2019秋计算机网络与信息安全网络协议分析大作业说明

**主要内容：**

访问一个Web网站，通过用Wireshark软件捕获的相应的数据文件，分析访问web的整个过程。

针对TCP/IP网络体系结构，通过对数据包捕获、分析，来了解TCP/IP的各层协议的工作原理，包括应用层报文、传输层端口，传输层报文头部，网络层IP数据报头部，数据链路层帧头部的组成与功能，了解报文的封装过程，对等层之间的通信原理。

**实验方式：**

合作方式：通过团队组织，分工协作，共同完成对协议的分析。

每班以3-4人为一组，共7-8组。

**内容要求：**

每组的同学负责分工完成，共同协商设计实验环节与软件环境，要求完成应用层报文分析，传输层报文分析，网络层协议报文分析等，共同完成分析报告。在报告中说明自己完成工作的完成度，以及分工，作为大作业最后每个的评分依据。组长负责整体实验的完成与组员的协调，决定最后的分工完成度。

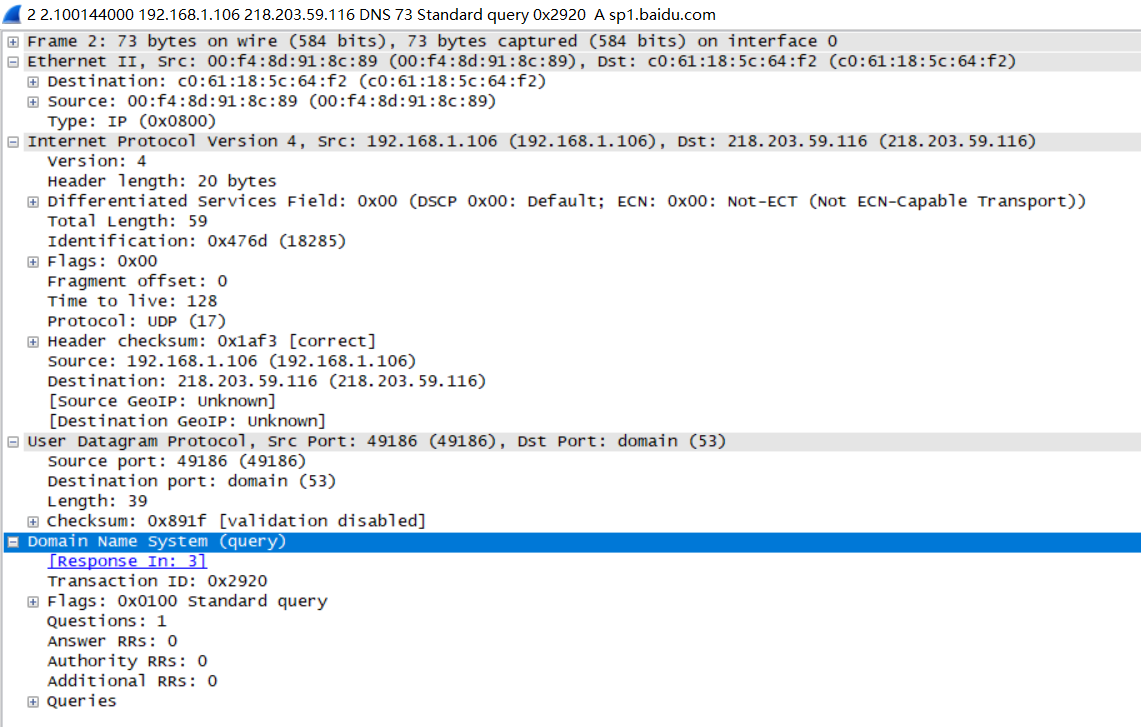
分析报告内容要求

在访问WEB站点的过程中，包括请求，响应和TCP的三次握手等过程。分工完成如下：

1. DNS分析

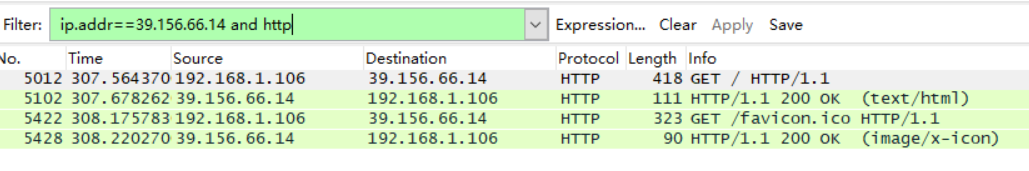
找到DNS将web网站解析为IP地址的相应帧，并分析其完成的请求与响应的过程，以及返回的IPV4和IPV6的情况。

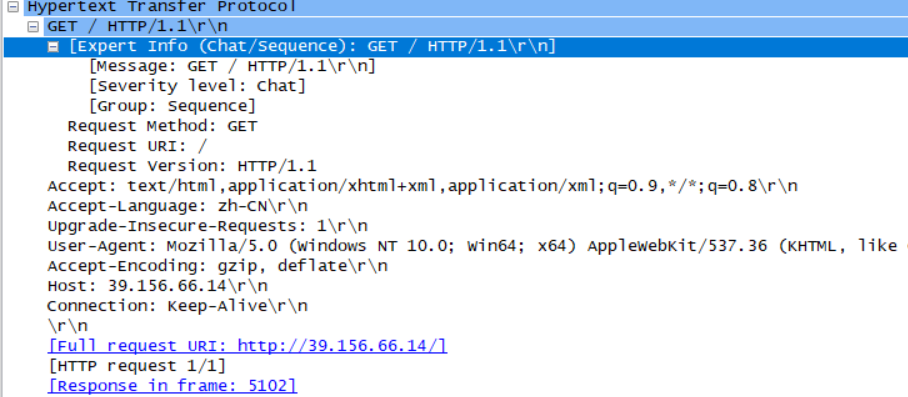
操作参考：在捕获一系列数据之后，使用DNS过滤器过滤其他协议，从头找到的查询和响应数据包，保存导出。然后分析捕获的报文。



1. 找到web请求响应的过程

找到客户端GET主页面以及服务器收到请求并发送响应包，以及服务器发送主页面给客户端的通信过程，并进行分析。



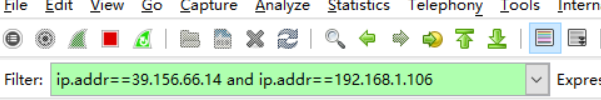


三、找到传输层三次握手的数据

传输层协议分析在捕获的数据包中要求找到TCP的三次握手报文，并结合网络原理进行分析。同时观察可变窗口的变化，结果理论进行分析说明。如果是UDP协议，要求找到其端口等关键信息。

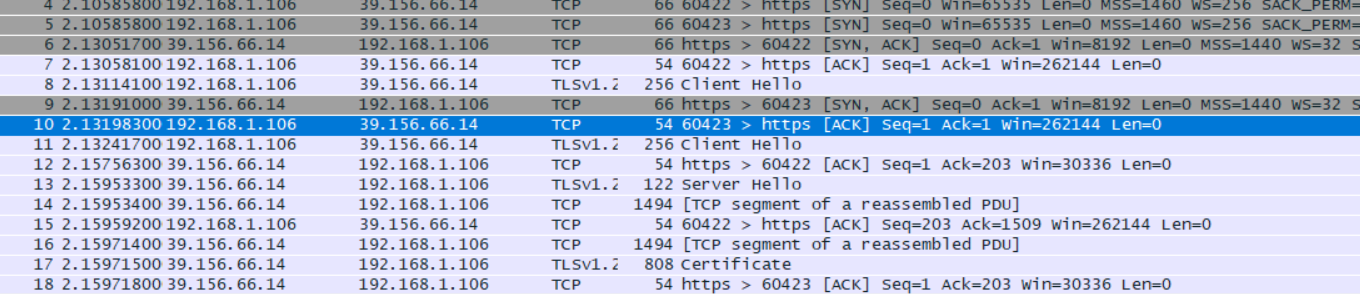
操作参考，在捕获一系列数据之后，

使用点击Analyze菜单并选择Display Filters来创建新的过滤条件。



查看与百度网站通信的过程。

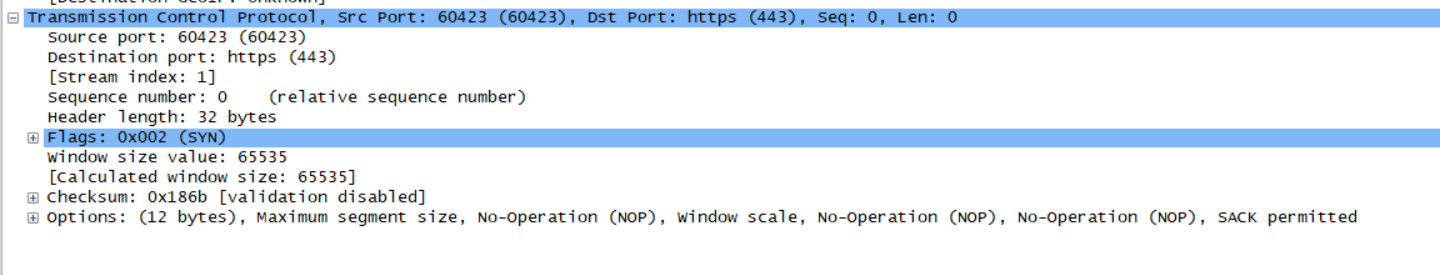
也可以使用TCP报文过滤器，将TCP报文过滤出来，从头查看。在前的三次握手过程。



如45是第一次，69是第二个，10是第三次。

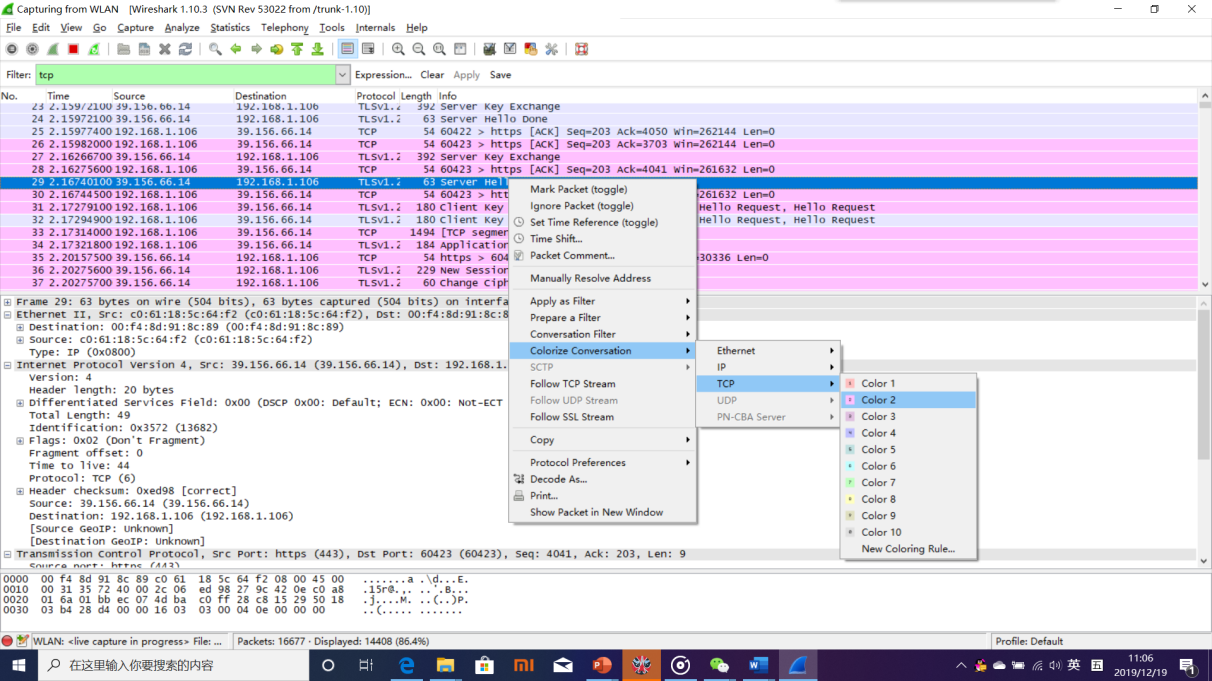
察看全部通信，看到双方的seq和ack以及win值 如何变化。

打开第一次握手报文，进行分析。



关于着色

可将某段报文单击右键，选择“colorize conversation”将属于同一个过程的数据包着色内，便于观察 。



四、网络层协议分析

在捕获的数据包中找到报文头部中关键字段，分析IP数据报的状态，如分片状况，观察TTL的变化，

找到第一次握手报文的IP层报文，分析各部分的内容

