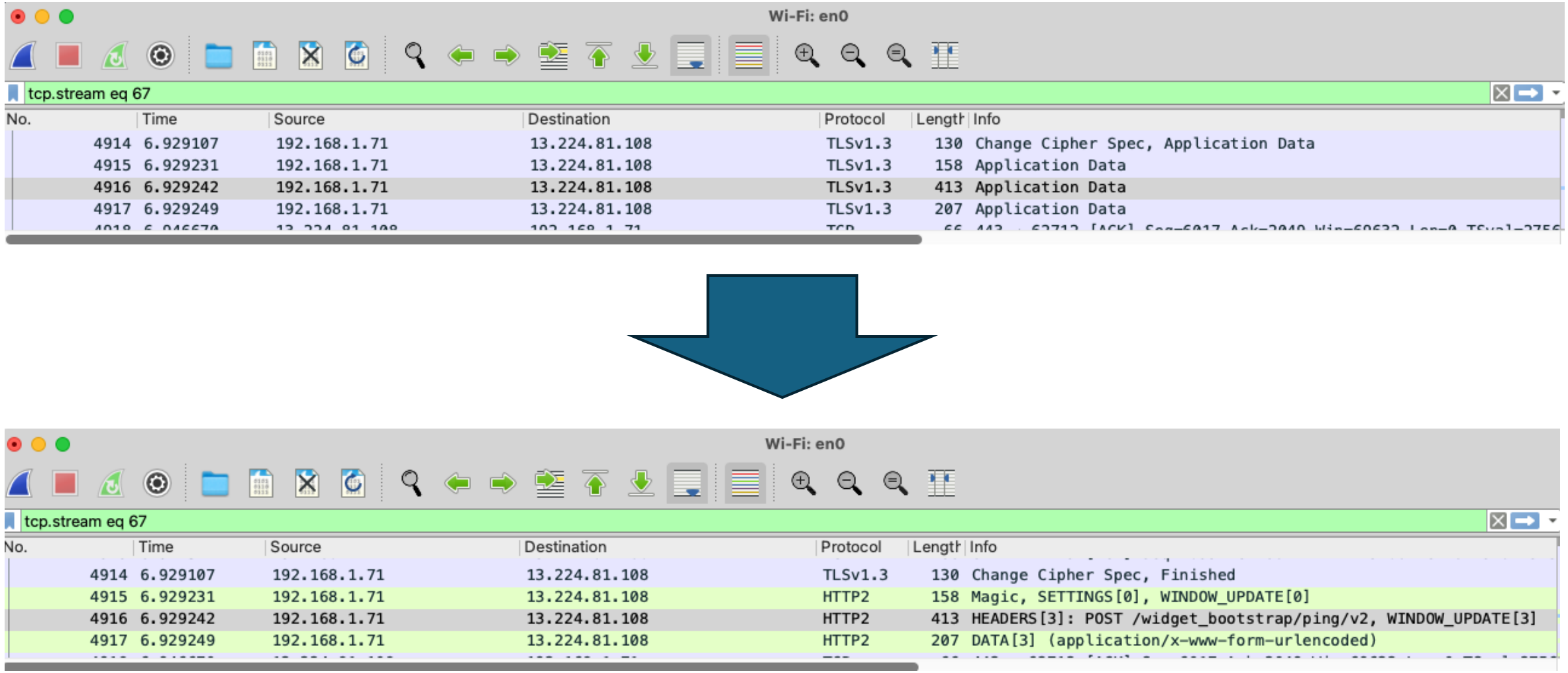
SSLKEYLOGFILE Extension for ECH

Yaroslav Rosomakho

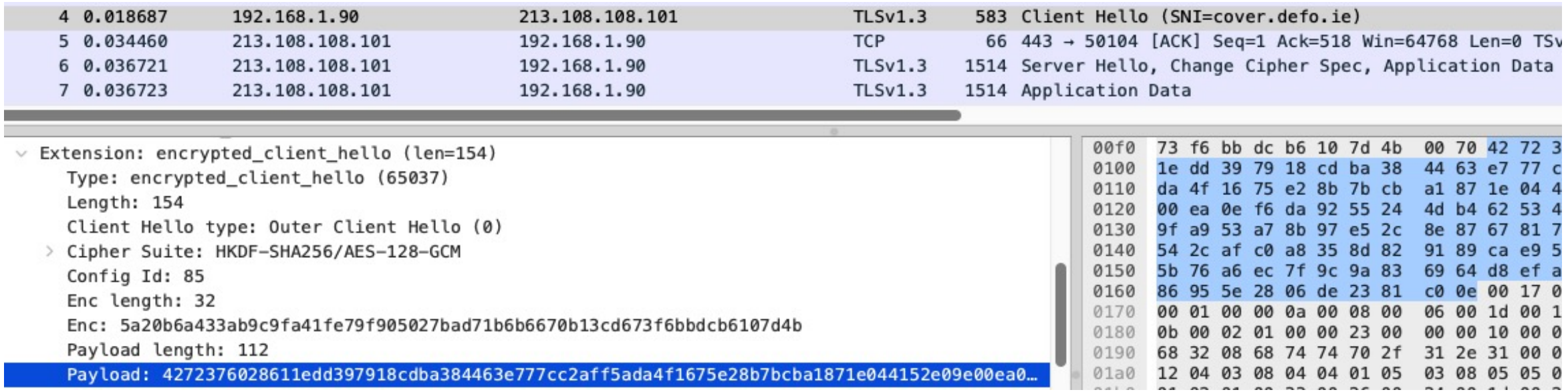
Hannes Tschofenig

SSLKEYLOG is a useful troubleshooting tool



Challenges of TLS troubleshooting with ECH

- Inspecting ECH
- Troubleshooting TLS handshake with ECH
- Decrypting TLS session when ECH is negotiated



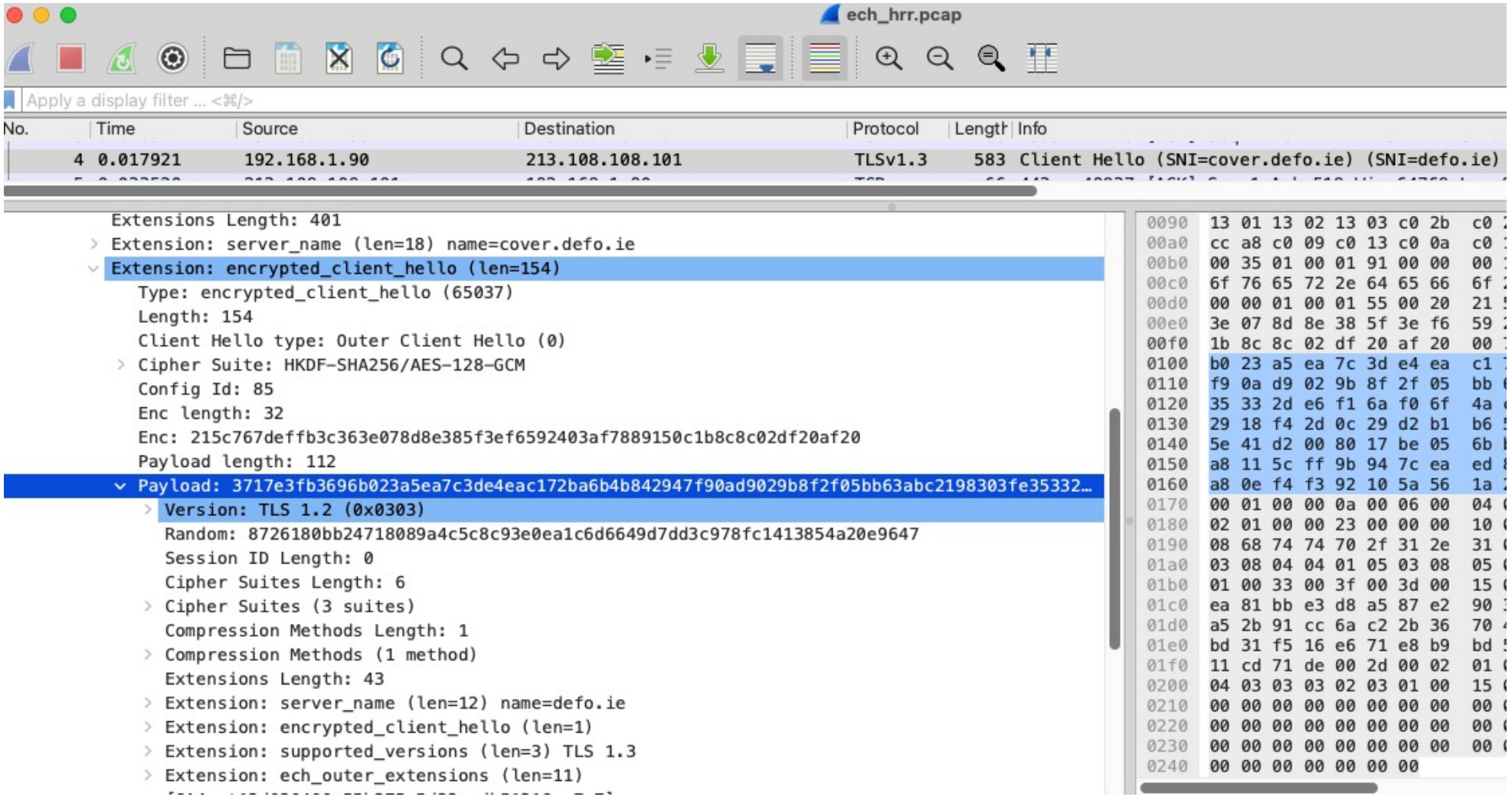
The proposed solution

- ECH_SECRET label to log HPKE shared_secret
- ECH_CONFIG label to log ECHConfig
- Outer ClientHello Random as keys for ECH_SECRET and ECH_CONFIG
- Inner ClientHello Random for the rest of the session as long as ECH was accepted

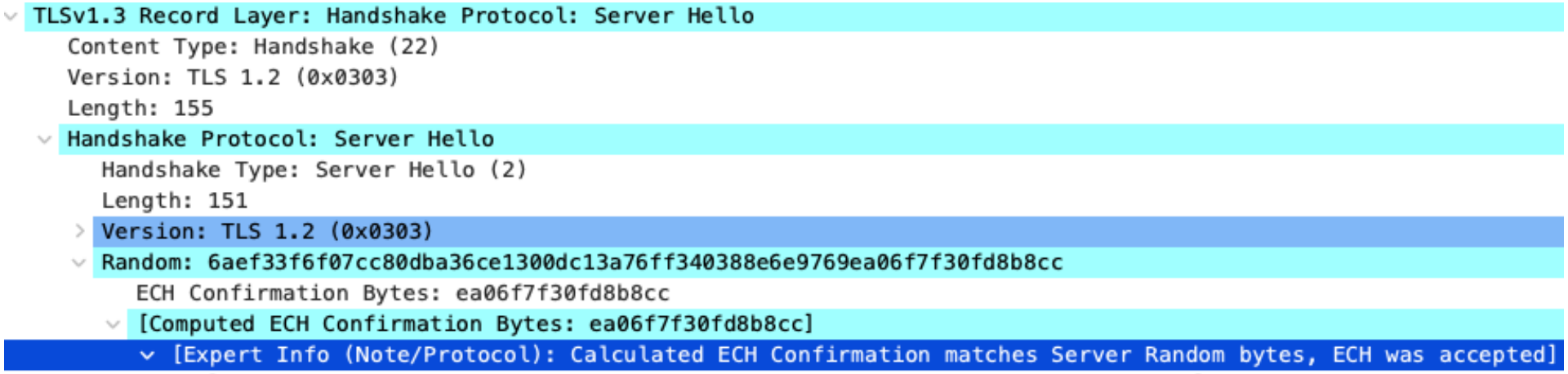
Prototype implementations

- NSS: https://github.com/yaroslavros/nss-echkeylog
  - Very straightforward as shared secret is a part of HPKE context
- BoringSSL: https://github.com/yaroslavros/boringssl-echkeylog
  - Required additional callback in HPKE key schedule process
- Wireshark: https://github.com/yaroslavros/wireshark-echkeylog

Visibility into ECH



Confirming server acceptance



Visibility into the rest of the session

4	0.017921	192.168.1.90	213.108.108.101	TLSv1.3	583	Client Hello (SNI=cover.defo.ie) (SNI=defo.ie)
5	0.033520	213.108.108.101	192.168.1.90	TCP	66	443 → 49837 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSv
6	0.033522	213.108.108.101	192.168.1.90	TLSv1.3	177	Hello Retry Request, Change Cipher Spec
7	0.033738	192.168.1.90	213.108.108.101	TCP	66	49837 → 443 [ACK] Seq=518 Ack=112 Win=131648 Len=0
8	0.034369	192.168.1.90	213.108.108.101	TLSv1.3	501	Change Cipher Spec, Client Hello (SNI=cover.defo.ie
9	0.050603	213.108.108.101	192.168.1.90	TCP	66	443 → 49837 [ACK] Seq=112 Ack=953 Win=64384 Len=0 T
10	0.052960	213.108.108.101	192.168.1.90	TLSv1.3	1514	Server Hello, Encrypted Extensions
11	0.052962	213.108.108.101	192.168.1.90	TLSv1.3	1514	Certificate
12	0.052963	213.108.108.101	192.168.1.90	TLSv1.3	353	Certificate Verify, Finished
13	0.053158	192.168.1.90	213.108.108.101	TCP	66	49837 → 443 [ACK] Seq=953 Ack=3295 Win=128448 Len=0
14	0.054652	192.168.1.90	213.108.108.101	TLSv1.3	124	Finished
15	0.069765	213.108.108.101	192.168.1.90	TCP	66	443 → 49837 [ACK] Seq=3295 Ack=1011 Win=64384 Len=0
16	0.069766	213.108.108.101	192.168.1.90	TLSv1.3	337	New Session Ticket
17	0.069767	213.108.108.101	192.168.1.90	TLSv1.3	337	New Session Ticket
18	0.069971	192.168.1.90	213.108.108.101	HTTP	121	GET / HTTP/1.1

Thank you!

- What do you think about the problem?
- What do you think about proposed solution?
- Should this work be adopted by the Working Group?