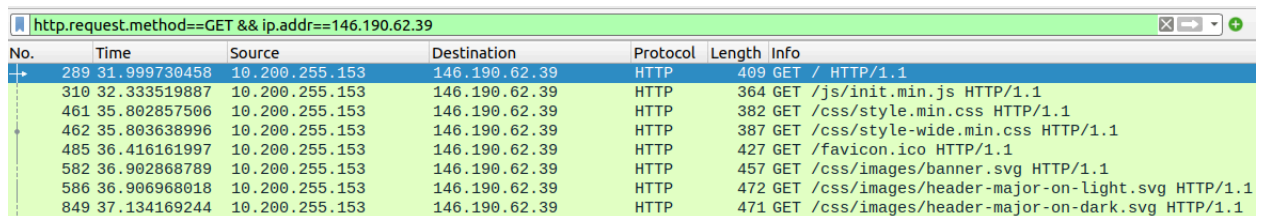


CS 315 : Computer Networks Lab
Assignment - 3
Wireshark Lab: HTTP

Ayush Mallick
CS22BT008

Part-1

1. *HTTP/1.1*
2. *GET*
3. *200 OK and 404 Not Found*
4. **http://httpforever.com/**
Number of HTTP GET requests : 8
Frame number for initial GET request : 289



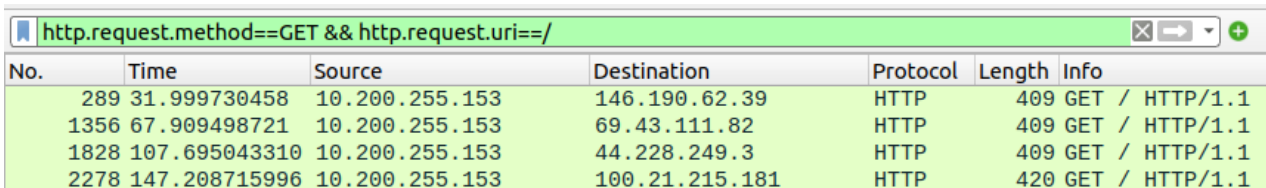
No.	Time	Source	Destination	Protocol	Length	Info
289	31.999730458	10.200.255.153	146.190.62.39	HTTP	409	GET / HTTP/1.1
310	32.333519887	10.200.255.153	146.190.62.39	HTTP	364	GET /js/init.min.js HTTP/1.1
461	35.802857506	10.200.255.153	146.190.62.39	HTTP	382	GET /css/style.min.css HTTP/1.1
462	35.803638996	10.200.255.153	146.190.62.39	HTTP	387	GET /css/style-wide.min.css HTTP/1.1
485	36.416161997	10.200.255.153	146.190.62.39	HTTP	427	GET /favicon.ico HTTP/1.1
582	36.902868789	10.200.255.153	146.190.62.39	HTTP	457	GET /css/images/banner.svg HTTP/1.1
586	36.906968018	10.200.255.153	146.190.62.39	HTTP	472	GET /css/images/header-major-on-light.svg HTTP/1.1
849	37.134169244	10.200.255.153	146.190.62.39	HTTP	471	GET /css/images/header-major-on-dark.svg HTTP/1.1

5. *en-US, en;q=0.5*
6. **http://httpforever.com/**
Source IP address : 10.200.255.153
Destination IP address : 146.190.62.39

http://web.simmons.edu/
Source IP address : 10.200.255.153
Destination IP address : 69.43.111.82

http://www.vulnweb.com/
Source IP address : 10.200.255.153
Destination IP address : 44.228.249.3

http://www.testingmcafeesites.com/
Source IP address : 10.200.255.153
Destination IP address : 100.21.215.181



No.	Time	Source	Destination	Protocol	Length	Info
289	31.999730458	10.200.255.153	146.190.62.39	HTTP	409	GET / HTTP/1.1
1356	67.909498721	10.200.255.153	69.43.111.82	HTTP	409	GET / HTTP/1.1
1828	107.695043310	10.200.255.153	44.228.249.3	HTTP	409	GET / HTTP/1.1
2278	147.208715996	10.200.255.153	100.21.215.181	HTTP	420	GET / HTTP/1.1

7. *no.*
8. **http://httpforever.com/**
Bytes returned : 5124

http://web.simmons.edu/
Bytes returned : 412

http://www.vulnweb.com/
Bytes returned : 4018

http://www.testingmcafeesites.com/
Bytes returned : 28634
9. **http://httpforever.com/**
Lines of data : 100

http://web.simmons.edu/
Lines of data : 9

http://www.vulnweb.com/
Lines of data : 73

http://www.testingmcafeesites.com/
Lines of data : 368

Part-2

1. No, there is no If-Modified-Since header in the HTTP GET request as the request for the file is being made for the first time, and the browser does not yet have a cached version.

```

▼ Hypertext Transfer Protocol
  ▼ 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 (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
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      [HTTP request 1/1]
      [Response in frame: 98]

```

2. Yes, as indicated by the status code (200 OK) and the file contents in the raw data in the response packet content window.

```
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-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```

3. Yes, it contains the timestamp of when the file was last modified, as cached by the browser (*If-Modified-Since: Sun, 26 Jan 2025 06:59:01 GMT*).

```
Hypertext Transfer Protocol
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 (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, 26 Jan 2025 06:59:01 GMT\r\n
If-None-Match: "173-62c967e9fb41d"\r\n
Priority: u=0, i\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: 136]
```

4. The server returned the status code 304 with status code description *Not Modified*, as the file in the browser's cache is still valid. No, the server did not explicitly return the contents of the file, to save bandwidth by avoiding retransmitting unchanged resources, as a mechanism for efficient web browsing.

```
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: Sun, 26 Jan 2025 14:26:55 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: "173-62c967e9fb41d"\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.307136920 seconds]
[Request in frame: 134]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Part-3

1. Number of HTTP GET request messages sent : 2
Packet number containing the GET message : 93

No.	Time	Source	Destination	Protocol	Length	Info
93	3.801037766	10.200.255.153	128.119.245.12	HTTP	439	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
101	4.165554799	128.119.245.12	10.200.255.153	HTTP	2415	HTTP/1.1 200 OK (text/html)
114	4.210884879	10.200.255.153	128.119.245.12	HTTP	459	GET /favicon.ico HTTP/1.1
126	4.505233134	128.119.245.12	10.200.255.153	HTTP	539	HTTP/1.1 404 Not Found (text/html)

2. Packet number containing the response with HTML file : 101

▼ Hypertext Transfer Protocol
▼ HTTP/1.1 200 OK\r\n
▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Sun, 26 Jan 2025 16:21:20 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: Sun, 26 Jan 2025 06:59:01 GMT\r\n
ETag: "1194-62c967e9f7d6c"\r\n
Accept-Ranges: bytes\r\n
▼ Content-Length: 4500\r\n
[Content length: 4500]
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: 0.364517033 seconds]
[Request in frame: 93]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
File Data: 4500 bytes

3. 200 OK

4. Number of TCP segments : 2

▼ [2 Reassembled TCP Segments (4861 bytes): #99(2500), #101(2361)]
[Frame: 99, payload: 0-2499 (2500 bytes)]
[Frame: 101, payload: 2500-4860 (2361 bytes)]
[Segment count: 2]
[Reassembled TCP length: 4861]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203236204a616e2032...]

Part-4


1. Number of HTTP GET request messages sent : 4
All GET requests were sent to 127.0.0.1 (localhost).

No.	Time	Source	Destination	Protocol	Length	Info
292	35.237258347	127.0.0.1	127.0.0.1	HTTP	529	GET /embedded_obj.html HTTP/1.1
296	35.253503514	127.0.0.1	127.0.0.1	HTTP	686	HTTP/1.0 200 OK (text/html)
304	35.284027235	127.0.0.1	127.0.0.1	HTTP	536	GET /sampleimage.jpg HTTP/1.1
308	35.284600570	127.0.0.1	127.0.0.1	HTTP	29769	HTTP/1.0 200 OK (JPEG JFIF image)
316	35.335902143	127.0.0.1	127.0.0.1	HTTP	529	GET /favicon.ico HTTP/1.1
320	35.336588069	127.0.0.1	127.0.0.1	HTTP	535	HTTP/1.0 404 File not found (text/html)
328	35.339973833	127.0.0.1	127.0.0.1	HTTP	546	GET /samplevideo.mp4 HTTP/1.1
489	35.349392195	127.0.0.1	127.0.0.1	MP4	7142	

2. Yes, the file sizes match, i.e. 29703 bytes.

sampleimage.jpg Properties

Basic Permissions Open With Image



Name

sampleimage.jpg

Type

JPEG image (image/jpeg)

Size

29.7 kB (29,703 bytes)

Parent folder

/home/ayushm/Documents/code/cnass3

Accessed

Sunday 26 January 2025 10:34:38 PM

Modified

Sunday 26 January 2025 10:34:00 PM

Created

Sunday 26 January 2025 10:34:00 PM

Hypertext Transfer Protocol

HTTP/1.0 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.0 200 OK\r\n]

[HTTP/1.0 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.0

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Server: SimpleHTTP/0.6 Python/3.10.12\r\n

Date: Sun, 26 Jan 2025 17:12:37 GMT\r\n

Content-type: image/jpeg\r\n

Content-Length: 29703\r\n

[Content length: 29703]

Last-Modified: Sun, 26 Jan 2025 17:04:00 GMT\r\n\r\n

[HTTP response 1/1]

[Time since request: 0.000573335 seconds]

[Request in frame: 304]

[Request URI: http://localhost:8080/sampleimage.jpg]

File Data: 29703 bytes

3. Yes, the response code to the HTTP GET request for favicon.ico returned a 404 File not found error, indicating that the fetch of favicon was unsuccessful.

Hypertext Transfer Protocol

HTTP/1.0 404 File not found\r\n

[Expert Info (Chat/Sequence): HTTP/1.0 404 File not found\r\n]

[HTTP/1.0 404 File not found\r\n]

[Severity level: Chat]

[Group: Sequence]

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: Sun, 26 Jan 2025 17:12:37 GMT\r\n

Connection: close\r\n

Content-Type: text/html; charset=utf-8\r\n

Content-Length: 469\r\n

[Content length: 469]

\r\n

[HTTP response 1/1]

[Time since request: 0.000685926 seconds]

[Request in frame: 316]

[Request URI: http://localhost:8080/favicon.ico]

File Data: 469 bytes

4. Source IP address : 127.0.0.1
Destination IP address : 127.0.0.1
This is because the HTTP server is hosted on the same machine as the client, and all traffic is looped back to the local system.

Part-5

1. Number of GET packets : 4
Number of POST packets : 2

http.request.method==GET or http.request.method==POST						
No.	Time	Source	Destination	Protocol	Length	Info
15	2.618350307	10.200.255.153	44.228.249.3	HTTP	422	GET /login.php HTTP/1.1
31	3.025128519	10.200.255.153	44.228.249.3	HTTP	391	GET /style.css HTTP/1.1
50	3.379688454	10.200.255.153	44.228.249.3	HTTP	451	GET /images/logo.gif HTTP/1.1
52	3.562774812	10.200.255.153	44.228.249.3	HTTP	444	GET /favicon.ico HTTP/1.1
152	17.991371947	10.200.255.153	44.228.249.3	HTTP	598	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
212	29.507735512	10.200.255.153	44.228.249.3	HTTP	706	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

2. Domain : <http://testphp.vulnweb.com/login.php>
IP address : 44.228.249.3

[\[Full request URI: http://testphp.vulnweb.com/login.php\]](http://testphp.vulnweb.com/login.php)
[\[HTTP request 1/1\]](#)
[\[Response in frame: 23\]](#)

3. Destination port : 80
Protocol : *HTTP (Hypertext Transfer Protocol)*
Yes, it is the standard port for HTTP communication.

Transmission Control Protocol, Src Port: 38440, Dst Port: 80, Seq: 1, Ack: 1, Len: 356
Source Port: 38440
Destination Port: 80

4. No, signifying that the page is loaded for the first time.

Hypertext Transfer Protocol
POST /userinfo.php HTTP/1.1\r\n
[Expert Info (Chat/Sequence): POST /userinfo.php HTTP/1.1\r\n]
[POST /userinfo.php HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: POST
Request URI: /userinfo.php
Request Version: HTTP/1.1
Host: testphp.vulnweb.com\r\nUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:134.0) Gecko/20100101 Firefox/134.0\r\nAccept: 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\n[Content length: 20]
Origin: 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[\[Full request URI: http://testphp.vulnweb.com/userinfo.php\]](http://testphp.vulnweb.com/userinfo.php)
[\[HTTP request 2/3\]](#)
[\[Prev request in frame: 50\]](#)
[\[Response in frame: 156\]](#)
[\[Next request in frame: 212\]](#)
File Data: 20 bytes

5. The second HTTP POST request does not contain the If-Modified-Since header.

```
▼ Hypertext Transfer Protocol
  ▼ POST /userinfo.php HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): POST /userinfo.php HTTP/1.1\r\n]
      [POST /userinfo.php HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: POST
      Request URI: /userinfo.php
      Request Version: HTTP/1.1
      Host: testphp.vulnweb.com\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
      Content-Type: application/x-www-form-urlencoded\r\n
      Content-Length: 98\r\n
    ▼ [Content length: 98]
      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
      Cookie pair: login=test%2Ftest
      Upgrade-Insecure-Requests: 1\r\n
      Priority: u=0, i\r\n
      \r\n
      [Full request URI: http://testphp.vulnweb.com/userinfo.php]
      [HTTP request 3/3]
      [Prev request in frame: 152]
      [Response in frame: 216]
      File Data: 98 bytes
```

6.

a. Both the username (*test*) and the password (*test*) is included.

```
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "uname" = "test"
  ▶ Form item: "pass" = "test"
```

b. Yes, the server responds with a 200 OK message, and a new webpage, displaying the user's details.

7.

a. Packet containing updated information : 212

```
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "urname" = "Wow"
  ▶ Form item: "ucc" = "1234-5678-2300"
  ▶ Form item: "uemail" = "email@email.com"
  ▶ Form item: "uphone" = "2323345"
  ▶ Form item: "uaddress" = "iitdh"
  ▶ Form item: "update" = "update"
```

b. Yes, the updated information is reflected in the response packet for the HTTP POST update request. The response packet contains the HTML of the page to be displayed after updating the information.