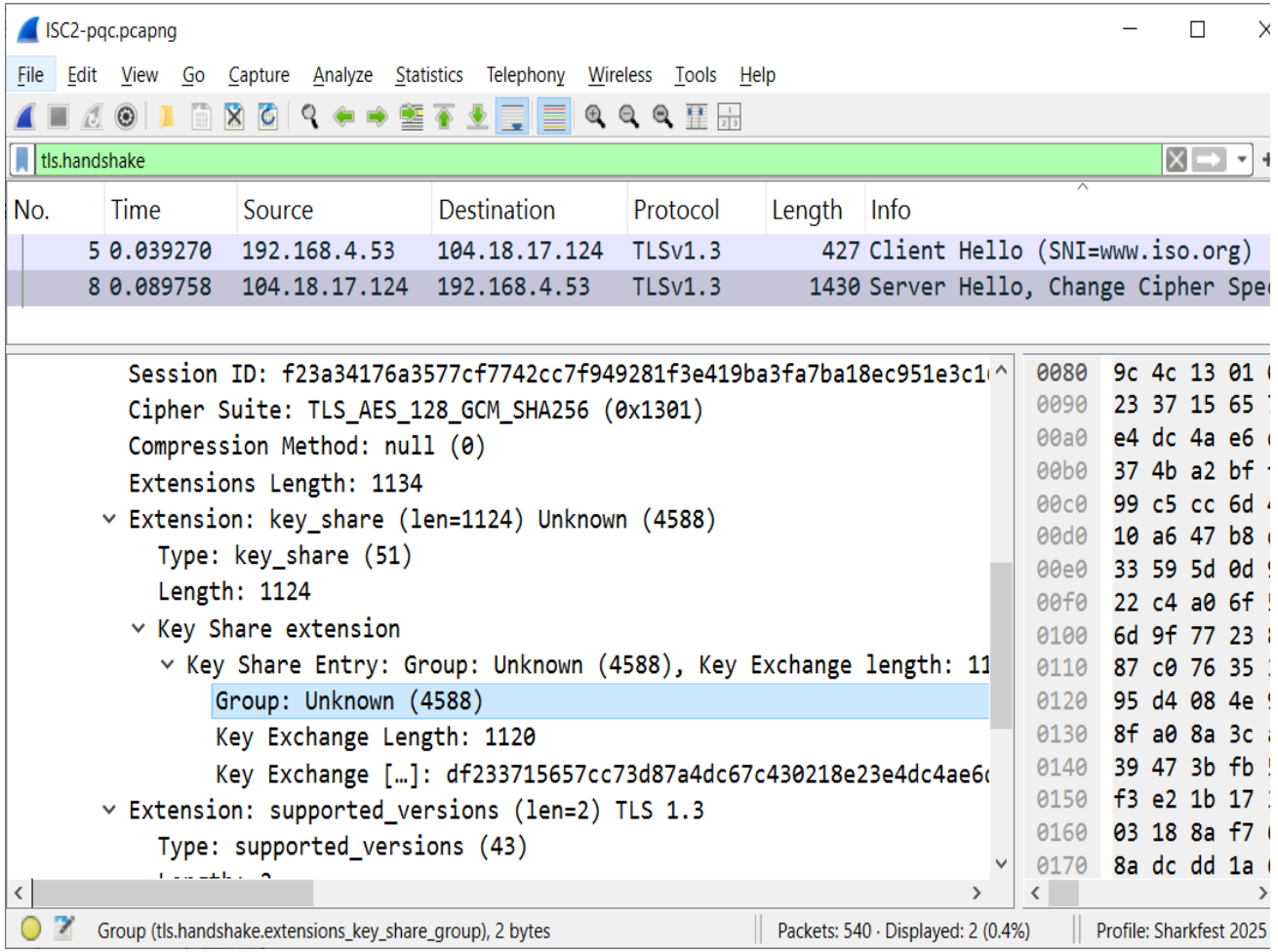
Are You Ready for Post Quantum Encryption?

Larry Greenblatt
hlgreenblatt@internetworkdefense.com

#sf25us

Let me introduce myself



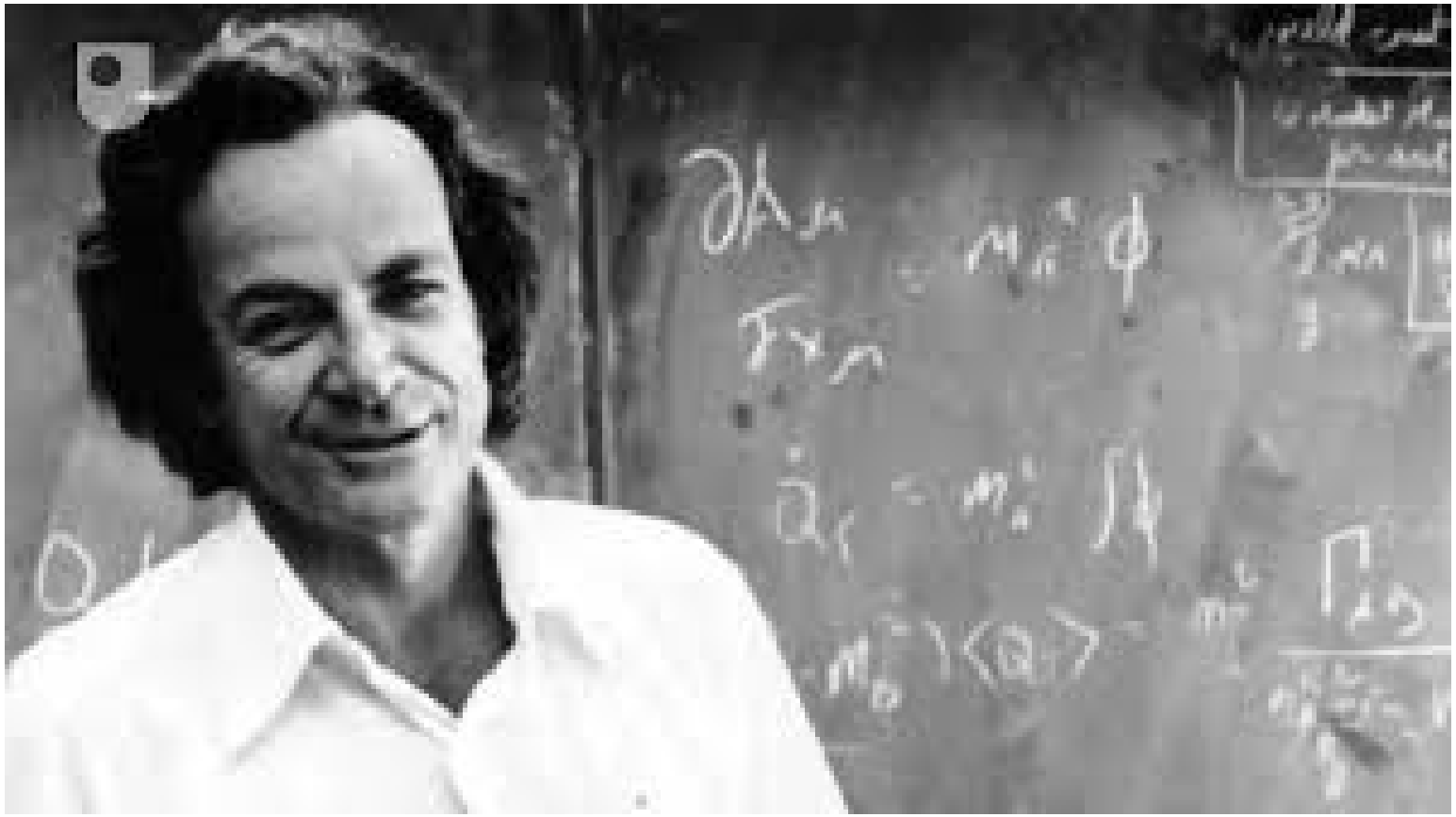
- Founder InterNetwork Defense (2001)
- Star Trek Nerd/Geek
- Cybersecurity instructor, martial artist, musician.
- 40+ years of infosec. Deep roots in cryptography, PKI, and protocol analysis
- Showing how post-quantum crypto is landing in TLS 1.3

  Client Hello

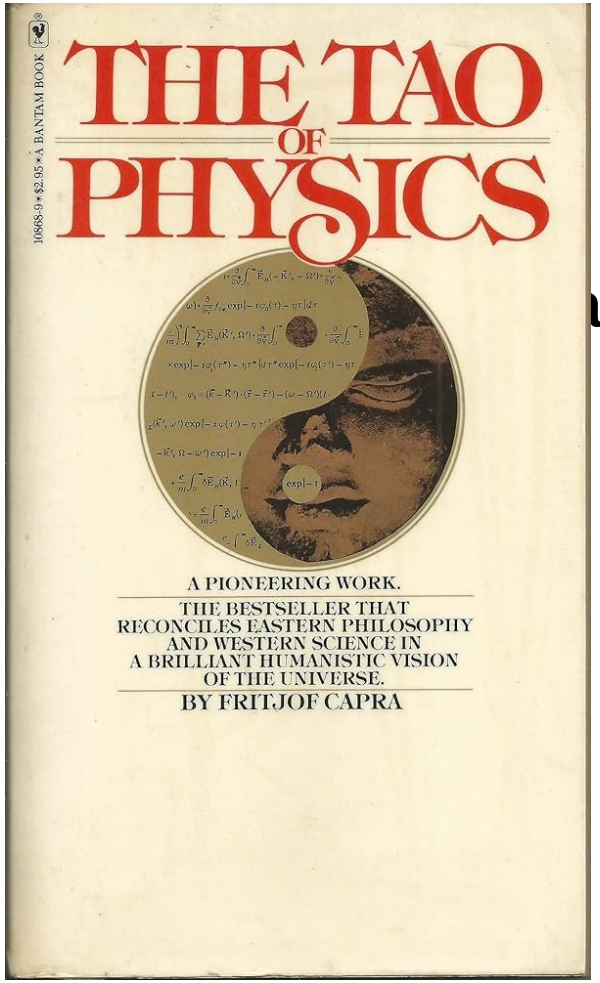
  Server Hello (got my 1st!)

What I Understand About Quantum Theory

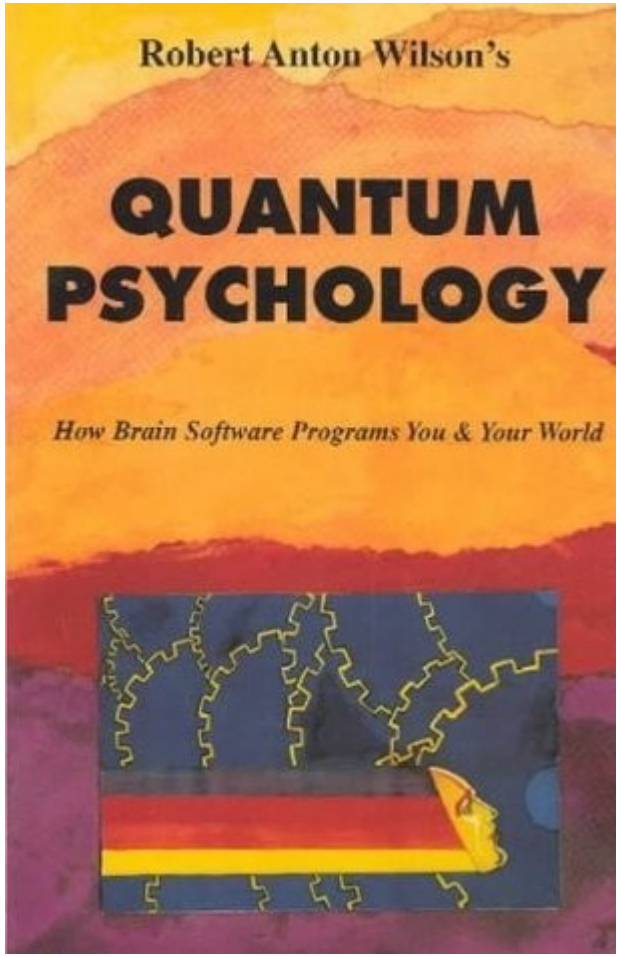
"If you think you understand quantum mechanics, you don't understand quantum mechanics"

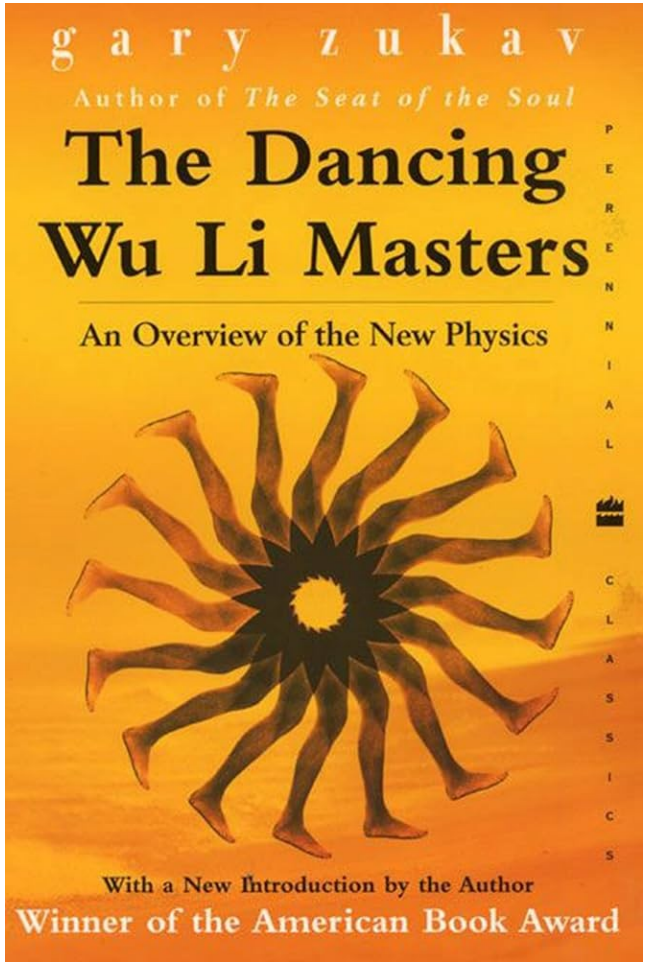


Still, as both a Trekkie and a Taiji Nerd…



…ated by





If a Woodchuck Could Chuck Wood

- **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

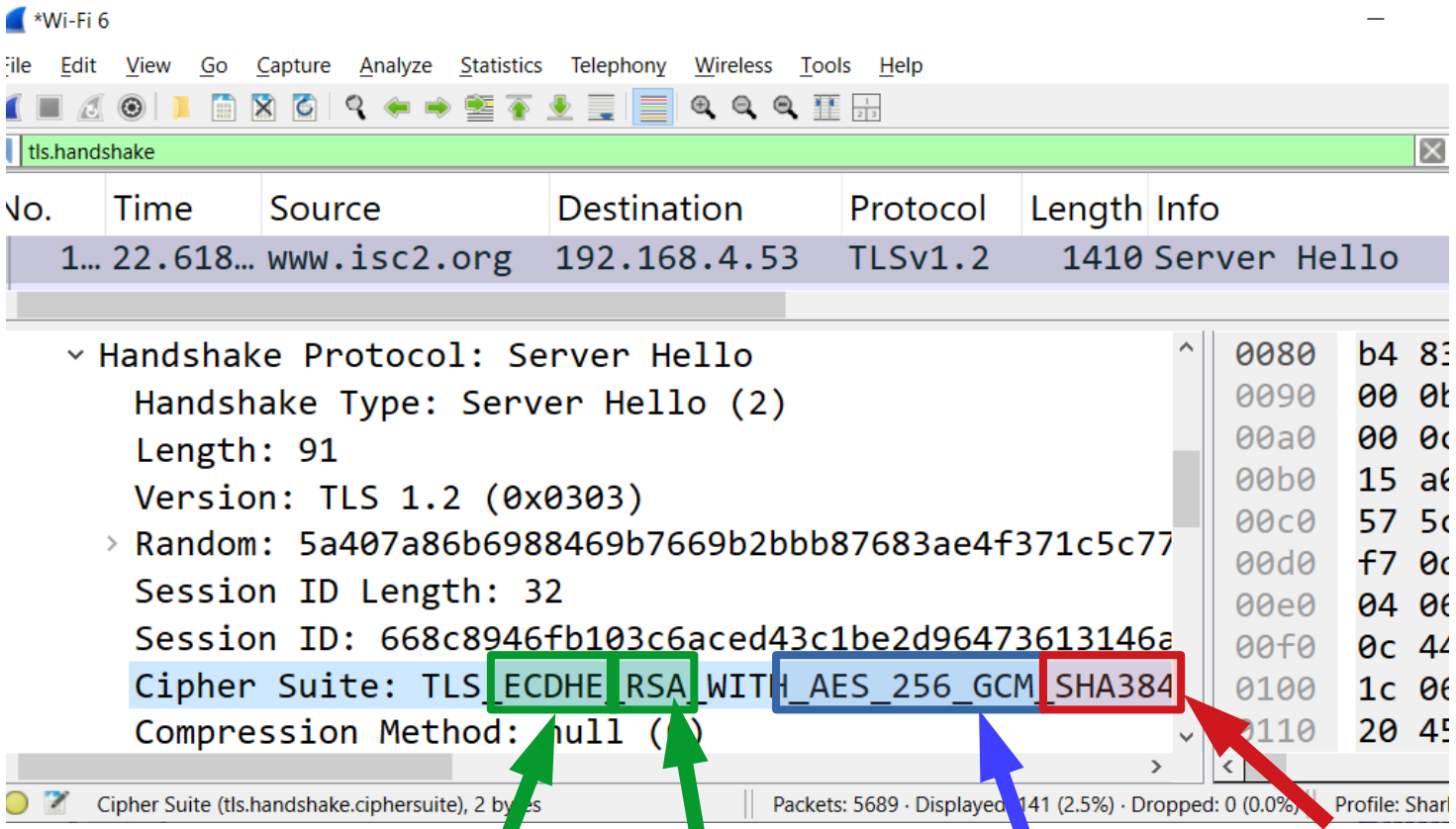
- **Personally, I am not Worried:**

  Ray Kurzweil

  Sabine Hossenfelder

And Even Perhaps...

Cryptography Review: Understanding a Cipher Suite (TLS 1.2)



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

Proof of ID: Asymmetric (Private/Public) the Digital Credentials

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

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

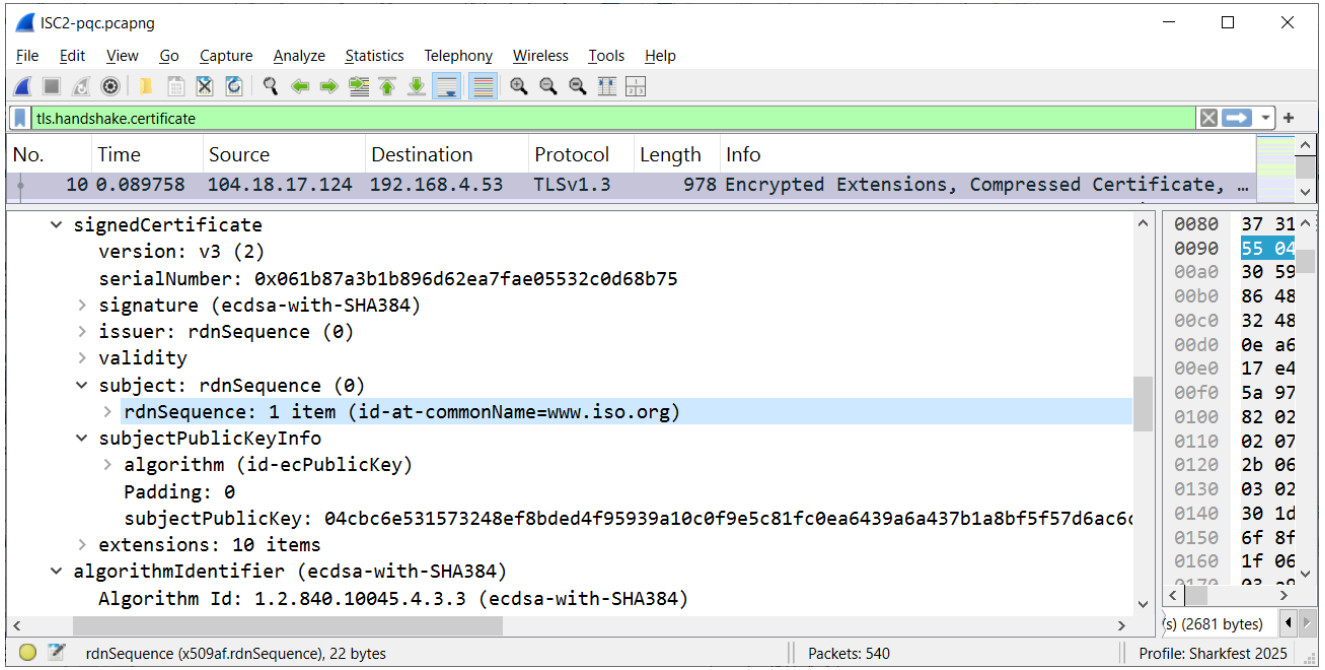
  Public Key Infrastructures

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

  Servers

  Clients

  APIs (includes AI Agents)



What is the Concern?

- **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***

Federal Information Processing Standards (FIPS)

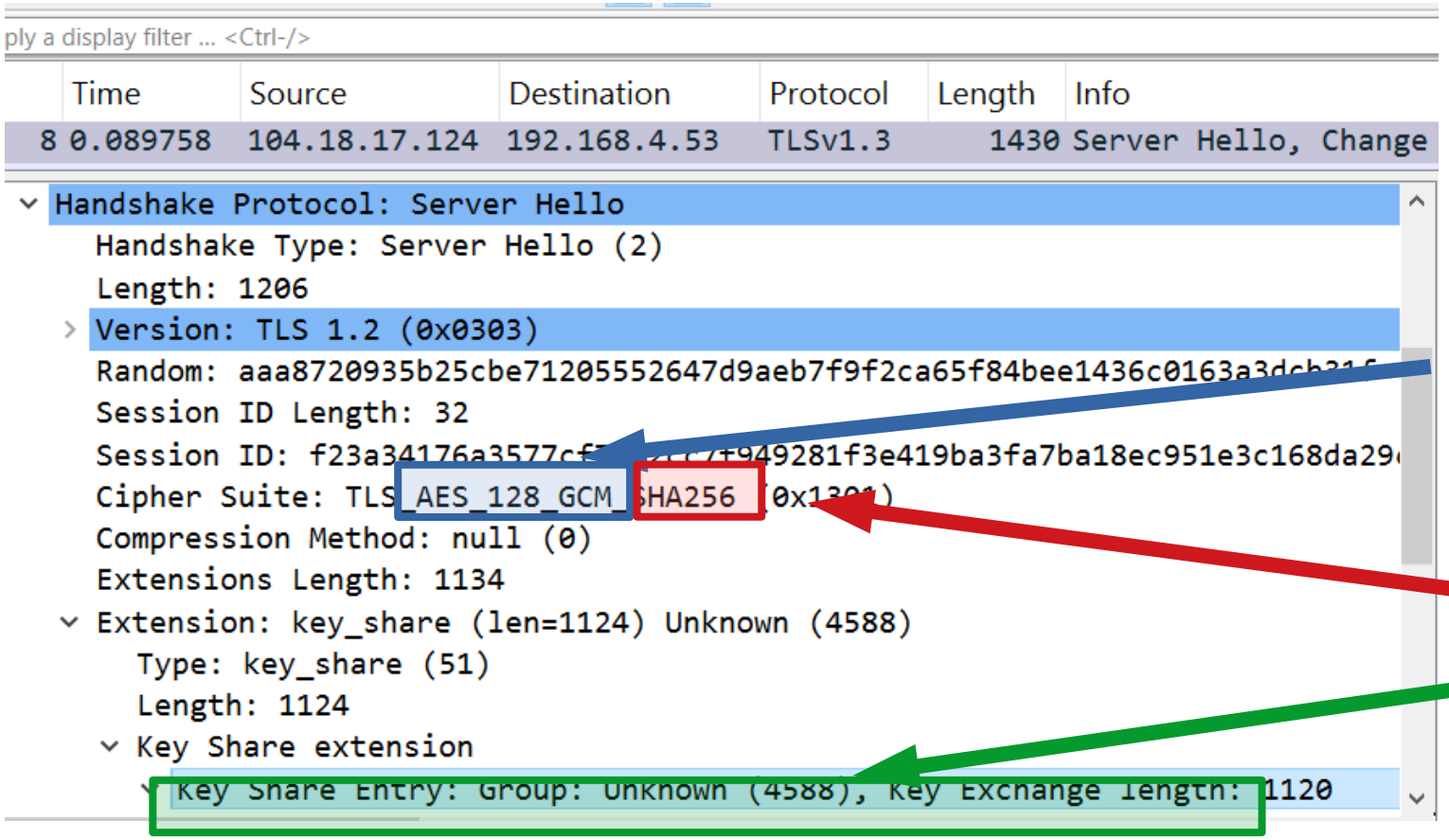
- **FIPS 203, 204 & 205**
  - To address Key Agreement

    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)



A "Cipher Suite"

Symmetric Services

AES_128_GCM

Hashing Services

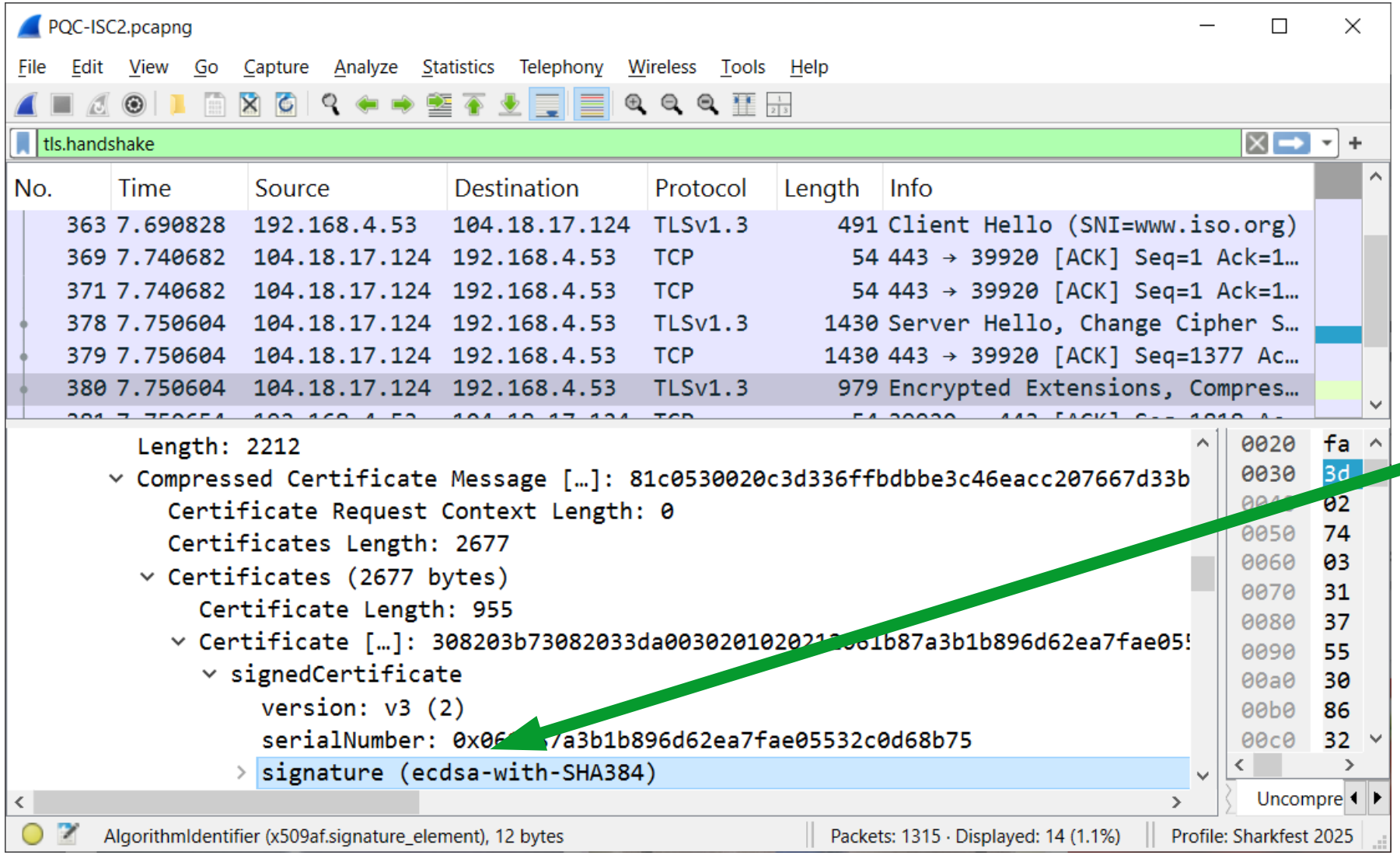
SHA256

Asymmetric Services:

(4588) ECDHE-MLKEM

Where's the Signing Algorithm?

Understanding a Cipher Suite (TLS 1.3 Encrypted Extensions)



Asymmetric:
Signing Algorithm
ECDSA

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

Comparing Cryptogrpahic Strength “Entropy”

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

Summary

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

DH

RSA

ECC

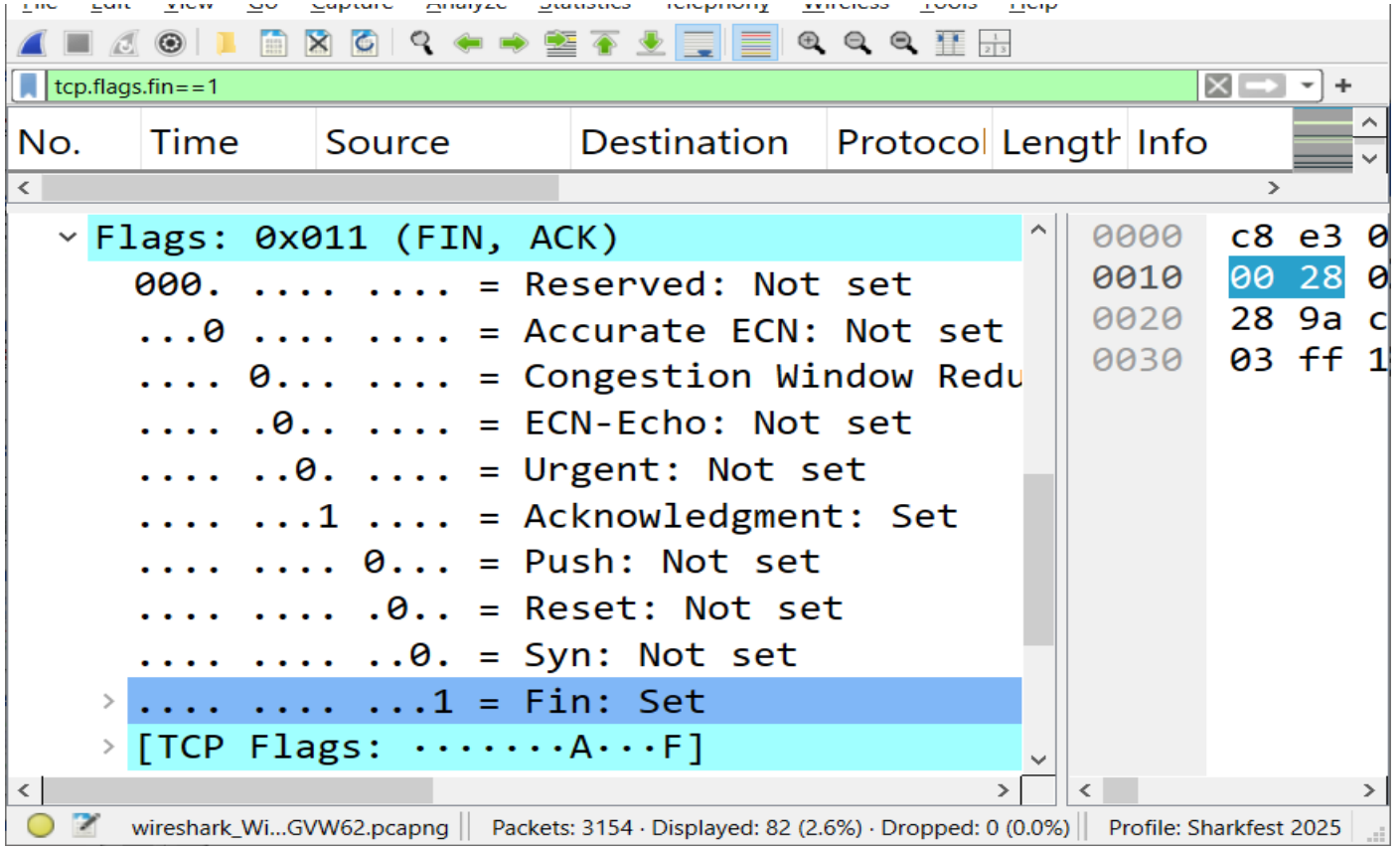
- FIPS 203, 204, 205

Kyber

Dillithium

SPHINCS

- Questions?



Feedback

#sf25us