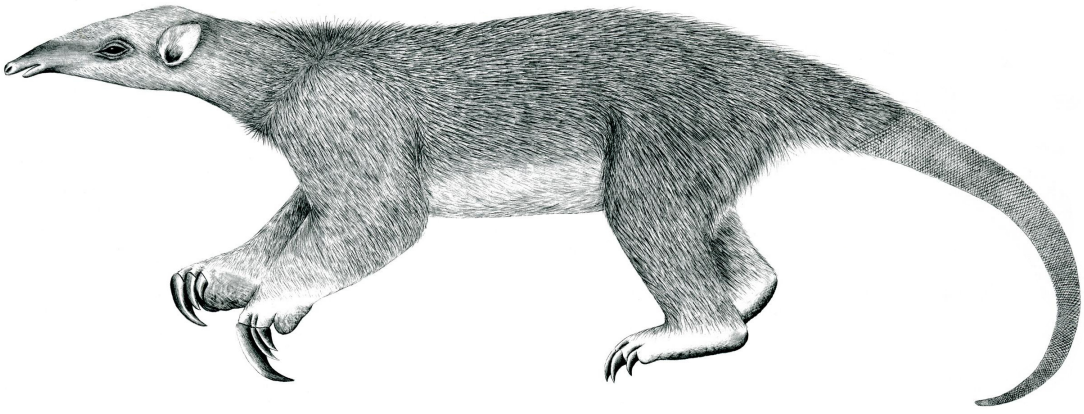
Tranalyzer2

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.
The required dependencies depend on the value of GEOIP_LIB:

- GEOIP_LIB=0:
  Legacy databases (GeoLiteCity.data.gz and GeoLiteCityv6.dat.gz) require *libgeoip*.
- GEOIP_LIB=1:
  GeoLite2 requires *libmaxminddb*.

		GEOIP_LIB=1	GEOIP_LIB=0
Ubuntu:	sudo apt-get install	libmaxminddb-dev	libgeoip-dev
Arch:	sudo pacman -S	libmaxminddb	geoip
Gentoo:	sudo emerge	libmaxminddb	geoip
openSUSE:	sudo zypper install	libmaxminddb-devel	libGeoIP-devel
Red Hat/Fedora[1]:	sudo dnf install	libmaxminddb-devel	GeoIP-devel
macOS[2]:	brew install	libmaxminddb	geoip

1.2.1 Databases Update

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_LIB	2	Library to use: 2: GeoLite2 / Internal libmaxmind (faster) 1: GeoLite2 / libmaxmind 0: GeoLite / geoip (legacy)
GEOIP_SRC	1	Display geo info for the source IP
GEOIP_DST	1	Display geo info for the destination IP

[1] If the dnf command could not be found, try with yum instead
[2] Brew is a packet manager for macOS that can be found here: https://brew.sh

Name	Default	Description
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*
GEOIP_CITY	1	Display the city of the IP
GEOIP_POSTCODE	1	Display the postal code of the IP
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)
If GEOIP_LIB!=0, the following flags are available:		
GEOIP_ACCURACY	1	Display the accuracy of the geolocation
GEOIP_TIMEZONE	1	Display the time zone
The six following flags are only available in GeoLite2 Enterprise databases:		
GEOIP_ORG	0	Display the organization of the IP
GEOIP_ISP	0	Display the ISP name of the IP
GEOIP_ASN	0	Display the autonomous systems number of the IP
GEOIP_ASNAME	0	Display the autonomous systems name of the IP
GEOIP_CONNT	0	Display the connection type of the IP
GEOIP_USRT	0	Display the user type of the IP
GEOIP_DB_FILE	"GeoLite2-City.mmdb"	Name of the database to use for IPv4 and IPv6 (combined)
GEOIP_LANG	"en"	Language to use: de: German, en: English, es: Spanish, fr: French, jp: Japanese, pt-BR: Brazilian Portuguese, ru: Russian, zh-CN: Simplified Chinese
GEOIP_BUFSIZE	64	Buffer size
If GEOIP_LIB==0, the following flags are available:		
GEOIP_REGION	*1*	*0: no region, 1: name, 2: code*
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*

Name	Default	Description
GEOIP_DB_CACHE	*2*	*0: read DB from file system (slower, least memory)* *1: index cache (cache frequently used index only)* *2: memory cache (faster, more memory)*
GEOIP_DB_FILE4	*"GeoLiteCity.dat"*	*Name of the database to use for IPv4*
GEOIP_DB_FILE6	*"GeoLiteCityv6.dat"*	*Name of the database to use for IPv6*
GEOIP_UNKNOWN	"--"	Representation of unknown locations (GeoIP's default)

1.3.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- GEOIP_DB_FILE (require GEOIP_LIB>0)
- GEOIP_DB_FILE4 (require GEOIP_LIB=0)
- GEOIP_DB_FILE6 (require GEOIP_LIB=0)
- GEOIP_UNKNOWN

1.4 Flow File Output

The geoip plugin outputs the following columns:

Column	Type	Description	Flags
The following columns prefixed with src are only output if GEOIP_SRC=1.			
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_LIB=0&&GEOIP_REGION=1
srcIpRegion	S	Region	GEOIP_LIB=0&&GEOIP_REGION=2
srcIpCity	S	City	GEOIP_CITY>0
srcIpPostcode	SC	Postal code	GEOIP_POSTCODE>0
srcIpAccuracy	U16	Accuracy of the geolocation (in km)	GEOIP_LIB>0&&GEOIP_ACCURACY=1
srcIpLat	D	Latitude	GEOIP_LIB>0&&GEOIP_POSITION=1
srcIpLong	D	Longitude	GEOIP_LIB>0&&GEOIP_POSITION=1
srcIpLat	F	Latitude	GEOIP_LIB=0&&GEOIP_POSITION=1
srcIpLong	F	Longitude	GEOIP_LIB=0&&GEOIP_POSITION=1
srcIpMetroCode	U16	Metro (DMA) code (US only)	GEOIP_LIB>0&&GEOIP_METRO_CODE=1
srcIpMetroCode	I32	Metro (DMA) code (US only)	GEOIP_LIB=0&&GEOIP_METRO_CODE=1
srcIpAreaCode	I32	Area code	GEOIP_LIB=0&&GEOIP_AREA_CODE=1
srcIpNetmask	U32	Netmask (CIDR)	GEOIP_LIB=0&&GEOIP_NETMASK=1
srcIpNetmask	H32	Netmask	GEOIP_LIB=0&&GEOIP_NETMASK=2
srcIpNetmask	IP4	Netmask	GEOIP_LIB=0&&GEOIP_NETMASK=3

Column	Type	Description	Flags
srcIpTimeZone	S	Time zone	GEOIP_LIB=0&&GEOIP_TIMEZONE=1
srcIpOrg	S	Organization	GEOIP_LIB>0&&GEOIP_ORG=1
srcIpISP	S	ISP	GEOIP_LIB>0&&GEOIP_ISP=1
srcIpASN	U32	AS number	GEOIP_LIB>0&&GEOIP_ASN=1
srcIpASName	S	AS name	GEOIP_LIB>0&&GEOIP_ASNAME=1
srcIpConnT	S	Connection type	GEOIP_LIB>0&&GEOIP_CONNT=1
srcIpUsrT	S	User type	GEOIP_LIB>0&&GEOIP_USRT=1

The same columns (with prefix dst instead of src) are output for the destination address if GEOIP_DST=1.

geoStat	H8	Status

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
2^1	(=0x02)	Source IP lookup failed
2^2	(=0x04)	Destination IP lookup failed

1.5 Post-Processing

1.5.1 genkml

The geoip plugin comes with the genkml 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 FILE_flows.txt
```

1.5.2 t2mmdb

The t2mmdb program can be used to query the MaxMind DB. It is a faster and easier to use version of the mmdblookup utility.

1.5.3 t2mmdba

The t2mmdba script can be used to transform the MaxMind DB into Tranalyzer subnet format.