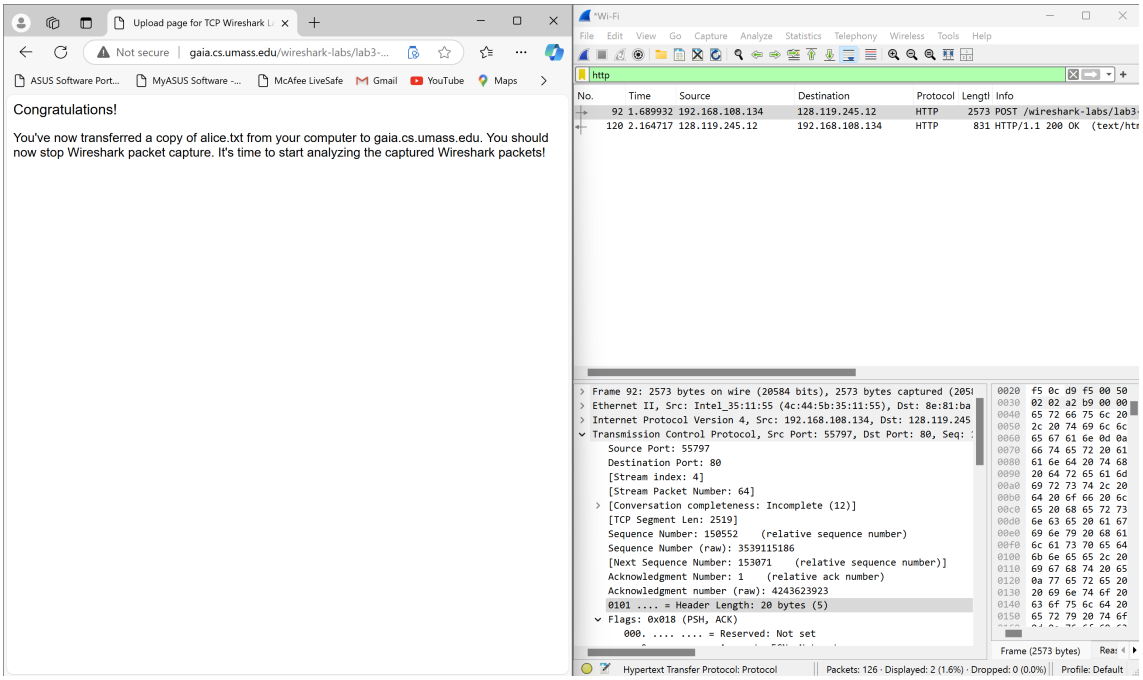
Tugas Pertemuan 9
Praktikum Sistem Komputer dan Jaringan

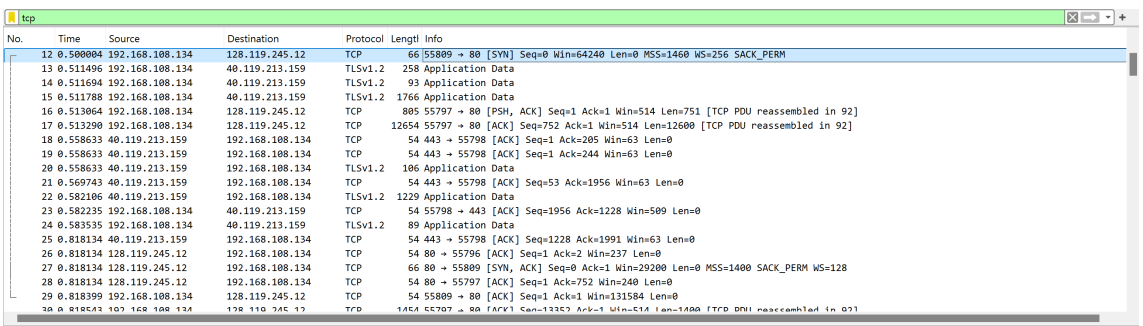
Kosmas Rio Legowo
23/512012/PA/21863
Departemen Ilmu Komputer dan Elektronika
Universitas Gadjah Mada
kosmasriolegowo@mail.ugm.ac.id

Chapter 9 Protokol Pengendalian Transmisi (TCP)

Aktivitas 1 - 9.3 Sniffing Transfer TCP dari File Besar yang Dikirim dari Komputer Anda ke Server Jarak Jauh

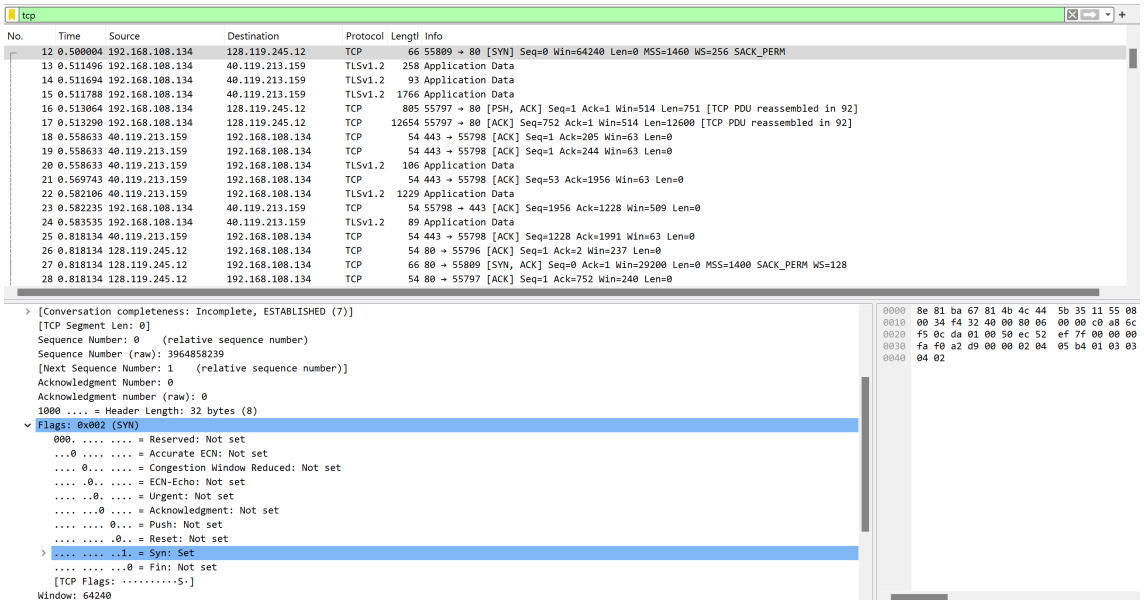
Hasil Aktivitas 1:





Pertanyaan-pertanyaan:

1. Berapakah nomor urut segmen TCP SYN yang digunakan untuk mem- ulai 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 :



   Sequence number (raw) TCP SYNACK yang digunakan untuk memulai koneksi TCP antara komputer klien dan gaia.cs.umass.edu adalah 3964858239.

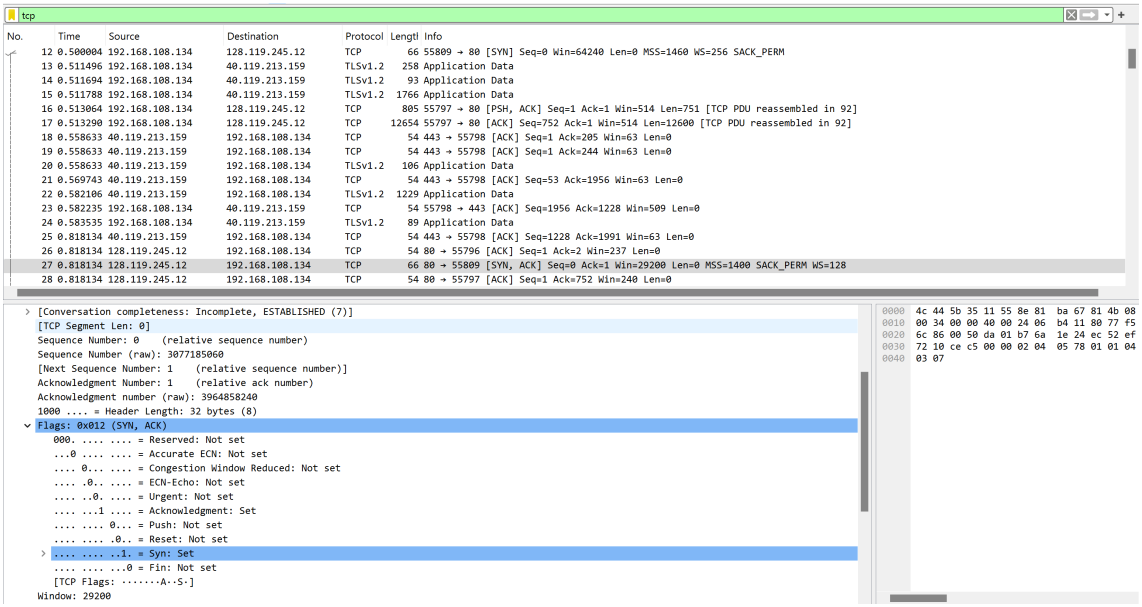
```
> [Conversation completeness: Incomplete, ESTABLISHED (7)]
  [TCP Segment Len: 0]
  Sequence Number: 0    (relative sequence number)
  Sequence Number (raw): 3964858239
  [Next Sequence Number: 1    (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
```

   Hal di dalam segmen TCP ini yang mengidentifikasikannya sebagai segmen SYN adalah karena nilai dari SYN adalah 1 (set).

```
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
  Window: 64240
```

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 :



Sequence number (raw) segmen SYNACK yang dikirim oleh gaia.cs.umass.edu ke komputer klien sebagai tanggapan terhadap SYN adalah 3964858240.

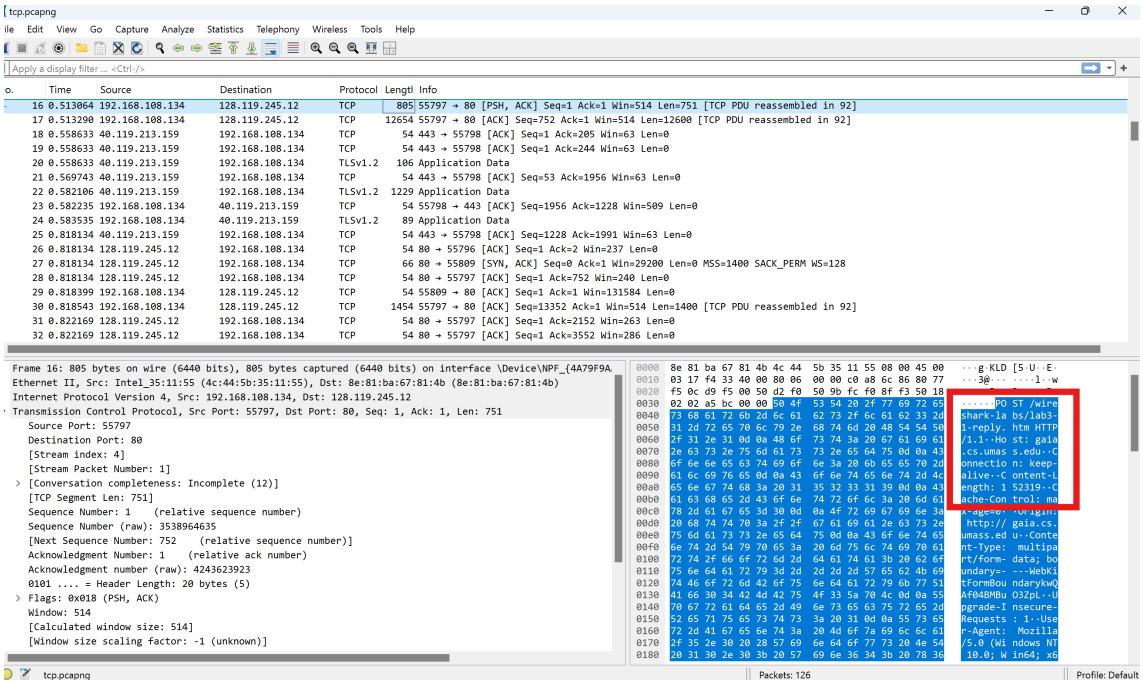
```
  > [Conversation completeness: Incomplete, ESTABLISHED (7)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3077185060
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3964858240
    1000 .... = Header Length: 32 bytes (8)
```

Hal di dalam segmen TCP ini yang mengidentifikasikannya sebagai segmen SYNACK adalah karena nilai dari SYN adalah 1 (set) dan juga nilai dari ACK adalah 1 (Set).

```
Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-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: 29200
```

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 data yang terdapat dalam bidang payload (data) segmen TCP ini? Apakah semua data dalam file alice.txt yang ditransfer muat dalam satu segmen ini?

   Jawab :



   sequence Number (raw) dari TCP segment yang berisi header POST memiliki nilai 3539115186. Tidak seluruh data pada file alice.txt dikirimkan pada satu segment ini, data pada file alice.txt dipecah pada beberapa segment yang dikirimkan setelah TCP segment POST ini.

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

   Jawab :

```
TCP payload (2519 bytes)
TCP segment data (2519 bytes)
```

Payload field pada segment ini memiliki 2519 bytes dan juga headernya adalah 2519 bytes.

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

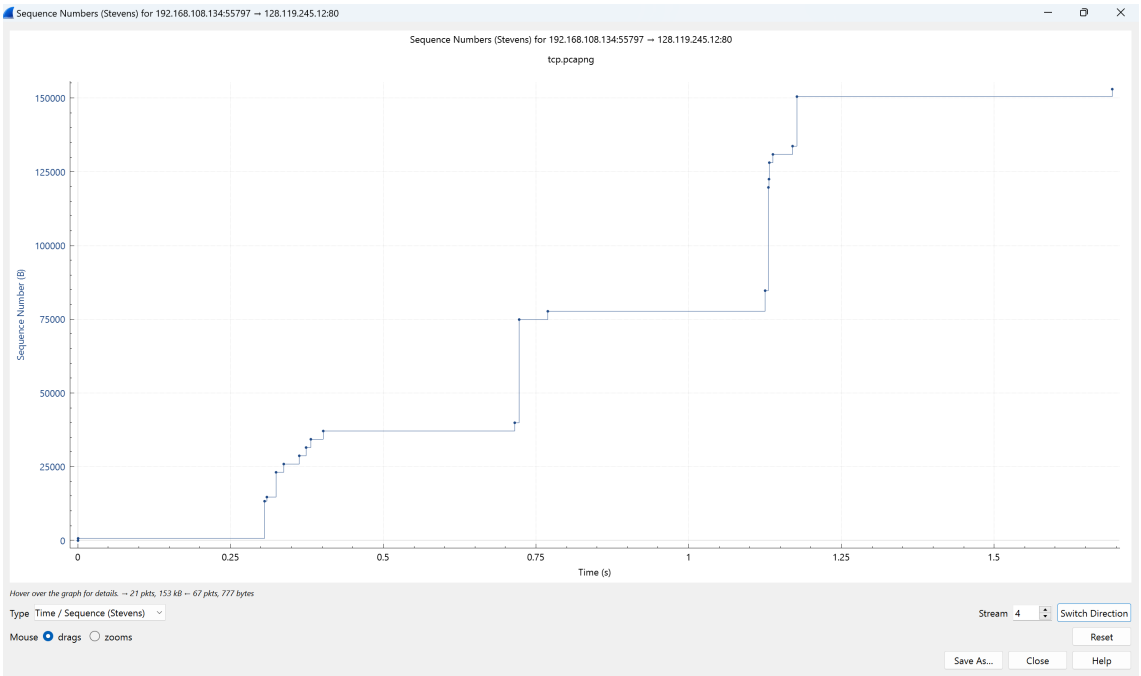
   (a) Pilih salah satu segmen TCP yang dikirim dari komputer Anda ke server dari Daftar Paket.

   (b) Pilih menu: Statistik → Grafik Aliran TCP → Urutan Waktu (Stevens).

   (c) Anda akan melihat plot nomor urut versus waktu. Setiap titik pada plot ini mewakili kapan segmen TCP dikirim dari PC Anda ke server.

   (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.

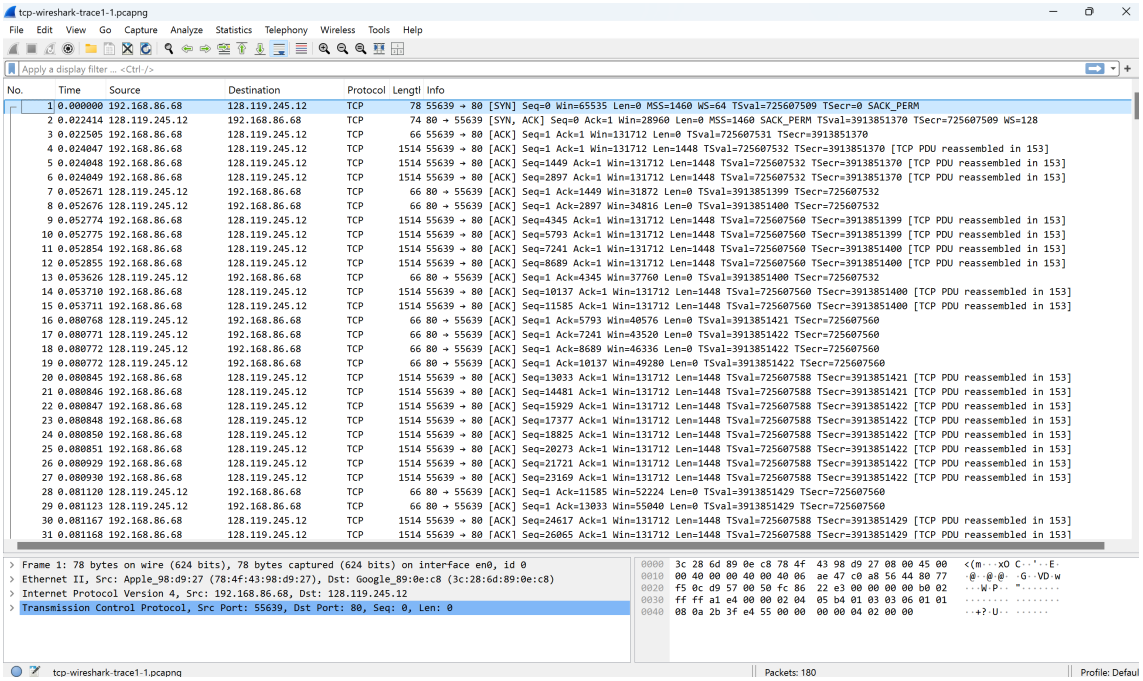
Jawab :

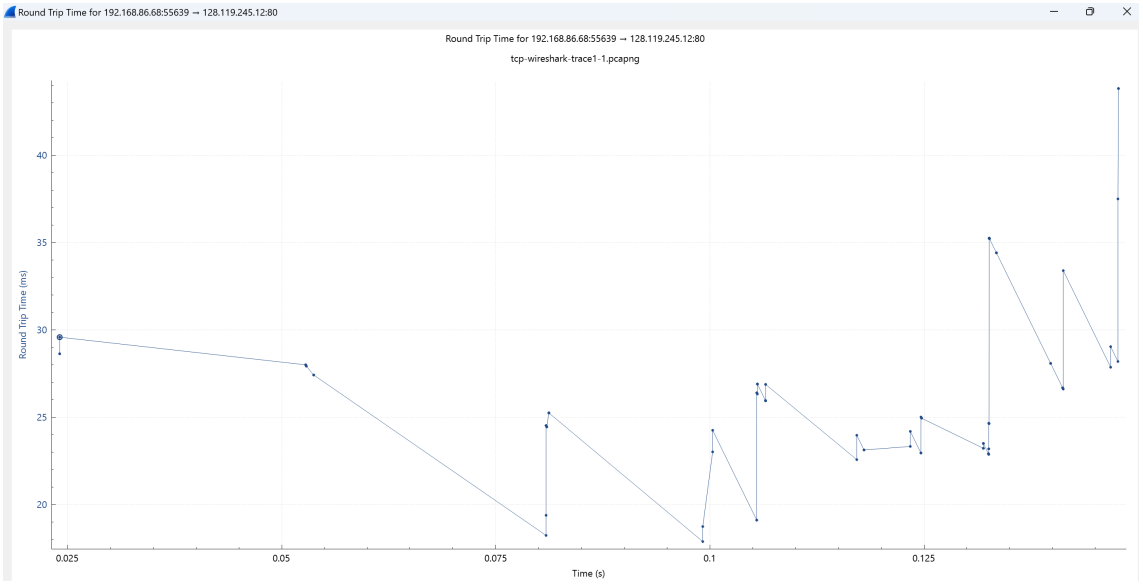


Tidak ada segmen yang diteruskan. Kita dapat memverifikasinya dengan memeriksa nomor urut segmen TCP dalam file jejak tersebut. Pada Grafik Urutan-Waktu (Stevens) dari jejak ini, semua sequence number dari sumber (192.168.108.134) ke tujuan (128.119.245.12) meningkat secara monoton seiring dengan waktu. Jika ada segmen yang dikirim ulang, nomor urut dari segmen yang dikirim ulang tersebut seharusnya lebih kecil daripada segmen di sekitarnya.

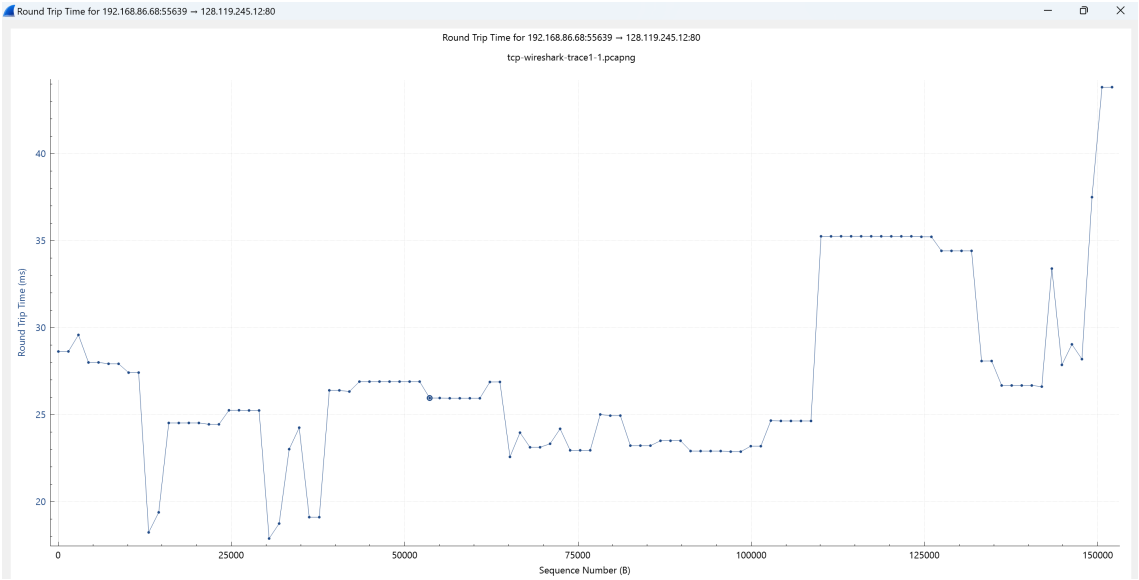
Aktivitas 2 - 9.4 Menganalisis File Jejak Wireshark dan Menghitung RTT (Round Trip Time)

Hasil Aktivitas 2:





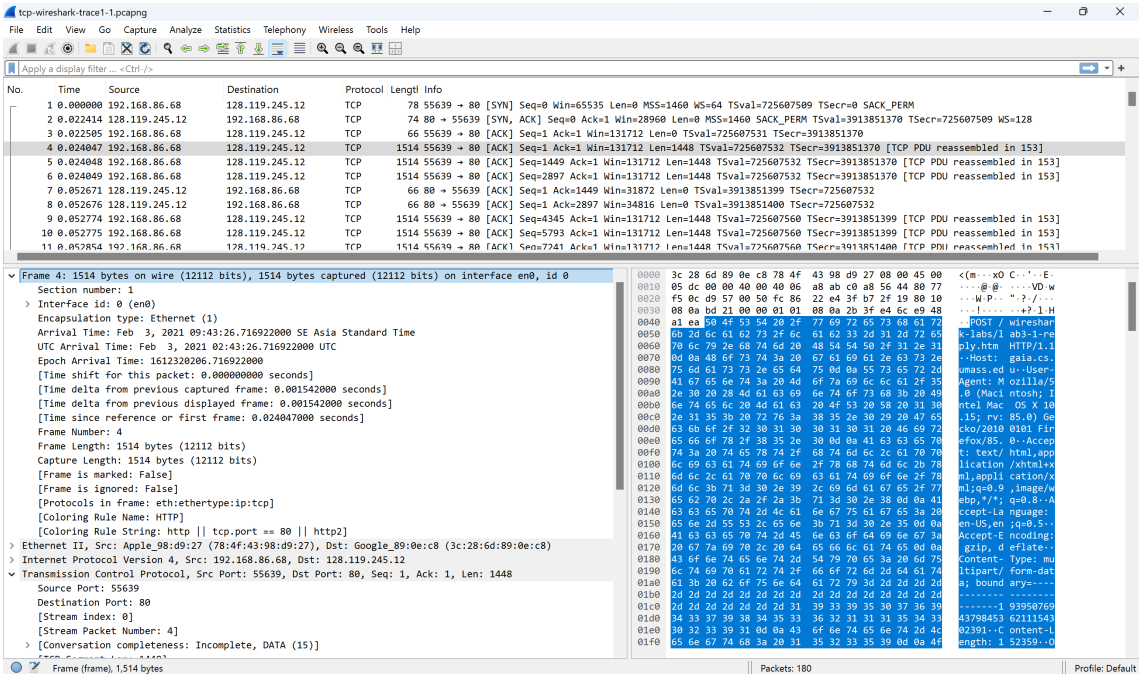
Grafik RTT terhadap waktu



Grafik RTT terhadap sequence number

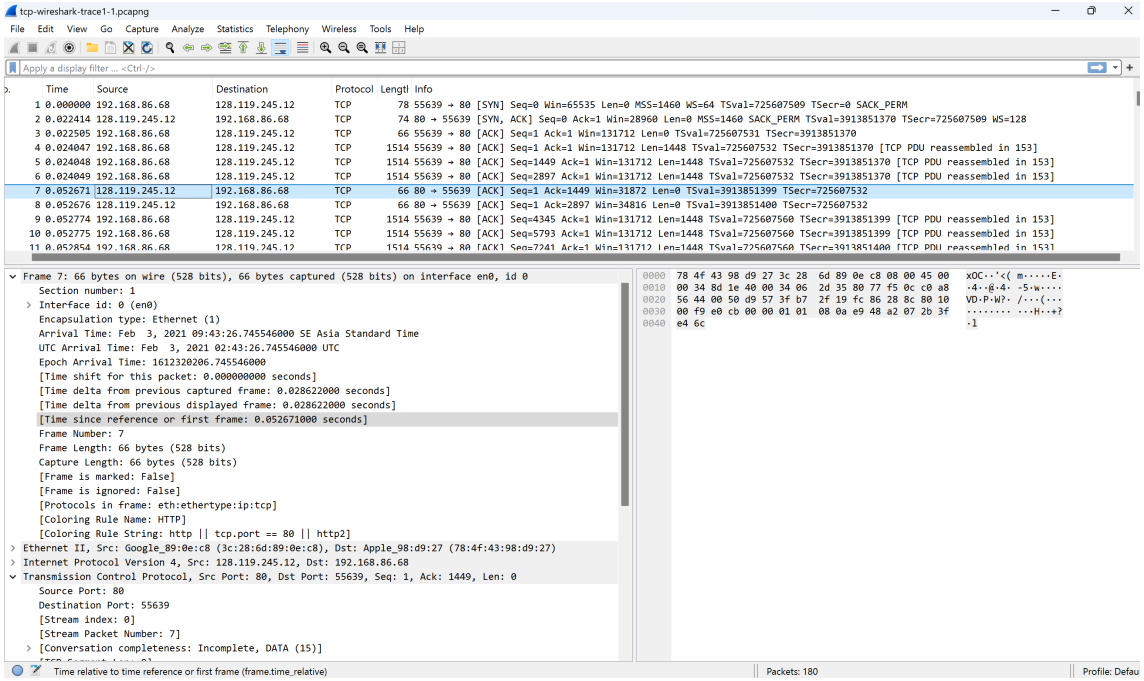
Pertanyaan-pertanyaan:

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



Pada pukul 09:43:26.716922000 SE Asia Standard Time (02:43:26.716922000 UTC) atau pada waktu 0.024047000 detik setelah paket pertama diterima, nilai ini terlihat dari Time since reference or first frame.

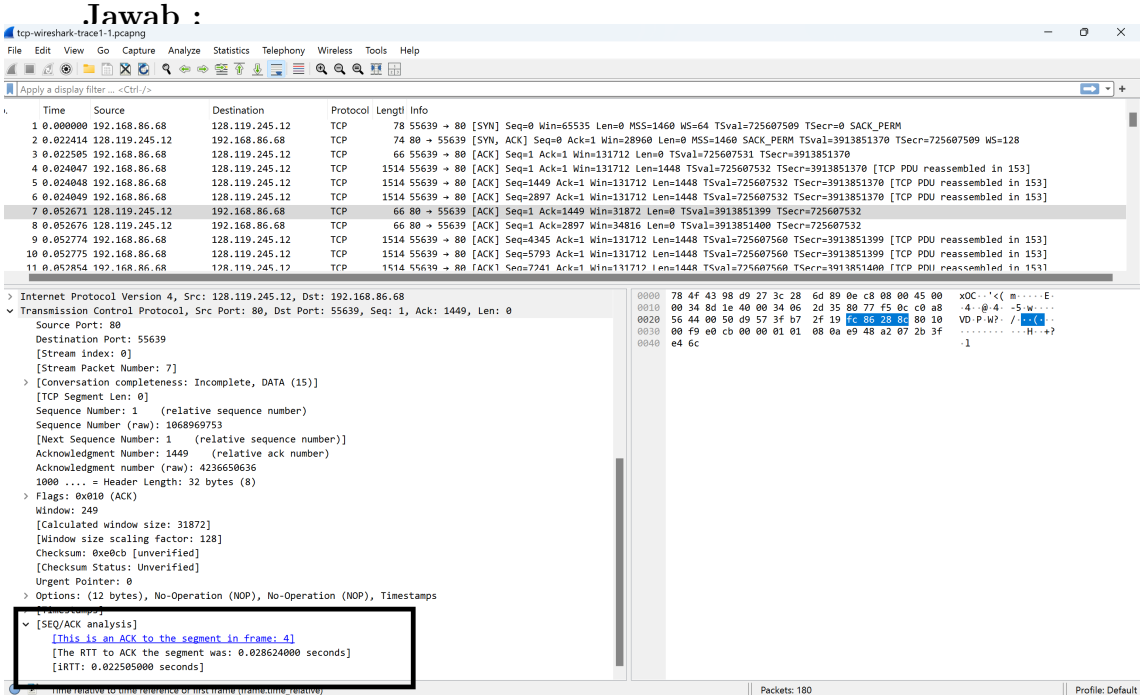
2. Pada pukul berapa ACK untuk segmen pertama yang berisi data ini diterima?
   Jawab :



Pada pukul 09:43:26.745546000 SE Asia Standard Time (02:43:26.745546000 UTC) atau pada waktu 0.052671000 detik setelah paket pertama diterima, nilai ini terlihat dari Time since reference or first frame.

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

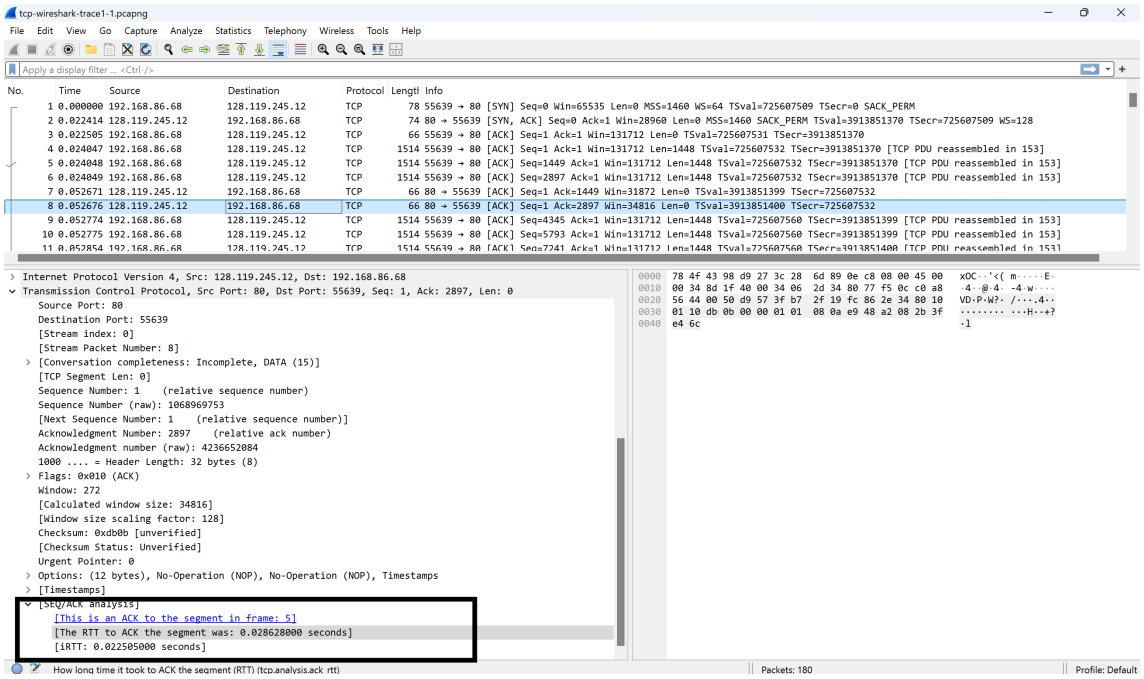
Jawab :



Nilai RTT pada segment yang berisi data pertama dapat terlihat pada field SEQ/ACK analysis yang menunjukan bahwa RTT pada segment ini sebesar 0.028624000 detik

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

Jawab :



RTT value dari TCP segment yang berisi data kedua sebesar 0.028628000 detik.

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

   Jawab :

   Formula untuk menentukan EstimatedRTT:

$$\text{EstimatedRTT} = (1 - \alpha) \times \text{EstimatedRTT} + \alpha \times \text{SampleRTT}$$

   Dengan nilai $\alpha = 0.125$, kita dapatkan:

$$\text{EstimatedRTT} = (1 - 0.125) \times \text{EstimatedRTT} + 0.125 \times \text{SampleRTT}$$

   Menggunakan nilai RTT segment sebelumnya dan segment data sekarang kita dapatkan:

$$\text{EstimatedRTT} = 0.875 \times 0.028624000 + 0.125 \times 0.028628000$$

$$\text{EstimatedRTT} = 0.286245000$$

   Jadi EstimatedRTT (RTT yang diperkirakan) adalah 0.286245000 detik.