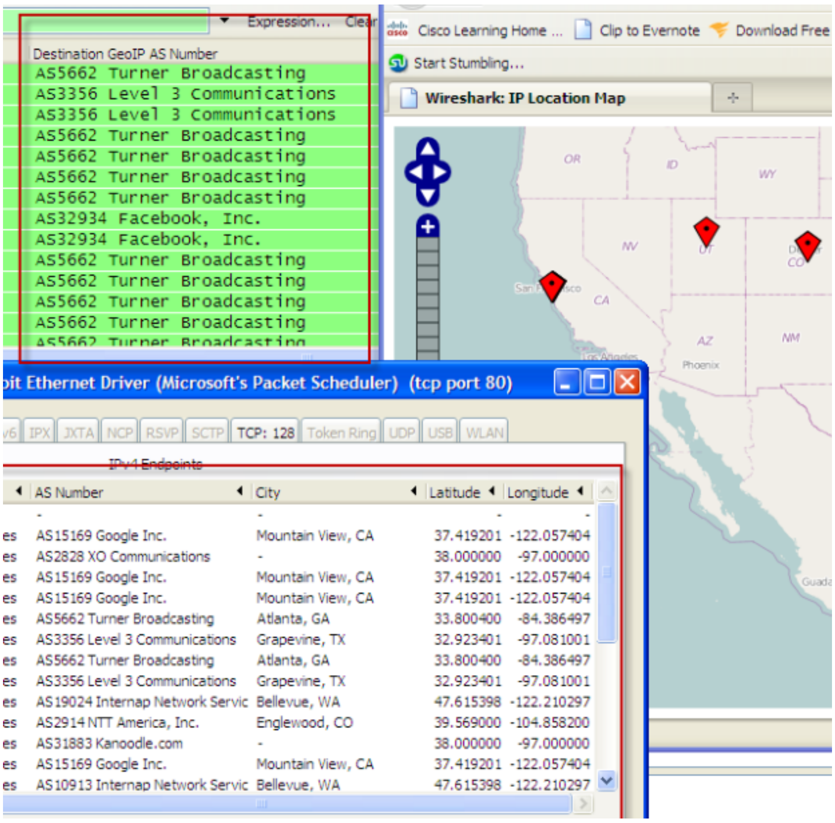
VIP Perspectives

Geolocation in Wireshark

Posted by Paul Stewart - CCIE Security in VIP Perspectives on Dec 11, 2010 10:40:32 AM

Throughout my career, I have spent a considerable amount of time using and studying packet captures. One of the more difficult things when analyzing traffic is simply wading through the unimportant stuff and looking for that which is more significant. If you have not spent a good deal of time studying traffic, it may even take a few minutes to even find the conversation that you are looking for. I typically do a combination of string searches, name resolution and filters to narrow down my field of view and focus in on what we are interested in. Wireshark, my favorite protocol analyzer, has come a long way since its earlier days of Ethereal. The traditional filter mechanisms are elegant and full featured, but I would like to introduce one of the new and exciting features and how it expands our capability to filter.

This cool new feature is the GeoIP capability. If you have the current version of Wireshark, you may have the ability to use MaxMind's GeoIP database during your network analysis process. It is really cool to be able to do things like filter by city, country, BGP Autonomous System Number (ASN), latitude range, longitude range, and company name. Furthermore, it is nice to have the awareness that can be realized by having a column for the company name/ASN and Country in the packet lists and the ability to plot the endpoints on a map. This feature is not enabled by default and can have an impact on performance. So this is one of those things that you may want to use on a circumstance by circumstance basis. Additionally, there is a little bit of work that is required to getting this going the first time.

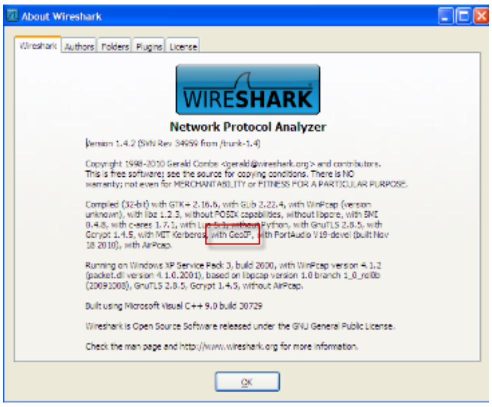


Destination GeoIP AS Number
AS5662 Turner Broadcasting
AS3356 Level 3 Communications
AS3356 Level 3 Communications
AS5662 Turner Broadcasting
AS5662 Turner Broadcasting
AS5662 Turner Broadcasting
AS5662 Turner Broadcasting
AS32934 Facebook, Inc.
AS32934 Facebook, Inc.
AS5662 Turner Broadcasting
AS5662 Turner Broadcasting
AS5662 Turner Broadcasting
AS5662 Turner Broadcasting
AS5662 Turner Broadcasting

bit Ethernet Driver (Microsoft's Packet Scheduler) (tcp port 80)

	AS Number	City	Latitude	Longitude
	-	-	-	-
es	AS15169 Google Inc.	Mountain View, CA	37.419201	-122.057404
es	AS2828 XO Communications	-	38.000000	-97.000000
es	AS15169 Google Inc.	Mountain View, CA	37.419201	-122.057404
es	AS15169 Google Inc.	Mountain View, CA	37.419201	-122.057404
es	AS5662 Turner Broadcasting	Atlanta, GA	33.800400	-84.386497
es	AS3356 Level 3 Communications	Grapevine, TX	32.923401	-97.081001
es	AS5662 Turner Broadcasting	Atlanta, GA	33.800400	-84.386497
es	AS3356 Level 3 Communications	Grapevine, TX	32.923401	-97.081001
es	AS19024 Internap Network Servic	Bellevue, WA	47.615398	-122.210297
es	AS2914 NTT America, Inc.	Englewood, CO	39.569000	-104.858200
es	AS31883 Kanoodle.com	-	38.000000	-97.000000
es	AS15169 Google Inc.	Mountain View, CA	37.419201	-122.057404
es	AS10913 Internap Network Servic	Bellevue, WA	47.615398	-122.210297

To use the GeoIP features in Wireshark, it is first necessary to make sure that the feature was compiled in the version of Wireshark that you are currently running. To do this, simply launch Wireshark then go to "Help" and "About Wireshark". On the "Wireshark" tab, look for the words "with GeoIP". If this is present, your version of Wireshark supports GeoIP.



Network Protocol Analyzer

Version 1.4.2 (SVN Rev 34959 from /trunk-1.4)

Copyright 1998-2010 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (32-bit) with GTK+ 2.16.6, with GLib 2.22.4, with WinPcap (version unknown), with libz 1.2.3, without POSIX capabilities, without libpcre, with SMI 0.4.8, with c-ares 1.7.1, with Lua 5.1, without Python, with GnuTLS 2.8.5, with Gcrypt 1.4.5, with MIT Kerberos, with GeoIP, with PortAudio V19-devel (built Nov 18 2010), with AirPcap.

Running on Windows XP Service Pack 3, build 2600, with WinPcap version 4.1.2 (packet.dll version 4.1.0.2001), based on libpcap version 1.0 branch 1_0_rel0b (20091008), GnuTLS 2.8.5, Gcrypt 1.4.5, without AirPcap.

Built using Microsoft Visual C++ 9.0 build 30729

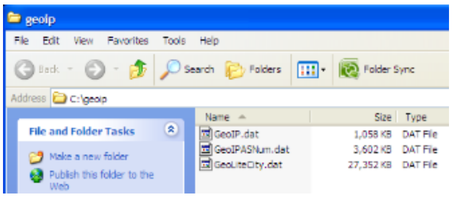
Wireshark is Open Source Software released under the GNU General Public License.

Check the man page and http://www.wireshark.org for more information.

The next thing we need is the actual GeoIP databases. Wireshark currently uses the MaxMind binary GeoIP databases. There are free and paid versions that are available. The free ones are called "GeoLite" Country, City and ASN. The free Country and City databases are slightly less accurate than the subscription based ones. In any case, these are a good starting place if you are interested in the GeoIP features in Wireshark. To download, go to the following urls:

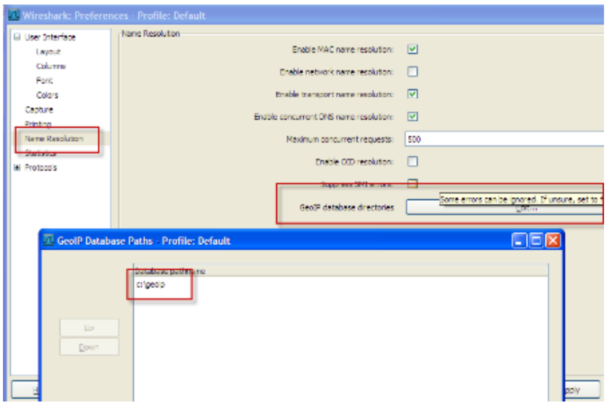
http://www.maxmind.com/app/geolitecountry >> Download the latest GeoLite Country Binary Format
http://www.maxmind.com/app/geolitecity >> Download the latest GeoLite City Binary Format
http://www.maxmind.com/app/asnum >> Download the free database "GeoIPASNum.dat.gz"

The next step is to extract these files into a common directory using an archive utility like Gzip (*NIX) or 7-zip (Windows).



Name	Size	Type
GeoIP.dat	1,058 KB	DAT File
GeoIPASNum.dat	3,602 KB	DAT File
GeoLiteCity.dat	27,352 KB	DAT File

Now that we have the necessary databases, we need to point Wireshark to the databases and enable GeoIP as a resolution method. To do this, go to "Edit" then "Preferences". Then in the left column expand "User Interface" and choose "Name Resolution". To set the database location, choose the Edit button for GeoIP database directories. Next set the directory as appropriate, "c:\geoip" in my example.



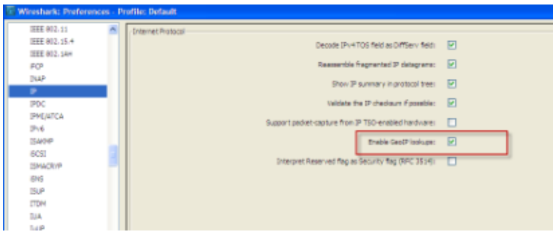
Name Resolution

Enable MAC name resolution: ☑
Enable network name resolution: □
Enable transport name resolution: ☑
Enable concurrent DNS name resolution: ☑
Maximum concurrent requests: 500
Enable OID resolution: □
Suppress SMI errors: □
GeoIP database directories: Edit...

Some errors can be ignored. If unsure, set to f

Database pathname
c:\geoip

Apply those settings but don't fully exit out of "Preferences". We still have another thing that we have to do. So still in "Preferences" we need to enable IP GeoIP resolutions. To do this, expand the "Protocols" in and select "IP". Place a checkmark in the box "Enable GeoIP lookups". Now we can start using this cool new feature.

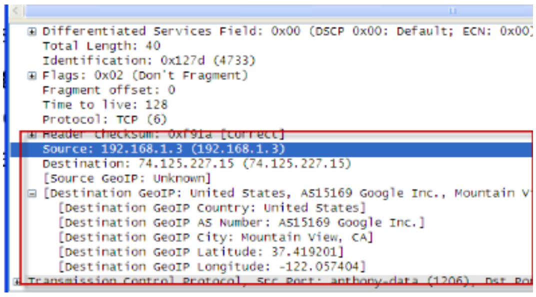


Internet Protocol

Decode IPv4 TOS field as DiffServ field: ☑
Reassemble fragmented IP datagrams: ☑
Show IP summary in protocol tree: ☑
Validate the IP checksum if possible: ☑
Support packet-capture from IP TSO-enabled hardware: □
Enable GeoIP lookups: ☑
Interpret Reserved flag as Security flag (RFC 3514): □

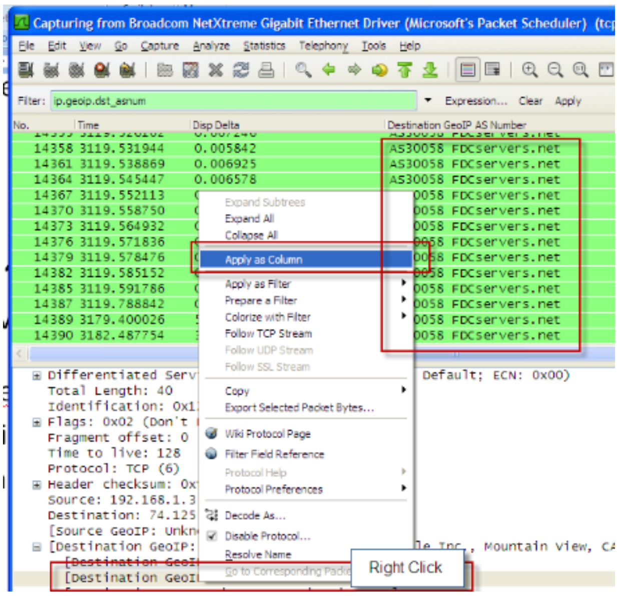
The first thing to note is that there is no GeoIP data populated for private address ranges. So make sure that you capture some real data that is going to a non-RFC1918 address space. After doing so, there are some new things that you will notice.

Expand an IP header in the “Packet Details” and you should see source and/or destination GeoIP information.



```
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 40
  Identification: 0x127d (4733)
⊞ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
⊞ Header checksum: 0xf91a [correct]
  Source: 192.168.1.3 (192.168.1.3)
  Destination: 74.125.227.15 (74.125.227.15)
  [Source GeoIP: Unknown]
⊟ [Destination GeoIP: United States, AS15169 Google Inc., Mountain V
    [Destination GeoIP Country: United States]
    [Destination GeoIP AS Number: AS15169 Google Inc.]
    [Destination GeoIP City: Mountain View, CA]
    [Destination GeoIP Latitude: 37.419201]
    [Destination GeoIP Longitude: -122.057404]
⊞ Transmission Control Protocol, Src Port: anthony-data (1206), Dst Por
```

I also wanted some of this information displayed in the “Packet List” so I added a column for “Destination GeoIP AS Number” by right-clicking the appropriate field and choosing “Apply as Column”



```
No.    Time         Disp Delta      Destination GeoIP AS Number
14358 3119.531944   0.005842        AS30058 FDCservers.net
14361 3119.538869   0.006925        AS30058 FDCservers.net
14364 3119.545447   0.006578        AS30058 FDCservers.net
14367 3119.552113                     0058 FDCservers.net
14370 3119.558750                     0058 FDCservers.net
14373 3119.564932                     0058 FDCservers.net
14376 3119.571836                     0058 FDCservers.net
14379 3119.578476                     0058 FDCservers.net
14382 3119.585152                     0058 FDCservers.net
14385 3119.591786                     0058 FDCservers.net
14387 3119.788842                     0058 FDCservers.net
14389 3179.400026                     0058 FDCservers.net
14390 3182.487754                     0058 FDCservers.net
```

```
⊞ Differentiated Serv                 Default; ECN: 0x00)
  Total Length: 40
  Identification: 0x1
⊞ Flags: 0x02 (Don't
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
⊞ Header checksum: 0x
  Source: 192.168.1.3
  Destination: 74.125
  [Source GeoIP: Unkn
⊟ [Destination GeoIP:                 le Inc., Mountain View, CA
    [Destination GeoI
    [Destination GeoI
```

We also now have the ability to add more creative filters. For example, we could use the following filters.

Match Packets with a Destination IP address in the United Starts
ip.geoip.dst_country == "United States"

Match Packets to or from an IP address North of the Arctic Circle
ip.geoip.lat > "66.5"

Match packets to or from an IP address in California.
ip.geoip.city contains "CA"

The display filter syntax has actually been expanded to include the following:

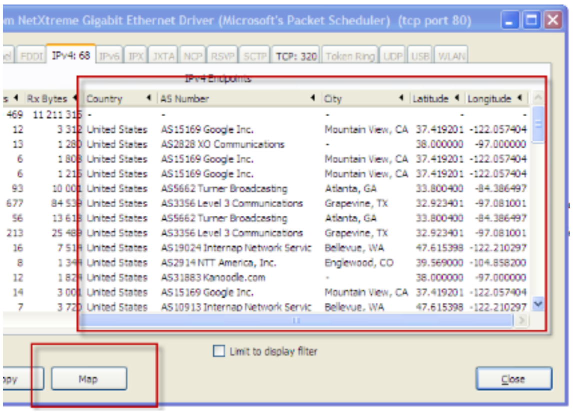
ip.geoip.asnum
ip.geoip.city
ip.geoip.country
ip.geoip.dst_asnum
ip.geoip.dst_city
ip.geoip.dst_country
ip.geoip.dst_lat
ip.geoip.dst_lon
ip.geoip.lat
ip.geoip.lon
ip.geoip.src_asnum
ip.geoip.src_city
ip.geoip.src_country
ip.geoip.src_lat
ip.geoip.src_lon

I have not seen the following work, but they are also included in the documentation. Maybe they are "coming soon", or possibly they require another database.

ip.geoip.dst_isp
ip.geoip.isp

ip.geoip.org
ip.geoip.dst_org
ip.geoip.src_isp
ip.geoip.src_org

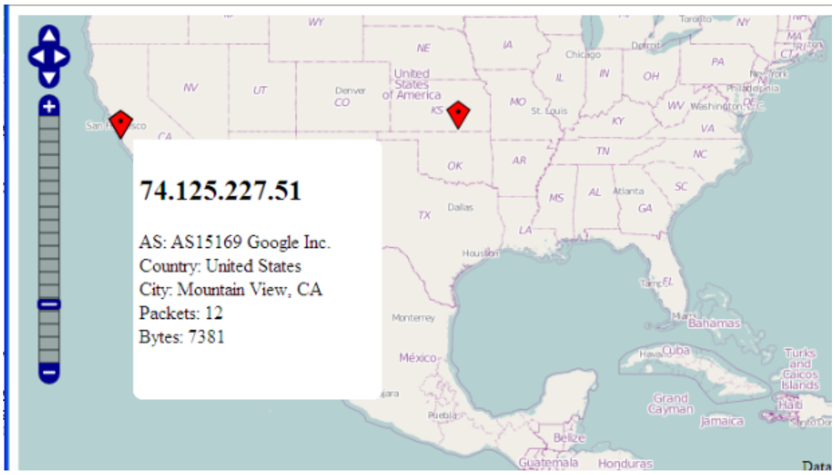
The final feature that was added with GeoIP is the ability to see this information in “Endpoints”. So if I click “Statistics” then “Endpoints”, I bring up a list of all endpoints from different layers of the OSI model. By choosing “IPv4”, I can see the new columns of “Country”, “AS Number”, “City”, “Latitude” and “Longitude”. I also have the “Map” button.


m NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) (tcp port 80)
el | FDDI | IPv4: 68 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 320 | Token Ring | UDP | USB | WLAN
IPv4 Endpoints

s	Rx Bytes	Country	AS Number	City	Latitude	Longitude
469	11 211 315	-	-	-	-	-
12	3 312	United States	AS15169 Google Inc.	Mountain View, CA	37.419201	-122.057404
13	1 280	United States	AS2828 XO Communications	-	38.000000	-97.000000
6	1 808	United States	AS15169 Google Inc.	Mountain View, CA	37.419201	-122.057404
6	1 215	United States	AS15169 Google Inc.	Mountain View, CA	37.419201	-122.057404
93	10 001	United States	AS5662 Turner Broadcasting	Atlanta, GA	33.800400	-84.386497
677	84 539	United States	AS3356 Level 3 Communications	Grapevine, TX	32.923401	-97.081001
56	13 618	United States	AS5662 Turner Broadcasting	Atlanta, GA	33.800400	-84.386497
213	25 489	United States	AS3356 Level 3 Communications	Grapevine, TX	32.923401	-97.081001
16	7 514	United States	AS19024 Internap Network Servic	Bellevue, WA	47.615398	-122.210297
8	1 344	United States	AS2914 NTT America, Inc.	Englewood, CO	39.569000	-104.858200
12	1 824	United States	AS31883 Kanoodle.com	-	38.000000	-97.000000
14	3 001	United States	AS15169 Google Inc.	Mountain View, CA	37.419201	-122.057404
7	3 720	United States	AS10913 Internap Network Servic	Bellevue, WA	47.615398	-122.210297

☐ Limit to display filter

If I choose “Map”, Wireshark launches an OpenStreetMap view of my endpoints in my default browser. By clicking individual endpoints, the AS Number, Country, City, Packet and Byte counts are displayed.


74.125.227.51

AS: AS15169 Google Inc.
Country: United States
City: Mountain View, CA
Packets: 12
Bytes: 7381

Packet analysis can be a daunting task. However, it is something that the more that you do it, the easier it becomes. Becoming comfortable with doing protocol analysis is crucial to most of our careers. Not doing so can limit our knowledge and our potential. I would recommend that everyone work to further their skills in this area. I also want to mention that Laura Chappell wrote an excellent book about Wireshark and protocol analysis. I recommend it to anyone seriously desiring to understand how things work. Understanding what is going on from the wire perspective is crucial to configuring the Cisco products that we use to transmit frames and packets as well as to understanding security. When troubleshooting, I often see people using a “sniffer” as last choice. In many cases it should be the first choice.   If not very familiar with protocol analysis, people tend to be overwhelmed with gazillions of packets, or focus on something that is meaningless in the big scheme of things. I see one benefit of GeoIP is helping us get a 10,000 foot view. That can help bridge the gap between the 40,000 foot view and the 1,000 foot view. By providing new and exciting ways to create display filters, Wireshark can help us more quickly focus on what is important to us.

Links from this article
MaxMind Geolocation Technology
7ZIP
Wireshark
Wireshark Network Analysis Study Guide

12481 Views Tags:

MOST LIKED

6 Comments

Scott Morris - CCDE/4xCCIE/2xJNCIE Dec 12, 2010 9:12 PM

Excellent post by the way!

But the one thing I'll caution everyone about is that it's not perfect. The geolocation relies on the accuracy of BGP information and what SWIP (whois stuff) that has been filled out for allocations and suballocations.

Many times, you'll find things aren't entirely accurate. All of the IPs that I have control over show up as "Nicholasville, KY" which is true from an adminsitrative point of view, but has nothing to do with the physical location of equipment as the equipment may be in several different locations.

I had picked a few things from other well known sites and was able to pick IPs that I knew the physical locations of and still found the geolocation picking the "admin" location of the whois lookups.

Still quite cool, and MAY be very useful in looking at things. But just be aware it's not perfect! Fun though!

Awesome post though.

Scott

Actions

Paul Stewart - CCIE Security Dec 13, 2010 2:56 AM (in response to Scott Morris - CCDE/4xCCIE/2xJNCIE)

Scott, that is a very good point. Geolocation isn't as perfect as a GPS in our phone constantly giving away our location. It is, as you pointed out, an administered database and subject to the limitations and errors of that.

Actions

Sean Iverson Dec 21, 2010 9:28 AM

Really great post -- and great layout. Thank you!!

Actions

navlesh Mar 15, 2011 9:59 AM

its very nice ....thank's for helping...

Actions

JCMan1123 Jul 17, 2014 11:41 AM

I have a question regarding this feature. First off this is a way cool tool to learn about in Wireshark! My issue is when I load the databases into the path for Wireshark, and then go to protocols, I don't have just the "IP" option, I have IPV4 and 6. So I enabled lookups in both. However after I check a public IP and try to load maps it says "no Longitute or Latitude found". When I downloaded the three files I didn't have to extract anything. Just copied to desired directory. Am I missing something?

Cheers.

Actions

JCMan1123 Oct 30, 2014 2:53 PM

Did a new download and install of the database files, enabled lookups and still getting "no longitude or laditude found". Has anyone else seen this issue? Thanks.

Actions

Terms & Conditions   Privacy Statement   Cookie Policy   Trademarks   Languages   Follow us: