# USB Storage Device Forensics for Windows 10

**Article** *in* Journal of Forensic Sciences · July 2017

DOI: 10.1111/1556-4029.13596



**3 authors:**

Ayesha Arshad
National University of Sciences and Technology
**1** PUBLICATION **7** CITATIONS
SEE PROFILE

Waseem Iqbal
National University of Sciences and Technology
**62** PUBLICATIONS **497** CITATIONS
SEE PROFILE

Haider Abbas
National University of Sciences and Technology
**166** PUBLICATIONS **3,824** CITATIONS
SEE PROFILE

JOURNAL OF FORENSIC SCIENCES

*J Forensic Sci*, 2017
doi: 10.1111/1556-4029.13596
Available online at: onlinelibrary.wiley.com

**TECHNICAL NOTE**

**DIGITAL & MULTIMEDIA SCIENCES**

*Ayesha Arshad*,[1] *M.Sc.; Waseem Iqbal*,[1] *M.S.; and Haider Abbas*,[2] *Ph.D.*

# USB Storage Device Forensics for Windows 10

**ABSTRACT:** Significantly increased use of USB devices due to their user-friendliness and large storage capacities poses various threats for many users/companies in terms of data theft that becomes easier due to their efficient mobility. Investigations for such data theft activities would require gathering critical digital information capable of recovering digital forensics artifacts like date, time, and device information. This research gathers three sets of registry and logs data: first, before insertion; second, during insertion; and the third, after removal of a USB device. These sets are analyzed to gather evidentiary information from Registry and Windows Event log that helps in tracking a USB device. This research furthers the prior research on earlier versions of Microsoft Windows and compares it with latest Windows 10 system. Comparison of Windows 8 and Windows 10 does not show much difference except for new subkey under USB Key in registry. However, comparison of Windows 7 with latest version indicates significant variances.

**KEYWORDS:** forensic science, USB forensics investigation, USB storage device, Windows 10 forensics, Registry, Microsoft event log

Portable devices are one of the main security threats that any user/business faces today. These devices can be plugged or inserted in any system to perform malicious activities. These activities include stealing of personal and business digital data, transferring confidential data, propagation of malware or viruses, etc (1). Floppy devices, CDs, and DVDs are replaced by USB devices as it can hold a large amount of data and provide plug and play technology. Some advantages of USB devices over traditional storage systems are as follows: high storage capacity; small size; low cost; and portability (2). Under these advantages, USBs are widely used in white-collar crimes, so it is very important to seize all the USB devices during digital forensic investigations (3).

Forensic investigations surrounding USB devices can be of two types. The first one is to search the Windows registry and logs of the traces left behind by suspected USB, whereas the second type is to find traces of all the devices plugged into system.

The timestamp of USB insertion and removal can give a picture of crime under investigation. For example, we can find that how long the USB was plugged into system from USB insertion and removal timestamp. This information can be compared with the transfer time of confidential files between USB and hard disk. If both times are same, we can presume that suspected USB has been used to transfer confidential data.

When USB device is plugged into a computer, Microsoft Windows-based operating systems update Windows registry file and event log files (4,5). With the release of Microsoft Windows 10, it is very important to understand forensic traces left behind by USB devices and highlight difference in traces from previous Microsoft operating system versions. This research will explore Windows 10 for gathering USB artifacts using USB Mass Storage Class (MSC) protocol, Picture Transport Protocol (PTP), and Media Transport Protocol (MTP) for communication.

Microsoft Windows 10 preserves a pool of facts when USB devices are used, which can provide sufficient proof to investigator for a case under investigation. Hence, it is important for an investigator to know the forensic artifacts sources before starting an investigation. In this research, we have made an attempt to look at the Microsoft Windows 10 key registry elements and event logs to discover meaningful evidence for tracing the insertion and removal timestamps of MSC-, MTP-, and PTP-enabled USB devices. No such work on Microsoft Windows 10 is done so far with respect to the three protocols mentioned, and we have tried to give a clear picture of the differences in Microsoft Windows 10 by comparing it with Microsoft Windows 7 and 8.

The article is divided into five sections. Section II of this study describes important concepts and related work of various researchers. Section III explains the methodology used in this research to carry out the analysis. This section also explains the USB protocols and test environment of research work. In section IV, various artifacts left behind by USB devices when plugged-in are discussed along with the insertion and removal timestamps. Section V covers the comparison of forensic artifacts in Microsoft Windows 10 with Microsoft Windows 7 and Windows 8. Section VI concludes the study.

## Technical Background And Prior Work

### *MSC, PTP and MTP*

Relying upon the transfer protocol utilized by a USB device, distinct types of artifacts are left behind, based on their utilization. The USB devices are accessible to computer as a removable media because of the USB device Class transfer protocols.

Mass Storage Class (MSC) protocol defines standard for communication between operating system and USB devices (6). Microsoft has been supporting this protocol since Windows 2000 (7). It is used to transfer data including text files, system files,

[1]National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan.
[2]Florida Institute of Technology (FIT), Melbourne, FL 32901, USA.

Received 6 Feb. 2017; and in revised form 20 April 2017, 29 May 2017; accepted 6 June 2017.

zip files, multimedia files and is also used by removable devices including: External magnetic and optical hard drives; Flash memory devices; solid-state devices; flash memory cards; personal digital assistant; mobile phones; and digital media players.

Picture Transport Protocol (PTP) was developed by International Imaging Industry Association (I3A). This protocol is used by direct printers, scanners, and other Digital still photography devices (DSPDs) to transfer image files (8).

Media Transport Protocol (MTP) is an extension of Picture Transport Protocol (PTP) (9). This protocol allows transfer of audio and media files from digital media players to the computer. MTP and PTP share the same class code as the data transfer layer used by MTP is the PTP specification (10).

### *Registry Hives*

In Microsoft Windows architecture, the Registry is a hierarchical database of configured values stored in more than one places. Microsoft provides an overview of Windows Registry including structure and functioning of the registry (11). The Registry holds significant USB-related information which is very much valuable for forensic investigation. USB build, driver installation timestamp, last insertion, and removal timestamp are some of the artifacts that can be gathered from Windows Registry. The values of building block of registry are organized in hives (12). Important registry hives in Microsoft Windows 10 are as follows:

- HKEY_LOCAL_MACHINE\SYSTEM
- HKEY_LOCAL_MACHINE\SAM
- HKEY_LOCAL_MACHINE\Software
- HKEY_LOCAL_MACHINE\Security
- HKEY_CURRENT_CONFIG
- HKEY_CURRENT_USER
- HKEY_USERS\DEFAULT

USBSTOR, USB, and DeviceClasses located in HKEY_LOCAL_MACHINE\SYSTEM are key registry hives and most crucial in this research.

### *Setupapi.dev Log*

One of the most important log files that identify the timestamp of device first inserted to system is setupapi.dev.

Latest version of Microsoft Windows operating systems including Windows 10 has SetupAPI that supports device installation text log (setupapi.dev.log) (13).

The Plug and Play (PnP) Manager logs information of new devices plugged-in and installed in the setupapi.dev file. This plain text log file contains information including timestamp of driver first installed, and it also stores information of device including serial no, product ID, and vendor ID (13). By default, setupapi.dev log file is located in Windows INF file directory.

### *Event Log*

Microsoft Windows operating system maintains log files related to System and Application events. In digital forensic investigation, the Windows' events log is a critical resource, where digital evidence related to event surrounding the incident can be found. This log file contains information when USB device was inserted and when it was removed from the system. With this information, the investigator can find out how long the suspected device was plugged into system.

### *Prior Work*

Saidi, Ahmad, M. Noor, and Younas have defined ways to investigate illegal activities and cyber-crimes through studying Windows 7 registry (14). Their research focuses on detecting unwanted and unauthorized access by application or user to machine with regard to user's malicious activities. These malicious activities are investigated using AccessData FTK Imager (14).

Talebi, Dehghantanha, and Mahmoud have extensively analyzed Windows 8 Event log. They explained that one of most important parts of any forensic investigation is to examine event logs. The study explains event log format and methods to gather log for digital investigation and incident handling (15).

S. Uerma, Singh, and Laxmi have discussed that USB devices are most commonly used by employees or internal people for credit card frauds. They presented a way to identify the source of these frauds for forensic investigation (16).

Swasti and Arjun presented a method to retrieve USB insertion and removal timestamps from Windows 8 (17). Victor Chileshe Luo has explained the ways to trace USB artifacts from Windows XP (18), similarly Alghafli and other have described how to conduct forensic analysis on the Windows 7 registry (19).

## Methodology

### *Test Environment*

For this research, seven USB devices have been forensically analyzed with respect to insertion and removal timestamp. Following seven devices are selected based on the three protocols mentioned earlier:

- MTP- and PTP-enabled devices
  1) Huawei P8 Lite
  2) Samsung Galaxy Tab 3
  3) Apple iPhone 4s
  4) Nikon D5300
- MSC-enabled devices
  5) Kingston Data Traveler 2.0 Generation 3 USB Flash Drive – 8 GB
  6) Kingston Micro SD Class 10 UHC-1 – SDC10/32 GB
  7) HP USB 3.0 x720w – 32 GB

### *Software Requirements*

Software that is used to collect artifacts from Microsoft Windows 10 registry and event logs is as follows:

- AccessData FTK Imager (Version 3.4.0.5)
- AccessData Registry Viewer (Version 1.8.0.5)
- Regshot (Version 1.9.0)
- Windows Event Viewer
- ExamDiff (Version 1.9)

Forensic Toolkit Imager (FTK Imager) (20) is a forensic tool developed by AccessData that is used to create forensic images of both physical (local hard drives, floppy diskettes, Zip disks, CDs, and DVDs) and logical (RAM) memory, mounting and reading of forensic images, and reporting of findings. FTK Imager allows to take a copy of live Registry files that otherwise is not possible through Windows operating system. Registry Viewer (21) is a forensic tool also developed by AccessData, which is used to view Windows operating system registries. It

gives access to Windows registry protected storage that contains values like password and username. Regshot is an open-source utility that is used to take snapshot of registry and then compare it with second one that is taken after some changes to the system (22). Windows Event Viewer allows viewing and managing of events from multiple log files including System, Application,

```
\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}\##?#SWD#WPDBU
\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}\##?#SWD#WPDBU
\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#USBSTOR#D
\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#USBSTOR#D
\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#V
\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#V
\DeviceClasses\{6ac27878-a6fa-4155-ba85-f98f491d4f33}\##?#SWD#WPDBU
\DeviceClasses\{6ac27878-a6fa-4155-ba85-f98f491d4f33}\##?#SWD#WPDBU
\DeviceClasses\{7f108a28-9833-4b3b-b780-2c6b5fa5c062}\##?#STORAGE#V
\DeviceClasses\{7f108a28-9833-4b3b-b780-2c6b5fa5c062}\##?#STORAGE#V
\DeviceClasses\{7fccc86c-228a-40ad-8a58-f590af7bfdce}\##?#USBSTOR#D
\DeviceClasses\{7fccc86c-228a-40ad-8a58-f590af7bfdce}\##?#USBSTOR#D
\DeviceClasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#USB#VID_0
\DeviceClasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#USB#VID_0
\DeviceClasses\{f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae}\##?#SWD#WPDBU
\DeviceClasses\{f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae}\##?#SWD#WPDBU
```

FIG. 1—*DeviceClasses get from comparing registry files using Regshot.*

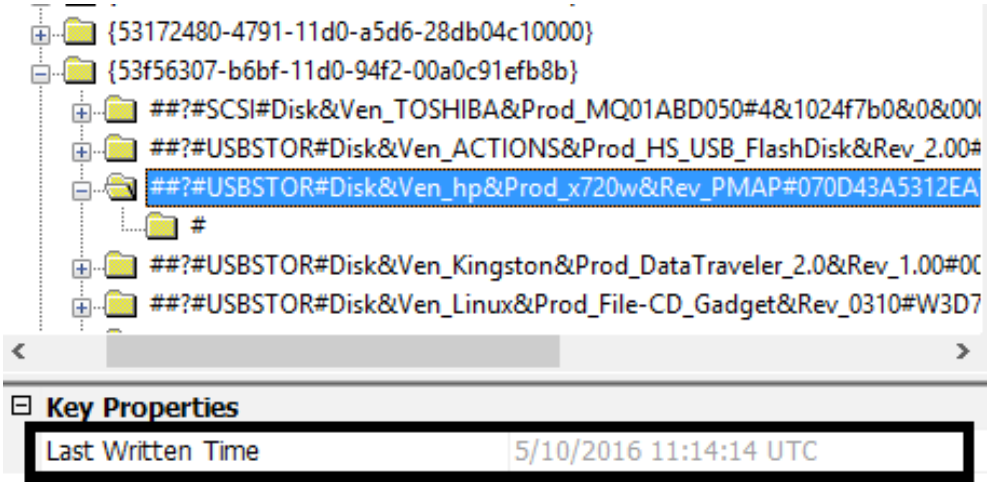


FIG. 2—*First insertion timestamp obtained from "53f56307-b6bf-11d0-94f2-00a0c91efb8b" DeviceClass.*

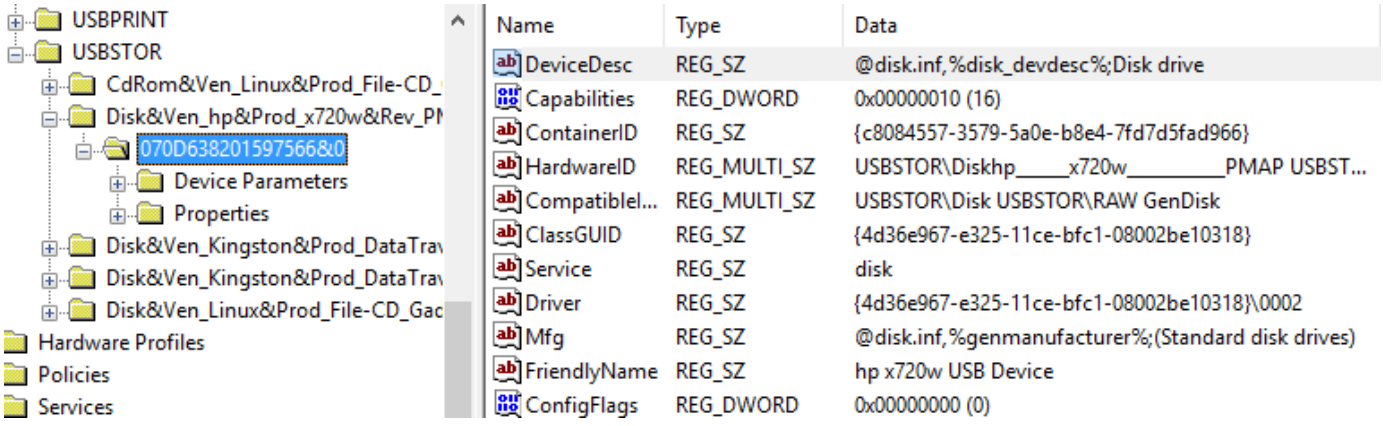


FIG. 3—*Device specification from USBSTOR key.*

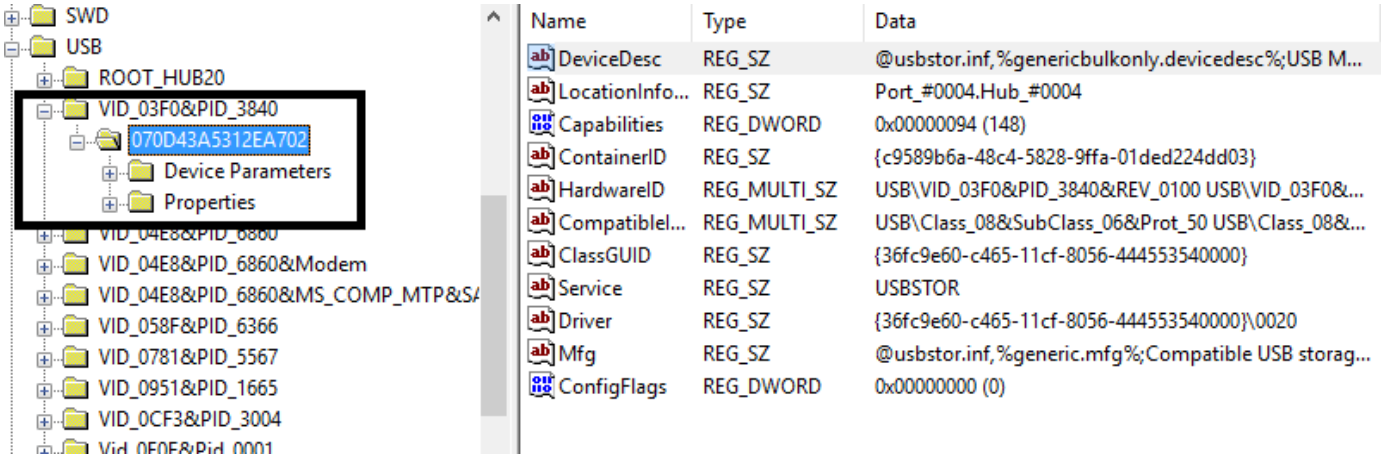


FIG. 4—*Path to USB Key in registry.*

```
>>> [Device Install (Hardware initiated) - SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_hp&Prod_x720w&F
>>> Section start 2016/05/10 16:14:14.784
dvi: {Build Driver List} 16:14:15.421
dvi:      Searching for compatible ID(s):
dvi:           wpdbusenum\fs
dvi:           swd\generic
dvi:      Created Driver Node:
dvi:           HardwareID   - wpdbusenum\fs
dvi:           InfName      - C:\WINDOWS\System32\DriverStore\FileRepository\wpdfs.inf_amc
dvi:           DevDesc      - WPD FileSystem Volume Driver
dvi:           Section      - Basic_Install
dvi:           Rank         - 0x00ff2000
dvi:           Signer Score - INBOX
dvi:           DrvDate      - 06/21/2006
dvi:           Version      - 10.0.10586.0
dvi: {Build Driver List - exit(0x00000000)} 16:14:15.904
```

FIG. 5—*First insertion timestamp in setapi.dev log.*

Security, and Setup (23). ExamDiff is freeware comparison tool that has the ability to visually compare two files (24). Registry files taken from different versions of Windows are compared using this tool.

### *Important Files and Their Location*

Folders and files that are forensically analyzed in this research are as follows:

- Event Logs—C:\Windows\System32\winevt\Logs\
- Registry hives—C:\Windows\System32\config\
- Plug and Play manager logs—C:\Windows\inf\setupapi.dev.log

These files and folders will be analyzed one by one using software tools mentioned in section III (B) for retrieving insertion and removal timestamps of USB devices.

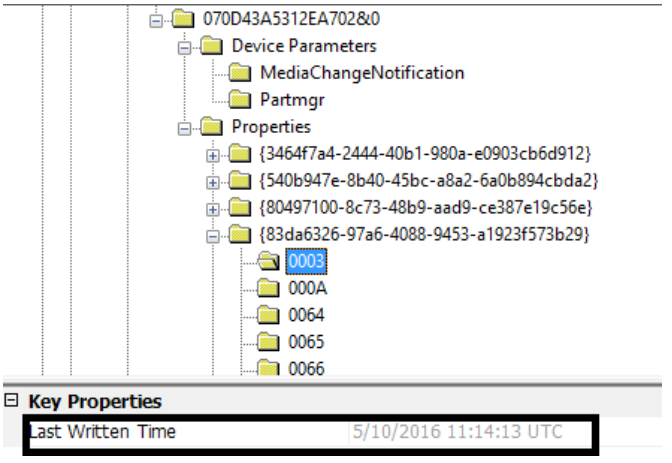


FIG. 6—*First insertion timestamp from USBSTOR's subkeys.*

### *Experimental Setup*

The researchers used a Samsung 300E4V laptop machine running 64-bit Microsoft Windows 10 operating system. Machine has Intel Core i3 processor that runs at 2.50 GHz and 4GB RAM. As three different versions of Windows (7, 8, and 10) are forensically analyzed, the researchers created three virtual machines for each version using VMware Workstation Pro (version 12.1.1). Each virtual machine is configured with maximum 60GB of host computer's physical disk and 1GB of RAM; 64-bit Windows 7 Professional, 64-bit Windows 8 Core, and 64-bit Windows 10 Pro are three Windows versions installed on virtual machines. Regshot and AccessData FTK Imager are installed on each virtual machine to gather registry data, whereas these data are analyzed on host machine where AccessData Registry Viewer and ExamDiff are installed. Event logs are analyzed on each virtual machine using Windows Event Viewer.

TABLE 1—*USBSTOR's subkeys that are used to obtain first insertion timestamp in MSC-enabled USB.*

| Key Location |
|---|
| 1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_[VendorName]&Prod_[ProductName]&Rev_1.00\[SerialNo]\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0003 |
| 2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_[VendorName]&Prod_[ProductName]&Rev_1.00\[SerialNo]\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\000A |
| 3. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_[VendorName]&Prod_[ProductName]&Rev_1.00\[SerialNo]\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0064 |
| 4. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_[VendorName]&Prod_[ProductName]&Rev_1.00\[SerialNo]\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0065 |

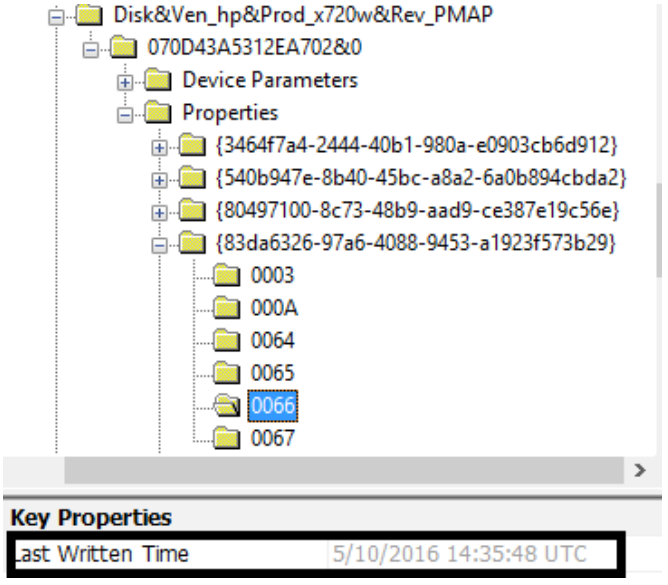


FIG. 7—*Last insertion timestamp from USBSTOR's subkeys.*

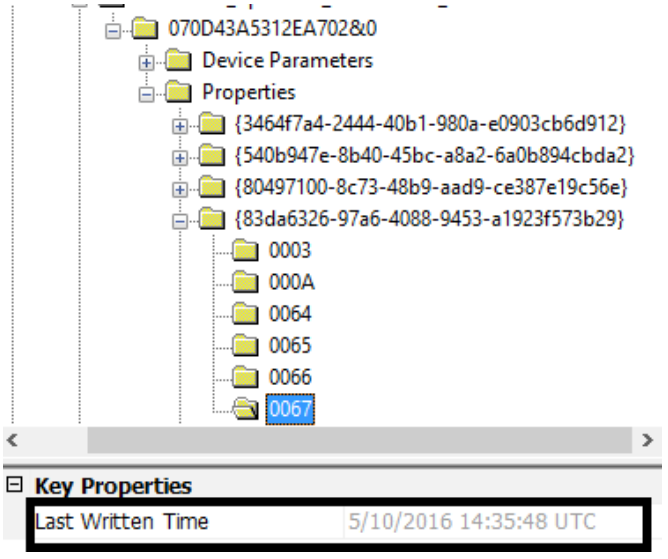


FIG. 8—*Last removal timestamp—USBSTOR.*

## Forensic Artifacts Gathering

*Results Gathered from MSC-enabled USB Devices*

On each virtual machine, the researchers have gathered artifacts at three different stages: before USB insertion, during USB inserted to the system, and after removal of USB from system. Snapshot of virtual machine was taken after installation of required softwares so that it could be possible to roll back to the previous state after gathering artifacts of each USB device. Artifacts gathered from these three stages are later analyzed on host machine. Results gathered from these three states are discussed in next sections.

*DeviceClasses*—When a new Plug and Play device driver is successfully loaded, DeviceClasses subkey is added in Registry. Hence, new keys are created under DeviceClasses when a USB is inserted to a system for the very first time. Use Regshot to compare log of two shots, one before the insertion and other after the insertion of USB. As shown in Fig. 1, the comparison will give details of added keys in DeviceClasses.

DeviceClasses of MSC-enabled devices, which update under key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses, are:

- 10497b1b-ba51-44e5-8318-a65c837b6661
- 53f56307-b6bf-11d0-94f2-00a0c91efb8b
- 53f5630d-b6bf-11d0-94f2-00a0c91efb8b
- 6ac27878-a6fa-4155-baS5-f9Sf491d4f33
- 7f108a28-9833-4b3b-b780-2c6b5fa5c062
- 7fccc86c-228a-40ad-8a58-f590af7bfdce
- a5dcbf10-6530-11d2-901f-00c04fb951ed
- f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae

The format of key generated under these DeviceClasses includes the following: #USBSTOR#Disk&Ven_[VenderName]&Prod_[ProductName]&Rev_PMAP#[SerialNo.]#{[DeviceClassID]}.

Serial number is unique to each USB device. When compared registry log files are created using regshot after first insertion of Microsoft Windows 8 and 10, the researchers have found that DeviceClasses are same in both versions. These DeviceClasses keys are used to find the first insertion timestamp of USB, and it can be viewed in AccessData Registry Viewer as shown in Fig. 2.

Last written time of each DeviceClasses in Registry correlates with the first-time USB was inserted. It shows time in 64-bit FILETIME format.

*Device Specification—USBSTOR Key*—In Access Data Registry Viewer, scroll to key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_[VendorName]&Prod_[ProductName]&Rev_PMAP\[SerialNo]. This key is important to identify the USB make, serial no, product id, container ID, etc.

ContainerID is specifically very important as it provides the identification string that uniquely groups the functional devices (25). Its value will be used to correlate insertion time of USB every time it is plugged into the system in Windows Event Viewer. Fig. 3 illustrates specification of device that can be obtained from USBSTOR key.

*USB Key*—As shown in Fig. 4, path to this key is HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\VID_[VendorID]&PID_[ProductID]\[SerialNo].

Last written time of ..\..\[SerialNo] correlates with last time USB inserted to the Windows 10 similar to Windows 8.

In Windows 10, a new key is added USB\VID_[VendorID] &PID_[ProductID]\[SerialNo]\ Device Parameters\e5b3b5ac-9725-4f78-963f-03dfb1d828c7.

*Setupapi.dev Log*—When USB device is first plugged into the system, PnP Manager has installed the driver of USB and created event entry in setupapi.dev log file. Fig. 5 shows the driver installation timestamp. The timestamp shown in Fig. 5 is local time of system when USB was first inserted and driver of USB

TABLE 2—*Timestamps from Windows Event Viewer for MSC-enabled devices.*

| Event ID | Path | Query | Importance |
|---|---|---|---|
| 20001, 20003 | System\Microsoft-Windows-UserPnp\ | *[System[(EventID='20001/20003')]] | First insertion timestamp. It has identification feature of device as shown in Fig. 9. |
| 10000 | System\Microsoft-Windows-DriverFrameworks-UserMode | *[System[(EventID='10000')]] | First insertion timestamp. It has identification feature of device as shown in Fig. 10. |
| 10100 | System\Microsoft-Windows-DriverFrameworks-UserMode | *[System[(EventID='10100')]] | Event Id 10100 holds the log of installation or update of device driver. First insertion timestamp can be obtained from this event. It does not have identification feature of device. |
| 112 | Microsoft/Windows/DeviceSetupManager/Admin | *[System[(EventID='112')]] and *[EventData[(Data='{y*}')]]. Here y* is ContainerID of device. | Timestamp of every time USB inserted into system. It has no device specification information. To correlate this event with device, ContainerID found from USBSTOR key is used. It is illustrated in Fig. 11. |

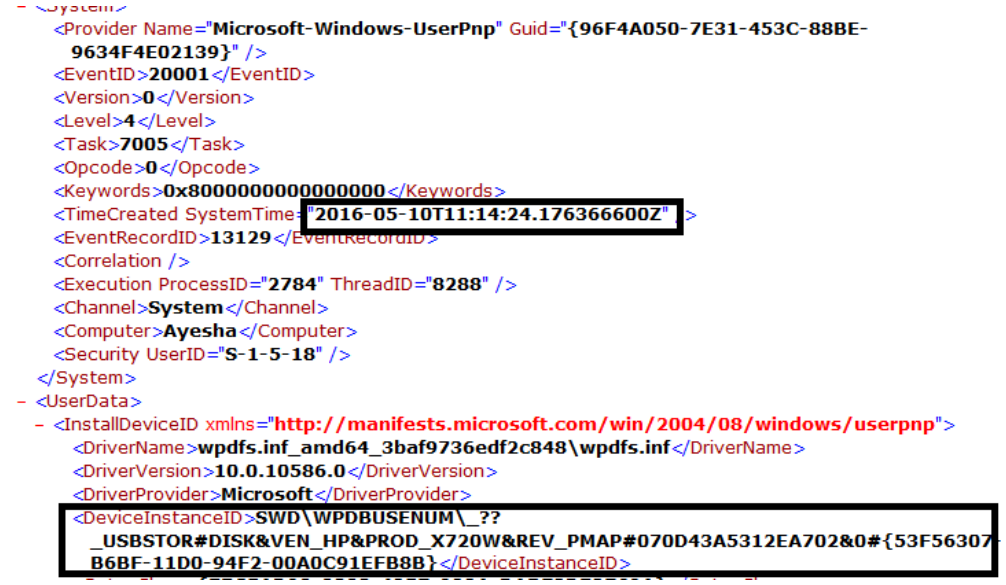


FIG. 9—*First insertion timestamp obtained from Windows Event Viewer - Event ID: 20001.*

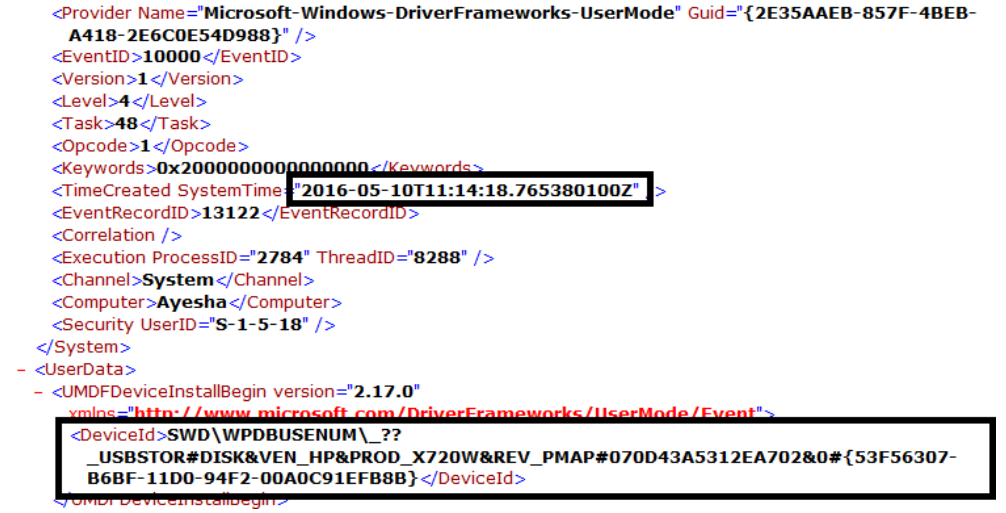


FIG. 10—*First insertion timestamp obtained from Windows Event Viewer - Event ID: 10000.*

was installed. The method of finding the timestamp of first insertion is similar in Windows 8.

*First Insertion Timestamp from USBSTOR Key*—Fig. 6 shows that four subkeys are available in Windows 10 that give the first insertion timestamp in 64-bit FILETIME format. These subkeys are also available in Windows 8. List of these subkeys are presented in Table 1.

*Last Insertion Timestamp from USBSTOR Key*—As shown in Fig. 7, the subkey that is used to identify the last insertion timestamp in Windows 10, like Windows 8, is as follows:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_[VendorName]&Prod_[ProductName]&Rev_1.00\[SerialNo]\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0066.

*Last Removal Timestamp from USBSTOR Key*—As shown in Fig. 8, the subkey that is used to identify the last removal timestamp in Windows 10, like Windows 8, is as follows:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_[VendorName]&Prod_[ProductName]&Rev_1.00\[SerialNo]\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0067.

*First Insertion Time from Software Hive*—In software hive, following registry key is used to find first insertion time in Windows 10, which is similar in Windows 8: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Portable Devices\Devices\SWD#WPDBUSENUM#_??_USBSTOR#DISK&VEN_[VenderName]&PROD_[ProductName]&REV_PMAP#[SerialNo]#{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}.

*Timestamps from Windows Event Viewer*—When we insert or remove an MSC-enabled USB, a number of events are logged in Windows. These events are similar in both Windows 8 and Windows 10 and can be viewed using Windows's Event Viewer application. Events which are logged are presented in Table 2 and also shown in Figs 9, 10, and 11.

### *Results Gathered From MTP- and PTP-enabled USB Devices*

*DeviceClasses*—By comparing Regshot captures (Fig. 12), the researchers have gathered that MTP- and PTP-enabled USB devices use following device Classes:

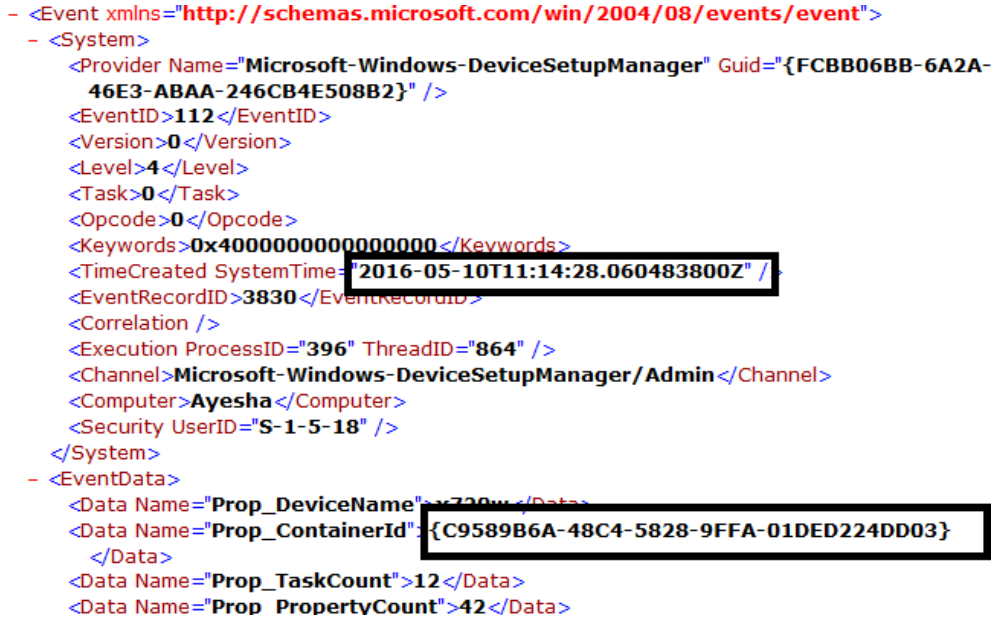


FIG. 11—*Insertion timestamp obtained from Windows Event Viewer - Event ID: 112.*

```
DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}\##?#USB#
DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}\##?#USB#
DeviceClasses\{6ac27878-a6fa-4155-ba85-f98f491d4f33}\##?#USB#
DeviceClasses\{6ac27878-a6fa-4155-ba85-f98f491d4f33}\##?#USB#
DeviceClasses\{6bdd1fc6-810f-11d0-bec7-08002be2092f}\##?#USB#
DeviceClasses\{6bdd1fc6-810f-11d0-bec7-08002be2092f}\##?#USB#
DeviceClasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#USB#
DeviceClasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\##?#USB#
DeviceClasses\{f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae}\##?#USB#
DeviceClasses\{f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae}\##?#USB#
```

FIG. 12—*DeviceClasses of MTP- and PTP-enabled devices obtained from Regshot's compare log file.*

- 10497b1b-ba51-44e5-8318-a65c837b6661
- 6ac27878-a6fa-4155-ba85-f98f491d4f33
- 6bdd1fc6-810f-11d0-bec7-08002be2092f
- a5dcbf10-6530-11d2-901f-00c04fb951ed
- f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae

The format of keys generated under these DeviceClasses is as follows:

##?#USB#VID_[VendorId]&PID_[ProductID]#[DeviceSerialNo] #{[DeviceClassesID]}.

Last written time of these keys correlates with the first-time MTP- and PTP-enabled device is inserted to system.

When compared registry log files were created using regshot after the first insertion of USB device on both Windows 8, we found that DeviceClasses are same in both versions.

*Device Specification—USB Key*—Device specifications of MTP- and PTP-enabled devices (shown in Fig. 13) are found under following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\VID_[VendorID]&PID_[ProductID].

In Windows 10, a new key is added USB\VID_[VendorID]&PID_[ProductID]\[SerialNo]\ Device Parameters\e5b3b5ac-9725-4f78-963f-03dfb1d828c7.

Last written time of ..\USB\VID_[VendorID]&PID_[ProductID] correlates with first-time USB was inserted to the Windows 10 similar to Windows 8.

Last written time of ..\USB\VID_[VendorID]&PID_[ProductID]\[SerialNo] correlates with timestamp of last insertion the Windows 10 similar to Windows 8.

*First-Time Insertion Date and Time—setupapi.dev*—Like MSC-enabled device, first insertion timestamp can also be found from setupapi.dev file (Fig. 14). This way of finding first insertion timestamp is common to both Windows 8 and Windows 10.

*First Insertion Timestamp from USB Key*—The subkeys shown in Table 3 are available in Windows 10, just like Windows 8, that gives the first insertion timestamp in 64bit FILETIME format:

*Last Insertion Timestamp from USB Key*—The following subkeys are available in Windows 10, just like Windows 8, that gives the last insertion timestamp in 64-bit FILETIME format:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\VID_[VendorID]&PID_[ProductID]\[SerialNo]\Properties\{83da6326-97a6-4088-9453 a1923f573b29}\0066.

*Last Removal Timestamp from USB Key*—The following subkeys are available in Windows 10, just like Windows 8, that gives the last removal timestamp in 64-bit FILETIME format:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\VID_[VendorID]&PID_[ProductID]\[SerialNo]\Properties\{83da6326-97a6-4088-9453 a1923f573b29}\0067.

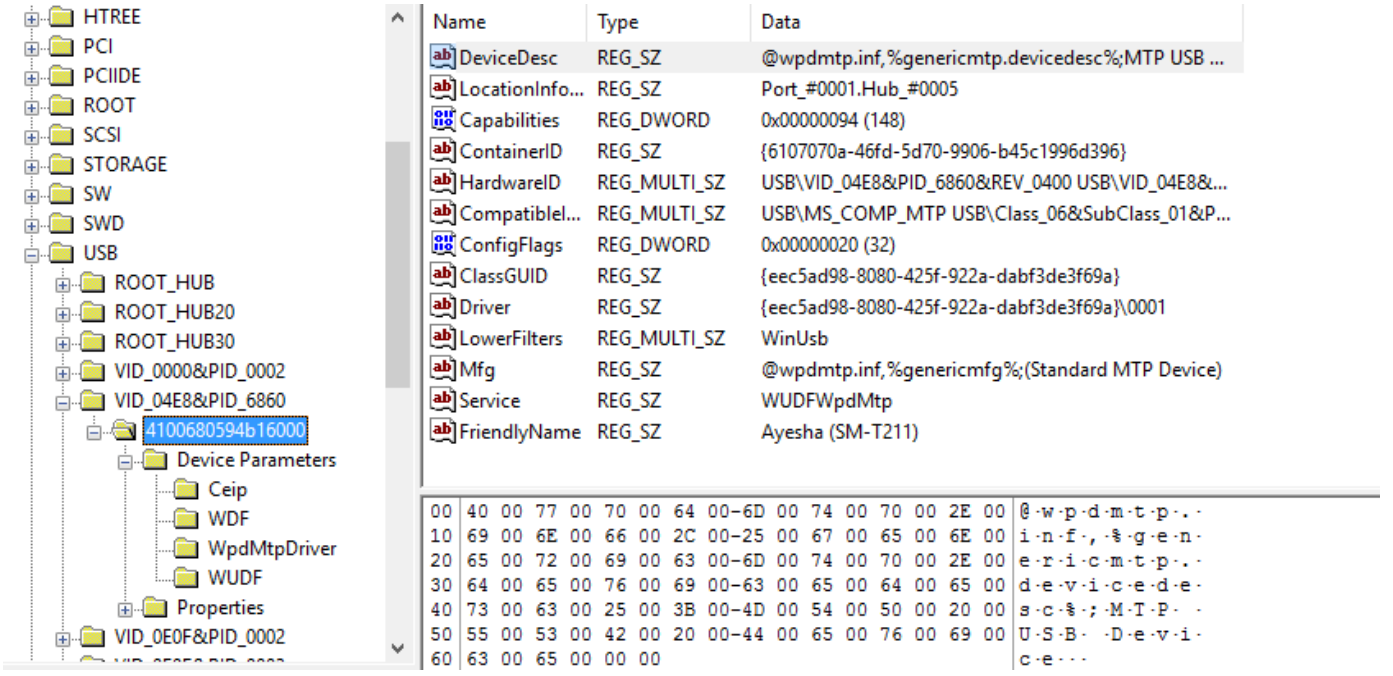


FIG. 13—*Device specifications of MTP- and PTP-enabled devices obtained from USB Key.*

```
[Device Install (Hardware initiated) - USB\VID_04E8&PID_6860\4100680594b16000]
Section start 2016/04/24 10:56:35.471
dvi: {Build Driver List} 10:56:36.377
dvi:      Searching for hardware ID(s):
dvi:           usb\vid_04e8&pid_6860&rev_0400
dvi:           usb\vid_04e8&pid_6860
```

FIG. 14—*First insertion time of MTP- and PTP-enabled device in setupapi.dev file.*

*Timestamps from Windows Event Viewer*—Logs of number of activities were generated when we insert or remove MTP- and PTP-enabled devices. All these activities are similar in both Windows 10 and Windows 8. Table 4 presents event id, path, query to get event id, and importance of these events in getting timestamp from Windows Event Viewer for MTP- and PTP-enabled devices. Figs 15 and 16 also show log entry of event 20003 and 24576, respectively, in Windows Event Viewer.

Events 24576, 24577, 24578, 1000, 1001, 1002, and 1003 are unique to MTP- and PTP-enabled devices. Other events are common to MSC, MTP, and PTP devices.

TABLE 3—*USBSTOR subkeys to find the first insertion timestamp from MTP- and PTP-enabled devices.*

| Key Location |
|---|
| 1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum \USBSTOR\VID_[VendorID]&PID_[ProductID]\[SerialNo]\Properties \{83da6326-97a6-4088-9453-a1923f573b29}\0003 |
| 2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum \USBSTOR\VID_[VendorID]&PID_[ProductID]\[SerialNo]\Properties \{83da6326-97a6-4088-9453-a1923f573b29}\0007 |
| 3. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum \USBSTOR\VID_[VendorID]&PID_[ProductID]\[SerialNo]\Properties \{83da6326-97a6-4088-9453-a1923f573b29}\0008 |
| 4. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum \USBSTOR\VID_[VendorID]&PID_[ProductID]\[SerialNo]\Properties \{83da6326-97a6-4088-9453-a1923f573b29}\0009 |
| 5. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum \USBSTOR\VID_[VendorID]&PID_[ProductID]\[SerialNo]\Properties \{83da6326-97a6-4088-9453-a1923f573b29}\000A |
| 6 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum \USBSTOR\VID_[VendorID]&PID_[ProductID]\[SerialNo]\Properties \{83da6326-97a6-4088-9453-a1923f573b29}\0064 |
| 7. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum \USBSTOR\VID_[VendorID]&PID_[ProductID]\[SerialNo]\Properties \{83da6326-97a6-4088-9453-a1923f573b29}\0065 |

## Analysis and the Comparison of the Results with Other Operating Systems

This section will give the comparison of Microsoft Windows 10 with previous OS versions (Microsoft Windows 7 and 8) for MSC-, MTP-, and PTP-enabled USB devices. It has been noticed that the difference between Windows 8 and Windows 10 are trivial and minimal, but by comparing Windows 7 and Windows 10, many differences have been noted. This comparison will help the investigator to determine whether there are significant differences that can impact the process of investigation.

### *Comparison of Previous OS Versions—MSC Devices*

Table 5 presents the comparison between Windows 7, Windows 8, and Windows 10 for MSC-enabled USB devices. These differences will support investigator in collecting USB artifacts from systems running different flavors of Windows.

By comparing artifacts left behind by MSC-enabled devices on Windows 8 and Windows 10, it has been discovered that finding insertion timestamp from DeviceClasses, USBSTOR, and Software Hive is same. In Windows 10, a new subkey under USB Key is added that also correlates with first insertion timestamp. Determining the last removal and last insertion timestamp is similar in both Windows 8 and Windows 10. Many significant differences have been seen when Windows 7 is compared with Windows 8 and Windows 10. New DeviceClasses are added and similarly removed in Windows 8 and 10. Subkeys "000A," "0066," and "0067" under USBSTOR key are not present in Windows 7. The investigators who have experienced finding USB artifacts on Windows 7 and Windows 8 can easily trace the difference in finding artifacts from Windows 10 using above table.

### *Comparison of Previous OS Versions—MTP and PTP Devices*

Table 6 presents the comparison of artifacts collected using the environment of Windows 7, Windows 8, and Windows 10

TABLE 4—*Timestamps from Windows Event Viewer for MTP- and PTP-enabled devices.*

| Event ID | Path | Query | Importance |
|---|---|---|---|
| 20001, 20003 | System\Microsoft-Windows-UserPnp\ | *[System[(EventID='**EventId**')]] and *[UserData[InstallDeviceID[(Device InstanceID='USB\VID_**VendorID**& PID_**ProductID\SericalNo**')]]]. | First insertion timestamp. It has identification feature of device as shown in Fig. 15. |
| 24576, 24577, 24578 | System\Microsoft-Windows-WPDClassInstaller\ | *[System[(EventID='**EventID**)]] and *[EventData[(Data='USB\VID_**VendorID** &PID_ **ProductID** &REV_0400')]] | First insertion timestamp. It has identification feature of device as shown in Fig. 16. |
| 10000 | System\Microsoft-Windows-DriverFrameworks-UserMode | *[UserData[UMDFDeviceInstallBegin [(DeviceId ='USB\VID_**VendorId**& PID_**ProductId\SerialNo**)]]]. | Event Id 10000 holds the log of installation or update of device driver. First insertion timestamp can be obtained from this event. It has identification feature of device. |
| 10100 | System\Microsoft-Windows-DriverFrameworks-UserMode | *[System[(EventID='10100')]] | Event Id 10100 holds the log of installation or update of device driver. First insertion timestamp can be obtained from this event. It does not have identification feature of device. |
| 1000, 1001, 1003 | Microsoft\Windows\ WPD-MTPClassDriver\Operational | | Last insertion timestamp of MTP- and PTP-enabled USB devices. It does not have identification feature of device. To chain events, we need to link Execution ProcessID and ThreadID. |
| 1002 | Microsoft\Windows\ WPD-MTPClassDriver\Operational | | Last removal timestamp of MTP- and PTP-enabled USB devices. It does not have identification feature of device. To chain events, we need to link Execution ProcessID and ThreadID. |

operating systems. This is evident from the data presented in this table that many significant artifacts and their keys or subkeys differ at some points that might affect/change the investigation process.

Like MSC-enabled devices, comparison of Windows 8 and Windows 10 for MTP- and PTP-enabled devices does not show much difference except for new subkey under USB Key. However, comparison of Windows 7 with the latest version indicates significant differences. DeviceClasses "EEC5AD98-8080-425f-922A-DABF3DE3F69A" has been removed from Windows 8 and Windows 10. First insertion timestamp from USB Key can only be found through "006A" and "0065" subkeys in Windows 7. Moreover, subkeys "0066" and "0067" under USB Key that correlates with last insertion and last removal timestamp, respectively, are not present in Windows 7.

## Conclusion

Registry and Windows Event Viewer both are important from USB forensic analysis point of view in Windows 10. The research presented in this article has focused on retrieving digital artifacts left behind by MSC-, PTP-, and MTP-enabled devices on a suspected system running Windows 10. In section IV, it is observed that finding first insertion timestamp of any USB device is quite easy. First insertion timestamp can also be tracked from DeviceClassses in registry. In addition to first insertion timestamp, USB specifications can also be found in registry.

USB insertion and removal timestamp can be tracked from Microsoft\Windows\WPD-MTPClassDriver\Operational events in Windows Event Viewer. As specification detail is missing in

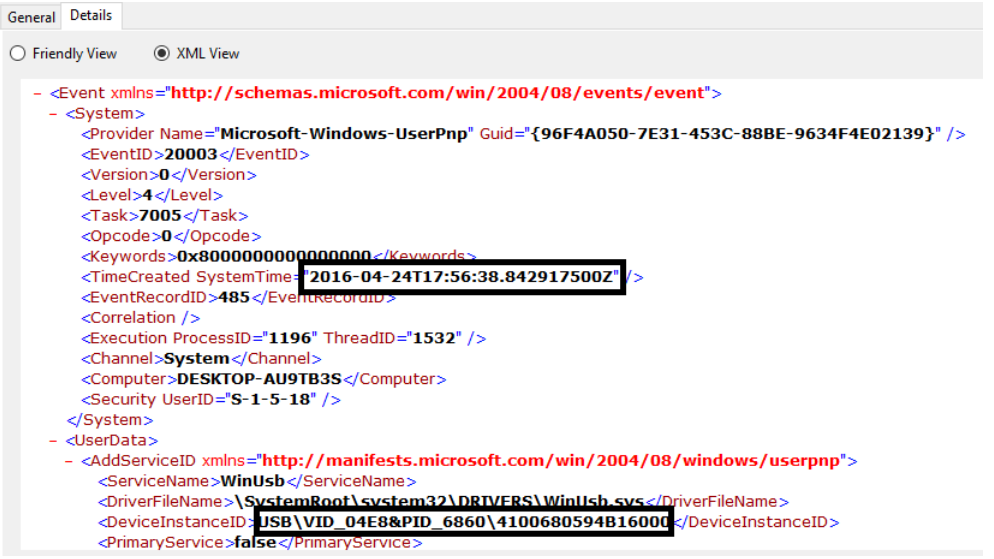


FIG. 15—*Insertion timestamp of MTP- and PTP-enabled USB devices—Event ID: 20003.*

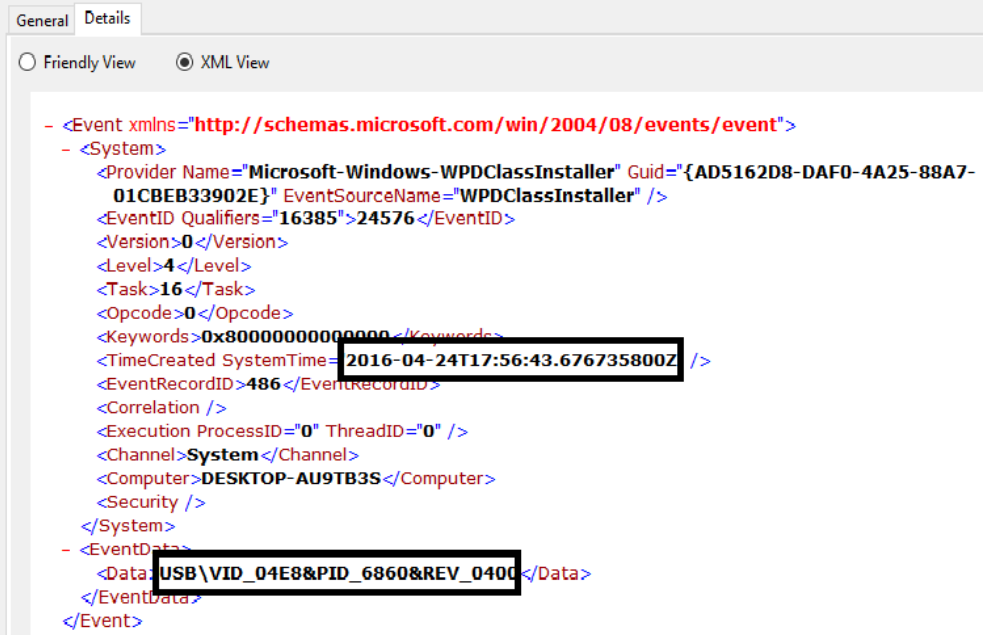


FIG. 16—*Insertion timestamp of MTP- and PTP-enabled USB devices—Event ID: 24576.*

TABLE 5—*MSC devices—comparison of artifacts in different operating systems.*

| | Key/Subkey | Win 7 | Win 8 | Win 10 |
|---|---|---|---|---|
| First insertion time from DeviceClasses key in System Hive | 10497b1b-ba51-44e5-8318-a65c837b6661 | ✓ | ✓ | ✓ |
| | 53f56307-b6bf-11d0-94f2-00a0c91efb8b | ✓ | ✓ | ✓ |
| | 53f5630d-b6bf-11d0-94f2-00a0c91efb8b | ✓ | ✓ | ✓ |
| | 65a9a6cf-64 cd-480b-843e-32c86e1ba19f | ✓ | | |
| | 6ac27878-a6fa-4155-baS5-f9Sf491d4f33 | ✓ | ✓ | ✓ |
| | 7f108a28-9833-4b3b-b780-2c6b5fa5c062 | | ✓ | ✓ |
| | 7fccc86c-228a-40ad-8a58-f590af7bfdce | | ✓ | ✓ |
| | a5dcbf10-6530-11d2-901f-00c04fb951ed | ✓ | ✓ | ✓ |
| | EEC5AD98-8080-425f-922A-DABF3DE3F69A | ✓ | | |
| | f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae | ✓ | ✓ | ✓ |
| First insertion time from System Hive Under USBSTOR Property Key | 0003 | ✓ | ✓ | ✓ |
| | 000A | | ✓ | ✓ |
| | 0064 | ✓ | ✓ | ✓ |
| | 0065 | ✓ | ✓ | ✓ |
| Last insertion time from System Hive Under USBSTOR Property Key | 0066 | | ✓ | ✓ |
| Last removal time from System Hive Under USBSTOR Property Key | 0067 | | ✓ | ✓ |
| First insertion time from System Hive under USB Key | VID_[VendorID]&PID_[ProductID]\[SerialNo]\DeviceParameters \e5b3b5ac-9725-4f78-963f-03dfb1d828c7 | | | ✓ |
| Last insertion time from System Hive under USB Key | VID_[VendorID]&PID_[ProductID]\[SerialNo]\ | ✓ | ✓ | ✓ |
| First insertion time from Software Hive | Microsoft\Windows Portable Devices\Devices \SWD#WPDBUSENUM#_??_ USBSTOR#DISK&VEN_[VenderName] &PROD_[ProductName]&REV_PMAP#[SerialNo]#{53F56307-B6BF-11D0-94F2-00A0C91EFB8B} | ✓ | ✓ | ✓ |

TABLE 6—*MTP and PTP devices—comparison of artifacts in different operating systems.*

| | Key/Subkey | Win 7 | Win 8 | Win 10 |
|---|---|---|---|---|
| First insertion Time from DeviceClasses key in System Hive | 10497b1b-ba51-44e5-8318-a65c837b6661 | ✓ | ✓ | ✓ |
| | 6ac27878-a6fa-4155-baS5-f9Sf491d4f33 | ✓ | ✓ | ✓ |
| | 6bdd1fc6-810f-11d0-bec7-08002be2092f | ✓ | ✓ | ✓ |
| | a5dcbf10-6530-11d2-901f-00c04fb951ed | ✓ | ✓ | ✓ |
| | EEC5AD98-8080-425f-922A-DABF3DE3F69A | ✓ | | |
| | f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae | ✓ | ✓ | ✓ |
| First insertion time from System Hive Under USB Property Key | 0003 | ✓ | ✓ | ✓ |
| | 0007 | | ✓ | ✓ |
| | 0008 | | ✓ | ✓ |
| | 0009 | | ✓ | ✓ |
| | 000A | | ✓ | ✓ |
| | 0064 | ✓ | ✓ | ✓ |
| | 0065 | ✓ | ✓ | ✓ |
| Last insertion time from System Hive Under USB Property Key | 0066 | | ✓ | ✓ |
| Last removal time from System Hive Under USB Property Key | 0067 | | ✓ | ✓ |
| First insertion time from System Hive under USB Key | VID_[VendorID]&PID_[ProductID]\[SerialNo]\DeviceParameters \e5b3b5ac-9725-4f78-963f-03dfb1d828c7 | | | ✓ |
| Last insertion time from System Hive under USB Key | VID_[VendorID]&PID_[ProductID]\[SerialNo]\ | ✓ | ✓ | ✓ |

these events, it will be difficult for a forensic investigator to correlate these events with specific events.

Comparison of footprints from registry of Microsoft Windows 7 with Microsoft Windows 8 and 10 to find insertion and removal timestamp of MSC-, MTP-, and PTP-enabled devices helps in collecting artifacts from environment where different versions of Windows are used.

As the main focus of this research is to find the timestamp of MTP-, PTP-, and MSC-enabled devices, future work may be extended to carry forward this research for analysis of complete history of plugged USB devices. Also, the results of this research can be validated with other open-source tools like yet another registry utility (YURU), USB Device Forensics, USB Historian, and RegRipper.

## References


1. Walters P. The risks of using portable devices; https://www.us-cert.gov/sites/default/files/publications/RisksOfPortableDevices.pdf (accessed January 14, 2017).
2. Lee KG, Lee HW, Park CW, Bang JW, Kim KY, Lee S. USBPassOn: secure USB thumb drive forensic toolkit. Proceedings of the Second International Conference on Future Generation Communication and Networking; 2008 Dec 13-15; Hainan Island, China. Piscataway, NJ: IEEE, 2008.
3. Chang KS, Yoo MK, Kim KN, Park JH. Approach to USB memory recovery – physical repair and logical restoration. J Digital Forensics (Digital Forensics Society of Korea) 2007;11:79–103.
4. Thomas P, Morris A. An investigation into the development of an anti-forensic tool to obscure USB flash drive device information on a Windows XP platform. Proceedings of the Third International Annual Workshop on Digital Forensics and Incident Analysis; 2008 Oct 9; Malaga, Spain. Piscataway, NJ: IEEE, 2008.

5. USB history viewing; http://www.forensicswiki.org/wiki/USB_History_Viewing (accessed January 18, 2017).
6. USB mass storage class specification overview version 1.4; http://www.usb.org/developers/docs/devclass_docs/Mass_Storage_Specification_Overview_v1.4_2-19-2010.pdf (accessed January 14, 2017).
7. USB storage – FAQ for driver and hardware developers; https://msdn.microsoft.com/en-us/library/windows/hardware/dn653578(v=vs.85).aspx (accessed January 14, 2017).
8. ISO 15740:2013. Photography – Electronic Still Picture Imaging – Picture Transfer Protocol (PTP) for Digital Still Photography Devices. Geneva, Switzerland: International Organization for Standardization, 2013.
9. MTPv1_1.zip; http://www.usb.org/developers/docs/devclass_docs/MTPv1_1.zip (accessed January 14, 2017).
10. Kolokowsky S, Davis T. Introduction to MTP: Media Transfer Protocol. San Jose, CA: Cypress Semiconductor Corp, 2008.
11. Registry; https://msdn.microsoft.com/en-us/library/windows/desktop/ms724871(v=vs.85).aspx (accessed January 14, 2017).
12. Registry hives; https://msdn.microsoft.com/en-us/library/windows/desktop/ms724877(v=vs.85).aspx (accessed January 14, 2017).
13. SetupAPI text logs; https://msdn.microsoft.com/en-us/windows/hardware/drivers/install/setupapi-text-logs (accessed January 14, 2017).
14. Saidi RM, Ahmad SA, Noor NM, Younas R. Window registry analysis for forensic investigation. Proceedings of the 2013 International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE); 2013 May 9-11; Konya, Turkey. Piscataway, NJ: IEEE, 2013.
15. Talebi J, Dehghantanha A, Mahmoud R. Introduction and analysis of Window 8 event log for forensic purposes. In: Garain U, Shafait F, editors. Computational Forensics. Lecture Notes in Computer Science. Vol. 8915. Cham, Switzerland: Springer International Publishing, 2015;145–62.
16. Verma S, Singh A, Singh D, Laxmi V. Computer forensic IT audit and credit card fraud investigation for USB devices. Proceedings of the 2014 International Conference on Computing for Sustainable Global Development; 2014 March 5-7; New Delhi, India. Piscataway, NJ: IEEE 2014.
17. Deb SB, Chetry A. USB device forensics: insertion and removal timestamps of USB devices in Windows 8. Proceedings of the 2015 International Symposium on Advanced Computing and Communication; 2015 Sept 14-15; Silchar, India. Piscataway, NJ: IEEE, 2015.
18. Luo VC. Tracing USB device artefacts on Windows XP operating system for forensic purpose. In: Valli C, Woodward A, editors. Proceedings of the 5th Australian Digital Forensics Conference; 2007 Dec 3; Perth, Western Australia. Perth, Western Australia: School of Computer and Information Science, Edith Cowan University, 2007.
19. Alghafli KA, Jones A, Martin TA. Forensic analysis of the Windows 7 registry. J Digital Forensics, Secur and Law 2011;5(4):5–30.
20. Mobile Phone Examiner Plus (MPE+) 5.5.3; http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.0.5 (accessed January 9, 2017).
21. Registry viewer 1.8.0.5; http://accessdata.com/product-download/digital-forensics/registry-viewer-1-8-0-5 (accessed January 9, 2017).
22. Regshot; https://sourceforge.net/projects/regshot/ (accessed January 9, 2017).
23. Event viewer; https://technet.microsoft.com/en-us/library/cc766042(v=ws.11).aspx (accessed January 9, 2017).
24. ExamDiff; http://www.prestosoft.com/edp_examdiff.asp (accessed January 9, 2017).
25. Container ID; https://msdn.microsoft.com/en-us/windows/hardware/drivers/install/container-ids (accessed January 14, 2017).

Additional information and reprint requests:
Haider Abbas, Ph.D.
National University of Sciences and Technology (NUST)
Islamabad 44000, Pakistan
E-mail: haidera@kth.se