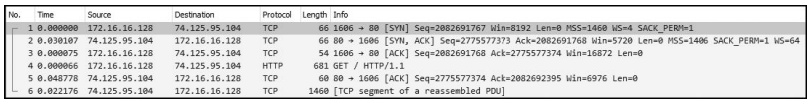
11.4.1 正常通信

我们将在本章的稍后部分详细讨论网络基线。目前，只知道你需要一个正常通信的基线，并与高延迟的情况作比较。在这些例子中，我们将使用 latency1.pcap 文件。由于我们已经讨论过了 TCP 握手和 HTTP 通信的细节，因此在这里我们将跳过它们。实际上，我们根本不需要再看 Packet Details 面板。如图 11-22 所示，我们只关心 Time 列。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.16.128	74.125.95.104	TCP	66	1606 → 80 [SYN] Seq=2082691767 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.030107	74.125.95.104	172.16.16.128	TCP	66	80 → 1606 [SYN, ACK] Seq=2775577373 Ack=2082691768 Win=5720 Len=0 MSS=1406 SACK_PERM=1 WS=64
3	0.000075	172.16.16.128	74.125.95.104	TCP	54	1606 → 80 [ACK] Seq=2082691768 Ack=2775577374 Win=16872 Len=0
4	0.000066	172.16.16.128	74.125.95.104	HTTP	681	GET / HTTP/1.1
5	0.048778	74.125.95.104	172.16.16.128	TCP	60	80 → 1606 [ACK] Seq=2775577374 Ack=2082692395 Win=6976 Len=0
6	0.022176	74.125.95.104	172.16.16.128	TCP	1460	[TCP segment of a reassembled PDU]

图 11-22　这些流量发生得相当快，被认为是正常的

这个通信序列是相当快的，全过程花了不到 0.1s。

接下来我们查看的几个捕获文件将包含相同的流量模式，只是在数据包时序上有些许不同。