Win XP Time Synchronisation Function

The Forensic Benefits

Within the Microsoft Windows XP operating system there is a function called the Time Synchronisation Function.

This can be located by double clicking on the time that is displayed in the bottom right of the screen.

It should be noted that in addition to the usual Date & Time and Time Zone tabs there is now an Internet Time tab.

This tab will only be visible to the user if the computer **is not part of a domain**.

Under this tab there is the option to tick a box to automatically synchronise with an internet time server. By default this option will be enabled when XP is installed.

There is the option of two internet time servers, "**time.windows.com"** and "**time.nist.gov"**. By default it will be set for time.windows.com.

If synchronisation is enabled then every seven days the computer clock will synchronise with the time server provided there is an internet connection.

The user also has the option to force a manual synchronisation.

A number of events may cause a failure in synchronisation.
No internet connection
Time servers busy
Firewall blocking function
System clock is to far from the correct time.

If the system clock is more then 15 hours (54000 seconds) from the correct time then synchronisation will be prevented.

When ever the system attempts to synchronise with a time server the event will be logged within the event viewer under the system tab.

Therefore by examining the event viewer it is possible to determine if the system clock has been regularly updated and if not the reason why.

In the event that the system clock is more then 15 hours out of sync with the correct time then the event viewer will record exactly how many seconds the clock is out.

It can be seen that this function can be of enormous benefit to forensic examiners when trying to determine if the system clock was accurate at the time when the offences were committed.

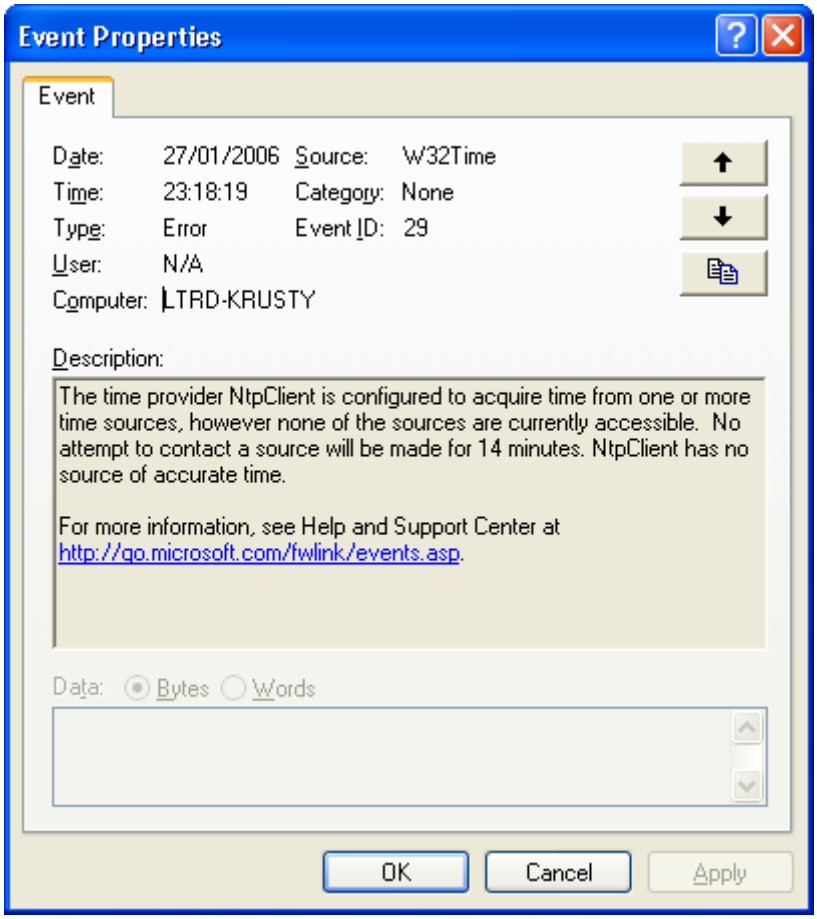
If using Forensic Software Encase, then it is a simple matter of using the Windows Event Log Parser Enscript to export out the data in a HTML format.

The registry key for the function is the **W32Time** key.

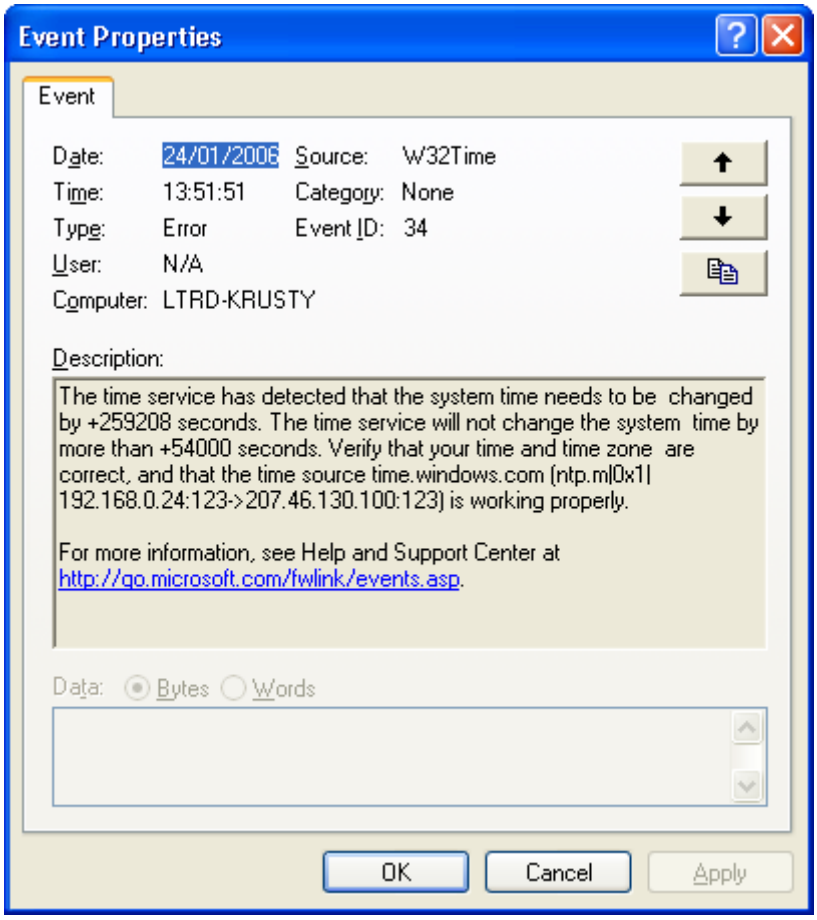
By searching for W32Time through the exported data you can quickly locate the events and the time and date they occurred.

If in doubt about an event, go to www.eventid.net where you can type in source (W32Time) and event id number to display full details of the event.

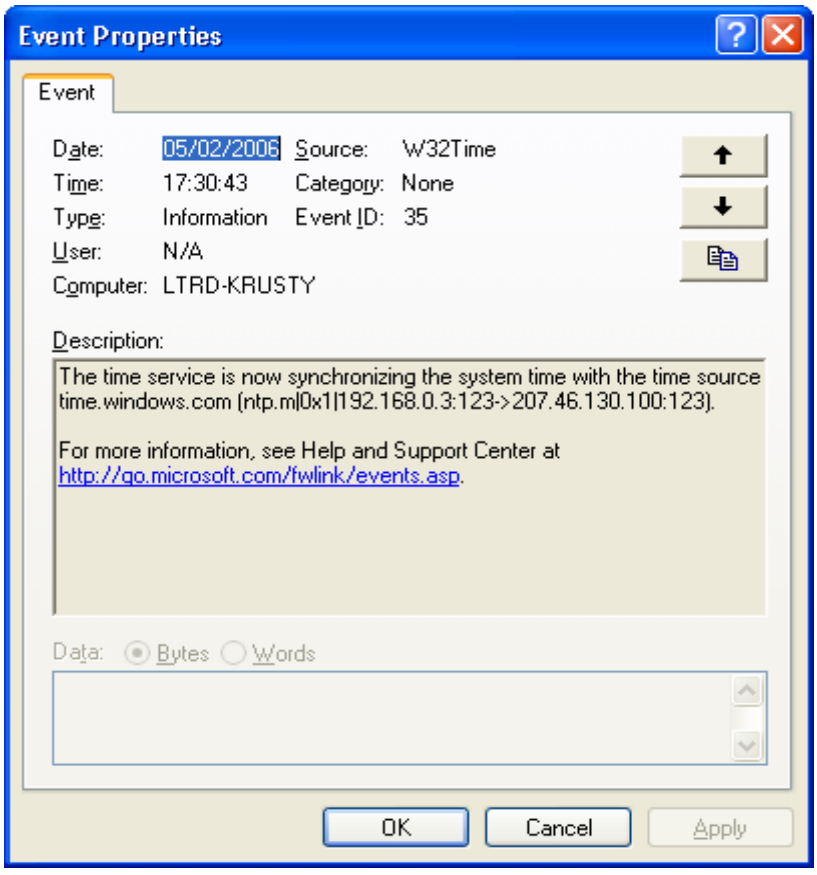
Event ID 29



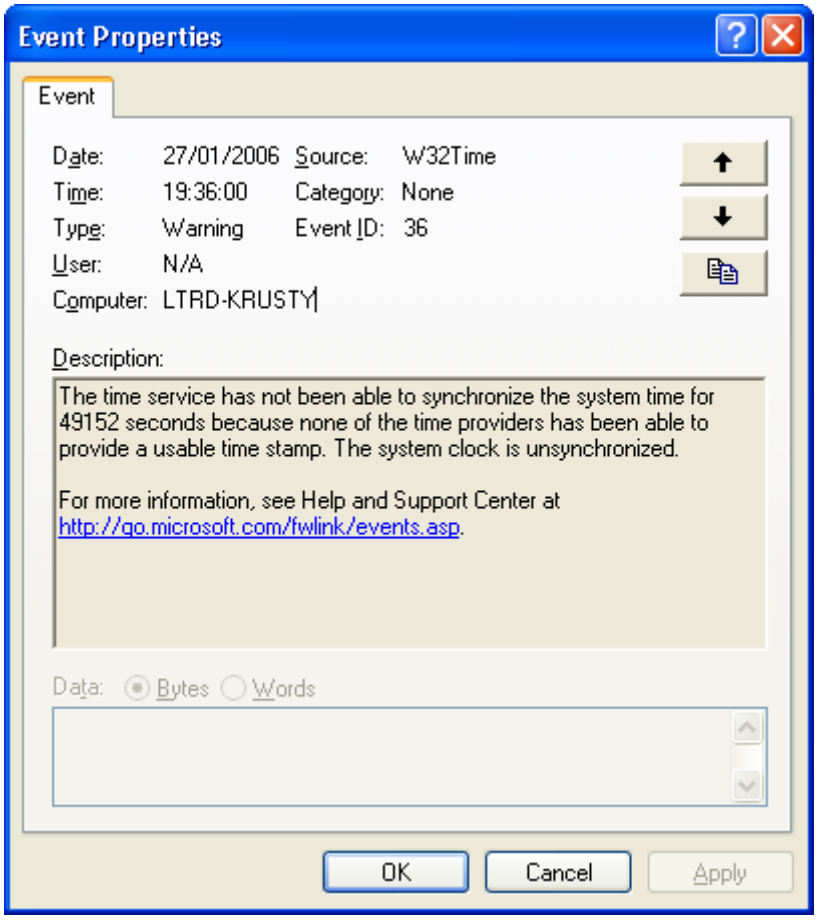
Event ID 34



Event 35



Event 36



Registry Keys for Time Synchronisation Function