CSCE-5580 Computer Network

Lab-2 HTTP

1. Start up the Wireshark packet sniffer, as described in the introductory lab (but don’t yet start packet capture).
2. Enter “http” (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We’re only interested in the HTTP protocol here, and don’t want to see the clutter of all captured packets).
3. Start capturing the packets.

Graphical user interface, text, application

Description automatically generated

**NOTE: Take and attach screenshots for all the questions in work documents (Use the snipper tool).**

* 1. Answer the following question after running the following link in the browser <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

1. What is the version of HTTP on the server and your browser with Screenshots? What is the language accepted by your browser?

The version of HTTP on the server is HTTP/1.1. The version of HTTP in the browser is also HTTP/1.1. The accepted language by the browser is English (United States en-us) and English (United Kingdom en-gb), as indicated by the "Accept-Language" header in the HTTP request.

Graphical user interface, text, application, email

Description automatically generated

Language:

Graphical user interface, text, application, email

Description automatically generated

1. What is the source IP address of the response that you received after sending the GET request?

Graphical user interface, text, application

Description automatically generated

1. What is the status code that you received in the response? Write about any two-status code.

The status code received in the response is 200. Two other common HTTP status codes are 304 NOT MODIFIED and 404 NOT FOUND. HTTP 200 OK status code indicates that the request has succeeded, and the response contains the requested data. HTTP 404 NOT FOUND status code indicates that the requested resource was not found on the server. HTTP 304 NOT MODIFIED status code indicates that the requested resource has not been modified since the last request.

Graphical user interface, text, application, email

Description automatically generated

1. What is the last modified date with the time of the file that you’ve received in the response with a screenshot?

The last modified date and time of the file that was received in the response are Fri, 24 Mar 2023 05:59:02 GMT. You can find this information in the "Last-Modified" header of the server response. Here's a screenshot that highlights the Last-Modified field:

Graphical user interface, text, application, email

Description automatically generated

1. What are timeout and max field values? (Hint: you can find this in the keepalive field)

The "Keep-Alive" field in the response header contains the "timeout" and "max" values. The "timeout" field specifies the maximum number of seconds the server should keep the connection open if there are no new requests from the client. In this case, it is set to 5 seconds. The "max" field specifies the maximum requests the client can send during the keep-alive connection. In this case, it is set to 100 submissions.

Graphical user interface, text, application, email

Description automatically generated

1. Answer the following question after running the following link in the browser <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>
2. What is the length of the response packet after running the above link in your browser?

The Total Length field in the IP header gives the correct packet length for the IP packet, which includes both the IP header and the encapsulated TCP segment with its payload data. In this case, the Total Length field value is **770 bytes**. The the length of the payload data carried in the HTTP response, then the Content-Length header value of **371 bytes** would be more relevant. The frame length 784 refers to the size of the captured packet that Wireshark reports. The TCP payload field 730 indicates the size of the data that is being transmitted in the packet.

Graphical user interface, text, application, email

Description automatically generated

1. What is the difference between the length of the response packets? (1st Response and 2nd response)

Difference = Length of the response packets 1 - Length of the response packet 2

= 770 – 280

= 49

First Response:

Graphical user interface, text, application, email

Description automatically generated

Second Response:

Graphical user interface, text, application

Description automatically generated

1. Enter the following link again then answer the questions.

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

1. What is the status code for the response?

The status code for the response is "304 Not Modified" because we are just reloading the file again, that was just loaded few minutes ago. It is an HTTP response status code that indicates that the requested resource has not been modified since the last time it was accessed by the client, which means that the client's cached version of the requested resource is still valid, and the server did not send the complete content of the requested file.

Graphical user interface, text, application, email

Description automatically generated

1. Answer the following question after running the following link in the browser. <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>
2. What is the file length after running the above link in your browser?

The file length is 4500. This indicates that the file being transmitted in this capture is 4500 bytes in length.

Graphical user interface, text, application

Description automatically generated

1. What is the background(bgcolor) color mentioned in the HTML document?

The HTML response from the server does not contain any "background" attribute, so it is not possible to determine the background color of the HTML page from this packet capture. The background(bgcolor) color mentioned in the HTML document is "#FFFFFF", which represents white.

Text

Description automatically generated

1. How many GET request was sent to receive The Bill of Rights HTML file from the server?

Only one Get Request was sent to receive The Bill of Rights HTML file from the server.

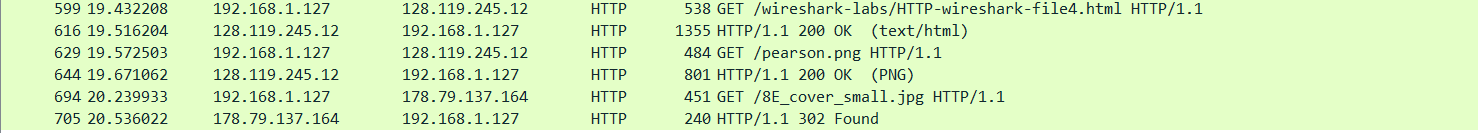
Graphical user interface, text, application, email

Description automatically generated



1. Answer the following question after running the following link in the browser. <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>
2. What is the content-type of the file that was received in the response after the first GET Request? How many GET requests were sent to retrieve the whole page?

There were three GET requests sent to retrieve the whole page.



First GET Request: to load the webpage as text/html.

Graphical user interface, text, application, email

Description automatically generated

Second GET Request: to get the PNG image.

Graphical user interface, text, application, email

Description automatically generated

Third GET Request: to get the JPG image.

Graphical user interface, text, application, email

Description automatically generated

The content type of the file received in response to the first GET request (/wireshark-labs/HTTP-wireshark-file4.html) is "text/html".

Graphical user interface, text, application, email

Description automatically generated

1. What is the width and height of the file received in response (PNG - Portable Network Graphics)? Include File Data as well?

The file received in response is a PNG file with a width of 253 pixels and a height of 199 pixels. The file data starts with the PNG signature bytes: 89 50 4E 47 0D 0A 1A 0A.

Text

Description automatically generated

File Data:

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

1. What is the host of the GET request of /8E\_cover\_small.jpg?

The host of the GET request for /8E\_cover\_small.jpg is:

Host: kurose.cslash.net\r\n

Graphical user interface, text, application, email

Description automatically generated

1. What is the location of /8E\_cover\_small.jpg file in response 302 found?

The location of the /8E\_cover\_small.jpg file in the HTTP response 302 Found is:

Location: <https://block.charter-prod.hosted.cujo.io/warn.html?url=http://kurose.cslash.net/8E_cover_small.jpg&token=46ddd919>

It is specified in the "Location" header of the HTTP response.

Graphical user interface, text, application, email

Description automatically generated