William Fu

Wireshark Lab 2

2/15/18

1. Using HTTP 1.1. Server runs 1.1

2. Accept Language: en-US, en; 1=0.9\r\n

3. Source: 10.20.65.22 Destination: 128.119.245.12

4. 200 OK

5. Last-Modified: Thu, 15 Feb 2018 06:59:01 GMT\r\n

6. 128 Bytes

7. No I don’t see any in the http

8. Cannot find an IF-MODIFIED-SINCE line

9. I think? Within the Line-based text data: tells us what the server’s response is

Ex: Congratulations again! Now you’ve downloaded the file lab2-2.html. This file’s last modification date will not change. Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the In-MODIFIED-SINCE field in your bowser’s HTTP GET request to the server.

10. Yes. If-Modified-Since: Thu, 15 Feb 2018 06:59:01 GMT\r\n

11. 320 Not Modified

12. 1. Packet number with GET message for Bill of Rights: 8

13. 10 packets

14. 200 (OK)

15. 3 packets (10, 11, 13 in the trace)

16. there were three HTTP GET messages sent: packet 10 in the trace (to get the base file), packet 17 (to get the Pearson logo) and packet 20 (to get the 5th edition textbook cover)

Each of these three GET messages were sent to different IP addresses! Packet 10 was sent to 128.119.245.12, packet 17 to 165.193.123.218, and packet 20 to 134.241.6.82.

17. The downloads occurred in parallel. The two GET messages for the images are in packets 17 and 20. The images are in packets 25, and 54. Second image file (packet 20) was before packet 25, the first image file was received.

18. Packet 6 contains the first GET and packet 9 contains the REPLY. Server’s in packet 9 is: 401 Authorization Required

19. The HTTP GET includes the Authorization: Basic: field