Chapter 07. 애플리케이션 서비스

Cookie & SSL/TLS

목차

- HTTP 속성
- HTTP Cookie
- SSL/TLS

HTTP 속성

- **Stateless**
  HTTP는 통신이 끝나면 상태 정보를 유지 하지 않는다

  서버는 HTTP 요청에 대한 응답을 보내고 접속을 끊어 커넥션 리소스 비용을 줄인다

  단순 페이지 또는 문서 정보 열람은 가능

  하지만 클라이언트가 새로운 페이지를 접속 할 때마다 서버는 신원을 알 수 없다

  예를 들어, 인터넷 쇼핑몰의 경우 페이지 마다 인증이 필요

  회원 정보 식별, 로그인 여부, 결제 정보 및 장바구니 등

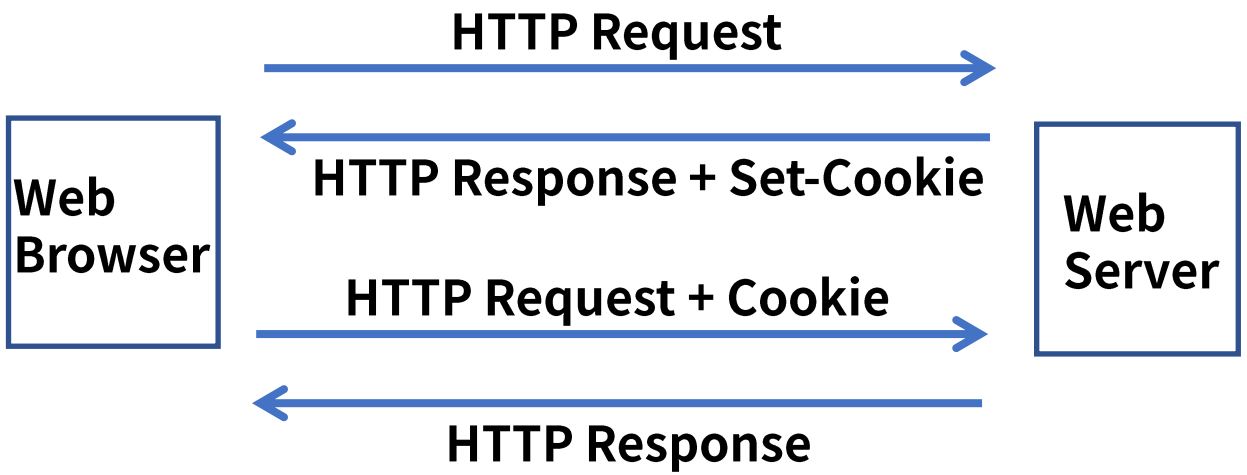
  해결책 = Cookie & Session

  Stateful: 상태 정보 유지

HTTP Cookie

- **정의**
  클라이언트 웹 브라우저 로컬에 저장되는 키와 값이 들어 있는 파일

  이름, 값, 도메인, 만료일, 경로 - 일정 시간 정보 저장 -> 로그인, 장바구니



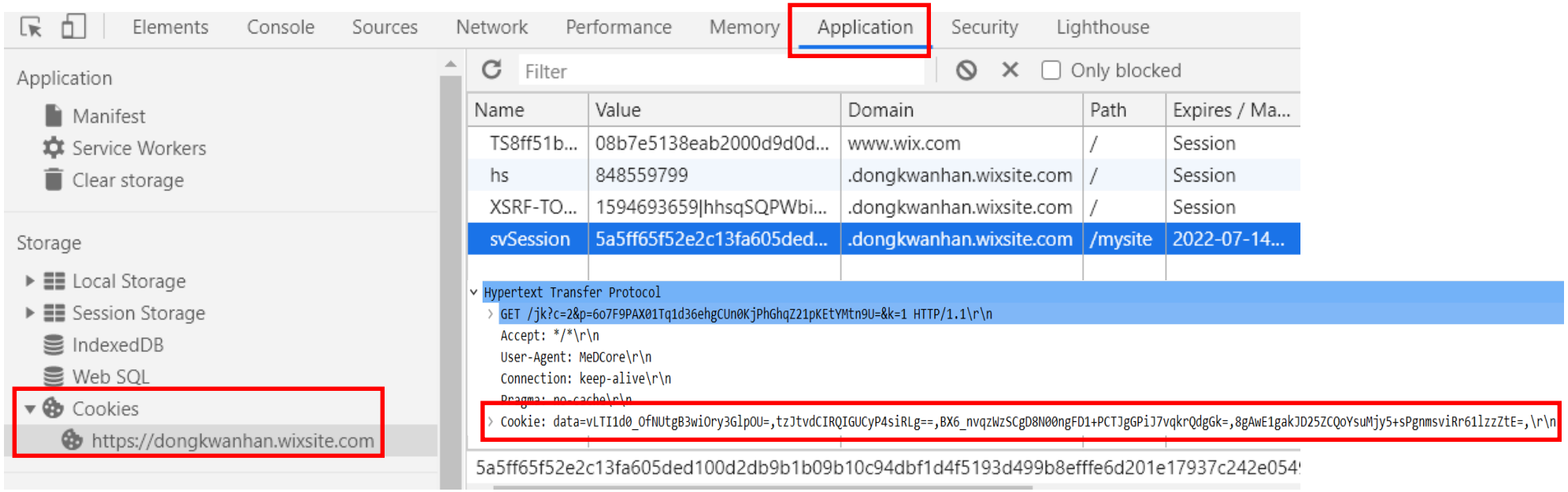
Session: 서버는 일정 시간 같은 웹브라우저의 요청이 들어오면 하나의 상태로 유지

서버는 클라이언트에 대한 세션ID 발급 및 보유 -> 쿠키로 전달 -> 동일 세션ID로 접속 -> 정보 확인

HTTP Cookie

- **Cookie 확인**

  웹브라우저(크롬)에서 웹사이트 접속 후 F12 클릭 - 메뉴 - Application - Cookie



Cookie는 사용자 로컬에 정보가 저장 - 유출 또는 조작 가능

Session은 서버에 정보를 저장(안전) - 인증에 세션을 사용 - 세션 하이재킹? - HTTPS - SSL/TLS

SSL/TLS

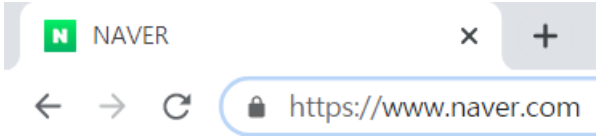
- **정의**

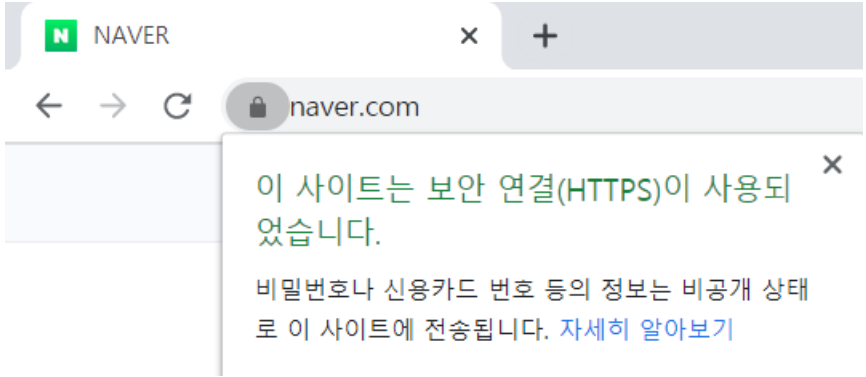
  SSL(Secure Socket Layer) / TLS(Transport Layer Security)
  TCP/IP 네트워크 통신간 보안을 제공하는 프로토콜

  Netscape SSL 1.0 -> SSL 2.0 -> SSL 3.0(1996년)

  IETF 1999년 TLS 1.0 -> TLS 1.1 -> TLS 1.2(SHA2) -> TLS 1.3(2018년) - 확장 SNI 암호

  HTTPS(Hypertext Transfer Protocol Secure) = HTTP over TLS





주요 웹 브라우저 2020년 상반기 TLS 1.0, TLS 1.1 지원 중단 - POODLE & BEAST 취약점

SSL/TLS

- **기능**
  인증 - Client to Server 통신 간 상대방에 대한 인증 - RSA, DSS

  무결성 - 메시지 인증 코드로 제공 HMAC - MD5, SHA-2

  기밀성 - 데이터 암호 - 3DES, RC4

- **프로토콜 구성**
  상위
  HandShake: 키 교환 방식, 암호화 방식, HMAC 방식 , 압축 방식 등을 협상

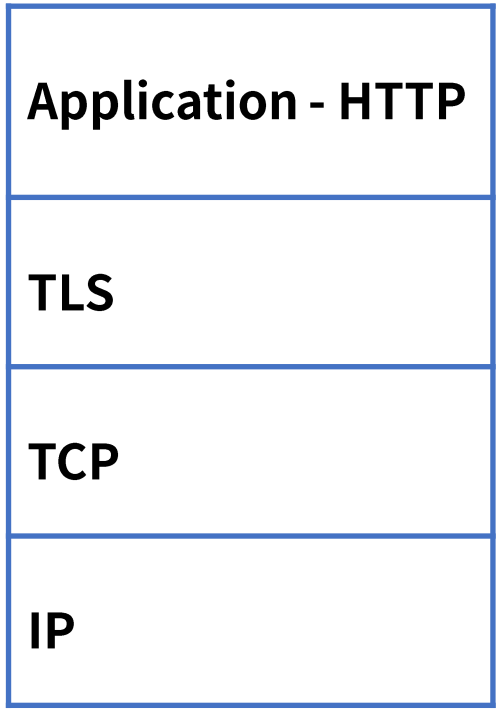
  Change Cipher Spec: 협상 정보가 적용됨을 알림

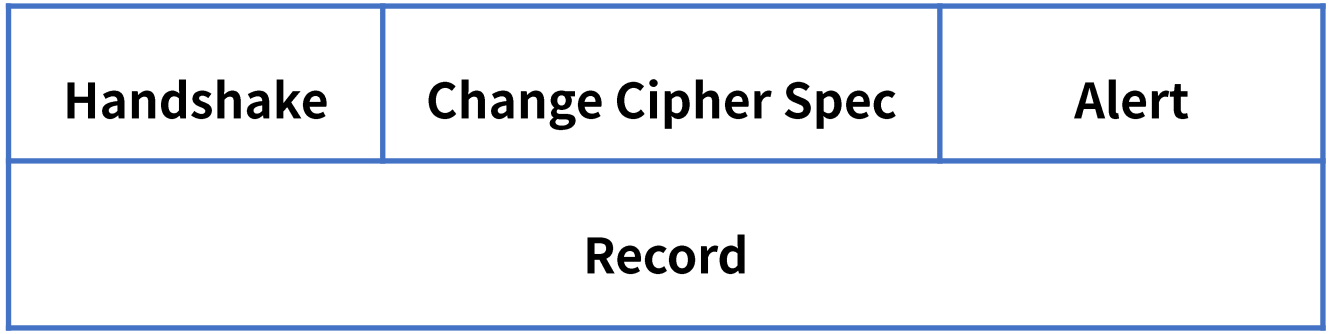
  Alert: 협상 과정에서 제시한 암호화 방식을 지원 못하는 경우 알림

  하위
  Record: 데이터 교환, 메시지를 전송

SSL/TLS

- **TLS Stack**

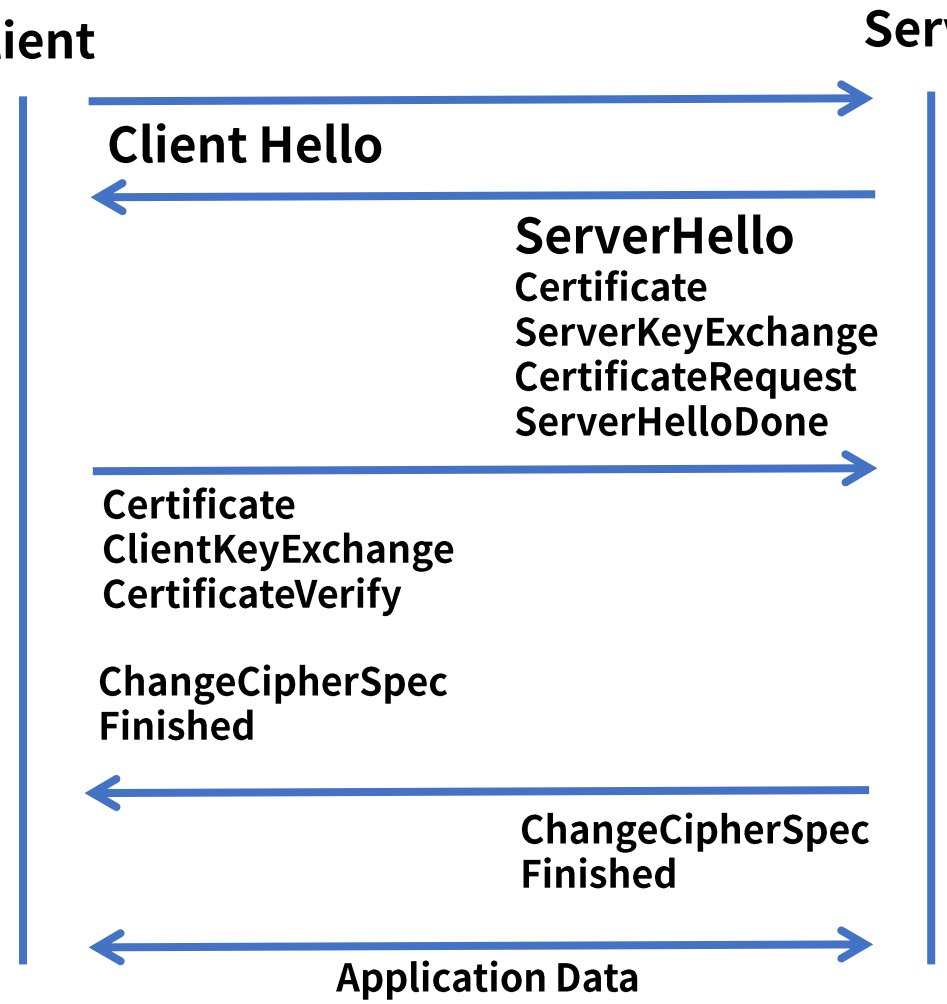




TLS 계층은 상위 3개 프로토콜, 하위 Record 프로토콜로 구분
상위 계층에서 협상 후 Record 프로토콜에서 Application 데이터를 분할, 압축, 암호화 해서 전달

SSL/TLS

- 동작 과정



1. 클라이언트는 지원 가능한 cipher suite 전달

2. 서버는 자신이 지원하는 cipher suite 전달

3. Certificate: 서버 인증서 전달
   ServerKeyExchange: DH 키교환 - 키 전달
   CertificateRequest: 인증서 요청
   ServerHelloDone: 모든 메시지 전달 완료

4. Certificate: 클라이언트 인증서 전달
   ClientKeyExchange: DH, 클라이언트 키 교환
   CertificateVerify: 인증서 확인

   버전, cipher suite 결정, 상대방 신원 확인 완료

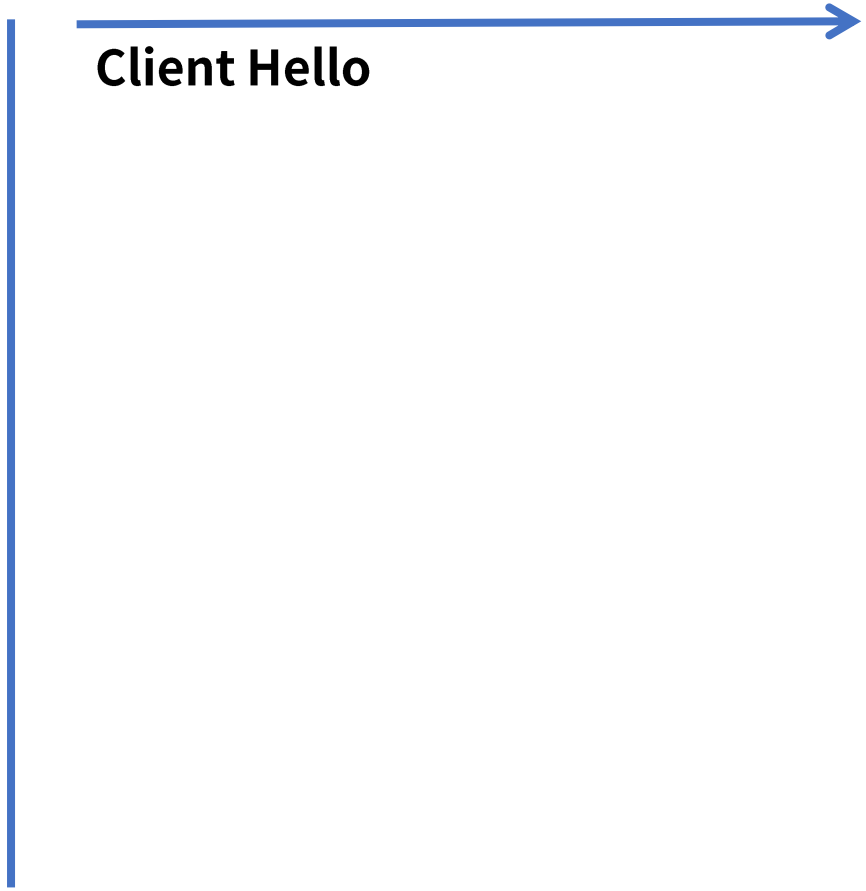
5. ChangeCipherSpec Finished
   TLSCiphertxt 전송, 협상된 키가 맞는지 검증

SSL/TLS

- 동작 과정

Client

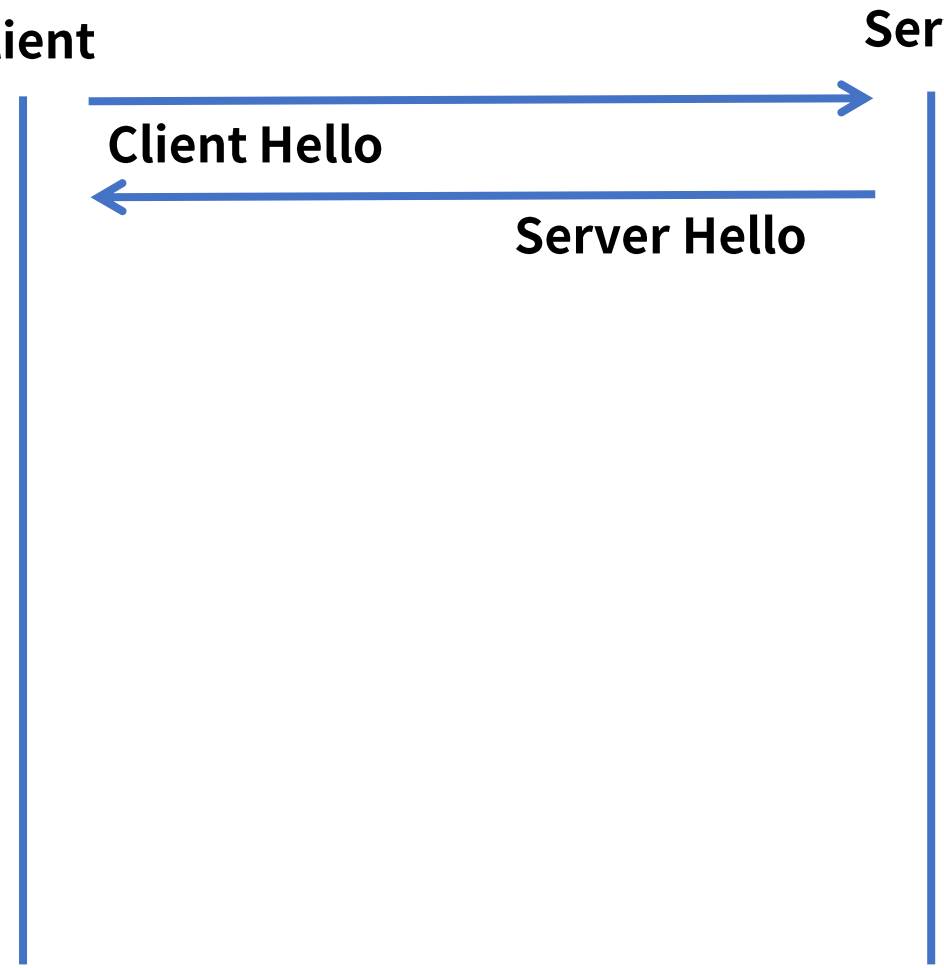
Server




```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 508
      Version: TLS 1.2 (0x0303)
    Random: 1ed5730df398acf1d0851ddb419f435e375069cf11640302…
      Session ID Length: 32
      Session ID: 04a20421b6485405b043ad68aa63ad46ad924574b22fc94d…
      Cipher Suites Length: 32
    Cipher Suites (16 suites)
      Cipher Suite: Reserved (GREASE) (0x8a8a)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
      Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
      Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
      Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
      Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
```

SSL/TLS

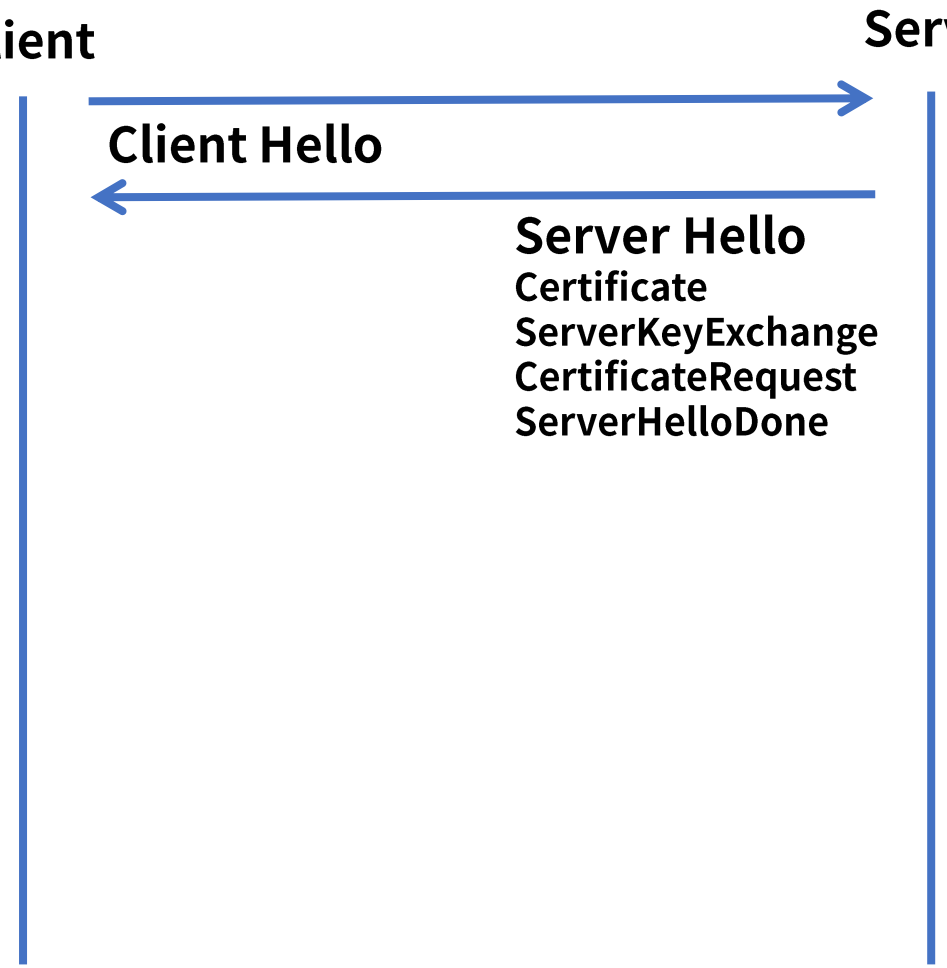
- 동작 과정




```
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 84
    ▼ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 80
        Version: TLS 1.2 (0x0303)
      ▶ Random: 142fd630405b54ff3b5864ce232d742064d0e54efde82c9e…
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 40
      ▶ Extension: renegotiation_info (len=1)
      ▶ Extension: server_name (len=0)
      ▶ Extension: ec_point_formats (len=4)
      ▶ Extension: session_ticket (len=0)
      ▶ Extension: status_request (len=0)
      ▶ Extension: application_layer_protocol_negotiation (len=11)
```

SSL/TLS

- 동작 과정

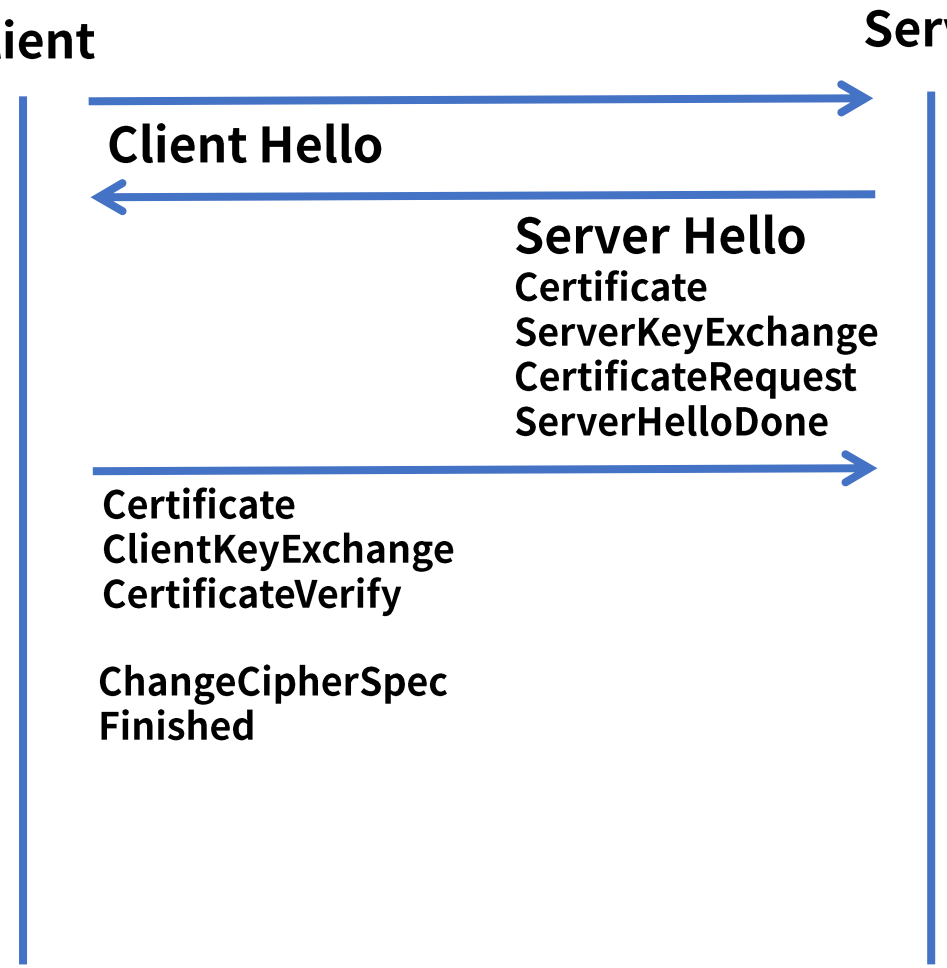



```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3189
    > Handshake Protocol: Certificate
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Certificate Status
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 479
    > Handshake Protocol: Certificate Status
```

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
    > Handshake Protocol: Server Key Exchange
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4
    > Handshake Protocol: Server Hello Done
```

SSL/TLS

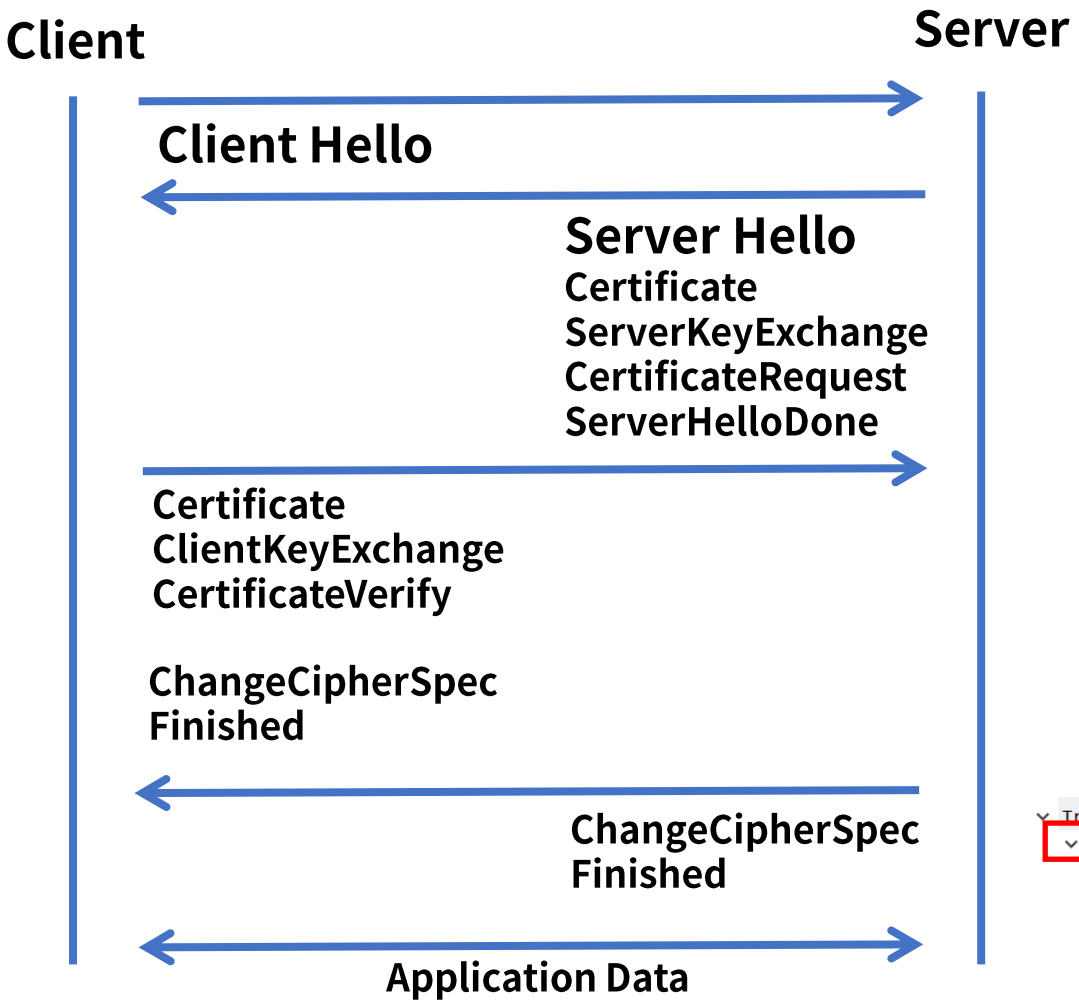
- 동작 과정

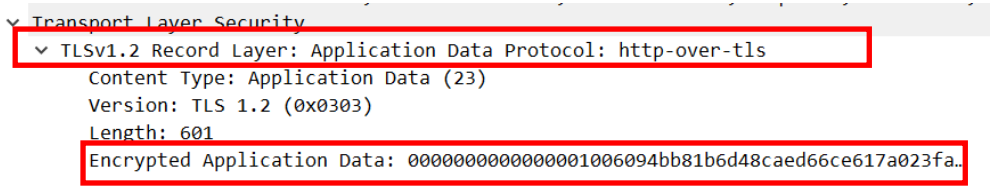



```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 66
      EC Diffie-Hellman Client Params
  TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

SSL/TLS

- 동작 과정





Wrap up

- HTTP는 Stateless로 통신이 끝나면 상태 정보를 유지 하지 않는다
- 상태 정보가 필요한 경우를 위해서 Cookie & Session 기술이 있다
- Cookie는 클라이언트 웹 브라우저 로컬에 저장되는 정보 - 로그인
- Session은 동일한 웹브라우저의 요청을 하나의 상태로 구분하여 서버에 정보를 저장
- SSL/TLS(Transport Layer Security)은 TCP/IP 통신간 보안을 제공하는 프로토콜
- TLS는 상위 HandShake, Change Cipher Spec, Alert, 하위 Record 프로토콜로 구성