

## Lab 2 by John Dao, z5258962

### Exercise 3: Using Wireshark to understand basic HTTP request/response messages (marked, include in your report)

The full response (HTTP):

```
▼ HTTP/1.1 200 OK\r\n
  ▼ [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, 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
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.024143000 seconds]
    [Request in frame: 10]
    [Next request in frame: 13]
    [Next response in frame: 14]
    [Request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-1.html]
    File Data: 73 bytes
  Line-based text data: text/html (3 lines)
```

Q1: What is the status code and phrase returned from the server to the client browser?

The status code and phrase returned from the server to the client is **200** with status description of “**ok**”

Q2: When was the HTML file that the browser is retrieving last modified at the server? Does the response also contain a DATE header? How are these two fields different?

The date that the HTML file that is retrieved by the browser was last modified on **tuesday, 23 Sep 2003 at 05:29:00 GMT**

Q3: Is the connection established between the browser and the server persistent or non-persistent? How can you infer this?

The Connection established is persistent with the fact that the connection header contains **Keep-Alive** with a timeout of 10 and max of 100. This means that every connection will

continue to sent and receive HTTP requests without the need to continually refresh/open a new connection.

Q4: How many bytes of content are being returned to the browser?

The file data size is **73 bytes** as designated by the header named “File Data”

Q5: What is the data contained inside the HTTP response packet?

```
File Data: 73 bytes
Line-based text data: text/html (3 lines)
<html>\n
Congratulations. You've downloaded the file lab2-1.html!\n
</html>\n
```

## Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction (marked, include in your report)

The full response (GET):

```
> Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
▼ Hypertext Transfer Protocol
  ▼ GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
      [GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /ethereal-labs/lab2-2.html
      Request Version: HTTP/1.1
      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\
      Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng
      Accept-Language: en-us, en;q=0.50\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
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
      [HTTP request 1/2]
```

Q1: 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?

No, there is no such line in the HTTP GET

Q2: Does the response indicate the last time that the requested file was modified?

Yes. The file was last modified **Tue, 23 sep 2003 at 05:35:00 GMT**

Q3: 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?

Full response:



The screenshot shows the 'Hypertext Transfer Protocol' tab in a browser's developer tools. It displays the details of a GET request to `/ethereal-labs/lab2-2.html` over HTTP/1.1. The request includes various headers such as `User-Agent`, `Accept`, `Accept-Language`, `Accept-Encoding`, `Accept-Charset`, `Keep-Alive`, `Connection`, `If-Modified-Since`, `If-None-Match`, and `Cache-Control`. The `If-Modified-Since` header is set to `Tue, 23 Sep 2003 05:35:00 GMT` and the `If-None-Match` header is set to `"1bfef-173-8f4ae900"`. The status bar at the bottom indicates the request is the second of two for this frame.

```
▼ Hypertext Transfer Protocol
  ▼ GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
      [GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /ethereal-labs/lab2-2.html
      Request Version: HTTP/1.1
      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,ir\r\n
      Accept-Language: en-us, en;q=0.50\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
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
      [HTTP request 2/2]
      [Prev request in frame: 8]
      [Response in frame: 15]
```

Yes.

“IF-MODIFIED-SINCE:” contains: TUE, 23 Sep 2003 05:35:00 GMT

“IF-NONE-MATCH” contains: “1bfef-173-8f4ae900”

Q4: 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.

Full response:

```
▼ 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, 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]
```

The HTTP status was **304** with a description of **Not modified**.

In this event where the status was not modified, the server did not return the contents of the file. This is due to the fact that there was no change in the file and thus no need to modify the local file.

Q5: 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?

The value of the Etag in the 2nd response is **ETag: "1bfef-173-8f4ae900"**.

This value has not changed since the 1st response message was received.

The etag is used to compare whether the cache and the incoming resources are different.

They are different when the etags are not matched and in this case, the cache and the incoming resource are the same, explaining the 304 not modified status.

**Exercise 5: Ping Client (marked, submit source code as a separate file, include sample output in the report)**

```
λ python PingClient.py 127.0.0.1 100
Ping to 127.0.0.1, seq = 3331, time out
Ping to 127.0.0.1, seq = 3332, rtt = 30 ms
Ping to 127.0.0.1, seq = 3333, rtt = 160 ms
Ping to 127.0.0.1, seq = 3334, rtt = 159 ms
Ping to 127.0.0.1, seq = 3335, rtt = 190 ms
Ping to 127.0.0.1, seq = 3336, rtt = 189 ms
Ping to 127.0.0.1, seq = 3337, rtt = 85 ms
Ping to 127.0.0.1, seq = 3338, rtt = 139 ms
Ping to 127.0.0.1, seq = 3339, rtt = 199 ms
Ping to 127.0.0.1, seq = 3340, rtt = 42 ms
Ping to 127.0.0.1, seq = 3341, time out
Ping to 127.0.0.1, seq = 3342, rtt = 51 ms
Ping to 127.0.0.1, seq = 3343, rtt = 5 ms
Ping to 127.0.0.1, seq = 3344, rtt = 122 ms
Ping to 127.0.0.1, seq = 3345, rtt = 95 ms
Minimum rtt is: 5.357177734375
Maximum of rtt is: 199.002685546875
average rtt is: 113.22278771033653
```