10.4.2 分析

如图 10-25 所示，捕获文件的开头是发送打印作业的主机（172.16.0.8）与打印机（172.16.0.253）的 TCP 握手。握手之后，一个大小为 1460 字节的 TCP 数据包发送到打印机 ❶。数据大小既可以在 Packet List 面板 Info 列的右边看到，也可以在 Packet Details 面板的 TCP 头部信息的底部看到。

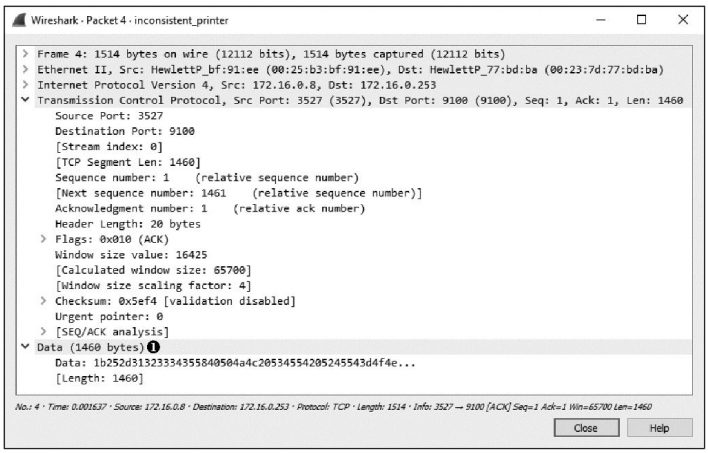

图 10-25 通过 TCP 传输到打印机的数据

数据包 4 后面是另一个包含 1460 字节的数据包 ❶，如图 10-26 所示。这个数据被打印机 ❷ 确认了。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.0.8	172.16.0.253	TCP	66	3527 → 9100 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.000166	172.16.0.253	172.16.0.8	TCP	66	9100 → 3527 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1460 WS=1 SACK_PERM=1
3	0.000201	172.16.0.8	172.16.0.253	TCP	54	3527 → 9100 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.001637	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=1 Ack=1 Win=65700 Len=1460
5	0.001646	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=1461 Ack=1 Win=65700 Len=1460 ❶
❷ 6	0.005493	172.16.0.253	172.16.0.8	TCP	160	9100 → 3527 [PSH, ACK] Seq=1 Ack=2921 Win=7888 Len=106
7	0.005561	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=2921 Ack=107 Win=65592 Len=1460
8	0.005571	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=4381 Ack=107 Win=65592 Len=1460
9	0.005578	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=5841 Ack=107 Win=65592 Len=1460
10	0.005585	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=7301 Ack=107 Win=65592 Len=1460
11	0.033569	172.16.0.253	172.16.0.8	TCP	60	9100 → 3527 [ACK] Seq=107 Ack=8761 Win=6144 Len=0
12	0.033626	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=8761 Ack=107 Win=65592 Len=1460
13	0.033640	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=10221 Ack=107 Win=65592 Len=1460
14	0.033649	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=11681 Ack=107 Win=65592 Len=1460
15	0.033658	172.16.0.8	172.16.0.253	TCP	1514	3527 → 9100 [ACK] Seq=13141 Ack=107 Win=65592 Len=1460
16	0.098314	172.16.0.253	172.16.0.8	TCP	60	9100 → 3527 [ACK] Seq=107 Ack=14601 Win=4400 Len=0

图 10-26 正常的数据传输和 TCP 确认

在捕获文件的最后两个数据包之前，数据流一直正常。数据包 121 是一个 TCP 重传数据包，也是故障的第一个标志，如图 10-27 所示。

当一个设备发送 TCP 数据包给远程设备，而远程设备没有确认此次传输时，就发送一个 TCP 重传数据包。一旦到达重传门限，发送设备就假设远程设备没有收到数据，从而立刻重传数据包。在通信停止之前，这个过程重复了多次。

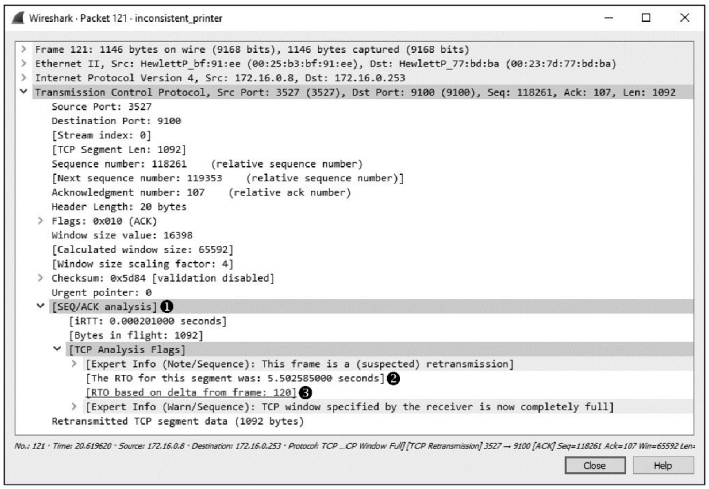

图 10-27　这些 TCP 重传数据包是故障的一个标志

在这个场景中，因为打印机没有确认传输的数据，所以客户工作站就向打印机发送重传数据包。如果展开 TCP 头部的 SEQ/ACK analysis 部分以及下方的额外信息，如图 10-27 所示 ❶，你就可以从细节中看到为什么这是重传。根据 Wireshark 加工的细节，数据包 121 是数据包 120 的重传 ❸。另外，重传数据包的重传超时（RTO）在 5.5s ❷ 左右。

当分析数据包间隔时间时，你可以更改时间显示格式以适应特定情形。在这个案例中，我们想看一看之前的数据包在发送多久后发生了重传，于是选择 View->Time Display Format 并改成 Seconds Since Previous Captured Packet 这个选项。然后，如图 10-28 所示，你可以清楚地看见初始数据包（数据包 120）发送 5.5s 后发生了数据包 121 的重传 ❶。

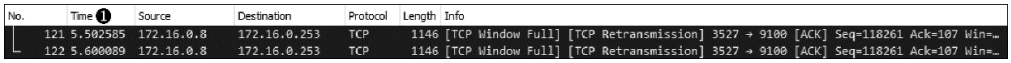

图 10-28　查看数据包间隔时间有利于解决问题

下一个数据包是数据包 120 的另一个重传。这个数据包的 RTO 是 11.10s，包括上一个数据包的 5.5s RTO。Packet List 面板的 Time 列告诉我们，在上一次重传 5.6s 后发生了这次重传。这好像是捕获文件中的最后一个数据包，巧合的是，打印机大概在这个时间停止打印了。

好在这个分析场景只涉及内网的两台设备，所以我们只需要确定是客户工作站还是打印机的问题。我们可以看见数据正常流动了相当长的时间，然而在某一时刻，打印机停止响应工作站了。工作站尽了最大努力投递数据包，重传就是一个明证，但打印机就是没有响应。这个问题可以在其他工作站上重现，所以我们猜测打印机才是问题的来源。

进一步分析后，我们发现打印机的内存出故障了。当大量打印作业发送到打印机时，它只打印一定的页数，一旦访问到特定内存区域就停止工作。由此可见，内存问题导致打印机无法接收新数据，并中断了与主机的通信。