Date, Time, and Time Zone Examination

A Discussion of Computer Date-Time Representation and Its Impact on Forensic Investigation with an Emphasis on EnCase Versions 3 & 4

White Paper

April 2003

By Kimberly Stone-Kaplan and Michele Roter

Introduction

This document will discuss methods of storing dates and times on computer systems, time zones, and how different File Systems, EnCase Version 3 and EnCase Version 4 handle and interpret dates and times. Further, it shall also address the known forensics issues concerning timestamp interpretation. The definitions of the terms used in this paper, as well as instructions for accessing the new features that are detailed, are available at the end of the document.

Timestamps are often central to a forensic computer examination. They are used not only to verify when activity occurred, but also to determine times of inactivity. Ensuring that the times an investigator sees are correct is a crucial part of forensic computer investigations. A multitude of complications arise when interpreting these dates correctly. Each file system has its own method of storing the data as well as interpreting the dates based on time zone and daylight savings change. EnCase v4 seeks to ease the burden on investigators with the newly integrated time zone and Daylight Saving Time support.

1. Representation of Dates and Times

Dates and times on a computer are stored in binary – as is everything else. Although values may appear equivalent, each operating system interprets the data based upon its own internal definition for a date and time. On a Unix system, for example, the date and time is a 4-byte numeric value representing the number of seconds since January 1, 1970. In contrast, on a Windows system, the timestamp is an 8-byte number representing the number of 100-nanosecond intervals since January 1, 1601. Whereas, a DOS system stores the date and time as a 4-byte value representing the number of seconds since January 1, 1980.

In addition to calculating the values based on the operating system, the time zone offset for these values must be taken into consideration. Some systems, such as NTFS and HFS+, store the values converted into Greenwich Mean Time, GMT, regardless of the time zone the system was set to. Other operating systems store the timestamp without any conversion, in local time. Those systems, which include FAT (under DOS), HFS and CDFS, store the time as is shown on the system clock.

When the time is displayed to the user, if it was stored in GMT, it is converted to the local time zone based upon the current time zone settings. A local-time system simply displays the date as stored. Switching the time zone on a GMT system is trivial; the stored GMT time is just converted and displayed in the desired time zone. However, a local-time system requires that the initial time zone be established prior to comparing dates, since there's no marker to indicate the time zone used when storing that time. If a particular timestamp is 7:00 pm 4/2/2001, and it needs to be adjusted to Eastern Standard Time, how many hours need to be added or subtracted from the original time? Clearly, in a local time environment, the original time zone must be known to facilitate proper adjustment to a different time zone.

2. Daylight Saving Time

When interpreting dates and times, Daylight Saving Time (DST) must also be accounted for. On a local-time system, DST is not an issue since the time that an action occurred is precisely the time stored. However, on a GMT system, DST may modify the offset from GMT during a particular season and therefore must be incorporated. For example, as Table 1 illustrates, Pacific Time is 8 hours behind GMT in the winter. However, when DST begins, clocks are set forward an hour and the offset changes to 7 hours during this season.

Ex.	Local Time	GMT Offset	Stored Time (GMT)
1	2pm 1/3/01 PST	-8 hours	10pm 1/3/01
2	2pm 8/3/01 PDT	-7 hours	9pm 8/3/01

Table 1: Local Time to Stored GMT Time

3. EnCase Version 3 and Other Forensic Tools

As stated previously, currently existing methods of storing timestamps do not store any information related to time zone or DST status. The repercussions of the DST issue can be seen in the Windows operating system itself; if a file is created at 2pm on January 3rd, and the Properties for that file are viewed in July (during DST), the creation time will be displayed as 3pm. Conversely, if a file is created at 2pm on August 3rd (during DST), and the Properties for that file are later viewed in March (Standard Time), the creation date will be displayed as 1pm. Windows does not adjust the timestamps to accurately reflect the original creation time.

When displaying a time in a GMT-time system, EnCase v3 uses the time zone settings of the investigating computer to obtain the time zone offset. That offset is used to adjust any GMT times in the evidence file from GMT to the local time zone. As long as the time zone of the investigating computer matches that of the file system on the evidence file, the times shown in EnCase v3 should in theory correlate to the time on the suspect machine when the event took place. However, on a GMT system, DST becomes an issue. EnCase v3 applies the current time zone offset to all times in the evidence file, thus if the time in question occurred in the opposite time of the year (Daylight or Standard) from the current one, then the time EnCase v3 reports would be off by an hour. Table 2 illustrates these differences – the stored times are referenced from Table 1.

Ex.	Stored Time (GMT)	Date Investigated	Displayed time
1.1	10pm 1/3/01	3/5/02 (PST)	2pm 1/3/01
1.2	10pm 1/3/01	8/12/02 (PDT)	*3pm 1/3/01*
2.1	9pm 8/3/01	3/5/02 (PST)	*1pm 8/3/01*
2.2	9pm 8/3/01	8/12/02 (PDT)	2pm 8/3/01

Table 2: Stored GMT Time to Displayed Time in EnCase v3

Although the original local times are the same in the two examples in Table 1, the displayed times (in Table 2) are not always equivalent to the original local times due to DST issues. This anomaly occurs due to the conversions based on the GMT offset, which does not remain constant in all scenarios due to DST. Issues with the conversion are clearly identifiable in Table 2, examples 1.1 and 1.2 versus 2.1 and 2.2. The times from the first two examples occurred in January, thus the GMT offset was -8 hours since the user's time zone was set to Pacific Time. The same local time in July however, would yield a stored GMT time with an offset of –7 hours. Though the times are both meant to represent 2pm, the hour component of the timestamp differs from standard to daylight time.

If the date that the evidence is viewed is during standard time, all of the suspect's times that occurred during daylight time will be decreased by an hour (see Table 2, ex. 2.1). If however, the date the evidence is viewed is during DST, then all the local times stored during standard time will display an additional hour (see Table 2, ex 1.2). Investigators need to be cognizant of this issue (which is part of the EnCase Forensic Methodology training) and adjust certain times accordingly when using EnCase v3.

EnCase Version 3 / Other Tools Scenario: A man in California was suspected of a criminal act, however he states that during the time of the alleged act, 3PM on August 22nd 2001, he was at home on his computer. The computer, running NTFS on Microsoft Windows 2000, a GMT conversion file system, was subsequently seized and the investigation begins.

On January 3rd 2002, after acquisition of the hard drives in the machine, the investigator is searching for timestamps to indicate active use during the time the user claimed to be using his system. Using

EnCase v3, the investigator finds a Microsoft Word document with a file creation date of 3:10PM on August 22nd. This time is remarkably close to the time of the alleged act, which would support the suspect's claim. The next question the investigator must address is whether the times were converted correctly.

Initially, the investigator can easily note that the date in question, 8/22/01, is in DST, and the current date (1/3/02) is not. This, coupled with the fact that the OS being investigated is NTFS, a GMT-based system, indicates that the displayed time is not being converted correctly. He then looks into the timestamp issue further to determine the correct conversion.

First, the investigator verifies that the time zone of the investigating computer is set to Pacific Time as well, which it is. Next, he calculates what the stored time should be. If the original time of file creation was 3:10PM, and Daylight Savings was in effect in August, then the time offset is –7 hours, and the stored time in GMT is determined to be 10:10PM.

Reported Time – GMT offset = Stored Time
3:10PM – (-7) hours = 10:10 PM

Then, the investigator must determine if the investigative computer is in the same season as the timestamp in question, to check if DST must be taken into account. If the examination is on January 3rd, 2002 and the time zone is Pacific Time, this date does not fall within Daylight Savings, and the active GMT offset is –8 hours. The stored GMT time, 10:10PM, plus the GMT offset, -8 hours, provides the original display time: 2:10PM. Thus, the display time of 3:10PM on August 22nd does not absolve the suspect since the local time was in fact 2:10PM, not 3:10PM.

Stored Time + GMT offset = Original Time
10:10 PM + (-8) hours = 2:10 PM

This conversion can be verified by setting the date of the examination computer to a date in Daylight Saving Time, restarting EnCase v3, and viewing the file creation date. Because the seasons of the investigating computer and of the file creation dates in question are now the same, the file time will be displayed correctly.

With the additional features in EnCase Version 4, these types of verifications for dates are no longer required.

5. EnCase Version 4

EnCase v4 has many new features to assist making date and time interpretation easier for the investigator. The extra calculations as described for EnCase v3, Windows and other tools, have been eliminated.

Daylight Saving Time Adjustment: EnCase v4 automatically adjusts the times for Daylight Saving Time based upon when the date occurred. The investigator does not need to add or subtract an hour to adjust for times that occurred in the opposite season of the current one. EnCase will adjust the times on a GMT system by default.

To revisit the example previously used, Table 3 illustrates the local time to stored time conversion for a GMT system in the Pacific Time Zone.

Ex.	Local Time	GMT Offset	Stored Time (GMT)
1	2pm 1/3/01 PST	-8 hours	10pm 1/3/01
2	2pm 8/3/01 PDT	-7 hours	9pm 8/3/01

Table 3: Local Time to Stored GMT Time

EnCase v4 recognizes GMT times based upon the file system being examined, and applies the time zone rules for the active time zone to determine whether each date-time fell within daylight or standard time. Table 4 demonstrates the result of viewing the times of Table 3 in EnCase v4.

Ex.	Stored Time (GMT)	Date Investigated	Displayed time
1.1	10pm 1/3/01	3/5/02 (PST)	2pm 1/3/01
1.2	10pm 1/3/01	8/12/02 (PDT)	2pm 1/3/01
2.1	9pm 8/3/01	3/5/02 (PST)	2pm 8/3/01
2.2	9pm 8/3/01	8/12/02 (PDT)	2pm 8/3/01

Table 4: Stored GMT Time to Displayed Time in EnCase v4

With the automatic adjustments, the displayed times now accurately reflect the original local time regardless of when the investigator views the data.

Volume Time Zones: EnCase v4 also allows the investigator to set the time zone for each volume or device in the case individually. If no time zone is specified, the time zone is set by default to that of the investigating computer. This feature allows the investigator to correctly view the times on evidence files with differing original time zones in the same case. Times will visibly change on a GMT-based volume when a different time zone is set; rather than using the offset from the investigating computer to convert from stored GMT time to displayed local time, EnCase will use the offsets applicable to the selected time zone. Times will not change if the time zone is set on a local-time system because the times are already displayed as the original user viewed them, but establishing the time zone is very important when utilizing the third new time feature in EnCase v4 – the ability to convert all times to correspond to one time zone.

Correspond to One Time Zone: This feature allows the investigator to view all times on different evidence files in a case file adjusted to the same time zone offset. For example, if an investigator was examining two systems – one from Los Angeles and one from New York – and wanted to compare event times, it would be easier to view the times relative to one time zone rather than do the 3-hour conversion each time. If a particular file event (example 1) occurred at 12:30 pm in LA, and was compared to an event (example 2) occurring at 12:30 pm in NY on the same day, it may be more straightforward to see that the event (example 1) from LA occurred at 12:30pm Pacific Time and the event (example 2) from NY occurred at 3:30pm Pacific Time.

Any necessary daylight adjustments are taken into account before the final case-level offset is applied to the times. The original time (GMT) is placed into the volume-defined local time zone, the daylight adjustment is applied (if necessary), the time is converted back to GMT, and then the case-level offset is applied. The necessity of the conversion to GMT is why establishing the time zone for local-time systems is crucial to obtaining accurate results.

Table 5 illustrates the sequence of steps involved in determining the display value when '…correspond to One Time Zone' is set to adjust all times to PST (-8 hours). It shows how EnCase uses the volume time zone settings, DST calculations, and case time zone settings to arrive at the final displayed time.

Original Local Date & Time	GMT offset (w/DST)	Stored Time (in Windows)	Adjusted Local Time (based on volume settings) *internal EnCase processing*
12:30 pm 2/4/02 PST	-8 hours	8:30 pm GMT	-8 hours = 12:30 pm
12:30 pm 8/4/02 PDT	-7 hours	7:30 pm GMT	-8 hours = 11:30 am
12:30 pm 2/4/02 EST	-5 hours	5:30 pm GMT	-5 hours = 12:30 pm
12:30 pm 8/4/02 EDT	-4 hours	4:30 pm GMT	-5 hours = 11:30 am

Adjusted Local Time (based on volume settings) *internal EnCase processing*	Adjust for DST *internal processing*	Back to GMT (based on volume settings) *internal processing*	PST Display Time (apply case settings)
-8 hours = 12:30 pm	+0 hr = 12:30 pm	+8 hours = 8:30 pm	**-8 hours = 12:30 pm**
-8 hours = 11:30 am	+1 hr = 12:30 pm	+8 hours = 8:30 pm	**-8 hours = 12:30 pm**
-5 hours = 12:30 pm	+0 hr = 12:30 pm	+5 hours = 5:30 pm	**-8 hours = 9:30 am**
-5 hours = 11:30 am	+1 hr = 12:30 pm	+5 hours = 5:30 pm	**-8 hours = 9:30 am**

Table 5: Detailed representation of EnCase v4 timestamp conversion with case-level adjustments for comparison to one time zone

This one time zone comparison is extremely valuable to an investigator to determine what events across multiple time zones are taking place at the same moment. The times derived for this comparison must not be used to state that a suspect initiated the event at this derived comparison time. To determine when a suspect performed an event, the file times must be displayed using the original time zone of the suspect's computer with the Daylight Saving Time adjustment enabled

6. Conclusion

This paper has addressed the main aspects of timestamp interpretation as related to forensic computer examination. The investigator must be aware of the effects of Daylight Saving Time and time zone upon computer timestamps, as this knowledge is necessary to correctly interpret timestamps under EnCase v3, Windows and other tools, and while examining the system itself. EnCase v4 offers multiple features to assist investigators in handling DST and time zone issues, including the ability to establish time zones on individual volumes within a case, automatic adjustment for DST, and the ability to compare all volumes to a single time zone. While these additions are powerful, the investigator should still be aware of the underlying behavior to fully appreciate and use these features.

Definition of Terms

DST: Daylight Saving Time; the dates during which DST is in effect

GMT: Greenwich Mean Time

GMT system: A file system that stores the dates and time by converting to GMT.

Local-Time system: A file system that stores dates and times as currently displayed on the clock.

PST: Pacific Standard Time

PDT: Pacific Daylight Time

User Interface Notes

Automatic Daylight Savings Adjustment in EnCase v4: This feature can be turned off by right clicking on the case, selecting 'Modify Time Settings…' and unselecting the 'Account For Seasonal Daylight Saving Time Adjustment' checkbox. Doing so will produce the times seen in EnCase version 3.

Case-level Time Zone Settings in EnCase v4:
To access these settings, right click on the case, select 'Modify Time Settings…' and select the 'Convert all dates to correspond to one time zone' checkbox. Selecting this box will enable the list of time zones. If a time zone that observes Daylight Saving Time is selected, the 'Daylight Setting' selection box will also be enabled. A particular season must be selected to determine what the standard offset from GMT will be. For example, PST is –8 hours from GMT, but PDT is –7hours. The selected offset will be applied to all files from their GMT representation.

Volume Time Zone Settings in EnCase v4: To access these settings, right click on the volume and select "Modify Time Zone Settings" The time zone data is read from the Windows registry. If the selected time zone observes DST, the DST settings will be enabled. The options will be filled with the settings in the Windows registry for the selected time zone; the investigator can change them, but it is strongly recommended to keep the default settings.