💻 Client | 🖥️ MQTT Broker

📁 **mqtt_tls_ws.pcapng**

🔗 TCP (SYN) →

Frame 1 | 2020-11-29T15:15:50.543899Z

← 🔗 TCP (SYN, ACK)

Frame 2 | 2020-11-29T15:15:50.634705Z

🤝 TLS Client Hello →

💡 TLS Client Hello for MQTT over TLS (port 8883) — SNI identifies the MQTT broker; secures IoT telemetry data in transit

🔐 Cipher	TLS_AES_128_GCM_SHA256 (0x1301)
🔐 Cipher	TLS_AES_256_GCM_SHA384 (0x1302)
🔐 Cipher	TLS_CHACHA20_POLY1305_SHA256 (0x1303)
🔐 Cipher	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
🔐 Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
🔐 Cipher	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
🔐 Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
🔐 Cipher	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
🔐 Cipher	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
🔐 Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
🔐 Cipher	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
🔐 Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
🔐 Cipher	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
🔐 Cipher	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
🔐 Cipher	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)...
	4 more

← 🤝 TLS Server Hello

Frame 7 | 2020-11-29T15:15:50.740692Z

🔐 Cipher	TLS_AES_256_GCM_SHA384 (0x1302)

🔒 TLS Change Cipher Spec →

Frame 12 | 2020-11-29T15:15:50.744821Z

← 🔗 TCP (FIN, ACK)

Frame 91 | 2020-11-29T15:15:59.451942Z

🔗 TCP (FIN, ACK) →

Frame 93 | 2020-11-29T15:15:59.452119Z