

## Lab 02 - Ryan McClue (z5346008)

### 1. Wireshark HTTP GET Request/Response

No.	Time	Source	Destination	Protocol	Length	Info
104.694850		192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
124.718993		128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
134.724332		192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
144.750366		128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

▶ Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)

▶ Ethernet II, Src: LinksysG\_da:af:73 (00:06:25:da:af:73), Dst: Dell\_4f:36:23 (00:08:74:4f:36:23)

▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385

▼ Hypertext Transfer Protocol

▶ HTTP/1.1 200 OK\r\n

Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n

Server: Apache/2.0.40 (Red Hat Linux)\r\n

Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n

ETag: "1bfed-49-79d5bf00"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 73\r\n

Keep-Alive: timeout=10, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=ISO-8859-1\r\n

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

Status Code: 200

Status Phrase: OK

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

Tue, 23 Sep 2003, 5:29:00 GMT

2.2 *Does the response also contain a DATE header?*

Yes. It's Tue, 23 Sep 2003, 5:29:50 GMT

2.3 *How are these two fields different?*

The **Date** header is the time when the server sent the response message. The **Last-Modified** header is the time when the server believes the resource requested was last changed.

3.1 *Is the connection established between the browser and the server persistent or non-persistent?*

Persistent.

3.2 *How can you infer this?*

HTTP1.1 is being used, which introduced persistent connection capabilities. Furthermore, the presence of the header field **Connection: Keep-Alive** in the HTTP request/response indicates that a single TCP connection can be used for multiple requests/responses.

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

73

- Line-based text data: text/html (3 lines)

A html file containing:

## 2. Wireshark HTTP Conditional GET Request/Response

No.	Time	Source	Destination	Protocol	Length	Info
82.331268		192.168.1.102	128.119.245.12	HTTP	555 GET	/etheral-labs/lab2-2.html HTTP/1.1
102.357902		128.119.245.12	192.168.1.102	HTTP	739 HTTP/1.1 200 OK	(text/html)
145.517390		192.168.1.102	128.119.245.12	HTTP	668 GET	/etheral-labs/lab2-2.html HTTP/1.1
155.540216		128.119.245.12	192.168.1.102	HTTP	243 HTTP/1.1 304 Not Modified	

No

No.	Time	Source	Destination	Protocol	Length	Info
+	82.331268	192.168.1.102	128.119.245.12	HTTP	555 GET	/etherbase-labs/lab2-2.html HTTP/1.1
-	102.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
-	145.517390	192.168.1.102	128.119.245.12	HTTP	668 GET	/etherbase-labs/lab2-2.html HTTP/1.1
-	155.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Yes.

### 3.1 Do you see an “IF-MODIFIED-SINCE:” and “IF-NONE-MATCH” lines in

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

```
Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614
Hypertext Transfer Protocol
GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css;*/\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
Accept-Charset: ISO-8859-1, utf-8;q=0.66, */q=0.66\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
If-None-Match: "1bfef-173-8f4ae900"\r\n
Cache-Control: max-age=0\r\n
```

the HTTP GET?

Yes

### 3.2 If so, what information is contained in these header lines?

If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT

If-None-Match: "1bfef-173-8f4ae900"

### 4.1 What is the HTTP status code and phrase returned from the server in re-

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

```
Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 686, Ack: 1116, Len: 189
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n
Server: Apache/2.0.40 (Red Hat Linux)\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=10, max=99\r\n
ETag: "1bfef-173-8f4ae900"\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.022826000 seconds]
[Prev request in frame: 8]
[Prev response in frame: 10]
[Request in frame: 14]
[Request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
```

sponse to this second HTTP GET?

Status Code: 304

Status Phrase: Not Modified

### 4.2 Did the server explicitly return the contents of the file? Explain.

No. The webserver determined that the file requested was already present in the client's browser cache and therefore did not need to return the file contents.

### 5.1 What is the value of the Etag field in the 2nd response message and how it is used?

ETag: "1bfef-173-8f4ae900". It's used to determine if the content of a requested resource has changed on the server side and needs to be sent back to the client. Furthermore, it's used in conjunction with the timestamp given by If-Modified-Since to implement conditional GET requests.

### 5.2 Has this value changed since the 1st response message was received?

No

### 3. PingClient

```
Received from 127.0.0.1: PING 3341 4156850
  Reply sent.
Received from 127.0.0.1: PING 3342 4156954
  Reply sent.
Received from 127.0.0.1: PING 3343 4157097
  Reply sent.
Received from 127.0.0.1: PING 3344 4157287
  Reply sent.
Received from 127.0.0.1: PING 3345 4157359
  Reply sent.
```

```
ping to 127.0.0.1, seq = 1, rtt = 'time out'
ping to 127.0.0.1, seq = 2, rtt = 'time out'
ping to 127.0.0.1, seq = 3, rtt = 189 ms
ping to 127.0.0.1, seq = 4, rtt = 'time out'
ping to 127.0.0.1, seq = 5, rtt = 'time out'
ping to 127.0.0.1, seq = 6, rtt = 90 ms
ping to 127.0.0.1, seq = 7, rtt = 'time out'
ping to 127.0.0.1, seq = 8, rtt = 'time out'
ping to 127.0.0.1, seq = 9, rtt = 69 ms
ping to 127.0.0.1, seq = 10, rtt = 14 ms
ping to 127.0.0.1, seq = 11, rtt = 104 ms
ping to 127.0.0.1, seq = 12, rtt = 143 ms
ping to 127.0.0.1, seq = 13, rtt = 190 ms
ping to 127.0.0.1, seq = 14, rtt = 72 ms
ping to 127.0.0.1, seq = 15, rtt = 96 ms
min. rtt: 14 ms, max. rtt: 190 ms, avg. rtt: 107.44 ms
```