Lab3 Wireshark 分析 TCP 协议

宁晨然 17307130178

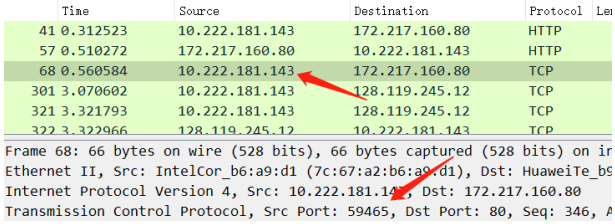
一、实验目的

认识 TCP 协议
熟悉 TCP 三次握手的过程

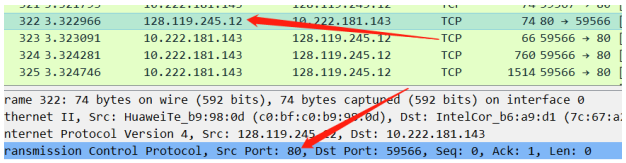
二、实验过程

1.What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

客户端使用的 IP 地址是 10.222.181.143，使用的 TCP 端口是 59465。

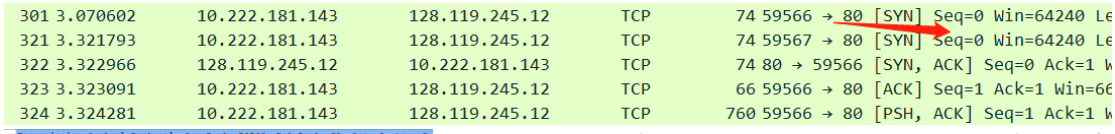


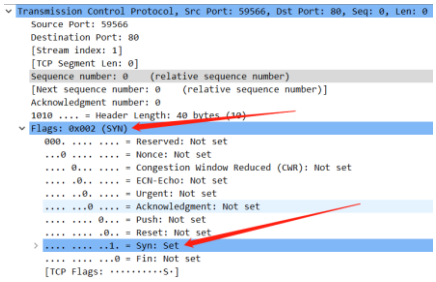
2.What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?



网址的 IP 地址是 128.119.245.12，使用的 TCP 端口是 80。

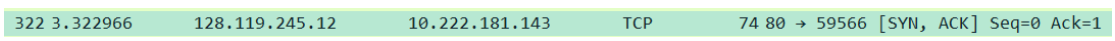
3.What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

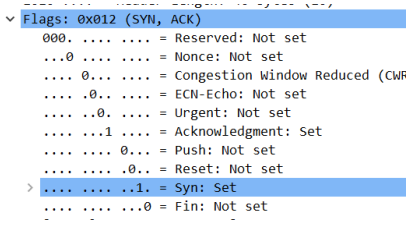




用于初始化连接的 TCP SYN=0,下图是建立连接时三次握手过程，客户端先向服务端发送了 SYN（SEQ=0），服务端反馈 SYN(SEQ=0,ACK=0+1=1)，客户端再次发送 SYN（SEQ=0+1，ACK=0+1）。TCP 段中，控制标志中的 SYN 标志用于建立 TCP 连接，如果 SYN=1,ACK=0 为发起/申请连接，SYN=1,ACK=1 表示响应接受连接。所以 SYN 标志位为 1 表示其为 SYN。

4.What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

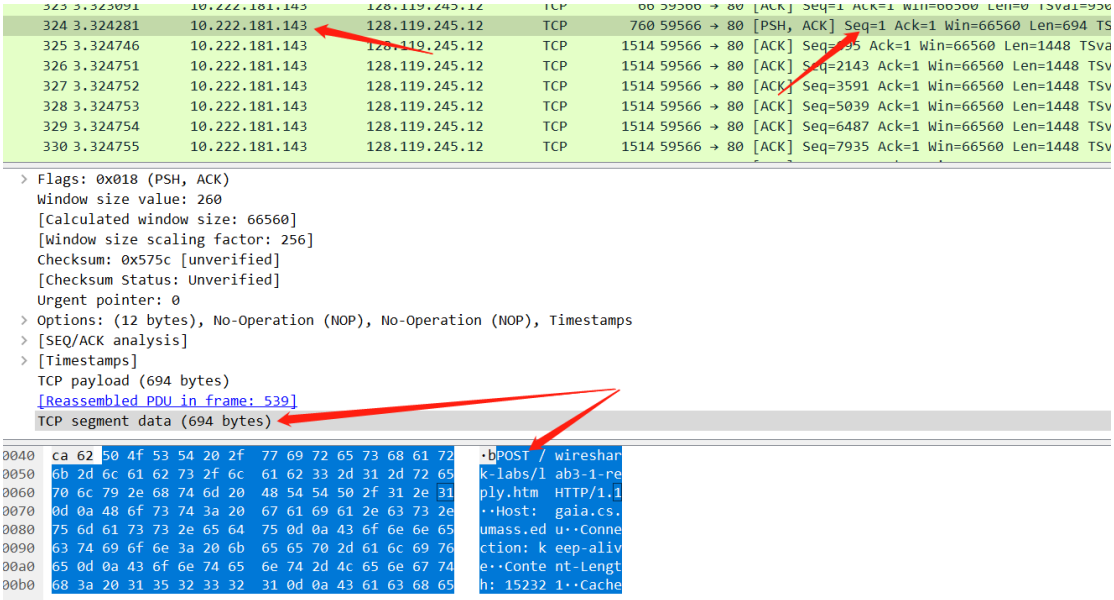




根据三次握手 TCP 建立连接的过程，第二阶段服务端发送给客户端 SYN(SEQ=y,ACK=x+1)，根据上图可知第一次客户端发送的 SEQ=0，即 x=0，并且返回的 SYN 中 y=0，发送的 ACK 值为 x+1=1。第二阶段服务端发送的 ACK 的值为第一阶段客户端发送的 SEQ 值+1，用于确认连接的号码无误。

不同于第一阶段客户端的 SYN 类型的确认只需要 control flags 中的 SYN=1，ACK=0；第二阶段服务端的 SYN 需要 flags 中的 SYN=1,ACK=1。用来表示服务端接收该 TCP 请求。

5.What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.



这是由客户端发送到服务端的 TCP 段，根据段中 data 部分的信息可以知道发送了 POST 请求的命令。可知该 SEQ=1。

三、实验感受

本次实验的重点就是 TCP 连接创建过程，三次握手的实现方式的实践，难度不大。认识的 TCP 的结构、加深了对于三次握手的理解，并且认知到了 TCP 的连接中各种不稳定因素，TCP 在不稳定网络中建立了稳定的连接。