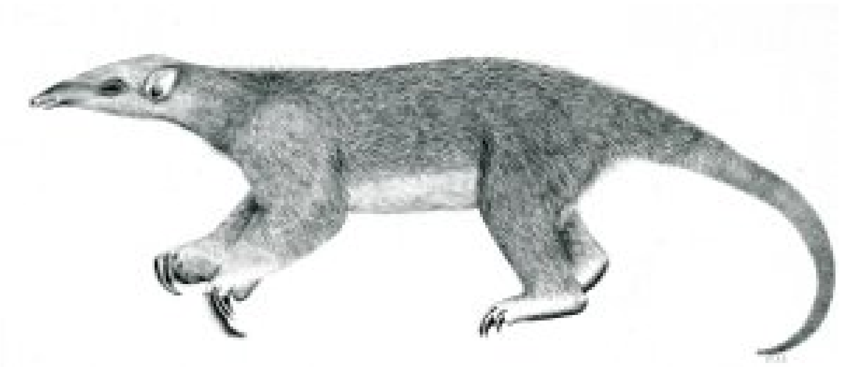
# Tranalyzer2

## geoip

Geo-Localization of IP Addresses



Tranalyzer Development Team

# Contents

# 1 geoip

## 1.1 Description

This plugin outputs the geographic location of IP addresses.

## 1.2 Dependencies

This product includes GeoLite2 data created by MaxMind, available from http://www.maxmind.com.
Legacy databases (`GeoLiteCity.data.gz` and `GeoLiteCityv6.dat.gz`) require *libgeoip*, while GeoLite2 requires *libmaxminddb*.

**Ubuntu:** `sudo apt-get install libgeoip-dev libmaxminddb-dev`

**Kali:** `sudo apt-get install libgeoip-dev`

**OpenSUSE:** `sudo zypper install libGeoIP-devel`

**Arch:** `sudo pacman -S geoip`
*libmaxminddb* can be found in the Arch User Repository (AUR) at
https://aur.archlinux.org/packages/libmaxminddb.

**Mac OS X:** `brew install geoip libmaxminddb`

### 1.2.1 Databases Update

The geoIP databases can be updated with the `updatedb.sh` script as follows:

```
./scripts/updatedb.sh
```

Alternatively the latest version of the databases can be found at https://dev.maxmind.com/geoip/geoip2/geolite2/ (GeoLite2-City). Legacy databases, the latest version of which can be found at https://dev.maxmind.com/geoip/legacy/geolite (Geo Lite City and Geo Lite City IPv6), are also supported.

## 1.3 Configuration Flags

The following flags can be used to control the output of the plugin (Information in italic only applies to legacy databases):

| Name | Default | Description |
|---|---|---|
| `GEOIP_LEGACY` | 0 | Whether to use GeoLite2 (0) or the GeoLite legacy database (1) |
| `GEOIP_SRC` | 1 | Display geo info for the source IP |
| `GEOIP_DST` | 1 | Display geo info for the destination IP |
| `GEOIP_CONTINENT` | 2 | 0: no continent, 1: name (**GeoLite2**), 2: two letters code |
| `GEOIP_COUNTRY` | 2 | 0: no country, 1: name, 2: two letters code, *3: three letters code* |

| Name | Default | Description |
|---|---|---|
| GEOIP_REGION | *1* | *0: no region, 1: name, 2: code* |
| GEOIP_CITY | 1 | Display the city of the IP |
| GEOIP_POSTCODE | 1 | Display the postal code of the IP |
| GEOIP_ACCURACY | 1 | (**GeoLite2**) Display the accuracy of the geolocation |
| GEOIP_POSITION | 1 | Display the position (latitude, longitude) of the IP |
| GEOIP_METRO_CODE | 0 | Display the metro (dma) code of the IP (US only) |
| GEOIP_AREA_CODE | *0* | *Display the telephone area code of the IP* |
| GEOIP_NETMASK | *1* | *0: no netmask, 1: netmask as int (cidr), 2: netmask as hex, 3: netmask as IP* |
| GEOIP_TIME_ZONE | 1 | (**GeoLite2**) Display the time zone |
| GEOIP_LANG | "en" | (**GeoLite2**) Language to use:<br>Brazilian Portuguese (pt-BR), English (en), French (fr), German (de), Japanese (jp), Russian (ru), Simplified Chinese (zh-CN) or Spanish (es) |
| GEOIP_BUFSIZE | 64 | (**GeoLite2**) Buffer size |
| GEOIP_DB_CACHE | *2* | *0: read DB from file system (slower, least memory)*<br>*1: index cache (cache frequently used index only)*<br>*2: memory cache (faster, more memory)* |
| GEOIP_UNKNOWN | "--" | Representation of unknown locations (GeoIP's default) |

## 1.4 Flow File Output

The geoip plugin outputs the following columns (for src and dst IP):

| Column | Type | Description | Flags |
|---|---|---|---|
| srcIpContinent | S | Continent name | GEOIP_CONTINENT=1 |
| srcIpContinent | SC | Continent code | GEOIP_CONTINENT=2 |
| srcIpCountry | S | Country name | GEOIP_COUNTRY=1 |
| srcIpCountry | SC | Country code | GEOIP_COUNTRY=2\|3 |
| srcIpRegion | SC | Region | GEOIP_REGION=1 |
| srcIpRegion | S | Region | GEOIP_REGION=2 |
| srcIpCity | S | City | |
| srcIpPostcode | SC | Postal code | |
| srcIpAccuracy | U16 | Accuracy of the geolocation (in km) | |
| srcIpLatitude | D | Latitude | GEOIP_LEGACY=0 |
| srcIpLongitude | D | Longitude | GEOIP_LEGACY=0 |
| srcIpLatitude | F | Latitude | GEOIP_LEGACY=1 |
| srcIpLongitude | F | Longitude | GEOIP_LEGACY=1 |
| srcIpMetroCode | U16 | Metro (DMA) code (US only) | GEOIP_LEGACY=0 |
| srcIpMetroCode | I32 | Metro (DMA) code (US only) | GEOIP_LEGACY=1 |
| srcIpAreaCode | I32 | Area code | |
| srcIpNetmask | U32 | Netmask (CIDR) | GEOIP_NETMASK=1 |
| srcIpNetmask | H32 | Netmask | GEOIP_NETMASK=2 |

| **Column** | **Type** | **Description** | **Flags** |
|---|---|---|---|
| srcIpNetmask | IP4 | Netmask | GEOIP_NETMASK=3 |
| srcIpTimeZone | S | Time zone | |
| geoStat | H8 | Status | GEOIP_LEGACY=0 |

### 1.4.1 srcIpContinent

Continent codes are as follows:

| Code | Description |
|---|---|
| AF | Africa |
| AS | Asia |
| EU | Europe |
| NA | North America |
| OC | Oceania |
| SA | South America |
| -- | Unknown (see GEOIP_UNKNOWN) |

### 1.4.2 geoStat

The geoStat column is to be interpreted as follows:

| geoStat | Description |
|---|---|
| $2^0$ (=0x01) | A string had to be truncated... increase GEOIP_BUFSIZE |

## 1.5 Post-Processing

The geoIP plugin comes with the genkml.sh script which generates a KML (Keyhole Markup Language) file from a flow file. This KML file can then be loaded in Google Earth to display the location of the IP addresses involved in the dump file. Its usage is straightforward:

```
./scripts/genkml.sh FILE_flows.txt
```