

4차 산업혁명과 함께하는 네트워크

네트워크 개론 3판

진혜진 지음



HTTP 서비스

02. 응용 계층 프로토콜 및 서비스

■ HTTP 서비스(TCP 포트: 80)

- HTTP는 클라이언트의 웹 브라우저가 서버에 웹 서비스를 요청하면 서버가 적절한 응답을 하여 클라이언트의 사용자에게 웹 페이지를 제공하는 서비스이다. 즉 HTTP는 서버와 클라이언트 간에 하이퍼텍스트 문서를 송수신하는 프로토콜이다. HTTP의 동작 과정을 살펴보자. 클라이언트는 접속하려는 웹 사이트의 URL이나 IP 주소를 알고 있어야 한다.
- 클라이언트는 웹 브라우저에 URL 주소(<http://www.hanb.co.kr>)를 입력하고, TCP 포트 번호 80을 이용하여 접속하려는 서버(한빛출판네트워크)에 연결을 시도한다. 그러면 클라이언트는 TCP 요청 소켓을 이용하여 URL 주소를 포함한 요청 메시지를 서버에 전송한다. 서버는 클라이언트의 요청 메시지에 응답하여 소켓을 통해 메시지를 전송하고 TCP 연결 설정을 해제한다.



그림 7-14 HTTP 요청과 응답

02. 응용 계층 프로토콜 및 서비스

- 클라이언트가 데이터를 요청할 때는 GET이라는 요청 정보, 파일 이름, 버전 등을 서버에 전송한다.
- 서버는 요청을 정상적으로 처리했다는 OK 정보를 응답으로 반환한다.
- HTTP 1.0에서는 전송받을 문서에 이미지가 있으면 문서를 받을 때와 이미지를 받을 때 각각 연결을 설정한다.

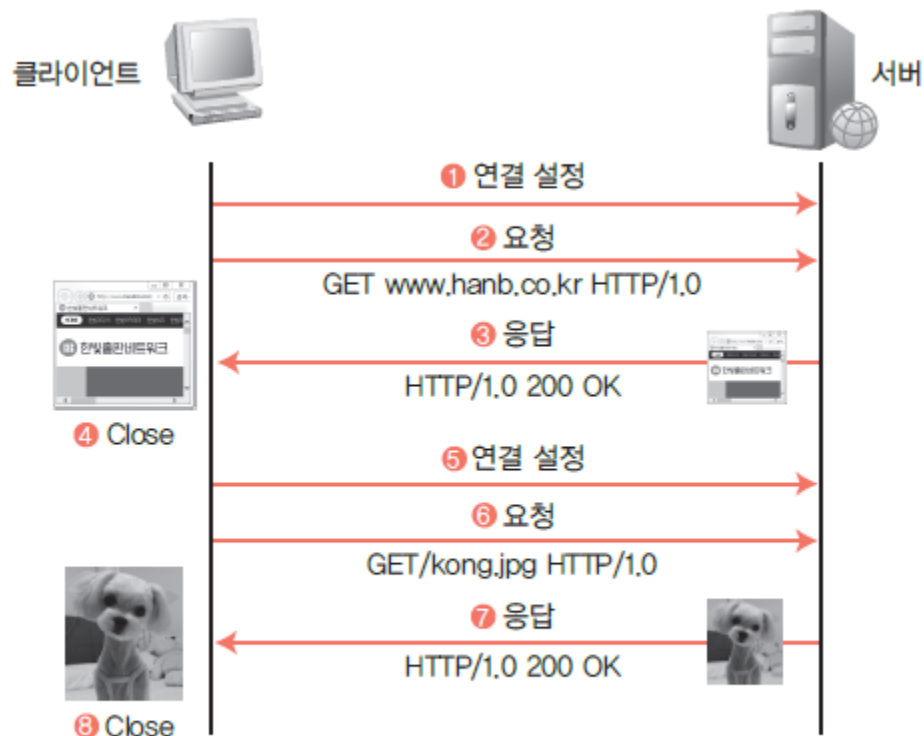


그림 7-15 문서에 이미지가 있을 때 HTTP 1.0의 동작 과정

02. 응용 계층 프로토콜 및 서비스

- HTTP 1.1에서는 다시 연결을 설정하지 않고 연결된 소켓을 통해 데이터(이미지)를 전송 받는다. 이를 통해 프로토콜의 수행 성능이 향상된 것을 확인할 수 있다.

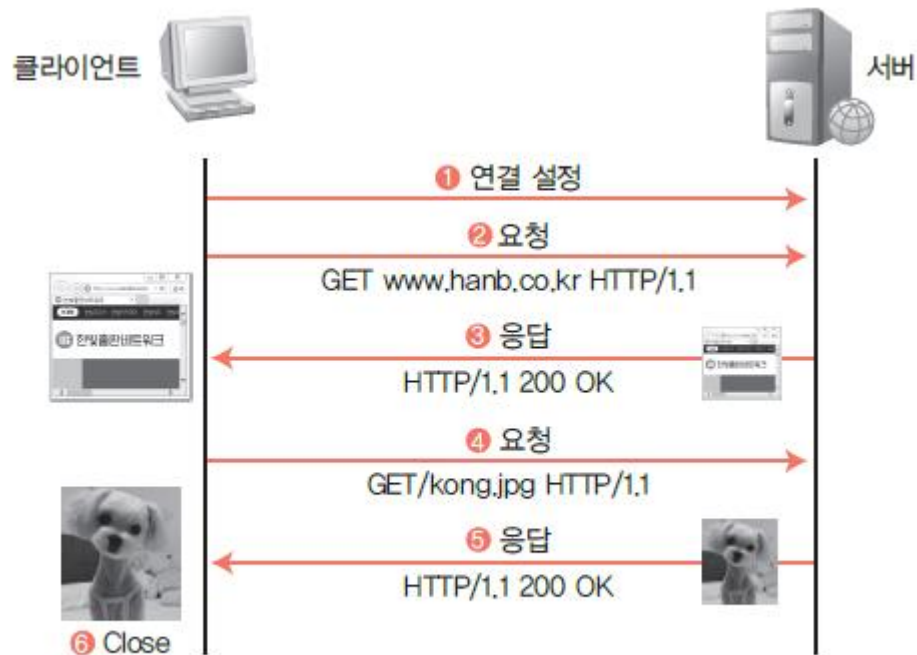


그림 7-16 문서에 이미지가 있을 때 HTTP 1.1의 동작 과정

03. HTTP 덤프 분석 - 실습

1. HTTP 통신 추출

- 와이어샤크를 이용하여 간단한 웹 페이지 통신에서 이미지를 추출해보자. HTTP 통신을 추출하면 와이어샤크는 패킷에서 데이터를 복원해서 추출할 수 있다.
- 1. 와이어샤크를 실행하고 추출하고자 하는 웹 페이지에 접속한다. 필자는 한빛출판네트워크의 네트워크 개론 도서 정보 페이지 (http://www.hanbit.co.kr/store/books/look.php?p_code=B8069473976)에 접속했다.

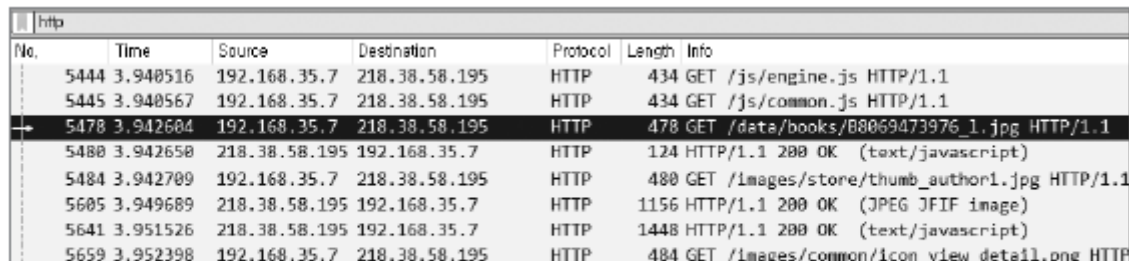
03. HTTP 덤프 분석 - 실습



그림 7-34 웹 페이지 접속

03. HTTP 덤프 분석 - 실습

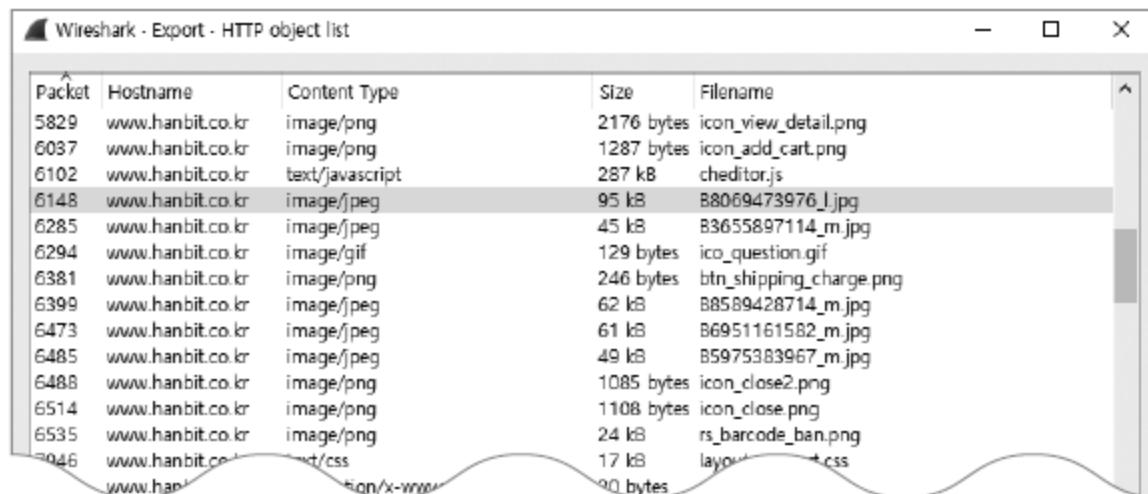
2. 와이어샤크 화면으로 전환하여 패킷 캡처를 중지한다. HTTP로 통신된 이미지 데이터를 추출해보자.



No.	Time	Source	Destination	Protocol	Length	Info
5444	3.940516	192.168.35.7	218.38.58.195	HTTP	434	GET /js/engine.js HTTP/1.1
5445	3.940567	192.168.35.7	218.38.58.195	HTTP	434	GET /js/common.js HTTP/1.1
5478	3.942604	192.168.35.7	218.38.58.195	HTTP	478	GET /data/books/B8069473976_1.jpg HTTP/1.1
5480	3.942650	218.38.58.195	192.168.35.7	HTTP	124	HTTP/1.1 200 OK (text/javascript)
5484	3.942709	192.168.35.7	218.38.58.195	HTTP	480	GET /images/store/thumb_author1.jpg HTTP/1.1
5605	3.949689	218.38.58.195	192.168.35.7	HTTP	1156	HTTP/1.1 200 OK (JPEG JFIF image)
5641	3.951526	218.38.58.195	192.168.35.7	HTTP	1448	HTTP/1.1 200 OK (text/javascript)
5659	3.952398	192.168.35.7	218.38.58.195	HTTP	484	GET /images/common/icon_view_detail.png HTTP

그림 7-35 캡처된 패킷

3. 메뉴에서 [File]-[Export Objects]를 선택한 후 서브메뉴에서 [HTTP]를 선택하면 HTTP 오브젝트 리스트 화면을 확인할 수 있다.



Packet	Hostname	Content Type	Size	Filename
5829	www.hanbit.co.kr	image/png	2176 bytes	icon_view_detail.png
6037	www.hanbit.co.kr	image/png	1287 bytes	icon_add_cart.png
6102	www.hanbit.co.kr	text/javascript	287 kB	cheditor.js
6148	www.hanbit.co.kr	image/jpeg	95 kB	B8069473976_1.jpg
6285	www.hanbit.co.kr	image/jpeg	45 kB	83655897114_m.jpg
6294	www.hanbit.co.kr	image/gif	129 bytes	ico_question.gif
6381	www.hanbit.co.kr	image/png	246 bytes	btn_shipping_charge.png
6399	www.hanbit.co.kr	image/jpeg	62 kB	88589428714_m.jpg
6473	www.hanbit.co.kr	image/jpeg	61 kB	86951161582_m.jpg
6485	www.hanbit.co.kr	image/jpeg	49 kB	85975383967_m.jpg
6488	www.hanbit.co.kr	image/png	1085 bytes	icon_close2.png
6514	www.hanbit.co.kr	image/png	1108 bytes	icon_close.png
6535	www.hanbit.co.kr	image/png	24 kB	rs_barcode_ban.png
6946	www.hanbit.co.kr	text/css	17 kB	layout.css
7046	www.hanbit.co.kr	text/css	90 bytes	font/x-ww

그림 7-36 HTTP 오브젝트 리스트

03. HTTP 덤프 분석 - 실습

4. 이미지 이름을 찾아 저장한다. 저장한 경로를 탐색기에서 확인하면 HTTP 통신에서 이미지 파일이 출력된 것을 확인할 수 있다.



그림 7-37 HTTP 통신 이미지

03. HTTP 덤프 분석 - 실습

5. 데이터를 모두 분석할 수 있는 것은 아니지만, 캡처한 HTTP 패킷에서 모든 데이터를 저장하려면 HTTP 오브젝트 리스트 화면에서 <모두 저장>을 클릭한다. 저장 경로에 모든 데이터가 저장되며, 이미지 파일뿐만 아니라 HTTP로 전송된 다양한 형식의 데이터가 파일로 복원된다.

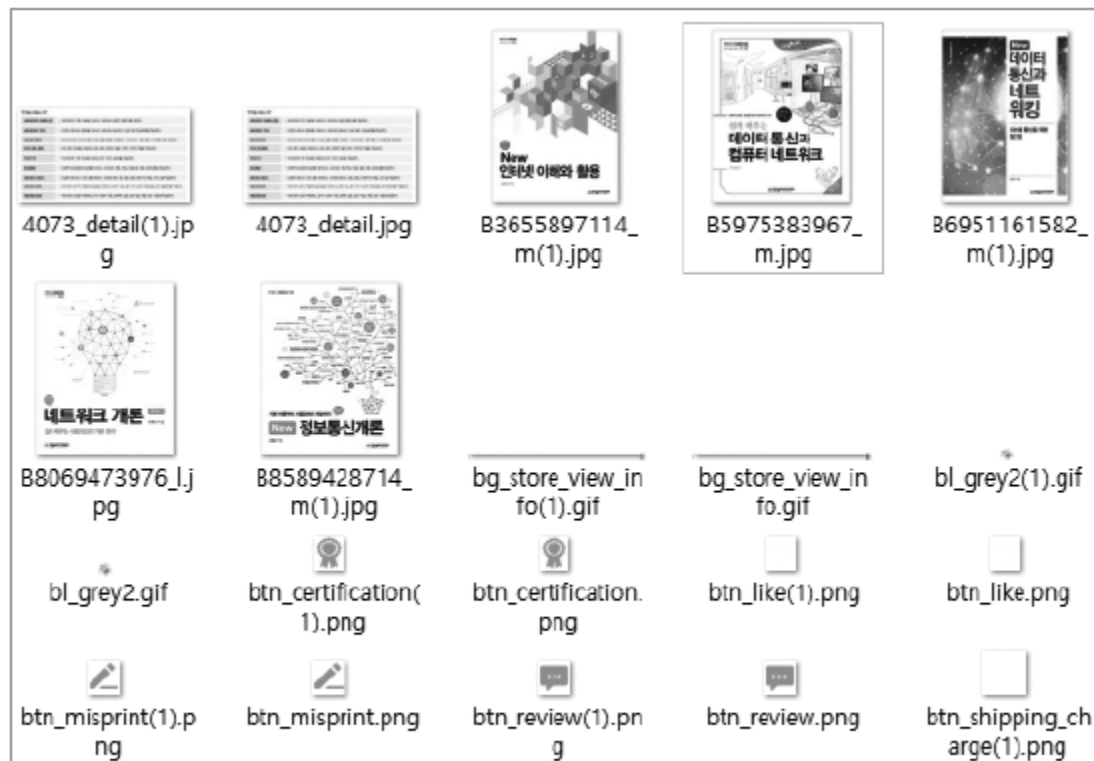


그림 7-38 모든 데이터 복원

03. HTTP 덤프 분석 - 실습

2. HTTP 덤프 분석

- HTTP는 웹 페이지 송수신을 위한 프로토콜이다. 서버의 80번 포트로 확립된 소켓상에서 HTTP 요청과 HTTP 응답을 교환함으로써 네트워크 통신이 이루어진다. HTTP 패킷의 덤프 분석을 해보자.

1. HTTP 요청 메시지

- 패킷 리스트 영역의 Info 열에 GET /파일명 HTTP/1.1로 표시된 프레임이 HTTP 요청 메시지가 포함된 패킷이다. 이 프레임을 선택하고 패킷 상세 영역에서 Hypertext Transfer Protocol을 클릭한다.

3135	3.784592	192.168.35.7	218.38.58.195	HTTP	356 GET /store/books/look.php?p_code=88069473976 HTTP/1.1
3163	3.817534	192.168.35.7	218.38.58.195	HTTP	416 GET /css/common.css HTTP/1.1
3171	3.819801	192.168.35.7	218.38.58.195	HTTP	415 GET /css/hover.css HTTP/1.1
3178	3.820299	218.38.58.195	192.168.35.7	HTTP	275 HTTP/1.1 200 OK (text/css)

그림 7-39 HTTP 요청 메시지가 포함된 패킷

- 3163번 패킷은 GET 메소드를 사용하여 HTTP 1.1 프로토콜로 common.css 페이지를 가져오라는 명령이다.

03. HTTP 덤프 분석 - 실습

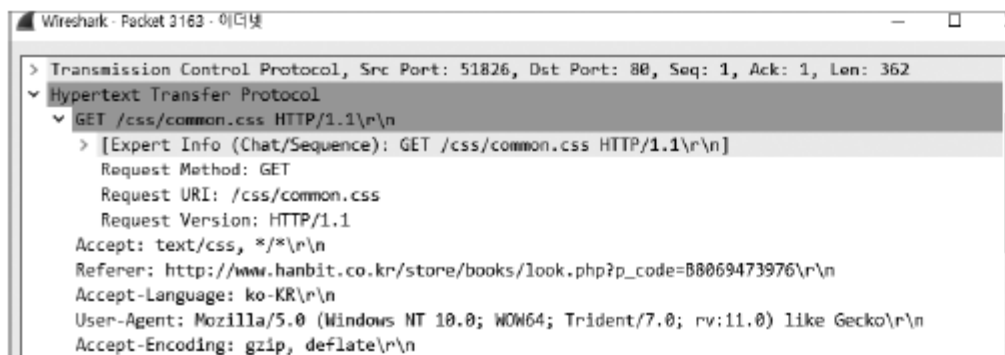


그림 7-40 HTTP 요청 메시지

- Request Method: 웹 페이지를 가져오라는 GET 메소드이다.
- Request URI: 웹 페이지의 위치에 대해 common.css 페이지를 가져오라는 명령을 나타낸다.
- Request Version: 웹 페이지를 가져올 때의 방식이며, HTTP 1.1 버전을 사용한다는 것을 나타낸다.
- Accept: 웹 브라우저가 받아들일 수 있는 필드 형식이 지정되어 있다.
- Accept-Language: 웹 브라우저가 받아들일 수 있는 언어가 지정되어 있다.

03. HTTP 덤프 분석 - 실습

2. HTTP 응답 메시지

- 패킷 리스트 영역의 Info 열에 HTTP/1.1 200 OK로 표시된 프레임이 HTTP 응답 메시지가 포함된 패킷이다. 이 프레임을 선택하고 패킷 상세 영역에서 Hypertext Transfer Protocol을 클릭한다.

3285	6.198690	gms.wip.ahn1...	192.168.35.7	HTTP	406 HTTP/1.1 200 OK
3299	6.215116	192.168.35.7	www.hanbit.co.kr	HTTP	377 GET /css/common.css HTTP/1.1
3314	6.218094	www.hanbit.co...	192.168.35.7	HTTP	275 HTTP/1.1 200 OK (text/css)
3316	6.218137	192.168.35.7	www.hanbit.co.kr	HTTP	376 GET /css/hover.css HTTP/1.1

그림 7-41 HTTP 응답 메시지가 포함된 패킷

03. HTTP 덤프 분석 - 실습

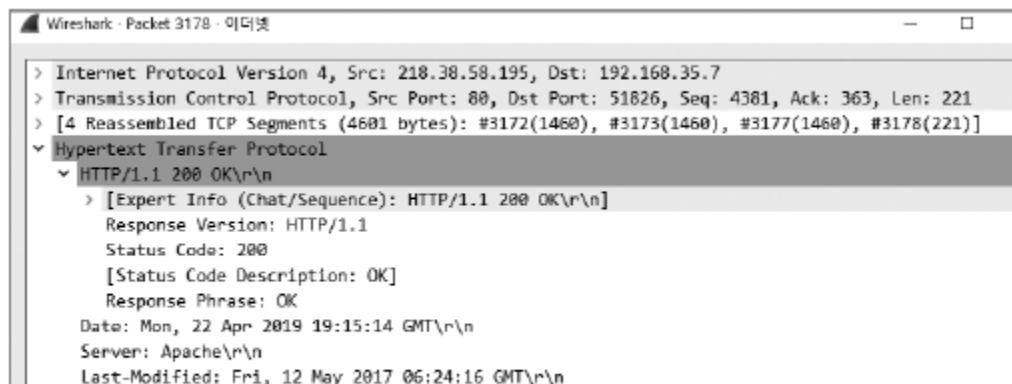


그림 7-42 HTTP 응답 메시지

- HTTP 응답 코드인 HTTP/1.1 200 OK는 정상 응답을 의미한다.
- Response Version: HTTP 1.1 버전을 사용한다는 것을 알 수 있다.
- Status Code: 200은 정상적인 응답을 의미한다. 비정상적인 응답일 때는 문서를 찾을 수 없음을 의미하는 404(Not Found) 등 다양한 오류 응답 코드가 나타난다.
- Date: 웹 서버가 응답을 한 시각을 나타낸다.
- Server: 응답을 한 서버의 정보로, 서버의 종류나 버전을 확인할 수 있다.