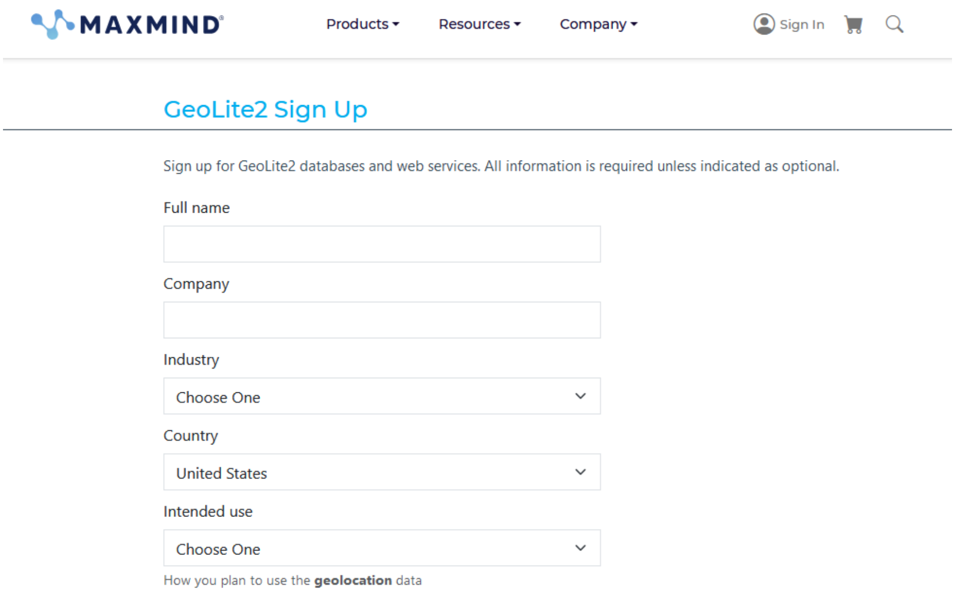
Enhancing Investigations in Wireshark through using MaxMind GeoIP databases

1. Introduction

Mapping addresses to their geographical locations can be incredibly beneficial when investigating PCAPs in Wireshark. Utilising GeoIP within Wireshark enables analysts and network forensic investigators to analyse network traffic with additional context, enhancing their ability to identify anomalous and malicious traffic. This document outlines the process of setting up GeoIP in Wireshark (for free) and discusses its applications and benefits for cybersecurity professionals.

2. Setting up GeoIP in Wireshark

To start, create an account on GeoLite2:



GeoLite2 Sign Up

Sign up for GeoLite2 databases and web services. All information is required unless indicated as optional.

Full name

Company

Industry

Choose One

Country

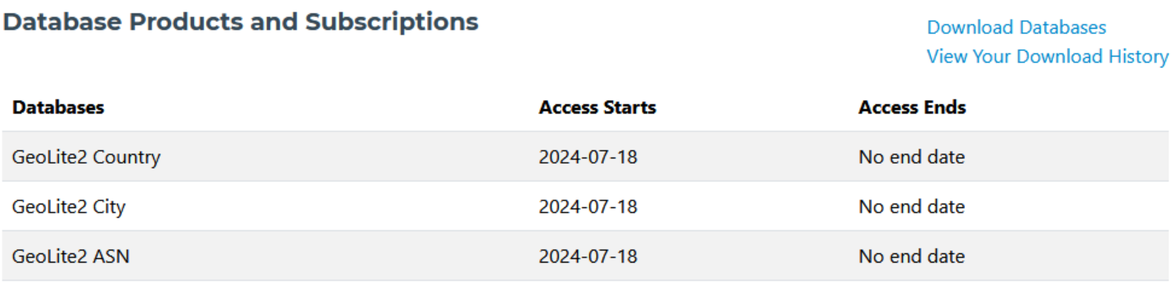
United States

Intended use

Choose One

How you plan to use the **geolocation** data

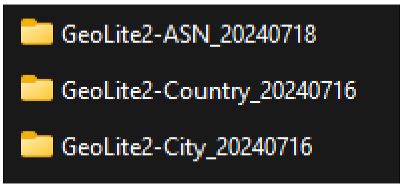
Once you have gone through the account creation process, you will be presented with a page like as follows:



Database Products and Subscriptions

Databases	Access Starts	Access Ends
GeoLite2 Country	2024-07-18	No end date
GeoLite2 City	2024-07-18	No end date
GeoLite2 ASN	2024-07-18	No end date

We want to download all of these databases. To do so, simply click the Download Databases button and download those 3 databases as a GZIP file. Make sure to unzip the files, after doing so, you should have something like as follows:



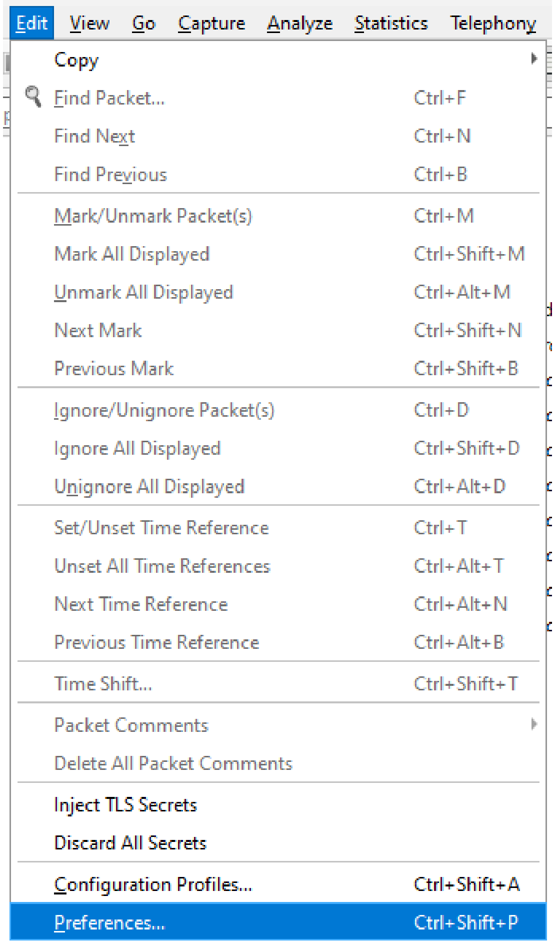
GeoLite2-ASN_20240718

GeoLite2-Country_20240716

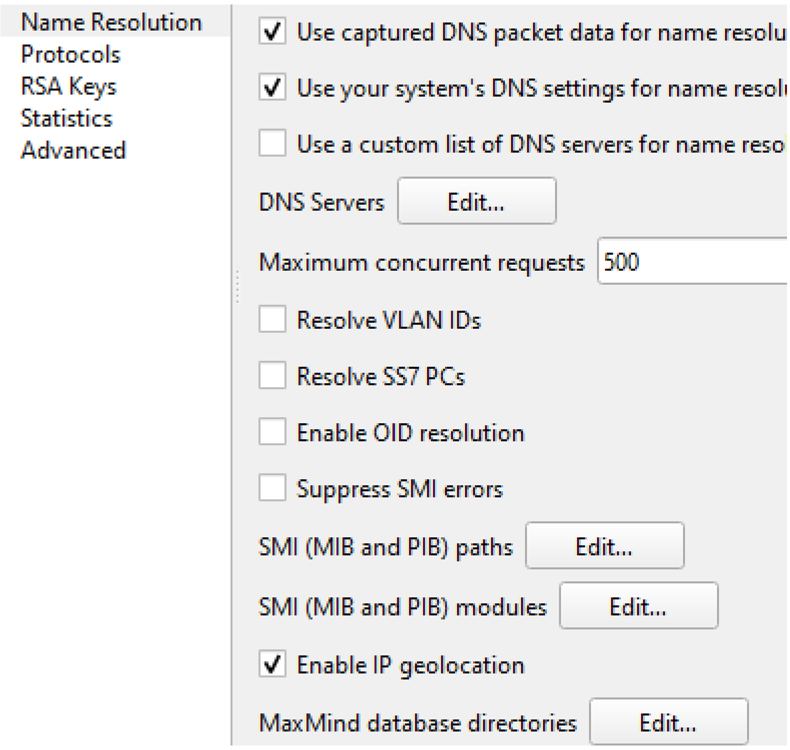
GeoLite2-City_20240716

3. Configuring Wireshark

open up Wireshark and navigate to Edit -> Preferences:


Edit
View
Go
Capture
Analyze
Statistics
Telephony
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet(s) Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet(s) Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comments
Delete All Packet Comments
Inject TLS Secrets
Discard All Secrets
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P

Then navigate to the Name Resolution section and click edit next to ‘MaxMind database directories’:



Name Resolution
Protocols
RSA Keys
Statistics
Advanced

☑ Use captured DNS packet data for name resolu

☑ Use your system's DNS settings for name resol

□ Use a custom list of DNS servers for name reso

DNS Servers

Maximum concurrent requests 500

□ Resolve VLAN IDs

□ Resolve SS7 PCs

□ Enable OID resolution

□ Suppress SMI errors

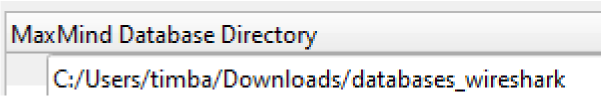
SMI (MIB and PIB) paths

SMI (MIB and PIB) modules

☑ Enable IP geolocation

MaxMind database directories

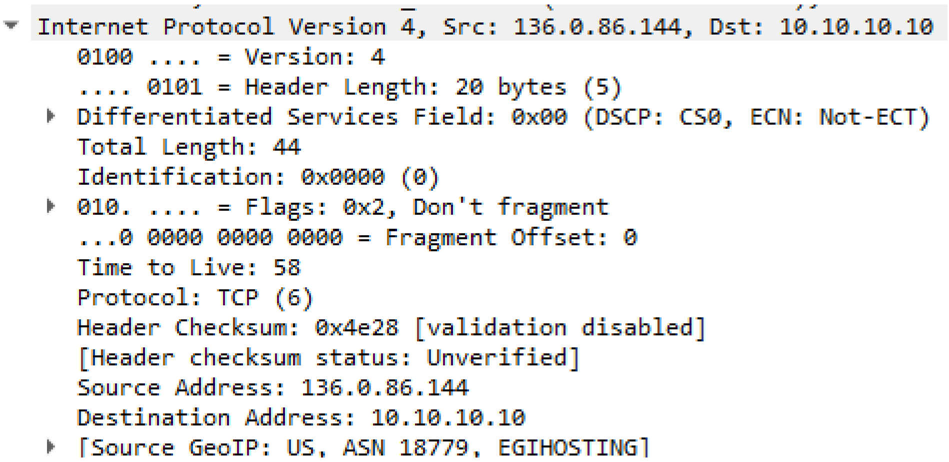
Once you have click edit, all we need to do is click the + button and add the location of the folder where all three databases are installed:



MaxMind Database Directory
C:/Users/timba/Downloads/databases_wireshark

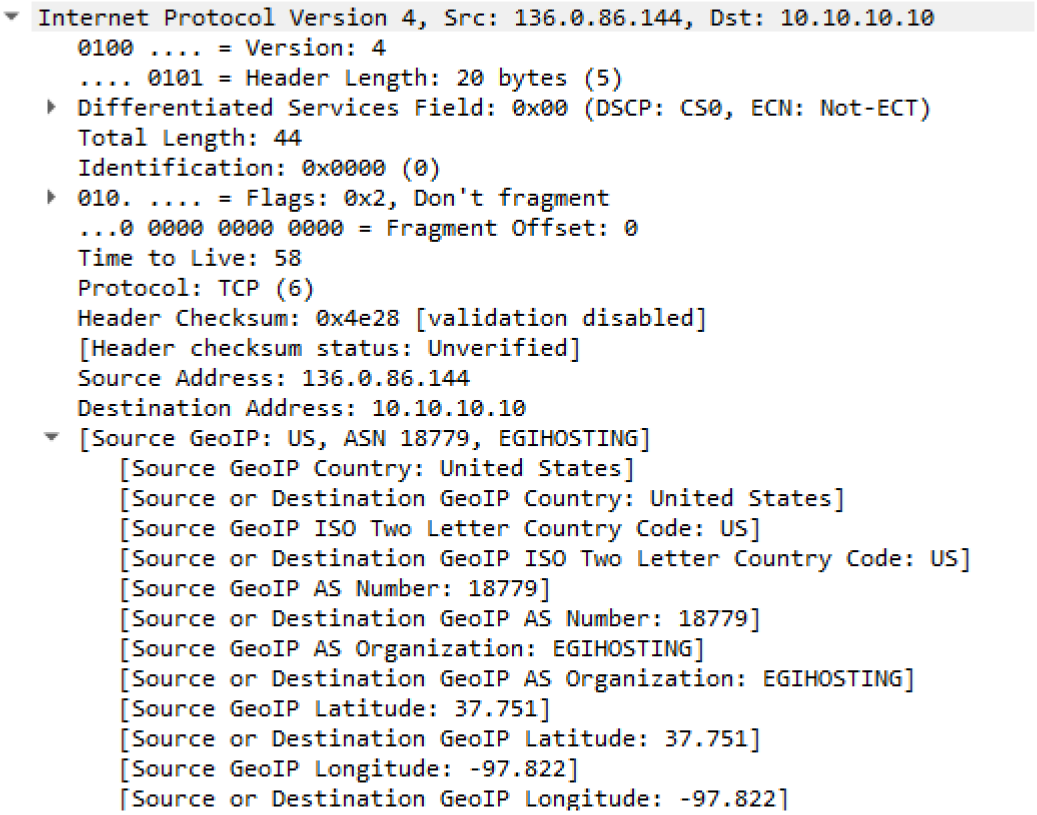
That’s it! we can now see the GeoIP information for a packet.

Let’s test this out using a PCAP file which captured a DDoS attack. To see the GeoIP information for a packet, simply expand the IP field in the packet details pane and look at the bottom of its details:



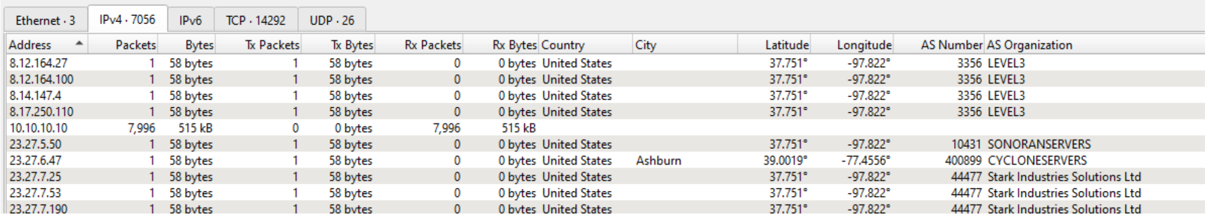
```
▾ Internet Protocol Version 4, Src: 136.0.86.144, Dst: 10.10.10.10
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 44
     Identification: 0x0000 (0)
   ▸ 010. .... = Flags: 0x2, Don't fragment
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 58
     Protocol: TCP (6)
     Header Checksum: 0x4e28 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 136.0.86.144
     Destination Address: 10.10.10.10
   ▸ [Source GeoIP: US, ASN 18779, EGIHOSTING]
```

If you expand the Source GeoIP field, you will see something like the following:



```
▾ Internet Protocol Version 4, Src: 136.0.86.144, Dst: 10.10.10.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 44
    Identification: 0x0000 (0)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 58
    Protocol: TCP (6)
    Header Checksum: 0x4e28 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 136.0.86.144
    Destination Address: 10.10.10.10
  ▾ [Source GeoIP: US, ASN 18779, EGIHOSTING]
       [Source GeoIP Country: United States]
       [Source or Destination GeoIP Country: United States]
       [Source GeoIP ISO Two Letter Country Code: US]
       [Source or Destination GeoIP ISO Two Letter Country Code: US]
       [Source GeoIP AS Number: 18779]
       [Source or Destination GeoIP AS Number: 18779]
       [Source GeoIP AS Organization: EGIHOSTING]
       [Source or Destination GeoIP AS Organization: EGIHOSTING]
       [Source GeoIP Latitude: 37.751]
       [Source or Destination GeoIP Latitude: 37.751]
       [Source GeoIP Longitude: -97.822]
       [Source or Destination GeoIP Longitude: -97.822]
```

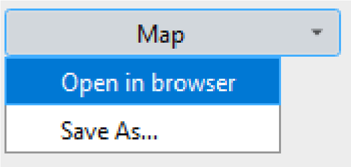
Don't freak out if you cant see the GeoIP information, first make sure that you are investigating a packet with external IP addresses as it can identify the geolocation for private IP addresses. The information seen above is very handy, as we could simply add the source city and country as a column and maybe drill down for traffic from unusual countries, like Russia for example. You can also see the GeoIP information in the Statistics -> Endpoints screen:

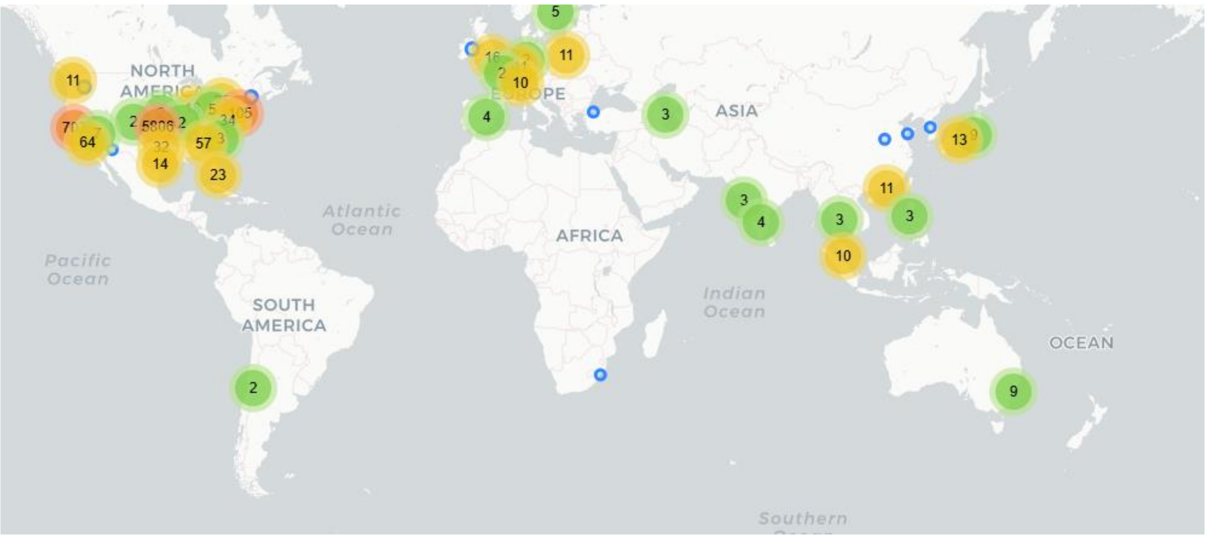


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
8.12.164.27	1	58 bytes	1	58 bytes	0	0 bytes	United States		37.751°	-97.822°	3356	LEVEL3
8.12.164.100	1	58 bytes	1	58 bytes	0	0 bytes	United States		37.751°	-97.822°	3356	LEVEL3
8.14.147.4	1	58 bytes	1	58 bytes	0	0 bytes	United States		37.751°	-97.822°	3356	LEVEL3
8.17.250.110	1	58 bytes	1	58 bytes	0	0 bytes	United States		37.751°	-97.822°	3356	LEVEL3
10.10.10.10	7,996	515 kB	0	0 bytes	7,996	515 kB						
23.27.5.50	1	58 bytes	1	58 bytes	0	0 bytes	United States		37.751°	-97.822°	10431	SONORANSERVERS
23.27.6.47	1	58 bytes	1	58 bytes	0	0 bytes	United States	Ashburn	39.0019°	-77.4556°	400899	CYCLONESERVERS
23.27.7.25	1	58 bytes	1	58 bytes	0	0 bytes	United States		37.751°	-97.822°	44477	Stark Industries Solutions Ltd
23.27.7.53	1	58 bytes	1	58 bytes	0	0 bytes	United States		37.751°	-97.822°	44477	Stark Industries Solutions Ltd
23.27.7.190	1	58 bytes	1	58 bytes	0	0 bytes	United States		37.751°	-97.822°	44477	Stark Industries Solutions Ltd

4. Visualising the Data

Another great transformation we can do is click the Map button on this Endpoint screen and select open in browser:





This provides a neat visualisation of all the locations where traffic originated from.

5. Conclusion

Integrating GeoIP with Wireshark offers significant advantages for cybersecurity professionals. It enhances network traffic analysis by providing geographic context, aiding in incident response, and more. By following the setup steps outlined above, you should be able to leverage GeoIP data to improve your Wireshark investigations.