

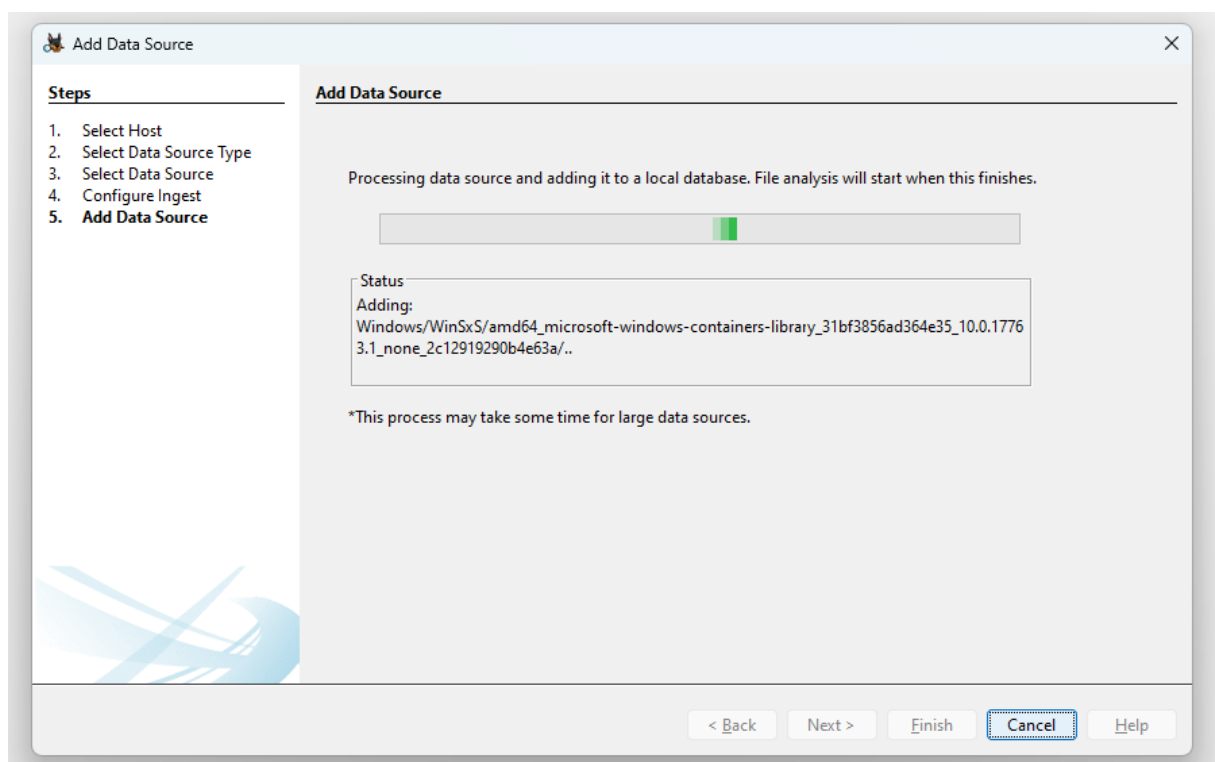
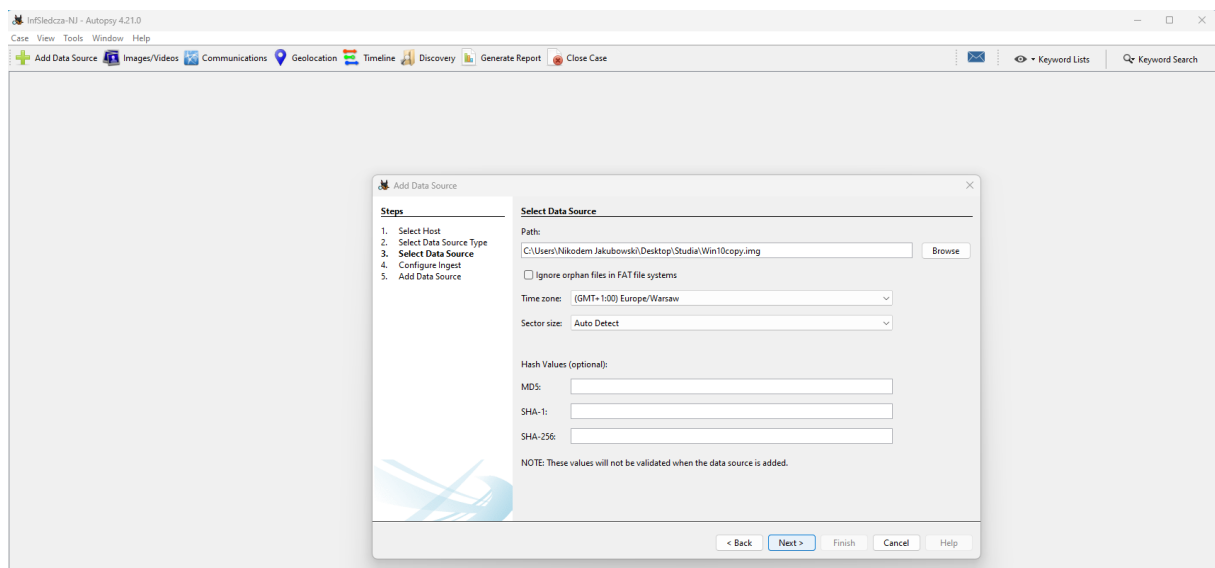
Analiza w Autopsy.

Spis treści

Konfiguracja wstępna.	2
Czym jest Autopsy – notatka.	2
Analiza – opis modułów z nagłówka.....	3
Images/Videos.	3
Communications.....	3
Geolocation.	4
Timeline.	4
Discovery.....	5
Generate Report.	5
Analiza – opis pozostałych, ciekawych modułów.	7
Data Sources - informacje o źródle danych.	7
EXIF Metadata.	7
Encryption Suspected.....	8
Extension Mismatch Detected.....	8
Keyword Hits.....	9
OS Accounts.....	9
File views.	10
Data Artifacts.	10
Score.	11

Konfiguracja wstępna.

Pobrałem program, utworzyłem nową sprawę i dodałem zrzut systemu, który otrzymałem od kolegi (inny student). Skorzystałem ze wszystkich modułów. Poniżej przedstawiam okna konfiguracji.

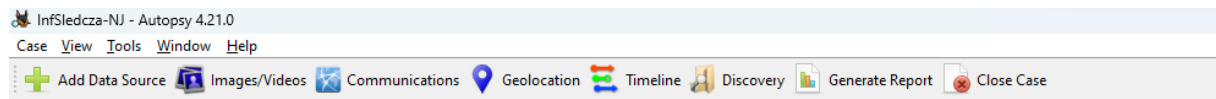


Czym jest Autopsy – notatka.

Sleuth to biblioteka i zbiór narzędzi wiersza poleceń używanych do badania obrazów dysków. Autopsy to GUI dla Sleutha. W Autopsy są wyświetlane wyniki tych analiz, pomagają one zlokalizować odpowiednie sekcje danych w dochodzeniu. Autopsy może być również użyte do odzyskiwania usuniętych danych z urządzeń cyfrowych.

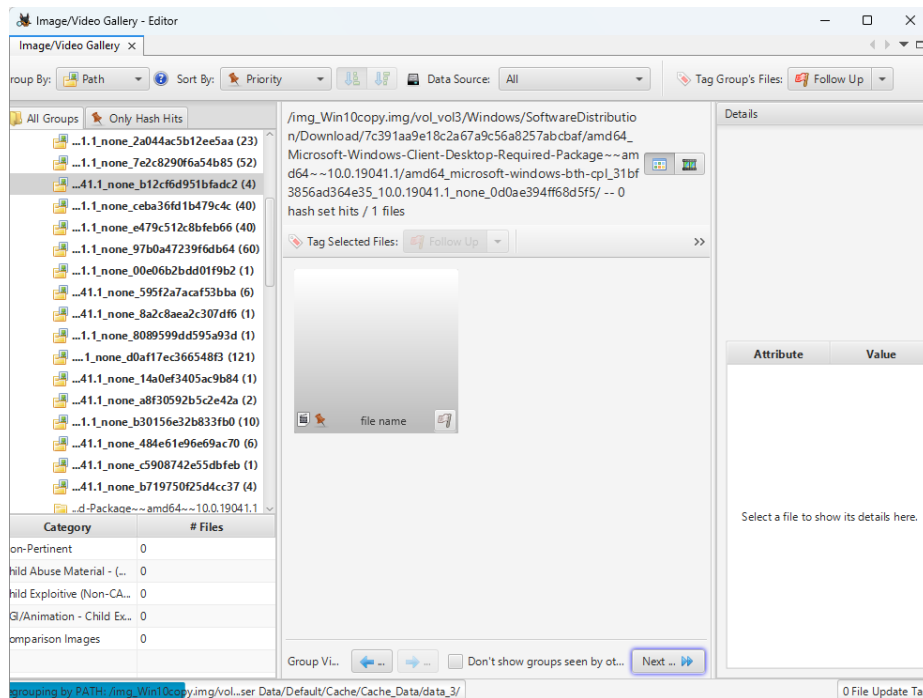
Analiza – opis modułów z nagłówka.

Mam na myśli te moduły, w większości mówią same za siebie, ale sobie przez nie przejdziemy.



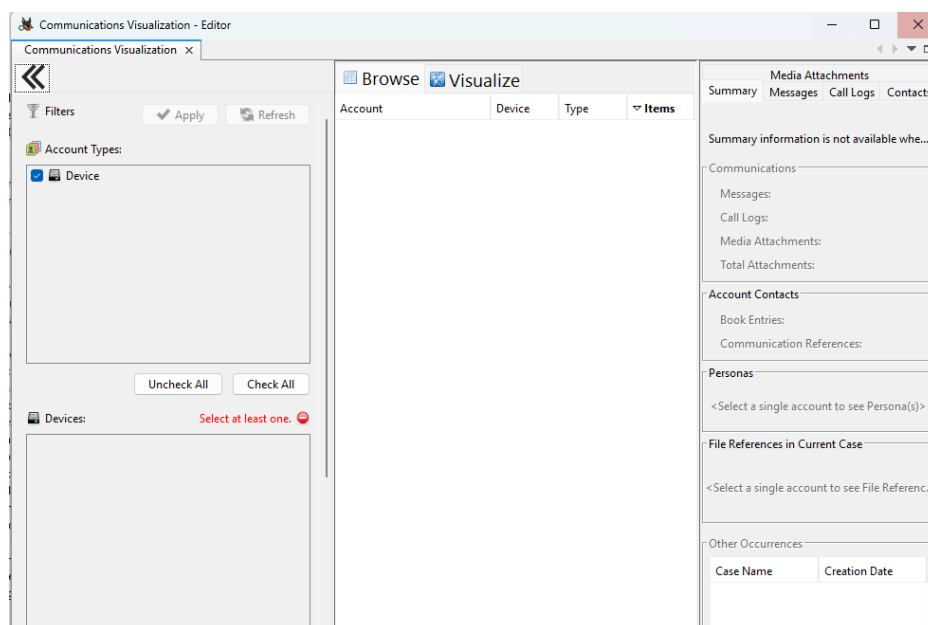
Images/Videos.

Po kliknięciu, w nowym oknie otwiera się eksplorator dedykowany do przeglądania i szukania zdjęć i filmów w całym systemie.



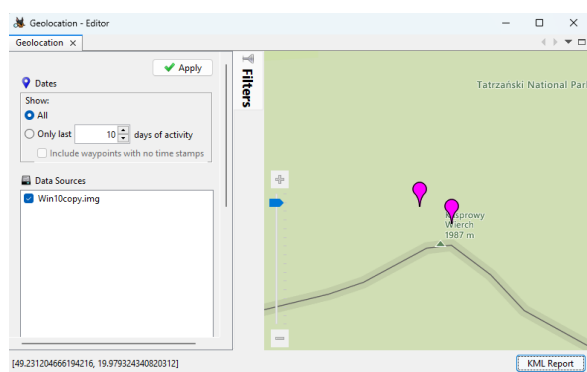
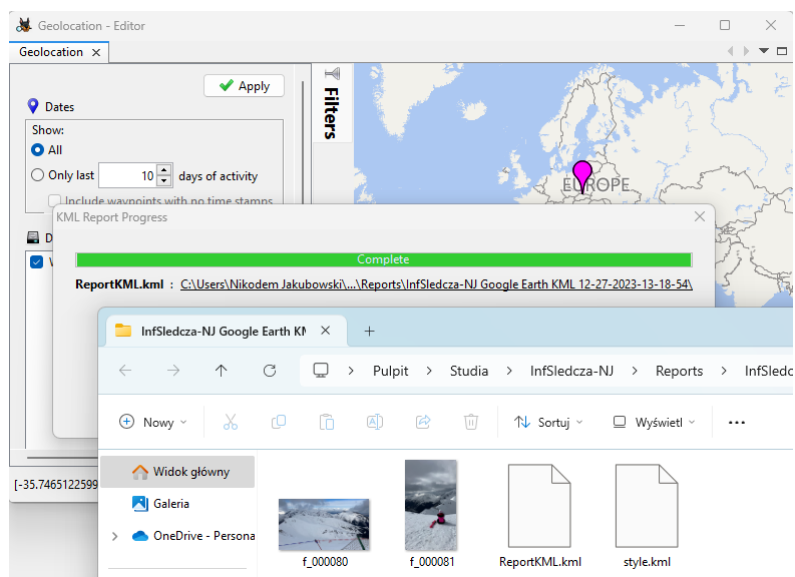
Communications.

Ten zrzut informuje o korelacji systemu z innymi urządzeniami.



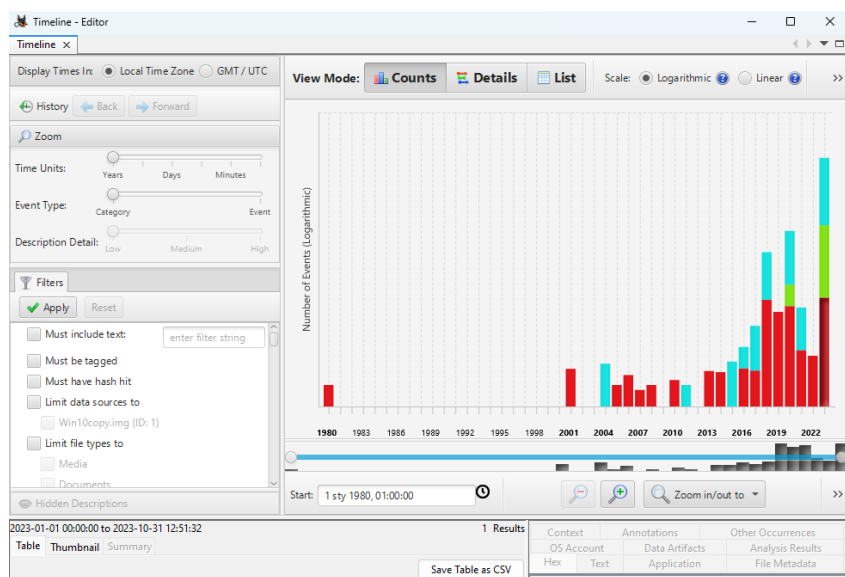
Geolocation.

Nazwa mówi sama za siebie, artefakty związane z lokalizacją. Bardzo podoba mi się ten moduł, Autopsy od razu generuje raport z innymi plikami powiązanymi z tą lokalizacją.



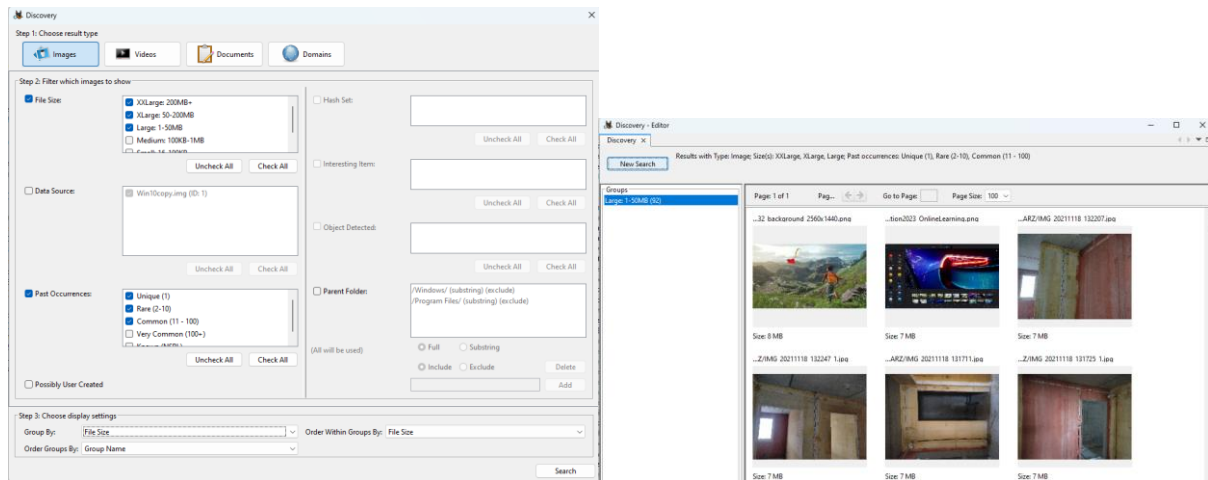
Timeline.

Oczywiście informuje nas o aktywności użytkownika oraz dacie powstawania niektórych plików (nawet 1980 r. czyli tych od twórców).



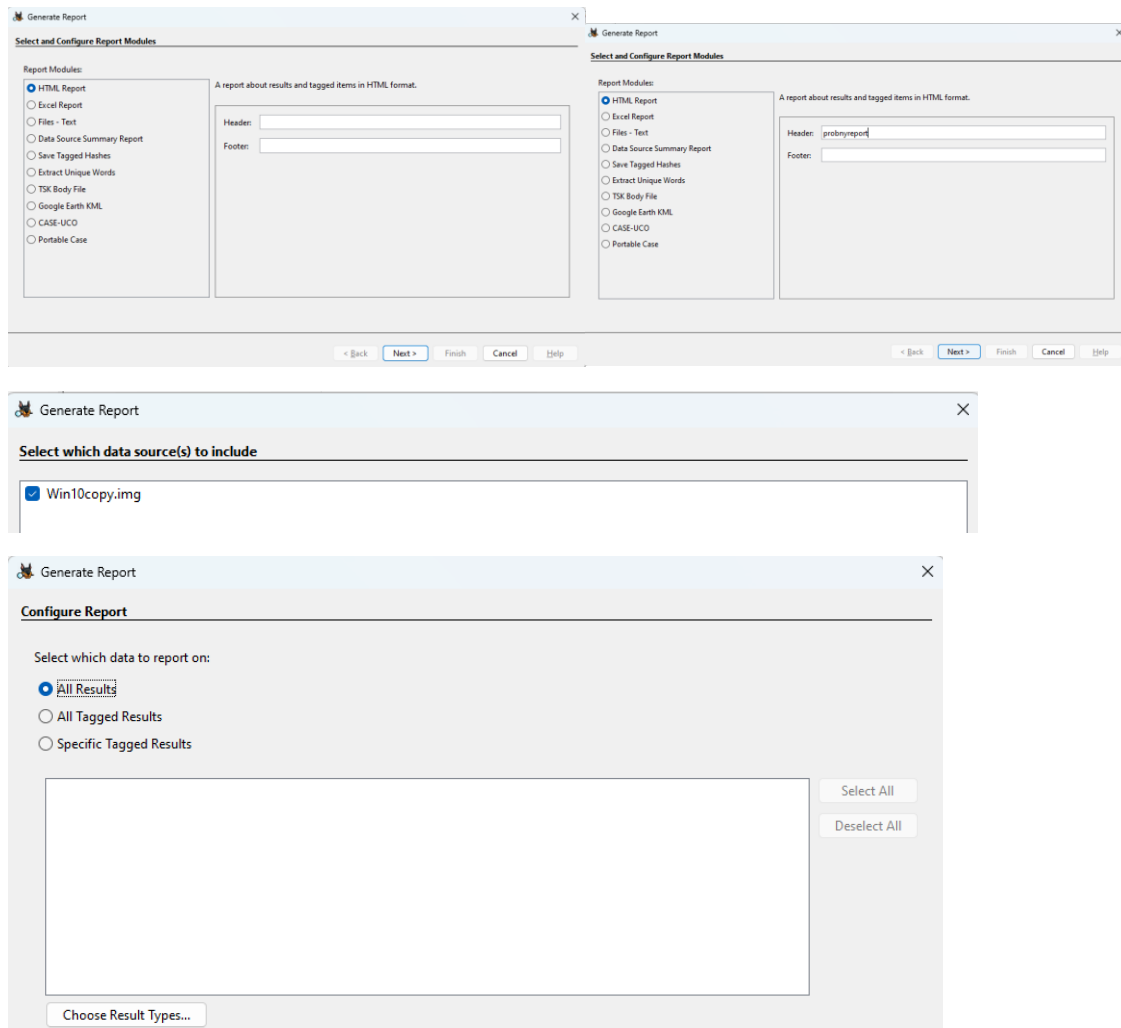
Discovery.

Narzędzie, które pozwala nam na bardzo dokładne wyszukiwanie pewnych rzeczy. Podejrzewam, że na przykład w trakcie śledztwa można by dostać informację, że szukamy np. starych faktur, wtedy to narzędzie byłoby bardzo przyjemne.



Generate Report.

Nazwa mówi sama za siebie, kolejny raz idealne narzędzie do prowadzenia śledztwa.



W efekcie mamy wygenerowany raport w formie strony.

Report Navigation

Case Summary

Chromium Extensions (6)

Chromium Profiles (1)

Data Source Usage (1)

EXIF Metadata (48)

Encryption Suspected (5)

Extension Mismatch Detected (82)

Favicon (114)

Installed Programs (32)

Keyword Hits (2707)

Metadata (118)

Operating System Information (1)

Recent Documents (31)

Recycle Bin (2)

Run Programs (1214)

Shell Bags (27)

Tagged Files (0)

Tagged Images (0)

Tagged Results (0)

USB Device Attached (2)

User Content Suspected (48)

Web Bookmarks (1)

Web Cache (1806)

probnyreport

Autopsy Forensic Report

HTML Report Generated on 2023/12/27 13:54:04

Case:

InfSledcza-NJ

Case Number:

1

Number of data sources in case:

1

Examiner:

Nikodem

Image Information:

Win10copy.img

Timezone:

Europe/Warsaw

Path:

C:\Users\Nikodem Jakubowski\Desktop\Studia\Win10copy.img

Software Information:

Autopsy Version:

4.21.0

Android Analyzer Module:

4.21.0

Android Analyzer (aLEAPP) Module:

4.21.0

Central Repository Module:

4.21.0

DJI Drone Analyzer Module:

4.21.0

Data Source Integrity Module:

4.21.0

Email Parser Module:

4.21.0

Embedded File Extractor Module:

4.21.0

Encryption Detection Module:

4.21.0

Extension Mismatch Detector Module:

4.21.0

Do tego informacje o użytych narzędziach.

Report Navigation

Case Summary

Chromium Extensions (6)

Chromium Profiles (1)

Data Source Usage (1)

EXIF Metadata (48)

Encryption Suspected (5)

Extension Mismatch Detected (82)

Favicon (114)

Installed Programs (32)

Keyword Hits (2707)

Metadata (118)

Operating System Information (1)

Recent Documents (31)

Recycle Bin (2)

Run Programs (1214)

Shell Bags (27)

Tagged Files (0)

Tagged Images (0)

Tagged Results (0)

USB Device Attached (2)

User Content Suspected (48)

Web Bookmarks (1)

Web Cache (1806)

Ingest History:

Job 1:

Data Source:

Win10copy.img

Status:

COMPLETED

Enabled Modules:

Recent Activity

Hash Lookup

File Type Identification

Extension Mismatch Detector

Embedded File Extractor

Picture Analyzer

Keyword Search

Email Parser

Encryption Detection

Interesting Files Identifier

Central Repository

PhotoRec Carver

Virtual Machine Extractor

Data Source Integrity

Android Analyzer (aLEAPP)


DJI Drone Analyzer

YARA Analyzer

iOS Analyzer (iLEAPP)

GPX Parser

Android Analyzer



Powered by Autopsy Open Source Digital Forensics Platform - www.sleuthkit.org

Analiza – opis pozostałych, ciekawych modułów.

Data Sources- informacje o źródle danych.

Wszystko się zgadza, kolega twierdził, że używał tego systemu w technikum jako maszyna wirtualna, wielkość się zgadza.

The screenshot shows the 'Listing' window for 'Win10copy.img_1 Host'. The 'Table' tab is active, displaying a single file entry:

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
Win10copy.img	image	53887091200	512	Europe/Warsaw	765d79ef-db78-456c-b3d5-baf127484779

Below the table, the 'Operating System Information' tab is active, showing details for 'DESKTOP-33UAHEC' (Windows 10 Pro, AMD64 architecture). The 'Source File Path' is '/img_Win10copy.img' and the 'Artifact ID' is '-9223372036854775694'.

EXIF Metadata.

Moduł zawiera wszystkie pliki typu image (.jpg, .png itd.), które mają w sobie jakieś sygnatury EXIF. Poddawaliśmy analizie takie pliki na laboratoriach. Dodatkowo jest również możliwość przeglądania sobie tych zdjęć i analizowania innych metadanych takich jak: data zrobienia zdjęcia, lokalizacja i inne.

The screenshot shows the 'Listing' window for 'EXIF Metadata'. The 'Table' tab is active, displaying a list of image files with their EXIF metadata. The 'Source Name' column lists files like 'IMG_20211118_132040.jpg', 'IMG_20211118_132047.jpg', etc. The 'Date Created' column shows dates like '2021-11-18 13:20:40 CET'. The 'File Path' column shows paths like '/img_Win10copy.img/vol_vol3/\$Recycle.Bin/S-1-5-21...'. The 'Size' column shows file sizes like '5951533', '5459860', etc. The 'Path' column shows paths like '/img_Win10copy.img/vol_vol3/\$Recycle.Bin/S-1-5-21...'. The 'Tags Menu' is visible on the right side of the window.

Below the table, a preview of a photo is shown. The photo is a close-up of a red door or wall, with a small window or opening visible. The photo is labeled 'bg1a_thumb.png'.

Encryption Suspected.

Moduł wykrywa pliki, które są zabezpieczone hasłem lub są zaszyfrowane.

Listing

Encryption Suspected

5 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment
mpenginedb.db			0	File	Likely Notable			Suspected encryption due to high entropy (7,974544).	Suspected encryption due to high entropy (7,974544).
AgGIFaultHistory.db			0	File	Likely Notable			Suspected encryption due to high entropy (7,908174).	Suspected encryption due to high entropy (7,908174).
AgGIFgAppHistory.db			0	File	Likely Notable			Suspected encryption due to high entropy (7,840580).	Suspected encryption due to high entropy (7,840580).
AgGIUAD_S-1-5-21-3184859854-501446439-2400474			0	File	Likely Notable			Suspected encryption due to high entropy (7,723147).	Suspected encryption due to high entropy (7,723147).
AgGIGlobalHistory.db			0	File	Likely Notable			Suspected encryption due to high entropy (7,847175).	Suspected encryption due to high entropy (7,847175).

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

xxsB
*7X]
ldZ
3= ~x
VE=>q1
8Pj
Ga379
oo~g
Ud+X
~FO[
mp]p6
.pr~
R2oo9
S.i
&eqR
0Ph%
>Qfow
zS~Dx;

Extension Mismatch Detected.

Wykrywacz plików, których rozszerzenia nie zgadzają się z ich typami MIME. Mogą być one podejrzane.

Listing

Extension Mismatch Detected

82 Results

Table Thumbnail Summary

Save Table as CSV

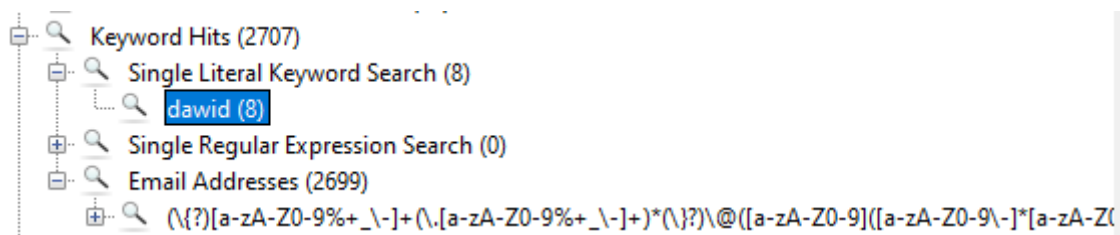
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Extension	MIME Type	File Path
10260_snowing_icon.bytes			0	File	Likely Notable			File has MIME type of image/png	bytes	image/png	/img_Win10
10297_ag_bokeh_sparkles_icon.bytes			0	File	Likely Notable			File has MIME type of image/png	bytes	image/png	/img_Win10
10425_confetti_explosion_icon.bytes			0	File	Likely Notable			File has MIME type of image/png	bytes	image/png	/img_Win10
RemixEffect_Icon_312.bytes			0	File	Likely Notable			File has MIME type of image/png	bytes	image/png	/img_Win10
comempty.dat			1	File	Likely Notable			File has MIME type of application/x-msoffice	dat	application/x-msoffice	/img_Win10
comempty.dat			1	File	Likely Notable			File has MIME type of application/x-msoffice	dat	application/x-msoffice	/img_Win10
demomodeink.dat			1	File	Likely Notable			File has MIME type of image/gif	dat	image/gif	/img_Win10
starttile.hcp			1	File	Likely Notable			File has MIME type of application/x-ooxml	hcp	application/x-ooxml	/img_Win10
demomodeink.dat			1	File	Likely Notable			File has MIME type of image/gif	dat	image/gif	/img_Win10
starttile.hcp			1	File	Likely Notable			File has MIME type of application/x-ooxml	hcp	application/x-ooxml	/img_Win10
comempty.dat			1	File	Likely Notable			File has MIME type of application/x-msoffice	dat	application/x-msoffice	/img_Win10
9.txt			1	File	Likely Notable			File has MIME type of image/png	txt	image/png	/img_Win10
comempty.dat			1	File	Likely Notable			File has MIME type of application/x-msoffice	dat	application/x-msoffice	/img_Win10
9.txt			1	File	Likely Notable			File has MIME type of image/png	txt	image/png	/img_Win10
comempty.dat			1	File	Likely Notable			File has MIME type of application/x-msoffice	dat	application/x-msoffice	/img_Win10
amd64_microsoft-windows-onecore-ras-base-vpn_			1	File	Likely Notable			File has MIME type of image/png	png_e607ca23	image/png	/img_Win10
wow64_microsoft-windows-onecore-ras-base-vpn_			1	File	Likely Notable			File has MIME type of image/png	png_e607ca23	image/png	/img_Win10
comempty.dat			1	File	Likely Notable			File has MIME type of application/x-msoffice	dat	application/x-msoffice	/img_Win10

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

0° 409% Reset Tags Menu

Keyword Hits.

Tutaj specyficzne słowo, hasło, znak mogą być szybko wyszukane w całym obrazie. Można tutaj używać wyrażeń regularnych i innych technik, co nawet widać na zrzucie ekranu poniżej.



Tutaj prawdopodobnie jakieś maile typu SPAM.

Listing Keyword search 1 - dawid x	
\([?][a-zA-Z0-9%+_-]+\.[a-zA-Z0-9%+_-]+)*(\?)\@[a-zA-Z0-9]([a-zA-Z0-9\.-]*[a-zA-Z0-9])?\.[a-zA-Z]{2,4}	
Table	Thumbnail Summary
List Name	
Files with Hits	
bar@souhuu.combar.souhuu.com (1)	1
barlinek@wakacje.pl (1)	1
belchatow@wakacje.pl (1)	1
ben@benlesh.com (1)	1
bia@p7aca9.pe (1)	1
bialogard@wakacje.pl (1)	1
bialystok-hetmanska@wakacje.pl (1)	1
bialystok-ryska@wakacje.pl (1)	1
bialystok@wakacje.pl (1)	1
bielsk-podlaski@wakacje.pl (1)	1
bielsko@wakacje.pl (1)	1
bilcza@wakacje.pl (1)	1
bilgoraj@wakacje.pl (1)	1
bochnia@wakacje.pl (1)	1
bojano@wakacje.pl (1)	1
boleslawiec-slaski@wakacje.pl (1)	1
bony@wakacje.pl (1)	1
boris@highscore.de (1)	1

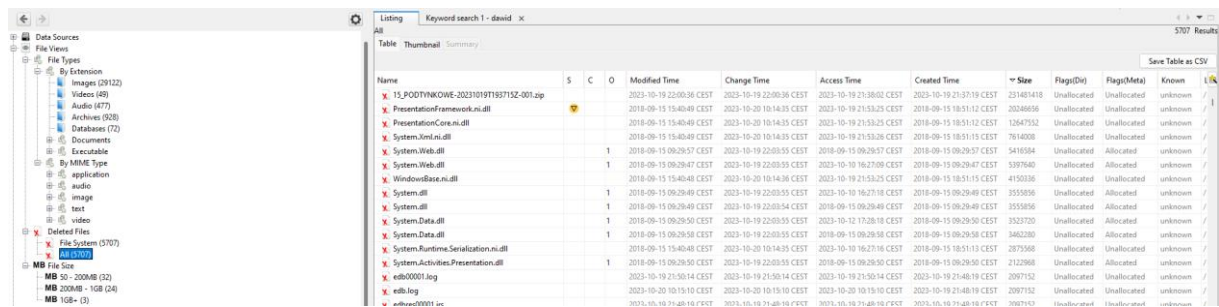
OS Accounts.

Moduł listuje informacje o wszystkich kontach znalezionych w plikach systemu.

Listing Keyword search 1 - dawid x									
Table Thumbnail Summary									
Save Table as CSV									
Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time	
S-1-5-21-3184859854-501446439-2400474765-1001	0			admin	Win10co...	Domain		2020-09-02 17:23:42 CEST	
S-1-5-21-3184859854-501446439-2400474765-503	0			Konto domyslnie	Win10co...	Domain		2020-09-02 17:16:51 CEST	
S-1-5-21-3184859854-501446439-2400474765-504	0			WDAGUtilityAccount	Win10co...	Domain		2020-09-02 17:16:51 CEST	
S-1-5-21-3184859854-501446439-2400474765-500	0			Administrator	Win10co...	Domain		2020-09-02 17:16:51 CEST	
S-1-5-21-3184859854-501446439-2400474765-501	0			Gość	Win10co...	Domain		2020-09-02 17:16:51 CEST	
S-1-5-18				SYSTEM	Win10co...	Local	NT AUTHORITY		
S-1-5-80-956008885-3418522649-1831038044-18532	0				Win10co...	Local	NT SERVICE		
S-1-5-80-3028837079-3186095147-955107200-37019	0				Win10co...	Local	NT SERVICE		
S-1-5-19				LOCAL SERVICE	Win10co...	Local	NT AUTHORITY		
S-1-5-21-3184859854-501446439-2400474765-1000	0				Win10co...	Domain			
S-1-5-80-2620923248-4247863784-3378508180-2659	0				Win10co...	Local	NT SERVICE		
S-1-5-20				NETWORK SERVICE	Win10co...	Local	NT AUTHORITY		
S-1-5-21-397955417-626881126-188441444-4882392	0				Win10co...	Domain			

File views.

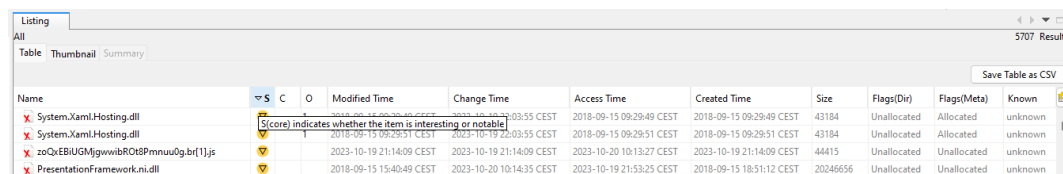
Bardzo rozbudowany moduł, który segreguje pliki według różnych kryteriów.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
15_PODTYNKOWE-20231019175132-201.jpg				2023-10-19 22:00:38 CEST	2023-10-19 22:00:38 CEST	2023-10-19 21:58:02 CEST	2023-10-19 21:57:19 CEST	231481418	Unallocated	Unallocated	unknown
PresentationFramework.dll				2018-09-15 15:40:49 CEST	2023-10-20 10:14:35 CEST	2023-10-19 21:53:25 CEST	2018-09-15 18:51:12 CEST	20246656	Unallocated	Unallocated	unknown
PresentationCore.dll				2018-09-15 15:40:49 CEST	2023-10-20 10:14:35 CEST	2023-10-19 21:53:25 CEST	2018-09-15 18:51:12 CEST	12647552	Unallocated	Unallocated	unknown
System.Xaml.dll				2018-09-15 15:40:49 CEST	2023-10-20 10:14:35 CEST	2023-10-19 21:53:26 CEST	2018-09-15 18:51:15 CEST	7614008	Unallocated	Unallocated	unknown
System.Web.dll			1	2018-09-15 09:29:57 CEST	2023-10-19 22:03:55 CEST	2018-09-15 09:29:57 CEST	2018-09-15 09:29:57 CEST	5416184	Unallocated	Allocated	unknown
System.Windows.dll			1	2018-09-15 09:29:47 CEST	2023-10-19 22:03:55 CEST	2023-10-19 16:27:08 CEST	2018-09-15 09:29:47 CEST	5597640	Unallocated	Unallocated	unknown
System.dll			1	2018-09-15 15:40:48 CEST	2023-10-20 10:14:36 CEST	2023-10-19 21:53:25 CEST	2018-09-15 18:51:15 CEST	4150336	Unallocated	Unallocated	unknown
System.dll			1	2018-09-15 09:29:49 CEST	2023-10-19 22:03:55 CEST	2023-10-10 16:27:18 CEST	2018-09-15 09:29:49 CEST	3555856	Unallocated	Allocated	unknown
System.dll			1	2018-09-15 09:29:50 CEST	2023-10-19 22:03:55 CEST	2018-09-15 09:29:49 CEST	2018-09-15 09:29:49 CEST	3555856	Unallocated	Allocated	unknown
System.Data.dll			1	2018-09-15 09:29:50 CEST	2023-10-19 22:03:55 CEST	2023-10-12 17:28:18 CEST	2018-09-15 09:29:50 CEST	3523720	Unallocated	Allocated	unknown
System.Data.dll			1	2018-09-15 09:29:50 CEST	2023-10-19 22:03:55 CEST	2018-09-15 09:29:50 CEST	2018-09-15 09:29:50 CEST	3462280	Unallocated	Allocated	unknown
System.Runtime.Serialization.dll				2018-09-15 15:40:48 CEST	2023-10-20 10:14:35 CEST	2023-10-10 16:27:16 CEST	2018-09-15 18:51:13 CEST	2875568	Unallocated	Unallocated	unknown
System.Activities.Presentation.dll			1	2018-09-15 09:29:50 CEST	2023-10-19 22:03:55 CEST	2018-09-15 09:29:50 CEST	2018-09-15 09:29:50 CEST	2122968	Unallocated	Allocated	unknown
win00001.log				2023-10-19 21:40:14 CEST	2023-10-19 21:40:14 CEST	2023-10-19 21:40:14 CEST	2023-10-19 21:40:19 CEST	2097152	Unallocated	Unallocated	unknown
win00001.log				2023-10-20 10:15:10 CEST	2023-10-20 10:15:10 CEST	2023-10-20 10:15:10 CEST	2023-10-20 10:15:10 CEST	2097152	Unallocated	Unallocated	unknown
win00001.log				2023-10-10 19:48:10 CEST	2023-10-10 19:48:10 CEST	2023-10-10 19:48:10 CEST	2023-10-10 19:48:10 CEST	2097152	Unallocated	Unallocated	unknown

Można sortować po rozszerzeniu, po MIME, tylko usunięte albo po przedziale rozmiarów.

Szczególnie ciekawe wydają się usunięte pliki. Można je również posegregować według kryterium Score, które ocenia czy dany artefakt się wyróżnia, wymaga uwagi lub analizy. Oczywiście jest cała masa innych opcji sortowania.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
System.Xaml.Hosting.dll				2018-09-15 09:29:51 CEST	2023-10-19 22:03:55 CEST	2018-09-15 09:29:49 CEST	2018-09-15 09:29:49 CEST	43184	Unallocated	Allocated	unknown
System.Xaml.Hosting.dll			1	2018-09-15 09:29:51 CEST	2023-10-19 22:03:55 CEST	2018-09-15 09:29:51 CEST	2018-09-15 09:29:51 CEST	43184	Unallocated	Allocated	unknown
zoQzEBiUGMgigwibR0t8Pmnuu0g.br[1].js				2023-10-19 21:14:09 CEST	2023-10-19 21:14:09 CEST	2023-10-20 10:13:27 CEST	2023-10-19 21:14:09 CEST	44415	Unallocated	Unallocated	unknown
PresentationFramework.dll				2018-09-15 15:40:49 CEST	2023-10-20 10:14:35 CEST	2023-10-19 21:53:25 CEST	2018-09-15 18:51:12 CEST	20246656	Unallocated	Unallocated	unknown

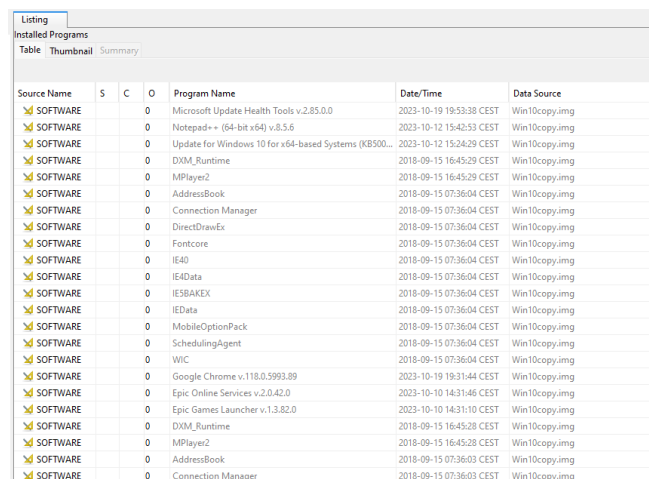
Data Artifacts.

Moduł zawiera przeróżne artefakty znalezione w systemie, przykłady poniżej.


























Artifact Type	Child Count
Chromium Extensions (6)	6
Chromium Profiles (1)	1
Favicons (114)	114
Installed Programs (32)	32
Metadata (118)	118
Operating System Information (1)	1
Recent Documents (31)	31
Recycle Bin (2)	2
Run Programs (1214)	1214
Shell Bags (27)	27
USB Device Attached (2)	2
Web Bookmarks (1)	1
Web Cache (1806)	1806
Web Cookies (331)	331
Web Downloads (26)	26
Web Form Autofill (1)	1
Web History (256)	256
Web Search (31)	31

Z ciekawszych elementów mamy pobrane programy, można nawet zobaczyć datę pobrania.





Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	Microsoft Update Health Tools v.2.85.0.0	2023-10-19 19:53:38 CEST	Win10copy.img
SOFTWARE			0	Notepad++ (64-bit x64) v.8.5.6	2023-10-12 15:42:53 CEST	Win10copy.img
SOFTWARE			0	Update for Windows 10 for x64-based Systems (KB900...	2023-10-12 15:24:29 CEST	Win10copy.img
SOFTWARE			0	DXM_Runtime	2018-09-15 16:45:29 CEST	Win10copy.img
SOFTWARE			0	MPlayer2	2018-09-15 16:45:29 CEST	Win10copy.img
SOFTWARE			0	AddressBook	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	Connection Manager	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	DirectDrawEx	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	Fontcore	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	IE40	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	IE40Data	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	IE8BAKEX	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	IEData	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	MobileOptionPack	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	SchedulingAgent	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	WIC	2018-09-15 07:36:04 CEST	Win10copy.img
SOFTWARE			0	Google Chrome v.118.0.5993.89	2023-10-19 19:31:44 CEST	Win10copy.img
SOFTWARE			0	Epic Online Services v.2.0.42.0	2023-10-10 14:31:46 CEST	Win10copy.img
SOFTWARE			0	Epic Games Launcher v.1.3.82.0	2023-10-10 14:31:10 CEST	Win10copy.img
SOFTWARE			0	DXM_Runtime	2018-09-15 16:45:28 CEST	Win10copy.img
SOFTWARE			0	MPlayer2	2018-09-15 16:45:28 CEST	Win10copy.img
SOFTWARE			0	AddressBook	2018-09-15 07:36:03 CEST	Win10copy.img
SOFTWARE			0	Connection Manager	2018-09-15 07:36:03 CEST	Win10copy.img

Kolejny element warty uwagi to ostatnie (otwarte) dokumenty.

Listing						
Recent Documents						
Table	Thumbnail	Summary				
Source Name	S	C	O	Path	Date Accessed	Data Source
 15_PODTYNKOWE-20231019T193715Z-001.Link				C:\Users\admin\Downloads\15_PODTYNKOWE-20231...	2023-10-19 21:37:56 CEST	Win10copy.img
 https--www.xiaoyalab.com-real-heic-file-viewer-o				No preferred path found	2023-10-19 21:54:31 CEST	Win10copy.img
 IMG_0243.Link				C:\Users\admin\Downloads\IMG_0243.MOV	2023-10-19 21:50:42 CEST	Win10copy.img
 IMG_0256.Link				C:\Users\admin\Desktop\wakacje\IMG_0256.heic	2023-10-19 21:46:02 CEST	Win10copy.img
 Internet.Link				No preferred path found	2020-09-02 17:25:01 CEST	Win10copy.img
 Konta użytkowników (2).Link				No preferred path found	2023-10-10 16:27:17 CEST	Win10copy.img
 Konta użytkowników.Link				No preferred path found	2023-10-10 16:27:17 CEST	Win10copy.img
 lista zakupow.Link				C:\Users\admin\plik\lista zakupow.txt	2023-10-19 22:01:33 CEST	Win10copy.img
 ms-windows-store--pdp-productid=9nmzt573rj7i				No preferred path found	2023-10-19 21:46:24 CEST	Win10copy.img
 plik1.bt.Link				C:\Users\admin\plik\plik1.bt.txt	2023-10-19 21:41:10 CEST	Win10copy.img
 pliki.Link				C:\Users\admin\pliki	2023-10-19 21:41:10 CEST	Win10copy.img
 Pobrane.Link				C:\Users\admin\Downloads	2023-10-19 21:50:42 CEST	Win10copy.img
 PRZEWODNIK-PO-KRECIE.Link				C:\Users\admin\Downloads\PRZEWODNIK-PO-KREC...	2023-10-19 21:59:34 CEST	Win10copy.img
 Usun konta użytkowników.Link				No preferred path found	2023-10-10 16:28:08 CEST	Win10copy.img
 wakacje.Link				C:\Users\admin\Desktop\wakacje	2023-10-19 21:45:37 CEST	Win10copy.img
 Wszystkie zadania.Link				No preferred path found	2023-10-10 16:28:08 CEST	Win10copy.img
 IMG_0243.MOV.Link				C:\Users\admin\Downloads\IMG_0243.MOV	0000-00-00 00:00:00	Win10copy.img
 No preferred path found.Link				No preferred path found	0000-00-00 00:00:00	Win10copy.img
 PRZEWODNIK-PO-KRECIE.pdf.Link				C:\Users\admin\Downloads\PRZEWODNIK-PO-KREC...	0000-00-00 00:00:00	Win10copy.img
 IMG_0256.heic.Link				C:\Users\admin\Desktop\wakacje\IMG_0256.heic	0000-00-00 00:00:00	Win10copy.img
 lista zakupow.bt.Link				C:\Users\admin\plik\lista zakupow.bt	0000-00-00 00:00:00	Win10copy.img
 plik1.bt.bt.Link				C:\Users\admin\plik\plik1.bt.bt	0000-00-00 00:00:00	Win10copy.img
 Pictures.Link				C:\Users\admin\Pictures	0000-00-00 00:00:00	Win10copy.img

Istnieje również możliwość przeszukania kosza.

Listing							
Recycle Bin							
Table	Thumbnail	Summary					
Source Name	S	C	O	Path	Time Deleted	Username	Data Source
 SR43MB9R.txt				C:\Users\admin\plik\plik1.txt.txt	2023-10-19 22:01:49 CEST		Win10copy.img
 SRPS20PV.zip				C:\Users\admin\Downloads\15_PODTYNKOWE-20231...	2023-10-19 22:00:36 CEST		Win10copy.img

Kolejny to dołączone urządzenia USB.



Listing

USB Device Attached

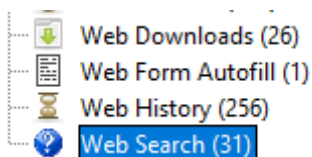
Table

Thumbnail

Summary

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
 SYSTEM			0	2023-10-20 10:13:11 CEST		ROOT_HUB	4&24d6eb65&0	Win10copy.img
 SYSTEM			0	2023-10-20 10:13:12 CEST	VirtualBox	USB Tablet	5&18f54cb7&0&1	Win10copy.img

Mamy jeszcze kilka innych elementów dot. historii przeglądania, egzemplarzy autouzupełnienia, historii przeglądania i wyszukiwania. Ze względu na prywatność nie pokażę zawartości. Tak wyglądają ikony odpowiedzialne za listowanie powyższych.



Score.

Listuje nam podejrzane, dziwne lub niestandardowe pliki wymagające analizy.

Listing

Score

2 Results

Table

Thumbnail

Summary

Save Table as CSV

Type

Bad Items (0)

Suspicious Items (1136)