

Tugas Pertemuan 7

Praktikum Sistem Komputer dan Jaringan

Kosmas Rio Legowo

23/512012/PA/21863

Departemen Ilmu Komputer dan Elektronika

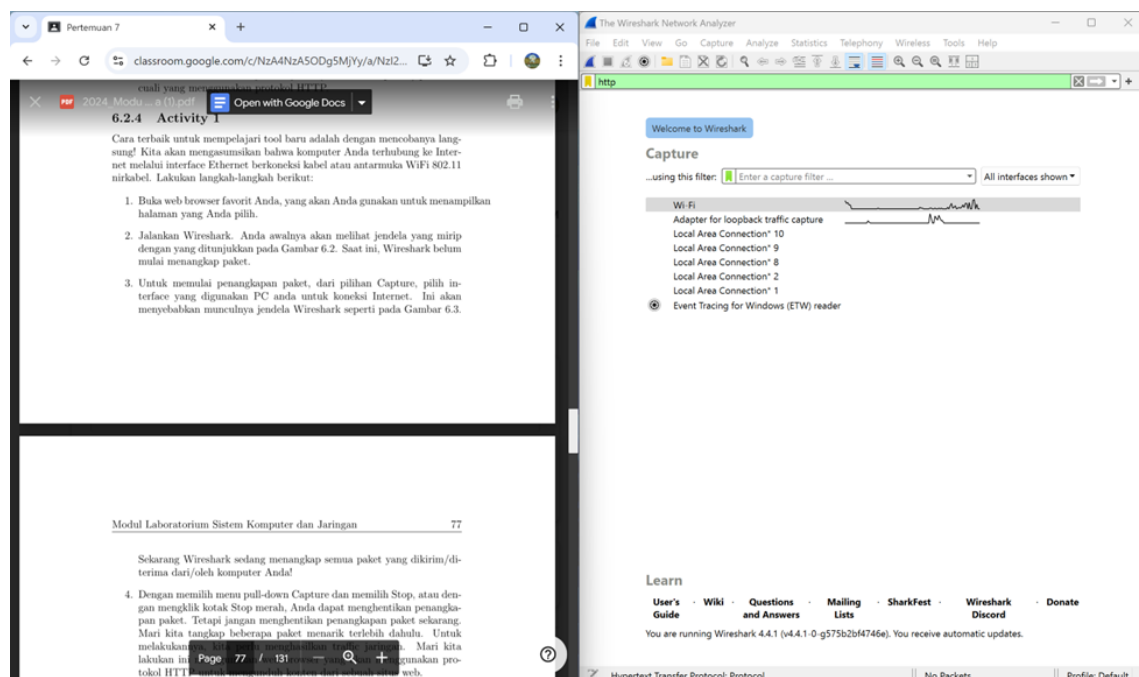
Universitas Gadjah Mada

kosmasriolegowo@mail.ugm.ac.id

Chapter 6 Wireshark

Aktivitas 1

Nomor 1-2



Nomor 3-4

1. Buka web browser favorit Anda sesuai yang Anda sukai untuk menampilkan halaman ini.

2. Jalankan Wireshark. Anda awalnya akan melihat jendela yang mirip dengan yang ditunjukkan pada Gambar 6.2. Saat ini, Wireshark belum mulai menangkap paket.

3. Untuk memulai penangkapan paket, dari pilihan Capture, pilih interface yang digunakan PC anda untuk koneksi Internet. Ini akan menyebabkan munculnya jendela Wireshark seperti pada Gambar 6.3.

Modul Laboratorium Sistem Komputer dan Jaringan 77

Sekarang Wireshark sedang menangkap semua paket yang dikirim/diterima dari/oleh komputer Anda!

4. Dengan memilih menu pull-down Capture dan memilih Stop, atau dengan mengklik kotak Stop merah, Anda dapat menghentikan penangkapan paket. Tetapi jangan menghentikan penangkapan paket sekarang. Mari kita tangkap beberapa paket menarik terlebih dahulu. Untuk melakukannya, kita perlu menghasilkan traffic jaringan. Mari kita lakukan ini menggunakan web browser yang akan menggunakan protokol HTTP untuk mengunduh konten dari sebuah situs web.

5. Saat Wireshark berjalan, masukkan URL: <http://gaia.cs.umass.edu/wireshark-labs/> dan tampilkan halaman tersebut di browser Anda. Untuk menampilkan halaman ini, browser Anda akan menghubungi server HTTP di gaia.cs.umass.edu dan bertukar pesan HTTP dengan server untuk mengunduh halaman ini. Frame Ethernet atau WiFi yang berisi pesan HTTP ini (serta semua frame yang terkait) akan ditampilkan di jendela Wireshark Anda.

6. Setelah browser Anda menampilkan halaman INTRO-wireshark-labs.html

Capturing from Wi-Fi

No.	Time	Source	Destination	Protocol	Length	Info
14	3.083920	128.119.245.12	192.168.69.134	TCP	54	80 → 50564 [FIN, ACK] Seq=1
15	3.083994	192.168.69.134	128.119.245.12	TCP	54	50564 → 80 [ACK] Seq=1
16	3.545982	192.168.69.134	142.251.175.95	UDP	71	51778 → 443 Len=29
17	3.599817	142.251.175.95	192.168.69.134	UDP	67	443 → 51778 Len=25
18	6.807695	192.168.69.134	142.251.175.95	UDP	71	51778 → 443 Len=29
19	6.869788	142.251.175.95	192.168.69.134	UDP	67	443 → 51778 Len=25
20	7.497932	192.168.69.134	20.198.119.84	TLSv1.2	97	Application Data
21	7.683727	20.198.119.84	192.168.69.134	TLSv1.2	228	Application Data
22	7.683727	114.10.2.57	192.168.69.134	TLSv1.2	394	Application Data
23	7.683727	114.10.2.57	192.168.69.134	TLSv1.2	85	Application Data
24	7.683814	192.168.69.134	114.10.2.57	TCP	54	50566 → 443 [ACK] Seq=1
25	7.732700	192.168.69.134	20.198.119.84	TCP	54	50553 → 443 [ACK] Seq=1
26	7.952539	192.168.69.134	11.107.246.59	TCP	54	50519 → 443 [RST, ACK] Seq=1
27	8.087889	192.168.69.134	162.159.61.3	QUIC	1292	Initial, DCID=4e31275397
28	8.088280	192.168.69.134	162.159.61.3	QUIC	1292	Initial, DCID=4e31275397
29	8.088763	192.168.69.134	162.159.61.3	QUIC	121	0-RTT, DCID=4e3127539744
30	8.089232	192.168.69.134	162.159.61.3	QUIC	302	0-RTT, DCID=4e3127539744
31	8.089648	192.168.69.134	162.159.61.3	QUIC	107	0-RTT, DCID=4e3127539744

Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
Ethernet II, Src: Intel_35:11:55 (4c:44:5b:35:11:55), Dst: 192.168.69.12
Internet Protocol Version 4, Src: 192.168.69.12, Dst: 142.251.175.95
User Datagram Protocol, Src Port: 51778, Dst Port: 443
Data (29 bytes)

0000 8e 81 ba 67 81 4b 4c 44 5b 35 11 55 08 00 00 00
0010 00 39 1c 49 40 00 00 11 00 00 c0 a8 45 86
0020 af 5f ca 42 01 bb 00 25 44 c0 46 f3 8a 00
0030 a3 fd 5b 9d 79 e8 6e 53 6e ee 87 a2 db
0040 7c b4 16 5a cc 7e fc

Wi-Fi: live capture in progress | Packets: 1543 | Profile: Default

Nomor 5-7

Congratulations! You've downloaded the first Wireshark lab file!

Modul Laboratorium Sistem Komputer dan Jaringan 77

Sekarang Wireshark sedang menangkap semua paket yang dikirim/diterima dari/oleh komputer Anda!

4. Dengan memilih menu pull-down Capture dan memilih Stop, atau dengan mengklik kotak Stop merah, Anda dapat menghentikan penangkapan paket. Tetapi jangan menghentikan penangkapan paket sekarang. Mari kita tangkap beberapa paket menarik terlebih dahulu. Untuk melakukannya, kita perlu menghasilkan traffic jaringan. Mari kita lakukan ini menggunakan web browser yang akan menggunakan protokol HTTP untuk mengunduh konten dari sebuah situs web.

5. Saat Wireshark berjalan, masukkan URL: <http://gaia.cs.umass.edu/wireshark-labs/> dan tampilkan halaman tersebut di browser Anda. Untuk menampilkan halaman ini, browser Anda akan menghubungi server HTTP di gaia.cs.umass.edu dan bertukar pesan HTTP dengan server untuk mengunduh halaman ini. Frame Ethernet atau WiFi yang berisi pesan HTTP ini (serta semua frame yang terkait) akan ditampilkan di jendela Wireshark Anda.

6. Setelah browser Anda menampilkan halaman INTRO-wireshark-labs.html

Capturing from Wi-Fi

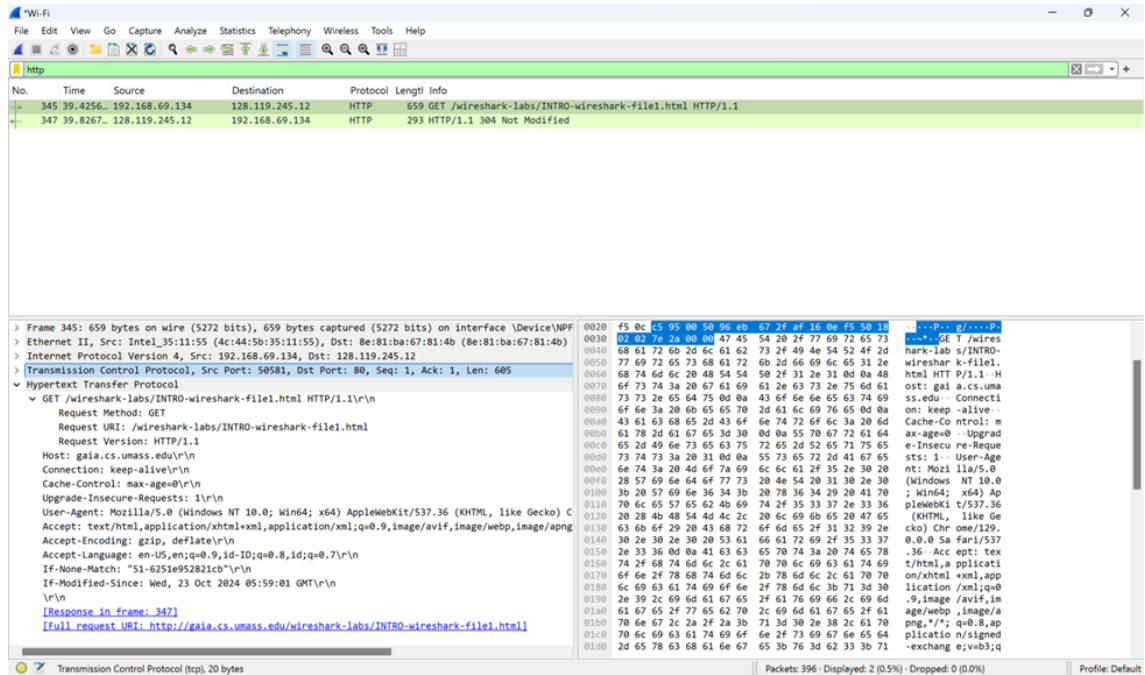
No.	Time	Source	Destination	Protocol	Length	Info
345	39.4256...	192.168.69.134	128.119.245.12	HTTP	659	GET /wireshark-labs/INTRO
347	39.8267...	128.119.245.12	192.168.69.134	HTTP	293	HTTP/1.1 304 Not Modified

Frame 345: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits) on interface 0
Ethernet II, Src: Intel_35:11:55 (4c:44:5b:35:11:55), Dst: 192.168.69.12
Internet Protocol Version 4, Src: 192.168.69.12, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50581, Dst Port: 80
Hypertext Transfer Protocol

0000 8e 81 ba 67 81 4b 4c 44 5b 35 11 55 08 00 00
0010 02 85 ea b1 40 00 80 06 00 00 c0 a8 45 86
0020 f5 0c c5 95 00 50 9e eb 67 2f af 16 0e 00
0030 02 02 7e 2a 00 00 47 45 54 20 2f 77 69 00
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 00
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 00
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 00
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 00
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 00
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 00
00a0 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 00
00b0 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 00
00c0 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 00
00d0 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 00
00e0 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 00
00f0 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 00
0100 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 00
0110 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 00
0120 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 00
0130 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 00
0140 30 2e 30 2e 30 20 53 61 66 61 72 69 2f 00
0150 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 00
0160 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 00

Hypertext Transfer Protocol: Protocol | Packets: 396 - Displayed: 2 (0.5%) - Dropped: 0 (0.0%) | Profile: Default

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.

No.	Time	Source	Destination	Protocol	Length	Info
255	16.2773...	192.168.69.134	128.119.245.12	TCP	54	50581 → 80 [ACK] Seq=...
256	16.2827...	128.119.245.12	192.168.69.134	TCP	54	80 → 50580 [ACK] Seq=...
279	18.4210...	192.168.69.134	142.251.10.94	QUIC	77	Protected Payload (0.0.0.0)
280	18.4639...	142.251.10.94	192.168.69.134	QUIC	162	Protected Payload (0.0.0.0)
345	39.4256...	192.168.69.134	128.119.245.12	HTTP	659	GET /wireshark-labs/INTRO-wireshark-file.html HTTP/1.1
347	39.8267...	128.119.245.12	192.168.69.134	HTTP	293	HTTP/1.1 304 Not Modified
27	0.234454	192.168.69.243	192.168.69.134	DNS	117	Standard query response 0
33	0.279109	192.168.69.243	192.168.69.134	DNS	158	Standard query response 0
116	1.180785	142.251.175.95	192.168.69.134	UDP	67	443 → 65417 Len=25
117	1.394197	192.168.69.134	142.251.175.95	UDP	71	65417 → 443 Len=29
392	43.5916...	192.168.69.134	20.198.119.84	TLSv1.2	97	Application Data
393	43.6894...	20.198.119.84	192.168.69.134	TLSv1.2	228	Application Data

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:

No.	Time	Source	Destination	Protocol	Length	Info
345	39.4256...	192.168.69.134	128.119.245.12	HTTP	659	GET /wireshark-labs/INTRO-wireshark-file.html HTTP/1.1
347	39.8267...	128.119.245.12	192.168.69.134	HTTP	293	HTTP/1.1 304 Not Modified

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

Dalam time-of-day:

No.	Time	Source	Destination	Protocol	Length	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 Modified

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)
✓ 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.

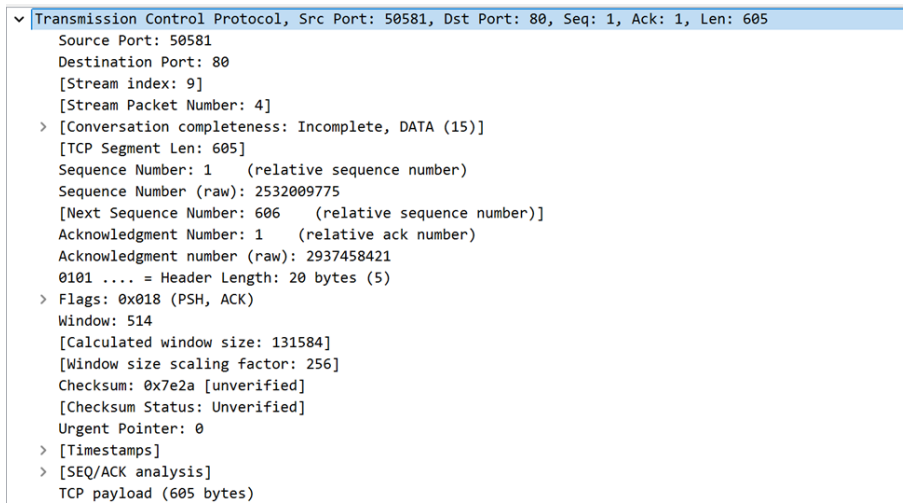
Jawab : Browser Google Chrome versi 129.0.0.0.

```
✓ Hypertext Transfer Protocol
  > 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?

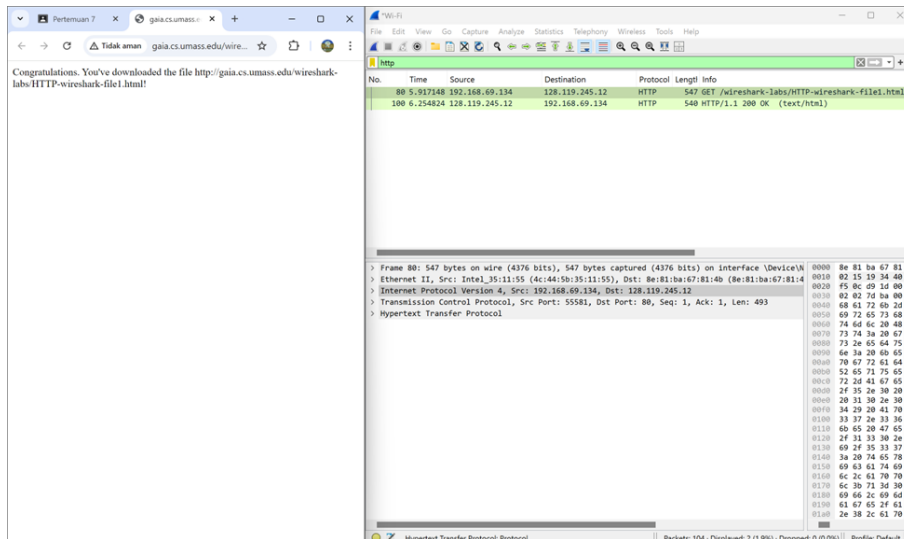
Jawab : Nomor port tujuan yaitu 80.



Chapter 7 HTTP

Aktivitas 1: Interaksi HTTP GET/response pada HTTP

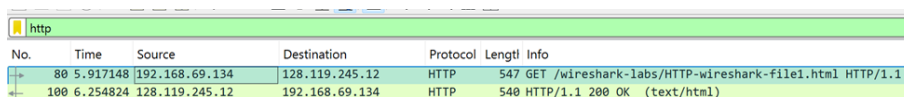
Hasil aktivitas 1 nomor 1-4:



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-Language" berikut:

```
✓ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\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/130.0.0.0 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
    \r\n
    [Response in frame: 100]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

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.

The image shows a Wireshark packet capture of an HTTP GET request and response. The packet list shows a single packet (No. 100) from 192.168.69.134 to 128.119.245.12, which is an HTTP GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details show the request headers, including the User-Agent, Accept, and Accept-Encoding. The packet bytes show the raw HTTP request and response data.

Aktivitas 2: Interaksi CONDITIONAL GET/response pada HTTP

Hasil aktivitas 2 nomor 1-5:

The screenshot shows a web browser window with the address bar displaying the URL <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2-2.html>. The page content shows a message: "Congratulations again! Now you've downloaded the file lab2-2.html. This file's last modification date will not change." Below this message, it says: "Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE field in your browser's HTTP GET request to the server."

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.

No.	Time	Source	Destination	Protocol	Length	Info
37	1.677330	192.168.69.134	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	2.800627	128.119.245.12	192.168.69.134	HTTP	784	HTTP/1.1 200 OK (text/html)
112	9.274186	192.168.69.134	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
116	9.602098	128.119.245.12	192.168.69.134	HTTP	294	HTTP/1.1 304 Not Modified


```

> Frame 37: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF_{4A79F9AA-62B0-4029-8B1D-9C01084446CE}, id 0
> 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)
> Internet Protocol Version 4, Src: 192.168.69.134, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55700, Dst Port: 80, Seq: 1, Ack: 1, Len: 433
> Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 43]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

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.

No.	Time	Source	Destination	Protocol	Length	Info
37	1.677330	192.168.69.134	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	2.800627	128.119.245.12	192.168.69.134	HTTP	784	HTTP/1.1 200 OK (text/html)
112	9.274186	192.168.69.134	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
116	9.602098	128.119.245.12	192.168.69.134	HTTP	294	HTTP/1.1 304 Not Modified


```

> Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 24 Oct 2024 01:47:24 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 23 Oct 2024 05:59:01 GMT\r\n
    ETag: "173-6251e9528d23"\r\n
    Accept-Ranges: bytes\r\n
    > Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 37]
    [Time since request: 0.323297000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
  > Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change. <p>\n
    Thus if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n

```

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.

No.	Time	Source	Destination	Protocol	Length	Info
37	1.677330	192.168.69.134	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	9.080627	128.119.245.12	192.168.69.134	HTTP	784	HTTP/1.1 200 OK (text/html)
112	9.274186	192.168.69.134	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
116	9.602098	128.119.245.12	192.168.69.134	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 112: 573 bytes on wire (4584 bits), 573 bytes captured (4584 bits) on interface \Device\NPF_{4A79F9AA-62B0-4029-8B1D-9C01084446CE}, id 0
> 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)
> Internet Protocol Version 4, Src: 192.168.69.134, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55703, Dst Port: 80, Seq: 1, Ack: 1, Len: 519
> Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Wed, 23 Oct 2024 05:59:01 GMT\r\n
If-None-Match: "173-6251e95283d23"\r\n
Priority: u=0, i\r\n
\r\n

[Response in frame: 116]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

4. Apa kode status HTTP dan frasa yang dikembalikan oleh server sebagai respons terhadap HTTP GET kedua ini? Apakah server secara eksplisit mengembalikan 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.

No.	Time	Source	Destination	Protocol	Length	Info
37	1.677330	192.168.69.134	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	9.080627	128.119.245.12	192.168.69.134	HTTP	784	HTTP/1.1 200 OK (text/html)
112	9.274186	192.168.69.134	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
116	9.602098	128.119.245.12	192.168.69.134	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 116: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{4A79F9AA-62B0-4029-8B1D-9C01084446CE}, id 0
> Ethernet II, Src: 8e:81:ba:67:81:4b (8e:81:ba:67:81:4b), Dst: Intel_35:11:55 (4c:44:5b:35:11:55)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.69.134
> Transmission Control Protocol, Src Port: 80, Dst Port: 55703, Seq: 1, Ack: 520, Len: 240
> Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n
Date: Thu, 24 Oct 2024 01:47:31 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "173-6251e95283d23"\r\n
\r\n

[Request in frame: 112]
[Time since request: 0.327912000 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

Aktivitas 3: Mengunduh File Berukuran Besar

Hasil aktivitas 3 nomor 1-4:

Historical Documents:THE BILL OF F X

gaia.cs.umass.edu/wireshark-labs/HTTP-wire...

THE BILL OF RIGHTS

Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment V

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
8	0.367262	192.168.69.134	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
15	0.777090	128.119.245.12	192.168.69.134	HTTP	715	HTTP/1.1 200 OK (text/html)
17	0.780932	192.168.69.134	128.119.245.12	HTTP	461	GET /favicon.ico HTTP/1.1
19	1.084182	128.119.245.12	192.168.69.134	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 8: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface 0

> Ethernet II, Src: Intel_35:11:55 (4c:44:5b:35:11:55), Dst: 8e:81:ba:67:81:4b

> Internet Protocol Version 4, Src: 192.168.69.134, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 56415, Dst Port: 80, Seq: 1, Ack: 1, Window: 0

> Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

Host: gaia.cs.umass.edu

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

Upgrade-Insecure-Requests: 1

Priority: u=0, i=0

Response in frame: 151

Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

Hypertext Transfer Protocol: Protocol | Packets: 20 | Displayed: 4 (20.0%) | Dropped: 0 (0.0%) | Profile: Default

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 berisi pesan HTTP Get adalah 8.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.367262	192.168.69.134	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
15	0.777090	128.119.245.12	192.168.69.134	HTTP	715	HTTP/1.1 200 OK (text/html)
17	0.780932	192.168.69.134	128.119.245.12	HTTP	461	GET /favicon.ico HTTP/1.1
19	1.084182	128.119.245.12	192.168.69.134	HTTP	539	HTTP/1.1 404 Not Found (text/html)

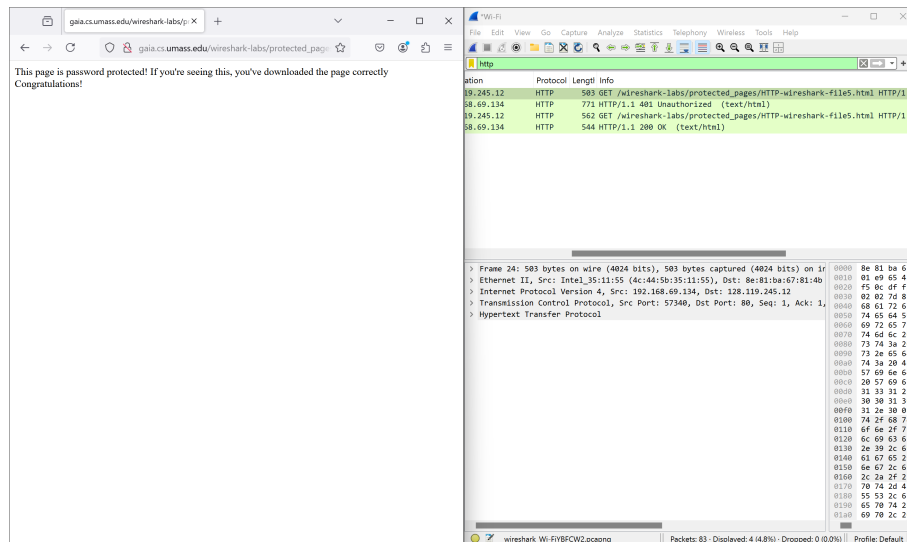
2. Berapa banyak segmen TCP berisi pecahan data yang diperlukan untuk mengirim file HTML yang panjang tersebut?

Jawab : Untuk mengirim file HTML tersebut, diperlukan 2 segmen TCP yang terlihat dari paket 13 berukuran 2854 bytes dan paket 15 berukuran 1454 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.088372	192.168.69.134	128.119.245.12	TCP	66	56415 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5	0.253175	192.168.69.134	128.119.245.12	TCP	66	56416 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6	0.369999	128.119.245.12	192.168.69.134	TCP	66	80 → 56415 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
7	0.367054	192.168.69.134	128.119.245.12	TCP	54	56415 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
8	0.367262	192.168.69.134	128.119.245.12	HTTP	487	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
9	0.543675	128.119.245.12	192.168.69.134	TCP	66	80 → 56416 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
10	0.543725	192.168.69.134	128.119.245.12	TCP	54	56416 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
11	0.690207	128.119.245.12	192.168.69.134	TCP	54	80 → 56415 [ACK] Seq=1 Ack=434 Win=30336 Len=0
12	0.726255	128.119.245.12	192.168.69.134	TCP	2854	80 → 56415 [ACK] Seq=1 Ack=434 Win=30336 Len=2800 [TCP PDU reassembled in 15]
13	0.726318	192.168.69.134	128.119.245.12	TCP	54	56415 → 80 [ACK] Seq=434 Ack=2801 Win=131584 Len=0
14	0.767219	128.119.245.12	192.168.69.134	TCP	1454	80 → 56415 [ACK] Seq=2801 Ack=434 Win=30336 Len=1400 [TCP PDU reassembled in 15]
15	0.777090	128.119.245.12	192.168.69.134	HTTP	715	HTTP/1.1 200 OK (text/html)
16	0.777115	192.168.69.134	128.119.245.12	TCP	54	56415 → 80 [ACK] Seq=434 Ack=4862 Win=131584 Len=0
17	0.780932	192.168.69.134	128.119.245.12	HTTP	461	GET /favicon.ico HTTP/1.1

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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm0=. 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.

