Orion Investigations
16th 20th Floor, Unit 1601, 2001-2002, 29 Sukhumvit 63, North Klong Tan
Wattana, Bangkok 10110

Orion Investigations

Computer Forensics | Mobile Phone Forensics| Malware Investigations | Training |Data Recovery

Computer Forensics Services

Microsoft Windows 10 USB Forensic Artefacts

September 2015

Date: 17-09-2015

Author: Andrew Smith

As the capacity of USB storage devices continues to increase and the price decreases, USB forensics will often play an important part in many forensic investigations. Add to the mix a range of mobile devices such as smart phones, tablets, digital cameras and the ease of connectivity means that there are a lot of USB artefacts to be found if we know where to look. For example in Windows 7, the Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx log file contains useful information such as time stamps for the connection and disconnection of USB removable drives.

Many portable devices such as smart phones support the Media Transfer Protocol (MTP) and as a result we need to be looking in additional locations such as HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Portable Devices.

When the investigation involves USB devices the questions that often need to be answered include:

- What devices have been connected to the computer?
- When were the devices connected?
- Who connected the USB device to the computer?
- Was any data transferred to the USB device?

After returning from a trip to the UK in June this year and as a result of a discussion on USB artefacts with a former colleague, I felt inspired to do some research of my own. My aim was to create a portable tool that would collect the USB artefacts from all the different locations and present the results so the investigator can easily answer most of the above questions using just one tool. The result was a tool called USB Forensic Tracker.

I recently took the plunge and installed Windows 10 Professional on my laptop and I have to say I like it. I decided to take the opportunity to see if Windows 10 would offer any new locations where we may be able to recover USB artefacts. The main focus for this initial research was the log files within the following location: "C:\Windows\System32\winevt\Logs".

Below are details of my initial findings:

“C:\Windows\System32\winevt\Logs\Microsoft-Windows-Storage-ClassPnP%4Operational.evtx"

- The content of my log file contained 199 entries. All of them were error level entries and related to USB devices that had been connected to my computer
- The entries included details of the USB devices including vendor details, model details, firmware version and serial number of the devices
- There is a time and date stamp for the entries that could be used to show when the devices were connected
- Entries appeared for USB removable pen drives, USB fixed hard drives and pen drives that appear as fixed drives
- Entries also appeared for my laptop internal hard drive
- No entries seem to appear in the log file for MPT devices

- The log entries also include a device number. When a USB device is connected it will be device number 1. If the first device is still connected when another USB device is connected, the second device will become device number 2 and so on.
- Below are details of the Event ID's found in the log file. The Event ID 507 was the most common one found followed by Event ID 504.

Event ID	Source	Message
500	StorDiag	Completing a failed upper level read request
502	StorDiag	Completing a failed upper level paging read request
503	StorDiag	Completing a failed upper level paging write request
504	StorDiag	Completing a failed IOCTL request
505	StorDiag	Completing a failed Read SCSI SRB request
506	StorDiag	Completing a failed Write SCSI SRB request
507	StorDiag	Completing a failed non-ReadWrite SCSISRB request
510	StorDiag	Completing a failed Power request

I also wanted to see if we could find evidence of MTP devices having been connected to the computer.

Below are details of my initial findings:

"C:\Windows\System32\winevt\Logs\Microsoft-Windows-WPD-MTPClassDriver%4Operational.evtx"

This log file was also present on Windows 7 but was not present on my Windows 8.1 test machine.

For my testing I used a Samsung Galaxy S5.

- Every time the device was connected to the computer, information entries were created in the log file.
- The entries provide a time and date stamp that can be used to show when a device was connected
- Unfortunately no details such as make or model of device are included in the log entries
- Below are details of the Event ID's found in the log file.

Event ID	Source	Message
1000	WPD-MTPClassDriver	MTP Driver started successfully
1001	WPD-MTPClassDriver	Device will enter the suspend state if idle for 30 seconds
1002	WPD-MTPClassDriver	Device is entering the idle state (idle state:4; Return code: 0x0)
1003	WPD-MTPClassDriver	Device is resuming operation from idle state(idle state: 4; Return code: 0x0)

USB Forensic Tracker has been updated to extract USB artefacts from the above locations.