

Tugas Praktikum SKJ ke-7

Nama : Bagus Cipta Pratama

NIM : 23/516539/PA/22097

Kelas : KOMC

Pembahasan Bab 6 :

A. Aktivitas 1 :

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?

Berikut adalah protokol yang terlihat dan muncul Ketika saya urutkan :

4	1.021885	TpLinkTechno_90:20:...	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.2
5	2.046175	TpLinkTechno_90:20:...	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.2
6	3.273770	TpLinkTechno_90:20:...	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.2
8	4.301517	TpLinkTechno_90:20:...	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.2
10	5.117157	TpLinkTechno_90:20:...	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.2
13	6.345682	TpLinkTechno_90:20:...	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.2
20	7.370707	TpLinkTechno_90:20:...	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.2
21	8.394682	TpLinkTechno_90:20:...	Broadcast	ARP	42	Who has 192.168.1.71? Tell 192.168.1.2
22	8.395145	Intel_e0:53:49	Broadcast	ARP	60	Who has 169.254.169.254? Tell 192.168.1.57
311	18.073129	192.168.1.67	192.168.1.2	DNS	75	Standard query 0xf582 A play.google.com
312	18.073292	192.168.1.67	192.168.1.2	DNS	75	Standard query 0x55b6 HTTPS play.google.com
313	18.075423	192.168.1.2	192.168.1.67	DNS	171	Standard query response 0xf582 A play.google.com A 172.217.194.101 A 172.217.194.100 A 172.217.194.102
315	18.095765	192.168.1.2	192.168.1.67	DNS	382	Standard query response 0x7dd9 A code.jquery.com A 151.101.66.137 A 151.101.2.137 A 151.101.1.137
316	18.097014	192.168.1.2	192.168.1.67	DNS	318	Standard query response 0x7117 HTTPS code.jquery.com NS f.root-servers.net NS g.root-servers.net
318	18.098004	192.168.1.67	192.168.1.2	DNS	80	Standard query 0xe68a A fonts.googleapis.com
319	18.098110	192.168.1.67	192.168.1.2	DNS	80	Standard query 0xcff7 HTTPS fonts.googleapis.com
324	18.169039	192.168.1.2	192.168.1.67	DNS	339	Standard query response 0xe68a A fonts.googleapis.com A 74.125.200.95 NS j.root-servers.net
581	20.299852	192.168.1.67	128.119.245.12	HTTP	548	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
589	20.592835	128.119.245.12	192.168.1.67	HTTP	492	HTTP/1.1 200 OK (text/html)
591	20.742606	192.168.1.67	128.119.245.12	HTTP	494	GET /favicon.ico HTTP/1.1
601	21.083003	128.119.245.12	192.168.1.67	HTTP	538	HTTP/1.1 404 Not Found (text/html)
85	16.589320	fe80::1480:79fc:ad1::fb	fe80::fb	MDNS	219	Standard query 0x0000 PTR lb_dns-sd_udp.local, "QU" question PTR _companion-link_tcp.local
86	16.596191	192.168.1.145	224.0.0.251	MDNS	346	Standard query response 0x0000 PTR_rdlink_tcp.local TXT PTR, cache flush obedd.local PTR, c
87	16.600139	fe80::1480:79fc:ad1::fb	fe80::fb	MDNS	366	Standard query response 0x0000 PTR_rdlink_tcp.local TXT PTR, cache flush obedd.local PTR, c
148	16.791353	192.168.1.145	224.0.0.251	MDNS	140	Standard query 0x0000 ANY obedd_rdlink_tcp.local, "QM" question SRV 0 0 49152 obedd.local
149	16.793196	fe80::1480:79fc:ad1::fb	fe80::fb	MDNS	160	Standard query 0x0000 ANY obedd_rdlink_tcp.local, "QM" question SRV 0 0 49152 obedd.local
180	16.996156	192.168.1.145	224.0.0.251	MDNS	144	Standard query 0x0000 ANY obedd.local, "QU" question AAAA fe80::1480:79fc:ad1b:8783 A 192.168
181	16.998258	fe80::1480:79fc:ad1::fb	fe80::fb	MDNS	164	Standard query 0x0000 ANY obedd.local, "QU" question AAAA fe80::1480:79fc:ad1b:8783 A 192.168
219	17.202257	192.168.1.145	224.0.0.251	MDNS	140	Standard query 0x0000 ANY obedd_rdlink_tcp.local, "QM" question SRV 0 0 49152 obedd.local
628	23.027089	192.168.1.67	142.251.12.95	QUIC	74	Protected Payload (KP0), ULID=fc4dfe7df80d9dba
629	23.042475	142.251.12.95	192.168.1.67	QUIC	162	Protected Payload (KP0)
630	23.075285	192.168.1.67	142.251.12.95	QUIC	74	Protected Payload (KP0), DCID=fc4dfe7df80d9dba
3	0.007469	192.168.1.123	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
563	19.866894	192.168.1.130	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
16	6.413223	172.64.148.154	192.168.1.67	TCP	54	443 → 49715 [ACK] Seq=26 Ack=30 Win=8 Len=0
19	7.116767	192.168.1.67	20.198.162.78	TCP	54	49725 → 443 [ACK] Seq=44 Ack=175 Win=254 Len=0
26	9.680235	192.168.1.67	20.212.88.117	TCP	55	49934 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1
27	9.762448	20.212.88.117	192.168.1.67	TCP	66	443 → 49934 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2
42	14.604740	172.64.148.154	192.168.1.67	TCP	54	443 → 49751 [ACK] Seq=26 Ack=30 Win=12 Len=0
47	15.821899	192.168.1.67	48.218.104.163	TCP	54	49847 → 443 [ACK] Seq=51 Ack=40 Win=256 Len=0
50	16.141263	48.218.104.163	192.168.1.67	TCP	93	[TCP Spurious Retransmission] 443 → 49847 [PSH, ACK] Seq=1 Ack=51 Win=16382 Len=39
52	16.141369	192.168.1.67	48.218.104.163	TCP	66	[TCP Dup ACK 47#1] 49847 → 443 [ACK] Seq=51 Ack=40 Win=256 Len=0 SLE=1 SRE=40
491	19.462791	192.168.1.67	128.119.245.12	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
552	19.760691	128.119.245.12	192.168.1.67	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
661	31.766126	172.64.148.154	192.168.1.67	TLSv1.2	79	Application Data
662	31.767230	192.168.1.67	172.64.148.154	TLSv1.2	83	Application Data
369	18.370848	192.168.1.67	13.230.69.152	TLSv1.3	1849	Client Hello (SNI=threat.api.mcafee.com)
398	18.565107	13.230.69.152	192.168.1.67	TLSv1.3	181	Server Hello
399	18.565107	13.230.69.152	192.168.1.67	TLSv1.3	86	[TCP Previous segment not captured], Application Data
411	18.578475	13.230.69.152	192.168.1.67	TLSv1.3	458	Application Data
446	19.081944	13.230.69.152	192.168.1.67	TLSv1.3	112	[TCP Previous segment not captured], Application Data
455	19.225678	192.168.1.67	13.230.69.152	TLSv1.3	1817	Client Hello (SNI=threat.api.mcafee.com)
28	10.052555	192.168.1.116	255.255.255.255	UDP	504	55239 → 55239 Len=62
29	10.036206	192.168.1.105	192.168.1.255	UDP	82	57621 → 57621 Len=40
37	13.516140	192.168.1.83	255.255.255.255	UDP	214	59731 → 6667 Len=172
43	15.155271	192.168.1.116	255.255.255.255	UDP	304	63239 → 6667 Len=262
382	18.441593	192.168.1.83	255.255.255.255	UDP	214	59731 → 6667 Len=172
572	20.069444	192.168.1.116	255.255.255.255	UDP	304	63239 → 6667 Len=262
631	23.551806	192.168.1.83	255.255.255.255	UDP	214	59731 → 6667 Len=172

Dapat dilihat bahwa dari screenshot yang saya lakukan bahwa kesemua protokol yang disebutkan tadi ada di dalam screenshot yang saya lakukan .

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).

No.	Time	Source	Destination	Protocol	Length	Info
581	20.299852	192.168.1.67	128.119.245.12	HTTP	548	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
589	20.592835	128.119.245.12	192.168.1.67	HTTP	492	HTTP/1.1 200 OK (text/html)
591	20.742696	192.168.1.67	128.119.245.12	HTTP	494	GET /favicon.ico HTTP/1.1
601	21.083993	128.119.245.12	192.168.1.67	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Dapat dilihat bahwa ada selisih detik yang sangat sedikit diantara http get ke http ok , untuk mencari perbedaan waktunya kita mengurangkan http get terhadap http ok sehingga dihasilkan sekitar 0,293 detik.

3. Apa alamat Internet (IP address) dari gaia.cs.umass.edu? Apa alamat Internet komputer Anda yang mengirim pesan HTTP GET?

Perlu diperhatikan bahwa Pada paket HTTP GET, kolom “Source” menunjukkan alamat IP komputer saya, sedangkan kolom “Destination” menunjukkan alamat IP dari server. Berdasarkan screenshot yang saya lakukan dapat dilihat bahwa Alamat ip komputer saya adalah 192.168.1.67 sedangkan Alamat ip server adalah 128.119.245.12

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. [Nilai field ini digunakan sebuah web server untuk mengetahui jenis browser yang digunakan user.]

```

> Frame 581: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface \Device\NPF_{C8FD3360-5644-4F0D-8009-3145D919E8F3}
> Ethernet II, Src: Intel_d4:ea:13 (58:1c:f8:d4:ea:13), Dst: TplinkTechno_90:20:14 (f8:d1:11:90:20:14)
> Internet Protocol Version 4, Src: 192.168.1.67, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50105, Dst Port: 80, Seq: 1, Ack: 1, Len: 494
< Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-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\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: 589]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

```

Berdasarkan screenshot tersebut dapat dilihat bahwa 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 . Informasi ini menunjukkan bahwa permintaan dilakukan menggunakan browser yang memiliki identifikasi User-Agent sebagai Google Chrome versi 130 pada sistem operasi Windows 10 64-bit.

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?

```

< Transmission Control Protocol, Src Port: 50105, Dst Port: 80, Seq: 1, Ack: 1, Len: 494
  Source Port: 50105
  Destination Port: 80
  [Stream index: 11]
  [Stream Packet Number: 4]
  > [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 494]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2574908843
  [Next Sequence Number: 495 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1899142413
  Header Length: 20 bytes (5)

```

Perhatikan bahwa kita bisa melihat disini destination portnya bernilai 80 . Port 80 adalah port standar untuk protokol HTTP, yang digunakan untuk komunikasi web tanpa enkripsi (tidak aman). Ketika sebuah paket HTTP dikirim ke port 80, itu menunjukkan bahwa koneksi adalah *HTTP* biasa, bukan *HTTPS* yang lebih aman (yang menggunakan port 443).

Dengan kata lain, nilai port 80 menunjukkan bahwa permintaan ini adalah komunikasi HTTP biasa antara komputer saya sebagai klien dan server, dan data yang dikirim atau diterima tidak dienkripsi.

Pembahasan Bab 7 :

A. Aktivitas 7.1 :

1. Apakah web browser Anda menggunakan HTTP versi 1.0, 1.1, atau 2? Versi HTTP apa yang digunakan oleh server?

```
> GET /wireshark-labs/INTRO-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
```

Dari screenshot tersebut dapat dilihat bahwa web browser saya menggunakan HTTP versi 1.1

2. Bahasa apa (jika ada) yang dapat diterima oleh web browser Anda?

```
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
```

Berdasarkan screenshot tersebut dapat dilihat bahwa Bahasa yang dapat diterima oleh web browser adalah Bahasa inggris US

3. Apa kode status yang dikembalikan oleh server ke web browser Anda?

```
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Sun, 27 Oct 2024 05:47:37 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Pe
Last-Modified: Sun. 27 Oct 2024 05:47:02 GMT\r\n
```

Berdasarkan screenshot yang ada , muncul status 200 ok yang berarti permintaan sukses .

4. Kapan file HTML yang Anda unduh terakhir kali dimodifikasi di server?

```
> HTTP/1.1 200 OK\r\n
Date: Sun, 27 Oct 2024 05:47:37 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Pe
Last-Modified: Sun, 27 Oct 2024 05:47:02 GMT\r\n
ETag: "51-6256ee1a05112"\r\n
Accept-Ranges: bytes\r\n
```

Dapat dilihat disini bahwa saya terakhir kali memodifikasi pada hari minggu 27 oktober 2024 dengan waktu 05:47:37 GMT sesuai gambar diatas .

B. Aktivitas 7.2 :

No.	Time	Source	Destination	Protocol	Length	Info
4001	20.807267	192.168.1.67	128.119.245.12	HTTP	659	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4009	21.080153	128.119.245.12	192.168.1.67	HTTP	294	HTTP/1.1 304 Not Modified
4077	25.840590	192.168.1.67	152.195.38.76	HTTP	290	GET /MFEwTzBNMEswSTA3BgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2F
4079	25.866223	152.195.38.76	192.168.1.67	OCSP	791	Response
4080	25.884016	192.168.1.67	152.195.38.76	HTTP	286	GET /MFEwTzBNMEswSTA3BgUrDgMCGgUABBTk45WiKdPUwcMf8JgMC07A
4081	25.937960	152.195.38.76	192.168.1.67	OCSP	791	Response

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

```
✓ Hypertext Transfer Protocol
  ✓ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.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,
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/v
    Accept-Encoding: gzip, deflate\r\n
```

tidak ada header if modified since, berarti browser belum menyertakan permintaan kondisional pada GET pertama.

2. Periksa isi respons dari server. Apakah server secara eksplisit me-return file HTML yang diminta? Bagaimana Anda dapat mengetahuinya?

```
✓ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Accept-Ranges: bytes\r\n
    Age: 5062\r\n
    Cache-Control: max-age=7200\r\n
    Content-Type: application/ocsp-response\r\n
```

Ya, server mengembalikan file HTML yang diminta dengan status 200 ok.

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:"?

```
If-Modified-Since: Sun, 27 Oct 2024 05:59:02 GMT\r\n\r\n
```

Ada if modified since diikuti informasi waktunya yaitu sun , 27 okt 2024 05:59:02 GMT seperti yang ditunjukkan diatas .

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

```
✓ Hypertext Transfer Protocol
  ✓ HTTP/1.1 304 Not Modified\r\n
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
```

Kode 304 menunjukkan bahwa server tidak mengirimkan ulang file HTML karena tidak ada perubahan sejak terakhir kali dimodifikasi.

C. Aktivitas 7.3:

1. Berapa banyak pesan HTTP GET yang dikirimkan oleh browser Anda? Berapa nomor paket yang berisi pesan HTTP GET tersebut?

```
✓ Hypertext Transfer Protocol
  ✓ GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file3.html
    Request Version: HTTP/1.1
    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
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
```

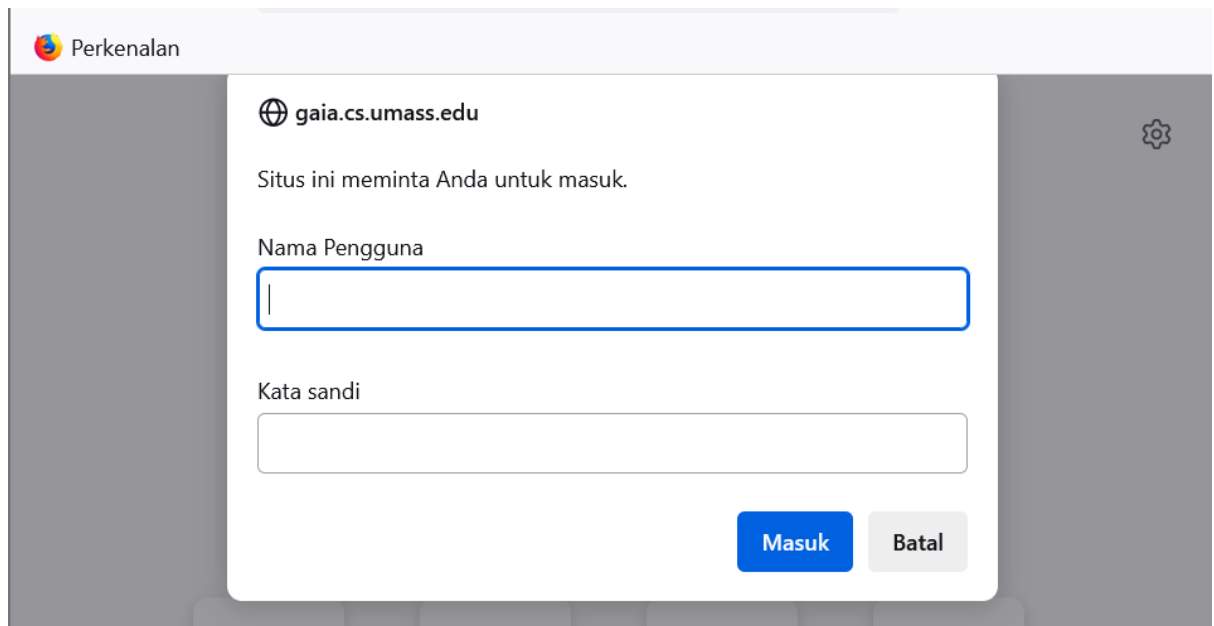
Dapat dilihat bahwa disini hanya ada satu pesan HTTP GET yang dikirimkan oleh browser untuk mengakses file HTML besar ini .

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

```
✓ [4 Reassembled TCP Segments (4861 bytes): #2045(1410), #2051(1410), #2054(1410), #2063(631)]
  [Frame: 2045, payload: 0-1409 (1410 bytes)]
  [Frame: 2051, payload: 1410-2819 (1410 bytes)]
  [Frame: 2054, payload: 2820-4229 (1410 bytes)]
  [Frame: 2063, payload: 4230-4860 (631 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data [...]: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203237204f637420
```

Dapat diperhatikan disini ada 4 segmen tcp yang berisi pecahan data yang diperlukan untuk mengirim file html yang Panjang

D. Aktivitas 7.4 :



Perkenalkan

gaia.cs.umass.edu

Situs ini meminta Anda untuk masuk.

Nama Pengguna

Kata sandi

Masuk Batal

No.	Time	Source	Destination	Protocol	Length	Info
1003	115.897121	192.168.1.67	128.119.245.12	HTTP	484	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.htm HTTP/1.1
1010	116.217253	128.119.245.12	192.168.1.67	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
1211	153.659892	192.168.1.67	128.119.245.12	HTTP	543	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.htm HTTP/1.1
1214	153.998087	128.119.245.12	192.168.1.67	HTTP	583	HTTP/1.1 404 Not Found (text/html)
1219	154.122571	192.168.1.67	128.119.245.12	HTTP	441	GET /favicon.ico HTTP/1.1
1222	154.496444	128.119.245.12	192.168.1.67	HTTP	538	HTTP/1.1 404 Not Found (text/html)

1. Apa respons dari server (kode status dan frasa) terhadap pesan HTTP GET pertama dari browser Anda?
Dapat dilihat bahwa status code pada http get pertama adalah 401 unauthorized .
2. Ketika browser Anda mengirimkan pesan HTTP GET untuk kedua kalinya, field baru apa yang disertakan dalam pesan HTTP GET tersebut?

```
✓ Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzM5ldHdvcms=\r\n
  Credentials: wireshark-students:network
\r\n
[Response in frame: 1214]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protecte
```

header HTTP yang digunakan untuk otentikasi terlihat menggunakan metode Basic Authentication, dengan nilai Authorization yang di-encode dalam format Base64 sebagai d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=. Setelah di-decode, nilai ini menunjukkan username wireshark-students dan password network. Permintaan ini diarahkan ke URI <http://gaia.cs.umass.edu/wireshark-labs/protected>, dan respons untuk permintaan ini terdapat di Frame 1214

-----*Terima Kasih*-----