컴퓨터망 과제
(2020 겨울계절)

고석주 교수님

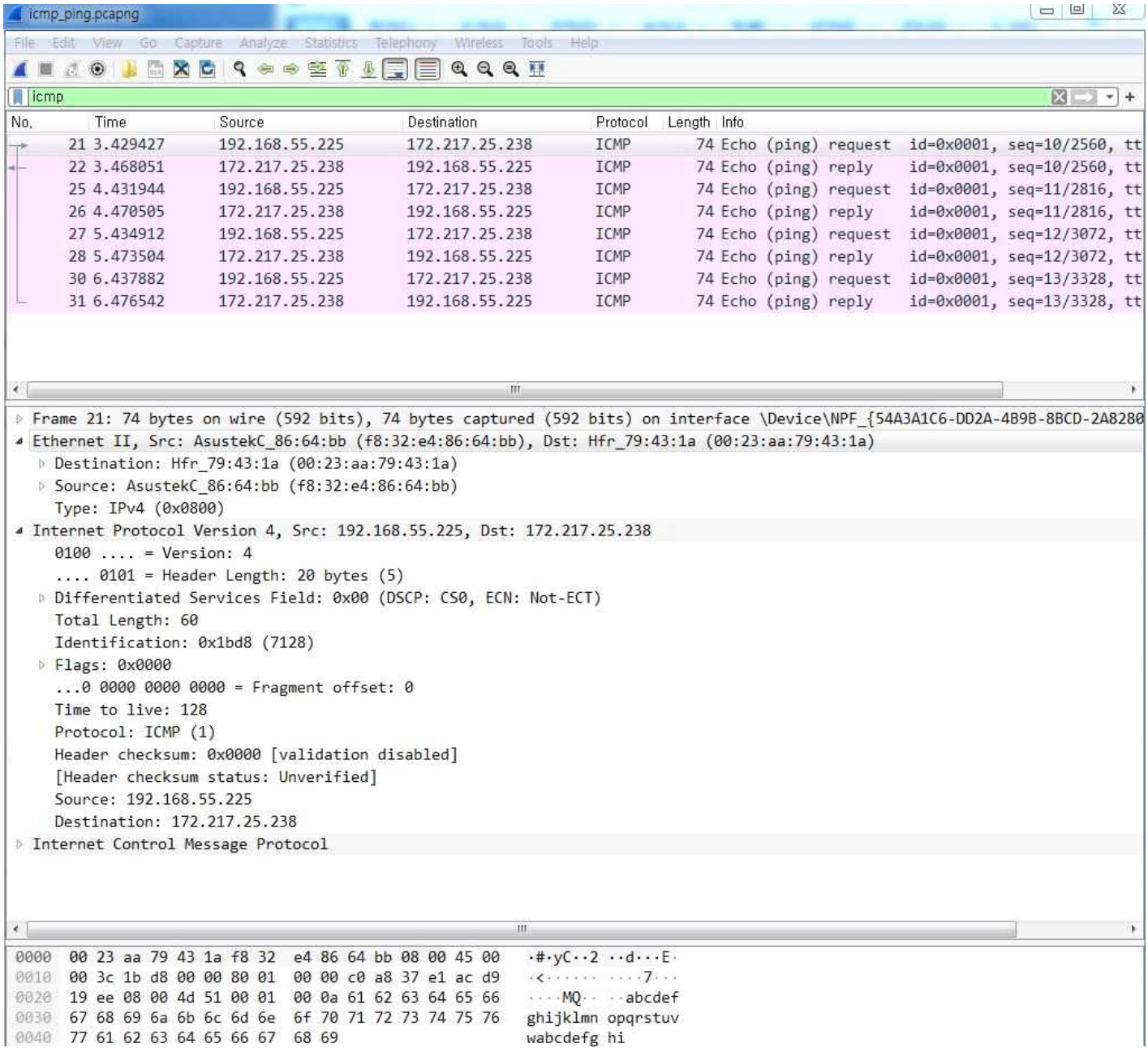
전자공학부
2014104276
이찬구

① ping(ICMP)

- 서버가 죽었는지 살았는지 확인할 때 사용

```
C:₩Users₩ASUS 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₩ASUS B150M-A>
```

● 내 컴퓨터 => 구글

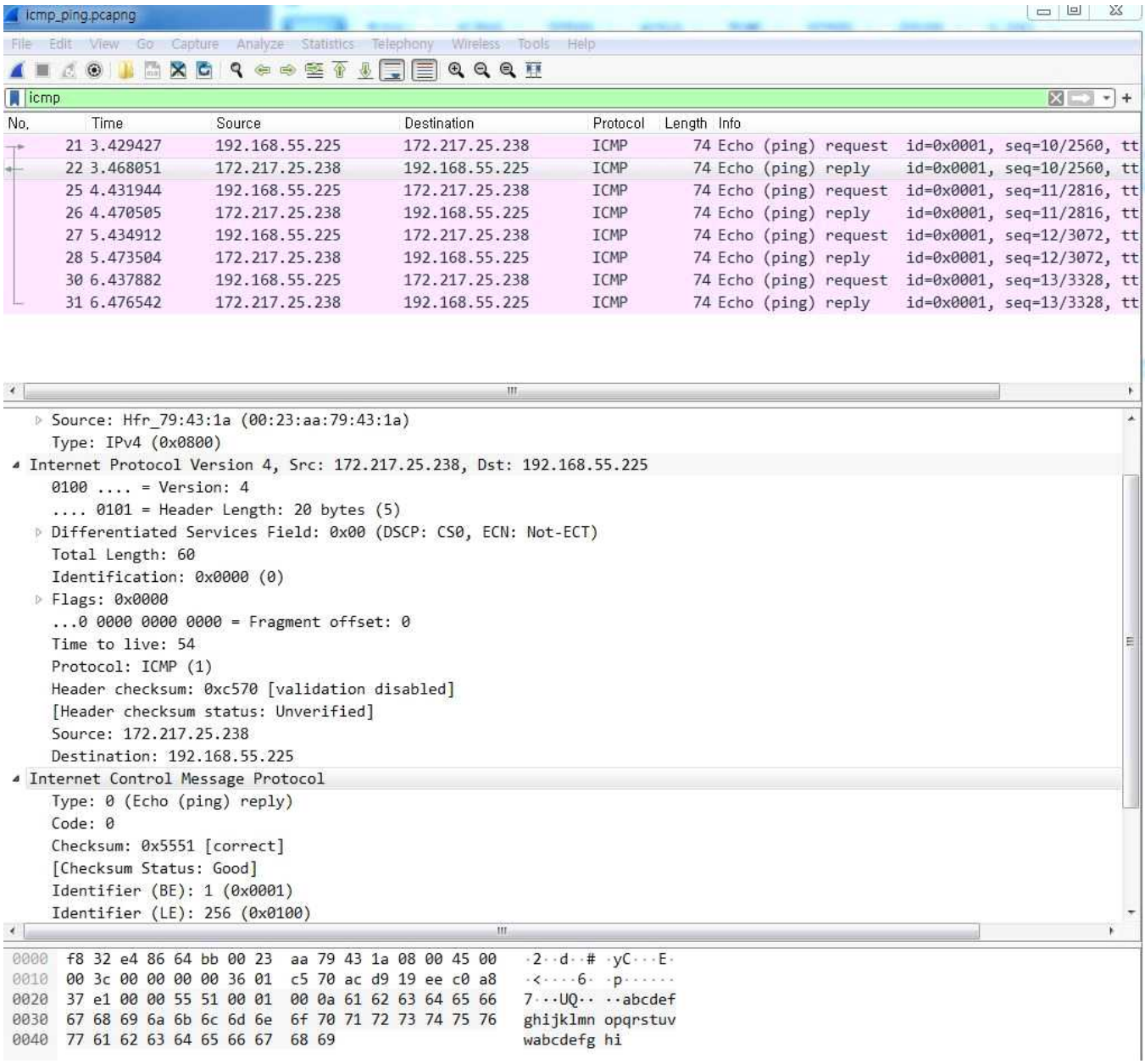


- 나의 IP address : 192.168.55.225
- google의 IP address 172.217.25.238

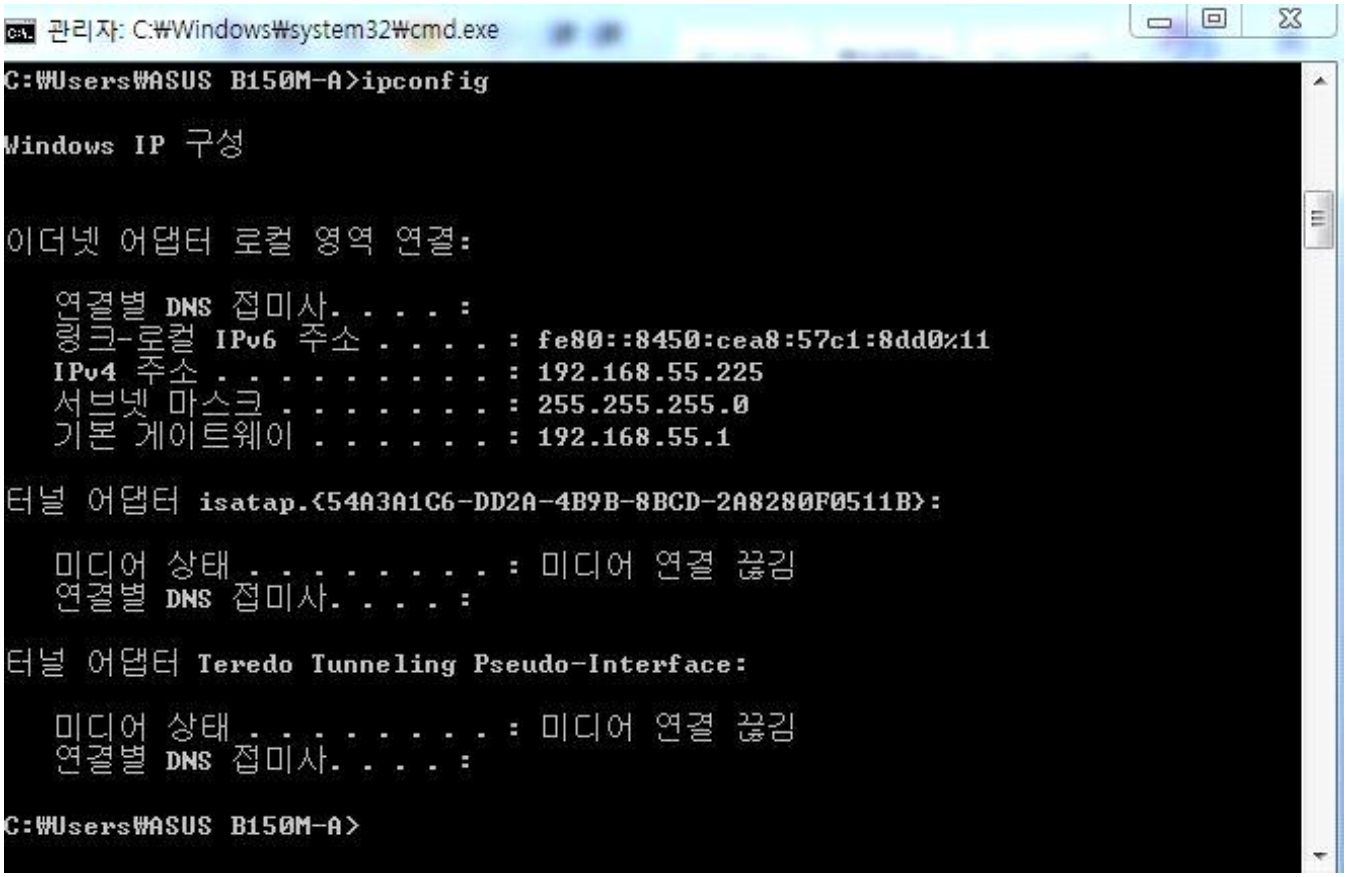
- 나의 IP와 구글의 IP가 네 번 핑을 주고받은 상태이다. (request – reply 응답이 네 번 있다)

- 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



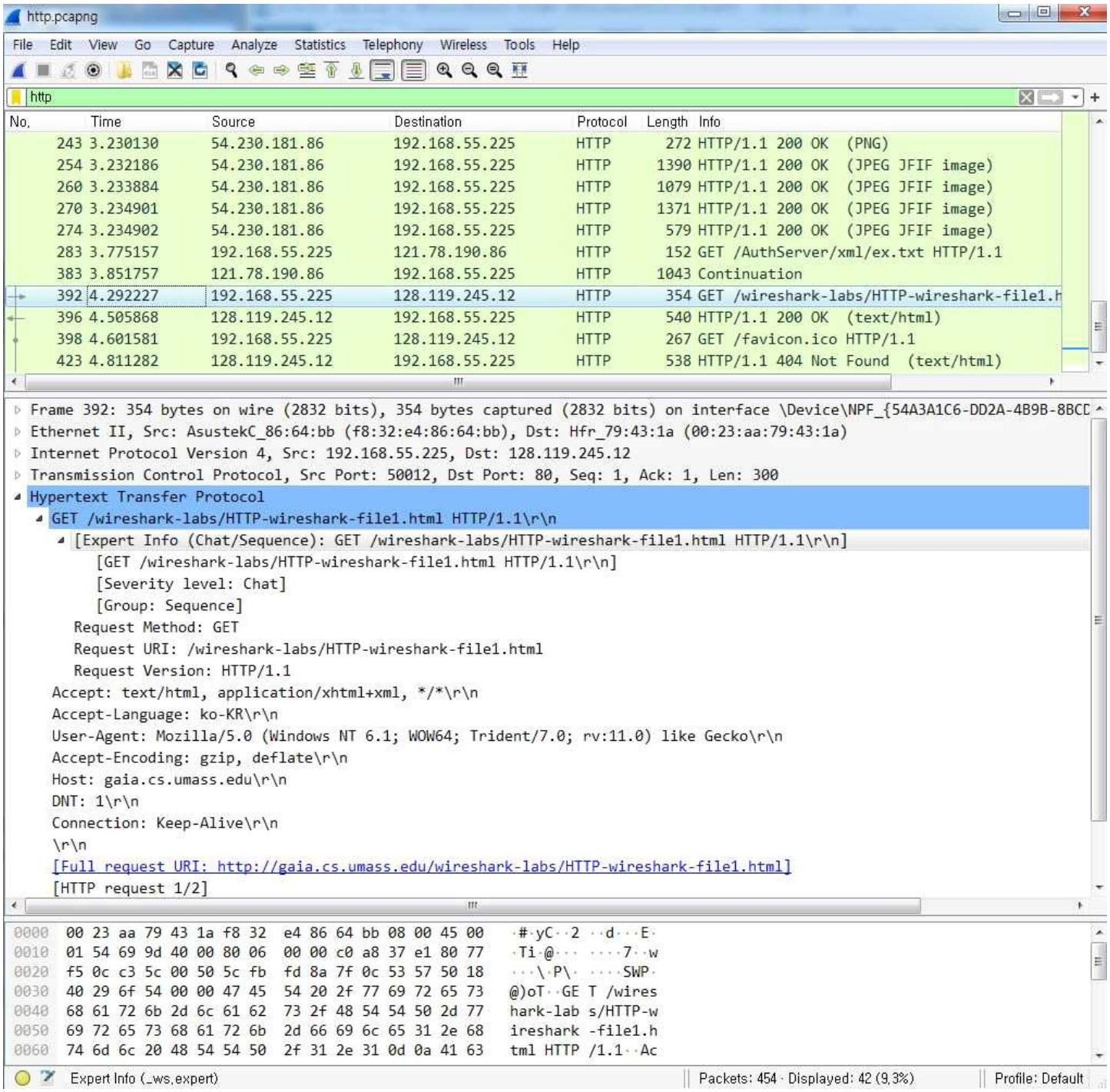
- IPv4를 사용하고 있다.
- Header length는 20bytes이다. IP 헤더의 크기를 의미한다.
- Service는 0x00(기본서비스)를 사용하고 있다.
- Total length는 60bytes이다.(데이터와 헤더를 모두 포함한 길이)
- TTL(Time To Live)는 54이다. 54개의 라우터를 통과하면 소멸.
- 프로토콜은 ICMP이다.
- Header checksum을 사용하고 있다.(Header에 대해서만 체크)

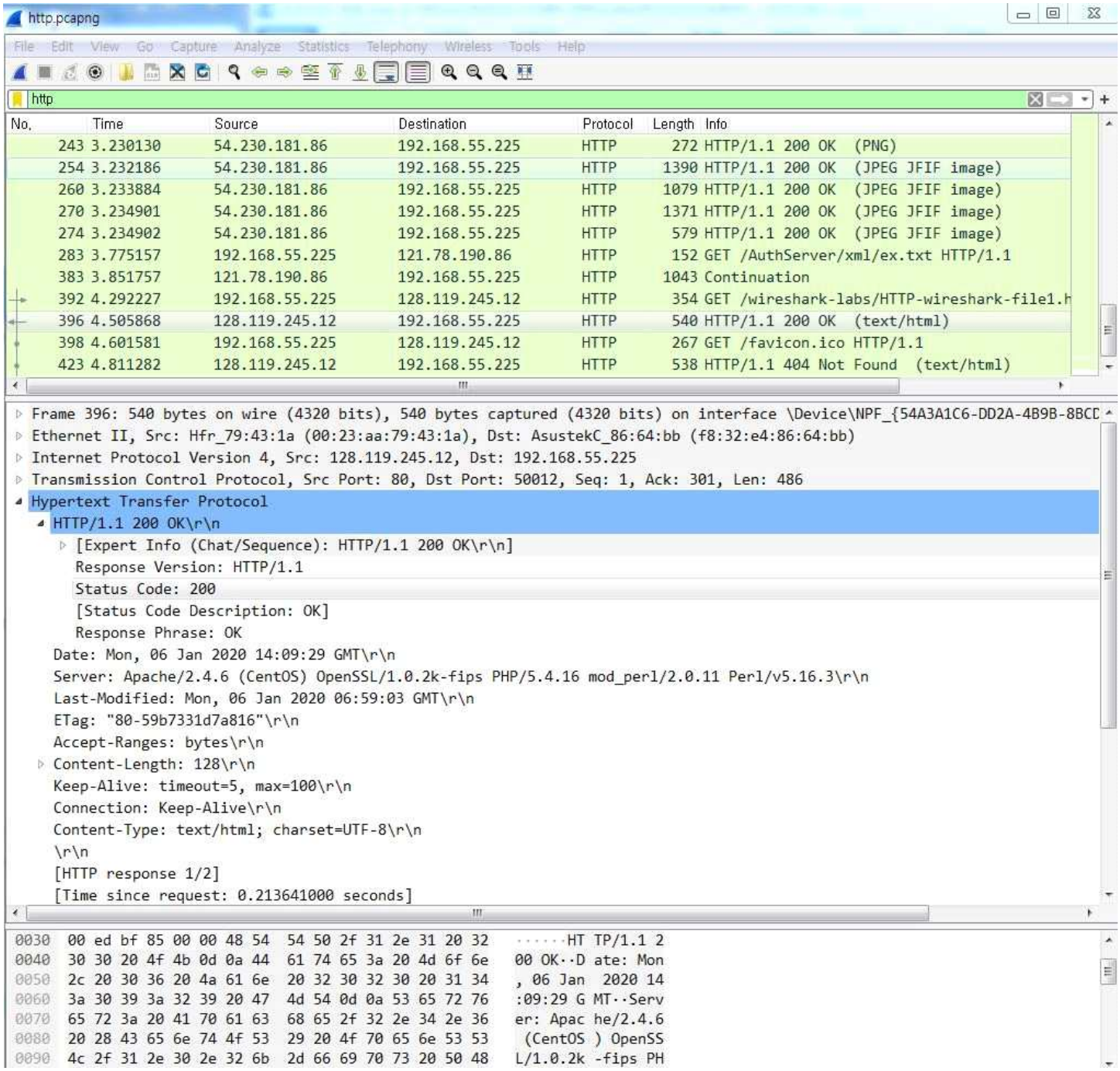


- ipconfig를 이용하여 나의 컴퓨터의 IP주소가 192.168.55.225임을 확인

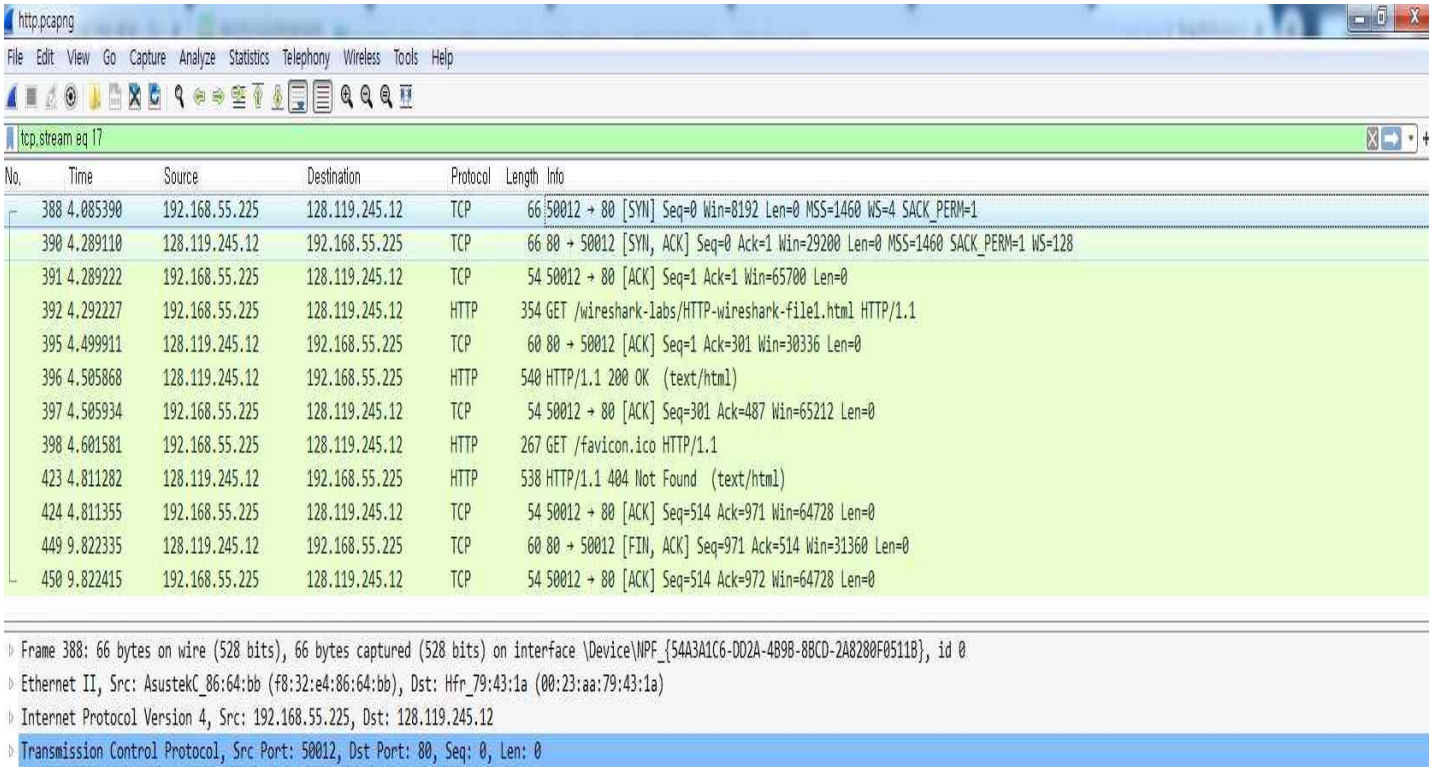
② website visit(TCP, HTTP)

1. The Basic HTTP GET/response interaction





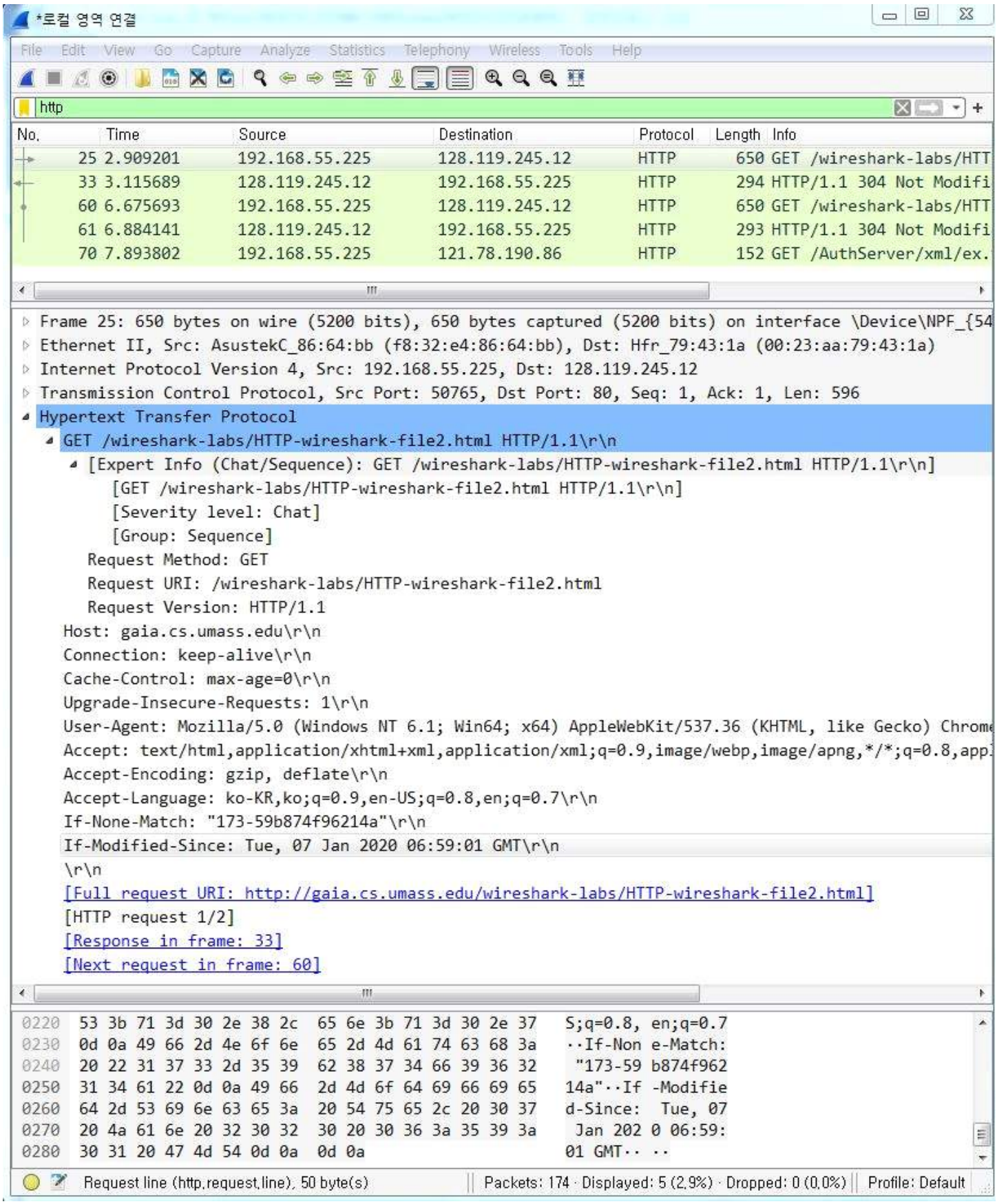
- 내 컴퓨터와 서버 모두 HTTP1.1을 사용중
- Accept-Ranges는 bytes이다.
- 내 컴퓨터의 IP address는 192.168.55.225, gaia.cs.umass.edu 서버의 IP address는 128.119.245.12
- Status code는 200이다.(응답이 정상이라는 의미)
- 2020년 1월 6일 06:59:03에 HTML파일이 서버에서 마지막으로 수정되었다.
- content-Length는 128이다.

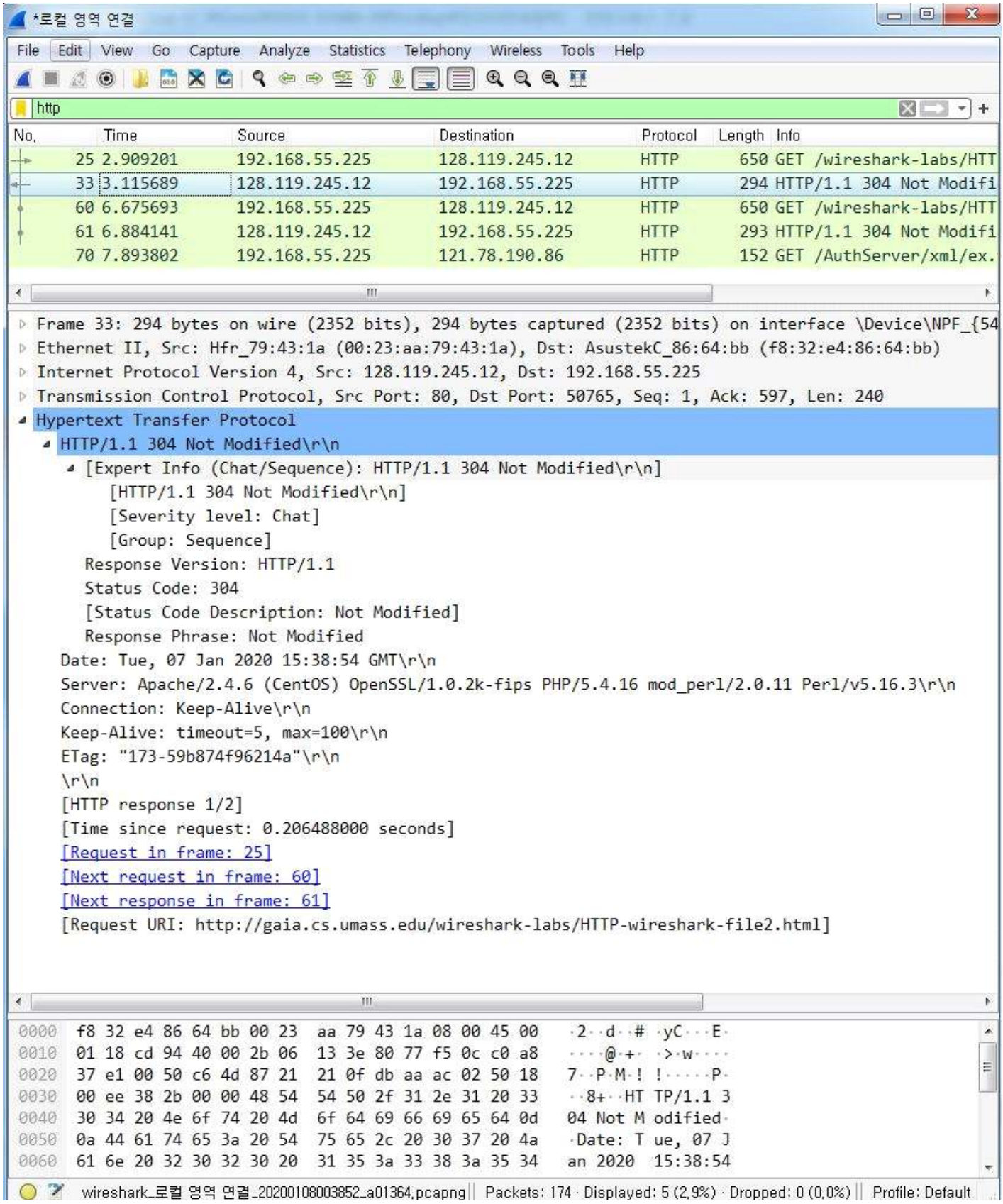


- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK (3-way Handshake과정)순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 연결이 완료 된 후 클라이언트 컴퓨터는 GET 방식으로 HTTP를 요청한다.
- seq는 보내는 데이터가 몇 번부터 시작을 하는지를 의미하며 ack은 내가 그다음 받아야하는 데이터가 어디인지에 대한 정보가 포함되어있다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.
- port 80은 well-know port number로써 서버를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

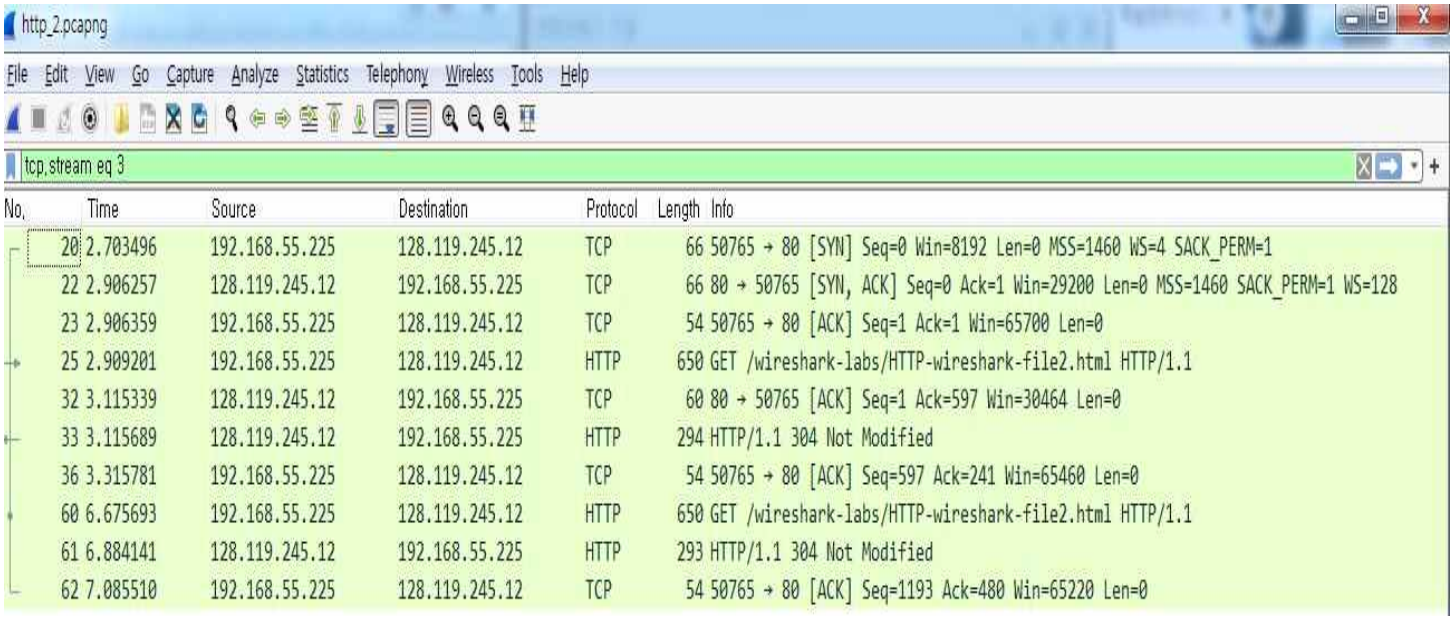
2. The HTTP CONDITIONAL GET/response interaction

● first



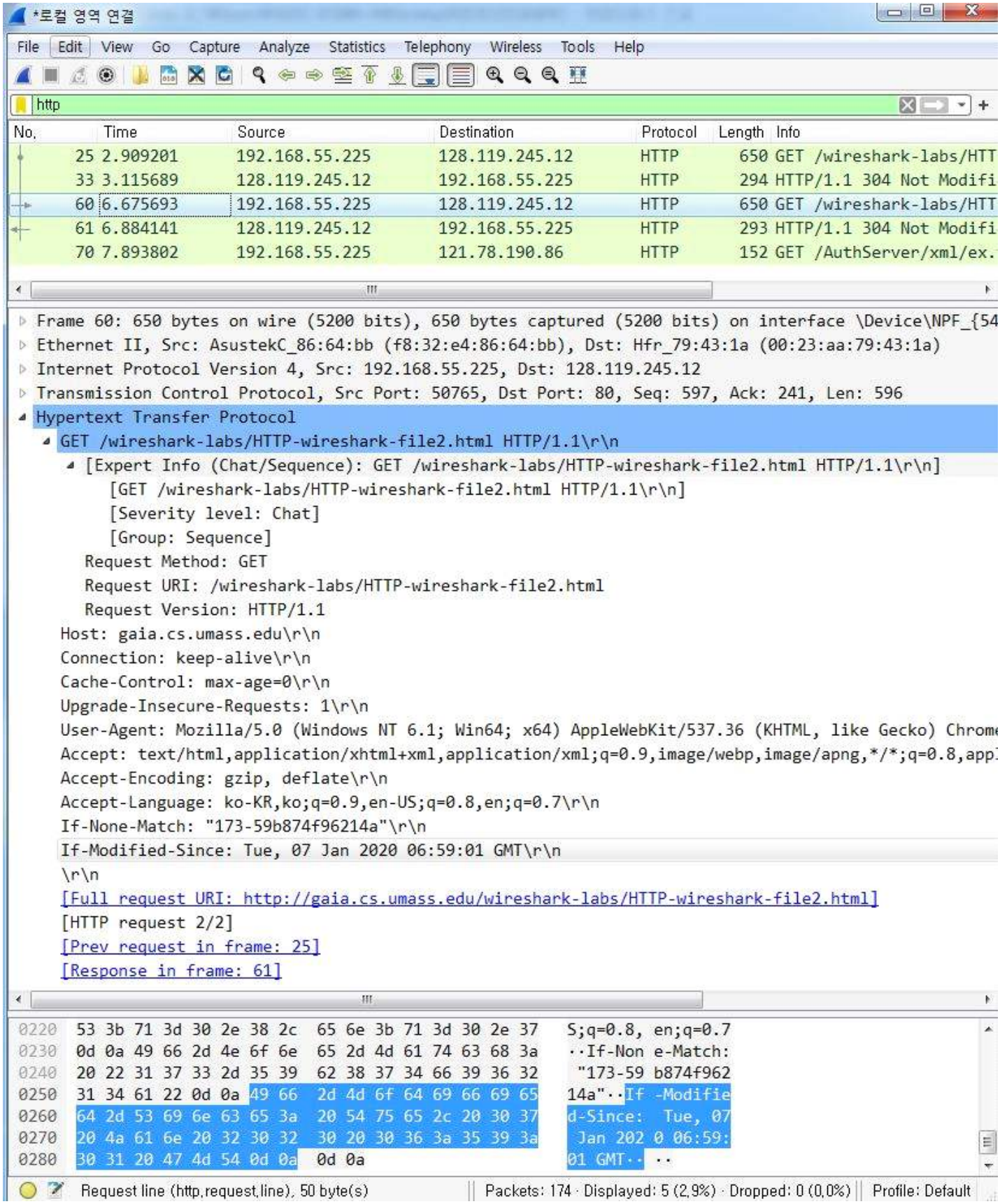


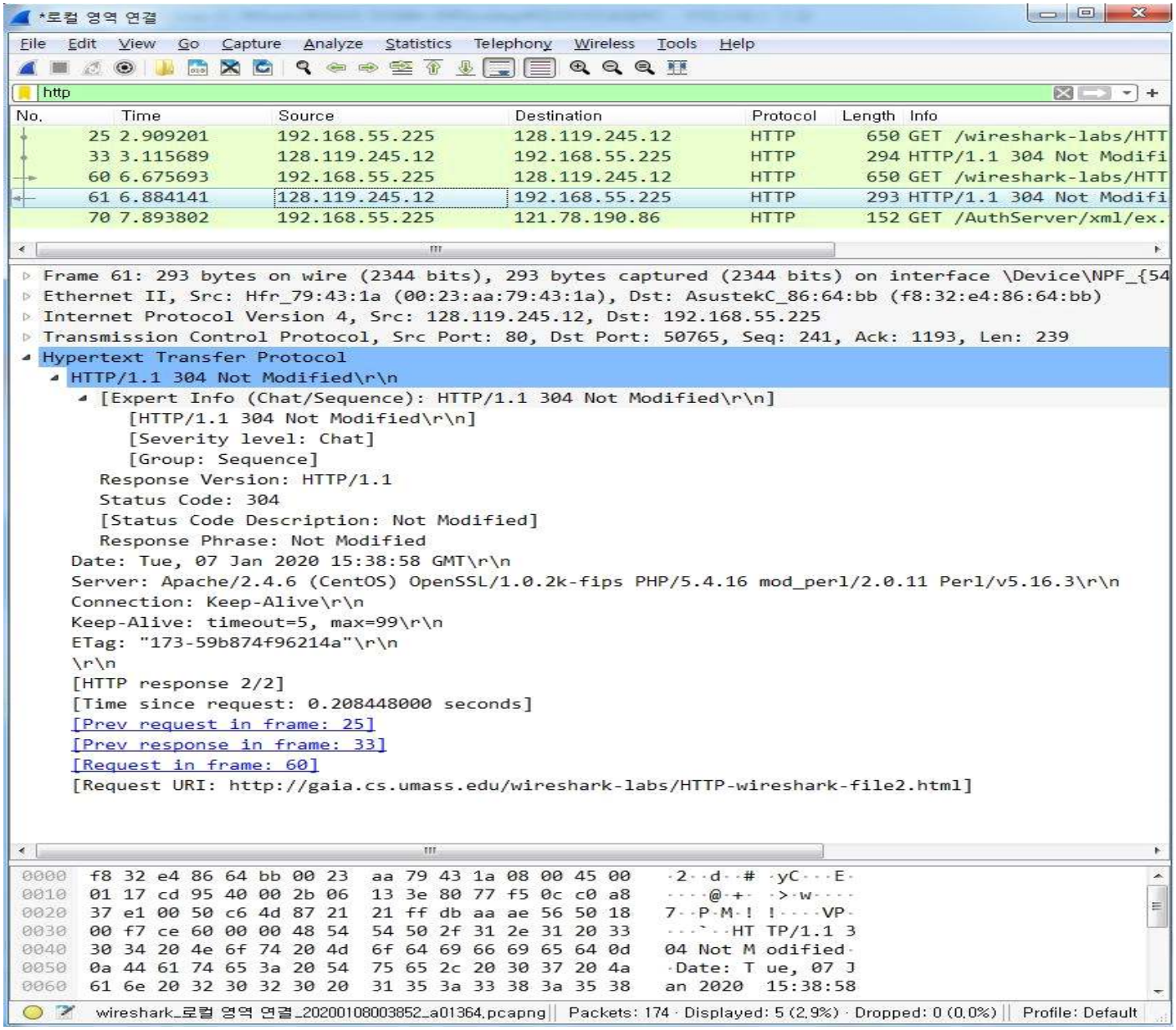
- If-Modified-Since: 2020년 1월 7일 화요일

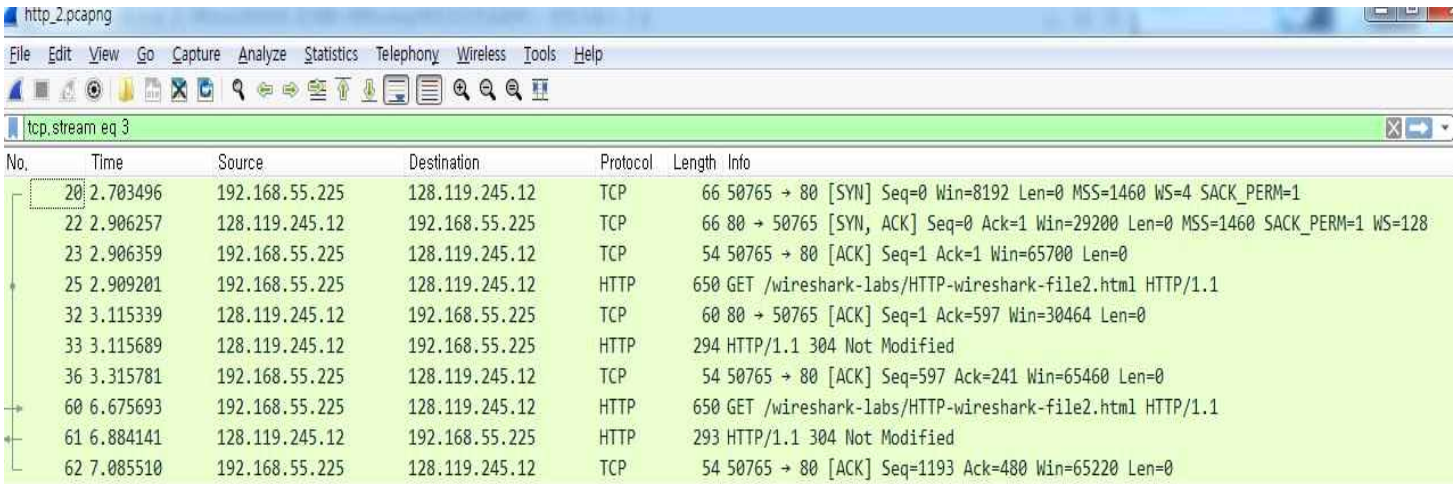


- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK 순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.

● Second

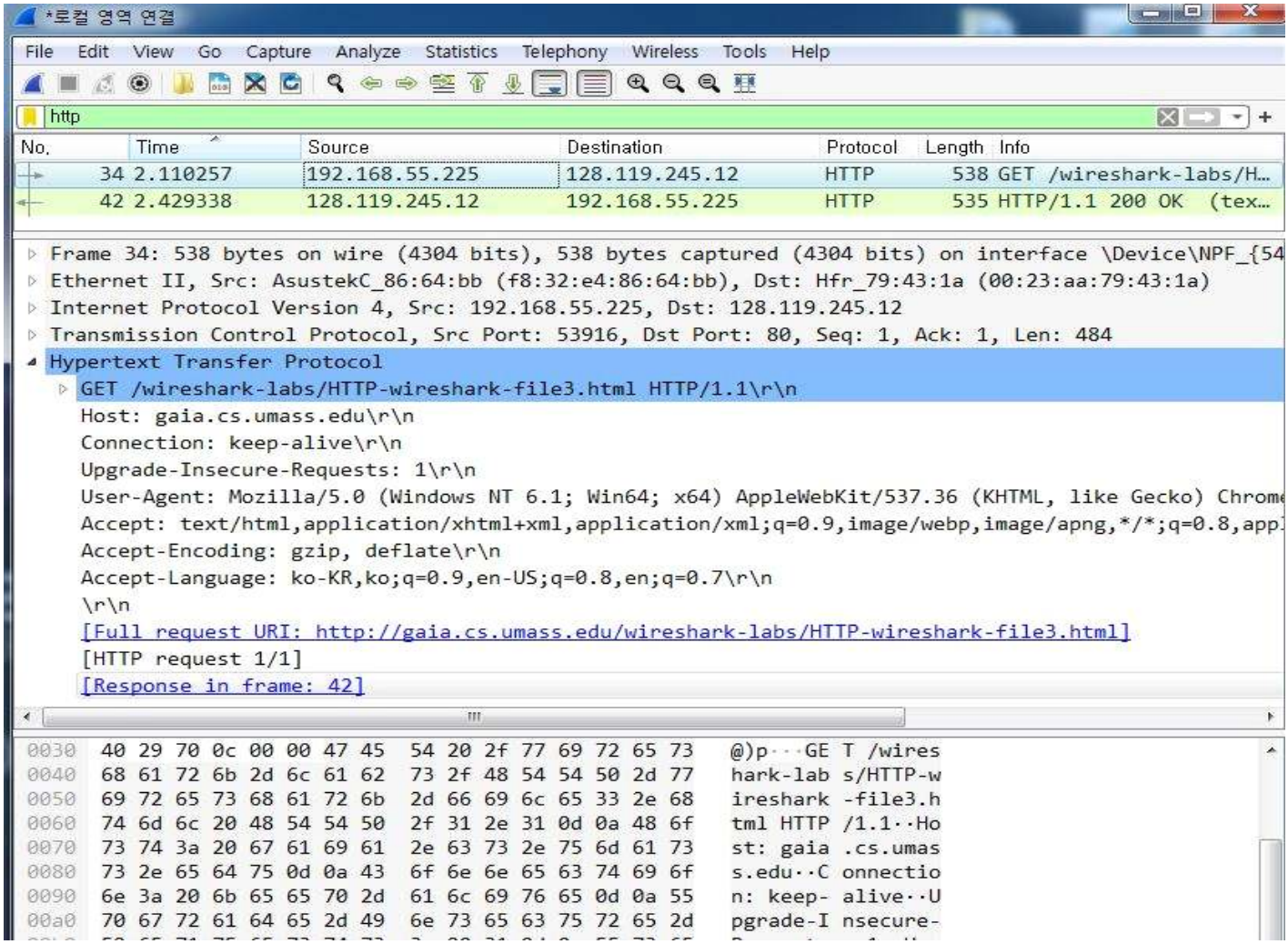

*로컬 영역 연결
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
25 2.909201 192.168.55.225 128.119.245.12 HTTP 650 GET /wireshark-labs/HTT
33 3.115689 128.119.245.12 192.168.55.225 HTTP 294 HTTP/1.1 304 Not Modifi
60 6.675693 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) Chrom
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

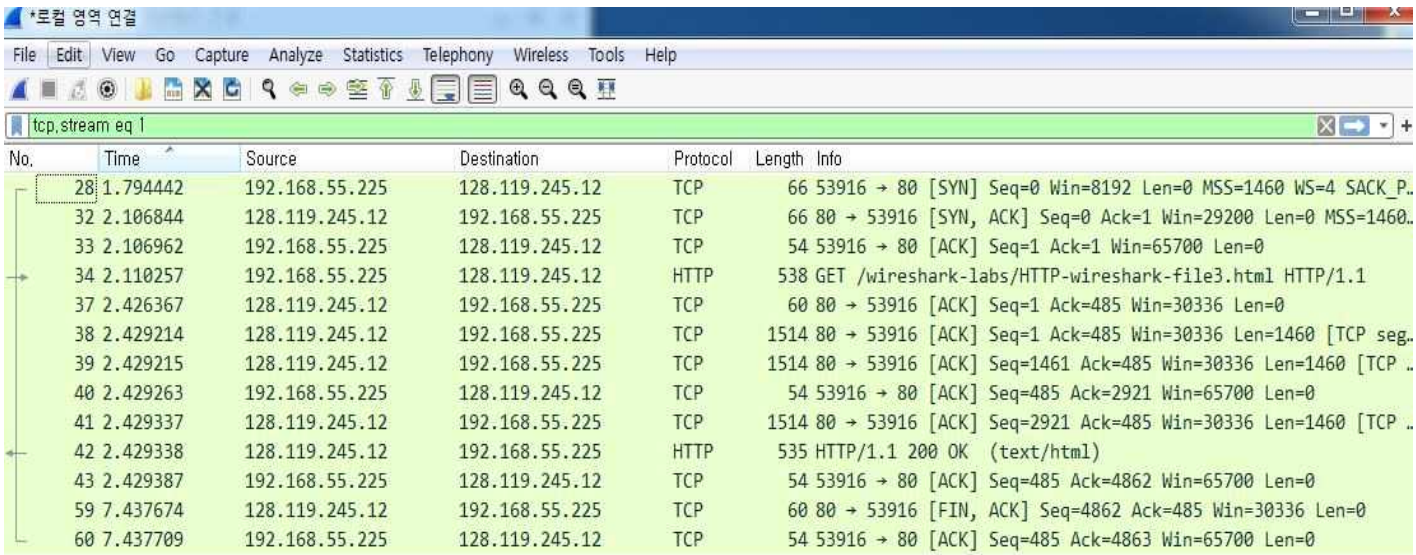




- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK 순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.

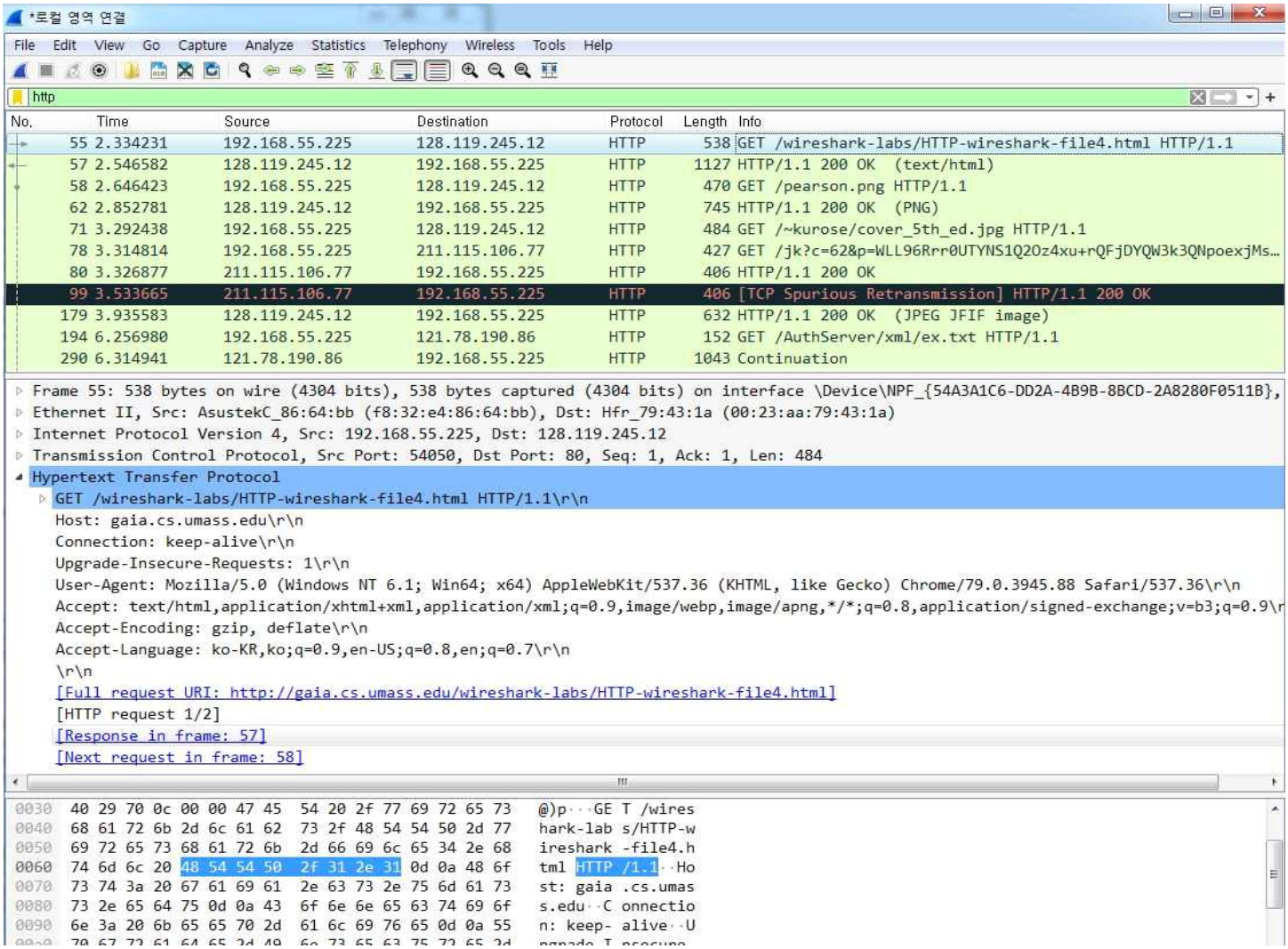
3. Retrieving Long Documents

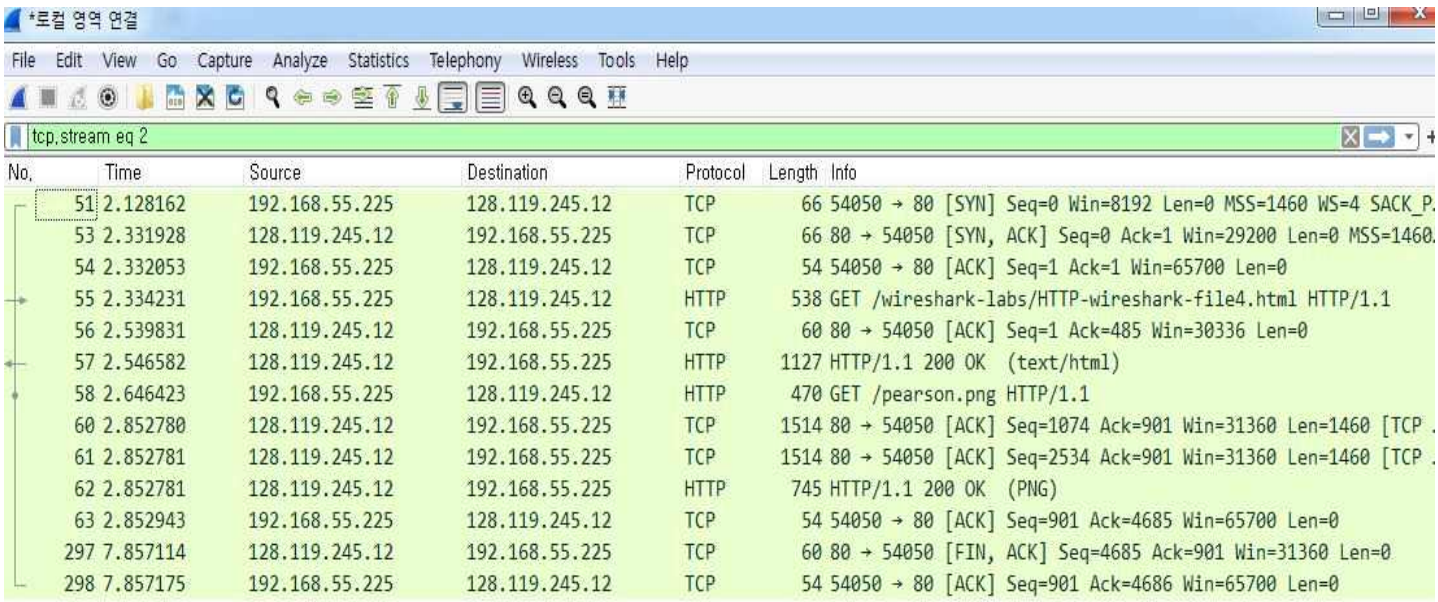




- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK 순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.

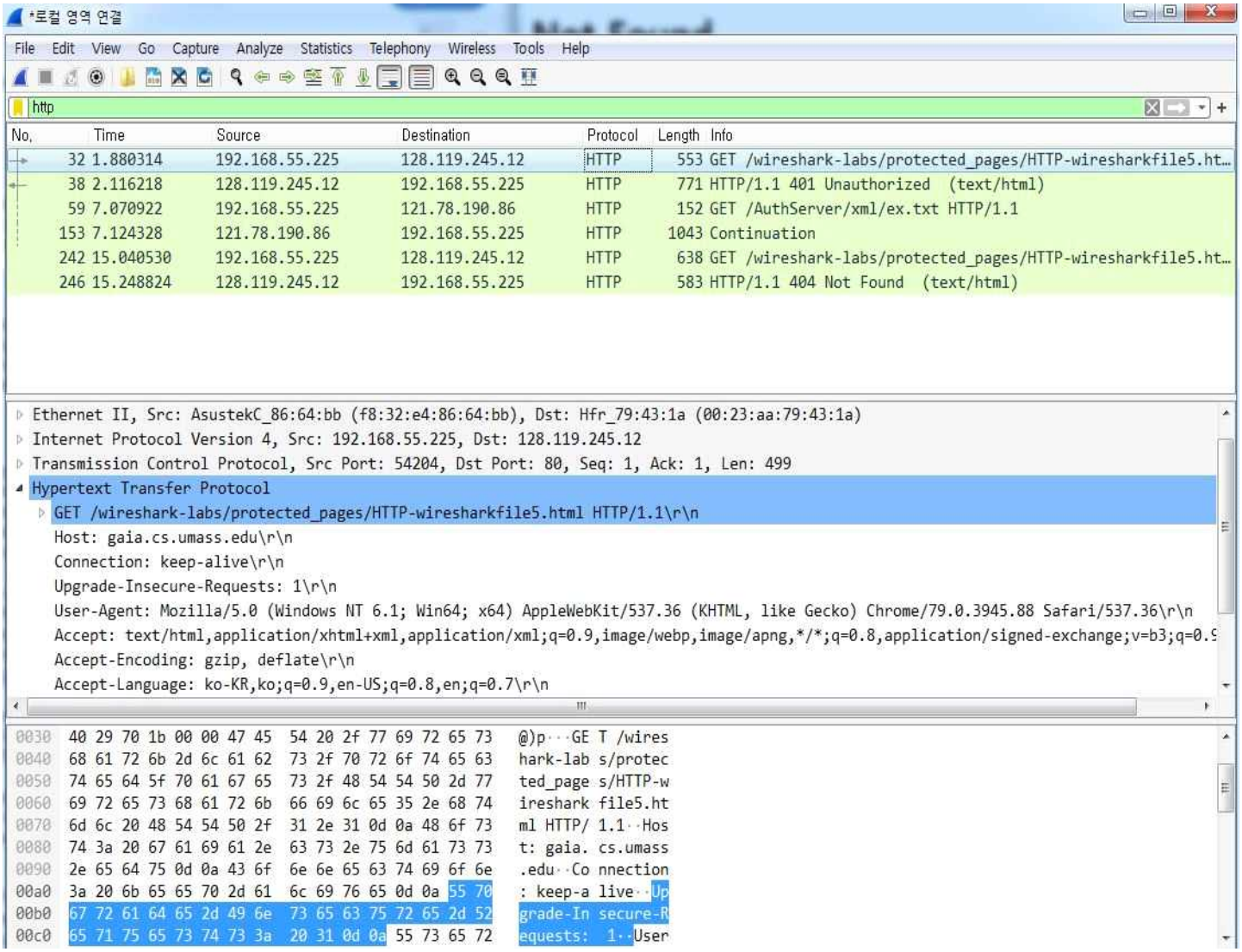
4. HTML Documents with Embedded Objects



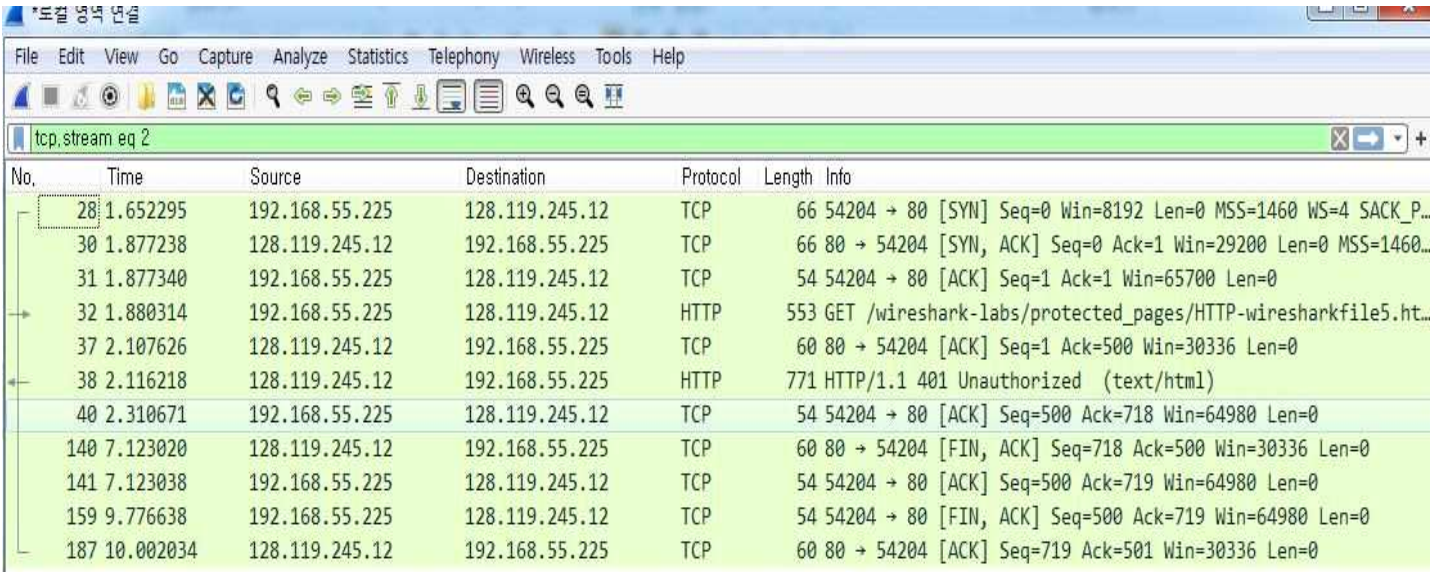


- 데이터를 주고받기 전에 SYN -> SYN,ACK -> ACK 순서로 신호를 주고 받아서 connection준비를 완료하였다.
- 데이터를 모두 주고받은 다음에는 FIN,ACK -> ACK 순서로 진행되었다.

5 HTTP Authentication

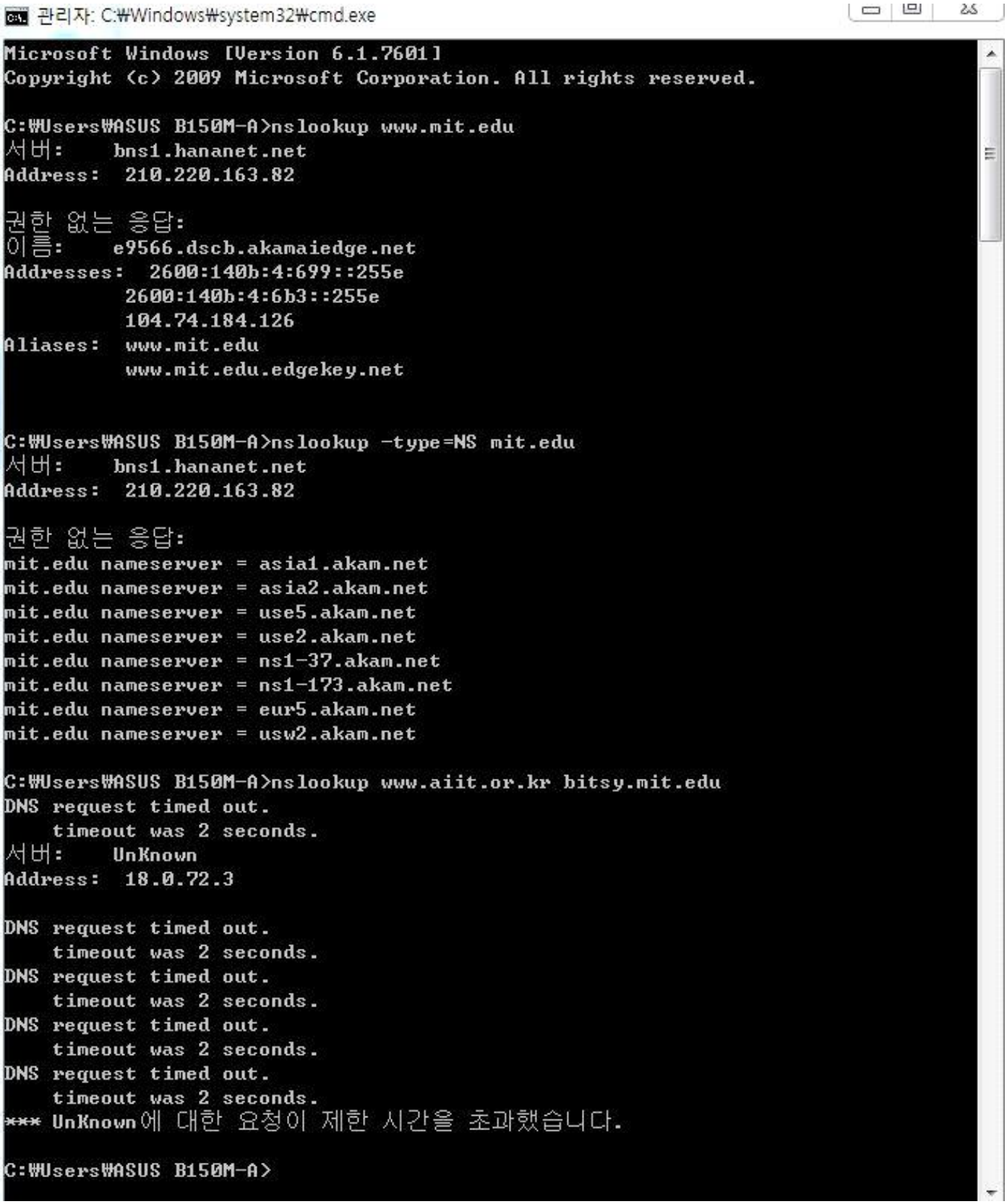


- 알맞게 네임과 비밀번호를 입력하였지만 Unauthorized 되었다.



③ nslookup(DNS)

● nslookup을 이용하여 도메인의 ip주소를 찾을수 있다.



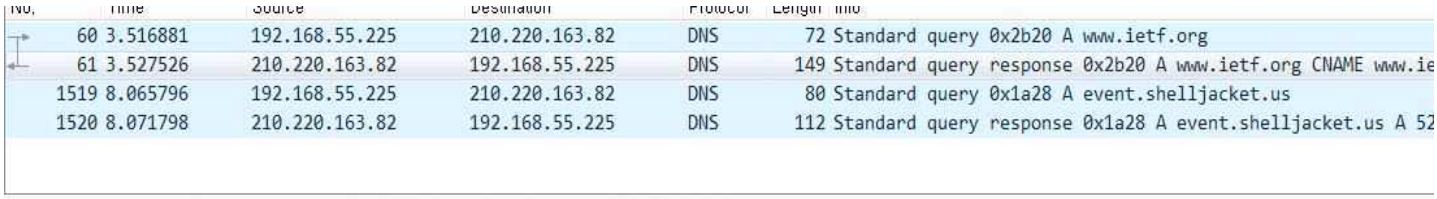
● ipconfig


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 . . . . . : 00-00-00-00-00-00-00-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 . . . . . : 00-00-00-00-00-00-00-E0
DHCP 사용 . . . . . : 아니요
자동 구성 사용. . . . . : 예
C:₩Users₩ASUS B150M-A>

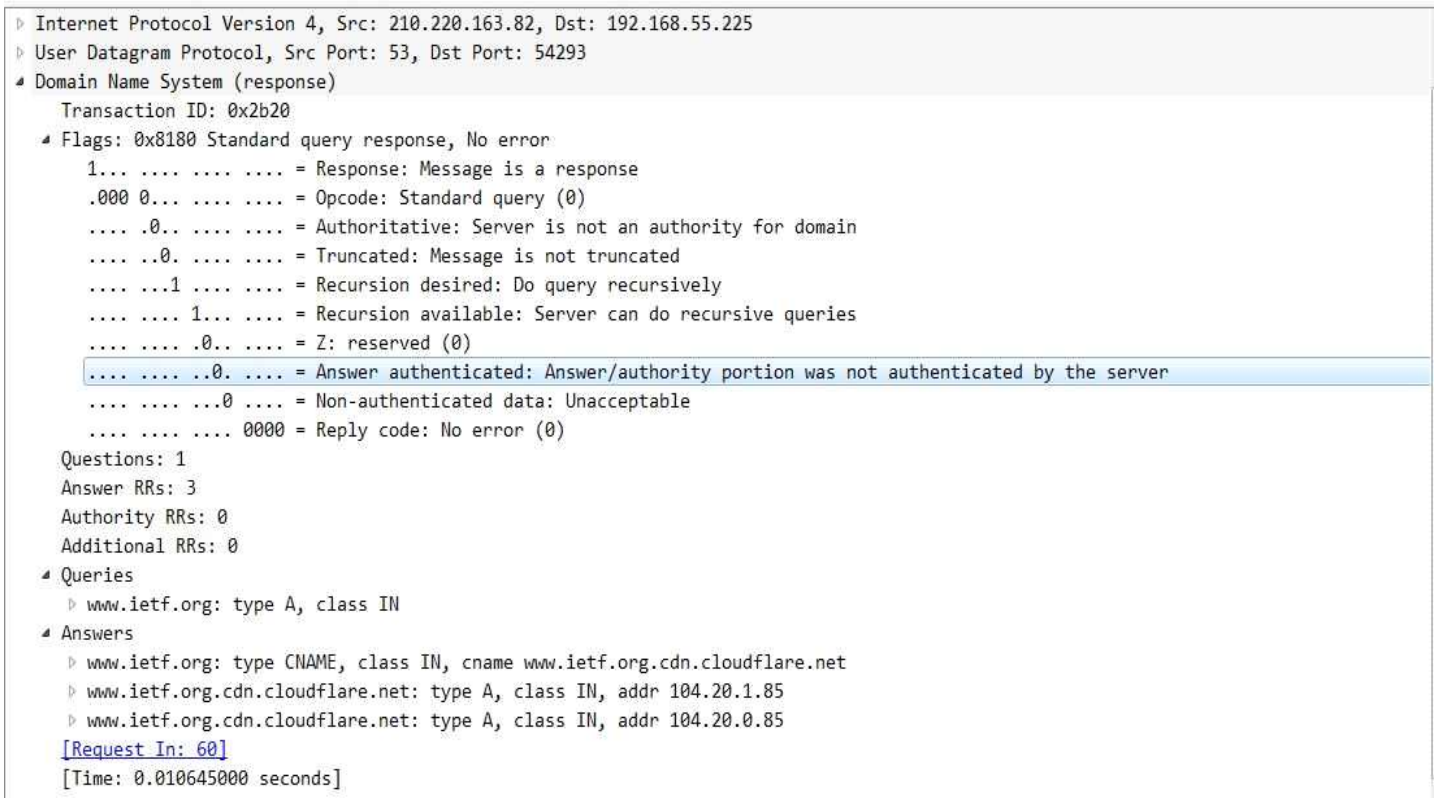
● Tracing DNS with Wireshark

- ipconfig를 이용하여 DNS cache를 비운다.

```
C:₩Users₩ASUS B150M-A>ipconfig /flushdns

Windows IP 구성

DNS 확인자 캐시를 플러시했습니다.

C:₩Users₩ASUS 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.ie
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.
- Recurison Desired가 1이므로 재귀 쿼리를 사용한다.
- Reply code가 0이므로 에러가 없음을 알 수 있다.