5.3.2 名称解析的潜在弊端

名称解析有着很多优点，使用名称解析看上去很容易，但是也存在着一些潜在的弊端。首先，网络名称解析可能会失败，尤其是当没有可用的 DNS 服务器时。名称解析的信息是不会保存在捕获文件里的，所以在你每次打开一个捕获文件的时候都要重新进行一次名称解析。如果你在一个网络环境下捕获了流量，那么在另一个网络环境中打开该捕获文件时，你的系统可能访问不到之前的 DNS 服务器。

除此之外，名称解析还会带来额外的处理开销。如果你正在处理一个非常大的捕获文件而内存不剩多少的时候，你可能需要关闭名称解析，来节约系统资源。

另一个问题就是，对 DNS 名称解析的依赖会产生额外的数据包，也就是说你的捕获文件可能会被解析那些基于 DNS 地址的流量所占据。我们还可以再把问题想得复杂一些，如果在你分析的捕获文件中含有恶意 IP 地址，那么试图去解析它们会生成对攻击者控制的基础架构的查询，这样攻击者就有可能知道你的动作，甚至把你自己变成靶子。要避免跟攻击者打交道，请在名称解析选项对话框中关掉 Use an external network name resolver。