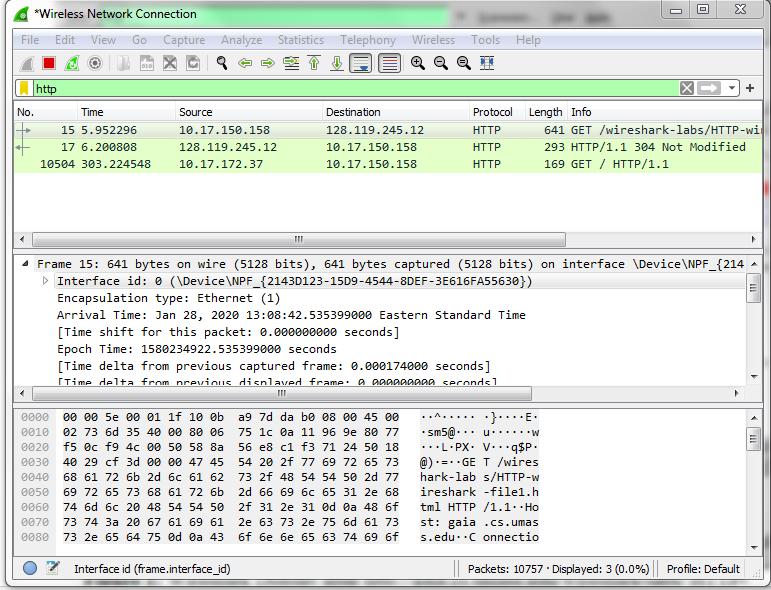
Wireshark Lab: HTTP

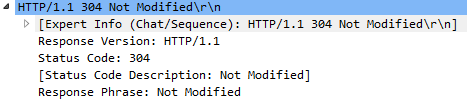
**1. The Basic HTTP GET/response interaction**

Began Wireshark packet sniffing with HTTP filter applied, then ran the web page link provided in the lab (<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>). The resulting packets captured are shown below.

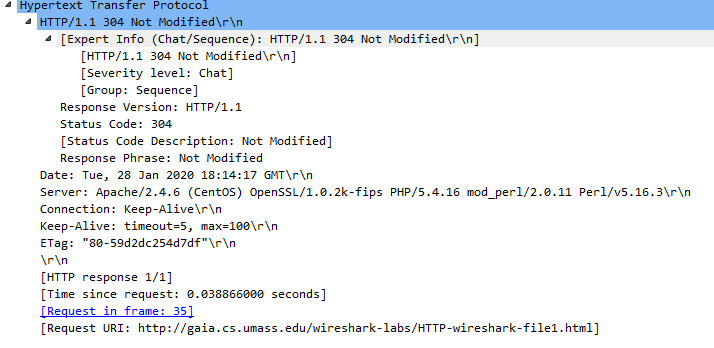


Questions:

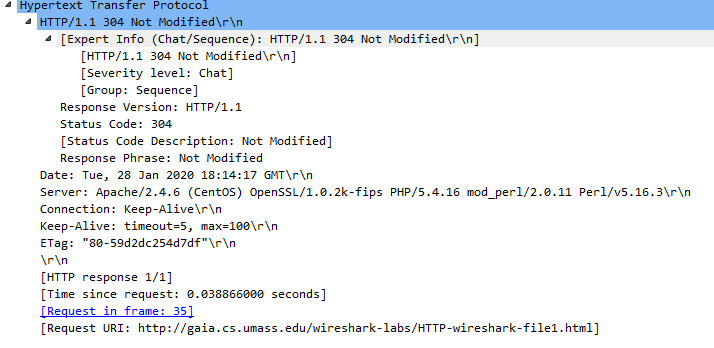
1. My browser is currently running HTTP 1.1, according to the GET packet that was captured. This is found in the Info section of the captured packet.
2. According to the GET packet, the browser indicates that it can accept en-GB and en-US. Which is English-Great Britain and English-United States. This is found under the HTTP tab in Wireshark. 
3. The IP address of this computer will be the Source IP in the GET packet and the IP address of gaia.cs.umass.edu is the Destination IP in the GET packet. Therefore the computer IP is 10.17.150.158 and the IP address of gaia.cs.umass.edu is 128.119.245.12.
4. The status code returned to my browser from the server is 304.



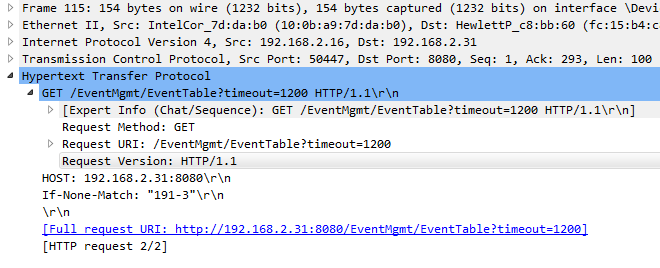
1. No information on return packet to browser with date of last modification of file.



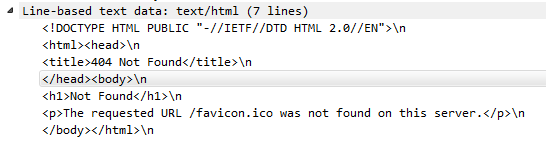
1. No information on Content-Length listed in returning packet



1. I can see in the raw data of the outgoing packet to the server that some data such as the Globally unique address, the Individual address in the Ethernet II tab. In the response packet back to my browser I can see at the end more information was coming but seemed to be cut off.
2. There is no IF-MODIFIED-SINCE request from the first HTTP GET request.



1. The server tries to display the HTML in the Line-based Text Data but is unable to produce all of it.



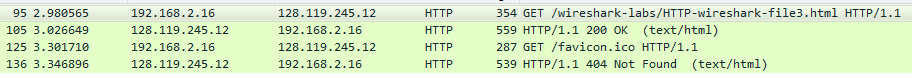
1. In the second GET request I do see a IF-MODIFIED-SINCE line. The information following is the **Thu, 30 Jan 2020 06:59:04 GMT**.



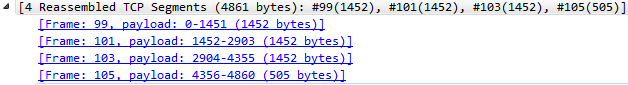
1. The Status Code is 304 and the Response Phrase is Not Modified. The server did not explicitly return the contents of the file in this response packet. This is due to the file being loaded from the cache the second time it is loaded.



1. There were 2 HTTP GET requests were sent.



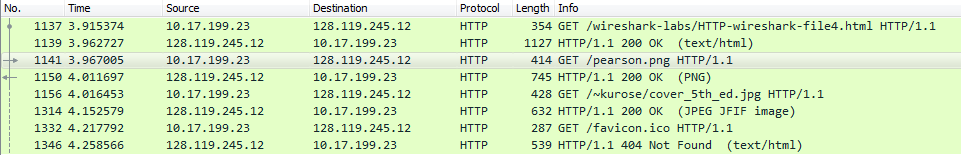
1. There were 4 TCP segments that carried data needed to carry the single HTTP response.



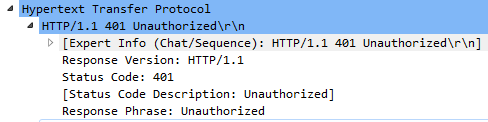
1. The Status Code is 200 and the Response Phrase is OK.



1. No there are no HTTP status lines in the data that indicate or associate with a TCP induced Continuation.
2. I received 4 HTTP GET requests but I believe one of them is a result of using Internet Explorer as it is a packet from favicon.ico and not the website provided. They were sent to 128.119.245.12.



1. The images were downloaded serially as we can see there are 2 TCP packets that are sent with different destination ports. Also, we can see there are 2 different packets with 2 different HTTP GET requests that contain the image.
2. Status Code: 401 Phrase: Unauthorized



1. Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

