Wiresharkæology: How it started and where we’re headed

Gerald Combs

Director of Open Source Projects @ Sysdig

Creator of Wireshark

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

sysdig SECURE
EVERY
SECOND.

Who Am I?

Creator & lead developer of Wireshark

Co-creator of Stratoshark

CFO of the Wireshark Foundation

Director of Open Source Projects at Sysdig

Accidentally deleted the Kansas City Chiefs website that one time

Life at a Small ISP

“Can I have a Sniffer?” “No.”

“Can I have a Sniffer?” “No.”

“Can I have a Sniffer?” “No.”

“Can I at least have EtherPeek?” “No.”

“Fine. I'll just write one. This open source stuff seems nice enough.”

Original Goals

Look at packets on the network

Contribute back to 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

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

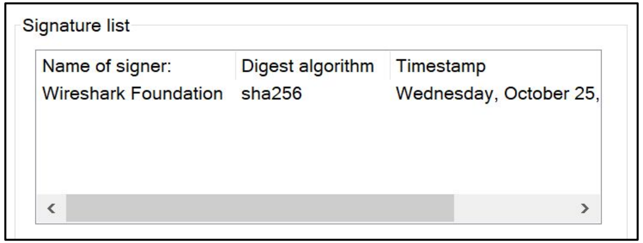
Getting to the Goal

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?



Signature list

Name of signer:	Digest algorithm	Timestamp
Wireshark Foundation	sha256	Wednesday, October 25,

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

Ethereal

WIRESHARK®

AirPcap

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

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/

Open Source Business Models

~~Use a project hosting service~~

~~Corporate overlord~~

~~Umbrella organization~~

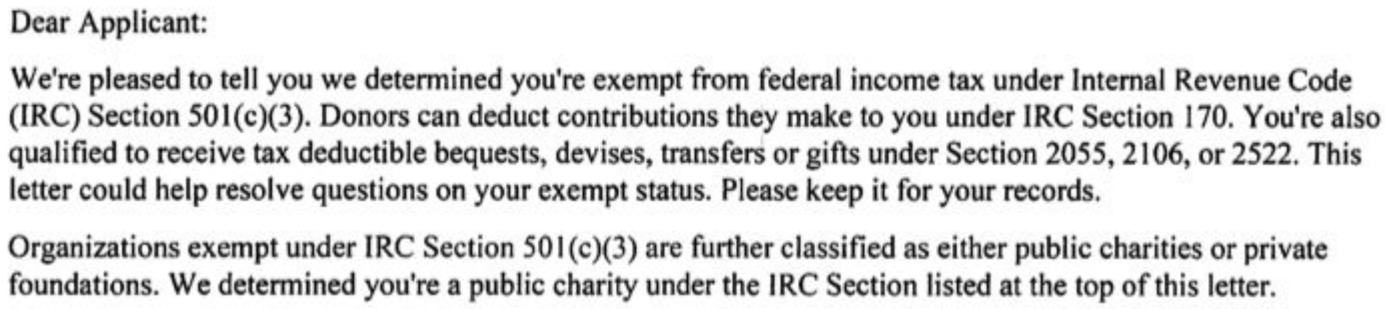
Independent not-for-profit

…so that is what we did

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

wiresharkfoundation.org

WIRESHARK
FOUNDATION



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.

Refining the Goal

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

What’s Next?

System calls! and logs!

STRATOSHARK

More SharkFests and other events!

More stuff which we’ll announce in few months

Thank You

Bonus Slides

Learning By Doing

“An expert is a person who has made all the mistakes that can be made in a very narrow field.”

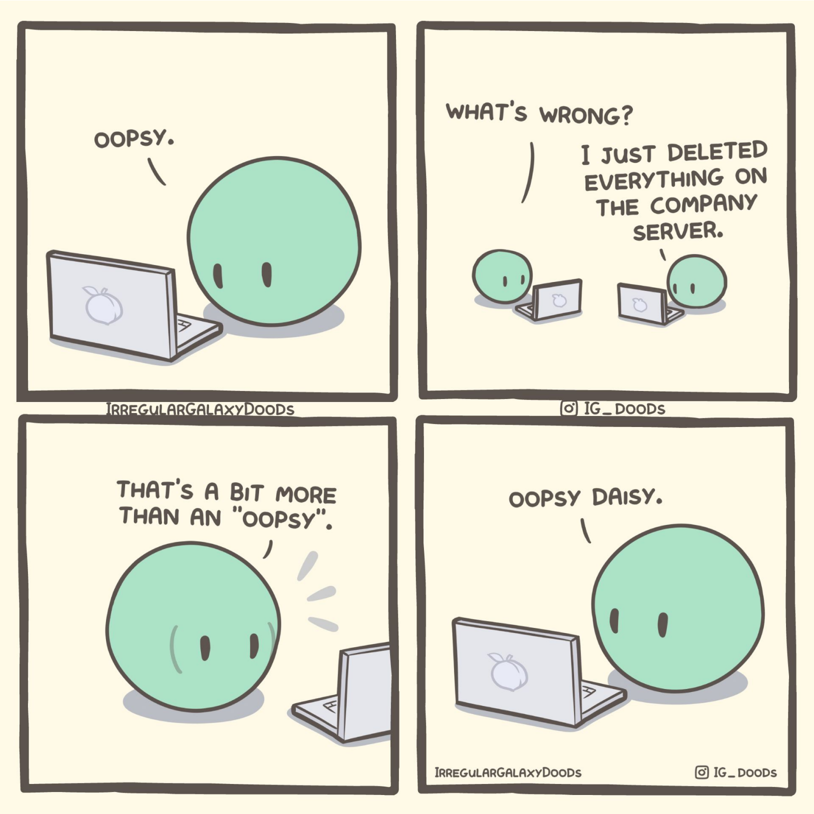
– Niels Bohr

Making Use of Mistakes

Quick (and often only) way to learn things

Can point you in the right direction

Keeps you humble



Early Career Mistakes

Deleted the Kansas City Chiefs website.

snmpwalked our core router.

Started an open source project, then bought a house.

Project Hosting: Second Try

Bought another server 600 MHz SPARCstation 20, 512 MB RAM

Asked my boss if I could put in in our data center

sgistuff.net/