

Nama: Daffa Harikhsan  
NIM: 23/513044/PA/21918

## Tugas 9

No.	Time	Source	Destination	Protocol	Length	Info
96	4.147482	192.168.0.101	192.168.0.1	HTTP	250	GET /gatedesc.xml HTTP/1.1
102	4.159517	192.168.0.1	192.168.0.101	HTTP/X..	531	HTTP/1.1 200 OK
147	14.240977	192.168.0.101	192.168.0.1	HTTP	250	GET /gatedesc.xml HTTP/1.1
152	14.132037	192.168.0.1	192.168.0.101	HTTP/X..	531	HTTP/1.1 200 OK
420	24.342530	192.168.0.101	192.168.0.1	HTTP	250	GET /gatedesc.xml HTTP/1.1
426	24.345861	192.168.0.1	192.168.0.101	HTTP/X..	531	HTTP/1.1 200 OK
572	34.314344	192.168.0.101	192.168.0.1	HTTP	250	GET /gatedesc.xml HTTP/1.1
582	34.330302	192.168.0.101	192.168.0.1	HTTP/X..	531	HTTP/1.1 200 OK
875	44.514177	192.168.0.101	128.119.245.12	HTTP	1289	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
870	44.717262	192.168.0.101	192.168.0.1	HTTP	250	GET /gatedesc.xml HTTP/1.1
879	44.720815	192.168.0.1	192.168.0.101	HTTP/X..	531	HTTP/1.1 200 OK
915	44.827524	128.119.245.12	192.168.0.1	HTTP	831	HTTP/1.1 200 OK (text/html)
922	44.979876	192.168.0.101	128.119.245.12	HTTP	484	GET /favicon.ico HTTP/1.1
931	45.258462	128.119.245.12	192.168.0.1	HTTP	538	HTTP/1.1 404 Not Found (text/html)
972	54.361901	192.168.0.1	192.168.0.1	HTTP	250	GET /gatedesc.xml HTTP/1.1
977	54.376203	192.168.0.1	192.168.0.101	HTTP/X..	531	HTTP/1.1 200 OK

Ethernet II, Src: 88:85:9b:5c:34:bd (88:85:9b:5c:34:bd), Dst: TplinkTechno\_2f:d3:04 (b0:4e:26:2f:d3:04)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 64025, Dst Port: 80, Seq: 151718, Ack: 1, Len: 1235

[Information] TCP Segments (152952 bytes): #701(633), #702(1412), #703(1412), #704(1412), #705(1412), #706(1412), #707(1412), #708(1412), #709(1412), #710(1412)

Hypertext Transfer Protocol

POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nContent-Length: 152319\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36\r\nOrigin: null\r\nContent-Type: multipart/form-data; boundary=---WebKitFormBoundaryt8HIN8ok6Etyjn3\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7\r\n\r\n[Response in frame: 915]

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm]

File Data: 152319 bytes

MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryt8HIN8ok6Etyjn3"

Frame (1289 bytes)

Reassembled TCP (152952 bytes)

Hypertext Transfer Protocol	Packets: 982 · Displayed: 16 (1.6%) · Dropped: 0 (0.0%)	Profile: Default
Ethernet II, Src: 88:85:9b:5c:34:bd (88:85:9b:5c:34:bd), Dst: TplinkTechno_2f:d3:04 (b0:4e:26:2f:d3:04)		
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 128.119.245.12		
Transmission Control Protocol, Src Port: 64025, Dst Port: 80, Seq: 151718, Ack: 1, Len: 1235		
[Information] Reassembled TCP Segments (152952 bytes): #701(633), #702(1412), #703(1412), #704(1412), #705(1412), #706(1412), #707(1412), #708(1412), #709(1412), #710(1412)		
Hypertext Transfer Protocol		
POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nContent-Length: 152319\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36\r\nOrigin: null\r\nContent-Type: multipart/form-data; boundary=---WebKitFormBoundaryt8HIN8ok6Etyjn3\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7\r\n\r\n[Response in frame: 915]		
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm]		
File Data: 152319 bytes		
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundaryt8HIN8ok6Etyjn3"		

### Activity 9.3

1. Berapakah nomor urut segmen TCP SYN yang digunakan untuk memulai koneksi TCP antara komputer klien dan gaia.cs.umass.edu? Catatan: pertanyaan di sini mengacu pada nomor urut "mentah" yang dibawa dalam segmen TCP itu sendiri, dan BUKAN nomor paket dalam kolom "No." yang diberikan oleh Wireshark. Ingat bahwa tidak ada yang disebut "nomor paket" dalam TCP atau UDP; namun, ada nomor urut dalam TCP, dan itulah yang kita cari di sini. Juga, perhatikan bahwa ini bukan nomor urut relatif terhadap nomor urut awal sesi TCP ini. Apa yang ada dalam segmen TCP ini yang mengidentifikasikannya sebagai segmen SYN?

Jawab:

697	43.019533	192.168.0.101	128.119.245.12	TCP	66	64025	+ 80	[SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	8555
698	43.019738	192.168.0.101	128.119.245.12	TCP	66	64026	+ 80	[SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	8555
699	43.370918	128.119.245.12	192.168.0.101	TCP	66	80	+ 64025	[SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128	8555
700	43.371016	192.168.0.101	128.119.245.12	TCP	54	60205	+ 80	[ACK] Seq=1 Ack=1 Win=65280 Len=0	8555
701	43.371488	192.168.0.101	128.119.245.12	TCP	687	64025	+ 80	[PSH, ACK] Seq=1 Ack=1 Win=65280 Len=633 [TCP PDU reassembled in 8555]	8555
702	43.371568	192.168.0.101	128.119.245.12	TCP	1466	64025	+ 80	[ACK] Seq=634 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 8555]	8555
703	43.371568	192.168.0.101	128.119.245.12	TCP	1466	64025	+ 80	[ACK] Seq=2046 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 8555]	8555
704	43.371568	192.168.0.101	128.119.245.12	TCP	1466	64025	+ 80	[ACK] Seq=3458 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 8555]	8555
705	43.371568	192.168.0.101	128.119.245.12	TCP	1466	64025	+ 80	[ACK] Seq=4822 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 8555]	8555
706	43.371568	192.168.0.101	128.119.245.12	TCP	1466	64025	+ 80	[ACK] Seq=6282 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 8555]	8555
707	43.371568	192.168.0.101	128.119.245.12	TCP	1466	64025	+ 80	[ACK] Seq=7694 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 8555]	8555
708	43.371568	192.168.0.101	128.119.245.12	TCP	1466	64025	+ 80	[ACK] Seq=9106 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 8555]	8555
709	43.371568	192.168.0.101	128.119.245.12	TCP	1466	64025	+ 80	[ACK] Seq=10518 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 8555]	8555
710	43.371568	192.168.0.101	128.119.245.12	TCP	1466	64025	+ 80	[ACK] Seq=11930 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 8555]	8555
711	43.484551	128.119.245.12	192.168.0.101	TCP	66	80	+ 64026	[SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128	8555
712	43.484559	128.119.245.12	192.168.0.101	TCP	66	8025	+ 64026	[SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128	8555

```

Transmission Control Protocol, Src Port: 64026, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 64026
  Destination Port: 80
  [Stream index: 30]
  [Stream Packet Number: 1]
  [Conversation completeness: Incomplete, ESTABLISHED (7)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 4166021214
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x002 (SYN)
  Window: 65535
  [Calculated window size: 65535]
  Checksum: 0xd564 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  [Timestamps]

```

- Nomor urut segmen TCP SYN yang digunakan untuk memulai koneksi TCP antara komputer klien dan gaia.cs.umass.edu adalah 4166021214.
- Untuk mengetahui bahwa ini merupakan segmen SYN terlihat pada Flags: 0x002 (SYN)

2. Berapakah nomor urut segmen SYNACK yang dikirim oleh gaia.cs.umass.edu ke komputer klien sebagai tanggapan terhadap SYN? Apa yang ada dalam segmen yang mengidentifikasikannya sebagai segmen SYNACK? Berapa nilai bidang Pengakuan dalam segmen SYNACK? Bagaimana gaia.cs.umass.edu menentukan nilai ini?

Jawab:

697	43.018533	192.168.0.101	128.119.245.12	TCP	66 64025 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
698	43.147390	192.168.0.101	128.119.245.12	TCP	66 64026 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
699	43.370918	128.119.245.12	192.168.0.101	TCP	66 80 → 64025 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
700	43.371016	192.168.0.101	128.119.245.12	TCP	54 64025 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
701	43.371488	192.168.0.101	128.119.245.12	TCP	687 64025 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=633 [TCP PDU reassembled in 855]
702	43.371568	192.168.0.101	128.119.245.12	TCP	1466 64025 → 80 [ACK] Seq=634 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 855]
703	43.371568	192.168.0.101	128.119.245.12	TCP	1466 64025 → 80 [ACK] Seq=2046 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 855]
704	43.371568	192.168.0.101	128.119.245.12	TCP	1466 64025 → 80 [ACK] Seq=3458 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 855]
705	43.371568	192.168.0.101	128.119.245.12	TCP	1466 64025 → 80 [ACK] Seq=4870 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 855]
706	43.371568	192.168.0.101	128.119.245.12	TCP	1466 64025 → 80 [ACK] Seq=6282 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 855]
707	43.371568	192.168.0.101	128.119.245.12	TCP	1466 64025 → 80 [ACK] Seq=7694 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 855]
708	43.371568	192.168.0.101	128.119.245.12	TCP	1466 64025 → 80 [ACK] Seq=9106 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 855]
709	43.371568	192.168.0.101	128.119.245.12	TCP	1466 64025 → 80 [ACK] Seq=10518 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 855]
710	43.371568	192.168.0.101	128.119.245.12	TCP	1466 64025 → 80 [ACK] Seq=11930 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 855]
711	43.484551	128.119.245.12	192.168.0.101	TCP	66 80 → 64026 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
712	43.484550	192.168.0.101	128.119.245.12	TCP	54 64026 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0

```

Transmission Control Protocol, Src Port: 80, Dst Port: 64025, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 64025
  [Stream index: 29]
  [Stream Packet Number: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 4267660124
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 782396060
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x012 (SYN, ACK)
  Window: 29200
  [Calculated window size: 29200]
  Checksum: 0xe12a [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
  [Timestamps]
  [SEQ/ACK analysis]

```

- Nomor urut segmen SYNACK yang dikirim oleh gaia.cs.umass.edu ke komputer klien adalah 4267660124
- Yang ada didalam segmen yang mengidentifikasikannya sebagai segmen SYNACK adalah Flags: 0x012 (SYN, ACK)
- Nilai bidang pengakuannya (Acknowledgment number) yakni 782396060
- Cara gaia.cs.umass.edu menentukannya dalam segmen SYNACK adalah satu lebih tinggi dari nomor urut (Sequence Number) dari segmen SYN yang dikirim oleh klien. Dengan kata lain sequence number dari segmen SYN ditambah 1, sebagai tanda bahwa telah menerima segmen SYN dan mengharapkan data berikutnya dimulai dari nomor tersebut.

3. Berapakah nomor urut segmen TCP yang berisi header pesan HTTP POST? Catatan bahwa untuk menemukan header pesan POST, Anda perlu melihat lebih dalam ke Konten Paket di bagian bawah jendela Wireshark. Cari segmen yang berisi teks ASCII "POST" di bidang DATA. Berapa banyak byte

Jawab:

- Nomor urut segmen TCP = sequence number (RAW) 782547777

- Jumlah Byte data dalam Payload = 1234 bytes

- Semua data tidak muat dalam satu segment. Terdapat indikasi bahwa ini adalah bagian dari beberapa segmen yang direkonstruksi, yang artinya data *alice.txt* lebih besar dari satu segmen dan memerlukan beberapa segmen untuk pengirimannya. [segmen count:109] [reassembled TCP length: 152952] artinya bahwa ada total 109 segmen yang direkonstruksi untuk menyusun data sebesar 152,391 bytes. Jika data *alice.txt* hanya muat dalam satu segmen, tidak akan ada informasi bahwa banyak segmen telah direkonstruksi.

4. Berapa panjang (header dan payload) dari segmen yang berisi header pesan POST?

Jawab:

```

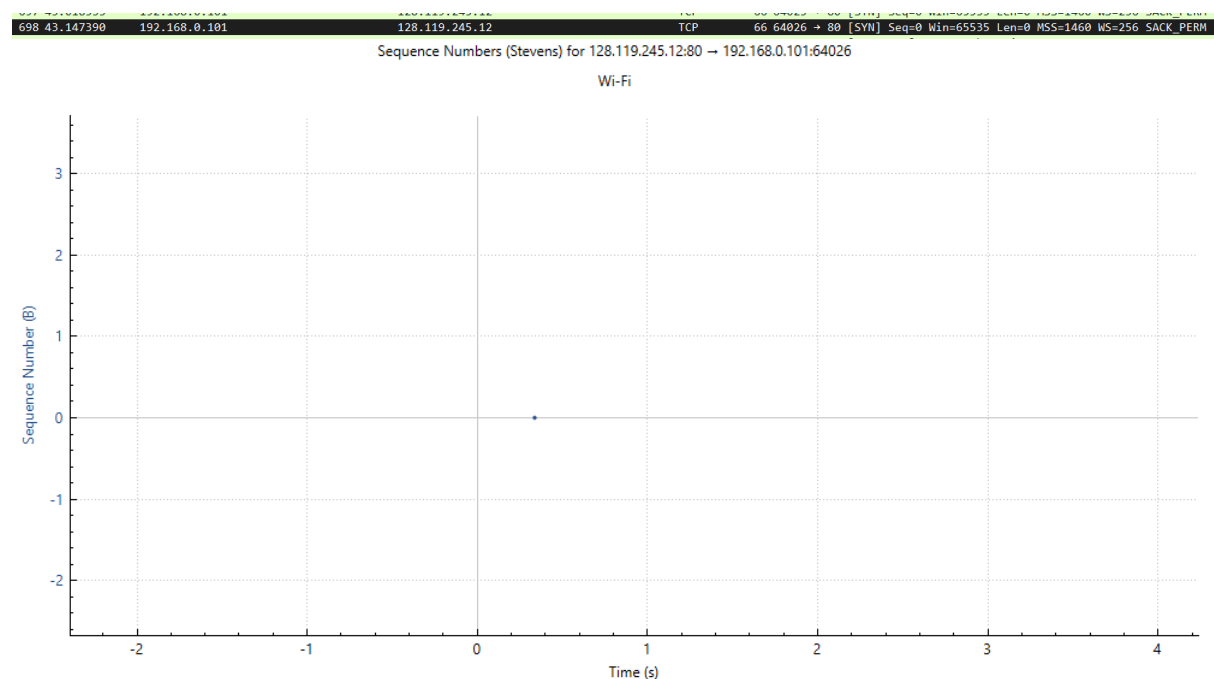
▶ Frame 855: 1289 bytes on wire (10312 bits), 1289 bytes captured (10312 bits) on interface \Device\NPF_{C4EE137D-D70F-4D72-AE40-8E14E88054CA}, id 0
▶ Ethernet II, Src: 88:85:9b:5c:34:bd (88:85:9b:5c:34:bd), Dst: TplinkTechno_2f:d3:04 (b0:4e:26:2f:d3:04)
▶ Internet Protocol Version 4, Src: 192.168.0.101, Dst: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 64025, Dst Port: 80, Seq: 151718, Ack: 1, Len: 1235
    Source Port: 64025
    Destination Port: 80
    [Stream index: 29]
    [Stream Packet Number: 146]
    ▶ [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1235]
    Sequence Number: 151718 (relative sequence number)
    Sequence Number (raw): 782547777
    [Next Sequence Number: 152953 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 4267660125
    0101 ... = Header Length: 20 bytes (5)
    ▶ Flags: 0x018 (PSH, ACK)
    Window: 255
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
    Checksum: 0x3a01 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    ▶ [Timestamps]
    ▼ [SEQ/ACK analysis]
        [iRTT: 0.352483000 seconds]
        [Bytes in flight: 63363]
        [Bytes sent since last PSH flag: 4059]
        TCP payload (1235 bytes)
        TCP segment data (1235 bytes)
    ▶ [109 Reassembled TCP Segments (152952 bytes): #701(633), #702(1412), #703(1412), #704(1412), #705(1412), #706(1412), #707(1412), #708(1412), #709(1412), #710(1412), #711(1412), #712(1412), #713(1412), #714(1412), #715(1412), #716(1412), #717(1412), #718(1412), #719(1412), #720(1412), #721(1412), #722(1412), #723(1412), #724(1412), #725(1412), #726(1412), #727(1412), #728(1412), #729(1412), #730(1412), #731(1412), #732(1412), #733(1412), #734(1412), #735(1412), #736(1412), #737(1412), #738(1412), #739(1412), #740(1412), #741(1412), #742(1412), #743(1412), #744(1412), #745(1412), #746(1412), #747(1412), #748(1412), #749(1412), #750(1412), #751(1412), #752(1412), #753(1412), #754(1412), #755(1412), #756(1412), #757(1412), #758(1412), #759(1412), #760(1412), #761(1412), #762(1412), #763(1412), #764(1412), #765(1412), #766(1412), #767(1412), #768(1412), #769(1412), #770(1412), #771(1412), #772(1412), #773(1412), #774(1412), #775(1412), #776(1412), #777(1412), #778(1412), #779(1412), #780(1412), #781(1412), #782(1412), #783(1412), #784(1412), #785(1412), #786(1412), #787(1412), #788(1412), #789(1412), #790(1412), #791(1412), #792(1412), #793(1412), #794(1412), #795(1412), #796(1412), #797(1412), #798(1412), #799(1412), #800(1412), #801(1412), #802(1412), #803(1412), #804(1412), #805(1412), #806(1412), #807(1412), #808(1412), #809(1412), #810(1412), #811(1412), #812(1412), #813(1412), #814(1412), #815(1412), #816(1412), #817(1412), #818(1412), #819(1412), #820(1412), #821(1412), #822(1412), #823(1412), #824(1412), #825(1412), #826(1412), #827(1412), #828(1412), #829(1412), #830(1412), #831(1412), #832(1412), #833(1412), #834(1412), #835(1412), #836(1412), #837(1412), #838(1412), #839(1412), #840(1412), #841(1412), #842(1412), #843(1412), #844(1412), #845(1412), #846(1412), #847(1412), #848(1412), #849(1412), #850(1412), #851(1412), #852(1412), #853(1412), #854(1412), #855(1412), #856(1412), #857(1412), #858(1412), #859(1412), #860(1412), #861(1412), #862(1412), #863(1412), #864(1412), #865(1412), #866(1412), #867(1412), #868(1412), #869(1412), #870(1412), #871(1412), #872(1412), #873(1412), #874(1412), #875(1412), #876(1412), #877(1412), #878(1412), #879(1412), #880(1412), #881(1412), #882(1412), #883(1412), #884(1412), #885(1412), #886(1412), #887(1412), #888(1412), #889(1412), #890(1412), #891(1412), #892(1412), #893(1412), #894(1412), #895(1412), #896(1412), #897(1412), #898(1412), #899(1412), #900(1412), #901(1412), #902(1412), #903(1412), #904(1412), #905(1412), #906(1412), #907(1412), #908(1412), #909(1412), #910(1412), #911(1412), #912(1412), #913(1412), #914(1412), #915(1412), #916(1412), #917(1412), #918(1412), #919(1412), #920(1412), #921(1412), #922(1412), #923(1412), #924(1412), #925(1412), #926(1412), #927(1412), #928(1412), #929(1412), #930(1412), #931(1412), #932(1412), #933(1412), #934(1412), #935(1412), #936(1412), #937(1412), #938(1412), #939(1412), #940(1412), #941(1412), #942(1412), #943(1412), #944(1412), #945(1412), #946(1412), #947(1412), #948(1412), #949(1412), #950(1412), #951(1412), #952(1412), #953(1412), #954(1412), #955(1412), #956(1412), #957(1412), #958(1412), #959(1412), #960(1412), #961(1412), #962(1412), #963(1412), #964(1412), #965(1412), #966(1412), #967(1412), #968(1412), #969(1412), #970(1412), #971(1412), #972(1412), #973(1412), #974(1412), #975(1412), #976(1412), #977(1412), #978(1412), #979(1412), #980(1412), #981(1412), #982(1412), #983(1412), #984(1412), #985(1412), #986(1412), #987(1412), #988(1412), #989(1412), #990(1412), #991(1412), #992(1412), #993(1412), #994(1412), #995(1412), #996(1412), #997(1412), #998(1412), #999(1412), #1000(1412), #1001(1412), #1002(1412), #1003(1412), #1004(1412), #1005(1412), #1006(1412), #1007(1412), #1008(1412), #1009(1412), #1010(1412), #1011(1412), #1012(1412), #1013(1412), #1014(1412), #1015(1412), #1016(1412), #1017(1412), #1018(1412), #1019(1412), #1020(1412), #1021(1412), #1022(1412), #1023(1412), #1024(1412), #1025(1412), #1026(1412), #1027(1412), #1028(1412), #1029(1412), #1030(1412), #1031(1412), #1032(1412), #1033(1412), #1034(1412), #1035(1412), #1036(1412), #1037(1412), #1038(1412), #1039(1412), #1040(1412), #1041(1412), #1042(1412), #1043(1412
```

untuk panjang header = 20 bytes, dan untuk payload = 1235 bytes maka jika panjang total segmen =  $20 + 1235 = 1255$  bytes (header + payload).

5. Berapa banyak segmen yang diteruskan? Untuk menjawab pertanyaan ini, lakukan hal berikut:

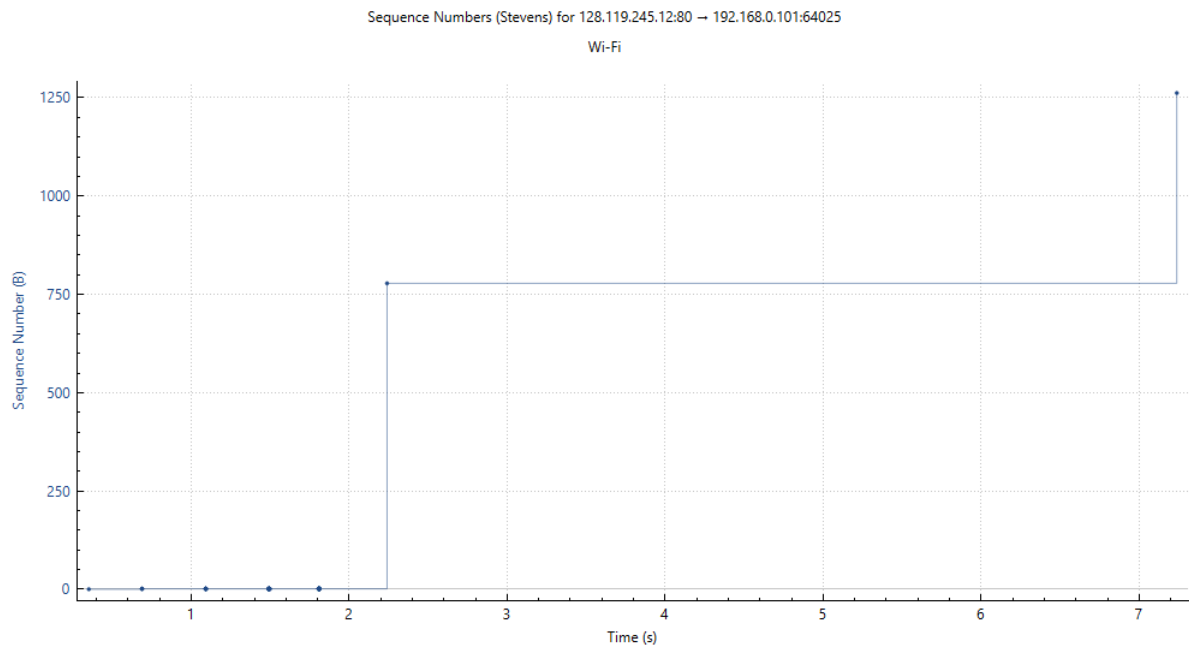
- Pilih salah satu segmen TCP yang dikirim dari komputer Anda ke server dari Daftar Paket.
- Pilih menu: Statistik → Grafik Aliran TCP → Urutan Waktu (Stevens).
- Anda akan melihat plot nomor urut versus waktu. Setiap titik pada plot ini mewakili kapan segmen TCP dikirim dari PC Anda ke server.

Dari TCP

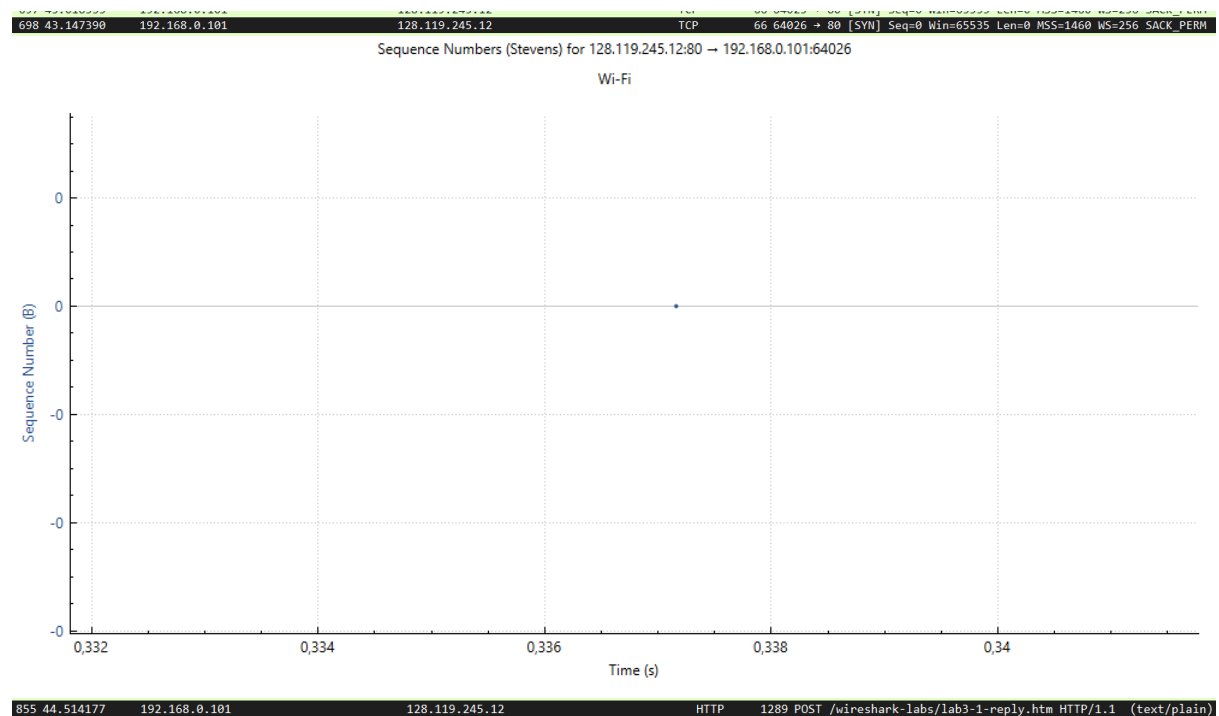


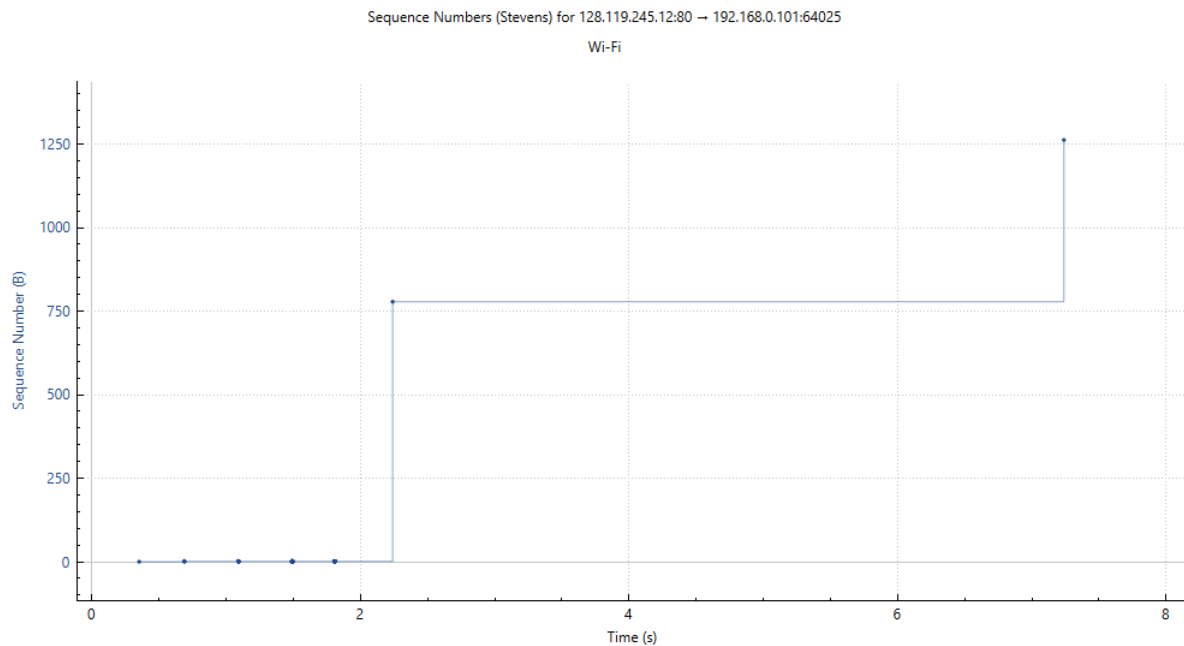
Dari HTTP

855	44.514177	192.168.0.101	128.119.245.12	HTTP	1289	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
-----	-----------	---------------	----------------	------	------	---



(d) Karena transmisi paket terjadi dalam waktu yang sangat singkat, zoom in (gulir ke atas) pada rentang waktu yang perlu dianalisis secara detail. Perhatikan bahwa sekelompok titik yang menumpuk ke atas pada waktu yang sama menunjukkan serangkaian paket yang dikirim secara berurutan oleh pengirim. Pikirkan tentang apa yang perlu Anda periksa untuk menentukan apakah ada segmen yang diteruskan.





## Activity 9.4

http					
No.	Time	Source	Destination	Protocol	Length Info
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104 POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784 HTTP/1.1 200 OK (text/html)

1. Pada pukul berapa segmen pertama (yang berisi HTTP POST) dikirim?

Jawab:

```

▼ Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
  Encapsulation type: Ethernet (1)
    Arrival Time: Aug 21, 2004 20:44:25.867722000 SE Asia Standard Time
    UTC Arrival Time: Aug 21, 2004 13:44:25.867722000 UTC
    Epoch Arrival Time: 1093095865.867722000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000084000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 5.297341000 seconds]
    Frame Number: 199
    Frame Length: 104 bytes (832 bits)
    Capture Length: 104 bytes (832 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:mime_multipart:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
  
```

**Arrival Time:** August 21, 2004, 20:44:25.867722000 SE Asia Standard Time.

2. Pada pukul berapa ACK untuk segmen pertama yang berisi data ini diterima?

Jawab:

TCP (ACK,SYN) (SEGMENT pertama)

6	0.053937	128.119.245.12	192.168.1.102	TCP	60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
---	----------	----------------	---------------	-----	---

```

▼ Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Aug 21, 2004 20:44:20.624318000 SE Asia Standard Time
  UTC Arrival Time: Aug 21, 2004 13:44:20.624318000 UTC
  Epoch Arrival Time: 1093095860.624318000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.012200000 seconds]
  [Time delta from previous displayed frame: 0.012200000 seconds]
  [Time since reference or first frame: 0.053937000 seconds]
  Frame Number: 6
  Frame Length: 60 bytes (480 bits)
  Capture Length: 60 bytes (480 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
▼ Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a)
  ▶ Destination: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a)
  ▶ Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  Type: IPv4 (0x0800)
  [Stream index: 0]
  ▶ Trailer: da12000047a5
▼ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x5872 (22642)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 55
  Protocol: TCP (6)
  Header Checksum: 0xb3cb [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 128.119.245.12
  Destination Address: 192.168.1.102
  [Stream index: 0]
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 566, Len: 0
  Source Port: 80
  Destination Port: 1161
  [Stream index: 0]
  [Stream Packet Number: 6]
  ▶ [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 883061786
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 566 (relative ack number)
  Acknowledgment number (raw): 232129578
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x010 (ACK)
  Window: 6780
  [Calculated window size: 6780]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x9e30 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0

```

- Acknowledge Number = 566 yang artinya bahwa ini adalah paket ACK untuk data yang dikirim sebelumnya
- Waktu Kedatangan (Arrival Time) untuk paket ini adalah 21 Agustus 2004, 20:44:20.624318000 SE Asia Standard Time.

3. Berapa nilai RTT untuk segmen pertama yang berisi data ini?

Jawab:

Nilai RTT untuk segmen pertama yang berisi data adalah 30.672 milidetik. Ini didapatkan dari:

$$\begin{aligned}
 \text{RTT} &= \text{Waktu penerimaan ACK} - \text{Waktu pengiriman} \\
 &= 20:44:20.624318000 - 20:44:20.593646000 \\
 &= 0.030672 \text{ detik atau } \mathbf{30.672 \text{ milidetik}}
 \end{aligned}$$

4. Berapa nilai RTT untuk segmen TCP yang mengangkut potongan data kedua dan ACK-nya?

Jawab:

TCP( ACK, SYN) (SEGMENT kedua)

Time	Source	Destination	Protocol	Length	Info
9 0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0



```

▼ Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Aug 21, 2004 20:44:20.647675000 SE Asia Standard Time
  UTC Arrival Time: Aug 21, 2004 13:44:20.647675000 UTC
  Epoch Arrival Time: 1093095860.647675000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.022604000 seconds]
  [Time delta from previous displayed frame: 0.022604000 seconds]
  [Time since reference or first frame: 0.077294000 seconds]
  Frame Number: 9
  Frame Length: 60 bytes (480 bits)
  Capture Length: 60 bytes (480 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
▼ Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a)
  ▶ Destination: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a)
  ▶ Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  Type: IPv4 (0x0800)
  [Stream index: 0]
  ▶ Trailer: 879e00003a30
▼ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 40
  Identification: 0x5873 (22643)
  ▶ 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 55
  Protocol: TCP (6)
  Header Checksum: 0xb3ca [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 128.119.245.12
  Destination Address: 192.168.1.102
  [Stream index: 0]
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 2026, Len: 0
  Source Port: 80
  Destination Port: 1161
  [Stream index: 0]
  [Stream Packet Number: 9]
  ▶ [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 883061786
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 2026 (relative ack number)
  Acknowledgment number (raw): 232131038
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x010 (ACK)
  Window: 8760
  [Calculated window size: 8760]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x90c0 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▼ [Timestamps]

```

RTT Kedua = Waktu penerimaan ACK – Waktu pengiriman  
 = 20:44:20.647675000 – 20:44:20.624318000  
 = 0.023357 detik atau **23.357** milidetik

Jadi RTT kedua sekitar 23.357 milidetik

5. Berapa nilai RTT yang Diperkirakan setelah ACK untuk segmen data kedua diterima? Untuk menghitung RTT yang Diperkirakan setelah ACK untuk segmen kedua diterima, anggap bahwa nilai awal RTT yang Diperkirakan sama dengan RTT "aktual" yang diukur untuk segmen pertama.

Kemudian, hitung menggunakan persamaan RTT yang Diperkirakan dan nilai  $\alpha = 0.125$ .

Jawab:

**RTT yang diperkirakan<sub>Baru</sub> = (1-  $\alpha$ ) x RTT yang diperkirakan<sub>Lama</sub> +  $\alpha$  x RTT<sub>aktual</sub> kedua**



Dimana:

- **RTT yang Diperkirakan lama** = 30.672 ms (dari segmen pertama)
- **RTT aktual kedua** = 23.357 ms
- $\alpha = 0.125$

Kita hitung:

$$\begin{aligned}\text{RTT yang diperkirakan}_{\text{Baru}} &= (1 - 0.125) \times 30.672 + 0.125 \times 23.357 \\ &= 0.875 \times 30.672 + 0.125 \times 23.357 \\ &= 26.839 + 2.919625 \\ &= 29.758625 \text{ ms}\end{aligned}$$

Jadi RTT yang diperkirakan setelah ACK untuk segmen data kedua diterima adalah sekitar **29.759 ms**.