9.2.2 一次简单的 DNS 查询过程

DNS 以查询/响应的模式工作。当一个客户端想要将一个 DNS 名字解析成 IP 地址时，它会向 DNS 服务器发送一个查询，然后服务器在响应中提供所请求的信息。在较简单的情形下，这个过程包含着两个数据包，正如在捕获文件 dns_query_response.pcap 中所看到的那样。

第一个数据包如图 9-11 所示，是由 192.168.0.114 的客户端通过 DNS 的标准 25 端口发向 205.152.37.23 的服务器的 DNS 查询。

当检查这个数据包的头部时，你会发现 DNS 也是基于 UDP 协议的。

在数据包的 DNS 区段，你可以看到数据包开头的一些较小域都被 Wireshark 合并成为了一个标志区段（Flags section）。展开这个区段，你会看到这个消息是一个典型的请求：没有被截断并且期望递归查询（我们随后将介绍递归查询）。在展开查询区段时，里面也仅有一个问题。这个问题是查询名字为 wireshark.org 的主机类型（type A）互联网（IN）地址。这个数据包基本就是在问：「哪个 IP 地址对应着 wireshark.org 域?」

数据包 2 响应了这个请求，如图 9-12 所示。因为这个数据包拥有唯一的标识码，所以我们知道这里包含着对于原始查询的正确响应。

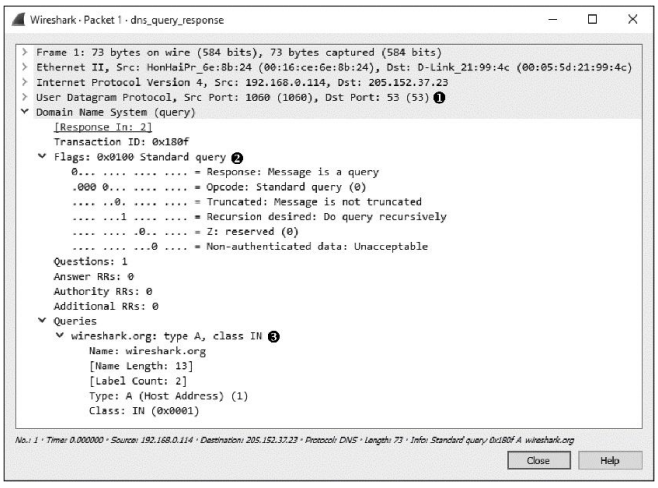

图 9-11　DNS 查询数据包

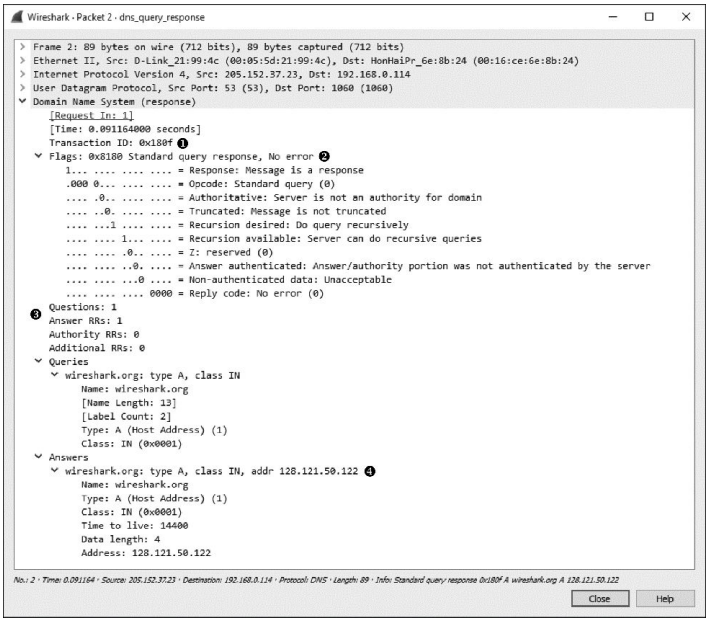

图 9-12　DNS 响应数据包

标志区段可以确保这是一个响应并且允许必要的递归。这个数据包仅包含一个问题和一个资源记录，因为它将原问题和回答连接了起来。展开回答区段可以看到对于查询的回答：wireshark.org 的地址是 128.121.50.122。有了这个信息，客户端就可以开始构建 IP 数据包，并与 wireshark.org 进行通信了。