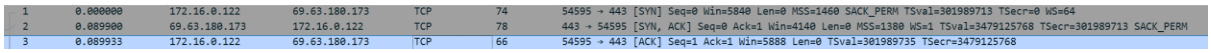
SSL 패킷 분석을 통한 HTTPS 통신 흐름 이해

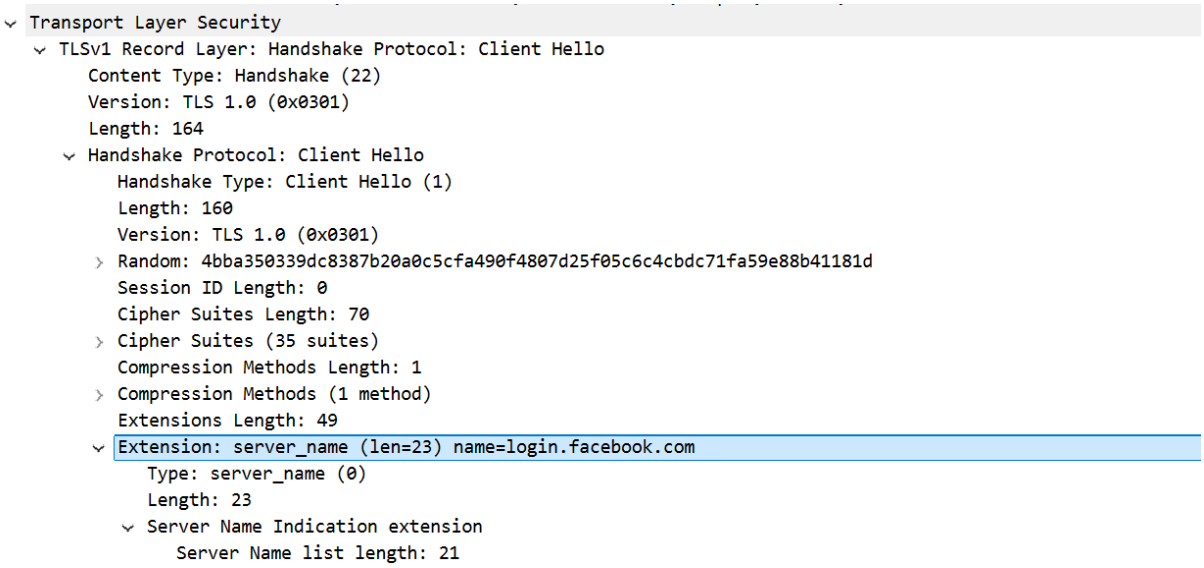
추적파일 기반으로 SSL Handshake 단계별 분석 및 시각화

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.



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



3. **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.

```
Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 70
    Version: TLS 1.0 (0x0301)
    Random: b9bb3b517aba70530291e8b0f97bb711647b94836658c94c504630a260363a71
    Session ID Length: 32
    Session ID: 798e78f8199088e83fcf3e2ece32d14d26bc29eda5eb914989f242f9277c1adf
    Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
    Compression Method: null (0)
    [JA3S Fullstring: 769,4,]
    [JA3S: 53611273a714cb4789c8222932efd5a7]
```

4. **인증서 검증**

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

```
TLSv1 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 844
  Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 840
      Certificates Length: 837
    Certificates (837 bytes)
        Certificate Length: 834
      Certificate […]: 3082033e308202a7a00302010202030c183f300d06092a864886f70d0101050500304e310b3009060355
        signedCertificate
            version: v3 (2)
            serialNumber: 0x0c183f
          signature (sha1WithRSAEncryption)
          issuer: rdnSequence (0)
          validity
          subject: rdnSequence (0)
          subjectPublicKeyInfo
          extensions: 5 items
        algorithmIdentifier (sha1WithRSAEncryption)
        Padding: 0
```

5. **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.

```
TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 134
  Handshake Protocol: Client Key Exchange
      Handshake Type: Client Key Exchange (16)
      Length: 130
    RSA Encrypted PreMaster Secret
        Encrypted PreMaster length: 128
        Encrypted PreMaster […]: 3b68c9a6fea0f7888813d309c8a1d81344b4b01f17d9a8ece47063eb407bd4aa9c2bfd6666d7…
```

6. **Change Cipher Spec**

   양측은 Change Cipher Spec 메시지를 교환하여 암호화 시작을 선언합니다.

```
TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.0 (0x0301)
    Length: 1
    Change Cipher Spec Message
TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 32
    Handshake Protocol: Encrypted Handshake Message
```

7. **Finished**

   이어서 Finished 메시지를 암호화하여 서로 전송합니다. TLS HandShake가 완료됩니다.

8. **암호화된 HTTP 데이터 전송**

   이제부터 HTTP 요청/응답이 TLS Record로 암호화되어 TCP를 통해 전송됩니다. Encrypted Application Data로 표시됩니다.

```
Frame 11: 1247 bytes on wire (9976 bits), 1247 bytes captured (9976 bits)
Ethernet II, Src: 00:26:0b:31:07:33, Dst: 00:21:70:c0:56:f0
Internet Protocol Version 4, Src: 69.63.180.173, Dst: 172.16.0.122
Transmission Control Protocol, Src Port: 443, Dst Port: 54595, Seq: 981, Ack: 1334, Len: 1181
Transport Layer Security
  TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 1176
      Encrypted Application Data […]: e51b83dfe2c03f70c3a9a1b386e1c1aadf95fdbcb48bc016df9f12244384c6689de406b83db0
      [Application Data Protocol: Hypertext Transfer Protocol]
```

9. **세션 종료**

   클라이언트가 close_notify Alert 메시지를 암호화하여 전송합니다.

```
Frame 63: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
Ethernet II, Src: 00:21:70:c0:56:f0, Dst: 00:26:0b:31:07:33
Internet Protocol Version 4, Src: 172.16.0.122, Dst: 69.63.180.173
Transmission Control Protocol, Src Port: 54595, Dst Port: 443, Seq: 1334, Ack: 2162, Len: 23
Transport Layer Security
  TLSv1 Record Layer: Encrypted Alert
      Content Type: Alert (21)
      Version: TLS 1.0 (0x0301)
      Length: 18
      Alert Message: Encrypted Alert
```

10. **TCP 연결 종료**

    TCP 연결이 FIN → ACK 순서로 종료됩니다.