5.6 数据包长度

一个或一组数据包的大小可以让你了解很多情况。在正常情况下，一个以太网上的帧最大长度为 1518 字节，除去以太网、IP 以及 TCP 头，还剩下 1460 字节以供应用层协议的头或者数据使用。如果你知道报文传输的最小需求，那么我们就可以通过一个捕获文件中数据包长度的分布情况，做一些对流量的合理猜测。这个技巧对我们尝试理解捕获文件的组成结构十分重要。Wireshark 提供了数据包长度窗口，帮助你查看数据包基于其长度的分布情况。

文件 download-slow.pcapng 就是一个很好的例子。打开文件后，选择 Statistics->Packet Lengths，就会出现一个如图 5-16 所示的数据包长度对话框。

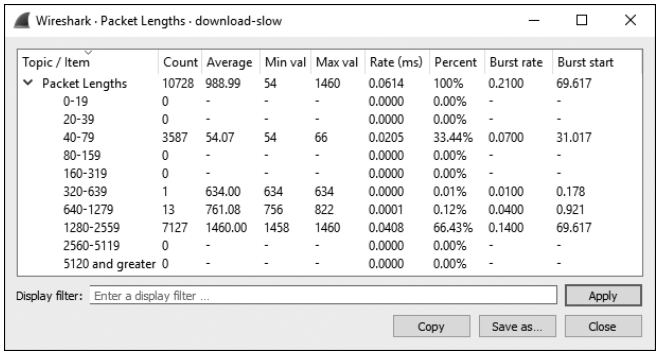

图 5-16　数据包长度窗口帮助你对捕获文件中的流量进行合理的猜测

特别注意那些大小为 1280～2559 字节的数据包统计的行。这些较大的数据包通常表示数据传输，而较小的数据包则表示协议控制序列。在这个例子中，我们看到较大的数据包占了相当大的比重（66.43%）。即使不看这个文件中的数据包，我们也仍然可以知道捕获中包含了一个或多个数据传输流量。这可能是 HTTP 下载、FTP 上传，或者其他类型在主机之间进行数据传输的网络通信。

剩下的大多数数据包（33.44%）都是在 40～79 字节范围内，而处于这个范围的数据包通常是不包含数据的 TCP 控制数据包。我们可以想一下协议头一般的大小。以太网报头是 14 字节（包含 4 字节 CRC），IP 报头至少 20 字节，没有数据以及选项的 TCP 数据包也是 20 字节，也就意味着典型的 TCP 控制数据包——例如 TCP、ACK、RST 和 FIN 数据包——大约是 54 字节并落入了这个区域。当然 IP 或 TCP 的额外选项会增加它的大小。

查看数据包长度是一个鸟瞰捕获文件的好方法。如果存在着很多较大的数据包，那么很可能是进行了数据传输。如果绝大多数的数据包都很小，我们便可以假设这个捕获中存在协议控制命令，而没有传输大规模的数据。虽然这不是一个必需的操作，但在深入分析前做一些类似的假设，有时还是很保险的。