Windows FILETIME format

- Windows records timestamps when applications create, access, and write to files in FILETIME format.

- A FILETIME is a 64-bit value that represents the number of 100-nanosecond intervals that have elapsed since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC).

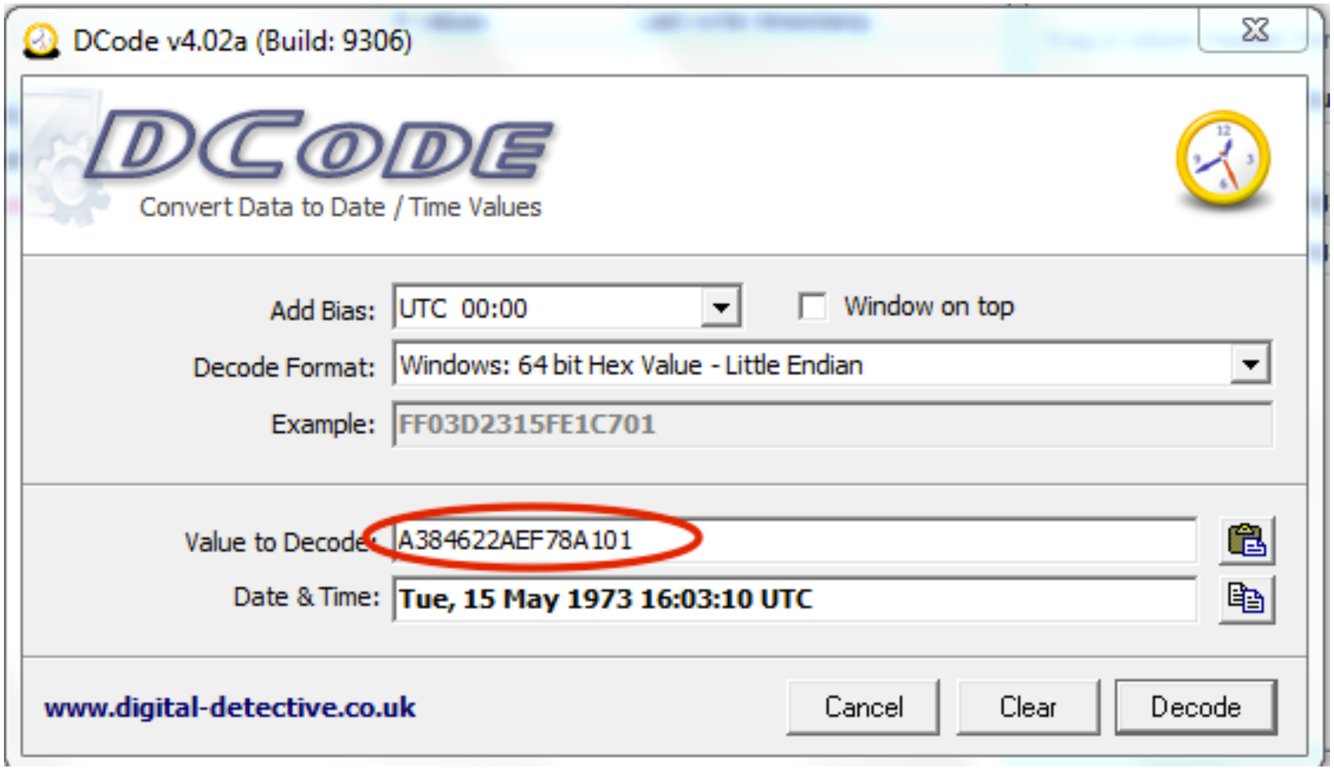
  e.g. November 26, 2002 at 7:25p PST = 0x01C295C4:91150E00.

  https://msdn.microsoft.com/en-us/library/windows/desktop/ms724290(v=vs.85).aspx

- Tools such as Dcode (http://www.digital-detective.net) can be used to covert the FILETIME data into Date & Time values.

Using Dcode

- For registry key value (timestamp): A3 84 62 2A EF 78 A1 01
- Enter the FILETEIME data in ‘Value to Decode’ area and click ‘Decode’.



DCode v4.02a (Build: 9306)
DCODE
Convert Data to Date / Time Values
□ Window on top
www.digital-detective.co.uk
Cancel
Clear
Decode

Add Bias: UTC 00:00

Decode Format: Windows: 64 bit Hex Value - Little Endian

Example: FF03D2315FE1C701

Value to Decode: A384622AEF78A101

Date & Time: Tue, 15 May 1973 16:03:10 UTC