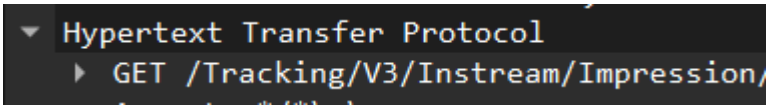
PBL 3-2

패킷 분석

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.108	50.19.229.205	TCP	66	60139 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 S
2	0.092419	50.19.229.205	192.168.1.108	TCP	66	80 → 60139 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
3	0.092521	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.094027	192.168.1.108	50.19.229.205	HTTP	1384	GET /Tracking/V3/Instream/Impression/?start|2873|7214
5	0.196174	50.19.229.205	192.168.1.108	TCP	54	80 → 60139 [ACK] Seq=1 Ack=1331 Win=8960 Len=0
6	0.204299	50.19.229.205	192.168.1.108	HTTP	607	HTTP/1.1 302 Found
7	0.221142	192.168.1.108	50.19.229.205	HTTP	1380	GET /Tracking/V3/Instream/Impression/?0|2873|72147|75
8	0.326624	50.19.229.205	192.168.1.108	HTTP	607	HTTP/1.1 302 Found
9	0.600950	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=2657 Ack=1107 Win=64592 Len=0
10	0.674498	50.19.229.205	192.168.1.108	HTTP	607	[TCP Spurious Retransmission] HTTP/1.1 302 Found
11	0.674551	192.168.1.108	50.19.229.205	TCP	66	[TCP Dup ACK 9#1] 60139 → 80 [ACK] Seq=2657 Ack=1107
12	3.675382	192.168.1.108	50.19.229.205	HTTP	1428	GET /Tracking/V3/Instream/Impression/?25|2873|72147|7
13	3.776869	50.19.229.205	192.168.1.108	HTTP	607	HTTP/1.1 302 Found
14	3.975053	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=4031 Ack=1660 Win=65700 Len=0
15	11.175009	192.168.1.108	50.19.229.205	HTTP	1428	GET /Tracking/V3/Instream/Impression/?75|2873|72147|7
16	11.283854	50.19.229.205	192.168.1.108	HTTP	607	HTTP/1.1 302 Found
17	11.478274	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=5405 Ack=2213 Win=65144 Len=0
18	70.319743	50.19.229.205	192.168.1.108	TCP	54	80 → 60139 [FIN, ACK] Seq=2213 Ack=5405 Win=17664 Len
19	70.319865	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=5405 Ack=2214 Win=65144 Len=0
20	74.757892	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [RST, ACK] Seq=5405 Ack=2214 Win=0 Len=0

1. 왼쪽 No.열을 확인해보면 총 패킷 개수는 20개인 것을 확인할 수 있다.

2. IP호스트는 3-Way Handshake를 통해 1,2,3번 프레임에서 TCP 연결을 만든다.



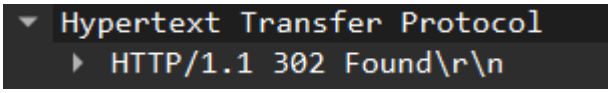
3. 프레임4 패킷의 데이터부분을 확인해보면 HTTP GET 명령어를 보낸 것을 알 수 있다.

No.	Time	Source	Destination	Protocol	Lenç
15	11.175009	192.168.1.108	50.19.229.205	HTTP	1428
12	3.675382	192.168.1.108	50.19.229.205	HTTP	1428
4	0.094027	192.168.1.108	50.19.229.205	HTTP	1384
7	0.221142	192.168.1.108	50.19.229.205	HTTP	1380

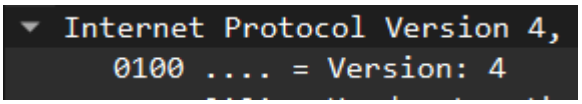
4. 이 파일 내에서 가장 긴 프레임의 길이는 1428Byte로, 12번과 15번 패킷이 가장 긴 것을 알 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.108	50.19.229.205	TCP	66	60139 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 S
2	0.092419	50.19.229.205	192.168.1.108	TCP	66	80 → 60139 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
3	0.092521	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.094027	192.168.1.108	50.19.229.205	HTTP	1384	GET /Tracking/V3/Instream/Impression/?start|2873|7214
5	0.196174	50.19.229.205	192.168.1.108	TCP	54	80 → 60139 [ACK] Seq=1 Ack=1331 Win=8960 Len=0
6	0.204299	50.19.229.205	192.168.1.108	HTTP	607	HTTP/1.1 302 Found
7	0.221142	192.168.1.108	50.19.229.205	HTTP	1380	GET /Tracking/V3/Instream/Impression/?0|2873|72147|75
8	0.326624	50.19.229.205	192.168.1.108	HTTP	607	HTTP/1.1 302 Found
9	0.600950	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=2657 Ack=1107 Win=64592 Len=0
10	0.674498	50.19.229.205	192.168.1.108	HTTP	607	[TCP Spurious Retransmission] HTTP/1.1 302 Found
11	0.674551	192.168.1.108	50.19.229.205	TCP	66	[TCP Dup ACK 9#1] 60139 → 80 [ACK] Seq=2657 Ack=1107
12	3.675382	192.168.1.108	50.19.229.205	HTTP	1428	GET /Tracking/V3/Instream/Impression/?25|2873|72147|7
13	3.776869	50.19.229.205	192.168.1.108	HTTP	607	HTTP/1.1 302 Found
14	3.975053	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=4031 Ack=1660 Win=65700 Len=0
15	11.175009	192.168.1.108	50.19.229.205	HTTP	1428	GET /Tracking/V3/Instream/Impression/?75|2873|72147|7
16	11.283854	50.19.229.205	192.168.1.108	HTTP	607	HTTP/1.1 302 Found
17	11.478274	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=5405 Ack=2213 Win=65144 Len=0
18	70.319743	50.19.229.205	192.168.1.108	TCP	54	80 → 60139 [FIN, ACK] Seq=2213 Ack=5405 Win=17664 Len
19	70.319865	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [ACK] Seq=5405 Ack=2214 Win=65144 Len=0
20	74.757892	192.168.1.108	50.19.229.205	TCP	54	60139 → 80 [RST, ACK] Seq=5405 Ack=2214 Win=0 Len=0

5. Protocol 열을 확인해보면 TCP와 HTTP 프로토콜 두 가지가 있는 것을 확인할 수 있다.



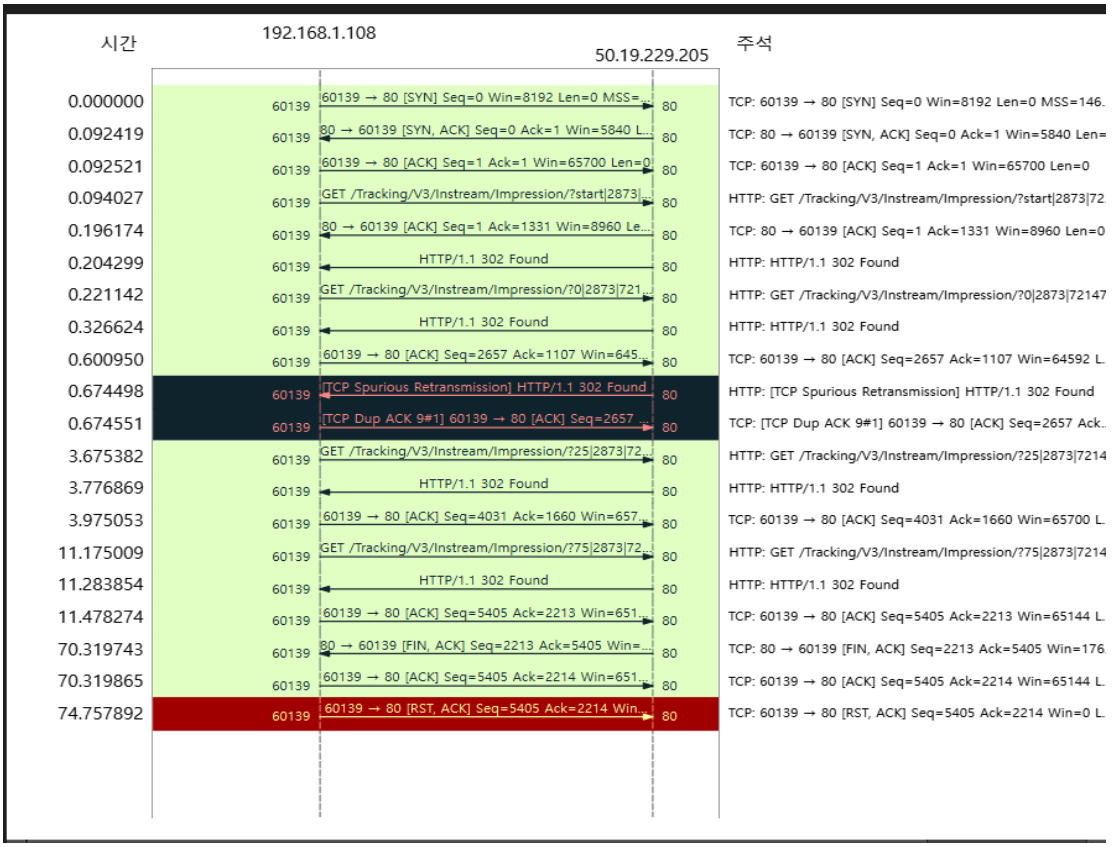
6. HTTP 응답인 6번 패킷을 확인하면, Redirection을 의미하는 HTTP 302 응답을 확인할 수 있다.



7. IP 헤더 부분을 확인하면 어떤 버전을 사용했는지 알 수가 있는데, 모든 패킷은 위와 같이 IPv4를 사용한 트래픽으로 IPv6트래픽은 존재하지 않는 것을 확인할 수 있었다.

추가 분석

- Flow Graph



1. 추가적으로 파일의 Flow Graph를 확인해보면, 프레임 1,2,3에서 3WHS를 통해 TCP 연결을 만드는 것을 알 수 있다.
    a. 먼저 SYN 요청을 보낸 108이 클라이언트, 205가 응답 서버인 것을 알 수 있다.

2. 클라이언트에서 HTTP서버로 GET요청을 보내는 패킷을 확인할 수 있다.

3. 서버는 이를 정상적으로 받았다는 ACK를 보내고, Redirection을 의미하는 302응답을 보낸다.

4. 302응답에도 불구하고 클라이언트는 GET 요청을 보내는 것을 확인할 수 있다.

5. 이 과정 이후 클라이언트에서 ACK를 보냈지만 다음 패킷으로 GET요청을 다시 보낸다. 마찬가지로 서버는 302응답을 다시 보내게 된다.
    a. 정상적인 통신이 이루어지지 않는다고 판단할 수 있다.

6. 이후 18번 패킷부터 20번 패킷을 보면 서버가 클라이언트에게 FIN 요청을 보내 종료 요청을 하고, 클라이언트가 RST를 통해 비정상 종료를 한 것을 확인할 수 있다.