**Brent Berghmans 1334252**

**Wireshark HTTP**

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

Mijn browser gebruikt HTTP 1.1.

De server gebruikt ook HTTP 1.1.

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

Nederlands en Engels. (nl-NL en en-US).

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

Mijn computer: 192.168.0.198

gaia.cs.umass.edu: 128.119.245.12

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

Na de pagina op te vragen stuurt de server de status code 200 (OK) terug.

Hierna probeert chrome ook een favicon.ico op te vragen maar dit heeft de website niet dus hier stuurt de server 404 ((Not found) terug.

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

Op 10 oktober 2015 19:45:27 GMT.

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

De content length is 128 dus ik vermoed 128 bytes.

**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.**

ETag wordt niet getoond.

**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?**

Neen.

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

Ja, de response heeft de hele HTML content als text data bijgeleverd.

De response is ook van het type 200 OK.

**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?**

Een datum. In het bijzonder: Sat, 10 Oct 2015 05:59:02 GMT.

Dit is de datum die de server bij de vorige request heeft teruggestuurd als Last-Modified.

**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.

Er zit geen text-data veld bij de http response dus de html content is niet teruggestuurd.

**12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?**

1 HTTP GET request.

Het pakket nummer is 61.

**13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**

Pakket nummer 68.

**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 TCP Segmenten.

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

Er waren 4 GET requests verzonden.

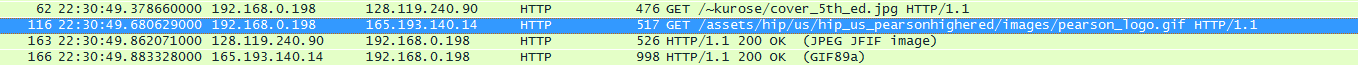
1 Request naar: 128.119.245.12

2 Requests naar: 128.199.240.90

1 Request naar: 165.193.140.14

**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.**

Ik vermoed parallel omdat er chronologisch eerst 2 HTTP GET requests verstuurd werden en daarna 2 HTTP 200 OK requests ontvangen werden.



**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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

Credentials: wireshark-students:network