5.2 基于协议分层结构的统计

当在与未知的捕获文件打交道时，有时需要知道文件中协议的分布情况，也就是捕获中 TCP、IP、DHCP 等所占的百分比是多少。除了计算并汇总数据包之外，使用 Wireshark 的 Protocol Hierarchy Statistics（协议分层统计）窗口也是一个对你的网络进行基准分析的好方法。

举例来说，保持 lotsofweb.pcapng 文件打开并且清除之前的过滤器，选择 Statistics->Protocol Hierarchy 打开协议分层统计窗口（见图 5-7）。

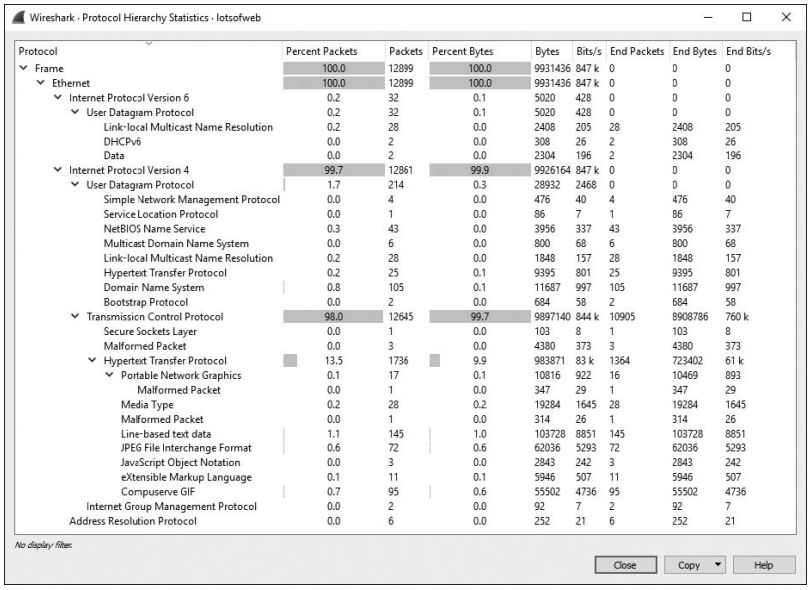

图 5-7　协议分层统计窗口给出了各种协议的分布统计情况

协议分层统计窗口就像一张快照，会让你直观地看到网络活动中的各种类型。在图 5-7 中，以太网流量占 100%，IPv4 流量占 99.7%，TCP 流量占 98%，来自网页浏览的 HTTP 流量占 13.5%。这些信息给我们提供了一个很好的测试网络的方式，特别是当你在脑海中对网络流量通常是什么样子有了大致的印象后。举个例子，假设在正常情况下你的网络流量有 10% 是 ARP 流量，但在最近的一次捕获中发现有 50% 的 ARP 流量，你就可以推断也许哪里出问题了。在一些情况下，一种很少见的协议出现在流量中也比较有趣。如果你没去设置使用生成树协议（STP）的设备但又在协议分层统计中看到 STP 流量，这说明有设备设置错误。

假以时日，你就可以通过查看正在使用协议的分布情况，来得到网络中用户和设备的情况。比如说，当你看到高 HTTP 流量时，说明有很多网页浏览在进行。你会发现只需要简单地查看网段中的流量，就可以立即分辨这个网段属于哪个部门。IT 部门网段的流量中通常包含管理协议，例如 ICMP 或

者 SNMP 的数据，订单管理部门通常会导致大量的 SMTP 流量，甚至我还可以在一些讨厌的实习生的网络区段内找到他们玩魔兽世界的流量！