

CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-3
Wireshark Lab: HTTP
January 26, 2025

Part-1: The Basic HTTP GET/response interaction

Answer the following questions based on the information you observed when tracing the above HTTP requests and responses.

Enter these links on your browser one after another:

- <http://httpforever.com/>
- <http://web.simmons.edu/>
- <http://www.vulnweb.com/>
- <http://www.testingmcafesites.com/>

1. What type of HTTP version do you observe in the above trace?

Time	No.	Source	Destination	Protocol	Length Info
19.937221146	284	10.240.118.79	146.190.62.39	HTTP	486 GET / HTTP/1.1
20.190278127	303	146.190.62.39	10.240.118.79	HTTP	2806 HTTP/1.1 200 OK (text/html)
20.288157007	314	10.240.118.79	146.190.62.39	HTTP	372 GET /js/init.min.js HTTP/1.1
20.223263572	320	10.240.118.79	23.58.26.110	HTTP	310 GET / HTTP/1.1
20.241642037	332	23.58.26.110	10.240.118.79	HTTP	1830 HTTP/1.1 200 OK (application/pkix-cert)
20.348671717	399	10.240.118.79	23.47.251.246	HTTP	310 GET / HTTP/1.1
20.367354588	401	23.47.251.246	10.240.118.79	HTTP	1731 HTTP/1.1 200 OK (application/pkix-cert)
20.462881972	407	146.190.62.39	10.240.118.79	HTTP	1896 HTTP/1.1 200 OK (application/javascript)
20.471893364	409	10.240.118.79	146.190.62.39	HTTP	390 GET /css/style.min.css HTTP/1.1
20.976623859	422	146.190.62.39	10.240.118.79	HTTP	1372 HTTP/1.1 200 OK (text/css)
21.127428090	488	10.240.118.79	146.190.62.39	HTTP	457 GET /css/images/banner.svg HTTP/1.1
21.353786003	688	10.240.118.79	146.190.62.39	HTTP	430 GET /favicon.ico HTTP/1.1
21.358583823	691	10.240.118.79	146.190.62.39	HTTP	472 GET /css/images/header-major-on-light.svg HTTP/1.1
21.376977702	692	146.190.62.39	10.240.118.79	HTTP/X..	1377 HTTP/1.1 200 OK

The HTTP version observed in the trace is **HTTP/1.1**. This can be deduced from the snippet: GET / HTTP/1.1, where the HTTP/1.1 explicitly states the version of the HTTP protocol being used for this request.

2. Mention the HTTP request method used to request these four websites.

Time	No.	Source	Destination	Protocol	Length Info
19.937221146	284	10.240.118.79	146.190.62.39	HTTP	486 GET / HTTP/1.1
20.288157007	314	10.240.118.79	146.190.62.39	HTTP	372 GET /js/init.min.js HTTP/1.1
20.471893364	409	10.240.118.79	146.190.62.39	HTTP	390 GET /css/style.min.css HTTP/1.1
21.127428090	488	10.240.118.79	146.190.62.39	HTTP	457 GET /css/images/banner.svg HTTP/1.1
21.353786003	688	10.240.118.79	146.190.62.39	HTTP	430 GET /favicon.ico HTTP/1.1
21.358583823	691	10.240.118.79	146.190.62.39	HTTP	472 GET /css/images/header-major-on-light.svg HTTP/1.1
21.376977702	694	10.240.118.79	146.190.62.39	HTTP	471 GET /css/images/header-major-on-dark.svg HTTP/1.1


```

Internet Protocol Version 4, Src: 10.240.118.79, Dst: 146.190.62.39
Transmission Control Protocol, Src Port: 40698, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
HyperText Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: httpforever.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en;q=0.9\r\n
  \r\n
[Response in frame #03]
[Full request URL: http://httpforever.com/]

```

0110 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 .-Accept
0120 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f tm,appl
0130 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 xhtml+xm
0140 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c ation/xm
0150 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 image/av
0160 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 /webp,im
0170 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 78 6c 69 ,/*";q=0
0180 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 cation/s
0190 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e change:v
01a0 37 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 7..-Accp
01b0 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 e..-Accp
01c0 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 ng: gzip
01d0 67 85 3a 2b 65 6e 2d 47 42 2c 65 6e 3b 71 3d 30 ge: en-G
01e0 2e 39 0d 0a 0d 0a .9...

In the provided trace (GET / HTTP/1.1), the HTTP request method is **GET** for <http://httpforever.com/>.

http.request.method && http.host==web.simmons.edu						
Time	No.	Source	Destination	Protocol	Length	Info
+ 50.773194771	1502	10.240.118.79	69.43.111.82	HTTP	486	GET / HTTP/1.1
51.047857225	1508	10.240.118.79	69.43.111.82	HTTP	430	GET /favicon.ico HTTP/1.1

```

Internet Protocol Version 4, Src: 10.240.118.79, Dst: 69.43.111.82
Transmission Control Protocol, Src Port: 44936, Dst Port: 80, Seq: 1, Ack: 1, Len: 1502
Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: web.simmons.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en;q=0.9\r\n
  \r\n
  [Response in frame: 1506]
  [Full request URL: http://web.simmons.edu/]

```

```

0110 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68  .-Accept
0120 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f tml,appl
0130 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 xhtml+xm
0140 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c ation+xm
0150 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 image/av
0160 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 /webp,im
0170 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 /*";j=@
0180 63 61 74 69 6f 6e 2f 73 69 67 66 65 64 2d 65 78 cation/s
0190 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e change;v
01a0 37 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 7- Accep
01b0 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 ng: gzip
01c0 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 e- Accep
01d0 67 65 3a 20 65 6e 2d 47 42 2c 65 6e 3b 71 3d 30 ge: en-G
01e0 2e 39 0d 0a 0d 0a .9.....

```

In the provided trace (GET / HTTP/1.1), the HTTP request method is **GET** for **http://web.simmons.edu/**.

http.request.method && http.host==www.vulnweb.com						
Time	No.	Source	Destination	Protocol	Length	Info
+ 73.598188376	1691	10.240.118.79	44.228.249.3	HTTP	486	GET / HTTP/1.1
73.890068994	1698	10.240.118.79	44.228.249.3	HTTP	436	GET /acunetix-logo.png HTTP/1.1
73.894128890	1699	10.240.118.79	44.228.249.3	HTTP	382	GET /style.css HTTP/1.1
74.214249163	1717	10.240.118.79	44.228.249.3	HTTP	430	GET /favicon.ico HTTP/1.1

http.request.method && http.host==www.vulnweb.com						
Time	No.	Source	Destination	Protocol	Length	Info
+ 73.598188376	1691	10.240.118.79	44.228.249.3	HTTP	486	GET / HTTP/1.1
73.890068994	1698	10.240.118.79	44.228.249.3	HTTP	436	GET /acunetix-logo.png HTTP/1.1
73.894128890	1699	10.240.118.79	44.228.249.3	HTTP	382	GET /style.css HTTP/1.1
74.214249163	1717	10.240.118.79	44.228.249.3	HTTP	430	GET /favicon.ico HTTP/1.1

```

Internet Protocol Version 4, Src: 10.240.118.79, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 55294, Dst Port: 80, Seq: 1, Ack: 1, Len: 1691
Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en;q=0.9\r\n
  \r\n
  [Response in frame: 1698]
  [Full request URL: http://www.vulnweb.com/]

```

```

0110 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68  .-Accept
0120 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f tml,appl
0130 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 xhtml+xm
0140 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c ation+xm
0150 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 image/av
0160 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 /webp,im
0170 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 /*";j=@
0180 63 61 74 69 6f 6e 2f 73 69 67 66 65 64 2d 65 78 cation/s
0190 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e change;v
01a0 37 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 7- Accep
01b0 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 ng: gzip
01c0 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 e- Accep
01d0 67 65 3a 20 65 6e 2d 47 42 2c 65 6e 3b 71 3d 30 ge: en-G
01e0 2e 39 0d 0a 0d 0a .9.....

```

In the provided trace (GET / HTTP/1.1), the HTTP request method is **GET** for **http://www.vulnweb.com/**.

http.request.method && http.host==www.testingmcafesites.com						
Time	No.	Source	Destination	Protocol	Length	Info
+ 96.491077614	2076	10.240.118.79	34.218.221.118	HTTP	497	GET / HTTP/1.1
96.812155556	2087	10.240.118.79	34.218.221.118	HTTP	452	GET /favicon.ico HTTP/1.1

http.request.method && http.host==www.testingmcafesites.com						
Time	No.	Source	Destination	Protocol	Length	Info
+ 96.491077614	2076	10.240.118.79	34.218.221.118	HTTP	497	GET / HTTP/1.1
96.812155556	2087	10.240.118.79	34.218.221.118	HTTP	452	GET /favicon.ico HTTP/1.1

```

Internet Protocol Version 4, Src: 10.240.118.79, Dst: 34.218.221.118
Transmission Control Protocol, Src Port: 55254, Dst Port: 80, Seq: 1, Ack: 1, Len: 2076
Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.testingmcafesites.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en;q=0.9\r\n
  \r\n
  [Response in frame: 2085]
  [Full request URL: http://www.testingmcafesites.com/]

```

```

0110 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61  ept: tex
0120 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c  applicati
0130 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e +xml,app
0140 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 /xml;q=0
0150 62 71 66 69 62 6c 69 6d 61 67 65 2f 77 62 70 67 ,/avif,im
0160 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 62 70 67 /avif,im
0170 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b ,image/a
0180 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f q=0.8,ap
0190 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 n/signed
01a0 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41 63 e;vb3;q
01b0 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Enc
01c0 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 zip,def
01d0 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 65 cept-Lan
01e0 6e 2d 47 42 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 0d n-GB,en;
01f0 0a .

```

In the provided trace (GET / HTTP/1.1), the HTTP request method is **GET** for **http://www.testingmcafesites.com/**.

3. What are the status codes returned by the server to the browser?

Time	No.	Source	Destination	Protocol	Length Info
20.190278127	303	146.190.62.39	10.240.118.79	HTTP	2806 HTTP/1.1 200 OK (text/html)
20.241642037	332	23.58.26.110	10.240.118.79	HTTP	1830 HTTP/1.1 200 OK (application/pkix-cert)
20.367354588	491	23.47.251.246	10.240.118.79	HTTP	1731 HTTP/1.1 200 OK (application/pkix-cert)
20.462881972	497	146.190.62.39	10.240.118.79	HTTP	1896 HTTP/1.1 200 OK (application/javascript)
20.976623859	422	146.190.62.39	10.240.118.79	HTTP	1372 HTTP/1.1 200 OK (text/css)
21.376977702	692	146.190.62.39	10.240.118.79	HTTP/X..	1377 HTTP/1.1 200 OK
21.581301290	699	146.190.62.39	10.240.118.79	HTTP/X..	1327 HTTP/1.1 200 OK
21.591830353	704	146.190.62.39	10.240.118.79	HTTP/X..	1333 HTTP/1.1 200 OK
21.633274281	706	146.190.62.39	10.240.118.79	HTTP/X..	2267 HTTP/1.1 200 OK (image/x-icon)
34.148201552	883	34.104.35.123	10.240.118.79	HTTP	685 HTTP/1.1 200 OK
34.425011231	916	34.104.35.123	10.240.118.79	HTTP	541 HTTP/1.1 200 OK
34.713047907	963	34.104.35.123	10.240.118.79	HTTP	2519 HTTP/1.1 200 OK
35.012301980	1059	34.104.35.123	10.240.118.79	HTTP	971 HTTP/1.1 200 OK
35.687826489	1090	34.104.35.123	10.240.118.79	HTTP	2928 HTTP/1.1 200 OK

```

Referer-Policy: strict-origin-when-cross-origin\r\n
X-Content-Type-Options: nosniff\r\n
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroso
[...]Content-Security-Policy: default-src 'self'; script-src cdnjs.cloudflare.com
Content-Encoding: gzip\r\n
\r\n
[Request in frame: 284]
[Time since request: 0.253056981 seconds]
[Request URI: /]
[Full request URL: http://httpforever.com/]

```

In the provided trace (HTTP/1.1 200 OK) for <http://httpforever.com/>, the status codes returned by the server to the browser is **200 OK** signifies that the server successfully processed the request and returned the requested resource.

Time	No.	Source	Destination	Protocol	Length Info
35.012301980	1059	34.104.35.123	10.240.118.79	HTTP	971 HTTP/1.1 200 OK
35.687826489	1090	34.104.35.123	10.240.118.79	HTTP	2828 HTTP/1.1 200 OK
+ 51.015927297	1506	69.43.111.82	10.240.118.79	HTTP	762 HTTP/1.1 200 OK (text/html)
51.289933366	1509	69.43.111.82	10.240.118.79	HTTP	462 HTTP/1.1 404 Not Found (text/html)
65.183112201	1620	185.125.190.96	10.240.118.79	HTTP	251 HTTP/1.1 204 No Content
73.879236612	1696	44.228.249.3	10.240.118.79	HTTP	1691 HTTP/1.1 200 OK (text/html)
74.166808990	1709	44.228.249.3	10.240.118.79	HTTP	1272 HTTP/1.1 200 OK (text/css)
74.494926117	1720	44.228.249.3	10.240.118.79	HTTP	1044 HTTP/1.1 404 Not Found (text/html)
74.494926117	1720	44.228.249.3	10.240.118.79	HTTP	440 HTTP/1.1 404 Not Found (text/html)
96.782272523	2085	34.218.221.118	10.240.118.79	HTTP	2846 HTTP/1.1 200 OK (text/html)
97.101740563	2090	34.218.221.118	10.240.118.79	HTTP	1622 HTTP/1.1 404 Not Found (text/html)
104.482099068	2410	202.144.79.6	10.240.118.79	OCSP	955 Response
104.484612307	2413	202.144.79.6	10.240.118.79	OCSP	955 Response

```

Last-Modified: Wed, 06 Mar 2024 15:36:23 GMT\r\n
ETag: "19c-612ffb89b8b71"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 412\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[Request in frame: 282]
[Time since request: 0.24273256 seconds]
[Request URI: /]
[Full request URL: http://web.simmons.edu/]
File Data: 412 bytes

```

In the provided trace (HTTP/1.1 200 OK) for <http://web.simmons.edu/>, the status codes returned by the server to the browser is **200 OK** signifies that the server successfully processed the request and returned the requested resource.

Time	No.	Source	Destination	Protocol	Length Info
35.012301980	1059	34.104.35.123	10.240.118.79	HTTP	971 HTTP/1.1 200 OK
35.687826489	1090	34.104.35.123	10.240.118.79	HTTP	2028 HTTP/1.1 200 OK
+ 51.015927297	1506	69.43.111.82	10.240.118.79	HTTP	762 HTTP/1.1 200 OK (text/html)
51.289933366	1509	69.43.111.82	10.240.118.79	HTTP	462 HTTP/1.1 404 Not Found (text/html)
65.183112201	1620	185.125.190.96	10.240.118.79	HTTP	251 HTTP/1.1 204 No Content
+ 73.879236612	1696	44.228.249.3	10.240.118.79	HTTP	1691 HTTP/1.1 200 OK (text/html)
74.166808990	1709	44.228.249.3	10.240.118.79	HTTP	1272 HTTP/1.1 200 OK (text/css)
74.170622267	1715	44.228.249.3	10.240.118.79	HTTP	1644 HTTP/1.1 200 OK (PNG)
74.494926117	1720	44.228.249.3	10.240.118.79	HTTP	440 HTTP/1.1 404 Not Found (text/html)
96.782272523	2085	34.218.221.118	10.240.118.79	HTTP	2846 HTTP/1.1 200 OK (text/html)
97.101740563	2090	34.218.221.118	10.240.118.79	HTTP	1622 HTTP/1.1 404 Not Found (text/html)
104.482099068	2410	202.144.79.6	10.240.118.79	OCSP	955 Response
104.484612307	2413	202.144.79.6	10.240.118.79	OCSP	955 Response

```

Content-Type: text/html\r\n
Last-Modified: Tue, 28 Jul 2020 09:20:49 GMT\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
ETag: W/"5f1fedf1-fb2"\r\n
Content-Encoding: gzip\r\n
\r\n
[Request in frame: 1691]
[Time since request: 0.281048236 seconds]
[Request URI: /]
[Full request URL: http://www.vulnweb.com/]
HTTP chunked response

```

In the provided trace (HTTP/1.1 200 OK) for <http://www.vulnweb.com/>, the status codes returned by the server to the browser is **200 OK** signifies that the server successfully processed the request and returned the requested resource.

http.response.code						
Time	No.	Source	Destination	Protocol	Length	Info
35. 012301988	1059	34. 104. 35. 123	10. 240. 118. 79	HTTP	971	HTTP/1.1 200 OK
35. 687826489	1090	34. 104. 35. 123	10. 240. 118. 79	HTTP	2028	HTTP/1.1 200 OK
51. 015927297	1508	69. 43. 111. 82	10. 240. 118. 79	HTTP	762	HTTP/1.1 200 OK (text/html)
51. 289933366	1509	69. 43. 111. 82	10. 240. 118. 79	HTTP	462	HTTP/1.1 404 Not Found (text/html)
65. 103112206	1620	185. 125. 190. 96	10. 240. 118. 79	HTTP	251	HTTP/1.1 204 No Content
73. 879236612	1696	44. 228. 249. 3	10. 240. 118. 79	HTTP	1691	HTTP/1.1 200 OK (text/html)
74. 166880999	1708	44. 228. 249. 3	10. 240. 118. 79	HTTP	1272	HTTP/1.1 200 OK (text/css)
74. 170622267	1715	44. 228. 249. 3	10. 240. 118. 79	HTTP	1644	HTTP/1.1 200 OK (PNG)
74. 494926117	1720	44. 228. 249. 3	10. 240. 118. 79	HTTP	440	HTTP/1.1 404 Not Found (text/html)
96. 78227253	2085	34. 218. 221. 118	10. 240. 118. 79	HTTP	2846	HTTP/1.1 200 OK (text/html)
97. 161740563	2090	34. 218. 221. 118	10. 240. 118. 79	HTTP	1622	HTTP/1.1 404 Not Found (text/html)
104. 482099068	2410	202. 144. 79. 6	10. 240. 118. 79	OCSP	955	Response
104. 484612307	2413	202. 144. 79. 6	10. 240. 118. 79	OCSP	955	Response

In the provided trace (HTTP/1.1 200 OK) for <http://www.testingmcafesites.com/>, the status codes returned by the server to the browser is **200 OK** signifies that the server successfully processed the request and returned the requested resource.

4. List the number of HTTP GET requests and frame number for “<http://httpforever.com/>” request.

http.request.method == "GET" && http.host == "httpforever.com"						
Time	No.	Source	Destination	Protocol	Length	Info
19. 037221146	284	10. 240. 118. 79	146. 190. 62. 39	HTTP	486	GET / HTTP/1.1
20. 208157087	314	10. 240. 118. 79	146. 190. 62. 39	HTTP	372	GET /js/init.min.js HTTP/1.1
20. 471893364	409	10. 240. 118. 79	146. 190. 62. 39	HTTP	390	GET /css/style.min.css HTTP/1.1
21. 127428090	488	10. 240. 118. 79	146. 190. 62. 39	HTTP	457	GET /css/images/banner.svg HTTP/1.1
21. 353786003	688	10. 240. 118. 79	146. 190. 62. 39	HTTP	438	GET /favicon.ico HTTP/1.1
21. 358583823	691	10. 240. 118. 79	146. 190. 62. 39	HTTP	472	GET /css/images/header-major-on-light.svg HTTP/1.1
21. 378472265	694	10. 240. 118. 79	146. 190. 62. 39	HTTP	471	GET /css/images/header-major-on-dark.svg HTTP/1.1

Frame 284: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits) on interface: Ethernet II, Src: HP_0a:79:2c (e0:73:e7:0a:79:2c), Dst: Cisco 13:e0:82 (bc:d2:95:1:2:1)						
Internet Protocol Version 4, Src: 10.240.118.79, Dst: 146.190.62.39						
Transmission Control Protocol, Src Port: 40698, Dst Port: 80, Seq: 1, Ack: 1, Len: 486						
<pre>> Hypertext Transfer Protocol > GET / HTTP/1.1\r\n Host: httpforever.com\r\n Connection: keep-alive\r\n Upgrade-Insecure-Requests: 1\r\n User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w Accept-Encoding: gzip, deflate\r\n Accept-Language: en-GB,en;q=0.9\r\n \r\n</pre>						

- Number of HTTP GET Requests: There are 7 GET requests to <http://httpforever.com/>.
- Frame Numbers for Each Request: Frame 284, Frame 314, Frame 409, Frame 488, Frame 688, Frame 691 and Frame 694.

5. What languages does your browser indicate that it can accept to the server?

http.request						
Time	No.	Source	Destination	Protocol	Length	Info
18. 479574168	256	10. 240. 118. 97	239. 255. 255. 250	SSDP	215	M-SEARCH * HTTP/1.1
19. 576492654	263	10. 240. 118. 99	239. 255. 255. 250	SSDP	215	M-SEARCH * HTTP/1.1
19. 037221146	284	10. 240. 118. 79	146. 190. 62. 39	HTTP	486	GET / HTTP/1.1
20. 208157087	314	10. 240. 118. 79	146. 190. 62. 39	HTTP	372	GET /js/init.min.js HTTP/1.1
20. 471893364	409	10. 240. 118. 79	146. 190. 62. 39	HTTP	390	GET /css/style.min.css HTTP/1.1
21. 127428090	488	10. 240. 118. 79	146. 190. 62. 39	HTTP	457	GET /css/images/banner.svg HTTP/1.1
21. 348671717	688	10. 240. 118. 79	146. 190. 62. 39	HTTP	438	GET /favicon.ico HTTP/1.1
21. 353786003	691	10. 240. 118. 79	146. 190. 62. 39	HTTP	472	GET /css/images/header-major-on-light.svg HTTP/1.1
21. 378472265	694	10. 240. 118. 79	146. 190. 62. 39	HTTP	471	GET /css/images/header-major-on-dark.svg HTTP/1.1
21. 387422223	698	10. 240. 118. 97	239. 255. 255. 250	SSDP	215	M-SEARCH * HTTP/1.1
21. 387422223	698	10. 240. 118. 99	239. 255. 255. 250	SSDP	215	M-SEARCH * HTTP/1.1
21. 387422223	700	10. 240. 118. 97	239. 255. 255. 250	SSDP	215	M-SEARCH * HTTP/1.1
21. 387422223	700	10. 240. 118. 99	239. 255. 255. 250	SSDP	215	M-SEARCH * HTTP/1.1
<pre>> Hypertext Transfer Protocol, Src Port: 40698, Dst Port: 80, Seq: 1, Ack: 1, Len: 486 > GET / HTTP/1.1\r\n Host: httpforever.com\r\n Connection: keep-alive\r\n Upgrade-Insecure-Requests: 1\r\n User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w Accept-Encoding: gzip, deflate\r\n Accept-Language: en-GB,en;q=0.9\r\n \r\n</pre>						

Accept-Language: en-GB,en;q=0.9\r\n

6. List the source and the destination IP address details for all the above HTTP requests.

Using question 2 images of 4 websites we can fill this-

Domain	Source IP	Destination IP
http://httpforever.com/	10.240.118.79	146.190.62.39
http://web.simmons.edu/	10.240.118.79	69.43.111.82
http://www.vulnweb.com/	10.240.118.79	44.228.249.3
http://www.testingmcafesites.com/	10.240.118.79	34.218.221.118

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, the raw data displayed in the packet content window corresponds exactly to what is shown in the packet-listing window. There are no additional headers visible in the packet content window that are not already displayed in the packet-listing window.

8. For each url requested, provide the number of bytes returned by the server corresponding to the first HTTP GET request.

The screenshot shows the NetworkMiner tool interface. The packet list pane shows several HTTP requests from 10.240.118.79 to 146.190.62.39. The details pane shows the first request (HTTP/1.1 200 OK) with its raw content. The content pane displays the raw HTTP response, which includes the header 'Content-Encoding: gzip' and the compressed content itself. The status bar at the bottom indicates 'Line-based text data: text/html (100 lines)'.

```

http.response && ip.addr==146.190.62.39
Time No. Source Destination Protocol Length Info
+-- 20.190278127 303 146.190.62.39 10.240.118.79 HTTP 2806 HTTP/1.1 200 OK (text/html)
20.462881972 407 146.190.62.39 10.240.118.79 HTTP 1896 HTTP/1.1 200 OK (application/javascript)
20.976623859 422 146.190.62.39 10.240.118.79 HTTP 1372 HTTP/1.1 200 OK (text/css)
21.376977782 692 146.190.62.39 10.240.118.79 HTTP/X... 1377 HTTP/1.1 200 OK
21.581301290 699 146.190.62.39 10.240.118.79 HTTP 2267 HTTP/1.1 200 OK (image/x-icon)
21.591830353 704 146.190.62.39 10.240.118.79 HTTP/X... 1327 HTTP/1.1 200 OK

HTTP/1.1 200 OK\r\n
Server: nginx/1.18.0 (Ubuntu)\r\n
Date: Mon, 20 Jan 2025 03:34:27 GMT\r\n
Content-Type: text/html\r\n
Last-Modified: Wed, 22 Mar 2023 14:54:48 GMT\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
ETag: W/"641b16b8-1404"\r\n
Referer-Policy: strict-origin-when-cross-origin\r\n
X-Content-Type-Options: nosniff\r\n
Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyrosc...
Content-Security-Policy: default-src 'self'; script-src cdnjs.cloudflare.com
Content-Encoding: gzip\r\n
\r\n
[Request in frame: 28a]
[Time since request: 0.253056981 seconds]
[Request URI: /]
[Full request URI: http://httpforever.com/]
HTTP chunked response
Content-encoded entity body (gzip): 1910 bytes -> 5124 bytes
File Data: 5124 bytes
Line-based text data: text/html (100 lines)

```

for <http://httpforever.com/> , number of bytes returned by the server corresponding to the first HTTP GET request 1910 bytes, which is the size of the compressed content (gzip).This is the amount of data transmitted over the network in response to the HTTP GET request. The decompressed size (5124 bytes) represents the expanded size of the content after it is processed

by the client, but it is not what the server physically transmitted. Therefore, the correct value to consider for the server's response is 1910 bytes.

```

http.response && ip.addr==69.43.111.82
Time          No.    Source           Destination        Protocol Length Info
+ 51.015927297   1506  69.43.111.82      10.240.118.79    HTTP     762 HTTP/1.1 200 OK (text/html)
| 51.289933366   1509  69.43.111.82      10.240.118.79    HTTP     462 HTTP/1.1 404 Not Found (text/html)

[+] 1506 69.43.111.82
HTTP/1.1 200 OK
Date: Mon, 20 Jan 2025 03:34:58 GMT
Server: Apache
Last-Modified: Wed, 06 Mar 2024 15:36:23 GMT
ETag: "19c-612ff89b8b71"
Accept-Ranges: bytes
Content-Length: 412
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
[Request in frame: 1502]
[Time since request: 0.242732526 seconds]
[Request URI: /]
[Full request URL: http://web.simmons.edu/]
File Data: 412 bytes
Line-based text data: text/html (9 lines)

[+] 1509 69.43.111.82
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=UTF-8
Content-Length: 462
[Request in frame: 1503]
[Time since request: 0.000000000 seconds]
[Request URI: /]
[Full request URL: http://web.simmons.edu/]
File Data: 462 bytes
Line-based text data: text/html (1 lines)

```

for <http://web.simmons.edu/>, number of bytes returned by the server corresponding to the first HTTP GET request = 412 bytes.

```

http.response && ip.addr==44.228.249.3
Time          No.    Source           Destination        Protocol Length Info
+ 73.879236612   1696  44.228.249.3      10.240.118.79    HTTP     1691 HTTP/1.1 200 OK (text/html)
| 74.166808990   1709  44.228.249.3      10.240.118.79    HTTP     1272 HTTP/1.1 200 OK (text/css)
| 74.170622267   1715  44.228.249.3      10.240.118.79    HTTP     1644 HTTP/1.1 200 OK (PNG)
| 74.494926117   1720  44.228.249.3      10.240.118.79    HTTP     440 HTTP/1.1 404 Not Found (text/html)

[+] 1696 44.228.249.3
HTTP/1.1 200 OK
Date: Mon, 20 Jan 2025 03:35:20 GMT
Content-Type: text/html
Last-Modified: Tue, 28 Jul 2020 09:20:49 GMT
Transfer-Encoding: chunked
Connection: keep-alive
ETag: W/"5f5fedf1-fb2"
Content-Encoding: gzip
[Request in frame: 1691]
[Time since request: 0.281048236 seconds]
[Request URI: /]
[Full request URL: http://www.vulnweb.com/]
HTTP chunked response
Content-encoded entity body (gzip): 1364 bytes -> 4018 bytes
File Data: 4018 bytes
Line-based text data: text/html (73 lines)

[+] 1709 44.228.249.3
HTTP/1.1 200 OK
Content-Type: text/css
Last-Modified: Fri, 20 Jan 2025 03:35:20 GMT
Content-Encoding: gzip
[Request in frame: 1709]
[Time since request: 0.000000000 seconds]
[Request URI: /]
[Full request URL: http://www.vulnweb.com/]
File Data: 1272 bytes
Line-based text data: text/css (1 lines)

[+] 1715 44.228.249.3
HTTP/1.1 200 OK
Content-Type: image/png
Last-Modified: Fri, 20 Jan 2025 03:35:20 GMT
Content-Encoding: gzip
[Request in frame: 1715]
[Time since request: 0.000000000 seconds]
[Request URI: /]
[Full request URL: http://www.vulnweb.com/]
File Data: 1644 bytes
Line-based text data: image/png (1 lines)

[+] 1720 44.228.249.3
HTTP/1.1 404 Not Found
Content-Type: text/html
Content-Length: 440
[Request in frame: 1720]
[Time since request: 0.000000000 seconds]
[Request URI: /]
[Full request URL: http://www.vulnweb.com/]
File Data: 440 bytes
Line-based text data: text/html (1 lines)

```

for <http://www.vulnweb.com/>, number of bytes returned by the server corresponding to the first HTTP GET request 1364 bytes, which is the size of the compressed content (gzip). This is the amount of data transmitted over the network in response to the HTTP GET request. The decompressed size (4018 bytes) represents the expanded size of the content after it is processed by the client, but it is not what the server physically transmitted. Therefore, the correct value to consider for the server's response is 1364 bytes.

http.response && ip.addr==34.218.221.118

Time	No.	Source	Destination	Protocol	Length Info
+ 96.782272523	2085	34.218.221.118	10.240.118.79	HTTP	2846 HTTP/1.1 200 OK (text/html)
97.101740563	2090	34.218.221.118	10.240.118.79	HTTP	1622 HTTP/1.1 404 Not Found (text/html)

```

Date: Mon, 20 Jan 2025 03:35:43 GMT\r\n
Content-Type: text/html\r\n
Content-Length: 2335\r\n
Connection: keep-alive\r\n
Cache-Control: private, no-store, no-cache, must-revalidate\r\n
Content-Encoding: gzip\r\n
Last-Modified: Fri, 08 Apr 2022 16:54:52 GMT\r\n
Accept-Ranges: bytes\r\n
ETag: "0d6835d694bd81:0"\r\n
Vary: Accept-Encoding\r\n
Server: Microsoft-IIS/10.0\r\n
Server-Timing: intid;desc=48508d0b2f20b315\r\n
X-Powered-By: ASP.NET\r\n
SN: EC2AMAZ-BSL60N\r\n
\r\n
[Request in frame: 2076]
[Time since request: 0.291194909 seconds]
[Request URI: /]
[Full request URL: http://www.testingmcafesites.com/]
Content-encoded entity body (gzip): 2335 bytes -> 28634 bytes
File Data: 28634 bytes
Line-based text data: text/html (368 lines)

```

for <http://www.testingmcafesites.com/>, number of bytes returned by the server corresponding to the first HTTP GET request 2335 bytes, which is the size of the compressed content (gzip). This is the amount of data transmitted over the network in response to the HTTP GET request. The decompressed size (28634 bytes) represents the expanded size of the content after it is processed by the client, but it is not what the server physically transmitted. Therefore, the correct value to consider for the server's response is 2335 bytes.

9. Obtain the number of lines of data and the content being received by your browser for the above first HTTP GET requests.

http.response && ip.addr==146.190.62.39

Time	No.	Source	Destination	Protocol	Length Info
+ 20.190278127	303	146.190.62.39	10.240.118.79	HTTP	2806 HTTP/1.1 200 OK (text/html)
20.462881972	487	146.190.62.39	10.240.118.79	HTTP	1896 HTTP/1.1 200 OK (application/javascript)
20.976623859	422	146.190.62.39	10.240.118.79	HTTP	1372 HTTP/1.1 200 OK (text/css)
21.376977702	692	146.190.62.39	10.240.118.79	HTTP/X...	1377 HTTP/1.1 200 OK
21.581301290	699	146.190.62.39	10.240.118.79	HTTP	2267 HTTP/1.1 200 OK (image/x-icon)
21.591830353	704	146.190.62.39	10.240.118.79	HTTP/X...	1327 HTTP/1.1 200 OK

```

HTTP chunked response
Content-encoded entity body (gzip): 1910 bytes -> 5124 bytes
File Data: 5124 bytes
Line-based text data: text/html (100 lines)
<!DOCTYPE HTML>\r\n<html>\r\n
```

for <http://httpforever.com/>, number of lines of data and the content being received by your browser for the above first HTTP GET requests= 100 lines.

http.response && ip.addr==69.43.111.82

Time	No.	Source	Destination	Protocol	Length Info
+ 51.015927297	1506	69.43.111.82	10.240.118.79	HTTP	762 HTTP/1.1 200 OK (text/html)
51.2899333366	1509	69.43.111.82	10.240.118.79	HTTP	462 HTTP/1.1 404 Not Found (text/html)

```

ETag: "19c-612ffb89b8b71"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 412\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[Request in frame: 1502]
[Time since request: 0.242732526 seconds]
[Request URI: /]
[Full request URL: http://web.simmons.edu/]
File Data: 412 bytes
Line-based text data: text/html (9 lines)
<!DOCTYPE html>\n<html lang="en">\n
```

for <http://web.simmons.edu/>, number of lines of data and the content being received by your browser for the above first HTTP GET requests= 9 lines.

Time	No.	Source	Destination	Protocol	Length Info
+ 73.879236612	1696	44.228.249.3	10.240.118.79	HTTP	1691 HTTP/1.1 200 OK (text/html)
74.166880890	1709	44.228.249.3	10.240.118.79	HTTP	1272 HTTP/1.1 200 OK (text/css)
74.170622267	1715	44.228.249.3	10.240.118.79	HTTP	1644 HTTP/1.1 200 OK (PNG)
74.494926117	1720	44.228.249.3	10.240.118.79	HTTP	440 HTTP/1.1 404 Not Found (text/html)

```
* Line-based text data: text/html (73 lines)
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/1999/xhtml">\n
```

for <http://www.vulnweb.com/>, number of lines of data and the content being received by your browser for the above first HTTP GET requests= 73 lines.

Time	No.	Source	Destination	Protocol	Length Info
+ 96.782272523	2085	34.218.221.118	10.240.118.79	HTTP	2846 HTTP/1.1 200 OK (text/html)
97.101740563	2090	34.218.221.118	10.240.118.79	HTTP	1622 HTTP/1.1 404 Not Found (text/html)

```
* Line-based text data: text/html (368 lines)
\r\n
<html>\r\n
```

for <http://www.testingmcafesites.com/>, number of lines of data and the content being received by your browser for the above first HTTP GET requests= 368 lines.

Part 2: The HTTP CONDITIONAL GET/response interaction

- Enter the following URL into your browser
<http://gaia.cs.umass.edu/wiresharklabs/HTTP-wireshark-file2.html> Your browser should display a very simple five-line HTML file.

Answer the following questions:

- 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?

Time	No.	Source	Destination	Protocol	Length Info
+ 5.534653947	854	10.240.118.79	128.119.245.12	HTTP	439 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
31.997613109	1281	10.240.118.79	128.119.245.12	HTTP	525 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

```
* Transmission Control Protocol, Src Port: 45916, Dst Port: 80, Seq: 1, Ack: 1, Len: 439
* 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 (X11; Ubuntu; Linux x86_64; rv:134.0) Gecko/20100101 Firefox/134.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u0, i0\r\n
  \r\n
  [Response in frame: 923]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

The “IF-MODIFIED-SINCE” line is not seen inside Hypertext Transfer Protocol, for the first HTTP GET request, indicating the browser has no cached copy yet.

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

For the first HTTP GET request, the server explicitly returned the file contents because the response had a **200 OK** status and included the file's text data. This confirms the file was sent by the server.

Time	No.	Source	Destination	Protocol	Length Info
+ 5.790490342	923	128.119.245.12	10.240.118.79	HTTP	784 HTTP/1.1 200 OK (text/html)
+ 32.271361158	1286	128.119.245.12	10.240.118.79	HTTP	294 HTTP/1.1 304 Not Modified

```

> HTTP/1.1 200 OK\r\n
Date: Mon, 20 Jan 2025 04:42:58 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Per
Last-Modified: Sun, 19 Jan 2025 06:59:01 GMT\r\n
ETag: "173-62c09adbeff9f3"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[Request in frame: 854]
[Time since request: 0.255836395 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. </p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SIN
field in your browser's HTTP GET request to the server.\n

```

- 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?

Time	No.	Source	Destination	Protocol	Length Info
5.534653947	854	10.240.118.79	128.119.245.12	HTTP	439 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
+ 31.997613109	1281	10.240.118.79	128.119.245.12	HTTP	525 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

```

> Frame 1281: 525 bytes on wire (4200 bits), 525 bytes captured (4200 bits) on interface
> Ethernet II, Src: HP_0a:79:2c (e0:73:e7:0a:79:2c), Dst: Cisco_13:e0:82 (bc:d2:95:13)
> Internet Protocol Version 4, Src: 10.240.118.79, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 48524, Dst Port: 80, Seq: 1, Ack: 1, Len: 4
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 (X11; Ubuntu; Linux x86_64; rv:134.0) Gecko/20100101 Firefox/134.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Sun, 19 Jan 2025 06:59:01 GMT\r\n
If-None-Match: "173-62c09adbeff9f3"\r\n
Priority: u=0, i\r\n
\r\n
[Response in frame: 1286]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

In the second HTTP GET request, the **IF-MODIFIED-SINCE** header is present inside Hypertext Transfer Protocol, indicating the timestamp when the resource was last downloaded by the browser. This header helps the server determine whether the resource has changed since the specified time.

```
http.response && ip.addr == 128.119.245.12
Time No. Source Destination Protocol Length Info
5.790490342 923 128.119.245.12 10.240.118.79 HTTP 784 HTTP/1.1 200 OK (text/html)
32.271361158 1286 128.119.245.12 10.240.118.79 HTTP 294 HTTP/1.1 304 Not Modified

Frame 1286: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface
Ethernet II, Src: Cisco_13:0e:82 (bc:d2:95:13:0e:82), Dst: HP_0a:79:2c (e0:73:e7:0a:0f:00)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.240.118.79
Transmission Control Protocol, Src Port: 80, Dst Port: 48524, Seq: 1, Ack: 472, Len: 294
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Mon, 20 Jan 2025 04:43:24 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/5.34
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "173-62c09adbef9f"\r\n
  \r\n
[Request in frame: 1281]
[Time since request: 0.273748049 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
[Full request URI: http://gaiac.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.htm
0000 e0 73 e7 0a 79 2c bc d2 95 13 e0 82 08 00 45 28 s y, .
0010 01 18 46 ce 40 00 2e 06 0e 27 80 77 f5 0c 0a f0 ..F@ . .
0020 76 4f 00 50 bd 8c 53 b2 d4 67 f2 de 3d bb 50 18 VO P S .
0030 00 ed 87 bc 00 00 48 54 54 50 2f 31 2e 31 20 33 ....HT T
0040 30 34 20 4e 6f 24 20 4d 6f 64 69 66 69 65 64 0d 04 Not M o
0050 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 32 30 20 4a Date: M o
0060 61 2e 20 32 30 32 35 20 30 34 3a 34 33 3a 32 34 an 2025 0d
0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT- Se r
0080 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 ace/2.4 .6
0090 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open S
00a0 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 3e 24 2k-fips
00b0 33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 33 mod_p e
00c0 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 11 Perl/ v
00d0 0a 43 6f 6e 66 65 63 74 69 6f 6e 3a 20 4b 65 65 Connect i
00e0 70 2d 41 6c 69 76 65 0d 0a 4b 65 65 70 2d 41 6c p-Alive i
00f0 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 28 live: tim e
0100 6d 61 78 3d 31 30 3d 0d 0a 45 54 61 67 3a 20 22 max=100
0110 31 37 33 2d 36 32 63 30 39 61 64 62 65 66 39 66 173-62c09
0120 33 22 0d 0a 0d 0a 3" . .
```

If the resource is unchanged, the server responds with a **304 Not Modified** status, signaling the browser to use the cached version without downloading it again. This mechanism improves performance by reducing unnecessary data transfer and saving bandwidth. The **IF-MODIFIED-SINCE** header typically appears when refreshing or reentering a URL.

4. 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.

From above image, the HTTP status code for the **second GET response** is **304**, and the phrase is **Not Modified**. The server did not explicitly return the file contents, as this status indicates the resource has not changed since the client last requested it. Instead, the browser uses the cached version of the resource. This mechanism reduces bandwidth usage and improves performance by avoiding redundant downloads.

Part 3: Retrieving Long Documents

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

```
http.request.method==GET
Time           No.    Source          Destination       Protocol Length Info
2.811170367   24 10.240.118.79  34.107.221.82   HTTP     367 GET /canonical.html HTTP/1.1
2.876229333   44 10.240.118.79  34.107.221.82   HTTP     384 GET /success.txt?ipv4 HTTP/1.1
3.253714053   579 10.240.118.79  34.107.221.82   HTTP     384 GET /success.txt?ipv4 HTTP/1.1
+ 4.939673873  745 10.240.118.79  128.119.245.12  HTTP     439 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
| 5.265248129  779 10.240.118.79  128.119.245.12  HTTP     459 GET /favicon.ico HTTP/1.1

Ethernet II, Src: HP_0a:79:2c (e0:73:e7:0a:79:2c), Dst: Cisco_13:e0:82 (bc:d2:95:1:0)
Internet Protocol Version 4, Src: 10.240.118.79, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52424, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:134.0) Gecko/20100101 Firefox/134.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i=\r\n
\r\n[Response in frame: 769]
[Full request URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
```

My browser sent **5** GET request messages and **745th** packet contains the GET request for the Bill of Rights.

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

Time	No.	Source	Destination	Protocol	Length Info
+ 5.222284523	769	128.119.245.12	10.240.118.79	HTTP	4915 HTTP/1.1 200 OK (text/html)
5.490499540	787	128.119.245.12	10.240.118.79	HTTP	539 HTTP/1.1 404 Not Found (text/html)


```

Date: Mon, 20 Jan 2025 04:53:46 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Per
Last-Modified: Sun, 19 Jan 2025 06:59:01 GMT\r\n
ETag: "1194-62c0adbec342"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 4500\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[Request in frame: 745]
[Time since request: 0.282610650 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file3.html]
[Full request URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
[File Data: 4500 bytes]
> Line-based text data: text/html (98 lines)

```

769th packet contains the status code and phrase associated with the response to the HTTP GET request which is **200 OK**.

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

The status code is **200** and the phrase is **OK**.

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

Time	No.	Source	Destination	Protocol	Length Info
+ 5.222284523	769	128.119.245.12	10.240.118.79	HTTP	4915 HTTP/1.1 200 OK (text/html)
5.490499540	787	128.119.245.12	10.240.118.79	HTTP	539 HTTP/1.1 404 Not Found (text/html)


```

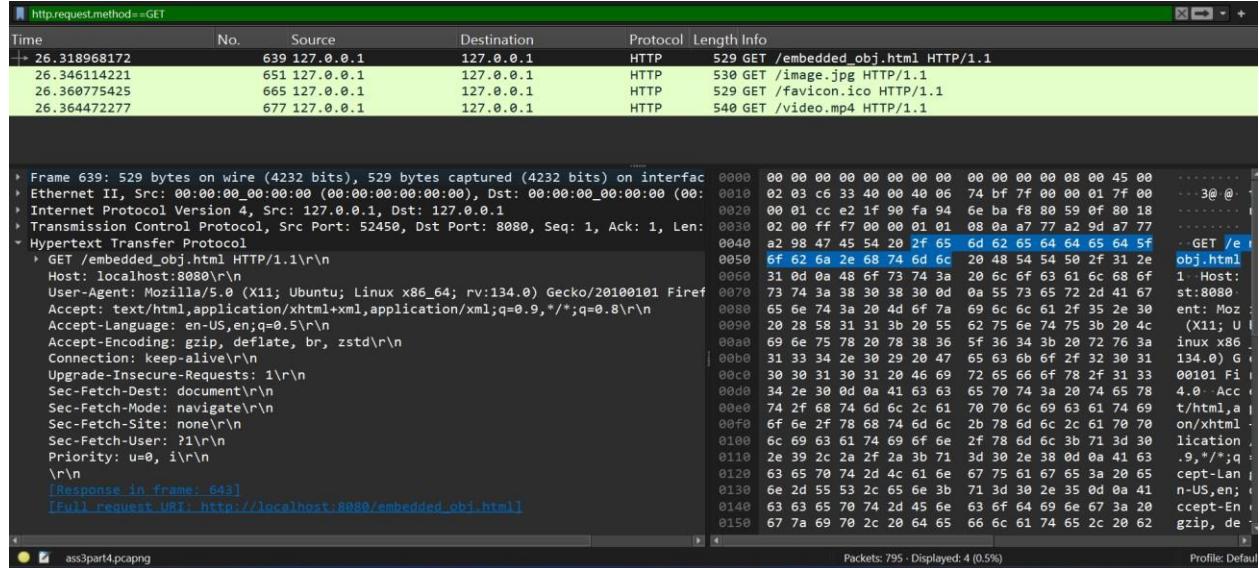
Transmission Control Protocol, Src Port: 80, Dst Port: 52424, Seq: 1, Ack: 386, Len: 4500
Source Port: 80
Destination Port: 52424
[Stream index: 23]
> [Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 4861]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2082262253
[Next Sequence Number: 4862 (relative sequence number)]
Acknowledgment Number: 386 (relative ack number)
Acknowledgment number (raw): 2668777007
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 237
[Calculated window size: 30336]
[Window size scaling factor: 128]
Checksum: 0x09db [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (4861 bytes)

```

TCP payload is **4861 bytes** and one data containing TCP segment was needed to carry the single HTTP response and the text of the Bill of Rights.

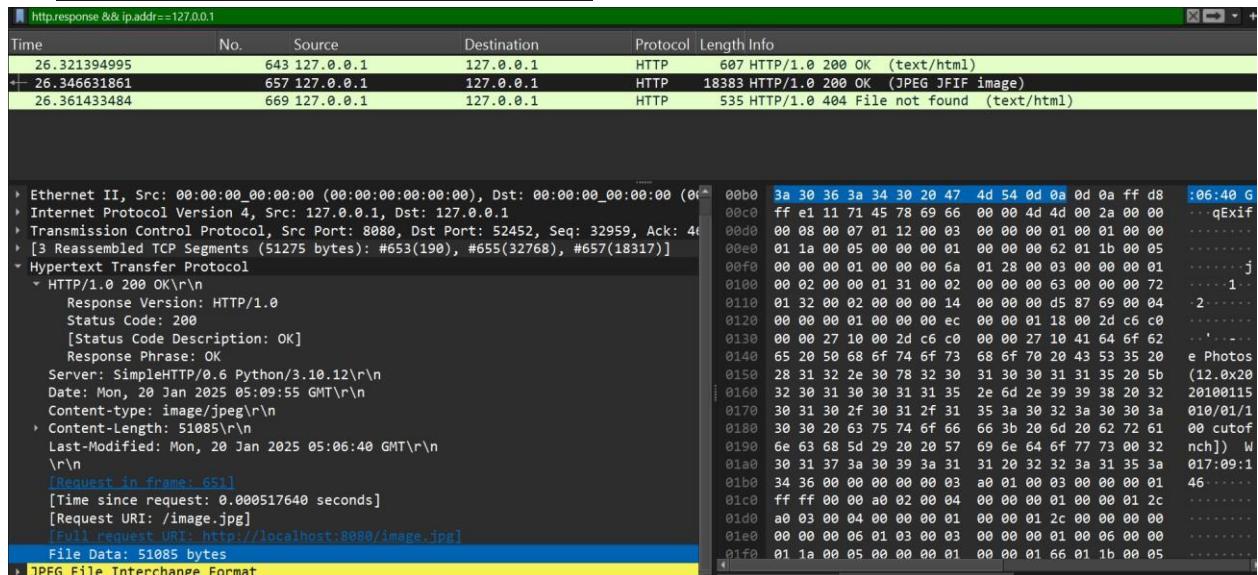
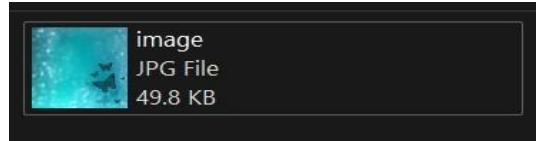
Part-4: HTML Documents with Embedded Objects

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



Browser sent 4 HTTP GET request messages. These GET requests are sent to the Internet address **127.0.0.1**

2. Is the size of the image file matching with the size of the file in the Wireshark? Provide the image file size in bytes.



The size of the image file we downloaded is of 49.8 KB which is of 50995.2 bytes whereas the size of the file in wireshark is 51085 bytes. Therefore, both are not matching.

3. Were there any HTTP response codes indicating errors (e.g., 4xx or 5xx)? If so, what do they indicate?

Time	No.	Source	Destination	Protocol	Length Info
26.3121394995	643	127.0.0.1	127.0.0.1	HTTP	607 HTTP/1.0 200 OK (text/html)
26.346631861	657	127.0.0.1	127.0.0.1	HTTP	18383 HTTP/1.0 200 OK (JPEG/JFIF image)
+ 26.361433484	669	127.0.0.1	127.0.0.1	HTTP	535 HTTP/1.0 404 File not found (text/html)

```

> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8080, Dst Port: 52458, Seq: 187, Ack: 464
[2 Reassembled TCP Segments (655 bytes): #667(186), #669(469)]
Hypertext Transfer Protocol
  - HTTP/1.0 404 File not found\r\n
    Response Version: HTTP/1.0
    Status Code: 404
    [Status Code Description: Not Found]
    Response Phrase: File not found
    Server: SimpleHTTP/0.6 Python/3.10.12\r\n
    Date: Mon, 20 Jan 2025 05:09:55 GMT\r\n
    Connection: close\r\n
    Content-Type: text/html; charset=utf-8\r\n
  Content-Length: 469\r\n
\r\n
[Request in frame: 665]
[Time since request: 0.000658059 seconds]
[Request URI: /favicon.ico]
[Full request URL: http://localhost:8080/favicon.ico]
File Data: 469 bytes
Line-based text data: text/html (14 lines)
  
```

Reassembled TCP (655 bytes)

Yes, there was an HTTP response code **404** with the phrase **File Not Found**. This indicates that the server could not find the requested resource. It typically occurs when the URL is incorrect, the resource has been moved or deleted, or there is a restriction on accessing the resource. The 404 code means the server was unable to locate the file or page, often due to issues with the request's path or the server configuration.

4. Mention the source and destination IP addresses for the HTTP requests made to the image and video files. Explain.

When hosting a local server and accessing resources via <http://localhost>, the communication happens on the loopback interface (lo).

Time	No.	Source	Destination	Protocol	Length Info
26.318968172	639	127.0.0.1	127.0.0.1	HTTP	529 GET /embedded_obj.html HTTP/1.1
26.321394995	643	127.0.0.1	127.0.0.1	HTTP	607 HTTP/1.0 200 OK (text/html)
+ 26.346114221	651	127.0.0.1	127.0.0.1	HTTP	530 GET /image.jpg HTTP/1.1
26.346631861	657	127.0.0.1	127.0.0.1	HTTP	18383 HTTP/1.0 200 OK (JPEG/JFIF image)
26.360775425	665	127.0.0.1	127.0.0.1	HTTP	529 GET /favicon.ico HTTP/1.1
26.361433484	669	127.0.0.1	127.0.0.1	HTTP	535 HTTP/1.0 404 File not found (text/html)
26.364472277	677	127.0.0.1	127.0.0.1	HTTP	540 GET /video.mp4 HTTP/1.1

For each HTTP request made for the HTML, image, and video files, the IP addresses are:

- Source IP: **127.0.0.1** (the local machine initiating the request).
- Destination IP: **127.0.0.1** (the server on the same machine).

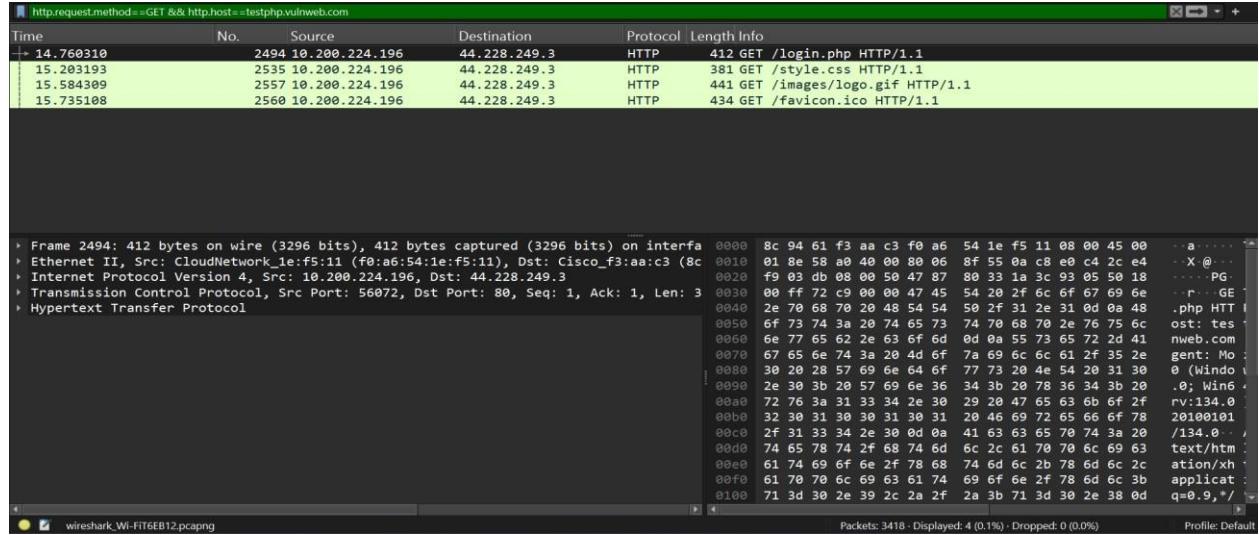
This is because the loopback interface is used for local communication, which doesn't require external network traffic.

Part-5: HTTP Authentication

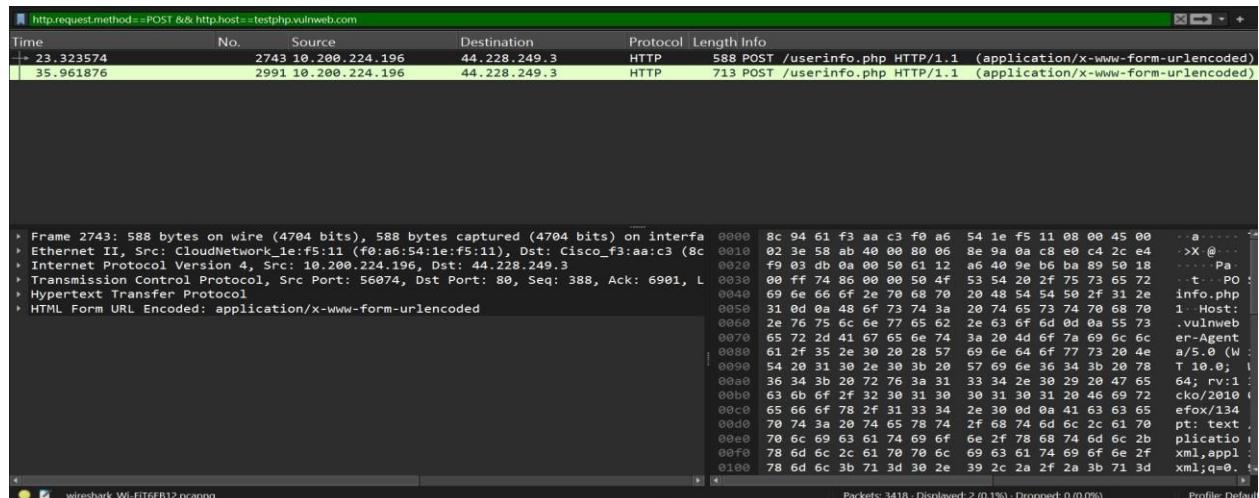
Do the following:

- Open the browser and paste the URL: <http://testphp.vulnweb.com/login.php>
- Add the username and password as “test” and click on the “login” button
- Change any one of the field's values of any of the information presented on the screen and click on the “update” button

1. How many GET and POST packets do you observe in the trace?



The number of GET packets is 4.



The number of POST packets is 2.

2. Write the domain and the corresponding IP address that you visited.

The domain **testphp.vulnweb.com** resolves to the IP address **44.228.249.3**.

3. What is the web server's destination port you have requested, and is it a standard port? If yes, then which protocol?

Time	No.	Source	Destination	Protocol	Length Info
14.760310	2494	10.200.224.196	44.228.249.3	HTTP	412 GET /login.php HTTP/1.1
15.203193	2535	10.200.224.196	44.228.249.3	HTTP	381 GET /style.css HTTP/1.1
15.584389	2557	10.200.224.196	44.228.249.3	HTTP	441 GET /images/logo.gif HTTP/1.1
15.735188	2560	10.200.224.196	44.228.249.3	HTTP	434 GET /favicon.ico HTTP/1.1
23.323574	2743	10.200.224.196	44.228.249.3	HTTP	588 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
35.961876	2991	10.200.224.196	44.228.249.3	HTTP	713 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

Frame 2494: 412 bytes on wire (3296 bits), 412 bytes captured (3296 bits) on interface
Ethernet II, Src: CloudNetwork_1e:f5:11 (00:0e:65:54:1e:f5:11), Dst: Cisco_F3:aa:c3 (8c:00:01:8e:58:a0)
Internet Protocol Version 4, Src: 10.200.224.196, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 56072, Dst Port: 80, Seq: 1, Ack: 1, Len: 3
Hypertext Transfer Protocol

0000 8c 94 61 f3 aa c3 f0 a6 54 1e f5 11 08 00 45 00 ...a...
0010 01 8e 58 a0 40 00 80 06 8f 55 0a c8 e0 c4 2c e4 ...X@...
0020 f9 03 db 0a 00 50 61 12 a6 40 9e b6 ba 89 50 18 ...PG
0030 00 ff 72 c9 00 00 47 45 54 20 2f 6c 6f 67 69 6e ...r...GE
0040 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 .php HTT
0050 6f 73 74 3a 20 74 65 73 74 70 68 70 2e 76 75 6c est: tes

The web server's destination port is **port 80**, which is a standard port for **HTTP (Hypertext Transfer Protocol)**.

- **Port 80** is the default port used by web servers to handle HTTP requests, meaning all regular web traffic is routed through this port unless specified otherwise.
- If no port is explicitly mentioned in the URL, the browser automatically assumes **port 80** for HTTP requests.
- This is the standard, unencrypted protocol used for most web browsing, in contrast to HTTPS, which operates on **port 443** for encrypted communication.

4. Inspect the contents of the first HTTP POST request sent from your browser to the server. Do you notice an If-Modified-Since line in the HTTP POST request? If so, what is its significance?

Time	No.	Source	Destination	Protocol	Length Info
23.323574	2743	10.200.224.196	44.228.249.3	HTTP	588 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
35.961876	2991	10.200.224.196	44.228.249.3	HTTP	713 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

Internet Protocol Version 4, Src: 10.200.224.196, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 56074, Dst Port: 80, Seq: 388, Ack: 6901, Hypertext Transfer Protocol
POST /userinfo.php HTTP/1.1\r\nHost: testphp.vulnweb.com\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 F Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nContent-Type: application/x-www-form-urlencoded\r\nContent-Length: 20\r\nOrigin: http://testphp.vulnweb.com\r\nConnection: keep-alive\r\nReferer: http://testphp.vulnweb.com/login.php\r\nUpgrade-Insecure-Requests: 1\r\nPriority: u=0, i\r\n\r\n

0000 8c 94 61 f3 aa c3 f0 a6 54 1e f5 11 08 00 45 00 ...a...
0010 02 3e 58 ab 40 00 80 06 8e 9a 0a c8 e0 c4 2c e4 ...X@...
0020 f9 03 db 0a 00 50 61 12 a6 40 9e b6 ba 89 50 18 ...PG
0030 00 ff 72 c9 00 00 47 45 53 54 20 2f 75 73 65 72 ...r...GE
0040 69 6e 66 6f 2e 70 68 70 28 48 54 54 50 2f 31 2e .info.php
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 1- Host:
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 55 73 .vulnweb
0070 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent
0080 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W
0090 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; i
00a0 36 34 3b 20 72 76 3a 31 33 34 2e 30 20 47 65 64; rv:1
00b0 63 6b 6f 2f 32 30 31 30 30 31 30 20 46 69 72 cko/2010
00c0 65 66 6f 78 2f 31 33 34 2e 30 0d 0a 41 63 63 65 efox/134
00d0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2e 61 70 pt: text
00e0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio
00f0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml.appl
0100 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d xml;q=0.!

The **If-Modified-Since** line is not present in the first HTTP POST request because POST requests are used to send data to the server, not for validating cached resources like GET requests.

5. Now inspect the contents of the second HTTP POST request from your browser to the server. What information follows the “IF-MODIFIED-SINCE:” header?

http.request.method==POST && http.host==testphp.vulnweb.com						
Time	No.	Source	Destination	Protocol	Length Info	
23.323574	2743	10.200.224.196	44.228.249.3	HTTP	588 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)	
+ 35.961876	2991	10.200.224.196	44.228.249.3	HTTP	713 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)	

```

> Transmission Control Protocol, Src Port: 56074, Dst Port: 80, Seq: 922, Ack: 9826,
+ Hypertext Transfer Protocol
  > POST /userinfo.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 F
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  > Content-Length: 114\r\n
  Origin: http://testphp.vulnweb.com\r\n
  Connection: keep-alive\r\n
  Referer: http://testphp.vulnweb.com/userinfo.php\r\n
  > Cookie: login=test2ftest\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i\r\n
  \r\n

```

```

0000 8c 94 61 f3 aa c3 f0 a6 54 1e f5 11 08 00 45 00  a ...
0010 02 bb 5b b1 40 00 80 06 8e 17 0a c8 e0 c4 2c e4  .X @ ...
0020 f9 03 db 0a 00 50 61 12 a8 56 9e b6 c5 f6 50 18  ...Pa ...
0030 00 ff 2a da 00 00 50 4f 53 54 20 2f 75 73 65 72  ...*... PO ...
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70  1- Host:
0060 2e 76 75 6e 66 77 65 62 2e 63 6f 6d 0d 0a 55 73  .vulnweb
0070 65 72 2d 41 67 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent
0080 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W
0090 54 28 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; I
00a0 36 34 3b 20 72 76 3a 31 33 34 2e 30 29 20 47 65 64; rv:1
00b0 63 6b 6f 2f 32 30 31 30 30 31 30 21 20 46 69 72 cko/2010
00c0 65 66 6f 78 2f 31 33 34 2e 30 0d 0a 41 63 63 65 efox/134
00d0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: text
00e0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio
00f0 78 6d 6c 2c 61 70 70 6e 69 63 61 74 69 6f 6e 2f xml,appl
0100 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d xml;q=0.5

```

In the second HTTP POST request, the **IF-MODIFIED-SINCE:** line is not present. This is because **POST requests** are used to send data to the server (such as form submissions or file uploads) rather than retrieve or validate cached resources. The **IF-MODIFIED-SINCE:** line is relevant for **GET requests** to check if the resource has changed, while POST requests focus on submitting new data, making the caching validation unnecessary.

6. Trace the HTTP communication when accessing the authentication server for the website <http://testphp.vulnweb.com/login.php>. Analyze the following:

- a. Request Details: What information (e.g., username and password) is included in the HTTP request when you attempt to log in?

http.request.method && http.host==testphp.vulnweb.com						
Time	No.	Source	Destination	Protocol	Length Info	
14.760310	2494	10.200.224.196	44.228.249.3	HTTP	412 GET /login.php HTTP/1.1	
15.203193	2535	10.200.224.196	44.228.249.3	HTTP	381 GET /style.css HTTP/1.1	
15.584309	2557	10.200.224.196	44.228.249.3	HTTP	441 GET /images/logo.gif HTTP/1.1	
15.735108	2560	10.200.224.196	44.228.249.3	HTTP	434 GET /favicon.ico HTTP/1.1	
+ 23.323574	2743	10.200.224.196	44.228.249.3	HTTP	588 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)	
+ 35.961876	2991	10.200.224.196	44.228.249.3	HTTP	713 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)	

```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
  > Content-Length: 20\r\n
  Origin: http://testphp.vulnweb.com\r\n
  Connection: keep-alive\r\n
  Referer: http://testphp.vulnweb.com/login.php\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i\r\n
  \r\n
[Response in frame: 2748]
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
File Data: 20 bytes
  > HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "uname" = "test"
    > Form item: "pass" = "test"

```

```

0000 8c 94 61 f3 aa c3 f0 a6 54 1e f5 11 08 00 45 00  a ...
0010 02 3e 58 ab 40 00 80 06 8e 9a 0a c8 e0 c4 2c e4  .X @ ...
0020 f9 03 db 0a 00 50 61 12 a6 40 9e b6 ba 89 50 18  ...Pa ...
0030 00 ff 2a da 00 00 50 4f 53 54 20 2f 75 73 65 72  ...*... PO ...
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70  1- Host:
0060 2e 76 75 6e 66 77 65 62 2e 63 6f 6d 0d 0a 55 73  .vulnweb
0070 65 72 2d 41 67 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent
0080 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W
0090 54 28 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; I
00a0 36 34 3b 20 72 76 3a 31 33 34 2e 30 29 20 47 65 64; rv:1
00b0 63 6b 6f 2f 32 30 31 30 31 30 21 20 46 69 72 cko/2010
00c0 65 66 6f 78 2f 31 33 34 2e 30 0d 0a 41 63 63 65 efox/134
00d0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: text
00e0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio
00f0 78 6d 6c 2c 61 70 70 6e 69 63 61 74 69 6f 6e 2f xml,appl
0100 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d xml;q=0.5

```

From the HTTP POST request for <http://testphp.vulnweb.com/login.php> inside Hypertext Transfer Protocol we can get the information of username and password entered during login, sent as form data in the request body (here, `username=test &password=test`).

b. Response Behavior: After submitting the login details, does the server respond with a new webpage? If so, what information is displayed on this page?

```

Time          No.  Source           Destination         Protocol Length Info
1 1.129576   2517 44.228.249.3  10.200.224.196   HTTP    302 HTTP/1.1 200 OK (text/html)
2 15.583269  2555 44.228.249.3  10.200.224.196   HTTP    536 HTTP/1.1 200 OK (text/css)
3 15.951726  2571 44.228.249.3  10.200.224.196   HTTP    464 HTTP/1.1 200 OK (GIF89a)
4 16.104139  2588 44.228.249.3  10.200.224.196   HTTP    948 HTTP/1.1 200 OK (image/x-icon)
5 23.698852  2748 44.228.249.3  10.200.224.196   HTTP    479 HTTP/1.1 200 OK (text/html)
6 37.591778  3023 44.228.249.3  10.200.224.196   HTTP    454 HTTP/1.1 200 OK (text/html)

```

The captured traffic shows the following sequence:

- Packet 1: GET /index.php?username=justin&password=123456789000 HTTP/1.1 from 10.200.224.196 to 44.228.249.3.
- Packet 2: 302 Found response with Location: /login.php.
- Packet 3: CSS file (text/css) returned by the server.
- Packet 4: GIF89a image returned by the server.
- Packet 5: HTML response (text/html) containing the user input "Name: justin".
- Packet 6: HTML response (text/html) containing the user input "Name: justin".

After submitting the login details, the server responds with a new webpage that contains user-specific information. This information is displayed as part of the HTML content returned in response to the first **GET** request following a successful login. From, the content we get the information displayed on the page which may include details like the Name, Credit card number, E-Mail, Phone number, Address.

7. Update information

a. Request Packet: Which packet in the HTTP trace contains the updated information you entered, and can you observe this information in the request?

Time	No.	Source	Destination	Protocol	Length	Info
14.760310	2494	10.200.224.196	44.228.249.3	HTTP	412	GET /login.php HTTP/1.1
15.203193	2535	10.200.224.196	44.228.249.3	HTTP	381	GET /style.css HTTP/1.1
15.584309	2557	10.200.224.196	44.228.249.3	HTTP	441	GET /images/logo.gif HTTP/1.1
15.735108	2560	10.200.224.196	44.228.249.3	HTTP	434	GET /favicon.ico HTTP/1.1
23.323574	2743	10.200.224.196	44.228.249.3	HTTP	588	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
35.961876	2991	10.200.224.196	44.228.249.3	HTTP	713	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

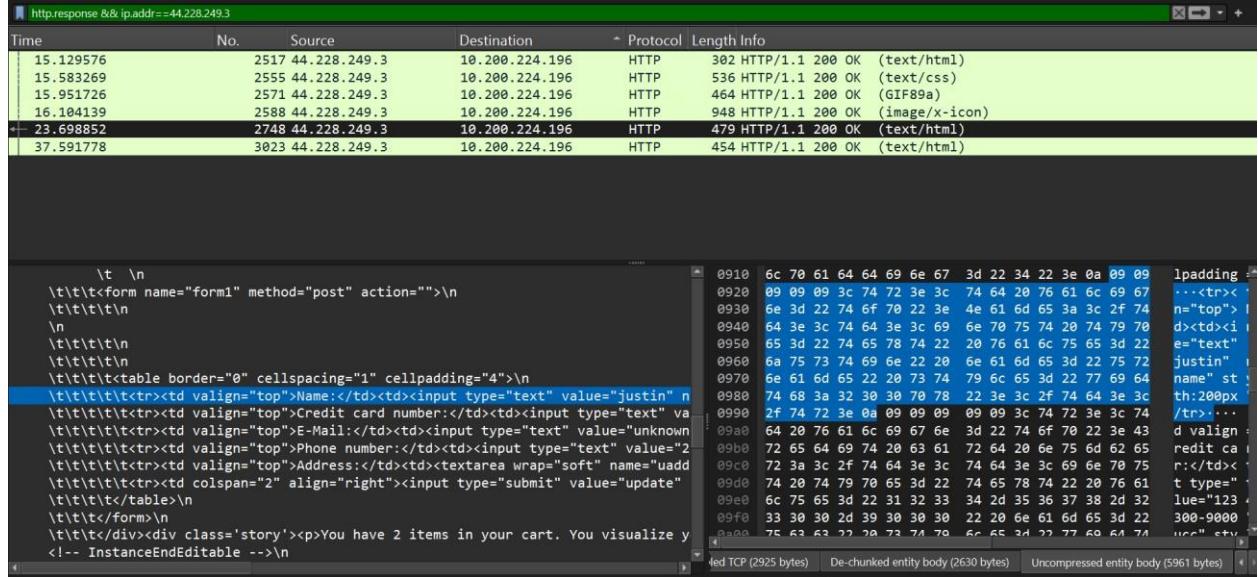
Packet 2991 details:

- Origin: http://testphp.vulnweb.com\r\n
- Connection: keep-alive\r\n
- Referer: http://testphp.vulnweb.com/userinfo.php\r\n
- > Cookie: login=test%2ftest\r\n
- Upgrade-Insecure-Requests: 1\r\n
- Priority: u=0, i\r\n
- \r\n
- [Response in frame: 3023]
- [Full request URI: http://testphp.vulnweb.com/userinfo.php]
- File Data: 114 bytes
- HTML Form URL Encoded: application/x-www-form-urlencoded
 - > Form item: "uname" = "John"
 - > Form item: "ucc" = "1234-5678-2300-9000"
 - > Form item: "uemail" = "unknownclone17@gmail.com"
 - > Form item: "uphone" = "2323345"
 - > Form item: "uaddress" = "abcdef"
 - > Form item: "update" = "update"

The 2991th packet, which corresponds to the second HTTP POST request, contains the updated information I entered. This packet includes the data submitted in the request, such as the Name, Credit card number, E-Mail, Phone number, Address which can be

observed in the request body. The details are visible as form data within the HTTP request, confirming that the updated information was sent to the server.

b. Response Packet: Do you see the updated information reflected in the response packet for the corresponding HTTP request?



The screenshot shows a NetworkMiner capture of a POST request to port 228. The request body contains a form with a single input field named "Name" with the value "justin".

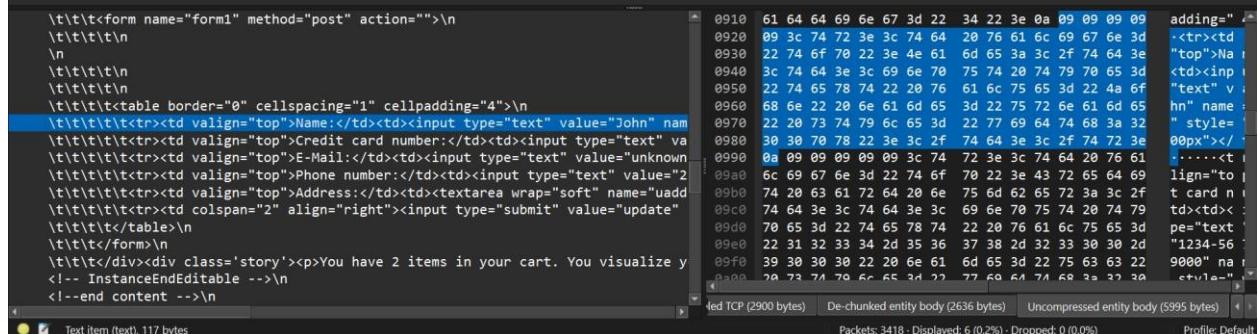
```

    \t \n
    \t\|t\|t<form name="form1" method="post" action="">\n
    \t\|t\|t\|t\n
    \n
    \t\|t\|t\|t\n
    \t\|t\|t\|t\|t<table border="0" cellspacing="1" cellpadding="4">\n
    \t\|t\|t\|t\|t<tr><td valign="top">Name:</td><td><input type="text" value="justin" n
    \t\|t\|t\|t\|t<tr><td valign="top">Credit card number:</td><td><input type="text" va
    \t\|t\|t\|t\|t<tr><td valign="top">E-Mail:</td><td><input type="text" value="unknown
    \t\|t\|t\|t\|t<tr><td valign="top">Phone number:</td><td><input type="text" value="2
    \t\|t\|t\|t\|t<tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uadd
    \t\|t\|t\|t\|t<tr><td colspan="2" align="right"><input type="submit" value="update"
    \t\|t\|t\|t</table>\n
    \t\|t\|t</form>\n
    \t\|t\|t</div><div class='story'><p>You have 2 items in your cart. You visualize y
    <!-- InstanceEndEditable -->\n

```



The screenshot shows the corresponding HTTP response. The server has processed the update and returned a modified HTML page where the name "justin" has been replaced by "John".



This screenshot shows another view of the NetworkMiner capture, highlighting the same response packet. The HTML content now reflects the updated name "John".

Yes, we can see the updated information is reflected in the response packet. After submitting the updated data, the server's response, which is in the form of HTML code, shows the changes. Here, the name previously set to "Justin" is now updated to "John" in the server's response, confirming that the new information was processed successfully.