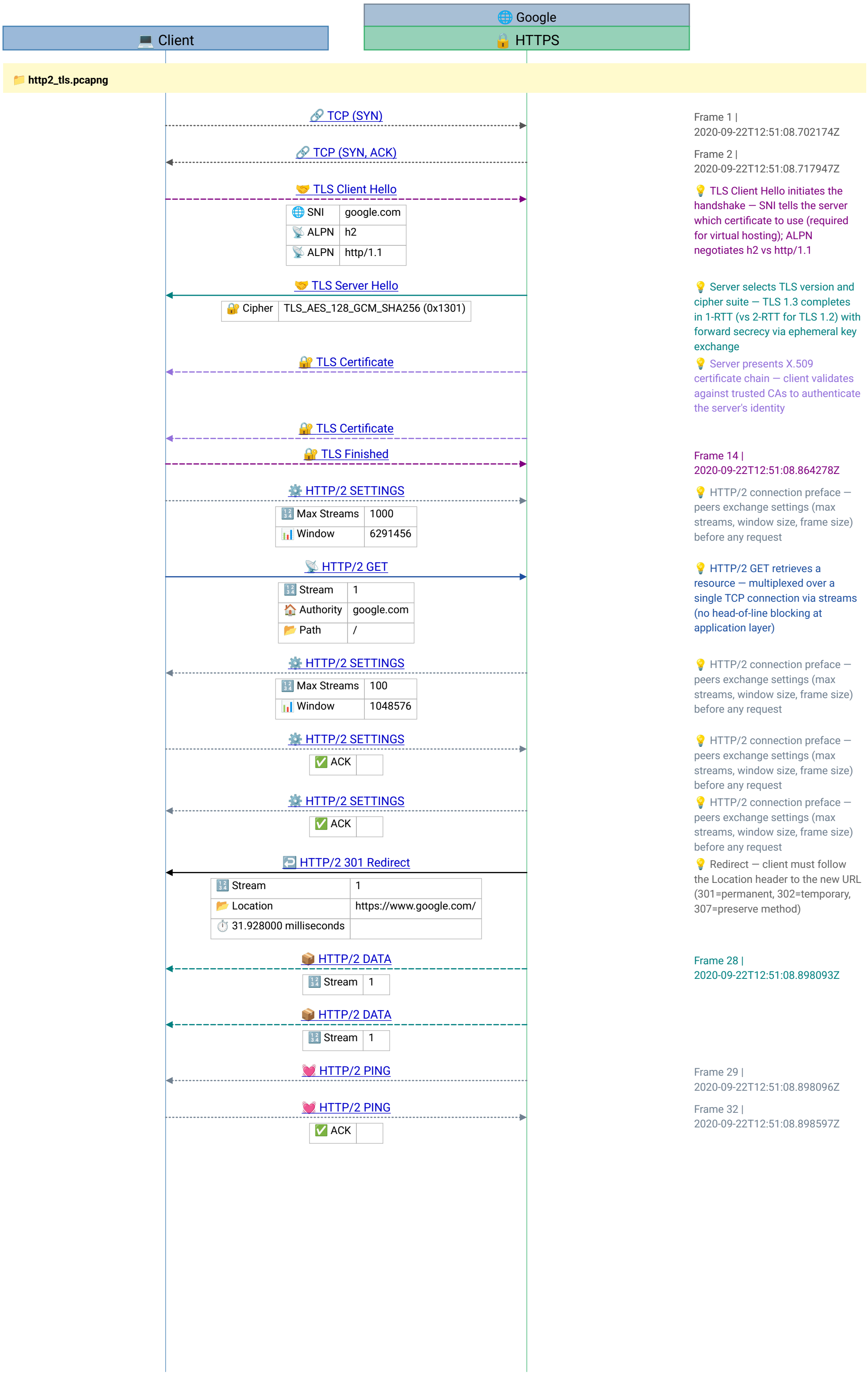
Client
Google
HTTPS
http2_tls.pcapng
TCP (SYN)
TCP (SYN, ACK)
TLS Client Hello
SNI google.com
ALPN h2
ALPN http/1.1
TLS Server Hello
Cipher TLS_AES_128_GCM_SHA256 (0x1301)
TLS Certificate
TLS Certificate
TLS Finished
HTTP/2 SETTINGS
Max Streams 1000
Window 6291456
HTTP/2 GET
Stream 1
Authority google.com
Path /
HTTP/2 SETTINGS
Max Streams 100
Window 1048576
HTTP/2 SETTINGS
ACK
HTTP/2 SETTINGS
ACK
HTTP/2 301 Redirect
Stream 1
Location https://www.google.com/
31.928000 milliseconds
HTTP/2 DATA
Stream 1
HTTP/2 DATA
Stream 1
HTTP/2 PING
HTTP/2 PING
ACK
Frame 1 | 2020-09-22T12:51:08.702174Z
Frame 2 | 2020-09-22T12:51:08.717947Z
TLS Client Hello initiates the handshake — SNI tells the server which certificate to use (required for virtual hosting); ALPN negotiates h2 vs http/1.1
Server selects TLS version and cipher suite — TLS 1.3 completes in 1-RTT (vs 2-RTT for TLS 1.2) with forward secrecy via ephemeral key exchange
Server presents X.509 certificate chain — client validates against trusted CAs to authenticate the server's identity
Frame 14 | 2020-09-22T12:51:08.864278Z
HTTP/2 connection preface — peers exchange settings (max streams, window size, frame size) before any request
HTTP/2 GET retrieves a resource — multiplexed over a single TCP connection via streams (no head-of-line blocking at application layer)
HTTP/2 connection preface — peers exchange settings (max streams, window size, frame size) before any request
HTTP/2 connection preface — peers exchange settings (max streams, window size, frame size) before any request
HTTP/2 connection preface — peers exchange settings (max streams, window size, frame size) before any request
Redirect — client must follow the Location header to the new URL (301=permanent, 302=temporary, 307=preserve method)
Frame 28 | 2020-09-22T12:51:08.898093Z
Frame 29 | 2020-09-22T12:51:08.898096Z
Frame 32 | 2020-09-22T12:51:08.898597Z