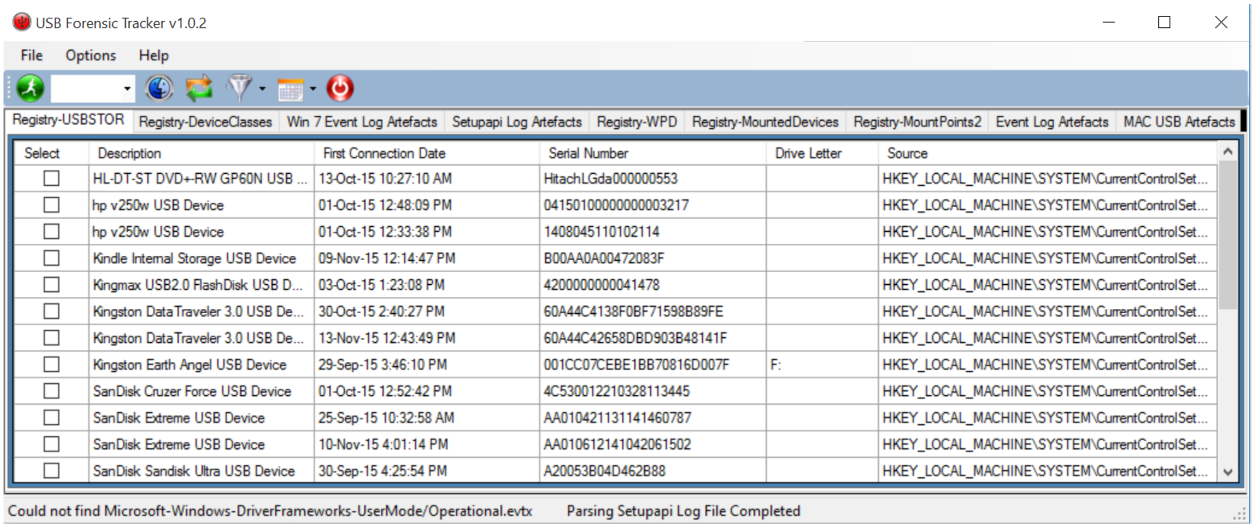
USB Forensic Tracker v1.0.3

Introduction

USB Forensic Tracker (USBFT) is a comprehensive forensic tool that extracts USB device connection artefacts from a range of locations within the live system, from mounted forensic images and from extracted Mac OSX system files. The extracted information from each location is displayed within its own table view. The information can be exported to an Excel file.



Select	Description	First Connection Date	Serial Number	Drive Letter	Source
☐	HL-DT-ST DVD+-RW GP60N USB ...	13-Oct-15 10:27:10 AM	HitachLGda000000553		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	hp v250w USB Device	01-Oct-15 12:48:09 PM	0415010000000003217		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	hp v250w USB Device	01-Oct-15 12:33:38 PM	1408045110102114		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	Kindle Internal Storage USB Device	09-Nov-15 12:14:47 PM	B00AA0A00472083F		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	Kingmax USB2.0 FlashDisk USB D...	03-Oct-15 1:23:08 PM	4200000000041478		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	Kingston DataTraveler 3.0 USB De...	30-Oct-15 2:40:27 PM	60A44C4138F0BF71598B89FE		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	Kingston DataTraveler 3.0 USB De...	13-Nov-15 12:43:49 PM	60A44C42658DBD903B48141F		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	Kingston Earth Angel USB Device	29-Sep-15 3:46:10 PM	001CC07CEBE1BB70816D007F	F:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	SanDisk Cruzer Force USB Device	01-Oct-15 12:52:42 PM	4C530012210328113445		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	SanDisk Extreme USB Device	25-Sep-15 10:32:58 AM	AA010421131141460787		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	SanDisk Extreme USB Device	10-Nov-15 4:01:14 PM	AA010612141042061502		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
☐	SanDisk Sandisk Ultra USB Device	30-Sep-15 4:25:54 PM	A20053B04D462B88		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...

```
Could not find Microsoft-Windows-DriverFrameworks-UserMode/Operational.evtx      Parsing Setupapi Log File Completed
```

USBFT extracts information from the following locations:

Windows

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
- HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses
- HKEY_USERS\SID\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Portable Devices
- Microsoft-Windows-DriverFrameworks-UserMode/Operational Event Log (Windows 7)
- Microsoft-Windows-Storage-ClassPnP/Operational.evtx Event Log (Window 10)
- Microsoft-Windows-WPD-MTPClassDriver/Operational.evtx
- C:\Windows\inf\setupapi.dev.log
- C:\Windows\setupapi.log

Mac OSX (tested on OSX 10.6.8 and 10.10.3)

1) /private/var/log/kernel.log
2) /private/var/log/kernel.log.incrementalnumber.bz2
3) /private/var/log/system.log
4) /private/var/log/system.log.incrementalnumber.gz

Instructions

Window Live System

1) To run USBFT on a live Windows system, open USBFT and press the "Run" button

2) Make sure you run the 64 bit version on a 64 bit machine. If you run the 32 bit version it will not extract all of the USB artefacts.

3) USBFT will automatically extract information from the registry, selected event logs if they are present and the setupapi.log (or setupapi.dev.log). Each table corresponding to extraction location will be populated.

4) Status messages will be displayed at bottom of GUI.

5) By default USBFT will display time stamps in local time. From the "Options => Time Settings" menu, the user can select either local time or UTC.

6) From the "Options => Date Format menu, the user can select how the date stamps will be displayed". Set the format prior to running the tool.

7) The user can filter the results that are displayed by checking the checkboxes and pressing the filter button.

8) After filtering, if you wish to view all results press the reload button.

9) The user has the option to export all records or selected records to Excel spreadsheet. When exporting to Excel each of the table views will be placed into its own work sheet.

Extracting USB artefacts from a mounted forensic image

1) USBFT can analyze either mounted forensic images or additional connected hard drives that contain a Windows OS.

2) Once the forensic image has been mounted, open USBFT and from the drop down list select the drive letter that corresponds to the volume that contains the Windows OS. D:\

3) Once selected USBFT will automatically locate and temporarily load the required registry hives into the registry of the examination machine. The required event logs will also be located and copied to the user temp folder for processing.

4) Once the files have been loaded press the run button to begin the extraction.

5) When you close USBFT the loaded registry files will be automatically unloaded from the registry and all temp files deleted before closing USBFT. If USBFT is interrupted during this process and as a result doesn't cleanly remove all temp registry files, just open and close USBFT again and it will clear the registry.

Extracting USB artefacts from extracted Mac OSX files

1) USBFT can now extract USB artefacts from kernel.log, kernel.log.incrementalnumber.bz2, system.log and system.log.incrementalnumber.gz Mac OSX files.
2) Extract the required files to a folder on the Windows examination machine.
3) Open USBFT and press the MAC Analysis button.
4) Select the folder containing the required files and click OK.
5) When you click OK, the extraction process will begin automatically. Do not press the "Run" button.

A 32bit and 64 bit version of USB Forensic Tracker is included in the download. If you run the 32 bit version on a 64 bit machine, USBFT will not display the results for the Event Log artefacts or for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Portable Devices.

From the "Help" menu the user can check for updates.

Time Stamp Information:

Many of the time stamps are obtained from the last written time stamp of the registry keys.

SOFTWARE\Microsoft\Windows Portable Devices\Devices

Last Written Date is created when pen drive first connected
Last Written Date is not updated each time the pen drive is connected and is assigned the same drive letter as previously assigned
Last Written Date will update when the pen drive is connected and assigned a new drive letter

SYSTEM\CurrentControlSet\Enum\USBSTOR

Last Written Date is created when pen drive first connected
Last Written Date is not updated each time the pen drive is connected

Microsoft-Windows-DriverFrameworks-UserMode/Operational Event Log

Time Date stamps reflects each time the pen drive is connected or disconnected from the system

Microsoft-Windows-Storage-ClassPnP/Operational.evtx Event Log

Time Date stamps reflects each time the pen drive is connected to the system

License

This utility is released as freeware. You are allowed to freely distribute this program via any method, as long as you don't charge anything for this. If you distribute this utility, you must include all files in the distribution package, without any modification!

Icons by Everaldo Coelho from the Crystal project are used; these are released under the LGPL license.

Disclaimer

The software is provided "AS IS" without any warranty, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The author will not be liable for any special, incidental, consequential or indirect damages due to loss of data or any other reason.

Version 1.0.3 November 2015

1) Added additional support for Mac OSX files. USBFT will now also process_kernel.log and kernel.log.incrementalnumber.bz2 files
2) Modified code for USBSTOR section. For devices such as multi card readers that show as multiple drives with different drive letters but the same serial number, USBFT will now correctly display all of the drive letters.
3) Renamed the “Last Connection Date” column in the Device Classes section to “Connection Date”

Version 1.0.2 November 2015

1) Added the ability to extract USB artefacts from mounted forensic images.
2) Added the ability to extract USB artefacts from Mac OSX system files
3) Made changes to code relating to obtaining the last modified date of registry keys
4) Other minor changes made to some of the code to make more robust

Version 1.0.1 September 2015

1) USBFT now parses the Microsoft-Windows-Storage-ClassPnP/Operational.evtx event log (Window 10) and the Microsoft-Windows-WPD-MTPClassDriver/Operational.evtx event log.
   Limited information can be extracted from the Microsoft-Windows-WPD-MTPClassDriver/Operational.evtx event log but it does indicate when a Media Transfer Protocol (MTP) portable device has been connected to the computer.
2) Under the “Options” button added the ability for a user to set the format for the date stamps.
3) Made a slight change to the code so USBFT now displays the correct user SID in the Source column of the Registry-Mountpoints2 table view.