

# SharkFest '16

## Network Baselineing with Wireshark

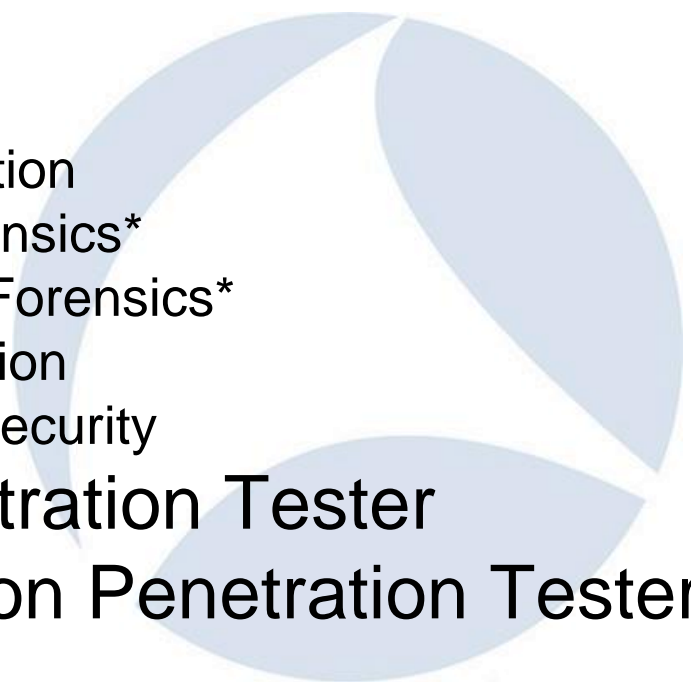
14 June 2016



Jon Ford

Jack of All | MainNerve llc.

# Jack of All

- **US Marine Corps**
    - 1998 - 2007
  - **Instructor**
    - Wireless Exploitation
    - Basic Digital Forensics\*
    - Basic Cellphone Forensics\*
    - Network Exploitation
    - Personal Cyber Security
  - **Network Penetration Tester**
  - **Web Application Penetration Tester**
- 

# Creating a Baseline with Wireshark



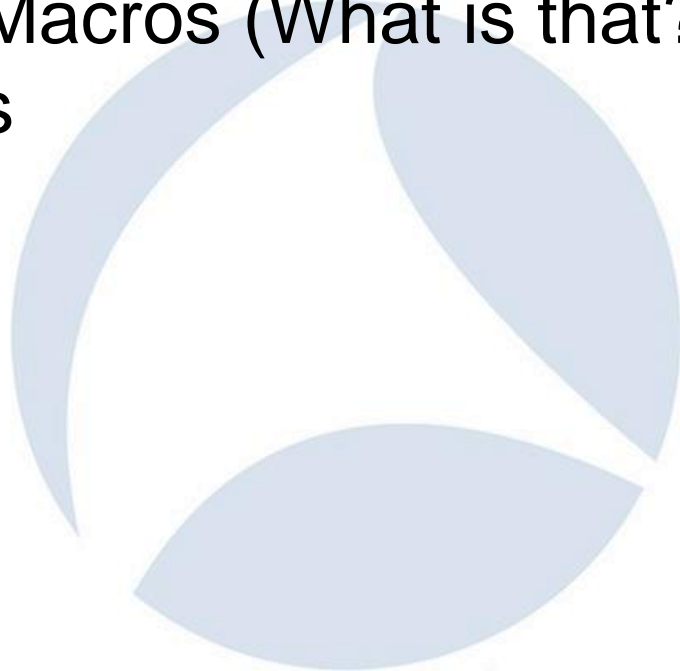
The Wireshark logo is a circular emblem composed of three overlapping, teardrop-shaped segments in a light blue color, arranged in a triangular pattern. The text "Wireshark's Built in Features" is centered over the logo in a dark blue, sans-serif font.

# Wireshark's Built in Features

SharkFest '16 • Computer History Museum • June 13-16, 2016

# Wireshark Features

- Display Filter (and – the Quick Button)
- Display Filter Macros (What is that?)
- Coloring Rules
- Statistics
- GeoIP\*



# Filters

Most of us will use a filter to filter in what we want to see not what we don't, because we know what we want to see.

The idea behind a baseline is to create a filter to hide what we know is ok or trusted so the bad guys can't hide.

# Display Filter

- Valid Filter Fields

- <https://www.wireshark.org/docs/dfref/> <https://goo.gl/uut6kM>

- Examples

- ip.addr
- ip.geoip.asnum
- ip.geoip.country



# Display Filter Macros

- What is a Display Filter Macro?
  - `${FilterName}`
- Filter to Isolate, First.
- Example:
  - `!( arp ) && !( llmnr ) && ( ip.addr == 67.325.123.122 )`
  - Ensure that all you see is packets to or from 67.325.123.122
  - Now add the NOT
  - `!( arp ) && !( llmnr ) && !( ip.addr == 67.325.123.122 )`
  - This will prevent you from filtering out more than you want



# Coloring Rules

- Black out trusted packets
  - Comparison of Trusted vs Unverified packet use
- Color code based upon country of origin
  - 660K character Rule of `ip.addr == NETBLOCK/BITMASK*`
  - <https://www.ripe.net/participate/member-support/info/list-of-members/list-of-country-codes-and-rirs> <https://goo.gl/W2ZdUf>
  - ( `ip.geoip.country == Italy` )
    - Case Sensitive

# Statistics

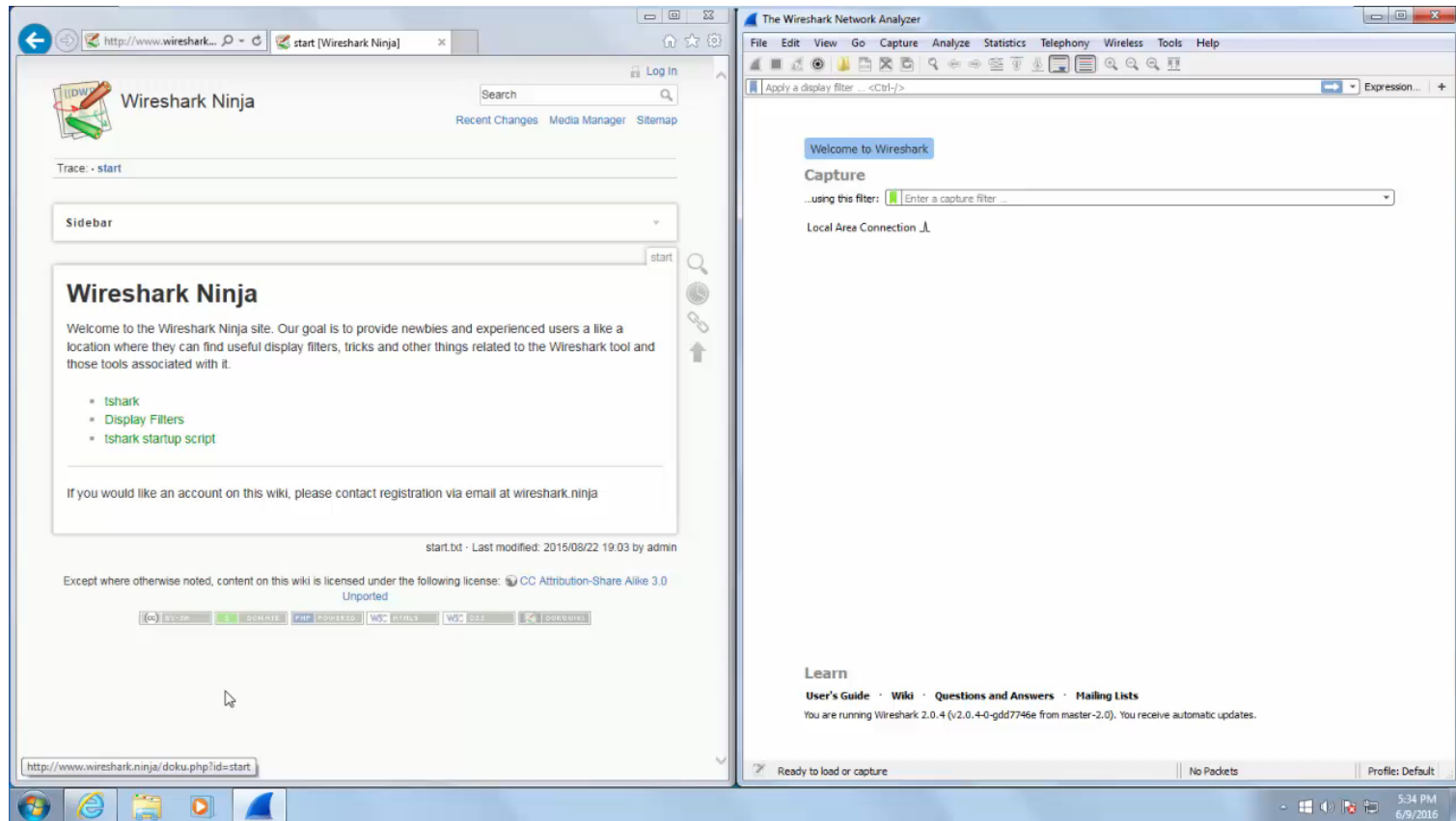
- Conversations
- Endpoints
- Destinations and Ports
- All IP Addresses



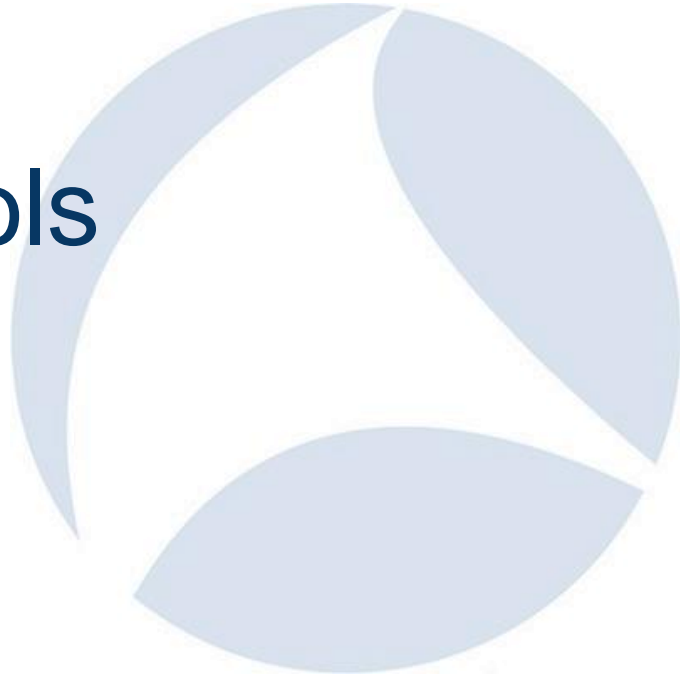
# GeoIP

- Country
- ASN
- Lat/Long
- Other (Paid For Databases)
- <https://wiki.wireshark.org/HowToUseGeoIP>

# GeoIP and Wireshark



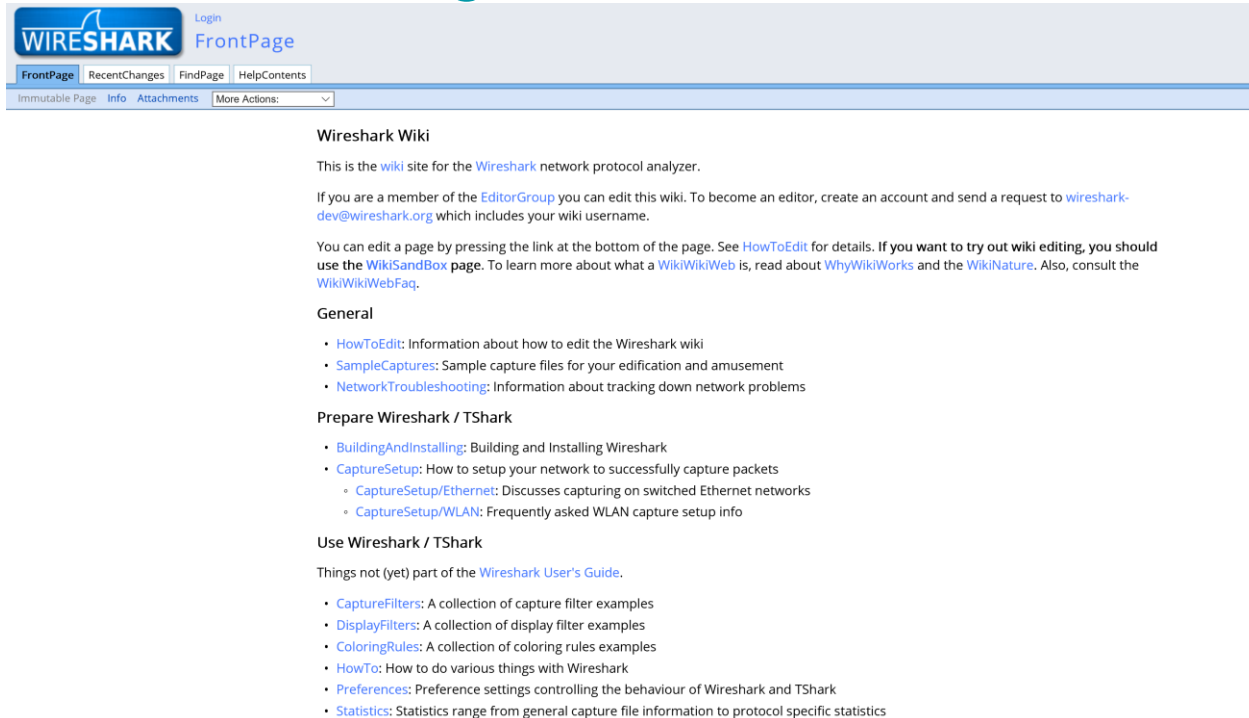
# Online Tools



# Wireshark Wiki

- <https://wiki.wireshark.org>

- Duh!



The screenshot shows the top portion of the Wireshark Wiki website. At the top left is the Wireshark logo. To its right are links for 'Login' and 'FrontPage'. Below these are navigation tabs: 'FrontPage', 'RecentChanges', 'FindPage', and 'HelpContents'. A secondary row of tabs includes 'Immutable Page', 'Info', 'Attachments', and a 'More Actions:' dropdown menu. The main content area begins with the heading 'Wireshark Wiki' followed by a paragraph explaining the site's purpose. Below this is a paragraph about editing the wiki, mentioning the 'EditorGroup' and providing an email address. A third paragraph explains how to edit a page, mentioning 'HowToEdit', 'WikiSandBox', 'WikiWikiWeb', 'WhyWikiWorks', and 'WikiNature'. The 'General' section follows, containing a bulleted list of links: 'HowToEdit', 'SampleCaptures', and 'NetworkTroubleshooting'. The 'Prepare Wireshark / TShark' section contains a bulleted list: 'BuildingAndInstalling', 'CaptureSetup', and 'CaptureSetup/WLAN'. The 'Use Wireshark / TShark' section contains a paragraph about the 'Wireshark User's Guide' and a bulleted list: 'CaptureFilters', 'DisplayFilters', 'ColoringRules', 'HowTo', 'Preferences', and 'Statistics'.

**Wireshark Wiki**

This is the [wiki](#) site for the [Wireshark](#) network protocol analyzer.

If you are a member of the [EditorGroup](#) you can edit this wiki. To become an editor, create an account and send a request to [wiresark-dev@wireshark.org](mailto:wiresark-dev@wireshark.org) which includes your wiki username.

You can edit a page by pressing the link at the bottom of the page. See [HowToEdit](#) for details. If you want to try out wiki editing, you should use the [WikiSandBox](#) page. To learn more about what a [WikiWikiWeb](#) is, read about [WhyWikiWorks](#) and the [WikiNature](#). Also, consult the [WikiWikiWebFaq](#).

**General**

- [HowToEdit](#): Information about how to edit the Wireshark wiki
- [SampleCaptures](#): Sample capture files for your edification and amusement
- [NetworkTroubleshooting](#): Information about tracking down network problems

**Prepare Wireshark / TShark**

- [BuildingAndInstalling](#): Building and Installing Wireshark
- [CaptureSetup](#): How to setup your network to successfully capture packets
  - [CaptureSetup/Ethernet](#): Discusses capturing on switched Ethernet networks
  - [CaptureSetup/WLAN](#): Frequently asked WLAN capture setup info

**Use Wireshark / TShark**

Things not (yet) part of the [Wireshark User's Guide](#).

- [CaptureFilters](#): A collection of capture filter examples
- [DisplayFilters](#): A collection of display filter examples
- [ColoringRules](#): A collection of coloring rules examples
- [HowTo](#): How to do various things with Wireshark
- [Preferences](#): Preference settings controlling the behaviour of Wireshark and TShark
- [Statistics](#): Statistics range from general capture file information to protocol specific statistics

# Sites to identify protocols

- **Google, duh!**
- **List of Protocols**
  - [https://en.wikipedia.org/wiki/Lists\\_of\\_network\\_protocols](https://en.wikipedia.org/wiki/Lists_of_network_protocols)
- **For the more advanced**
  - RFCs <https://www.ietf.org/assignments/>
- **The Wireshark Wiki**
  - <https://wiki.wireshark.org/ProtocolReference>

# Sites to Identify IP Information

- Owner
- Country of Origin
- Reputation



## IP Reputation Check

Enter an IP address in the box below to check its current reputation.

[Disclaimer](#)

IP Address:



Enter the text:

### How accurate is ip2nation?

It is hard to say how accurate ip2nation is. The database is based primarily on data (i.e. the location stated by the holder of each IP range). We estimate that it is around 98-99% for a randomly generated IP, but it may be higher or lower for your visitor base. Please feel free to test the database using the form below.

Russia

[Subscribe to updates](#)

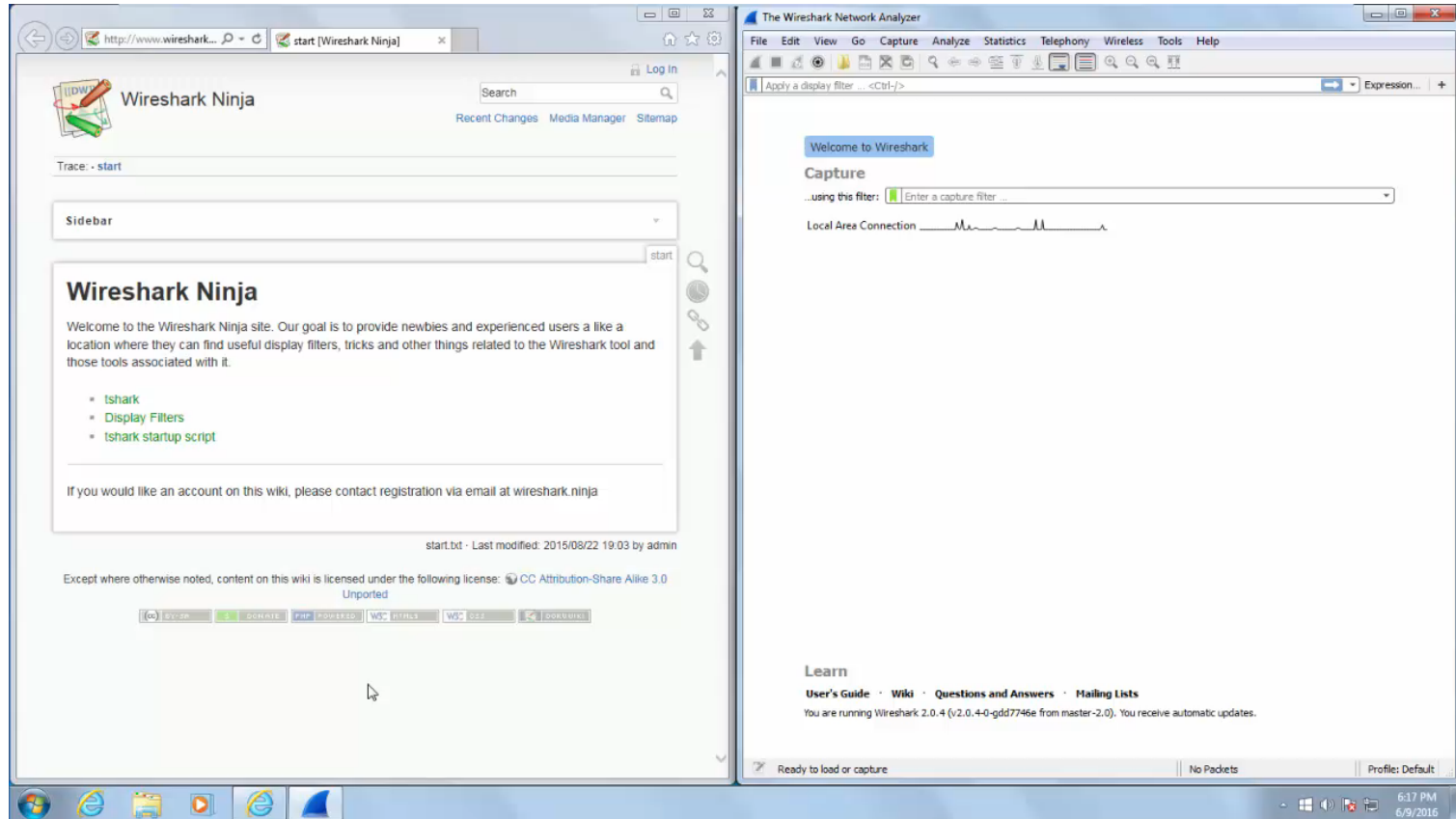
Network	
Net Range	108.178.0.0 - 108.178.63.255
CIDR	108.178.0.0/18
Name	SINGLEHOP
Handle	NET-108-178-0-0-1
Parent	NET108 (NET-108-0-0-0-0)
Net Type	Direct Allocation
Origin AS	AS32475
Organization	SingleHop, Inc. (SINGL-8)
Registration Date	2012-02-27
Last Updated	2012-02-27
Comments	
RESTful Link	<a href="https://whois.arin.net/rest/net/NET-108-178-0-0-1">https://whois.arin.net/rest/net/NET-108-178-0-0-1</a>
See Also	<a href="#">Related organization's POC records.</a>
See Also	<a href="#">Related delegations.</a>



# IP Address Owner

- Not always informative
- Registries
  - American Registry for Internet Numbers (ARIN)
    - <https://www.arin.net/>
  - Latin America and Caribbean Network Information Centre (LACNIC)
    - <http://www.lacnic.org> \*
  - Asia Pacific Network Information Centre (APNIC)
    - <https://www.apnic.net>
  - African Network Information Center (AFRINIC)
    - <https://www.afrinic.net> \*
  - Réseaux IP Européens (RIPE)
    - <https://www.ripe.net>
    - Europe and Middle East

# Using Arin



# IP Address Country of Origin

- Sites that will identify the country of an IP
  - [https://www.countryipblocks.net/country\\_selection.php](https://www.countryipblocks.net/country_selection.php)
  - <http://www.ip2nation.com/> <https://goo.gl/AoDgKq>
- Sites for building a list of IPs per country
  - <http://www.ip2location.com/blockvisitorsbycountry.aspx>
  - <http://www.ipdeny.com/ipblocks/> <http://goo.gl/l0icNa>
  - <http://services.ce3c.be/ciprg/>
  - <http://www.nirsoft.net/countryip/>

# IP Address Reputation

- Use more than one resource
- Read the results carefully
- Mostly for SPAM bots
- Resources
  - <http://www.brightcloud.com/tools/url-ip-lookup.php>
  - <http://www.cyren.com/ip-reputation-check.html>
  - <http://www.borderware.com/>
  - <http://www.barracudacentral.org/lookups/lookup-reputation>
  - <http://www.ipvoid.com>

# One Stop Shops

- <http://www.centralops.net>
- <http://ping.eu>
- <http://www.infobyip.com>
- <http://manytools.org/network/>
- <http://network-tools.com/>

# Sites to Identify Port Assignments

- Google, Duh!
- Wikipedia
  - [https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)  
<https://goo.gl/fcBhW>
- The Wireshark Wiki
  - <https://wiki.wireshark.org/PortReference>

# Looking inside the packets



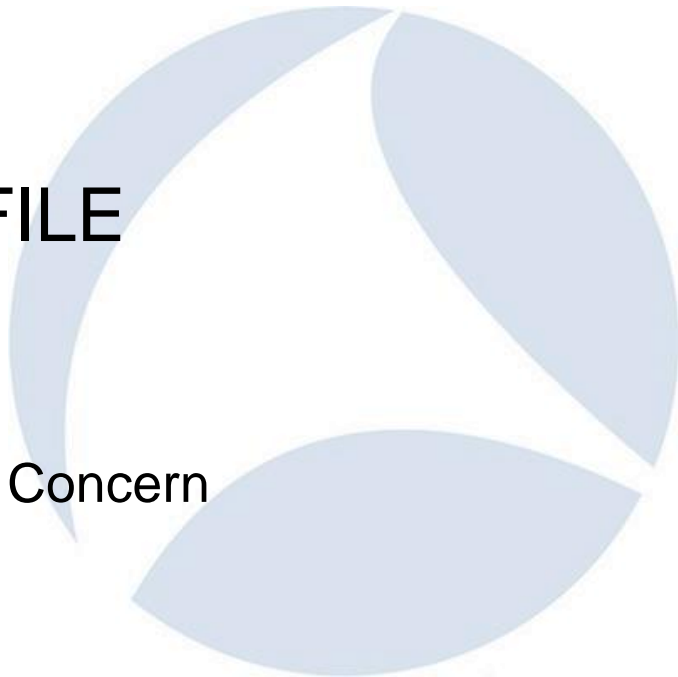
# Follow the Yellow Brick... umm.. Stream?

- **Follow Stream Protocols**

- TCP
- USP
- SSL\*

- **SSLKEYLOGFILE**

- For SSL.
- Trivial to setup
- Not Trivial to use
- Potential Security Concern
- Browser only





# Difficulties / Concerns

- Encrypted Communications
- HTTP2
- Root Kits

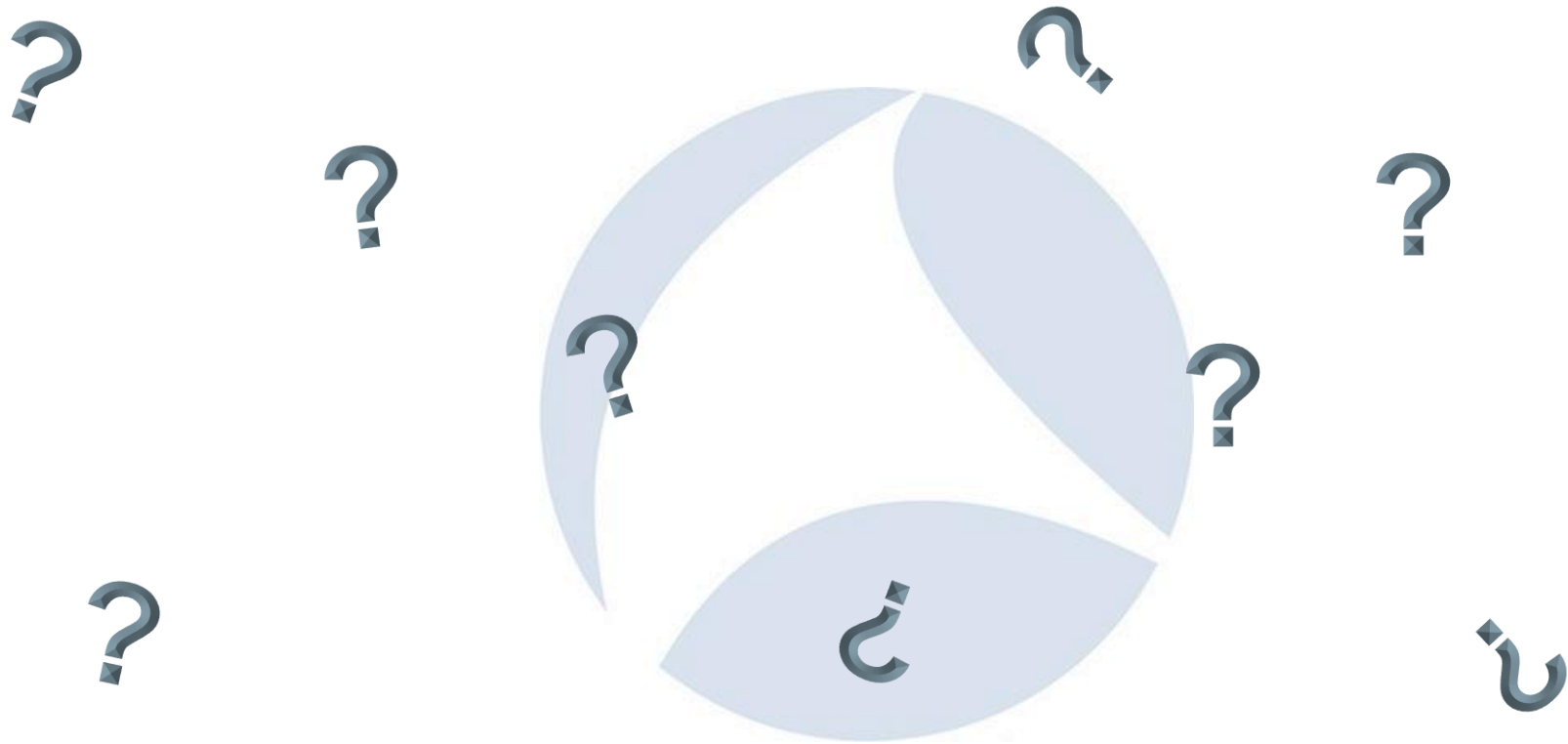




# Survey Submission Time

SharkFest '16 • Computer History Museum • June 13-16, 2016

# Questions





# MAINNERVE

MainNerve, LLC  
Corporate Headquarters  
5825 Mark Dabling Blvd, Ste 160  
Colorado Springs, CO 80919  
info@mainnerve.com

Jon Ford  
Training/R&D  
719-266-3934 Office  
jon.ford@mainnerve.com

Network Penetration Testing  
Web Application Penetration Testing  
Risk Assessment/Compliance  
Small to Medium Business Focused