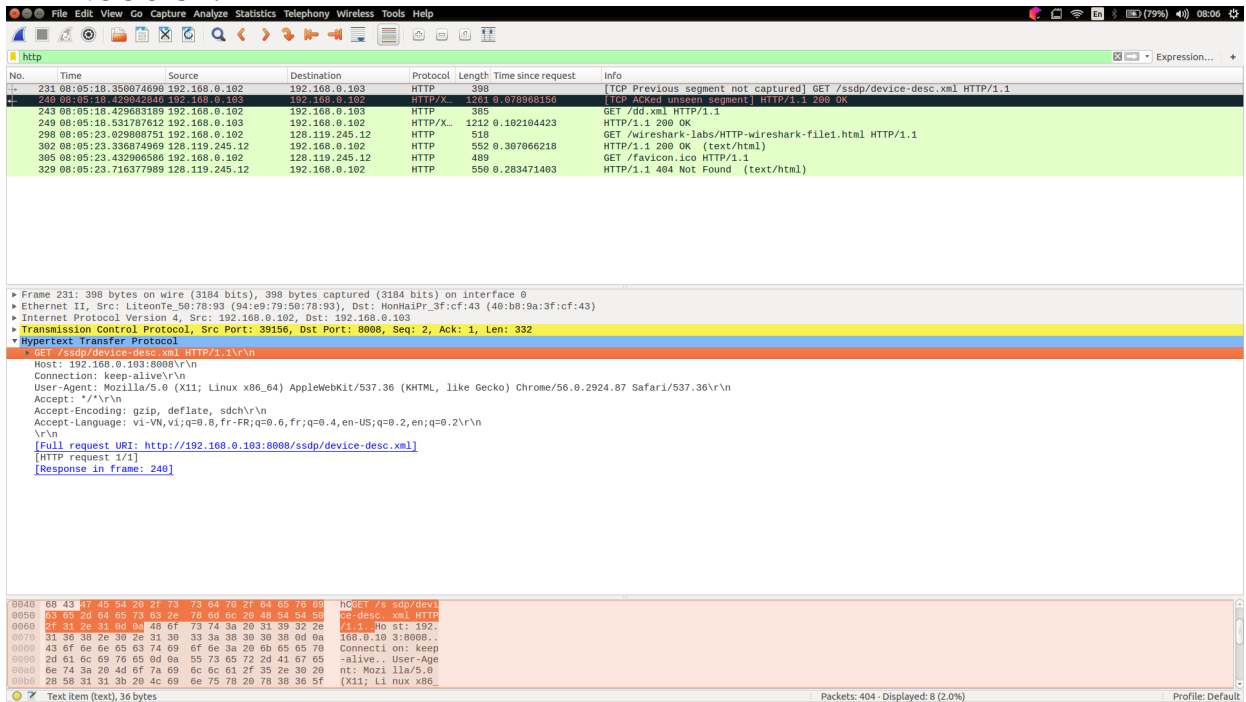


1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

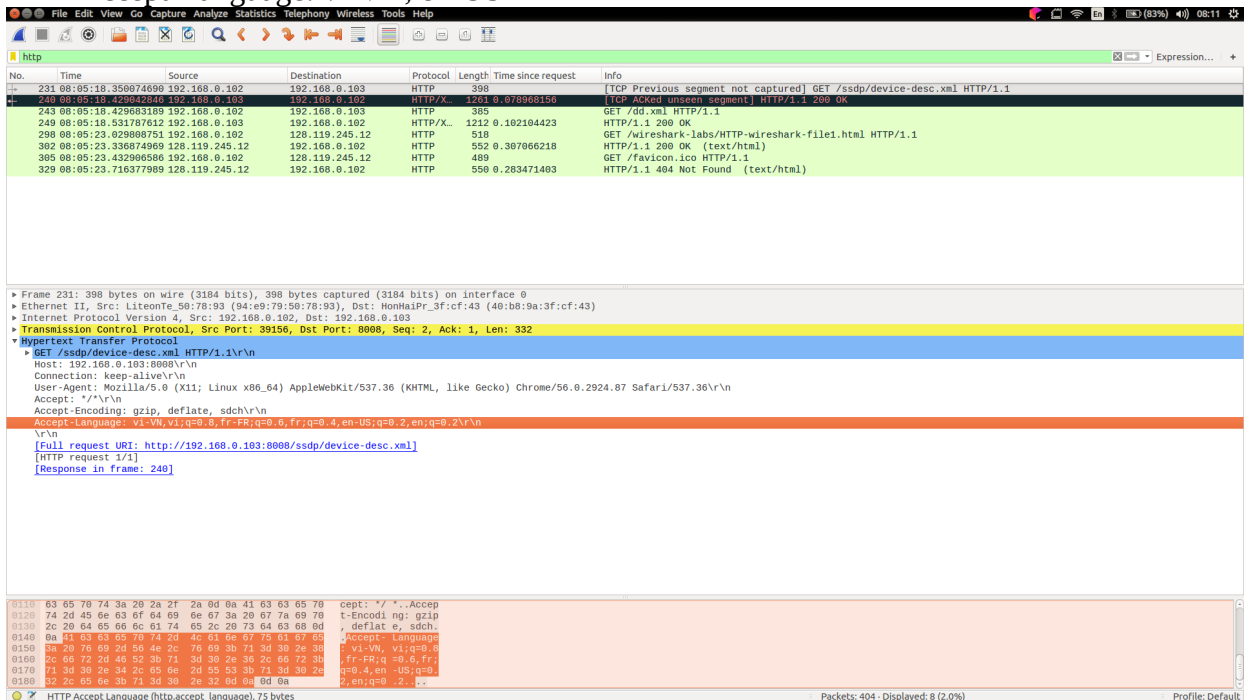
Versions 1.1



The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows three packets: a GET request (No. 231), a 200 OK response (No. 243), and a 200 OK response (No. 249). The packet details pane for packet 243 shows the HTTP response structure, including the status line "HTTP/1.1 200 OK" and the "Content-Type" header "text/html". The packet bytes pane shows the raw data of the response, including the status line and headers.

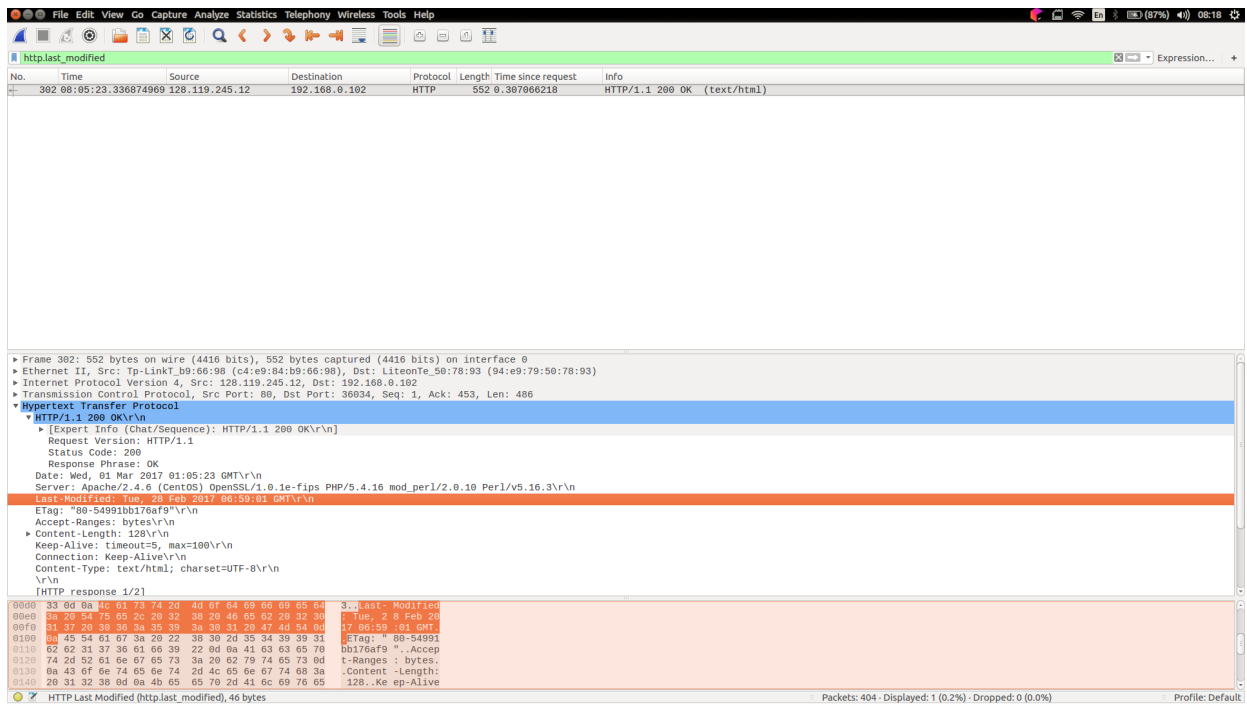
2. What languages (if any) does your browser indicate that it can accept to the server?

Accept-Language: vi-VN, en-US



The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows three packets: a GET request (No. 231), a 200 OK response (No. 243), and a 200 OK response (No. 249). The packet details pane for packet 243 shows the HTTP response structure, including the status line "HTTP/1.1 200 OK" and the "Content-Type" header "text/html". The packet bytes pane shows the raw data of the response, including the status line and headers.

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
IP address of my computer: 192.168.0.102
IP address of the gaia.cs.umass.edu: 128.119.245.12
4. What is the status code returned from the server to your browser?
200 OK
5. When was the HTML file that you are retrieving last modified at the server?
Last-Modified: Tue, 28 Feb 2017 06:59:01 GMT\r\n



6. How many bytes of content are being returned to your browser?

128

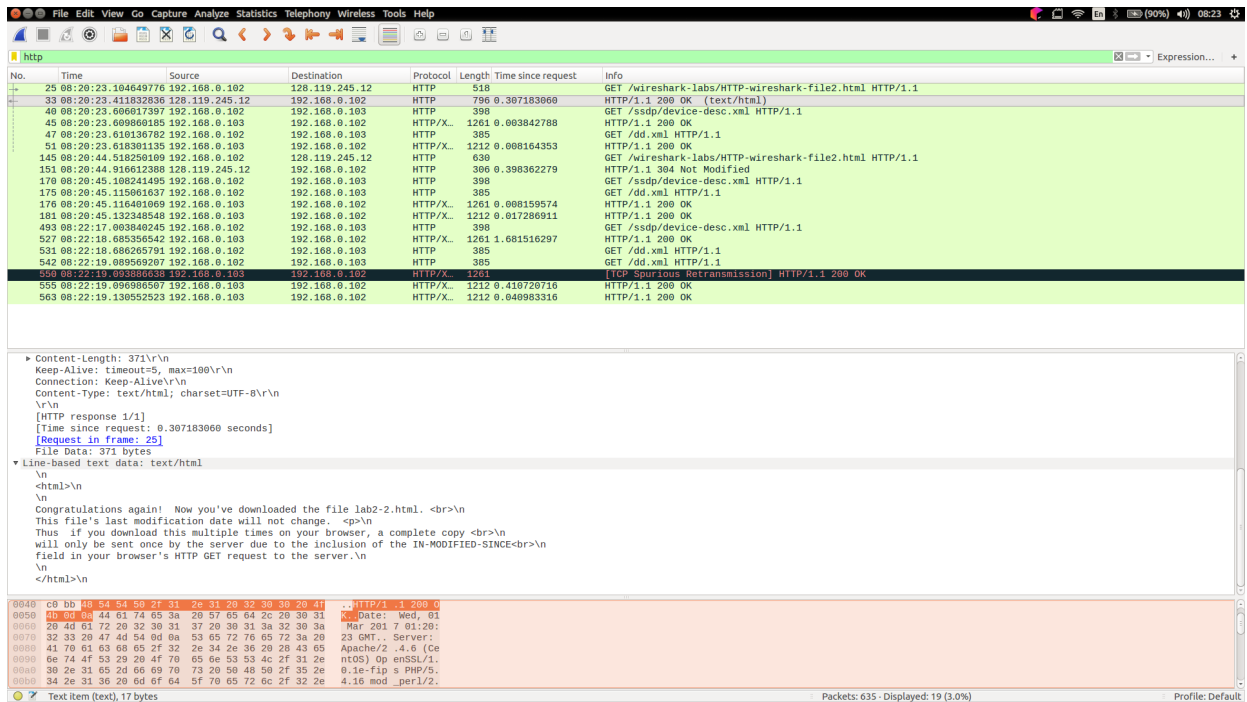
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No.

8. 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?

Yes.

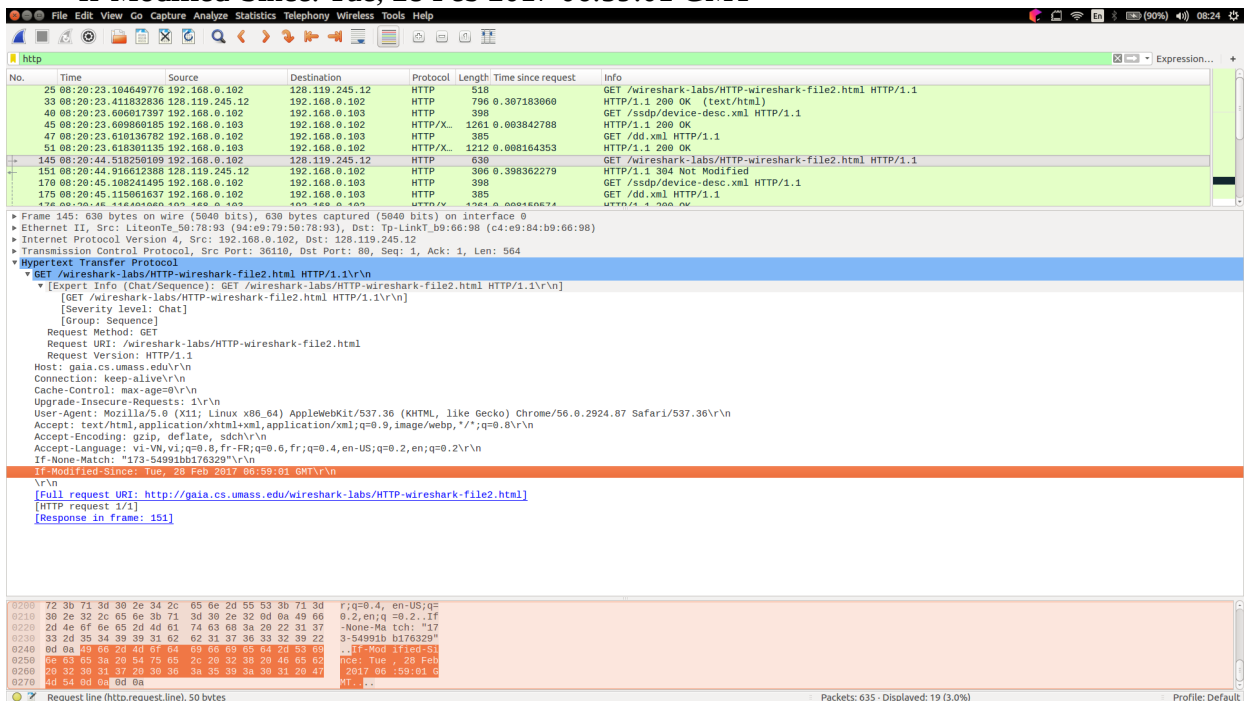
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? Yes.



10. 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 GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Yes

If-Modified-Since: Tue, 28 Feb 2017 06:59:01 GMT



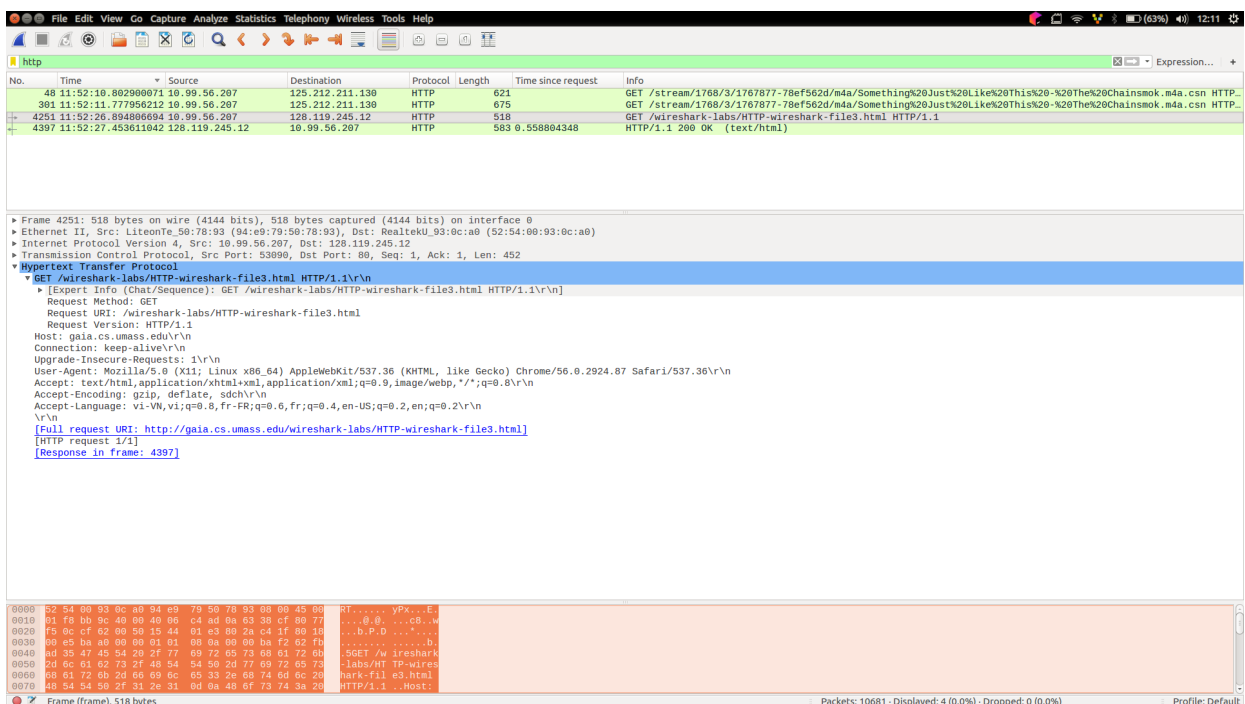
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

304 Not Modified.

No, the server didn't return the contents of the file because it was returned from the first requested.

12. How many HTTP GET request messages did your browser send? 1

Which packet number in the trace contains the GET message for the Bill of Rights? 4251



13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? 4397
14. What is the status code and phrase in the response? 200 OK
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? 4

The screenshot shows a Wireshark capture of an HTTP GET request and response. The response is split into four TCP segments. The status code and phrase '200 OK' are visible in the first segment of the response.

No.	Time	Source	Destination	Protocol	Length	Time since request	Info
4397	11:52:27.453611042	128.119.245.12	10.99.56.207	HTTP	583	0.558804348	HTTP/1.1 200 OK (text/html)

Frame 4397: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
 Ethernet II, Src: RealtekU_93:0c:a0 (52:54:00:93:0c:a0), Dst: LiteonTe_50:78:93 (94:e9:79:50:78:93)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.99.56.207
 Transmission Control Protocol, Src Port: 80, Dst Port: 53990, Seq: 4345, Ack: 453, Len: 517
 4 Reassembled TCP Segments (4861 bytes): #4391(1448), #4393(1448), #4395(1448), #4397(517)
 Hypertext Transfer Protocol
 Line-based text data: text/html

0000 48 54 54 50 2f 31 2e 31 20 32 30 39 20 4f 4b 00 HTTP/1.1 200 OK
 0010 3a 44 61 74 65 3a 20 57 65 64 2c 20 30 31 29 4d Date: Wed, 01 M
 0020 61 72 20 32 30 31 37 20 30 34 3a 35 32 3a 32 37 ar 2017 04:52:27
 0030 20 47 4d 54 6d 0a 53 65 72 76 65 72 3a 20 41 76 GMT..Se rver: Ap
 0040 31 63 68 65 2f 32 2e 34 2e 30 30 28 43 65 6e 74 iche/2-4- 8 (Cont
 0050 4f 53 29 20 4f 79 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0.

Frame (583 bytes) Reassembled TCP (4861 bytes)
 TCP Segments (tcp.segments), 4861 bytes Packets: 10681 - Displayed: 4 (0.0%) - Dropped: 0 (0.0%) Profile: Default

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
 4
 128.119.245.12 ; 128.119.240.90

The screenshot shows a Wireshark capture of multiple HTTP GET requests. The requests are sent to different IP addresses: 128.119.245.12, 128.119.240.90, and 128.119.240.90.

No.	Time	Source	Destination	Protocol	Length	Time since request	Info
239	12:23:05.075036285	10.99.56.207	128.119.245.12	HTTP	510		GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
251	12:23:05.484085720	128.119.245.12	10.99.56.207	HTTP	1139	0.408859435	HTTP/1.1 200 OK (text/html)
253	12:23:05.491010766	10.99.56.207	128.119.245.12	HTTP	489		GET /pearson.png HTTP/1.1
255	12:23:05.500160141	128.119.245.12	10.99.56.207	HTTP	1514		[TCP Previous segment not captured] Continuation
261	12:23:05.500160141	128.119.245.12	10.99.56.207	HTTP	761		Continuation
293	12:23:07.359071559	10.99.56.207	128.119.240.90	HTTP	503		GET /-kurose/cover_5th_ed.jpg HTTP/1.1
297	12:23:08.233440289	128.119.240.90	10.99.56.207	HTTP	522	0.074377730	HTTP/1.1 302 Found (text/html)
325	12:23:08.498624536	10.99.56.207	128.119.240.90	HTTP	503		GET /-kurose/cover_5th_ed.jpg HTTP/1.1
476	12:23:08.721030547	128.119.240.90	128.119.240.90	HTTP	1300	1.223574411	HTTP/1.1 200 OK (JPEG image)

Frame 478: 1366 bytes on wire (10928 bits), 1366 bytes captured (10928 bits) on interface 0
 Ethernet II, Src: RealtekU_93:0c:a0 (52:54:00:93:0c:a0), Dst: LiteonTe_50:78:93 (94:e9:79:50:78:93)
 Internet Protocol Version 4, Src: 128.119.240.90, Dst: 10.99.56.207
 Transmission Control Protocol, Src Port: 80, Dst Port: 43918, Seq: 99913, Ack: 438, Len: 1306
 70 Reassembled TCP Segments (101212 bytes): #333(1448), #335(1448), #337(1448), #339(1448), #341(1448), #343(1448), #345(1448), #347(1448), #349(1448), #351(1448), #355(1448), #357(1448), #359(1448), #361(1448)
 Hypertext Transfer Protocol
 JPEG File Interchange Format

00000000 48 54 54 50 2f 31 2e 31 20 32 30 39 20 4f 4b 00 HTTP/1.1 200 OK
 00000010 3a 44 61 74 65 3a 20 57 65 64 2c 20 30 31 29 4d Date: Wed, 01 M
 00000020 61 72 20 32 30 31 37 20 30 35 3a 32 33 3a 30 38 ar 2017 05:23:08
 00000030 20 47 4d 54 6d 0a 53 65 72 76 65 72 3a 20 41 76 GMT..Se rver: Ap
 00000040 31 63 68 65 00 0a 4e 61 73 74 20 40 01 64 60 65 acher..La st-Modif
 00000050 69 65 64 3a 20 54 75 65 2c 20 31 35 20 53 65 76 ied: Tue 15 Sep

Frame (1366 bytes) Reassembled TCP (101212 bytes)
 TCP Segments (tcp.segments), 101212 bytes Packets: 1137 - Displayed: 9 (0.8%) Profile: Default

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.

Serially, because it was downloaded by the order in HTML file

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

401 Unauthorized

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

▼ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n
Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n