Software Define Network Homework1

**作业要求：**

Use Wireshark to understand the process of network communication

–Start your device from a clean state, without an IP address

–Run Wireshark to capture packets

–Use your browser to visit a website (e.g., [www.baidu.com](http://www.baidu.com/))

–Read the captured packets in sequence

Requirement

–Capture as more protocol packets as possible, including but not limited to DHCP, ARP, DNS, HTTP, TCP, UDP, STP, …

–A report that describes the detailed communication process, and what you newly understand after this Wireshark lab

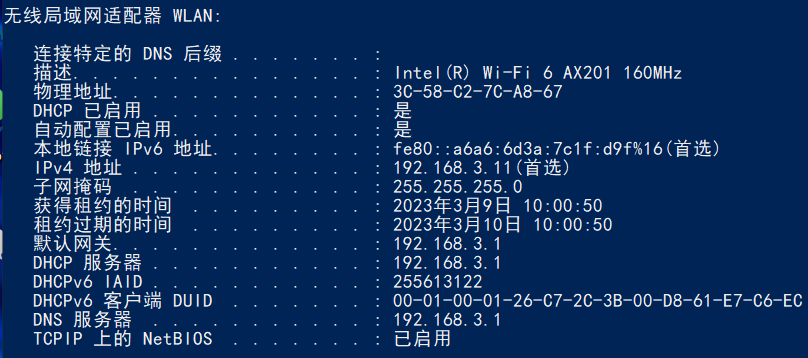
**使用软件：**

Windows Powershell, WireShark

**实验过程：**

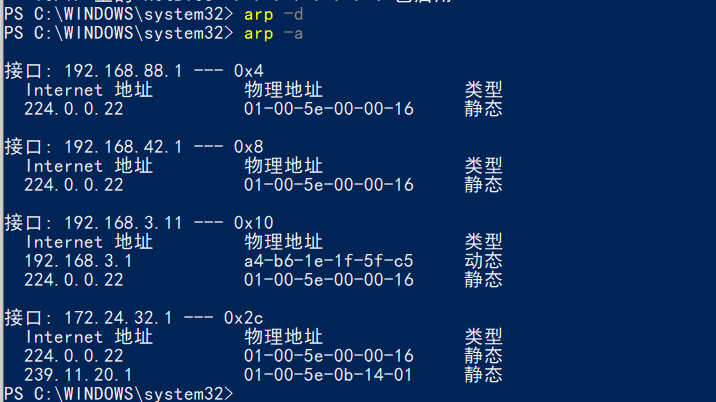
1. 了解本机网络相关信息

打开Windows Powershell，输入指令ipconfig /all，查看本机网络相关信息



可以看到，本机内网IP地址为192.168.3.11，本机默认网关IP地址为192.168.3.1，本机MAC地址为3C-58-C2-7C-A8-67，DNS服务器IP地址为192.168.3.1

在Windows Powershell内输入指令arp -d，清空本机内ARP协议缓存



打开WireShark，开始捕获

在Windows Powershell内输入指令start www.baidu.com，使用浏览器打开网页

等待数秒后，停止捕获

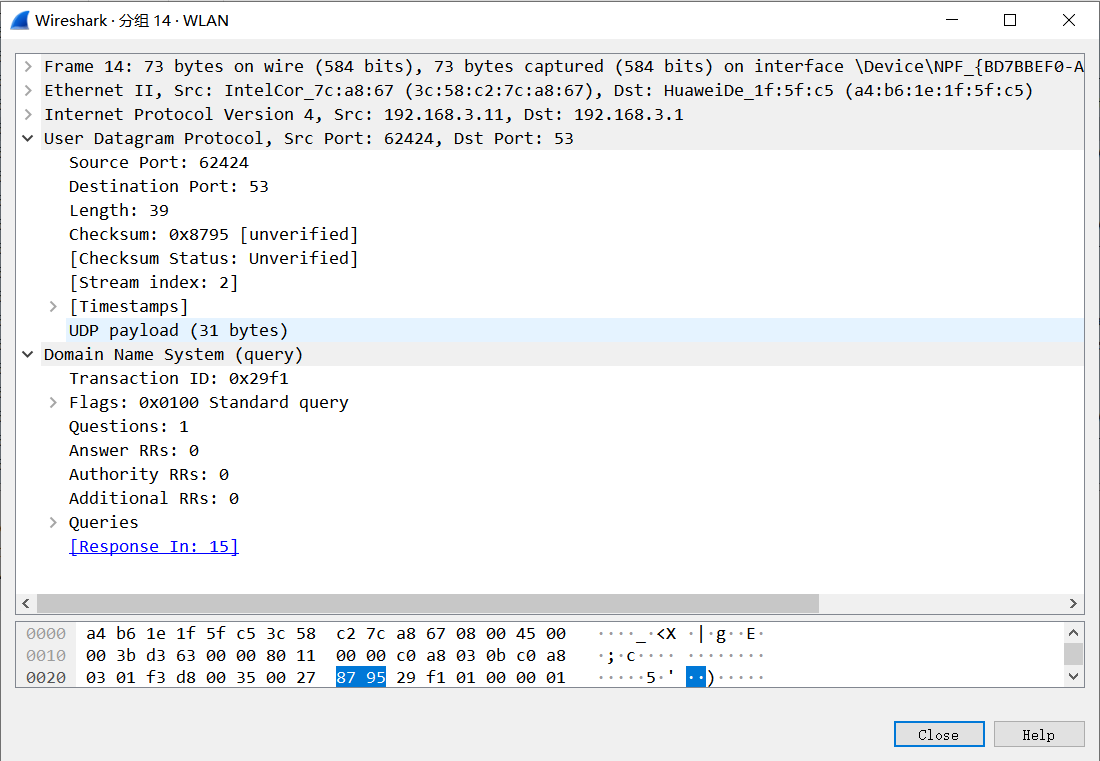
**结果分析：**

最先我们使用DNS协议，向DNS服务器询问目标网站域名www.baidu.com的IP地址。

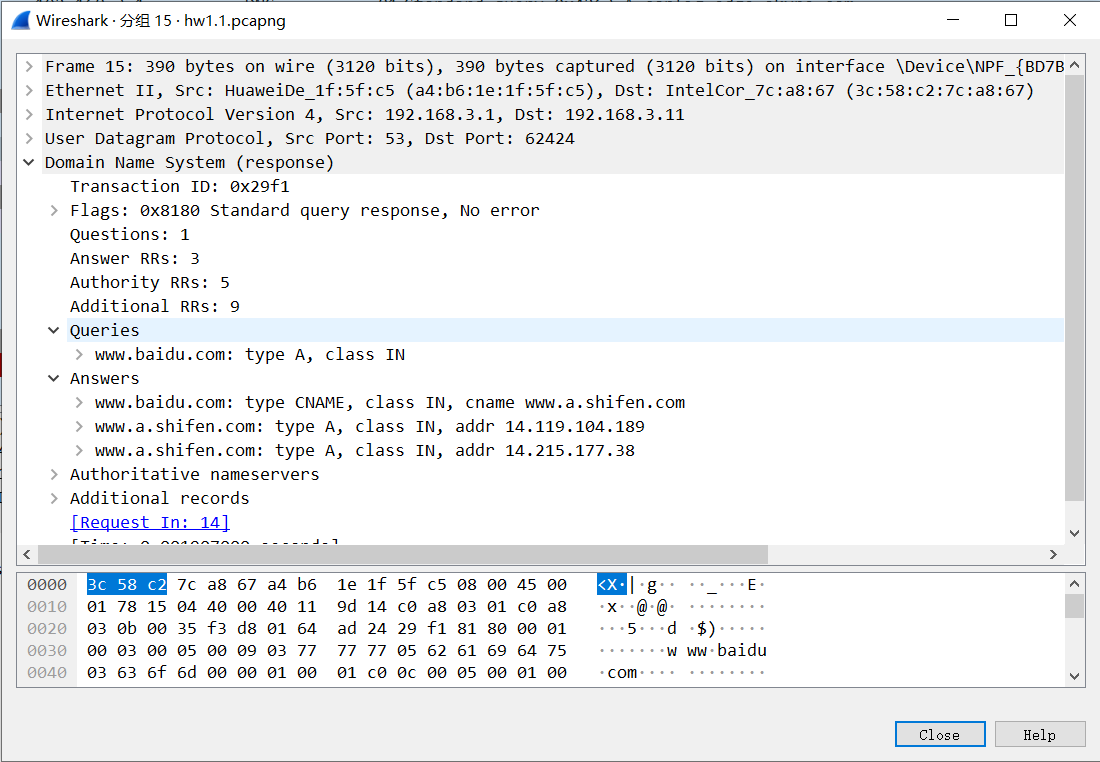


No.14 本机内网IP地址为192.168.3.11，DNS服务器IP地址为192.168.3.1。本机向DNS服务器发出申请，查询目标网站域名对应的IP地址。

No.15 DNS服务器返回结果，目标网站域名为www.baidu.com，别名(CNAME)为www.a.shifen.com，IP地址(A)为14.119.104.189与14.215.177.38。



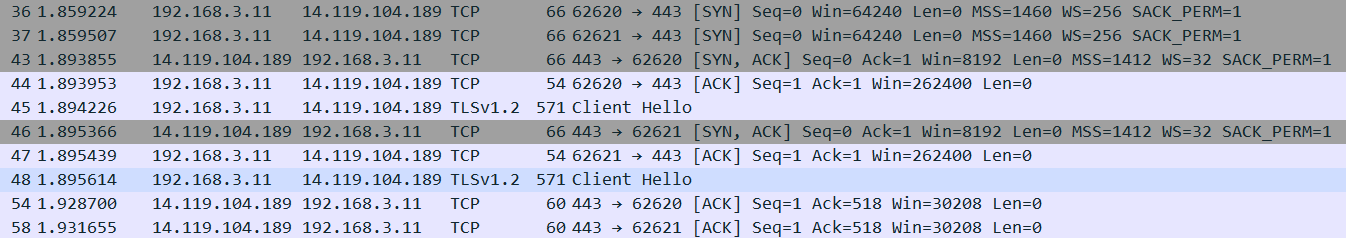
同时我们打开序号为14的报文，可以看到，DNS域名解析服务是基于UDP协议的。UDP源端口为62424，目的端口为53，校验和为0x8795。



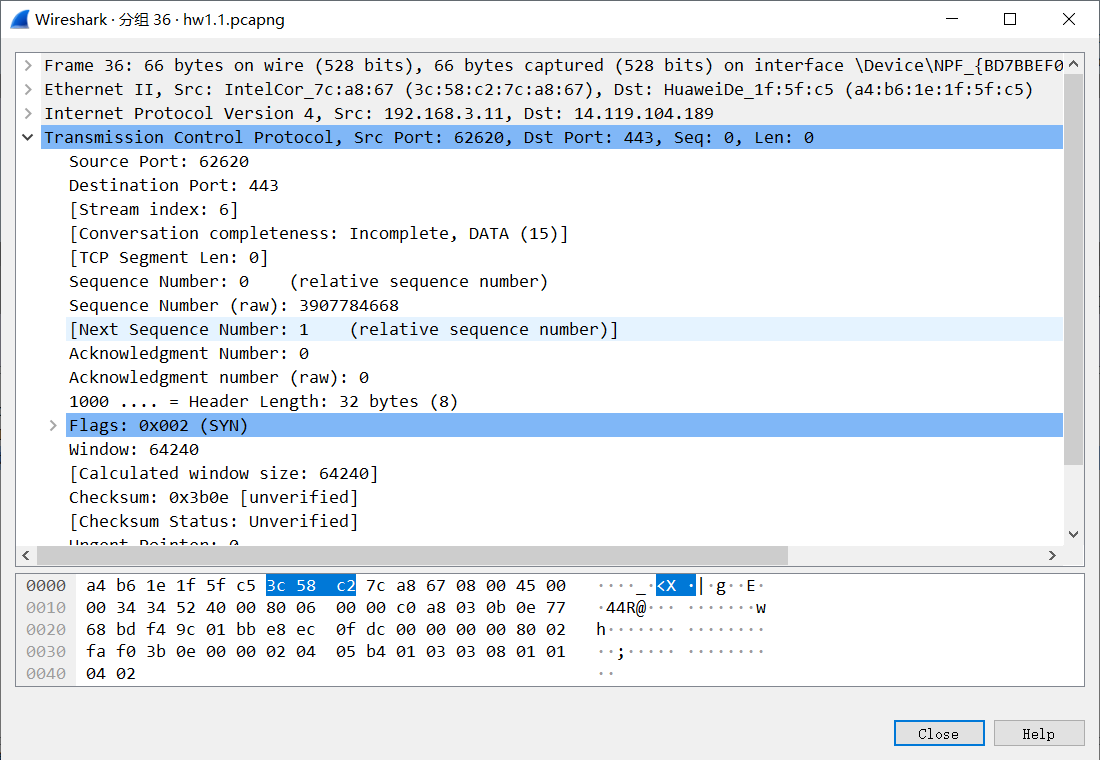
我们打开序号为15的报文，这是DNS服务器回复我们DNS查询请求的报文，

目标网站域名为www.baidu.com，别名(CNAME)为www.a.shifen.com，IP地址(A)为14.119.104.189与14.215.177.38。

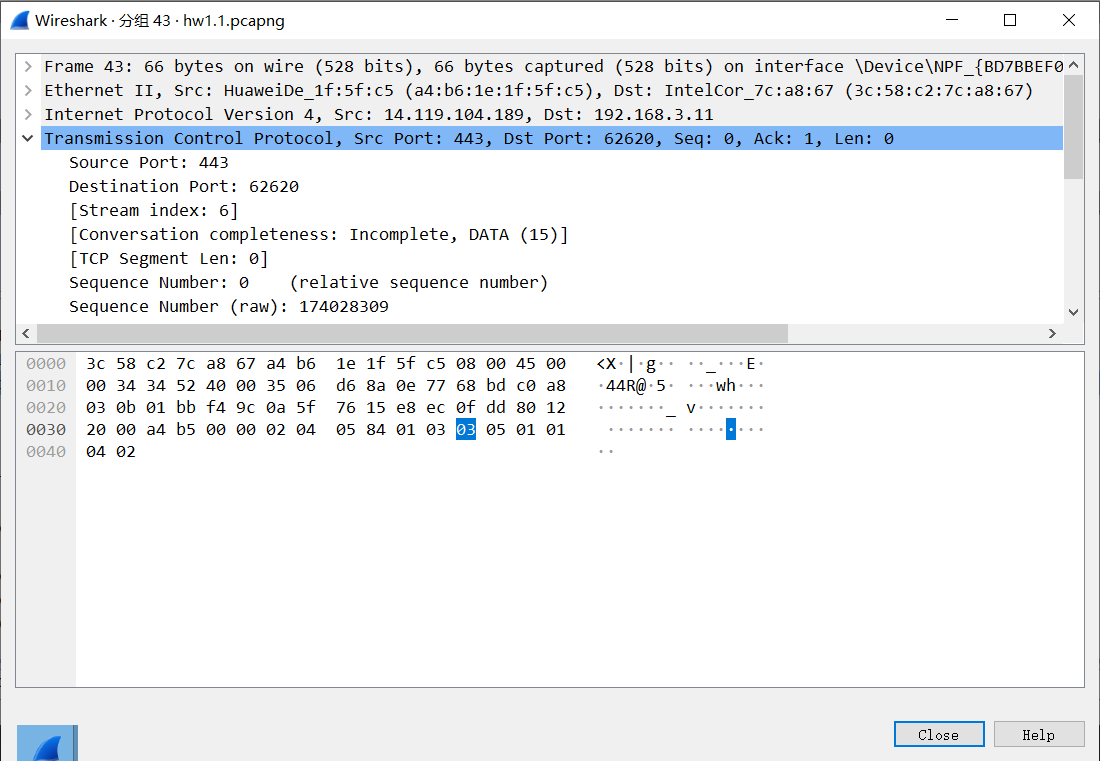
随后使用TCP协议，三次握手建立连接。



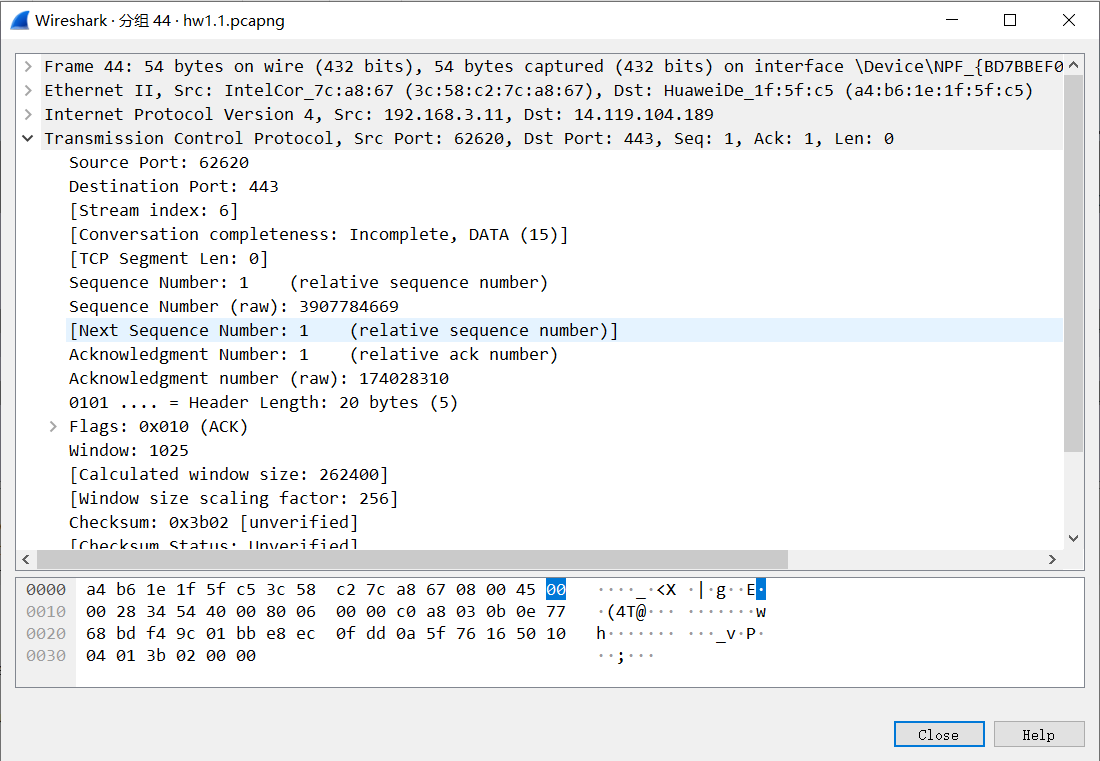
序号为36，43，44的报文是本机通过端口62620与目标网站建立TCP连接三次握手的报文，序号为37，46，47的报文是本机通过端口62621与目标网站建立TCP连接三次握手的报文。



No.36 本机向目标网站发出建立TCP连接的申请，SYN = 1，Seq = 0，Len = 0，是本机申请建立连接的请求报文。源端口为62620，目的端口为443。



No.43 目的网站回复本机发出的建立连接的申请，SYN = 1，Seq = 0，ACK = No.36.Seq + 1 = 1，是服务器回复本机的报文。

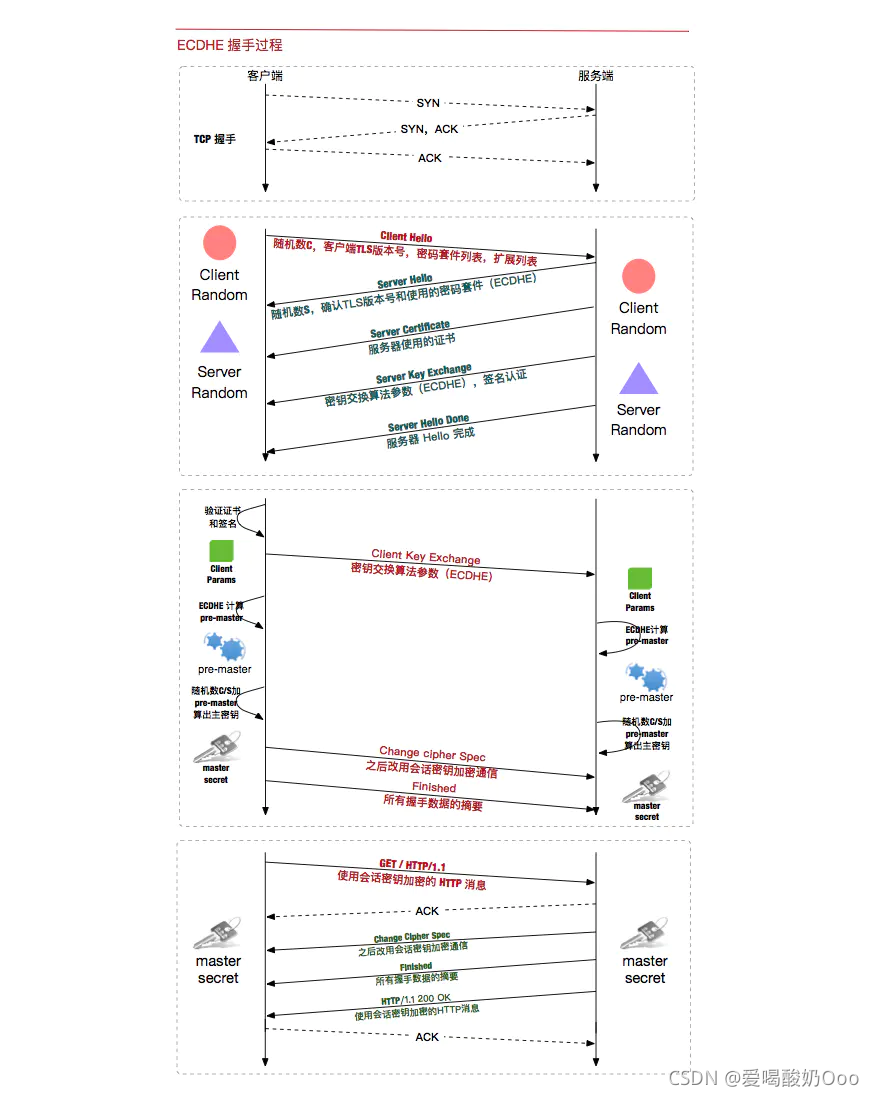


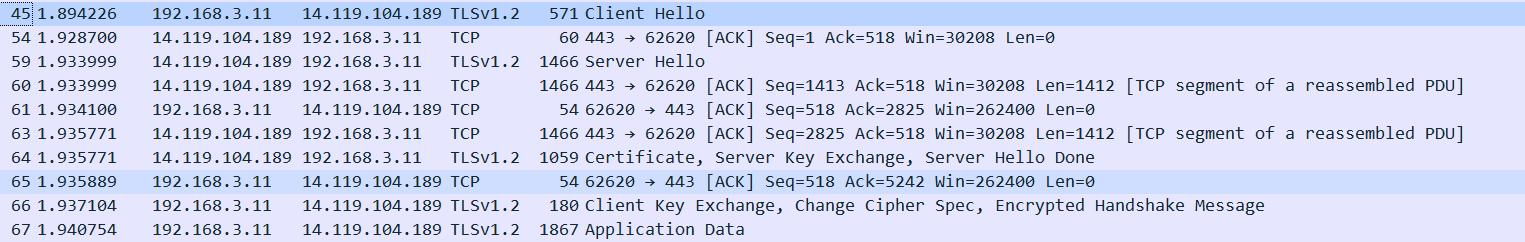
No.44 本机回复目的网站的报文，Seq = 1，ACK = No.43.Seq + 1 = 1。

到此为止，TCP通过三次握手，建立连接。

随后使用TLS协议建立安全的传输层连接。

TLS一共出现过三个版本，1.1、1.2和1.3，目前最广泛使用的是 1.2。在 TLS 1.2 的握手中，一般是需要4次握手，先要通过Client Hello （第1次握手）和Server Hello（第2次握手）消息协商出后续使用的加密算法，再互相交换公钥（第3和第4次握手），然后计算出最终的会话密钥。





序号为45，59，64，66，67的报文是TLS协议的报文。

No.45 本机对目的网站发出Client Hello报文，进行第一次握手。

No.59 目的网站服务器发出Server Hello报文，进行第二次握手。

No.64 目的网站服务器发出Certificate，使用证书证实自己的身份；再发出Server Key Exchange，告知自己的密匙交换算法参数和签名认证；最后服务器发出Server Hello Done，完成服务器Hello过程。

No.66 本机发出Client Key Exchange，告知自己的密匙交换算法参数；再发出Change Cipher Spec，告知服务器之后改用密匙加密通信；最后本机发出Encrypted Handshake Message，对前面的信息做个摘要，验证对称钥匙是否可用。

No.67 本机与目的网站服务器开始进行应用数据传输，基于加密后的通信，建立HTTP-over-TLS，即HTTPS。

在网关接收缓冲区满之后，网关将要把接收道德数据转发给本机，需要使用ARP协议。

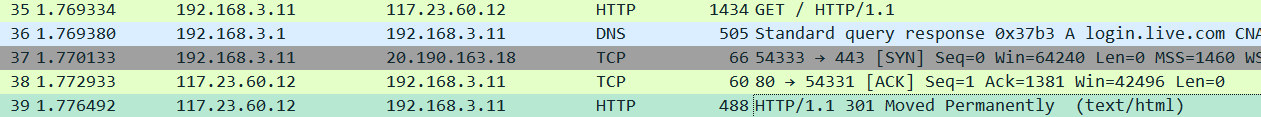


序号为530和531的报文是ARP协议报文。

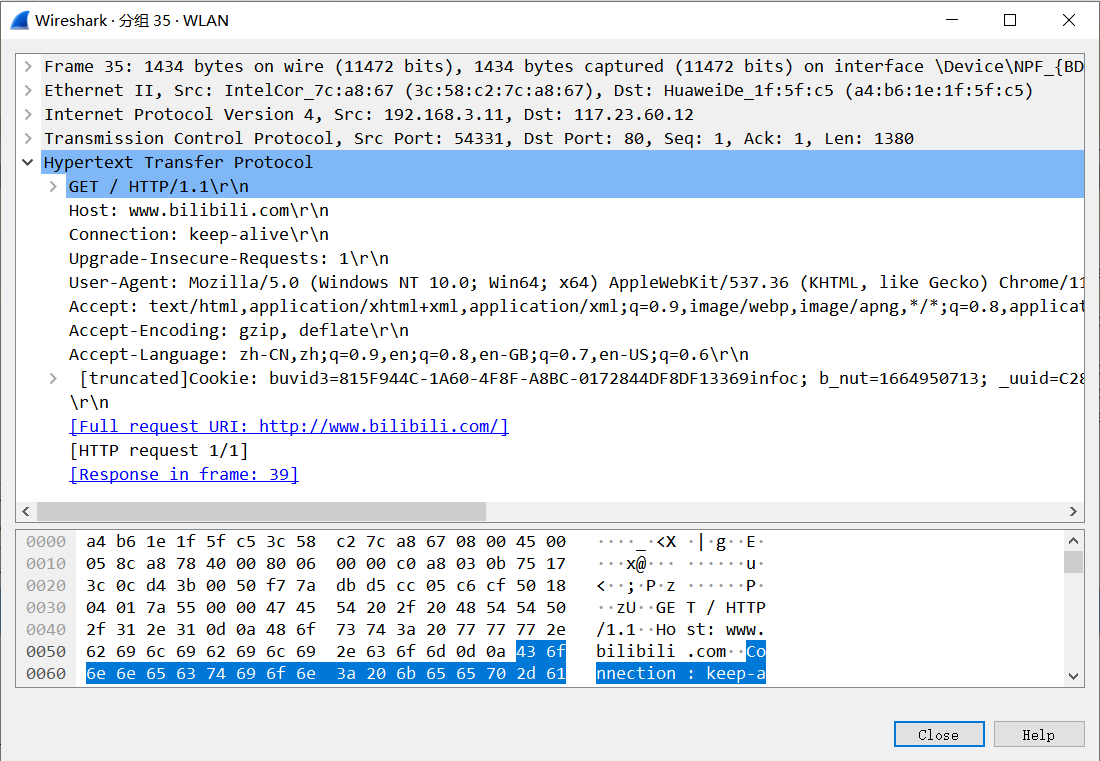
No.530 网关询问192.168.3.11（本机）的MAC地址，并要求本机回复给网关192.168.3.1。

No.531 本机回复网关，本机的MAC地址为3C-58-C2-7C-A8-67。

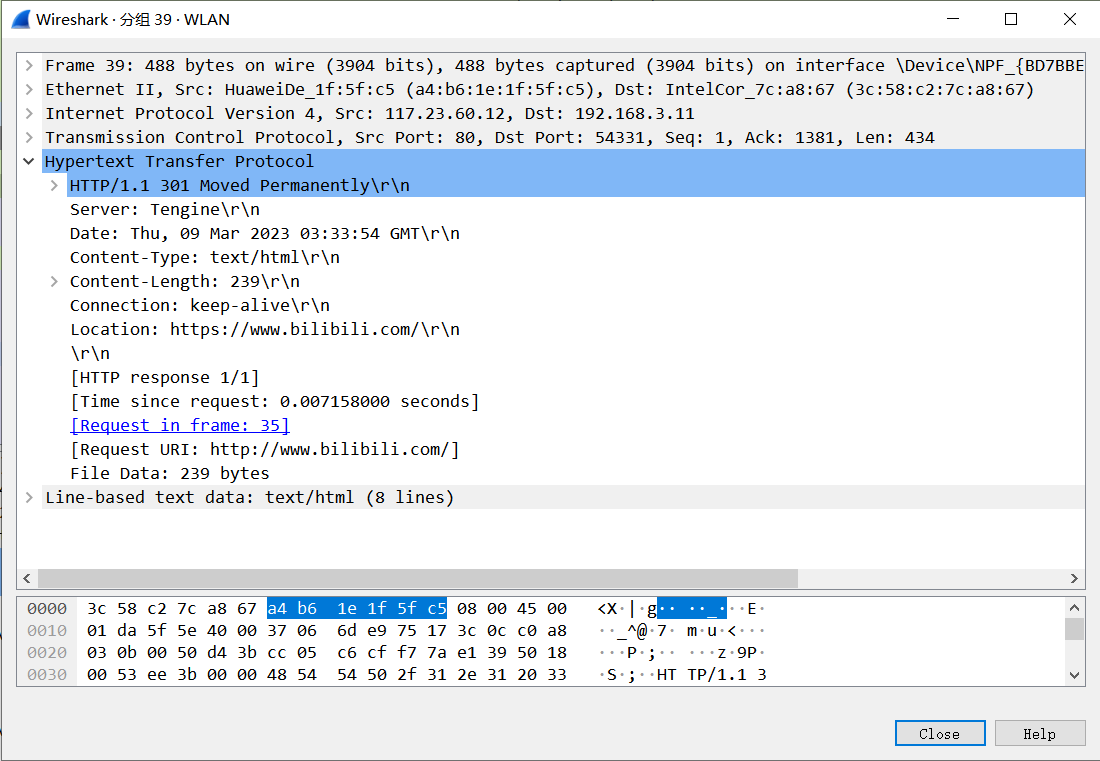
我们访问另一个网站www.bilibili.com，开始捕获，捕获到HTTP协议数据包。



序号为35和39的报文基于HTTP协议。



No.35 本机对目的网站的服务器发出HTTP请求报文，调用GET方法，HTTP协议版本为1.1，目的主机域名为www.bilibili.com，连接类型为Keep-alive。



No.39 目的网站服务器回复HTTP回复报文，状态码为301，Move Permanently，请求的网页已永久移动到新位置。服务器返回此响应（对 GET 或 HEAD 请求的响应）时，会自动将请求者转到新位置。