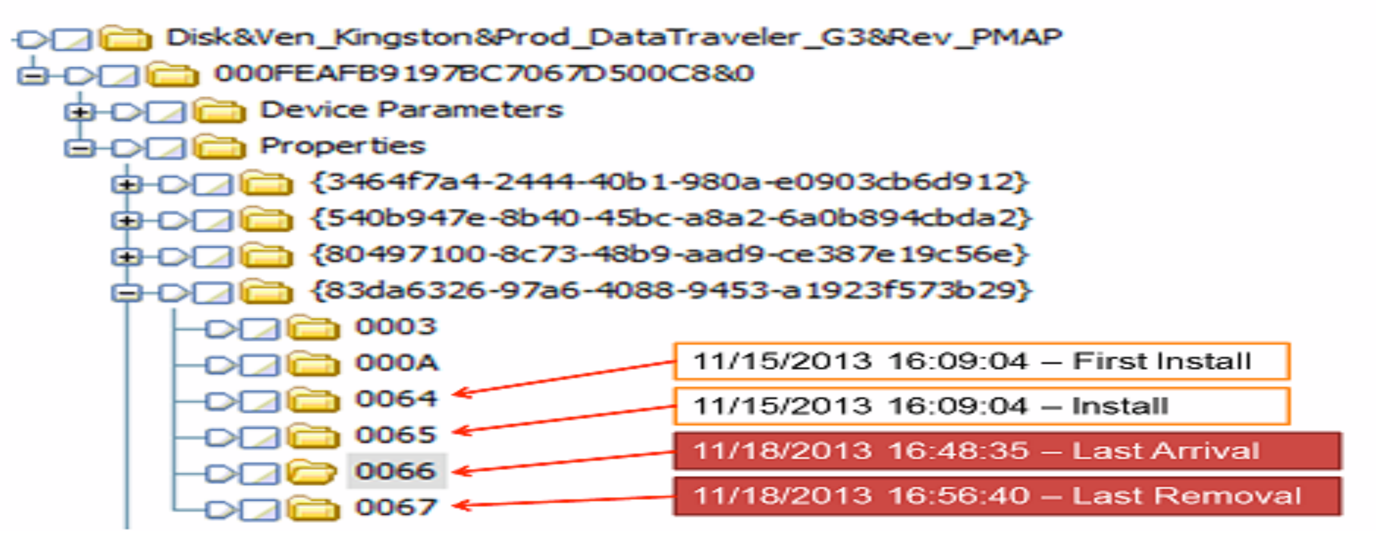
What can you find from SYSTEM?

- SYSTEM
  - Computer Name
  - Device Drivers and driver letter mappings
  - The Last Known Good Configuration
  - Setup information
  - Hardware profile
- Use of SYSTEM
  - Determine which control set is active
  - Find out timezone, Mounted devices

What can you find from SYSTEM (Con’t)?

- Finding USB last insertion and removal time.
  - In USBSTOR under:
    \ControlSet00x\Enum\USBSTOR
  - Timestamps to the registry for Device **Last Insertion (66)** Date, Device **Last Removal (67)** Date and Firmware Date.



```
Disk&Ven_Kingston&Prod_DataTraveler_G3&Rev_PMAP
  000FEAFB9197BC7067D500C8&0
    Device Parameters
    Properties
      {3464f7a4-2444-40b1-980a-e0903cb6d912}
      {540b947e-8b40-45bc-a8a2-6a0b894cbda2}
      {80497100-8c73-48b9-aad9-ce387e19c56e}
      {83da6326-97a6-4088-9453-a1923f573b29}
        0003
        000A
        0064
        0065
        0066
        0067
```

0064: 11/15/2013 16:09:04 – First Install

0065: 11/15/2013 16:09:04 – Install

0066: 11/18/2013 16:48:35 – Last Arrival

0067: 11/18/2013 16:56:40 – Last Removal

Windows FILETIME format

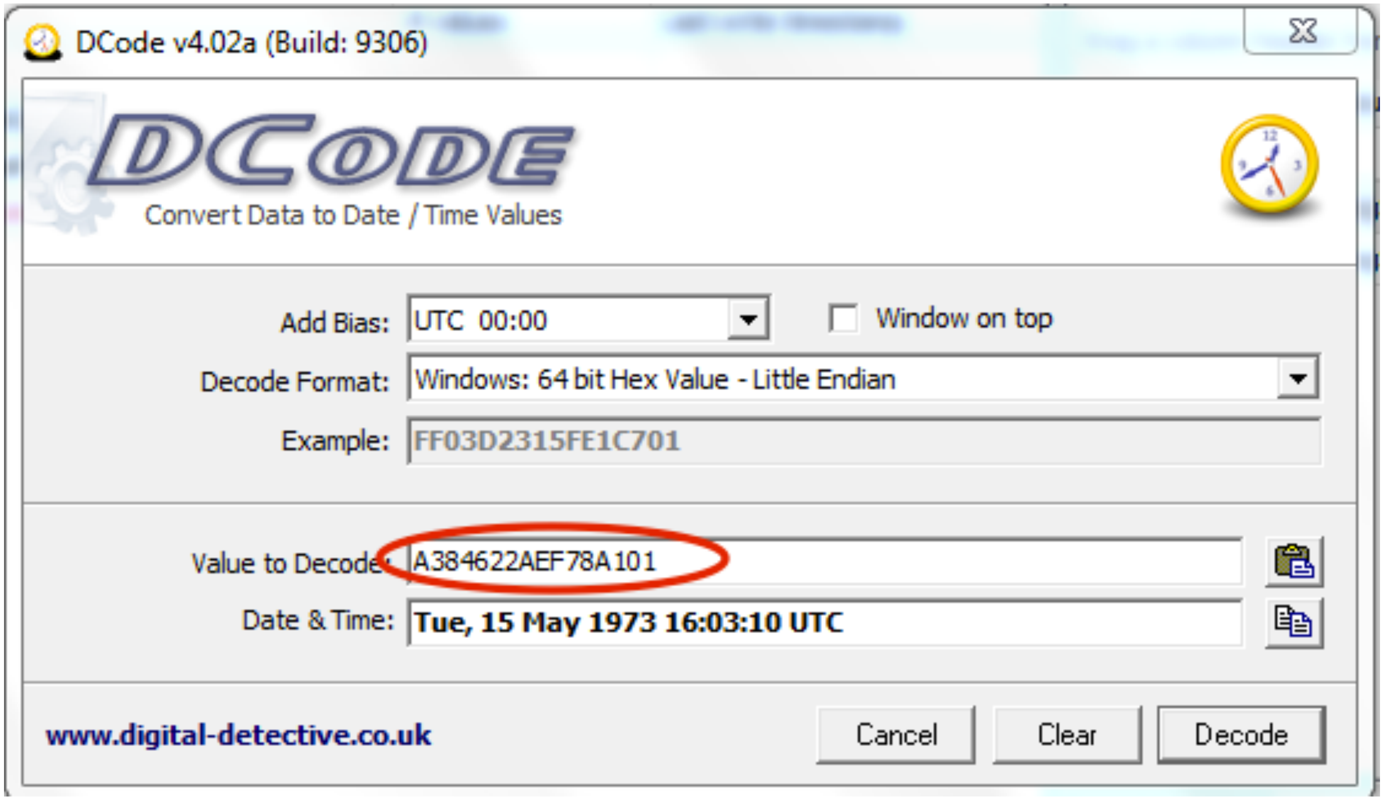
- Windows records timestamps when applications create, access, and write to files in FILETIME format.
- A FILETIME is a 64-bit value that represents the number of 100-nanosecond intervals that have elapsed since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC).

  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)

Add Bias: UTC 00:00

☐ Window on top

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

DCODE
Convert Data to Date / Time Values
www.digital-detective.co.uk
Cancel
Clear
Decode