Network

(Lab Assignment 1)

Wireshark

컴퓨터소프트웨어 학부
2018008559
신상윤

1. The Basic HTTP GET/response interaction

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.8
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applic
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  [HTTP request 1/1]
  [Response in frame: 985]
```

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sat, 25 Sep 2021 09:59:23 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Sat, 25 Sep 2021 05:59:01 GMT\r\n
  ETag: "80-5cccb8f83fbea"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 128\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.222354000 seconds]
  [Request in frame: 981]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

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

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

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

```
981 19.674616       192.168.0.27          128.119.245.12        HTTP        550 GET /wireshark-labs/HTTP-wireshark-file1.
```

나 : 192.168.0.27 서버 : 128.119.245.12

4. What is the status code returned from the server to your browser? 200

```
985 19.896970       128.119.245.12        192.168.0.27          HTTP        540 HTTP/1.1 200 OK  (text/html)
```

5. When was the HTML file that you are retrieving last modified at the server? Sat, 25 Sep 2021 05:59:01 GMT

6. How many bytes of content are being returned to your browser? 128(bytes)

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one. 없다. 모든 header는 raw data 에서 찾을 수 있다.

2. The HTTP CONDITIONAL GET/response interaction

8. 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? 아니오

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/2]
  [Response in frame: 74]
  [Next request in frame: 90]
```

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

```
Line-based text data: text/html (10 lines)
  \n
  <html>\n
  \n
  Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
  This file's last modification date will not change.  <p>\n
  Thus  if you download this multiple times on your browser, a complete copy <br>\n
  will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
  </html>\n
```

"Line-Based Text Data" 항목을 확인하면 파일의 정보를 명확하게 return 했다는 것을 확인할 수 있다.

10. 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?

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  If-None-Match: "173-5cccb8f83f41a"\r\n
  If-Modified-Since: Sat, 25 Sep 2021 05:59:01 GMT\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 2/2]
  [Prev request in frame: 71]
  [Response in frame: 91]
```

예, "IF-MODIFIED-SINCE:" 항목이 보인다. 마지막으로 수정한 날짜, 시간의 정보를 포함한다.

11. 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.

```
91 -5.005052    128.119.245.12    192.168.0.27    HTTP    293 HTTP/1.1 304 Not Modified
```

코드는 "304: Not Modified" 이다. 이미 불러왔던 정보가 컴퓨터 안에 있어 다시 return 하지 않았다.

3. Retrieving Long Documents

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

```
214 12.488758    192.168.0.27    128.119.245.12    HTTP    550 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
```

13. How many data-containing TCP segments were needed to carry the single HTTP response? 4

```
Transmission Control Protocol, Src Port: 80, Dst Port: 56136, Seq: 4381, Ack: 497, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #232(1460), #233(1460), #234(1460), #235(481)]
Hypertext Transfer Protocol
Line-based text data: text/html (98 lines)
```

14. What is the status code and phrase associated with the response to the HTTP GET request?

```
535 HTTP/1.1 200 OK  (text/html)
```

"200 OK"

15. Are there any HTTP status lines in the transmitted data associated with a TCP-induced "Continuation" ? 없다.

4. HTML Documents with Embedded Objects

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

```
192.168.0.27        128.119.245.12      HTTP     550 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
192.168.0.27        211.115.106.209     HTTP     427 GET /jk?c=62&p=MSypsc4_M5EJAYGcIWwrDOn951tTxhTNbl4q+pYz5_c=&k=1 HTTP/1.1
211.115.106.209     192.168.0.27        HTTP     405 HTTP/1.1 200 OK
128.119.245.12      192.168.0.27        HTTP    1355 HTTP/1.1 200 OK  (text/html)
192.168.0.27        128.119.245.12      HTTP     496 GET /pearson.png HTTP/1.1
128.119.245.12      192.168.0.27        HTTP     745 HTTP/1.1 200 OK  (PNG)
192.168.0.27        211.115.106.209     HTTP     427 GET /jk?d=62&p=MSypsc4_M5EJAYGcIWwrDOn951tTxhTNbl4q+pYz5_c=&k=1 HTTP/1.1
211.115.106.209     192.168.0.27        HTTP     405 HTTP/1.1 200 OK
192.168.0.27        178.79.137.164      HTTP     463 GET /8E_cover_small.jpg HTTP/1.1
178.79.137.164      192.168.0.27        HTTP     225 HTTP/1.1 301 Moved Permanently
```

3가지 요청 메시지가 있다.
GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
GET /pearson.png HTTP/1.1
GET /8E_cover_small.jpg HTTP/1.1
각각
128.119.245.12 , 128.119.245.12 , 178.79.137.164 에서 요청됐다.

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

이미지를 직렬로(순차적으로) 다운로드했다. 병렬로 다운로드했으면 두 파일이 동시에 요청되어 주소가 같았을 것이다.

5. HTTP Authentication

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

```
565 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
427 GET /jk?c=62&p=MSypsc4_M5EJAYGcIWwrDOn951tTxhTNbl4q+pYz5_c=&k=1 HTTP/1.1
405 HTTP/1.1 200 OK
771 HTTP/1.1 401 Unauthorized  (text/html)
650 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
583 HTTP/1.1 404 Not Found  (text/html)
```

"401 Unauthorized"

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

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
  [HTTP request 1/1]
  [Response in frame: 242]
```

새롭게 "Authorization" 항목이 추가되었다.