

SharkFest'26 Europe

Wireshark Progress, Problems, and Plans

Gerald Combs
Core Developers

Sponsored by:
PROFI TAP DEEP NETWORK OBSERVABILITY
cPacket
TCP/IP training
endace Record. Respond.

Getting Ready for 5.0 (and 1.0)

More details in the next session

We have new artwork!





Trivia: The fin originally pointed the other direction



Icons are a function of design and display technology constraints

In the olden days, pixels were *huge*, and carved from CRT shadow masks and whale bone.

Now they are varying degrees of smallness and might need to be drawn light or dark modes.

They also need to conform to current style guidelines on our supported operating systems.

Roland added themes, which gave me an excuse to update our icon set, but which one?

Our new icons need to be: vector (SVG), well-designed, and have a compatible license.

Tons of choices: Bootstrap, Ionicons, Mono, Tabler, Fluent, Hero, ~~SF Symbols~~.

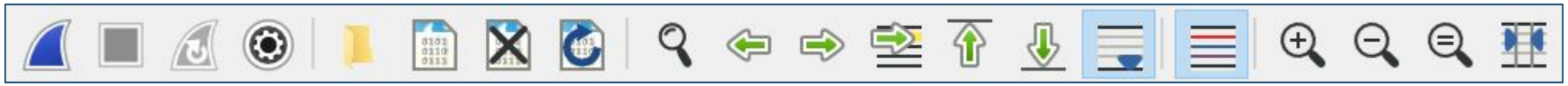
Ended up choosing Fluent, mainly because most of our users use Windows and Apple's license for SF Symbols is unclear.

Toolbars over time

2003

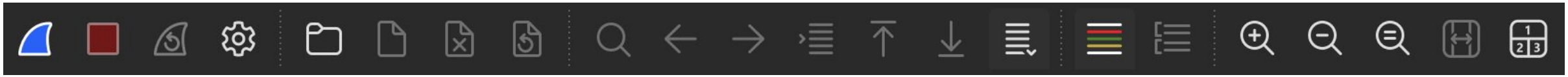


2013



2026





We almost didn’t have the fin icon



Early 2013: My brilliance is unmatched and surely everyone will celebrate this fact.

What was I thinking?

These are standard[1] symbols that:

- Have been around for decades
- Are used across industries in both hardware and software
- Are easy to implement
- May be associated with happiness

They are right there! On your phone!

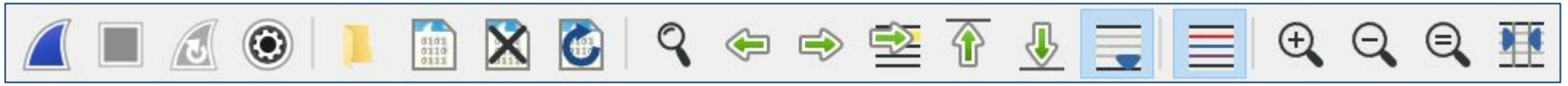
1. ISO 7000 / IEC 60417,

OK, let's try this again

Early 2013:



Later in 2013, after not one but two long wireshark-dev discussions:



Things turned out OK

It would be easy to say that this was bikeshedding (https://en.wikipedia.org/wiki/Law_of_triviality):

> "The law of triviality is C. Northcote Parkinson's 1957 argument that people within an organization commonly give disproportionate weight to trivial issues."

> alternatively, "What color should we paint the bike shed?"

However, this is a fundamental feature of the application. It's anything but trivial.

Everyone involved genuinely wanted to make Wireshark better.

Anyway, I really hope you like the new icons.

Version numbers

We've been using odd=development / even=stable numbers for a long time.

Dev	Stable
0.99	1.0
1.1	1.2
…	…
4.5	4.6
4.7	5.0
5.1rc0	5.1

This is awkward and can be confusing.

We will stop doing that next year. The next major stable release will be 5.1.

I'd also like to make the Stratoshark version the same as the Wireshark version.

However, Stratoshark 1.0 → Stratoshark 5.1 is kind of an ugly jump.

Stratoshark updates

Capture source / extcap bookmarks (also in Wireshark!)

Architectural fixes (raw block engine)

Procmon support

Sadly, no live capture on Windows or macOS just yet

When

Tell us. When?



When can I get my hands on 5.0?

This is the plan. Reality will undoubtedly have other ideas.

~~September 2: Release Wireshark 4.7.3 & Stratoshark 0.10.3~~

~~October 14: Create the release-5.0 branch~~

~~October 21: Release Wireshark 5.0.0rc1 & Stratoshark 1.0.0rc1~~

November 2–6: SharkFest EU ⬅ We are here

November 12: Release Wireshark 4.6.10 and 4.4.20

November 12: Release Wireshark 5.0.0rc2 & Stratoshark 1.0.0rc2

November ??: Release Wireshark 5.0.0 & Stratoshark 1.0.0

You can download builds at **https://www.wireshark.org/download/automated/**

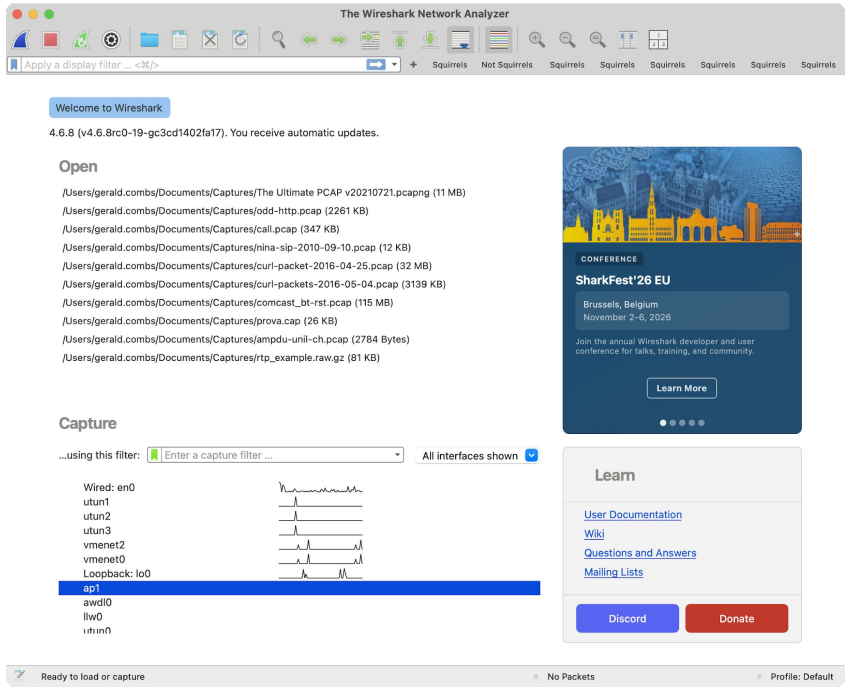
You are at a conference with a bunch of Wireshark developers this week.

Sweet merciful crap the 4.6.5 release was rough

Normal releases take about a half day of preparation followed by a half day of release work.

4.6.5 was a perfect storm of:

- An overdue release (9 weeks instead of 6)
- An absolute truckload of security fixes
- A new, not quite fully cooked feature
- Hardware failure



Ultimately several days of prep plus 12+ hours of release work.

Users ended up with a new feature they couldn't disable.

Shipping was ultimately our decision. We went with getting the fixes out.

Wherein we risk angering the audience

Each of these are individually valid and completely reasonable:

Being upset or annoyed about sponsor slides on the welcome page.

Making a living using Wireshark.

Not donating to the project.

Any **two** are absolutely fine and also valid completely reasonable.

...but *all three?*

Project statistics

Millions of lines of code ...4M or maybe 7M?

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

~ 93% Windows, ~5% macOS ...again, on the servers we manage

16.5k Discord users

3200 protocols, 271k fields

2500 authors

Yearly conferences and events

1 certification

Project statistics

Millions of lines of code ...4M or maybe 7M?

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

~ 93% Windows, ~5% macOS ...again, on the servers we manage

16.5k Discord users

3200 protocols, 271k fields

2500 authors

Yearly conferences and events

1 certification

Quiz: What's our most popular download?

Project statistics

Millions of lines of code ...4M or maybe 7M?

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

~ 93% Windows, ~5% macOS ...again, on the servers we manage

16.5k Discord users

3200 protocols, 268k fields

2500 authors

Yearly conferences and events

1 certification

Quiz: What's our most popular download?

www.wireshark.org/download/automated/manuf

Foundation Updates

Our mission

"The Wireshark Foundation helps as many people as possible understand their networks and systems as much as possible.

This starts and ends with you

Modern society is defined by software talking to other software over networks.

Most of you keep little corners of that world fast, reliable, and secure. Your jobs are important.

Our mission is to give you the tools and understanding to do that. By extension, our job is important.

So, how do we achieve the mission?

Hosting: SharkFest, education days, Wireshark meetups.

Participating: FOSDEM, other conferences.

Validating: Wireshark Certified Analyst, scholarships, and other career advancement.

Operating: Wireshark has infrastructure, and someone needs to run it.

Managing: Technical Steering Committee, Board of Directors.

Wireshark Certified Analyst



- 1 year anniversary!
- About 50 WCA's to date.
- Rigorous exam matching Wireshark's standards.

Wireshark Certified Analyst

Seeking Organizations to include the WCA in position requirements.



Wireshark Certified Analyst



SharkFest EU 26 WCA Promo

Use coupon code at checkout:

SFEU26

https://webassessor.com/WIRESHARK

Foundation finances

Quiz: What was our 2025 revenue and expenditures?

Foundation finances

2025:

Revenue: $633,587

Expenditures: $648,910

Total: ($15,323)

Most of this is SharkFest.

This year is better so far ($40k in donations), but we're still treading water.

We could do so much more.

Conferences are flippin’ expensive

Conferences were expensive before COVID. After COVID…

Venues want payment up front, months before anyone registers.

Bandwidth is somehow rare and precious. Is printer ink involved somehow? I don’t know.

We have a new board!

As of August 12, we have a new board of directors!

Gerald Combs

Janice Spampinato

Loris Degioanni

Kary Rogers

Jasper Bongertz

Kelley Misata (chair)

Chris Greer

Geoffrey Kempenich

Sharareh (Sheri) Najafi

Developer Time





Magic vs Magical



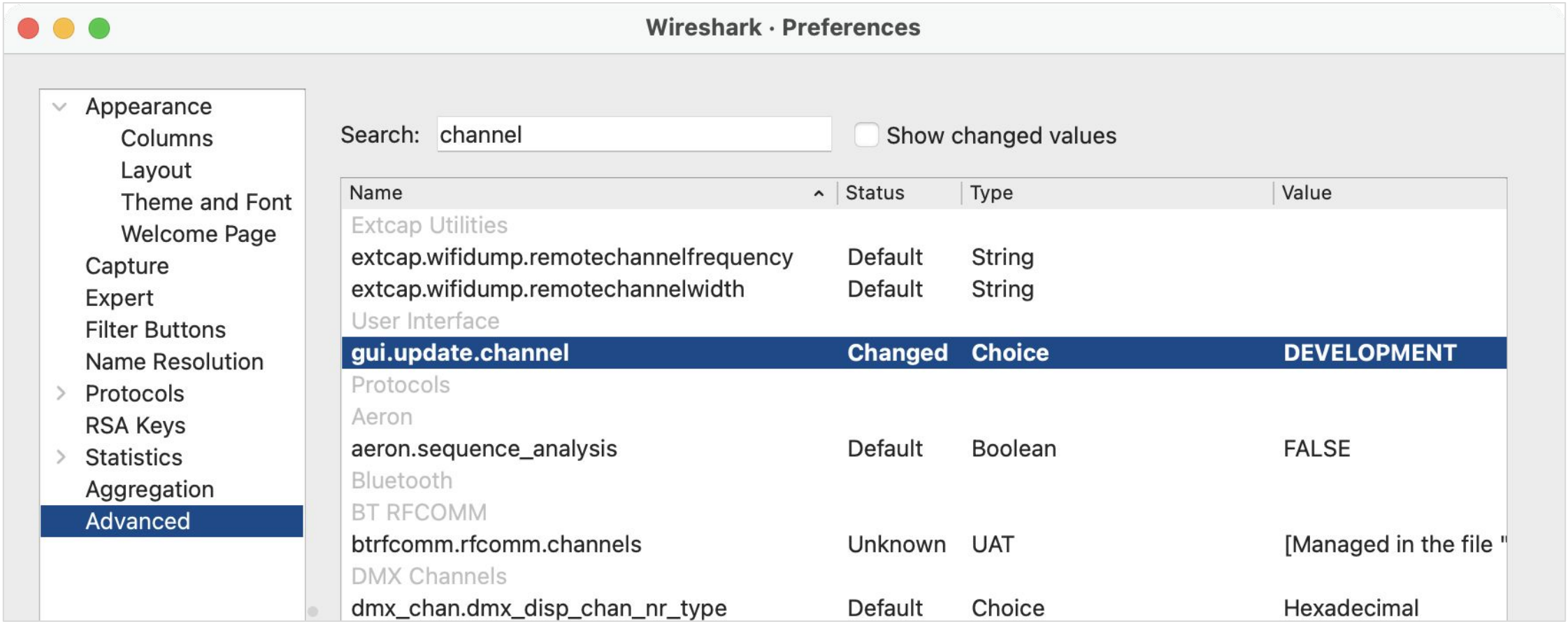
Thank You!



Bonus Slides



How adventurous are you?



We have a new application icon



1998



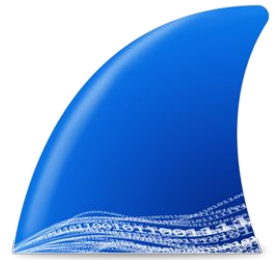
2001



2006



2006



2013





2026


HOME TAPING IS KILLING
RECORD INDUSTRY PROFITS!
SIDE
TWO
WE LEFT THIS SIDE BLANK
SO YOU CAN HELP