USB Detective User Guide

Contents

Usage 5

Case Folder 5

Excluding LNK File System Dates 5

Processing Stand-Alone Artifacts 6

Processing Artifacts from a Logical Drive 8

Processing Artifacts from a Live System 8

Processing Artifacts from Volume Shadow Copies 9

Processing LNK Files & Jump Lists 9

Processing ShellBags 11

Additional Processing Features 11

Replaying Transaction Logs 11

Removal of Unreliable Timestamps from Results 11

Processing Statistics 12

Viewing the Results 13

Results Grid 13

Results Grid Context Menu 13

View All Values 14

View Verbose Details 14

View Other Connection Times 14

View Files Accessed on This Device 15

Export Device MBR & VBR 15

Export Device Timeline 15

Device and Volume Encryption Detection 15

Consistency levels 16

High Consistency Level Values 16

Mid Consistency Level Values 16

Low Consistency Level Values 16

Consistency Level Not Calculated 17

Reporting 17

Results Grid 17

Preserve Timestamp Consistency Color-Coding 17

Include All Values List as Comment 17
Include Opened/Accessed Files 17
Include Directory Interactions 18
Timeline 18
Include Device Deletion Times 18
Include OS Install Time(s) 18
Include Opened/Accessed Files 19
Include Directory Interactions 19
Add to Results Grid XLSX Report 19
Verbose Report 20
Options 20
General Options 20
Show Data Input Selector on Startup 20
Show 64-bit VSNs 20
Verbose Logging 20
Auto-Save Log 20
Log in UTC 21
Show Log Pane by Default 21
Show Legend by Default 21
Check for Updates on Start 21
Alert When X or More Reported Timestamps in the Same Column are Identical 21
Processing Options 21
Include Ambiguous Devices in Results 21
Include Non-Removable Devices in Results 22
Include LNKs for C:\ 22
Include LNKs without VSN 22
Process ShellBags 22
Include All ShellBags in Results 22
Time Zone Options 22
Displayed Time Zone 22
Automatically Set Based on SYSTEM Registry Hive 22

Interpret Local Timestamps using Displayed Time Zone Setting Specified Above 23

Consistency Level Options 23

Display Consistency Levels 23

Consistency Level Threshold 23

Consistency Level Colors 23

Acknowledgments 24

Changelog 24

Version 1.6.2 24

Version 1.6.1 24

Version 1.6.0 25

Version 1.5.4 25

Version 1.5.3 25

Version 1.5.2 26

Version 1.5.1 26

Version 1.5.0 26

Version 1.4.1 27

Version 1.4.0 27

Version 1.3.6 27

Version 1.3.5 27

Version 1.3.0 28

Version 1.2.0 28

Version 1.1.7 28

Version 1.1.6 29

Version 1.1.5 29

Version 1.1.0 30

Version 1.0.4 30

Version 1.0.3 30

Version 1.0.2 30

Version 1.0.1 31

Version 1.0.0 31

NOTE: You must have .NET version 4.6.1 or higher installed to run USB Detective!

Usage

Upon launching USB Detective, the user will be greeted with a window prompting for the type of data to be processed by USB Detective. The current options are individual files/folders, logical drive, or the live system. Displaying the data input selector on startup is configurable in the USB Detective options and is further explained here.

Case Folder

USB Detective allows for the path to a Case Folder to be supplied prior to processing data. The Case Folder is the location where the USB Detective log will be auto-saved as well as the default location for saving reports created by USB Detective (including those automatically saved during live system processing). If a Case Folder is not supplied, auto-saved logs and the default location for reports will be the current directory of USB Detective.

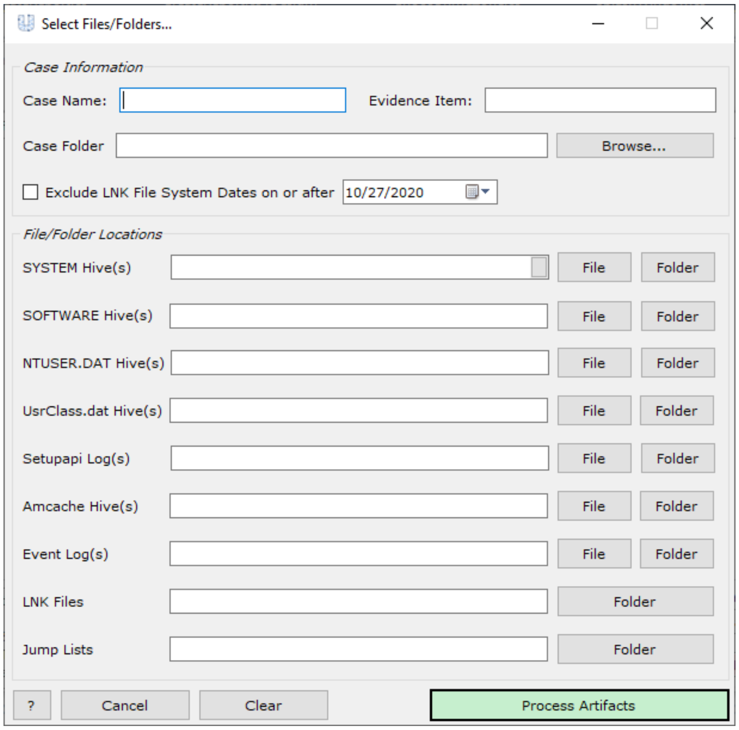
Excluding LNK File System Dates

When processing artifacts using the Files/Folders option of USB Detective, there is an additional option to exclude LNK file system timestamps on or after a specified date. When enabled, this option ignores the last modified timestamp of LNK files when it occurs on or after the specified date.

Under normal circumstances, the last modified timestamp of a LNK file could be used to identify the last time the LNK target file was opened/accessed. However, when LNK files are carved from the unallocated clusters of a system, their original file system timestamps are unavailable and often assigned to the carved LNK files upon recovery or export from a forensic tool. In this scenario, the file system timestamps of the carved LNK file would reflect the time of recovery or when it was saved to the examiner's storage device. While the embedded content of carved LNK files (target file timestamps, volume information, etc.) may still be reliable, the last modified timestamp of the carved LNK file should not be used to identify the last time the target file was opened/accessed. When supplying USB Detective with carved LNK files, enabling the "Exclude LNK file system dates on or after" option and setting the "on or after" date to the date of imaging will help to avoid the inclusion of these potentially misleading timestamps in USB Detective timeline reports.

Processing Stand-Alone Artifacts

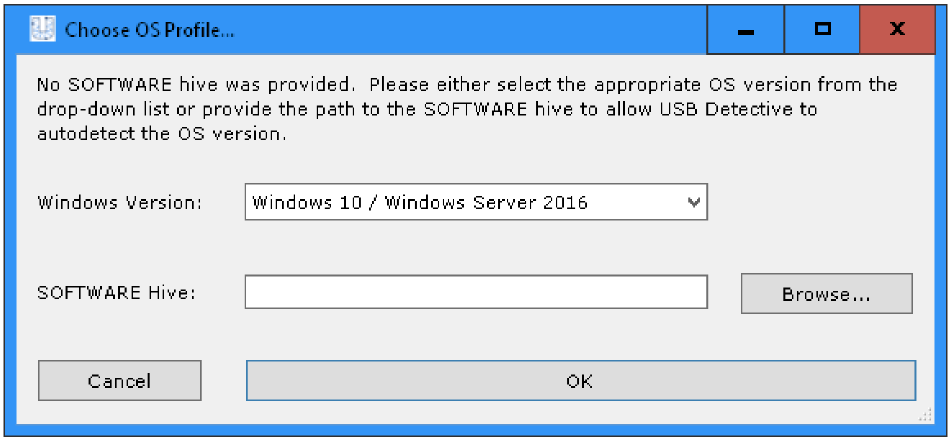
To supply USB Detective with stand-alone artifacts for processing, choose the option for "Files/Folders" in the initial data input selector or choose File > Select Files/Folders from within the main window of USB Detective. For each artifact, browse to the location of each file or select the directory containing the file(s) to be processed. The small unmarked button on the right side of the SYSTEM Hive(s) text box copies the value of the SYSTEM Hive(s) text box to all other text boxes in the Select Files/Folders form. Currently supported files include the SYSTEM, SOFTWARE, NTUSER.DAT, and UsrClass.dat registry hives, setupapi log files, amcache.hve hives, event logs, LNK files, and automatic jump lists. The System, Microsoft-Windows-DriverFrameworks-UserMode\Operational, Microsoft-Windows-Kernel-PnP\Configuration, Microsoft-Windows-Partition\Diagnostic, and Microsoft-Windows-Storsvc\Diagnostic event logs for Windows 7-10 are currently supported.



□ Exclude LNK File System Dates on or after 10/27/2020

For all supported artifacts, a folder can optionally be provided instead of the path to an individual file. This allows the user to pass in multiple versions of all artifacts in order to build a more complete picture of USB device activity. The supplied folder should be the top-level directory containing the artifacts. The provided folder will be recursively scanned for applicable files. For example, in addition to the traditional setupapi(.dev).log files, setup.upgrade.log files are also accepted and parsed when a folder path is provided. You can provide any combination of the supported artifacts, but the parsing process will be more thorough as additional artifacts are supplied for processing. For examples of the default storage location of each of the supported artifacts, click the "?" button next to the Cancel button in the Select Files/Folders window. After providing the path to all files to be parsed, select "Process Artifacts".

If a software hive was not provided, a dialog requesting the operating system version or the path to the SOFTWARE hive will be displayed. Since there are differences across versions of Windows with respect to USB device artifacts, the operating system version should be known in order to properly interpret the artifacts for the specific version of Windows.



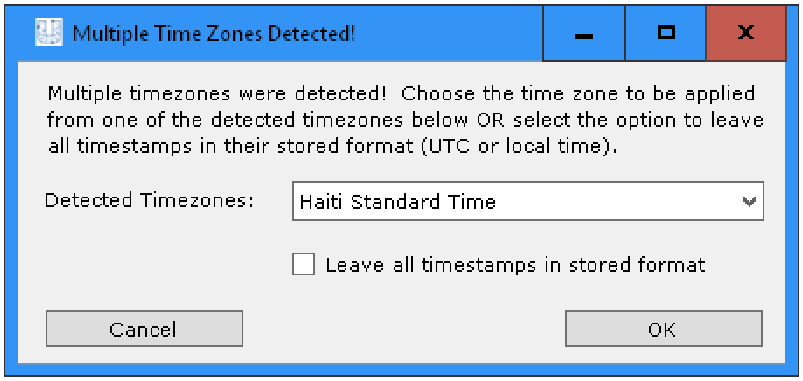
No SOFTWARE hive was provided. Please either select the appropriate OS version from the drop-down list or provide the path to the SOFTWARE hive to allow USB Detective to autodetect the OS version.

Windows Version: Windows 10 / Windows Server 2016

SOFTWARE Hive:

If multiple time zones are detected in the SYSTEM hives provided for processing, USB Detective will request which time zone to apply from the list of time zones detected in the SYSTEM hives. Alternatively, the user may opt to leave all timestamps in their stored format using the available checkbox option. This window will only be displayed if the USB Detective options are set to display timestamps based on the time zone determined from the SYSTEM hive.

USB Detective will parse the provided registry hives and setupapi log files, identifying key attributes about connected USB devices such as serial/UID, description, first/last connected/disconnected, drive letter, volume name, volume serial number, and more. USB Detective does not rely on a single data point such as the USBSTOR subkey and thus is not as susceptible to anti-forensics or cleanup methods as tools or techniques that rely on a single data point to build the list of connected devices.



Multiple timezones were detected! Choose the time zone to be applied from one of the detected timezones below OR select the option to leave all timestamps in their stored format (UTC or local time).

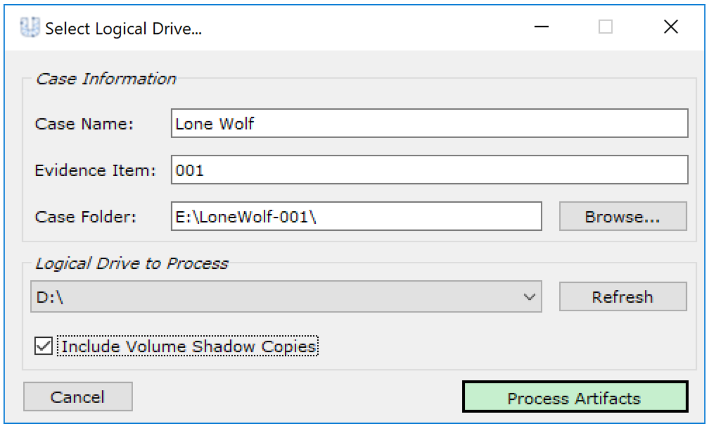
Detected Timezones: Haiti Standard Time

□ Leave all timestamps in stored format

Details on the parsing process are logged in the USB Detective log box below the results grid. In addition to updates on the parsing process, key attributes about the system such as the operating system version, time zone, and computer name are logged (if these attributes are available from the provided artifacts).

Processing Artifacts from a Logical Drive

To supply USB Detective with a logical drive containing artifacts for processing, navigate to File > Select Logical Drive and choose the drive letter associated with the artifacts to be processed. This option is intended to be used for logical drives that are not associated with the live system on which USB Detective is running. The most common use case for this is running USB Detective against a mounted forensic image. After selecting the drive letter to be processed, click the "Process Artifacts" button.


Select Logical Drive...

Case Information

Case Name: Lone Wolf

Evidence Item: 001

Case Folder: E:\LoneWolf-001\

Logical Drive to Process

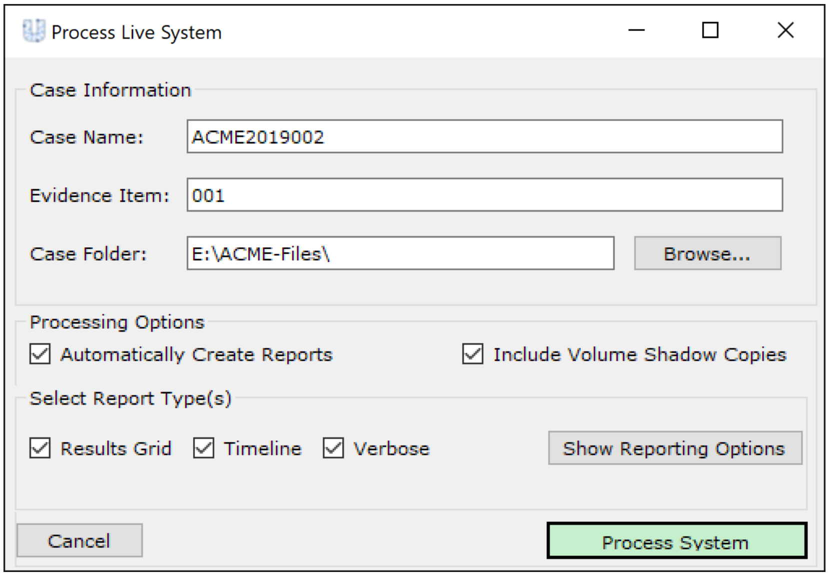
D:\

☑ Include Volume Shadow Copies

USB Detective will attempt to locate the same artifacts that can be manually supplied to USB Detective by searching within the expected directory for each artifact. A recursive scan of the entire logical drive is not performed. If you wish to process supported artifacts that are not stored in their normal locations, please supply them manually using the Select Artifacts option of USB Detective. The full path to each identified artifact available for processing is logged in USB Detective.

Processing Artifacts from a Live System

To run USB Detective against a live system, select "Process Live System" from the splash screen that appears when starting the program or via the File > Process Live System menu option. USB Detective will then ask for the case name, evidence number, and case folder. If the case folder is left blank, the directory from which USB Detective is running is treated as the case folder.


Process Live System

Case Information

Case Name: ACME2019002

Evidence Item: 001

Case Folder: E:\ACME-Files\

Processing Options

☑ Automatically Create Reports ☑ Include Volume Shadow Copies

Select Report Type(s)

☑ Results Grid ☑ Timeline ☑ Verbose

When processing a live system, USB Detective provides the default option to automatically create reports. When this option is selected, the chosen report type(s) will be generated and saved in the case folder following system processing. This allows a first responder to quickly generate reports without navigating the reporting module post processing. Additional reporting options can be selected using the “Show Reporting Options” button in the Process Live System window. In addition to automatically creating reports, USB Detective defaults to processing the artifacts from any existing volume shadow copies on the live system. All artifacts supported through file/folder or logical drive processing are also supported in live system processing, including files that are locked or in use by the operating system.

NOTE: USB Detective must be executed from an NTFS-formatted removable device in order to access the volume shadow copies of the live system. Additionally, USB Detective requires .NET 4.6.1 to be installed on the system from which it is executed. While this is standard on Windows 10 systems, older operating systems may not necessarily have the .NET version appropriate for running USB Detective.

Processing Artifacts from Volume Shadow Copies

In order for USB Detective to process volume shadow copies from a forensic image, the image should be mounted in a manner that makes any VSCs accessible. Arsenal Image Mounter (https://arsenalrecon.com) is an example of mounting software that allows any VSCs on the forensic image to be accessed.

To process artifacts from volume shadow copies, select the Logical Drive or Live System option in USB Detective and select the option to Include Volume Shadow Copies. When this option is selected, USB Detective will attempt to process all supported artifacts from each volume shadow copy accessible to USB Detective. The information obtained from VSCs is automatically aggregated with the results from the active volume data identified by USB Detective. When documenting the source of a data point identified in a VSC, USB Detective will record the snapshot ID of the VSC in which the data point was located (e.g. *VSC{2b03870e-d9f3-410d-8699-53d49e76fd25}\Windows\System32\config\SYSTEM*).

It is recommended to run USB Detective on a Windows 10 system when processing VSCs. Running USB Detective on some Windows versions – specifically Windows 7 – may result in the inability to access VSCs on a Windows 10 forensic image. If this happens, USB Detective will log the error and proceed with the processing of the active volume.

Processing LNK Files & Jump Lists

When provided via the Select Artifacts window, a logical drive, or live system processing, LNK files and automatic jump lists are processed by USB Detective. It is beyond the scope of this user guide to detail the internal structure or analysis methodology of LNK files and jump lists, but the section below summarizes the usefulness of these files as it relates to USB device investigations.

LNK files and jump lists can be very helpful in forensic investigations involving removable media because they reveal information about file access and storage on USB devices. One of the fields embedded in LNK files and jump lists is the volume serial number of the device on which the target file (i.e. the file or folder referenced by the LNK file or jump list record) was stored the last time the target file was opened. By matching this field with the volume serial number of a device that was connected to the system, an examiner can correlate the information contained in the LNK file or jump list with a specific device. Among other things, this allows an examiner to detail the time that a particular file or folder was accessed on a specific device as well as the creation, last modification, and last accessed time of the file or folder the last time it was opened.

Currently, the following folders are scanned for LNK files and automatic jump lists when USB Detective is provided with a logical drive letter or live system to process:

- Users\<username>\AppData\Roaming\Microsoft\Windows\Recent (Vista+)
- Users\<username>\AppData\Roaming\Microsoft\Office\Recent (Vista+)
- Documents and Settings\<username>\Recent (XP)
- Documents and Settings\<username>\Application Data\Microsoft\Office\Recent (XP)

If you need to process LNK files or automatic jump lists that are not located in one of the directories above (e.g. LNK files carved from unallocated space), they should be processed using the Select Artifacts method of USB Detective.

The number of LNK file and jump list records on a system can be quite voluminous as files opened on the operating system volume (e.g. C:\), network shares, and more result in the creation of a LNK file and/or jump list record. In order to help reduce the potential "noise" of LNK file and jump list records referencing locations such as the C:\ drive or network shares, USB Detective optionally excludes LNK files and jump list records referencing files and folders on the "C:\" drive as well as records that do not contain an embedded VSN (e.g. files stored on network shares). The option to exclude LNK file and jump list records referencing "C:\" and those that do not contain an embedded VSN is enabled by default. To read more about these options, see here. To include the "C:\" records and/or those that do not contain an embedded VSN, simply enable the applicable options via Tools > Options. When a LNK file or jump list record is excluded because it references "C:\" or does not contain an embedded VSN, a USB Detective log entry will be created to document the exclusion.

As data from LNK files and jump lists can be duplicative in nature (e.g. when volume shadow copies, carved files, or otherwise are processed), USB Detective attempts to remove records from LNK files and jump lists that are duplicative. To assess whether a record is a duplicate, USB Detective compares the full path of the target file as well as the last opened/accessed time of the file. The number of duplicate LNK files and jump lists records excluded is logged in the USB Detective log file.

Processing ShellBags

When a UsrClass.dat registry hive is provided via the Select Artifacts window, a logical drive, or live system processing, shellbags existing in the provided UsrClass.dat hive(s) are processed by USB Detective. It is beyond the scope of this user guide to detail the forensic analysis methodology or internal structure of shellbags, but at a high level, shellbags are useful in identifying directories that exist (or existed) on storage mediums with which the Windows operating system interfaced.

Shellbags may include references to directories on the operating system volume, network storage devices, removable storage devices, and even .zip archives. By default, shellbags referencing a directory path with drive letters other than "C:\" are included in the results. To include all shellbags in the results of USB Detective (i.e. shellbags referencing directories on the C:\ drive and those without a drive letter), enable the "Include All ShellBags in Results" option available via Tools > Options. Data from shellbags processed by USB Detective is included in the "Directory Interaction" category available during reporting.

During processing, shellbags identified by USB Detective are deduplicated. This helps to avoid duplicate directory interaction records, especially when volume shadow copies, carved registry hives, and other backups sources are included during processing. After processing is complete, the identified directory interaction timestamps are checked for reliability and timestamps deemed to be unreliable are excluded from the results. This functionality is further documented here. ShellBags processed by USB Detective can be included in either the Results Grid report or as part of a USB Detective Timeline report.

Additional Processing Features

Replaying Transaction Logs

Registry transaction log files are automatically replayed in the Professional version of USB Detective. The transaction log files are expected to be named the same as the associated hive prior to the file extension (e.g. SYSTEM.LOG1, SYSTEM.LOG2, etc.) and stored in the same directory as the hive with which they are associated. All dirty hives are recorded in the USB Detective log, as well as whether any provided transaction logs were replayed.

Removal of Unreliable Timestamps from Results

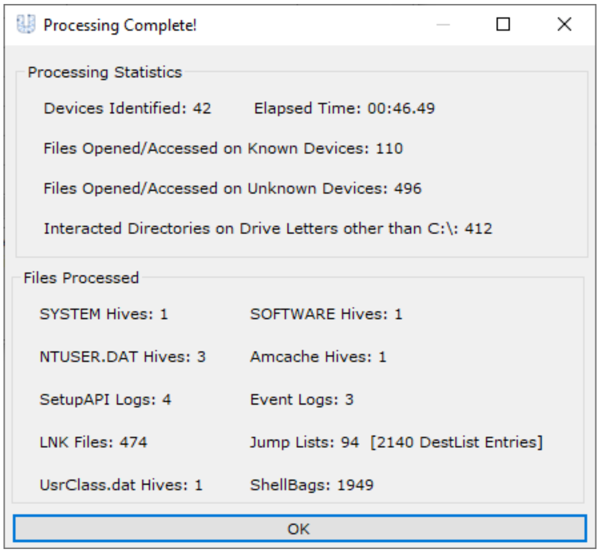
After all processing is complete, USB Detective performs a check for unreliable timestamps and removes them from the results (if any are identified). Currently, the timestamps queried from the Enum\USB subkey hierarchy are evaluated to determine whether the LastWrite time of the Enum\USB\{S/N} subkey for two or more devices is the same. If two or more {S/N} LastWrite times are the same, that data point/timestamp is deemed unreliable by USB Detective and excluded from the results. Similarly, the interaction time of directories extracted from shellbags in the BagMRU subkey hierarchy are checked for duplicate timestamps. Since Windows 10 Feature Updates can impact the LastWrite time of the BagMRU subkey hierarchy, many directory interaction timestamps may be removed from the results during this process. While this exclusion is not apparent in the Results Grid view of USB Detective, it may significantly impact the number of records available in the timeline report when directory interactions are included in a timeline. When an unreliable timestamp is excluded, it is logged by USB Detective.

Since the unreliable device connection timestamps are not included in the results, they are not included in consistency level calculations. This prevents values with otherwise consistent data points from being displayed as a mid or low consistency value due to an unreliable timestamp. It also prevents USB Detective from displaying the same timestamp for the last time that multiple devices were connected (when no other last connected data points are available).

Processing Statistics

After all processing is complete, USB Detective displays a Processing Statistics window that provides a high-level overview of the processed data.

The fields included in the Processing Statistics window detail the number of each supported type of artifact (e.g. SYSTEM hives, event logs, LNK files, etc.) identified and processed by USB Detective. The displayed number includes artifacts that are located in volume shadow copies as well as duplicate LNK files, jump list records, and shellbags. The "Jump Lists" field includes the number of jump list files processed as well as the number of individual DestList entries across all processed jump lists.



Processing Statistics

Devices Identified: 42   Elapsed Time: 00:46.49

Files Opened/Accessed on Known Devices: 110

Files Opened/Accessed on Unknown Devices: 496

Interacted Directories on Drive Letters other than C:\: 412

Files Processed

SYSTEM Hives: 1   SOFTWARE Hives: 1

NTUSER.DAT Hives: 3   Amcache Hives: 1

SetupAPI Logs: 4   Event Logs: 3

LNK Files: 474   Jump Lists: 94 [2140 DestList Entries]

UsrClass.dat Hives: 1   ShellBags: 1949

The "Files Opened/Accessed on Known Devices" and "Files Opened/Accessed on Unknown Devices" fields detail the number of unique LNK file or jump list records referencing file/folder access on a device known to USB Detective and those on a device unknown to USB Detective, respectively. In order for a LNK file or jump list record to be associated with a known device, the VSN embedded in the LNK file or jump list record must match a device VSN identified by USB Detective. If a VSN is not available for a device identified by USB Detective, the device will not be tied to any LNK file or jump list records.

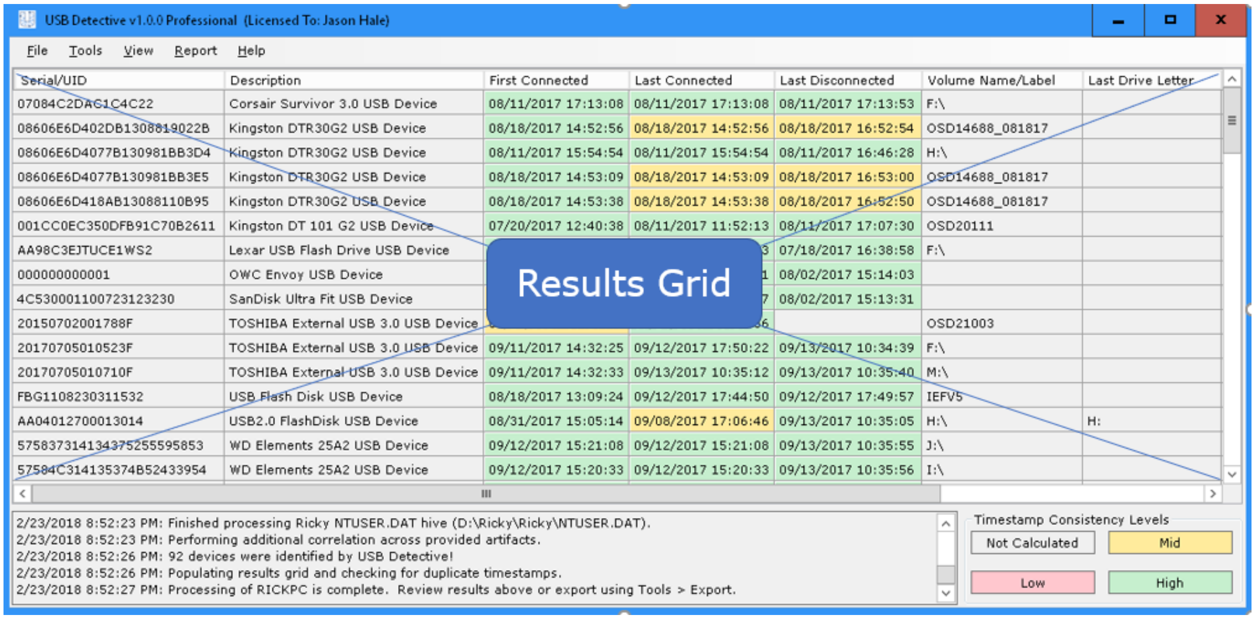
The "Files Opened/Accessed on Unknown Devices" field details the number unique LNK file or jump list records processed by USB Detective that cannot be directly associated with a device identified by USB Detective based on VSN. If LNK file and jump list records referencing "C:\" or those without an embedded VSN are optionally processed by USB Detective, they will be added to the "Files Opened/Accessed on Unknown Devices" field.

The "Interacted Directories on Drive Letters other than C:\" field details the number of directories identified through shellbags that references a path including a drive letter other than "C:\" (e.g. "F:\files\personal", "Y:\backup\docs", etc.).

Viewing the Results

Results Grid

After USB Detective finishes processing the provided artifacts, the results will be displayed in the results grid. If a consistency level was calculated for a value, the cell containing the value will be color-coded according to the consistency level legend available in the main window of USB Detective. Consistency levels are further explained here.


USB Detective v1.0.0 Professional (Licensed To: Jason Hale)
File
Tools
View
Report
Help
Results Grid
Timestamp Consistency Levels
Not Calculated
Mid
Low
High

Serial/UID	Description	First Connected	Last Connected	Last Disconnected	Volume Name/Label	Last Drive Letter
07084C2DAC1C4C22	Corsair Survivor 3.0 USB Device	08/11/2017 17:13:08	08/11/2017 17:13:08	08/11/2017 17:13:53	F:\	
08606E6D402DB1308819022B	Kingston DTR30G2 USB Device	08/18/2017 14:52:56	08/18/2017 14:52:56	08/18/2017 16:52:54	OSD14688_081817	
08606E6D4077B130981BB3D4	Kingston DTR30G2 USB Device	08/11/2017 15:54:54	08/11/2017 15:54:54	08/11/2017 16:46:28	H:\	
08606E6D4077B130981BB3E5	Kingston DTR30G2 USB Device	08/18/2017 14:53:09	08/18/2017 14:53:09	08/18/2017 16:53:00	OSD14688_081817	
08606E6D418AB13088110B95	Kingston DTR30G2 USB Device	08/18/2017 14:53:38	08/18/2017 14:53:38	08/18/2017 16:52:50	OSD14688_081817	
001CC0EC350DFB91C70B2611	Kingston DT 101 G2 USB Device	07/20/2017 12:40:38	08/11/2017 11:52:13	08/11/2017 17:07:30	OSD20111	
AA98C3EJTUCE1WS2	Lexar USB Flash Drive USB Device		3	07/18/2017 16:38:58	F:\	
000000000001	OWC Envoy USB Device		1	08/02/2017 15:14:03		
4C530001100723123230	SanDisk Ultra Fit USB Device		7	08/02/2017 15:13:31		
20150702001788F	TOSHIBA External USB 3.0 USB Device		6		OSD21003	
20170705010523F	TOSHIBA External USB 3.0 USB Device	09/11/2017 14:32:25	09/12/2017 17:50:22	09/13/2017 10:34:39	F:\	
20170705010710F	TOSHIBA External USB 3.0 USB Device	09/11/2017 14:32:33	09/13/2017 10:35:12	09/13/2017 10:35:40	M:\	
FBG1108230311532	USB Flash Disk USB Device	08/18/2017 13:09:24	09/12/2017 17:44:50	09/12/2017 17:49:57	IEFV5	
AA04012700013014	USB2.0 FlashDisk USB Device	08/31/2017 15:05:14	09/08/2017 17:06:46	09/13/2017 10:35:05	H:\	H:
575837314134375255595853	WD Elements 25A2 USB Device	09/12/2017 15:21:08	09/12/2017 15:21:08	09/13/2017 10:35:55	J:\	
57584C314135374B52433954	WD Elements 25A2 USB Device	09/12/2017 15:20:33	09/12/2017 15:20:33	09/13/2017 10:35:56	I:\	

```
2/23/2018 8:52:23 PM: Finished processing Ricky NTUSER.DAT hive (D:\Ricky\Ricky\NTUSER.DAT).
2/23/2018 8:52:23 PM: Performing additional correlation across provided artifacts.
2/23/2018 8:52:26 PM: 92 devices were identified by USB Detective!
2/23/2018 8:52:26 PM: Populating results grid and checking for duplicate timestamps.
2/23/2018 8:52:27 PM: Processing of RICKPC is complete.  Review results above or export using Tools > Export.
```

For each value in the description, first connected, last connected, last disconnected, volume name/label, VSN, drive letter, and last user column, USB Detective maintains all sources and values that were queried for that specific field. All values for the given field are available either via tool-tip when hovering over the cell containing the value of interest, the "View All Values" context menu option, or the “View Verbose Details” context menu option (explained below). This allows the user to easily see all queried values for the data point and is particularly useful in assessing values that were assigned low or mid consistency levels.

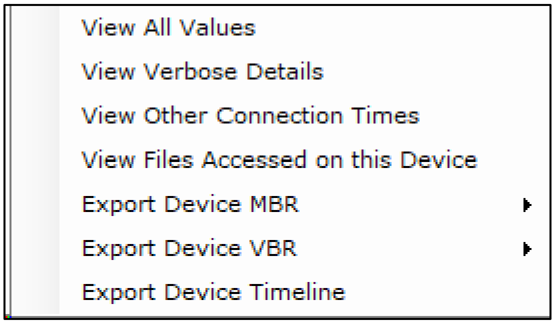
The Last User column of USB Detective includes the name of the parent directory where the NTUSER.DAT hive having the most recent MountPoints2 LastWrite time is stored. This feature is obviously more beneficial if multiple NTUSER.DAT registry hives are provided. Any provided NTUSER.DAT hives should be stored in a directory named by the user account from which the hive originated.

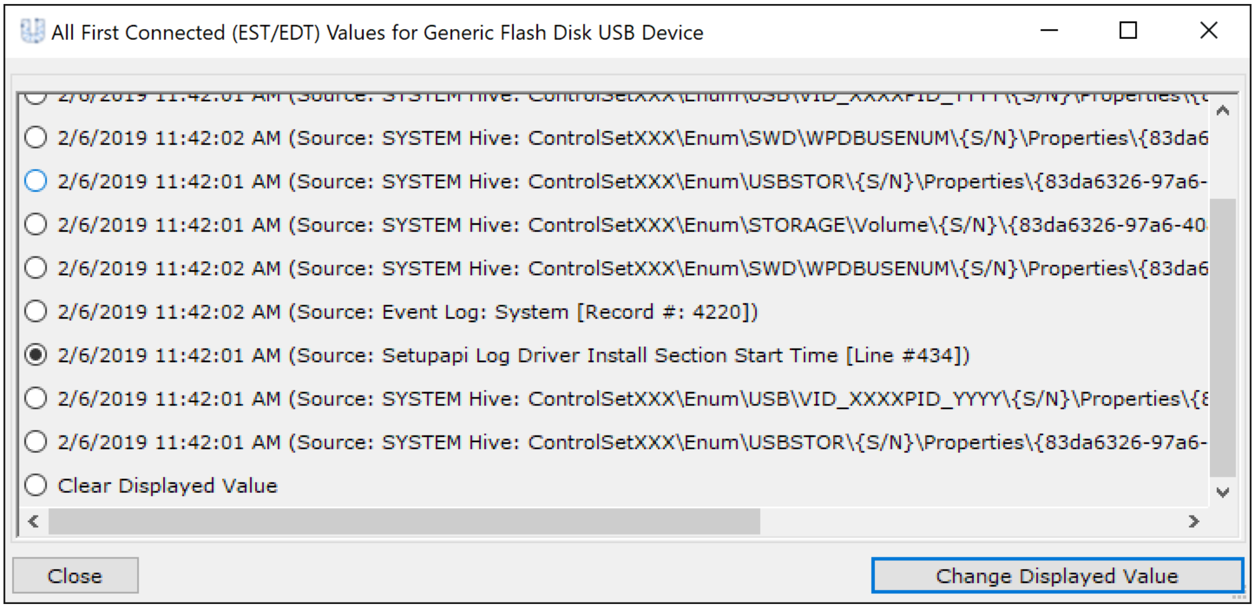
Results Grid Context Menu

The USB Detective Results Grid include a context menu with additional features or alternate ways to access data available within the program. The following sections explain each option available in the context menu.

View All Values

The View All Values option opens a secondary window displaying all values identified for the selected column (e.g. First Connected, Last Connected, etc.) of the selected device. In addition, the secondary window allows the user to change the value displayed in the Results Grid to a separate value obtained by USB Detective if the value displayed is found not to be reliable for the given source. Similarly, if the user determines that none of the available values are accurate, the value displayed in the USB Detective results grid can be cleared. This allows Results Grid report to include the non-default values as selected by the user.




All First Connected (EST/EDT) Values for Generic Flash Disk USB Device

○ 2/6/2019 11:42:01 AM (Source: SYSTEM Hive: ControlSetXXX\Enum\USB\VID_XXXXPID_YYYY\{S/N}\Properties\{8

○ 2/6/2019 11:42:02 AM (Source: SYSTEM Hive: ControlSetXXX\Enum\SWD\WPDBUSENUM\{S/N}\Properties\{83da6

○ 2/6/2019 11:42:01 AM (Source: SYSTEM Hive: ControlSetXXX\Enum\USBSTOR\{S/N}\Properties\{83da6326-97a6-

○ 2/6/2019 11:42:01 AM (Source: SYSTEM Hive: ControlSetXXX\Enum\STORAGE\Volume\{S/N}\{83da6326-97a6-40

○ 2/6/2019 11:42:02 AM (Source: SYSTEM Hive: ControlSetXXX\Enum\SWD\WPDBUSENUM\{S/N}\Properties\{83da6

○ 2/6/2019 11:42:02 AM (Source: Event Log: System [Record #: 4220])

● 2/6/2019 11:42:01 AM (Source: Setupapi Log Driver Install Section Start Time [Line #434])

○ 2/6/2019 11:42:01 AM (Source: SYSTEM Hive: ControlSetXXX\Enum\USB\VID_XXXXPID_YYYY\{S/N}\Properties\{8

○ 2/6/2019 11:42:01 AM (Source: SYSTEM Hive: ControlSetXXX\Enum\USBSTOR\{S/N}\Properties\{83da6326-97a6-

○ Clear Displayed Value

View Verbose Details

The View Verbose Details context menu option displays all identified information for a device in separate window. The verbose details pane for a device can also be accessed by double-clicking on a device row in the USB Detective Results Grid. Of particular note is the "Additional Attributes" field of the verbose details pane; this section includes information not displayed in the Results Grid such as diskId, container ID, file system type, encryption type, additional timestamps (e.g. first connected after last reboot), and much more.

View Other Connection Times

The View Other Connection Times context menu option opens a secondary window displaying other connected times for the selected device. These include additional connection and disconnection times (since only the first/last is displayed in the Results Grid) and are often obtained from event logs, volume shadow copies, and registry locations associated with Windows 10 cleanup and upgrade operations.

View Files Accessed on This Device

The View Files Accessed on This Device context menu option allows the user to view the LNK file and jump list records corresponding to the device selected in the Results Grid. The LNK file and jump list records are matched with the selected device based on volume serial number (VSN). This option is not available when there are no LNK file or jump list records that can be correlated to the selected device based on VSN.

Export Device MBR & VBR

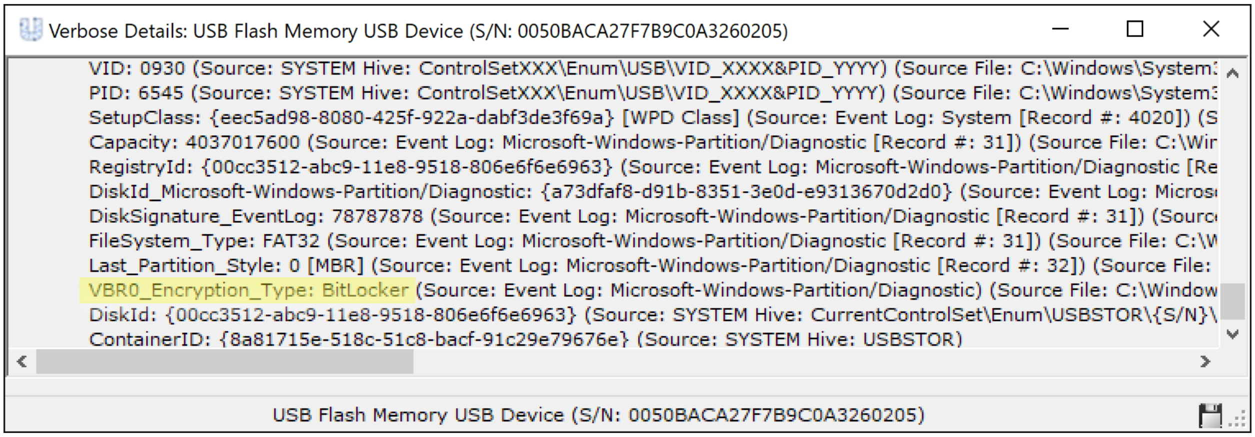
The Export Device MBR and Export Device VBR context menu options allow a user to export a .bin file containing the raw MBR or VBR of a selected device, when available. The raw MBR and VBR may be available from the event logs of some versions of Windows. Both the Export Device MBR and Export Device VBR menu options include a submenu that lists the date(s) associated with the raw MBR or VBR identified by USB Detective. When multiple unique versions of a device MBR or VBR are available, the date associated with each will be listed in the submenu and available for export.

Export Device Timeline

The Export Device Timeline context menu option of USB Detective allows a user to quickly create a timeline report consisting of all unique connection, disconnection, and file access timestamps for the selected device. This includes the values displayed in the Results Grid as well as additional connection and disconnection timestamps identified in volume shadow copies, event logs, or alternate registry locations. In addition, files accessed on the selected device (based on a matching VSN in any processed LNK files and jump lists) will be included in this report. This option exports the device timeline report to the USB Detective case folder.

Device and Volume Encryption Detection

When the raw MBR or VBR of a device is available, USB Detective will automatically check the raw MBR or VBR for known disk or volume encryption signatures. When device or volume encryption is detected, the encryption type is listed in the "Additional Attributes" section of the verbose details for a device.



Verbose Details: USB Flash Memory USB Device (S/N: 0050BACA27F7B9C0A3260205)

```
VID: 0930 (Source: SYSTEM Hive: ControlSetXXX\Enum\USB\VID_XXXX&PID_YYYY) (Source File: C:\Windows\System
PID: 6545 (Source: SYSTEM Hive: ControlSetXXX\Enum\USB\VID_XXXX&PID_YYYY) (Source File: C:\Windows\System
SetupClass: {eec5ad98-8080-425f-922a-dabf3de3f69a} [WPD Class] (Source: Event Log: System [Record #: 4020]) (S
Capacity: 4037017600 (Source: Event Log: Microsoft-Windows-Partition/Diagnostic [Record #: 31]) (Source File: C:\Wir
RegistryId: {00cc3512-abc9-11e8-9518-806e6f6e6963} (Source: Event Log: Microsoft-Windows-Partition/Diagnostic [Re
DiskId_Microsoft-Windows-Partition/Diagnostic: {a73dfaf8-d91b-8351-3e0d-e9313670d2d0} (Source: Event Log: Micros
DiskSignature_EventLog: 78787878 (Source: Event Log: Microsoft-Windows-Partition/Diagnostic [Record #: 31]) (Sourc
FileSystem_Type: FAT32 (Source: Event Log: Microsoft-Windows-Partition/Diagnostic [Record #: 31]) (Source File: C:\W
Last_Partition_Style: 0 [MBR] (Source: Event Log: Microsoft-Windows-Partition/Diagnostic [Record #: 32]) (Source File:
VBR0_Encryption_Type: BitLocker (Source: Event Log: Microsoft-Windows-Partition/Diagnostic) (Source File: C:\Window
DiskId: {00cc3512-abc9-11e8-9518-806e6f6e6963} (Source: SYSTEM Hive: CurrentControlSet\Enum\USBSTOR\{S/N}\
ContainerID: {8a81715e-518c-51c8-bacf-91c29e79676e} (Source: SYSTEM Hive: USBSTOR)
```

USB Flash Memory USB Device (S/N: 0050BACA27F7B9C0A3260205)

The following types of encryption are currently supported by USB Detective: BitLocker, CheckPoint, GuardianEdge/Symantec Endpoint, McAfee SafeBoot/Endpoint, Sophos Safeguard, Symantec PGP.

Consistency levels

USB Detective leverages multiple queried sources to create and display a consistency level associated with a value displayed in the USB Detective results grid. Consistency level calculations are currently performed on the first connected, last connected, and last disconnected timestamp fields.

When USB Detective identifies multiple values for a particular timestamp (e.g. first connected), the values are compared to determine whether they are within a certain threshold of one another. If the two timestamps are within the provided threshold, they are considered to be the same for the purposes of consistency level calculations. As the number of identical timestamps (or those within the consistency level threshold), increases, the consistency level of the timestamp displayed in the USB Detective results grid increases.

The goal of visually representing consistency levels is to allow the user to quickly identify timestamps that have discrepancies across the queried sources and those that contain multiple sources of corroborating data.

Details about how each consistency level in USB Detective is calculated can be found below. The number of possible corroborating data sources for a value will be limited based on what artifacts are provided for processing. It is strongly recommended that the user provide all artifacts accepted by USB Detective or run USB Detective against a mounted forensic image to allow the application to automatically identify the artifacts.

High Consistency Level Values

When USB Detective displays a high consistency level for a value, that value has two or more corroborating data sources and no queried data sources that are contradictory.

Mid Consistency Level Values

When USB Detective displays a mid consistency level for a value, that value has at least one corroborating data source to the default displayed value but another data source that is different (e.g. two out of three timestamps are within the consistency level threshold with one being the default displayed value).

Low Consistency Level Values

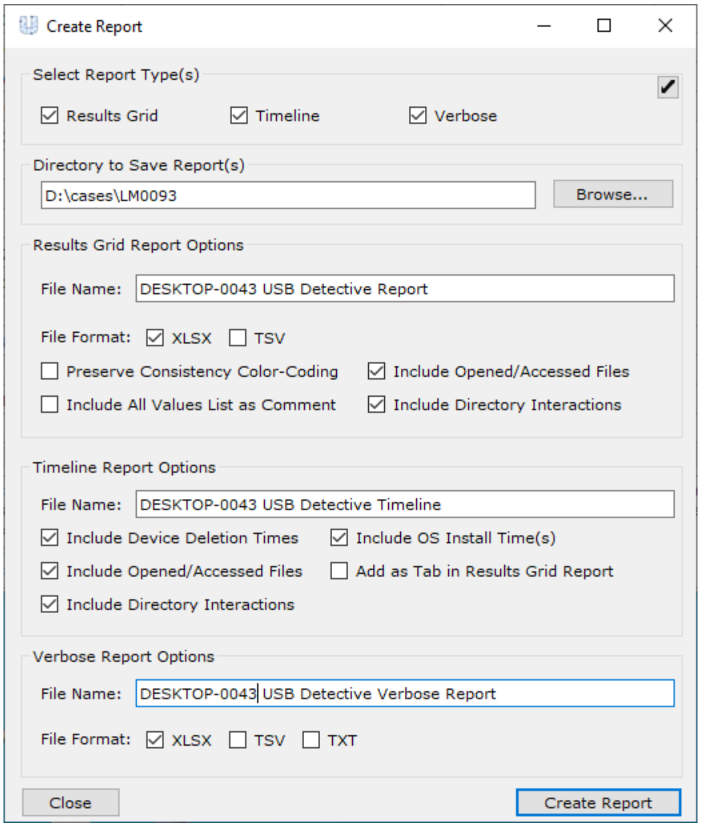
When USB Detective displays a low consistency level for a value, that value has two or more variations from the default displayed value or both available data sources are different.

Consistency Level Not Calculated

When USB Detective displays a “Not Calculated” consistency level, the consistency level of that value was not calculated because there was only one available data source or the value is not supported in consistency level calculations.

Reporting

The results of USB Detective can be exported to a separate file using the Report menu of USB Detective (or automatically using the Live System option). Reports can be generated simultaneously for any number of different formats supported by USB Detective by selecting the desired options in the Create Report module. When the “Create Report” button is clicked, all selected report types are generated according to the options selected in the Create Report window.



Create Report

Select Report Type(s) ☑

☑ Results Grid ☑ Timeline ☑ Verbose

Directory to Save Report(s)

D:\cases\LM0093

Results Grid Report Options

File Name: DESKTOP-0043 USB Detective Report

File Format: ☑ XLSX □ TSV

□ Preserve Consistency Color-Coding ☑ Include Opened/Accessed Files

□ Include All Values List as Comment ☑ Include Directory Interactions

Timeline Report Options

File Name: DESKTOP-0043 USB Detective Timeline

☑ Include Device Deletion Times ☑ Include OS Install Time(s)

☑ Include Opened/Accessed Files □ Add as Tab in Results Grid Report

☑ Include Directory Interactions

Verbose Report Options

File Name: DESKTOP-0043 USB Detective Verbose Report

File Format: ☑ XLSX □ TSV □ TXT

Results Grid

The Results Grid report option exports the results displayed in the results grid to either a tab separated values file or an Excel spreadsheet. If exporting to an Excel spreadsheet, the color-coded consistency levels and all values for each data point can optionally be included. The available Excel reporting options are further described below.

Preserve Timestamp Consistency Color-Coding

When checked, the “Preserve Timestamp Consistency Color-Coding” option instructs USB Detective to carry over the consistency level color-coding displayed in the USB Detective results grid to the Results Grid XLSX report.

Include All Values List as Comment

When checked, the “Include All Values List as Comment” option instructs USB Detective to carry over the list of all values associated with each data point to the Results Grid XLSX report. The list of all values will be added to each associated cell as a comment.

Include Opened/Accessed Files

The “Include Opened/Accessed Files” Results Grid Report option is a three-state checkbox and is only available when creating an XLSX format report.

When fully checked, this option instructs USB Detective to include an additional tab in the XLSX Results Grid report that includes all LNK file and jump list records processed by USB Detective. This would include records referencing removable devices containing a VSN unknown to USB Detective (i.e. unknown devices) as well records referencing the C:\ volume and those without an embedded VSN, if they were optionally processed by USB Detective.

When this option is half checked (i.e. indeterminate), USB Detective will include an additional tab in the XLSX Results Grid report that will include only the LNK file and jump list records associated with devices known to USB Detective (i.e. matching the VSN of a device identified by USB Detective).

Include Directory Interactions

The "Include Directory Interactions" Results Grid Report option instructs USB Detective to include an additional tab in the XLSX Results Grid report that includes directory interactions as identified through shellbags processed by USB Detective. This is intended to give the analyst a quick view of the directories references by the shellbags in any provided UsrClass.dat hives and intentionally does not expose all available shellbag information. For a more complete view of shellbag data from a system, it is recommended that a tool such as ShellBags Explorer be used.

The directory interactions included as a result of this report option are subject to the Processing Options relevant to shellbags as detailed here. For example, if this report option is selected but the only drive letter referenced by provided shellbags is "C:\", the report would not contain any directory interaction or creation records unless the "Include All ShellBags in Results" option is selected prior to processing.

Timeline

The Timeline report option exports all displayed timestamps in the results grid as well as all other connection and disconnection timestamps identified to an Excel spreadsheet. The timeline is auto-sorted in ascending date order upon creation. Duplicative connection and disconnection timestamps for a device are not added to the timeline. The timeline includes the date/time, type of event (connect or disconnect), and device information (serial, description, volume name, etc.).

Include Device Deletion Times

When checked, the "Include Device Deletion Times" option instructs USB Detective to include all identified device deletion times in addition to the connection and disconnection times normally displayed in the timeline report.

Include OS Install Time(s)

When checked, the "Include OS Install Time(s)" option instructs USB Detective to include any identified Windows installation times in addition to the connection and disconnection times normally displayed in the timeline report. Since multiple installation times may be available in Windows 10 (where an installation time coincides with a Windows upgrade), the installation timestamps can be helpful to include in a timeline report to add context to the connection and disconnection timestamps displayed in the report.

Include Opened/Accessed Files

The "Include Opened/Accessed Files" Timeline Report option instructs USB Detective to include timestamps from LNK files and jump list records in the Timeline Report. The last opened/accessed time from the LNK file or jump list record is included in addition to the target file creation time and target file last modified time. This will add a "File Opened/Accessed", "File Created", and "File Modified" event to the USB Detective Timeline Report, respectively.

The "Include Opened/Accessed Files" Timeline Report option is a three-state checkbox that behaves in the same manner as the three-state checkbox for the Results Grid report. When fully checked, this option instructs USB Detective to include the last opened/accessed time, target file creation time, and target file last modified time for all LNK file and jump list records processed by USB Detective. This would include records referencing removable devices containing a VSN unknown to USB Detective (i.e. unknown devices) as well records referencing the C:\ volume and those without an embedded VSN, if they were optionally processed by USB Detective.

When this option is half checked (i.e. indeterminate), USB Detective will include the last opened/accessed time, target file creation time, and target file last modified time for only the LNK file and jump list records associated with devices known to USB Detective (i.e. matching the VSN of a device identified by USB Detective).

Include Directory Interactions

The "Include Directory Interactions" Timeline Report option instructs USB Detective to include directory interactions identified through shellbags in the Timeline Report. In addition to the interaction time(s), the creation time of the directory, which is also extracted from shellbags, is included in the timeline. The directory interaction and creation time will add a "Directory Interaction" and "Directory Created" event to the USB Detective Timeline, respectively.

The directory interaction and creation times included as a result of this report option are subject to the Processing Options relevant to shellbags as detailed here. Note that the timeline records associated with directory interactions are intended to give the analyst a quick view of the directories references by the shellbags and intentionally do not include all available shellbag information. For a more complete view of shellbag data from a system, it is recommended that a tool such as ShellBags Explorer be used.

Add to Results Grid XLSX Report

The "Add to Results Grid XLSX Report" option instructs USB Detective to append the timeline report as an additional tab in the Results Grid XLSX report instead of creating a separate spreadsheet file for the timeline report. This option is only available when the Results Grid XLSX format option is selected.

Verbose Report

The Verbose View report option exports the contents of the Verbose View in USB Detective, which includes all data points and source files for each device identified by USB Detective. The Verbose View report can be exported as either an Excel spreadsheet, a tab separated values files, or a flat text file.

Options

USB Detective features several options for customizing the behavior of the application. The Tools > Options menu of USB Detective displays the available options. Clicking Save in the Options window saves a settings file in the same directory as the USB Detective executable. The settings file, if it exists, is loaded each time the application is started. This allows the settings from previous sessions to be maintained across executions.

The following options are available in USB Detective:

General Options

Show Data Input Selector on Startup

The Show Data Input Selector on Startup option controls whether USB Detective will display a window prompting for the type of input data when USB Detective is launched. Unchecking this option prevents the window from appearing when USB Detective is started.

Show 64-bit VSNs

The Show 64-bit VSNs option controls whether USB Detective will display 64-bit VSNs for a device in the result grid when a 64-bit VSN is available for that device. Depending on the location from which the VSN is obtained and the file system of the device, a 64-bit version of the VSN may be available. This value may not be as useful as the 32-bit version of the VSN since the 32-bit version is typically used in correlation with other activity found in LNK files, etc. If this option is disabled, the 32-bit VSN will be displayed even if a 64-bit VSN is available for a device. Even if the 64-bit VSN is not displayed in the results grid, the verbose details of a device will contain an entry for the 64-bit version.

Verbose Logging

The verbose logging option instructs USB Detective to perform additional logging that is generally not shown in the log box. This option may be helpful in troubleshooting any issues encountered with USB Detective.

Auto-Save Log

The Auto-Save Log option controls whether the USB Detective log will be automatically saved. When the log is automatically saved, it is stored either in the supplied Case Folder or the current directory of USB Detective.

Log in UTC

The Log in UTC option controls whether the timestamps included in the internal USB Detective log (available via File > Save Log) are recorded in UTC or local time. If this option is unchecked, timestamps in the USB Detective log are recorded in local time.

Show Log Pane by Default

The Show Log Pane by Default option controls whether the USB Detective log pane will be displayed along the bottom of the Results Grid. This setting is saved to the USB Detective settings file and thus serves as the default option when loading USB Detective. USB Detective will need to be restarted for any changes to this option to take effect. To show/hide the log pane on demand or for a single session, use the View > Show > Log Pane option.

Show Legend by Default

The Show Legend by Default option controls whether the consistency-level legend will be displayed along the bottom of the Results Grid. This setting is saved to the USB Detective settings file and thus serves as the default option when loading USB Detective. USB Detective will need to be restarted for any changes to this option to take effect. To show/hide the legend on demand or for a single session, use the View > Show > Legend option.

Check for Updates on Start

The Check for Updates on Start option controls whether USB Detective will automatically check for available updates to USB Detective each time it is started. Regardless of whether this option is enabled, a manual check for updates can always be performed via Help > Check for Updates.

Alert When X or More Reported Timestamps in the Same Column are Identical

The Alert When X or More Reported Timestamps in the Same Column are Identical option controls the number of displayed timestamps that must be identical in the same column before the user is notified. It is helpful to know when timestamps across multiple devices are identical, as they may be less reliable.

Processing Options

Include Ambiguous Devices in Results

The Include Ambiguous Devices in Results option controls whether USB Detective will display the devices whose type (e.g. storage or non-storage) could not be determined. A device is classified as ambiguous by USB Detective when the only identification data point(s) located by USB Detective do not indicate whether the device is a storage or non-storage device and there are no mechanisms by which USB Detective can correlate the device with a device whose type is known.

Include Non-Removable Devices in Results

The Include Non-Removable Devices in Results option controls whether USB Detective will display the devices it identifies as being non-removable, such as internal physical disks (e.g. PhysicalDisk0). NOTE: Enabling this option may result in duplicate devices listed in the results of USB Detective.

Include LNKs for C:\

The Include LNKs for C:\ option controls whether USB Detective will include the LNK file and jump list records referencing a file or folder on the C:\ drive. Since the C:\ drive is most commonly associated with the operating system volume, it may be helpful to exclude the "C:\" records from LNK file and jump list processing to more quickly focus on the records referencing removable media.

Include LNKs without VSN

The Include LNKs without VSN option controls whether USB Detective will include the LNK file and jump list records that do not contain an embedded VSN. Since the activity reflected by LNK files and jump lists records is commonly correlated to a specific device based on volume serial number (VSN), excluding LNK files and jump list records without an embedded VSN can be helpful to more quickly focus on the records referencing removable media and reduce the "noise" caused by a large number of records referencing network shares and other locations.

Process ShellBags

The Process ShellBags option controls whether USB Detective will process and include shellbags identified from provided UsrClass.dat registry hives in the results.

Include All ShellBags in Results

The Include All ShellBags in Results option controls whether USB Detective will include shellbags referencing the C:\ volume and those without drive letters in the results. If this option is not selected, the interacted directories category of data within USB Detective will only include shellbags that reference drive letters other than C:\. As an example, a reference to the directory "F:\Work\Documents\" would be included when this option is not selected. However, shellbag references to "C:\Work\Documents" would be excluded if this option is not selected.

Time Zone Options

Displayed Time Zone

The displayed time zone drop-down box allows the user to manually select the time zone offset that will be applied to all UTC timestamps displayed by USB Detective.

Automatically Set Based on SYSTEM Registry Hive

When checked, the "Automatically Set Based on SYSTEM Registry Hive" option instructs USB Detective to adjust the displayed time zone based on the time zone setting specified in the

CurrentControlSet\Control\TimeZoneInformation subkey of the SYSTEM registry hive. The displayed time zone is identified in the column headers of the First Connected, Last Connected, and Last Disconnected columns of the Results Grid.

Interpret Local Timestamps using Displayed Time Zone Setting Specified Above

When checked, the "Interpret Local Timestamps using Displayed Time Zone Setting Specified Above" option instructs USB Detective to interpret any local-time timestamps, such as those in the setupapi log, using the displayed time zone. This option allows the user to normalize the local-time timestamps with the UTC timestamps, which enables them to be included in consistency level calculations. If this option is not checked, local-time timestamps will not be included in consistency level calculations and will have "LT" appended to them.

Consistency Level Options

Display Consistency Levels

The Display Consistency Levels option controls whether the consistency level highlighting will be shown in the Results Grid.

Consistency Level Threshold

The consistency level threshold value controls the number of seconds that two timestamps can be apart and still be counted the same for consistency level calculations. For example, if the consistency level threshold is set to 10 seconds and two potential first connected timestamps for a device are 9 seconds apart, they will be counted the same in consistency level calculations. The 9 second difference will not reduce the displayed consistency level of the data point being calculated.

It is common to see a small variance in two timestamps often used for demonstrating the same data point, such as the first connected time. For example, the date/time located in the SYSTEM\CurrentControlSet\Enum\USBSTOR\{S/N}\ Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0064 subkey of applicable systems is not always the exact same date/time recorded in the setupapi log as the installation time for the associated device driver. It can be helpful to allow an acceptable level of variance in timestamps intended to represent the same data point in order to efficiently identify timestamps that have more significant differences in queried values.

Consistency Level Colors

The color associated with each consistency level (and that is displayed in the Results Grid) can be changed using the available color palette. Use the "Reset to Default Colors" button to revert the consistency level colors to the original colors.

Acknowledgments

USB Detective utilizes the following components for various functionality offered by the software:

- ClosedXML GitHub repository Copyright © 2016 ClosedXML, licensed under the MIT License.
- DiscUtils GitHub Repository Copyright © 2008-2011, Kenneth Bell and © 2014 Quamotion, licensed under the MIT License.
- JumpList GitHub repository Copyright © 2016 Eric Zimmerman, licensed under the MIT license.
- Lnk GitHub repository Copyright © 2016 Eric Zimmerman, licensed under the MIT license.
- Registry GitHub repository Copyright © 2015 Eric Zimmerman, licensed under the MIT License.
- TimeZoneNames GitHub repository Copyright © 2014 Matt Johnson, licensed under the MIT License.
- wyUpdate GitHub Repository Copyright © 2017 wyDay, licensed under the BSD 2-Clause License.

Your use of USB Detective for commercial or business purposes acknowledges that you have read, understood, and agree to be bound by and comply with the USB Detective License Agreement.

Changelog

Version 1.6.2

- ADD: Support for identification of exFAT volumes and parsing exFAT VSNs, when available in the Microsoft-Windows-Partition\Diagnostic event log. exFAT VSNs will also be correlated to any available LNK files and jump lists.
- ADD: Details about additional device MBRs and VBRs (when available) from the Microsoft-Windows-Partition\Diagnostic event log are now included in the verbose view.
- CHANGE: Auxiliary reports (accessed files, interacted directories, timeline) can now be created even when no USB devices are identified.
- CHANGE: The Results Grid will now display the most common Volume Name identified for a device (when multiple volume names are identified). Previously, the occurrence count was not used in displaying the volume name.
- CHANGE: Improved handling of non-removable devices.
- CHANGE: Various UI enhancements throughout.
- FIX: Resolved issue where certain iPhones were not properly identified in Windows XP.
- FIX: Resolved issue where the source file path of files accessed of a USB device listed in the Verbose Details was missing.

Version 1.6.1

- ADD: Support for the Microsoft-Windows-Storsvc/Diagnostic event log.

- ADD: Non-removable (i.e. internal) disks can now be optionally included in the results. To enable this non-default option, select “Include Non-Removable Devices in Results” in the Tools > Options window.
- ADD: Support for ‘SCSI’ subkey of ‘DeviceMigration’ subkey hierarchy, which includes Storport devices and non-removable devices (when enabled).
- ADD: Default artifact storage locations now available via “?” button in the Select Files/Folders processing window.
- CHANGE: Automatic check for updates is now enabled. This option can be disabled via Tools > Options.
- CHANGE: Various logging enhancements throughout.
- FIX: Resolved issue where the wrong timezone abbreviation could be displayed in the Results Grid column header when multiple timezone settings were identified and the “leave in stored format” option was selected during processing.

Version 1.6.0

- ADD: Support for processing and reporting on ShellBags from Vista+ systems. See here for more detail.
- ADD: Processing Statistics window is now available for viewing on-demand after processing completes via the View > Processing Statistics menu option.
- CHANGE: Improved handling of certain jump lists where the DestList path field does not include a real file path.
- CHANGE: By default, all timestamps are now displayed in UTC (including those in the USB Detective log). To dynamically adjust the displayed timezone, reference the Time Zone Options available in Tools > Options. Use the “Log in UTC” option under the General Options available in Tools > Options to control whether the USB Detective log displays its records in UTC.
- CHANGE: Various UI enhancements throughout.

Version 1.5.4

- CHANGE: Hostname and Network Share Name are now included in Opened/Accessed Files section of the Results Grid report when the “Include LNKs Without VSN” option is enabled. Since enabling this option will cause LNK and jump list references to network shares to be included, the Hostname and Network Share Name are added as additional fields to provide more context to the report record. When creating a timeline report that includes opened/accessed files, the Network Share Name is listed in the Description column of the timeline.
- CHANGE: Various small UI enhancements.
- FIX: Resolved issue where the “Include LNKs Without VSN” option would not be applied to certain jump list records.

Version 1.5.3

- CHANGE: Improved correlation of devices located only in the ‘DeviceMigration’ subkey hierarchy (i.e. removed by a Windows feature update and not connected again).
- CHANGE: Improved correlation of certain UIDs associated with generic USB disks.
- CHANGE: Improved handling of LNK and jump list record deduplication.
- CHANGE: Improved handling of jump list records that do not have an embedded VSN but may associated with a removable device.

- CHANGE: The "Include LNKs without VSN" option now applies to jump list records as well.
- CHANGE: The "Include Opened/Accessed Files" Results Grid reporting option now defaults to including all LNK file and jump list records, regardless of whether they are associated with a known device.

Version 1.5.2

- FIX: Resolved issue preventing some hives from being processed when no transaction logs were provided.
- FIX: Resolved issue preventing some SYSTEM and SOFTWARE hives located in a Windows.old directory from being identified when the logical drive or live system processing option was chosen.

Version 1.5.1

- ADD: Option to exclude LNK file system timestamps after a specified date when processing files/folders. When enabled, this option ignores LNK file system timestamps (not embedded content) that occur on or after the specified date. This can be useful when providing USB Detective with carved LNK files that do not have reliable file system timestamps and should not be included in a timeline report. See here for more detail.
- ADD: Option to show/hide the log pane.
- ADD: Option to show/hide the consistency-level legend.
- CHANGE: If transaction logs are replayed against a provided hive, the primary hive is now processed again without replaying the transaction logs. This helps to avoid a scenario where a pending change in the transaction logs removes information related to USB devices.
- CHANGE: Various small UI improvements.
- FIX: Resolved issue in the timeline report that caused some timestamps from the Partition/Diagnostic event log to be displayed in UTC instead of their timezone-adjusted value.

Version 1.5.0

- ADD: Support for processing and correlation of LNK files and jump lists. See here for more detail.
- ADD: Reporting features for opened/accessed file as identified by LNK files and jump list records.
- ADD: Log entry added to document internal devices that are excluded from the results.
- CHANGE: Improved support for identifying certain Apple device drivers and descriptions from the Enum\USB subkey.
- CHANGE: Improved handling of devices with all zeroes listed as their S/N.
- CHANGE: Improved handling of duplicate device timestamps found in the Enum\USB subkey hierarchy across multiple SYSTEM hives.
- CHANGE: Various reporting improvements, including auto-formatting Excel spreadsheets as tables and removing “USB Detective” from tab names in reports.
- CHANGE: Various UI improvements.
- FIX: Resolved issue that caused reports to be saved in the current directory of USB Detective instead of the directory specified in the Reports window in some instances.

Version 1.4.1

- ADD: Option to append timeline report as an additional worksheet in the Results Grid Excel report.
- ADD: "Check All" button added to Create Report window. Allows a user to quickly select all options and create all available report types.
- CHANGE: Device timeline report now saved to the USB Detective case folder instead of the directory from which USB Detective is running.
- CHANGE: Improved handling of the Microsoft-Windows-Kernel-PnP\Configuration event log.
- CHANGE: Improved handling of devices identified in the DeviceContainers subkey.

Version 1.4.0

- ADD: Support for processing live systems. All supported artifacts, including VSCs, are included in live system processing. See here for more details.
- ADD: Ability to create per-device timeline reports. See here for more details.
- ADD: Ability to check for software updates via Help > Check for Updates.
- ADD: Ability to detect certain types of device or volume encryption when the raw MBR or VBR is available. See here for more details.
- ADD: Option to set/change the case folder from the Set/Change Case Details window.
- CHANGE: Improved handling of partially corrupt event logs.
- CHANGE: Improved correlation of data from DeviceMigration subkeys.
- ADD: DiskId now parsed from DeviceMigration subkeys, when present.
- CHANGE: Various small UI improvements.

Version 1.3.6

- CHANGE: Improved correlation of composite devices listed in the Enum\USB subkey hierarchy. This helps to remove "duplicate" entries in the Results Grid that are referring to the same device.
- FIX: Resolved issue where some Storport devices were listed with their ParentIdPrefix in the Results Grid instead of their serial number.
- FIX: Resolved issue with the auto-save log being named with the incorrect month when the default log name was not changed.

Version 1.3.5

- ADD: Official support for Storport drives.
- ADD: Support for the {2accfe60-c130-11d2-b082-00a0c91efb8b} DeviceClasses subkey from SYSTEM hive.
- ADD: Improved correlation of storport and other external drives with the Windows Portable Devices subkey. The volume name/label of storport drives is now pulled from WPD.
- ADD: Support for identifying multiple volume names for a single device located in the Windows Portable Devices subkey.
- ADD: Support for Enum\SCSI subkey.
- ADD: Ability to change case name/evidence number via Tools > Set Case Details.
- ADD: Support for "Case Folder" functionality. The Case Folder is the location where the log will be auto-saved (when this option is selected) and the default location for saving reports.
- ADD: "Processing Statistics" window now displayed post-processing.

- ADD: Option to auto-save the USB Detective log. The log file is saved to the Case Folder (when one is entered) or the current directory of USB Detective.
- ADD: Ability to customize the consistency-level highlighting via Tools > Options.
- ADD: Ability to disable the consistency-level highlighting in the Results Grid via Tools > Options.
- ADD: USB Device Setup Class now pulled from System event log.
- CHANGE: Previous versions of the Enum\USB subkey hierarchy timestamps are now checked for reliability using the methodology described here.
- CHANGE: Improved correlation leveraging the DeviceContainers subkey.
- CHANGE: Improved handling of timestamps added to "Other Connection Times" and "Other Disconnection Times".
- CHANGE: Improved correlation for USB composite devices.
- CHANGE: Improved parsing of Partition/Diagnostic event log in Windows 10.
- CHANGE: Various small UI improvements.
- FIX: Resolved issue that caused some timestamps from setupapi logs to be converted using the displayed time zone settings (instead of being left in local time).
- FIX: Resolved issue that caused an error to be displayed in the Select Logical Drive window when no logical drives were available for processing.

Version 1.3.0

- ADD: Support for processing and including artifacts from volume shadow copies.
- CHANGE: Last drive letter and timezone offset now included in Timeline report.
- CHANGE: Last Connected cell in the Results Grid will now display timestamps consistent with the first connection after last reboot if no last connected timestamps for the device are available. When this occurs, a note is added to the tool tip for the Result Grid cell displaying the timestamp. If any last connected timestamps are identified, the first connect after last reboot timestamps are only available in verbose mode and the Timeline Report as they were in previous versions.
- CHANGE: Various small UI improvements.
- FIX: Various small bug fixes.

Version 1.2.0

- ADD: Support for replaying transaction logs. See here for more details.
- ADD: Ability to specify the case name and evidence number for the data set being processed. The case name/evidence number is displayed in the title bar as well as prepended to the report file names.
- CHANGE: Improved support for ambiguous devices identified in DriverFrameworks-UserMode/Operational event log.
- CHANGE: Various UI improvements.
- FIX: Resolved issue that prevented some Windows Vista hives from being processed.

Version 1.1.7

- ADD: Option to include operating system installation time(s) in the timeline report.
- ADD: Ability to save multiple device VBRs and MBRs, when available. This option is available via the Results Grid context menu.
- ADD: Option to include ambiguous devices in the results (see description above). Any ambiguous devices identified are logged in the USB Detective log regardless of whether this setting is enabled.

- ADD: Option to change USB Detective internal log to UTC timestamps instead of local.
- CHANGE: Improved parsing of USB Attached SCSI (UASP) devices throughout.
- CHANGE: Improved support for MTP and UASP devices that have been deleted via Windows 10 device cleanup.
- CHANGE: Improved exclusion of unreliable timestamps in Enum\USB hierarchy. Now supports multiple timestamps that are repeated.
- CHANGE: Improved correlation of devices identified only by disk ID in the event logs.
- CHANGE: Improved parsing of MTP devices from event logs.
- CHANGE: Various UI improvements.
- FIX: Resolved issue in parsing some UMB devices from Windows 8.1 setupapi logs.

Version 1.1.6

- ADD: Detection of multiple disk signatures for a device from event logs. Multiple disk signatures may be available for a device if the device was formatted and re-connected to the system.
- ADD: Detection of the partition style (MBR or GPT) from event logs.
- ADD: Detection of multiple volume GUIDs for a device, which may be available for a device is the device was formatted and re-connected to the system.
- CHANGE: Improved support for mounted forensic images (logical drive option), including X-Ways Forensics mounting and FTK Imager mounting.
- CHANGE: Improved correlation of disk signature for fixed devices in MountedDevices subkey. Allows for identification of multiple drive letters once associated with a fixed USB device.
- CHANGE: Improved correlation of removable drives in MountedDevices subkey. Allows for identification of multiple drive letters once associated with a removable USB device.
- CHANGE: Improved setupapi log parsing for fixed devices. Records identifying a device by disk ID can now be parsed if the disk ID is already known. This can increase the number of connection times associated with a device.
- CHANGE: Improved detection of MTP devices in setupapi logs.
- CHANGE: Improved handling of corrupt event logs.
- CHANGE: Improved handling of corrupt and partially corrupt SOFTWARE hives.
- CHANGE: Various small UI enhancements.

Version 1.1.5

- ADD: Report creation revamped. All report creation and options now available in Report > Create Report window. Allows for multiple report types and formats to be created simultaneously.
- ADD: Checks for unreliable timestamps before populating results. If a timestamp is deemed unreliable, it is logged and excluded from the results. See details above.
- ADD: Time zone abbreviation added to timestamp column headers.
- ADD: Button to copy value in SYSTEM Hive(s) text box to all other text boxes in Select Files/Folders window.
- CHANGE: Improved sorting speed in results grid.
- CHANGE: Various UI enhancements.
- FIX: Resolved issue that caused some tool tip information to not be displayed.
- FIX: Resolved issue that caused some VSNs to be displayed in Big Endian.
- FIX: Various small bug fixes.

Version 1.1.0

- ADD: Event log support. The following event logs are supported for Windows 7-10 (where enabled):
    - System – exposes additional connection times and devices.
    - Microsoft-Windows-DriverFrameworks\UserMode – exposes additional connection/disconnection times and devices.
    - Microsoft-Windows-Kernel-PnP\Configuration – exposes additional connection times, deletion times, and devices.
    - Microsoft-Windows-Partition\Diagnostic – exposes additional connection/disconnection times, devices, device volume boot records, and much more.
- ADD: Ability to save device volume boot record and master boot record for interpretation in other tools (Note: USB Detective parses information from these for correlation/reporting as well).
- ADD: Option to include device deletion times in Timeline Report.
- ADD: Option to show 64-bit VSNs (when available).
- CHANGE: Improved correlation for external hard drives by leveraging information available in event logs with registry-based data.
- CHANGE: "Other Details" column removed from Results Grid. All information previously available in this column is now available in the Verbose Details view.
- CHANGE: Various UI improvements.
- FIX: Resolved issue that prevented the results grid from being displayed when certain non-English time zones were identified in the provided SYSTEM hive and the option to adjust timestamps based on the SYSTEM hive was enabled.
- FIX: Various small bug fixes.

Version 1.0.4

- CHANGE: Improved corrupt data handling throughout, including registry hives where the hive signature is in tact but core key hierarchies within the hive are corrupt or missing.
- CHANGE: "View Other Connection Times" context menu option is now disabled if there are no other connection times available for the selected device.
- CHANGE: Improved support for Windows XP setupapi logs with alternative formatting.
- CHANGE: Boot volume of system on which USB Detective is running is no longer shown in the logical drive down-down list.

Version 1.0.3

- ADD: Export to Timeline added to Reporting options.
- CHANGE: Timestamps with the same date, hour, minute, and second now deduplicated from the list of other connection and disconnection times. Timestamps in these lists were previously deduplicated based on entire FILETIME value.

Version 1.0.2

- ADD: Previous connection and disconnection times now available in verbose details or via "View Other Connection Times" context menu option.
- CHANGE: Additional timestamps now evaluated in first connected, last connected, and last disconnected consistency level calculations.

- CHANGE: First Connected, Last Connected, and Last Disconnected columns of Results Grid are now sortable by date.
- FIX: Resolved issue that prevented the value of a results grid cell from being updated via the “Change Displayed Value” feature after it had been cleared.

Version 1.0.1

- FIX: Resolved issue with some non-US local system cultures encountering errors during timestamp parsing.

Version 1.0.0

- Initial Release