4.4.2 输出标签页

与传统的先抓流量再存文件的方式不同的是，输出标签页（见图 4-11）允许你把所抓的流量包存成一个文件。这样做可以使管理捕获流量包的存储方式更具灵活性。你可以选择把流量包都存成一个文件、文件集或使用环状缓冲（我们待会儿就会讲到）来控制创建文件的个数。要开启这项功能，可以在文件文本框内输入一个完整的绝对路径和名字，你也可以通过使用 Browse 按钮来选择一个目录并给文件起名。

当你要捕获一个大流量或者进行长时间抓包时，文件集合是你的得力帮手。文件集合就是按照特定的条件组成的多个文件的分组。要保存成文件集合，请单击 Create a new file automatically after... 选项。

Wireshark 使用多个不同的基于时间或文件大小的触发器，来管理保存为文件集合。要想开启其中的一个触发器，可以选中该触发器，用小箭头按钮调节比率大小并选择单位。如图 4-12 所示，你可以把触发器设置为每抓取 1MB 的流量就新存一个文件，或者每过 1min 就新存一个文件。

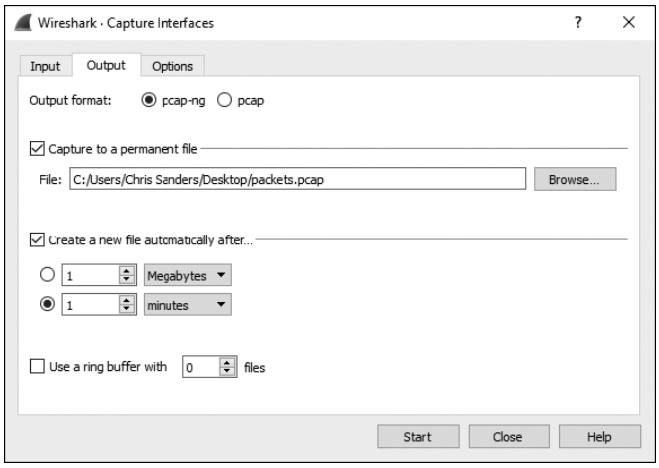

图 4-11　捕获接口的输出标签页

图 4-12　Wireshark 每隔 1min 建立的文件集合

使用 ring buffer（环状缓冲）允许你指定一个特定的文件数量，一旦超过了这个数量，Wireshark 就会用新数据覆盖最老的数据。虽然环状缓冲

有多重含义，但在这里指的是一旦最后的文件被写满了，则第一个文件就会被覆盖。换句话说，这实现了一个先进先出（FIFO）的写入数据到文件的方式。你可以选中这个功能，然后设置一个你想要回写的文件的最大数量。举例来说，如果你选择使用文件集合并且每隔 1h 创建一个新文件，并且你设置了环状缓冲值为 6。一旦第 6 个文件被生成，则环状缓冲将循环返回并覆盖第一个文件，而不是新建第七个文件。这个机制保证了在不断有新文件写入的同时又不会持续增加文件的数量。

在输出标签页上你也可以设定最终文件保存的格式是否使用.pcapng。如果你有对该格式不兼容的第三方工具的话，则可以选择.pcap 格式。