Laboration 2 - HTTP - Answers

15123668X
Jesper Karlsson

Q1

```
GET /~comp2322/HTTP-1.html HTTP/1.1
Host: www4.comp.polyu.edu.hk
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/48.0.2564.116 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: IPCZQX03aee143e3=01001900ca7dc8febb4375e5f6b9eb3d6568fa52; ZNPCQ003-32303500=3474b0f8;
_ga=GA1.3.369838944.1453925920

HTTP/1.1 200 OK
Date: Sun, 21 Feb 2016 14:47:26 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.6.16
Last-Modified: Thu, 28 Jan 2016 09:09:11 GMT
ETag: "49-52a614592dbc0"
Accept-Ranges: bytes
Content-Length: 73
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

A. What version(s) of HTTP are your browser and the server running?

I am using HTTP version 1.1, and so does the server.

B. What language(s) (if any) does your browser indicate that it can accept from the server?

According to the picture above, en=US or en, American or regular English are the languages accepted.

C. What are the IP addresses of your computer and the server?

1396	3.014181	202.125.200.254	158.132.10.21	TCP	62525 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8 SACK_PERM=1
1399	3.017089	158.132.10.21	202.125.200.254	TCP	http > 62525 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
1401	3.017155	202.125.200.254	158.132.10.21	TCP	62525 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
1523	3.242428	202.125.200.254	158.132.10.21	HTTP	GET /~comp2322/HTTP-1.html HTTP/1.1
1524	3.244608	158.132.10.21	202.125.200.254	TCP	http > 62525 [ACK] Seq=1 Ack=530 Win=15744 Len=0
1603	3.430104	158.132.10.21	202.125.200.254	HTTP	HTTP/1.1 200 OK (text/html)
1606	3.447034	202.125.200.254	158.132.10.21	HTTP	GET /favicon.ico HTTP/1.1
1608	3.451488	158.132.10.21	202.125.200.254	TCP	http > 62525 [ACK] Seq=402 Ack=1010 Win=16768 Len=0
1609	3.451489	158.132.10.21	202.125.200.254	HTTP	HTTP/1.1 404 Not Found (text/html)
1645	3.502275	202.125.200.254	158.132.10.21	TCP	62525 > http [ACK] Seq=1010 Ack=857 Win=64768 Len=0

My IP address is 202.125.200.254 and the servers is 158.132.10.21.

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

It responded with 200 which means OK.

E. When was the HTML file that you retrieved last modified at the server?

In the picture above, we can see that it was last modified on Thursday the 28’th of January 2016, 09:09 in the morning.

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

If you look in the content-length part of the TCP stream you can see that the bytes recieved is 73.

Q2

A. **Do you see an "If-Modified-Since" line in the HTTP GET?**

```
GET /~comp2322/HTTP-2.html HTTP/1.1
Host: www4.comp.polyu.edu.hk
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/48.0.2564.116 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Date: Sun, 21 Feb 2016 17:02:24 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.6.16
Last-Modified: Thu, 28 Jan 2016 09:09:01 GMT
ETag: "16f-52a6144fa4540"
Accept-Ranges: bytes
Content-Length: 367
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

No I do not.

B. **Did the server explicitly return the contents of the file? How can you tell?**

Yes it did, we can observe this under the "Line based text data" tab in the incoming TCP frame.

C. **Do you see an "If-Modified-Since" line in the HTTP GET? If so, what information follows the "If-Modified-Since" header?**

Yes, and due to the page stating it would not change the information that follows is "Thu, 28 Jan 2016 09:09:01"

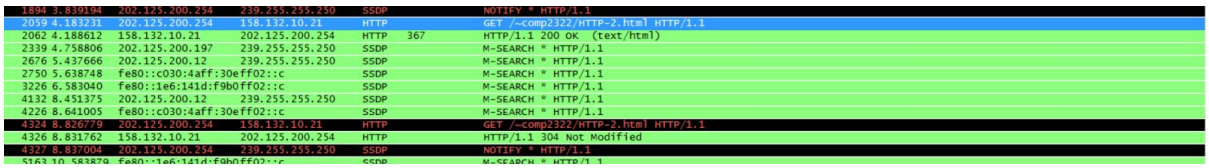
D. **What is the status code and phrase returned from the server's response to this second HTTP GET?**

304 Not modified.

E. **Did the server explicitly return the contents of the file? Explain.**

Since it's quicker, the browser loaded up the data from its cache.

Q3



A. Did the server explicitly return the contents of the file in response to the first HTTP GET request?

Yes it did, which we can see through the 200 OK response.

B. How about for the second HTTP GET request?

It did not, as we can se under the following GET request in the picture above it gave the 304 not modified which means it loaded from the cache.

C. Please explain this behavior. When does the browser clear all the cache when browsing in incognito or private mode?

Incognito mode clears the cache when the browser is shut down, until then it is stored in temporary files.

Q4

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

Just one.

B. How many data-containing TCP segments were needed to carry the single HTTP response?

Four, which can be seen in the picture above just under the 200 OK answer.

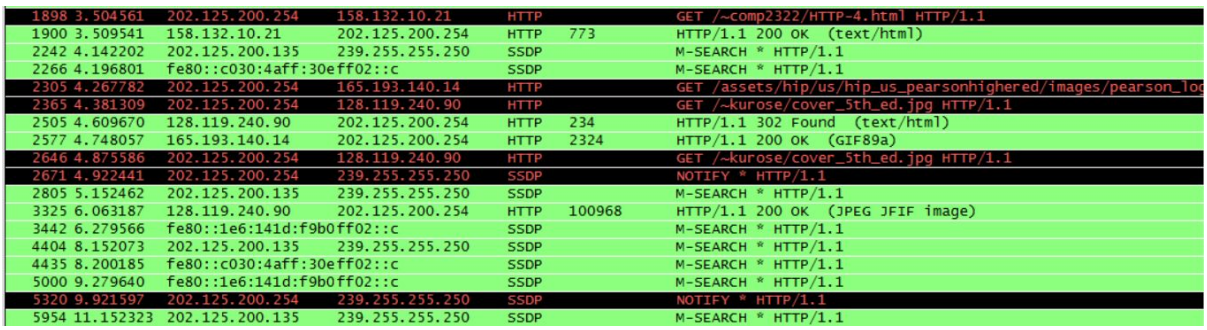
C. What is the status code and phrase associated with the response to the HTTP GET request?

It should be 200 OK, as seen in the picture above.

D. Are there any HTTP status lines in the transmitted data associated with a TCP-induced “Continuation”?

No there’s nothing like that from what I can see.

Q5



1898 3.504561	202.125.200.254	158.132.10.21	HTTP		GET /~comp2322/HTTP-4.html HTTP/1.1
1900 3.509541	158.132.10.21	202.125.200.254	HTTP	773	HTTP/1.1 200 OK (text/html)
2242 4.142202	202.125.200.135	239.255.255.250	SSDP		M-SEARCH * HTTP/1.1
2266 4.196801	fe80::c030:4aff:30eff02::c		SSDP		M-SEARCH * HTTP/1.1
2305 4.267782	202.125.200.254	165.193.140.14	HTTP		GET /assets/hip/us/hip_us_pearsonhighered/images/pearson_log
2365 4.381309	202.125.200.254	128.119.240.90	HTTP		GET /~kurose/cover_5th_ed.jpg HTTP/1.1
2505 4.609670	128.119.240.90	202.125.200.254	HTTP	234	HTTP/1.1 302 Found (text/html)
2577 4.748057	165.193.140.14	202.125.200.254	HTTP	2324	HTTP/1.1 200 OK (GIF89a)
2646 4.875586	202.125.200.254	128.119.240.90	HTTP		GET /~kurose/cover_5th_ed.jpg HTTP/1.1
2671 4.922441	202.125.200.254	239.255.255.250	SSDP		NOTIFY * HTTP/1.1
2805 5.152462	202.125.200.135	239.255.255.250	SSDP		M-SEARCH * HTTP/1.1
3325 6.063187	128.119.240.90	202.125.200.254	HTTP	100968	HTTP/1.1 200 OK (JPEG JFIF image)
3442 6.279566	fe80::1e6:141d:f9b0ff02::c		SSDP		M-SEARCH * HTTP/1.1
4404 8.152073	202.125.200.135	239.255.255.250	SSDP		M-SEARCH * HTTP/1.1
4435 8.200185	fe80::c030:4aff:30eff02::c		SSDP		M-SEARCH * HTTP/1.1
5000 9.279640	fe80::1e6:141d:f9b0ff02::c		SSDP		M-SEARCH * HTTP/1.1
5320 9.921597	202.125.200.254	239.255.255.250	SSDP		NOTIFY * HTTP/1.1
5954 11.152323	202.125.200.135	239.255.255.250	SSDP		M-SEARCH * HTTP/1.1

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

There were 4 GET messages sent, one to the server (158.132.10.21), one for the server where the Pearson image is stored (165.193.140.14 or internet address www.pearsonhighered.com/assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif) and two for the Book cover (128.119.240.90 or internet address manic.cs.umass.edu/~kurose/cover_5th_ed.jpg / caite.cs.umass.edu/~kurose/cover_5th_ed.jpg).

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

The pages could have been downloaded parrallel, but the book cover came in after since it the page first link had moved, thus an entirely new GET message needed to be sent.

Q6

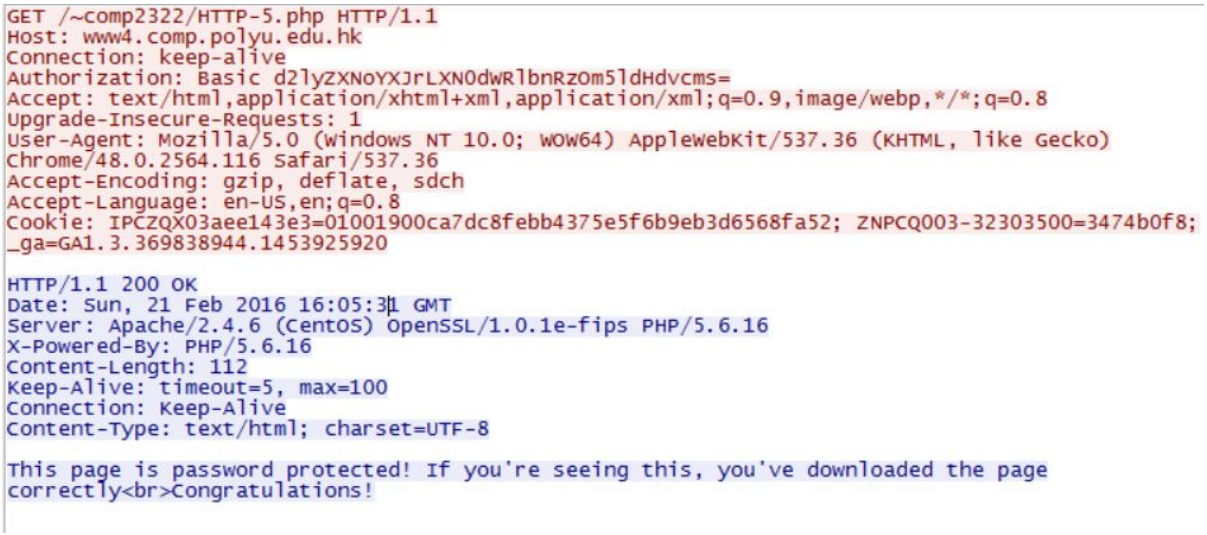
A. What is the status code and phrase of the server's response to the initial HTTP GET message from your browser?

```
GET /~comp2322/HTTP-5.php HTTP/1.1
Host: www4.comp.polyu.edu.hk
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/48.0.2564.116 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: IPCZQX03aee143e3=01001900ca7dc8febb4375e5f6b9eb3d6568fa52; ZNPCQ003-32303500=3474b0f8;
_ga=GA1.3.369838944.1453925920

HTTP/1.0 401 Unauthorized
Date: Sun, 21 Feb 2016 16:05:17 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.6.16
X-Powered-By: PHP/5.6.16
WWW-Authenticate: Basic realm="wireshark-students only"
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

The code I get is 401, Unauthorized.

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



```
GET /~comp2322/HTTP-5.php HTTP/1.1
Host: www4.comp.polyu.edu.hk
Connection: keep-alive
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/48.0.2564.116 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: IPCZQX03aee143e3=01001900ca7dc8febb4375e5f6b9eb3d6568fa52; ZNPCQ003-32303500=3474b0f8;
_ga=GA1.3.369838944.1453925920

HTTP/1.1 200 OK
Date: Sun, 21 Feb 2016 16:05:31 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.6.16
X-Powered-By: PHP/5.6.16
Content-Length: 112
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

This page is password protected! If you're seeing this, you've downloaded the page
correctly<br>Congratulations!
```

We send authorization data to convey usernames and passwords whih enables us to access the wepage.

Q7

A. What is the new status code and what is it for?

The new status code is called 451, and it is to distinguish cencored content, or in nicer words “Unavalible due to legal reasons”.