

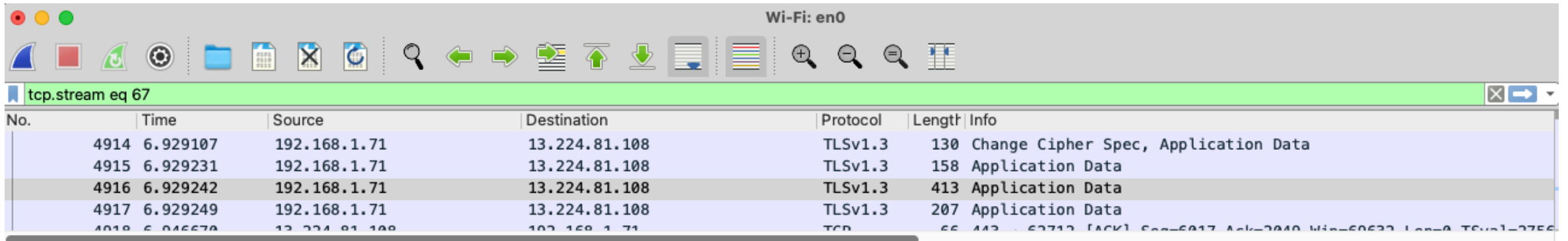
# SSLKEYLOGFILE

## Extension for ECH

Yaroslav Rosomakho

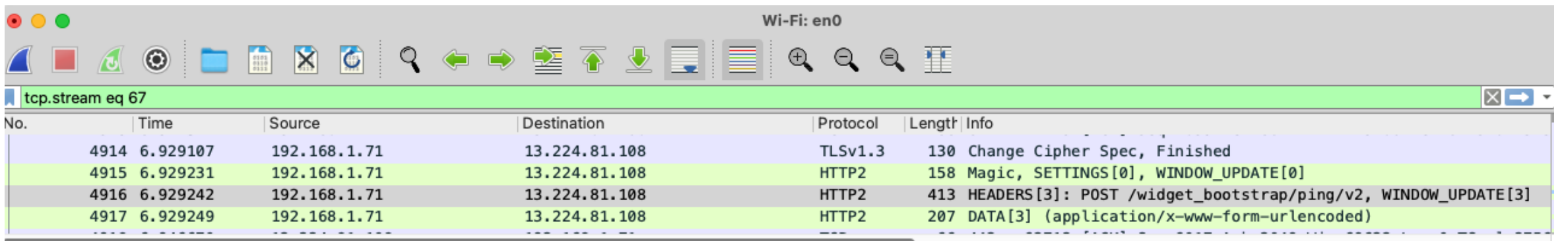
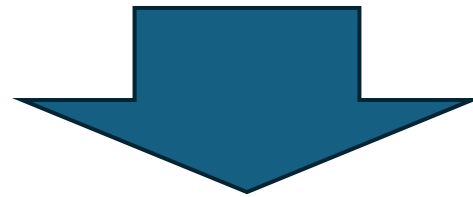
Hannes Tschofenig

# SSLKEYLOG is a useful troubleshooting tool



Wireshark capture showing traffic on interface Wi-Fi: en0. The selected packet is a TCP stream (eq 67) containing TLSv1.3 application data. The table below shows the details of the captured packets.

No.	Time	Source	Destination	Protocol	Length	Info
4914	6.929107	192.168.1.71	13.224.81.108	TLSv1.3	130	Change Cipher Spec, Application Data
4915	6.929231	192.168.1.71	13.224.81.108	TLSv1.3	158	Application Data
4916	6.929242	192.168.1.71	13.224.81.108	TLSv1.3	413	Application Data
4917	6.929249	192.168.1.71	13.224.81.108	TLSv1.3	207	Application Data
4918	6.946670	13.224.81.108	192.168.1.71	TCP	66	443 → 62712 [ACK] Seq=6017 Ack=2040 Win=60632 Len=0 TLSv1=2756



Wireshark capture showing traffic on interface Wi-Fi: en0. The selected packet is a TCP stream (eq 67) containing HTTP2 application data. The table below shows the details of the captured packets.

No.	Time	Source	Destination	Protocol	Length	Info
4914	6.929107	192.168.1.71	13.224.81.108	TLSv1.3	130	Change Cipher Spec, Finished
4915	6.929231	192.168.1.71	13.224.81.108	HTTP2	158	Magic, SETTINGS[0], WINDOW_UPDATE[0]
4916	6.929242	192.168.1.71	13.224.81.108	HTTP2	413	HEADERS[3]: POST /widget_bootstrap/ping/v2, WINDOW_UPDATE[3]
4917	6.929249	192.168.1.71	13.224.81.108	HTTP2	207	DATA[3] (application/x-www-form-urlencoded)

# Challenges of TLS troubleshooting with ECH

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

4	0.018687	192.168.1.90	213.108.108.101	TLSv1.3	583	Client Hello (SNI=cover.defo.ie)
5	0.034460	213.108.108.101	192.168.1.90	TCP	66 443 → 50104	[ACK] Seq=1 Ack=518 Win=64768 Len=0 TSv
6	0.036721	213.108.108.101	192.168.1.90	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
7	0.036723	213.108.108.101	192.168.1.90	TLSv1.3	1514	Application Data

▼ Extension: encrypted\_client\_hello (len=154)  
Type: encrypted\_client\_hello (65037)  
Length: 154  
Client Hello type: Outer Client Hello (0)  
> Cipher Suite: HKDF-SHA256/AES-128-GCM  
Config Id: 85  
Enc length: 32  
Enc: 5a20b6a433ab9c9fa41fe79f905027bad71b6b6670b13cd673f6bbdcb6107d4b  
Payload length: 112  
Payload: 4272376028611edd397918cdba384463e777cc2aff5ada4f1675e28b7bcba1871e044152e09e00ea0...

00f0	73	f6	bb	dc	b6	10	7d	4b	00	70	42	72	3
0100	1e	dd	39	79	18	cd	ba	38	44	63	e7	77	c
0110	da	4f	16	75	e2	8b	7b	cb	a1	87	1e	04	4
0120	00	ea	0e	f6	da	92	55	24	4d	b4	62	53	4
0130	9f	a9	53	a7	8b	97	e5	2c	8e	87	67	81	7
0140	54	2c	af	c0	a8	35	8d	82	91	89	ca	e9	5
0150	5b	76	a6	ec	7f	9c	9a	83	69	64	d8	ef	a
0160	86	95	5e	28	06	de	23	81	c0	0e	00	17	0
0170	00	01	00	00	0a	00	08	00	06	00	1d	00	1
0180	0b	00	02	01	00	00	23	00	00	00	10	00	0
0190	68	32	08	68	74	74	70	2f	31	2e	31	00	0
01a0	12	04	03	08	04	04	01	05	03	08	05	05	0

# 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

The image shows a Wireshark packet capture window titled "ech\_hrr.pcap". The packet list pane shows a single packet (No. 4) at time 0.017921, from source 192.168.1.90 to destination 213.108.108.101, protocol TLSv1.3, length 583. The packet details pane shows the following structure:

- Extensions Length: 401
  - Extension: server\_name (len=18) name=cover.defo.ie
  - Extension: encrypted\_client\_hello (len=154)
    - Type: encrypted\_client\_hello (65037)
    - Length: 154
    - Client Hello type: Outer Client Hello (0)
    - Cipher Suite: HKDF-SHA256/AES-128-GCM
    - Config Id: 85
    - Enc length: 32
    - Enc: 215c767deffb3c363e078d8e385f3ef6592403af7889150c1b8c8c02df20af20
    - Payload length: 112
    - Payload: 3717e3fb3696b023a5ea7c3de4eac172ba6b4b842947f90ad9029b8f2f05bb63abc2198303fe35332...
      - Version: TLS 1.2 (0x0303)
      - Random: 8726180bb24718089a4c5c8c93e0ea1c6d6649d7dd3c978fc1413854a20e9647
      - Session ID Length: 0
      - Cipher Suites Length: 6
      - Cipher Suites (3 suites)
      - Compression Methods Length: 1
      - Compression Methods (1 method)
      - Extensions Length: 43
        - Extension: server\_name (len=12) name=defo.ie
        - Extension: encrypted\_client\_hello (len=1)
        - Extension: supported\_versions (len=3) TLS 1.3
        - Extension: ech\_outer\_extensions (len=11)

# Confirming server acceptance

- ▼ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 155
  - ▼ Handshake Protocol: Server Hello
    - Handshake Type: Server Hello (2)
    - Length: 151
    - > Version: TLS 1.2 (0x0303)
    - ▼ Random: 6aef33f6f07cc80dba36ce1300dc13a76ff340388e6e9769ea06f7f30fd8b8cc
      - ECH Confirmation Bytes: ea06f7f30fd8b8cc
      - ▼ [Computed ECH Confirmation Bytes: ea06f7f30fd8b8cc]
      - ▼ [Expert Info (Note/Protocol): Calculated ECH Confirmation matches Server Random bytes, ECH was accepted]

# 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?