Tool Validation Report
USB Connections

USB Detective (Trial)
Version 1.6.3

Released: 6 May 2023

KHYRENZ
LIMITED

Contents

Executive Summary

The test image Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01[1] was mounted using Arsenal Image Mounter 3.9.226 using the option:

Mount disk image → <select image> → Open

The resultant logical drive letter provided by Arsenal Image Mounter (E:\) was then analysed in USB Detective 1.6.3 using the option:

File → Select Logical Drive → Logical Drive to Process → <select E:\> → Process Artifacts

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

USB Make/Model	S/N	Volume Name	Volume S/N	Last User	Mounted As	Connection Times	Disconnection Times
VendorCo ProductCode	✓	✓	✓	✓	×	✓	✓
Samsung SSD T7 (SCSI)	✓	✓	✓	-	✓	✓	✓
SPECIFIC STORAGE_DEVICE	✓	✓	×	✓	×	✓	✓
General UDisk	✓×	-	✓	✓	✓	✓	✓
Generic	✓	✓	×	✓	×	✓	-
Total	**6/5**	**4/4**	**3/5**	**4/4**	**2/5**	**10/10**	**4/4**
Percentage	**100%**	**100%**	**60%**	**100%**	**40%**	**100%**	**100%**

As this table shows, many of the available artefacts were recovered exactly. Two volume serial numbers and the drive letter that three devices were connected under were missing in the tool output.

Introduction

Khyrenz Ltd is a Digital Forensic consultancy based in the UK. We provide this report to document our tool validation process against version 1.6.3 of the (trial) USB Detective application, run against a mounted logical disk image.

Scope

This report documents the results obtained by evaluating the USB connection artefacts extracted by USB Detective version 1.6.3, from the image file: Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01. This image file was mounted using Arsenal Image Mounter version 3.9.226 and the resultant mounted logical drive was subsequently analysed using USB Detective.

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/.

USB Detective was downloaded and a trial license obtained from https://usbdetective.com/.

Arsenal Image Mounter was downloaded from https://arsenalrecon.com/downloads/.

Both tools were run on a Windows 10 Professional 22H2 system. The default configuration of both applications 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.

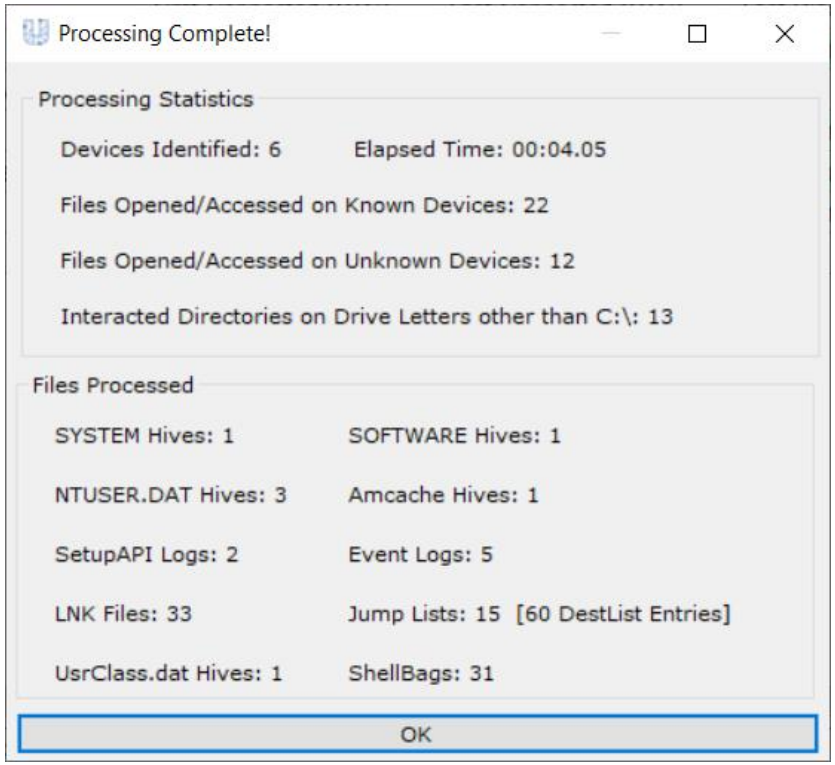
A logical E01 image of the virtual machine was generated using FTK Imager 4.2.0.13[2].

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

USB Detective successfully processed the artefacts shown in the screenshot below.



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

Serial/UID	Description	Connected (UTC)	Disconnected (UTC)	Volume Name/Label	Drive Letter(s)	VSN	Last User
7&f810be1	General UDisk USB Device	2023-03-04 17:55:41 2023-03-04 18:43:31	2023-03-04 19:29:47	E:\	E:	02010BAD	user
EFC74121	Generic Flash Disk USB Device	2023-03-04 18:08:48		HEDGEHOG			user
60875343	Specific STORAGE DEVICE USB Device	2023-03-04 17:19:12 2023-03-04 17:34:22	2023-03-04 17:47:08	BAND			user
7918331133733033	VendorCo ProductCode USB Device	2023-03-04 16:11:36	2023-03-04 16:34:07	ROSE		1AB9C03E	user
S5TANK0N502382A	Samsung PSSD T7	2023-03-04 16:36:36 2023-03-04 18:58:48 2023-03-04 20:05:18 2023-03-05 23:44:59	2023-03-05 23:47:39	T7	F:	EAAE79DE	
6&30C5D09C&0&6	General UDisk	2023-03-04 17:55:43 2023-03-04 18:43:57					

Timestamps shown in the table are primarily those taken from the SYSTEM and NTUSER.DAT Hives, Plug 'n' Play driver log C:\Windows\INF\setupapi.dev.log, and Event Log Microsoft-Windows-Partition/Diagnostic, Event ID 1006.

Appendix 1 – USB Artefacts within Test Image

* Items in red are not present in the Registry, setupapi.dev.log file, Event Logs, or LNK files

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