Computer Networks Lab Task – 8

Instructor: Ma'am Hurmat Hidayat

Roll No: 20P-0563

Name: Mahad Ashraf

Section: B

Task: HTTP analysis using Wireshark by looking at the information in the HTTP GET and response messages, answer the following questions

First we open Wireshark then we go on the using the filter option and write down http so we can filter out the http protocols and then we Start up the Wireshark packet sniffer. From our browser only http protocols and then we open the following link

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

Then we will get this output
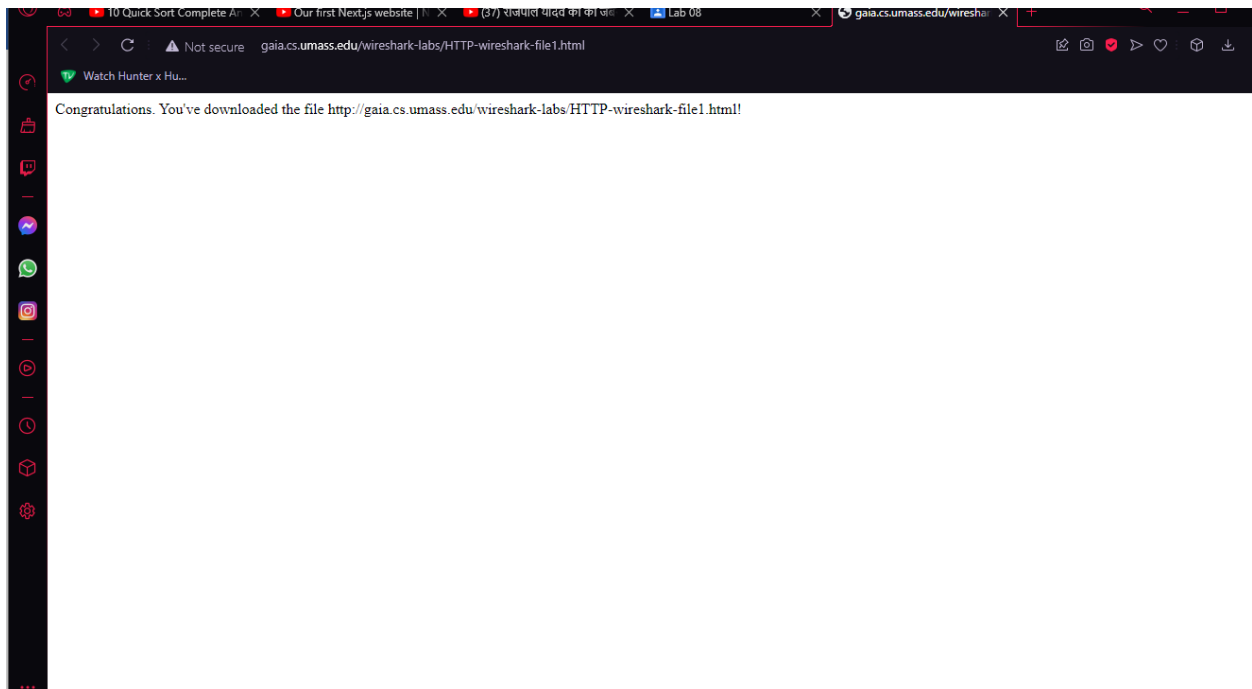
And when we open our Wireshark we will get these two get and response between the server and our pc we get a 200 OK

Answer the Following Questions:

Q1: Is your browser running HTTP version 1.0, 1.1, or 2?

Q2: What version of HTTP is the server running?

Q3: What languages (if any) does your browser indicate that it can accept to the server?

```
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KI
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
```

Q4: What is the IP address of your computer? What is the IP address of the Gaia.cs.umass.edu server?

```
> Internet Protocol Version 4, Src: 172.17.2.84, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50232, Dst Port: 80, Seq: 1, Ack: 1, Le
v Hypertext Transfer Protocol
```

Q5: What is the status code returned from the server to your browser?

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

Q6: When was the HTML file that you are retrieving last modified at the server?

```
Date: Tue, 18 Oct 2022 09:56:49 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Tue, 18 Oct 2022 05:59:01 GMT\r\n
ETag: "173-5eb48c9f49aa2"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
```

Q7: How many bytes of content are being returned to your browser?

```
∨ Content-Length: 128\r\n
      [Content length: 128]
   Keep-Alive: timeout=5, max=100\r\n
   Connection: Keep-Alive\r\n
   Content-Type: text/html; charset=UTF-8\r\n
```

Q8: 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

```
▾ Line-based text data: text/html (4 lines)
      <html>\n
      Congratulations.  You've downloaded the file \n
      http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
      </html>\n
```

No, I do not see any headers in the http since they were missing.

Task: The HTTP CONDITIONAL GET/response interaction

First we open Wireshark then we go on the using the filter option and write down http so we can filter out the http protocols and then we Start up the Wireshark packet sniffer. From our browser only http protocols and then we open the following link

 Enter the following URL into your browser: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Then we will get this output
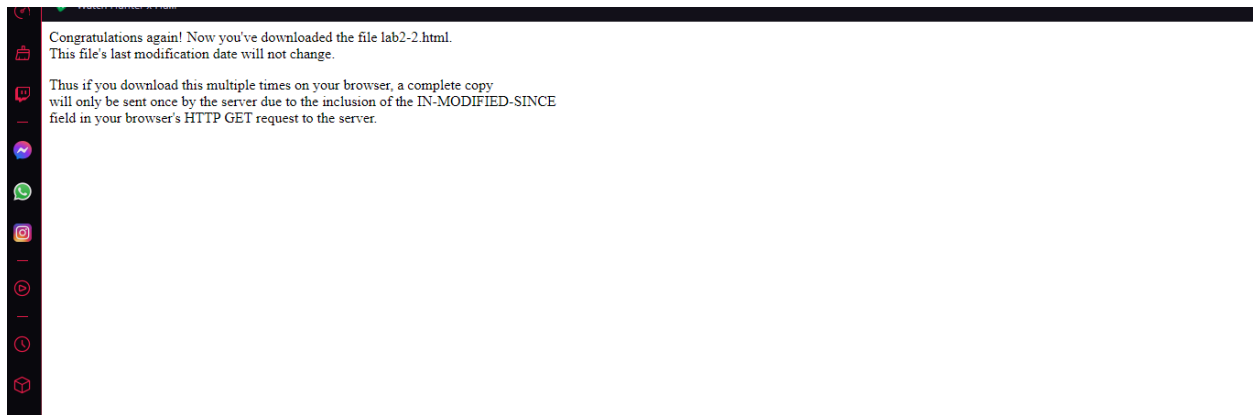
In the first get response we get 200 ok but then when we refresh our page and try again we get a 304 not modified
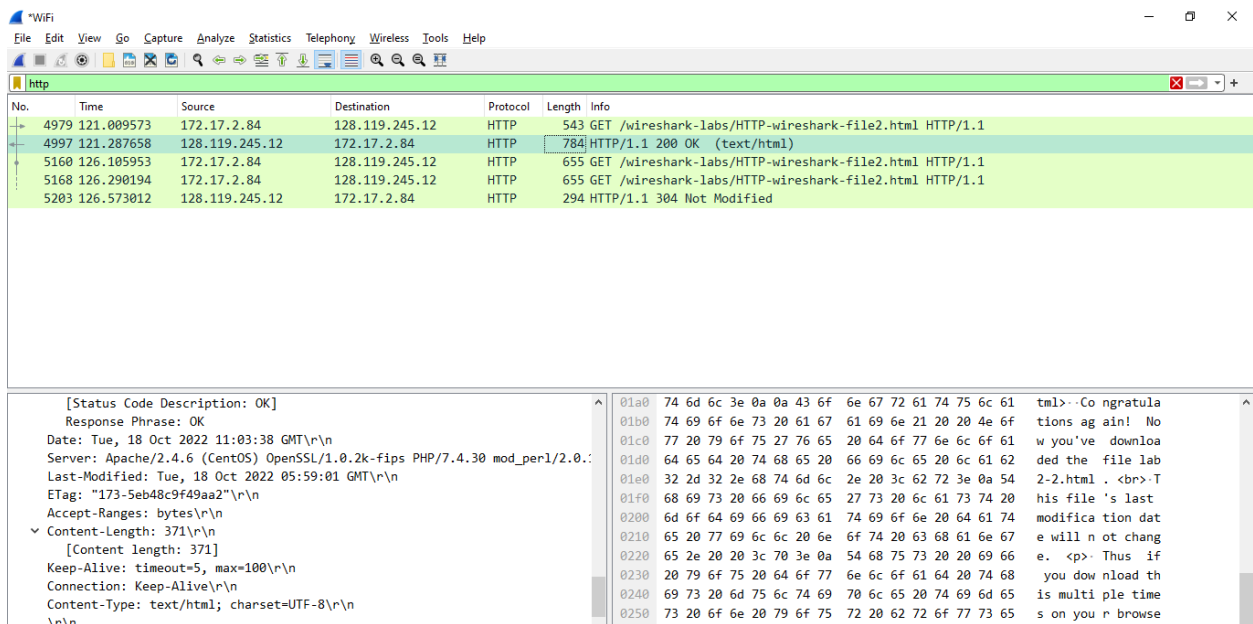
Answer the following questions:

Q1: Inspect the contents of the first HTTP GET request from your browser to the server. Do you See an "IF-MODIFIED-SINCE" line in the HTTP GET?

No there is no IF-MODIFIED-SINCE line in the GET message.

Q2: Inspect the contents of the server response. Did the server explicitly return the contents of the

File? How can you tell?

174 4.223664	172.17.2.84	128.119.245.12	HTTP	543 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
189 4.485725	128.119.245.12	172.17.2.84	HTTP	784 HTTP/1.1 200 OK (text/html)
3693 106.061347	172.17.2.84	128.119.245.12	HTTP	655 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
3704 106.356187	128.119.245.12	172.17.2.84	HTTP	294 HTTP/1.1 304 Not Modified
4055 118.858736	172.17.2.84	128.119.245.12	HTTP	655 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4062 119.126494	128.119.245.12	172.17.2.84	HTTP	294 HTTP/1.1 304 Not Modified
4341 128.385719	172.17.2.84	128.119.245.12	HTTP	655 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4363 128.651258	128.119.245.12	172.17.2.84	HTTP	294 HTTP/1.1 304 Not Modified
4472 132.153309	172.17.2.84	128.119.245.12	HTTP	655 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
4479 132.417033	128.119.245.12	172.17.2.84	HTTP	293 HTTP/1.1 304 Not Modified

```
  [HTTP response 1/1]
  [Time since request: 0.262061000 seconds]
  [Request in frame: 174]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2
  File Data: 371 bytes
v 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
  will only be sent once by the server due to the inclusion of the IN-MODIFII
  field in your browser's HTTP GET request to the server.\n
  \n
```

```
0000  e0 94 67 f4 58 9e cc 2d  e0 1e 0c 99 08 00 45 00   ··g·X··- ······E·
0010  03 02 66 cb 40 00 29 06  c4 41 80 77 f5 0c ac 11   ··f·@·)· ·A·w····
0020  02 54 00 50 cd 17 0f e4  7b 7b 11 92 88 06 50 18   ·T·P···· {{····P·
0030  00 ed 08 6e 00 00 48 54  54 50 2f 31 2e 31 20 32   ···n··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK··D ate: Tue
0050  2c 20 31 38 20 4f 63 74  20 32 30 32 32 20 31 31   , 18 Oct  2022 11
0060  3a 30 39 3a 34 37 20 47  4d 54 0d 0a 53 65 72 76   :09:47 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 33 30  20 6d 6f 64 5f 70 65 72   P/7.4.30  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 54 75  65 2c 20 31 38 20 4f 63   fied: Tu e, 18 Oc
00e0  74 20 32 30 32 32 20 30  35 3a 35 39 3a 30 31 20   t 2022 0 5:59:01 
```

Q3: 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 GET6? If so, what information follows the "IF-MODIFIED-SINCE:" header?

The HTTP status code is "304: Not Modified"

Q4: 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.

The server did not return the contents of the file because the browser simply retrieved the contents from its cache. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead it simply told my browser to retrieve the old file from its cached memory.