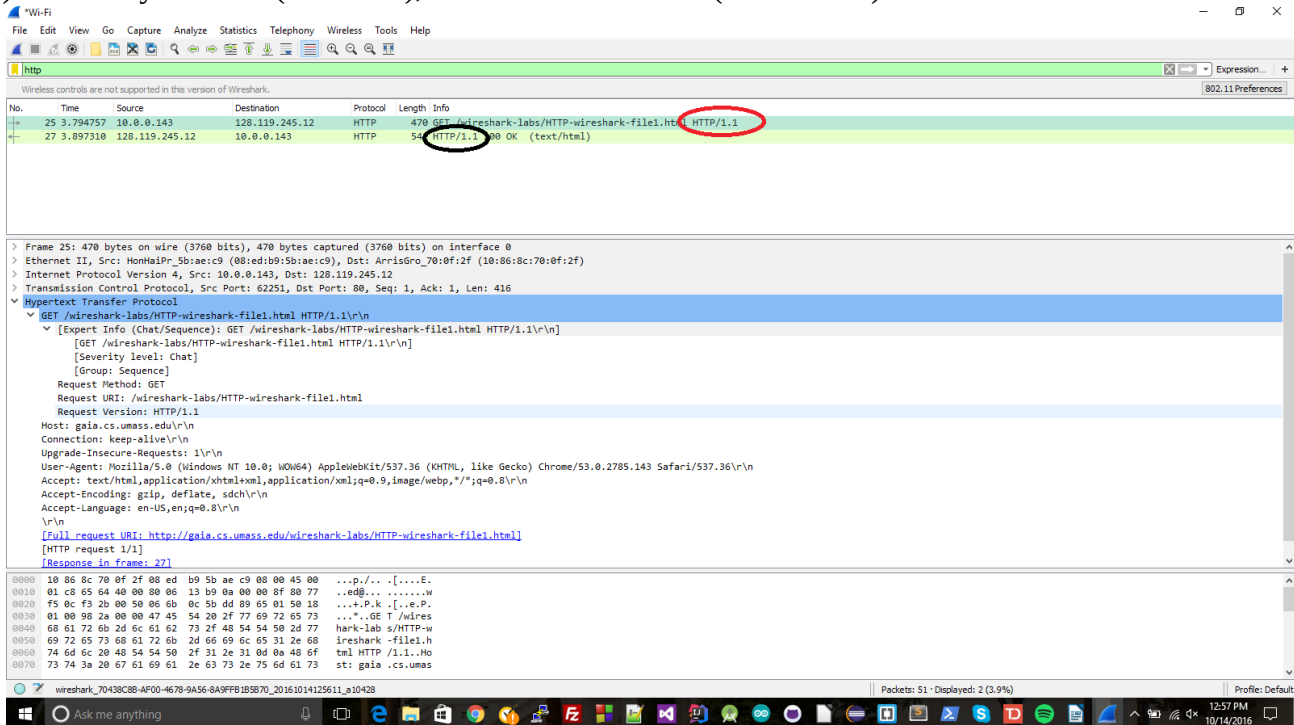
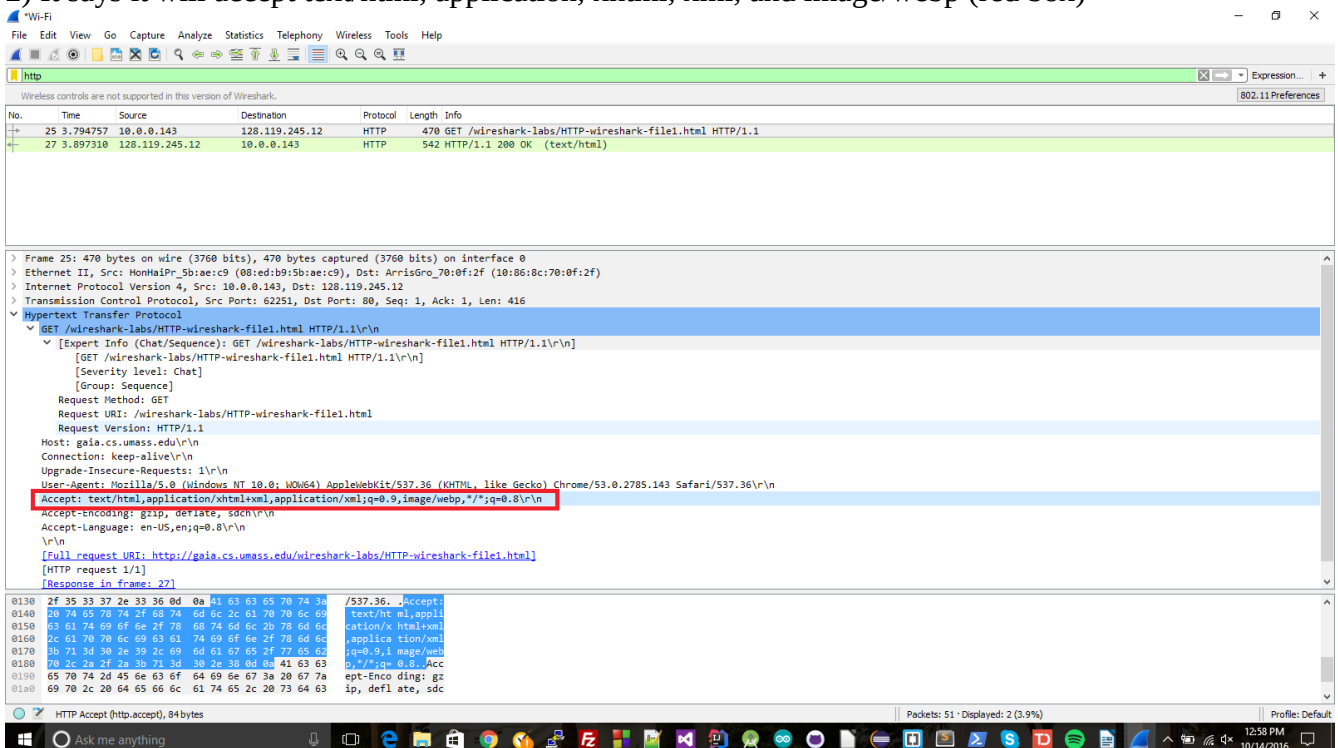


1) 1.1 for my browser (red circle), and 1.1 for the server (black circle)



2) It says it will accept text/html, application, xhtml, xml, and image/webp (red box)



3) My IP address is 10.0.0.143 (black box). The IP address of the server is 128.119.245.12 (red box)

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list at the top shows two packets: a GET request (No. 25) and an HTTP 200 OK response (No. 27). The packet details pane for packet 25 is expanded, showing the Hypertext Transfer Protocol section. The request method is GET, and the URI is /wireshark-labs/HTTP-wireshark-file1.html. The status code is 200 OK. The packet bytes pane at the bottom shows the raw data of the response, including the status line: HTTP/1.1 200 OK (text/html).

4) 200-OK (orange circle)

The screenshot shows a Wireshark capture of an HTTP 200-OK response. The packet list at the top shows two packets: a GET request (No. 25) and an HTTP 200 OK response (No. 27). The packet details pane for packet 27 is expanded, showing the Hypertext Transfer Protocol section. The status code is 200 OK, which is circled in orange. The response phrase is OK. The packet bytes pane at the bottom shows the raw data of the response, including the status line: HTTP/1.1 200 OK (text/html).

5) The last modified time is Fri, 14 Oct 2016, 5:59:01 GMT (purple box)

Wireshark packet capture showing an HTTP GET request. The packet list shows packet 27 selected. The packet details pane shows the Hypertext Transfer Protocol section with the Last-Modified header highlighted in a purple box.

Frame 27: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0

Ethernet II, Src: ArrisGro_70:0f:2f (10:06:8c:70:0f:2f), Dst: MonHaiPr_5b:ae:c9 (08:ed:b9:5b:ae:c9)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.143

Transmission Control Protocol, Src Port: 80, Dst Port: 62251, Seq: 1, Ack: 417, Len: 488

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]

Request Version: HTTP/1.1

Status Code: 200

Response Phrase: OK

Date: Fri, 14 Oct 2016 19:56:15 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n

Last-Modified: Fri, 14 Oct 2016 05:59:01 GMT\r\n

Etag: "80-53ecce48a795"\r\n

Accept-Ranges: bytes\r\n

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

\r\n

6) According to the HTTP header, 128 bytes (red box)

Wireshark packet capture showing an HTTP GET request. The packet list shows packet 27 selected. The packet details pane shows the Hypertext Transfer Protocol section with the Content-Length header highlighted in a red box.

Frame 27: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0

Ethernet II, Src: ArrisGro_70:0f:2f (10:06:8c:70:0f:2f), Dst: MonHaiPr_5b:ae:c9 (08:ed:b9:5b:ae:c9)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.143

Transmission Control Protocol, Src Port: 80, Dst Port: 62251, Seq: 1, Ack: 417, Len: 488

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]

Request Version: HTTP/1.1

Status Code: 200

Response Phrase: OK

Date: Fri, 14 Oct 2016 19:56:15 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n

Last-Modified: Fri, 14 Oct 2016 05:59:01 GMT\r\n

Etag: "80-53ecce48a795"\r\n

Accept-Ranges: bytes\r\n

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

\r\n

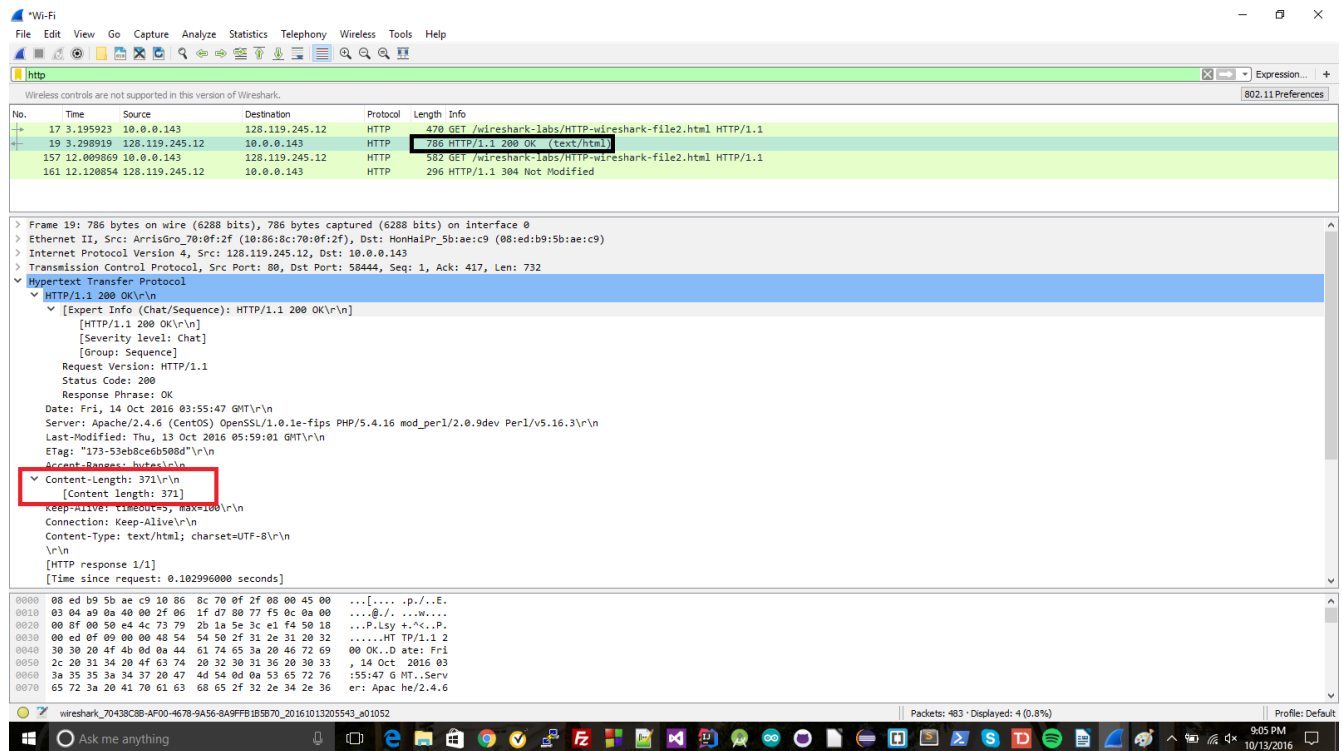
7) There were no headers in the data that weren't already displayed in the packet listing window, though there were some headers that weren't in the data, such as the Full Request URI, the HTTP request number, and the Response in frame. These are in the red box, while the black box shows that the last header included in the raw data was Accepted Languages.

Wireshark packet capture showing an HTTP GET request. The packet list shows packet 27 selected. The packet details pane shows the HTTP request structure. The packet bytes pane shows the raw data with a red box highlighting the full request URI and response in frame, and a black box highlighting the 'Accept-Language' header.

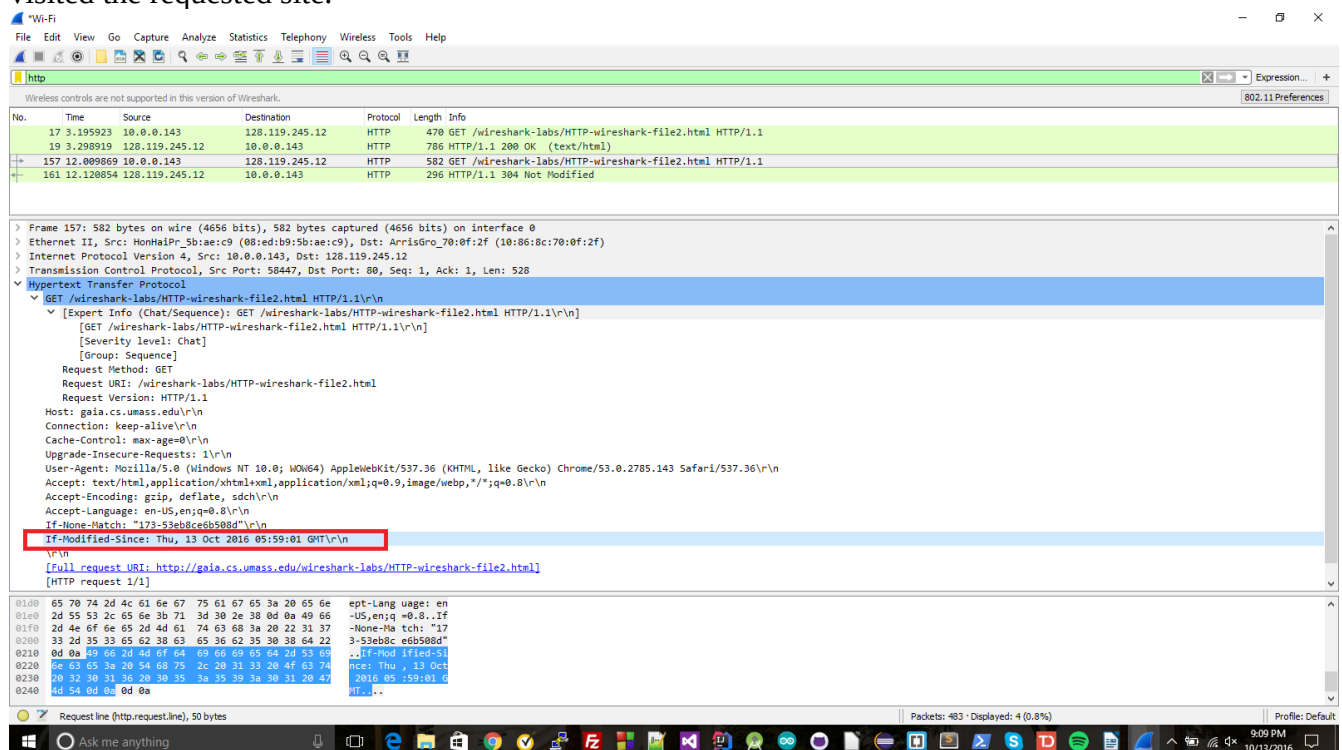
8) There is not:

Wireshark packet capture showing an HTTP GET request. The packet list shows packet 19 selected. The packet details pane shows the HTTP request structure. The packet bytes pane shows the raw data with a red box highlighting the full request URI and response in frame, and a black box highlighting the 'Accept-Language' header.

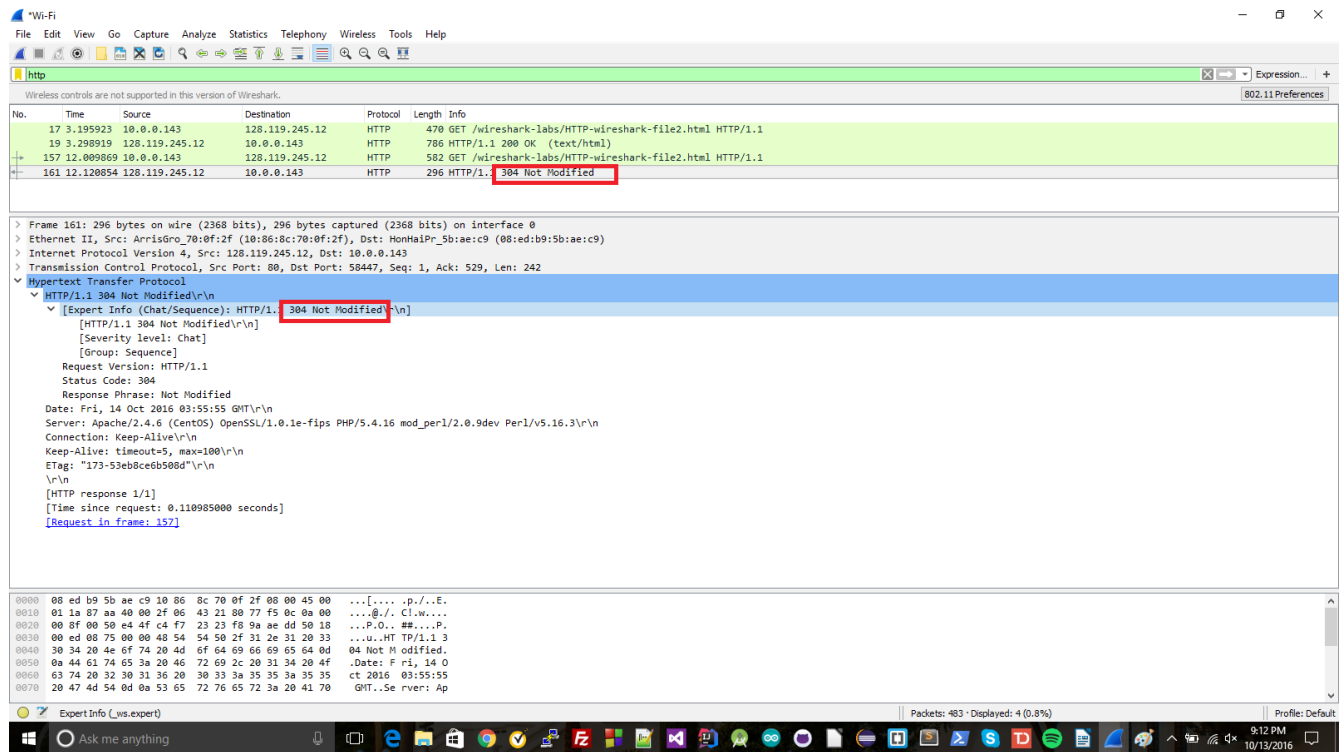
9) It did return the contents of the file: I can tell because the red square contains a content length section saying there was content sent, and because of the HTTP response, which was 200 OK, meaning that the response contains the requested item (in this case an html file)



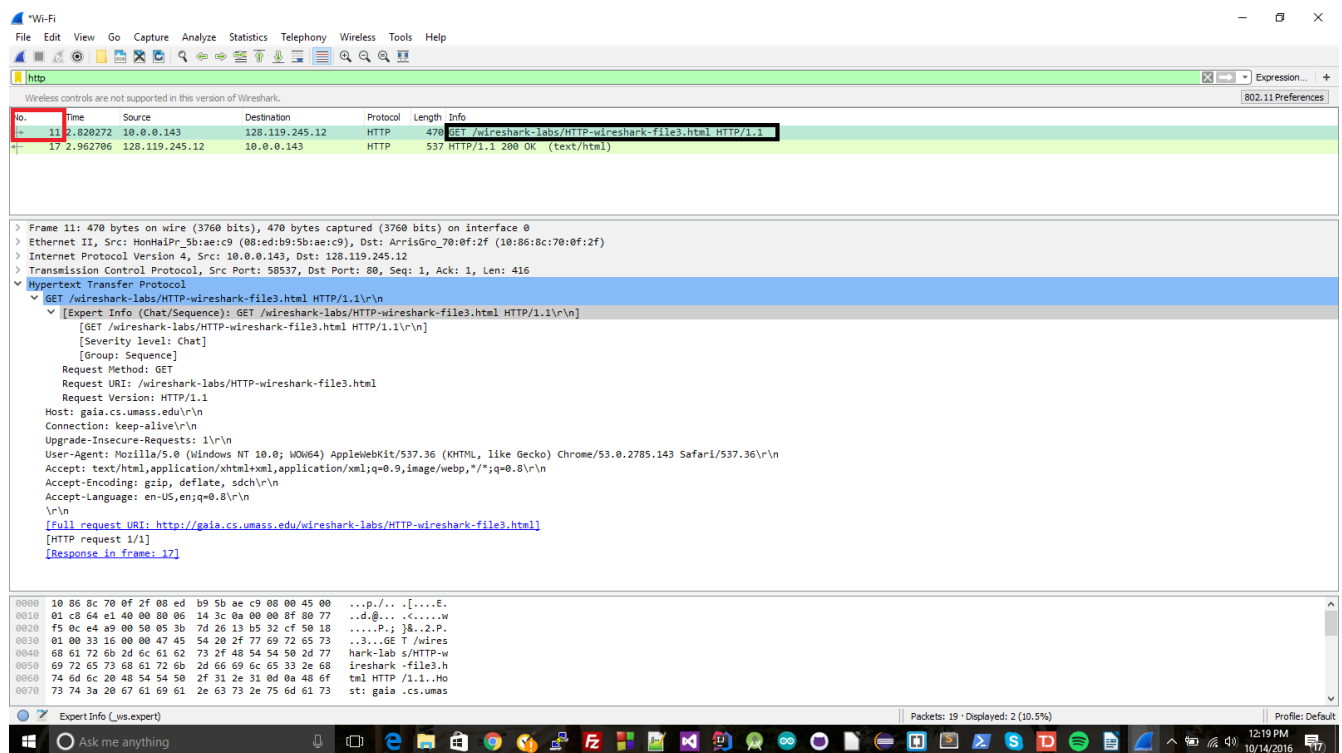
10) There is; the date/time given is 13 Oct 2016, 05:59:01 GMT. This would be the time that I last visited the requested site.



11) The response code is 304 Not Modified. This means the server did not return the contents of the file, because it had not been modified since the last date/time it had been viewed.



12) There was one GET message sent (black box). The packet number was number 11.



13) The packet number response is 17 (purple box)

The screenshot shows the Wireshark interface with packet 17 selected in the packet list. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
11	2.820272	10.0.0.143	128.119.245.12	HTTP	470	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
17	2.962706	128.119.245.12	10.0.0.143	HTTP	537	HTTP/1.1 200 OK (text/html)

The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the full request and response details. The status bar at the bottom indicates 'Packets: 19 - Displayed: 2 (10.5%)'.

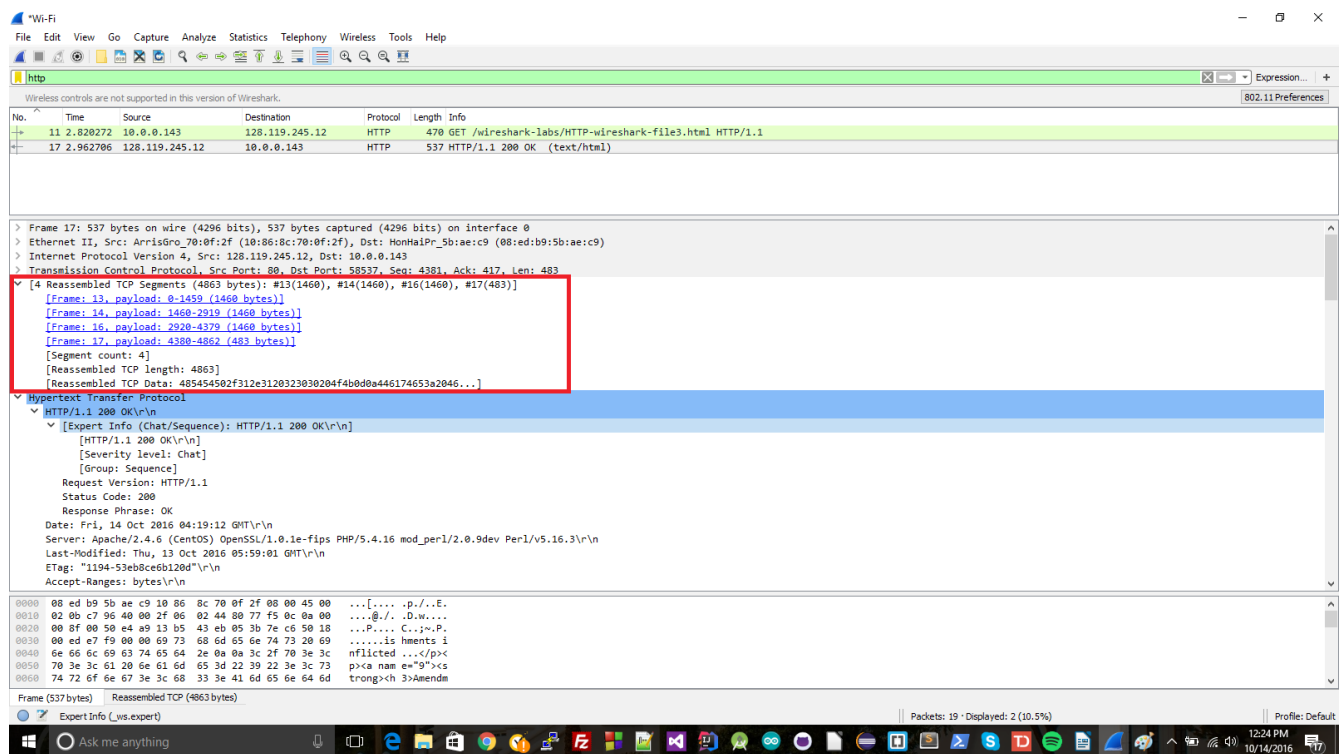
14) The status code and phrase is 200 OK (orange box)

The screenshot shows the Wireshark interface with packet 17 selected. The packet list table is as follows:

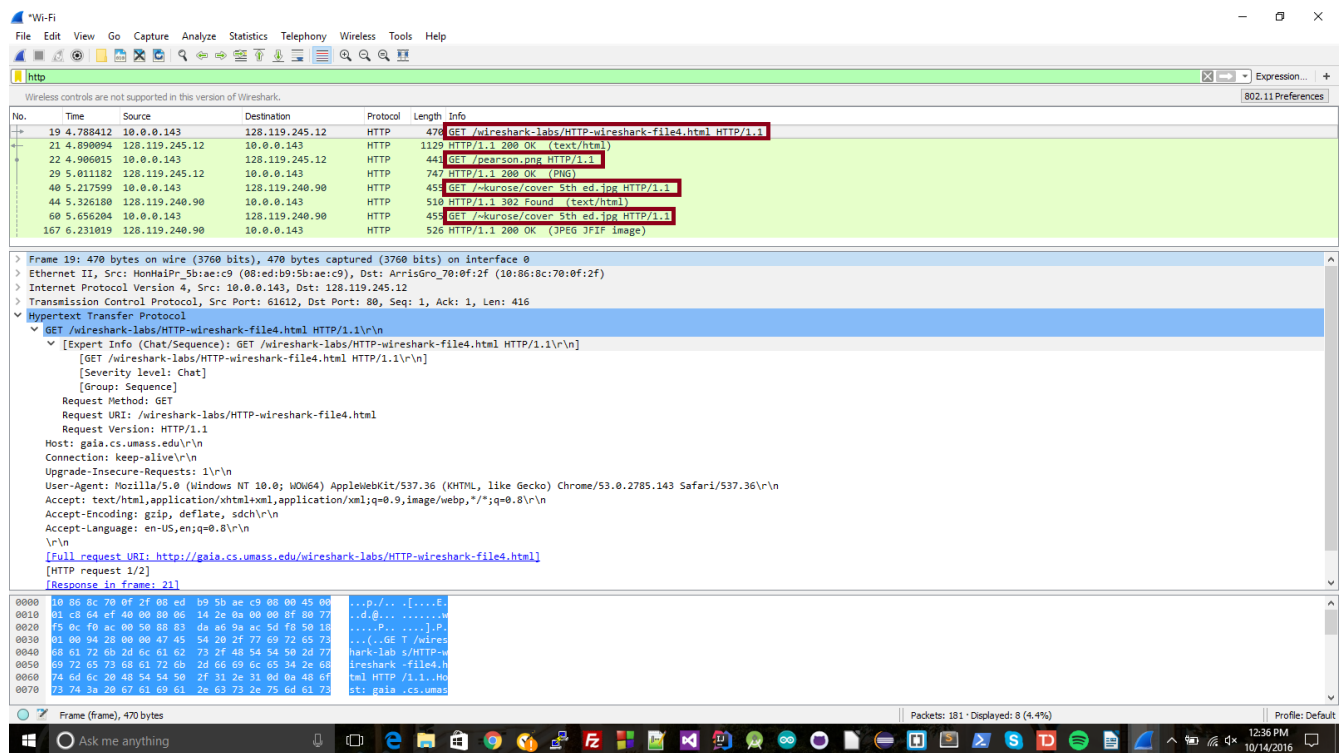
No.	Time	Source	Destination	Protocol	Length	Info
11	2.820272	10.0.0.143	128.119.245.12	HTTP	470	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
17	2.962706	128.119.245.12	10.0.0.143	HTTP	537	HTTP/1.1 200 OK (text/html)

The packet details pane shows the Hypertext Transfer Protocol section expanded. The status code and phrase '200 OK' are highlighted in orange in the original image. The status bar at the bottom indicates 'Packets: 19 - Displayed: 2 (10.5%)'.

15) There were four TCP segments needed to carry the respons (red box)



16) Four, all in red boxes



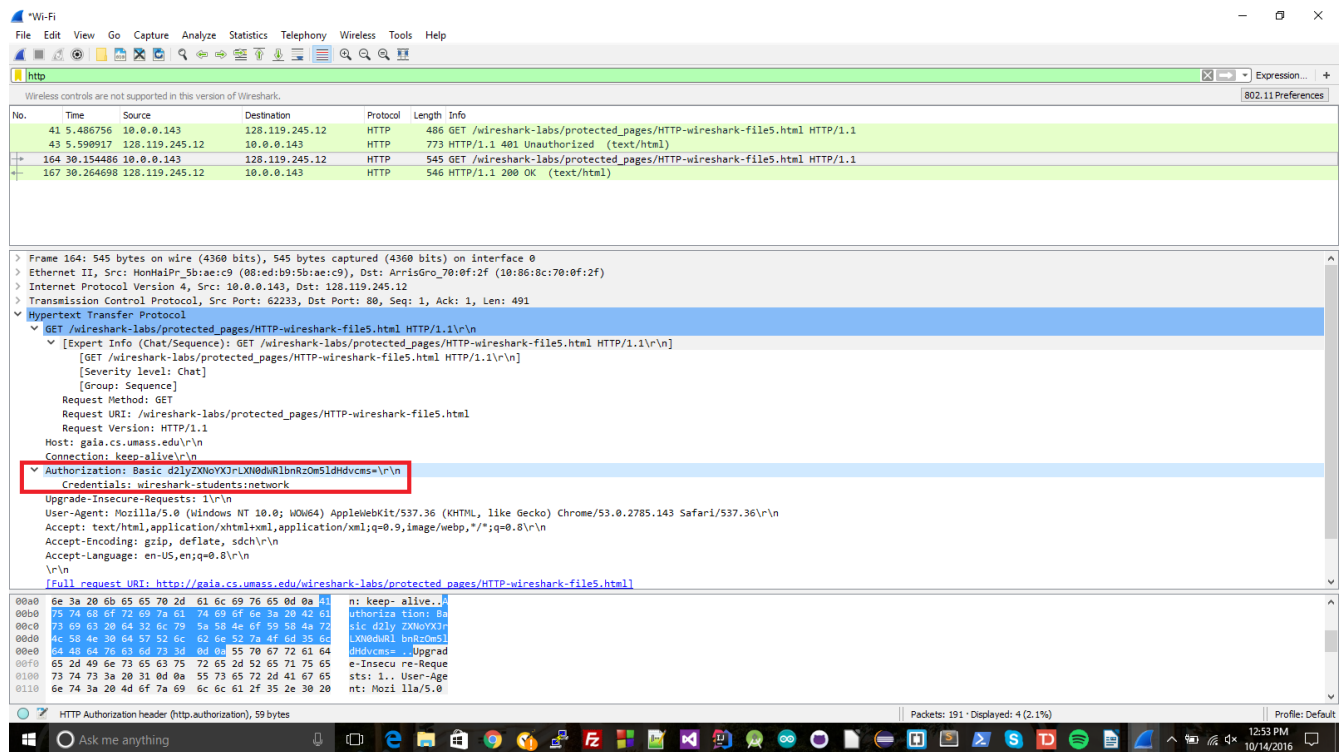
17) They were downloaded serially. I can tell by looking at the time on them. We can see that a GET message isn't sent out until after the reply is received from the previous GET message. In below image, times are in the orange box, and each reply message is underlined with a black line, showing that the time for the next GET is after the time of the response. If images were received in parallel, then GET messages would have been sent out at once (or close to it, anyway)

The image shows a Wireshark capture of an HTTP session. The packet list pane at the top shows several GET requests to various files. The 'Time' column for each request is highlighted in orange. The packet details pane for the first GET request (No. 19) is expanded, showing the request method, URI, version, host, connection, upgrade-insecure-requests, user-agent, accept, accept-encoding, and accept-language. The packet bytes pane at the bottom shows the raw data of the first GET request.

18) 401 Unauthorized (red boxes)

The image shows a Wireshark capture of an HTTP session. The packet list pane at the top shows several GET requests to various files. The packet details pane for the first GET request (No. 41) is expanded, showing the request method, URI, version, host, connection, upgrade-insecure-requests, user-agent, accept, accept-encoding, and accept-language. The packet bytes pane at the bottom shows the raw data of the first GET request.

19) Authorization and Credentials (red box)



Wireshark packet capture showing an HTTP GET request. The packet list pane shows a packet of 545 bytes on the wire (4360 bits) captured on interface 0. The packet details pane shows the following structure:

- Frame 164: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface 0
- Ethernet II, Src: NonHAIr_5b:ae:c9 (08:ed:b9:5b:ae:c9), Dst: ArrisGro_70:0f:2f (10:86:8c:70:0f:2f)
- Internet Protocol Version 4, Src: 10.0.0.143, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 62233, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
- Hypertext Transfer Protocol
 - GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1]
 - [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
 - Connection: keep-alive
 - Authorization: Basic d2lyZXNoYXJrLXN0dWRLbmRzOm5ldHdvcm0=**
 - Credentials: wireshark-students:network
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 - Accept-Encoding: gzip, deflate, sdch
 - Accept-Language: en-US,en;q=0.8
 - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]

The packet bytes pane shows the raw data of the packet, including the Authorization header.

HTTP Authorization header (http.authorization), 59 bytes

Packets: 191 · Displayed: 4 (2.1%)

Profile: Default

12:53 PM 10/14/2016