

Bryan Arnold

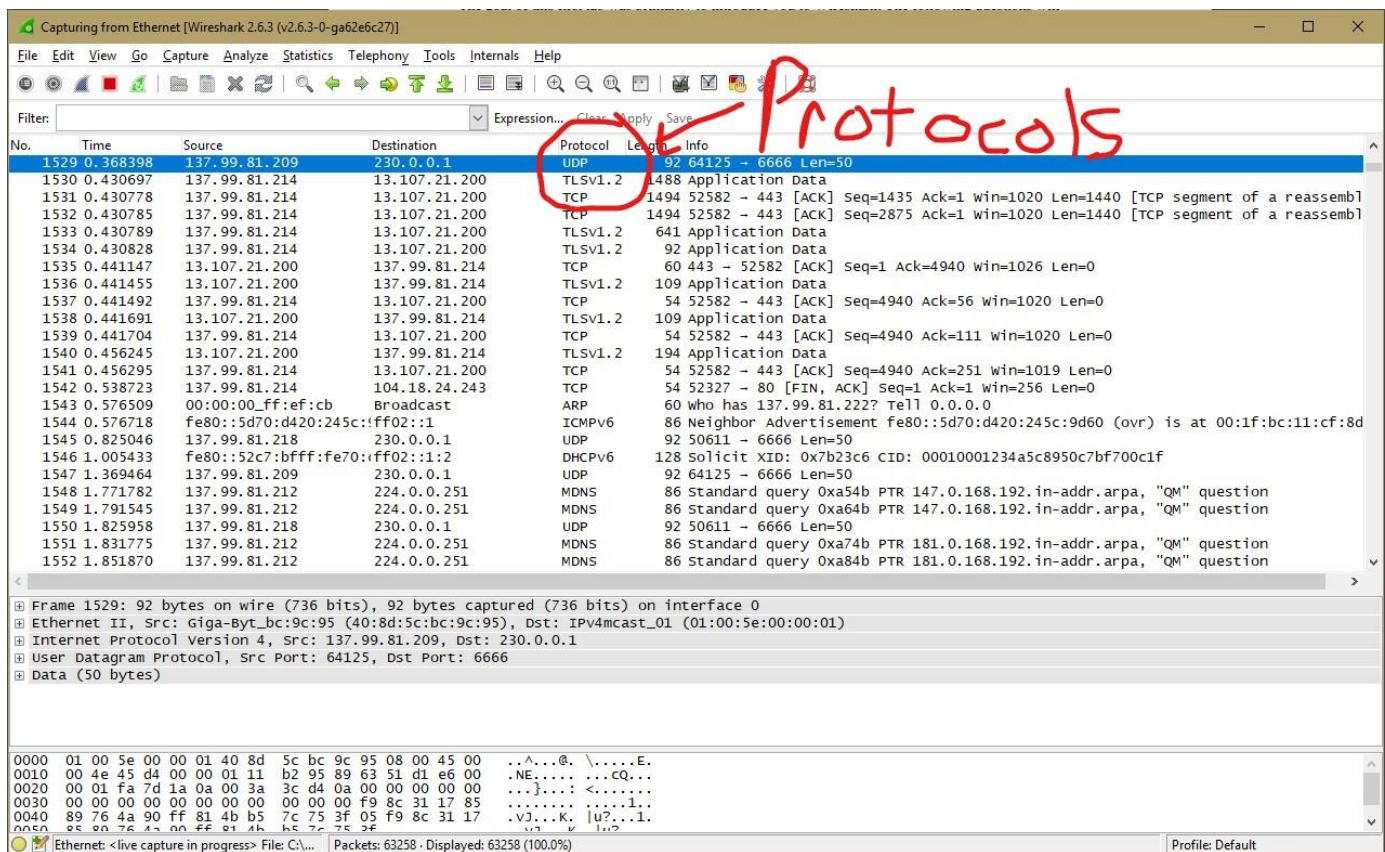
CSE 3300

10/5/18

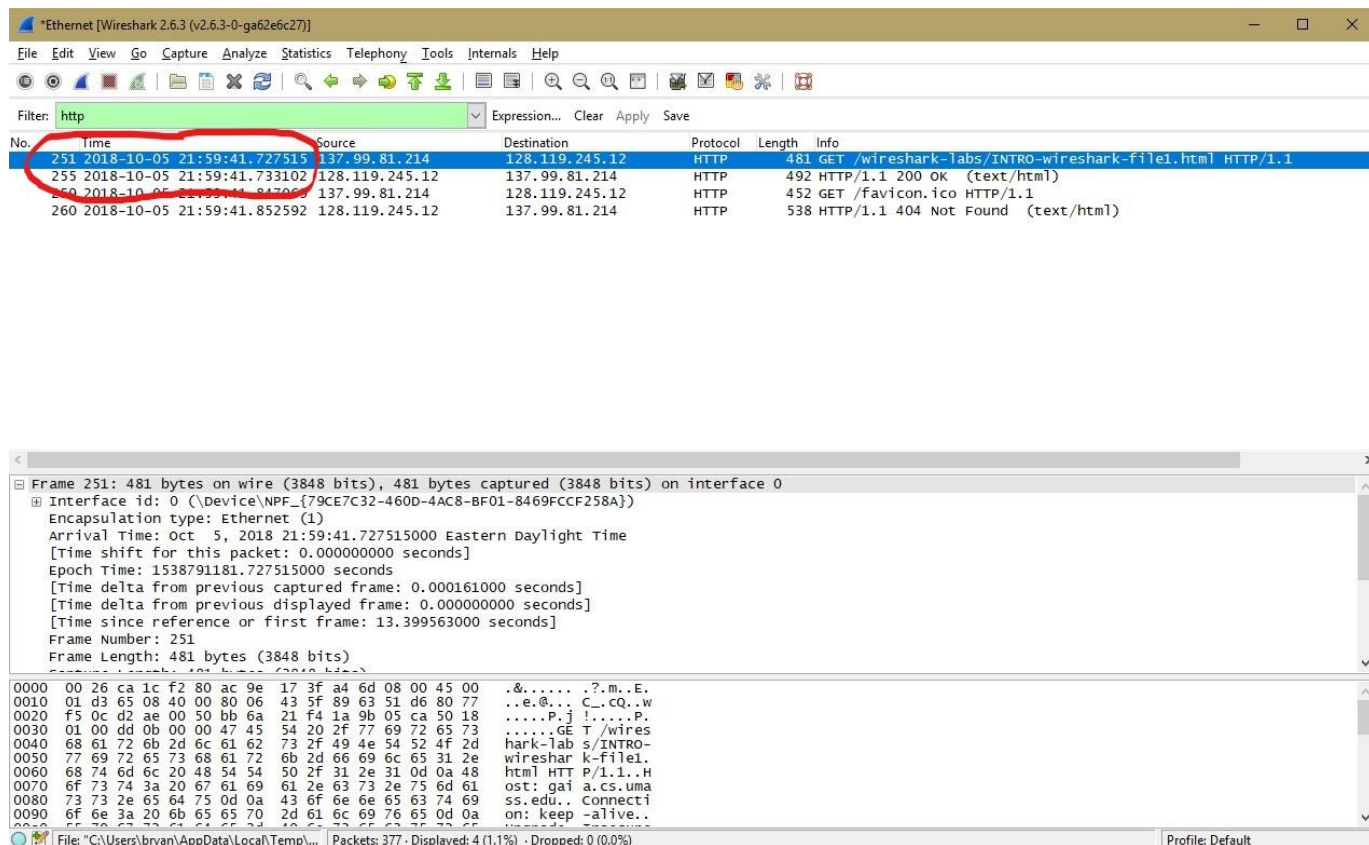
Programming Assignment 1

## Part 1: Getting Started

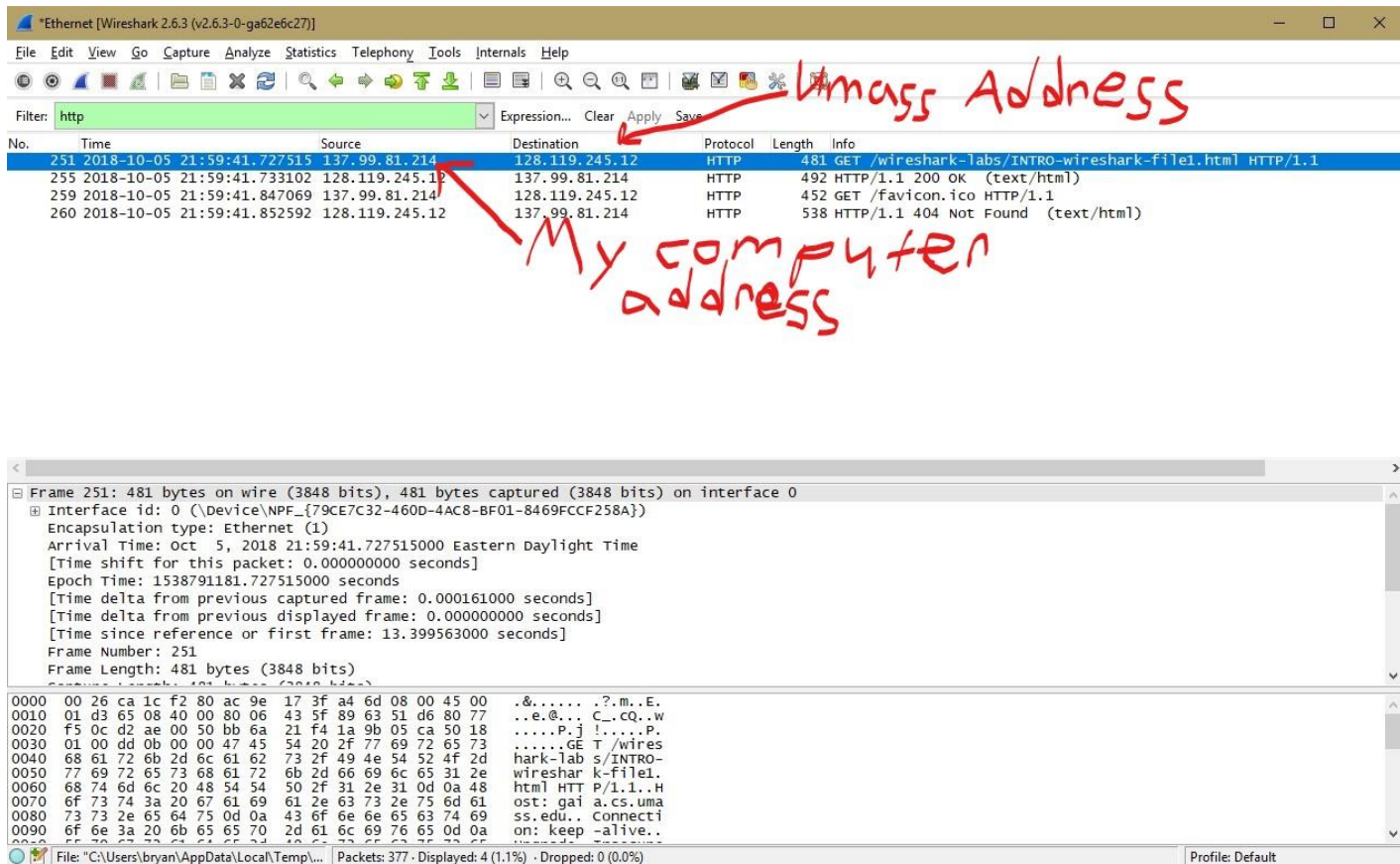
- 1) Three protocols that appeared in my unfiltered packet-listing window in the protocol column were the UDP, TLSv1.2, and TCP protocols. Here you can see them circled in red:



- 2) The GET request was sent at 21:59:41.727515 and the OK response was received at 21:59:41.733102. So, the time it took for the GET request to be sent and then receive an OK response was approximately 0.005587 seconds. Here you can see the times of each:



- 3) The Internet address for gaia.cs.umass.edu 128.119.245.12 and the Internet address of my computer is 137.99.81.214. Here you can see the addresses of both:



#### 4) Here is the printed packet information for the GET request:

```
No. Time Source Destination Protocol Length
Info
251 2018-10-05 21:59:41.727515 137.99.81.214 128.119.245.12 HTTP 481
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 251: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on
interface 0
Interface id: 0 (\Device\NPF_{79CE7C32-460D-4AC8-BF01-8469FCCF258A})
Encapsulation type: Ethernet (1)
Arrival Time: Oct 5, 2018 21:59:41.727515000 Eastern Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1538791181.727515000 seconds
[Time delta from previous captured frame: 0.000161000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 13.399563000 seconds]
Frame Number: 251
Frame Length: 481 bytes (3848 bits)
Capture Length: 481 bytes (3848 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
```

[Coloring Rule String: http || tcp.port == 80 || http2]  
Ethernet II, Src: AsustekC\_3f:a4:6d (ac:9e:17:3f:a4:6d), Dst: Cisco\_1c:f2:80 (00:26:ca:1c:f2:80)  
Destination: Cisco\_1c:f2:80 (00:26:ca:1c:f2:80)  
Source: AsustekC\_3f:a4:6d (ac:9e:17:3f:a4:6d)  
Type: IPv4 (0x0800)  
Internet Protocol Version 4, Src: 137.99.81.214, 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: 467  
Identification: 0x6508 (25864)  
Flags: 0x4000, Don't fragment  
Time to live: 128  
Protocol: TCP (6)  
Header checksum: 0x435f [validation disabled]  
[Header checksum status: Unverified]  
Source: 137.99.81.214  
Destination: 128.119.245.12  
Transmission Control Protocol, Src Port: 53934, Dst Port: 80, Seq: 1, Ack: 1, Len: 427  
Source Port: 53934  
Destination Port: 80  
[Stream index: 11]  
[TCP Segment Len: 427]  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 428 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window size value: 256  
[Calculated window size: 65536]  
[Window size scaling factor: 256]  
Checksum: 0xdd0b [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
[SEQ/ACK analysis]  
[Timestamps]  
TCP payload (427 bytes)  
Hypertext Transfer Protocol  
GET /wireshark-labs/INTRO-wireshark-file1.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/69.0.3497.100 Safari/537.36\r\n  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8\r\n  
Accept-Encoding: gzip, deflate\r\n  
Accept-Language: en-US,en;q=0.9\r\n  
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]  
[HTTP request 1/2]

[Response in frame: 255]  
[Next request in frame: 259]

Here is the printed packet information from the OK response:

No. Time Source Destination Protocol Length  
Info  
255 2018-10-05 21:59:41.733102 128.119.245.12 137.99.81.214 HTTP 492  
HTTP/1.1 200 OK (text/html)  
Frame 255: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on  
interface 0  
Interface id: 0 (\Device\NPF\_{79CE7C32-460D-4AC8-BF01-8469FCCF258A})  
Encapsulation type: Ethernet (1)  
Arrival Time: Oct 5, 2018 21:59:41.733102000 Eastern Daylight Time  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1538791181.733102000 seconds  
[Time delta from previous captured frame: 0.000500000 seconds]  
[Time delta from previous displayed frame: 0.005587000 seconds]  
[Time since reference or first frame: 13.405150000 seconds]  
Frame Number: 255  
Frame Length: 492 bytes (3936 bits)  
Capture Length: 492 bytes (3936 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]  
[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]  
Ethernet II, Src: Cisco\_1c:f2:80 (00:26:ca:1c:f2:80), Dst: AsustekC\_3f:a4:6d  
(ac:9e:17:3f:a4:6d)  
Destination: AsustekC\_3f:a4:6d (ac:9e:17:3f:a4:6d)  
Source: Cisco\_1c:f2:80 (00:26:ca:1c:f2:80)  
Type: IPv4 (0x0800)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 137.99.81.214  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 478  
Identification: 0xf62f (63023)  
Flags: 0x4000, Don't fragment  
Time to live: 50  
Protocol: TCP (6)  
Header checksum: 0x002d [validation disabled]  
[Header checksum status: Unverified]  
Source: 128.119.245.12  
Destination: 137.99.81.214  
Transmission Control Protocol, Src Port: 80, Dst Port: 53934, Seq: 1, Ack:  
428, Len: 438  
Source Port: 80  
Destination Port: 53934  
[Stream index: 11]  
[TCP Segment Len: 438]  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 439 (relative sequence number)]  
Acknowledgment number: 428 (relative ack number)  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window size value: 237

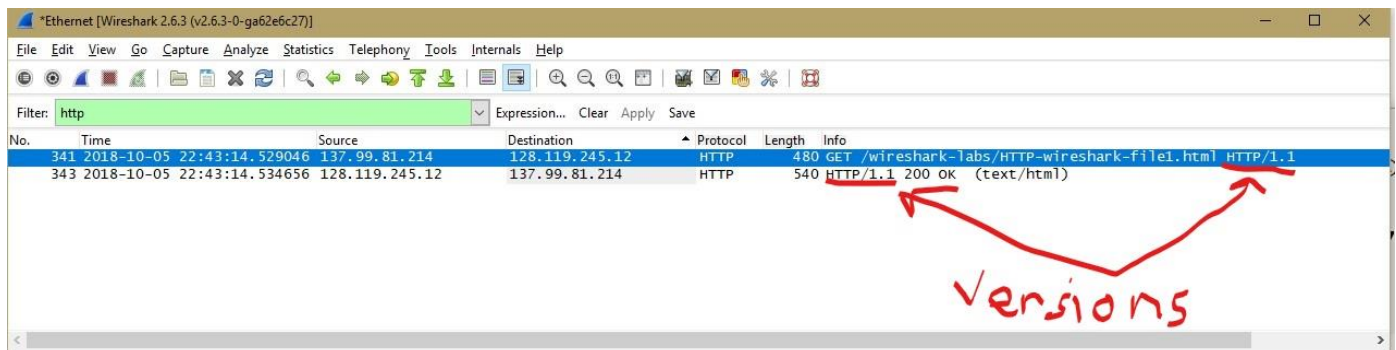
```

[Calculated window size: 30336]
[Window size scaling factor: 128]
Checksum: 0x1625 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (438 bytes)
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sat, 06 Oct 2018 01:59:38 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10
Perl/v5.16.3\r\n
Last-Modified: Fri, 05 Oct 2018 05:59:01 GMT\r\n
ETag: "51-57774f7d96258"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\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: 0.005587000 seconds]
[Request in frame: 251]
[Next request in frame: 259]
[Next response in frame: 260]
File Data: 81 bytes
Line-based text data: text/html (3 lines)

```

## **Part 2: HTTP**

- 1) The HTTP version on my browser and the server are both 1.1. Here you can see the version numbers:



- 2) The languages my browsers can accept onto the server are en-US, en; q=0.9. Here is the header that indicates so:



```

Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
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/69.0.3497.100 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng/*;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://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 343]

```

3) The Internet address for gaia.cs.umass.edu 128.119.245.12 and the Internet address of my computer is 137.99.81.214. Here you can see the addresses of both:

```

*Ethernet [Wireshark 2.6.3 (v2.6.3-0-ga62e6c27)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
No. Time Source Destination Protocol Length Info
341 2018-10-05 22:43:14.529046 137.99.81.214 128.119.245.12 HTTP 480 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
343 2018-10-05 22:43:14.534656 128.119.245.12 137.99.81.214 HTTP 540 HTTP/1.1 200 OK (text/html)

```

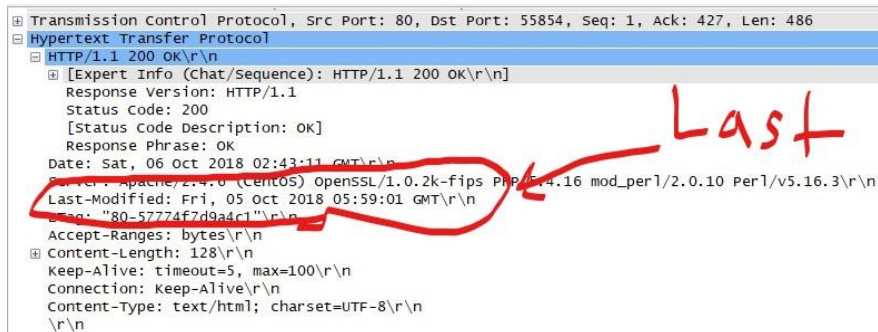
4) The status code returned from the browser is 200. Here you can see the returned status code for OK:

```

Transmission Control Protocol, Src Port: 80, Dst Port: 55854, Seq: 1, Ack: 427, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Sat, 06 Oct 2018 02:43:11 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Fri, 05 Oct 2018 05:59:01 GMT\r\n
ETag: "80-57774f7d9a4c1"\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

```

5) The HTML file from the server was last modified on October 5<sup>th</sup>, 2018 at 5:59:01 GMT. Here is the header that indicates so:

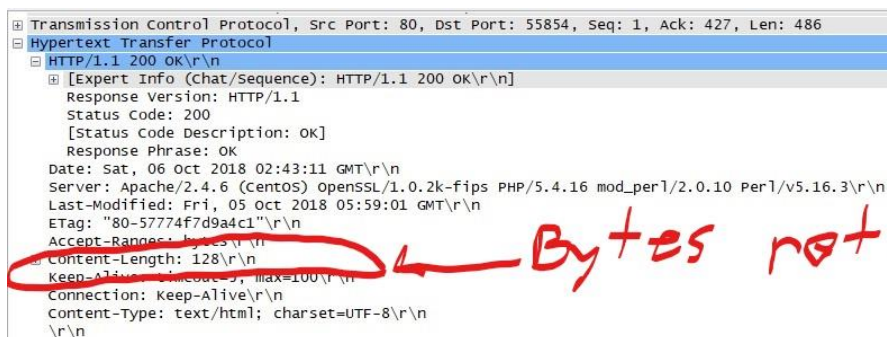


```

Transmission Control Protocol, Src Port: 80, Dst Port: 55854, Seq: 1, Ack: 427, Len: 486
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Sat, 06 Oct 2018 02:43:11 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Fri, 05 Oct 2018 05:59:01 GMT\r\n
    ETag: "80-57774f7d9a4c1"\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

```

6) There are 128 bytes being returned from the server. Here is the header that indicates so:

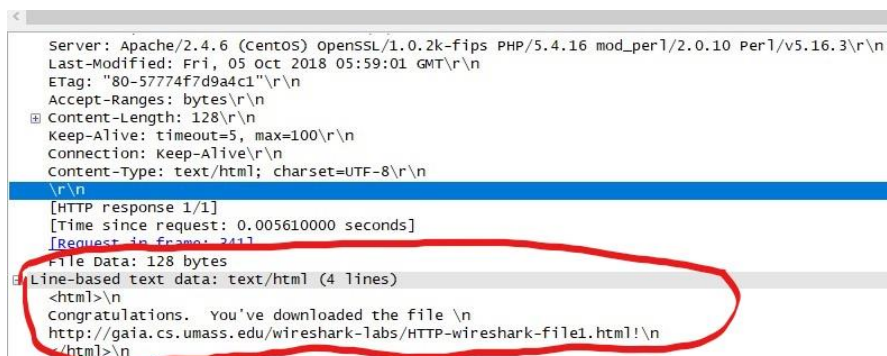


```

Transmission Control Protocol, Src Port: 80, Dst Port: 55854, Seq: 1, Ack: 427, Len: 486
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Sat, 06 Oct 2018 02:43:11 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Fri, 05 Oct 2018 05:59:01 GMT\r\n
    ETag: "80-57774f7d9a4c1"\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

```

7) I do not see any additional headers by inspecting the raw data of the packet. Here you can see there are no additional headers in the data:



```

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Fri, 05 Oct 2018 05:59:01 GMT\r\n
ETag: "80-57774f7d9a4c1"\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 1/1]
[Time since request: 0.005610000 seconds]
[Request in file: 241]
File Data: 128 bytes
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

```

## Part 3: HTTP Conditional GET

8) There is no IF-MODIFIED-SINCE header in the first GET:



```

Transmission Control Protocol, Src Port: 56934, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
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]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
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/69.0.3497.100 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;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://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 316]

```

- 9) The server did explicitly return the contents of the file because in the raw data of the file I can see what was displayed on the webpage when I entered the URL:

```

Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.005723000 seconds]
[Request in frame: 312]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
\r\n
<html>\r\n
\r\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\r\n
This file's last modification date will not change. <p>\r\n
Thus if you download this multiple times on your browser, a complete copy <br>\r\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\r\n
field in your browser's HTTP GET request to the server.\r\n
\r\n
</html>\r\n

```

- 10) Yes, there is an IF-MODIFIED-SINCE header and it contains a date on October 5<sup>th</sup>, 2018 at 5:59:01 GMT:

```

[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\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/69.0.3497.100 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5774f/d99521"\r\n
If-Modified-Since: Fri, 05 Oct 2018 05:59:01 GMT\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: 435]

```

- 11) The HTTP status code is 304 and the phrase is “Not Modified”. There was also no contents/data of the file explicitly returned as I cannot view the raw data of the file in Wireshark:

```
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 137.99.81.214
Transmission Control Protocol, Src Port: 80, Dst Port: 56940, Seq: 1, Ack: 539, Len: 240
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
      Date: Sat, 27 Oct 2018 03:13:27 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
      Connection: Keep-Alive\r\n
      Keep-Alive: timeout=5, max=100\r\n
      ETag: "173-57774f7d99521"\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.005601000 seconds]
      [Request in frame: 431]
```

Code/phrase  
No data below

## Part 4: Long Documents

12) My browser sent 1 HTTP GET requests and the 1<sup>st</sup> packet has the GET message:

\*Ethernet [Wireshark 2.6.3 (v2.6.3-0-ga62e6c27)]

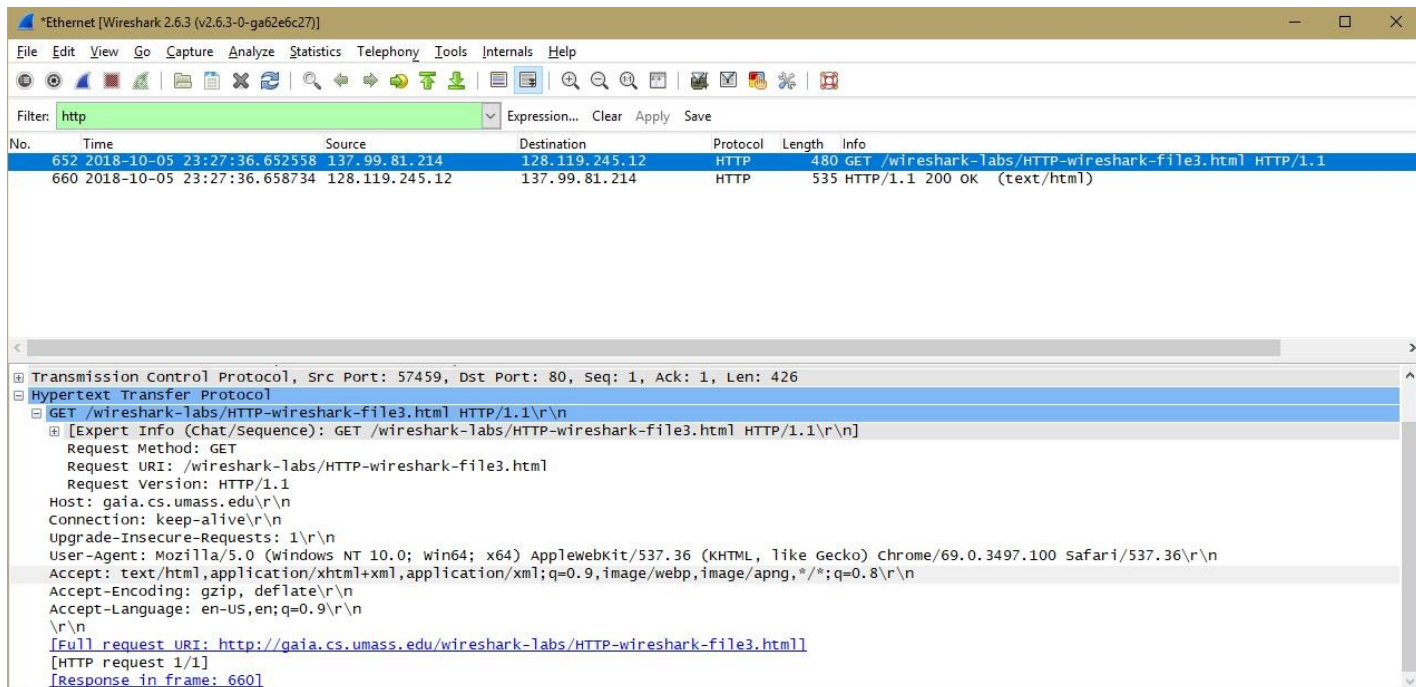
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

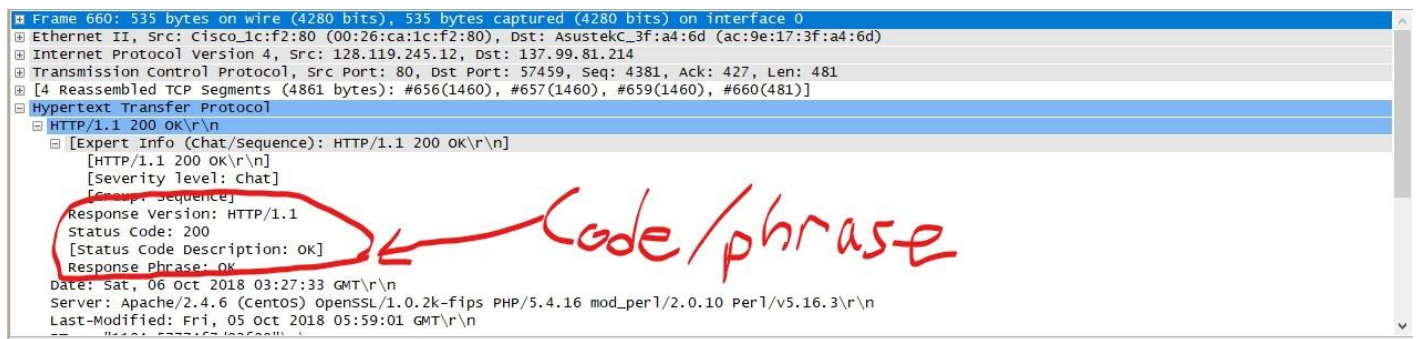
No.	Time	Source	Destination	Protocol	Length	Info
652	2018-10-05 23:27:36.652558	137.99.81.214	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
660	2018-10-05 23:27:36.658734	128.119.245.12	137.99.81.214	HTTP	535	HTTP/1.1 200 OK (text/html)

```
Transmission Control Protocol, Src Port: 57459, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.html
      Request version: HTTP/1.1
      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/69.0.3497.100 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;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://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
      [HTTP request 1/1]
      [Response in frame: 660]
```

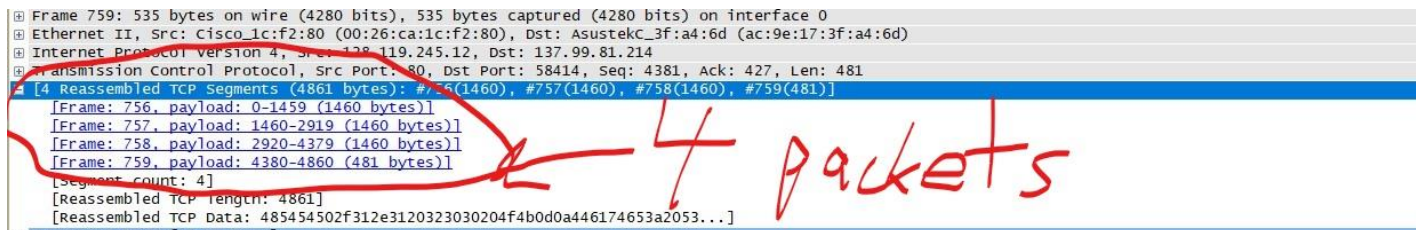
13) The 1<sup>st</sup> packet has the phrase associated with the GET request:



14) The status code is 200 and the phrase is “OK”:



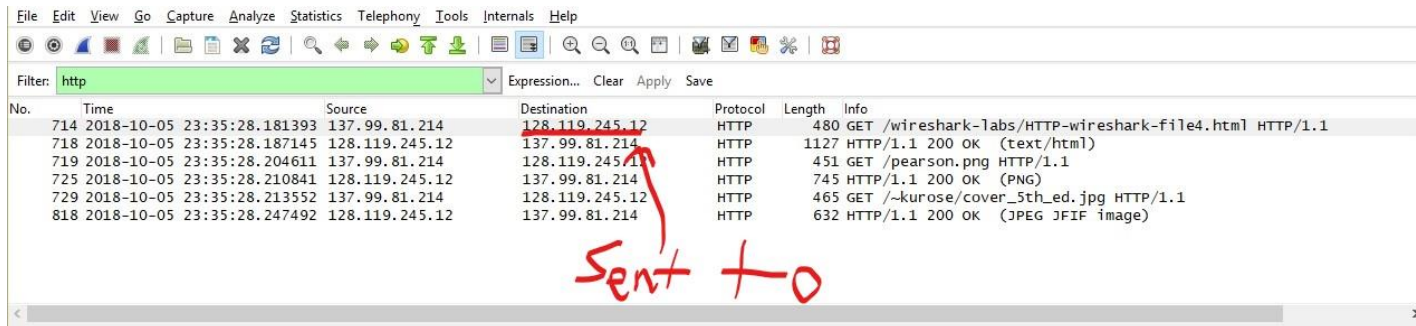
15) Four packets were needed to carry all the data in the trace:



## PART 5: Documents with Embedded Objects

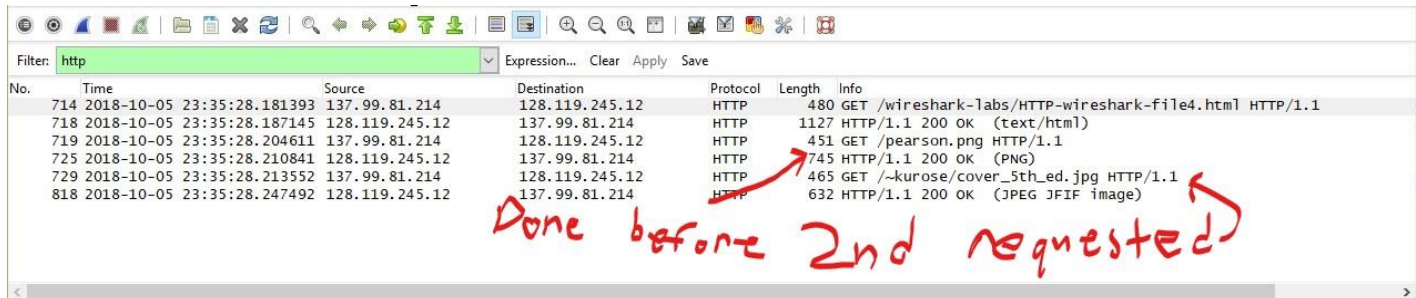


- 16) There was a total of three GET requests sent to the server, and all GET requests were sent to the same Internet address at 128.119.245.12:



No.	Time	Source	Destination	Protocol	Length	Info
714	2018-10-05 23:35:28.181393	137.99.81.214	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
718	2018-10-05 23:35:28.187145	128.119.245.12	137.99.81.214	HTTP	1127	HTTP/1.1 200 OK (text/html)
719	2018-10-05 23:35:28.204611	137.99.81.214	128.119.245.12	HTTP	451	GET /pearson.png HTTP/1.1
725	2018-10-05 23:35:28.210841	128.119.245.12	137.99.81.214	HTTP	745	HTTP/1.1 200 OK (PNG)
729	2018-10-05 23:35:28.213552	137.99.81.214	128.119.245.12	HTTP	465	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
818	2018-10-05 23:35:28.247492	128.119.245.12	137.99.81.214	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

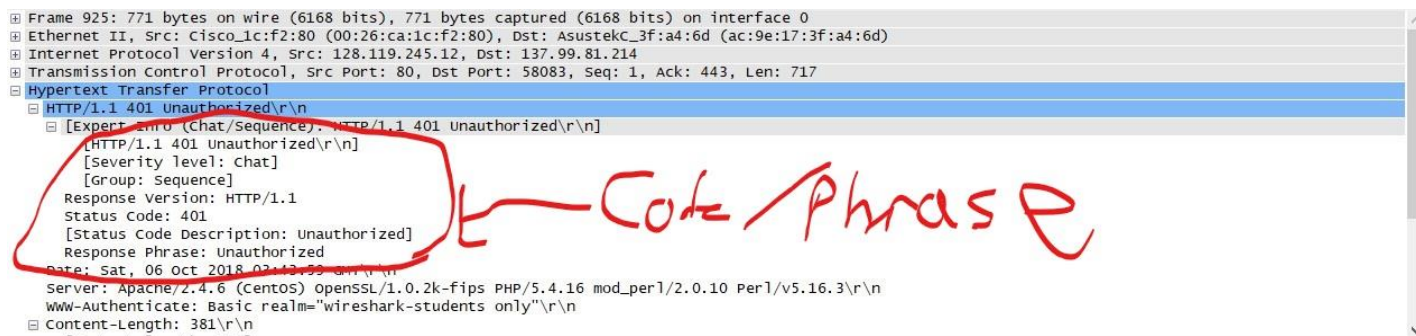
- 17) The images were downloaded serially. You can see this in the order in which they were downloaded as well as the time. The first images' get request got a response before the second images' GET request was even sent out, meaning the first image was downloaded before the second image was even requested:



No.	Time	Source	Destination	Protocol	Length	Info
714	2018-10-05 23:35:28.181393	137.99.81.214	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
718	2018-10-05 23:35:28.187145	128.119.245.12	137.99.81.214	HTTP	1127	HTTP/1.1 200 OK (text/html)
719	2018-10-05 23:35:28.204611	137.99.81.214	128.119.245.12	HTTP	451	GET /pearson.png HTTP/1.1
725	2018-10-05 23:35:28.210841	128.119.245.12	137.99.81.214	HTTP	745	HTTP/1.1 200 OK (PNG)
729	2018-10-05 23:35:28.213552	137.99.81.214	128.119.245.12	HTTP	465	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
818	2018-10-05 23:35:28.247492	128.119.245.12	137.99.81.214	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

## Part 6: Authentication

- 18) The status code of the response is 401 and the phrase is "Unauthorized":



Frame	Time	Source	Destination	Protocol	Length	Info
925	2018-10-05 23:35:28.247492	137.99.81.214	128.119.245.12	HTTP	771	HTTP/1.1 401 Unauthorized\r\n

Code / Phrase

19) In the second HTTP GET request, the new header that is included is an “Authorization” header with the contents being “Basic eGNkc2Zn0mFzZGZ”:



The image shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows a packet of type HTTP. The packet details pane on the right shows the structure of the request. The 'Authorization' header is highlighted with a red circle, and a red arrow points to it with the handwritten text 'New header'. The 'Authorization' header value is 'Basic eGNkc2Zn0mFzZGZ'. The 'Credentials' field is also visible, showing 'xcdfn:asdfa'. The 'User-Agent' field is 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36'. The 'Accept' field is 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8'. The 'Accept-Encoding' field is 'gzip, deflate'. The 'Accept-Language' field is 'en-US,en;q=0.9'. The 'Full request URI' is 'http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html'. The packet is labeled '[HTTP request 1/1]'.

```
[GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Authorization: Basic eGNkc2Zn0mFzZGZ\r\n
Credentials: xcdfn:asdfa
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;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://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
```