5.3.3 使用自定义 hosts 文件

在一个大型捕获文件中，不断从多个主机之间跟踪流量是一件很乏味的事情，特别是当外部主机解析服务访问不到的时候。好在我们可以根据它们的 IP 地址并且通过一个叫 Wireshark hosts 的文件来手动地标识系统。Wireshark 的 hosts 文件实质是由 IP 地址列表和与之对应的名字组成的文本文件。为了快速查询，你可以在 Wireshark 里使用 hosts 文件来标记地址。这些名字会显示在数据包列表窗格里。

要使用 hosts 文件，请按照以下步骤操作。

（1）单击 Edit->Preferences->Name Resolution 并且选择 Only use the profile「hosts」 file。

（2）使用 Windows 记事本或者类似的文本编辑器创建一个新文件。该文件应该包含至少一条 IP 和对应名称的记录，如图 5-9 所示。Wireshark 会根据这个映射来把相应的 IP 地址替换为 hosts 文件里对应的名称并最终显示在包列表窗格里。

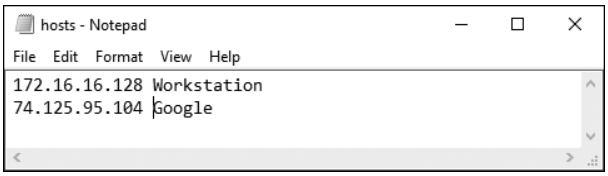

图 5-9　创建一个 Wireshark hosts 文件

（3）把文件以文本格式存为 hosts 并将其保存到正确的目录下，如下所示。请确保文件名没有后缀！

- Windows: <USERPROFILE>\Application Data\Wireshark\hosts
- OS X: /Users/<username>/.wireshark/hosts
- Linux: /home/<usename>/.wireshark/hosts

现在打开一个捕获文件，如图 5-10 所示，所有在 hosts 文件里的 IP 地址都被解析成了明确的名称。现在有着更有意义的名称显示在源和目的列中而不是之前的 IP 地址。

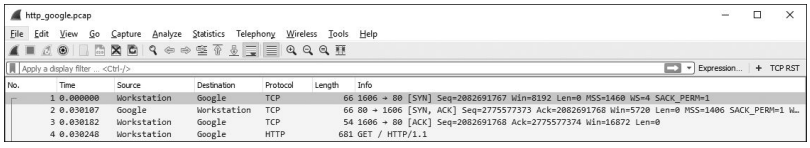

图 5-10　根据 Wireshark hosts 文件进行名称解析

用这种 hosts 文件的方式可以在分析中大幅增强识别特定主机的能力。当团队协作分析时，请考虑将 hosts 文件共享给其他网络上的同事。这会帮助你的团队迅速识别一些使用静态地址的基础系统，比如服务器和路由器。

> 注意
>
> 如果你的 hosts 文件不起作用了，请确保你没有意外地在文件名后面加后缀名。这个文件的名字就叫 hosts。