Taking a Bite at Apple's Network Stack

Reversing Proprietary Multi-Device Protocols with logfuse

Henri Jäger

whoami

PhD Student @ Hasso Plattner Institute

Mobile and Wireless Security

Universität Potsdam

HPI Hasso Plattner Institut

Digital Engineering · Universität Potsdam

[1] [2]

Fellow Researcher @ OpenKRITIS

EU / German Cyber Security Regulations

OpenKRITIS NIS2 Europa Betreiber Security School

KRITIS – auf den zweiten Blick

OpenKRITIS ist eine unabhängige Plattform für den Schutz Kritischer Infrastrukturen. Wir unterstützen Betreiber und Prüfer in der KRITIS und NIS2-Regulierung: Klare Strukturen zur Umsetzung von Cybersecurity, Governance und Prüfungen.

KRITIS und NIS2

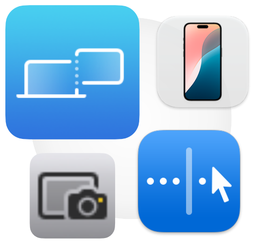
[D]

Kritische Infrastrukturen

OpenDrop

WatchWitch

OpenHaystack

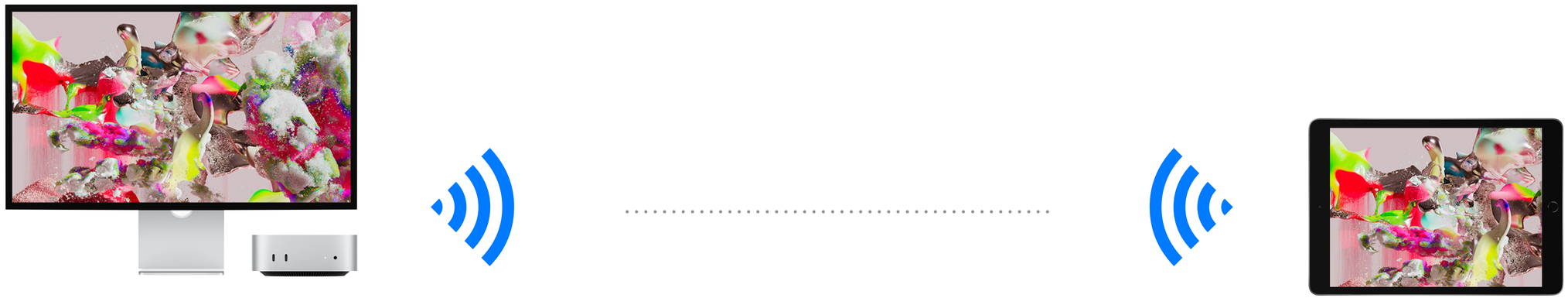


Pending?

[3] [4] [5] [A] [B] [C]

[6] [7] [8] [9]

Sidecar Display



Previous research on Continuity Camera and Sidecar Display has been conducted by Inga Dischinger [D] and Jan Röper [E]

Continuity Camera

[10] [11]

Universal Control

[12] [13] [14]

Low-Latency WiFi 🪄

Real-Time Constraints

Video and Audio

Access Category
Voice

Access Control Mandatory Frame Reordering
NAV
MAC-Layer Efficiency
Threshold
Block Acknowledgements Reverse Direction Grant

80 MHz
Channel Bandwidth

Ultra LLW **Real-time** LLW

More Operational Modes

Low-Latency Mechanisms of Low-Latency WiFi

Aggregated **MSDU** | Aggregated **MPDU**

Frame Overhead Reduction

IEEE 802.11e/n/ac
QoS | HT | VHT

1.504 ms **TXOP** | **Long Transmission Intervals**

3 slots CWmin | 7 slots CWmax | 2 slots AIFSN

***Fast* Channel Access**

Traffic Identifier 7

High-Priority Network Traffic

This talk is about the tooling.

Logging

Kernel Traces

XPC Communication

Backtraces

Packet Captures

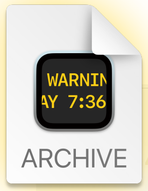
`en0, awdl0, llw0, BLE, ...`

Logging

Kernel Traces

XPC Communication

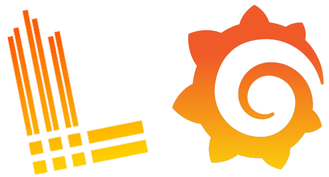
Backtraces




```
17:24:16.704 SidecarDisplayAgent        === Sideca
17:24:16.772 rapportd      Added policy: order = 9 re
17:24:16.792 kernel.development         SK[1]: channe
17:24:17.542 avconferenced              VCMediaStream
17:24:18.565 kernel.development         SK[7]: ch_eve
17:24:18.566 airportd      [corewifi] @[13190.661012]
17:24:22.688 SidecarRelay nw_channel_create_with_nex
17:24:24.563 mDNSResponder SysEventCallBack -- event
17:24:24.563 configd       Process interface link up:
17:24:24.566 nsattributedstringagent    SLSTransacti
```

```
4:17.127 SidecarRelay === IDS F090DC4A:remote:/
17:24:17.128 kernel        wlan0:com.apple.p2p: AWDLS
17:24:17.130 rapportd      48: SendEventID 'com.apple
17:24:17.133 runningboardd              _checkForSusp
17:24:28.103 wifip2pd      XPCSession[avconferenced 1
17:24:19.931 +0200         avconferenced [C96 IPv6#5c
17:24:20.588 kernel        rt_lookup_common:3376 (::,
17:24:23.170 kernel        wlan0:com.apple.p2p: IO802
17:24:25.972 kernel        cacheVerifiedACM <- reset
17:24:27.973 kernel AppleBiometricServices::message
```


```
17:24:16.704 SidecarDisplayAgent      === Sidecar (
17:24:16.772 rapportd     Added policy: order = 9 re
17:24:17.128 kernel       wlan0:com.apple.p2p: AWDLS
17:24:16.792 kernel.development       SK[1]: channe
17:24:17.130 rapportd     48: SendEventID 'com.apple
17:24:17.133 runningboardd            _checkForSusp
17:24:18.103 wifip2pd     XPCSession[avconferenced 1
17:24:17.542 avconferenced            VCMediaStream
17:24:18.565 kernel.development       SK[7]: ch_eve
17:24:19.931 +0200        avconferenced [C96 IPv6#5c
17:24:18.566 airportd     [corewifi] @[13190.661012]
17:24:20.588 kernel       rt_lookup_common:3376 (::,
17:24:23.170 kernel       wlan0:com.apple.p2p: IO802
17:24:22.688 SidecarRelay nw_channel_create_with_nex
17:24:25.972 kernel       cacheVerifiedACM <- reset
17:24:24.563 mDNSResponder SysEventCallBack -- event
17:24:24.563 configd      Process interface link
```

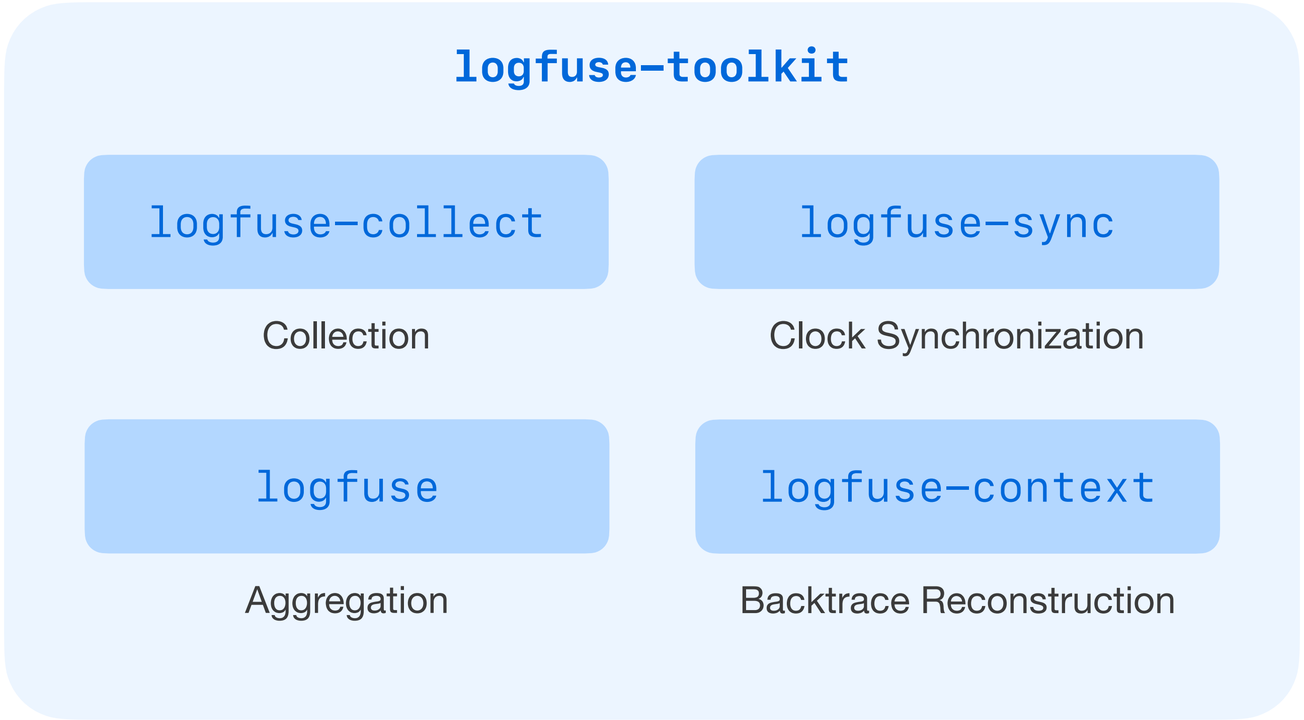


Limited log collection on iDevices

Do not account for clock drift

No context for static reverse engineering

[15] [16] [17] [18]


logfuse-toolkit
logfuse-collect
Collection
logfuse-sync
Clock Synchronization
logfuse
Aggregation
logfuse-context
Backtrace Reconstruction

Examples

aggregated-1.pcapng

(frame contains "llw" or frame contains "tshark" or frame contains "tcpdump") and (not(frame contains "kernel.development"))

Packet Commer	Interface	Info
Mac-mini	logarchive-Mac…	USER.ERR: 1 SidecarRelay (Network) (Mac-mini) PID: log_collect nw_listener_reconcile_inboxes_on_queue_block_invok
Mac-mini	logarchive-Mac…	USER.ERR: 1 SidecarRelay (Network) (Mac-mini) PID: log_collect nw_channel_create_with_nexus_flow nw_path_flow_get
Mac-mini	logarchive-Mac…	USER.ERR: 1 SidecarRelay (Network) (Mac-mini) PID: log_collect -[nw_ip_channel_inbox initWithPath:flow:parameters
Mac-mini	logarchive-Mac…	USER.ERR: 1 SidecarRelay (Network) (Mac-mini) PID: log_collect nw_listener_reconcile_inboxes_on_queue_block_invok
Mac-mini	logarchive-Mac…	USER.ERR: 1 SidecarRelay (CoreUtils) (Mac-mini) PID: log_collect Session started: Server, ID '719D44F5:AVCVideoSt
Mac-mini	com.apple.ioki…	[TCP Dup ACK 5633512#1] CC: Net llw0 59840 → 58874 [ACK] Seq=1750 Ack=1593 Win=130432 Len=0 TSval=3808603038 TSecr
iPad	logarchive-iPad	USER.ERR: 1 SidecarRelay (Network) (iPad) PID: log_collect [L48 udp, definite, server, allow duplicate updates, a
iPad	logarchive-iPad	USER.ERR: 1 SidecarRelay (Network) (iPad) PID: log_collect nw_listener_reconcile_inboxes_on_queue_block_invoke [L
iPad	logarchive-iPad	USER.ERR: 1 SidecarRelay (Network) (iPad) PID: log_collect nw_listener_start_on_queue_block_invoke [L48] Handling
iPad	logarchive-iPad	USER.ERR: 1 SidecarRelay (Network) (iPad) PID: log_collect nw_listener_reconcile_inboxes_on_queue_block_invoke [L
Mac-mini	logarchive-Mac…	USER.ERR: 1 wifip2pd (wifip2pd) (Mac-mini) PID: log_collect Posted peer presence for f6:98:bb:2c:cb:0b on llw0 |
iPad	logarchive-iPad	USER.ERR: 1 SidecarRelay (Network) (iPad) PID: log_collect nw_channel_create_with_nexus_flow nw_path_flow_get_nex
iPad	logarchive-iPad	USER.ERR: 1 SidecarRelay (Network) (iPad) PID: log_collect -[nw_ip_channel_inbox initWithPath:flow:parameters:del
iPad	logarchive-iPad	USER.ERR: 1 SidecarRelay (Network) (iPad) PID: log_collect nw_listener_reconcile_inboxes_on_queue_block_invoke [L
iPad	logarchive-iPad	USER.ERR: 1 SidecarRelay (CoreUtils) (iPad) PID: log_collect Register traffic: [fd02:5c7e:2d18::19%llw0]:59611, 0
iPad	logarchive-iPad	USER.ERR: 1 SidecarRelay (CoreUtils) (iPad) PID: log_collect Session started: Client, ID '719D44F5:AVCVideoStream
iPad	com.apple.ioki…	setLinkStateInternal: on llw0 linkState:UP reason:1
iPad	com.apple.driv…	setLinkStateInternal: on llw0 linkState:UP reason:1
iPad	logarchive-iPad	USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect [C96 4274B926-0BDB-4E52-BF47-95929CBB81D4 IPv6#5c591c
iPad	logarchive-iPad	USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect [C96 IPv6#5c591cee.59611 waiting parent-flow (satisfi
iPad	logarchive-iPad	USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect nw_connection_endpoint_report_on_nw_queue_block_invok

Packet comments

Frame 5826822: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface logarchive-Mac-mini, id 0

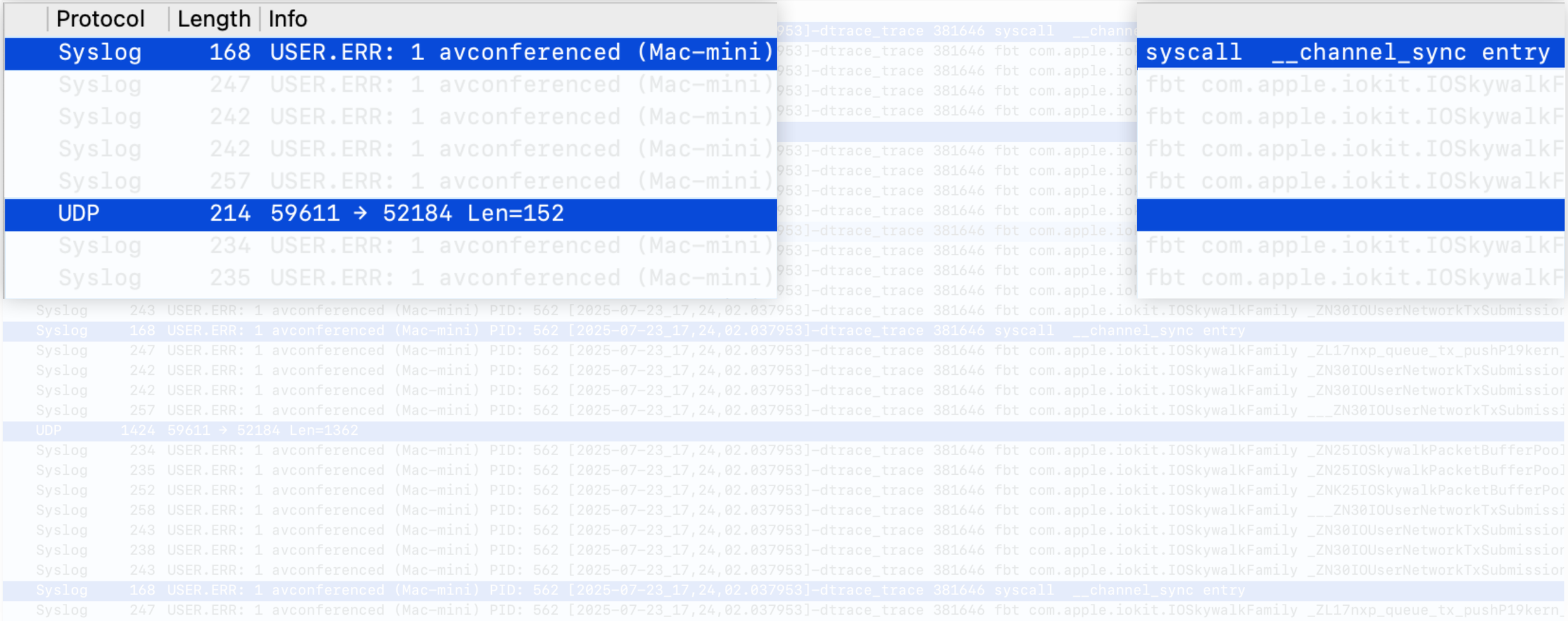
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

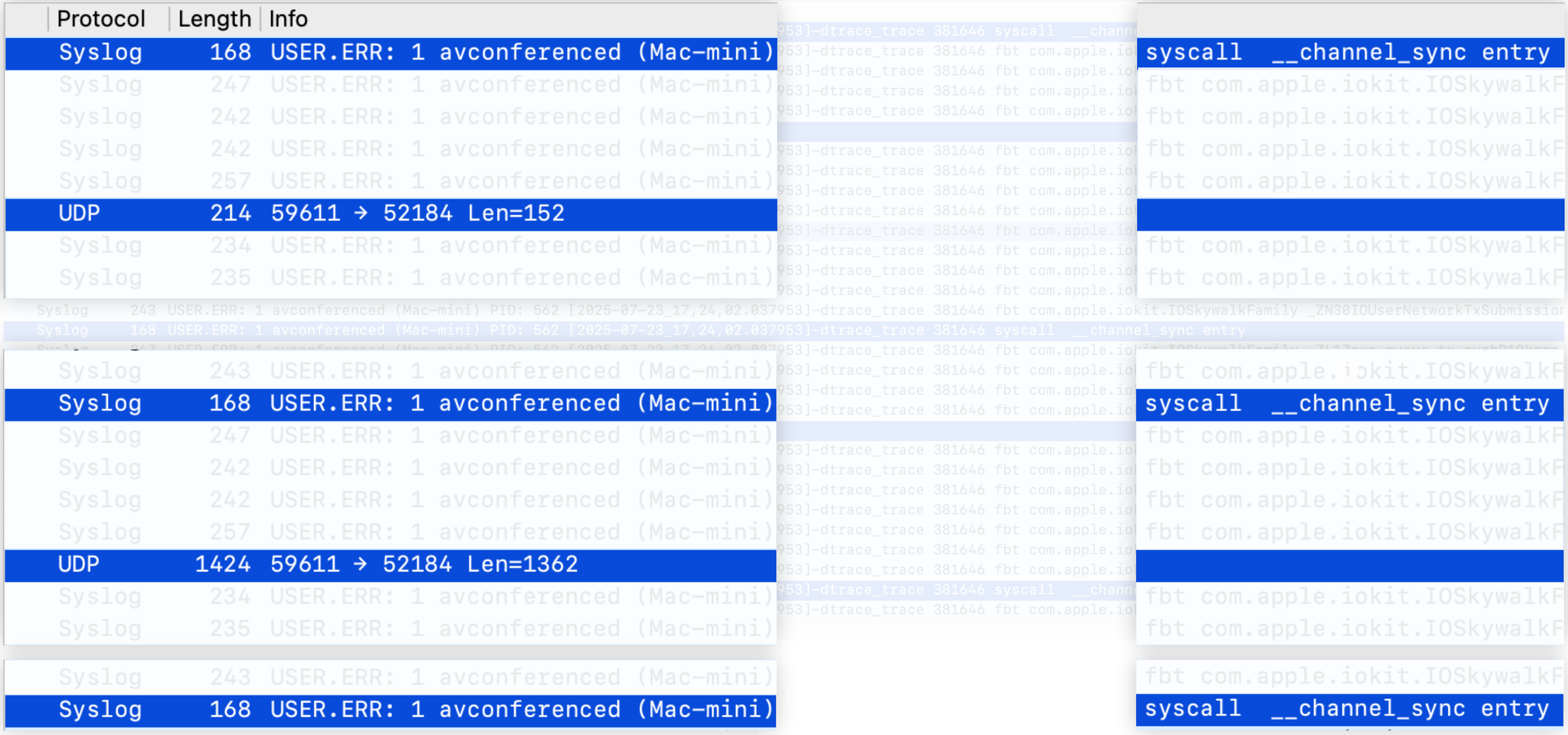
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 0.0.0.0

User Datagram Protocol, Src Port: 0, Dst Port: 514

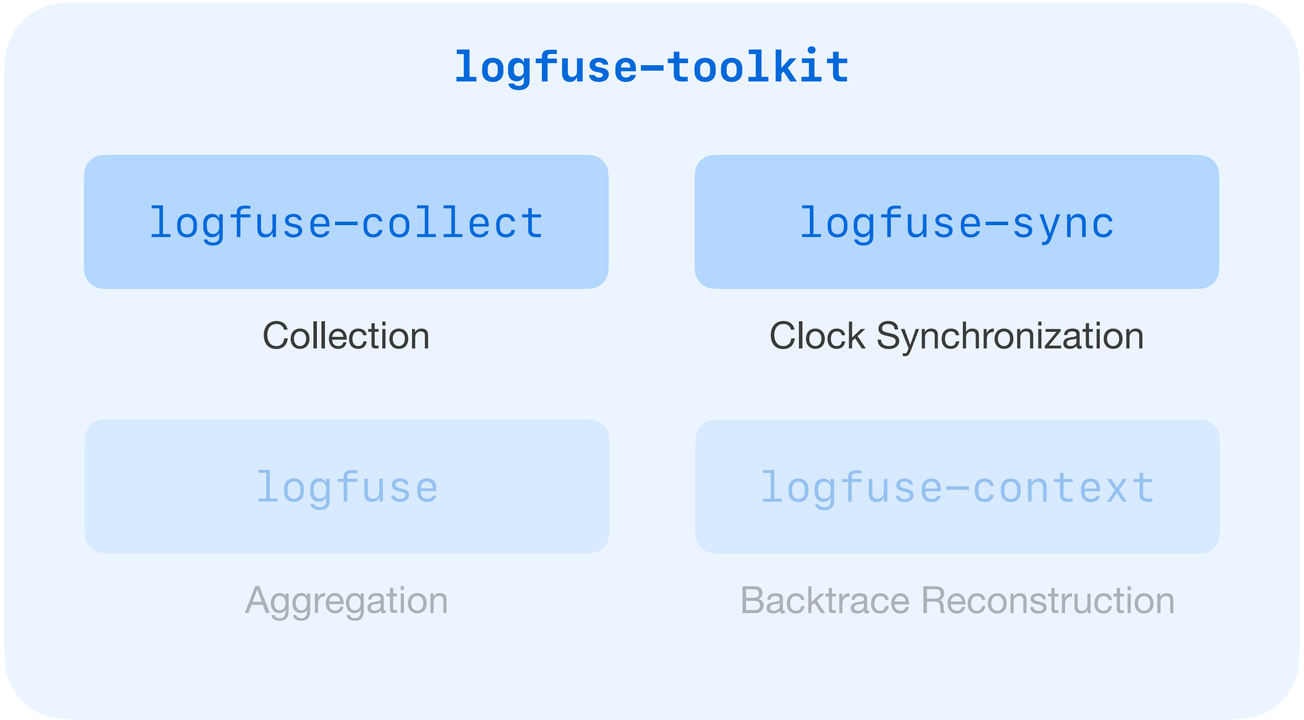
Syslog message: USER.ERR: 1 wifip2pd (wifip2pd) (Mac-mini) PID: log_collect Posted peer presence for f6:98:bb:2c:cb:0b on llw0 | [NO_MAP] | Pos

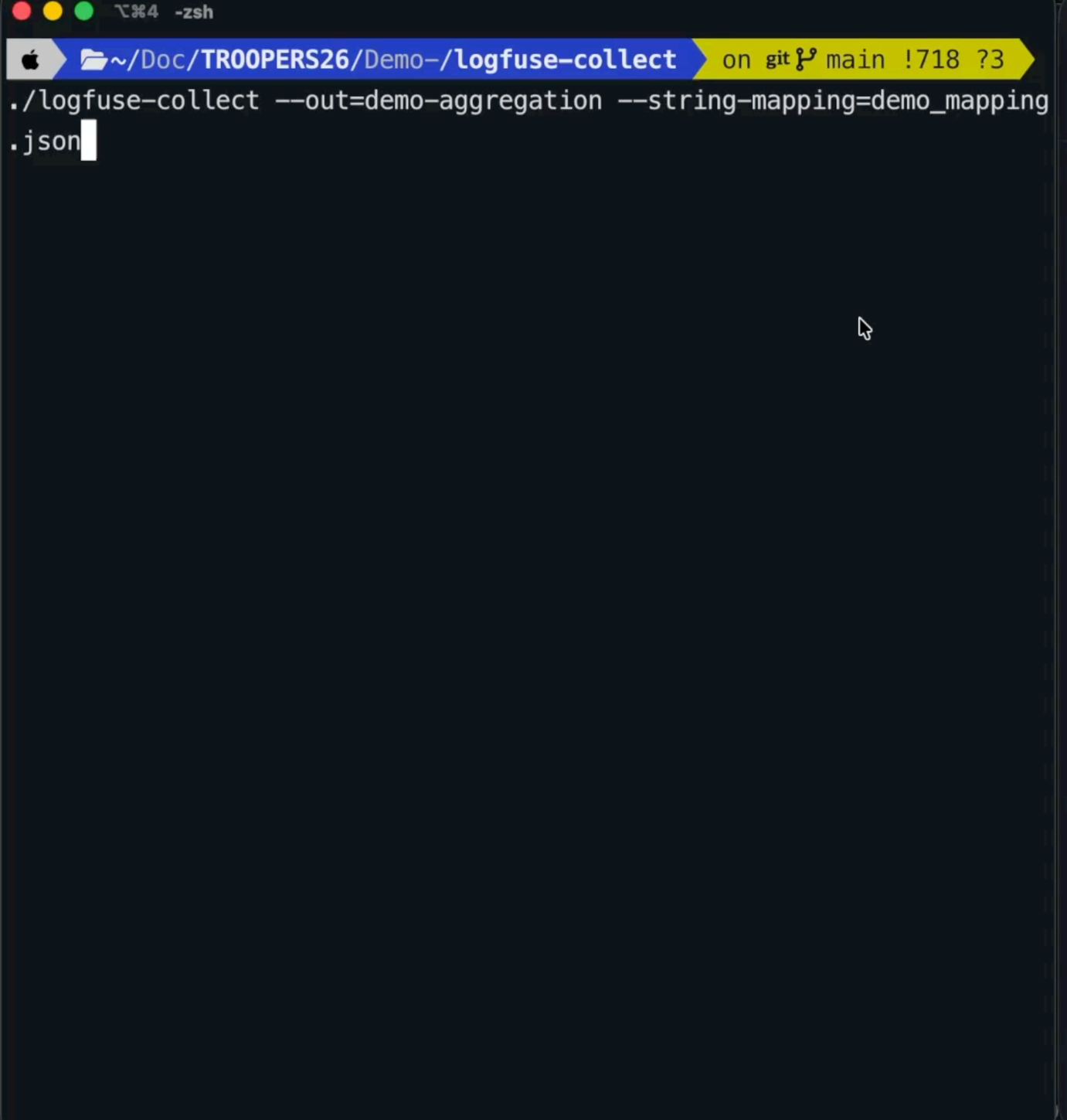
Protocol	Length	Info
Syslog	168	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 syscall __channel_sync entry
Syslog	247	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZL17nxp_queue_tx_pushP19kern_
Syslog	242	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	242	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	257	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily ___ZN30IOUserNetworkTxSubmissi
UDP	214	59611 → 52184 Len=152
Syslog	234	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN25IOSkywalkPacketBufferPool
Syslog	235	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN25IOSkywalkPacketBufferPool
Syslog	252	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZNK25IOSkywalkPacketBufferPoc
Syslog	258	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily ___ZN30IOUserNetworkTxSubmissi
Syslog	243	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	238	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	239	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	271	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	243	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	168	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 syscall __channel_sync entry
Syslog	247	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZL17nxp_queue_tx_pushP19kern_
Syslog	242	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	242	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	257	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily ___ZN30IOUserNetworkTxSubmissi
UDP	1424	59611 → 52184 Len=1362
Syslog	234	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN25IOSkywalkPacketBufferPool
Syslog	235	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN25IOSkywalkPacketBufferPool
Syslog	252	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZNK25IOSkywalkPacketBufferPoc
Syslog	258	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily ___ZN30IOUserNetworkTxSubmissi
Syslog	243	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	238	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	243	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog	168	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 syscall __channel_sync entry
Syslog	247	USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZL17nxp_queue_tx_pushP19kern_

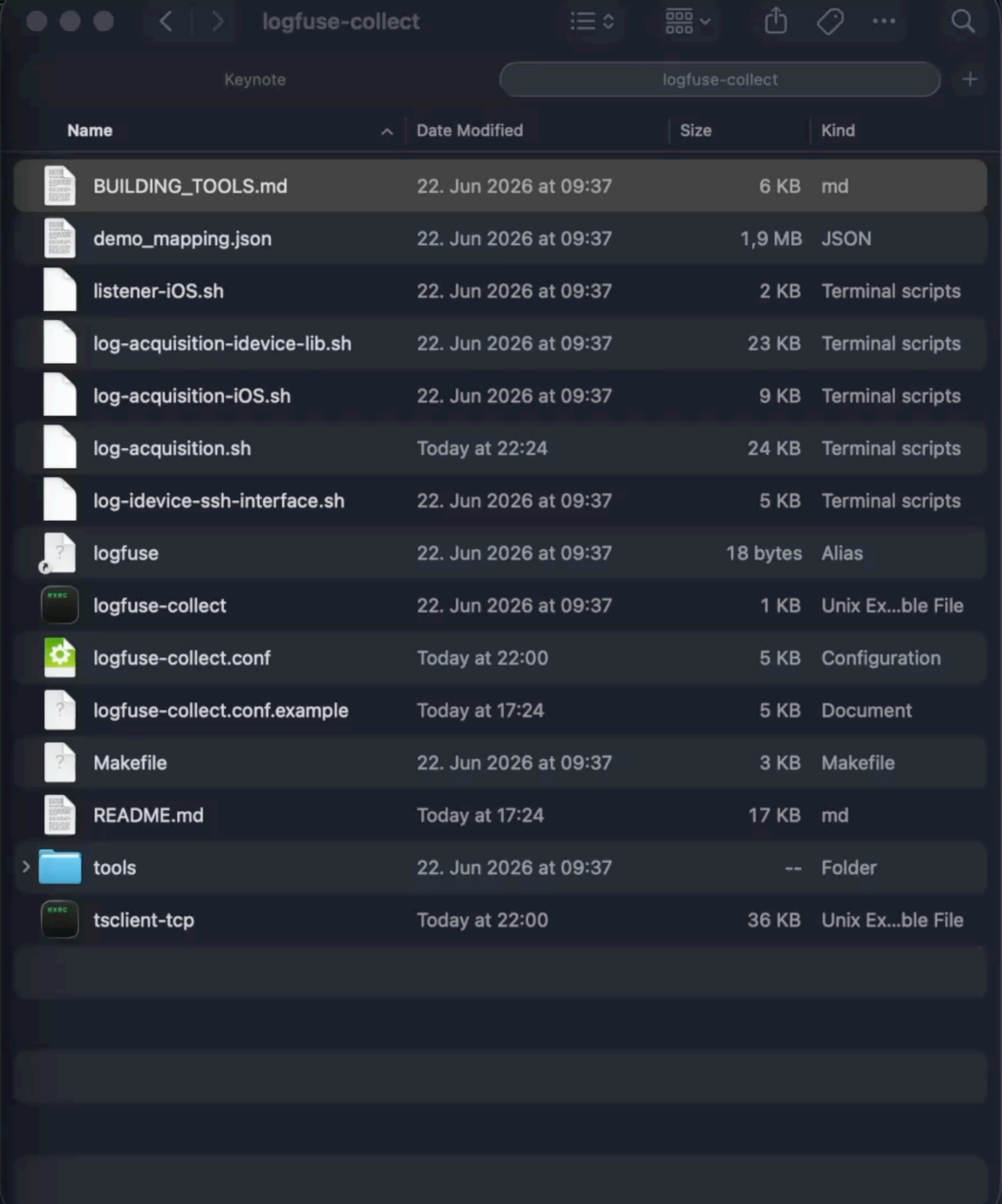

Protocol Length Info
Syslog 168 USER.ERR: 1 avconferenced (Mac-mini)
Syslog 247 USER.ERR: 1 avconferenced (Mac-mini)
Syslog 242 USER.ERR: 1 avconferenced (Mac-mini)
Syslog 242 USER.ERR: 1 avconferenced (Mac-mini)
Syslog 257 USER.ERR: 1 avconferenced (Mac-mini)
UDP 214 59611 → 52184 Len=152
Syslog 234 USER.ERR: 1 avconferenced (Mac-mini)
Syslog 235 USER.ERR: 1 avconferenced (Mac-mini)
syscall __channel_sync entry
fbt com.apple.iokit.IOSkywalkF
fbt com.apple.iokit.IOSkywalkF
fbt com.apple.iokit.IOSkywalkF
fbt com.apple.iokit.IOSkywalkF
fbt com.apple.iokit.IOSkywalkF
fbt com.apple.iokit.IOSkywalkF
Syslog 243 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog 168 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 syscall __channel_sync entry
Syslog 247 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZL17nxp_queue_tx_pushP19kern_
Syslog 242 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog 242 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog 257 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily ___ZN30IOUserNetworkTxSubmissi
UDP 1424 59611 → 52184 Len=1362
Syslog 234 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN25IOSkywalkPacketBufferPool
Syslog 235 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN25IOSkywalkPacketBufferPool
Syslog 252 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZNK25IOSkywalkPacketBufferPoo
Syslog 258 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily ___ZN30IOUserNetworkTxSubmissi
Syslog 243 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog 238 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog 243 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZN30IOUserNetworkTxSubmissior
Syslog 168 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 syscall __channel_sync entry
Syslog 247 USER.ERR: 1 avconferenced (Mac-mini) PID: 562 [2025-07-23_17,24,02.037953]-dtrace_trace 381646 fbt com.apple.iokit.IOSkywalkFamily _ZL17nxp_queue_tx_pushP19kern_


Protocol Length Info
Syslog 168 USER.ERR: 1 avconferenced (Mac-mini)
UDP 214 59611 → 52184 Len=152
Syslog 168 USER.ERR: 1 avconferenced (Mac-mini)
UDP 1424 59611 → 52184 Len=1362
Syslog 168 USER.ERR: 1 avconferenced (Mac-mini)
syscall __channel_sync entry

Collecting Logs with `logfuse`


logfuse-toolkit
logfuse-collect
Collection
logfuse-sync
Clock Synchronization
logfuse
Aggregation
logfuse-context
Backtrace Reconstruction


⌥⌘4 -zsh
~/Doc/TROOPERS26/Demo-/logfuse-collect
on git main !718 ?3
./logfuse-collect --out=demo-aggregation --string-mapping=demo_mapping
.json


logfuse-collect
Keynote
logfuse-collect
Name
Date Modified
Size
Kind
BUILDING_TOOLS.md 22. Jun 2026 at 09:37 6 KB md
demo_mapping.json 22. Jun 2026 at 09:37 1,9 MB JSON
listener-iOS.sh 22. Jun 2026 at 09:37 2 KB Terminal scripts
log-acquisition-idevice-lib.sh 22. Jun 2026 at 09:37 23 KB Terminal scripts
log-acquisition-iOS.sh 22. Jun 2026 at 09:37 9 KB Terminal scripts
log-acquisition.sh Today at 22:24 24 KB Terminal scripts
log-idevice-ssh-interface.sh 22. Jun 2026 at 09:37 5 KB Terminal scripts
logfuse 22. Jun 2026 at 09:37 18 bytes Alias
logfuse-collect 22. Jun 2026 at 09:37 1 KB Unix Ex...ble File
logfuse-collect.conf Today at 22:00 5 KB Configuration
logfuse-collect.conf.example Today at 17:24 5 KB Document
Makefile 22. Jun 2026 at 09:37 3 KB Makefile
README.md Today at 17:24 17 KB md
tools 22. Jun 2026 at 09:37 -- Folder
tsclient-tcp Today at 22:00 36 KB Unix Ex...ble File

Log Collection Challenges

Log Sources

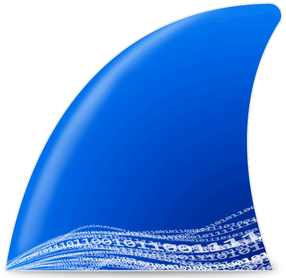
Multi-Device Orchestration

Clock Offset Correction

Console

dtrace

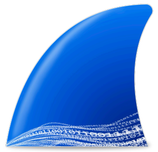
ktrace



Wireshark

cctool

PacketLogger

						
macOS	✅	✅	✅	✅	✅	✅
iOS	✅ `log`	✅ `tcpdump*`	✅	❌	✅ from source*	✅ reimplementation*

Jailbreak required — our setup includes an iPad (7th generation)

Log Collection Challenges

Log Sources

Multi-Device Orchestration

Clock Offset Correction

log-acquisition.sh

Command-Line Interface

`log-acquisition.sh --format=pcap`

log-acquisition-idevice-lib.sh

Remote Device Management

`get_latest_dir_on_iPad(), ...`

log-acquisition-iOS.sh

log-idevice-ssh-interface.sh

SSH communication

`start_iproxy(), send_to_iPad(), ...`

listener-iOS.sh

ssh tunnel

log-acquisition.sh

Command-Line Interface

`log-acquisition.sh --format=pcap`

log-acquisition-idevice-lib.sh

Remote Device Management

`get_latest_dir_on_iPad(), ...`

log-idevice-ssh-interface.sh

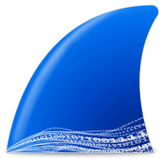
SSH communication

`start_iproxy(), send_to_iPad(), ...`

log-acquisition-iOS.sh

listener-iOS.sh

ssh tunnel



log-acquisition.sh

Command-Line Interface

`log-acquisition.sh --format=pcap`

log-acquisition-idevice-lib.sh

Remote Device Management

`get_latest_dir_on_iPad(), ...`

log-acquisition-iOS.sh

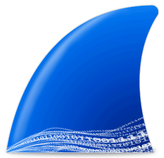
log-idevice-ssh-interface.sh

SSH communication

`start_iproxy(), send_to_iPad(), ...`

listener-iOS.sh

ssh tunnel



log-acquisition.sh

log-acquisition-idevice-lib.sh

log-idevice-ssh-interface.sh

log-acquisition-iOS.sh

listener-iOS.sh

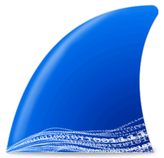
ssh tunnel

Process Management

`start_pre_session_commands(), ...`

Command Injection

`Relay remote commands to upper layer`



log-acquisition.sh

log-acquisition-idevice-lib.sh

log-idevice-ssh-interface.sh

log-acquisition-iOS.sh

listener-iOS.sh

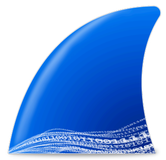
Process Management

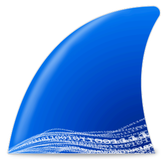
`start_pre_session_commands(), ...`

Command Injection

`Relay remote commands to upper layer`

ssh tunnel





Log Collection Challenges

Log Sources

Multi-Device Orchestration

Clock Offset Correction

Logging

Kernel Traces

XPC Communication

Backtraces

Packet Captures

`en0, awdl0, llw0, BLE, ...`

Logging

Kernel Traces

XPC Communication

Backtraces

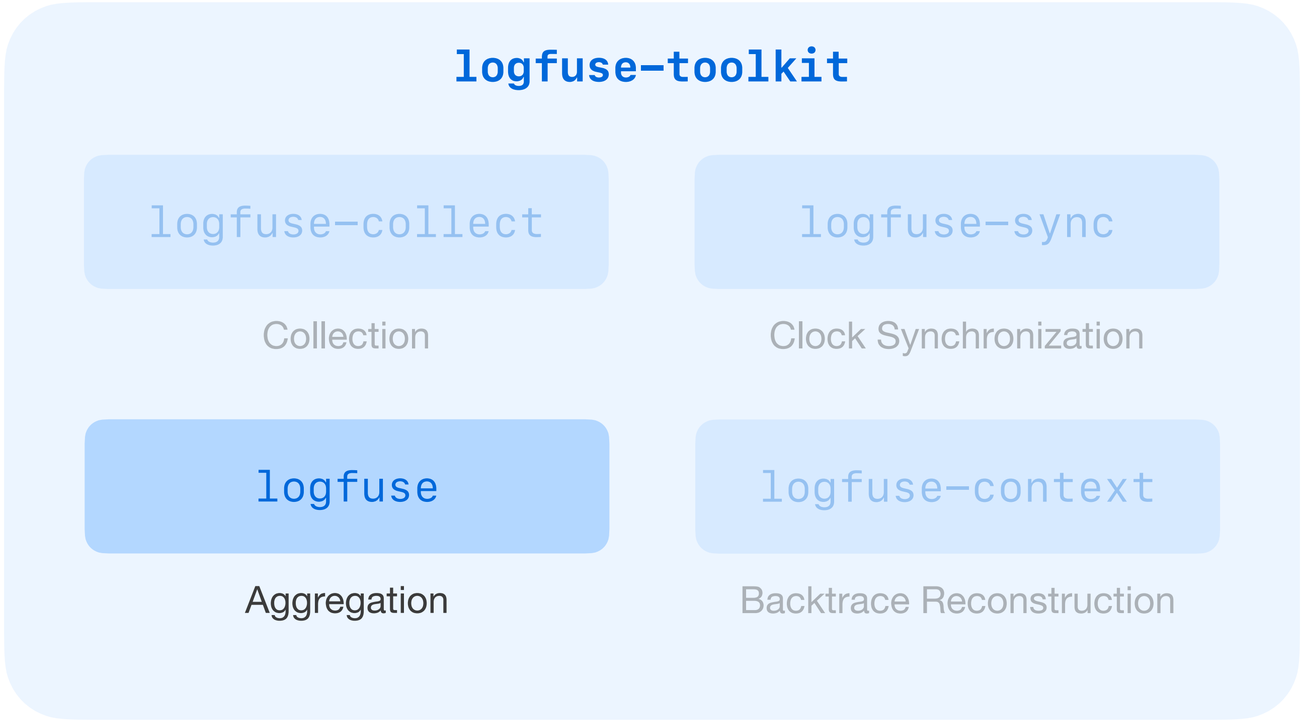
NTP Client

collect clock offsets using NTP

TCP via usbmuxd / iproxy

NTP Server

Aggregating Logs with `logfuse`


logfuse-toolkit
logfuse-collect
Collection
logfuse-sync
Clock Synchronization
logfuse
Aggregation
logfuse-context
Backtrace Reconstruction

ktrace output

Packet Captures

Log Archive

Text Files &
Custom Output

ktrace parser | pcapng parser | logarchive parser | dtrace parser | txt parser

Parse Input Files into Business Logic

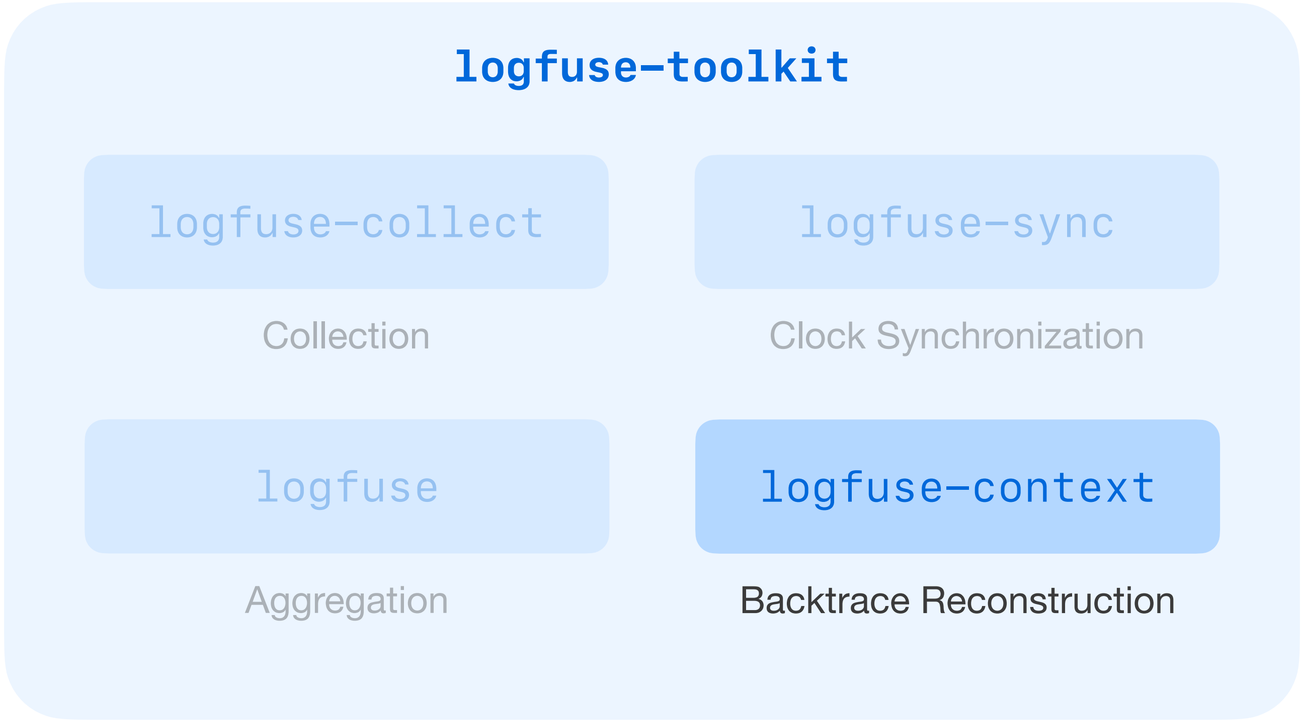
Filter Pre-Recorded Noise

Apply Static Filter Criteria

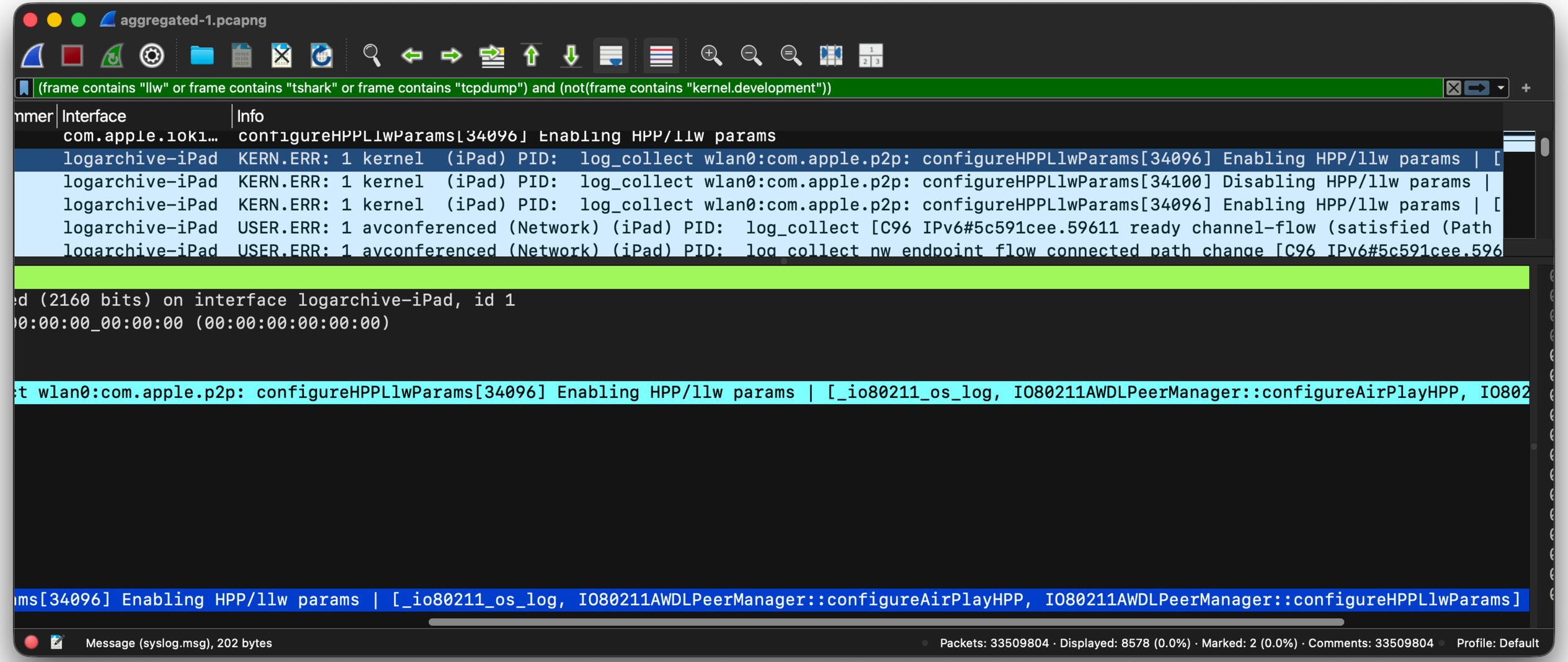
Resolve Logs to
User / Kernel-Space Functions

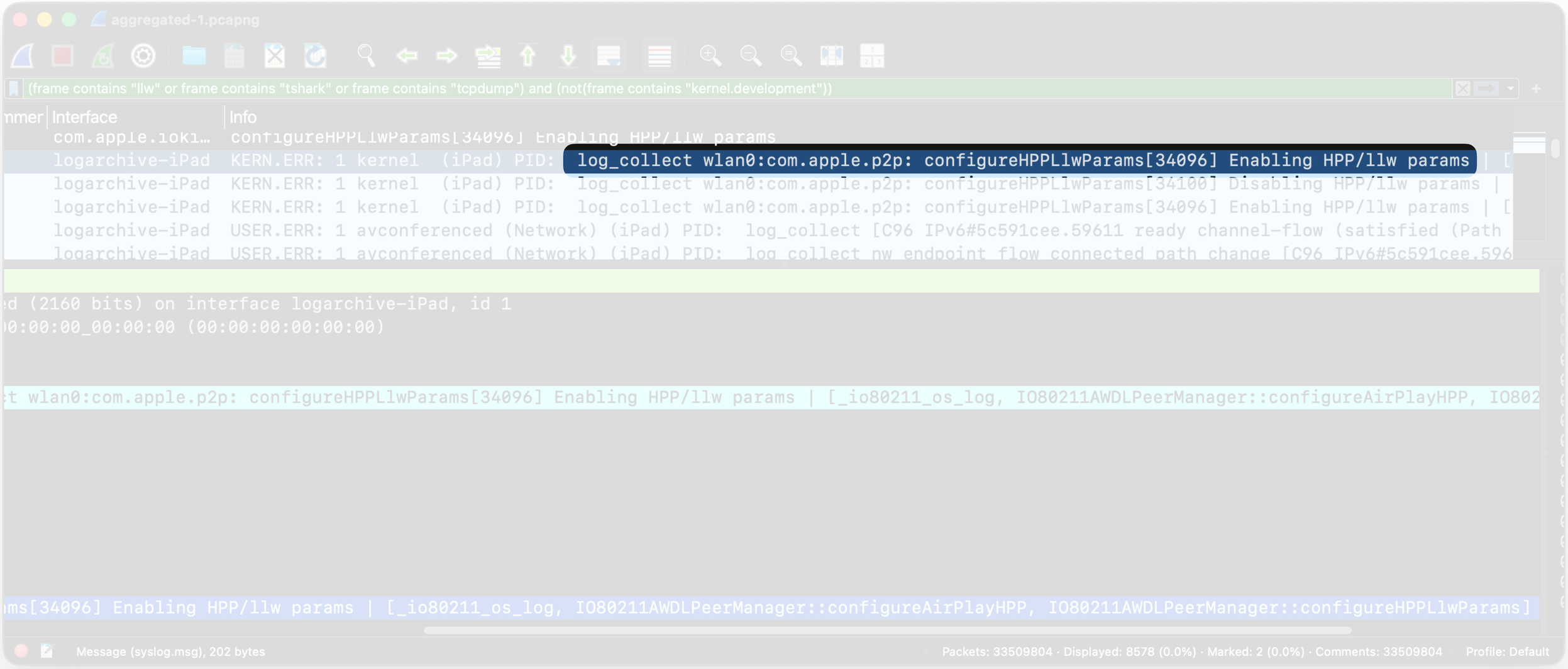
Write .pcapng File
with `python-pcapng`

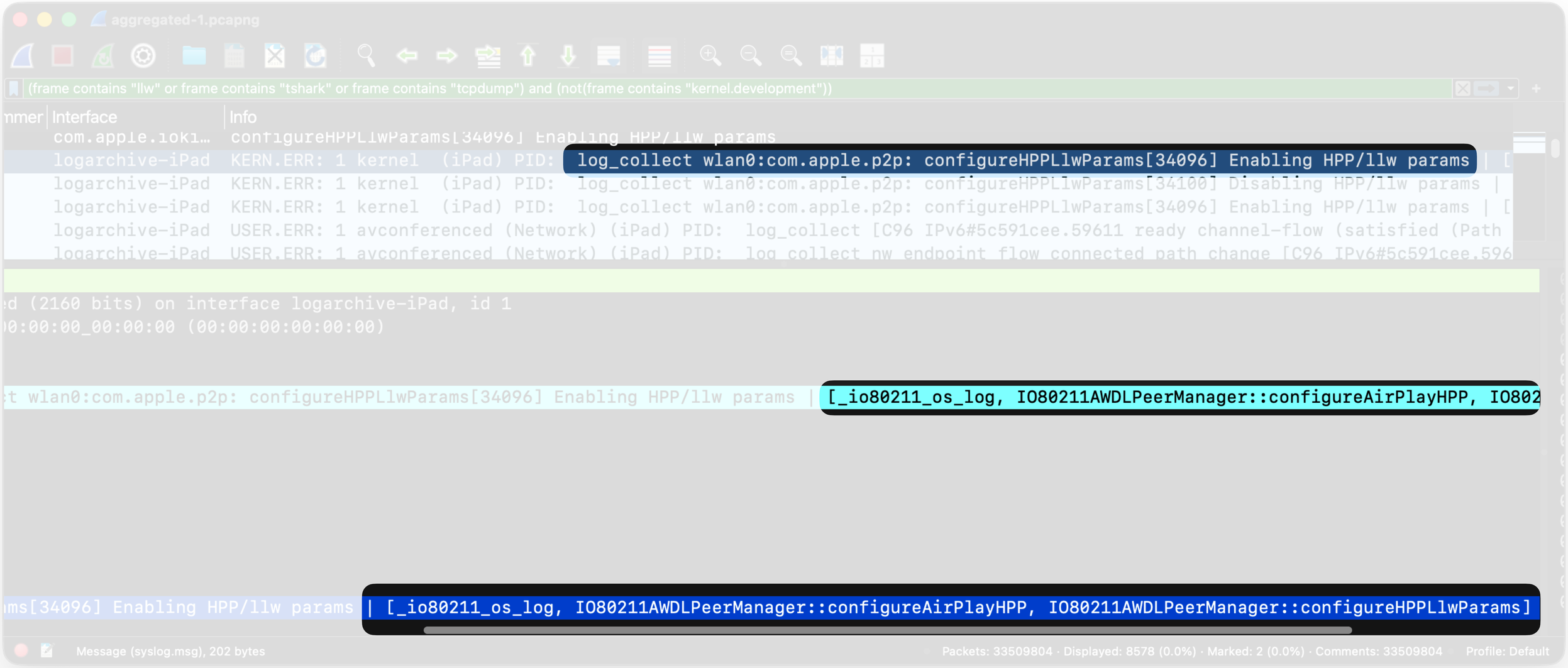
Log to
macOS' Unified Logging System


logfuse-toolkit
logfuse-collect
Collection
logfuse-sync
Clock Synchronization
logfuse
Aggregation
logfuse-context
Backtrace Reconstruction

Backtrace Reconstruction


aggregated-1.pcapng
(frame contains "llw" or frame contains "tshark" or frame contains "tcpdump") and (not(frame contains "kernel.development"))
nmer | Interface | Info
com.apple.lokl… configureHPPLlwParams[34096] Enabling HPP/llw params
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34100] Disabling HPP/llw params |
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [
logarchive-iPad USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect [C96 IPv6#5c591cee.59611 ready channel-flow (satisfied (Path
logarchive-iPad USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect nw_endpoint_flow_connected_path_change [C96 IPv6#5c591cee.596
ed (2160 bits) on interface logarchive-iPad, id 1
00:00:00_00:00:00 (00:00:00:00:00:00)
t wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [_io80211_os_log, IO80211AWDLPeerManager::configureAirPlayHPP, IO802
ms[34096] Enabling HPP/llw params | [_io80211_os_log, IO80211AWDLPeerManager::configureAirPlayHPP, IO80211AWDLPeerManager::configureHPPLlwParams]
Message (syslog.msg), 202 bytes
Packets: 33509804 · Displayed: 8578 (0.0%) · Marked: 2 (0.0%) · Comments: 33509804
Profile: Default


aggregated-1.pcapng
(frame contains "llw" or frame contains "tshark" or frame contains "tcpdump") and (not(frame contains "kernel.development"))
nmer Interface Info
com.apple.iokit… configureHPPLlwParams[34096] Enabling HPP/llw params
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34100] Disabling HPP/llw params |
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [
logarchive-iPad USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect [C96 IPv6#5c591cee.59611 ready channel-flow (satisfied (Path
logarchive-iPad USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect nw_endpoint_flow_connected_path_change [C96 IPv6#5c591cee.596
ed (2160 bits) on interface logarchive-iPad, id 1
0:00:00_00:00:00 (00:00:00:00:00:00)
t wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [_io80211_os_log, IO80211AWDLPeerManager::configureAirPlayHPP, IO802
ms[34096] Enabling HPP/llw params | [_io80211_os_log, IO80211AWDLPeerManager::configureAirPlayHPP, IO80211AWDLPeerManager::configureHPPLlwParams]
Message (syslog.msg), 202 bytes
Packets: 33509804 · Displayed: 8578 (0.0%) · Marked: 2 (0.0%) · Comments: 33509804
Profile: Default


aggregated-1.pcapng
(frame contains "llw" or frame contains "tshark" or frame contains "tcpdump") and (not(frame contains "kernel.development"))
nmer Interface Info
com.apple.1ok1… configureHPPLlwParams[34096] Enabling HPP/llw params
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34100] Disabling HPP/llw params |
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [
logarchive-iPad USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect [C96 IPv6#5c591cee.59611 ready channel-flow (satisfied (Path
logarchive-iPad USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect nw_endpoint_flow_connected_path_change [C96 IPv6#5c591cee.596
ed (2160 bits) on interface logarchive-iPad, id 1
0:00:00_00:00:00 (00:00:00:00:00:00)
t wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [_io80211_os_log, IO80211AWDLPeerManager::configureAirPlayHPP, IO802
ms[34096] Enabling HPP/llw params | [_io80211_os_log, IO80211AWDLPeerManager::configureAirPlayHPP, IO80211AWDLPeerManager::configureHPPLlwParams]
Message (syslog.msg), 202 bytes
Packets: 33509804 · Displayed: 8578 (0.0%) · Marked: 2 (0.0%) · Comments: 33509804
Profile: Default

macOS	✅	☑	☑	☑	✅	☑
iOS	✅ `log`	☑ `tcpdump*`	☑	❌	✅ from source*	☑ reimplementation*

* Jailbreak required — our setup includes an iPad (7th generation)

macOS	✅	☑	☑	☑	☑	☑
iOS	✅ `log`	☑ `tcpdump*`	☑	✕	☑ from source*	☑ reimplementation*

Jailbreak required — our setup includes an iPad (7th generation)

[2026-06-23_17,25,01.630652]-log_collect.logarchive
114.616 messages

All Messages | Errors and Faults

Search

Type	Process	Message	
	kernel.development	SK[1]: pkt_copy_from_pkt	kernel_task(0) RX len 112, copy+sum 0 (csum 0x0000), start 0
	kernel.development	SK[1]: pkt_copy_from_pkt	pkt 0xfffffe748185fd10 doff 0 csumf/rxstart/rxval 0x0/0/0x0000
	kernel.development	SK[1]: pkt_copy_from_pkt	kernel_task(0) RX buf 0xfffffe7481882800 len 112 lim 2048 0: d6 b9 9d c5 ff dd f
	kernel.development	SK[1]: kr_exit	kr "netif_vp:2 RX0" (0xfffffe200e3b8400) right released (0 waiters)
	kernel.development	SK[1]: filt_chrw	na "netif_vp:2" (0xfffffe200ec76600) ch 0xfffffe1679382f20 kn 0xfffffe1b41ff6e00 (re
	kernel.development	SK[2]: ch_event_log	enter: na "netif_vp:2" (0xfffffe200ec76600) ch 0xfffffe1679382f20 avconferenced(562)
	kernel.development	SK[2]: kr_enter	kr "netif_vp:2 RX0" (0xfffffe200e3b8400) right acquired
	kernel.development	SK[2]: kr_rxsync_prologue	avconferenced(562) kr "netif_vp:2 RX0", kh 279 kt 280 | rh 279 rt 279 | h 279 t 279
	kernel.development	SK[2]: kr_externalize_metadata_internal	avconferenced(562) kring 0xfffffe200e3b8400 kqum 0xfffffe748185fd10 -> uqum 0xffff
	kernel.development	SK[2]: kr_rxsync_finalize	avconferenced(562) kr "netif_vp:2 RX0", kh 279 kt 280 | rh 279 rt 280 | h 279 t 280
	kernel.development	SK[2]: kr_exit	kr "netif_vp:2 RX0" (0xfffffe200e3b8400) right released (0 waiters)
	kernel.development	SK[2]: ch_event_log	exit: na "netif_vp:2" (0xfffffe200ec76600) ch 0xfffffe1679382f20 avconferenced(562)
	kernel.development	SK[2]: ch_event_log	enter: na "netif_vp:2" (0xfffffe200ec76600) ch 0xfffffe1679382f20 avconferenced(562)
	kernel.development	SK[2]: kr_enter	kr "netif_vp:2 RX0" (0xfffffe200e3b8400) right acquired
	kernel.development	SK[2]: kr_rxsync_prologue	avconferenced(562) kr "netif_vp:2 RX0", kh 279 kt 280 | rh 279 rt 280 | h 280 t 280
	kernel.development	SK[2]: kr_rxsync_finalize	avconferenced(562) kr "netif_vp:2 RX0", kh 280 kt 280 | rh 280 rt 280 | h 280 t 280
	kernel.development	SK[2]: kr_exit	kr "netif_vp:2 RX0" (0xfffffe200e3b8400) right released (0 waiters)

Showing: All Messages

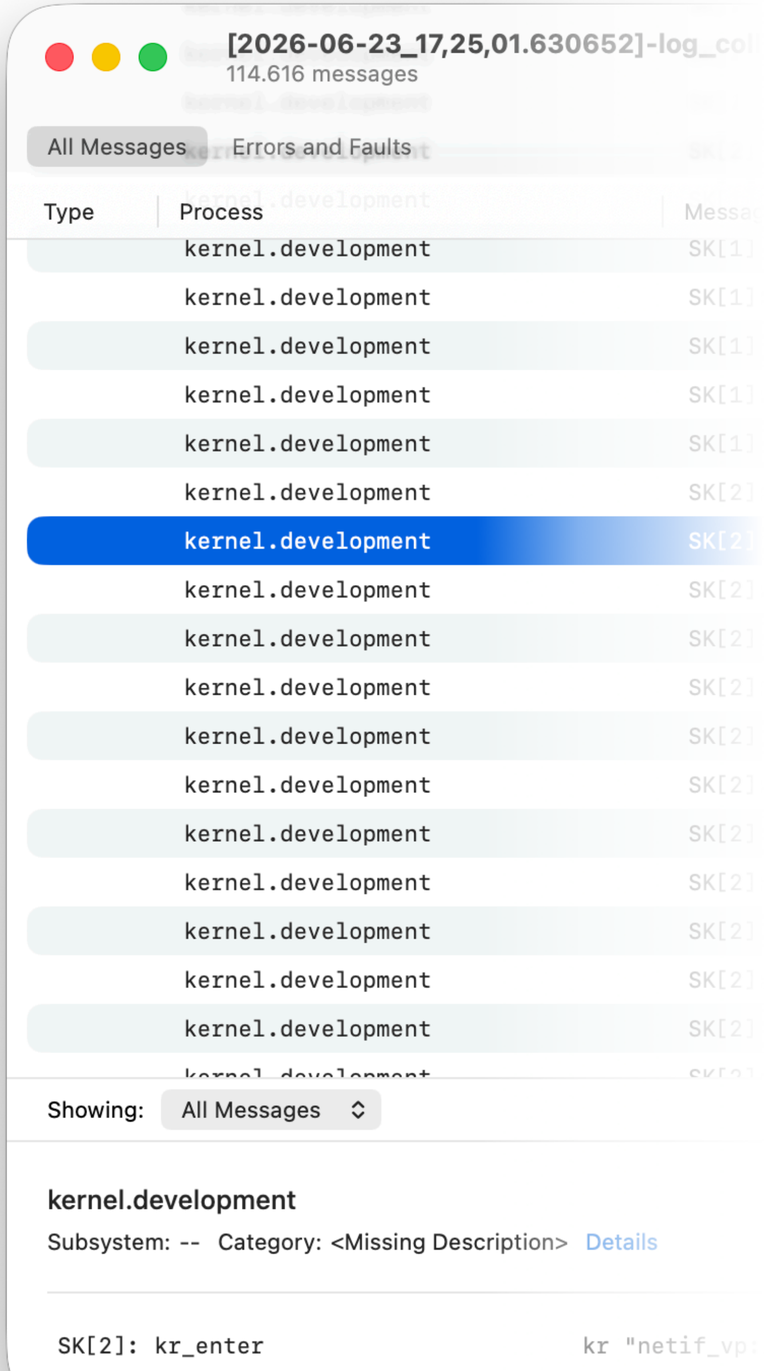
kernel.development

Volatile

Subsystem: -- Category: <Missing Description> Details

2025-07-23 17:24:25.280451+0200

SK[2]: kr_enter kr "netif_vp:2 RX0" (0xfffffe200e3b8400) right acquired




```
{
   "timezoneName" : "",
   "messageType" : "Default",
   "eventType" : "logEvent",
   "machTimestamp" : 316687745458,
   "formatString" : "SK[%u]: %-30s kr "%s" (0x%llx) right acquired",
   "eventMessage" : "SK[6]: kr_enter kr "netif_vp:2 RX0" (0xfffffe200e3b8400) right acquired",
   "processImagePath" : "/kernel.development",
   "senderImagePath" : "/kernel.development",
   ...
}
```

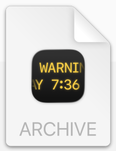

```
SK[%u]: %-30s kr "%s"
(0x%llx) right
acquired
```

f-string


```
SK[%u]: %-30s kr "%s"
(0x%llx) right
acquired
```

f-string

Dynamic RE




```
SK[%u]: %-30s kr "%s"
(0x%llx) right
acquired
```

f-string

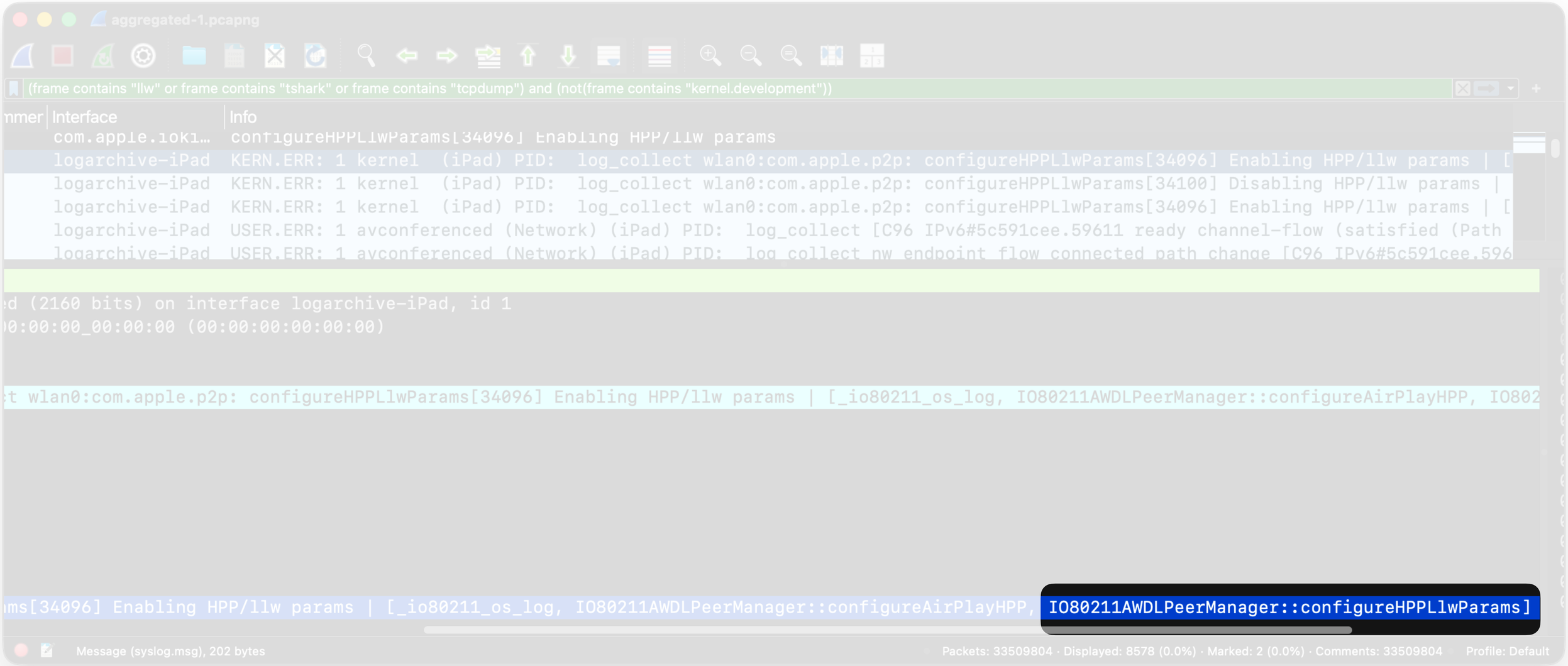
Static RE

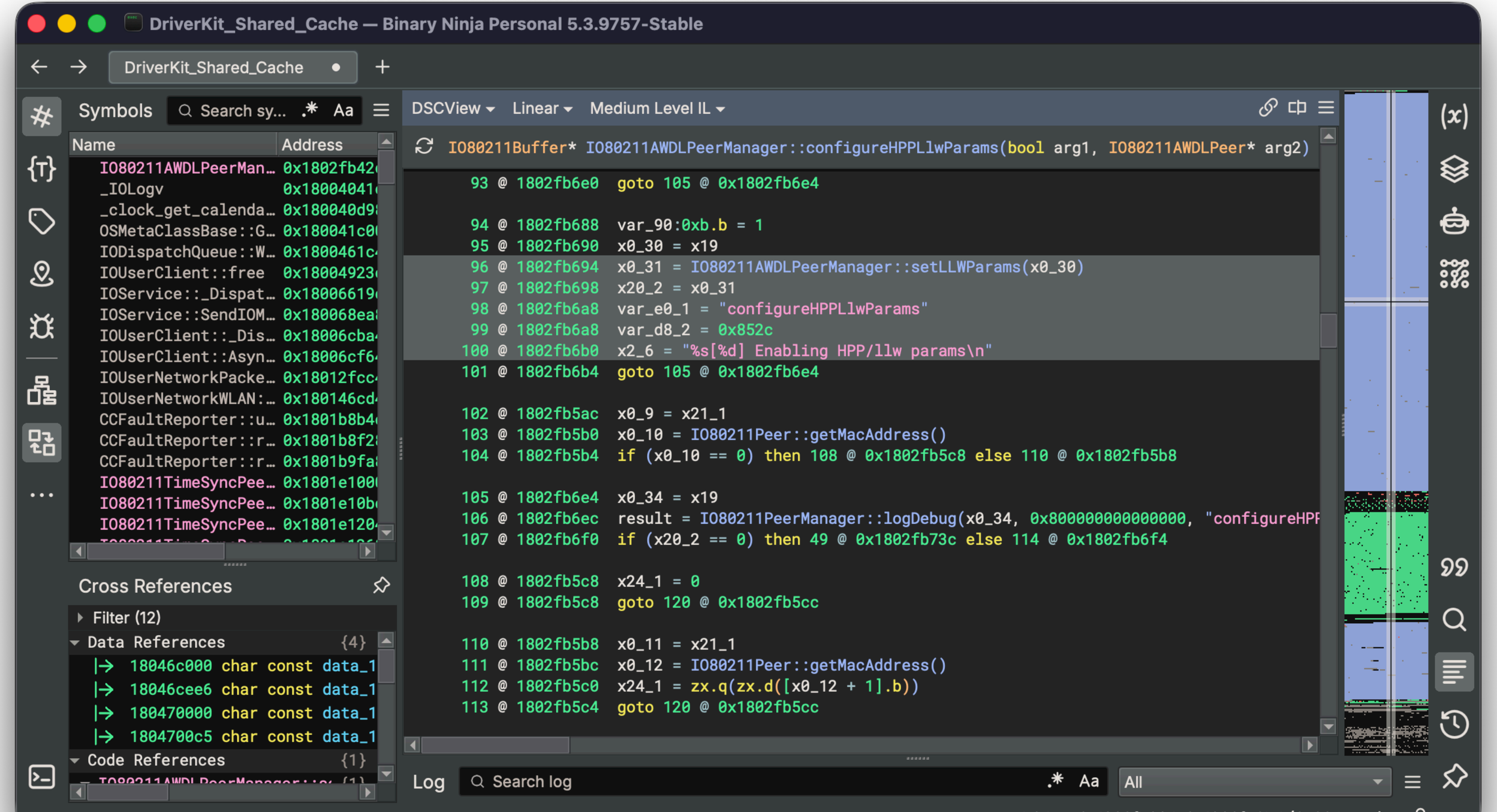

```
SK[%u]: %-30s kr "%s"
(0x%llx) right
acquired
```

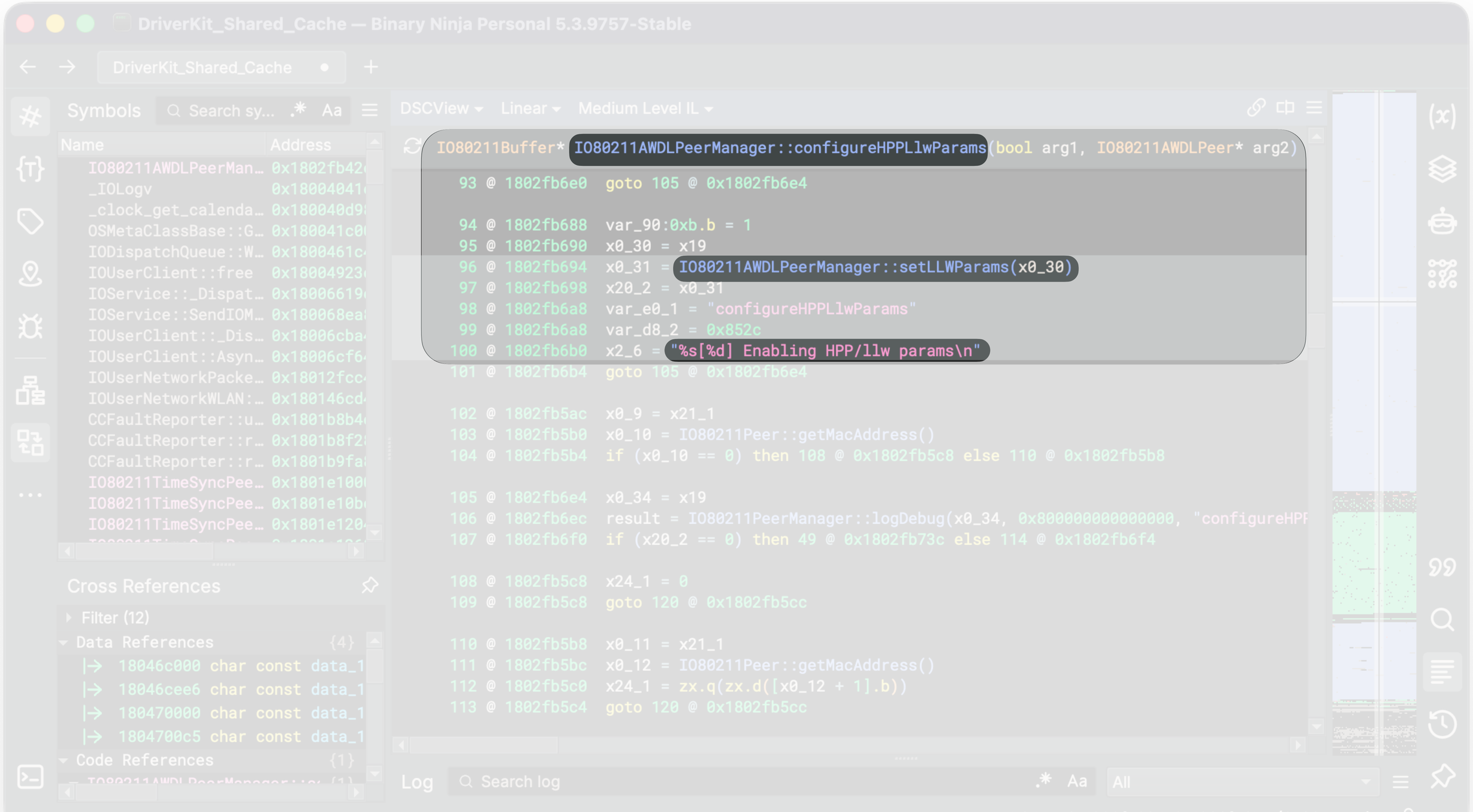
f-string

Event Message →  → Function

[19]


aggregated-1.pcapng
(frame contains "llw" or frame contains "tshark" or frame contains "tcpdump") and (not(frame contains "kernel.development"))
nmer Interface Info
com.apple.lokl… configureHPPLlwParams[34096] Enabling HPP/llw params
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34100] Disabling HPP/llw params |
logarchive-iPad KERN.ERR: 1 kernel (iPad) PID: log_collect wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [
logarchive-iPad USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect [C96 IPv6#5c591cee.59611 ready channel-flow (satisfied (Path
logarchive-iPad USER.ERR: 1 avconferenced (Network) (iPad) PID: log_collect nw_endpoint_flow_connected_path_change [C96 IPv6#5c591cee.596
ed (2160 bits) on interface logarchive-iPad, id 1
0:00:00_00:00:00 (00:00:00:00:00:00)
t wlan0:com.apple.p2p: configureHPPLlwParams[34096] Enabling HPP/llw params | [_io80211_os_log, IO80211AWDLPeerManager::configureAirPlayHPP, IO802
ms[34096] Enabling HPP/llw params | [_io80211_os_log, IO80211AWDLPeerManager::configureAirPlayHPP, IO80211AWDLPeerManager::configureHPPLlwParams]
Message (syslog.msg), 202 bytes
Packets: 33509804 · Displayed: 8578 (0.0%) · Marked: 2 (0.0%) · Comments: 33509804
Profile: Default


DriverKit_Shared_Cache — Binary Ninja Personal 5.3.9757-Stable
DriverKit_Shared_Cache
Symbols
Search sy...
Name
Address
IO80211AWDLPeerMan… 0x1802fb42
_IOLogv 0x18004041
_clock_get_calenda… 0x180040d9
OSMetaClassBase::G… 0x180041c0
IODispatchQueue::W… 0x1800461c
IOUserClient::free 0x18004923
IOService::_Dispat… 0x18006619
IOService::SendIOM… 0x180068ea
IOUserClient::_Dis… 0x18006cba
IOUserClient::Asyn… 0x18006cf6
IOUserNetworkPacke… 0x18012fcc
IOUserNetworkWLAN:… 0x180146cd
CCFaultReporter::u… 0x1801b8b4
CCFaultReporter::r… 0x1801b8f2
CCFaultReporter::r… 0x1801b9fa
IO80211TimeSyncPee… 0x1801e100
IO80211TimeSyncPee… 0x1801e10b
IO80211TimeSyncPee… 0x1801e120
Cross References
Filter (12)
Data References {4}
18046c000 char const data_1
18046cee6 char const data_1
180470000 char const data_1
1804700c5 char const data_1
Code References {1}
DSCView
Linear
Medium Level IL
IO80211Buffer* IO80211AWDLPeerManager::configureHPPLlwParams(bool arg1, IO80211AWDLPeer* arg2)
93 @ 1802fb6e0 goto 105 @ 0x1802fb6e4
94 @ 1802fb688 var_90:0xb.b = 1
95 @ 1802fb690 x0_30 = x19
96 @ 1802fb694 x0_31 = IO80211AWDLPeerManager::setLLWParams(x0_30)
97 @ 1802fb698 x20_2 = x0_31
98 @ 1802fb6a8 var_e0_1 = "configureHPPLlwParams"
99 @ 1802fb6a8 var_d8_2 = 0x852c
100 @ 1802fb6b0 x2_6 = "%s[%d] Enabling HPP/llw params\n"
101 @ 1802fb6b4 goto 105 @ 0x1802fb6e4
102 @ 1802fb5ac x0_9 = x21_1
103 @ 1802fb5b0 x0_10 = IO80211Peer::getMacAddress()
104 @ 1802fb5b4 if (x0_10 == 0) then 108 @ 0x1802fb5c8 else 110 @ 0x1802fb5b8
105 @ 1802fb6e4 x0_34 = x19
106 @ 1802fb6ec result = IO80211PeerManager::logDebug(x0_34, 0x800000000000000, "configureHPP
107 @ 1802fb6f0 if (x20_2 == 0) then 49 @ 0x1802fb73c else 114 @ 0x1802fb6f4
108 @ 1802fb5c8 x24_1 = 0
109 @ 1802fb5c8 goto 120 @ 0x1802fb5cc
110 @ 1802fb5b8 x0_11 = x21_1
111 @ 1802fb5bc x0_12 = IO80211Peer::getMacAddress()
112 @ 1802fb5c0 x24_1 = zx.q(zx.d([x0_12 + 1].b))
113 @ 1802fb5c4 goto 120 @ 0x1802fb5cc
Log
Search log
All


DriverKit_Shared_Cache — Binary Ninja Personal 5.3.9757-Stable
DriverKit_Shared_Cache
Symbols
Search sy...
Name
Address
IO80211AWDLPeerMan… 0x1802fb42
_IOLogv 0x18004041
_clock_get_calenda… 0x180040d9
OSMetaClassBase::G… 0x180041c0
IODispatchQueue::W… 0x1800461c
IOUserClient::free 0x18004923
IOService::_Dispat… 0x18006619
IOService::SendIOM… 0x180068ea
IOUserClient::_Dis… 0x18006cba
IOUserClient::Asyn… 0x18006cf6
IOUserNetworkPacke… 0x18012fcc
IOUserNetworkWLAN:… 0x180146cd
CCFaultReporter::u… 0x1801b8b4
CCFaultReporter::r… 0x1801b8f2
CCFaultReporter::r… 0x1801b9fa
IO80211TimeSyncPee… 0x1801e100
IO80211TimeSyncPee… 0x1801e10b
IO80211TimeSyncPee… 0x1801e120
Cross References
Filter (12)
Data References {4}
|-> 18046c000 char const data_1
|-> 18046cee6 char const data_1
|-> 180470000 char const data_1
|-> 1804700c5 char const data_1
Code References {1}
DSCView
Linear
Medium Level IL
IO80211Buffer* IO80211AWDLPeerManager::configureHPPLlwParams(bool arg1, IO80211AWDLPeer* arg2)
93 @ 1802fb6e0 goto 105 @ 0x1802fb6e4
94 @ 1802fb688 var_90:0xb.b = 1
95 @ 1802fb690 x0_30 = x19
96 @ 1802fb694 x0_31 = IO80211AWDLPeerManager::setLLWParams(x0_30)
97 @ 1802fb698 x20_2 = x0_31
98 @ 1802fb6a8 var_e0_1 = "configureHPPLlwParams"
99 @ 1802fb6a8 var_d8_2 = 0x852c
100 @ 1802fb6b0 x2_6 = "%s[%d] Enabling HPP/llw params\n"
101 @ 1802fb6b4 goto 105 @ 0x1802fb6e4
102 @ 1802fb5ac x0_9 = x21_1
103 @ 1802fb5b0 x0_10 = IO80211Peer::getMacAddress()
104 @ 1802fb5b4 if (x0_10 == 0) then 108 @ 0x1802fb5c8 else 110 @ 0x1802fb5b8
105 @ 1802fb6e4 x0_34 = x19
106 @ 1802fb6ec result = IO80211PeerManager::logDebug(x0_34, 0x800000000000000, "configureHPF
107 @ 1802fb6f0 if (x20_2 == 0) then 49 @ 0x1802fb73c else 114 @ 0x1802fb6f4
108 @ 1802fb5c8 x24_1 = 0
109 @ 1802fb5c8 goto 120 @ 0x1802fb5cc
110 @ 1802fb5b8 x0_11 = x21_1
111 @ 1802fb5bc x0_12 = IO80211Peer::getMacAddress()
112 @ 1802fb5c0 x24_1 = zx.q(zx.d([x0_12 + 1].b))
113 @ 1802fb5c4 goto 120 @ 0x1802fb5cc
Log
Search log
All

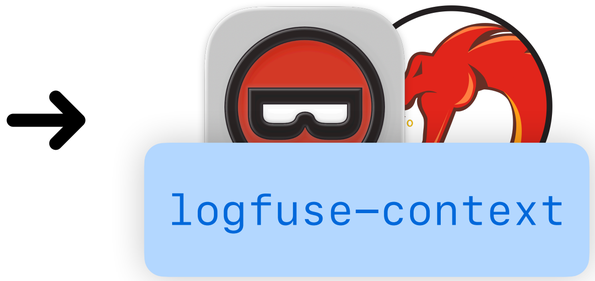
logfuse-context

Take a binary

Analyze

Map (f-)strings to functions

Tag traces with function names during aggregation



Take a binary

Analyze

Map (f-)strings to functions

Tag traces with function names during aggregation

```
⌥⌘1 -zsh
~/Doc/TROOPERS26/D/logfuse-context on git main !719 ?2 logfuse-context map-strings --backend=bn --interactive --config=logfuse-context.conf --output=string_mapping.json
```

DriverKit_Shared_Cache — Binary Ninja Personal 5.3.9757-Stable

DriverKit_Shared_Cache

Symbols llw

Name

- IO80211NANInfraManager::clearLLWStats
- IO80211NANInfraManager::getInfraAssocCountW
- IO80211NANInfraManager::getInfraDisassocCou
- IO80211NANInfraManager::getInfraScanCountWh
- IO80211NANDataPathSession::isNonSDBLLWSessi
- IO80211AWDLPeerManager::configureHPPLlwPara
- IO80211AWDLPeerManager::getLLWParams
- IO80211AWDLPeerManager::setLLWParams
- IO80211PeerManager::defaultLLWParams
- IO80211PeerManager::defaultVOLLWParams
- IO80211Peer::llwComputeTxConsecutiveErrorCo
- non-virtual_thunk_to_IO80211Peer::llwComput
- IO80211Peer::llwLoadPacketLifetimeHistogram
- non-virtual_thunk_to_IO80211Peer::llwLoadPa
- IO80211Controller::getLLWInterface

Cross References

Filter (9)

Code References {9}

- IO80211AWDLPeerManager::awdlChipRestor {1}
  - 1802ea080 bl IO80211AWDLPeerManag
- IO80211AWDLPeerManager::removePeerFrom {1}

DSCView DSCTriage

Images Symbols Mappings & Regions

80211

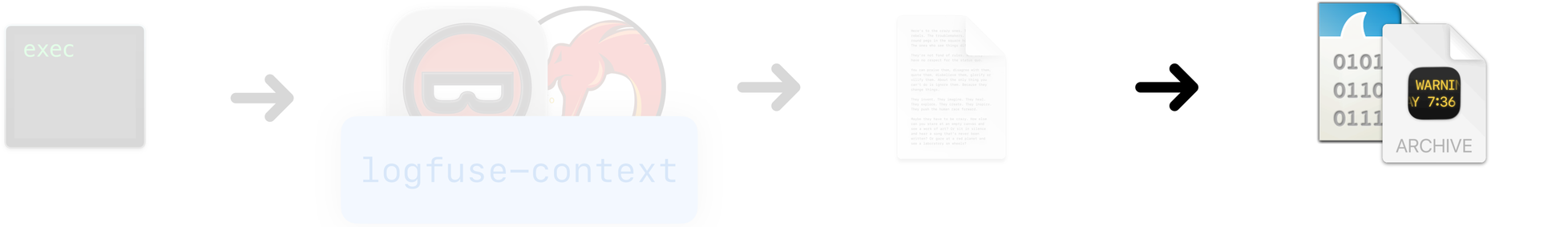
Address	Loaded	Name
0x1801dd000	✓	/System/DriverKit/System/Library/PrivateFrameworks/IO80211DriverKit.framework/…

Load Selected Refresh

Console Python

```
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
```

mac-aarch64 0x0



Take a binary

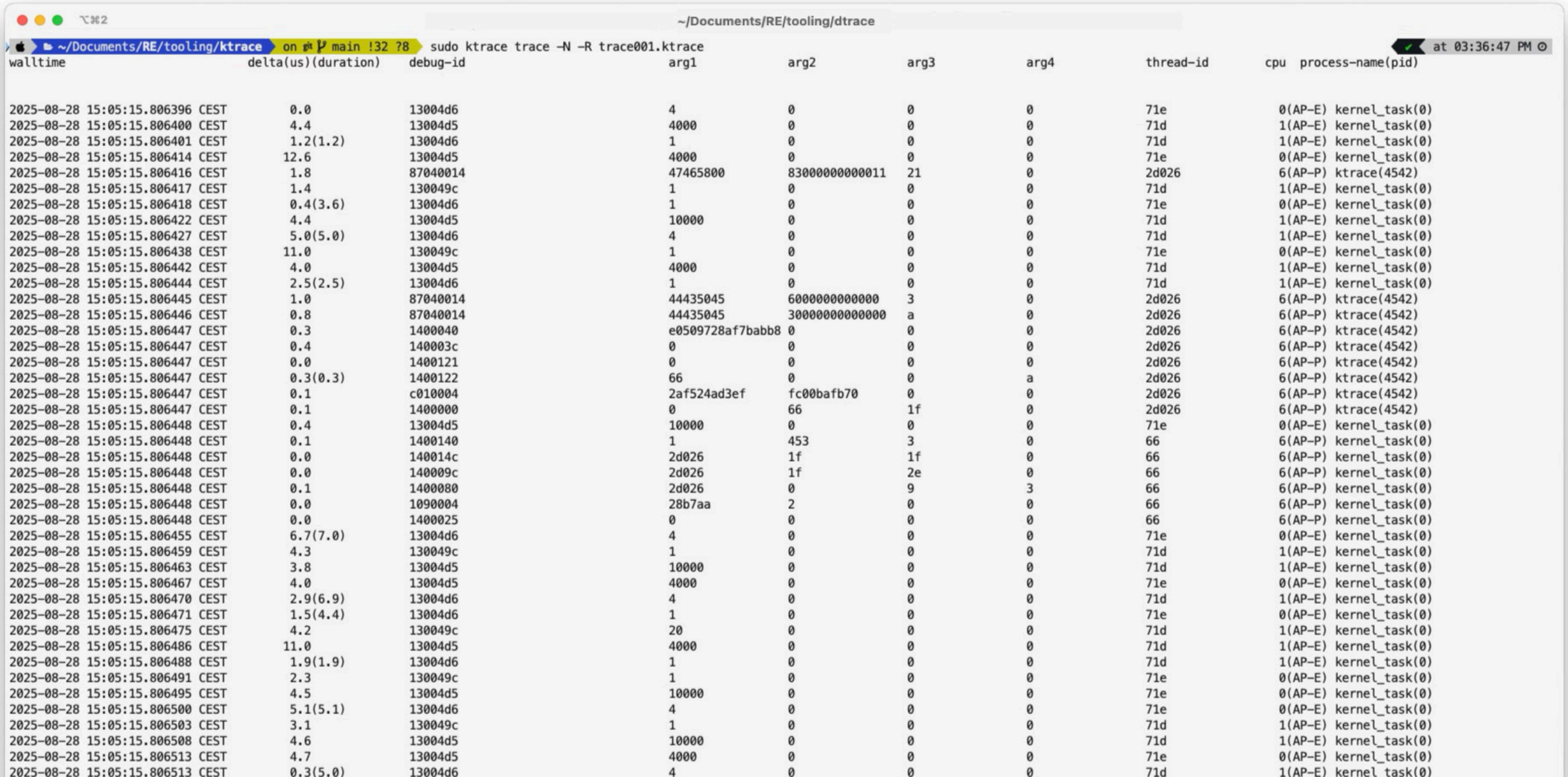
Analyze

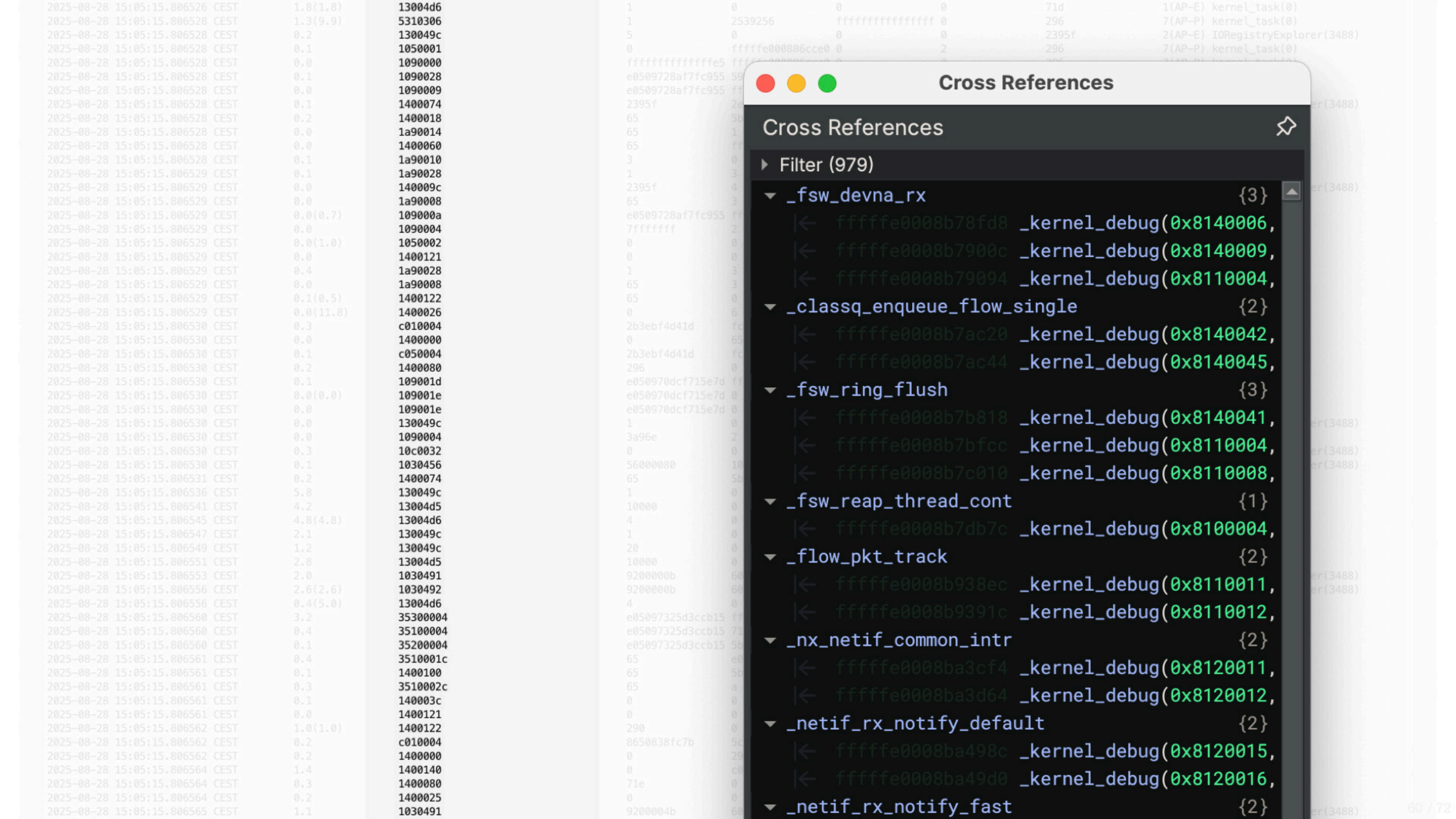
Map (f-)strings to functions

Tag logs with function names during aggregation

macOS	✅	✅	✅	✅	✅	✅
iOS	✅ `log`	✅ `tcpdump*`	✅	❌	✅ from source*	✅ reimplementation*

* Jailbreak required — our setup includes an iPad (7th generation)


~/Documents/RE/tooling/dtrace
~/Documents/RE/tooling/ktrace on main !32 ?8 sudo ktrace trace -N -R trace001.ktrace
at 03:36:47 PM
walltime delta(us)(duration) debug-id arg1 arg2 arg3 arg4 thread-id cpu process-name(pid)
2025-08-28 15:05:15.806396 CEST 0.0 13004d6 4 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806400 CEST 4.4 13004d5 4000 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806401 CEST 1.2(1.2) 13004d6 1 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806414 CEST 12.6 13004d5 4000 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806416 CEST 1.8 87040014 47465800 83000000000011 21 0 2d026 6(AP-P) ktrace(4542)
2025-08-28 15:05:15.806417 CEST 1.4 130049c 1 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806418 CEST 0.4(3.6) 13004d6 1 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806422 CEST 4.4 13004d5 10000 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806427 CEST 5.0(5.0) 13004d6 4 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806438 CEST 11.0 130049c 1 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806442 CEST 4.0 13004d5 4000 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806444 CEST 2.5(2.5) 13004d6 1 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806445 CEST 1.0 87040014 44435045 6000000000000 3 0 2d026 6(AP-P) ktrace(4542)
2025-08-28 15:05:15.806446 CEST 0.8 87040014 44435045 30000000000000 a 0 2d026 6(AP-P) ktrace(4542)
2025-08-28 15:05:15.806447 CEST 0.3 1400040 e0509728af7babb8 0 0 0 2d026 6(AP-P) ktrace(4542)
2025-08-28 15:05:15.806447 CEST 0.4 140003c 0 0 0 0 2d026 6(AP-P) ktrace(4542)
2025-08-28 15:05:15.806447 CEST 0.0 1400121 0 0 0 0 2d026 6(AP-P) ktrace(4542)
2025-08-28 15:05:15.806447 CEST 0.3(0.3) 1400122 66 0 0 a 2d026 6(AP-P) ktrace(4542)
2025-08-28 15:05:15.806447 CEST 0.1 c010004 2af524ad3ef fc00bafb70 0 0 2d026 6(AP-P) ktrace(4542)
2025-08-28 15:05:15.806447 CEST 0.1 1400000 0 66 1f 0 2d026 6(AP-P) ktrace(4542)
2025-08-28 15:05:15.806448 CEST 0.4 13004d5 10000 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806448 CEST 0.1 1400140 1 453 3 0 66 6(AP-P) kernel_task(0)
2025-08-28 15:05:15.806448 CEST 0.0 140014c 2d026 1f 1f 0 66 6(AP-P) kernel_task(0)
2025-08-28 15:05:15.806448 CEST 0.0 140009c 2d026 1f 2e 0 66 6(AP-P) kernel_task(0)
2025-08-28 15:05:15.806448 CEST 0.1 1400080 2d026 0 9 3 66 6(AP-P) kernel_task(0)
2025-08-28 15:05:15.806448 CEST 0.0 1090004 28b7aa 2 0 0 66 6(AP-P) kernel_task(0)
2025-08-28 15:05:15.806448 CEST 0.0 1400025 0 0 0 0 66 6(AP-P) kernel_task(0)
2025-08-28 15:05:15.806455 CEST 6.7(7.0) 13004d6 4 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806459 CEST 4.3 130049c 1 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806463 CEST 3.8 13004d5 10000 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806467 CEST 4.0 13004d5 4000 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806470 CEST 2.9(6.9) 13004d6 4 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806471 CEST 1.5(4.4) 13004d6 1 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806475 CEST 4.2 130049c 20 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806486 CEST 11.0 13004d5 4000 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806488 CEST 1.9(1.9) 13004d6 1 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806491 CEST 2.3 130049c 1 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806495 CEST 4.5 13004d5 10000 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806500 CEST 5.1(5.1) 13004d6 4 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806503 CEST 3.1 130049c 1 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806508 CEST 4.6 13004d5 10000 0 0 0 71d 1(AP-E) kernel_task(0)
2025-08-28 15:05:15.806513 CEST 4.7 13004d5 4000 0 0 0 71e 0(AP-E) kernel_task(0)
2025-08-28 15:05:15.806513 CEST 0.3(5.0) 13004d6 4 0 0 0 71d 1(AP-E) kernel_task(0)


Cross References
Cross References
Filter (979)
_fsw_devna_rx {3}
ffffffe0008b78fd8 _kernel_debug(0x8140006,
ffffffe0008b7900c _kernel_debug(0x8140009,
ffffffe0008b79094 _kernel_debug(0x8110004,
_classq_enqueue_flow_single {2}
ffffffe0008b7ac20 _kernel_debug(0x8140042,
ffffffe0008b7ac44 _kernel_debug(0x8140045,
_fsw_ring_flush {3}
ffffffe0008b7b818 _kernel_debug(0x8140041,
ffffffe0008b7bfcc _kernel_debug(0x8110004,
ffffffe0008b7c010 _kernel_debug(0x8110008,
_fsw_reap_thread_cont {1}
ffffffe0008b7db7c _kernel_debug(0x8100004,
_flow_pkt_track {2}
ffffffe0008b938ec _kernel_debug(0x8110011,
ffffffe0008b9391c _kernel_debug(0x8110012,
_nx_netif_common_intr {2}
ffffffe0008ba3cf4 _kernel_debug(0x8120011,
ffffffe0008ba3d64 _kernel_debug(0x8120012,
_netif_rx_notify_default {2}
ffffffe0008ba498c _kernel_debug(0x8120015,
ffffffe0008ba49d0 _kernel_debug(0x8120016,
_netif_rx_notify_fast {2}

debug identifiers are somewhat unique

```
__kernel_debug(0x40c0800)
```

```
someFunction()
```

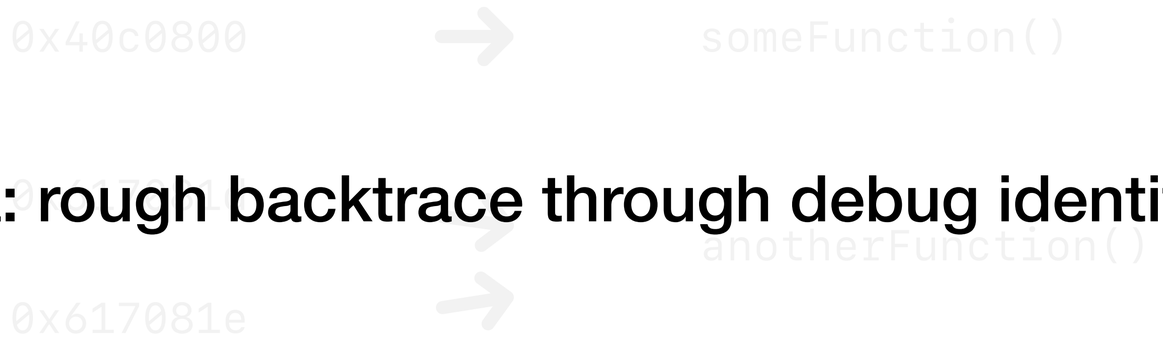
```
__kernel_debug(0x617081d)
```

```
anotherFunction()
```

```
__kernel_debug(0x617081e)
```

...

debug identifiers are somewhat unique



Idea: rough backtrace through debug identifiers

logfuse-context

Take a kernel(cache)

Analyze

Map debug-ids to kernel functions

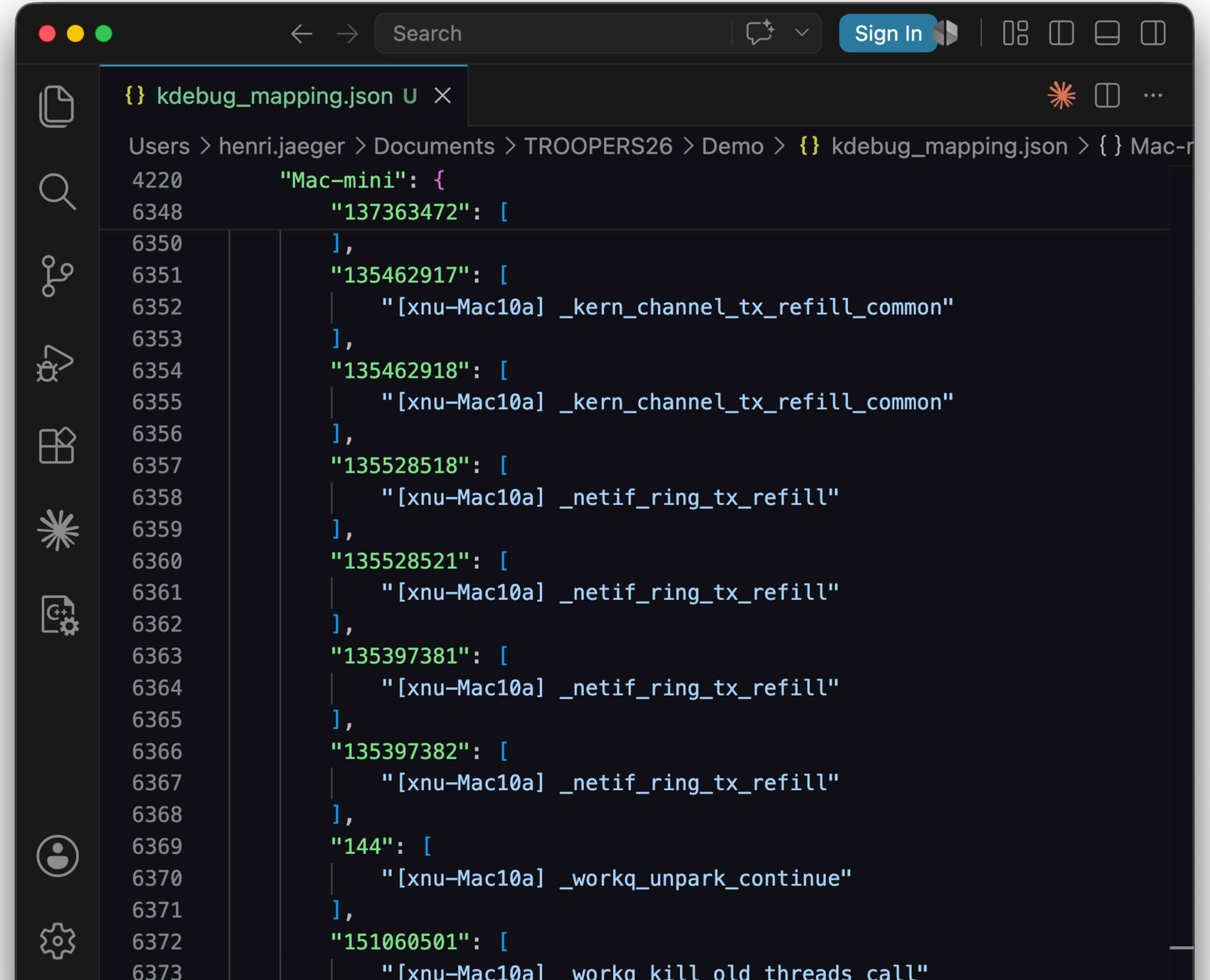
Tag traces with function names during aggregation

Take a kernel(cache)

Analyze

Map debug-ids to kernel functions

Tag traces with function names during aggregation


Search
Sign In
{} kdebug_mapping.json U
Users > henri.jaeger > Documents > TROOPERS26 > Demo > {} kdebug_mapping.json > { } Mac-r
4220 "Mac-mini": {
6348 "137363472": [
6350],
6351 "135462917": [
6352 "[xnu-Mac10a] _kern_channel_tx_refill_common"
6353],
6354 "135462918": [
6355 "[xnu-Mac10a] _kern_channel_tx_refill_common"
6356],
6357 "135528518": [
6358 "[xnu-Mac10a] _netif_ring_tx_refill"
6359],
6360 "135528521": [
6361 "[xnu-Mac10a] _netif_ring_tx_refill"
6362],
6363 "135397381": [
6364 "[xnu-Mac10a] _netif_ring_tx_refill"
6365],
6366 "135397382": [
6367 "[xnu-Mac10a] _netif_ring_tx_refill"
6368],
6369 "144": [
6370 "[xnu-Mac10a] _workq_unpark_continue"
6371],
6372 "151060501": [

Take a kernel(cache)

Analyze

Map debug-ids to kernel functions

Tag traces with function names during aggregation

Backtrace Reconstruction

logfuse-toolkit

Multi-Device Support

k trace

Support on iOS

cc tool

Support on iOS

Log Aggregation Toolkit

.pcap .json .pcapng

Support for 6+ Input Formats

custom output .pklg .txt

Clock Offset Correction

Milestone Markers

Noise Filtering

Support for logarchive Output

Support for pcapng Output

Extensible to More Tracing Tools

Stability Improvements

Backtrace Reconstruction

Setup Enhancements

Available

This Week

Available

This Week

henrijaeger/logfuse-toolkit

Funding provided by

Thoughts?

henri.jaeger@hpi.de

Special thanks to the NLnet Foundation.

Literature

[A] https://github.com/seemoo-lab/opendrop (visited on 24/06/2026)

[B] https://github.com/seemoo-lab/watchwitch (visited on 24/06/2026)

[C] https://github.com/seemoo-lab/openhaystack (visited on 24/06/2026)

[D] Inga Susanna Dischinger. Security Analysis of Apple's Continuity Camera for iPhone. Technische Universität Darmstadt, October 30, 2023

[E] Jan Dominik Röper. Sicherheitsanalyse von Apple's Sidecar-Protokoll. Technische Universität Darmstadt, August 02, 2023

[F] https://media.ccc.de/v/39c3-cracking-open-what-makes-apple-s-low-latency-wifi-so-fast (visited on 24/06/2026)

Figures

[1] https://de.wikipedia.org/wiki/Universität_Potsdam#/media/Datei:Universität_Potsdam_logo.svg (visited on 24/06/2026)

[2] https://upload.wikimedia.org/wikipedia/commons/thumb/f/f2/Hasso-Plattner-Institut_logo.svg/1920px-Hasso-Plattner-Institut_logo.svg.png (visited on 24/06/2026)

[3] https://web.archive.org/web/20250904210947/https://de.wikipedia.org/wiki/AirDrop#/media/Datei:AirDrop_logo.svg (visited on 24/06/2026)

[4] https://www.apple.com/newsroom/images/live-action/wwdc-2023/standard/watchos-10/Apple-WWDC23-watchOS-10-new-Watch-faces-Palette-Iris-230605_inline.jpg.large.jpg (visited on 24/06/2026)

[5] https://en.wikipedia.org/wiki/Find_My#/media/File:Find_My_logo.svg (visited on 24/06/2026)

[6] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/studio-display-gallery-1-202203?wid=640&hei=528&fmt=p-jpg&qlt=95 (visited on 24/06/2026)

[7] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/mac-mini-select-202410?wid=904&hei=840&fmt=jpeg&qlt=90&.v=WG0zcWo4VEd2YnZ3WTlBVlBwSHNCUnZ0SFlIdzZrSzBMWjRQMnF1U2Y2enZhWUNqTDdqTGdxV2EvMEFJcW1vNDg0SERaYTF4eEZ1aW9ZbGpONkszSXRhaHNubVVXOWRtVW4zMGQxeFF6U00 (visited on 24/06/2026)

[8] https://upload.wikimedia.org/wikipedia/commons/thumb/d/d2/IPad_10.2-inch.png/1280px-IPad_10.2-inch.png (visited on 24/06/2026)

Figures

[9] https://cdsassets.apple.com/live/SZLF0YNV/images/sp/111911_sp807-ipad-7th-gen.png (visited on 24/06/2026)

[10] https://cdsassets.apple.com/live/7WUAS350/images/macos/ventura/macos-ventura-macbook-pro-iphone-13-pro-continuity-camera-desk-view-hero.png (visited on 24/06/2026)

[11] https://istore.co.na/cdn/shop/files/iPhone_15_Pro_White_Titanium_PDP_Image_Position-8__WWEN_76d79726-ff49-4320-ab7b-316723a4ab0d_5000x.jpg?v=1707992983 (visited 24/06/2026)
[12] https://drive.google.com/file/d/1QvLTWECNhQpd10llW1nz8nUTKvFup_jk/view (visited on 24/06/2026)

[13] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/MXK53_AV1?wid=1144&hei=1144&fmt=jpeg&qlt=90&.v=QytENXB3MzdYRFA4RU1McS9kQ1d6VlZya2lKWlJmUEwrYndWOTJiVWJWQUYwVmtIbGRkS25RMVpBRlo0bk5DUStteWFnS2JDbkxFb1JqRG5KS1RPUWc (visited on 24/06/2026)

[14] https://store.storeimages.cdn-apple.com/1/as-images.apple.com/is/MXCL3D?wid=1144&hei=1144&fmt=jpeg&qlt=90&.v=MWhTMGgwN3h3cm1YQ0hHelVYWWZ2RExJNzJtbW9WRzBUckZ4SDR0aldyMFY0ZGtxRm5nMGhUUUYyQ1NONFVVUnBSYmQxNkhWTGV4d1BxVjd4aUJPSGc (visited on 24/06/2026)

Figures

[15] https://upload.wikimedia.org/wikipedia/commons/thumb/1/1d/Splunk_logo.svg/1280px-Splunk_logo.svg.png (visited on 24/06/2026)

[16] https://miro.medium.com/v2/resize:fit:4800/format:webp/1*vZDu4Bwj2GxQh8t1IjDq4w.png (visited on 24/06/2026)

[17] https://grafana.com/docs/loki/latest/ (visited on 24/06/2026)

[18] https://upload.wikimedia.org/wikipedia/commons/thumb/3/3b/Grafana_icon.svg/960px-Grafana_icon.svg.png?_=20230113182558 (visited on 24/06/2026)

[19] https://en.wikipedia.org/wiki/Ghidra#/media/File:Ghidra_logo.svg (visited on 24/06/2026)

[20] https://img.freepik.com/free-photo/grunge-wall-texture_1194-6371.jpg?t=st=1764838379~exp=1764841979~hmac=9cbca8804f3cd7de594b4b763122a01b62f23463ffc73b72ead16e1a0ce18e63&w=2000 (visited on 24/06/2026)

[21] https://upload.wikimedia.org/wikipedia/commons/4/4e/Codeberg_Logo.svg (visited on 24/06/2026)