

Lab 1

Oliver Lundin & Emma Zettervall (olilu316, emmze999)

1. The Basic HTTP GET/response interaction

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

Both server and browser is running 1.1 (HTTP/1.1)

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

sv-SE,sv;q=0.9,en-US;q=0.8,en;q=0.7 (Svenska/Engelska)

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

10.241.202.10 is my address, 128.119.245.12 is the server address.

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

Status Code: 200 OK

No.	Time	Source	Destination	Protocol	Length	Info
1501	9.279986	10.241.246.1	128.119.245.12	HTTP	524	GET /ethereal-labs/HTTP-ethereal-
1522	9.399073	128.119.245.12	10.241.246.1	HTTP	538	HTTP/1.1 200 OK (text/html)
1529	9.446217	10.241.246.1	128.119.245.12	HTTP	470	GET /favicon.ico HTTP/1.1
1547	9.564493	128.119.245.12	10.241.246.1	HTTP	538	HTTP/1.1 404 Not Found (text/htm

>	Transmission Control Protocol, Src Port: 80, Dst Port: 54738, Seq: 1, Ack: 471, Len: 484
▼	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

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

This morning.

```

> Transmission Control Protocol, Src Port: 80, Dst Port: 54738, Seq: 1, Ack: 471, Len: 484
< 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: Tue, 12 Sep 2023 13:28:26 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: Tue, 12 Sep 2023 05:59:01 GMT\r\n

```

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

```

      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 12 Sep 2023 13:28:26 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: Tue, 12 Sep 2023 05:59:01 GMT\r\n
    ETag: "7e-6052323b6978f"\r\n
    Accept-Ranges: bytes\r\n
  < Content-Length: 126\r\n
    [Content length: 126]
    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 1/2]
    [Time since request: 0.119087000 seconds]
    [Request in frame: 1501]
    [Next request in frame: 1529]
    [Next response in frame: 1547]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 126 bytes
  > Line-based text data: text/html (4 lines)

```

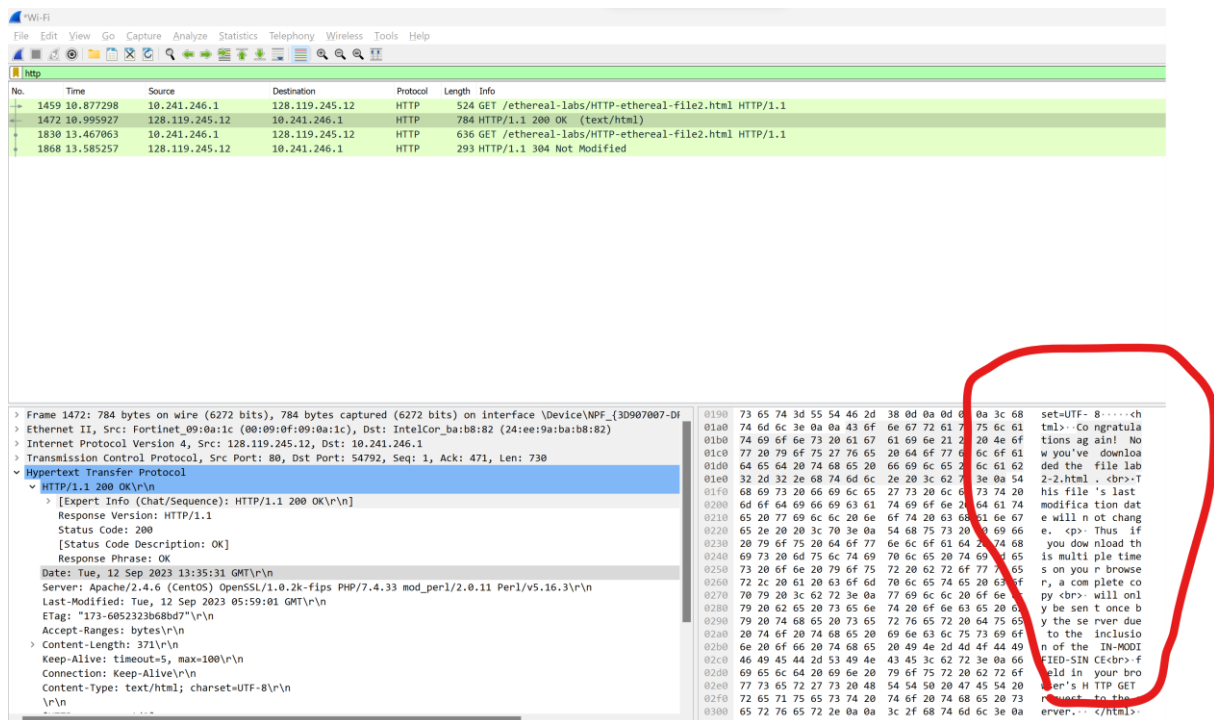
Content should be 126 bytes.

2. The HTTP CONDITIONAL GET/response interaction

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 we do not see it.

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



We can tell because the content from the web browser is being displayed in wireshark.

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, If-Modified-Since: Thu, 07 Sep 2023 05:59:02 GMT\r\n, A date.

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.

Status Code: 304, Response Phrase: Not Modified, it did not return the contents because the file was not modified.

3. Retrieving Long Documents

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

1

fraga3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1681	12.387091	10.241.246.1	128.119.245.12	HTTP	524	GET /ethereal-labs/HTTP-ethereal-1
1697	12.508511	128.119.245.12	10.241.246.1	HTTP	769	HTTP/1.1 200 OK (text/html)

> Frame 1697: 715 bytes on wire (6152 bits), 769 bytes captured (6152 bits) on interface \Device\NPF_{3D907007-D...}

> Ethernet II, Src: Fortinet_09:0a:1c (00:09:0f:09:0a:1c), Dst: IntelCor_ba:b8:82 (24:ea:9a:ba:b8:82)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.241.246.1

> Transmission Control Protocol, Src Port: 80, Dst Port: 54828, Seq: 4147, Ack: 471, Len: 715

> [2 Reassembled TCP Segments (4861 bytes): #1695(4146), #1697(715)]

[Frame: 1695, payload: 0-4145 (4146 bytes)]

[Frame: 1697, payload: 4146-4860 (715 bytes)]

[Segment count: 2]

[Reassembled TCP length: 4861]

[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054756552c203132205365702032...]

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

Status Code: 200, Response Phrase: OK

The image shows a Wireshark packet capture of an HTTP GET request and response. The packet list shows three packets: a GET request (No. 1681, Time 12.387091, Source 10.241.246.1, Destination 128.119.245.12, Protocol HTTP, Length 524, Info GET /ethereal-labs/HTTP-ethereal-file3.html HTTP/1.1), a response (No. 1697, Time 12.508511, Source 128.119.245.12, Destination 10.241.246.1, Protocol HTTP, Length 769, Info HTTP/1.1 200 OK (text/html)), and a third packet (No. 1698, Time 12.508511, Source 128.119.245.12, Destination 10.241.246.1, Protocol HTTP, Length 769, Info HTTP/1.1 200 OK (text/html)). The packet details pane shows the structure of the HTTP request and response, including the request line, headers, and body. The response status line is 200 OK (text/html).

4. HTML Documents with Embedded Objects

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

3 requests are sent. 1 for the website, 1 for the first picture and 1 for the second.

No.	Time	Source	Destination	Protocol	Length	Info
831	4.669955	10.241.246.1	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
860	4.789247	128.119.245.12	10.241.246.1	HTTP	1355	HTTP/1.1 200 OK (text/html)
864	4.810855	10.241.246.1	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
891	4.929999	128.119.245.12	10.241.246.1	HTTP	901	HTTP/1.1 200 OK (PNG)
1006	5.394862	10.241.246.1	178.79.137.164	HTTP	460	GET /8E_cover_small.jpg HTTP/1.1
1015	5.423271	178.79.137.164	10.241.246.1	HTTP	225	HTTP/1.1 301 Moved Permanently

The first two requests are sent to the address: 128.119.245.12 and the third is to another address: 178.79.137.164.

15. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

They should be downloaded in parallel since the arrival times are very close. If it was serial it would be a bigger difference in arrival time since the 3rd GET should be sent after the 2nd is done.

2nd Arrival Time: Sep 12, 2023 16:04:45.592493000 W. Europe Daylight Time

3rd Arrival Time: Sep 12, 2023 16:04:46.176500000 W. Europe Daylight Time

5. HTTP Authentication

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

401: Authorization required

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

A field for authentication.