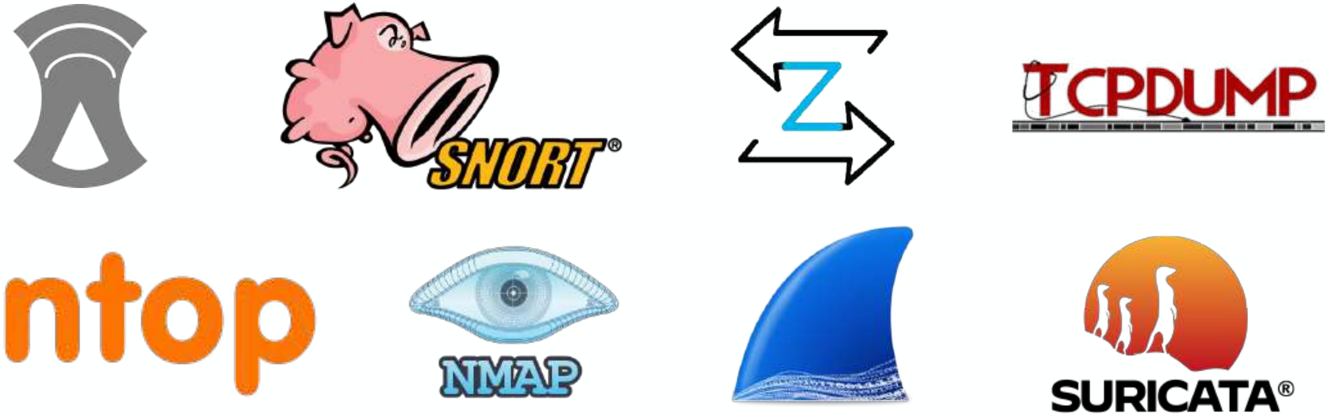
SharkFest'24 US
June 15-20 · Fairfax, VA

Ecosystem Expansion

Gerald Combs
Core Developers

What Do All Of These Have In Common?



If your favorite isn’t here, I ran out of space for logos. Sorry.

What Do All Of These Have In Common?

SNORT®
TCPDUMP
Z
ntop
NMAP
SURICATA®
LiBPCAP
WinPcap
Npcap

Libpcap + .pcap + .pcapng

Lets application developers focus on features

Capture anywhere (with WinPcap/Npcap)

Common file format is a productivity multiplier

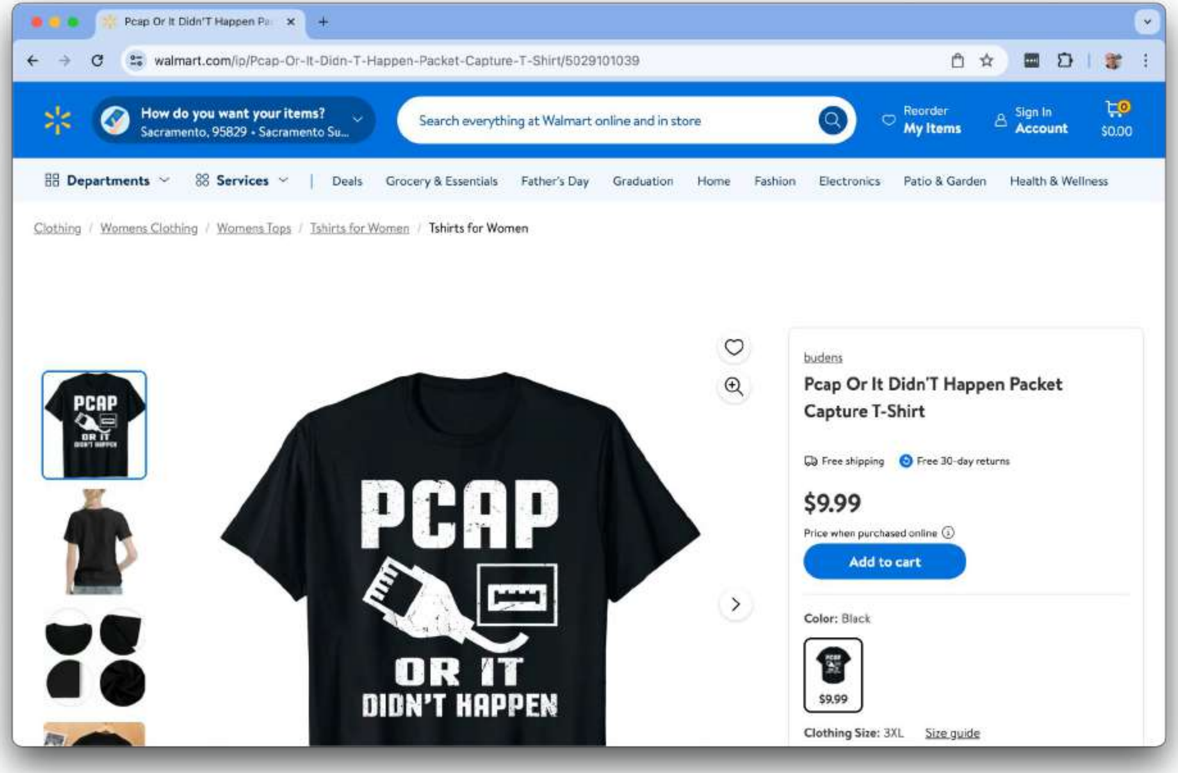
Why Packets?

They're *truthful*, *accessible*, and *reliable*.

Zeitgeisty

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

Zeitgeistier


Pcap Or It Didn'T Happen Pa
walmart.com/ip/Pcap-Or-It-Didn-T-Happen-Packet-Capture-T-Shirt/5029101039
How do you want your items?
Sacramento, 95829 · Sacramento Su...
Search everything at Walmart online and in store
Reorder
My Items
Sign In
Account
0
$0.00
Departments
Services
Deals
Grocery & Essentials
Father's Day
Graduation
Home
Fashion
Electronics
Patio & Garden
Health & Wellness
Clothing / Womens Clothing / Womens Tops / Tshirts for Women / Tshirts for Women
PCAP
OR IT
DIDN'T HAPPEN
Add to cart
Size guide

budens

Pcap Or It Didn'T Happen Packet Capture T-Shirt

Free shipping · Free 30-day returns

$9.99

Price when purchased online

Color: Black

$9.99

Clothing Size: 3XL

https://www.walmart.com/ip/Pcap-Or-It-Didn-T-Happen-Packet-Capture-T-Shirt/5029101039

This Works Great!

Having a common library and file formats works really well.

What other sources of truth are available?

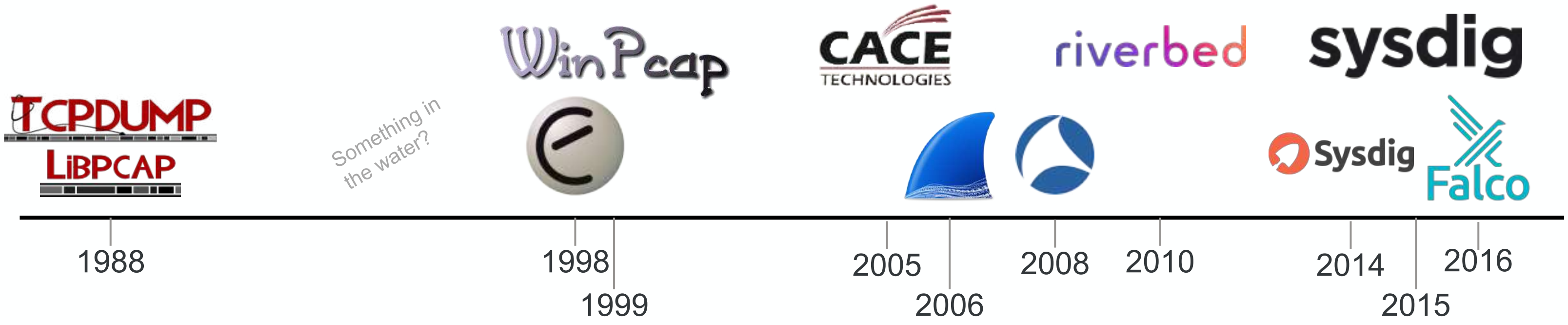
This Works Great!

Having a common library and file formats works really well.

What other sources of truth are available?

What about system calls and logs?

Story Time



Something in the water?

1988

1998

1999

2005

2006

2008

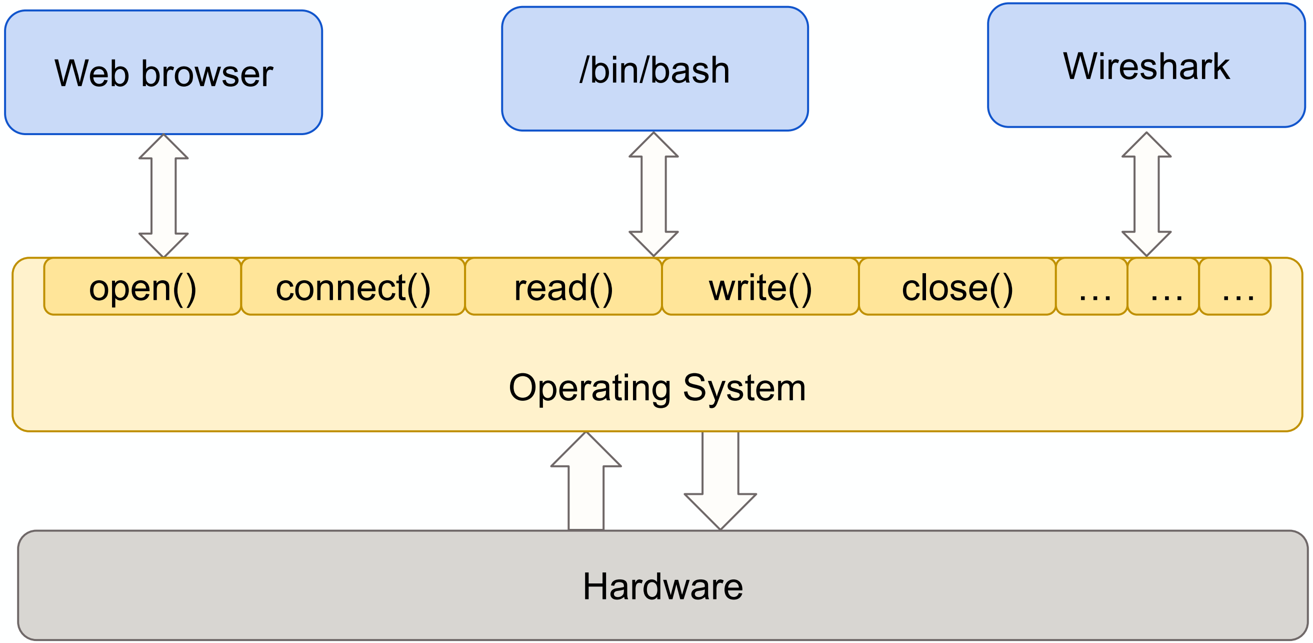
2010

2014

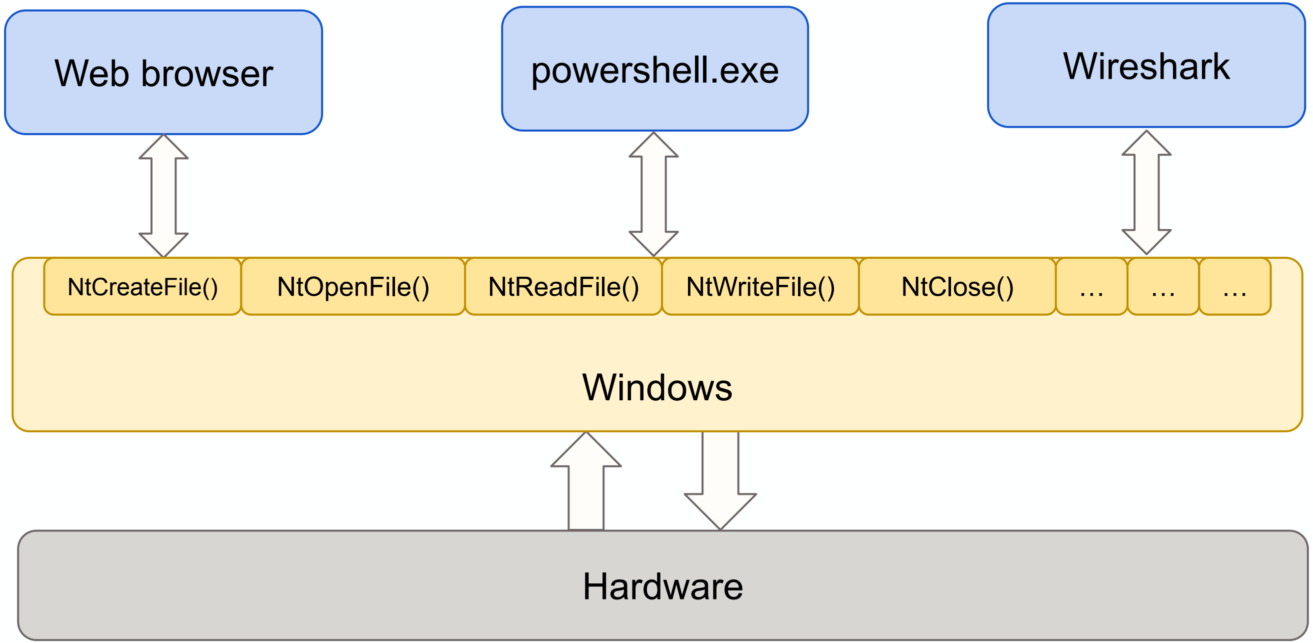
2015

2016

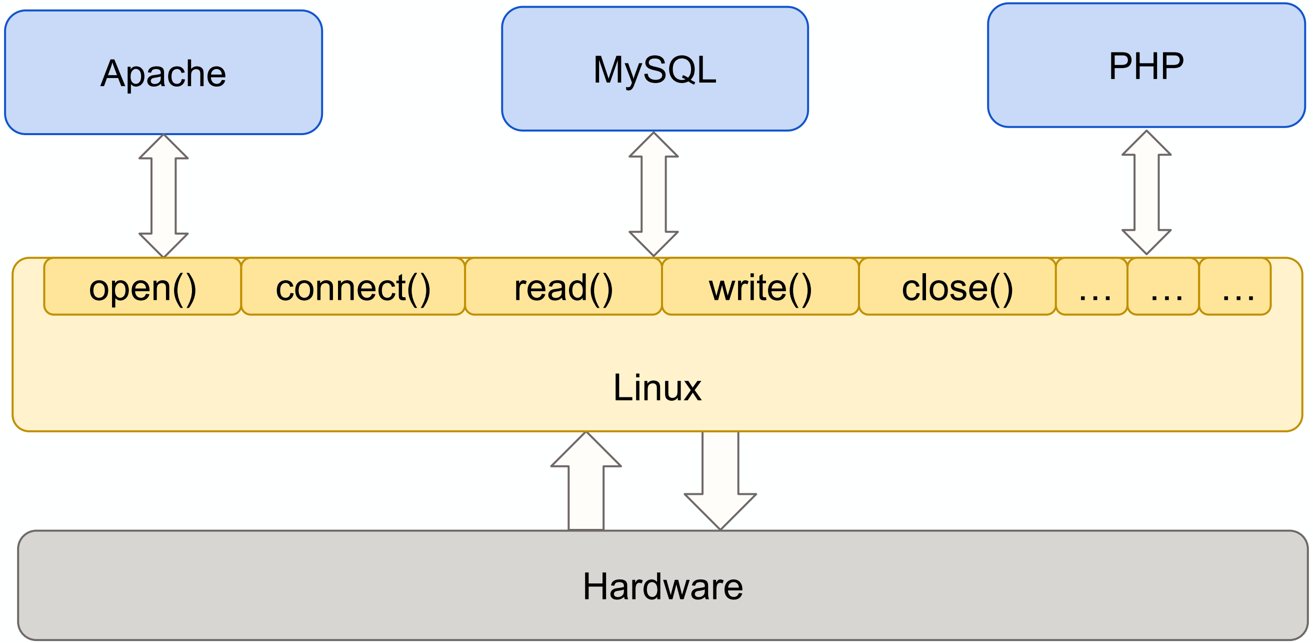
System Calls



System Calls

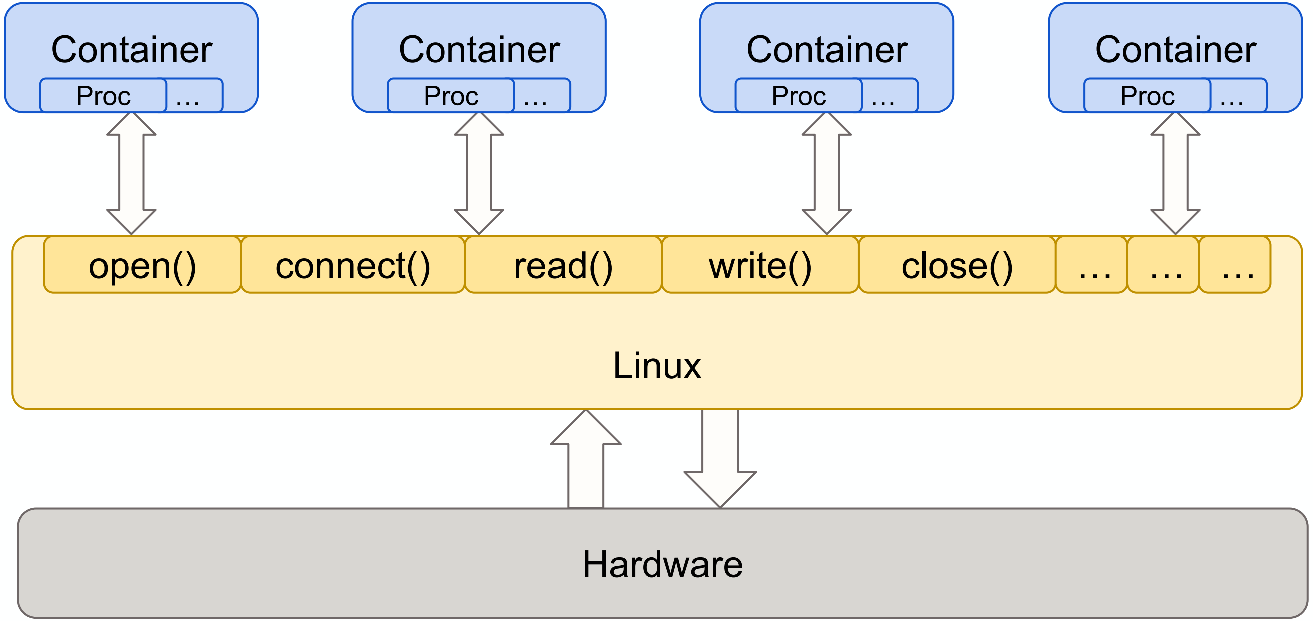


Ye Olde LAMP Stack

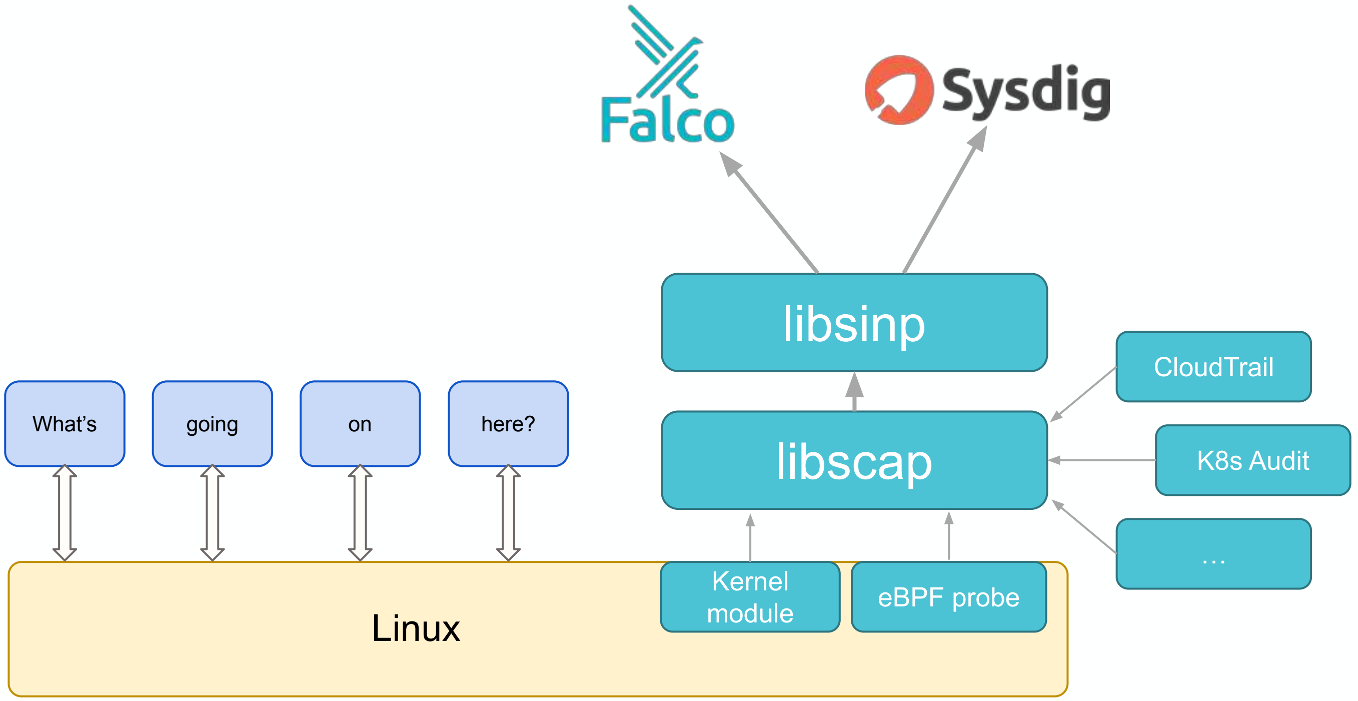


Present Day

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us

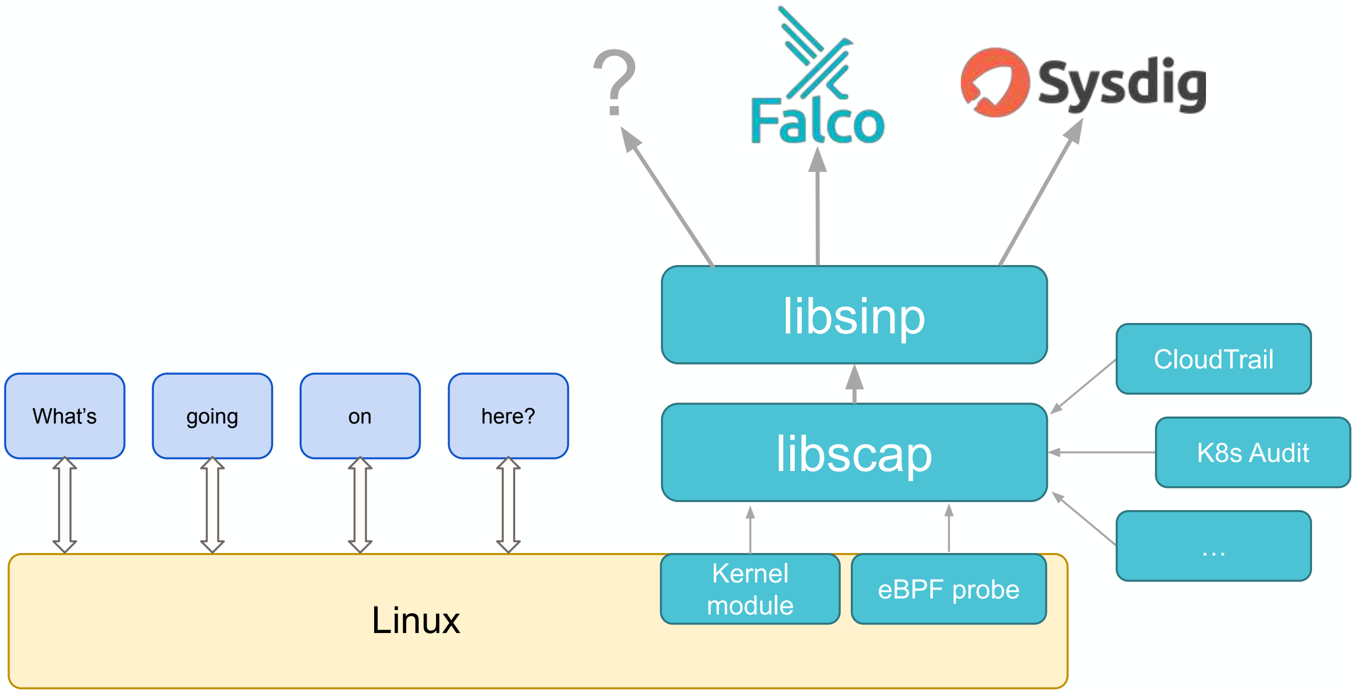


libscap + libsinsp

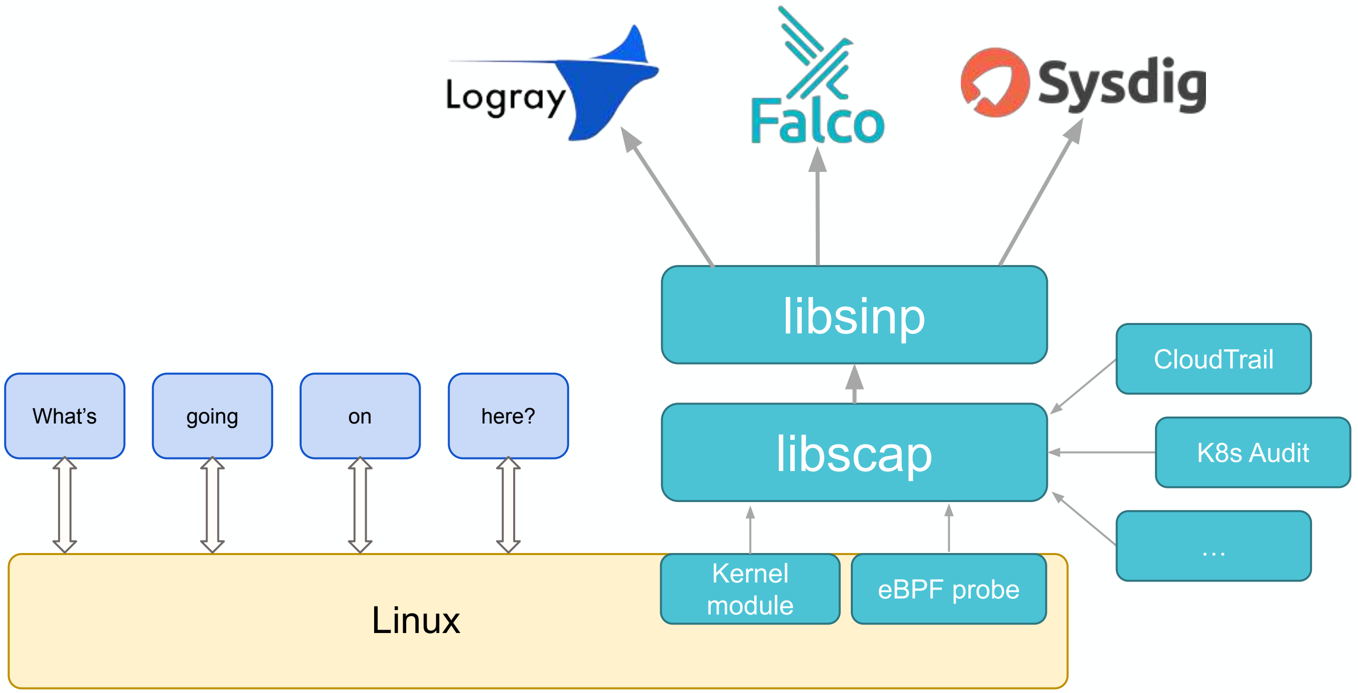


https://github.com/falcosecurity/libs

libscap + libsinsp



libscap + libsinsp



Demo Time[1]

[1] May contain traces of danger and stupidity

Expectation Management

This is in addition to, and not instead of, Wireshark

Rough in the sense that there’s still lots to fill in and smooth out

The slate is intentionally blank

When?

Officially? Soon.

Technically? Now.

The State of Wireshark

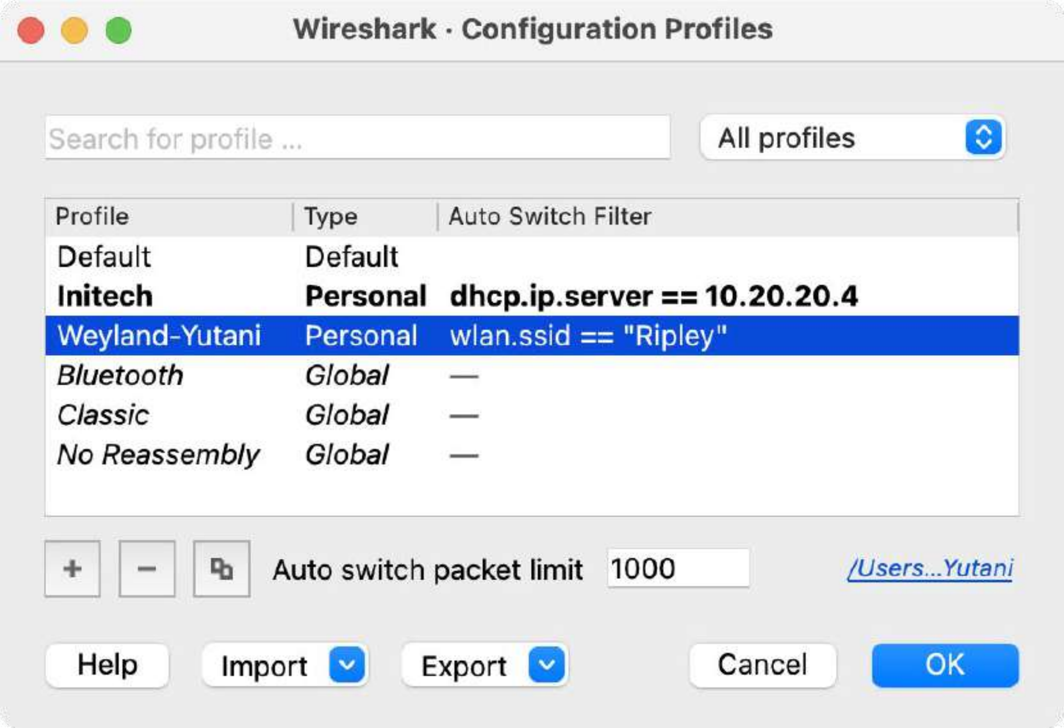
Next major release this summer?

Updates:

- Automatic profile switching
- Lua 5.3 / 5.4
- Display filter, I/O graph, Sequence Diagram, TCP Stream Graph
- More custom column support

Automatic Profile Switching

SharkFest'24 US
June 15-20 · Fairfax, VA
#sf24us



Wireshark · Configuration Profiles

Profile	Type	Auto Switch Filter
Default	Default	
Initech	**Personal**	**dhcp.ip.server == 10.20.20.4**
Weyland-Yutani	Personal	wlan.ssid == "Ripley"
Bluetooth	*Global*	—
Classic	*Global*	—
No Reassembly	*Global*	—

Auto switch packet limit 1000

/Users...Yutani

Vital Statistics

~ 1.5M Downloads / month …on the servers we manage

~83% Windows, ~16% macOS …again, on the servers we manage

3000 protocols, 250k fields

> 2300 authors

> 4100 Discord users

3.4M lines of code. Or maybe 6.2?

The State of the Foundation

Steering committee is now official

Platinum members: Endace, LiveAction

Silver members: Veeam, Npcap

How You Can Help

Good: Donate at wiresharkfoundation.org

Better: Set up a recurring donation

Best: Get your employer to match donations or become a member

Developer Time

Thank You

Links

Automated builds

https://www.wireshark.org/download/automated

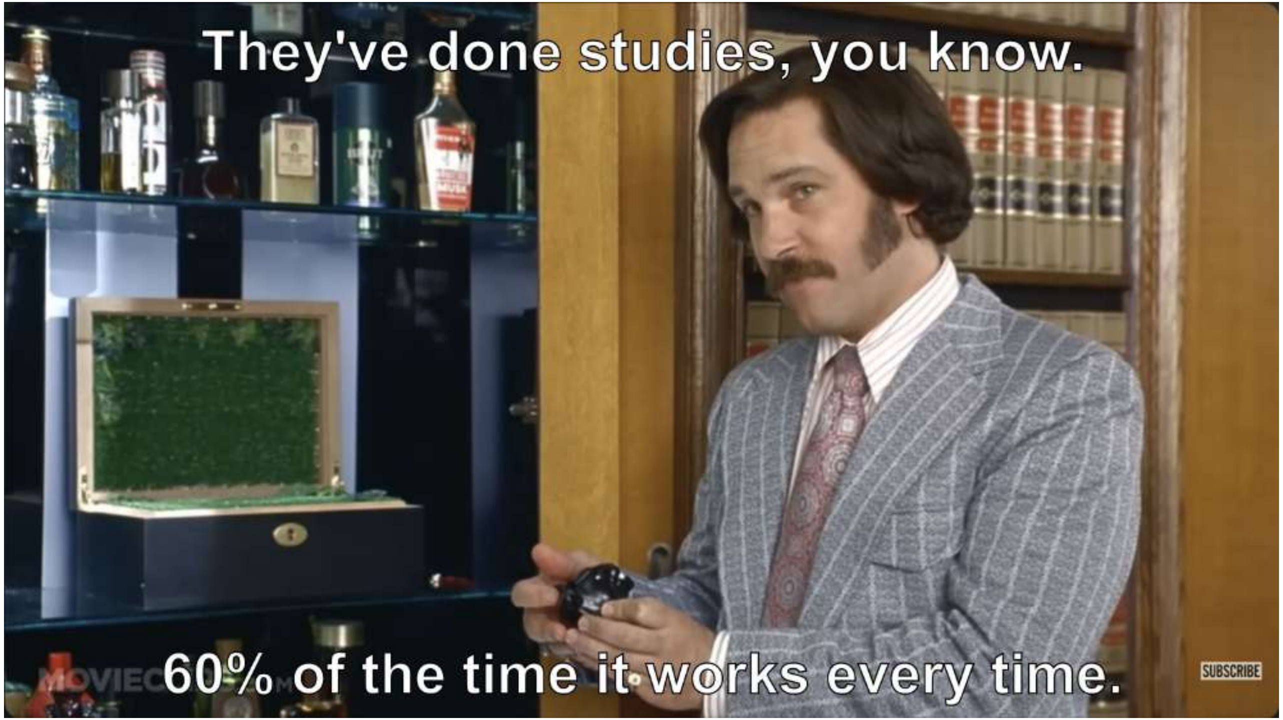
event-extras.lua

https://gist.github.com/geraldcombs/d7d541af18890750f1a4197e406e7cf9

Linux system calls

https://filippo.io/linux-syscall-table/

Bonus Slides



They've done studies, you know.
60% of the time it works every time.
MOVIECLIPS
SUBSCRIBE