The Search For Network Truths

Gerald Combs
Wireshark Foundation
The State Of Wireshark
Next Release

Next major release: 3.6

Some time soon-ish?
New In 3.6

Better documentation thanks to the Google Season of Docs

Better git dissector thanks to Outreachy

RTP player updates

macOS Apple Silicon installer (soon, we hope)
Statistics

> 1M Downloads / month ...on the servers we manage

90-ish% Windows, 69% Win64 ...mostly due to automatic updates

2650 protocols, 221k fields

> 1900 authors

3M lines of code. Or maybe 4.7?
Network Truths
“Revelation of the truth should be the undergirding of all meaningful work.”

— Kristin Dow
Ceci n'est pas une packet
A Minimal Network Analyzer

packets := open_interface(interface_name);
for each packet in packets {
    print (timestamp);
    print (hex_dump(packet));
}
Hex Dumps Aren’t Enough

Details: Protocol analyzers, IDSes

Summary: Flow monitors & analyzers

Interaction: Port scanners & replay
Helping People Avoid Hex Dumps

Packets

Blobs of bytes

Dissected fields

Features

BPF Filters

Display Filters

You, The All-Important User
It’s More Than Hex Dumps

Goal: Help people run away from hex dumps

Goal: To help as many people as possible to understand their networks as much as possible
Getting To The Goal

Provide lots of details about lots of protocols

Provide context and identify relationships

Run on lots of systems

Integrate with other tools
How Did We Get Here?

Open source helps

So does having a great community
Removing Friction

Make sure Wireshark is easy to obtain

Make sure developers have tools they need

Make sure community can operate
Wireshark Isn’t Enough

We aren’t

• An IDS
• A port scanner
• A long-term monitoring tool
• A high-volume monitoring tool
...and that’s fine!
Wireshark *Still* Isn’t Enough

We show as much detail as we can

It’s up to you to interpret that

That’s where SharkFest comes in
Getting The Most Out Of SharkFest

If this were a physical event you could:

Attend talks
Talk to each other & to the sponsors
Stop by the Developer Den & other rooms
Do the challenges

Since this is a virtual event, you’ll have to settle for the following:

Attend talks
Talk to each other & to the sponsors
Stop by the Developer Den & other rooms
Do the challenges
Hollywood Hacking

Hollywood Hacking is when some sort of convoluted metaphor is used not only to describe hacking, but actually to put it into practice. Characters will come up with rubbish like, "Extinguish the firewall!" and "I'll use the Millennium Bug to launch an Overclocking Attack on the whole Internet!" - even hacking light switches and electric razors, which is even sillier if said electric razor is unplugged. The intent is to employ a form of Artistic License or hand waving which takes advantage of presumed technophobia among the audience. You can also expect this trope to annoy those within the audience whose occupation involves computers or the Internet.

https://tvtropes.org/pmwiki/pmwiki.php/Main/HollywoodHacking
## Hollywood vs Reality

<table>
<thead>
<tr>
<th>Tool</th>
<th>LoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brim</td>
<td>83561</td>
</tr>
<tr>
<td>Kismet</td>
<td>1028238</td>
</tr>
<tr>
<td>Nmap</td>
<td>781262</td>
</tr>
<tr>
<td>ntopng</td>
<td>883664</td>
</tr>
<tr>
<td>Scapy</td>
<td>169971</td>
</tr>
<tr>
<td>Snort</td>
<td>483634</td>
</tr>
<tr>
<td>tcpdump</td>
<td>121150</td>
</tr>
<tr>
<td>Wireshark</td>
<td>5424249</td>
</tr>
<tr>
<td>Zeek</td>
<td>185854</td>
</tr>
</tbody>
</table>

LoC of main repository, measured using tokei
Joy In Truth
What You Do Is Important

“Software is eating the world.”
  – Marc Andreessen

“The network is always up, fast, and secure, right?”
  – Everyone writing that software
Thank You
Questions?
Bonus Slides
Correcting Ourselves

commit 4628dc0118
Author: Gerald Combs <gerald@wireshark.org>
Date:   Wed Apr 16 13:23:04 2014 -0700

Disable transport name resolution by default.

Modern hosts typically open many more TCP and UDP connections than in years past. For an example opening a popular news site in a web browser can easily trigger dozens of separate connections. At the same time our services file has accumulated a lot of cruft over time. As a result transport name resolution is a bunch of lies.
Keep Practicing