Lab 02 - HTTP & Socket Programming

2020-03-06

Using Telnet to interact with a Web Server

Code

```
$> telnet vision.ucla.edu 80
Trying 131.179.176.147...
Connected to vision.ucla.edu.
Escape character is '^]'.
GET / HTTP/1.1
host: www.vision.ucla.edu

HTTP/1.1 200 OK
Date: Fri, 06 Mar 2020 00:17:42 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Thu, 01 Nov 2018 00:17:53 GMT
ETag: "12e7-5798f598e178e"
Accept-Ranges: none
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Content-Type: text/html
Content-Length: 4839
Via: HTTP/1.1 forward.http.proxy:3128
Connection: keep-alive

<!DOCTYPE html>
<html lang="en" class="h-100">
...
</html>

Connection closed
```

What is the content type of the response?

The response is a `text/html` type (Content-Type)

What is the size of the response?

`4839` bytes (Content-Length)

When was the webpage last modified?

`Thu, 01 Nov 2018 00:17:53 GMT` (Last-Modified)

Do you see an “Accept-Ranges” header field? What may this be used for?

It is currently set to `none`.
This header is used to indicate whether the server is able to send partial parts of the document.

For example, if downloading a large file - If you pause a download, there is no need to download the already saved parts of the file.

Perform a HEAD request on the same address

Code

```
$> telnet vision.ucla.edu 80
Trying 131.179.176.147...
Connected to vision.ucla.edu.
Escape character is '^]'.
HEAD / HTTP/1.1
host: www.vision.ucla.edu

HTTP/1.1 200 OK
Date: Fri, 06 Mar 2020 00:22:49 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Thu, 01 Nov 2018 00:17:53 GMT
ETag: "12e7-5798f598e178e"
Accept-Ranges: bytes
Content-Length: 4839
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Content-Type: text/html
Via: HTTP/1.1 forward.http.proxy:3128
Connection: keep-alive
```

What is the content type of the response?

text/html (Content-Type)

What is the size of the response?

4839 bytes (Content-Length)

Using telnet, find a way to get the people.html webpage from vision.ucla.edu

We can do the following:

Code

```
$> telnet vision.ucla.edu 80
GET /people.html HTTP/1.1
host: www.vision.ucla.edu
```

Results:

Code

```
$> telnet vision.ucla.edu 80
Trying 131.179.176.147...
Connected to vision.ucla.edu.
Escape character is '^]'.
GET /people.html HTTP/1.1
host: www.vision.ucla.edu

HTTP/1.1 200 OK
Date: Fri, 06 Mar 2020 00:25:29 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Sun, 16 Jun 2019 00:49:00 GMT
ETag: "c87b-58b663ed787b0"
Accept-Ranges: none
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Content-Type: text/html
Content-Length: 51323
Via: HTTP/1.1 forward.http.proxy:3128
Connection: keep-alive

...
```

Why is there the need to include the host in the GET (and HEAD) HTTP 1.1 request messages?

A webserver may be hosting several websites on the same machine, so there needs to be a way for clients to access the correct site.

Exercise 2: Understanding Internet Cookies

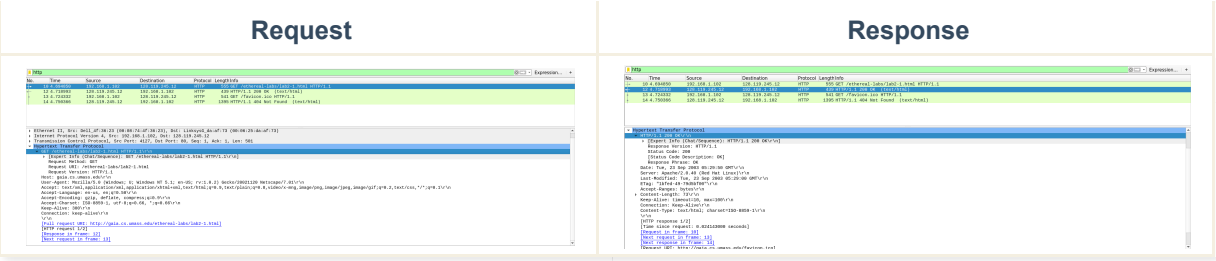
> Cookies are bits of data that are stored locally on the client's browser.
> When a client visits a website, they append the respective cookies in their requests to the website.
> Cookies have several uses: e.g. to identify a user, or to register that a user has performed an action (as to not show a prompt again).

Websites will have a `Set-Cookie` header in their response if they want to store cookies on the client's browser.

Exercise 3: Using Wireshark to understand basic HTTP request/response messages

File: http-ethereal-trace-1

Request	Response



What is the status code and phrase returned from the server to the client browser?

`200 OK`

When was the HTML file that the browser is retrieving last modified at the server?

`Tue, 23 Sep 2003 05:29:00 GMT`

Does the response also contain a DATE header? How are these two fields different?

Yes, it has a value of `Tue, 23 Sep 2003 05:29:50 GMT` .

These two fields differ, as the `Date` header is the time the server responds to the request, whereas the `Last-Modified` header refers to the time the file was modified.

Is the connection established between the browser and the server persistent or non-persistent? How can you infer this?

We can infer that the connetion is persistent, from the headers in the request.

Code

```
1  Keep-Alive: 300
2  Connection: keep-alive
```

There are also headers in the response, as seen below

Code

```
1  Keep-Alive: timeout=10, max=100
2  Connection: Keep-Alive
```

Which suggests that the established connection is persistent.

How many bytes of content are being returned to the browser?

`73` bytes (Content-Length)

What is the data contained inside the HTTP response packet?

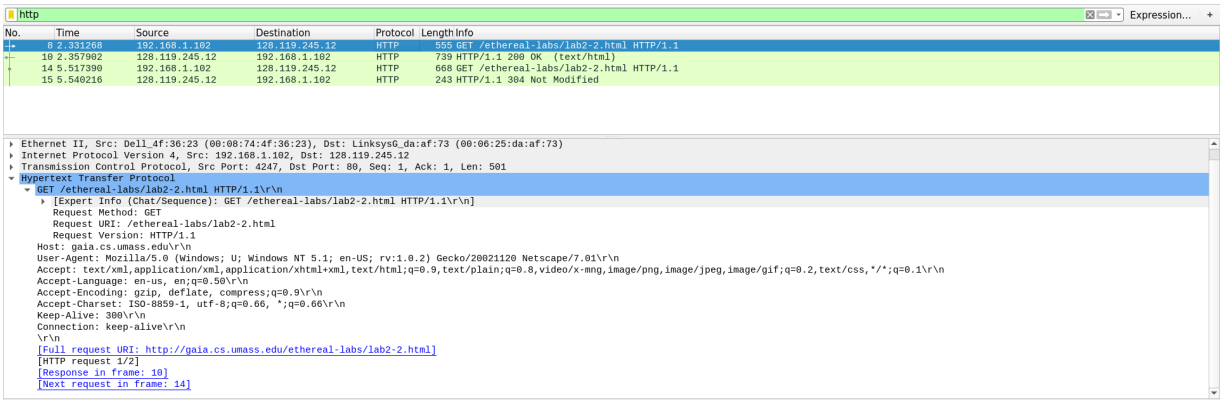
Code

```
1  <html>\n
2  Congratulations.  You've downloaded the file lab2-1.html!\n
3  </html>\n
```

Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction

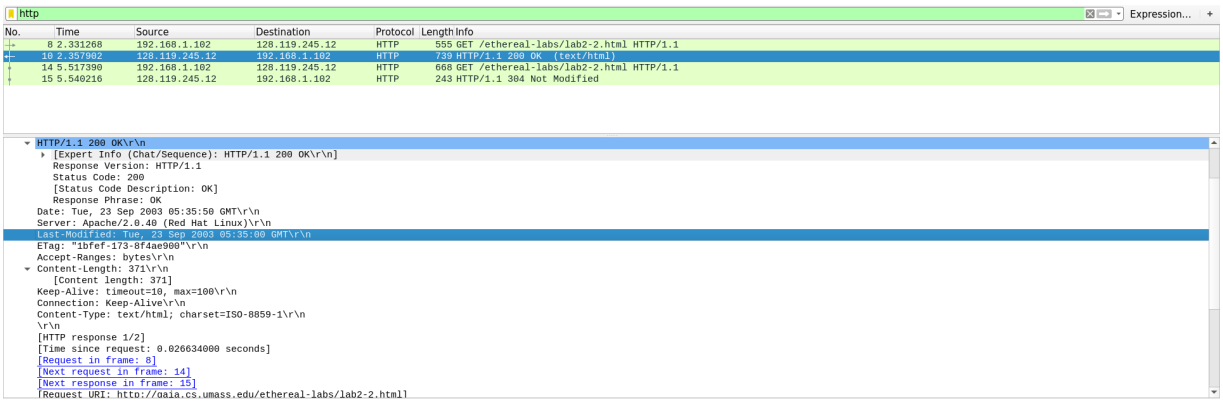
File: http-ethereal-trace-2

Inspect the contents of the first HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?



Nope

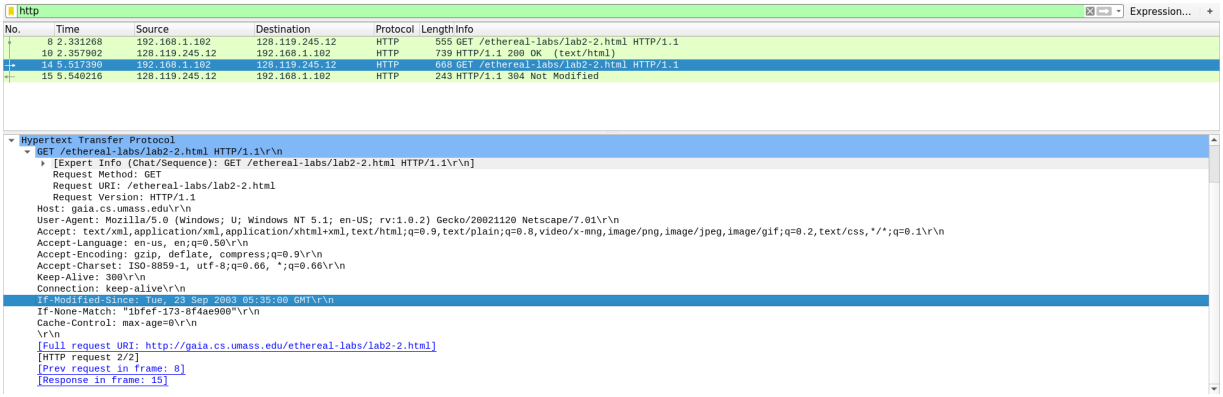
Does the response indicate the last time that the requested file was modified?



Yes, `Tue, 23 Sep 2003 05:35:00 GMT`

Now inspect the contents of the second HTTP GET request from the

browser to the server. Do you see an “IF-MODIFIED-SINCE” and “IF-NONE-MATCH” lines in the HTTP GET? If so, what information is contained in these header lines?

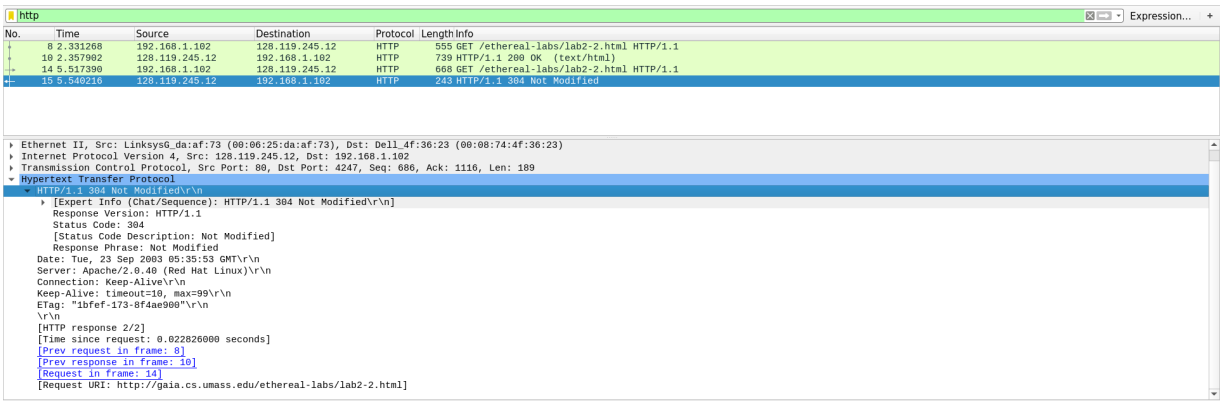


Yes, the information contained is as follows

Code

```
1  If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT
2  If-None-Match: "1bfef-173-8f4ae900"
```

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.



A `304 Not Modiified` response was returned.
The server did not explicity return the contents of the file, rather the client should respond to this message by using the locally stored copy of the requested file.s

What is the value of the Etag field in the 2nd response message and how it is used? Has this value changed since the 1st response message was received?

ETag in first response: `1bfef-173-8f4ae900`

ETag in second response: `1bfef-173-8f4ae900`

The Etag field has not changed in value.

Exercise 5: Ping Client

Server: PingServer.java - `LOSS_RATE = 0.5` , `AVERAGE_DELAY = 100`
Client: PingClient.py

Server

Code

```
$> java PingServer 1025
Received from 127.0.0.1: PING 0 1583458445519
   Reply not sent.
Received from 127.0.0.1: PING 1 1583458446521
   Reply sent.
Received from 127.0.0.1: PING 2 1583458446591
   Reply not sent.
Received from 127.0.0.1: PING 3 1583458447593
   Reply sent.
Received from 127.0.0.1: PING 4 1583458447768
   Reply not sent.
Received from 127.0.0.1: PING 5 1583458448769
   Reply not sent.
Received from 127.0.0.1: PING 6 1583458449771
   Reply sent.
Received from 127.0.0.1: PING 7 1583458449795
   Reply not sent.
Received from 127.0.0.1: PING 8 1583458450795
   Reply sent.
Received from 127.0.0.1: PING 9 1583458450888
   Reply not sent.
```

Client

Code

```
$> python3 PingClient.py localhost 1025
ping to localhost, seq = 0, time out
ping to localhost, seq = 1, rtt = 70ms
ping to localhost, seq = 2, time out
ping to localhost, seq = 3, rtt = 174ms
ping to localhost, seq = 4, time out
ping to localhost, seq = 5, time out
ping to localhost, seq = 6, rtt = 24ms
ping to localhost, seq = 7, time out
ping to localhost, seq = 8, rtt = 93ms
ping to localhost, seq = 9, time out

Minimum RTT: 24ms
Maximum RTT: 174ms
Average RTT: 90.25ms
```

‹ Delay