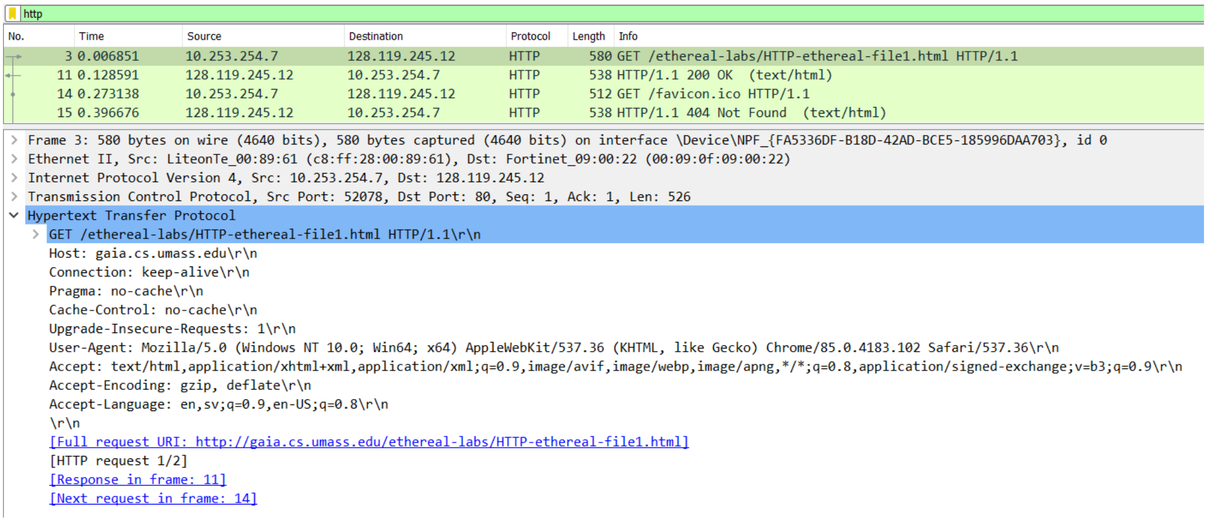
## Lab 1:

## Philip Ngo – phing272

## Henrik Rosander – henro926

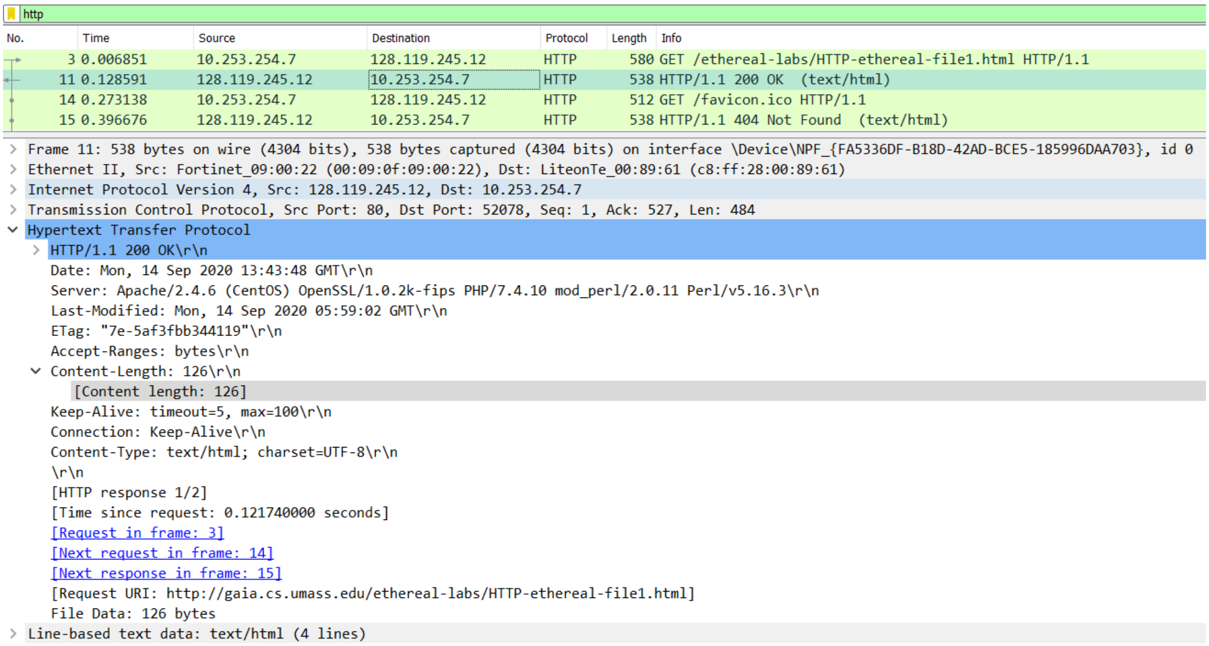
## Part 1:



```
http
No.   Time       Source           Destination      Protocol  Length  Info
    3 0.006851   10.253.254.7     128.119.245.12   HTTP      580 GET /ethereal-labs/HTTP-ethereal-file1.html HTTP/1.1
   11 0.128591   128.119.245.12   10.253.254.7     HTTP      538 HTTP/1.1 200 OK  (text/html)
   14 0.273138   10.253.254.7     128.119.245.12   HTTP      512 GET /favicon.ico HTTP/1.1
   15 0.396676   128.119.245.12   10.253.254.7     HTTP      538 HTTP/1.1 404 Not Found  (text/html)

> Frame 3: 580 bytes on wire (4640 bits), 580 bytes captured (4640 bits) on interface \Device\NPF_{FA5336DF-B18D-42AD-BCE5-185996DAA703}, id 0
> Ethernet II, Src: LiteonTe_00:89:61 (c8:ff:28:00:89:61), Dst: Fortinet_09:00:22 (00:09:0f:09:00:22)
> Internet Protocol Version 4, Src: 10.253.254.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52078, Dst Port: 80, Seq: 1, Ack: 1, Len: 526
v Hypertext Transfer Protocol
  > GET /ethereal-labs/HTTP-ethereal-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en,sv;q=0.9,en-US;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html]
    [HTTP request 1/2]
    [Response in frame: 11]
    [Next request in frame: 14]
```

1. It is running HTTP 1.1
2. It accepts en, sv; q=0.9, en-US; q=0.8
3. The computer IP-address is 10.253.254.7 and server address is 128.119.245.12
4. The status code returned was "200 OK"

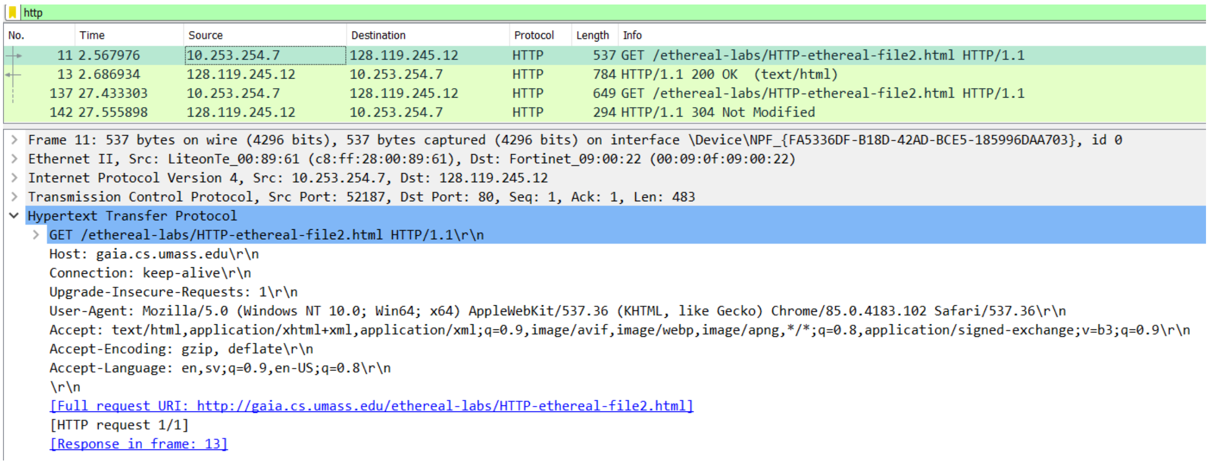


```
http
No.   Time       Source           Destination      Protocol  Length  Info
    3 0.006851   10.253.254.7     128.119.245.12   HTTP      580 GET /ethereal-labs/HTTP-ethereal-file1.html HTTP/1.1
   11 0.128591   128.119.245.12   10.253.254.7     HTTP      538 HTTP/1.1 200 OK  (text/html)
   14 0.273138   10.253.254.7     128.119.245.12   HTTP      512 GET /favicon.ico HTTP/1.1
   15 0.396676   128.119.245.12   10.253.254.7     HTTP      538 HTTP/1.1 404 Not Found  (text/html)

> Frame 11: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{FA5336DF-B18D-42AD-BCE5-185996DAA703}, id 0
> Ethernet II, Src: Fortinet_09:00:22 (00:09:0f:09:00:22), Dst: LiteonTe_00:89:61 (c8:ff:28:00:89:61)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.253.254.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 52078, Seq: 1, Ack: 527, Len: 484
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 14 Sep 2020 13:43:48 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 14 Sep 2020 05:59:02 GMT\r\n
    ETag: "7e-5af3fbb344119"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 126\r\n
      [Content length: 126]
    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: 0.121740000 seconds]
    [Request in frame: 3]
    [Next request in frame: 14]
    [Next response in frame: 15]
    [Request URI: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html]
    File Data: 126 bytes
> Line-based text data: text/html (4 lines)
```

5. Last modified Mon, 14 September, 2020, 05:59:02 GMT
6. 126 bytes (from the length)

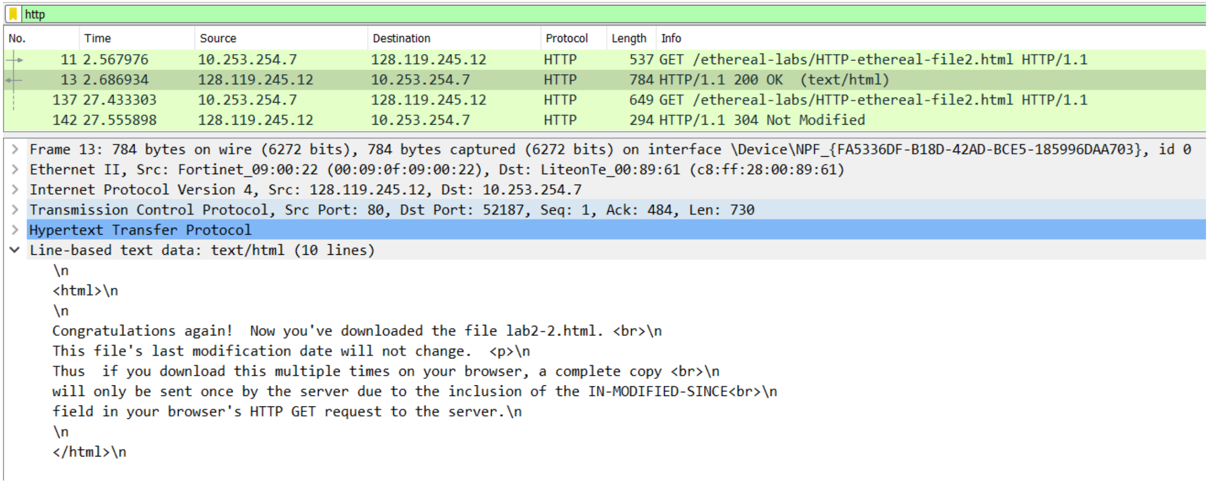
**Part 2:**



```
http
No.     Time        Source          Destination     Protocol  Length  Info
    11 2.567976    10.253.254.7    128.119.245.12  HTTP       537 GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1
    13 2.686934    128.119.245.12  10.253.254.7    HTTP       784 HTTP/1.1 200 OK  (text/html)
   137 27.433303   10.253.254.7    128.119.245.12  HTTP       649 GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1
   142 27.555898   128.119.245.12  10.253.254.7    HTTP       294 HTTP/1.1 304 Not Modified

> Frame 11: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface \Device\NPF_{FA5336DF-B18D-42AD-BCE5-185996DAA703}, id 0
> Ethernet II, Src: LiteonTe_00:89:61 (c8:ff:28:00:89:61), Dst: Fortinet_09:00:22 (00:09:0f:09:00:22)
> Internet Protocol Version 4, Src: 10.253.254.7, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52187, Dst Port: 80, Seq: 1, Ack: 1, Len: 483
v Hypertext Transfer Protocol
   > GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1\r\n
     Host: gaia.cs.umass.edu\r\n
     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 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36\r\n
     Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
     Accept-Encoding: gzip, deflate\r\n
     Accept-Language: en,sv;q=0.9,en-US;q=0.8\r\n
     \r\n
     [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file2.html]
     [HTTP request 1/1]
     [Response in frame: 13]
```

7. No, we do not. See image above



```
http
No.     Time        Source          Destination     Protocol  Length  Info
    11 2.567976    10.253.254.7    128.119.245.12  HTTP       537 GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1
    13 2.686934    128.119.245.12  10.253.254.7    HTTP       784 HTTP/1.1 200 OK  (text/html)
   137 27.433303   10.253.254.7    128.119.245.12  HTTP       649 GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1
   142 27.555898   128.119.245.12  10.253.254.7    HTTP       294 HTTP/1.1 304 Not Modified

> Frame 13: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{FA5336DF-B18D-42AD-BCE5-185996DAA703}, id 0
> Ethernet II, Src: Fortinet_09:00:22 (00:09:0f:09:00:22), Dst: LiteonTe_00:89:61 (c8:ff:28:00:89:61)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.253.254.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 52187, Seq: 1, Ack: 484, Len: 730
> Hypertext Transfer Protocol
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
```

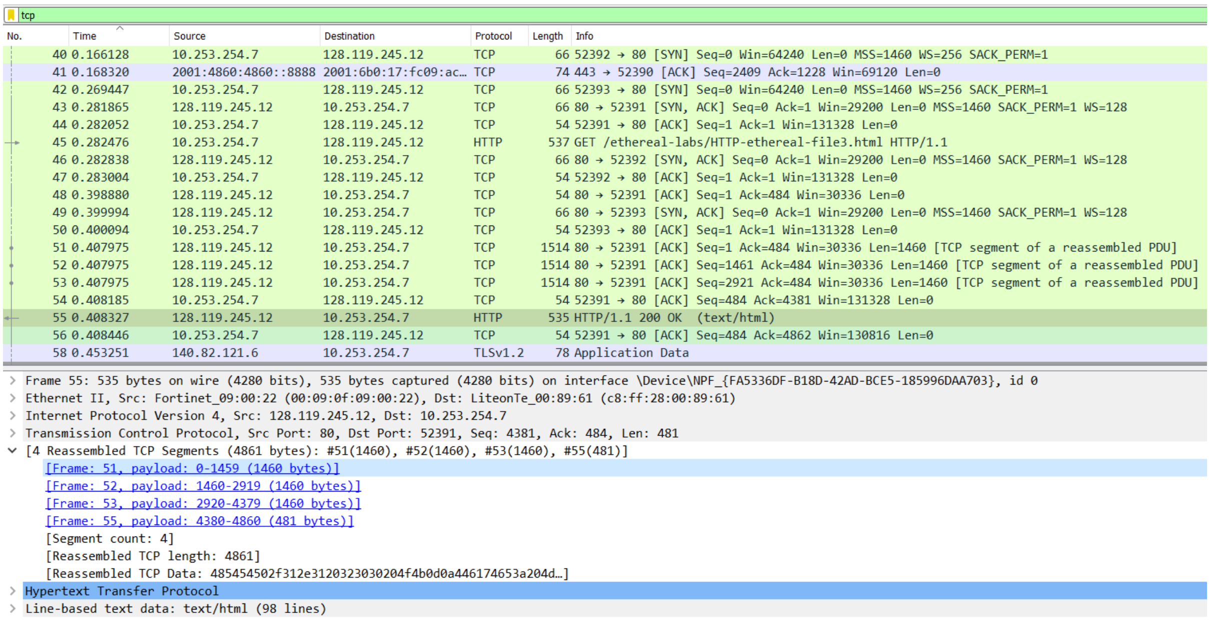
8. Yes, it did. See image above

9. IF-MODIFIED-SINCE: is Mon, 14 September, 2020, 05:59:02 GMT

10. HTTP Status Code “304 Not Modified”. The server did not return any content because the website the website was unmodified from its previous request. When we did our first HTTP GET request, the text was saved in chromes memory cache. So when we reload the page, we don’t need to get new data since the webpage is unmodified.

## Part 3:

11. One HTTP GET request messages were sent by the browser



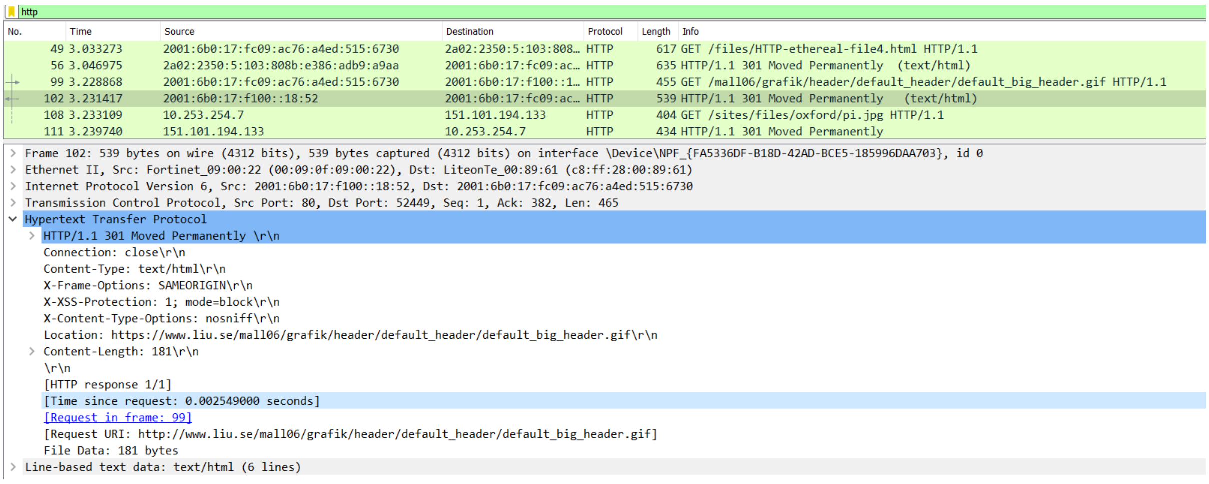
```
tcp
No.    Time       Source                  Destination            Protocol  Length  Info
    40 0.166128   10.253.254.7            128.119.245.12         TCP         66 52392 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    41 0.168320   2001:4860:4860::8888    2001:6b0:17:fc09:ac…   TCP         74 443 → 52390 [ACK] Seq=2409 Ack=1228 Win=69120 Len=0
    42 0.269447   10.253.254.7            128.119.245.12         TCP         66 52393 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    43 0.281865   128.119.245.12          10.253.254.7           TCP         66 80 → 52391 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
    44 0.282052   10.253.254.7            128.119.245.12         TCP         54 52391 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
    45 0.282476   10.253.254.7            128.119.245.12         HTTP       537 GET /ethereal-labs/HTTP-ethereal-file3.html HTTP/1.1
    46 0.282838   128.119.245.12          10.253.254.7           TCP         66 80 → 52392 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
    47 0.283004   10.253.254.7            128.119.245.12         TCP         54 52392 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
    48 0.398880   128.119.245.12          10.253.254.7           TCP         54 80 → 52391 [ACK] Seq=1 Ack=484 Win=30336 Len=0
    49 0.399994   128.119.245.12          10.253.254.7           TCP         66 80 → 52393 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
    50 0.400094   10.253.254.7            128.119.245.12         TCP         54 52393 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
    51 0.407975   128.119.245.12          10.253.254.7           TCP       1514 80 → 52391 [ACK] Seq=1 Ack=484 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
    52 0.407975   128.119.245.12          10.253.254.7           TCP       1514 80 → 52391 [ACK] Seq=1461 Ack=484 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
    53 0.407975   128.119.245.12          10.253.254.7           TCP       1514 80 → 52391 [ACK] Seq=2921 Ack=484 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
    54 0.408185   10.253.254.7            128.119.245.12         TCP         54 52391 → 80 [ACK] Seq=484 Ack=4381 Win=131328 Len=0
    55 0.408327   128.119.245.12          10.253.254.7           HTTP       535 HTTP/1.1 200 OK  (text/html)
    56 0.408446   10.253.254.7            128.119.245.12         TCP         54 52391 → 80 [ACK] Seq=484 Ack=4862 Win=130816 Len=0
    58 0.453251   140.82.121.6            10.253.254.7           TLSv1.2     78 Application Data

> Frame 55: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{FA5336DF-B18D-42AD-BCE5-185996DAA703}, id 0
> Ethernet II, Src: Fortinet_09:00:22 (00:09:0f:09:00:22), Dst: LiteonTe_00:89:61 (c8:ff:28:00:89:61)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.253.254.7
> Transmission Control Protocol, Src Port: 80, Dst Port: 52391, Seq: 4381, Ack: 484, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #51(1460), #52(1460), #53(1460), #55(481)]
    [Frame: 51, payload: 0-1459 (1460 bytes)]
    [Frame: 52, payload: 1460-2919 (1460 bytes)]
    [Frame: 53, payload: 2920-4379 (1460 bytes)]
    [Frame: 55, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d…]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

12. 4 TCP segments for the HTTP GET. See image above
13. The status code is “200 OK”

## Part 4:

14. 3 total HTTP GET requests were sent, whereas two were sent to https://liu.se/mall06/grafik/header/default_header/default_big_header.gif?fbclid=IwAR2ZkNhAtCaDOh-k7UnlLBy5O_mlwRFjfexFo5D1IBSKIDTVnWtNUx0VxzU and https://www.ox.ac.uk/sites/files/oxford/pi.jpg?fbclid=IwAR2ZkNhAtCaDOh-k7UnlLBy5O_mlwRFjfexFo5D1IBSKIDTVnWtNUx0VxzU

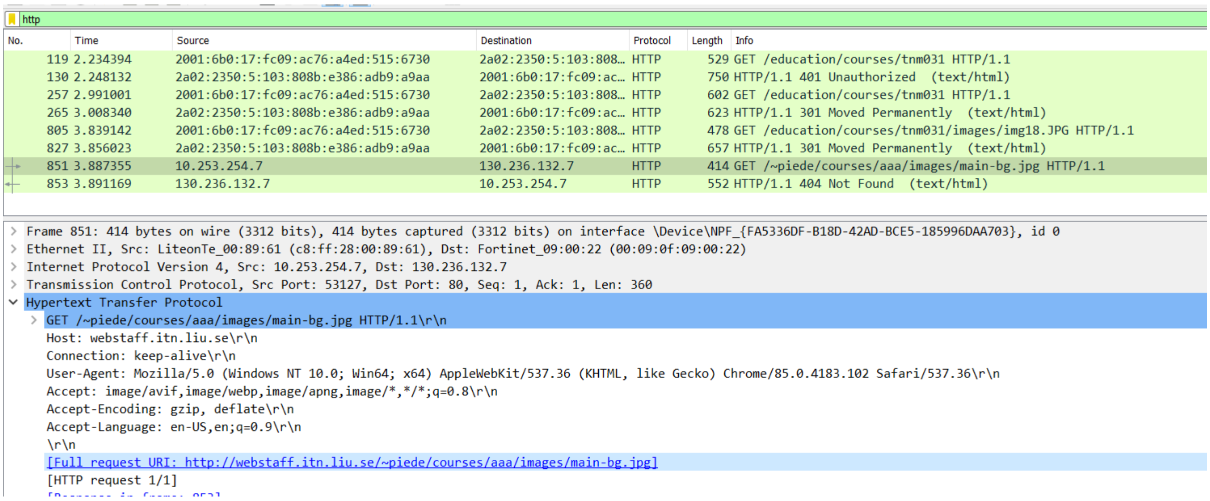


```
http
No.    Time       Source                                Destination              Protocol  Length  Info
    49 3.033273   2001:6b0:17:fc09:ac76:a4ed:515:6730   2a02:2350:5:103:808…     HTTP       617 GET /files/HTTP-ethereal-file4.html HTTP/1.1
    56 3.046975   2a02:2350:5:103:808b:e386:adb9:a9aa   2001:6b0:17:fc09:ac…     HTTP       635 HTTP/1.1 301 Moved Permanently  (text/html)
    99 3.228868   2001:6b0:17:fc09:ac76:a4ed:515:6730   2001:6b0:17:f100::1…     HTTP       455 GET /mall06/grafik/header/default_header/default_big_header.gif HTTP/1.1
   102 3.231417   2001:6b0:17:f100::18:52               2001:6b0:17:fc09:ac…     HTTP       539 HTTP/1.1 301 Moved Permanently   (text/html)
   108 3.233109   10.253.254.7                          151.101.194.133          HTTP       404 GET /sites/files/oxford/pi.jpg HTTP/1.1
   111 3.239740   151.101.194.133                       10.253.254.7             HTTP       434 HTTP/1.1 301 Moved Permanently

> Frame 102: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{FA5336DF-B18D-42AD-BCE5-185996DAA703}, id 0
> Ethernet II, Src: Fortinet_09:00:22 (00:09:0f:09:00:22), Dst: LiteonTe_00:89:61 (c8:ff:28:00:89:61)
> Internet Protocol Version 6, Src: 2001:6b0:17:f100::18:52, Dst: 2001:6b0:17:fc09:ac76:a4ed:515:6730
> Transmission Control Protocol, Src Port: 80, Dst Port: 52449, Seq: 1, Ack: 382, Len: 465
v Hypertext Transfer Protocol
  > HTTP/1.1 301 Moved Permanently \r\n
    Connection: close\r\n
    Content-Type: text/html\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    X-XSS-Protection: 1; mode=block\r\n
    X-Content-Type-Options: nosniff\r\n
    Location: https://www.liu.se/mall06/grafik/header/default_header/default_big_header.gif\r\n
  > Content-Length: 181\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.002549000 seconds]
    [Request in frame: 99]
    [Request URI: http://www.liu.se/mall06/grafik/header/default_header/default_big_header.gif]
    File Data: 181 bytes
> Line-based text data: text/html (6 lines)
```

15. Serially, since the timestamps are different.

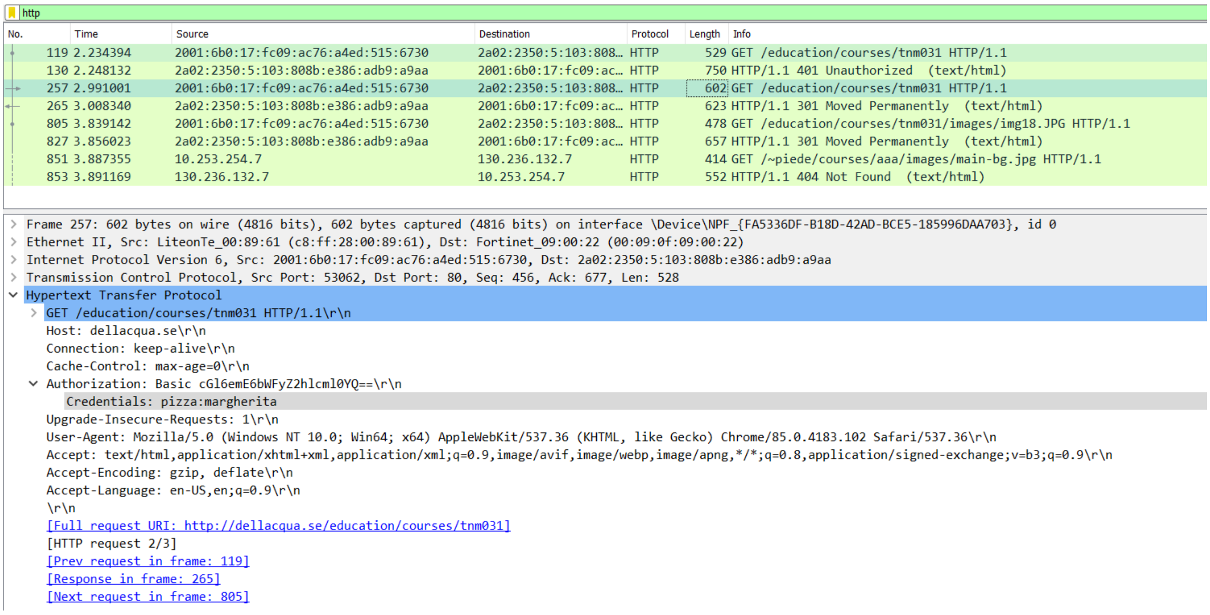
## Part 5:



```
No.      Time      Source                                Destination              Protocol  Length  Info
     119 2.234394  2001:6b0:17:fc09:ac76:a4ed:515:6730   2a02:2350:5:103:808…     HTTP      529 GET /education/courses/tnm031 HTTP/1.1
     130 2.248132  2a02:2350:5:103:808b:e386:adb9:a9aa   2001:6b0:17:fc09:ac…     HTTP      750 HTTP/1.1 401 Unauthorized  (text/html)
     257 2.991001  2001:6b0:17:fc09:ac76:a4ed:515:6730   2a02:2350:5:103:808…     HTTP      602 GET /education/courses/tnm031 HTTP/1.1
     265 3.008340  2a02:2350:5:103:808b:e386:adb9:a9aa   2001:6b0:17:fc09:ac…     HTTP      623 HTTP/1.1 301 Moved Permanently  (text/html)
     805 3.839142  2001:6b0:17:fc09:ac76:a4ed:515:6730   2a02:2350:5:103:808…     HTTP      478 GET /education/courses/tnm031/images/img18.JPG HTTP/1.1
     827 3.856023  2a02:2350:5:103:808b:e386:adb9:a9aa   2001:6b0:17:fc09:ac…     HTTP      657 HTTP/1.1 301 Moved Permanently  (text/html)
     851 3.887355  10.253.254.7                          130.236.132.7            HTTP      414 GET /~piede/courses/aaa/images/main-bg.jpg HTTP/1.1
     853 3.891169  130.236.132.7                         10.253.254.7             HTTP      552 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 851: 414 bytes on wire (3312 bits), 414 bytes captured (3312 bits) on interface \Device\NPF_{FA5336DF-B18D-42AD-BCE5-185996DAA703}, id 0
> Ethernet II, Src: LiteonTe_00:89:61 (c8:ff:28:00:89:61), Dst: Fortinet_09:00:22 (00:09:0f:09:00:22)
> Internet Protocol Version 4, Src: 10.253.254.7, Dst: 130.236.132.7
> Transmission Control Protocol, Src Port: 53127, Dst Port: 80, Seq: 1, Ack: 1, Len: 360
v Hypertext Transfer Protocol
  > GET /~piede/courses/aaa/images/main-bg.jpg HTTP/1.1\r\n
    Host: webstaff.itn.liu.se\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36\r\n
    Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://webstaff.itn.liu.se/~piede/courses/aaa/images/main-bg.jpg]
    [HTTP request 1/1]
    [Response in frame: 853]
```

16. The servers response code is “401 Unauthorized”. See image above



```
No.      Time      Source                                Destination              Protocol  Length  Info
     119 2.234394  2001:6b0:17:fc09:ac76:a4ed:515:6730   2a02:2350:5:103:808…     HTTP      529 GET /education/courses/tnm031 HTTP/1.1
     130 2.248132  2a02:2350:5:103:808b:e386:adb9:a9aa   2001:6b0:17:fc09:ac…     HTTP      750 HTTP/1.1 401 Unauthorized  (text/html)
     257 2.991001  2001:6b0:17:fc09:ac76:a4ed:515:6730   2a02:2350:5:103:808…     HTTP      602 GET /education/courses/tnm031 HTTP/1.1
     265 3.008340  2a02:2350:5:103:808b:e386:adb9:a9aa   2001:6b0:17:fc09:ac…     HTTP      623 HTTP/1.1 301 Moved Permanently  (text/html)
     805 3.839142  2001:6b0:17:fc09:ac76:a4ed:515:6730   2a02:2350:5:103:808…     HTTP      478 GET /education/courses/tnm031/images/img18.JPG HTTP/1.1
     827 3.856023  2a02:2350:5:103:808b:e386:adb9:a9aa   2001:6b0:17:fc09:ac…     HTTP      657 HTTP/1.1 301 Moved Permanently  (text/html)
     851 3.887355  10.253.254.7                          130.236.132.7            HTTP      414 GET /~piede/courses/aaa/images/main-bg.jpg HTTP/1.1
     853 3.891169  130.236.132.7                         10.253.254.7             HTTP      552 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 257: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface \Device\NPF_{FA5336DF-B18D-42AD-BCE5-185996DAA703}, id 0
> Ethernet II, Src: LiteonTe_00:89:61 (c8:ff:28:00:89:61), Dst: Fortinet_09:00:22 (00:09:0f:09:00:22)
> Internet Protocol Version 6, Src: 2001:6b0:17:fc09:ac76:a4ed:515:6730, Dst: 2a02:2350:5:103:808b:e386:adb9:a9aa
> Transmission Control Protocol, Src Port: 53062, Dst Port: 80, Seq: 456, Ack: 677, Len: 528
v Hypertext Transfer Protocol
  > GET /education/courses/tnm031 HTTP/1.1\r\n
    Host: dellacqua.se\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  v Authorization: Basic cGl6emE6bWFyZ2hlcml0YQ==\r\n
      Credentials: pizza:margherita
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://dellacqua.se/education/courses/tnm031]
    [HTTP request 2/3]
    [Prev request in frame: 119]
    [Response in frame: 265]
    [Next request in frame: 805]
```

17. We can see Authorization: “Credentials: pizza : margherita”. See image above

## Part 6 (Optional):

18. *ring ring*, “Test”(or Check), “One”, “Two”, “Three”