Reference for Lab Exercise – 3

Wireshark – HTTP

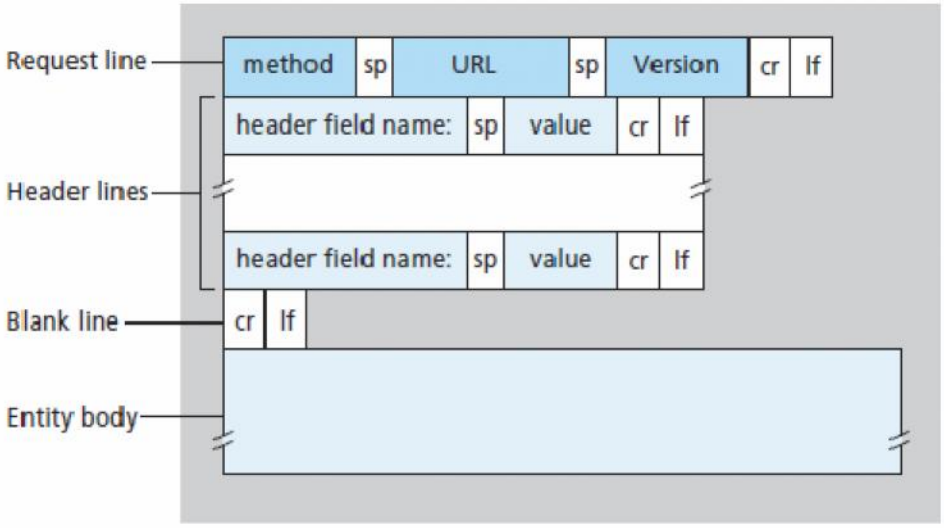

Figure 2.8 ♦ General format of an HTTP request message

HTTP Request Message

Below we provide a typical HTTP request message:
GET /somedir/page.html HTTP/1.1
Host: www.someschool.edu
Connection: close
User-agent: Mozilla/5.0
Accept-language: fr

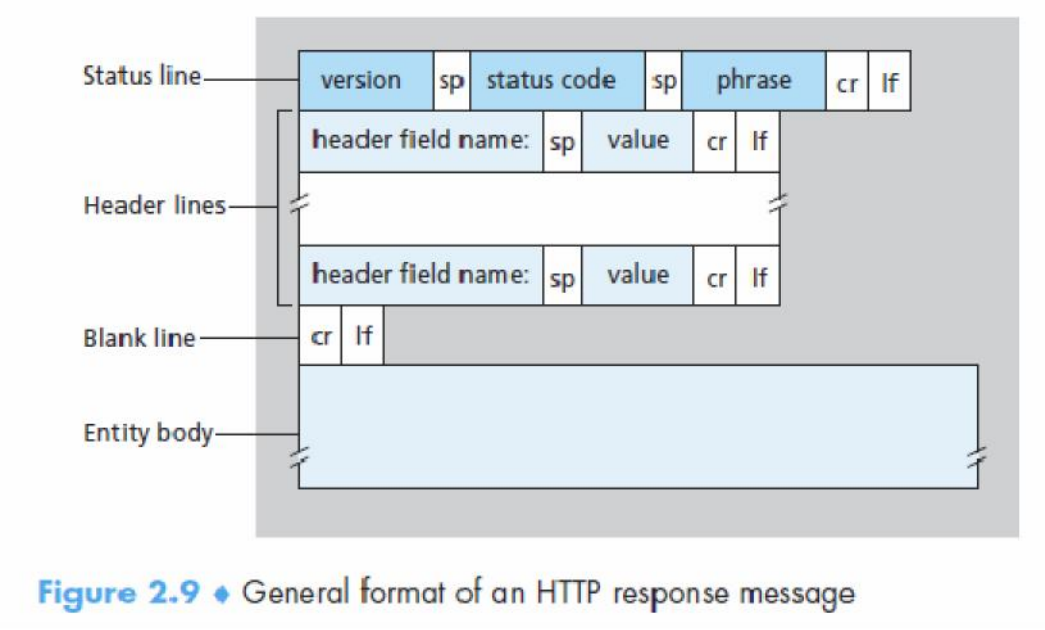

Figure 2.9 ♦ General format of an HTTP response message

HTTP Response Message

HTTP/1.1 200 OK
Connection: close
Date: Tue, 09 Aug 2011 15:44:04 GMT
Server: Apache/2.2.3 (CentOS)
Last-Modified: Tue, 09 Aug 2011 15:11:03 GMT
Content-Length: 6821
Content-Type: text/html
(data data data data data ...)

Conditional GET
First Request

```
GET /fruit/kiwi.gif HTTP/1.1
Host: www.exotiquecuisine.com
```

First Response

```
HTTP/1.1 200 OK
Date: Sat, 8 Oct 2011 15:39:29
Server: Apache/1.3.0 (Unix)
Last-Modified: Wed, 7 Sep 2011 09:23:24
Content-Type: image/gif

(data data data data data ...)
```

Second Request

```
GET /fruit/kiwi.gif HTTP/1.1
Host: www.exotiquecuisine.com
If-modified-since: Wed, 7 Sep 2011 09:23:24
```

Second Response

```
HTTP/1.1 304 Not Modified
Date: Sat, 15 Oct 2011 15:39:29
Server: Apache/1.3.0 (Unix)

(empty entity body)
```

The Basic HTTP GET/response interaction

Do the following:

1. Start up your web browser.

2. Start up the Wireshark packet sniffer, (but don't yet begin packet capture). Enter "http in the display-filter-specification window

3. Wait a bit more than one minute, and then begin Wireshark packet capture.

4. Enter the following to your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html Your browser should display the very simple, one-line HTML file.

5. Stop Wireshark packet capture.

The HTTP CONDITIONAL GET/response interaction

Make sure your browser's cache is empty. For Internet Explorer, select *Tools->Internet Options->Delete File;* these actions will remove cached files from your browser's cache. Now do the following:

1. Start up your web browser, and make sure your browser's cache is cleared.

2. Start up the Wireshark packet sniffer.

3. Enter the following URL into your browser
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

4. Your browser should display a very simple five-line HTML file.

5. Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)

6. Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Retrieving Long Documents

1. Start up your web browser, and make sure your browser's cache is cleared.

2. Start up the Wireshark packet sniffer

3. Enter the following URL into your browser
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html
   Your browser should display the lengthy US Bill of Rights.

4. Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

HTML Documents with Embedded Objects

1. Start up your web browser, and make sure your browser's cache is cleared

2. Start up the Wireshark packet sniffer

3. Enter the following URL into your browser
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

   Note: Your browser should display a short HTML file with two images. These two images are referenced in the base HTML file. That is, the images themselves are not contained in the HTML; instead the URLs for the images are contained in the downloaded HTML file. your browser will have to retrieve these logos from the indicated web sites. The publisher's logo is retrieved from the www.aw-bc.com web site. The image of the book's cover is stored at the manic.cs.umass.edu server.

4. Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

HTTP Authentication

Do the following:

1. Make sure your browser's cache is cleared

2. Then, start up your browser

3. Start up the Wireshark packet sniffer

4. Enter the following URL into your browser
   http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
   Type the user name as *wireshark-students* and password *network* into the pop up box.

5. Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.