4.3.1 时间显示格式

Wireshark 所捕获的每一个数据包都会由操作系统给予一个时间戳。Wireshark 可以显示这个数据被捕获时的绝对时间戳，也可以是与上一个被捕获的数据包或是捕获开始及结束相关的相对时间戳。

与时间显示相关的选项可以在主菜单的 View 菜单中找到，如图 4-7 所示，可以让你设置时间的精度。

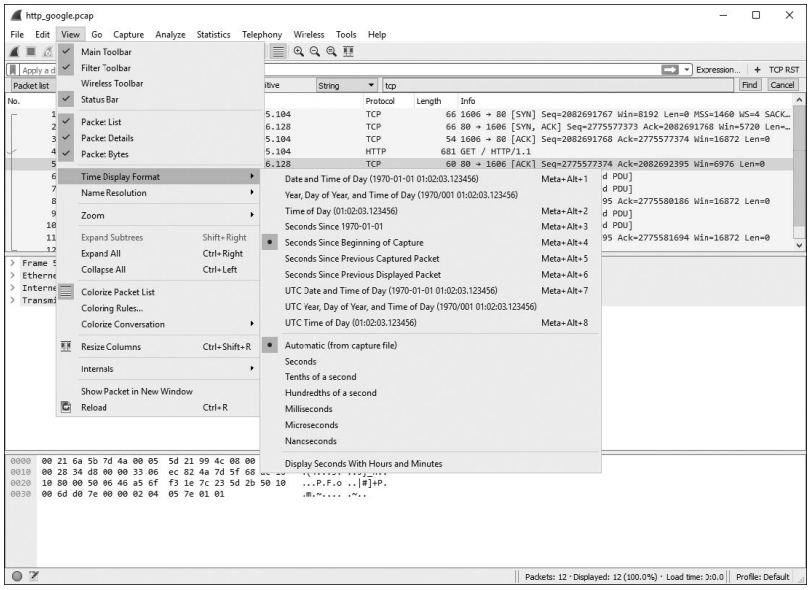

图 4-7　多种可用的时间显示格式

时间表示格式选项可以让你根据时间显示方式调整不同的设置。这包含了日期和时间、UTC 日期和时间、自 UNIX 纪元起的秒数、自第一个包起的秒数（默认）、自上一个包起的秒数等。

格式选项允许你选择不同的格式，而精度选项允许你将精度设定为自动或者手动，比如秒、毫秒、微秒等。在本书后面，我们将调整这些设置，所以你现在就需要熟悉它。

> 注意
>
> 从多个设备中比较包数据，一定要确认这些设备之间的时间是同步的，特别是当你做取证分析和检查问题时。你可以使用网络时间协议（NTP）来确保网络设备的时间是同步的。当包数据来自不同时区的设备时，请考虑使用统一的 UTC 时间来避免干扰。