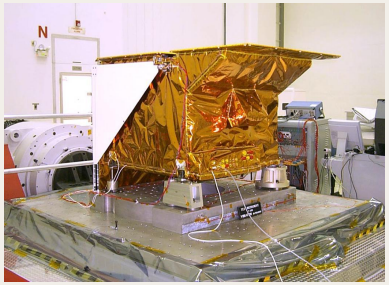
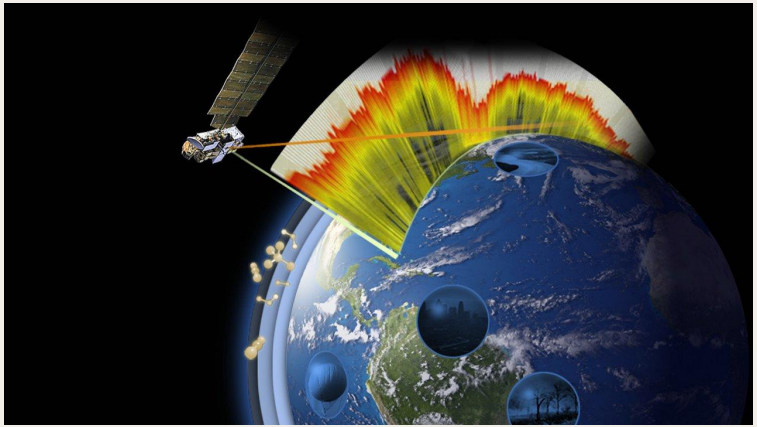
OpenSSL Foundation

State of the OpenSSL Community 3.6

Jon Ericson
Communities Manager
OpenSSL Foundation
October 7, 2025
Prague

My first dream job





The dream of processing data!

JPL D-41884

Earth Observing System (EOS)
Aura Spacecraft

Tropospheric Emission Spectrometer (TES)

Level 3 (L3) Data/Plot User's Guide

Version 1.0

December 17, 2007

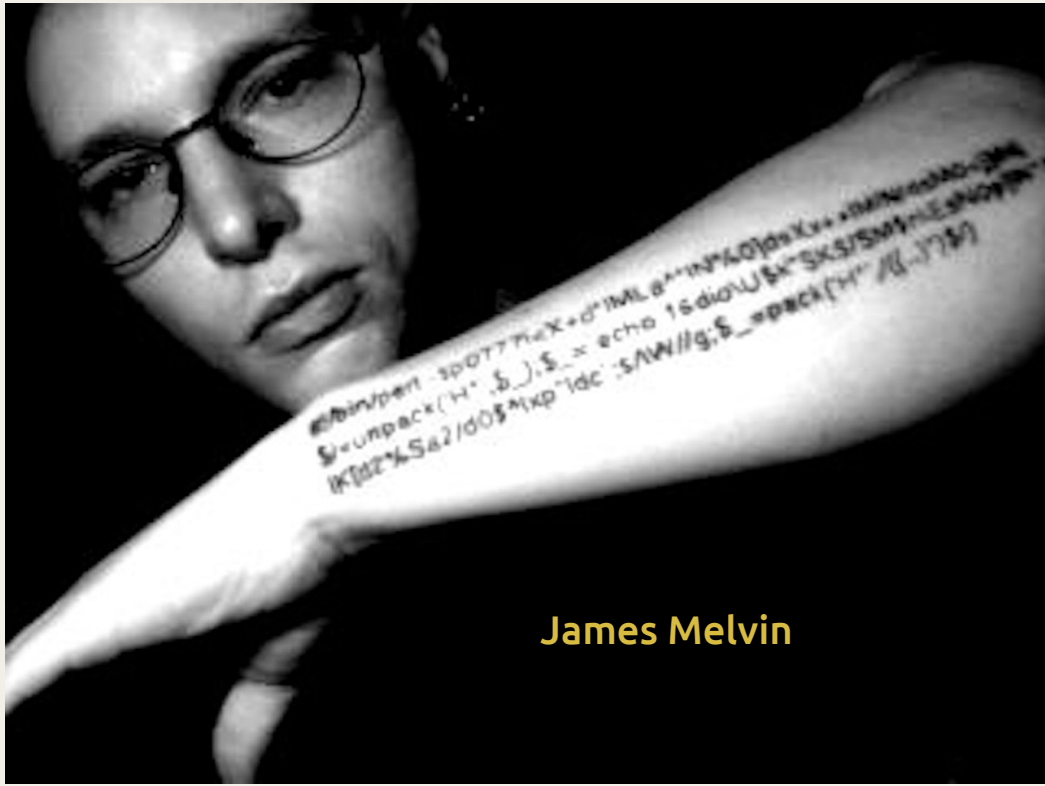
A cultural history

The OpenSSL Mission

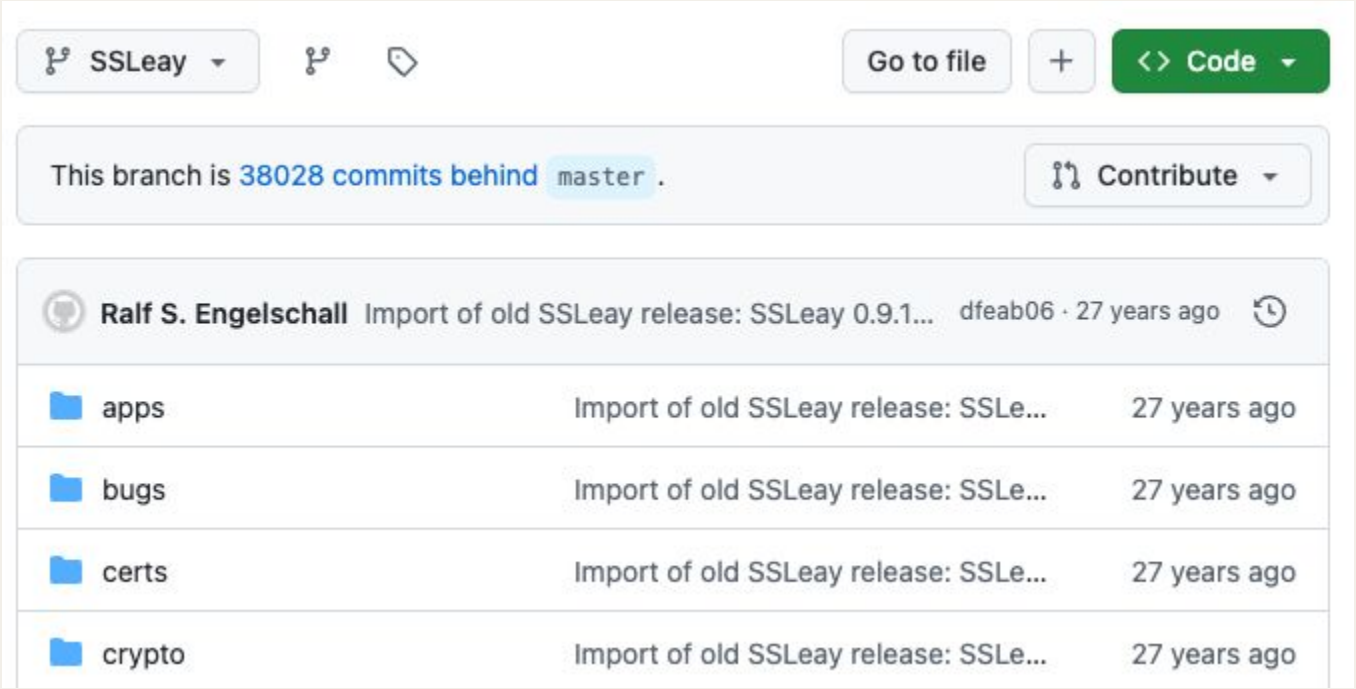
We believe **everyone** should have access to **security** and **privacy** tools, whoever they are, wherever they are or whatever their personal beliefs are, as a **fundamental human right**.

Arms


NETSCAPE NAVIGATOR™
Version 1.1
for Macintosh
US and Canada Only - Not For Export
N
NETSCAPE
Run "Installer" To Setup


James Melvin

SSLeay 0.9.1a 06-Jul-1998



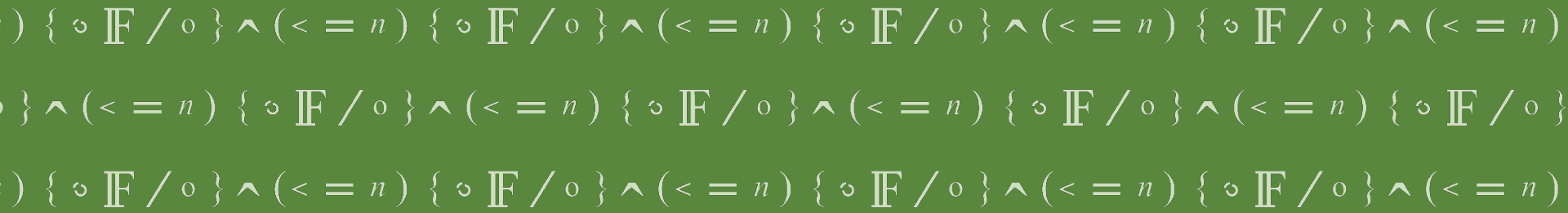
List: ssl-users
Subject: [ssl-users] ANNOUNCE: OpenSSL (Take 2)
From: Ben Laurie <ben () algroup ! co ! uk>
Date: 1999-01-06 22:03:02

```
  ___                   ____ ____  _
 / _ \ _ __  ___ _ __ / ___/ ___|| |     OpenSSL
| | | | '_ \/ _ \ '_ \\___ \___ \| |     The Open Source toolkit for SSL/TLS
| |_| | |_) | __/ | | |___) |__) | |___  http://www.openssl.org/
 \___/| .__/\___|_| |_|____/____/|_____|
_____ |_| ____________________________________________________________________
```

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, fully featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols with full-strength cryptography world-wide. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL tookit and its related documentation.

OpenSSL is based on the excellent SSLeay library developed by Eric A. Young and Tim J. Hudson. The OpenSSL toolkit is licensed under an Apache-style licence, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions.

Open culture won

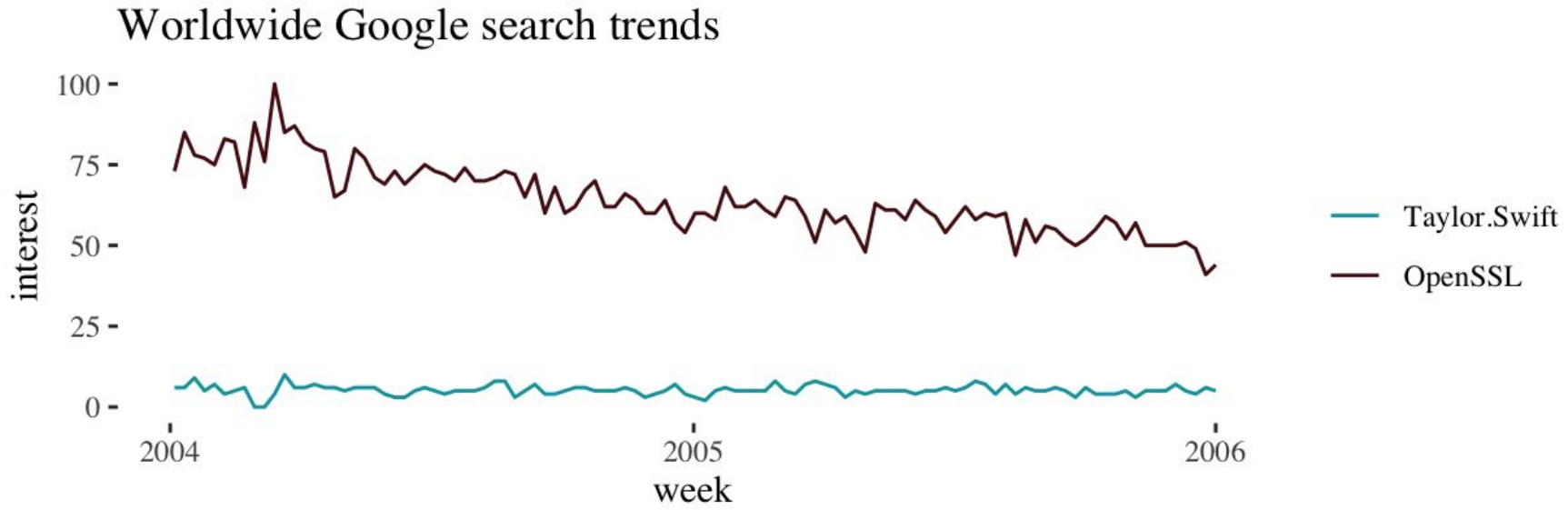


openSSL Foundation

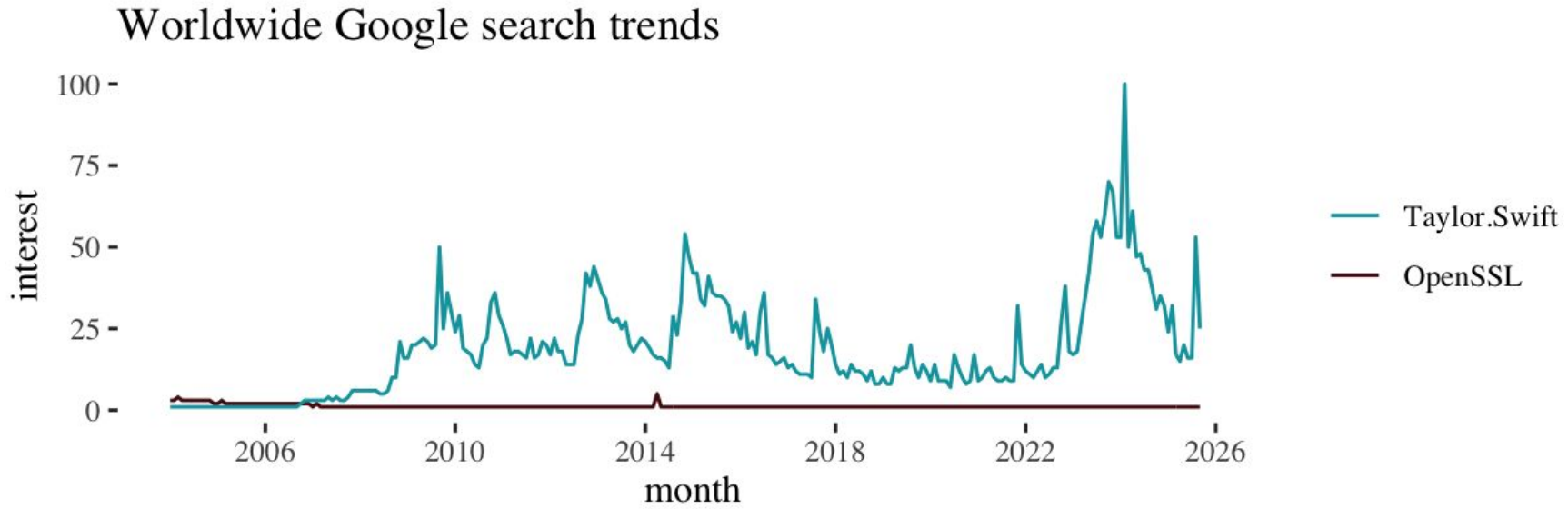
Reality check


MAD MEN
I DON'T THINK ABOUT YOU AT ALL.

More popular than Taylor Swift!



. . . before her first album



This conference is the rare place where we don’t need to explain what OpenSSL is

Developers *do* think about OpenSSL . . . if they need it for some reason


```
$ /usr/bin/openssl version
LibreSSL 3.3.6
```

```
$ brew install openssl
$ openssl version
OpenSSL 3.5.2 5 Aug 2025
(Library: OpenSSL 3.5.2 5 Aug 2025)
```

2150 of 7898 Homebrew Formulae depend on OpenSSL

Formula Install On Request Events (365 days)

/api/analytics/install-on-request/365d.json (JSON API)

Start Date: 2024-09-16

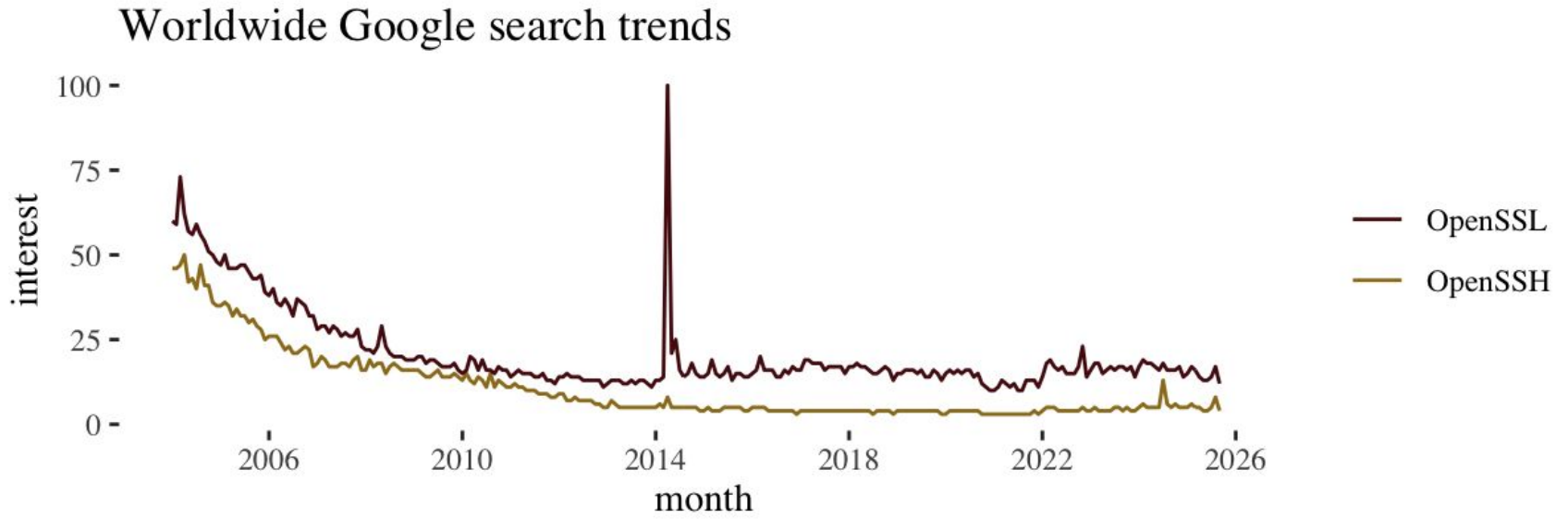
Total Events: 97179963

	Formula	Events	%
#1	node	2,324,716	2.39%
#2	awscli	2,048,067	2.11%
#3	gh	1,707,848	1.76%
#4	git	1,568,636	1.61%
#5	pyenv	1,429,823	1.47%
#6	ffmpeg	1,385,819	1.43%
#7	cmake	1,199,468	1.23%
#8	python@3.13		
#9	harfbuzz	983,758	1.01%
#10	glib	927,601	0.95%
#11	wget	870,251	0.90%
#12	go	859,670	0.88%
#13	python@3.12	804,758	0.83%
#14	imagemagick	788,918	0.81%
#15	openssl@3	776,877	0.80%

Depends on:

mpdecimal	4.0.1	Library for decimal floating point arithmetic
openssl@3	3.5.2	Cryptography and SSL/TLS Toolkit
sqlite	3.50.4	Command-line interface for SQLite
xz	5.8.1	General-purpose data compression with high compression ratio

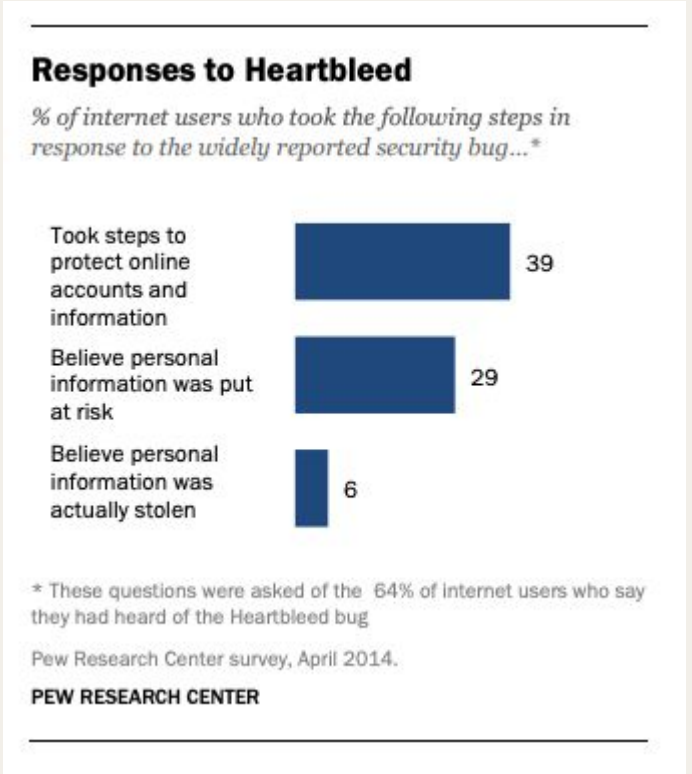
A closer comparison



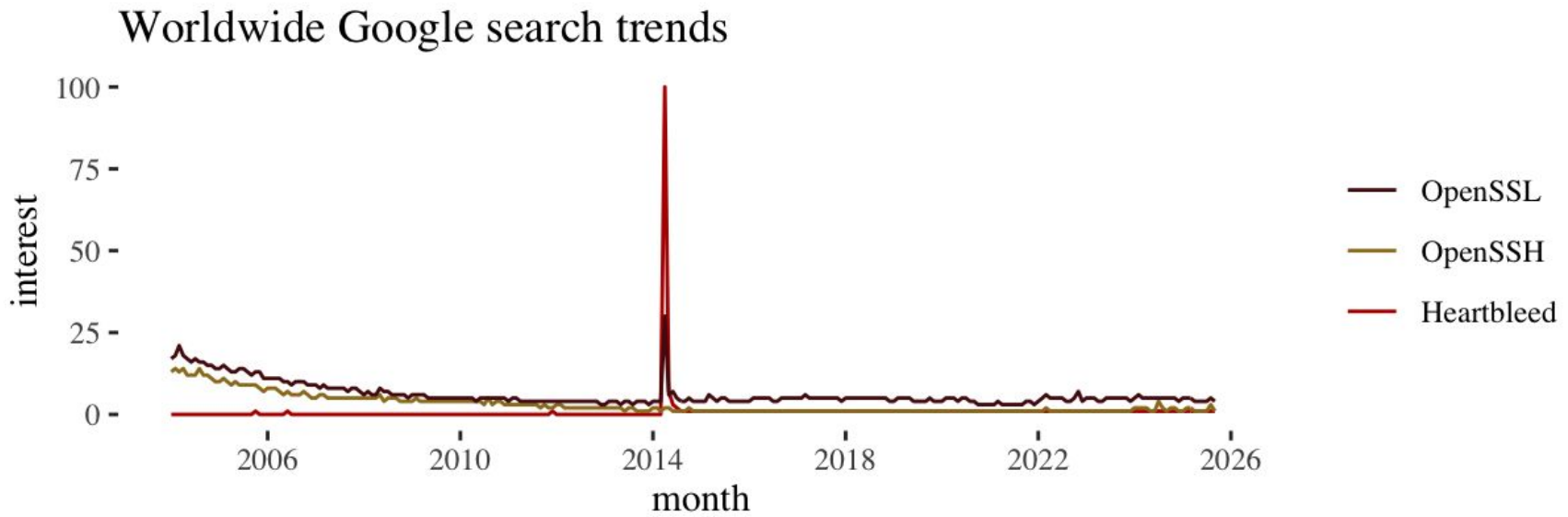
Heartbleed

"Heartbleed - the first buffer overflow bug with a website, a logo, and a marketing department."
– Stack Overflow Podcast
recorded Friday April 11, 2014

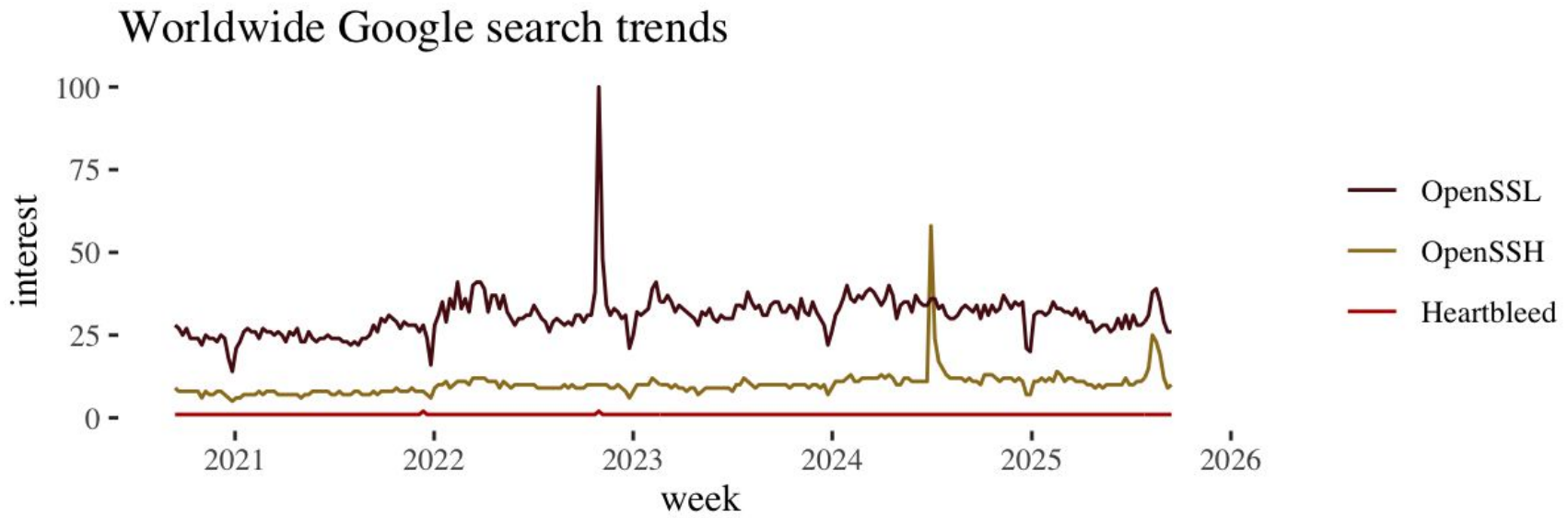
```
if (1 + 2 + payload + 16 > s->s3->rrec.length)
    return 0;
```



Heartbleed was a huge, but momentary blip

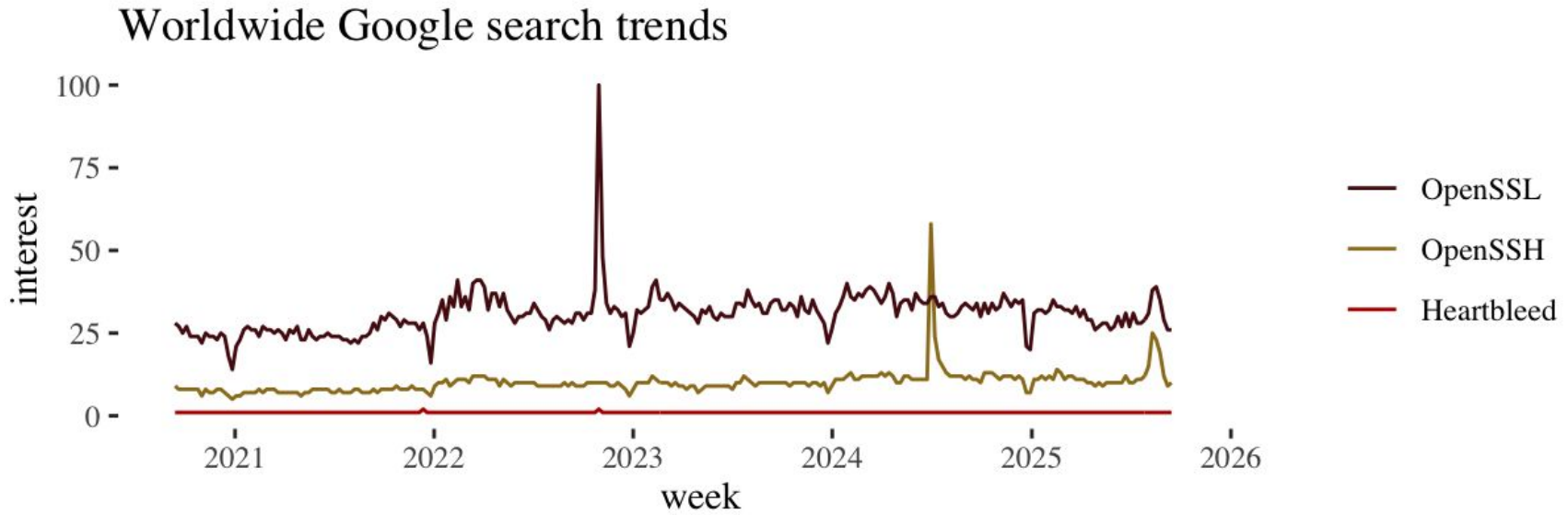


What happened in November, 2022?



Vulnerabilities put OpenSSL in the news

OpenSSH had its own moment in the sun



Post-quantum cryptography might be an exception

OpenSSL Foundation

The Features of 3.5: Post-quantum cryptography

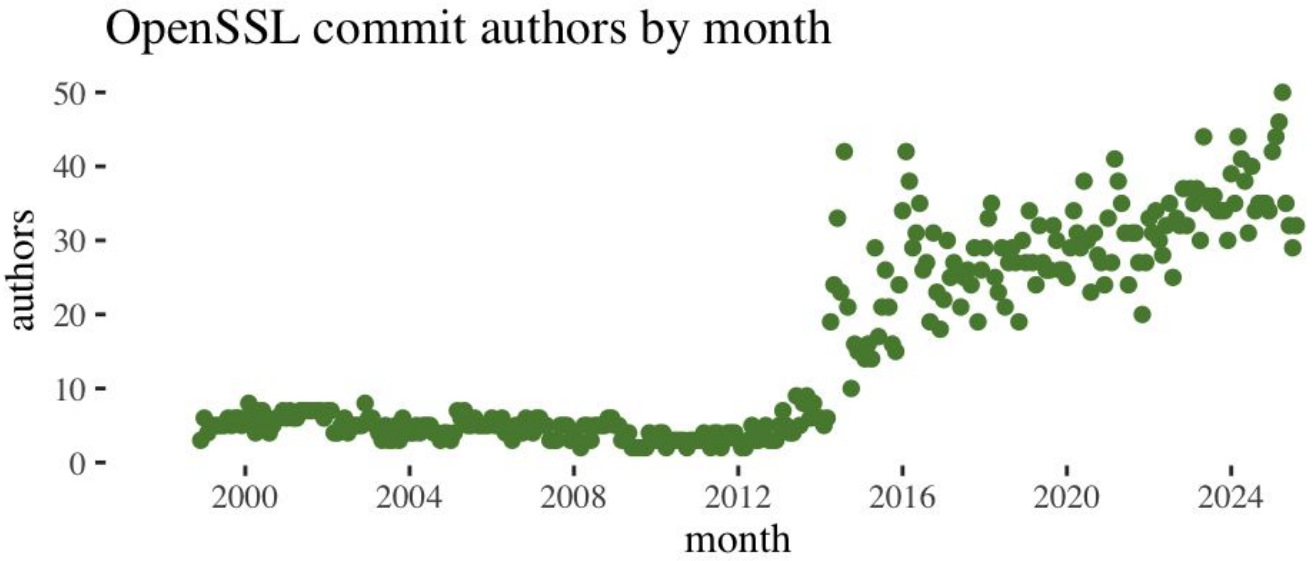
Apr 22, 2025

This is the third in a series of posts about the features of OpenSSL 3.5. Its target audience is people who are curious about internet security, but who don't recognize the acronyms in that list.

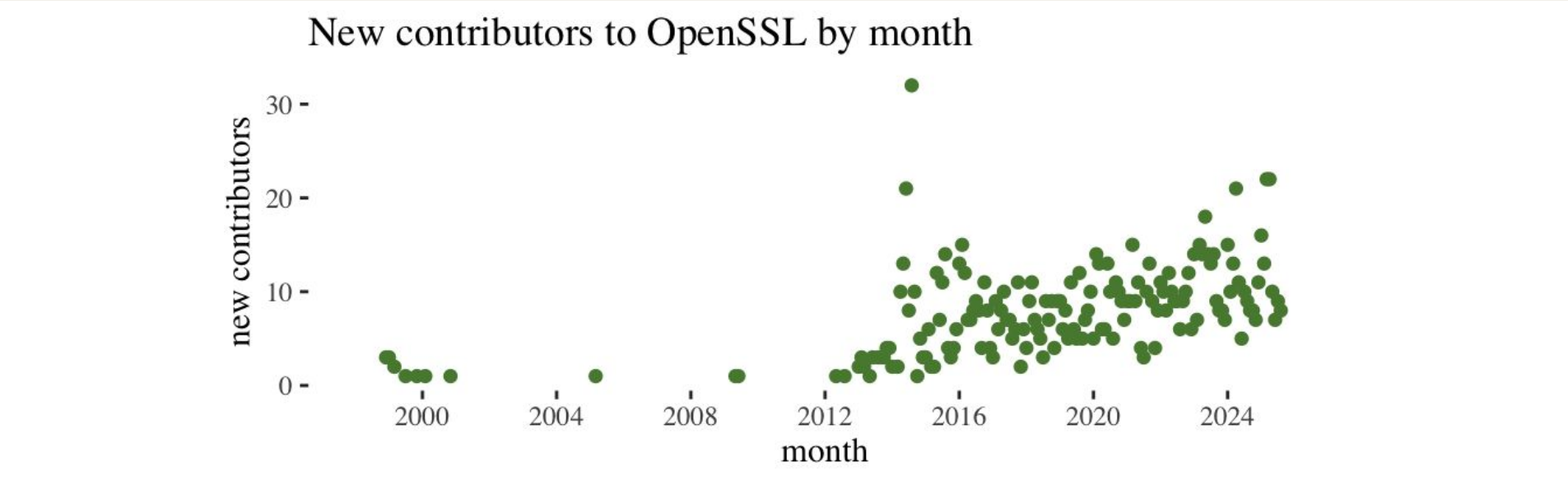
1. *QUIC server*
2. *External QUIC library interface*
3. *Post-quantum cryptography*
4. *Hybrid ML-KEM in TLS v1.3*
5. *EVP_SKEY*

Perspective inside of the community

1288 commit authors



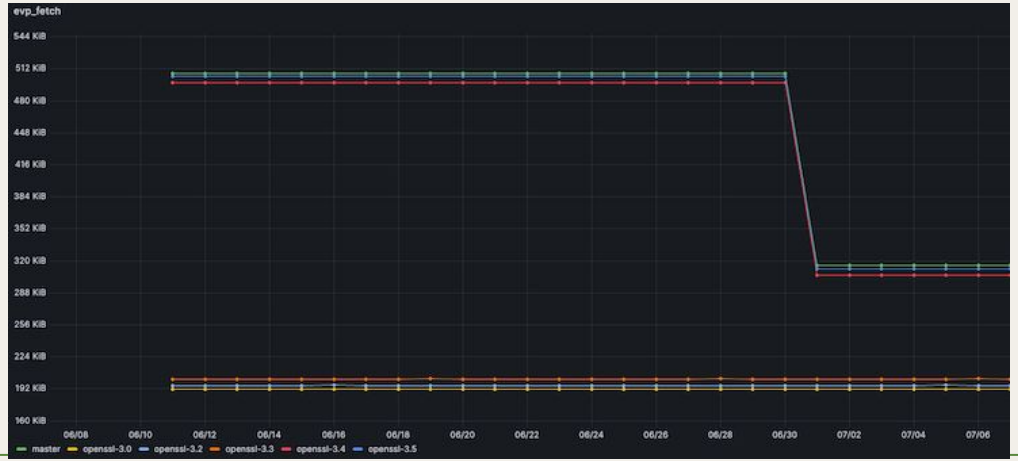
New contributors by month



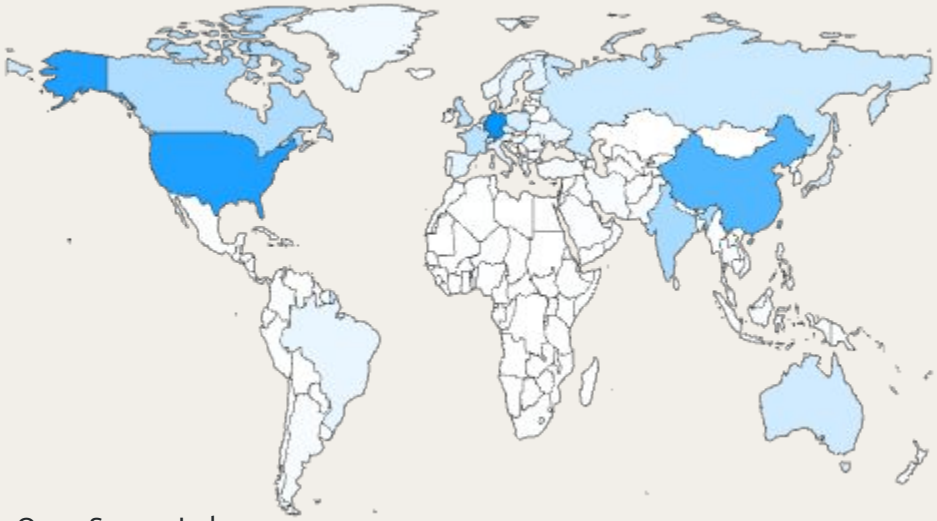
A first time pull request

```
#define NAMEMAP_HT_BUCKETS 2048
```

```
#define NAMEMAP_HT_BUCKETS 512
```



Where OpenSSL contributors come from



Unknown location
1,161 contributors • 78%

According to the Linux Foundation Open Source Index

19 Committers


Nicola Tuveri **romen**


Sashan


Richard Levitte **levitte**


Paul Yang **InfoHunter**


Neil Horman **nhorman**


Viktor Dukhovni **vdukhovni**


Kurt Roeckx **kroeckx**


Hugo Landau **hlandau**


David von Oheimb **DDvO**


Tomáš Mráz **t8m**


Tim Hudson **t-j-h**


Matt Caswell **mattcaswell**


Todd Short **tmshort**


Tom Cosgrove **tom-cosgrove-arm**

Dmitry Belyavskiy **beldmit**

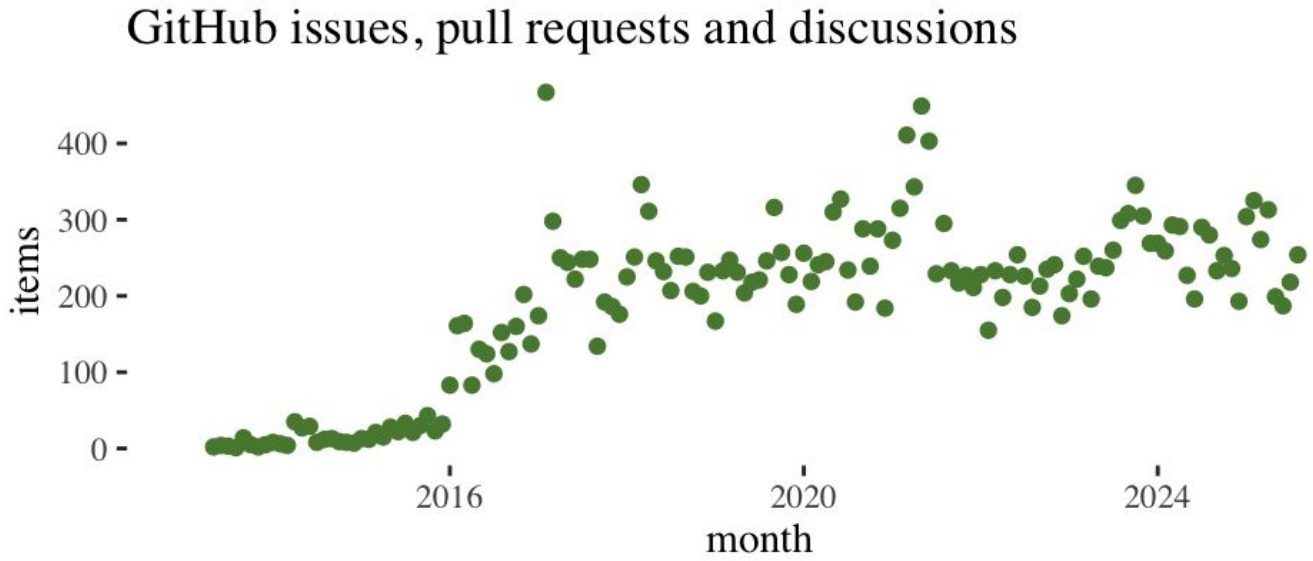

Bernd Edlinger **bernd-edlinger**


Pauli **paulidale**

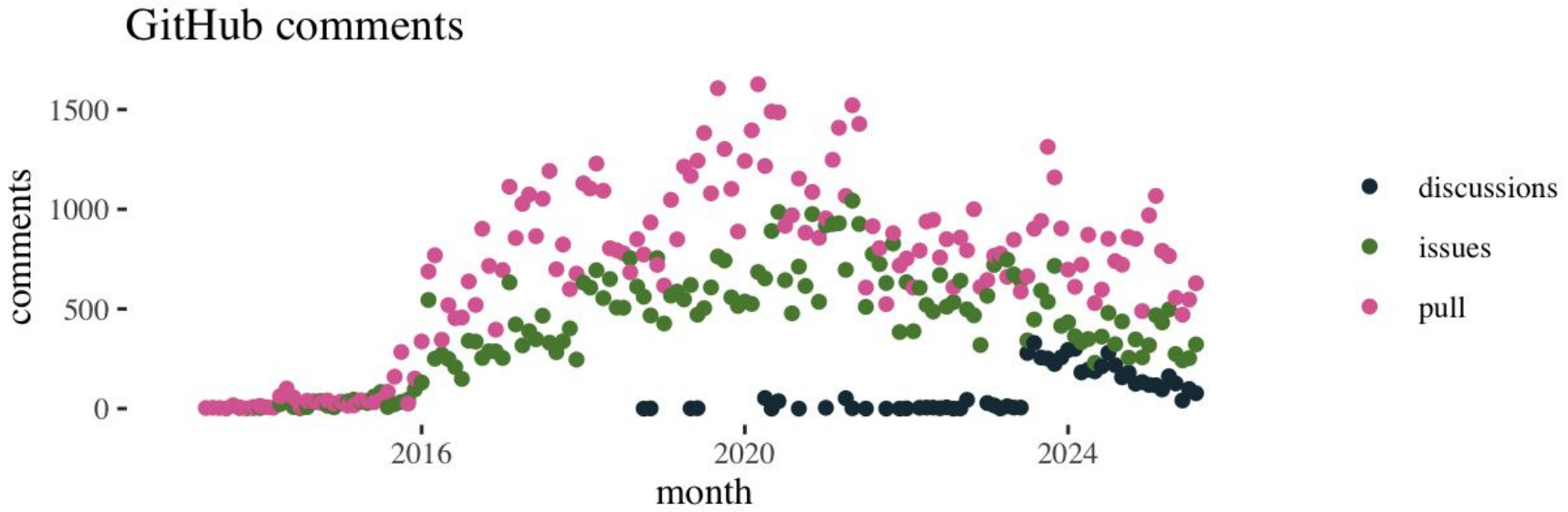

Shane **slontis**


fwh-dc

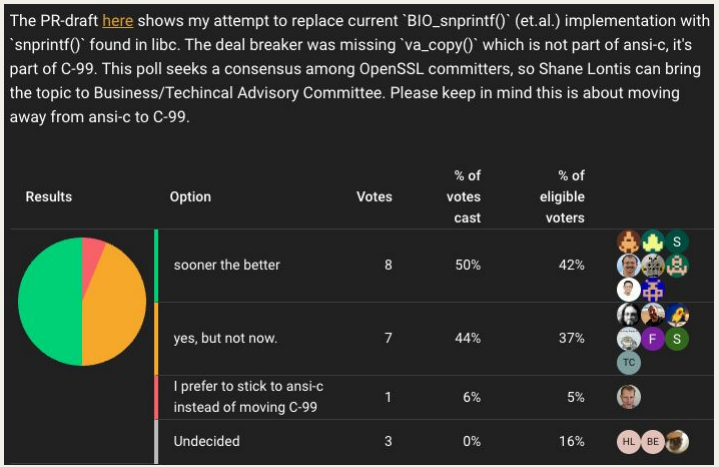
Where community happens



Interacting with each other



https://openssl-communities.org/hub/

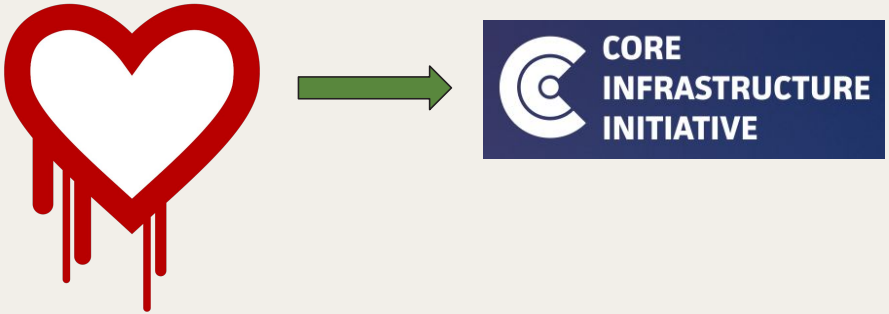


Individuals	140
Large Businesses	123
Small Businesses	55
Distributions	30
Academics	29
Committers	24
General Discussion	196*

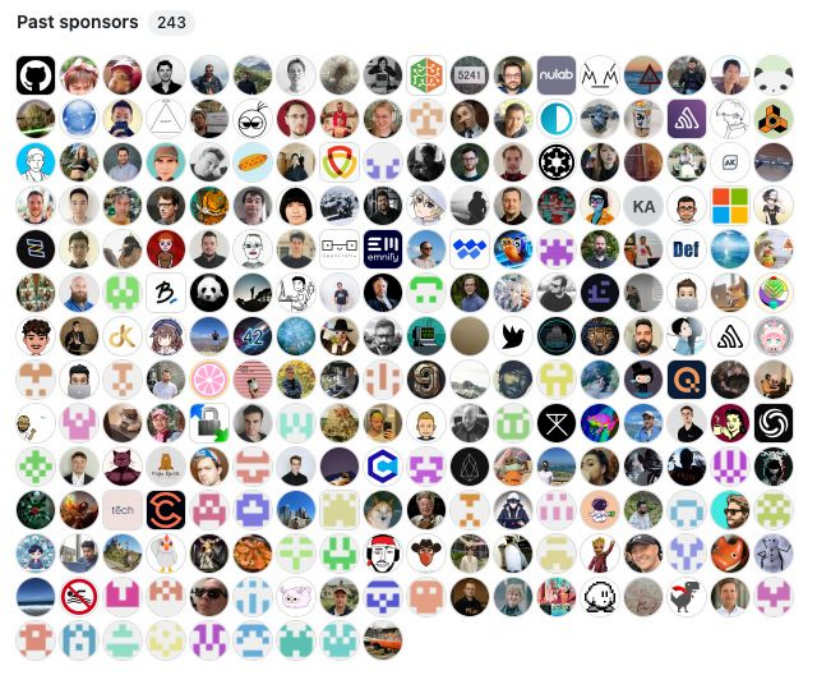
* I invited everyone from all the other groups to General Discussion

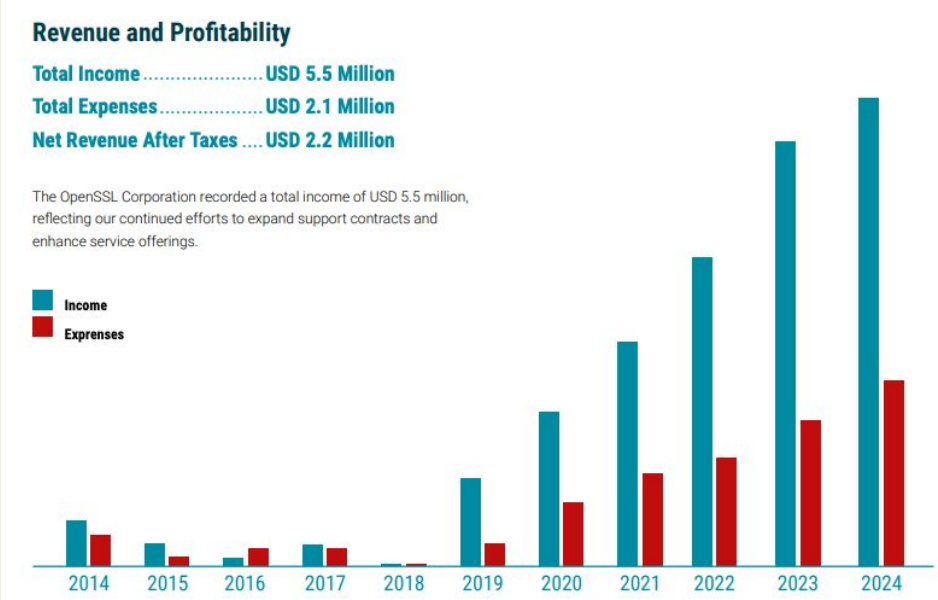
Started as a library/open source project

Heartbleed changed the way Open Source projects are funded

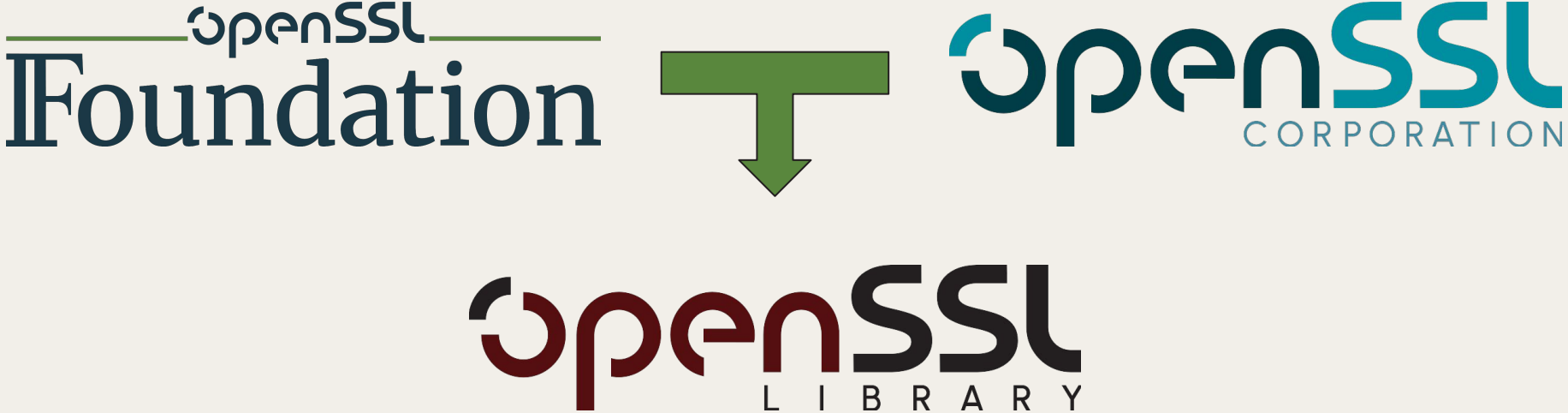


Commercial and non-commercial interests





Two independent organisations that co-manage the library



Thank you to our leading supporters!

PREMIER SUPPORTERS

OpenSSL CORPORATION

cisco

Sovereign Tech Fund

FLOSS/fund by ZERODHA

CODE PROTECTORS

Bloomberg

NetApp

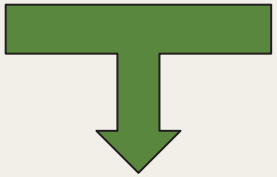
COMCAST

OpenSSL Foundation

The OpenSSL Foundation Mission

The OpenSSL Foundation works to ensure that everyone, including nonprofits, academics, and independent developers, has access to fundamental data privacy and security tools that are the backbone of internet protection, quietly safeguarding millions of users. We do this to help build a safer internet — one that **serves the public interest** and upholds privacy and security as foundational rights.

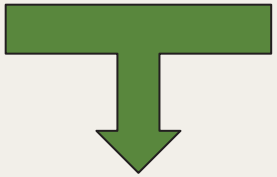
Connecting the Community to the Library



Advisory committees representing subcommunities

Business Advisory Committee (F-BAC)	Technical Advisory Committee (F-TAC)

Business Advisory Committee (C-BAC)	Technical Advisory Committee (C-TAC)



Where do we go from here?

Upcoming initiatives

Sovereign Tech Fund

- Constant-time BIGNUM to address potential side-channel attacks
- GitHub issue backlog

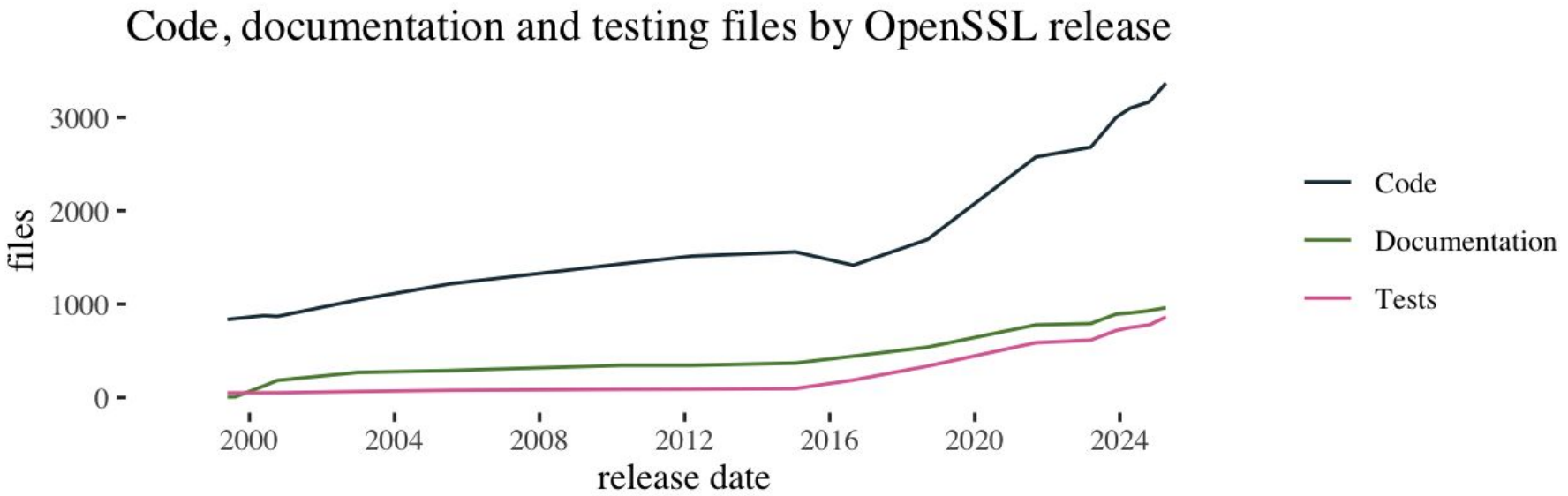
Ongoing

- DTLS 1.3
- Additional Post-Quantum Cryptography (PQC) work
- QUIC projects
- Encrypted Client Hello

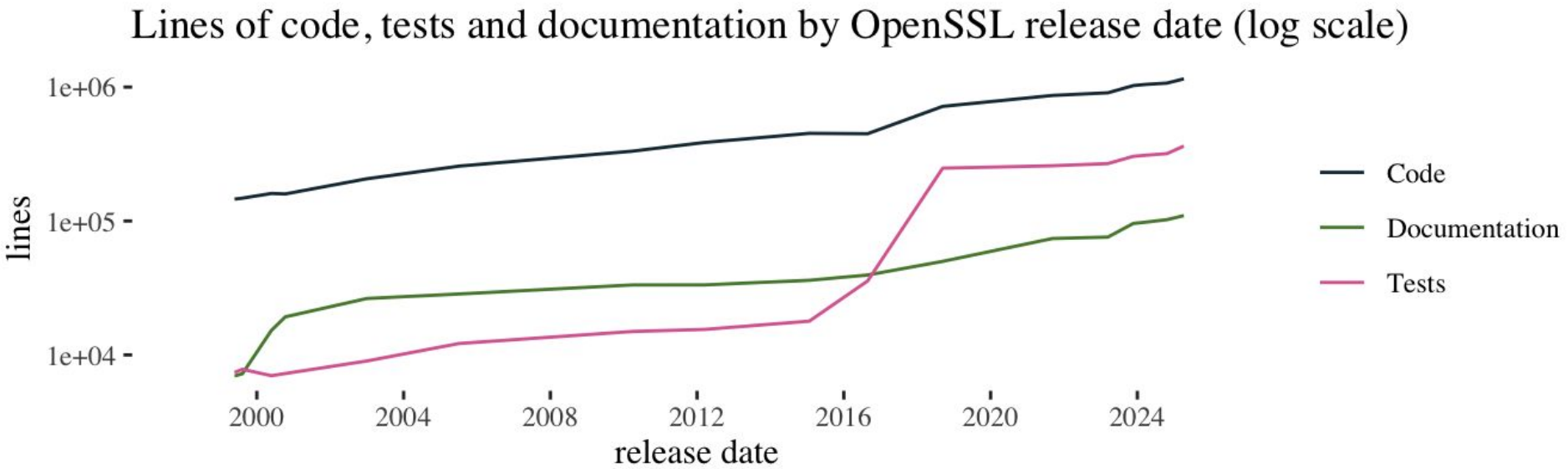
OpenSSL 4.0

- Remove deprecated features to simplify the code

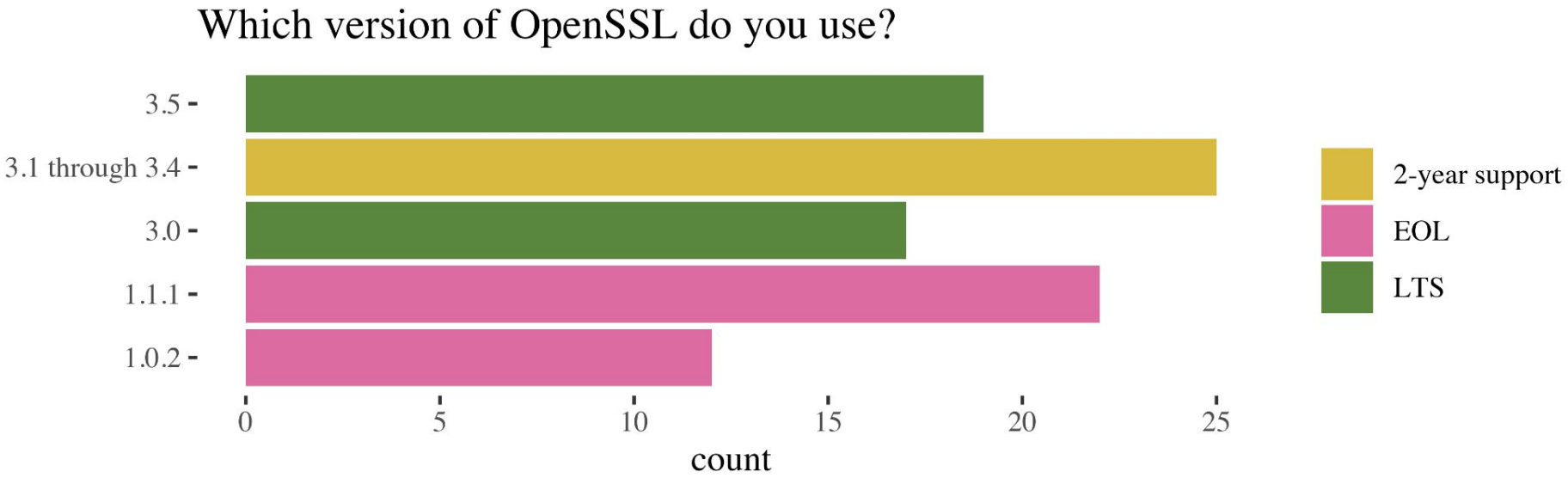
Increasing code, but lagging tests and documentation



Take with a grain of salt



Survey says!


Which version of OpenSSL do you use?
3.5
3.1 through 3.4
3.0
1.1.1
1.0.2
0
5
10
15
20
25
count
2-year support
EOL
LTS

Get involved!

- Take the survey
- Contribute
  - Code
  - Documentation
  - Tests
- Join a community
- Run for an advisory committee
- GitHub Sponsorship

Thank you to our leading supporters!

PREMIER SUPPORTERS

OpenSSL CORPORATION

cisco

Sovereign Tech Fund

FLOSS/fund by ZERODHA

CODE PROTECTORS

Bloomberg

NetApp

COMCAST

OpenSSL Foundation

Beyond this slide are random slides I didn't include for some reason. You probably don't need them.

Heartbleed changed the way OpenSSL is funded

Amazon Web Services, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, VMware and The Linux Foundation Form New Initiative to Support Critical Open Source Projects

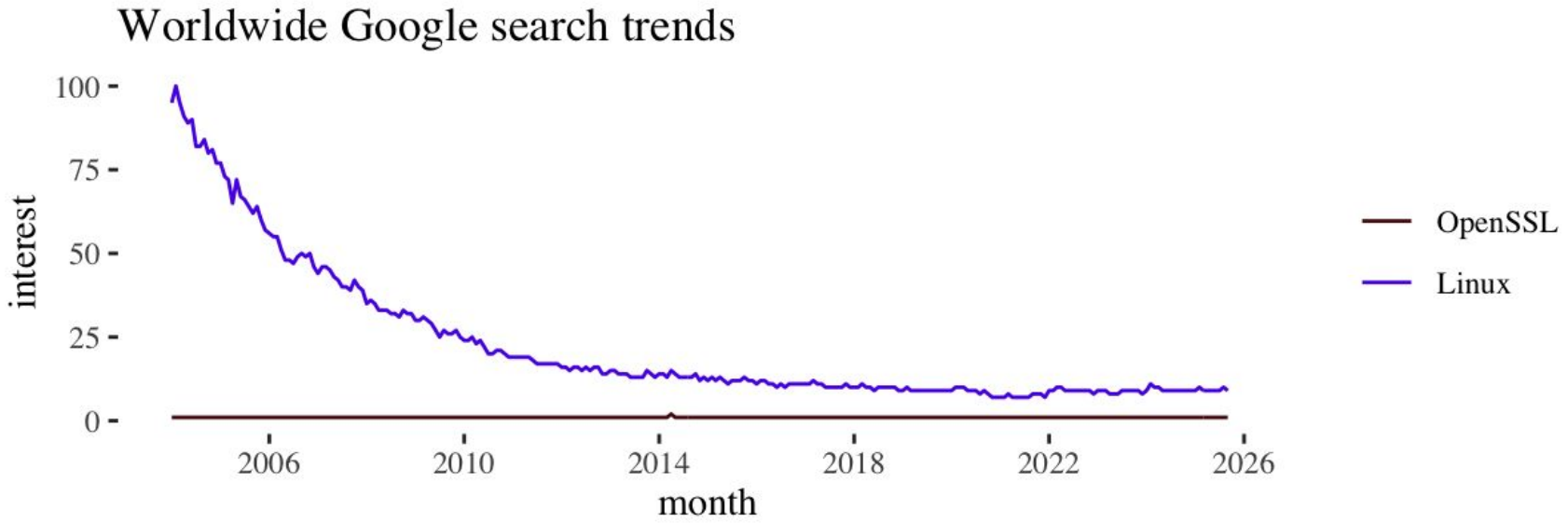
By linuxfoundationblank - April 24, 2014 - 4:00am

Newly formed Core Infrastructure Initiative is the industry's collective response to the Heartbleed crisis

SAN FRANCISCO, April 24, 2014 – The Linux Foundation today announced it has formed a new project to fund and support critical elements of the global information infrastructure. The Core Infrastructure Initiative enables technology companies to collaboratively identify and fund open source projects that are in need of assistance, while allowing the developers to continue their work under the community norms that have made open source so successful. Founding backers of the Initiative include Amazon Web Services, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, VMware and The Linux Foundation.

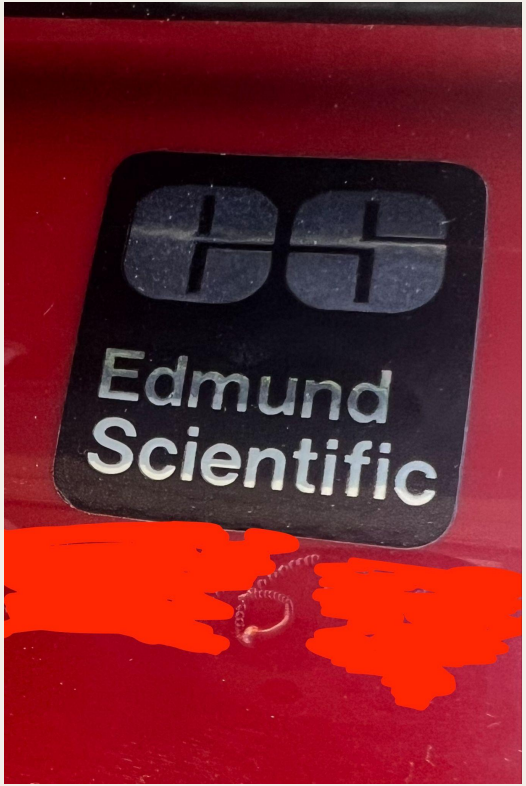
The first project under consideration to receive funds from the Initiative will be OpenSSL, which could receive fellowship funding for key developers as well as other resources to assist the project in improving its security, enabling outside reviews, and improving responsiveness to patch requests.

Relative, not absolute, interest

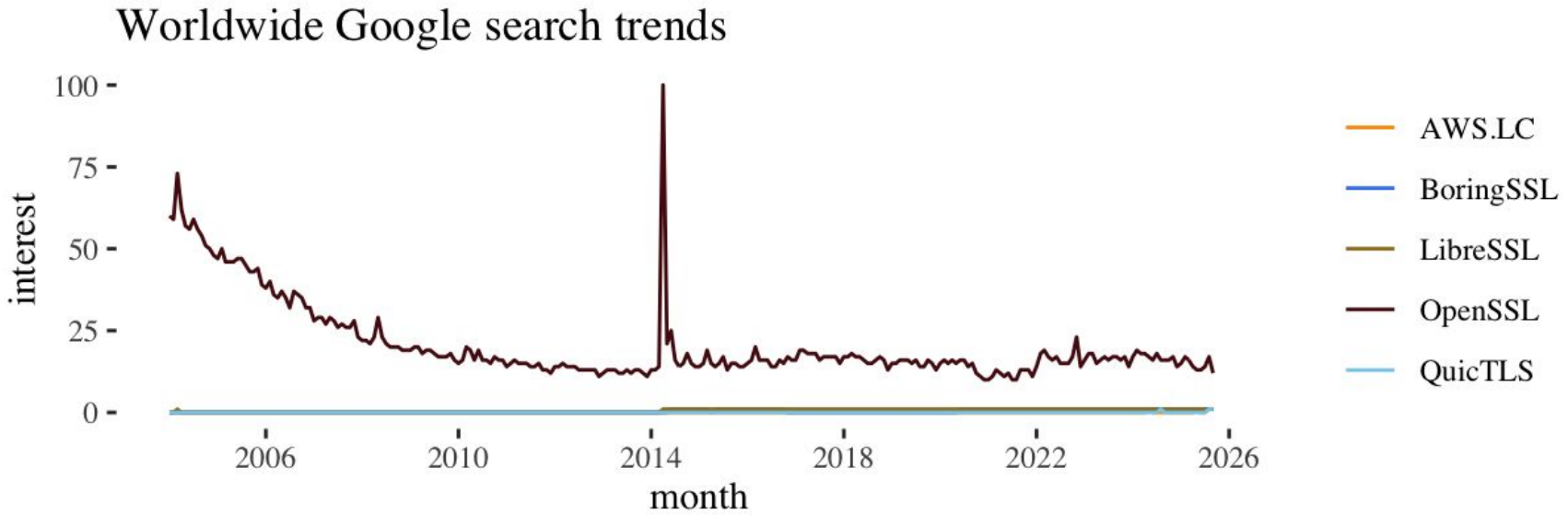


The OpenSSL governance community

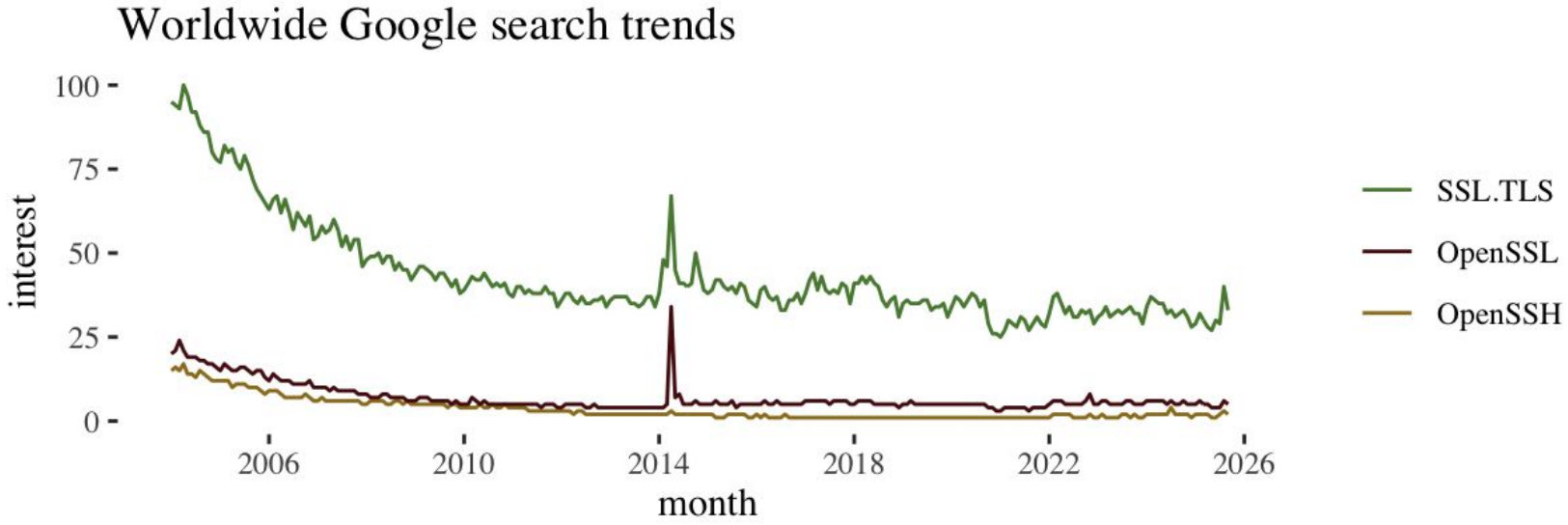
Who I am



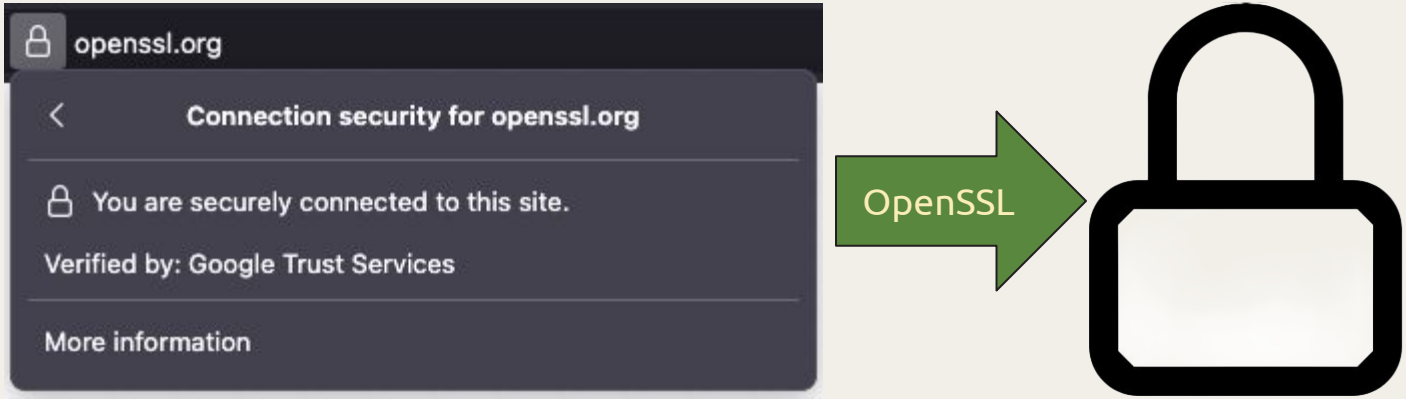
Forks


Worldwide Google search trends
interest
100
75
50
25
0
2006
2010
2014
2018
2022
2026
month
AWS.LC
BoringSSL
LibreSSL
OpenSSL
QuicTLS

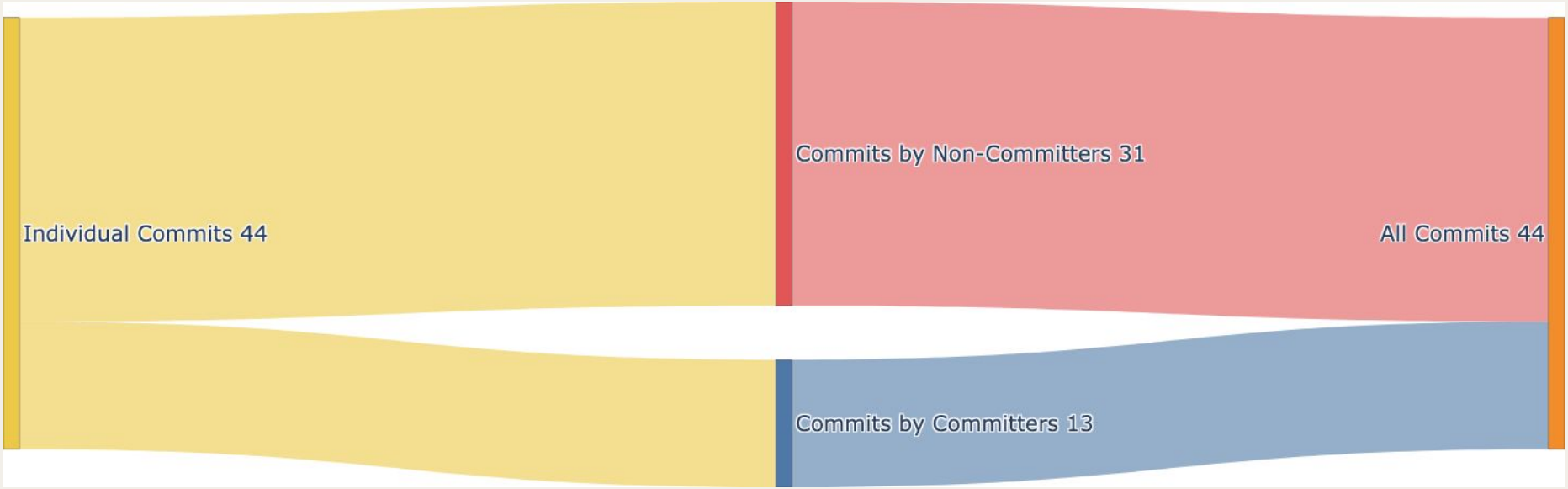
More useful comparisons



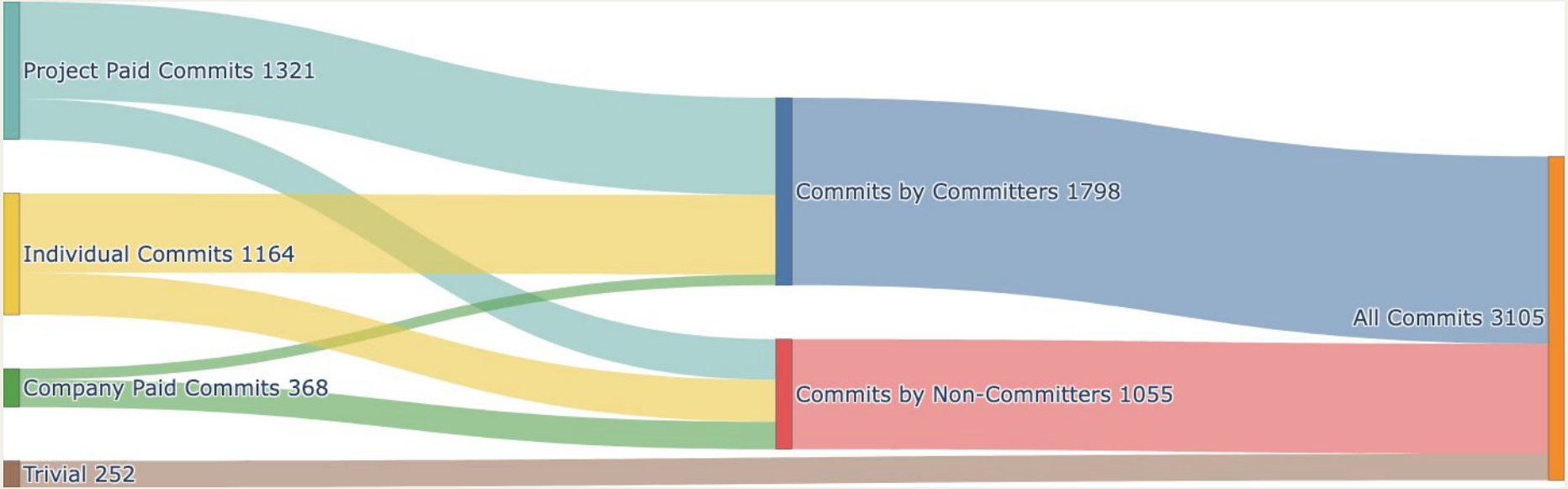
OpenSSL


openssl.org
Connection security for openssl.org
You are securely connected to this site.
Verified by: Google Trust Services
More information
OpenSSL

Commit summary from 1998



Commit summary for 2025



Just the forks