WIRESHARK FOUNDATION

Wiresharkæology

How it started and where we're headed

Gerald Combs
Wireshark Foundation
Sysdig

@geraldcombs@infosec.exchange
@geraldcombs.bsky.social

Wireshark Prehistory

Used a Sniffer® early on in my career

Changed jobs, new employer had no budget for a Sniffer

Needed an analyzer that ran on Linux and Solaris

Wrote Ethereal, released as open source

Project Hosting: Pioneer Days

Bought a “server” 40 MHz SPARCstation IPX, 64 MB RAM

Installed and maintained a bunch of software

Traded consulting gigs for rack hosting

Worked great … until it didn’t

How We Got Wireshark

In the mid-aughts 802.11 became popular…

…but you couldn’t troubleshoot it on Windows XP

Sent an email to the WinPcap developers

Renamed to Wireshark (and learned about the importance of trademarks)

…and started a conference

Original Goals

Look at packets on the network

Contribute back to open source

Goals 3 Months Later

Help UNIX and Linux users look at packets on their networks

~~Look at packets on the network~~

Goals 1 Year Later

Help Linux, UNIX, and Windows users look at packets on their networks

~~Help UNIX and Linux users look at packets on their networks~~

~~Look at packets on the network~~

Goals 3 Years Later

Help Linux, UNIX, Windows, and macOS users look at packets on their networks

~~Help Linux, UNIX, and Windows users look at packets on their networks~~

~~Help UNIX and Linux users look at packets on their networks~~

~~Look at packets on the network~~

Goals Several Years Later

Help Linux, UNIX, Windows, and macOS users look at packets on their networks. And authors. And educators. And students. And security researchers.

~~Help Linux, UNIX, and Windows users look at packets on their networks~~

~~Help UNIX and Linux users look at packets on their networks~~

~~Look at packets on the network~~

New, Improved Goal

Help as many people as possible understand their networks as much as possible

Getting to the Goal

How do we ensure that…

Developers have the tools to create a great application?

Wireshark is easy to obtain and install?

Community has access to support & educational resources?

Let’s get a business model!

Open Source Business Models

None (Just use a project hosting service)

Corporate overlord (aka “ask your boss”)

Umbrella organization

Independent not-for-profit

The Easy Way

If you can get away with it, *no model is the easiest option*.

…but note that neither GitHub not GitLab have “talk to a lawyer” or “talk to an accountant” button.

GitHub

GitLab

Open Source Business Models

~~None (Just use a project hosting service)~~

Corporate overlord (aka “ask your boss”)

Umbrella organization

Independent not-for-profit

Corporate Overlords

1998 - Network Integration Services

2006 - CACE Technologies

2010 - Riverbed

2021 - Sysdig

Single Points of Failure

Having your employer pay for everything is really convenient, but:

- Overlap between the project and my employer was minimal
- This convenience carried financial risks

What do networking people do with single points of failure?

Open Source Business Models

~~Use a project hosting service~~

~~Corporate overlord~~

Umbrella organization

Independent not-for-profit

WIRESHARK FOUNDATION

Umbrella Organizations

Organization as a service

Provide everything GitHub & GitLab don’t

They own IP assets

Can be a great choice…

…unless you already have a strong organization

“Americans can always be counted on to do the right thing … after they have exhausted all other possibilities.”

— Probably Not Winston Churchill

https://quoteinvestigator.com/2012/11/11/exhaust-alternatives/

WIRESHARK FOUNDATION

Open Source Business Models

~~Use a project hosting service~~

~~Corporate overlord~~

~~Umbrella organization~~

Independent not-for-profit

…so that is what we did

Incorporated as a 501(c)(3) non profit in the US

wiresharkfoundation.org

Dear Applicant:

We're pleased to tell you we determined you're exempt from federal income tax under Internal Revenue Code (IRC) Section 501(c)(3). Donors can deduct contributions they make to you under IRC Section 170. You're also qualified to receive tax deductible bequests, devises, transfers or gifts under Section 2055, 2106, or 2522. This letter could help resolve questions on your exempt status. Please keep it for your records.

Organizations exempt under IRC Section 501(c)(3) are further classified as either public charities or private foundations. We determined you're a public charity under the IRC Section listed at the top of this letter.

What’s Next?

Wireshark Today

Millions of lines of code …3.6M or maybe 6.6M?

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

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

4100 Discord users

3000 protocols, 265k fields

2300 authors

2 yearly conferences

Wireshark Vital Statistics

Millions of lines of code …3.6M or maybe 6.6M?

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

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

4100 Discord users

3000 protocols, 265k fields ⇐ What does this mean, exactly ?

2300 authors

2 yearly conferences

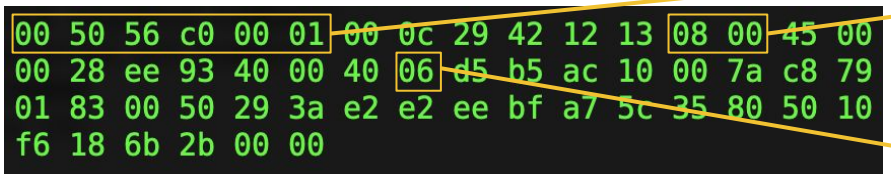
Wireshark takes this…

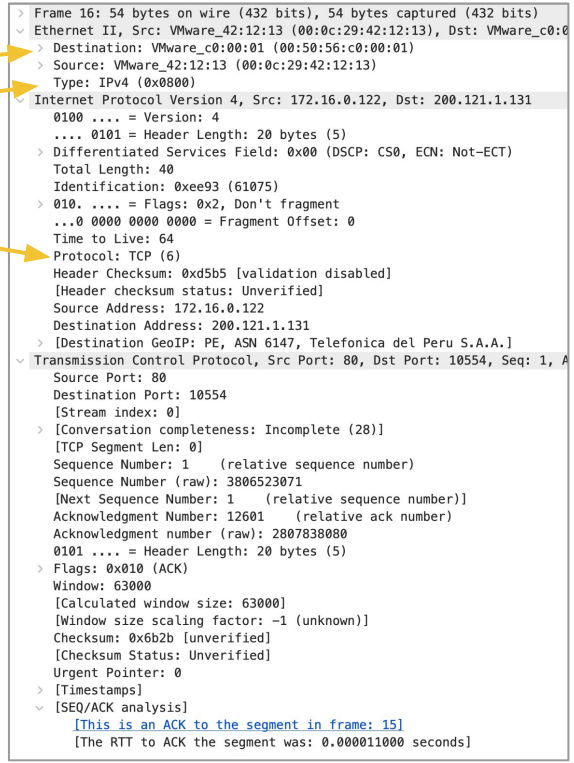
Different numbers determine how it's routed and what happens when it arrives.

You can memorize all of the numbers (some people do!) or…

```
00 50 56 c0 00 01 00 0c 29 42 12 13 08 00 45 00
00 28 ee 93 40 00 40 06 d5 b5 ac 10 00 7a c8 79
01 83 00 50 29 3a e2 e2 ee bf a7 5c 35 80 50 10
f6 18 6b 2b 00 00
```

…and gives you this

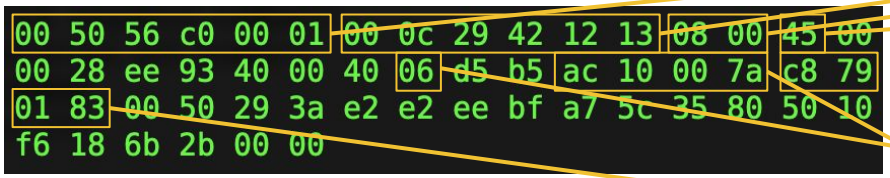


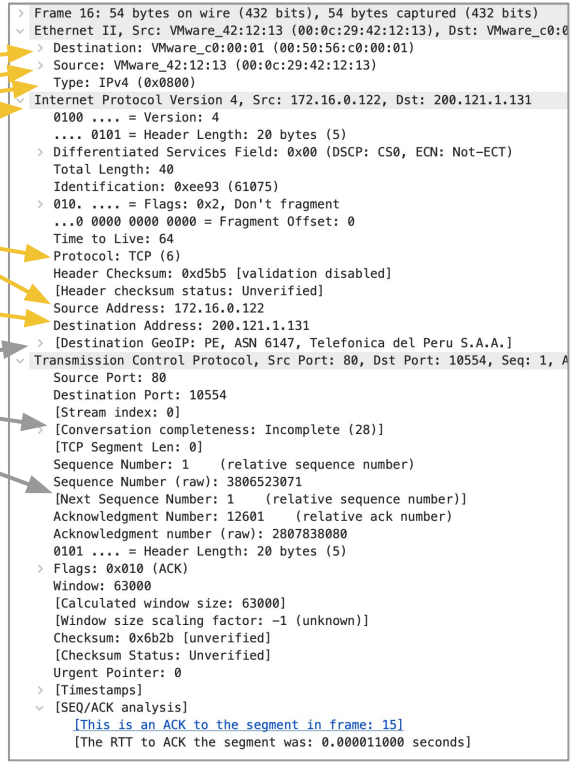


Wireshark's dissection engine takes blobs of bytes and breaks them up into fields

This lets us build powerful and useful features

…and gives you this





These aren't in the packet!

Wireshark's dissection engine takes blobs of bytes and breaks them up into fields

This lets us build powerful and useful features

Protocol Fields

Every protocol has a set of associated *fields*.

Fields have a name, type, length, etc.

Wireshark supports over 265,000 of them.

Display Filter Reference: Internet Protocol Version 4

Protocol field name: ip

Versions: 1.0.0 to 4.0.7

Back to Display Filter Reference

Field name	Description	Type
ip.addr	Source or Destination Address	IPv4 address
ip.bogus_header_length	Bogus IP header length	Label
ip.bogus_ip_length	Bogus IP length	Label
ip.bogus_ip_version	Bogus IP version	Label
ip.checksum	Header Checksum	Unsigned integer (16 bits)
ip.checksum.status	Header checksum status	Unsigned integer (8 bits)
ip.checksum_bad	Bad	Boolean
ip.checksum_bad.expert	Bad checksum	Label
ip.checksum_calculated	Calculated Checksum	Unsigned integer (16 bits)
ip.checksum_good	Good	Boolean

Fields Enable Features

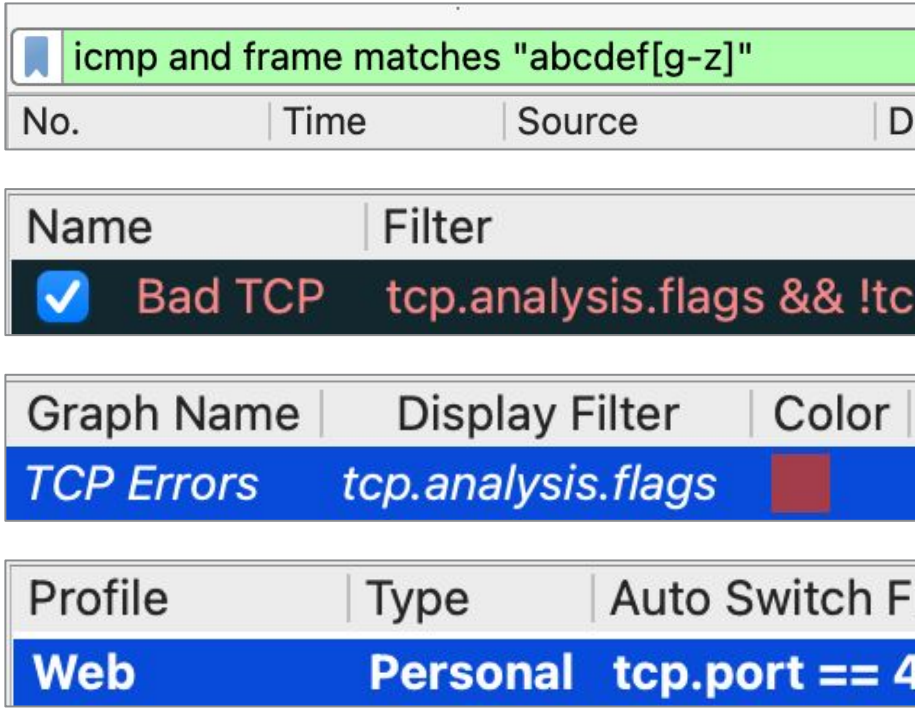
It takes all of the bits and bytes in each packet and breaks them down into fields

Fields are filterable…

…and colorable

…and graphable

…and lots of other -ables.



Where can we go with this?

Wireshark is part of an ecosystem

Libpcap + .pcap + .pcapng

Lets application developers focus on features

Capture anywhere (with WinPcap/Npcap)

Common file format is a productivity multiplier

This Works Great!

Having a common library and file formats works really well.

Where can we duplicate this success?

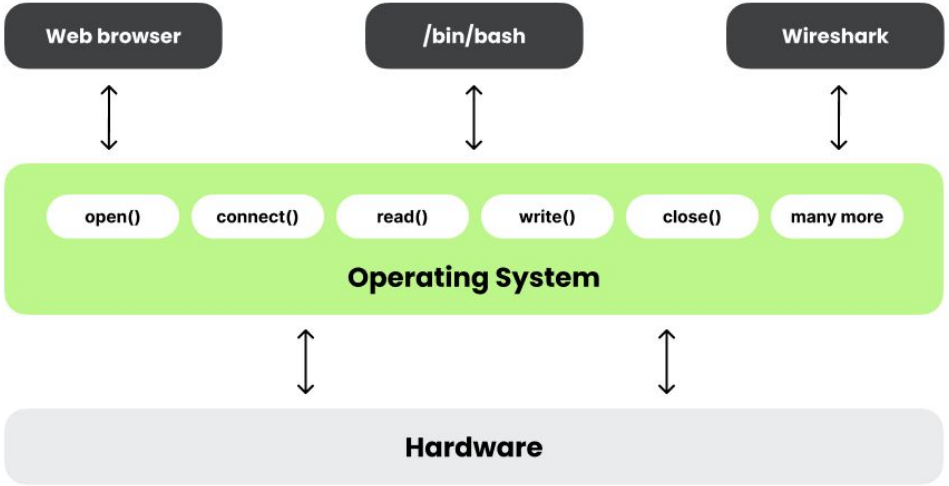
This Works Great!

Having a common library and file formats works really well.

Can other ecosystems benefit from our dissection engine?

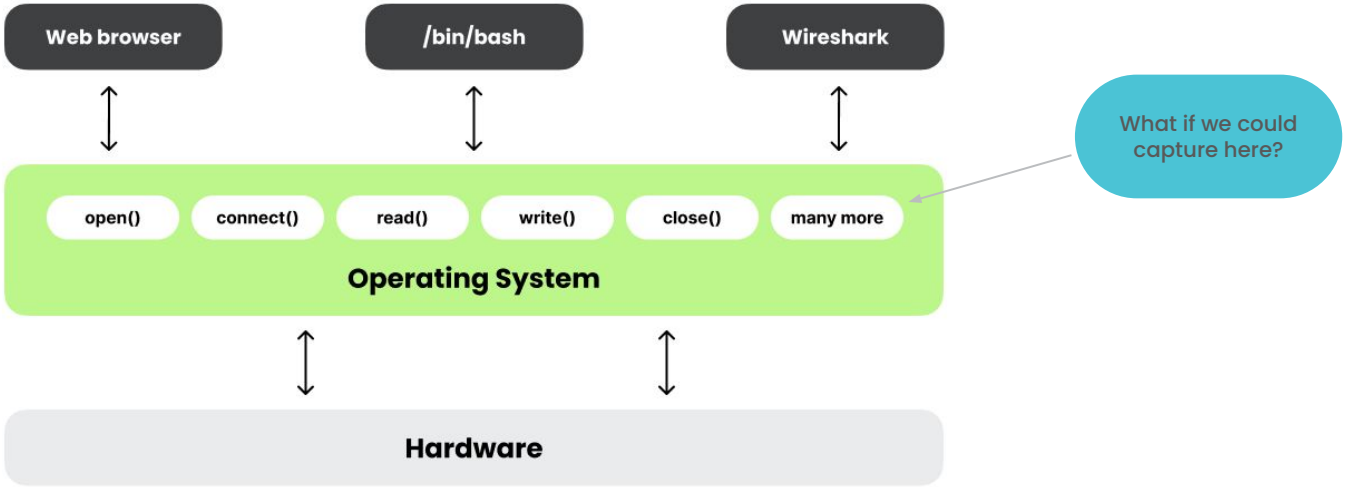
- System calls
- Logs
- Whatever erupts from your fevered imagination

System Calls



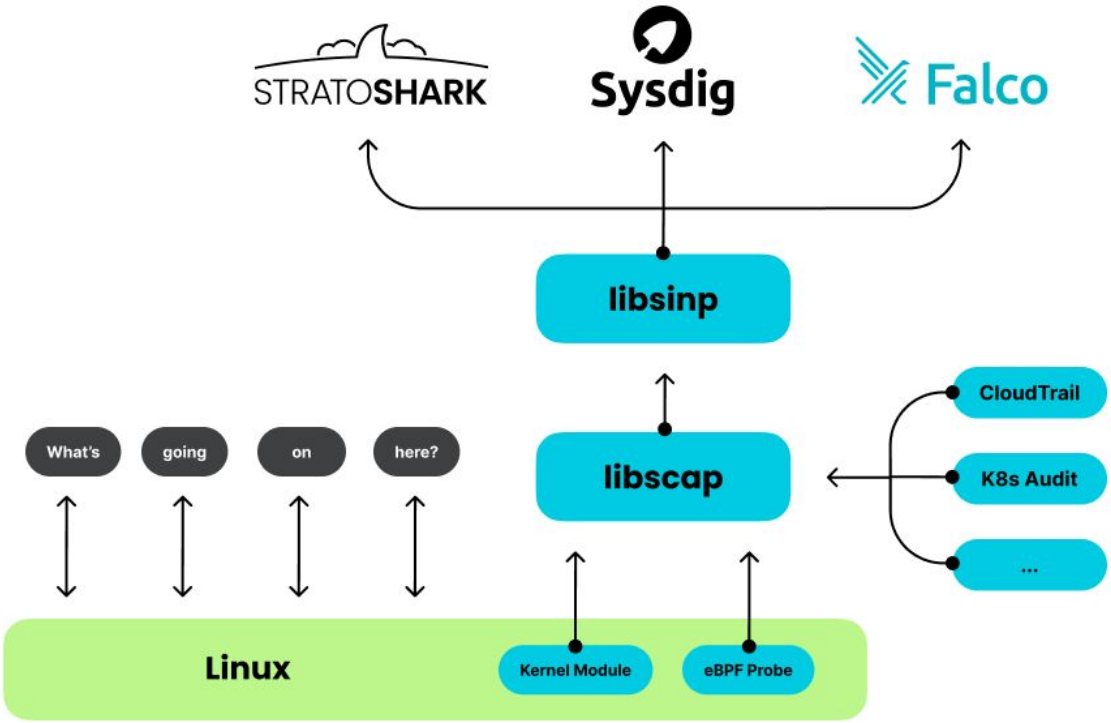
Have you ever read man pages on Linux or macOS? System calls are section 2!

System Calls



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

libscap + libsinsp



https://github.com/falcosecurity/libs

Designed to be a single video camera

- *The best single video camera, but still…it's just one sensor!*
- *Doing more requires more technology from the OSS ecosystem (that's why we have plugins)*

Only looks for what the rules tell it to look for

- *If the rules don't find anything, Falco doesn't find anything!*
- *New attacks need new rules, and we always have new attacks*

Only does threat detection

- *The best at threat detection, but organizations need more*
- *Stratoshark helps Falco with Digital Forensics & Incident Response (DFIR)*

Demo Time[1]

1. May contain traces of danger and stupidity

Refining the Goal

Help as many people as possible understand their networks and systems as much as possible

Thank You

Bonus Slides

How We Got Ethereal

Used a Sniffer® early on in my career

Changed jobs, new employer had no budget for a Sniffer

Needed an analyzer that ran on Linux and Solaris

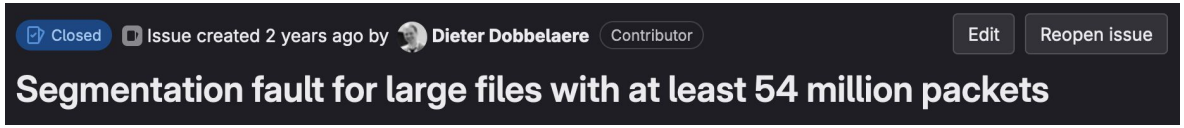
Wrote Ethereal, released as open source

Part of Something Big

The ‘90s saw two important developments:

Off-the-shelf hardware became more powerful

Less (*but not no*) need for specialized capture hardware



(we fixed this bug)

The Internet allowed for large-scale, distributed collaboration

Linux, Apache, 7-Zip, curl, VLC, **Ethereal**, many other open source projects

How We Got Wireshark

In the mid-aughts 802.11 became popular…

…but you couldn’t troubleshoot it on Windows XP

Sent an email to the WinPcap developers (one was a former Endace intern)

Renamed to Wireshark (and learned about the importance of trademarks)

…and started a conference

Wireshark Speedrun

The Wireshark Foundation

the insidious plot to help me sleep better at night

Thank You