Tevin Jeffrey – CS 356

Wireshark Lab 2

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

1.1

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

English-US

**3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?**

gaia.cs.umass.edu = 128.119.245.12

My computer = 192.168.0.112

**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?**

Mon, 25 Jan 2016 06:59:01 GMT

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

81

**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?**

No

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

Yes, because the server says to expect content of length 371 bytes.

**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, there is some date information. Incidentally, it’s the last modified date from the earlier request.

*If-Modified-Since: Tue, 26 Jan 2016 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.**

The status code is 304 – Not Modified. No, the server did not return any content from the server. Presumably the server is telling my application to use a cached copy of the file that lives on my local machine since the one on the server has not been modified since a particular time.

**12. How many HTTP GET request messages were sent by your browser?**

One GET request was sent by my browser.

**13. How many data-containing TCP segments were needed to carry the single HTTP response?**

Four data-containing TCP segments were needed to carry the single HTTP response.

**14. What is the status code and phrase associated with the response to the HTTP GET request?**

200 OK

**15. Are there any HTTP status lines in the transmitted data associated with a TCP induced “Continuation”?**

Yes, there’s indication of continuation in the use of relative sequence numbers.

**16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?**

Four get requests were sent by my browser.

**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, the last packet of the first image arrived well before the first packet of the second image.

**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?**

http.authorization