IP Finder & GeoIP for Fun

2012.3.3 FORENSIC INSIGHT

Kevin Koo
(kevinkoo001@gmail.com)

개요

- MaxMind
- GeoIP
- GeoIP API

MaxMind 기본

1. The accuracy of the GeoIP Databases

- 99.8% accurate on a country level
- 90% accurate on a state level
- 83% accurate for cities in the US within a 25 miles

2. How many IP addresses are in the database? (AS OF 2012.2.1)

- http://www.maxmind.com/app/techinfo
- Total number of IP Blocks on the country level (Database records): 153,821
- Total number of IP addresses: 3,431,032,465
- Total number of countries: 248

3. Free Download (AS OF 2012.2.7, Next update 2012.3.6)

- http://geolite.maxmind.com/download/geoip/database/GeoIPCountryCSV.zip
- http://geolite.maxmind.com/download/geoip/database/GeoIPv6.csv.gz
- http://geolite.maxmind.com/download/geoip/database/GeoLiteCity_CSV/GeoLiteCity_20120207.zip

MaxMind 활용

4. A1 = Anonymous Proxy Entries

- IP addresses that belong to anonymous proxies or VPN services such as Anonymizer
- Used by users to hide or to disguise their IP address

5. A2 = Satellite Providers

- ISPs that offer Internet access to many countries through satellites

6. Proxy Detection Web Service

- Perl, ASP and PHP with license key
- http://www.maxmind.com/app/web_services_ipauth_usage

MaxMind 활용

http://ipinfodb.com/

(1) IP Location API
XML API: http://api.ipinfodb.com/v3/ip-city/?key=<key>&ip=74.125.45.100
JSON API: http://api.ipinfodb.com/v3/ip-city/?key=<key>&ip=74.125.45.100&format=json

```
{                   "statusCode" : "OK",
                    "statusMessage" : "",
                    "ipAddress" : "74.125.45.100",
                    "countryCode" : "US",
                    "countryName" : "UNITED STATES",
                    "regionName" : "GEORGIA",  "cityName" : "ATLANTA",
                    "zipCode" : "30301",
                    "latitude" : "33.809",
                    "longitude" : "-84.3548",
                    "timeZone" : "-05:00“
}
```

(2) Block IP by Country

(3) Fraud Detection API
http://api.ipinfodb.com/v2/fraud_query.php?key=<key>&ip=74.125.45.100&country_code=us

GeoIP APIs

GeoIP APIs

- C Library
- Perl Module
- PHP Module
- Apache Module (mod_geoip)
- Java Class
- Python Class
- C# Class
- Ruby Module
- MS COM Object (ASP, ColdFusion, Pascal, PHP, Perl, Python, and Visual Basic code)
- VB.NET (Only works with GeoIP Country)
- Pascal
- JavaScript

GeoIP APIs

GeoIP APIs with C Library

(1) Installation

```
# ./configure
# make; make check; make install
```

(2) Compilation

```
# gcc -lGeoIP getip.c –o getip
```

(3) Usage

```
#include <GeoIP.h>
int main (int argc, char *argv[]) {
    GeoIP * gi;
    gi = GeoIP_new(GEOIP_STANDARD);
    printf("code %s\n“,  GeoIP_country_code_by_name(gi, "yahoo.com"));
}
```

GeoIP APIs

GeoIP APIs with Python (Pygeoip)

https://github.com/appliedsec/pygeoip

(1) Installation

```
# wget http://geolite.maxmind.com/download/geoip/database/GeoLiteCity_CSV/GeoLiteCity_20120207.zip
# unzip -d GeoLiteCity_20120207.zip
# wget http://pygeoip.googlecode.com/files/pygeoip-0.2.2.tar.gz
# tar zxvf pygeoip-0.2.2.tar.gz
# cd pygeoip-0.2.2
# python setup.py build
# python setup.py install
```

(2) Test

```
# python
 >>> import pygeoip
 >>> gip = pygeoip.GeoIP(‘GeoLiteCity.dat’)
 >>> rec = gip.record_by_name(‘yahoo.com’)
 >>> for key,val in rec.items():
 … print “%s: %s” % (key,val)
 …
```

```
city: Sunnyvale
region_name: CA
area_code: 408
longitude: -122.0074
country_code3: USA
latitude: 37.4249
postal_code: 94089
dma_code: 807
country_code: US
country_name: United States
```

Applied GeoIP APIs

Generating Static Images with Matplotlib

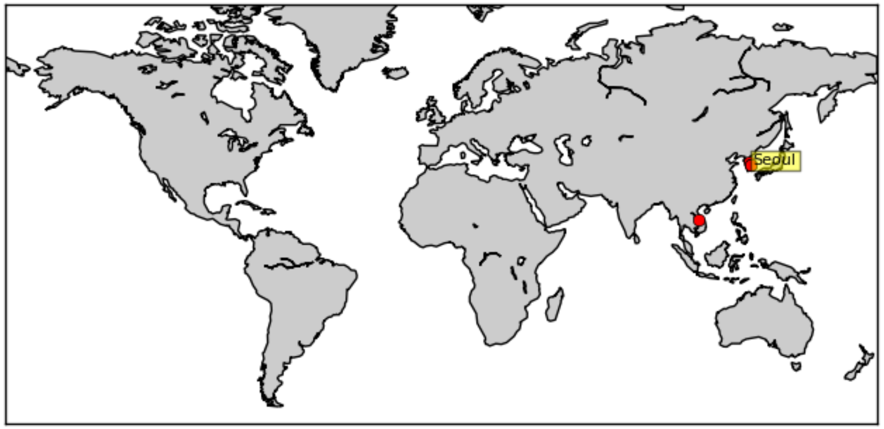
http://sourceforge.net/projects/matplotlib/files/matplotlib-toolkits/basemap-0.99.4/basemap-0.99.4.tar.gz

(1) Installation

```
# apt-get install python-tk python-numpy python-matplotlib python-dev
# tar -xvzf basemap-0.99.4.tar.gz
# cd basemap-0.99.4/geos-2.2.3
# ./configure; make; make install
# cd ..
# python setup.py build
# python setup.py install
```

(2) Test

```
# python mapper.py –a 112.213.89.30,116.193.83.147,119.70.227.138,121.88.250.247,124.217.218.6
```



What I did with GeoIP

* EXCEL with GeoIPCountry.csv

END

QUESTIONS?