What's New In 4.6?

Gerald Combs
Core Developers

What’s new in Wireshark 4.6?

Plots

macOS process information

macOS universal packages

Lots of other stuff (force light/dark mode, …)

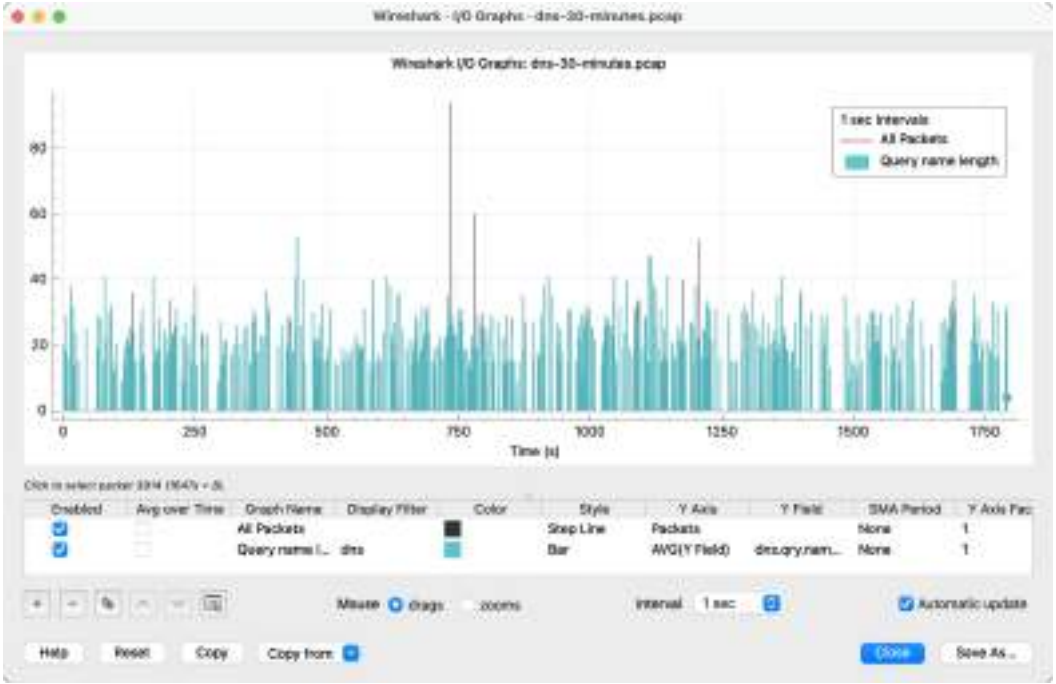
See the release notes for details

https://www.wireshark.org/docs/relnotes/wireshark-4.6.0.html

Plots

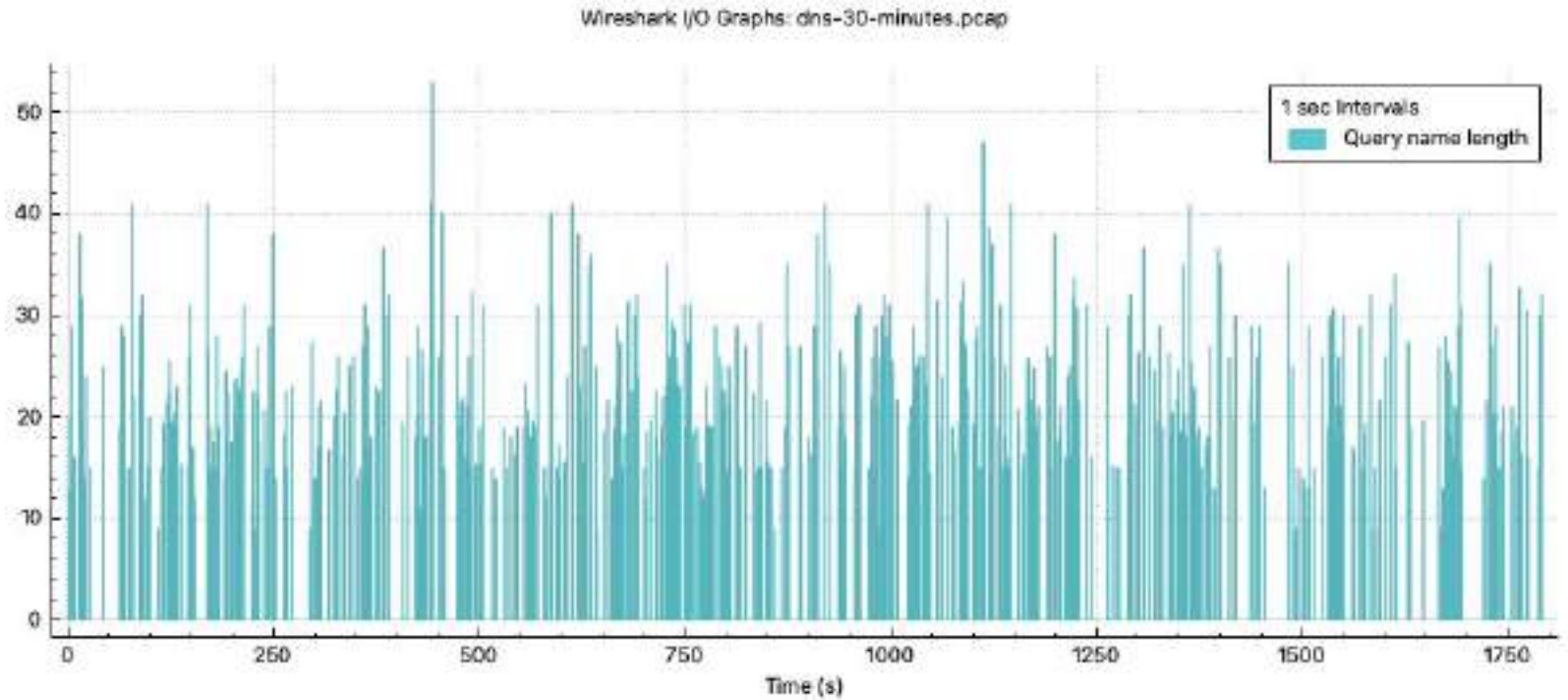
(Wait. Don’t we already have I/O Graphs?)

Average DNS query name length over time

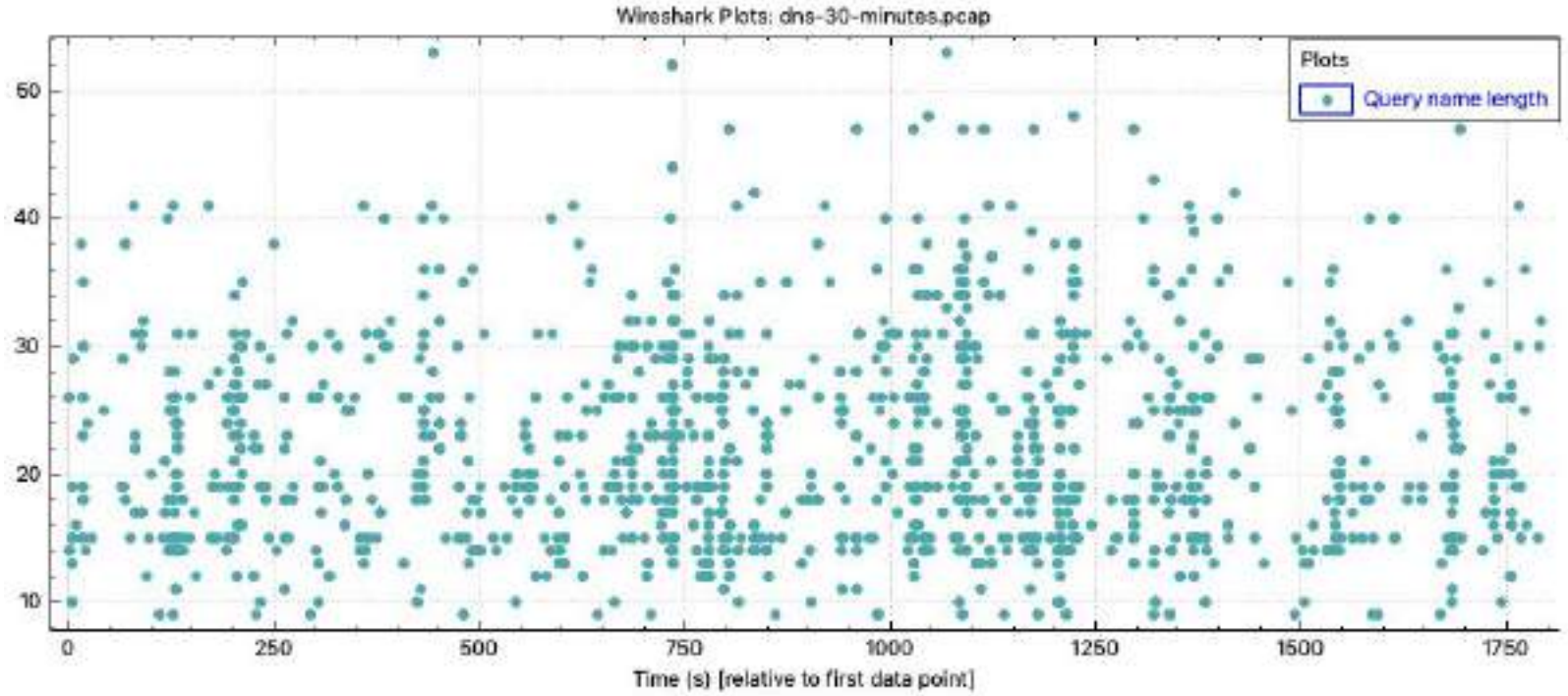


We've had graphs since 2001! (version 0.9.0)

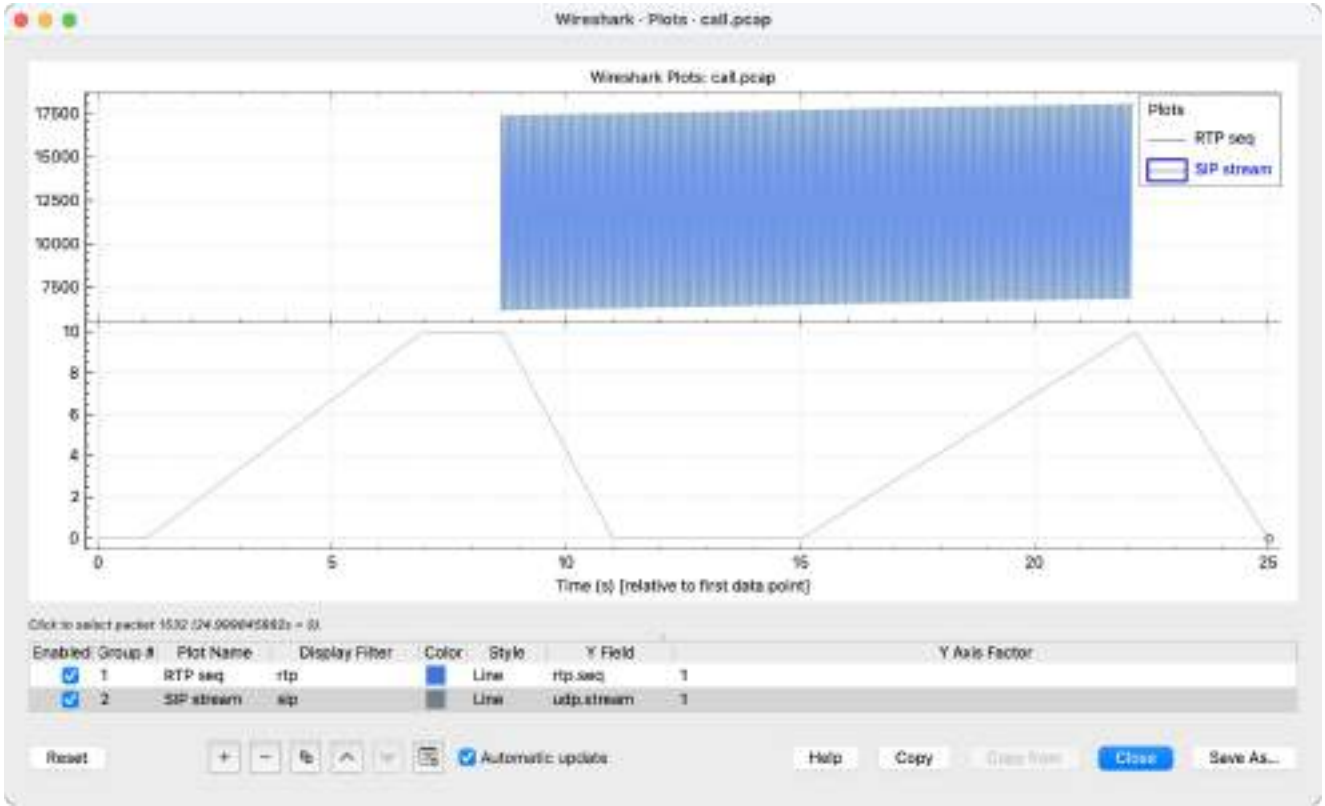
Pattern Recognition



Pattern Recognition



Multiple Plots



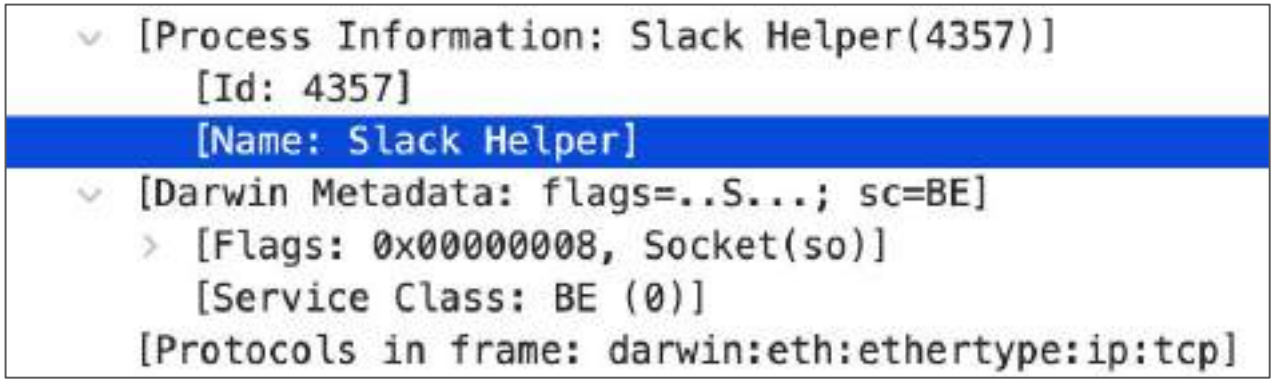
Why Aren’t They Combined?

macOS Process Information

Run `tcpdump -i pktap,<interface>`

Gives you process information, flow ID, other info

```
frame.darwin.process_info.pname contains "Slack"
```



macOS Universal Packages

Different OSes use different file formats for executables

Windows: PE, Linux: ELF, macOS: Mach-O

You can stuff code for multiple architectures (PPC, x86, x64, Arm64) into the same Mach-O file

This helped smooth the PPC → x86 → x64 → Arm64 transitions

“Universal” today means x64 + Arm64

…so what took us so long?

We ship more than just Wireshark with 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	USBPcap
GMP	Libtasn1	OpenCORE AMR	WinSparkle
Libgcrypt	libxml	p11-kit	zlib-ng
libgpg-error	Lz4	PCRE2	zstd

How do we get from here…

…to here?

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	USBPcap
GMP	Libtasn1	OpenCORE AMR	WinSparkle
Libgcrypt	libxml	p11-kit	zlib-ng
libgpg-error	Lz4	PCRE2	zstd

It’s package deployment pipelines all the way down

We have a lot of infrastructure dedicated to building Windows and macOS packages.

All but maybe 2 or 3 of the libraries in the previous slide have something similar. So…

…we have a whole separate infrastructure dedicated to building Windows and macOS libraries so so that we can deliver Windows and macOS packages.

Developer Time

Wireshark Is Healthy

Millions of lines of code …3.6M or maybe 6.7M?

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

~91% Windows, ~7% macOS …again, on the servers we manage

4100 Discord users

3100 protocols, 269k fields

2400 authors

2 yearly conferences

1 certification

Stratoshark

Stratoshark Updates

Raw Kubernetes audit, CloudTrail, and GCP audit logs

JSON view

Better Falco integration

Initial Procmon (needs additional work)

1.0 at some point

Wireshark Foundation

Certification

Wireshark is part of two ecosystems:

- The pcap ecosystem
- The “let’s keep modern civilization from collapsing” ecosystem

The foundation tries to help and foster both

Wireshark Certified Analyst

- Continues our goal of educating users
- Official recognition of your skills and knowledge
  - Helps you
  - Helps the project
  - Helps the foundation

SharkFest Europe Certification Specials

On-Site Exam (limited availability)

€159

Proctored Exam (Online/Exam Center)

€87 ($100) off exam

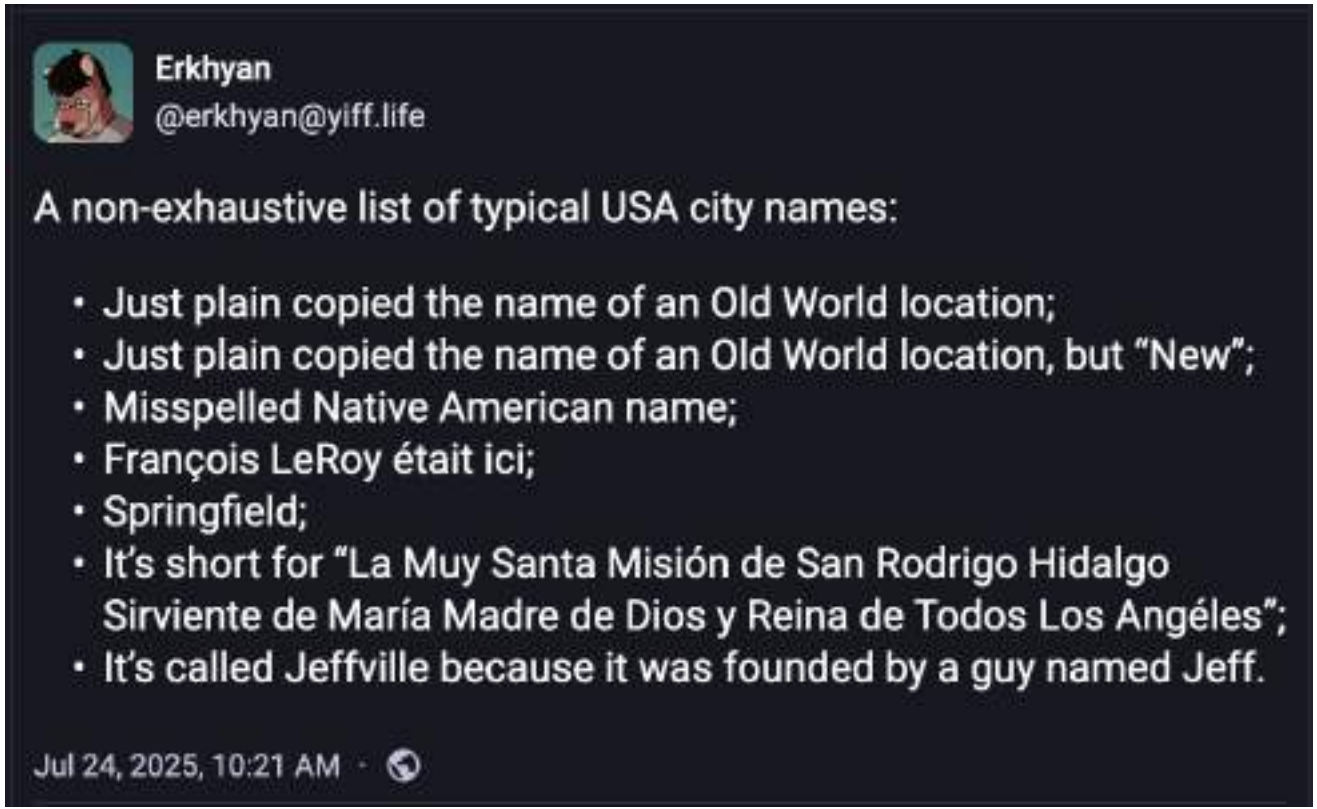
Coupon code: SFEU25

Thank You


SharkFest'25
EUROPE

Bonus Slides

There are 17 “Warsaw”s in the U.S.



Erkhyan
@erkhyan@yiff.life

A non-exhaustive list of typical USA city names:

- Just plain copied the name of an Old World location;
- Just plain copied the name of an Old World location, but “New”;
- Misspelled Native American name;
- François LeRoy était ici;
- Springfield;
- It’s short for “La Muy Santa Misión de San Rodrigo Hidalgo Sirviente de María Madre de Dios y Reina de Todos Los Angéles”;
- It’s called Jeffville because it was founded by a guy named Jeff.

Jul 24, 2025, 10:21 AM ·

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!

We Accumulate Interest

We rarely introduce big changes, but we've been around a while

However, a lot of little changes over time adds up

…and we've been around a *long* time

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"?

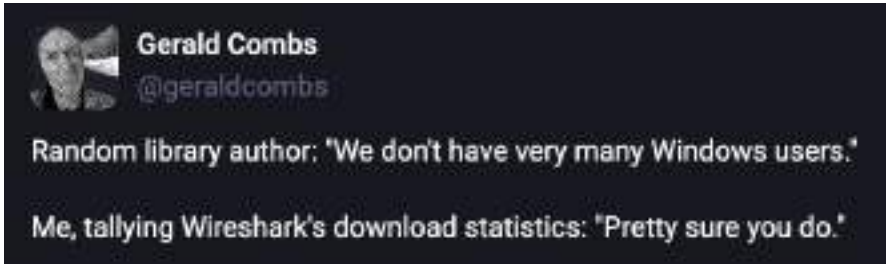
STRATOSHARK

Fixing This

C & C++ need one good obvious build system. We have several OK-ish ones.

C & C++ need one good obvious library packaging system. We have a couple of OK-ish ones. Perl, Python, Go, Rust, Zig, and others have plenty of good prior art worth stealing.

Projects need resources.



Quick Terminology

Build systems

Turn source code into executable code

Discover what system you're building for and find dependencies

In a restaurant this would be the back of the house: food prep, cooking, etc.

Package managers

Deliver built code to developers

In a restaurant this would be the front of the house: delivering dishes consistently and repeatably