Tool Validation Report
USB Connections

Registry Explorer
Version 2.0.0.0

Released: 30 April 2023

KHYRENZ
LIMITED

Contents

Executive Summary

The System, Software, and NTUSER.DAT hive within the test image Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01[1] were loaded into Registry Explorer using the option:

File → Load hive → <select hive>

None of the hives were identified as 'dirty' by Registry Explorer.

The below table is a summary of the USB connection data that Registry Explorer plugins extracted from this image. Analysis of the raw Registry data was not performed; much more data could be accessed and analysed using the tool in this way.

USB Make/Model	S/N	Volume Name	Mounted As	Connection Timestamps	Disconnection Timestamps
VendorCo ProductCode	✓	✓	-	✓	✓
Samsung SSD T7 (SCSI)	(MSFT30 not removed)	✓	-	✓	✓
SPECIFIC STORAGE_DEVICE	✓	✓	-	✓	✓
General UDisk	✓	-	✓	✓	✓
Generic	✓	✓	×	✓	-
Total	**4/5**	**4/4**	**1/2**	**8/8**	**4/4**
Percentage	**80%**	**100%**	**50%**	**100%**	**100%**

As this table shows, the majority of the available artefacts were recovered exactly Exceptions were that the serial number of the one connected SCSI device was recovered as per the Registry key name rather than removing the MSFT30 prefix, and one of the last know drive letters (for the Generic Flash Drive) was not recovered. This particular drive letter was in value slack space.

Introduction

Khyrenz Ltd is a Digital Forensic consultancy based in the UK. We provide this report to document our tool validation process against the Registry Explorer GUI application, specifically with respect to USB connection artefact plugins.

Scope

This report documents the results obtained by evaluating only the USB connection artefact plugin capabilities within Registry Explorer, version 2.0.0.0, against the System, Software, and NTUSER.DAT Registry hives within the image file: Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01. Capability within Registry Explorer to view the raw Registry data was not evaluated.

The image file, as well as a full list of the actual artefacts to be extracted from this image, are provided at: https://www.khyrenz.com/resources/.

Registry Explorer 2.0.0.0 was downloaded from https://ericzimmerman.github.io/ and run with Administrator privileges on a Windows 10 Professional 22H2 system. The following plugins were accessed relating to USB connection artefacts:

USB – SYSTEM\ControlSet001\Enum\USB

USBSTOR – SYSTEM\ControlSet001\Enum\USBSTOR

SCSI – SYSTEM\ControlSet001\Enum\SCSI

MountedDevices – SYSTEM\MountedDevices

Windows Portable Devices – SOFTWARE\Microsoft\Windows Portable Devices

The default configuration of the application was used.

Measuring Test Results

How well the tool performed against expected results is determined purely by whether the tool returns an exact match to the value requested. Where at least one plugin returned an exact match, this was deemed a successful result.

Test Data

Test Image Creation Process

A clean Windows 11 Professional virtual machine was created and a number of different USB devices were connected according to a test plan.

A logical E01 image of the virtual machine was generated using FTK Imager 4.2.0.13[2].

USB Connection Summary

A summary of the expected USB connection artefacts to be extracted is provided in Appendix 1 – USB Artefacts within Test Image.

Test Results

The tables below show the USB connection artefacts extracted from the test image by Registry Explorer.

USB plugin

Timestamp	Key Name	Serial Number	Parentid Prefix	Service	Device Name
2023-03-04 16:36:36	VID_04E8&PID_4001	MSFT30S5TANK0N502382A	7&26c0ac83&0	UASPStor	USB Attached SCSI (UAS) Mass Storage Device
2023-03-04 18:08:48	VID_058F&PID_6387	EFC74121		USBSTOR	USB Mass Storage Device
2023-03-04 17:34:22	VID_1F75&PID_0918	60875343		USBSTOR	USB Mass Storage Device
2023-03-04 18:43:31	VID_ABCD&PID_1234	6&30c5d09c&0&6	7&f810be1&0	USBSTOR	USB Mass Storage Device
2023-03-04 16:11:36	VID_FFFF&PID_5678	7918331133733033		USBSTOR	USB Mass Storage Device

USBSTOR plugin

Serial Number	Device Name	First Installed	Last Connected	Last Removed
7&f810be1&0&_&0	General UDisk USB Device	2023-03-04 17:55:41	2023-03-04 18:43:31	2023-03-04 19:29:47
EFC74121&0	Generic Flash Disk USB Device	2023-03-04 18:08:48	2023-03-04 18:08:48	
60875343&0	Specific STORAGE DEVICE USB Device	2023-03-04 17:19:12	2023-03-04 17:34:22	2023-03-04 17:47:08
79183311337330 33&0	VendorCo ProductCode USB Device	2023-03-04 16:11:36	2023-03-04 16:11:36	2023-03-04 16:34:07

SCSI plugin

Serial Number	Device Name	First Installed	Last Connected	Last Removed
7&26c0ac83&0&000000	Samsung PSSD T7 SCSI Disk Device	2023-03-04 16:36:36	2023-03-05 23:44:59	2023-03-05 23:47:40

MountedDevices plugin

Device Name	Device Data
\DosDevices\E:	_??_USBSTOR#Disk&Ven_General&Prod_UDisk&Rev_5.00#7&f810be1&0&_&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Windows Portable Devices plugin

Device	Serial Number	Friendly Name
DISK&VEN_GENERAL&PROD_UDISK&REV_5.00	7&F810BE1&0&_&0	E:\
DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07	EFC74121&0	HEDGEHOG
DISK&VEN_SPECIFIC&PROD_STORAGE_DEVICE&REV_0009	60875343&0	BAND
DISK&VEN_VENDORCO&PROD_PRODUCTCODE&REV_2.00	7918331133733033&0	ROSE
		T7

Combined information from plugins

USB Make/Model	iSerialNumber / Serial Number	Volume Name	Mounted As	Connection Timestamps	Disconnection Timestamps
VendorCo ProductCode USB Device*	7918331133733033§ 7918331133733033&0*†	ROSE†		2023-03-04 16:11:36*	2023-03-04 16:34:07*
Samsung PSSD T7 SCSI Disk Device‡	MSFT30S5TANK0N502382A§ 7&26c0ac83&0&000000‡	T7†		2023-03-04 16:36:36‡ 2023-03-05 23:44:59‡	2023-03-05 23:47:40‡
Specific STORAGE DEVICE USB Device*	60875343§ 60875343&0*†	BAND†		2023-03-04 17:19:12* 2023-03-04 17:34:22*	2023-03-04 17:47:08*
General UDisk USB Device*	6&30c5d09c&0&6§ 7&f810be1&0&_&0*		E:**†	2023-03-04 17:55:41* 2023-03-04 18:43:31*	2023-03-04 19:29:47*
Generic Flash Disk USB Device*	EFC74121§ EFC74121&0*	HEDGEHOG†		2023-03-04 18:08:48*	

* USBSTOR plugin
† Windows Portable Devices plugin
‡ SCSI plugin
§ USB plugin
** MountedDevices plugin

Appendix 1 – USB Artefacts within Test Image

* Items in red are not present in the Registry, so would not be extracted using a tool that only analyses the Registry

USB Make/Model	iSerialNumber / Serial Number	Volume Name	Volume Serial Number	Mounted As	Connected By	Connection Timestamps	Physical (test plan) Connection Timestamps	Disconnection Timestamps	Physical (test plan) Disconnection Timestamps
VendorCo ProductCode	7918331133733033	ROSE	1AB9-C03E	E:\	user	2023-03-04 16:11:36	2023-03-04 16:11:28	2023-03-04 16:34:07	2023-03-04 16:28:28 (eject fail) 2023-03-04 16:34:00 (eject) 2023-03-04 16:35:04
Samsung SSD T7 (SCSI)	S5TANK0N502382A	T7	EAAE-79DE	E:\ F:\ F:\ F:\	user	2023-03-04 16:36:36 2023-03-04 18:58:48 2023-03-04 20:05:18 2023-03-05 23:44:59	2023-03-04 16:36:28 2023-03-04 18:58:41 2023-03-04 20:05:03 2023-03-05 23:44:50	 2023-03-05 23:47:40	2023-03-04 17:32:35 2023-03-04 19:21:28 (eject) 2023-03-04 19:22:48 - 2023-03-05 23:47:31
SPECIFIC STORAGE_DEVICE	60875343	BAND	EC2C-F4E0	F:\ F:\	user	2023-03-04 17:19:12 2023-03-04 17:34:22	2023-03-04 17:19:05 2023-03-04 17:34:14	- 2023-03-04 17:47:08	2023-03-04 17:33:54 2023-03-04 17:47:00 (eject) 2023-03-04 17:53:23
General UDisk	7&f810be1 (non-unique)	USB Drive	0201-0BAD	E:\ E:\	user	2023-03-04 17:55:41 2023-03-04 18:43:31	2023-03-04 17:55:34 2023-03-04 18:43:23	- 2023-03-04 19:29:47	- 2023-03-04 19:29:40
Generic Flash Disk	EFC74121	HEDGE HOG	08C1-D2C1	F:\	user	2023-03-04 18:08:48	2023-03-04 18:08:40		-

[1] https://www.khyrenz.com/resources/
[2] https://www.exterro.com/ftk-imager