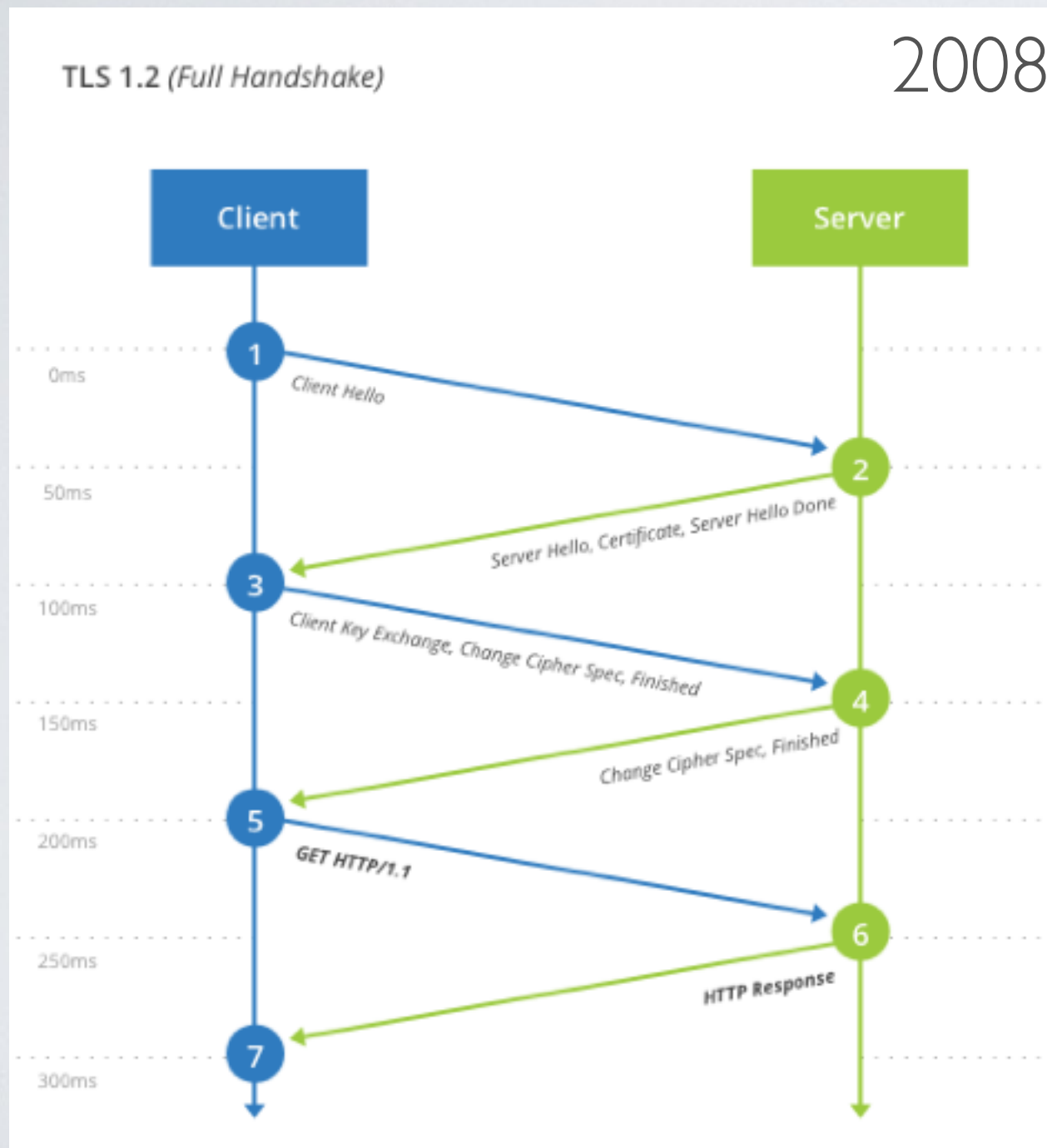


# TLS - Transport Layer Protection

- ➔ Transport Layer Security (formerly SSL) provides
  - **integrity:** authentication handshake
  - **confidentiality:** end-to-end secure channel
- ✓ Prevents all kinds of eavesdropping and spoofing for application protocols e.g HTTP + TLS = HTTPS
- ⦿ 2-10 times slower than an insecure TCP connection

# TLS Authentication Handshake 1.2 vs 1.3



source <https://www.cloudflare.com/learning-resources/tls-1-3/>