The sys admin's daily grind: GeoIP lookup

Land Ahoy!

The global village is big enough to want to find out where your friend and enemies have set up camp. Charly offers a quick IP-based introduction to geography. *By Charly Kühnast*

All popular distributions include one or more packages that identify the country of origin of an IP address. On my Ubuntu lab machine, I use the `geoip-bin` and `geoip-database` packages. Now, you can also use the `geoiplookup` command, and `geoiplookup6` for IPv6 addresses, with an IP address or a name as a command-line parameter:

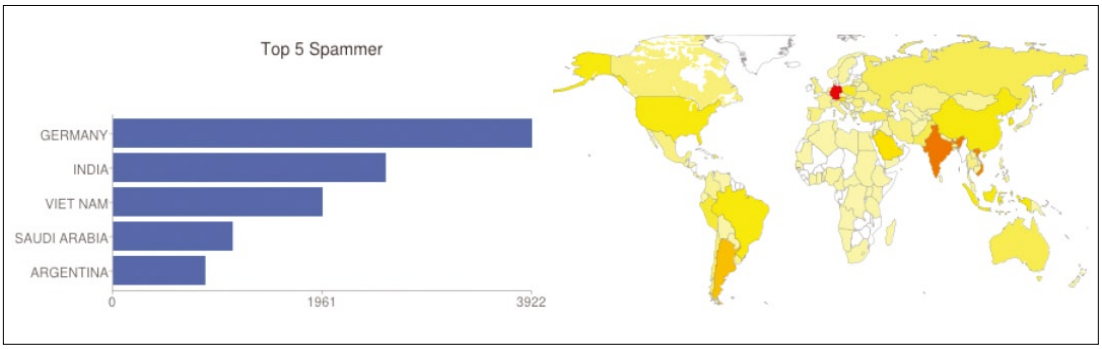

Figure 1: Germany is the world champion! At least on this strange Sunday and for Charly's antispam system with its integrated GeoIP lookup.

```
$ geoiplookup linuxfoundation.org
GeoIP Country Edition: US, United States
```

For most purposes, I just need to map the IP address to a country. My spam filters use this technique to determine the top five spammer domiciles on a daily basis. Figure 1 shows that this is Germany, but this is likely because I grabbed the screenshot on a Sunday. Germany is very rarely in the top five during the week.

If you need more granular resolution – that is, you don't just want the country, but the city, region, or organization – you can use GeoIP data by commercial providers. Typing `geoiplookup linuxfoundation.org` would then reveal the following:

```
GeoIP Country Edition:US, United States
GeoIP City Edition, Rev 1: US, OR, ➥
  Medford,N/A, 42.326500, -122.875603, ➥
  813, 541
GeoIP ASNum Edition: AS3701 Oregon ➥
  JointGraduate Schools of Engineering
```

A `libapache2_mod_geoip` module is available for web servers. This helps me direct users to the area of the site localized for them based on their origin.

Sorting by Country

To sort by country, I added the following to my `httpd.conf`:

```
GeoIPEnable On
GeoIPDBFile /usr/share/geoip/geoip.dat
```

You might also need to modify the path. I then added the lines from Listing 1 to my `.htaccess` file.

The accuracy of the geodetic data is almost always good enough, at least at the country level, but exceptions just go to prove the rule.

Cellular radio providers route their HTTP traffic through mandatory proxies. Depending on the network load, the proxy might be in a neighboring country, giving rise to suspicions of mass emigrations. ■■■

LISTING 1: .htaccess Additions

```
01 #IP Address of .de
02 RewriteEngine on
03 RewriteCond %{ENV:GEOIP_COUNTRY_CODE} ^DE$
04 RewriteRule ^(.*)$ http://www.example.com/de
05
06 #Everyone else sees the English page:
07 RewriteEngine on
08 RewriteRule ^(.*)$ http://www.example.com/en/
```

AUTHOR

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, freshwater aquariums, and learning Japanese, respectively.