

Assignment 3

Part-1

1. The browser is running HTTP version 1.1(Request Version: HTTP/1.1)

The screenshot shows a Wireshark capture of an HTTP request. The packet list pane displays four packets: a GET request for /wireshark-labs/HTTP-wireshark-file1.html (1450 bytes), a 200 OK response (540 bytes), a GET request for /favicon.ico (402 bytes), and a 404 Not Found response (539 bytes). The packet details pane for the first packet (1450) shows the Hypertext Transfer Protocol section expanded, displaying the GET method, URI, and version (HTTP/1.1). The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
1450	16:08:28.455927	10.196.178.11	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1473	16:08:28.736864	128.119.245.12	10.196.178.11	HTTP	540	HTTP/1.1 200 OK (text/html)
1480	16:08:28.787990	10.196.178.11	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
1532	16:08:29.069604	128.119.245.12	10.196.178.11	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Frame 1450: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-4C87-AAD4-4BFA9668CF4E}, id 0
Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
Internet Protocol Version 4, Src: 10.196.178.11, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54178, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1

The server is running HTTP version 1.1(Response Version: HTTP/1.1)

The screenshot shows a Wireshark capture of an HTTP response. The packet list pane displays four packets: a GET request for /wireshark-labs/HTTP-wireshark-file1.html (1450 bytes), a 200 OK response (540 bytes), a GET request for /favicon.ico (402 bytes), and a 404 Not Found response (539 bytes). The packet details pane for the second packet (1473) shows the Hypertext Transfer Protocol section expanded, displaying the 200 OK status, version (HTTP/1.1), and response version (HTTP/1.1). The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
1450	16:08:28.455927	10.196.178.11	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1473	16:08:28.736864	128.119.245.12	10.196.178.11	HTTP	540	HTTP/1.1 200 OK (text/html)
1480	16:08:28.787990	10.196.178.11	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
1532	16:08:29.069604	128.119.245.12	10.196.178.11	HTTP	539	HTTP/1.1 404 Not Found (text/html)

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

2. Accept-language: en-US,en with q(relative-factor)=0.5

The browser indicates that it can accept US English and other types of english to the server.

Wireshark capture showing HTTP traffic. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the request method, URI, and version.

No.	Time	Source	Destination	Protocol	Length	Info
1450	16:08:28.455927	10.196.178.11	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1473	16:08:28.736864	128.119.245.12	10.196.178.11	HTTP	540	HTTP/1.1 200 OK (text/html)
1480	16:08:28.787990	10.196.178.11	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
1532	16:08:29.069604	128.119.245.12	10.196.178.11	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Frame 1450: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-4C87-AAD4-4BFA9668CF4E}, id 0

Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)

Internet Protocol Version 4, Src: 10.196.178.11, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 54178, Dst Port: 80, Seq: 1, Ack: 1, Len: 391

Hypertext Transfer Protocol

- GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 - [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file1.html
 - Request Version: HTTP/1.1
 - Host: gaia.cs.umass.edu\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
 - Accept-Language: en-US,en;q=0.5\r\n

3. IP address of my computer is 10.196.178.11

IP address of the gaia.cs.umass.edu server is 128.119.245.12

Wireshark capture showing HTTP traffic. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the request method, URI, and version.

No.	Time	Source	Destination	Protocol	Length	Info
1450	16:08:28.455927	10.196.178.11	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1473	16:08:28.736864	128.119.245.12	10.196.178.11	HTTP	540	HTTP/1.1 200 OK (text/html)

4. The status code returned from the server to my browser is 200(Status Code Description: OK)

Wireshark capture showing HTTP traffic. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the response status code 200 OK.

No.	Time	Source	Destination	Protocol	Length	Info
1450	16:08:28.455927	10.196.178.11	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1473	16:08:28.736864	128.119.245.12	10.196.178.11	HTTP	540	HTTP/1.1 200 OK (text/html)
1480	16:08:28.787990	10.196.178.11	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
1532	16:08:29.069604	128.119.245.12	10.196.178.11	HTTP	539	HTTP/1.1 404 Not Found (text/html)

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]

5. The HTML file that I am retrieving was last modified at the server at Tuesday, 16th Jan 2024 06:59:02 AM.

The screenshot shows the Wireshark interface with a packet capture of an HTTP transaction. The packet list shows four packets: a GET request for file1.html (1450), the corresponding 200 OK response (1473), a GET request for favicon.ico (1480), and a 404 Not Found response (1532). The packet details pane for the selected HTTP response (1473) shows the following information:

- Protocol: 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: Tue, 16 Jan 2024 10:38:28 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: Tue, 16 Jan 2024 06:59:02 GMT\r\n

The packet bytes pane on the right shows the raw data of the response, starting with 0070 65 72 3a 20 41 70 61.

6. 128 bytes of content are being returned to your browser(Content-Length: 128).

The screenshot shows the Wireshark interface with the same packet capture. The packet details pane for the selected HTTP response (1473) now shows the following information:

- Content-Length: 128\r\n
- Keep-Alive: timeout=5, max=100\r\n
- Connection: Keep-Alive\r\n
- Content-Type: text/html; charset=UTF-8\r\n
- \r\n
- [HTTP response 1/1]
- [Time since request: 0.280937000 seconds]
- [Request in frame: 1450]
- [Request URI: http://gala.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
- File Data: 128 bytes

7. No, I don't see any headers within the data that are not displayed in the packet-listing window.

The below is an example checking for a GET message, similarly for all other requests/responses every field is displayed in the packet-listing window.

No.	Time	Source	Destination	Protocol	Length	Info
445	20:51:01.968415	10.240.204.85	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
449	20:51:02.202525	128.119.245.12	10.240.204.85	HTTP	540	HTTP/1.1 200 OK (text/html)
461	20:51:02.267019	10.240.204.85	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
476	20:51:02.505596	128.119.245.12	10.240.204.85	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 445: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-40...}	0000	f8 7a 41 13 2a c2 14 13 33 c7 3e 39 08 00 45 00
> Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2)	0010	01 af 77 1a 40 00 80 06 35 65 0a f0 cc 55 80 77
> Internet Protocol Version 4, Src: 10.240.204.85, Dst: 128.119.245.12	0020	f5 0c f8 c2 00 50 c8 39 7b 26 df dd b9 11 50 18
> Transmission Control Protocol, Src Port: 63682, Dst Port: 80, Seq: 1, Ack: 1, Len: 391	0030	02 00 b7 83 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
	0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68
	0060	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
	0070	73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73
	0080	73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e
	0090	74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28
	00a0	57 69 6a 64 6f 77 72 20 4e 54 20 31 30 2a 30 3b
	00b0	20 57 69 6a 36 34 3b 20 78 36 34 3b 20 72 76 3a
	00c0	31 32 31 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31
	00d0	30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 32
	00e0	31 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78
	00f0	74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69
	0100	6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70
	0110	6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30
	0120	2e 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d
	0130	61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30
	0140	2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75
	0150	61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d
	0160	30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f
	0170	64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c
	0180	61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a
	0190	20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67
	01a0	73 61 64 65 34 40 6a 73 65 63 75 73 65 74 53 6f

No.	Time	Source	Destination	Protocol	Length	Info
445	20:51:01.968415	10.240.204.85	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
449	20:51:02.202525	128.119.245.12	10.240.204.85	HTTP	540	HTTP/1.1 200 OK (text/html)
461	20:51:02.267019	10.240.204.85	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
476	20:51:02.505596	128.119.245.12	10.240.204.85	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 445: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-40...}	0000	f8 7a 41 13 2a c2 14 13 33 c7 3e 39 08 00 45 00
> Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2)	0010	01 af 77 1a 40 00 80 06 35 65 0a f0 cc 55 80 77
> Internet Protocol Version 4, Src: 10.240.204.85, Dst: 128.119.245.12	0020	f5 0c f8 c2 00 50 c8 39 7b 26 df dd b9 11 50 18
> Transmission Control Protocol, Src Port: 63682, Dst Port: 80, Seq: 1, Ack: 1, Len: 391	0030	02 00 b7 83 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
	0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68
	0060	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f

No.	Time	Source	Destination	Protocol	Length	Info
445	20:51:01.968415	10.240.204.85	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
449	20:51:02.202525	128.119.245.12	10.240.204.85	HTTP	540	HTTP/1.1 200 OK (text/html)
461	20:51:02.267019	10.240.204.85	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
476	20:51:02.505596	128.119.245.12	10.240.204.85	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 445: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-40...}	0000	f8 7a 41 13 2a c2 14 13 33 c7 3e 39 08 00 45 00
> Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2)	0010	01 af 77 1a 40 00 80 06 35 65 0a f0 cc 55 80 77
> Internet Protocol Version 4, Src: 10.240.204.85, Dst: 128.119.245.12	0020	f5 0c f8 c2 00 50 c8 39 7b 26 df dd b9 11 50 18
> Transmission Control Protocol, Src Port: 63682, Dst Port: 80, Seq: 1, Ack: 1, Len: 391	0030	02 00 b7 83 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
	0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68
	0060	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
	0070	73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73

No.	Time	Source	Destination	Protocol	Length	Info
445	20:51:01.968415	10.240.204.85	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
449	20:51:02.202525	128.119.245.12	10.240.204.85	HTTP	540	HTTP/1.1 200 OK (text/html)
461	20:51:02.267019	10.240.204.85	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
476	20:51:02.505596	128.119.245.12	10.240.204.85	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 445: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-40...}	0020	f5 0c f8 c2 00 50 c8 39 7b 26 df dd b9 11 50 18
> Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2)	0030	02 00 b7 83 00 00 47 45 54 20 2f 77 69 72 65 73
> Internet Protocol Version 4, Src: 10.240.204.85, Dst: 128.119.245.12	0040	68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77
> Transmission Control Protocol, Src Port: 63682, Dst Port: 80, Seq: 1, Ack: 1, Len: 391	0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68
> Hypertext Transfer Protocol	0060	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
	0070	73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73
	0080	73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e
	0090	74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28

http								
No.	Time	Source	Destination	Protocol	Length	Info		
445	20:51:01.968415	10.240.204.85	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1		
449	20:51:02.202525	128.119.245.12	10.240.204.85	HTTP	540	HTTP/1.1 200 OK (text/html)		
461	20:51:02.267019	10.240.204.85	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1		
476	20:51:02.505596	128.119.245.12	10.240.204.85	HTTP	539	HTTP/1.1 404 Not Found (text/html)		
> Frame 445: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-44... > Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2) > Internet Protocol Version 4, Src: 10.240.204.85, Dst: 128.119.245.12 > Transmission Control Protocol, Src Port: 63682, Dst Port: 80, Seq: 1, Ack: 1, Len: 391 > Hypertext Transfer Protocol							0020	f5 0c f8 c2 00 50 c8 39 7b 26 df dd b9 11 50 18
							0030	02 00 b7 83 00 00 47 45 54 20 2f 77 69 72 65 73
							0040	68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77
							0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68
							0060	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
							0070	73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73
							0080	73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e
							0090	74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28
							00a0	57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b
							00b0	20 57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 3a
							00c0	31 32 31 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31
							00d0	30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 32
							00e0	31 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78
							00f0	74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69
							0100	6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70
							0110	6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30
							0120	2e 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d
							0130	61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30
							0140	2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75
							0150	61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d
							0160	30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f
							0170	64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c
							0180	61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a
							0190	20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67
							01a0	72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65
							01b0	71 75 65 73 74 73 3a 20 31 0d 0a 0d 0a

Part-2

1. No, "IF-MODIFIED-SINCE" line in the first HTTP GET is not present.

http								
No.	Time	Source	Destination	Protocol	Length	Info		
736	17:00:12.841207	10.196.178.11	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1		
767	17:00:13.132948	128.119.245.12	10.196.178.11	HTTP	784	HTTP/1.1 200 OK (text/html)		
795	17:00:13.221933	10.196.178.11	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1		
1647	17:00:22.072938	10.196.178.11	128.119.245.12	HTTP	531	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1		
1661	17:00:22.351339	128.119.245.12	10.196.178.11	HTTP	294	HTTP/1.1 304 Not Modified		
> Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: ExtremeNetworks_9a:82:e8 (02:04:96... > Internet Protocol Version 4, Src: 10.196.178.11, Dst: 128.119.245.12 > Transmission Control Protocol, Src Port: 55775, Dst Port: 80, Seq: 1, Ack: 1, Len: 391 > Hypertext Transfer Protocol							0010	01 af 55 19 40 00 80 06
							0020	f5 0c d9 df 00 50 2e 1b
							0030	02 01 25 26 00 00 47 45
							0040	68 61 72 6b 2d 6c 61 62
							0050	69 72 65 73 68 61 72 6b
							0060	74 6d 6c 20 48 54 54 50
							0070	73 74 3a 20 67 61 69 61
							0080	73 2e 65 64 75 0d 0a 55
							0090	74 3a 20 4d 6f 7a 69 6c
							00a0	57 69 6e 64 6f 77 73 20
							00b0	20 57 69 6e 36 34 3b 20
							00c0	31 32 31 2e 30 29 20 47
							00d0	30 30 31 30 31 20 46 69
							00e0	31 2e 30 0d 0a 41 63 63
							00f0	74 2f 68 74 6d 6c 2c 61
							0100	6f 6e 2f 78 68 74 6d 6c
							0110	6c 69 63 61 74 69 6f 6e
							0120	2e 39 2c 69 6d 61 67 65
							0130	61 67 65 2f 77 65 62 70
							0140	2e 38 0d 0a 41 63 63 65
							0150	61 67 65 3a 20 65 6e 2d
							0160	30 2e 35 0d 0a 41 63 63
							0170	64 69 6e 67 3a 20 67 7a
							0180	61 74 65 0d 0a 43 6f 6e
							0190	20 6b 65 65 70 2d 61 6c
							01a0	72 61 64 65 2d 49 6e 73
							01b0	71 75 65 73 74 73 3a 20
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n] [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n] [Severity level: Chat] [Group: Sequence] Request Method: GET Request URI: /wireshark-labs/HTTP-wireshark-file2.html Request Version: HTTP/1.1 Host: gaia.cs.umass.edu\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n Accept-Encoding: gzip, deflate\r\n Connection: keep-alive\r\n Upgrade-Insecure-Requests: 1\r\n \r\n [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html] [HTTP request 1/1] [Response in frame: 767]								

2. The server explicitly returned the contents of the file. The "Line-based text data" field in the message represents the file content.

No.	Time	Source	Destination	Protocol	Length	Info
736	17:00:12.841207	10.196.178.11	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
767	17:00:13.132948	128.119.245.12	10.196.178.11	HTTP	784	HTTP/1.1 200 OK (text/html) Information
795	17:00:13.221933	10.196.178.11	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
1647	17:00:22.072938	10.196.178.11	128.119.245.12	HTTP	531	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1661	17:00:22.351339	128.119.245.12	10.196.178.11	HTTP	294	HTTP/1.1 304 Not Modified

Accept-Range: bytes\r\n	0160	63	74	69	6f
> Content-Length: 371\r\n	0170	65	0d	0a	43
Keep-Alive: timeout=5, max=100\r\n	0180	20	74	65	78
Connection: Keep-Alive\r\n	0190	73	65	74	3d
Content-Type: text/html; charset=UTF-8\r\n	01a0	74	6d	6c	3e
\r\n	01b0	74	69	6f	6e
[HTTP response 1/1]	01c0	77	20	79	6f
[Time since request: 0.291741000 seconds]	01d0	64	65	64	20
[Request in frame: 736]	01e0	32	2d	32	2e
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]	01f0	68	69	73	20
File Data: 371 bytes	0200	6d	6f	64	69
Line-based text data: text/html (10 lines)	0210	65	20	77	69
\n	0220	65	2e	20	20
<html>\n	0230	20	79	6f	75
\n	0240	69	73	20	6d
Congratulations again! Now you've downloaded the file lab2-2.html. \n	0250	73	20	6f	6e
This file's last modification date will not change. <p>\n	0260	72	2c	20	61
Thus if you download this multiple times on your browser, a complete copy \n	0270	70	79	20	3c
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE \n	0280	79	20	62	65
field in your browser's HTTP GET request to the server.\n	0290	79	20	74	68
\n	02a0	20	74	6f	20
</html>\n	02b0	6e	20	6f	66
	02c0	46	49	45	44
	02d0	69	65	6c	64
	02e0	77	73	65	72
	02f0	72	65	71	75
	0300	65	72	76	65

3. Yes, "IF-MODIFIED-SINCE" line in the second HTTP GET is present. The information followed by it is: Tue, 16 Jan 2024 06:59:02 GMT.

No.	Time	Source	Destination	Protocol	Length	Info
736	17:00:12.841207	10.196.178.11	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
767	17:00:13.132948	128.119.245.12	10.196.178.11	HTTP	784	HTTP/1.1 200 OK (text/html)
795	17:00:13.221933	10.196.178.11	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
1647	17:00:22.072938	10.196.178.11	128.119.245.12	HTTP	531	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1661	17:00:22.351339	128.119.245.12	10.196.178.11	HTTP	294	HTTP/1.1 304 Not Modified

> Transmission Control Protocol, Src Port: 55782, Dst Port: 80, Seq: 1, Ack: 1, Len: 477	0000	02	04	96	9a	82	e8	14	1:
> Hypertext Transfer Protocol	0010	02	05	55	28	40	00	80	0:
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n	0020	f5	0c	d9	e6	00	50	c4	d:
> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]	0030	02	01	d7	c2	00	00	47	4:
> [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]	0040	68	61	72	6b	2d	6c	61	6:
> [Severity level: Chat]	0050	69	72	65	73	68	61	72	6:
> [Group: Sequence]	0060	74	6d	6c	20	48	54	54	5:
> Request Method: GET	0070	73	74	3a	20	67	61	69	6:
> Request URI: /wireshark-labs/HTTP-wireshark-file2.html	0080	73	2e	65	64	75	0d	0a	5:
> Request Version: HTTP/1.1	0090	74	3a	20	4d	6f	7a	69	6:
> Host: gaia.cs.umass.edu\r\n	00a0	57	69	6e	64	6f	77	73	2:
> User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n	00b0	20	57	69	6e	36	34	3b	2:
> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n	00c0	31	32	31	2e	30	29	20	4:
> Accept-Language: en-US,en;q=0.5\r\n	00d0	30	30	31	30	31	20	46	6:
> Accept-Encoding: gzip, deflate\r\n	00e0	31	2e	30	0d	0a	41	63	6:
> Connection: keep-alive\r\n	00f0	74	2f	68	74	6d	6c	2c	6:
> Upgrade-Insecure-Requests: 1\r\n	0100	6f	6e	2f	78	68	74	6d	6:
> If-Modified-Since: Tue, 16 Jan 2024 06:59:02 GMT\r\n	0110	6c	69	63	61	74	69	6f	6:
> If-None-Match: "173-60f0aaa58b571"\r\n	0120	2e	39	2c	69	6d	61	67	6:
	0130	61	67	65	2f	77	65	62	7:
	0140	2e	38	0d	0a	41	63	63	6:
	0150	61	67	65	3a	20	65	6e	2:
	0160	30	2e	35	0d	0a	41	63	6:

The If-Modified-Since HTTP header indicates the time for which a browser first downloaded a resource from the server. When used in combination with the If-None-Match, it is ignored, unless the server does not support If-None-Match.

4. For the second HTTP GET,
Status code: 200

Response phrase: OK

The server didn't explicitly return the contents of the file. As the "Line-based text data" field is not present in the response. This may be due to:

Here the content is already in the browser's cache, the browser issued a conditional GET request, and the server responded with a "304 Not Modified" status instead of sending the full content.

Modern web browsers use HTTP persistent connections to improve performance. This means that a single TCP connection is reused for multiple requests, reducing the overhead of establishing new connections. The HTTP "Keep-Alive" header is used to request that the connection be kept open for additional requests. Here the connection between server and the browser is kept alive throughout, so we can say subsequent requests may be part of the same TCP connection.

http						
No.	Time	Source	Destination	Protocol	Length	Info
736	17:00:12.841207	10.196.178.11	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
767	17:00:13.132948	128.119.245.12	10.196.178.11	HTTP	784	HTTP/1.1 200 OK (text/html)
795	17:00:13.221933	10.196.178.11	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
1647	17:00:22.072938	10.196.178.11	128.119.245.12	HTTP	531	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1661	17:00:22.351339	128.119.245.12	10.196.178.11	HTTP	294	HTTP/1.1 304 Not Modified

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.196.178.11

> Transmission Control Protocol, Src Port: 80, Dst Port: 55782, Seq: 1, Ack: 478, Len: 240

> Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]

[HTTP/1.1 304 Not Modified\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 304

[Status Code Description: Not Modified]

Response Phrase: Not Modified

Date: Tue, 16 Jan 2024 11:30:22 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n

Connection: Keep-Alive\r\n

Keep-Alive: timeout=5, max=100\r\n

ETag: "173-60f0aaa58b571"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.278401000 seconds]

[Request in frame: 1647]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

0000 14 13 33 c7

0010 01 18 ef a2

0020 b2 0b 00 50

0030 00 ed 10 93

0040 30 34 20 4e

0050 0a 44 61 74

0060 61 6e 20 32

0070 20 47 4d 54

0080 61 63 68 65

0090 4f 53 29 20

00a0 32 6b 2d 66

00b0 33 33 20 6d

00c0 31 31 20 50

00d0 0a 43 6f 6e

00e0 70 2d 41 6c

00f0 69 76 65 3a

0100 6d 61 78 3d

0110 31 37 33 2d

0120 31 22 0d 0a

Part-3

http						
No.	Time	Source	Destination	Protocol	Length	Info
456	16:49:35.912388	10.240.128.176	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
464	16:49:36.152977	128.119.245.12	10.240.128.176	HTTP	1165	HTTP/1.1 200 OK (text/html)
478	16:49:36.202894	10.240.128.176	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
499	16:49:36.451318	128.119.245.12	10.240.128.176	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Transmission Control Protocol, Src Port: 80, Dst Port: 60321, Seq: 3751, Ack: 392, Len: 1111
 ✓ [4 Reassembled TCP Segments (4861 bytes): #460(1250), #461(1250), #462(1250), #464(1111)]
 [Frame: 460, payload: 0-1249 (1250 bytes)]
 [Frame: 461, payload: 1250-2499 (1250 bytes)]
 [Frame: 462, payload: 2500-3749 (1250 bytes)]
 [Frame: 464, payload: 3750-4860 (1111 bytes)]
 [Segment count: 4]
 [Reassembled TCP length: 4861]
 [Reassembled TCP Data [truncated]: 485454502f312e3120323030204f4b0d0a446174653a204672692c203139204a616e203230]

0030 20 47 4d 54
 0040 61 63 68 65
 0050 4f 53 29 20
 0060 32 6b 2d 66
 0070 33 33 20 6d
 0080 31 31 20 50
 0090 0a 4c 61 73
 00a0 46 72 69 2c
 00b0 20 30 36 3a
 00c0 54 61 67 3a
 00d0 30 33 64 38
 00e0 74 2d 52 61
 00f0 0a 43 6f 6e
 0100 20 34 35 30
 0110 65 3a 20 74
 0120 78 3d 31 30
 0130 6e 3a 20 4b
 0140 6f 6e 74 65
 0150 74 2f 68 74

✓ 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

1. 1 HTTP GET request message was sent by my browser. 456 packet number in the trace contains the GET message for the Bill of Rights.
2. The 464 packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request.
3. Status code: 200
Response phrase: OK
4. A total of 4 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

Part-4

1.

http						
No.	Time	Source	Destination	Protocol	Length	Info
65	16:08:27.285001	10.240.128.176	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
81	16:08:27.524235	128.119.245.12	10.240.128.176	HTTP	105	HTTP/1.1 200 OK (text/html)
98	16:08:27.578016	10.240.128.176	128.119.245.12	HTTP	402	GET /pearson.png HTTP/1.1
121	16:08:27.744554	10.240.128.176	178.79.137.164	HTTP	369	GET /8E_cover_small.jpg HTTP/1.1
135	16:08:27.779790	10.240.128.176	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
145	16:08:27.824702	128.119.245.12	10.240.128.176	HTTP	1166	HTTP/1.1 200 OK (PNG)
155	16:08:27.906548	178.79.137.164	10.240.128.176	HTTP	225	HTTP/1.1 301 Moved Permanently
159	16:08:28.016802	128.119.245.12	10.240.128.176	HTTP	539	HTTP/1.1 404 Not Found (text/html)

A total of 4(packet no: 65,98,121,135) GET messages(including GET message for favicon icon, else 3 GET messages) are sent from the browser. The requests are sent to the following Internet addresses:

[\[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\]](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html)
[\[HTTP request 1/1\]](#)
[\[Response in frame: 81\]](#)

[Full request URI: <http://gaia.cs.umass.edu/pearson.png>]
[HTTP request 1/1]
[Response in frame: 145]

[Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]
[HTTP request 1/1]
[Response in frame: 155]

[Full request URI: <http://gaia.cs.umass.edu/favicon.ico>]
[HTTP request 1/1]
[Response in frame: 159]

1st GET request sent to “<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>”

2nd GET request sent to “<http://gaia.cs.umass.edu/pearson.png>”

3rd GET request sent to “http://kurose.cslash.net/8E_cover_small.jpg”

4th GET request sent to “<http://gaia.cs.umass.edu/favicon.ico>”

2. The two images were downloaded from the two websites in parallel.

98	16:08:27.578016	10.240.128.176	128.119.245.12	HTTP	402 GET /pearson.png HTTP/1.1
121	16:08:27.744554	10.240.128.176	178.79.137.164	HTTP	369 GET /8E_cover_small.jpg HTTP/1.1
135	16:08:27.779790	10.240.128.176	128.119.245.12	HTTP	402 GET /favicon.ico HTTP/1.1
145	16:08:27.824702	128.119.245.12	10.240.128.176	HTTP	1166 HTTP/1.1 200 OK (PNG)
155	16:08:27.906548	178.79.137.164	10.240.128.176	HTTP	225 HTTP/1.1 301 Moved Permanently
159	16:08:28.016802	128.119.245.12	10.240.128.176	HTTP	539 HTTP/1.1 404 Not Found (text/html)

98	16:08:27.578016	10.240.128.176	128.119.245.12	HTTP	402 GET /pearson.png HTTP/1.1
121	16:08:27.744554	10.240.128.176	178.79.137.164	HTTP	369 GET /8E_cover_small.jpg HTTP/1.1
135	16:08:27.779790	10.240.128.176	128.119.245.12	HTTP	402 GET /favicon.ico HTTP/1.1
145	16:08:27.824702	128.119.245.12	10.240.128.176	HTTP	1166 HTTP/1.1 200 OK (PNG)
155	16:08:27.906548	178.79.137.164	10.240.128.176	HTTP	225 HTTP/1.1 301 Moved Permanently
159	16:08:28.016802	128.119.245.12	10.240.128.176	HTTP	539 HTTP/1.1 404 Not Found (text/html)

The GET requests for the two images having packet numbers 98 and 121 respectively are sent simultaneously before either of their responses(i.e. packet no: 145 and 155) are received. Therefore, we can say the images are fetched simultaneously.

Part-5

1. The server's response to the initial HTTP GET message from my browser is
Status Code: 401

No.	Time	Source	Destination	Protocol	Length	Info
615	17:32:44.791511	10.196.178.11	128.119.245.12	HTTP	461	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
665	17:32:45.073722	128.119.245.12	10.196.178.11	HTTP	271	HTTP/1.1 401 Unauthorized (text/html)
2696	17:32:57.054047	10.196.178.11	128.119.245.12	HTTP	520	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2717	17:32:57.347144	128.119.245.12	10.196.178.11	HTTP	544	HTTP/1.1 200 OK (text/html)
2745	17:32:57.435522	10.196.178.11	128.119.245.12	HTTP	418	GET /favicon.ico HTTP/1.1
2790	17:32:57.727676	128.119.245.12	10.196.178.11	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Hypertext Transfer Protocol		0020	b2 0b 00 50 dd 7e cd d9 3e
HTTP/1.1 401 Unauthorized\r\n		0030	00 ed 08 e0 00 00 48 54 5a
[Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]		0040	30 31 28 55 6e 61 75 74 68
[HTTP/1.1 401 Unauthorized\r\n]		0050	0a 44 61 74 65 3a 20 54 75
[Severity Level: Chat]		0060	61 6e 20 32 30 32 3a 20 31
[Group: Sequence]		0070	20 47 4d 54 0d 0a 53 65 72
Response Version: HTTP/1.1		0080	61 63 68 65 2f 32 2e 3a 2e
Status Code: 401		0090	4f 53 29 4f 70 65 6e 53
[Status Code Description: Unauthorized]		00a0	32 6b 2d 66 69 70 73 20 50
Response Phrase: Unauthorized		00b0	33 32 20 6d 6f 64 5f 70 65
Date: Tue, 16 Jan 2024 12:02:44 GMT\r\n		00c0	31 31 20 50 65 72 6c 2f 76
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		00d0	0a 57 57 2d 41 75 74 68
WWW-Authenticate: Basic realm="wireshark-students only"\r\n		00e0	65 3a 20 42 61 73 69 63 20
> Content-Length: 381\r\n		00f0	77 69 72 65 73 68 61 72 6d
Keep-Alive: timeout=5, max=100\r\n		0100	74 73 20 6f 6e 6c 79 20 0b
Connection: Keep-Alive\r\n		0110	74 2d 4c 65 6e 67 74 68 3a
Content-Type: text/html; charset=iso-8859-1\r\n		0120	65 65 70 2d 41 6c 69 67 65
\r\n		0130	75 74 3d 35 2c 20 6d 61 78
[HTTP response 1/1]		0140	6f 6e 6e 65 63 74 69 6f 6e
[Time since request: 0.282211000 seconds]		0150	41 6c 69 76 65 0d 0a 43 6f
[Request in frame: 615]		0160	79 70 65 3a 20 74 65 78 74
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]		0170	63 68 61 72 73 65 74 3d 69
		0180	2d 31 0d 0a 0d 0a 3c 21 44
		0190	48 54 4d 4c 20 50 55 42 4c
		01a0	49 45 54 4e 2f 2f 44 54 44
		01b0	2e 30 2f 2f 45 4e 22 3e 0a

No.	Time	Source	Destination	Protocol	Length	Info
615	17:32:44.791511	10.196.178.11	128.119.245.12	HTTP	461	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
665	17:32:45.073722	128.119.245.12	10.196.178.11	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
2696	17:32:57.054047	10.196.178.11	128.119.245.12	HTTP	520	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2717	17:32:57.347144	128.119.245.12	10.196.178.11	HTTP	544	HTTP/1.1 200 OK (text/html)
2745	17:32:57.435522	10.196.178.11	128.119.245.12	HTTP	418	GET /favicon.ico HTTP/1.1
2790	17:32:57.727676	128.119.245.12	10.196.178.11	HTTP	538	HTTP/1.1 404 Not Found (text/html)

>	Frame 2696: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{27A30D6E-F35B-4000-8000-000000000000}
>	Ethernet II, Src: AzureWaveTec_73e:39:14 (14:13:33:c7:3e:39), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
>	Internet Protocol Version 4, Src: 10.196.178.11, Dst: 128.119.245.12
>	Transmission Control Protocol, Src Port: 56707, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
>	Hypertext Transfer Protocol
>	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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:121.0) Gecko/20100101 Firefox/121.0\r\n
>	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
>	Accept-Language: en-US,en;q=0.5\r\n
>	Accept-Encoding: gzip, deflate\r\n
>	Connection: keep-alive\r\n
>	Upgrade-Insecure-Requests: 1\r\n
>	Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcmcs\r\n\r\n
>	[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
>	[HTTP request 1/2]
>	[Response in frame: 2717]
>	[Next request in frame: 2745]

1st GET message:

http						
No.	Time	Source	Destination	Protocol	Length	Info
615	17:32:44.791511	10.196.178.11	128.119.245.12	HTTP	461	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
665	17:32:45.073722	128.119.245.12	10.196.178.11	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
2696	17:32:57.054047	10.196.178.11	128.119.245.12	HTTP	520	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2717	17:32:57.347144	128.119.245.12	10.196.178.11	HTTP	544	HTTP/1.1 200 OK (text/html)
2745	17:32:57.435522	10.196.178.11	128.119.245.12	HTTP	418	GET /favicon.ico HTTP/1.1
2790	17:32:57.727676	128.119.245.12	10.196.178.11	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 615: 461 bytes on wire (3688 bits), 461 bytes captured (3688 bits) on interface \Device\NPF_{27A30D6E-F35B-46	0030	02 01 6f b0 00 00 47 45 54
> Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)	0040	68 61 72 6b 2d 6c 61 62 73
> Internet Protocol Version 4, Src: 10.196.178.11, Dst: 128.119.245.12	0050	74 65 64 5f 70 61 67 65 73
> Transmission Control Protocol, Src Port: 56702, Dst Port: 80, Seq: 1, Ack: 1, Len: 407	0060	69 72 65 73 68 61 72 6b 2d
> Hypertext Transfer Protocol	0070	74 6d 6c 20 48 54 54 50 2f
> GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n	0080	73 74 3a 20 67 61 69 61 2e
Host: gaia.cs.umass.edu\r\n	0090	73 2e 65 64 75 0d 0a 55 73
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n	00a0	74 3a 20 4d 6f 7a 69 6c 6c
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n	00b0	57 69 6e 64 6f 77 73 20 4e
Accept-Language: en-US,en;q=0.5\r\n	00c0	20 57 69 6e 36 34 3b 20 78
Accept-Encoding: gzip, deflate\r\n	00d0	31 32 31 2e 30 29 20 47 65
Connection: keep-alive\r\n	00e0	30 30 31 30 31 20 46 69 72
Upgrade-Insecure-Requests: 1\r\n	00f0	31 2e 30 0d 0a 41 63 63 65
\r\n	0100	74 2f 68 74 6d 6c 2c 61 70
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]	0110	6f 6e 2f 78 68 74 6d 6c 2b
[HTTP request 1/1]	0120	6c 69 63 61 74 69 6f 6e 2f
[Response in frame: 665]	0130	2e 39 2c 69 6d 61 67 65 2f
	0140	61 67 65 2f 77 65 62 70 2c
	0150	2e 38 0d 0a 41 63 63 65 70
	0160	61 67 65 3a 20 65 6e 2d 55
	0170	30 2e 35 0d 0a 41 63 63 65