Identification of Time Zone Settings on Suspect Computer

Introduction

In a forensic examination, establishing the time zone from the suspect system is one of the first tasks for a forensic examiner. If this information is not established at an early stage and taken into account, then the validity of all date/time values may be brought into question due to the way operating systems and browser applications store date/time information.

Date/Time Values

Operating systems and browser applications store date/time information in different ways using a variety of different timestamp formats. Many timestamps are stored in UTC, and then converted to local time when presented to the user, and some are stored in local time. It is therefore extremely important to establish the correct time zone setting for the system to correctly convert these timestamps.

Universal Coordinated Time

Coordinated Universal Time (UTC) is the international standard upon which civil time is based and by which the world regulates time. UTC is based upon UT1, which is the time determined by the rotation of the Earth. In accordance with international agreement, UTC and UT1 are not permitted to differ by more than 0.9 of a second. When it appears that the difference is approaching this limit, a one second change is introduced to bring the two back into alignment. On average, this occurs once every 12 - 18 months. Since the 1st January 1972, there have been 24 positive leap second adjustments. UTC is the time standard used for many Internet and World Wide Web protocols. The Network Time Protocol (NTP) is designed to synchronise clocks and computers over the Internet and encodes time using the UTC system. It is widely used as it avoids confusion with time zones and daylight saving changes. Each local time is represented as an offset from UTC, with some zones making adjustments during the year for daylight saving. Greenwich Mean Time is a widely used historical term, however, due to ambiguity, its use is no longer recommended in technical contexts.

Daylight Saving and Standard Time

UTC does not change with a change of seasons; however, local time or civil time may change if a time zone jurisdiction observes Daylight Saving Time or summer time. For example, UTC is 5 hours ahead of local time on the east coast of theUnited Statesduring the winter but 4 hours ahead during the summer. Not all time zones observe daylight saving. To deal with the numerous time zone changes throughout the world, Microsoft periodically release a time zone update to accommodate Daylight Saving Time (DST) changes in several countries.

How NetAnalysis deals with Time Zones

NetAnalysis provides the forensic examiner with the necessary tools to automatically convert UTC timestamps to local time (and vice versa) during import. It is extremely important that NetAnalysis is set to the time zone of the suspect system and not that of the forensic examiner's workstation. In some situations, you may discover browser records from multiple time zones. In this situation, it is difficult to accurately convert between UTC and local time. NetAnalysis has built-in functionality to easily deal with this scenario. To access the time zone settings, select Tools » Options from the Tools menu. Figure 1 shows the Time Zone Settings page.

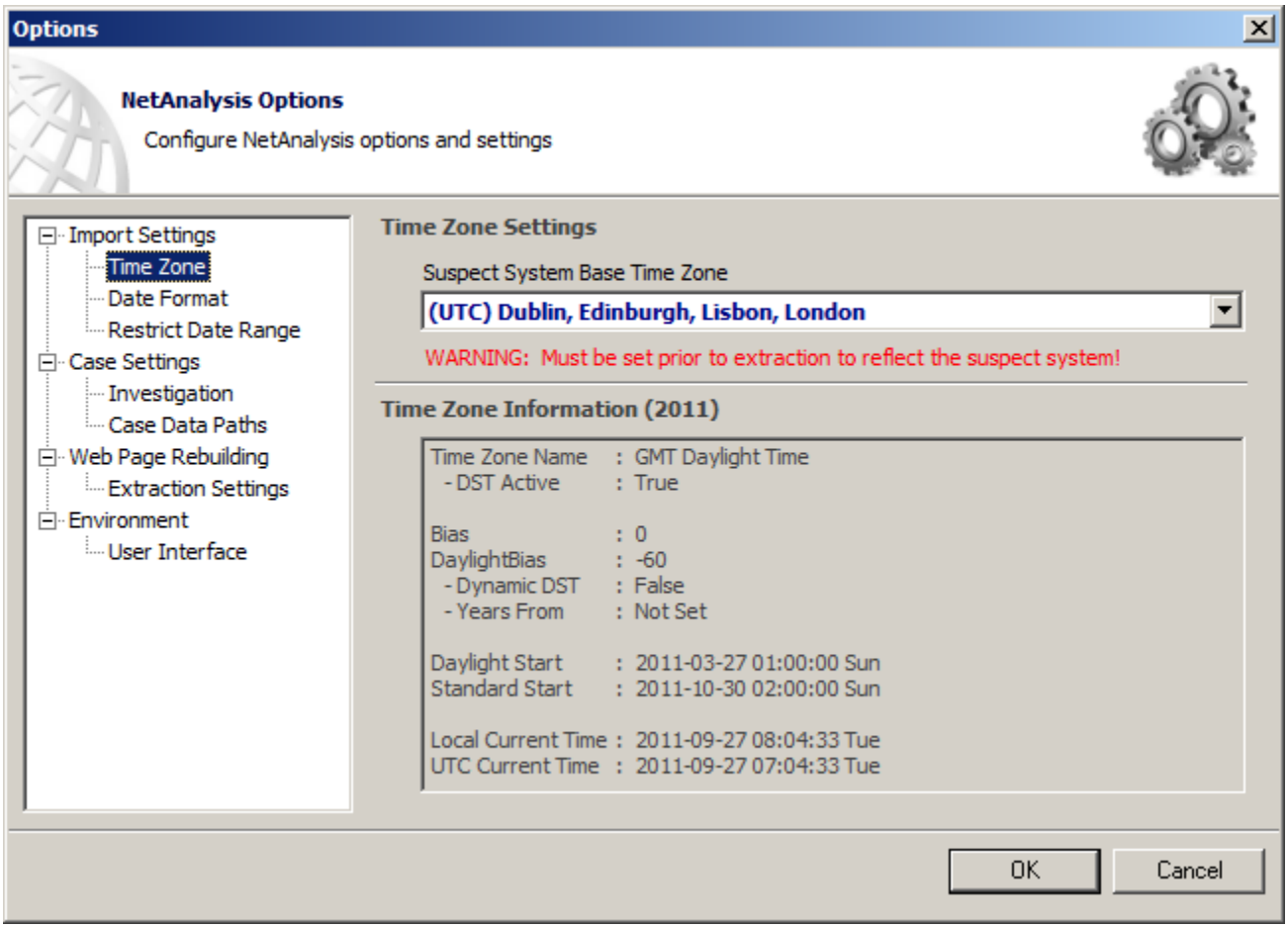


Figure 1

If the time zone of the suspect computer is not identified prior to extracting and viewing any Internet history or cache data then the date/time stamps may not be accurately represented! You MUST establish the correct settings prior to importing any data.

Identification of Suspect Machine Time Zone

When examining a Microsoft Windows NT system, the time zone information can be established by reviewing the SYSTEM registry hive. To enable us to identify the correct Time Zone Information sub-key, we need to establish which Control Set was active when the computer was seized.

ControlSets

A control set contains system configuration information such as device drivers and services. You may notice several instances of control sets when viewing the registry. Some are duplicates or mirror images of others and some are unique. Control sets are stored in the HKEY_LOCAL_MACHINE sub tree, under the SYSTEM key. There may be several control sets depending on how often the user changed their system. A typical installation of Windows NT will contain three:

Windows NT Control Sets
HKEY_LOCAL_MACHINE\System\ControlSet001
HKEY_LOCAL_MACHINE\System\ControlSet002
HKEY_LOCAL_MACHINE\System\CurrentControlSet

ControlSet001 may be the last control set the system booted with, while ControlSet002 could be what is known as the last known good control set, or the control set that last successfully booted Windows NT.

The CurrentControlSet sub-key is a pointer to one of the ControlSetXXX keys and will only be visible when viewing a live registry. During a post-mortem examination, this key will not exist. In order to better understand how these control sets are used, you need to be aware of another sub-key, 'Select'.

Windows NT Select Key
HKEY_LOCAL_MACHINE\System\Select

The Select sub-key contains the values (as can be seen in Figure 2) Current, Default, Failed and LastKnownGood. Each of these values contains a REG_DWORD data type and refers to a specific control set. For example, if the Current value is set to 0x01, then CurrentControlSet would be pointing to ControlSet001. Similarly, if LastKnownGood was set to 0x02, then the last known good control set would be ControlSet002. The Default value usually agrees with Current, and Failed refers to a control set that was unable to boot Windows NT successfully.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

Figure 2

The most valuable set is CurrentControlSet as that reflects the active control set at the time the system was last active. If we examine the SYSTEM hive from our case, we can see that the CurrentControlSet value is 0x01 which reflects ControlSet001 (see Figure 57).

Time Zone Information Sub-Key

Now that the CurrentControlSet has been identified, we can navigate to the sub-key containing the time zone information.

Windows NT TimeZoneInformation Sub-Key
HKEY_LOCAL_MACHINE\ControlSet001\Control\TimeZoneInformation

Figure 3 shows the various values stored under this sub-key.

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0xffffff4c (4294967116)
Bias	REG_DWORD	0xffffff88 (4294967176)
DaylightBias	REG_DWORD	0xfffffc4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-1501
DaylightStart	REG_BINARY	00 00 03 00 05 00 03 00 00 00 00 00 00 00 01 00
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-1502
StandardStart	REG_BINARY	00 00 0a 00 05 00 04 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Turkey Standard Time

Figure 3

ActiveTimeBias

This value is the current time difference from UTC in minutes, regardless of whether daylight saving is in effect or not. It is this value that helps establish the current time zone settings.

Bias

This value is the normal time difference from UTC in minutes. This value is the number of minutes that would need to be added to local time to return a UTC value.

StandardBias

This value is added to the value of the Bias member to form the bias used during standard time. In most time zones the value of this member is zero.

DaylightBias

This value specifies a bias value to be used during local time translations that occur during daylight time. This value is added to the value of the Bias member to form the bias used during daylight time. In most time zones the value of this member is -60.

The ActiveTimeBias determines the offset of local time from UTC and is a dynamic value. It is calculated based on the values of the Bias, StandardBias and DaylightBias dependent upon whether Standard Time is in operation or not.

ActiveTimeBias Calculations for DST and Standard Time	
Daylight Saving	ActiveTimeBias = Bias + DaylightBias
Standard Time	ActiveTimeBias = Bias + StandardBias

The above table shows the calculations for establishing the ActiveTimeBias during Daylight Saving and Standard Time.

The table below shows the calculations for converting between UTC and local time using the ActiveTimeBias. It is also possible to calculate the ActiveTimeBias when a UTC and local time are known.

UTC / Local Time Calculations with ActiveTimeBias
UTC = LocalTime + ActiveTimeBias
LocalTime = UTC - ActiveTimeBias
ActiveTimeBias = UTC - LocalTime

DaylightName

The operating system uses this name during daylight saving months to display the current time zone setting (see Returning Daylight / Standard Name Values on Page 79).

DaylightStart

This binary data is stored in a SYSTEMTIME structure; it is used to identify the date/time that daylight saving will commence for this time zone.

StandardName

The operating system uses this name during non-daylight saving months to display the current time zone setting (see Returning Daylight / Standard Name Values on Page 79).

StandardStart

This binary data is stored in a SYSTEMTIME structure; it is used to identify the date/time that standard time will commence for this time zone.

DynamicDaylightTimeDisabled

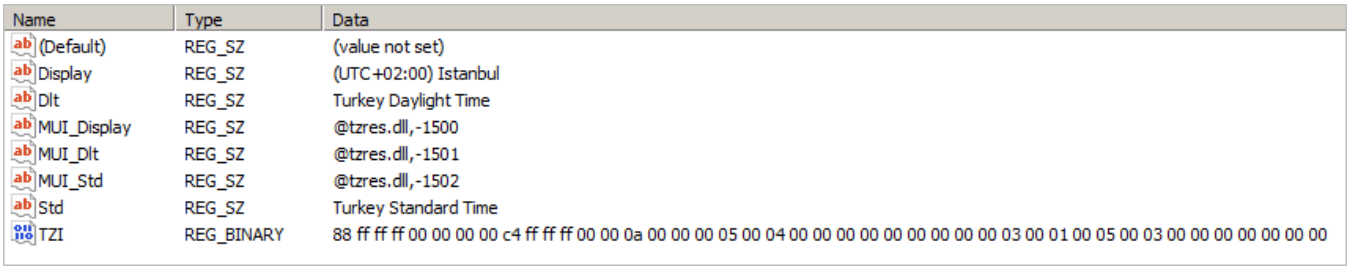
This is a Boolean value which indicates whether a DST adjustment is to be applied.

TimeZoneKeyName

This string relates to the sub-key in the SYSTEM hive where all of the available time zones are stored on a Windows NT system.

Windows NT Time Zones
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\{TimeZoneKeyName}

Figure 4 shows the Turkey Standard Time sub-key.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Display	REG_SZ	(UTC+02:00) Istanbul
Dlt	REG_SZ	Turkey Daylight Time
MUI_Display	REG_SZ	@tzres.dll,-1500
MUI_Dlt	REG_SZ	@tzres.dll,-1501
MUI_Std	REG_SZ	@tzres.dll,-1502
Std	REG_SZ	Turkey Standard Time
TZI	REG_BINARY	88 ff ff ff 00 00 00 00 c4 ff ff ff 00 00 0a 00 00 00 05 00 04 00 00 00 00 00 00 00 00 00 03 00 01 00 05 00 03 00 00 00 00 00 00 00

Figure 4

Directly below the Turkey Standard Time sub-key, there is a Dynamic DST sub-key. This holds information and structures relating to the dynamic DST settings.

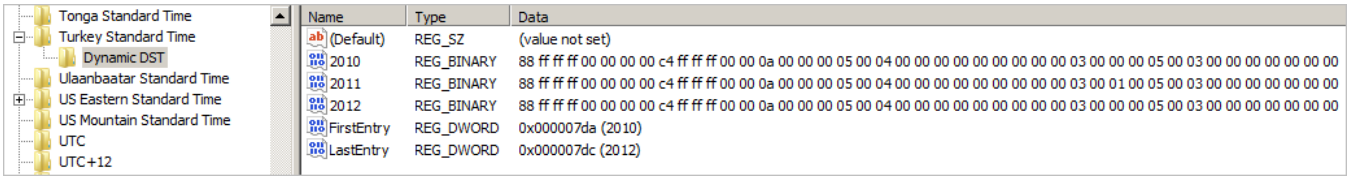


Figure 5

Dynamic DST

The implementation of Daylight Saving Time varies from country to country. Some countries may not observe Daylight Saving Time, whereas other countries may change the start dates and end dates for Daylight Saving Time every year. Dynamic Daylight Saving Time provides support for time zones whose boundaries for Daylight Saving Time change from year to year. This feature enables easier updating of systems, especially for locales where the yearly DST boundaries are known in advance. After the time zone has been updated, the current time zone setting is applied to all time operations, even when the time in question occurred before the time zone changed.