**Assignment #003:**

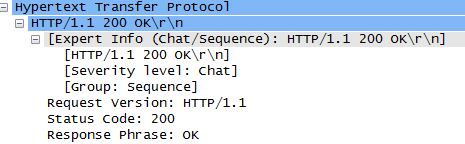
Use Wireshark to study HTTP. You’ll explore several aspects of the HTTP protocol: the basic GET/response interaction, HTTP message formats, retrieving HTML files with embedded objects, and HTTP authentication and security.

**1. HTTP GET/response interaction**

Begin your exploration of HTTP by downloading a very simple HTML file - one that is very short, and contains embedded objects. Please show your screen shots, answer the following questions and circle the answers on your screen shots:

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

**Answer: My browser runs HTTP 1.1 and the server runs HTTP 1.1 too.**

****

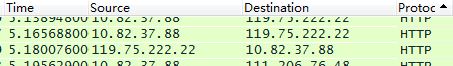
1. What languages does your browser indicate that it can accept to the server?

**Answer: zh-CN, zh; q=0.8**

**C:\Users\Administrator\Desktop\2.JPG**

1. What is the IP address of your computer and of the server?

**Answer: The IP address of my computer is ‘10.82.37.88’ and the IP address of the server is ‘119.75.222.22’.**

****

1. What is the status code returned from the server to your browser?

**Answer: 200 OK**

**C:\Users\Administrator\Desktop\4.JPG**

**C:\Users\Administrator\Desktop\5.JPG**

1. When was the HTML file that you are retrieving last modified at the server?

**Answer: Fri Apr 10 19:39:22 2015**

**C:\Users\Administrator\Desktop\6.JPG**

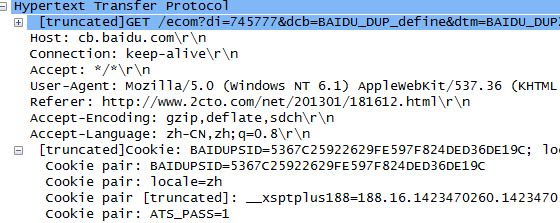
1. How many bytes of content are being returned to your browser?

**Answer: 320 bytes**

**C:\Users\Administrator\Desktop\7.JPG**

1. 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?

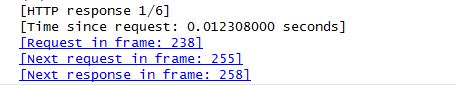
**Answer: No.**

****

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

**Answer: No.**

**C:\Users\Administrator\Desktop\11.JPG**

****

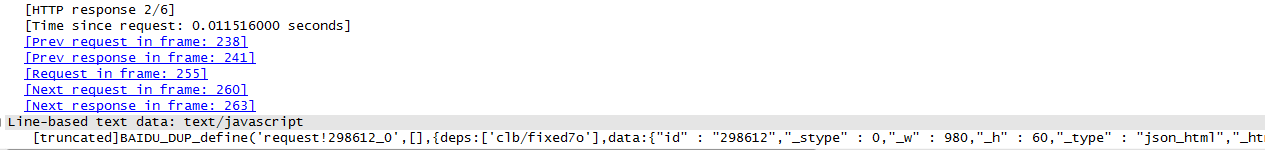
1. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

**Answer: No.**

****

1. 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: 200 OK**



**2. HTTP Authentication**

Please try visiting a web site that is password-protected and examine the sequence of HTTP message exchanged for such a site. Do the following:

1. Make sure your browser’s cache is cleared, as discussed above, and close down your browser. Then, start up your browser
2. Start up the Wireshark packet sniffer
3. Enter the URL into your browser
4. Type the requested user name and password into the pop up box.
5. 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.

(**Note:** You might want to first read up on HTTP authentication by reviewing the Wikipedia entry at <http://en.wikipedia.org/wiki/Basic_access_authentication>. )

Please show your screen shots, answer the following questions and circle the answers on your screen shots:

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

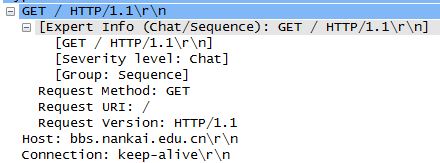
**Answer: 302 Found**

****

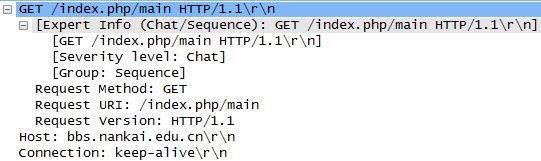
1. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

**Answer: The new field is ‘index.php/main’.**

**The First Time:**

****

**The Second Time:**

****

**学号：1210565**

**2015年4月10日星期五**