

Sai Valluru

Professor Bo Sheng

CS446

09/29/2023

Wireshark Lab: HTTP

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

- My browser is running HTTP version 1.1
- The server is running HTTP version 1.1

Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n

Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

51	5.523655	10.0.0.122	128.119.245.12	HTTP	545	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
55	5.545392	128.119.245.12	10.0.0.122	HTTP	540	HTTP/1.1 200 OK (text/html)

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

- My browser accepts American English, as stated as “en-US”
- But it can also accept other forms of English, as it also states “en” in general

Accept-Language: en-US,en;q=0.9\r\n

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

- The IP address of my computer is 10.0.0.122
- The IP address of the **`gaia.cs.umass.edu`** server is 128.119.245.12

```
Internet Protocol Version 4, Src: 10.0.0.122, Dst: 128.119.245.12
```

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

- The status code returned from the server to my browser is 200

```
Hypertext Transfer Protocol  
> HTTP/1.1 200 OK\r\n
```

```
HTTP 540 HTTP/1.1 200 OK (text/html)
```

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

- The HTML file that I retrieved was last modified, on Thursday, September 28th, 2023, 05:59:01 GMT

```
Last-Modified: Thu, 28 Sep 2023 05:59:01 GMT\r\n
```

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

- The number of bytes of content being returned to my browser is 128

```
Content-Length: 128\r\n[Content length: 128]
```

7. 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, I don’t see any “IF-MODIFIED-SINCE” in the first HTTP GET

183	8.947164	10.0.0.122	128.119.245.12	HTTP	449	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
-----	----------	------------	----------------	------	-----	--

```
> Frame 183: 449 bytes on wire (3592 bits), 449 bytes captured (3592 bits) on interface en0, id 0
> Ethernet II, Src: Apple_5e:c7:3d (a4:83:e7:5e:c7:3d), Dst: VantivaU_dc:e6:bb (d4:e2:cb:dc:e6:bb)
> Internet Protocol Version 4, Src: 10.0.0.122, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60426, Dst Port: 80, Seq: 1, Ack: 1, Len: 395
< Hypertext Transfer Protocol
  < GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      [HTTP request 1/1]
      [Response in frame: 187]
```

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

- Yes, I was able to see the text data which was retrieved from the first HTTP GET

187	8.968338	128.119.245.12	10.0.0.122	HTTP	784	HTTP/1.1 200 OK (text/html)
-----	----------	----------------	------------	------	-----	-----------------------------

```

> Frame 187: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface en0, id 0
> Ethernet II, Src: VantivaU_dc:e6:bb (d4:e2:cb:dc:e6:bb), Dst: Apple_5e:c7:3d (a4:83:e7:5e:c7:3d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.122
> Transmission Control Protocol, Src Port: 80, Dst Port: 60426, Seq: 1, Ack: 396, Len: 730
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Thu, 28 Sep 2023 14:59:32 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Thu, 28 Sep 2023 05:59:01 GMT\r\n
      ETag: "173-606650133eeec"\r\n
      Accept-Ranges: bytes\r\n
    > Content-Length: 371\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=UTF-8\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.021174000 seconds]
      [Request in frame: 183]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      File Data: 371 bytes
  < Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change. <p>\n
    Thus if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n

```

9. 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, I do see an “IF-MODIFIED-SINCE” in the second HTTP GET
- The information that follows the “IF-MODIFIED-SINCE:” header is the date and time since, which the resource should be modified for the server to return to the client. **If-Modified-Since: Thu, 28 Sep 2023 05:59:01 GMT**

```

> Frame 350: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface en0, id 0
> Ethernet II, Src: Apple_5e:c7:3d (a4:83:e7:5e:c7:3d), Dst: VantivaU_dc:e6:bb (d4:e2:cb:dc:e6:bb)
> Internet Protocol Version 4, Src: 10.0.0.122, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60444, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
< Hypertext Transfer Protocol
  < GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      If-Modified-Since: Thu, 28 Sep 2023 05:59:01 GMT\r\n
      If-None-Match: "173-606650133eeec"\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      [HTTP request 1/1]
      [Response in frame: 353]

```

10. 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 **HTTP** status code and phrase returned from the server in response to the second **HTTP GET** is 304 Not Modified
- The server didn't return the contents of the file because the requested resource had not been modified since the **If-Modified-Since** date.

353	17.284985	128.119.245.12	10.0.0.122	HTTP	294	HTTP/1.1 304 Not Modified
-----	-----------	----------------	------------	------	-----	---------------------------

```
> Frame 353: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface en0, id 0
> Ethernet II, Src: VantivaU_dc:e6:bb (d4:e2:cb:dc:e6:bb), Dst: Apple_5e:c7:3d (a4:83:e7:5e:c7:3d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.122
> Transmission Control Protocol, Src Port: 80, Dst Port: 60444, Seq: 1, Ack: 482, Len: 240
< Hypertext Transfer Protocol
  < HTTP/1.1 304 Not Modified\r\n
    < [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n
      [HTTP/1.1 304 Not Modified\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
      Date: Thu, 28 Sep 2023 14:59:40 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Connection: Keep-Alive\r\n
      Keep-Alive: timeout=5, max=100\r\n
      ETag: "173-606650133eec"\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.087787000 seconds]
      [Request in frame: 350]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```