



# 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.

# They're Part Of An Ecosystem

SharkFest'24 EUROPE

Vienna, Austria ■ #sf24eu



ntop



SNORT



TCPDUMP



SURICATA

**LIBPCAP**

WinPcap

Npcap



Lets application developers focus on features

Capture anywhere (with WinPcap/Npcap)

Common file format is a productivity multiplier



Having a common library and file formats works really well.

Where can we duplicate this success?



Having a common library and file formats works really well.

Where can we duplicate this success?

System calls

Logs

Whatever erupts from your fevered imagination



We need to...

...literally fix  
the internet



1988

...monitor, scan,  
detect & analyze  
packets



1994

...capture on  
Windows

WinPcap



1998

... capture 802.11  
on Windows



2006

...have cloud  
visibility



2014



2016





.pcap era

.pcapng era

.scap era



1988

Something in the water?

WinPcap



1998

1999

CACE  
TECHNOLOGIES



2005

2006



2008

riverbed

2010

sysdig



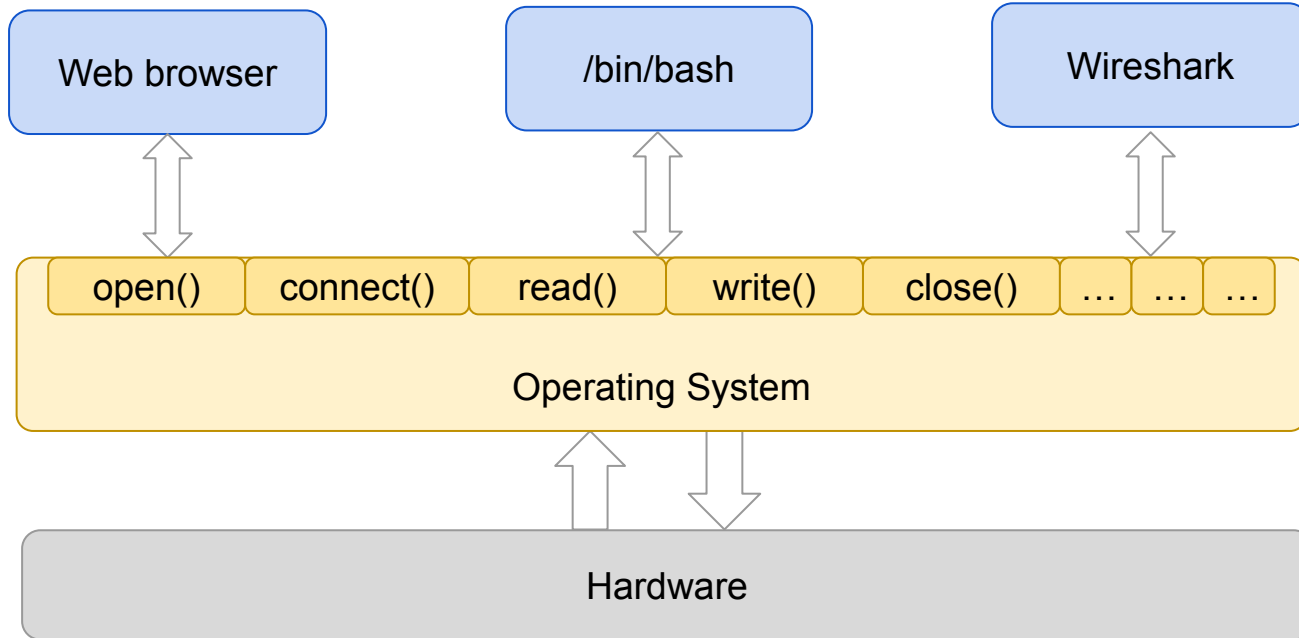
2014

2015

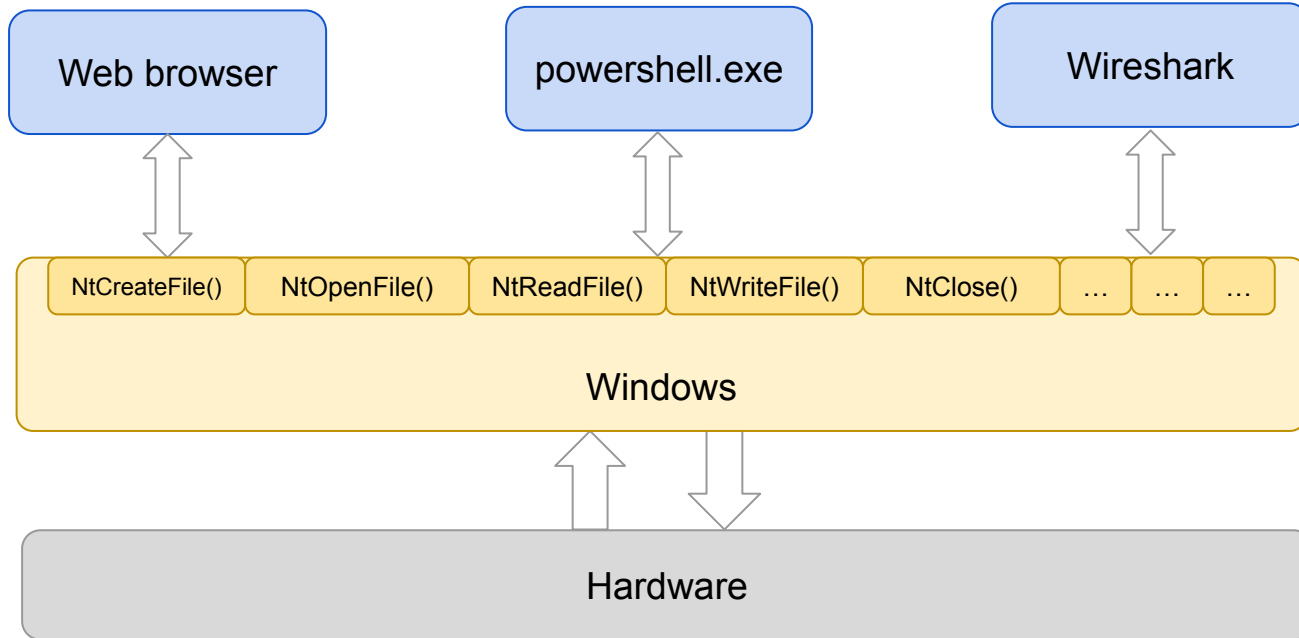


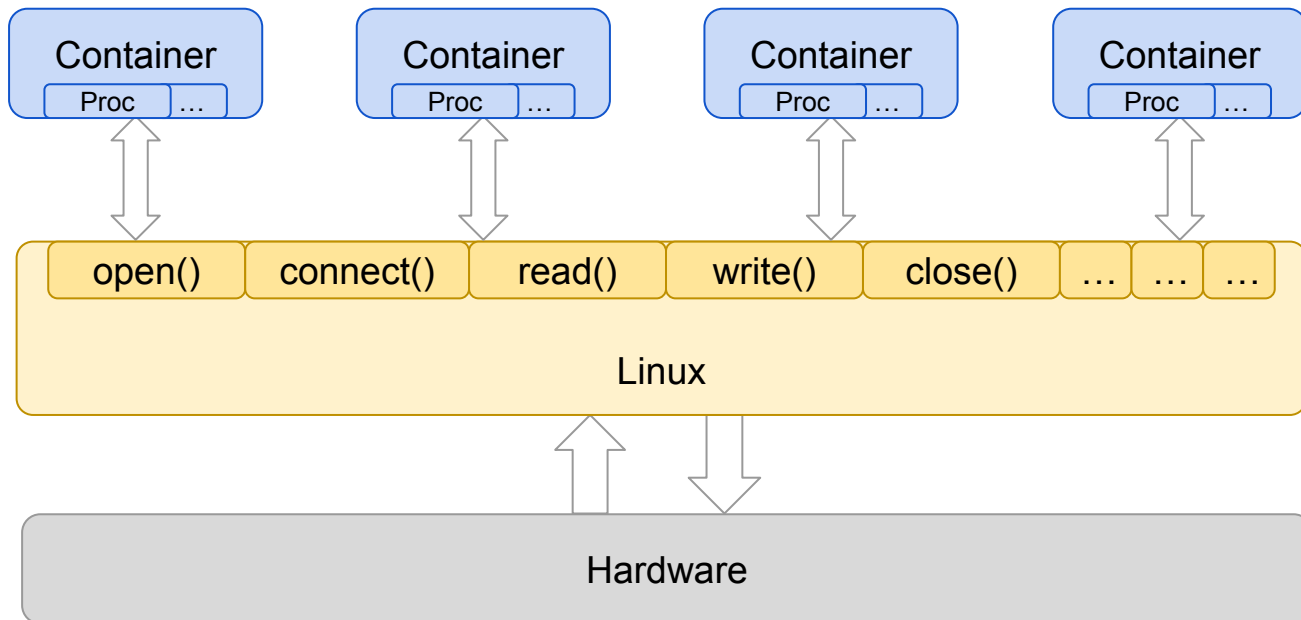
2016

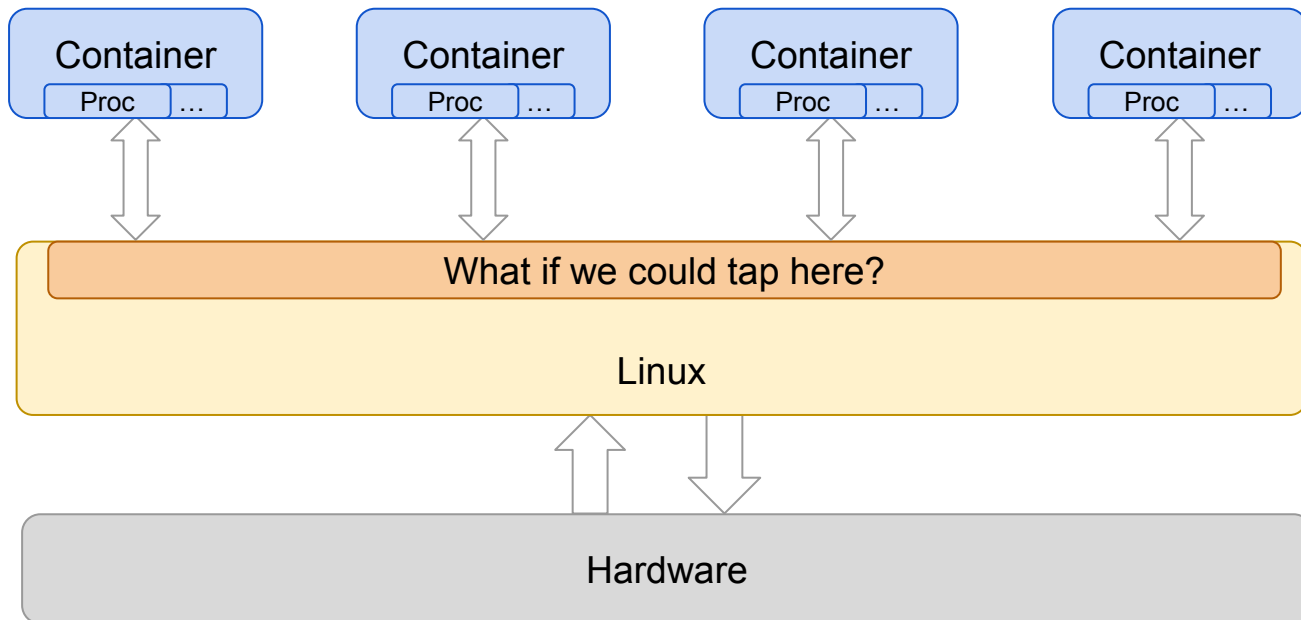


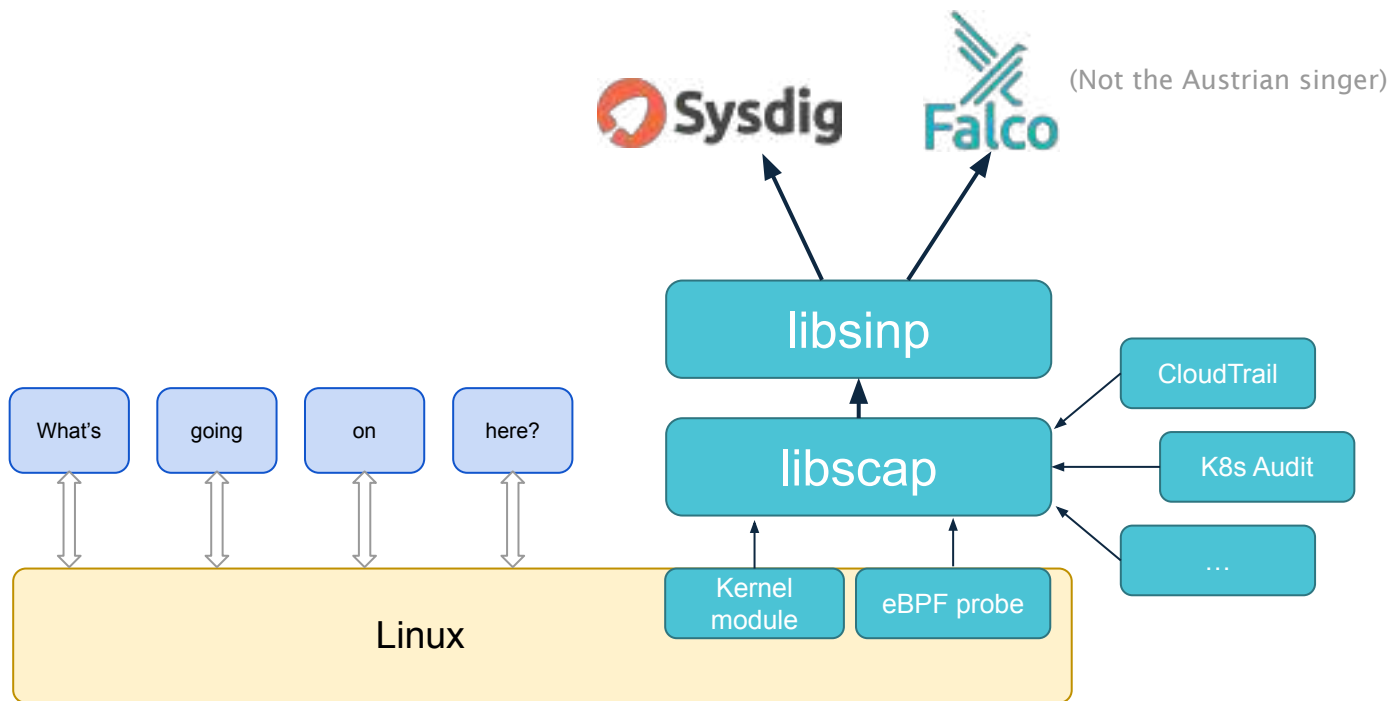


Have you ever read man pages on Linux or macOS? System calls are section 2!

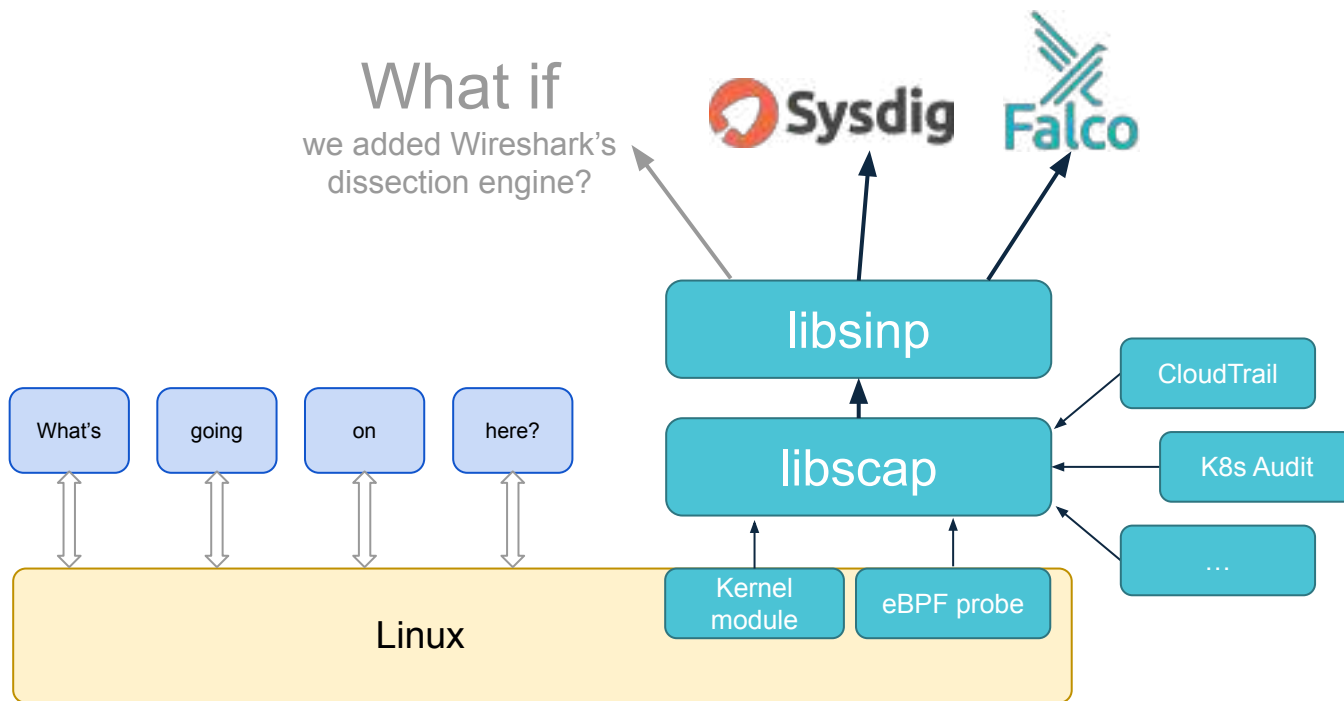


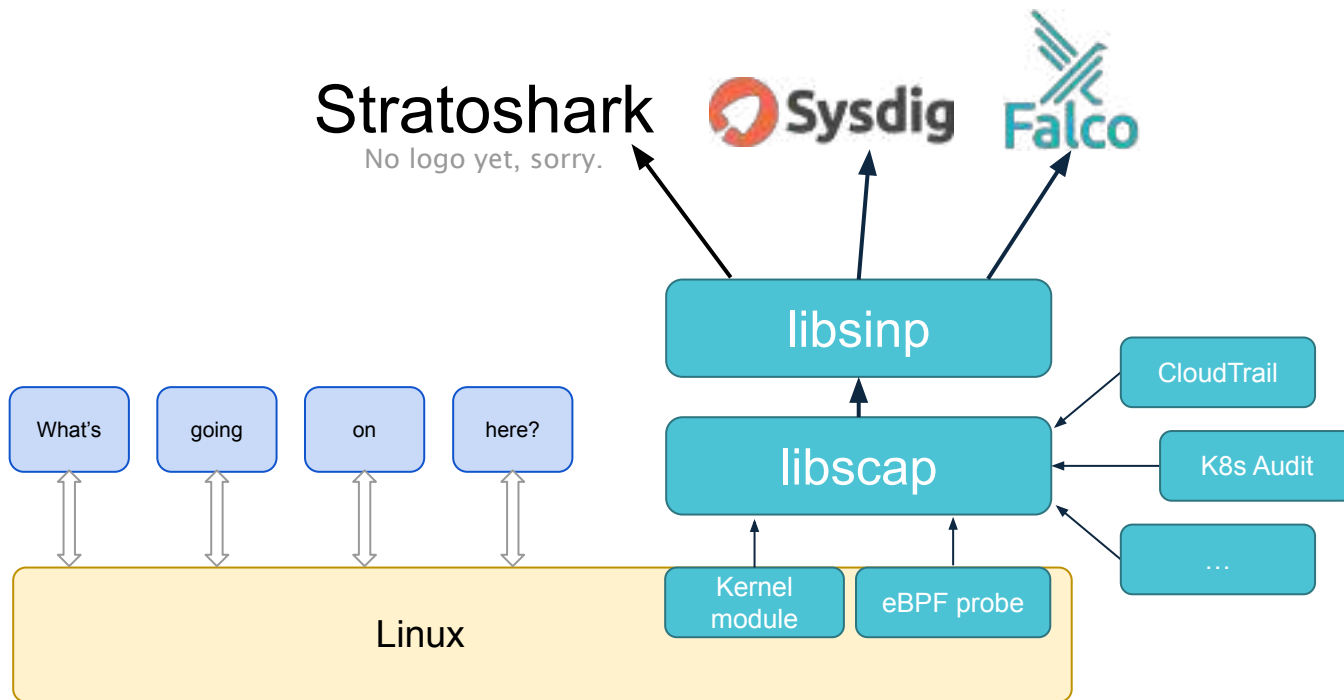






<https://github.com/falcosecurity/libscap>







# Demo Time<sup>1</sup>

1. May contain traces of danger and stupidity





# When?

Officially? Early 2025.

Technically? Now.

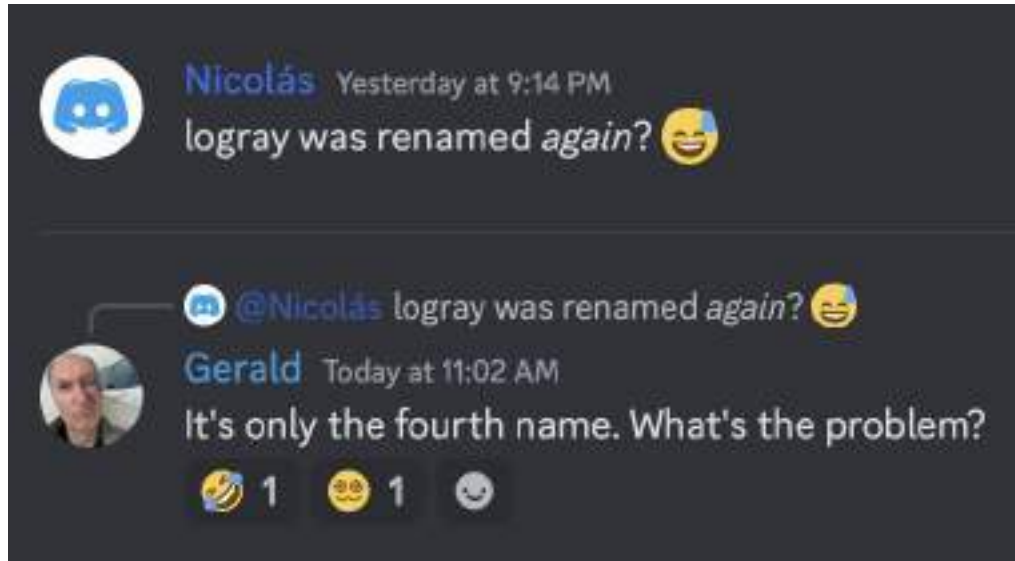
<https://www.wireshark.org/download/automated/>



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





Wireshark lives in your network,  
Stratoshark lives in your cloud

Not just logs – syscalls are  
prominently featured

"Shark" brand is very strong





# Developer Time



4.4 added and improved:

Lua 5.3 / 5.4

Display filter updates

Automatic profile switching

I/O Graph, Sequence Diagram, TCP Stream Graph

More custom column support



Probably summer 2025

Considerations:

Have we accumulated significant features?

Qt LTS version maturity

Left edge of Linux LTS version windows



Millions of lines of code ...3.5M or maybe 6.4M?

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

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

4100 Discord users

3000 protocols, 250k fields

2300 authors

Two yearly conferences

One foundation





Steering committee is now official

Platinum member: Endace

Silver members: Veeam, Npcap



*Good:* Donate at [wiresharkfoundation.org](https://www.wiresharkfoundation.org)

*Better:* Set up a recurring donation

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



**Thank You**



Automated builds

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

event-extras.lua

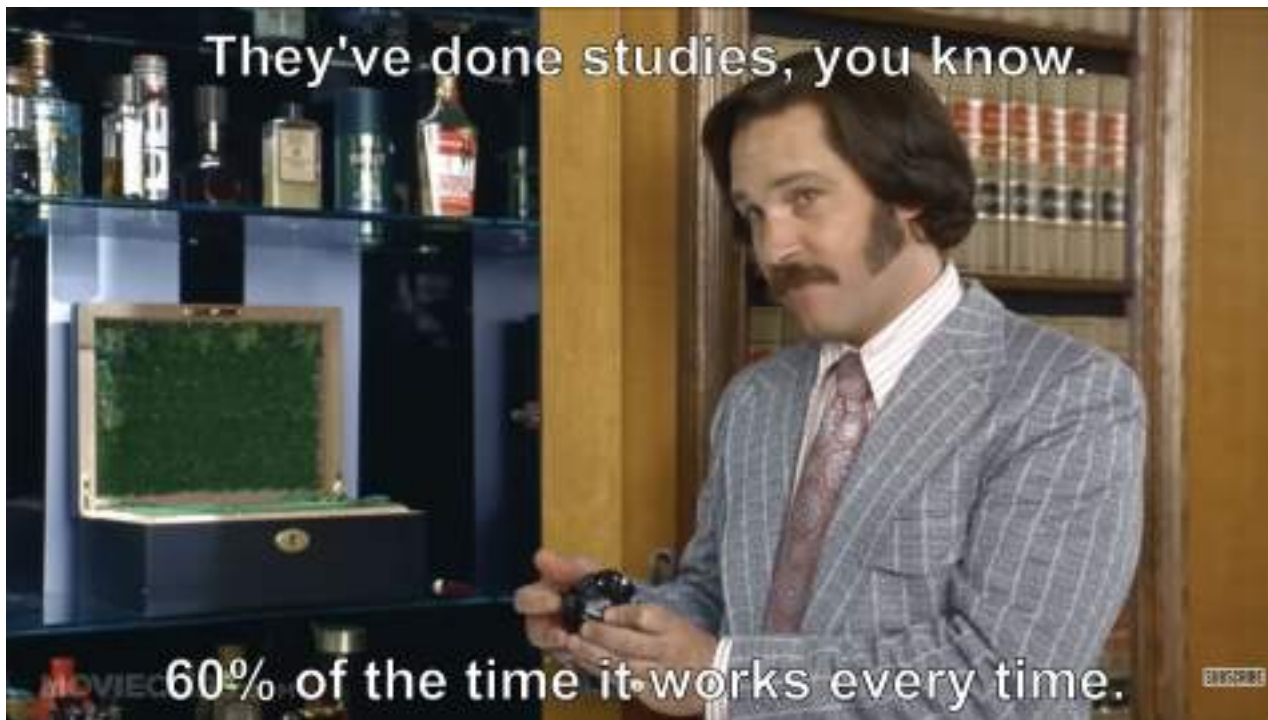
<https://gist.github.com/geraldcombs/d7d541af18890750f1a4197e406e7cf9>

Linux system calls


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



# Bonus Slides





mos\_8502 

@mos\_8502@studio8502.ca

Hot take: open source is good. But open data formats are far more important. Programs can be replaced. Often your data cannot.

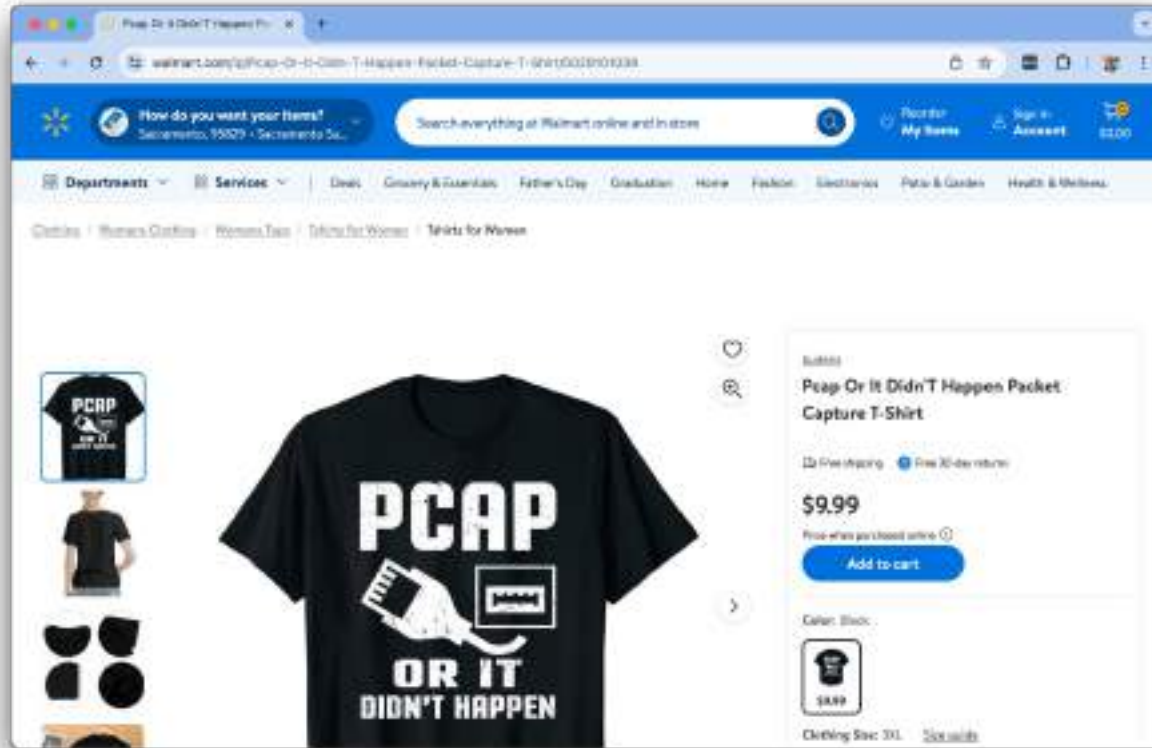
Oct 19, 2024, 09:43 AM ·  · Mona for iPhone



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









*If you are a user or provide technical support:*

I regret to inform you that this is the world we've built and it's only going to get worse as time goes on.

*If you are on the receiving end of an IT budget:*

I am delighted to inform you that this is the world we've built and it's only going to get worse as time goes on.

# How Do We Make Sense of This?



What sources of information are

- Truthful
- Accessible
- Reliable



What sources of information are

- Truthful
- Accessible
- Reliable

How about packets, system calls, and logs?