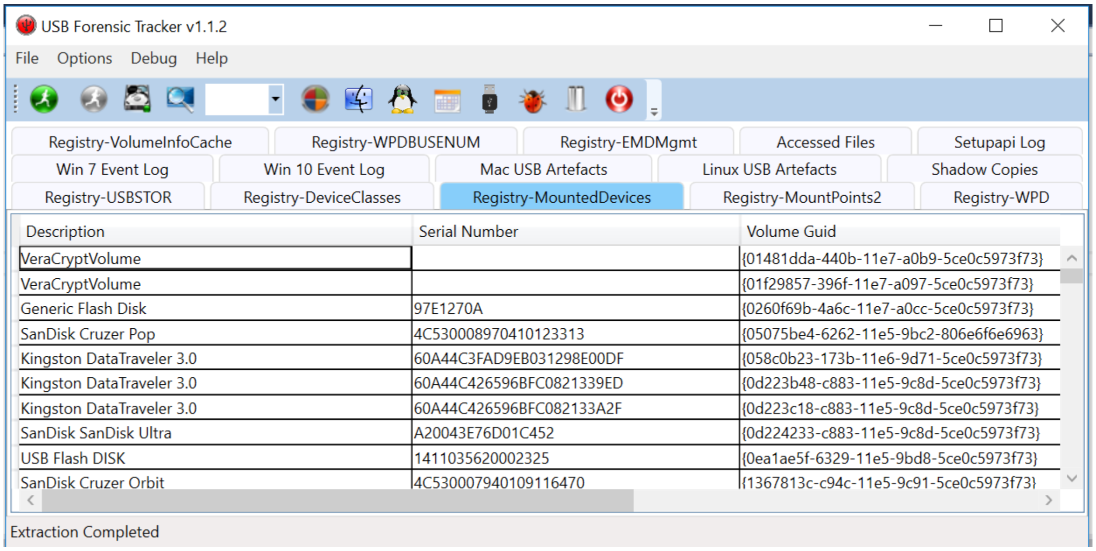
USB Forensic Tracker v1.1.3

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, from extracted Windows system files and from both extracted Mac OSX and Linux system files. The extracted information from each location is displayed within its own table view. The information can be exported to an Excel file.

USBFT now has the ability to do the following:

- Mount forensic images and volume shadow copies.
- Display information about previously mounted TrueCrypt and VeraCrypt volumes.
- Display information about files accessed from USB devices and link the files to specific USB devices.



Description	Serial Number	Volume Guid
VeraCryptVolume		{01481dda-440b-11e7-a0b9-5ce0c5973f73}
VeraCryptVolume		{01f29857-396f-11e7-a097-5ce0c5973f73}
Generic Flash Disk	97E1270A	{0260f69b-4a6c-11e7-a0cc-5ce0c5973f73}
SanDisk Cruzer Pop	4C530008970410123313	{05075be4-6262-11e5-9bc2-806e6f6e6963}
Kingston DataTraveler 3.0	60A44C3FAD9EB031298E00DF	{058c0b23-173b-11e6-9d71-5ce0c5973f73}
Kingston DataTraveler 3.0	60A44C426596BFC0821339ED	{0d223b48-c883-11e5-9c8d-5ce0c5973f73}
Kingston DataTraveler 3.0	60A44C426596BFC082133A2F	{0d223c18-c883-11e5-9c8d-5ce0c5973f73}
SanDisk SanDisk Ultra	A20043E76D01C452	{0d224233-c883-11e5-9c8d-5ce0c5973f73}
USB Flash DISK	1411035620002325	{0ea1ae5f-6329-11e5-9bd8-5ce0c5973f73}
SanDisk Cruzer Orbit	4C530007940109116470	{1367813c-c94c-11e5-9c91-5ce0c5973f73}

Extraction 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_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\SWD\WPDBUSENUM
- 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
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Search\VolumeInfoCache
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\EMDMgmt
- C:\Windows\System32\winevt\Logs\Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx (Windows 7)
- C:\Windows\System32\winevt\Logs\Microsoft-Windows-Storage-ClassPnP/Operational.evtx
- C:\Windows\System32\winevt\Logs\Microsoft-Windows-WPD-MTPClassDriver/Operational.evtx
- C:\Windows\System32\winevt\Logs\Microsoft-Windows-Partition%4Diagnostic.evtx
- C:\Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4Operational.evtx
- C:\Windows\INF\setupapi.dev.log
- C:\Windows\INF\ setupapi.dev.yyyymmdd_hhmmss.log
- C:\Windows\setupapi.log
- “Windows.old” folder
- Volume Shadow Copies
- C:\Users\<user account>\AppData\Roaming\Microsoft\ Windows\ Recent\ <Lnk files>

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

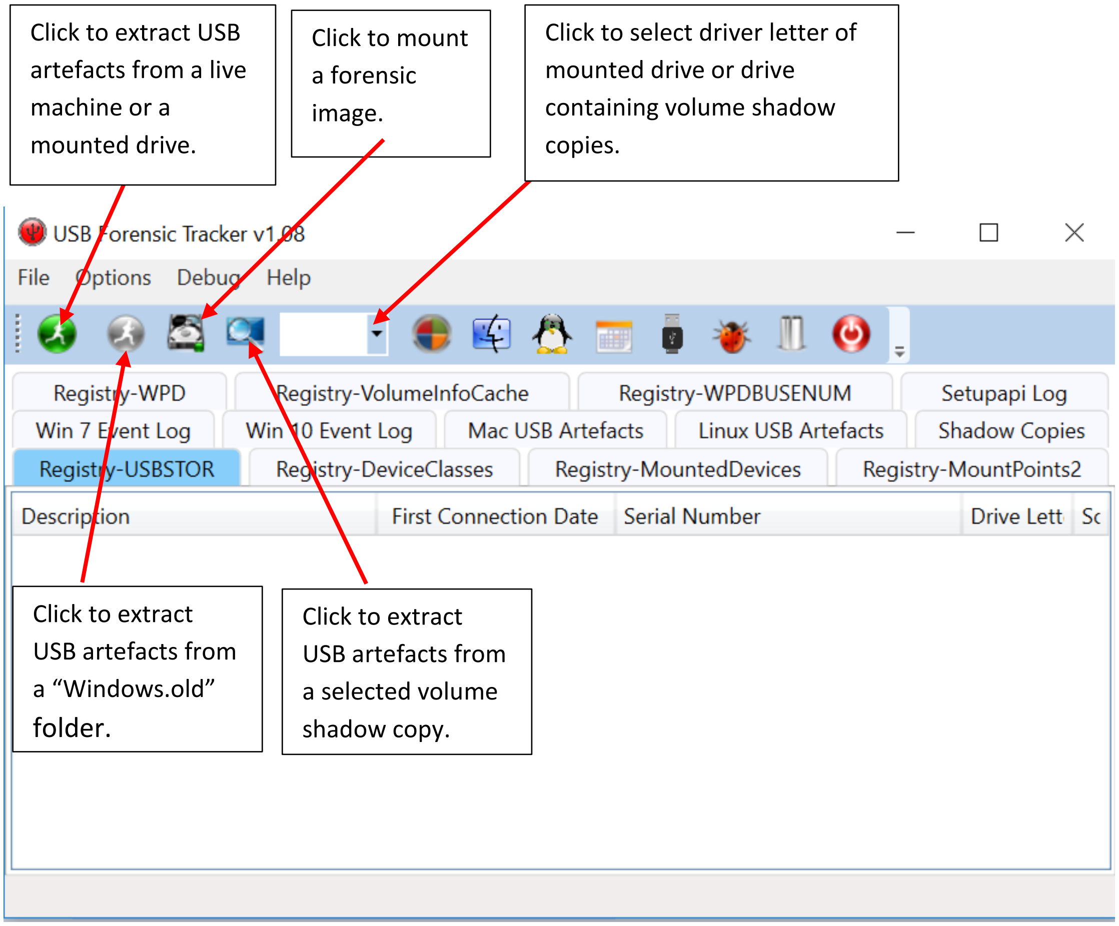
Linux (tested on Ubuntu 17.04)

1) /var/log/syslog

Requirements

USBFT requires Net Framework 4.5 to be installed on the system.

Instructions



Click to extract USB artefacts from a live machine or a mounted drive.

Click to mount a forensic image.

Click to select driver letter of mounted drive or drive containing volume shadow copies.

Click to extract USB artefacts from a "Windows.old" folder.

Click to extract USB artefacts from a selected volume shadow copy.

Extracting USB artefacts from a Windows Live System

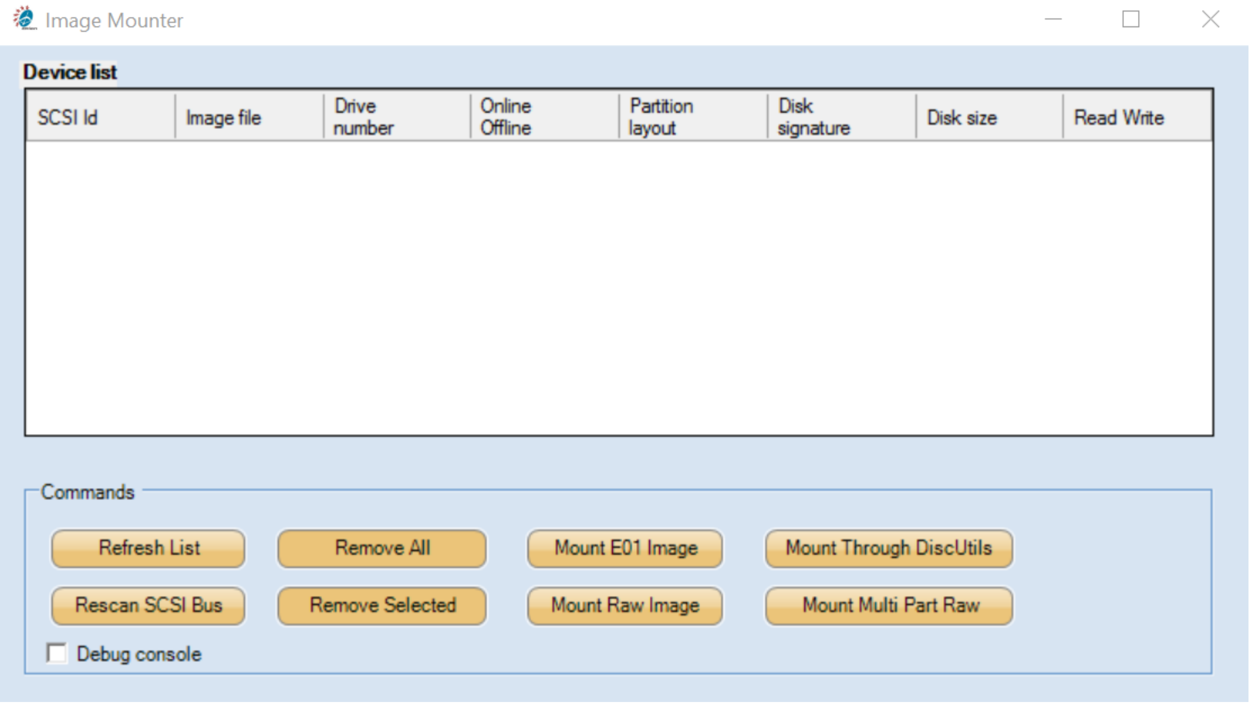
1) To run USBFT on a live Windows system, open USBFT and press the "Run" button
2) Make sure you run the 64 bit version on a 64 bit machine. If you run the 32 bit version it will not extract all of the USB artefacts.
3) USBFT will automatically extract information from the registry, selected event logs if they are present and the setupapi logs). Each table corresponding to the extraction location will be populated.
4) Status messages will be displayed at bottom of the 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. Change the time zone before running USBFT.
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 has the option to export all 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 "Windows.old" folder

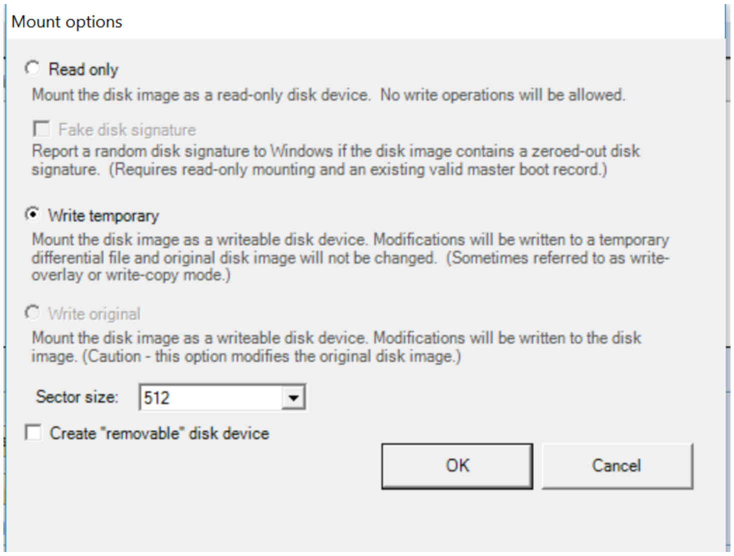
1) USBFT can also extract USB artefacts from the "Windows.old" folder. From the drop down menu select the drive letter of the drive that contains the "Windows.old" folder
2) Press the grey run button to begin the extraction process.
3) Within the "Windows.old" folder USBFT will examine all the same files as for the live system.

Mounting a Forensic Image

1) To mount a forensic image or raw image, press the button.
2) The image mounter will open as shown below:



3) For example to mount an E01 image press the "Mount E01 Image' button and navigate to the location of the image file and select the image file.
4) The following window will open:



Mount options

○ Read only

Mount the disk image as a read-only disk device. No write operations will be allowed.

☐ Fake disk signature

Report a random disk signature to Windows if the disk image contains a zeroed-out disk signature. (Requires read-only mounting and an existing valid master boot record.)

● Write temporary

Mount the disk image as a writeable disk device. Modifications will be written to a temporary differential file and original disk image will not be changed. (Sometimes referred to as write-overlay or write-copy mode.)

○ Write original

Mount the disk image as a writeable disk device. Modifications will be written to the disk image. (Caution - this option modifies the original disk image.)

Sector size: 512

☐ Create "removable" disk device

5) Select the “Write Temporary” option and click “OK”.

6) Once the image is mounted identify which mounted volume contains the operating system.

7) You can then use USBFT to process the mounted volume or to process selected volume shadow copies.

8) To unmount the image file, press either the “Remove All” or “Remove Selected” button.

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) The forensic image must be mounted as **WRITABLE** otherwise the registry hives will not load.

3) 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:\

4) Once selected USBFT will automatically locate and temporarily load the required registry hives into the registry of the examination machine. Once the files have been loaded press the green run button to begin the extraction.

5) When you close USBFT the loaded registry files will be automatically unloaded from the registry 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.

6) USBFT will automatically locate all the required files within the mounted image and extract the artefacts the same as for a live system.

Extracting USB artefacts from a mounted Volume Shadow Copy

1) USBFT can also extract USB artefacts from mounted volume shadow copies. From the drop down menu select the drive letter of the drive that contains volume shadow copies.
2) As soon as you select a drive letter USBFT will automatically extract details of any volume shadow copies located on the volume. The information will be stored under the "Shadow Copies" tab.
3) From the "Shadow Copies" tab highlight the volume shadow copy you wish to process.
4) Press the Shadow Copy button. USBFT will automatically begin extracting the USB artefacts.

Extracting USB artefacts from extracted Windows files

- USBFT now has the option to process Window files that have been saved to a custom folder. The registry files and Window logs can be saved to the root of the folder. However to process all the NTUser.dat files for each user accounts requires the NTUser.dat files to be saved in a specific folder structure as shown below:
- **Custom Folder**
  - Registry File – Software
  - Registry File – System
  - 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
  - setupapi.dev.log
  - setupapi.upgrade.log
  - **Users** (directory)
    - **UserProfile1** (directory)
      - NTUser.dat
      - Lnk Files
    - **UserProfile2** (directory)
      - NTUser.dat
      - Lnk Files
    - **UserProfile3 (**directory)
      - NTUser.dat
      - Lnk Files

The name of the "UserProfile" folder should have the same name as the sub folders in the Users folder on the system under examination.

In order to identify details of files accessed from USB devices, USBFT will first extract Volume Serial Numbers from the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\EMDMgmt and then search through the Lnk files located under each user profile for the VSN. USBFT will search through Lnk files in the following location by default. C:\Users\<user account>\AppData\Roaming\Microsoft\ Windows\ Recent\ <Lnk files>. When extracting USB artefacts from extracted Windows files in a custom folder the Lnk files for each user profile will need to be copied to the custom folder as shown in the folder structure above.

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.

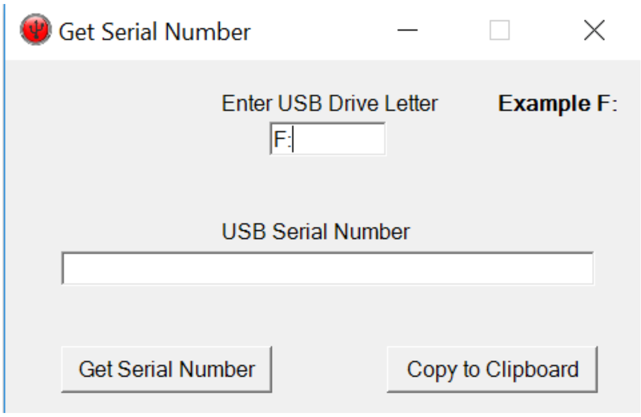
Extracting USB artefacts from extracted Linux files

1) USBFT can extract USB artefacts from Ubuntu syslog files
2) Extract the required files to a folder on the Windows examination machine.
3) Open USBFT and press the Linux 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.

Extracting serial number from a connected USB device

The user now has the option to connect a USB device to a computer and extract the serial number.

1) Connect a USB device to the computer.
2) Click the USB button
3) A form will open
4) Enter the drive letter of the USB device followed by “:” into the form.



5) Click “Get Serial Number”.
6) You can click “Copy to Clipboard” button to save the serial number.

Exporting data to Excel spreadsheet

1) By default when you export the data, the content of all the data grids will be exported into a single Excel spreadsheet.
2) Occasionally a data grid may contain characters that is not compatible with Excel. Once the data has been exported to Excel when you try to open the spreadsheet you will receive an error message and will be unable to open the spreadsheet.
3) If this occurs you can identify which data grid contains the illegal characters by going to Options => Export Options and deselecting the data grids one at a time until you identify the problem.

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.

Debug Option

1) USBFT now has the option to enable debugging if required. By default debugging is disabled.
2) To enable debugging press the “Debug” menu button and check “Enable Debugging”.
3) Debug information will be saved to a txt file called “Debug Log.txt which will be located in the same directory as the USBFT executable file.

4) To view the debug log file press the debug button. 🐞

5) To delete the debug log press the delete debug button. 🗑

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.

Image Mounter

Mark Spencer president of Arsenal Recon has very kindly granted me permission to incorporate Arsenal Image Mounter (AIM) within USBFT. AIM has a big advantage over many other free image mounting tools. AIM mounts the contents of disk images as complete disks in Microsoft Windows. This allows the investigator access to the volume shadow copies located on the mounted drive.

AIM also has a lot of other useful features. If you have not used Arsenal Image Mounter before I would recommend that you visit their website and download the stand alone version.

https://arsenalrecon.com/weapons/image-mounter/

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 1.1.3 August 2018

1) Fixed bug in the WPDBUSENUM tab where the time was not changing to UTC when selected by the user.
2) Changed the code so USBFT no longer processes the setupapi.upgrade.log file in order to avoid confusion between user generated times and dates and system generated times and dates.
3) In WPD tab changed code so if there is no description for the USB device it will not display any data in the serial column.
4) Merged the Description and MFG columns within the WPD tab into a single Description column in order to keep the same description format as the other tabs.
5) USBFT will now operate correctly when selecting the custom folder option when the folder path has spaces within it.

Version 1.1.2 July 2018

1) Added 3 new columns to the “Win 10 Event Log” tab
    a. Volume Serial Number
    b. Volume GUID
    c. Drive Letter
2) USBFT now extracts information from the “Microsoft-Windows-Partition%4Diagnostic.evtx” log (including volume serial number)
3) USBFT now extracts information from the “Microsoft-Windows-Ntfs%4Operational” log
4) Added horizontal scroll bars to all tab views
5) Added word wrap to all columns
6) Minor changes to code

Version 1.1.1 June 2018

7) Added a new information tab to the UI (Accessed Files).
8) USBFT now extracts information about files accessed from USB devices and link the files to specific USB devices.
9) Made some minor changes to code.

Version 1.1.0 May 2018

1) Fixed a bug in code so USBFT now correctly extracts USB artefacts from the C:\Windows\INF\setupapi.upgrade.log file.
2) USBFT now extracts information about mounted TrueCrypt and VeraCrypt volumes. The information can be found under the "Registry-Mounted Devices" tab.
3) Fixed a bug in code so when wishing to export results from multiple mounted images to Excel, you no longer have to close and reopen USBFT between exports.

Version 1.0.9 February 2018

1) USBFT now extracts USB artefacts from the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\EMDMgmt

Version 1.0.8 October 2017

1) USBFT now extracts USB artefacts from C:\Windows\INF\ setupapi.dev.yyyymmdd_hhmmss.log
2) USBFT now extracts USB artefacts from C:\Windows\INF\setupapi.upgrade.log
3) Added a RecordID column to the Win10 Event Log tab
4) Added a RecordID column to the Win 7 Event Log tab
5) Added the ability to mount forensic images
6) Added the ability to extract volume shadow copy information
7) Added the ability to extract USB artefacts from mounted volume shadow copies
8) Added the option to enable debugging.
9) Added a view debug log button
10) Added a delete debug log button
11) Made improvements to the code to make it more reliable and to support debugging
12) Updated Help file.

Version 1.0.7 August 2017

1) USBFT now supports the extraction of USB artefacts from Linux (Ubuntu) syslog files
2) Added styling and formatting to the Excel report

Version 1.0.6 August 2017

1) USBFT now extracts data from the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\SWD\WPDBUSENUM
2) Setupapi Log – changed the name of the "Connection Date" column to "Device Install Date".
3) Added a new column called "Device Delete Date". USBFT extracts the time and date when the device drivers are installed for a USB device (typically the first time it is connected).
4) USBFT now displays the time and date when the Windows Plug and Play Cleanup service deletes the drivers for a USB device and deletes the entries for the device from the registry. The time and date is displayed in the "Device Delete Date" column.

Version 1.0.5 July 2017

1) Changed the project over from Windows Forms to WPF MVVM to make it easier to maintain and update in the future.
2) Made major changes to the code throughout the project to accommodate the new format.
3) Added the ability to process a custom folder that contains the extracted Windows registry files, Windows logs and NTUser.dat files
4) Added the ability to extract USB artefacts from the "Windows.old" folder.
5) Added the ability to extract USB artefacts from HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Search\VolumeInfoCache
6) Added the ability for a user to extract the serial number of a USB device connected to the system.
7) Made changes to the title of the Win7 and Win10 Event Log tabs.
8) Added an EventID column to the Windows7 Event Log data grid and the Win10 Event Log data grid.
9) Removed the checkbox column from the data grids.
10) Removed the filter button from the menu (used to filter checked files).
11) Removed the Reload button (now redundant)
12) Under Options => Export Options, added the ability for the user to select which data grids will be exported to the excel spreadsheet.
13) Combined all the DLL's with the exe to make a single exe file for ease of deployment.

Version 1.0.4 July 2016

1) Made a slight change to the code and to the README file to make it clear that when analyzing mounted forensic images they must be mounted in writable mode.

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.