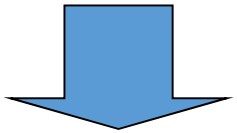
SSL/TLS Protocol

암호화의 역할

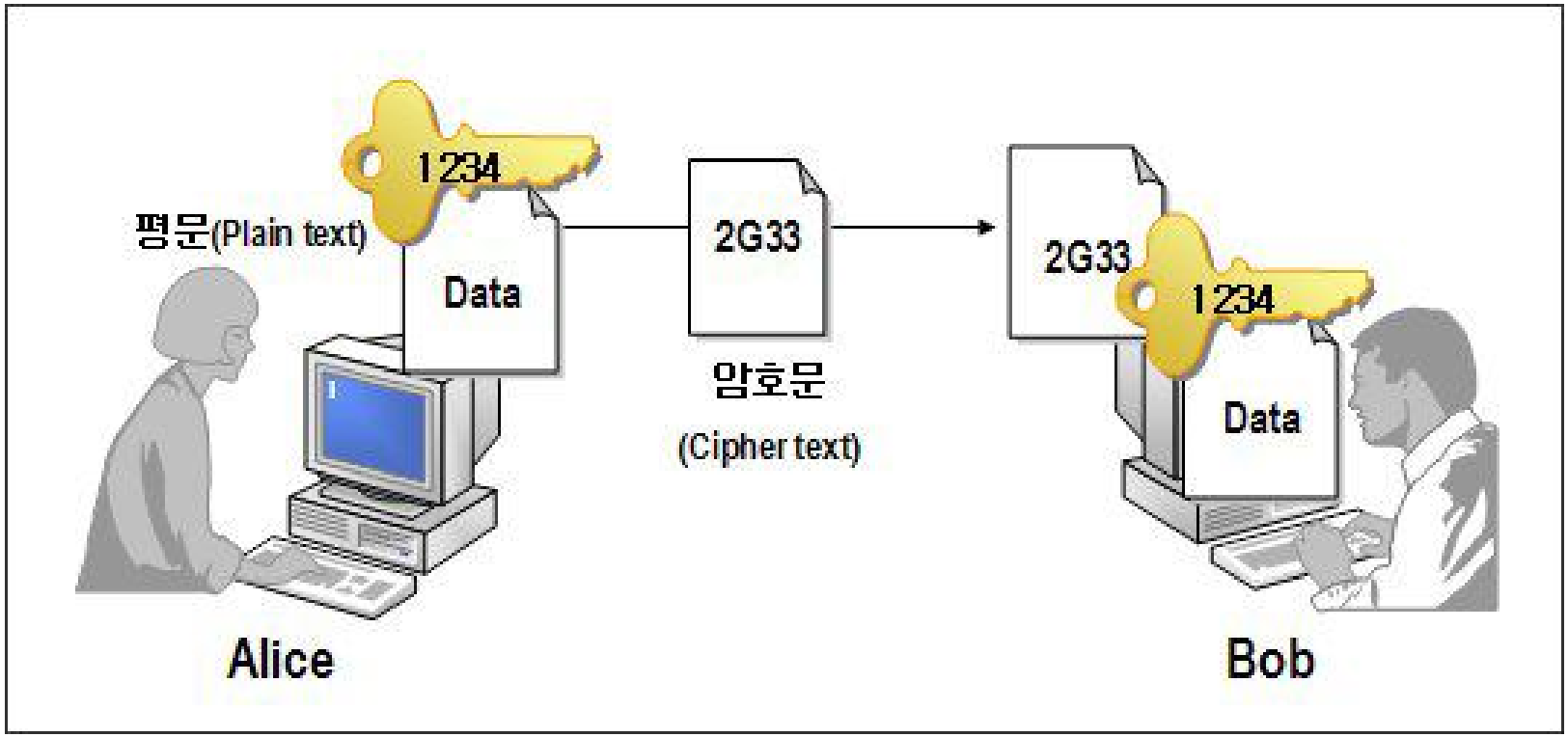
- Confidentiality (기밀성)
- Authenticity (신뢰성)
- Integrity (무결성)



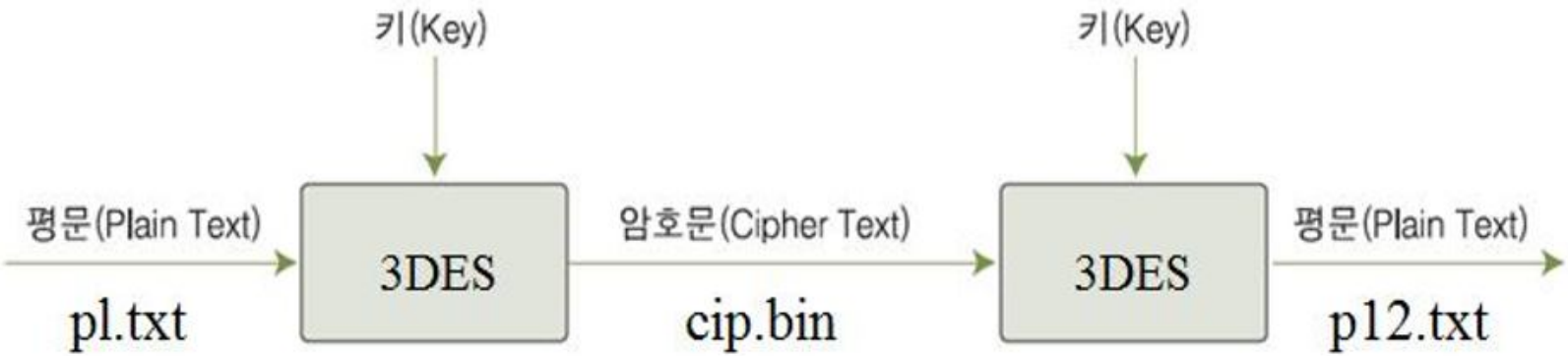
Key를 이용한 암호화 기술로서 해결

Symmetric Key(대칭키)

- Encryption Key = Decryption Key



- DES, 3DES 등의 프로토콜이 해당됨

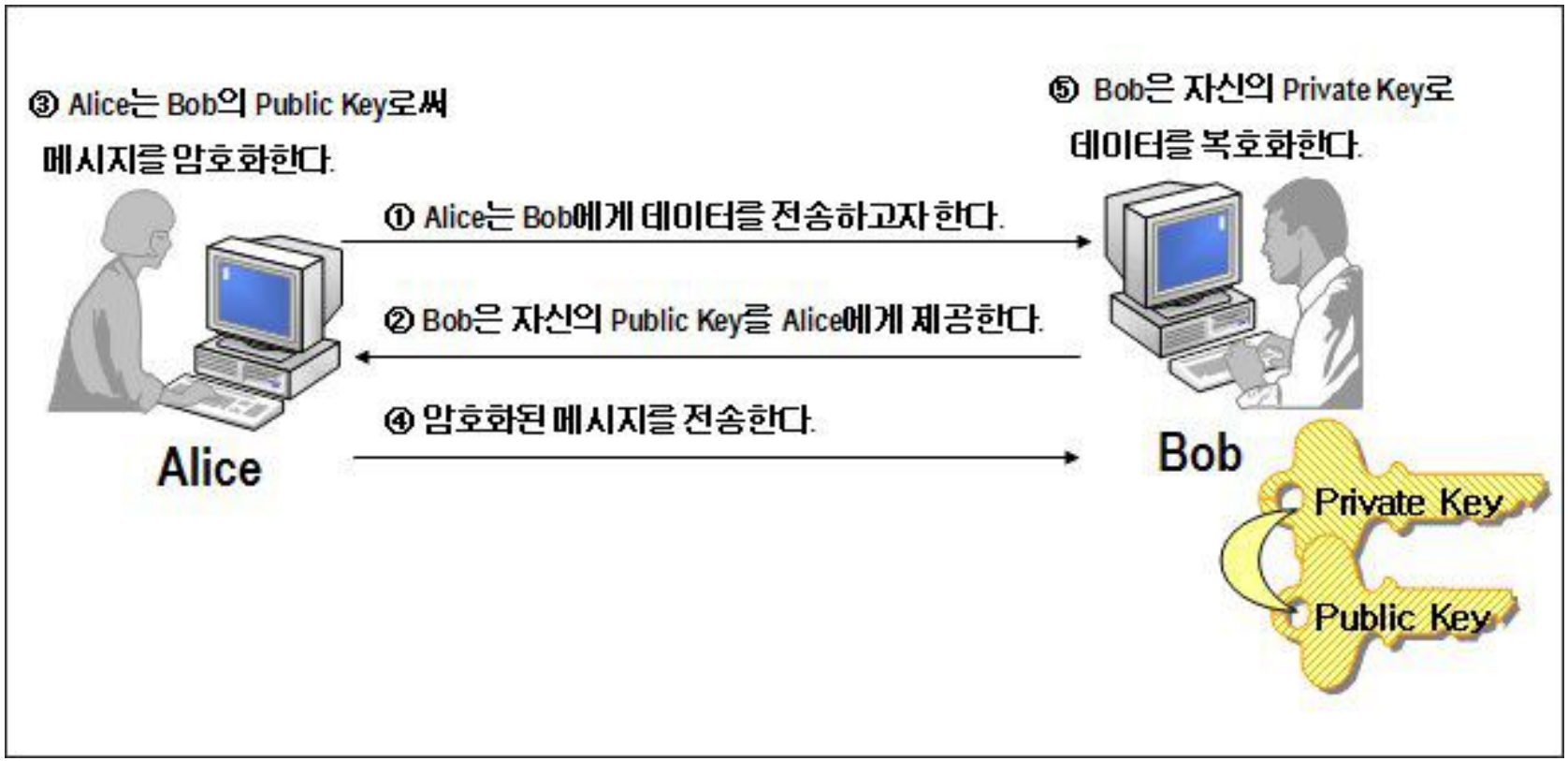


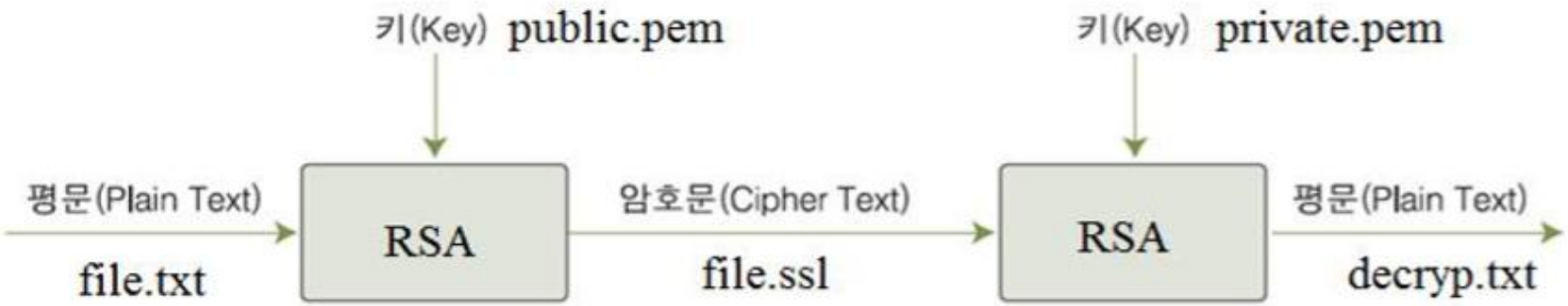
암호화	echo 'this is the plain text' > pl.txt openssl enc -e -des3 -salt -in pl.txt -out cip.bin · enc -e -des3 : des3 방식으로 암호화 · -in pl.txt -out cip.bin : pl.txt 파일의 암호화 한 결과를 cip.bin 파일에 저장
복호화	openssl enc -d -des3 -in cip.bin -out p2.txt · enc -d –des3 : cip.bin 파일을 p2.txt 파일로 복호화

Public Key (공용키)

- Encryption Key ≠ Decryption Key
  - 비대칭키, 공용키, 페어(Pair)키에 해당함
- Public Key와 Private Key로 구성
  - Public Key(공용키) = 공개가 되는 키
  - Private Key(개인키) = 오직 발행주체만이 가지는 비밀키
- RSA 알고리즘

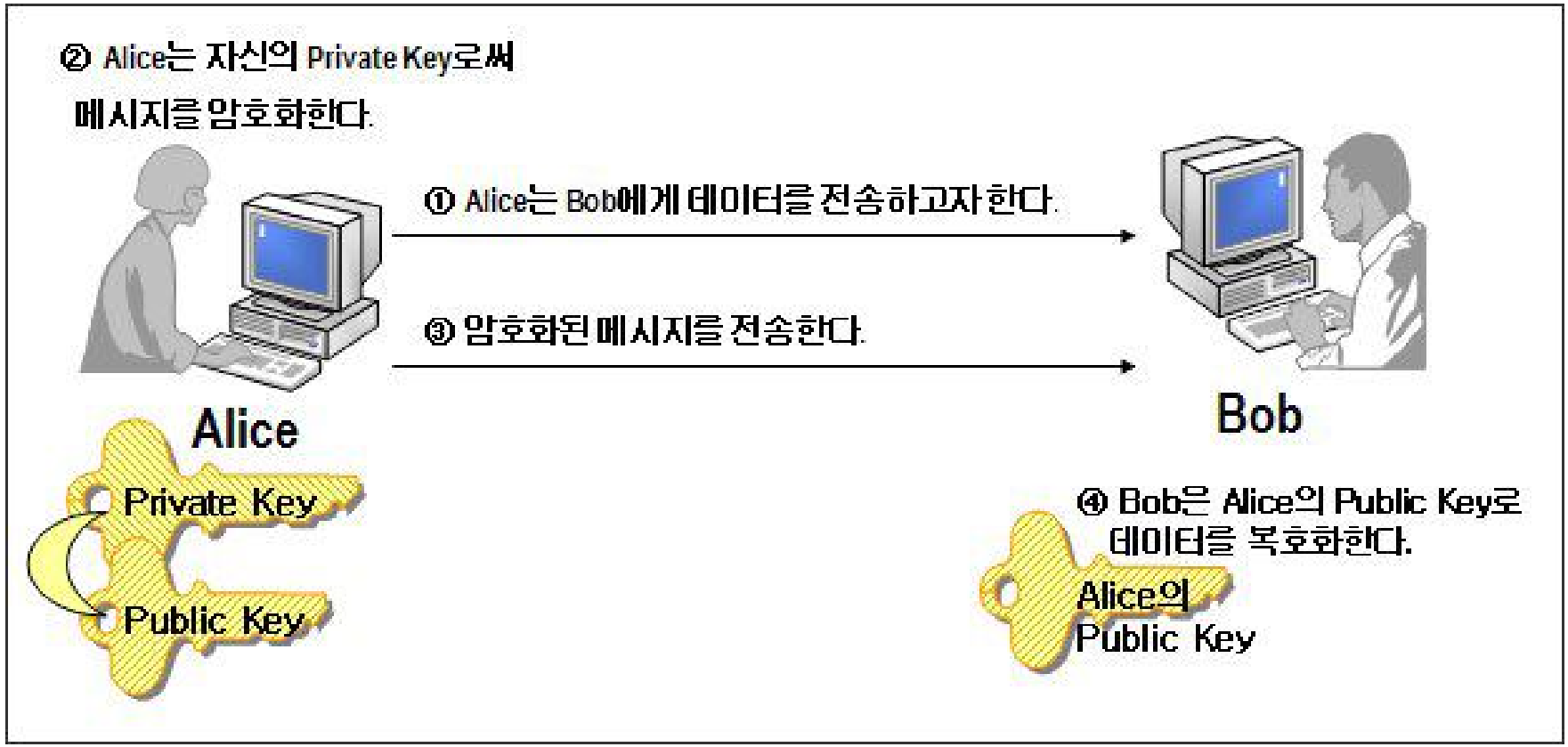
Public Key암호화(Confidentiality제공)



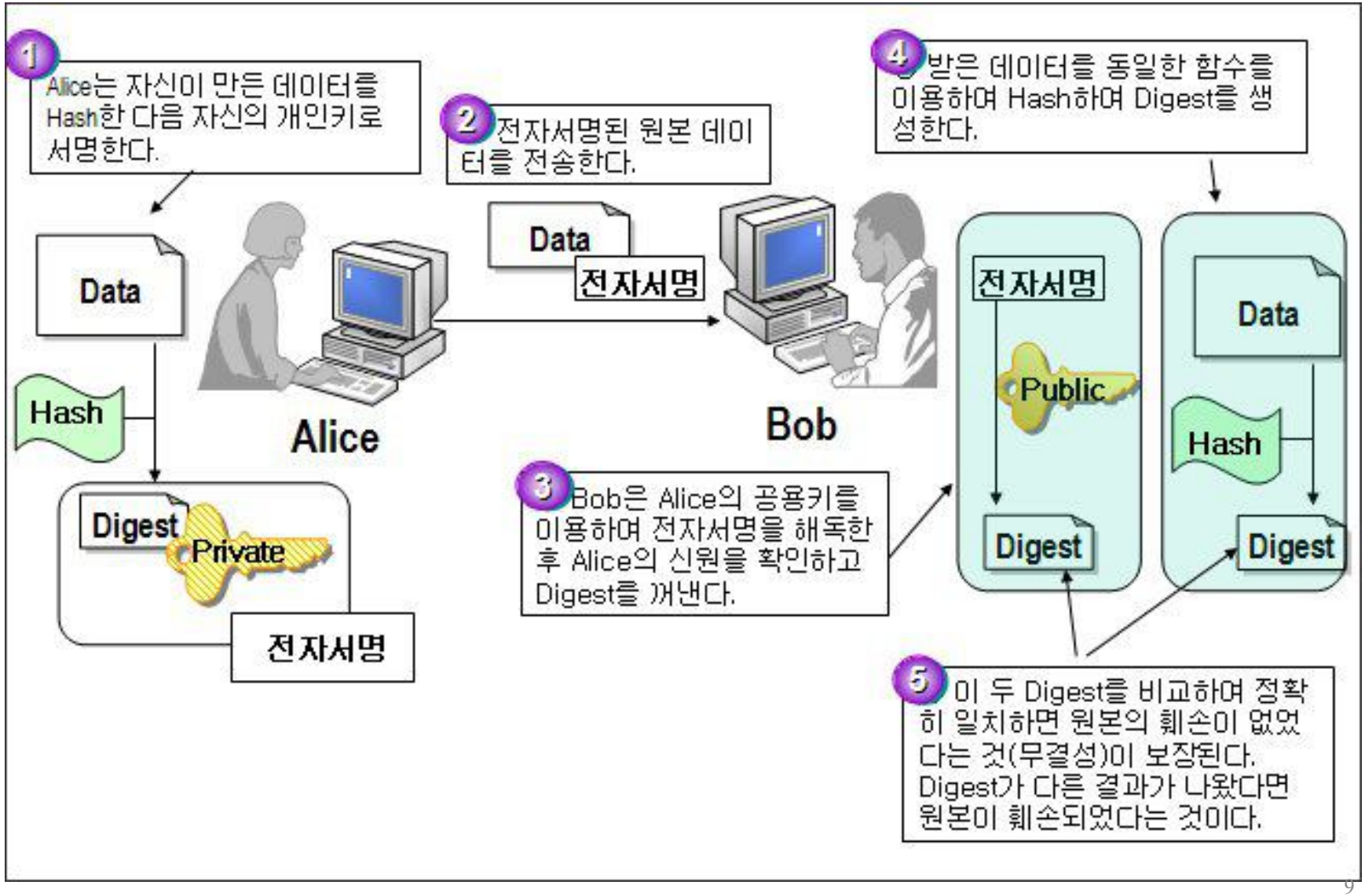


개인키 생성	openssl genrsa -out private.pem 1024 • RSA로 개인키 private.pem 생성, • private.pem 키는 1024bit 길이로 이 숫자가 높을수록 안전
공개키 생성	openssl rsa -in private.pem -out public.pem -outform PEM -pubout • 개인키 private.pem 에 대한 공개키 public.pem 생성 • 공개키를 자신에게 정보를 제공할 사람에게 전송
공개키로 암호화	echo 'coding everybody' > file.txt openssl rsautl -encrypt -inkey public.pem -pubin -in file.txt -out file.ssl • file.txt의 내용을 RSA방식으로 암호화한 파일 file.ssl 생성
개인키로 복호화	openssl rsautl -decrypt -inkey private.pem -in file.ssl -out decryp.txt • 개인키 private.pem로 file.ssl의 복호화한 결과를 decryp.txt로 생성

Private Key 암호화 (Authenticity 제공)

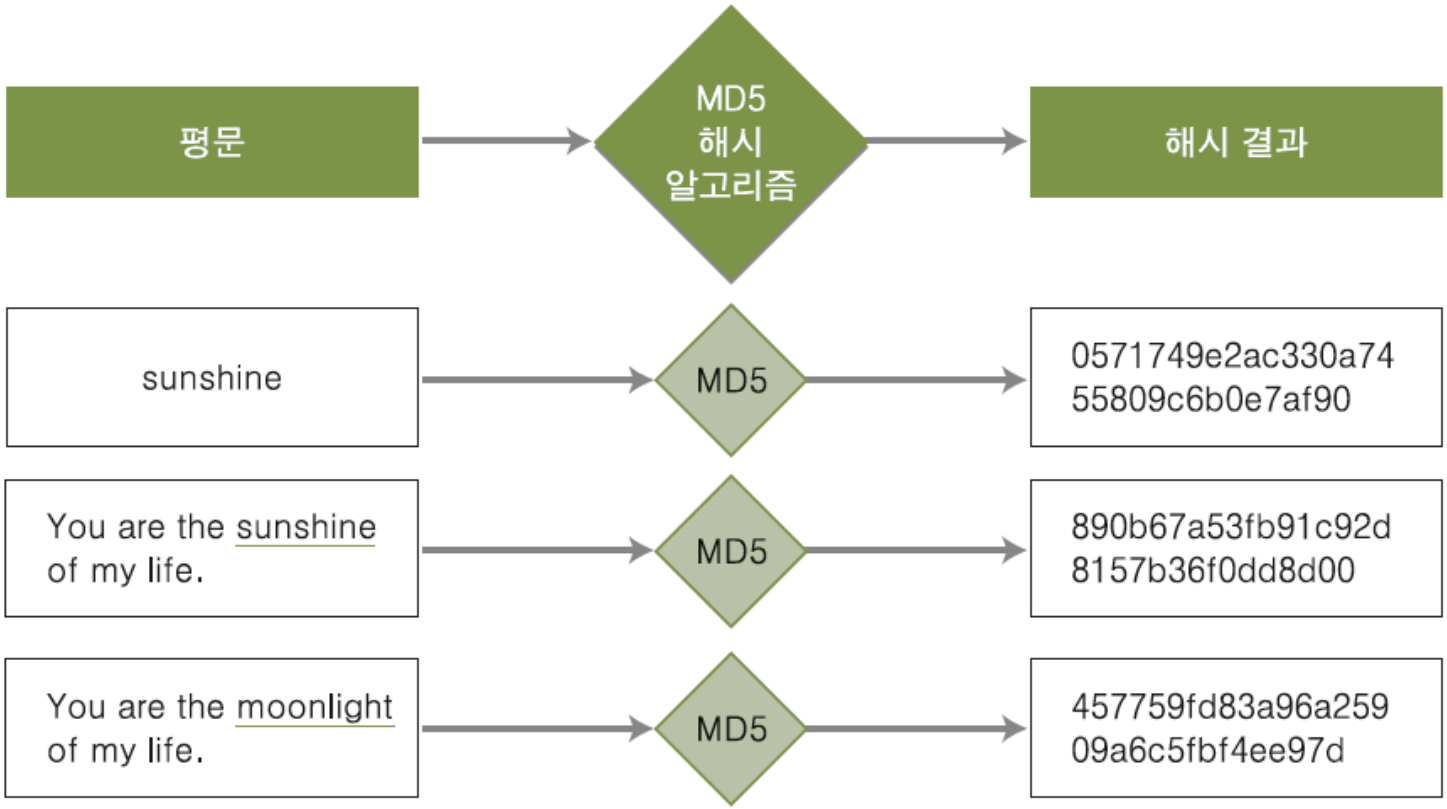


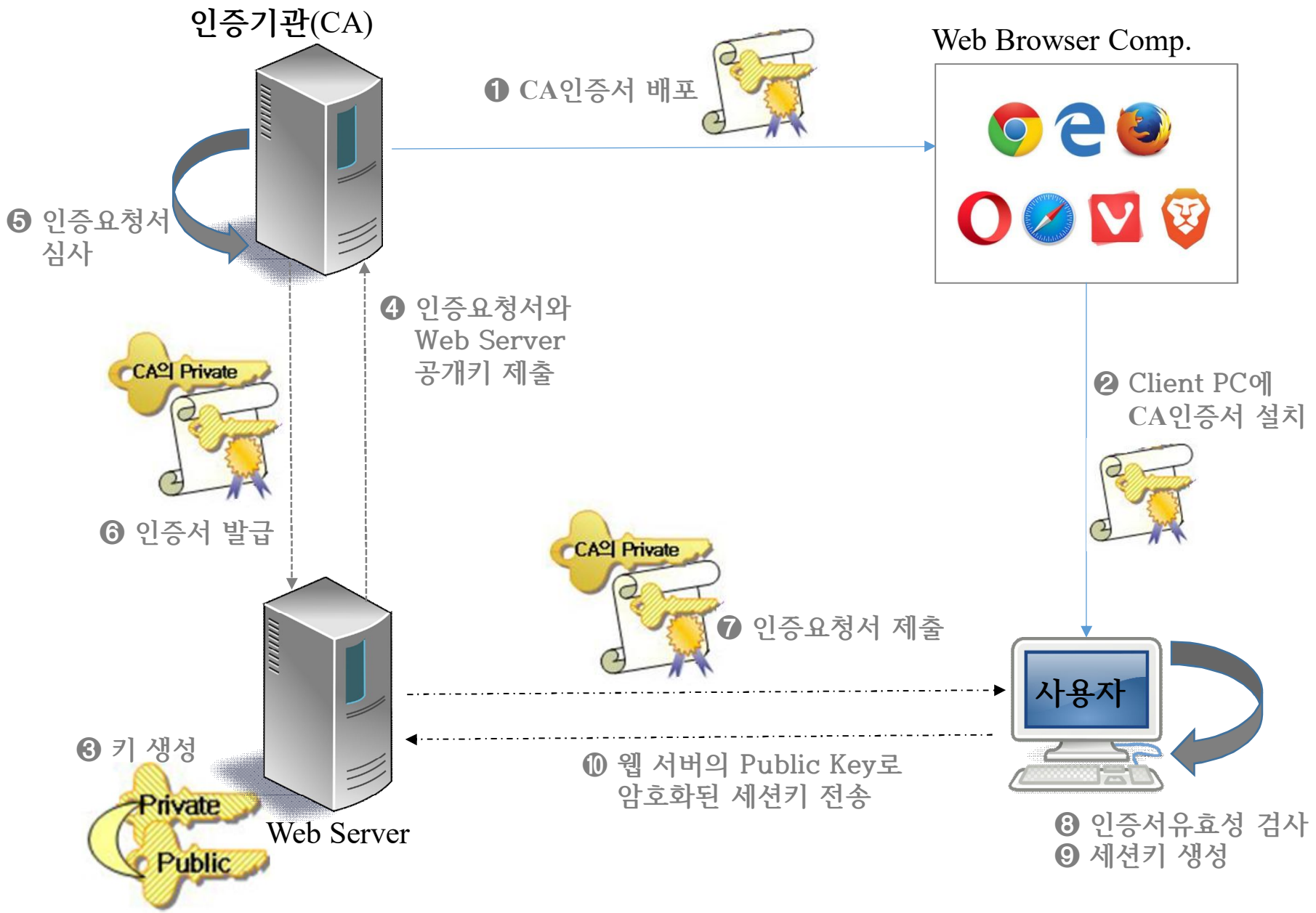
Hash Function & Digest (Integrity 제공)



해시(Hash)

- 하나의 문자열을, 이를 상징하는 짧은 길이의 값이나 키로 변환하는 것
- 보안에서는 해시를 무결성 확인을 위한 알고리즘으로 사용
- 해시 값을 통해 해시 되기 전의 값을 추측하는 것이 불가능




인증기관(CA)
Web Browser Comp.
❶ CA인증서 배포
❷ Client PC에
CA인증서 설치
❸ 키 생성
Private
Public
Web Server
❹ 인증요청서와
Web Server
공개키 제출
❺ 인증요청서
심사
❻ 인증서 발급
CA의 Private
CA의 Private
❼ 인증요청서 제출
사용자
❽ 인증서유효성 검사
❾ 세션키 생성
❿ 웹 서버의 Public Key로
암호화된 세션키 전송

SSL/TLS(1)

Handshake protocol

① 인증과 키 교환 담당 프로토콜

② 클라이언트와 서버의 상호 인증, 암호 알고리즘, MAC 알고리즘 등의 속성을 사전합의

③ 사용할 알고리즘 결정 및 키 분배 수행

SSL/TLS(2)

Change Cipher Spec

① 상호 보안 알고리즘 정보를 결정하는 일련의 보안 매개변수를 상대에게 전송

② 하나의 메시지로 되어 있으며 값 1을 갖는 한 바이트로 구성

· Handshake 프로토콜에 의해 협상된 압축, MAC, 암호화 방식 등이 이후부터 적용됨을 상대방에게 알려줌

SSL/TLS(3)

Alert protocol

① 오류 발생 관련 프로토콜

② 통신 과정 상의 다양항 오류 메시지 전달 (TLS 관련 경로를 전달)

③ 경고 메시지는 압축되고 암호화 됨

④ 프로토콜에 있는 각 메시지는 2 바이트로 되어 있음

- 첫 바이트 : 메시지의 심각성을 전달하기 위해 warning(1) 또는 fatal(2)의 값을 가짐 만일 레벨이 fatal이면, TLS는 즉시 연결을 종료
- 두 번째 바이트 : 특정 경고를 지시하는 코드가 들어 있음

SSL/TLS(4)

Record protocol

① 암호화된 메시지 송수신 프로토콜

· Connection States : 압축 알고리즘, 암호화 알고리즘, MAC 알고리즘 등을 지정.

· Record layer : Fragmentation, Record compression, Record payload protection

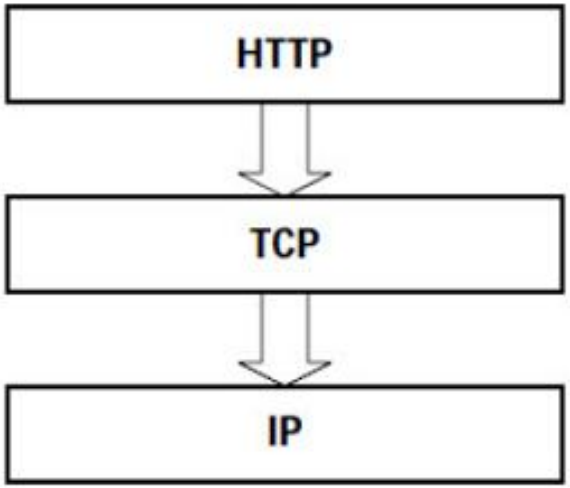
② 데이터를 블록으노 나누고 메시지를 전송

③ 경우에 따라서는 데이터를 압축하며, MAC을 제공해서 암호화하고 그 결과 전송

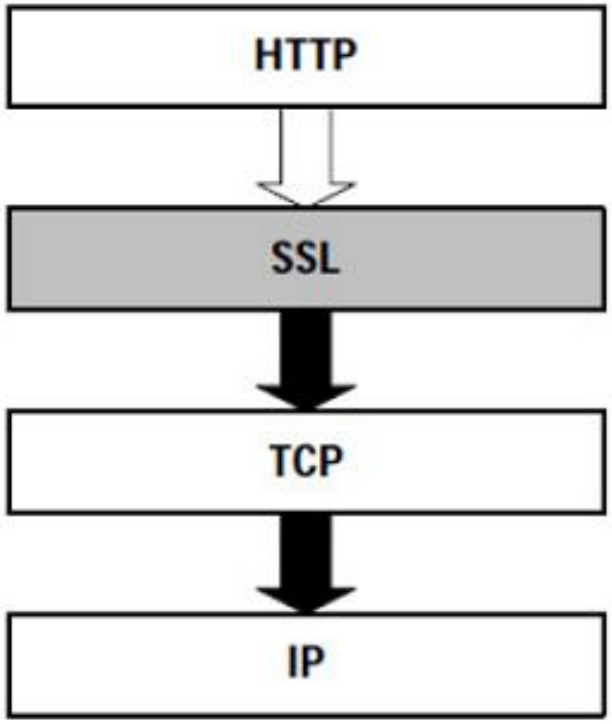
· 전송 받은 데이터는 복호화, 검증, 압축 해제, 재결합 하여 상위 계층의

클라이언트에게 보내줌

- HTTP와 HTTPS

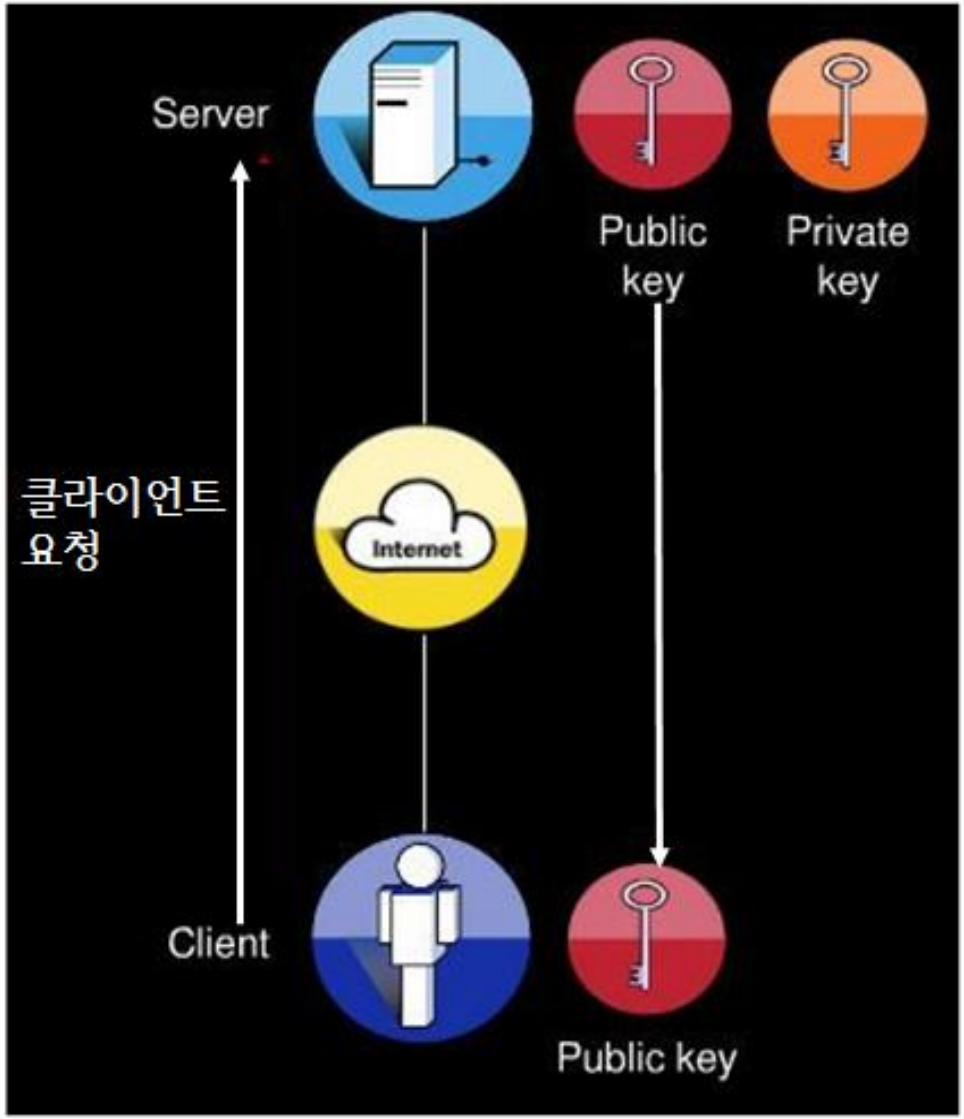


HTTP

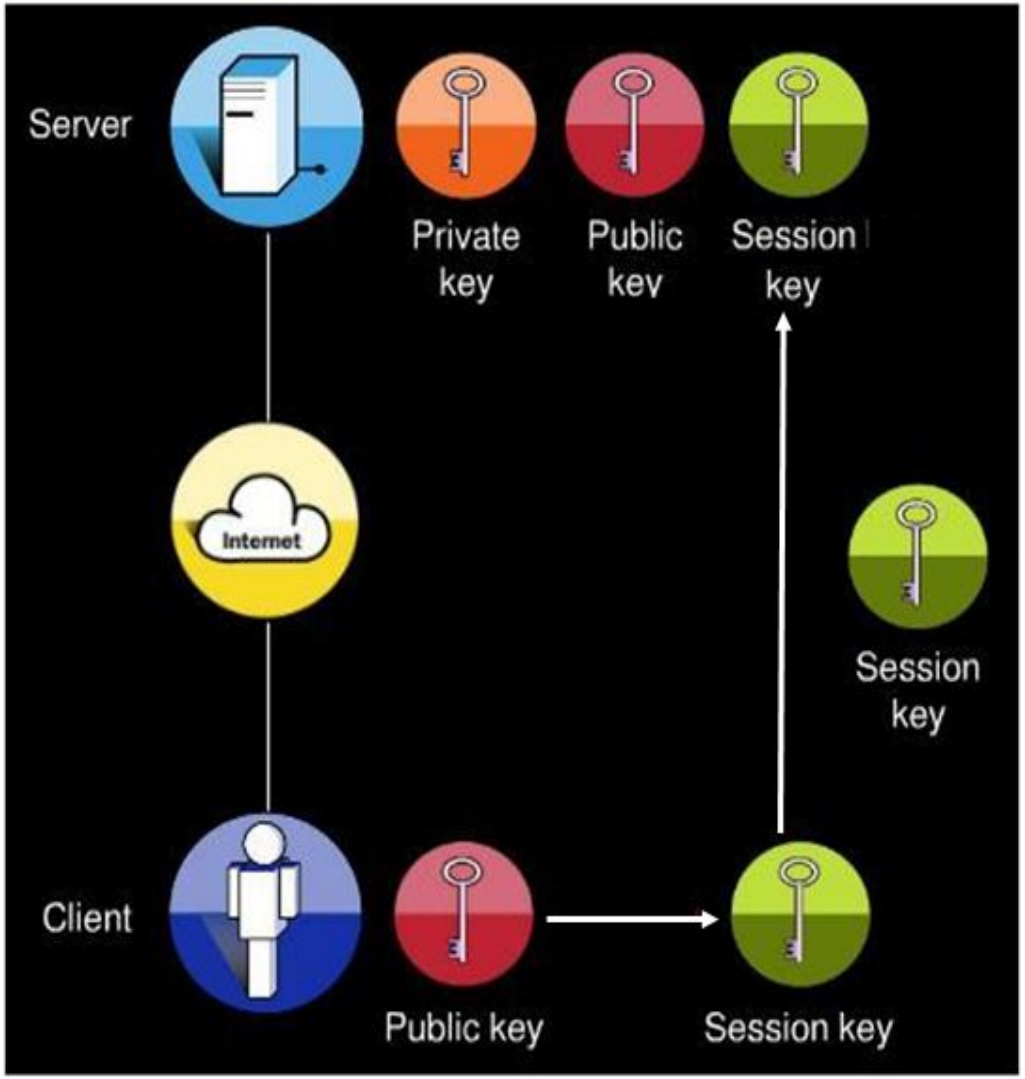


HTTPS

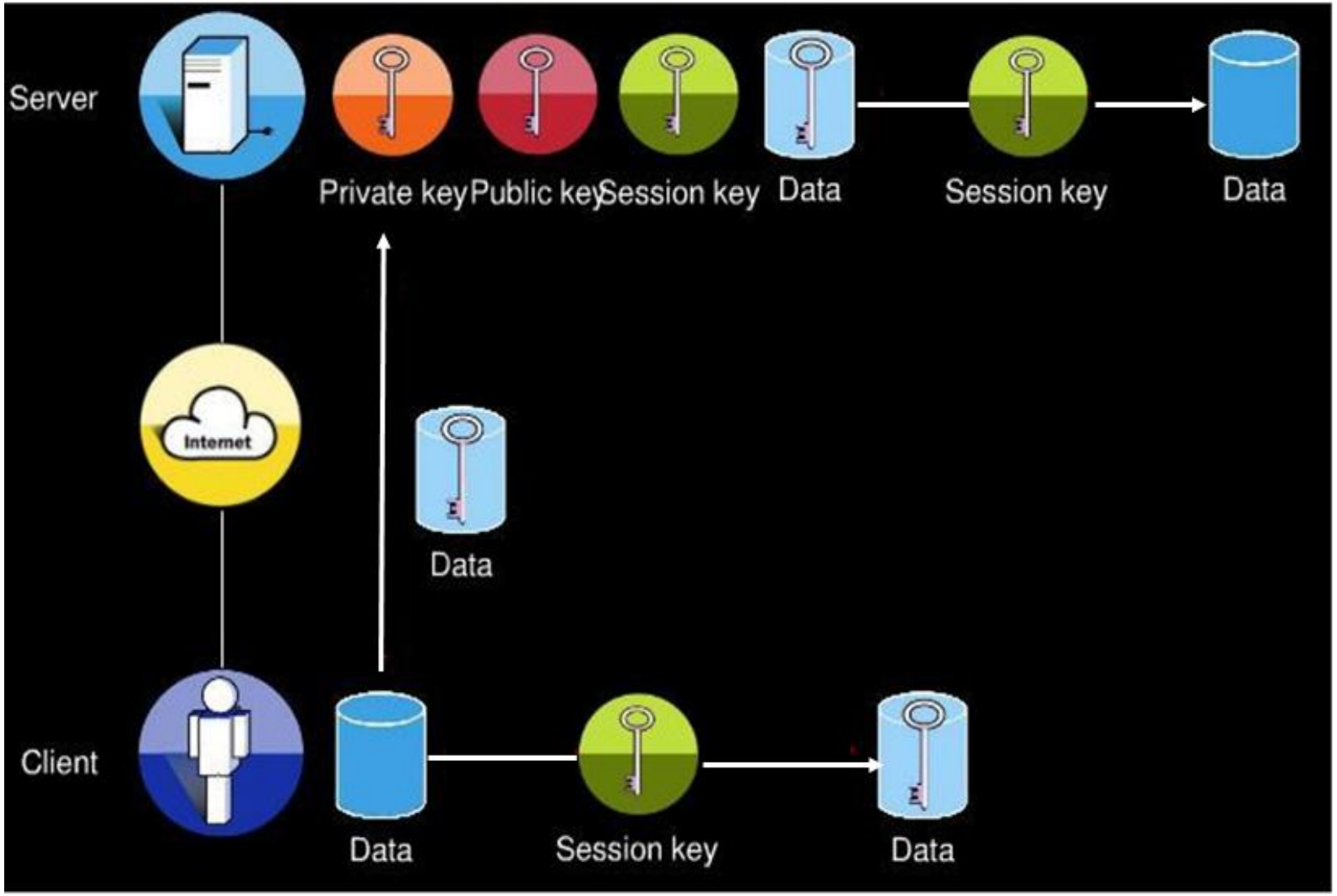
SSL/TLS Processing



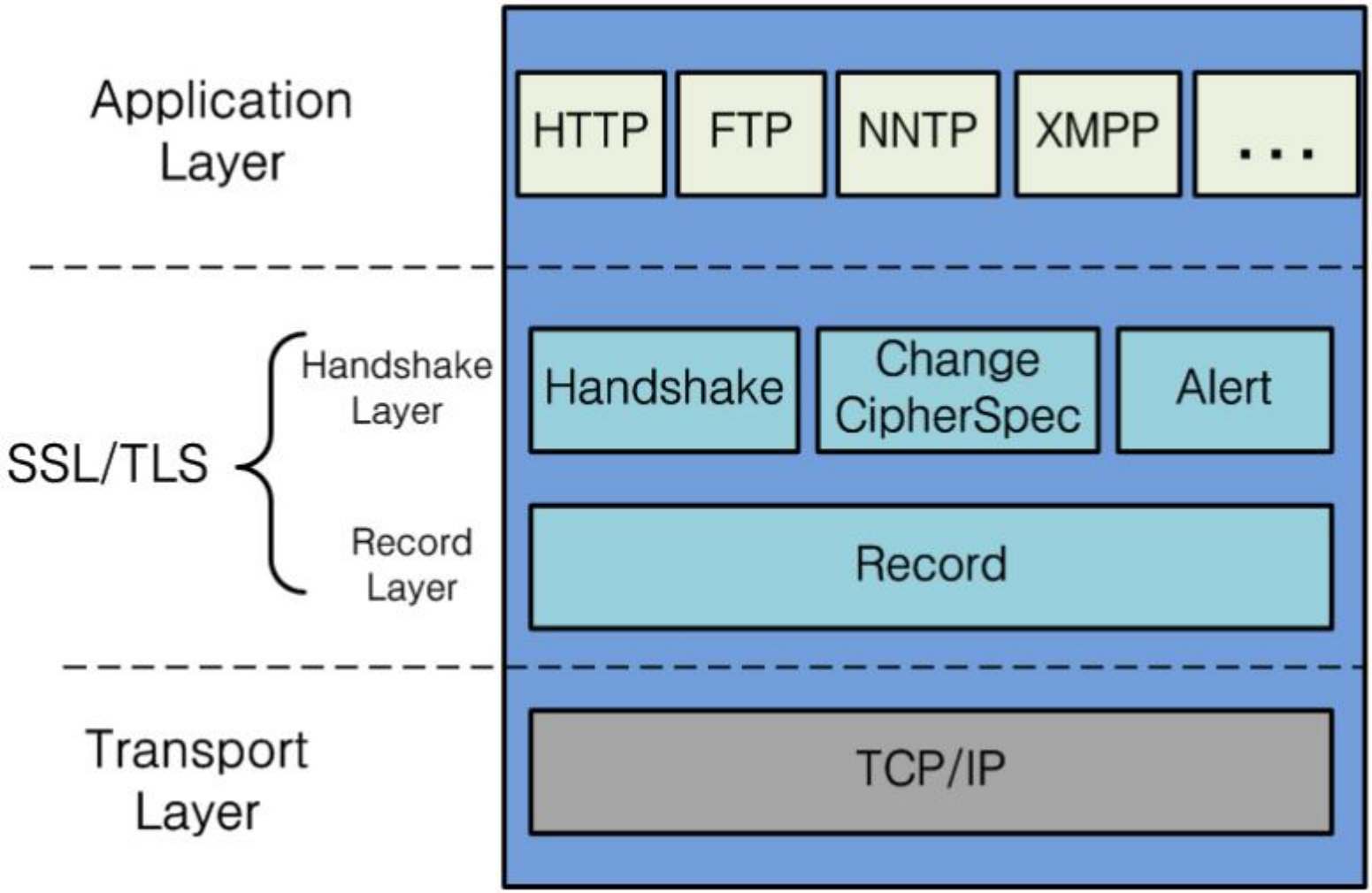
SSL/TLS Processing



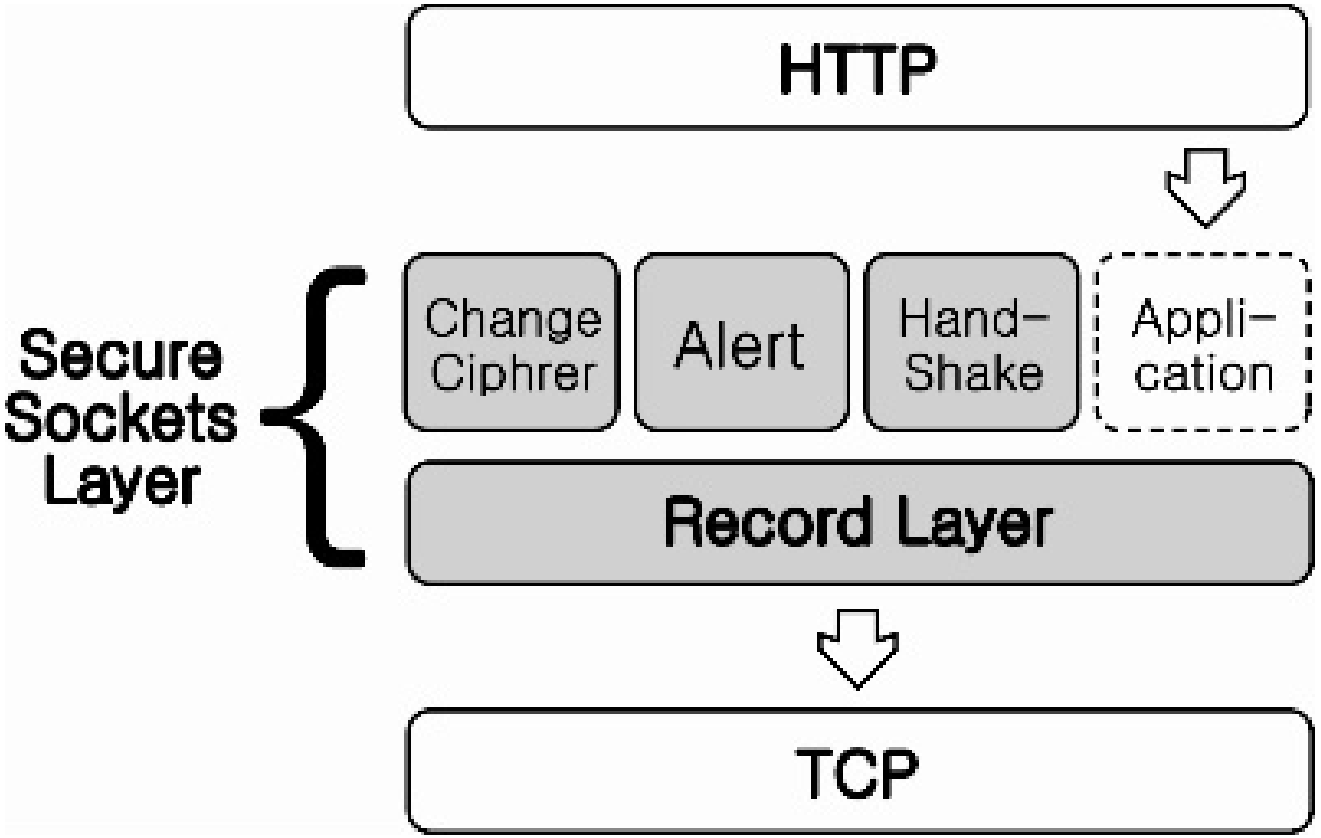
SSL/TLS Processing



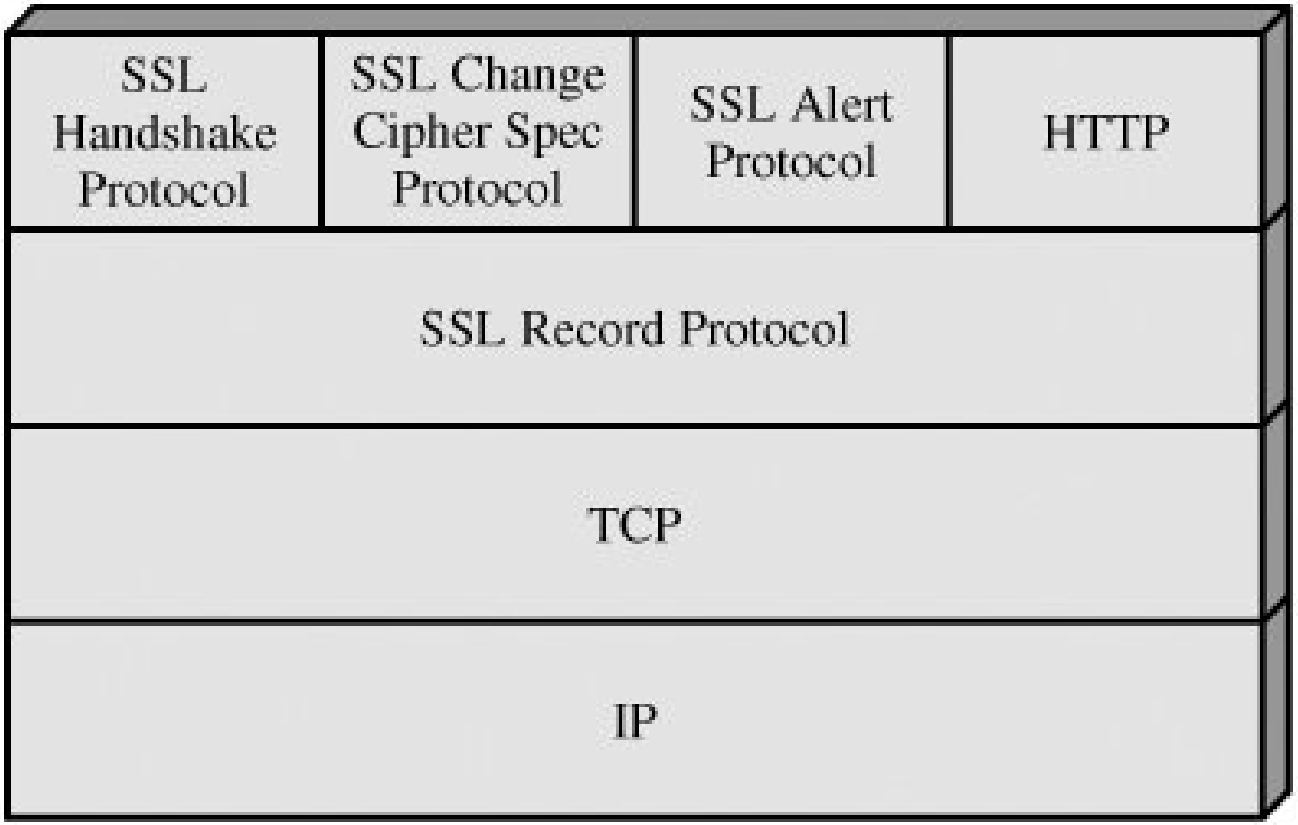
SSL/TLS Protocol stack

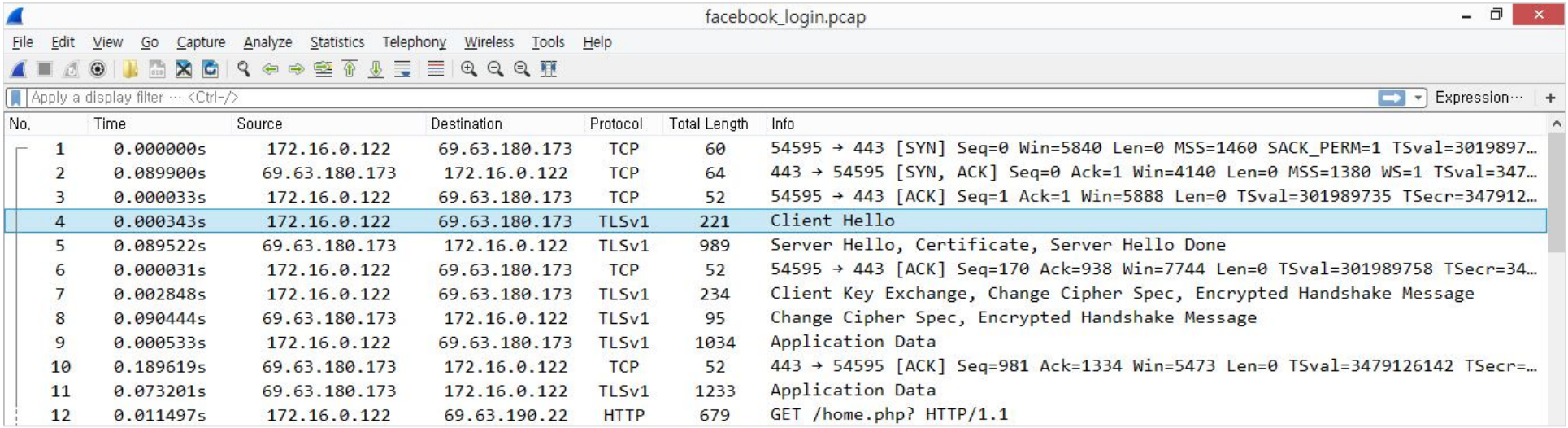


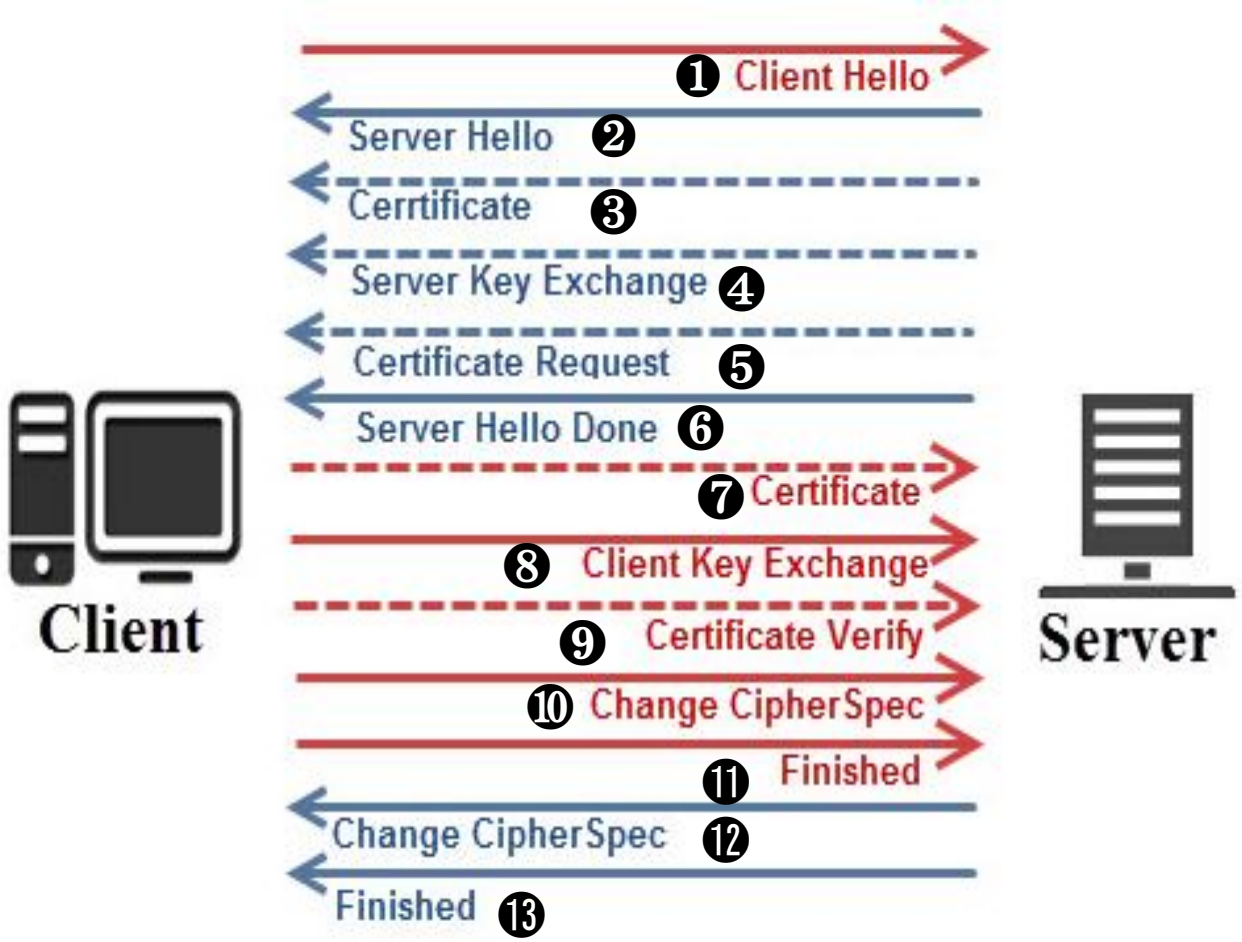
SSL/TLS Protocol stack



SSL/TLS Protocol stack



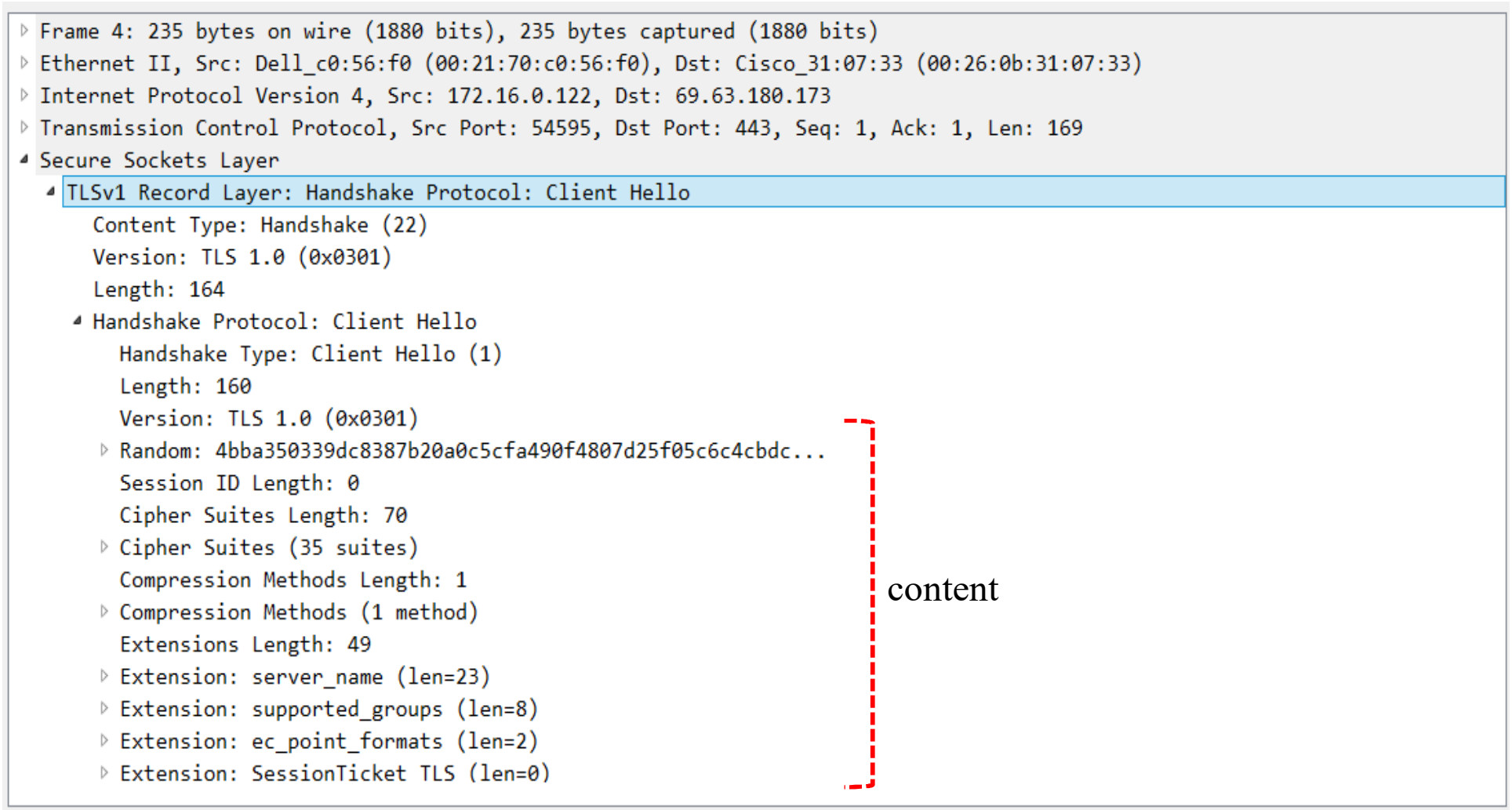

facebook_login.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Expression···
No. Time Source Destination Protocol Total Length Info
1 0.000000s 172.16.0.122 69.63.180.173 TCP 60 54595 → 443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3019897…
2 0.089900s 69.63.180.173 172.16.0.122 TCP 64 443 → 54595 [SYN, ACK] Seq=0 Ack=1 Win=4140 Len=0 MSS=1380 WS=1 TSval=347…
3 0.000033s 172.16.0.122 69.63.180.173 TCP 52 54595 → 443 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=301989735 TSecr=347912…
4 0.000343s 172.16.0.122 69.63.180.173 TLSv1 221 Client Hello
5 0.089522s 69.63.180.173 172.16.0.122 TLSv1 989 Server Hello, Certificate, Server Hello Done
6 0.000031s 172.16.0.122 69.63.180.173 TCP 52 54595 → 443 [ACK] Seq=170 Ack=938 Win=7744 Len=0 TSval=301989758 TSecr=34…
7 0.002848s 172.16.0.122 69.63.180.173 TLSv1 234 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
8 0.090444s 69.63.180.173 172.16.0.122 TLSv1 95 Change Cipher Spec, Encrypted Handshake Message
9 0.000533s 172.16.0.122 69.63.180.173 TLSv1 1034 Application Data
10 0.189619s 69.63.180.173 172.16.0.122 TCP 52 443 → 54595 [ACK] Seq=981 Ack=1334 Win=5473 Len=0 TSval=3479126142 TSecr=…
11 0.073201s 69.63.180.173 172.16.0.122 TLSv1 1233 Application Data
12 0.011497s 172.16.0.122 69.63.190.22 HTTP 679 GET /home.php? HTTP/1.1



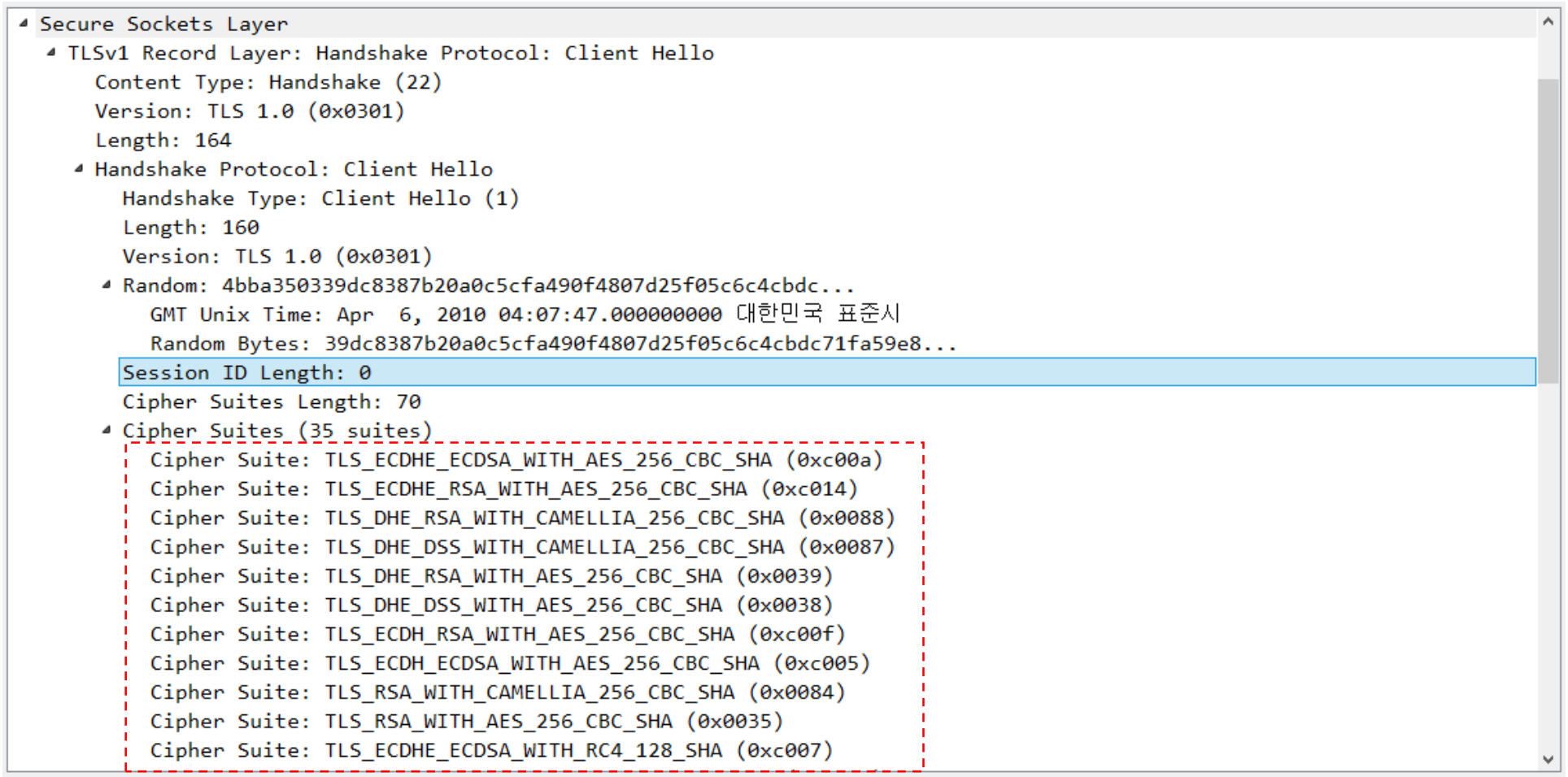
ssl

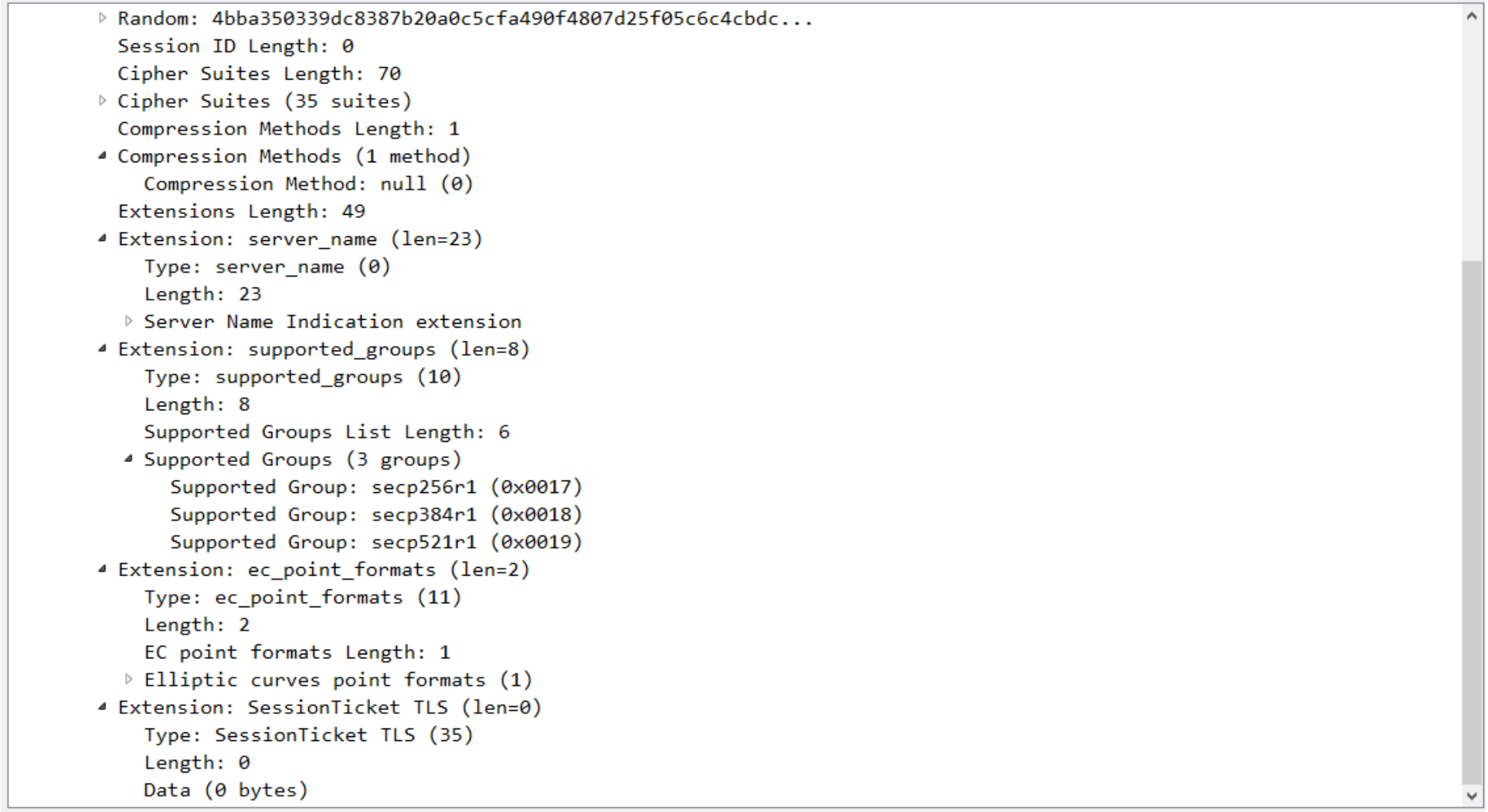
No.	Time	Source	Destination	Protocol	Total Length	Info
4	0.000000s	172.16.0.122	69.63.180.173	TLSv1	221	Client Hello
5	0.089522s	69.63.180.173	172.16.0.122	TLSv1	989	Server Hello, Certificate, Server Hello Done
7	0.002879s	172.16.0.122	69.63.180.173	TLSv1	234	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
8	0.090444s	69.63.180.173	172.16.0.122	TLSv1	95	Change Cipher Spec, Encrypted Handshake Message
9	0.000533s	172.16.0.122	69.63.180.173	TLSv1	1034	Application Data
11	0.262820s	69.63.180.173	172.16.0.122	TLSv1	1233	Application Data
63	5m 1.502778s	172.16.0.122	69.63.180.173	TLSv1	75	Encrypted Alert

1 단계. Client Hello message

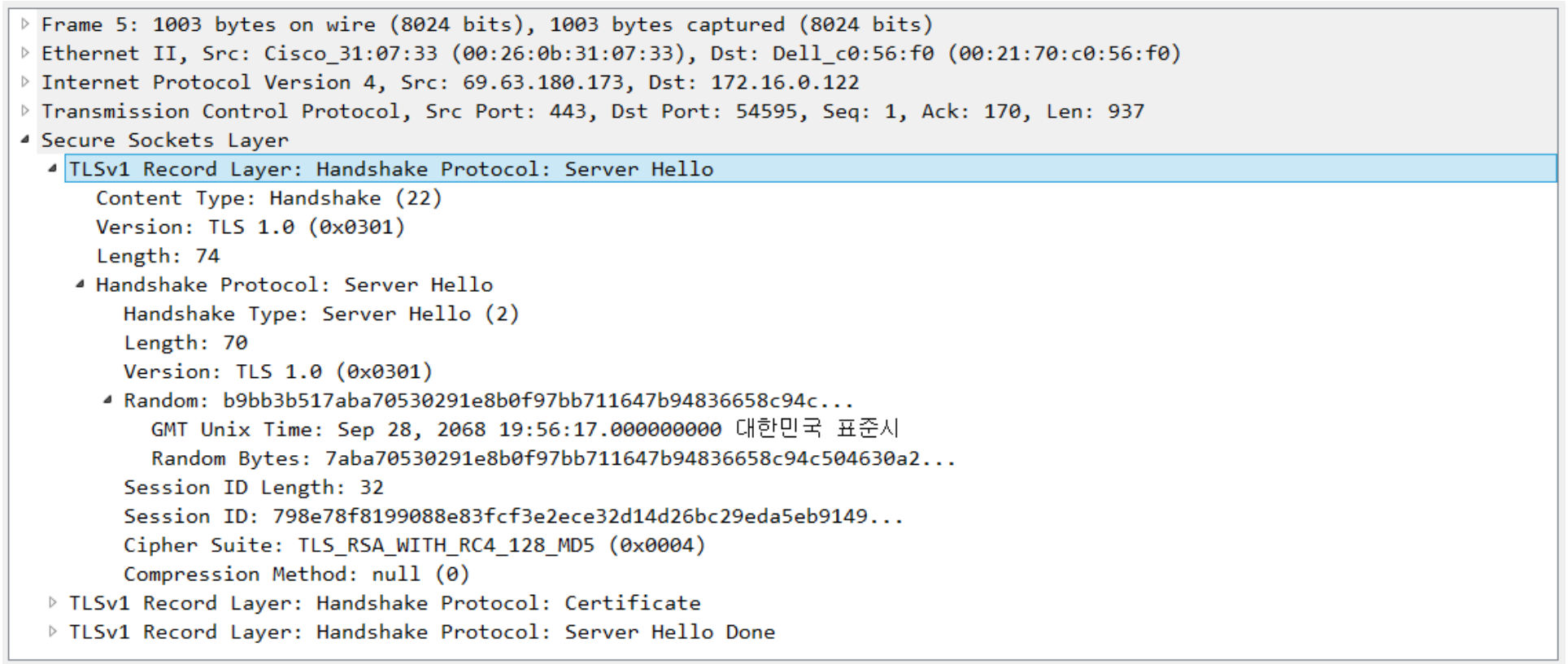


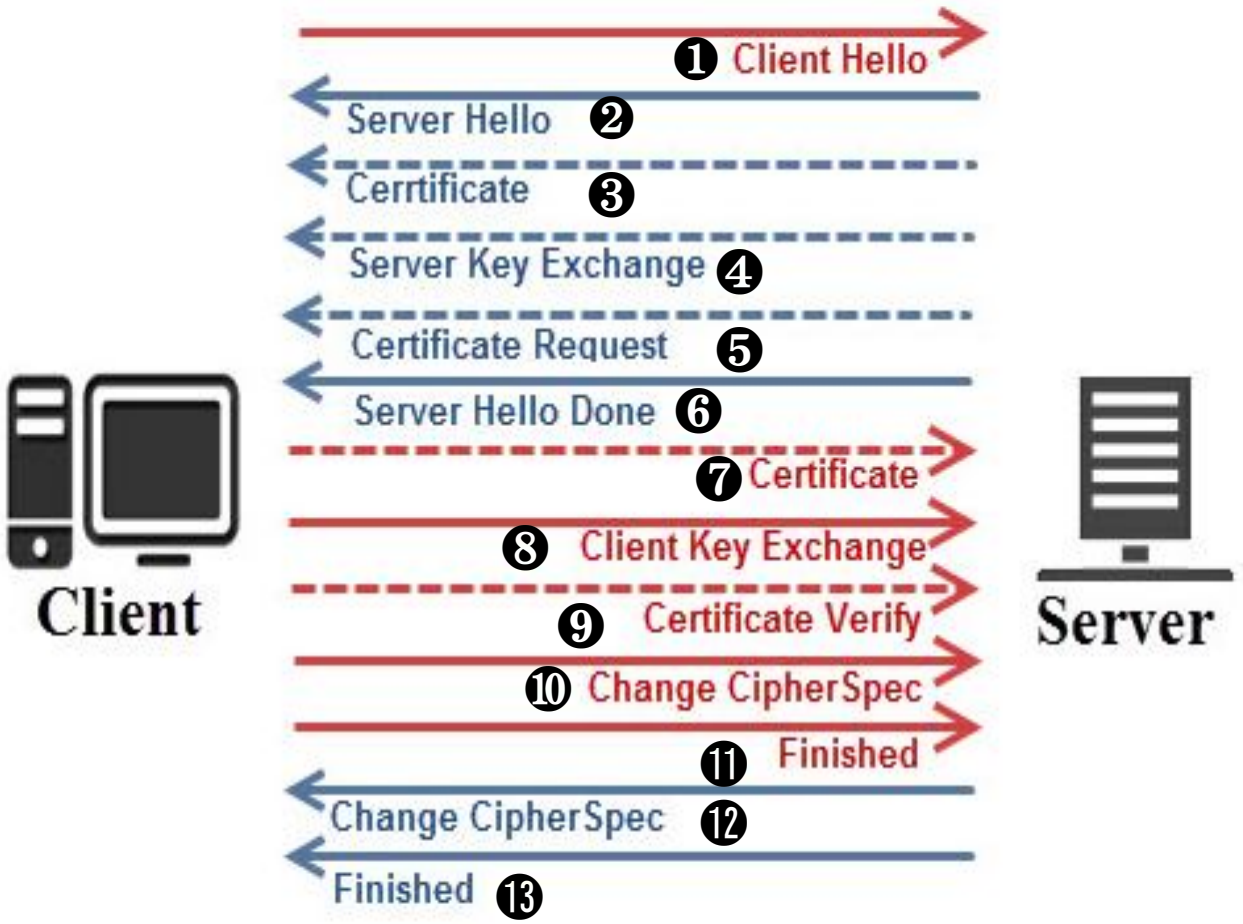
Protocol Suite




Random: 4bba350339dc8387b20a0c5cfa490f4807d25f05c6c4cbdc...
Session ID Length: 0
Cipher Suites Length: 70
Cipher Suites (35 suites)
Compression Methods Length: 1
Compression Methods (1 method)
Compression Method: null (0)
Extensions Length: 49
Extension: server_name (len=23)
Type: server_name (0)
Length: 23
Server Name Indication extension
Extension: supported_groups (len=8)
Type: supported_groups (10)
Length: 8
Supported Groups List Length: 6
Supported Groups (3 groups)
Supported Group: secp256r1 (0x0017)
Supported Group: secp384r1 (0x0018)
Supported Group: secp521r1 (0x0019)
Extension: ec_point_formats (len=2)
Type: ec_point_formats (11)
Length: 2
EC point formats Length: 1
Elliptic curves point formats (1)
Extension: SessionTicket TLS (len=0)
Type: SessionTicket TLS (35)
Length: 0
Data (0 bytes)

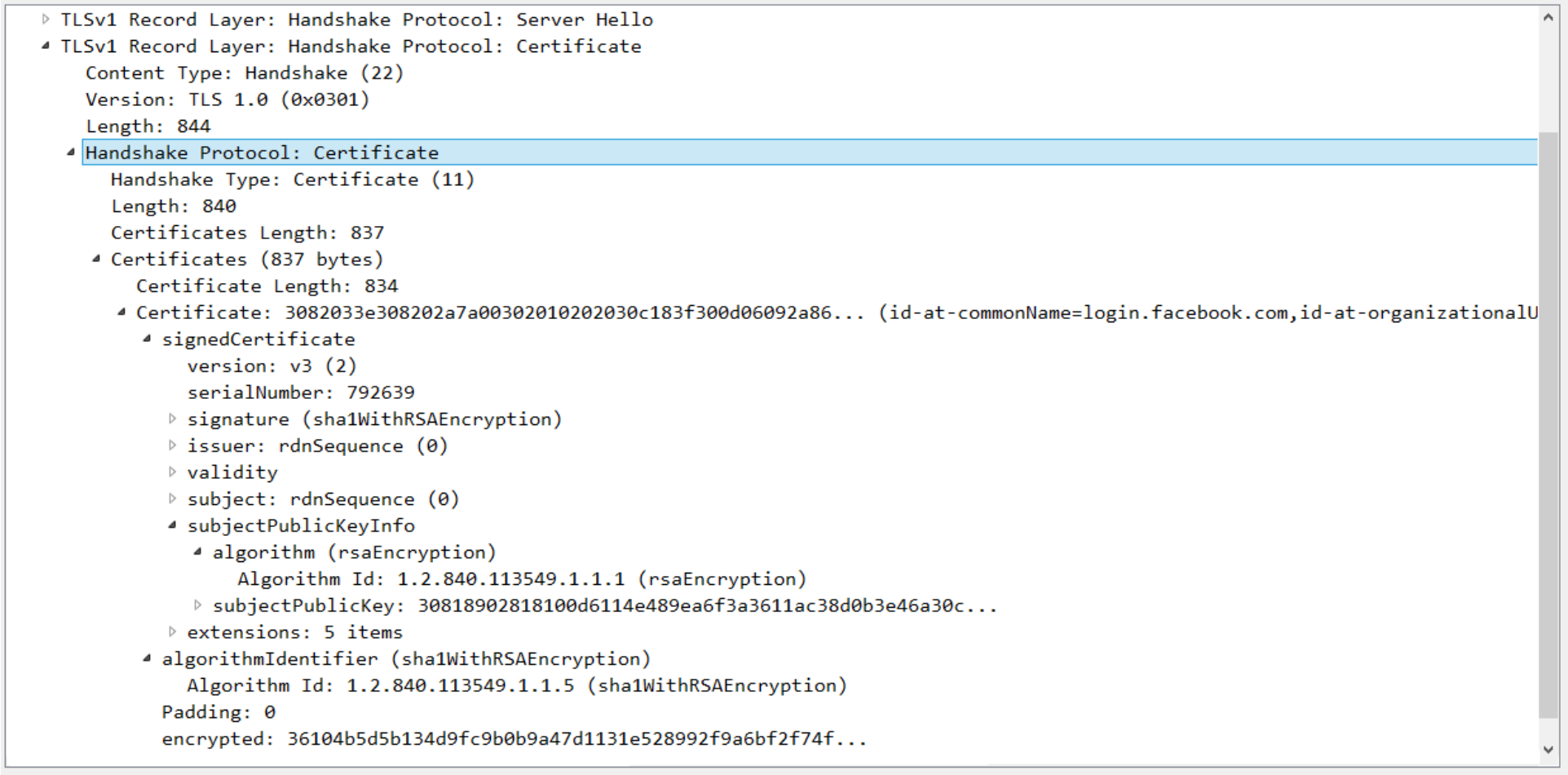
1 단계. Server Hello message



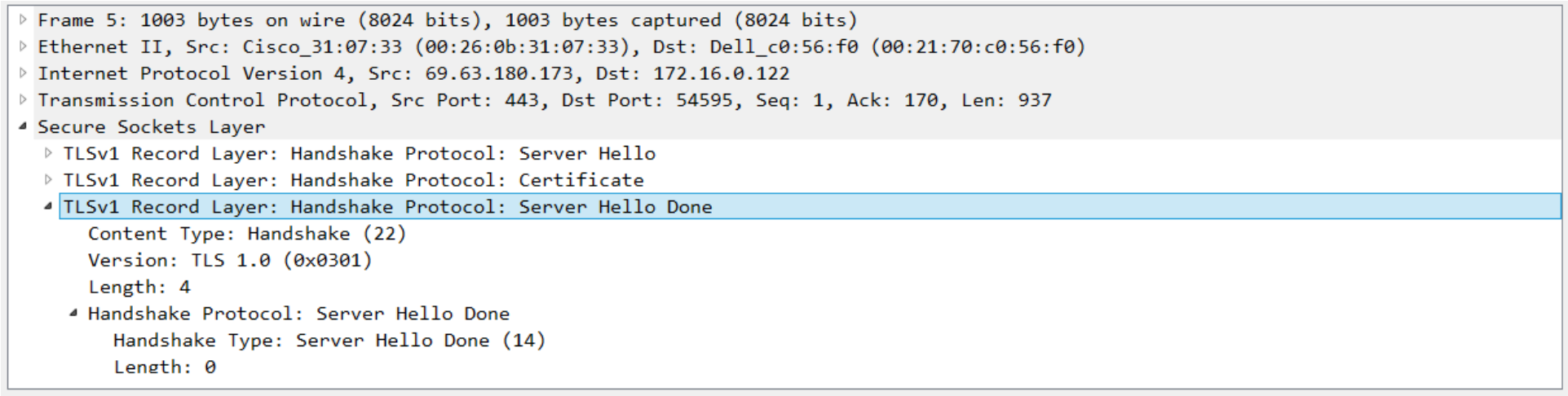


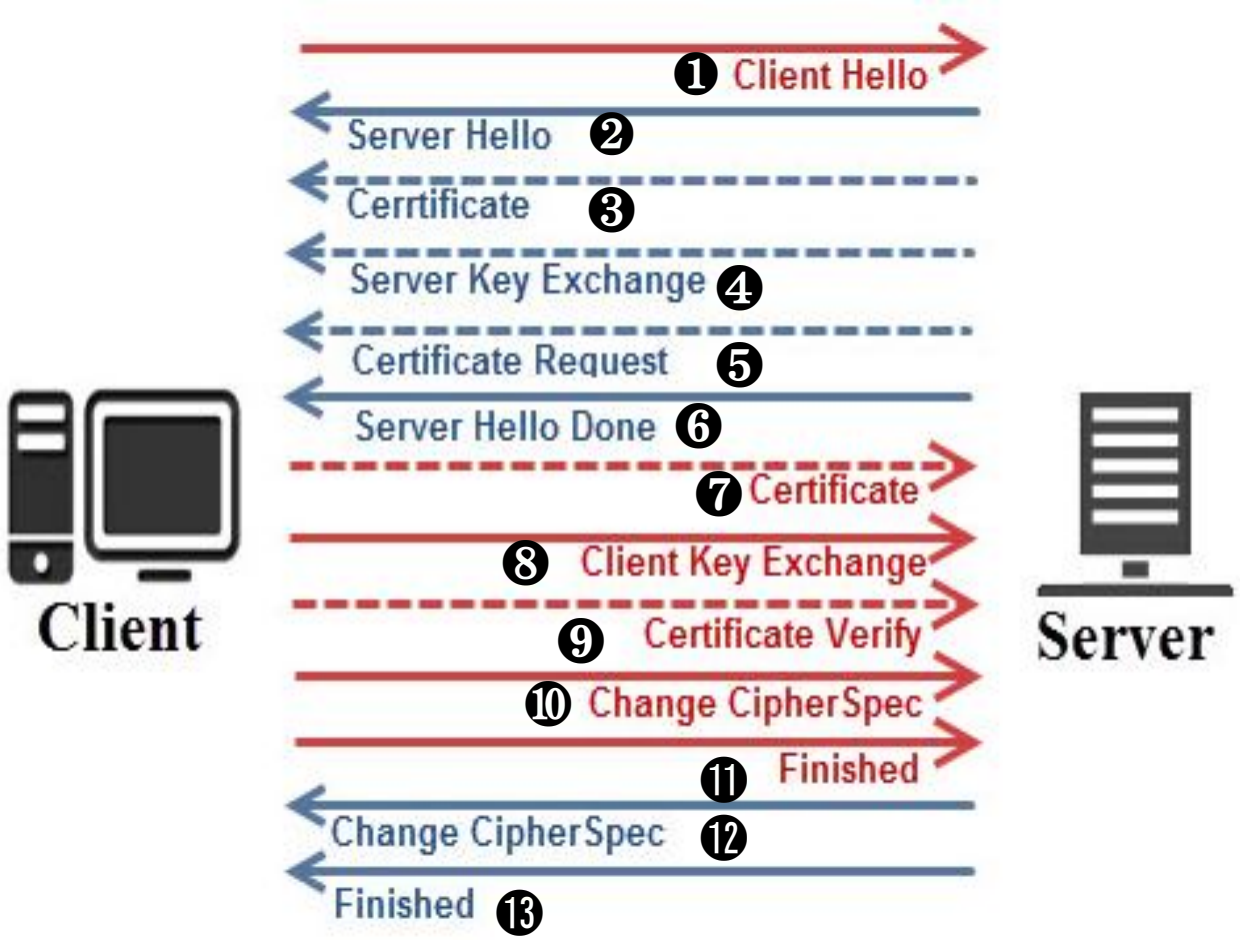

```
▷ Frame 5: 1003 bytes on wire (8024 bits), 1003 bytes captured (8024 bits)
▷ Ethernet II, Src: Cisco_31:07:33 (00:26:0b:31:07:33), Dst: Dell_c0:56:f0 (00:21:70:c0:56:f0)
▷ Internet Protocol Version 4, Src: 69.63.180.173, Dst: 172.16.0.122
▷ Transmission Control Protocol, Src Port: 443, Dst Port: 54595, Seq: 1, Ack: 170, Len: 937
◢ Secure Sockets Layer
  ▷ TLSv1 Record Layer: Handshake Protocol: Server Hello
  ▷ TLSv1 Record Layer: Handshake Protocol: Certificate
  ▷ TLSv1 Record Laver: Handshake Protocol: Server Hello Done
```

2 단계. Certificate message



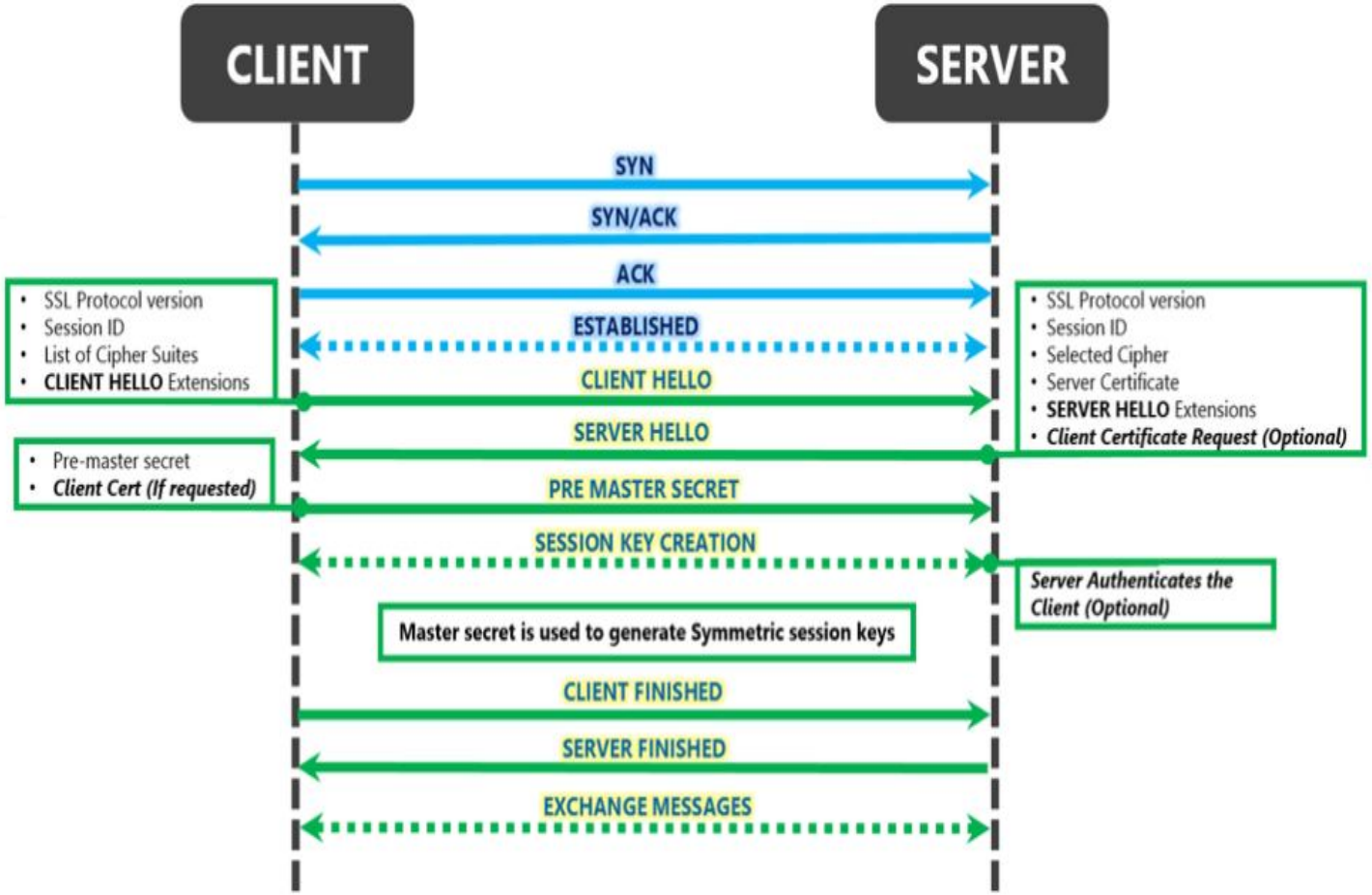
2 단계. Server Hello Done message



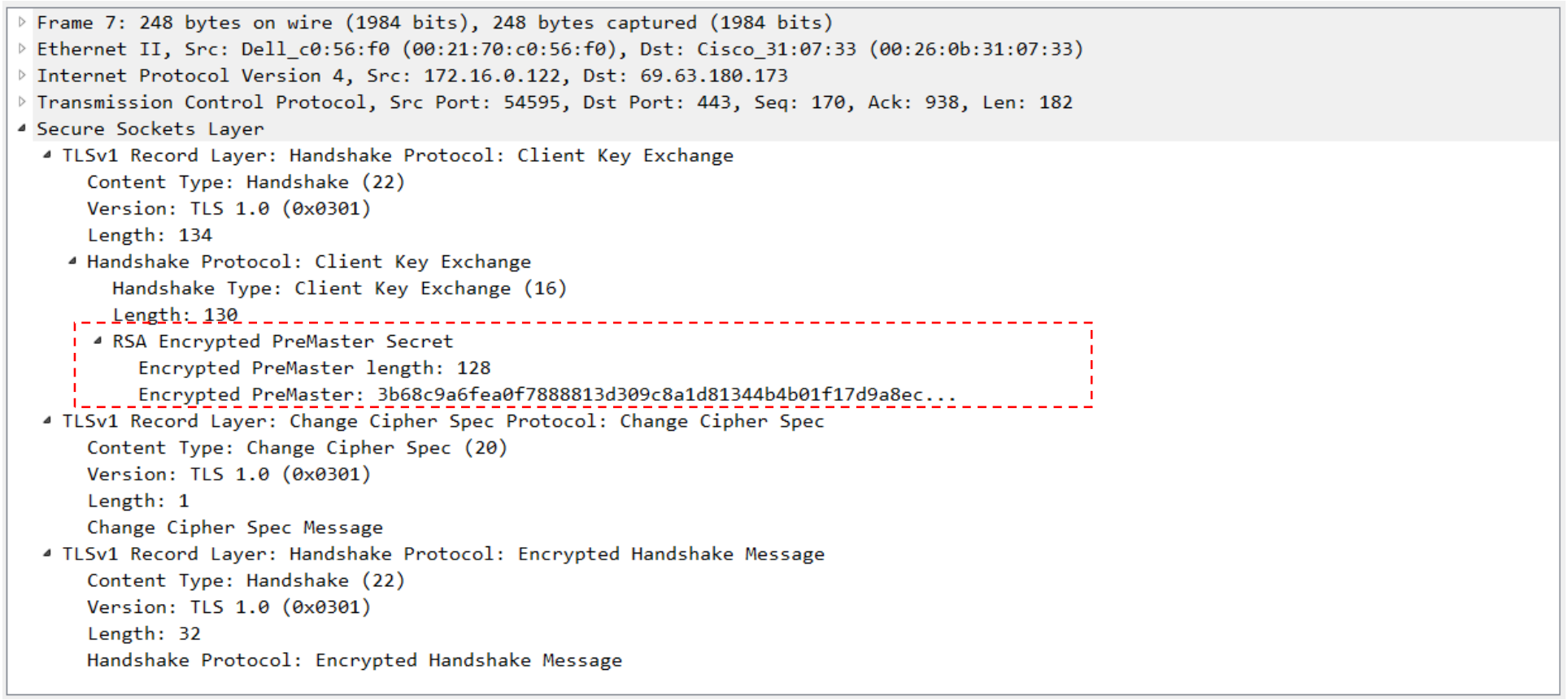


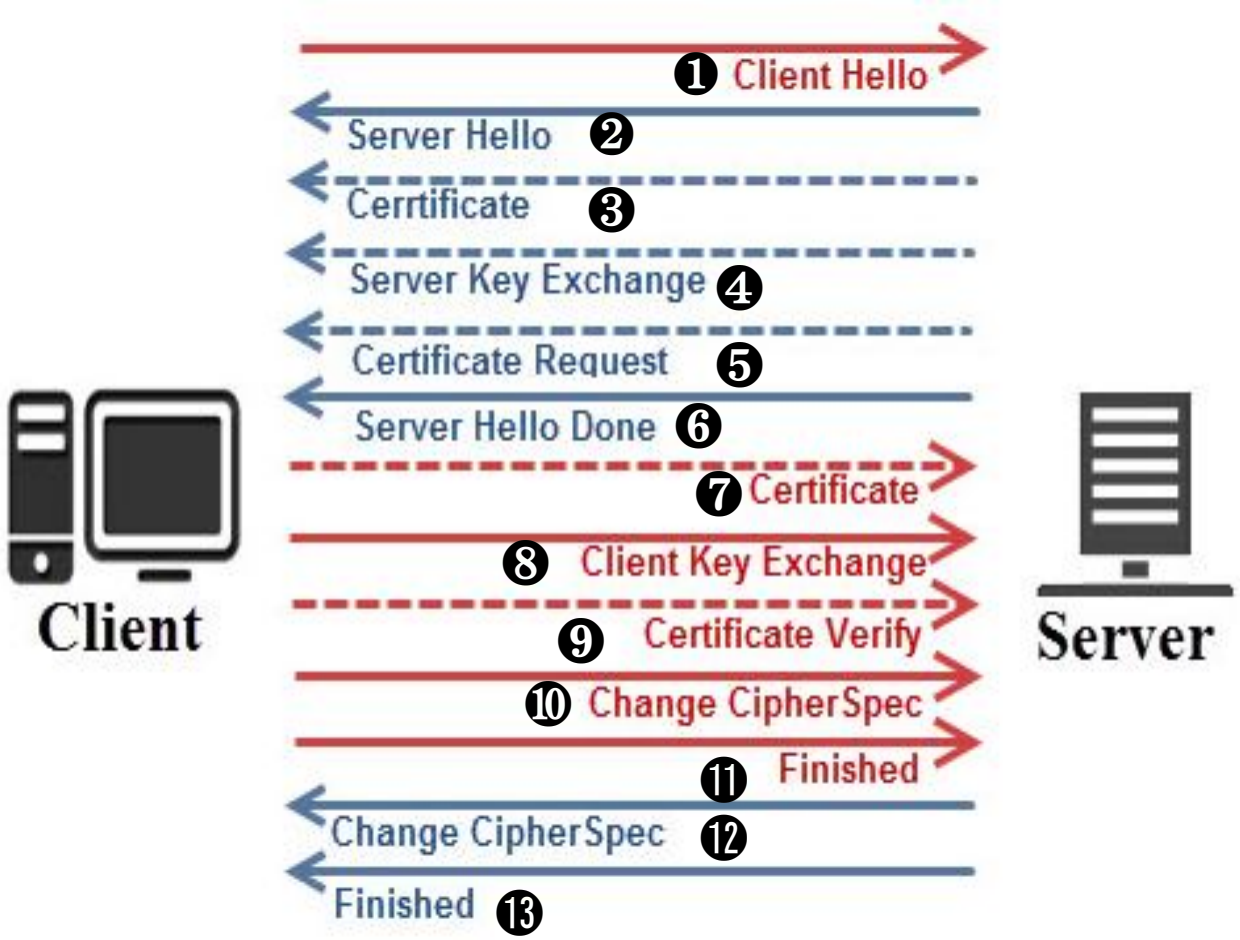
	Time	Source	Destination	Protocol	Total Length	Info
1	0.000000s	172.16.0.122	69.63.180.173	TCP	60	54595 → 443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3019897…
2	0.089900s	69.63.180.173	172.16.0.122	TCP	64	443 → 54595 [SYN, ACK] Seq=0 Ack=1 Win=4140 Len=0 MSS=1380 WS=1 TSval=347…
3	0.000033s	172.16.0.122	69.63.180.173	TCP	52	54595 → 443 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=301989735 TSecr=347912…
4	0.000343s	172.16.0.122	69.63.180.173	TLSv1	221	Client Hello
5	0.089522s	69.63.180.173	172.16.0.122	TLSv1	989	Server Hello, Certificate, Server Hello Done
6	0.000031s	172.16.0.122	69.63.180.173	TCP	52	54595 → 443 [ACK] Seq=170 Ack=938 Win=7744 Len=0 TSval=301989758 TSecr=34…
7	0.002848s	172.16.0.122	69.63.180.173	TLSv1	234	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
8	0.090444s	69.63.180.173	172.16.0.122	TLSv1	95	Change Cipher Spec, Encrypted Handshake Message
9	0.000533s	172.16.0.122	69.63.180.173	TLSv1	1034	Application Data
10	0.189619s	69.63.180.173	172.16.0.122	TCP	52	443 → 54595 [ACK] Seq=981 Ack=1334 Win=5473 Len=0 TSval=3479126142 TSecr=…
11	0.073201s	69.63.180.173	172.16.0.122	TLSv1	1233	Application Data
12	0.011497s	172.16.0.122	69.63.190.22	HTTP	679	GET /home.php? HTTP/1.1

3 단계.

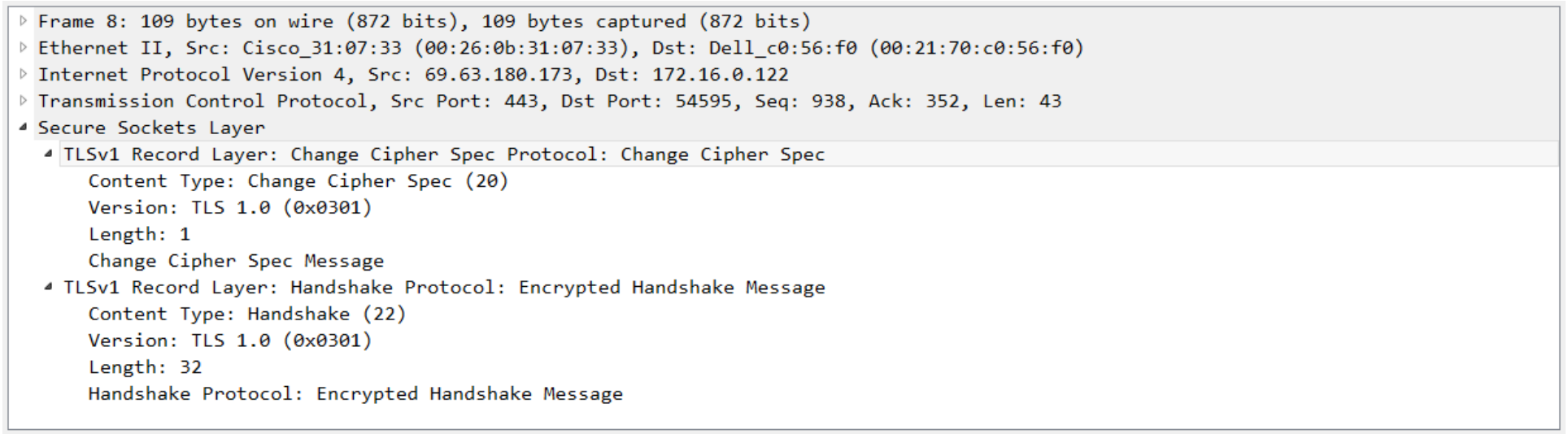



```
▷ Frame 7: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits)
▷ Ethernet II, Src: Dell_c0:56:f0 (00:21:70:c0:56:f0), Dst: Cisco_31:07:33 (00:26:0b:31:07:33)
▷ Internet Protocol Version 4, Src: 172.16.0.122, Dst: 69.63.180.173
▷ Transmission Control Protocol, Src Port: 54595, Dst Port: 443, Seq: 170, Ack: 938, Len: 182
◢ Secure Sockets Layer
  ▷ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
  ▷ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  ▷ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
```


Frame 7: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits)
Ethernet II, Src: Dell_c0:56:f0 (00:21:70:c0:56:f0), Dst: Cisco_31:07:33 (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: 170, Ack: 938, Len: 182
Secure Sockets Layer
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: 3b68c9a6fea0f7888813d309c8a1d81344b4b01f17d9a8ec...
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



No.	Time	Source	Destination	Protocol	Total Length	Info
1	0.000000s	172.16.0.122	69.63.180.173	TCP	60	54595 → 443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3019897…
2	0.089900s	69.63.180.173	172.16.0.122	TCP	64	443 → 54595 [SYN, ACK] Seq=0 Ack=1 Win=4140 Len=0 MSS=1380 WS=1 TSval=347…
3	0.000033s	172.16.0.122	69.63.180.173	TCP	52	54595 → 443 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=301989735 TSecr=347912…
4	0.000343s	172.16.0.122	69.63.180.173	TLSv1	221	Client Hello
5	0.089522s	69.63.180.173	172.16.0.122	TLSv1	989	Server Hello, Certificate, Server Hello Done
6	0.000031s	172.16.0.122	69.63.180.173	TCP	52	54595 → 443 [ACK] Seq=170 Ack=938 Win=7744 Len=0 TSval=301989758 TSecr=34…
7	0.002848s	172.16.0.122	69.63.180.173	TLSv1	234	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
8	0.090444s	69.63.180.173	172.16.0.122	TLSv1	95	Change Cipher Spec, Encrypted Handshake Message
9	0.000533s	172.16.0.122	69.63.180.173	TLSv1	1034	Application Data
10	0.189619s	69.63.180.173	172.16.0.122	TCP	52	443 → 54595 [ACK] Seq=981 Ack=1334 Win=5473 Len=0 TSval=3479126142 TSecr=…
11	0.073201s	69.63.180.173	172.16.0.122	TLSv1	1233	Application Data
12	0.011497s	172.16.0.122	69.63.190.22	HTTP	679	GET /home.php? HTTP/1.1


Frame 8: 109 bytes on wire (872 bits), 109 bytes captured (872 bits)
Ethernet II, Src: Cisco_31:07:33 (00:26:0b:31:07:33), Dst: Dell_c0:56:f0 (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: 938, Ack: 352, Len: 43
Secure Sockets Layer
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