Sniff HTTP traffic using Wireshark

## Network Applications and Design Homework Assignment #1

20172864 서정현

**[A]. The Basic HTTP GET/response interaction**

Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

A1. HTTP version 1.1.



텍스트이(가) 표시된 사진

자동 생성된 설명

Q2. What is the IP address of your computer? Of the web server?

A2. My computer address(source address) is 192.168.0.102, web server address(destination address) is 128.119.245.12.

텍스트이(가) 표시된 사진

자동 생성된 설명

Q3. What is the status code returned from the server to your browser?

A3. 200, it means “OK”.

텍스트이(가) 표시된 사진

자동 생성된 설명

Q4. When was the HTML file that you are retrieving last modified at the server?

A4. Sun, 27 Mar 2022 05:59:02 GMT.

텍스트이(가) 표시된 사진

자동 생성된 설명

Q5. How many bytes of content are being returned to your browser?

A5. 128 bytes.

텍스트이(가) 표시된 사진

자동 생성된 설명

**[B]. The HTTP CONDITIONAL GET/response interaction**

Q6. 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?

A6. No.

텍스트이(가) 표시된 사진

자동 생성된 설명

Q7. Inspect the contents of the server response. Did the server explicitly return the contents of the file?

A7. Yes, I can find out it in the first response packet, but not in the second response packet.

텍스트이(가) 표시된 사진

자동 생성된 설명

Q8. 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?

A8. Yes, I can see it. The second request packet contains “Last-Modified” information (A4, Sun, 27 Mar 2022 05:59:02 GMT) received in the first response packet as “If-Modified-Since”. This information is used when the server decides whether to retransmit the contents.

텍스트이(가) 표시된 사진

자동 생성된 설명

Q9. 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.

A9. The status code is 304, it means “Not Modified”. The server don’t return the contents. Since the "If-Modified-Since" value of the request packet is the same as the last modified time of the file, there is no reason to retransmit the contents.

텍스트이(가) 표시된 사진

자동 생성된 설명

**[C]. Retrieving Long Documents**

Q10. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the ‘Bill of Rights’?

A10. Once, the packet number is 53.

텍스트이(가) 표시된 사진

자동 생성된 설명

Q11. What is the status code and phrase in the response?

A11. 200, it means “OK”.

텍스트이(가) 표시된 사진

자동 생성된 설명

Q12. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

A12. I checked [4 Reassembled TCP Segments ...], but when I searched for ‘tcp’ with filter, there were actually 3 data-containing packets.

텍스트이(가) 표시된 사진

자동 생성된 설명

테이블이(가) 표시된 사진

자동 생성된 설명

**[D]. HTML Documents with Embedded Objects**

Q13. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

A13. Eight.

테이블이(가) 표시된 사진

자동 생성된 설명

Q14. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel?

A14. Images are downloaded serially. If you look at the time the packets returned with images (JPEG or PNG) was captured, you can see that new requests are sequentially sent when a response arrives.

