Tool Validation Report
USB Connections

X-Ways Forensic
Version 20.8

Released: 13 May 2023

KHYRENZ
LIMITED

Contents

Executive Summary

The test image Khyrenz-USBconnKeywordImage-Win11-logical-25GB.E01[1] was loaded into X-Ways Forensics.

The below table is a summary of the USB connection data that the Registry Report feature of X-Ways Forensics extracted from this image.

USB Make/Model	S/N	Volume Name	Mounted As	Connected By	Connection Timestamps	Disconnection Timestamps
VendorCo ProductCode	(&0 not removed)	✓	-	×	✓	✓
Samsung SSD T7 (SCSI)	×	✓	-	✓	1/2	×
SPECIFIC STORAGE_DEVICE	(&0 not removed)	✓	-	×	✓	✓
General UDisk	(&0 not removed)	-	✓	×	✓	✓
Generic	(&0 not removed)	✓	✓	×	✓	-
Total	**0/5**	**4/4**	**2/2**	**-1/4**	**7/8**	**3/4**
Percentage	**0%**	**100%**	**100%**	**ERROR**	**87.5%**	**75%**

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

X-Ways Forensics was also able to successfully extract the last known drive letter for the Generic Flash USB Device, which was in value slack space.

Data regarding connected SCSI devices was either not extracted or unreliable. Somehow X-Ways Forensics was able to connect the T7 SCSI device to the 'user' account without the device's DiskID ever actually appearing in the NTUSER.dat hive. As the Registry Reports do not include the full key paths or names to show where the data was extracted from, it was not possible to investigate this anomaly, so despite the information being factually correct (the T7 device was indeed connected when the 'user' account was logged in), merit cannot be awarded in this instance. In addition, despite all of the other devices' DiskIDs being present in the NTUSER.dat hive under MountPoints2, none were associated to the 'user' account.

Introduction

Khyrenz Ltd is a Digital Forensic consultancy based in the UK. We provide this report to document our tool validation process against X-Ways Forensics version 20.8, specifically with respect to USB connection artefacts extracted using the Registry Reports feature.

Scope

This report documents the results obtained by evaluating only the USB connection artefact extraction capabilities within the Registry Report feature in X-Ways Forensics, version 20.8, which was run against the System, Software, and NTUSER.DAT Registry hives within 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/.

X-Ways Forensics was run with Administrator privileges on a Windows 10 Professional 22H2 system. The following Registry Reports were run relating to USB connection artefacts:

Devices

System

The default configuration of the application was used and no other features within the tool were accessed.

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 Report 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 X-Ways Forensics.

Devices Report

Device	Serial Number	Friendly Name	Mounted As	Connection Timestamps	Disconnection Timestamps
General UDisk USB Device	7&F810BE1&0&_&0	E:\	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&0	HEDGEHOG	F:*	2023-03-04 18:08:48	-
Specific STORAGE DEVICE USB Device	60875343&0	BAND		2023-03-04 17:19:12 2023-03-04 17:34:22	2023-03-04 17:47:08
VendorCo ProductCode USB Device	7918331133733033&0	ROSE		2023-03-04 16:11:36	2023-03-04 16:34:07
Samsung PSSD T7 SCSI Disk Device		T7		2023-03-04 16:36:36	

System Report

Description	Mounted As	Connected By	Connection Timestamp
Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07			2023-03-04 18:08:48
Disk&Ven_General&Prod_UDisk&Rev_5.00	E:\		2023-03-04 17:55:41
Disk&Ven_Specific&Prod_STORAGE_DEVICE&Rev_0009			2023-03-04 17:19:12
Disk&Ven_Samsung&Prod_PSSD_T7		user†	2023-03-04 16:36:36
Disk&Ven_VendorCo&Prod_ProductCode&Rev_2.00			2023-03-04 16:11:36

The ‘user’ entry in the table above has been coloured red because the key that X-Ways Forensics appears to claim to get this information from does not exist in the NTUSER.dat Registry hive, so despite the information being factually correct, the source of the data is unclear. This statement is made under the assumption that ‘Mount History’ in the System Registry Report, which refers to

* Recovered from slack space

† Determined by taking the DiskID from ‘Mount History’ in the System Report and matching to the Windows Portable Devices key information shown in the Devices Report

'\??\C:\Users\user\ntuser.dat' is referring to the Registry key: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2, and that the DiskID listed in the Report (0cd20f15-ba8c-11ed-86fe-000c2968ee15) would be expected as a subkey but is not present. Viewing the raw Registry data in NTUSER.dat and grepping for the DiskID within the hive yielded no results.

Combined information from Registry Reports

Device	Serial Number	Friendly Name	Mounted As	Connected By	Connection Timestamps	Disconnection Timestamps
General UDisk USB Device	7&F810BE1&0&_&0	E:\	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&0	HEDGEHOG	F:\		2023-03-04 18:08:48	-
Specific STORAGE DEVICE USB Device	60875343&0	BAND			2023-03-04 17:19:12 2023-03-04 17:34:22	2023-03-04 17:47:08
VendorCo ProductCode USB Device	7918331133733033&0	ROSE			2023-03-04 16:11:36	2023-03-04 16:34:07
Samsung PSSD T7 SCSI Disk Device		T7		user	2023-03-04 16:36:36	

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