

## HTTP 분석

미디어학과 201821048 이서영

### 1. 관찰 환경 및 방법

장소 : 집에서 와이파이를 이용해 인터넷에 연결했다.

시간 : 사이트에서 F5 를 눌러 약 10 초 이내의 패킷을 캡처했다.

사용한 기능 : 와이어샤크에서 http 패킷만을 분석하기 위해 필터링 기능을 사용했다.

실습 방법 :

1. 새로운 창을 열었다.
2. http 로 된 사이트를 찾았다.
3. 와이어샤크의 캡처 기능을 사용했다.
4. 웹사이트를 새로고침 해 원하는 패킷(HTTP)을 기록했다.
5. 와이어샤크 캡처기능을 멈추고 저장했다.
5. http 만을 분석하기 위해 필터에 http 를 입력해 해당 내용만을 정렬했다.
6. 각 패킷의 세부내용을 펼쳐 관찰했다.

### 2. Protocol 분석

#### 1) HTTP request 와 response message 의 header 분석

Request Header : 요청하는 페이지의 주소와 현재 컴퓨터의 정보가 전송된다.

Request Body : POST 요청 시 전송되는 데이터가 들어간다. GET 요청 때는 빈칸이다.

Response Header : 응답 페이지의 상태와 서버에 관한 정보가 전송된다.

Response Body : 페이지의 HTML 소스가 전송된다.

첫번째로 교환한 HTTP Request Header 의 자세한 내용이다.

No.	Time	Source	Destination	Protocol	Length	Info
76	4.916344	192.168.0.10	182.162.110.129	HTTP	823	GET / HTTP/1.1
160	5.108082	182.162.110.129	192.168.0.10	HTTP	500	HTTP/1.1 200 OK (text/html)
166	5.236273	192.168.0.10	118.219.56.66	HTTP	704	GET /upload/2018/07/06/data/i14438289016.jpg HTTP/1.1
167	5.242218	192.168.0.10	118.219.56.66	HTTP	630	GET /upload/2020/04/23/bbs/thumb/s15740355186.png HTTP/1.1
168	5.252884	118.219.56.66	192.168.0.10	HTTP	376	HTTP/1.1 304 Not Modified
186	5.275278	118.219.56.66	192.168.0.10	HTTP	227	HTTP/1.1 200 OK (JPEG JFIF image)
195	5.302643	192.168.0.10	118.219.56.66	HTTP	624	GET /upload/2018/12/10/bbs/i14501612898.jpg HTTP/1.1
239	5.324079	118.219.56.66	192.168.0.10	HTTP	996	HTTP/1.1 200 OK (JPEG JFIF image)
250	5.343239	192.168.0.10	117.52.90.29	HTTP	1039	GET /imp?slot=1318&type=if HTTP/1.1
278	5.366450	117.52.90.29	192.168.0.10	HTTP	719	HTTP/1.1 200 OK
287	5.470847	192.168.0.10	110.10.122.38	HTTP	675	GET /ad/ad_script/content_id02.js HTTP/1.1

> Frame 76: 823 bytes on wire (6584 bits), 823 bytes captured (6584 bits) on interface \Device\NPF\_{357E97B7-B0A5-4B3F-9F0C-7ACF01DC2B70}, id  
 > Ethernet II, Src: AzureWav\_98:e7:51 (dc:f5:05:98:e7:51), Dst: EFMNetwo\_1c:b5:d8 (70:5d:cc:1c:b5:d8)  
 > Internet Protocol Version 4, Src: 192.168.0.10, Dst: 182.162.110.129  
 > Transmission Control Protocol, Src Port: 56237, Dst Port: 80, Seq: 1, Ack: 1, Len: 769

> Hypertext Transfer Protocol  
 > GET / HTTP/1.1\r\n  
 Host: maple.inven.co.kr\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 Gecko) Chrome/81.0.4044.122 Safari/537.36\r\n  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n  
 Referer: https://www.google.com/\r\n  
 Accept-Encoding: gzip, deflate\r\n  
 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,de;q=0.6,pt;q=0.5\r\n  
 > [truncated]Cookie: MOBILE\_V3=NONE; \_ga=GA1.3.1613538263.1583876656; OAX=dxFLx16es+oADE9S; \_ga=GA1.4.1613538263.1583876656; a1\_gid=dxFLx1\r\n  
 [Full request URI: http://maple.inven.co.kr/]  
 [HTTP request 1/1]  
 [Response in frame: 160]

1. GET : 명령어로 페이지를 가져오려고 한다. http 1.1 버전이다.
2. HOST : 도메인은 maple.inven.co.kr 이다.
3. Connection : Keep-alive 로 서버에서 정한 시간만큼 연결을 유지한다.
4. Cache-Control : 서버측에 대한 캐시 컨트롤 요청이다.
5. User-Agent : 브라우저, 운영체제에 대한 정보가 들어있다.
6. Accept : 현재 브라우저가 요청하는 파일의 mime type 이 기록된다.
7. Referer : HTTP 요청을 시도한 페이지의 URL 이다. 어떤 페이지를 통해 현재 페이지로 들어왔는지 정보를 제공한다.
8. Accept-Encoding : 브라우저가 받아들일 수 있는 압축 알고리즘이 전송된다.
9. Accept-Language : 사용자가 이해할 수 있는 자연어의 종류가 전송된다.
10. Cookie : 쿠키 값이 전송된다.
11. 요청 URL 은 서버에서 파일의 위치이다.

Response Header 의 자세한 내용이다.

No.	Time	Source	Destination	Protocol	Length	Info
76	4.916344	192.168.0.10	182.162.110.129	HTTP	823	GET / HTTP/1.1
160	5.108082	182.162.110.129	192.168.0.10	HTTP	500	HTTP/1.1 200 OK (text/html)
166	5.236273	192.168.0.10	118.219.56.66	HTTP	704	GET /upload/2018/07/06/data/i14438289016.jpg HTTP/1.1
167	5.242218	192.168.0.10	118.219.56.66	HTTP	630	GET /upload/2020/04/23/bbs/thumb/s15740355186.png HTTP/1.1
168	5.252884	118.219.56.66	192.168.0.10	HTTP	376	HTTP/1.1 304 Not Modified
186	5.275278	118.219.56.66	192.168.0.10	HTTP	227	HTTP/1.1 200 OK (JPEG JFIF image)
195	5.302643	192.168.0.10	118.219.56.66	HTTP	624	GET /upload/2018/12/10/bbs/i14501612898.jpg HTTP/1.1
239	5.324079	118.219.56.66	192.168.0.10	HTTP	996	HTTP/1.1 200 OK (JPEG JFIF image)
250	5.343239	192.168.0.10	117.52.90.29	HTTP	1039	GET /imp?slot=1318&type=if HTTP/1.1
278	5.366450	117.52.90.29	192.168.0.10	HTTP	719	HTTP/1.1 200 OK
287	5.470847	192.168.0.10	110.10.122.38	HTTP	675	GET /ad/ad_script/content_id02.js HTTP/1.1
301	5.477300	192.168.0.10	117.52.90.29	HTTP	1039	GET /imp?slot=1318&type=if HTTP/1.1

```

> Frame 160: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits) on interface \Device\NPF_{357E97B7-B0A5-4B3F-9F0C-7ACF01DC2B70}, ic
> Ethernet II, Src: EFMNetwo_1c:b5:d8 (70:5d:cc:1c:b5:d8), Dst: AzureWav_98:e7:51 (dc:f5:05:98:e7:51)
> Internet Protocol Version 4, Src: 182.162.110.129, Dst: 192.168.0.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 56237, Seq: 57295, Ack: 770, Len: 446
> [41 Reassembled TCP Segments (57740 bytes): #107(354), #108(1460), #109(1460), #111(1460), #112(1460), #114(1460), #115(1460), #117(1460), #
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Server: nginx\r\n
    Date: Thu, 23 Apr 2020 08:46:40 GMT\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    Cache-Control: no-cache, must-revalidate\r\n
    Set-Cookie: VISIT_SITE=maple%7Cwebzine; expires=Sat, 23-May-2020 08:46:39 GMT; Max-Age=2592000; path=/; domain=.inven.co.kr\r\n
    Content-Encoding: gzip\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.191738000 seconds]
    [Request in frame: 76]
    [Request URI: http://maple.inven.co.kr/]
  > HTTP chunked response

```

1. 200 OK : 정상적으로 응답이 처리되었다.
2. Server : 응답을 담당하는 웹 서버의 종류를 나타낸다.
3. Data : 웹 서버의 현재 시간을 나타낸다.
4. Content-Type : 응답의 mime-type 을 나타낸다.
5. Connection : 소켓 연결을 유지할지 결정한다.
6. Cache-Control : 브라우저 쪽의 캐싱 여부를 결정한다.
7. Set-Cookie : 사용자의 브라우저에 쿠키값을 설정한다.

## 2) Persistent connection

Pipelining : 여러 세션을 연결한 후 여러 개의 request 를 받아온다.

166	5.236273	192.168.0.10	118.219.56.66	HTTP	704	GET /upload/2018/07/06/data/i14438289016.jpg HTTP/1.1
167	5.242218	192.168.0.10	118.219.56.66	HTTP	630	GET /upload/2020/04/23/bbs/thumb/s15740355186.png HTTP/1.1
168	5.252884	118.219.56.66	192.168.0.10	HTTP	376	HTTP/1.1 304 Not Modified
186	5.275278	118.219.56.66	192.168.0.10	HTTP	227	HTTP/1.1 200 OK (JPEG JFIF image)
195	5.302643	192.168.0.10	118.219.56.66	HTTP	624	GET /upload/2018/12/10/bbs/i14501612898.jpg HTTP/1.1
239	5.324079	118.219.56.66	192.168.0.10	HTTP	996	HTTP/1.1 200 OK (JPEG JFIF image)

HTTP Connctcion 은 Short-lived connection, Persistent connection, Pipelining 3 가지 종류가 있다.

( : establish connection

) : close connection

->, -< : 패킷 전송

Short-lived connection : (-> <-)(-> <-)(-> <-)

Persistent connection : -> <--> <--> <--

Pipelining : ->->->-<-<-<-

직관적으로 보이듯이 파이프라인 방식을 사용하면 같은 양의 정보를 전달할 때 훨씬 빠르게 전달할 수 있다.

### 3) Redirection 사례

필터에 `http.response.code > 299 && http.response.code < 400` 을 적용해 redirection 과 관련된 내용을 검색해 보았다. 하지만 304 만 나와 관찰할 수 없었다.

304 Not Modified : URL 이 변경되지 않는 모습을 보였다.

http.response.code > 299 && http.response.code < 400						
No.	Time	Source	Destination	Protocol	Length	Info
168	5.252884	118.219.56.66	192.168.0.10	HTTP	376	HTTP/1.1 304 Not Modified
293	5.488518	110.10.122.38	192.168.0.10	HTTP	321	HTTP/1.1 304 Not Modified
303	5.545274	110.10.122.38	192.168.0.10	HTTP	321	HTTP/1.1 304 Not Modified
306	5.598770	110.10.122.38	192.168.0.10	HTTP	321	HTTP/1.1 304 Not Modified
309	5.632831	110.10.122.38	192.168.0.10	HTTP	320	HTTP/1.1 304 Not Modified
379	5.816895	110.10.122.38	192.168.0.10	HTTP	321	HTTP/1.1 304 Not Modified
388	5.845450	110.10.122.38	192.168.0.10	HTTP	321	HTTP/1.1 304 Not Modified
399	5.863381	110.10.122.38	192.168.0.10	HTTP	321	HTTP/1.1 304 Not Modified
473	5.901853	139.150.252.192	192.168.0.10	HTTP	300	HTTP/1.1 304 Not Modified

> Frame 388: 321 bytes on wire (2568 bits), 321 bytes captured (2568 bits) on interface \Device\NPF\_{357E...}

> Ethernet II, Src: EFMNetwo\_1c:b5:d8 (70:5d:cc:1c:b5:d8), Dst: AzureWav\_98:e7:51 (dc:f5:05:98:e7:51)

> Internet Protocol Version 4, Src: 110.10.122.38, Dst: 192.168.0.10

> Transmission Control Protocol, Src Port: 80, Dst Port: 56225, Seq: 1335, Ack: 3832, Len: 267

▼ Hypertext Transfer Protocol

> HTTP/1.1 304 Not Modified\r\n

Via: STON Edge Server/2.6.5\r\n

Date: Thu, 23 Apr 2020 08:46:39 GMT\r\n

> Content-Length: 0\r\n

ETag: "5e8fe6c5-12ad"\r\n

Age: 1091883\r\n

Server: nginx/1.10.3\r\n

Connection: Keep-Alive\r\n

Keep-Alive: timeout=30\r\n

Access-Control-Allow-Origin: \*\r\n

X-SVSZone: S\r\n

\r\n

3xx 은 Redirection 코드이다. 각 코드가 나타내는 내용은 다음과 같다.

300 Multiple Choices [RFC7231, Section 6.4.1]

301 Moved Permanently [RFC7231, Section 6.4.2]

302 Found [RFC7231, Section 6.4.3]

303 See Other [RFC7231, Section 6.4.4]

304 Not Modified [RFC7232, Section 4.1]

305 Use Proxy [RFC7231, Section 6.4.5]

306 (Unused) [RFC7231, Section 6.4.6]

307 Temporary Redirect [RFC7231, Section 6.4.7]

## 308 Permanent Redirect [RFC7538]

### 4) Web caching 기능

No.	Time	Source	Destination	Protocol	Length	Info
76	4.916344	192.168.0.10	182.162.110.129	HTTP	823	GET / HTTP/1.1
160	5.108082	182.162.110.129	192.168.0.10	HTTP	500	HTTP/1.1 200 OK (text/html)
166	5.236273	192.168.0.10	118.219.56.66	HTTP	704	GET /upload/2018/07/06/data/i1
167	5.242218	192.168.0.10	118.219.56.66	HTTP	630	GET /upload/2020/04/23/bbs/thu
168	5.252884	118.219.56.66	192.168.0.10	HTTP	376	HTTP/1.1 304 Not Modified
186	5.275278	118.219.56.66	192.168.0.10	HTTP	227	HTTP/1.1 200 OK (JPEG JFIF in
195	5.302643	192.168.0.10	118.219.56.66	HTTP	624	GET /upload/2018/12/10/bbs/i14
239	5.324079	118.219.56.66	192.168.0.10	HTTP	996	HTTP/1.1 200 OK (JPEG JFIF in

> Transmission Control Protocol, Src Port: 56237, Dst Port: 80, Seq: 1, Ack: 1, Len: 769

▼ Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n  
Host: maple.inven.co.kr\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 Gecko) Chrome/81.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application  
Referer: https://www.google.com/\r\n

<

0070 61 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 6f 6e alive..C ache-Con  
0080 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d trol: ma x-age=0  
0090 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 .Upgrade -Insecur  
00a0 65 2d 53 65 74 75 65 73 74 73 3a 20 0d 0a 55 s Request: text/html

1. Max-age : 캐시의 유효시간을 나타낸다.

No.	Time	Source	Destination	Protocol	Length	Info
76	4.916344	192.168.0.10	182.162.110.129	HTTP	823	GET / HTTP/1.1
160	5.108082	182.162.110.129	192.168.0.10	HTTP	500	HTTP/1.1 200 OK (text/html)
166	5.236273	192.168.0.10	118.219.56.66	HTTP	704	GET /upload/2018/07/06/data/i1443
167	5.242218	192.168.0.10	118.219.56.66	HTTP	630	GET /upload/2020/04/23/bbs/thumb/
168	5.252884	118.219.56.66	192.168.0.10	HTTP	376	HTTP/1.1 304 Not Modified
186	5.275278	118.219.56.66	192.168.0.10	HTTP	227	HTTP/1.1 200 OK (JPEG JFIF image
195	5.302643	192.168.0.10	118.219.56.66	HTTP	624	GET /upload/2018/12/10/bbs/i14501
239	5.324079	118.219.56.66	192.168.0.10	HTTP	996	HTTP/1.1 200 OK (JPEG JFIF image

> Transmission Control Protocol, Src Port: 80, Dst Port: 56237, Seq: 57295, Ack: 770, Len: 446

> [41 Reassembled TCP Segments (57740 bytes): #107(354), #108(1460), #109(1460), #111(1460), #112(1460), #114(1460), #115(1460), #116(1460), #117(1460), #118(1460), #119(1460), #120(1460), #121(1460), #122(1460), #123(1460), #124(1460), #125(1460), #126(1460), #127(1460), #128(1460), #129(1460), #130(1460), #131(1460), #132(1460), #133(1460), #134(1460), #135(1460), #136(1460), #137(1460), #138(1460), #139(1460), #140(1460), #141(1460), #142(1460), #143(1460), #144(1460), #145(1460), #146(1460), #147(1460), #148(1460), #149(1460), #150(1460), #151(1460), #152(1460), #153(1460), #154(1460), #155(1460), #156(1460), #157(1460), #158(1460), #159(1460), #160(1460), #161(1460), #162(1460), #163(1460), #164(1460), #165(1460), #166(1460), #167(1460), #168(1460), #169(1460), #170(1460), #171(1460), #172(1460), #173(1460), #174(1460), #175(1460), #176(1460), #177(1460), #178(1460), #179(1460), #180(1460), #181(1460), #182(1460), #183(1460), #184(1460), #185(1460), #186(1460), #187(1460), #188(1460), #189(1460), #190(1460), #191(1460), #192(1460), #193(1460), #194(1460), #195(1460), #196(1460), #197(1460), #198(1460), #199(1460), #200(1460), #201(1460), #202(1460), #203(1460), #204(1460), #205(1460), #206(1460), #207(1460), #208(1460), #209(1460), #210(1460), #211(1460), #212(1460), #213(1460), #214(1460), #215(1460), #216(1460), #217(1460), #218(1460), #219(1460), #220(1460), #221(1460), #222(1460), #223(1460), #224(1460), #225(1460), #226(1460), #227(1460), #228(1460), #229(1460), #230(1460), #231(1460), #232(1460), #233(1460), #234(1460), #235(1460), #236(1460), #237(1460), #238(1460), #239(1460), #240(1460), #241(1460), #242(1460), #243(1460), #244(1460), #245(1460), #246(1460), #247(1460), #248(1460), #249(1460), #250(1460), #251(1460), #252(1460), #253(1460), #254(1460), #255(1460), #256(1460), #257(1460), #258(1460), #259(1460), #260(1460), #261(1460), #262(1460), #263(1460), #264(1460), #265(1460), #266(1460), #267(1460), #268(1460), #269(1460), #270(1460), #271(1460), #272(1460), #273(1460), #274(1460), #275(1460), #276(1460), #277(1460), #278(1460), #279(1460), #280(1460), #281(1460), #282(1460), #283(1460), #284(1460), #285(1460), #286(1460), #287(1460), #288(1460), #289(1460), #290(1460), #291(1460), #292(1460), #293(1460), #294(1460), #295(1460), #296(1460), #297(1460), #298(1460), #299(1460), #300(1460), #301(1460), #302(1460), #303(1460), #304(1460), #305(1460), #306(1460), #307(1460), #308(1460), #309(1460), #310(1460), #311(1460), #312(1460), #313(1460), #314(1460), #315(1460), #316(1460), #317(1460), #318(1460), #319(1460), #320(1460), #321(1460), #322(1460), #323(1460), #324(1460), #325(1460), #326(1460), #327(1460), #328(1460), #329(1460), #330(1460), #331(1460), #332(1460), #333(1460), #334(1460), #335(1460), #336(1460), #337(1460), #338(1460), #339(1460), #340(1460), #341(1460), #342(1460), #343(1460), #344(1460), #345(1460), #346(1460), #347(1460), #348(1460), #349(1460), #350(1460), #351(1460), #352(1460), #353(1460), #354(1460), #355(1460), #356(1460), #357(1460), #358(1460), #359(1460), #360(1460), #361(1460), #362(1460), #363(1460), #364(1460), #365(1460), #366(1460), #367(1460), #368(1460), #369(1460), #370(1460), #371(1460), #372(1460), #373(1460), #374(1460), #375(1460), #376(1460), #377(1460), #378(1460), #379(1460), #380(1460), #381(1460), #382(1460), #383(1460), #384(1460), #385(1460), #386(1460), #387(1460), #388(1460), #389(1460), #390(1460), #391(1460), #392(1460), #393(1460), #394(1460), #395(1460), #396(1460), #397(1460), #398(1460), #399(1460), #400(1460), #401(1460), #402(1460), #403(1460), #404(1460), #405(1460), #406(1460), #407(1460), #408(1460), #409(1460), #410(1460), #411(1460), #412(1460), #413(1460), #414(1460), #415(1460), #416(1460), #417(1460), #418(1460), #419(1460), #420(1460), #421(1460), #422(1460), #423(1460), #424(1460), #425(1460), #426(1460), #427(1460), #428(1460), #429(1460), #430(1460), #431(1460), #432(1460), #433(1460), #434(1460), #435(1460), #436(1460), #437(1460), #438(1460), #439(1460), #440(1460), #441(1460), #442(1460), #443(1460), #444(1460), #445(1460), #446(1460), #447(1460), #448(1460), #449(1460), #450(1460), #451(1460), #452(1460), #453(1460), #454(1460), #455(1460), #456(1460), #457(1460), #458(1460), #459(1460), #460(1460), #461(1460), #462(1460), #463(1460), #464(1460), #465(1460), #466(1460), #467(1460), #468(1460), #469(1460), #470(1460), #471(1460), #472(1460), #473(1460), #474(1460), #475(1460), #476(1460), #477(1460), #478(1460), #479(1460), #480(1460), #481(1460), #482(1460), #483(1460), #484(1460), #485(1460), #486(1460), #487(1460), #488(1460), #489(1460), #490(1460), #491(1460), #492(1460), #493(1460), #494(1460), #495(1460), #496(1460), #497(1460), #498(1460), #499(1460), #500(1460), #501(1460), #502(1460), #503(1460), #504(1460), #505(1460), #506(1460), #507(1460), #508(1460), #509(1460), #510(1460), #511(1460), #512(1460), #513(1460), #514(1460), #515(1460), #516(1460), #517(1460), #518(1460), #519(1460), #520(1460), #521(1460), #522(1460), #523(1460), #524(1460), #525(1460), #526(1460), #527(1460), #528(1460), #529(1460), #530(1460), #531(1460), #532(1460), #533(1460), #534(1460), #535(1460), #536(1460), #537(1460), #538(1460), #539(1460), #540(1460), #541(1460), #542(1460), #543(1460), #544(1460), #545(1460), #546(1460), #547(1460), #548(1460), #549(1460), #550(1460), #551(1460), #552(1460), #553(1460), #554(1460), #555(1460), #556(1460), #557(1460), #558(1460), #559(1460), #560(1460), #561(1460), #562(1460), #563(1460), #564(1460), #565(1460), #566(1460), #567(1460), #568(1460), #569(1460), #570(1460), #571(1460), #572(1460), #573(1460), #574(1460), #575(1460), #576(1460), #577(1460), #578(1460), #579(1460), #580(1460), #581(1460), #582(1460), #583(1460), #584(1460), #585(1460), #586(1460), #587(1460), #588(1460), #589(1460), #590(1460), #591(1460), #592(1460), #593(1460), #594(1460), #595(1460), #596(1460), #597(1460), #598(1460), #599(1460), #600(1460), #601(1460), #602(1460), #603(1460), #604(1460), #605(1460), #606(1460), #607(1460), #608(1460), #609(1460), #610(1460), #611(1460), #612(1460), #613(1460), #614(1460), #615(1460), #616(1460), #617(1460), #618(1460), #619(1460), #620(1460), #621(1460), #622(1460), #623(1460), #624(1460), #625(1460), #626(1460), #627(1460), #628(1460), #629(1460), #630(1460), #631(1460), #632(1460), #633(1460), #634(1460), #635(1460), #636(1460), #637(1460), #638(1460), #639(1460), #640(1460), #641(1460), #642(1460), #643(1460), #644(1460), #645(1460), #646(1460), #647(1460), #648(1460), #649(1460), #650(1460), #651(1460), #652(1460), #653(1460), #654(1460), #655(1460), #656(1460), #657(1460), #658(1460), #659(1460), #660(1460), #661(1460), #662(1460), #663(1460), #664(1460), #665(1460), #666(1460), #667(1460), #668(1460), #669(1460), #670(1460), #671(1460), #672(1460), #673(1460), #674(1460), #675(1460), #676(1460), #677(1460), #678(1460), #679(1460), #680(1460), #681(1460), #682(1460), #683(1460), #684(1460), #685(1460), #686(1460), #687(1460), #688(1460), #689(1460), #690(1460), #691(1460), #692(1460), #693(1460), #694(1460), #695(1460), #696(1460), #697(1460), #698(1460), #699(1460), #700(1460), #701(1460), #702(1460), #703(1460), #704(1460), #705(1460), #706(1460), #707(1460), #708(1460), #709(1460), #710(1460), #711(1460), #712(1460), #713(1460), #714(1460), #715(1460), #716(1460), #717(1460), #718(1460), #719(1460), #720(1460), #721(1460), #722(1460), #723(1460), #724(1460), #725(1460), #726(1460), #727(1460), #728(1460), #729(1460), #730(1460), #731(1460), #732(1460), #733(1460), #734(1460), #735(1460), #736(1460), #737(1460), #738(1460), #739(1460), #740(1460), #741(1460), #742(1460), #743(1460), #744(1460), #745(1460), #746(1460), #747(1460), #748(1460), #749(1460), #750(1460), #751(1460), #752(1460), #753(1460), #754(1460), #755(1460), #756(1460), #757(1460), #758(1460), #759(1460), #760(1460), #761(1460), #762(1460), #763(1460), #764(1460), #765(1460), #766(1460), #767(1460), #768(1460), #769(1460), #770(1460), #771(1460), #772(1460), #773(1460), #774(1460), #775(1460), #776(1460), #777(1460), #778(1460), #779(1460), #780(1460), #781(1460), #782(1460), #783(1460), #784(1460), #785(1460), #786(1460), #787(1460), #788(1460), #789(1460), #790(1460), #791(1460), #792(1460), #793(1460), #794(1460), #795(1460), #796(1460), #797(1460), #798(1460), #799(1460), #800(1460), #801(1460), #802(1460), #803(1460), #804(1460), #805(1460), #806(1460), #807(1460), #808(1460), #809(1460), #810(1460), #811(1460), #812(1460), #813(1460), #814(1460), #815(1460), #816(1460), #817(1460), #818(1460), #819(1460), #820(1460), #821(1460), #822(1460), #823(1460), #824(1460), #825(1460), #826(1460), #827(1460), #828(1460), #829(1460), #830(1460), #831(1460), #832(1460), #833(1460), #834(1460), #835(1460), #836(1460), #837(1460), #838(1460), #839(1460), #840(1460), #841(1460), #842(1460), #843(1460), #844(1460), #845(1460), #846(1460), #847(1460), #848(1460), #849(1460), #850(1460), #851(1460), #852(1460), #853(1460), #854(1460), #855(1460), #856(1460), #857(1460), #858(1460), #859(1460), #860(1460), #861(1460), #862(1460), #863(1460), #864(1460), #865(1460), #866(1460), #867(1460), #868(1460), #869(1460), #870(1460), #871(1460), #872(1460), #873(1460), #874(1460), #875(1460), #876(1460), #877(1460), #878(1460), #879(1460), #880(1460), #881(1460), #882(1460), #883(1460), #884(1460), #885(1460), #886(1460), #887(1460), #888(1460), #889(1460), #890(1460), #891(1460), #892(1460), #893(1460), #894(1460), #895(1460), #896(1460), #897(1460), #898(1460), #899(1460), #900(1460), #901(1460), #902(1460), #903(1460), #904(1460), #905(1460), #906(1460), #907(1460), #908(1460), #909(1460), #910(1460), #911(1460), #912(1460), #913(1460), #914(1460), #915(1460), #916(1460), #917(1460), #918(1460), #919(1460), #920(1460), #921(1460), #922(1460), #923(1460), #924(1460), #925(1460), #926(1460), #927(1460), #928(1460), #929(1460), #930(1460), #931(1460), #932(1460), #933(1460), #934(1460), #935(1460), #936(1460), #937(1460), #938(1460), #939(1460), #940(1460), #941(1460), #942(1460), #943(1460), #944(1460), #945(1460), #946(1460), #947(1460), #948(1460), #949(1460), #950(1460), #951(1460), #952(1460), #953(1460), #954(1460), #955(1460), #956(1460), #957(1460), #958(1460), #959(1460), #960(1460), #961(1460), #962(1460), #963(1460), #964(1460), #965(1460), #966(1460), #967(1460), #968(1460), #969(1460), #970(1460), #971(1460), #972(1460), #973(1460), #974(1460), #975(1460), #976(1460), #977(1460), #978(1460), #979(1460), #980(1460), #981(1460), #982(1460), #983(1460), #984(1460), #985(1460), #986(1460), #987(1460), #988(1460), #989(1460), #990(1460), #991(1460), #992(1460), #993(1460), #994(1460), #995(1460), #996(1460), #997(1460), #998(1460), #999(1460), #1000(1460), #1001(1460), #1002(1460), #1003(1460), #1004(1460), #1005(1460), #1006(1460), #1007(1460), #1008(1460), #1009(1460), #1010(1460), #1011(1460), #1012(1460), #1013(1460), #1014(1460), #1015(1460), #1016(1460), #1017(1460), #1018(1460), #1019(1460), #1020(1460), #1021(1460), #1022(1460), #1023(1460), #1024(1460), #1025(1460), #1026(1460), #1027(1460), #1028(1460), #1029(1460), #1030(1460), #1031(1460), #1032(1460), #1033(1460), #1034(1460), #1035(1460), #1036(1460), #1037(1460), #1038(1460), #1039(1460), #1040(1460), #1041(1460), #1042(1460), #1043(1460), #1044(1460), #1045(1460), #1046(1460), #1047(1460), #1048(1460), #1049(1460), #1050(1460), #1051(1460), #1052(1460), #1053(1460), #1054(1460), #1055(1460), #1056(1460), #1057(1460), #1058(1460), #1059(1460), #1060(1460), #1061(1460), #1062(1460), #1063(1460), #1064(1460), #1065(1460), #1066(1460), #1067(1460), #1068(1460), #1069(1460), #1070(1460), #1071(1460), #1072(1460), #1073(1460), #1074(1460), #1075(1460), #1076(1460), #1077(1460), #1078(1460), #1079(1460), #1080(1460), #1081(1460), #1082(1460), #1083(1460), #1084(1460), #1085(1460), #1086(1460), #1087(1460), #1088(1460), #1089(1460), #1090(1460), #1091(1460), #1092(1460), #1093(1460), #1094(1460), #1095(1460), #1096(1460), #1097(1460), #1098(1460), #1099(1460), #1100(1460), #1101(1460), #1102(1460), #1103(1460), #1104(146

No.	Time	Source	Destination	Protocol	Length	Info
76	4.916344	192.168.0.10	182.162.110.129	HTTP	823	GET / HTTP/1.1
160	5.108082	182.162.110.129	192.168.0.10	HTTP	500	HTTP/1.1 200 OK (text/html)
166	5.236273	192.168.0.10	118.219.56.66	HTTP	704	GET /upload/2018/07/06/data/i14
167	5.242218	192.168.0.10	118.219.56.66	HTTP	630	GET /upload/2020/04/23/bbs/thum
168	5.252884	118.219.56.66	192.168.0.10	HTTP	376	HTTP/1.1 304 Not Modified
186	5.275278	118.219.56.66	192.168.0.10	HTTP	227	HTTP/1.1 200 OK (JPEG JFIF ima
195	5.302643	192.168.0.10	118.219.56.66	HTTP	624	GET /upload/2018/12/10/bbs/i145
239	5.324079	118.219.56.66	192.168.0.10	HTTP	996	HTTP/1.1 200 OK (JPEG JFIF ima

  

>	Transmission Control Protocol, Src Port: 80, Dst Port: 56182, Seq: 1, Ack: 651, Len: 322
▼	Hypertext Transfer Protocol
>	HTTP/1.1 304 Not Modified\r\n
	Via: STON Edge Server/2.6.5\r\n
	Date: Thu, 23 Apr 2020 08:46:39 GMT\r\n
>	Content-Length: 0\r\n
	ETag: 2a14e263:3af\r\n
	Cache-Control: public, max-age=1296000\r\n
	Expires: Thu, 19 Sep 2019 07:55:07 GMT\r\n
	Age: 1783080\r\n
	Connection: Keep-Alive\r\n

  

0060	53 65 72 76 65 72 2f 32	2e 36 2e 35 0d 0a 44 61	Server/2 .6.5..Da
0070	74 65 3a 20 54 68 75 2c	20 32 33 20 41 70 72 20	te: Thu, 23 Apr
0080	32 30 32 30 20 30 38 3a	34 36 3a 33 39 20 47 4d	2020 08: 46:39 GM
0090	54 0d 0a 43 6f 6e 74 65	6e 74 2d 4c 65 6e 67 74	T..Conte nt-Lengt
00a0	68 3a 20 30 0d 0a 45 54	61 67 3a 20 32 61 31 34	h: 0..ET ag: 2a14
00b0	65 32 36 33 3a 33 61 66	0d 0a 43 61 63 68 65 2d	e263:3af ..Cache-
00c0	43 6f 6e 74 72 6f 6c 3a	20 70 75 62 6c 69 63 2c	Control: public,
00d0	20 6d 61 78 2d 61 67 65	3d 31 32 39 36 30 30 30	max-age =1296000
00e0	0d 0a 45 78 70 69 72 65	73 3a 20 54 68 75 2c 20	..Expire s: Thu,

4. Public : 공유 캐시에 저장해도 된다.

5. ETag : 캐시 업데이트 정보를 위한 임의의 식별 숫자이다.

No.	Time	Source	Destination	Protocol	Length	Info
167	5.242218	192.168.0.10	118.219.56.66	HTTP	630	GET /upload/2020/04/23/bbs/thumb/s15740355186.png HTTP/1.1
168	5.252884	118.219.56.66	192.168.0.10	HTTP	376	HTTP/1.1 304 Not Modified
186	5.275278	118.219.56.66	192.168.0.10	HTTP	227	HTTP/1.1 200 OK (JPEG JFIF image)
195	5.302643	192.168.0.10	118.219.56.66	HTTP	624	GET /upload/2018/12/10/bbs/i14501612898.jpg HTTP/1.1
239	5.324079	118.219.56.66	192.168.0.10	HTTP	996	HTTP/1.1 200 OK (JPEG JFIF image)
250	5.343239	192.168.0.10	117.52.90.29	HTTP	1039	GET /imp?slot=1318&type=if HTTP/1.1
278	5.366450	117.52.90.29	192.168.0.10	HTTP	719	HTTP/1.1 200 OK
287	5.470847	192.168.0.10	110.10.122.38	HTTP	675	GET /ad/ad_script/content_id02.js HTTP/1.1

  

>	HTTP/1.1 200 OK\r\n
	P3P: CP="NOI DSP LAW NID PSA ADM OUR IND NAV COM"\r\n
	Connection: close\r\n
	Pragma: no-cache\r\n
	Cache-Control: private, max-age=0, no-cache, no-store\r\n
	Expires: Mon, 01 Jan 2000 00:00:00 +0900\r\n
	Date: Thu, 23-Apr-2020 17:46:40 +0900\r\n
>	Content-Length: 1728\r\n
	Set-Cookie: __ch5033=@1482587_200423_000000&@1482693_200422_000000&@1482505_200422_000000; expires=Sat, 23-May-2020 17:46:40 +0900\r\n
	\r\n
	HTTP response 1/1

  

0060	6f 2d 63 61 63 68 65 0d	0a 43 61 63 68 65 2d 43	o-cache..Cache-C
0070	6f 6e 74 72 6f 6c 3a 20	70 72 69 76 61 74 65 2c	ontrol: private,
0080	20 6d 61 78 2d 61 67 65	3d 30 2c 20 6e 6f 2d 63	max-age =0, no-c
0090	61 63 68 65 2c 20 6e 6f	2d 73 74 6f 72 65 0d 0a	ache, no -store..
00a0	45 78 70 69 72 65 73 3a	20 54 68 75 2c 20 30 30	Expires: Mon, 01

6. Private : '브라우저'같은 특정 사용자 환경에만 저장한다.

7. No-store : 캐시를 저장하지 않는다.

## 5) 자유 주제

HTTP 와 HTTPS 의 차이점 : 암호화

HTTP 로만 된 사이트에서 로그인을 했을 때 패킷을 분석해 보면 암호화가 되어있지 않다. 암호화가 중요한 이유는 패킷이 중간에 스푸핑 될 수 있기 때문이다. 만약 해커가

로그인 할 때의 패킷을 가지면 username 과 password 를 알 수 있다. 실습한 사이트에서는 그 사이트에서 직접 로그인이 불가능하고 네이버 로그인 페이지로 넘어갔기 때문에 해당 내용을 확인할 수 없었다.

### **3. 새로 알게 된 지식**

DNT(Do Not Track) : HTTP 요청 헤더 중 하나로 쿠키 등을 이용한 정보 추적을 금지한다는 의미를 웹서버에 전달한다.

각 프로토콜의 헤더만 분석하면 전송되는 데 필요한 정보들을 모두 얻을 수 있다.