UDP 报头结构

UDP 头比 TCP 头要小得多，也简单得多。如图 8-12 所示，以下是 UDP 报头的字段。

源端口：用来传输数据包的端口。

目标端口：数据包将要被传输到的端口。

数据包长度：数据包的字节长度。

校验和：用来确保 UDP 头和数据到达时的完整性。

用户数据报协议 (UDP)					
偏移位	八位组	0	1	2	3
八位组	位	0–7	8–15	16–23	24–31
0	0	源端口		目标端口	
4	32	数据包长度		校验和	

图 8-12　UDP 报头

文件 udp_dnsrequest.pcapng 中包含有一个数据包，这个数据包是一个使用 UDP 的 DNS 请求。当展开这个数据包的 UDP 头时，你可以看到 4 个域（见图 8-13）。

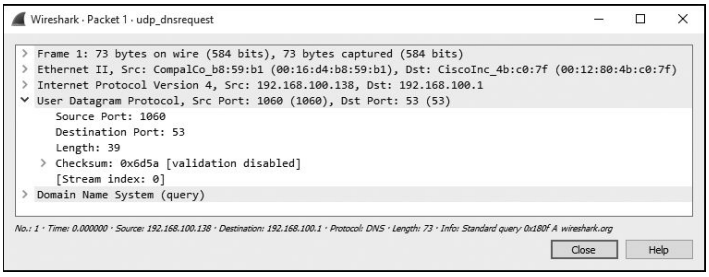

图 8-13　UDP 数据包的内容非常简单

需要记住的是，UDP 并不关心传输的可靠性，所以任何使用 UDP 的应用在必要的时候都需要采取特殊的步骤，保证可靠的传输。这一点和 TCP 相反，TCP 有自己的一套连接正式发起和结束的程序，也有自己的一些机制来校验数据包的成功传输。

这一章向你介绍了传输层协议——TCP 和 UDP。不像网络层协议，TCP 和 UDP 是日常在绝大多数网络上交互的核心，因此能否掌握有效分析它们的能力将会决定你能否成为一位数据包分析大师。在第 9 章，我们将看一看常见的应用层协议。