

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

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

- Status Code: 200, Response Phrase: 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 HTML file was last modified on Tue, 23 Sep 2003 05:29:00 GMT
- The response does contain a date header.
- Date is the date and time that the message was sent. Last-modified is the last modified date for the requested object.

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

- The connection established between is persistent.
- In both the HTTP request and response headers, we can see that the connection field is "Keep-Alive", which means using a single TCP connection to send and receive multiple HTTP requests / responses. This is by default on HTTP 1.1.

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

- 73 bytes of content

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

- Text and html data

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

**Q1: Do you see an "IF-MODIFIED-SINCE" line in the first HTTP GET request?**

- No there no "IF-MODIFIED-SINCE" line in the first HTTP GET request.

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

- Yes it does indicate that. The last-modified field shows Tue, 23 Sep 2003 05:35:00 GMT

**Q3: Do you see an "IF-MODIFIED-SINCE" line in the second HTTP GET request?**

- Yes there is an "IF-MODIFIED-SINCE" field.
- It shows the value Tue, 23 Sep 2003 05:35:00 GMT

**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.**

- The status code = 304, the phrase = "Not Modified"
- The server **did not return the body contents** of the file. This is due to the fact that the GET request is only conditional. The server will only send back the request resource if only it has been last modified after a given date. If the request has not been modified since, the response will be **304 status** without any body.
- This will save resources as the party making the GET request will not have to download the page again since nothing has been changed. They will only need to download it again when there is new information.
- One example use is Google's Webpage Crawlers who have to crawl through billions of webpages. If your page shows a 304 response then the bots won't need to waste bandwidth crawling the page again since it is still the same as last time.