과제3. 패킷 분석

20130961 조용진
20131143 최　현

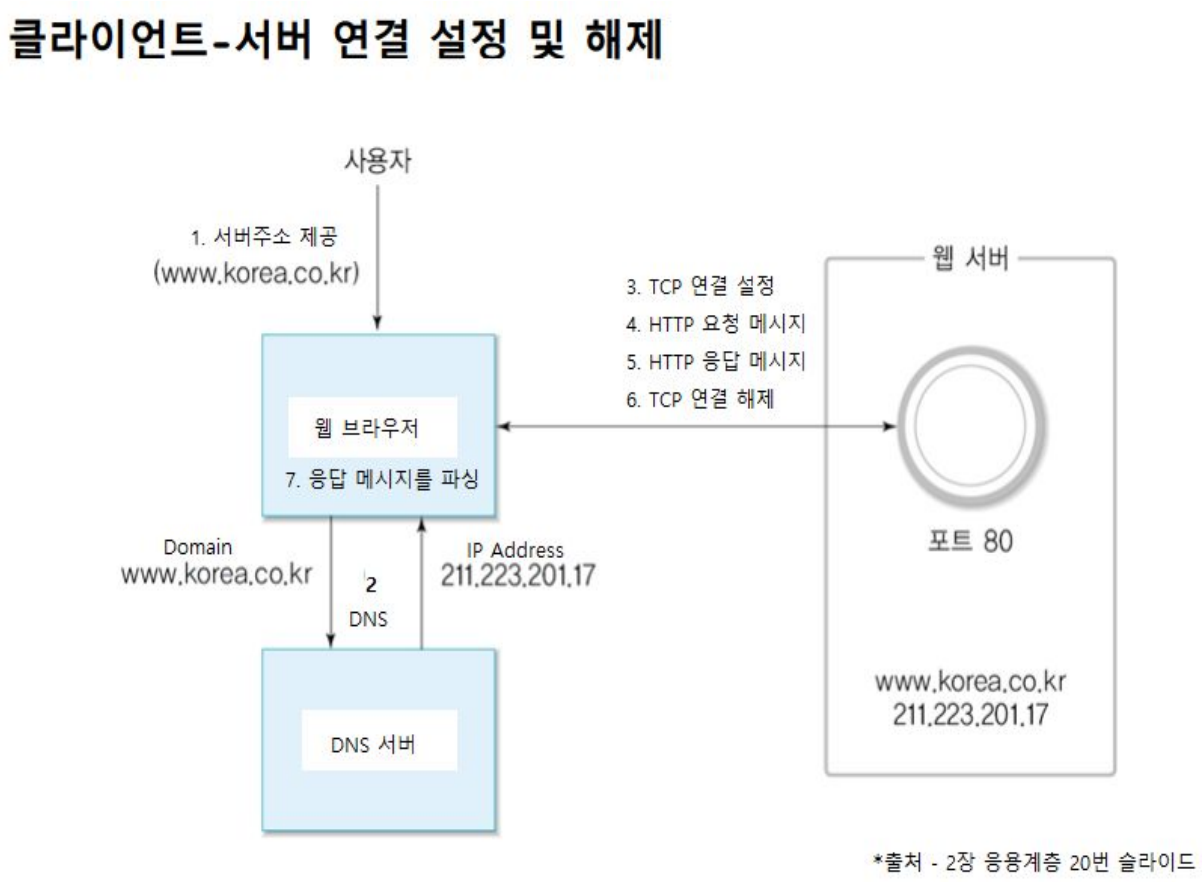
수업 명	컴퓨터 네트워크
팀원 명	20130961 조용진
	20131143 최　현
수업 교수	최정열 교수
작성일 자	2019. 11. 09

목차

I. 패킷 흐름

1. 클라이언트-서버 연결과정

- 일반적인 사용자가 인터넷 사이트에 접속할 때 쓰는 클라이언트-서버 모델의 연결과 해제는 다음과 같다.



< 그림 1. 클라이언트-서버 모델의 연결 설정 및 해제 흐름도 >

먼저 사용자가 웹 브라우저를 통해 서버주소를 입력하면 웹 브라우저는 해당 주소를 DNS 서버에 넘기고(Port #53) IP 주소를 받는다.

웹 브라우저는 DNS서버에서 제공받은 IP주소로 웹 서버(Port #80)에 TCP연결을 설정하고 HTTP의 요청/응답을 주고받은 후 TCP연결을 해제 한다. 웹 서버에서 온 응답 메시지는 웹 브라우저에서 응답 메시지를 파싱하여 사용자에게 최종 화면을 보여주게 된다.

2. Wireshark로 분석한 클라이언트-서버 연결 과정

1. 클라이언트-서버 연결 과정에서 살펴본 흐름을 와이어샤크를 통해 확인 해본 결과가 다음과 같다.

	Time	Source	Destination	Protocol	Length	Info
248	3.859406	115.140.24.224	1.214.68.2	DNS	68	Standard query 0x2b06 A nate.com
249	3.866832	1.214.68.2	115.140.24.224	DNS	100	Standard query response 0x2b06 A nate.com A 120.50.132.112 A 120.50.131.
250	3.867379	115.140.24.224	120.50.132.112	TCP	62	50824 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
251	3.867385	115.140.24.224	120.50.132.112	TCP	62	50825 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
252	3.871175	120.50.132.112	115.140.24.224	TCP	60	80 → 50825 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
253	3.871221	115.140.24.224	120.50.132.112	TCP	54	50825 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
254	3.871417	115.140.24.224	120.50.132.112	HTTP	315	GET / HTTP/1.1
255	3.872277	120.50.132.112	115.140.24.224	TCP	60	80 → 50824 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
256	3.872313	115.140.24.224	120.50.132.112	TCP	54	50824 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
257	3.875325	120.50.132.112	115.140.24.224	TCP	60	80 → 50825 [ACK] Seq=1 Ack=262 Win=30016 Len=0
258	3.879029	120.50.132.112	115.140.24.224	HTTP	432	HTTP/1.1 200 OK (text/html)
259	3.879029	120.50.132.112	115.140.24.224	TCP	60	80 → 50825 [FIN, ACK] Seq=379 Ack=262 Win=30016 Len=0
260	3.879051	115.140.24.224	120.50.132.112	TCP	54	50825 → 80 [ACK] Seq=262 Ack=380 Win=65157 Len=0
261	3.879141	115.140.24.224	120.50.132.112	TCP	54	50825 → 80 [FIN, ACK] Seq=262 Ack=380 Win=65157 Len=0
262	3.883038	120.50.132.112	115.140.24.224	TCP	60	80 → 50825 [ACK] Seq=380 Ack=263 Win=30016 Len=0

< 그림 2. 와이어샤크로 분석한 연결 설정 및 해제 패킷 정보 >

1) DNS서버에 서버주소 제공

2) DNS

- 사용자(115.140.24.224)가 ‘nate.com’이라는 도메인을 브라우저에 입력하고 브라우저는 해당 도메인을 DNS서버(1.214.68.2)에 Query로 보낸다. DNS서버는 받은 도메인에 해당하는 IP 주소(120.50.132.112, 120.50.131.112)를 응답한다.

3) TCP - 3-way handshake (TCP 연결 설정)

- 응답 받은 브라우저(클라이언트)는 임의의 포트번호(50824, 50825)를 할당하고 포트번호를 포함한 SYN을 서버(Port# 80)로 전송한다. 서버는 SYN요청을 받고 연결을 허가하는 의미의 SYN과 ACK 패킷을 클라이언트로 전송한다. 클라이언트는 요청에 대한 응답을 확인했다는 의미로 ACK 패킷을 전송한다.

4) 연결연결 성립 후 서버에게 HTTP요청

5) 서버가 클라이언트에게 HTTP응답(200 OK)

- HTTP 프로토콜은 클라이언트의 HTTP요청에 의해 필요한 파일을 전달한 후, 서버 측에서 연결 해제를 요청하고 클라이언트→서버의 연결해제, 서버→클라이언트의 연결해제를 통해 성립된 연결을 모두 해제한다.

6) TCP - 4-way handshake (TCP 해제 설정)

- 서버가 연결을 종료하겠다는 FIN플래그 전송을 하고 클라이언트는 확인메시지(ACK)전송 후 자신이 통신이 끝날 때까지 대기한다. 통신이 끝나면 클라이언트는 서버에게 FIN플래그 전송을 하고 서버는 ACK플래그를 전송한다.

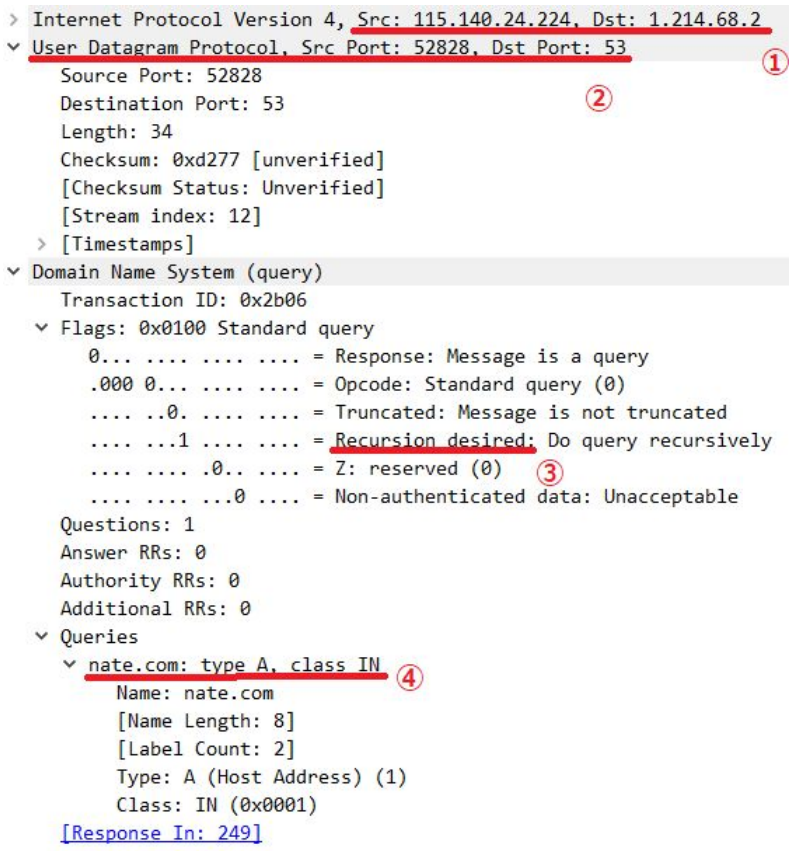
* DNS가 응답해준 IP가 2개였으므로 클라이언트는 두 IP 전부 TCP 연결 요청을 하였으나 먼저 응답이온 포트(50825)를 통해 HTTP연결이 이루어졌다.

II. 패킷 분석

1. DNS

DNS 서버에 IP 주소를 요청하는 과정이다.

1) 요청



< 그림 3. DNS서버에 IP주소 요청 (패킷 248) >

Datagram

① 소스IP(115.140.24.224)로 부터 DNS서버(1.214.68.2)로 보낸 패킷임을 확인할 수 있다.

UDP Segment

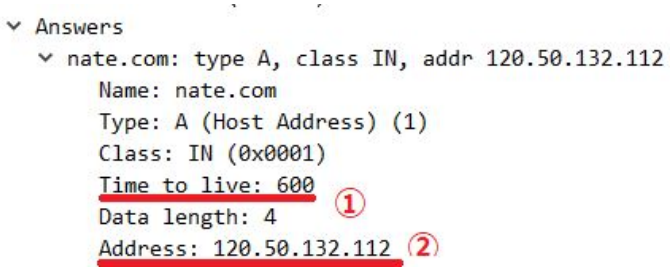
② DNS가 UDP상에서 수행되었음을 확인할 수 있으며 클라이언트는 임의의 포트(52828)을 사용하고, 목적지에는 DNS의 포트인 53이 사용된 것을 확인할 수 있다.

DNS Message

③ 재귀쿼리를 사용하는지 여부를 알려주는 비트이다.(재귀 사용)

④ ‘nate.com’(name)이라는 호스트 주소(type A, 쿼리 유형)를 묻는다.

2) 응답



< 그림 4. DNS 응답 (패킷 249) >

DNS Message

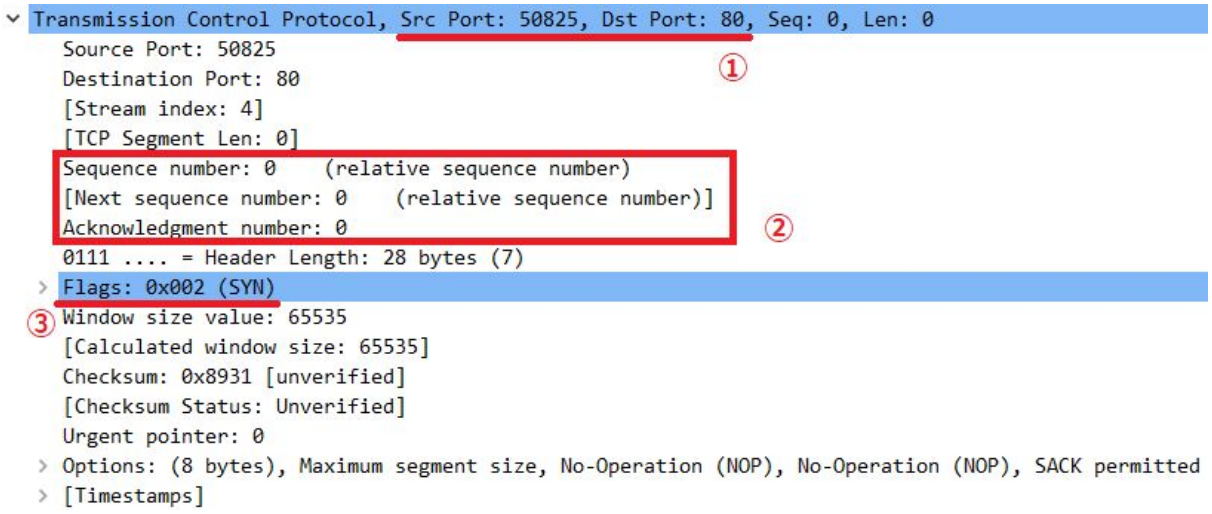
① DNS쿼리에 대한 결과값을 캐쉬에 저장하는 시간 (0이되면 폐기된다.)

② 쿼리에 대한 결과값 (nate.com은 120.50.132.112이다.)

2. TCP 연결 설정(3-way handshake)

3-way handshake을 통해 웹 서버와의 TCP 연결을 설정한다.

1) 서버에 연결 요청



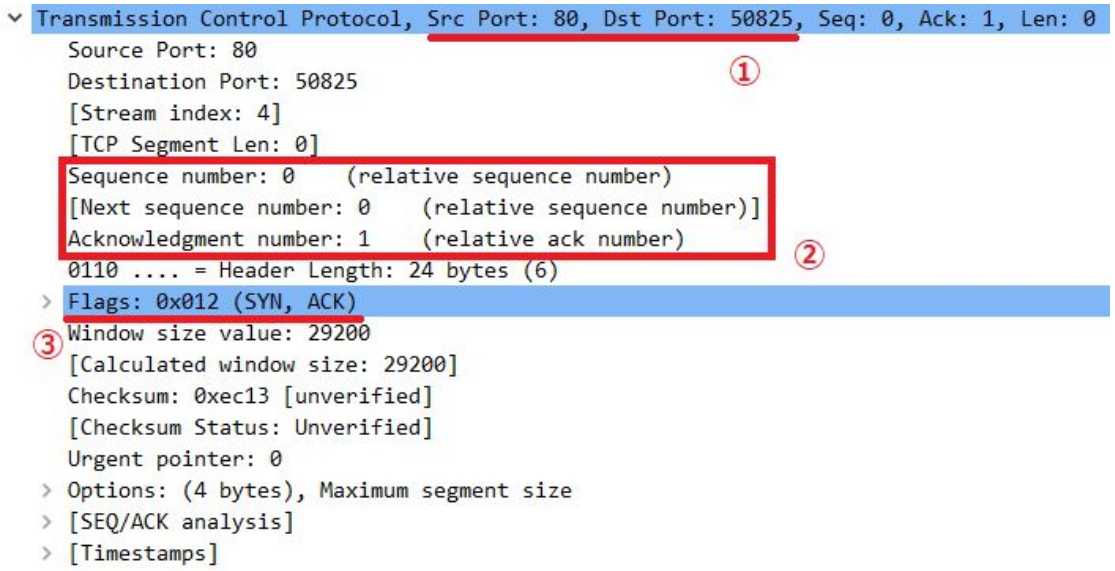
< 그림 5. TCP 연결 요청 (패킷 251) >

① 임의의 포트번호(50825)를 클라이언트에 할당하고 SYN을 서버(port# 80)로 전송한다.

② 순서번호와 확인 응답번호는 0이다.

③ 연결을 요청하는 SYN을 보낸다.

2) 서버의 허용



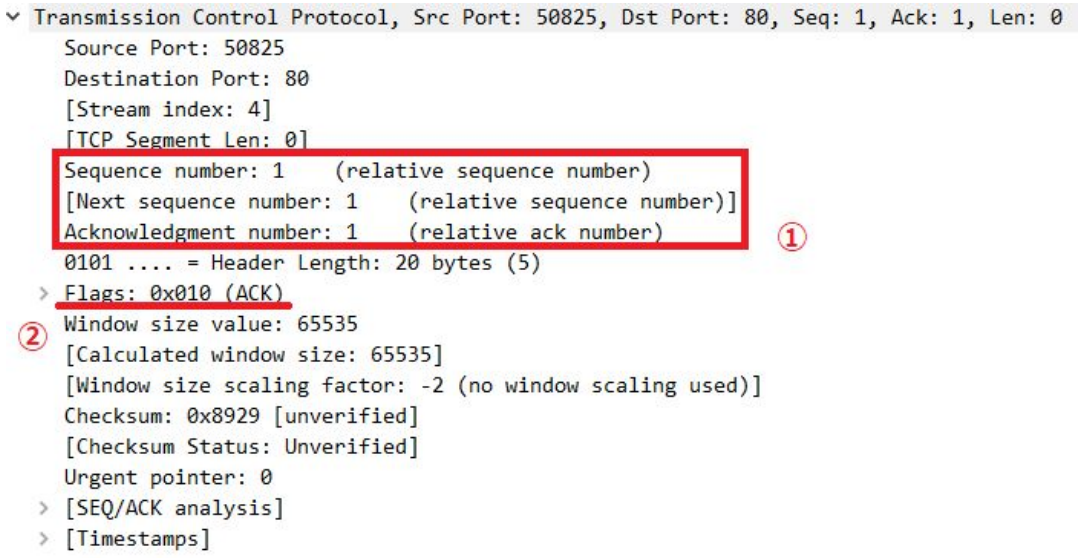
< 그림 6. TCP 연결 허용 (패킷 252) >

① 서버(port# 80)에서 클라이언트(port# 50825)로 연결 허용을 뜻하는 패킷을 보낸다.

② 다음 패킷을 보내라는 의미로 확인응답번호는 1이다.

③ 연결을 허용하는 의미로 SYN패킷과 1) 요청에 대한 응답으로 ACK패킷을 전송한다.

3) 서버에서의 응답 확인



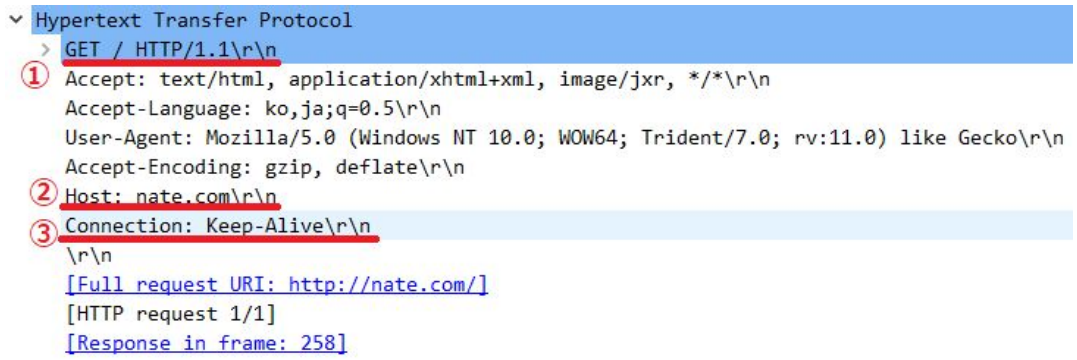
< 그림 7. TCP 응답 확인 (패킷 253) >

① 서버에서 보낼 패킷의 순서(1)을 보냈으므로 Seq는 1이고, 서버에서 온 패킷의 Seq(0)의 다음 에 받아야할 패킷 순서(1)을 확인 응답번호로 보낸다.

② 연결 허용 응답에 대한 확인의 의미로 ACK패킷을 서버로 보낸다.

3. HTTP

1) 요청



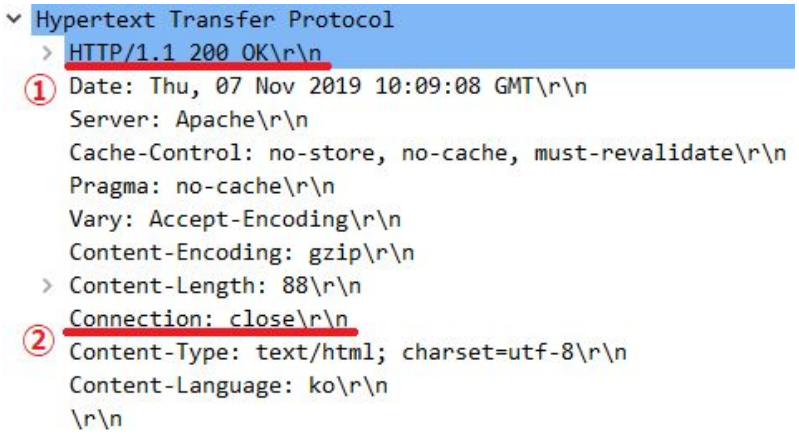
< 그림 8. HTTP요청문 (패킷 254) >

① GET메소드로 Body가 없고, 프로토콜 버전은 1.1이다.

② 클라이언트가 요청하는 웹서버의 주소이다.

③ 지속연결을 사용할 것을 명시하였다.

2) 응답



< 그림 9. HTTP응답문 (패킷 258) >

① 요청에 대한 응답 200 OK(요청이 성공적으로 수행됨)을 보낸다.

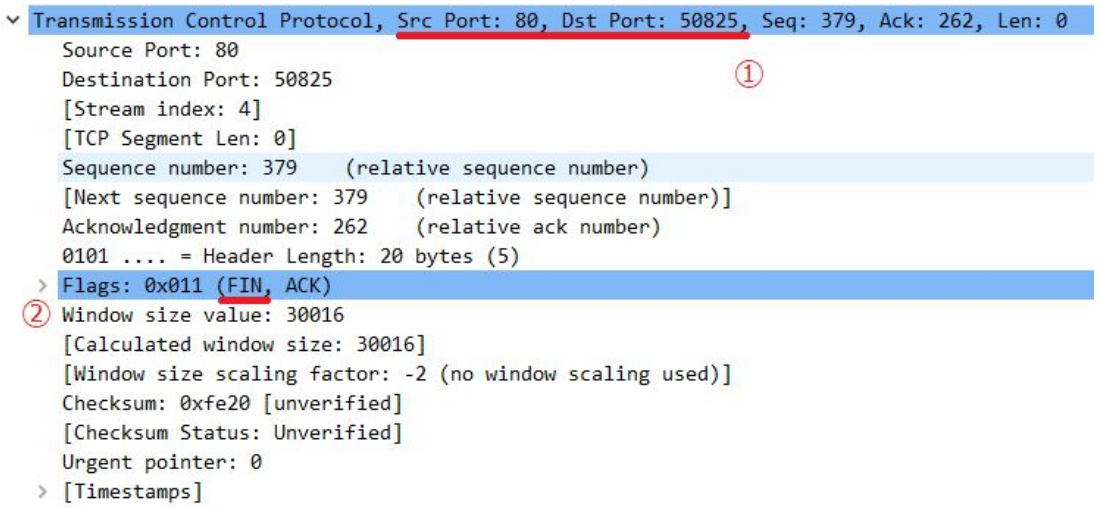
② TCP 연결을 해제할 것을 요청한다.

4. TCP 연결 해제(4-way handshake)

4-way handshake을 통해 웹 서버와의 TCP 연결을 해제한다.

* 원래라면 클라이언트가 먼저 FIN을 보내는 것으로 4-way handshake를 시작하나, 몇 번을 다시 캡쳐해봐도 서버쪽에서 먼저 FIN을 보내었다. 조사결과 어느쪽이되었든 FIN을 보낼 수 있다고 한다. (참고 자료 4.)

1) 해제 요청

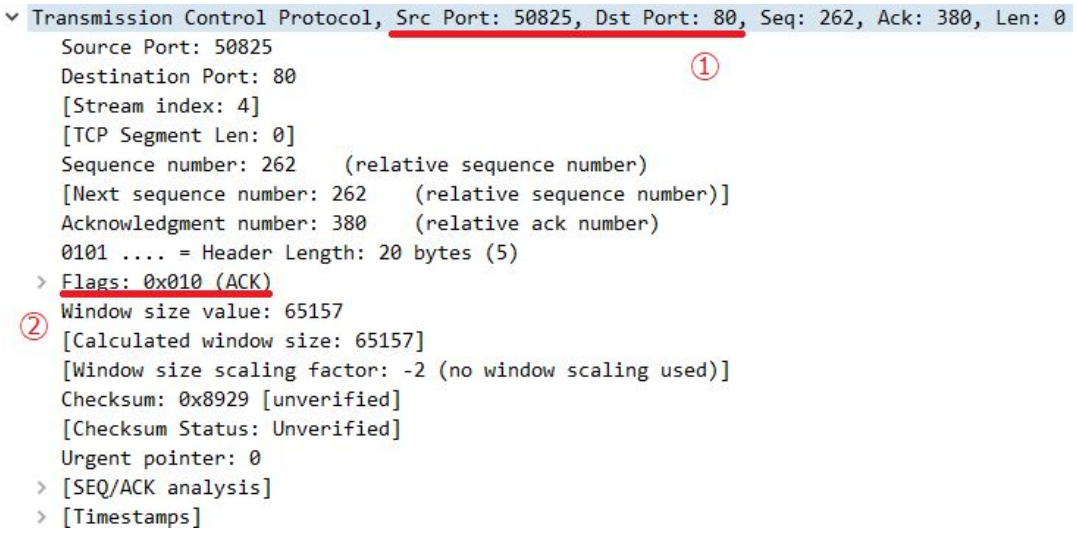


<그림 10. TCP 연결해제 요청 (패킷 259) >

① 서버쪽에서 클라이언트에게 연결 해제를 뜻하는 FIN을 보낸다.

② 연결 해제를 요청하는 FIN을 보낸다.

2) 요청 확인

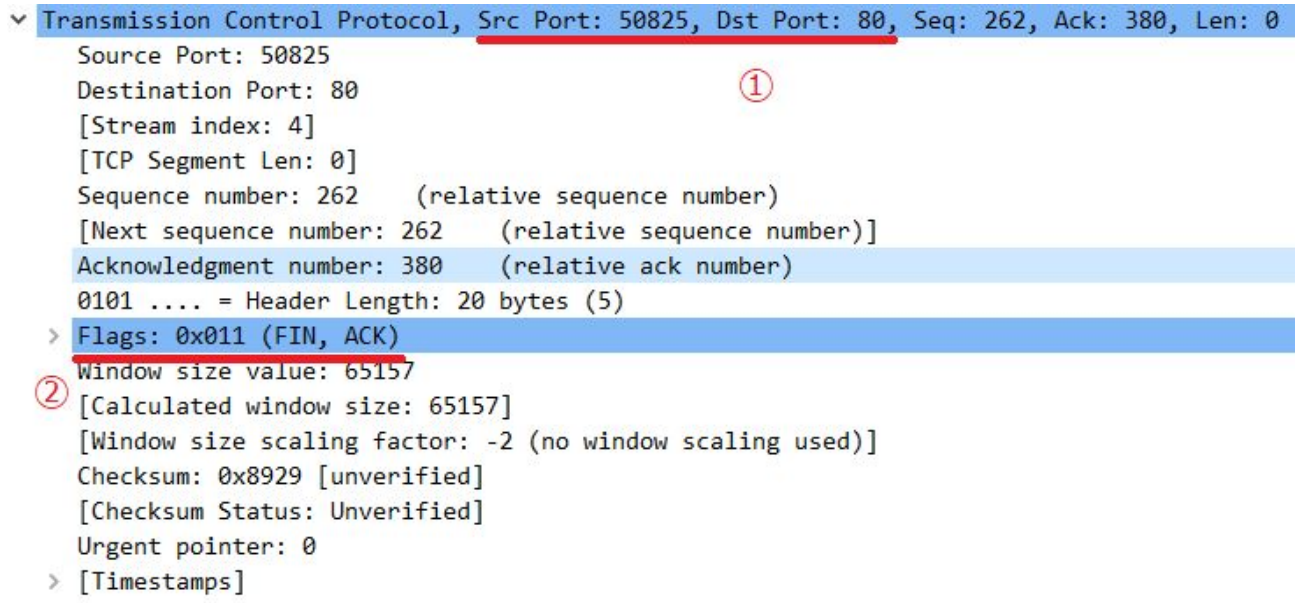


<그림 11. TCP 연결해제 요청확인 (패킷 260) >

① 클라이언트 쪽에서 서버쪽으로 요청에 대한 응답을 보낸다.

② FIN을 받았다는 의미인 ACK를 보낸다.

3) 연결 종료 통보

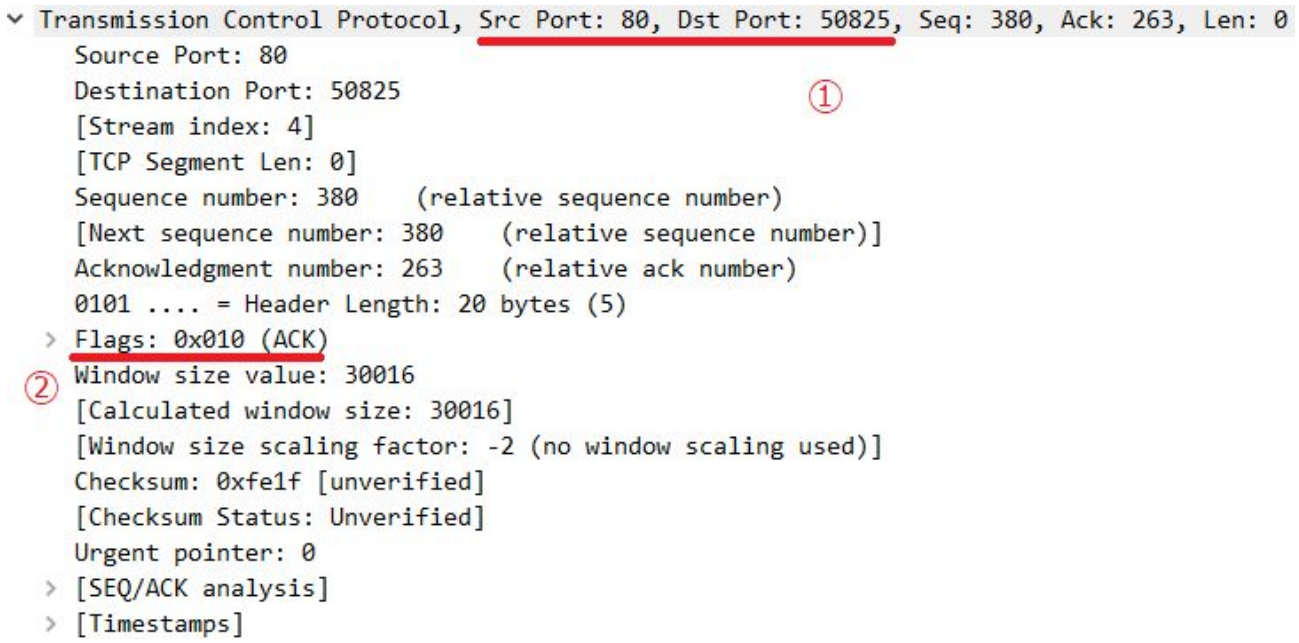


<그림 12. TCP 연결종료 통보 (패킷261) >

① 클라이언트에서 서버쪽으로 연결이 종료되었음을 뜻하는 FIN을 보낸다.

② 연결이 종료되었음을 뜻하는 FIN을 보낸다.

4) 연결 종료 확인



<그림 13. TCP 연결종료 확인 (패킷262) >

① 서버에서 클라이언트 쪽으로 FIN을 받았음을 확인하는 ACK를 보낸다.

② FIN을 받았음을 확인하는 FIN을 보낸다.

위와 같은 과정으로 TCP연결이 종료되었다.

III. 참고 자료

1.DNS가 UDP 사용하는 이유

https://www.atmarkit.co.jp/ait/articles/1508/25/news015.html

2. 기본적인 DNS 패킷 분석

https://darksoulstory.tistory.com/62

3. 와이어샤크 패킷 분석

http://blog.naver.com/PostView.nhn?blogId=wergreat10&logNo=220185986685

4. 서버가 먼저 FIN을 보내는 이유

https://osqa-ask.wireshark.org/questions/50641/fin-ack-sending-without-getting-prior-fin-from-counter-part