

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

Tugas 7

6.2.4 Activity 1

Wireshark packet capture showing HTTP traffic. The packet list shows four HTTP GET requests. The packet details pane shows the structure of an HTTP GET request. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
104	6.525160	2404:c0:9a25:96b:b5...	2404:c0:1000:b:8077:f50c	HTTP	568	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
166	7.088725	2404:c0:1000:b:807...	2404:c0:9a25:96b:b520:101d:803e:5959	HTTP	512	HTTP/1.1 200 OK (text/html)
173	7.151493	2404:c0:9a25:96b:b5...	2404:c0:1000:b:8077:f50c	HTTP	514	GET /favicon.ico HTTP/1.1
215	7.477928	2404:c0:1000:b:807...	2404:c0:9a25:96b:b520:101d:803e:5959	HTTP	558	HTTP/1.1 404 Not Found (text/html)

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:

Yang sering muncul UDP, DNS, QUIC, TCP, TLSv1.2, HTTP

DNS:

82	5.949183	192.168.246.180	192.168.246.254	DNS	92	Standard que
83	5.949420	192.168.246.180	192.168.246.254	DNS	92	Standard que
84	5.966830	192.168.246.254	192.168.246.180	DNS	220	Standard que
85	5.990065	2404:c0:9a25:96b:b5...	2404:c0:9a25:96b::2a	DNS	112	Standard que
86	6.006513	192.168.246.254	192.168.246.180	DNS	316	Standard que
87	6.037269	2404:c0:9a25:96b::2a	2404:c0:9a25:96b:b520:101d:803e:5959	DNS	199	Standard que
110	6.500041	192.168.246.180	192.168.246.254	DNS	83	Standard que
111	6.580318	192.168.246.180	192.168.246.254	DNS	83	Standard que
116	6.613543	2404:c0:9a25:96b:b5...	2404:c0:9a25:96b::2a	DNS	103	Standard que
117	6.613543	2404:c0:9a25:96b:b5...	2404:c0:9a25:96b::2a	DNS	103	Standard que
118	6.616925	192.168.246.254	192.168.246.180	DNS	166	Standard que
119	6.617216	192.168.246.254	192.168.246.180	DNS	214	Standard que
120	6.617741	2404:c0:9a25:96b::2a	2404:c0:9a25:96b:b520:101d:803e:5959	DNS	196	Standard que
121	6.618217	2404:c0:9a25:96b::2a	2404:c0:9a25:96b:b520:101d:803e:5959	DNS	244	Standard que
177	7.155840	192.168.246.180	192.168.246.254	DNS	83	Standard que
178	7.155317	192.168.246.180	192.168.246.254	DNS	83	Standard que
180	7.188979	2404:c0:9a25:96b:b5...	2404:c0:9a25:96b::2a	DNS	103	Standard que
181	7.188979	2404:c0:9a25:96b:b5...	2404:c0:9a25:96b::2a	DNS	103	Standard que
184	7.230507	192.168.246.254	192.168.246.180	DNS	189	Standard que
186	7.230507	2404:c0:9a25:96b::2a	2404:c0:9a25:96b:b520:101d:803e:5959	DNS	200	Standard que
187	7.281415	192.168.246.254	192.168.246.180	DNS	349	Standard que
188	7.281415	2404:c0:9a25:96b::2a	2404:c0:9a25:96b:b520:101d:803e:5959	DNS	369	Standard que
607	12.561358	192.168.246.180	192.168.246.254	DNS	74	Standard que
608	12.561625	192.168.246.180	192.168.246.254	DNS	74	Standard que
609	12.605102	2404:c0:9a25:96b:b5...	2404:c0:9a25:96b::2a	DNS	94	Standard que
610	12.605102	2404:c0:9a25:96b:b5...	2404:c0:9a25:96b::2a	DNS	94	Standard que
611	12.606375	192.168.246.254	192.168.246.180	DNS	229	Standard que
612	12.607756	2404:c0:9a25:96b::2a	2404:c0:9a25:96b:b520:101d:803e:5959	DNS	274	Standard que

UDP:

63	4.232070	2404:6800:4003:c02::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	87
64	4.232070	2404:6800:4003:c02::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	316
65	4.232242	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::69	UDP	93
66	4.232291	2404:c0:9a25:96b:b5::	2404:6800:4003:c02::69	UDP	93
67	4.300290	2404:6800:4003:c02::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	85
69	4.740416	192.168.246.180	239.255.255.250	SSDP	143
73	5.423617	2404:c0:9a25:96b:b5::	2404:6800:4003:c02::69	UDP	328
75	5.491489	2404:6800:4003:c02::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	90
76	5.514759	2404:6800:4003:c02::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	940
77	5.514759	2404:6800:4003:c02::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	87
78	5.514759	2404:6800:4003:c02::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	295
79	5.515243	2404:c0:9a25:96b:b5::	2404:6800:4003:c02::69	UDP	97
80	5.515342	2404:c0:9a25:96b:b5::	2404:6800:4003:c02::69	UDP	93
81	5.596713	2404:6800:4003:c02::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	86
82	5.949183	192.168.246.180	192.168.246.254	DNS	92
83	5.949420	192.168.246.180	192.168.246.254	DNS	92
84	5.986830	192.168.246.254	192.168.246.180	DNS	220
85	5.990865	2404:c0:9a25:96b:b5::	2404:c0:9a25:96b:b520:101d:803e:5959	DNS	112
86	6.006513	192.168.246.254	192.168.246.180	DNS	316
87	6.037269	2404:c0:9a25:96b:b52a	2404:c0:9a25:96b:b520:101d:803e:5959	DNS	199
95	6.396989	192.168.246.180	224.77.77.77	UDP	148
96	6.487914	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	305
97	6.492203	2404:c0:9a25:96b:b5::	2404:6800:4003:c00::5f	UDP	658
106	6.574031	2404:6800:4003:c00::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	758
107	6.574031	2404:6800:4003:c00::	2404:c0:9a25:96b:b520:101d:803e:5959	UDP	148
108	6.574031	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	90
109	6.574616	2404:c0:9a25:96b:b5::	2404:6800:4003:c00::5f	UDP	97
110	6.580041	192.168.246.180	192.168.246.254	DNS	83

QUIC:

30	1.892244	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	313 Pr
31	1.893658	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	151 Ha
32	1.893768	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	132 Pr
33	1.894003	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	1288 Pr
34	1.894036	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	369 Pr
35	1.957863	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	1046 Pr
36	1.957863	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	183 Pr
37	1.957863	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	89 Pr
38	1.958307	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	93 Pr
39	1.960975	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	1288 Pr
40	1.961255	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	97 Pr
41	1.962653	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	1292 Pr
42	1.962653	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	475 Pr
43	1.962900	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	93
44	2.033670	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	86 Pr
96	6.487914	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	305 Pr
108	6.574031	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	90 Pr
113	6.601394	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	539 Pr
114	6.601394	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	142 Pr
115	6.601739	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	97 Pr
123	6.628763	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	94 Pr
130	6.671923	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	86 Pr
248	10.216374	2404:c0:9a25:96b:b5::	2404:6800:4003:c06::54	QUIC	1292 In
249	10.216409	2404:c0:9a25:96b:b5::	2404:6800:4003:c06::54	QUIC	1292 In
282	10.277607	2404:6800:4003:c06::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	102 In
284	10.277607	2404:6800:4003:c06::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	1292 In
286	10.277993	2404:6800:4003:c06::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	1292 In
287	10.279306	2404:6800:4003:c06::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	1292 In

TCP:

1	0.000000	2404:c0:1000::b:a29::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.2	119 Ap
2	0.052441	2404:c0:9a25:96b:b5::	2404:c0:1000::b:a29f:87ea	TCP	74 55
5	1.538347	2404:c0:9a25:96b:b5::	2001:4488:fc31::7662:7170	TCP	1474 56
6	1.538347	2404:c0:9a25:96b:b5::	2001:4488:fc31::7662:7170	TLSv1.2	1474 Ap
7	1.538347	2404:c0:9a25:96b:b5::	2001:4488:fc31::7662:7170	TCP	1474 56
8	1.538347	2404:c0:9a25:96b:b5::	2001:4488:fc31::7662:7170	TCP	1474 56
9	1.538347	2404:c0:9a25:96b:b5::	2001:4488:fc31::7662:7170	TCP	1474 56
10	1.538347	2404:c0:9a25:96b:b5::	2001:4488:fc31::7662:7170	TLSv1.2	195 Ap
11	1.571893	2001:4488:fc31::766::	2404:c0:9a25:96b:b520:101d:803e:5959	TCP	74 44
12	1.571893	2001:4488:fc31::766::	2404:c0:9a25:96b:b520:101d:803e:5959	TCP	74 44
13	1.573105	2001:4488:fc31::766::	2404:c0:9a25:96b:b520:101d:803e:5959	TCP	74 44
14	1.579708	2001:4488:fc31::766::	2404:c0:9a25:96b:b520:101d:803e:5959	TCP	74 44
15	1.685656	2001:4488:fc31::766::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.2	445 Ap
16	1.685724	2404:c0:9a25:96b:b5::	2001:4488:fc31::7662:7170	TCP	74 44
45	2.436471	2404:c0:9a25:96b:b520::	2600:1901:114be::	TCP	75 53
46	2.464550	2600:1901:114be::	2404:c0:9a25:96b:b520:101d:803e:5959	TCP	74 44
68	4.707279	2404:c0:1000::b:40e::	2404:c0:9a25:96b:b520:101d:803e:5959	TCP	74 44
70	5.303572	192.168.246.180	104.199.241.202	TCP	65 51
71	5.345015	104.199.241.202	192.168.246.180	TCP	54 40
72	5.417962	104.199.241.202	192.168.246.180	TCP	65 40
74	5.473562	192.168.246.180	104.199.241.202	TCP	54 51
88	6.038453	192.168.246.180	23.22.242.2	TCP	66 56
89	6.068113	23.22.242.2	192.168.246.180	TCP	66 44
90	6.068186	192.168.246.180	23.22.242.2	TCP	54 56
91	6.068865	192.168.246.180	23.22.242.2	TCP	1454 56
92	6.068865	192.168.246.180	23.22.242.2	TLSv1.2	566 Cl
93	6.093800	23.22.242.2	192.168.246.180	TCP	54 44
94	6.101833	23.22.242.2	192.168.246.180	TCP	54 44

TLS v1.2

1	0.000000	2404:c0:1000::b:a29::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.2	119
6	1.538347	2404:c0:9a25:96b:b5::	2001:4488:fc31::7662:7170	TLSv1.2	1474
10	1.538347	2404:c0:9a25:96b:b5::	2001:4488:fc31::7662:7170	TLSv1.2	195
15	1.685656	2001:4488:fc31::766::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.2	445
18	1.764552	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	1292
19	1.764602	2404:c0:9a25:96b:b5::	2404:6800:4003:c01::5f	QUIC	1292
22	1.841645	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	1292
23	1.841645	2404:6800:4003:c01::	2404:c0:9a25:96b:b520:101d:803e:5959	QUIC	1292
92	6.068865	192.168.246.180	23.22.242.2	TLSv1.2	566
128	6.655438	2404:c0:9a25:96b:b5::	2404:6800:4003:c03::be	TLSv1.3	503
132	6.756018	2404:6800:4003:c03::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.3	1474
139	6.779242	23.22.242.2	192.168.246.180	TLSv1.2	1454
142	6.806936	2404:6800:4003:c03::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.3	797
143	6.808629	2404:c0:9a25:96b:b5::	2404:6800:4003:c03::be	TLSv1.3	148
144	6.808693	2404:c0:9a25:96b:b5::	2404:6800:4003:c03::be	TLSv1.3	166
145	6.808795	2404:c0:9a25:96b:b5::	2404:6800:4003:c03::be	TLSv1.3	781
146	6.808822	2404:c0:9a25:96b:b5::	2404:6800:4003:c03::be	TLSv1.3	372
147	6.812527	2404:c0:1000::b:a29::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.2	127
152	6.893067	2404:6800:4003:c03::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.3	1050
153	6.893770	2404:c0:9a25:96b:b5::	2404:6800:4003:c03::be	TLSv1.3	105
154	6.940340	2404:6800:4003:c03::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.3	105
157	7.017400	23.22.242.2	192.168.246.180	TLSv1.2	1179
158	7.018535	192.168.246.180	23.22.242.2	TLSv1.2	180
159	7.018597	192.168.246.180	23.22.242.2	TLSv1.2	153
160	7.018714	192.168.246.180	23.22.242.2	TLSv1.2	410
161	7.018738	192.168.246.180	23.22.242.2	TLSv1.2	436
162	7.032261	2404:6800:4003:c03::	2404:c0:9a25:96b:b520:101d:803e:5959	TLSv1.3	462
163	7.033000	2404:c0:9a25:96b:b5::	2404:6800:4003:c03::be	TLSv1.3	113

HTTP:

No.	Time	Source	Destination	Protocol	Length	Info
104	6.525160	2404:c0:9a25:96b:b5...	2404:c0:1000::b:8077:f50c	HTTP	568	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
166	7.088725	2404:c0:1000::b:807...	2404:c0:9a25:96b:b520:101d:803e:5959	HTTP	512	HTTP/1.1 200 OK (text/html)
173	7.151493	2404:c0:9a25:96b:b5...	2404:c0:1000::b:8077:f50c	HTTP	514	GET /favicon.ico HTTP/1.1
215	7.477928	2404:c0:1000::b:807...	2404:c0:9a25:96b:b520:101d:803e:5959	HTTP	558	HTTP/1.1 404 Not Found (text/html)

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:

104	6.525160	2404:c0:9a25:96b:b5...	2404:c0:1000::b:8077:f50c	HTTP	568	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
166	7.088725	2404:c0:1000::b:807...	2404:c0:9a25:96b:b520:101d:803e:5959	HTTP	512	HTTP/1.1 200 OK (text/html)

0.563565 Sekon

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

Jawab:

Time	Source	Destination	Protocol	Length	Info
104	6.525160	2404:c0:9a25:96b:b520:101d:803e:5959	HTTP	568	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
166	7.088725	2404:c0:1000::b:8077:f50c	HTTP	512	HTTP/1.1 200 OK (text/html)

IP Address gaia.cs.umass.edu: 2404:c0:1000::b:8077:f50c

Alamat Komputer saya: 2404:c0:9a25:96b:b520:101d:803e:5959

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.]

Jawab:

<ul style="list-style-type: none"> Frame 104: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits) on interface \Device\NPF_{C4EE137D-D70F-4D72-AE40-8E14E88054CA}, id 0 Ethernet II, Src: AzureWaveTec_a5:55:f3 (34:6f:24:a5:55:f3), Dst: 06:cd:df:ff:24:e6 (06:cd:df:ff:24:e6) Internet Protocol Version 6, Src: 2404:c0:9a25:96b:b520:101d:803e:5959, Dst: 2404:c0:1000::b:8077:f50c Transmission Control Protocol, Src Port: 56400, Dst Port: 80, Seq: 1, Ack: 1, Len: 494 Hypertext Transfer Protocol <ul style="list-style-type: none"> 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=b3;q=0.7\r\n Accept-Encoding: gzip, deflate\r\n Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7\r\n \r\n [Response in frame: 166] [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

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

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:

```

Transmission Control Protocol, Src Port: 56400, Dst Port: 80, Seq: 1, Ack: 1, Len: 494
  Source Port: 56400
  Destination Port: 80
  [Stream index: 6]
  [Stream Packet Number: 4]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 494]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1965137668
  [Next Sequence Number: 495 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 946022116
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x018 (PSH, ACK)
  Window: 255
  [Calculated window size: 65280]
  [Window size scaling factor: 256]
  Checksum: 0xfda2 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
  TCP payload (494 bytes)

```

Dest Port nya: 80

7.2.2 Activity 1

No.	Time	Source	Destination	Protocol	Length	Info
71	3.605538	2404:c0:9a25:96b:b520:101d:803e:5959	2404:c0:1000:b:8077:f50c	HTTP	567	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
112	4.205594	2404:c0:1000:b:8077:f50c	2404:c0:9a25:96b:b520:101d:803e:5959	HTTP	560	HTTP/1.1 200 OK (text/html)

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

Jawab:

```

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: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  \r\n
  [Response in frame: 112]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

```

HTTP yang digunakan server adalah versi 1.1

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

Jawab:

```

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: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  \r\n
  [Response in frame: 112]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

```

Accept-Language: id-ID,id; q=0.9, en-US;q=0.8,en;q=0.7\r\n\r\n

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

Jawab:

```
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
```

200 OK

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

Jawab:

```
Last-Modified: Tue, 29 Oct 2024 05:59:01 GMT\r\n
ETag: "80-62597482ddee7"\r\n
```

7.2.3 Activity 2

124	7.464765	192.168.246.180	128.119.245.12	HTTP	569	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
208	7.769686	128.119.245.12	192.168.246.180	HTTP	784	HTTP/1.1 200 OK (text/html)
1000	31.263944	192.168.246.180	128.119.245.12	HTTP	582	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1012	31.851263	128.119.245.12	192.168.246.180	HTTP	294	HTTP/1.1 304 Not Modified

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:

```
▼ 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: id,en-US;q=0.7,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=4\r\n
    \r\n
    [Response in frame: 208]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Tidak ada

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

Jawab:

Server secara eksplisit mereturn HTML yang diminta karena terlihat dari response (text/html)

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:

```
▼ 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: id,en-US;q=0.7,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Tue, 29 Oct 2024 05:59:01 GMT\r\n
    If-None-Match: "173-62597482dd716"\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 1012]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

If-Modified-Since: Tue, 29 Oct 2024 05:59:01 GMT\r\n

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.

Jawab:

Server tidak perlu secara eksplisit menuliskan nama file HTML dalam respons karena terdapat status code 304 not modified (tidak melakukan return karena tidak ada perubahan)

7.2.4 Activity 3

No.	Time	Source	Destination	Protocol	Length	Info
218	9.487845	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	2404:c0:1000:b:8077:f50c	HTTP	568	GET /wireshark-labs/HTTP-wireshark-file3.html. HTTP/1.1
274	10.090672	2404:c0:1000:b:8077:f50c	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	HTTP	589	HTTP/1.1 404 Not Found (text/html)
275	10.116976	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	2404:c0:1000:b:8077:f50c	HTTP	514	GET /favicon.ico HTTP/1.1
277	10.446773	2404:c0:1000:b:8077:f50c	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	HTTP	558	HTTP/1.1 404 Not Found (text/html)

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

Jawab:

Ada 2 HTTP GET dengan nomor 218 dan 275

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

Jawab:

Transmission Control Protocol, Src Port: 51138, Dst Port: 80, Seq: 1, Ack: 1, Len: 494						
Source Port: 51138						
Destination Port: 80						
[Stream index: 4]						
[Stream Packet Number: 4]						
[Conversation completeness: Complete, WITH_DATA (31)]						
[TCP Segment Len: 494]						
Sequence Number: 1 (relative sequence number)						
Sequence Number (raw): 1408334393						
[Next Sequence Number: 495 (relative sequence number)]						
Acknowledgment Number: 1 (relative ack number)						
Acknowledgment number (raw): 502612696						
0101 = Header Length: 20 bytes (5)						
Flags: 0x018 (PSH, ACK)						
Window: 255						
[Calculated window size: 65280]						
[Window size scaling factor: 256]						
Checksum: 0xb38d [unverified]						
[Checksum Status: Unverified]						
Urgent Pointer: 0						
[Timestamps]						
[Time since first frame in this TCP stream: 0.021785000 seconds]						
[Time since previous frame in this TCP stream: 0.000343000 seconds]						
[SEQ/ACK analysis]						
TCP payload (494 bytes)						
Hypertext Transfer Protocol						

7.2.5 Activity 4

No.	Time	Source	Destination	Protocol	Length	Info
440	11.332486	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	2404:c0:1000:b:8077:f50c	HTTP	562	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
508	11.907217	2404:c0:1000:b:8077:f50c	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	HTTP	791	HTTP/1.1 401 Unauthorized (text/html)
764	39.505726	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	2404:c0:1000:b:8077:f50c	HTTP	647	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
769	39.838395	2404:c0:1000:b:8077:f50c	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	HTTP	564	HTTP/1.1 200 OK (text/html)
772	39.890051	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	2404:c0:1000:b:8077:f50c	HTTP	508	GET /favicon.ico HTTP/1.1
774	40.215276	2404:c0:1000:b:8077:f50c	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	HTTP	558	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?

Jawab:

508	11.907217	2404:c0:1000:b:8077:f50c	2404:c0:9a25:96b:88d2:f8aa:f25d:3fbd	HTTP	791	HTTP/1.1 401 Unauthorized (text/html)
-----	-----------	--------------------------	--------------------------------------	------	-----	---------------------------------------

401 Unauthorized, karena belum dapat authorisasi

2. Ketika browser Anda mengirimkan pesan HTTP GET untuk kedua kalinya, field baru apa yang disertakan dalam pesan HTTP GET tersebut?

Jawab:


```
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  ▼ Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmcs=\r\n
    Credentials: wireshark-students:network
    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\r\n
    \r\n
    [Response in frame: 769]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
```

Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmcs=\r\n
Didalam field berisi seperti yang saya tuliskan diatas