SharkFest'17 US

Network Baselining with Wireshark

Jon Ford
Penetration Tester | MainNerve Llc.

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017

Jack of All

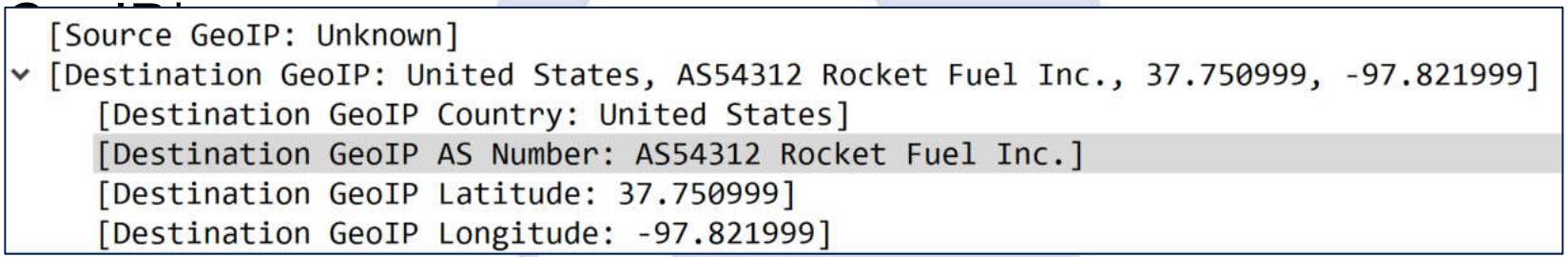
- US Marine Corps
  - 1998 - 2007
- Instructor
  - Wireless Exploitation
  - Basic Digital Forensics*
  - Basic Cellphone Forensics*
  - Network Exploitation
  - Personal Cyber Security
- Network Penetration Tester
- Web Application Penetration Tester

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
-



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.

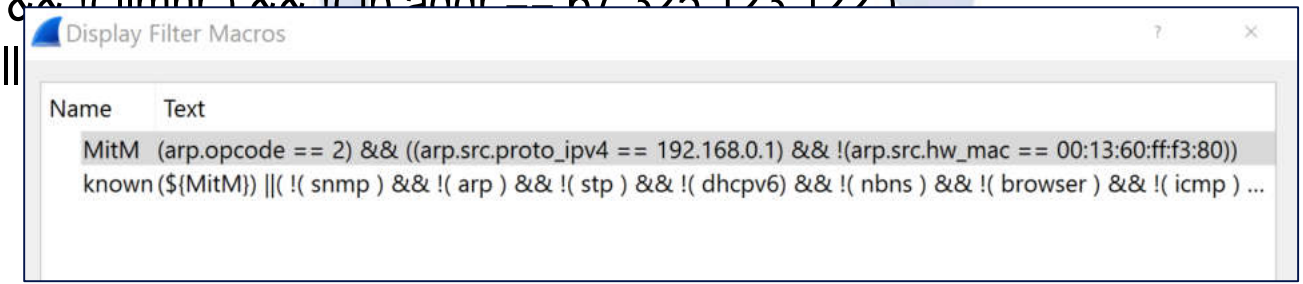
The idea behind a baseline is to create a filter to hide what we know is ok or trusted so the bad guys can't hide.

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

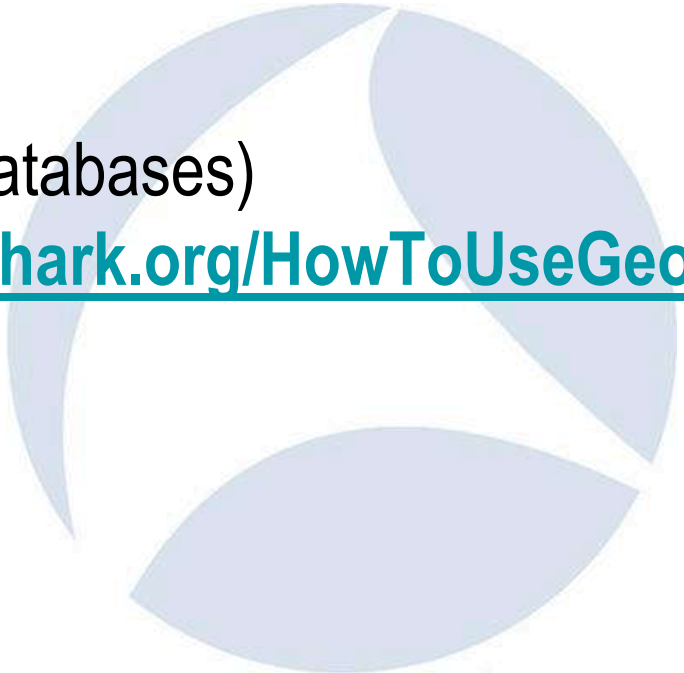


Coloring Rules

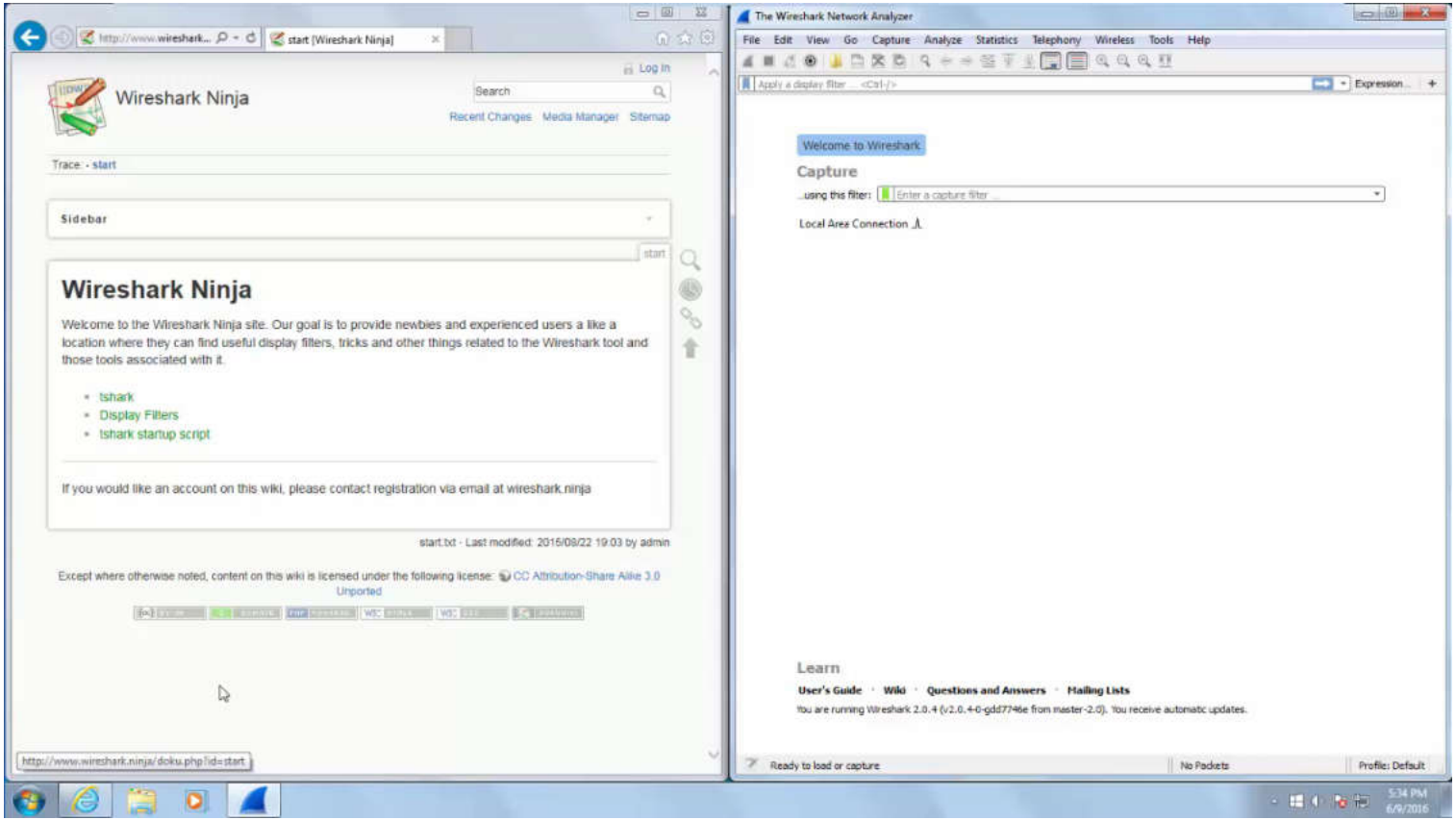
- Black out trusted packets
  - Comparison of Trusted vs Unverified packet use
- Color code based upon country of origin
  - https://www.ripe.net/participate/member-support/info/list-of-members/list-of-country-codes-and-rirs
  - (ip.geoip.country == Italy)
    - Case Sensitive

GeoIP

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

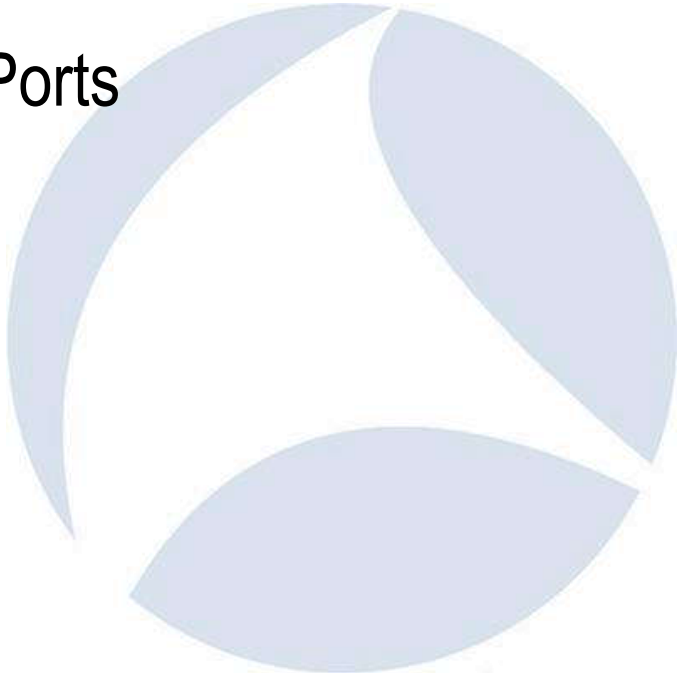


GeoIP and Wireshark



Statistics

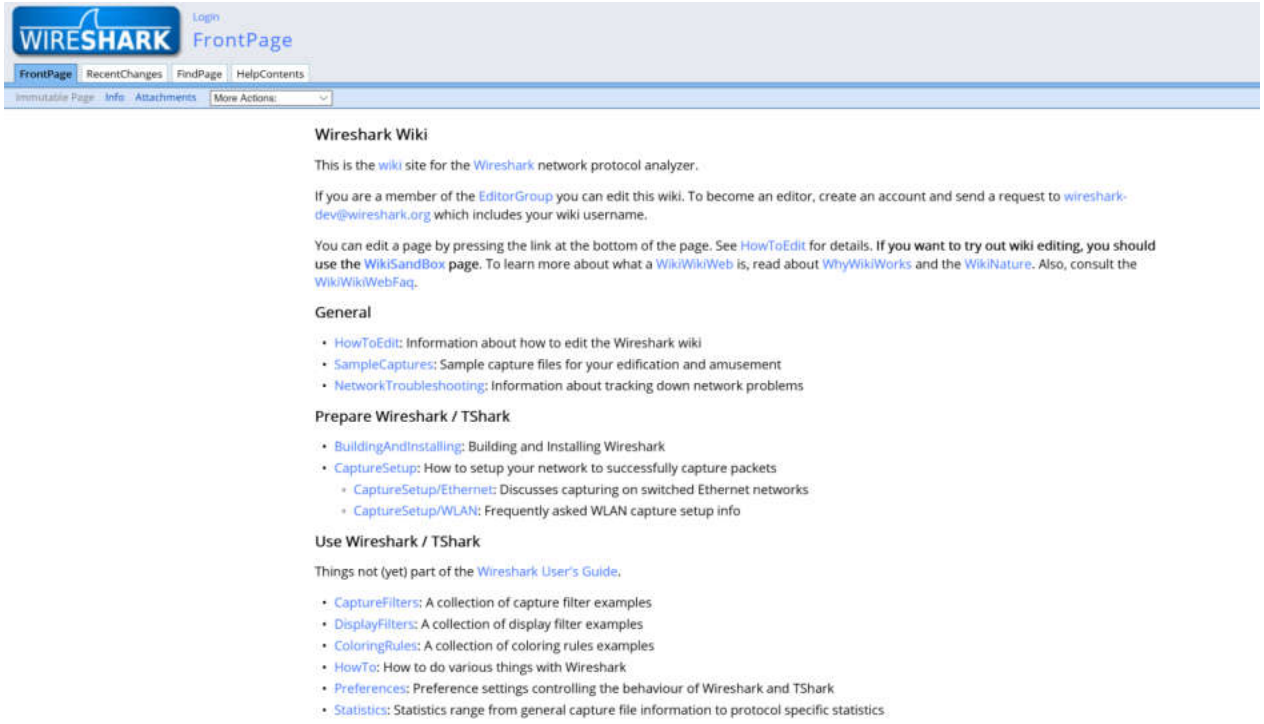
- Conversations
- Endpoints
- Destinations and Ports
- All IP Addresses



Online Tools

Wireshark Wiki

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

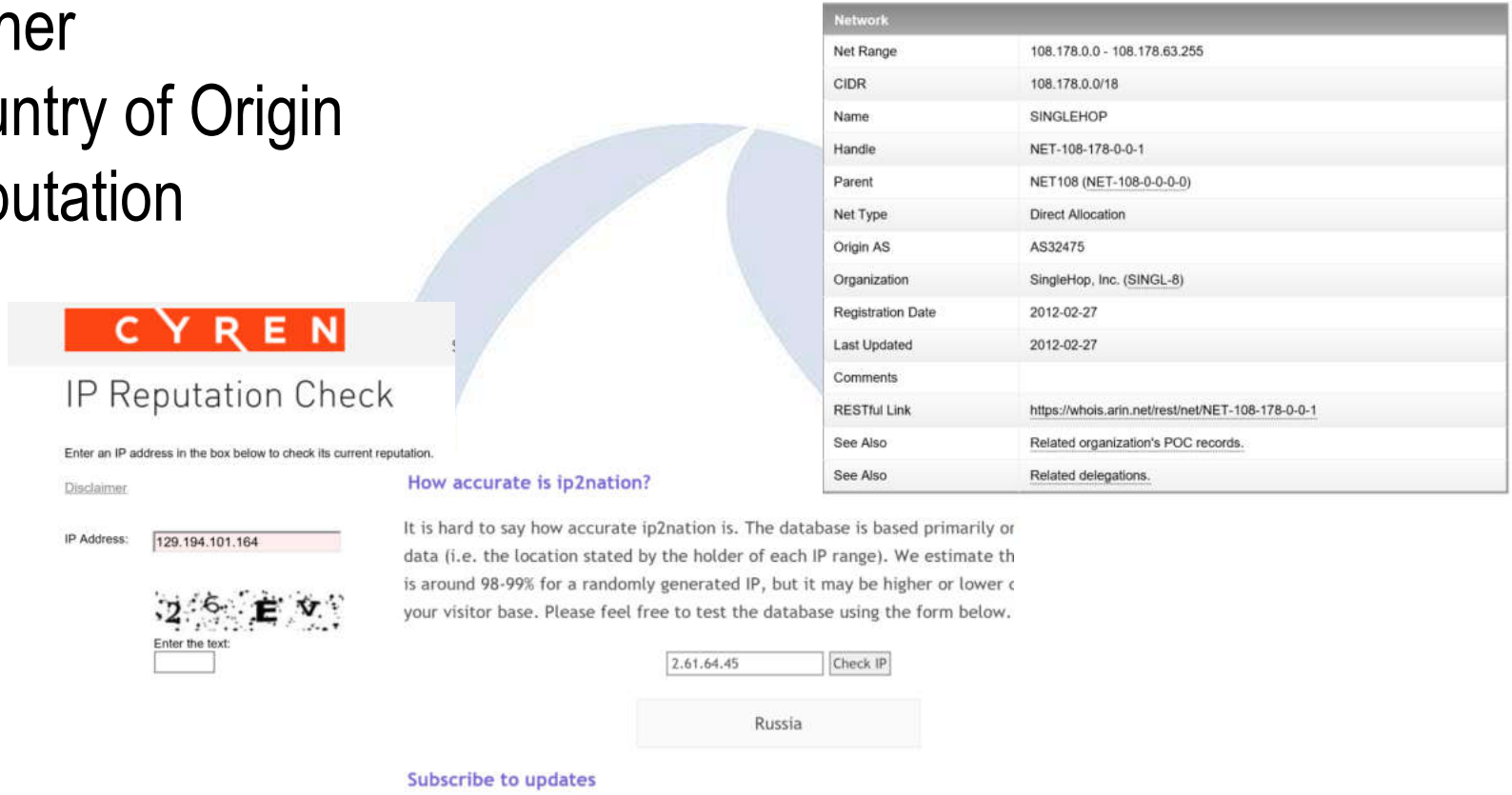


Sites to identify protocols

- **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

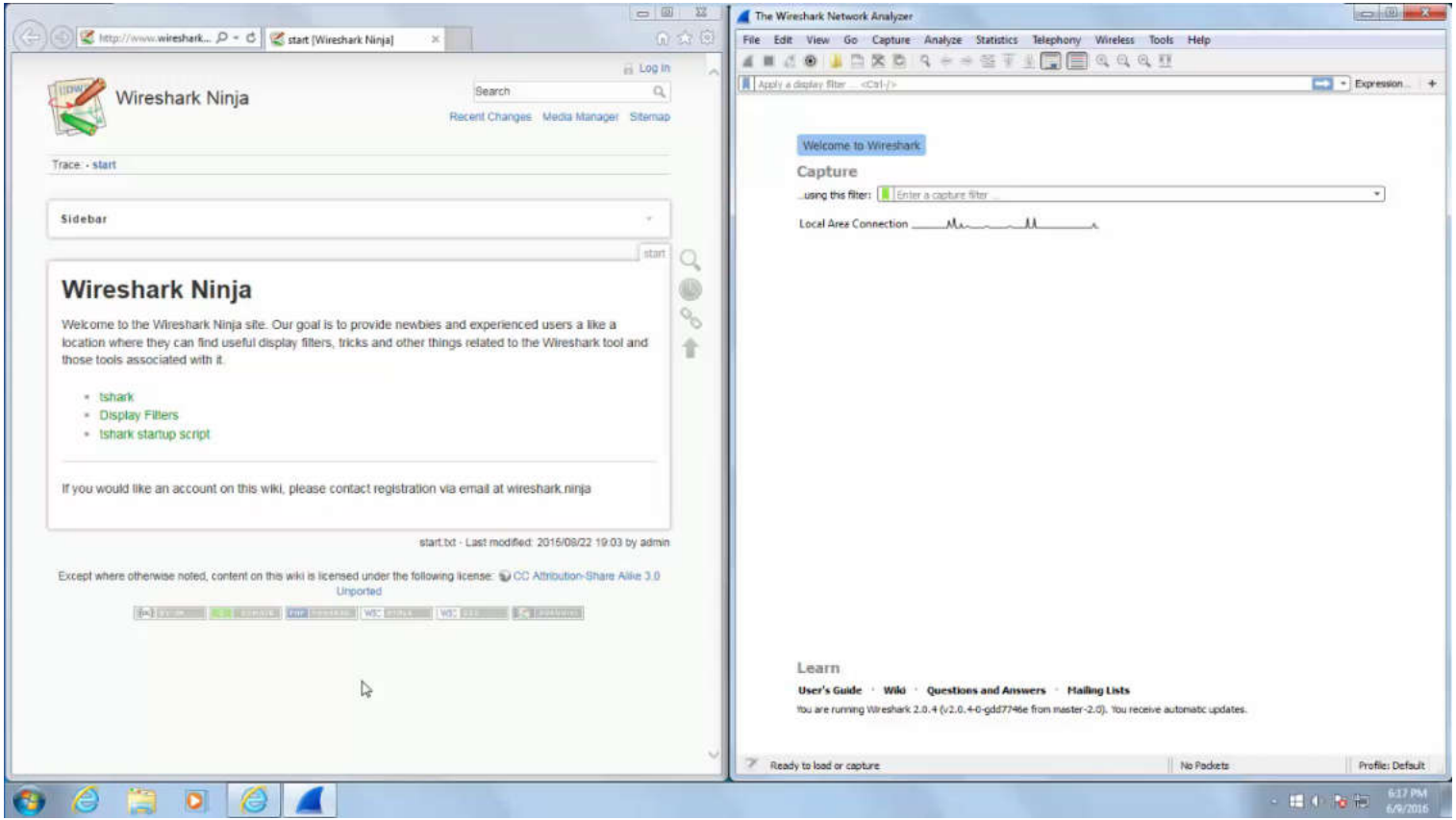
- Owner
- Country of Origin
- Reputation



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
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

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/

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/

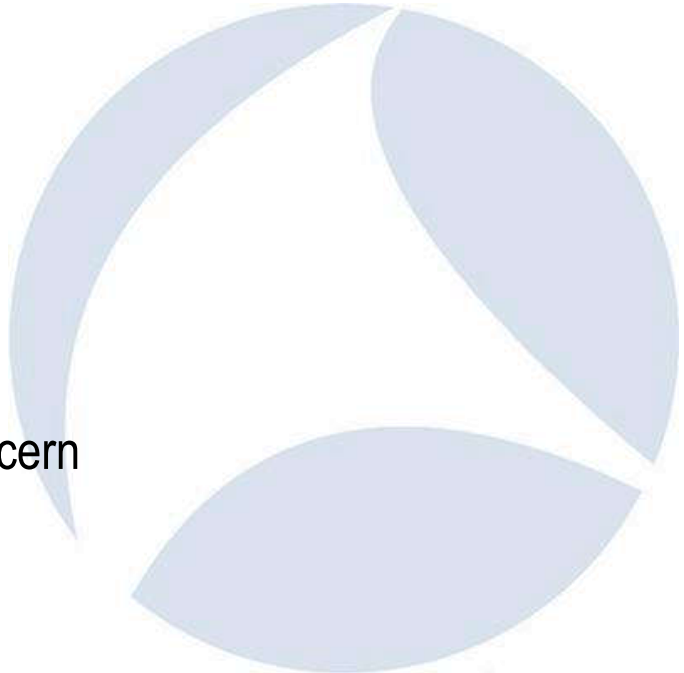
Sites to Identify Port Assignments

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