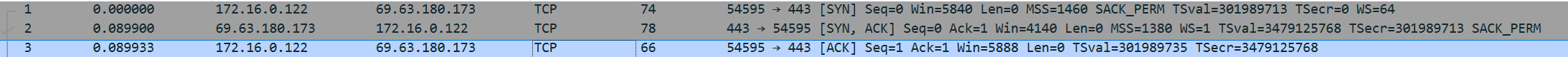
**SSL 패킷 분석을 통한 HTTPS 통신 흐름 이해**

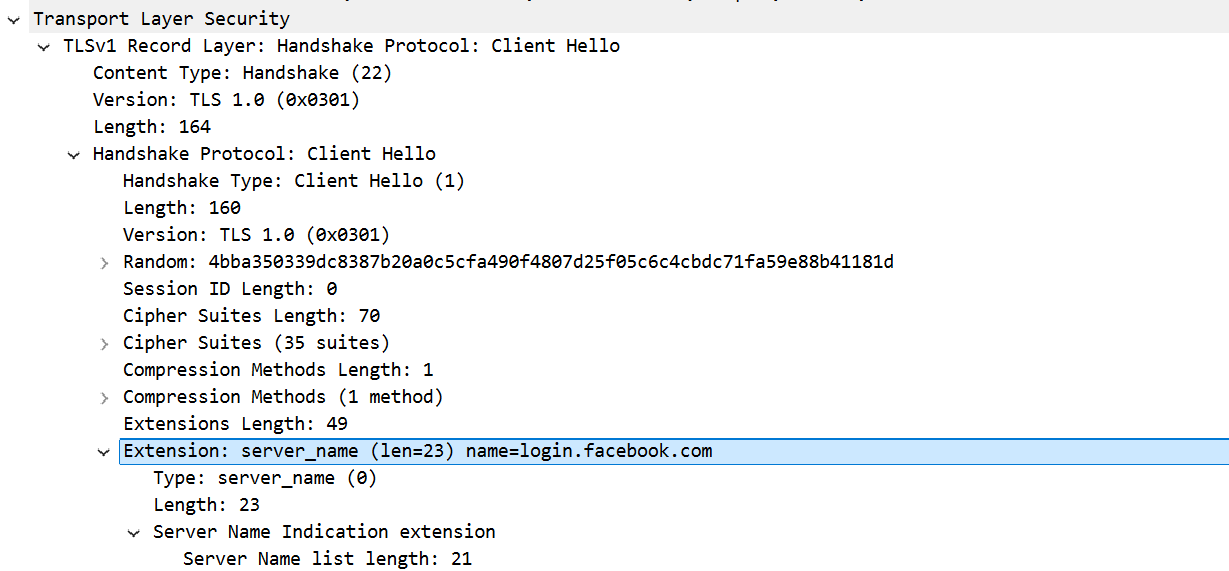
추적파일 기반으로 SSL Handshake 단계별 분석 및 시각화

총 71개의 패킷을 SSL Flow에 따라 분석합니다.

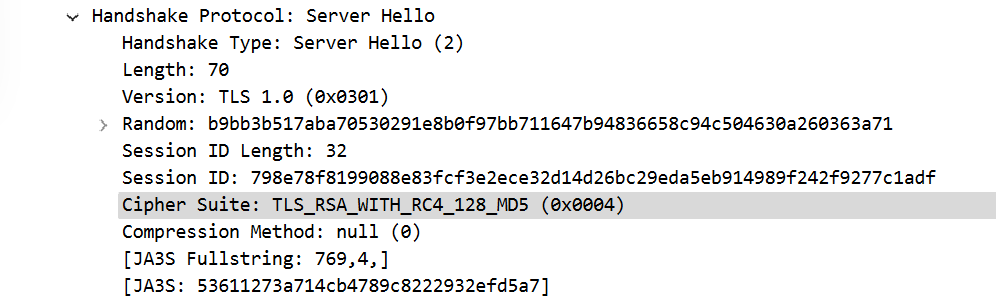
1. **TCP 3 Way Handshake**  
   클라이언트와 서버는 먼저 TCP 3 Way Handshake를 통해 연결을 수립합니다. 이 단계에서 SSL/TLS가 동작할 수 있는 기반을 마련합니다. HTTPS의 Well-Known 포트 번호 443번과 통신 중입니다.



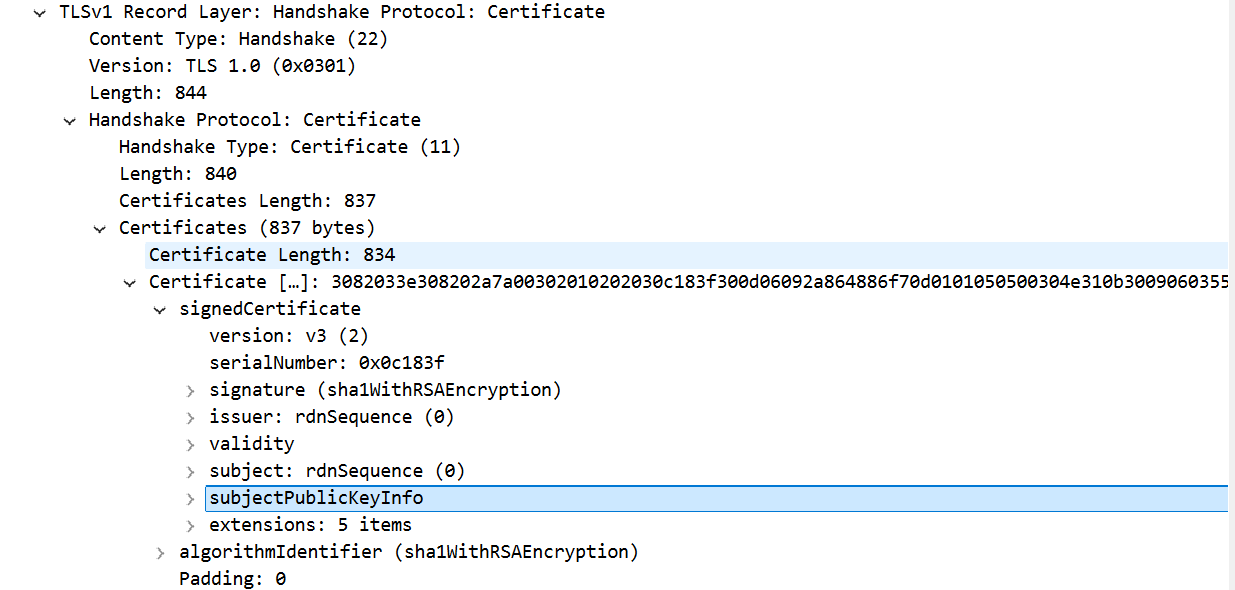
1. **Client Hello**  
   클라이언트가 서버에 Client Hello 메시지를 보냅니다. 지원하는 TLS 버전(1.0), Cipher Suites, 랜덤 값, 확장 정보 등이 포함됩니다.



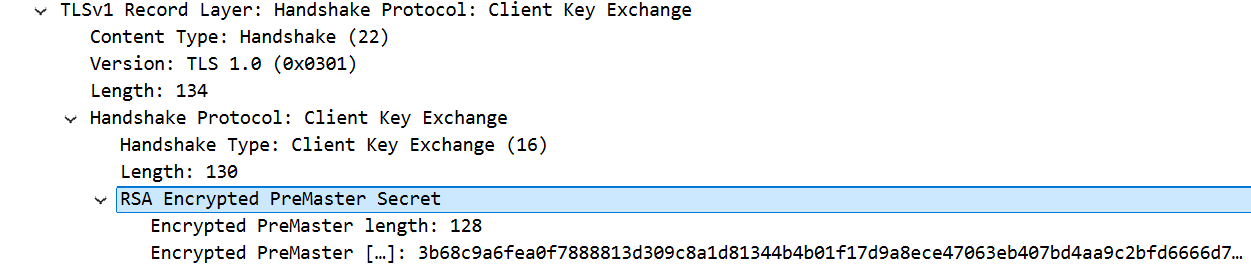
1. **Server Hello**  
   서버가 Server Hello 메시지로 응답합니다. 선택된 암호화 알고리즘(TLS RSA With RC4 128 MD5), 서버 인증서, 랜덤 값, 클라이언트 인증 요청 여부 등이 포함됩니다.



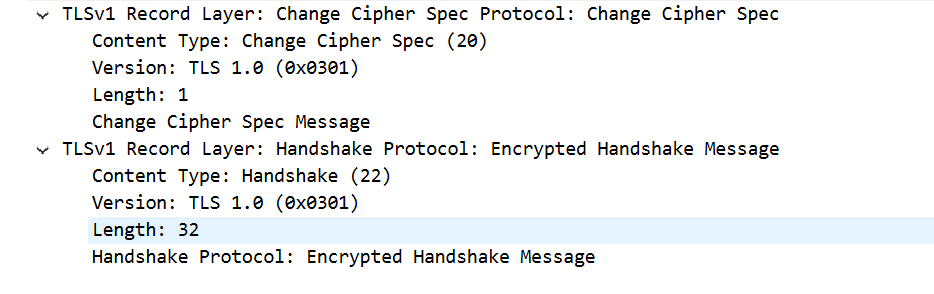
1. **인증서 검증**  
   클라이언트는 서버 인증서를 CA(Certificate Authority)를 통해 검증합니다. 도메인 일치 여부, 유효 기간, 서명 유효성이 포함됩니다.



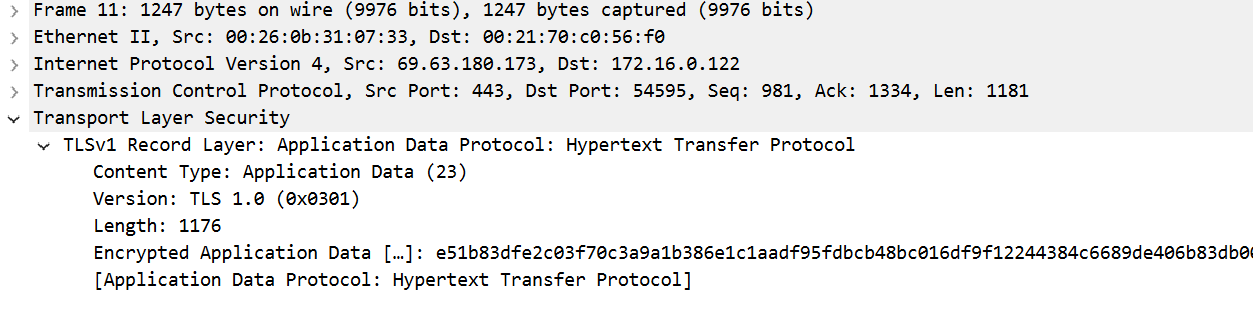
1. **Key Exchange**  
   클라이언트는 Pre-Master Secret을 생성하고 서버의 공개키로 암호화하여 전송합니다. 서버는 자신의 개인키로 이를 복호화합니다. 이후 클라이언트와 서버는 Client Random, Server Random, Pre-Master Secret을 기반으로 세션 키를 생성합니다.



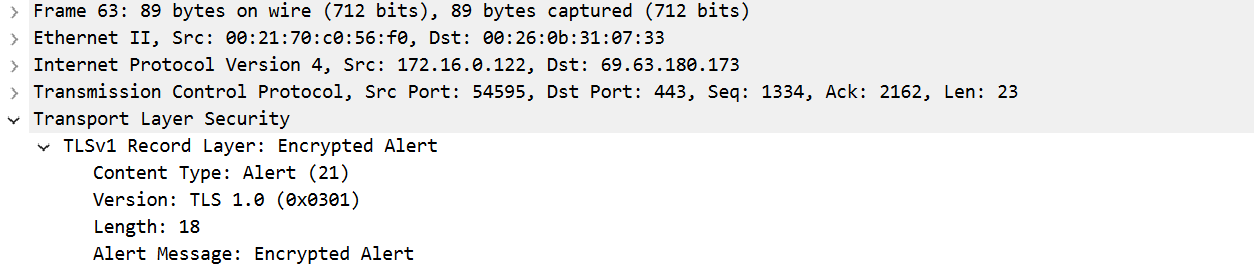
1. **Change Cipher Spec**  
   양측은 Change Cipher Spec 메시지를 교환하여 암호화 시작을 선언합니다.



1. **Finished**  
   이어서 Finished 메시지를 암호화하여 서로 전송합니다. TLS HandShake가 완료됩니다.
2. **암호화된 HTTP 데이터 전송**  
   이제부터 HTTP 요청/응답이 TLS Record로 암호화되어 TCP를 통해 전송됩니다. Encrypted Application Data로 표시됩니다.



1. **세션 종료**  
   클라이언트가 close\_notify Alert 메시지를 암호화하여 전송합니다.



1. **TCP 연결 종료**  
   TCP 연결이 FIN → ACK 순서로 종료됩니다.