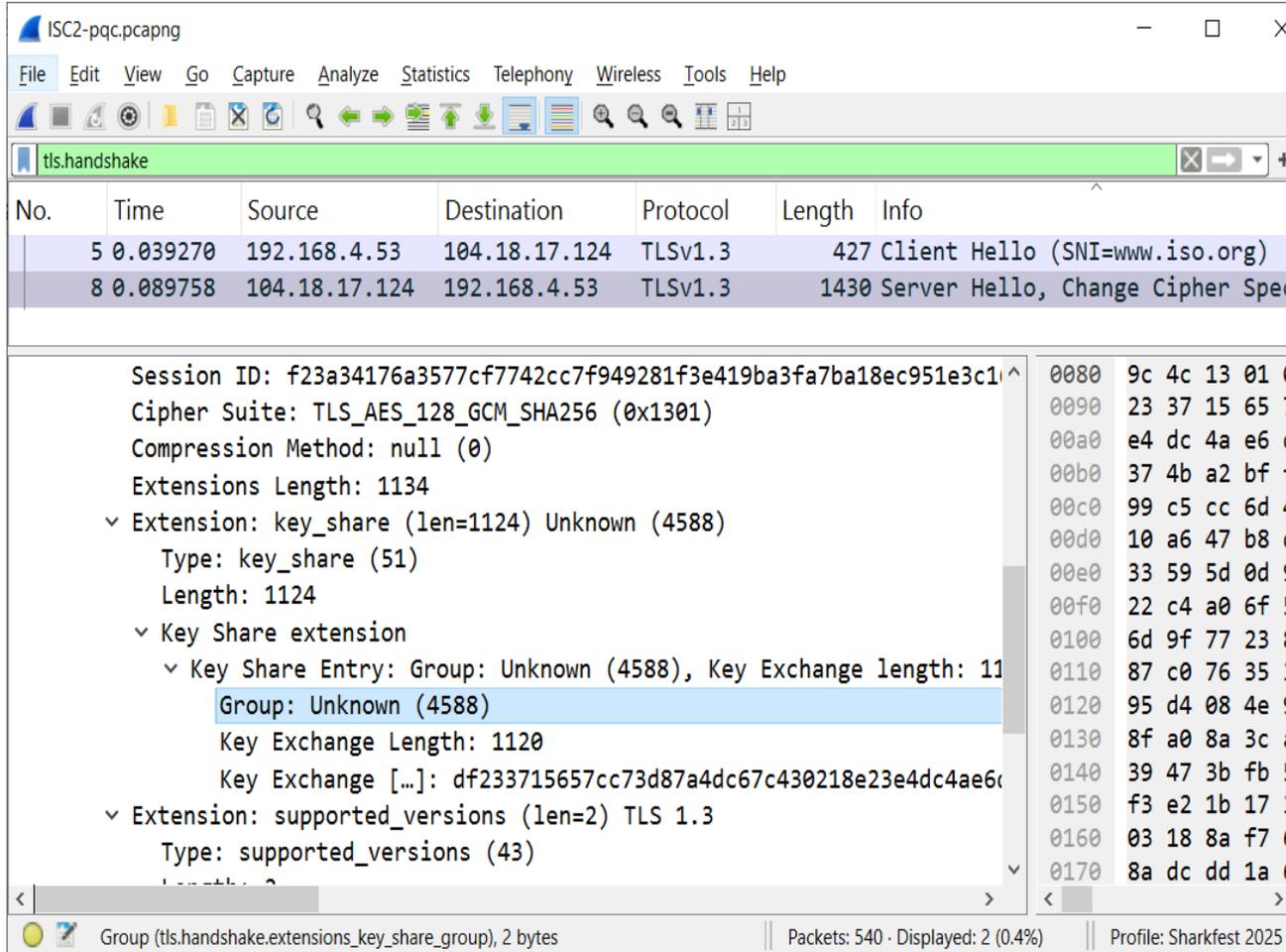


Are You Ready for Post Quantum Encryption?

Larry Greenblatt
hlgreenblatt@internetworkdefense.com

#sf25us

Let me introduce myself



ISIC2-pqc.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls.handshake

No.	Time	Source	Destination	Protocol	Length	Info
5	0.039270	192.168.4.53	104.18.17.124	TLSv1.3	427	Client Hello (SNI=www.iso.org)
8	0.089758	104.18.17.124	192.168.4.53	TLSv1.3	1430	Server Hello, Change Cipher Spe

Session ID: f23a34176a3577cf7742cc7f949281f3e419ba3fa7ba18ec951e3c1
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Compression Method: null (0)
Extensions Length: 1134

- Extension: key_share (len=1124) Unknown (4588)
 - Type: key_share (51)
Length: 1124
 - Key Share extension
 - Key Share Entry: Group: Unknown (4588), Key Exchange length: 1120
 - Group: Unknown (4588)
 - Key Exchange Length: 1120
 - Key Exchange [...]: df233715657cc73d87a4dc67c430218e23e4dc4ae6c
- Extension: supported_versions (len=2) TLS 1.3
 - Type: supported_versions (43)

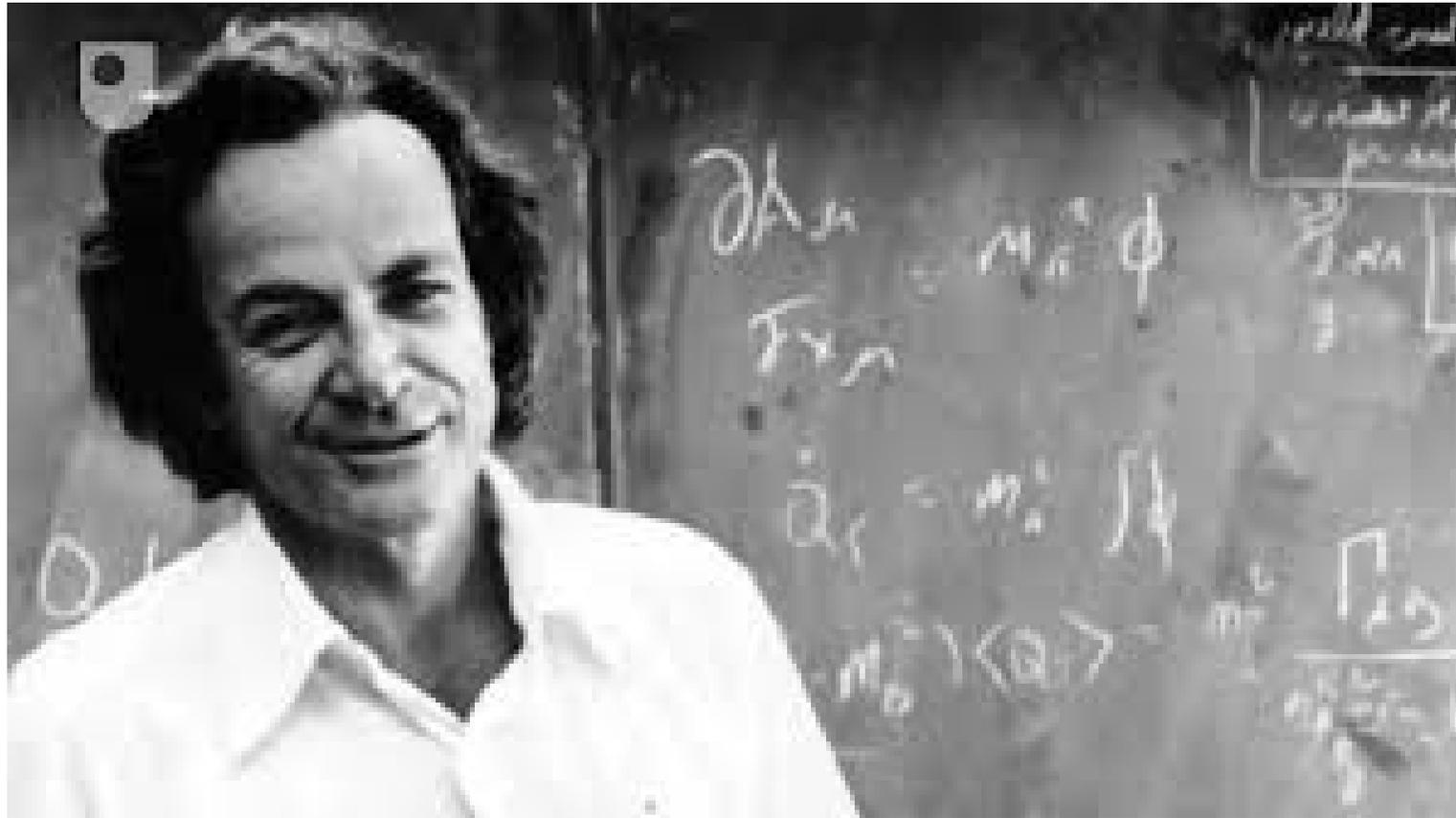
Group (tls.handshake.extensions_key_share_group), 2 bytes | Packets: 540 · Displayed: 2 (0.4%) | Profile: Sharkfest 2025

- Founder InterNetwork Defense (2001)
- Star Trek Nerd/Geek
- Cybersecurity instructor, martial artist, musician.
- 40+ years of infosec. Deep roots in cryptography, PKI, and protocol analysis
- Showing how post-quantum crypto is landing in TLS 1.3

Client Hello

Server Hello (got my 1st!)

**"If you think you understand quantum mechanics,
you don't understand quantum mechanics"**



- **No, Quantum Computing is Not Likely to Break the Internet.**

Even IF Quantum Computing Becomes Reality, We Have Fixes

- **The Push for Post Quantum Cryptography Compliance**

NIST (PQC)

FIPS

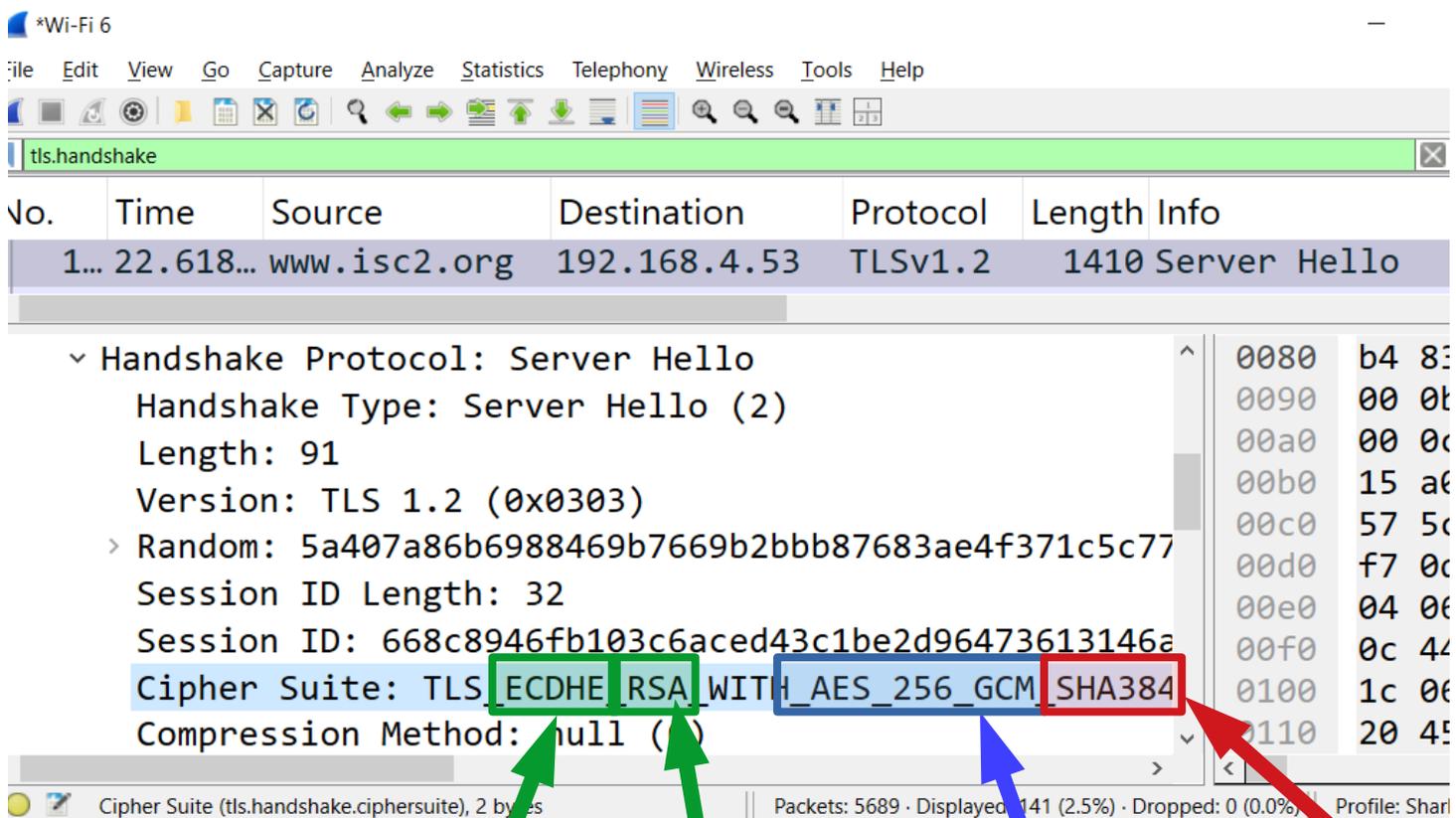
- **Personally, I am not Worried:**

Ray Kurzweil

Sabine Hossenfelder







Asymmetric 1
Key Encryption
"Who Can Decrypt"

Asymmetric 2
Signing the Hash
"Who Sent Message"

Symmetric Encryption
"Data Confidentiality"

Hashing
"Data Integrity"

A "Cipher Suite"

Asymmetric (Private/Public) Key Pairs:

1) Key Encapsulation

Encrypt (exchange/share/agree) the **DEK** (Data Encryption Key)
AES_256_GCM key

2) Digitally Sign

Authenticate the **SHA384** Hash

AES 256 GCM
to encrypt all data

SHA384
to ensure integrity

- **The 1st Step in any SDLC is “Who”**

Get this wrong and no other security matters (~_^)

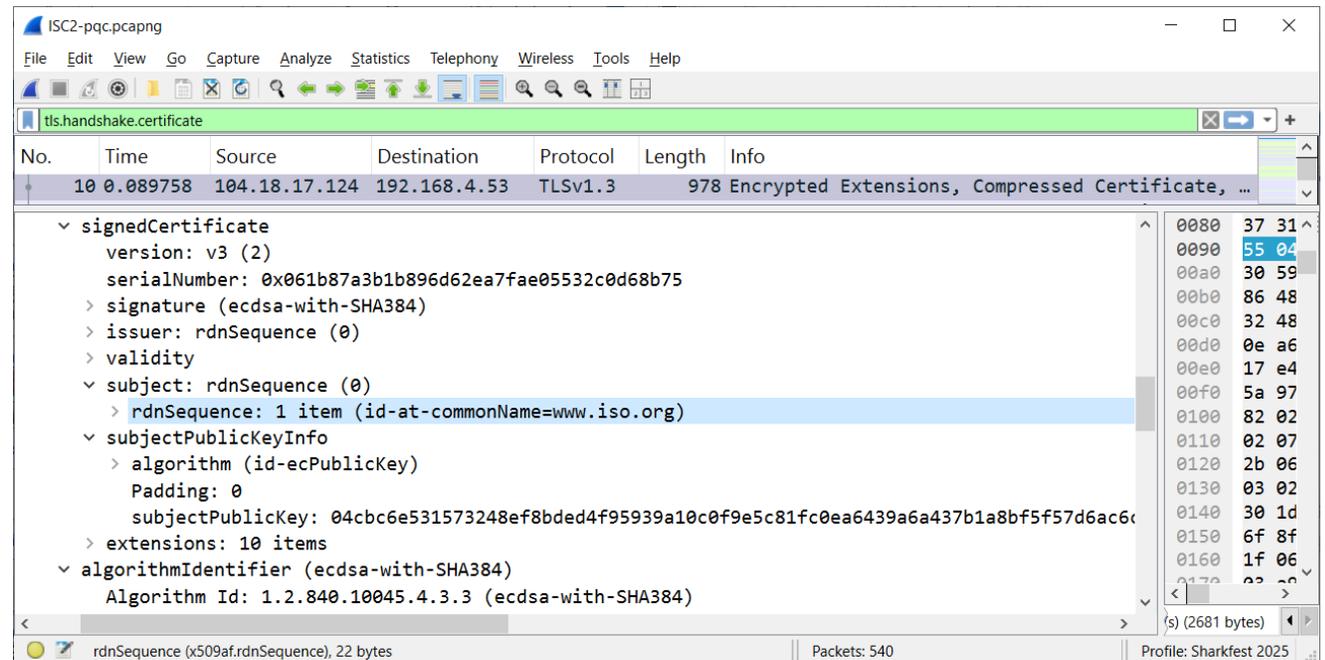
Public Key Infrastructures

- **Validating X.500 names with X.509 Certificates**

Servers

Clients

APIs (includes AI Agents)



• Quantum Computing and Encryption

Asymmetric Algorithms (Private / Public)

One Way Algorithms & Entropy (as compared to Symmetric)

Diffie-Hellman , RSA, ECC

Shor's Algorithm (With Enough* Q-Bits, Can Break RSA in a single operation (hours?))

Grover's Algorithm (Entropy reduced in half; 128 becomes 64)

AES (Recommended to use 256)

SHA Families (Recommended to use 512)

- **Post-Quantum Cryptography PQC**

- **To address Key Agreement**

- CRYSTALS-KYBER (2022)

- FIPS 203***

- HQC (2025)

- **For Signing**

- CRYSTALS-DILITHIUM (2022)

- FIPS 204***

- FALCON (2022)

- SPHINCS+ (2022)

- FIPS 205***



- **FIPS 203, 204 & 205**

- To address Key Agreement

FIPS 203 ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism Standard)

- For Signing

FIPS 204 ML-DSA (Module-Lattice-Based Digital Signature Standard)

FIPS 205 SLH-DSA (Stateless Hash-Based Digital Signature Standard)



Understanding a Cipher Suite (TLS 1.3)

Apply a display filter ... <Ctrl-/>

Time	Source	Destination	Protocol	Length	Info
8 0.089758	104.18.17.124	192.168.4.53	TLSv1.3	1430	Server Hello, Change

▼ Handshake Protocol: Server Hello

- Handshake Type: Server Hello (2)
- Length: 1206
- > Version: TLS 1.2 (0x0303)
- Random: aaa8720935b25cbe71205552647d9aeb7f9f2ca65f84bee1436c0163a3dcb21f...
- Session ID Length: 32
- Session ID: f23a34176a3577cf...7f949281f3e419ba3fa7ba18ec951e3c168da29...
- Cipher Suite: TLS **AES_128_GCM** **SHA256** (0x1301)
- Compression Method: null (0)
- Extensions Length: 1134
- ▼ Extension: key_share (len=1124) Unknown (4588)
- Type: key_share (51)
- Length: 1124
- ▼ Key Share extension
- Key Share Entry: Group: Unknown (4588), Key Exchange length: 1120

A “Cipher Suite”

Symmetric Services

AES 128 GCM

Hashing Services

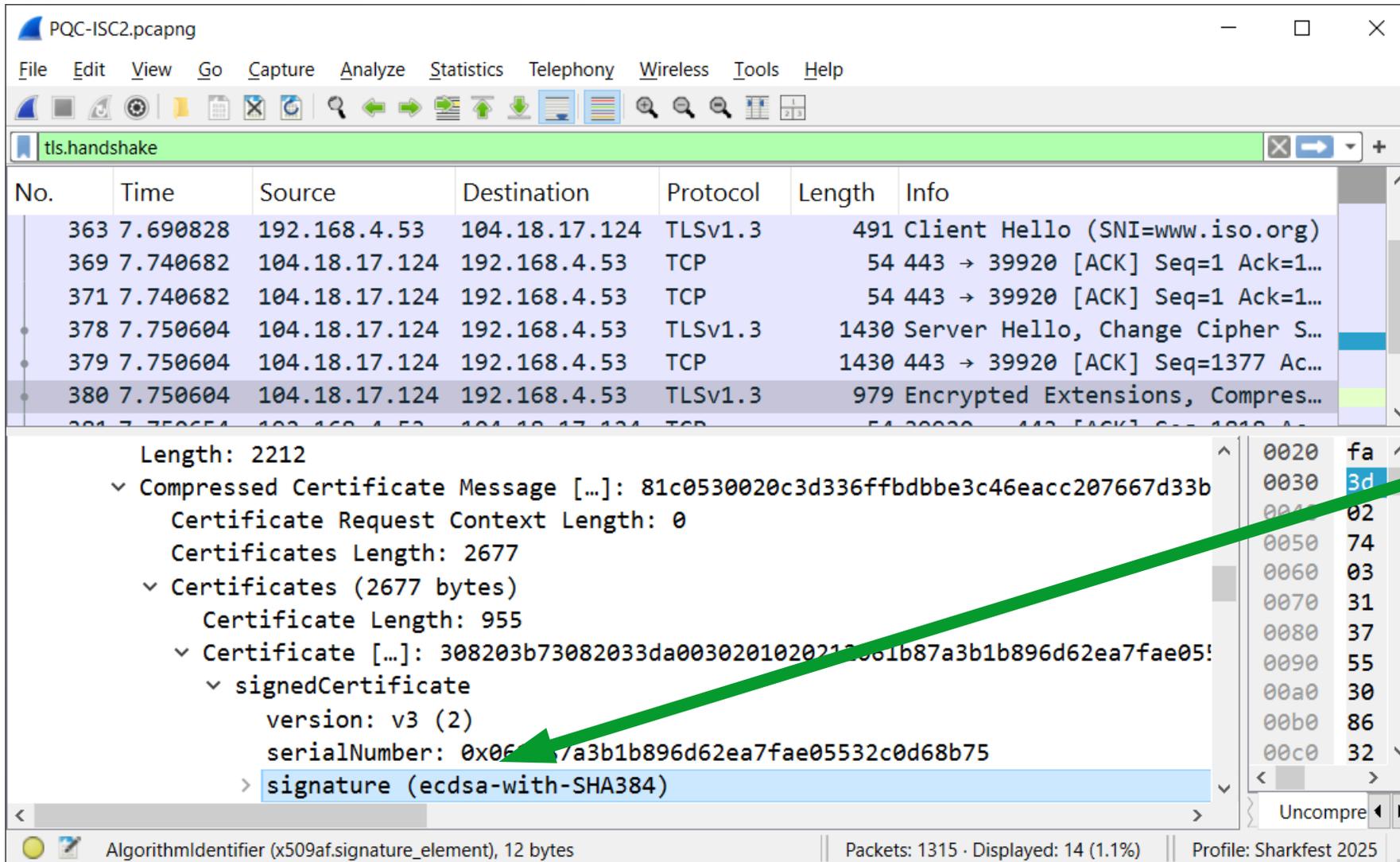
SHA256

Asymmetric Services:

(4588) ECDHE-MLKEM

Where’s the Signing Algorithm?

Understanding a Cipher Suite (TLS 1.3 Encrypted Extensions)



The image shows a Wireshark packet capture window titled "PQC-ISC2.pcapng" with a filter for "tls.handshake". The packet list shows a TLSv1.3 Client Hello (No. 363) and a corresponding Server Hello (No. 378). Packet No. 380 is selected, showing the "Encrypted Extensions" field. The details pane for this field is expanded to show a "signedCertificate" structure with the following fields:

- version: v3 (2)
- serialNumber: 0x06...7a3b1b896d62ea7fae05532c0d68b75
- signature (ecdsa-with-SHA384)

A green arrow points from the "signature" field in the details pane to the text on the right. The status bar at the bottom indicates "AlgorithmIdentifier (x509af.signature_element), 12 bytes" and "Profile: Sharkfest 2025".

**Asymmetric:
Signing Algorithm
ECDSA**

**No Support Yet for:
FIPS 204 (Dillithium)
FIPS 205 (SPHINCS)**

Comparing Cryptographic Strength "Entropy"

Symmetric	Asymmetric		
AES	DH / RSA	ECDHE ECDSA	<u>Kyber</u> <u>Dilithium</u>
128	3072	256	<u>768</u>

- Quantum Computing Risk vs Hype
- Effectuated Algorithms are our ID Keys (Private / Public Key Pairs)

DH

RSA

ECC

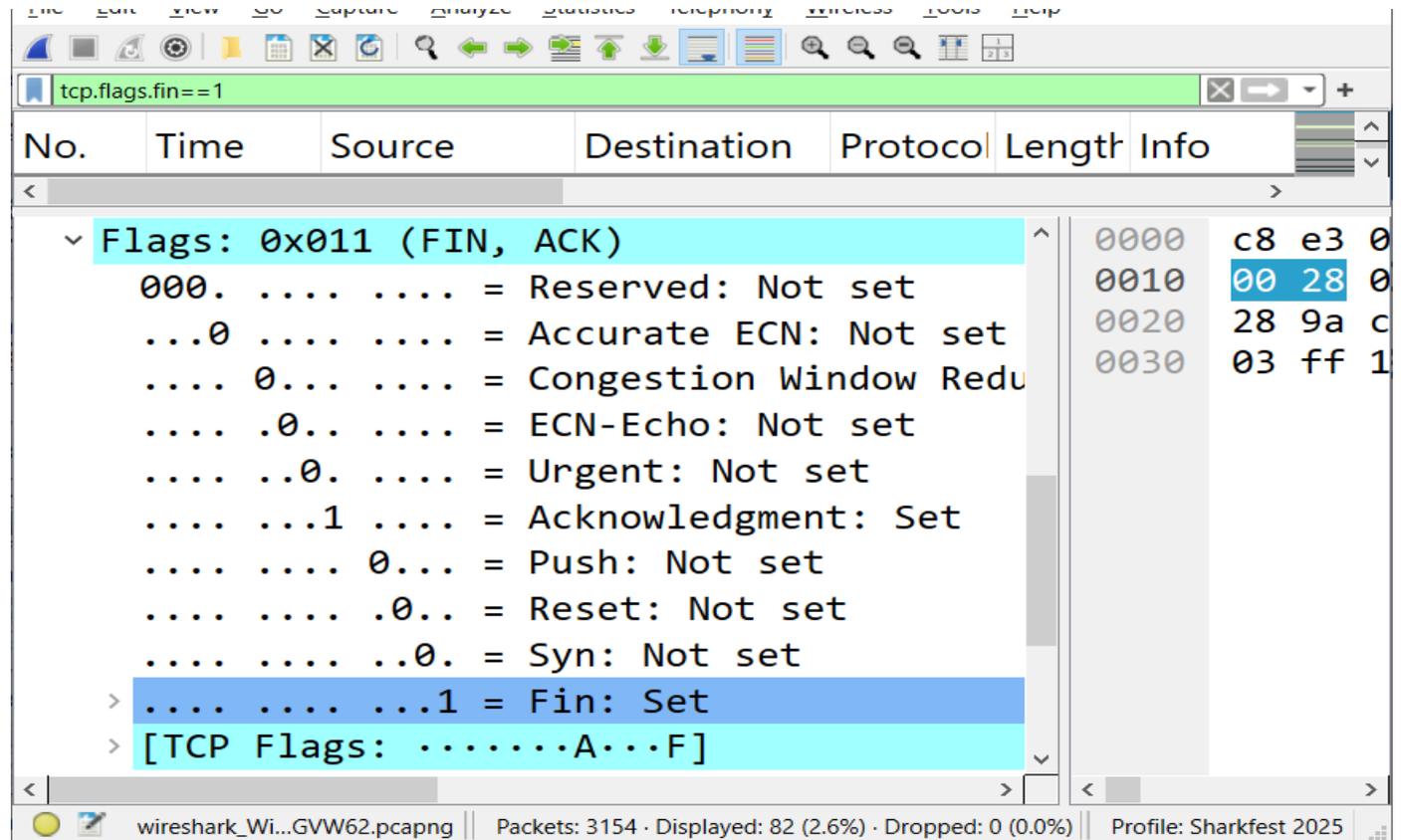
- FIPS 203, 204, 205

Kyber

Dillithium

SPHINCS

- Questions?



Feedback



#sf25us