

# 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?

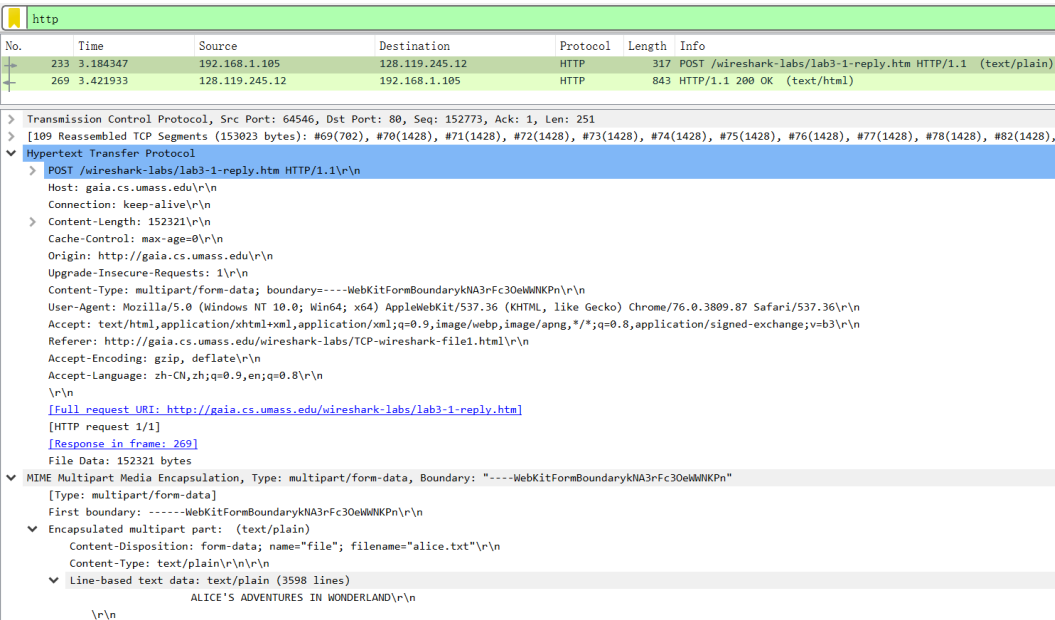


Figure 1: 客户端发送文件的封包

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?

http						
No.	Time	Source	Destination	Protocol	Length	Info
233	3.184347	192.168.1.105	128.119.245.12	HTTP	317	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
269	3.421933	128.119.245.12	192.168.1.105	HTTP	843	HTTP/1.1 200 OK (text/html)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105						
> Transmission Control Protocol, Src Port: 80, Dst Port: 64546, Seq: 1, Ack: 153024, Len: 777						
> Hypertext Transfer Protocol						
> HTTP/1.1 200 OK\r\n						
Date: Wed, 06 Nov 2019 08:52:45 GMT\r\n						
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n						
Last-Modified: Sat, 23 Oct 2010 11:38:58 GMT\r\n						
ETag: "1a2-4934734677880"\r\n						
Accept-Ranges: bytes\r\n						

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?

No.	Time	Source	Destination	Protocol	Length	Info
65	2.290577	192.168.1.105	128.119.245.12	TCP	74	64545 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=498388538 TSecr=0
66	2.291008	192.168.1.105	128.119.245.12	TCP	74	64546 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=498388538 TSecr=0
67	2.509034	128.119.245.12	192.168.1.105	TCP	74	80 → 64546 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1712639241 TS
68	2.509597	192.168.1.105	128.119.245.12	TCP	66	64546 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=498388753 TSecr=1712639241
69	2.506524	192.168.1.105	128.119.245.12	TCP	768	64546 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=792 TSval=498388754 TSecr=1712639241 [TCP
70	2.506044	192.168.1.105	128.119.245.12	TCP	4404	64546 → 80 [ACK] Seq=202 Ack=1 Win=65536 Len=0 TSval=498388754 TSecr=1712639241 [TCP

> Transmission Control Protocol, Src Port: 64546, Dst Port: 80, Seq: 0, Len: 0						
Source Port: 64546						
Destination Port: 80						
[Stream index: 4]						
[TCP Segment Len: 0]						
Sequence number: 0 (relative sequence number)						
[Next sequence number: 0 (relative sequence number)]						
Acknowledgment number: 0						
1010 .... = Header Length: 40 bytes (10)						
Flags: 0x002 (SYN)						
0000 .... = Reserved: Not set						
...0 .... = Nonce: Not set						
....0... .... = Congestion Window Reduced (CWR): Not set						
....0... .... = ECN-Echo: Not set						
....0... .... = Urgent: Not set						
....0... .... = Acknowledgment: Not set						
....0... .... = Push: Not set						
....0... .... = Reset: Not set						
> ....0... .... = Syn: Set						
....0... .... = Fin: Not set						
[TCP Flags: .....S-]						
Window size value: 8192						
[Calculated window size: 8192]						
Checksum: 0x7b90 [unverified]						
[Checksum Status: Unverified]						
Urgent pointer: 0						

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?

No.	Time	Source	Destination	Protocol	Length	Info
65	2.290577	192.168.1.105	128.119.245.12	TCP	74	64545 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=498388538 TSecr=0
66	2.291008	192.168.1.105	128.119.245.12	TCP	74	64546 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=498388538 TSecr=0
67	2.505634	128.119.245.12	192.168.1.105	TCP	74	80 → 64546 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1712639241 TSecr=498388538
68	2.505957	192.168.1.105	128.119.245.12	TCP	66	64546 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=498388753 TSecr=1712639241
69	2.506521	192.168.1.105	128.119.245.12	TCP	768	64546 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=762 TSval=498388754 TSecr=1712639241 [TCP segment of...

Transmission Control Protocol, Src Port: 80, Dst Port: 64546, Seq: 0, Ack: 1, Len: 0

Source Port: 80  
Destination Port: 64546  
[Stream index: 4]  
[TCP Segment Len: 0]  
Sequence number: 0 (relative sequence number)  
[Next sequence number: 0 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
1010 .... = Header Length: 40 bytes (10)

Flags: 0x012 [SYN, ACK]

0000 .... = Reserved: Not set  
...0 .... = Nonce: Not set  
...0 .... = Congestion Window Reduced (CWR): Not set  
...0 .... = ECH-Echo: Not set  
...0 .... = Urgent: Not set  
...1 .... = Acknowledgment: Set  
...0 .... = Push: Not set  
...0 .... = Reset: Not set  
...1 .... = Syn: Set  
...0 .... = Fin: Not set  
[TCP Flags: .....A..S..]  
Window size value: 28960  
[Calculated window size: 28960]  
Checksum: 0xf216 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale  
[SEQ/ACK analysis]

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)。

No.	Time	Source	Destination	Protocol	Length	Info
65	2.290577	192.168.1.105	128.119.245.12	TCP	74	64545 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=498388538 TSecr=0
66	2.291008	192.168.1.105	128.119.245.12	TCP	74	64546 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=498388538 TSecr=0
67	2.505634	128.119.245.12	192.168.1.105	TCP	74	80 → 64546 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1440 SACK_PERM=1 TSval=1712639241 TSecr=498388...
68	2.505957	192.168.1.105	128.119.245.12	TCP	66	64546 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=498388753 TSecr=1712639241
69	2.506524	192.168.1.105	128.119.245.12	TCP	768	64546 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=702 TSval=498388754 TSecr=1712639241 [TCP segment of...

Transmission Control Protocol, Src Port: 64546, Dst Port: 80, Seq: 1, Ack: 1, Len: 702

Source Port: 64546  
Destination Port: 80  
[Stream index: 4]  
[TCP Segment Len: 702]  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 703 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
1000 .... = Header Length: 32 bytes (8)  
Flags: 0x018 (PSH, ACK)  
000. .... = Reserved: Not set  
...0 .... = Nonce: Not set  
....0 .... = Congestion Window Reduced (CWR): Not set  
....0 .... = ECH-Echo: Not set  
....0 .... = Urgent: Not set  
....1 .... = Acknowledgment: Set  
....1 .... = Push: Set  
....0 .... = Reset: Not set  
....0 .... = Syn: Not set  
....0 .... = Fin: Not set  
[TCP Flags: .....AP...]  
Window size value: 256  
[Calculated window size: 65536]  
[Window size scaling factor: 256]  
Checksum: 0x1694 [unverified]  
len=702

0040 cd 00 50 4f 53 54 20 2f 77 69 72 65 73 68 61 72 POST / vareshar  
0050 20 2f 6c 61 62 73 2f 6c 61 62 33 20 31 20 72 65 <tab>/ abi-1-re  
0060 10 6c 72 2e 69 74 6d 20 45 54 54 59 2f 31 2e 31 <tab> http://  
0070 bd 0a 48 6f 73 74 3a 20 07 61 69 61 2e 63 73 2e --Host: gaia.cs.  
0080 25 6d 61 73 73 2e 65 64 75 6d 6d 43 6f 6e 6e 65 mss:ed u--Gone

Figure 5: 包含了 HTTP POST 指令的 TCP 段