Things I Love About Wireshark

and maybe a couple of things I don't

Gerald Combs
Core Developers

When An Easy Assignment Becomes Difficult

Introspection is kind of like looking behind your refrigerator

You find all sorts of useful, actionable, relevant information

Information can make you sad

Wireshark Is Healthy

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

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

~90% Windows, ~9% macOS …again, on the servers we manage

4100 Discord users

3000 protocols, 265k fields

2300 authors

2 yearly conferences

The instant that connection closes

Which connection? The one that delivered Wireshark to your computer

It's when the statistics from the previous slide turn into empowerment

It's when the work of a few is used by millions

In the time you have read this ~~THOUSANDS~~**PERHAPS SEVERAL** people have downloaded Wireshark

Sweet merciful crap it's the second quarter of the 21st century I'm still writing C why

Sweet merciful crap

It's the second quarter of the 21st century

I'm still writing C code

What am I even doing

This haiku is terrible

Sweet merciful crap it's the second quarter of the 21st century I'm still writing C why

C made more sense 25 years ago

We now live in Rustier, Swiftier times and the state of the art has improved

Other languages offer better memory safety and multicore support

There Is An Easter Egg

Have you looked at the bottom of the welcome screen? I mean *really* looked?

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are sniffing the glue that holds the Internet together using Wireshark 4.4.7 (v4.4.7-0-g7980339b1630). You receive automatic updates.

Or read the release notes source code?

```
35    The following bugs have been fixed:
36
37    //* wsbuglink:5000[]
38    //* wsbuglink:6000[Wireshark bug]
39    //* cveidlink:2014-2486[]
40    //* Wireshark grabs your ID at 3 am, goes to Waffle House, and insults people.
```

We accidentally built a time series data analyzer

pcapng can hold more than packets

The dissection engine doesn't care what you feed it

What if you just change the word "packet" to "event"?

STRATO**SHARK**

Drops

For all that we've added, we're still missing some important things

Drops

For all that we've added, we're still missing some important things

Accessibility

Multicore support

Multiple files

Lots of other stuff
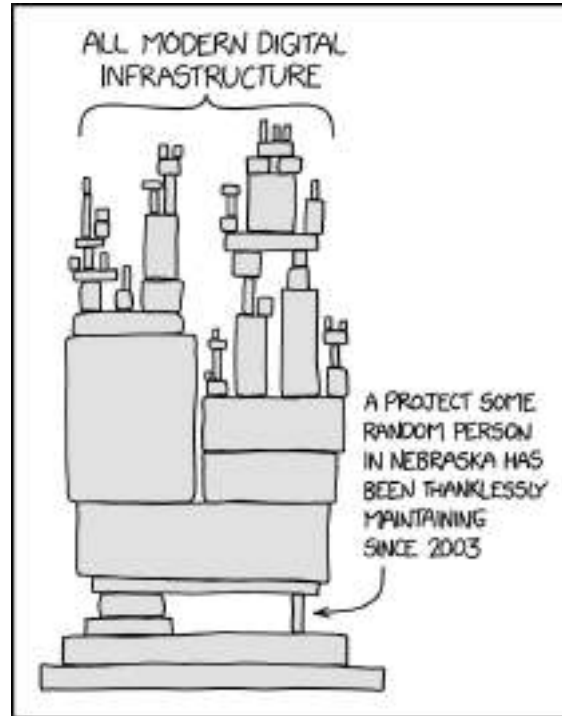
Wireshark Keeps Me Busy

There's *always* something to do, and I love fixing problems

It's easy to put too much effort and time into into something you love

Burnout

Open Source Burnout

https://xkcd.com/2347/

Wireshark Isn't Just Wireshark

bcg729	libilbc	Lua	Qt
Brotli	libmaxminddb	minizip-ng	SBC
c-ares	libpcap	Nettle	Snappy
Dirent	libscap	nghttp2	SpanDSP
Gettext	libsinsp	nghttp3	Sparkle
GLib	libsmi	npcap	SpeexDSP
GnuTLS	libssh	Opus	WinSparkle
GMP	Libtasn1	OpenCORE AMR	zlib-ng
Libgcrypt	libxml	p11-kit	zstd
libgpg-error	Lz4	PCRE2	

What Makes Open Source Special In This Regard?

The needs of the project exceeds the resources you can provide

Mismatched expectations, aka the Dollar Movie House Effect

What if these happen at "web scale"?

Expectation Mismatches

Open source suffers from the dollar movie house effect:

> If circumstances let you deliver one thing at a discount, people will expect you to deliver *everything* at a discount.

Expectation Mismatches

Open source suffers from the dollar movie house effect:

> If circumstances let you deliver one thing at a discount, people will expect you to deliver *everything* at a discount.

"You're only charging a dollar for tickets. Why do I have to pay full price for popcorn and soda?"

Expectation Mismatches

Open source suffers from the dollar movie house effect:

If circumstances let you deliver one thing at a discount, people will expect you to deliver *everything* at a discount.

"You're delivering your software for free. You therefore have no expenses."

"You're delivering your software for free. You therefore have infinite time and resources that you can devote to my needs."

Open Source Burnout

Attaching peoples' expectations to an activity you love will <mark>crush your soul</mark>

Open Source Burnout

I'm hesitant to talk about this

"Be lucky like me" is not actionable advice

With that out of the way, here are some things that help in my case

IT HAS BEEN

QUITE A FEW DAYS

SINCE GERALD'S SOUL HAS BEEN CRUSHED

https://avtanski.net/projects/days/

You Are All Amazing

The Wireshark community by and large is really very nice

Community interactions are almost always polite & productive

This really helps! Keep up the great work!

My Family Is Amazing

My daughter loves anthropology and is pursuing her degree(s).

…which means that my wife and I are able to send her to a university.

…which means that I make a comfortable living, even though I've spent the last 2.5 decades giving software away *for free*.

…and she has an an amazing mother.

The Open Source Community Is Amazing

I get to interact with the people behind several projects, mostly around networking

It might be due to shared trauma, but we're all pretty nice and supportive of each other

Our Sponsors Are Amazing

The foundation has an important mission

Our sponsors, members, and donors make it possible

The People I Work With Are Amazing

The Foundation: Sheri and Angelo

The People I Work With Are Amazing

The Foundation: Sheri and Angelo

Sysdig: the OSS and marketing teams

The People I Work With Are Amazing

The Foundation: Sheri and Angelo

Sysdig: the OSS and marketing teams

Wireshark: the core developers

Developer Time

Education and Career Advancement

The foundation has a mission: to help you learn about networking

There's a pleasant side effect here – knowing how things work at a low level is a valuable skill

Get Certified!

Wireshark Certified Analyst

Continues our goal of educating users

Official recognition of your skills and knowledge

    helps you

    helps the project, and

    helps the foundation

Thank You

How's My ~~Driving~~ Talking?

Bonus Slides