Lab 2 - Hypertext Transfer Protocol (HTTP)

Filippi Imperatriz Santos

This lab is adapted from "Wireshark Lab: HTTP v8.0 Supplement to Computer Networking: A Top-Down Approach" (Kurose and Ross, 2020).

Learning objectives

- Understand HTTP basic request and response messages.
- Understand the formats and contents of different HTTP messages.

Introduction

Lab1 provided an introduction to Wireshark, moving forward, we will be using Wireshark to investigate and explore some TCP/IP protocol suite. In this lab, you will be using Wireshark to explore HTTP request and response messages.

Download Windows **CCOM** template image on Desktop PC and complete the following tasks.

Tasks

1. Capturing HTTP messages

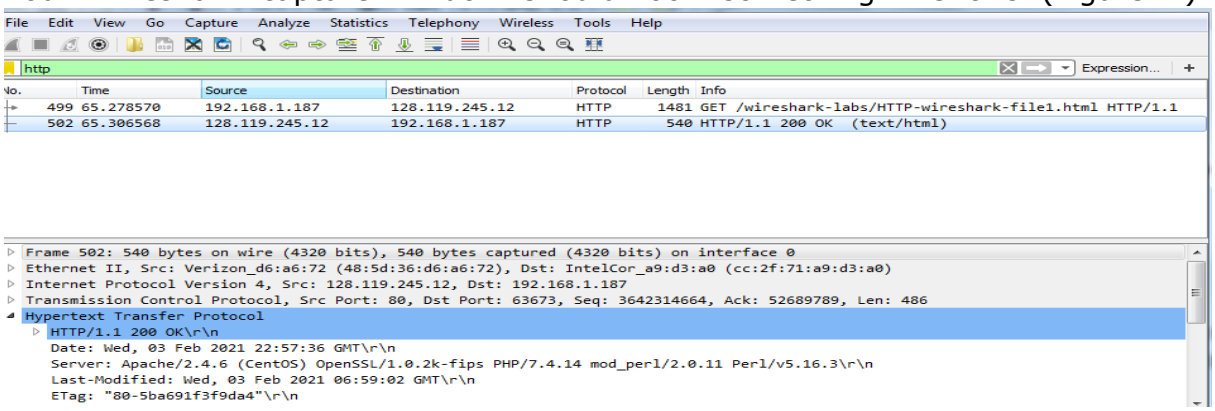
- Start web browser on your PC, by double-clicking 'Google Chrome' icon on desktop.
- Launch Wireshark by double-clicking the 'Wireshark' icon on desktop and start a new capture (see lab1 for instructions).
- In browser Widow, enter the URL http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html and press Return.
- Stop the capture, once your browser displayed the page shown below.

Congratulations. You've downloaded the file http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!

If you cannot capture HTTP packets, download 'HTTP-trace-1' file from MyBeckett (see 'Labs' folder, 'Wireshark Trace Files', Lab2-HTTP), and open it in Wireshark.

- Filter the packets displayed in the Wireshark window by entering 'http' (lowercase, no quotes) into the display filter specification window at the top of the Wireshark window, and press Return.

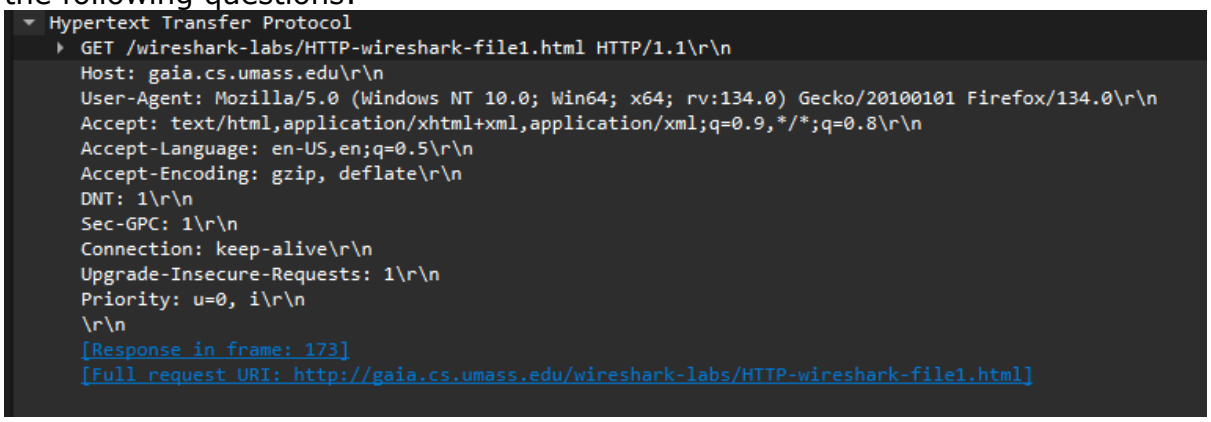
Your Wireshark capture window should look something like this (Figure 1).



(Fig 1)

Note - In this lab, we are studying Hypertext Transfer Protocol (HTTP), as shown in figure 1, only expand the HTTP section in 'Packet details' window and leave other protocols (i.e., Frame, Ethernet, IP and TCP) hidden. We will study the other protocols in later lectures and labs.

Select the client request message ('GET') in packet capture window and answer the following questions:



- Is your browser running HTTP version 1.0 or 1.1?
  1.1

- What languages (if any) does your browser indicate that it can accept to the server? **En, en-US**

- What is the IP address of your computer? SRC: 192.168.1.229 (not destination as highlighted)

```
    [Stream index: 1]
▾ Internet Protocol Version 4, Src: 192.168.1.22, Dst: 128.119.245.12
    0100 .... = Version: 4
```

Select the 'response' message from the server and answer the following questions:

- What version of HTTP is the server running? **1.1**
- What is the IP address of the server?

```
▾ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.229
```

- What is the status code returned from the server to your browser?

```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

- When the HTML file that you are retrieving was last modified at the server?

```
Date: Tue, 04 Feb 2025 14:07:49 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Tue, 04 Feb 2025 06:59:01 GMT\r\n
```

- How many bytes of content are being returned to your browser?

```
    File Data: 128 bytes
▾ Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
```

2. HTTP conditional GET request and response messages

As you recall from lecture2, web caching is used by the browser to improve the performance of accessing Web pages and it performs a conditional GET when retrieving an HTTP object.

Clear your Chrome browser cache by completing the following:

- Start Chrome browser.
- Click on the Settings menu (3 dots) in top-right corner.
- Click on Settings.
- On the left side, click Privacy and security.
- In the Privacy and security section click Delete browsing data
- Click the Basic tab.
- For Time range, select All time.
- Tick Cached images and files.
- Click Delete data button.

Make sure your browser cache is empty.

- Start Chrome browser on your PC.

- Launch Wireshark by double-clicking the 'Wireshark' icon on the desktop and start a new capture (see lab1 for instructions).

- In browser Widow, enter the URL http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html and press Return.

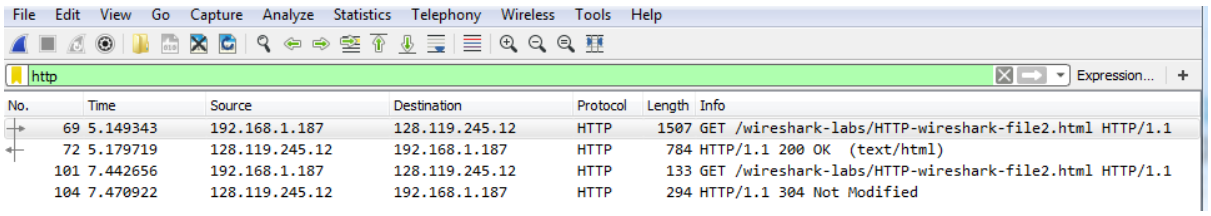
- Once your browser displayed the page, refresh your browser by clicking the refresh button . Alternatively, enter the above URL again and press Return.

- Stop the capture.

If you cannot capture HTTP packets, download 'HTTP-trace-2' file from MyBeckett (see 'Labs' folder, 'Wireshark Trace Files', Lab2-HTTP), and open it in Wireshark.

- Filter the packets displayed in the Wireshark window by entering 'http' (lowercase, no quotes) into the display filter specification window at the top of the Wireshark window, and press Return.

Your Wireshark capture window should look something like one below (Figure 2).



(Fig 2)

Select the first request message ('GET') in packet capture window.

- Do you see the "If-Modified Since"" line in the HTTP GET?

No

```
▼ Hypertext Transfer Protocol
  ▼ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/13
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: https://ukc-word-edit.officeapps.live.com/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 377]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

- Has the server returned the contents of the file that was requested by your browser? Yes

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 04 Feb 2025 14:17:02 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 04 Feb 2025 06:59:01 GMT\r\n
    ETag: "173-62d4b8b35ea45"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 375]
    [Time since request: 0.087432000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
▶ Line-based text data: text/html (10 lines)
```

- Select the second request message ('GET') in packet capture window.

- Do you see the "If-Modified-Since" line in the HTTP GET? If yes, what information is listed after If-Modified Since?
  Yes

```
▾ Hypertext Transfer Protocol
  ▾ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: https://ukc-word-edit.officeapps.live.com/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Tue, 04 Feb 2025 06:59:01 GMT\r\n
    If-None-Match: "173-62d4b8b35ea45"\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 515]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

- What is the HTTP status code and phrase returned from the server in response to the second HTTP GET message?

```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 304 Not Modified\r\n
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Tue, 04 Feb 2025 14:17:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-62d4b8b35ea45"\r\n
    \r\n
    [Request in frame: 513]
    [Time since request: 0.089530000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

- Did the server explicitly return the contents of the file?

No

3. Downloading a Web page with embedded objects

Next, we will look at what happens when your browser downloads a file (a web page) with embedded objects (images).

- Start Chrome browser on your PC.

- Launch Wireshark by double-clicking 'Wireshark' icon on desktop and start a new capture (see lab1 for instructions).

- In browser Widow, enter the URL http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html and press Return.

- Stop the capture once your browser displayed the page.

If you cannot capture HTTP packets, download the 'HTTP-trace-3' file from MyBeckett (see 'Labs' folder, 'Wireshark Trace Files', Lab2-HTTP), and open it in Wireshark.

- Filter the packets displayed in the Wireshark window by entering 'http' (lowercase, no quotes) into the display filter specification window at the top of the Wireshark window, and press Return.

Your Wireshark capture window should look something like one below (Figure 3).

http | Expression... | +

No.	Time	Source	Destination	Protocol	Length	Info
12	1.222524	192.168.1.187	128.119.245.12	HTTP	1507	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
17	1.255989	128.119.245.12	192.168.1.187	HTTP	1355	HTTP/1.1 200 OK (text/html)
19	1.293632	192.168.1.187	128.119.245.12	HTTP	1427	GET /pearson.png HTTP/1.1
25	1.321639	128.119.245.12	192.168.1.187	HTTP	745	HTTP/1.1 200 OK (PNG)
29	1.387687	192.168.1.187	178.79.137.164	HTTP	443	GET /8E_cover_small.jpg HTTP/1.1
31	1.478827	178.79.137.164	192.168.1.187	HTTP	225	HTTP/1.1 301 Moved Permanently

- How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
-

Source	Destination	Protocol	Length	Info
192.168.1.229	128.119.245.12	HTTP	440	GET /wireshark-labs/HTTP-wireshark-file4.htm HTTP/1.1
128.119.245.12	192.168.1.229	HTTP	567	HTTP/1.1 404 Not Found (text/html)
192.168.1.229	128.119.245.12	HTTP	441	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
128.119.245.12	192.168.1.229	HTTP	1355	HTTP/1.1 200 OK (text/html)
192.168.1.229	128.119.245.12	HTTP	464	GET /pearson.png HTTP/1.1
128.119.245.12	192.168.1.229	HTTP	762	HTTP/1.1 200 OK (PNG)
192.168.1.229	178.79.137.164	HTTP	431	GET /8E_cover_small.jpg HTTP/1.1
178.79.137.164	192.168.1.229	HTTP	225	HTTP/1.1 301 Moved Permanently
2a00:23c8:950b:6b01…	2a00:23a0:1c2:108::…	OCSP	515	Request
2a00:23c8:950b:6b01…	2a00:23a0:1c2:108::…	OCSP	515	Request
2a00:23a0:1c2:108::…	2a00:23c8:950b:6b01…	OCSP	963	Response
2a00:23a0:1c2:108::…	2a00:23c8:950b:6b01…	OCSP	963	Response
192.168.1.229	128.119.245.12	HTTP	527	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
128.119.245.12	192.168.1.229	HTTP	294	HTTP/1.1 304 Not Modified

3 -

- Can you tell whether your browser downloaded the two images from one or two web sites? Explain your answer.

Two different websites – different IP address on the destinations of the request – different hosts

```
Host: kurose.cslash.net\r\n
```

4. HTTP Authentication

Next you will try to download a page from a web site that is password-protected and examine the sequence of HTTP messages.

- Make sure your browser cache is empty (see task 2 for instructions).
- Close your browser, then open Chrome browser on your PC.
- Launch Wireshark by double-clicking the 'Wireshark' icon on the desktop and start a new capture (see lab1 for instructions).
- In browser Window, enter the URL http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html and press Return.
- Enter the 'wireshark-students' for username and 'network' for password (no quotes) and click "sign in" (ok) button.
- Stop the capture.

If you cannot capture HTTP packets, download 'HTTP-trace-4' file from MyBeckett (see 'Labs' folder, 'Wireshark Trace Files', Lab2-HTTP), and open it in Wireshark.

Source	Destination	Protocol	Length	Info
192.168.1.229	128.119.245.12	HTTP	509	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
128.119.245.12	192.168.1.229	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
192.168.1.229	128.119.245.12	HTTP	568	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
128.119.245.12	192.168.1.229	HTTP	583	HTTP/1.1 404 Not Found (text/html)
192.168.1.229	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
128.119.245.12	192.168.1.229	HTTP	538	HTTP/1.1 404 Not Found (text/html)

- Filter the packets displayed in the Wireshark window by entering 'http' (lowercase, no quotes) into the display filter specification window at the top of the Wireshark window, and press Return.
- What is the response status code and phrase to the initial to first HTTP GET message from your browser?

```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 401 Unauthorized\r\n
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
```

- Can you see any field sent in the second HTTP GET message? Explain.

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: https://ukc-word-edit.officeapps.live.com/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
        Credentials: wireshark-students:network
    \r\n
    [Response in frame: 280]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
```

- What is the response status code and phrase to the second HTTP GET message from your browser?

```
HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Sat, 06 Feb 2021 02:41:04 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Fri, 05 Feb 2021 06:59:01 GMT\r\n
  ETag: "84-5ba915ae602ea"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 132\r\n
    [Content length: 132]
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [Request in frame: 206]
  [Time since request: 0.039133000 seconds]
  [Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
  File Data: 132 bytes
```

5. Reflection and class discussion.