**计算机网络课程实验报告**

一、基本信息

实验题目：网络抓包与协议分析 完成人：09020328 王亮

报告日期：2022年11月1日

二、实验目的

通过实验，掌握 Wireshark 网络抓包工具的使用方法，在真实网络环境下捕 捉和分析网络应用数据包，掌握 HTTP、DNS、TCP、UDP 等应用层及传输层协 议报文的结构，深入理解相关协议的特点与工作原理，培养学生网络故障检测、 网络性能改进和网络安全分析的能力。

三、实验内容

1. 学习 Wireshark 网络抓包工具的基本操作，掌握捕获过滤器和显示过滤器的使用方法。

2. 访问 Web 网站并捕捉数据包，分析 HTTP 协议报文格式和交互过程，观察 TCP 协议报文格式，分析 TCP 协议采用的可靠传输机制、以及 TCP 连接建立和关闭的交互过程。

3. 使用 nslookup 命令查询域名并捕捉数据包，分析 DNS 协议报文格式和交互 过程，同时分析UDP协议报文格式和交互过程。

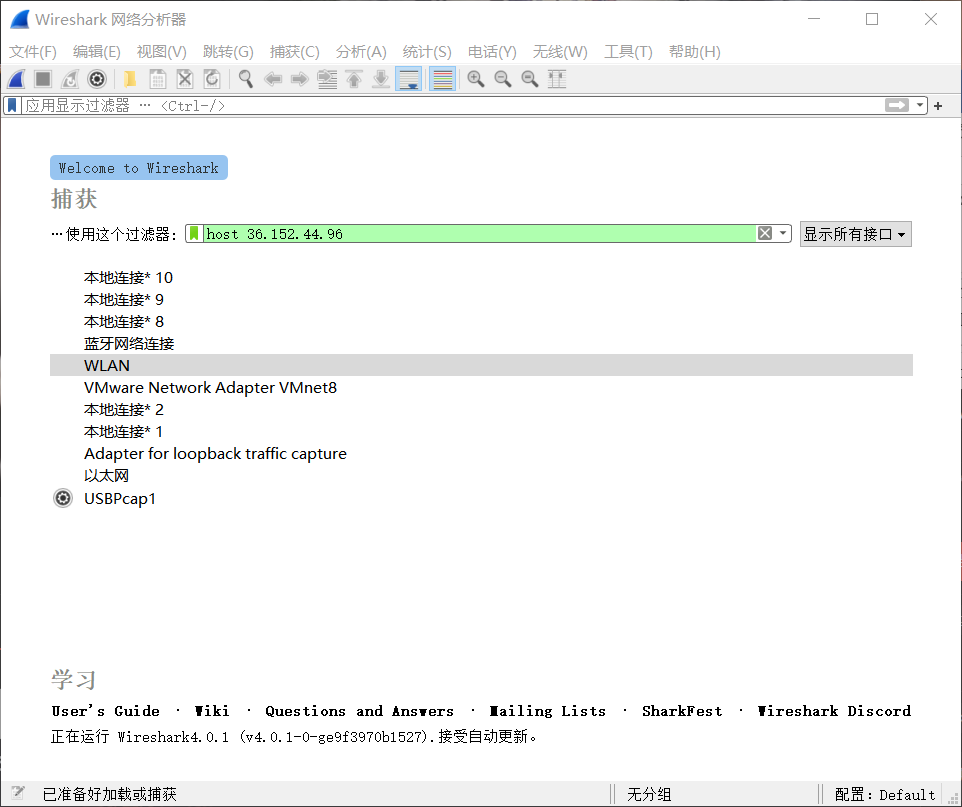
四、实验步骤

一、捕获过滤器和显示过滤器的使用：

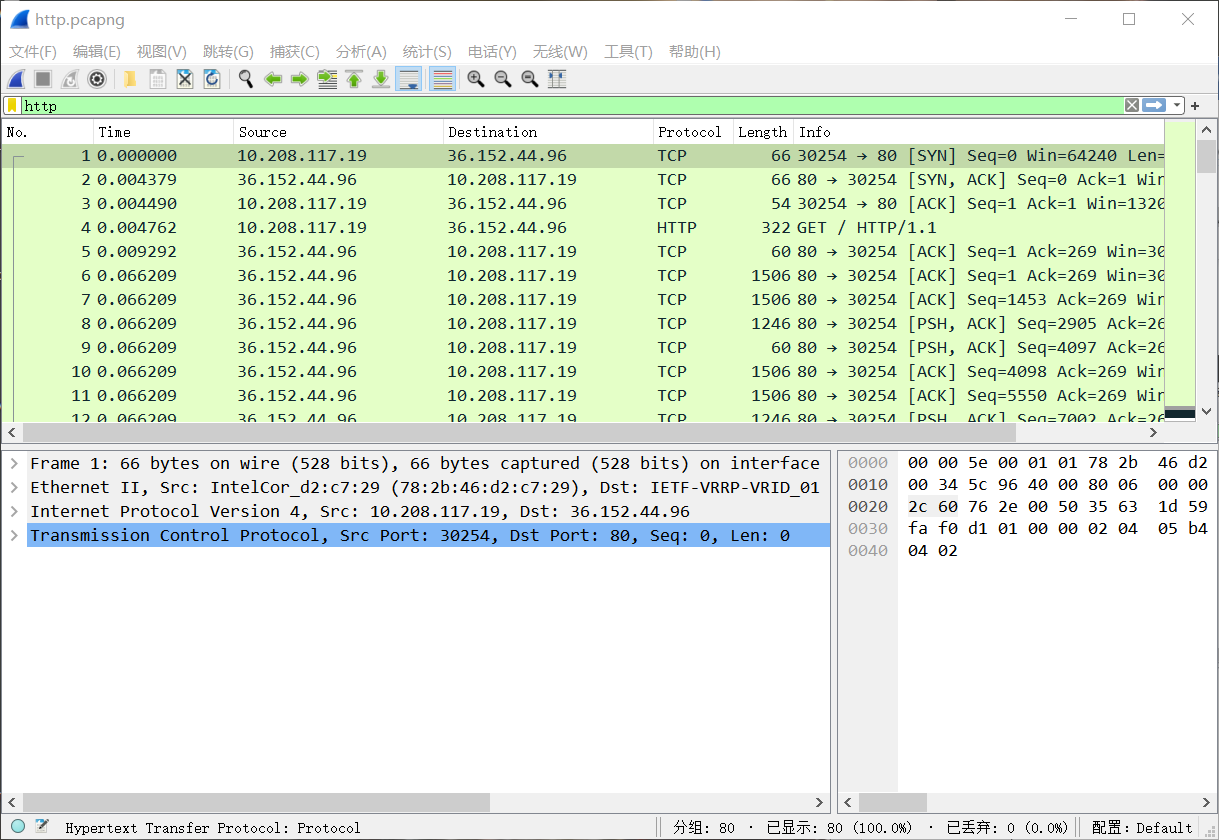
通过ping命令获取baidu的ip地址，用于缩小实验捕获范围。



如图填写捕获过滤器，这样我们只会捕获与此ip地址的交互数据

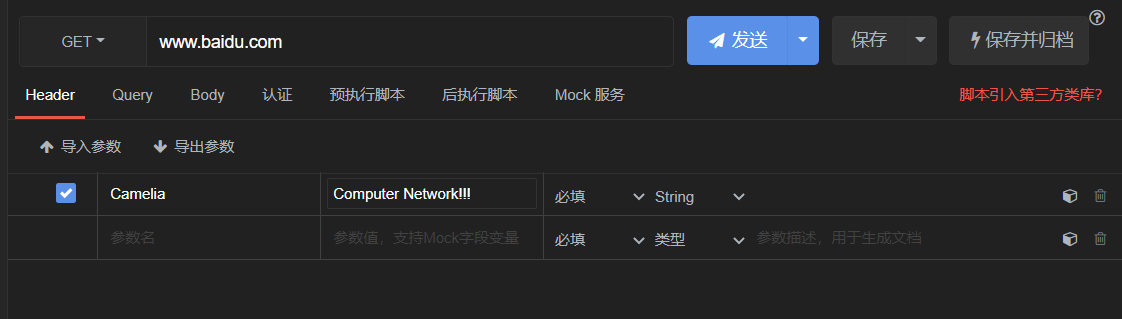


填写显示过滤器，仅显示接下来实验需要用到的数据

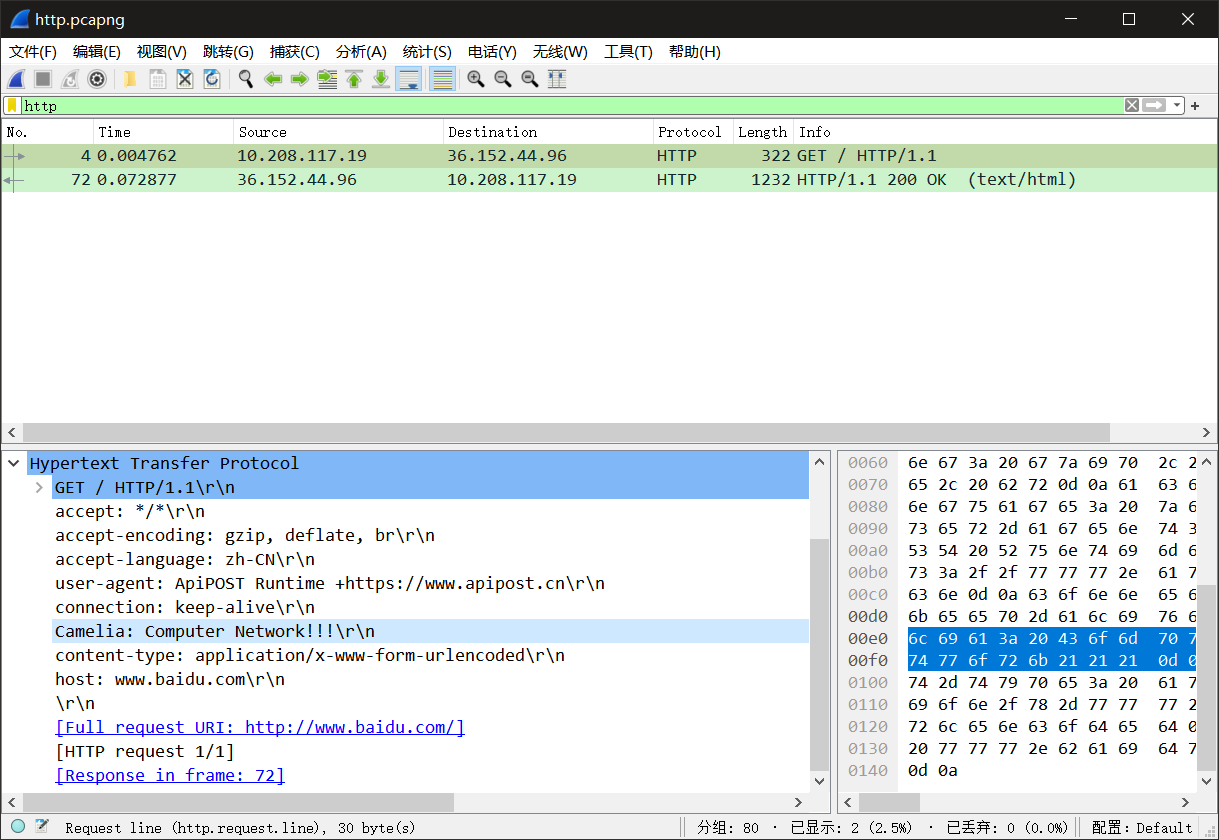


二、分析 HTTP 协议报文格式和交互过程

填写一些特殊标识，用于定位我们实验发送的请求，利用接口调试工具向baidu发送http请求



如图，可见请求已经正确发送出去



可对照下图进行HTTP请求分析

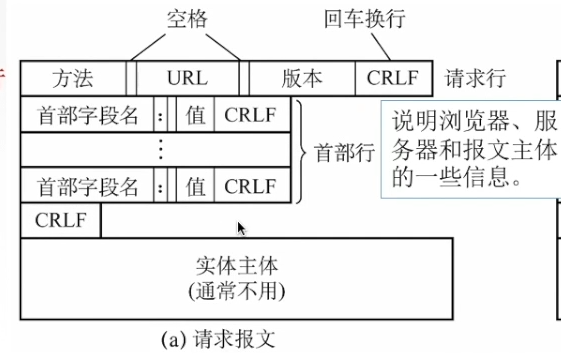
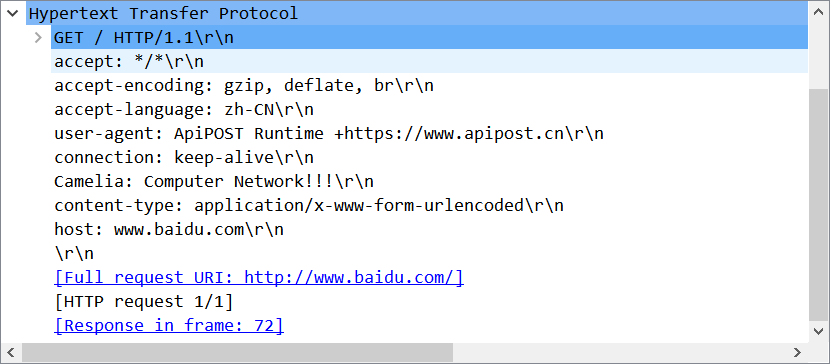
GET->方法

/ -> URL

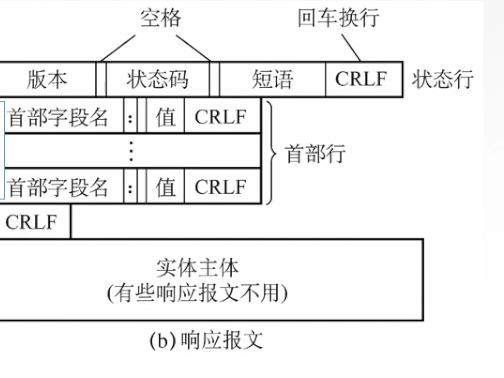
1.1-> HTTP版本

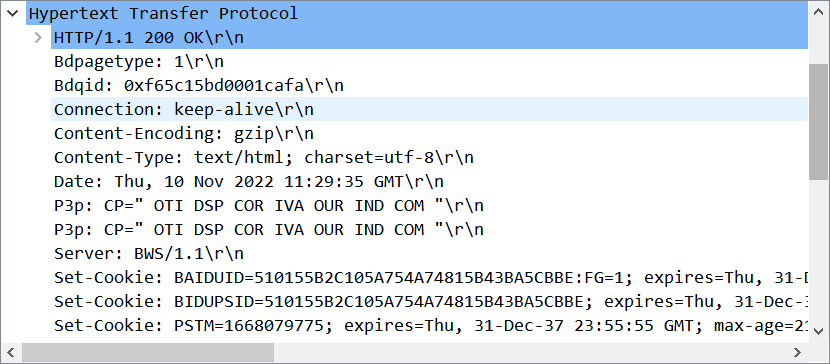
\r\n 就是回车换行了

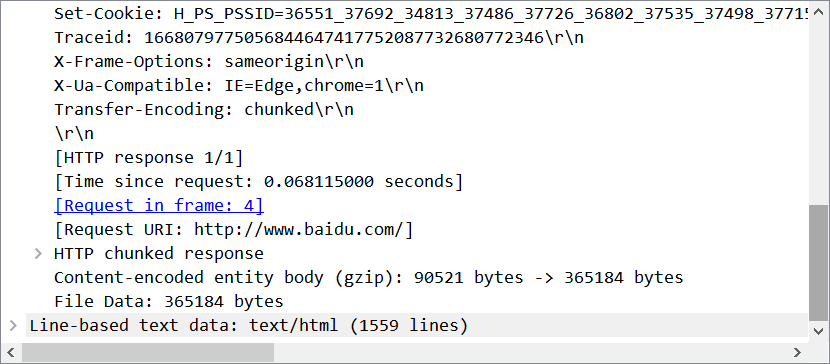
往后直到最后一个\r\n都是首部行，以首部字段名：值的形式出现，并以\r\n结尾

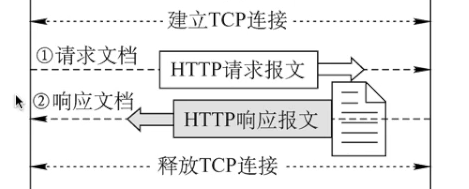
对于响应有类似结论，注意到状态行（对标请求行）发生了变化，在首部字段中有时也会多出cookie，在实体主体包含响应数据。





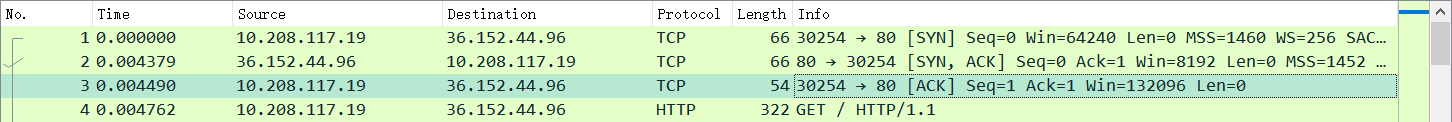


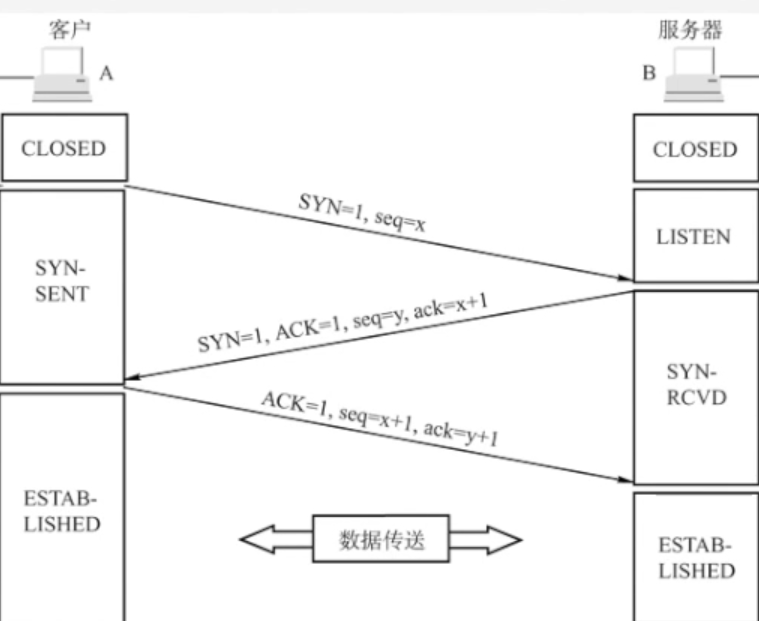
交互过程如图所示



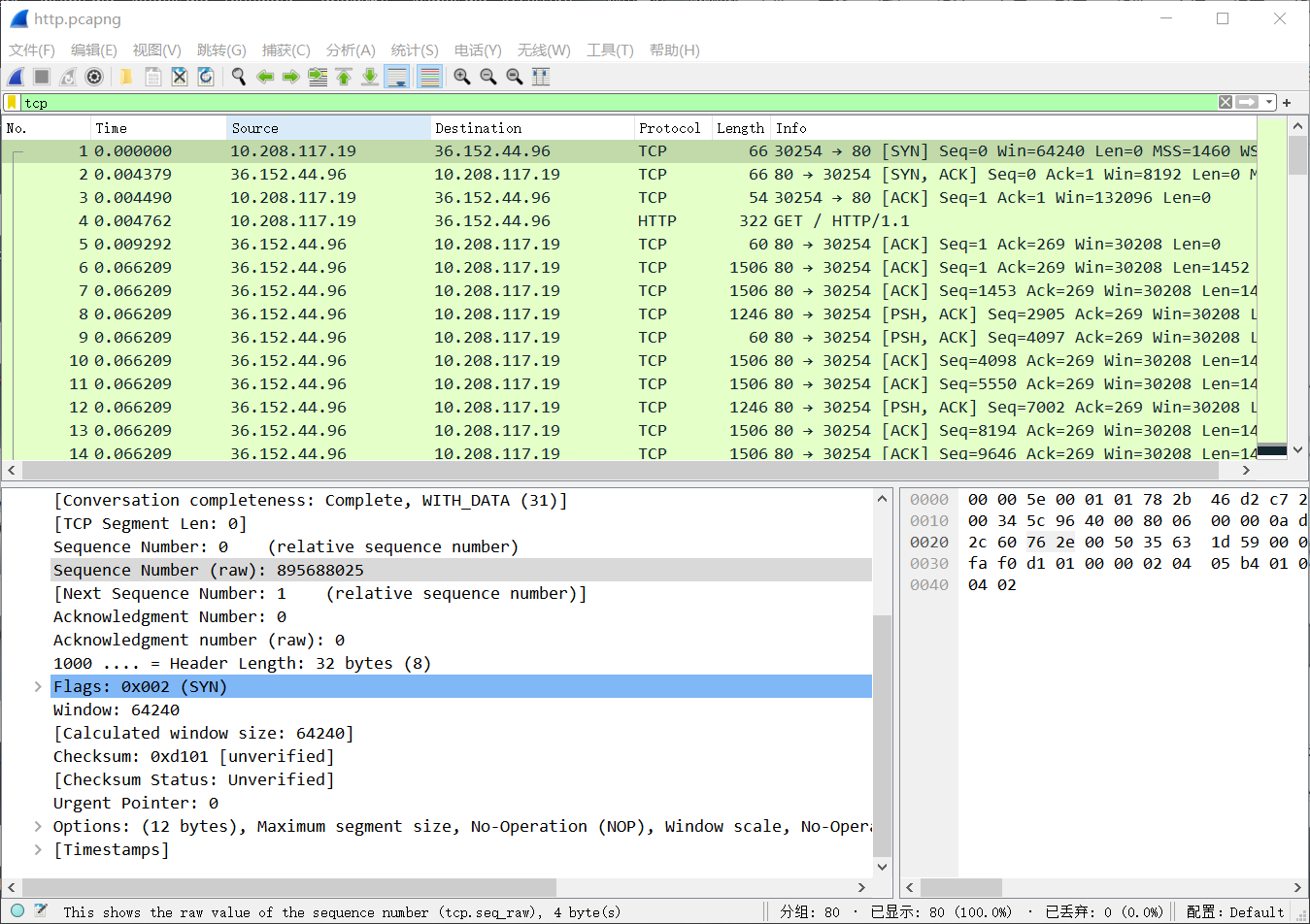
三、观察 TCP 协议报文格式，分析 TCP 协议采用的可靠传输机制、以及 TCP 连接建立和关闭的交互过程。

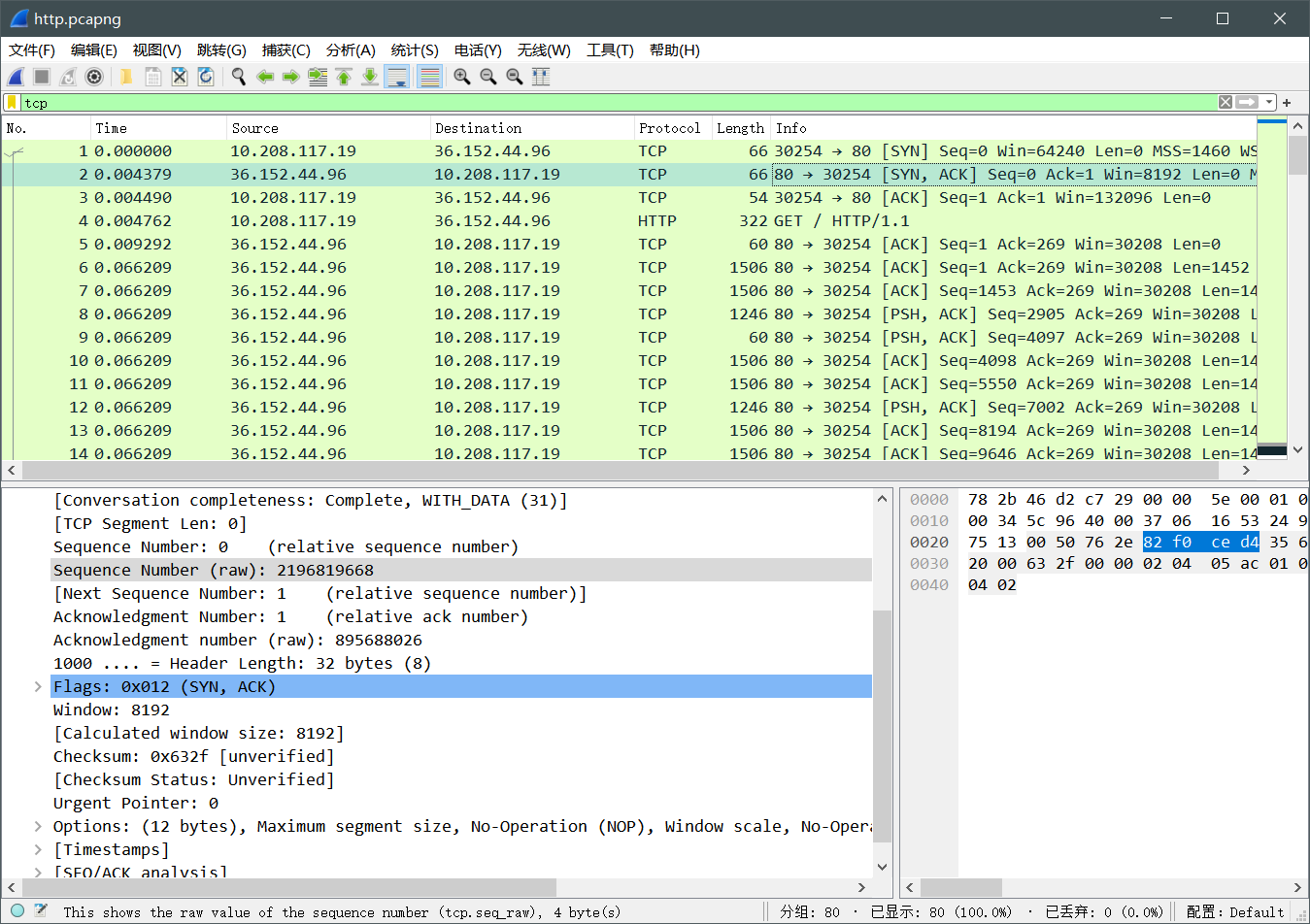
TCP连接建立的三次握手：

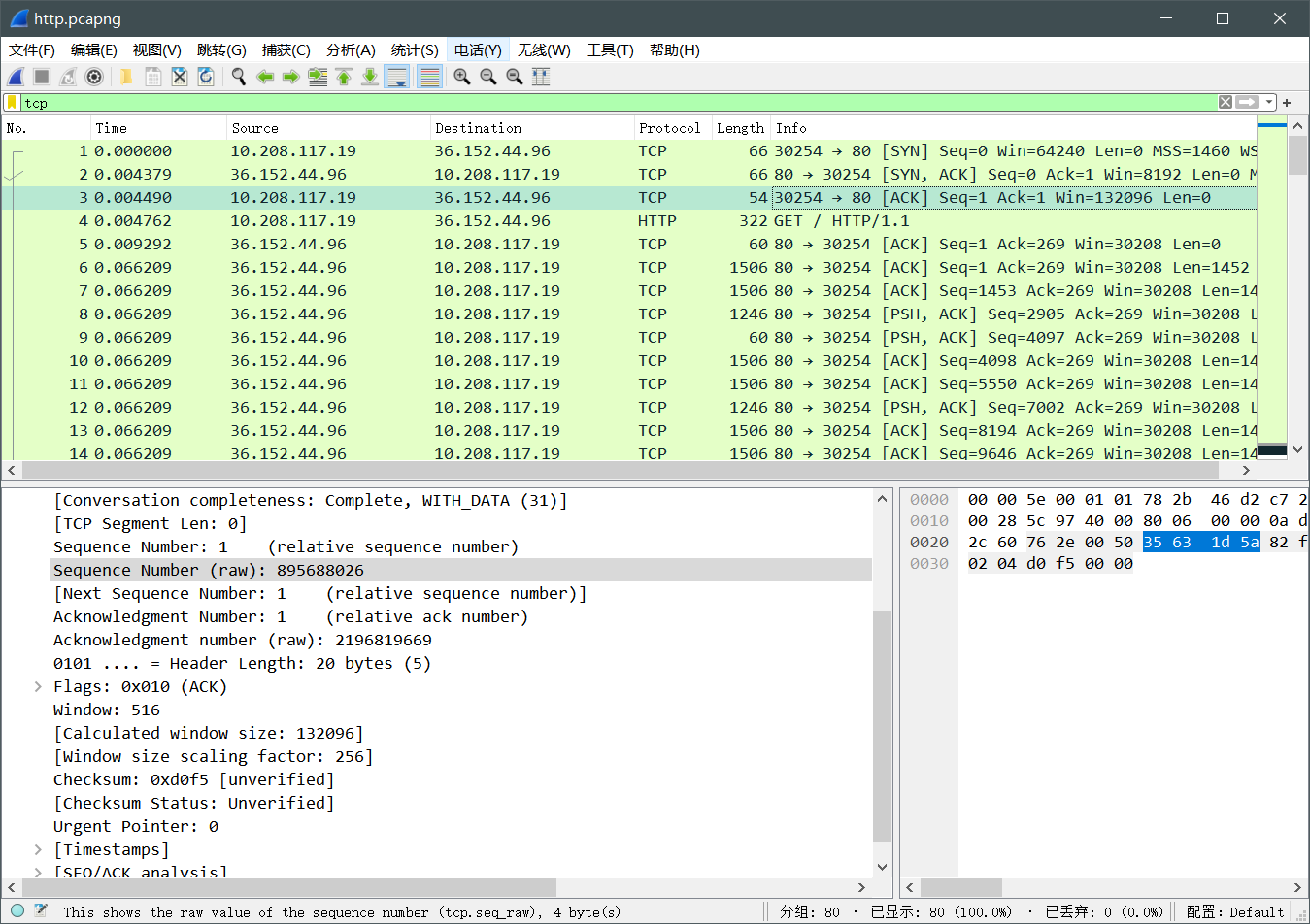




注意到下图中除了SYN ACK flags以外的Sequence Number 和 Acknowledge Number

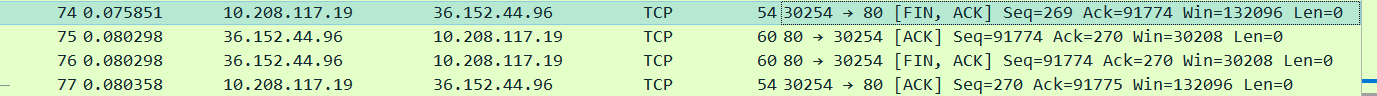


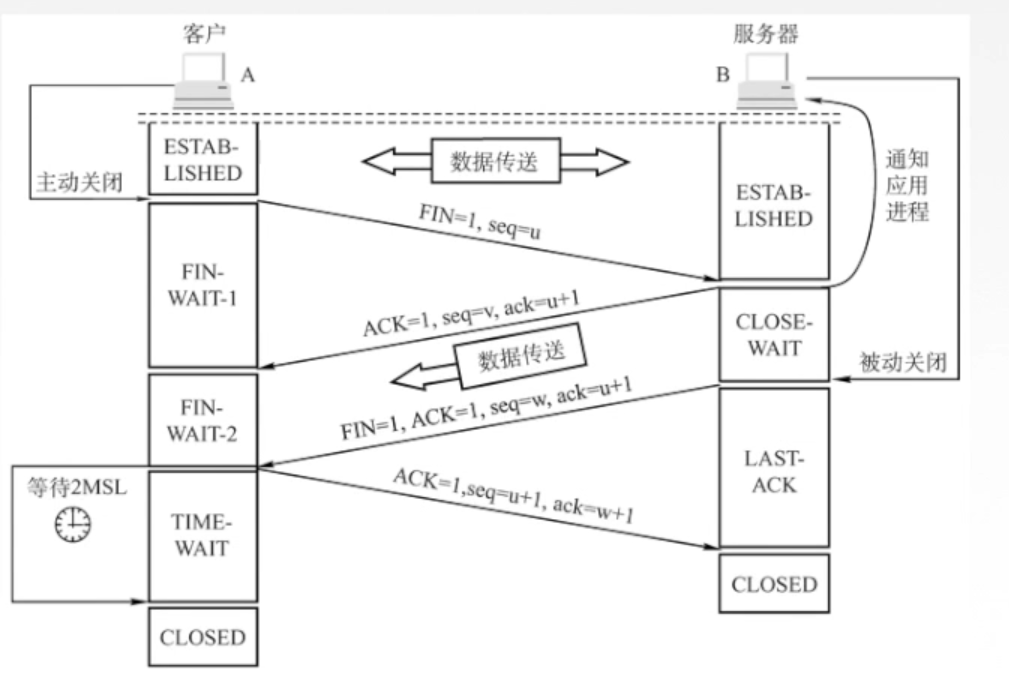




连接释放的四次挥手：

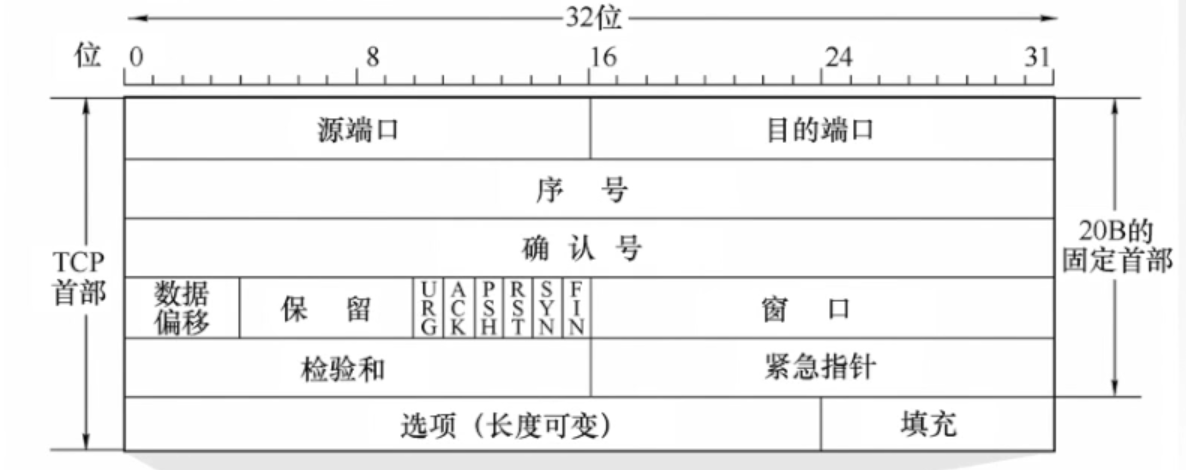
见图示，不再赘述

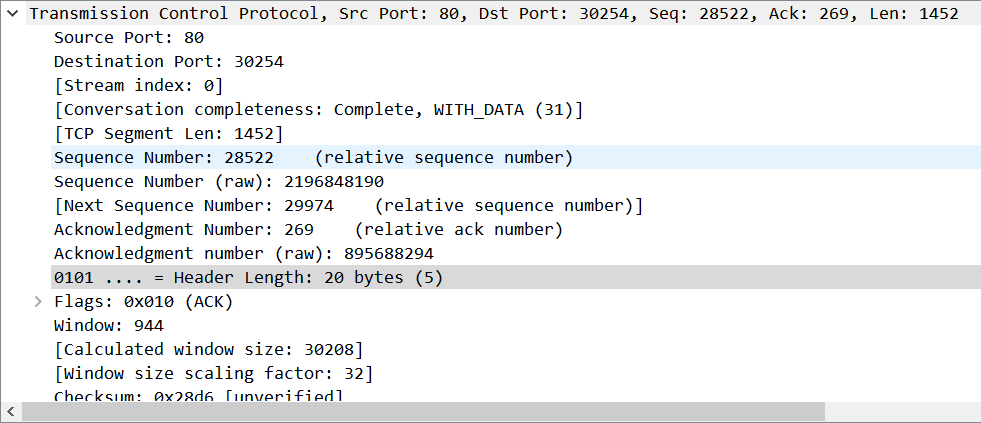


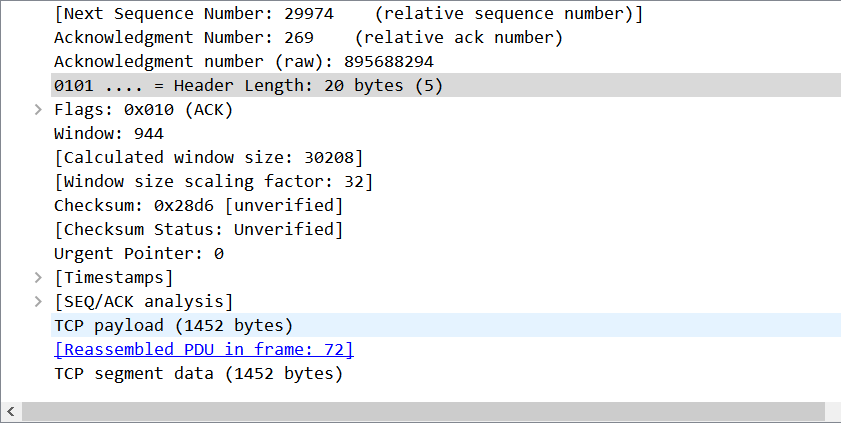


报文格式：

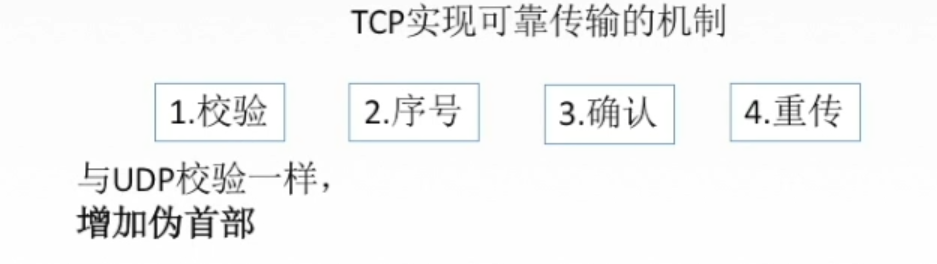
除开[]部分，按序对照即可





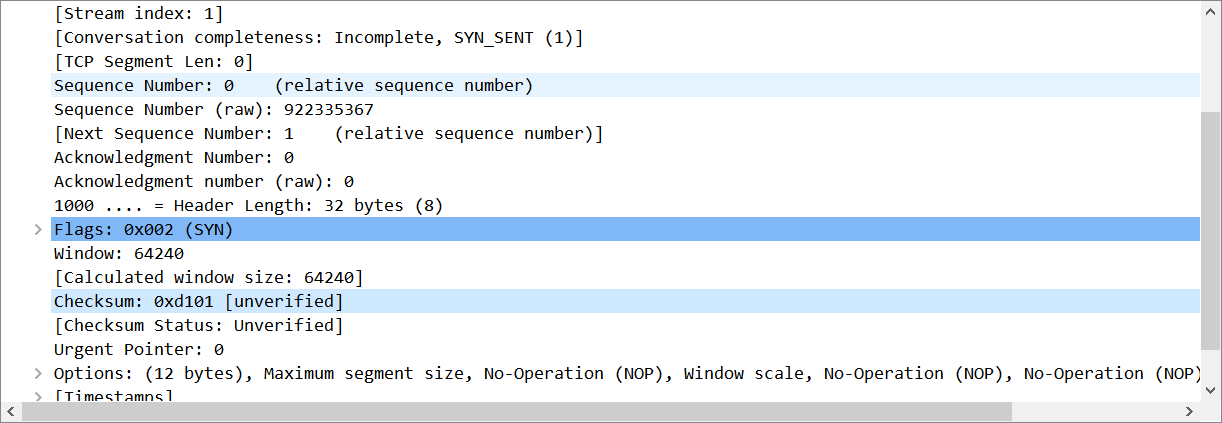


可靠性：



1. 校验

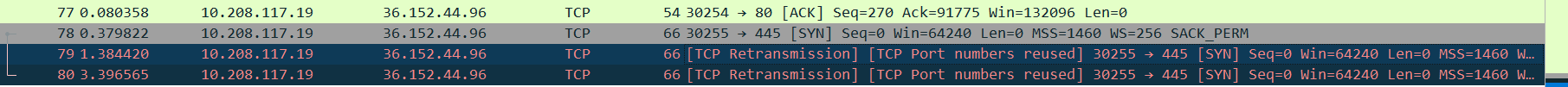
如图可以看到TCP校验和Checksum的信息，用于在添加伪首部后全部求和校验



1. 序号 | 确认

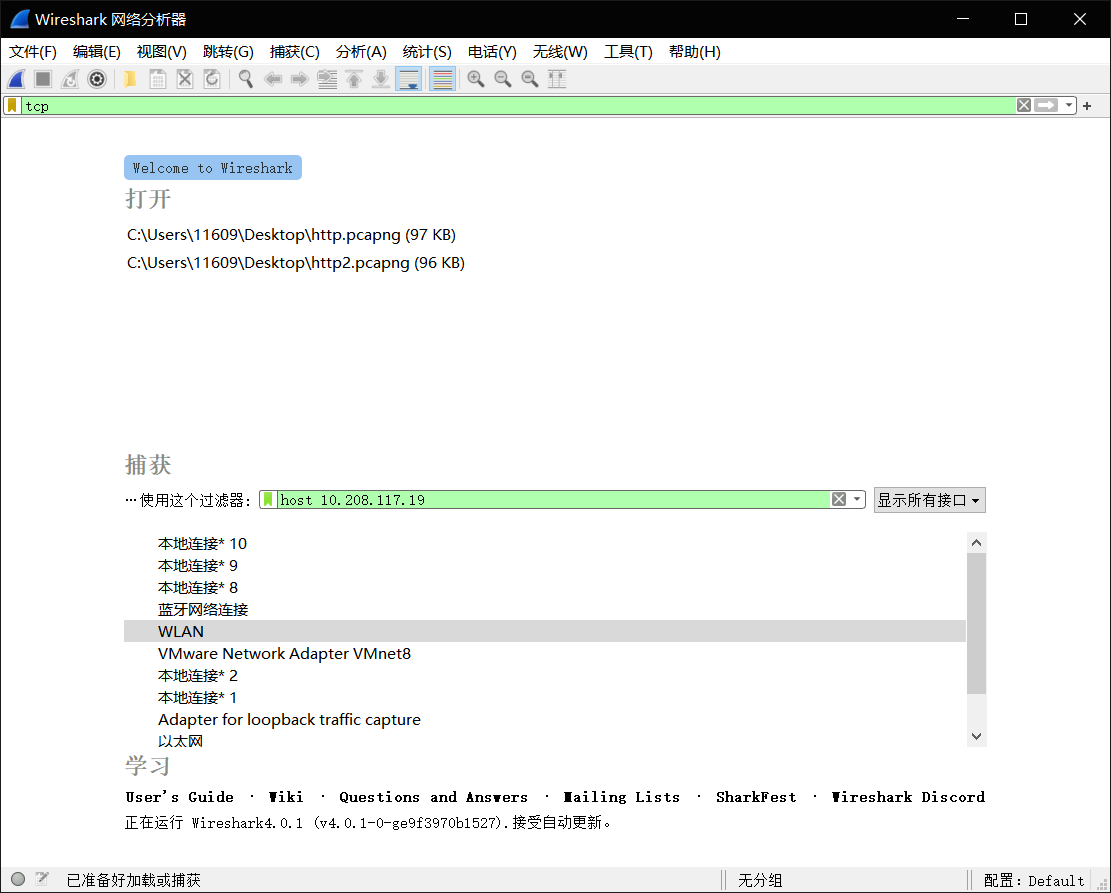
上述三次握手与四次挥手部分已经提及，不再赘述

4.超时重传示例

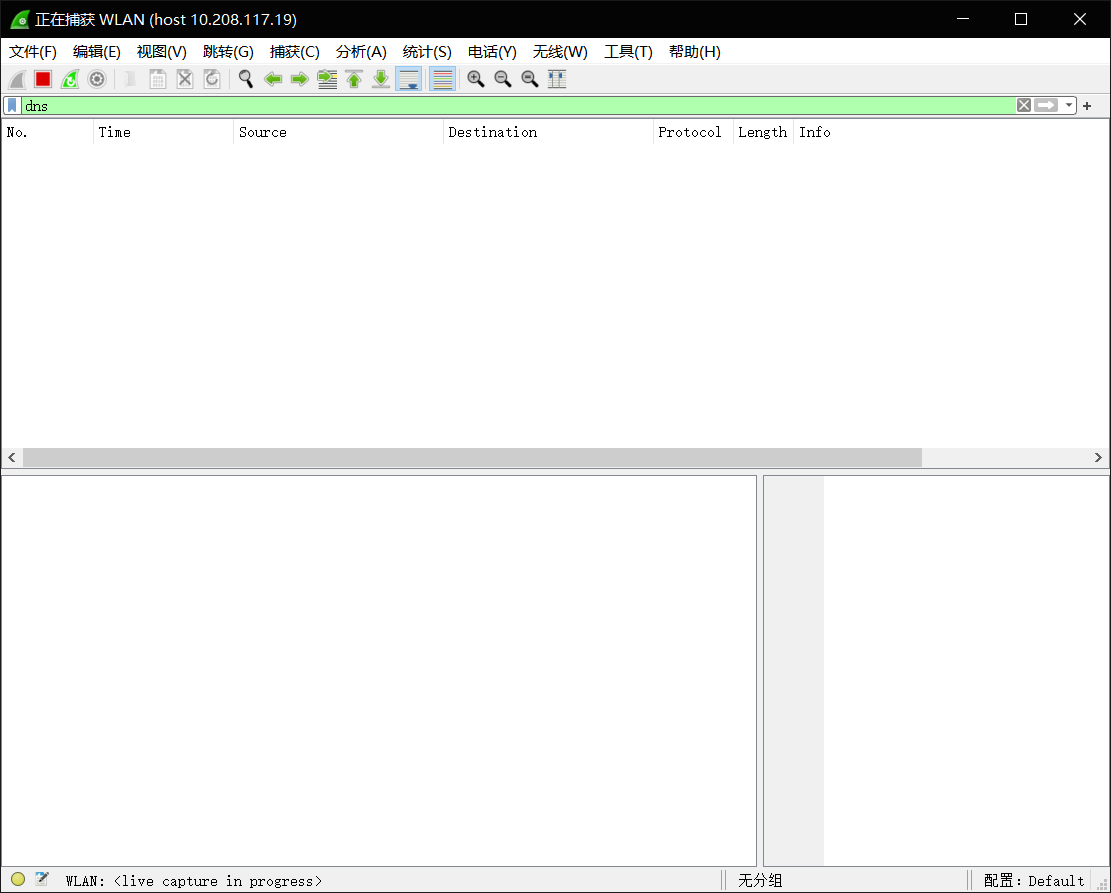


四、分析 DNS 协议报文格式和交互过程，同时分析UDP协议报文格式和交互过程。

重新输入dns服务器的ip



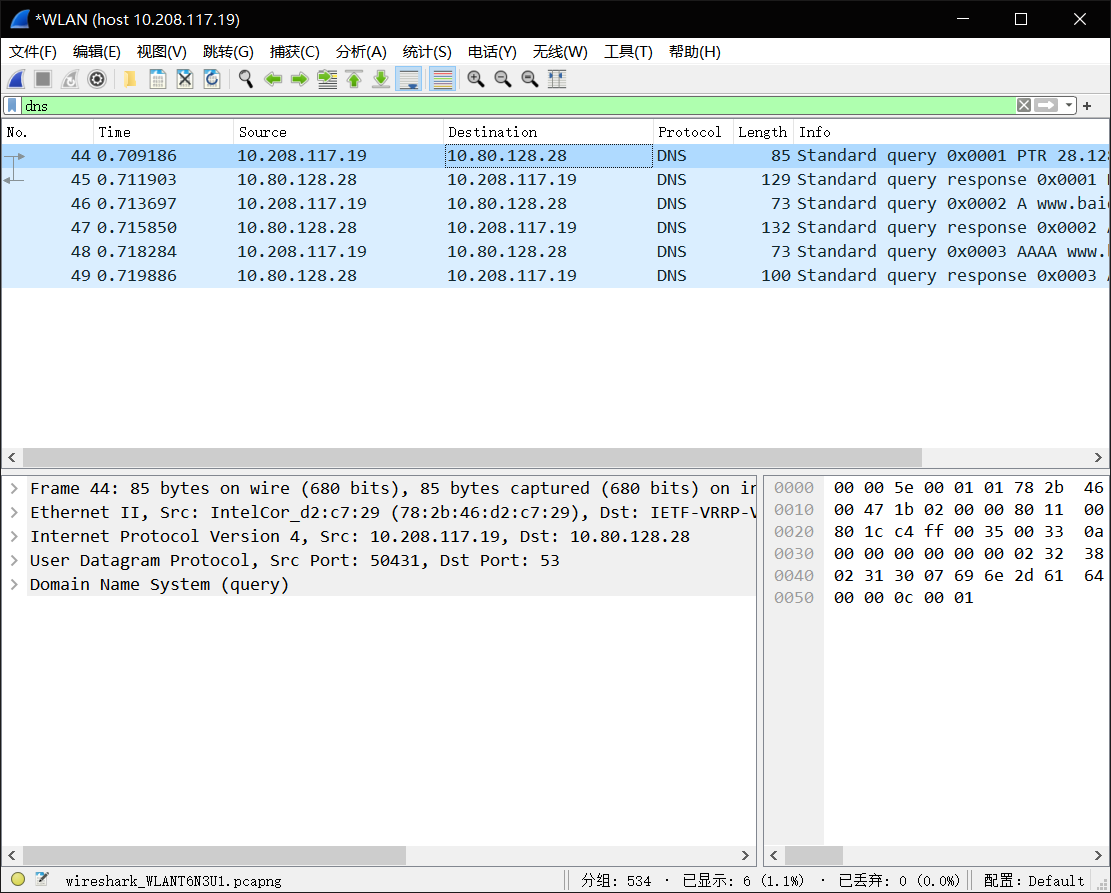
过滤dns



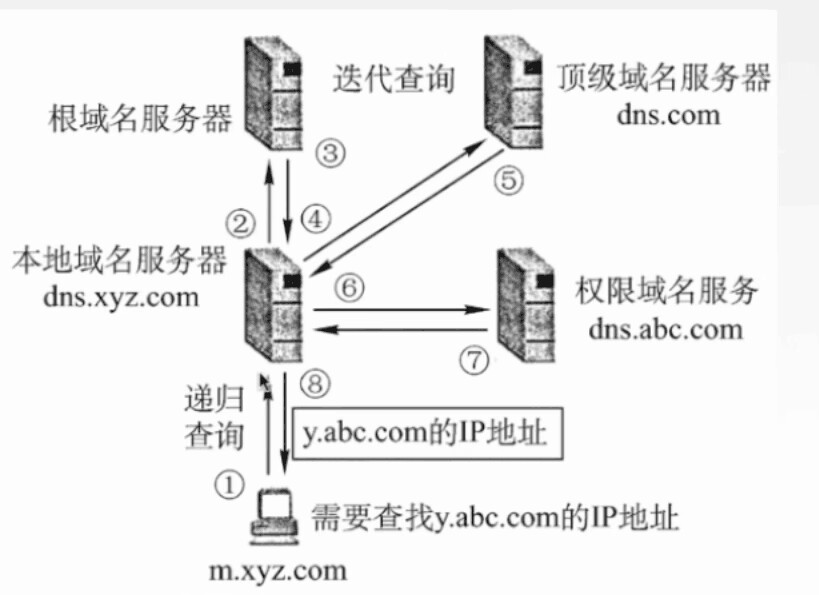
发送域名解析请求



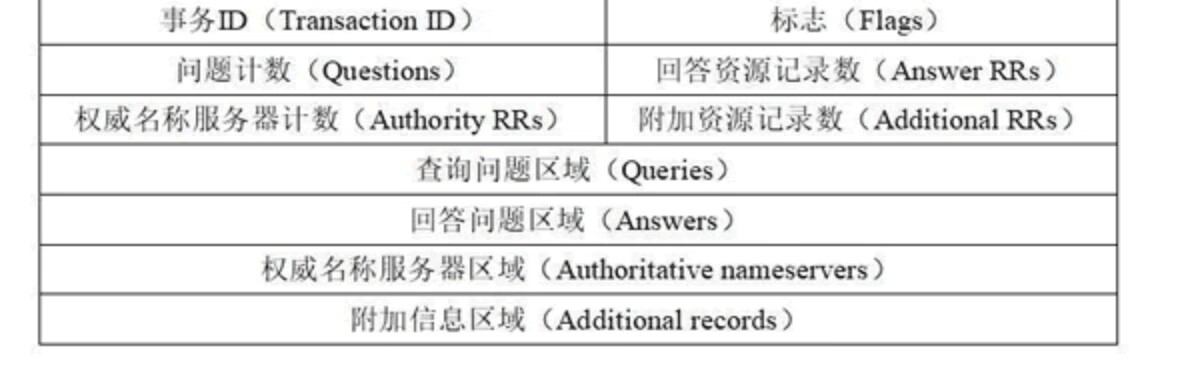
捕获到数据

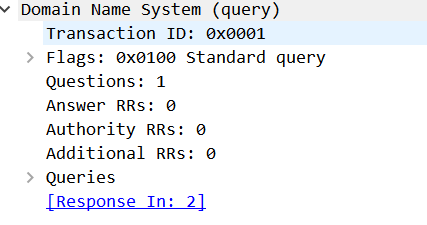


Dns交互过程见图



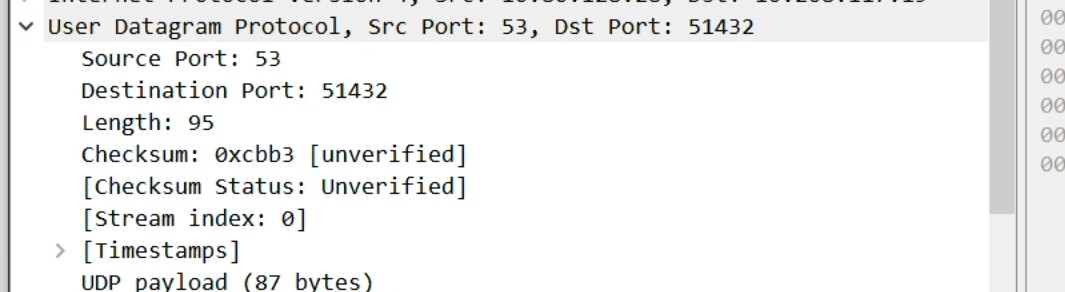
DNS协议报文格式





UDP协议报文格式





五、实验体会（实验中遇到的问题及解决方法、实验中产生的错误及原因分析、实验的体会及收获、对做好今后实验提出建设性建议等）

对各个协议的报文格式与交互过程形成了更为具体的认识，通过wireshark实际地观察到网络交互的过程，体会到网络交互中协议的重要作用。