Wireshark.

4. Trace packets using Wireshark for HTTP and Ans the following Questions.
The Basic HTTP{ GET/response interaction.
Use 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

Yes, brower running HTTP version 1.1

Request Version : HTTP/1.1

response version server : HTTP/1.1

(2) What language does your browser indicate that it can accept from the server

Accept-Language : en-US, en; q=0.5\r\n

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

Status Code : 204

(4) When was the HTML file, that you are retrieving last modified at the server

If-Modified-Since : Mon, 01 Apr 2024 05:59:02 GMT\r\n

(5) How many bytes of content are being returned to your browser

128 bytes of content are being returned

The HTTP CONDITIONAL GET/response interaction

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

6. 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?

No there is no IF-MODIFIED-SINCE line in GET msg

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

The server did explicitly return the contents of the file. Wireshark includes a section titled "Line-Based Text Data" which shows what the server sent back to my browser which is specifically what the website showed when I brought it up on my browser

8. 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 followed the "IF-MODIFIED-SINCE:" header?

Yes in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the data and time that I last accessed the webpage

9. What is the HTTP status code is '304 : Not and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

* The HTTP status code is "304 : Not Modified"

* The server did not return.

5. Trace packets Using Wireshark for HTTP and Answer the following Questions for Retrieving Long Documents use.

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

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

Solⁿ My browser sent 2 HTTP-Get request to the server. The packet the containind the Get message was packet number 16050, 16428

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

Solⁿ The data was sent in 2 TCP segments to the browser to carry the single HTTP Response & then resembled

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

Solⁿ The status code 200 with phrase OK.

4. Are there any HTTP status lines in the transmitted data associated with a TCP segment reassembled segmentes of a PDU?

Solⁿ

For HTML Documents with Embedded Objects use

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

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

Solⁿ My browser sent 2 HTTP-GET request messages one each to each for each of the following.

* Initial Page address:
* Pearson Logo:
* Pearson book, 5th Edition:

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

Solⁿ The browser downloaded the two images in serially. I belive this to be the case because the first image was requested and sent before the second image was requested by the browser. Had they been running in parallel, both files would have been reqdested then would have returned in the same time period. In this case however, the second image was only requested after the first image came back

For ~~A~~ HTTP Authentication use
Username : wireshark-students Password : "network"

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

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

Solⁿ The server initial response was

8. When does your browser send the HTTP GET message for the second time, what new field is included ~~ed~~ in the HTTP GET message?

Solⁿ The new field is now included is the authorization field. This is included because we sent the server a username and password along with our request stating that were authorized to receive the page.

3. Trace packet using wireshark for IP, ICMP and Answer the following Questions:

Use the following command to change the ICMP packet size.

```
Ping <ipaddress/url> -s <packetsize>
ex :- ping makemytrip.com . -S 2000
```

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet protocol part of the packet in the packet details window. What is the IP address of your computer?

Sol^n Source address :

2 Within the IP packet header, what is value in the upper layer protocol field

Protocol = ICMP (1), within the header, the value of upper layer protocol field is ICMP(1)

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes

Sol^n IP Header length = 20 bytes

Payload = Total length - IP Header length

= 84 - 20

= 64 bytes

∴ theyre are 20 bytes in IP header, & bytes total length, this gives bytes in the payload of the IP datagram.

4. Has this IP datagram been fragmented? Explain how you determined whether or not the data datagram has been fragmented.

Solⁿ The more fragments bit = 0, so the data is not fragmented.

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

Solⁿ Identification, Time to live and Header checksum always change.

6. Which fields stay constant?

Solⁿ The fields that stay constant across the IP datagram are:

* Version
* header length
* Source IP
* destination IP
* Differential Services
* Upper layer Protocol.

7. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size to be 2000. Has that message been fragmented across more than one IP datagram?

Solⁿ Yes, this packet has been fragmented across more than one IP datagram.

8 When does your browser send the HTTP GET message for the second time, what new field is included in the HTTP GET message?

8. Write the first fragment of the fragmented IP datagsam. What information in the IP header indicates that the datagram has been fragmented? What information in the IP header Indicates whether this is the first fragmented versus a latter fragment? How long is this IP datagram?

The flags bit for more fragmentes is set, indicating that the datagram has been fragmented. Since the fragmente offset is 0, we know that this is the first fragment. The first datagram has a total length of 1500, including the header.

9. What information in the IP header indicates that this is not the first datagsam fragment? Are there more fragments? How can you tell?

We can tell that this is not the first fragment, since the fricigment offset is 1480. It is the last fragment, since the more fragments flag is not set.

10. What fields change in the IP header between the first and second fragments?

The IP header fields that changed b/w the fragments are: total length, flags, fragment offset, and checksum.