

# HTTPS에서 바이너리 전송과정

## ▼ ChatGPT에게 물어보기



HTTPS와 HTTP에서 파일 전송과정이 어떻게 돼?



HTTP(Hypertext Transfer Protocol)와 HTTPS(HTTP Secure) 모두 파일 전송을 위한 프로토콜입니다. 두 프로토콜 모두 파일 전송을 위해서는 클라이언트가 서버에게 파일을 요청하고, 서버는 클라이언트에게 파일을 전송합니다.



그러나 HTTPS와 HTTP의 파일 전송 과정은 중요한 차이점이 있습니다. HTTPS는 SSL(Secure Sockets Layer) 또는 TLS(Transport Layer Security) 프로토콜을 사용하여 보안을 제공하므로, 전송되는 데이터가 암호화됩니다. 이와 달리, HTTP는 암호화되지 않으므로 전송되는 데이터는 쉽게 탈취될 수 있습니다.

따라서 HTTPS와 HTTP의 파일 전송 과정은 다음과 같은 차이가 있습니다.

### HTTP 파일 전송 과정

1. 클라이언트는 HTTP 요청을 서버에게 보냅니다. 이 요청은 일반 텍스트로 전송됩니다.
2. 서버는 요청을 받고, 요청한 파일을 찾아서 클라이언트에게 전송합니다. 이 파일은 일반적으로 바이너리 파일입니다.
3. 클라이언트는 서버로부터 받은 파일을 수신합니다. 이 파일은 일반적으로 바이너리 파일입니다.

HTTP의 파일 전송 과정에서는 데이터가 암호화되지 않기 때문에, 중간에 제3자가 데이터를 가로채서 파일의 내용을 확인할 수 있습니다.

### HTTPS 파일 전송 과정

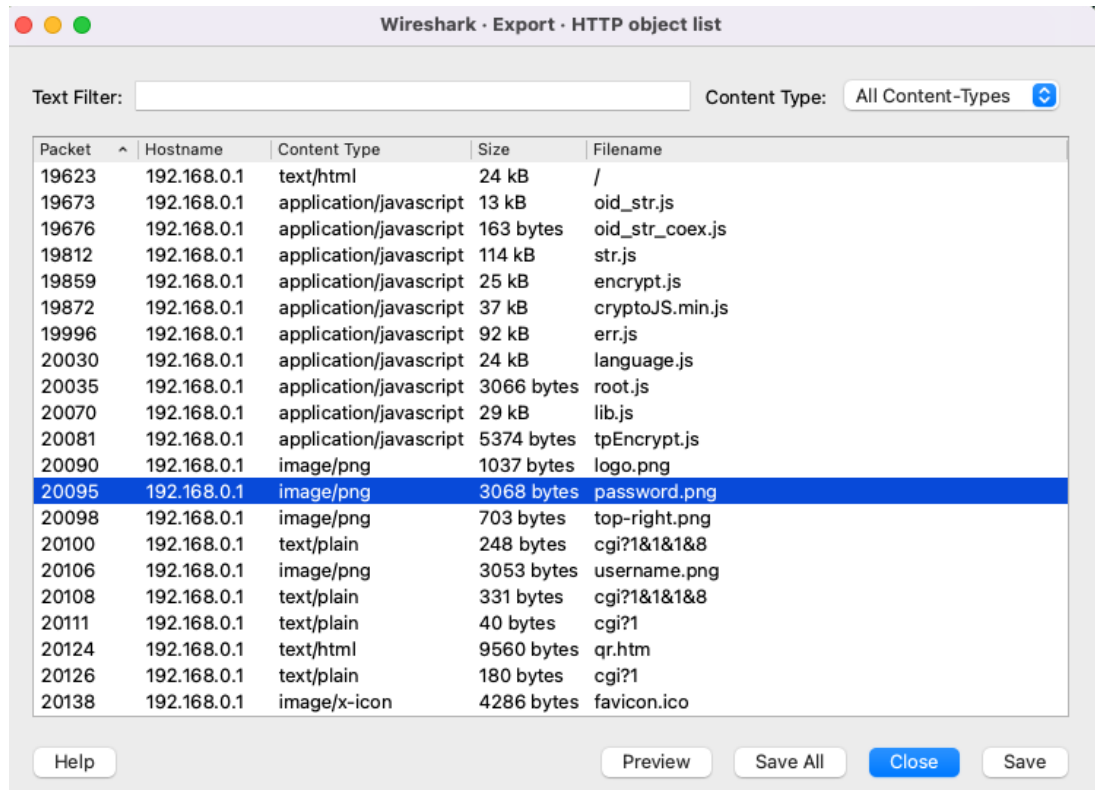
1. 클라이언트는 HTTPS 요청을 서버에게 보냅니다. 이 요청은 SSL/TLS 암호화된 데이터로 전송됩니다.
2. 서버는 요청을 받고, 요청한 파일을 찾아서 SSL/TLS 암호화된 데이터로 클라이언트에게 전송합니다. 이 파일은 일반적으로 바이너리 파일입니다.
3. 클라이언트는 SSL/TLS 암호화된 데이터를 수신하고, 대칭키를 사용하여 데이터를 복호화합니다. 이 파일은 일반적으로 바이너리 파일입니다.

HTTPS의 파일 전송 과정에서는 데이터가 SSL/TLS 프로토콜을 사용하여 암호화되기 때문에, 중간에 제3자가 데이터를 가로채도 데이터를 확인할 수 없습니다. 이를 통해 클라이언트와 서버 간의 통신이 안전하게 이루어집니다.

## HTTP, HTTPS 공통점과 차이점

- 공통점
  - 파일 전송을 위한 프로토콜

- 클라이언트가 서버에게 요청, 클라이언트에게 서버가 파일을 전송
- 차이점
  - HTTPS는 SSL, TLS 프로토콜로 암호화가 되어있어 데이터를 쉽게 탈취하지 못함
- ▼ WireShark를 활용한 HTTP, HTTPS 차이 보기



```
GET /js/str.js HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: */*
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.0.1/

HTTP/1.1 200 OK
Content-Type: application/javascript; charset=utf-8
Content-Length: 114439
Set-Cookie: JSESSIONID=deleted; SameSite=Lax; Expires=Thu, 01 Jan 1970 00:00:01 GMT; Path=/; HttpOnly
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff

var menu_str={status:".....",status6:"IPv6 .....",qs:".....",sysmod:".....",
.....,network:".....",wan:"WAN",wan6:"IPv6 WAN",ewan:"EWAN",usb3g:"3G/4G .....",group:".....",
.....,lan:"LAN",lan6:"IPv6 LAN",macclone:"MAC .....",alg:"ALG .....",dsl:"DSL .....",autopvc:"PVC .....",
.....,ipsec:"IPSec VPN",iptv:"IPTV",dhcp:"DHCP",dhcpserver:"DHCP .....",dhcpclient:"DHCP .....",
.....,address:".....",condnet:".....",dualband:".....",wlan:".....",wlan2g:"2.4GHz~5.2GHz.....",wlan5g:"5.8GHz~6.0GHz.....",wlan6g:"6.0GHz~6.8GHz.....",wlan7g:"6.8GHz~7.1GHz.....",wlan8g:"7.1GHz~7.9GHz.....",wlan9g:"7.9GHz~8.6GHz.....",wlan10g:"8.6GHz~10.0GHz.....",wlan11g:"10.0GHz~11.2GHz.....",wlan12g:"11.2GHz~12.5GHz.....",wlan13g:"12.5GHz~14.0GHz.....",wlan14g:"14.0GHz~15.0GHz.....",wlan15g:"15.0GHz~16.0GHz.....",wlan16g:"16.0GHz~17.0GHz.....",wlan17g:"17.0GHz~18.0GHz.....",wlan18g:"18.0GHz~19.0GHz.....",wlan19g:"19.0GHz~20.0GHz.....",wlan20g:"20.0GHz~21.0GHz.....",wlan21g:"21.0GHz~22.0GHz.....",wlan22g:"22.0GHz~23.0GHz.....",wlan23g:"23.0GHz~24.0GHz.....",wlan24g:"24.0GHz~25.0GHz.....",wlan25g:"25.0GHz~26.0GHz.....",wlan26g:"26.0GHz~27.0GHz.....",wlan27g:"27.0GHz~28.0GHz.....",wlan28g:"28.0GHz~29.0GHz.....",wlan29g:"29.0GHz~30.0GHz.....",wlan30g:"30.0GHz~31.0GHz.....",wlan31g:"31.0GHz~32.0GHz.....",wlan32g:"32.0GHz~33.0GHz.....",wlan33g:"33.0GHz~34.0GHz.....",wlan34g:"34.0GHz~35.0GHz.....",wlan35g:"35.0GHz~36.0GHz.....",wlan36g:"36.0GHz~37.0GHz.....",wlan37g:"37.0GHz~38.0GHz.....",wlan38g:"38.0GHz~39.0GHz.....",wlan39g:"39.0GHz~40.0GHz.....",wlan40g:"40.0GHz~41.0GHz.....",wlan41g:"41.0GHz~42.0GHz.....",wlan42g:"42.0GHz~43.0GHz.....",wlan43g:"43.0GHz~44.0GHz.....",wlan44g:"44.0GHz~45.0GHz.....",wlan45g:"45.0GHz~46.0GHz.....",wlan46g:"46.0GHz~47.0GHz.....",wlan47g:"47.0GHz~48.0GHz.....",wlan48g:"48.0GHz~49.0GHz.....",wlan49g:"49.0GHz~50.0GHz.....",wlan50g:"50.0GHz~51.0GHz.....",wlan51g:"51.0GHz~52.0GHz.....",wlan52g:"52.0GHz~53.0GHz.....",wlan53g:"53.0GHz~54.0GHz.....",wlan54g:"54.0GHz~55.0GHz.....",wlan55g:"55.0GHz~56.0GHz.....",wlan56g:"56.0GHz~57.0GHz.....",wlan57g:"57.0GHz~58.0GHz.....",wlan58g:"58.0GHz~59.0GHz.....",wlan59g:"59.0GHz~60.0GHz.....",wlan60g:"60.0GHz~61.0GHz.....",wlan61g:"61.0GHz~62.0GHz.....",wlan62g:"62.0GHz~63.0GHz.....",wlan63g:"63.0GHz~64.0GHz.....",wlan64g:"64.0GHz~65.0GHz.....",wlan65g:"65.0GHz~66.0GHz.....",wlan66g:"66.0GHz~67.0GHz.....",wlan67g:"67.0GHz~68.0GHz.....",wlan68g:"68.0GHz~69.0GHz.....",wlan69g:"69.0GHz~70.0GHz.....",wlan70g:"70.0GHz~71.0GHz.....",wlan71g:"71.0GHz~72.0GHz.....",wlan72g:"72.0GHz~73.0GHz.....",wlan73g:"73.0GHz~74.0GHz.....",wlan74g:"74.0GHz~75.0GHz.....",wlan75g:"75.0GHz~76.0GHz.....",wlan76g:"76.0GHz~77.0GHz.....",wlan77g:"77.0GHz~78.0GHz.....",wlan78g:"78.0GHz~79.0GHz.....",wlan79g:"79.0GHz~80.0GHz.....",wlan80g:"80.0GHz~81.0GHz.....",wlan81g:"81.0GHz~82.0GHz.....",wlan82g:"82.0GHz~83.0GHz.....",wlan83g:"83.0GHz~84.0GHz.....",wlan84g:"84.0GHz~85.0GHz.....",wlan85g:"85.0GHz~86.0GHz.....",wlan86g:"86.0GHz~87.0GHz.....",wlan87g:"87.0GHz~88.0GHz.....",wlan88g:"88.0GHz~89.0GHz.....",wlan89g:"89.0GHz~90.0GHz.....",wlan90g:"90.0GHz~91.0GHz.....",wlan91g:"91.0GHz~92.0GHz.....",wlan92g:"92.0GHz~93.0GHz.....",wlan93g:"93.0GHz~94.0GHz.....",wlan94g:"94.0GHz~95.0GHz.....",wlan95g:"95.0GHz~96.0GHz.....",wlan96g:"96.0GHz~97.0GHz.....",wlan97g:"97.0GHz~98.0GHz.....",wlan98g:"98.0GHz~99.0GHz.....",wlan99g:"99.0GHz~100.0GHz.....",wlan100g:"100.0GHz~101.0GHz.....",wlan101g:"101.0GHz~102.0GHz.....",wlan102g:"102.0GHz~103.0GHz.....",wlan103g:"103.0GHz~104.0GHz.....",wlan104g:"104.0GHz~105.0GHz.....",wlan105g:"105.0GHz~106.0GHz.....",wlan106g:"106.0GHz~107.0GHz.....",wlan107g:"107.0GHz~108.0GHz.....",wlan108g:"108.0GHz~109.0GHz.....",wlan109g:"109.0GHz~110.0GHz.....",wlan110g:"110.0GHz~111.0GHz.....",wlan111g:"111.0GHz~112.0GHz.....",wlan112g:"112.0GHz~113.0GHz.....",wlan113g:"113.0GHz~114.0GHz.....",wlan114g:"114.0GHz~115.0GHz.....",wlan115g:"115.0GHz~116.0GHz.....",wlan116g:"116.0GHz~117.0GHz.....",wlan117g:"117.0GHz~118.0GHz.....",wlan118g:"118.0GHz~119.0GHz.....",wlan119g:"119.0GHz~120.0GHz.....",wlan120g:"120.0GHz~121.0GHz.....",wlan121g:"121.0GHz~122.0GHz.....",wlan122g:"122.0GHz~123.0GHz.....",wlan123g:"123.0GHz~124.0GHz.....",wlan124g:"124.0GHz~125.0GHz.....",wlan125g:"125.0GHz~126.0GHz.....",wlan126g:"126.0GHz~127.0GHz.....",wlan127g:"127.0GHz~128.0GHz.....",wlan128g:"128.0GHz~129.0GHz.....",wlan129g:"129.0GHz~130.0GHz.....",wlan130g:"130.0GHz~131.0GHz.....",wlan131g:"131.0GHz~132.0GHz.....",wlan132g:"132.0GHz~133.0GHz.....",wlan133g:"133.0GHz~134.0GHz.....",wlan134g:"134.0GHz~135.0GHz.....",wlan135g:"135.0GHz~136.0GHz.....",wlan136g:"136.0GHz~137.0GHz.....",wlan137g:"137.0GHz~138.0GHz.....",wlan138g:"138.0GHz~139.0GHz.....",wlan139g:"139.0GHz~140.0GHz.....",wlan140g:"140.0GHz~141.0GHz.....",wlan141g:"141.0GHz~142.0GHz.....",wlan142g:"142.0GHz~143.0GHz.....",wlan143g:"143.0GHz~144.0GHz.....",wlan144g:"144.0GHz~145.0GHz.....",wlan145g:"145.0GHz~146.0GHz.....",wlan146g:"146.0GHz~147.0GHz.....",wlan147g:"147.0GHz~148.0GHz.....",wlan148g:"148.0GHz~149.0GHz.....",wlan149g:"149.0GHz~150.0GHz.....",wlan150g:"150.0GHz~151.0GHz.....",wlan151g:"151.0GHz~152.0GHz.....",wlan152g:"152.0GHz~153.0GHz.....",wlan153g:"153.0GHz~154.0GHz.....",wlan154g:"154.0GHz~155.0GHz.....",wlan155g:"155.0GHz~156.0GHz.....",wlan156g:"156.0GHz~157.0GHz.....",wlan157g:"157.0GHz~158.0GHz.....",wlan158g:"158.0GHz~159.0GHz.....",wlan159g:"159.0GHz~160.0GHz.....",wlan160g:"160.0GHz~161.0GHz.....",wlan161g:"161.0GHz~162.0GHz.....",wlan162g:"162.0GHz~163.0GHz.....",wlan163g:"163.0GHz~164.0GHz.....",wlan164g:"164.0GHz~165.0GHz.....",wlan165g:"165.0GHz~166.0GHz.....",wlan166g:"166.0GHz~167.0GHz.....",wlan167g:"167.0GHz~168.0GHz.....",wlan168g:"168.0GHz~169.0GHz.....",wlan169g:"169.0GHz~170.0GHz.....",wlan170g:"170.0GHz~171.0GHz.....",wlan171g:"171.0GHz~172.0GHz.....",wlan172g:"172.0GHz~173.0GHz.....",wlan173g:"173.0GHz~174.0GHz.....",wlan174g:"174.0GHz~175.0GHz.....",wlan175g:"175.0GHz~176.0GHz.....",wlan176g:"176.0GHz~177.0GHz.....",wlan177g:"177.0GHz~178.0GHz.....",wlan178g:"178.0GHz~179.0GHz.....",wlan179g:"179.0GHz~180.0GHz.....",wlan180g:"180.0GHz~181.0GHz.....",wlan181g:"181.0GHz~182.0GHz.....",wlan182g:"182.0GHz~183.0GHz.....",wlan183g:"183.0GHz~184.0GHz.....",wlan184g:"184.0GHz~185.0GHz.....",wlan185g:"185.0GHz~18
```

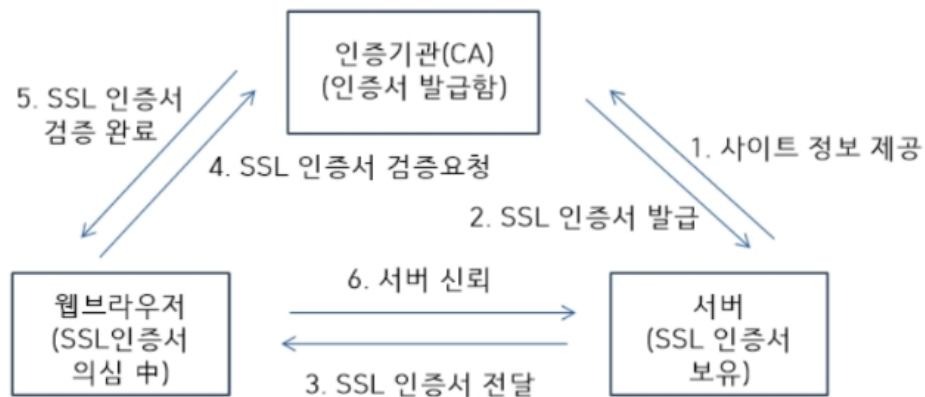
```

.....8....(
...+^'...T...N...>N...*...X...C...i...M...l...+.../...0.../...5...jj...
...+...ZZ...3...+...&-...b3'^l..G..!..L=..Wa..
..b...y...h2..http/1.1.#...Dl...h2..
.....
.....me.go.kr:...M..
rXF.J...Xr.r
.....+...
..TX...M...+5-...m6...'.d.K.A...r{b...+..
...A.#...P...l...5...qb...t...^b..i...|4*A.=&..@L...P}..R...YM.&g0...X...6.R...bw...a...96...M..
4.10~...L\...P...E...~)x.%N...".^...N?...((..26)...Z...v...G...S.K...9...r..I...RQ
...*.X...C...i...M...l...+...3...$...{...G...EX...X#...*..
..B[.0atg...~F.5...#...E.\F.D...T.:A...8...X...{...$..2..u...}.(.z...
...8...o...7...A..0F.4q.$..VX..T..v..qN...U...X..WyL...G.../...NmRF1...6U3..r...
..].h...n...%q.F@...@...F...5..V...S...5..4.h...E..jZ...2...S..u..3..W..b#...V...!@..]
(..K...=..SU...gl...<.UV'.E...^a..Q...4K...".Gfi...p...2...lp...p...QB...+..
..5...ij)...E.3.M...x.$..E..f"o..I...h...=..&h...=...@?...3...4*...((...hC...&...i...8v..o..M...n..L..q...Z...#...>?"uS4u..
{...Z
...i...@...{...U...
...W...zRp?...e.2...l!jp..hrc..w..u...;...=.|.}.a.9i..t...n...<..y...
..i..+T...n..5TEZ...15...cd...v...hD...nD4...76a...R.F...m.EK...

```

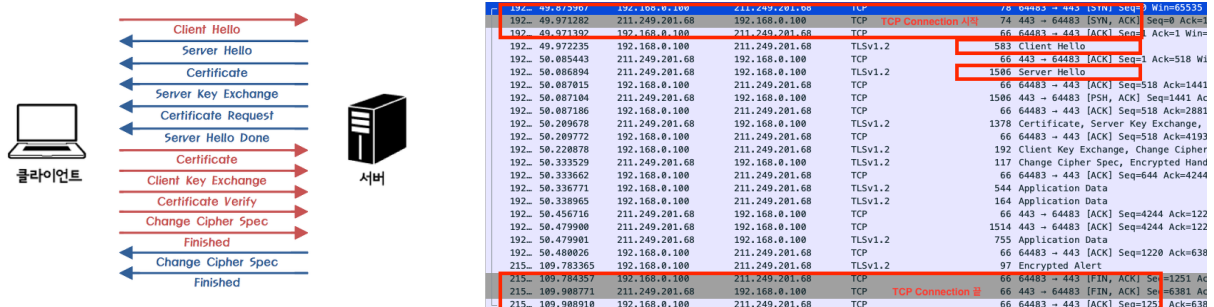
## HTTPS 파일 전송

- 암호화 검증과정



- 전송과정

- 클라이언트는 HTTPS를 활용해 서버에게 보낸다. (TLS/SSL 암호화 됨)
- 서버는 요청을 받고 파일을 찾아 암호화된 데이터를 클라이언트로 전달
- 클라이언트에서 수신하고 대칭키를 사용해 데이터를 복호화한다.

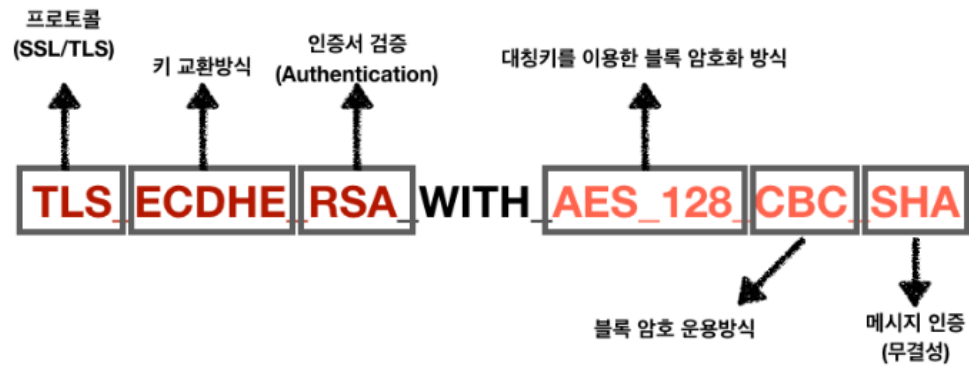


## ▼ 상세 처리 과정

### 1) Client Hello(Client → Server)

- 자신이 사용할 SSL 버전 정보, Cipher suite list[대칭키암호화 시스템 + 공개키 암호화 시스템 + 해시함수], 클라이언트 난수 생성후 전달

### ▼ CipherSuite List



<Cipher Suite의 구성>

```

▼ 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: f17225f14e937a2b2a28474daca742fc38738791f3b1cfc8a9cb5c72d2ec1f39
    Session ID Length: 32
    Session ID: 01c69c49433a74d6bd7075088701d4b85cc2d79c18ac37fafc1d37d749ca081d
    Cipher Suites Length: 42
  ▼ Cipher Suites (21 suites)
    Cipher Suite: Reserved (GREASE) (0x7a7a)
    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_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03d)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc008)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc007)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc000)
    Cipher Suite: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc001)
    Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
    Compression Methods Length: 1
  
```

## 2) Server Hello(Server → Client)

- 암호화 방법을 선택하고 서버난수를 생성해서 보낸다.

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 108
  Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 104
    Version: TLS 1.2 (0x0303)
  Random: 74cf055c18d74c1c475d74c1c91d4ea14f97d6284527007cfa76cbba5b175bc7
  Session ID Length: 32
  Session ID: 26335b5551090d4ce70d0daa7f30f3e2b6ee4c8a686b43d491a4d9fc53873a95
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  Compression Method: null (0)
  Extensions Length: 32
  Extension: server_name (len=0)
  Extension: renegotiation_info (len=1)
  Extension: ec_point_formats (len=4)
```

## 3) Certificate (Server → Client)

- 클라이언트는 CA의 공개키로 이 인증서를 해독해 서버의 공개키를 획득한다.

### ▼ 이미지

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 3727
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 3723
    Certificates Length: 3720
  Certificates (3720 bytes)
    Certificate Length: 1630
  Certificate: 3082065a30820542a00302010202100ce26754eca17d1c7048909ef51c1b25300d06092a... (id-at-commonName=*.kakao...)
    signedCertificate
      version: v3 (2)
      serialNumber: 0x0ce26754eca17d1c7048909ef51c1b25
      signature (sha256WithRSAEncryption)
        Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
      issuer: rdnSequence (0)
      validity
      subject: rdnSequence (0)
      subjectPublicKeyInfo
      extensions: 10 items
      algorithmIdentifier (sha256WithRSAEncryption)
      Padding: 0
      encrypted: 9fb81fa1e408acf2dfe211bcd374cc2c8c8386acecf75a43d41b370b32b84c40cae9e05...
    Certificate Length: 1167
  Certificate: 3082048b30820373a0030201020210090ee8c5de5bfa62d2ae2ff7097c4857300d06092a... (id-at-commonName=Thawte TI
    signedCertificate
      algorithmIdentifier (sha256WithRSAEncryption)
      Padding: 0
      encrypted: ba926d0a038b136f6558a44066fee2f61cbfe9657f41ecbfe16c9e0d72805eed5e7aa029...
    Certificate Length: 914
  Certificate: 3082038e30820276a0030201020210033af1e6a711a9a0bb2864b11d09fae5300d06092a... (id-at-commonName=DigiCert
    signedCertificate
      algorithmIdentifier (sha256WithRSAEncryption)
      Padding: 0
      encrypted: 606728946f0e4863eb31ddea6718d5897d3cc58b4a7fe9hedh2h17dfh05f73772a321339...
```

- 클라이언트는 클라이언트와 서버의 난수를 각각 사용해 Pre-Master-Secret(난수값) 생성
- PMS를 서버의 공개키로 암호화 해 서버에게 보내면 서버는 개인키를 활용해 암호문을 복호화 한다.

- 암호문이 복호화가 제대로 이루어지면 서버는 클라이언트에게 인증할 수 있다.

#### 4) Server Key Exchange(Server → Client)

- 인증서가 없거나 인증서가 서명용으로만 사용되어질 때 해당 메시지를 보낸다.
- 인증서 내부에 공개키가 있다면 Client가 CA 공개키를 통해 인증서를 복호화한 후 Server 공개키를 확보할 수 있음

#### 5) Server hello Done(Server → Client)

- 서버가 클라이언트에게 보낼 메시지를 모두 보냈음을 의미

#### 6) Client Key Exchange(Client → Server)

- PMS, 대칭 암호화키, 메시지 인증코드에 사용되는 46byte의 난수, 서버의 공개키로 만든 암호등이 포함

#### 7) Change Cipher Spec(Client → Server)

- 이후에 전송되는 모든 메시지는 서버와 협상된 알고리즘과 키를 이용해 암호화 시키겠다고 서버에 알림

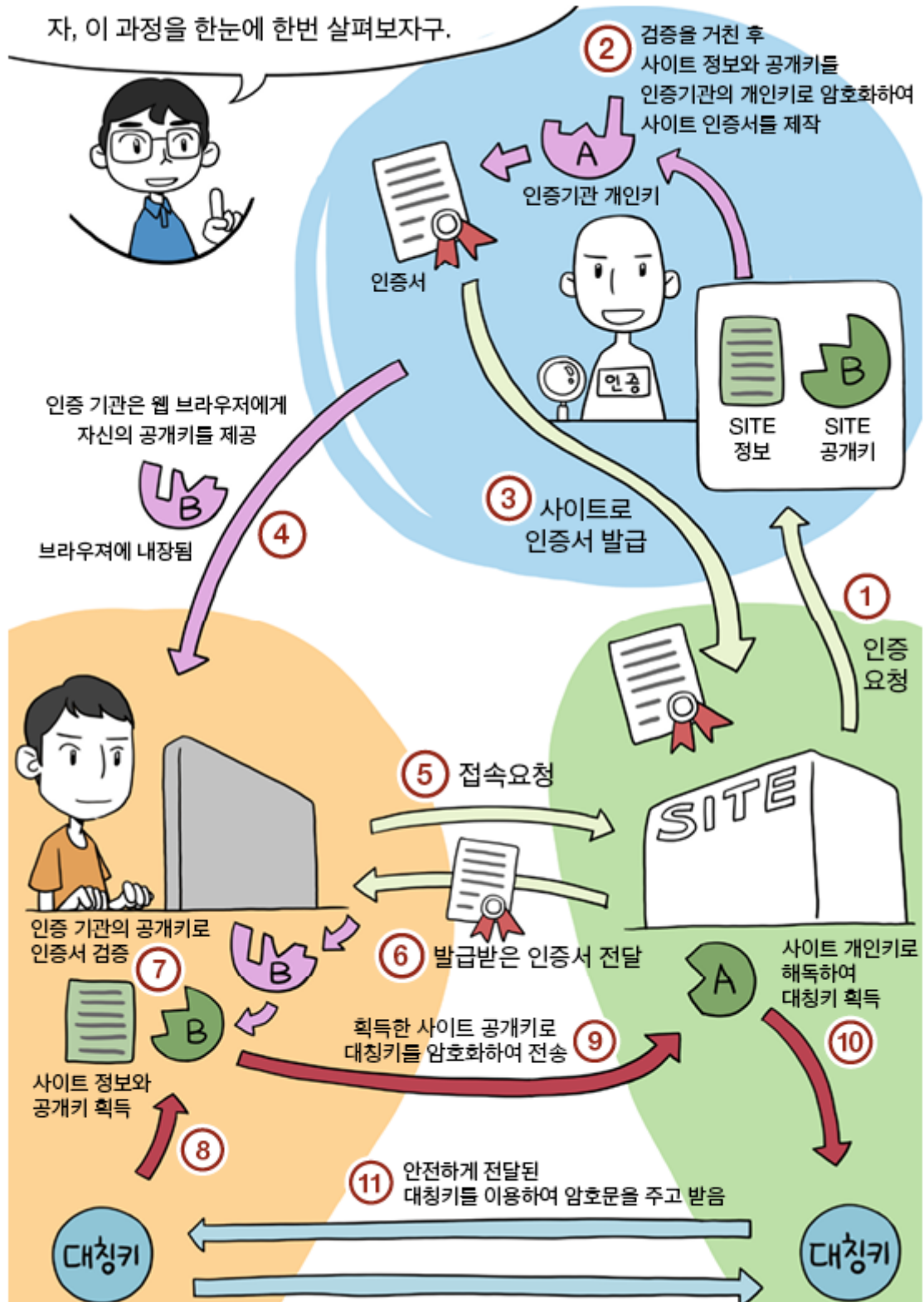
#### 8) Encrypted HandShake Message(Finished)

- 서버도 handShake가 성공적으로 완료됨을 알림. 지금부터 각자의 동일한 대칭키를 사용해 데이터를 암호화해 전송하거나 데이터를 복호화함.

#### 9) Application Data

서로 상대방에게 전송할 데이터를 암호화 해서 전송

**정리하자면!**



<HTTPS 통신 과정(출처 : 미닉스 김인성님 블로그)>

## 참고

<https://aws-hyoh.tistory.com/34>

<https://aws-hyoh.tistory.com/entry/HTTPS-통신과정-쉽게-이해하기-3SSL-Handshake>

[https://velog.io/@kaitlin\\_k/HTTPS-이해하기](https://velog.io/@kaitlin_k/HTTPS-이해하기)