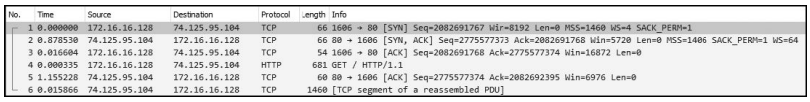
## 11.4.2 慢速通信——线路延迟

现在我们转向捕获文件 latency2.pcap。如图 11-23 所示，注意，除了时间值之外，所有数据包都和上一个文件中的相同。



| 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 | 0.878530 | 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 | 0.016604 | 172.16.16.128 | 74.125.95.104 | TCP | 54 | 1606 → 80 [ACK] Seq=2082691768 Ack=2775577374 Win=16872 Len=0 |
| 4 | 0.000335 | 172.16.16.128 | 74.125.95.104 | HTTP | 681 | GET / HTTP/1.1 |
| 5 | 1.155228 | 74.125.95.104 | 172.16.16.128 | TCP | 60 | 80 → 1606 [ACK] Seq=2775577374 Ack=2082692395 Win=6976 Len=0 |
| 6 | 0.015866 | 74.125.95.104 | 172.16.16.128 | TCP | 1460 | [TCP segment of a reassembled PDU] |

图 11-23　数据包 2 和 5 有很高的延迟

当我们开始逐个查看这 6 个数据包时，会很快遇到延迟的第一个标志。客户端（172.16.16.128）发送初始 SYN 数据包，开始 TCP 握手。在收到服务端（74.125.95.104）返回的 SYN/ACK 数据包之前有 0.87s 的延迟。这是我们受到线路延迟影响的第一个迹象，这是客户端和服务器之间的设备导致的。

由于数据包传输的特性，我们可以确定这是线路延迟的问题。当服务器收到一个 SYN 数据包时，由于不涉及任何传输层以上的处理，因此发送一个响应只需要非常小的处理量。即使服务器正承受巨大的流量负载，通常它也会迅速地向 SYN 数据包响应一个 SYN/ACK。这排除了服务器导致高延迟的可能性。

客户端的可能性也被排除了，因为它在此时除了接收 SYN/ACK 数据包以外什么也没干。排除了客户端和服务器的原因，那么网络缓慢的原因应该在捕获记录的前两个数据包里。

继续看，我们发现完成三次握手的 ACK 数据包传输很快，客户端发送的 HTTP GET 请求也同样如此。产生这两个数据包的处理过程是收到 SYN/ACK 后在客户端本地发生的，所以只要客户端没有沉重的处理负载，这两个数据包应该立刻就能发出去。

在数据包 5，我们看到它的时间值也高得令人难以置信。看来，我们发送初始 HTTP GET 请求之后，经过 1.15s 才收到从服务器返回的 ACK 数据包。收到 HTTP GET 请求后，服务器在发送数据之前先发送了一个 TCP ACK，同样这也不需要服务器耗费太多处理资源。这是线路延迟的另一个标志。

每次遇上线路延迟，你几乎都会在通信过程中初始握手的 SYN/ACK 以及其他 ACK 数据包中看到这样的情景。虽然这个信息并没有告诉你网络高延迟的确切原因，但它起码告诉你不是客户端或服务器的问题，所以你能意

识到延迟是因为中间的一些设备出了问题。此刻，你可以开始检查受影响主机之间的防火墙、路由器、代理服务器等设备，以确定问题所在。