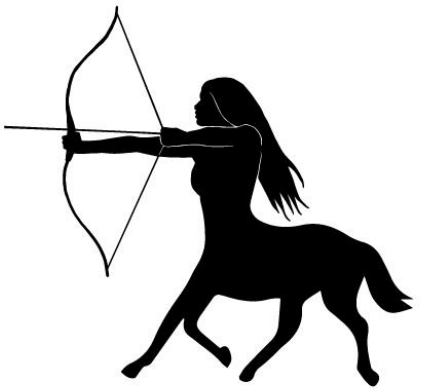
Tool Validation Report
USB Connections

parseUSBs
Version 1.4.4

Released: 30 October 2024



KHYRENZ
LIMITED

Contents

Executive Summary

The test image Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01[1] was mounted using Arsenal Image Mounter 3.11.282[2]. The tool parseUSBs[3] was then run against this mounted volume.

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

USB Make/Model	S/N	Volume Name	Mounted As	Connected By	Connection Timestamps	Disconnection Timestamps
VendorCo ProductCode	✓	✓	-	✓	✓	✓
Samsung SSD T7 (SCSI)	✓	✓	✓	-	✓	✓
SPECIFIC STORAGE_DEVICE	✓	✓	-	✓	✓	✓
General UDisk	✓	-	✓	✓	✓	✓
Generic	✓	✓	-	✓	✓	-
Total	**5/5**	**4/4**	**2/2**	**4/4**	**8/8**	**4/4**
Percentage	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

As this table shows, the available artefacts were recovered exactly.

In addition, all extra connection and disconnection timestamps that were in the Event Logs for these devices were found.

Introduction

Khyrenz Ltd is a Digital Forensic consultancy based in the UK. We provide this report to document our tool validation process against the parseUSBs python script.

Scope

This report documents the results obtained by evaluating the parseUSBs script version 1.4.4 against the image file: Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01.

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/.

The parseUSBs script was downloaded from https://github.com/khyrenz/parseusbs and run using WSL on a Windows 11 Professional 23H2 system. The following command was run against the image mounted as volume E:/ using Arsenal Image Mounter:

python3 parseUSBs.py -v /mnt/e -o csv

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.

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[4].

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 parseUSBs.

Device Friendly Name	iSerial Number	First Connected	Last Connected	Last Removed	Other Connections	Other Disconnections	Last Drive Letter	Volume Name	Volume Serial Numbers	User Accounts
General UDisk USB Device	7&f810be1	2023-03-04T17:55:41.693602+00:00	2023-03-04T18:43:31.059094+00:00	2023-03-04T19:29:47.869850+00:00			E:\			user
Generic Flash Disk USB Device	EFC74121	2023-03-04T18:08:48.615246+00:00	2023-03-04T18:08:48.583840+00:00		2023-03-04T18:08:48.675600+00:00			HEDGEHOG	08c1d2c1 (FAT32)	user
Specific STORAGE DEVICE USB Device	60875343	2023-03-04T17:19:12.934526+00:00	2023-03-04T17:34:22.244568+00:00	2023-03-04T17:47:08.060974+00:00	2023-03-04T17:19:12.960278+00:00|2023-03-04T17:34:22.273365+00:00	2023-03-04T17:34:01.114069+00:00|2023-03-04T17:47:08.037016+00:00		BAND	ec2cf4e0 (FAT32)||ec2cf4e0 (FAT32)|	user
VendorCo ProductCode USB Device	7918331133733030	2023-03-04T16:11:36.358904+00:00	2023-03-04T16:11:36.358904+00:00	2023-03-04T16:34:07.928854+00:00	2023-03-04T16:11:36.379852+00:00	2023-03-04T16:34:07.910849+00:00		ROSE	1ab9c03e (FAT32)|	user
Samsung PSSD T7 SCSI Disk Device	S5TANK0N502382A	2023-03-04T16:36:36.066416+00:00	2023-03-05T23:44:59.602200+00:00	2023-03-05T23:47:40.328228+00:00	2023-03-04T18:58:50.730045+00:00|2023-03-04T16:36:36.092859+00:00|2023-03-04T18:58:48.885019+00:00|2023-03-04T20:05:18.394655+00:00|2023-03-05T23:44:59.629297+00:00	2023-03-04T17:32:43.182426+00:00|2023-03-04T19:21:35.851362+00:00|2023-03-05T23:47:39.317173+00:00	F:\	T7	eaae79de (ExFAT)||eaae79de (ExFAT)||eaae79de (ExFAT)|eaae79de (ExFAT)||	

Appendix 1 – USB Artefacts within Test Image

* Items in red are not present in the artifacts parsed.

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	2023-03-04 17:32:43 2023-03-04 19:21:35 2023-03-05 23:47:39 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 17:34:01 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://arsenalrecon.com/downloads
[3] https://github.com/khyrenz/parseusbs
[4] https://www.exterro.com/ftk-imager