Geolocation Information

Log files contain IP addresses which are not immediately useful. Users typically require real-world names. For example users want to know the country their visitors are from, their city, their organisation name, the ISP they use etc. Log files do not contain real-world information so the best Sawmill can provide (without additional reference data) is to report the IP address and the 'hostname' obtained by DNS resolution.

To go one step further and convert an IP address into a real-world name Sawmill needs a reference database that correlates IP addresses against real-world names. Once provided with the database Sawmill can perform the comparison operation and provide reports containing real-world data. Such a family of trusted geolocation databases are marketed by Maxmind (www.maxmind.com).

To get users started the '**GeoLite City**' database is included in all Sawmill products at no additional cost and it correlates IP addresses and city level data. A more accurate and more detailed version is available from Maxmind called the '**GeoIP City**' database. This can be purchased directly from Maxmind and installed in the 'LogAnalysisInfo' directory over the existing.

Other Maxmind databases are supported by Sawmill and are listed below. Their function and the data they contain should be clear from the title of each

GeoIP City *(includes **GeoIP Country** and **GeoIP Region** databases)*	must be the binary version and named GeoIP-532.dat
GeoIP Organization	must be the binary version and named GeoIPOrg.dat
GeoIP ISP	must be the binary version and named GeoIPISP.dat
GeoIP Domain Name	must be the binary version and named GeoIPDomain.dat