# GeoIP List Conversion for Security Tools "geo2nginx.pl"

Ivan Bütler – 13.1.2010

**GeoIP Databases Conversion for your security tool**

This very short article teaches you how to generate open source security tool compatible target internet addresses out of  the public available GeoIP database.

## What is GeoIP (from the vendor)

**What is GeoIP?**

GeoIP® is the proprietary technology that drives MaxMind's IP geolocation data and services. GeoIP provides businesses with a non-invasive way to determine geographical and other information about their Internet visitors in real-time. When a person visits your website, GeoIP can determine which country, region, city, postal code, area code the visitor is coming from. Furthermore, GeoIP can provide information such as longitude/latitude, connection speed, ISP, company name, domain name, and whether the IP address is an anonymous proxy or satellite provider.

**How does GeoIP work?**

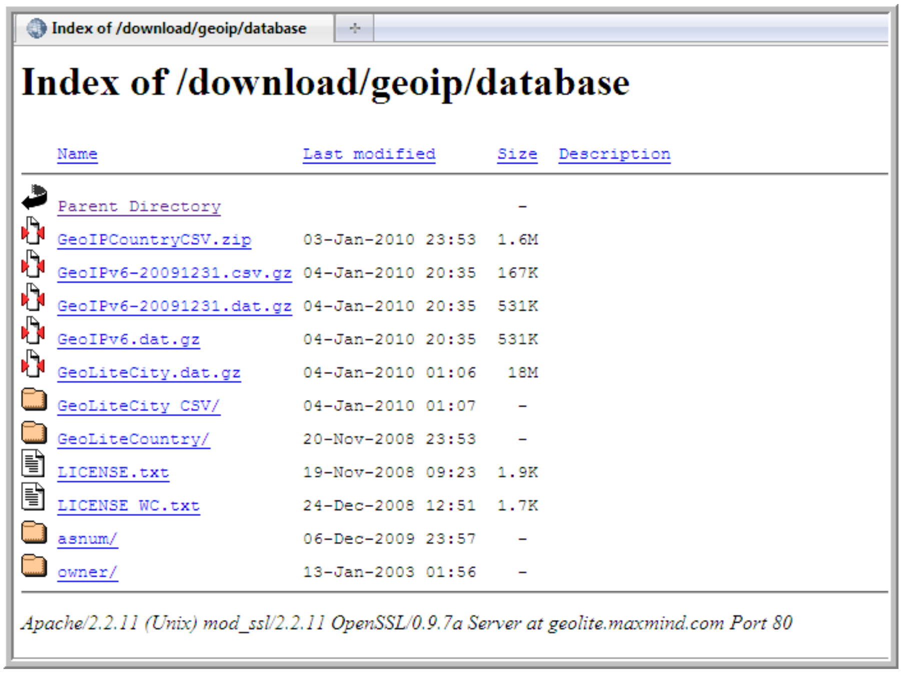
The idea behind GeoIP is simple but the process is complex. We employ user-entered location data from sites that ask web visitors to provide their geographic location. We then run millions of these datasets through a series of algorithms that identify, extract, and extrapolate location points for IP addresses.

**What can GeoIP be used for?**

To name a few applications, GeoIP can be used for delivering customized content, targeted ads, web log statistics, digital rights management, and regulatory compliance. In fact, you may already be using GeoIP without realizing it. MaxMind's GeoIP technology has been integrated by many of our partners for adserving, fraud screening, web analytics, firewall/spam protection, and anti-phishing/anti-identity theft applications.

## Download Free GEO IP (GeoIPCountryCSV.zip)

First of all, you need to download GeoIP from http://geolite.maxmind.com/download/geoip/database/



# Index of /download/geoip/database

```
     Name                         Last modified       Size  Description

     Parent Directory                                   -
     GeoIPCountryCSV.zip          03-Jan-2010 23:53  1.6M
     GeoIPv6-20091231.csv.gz      04-Jan-2010 20:35  167K
     GeoIPv6-20091231.dat.gz      04-Jan-2010 20:35  531K
     GeoIPv6.dat.gz               04-Jan-2010 20:35  531K
     GeoLiteCity.dat.gz           04-Jan-2010 01:06   18M
     GeoLiteCity_CSV/             04-Jan-2010 01:07    -
     GeoLiteCountry/              20-Nov-2008 23:53    -
     LICENSE.txt                  19-Nov-2008 09:23  1.9K
     LICENSE_WC.txt               24-Dec-2008 12:51  1.7K
     asnum/                       06-Dec-2009 23:57    -
     owner/                       13-Jan-2003 01:56    -
```

*Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.7a Server at geolite.maxmind.com Port 80*

Download the GeoIPCountryCSV.zip from the download area to your localhost

## Extract the Networks for a Country (Example Monaco)

```
grep -i monaco GeoIPCountryWhois.csv
"62.245.2.224","62.245.2.255","1056244448","1056244479","MC","Monaco"
"80.94.96.0","80.94.111.255","1348362240","1348366335","MC","Monaco"
"80.190.210.60","80.190.210.63","1354682940","1354682943","MC","Monaco"
"82.97.10.48","82.97.10.63","1382091312","1382091327","MC","Monaco"
"82.97.10.112","82.97.10.127","1382091376","1382091391","MC","Monaco"
"82.97.12.0","82.97.12.255","1382091776","1382092031","MC","Monaco"
"82.97.14.80","82.97.14.111","1382092368","1382092399","MC","Monaco"
"82.97.16.16","82.97.16.31","1382092816","1382092831","MC","Monaco"
"82.97.16.128","82.97.16.143","1382092928","1382092943","MC","Monaco"
"82.97.17.64","82.97.17.95","1382093120","1382093151","MC","Monaco"
"82.97.18.192","82.97.19.15","1382093504","1382093583","MC","Monaco"
"82.97.20.0","82.97.20.63","1382093824","1382093887","MC","Monaco"
"82.97.21.0","82.97.21.63","1382094080","1382094143","MC","Monaco"
"82.97.22.0","82.97.22.15","1382094336","1382094351","MC","Monaco"
```

```
"82.97.23.0","82.97.23.31","1382094592","1382094623","MC","Monaco"
"82.113.0.0","82.113.31.255","1383137280","1383145471","MC","Monaco"
"85.119.2.96","85.119.2.127","1433862752","1433862783","MC","Monaco"
"87.238.104.0","87.238.111.255","1475241984","1475244031","MC","Monaco"
"87.254.224.0","87.254.255.255","1476321280","1476329471","MC","Monaco"
"88.209.64.0","88.209.83.255","1490108416","1490113535","MC","Monaco"
"88.209.86.0","88.209.87.255","1490114048","1490114559","MC","Monaco"
"88.209.126.0","88.209.127.255","1490124288","1490124799","MC","Monaco"
"91.199.109.0","91.199.109.255","1539796224","1539796479","MC","Monaco"
"91.207.172.0","91.207.175.255","1540336640","1540337663","MC","Monaco"
"193.201.151.64","193.201.151.127","3251214144","3251214207","MC","Monaco"
"194.9.12.0","194.9.13.255","3255372800","3255373311","MC","Monaco"
"194.51.26.0","194.51.26.255","3258128896","3258129151","MC","Monaco"
"195.20.192.0","195.20.193.255","3272916992","3272917503","MC","Monaco"
"195.25.174.160","195.25.174.167","3273240224","3273240231","MC","Monaco"
"195.78.0.0","195.78.31.255","3276668928","3276677119","MC","Monaco"
"195.101.219.192","195.101.219.255","3278232512","3278232575","MC","Monaco"
"195.112.166.76","195.112.166.79","3278939724","3278939727","MC","Monaco"
"205.147.149.30","205.147.149.30","3449001246","3449001246","MC","Monaco"
"206.182.133.0","206.182.133.255","3468068096","3468068351","MC","Monaco"
"208.198.180.0","208.198.180.255","3502683136","3502683391","MC","Monaco"
"209.132.219.128","209.132.219.191","3515145088","3515145151","MC","Monaco"
"213.137.128.0","213.137.159.255","3582558208","3582566399","MC","Monaco"
"217.204.159.108","217.204.159.111","3654066028","3654066031","MC","Monaco"
```

The list cannot be used for most of the open source network security tools. We need to convert the ranges into the following format

[START-IP]-[STOP-IP] example 192.168.100.0-192.168.100.255

Or

[IP-NETWORK/Mask] example 192.168.100.0/24

## Geo IP Conversion Manually

```
grep -i monaco GeoIPCountryWhois.csv | \
awk 'BEGIN{FS=","}{print $1"-"$2}' | sed 's/"//g'

62.245.2.224-62.245.2.255
80.94.96.0-80.94.111.255
80.190.210.60-80.190.210.63
82.97.10.48-82.97.10.63
82.97.10.112-82.97.10.127
82.97.12.0-82.97.12.255
82.97.14.80-82.97.14.111
82.97.16.16-82.97.16.31
82.97.16.128-82.97.16.143
82.97.17.64-82.97.17.95
82.97.18.192-82.97.19.15
82.97.20.0-82.97.20.63
82.97.21.0-82.97.21.63
82.97.22.0-82.97.22.15
82.97.23.0-82.97.23.31
```

```
82.113.0.0-82.113.31.255
85.119.2.96-85.119.2.127
87.238.104.0-87.238.111.255
87.254.224.0-87.254.255.255
88.209.64.0-88.209.83.255
88.209.86.0-88.209.87.255
88.209.126.0-88.209.127.255
91.199.109.0-91.199.109.255
91.207.172.0-91.207.175.255
193.201.151.64-193.201.151.127
194.9.12.0-194.9.13.255
194.51.26.0-194.51.26.255
195.20.192.0-195.20.193.255
195.25.174.160-195.25.174.167
195.78.0.0-195.78.31.255
195.101.219.192-195.101.219.255
195.112.166.76-195.112.166.79
205.147.149.30-205.147.149.30
206.182.133.0-206.182.133.255
208.198.180.0-208.198.180.255
209.132.219.128-209.132.219.191
213.137.128.0-213.137.159.255
217.204.159.108-217.204.159.111
```

## Geo IP Conversion Perl Script

Because of my lazy nature, I was searching for an existing solution and found a perl written parser of GeoIP in the ngxinx webserver package

About ngxinx http://nginx.org/en/ "*nginx [engine x] is a HTTP and reverse proxy server, as well as a mail proxy server written by Igor Sysoev. It has been running for more than five years on many heavily loaded Russian sites including Rambler (RamblerMedia.com). According to Netcraft nginx served or proxied 4.24% busiest sites in January 2010. Here are some of success stories: FastMail.FM, Wordpress.com.*"

```
grep -i monaco GeoIPCountryWhois.csv | perl geo2nginx.pl
62.245.2.224/27 MC;
80.94.96.0/20 MC;
80.190.210.60/30 MC;
82.97.10.48/28 MC;
82.97.10.112/28 MC;
82.97.12.0/24 MC;
82.97.14.80/28 MC;
82.97.14.96/28 MC;
82.97.16.16/28 MC;
82.97.16.128/28 MC;
82.97.17.64/27 MC;
82.97.18.192/26 MC;
82.97.19.0/28 MC;
82.97.20.0/26 MC;
82.97.21.0/26 MC;
82.97.22.0/28 MC;
82.97.23.0/27 MC;
82.113.0.0/19 MC;
85.119.2.96/27 MC;
87.238.104.0/21 MC;
87.254.224.0/19 MC;
```

```
88.209.64.0/20 MC;
88.209.80.0/22 MC;
88.209.86.0/23 MC;
88.209.126.0/23 MC;
91.199.109.0/24 MC;
91.207.172.0/22 MC;
193.201.151.64/26 MC;
194.9.12.0/23 MC;
194.51.26.0/24 MC;
195.20.192.0/23 MC;
195.25.174.160/29 MC;
195.78.0.0/19 MC;
195.101.219.192/26 MC;
195.112.166.76/30 MC;
205.147.149.30/32 MC;
206.182.133.0/24 MC;
208.198.180.0/24 MC;
209.132.219.128/26 MC;
213.137.128.0/19 MC;
217.204.159.108/30 MC;
```

## Result

The resulting ip target lists can now be used with your preferred security tool.

## Thank you for Reading

14. January 2010 by Ivan Bütler

ivan.buetler@csnc.ch