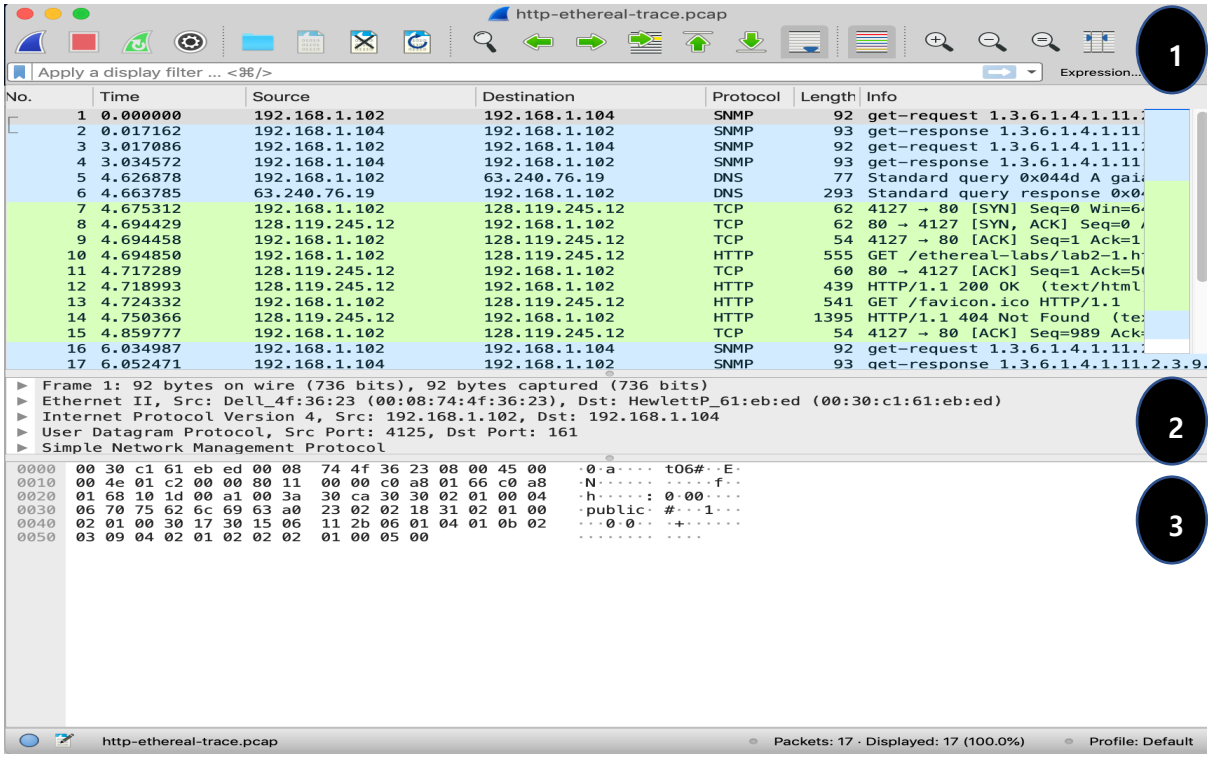
<GBC - Network #HW1>

21800758 최 하영

0.Analysis



[구성]

1) Packet List - 수집된 패킷들의 목록

2) Packet Detail - 해당 패킷의 정보

3) Packet Bytes - 패킷의 정보를 바이트로 표현

[메뉴]

No (packet number)

Time (수집된 시간)

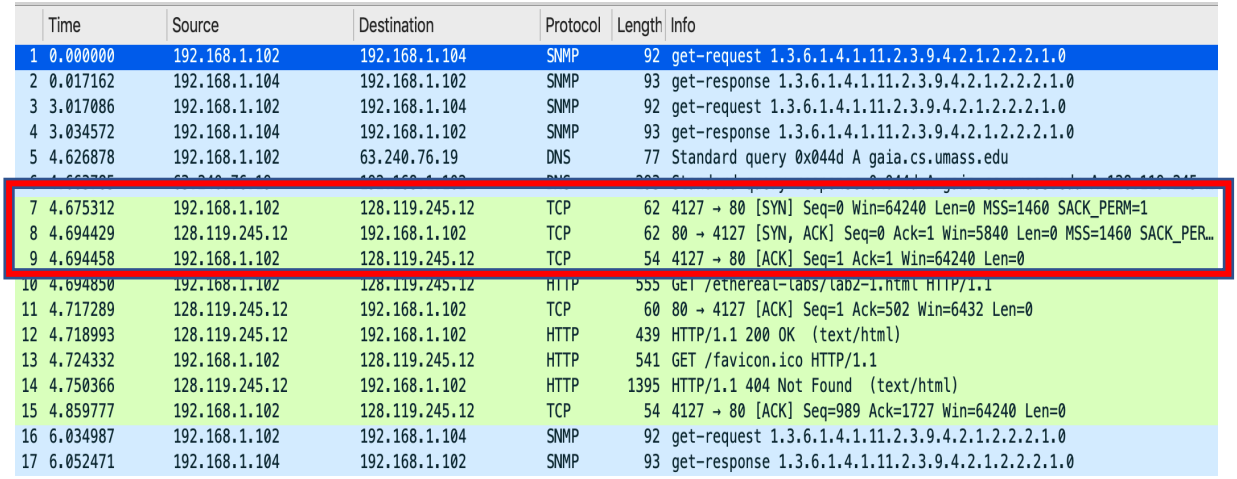
Source (출발지 주소)

Destination (도착지 주소)

Protocol (프로토콜)

Length(길이)

Info(목록)



	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.017162	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
3	3.017086	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
4	3.034572	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
5	4.626878	192.168.1.102	63.240.76.19	DNS	77	Standard query 0x044d A gaia.cs.umass.edu
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PER…
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
16	6.034987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

→ 통신 전의 클라이언트는 포트가 closed 상태이며, 서버는 해당 포트로 항상 서비스를 제공할 수 있는 listen 상태.

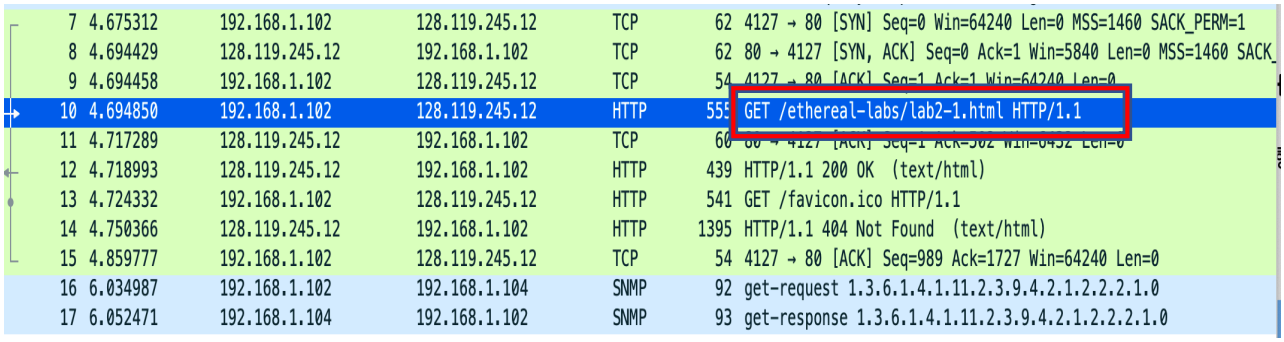
1 단계) 클라이언트가 통신을 하고자 하면, 임의의 포트번호(4127)를 클라이언트 브라우저에 할당하고, 클라이언트는 이 포트번호(4127)를 포함한 SYN 을 서버에 전송함.

2 단계) 서버는 클라이언트의 SYN 요청을 받고 SYN Received 상태
클라이언트에게 연결을 허용한다는 의미의 [SYN, ACK]패킷 전송

3 단계) 클라이언트는 연결 요청에 대한 서버의 응답을 확인했다는 의미로 ACK 패킷을 서버에게 전송 → 클라이언트와 서버가 연결이 성립되어 정상적으로 패킷을 주고받을 수 있는 상태가 됨.

1. Is the browser of a client computer running HTTP version 1.0 or 1.1?
What version of HTTP is the server running?

→ 클라이언트 브라우저는 HTTP 1.1 을 실행하고 있고, 서버에서 실행중인 HTTP 버전 또한 1.1

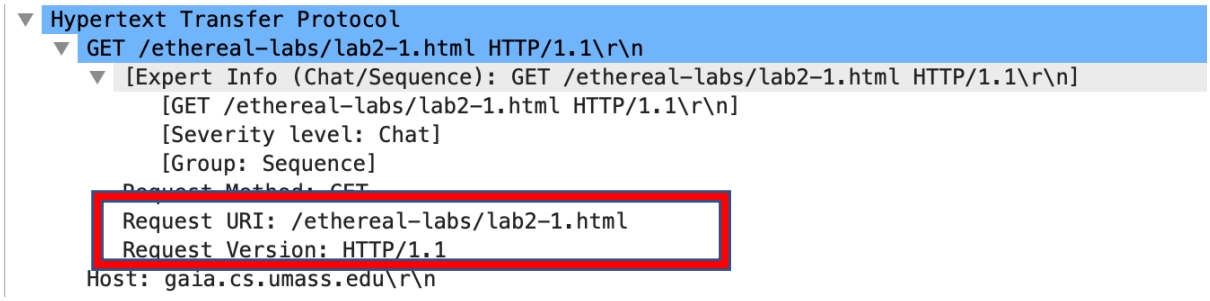


7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
16	6.034987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

→ 클라이언트 : GET 메소드 이용하여 HTTP 1.1 프로토콜로 해당 html (웹페이지 문서) 요청

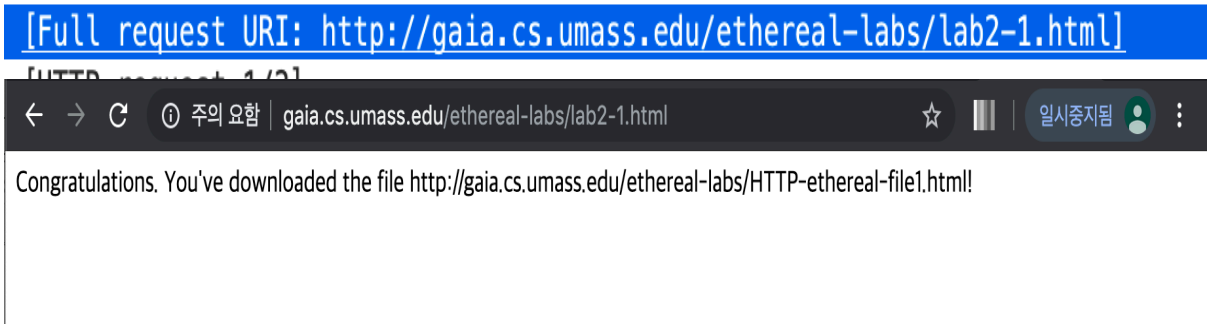
→ Request Version : HTTP/1.1 (홈페이지 가져올 때 HTTP 1.1 버전 사용)

→ Request URI : /ethereal-labs/lab2-1.html (가져오고 싶은 파일의 주소)



```
▼ Hypertext Transfer Protocol
  ▼ GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n]
        [GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /ethereal-labs/lab2-1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
```

→ Full request URI(요청하는 주소)도 다음과 같이 확인 할 수 있으며, 접속 시 아래와 같이 나온다.



```
[Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-1.html]
[HTTP request 1/2]
```

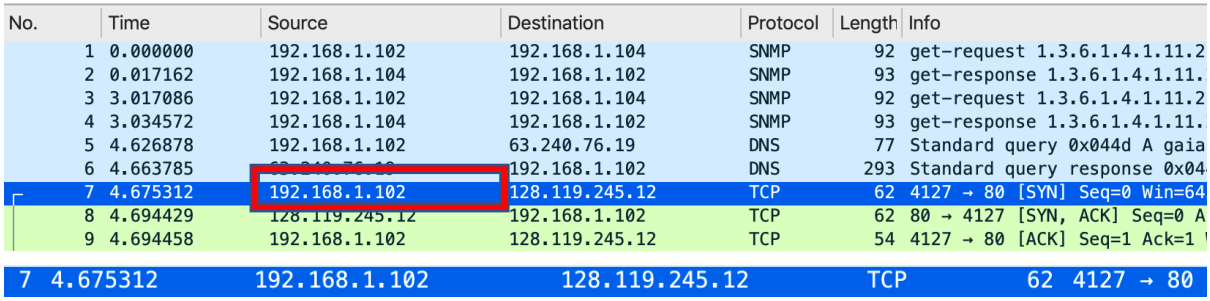

주의 요함 | gaia.cs.umass.edu/ethereal-labs/lab2-1.html

일시중지됨

Congratulations. You've downloaded the file http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html!

2. What is the IP address of the client computer?

→ 192.168.1.102



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2
2	0.017162	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.
3	3.017086	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2
4	3.034572	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.
5	4.626878	192.168.1.102	63.240.76.19	DNS	77	Standard query 0x044d A gaia
6	4.663785	63.240.76.19	192.168.1.102	DNS	293	Standard query response 0x04
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 A
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1

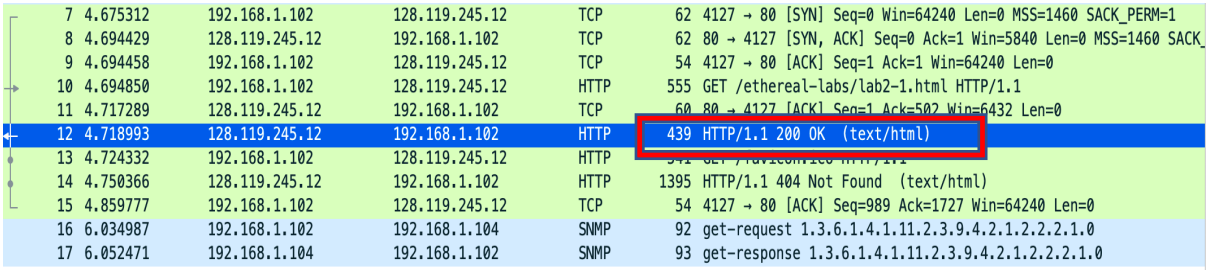
```
7  4.675312    192.168.1.102    128.119.245.12    TCP    62  4127 → 80
```

(서비스를 요청하는 쪽이 클라이언트 / 서버 : 80 번 포트 / 서버 IP : 128.119.245.12)

+) 80 번 포트 : 웹 서버나 HTTPD 에서 웹 클라이언트로부터 요구가 들어오기를 기대하는 포트

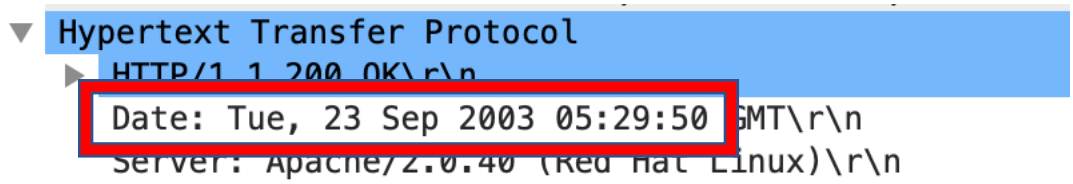
3. When was the HTML file that the client is retrieving last modified at the server? (for the first request)

> 첫번째 요청인지 검토 후, 해당 패킷 정보를 확인한다.



7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP		
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
16	6.034987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

→ Tue, 23 Sep 2003 05:29:50



4. How many bytes of content are being returned to the client browser for the first HTTP GET?

> 첫번째 HTTP GET 의 세부 정보에서 확인할 수 있다.

→ 73 byte