# Network Baselining with Wireshark

14 June 2016

Jon Ford
Jack of All | MainNerve llc.

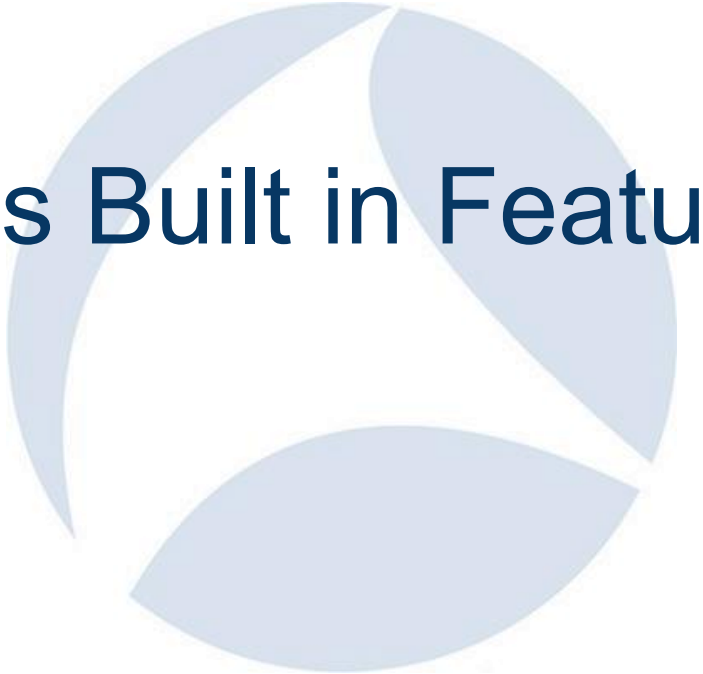
# Jack of All

- 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

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

# Wireshark‘s Built in Features



# Wireshark Features

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

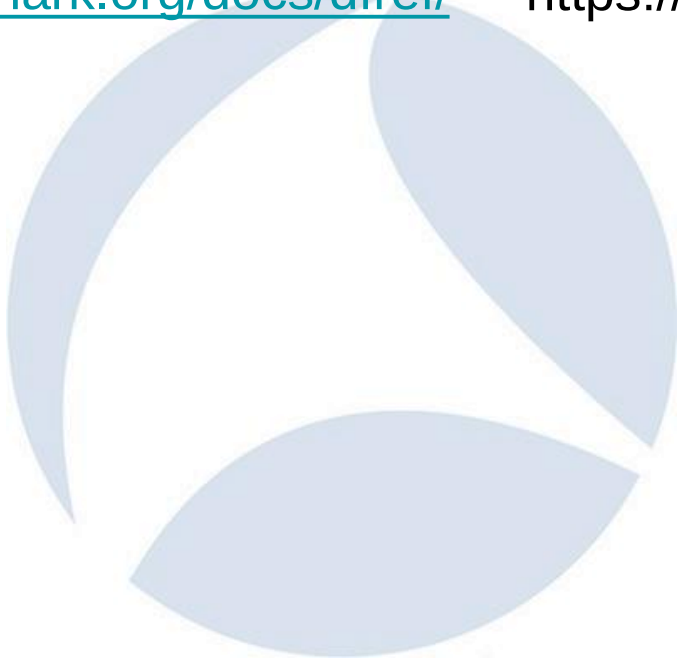
# Filters

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

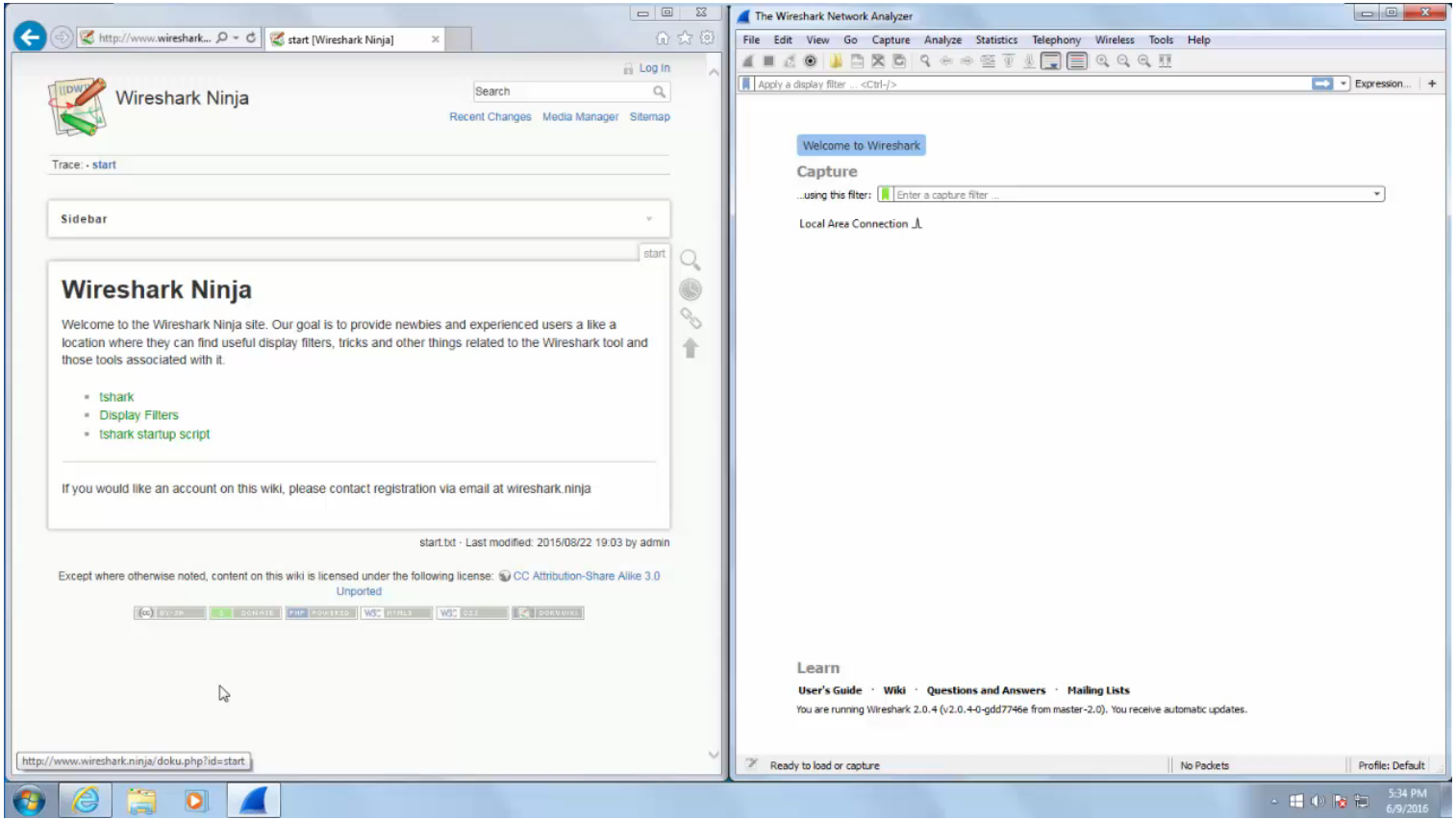
# Statistics

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

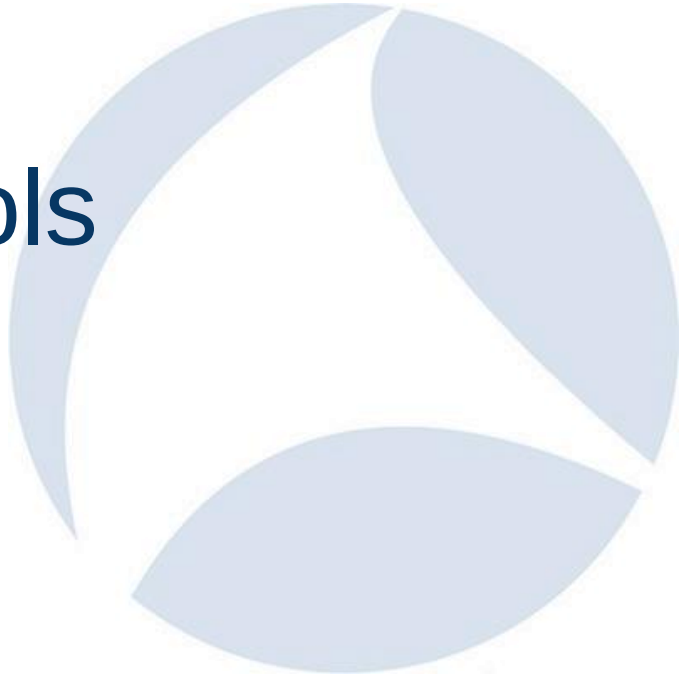
# GeoIP

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

# GeoIP and Wireshark

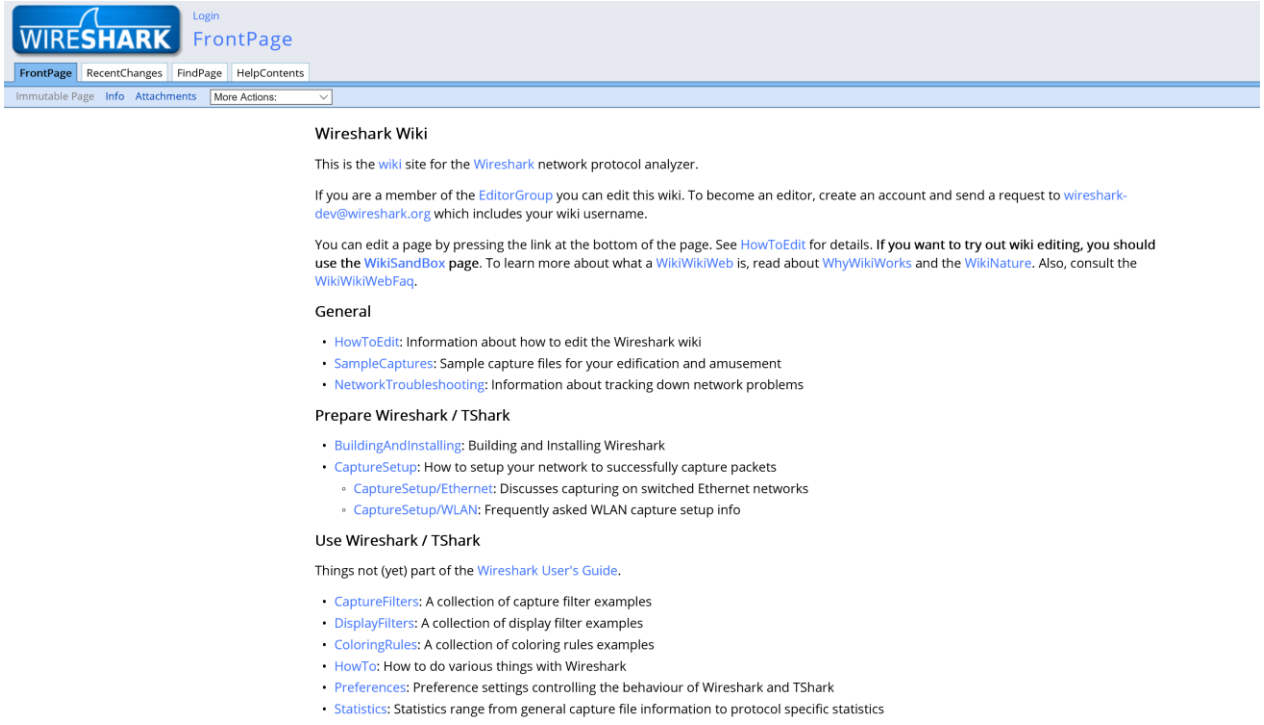


# Online Tools



# Wireshark Wiki

- https://wiki.wireshark.org
  - Duh!

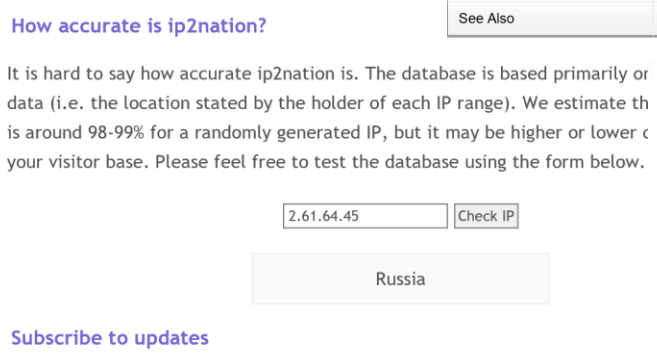


# Sites to identify protocols

- **Google, duh!**
- **List of 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

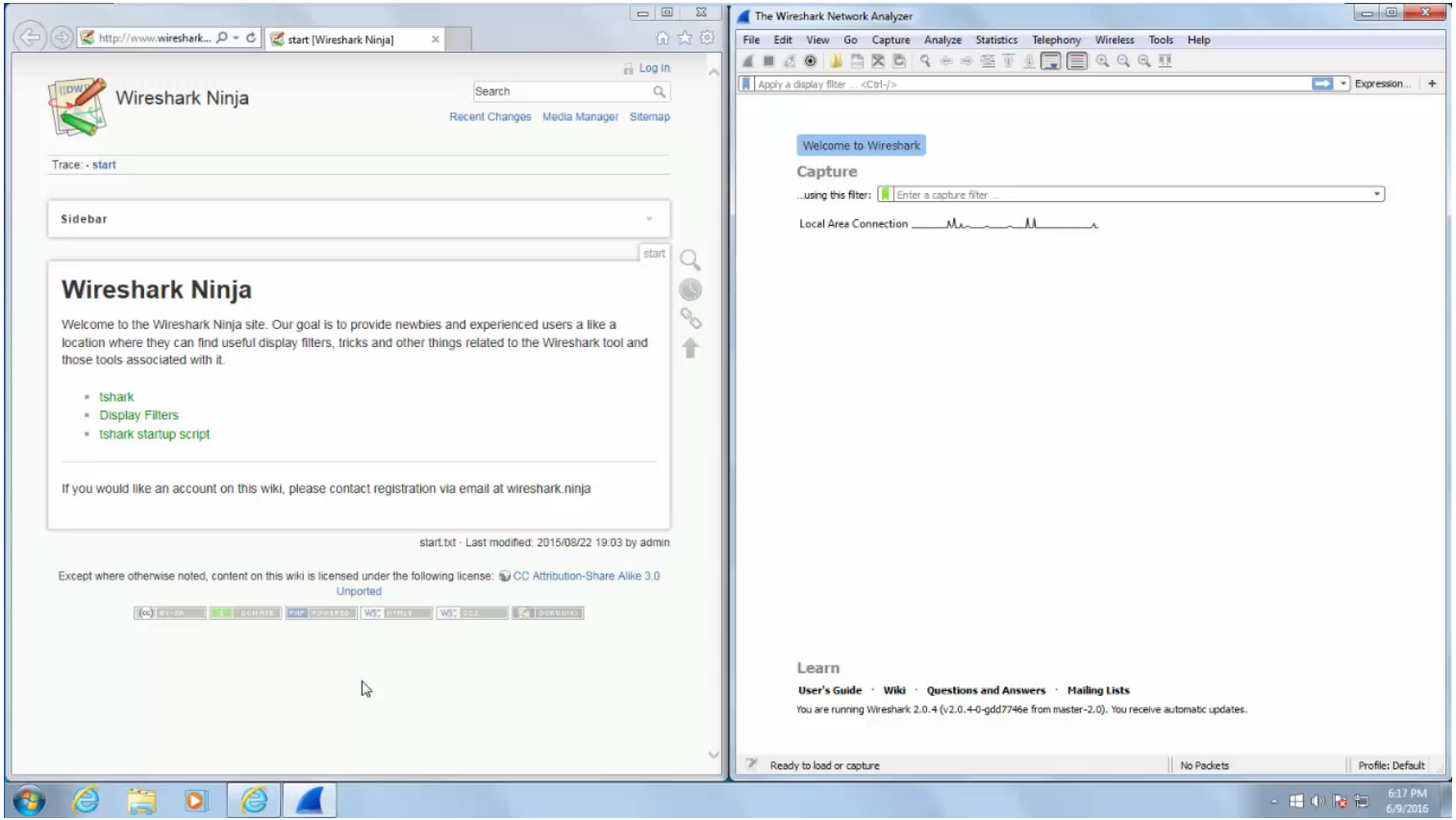




| Network | |
|---|---|
| Net Range | 108.178.0.0 - 108.178.63.255 |
| CIDR | 108.178.0.0/18 |
| Name | SINGLEHOP |
| Handle | NET-108-178-0-0-1 |
| Parent | NET108 (NET-108-0-0-0-0) |
| Net Type | Direct Allocation |
| Origin AS | AS32475 |
| Organization | SingleHop, Inc. (SINGL-8) |
| Registration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

# IP Address Owner

- Not always informative
- Registries
  - American Registry for Internet Numbers (ARIN)
    - **https://www.arin.net/**
  - Latin America and Caribean 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


start [Wireshark Ninja]
Log In
Wireshark Ninja
Search
Recent Changes
Media Manager
Sitemap
Trace: • start
Sidebar
Wireshark Ninja
Welcome to the Wireshark Ninja site. Our goal is to provide newbies and experienced users a like a location where they can find useful display filters, tricks and other things related to the Wireshark tool and those tools associated with it.
tshark
Display Filters
tshark startup script
If you would like an account on this wiki, please contact registration via email at wireshark.ninja
start.txt · Last modified: 2015/08/22 19:03 by admin
Except where otherwise noted, content on this wiki is licensed under the following license: CC Attribution-Share Alike 3.0 Unported
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Local Area Connection
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.0.4 (v2.0.4-0-gdd7746e from master-2.0). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default
6:17 PM
6/9/2016

# IP Address Country of Origin

- Sites that will identify the country of an IP
  - https://www.countryipblocks.net/country_selection.php
  - http://www.ip2nation.com/
- Sites for building a list of IPs per country
  - http://www.ip2location.com/blockvisitorsbycountry.aspx
  - http://www.ipdeny.com/ipblocks/
  - http://services.ce3c.be/ciprg/
  - http://www.nirsoft.net/countryip/

https://goo.gl/AoDgKq

http://goo.gl/l0icNa

# 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/

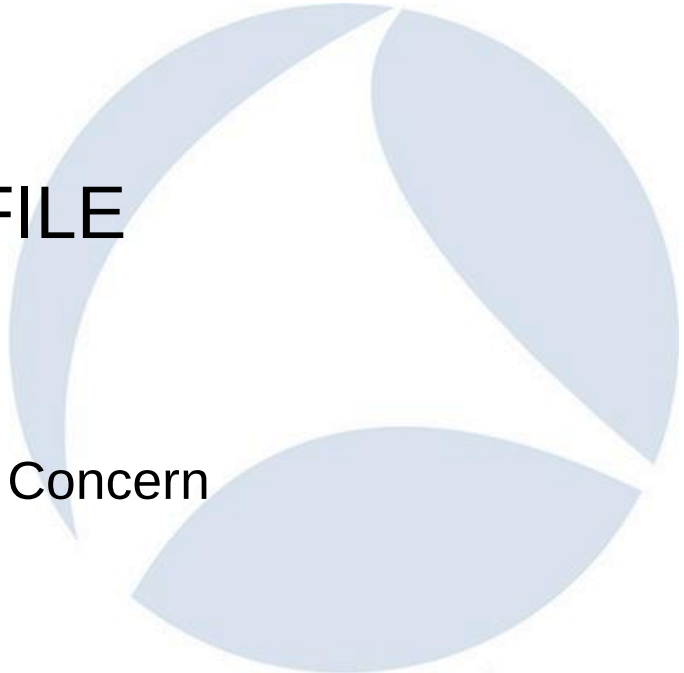
# Sites to Identify Port Assignments

- Google, Duh!
- Wikipedia
  - https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
    https://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

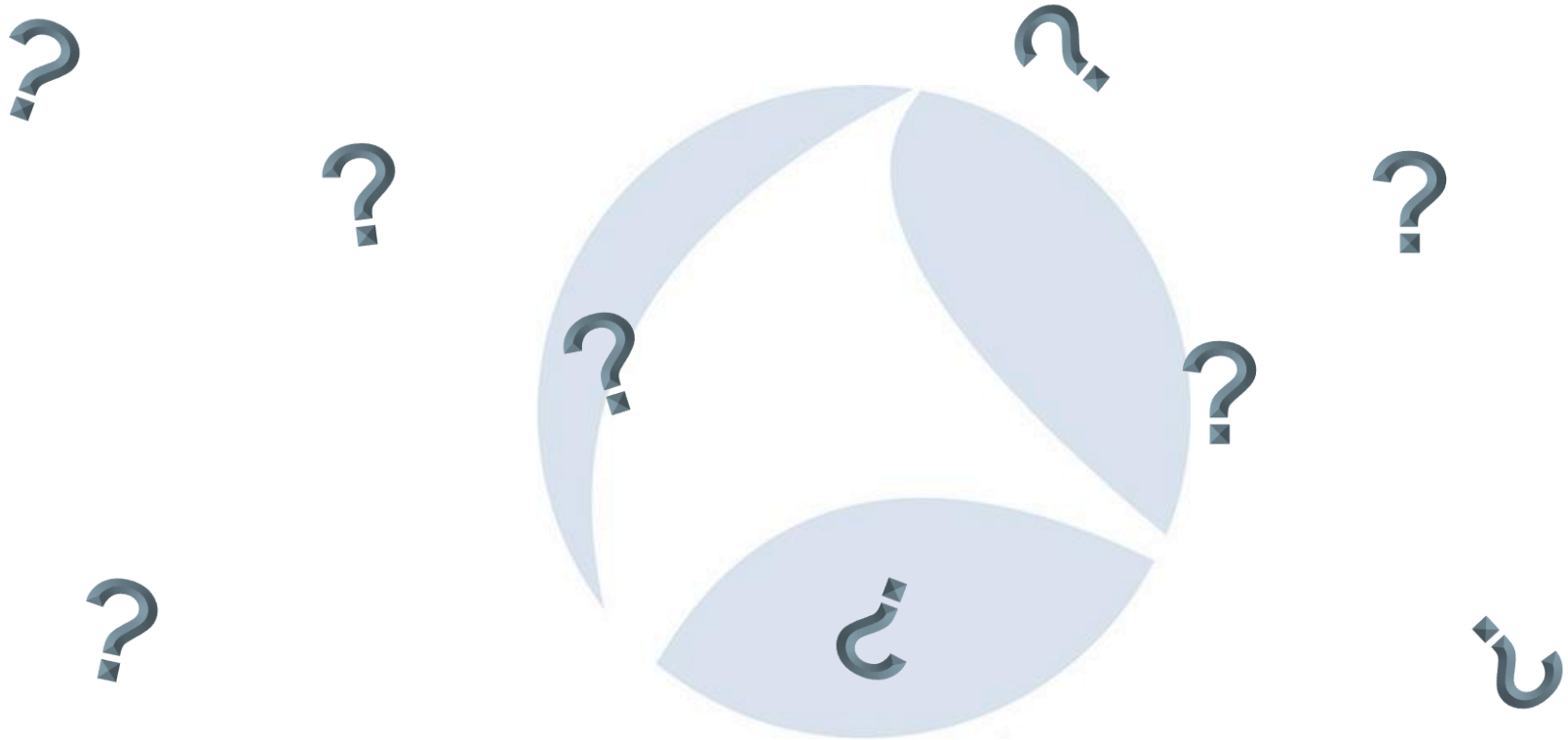


# Difficulties / Concerns

- Encrypted Communications
- HTTP2
- Root Kits

# Survey Submission Time

# Questions




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