

컴퓨터망 과제

(2020 겨울계절)

고석주 교수님

전자공학부

2014104276

이찬구

① ping(ICMP)

- 서버가 죽었는지 살았는지 확인할 때 사용

```
C:\Users\WASUS B150M-A>ping google.com

Ping google.com [172.217.25.238] 32바이트 데이터 사용:
172.217.25.238의 응답: 바이트=32 시간=38ms TTL=54
172.217.25.238의 응답: 바이트=32 시간=38ms TTL=54
172.217.25.238의 응답: 바이트=32 시간=38ms TTL=54
172.217.25.238의 응답: 바이트=32 시간=38ms TTL=54

172.217.25.238에 대한 Ping 통계:
패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간<밀리초>:
최소 = 38ms, 최대 = 38ms, 평균 = 38ms

C:\Users\WASUS B150M-A>
```

● 내 컴퓨터 => 구글

The image shows a Wireshark packet capture of an ICMP ping. The top pane displays a list of packets, and the bottom pane shows the detailed view of a selected packet (Frame 21).

No.	Time	Source	Destination	Protocol	Length	Info
21	3.429427	192.168.55.225	172.217.25.238	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, tt
22	3.468051	172.217.25.238	192.168.55.225	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, tt
25	4.431944	192.168.55.225	172.217.25.238	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, tt
26	4.470505	172.217.25.238	192.168.55.225	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, tt
27	5.434912	192.168.55.225	172.217.25.238	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, tt
28	5.473504	172.217.25.238	192.168.55.225	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, tt
30	6.437882	192.168.55.225	172.217.25.238	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, tt
31	6.476542	172.217.25.238	192.168.55.225	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, tt

Frame 21: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{54A3A1C6-DD2A-4B9B-8BCD-2A8280}

- Ethernet II, Src: AsustekC_86:64:bb (f8:32:e4:86:64:bb), Dst: Hfr_79:43:1a (00:23:aa:79:43:1a)
 - Destination: Hfr_79:43:1a (00:23:aa:79:43:1a)
 - Source: AsustekC_86:64:bb (f8:32:e4:86:64:bb)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.55.225, Dst: 172.217.25.238
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 60
 - Identification: 0x1bd8 (7128)
 - Flags: 0x0000
 - ...0 0000 0000 0000 = Fragment offset: 0
 - Time to live: 128
 - Protocol: ICMP (1)
 - Header checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.55.225
 - Destination: 172.217.25.238
- Internet Control Message Protocol

Packet Bytes:

Offset	Hex	ASCII
0000	00 23 aa 79 43 1a f8 32 e4 86 64 bb 08 00 45 00	..#.yC..2..d...E..
0010	00 3c 1b d8 00 00 80 01 00 00 c0 a8 37 e1 ac d9	..<.....7... ..
0020	19 ee 08 00 4d 51 00 01 00 0a 61 62 63 64 65 66	...MQ... ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

- 나의 IP address : 192.168.55.225
- google의 IP address 172.217.25.238
- 나의 IP와 구글의 IP가 네 번 핑을 주고받은 상태이다. (request - reply 응답이 네 번 있다)
- IPv4를 사용하고 있다.
- Header length는 20bytes이다. IP 헤더의 크기를 의미한다.
- Service는 0x00(기본서비스)를 사용하고 있다.
- Total length는 60bytes이다.(데이터와 헤더를 모두 포함한 길이)
- TTL(Time To Live)는 128이다. 128개의 라우터를 통과하면 소멸.
- 프로토콜은 ICMP이다.
- Header checksum을 사용하고 있다.(Header에 대해서만 체크)

● 구글 => 내 컴퓨터

The image shows a Wireshark packet capture titled 'icmp_ping.pcapng'. The packet list pane shows several ICMP Echo (ping) request and reply packets. The selected packet is an ICMP Echo (ping) reply from 172.217.25.238 to 192.168.55.225.

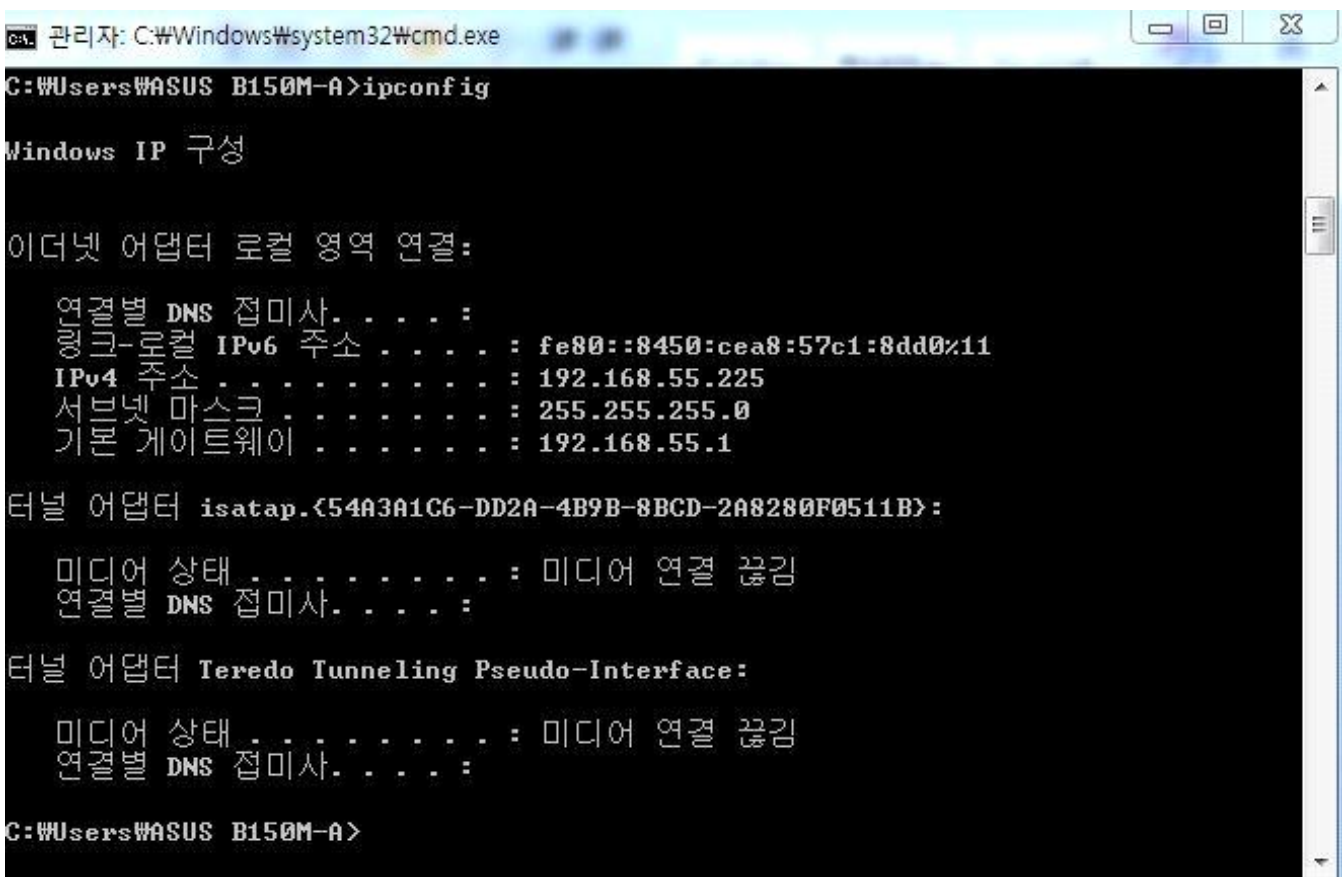
No.	Time	Source	Destination	Protocol	Length	Info
21	3.429427	192.168.55.225	172.217.25.238	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, tt
22	3.468051	172.217.25.238	192.168.55.225	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, tt
25	4.431944	192.168.55.225	172.217.25.238	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, tt
26	4.470505	172.217.25.238	192.168.55.225	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, tt
27	5.434912	192.168.55.225	172.217.25.238	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, tt
28	5.473504	172.217.25.238	192.168.55.225	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, tt
30	6.437882	192.168.55.225	172.217.25.238	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, tt
31	6.476542	172.217.25.238	192.168.55.225	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, tt

The packet details pane shows the following information for the selected packet:

- Source: Hfr_79:43:1a (00:23:aa:79:43:1a)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.217.25.238, Dst: 192.168.55.225
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 60
 - Identification: 0x0000 (0)
 - Flags: 0x0000
 - ...0 0000 0000 0000 = Fragment offset: 0
 - Time to live: 54
 - Protocol: ICMP (1)
 - Header checksum: 0xc570 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 172.217.25.238
 - Destination: 192.168.55.225
- Internet Control Message Protocol
 - Type: 0 (Echo (ping) reply)
 - Code: 0
 - Checksum: 0x5551 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)

The packet bytes pane shows the raw data of the packet, including the IP header, ICMP header, and the payload.

- IPv4를 사용하고 있다.
- Header length는 20bytes이다. IP 헤더의 크기를 의미한다.
- Service는 0x00(기본서비스)를 사용하고 있다.
- Total length는 60bytes이다.(데이터와 헤더를 모두 포함한 길이)
- TTL(Time To Live)는 54이다. 54개의 라우터를 통과하면 소멸.
- 프로토콜은 ICMP이다.
- Header checksum을 사용하고 있다.(Header에 대해서만 체크)



- ipconfig를 이용하여 나의 컴퓨터의 IP주소가 192.168.55.225임을 확인

② website visit(TCP, HTTP)

1. The Basic HTTP GET/response interaction

The image shows a Wireshark packet capture of an HTTP interaction. The top pane displays a list of packets, with packet 392 selected. The middle pane shows the details of packet 392, which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
243	3.230130	54.230.181.86	192.168.55.225	HTTP	272	HTTP/1.1 200 OK (PNG)
254	3.232186	54.230.181.86	192.168.55.225	HTTP	1390	HTTP/1.1 200 OK (JPEG JFIF image)
260	3.233884	54.230.181.86	192.168.55.225	HTTP	1079	HTTP/1.1 200 OK (JPEG JFIF image)
270	3.234901	54.230.181.86	192.168.55.225	HTTP	1371	HTTP/1.1 200 OK (JPEG JFIF image)
274	3.234902	54.230.181.86	192.168.55.225	HTTP	579	HTTP/1.1 200 OK (JPEG JFIF image)
283	3.775157	192.168.55.225	121.78.190.86	HTTP	152	GET /AuthServer/xml/ex.txt HTTP/1.1
383	3.851757	121.78.190.86	192.168.55.225	HTTP	1043	Continuation
392	4.292227	192.168.55.225	128.119.245.12	HTTP	354	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
396	4.505868	128.119.245.12	192.168.55.225	HTTP	540	HTTP/1.1 200 OK (text/html)
398	4.601581	192.168.55.225	128.119.245.12	HTTP	267	GET /favicon.ico HTTP/1.1
423	4.811282	128.119.245.12	192.168.55.225	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 392: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface \Device\NPF_{54A3A1C6-DD2A-4B9B-8BCC-...}

Ethernet II, Src: AsustekC 86:64:bb (f8:32:e4:86:64:bb), Dst: Hfr_79:43:1a (00:23:aa:79:43:1a)

Internet Protocol Version 4, Src: 192.168.55.225, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50012, Dst Port: 80, Seq: 1, Ack: 1, Len: 300

Hypertext Transfer Protocol

- GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 - [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file1.html
 - Request Version: HTTP/1.1
 - Accept: text/html, application/xhtml+xml, */*\r\n
 - Accept-Language: ko-KR\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Host: gaia.cs.umass.edu\r\n
 - DNT: 1\r\n
 - Connection: Keep-Alive\r\n
 - \r\n
 - [Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>]
 - [HTTP request 1/2]

0000 00 23 aa 79 43 1a f8 32 e4 86 64 bb 08 00 45 00 .#.yC..2..d...E.
0010 01 54 69 9d 40 00 80 06 00 00 c0 a8 37 e1 80 77 .Ti.@... ..7..w
0020 f5 0c c3 5c 00 50 5c fb fd 8a 7f 0c 53 57 50 18 ...\.P\.. ..SWP.
0030 40 29 6f 54 00 00 47 45 54 20 2f 77 69 72 65 73 @)oT...GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 tml HTTP /1.1..Ac

Expert Info (.ws,expert) | Packets: 454 · Displayed: 42 (9.3%) | Profile: Default

The image shows a Wireshark packet capture of an HTTP 200 OK response. The packet list at the top shows several packets, with packet 396 selected. The packet details pane shows the following information:

- Frame 396: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{54A3A1C6-DD2A-4B9B-8BCC}
- Ethernet II, Src: Hfr_79:43:1a (00:23:aa:79:43:1a), Dst: AsustekC_86:64:bb (f8:32:e4:86:64:bb)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.55.225
- Transmission Control Protocol, Src Port: 80, Dst Port: 50012, Seq: 1, Ack: 301, Len: 486
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Date: Mon, 06 Jan 2020 14:09:29 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
 - Last-Modified: Mon, 06 Jan 2020 06:59:03 GMT\r\n
 - ETag: "80-59b7331d7a816"\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 1/2]
 - [Time since request: 0.213641000 seconds]

The packet bytes pane at the bottom shows the raw data of the selected packet, which is the HTTP response.

- 내 컴퓨터와 서버 모두 HTTP1.1을 사용중
- Accept-Ranges는 bytes이다.
- 내 컴퓨터의 IP address는 192.168.55.225, gaia.cs.umass.edu 서버의 IP address는 128.119.245.12
- Status code는 200이다.(응답이 정상이라는 의미)
- 2020년 1월 6일 06:59:03에 HTML파일이 서버에서 마지막으로 수정되었다.
- content-Length는 128이다.

http.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 17

No.	Time	Source	Destination	Protocol	Length	Info
388	4.085390	192.168.55.225	128.119.245.12	TCP	66	50012 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
390	4.289110	128.119.245.12	192.168.55.225	TCP	66	80 → 50012 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
391	4.289222	192.168.55.225	128.119.245.12	TCP	54	50012 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
392	4.292227	192.168.55.225	128.119.245.12	HTTP	354	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
395	4.499911	128.119.245.12	192.168.55.225	TCP	60	80 → 50012 [ACK] Seq=1 Ack=301 Win=30336 Len=0
396	4.505868	128.119.245.12	192.168.55.225	HTTP	540	HTTP/1.1 200 OK (text/html)
397	4.505934	192.168.55.225	128.119.245.12	TCP	54	50012 → 80 [ACK] Seq=301 Ack=487 Win=65212 Len=0
398	4.601581	192.168.55.225	128.119.245.12	HTTP	267	GET /favicon.ico HTTP/1.1
423	4.811282	128.119.245.12	192.168.55.225	HTTP	538	HTTP/1.1 404 Not Found (text/html)
424	4.811355	192.168.55.225	128.119.245.12	TCP	54	50012 → 80 [ACK] Seq=514 Ack=971 Win=64728 Len=0
449	9.822335	128.119.245.12	192.168.55.225	TCP	60	80 → 50012 [FIN, ACK] Seq=971 Ack=514 Win=31360 Len=0
450	9.822415	192.168.55.225	128.119.245.12	TCP	54	50012 → 80 [ACK] Seq=514 Ack=972 Win=64728 Len=0

▶ Frame 388: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{5443A1C6-0D2A-4B9B-8BCD-2A8280F05118}, id 0
 ▶ Ethernet II, Src: Asustek_86:64:bb (f8:32:e4:86:64:bb), Dst: Hfr_79:43:1a (00:23:aa:79:43:1a)
 ▶ Internet Protocol Version 4, Src: 192.168.55.225, Dst: 128.119.245.12
 ▶ Transmission Control Protocol, Src Port: 50012, Dst Port: 80, Seq: 0, Len: 0

- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK (3-way Handshake과정)순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 연결이 완료 된 후 클라이언트 컴퓨터는 GET 방식으로 HTTP를 요청한다.
- seq는 보내는 데이터가 몇 번부터 시작을 하는지를 의미하며 ack은 내가 그다음 받아야하는 데이터가 어디인지에 대한 정보가 포함되어있다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.
- port 80은 well-know port number로써 서버를 의미하며 port 50012는 클라이언트를 의미.

2. The HTTP CONDITIONAL GET/response interaction

- first

The image shows a Wireshark packet capture window titled "*로컬 영역 연결". The packet list at the top shows several HTTP packets. Packet 25 is a GET request for "/wireshark-labs/HTTP-wireshark-file2.html" from 192.168.55.225 to 128.119.245.12. Packet 33 is a 304 Not Modified response from 128.119.245.12 to 192.168.55.225. Packet 60 is another GET request for the same file. Packet 61 is another 304 Not Modified response. Packet 70 is a GET request for "/AuthServer/xml/ex.". The details pane for packet 25 is expanded, showing the Hypertext Transfer Protocol section. The request line is "GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n". The Host is "gaia.cs.umass.edu\r\n". The User-Agent is "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome...". The Accept-Encoding is "gzip, deflate\r\n". The Accept-Language is "ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n". The If-None-Match is "173-59b874f96214a"\r\n". The If-Modified-Since is "Tue, 07 Jan 2020 06:59:01 GMT\r\n". The full request URI is "http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html". The status is "HTTP request 1/2". The response is in frame 33. The next request is in frame 60. The packet bytes pane at the bottom shows the raw data of the request line, which is 50 bytes long.

No.	Time	Source	Destination	Protocol	Length	Info
25	2.909201	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
33	3.115689	128.119.245.12	192.168.55.225	HTTP	294	HTTP/1.1 304 Not Modified
60	6.675693	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
61	6.884141	128.119.245.12	192.168.55.225	HTTP	293	HTTP/1.1 304 Not Modified
70	7.893802	192.168.55.225	121.78.190.86	HTTP	152	GET /AuthServer/xml/ex.

Frame 25: 650 bytes on wire (5200 bits), 650 bytes captured (5200 bits) on interface \Device\NPF_{54...}

Ethernet II, Src: AsustekC_86:64:bb (f8:32:e4:86:64:bb), Dst: Hfr_79:43:1a (00:23:aa:79:43:1a)

Internet Protocol Version 4, Src: 192.168.55.225, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50765, Dst Port: 80, Seq: 1, Ack: 1, Len: 596

Hypertext Transfer Protocol

- GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
 - [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file2.html
 - Request Version: HTTP/1.1
 - 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 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome...
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app...
 - 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: "173-59b874f96214a"\r\n
 - If-Modified-Since: Tue, 07 Jan 2020 06:59:01 GMT\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: 33]
 - [Next request in frame: 60]

0220 53 b 71 3d 30 2e 38 2c 65 6e 3b 71 3d 30 2e 37 S;q=0.8, en;q=0.7

0230 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a ..If-Non e-Match:

0240 20 22 31 37 33 2d 35 39 62 38 37 34 66 39 36 32 "173-59 b874f962

0250 31 34 61 22 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 14a"...If -Modifie

0260 64 2d 53 69 6e 63 65 3a 20 54 75 65 2c 20 30 37 d-Since: Tue, 07

0270 20 4a 61 6e 20 32 30 32 30 20 30 36 3a 35 39 3a Jan 202 0 06:59:

0280 30 31 20 47 4d 54 0d 0a 0d 0a 01 GMT... ..

Request line (http.request.line), 50 byte(s) | Packets: 174 · Displayed: 5 (2.9%) · Dropped: 0 (0.0%) | Profile: Default

*로컬 영역 연결

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
25	2.909201	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTT
33	3.115689	128.119.245.12	192.168.55.225	HTTP	294	HTTP/1.1 304 Not Modifi
60	6.675693	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTT
61	6.884141	128.119.245.12	192.168.55.225	HTTP	293	HTTP/1.1 304 Not Modifi
70	7.893802	192.168.55.225	121.78.190.86	HTTP	152	GET /AuthServer/xml/ex.

Frame 33: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{54...}

Ethernet II, Src: Hfr_79:43:1a (00:23:aa:79:43:1a), Dst: AsustekC_86:64:bb (f8:32:e4:86:64:bb)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.55.225

Transmission Control Protocol, Src Port: 80, Dst Port: 50765, Seq: 1, Ack: 597, Len: 240

Hypertext Transfer Protocol

- HTTP/1.1 304 Not Modified\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
 - [HTTP/1.1 304 Not Modified\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Response Version: HTTP/1.1
 - Status Code: 304
 - [Status Code Description: Not Modified]
 - Response Phrase: Not Modified
 - Date: Tue, 07 Jan 2020 15:38:54 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
 - Connection: Keep-Alive\r\n
 - Keep-Alive: timeout=5, max=100\r\n
 - ETag: "173-59b874f96214a"\r\n
 - \r\n
 - [HTTP response 1/2]
 - [Time since request: 0.206488000 seconds]
 - [Request in frame: 25]
 - [Next request in frame: 60]
 - [Next response in frame: 61]
 - [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

0000 f8 32 e4 86 64 bb 00 23 aa 79 43 1a 08 00 45 00 .2..d..# .yC...E.

0010 01 18 cd 94 40 00 2b 06 13 3e 80 77 f5 0c c0 a8@+..>.w....

0020 37 e1 00 50 c6 4d 87 21 21 0f db aa ac 02 50 18 7..P.M-!!.....P-

0030 00 ee 38 2b 00 00 48 54 54 50 2f 31 2e 31 20 33 ..8+..HT TP/1.1 3

0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not M odified.

0050 0a 44 61 74 65 3a 20 54 75 65 2c 20 30 37 20 4a .Date: T ue, 07 J

0060 61 6e 20 32 30 32 30 20 31 35 3a 33 38 3a 35 34 an 2020 15:38:54

wireshark_로컬 영역 연결_20200108003852_a01364.pcapng | Packets: 174 · Displayed: 5 (2,9%) · Dropped: 0 (0,0%) | Profile: Default

- If-Modified-Since: 2020년 1월 7일 화요일

http_2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 3

No.	Time	Source	Destination	Protocol	Length	Info
20	2.703496	192.168.55.225	128.119.245.12	TCP	66	50765 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
22	2.906257	128.119.245.12	192.168.55.225	TCP	66	80 → 50765 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
23	2.906359	192.168.55.225	128.119.245.12	TCP	54	50765 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
25	2.909201	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
32	3.115339	128.119.245.12	192.168.55.225	TCP	60	80 → 50765 [ACK] Seq=1 Ack=597 Win=30464 Len=0
33	3.115689	128.119.245.12	192.168.55.225	HTTP	294	HTTP/1.1 304 Not Modified
36	3.315781	192.168.55.225	128.119.245.12	TCP	54	50765 → 80 [ACK] Seq=597 Ack=241 Win=65460 Len=0
60	6.675693	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
61	6.884141	128.119.245.12	192.168.55.225	HTTP	293	HTTP/1.1 304 Not Modified
62	7.085510	192.168.55.225	128.119.245.12	TCP	54	50765 → 80 [ACK] Seq=1193 Ack=480 Win=65220 Len=0

- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK 순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.

● Second

*로컬 영역 연결

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
25	2.909201	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTT
33	3.115689	128.119.245.12	192.168.55.225	HTTP	294	HTTP/1.1 304 Not Modifi
60	6.675693	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTT
61	6.884141	128.119.245.12	192.168.55.225	HTTP	293	HTTP/1.1 304 Not Modifi
70	7.893802	192.168.55.225	121.78.190.86	HTTP	152	GET /AuthServer/xml/ex.

Frame 60: 650 bytes on wire (5200 bits), 650 bytes captured (5200 bits) on interface \Device\NPF_{54
 Ethernet II, Src: AsustekC_86:64:bb (f8:32:e4:86:64:bb), Dst: Hfr_79:43:1a (00:23:aa:79:43:1a)
 Internet Protocol Version 4, Src: 192.168.55.225, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 50765, Dst Port: 80, Seq: 597, Ack: 241, Len: 596
 Hypertext Transfer Protocol
 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
 [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
 [Severity level: Chat]
 [Group: Sequence]
 Request Method: GET
 Request URI: /wireshark-labs/HTTP-wireshark-file2.html
 Request Version: HTTP/1.1
 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 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app
 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: "173-59b874f96214a"\r\n
 If-Modified-Since: Tue, 07 Jan 2020 06:59:01 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: 25]
 [Response in frame: 61]

0220 53 3b 71 3d 30 2e 38 2c 65 6e 3b 71 3d 30 2e 37 S;q=0.8, en;q=0.7
 0230 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a ..If-Non e-Match:
 0240 20 22 31 37 33 2d 35 39 62 38 37 34 66 39 36 32 "173-59 b874f962
 0250 31 34 61 22 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 14a"··If -Modifie
 0260 64 2d 53 69 6e 63 65 3a 20 54 75 65 2c 20 30 37 d-Since: Tue, 07
 0270 20 4a 61 6e 20 32 30 32 30 20 30 36 3a 35 39 3a Jan 202 0 06:59:
 0280 30 31 20 47 4d 54 0d 0a 0d 0a 01 GMT·· ..

Request line (http,request,line), 50 byte(s) | Packets: 174 · Displayed: 5 (2,9%) · Dropped: 0 (0,0%) | Profile: Default

Wireshark interface showing a packet capture of an HTTP 304 Not Modified response.

No.	Time	Source	Destination	Protocol	Length	Info
25	2.909201	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
33	3.115689	128.119.245.12	192.168.55.225	HTTP	294	HTTP/1.1 304 Not Modified
60	6.675693	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
61	6.884141	128.119.245.12	192.168.55.225	HTTP	293	HTTP/1.1 304 Not Modified
70	7.893802	192.168.55.225	121.78.190.86	HTTP	152	GET /AuthServer/xml/ex...

Frame 61: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{54...}

Ethernet II, Src: Hfr_79:43:1a (00:23:aa:79:43:1a), Dst: AsustekC_86:64:bb (f8:32:e4:86:64:bb)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.55.225

Transmission Control Protocol, Src Port: 80, Dst Port: 50765, Seq: 241, Ack: 1193, Len: 239

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]

[HTTP/1.1 304 Not Modified\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 304

[Status Code Description: Not Modified]

Response Phrase: Not Modified

Date: Tue, 07 Jan 2020 15:38:58 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n

Connection: Keep-Alive\r\n

Keep-Alive: timeout=5, max=99\r\n

ETag: "173-59b874f96214a"\r\n

\r\n

[HTTP response 2/2]

[Time since request: 0.208448000 seconds]

[Prev request in frame: 25]

[Prev response in frame: 33]

[Request in frame: 60]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

Wireshark interface showing a packet capture of a TCP connection and HTTP request.

No.	Time	Source	Destination	Protocol	Length	Info
20	2.703496	192.168.55.225	128.119.245.12	TCP	66	50765 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
22	2.906257	128.119.245.12	192.168.55.225	TCP	66	80 → 50765 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
23	2.906359	192.168.55.225	128.119.245.12	TCP	54	50765 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
25	2.909201	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
32	3.115339	128.119.245.12	192.168.55.225	TCP	60	80 → 50765 [ACK] Seq=1 Ack=597 Win=30464 Len=0
33	3.115689	128.119.245.12	192.168.55.225	HTTP	294	HTTP/1.1 304 Not Modified
36	3.315781	192.168.55.225	128.119.245.12	TCP	54	50765 → 80 [ACK] Seq=597 Ack=241 Win=65460 Len=0
60	6.675693	192.168.55.225	128.119.245.12	HTTP	650	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
61	6.884141	128.119.245.12	192.168.55.225	HTTP	293	HTTP/1.1 304 Not Modified
62	7.085510	192.168.55.225	128.119.245.12	TCP	54	50765 → 80 [ACK] Seq=1193 Ack=480 Win=65220 Len=0

- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK 순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.

3. Retrieving Long Documents

The image displays two screenshots of the Wireshark network traffic analysis tool. The top screenshot shows a detailed view of an HTTP GET request (Frame 34) from 192.168.55.225 to 128.119.245.12. The request is for the file `/wireshark-labs/HTTP-wireshark-file3.html` on the host `gaia.cs.umass.edu`. The bottom screenshot shows a broader view of the TCP connection sequence (frames 28-60) between the same IP addresses. The sequence starts with a SYN exchange (frames 28-33) and ends with a FIN exchange (frames 59-60).

Top Screenshot: HTTP GET Request Details

No.	Time	Source	Destination	Protocol	Length	Info
34	2.110257	192.168.55.225	128.119.245.12	HTTP	538	GET /wireshark-labs/H...
42	2.429338	128.119.245.12	192.168.55.225	HTTP	535	HTTP/1.1 200 OK (tex...

Frame 34 Details:

- Frame 34: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{54...}
- Ethernet II, Src: AsustekC_86:64:bb (f8:32:e4:86:64:bb), Dst: Hfr_79:43:1a (00:23:aa:79:43:1a)
- Internet Protocol Version 4, Src: 192.168.55.225, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 53916, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
- Hypertext Transfer Protocol**
 - GET /wireshark-labs/HTTP-wireshark-file3.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 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome...
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,app...
 - 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-file3.html>]
 - [HTTP request 1/1]
 - [Response in frame: 42]

Bottom Screenshot: TCP Connection Sequence

No.	Time	Source	Destination	Protocol	Length	Info
28	1.794442	192.168.55.225	128.119.245.12	TCP	66	53916 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_P...
32	2.106844	128.119.245.12	192.168.55.225	TCP	66	80 → 53916 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460...
33	2.106962	192.168.55.225	128.119.245.12	TCP	54	53916 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
34	2.110257	192.168.55.225	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
37	2.426367	128.119.245.12	192.168.55.225	TCP	60	80 → 53916 [ACK] Seq=1 Ack=485 Win=30336 Len=0
38	2.429214	128.119.245.12	192.168.55.225	TCP	1514	80 → 53916 [ACK] Seq=1 Ack=485 Win=30336 Len=1460 [TCP seg...
39	2.429215	128.119.245.12	192.168.55.225	TCP	1514	80 → 53916 [ACK] Seq=1461 Ack=485 Win=30336 Len=1460 [TCP ...
40	2.429263	192.168.55.225	128.119.245.12	TCP	54	53916 → 80 [ACK] Seq=485 Ack=2921 Win=65700 Len=0
41	2.429337	128.119.245.12	192.168.55.225	TCP	1514	80 → 53916 [ACK] Seq=2921 Ack=485 Win=30336 Len=1460 [TCP ...
42	2.429338	128.119.245.12	192.168.55.225	HTTP	535	HTTP/1.1 200 OK (text/html)
43	2.429387	192.168.55.225	128.119.245.12	TCP	54	53916 → 80 [ACK] Seq=485 Ack=4862 Win=65700 Len=0
59	7.437674	128.119.245.12	192.168.55.225	TCP	60	80 → 53916 [FIN, ACK] Seq=4862 Ack=485 Win=30336 Len=0
60	7.437709	192.168.55.225	128.119.245.12	TCP	54	53916 → 80 [ACK] Seq=485 Ack=4863 Win=65700 Len=0

- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK 순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.

4. HTML Documents with Embedded Objects

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a packet capture of an HTTP GET request for a file named 'HTTP-wireshark-file4.html'. The packet list shows a sequence of requests for various resources, including a spurious retransmission. The packet details pane for frame 99 shows the full HTTP request, including the Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language headers. The packet bytes pane shows the raw data of the request.

The bottom screenshot shows a packet capture of a TCP stream. The packet list shows a sequence of TCP and HTTP packets. The packet details pane for frame 51 shows the TCP SYN packet, indicating the start of a new connection. The packet bytes pane shows the raw data of the SYN packet.

No.	Time	Source	Destination	Protocol	Length	Info
55	2.334231	192.168.55.225	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
57	2.546582	128.119.245.12	192.168.55.225	HTTP	1127	HTTP/1.1 200 OK (text/html)
58	2.646423	192.168.55.225	128.119.245.12	HTTP	470	GET /pearson.png HTTP/1.1
62	2.852781	128.119.245.12	192.168.55.225	HTTP	745	HTTP/1.1 200 OK (PNG)
71	3.292438	192.168.55.225	128.119.245.12	HTTP	484	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
78	3.314814	192.168.55.225	211.115.106.77	HTTP	427	GET /jk?c=62&p=WLL96Rrr0UTYNS1Q20z4xu+rQFjDYQW3k3QnpoejMs... HTTP/1.1
80	3.326877	211.115.106.77	192.168.55.225	HTTP	406	HTTP/1.1 200 OK
99	3.533665	211.115.106.77	192.168.55.225	HTTP	406	[TCP Spurious Retransmission] HTTP/1.1 200 OK
179	3.935583	128.119.245.12	192.168.55.225	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)
194	6.256980	192.168.55.225	121.78.190.86	HTTP	152	GET /AuthServer/xml/ex.txt HTTP/1.1
290	6.314941	121.78.190.86	192.168.55.225	HTTP	1043	Continuation

No.	Time	Source	Destination	Protocol	Length	Info
51	2.128162	192.168.55.225	128.119.245.12	TCP	66	54050 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_P...
53	2.331928	128.119.245.12	192.168.55.225	TCP	66	80 → 54050 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
54	2.332053	192.168.55.225	128.119.245.12	TCP	54	54050 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
55	2.334231	192.168.55.225	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
56	2.539831	128.119.245.12	192.168.55.225	TCP	60	80 → 54050 [ACK] Seq=1 Ack=485 Win=30336 Len=0
57	2.546582	128.119.245.12	192.168.55.225	HTTP	1127	HTTP/1.1 200 OK (text/html)
58	2.646423	192.168.55.225	128.119.245.12	HTTP	470	GET /pearson.png HTTP/1.1
60	2.852780	128.119.245.12	192.168.55.225	TCP	1514	80 → 54050 [ACK] Seq=1074 Ack=901 Win=31360 Len=1460 [TCP ...]
61	2.852781	128.119.245.12	192.168.55.225	TCP	1514	80 → 54050 [ACK] Seq=2534 Ack=901 Win=31360 Len=1460 [TCP ...]
62	2.852781	128.119.245.12	192.168.55.225	HTTP	745	HTTP/1.1 200 OK (PNG)
63	2.852943	192.168.55.225	128.119.245.12	TCP	54	54050 → 80 [ACK] Seq=901 Ack=4685 Win=65700 Len=0
297	7.857114	128.119.245.12	192.168.55.225	TCP	60	80 → 54050 [FIN, ACK] Seq=4685 Ack=901 Win=31360 Len=0
298	7.857175	192.168.55.225	128.119.245.12	TCP	54	54050 → 80 [ACK] Seq=901 Ack=4686 Win=65700 Len=0

- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK 순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.

5 HTTP Authentication

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list pane displays several packets, with packet 38 selected. The packet details pane shows the structure of the selected packet, which is an HTTP 401 Unauthorized response. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
32	1.880314	192.168.55.225	128.119.245.12	HTTP	553	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.ht...
38	2.116218	128.119.245.12	192.168.55.225	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
59	7.070922	192.168.55.225	121.78.190.86	HTTP	152	GET /AuthServer/xml/ex.txt HTTP/1.1
153	7.124328	121.78.190.86	192.168.55.225	HTTP	1043	Continuation
242	15.040530	192.168.55.225	128.119.245.12	HTTP	638	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.ht...
246	15.248824	128.119.245.12	192.168.55.225	HTTP	583	HTTP/1.1 404 Not Found (text/html)

Packet 38 details:

- Ethernet II, Src: AsustekC_86:64:bb (f8:32:e4:86:64:bb), Dst: Hfr_79:43:1a (00:23:aa:79:43:1a)
- Internet Protocol Version 4, Src: 192.168.55.225, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 54204, Dst Port: 80, Seq: 1, Ack: 1, Len: 499
- 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
 - Upgrade-Insecure-Requests: 1\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 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
 - 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

- 알맞게 네임과 비밀번호를 입력하였지만 Unauthorized 되었다.

The screenshot shows a Wireshark packet capture of a TCP connection and an HTTP transaction. The packet list pane displays several packets, with packet 38 selected. The packet details pane shows the structure of the selected packet, which is an HTTP 401 Unauthorized response. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
28	1.652295	192.168.55.225	128.119.245.12	TCP	66	54204 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_P...
30	1.877238	128.119.245.12	192.168.55.225	TCP	66	80 → 54204 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460...
31	1.877340	192.168.55.225	128.119.245.12	TCP	54	54204 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
32	1.880314	192.168.55.225	128.119.245.12	HTTP	553	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.ht...
37	2.107626	128.119.245.12	192.168.55.225	TCP	60	80 → 54204 [ACK] Seq=1 Ack=500 Win=30336 Len=0
38	2.116218	128.119.245.12	192.168.55.225	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
40	2.310671	192.168.55.225	128.119.245.12	TCP	54	54204 → 80 [ACK] Seq=500 Ack=718 Win=64980 Len=0
140	7.123020	128.119.245.12	192.168.55.225	TCP	60	80 → 54204 [FIN, ACK] Seq=718 Ack=500 Win=30336 Len=0
141	7.123038	192.168.55.225	128.119.245.12	TCP	54	54204 → 80 [ACK] Seq=500 Ack=719 Win=64980 Len=0
159	9.776638	192.168.55.225	128.119.245.12	TCP	54	54204 → 80 [FIN, ACK] Seq=500 Ack=719 Win=64980 Len=0
187	10.002034	128.119.245.12	192.168.55.225	TCP	60	80 → 54204 [ACK] Seq=719 Ack=501 Win=30336 Len=0

③ nslookup(DNS)

- nslookup을 이용하여 도메인의 ip주소를 찾을수 있다.

```
관리자: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\WASUS B150M-A>nslookup www.mit.edu
서버:      bns1.hananet.net
Address:   210.220.163.82

권한 없는 응답:
이름:      e9566.dsch.akamaiedge.net
Addresses: 2600:140b:4:699::255e
           2600:140b:4:6b3::255e
           104.74.184.126
Aliases:   www.mit.edu
           www.mit.edu.edgekey.net

C:\Users\WASUS B150M-A>nslookup -type=NS mit.edu
서버:      bns1.hananet.net
Address:   210.220.163.82

권한 없는 응답:
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = usw2.akam.net

C:\Users\WASUS B150M-A>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
서버:      UnKnown
Address:   18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** UnKnown에 대한 요청이 제한 시간을 초과했습니다.

C:\Users\WASUS B150M-A>
```


● ipconfig

```
관리자: C:\Windows\system32\cmd.exe
C:\Users\ASUS B150M-A>ipconfig /all

Windows IP 구성

호스트 이름 . . . . . : ASUSB150M-A-PC
주 DNS 접미사 . . . . . :
노드 유형 . . . . . : 혼성
IP 라우팅 사용 . . . . . : 아니요
WINS 프록시 사용 . . . . . : 아니요

이더넷 어댑터 로컬 영역 연결:

연결별 DNS 접미사. . . . . :
설명 . . . . . : Realtek PCIe GBE Family Controller
물리적 주소 . . . . . : F8-32-E4-86-64-BB
DHCP 사용 . . . . . : 예
자동 구성 사용 . . . . . : 예
링크-로컬 IPv6 주소 . . . . . : fe80::8450:cea8:57c1:8dd0%11<기본 설정>
IPv4 주소 . . . . . : 192.168.55.225<기본 설정>
서브넷 마스크 . . . . . : 255.255.255.0
임대 시작 날짜 . . . . . : 2020년 1월 8일 수요일 오후 3:29:26
임대 만료 날짜 . . . . . : 2020년 1월 8일 수요일 오후 5:29:25
기본 게이트웨이 . . . . . : 192.168.55.1
DHCP 서버 . . . . . : 192.168.55.1
DHCPv6 IAID . . . . . : 251146980
DHCPv6 클라이언트 DUID. . . : 00-01-00-01-1D-B3-6C-22-F8-32-E4-86-64-BB
DNS 서버 . . . . . : 210.220.163.82
                  210.220.163.82
Tcpip를 통한 NetBIOS. . . . . : 사용

터널 어댑터 isatap.{54A3A1C6-DD2A-4B9B-8BCD-2A8280F0511B}:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사. . . . . :
설명 . . . . . : Microsoft ISATAP Adapter
물리적 주소 . . . . . : 00-00-00-00-00-00-E0
DHCP 사용 . . . . . : 아니요
자동 구성 사용 . . . . . : 예

터널 어댑터 Teredo Tunneling Pseudo-Interface:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사. . . . . :
설명 . . . . . : Teredo Tunneling Pseudo-Interface
물리적 주소 . . . . . : 00-00-00-00-00-00-E0
DHCP 사용 . . . . . : 아니요
자동 구성 사용 . . . . . : 예

C:\Users\ASUS B150M-A>
```


● Tracing DNS with Wireshark

- ipconfig를 이용하여 DNS cache를 비운다.

```
C:\Users\WASUS B150M-A>ipconfig /flushdns

Windows IP 구성

DNS 확인자 캐시를 플러시했습니다.

C:\Users\WASUS B150M-A>
```

No.	Time	Source	Destination	Protocol	Length	Info
60	3.516881	192.168.55.225	210.220.163.82	DNS	72	Standard query 0x2b20 A www.ietf.org
61	3.527526	210.220.163.82	192.168.55.225	DNS	149	Standard query response 0x2b20 A www.ietf.org CNAME www.ietf.org
1519	8.065796	192.168.55.225	210.220.163.82	DNS	80	Standard query 0x1a28 A event.shelljacket.us
1520	8.071798	210.220.163.82	192.168.55.225	DNS	112	Standard query response 0x1a28 A event.shelljacket.us A 52

▶ Internet Protocol Version 4, Src: 210.220.163.82, Dst: 192.168.55.225

▶ User Datagram Protocol, Src Port: 53, Dst Port: 54293

▲ Domain Name System (response)

Transaction ID: 0x2b20

▲ Flags: 0x8180 Standard query response, No error

- 1... .. = Response: Message is a response
- .000 0... .. = Opcode: Standard query (0)
-0.. = Authoritative: Server is not an authority for domain
-0. = Truncated: Message is not truncated
-1 = Recursion desired: Do query recursively
-1 = Recursion available: Server can do recursive queries
-0.. = Z: reserved (0)
-0. = Answer authenticated: Answer/authority portion was not authenticated by the server
-0 = Non-authenticated data: Unacceptable
-0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

▲ Queries

- ▶ www.ietf.org: type A, class IN

▲ Answers

- ▶ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
- ▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
- ▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85

[Request In: 60]

[Time: 0.010645000 seconds]

- response가 1이므로 응답하는 패킷이다.
- Truncated가 0이므로 응답이 길어서 잘린경우가 아님을 알 수 있다.
- Recursion Desired가 1이므로 재귀 쿼리를 사용한다.
- Reply code가 0이므로 에러가 없음을 알 수 있다.