Tugas Pertemuan 7
Praktikum Sistem Komputer dan Jaringan

Kosmas Rio Legowo

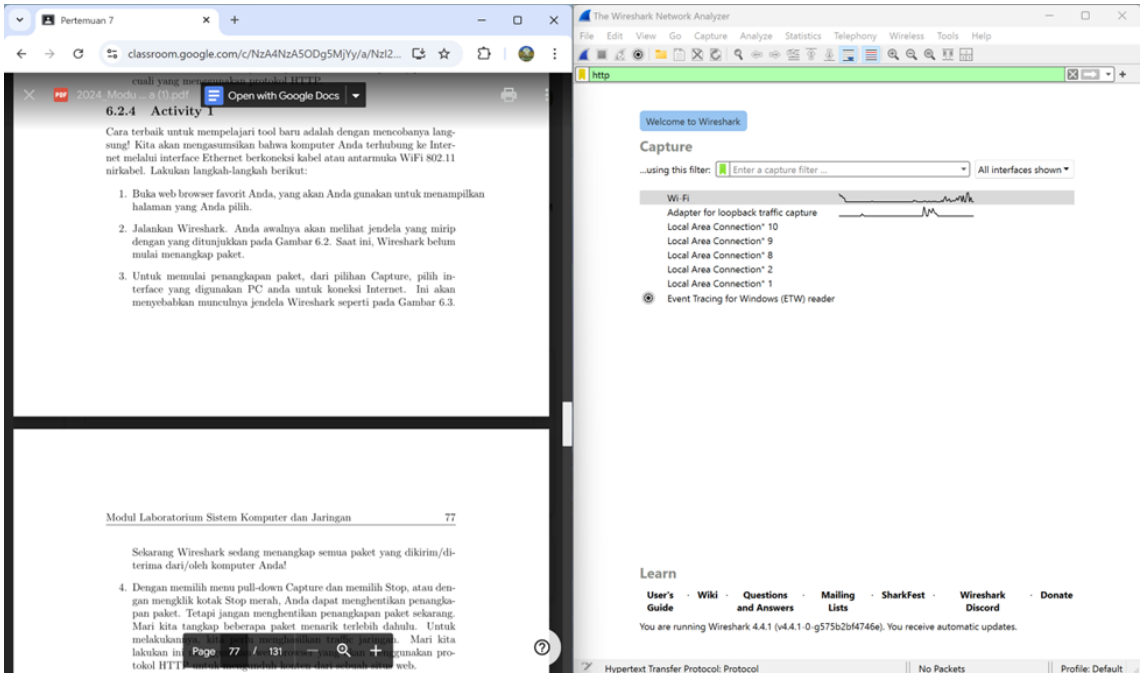
23/512012/PA/21863

Departemen Ilmu Komputer dan Elektronika
Universitas Gadjah Mada
kosmasriolegowo@mail.ugm.ac.id

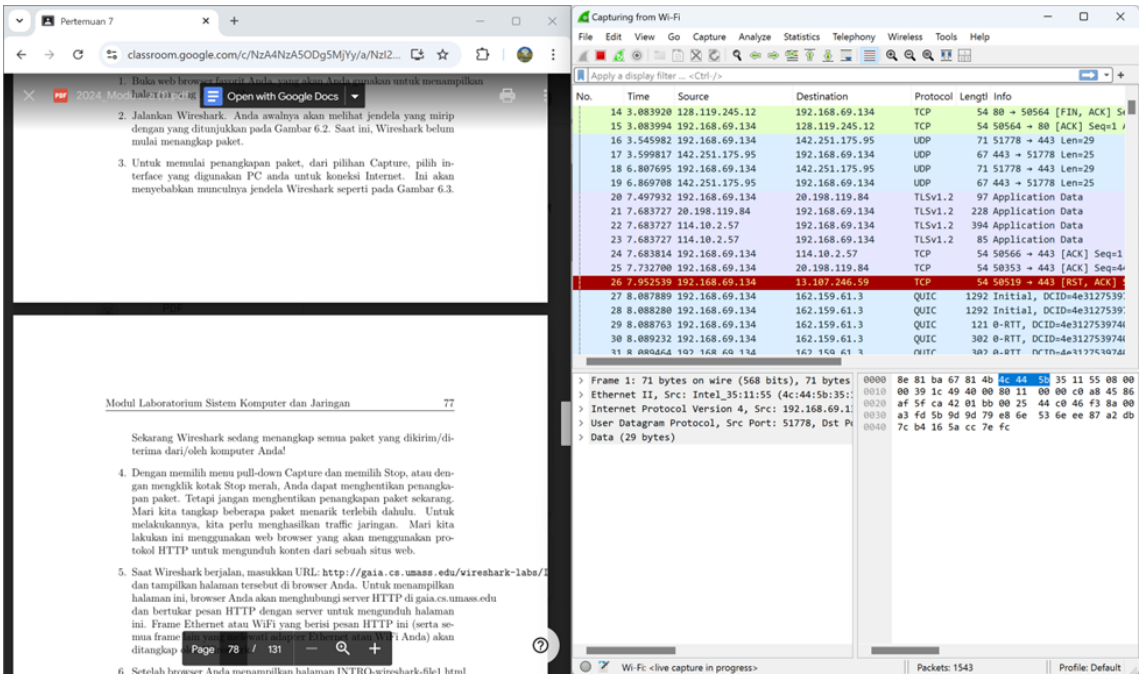
Chapter 6 Wireshark

Aktivitas 1

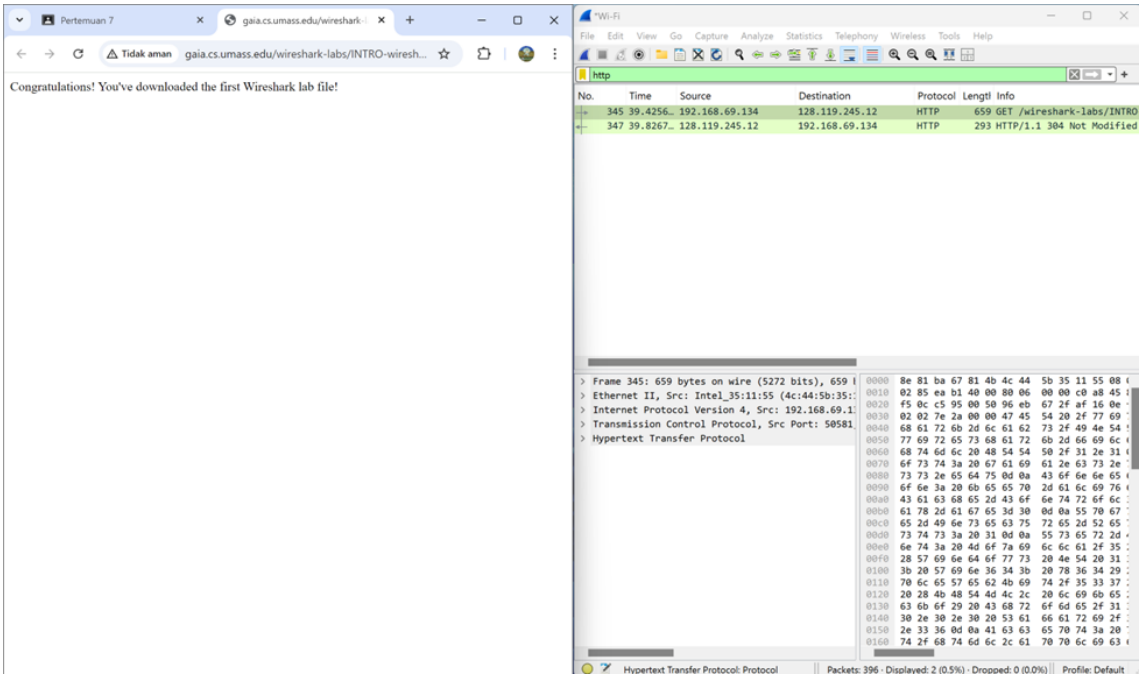
Nomor 1-2



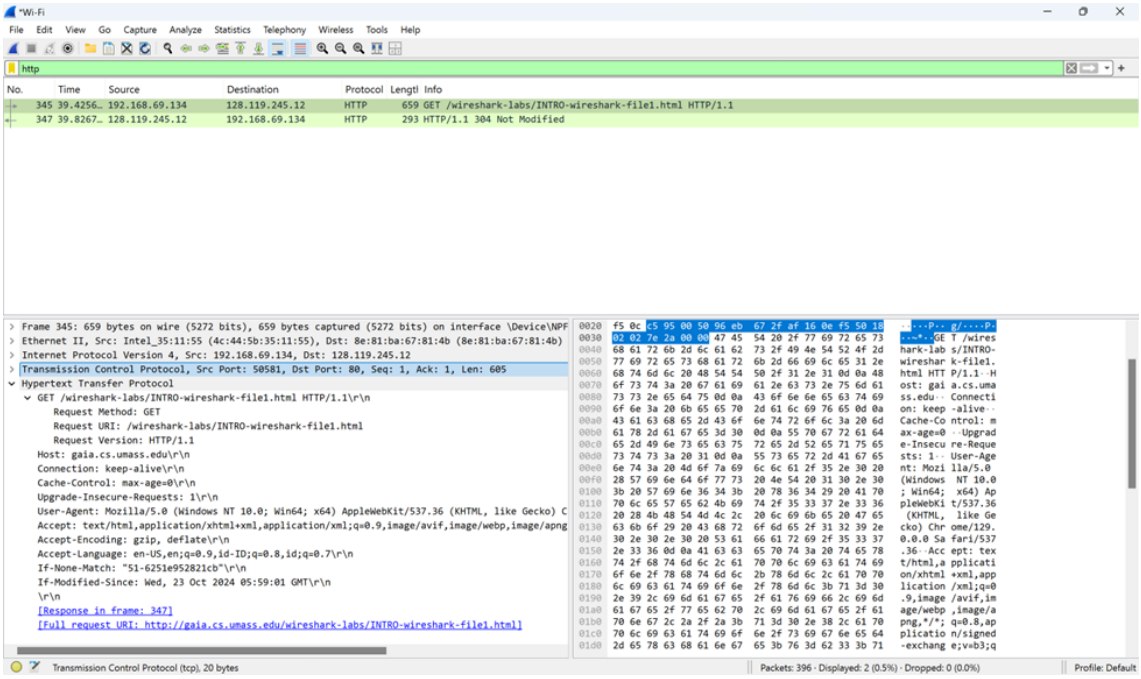
Nomor 3-4



Nomor 5-7

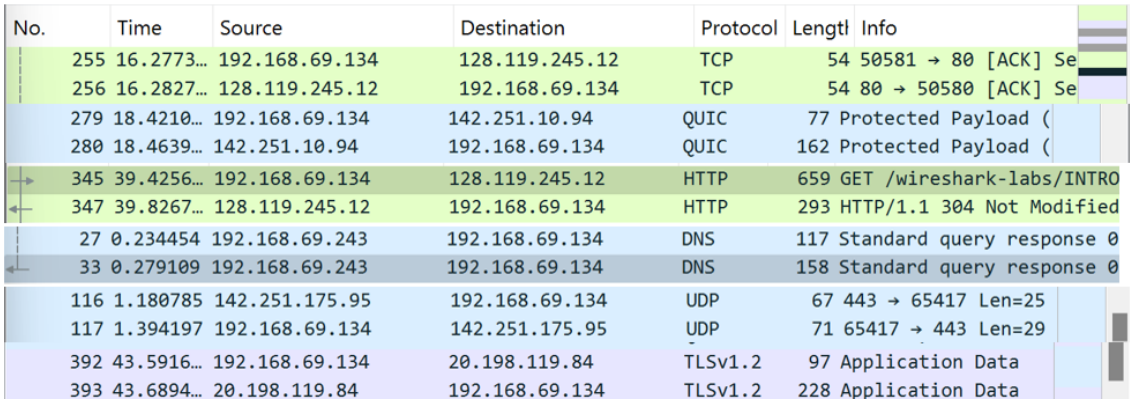


Nomor 8

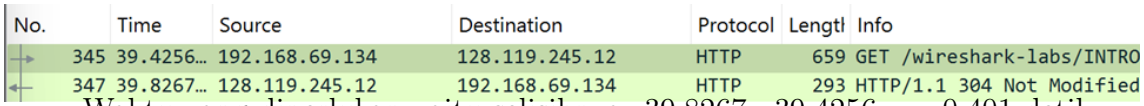


Pertanyaan-pertanyaan:

1. Protokol mana dari protokol-protokol berikut yang terlihat muncul (yaitu, tercantum dalam kolom Protocol Wireshark) pada hasil packet sniffing Anda: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?
   Jawab : Semuanya muncul seperti ditunjukkan pada gambar di bawah ini.



2. Berapa lama waktu yang diperlukan dari saat pesan HTTP GET dikirim hingga balasan HTTP OK diterima? (Secara default, nilai kolom Time pada Packet Listing adalah jumlah waktu, dalam detik, sejak penangkapan paket oleh Wireshark dimulai. Jika Anda ingin menampilkan waktu dalam format time-of-day, pilih menu pull-down View, lalu pilih Time, lalu pilih Time-of-day).
   Jawab :
   Dalam detik:



Waktu yang diperlukan yaitu selisihnya: 39.8267..-39.4256.. = 0.401 detik.

Dalam time-of-day:

No.	Time	Source	Destination	Protocol	Lengtl	Info
345	14:38:07.155098	192.168.69.134	128.119.245.12	HTTP	659	GET /wireshark-labs
347	14:38:07.556151	128.119.245.12	192.168.69.134	HTTP	293	HTTP/1.1 304 Not Mc

Waktu yang diperlukan yaitu selisihnya: .556151-.155098 = 0.401 detik.

3. Apa alamat Internet (IP address) dari gaia.cs.umass.edu? Apa alamat Internet komputer Anda yang mengirim pesan HTTP GET?
   Jawab : Alamat IP dari gaia.cs.umass.edu dapat dilihat pada kolom Destination yaitu 128.119.245.12. Alamat IP komputer yang mengirim pesan HTTP GET dapat dilihat pada kolom Source yaitu 192.168.69.134.
   Juga ditunjukkan pada gambar di bawah ini:

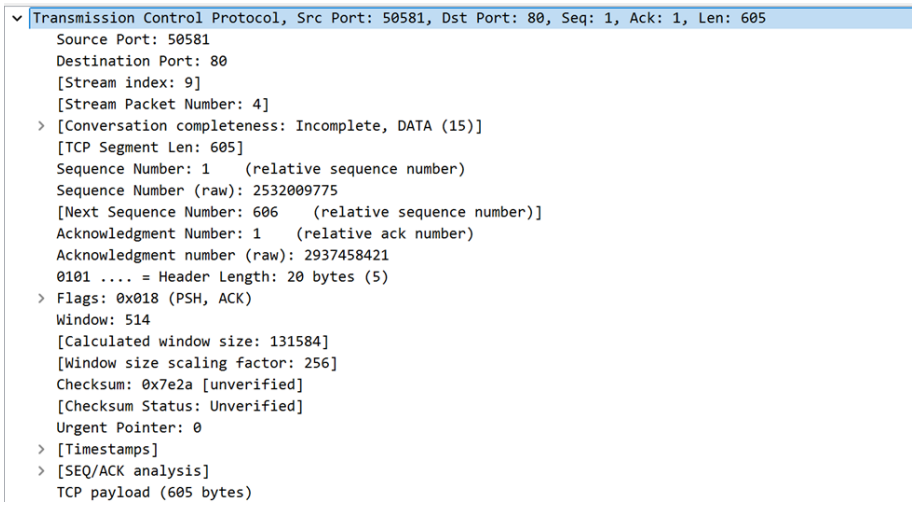
```
> Frame 345: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits) on interface \Device\NPF
> Ethernet II, Src: Intel_35:11:55 (4c:44:5b:35:11:55), Dst: 8e:81:ba:67:81:4b (8e:81:ba:67:81:4b)
v Internet Protocol Version 4, Src: 192.168.69.134, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 645
    Identification: 0xeab1 (60081)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.69.134
    Destination Address: 128.119.245.12
    [Stream index: 5]
> Transmission Control Protocol, Src Port: 50581, Dst Port: 80, Seq: 1, Ack: 1, Len: 605
> Hypertext Transfer Protocol
```

4. Perluas informasi pada pesan HTTP di bagian Packet-header Details (lihat Gambar 6.3 di atas) sehingga Anda dapat melihat field-field apa saja yang terkandung dalam pesan permintaan HTTP GET. Apa jenis web browser yang mengeluarkan permintaan HTTP tersebut? Jawabannya tertera di ujung kanan informasi setelah field ”User-Agent:” dalam tampilan pesan HTTP yang diperluas.
   Jawab : Browser Google Chrome versi 129.0.0.0.

```
v Hypertext Transfer Protocol
  v GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/INTRO-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36\r\n
    Accept: 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\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,id-ID;q=0.8,id;q=0.7\r\n
    If-None-Match: "51-6251e952821cb"\r\n
    If-Modified-Since: Wed, 23 Oct 2024 05:59:01 GMT\r\n
    \r\n
    [Response in frame: 347]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

5. Masih di bagian Packet-header Details, perluas informasi pada Transmission Control Protocol untuk paket ini sehingga Anda dapat melihat field-field dalam segmen TCP yang membawa pesan HTTP ini. Berapa nomor port tujuan

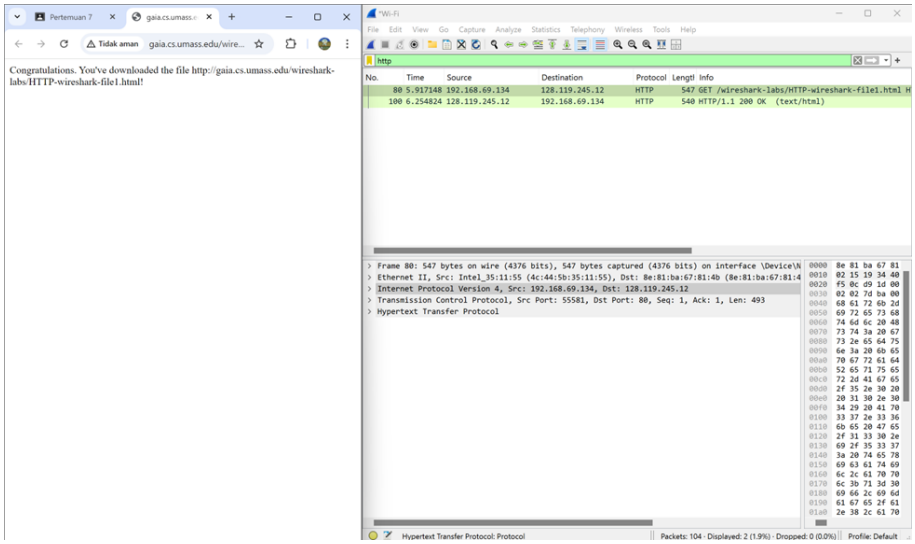
(angka setelah "Dest Port:") untuk segmen TCP yang berisi permintaan HTTP yang dikirimkan?
Jawab : Nomor port tujuan yaitu 80.



Chapter 7 HTTP

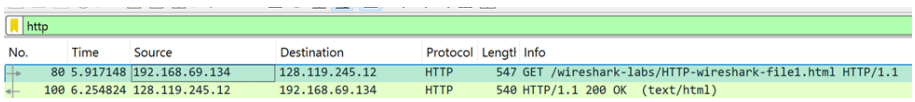
Aktivitas 1: Interaksi HTTP GET/response pada HTTP

Hasil aktivitas 1 nomor 1-4:



Pertanyaan-pertanyaan:

1. Apakah web browser Anda menggunakan HTTP versi 1.0, 1.1, atau 2?Versi HTTP apa yang digunakan oleh server?
   Jawab : Browser saya menggunakan HTTP versi 1.1. Server juga menggunakan HTTP versi 1.1. Hal ini terlihat pada tangkapan layar di bawah ini:

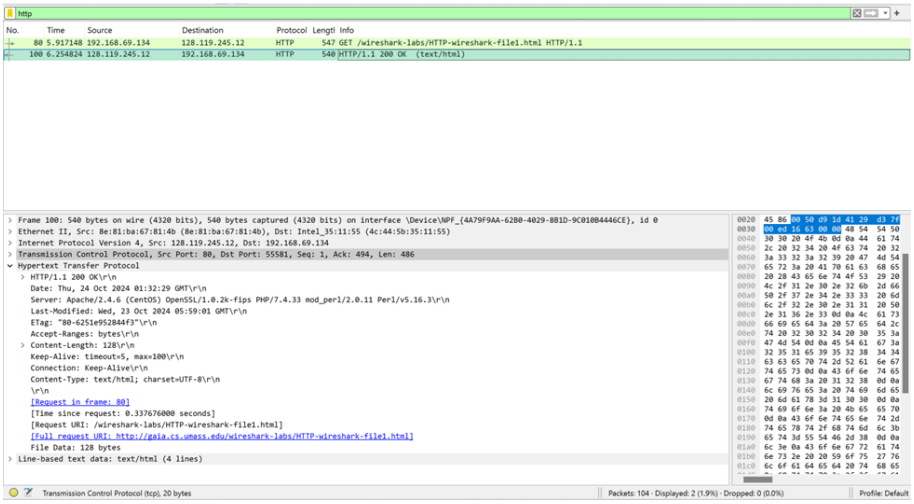


2. Bahasa apa (jika ada) yang dapat diterima oleh web browser Anda?
   Jawab : Browser saya dapat menerima bahasa "en-US,en" (Inggris) dan "id-ID" (Indonesia) seperti yang terlihat pada bagian "Accept-Langauge" berikut:

3. Apa kode status yang dikembalikan oleh server ke web browser Anda?
   Jawab : Kode status yang dikembalikan oleh server adalah 200 OK, menunjukkan bahwa permintaan berhasil.

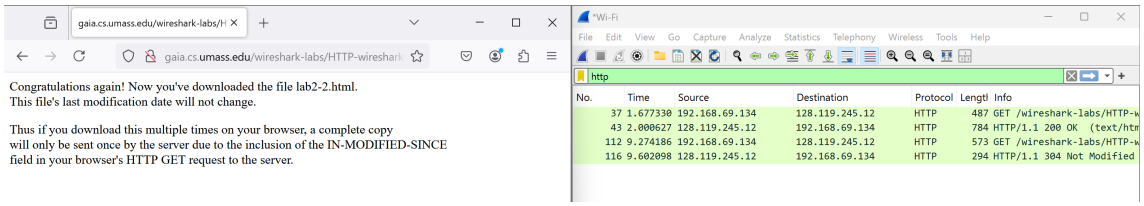
```
540 HTTP/1.1 200 OK  (text/html)
```

4. Apa kode status yang dikembalikan oleh server ke web browser Anda?
   Jawab : File tersebut terakhir dimodifikasi pada Rabu, 23 Oktober 2024 pukul 05:59:01 GMT.



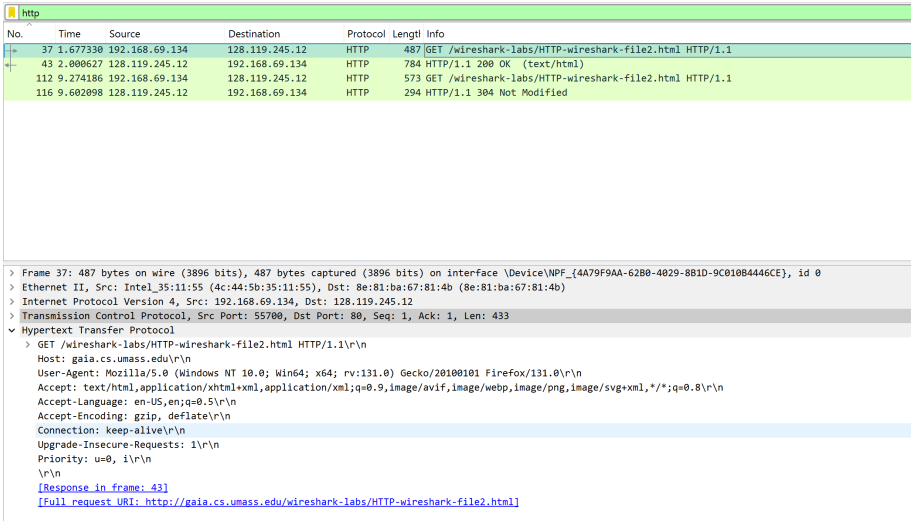
Aktivitas 2: Interaksi CONDITIONAL GET/response pada HTTP

Hasil aktivitas 2 nomor 1-5:

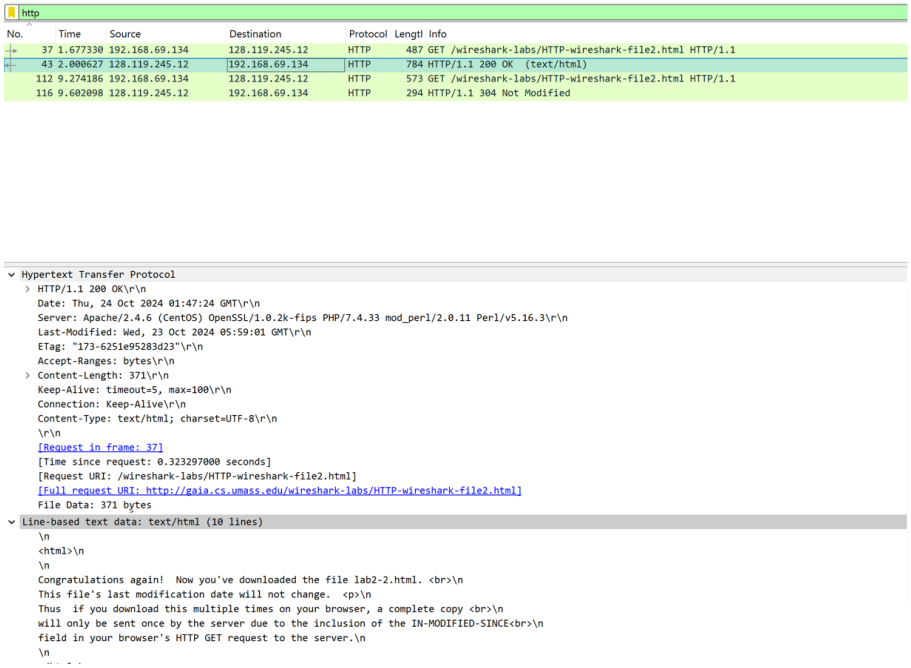


Pertanyaan-pertanyaan:

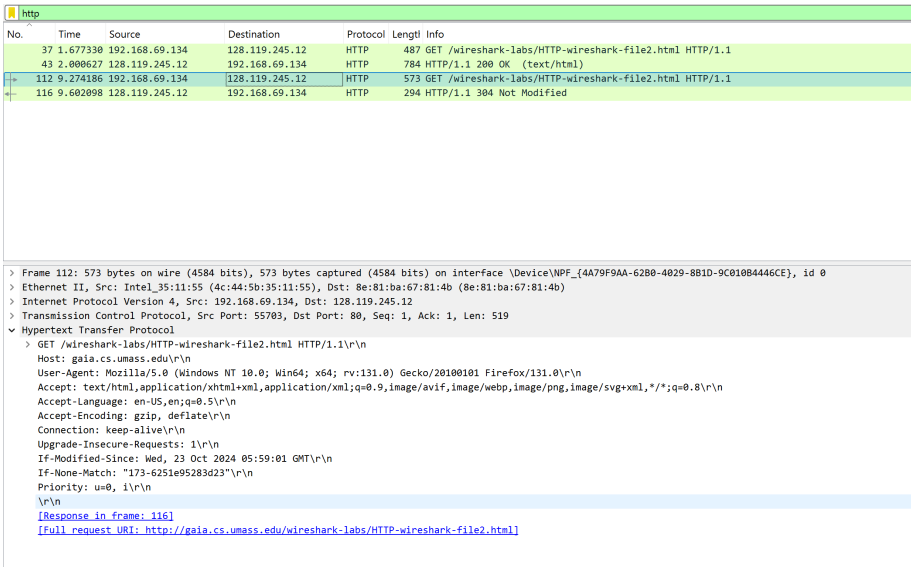
1. Periksa isi permintaan HTTP GET pertama yang dikirim browser Anda ke server. Apakah Anda melihat baris "IF-MODIFIED-SINCE" dalam HTTP GET tersebut?
   Jawab : Tidak ada baris tersebut.



2. Periksa isi respons dari server. Apakah server secara eksplisit me-return file HTML yang diminta? Bagaimana Anda dapat mengetahuinya?
   Jawab : Responsnya adalah 200 OK, yang berarti server berhasil mengirimkan file HTML yang diminta pada saat itu. Status 200 OK dan tipe konten "text/html" mengonfirmasi bahwa file tersebut telah dikirimkan oleh server.

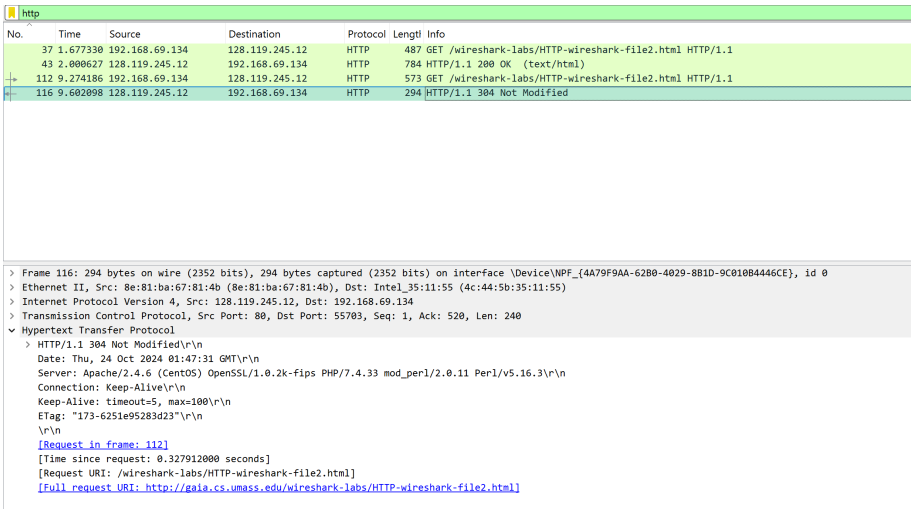


3. Sekarang periksa isi permintaan HTTP GET kedua dari browser Anda ke server. Apakah Anda melihat baris ”IF-MODIFIED-SINCE:” dalam HTTP GET tersebut? Jika ya, apa informasi yang mengikuti header ”IF-MODIFIED-SINCE:”?
   Jawab : Ya, baris "IF-MODIFIED-SINCE" ada dalam permintaan HTTP GET kedua. Informasi yang mengikuti header ini adalah: Wed, 23 Oct 2024 05:59:01 GMT. Hal ini berarti file tersebut terakhir dimodifikasi pada Rabu, 23 Oktober 2024 pukul 05:59:01 GMT.



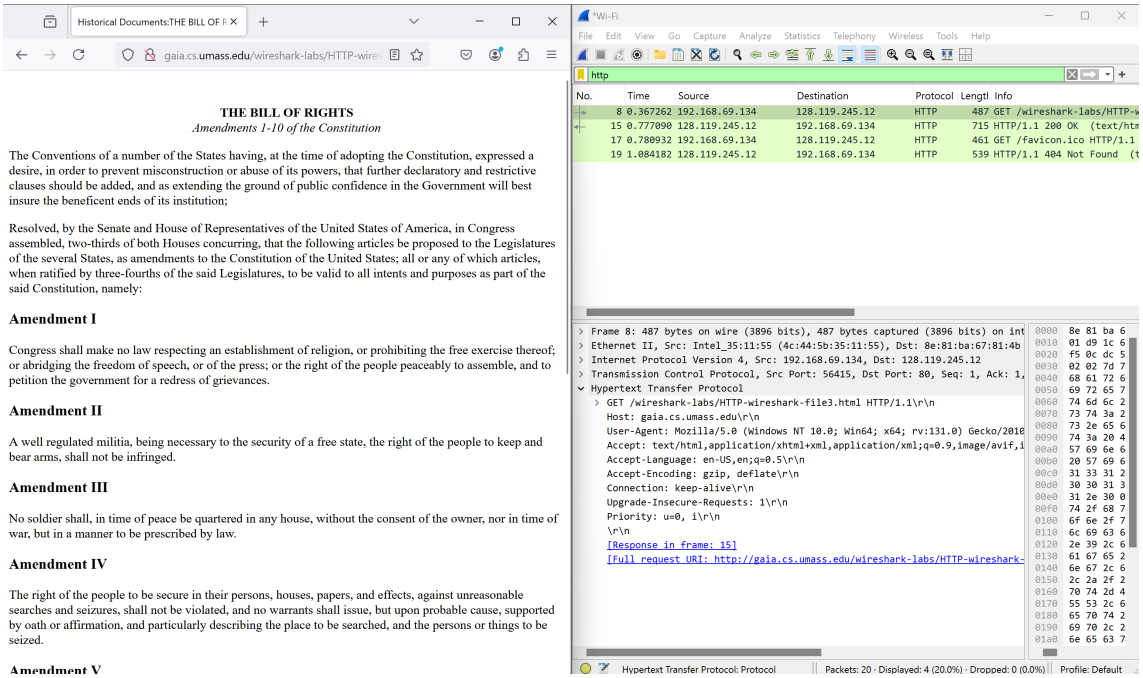
4. Apa kode status HTTP dan frasa yang dikembalikan oleh server sebagai respons terhadap HTTP GET kedua ini? Apakah server secara eksplisit mereturn file HTML yang diminta? Jelaskan

   Jawab : Server mengembalikan kode status 304 dengan frasa "Not Modified". Kode status 304 Not Modified menunjukkan bahwa file HTML yang diminta oleh klien belum berubah sejak versi terakhir yang dimiliki oleh klien (sesuai dengan waktu yang ditunjukkan dalam header "If-Modified-Since"). Karena file tersebut belum diubah, server tidak perlu mengirim ulang file HTML. Ini membuat transfer data lebih efisien karena tidak perlu mengirim ulang konten yang sudah dimiliki klien.



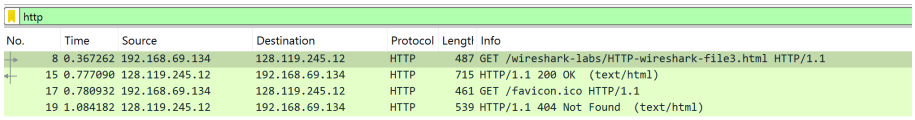
Aktivitas 3: Mengunduh File Berukuran Besar

Hasil aktivitas 3 nomor 1-4:

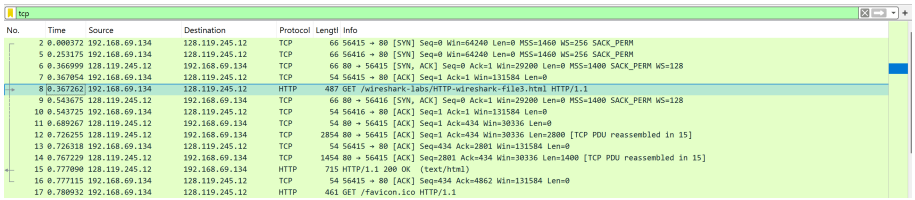


Pertanyaan-pertanyaan:

1. Berapa banyak pesan HTTP GET yang dikirimkan oleh browser Anda? Berapa nomor paket yang berisi pesan HTTP GET tersebut??
   Jawab : Hanya 1 pesan HTTP get. Nomor paket yang beirisi pesan HTTP Get adalah 8.

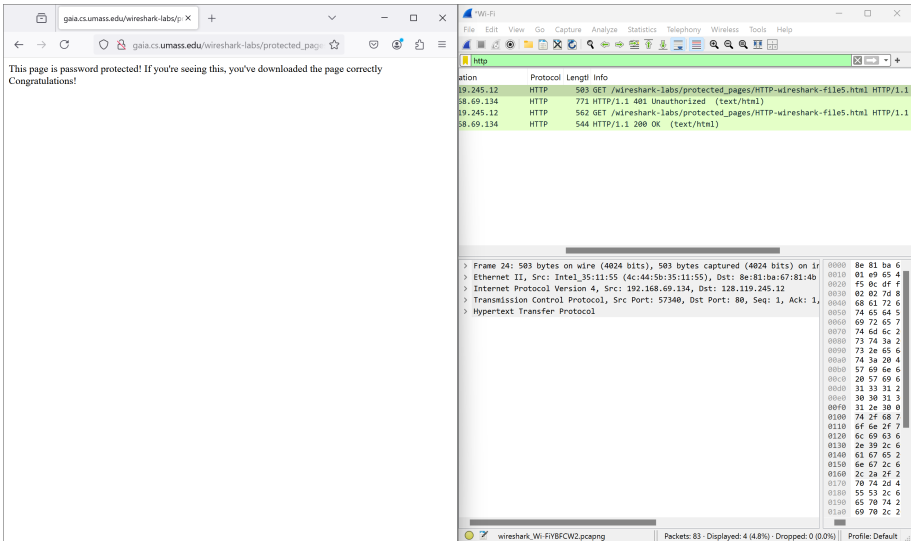


2. Berapa banyak segmen TCP berisi pecahan data yang diperlukan untuk mengirim file HTML yang panjang tersebut?
   Jawab : Untuk mengirim file HTML tersebut, diperlukan 2 segmen TCP yang terlihat dari paket 13 berukuran 2854 bytes dan paket 15 berukuran 1454 bytes.



Aktivitas 4: Autentikasi HTTP

Hasil aktivitas 4 nomor 1-4:



Pertanyaan-pertanyaan:

1. Apa respons dari server (kode status dan frasa) terhadap pesan HTTP GET pertama dari browser Anda?
   Jawab : Paket 6 berisi GET pertama dan paket 9 berisi respons dari server yaitu 401 Unauthorized. Respons ini menunjukkan bahwa server meminta informasi login dari klien (browser saya), karena halaman tersebut dilindungi.

```
24 1.790693 192.168.69.134      128.119.245.12      HTTP      503 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
30 2.092997 128.119.245.12      192.168.69.134      HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
```

2. Ketika browser Anda mengirimkan pesan HTTP GET untuk kedua kalinya, field baru apa yang disertakan dalam pesan HTTP GET tersebut?
   Jawab : Browser akan menyertakan field baru bernama Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=. Field ini mengandung informasi basic authentication yang merupakan hasil dari memasukkan username dan password pada kotak dialog authentication di browser. Informasi ini dikodekan dalam Base64.