Using Wireshark to Analyze Core Applications – FTP, HTTPs, and TLS

Chris Greer
NETWORK ANALYST

@packetpioneer www.packetpioneer.com

Module Overview

Let's talk FTP

- FTP vs. SFTP vs. TFTP
- Common issues in file transfers

Analyzing HTTPs

- Do we have to decrypt to troubleshoot?

Analyzing TLS

File Transfer Protocol

Simple File Transfer

FTP Client or built-in browser

File Transfer Methods

FTP

- Easy file transfer
- Not a secure protocol (clear text on wire)

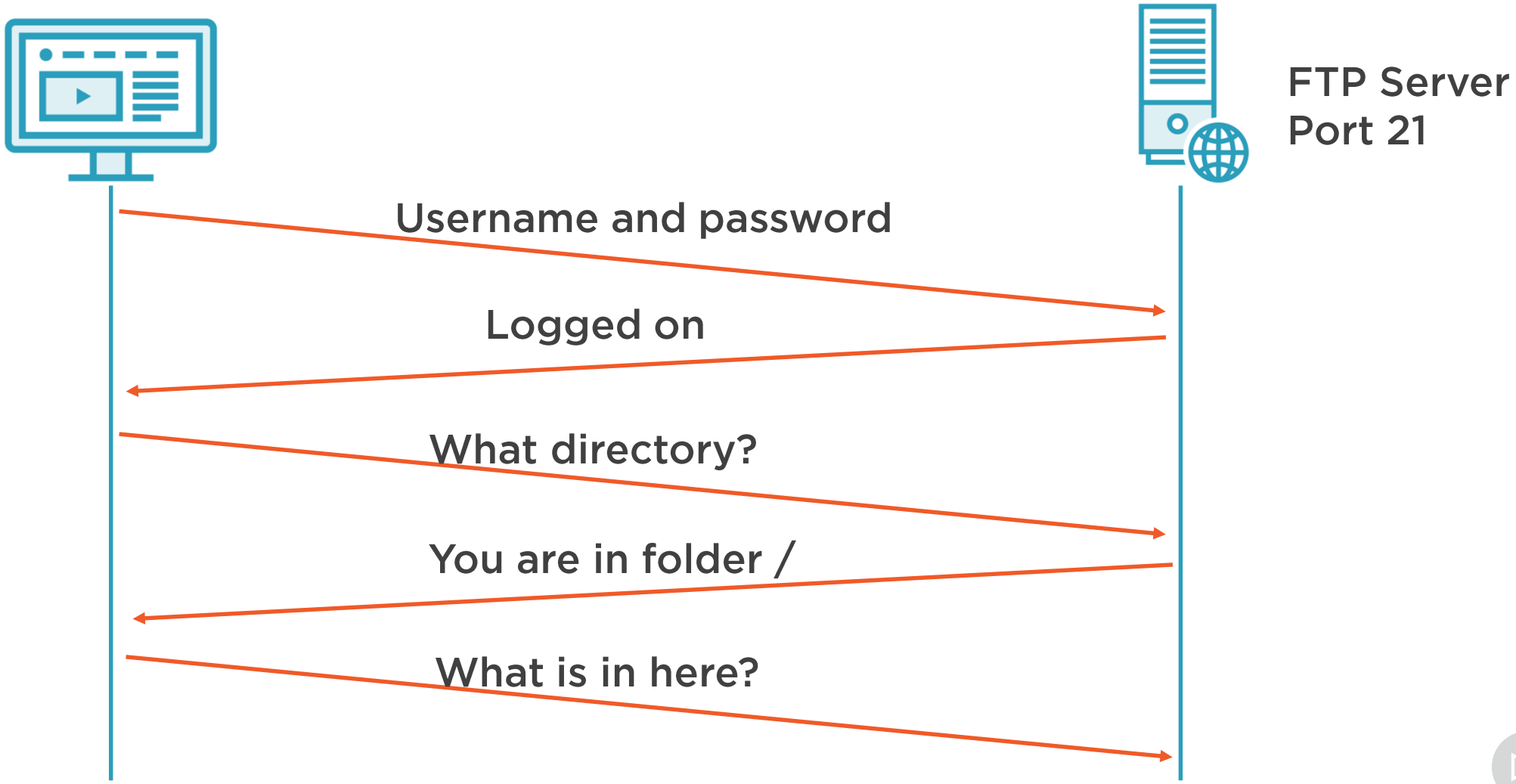
sFTP

- Secure FTP
- Adds a layer of transport security - SSH

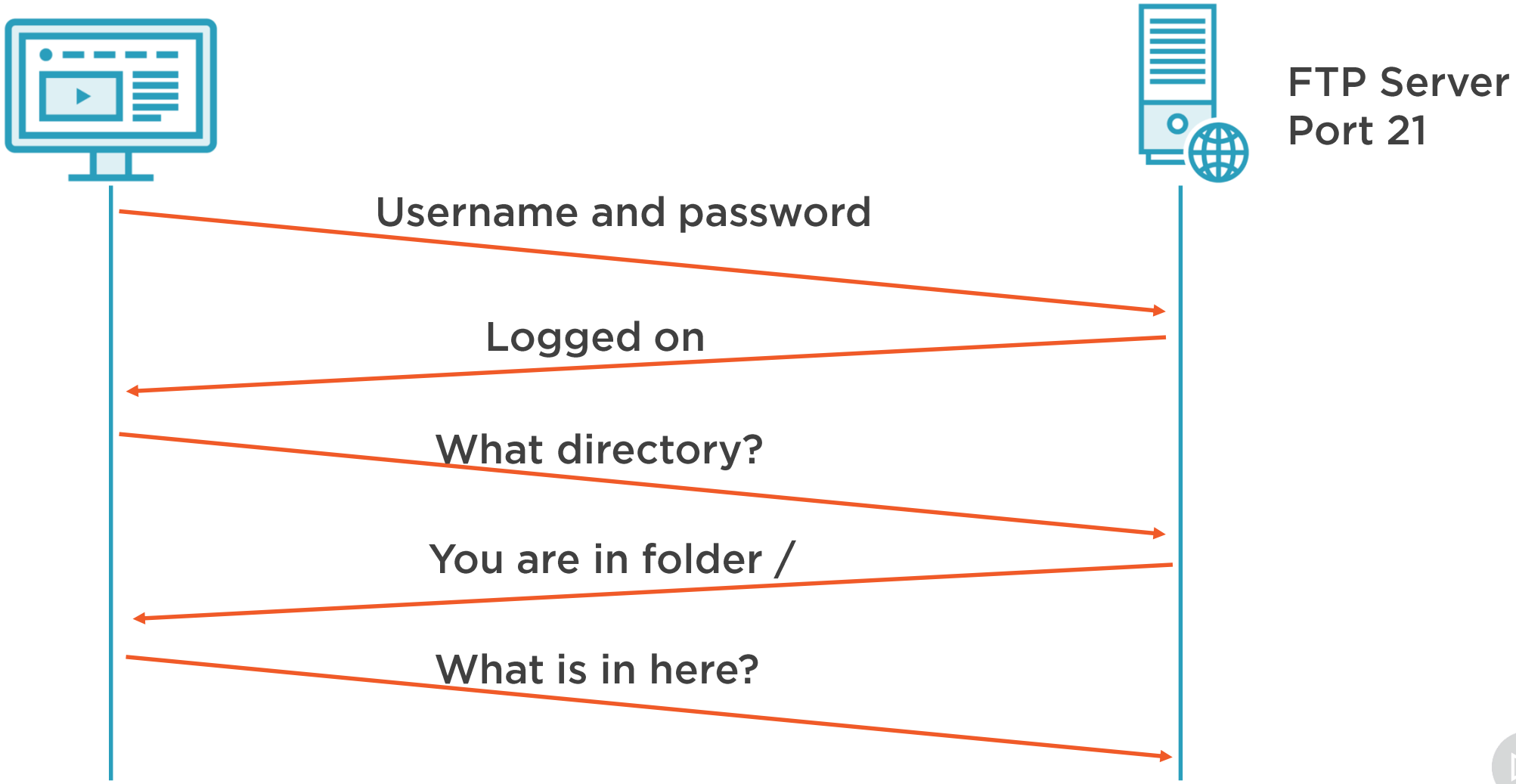
TFTP

- Trivial File Transfer Protocol – used within LAN over UDP
- Configuration files to network devices

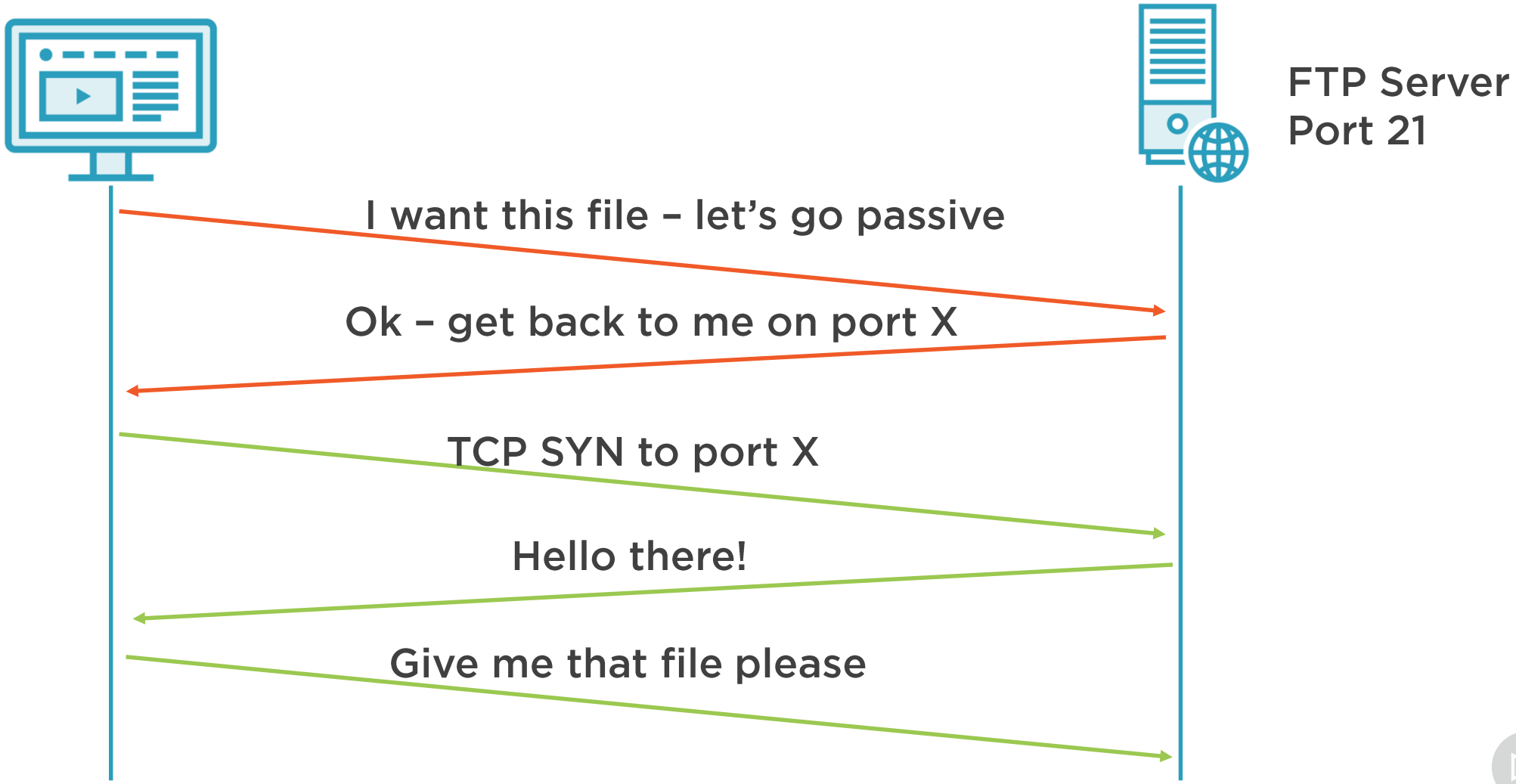
FTP Connect and Login



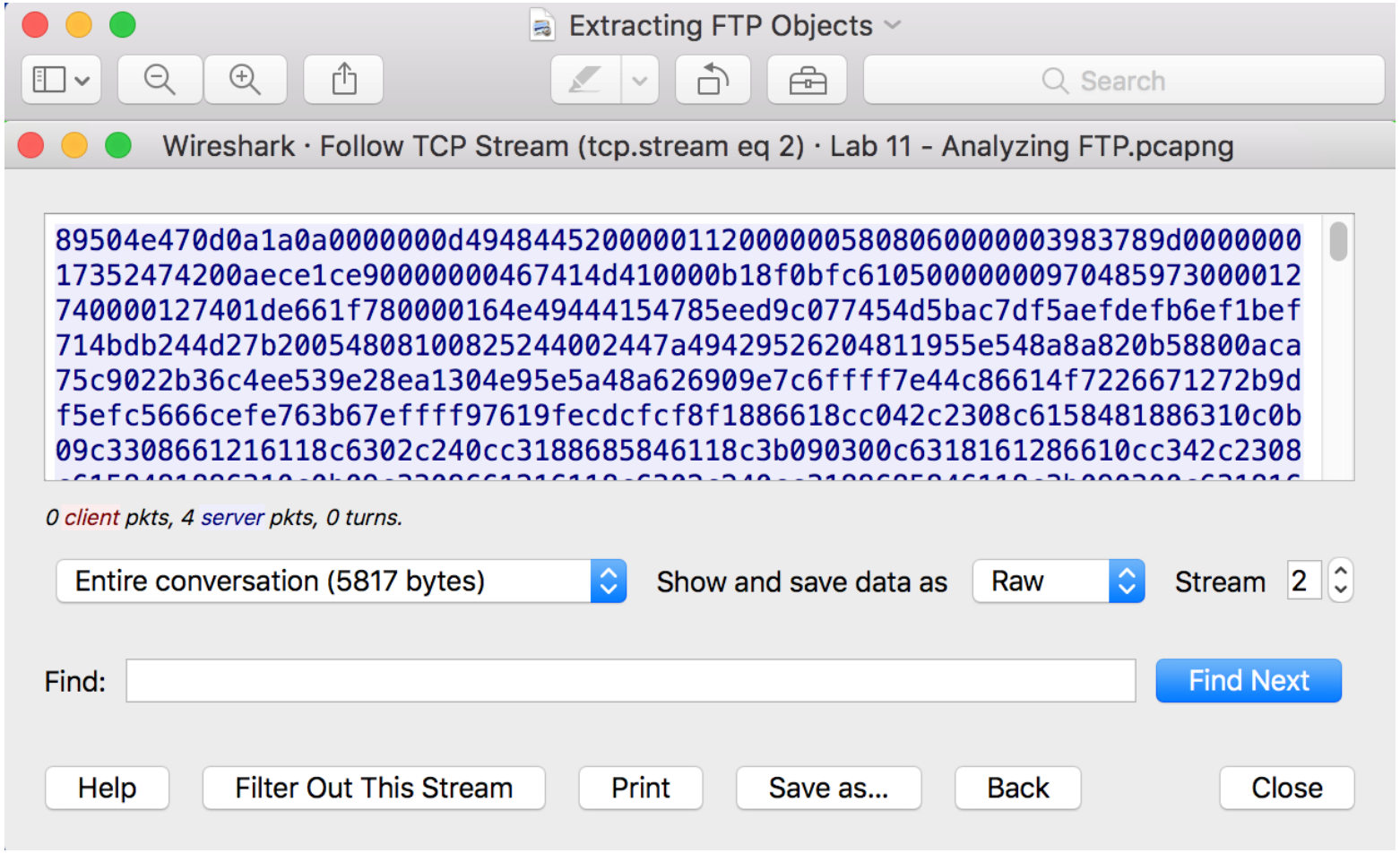
FTP Connect and Login



File Transfer



Exporting FTP Files in Wireshark

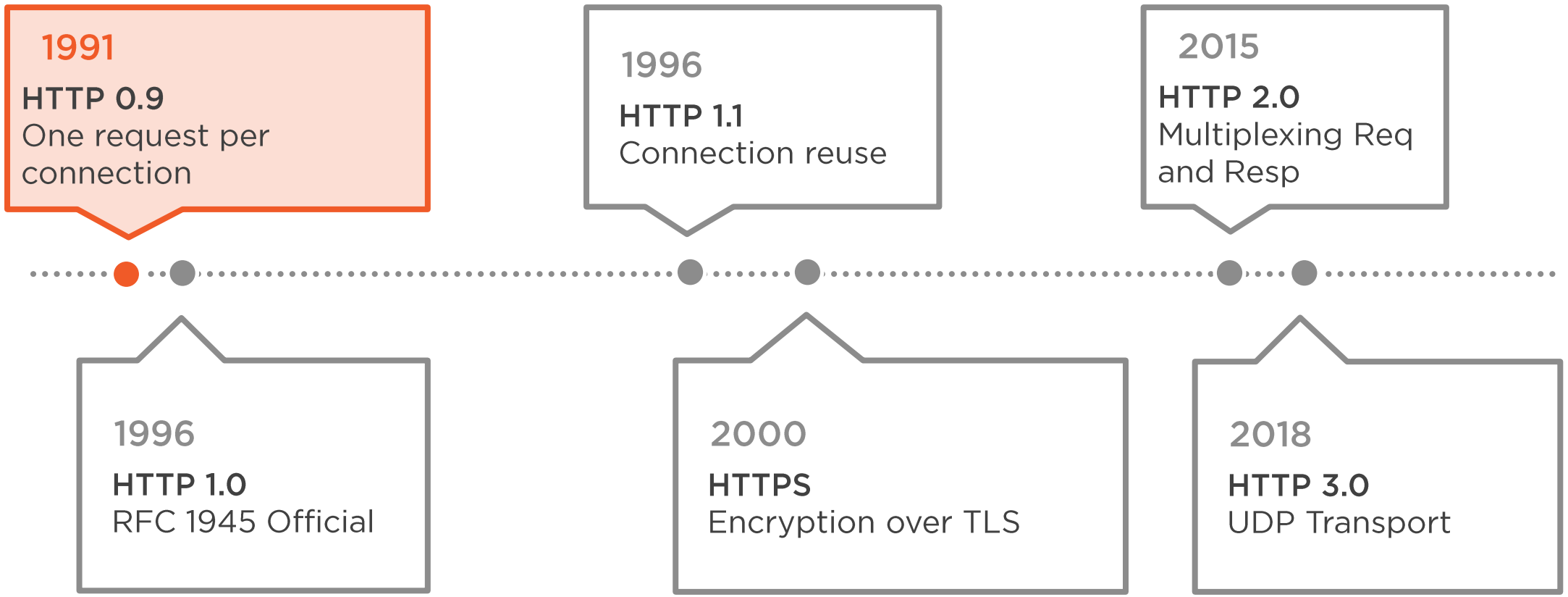


Demo

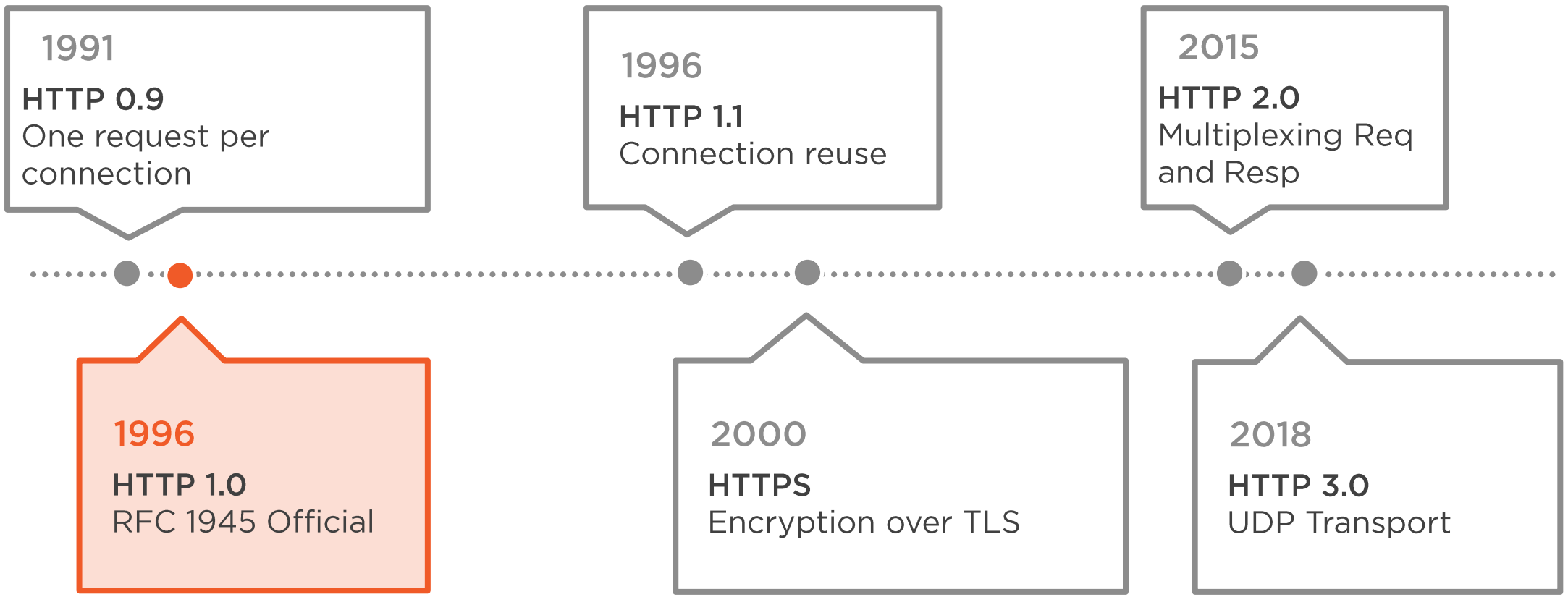
Analyzing FTP with Wireshark

HTTPs and TLS

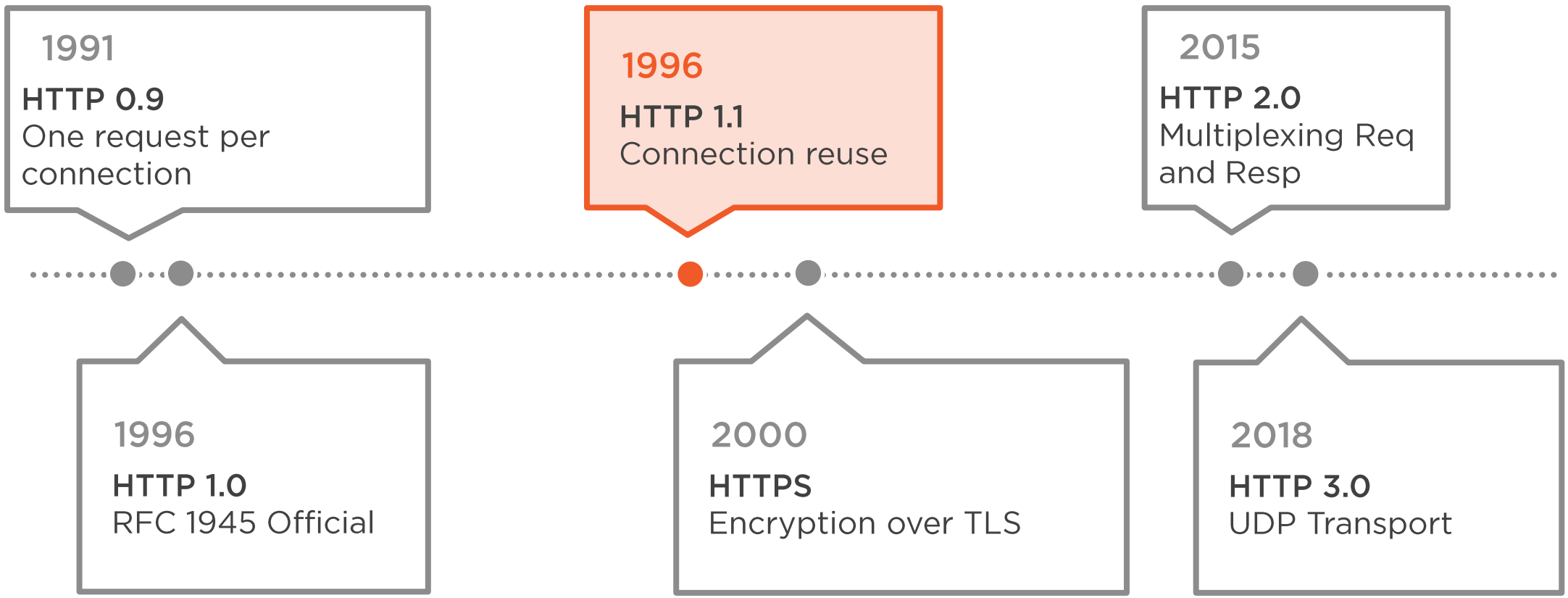
Hypertext Transfer Protocol



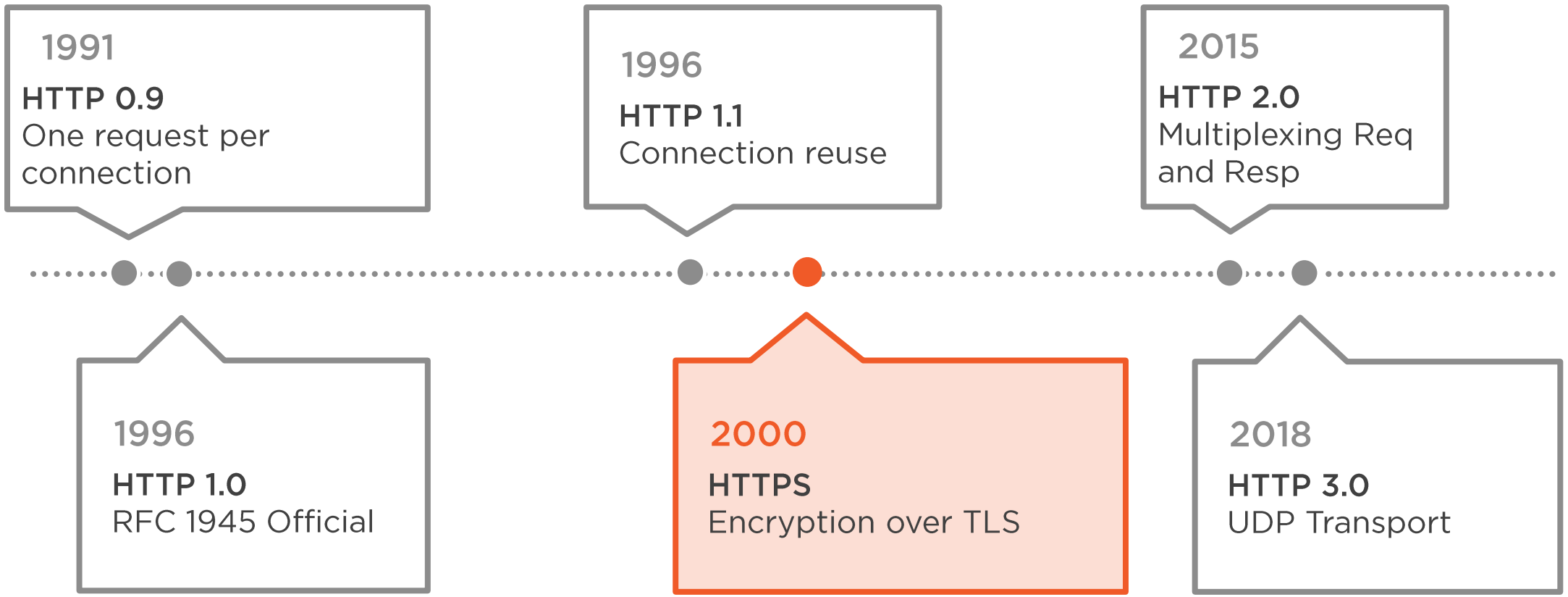
Hypertext Transfer Protocol



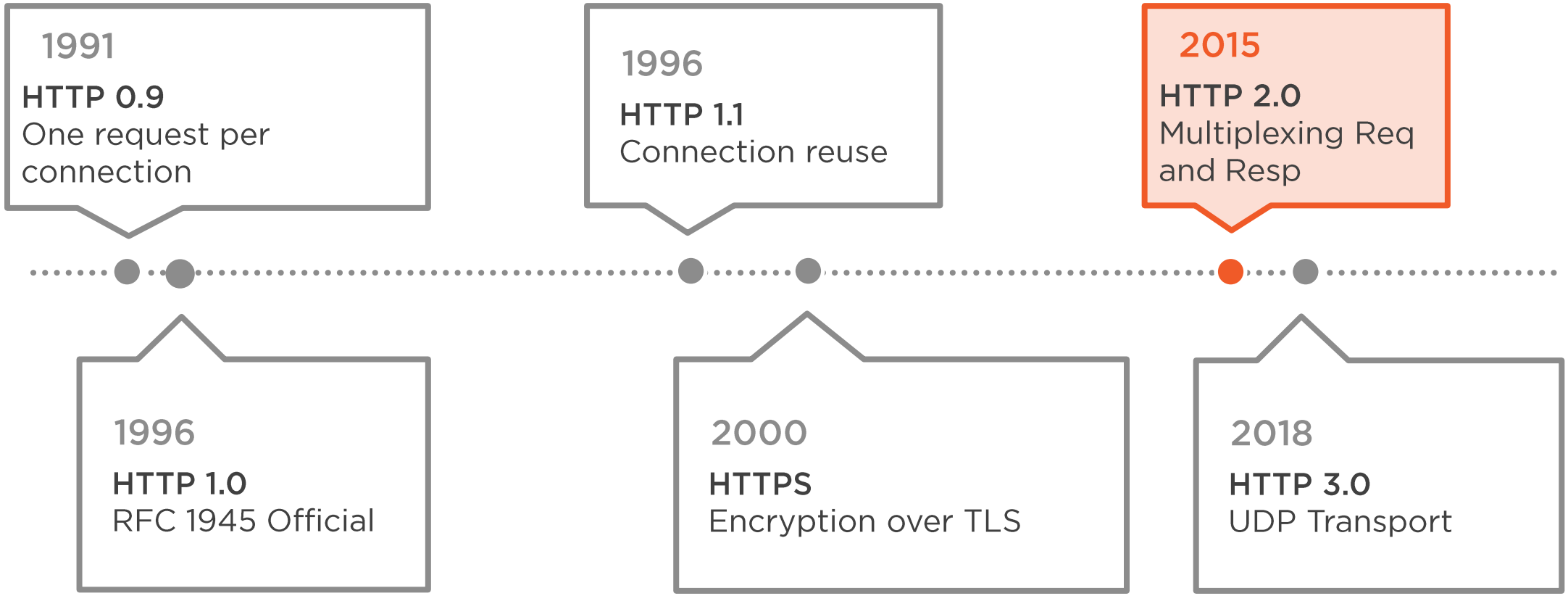
Hypertext Transfer Protocol



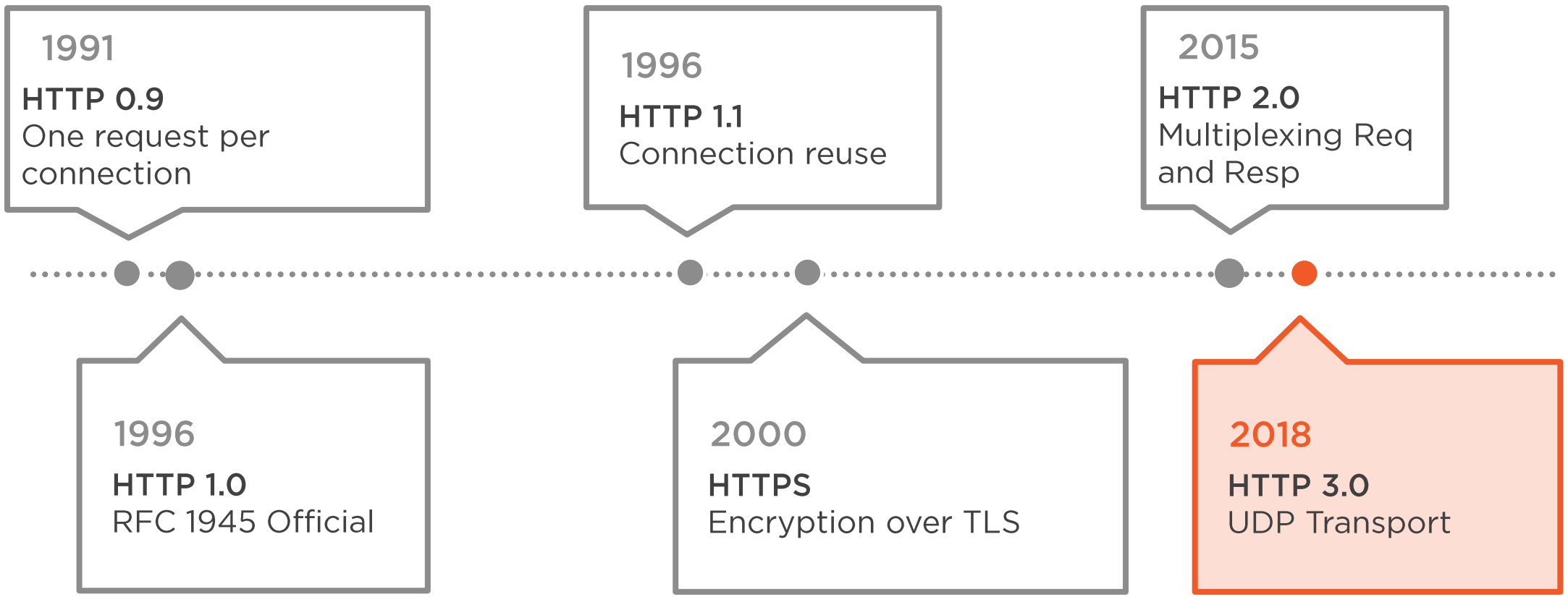
Hypertext Transfer Protocol



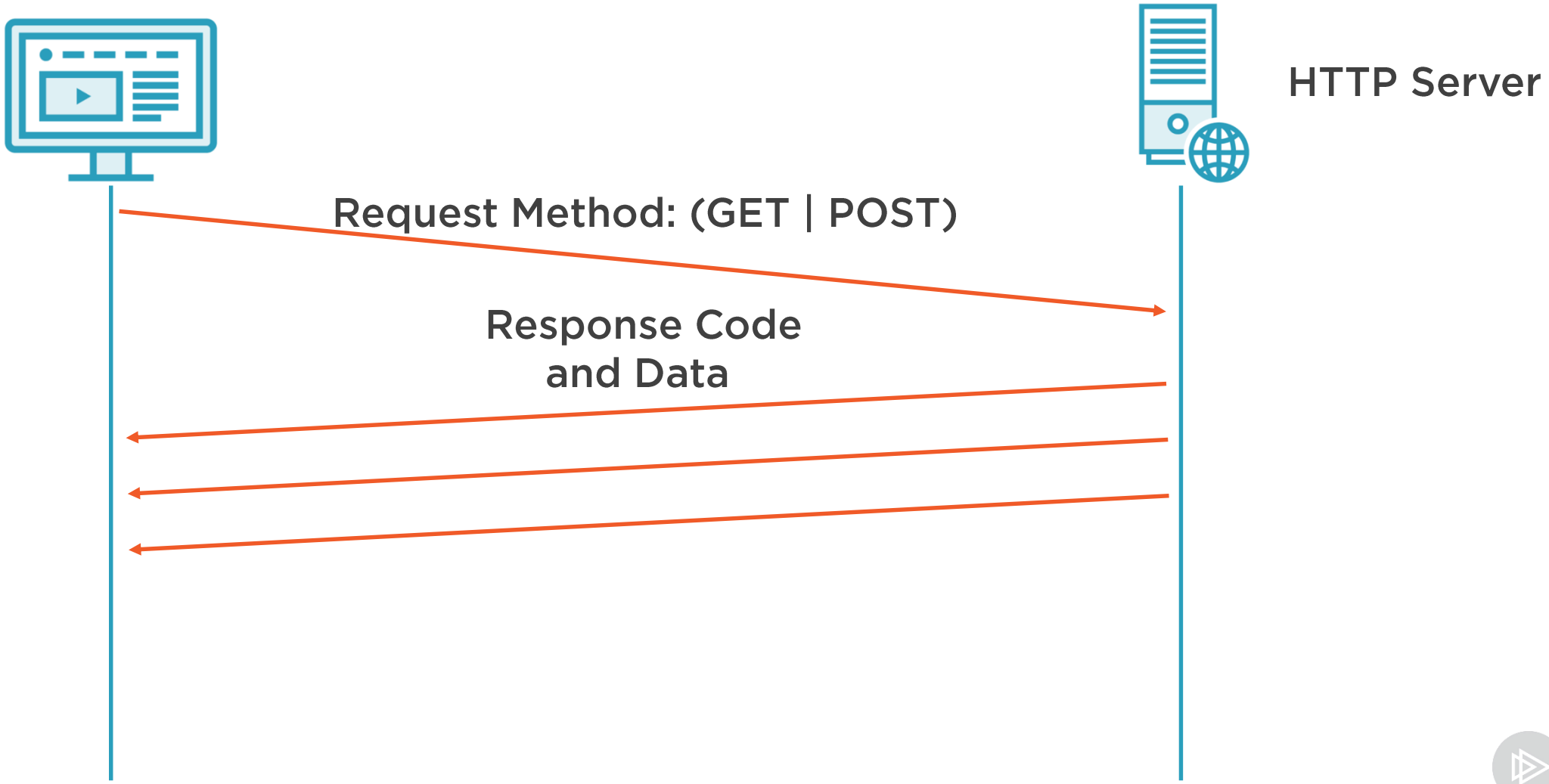
Hypertext Transfer Protocol



Hypertext Transfer Protocol



HTTP Request and Response



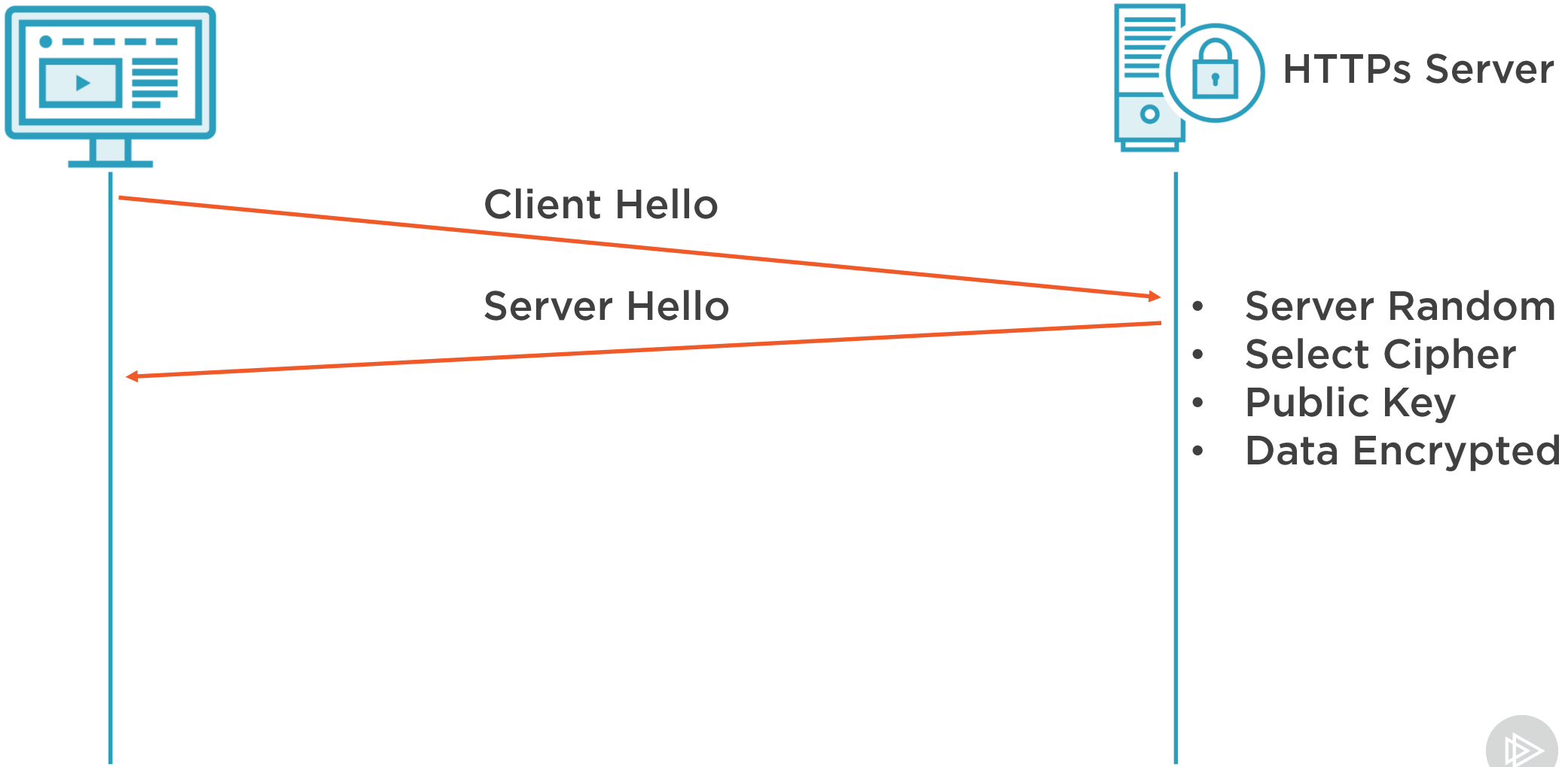
HTTP over TLS 1.3

HTTPs Server

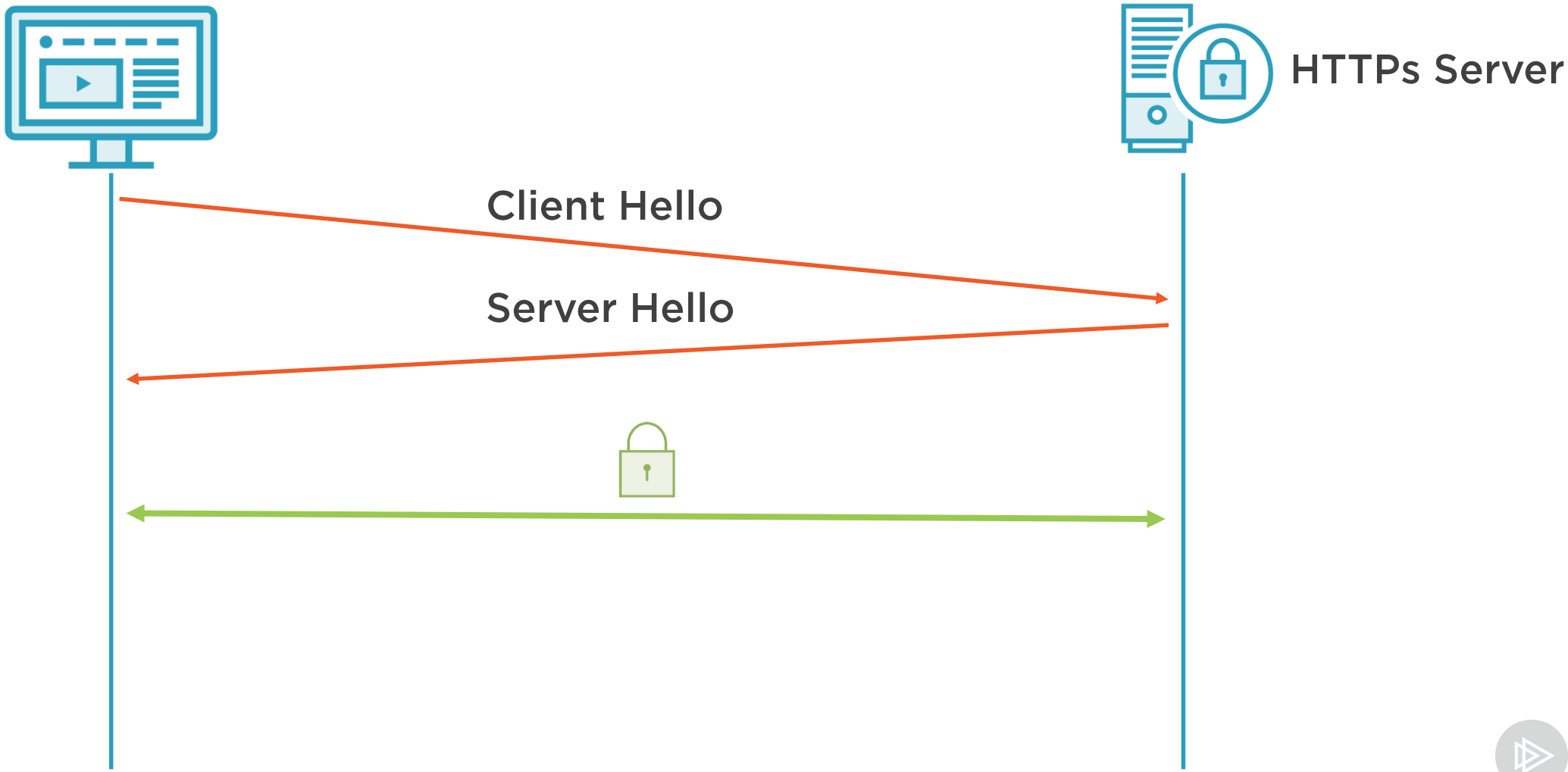
Client Hello

- Client Key Gen
- Client Random
- Cipher Suites
- Public Keys
- Protocol Versions

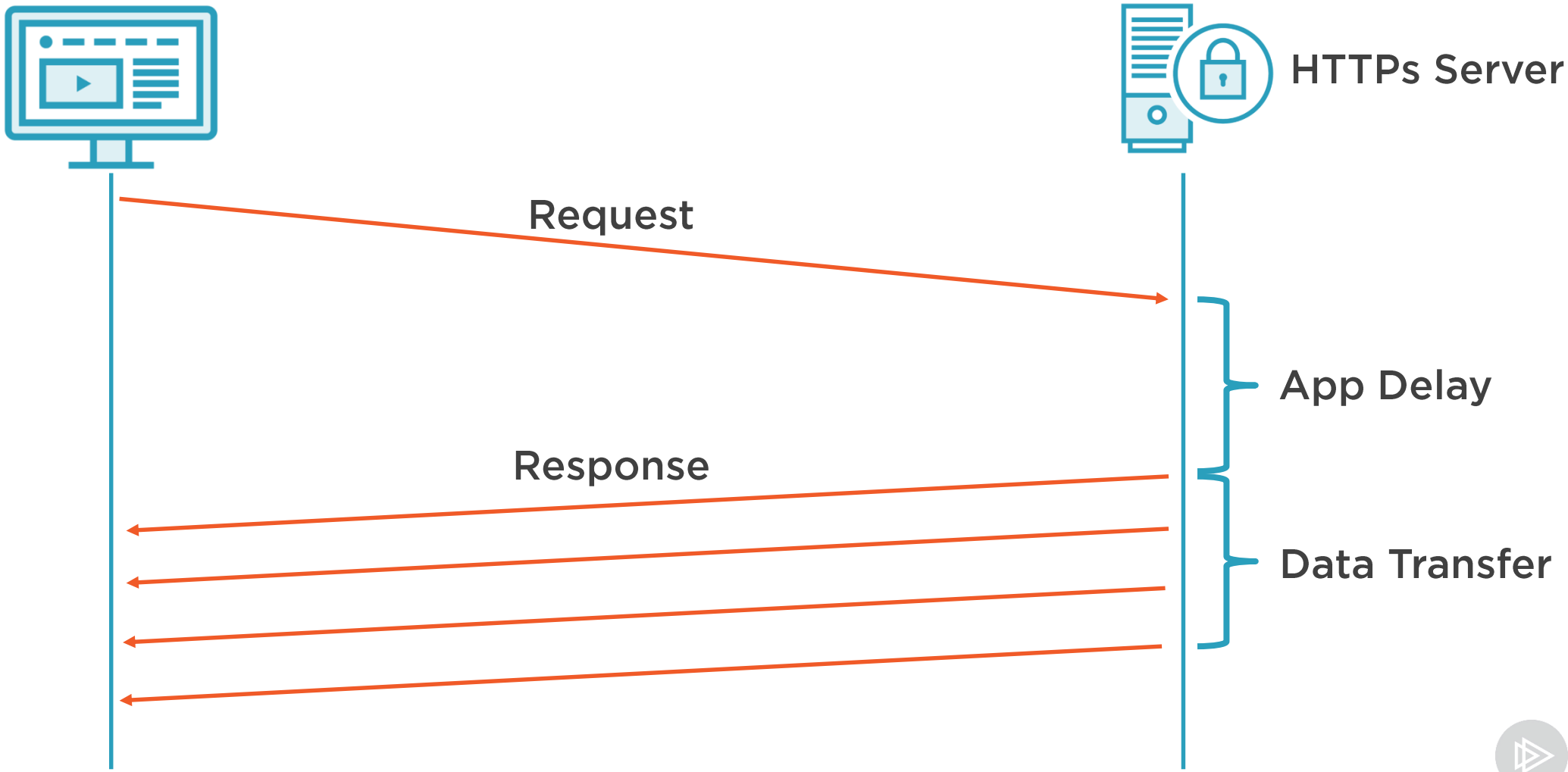
HTTP over TLS 1.3



HTTP over TLS 1.3



Do We Have to Decrypt?



Demo

Analyzing HTTPs over TLS

Review

FTP – Active vs. Passive

- File extraction and reassembly

Analyzing HTTPs

- Do we have to decrypt to troubleshoot?

Analyzing TLS