💻 Client | 🖥️ Server

📁 **ftps_act_get.pcapng**

🔗 TCP (SYN) — Frame 1 | 2019-04-02T15:35:58.971995Z

🔗 TCP (SYN, ACK) — Frame 2 | 2019-04-02T15:35:58.972886Z

🤝 FTP 220 Ready — 💡 Server is ready — announces software version and capabilities

🏷️ (vsFTPd 3.0.3)	

🤝 FTP FEAT — Frame 6 | 2019-04-02T15:35:58.999142Z

✅ FTP 211 — Frame 8 | 2019-04-02T15:35:59.000195Z

📋 Features:	
📂 CWD	

🔒 FTP AUTH — 💡 Upgrade to TLS/SSL encryption — all subsequent commands and data are protected

🔐 Method	TLS

🔒 FTP 234 AUTH OK — Frame 24 | 2019-04-02T15:35:59.003225Z

📋 Proceed with negotiation.	

🤝 TLS Client Hello — 💡 TLS handshake: client and server negotiate version and cipher suite

Version	TLS 1.2 (0x0303)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384 (0xc087)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc073)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256 (0xc086)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc072)
Cipher Suite	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)...
	43 more

🤝 TLS Server Hello — 💡 TLS handshake: client and server negotiate version and cipher suite

Version	TLS 1.2 (0x0303)
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

🔐 TLS Certificate — Frame 27 | 2019-04-02T15:35:59.04278Z

🔐 TLS New Session Ticket — Frame 28 | 2019-04-02T15:35:59.043986Z

🔒 TLS Application Data — 💡 Encrypted FTP commands and data — contents not visible without TLS keys

🔒 TLS Application Data — 💡 Encrypted FTP commands and data — contents not visible without TLS keys

🔒 TLS Application Data — 💡 Encrypted FTP commands and data — contents not visible without TLS keys

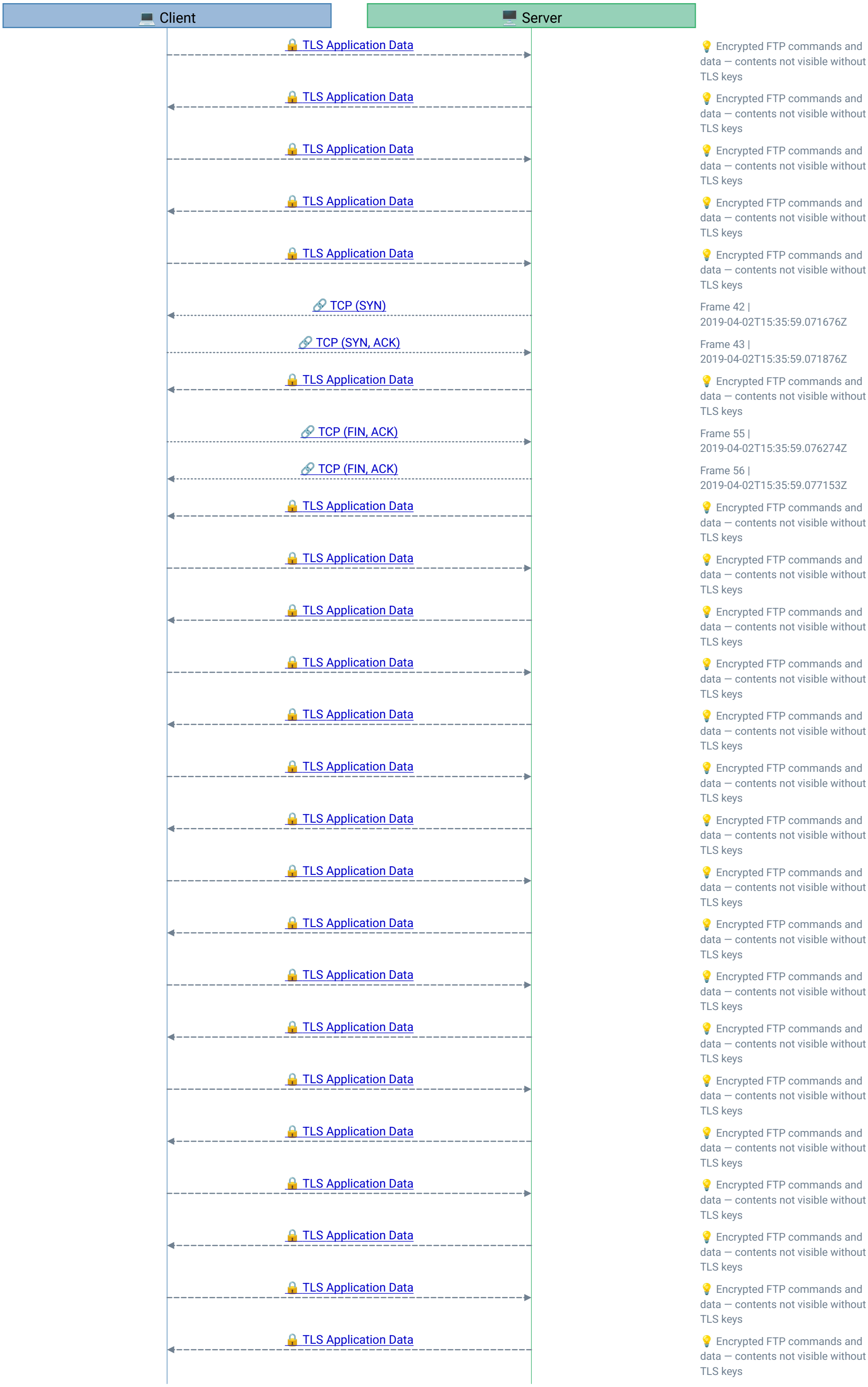
🔒 TLS Application Data — 💡 Encrypted FTP commands and data — contents not visible without TLS keys

🔒 TLS Application Data — 💡 Encrypted FTP commands and data — contents not visible without TLS keys

🔒 TLS Application Data — 💡 Encrypted FTP commands and data — contents not visible without TLS keys

🔒 TLS Application Data — 💡 Encrypted FTP commands and data — contents not visible without TLS keys

🔒 TLS Application Data — 💡 Encrypted FTP commands and data — contents not visible without TLS keys


Client
Server
TLS Application Data
Encrypted FTP commands and data — contents not visible without TLS keys
TCP (SYN)
Frame 42 | 2019-04-02T15:35:59.071676Z
TCP (SYN, ACK)
Frame 43 | 2019-04-02T15:35:59.071876Z
TCP (FIN, ACK)
Frame 55 | 2019-04-02T15:35:59.076274Z
Frame 56 | 2019-04-02T15:35:59.077153Z

Client
Server
TLS Application Data
Encrypted FTP commands and data — contents not visible without TLS keys
Frame 77 | 2019-04-02T15:35:59.096745Z
TCP (SYN)
Frame 78 | 2019-04-02T15:35:59.097196Z
TCP (SYN, ACK)
TLS Application Data
Encrypted FTP commands and data — contents not visible without TLS keys
Frame 90 | 2019-04-02T15:35:59.101516Z
TCP (FIN, ACK)
Frame 91 | 2019-04-02T15:35:59.102275Z
TCP (FIN, ACK)
TLS Application Data
Encrypted FTP commands and data — contents not visible without TLS keys
TLS Application Data
Encrypted FTP commands and data — contents not visible without TLS keys
TLS Application Data
Encrypted FTP commands and data — contents not visible without TLS keys
Frame 97 | 2019-04-02T15:35:59.105666Z
TCP (FIN, ACK)
Frame 99 | 2019-04-02T15:35:59.106063Z
TCP (FIN, ACK)
Frame 100 | 2019-04-02T15:35:59.106797Z
TCP (RST)
Frame 101 | 2019-04-02T15:35:59.106929Z
TCP (RST)