Tool Validation Report
USB Connections

RegRipper
Version 3.0

Released: 6 May 2023

KHYRENZ
LIMITED

Contents

Executive Summary

RegRipper 3.0 was run against the System Registry hive that was extracted from the test image Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01[1].

The below table is a summary of the USB connection data that RegRipper extracted from this image.

USB Make/Model	S/N	Connection Timestamps	Disconnection Timestamps
VendorCo ProductCode	✓	✓	✓
Samsung SSD T7 (SCSI)	(MSFT30 not removed)	✓	✓
SPECIFIC STORAGE_DEVICE	✓	✓	✓
General UDisk	(&0 ending not removed)	✓	✓
Generic	✓	✓	-
Total	**3/5**	**8/8**	**4/4**
Percentage	**60%**	**100%**	**100%**

As this table shows, of the artefacts supported by RegRipper, the majority were extracted exactly by a combination of the available plugins.

Introduction

Khyrenz Ltd is a Digital Forensic consultancy based in the UK. We provide this report to document our tool validation process against RegRipper, specifically with respect to USB connection artefacts.

Scope

This report documents the results obtained by testing USB connection artefact extraction capability within RegRipper, version 3.0, against the System Registry hive within the image file: Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01. This 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/.

RegRipper 3.0 was downloaded from https://github.com/keydet89/RegRipper3.0 and run on a Windows 10 Professional 22H2 system. The following commands were run, to execute available USB-related plugins and output the results to files:

rip.exe -r SYSTEM -p usb > usb.txt

rip.exe -r SYSTEM -p usbdevices > usbdevices.txt

rip.exe -r SYSTEM -p usbstor > usbstor.txt

rip.exe -r SYSTEM -p devclass > devclass.txt

The default configuration was used; transaction logs were not replayed, as this was not capability that was available using RegRipper. None of the Registry hives within the test image are dirty hives.

Measuring Test Results

How well the tool performs against expected results is determined purely by whether the tool returns an exact match to the value requested.

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 table below shows the USB connection artefacts extracted from the test image by RegRipper.

USB Make/Model	iSerialNumber / Serial Number	Connection Timestamps	Disconnection Timestamps
VendorCo ProductCode	7918331133733033&0[41] 7918331133733033[32]	2023-03-04 16:11:36[431]	2023-03-04 16:34:07[4] 2023-03-04 16:35:12[3]
-	MSFT30S5TANK0N5023 82A[3]	2023-03-04 16:36:36[3] 2023-03-05 23:44:59[3]	2023-03-05 23:47:40[3]
SPECIFIC STORAGE_DEVICE	60875343&0[41] 60875343[32]	2023-03-04 17:19:12[431] 2023-03-04 17:34:22[43]	2023-03-04 17:47:08[4] 2023-03-04 17:53:30[3]
General UDisk	7&f810be1&0&_&0[41] 6&30c5d09c&0&6[32]	2023-03-04 17:55:41[41] 2023-03-04 18:43:31[4]	2023-03-04 19:29:47[4]
Generic	EFC74121&0[41] EFC74121[32]	2023-03-04 18:08:48[431]	-

[1] Output by RegRipper devclass plugin
[2] Output by RegRipper usbdevices plugin
[3] Output by RegRipper usb plugin
[4] Output by RegRipper usbstor 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