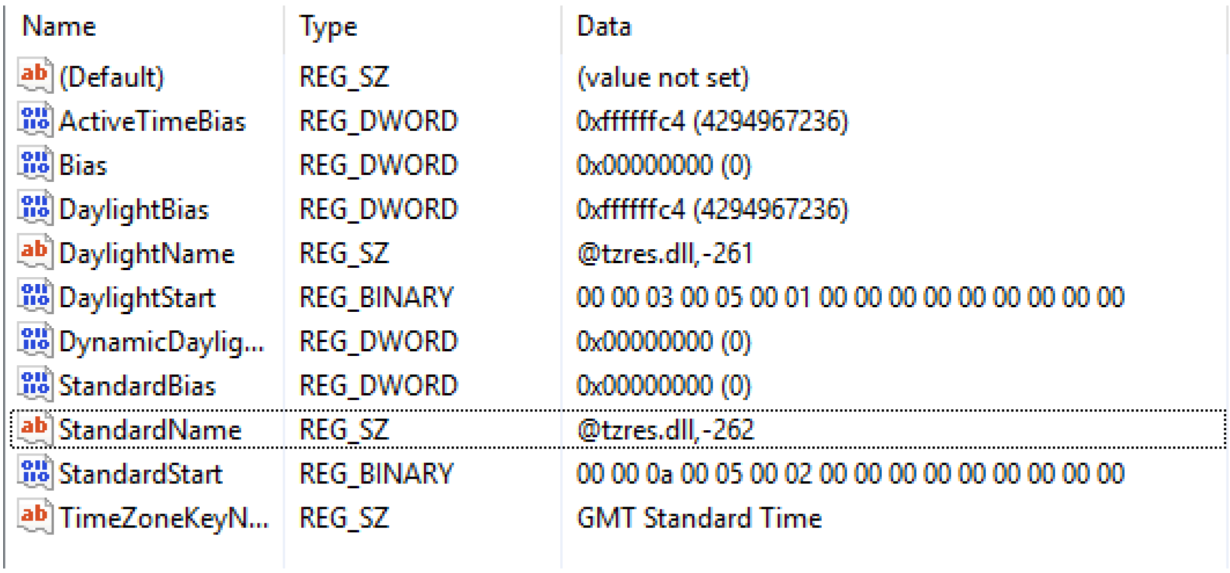
Forensic Lab sheet 3
Friday 21 October 2016.

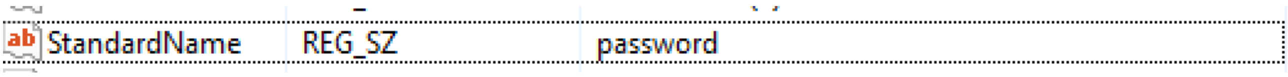
The Windows Registry contains a sufficient amount of information about a Windows computer. It would be possible for a person to hide data in there Windows registry. The registry supports the binary. Application can read and write binary data to the registry. This binary information can be modified by a person to hide text or passwords etc in their registry system. People can hide data in registry key values entries as well.

An example where a person can hide data in their registry is in the following the path.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation.
This path contains information about the time zone. There is keys in this path that the windows system does not need data for the key. They are called the DaylightName and the StandardName. These keys values are of binary. The following screenshot displays the name, type and data of the keys in this path.



Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0xffffffc4 (4294967236)
Bias	REG_DWORD	0x00000000 (0)
DaylightBias	REG_DWORD	0xffffffc4 (4294967236)
ab DaylightName	REG_SZ	@tzres.dll,-261
DaylightStart	REG_BINARY	00 00 03 00 05 00 01 00 00 00 00 00 00 00 00 00
DynamicDaylig...	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
ab StandardName	REG_SZ	@tzres.dll,-262
StandardStart	REG_BINARY	00 00 0a 00 05 00 02 00 00 00 00 00 00 00 00 00
ab TimeZoneKeyN...	REG_SZ	GMT Standard Time

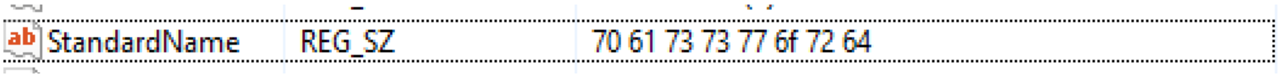
A person can easily right click in StandardName or DaylightName key and modify the value or the data binary data. Information such as passwords or text can be placed into the data. This would be extremely difficult for an forensic examiner to identify to see if the files have been modified or else identifying hidden data. As there is so much binary data, it would be very difficult to identify hiding data. A person could easily get their password and encode it to binary and simply replace the value one of the files listed above data.



ab StandardName	REG_SZ	password

I replaces the StandardName value to “password” and restarted the operating system to check if the value is saved and to see if the time on the Windows machine is correct as where we hid the data was in the time information registry.

After restarting the system. The information was saved and the time for the system was correct, therefore it is possible for people to hide messages in the registry file. It would be harder for an forensic examiner to identify hiding data if the person who was hiding information hid it in binary or hex. If data was hidden in plain text, it would be easier recognised compared to the data converted to hex.



StandardName REG_SZ 70 61 73 73 77 6f 72 64

The screenshot above is the text “password” converted to hex with space. This would be a lot harder to recognise then to the other screenshot above. The above screenshot displays text been hiding in the registry file. It is possible for people to hide data in other parts of the registry using the same technique. Identifying keys which can have their values modified without effecting the Operating system.

Reference:
https://articles.forensicfocus.com/2011/07/10/forensic-analysis-of-the-windows-registry/

http://sentinelchicken.com/data/TheWindowsNTRegistryFileFormat.pdf