

SharkFest'17 US

Network Baselineing with Wireshark

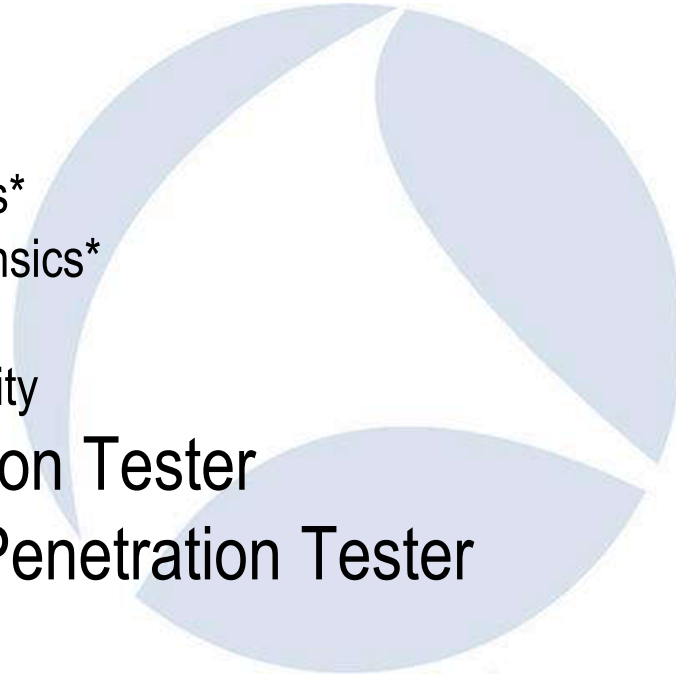


Jon Ford

Penetration Tester | 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



Wireshark's Built in Features



Wireshark Features

- Display Filter (and – the Quick Button)
- Display Filter Macros (What is that?)
- Coloring Rules
- Statistics
- ```
[Source GeoIP: Unknown]
v [Destination GeoIP: United States, AS54312 Rocket Fuel Inc., 37.750999, -97.821999]
 [Destination GeoIP Country: United States]
 [Destination GeoIP AS Number: AS54312 Rocket Fuel Inc.]
 [Destination GeoIP Latitude: 37.750999]
 [Destination GeoIP Longitude: -97.821999]
```

# 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/>

- Examples

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



# Display Filter Macros

- What is a Display Filter Macro?

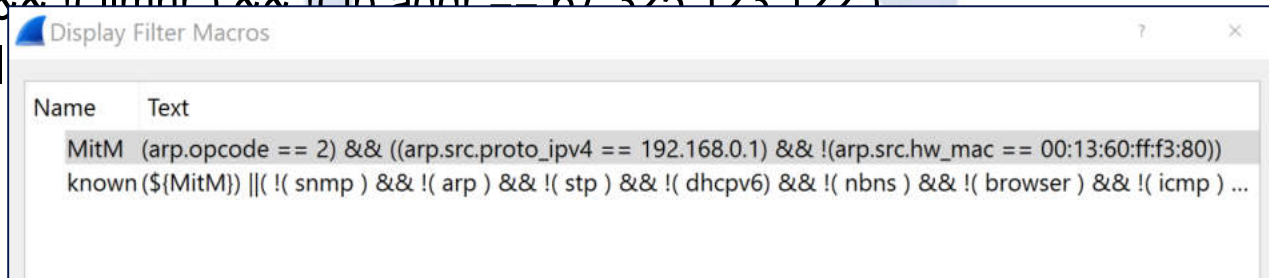
- `${FilterName}`

- Filter to Isolate, First.

- Example:

- `!( arp ) && !( llmnr ) && ( ip.addr == 67.325.123.122 )`
- Ensure that you only see packets to or from 67.325.123.122
- Now add the NOT
- `!( arp ) && !( llmnr ) && !( ip.addr == 67.325.123.122 )`

- This will





# Coloring Rules

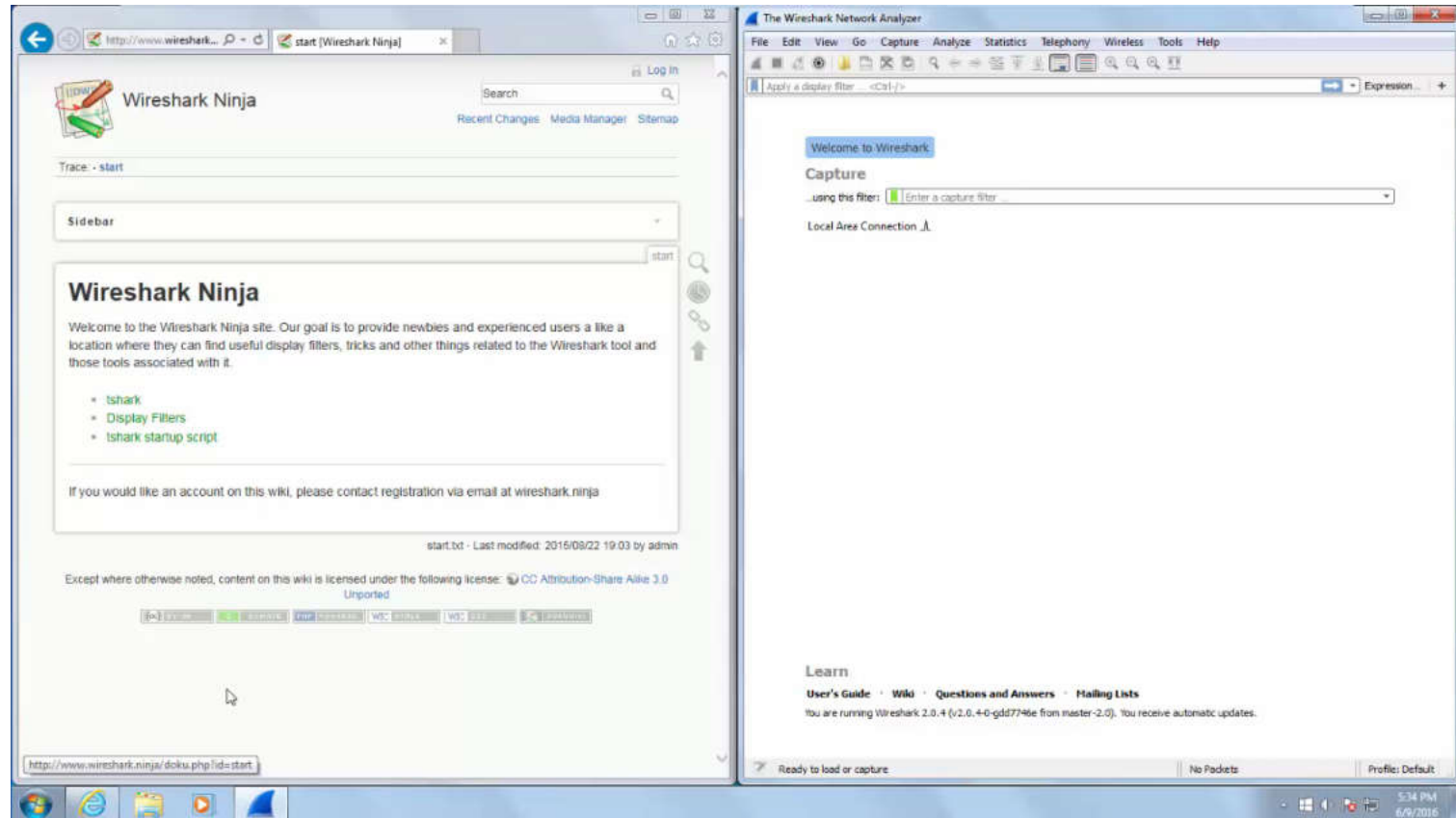
- Black out trusted packets
  - Comparison of Trusted vs Unverified packet use
- Color code based upon country of origin
  - <https://www.ripe.net/participate/member-support/info/list-of-members/list-of-country-codes-and-rirs>
  - ( ip.geoip.country == Italy )
    - Case Sensitive

# GeoIP

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

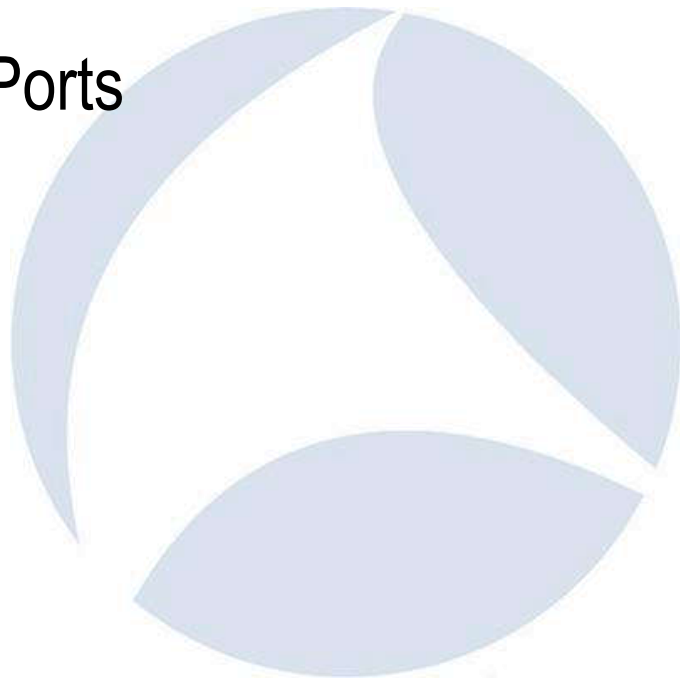


# GeoIP and Wireshark



# Statistics

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

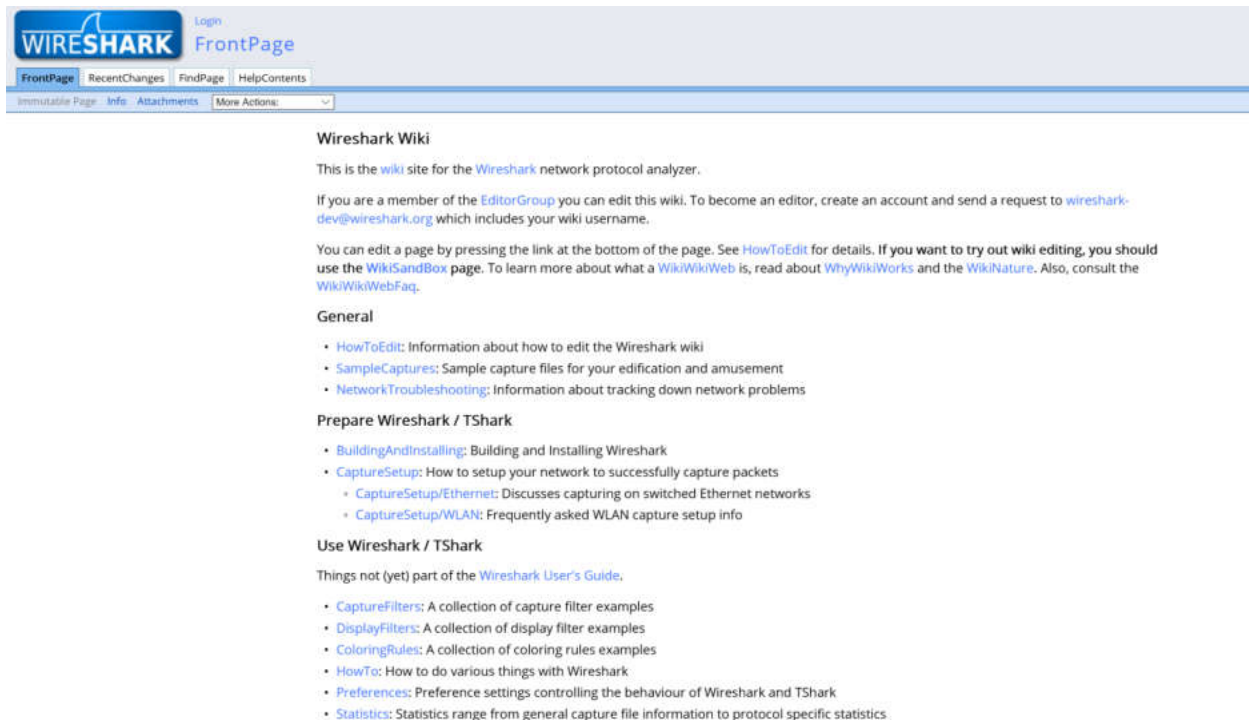


# Online Tools



# Wireshark Wiki

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



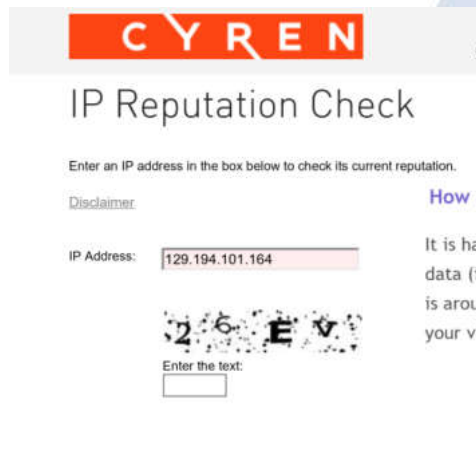
The screenshot shows the top portion of the Wireshark Wiki website. At the top left is the Wireshark logo. To its right are links for 'Login' and 'FrontPage'. Below the logo is a navigation bar with tabs for 'FrontPage', 'RecentChanges', 'FindPage', and 'HelpContents'. Underneath this is a secondary navigation bar with links for 'Immutable Page', 'Info', 'Attachments', and 'More Actions:'. The main content area begins with the heading 'Wireshark Wiki'. The text below explains that this is the wiki site for the Wireshark network protocol analyzer. It provides instructions for editing the wiki, mentioning the EditorGroup and the email address [wireshark-dev@wireshark.org](mailto:wireshark-dev@wireshark.org). It also points to the [HowToEdit](#) page for editing details and the [WikiSandBox](#) page for editing. A 'General' section follows, containing links to [HowToEdit](#), [SampleCaptures](#), and [NetworkTroubleshooting](#). Next is a 'Prepare Wireshark / TShark' section with links to [BuildingAndInstalling](#), [CaptureSetup](#), [CaptureSetup/Ethernet](#), and [CaptureSetup/WLAN](#). The 'Use Wireshark / TShark' section includes a link to the [Wireshark User's Guide](#) and a list of links for [CaptureFilters](#), [DisplayFilters](#), [ColoringRules](#), [HowTo](#), [Preferences](#), and [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




**CYREN**

## 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](#)

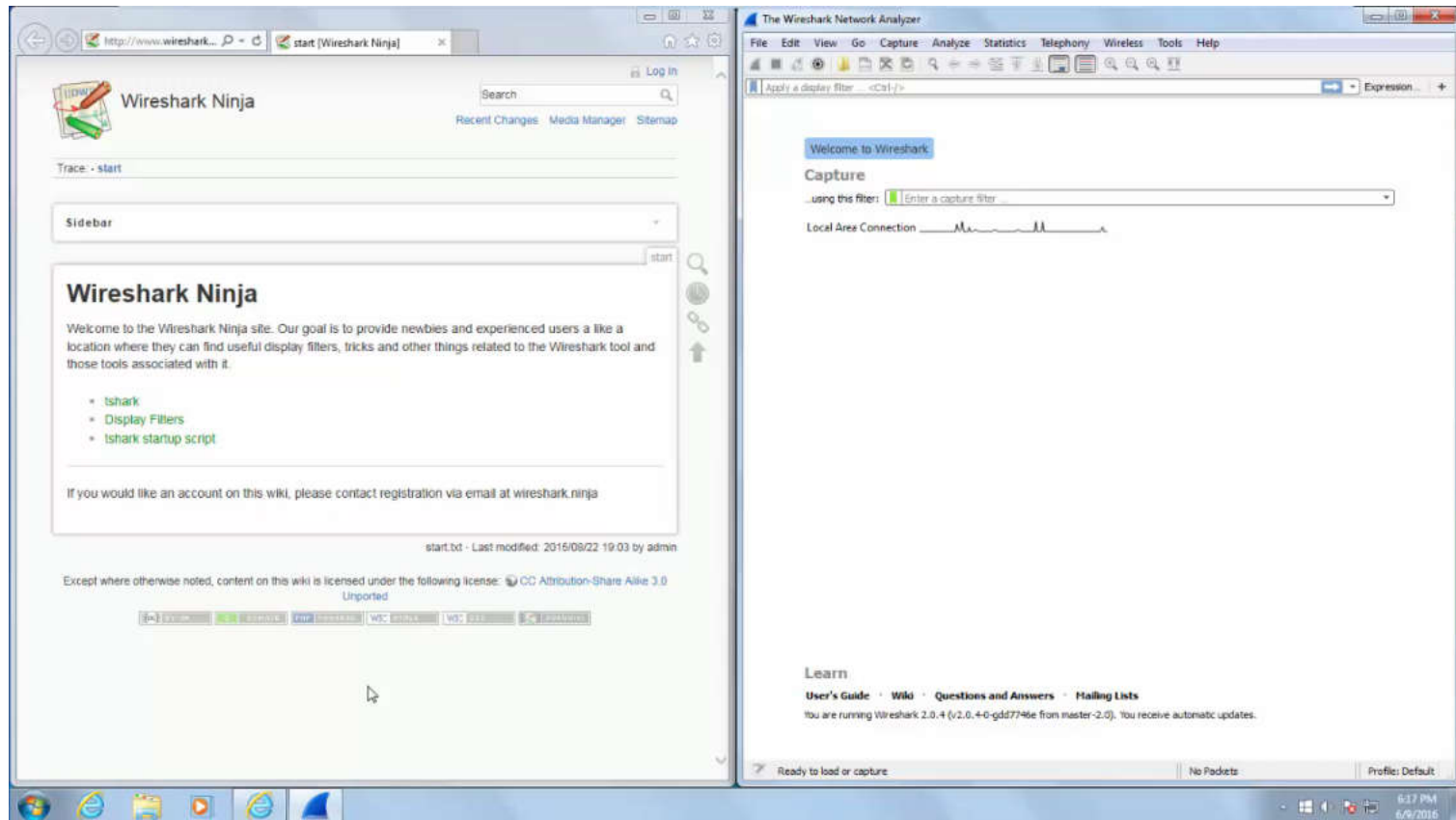
| Network           |                                                                                                                   |
|-------------------|-------------------------------------------------------------------------------------------------------------------|
| Net Range         | 108.178.0.0 - 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/>
- 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/>

# 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)
- 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



# Questions

