geoip

Synopsis

A display function that groups result events according to the extracted elements of the IP address in one or more of its geoip columns,.

Syntax

```
geoip ([IP_Column_Name]) group by [country,country code,city,region]
```

Required Arguments

`IP_column_name`

Syntax: <character string>

Description: The name of the column header that has IP address values

`country, country code, city, and/or region`

Description: The extracted part of the IP address according to which to group the results.

Optional Arguments

None

Description

For each event that has the specified IP_address_column_name with an IP address value, extracts the country name, country code, city, and/or region from the IP address, using an internal database, and then shows the result of performing a specific function on the search result events, according to the country name, country code, city, and/or region, as required.

Examples

Example 1:

```
* in log.access | count | geoip client ip group by country,city | order by count desc
```

Creates a summary table of the count of all events in log **access**, grouped according to the country and the city within the country, both extracted from the IP address in the **client ip** column. This table is ordered in descending order of the number of events in each city group.