LAB EXERCISE - 3

Trace HTTP using Wireshark.

Objective:

To understand the working of Hyper Text Transfer Protocol

- The Basic HTTP GET/response interaction
- The HTTP CONDITIONAL GET/response interaction
- Retrieving Long Documents
- HTML Documents with Embedded Objects
- HTTP Authentication

Introduction

EXERCISE QUESTIONS:-

URL : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window.

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.)

3. What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer?

The Basic HTTP GET/response interaction

EXERCISE QUESTIONS :-

URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

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

2. What languages does your browser indicate that it can accept from the server?

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

4. When was the HTML file, that you are retrieving last modified at the server?

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

The HTTP CONDITIONAL GET/response interaction

EXERCISE QUESTIONS :-

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

1. 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?

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

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?

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.

Retrieving Long Documents

URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

EXERCISE QUESTIONS :-

1. How many HTTP GET request messages were sent by your browser?

2. How many data-containing TCP segments were needed to carry the single HTTP Response ?

3. What is the status code and phrase associated with the response to the HTTP GET Request ?

HTML Documents with Embedded Objects

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

EXERCISE QUESTIONS :

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

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

HTTP Authentication

EXERCISE QUESTIONS :

http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

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

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