

The Ramifications of the 2007 Daylight Savings Time Changes on Computer Forensics

By now the dust has settled in most corporate IT offices, having passed through yet another threat to the sanity of a computer controlled world. The threat this time is a simple change that robs farmers of an hour of daylight and bestows it to commuters, school kids and evening softball leagues. Thanks to a bevy of patches, fixes and registry edits, the disruption caused by the change in the way daylight savings time (DST) is administered will be a one time inconvenience, that is, assuming that it is not further altered in the near future. However, for computer forensic examiners, the changes to DST are a lingering issue that may last for years in to the future.

A Quick Look at DST

Daylight saving time (DST), also known as **summer time** in British English, is the convention of advancing clocks so that evenings have more daylight and mornings have less. (Wikipedia, 2007) Proponents of DST point to studies that appear to show that additional daylight in the evening saves energy, reduces traffic accidents and nominally lowers crime. Until the current changes were implemented, the United States has been using DST on a set schedule since 1986. Since there are not a lot of Windows '86 PCs around, the change then from the previous standard is of little consequence to computer forensics. The chart below outlines the changes from the 1986 standard to the current 2007 schedule. (Microsoft, 2007) The net result is that DST now starts three weeks earlier and ends one week later than it did in 2006 and prior.

| Change in daylight saving time: | | | |
|--|---|-------------------------------|---|
| Previously DST started on: | With the new law, DST will start on: | Previous DST ended on: | With the new law, DST will end on: |
| First Sunday of April | Second Sunday of March | Last Sunday of October | First Sunday of November |

A Primer on Dates and Times

Before looking at the impact of the DST changes on computer forensic cases, it is necessary to understand a little about how different versions of Microsoft file systems store

dates and times. The issue here is not as much about operating systems as it is about disk file systems, however, the evolution of the two are closely related.

The dates and times that are most interesting from a forensic point of view are usually the modified, accessed and created (MAC) dates. The method used to store and decipher these MAC dates has changed as the file systems used have grown more robust. For sake of simplicity, the discussion of file systems and the storage of dates and times can be separated in to two categories, NTFS and everything before it.

NTFS is the file system primarily used by Microsoft in Windows NT, XP and Vista. This file system stores MAC dates and times in Coordinated Universal Time (UTC), otherwise known as Greenwich Mean Time (GMT) or Zulu (Z)time. In order to display date/time information in a format that is appropriate for a user's particular locale, Windows will translate the stored UTC time to local time using the time zone setting (also referred to as the time zone bias) on the local computer. Most major forensic tools will also perform this translation for the examiner to save the confusion and trouble of presenting evidence that is based on UTC.

File Allocation Table (FAT) file systems compromise Microsoft's offerings with most operating systems prior to those mentioned in the NTFS section above such as Windows 9X, ME etc. Although caveats exist, FAT file systems generally store MAC dates and times in local time bias, thus eliminating the need to translate from UTC during an exam.

The Evidentiary Problem

If all this techno gibberish has you wondering how this affects digital evidence, I believe that I have finally arrived at the point. The crux of the issue is that if a PC running Windows does not receive the 2007 DST patch, for 4 weeks out of every year it will be creating MAC dates and times that are one hour off from true. For those of you that are thinking that one hour off for four weeks out of every year is hardly a big deal and not worth the bits it took to store this document, then by all means read no further. For those that are bent on precision with the vigor of a Swiss watchmaker, let's press on.

NTFS – As previously mentioned, NTFS stores MAC dates in UTC format and relies on Windows or in our case, a wiz bang forensic analysis software suite to compute the local time for our view. As of this writing, the two major forensic software packages (EnCase and FTK) had both planned releases for their products that will be capable of "dynamic" DST translation that will apply the appropriate rules in effect based on the year that the MAC date occurs in.

These fixes should work pretty well to address the time change issues. Caution will have to be taken here though when dealing with pre Win XP NTFS systems such as Windows NT. Microsoft no longer provides updates for NT, and an examiner might well bump up against a

machine that was never manually updated by the user.

FAT – If you have been following along at home, you know that FAT file systems store MAC dates based on the local time in effect on the computer when the date/time stamp is created. Exams of FAT systems will be relatively unaffected **ASSUMING** (and this is a big assumption) that the system is updated to adjust for the 2007 DST changes.

Since most computers utilizing FAT file systems are pre – Win XP, and Microsoft only provides patches for Windows XP and later operating systems, chances are that there are many computer users that will not take the time to research and use the alternate methods to change an older OS to correctly deal with the 2007 DST changes. Some users might manually update their clock as necessary in March and November, while others might just let it be, knowing that it will only display incorrectly four weeks out of the year, which is better than a VCR that permanently flashes 12:00.

The Registry Tells All

If you haven't figured it out by now, you really need to know whether the computer you are going to examine has been patched or not. Other than booting it up and fiddling with the time zone settings (which I neither recommend nor condone), the most reliable source of this information is the Windows registry.

The registry key of interest here is:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

This key stores the current time zone that is being used by the computer as set in Windows. It also stores the time bias of this zone (the difference from UTC), whether or not the computer is set to automatically adjust for DST, and if so, when that occurs. Unless you are fluent in hexadecimal numbers (don't bother calling me for help), use a registry viewing program such as Access Data's Registry Viewer to look at this key and decipher the start of Standard time and the start of Daylight time that is currently set on the computer.

Computers patched to correctly deal with the 2007 DST will show a Standard time start date that begins with an "11" (the 11th month of the year), and a Daylight time start date that begins with a "3" (the 3rd month of the year)

Computers not patched will show a Standard start date that begins with “10” and a Daylight start date that begins with a “4”

Summary

If there is a bottom line summary to be made from this discussion it is that the 2007 daylight savings time changes are going to cause some changes in the way we look at dates and times during forensic exams. The combination of patched, unpatched and manually updated systems are going to create a myriad of different possibilities when analyzing dates and times that occur during the four weeks of the year that are different between the 2007 DST standard and the previous standard. Knowledge of the current settings that exist on a suspect machine will be necessary to ensure the correct reporting of this sometimes critical evidence.

Is This the End?

While this is the end of this article, it may not be the end of the story on the changes to DST. The law that mandated the change (The Energy Policy Act of 2005) mandates that the Energy Department study the impact of the 2007 changes on the usage of energy in the U.S. Should they find that the changes do not save energy as hoped I suppose we could be faced with a return to the old DST standard, or worse, a further modification of the new one.