**Wireshark使用技巧之GeoIP显示IP地理位置及经纬度信息**

**操作说明**

Wireshark软件通过安装第三方数据库是可以显示IP地址位置的。

所谓GeoIP，Geolocation IP，就是通过来访者的IP，定位他的经纬度，国家/地区，省市，甚至街道等位置信息。

安装的时候需要注意使用Wireshark的版本，新老版本的Wireshark在对第三方库的稍微有一点不一样，这里主要说明Wireshark3.0+的版本的安装方法。

**准备工作**

下载第三方库官方地址：

<https://dev.maxmind.com/geoip/geoip2/geolite2/>

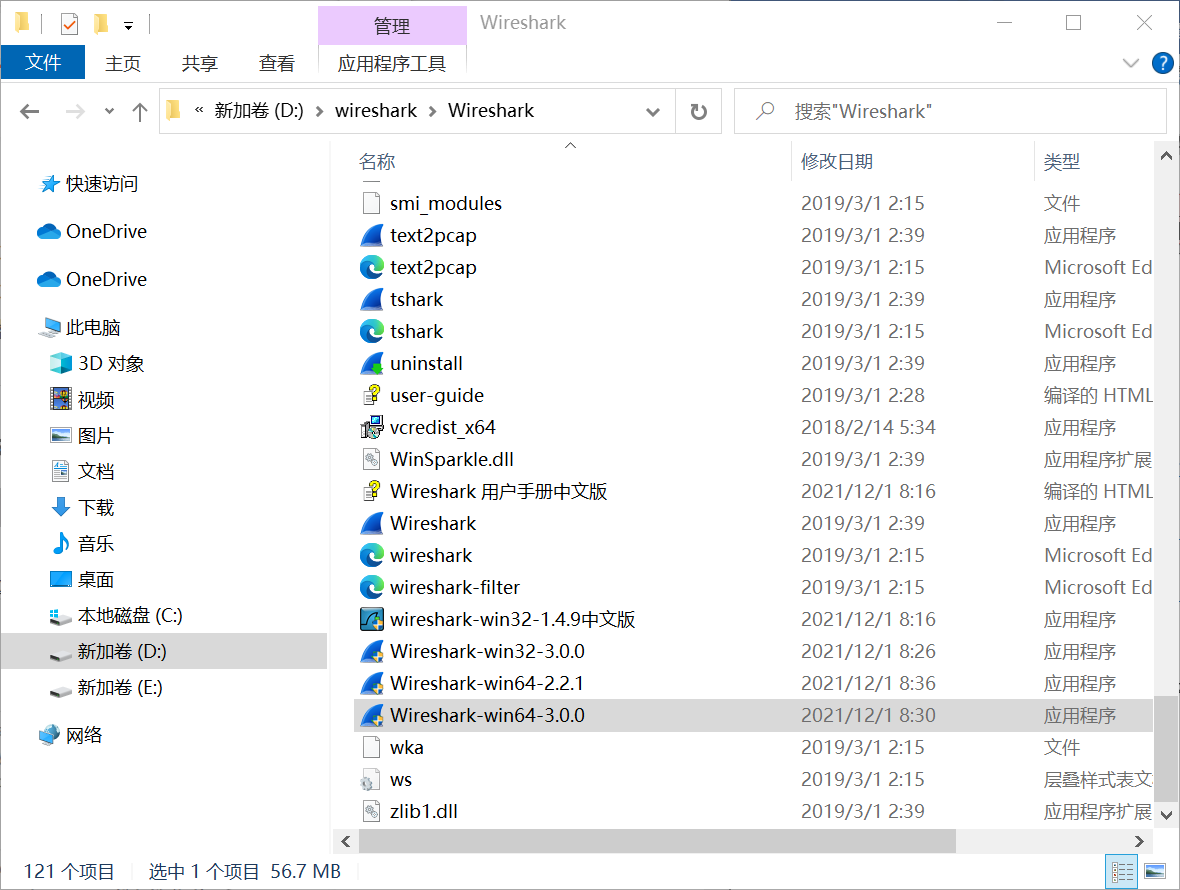
下载第三方库云盘地址：

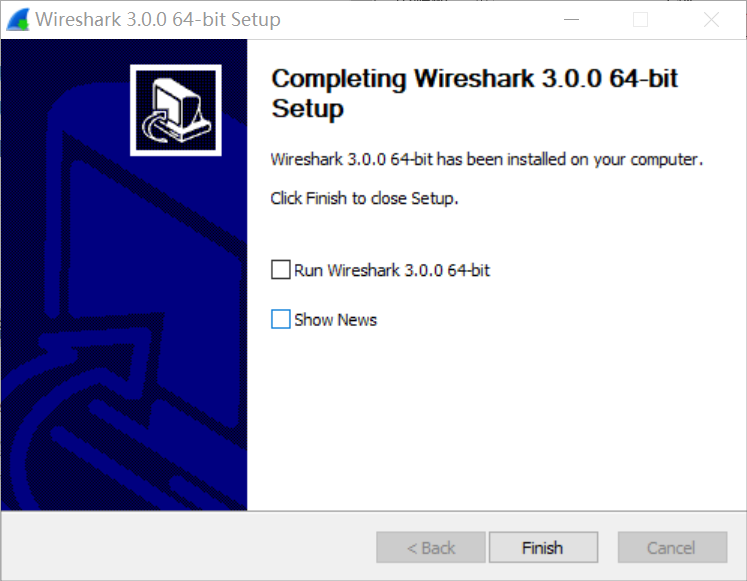
<https://pan.baidu.com/s/1UV_G-47gv1B7yhSXuM5Bbw> 提取码：lxu8

下载wireshark云盘地址：<https://pan.baidu.com/s/1BldA7cN5Vy8PH8j8MqLrrw> 提取码：9iav

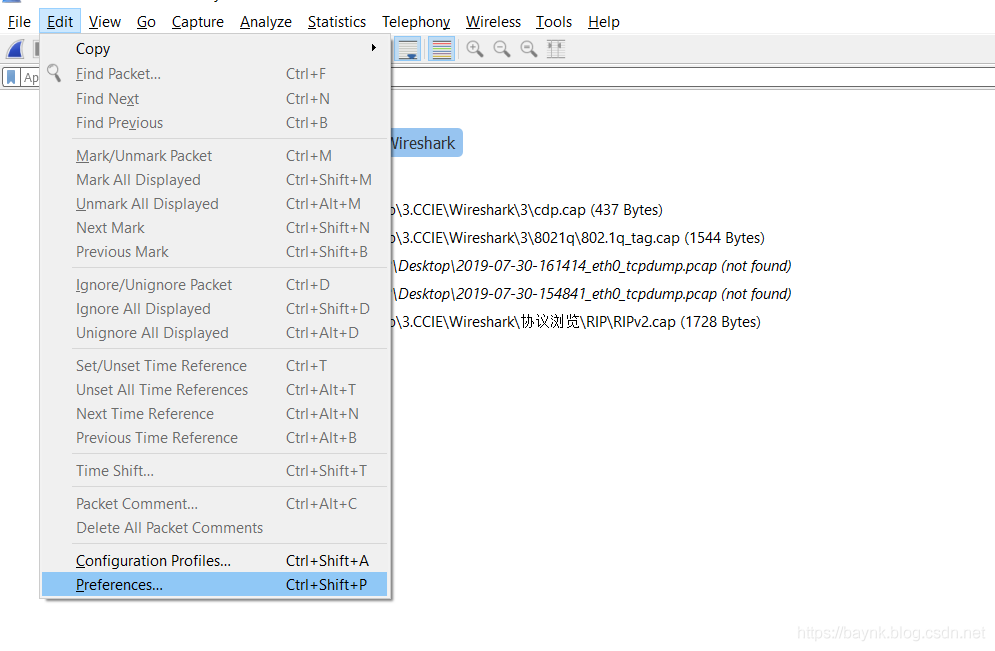
**Wireshark3+使用GeoIP**

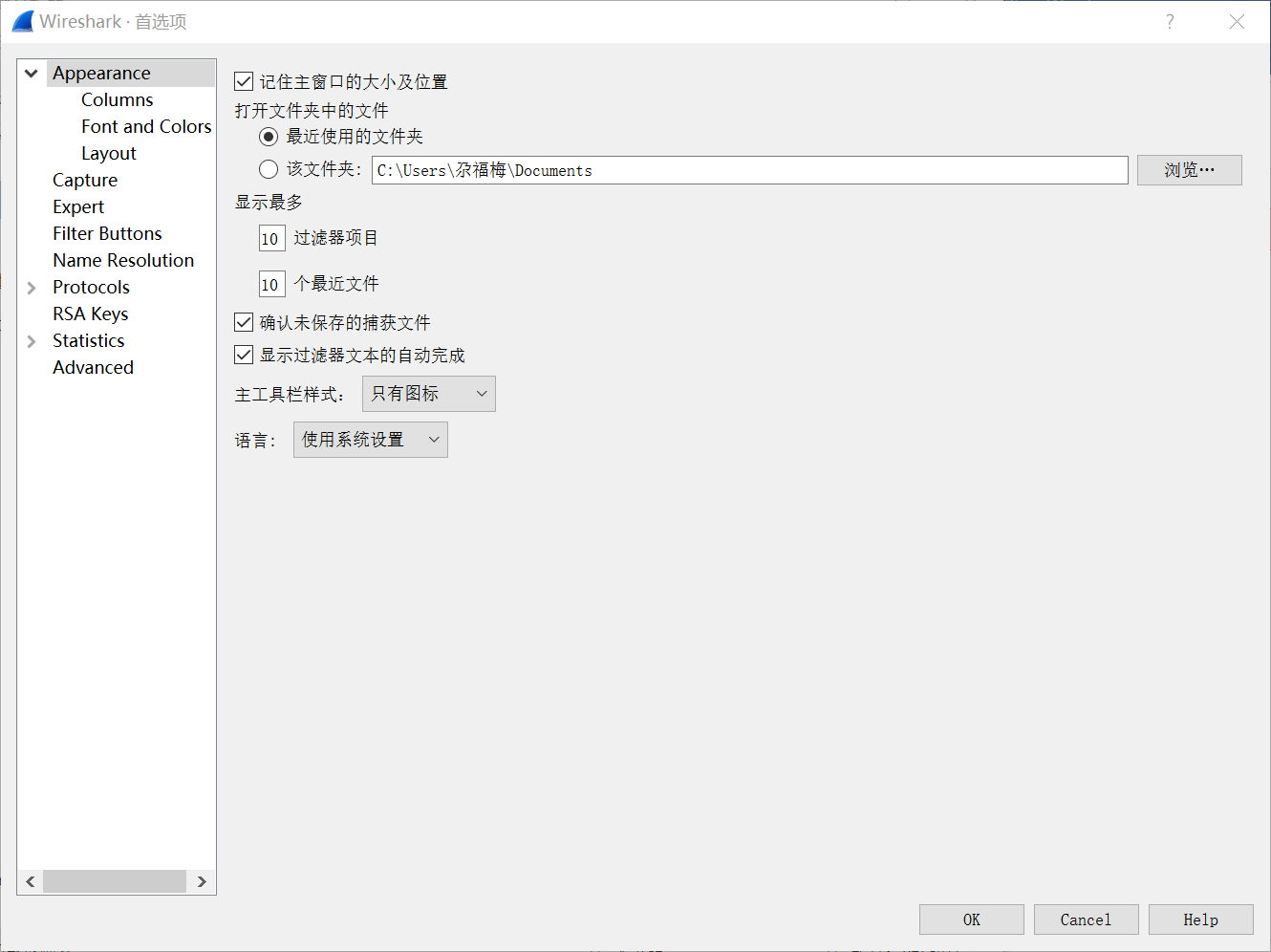
1.打开下载好的安装包，点击下载Wireshark-win64-3.0.0，下载完成



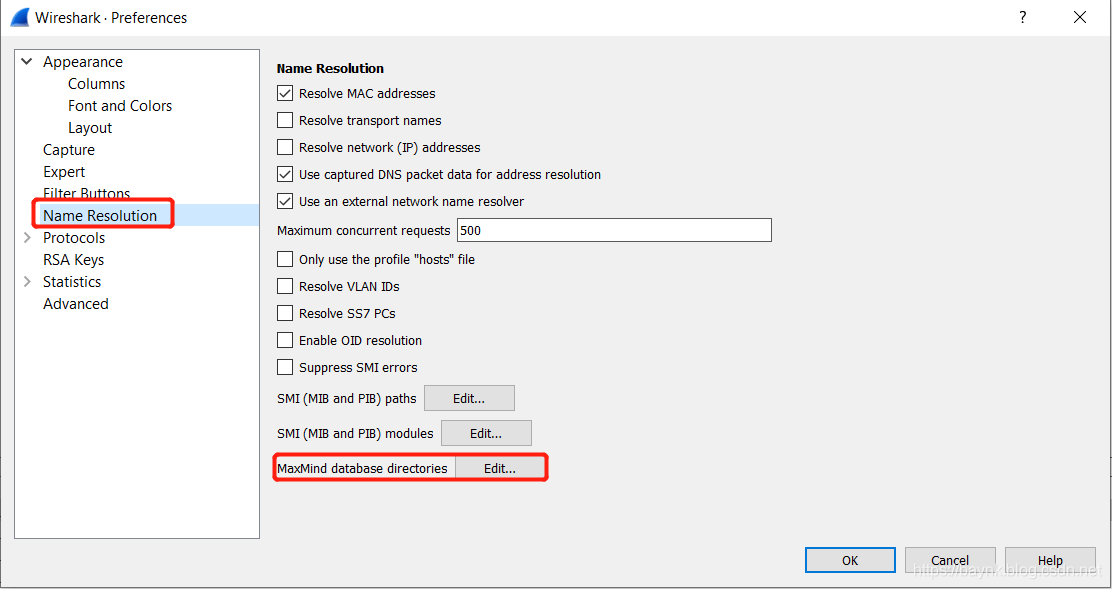


2.安装wireshark3.0后,打开wireshark界面,点击Edit(编辑)>Prefencens(首选项)

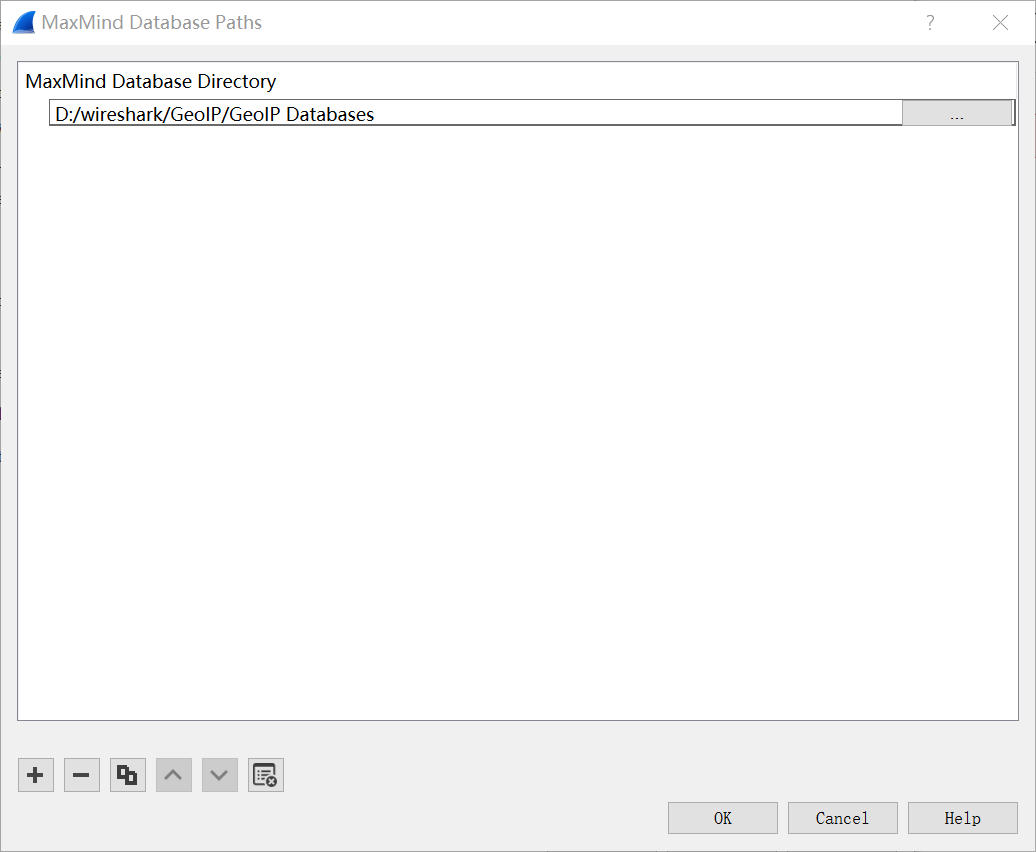




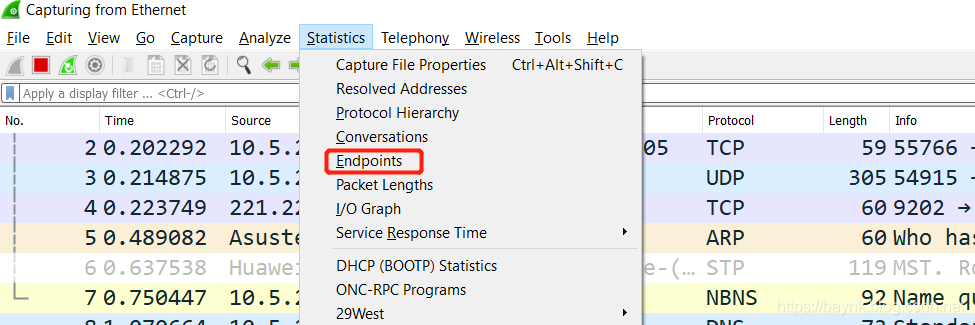
3. 点击Name Resolution->MaxMind database directories->Edit



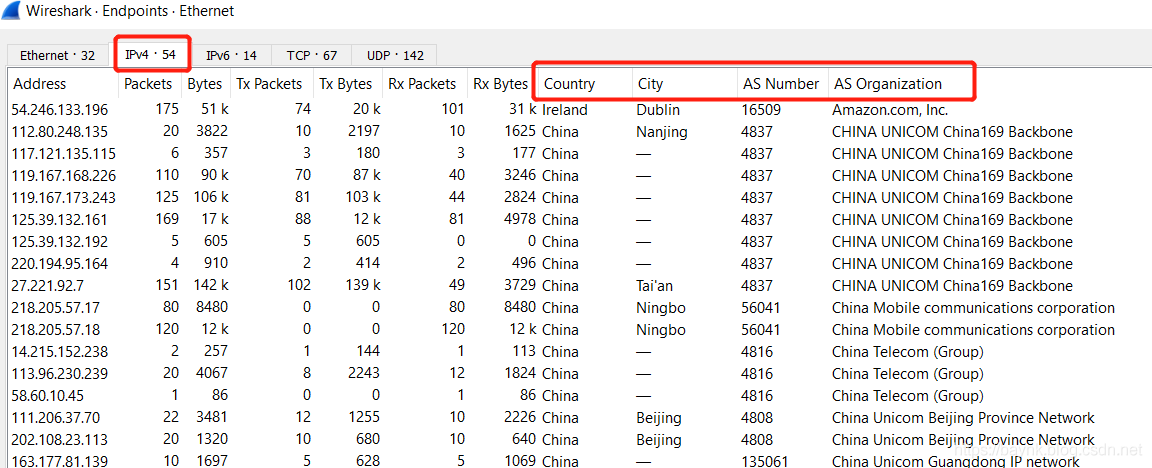
4. 添加第三方数据库的目录即可。这里稍微解释下，MaxMind DB 文件格式是使用高效的二进制搜索树将IPv4和IPv6地址映射到数据记录的数据库格式。



5. 重启wireshark后开启抓包，点击标签页中的Statistics->Endpoints



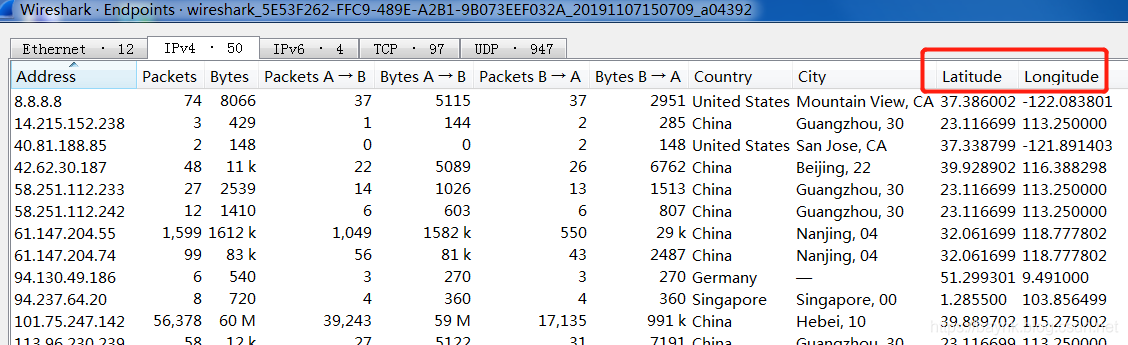
6. 点击IPv4标签页，即可看到Country,City,ASN,ASO等内容。



7. 设置就是这么简单，但是这里没有看到很多人想要的经纬度信息，这是因为在wireshark更新后，它支持的第三方库文件的后缀就变成了.mmdb格式，这种格式GeoIP并没有放出有经纬度信息的，记得好像是因为License的问题。当然如果有需要使用经纬度信息，那么就去安装wireshark3.0以下的版本吧。

**WireShark3-使用GeoIP**

1.设置方法基本一致，这里就不多说了，区别在于，Wireshark3以下用的第三方数据库文件的格式是.dat的，这里直接看效果就可以了。



2. 可以看到低版本中没有AS相关的信息，增加了经纬度的信息。一定要注意，longitude代表经度，也就是经度写在了后面，Latitude才是代表纬度，写在了前面。