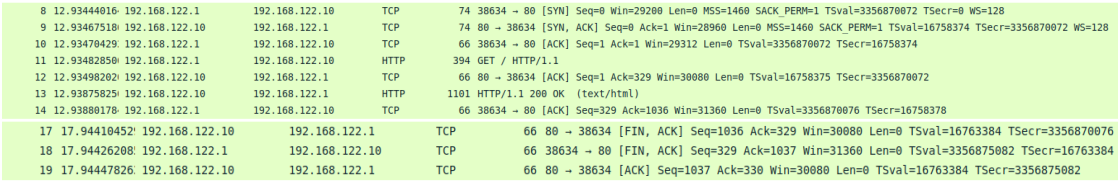
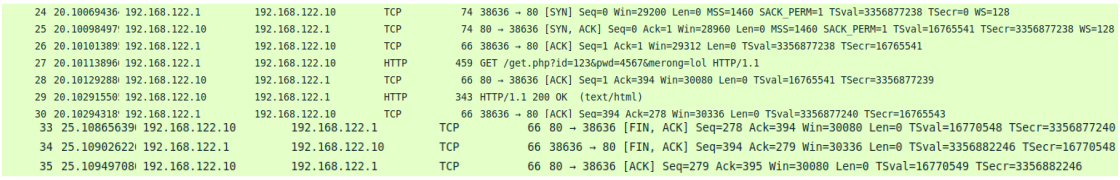
GET, POST 방식 패킷 분석

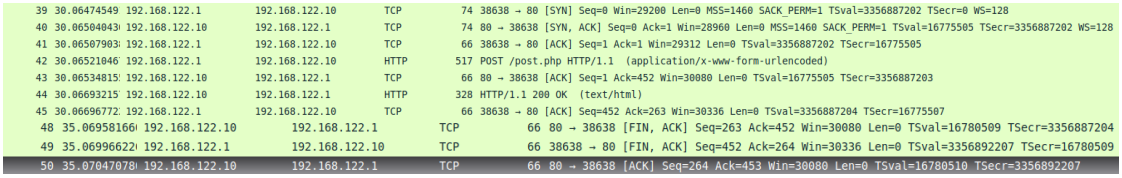
노트북: 숙제
만든 날짜: 2019-07-24 오전 12:06 **업데이트:** 2019-07-24 오전 12:06
작성자: 이종민



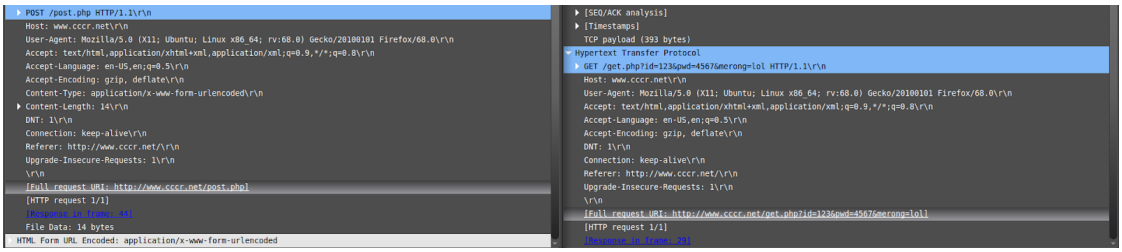
3 way hand shake 과정을 맺어서 HTTP 1.1 에 연결을 시도 해서 200 OK 정상적인 형태로 접속이 완료가 된 것에 대한 응답을 받고 FIN, ACK 를 통해 연결을 종료하는 것을 볼 수 있다.



GET 방식
3 way hand shake 맺어서 GET 방식으로 연결해서 정상적인 형태 200 OK, 파라미터 값 id, pwd, hidden에 대한 값이 보이는 걸 볼 수 있다.
해당 응답을 받으면 FIN, ACK 를 통해 세션을 종료한다.



POST 방식
3 way hand shake를 맺어서 POST 방식 접속 HTTP 1.1 200OK 정상적인 형태. POST 형식은 id, pwd, hidden에 대한 파라미터 값이 보이지 않는다. 해당 응답을 받으면 FIN, ACK를 통해 세션을 종료한다.



GET방식과 POST 방식의 패킷을 보면
GET 방식 패킷은 URI, 피라미터 값이 Id, pw, merong의 값을 URI에 전부 다 포함하고 있는걸 볼 수 있다.
반면 POST 방식 패킷은 URI, 피라미터 값이 나타나지 않는 것을 볼 수 있다.

host : www.cccr.net 서버의 도메인 네임을 나타낸다.
user-agent : mozilla firefox 사용자가 어떤 클라이언트를 이용해 요청을 보냈는지 볼 수 있다.
accept : text/html, */* 요청 보낼 때 어떤 타입으로 보내면 좋겠다고 명시를 한다.

html 형식인 응답을 처리하겠다는 뜻이다. 콤마를 적어서 여러 타입을 동시에 적어줄 수 있는데 html 형식이 아닌 */* 모든 형태의 응답을 처리 하겠다는 의미로 보인다.
accept-encoding, accept-language : 언어, 컨텐츠 압축 방식을 나타낸다.
dnt : 요청 헤더는 사용자의 트래킹 설정을 가르킨다. 0은 트래킹 허용한다, 1은 트래킹 허용을 하지 않는 것을 말하는데 현재 설정은 1 이므로 트래킹을 허용한다.

- dnt : 추적 중지, 사이트에서 추적하지 못하게 막는 방식 (firefox에서 기본적으로 적용된 옵션으로 보인다)

connection : 현재 전송이 완료된 후 네트워크 접속을 유지할지 말지를 제어한다.

- keep alive : tcp 연결을 재사용하는 기능이다. tcp를 무한정으로 유지할 수 없으므로 마지막으로 종료된 시점부터 정의된 시간까지 access가 없더라도 세션을 유지하는 구조이다.

referer : 이 페이지 이전의 페이지 주소가 담겨있다. 어떤 페이지에서 현재 페이지로 넘어왔는지 알 수 있다.

- 현재 www.cccr.net 에서 get 또는 post를 사용해서 다른 페이지로 넘어왔기 때문에 www.cccr.net 으로 보인다.