Introduction

usbdeviceforensics is a python script to extract numerous bits of information regarding USB devices. It initially used the information from a SANS blog (Rob Lee) post to retrieve operating system specific information. It now has the ability to process multiple NTUSER.dat registry hives in one go.

The python script was originally a Windows only .Net application but I decided that it was pointless having a GUI for this applicaton.

It should be noted that whilst the information in the blog posting is accurate, there is a caveat to be aware of. During my testing I have found that an unknown process (probably an update) can update the Date/Time values across all keys, in particular the USBSTOR keys. Therefore, you could see the same Last Written Date/Time value on each device key. If you see this occurring, then you obviously cannot rely on the values retrieved. All of the dates should be UTC.

Installation

This script needs the python-registry module created by Will Ballenthin

- Install git python python-dev
- sudo pip install enum34
- git clone https://github.com/williballenthin/python-registry.git
- cd python-registry
- sudo ./setup.py install

Links

- http://blogs.sans.org/computer-forensics/2009/09/09/computer-forensic-guide-to-profiling-usb-thumbdrives-on-win7-vista-and-xp
- https://blogs.sans.org/computer-forensics/files/2009/08/usb_device_forensics_xp_guide.pdf
- https://blogs.sans.org/computer-forensics/files/2009/08/usb_device_forensics_vista_win7_guide.pdf
- http://www.swiftforensics.com/2013/11/windows-8-new-registry-artifacts-part-1.html

Future Work

- Allow timezone manipulation

Data Locations

The following outlines the key registry locations that are used to extract the information:

```
SYSTEM\CurrentControlSet\Enum\USBStor
```

This location retrieves the Vendor, Product and Version, SerialNo, ParentPrefixId and (USBStor Date/Time).

```
SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_&Prod_yyyy\xxxxx\Properties\{83da6326-97a
```

This location retrieves a FILETIME value for "Install date"

```
SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_&Prod_yyyy\xxxxx\Properties\{83da6326-97a
```

This location retrieves a FILETIME value for "First Install Date" of the driver for that USB device

```
SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_&Prod_yyyy\xxxxx\Properties\{83da6326-97a
```

This location retrieves a FILETIME value for "Last Arrival Date"

```
SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_&Prod_yyyy\xxxxx\Properties\{83da6326-97a
```

This location retrieves a FILETIME value for "Last Removal Date" of the driver for that USB device

```
System \CurrentControlSet\Enum\USB
```

This location retrieves the Vid, Pid and (Enum\USB VIDPID DateTime).

```
System \CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
```

This location retrieves the (DeviceClasses date/time).

```
System \MountedDevices
```

This location retrieves the Drive Letter, Guid and MountPoint

```
Software\Microsoft\Windows Portable Devices\Devices
```

This location retrieves the Drive Letter and Volume Name

```
SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt
```

This location retrieves the Ready Boost related information (Noted from the win4n6 mailing list)

```
NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
```

This location retrieves the Last Time Connected (MountPoints2 Date/Time)

```
Setupapi.log/setupapi.dev.log
```

This file retrieves the Install Date/Time.

If more information is required, then refer to the original SANS blog posting. Registry Date/Times

According to the SANS posting the following date and times apply different values depending on the OS:

Windows XP

```
First Time Connected After Last Reboot: DeviceClasses Date/Time
First Time Connected After Last Reboot: Enum\USB VIDPID Date/Time
```

Windows Vista

```
First Time Connected After Last Reboot: USBSTOR Date/Time
First Time Connected After Last Reboot: DeviceClasses Date/Time
Last Time Connected: Enum\USB VIDPID Date/Time
```

Windows 7

```
First Time Connected After Last Reboot: USBSTOR Date/Time
First Time Connected After Last Reboot: DeviceClasses Date/Time
Last Time Connected: Enum\USB Date/Time
```