6.7 TShark 里的时间显示格式

TShark 里一个经常让新手们感到困惑的问题就是默认的时间戳。它显示从数据包捕获开始的相对时间戳。有些时候这种时间戳格式还比较有用，但在很多情况下你想看到的是包捕获的实际时间，而这是 Tcpdump 所使用的时间戳默认值。要想和 Tcpdump 的输出格式一样，你可以使用-t 参数再加上值 ad 以显示绝对时间。

```
C:\Program Files\Wireshark>tshark –r packets.pcap –t ad
```

这里是一个基于同样的捕获文件使用默认的相对时间戳 ❶ 和绝对时间戳 ❷ 之间的比较：

```
❶ C:\Program Files\Wireshark>tshark -r packets.pcap -c2
  1 0.000000 172.16.16.172 -> 4.2.2.1       ICMP Echo (ping)
request id=0x0001, seq=17/4352, ttl=128
  2 0.024500 4.2.2.1 -> 172.16.16.172       ICMP Echo (ping)
reply id=0x0001, seq=17/4352, ttl=54 (request in 1)
❷ C:\Program Files\Wireshark>tshark -r packets.pcap -t ad -c2
  1 2015-12-21 12:52:43.116551 172.16.16.172 -> 4.2.2.1 ICMP Ech
request id=0x0001, seq=17/4352, ttl=128
  2 2015-12-21 12:52:43.141051 4.2.2.1 -> 172.16.16.172 ICMP Ech
reply id=0x0001, seq=17/4352, ttl=54 (request in 1)
```

通过使用-t 参数，你可以自定义时间显示格式，就像你在 Wireshark 里看到的那样。这些格式值的含义都在表 6-1 中。

表 6-1　TShark 中可用的时间显示格式

值	时间戳	示例
a	包被捕获的绝对时间（在您的时区）	15:47:58.004669
ad	包被捕获的带日期的绝对时间（在您的时区）	2015-10-09 15:47:58.004669
d	自之前捕获的数据包以来的增量（时差）	0.000140

值	时间戳	示例
dd	之前显示的数据包	0.000140
e	亿元时间（1970 年 1 月 1 日以来的秒数）	1444420078.004669
r	第一个数据包和当前数据包之间的运行时间	0.000140
u	捕获数据包的绝对时间（UTC）	19:47:58.004669
ud	带日期的捕获数据包的绝对时间（UTC）	2015-10-09 19:47:58.004669

然而 Tcpdump 不提供这样多层面时间戳格式的控制。