

<GBC - Network #HW1>

21800758 최 하영

0. Analysis

1

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	0.017162	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11...
3	0.017086	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11...
4	0.034572	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 gai...
6	4.663785	63.240.76.19	192.168.1.102	DNS	293	Standard query response 0x0...
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=6...
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 /...
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1...
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.h...
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=5...
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 (te...
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack...
16	6.034987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11...
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...

2

3

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettP_61:eb:ed (00:30:c1:61:eb:ed)
▶ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
▶ User Datagram Protocol, Src Port: 4125, Dst Port: 161
▶ Simple Network Management Protocol

0000 00 30 c1 61 eb ed 00 08 74 4f 36 23 00 00 45 00 .0.a...t06#..E.
0010 00 4e 01 c2 00 00 80 11 00 00 c0 a8 01 66 c0 a8 .N.....f..
0020 01 68 10 1d 00 a1 00 3a 30 ca 30 30 02 01 00 04 .h.....:0.00..
0030 06 70 75 62 6c 69 63 a0 23 02 02 18 31 02 01 00 .public.#...1..
0040 02 01 00 30 17 30 15 06 11 2b 06 01 04 01 0b 02 ...0.0...+.....
0050 03 09 04 02 01 02 02 02 01 00 05 00
.....

http-ethereal-trace.pcap Packets: 17 · Displayed: 17 (100.0%) Profile: Default

[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
6	4.653385	63.240.76.19	192.168.1.102	DNS	88	Standard query response 0x044d A 63.240.76.19
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_PERM=1
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 /ethercat-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 포트에 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 1.1을 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_PERM=1
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	559	GET /etherreal-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=302 Win=0 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 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0

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

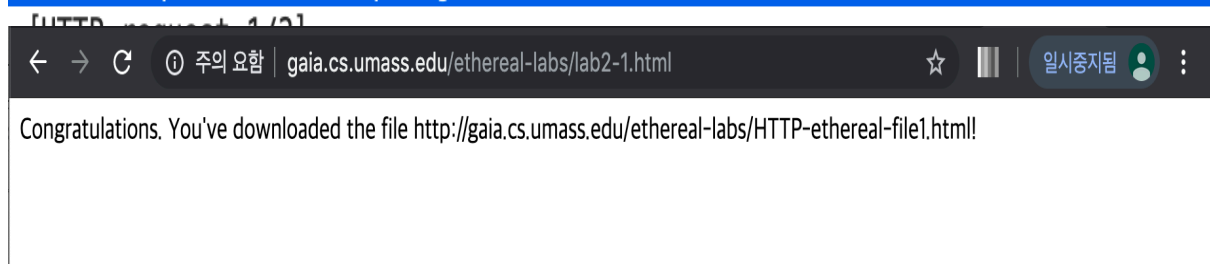
→ Request Version : HTTP/1.1 (홈페이지 가져올 때 HTTP 1.1 버전 사용)

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

▼ Hypertext Transfer Protocol
▼ GET /etherreal-labs/lab2-1.html HTTP/1.1\r\n
▼ [Expert Info (Chat/Sequence): GET /etherreal-labs/lab2-1.html HTTP/1.1\r\n]
[GET /etherreal-labs/lab2-1.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /etherreal-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/etherreal-labs/lab2-1.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	192.168.1.102	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

(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	542	GET /lab2-1.html 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 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.1.0

→ Tue, 23 Sep 2003 05:29:50

▼ Hypertext Transfer Protocol

▶ HTTP/1.1 200 OK\r\n

Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
Server: Apache/2.0.40 (Red Hat Linux)\r\n

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

▼ 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: Tue, 23 Sep 2003 05:29:50 GMT\r\n

Server: Apache/2.0.40 (Red Hat Linux)\r\n

Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n

ETag: "1bfed-49-79d5bf00"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 73\r\n

[Content length: 73]

Accept-Ranges: bytes\r\n

▼ Content-Length: 73\r\n

[Content length: 73]