实验三：使用 Wireshark 软件分析 TCP 协议

学号：16307130194，姓名：陈中钰

1 问题 1

1.1 捕获分组

访问http://gaia.cs.umass.edu/wiresharklabs/alice.txt并下载文件，接着访问http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html，选择刚刚下载的文件，点击开始捕获分组，在网页中点击上传，在文件上传完毕后结束捕获分组。

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

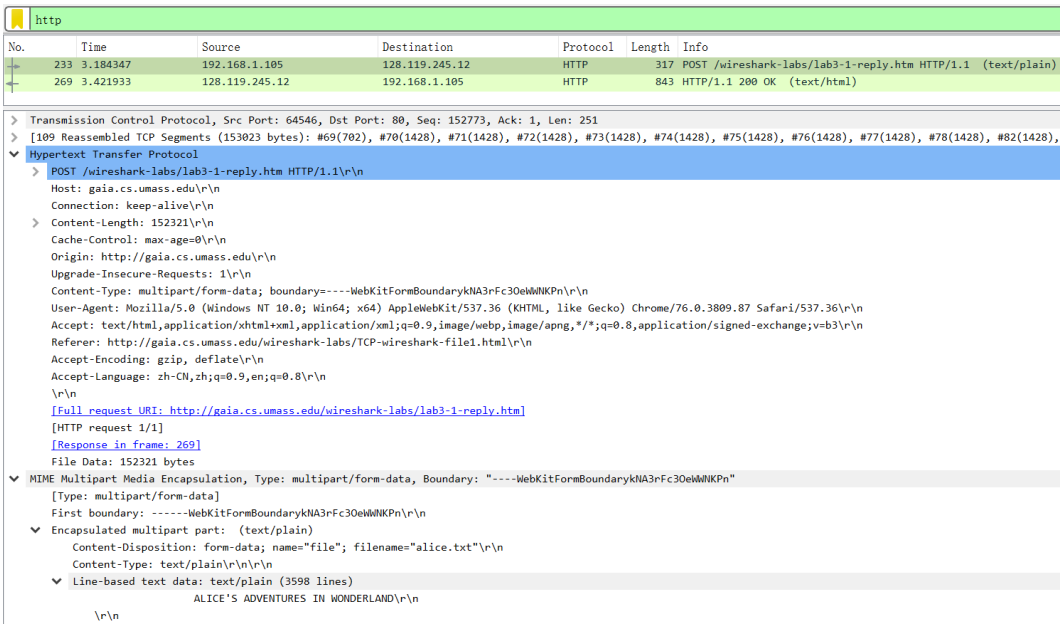

Figure 1: 客户端发送文件的封包

为了找到客户端发送文件的封包，设置过滤器为 http，过滤结果如 Figure 1所示。其中，No.233 封包的封包详细信息中，MIME Multipart Media Encapsulation 部分显示这个封包含有所发送的文件的名字和内容，说明该封包就是客户端发送文件的封包。因此，客户端的 IP 地址就是 Source 地址，也就是 192.168.1.105。另外，通过查看封包详细信息的 TCP 部分，可以得到 TCP 端口号为 64546。以上信息均能在 Figure 1中找到。

2 问题 2

2.1 What is the IP address of gaia.cs.umass.edu?

如 Figure 1所示，客户端发送文件的封包的 Destination 为 128.119.245.12，也就是 gaia.cs.umass.edu 的 IP 地址。

2.2 On what port number is it sending and receiving TCP segments for this connection?

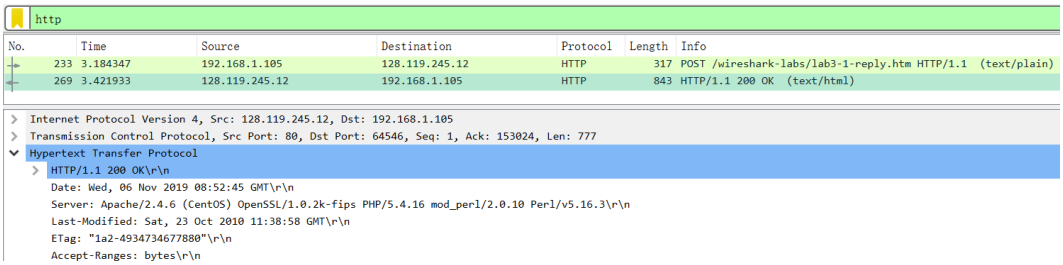

Figure 2: 服务端发送 TCP 段的封包

如 Figure 1所示，发送文件的封包的 TCP 部分中的 Dst Port 为 80，说明 gaia.cs.umass.edu 接收 TCP 段的端口号为 80。另外，如 Figure 2所示，No.269 封包是 gaia.cs.umass.edu 发送的，其发送端口号也是 80。因此综上所述，gaia.cs.umass.edu 发送和接收 TCP 段的端口号都是 80。

3 问题 3

3.1 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?

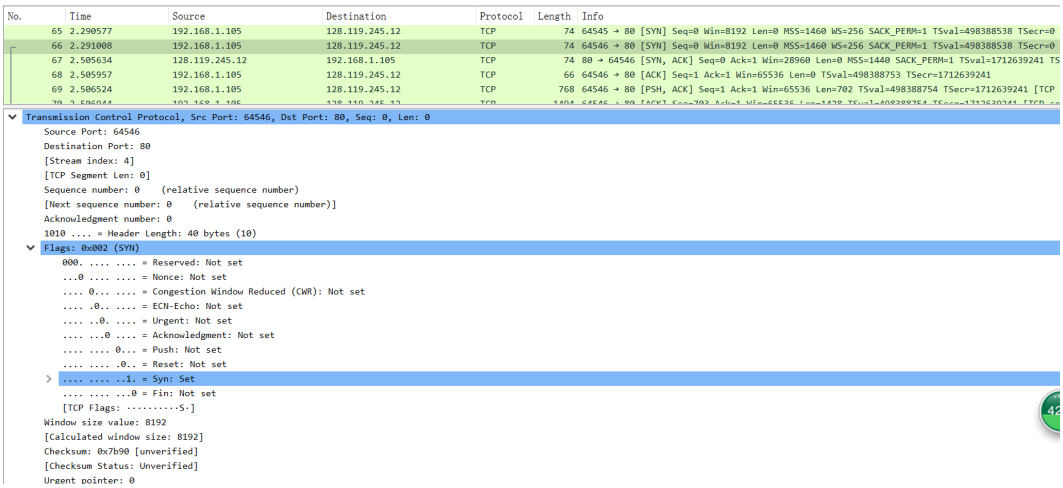

Figure 3: 请求 TCP 连接的 TCP SYN 段

在 Figure 1中的发送文件的封包前面，寻找一个含有 SYN 字段的封包，可以找到 Figure 3中的 No.66 封包，就是请求 TCP 连接的 TCP SYN 段。从这个封包的详细信息的 TCP 部分可以看到，sequence number 为 0 (relative sequence number)。

3.2 What is it in the segment that identifies the segment as a SYN segment?

如 Figure 3所示，这个封包的详细信息的 TCP 部分中，Flags 字段显示 Syn 为 Set，而且 Acknowledgment 为 Not set，标识了这个 TCP 段是一个 SYN 段。

4 问题 4

4.1 What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN?

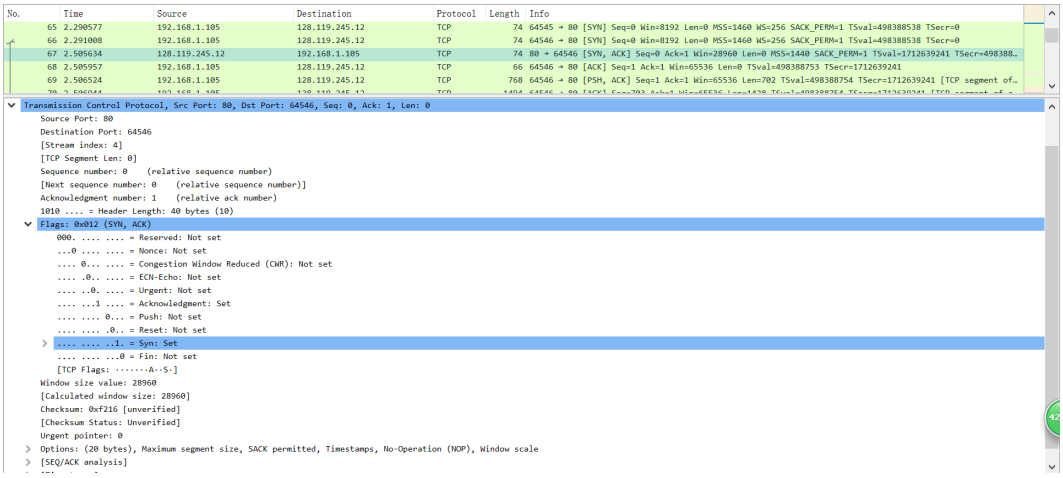

Figure 4: gaia.cs.umass.edu 回应的 TCP SYNACK 段

在 Figure 3的 TCP SYN 段后面，寻找一个含有 SYN、ACK 字段的封包，可以找到如 Figure 4所示的 No.67 封包，就是 gaia.cs.umass.edu 为了回应客户端的 SYN 而发送的 SYNACK 段。查看封包的详细信息，可知 sequence number 为 0 (relative sequence number)。

4.2 What is the value of the Acknowledgement field in the SYNACK segment?

SYNACK 段的详细信息如 Figure 4所示，Acknowledgement number 字段为 1，Flags 字段中的 Acknowledgement 字段为 Set。

4.3 How did gaia.cs.umass.edu determine that value?

SYNACK 段的 Acknowledgement 的值，就是发起 TCP 连接请求的 SYN 段的 sequence number 加 1，所以结果为 1。

4.4 What is it in the segment that identifies the segment as a SYNACK segment?

如 Figure 4所示，Flags 字段中的 Syn 为 Set、Acknowledgement 为 Set，标识了这个 TCP 段为 SYNACK 段。

5 问题 5

5.1 What is the sequence number of the TCP segment containing the HTTP POST command?

在 Figure 4中的 SYNACK 段的下面，逐个 TCP 段进行检查。可以找到 No.69 封包，如 Figure 5所示，在 TCP segment data 字段中可以找到"POST" 的字样，说明这个封包就是要找的封包。查看该封包的 TCP 详细信息可知，sequence number 为 1 (relative sequence number)。

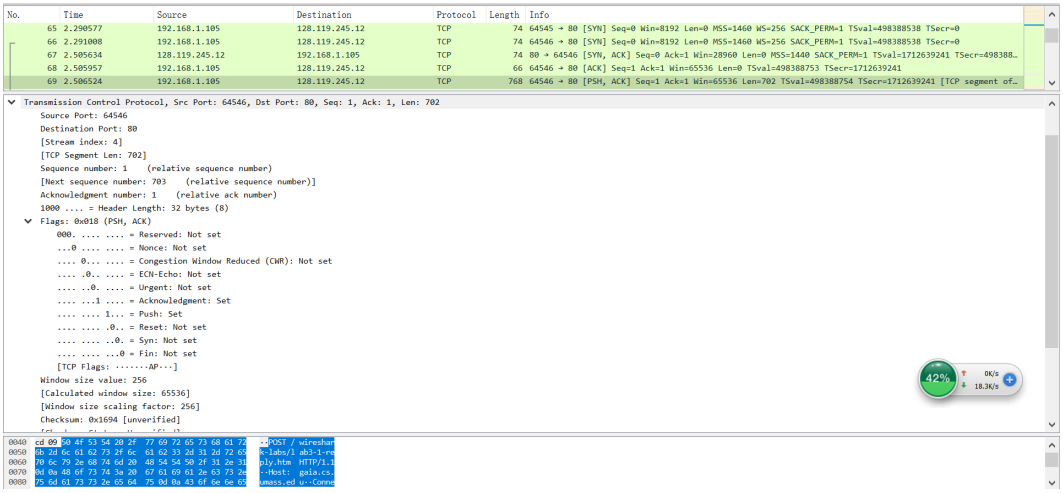

Figure 5: 包含了 HTTP POST 指令的 TCP 段