



LAB -1

DATA COMMUNICATIONS NETWORKS

Prof. Dr. Karim Banawan - Prof. Dr. Noha ElKorany
Communication & Electronics Department

Asmaa Gamal Abdel-Halem Mabrouk Nagy

أسماء جمال عبد الحليم مبروك ناجي

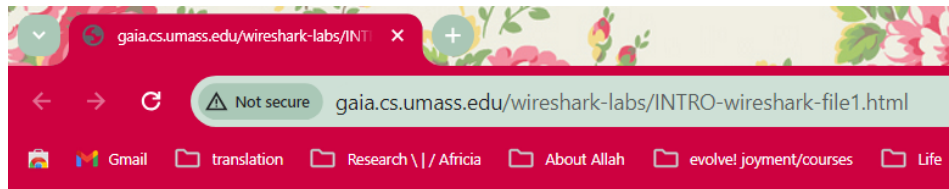
15010473 - section 8

Introduction To “Wireshark” Packet Sniffer Program



Section 0 : Taking Wireshark for a Test Run

The Task:



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

The Questions & Answers:

0. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

From the Wireshark capture below, we can see:

- TCP protocols
- QUIC protocols which are a new multiplexed transport built on top of UDP protocol
- HTTP protocols
- ARP (Address Resolution Protocol).
- DNS (Domain Name System protocol).

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
628	5.662137	172.217.18.234	192.168.1.5	QUIC	66	Protected Payload (KP0)
629	5.682454	142.251.37.46	192.168.1.5	QUIC	289	Protected Payload (KP0)
630	5.682691	192.168.1.5	142.251.37.46	QUIC	77	Protected Payload (KP0), DCID=ea0723a926dbf1b9
631	5.684865	142.251.37.46	192.168.1.5	QUIC	64	Protected Payload (KP0)
632	5.712419	192.168.1.5	142.251.37.46	QUIC	74	Protected Payload (KP0), DCID=ea0723a926dbf1b9
633	5.746979	142.251.37.46	192.168.1.5	QUIC	66	Protected Payload (KP0)
634	5.778132	128.119.245.12	192.168.1.5	TCP	54	80 → 1811 [ACK] Seq=1 Ack=567 Win=30336 Len=0
635	5.779670	128.119.245.12	192.168.1.5	HTTP	492	HTTP/1.1 200 OK (text/html)
636	5.823101	192.168.1.5	128.119.245.12	TCP	54	1811 → 80 [ACK] Seq=567 Ack=439 Win=131072 Len=0
637	5.984856	192.168.1.5	128.119.245.12	HTTP	505	GET /favicon.ico HTTP/1.1
638	6.058829	192.168.1.5	8.8.8.8	QUIC	251	Protected Payload (KP0), DCID=eca5f3fd7b57cebc
639	6.059056	192.168.1.5	8.8.8.8	QUIC	251	Protected Payload (KP0), DCID=eca5f3fd7b57cebc
640	6.096929	8.8.8.8	192.168.1.5	QUIC	69	Protected Payload (KP0)
641	6.098209	8.8.8.8	192.168.1.5	QUIC	69	Protected Payload (KP0)
642	6.098329	192.168.1.5	8.8.8.8	QUIC	73	Protected Payload (KP0), DCID=eca5f3fd7b57cebc
545	3.695685	192.168.1.5	142.250.201.4	QUIC	73	Protected Payload (KP0), DCID=fd5ef668f860c4e5
546	3.756685	142.250.201.4	192.168.1.5	QUIC	66	Protected Payload (KP0)
547	4.135227	Intel_db:e3:45	Broadcast	ARP	42	Who has 192.168.1.200? Tell 192.168.1.5
548	5.396256	192.168.1.5	8.8.8.8	QUIC	252	Protected Payload (KP0), DCID=eca5f3fd7b57cebc
549	5.396504	192.168.1.5	8.8.8.8	QUIC	252	Protected Payload (KP0), DCID=eca5f3fd7b57cebc
550	5.404372	192.168.1.5	8.8.8.8	DNS	70	Standard query 0x61fe A dns.google
551	5.404829	192.168.1.5	8.8.8.8	DNS	70	Standard query 0xfa7d HTTPS dns.google

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

http						
No.	Time	Source	Destination	Protocol	Length	Info
623	13:37:16.838630	192.168.1.5	128.119.245.12	HTTP	620	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
635	13:37:16.989271	128.119.245.12	192.168.1.5	HTTP	492	HTTP/1.1 200 OK (text/html)

To determine the time it took, we look at the get request and the HTTP OK arrival times and subtract the GET from the OK.

So, 16.989271 seconds - 16.838630 seconds = 0.150641 seconds.

3. What is the Internet address of the `gaia.cs.umass.edu` (also known as `www-net.cs.umass.edu`)? What is the Internet address of your computer?

No.	Time	Source	Destination	Protocol	Length	Info
623	13:37:16.838630	192.168.1.5	128.119.245.12	HTTP	620	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

As shown in the source and destination of the above screenshot:

- The Internet address of `gaia.cs.umass.edu` is 128.119.245.12
- The Internet address of my laptop computer is 192.168.1.5

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

Get:

```
C:\Users\DELL\AppData\Local\Temp\wireshark_Wi-FiLQN6J2.pcapng 698 total packets, 4 shown

No.      Time            Source            Destination        Protocol Length Info
 623 13:37:16.838630 192.168.1.5       128.119.245.12    HTTP      620    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 623: 620 bytes on wire (4960 bits), 620 bytes captured (4960 bits) on interface \Device\NPF_{1FE64003-
B61C-472C-8851-98EB49C717F6}, id 0
  Section number: 1
    Interface id: 0 (\Device\NPF_{1FE64003-B61C-472C-8851-98EB49C717F6})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 1, 2024 13:37:16.838630000 Egypt Standard Time
    UTC Arrival Time: Mar 1, 2024 11:37:16.838630000 UTC
    Epoch Arrival Time: 1709293036.838630000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000198000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 5.629029000 seconds]
    Frame Number: 623
    Frame Length: 620 bytes (4960 bits)
    Capture Length: 620 bytes (4960 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
  Ethernet II, Src: Intel_db:e3:45 (80:00:0b:db:e3:45), Dst: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46)
    Destination: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46)
    Source: Intel_db:e3:45 (80:00:0b:db:e3:45)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.1.5, 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: 606
    Identification: 0xa345 (41797)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
  Protocol: TCP (6)
    Header Checksum: 0x1e23 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.5
    Destination Address: 128.119.245.12
  Transmission Control Protocol, Src Port: 1811, Dst Port: 80, Seq: 1, Ack: 1, Len: 566
    Source Port: 1811
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 566]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 188178890
    [Next Sequence Number: 567 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 4210148017
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 514
    [Calculated window size: 131584]
    [Window size scaling factor: 256]
    Checksum: 0xba06 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (566 bytes)
  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/122.0.0.0 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
    dnt: 1\r\n
    If-None-Match: "51-6127fcb50c915"\r\n
```

```
If-Modified-Since: Thu, 29 Feb 2024 06:59:01 GMT\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]\n[HTTP request 1/2]\n[Response in frame: 635]\n[Next request in frame: 637]
```

OK:

C:\Users\DELL\AppData\Local\Temp\wireshark_WI-FILQN6J2.pcapng 698 total packets, 4 shown

```
No.      Time            Source                Destination            Protocol Length Info
635 13:37:16.989271 128.119.245.12        192.168.1.5            HTTP      492      HTTP/1.1 200 OK (text/html)
Frame 635: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{1FE64003-861C-472C-8851-98EB49C717F6}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{1FE64003-861C-472C-8851-98EB49C717F6})
Encapsulation type: Ethernet (1)
Arrival Time: Mar 1, 2024 13:37:16.989271000 Egypt Standard Time
UTC Arrival Time: Mar 1, 2024 11:37:16.989271000 UTC
Epoch Arrival Time: 1709293036.989271000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.001538000 seconds]
[Time delta from previous displayed frame: 0.150641000 seconds]
[Time since reference or first frame: 5.779670000 seconds]
Frame Number: 635
Frame Length: 492 bytes (3936 bits)
Capture Length: 492 bytes (3936 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46), Dst: Intel_db:e3:45 (80:00:0b:db:e3:45)
Destination: Intel_db:e3:45 (80:00:0b:db:e3:45)
Source: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 478
Identification: 0xf0e0 (61664)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 47
Protocol: TCP (6)
Header Checksum: 0x2208 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 1811, Seq: 1, Ack: 567, Len: 438
Source Port: 80
Destination Port: 1811
[Stream index: 4]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 438]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 4210148017
[Next Sequence Number: 439 (relative sequence number)]
Acknowledgment Number: 567 (relative ack number)
Acknowledgment number (raw): 188179456
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 237
[Calculated window size: 303361]

[Window size scaling factor: 128]
Checksum: 0xd31c [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (438 bytes)
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 01 Mar 2024 11:37:16 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: Fri, 01 Mar 2024 06:59:02 GMT\r\n
ETag: "51-61293e939040e8"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
```

C:\Users\DELL\AppData\Local\Temp\wireshark_WI-FILQN6J2.pcapng 698 total packets, 4 shown

```
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.150641000 seconds]
[Request in frame: 623]
[Next request in frame: 637]
[Next response in frame: 650]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Date: 81 bytes
Line-based text data: text/html (3 lines)
<html>\n
  <body>\n
    <h1>\n
      Congratulations! You've downloaded the first Wireshark lab file!\n
    </h1>\n
  </body>\n
</html>\n
```

Section1: The Basic HTTP GET/response interaction

The Task:

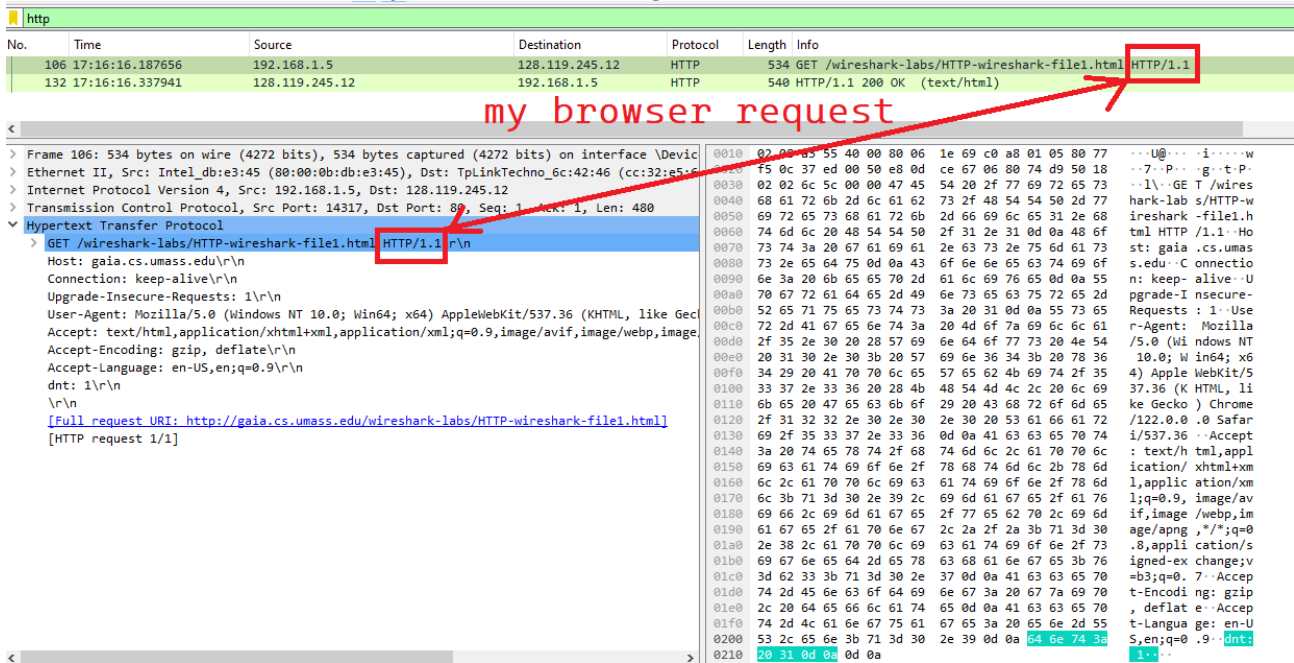


Congratulations. You've downloaded the file <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>!

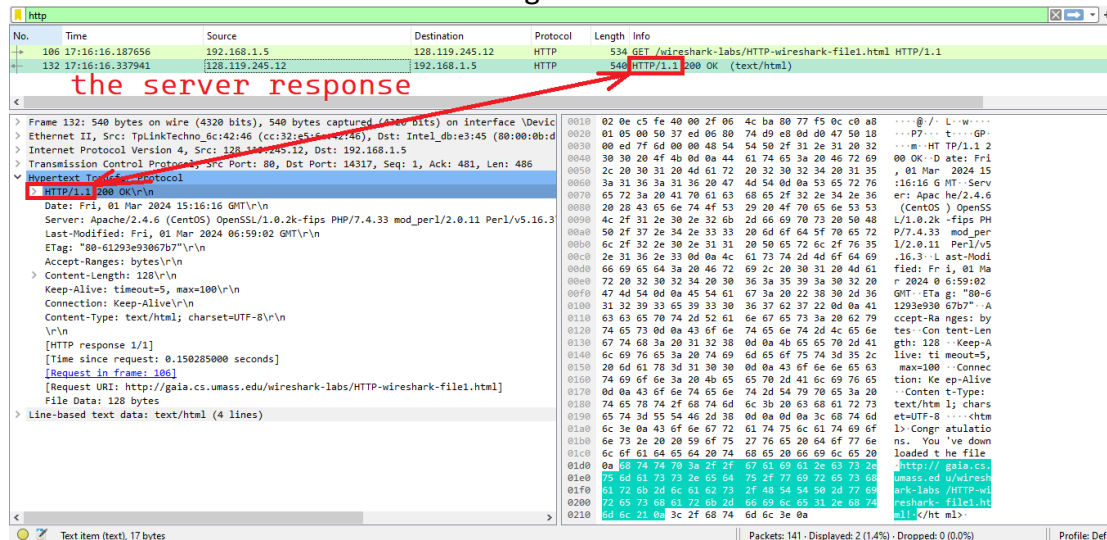
The Questions & Answers:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

This below screenshot shows my browser running HTTP version 1.1.



This below screenshot shows the server using HTTP version 1.1.



2. What languages (if any) does your browser indicate that it can accept to the server?

This below screenshot is where it says “Accept-Language”, it lists the US English as its accepted language:

```
> Frame 106: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device
> Ethernet II, Src: Intel_db:e3:45 (80:00:0b:db:e3:45), Dst: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 14317, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
▼ 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)
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image.
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    dnt: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 132]
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

As shown in the below screenshot:

- The IP of gaia.cs.umass.edu is 128.119.245.12
- The IP of my laptop computer is 192.168.1.5

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows two packets: a GET request (Frame 106) and a 200 OK response (Frame 132). Red boxes highlight the source IP (192.168.1.5) and destination IP (128.119.245.12) in the packet list. Red arrows point from the text above to these boxes. The details pane for the selected packet (Frame 106) shows the HTTP request details, including the Host, User-Agent, and Accept-Language headers.

No.	Time	Source	Destination	Protocol	Length	Info
106	17:16:16.187656	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
132	17:16:16.337941	128.119.245.12	192.168.1.5	HTTP	540	HTTP/1.1 200 OK (text/html)

4. What is the status code returned from the server to your browser?

The status code was a 200 OK.

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 01 Mar 2024 15:16:16 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: Fri, 01 Mar 2024 06:59:02 GMT\r\n
    ETag: "80-61293e93067b7"\r\n
    Accept-Ranges: bytes\r\n
```

5. When was the HTML file that you are retrieving last modified at the server?

The HTML file was Last-Modified on: Fri, 01 Mar 2024 06:59:02 GMT.

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 01 Mar 2024 15:16:16 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: Fri, 01 Mar 2024 06:59:02 GMT\r\n
    ETag: "80-61293e93067b7"\r\n
```

6. How many bytes of content are being returned to your browser?

128 bytes of content are being returned to my browser.

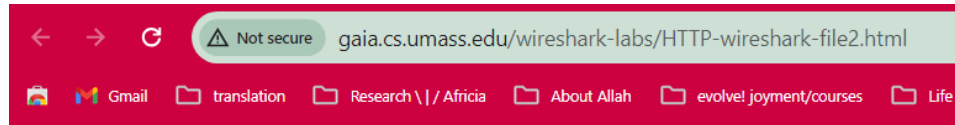
```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 01 Mar 2024 15:48:10 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 01 Mar 2024 06:59:02 GMT\r\n
    ETag: "80-61293e93067b7"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    [Content length: 128]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
```

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No, all packet headers are completely displayed in the packet-content window by an encoded format: (hexadecimal-ASCII). So, I do not see any headers that are not displayed in the packet window.

Section 2: The HTTP CONDITIONAL GET/response interaction

The Task:



Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

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.

The Questions & Answers:

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

No, there is no “IF-MODIFIED-SINCE” line in the HTTP GET.

No.	Time	Source	Destination	Protocol	Length	Info
123	18:53:10.086407	192.168.1.5	128.119.245.12	HTTP	560	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
142	18:53:10.237373	128.119.245.12	192.168.1.5	HTTP	784	HTTP/1.1 200 OK (text/html)
179	18:53:19.861691	192.168.1.5	128.119.245.12	HTTP	715	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
183	18:53:20.163139	128.119.245.12	192.168.1.5	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 123: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device\NPF_{1FE64003-B61C-472-0000-000000000000} (0.0.0.0)	0000	cc 32 e5 6c 42 46 80 00	0b db e3 45 00 00 45 00
> Ethernet II, Src: Intel_db:e3:45 (80:00:0b:db:e3:45), Dst: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46)	0010	02 22 a3 82 40 00 80 06	1e 22 c0 a8 01 05 80 77
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12	0020	f5 0c 3a 33 00 50 89 b6	b4 bc 1a 7f 16 96 50 18
> Transmission Control Protocol, Src Port: 14899, Dst Port: 80, Seq: 1, Ack: 1, Len: 506	0030	02 02 c1 3c 00 00 47 45	54 20 2f 77 69 72 65 73
> Hypertext Transfer Protocol	0040	68 61 72 6b 2d 6c 61 62	73 2f 48 54 54 50 2d 77
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n	0050	69 72 65 73 68 61 72 6b	2d 66 69 6c 65 32 2e 68
Host: gaia.cs.umass.edu\r\n	0060	74 6d 6c 20 48 54 54 50	2f 31 2e 31 0d 0a 48 6f
Connection: keep-alive\r\n	0070	73 74 3a 20 67 61 69 61	2e 63 73 2e 75 6d 61 73
Cache-Control: max-age=0\r\n	0080	73 2e 65 64 75 0d 0a 43	6f 6e 6e 65 63 74 69 6f
Upgrade-Insecure-Requests: 1\r\n	0090	6e 3a 20 6b 65 65 70 2d	61 6c 69 76 65 0d 0a 43
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36\r\n	00a0	61 63 68 65 2d 43 6f 6e	74 72 6f 6c 3a 20 6d 61
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=0.0\r\n	00b0	78 2d 61 67 65 3d 30 0d	0a 55 70 67 72 61 64 65
Accept-Encoding: gzip, deflate\r\n	00c0	2d 49 6e 73 65 63 75 72	65 2d 52 65 71 75 65 73
Accept-Language: en-US,en;q=0.9\r\n	00d0	74 73 3a 20 31 0d 0a 55	73 65 72 2d 41 67 65 6e
dnt: 1\r\n	00e0	74 3a 20 4d 6f 7a 69 6c	6c 61 2f 35 2e 30 20 2e
\r\n	00f0	57 69 6e 64 6f 77 73 20	4e 54 20 31 30 2e 30 3b
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]	0100	20 57 69 6e 36 34 3b 20	78 36 34 29 20 41 70 70
[HTTP request 1/1]	0110	6c 65 57 65 62 40 69 7a	2f 35 33 37 2e 33 36 20
[Response in frame: 142]	0120	20 4b 48 54 40 4c 2c 20	6c 69 0b 05 20 47 65 63
	0130	6b 6f 29 20 43 68 72 6f	6d 65 2f 31 32 32 2e 30
	0140	2e 30 2c 30 29 53 61 66	61 72 69 2f 35 33 37 2e
	0150	33 36 0d 0a 41 63 63 65	70 74 3a 20 74 65 78 74
	0160	2f 68 74 6d 6c 2c 61 70	70 6c 69 63 61 74 69 6f

9. Inspect the contents of the server first response. Did the server explicitly return the contents of the file? How can you tell?

Yes, the server explicitly returned the contents of the file after the first HTTP request. I am able to tell this because of the Line-based text data in the first OK response to the GET.

No.	Time	Source	Destination	Protocol	Length	Info
123	18:53:10.086407	192.168.1.5	128.119.245.12	HTTP	560	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
142	18:53:10.237373	128.119.245.12	192.168.1.5	HTTP	784	HTTP/1.1 200 OK (text/html)
179	18:53:19.861691	192.168.1.5	128.119.245.12	HTTP	715	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
183	18:53:20.163139	128.119.245.12	192.168.1.5	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 142: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{1FE64003-B61C-472-0000-000000000000} (0.0.0.0)	0130	6e 67 74 68 3a 20 33 37	31 0d 0a 4b 65 65 70 2d
> Ethernet II, Src: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46), Dst: Intel_db:e3:45 (80:00:0b:db:e3:45)	0140	41 6c 69 76 65 3a 20 74	69 6d 65 6f 75 74 3d 35
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5	0150	2c 20 6d 61 78 3d 31 30	30 0d 0a 43 6f 6e 6e 65
> Transmission Control Protocol, Src Port: 80, Dst Port: 14899, Seq: 1, Ack: 507, Len: 730	0160	63 74 69 6f 6e 3a 20 4b	65 65 70 2d 41 6c 69 76
> Hypertext Transfer Protocol	0170	65 0d 0a 43 6f 6e 74 65	6e 74 2d 54 79 70 65 3a
> Line-based text data: text/html (10 lines)	0180	20 74 65 78 74 2f 68 74	6d 6c 3b 20 63 68 61 72
\n	0190	73 65 74 3d 55 54 45 2d	38 0d 0a 0d 0a 3c 68
<html>\n	01a0	74 6d 6c 3e 0a 0a 43 6f	6e 67 72 61 74 75 6c 61
\n	01b0	74 69 6f 6e 73 20 61 67	61 69 6e 21 20 20 4e 6f
Congratulations again! Now you've downloaded the file lab2-2.html. \n	01c0	77 20 79 6f 75 27 76 65	20 64 6f 77 6e 6c 6f 61
This file's last modification date will not change. <p>\n	01d0	64 65 64 20 74 68 65 20	66 69 6c 65 20 6c 61 62
Thus if you download this multiple times on your browser, a complete copy \n	01e0	32 2d 32 2e 68 74 6d 6c	2e 20 3c 62 72 3e 0a 54
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE \n	01f0	68 69 73 20 66 69 6c 65	27 73 20 6c 61 73 74 20
field in your browser's HTTP GET request to the server.\n	0200	6d 6f 64 69 66 69 63 61	74 69 6f 6e 20 64 61 74
\n	0210	65 20 77 69 6c 6c 20 6e	6f 74 20 63 68 61 6e 67
</html>\n	0220	65 2e 20 20 3c 70 3e 0a	54 68 75 73 20 20 69 6e
	0230	20 79 6f 75 20 64 6f 77	6e 6c 6f 61 64 20 74 68
	0240	69 73 20 6d 75 6c 74 69	70 6c 65 20 74 69 6d 65
	0250	73 20 6f 6e 20 79 6f 75	72 20 62 72 6f 77 73 65
	0260	72 2c 20 61 20 63 6f 6d	70 6c 65 74 65 20 63 6f
	0270	70 79 20 3c 62 72 3e 0a	77 69 6c 6c 20 6f 6e 6c
	0280	79 20 62 65 20 73 65 6e	74 20 6f 6e 63 65 20 62
	0290	79 20 74 68 65 20 73 65	72 76 65 72 20 64 75 65
	02a0	20 74 6f 20 74 68 65 20	69 6e 63 6c 75 73 69 6f
	02b0	6e 20 6f 6e 20 74 68 65	20 49 4e 2d 4d 4f 44 49
	02c0	46 49 45 44 2d 53 49 4e	43 45 3c 62 72 3e 0a 54
	02d0	69 65 6c 64 20 69 6e 20	79 6f 75 72 20 62 72 6f
	02e0	77 73 65 72 73 20 48 54	54 54 50 20 47 45 54 20
	02f0	72 65 71 75 65 73 74 20	74 6f 20 74 68 65 20 73
	0300	65 72 76 65 72 2e 0a 3c	2f 68 74 6d 6c 3e 0a 54

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

There is an “IF-MODIFIED-SINCE:” line in the second HTTP GET request. The information that followed the “IF-MODIFIED-SINCE:” header represents the date it was modified that was not present in the first HTTP GET. Also, the information that are before the “IF-MODIFIED-SINCE” (and aren’t exist in the first http get request) are: a match query, cookies and cache-control (I suppose this is part of why the cookies/cache had to be cleared first).

No.	Time	Source	Destination	Protocol	Length	Info
123	18:53:10.086407	192.168.1.5	128.119.245.12	HTTP	560	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
142	18:53:10.237373	128.119.245.12	192.168.1.5	HTTP	784	HTTP/1.1 200 OK (text/html)
179	18:53:19.861691	192.168.1.5	128.119.245.12	HTTP	715	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
183	18:53:20.163139	128.119.245.12	192.168.1.5	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 179: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface \Device\NPF_{1FE64003-B61C-472-8000-000000000000} (08:00:0b:db:e3:45), Dst: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46)	0090	6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43
> Ethernet II, Src: Intel_db:e3:45 (80:00:0b:db:e3:45), Dst: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46)	00a0	61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12	00b0	78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 65
> Transmission Control Protocol, Src Port: 14900, Dst Port: 80, Seq: 1, Ack: 1, Len: 661	00c0	2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73
> Hypertext Transfer Protocol	00d0	74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n	00e0	74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28
Host: gaia.cs.umass.edu\r\n	00f0	57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b
Connection: keep-alive\r\n	0100	20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70
Cache-Control: max-age=0\r\n	0110	6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20
Upgrade-Insecure-Requests: 1\r\n	0120	28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36\r\n	0130	6b 6f 29 20 43 68 72 6f 6d 65 2f 31 32 32 2e 30
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=0.0\r\n	0140	2e 30 2e 30 20 53 61 66 61 72 69 2f 35 33 37 2e
Accept-Encoding: gzip, deflate\r\n	0150	33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74
Accept-Language: en-US,en;q=0.0\r\n	0160	2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f
Cookie: SL_G_WPT_T0=ar; SL_G_WPT_Show_Hide_tmp=1; SL_wptGlobTipTmp=1\r\n	0170	6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c
Cookie pair: SL_G_WPT_T0=ar	0180	69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e
Cookie pair: SL_G_WPT_Show_Hide_tmp=1	0190	39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61
Cookie pair: SL_wptGlobTipTmp=1	01a0	67 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70
Host: gaia.cs.umass.edu\r\n	01b0	6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70
Connection: keep-alive\r\n	01c0	6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d
Cache-Control: max-age=0\r\n	01d0	65 78 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d
Upgrade-Insecure-Requests: 1\r\n	01e0	30 2e 37 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36\r\n	01f0	64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c
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=0.0\r\n	0200	61 74 65 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f
Accept-Encoding: gzip, deflate\r\n	0210	75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71
Accept-Language: en-US,en;q=0.0\r\n	0220	3d 30 2e 39 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f
Cookie: SL_G_WPT_T0=ar; SL_G_WPT_Show_Hide_tmp=1; SL_wptGlobTipTmp=1\r\n	0230	5f 47 5f 50 54 5f 54 6f 4f 3d 61 72 3b 20 53 4c
Cookie pair: SL_G_WPT_T0=ar	0240	5f 47 5f 50 54 5f 54 6f 4f 3d 61 72 3b 20 53 4c
Cookie pair: SL_G_WPT_Show_Hide_tmp=1	0250	74 6d 70 3d 31 3b 20 53 4c 5f 77 70 74 47 6c 6f
Cookie pair: SL_wptGlobTipTmp=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/122.0.0.0 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=0.0\r\n		
Accept-Encoding: gzip, deflate\r\n		
Accept-Language: en-US,en;q=0.0\r\n		
Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html		
[HTTP request 1/1]		
[Response in frame: 183]		

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

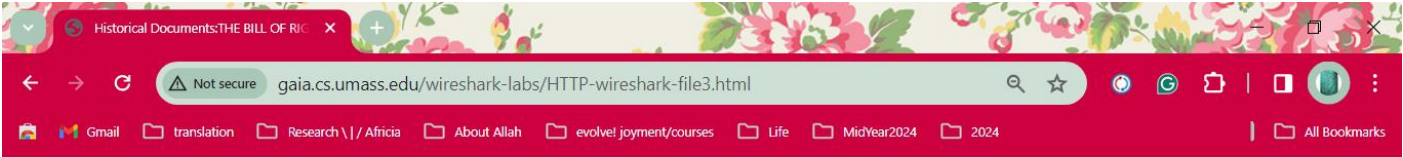
304 Not Modified. No, the server didn’t return the content of the data file again. The 304 Not Modified HTTP server response code (after a conditional GET) indicates that the requested resource has not been modified since the last time it was loaded, and there's no need to transfer it again. Since some data packets is already stored in the cache, it does not need sending again unless said cache is cleared, hence why the cache was requested to be removed.

No.	Time	Source	Destination	Protocol	Length	Info
123	18:53:10.086407	192.168.1.5	128.119.245.12	HTTP	560	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
142	18:53:10.237373	128.119.245.12	192.168.1.5	HTTP	784	HTTP/1.1 200 OK (text/html)
179	18:53:19.861691	192.168.1.5	128.119.245.12	HTTP	715	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
183	18:53:20.163139	128.119.245.12	192.168.1.5	HTTP	294	HTTP/1.1 304 Not Modified

> Frame 183: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{1FE64003-B61C-472-8000-000000000000} (08:00:0b:db:e3:45), Dst: Intel_db:e3:45 (80:00:0b:db:e3:45)	0000	80 00 0b db e3 45 cc 32 e5 6c 42 4e 08 00 45 00
> Ethernet II, Src: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46), Dst: Intel_db:e3:45 (80:00:0b:db:e3:45)	0010	01 18 13 00 40 00 2f 06 ff de 80 77 f5 0c c0 a8
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5	0020	01 05 00 50 3a 34 96 9a 9e 10 bb 9b 6d 50 50 18
> Transmission Control Protocol, Src Port: 80, Dst Port: 14900, Seq: 1, Ack: 662, Len: 240	0030	00 ef 2c 13 00 00 48 54 54 50 2f 31 2e 31 20 33
> Hypertext Transfer Protocol	0040	30 34 20 4e 6f 7a 20 4d 6f 64 69 66 69 65 64 0d
> HTTP/1.1 304 Not Modified\r\n	0050	0a 44 61 74 65 3a 20 46 72 69 2c 20 30 31 20 4d
Date: Fri, 01 Mar 2024 16:53:19 GMT\r\n	0060	61 72 20 32 30 32 34 20 31 36 3a 35 33 3a 31 39
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	0070	20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70
Connection: Keep-Alive\r\n	0080	61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74
Keep-Alive: timeout=5, max=100\r\n	0090	4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e
ETag: "173-61293e9305fe7"\r\n	00a0	32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e
\r\n	00b0	33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e
[HTTP response 1/1]	00c0	31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d
[Time since request: 0.301448000 seconds]	00d0	0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65
[Request in frame: 179]	00e0	70 2d 41 6c 69 76 65 0d 0a 4b 65 65 70 2d 41 6c
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]	00f0	69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20
	0100	6d 61 78 3d 31 30 30 0d 0a 45 54 61 67 3a 20 22
	0110	31 37 33 2d 36 31 32 39 33 65 39 33 30 35 66 65
	0120	37 22 0d 0a 0d 0a

Section 3: Retrieving Long Documents

The Task:



The Questions & Answers:

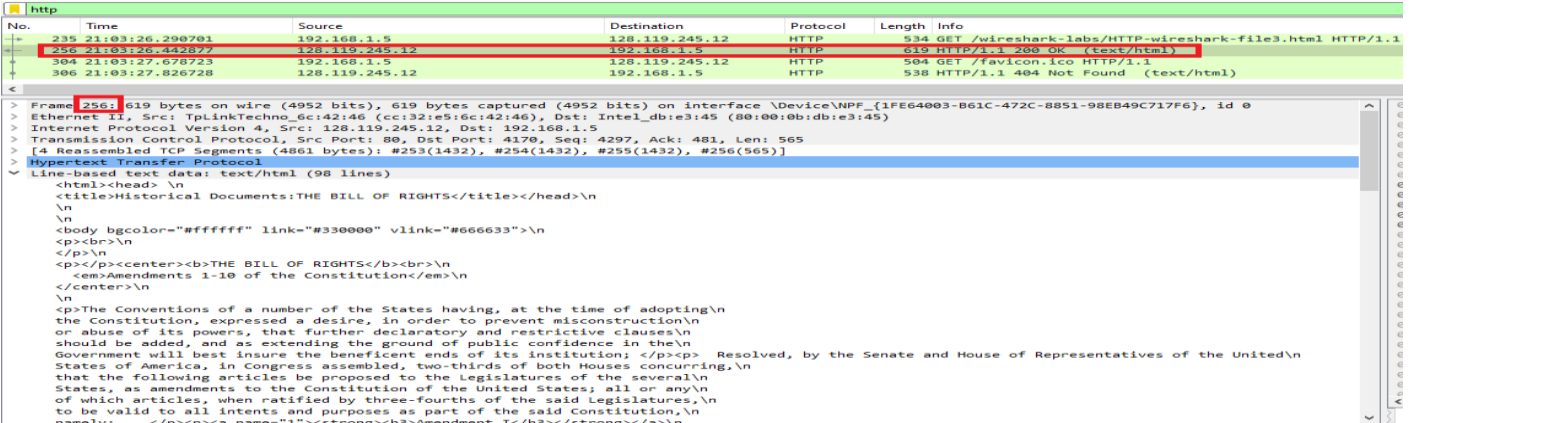
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

My browser sent only one HTTP GET request message. Packet number 235 contained the GET HTTP request for the Bill or Rights. Because we should ignore any HTTP GET and response for favicon.ico. If we see a reference to this file, it is the browser automatically asking the server if it (the server) has a small icon file that should be displayed next to the displayed URL in your browser. We'll ignore references to this pesky file in the whole lab.

http						
No.	Time	Source	Destination	Protocol	Length	Info
235	21:03:26.290701	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
256	21:03:26.442877	128.119.245.12	192.168.1.5	HTTP	619	HTTP/1.1 200 OK (text/html)
304	21:03:27.678723	192.168.1.5	128.119.245.12	HTTP	504	GET /favicon.ico HTTP/1.1
306	21:03:27.826728	128.119.245.12	192.168.1.5	HTTP	538	HTTP/1.1 404 Not Found (text/html)

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Packet 256 contains the status code and phrase associated with the response to the HTTP GET request.



14. What is the status code and phrase in the response?

In the response, the status code is 200, and the phrase is an OK.

No.	Time	Source	Destination	Protocol	Length	Info
235	21:03:26.290701	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
256	21:03:26.442877	128.119.245.12	192.168.1.5	HTTP	619	HTTP/1.1 200 OK (text/html)
304	21:03:27.678723	192.168.1.5	128.119.245.12	HTTP	504	GET /favicon.ico HTTP/1.1
306	21:03:27.826728	128.119.245.12	192.168.1.5	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 256: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface \Device\NPF_{1FE64003-B61C-472C-8851-98EB49C717F6}, id 0	00f1
> Ethernet II, Src: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46), Dst: Intel_db:e3:45 (80:00:0b:db:e3:45)	0100
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5	0110
> Transmission Control Protocol, Src Port: 80, Dst Port: 4170, Seq: 4297, Ack: 481, Len: 565	0120
> [4 Reassembled TCP Segments (4861 bytes): #253(1432), #254(1432), #255(1432), #256(565)]	0130
> Hypertext Transfer Protocol	0140
> HTTP/1.1 200 OK\r\n	0150
Date: Fri, 01 Mar 2024 19:03:25 GMT\r\n	0160
	0170

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

There are:

- 3 data-containing TCP segments “TCP segment of a reassembled PDU “.
- The fourth one is the http response itself.

So, the total count is 4 that are needed to carry the single HTTP response and the text of the Bill of Rights. As shown in the below screenshots:

Wireshark - Packet 256 - section 3 retrieving long documents.pcapng

Frame 256: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface \Device\NPF_{1FE64003-B61C-472C-8851-98EB49C717F6}, id 0

Ethernet II, Src: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46), Dst: Intel_db:e3:45 (80:00:0b:db:e3:45)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5

Transmission Control Protocol, Src Port: 80, Dst Port: 4170, Seq: 4297, Ack: 481, Len: 565

[4 Reassembled TCP Segments (4861 bytes): #253(1432), #254(1432), #255(1432), #256(565)]

[Frame: 253, payload: 0-1431 (1432 bytes)]

[Frame: 254, payload: 1432-2863 (1432 bytes)]

[Frame: 255, payload: 2864-4295 (1432 bytes)]

[Frame: 256, payload: 4296-4860 (565 bytes)]

[Segment count: 4]

first TCP segment

second TCP segment

third TCP segment

the http response

Frame (619 bytes)

Reassembled TCP (4861 bytes)

No: 256 - Time: 21:03:26.442877 - Source: 128.119.245.12 - Destination: 192.168.1.5 - Protocol: HTTP - Length: 619 - Info: HTTP/1.1 200 OK (text/html)

Show packet bytes

Close Help

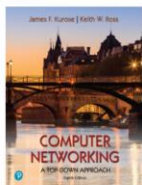
Source	Destination	Protocol	Length	Info
192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
192.168.1.5	128.119.245.12	TLSv1.2	122	Application Data
192.168.1.5	128.119.245.12	TLSv1.2	553	Application Data
192.168.1.5	128.119.245.12	TLSv1.2	85	Application Data
192.168.1.5	8.8.8.8	TCP	54	4164 → 443 [ACK] Seq=492 Ack=1314 Win=254 Len=0
192.168.1.5	74.125.68.91	TCP	66	4172 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8.8.8.8	192.168.1.5	TCP	54	443 → 4170 [ACK] Seq=1314 Ack=492 Win=273 Len=0
8.8.8.8	192.168.1.5	QUIC	1282	Handshake, SCID=e61ac43cfa092394
8.8.8.8	192.168.1.5	QUIC	106	Protected Payload (KP0)
192.168.1.5	8.8.8.8	QUIC	201	Protected Payload (KP0), DCID=e61ac43cfa092394
192.168.1.5	8.8.8.8	QUIC	74	Protected Payload (KP0), DCID=e61ac43cfa092394
8.8.8.8	192.168.1.5	QUIC	974	Protected Payload (KP0)
8.8.8.8	192.168.1.5	QUIC	163	Protected Payload (KP0)
192.168.1.5	8.8.8.8	QUIC	73	Protected Payload (KP0), DCID=e61ac43cfa092394
8.8.8.8	192.168.1.5	QUIC	66	Protected Payload (KP0)
128.119.245.12	192.168.1.5	TCP	66	80 → 4171 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1432 SACK_PERM WS=128
192.168.1.5	128.119.245.12	TCP	54	4171 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
128.119.245.12	192.168.1.5	TCP	54	80 → 4170 [ACK] Seq=1433 Ack=481 Win=30336 Len=0
128.119.245.12	192.168.1.5	TCP	1486	80 → 4170 [ACK] Seq=1433 Ack=481 Win=30336 Len=1432 [TCP segment of a reassembled PDU]
128.119.245.12	192.168.1.5	TCP	1486	80 → 4170 [ACK] Seq=2865 Ack=481 Win=30336 Len=1432 [TCP segment of a reassembled PDU]
128.119.245.12	192.168.1.5	TCP	1486	80 → 4170 [ACK] Seq=2865 Ack=481 Win=30336 Len=1432 [TCP segment of a reassembled PDU]
128.119.245.12	192.168.1.5	TCP	619	HTTP/1.1 200 OK (text/html)
192.168.1.5	128.119.245.12	TCP	54	4170 → 80 [ACK] Seq=481 Ack=4862 Win=131584 Len=0
192.168.1.5	74.125.68.91	TCP	66	4173 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
74.125.68.91	192.168.1.5	TCP	66	443 → 4172 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
192.168.1.5	74.125.68.91	TCP	54	4172 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
192.168.1.5	74.125.68.91	TLSv1.3	597	Client Hello (SNI=safebrowsing.google.com)
Intel_db:e3:45	Broadcast	ARP	42	Who has 192.168.1.200? Tell 192.168.1.5
74.125.68.91	192.168.1.5	TCP	66	443 → 4173 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256

Section 4: HTML Documents with Embedded Objects

The Task:



This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.cslash.net in France:



And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_ross.

The Questions & Answers:

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

There are 3 HTTP GET request messages that were sent by my browser (whose IP address is = 192.168.1.15) and were sent to 2 different IP addresses which are 128.119.245.12 (Host: gaia.cs.umass.edu), 178.79.137.164 (Host: kurose.cslash.net).

No.	Time	Source	Destination	Protocol	Length	Info
110	22:54:04.643330	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
129	22:54:04.793343	128.119.245.12	192.168.1.5	HTTP	1355	HTTP/1.1 200 OK (text/html)
131	22:54:04.862427	192.168.1.5	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
140	22:54:05.016559	128.119.245.12	192.168.1.5	HTTP	801	HTTP/1.1 200 OK (PNG)
152	22:54:05.093693	192.168.1.5	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
157	22:54:05.156137	178.79.137.164	192.168.1.5	HTTP	225	HTTP/1.1 301 Moved Permanently

As following:

- 1st GET is to retrieve the initial webpage.
- 2nd GET is to retrieve a referenced image from its base webpage at the same server.
- 3rd GET is to retrieve a 2nd referenced image from its base webpage at a different server.

No.	Time	Source	Destination	Protocol	Length	Info
110	22:54:04.643330	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
129	22:54:04.793343	128.119.245.12	192.168.1.5	HTTP	1355	HTTP/1.1 200 OK (text/html)
131	22:54:04.862427	192.168.1.5	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
140	22:54:05.016559	128.119.245.12	192.168.1.5	HTTP	801	HTTP/1.1 200 OK (PNG)
152	22:54:05.093693	192.168.1.5	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
157	22:54:05.156137	178.79.137.164	192.168.1.5	HTTP	225	HTTP/1.1 301 Moved Permanently

No.	Time	Source	Destination	Protocol	Length	Info
110	22:54:04.643330	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
129	22:54:04.793343	128.119.245.12	192.168.1.5	HTTP	1355	HTTP/1.1 200 OK (text/html)
131	22:54:04.862427	192.168.1.5	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
140	22:54:05.016559	128.119.245.12	192.168.1.5	HTTP	801	HTTP/1.1 200 OK (PNG)
152	22:54:05.093693	192.168.1.5	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
157	22:54:05.156137	178.79.137.164	192.168.1.5	HTTP	225	HTTP/1.1 301 Moved Permanently

No.	Time	Source	Destination	Protocol	Length	Info
110	22:54:04.643330	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
129	22:54:04.793343	128.119.245.12	192.168.1.5	HTTP	1355	HTTP/1.1 200 OK (text/html)
131	22:54:04.862427	192.168.1.5	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
140	22:54:05.016559	128.119.245.12	192.168.1.5	HTTP	801	HTTP/1.1 200 OK (PNG)
152	22:54:05.093693	192.168.1.5	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
157	22:54:05.156137	178.79.137.164	192.168.1.5	HTTP	225	HTTP/1.1 301 Moved Permanently

No.	Time	Source	Destination	Protocol	Length	Info
110	22:54:04.643330	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
129	22:54:04.793343	128.119.245.12	192.168.1.5	HTTP	1355	HTTP/1.1 200 OK (text/html)
131	22:54:04.862427	192.168.1.5	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
140	22:54:05.016559	128.119.245.12	192.168.1.5	HTTP	801	HTTP/1.1 200 OK (PNG)
152	22:54:05.093693	192.168.1.5	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
157	22:54:05.156137	178.79.137.164	192.168.1.5	HTTP	225	HTTP/1.1 301 Moved Permanently

No.	Time	Source	Destination	Protocol	Length	Info
110	22:54:04.643330	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
129	22:54:04.793343	128.119.245.12	192.168.1.5	HTTP	1355	HTTP/1.1 200 OK (text/html)
131	22:54:04.862427	192.168.1.5	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
140	22:54:05.016559	128.119.245.12	192.168.1.5	HTTP	801	HTTP/1.1 200 OK (PNG)
152	22:54:05.093693	192.168.1.5	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
157	22:54:05.156137	178.79.137.164	192.168.1.5	HTTP	225	HTTP/1.1 301 Moved Permanently

No.	Time	Source	Destination	Protocol	Length	Info
110	22:54:04.643330	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
129	22:54:04.793343	128.119.245.12	192.168.1.5	HTTP	1355	HTTP/1.1 200 OK (text/html)
131	22:54:04.862427	192.168.1.5	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
140	22:54:05.016559	128.119.245.12	192.168.1.5	HTTP	801	HTTP/1.1 200 OK (PNG)
152	22:54:05.093693	192.168.1.5	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
157	22:54:05.156137	178.79.137.164	192.168.1.5	HTTP	225	HTTP/1.1 301 Moved Permanently

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

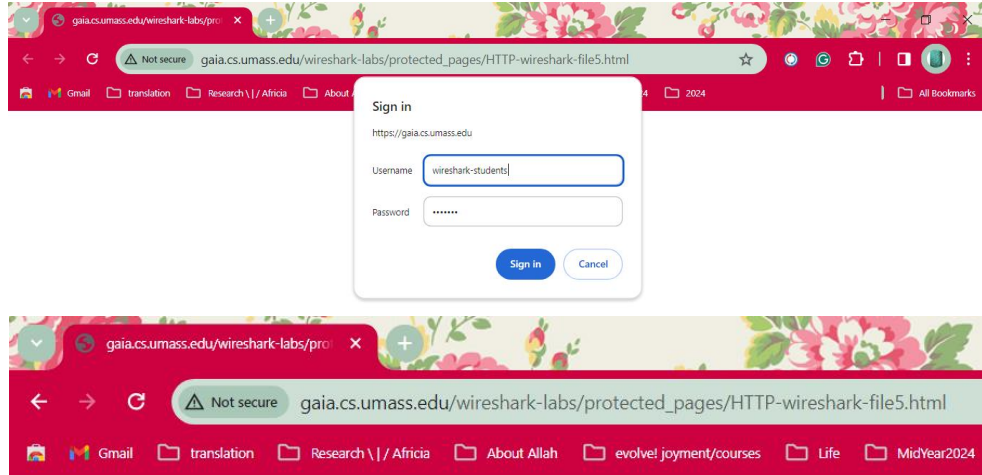
they were downloaded serially. Serially operation because they're on different time stamps as the GET is sent out after an response is seen. So, the first image appeared, then the second image started to load, although the second image was hosted in another website!

No.	Time	Source	Destination	Protocol	Length	Info
110	22:54:04.643330	192.168.1.5	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
129	22:54:04.793343	128.119.245.12	192.168.1.5	HTTP	1355	HTTP/1.1 200 OK (text/html)
131	22:54:04.862427	192.168.1.5	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
140	22:54:05.016559	128.119.245.12	192.168.1.5	HTTP	801	HTTP/1.1 200 OK (PNG)
152	22:54:05.093693	192.168.1.5	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
157	22:54:05.156137	178.79.137.164	192.168.1.5	HTTP	225	HTTP/1.1 301 Moved Permanently

1
2
3
serially

Section 5: HTTP Authentication

The Task:



This page is password protected! If you're seeing this, you've downloaded the page correctly
Congratulations!

The Questions & Answers:

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

The server's response to my HTTP GET message is a 401 Unauthorized :

- Required status code:401
- Required phrase: Unauthorized

No.	Time	Source	Destination	Protocol	Length	Info
171	00:02:57.754922	192.168.1.5	128.119.245.12	HTTP	550	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
214	00:02:57.907868	128.119.245.12	192.168.1.5	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
424	00:03:22.840065	192.168.1.5	34.104.35.123	HTTP	453	HEAD /cgi-bin/diffgen-puffin/hfnkpinlhgieaddgfemjhofmblnib/1.fae699802872dced

> Frame 214: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{1FE64003-B61C-472C-8851-98EB49C717F6}, id 0	0000	00 00 0b db e3 45 cc
> Ethernet II, Src: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46), Dst: Intel_db:e3:45 (80:00:0b:db:e3:45)	0010	02 f5 4b b5 40 00 2f
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5	0020	01 05 00 50 13 46 6f
> Transmission Control Protocol, Src Port: 80, Dst Port: 4934, Seq: 1, Ack: 497, Len: 717	0030	00 ed 4b 06 00 00 48
> Hypertext Transfer Protocol	0040	30 31 20 55 6e 61 75
> HTTP/1.1 401 Unauthorized	0050	0a 44 61 74 65 3a 20
Date: Fri, 01 Mar 2024 22:02:56 GMT	0060	61 72 20 32 30 32 34
	0070	20 47 4d 54 0d 0a 53

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The Authorization field with its credentials providing username & password for secure websites.

784	00:03:26.281113	192.168.1.1	192.168.1.5	HTTP/XML	404	HTTP/1.1 200 OK
878	00:03:29.068727	192.168.1.5	128.119.245.12	HTTP	635	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
880	00:03:29.220915	128.119.245.12	192.168.1.5	HTTP	544	HTTP/1.1 200 OK (text/html)
882	00:03:29.453829	192.168.1.5	128.119.245.12	HTTP	520	GET /favicon.ico HTTP/1.1
887	00:03:29.604311	128.119.245.12	192.168.1.5	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 878: 635 bytes on wire (5080 bits), 635 bytes captured (5080 bits) on interface \Device\NPF_{1FE64003-B61C-472C-8851-98EB49C717F6}, id 0	
> Ethernet II, Src: Intel_db:e3:45 (80:00:0b:db:e3:45), Dst: TplinkTechno_6c:42:46 (cc:32:e5:6c:42:46)	
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12	
> Transmission Control Protocol, Src Port: 4968, Dst Port: 80, Seq: 1, Ack: 1, Len: 581	
> Hypertext Transfer Protocol	
> GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1	
Host: gaia.cs.umass.edu	
Connection: keep-alive	
Cache-Control: max-age=0	
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5m=\r\n	Encoded Base64 format for username:password
Credentials: wireshark-students:network	username:password in ASCII
Upgrade-Insecure-Requests: 1	
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36	
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	

