5.3.1 开启名称解析

Wireshark 在显示数据包时，使用名称解析来简化分析。要启用这项功能，请选择 Edit -> Preferences -> Name Resolution，如图 5-8 所示。这里有一些 Wireshark 名称解析的主要选项。

解析**MAC**地址（**Resolve MAC addresses**）：这种类型的名称解析使用 ARP 协议，试图将第 2 层——数据链路层的 MAC 地址，例如 00:09:5B:01:02:03，转换为网络层地址，例如 10.100.12.1。如果这种转换尝试失败，那么 Wireshark 会使用程序目录中的 ethers 文件尝试进行转换。Wireshark 最后的尝试便是将 MAC 地址的前 3 个字节转换为设备 IEEE 指定的制造商名称，例如 Netgear_01:02:03。

解析传输名称（**Resolve Transport name**）：这种类型的名称解析尝试将一个端口号，转换成一个与其相关的名字。比如，将端口 80 显示为 http。当你碰到一个不常见的端口而又不知道这是什么协议的时候，这个功能显得尤为便利。

解析网络名称（**Resolve Network/IP name**）：这种类型的名称解析试图转换第 3 层——网络层的地址，例如将 IP 地址 192.168.1.50，转换为一个易读的域名。假如域名具有高描述性，则对我们理解该系统的目的或其所有者，将是非常有帮助的。

在图 5-8 中还包括其他几个有用的选项。

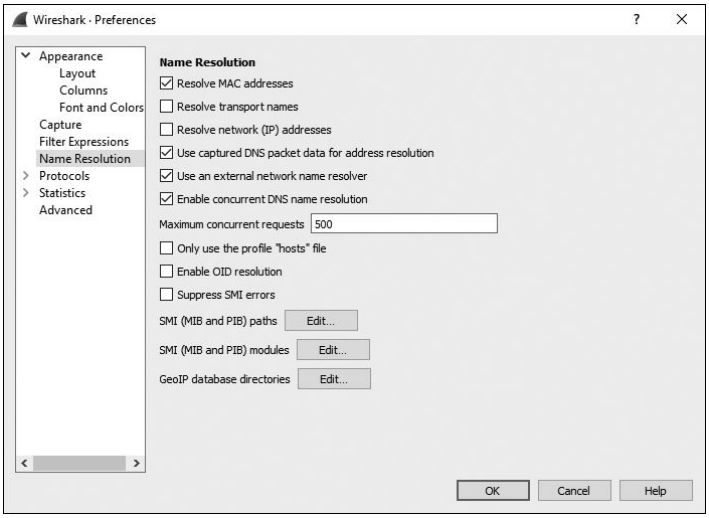

图 5-8　在 Capture Options 对话框中开启名称解析。前 3 项中只有 MAC 地址解析被选中了

Use captured DNS packet data for address resolution：从已捕获的 DNS 数据包中解析出了 IP 地址和 DNS 域名之间的映射。

Use an external network name resolver：允许 Wireshark 为你当前的分析机器使用的外网 DNS 服务器生成查询，从而获得 IP 地址和 DNS 域名之间的映射。当捕获的文件里没有 DNS 解析数据而你还需要 DNS 域名解析时，这个功能就比较实用了。

Maximum concurrent requests：该参数会限制当前的一次最多 DNS 请求数量。当你的捕获文件将产生大量的 DNS 查询而且你并不想让 DNS 查询占用过多带宽的时候，请使用这项功能。

Only use the profile "hosts" file：把 DNS 解析限制在与活动 Wireshark 文档关联的 host 文件中。我会在下面的小节讲到如何使用这个文件。

在 Preferences 中所修改的设置，会在 Wireshark 关闭并重启后生效。要想让名称解析设置立马生效，请在主下拉菜单的 View->Name Resolution 把名称解析设置打开。在这个子菜单下你可以启用或关闭物理、传输、网络地址的名称解析。

你可以利用各种名称解析工具使你的捕获文件变得更加具有可读性，从而在一些情况下节省大量时间。举例来说，你可以使用 DNS 名称解析，来轻松地识别你试图精确定位为特定数据包源的计算机名称。