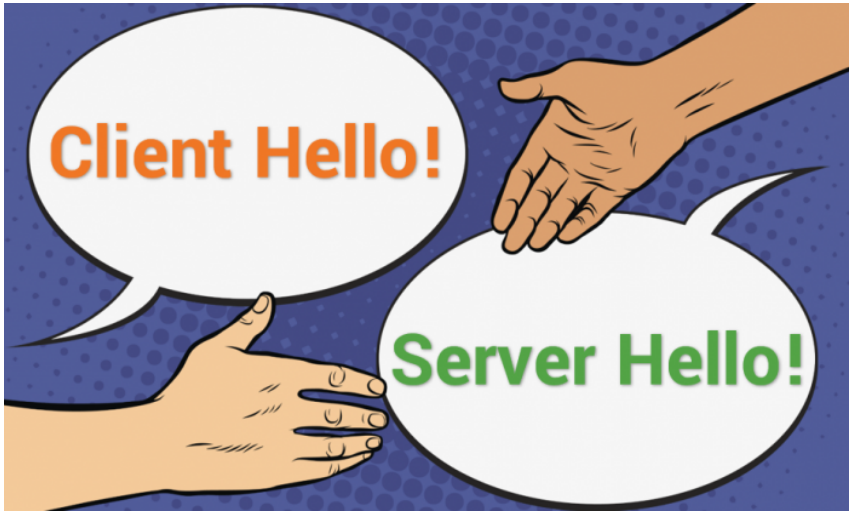
CS553: Crypto In Action Series

Image Source: Dall-E



CS 553

CRYPTOGRAPHY

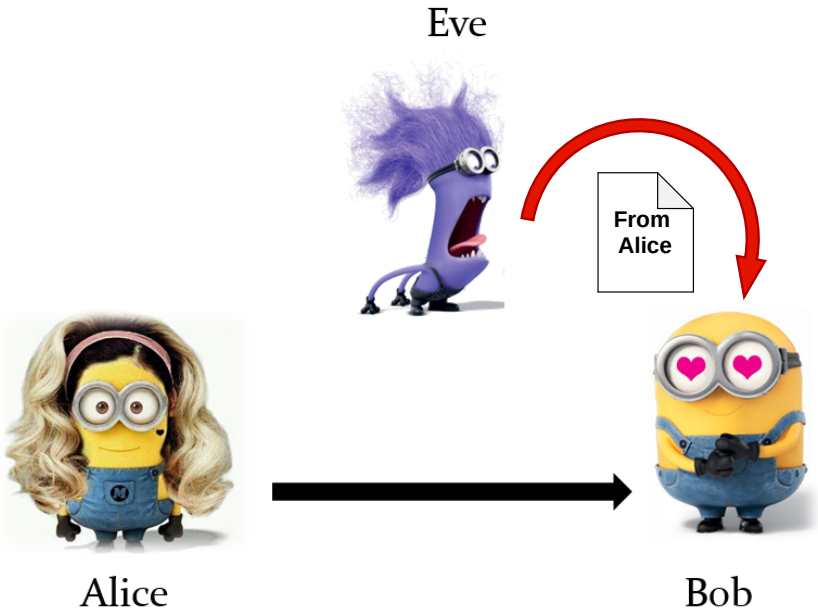
CIA: Crypto In Action

TLS 1.2 Handshake

Instructor
Dr. Dhiman Saha

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

Eve sends a message to Bob **claiming** to be Alice



How can Bob verify that the message was from Alice?

The Root of Trust — Solution

Digital Signatures, Certificates, Certificate Authorities

Establishing a connection with Google

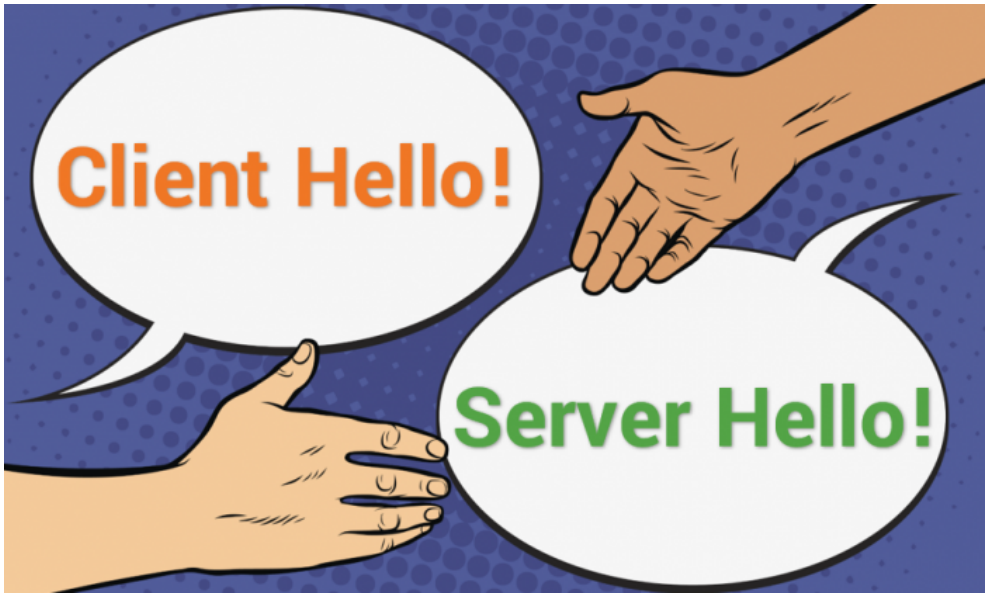
```
openssl s_client -connect www.google.com:443

CONNECTED(00000005)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = GTS CA 1O1
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.go
verify return:1
---
Certificate chain
0 s:C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google
i:C = US, O = Google Trust Services, CN = GTS CA 1O1
1 s:C = US, O = Google Trust Services, CN = GTS CA 1O1
i:OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
---
```

```
Server certificate
-----BEGIN CERTIFICATE-----
MIIEyTCCA7GgAwIBAgIRAOWJUBT/plbPAgAAAACAVf4wDQYJKoZIhvcNAQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczET
MBEGA1UEAxMKR1RTIENBIDFPMTAeFw0yMDExMDMwNzM5MThaFw0yMTAxMjYwNzM5
MThaMGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQH
Ew1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKEwpHb29nbGUgTExDMRcwFQYDVQQDEw53
d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABKLISJuNl7yH
5jysK2ykqVFELdZMVTRbFPRlBrEnB1a/6vZElDl+rPOfKoUwW2CN1jKDqiXon1xK
Iz6vKEwTmG6jggJdMIICWTAOBgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYB
BQUHAwEwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQUTWQgwfJywJC6xNo6YGWnciqQ
db8wHwYDVR0jBBgwFoAUmNH4bhDrz5vsYJ8YkBug630J/SswaAYIKwYBBQUHAQEE
XDBaMCsGCCsGAQUFBzABhh9odHRwOi8vb2NzcC5wa2kuZ29vZy9ndHMxbzFjb3Jl
MCsGCCsGAQUFBzAChh9odHRwOi8vcGtpLmdvb2cvZ3NyMi9HVFMxTzEuY3J0MBkG
A1UdEQQSMBCCDnd3dy5nb29nbGUuY29tMCEGA1UdIAQaMBgwCAYGZ4EMAQICMAwG
CisGAQQB1nkCBQMwMwYDVR0fBCwwKjAooCagJIYiaHR0cDovL2NybC5wa2kuZ29v
Zy9HVFMxTzFjb3JlLmNybDCCAQUGCisGAQQB1nkCBAIEgfYEgfMA8QB3APZclC/R
dzAiFFQYCDCUVo7jTRMZM7/fDC8gC8xO8WTjAAABdY1Cr9sAAAQDAEgwRgIhAKKl
OswFoVax1Gm+OFauNaszFKuS8tkzs2UN+POrEXP2AiEAsxbJcnseAqdUAG7GrrHt
cO1EgTRSEoq4Bi9eT7k98KkAdgCUILwejtWNbIhzH4KLIiwNOdpNXmxPlD1h204v
WE2iwgAAAXWNQq/jAAAEAwBHMEUCIQC5K2xWZDKpmY2VVEQeN1ZFXQdZ/4kyiOHb
U9EA/S89cwIgTUxrROzrhzIGQywvwhvtjA8+/9y2nm8xnjHtLNSlaZ4wDQYJKoZI
hvcNAQELBQADggEBAM5ae5eSabuI69PK7MMd+VKWNWvTkduN5SsNTNH2hMU+A2xJ
Rd1qbhQLn8FqqYgCmAHtaOt5YuKIctTLYmevZaWEDBqHy1rhZhW1E5Lcrx/Q1VD0
AR+qA9Li++vB2Sjk+cBIpyaMsk27IJz6yCA4lJKUYyxdYEMW54DWTFxRVIQ0uC1d
VYJ82bqdq0z839XRATdfZP0LRvld1lVqtN/TdES6pngj8FzhpyLvp1EfxaoAnTal
4oVg67pw7d42SpfMsYF1j8EC55iuyuLBLgeZ71B37dyGo3ZvfkTdGXwEFAEhn/eC
ne2mhh7QQGKD3Dp5mHmxPXDAQlJ6phDvsHVXCpE=
-----END CERTIFICATE-----
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com

issuer=C = US, O = Google Trust Services, CN = GTS CA 1O1

---
```

What is inside a certificate?

```
openssl x509 -text -noout
-----BEGIN CERTIFICATE-----
--snip--
-----END CERTIFICATE-----
```

TLS Handshake

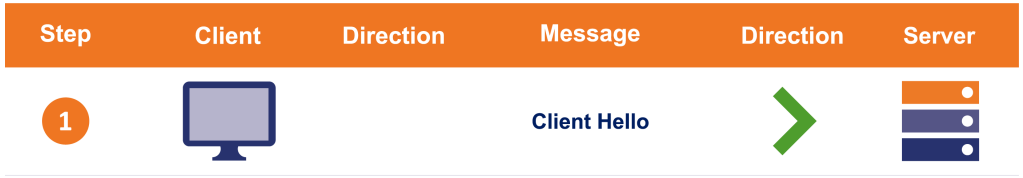


Three Main Steps

- Exchanging cipher suites and parameters
- Authenticating one or both parties
- Creating/Exchanging symmetric session keys

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

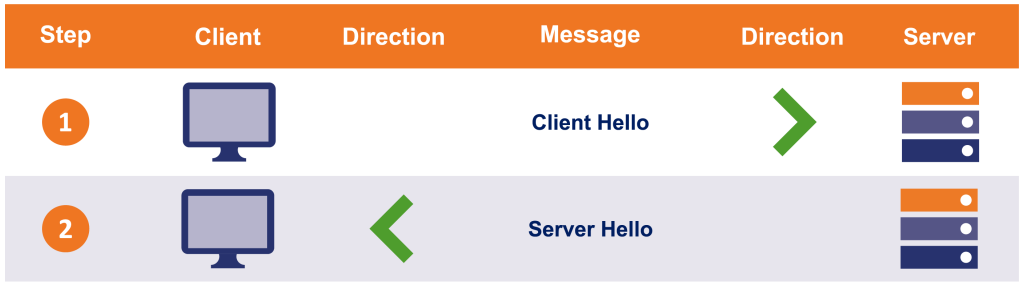
The Client Hello Message



- Lists the clients capabilities
- Also includes "client random"

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

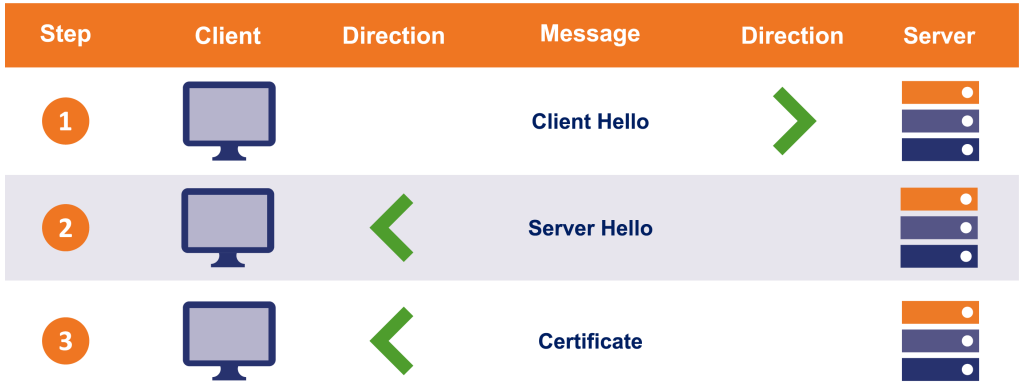
The Sever Hello Response



- Lists parameters selected from provided list
- Also includes "server random"
- Connection terminates if no common capabilities

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

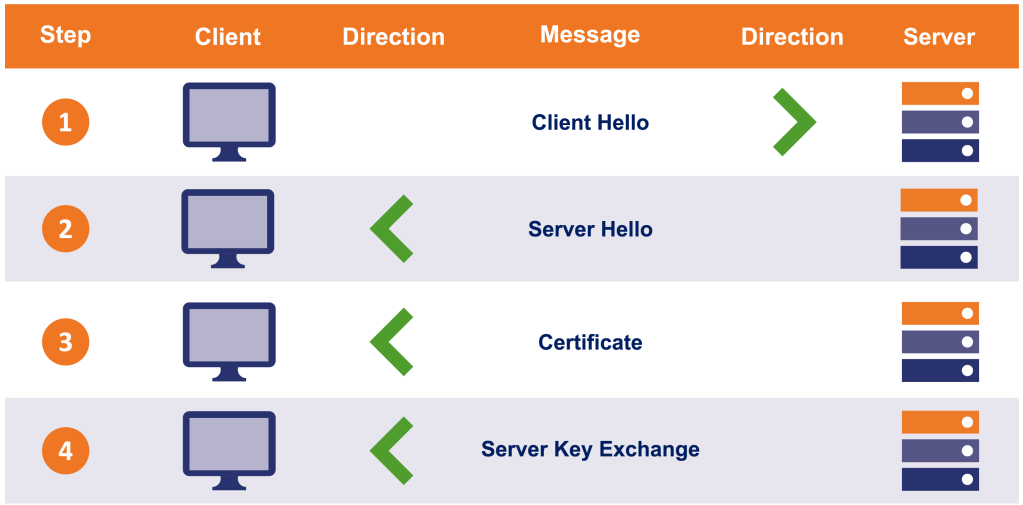
The Server Certificate Message



- Server sends its SSL certificate chain
- SSL certificate is signed by a CA
- Allows the client to verify that the certificate is legitimate
- Also verify server's possession of of the certificates private key

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

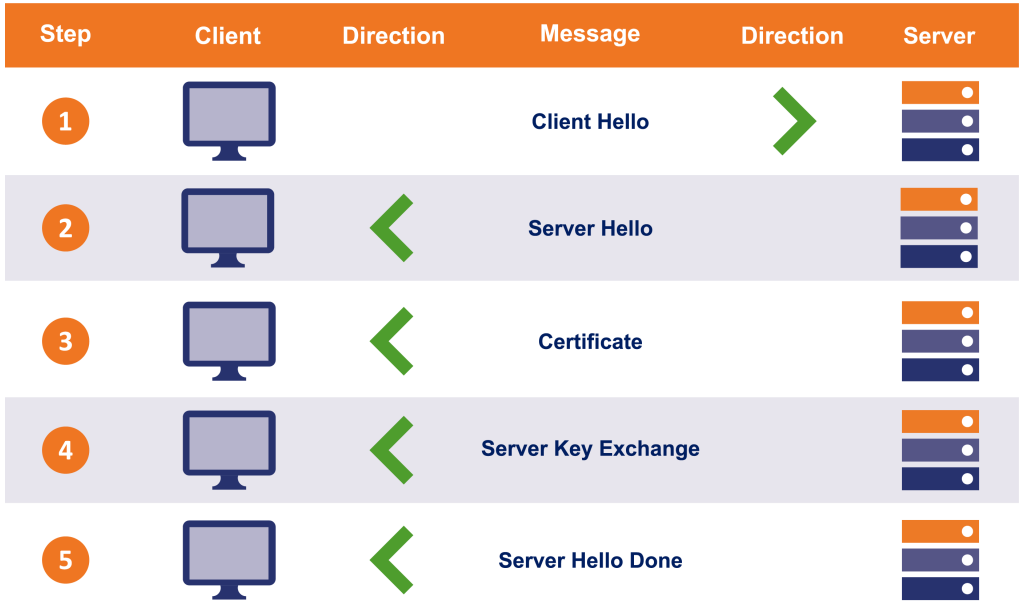
Key Exchange Related Info (Optional) for DH



- The server provides additional data to derive shared secret

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

The Server Hello Done Message



- Tells the client that it has sent over all its messages

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

Client's Contribution to Deriving the Session Key

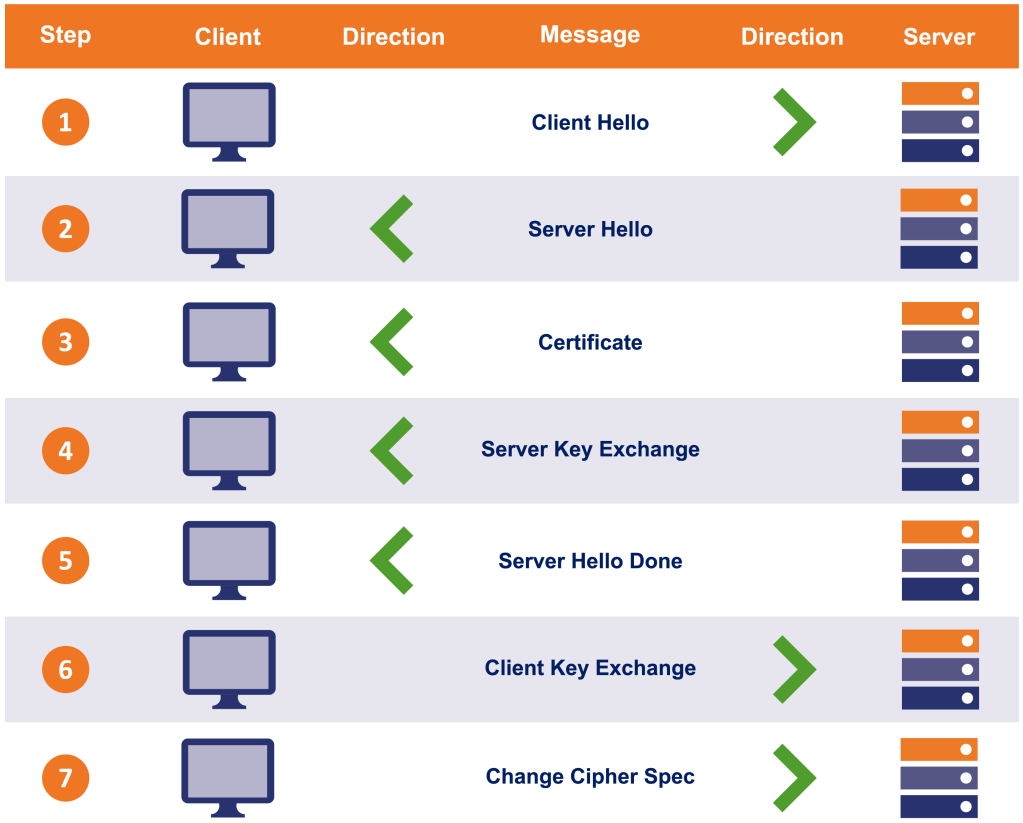
Step	Client	Direction	Message	Direction	Server
1			Client Hello	>	
2		<	Server Hello		
3		<	Certificate		
4		<	Server Key Exchange		
5		<	Server Hello Done		
6			Client Key Exchange	>	

- The Client derives shared secret
- May need to send info based on key-exchange scheme

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

The Change Cipher Spec Message

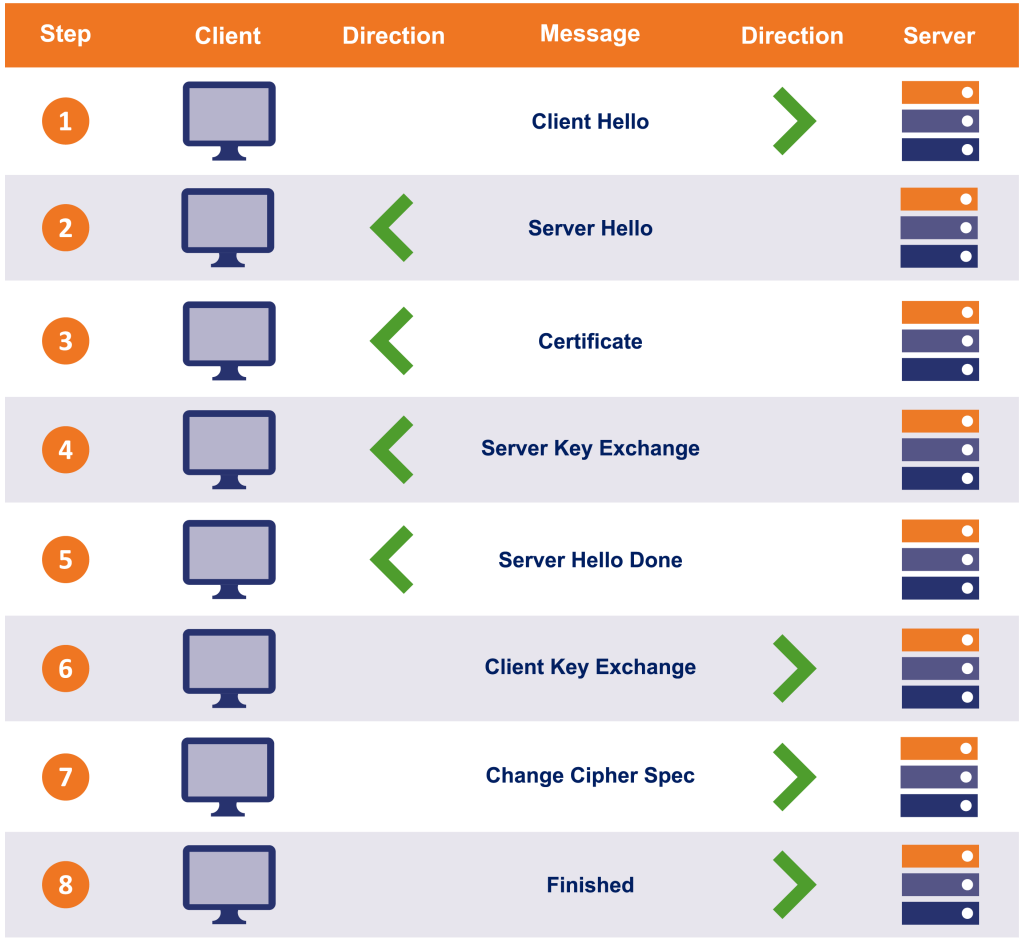
Client Side



- Session key generated
- Switching to encrypted communication

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

The `Finished` message

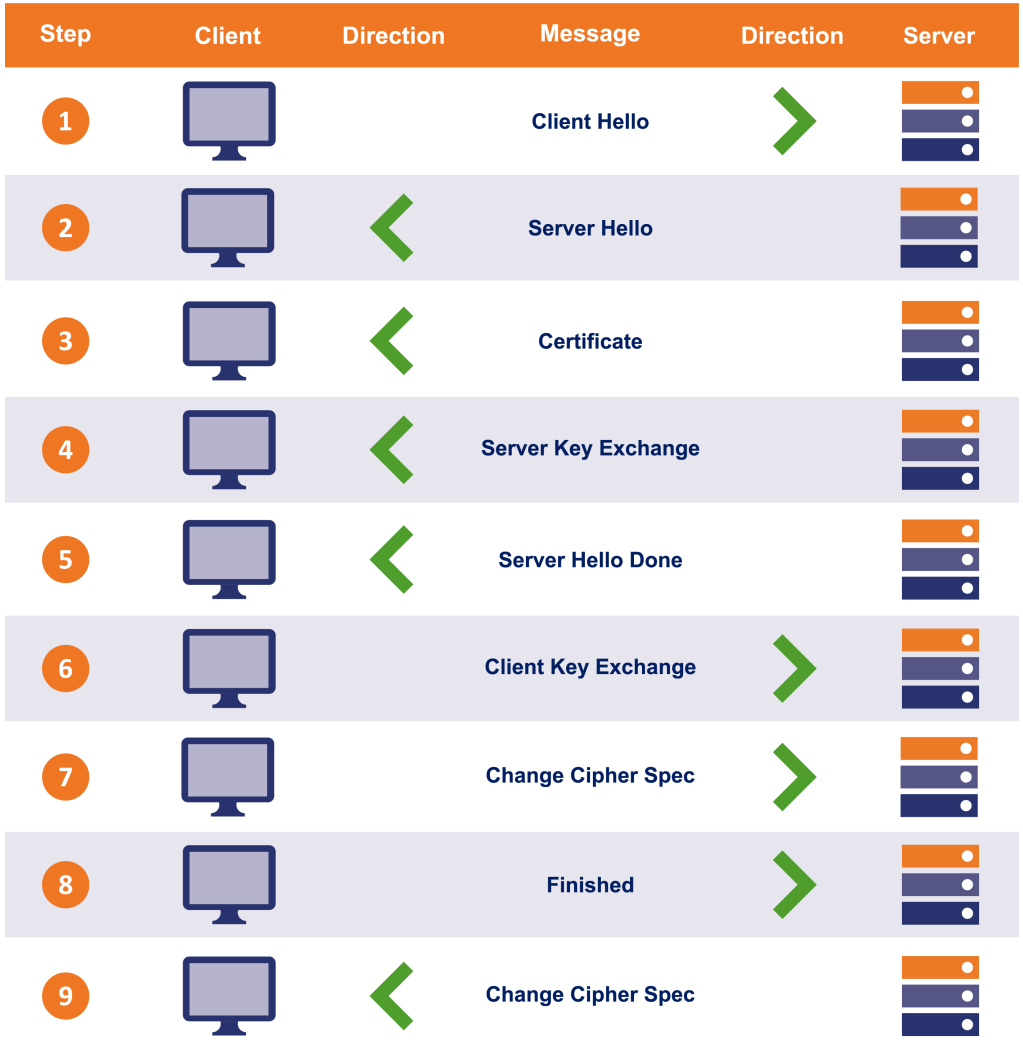


- Encrypted with session key
- Indicates that the handshake is complete on the client side
- Contains MAC
- To verify that handshake was not tampered with

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

The Change Cipher Spec Message

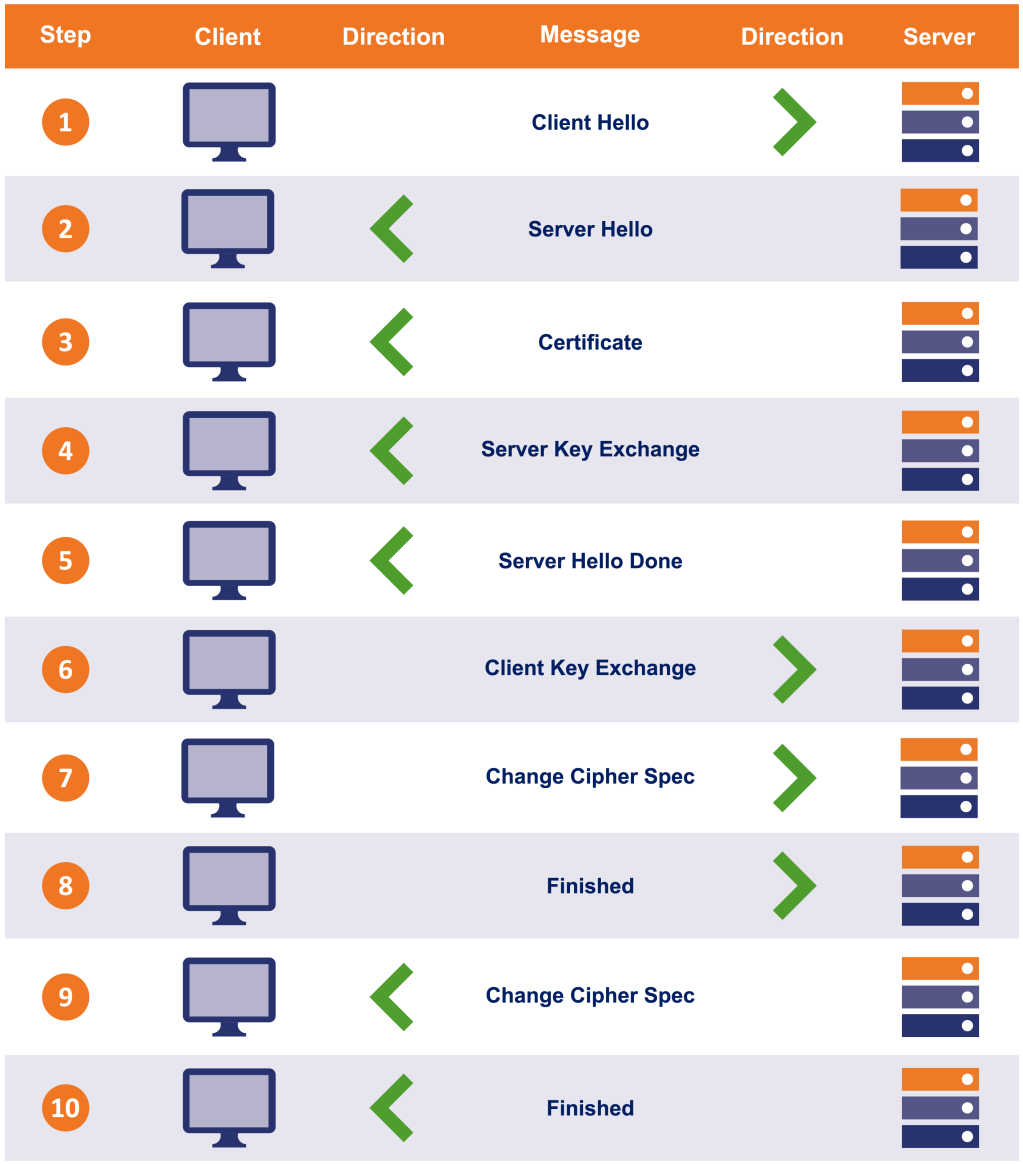
Server Side



- Session key generated
- Switching to encrypted communication

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/

The Finished message



- Sends Finished message using the symmetric session key generated,
- Also performs integrity-check of the handshake

Image Source: https://www.thesslstore.com/blog/explaining-ssl-handshake/