Assignment 4 Wireshark

Computer Network

Program: MScIT Sem-2

Group ID : 28

Student Name	Student ID
Dev Adnani	202212012
Saif Saiyed	202212083

202212012

2.1 Exercise:

1. Start your web browser.

Start the Wireshark tool, as described in the Introductory lab (but don't yet begin packet capture). 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 are only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).

2. Begin Wireshark packet capture.

3. Enter the following to your browser.
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1. Html

4. Stop Wireshark packet capture.

2.2 Questions - Answers:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer : 1.1

2.What languages (if any) does your browser indicate that it can accept to the server?

Answer : en-US,en;q=0.9\r\n

3. What is the IP address of your computer? and the gaia.cs.umass.edu server?

Answer: IPV 4, Src: 10.100.76.226, Dst: 128.119.245.12

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

Answer : 511

The HTTP 511 Network Authentication Required response status code **indicates that the client needs to authenticate to gain network access**

5. When was the HTML file that you are retrieving last modified at the Server?

Answer : If-Modified-Since: Wed, 08 Feb 2023 06:59:01 GMT\r\n

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

Answer : Capture Length: 627 bytes (5016 bits)

3.1 Exercise:

1. Start your web browser, and make sure your browsers cache is cleared.

2. Start the Wireshark tool.

Enter the following URL into your browser.
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2. html.
(Your browser should display a very simple five-line HTML file.)

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

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.

3.2 Questions - Answers:

Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an ”IF-MODIFIED-SINCE” line in the HTTP GET?

Answer : NO

2.Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer : : Yes

3. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an ”IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the ”IF-MODIFIED SINCE:” header?

Answer: : Yes. The information followed is: Wed, 08 Feb 2023 06:59:01 GMT\r\n which is the date of the last modification of the file from the previous get request.

4. 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.

Answer: The status code and phrase returned from the server is HTTP/1.1 304 Not Modified.

The server didn’t return the contents of the file since the browser loaded it from its cache.

4.1 Exercise:

1.Start up your web browser, and make sure your browsers cache is cleared, as discussed above.

2. Start up the Wireshark packet.

3. Enter the following URL into your browser.
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3. html
(Your browser should display the rather 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.

4.2 Questions - Answers:

1.How many HTTP GET request messages were sent by your browser?
Answer : HTTP GET request message sent by my browser

2.How many data-containing TCP segments were needed to carry the single HTTP response?
Answer :Reassembled TCP Segments (69882 bytes)

3. What is the status code and phrase associated with the response to the HTTP GET request?
Answer: 200 OK

5.1 Exercise:

1. Start up your web browser, and make sure your browsers cache is cleared, as discussed above.

2. Start up the Wireshark packet.

3. Enter the following URL into your browser.

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4. html
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. As discussed in the textbook, your browser will have to retrieve these logos from the indicated web sites.

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

5.2 Questions - Answers:

1. How many HTTP GET request messages were sent by your browser? To which Internet addresses were theseGET requests sent?

Answer:there were 2 HTTP GET requests sent to the following Internet addresses:
(a) 10.200.8.100
(b) 10.8.7.199

2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Answer: In this case the 2 images were transmitted over 2 TCP connections that means they were downloaded serially.

6.1 Exercise:

1. Make sure your browsers cache is cleared, as discussed above, and close down your browser. Then, start up your browser.

2. Start up the Wireshark packet.

3. Enter the following URL into your browser.
http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5html

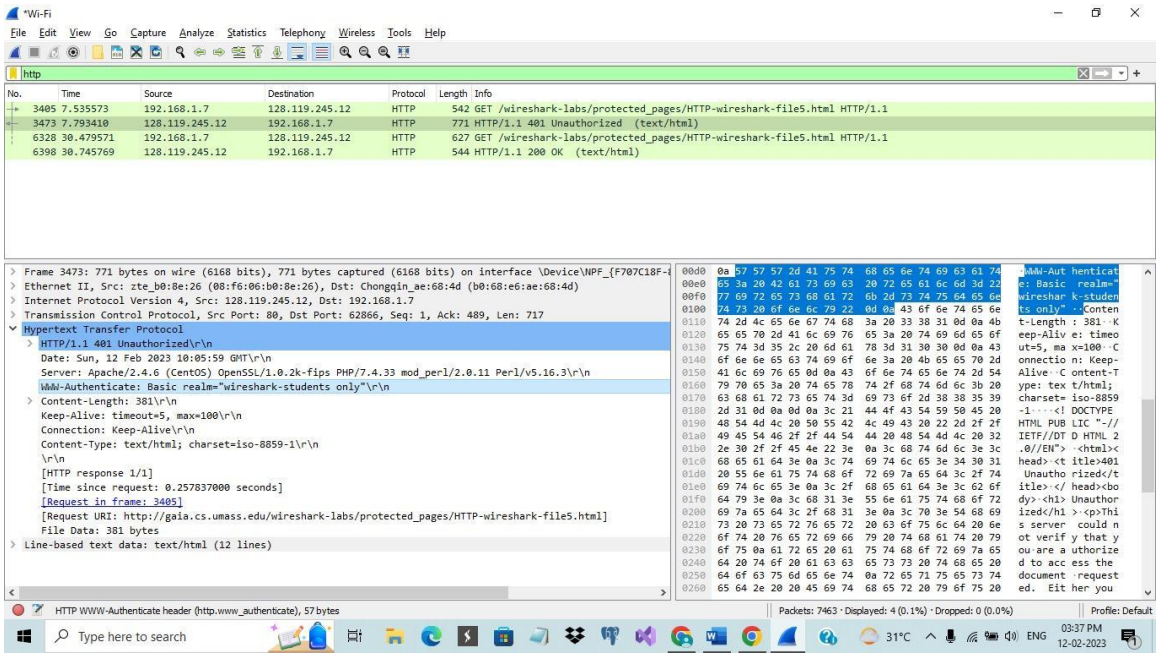
4. Type the requested user name and password into the pop up box.

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.

6.2 Questions - Answers:

1. What is the server response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer:



2. When your browsers send the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer:Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

202212083

2.1 Exercise:

1. Start your web browser.

Start the Wireshark tool, as described in the Introductory lab (but don't yet begin packet capture). 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 are only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).

2. Begin Wireshark packet capture.

3. Enter the following to your browser.
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1. Html

4. Stop Wireshark packet capture.

2.2 Questions - Answers:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer : 1.1

2.What languages (if any) does your browser indicate that it can accept to the server?

Answer : en-US,en;q=0.9\r\n

3. What is the IP address of your computer? and the gaia.cs.umass.edu server?

Answer: IPV 4, Src: 10.100.76.226, Dst: 128.119.245.12

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

Answer : 511

The HTTP 511 Network Authentication Required response status code **indicates that the client needs to authenticate to gain network access**

5. When was the HTML file that you are retrieving last modified at the Server?

Answer : If-Modified-Since: Wed, 08 Feb 2023 06:59:01 GMT\r\n

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

Answer : Capture Length: 627 bytes (5016 bits)

3.1 Exercise:

1. Start your web browser, and make sure your browsers cache is cleared.

2. Start the Wireshark tool.

Enter the following URL into your browser.
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2. html.
(Your browser should display a very simple five-line HTML file.)

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

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.

3.2 Questions - Answers:

Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an ”IF-MODIFIED-SINCE” line in the HTTP GET?

Answer : NO

2.Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer : : Yes

3. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an ”IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the ”IF-MODIFIED SINCE:” header?

Answer: : Yes. The information followed is: Wed, 08 Feb 2023 06:59:01 GMT\r\n which is the date of the last modification of the file from the previous get request.

4. 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.

Answer: The status code and phrase returned from the server is HTTP/1.1 304 Not Modified.

The server didn’t return the contents of the file since the browser loaded it from its cache.

4.1 Exercise:

1.Start up your web browser, and make sure your browsers cache is cleared, as discussed above.

2. Start up the Wireshark packet.

3. Enter the following URL into your browser.
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3. html
(Your browser should display the rather 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.

4.2 Questions - Answers:

1.How many HTTP GET request messages were sent by your browser?
Answer : HTTP GET request message sent by my browser

2.How many data-containing TCP segments were needed to carry the single HTTP response?
Answer :Reassembled TCP Segments (69882 bytes)

3. What is the status code and phrase associated with the response to the HTTP GET request?
Answer: 200 OK

5.1 Exercise:

1. Start up your web browser, and make sure your browsers cache is cleared, as discussed above.

2. Start up the Wireshark packet.

3. Enter the following URL into your browser.

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4. html
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. As discussed in the textbook, your browser will have to retrieve these logos from the indicated web sites.

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

5.2 Questions - Answers:

1. How many HTTP GET request messages were sent by your browser? To which Internet addresses were theseGET requests sent?

Answer:there were 2 HTTP GET requests sent to the following Internet addresses:
(a) 10.200.8.100
(b) 10.8.7.199

2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Answer: In this case the 2 images were transmitted over 2 TCP connections that means they were downloaded serially.

6.1 Exercise:

1. Make sure your browsers cache is cleared, as discussed above, and close down your browser. Then, start up your browser.

2. Start up the Wireshark packet.

3. Enter the following URL into your browser.
http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5html

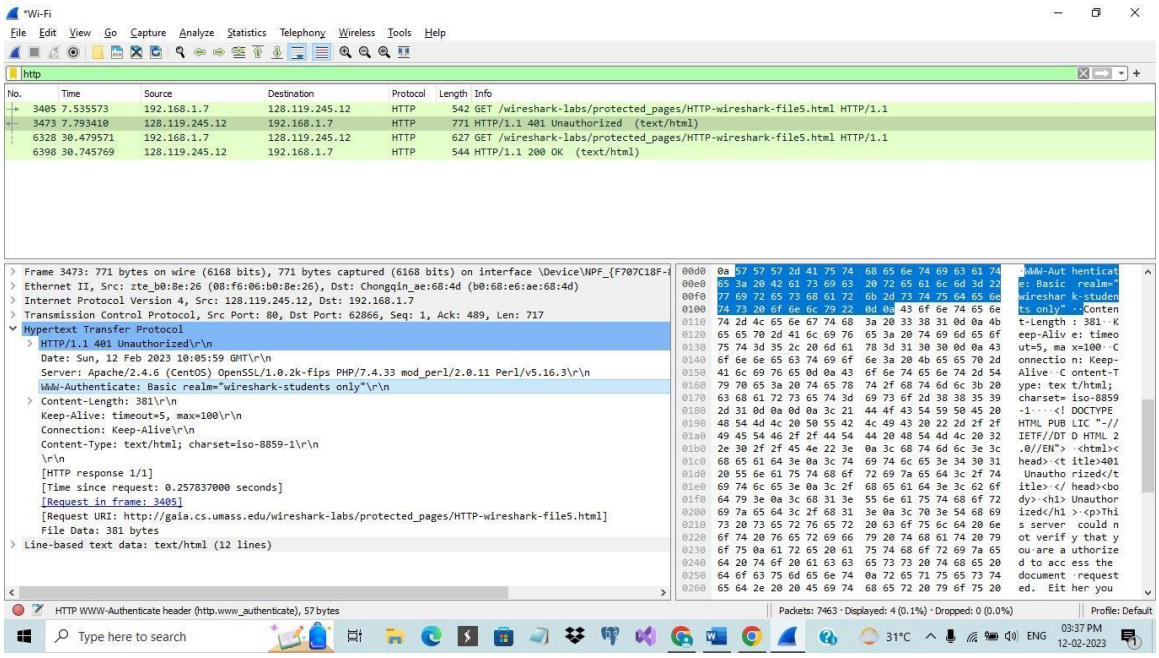
4. Type the requested user name and password into the pop up box.

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.

6.2 Questions - Answers:

1. What is the server response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer:



2. When your browsers send the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer:Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n