

Computer Networks

Bhuvana Kanakam - SE21UCSE035

The Basic HTTP GET/response interaction

Question 1 : Basic HTTP get response

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

My browser is running a version 1.1

```
Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
```

My server is running a version 1.1

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

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

Accept-Language: en-US,en;q=0.9

```

Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Upgrade-Insecure-Requests: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.2
Accept-Language: en-US,en;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 270]
```

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

```
Internet Protocol Version 4, Src: 10.70.9.139, Dst: 128.119.245.12
```

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

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

```

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?]

Last-Modified: Wed, 07 Feb 2024 06:59:01 GMT

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

```

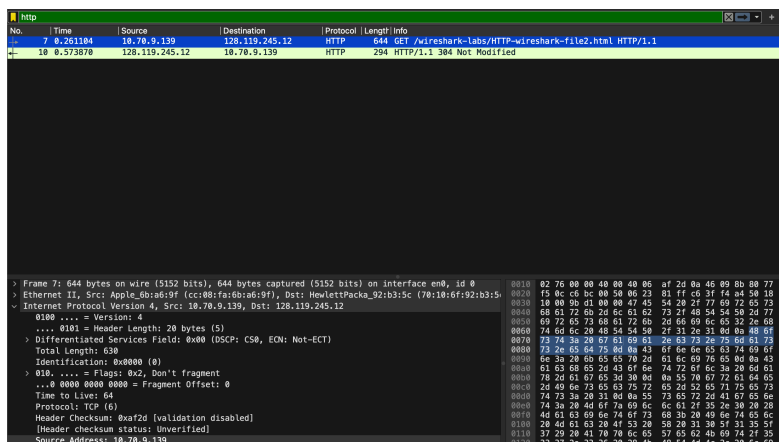
  ▾ Frame 4: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on
    Section number: 1
    > Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  8, 2024 10:14:54.634108000 IST
    UTC Arrival Time: Feb  8, 2024 04:44:54.634108000 UTC
    Epoch Arrival Time: 1707367494.634108000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000835000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.259084000 seconds]
    Frame Number: 4
    Frame Length: 462 bytes (3696 bits)
    Capture Length: 462 bytes (3696 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]

```

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, I do not see any headers within the data.

Question 2 : HTTP CONDITIONAL get/response interaction



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, I do not see an “IF-MODIFIED-SINCE” line in the HTTP GET

```

Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  > [Expert Info (Captured): 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
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  If-None-Match: "173-611520bb8c46e"\r\n
  If-Modified-Since: Wed, 14 Feb 2024 06:59:01 GMT\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: 10]

```

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

Yes, the server explicitly returned the contents of the file. It is visible under the Line-based text data tab.

```
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
```

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?

The contents of the second HTTP GET request from my browser to the server contains the “IF-MODIFIED-SINCE” line. The information followed is: If-Modified-Since: Wed, 14 Feb 2024 06:59:01 GMT

```
Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Ap
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-611520bb8c46e"\r\n
If-Modified-Since: Wed, 14 Feb 2024 06:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTT
[HTTP request 1/1]
[Response in frame: 221]
```

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 HTTP status code and phrase returned from the server in response to the second HTTP GET is 304 Not Modified. It simply returned the contents from the cache hence showing the Not Modified response phrase.

```
Hypertext Transfer Protocol
> HTTP/1.1 304 Not Modified\r\n
> [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
```

Question 3 : Retrieving Long Documents

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 message was sent by my browser. The packet number is 85.

No.	Time	Source	Destination	Protocol	Length	Info
85	6.615042	10.70.9.139	128.119.245.12	HTTP	558	GET /wireshark-labs/HTTP-wi...
90	6.909810	128.119.245.12	10.70.9.139	HTTP	769	HTTP/1.1 200 OK (text/html)

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

Packet number 90 contains the status code and phrase associated with the response to the HTTP GET request.

No.	Time	Source	Destination	Protocol	Length	Info
85	6.615042	10.70.9.139	128.119.245.12	HTTP	558	GET /wireshark-labs/HTTP-wi...
90	6.909810	128.119.245.12	10.70.9.139	HTTP	769	HTTP/1.1 200 OK (text/html)

14. What is the status code and phrase in the response?

The status code is 200 and the response phrase is OK

```
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
```

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 segments were needed to carry the single HTTP response

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 50980, Seq
  [4 Reassembled TCP Segments (4861 bytes): #87(1382), #88(1382), #
    [Frame: 87, payload: 0-1381 (1382 bytes)]
    [Frame: 88, payload: 1382-2763 (1382 bytes)]
    [Frame: 89, payload: 2764-4145 (1382 bytes)]
    [Frame: 90, payload: 4146-4860 (715 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data [truncated]: 485454502f312e3120323030204
```

Question 4 : HTML Documents with Embedded Objects

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

3 HTTP GET request messages were sent from my browser to the following internet addresses:

128.119.245.12

128.119.245.12

178.79.137.164

No.	Time	Source	Destination	Protocol	Length	Info
50	4.788513	10.70.9.139	128.119.245.12	HTTP	558	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
54	5.106274	128.119.245.12	10.70.9.139	HTTP	1355	HTTP/1.1 200 OK (text/html)
56	5.132242	10.70.9.139	128.119.245.12	HTTP	478	GET /pearson.png HTTP/1.1
57	5.132721	10.70.9.139	178.79.137.164	HTTP	445	GET /8E_cover_small.jpg HTTP/1.1
60	5.414265	128.119.245.12	10.70.9.139	HTTP	901	HTTP/1.1 200 OK (PNG)
62	5.414267	178.79.137.164	10.70.9.139	HTTP	225	HTTP/1.1 301 Moved Permanently

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.

The two images were downloaded parallelly. The request for the second image was sent before receiving a response for the first image.

56	5.132242	10.70.9.139	128.119.245.12	HTTP	478	GET /pearson.png HTTP/1.1
57	5.132721	10.70.9.139	178.79.137.164	HTTP	445	GET /8E_cover_small.jpg HTTP/1.1
60	5.414265	128.119.245.12	10.70.9.139	HTTP	901	HTTP/1.1 200 OK (PNG)
62	5.414267	178.79.137.164	10.70.9.139	HTTP	225	HTTP/1.1 301 Moved Permanently

Question 5 : HTTP Authentication

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

The status code of the initial HTTP GET message is 404, and the response phrase is Not Found.

```
Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
```

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

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-%20wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcmcs=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-%20wireshark-file
    [HTTP request 1/1]
    [Response in frame: 34]
```

```
Hypertext Transfer Protocol
  GET /gts1c3/MFAwtjBMMEowSDAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7xsAkB2MEFIp0f6%2BFze6VzT2c00JGFPNxm
    Host: ocsf.pki.goog\r\n
    X-Apple-Request-UUID: FA8953A6-5AEF-4E6F-A248-FB38940D70DB\r\n
    Accept: */*\r\n
    User-Agent: com.apple.trustd/3.0\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://ocsp.pki.goog/gts1c3/MFAwtjBMMEowSDAHBgUrDgMCGgQUxy55it3%2FYTSzuu1HQri7
    [HTTP request 1/1]
    [Response in frame: 429]
```