9.2.4 DNS 递归

由于互联网的 DNS 结构是层级式的，因此为了能够回答客户端提交的查询，DNS 服务器必须能够彼此通信。我们的内部 DNS 服务器知道本地局域网服务器的名字和 IP 地址的映射，但不太可能知道 Google 或者 Dell 的 IP 地址。

当 DNS 服务器需要查找一个 IP 地址时，它会代表发出请求的客户端向另一个 DNS 服务器进行查询。实际上，这个 DNS 服务器与客户端的行为相同。这个过程叫作递归查询。

打开文件 dns_recursivequery_client.pcap，可以分别看到 DNS 客户端和服务器视角的递归查询过程。这个文件包含了捕获客户端 DNS 流量文件的两个数据包。第一个数据包是从 DNS 客户端 172.16.0.8 发往 DNS 服务器 172.16.0.102 的初始查询，如图 9-13 所示。

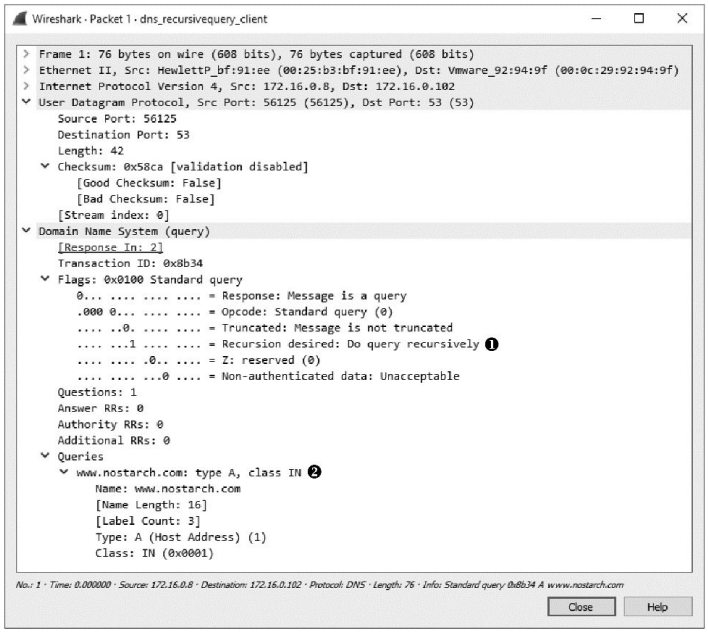

图 9-13　设置有期望递归位的 DNS 查询

当你展开这个数据包的 DNS 区段时，可以看到这是一个用以查找 DNS 名称 www.nostarch.com 的 A 类型记录的标准查询。展开标志区段，可以了解更多关于这个数据包的信息，你可以看到期望递归的标志。

第二个数据包是我们所希望看到的对于初始数据包的响应，如图 9-14 所示。

这个数据包的事务 ID 和我们的查询相匹配，也没有列出错误，所以我们就得到了 www.nostarch.com 所对应的 A 类型资源记录。

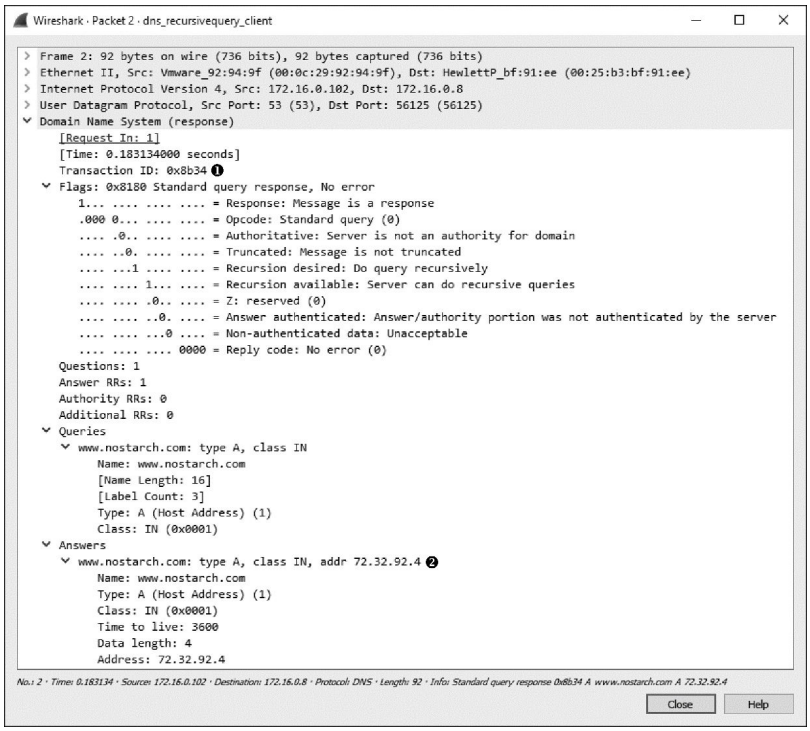

图 9-14　DNS 查询响应

如果我们想要知道查询是否被递归应答，唯一的方法就是当进行递归查询时监听 DNS 服务器的流量，正如文件 dns_recursivequery_server.pcap 中所示的那样。这个文件显示了查询进行时本地 DNS 服务器流量的捕获，如图 9-15 所示。第一个数据包和我们前一个捕获文件中的初始查询相同。这时，DNS 服务器接到了这个查询，在其本地数据包检查后，发现它并不知道关于 DNS 域名（nostarch.com）所对应 IP 地址这个问题的答案。由于这个数据包发送时设置了期望递归，困此你会在第二个数据包中看到，这个 DNS 服务器为了得到答案向其他 DNS 服务器询问这个问题。

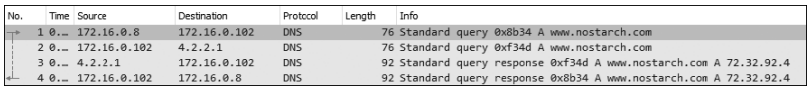

图 9-15　从服务器的角度进行 DNS 查询

在第二个数据包中，位于 172.16.0.102 的 DNS 服务器向 4.2.2.1，也就是其所设定的要转发上行请求的服务器，发送了一个新的查询，如图 9-16 所示。这个请求是原始的镜像，并将 DNS 服务器变成一个客户端。

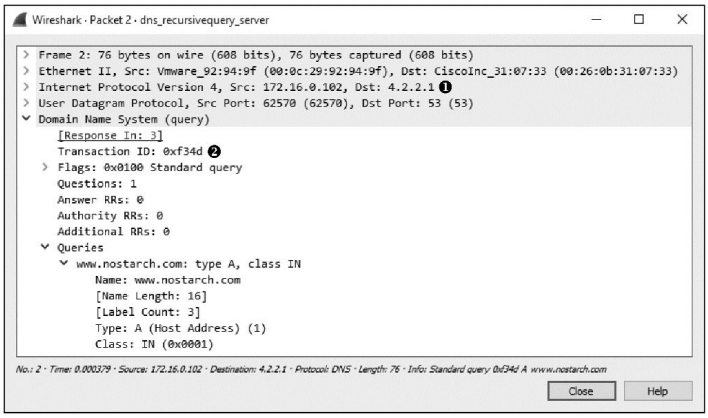

图 9-16　递归 DNS 查询

由于这个事务 ID 与之前捕获文件中的事务 ID 不同，因此我们可以将它作为一个新的查询。在这个数据包被服务器 4.2.2.1 接收之后，本地 DNS 服务器就接到了响应，如图 6-17 所示。

接到了这个响应后，本地 DNS 服务器就可以将第四个，也就是最后一个带有请求信息的数据包传递给 DNS 客户端。

虽然这个例子只展示了一层的递归，但对一个 DNS 请求来说递归查询可能会发生很多次。这里我们接到了来自 DNS 服务器 4.2.2.1 的回答，但那个服务器可能为了寻找答案也向其他服务器进行了递归查询。一个简单查询在其得到最终响应之前可能遍历了全世界。图 9-18 展示了递归 DNS 查询的过程。

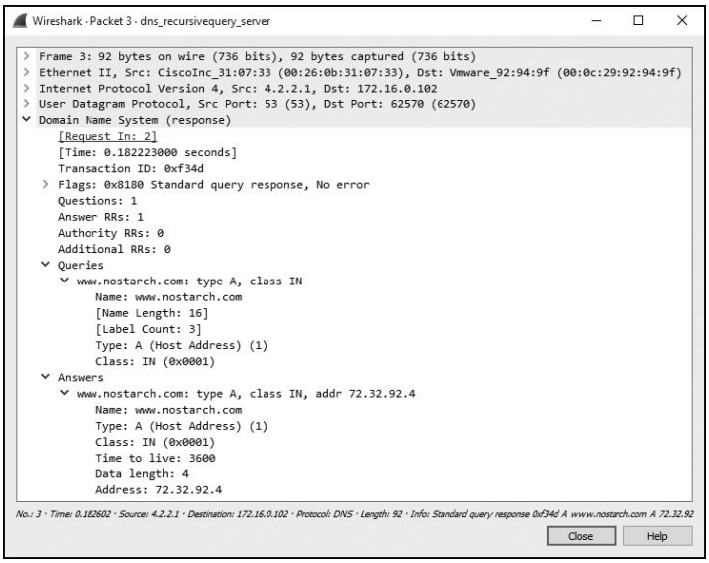

图 9-17　对递归 DNS 查询的响应

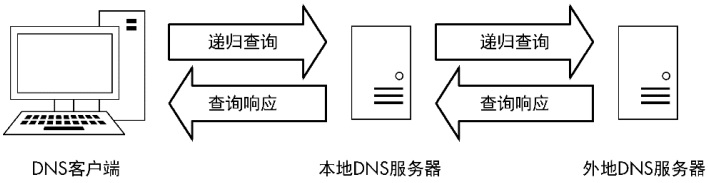

图 9-18　DNS 递归查询