Lab Report

Lab 2 HTTP

ZHOU Siyu

Questions:

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

No.	Time	Source	Destination	Protocol	Length	Info
937	35.150774	10.11.46.25	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
958	35.489060	128.119.245.12	10.11.46.25	HTTP	540	HTTP/1.1 200 OK (text/html)

3. **What is the IP address of your computer? Of the gaia.cs.umass.edu server?**
   IP address of my computer: 10.11.46.25
   IP address of gaia.cs.umass.edu server: 128.119.245.12

```
> Frame 937: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{93EBE42A-F
> Ethernet II, Src: a6:da:7a:61:8d:ad (a6:da:7a:61:8d:ad), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
v Internet Protocol Version 4, Src: 10.11.46.25, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 533
    Identification: 0x512c (20780)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.11.46.25
    Destination Address: 128.119.245.12
v Transmission Control Protocol, Src Port: 53662, Dst Port: 80, Seq: 1, Ack: 1, Len: 493
```

5. **When was the HTML file that you are retrieving last modified at the server?**
   Tue, 07 Feb 2023 08:55:02 GMT (current time)

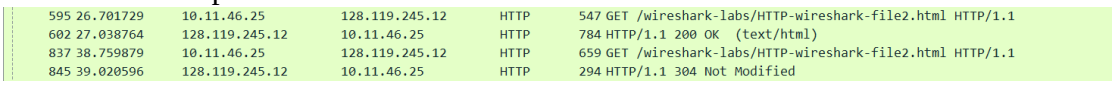
```
    TCP payload (486 bytes)
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 07 Feb 2023 08:55:02 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 07 Feb 2023 06:59:01 GMT\r\n
    ETag: "80-5f416aebd6a2e"\r\n
    Accept-Ranges: bytes\r\n
  > 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 1/2]
    [Time since request: 0.338286000 seconds]
    [Request in frame: 937]
    [Next request in frame: 985]
    [Next response in frame: 993]
```

9. **Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**
   Yes, because we can see the “Line-based text data” part below.

```
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 <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
```

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

Status code and phase returned: HTTP/1.1 304 Not Modified.

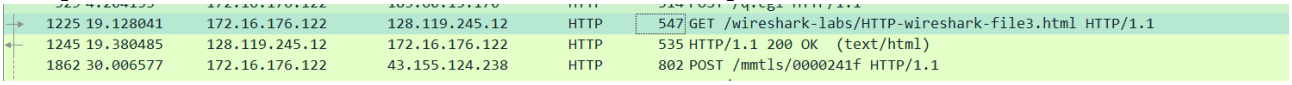


595	26.701729	10.11.46.25	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
602	27.038764	128.119.245.12	10.11.46.25	HTTP	784	HTTP/1.1 200 OK (text/html)
837	38.759879	10.11.46.25	128.119.245.12	HTTP	659	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
845	39.020596	128.119.245.12	10.11.46.25	HTTP	294	HTTP/1.1 304 Not Modified

The server didn't return the contents, because sever read from the cache.

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

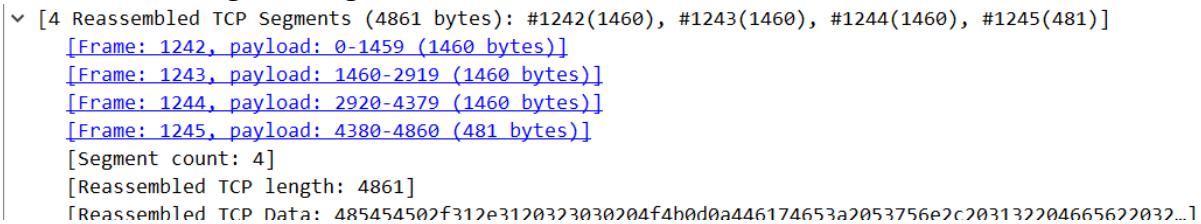
The packet number in trace contains the status code and phrace is 1225.



1225	19.128041	172.16.176.122	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1245	19.380485	128.119.245.12	172.16.176.122	HTTP	535	HTTP/1.1 200 OK (text/html)
1862	30.006577	172.16.176.122	43.155.124.238	HTTP	802	POST /mmtls/0000241f HTTP/1.1

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

4 data-containning TCP segments.

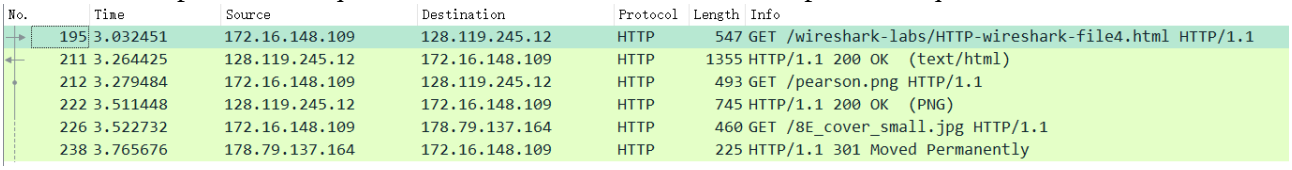


```
[4 Reassembled TCP Segments (4861 bytes): #1242(1460), #1243(1460), #1244(1460), #1245(481)]
    [Frame: 1242, payload: 0-1459 (1460 bytes)]
    [Frame: 1243, payload: 1460-2919 (1460 bytes)]
    [Frame: 1244, payload: 2920-4379 (1460 bytes)]
    [Frame: 1245, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c20313220466562…]
```

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

The images are download serially.

Because first picture is request to download before the second picture requested.



No.	Time	Source	Destination	Protocol	Length	Info
195	3.032451	172.16.148.109	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
211	3.264425	128.119.245.12	172.16.148.109	HTTP	1355	HTTP/1.1 200 OK (text/html)
212	3.279484	172.16.148.109	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
222	3.511448	128.119.245.12	172.16.148.109	HTTP	745	HTTP/1.1 200 OK (PNG)
226	3.522732	172.16.148.109	178.79.137.164	HTTP	460	GET /8E_cover_small.jpg HTTP/1.1
238	3.765676	178.79.137.164	172.16.148.109	HTTP	225	HTTP/1.1 301 Moved Permanently