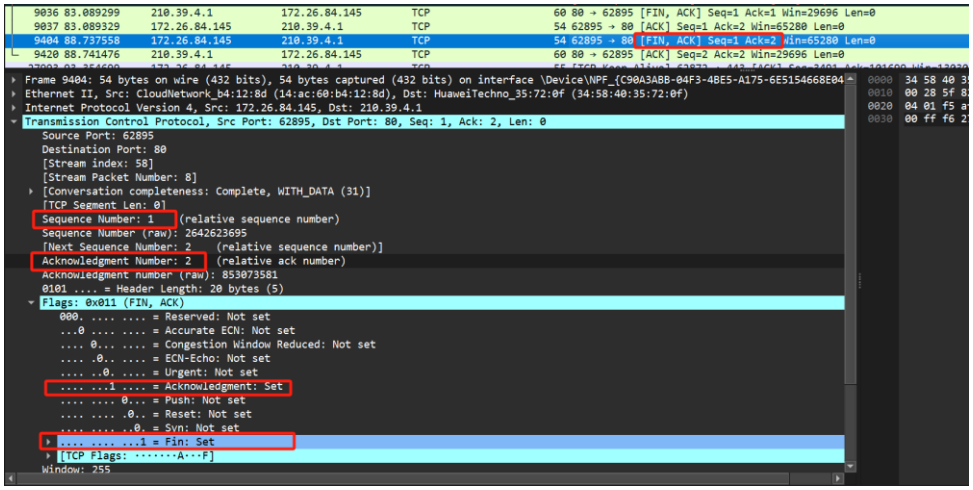
服务端确认断开连接（**在网站静止足够长的时间，会发现服务器端会自动发送断开连接的请求**）



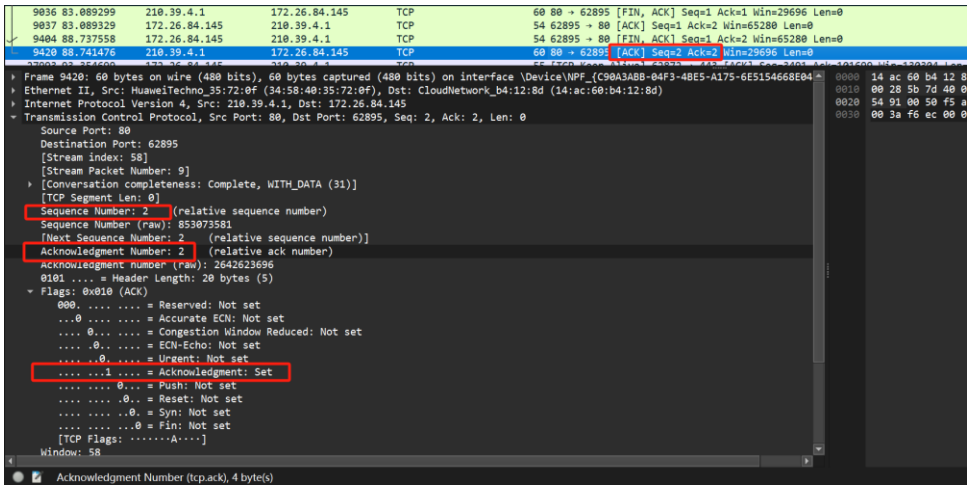
客户端发送 ACK，已确认将要断开连接。但为了确定是否还有信息未发送，此时并未真正断开连接。



客户端已确认信息全部发送完毕，确认断开连接

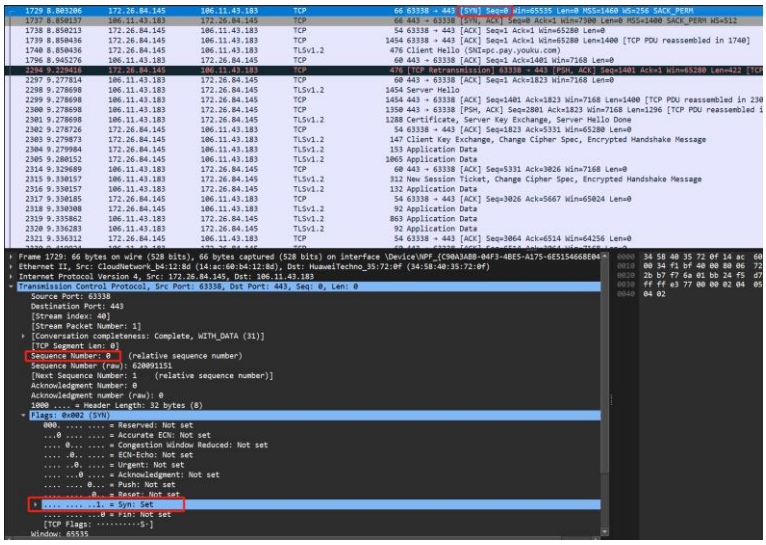


服务器确认断开连接

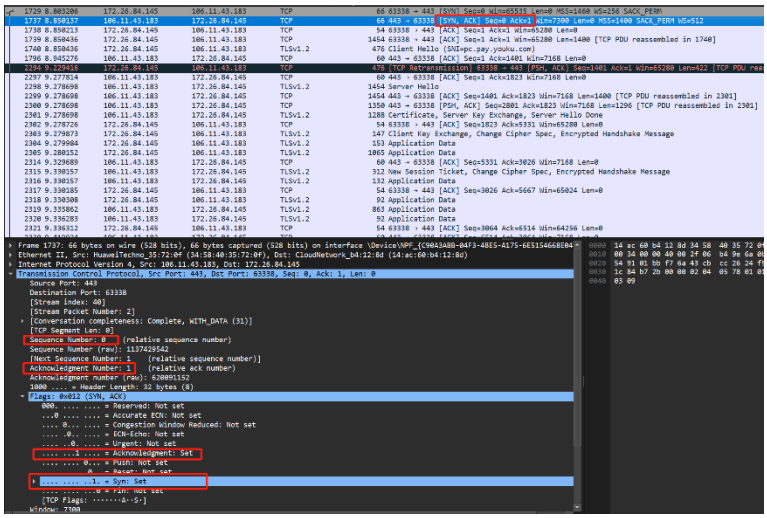


网址 2：www.youku.com --三次握手

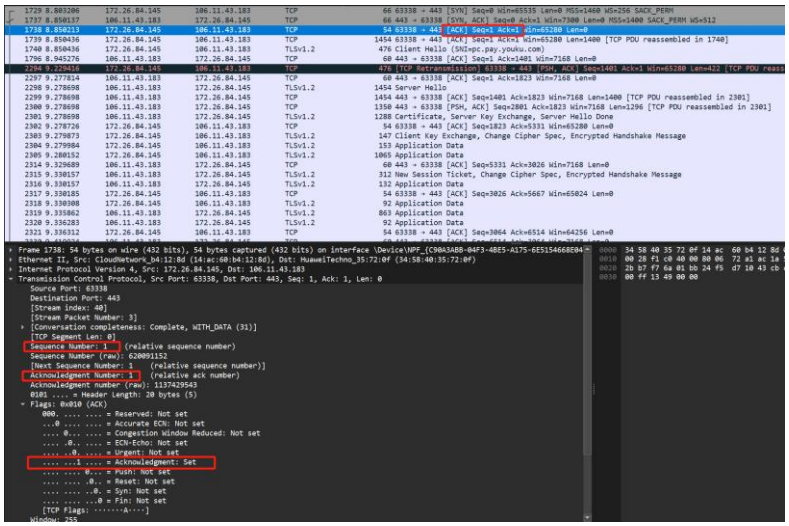
客户端发送连接请求



服务器端接收连接请求

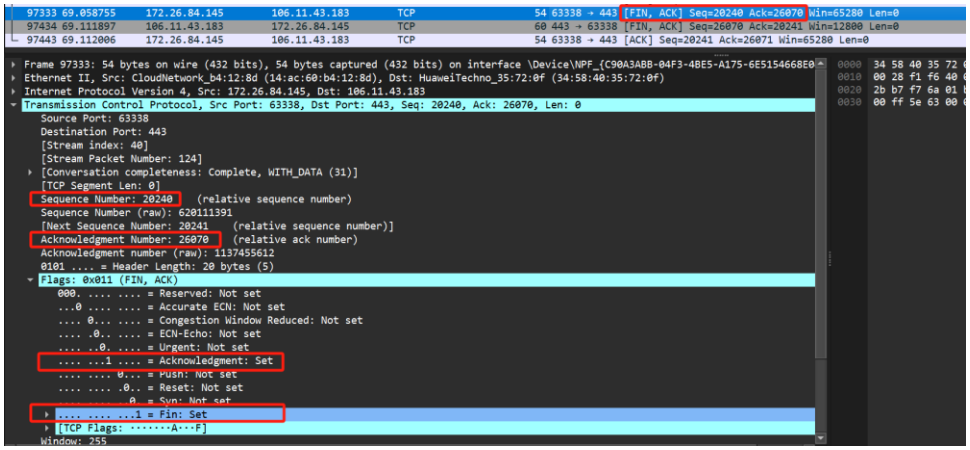


客户端确认

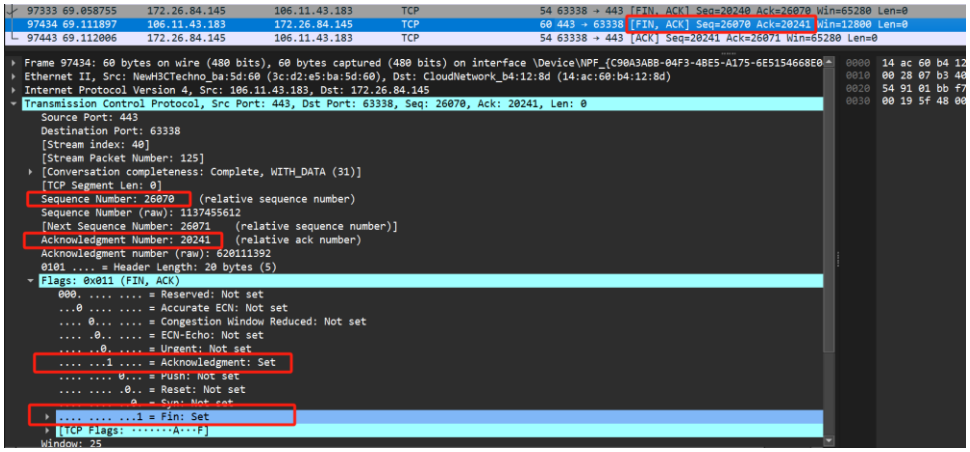


网址 2：www.youku.com –四次挥手（三次）

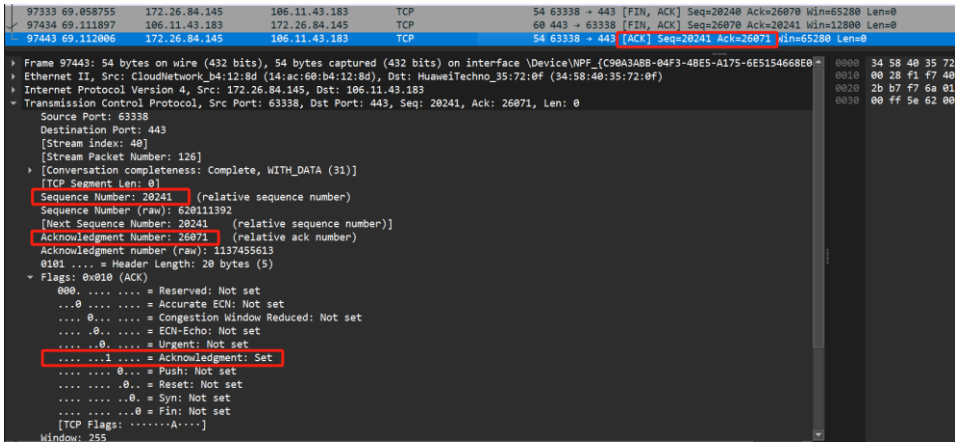
客户端确认断开连接



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。

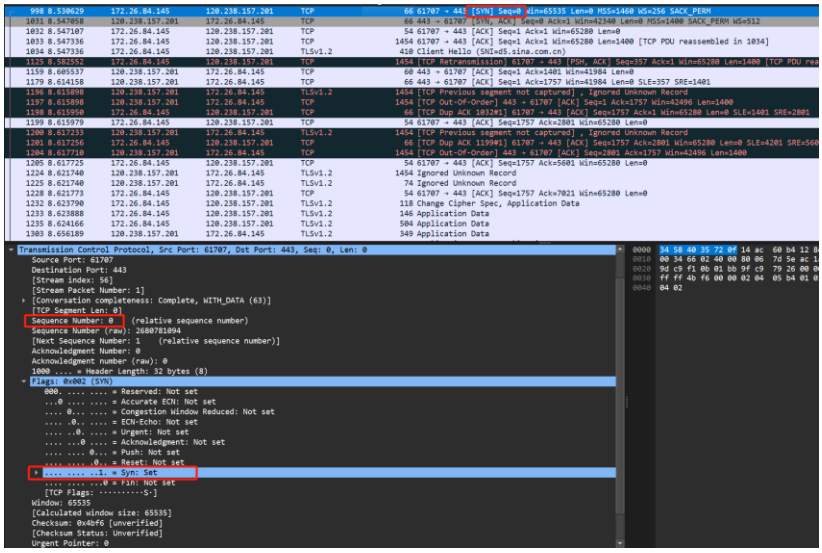


客户端确认断开连接

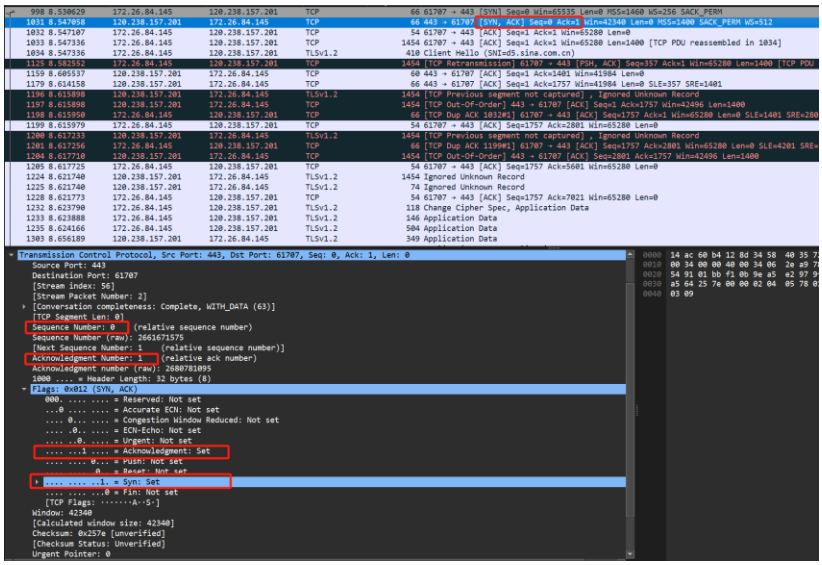


网址 3：www.sina.com.cn --三次握手

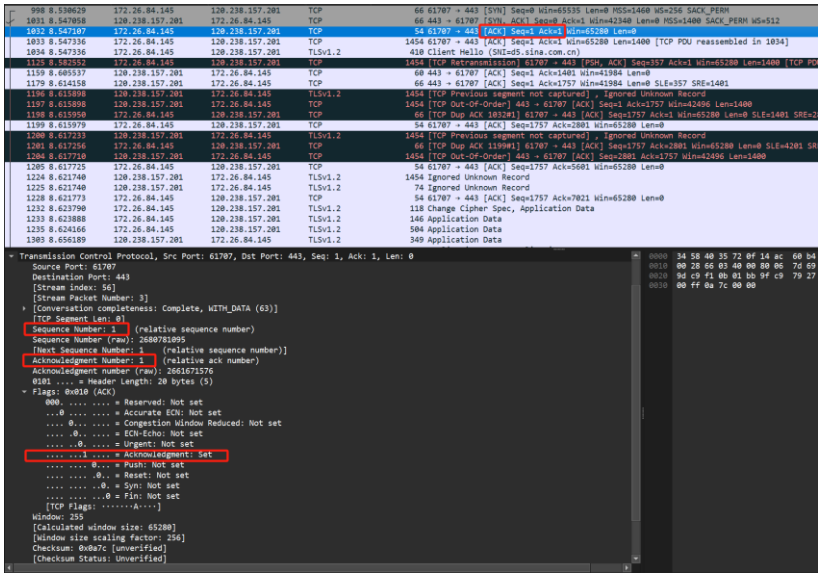
客户端发送连接请求



服务器端确认连接请求

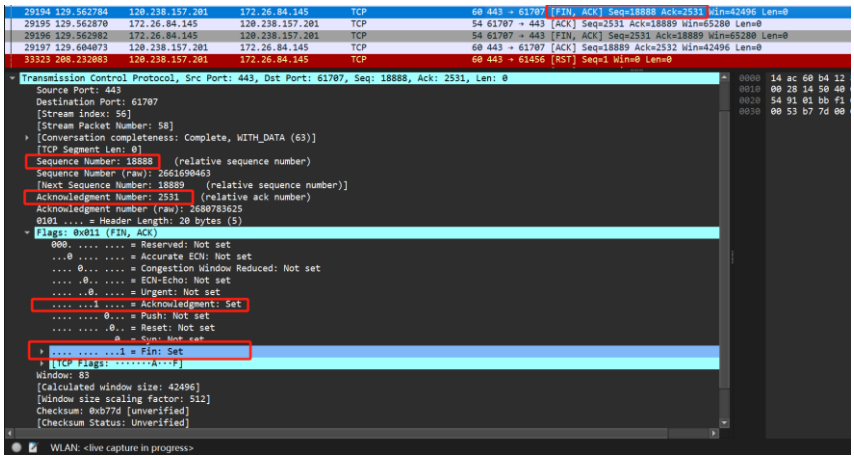


客户端确认

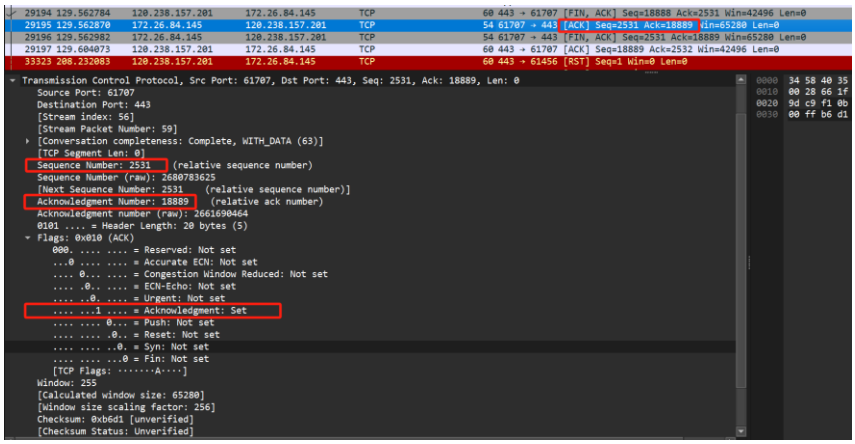


网址 3：www.sina.com.cn –四次挥手（在网站静止足够长的时间，会发现服务器端会自动发送断开连接的请求）

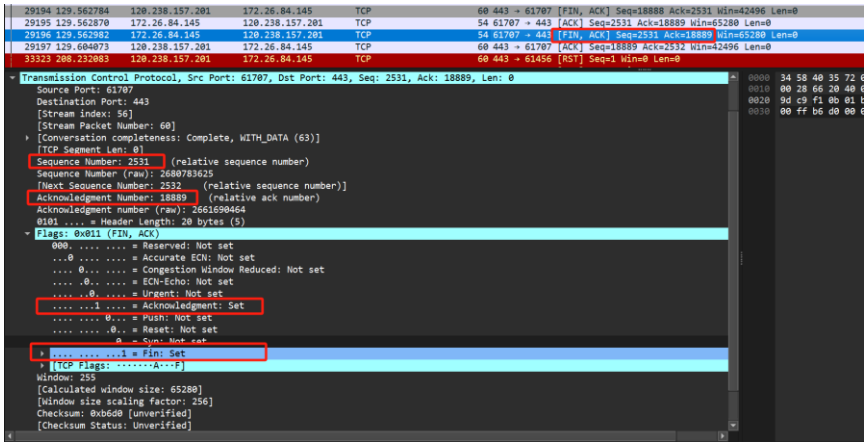
服务器端向客户端发送确认断开连接的请求



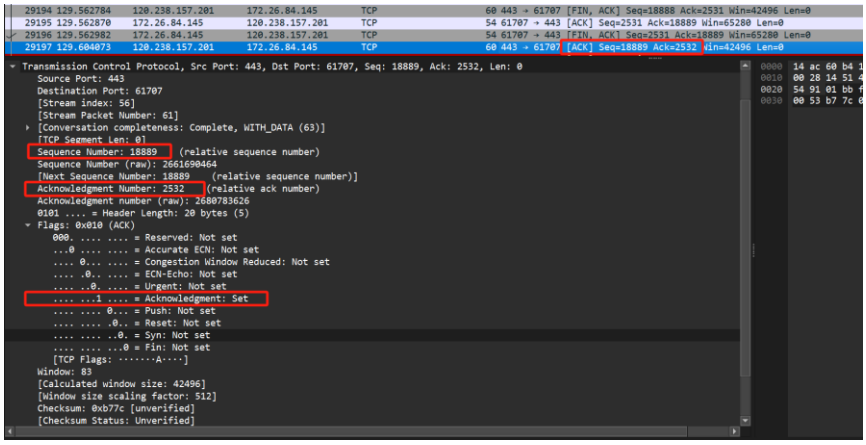
客户端发送 ACK，已确认将要断开连接。但为了确定是否还有信息未发送，此时并未真正断开连接。



客户端已确认信息全部发送完毕，确认断开连接

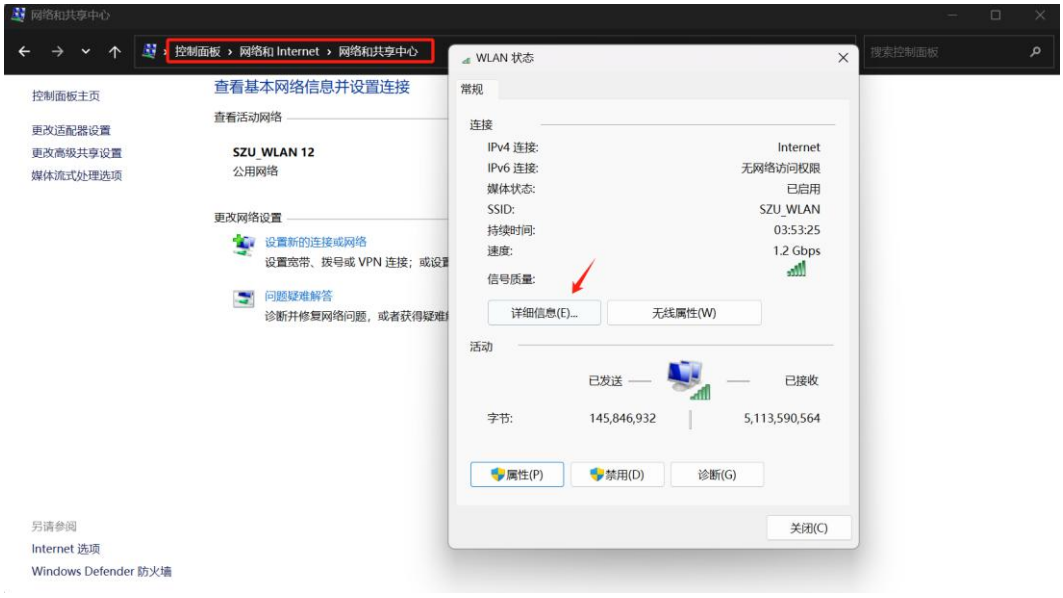


服务器确认断开连接

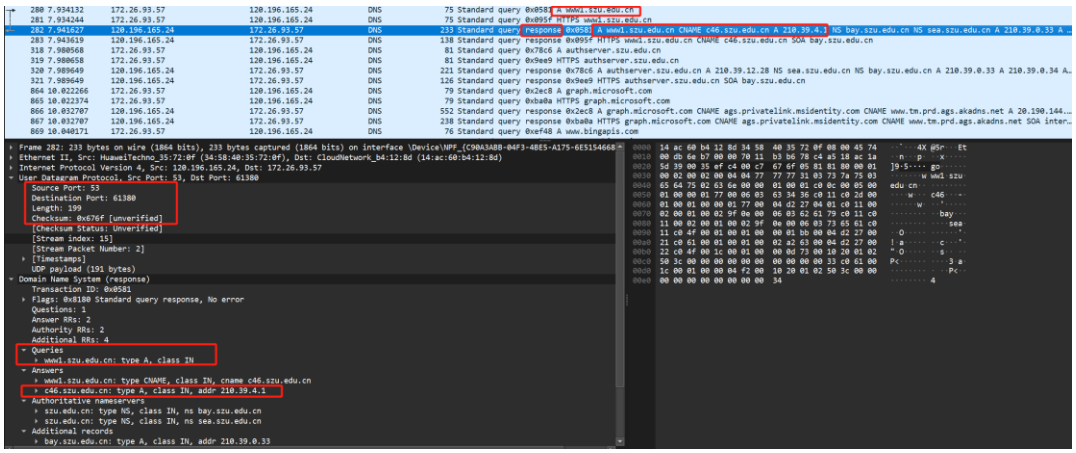


二、三个网址的 udp 和 dns 协议分析

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：

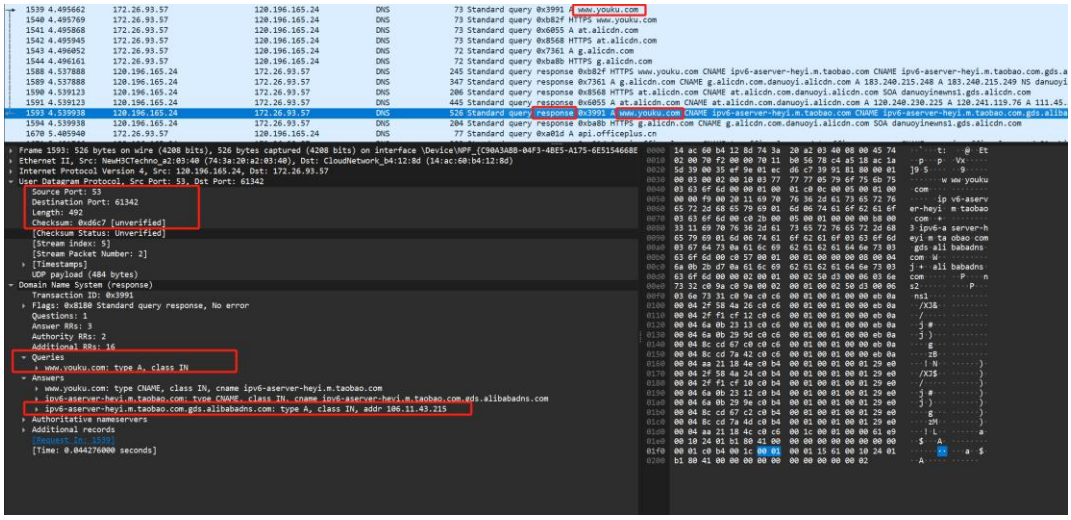
该数据包的源端口=53，目的端口=61380

长度=199，校验码=0x676f

需要转换的网址是：www1.szu.edu.cn

IP 地址是：210.39.4.1

网址 2：www.youku.com



由图可知

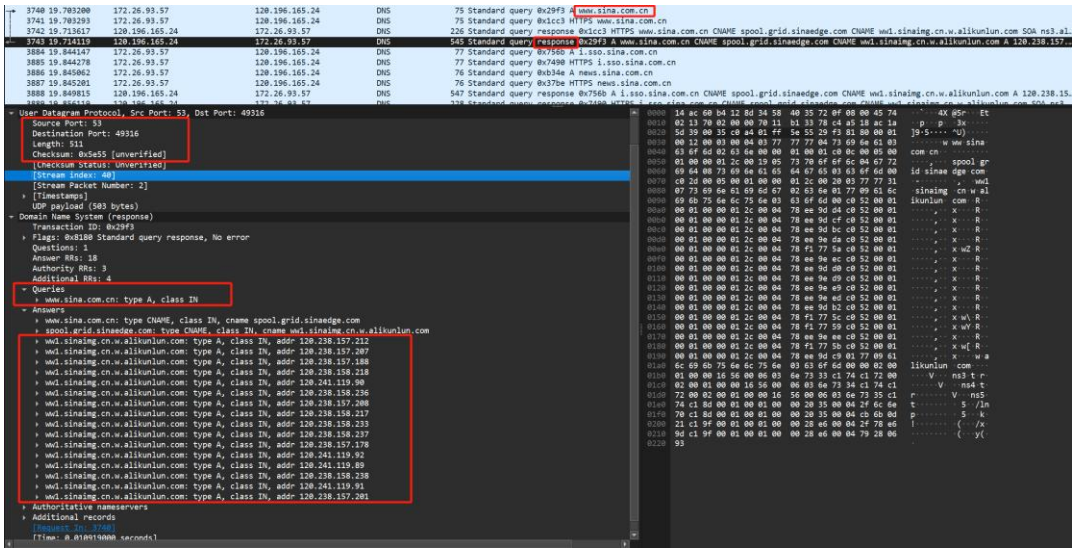
该数据包的源端口（DNS 服务器）=53，目的端口=61342

长度=492，校验码=0xd67

需要转换的网址是：www.youku..com

IP 地址：106.11.43.215

网址 3：www.sina.com.cn



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

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。

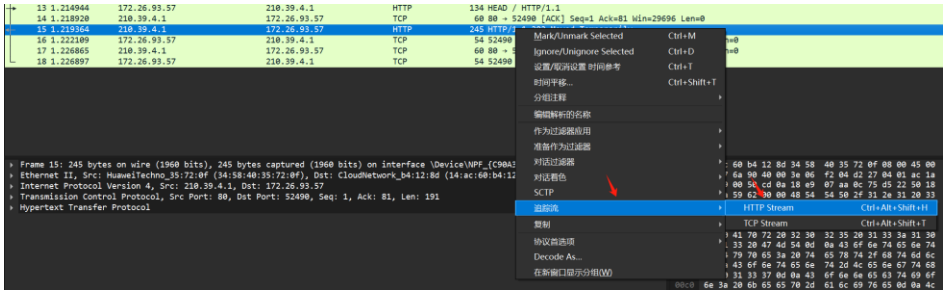
三、三个网站的 HTTP 协议分析

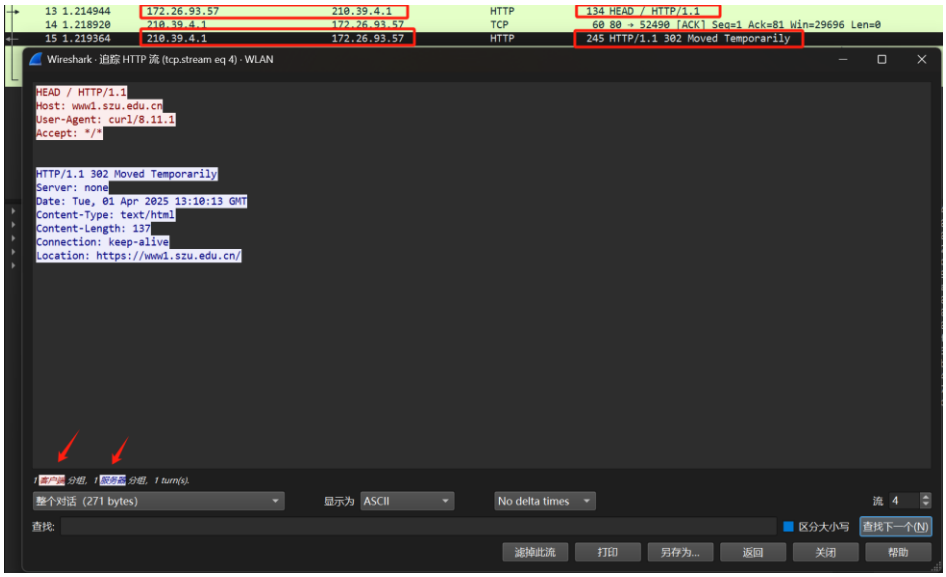
网址 1：www1.szu.edu.cn

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



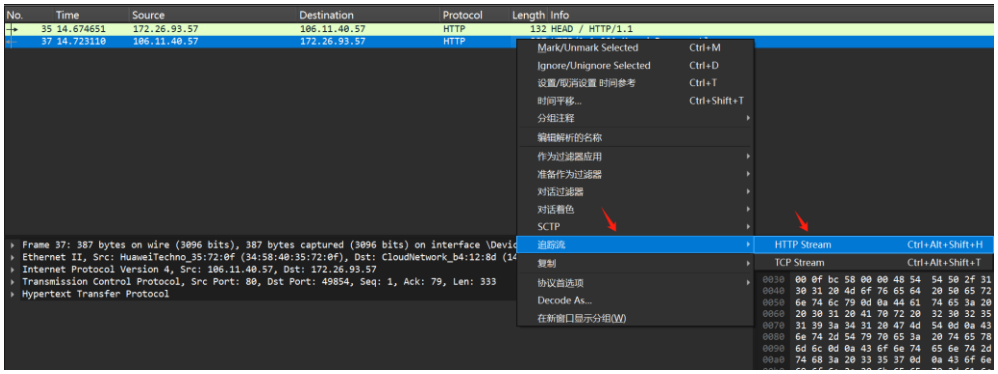


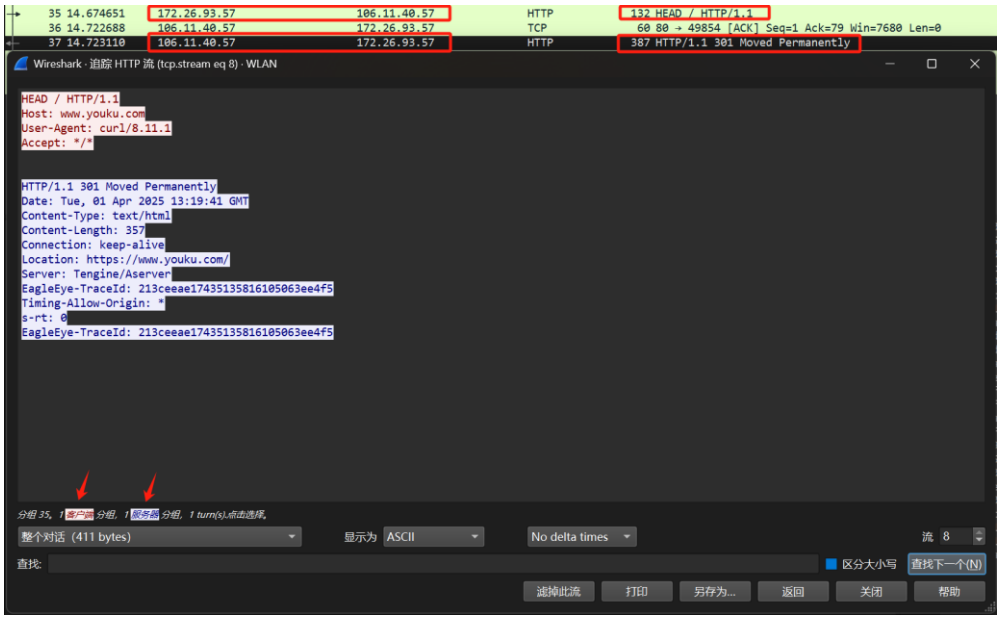
网址 2：www.youku.com

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



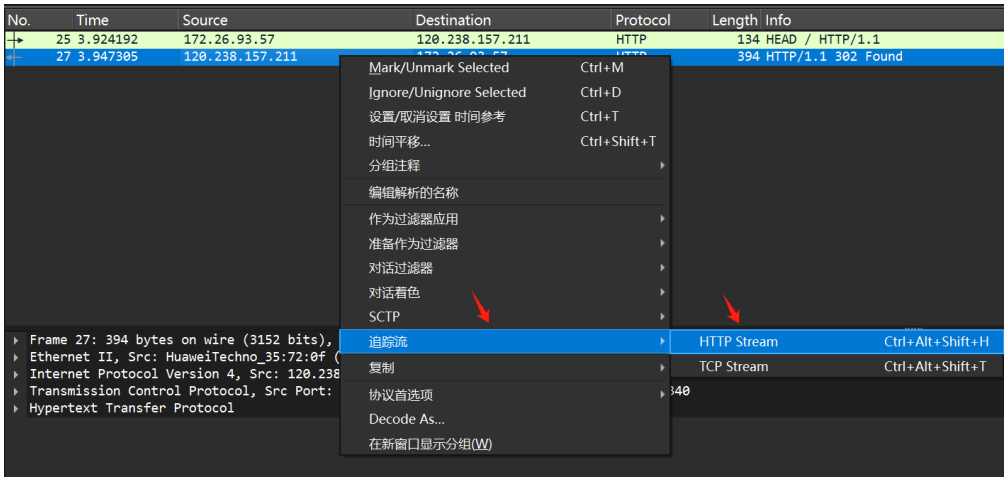


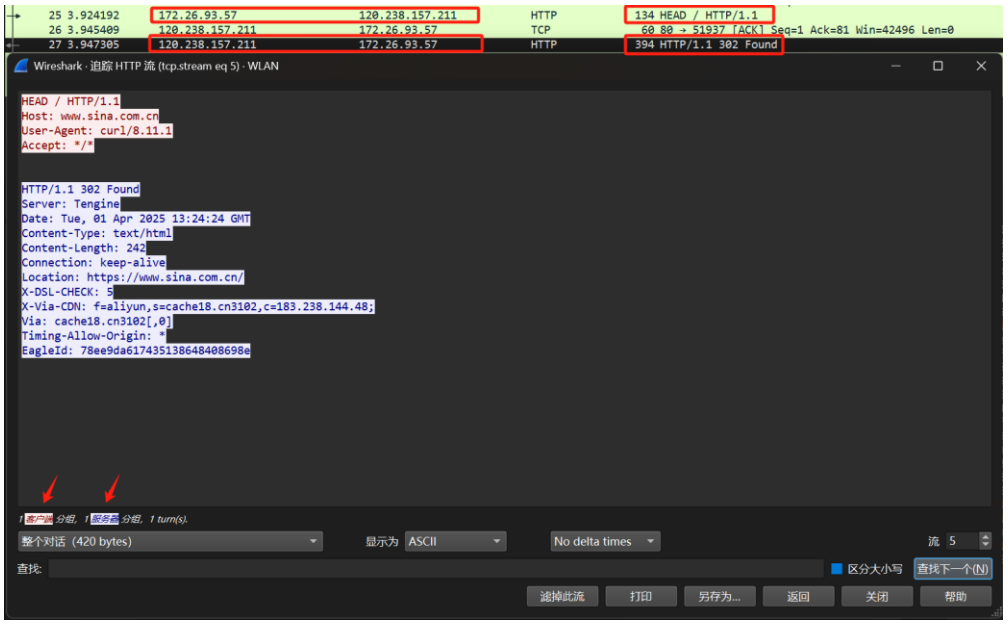
网址 3：www.sina.com.cn

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





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。