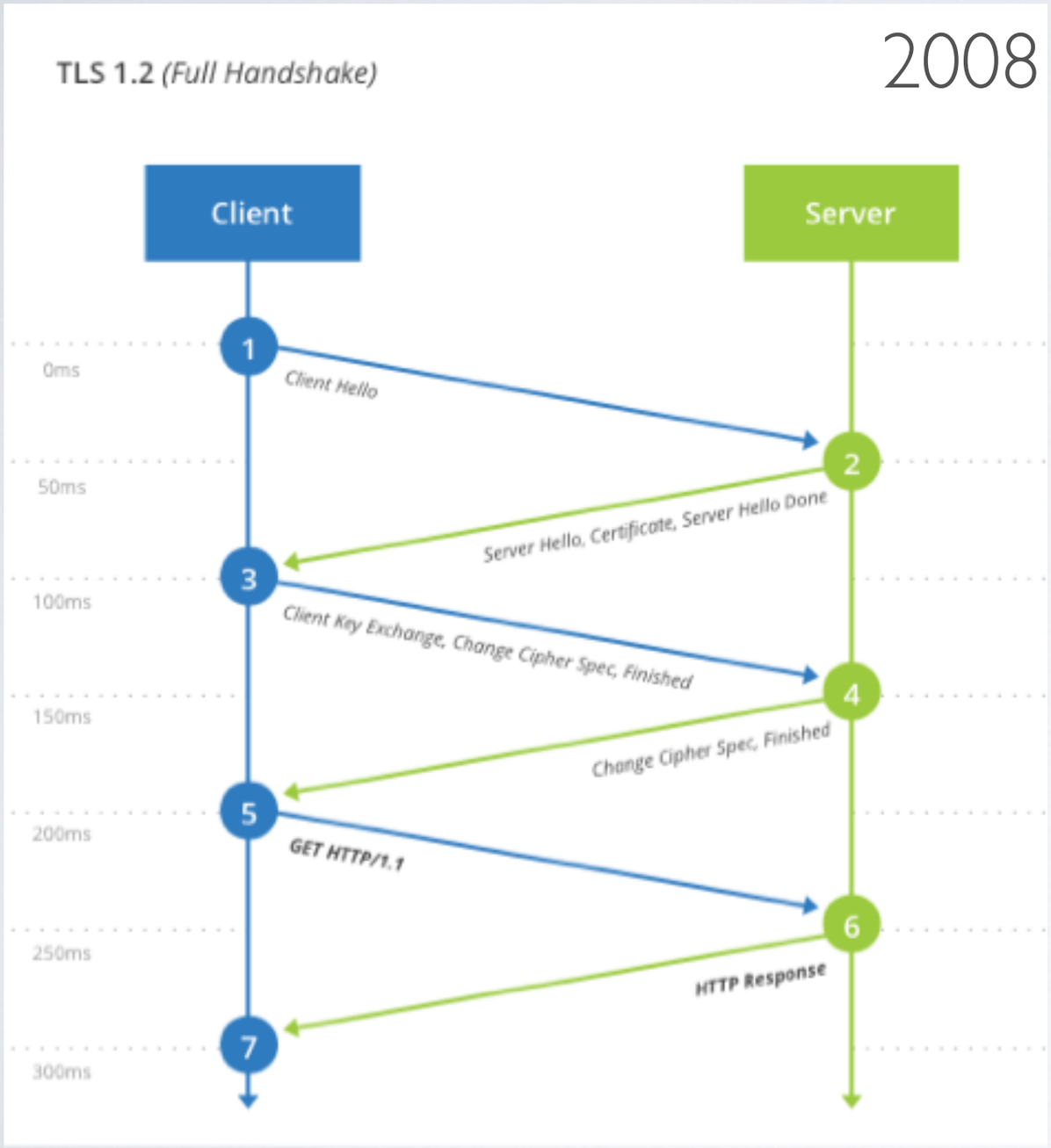
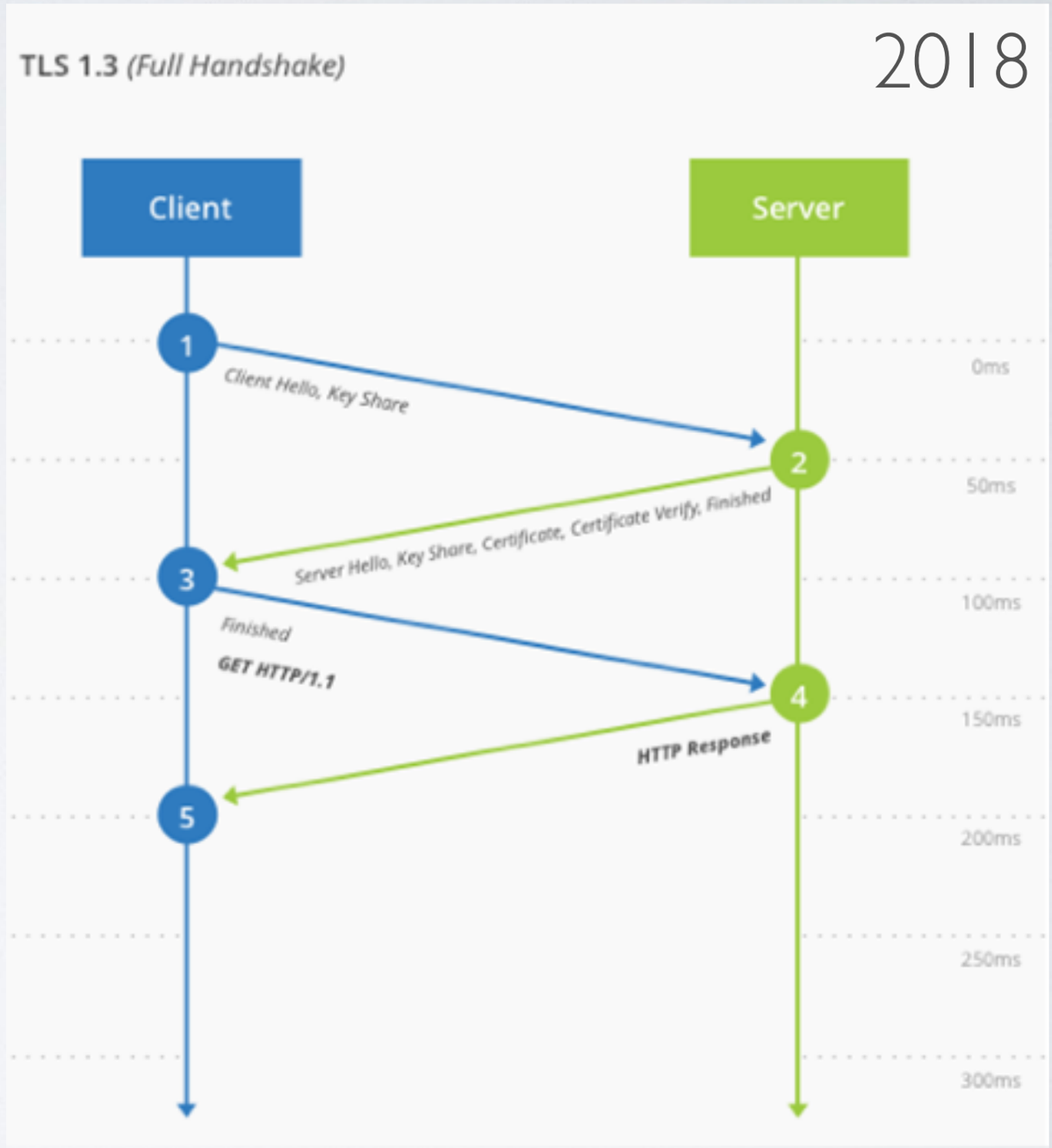
TLS Authentication Handshake 1.2 vs 1.3





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

Specific attacks of HTTPS

Webpages can be delivered either with HTTPS or HTTP

➡ The browser can automatically switch between HTTP and HTTPS

Sometime within the same webpage (mixed-content)
e.g the main page loads over HTTPS
but images, scripts or css load with HTTP

An attacker can do a MitM attack and remove the SSL protection

➡ **SSLStripping** attack (challenge coming next)