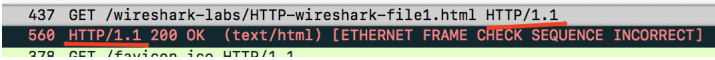


Basic HTTP Get/response interaction

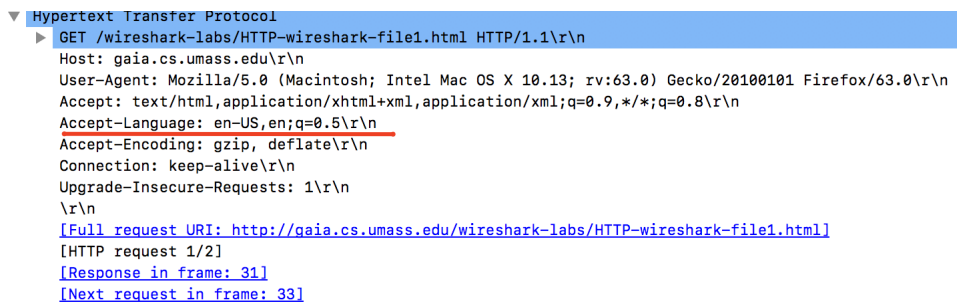
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

- Browser: HTTPv1.1
- Server: HTTPv1.1

- A screenshot of a Wireshark packet capture. The first packet (437) is a GET request for /wireshark-labs/HTTP-wireshark-file1.html using HTTP/1.1. The second packet (560) is an HTTP/1.1 200 OK response (text/html) with a note indicating an incorrect Ethernet frame check sequence. The third packet (378) is another GET request.

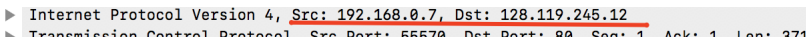
2. What languages does your browser indicate that it can accept to the server?

- My browser communicates that it can accept 'en-US'

- A screenshot of a Wireshark packet capture showing an HTTP GET request. The 'Accept-Language' header is highlighted in red and shows 'en-US,en;q=0.5'. Other headers include User-Agent (Mozilla/5.0), Accept (text/html, application/xhtml+xml, application/xml;q=0.9, */*;q=0.8), Accept-Encoding (gzip, deflate), and Connection (keep-alive). The status bar at the bottom shows the full request URI, HTTP request 1/2, response in frame 31, and next request in frame 33.

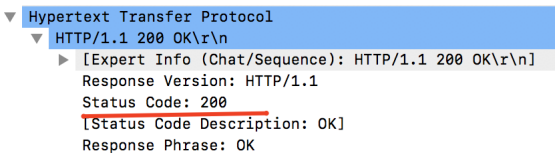
3. What is the IP address of your computer? Of the Server?

- Me: 10.106.41.52
- Server: 128.119.245.12

- A screenshot of a Wireshark packet capture showing an Internet Protocol Version 4 packet. The source IP is 192.168.0.7 and the destination IP is 128.119.245.12.

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

- Status Code: 200 OK

- A screenshot of a Wireshark packet capture showing an HTTP/1.1 200 OK response. The status code '200' is highlighted in red. The response phrase is 'OK'.

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

- Last Modified: THU, 08 Nov 2018 06:59:01 GMT

- A screenshot of a Wireshark packet capture showing the 'Last-Modified' header. The value is 'Tue, 13 Nov 2018 06:59:01 GMT'. The 'ETag' header is also visible with the value '80-57a865a368ebb'.

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

- 128 Bytes

```
Accept-Ranges: bytes\r\n
▼ Content-Length: 128\r\n
  [Content length: 128]
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
```

7. List a header not displayed in the packet listing:

- Connection: Keep Alive

HTTP CONDITIONAL GET/response interaction

- 1. 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 "IF-MODIFIED-SINCE" header in the first GET Request.
- 2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
 - Yes, there was a content length field, and a specified number of bytes indicating the server explicitly downloaded the contents.

```
► 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 1/4]
[Time since request: 0.076274000 seconds]
[Request in frame: 279]
[Next request in frame: 285]
[Next response in frame: 286]
— File Data: 371 bytes
```

- 3. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" header?

- There is an "IF-MODIFIED-SINCE" header in the HTTP GET request

```
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Tue, 13 Nov 2018 06:59:01 GMT\r\n
— If-None-Match: "173-57a865a3686eb"\r\n
```

- 4. 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 is 304, not modified.
- The server returned a cached version of the file, there is no file-data field, and no amount of bytes specified.

```

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: Tue, 13 Nov 2018 23:26:40 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=98\r\n
    ETag: "173-57a865a3686eb"\r\n
    \r\n
    [HTTP response 3/4]
    [Time since request: 0.064586000 seconds]
    [Prev request in frame: 285]
    [Prev response in frame: 286]
    [Request in frame: 292]
    [Next request in frame: 295]
    [Next response in frame: 296]

```

Retrieving Long Documents

- 1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
 - There was 1 HTTP Get request sent
 - Packet number 7 contains the GET message for the Bill of Rights

259	1.900679	192.168.0.7	128.119.245.12	TCP	78	55636 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=
263	1.967417	128.119.245.12	192.168.0.7	TCP	76	80 → 55636 [SYN, ACK] Seq=0 Ack=1 Win=28960
266	1.967547	192.168.0.7	128.119.245.12	TCP	66	55636 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=
268	1.969888	192.168.0.7	128.119.245.12	HTTP	437	GET /wireshark-labs/HTTP-wireshark-file3.ht
271	2.028512	128.119.245.12	192.168.0.7	TCP	68	80 → 55636 [ACK] Seq=1 Ack=372 Win=30080 Le
272	2.032148	128.119.245.12	192.168.0.7	TCP	1522	80 → 55636 [ACK] Seq=1 Ack=372 Win=30080 Le
273	2.032156	128.119.245.12	192.168.0.7	TCP	1522	80 → 55636 [ACK] Seq=1449 Ack=372 Win=30080
274	2.032254	192.168.0.7	128.119.245.12	TCP	66	55636 → 80 [ACK] Seq=372 Ack=2897 Win=12886
275	2.032323	128.119.245.12	192.168.0.7	TCP	1522	80 → 55636 [ACK] Seq=2897 Ack=372 Win=30080
276	2.032329	128.119.245.12	192.168.0.7	HTTP	591	HTTP/1.1 200 OK (text/html) [ETHERNET FRAM
277	2.032389	192.168.0.7	128.119.245.12	TCP	66	55636 → 80 [ACK] Seq=372 Ack=4862 Win=12688
278	2.032407	192.168.0.7	128.119.245.12	TCP	66	[TCP Window Update] 55636 → 80 [ACK] Seq=37
283	2.102255	192.168.0.7	128.119.245.12	HTTP	378	GET /favicon.ico HTTP/1.1
286	2.155337	128.119.245.12	192.168.0.7	HTTP	558	HTTP/1.1 404 Not Found (text/html) [ETHERN
287	2.155385	192.168.0.7	128.119.245.12	TCP	66	55636 → 80 [ACK] Seq=684 Ack=5346 Win=13056

- 2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
 - the 4th Packet from the top (packet 268) in the trace contains the status code

78	55636 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=520412433 TSecr=0 SACK_PERM=1
76	80 → 55636 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1213884894 TSecr=520412433 WS=128
66	55636 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=520412498 TSecr=1213884894
437	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

- 3. What is the status code and phrase in the response?
 - Status Code: 200
 - Response Phrase: OK

```

▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  [HTTP/1.1 200 OK\r\n]
  [Severity level: Chat]
  [Group: Sequence]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Date: Tue, 13 Nov 2018 23:30:29 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.1
  Last-Modified: Tue, 13 Nov 2018 06:59:01 GMT\r\n
  ETag: "11106_57-06563228-0"

```

4. How many data-containing TCP segments were need to carry the single HTTP response and the text of the bill of rights?

- There are three packets that contain data for the Bill of Rights
- 271, 272, and 273

271	2.028512	128.119.245.12	192.168.0.7	TCP	68	80 → 55636 [ACK] Seq=1 Ack=372 Win=30080 Len=0
272	2.032148	128.119.245.12	192.168.0.7	TCP	1522	80 → 55636 [ACK] Seq=1 Ack=372 Win=30080 Len=1
273	2.032156	128.119.245.12	192.168.0.7	TCP	1522	80 → 55636 [ACK] Seq=1449 Ack=372 Win=30080 Len=0

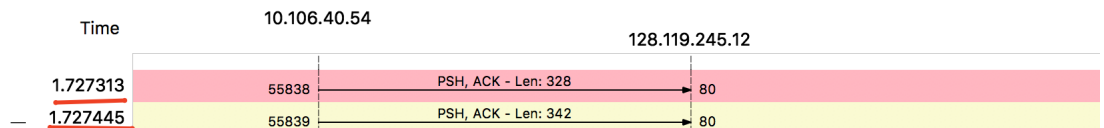
HTML Documents with Embedded Objects

1. How many HTTP GET request messaged did your browser send? To which Internet Addresses were these GET requests sent?

- My browser sent three HTTP GET requests ignoring the favicon request
 - (a) Packet 300 to 128.119.245.12 to download the Pearson.png
 - (b) Packet 301 to 128.119.245.12 to download the book cover
 - (c) Packet 307 to download the contents of the page

2. 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 images were downloaded in parallel because processing of the request can't have finished before the next tcp request is opened, they are milliseconds apart as seen in the image



HTTP Authentication

- 1. What is the servers response in response to the initial HTTP GET message from your browser?
 - Status Code: 401
 - Phrase: Unauthorized
- 2. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
 - 'Authorization: Basic' is the new field included in the get request.