LAB ASSIGNMENT 2

AIM:

To explore several aspects of the HTTP protocol: the basic GET/response interaction, HTTP message formats, retrieving large HTML files, retrieving HTML files with embedded objects, and HTTP authentication and security.

Basic HTTP GET/Response Interaction:

1. Start the web browser.
2. Start-up Wireshark packet sniffer. Enter “http” in the display-filer-specification window, so that only HTTP messages will be displayed in the packet listing window.
3. After a minute or so, begin Wireshark packet capture.
4. Enter the following link in the browser:

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

1. Stop Wireshark packet capture.

Question1: Is the browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?  
Answer: The browser is running http version 1.1. The server is also running http version 1.1.

Question2: What languages (if any) does your browser indicate that it can accept to the server?  
Answer: The browser can accept English-US and English languages from the server (en-US, en).

Question3: What is the IP address of the user’s computer? Of the gaia.cs.umass.edu server?  
Answer: The IP address of the user’s computer is 192.168.0.103. The IP address of the server is 184.26.162.89.

Question4: What is the status code returned from the server to the user’s browser?  
Answer: The status code returned was 200 OK.

Question5: When was the HTML file that you are retrieving last modified at the server?  
Answer: The file was last modified on Friday, Aug 25, 2015 at 6:30:07 GMT.

Question6: How many bytes of content are being returned to your browser?  
Answer: 128 bytes of content are being returned.

Question7: By inspecting the raw data in the packet content window, are there any headers within the data that are not displayed in the packet-listing window? If so, name one.  
Answer: No extra headers have been found in the raw data that is not present in the packet-listing window.

HTTP Conditional GET/Response Interaction:

* Start up your web browser, and make sure your browser’s cache is cleared, as discussed above.
* Start up the Wireshark packet sniffer
* Enter the following URL into your browser  
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html  
  The browser should display a very simple five-line HTML file.
* Question:uickly enter the same URL into your browser again (or simply select the refresh button on your browser)
* Stop Wireshark packet capture, and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Question8: Inspect the contents of the first HTTP GET request from your browser to the server. Is there an “IF-MODIFIED-SINCE” line in the HTTP GET?  
Answer: There is no “IF-MODIFIED-SINCE” line in the HTTP GET.

Question9: Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can it be determined?  
Answer: The server explicitly returns the contents of the file. The ‘Line-Based Text Data’ section in Wireshark displays what the server sent back to the browser which is what showed on the browser when I went on the website.

Question10: Inspect the contents of the second HTTP GET request from your browser to the server. Is there an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?  
Answer: An “IF-MODIFIED-SINCE:” line is present in the second HTTP GET request. The information following the header is the date and time at which the webpage was last accessed.

Question11: 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?  
Answer: The status code and phrase returned from the server is HTTP/1.1 304 Not Modified. The server didn’t return the contents of the file since the browser loaded it from its cache.

Retrieving Long Documents:

* Start up your web browser, and make sure your browser’s cache is cleared.
* Start up the Wireshark packet sniffer
* Enter the following URL into your browser  
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

Your browser should display the rather lengthy US Bill of Rights.

* Stop Wireshark packet capture, and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed.

Question12: How many HTTP GET request messages did the browser send? Which packet number in the trace contains the GET message for the Bill or Rights?  
Answer: The browser sent only one HTTP GET request message. The GET message was contained in the packet number 587.

Question13: Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?  
Answer: The packet number 698 contains the status code and phrase associated to the response the HTTP GET response.

Question14: What is the status code and phrase in the response?  
Answer: The code and phrase in the response is 200 OK.

Question15: How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?  
Answer The data was sent in 4 reassembled TCP segments.

HTML Documents with Embedded Objects:

* Start up your web browser, and make sure your browser’s cache is cleared.
* Start up the Wireshark packet sniffer
* Enter the following URL into your browser  
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
* Stop Wireshark packet capture, and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed.

Question16: How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?  
Answer: The browser sent 3 HTTP GET messages:

* 128.119.245.12 – Initial Page
* 165.193.140.14 – Pearson Logo
* 128.119.240.90 – Pearson book, 5th edition

Question17: Can it be determined whether the browser downloaded the two images serially, orwhether they were downloaded from the two web sites in parallel?  
Answer: The two images were downloaded serially, the logo being downloaded first followed by the book cover. This is so as the first image had been requested before the second. Also, the first image was returned before the request for the second image was sent.

HTTP Authentication:

* Make sure your browser’s cache is cleared
* Enter the following URL:  
  http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html
* Stop Wireshark packet capture and enter http in the filter

Question18: What is the server’s response (status code and phrase) in response to the initial HTTP GET message from the browser?  
Answer: The server’s response was ‘404 Not Found’.

Question19: When the browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?  
Answer: The browser does not send the HTTP GET message for the second time.

CONCLUSION:

This assignment gives us a clearer view of the HTTP send/response as well as familiarizes us with the various functionalities of the Wireshark packet sniffer.