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
• GeoIP

[Source GeoIP: Unknown]
[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/](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 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
  • [https://www.ripe.net/participate/member-support/info/list-of-members/list-of-country-codes-and-rirs](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/HowToUseGeolP](https://wiki.wireshark.org/HowToUseGeolP)
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
• 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

How accurate is ip2nation?

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

Network

<table>
<thead>
<tr>
<th>Network</th>
<th>108.178.0.0 - 108.178.63.255</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>108.178.0.0/18</td>
</tr>
<tr>
<td>Name</td>
<td>SINGLEHOP</td>
</tr>
<tr>
<td>Handle</td>
<td>NET-108-178-0-0-1</td>
</tr>
<tr>
<td>Parent</td>
<td>NET108 (NET-108-178-0-0-0)</td>
</tr>
<tr>
<td>Net Type</td>
<td>Direct Allocation</td>
</tr>
<tr>
<td>Origin AS</td>
<td>AS32475</td>
</tr>
<tr>
<td>Organization</td>
<td>SingleHop, Inc. (SINGL-8)</td>
</tr>
<tr>
<td>Registration Date</td>
<td>2012-02-27</td>
</tr>
<tr>
<td>Last Updated</td>
<td>2012-02-27</td>
</tr>
<tr>
<td>Comments</td>
<td></td>
</tr>
<tr>
<td>RESTful Link</td>
<td><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></td>
</tr>
<tr>
<td>See Also</td>
<td>Related organization's POC records.</td>
</tr>
<tr>
<td>See Also</td>
<td>Related delegations.</td>
</tr>
</tbody>
</table>

Subscribe to updates

2.61.64.45  Check IP

Russia
• 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
  • 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
- 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