Tool Validation Report
USB Connections

Partition%4DiagnosticParser
Version 1.4

Released: 24 November 2024

KHYRENZ
LIMITED

Contents

Executive Summary

The test image Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01[1] was mounted using Arsenal Image Mounter 3.11.293[2]. The tool Partition%4DiagnosticParser[3] was then run against this mounted volume.

The below table is a summary of the USB connection data that Partition%4DiagnosticParser extracted from this image.

USB Make/Model	S/N	Connection Timestamps	Disconnection Timestamps	Volume Serial Number
VendorCo ProductCode	✓	✓	✓	✓
Samsung SSD T7 (SCSI)	0.5*	✓	✓	✓
SPECIFIC STORAGE_DEVICE	×	✓	✓	✓
General UDisk	-	✓	✓	-
Generic	×	✓	-	✓
Total	**1.5/4**	**5/10**	**5/8**	**4/4**
Percentage	**37.5%**	**50%**	**62.5%**	**100%**

As this table shows, many of the available artefacts were recovered. However, not all of the connection and disconnection timestamps that were in the Event Logs for these devices were parsed. In addition, more than half of the available device serial numbers that were present in the event log were not parsed by the tool.

* For the Samsung T7, the tool extracted the 'SerialNumber' field, but not the iSerialNumber from the ParentId field. These values are often identical but for this device, they were different (the reverse of each other).

Introduction

Khyrenz Ltd is a Digital Forensic consultancy based in the UK. We provide this report to document our tool validation process against the Partition%4DiagnosticParser tool.

Scope

This report documents the results obtained by evaluating Partition%4DiagnosticParser version 1.4 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 Partition%4DiagnosticParser tool was downloaded from https://github.com/theAtropos4n6/Partition-4DiagnosticParser and run on a Windows 11 Professional 23H2 system. The image was mounted as volume E:/ using Arsenal Image Mounter. The following actions were then taken:

- The file E:\Windows\System32\winevt\Logs\Microsoft-Windows-Partition%4Diagnostic.evtx was copied to the host Desktop folder
- Partition%4DiagnosticParser was launched and the following options selected:
    - Input EVTX File: Desktop\Microsoft-Windows-Partition%4Diagnostic.evtx
    - Full report for all connected devices in the Event Log (selected)
    - Output Report File Location: Desktop
    - Analyze

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 Partition%4DiagnosticParser.

Device Friendly Name	iSerial Number	First Connected (UTC)	Last Connected	Volume Serial Number
General UDisk USB Device		2023-03-04T17:55:41.743783	2023-03-04T18:43:31.088787	
Generic Flash Disk USB Device	□E	2023-03-04T18:08:48.675600	2023-03-04T18:08:48.675600	08c1d2c1
Specific STORAGE DEVICE	0000000005□□	2023-03-04T17:19:12.960278	2023-03-04T17:34:22.273364	ec2cf4e0
VendorCo ProductCode	7918331133733033	2023-03-04T16:11:36.379852	2023-03-04T16:11:36.379852	1ab9c03e
Samsung PSSD T7	A283205N0KNAT5S	2023-03-04T16:36:36.092860	2023-03-05T23:44:59.629297	eaae79de

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/theAtropos4n6/Partition-4DiagnosticParser
[4] https://www.exterro.com/ftk-imager