Gurwinder Singh

4/14/2019

Lab 3- WireShark

1) IP address of source is : 192.168.1.102 and source port # is: 1161
2) IP address of gaia.cs.umass.edu is : 128.119.245.12 and desitination port # is 80

Proof:

```
C:\Users\GURWINDER\Downloads\wireshark-traces(1)\tcp-ethereal-trace-1 213 total packets, 213 shown

No.     Time              Source                Destination           Protocol Length Info
      1 06:44:20.570381    192.168.1.102         128.119.245.12        TCP      62     1161 → 80 [SYN] Seq=0 Win=16384 Len=0
MSS=1460 SACK_PERM=1
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0111 .... = Header Length: 28 bytes (7)
    Flags: 0x002 (SYN)
    Window size value: 16384
    [Calculated window size: 16384]
    Checksum: 0xf6e9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
    [Timestamps]
```

3) IP address of source is : 192.168.1.102 and source port # is: 1161

Proof:

```
C:\Users\GURWINDER\Downloads\wireshark-traces(1)\tcp-ethereal-trace-1 213 total packets, 213 shown

No.     Time              Source                Destination           Protocol Length Info
    199 06:44:25.867722    192.168.1.102         128.119.245.12        HTTP     104    POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1
(text/plain)
Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 50]
    Sequence number: 164041    (relative sequence number)
    [Next sequence number: 164091    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x9f0f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (50 bytes)
    TCP segment data (50 bytes)
[122 Reassembled TCP Segments (164090 bytes): #4(565), #5(1460), #7(1460), #8(1460), #10(1460), #11(1460), #13(1147), #18(1460),
#19(1460), #20(1460), #21(1460), #22(1460), #23(892), #30(1460), #31(1460), #32(1460), #33(1460), #34(1460), #3]
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "---------------------------265001916915724"
```

4) [TCP SYN] Sequence number 0 is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu. Flags is what identifies the segment as a SYN segment

Proof:

C:\Users\GURWINDER\Downloads\wireshark-traces(1)\tcp-ethereal-trace-1 213 total packets, 213 shown

```
No.     Time              Source                Destination           Protocol Length Info
      1 06:44:20.570381    192.168.1.102         128.119.245.12        TCP      62     1161 → 80 [SYN] Seq=0 Win=16384 Len=0
MSS=1460 SACK_PERM=1
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0111 .... = Header Length: 28 bytes (7)
    Flags: 0x002 (SYN)
    Window size value: 16384
    [Calculated window size: 16384]
    Checksum: 0xf6e9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
    [Timestamps]
```

5) [SYNACK] Sequence number 0 is sent by gaia.cs.umass.edu to the client computer in reply to the SYN. The value of the acknowledgement field in the computer in reply to the SSN is 1. (Gaia.cs.umass.edu) determine the value by looking at the next sequence number. Flags identify the segment as a SYNACK segment.

Proof:

C:\Users\GURWINDER\Downloads\wireshark-traces(1)\tcp-ethereal-trace-1 213 total packets, 213 shown

```
No.     Time              Source                Destination           Protocol Length Info
      2 06:44:20.593553    128.119.245.12        192.168.1.102         TCP      62     80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840
Len=0 MSS=1460 SACK_PERM=1
Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0111 .... = Header Length: 28 bytes (7)
    Flags: 0x012 (SYN, ACK)
    Window size value: 5840
    [Calculated window size: 5840]
    Checksum: 0x774d [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
    [SEQ/ACK analysis]
    [Timestamps]
```

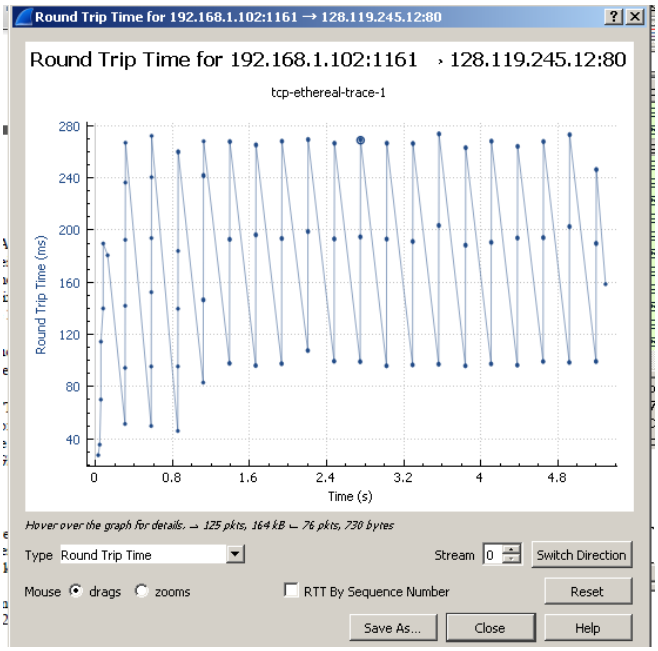
6) Sequence of TCP segment containing the HTTP POST command is 164041.

Proof:

	Time	Source	Destination	Protocol	Length	Info
199	06:44:25.867722	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-la
203	06:44:26.031556	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK

```
Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:2
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 5
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 50]
    Sequence number: 164041    (relative sequence number)
    [Next sequence number: 164091    (relative sequence number)]
```

7) Sequence number of first six segments is 0,1,1,566,2026,3486

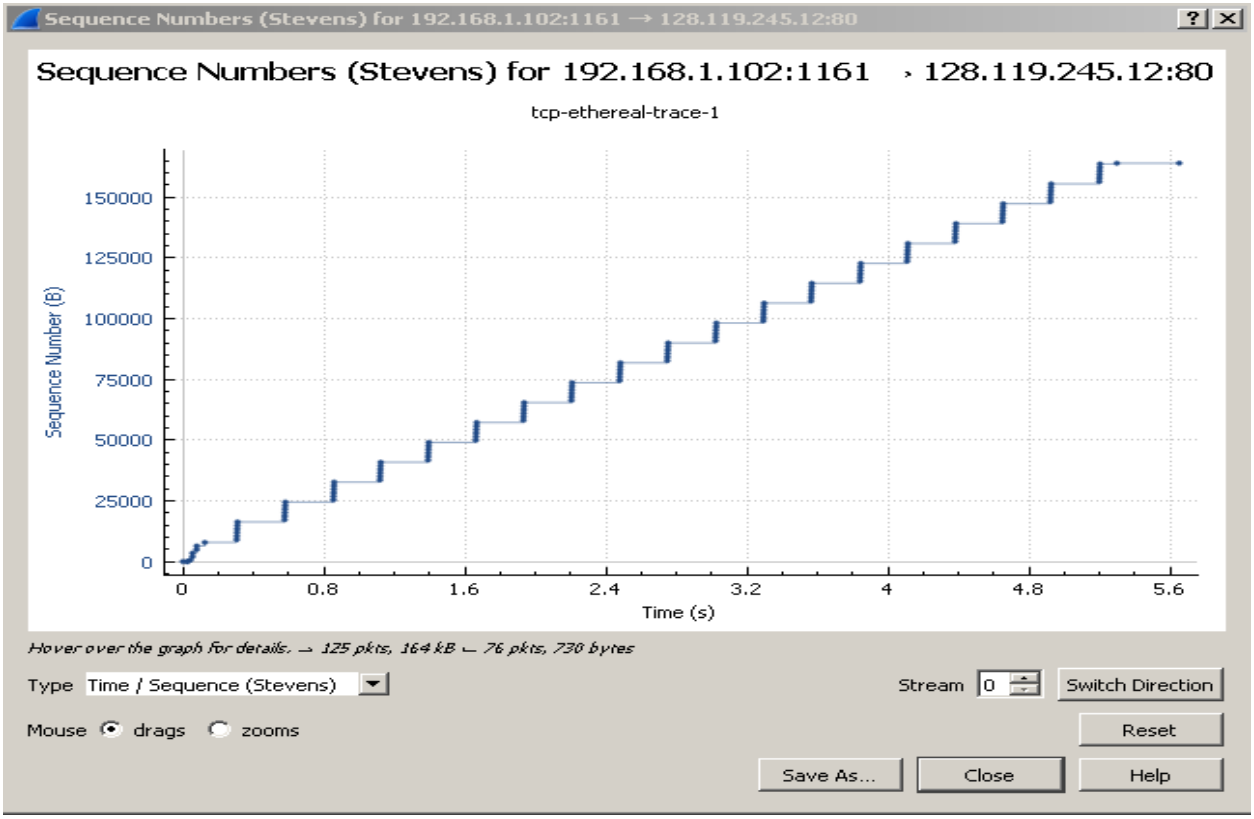


8) The length of the each of the first six TCP segments is

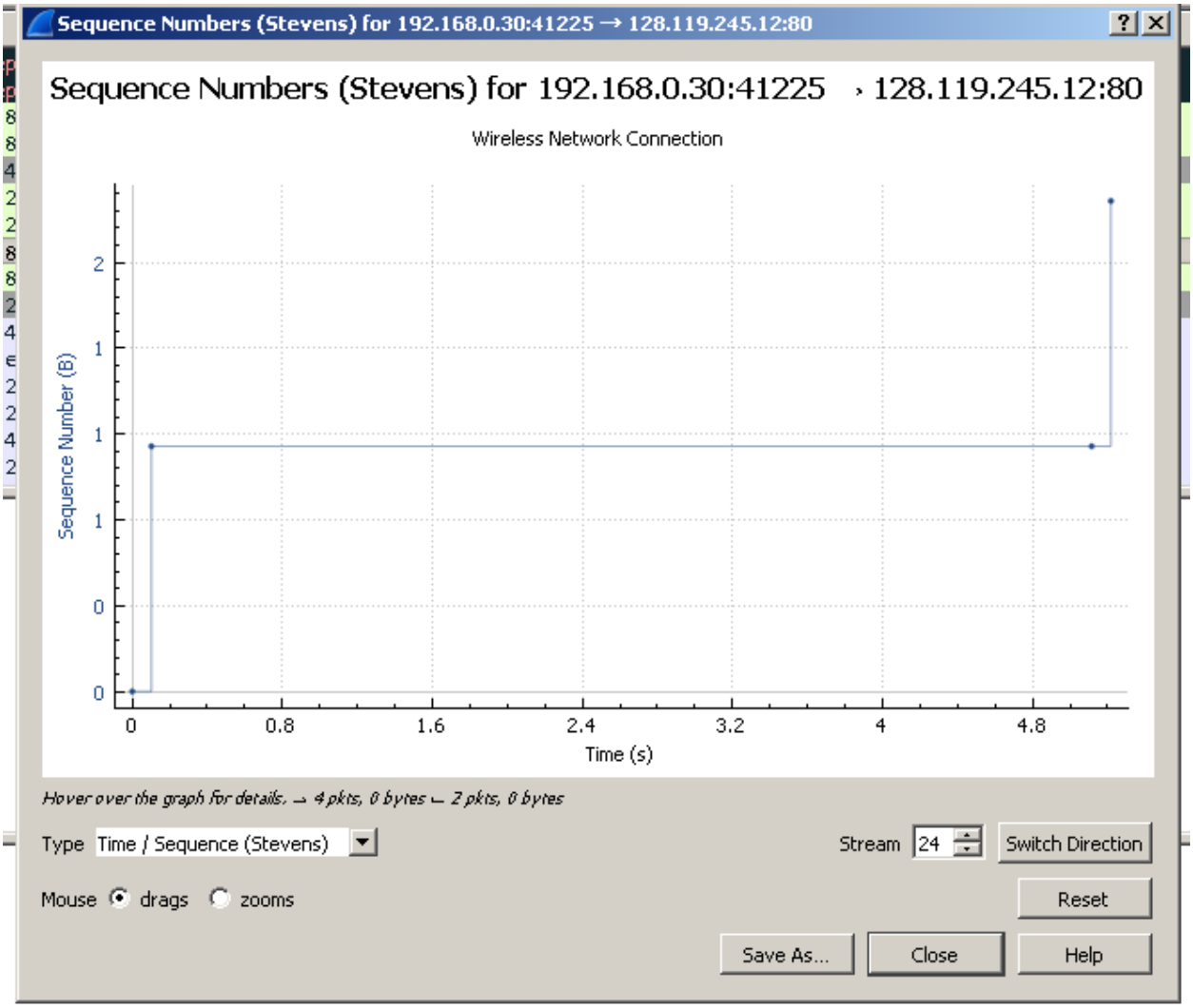
   a. 1- 0

b. 2- 0
c. 3- 0
d. 4- 565
e. 5- 1460
f. 6- 0

9) The minimum buffer space is determined by the calculated window which is 17520 bytes. In the HTTP POST, the SEQ/ACK analysis indicates Bytes sent last was 4702 which is nowhere near the minimum buffer size therefore there should be no throttling.
10) There are no retransmitted segments in the trace file. I have checked the SEQ number and ACK number if they have been resent.
11) Data that the receiver typically acknowledge in an ACK is 432 bits
12) ((731-0)/ 0.02326500 seconds) = 31,420.58, I have taken last ACK and minus that number with last ACK and divided that number with time of last ACK.
13) Slow start phase begins around 500 and ends around 125000. Congestion avoidance takes over at 1125000. TCP depends on application which affects the flow of traffic and according to this graph TCP senders are responsible for causing to much traffic.



14)


Sequence Numbers (Stevens) for 192.168.0.30:41225 → 128.119.245.12:80
Sequence Numbers (Stevens) for 192.168.0.30:41225 › 128.119.245.12:80
Wireless Network Connection
Sequence Number (B)
Time (s)
0
0.8
1.6
2.4
3.2
4
4.8
Hover over the graph for details. → 4 pkts, 0 bytes ← 2 pkts, 0 bytes
Type
Time / Sequence (Stevens)
Stream
24
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help