

Step-by-step tutorial: Autopsy

What is Autopsy:

- Free digital forensic tool for analyzing hard drives/partitions
- UI for „The Sleuth Kit“ (The Sleuth Kit: Collection of utilities for forensic analysis)

Features:

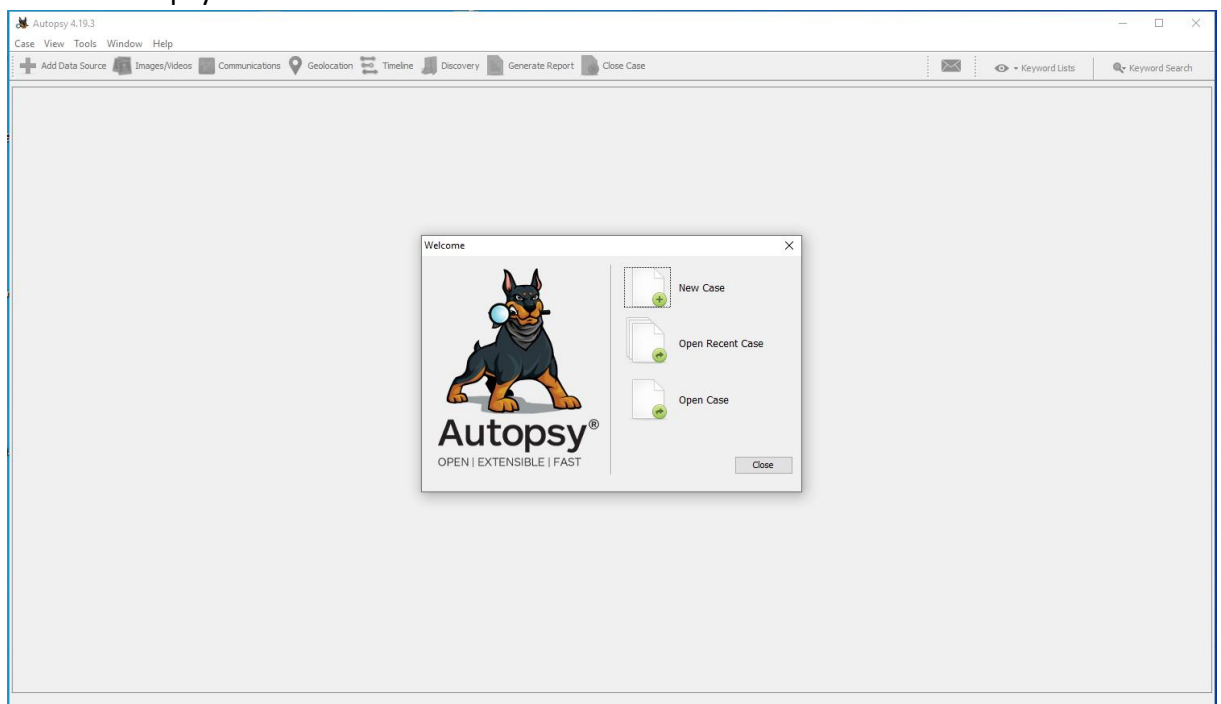
- Extensible: Plugins can add new functionalities
- Centralized: standard & consistent mechanism for accessing all features & modules
- Easy to use
- Multiple users: useable by one investigator or coordinate work of a team

Process:

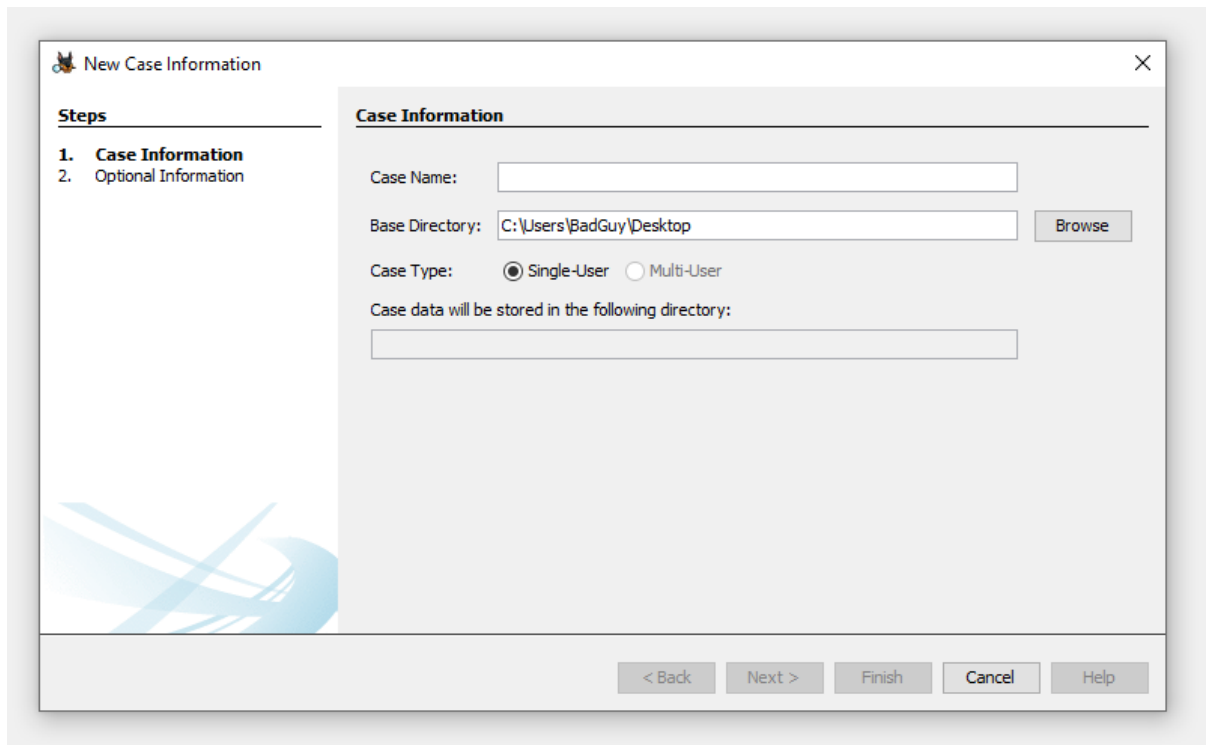
- Analyze major file systems (NTFS, FAT, ExFAT, Ext2/Ext3/...)
- Hashing all files
- Unpack standard archives
- Extract metadata
- Keyword search
- Search indexed files
- Create reports to summarize important activity
- Save partial image of files to virtual hard disk format

Step-by-step analysis:

1. Install Autopsy from the Autopsy Website (<https://www.autopsy.com/download/>)
2. Launch Autopsy



3. Create a new case

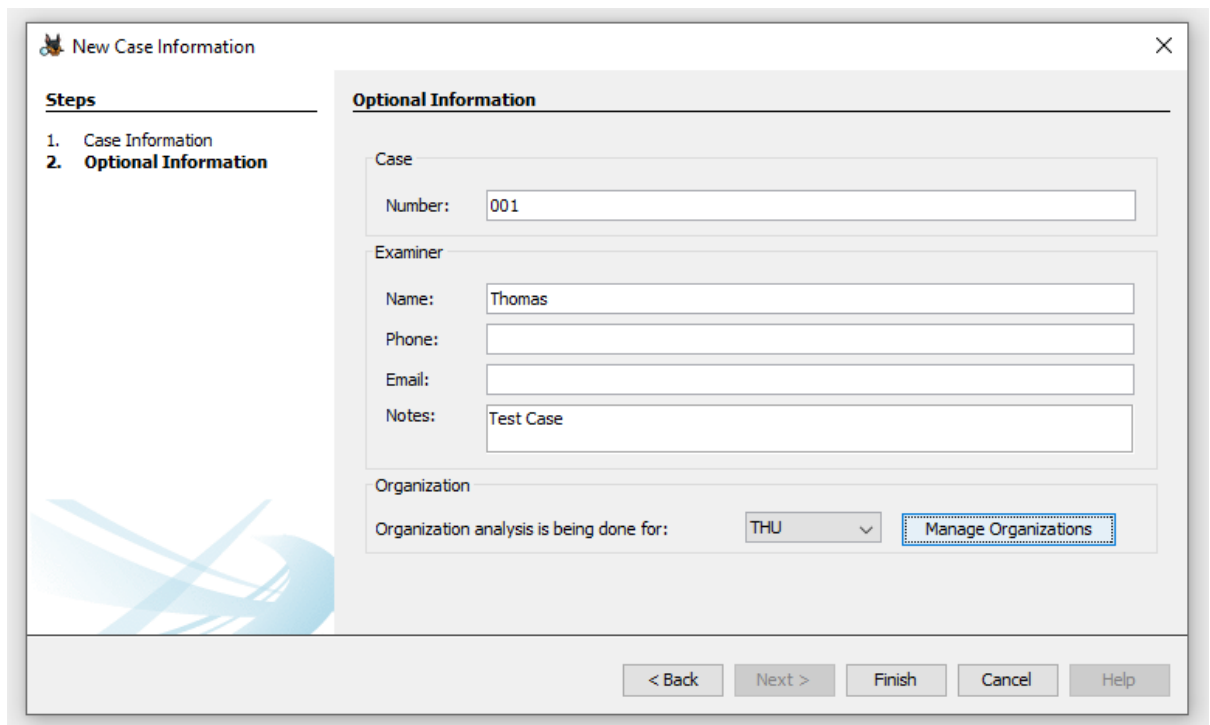


The dialog box is titled "New Case Information" and has a close button (X) in the top right corner. On the left, a "Steps" pane shows two steps: "1. Case Information" (selected) and "2. Optional Information". The main area is titled "Case Information" and contains the following fields:

- Case Name:** A text input field.
- Base Directory:** A text input field containing "C:\Users\BadGuy\Desktop" and a "Browse" button to its right.
- Case Type:** Two radio buttons: "Single-User" (selected) and "Multi-User".
- Case data will be stored in the following directory:** A text input field.

At the bottom, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

4. Insert all case informations needed

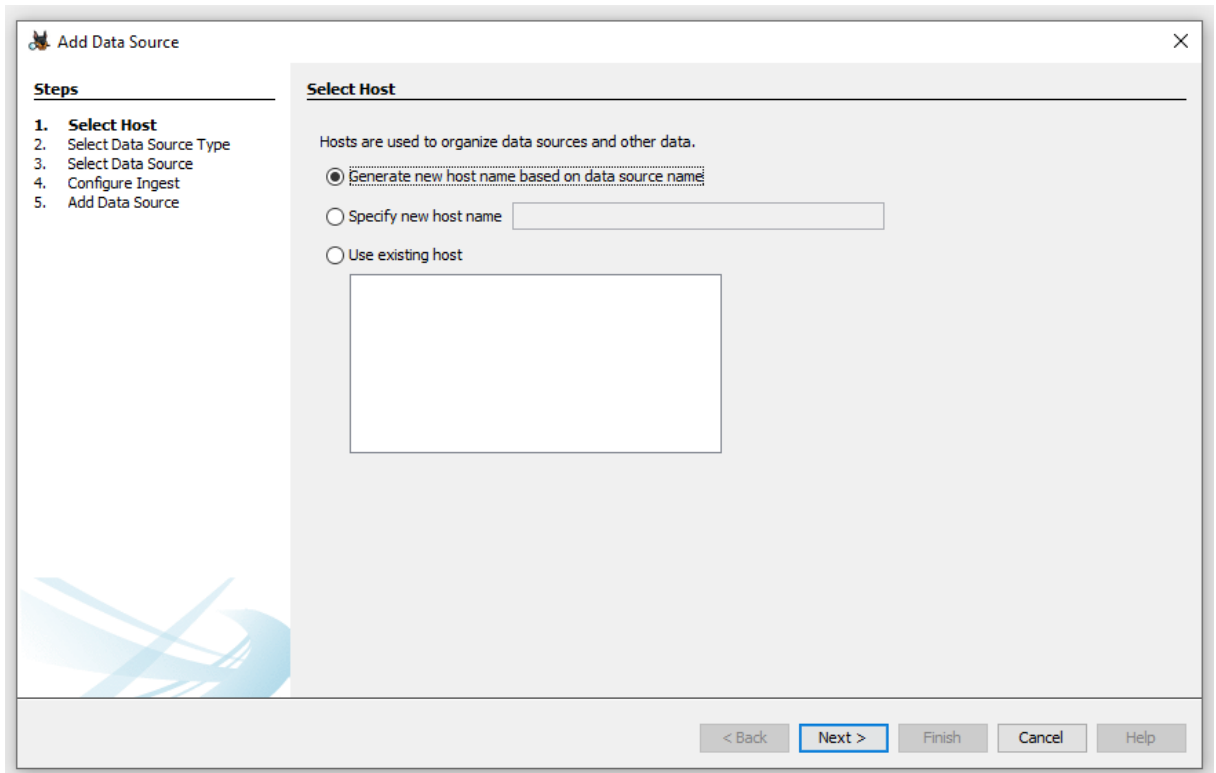


The dialog box is titled "New Case Information" and has a close button (X) in the top right corner. On the left, a "Steps" pane shows two steps: "1. Case Information" and "2. Optional Information" (selected). The main area is titled "Optional Information" and contains the following fields:

- Case:**
 - Number:** A text input field containing "001".
- Examiner:**
 - Name:** A text input field containing "Thomas".
 - Phone:** A text input field.
 - Email:** A text input field.
 - Notes:** A text input field containing "Test Case".
- Organization:**
 - Organization analysis is being done for:** A dropdown menu showing "THU" and a "Manage Organizations" button to its right.

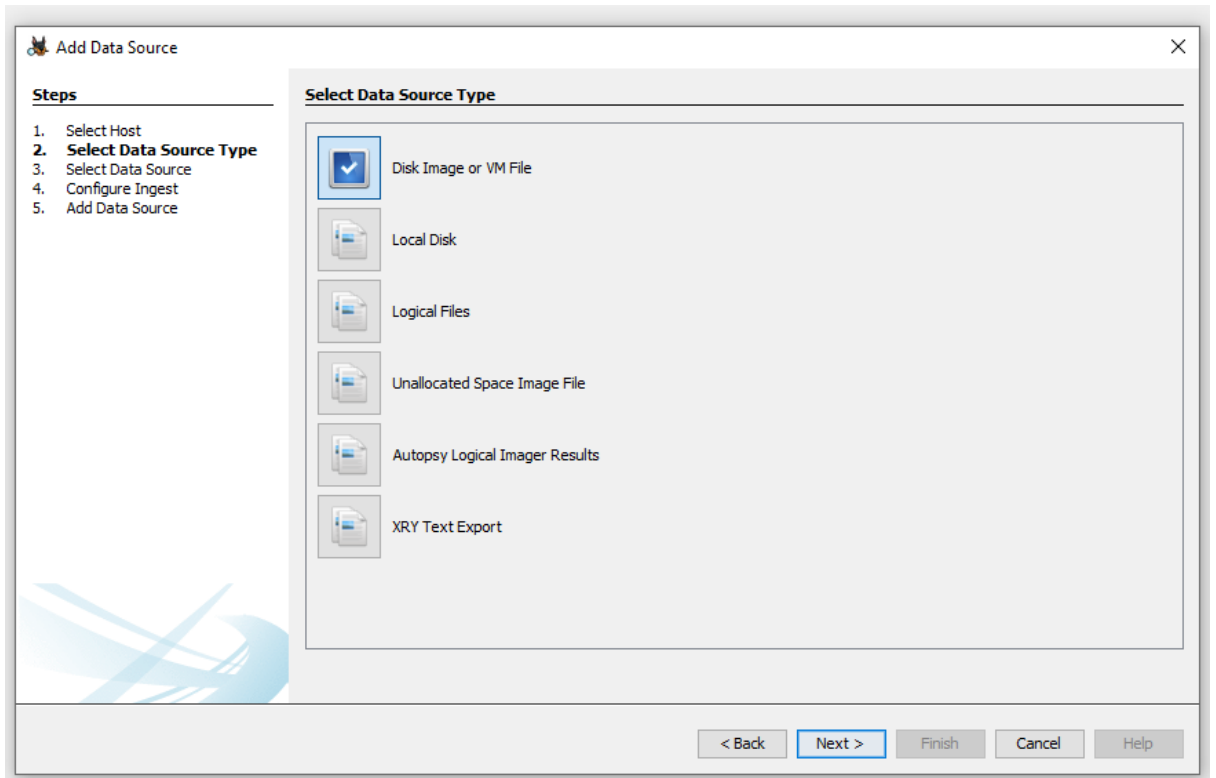
At the bottom, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

5. Generate a new host



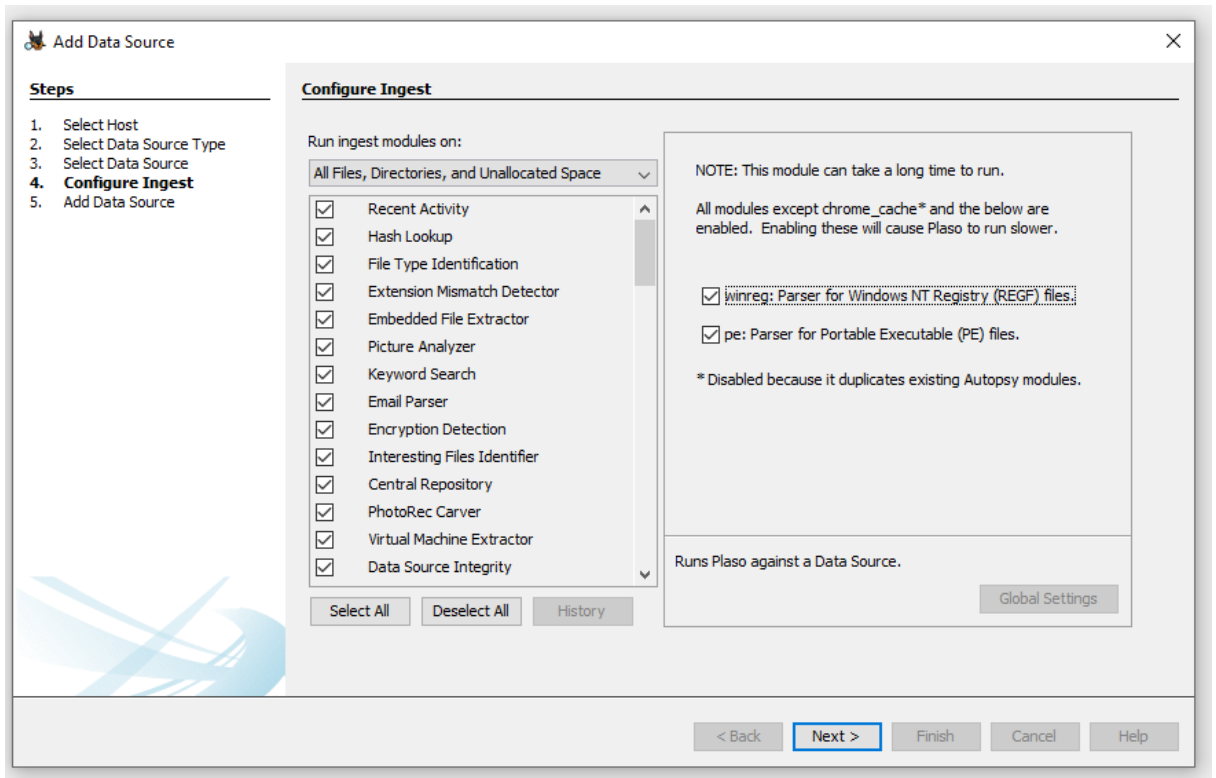
The screenshot shows the 'Add Data Source' dialog box with the title bar 'Add Data Source' and a close button. On the left, a 'Steps' list shows: 1. **Select Host**, 2. Select Data Source Type, 3. Select Data Source, 4. Configure Ingest, 5. Add Data Source. The main area is titled 'Select Host' and contains the text 'Hosts are used to organize data sources and other data.' Below this, there are three radio button options:
- ☒ Generate new host name based on data source name
- ☐ Specify new host name [text input field]
- ☐ Use existing host [empty rectangular box]
At the bottom right, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

6. Select data source type

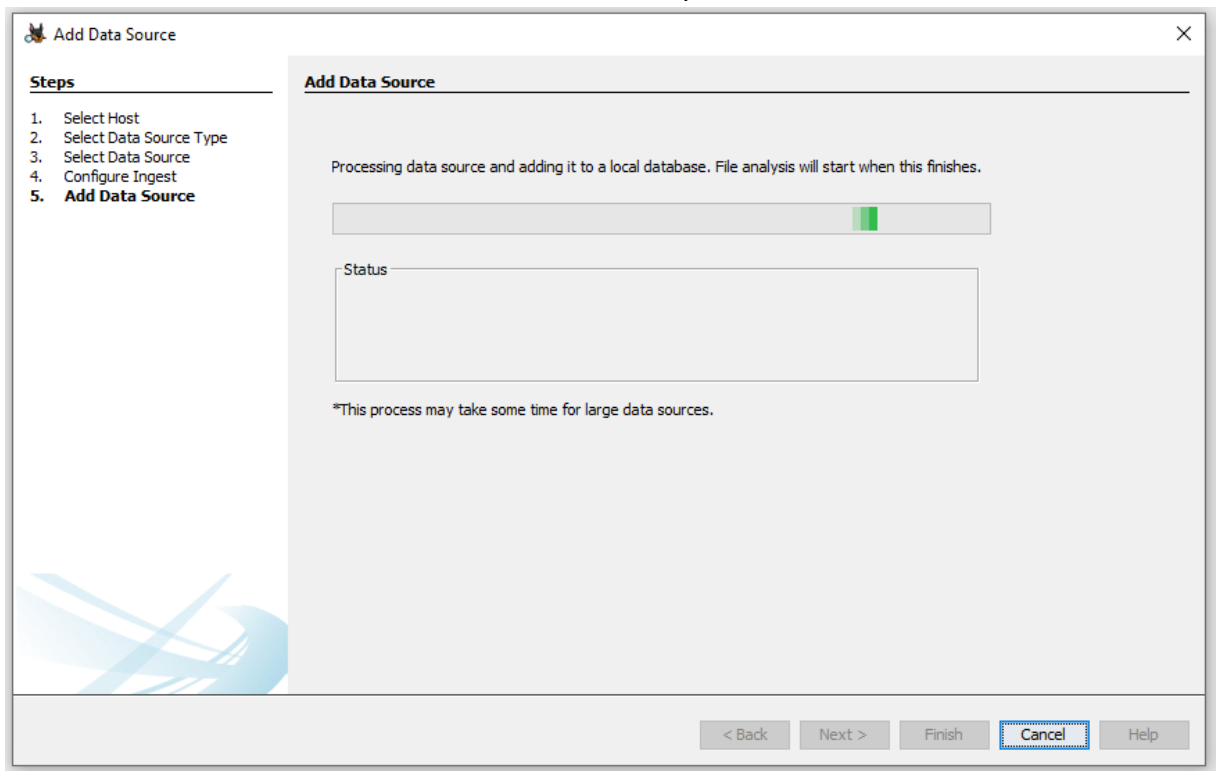


The screenshot shows the 'Add Data Source' dialog box with the title bar 'Add Data Source' and a close button. On the left, a 'Steps' list shows: 1. Select Host, 2. **Select Data Source Type**, 3. Select Data Source, 4. Configure Ingest, 5. Add Data Source. The main area is titled 'Select Data Source Type' and contains a list of six data source types, each with a folder icon and a checkbox:
- ☒ Disk Image or VM File
- ☐ Local Disk
- ☐ Logical Files
- ☐ Unallocated Space Image File
- ☐ Autopsy Logical Imager Results
- ☐ XRY Text Export
At the bottom right, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

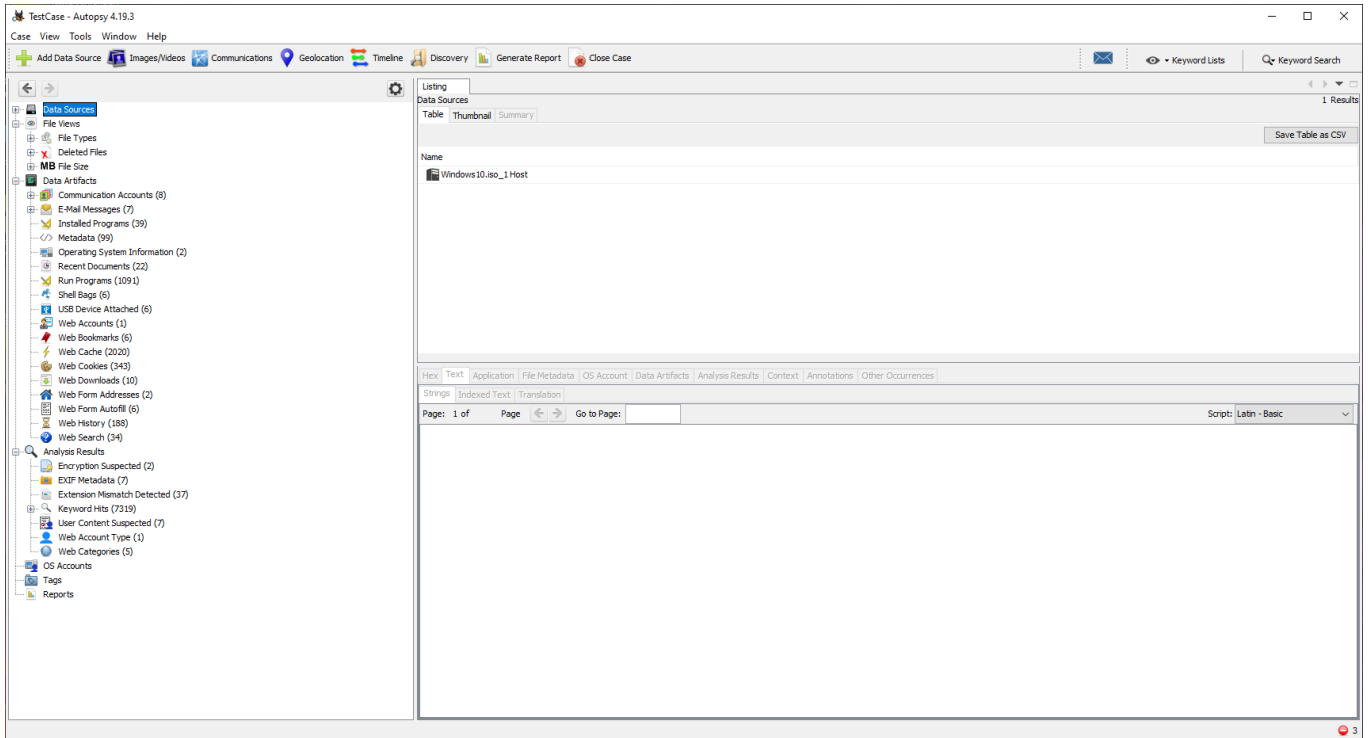
7. Configure ingests (what shall be searched for?)



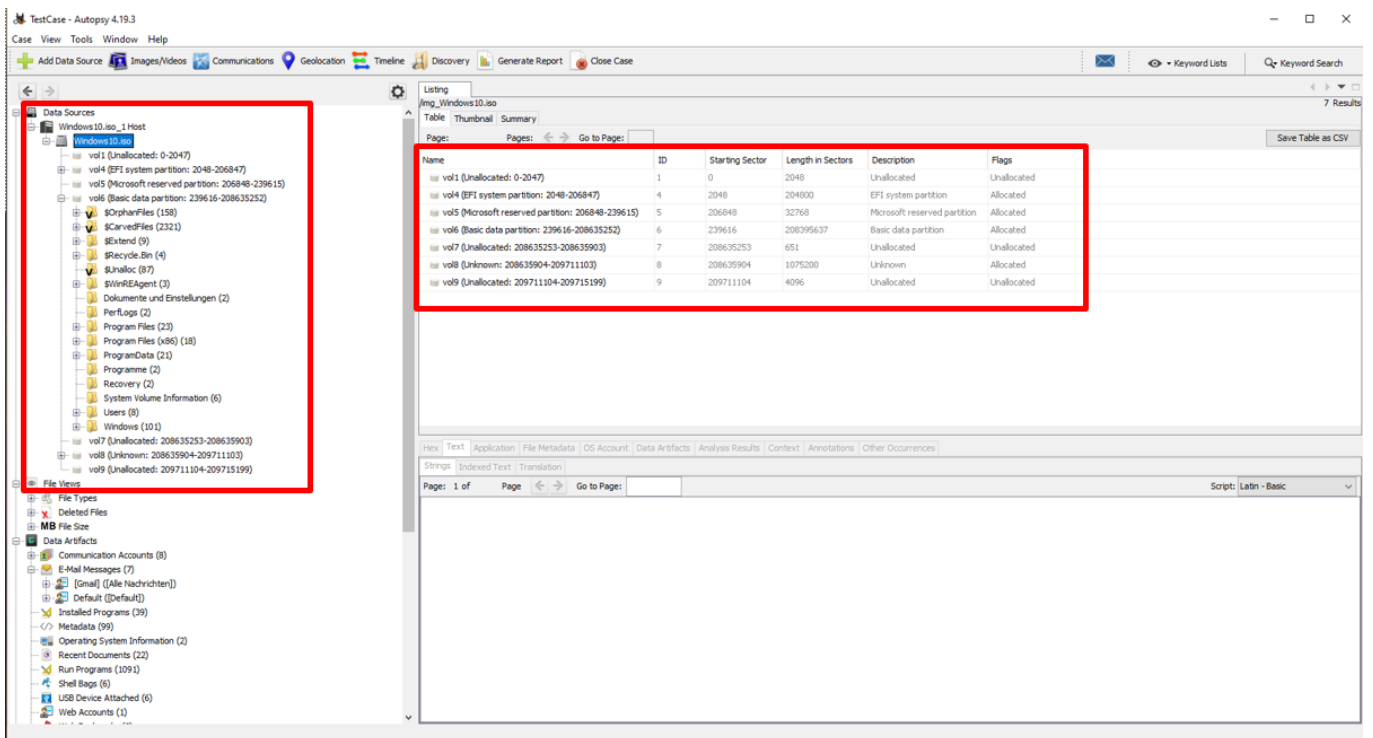
8. Add the data source & wait for the finish of the analysis



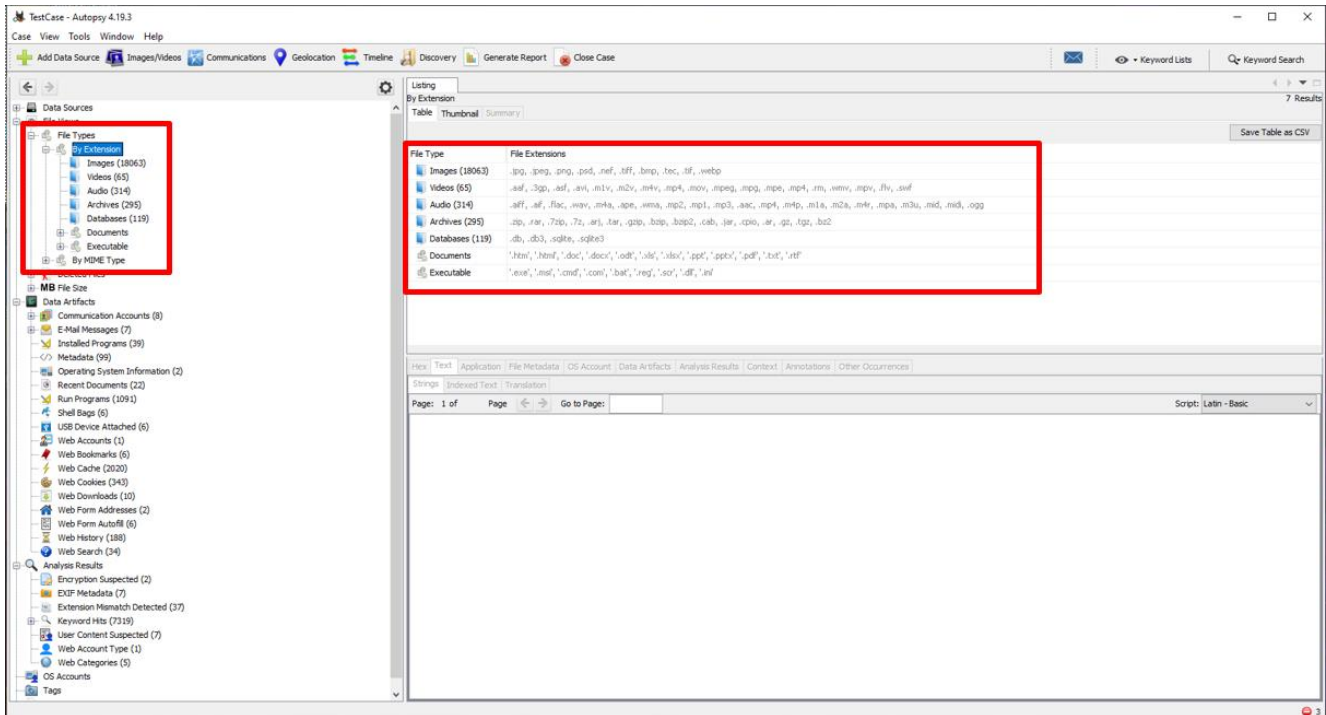
9. Ingest has finished



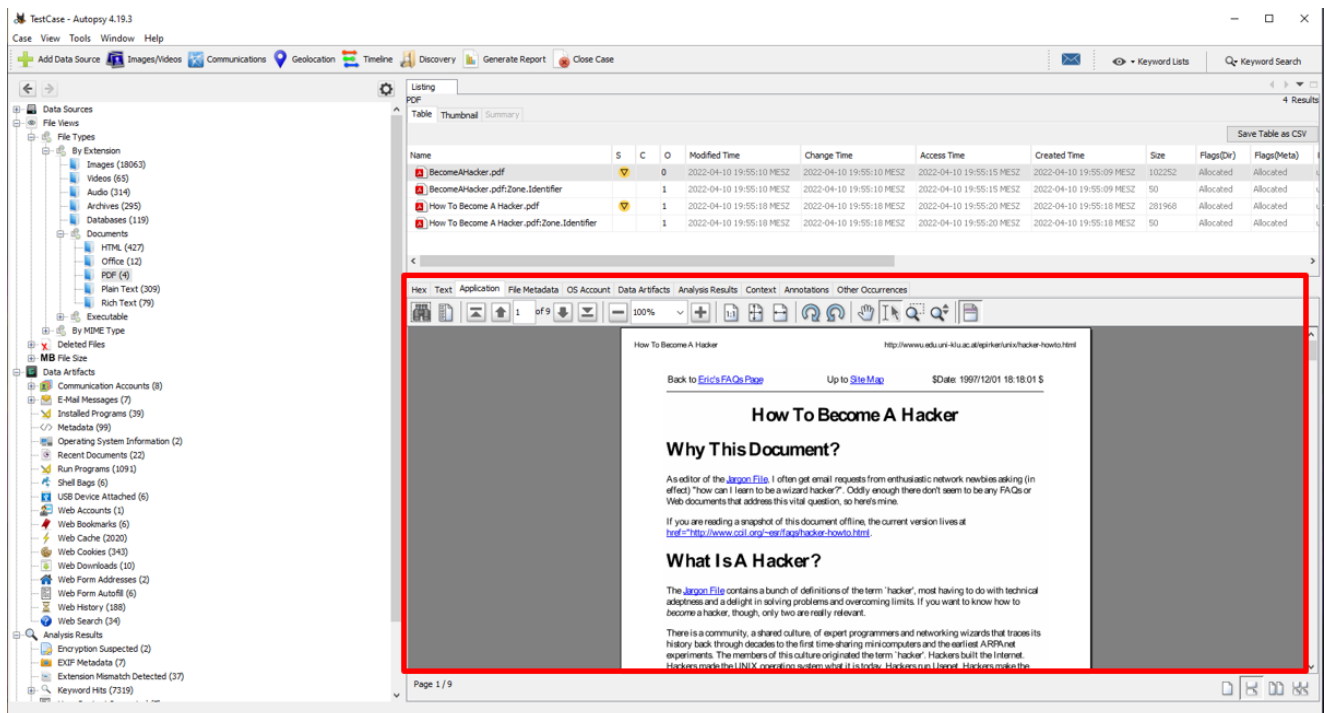
10. Search/browse filesystem



11. Browse files by extension



12. Document/file preview



TestCase - Autopsy 4.19.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing
PDF 4 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)
BecomeAHacker.pdf			0	2022-04-10 19:55:10 MESZ	2022-04-10 19:55:10 MESZ	2022-04-10 19:55:15 MESZ	2022-04-10 19:55:09 MESZ	102252	Allocated	Allocated
BecomeAHacker.pdf.Zone.Identifier			1	2022-04-10 19:55:18 MESZ	2022-04-10 19:55:18 MESZ	2022-04-10 19:55:20 MESZ	2022-04-10 19:55:18 MESZ	50	Allocated	Allocated
How To Become A Hacker.pdf			1	2022-04-10 19:55:18 MESZ	2022-04-10 19:55:18 MESZ	2022-04-10 19:55:20 MESZ	2022-04-10 19:55:18 MESZ	281968	Allocated	Allocated
How To Become A Hacker.pdf.Zone.Identifier			1	2022-04-10 19:55:18 MESZ	2022-04-10 19:55:18 MESZ	2022-04-10 19:55:20 MESZ	2022-04-10 19:55:18 MESZ	50	Allocated	Allocated

Save Table as CSV

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

Metadata

```

Name: /img_Windows10.iso_vol6/Users/BadGuy/Downloads/BecomeAHacker.pdf
Type: File System
MIME Type: application/pdf
Size: 102252
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2022-04-10 19:55:10 MESZ
Accessed: 2022-04-10 19:55:15 MESZ
Created: 2022-04-10 19:55:09 MESZ
Changed: 2022-04-10 19:55:10 MESZ
MD5: 396943411d9c4e70d274eb55cae31378
SHA-256: 25da8f7793c255450817e27aed2bd93B0c4504a4adeb628b5567ecf3724b3af27
Hash Lookup Results: UNKNOWN
Internal ID: 25193

```

From The Sleuth Kit Isat Tool:

```

IFT Entry Header Values:
Entry: 125945 Sequence: 2
FlagFile Sequence Number: 456337196
Allocated File
Links: 2

STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 1831 (S-1-8-21-1163160977-3019039153-1651624052-1001)
Last User Journal Update Number: 29167616

```

Case - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

10000 Results

Data Sources

- File Views
 - File Types
 - Deleted Files
 - X File System (12146)
 - X All (14468)
 - MB File Size
 - Web Services
 - Communication Accounts (8)
 - E-Mail Messages (7)
 - Installed Programs (39)
 - Metadata (39)
 - Operating System Information (2)
 - Recent Documents (22)
 - Run Programs (1091)
 - Shell Bags (6)
 - USB Device Attached (6)
 - Web Accounts (1)
 - Web Bookmarks (8)
 - Web Cache (2020)
 - Web Cookies (343)
 - Web Downloads (10)
 - Web Form Addresses (2)
 - Web Form Autofill (6)
 - User Content Suspicious (7)
 - Web Account Type (1)
 - Web Categories (5)
 - OS Accounts
 - Tags
 - Reports

Listing

File System

Table Thumbnail Summary

Page: 1 of 2 Pages: Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(O)
EventStore.db-wal				2022-04-10 19:39:46 MESZ	2022-04-10 19:39:46 MESZ	2022-04-10 19:39:46 MESZ	2022-04-10 19:23:45 MESZ	0	Unallocated	Unalloc
EventStore.db-shm				2022-04-10 19:23:45 MESZ	2022-04-10 19:23:45 MESZ	2022-04-10 19:23:45 MESZ	2022-04-10 19:23:45 MESZ	32768	Unallocated	Unalloc
EventStore.db-wal				2022-04-10 19:56:14 MESZ	2022-04-10 19:56:14 MESZ	2022-04-10 19:56:14 MESZ	2022-04-10 19:23:45 MESZ	362592	Unallocated	Unalloc
EventStore.db-shm				2022-04-10 19:23:45 MESZ	2022-04-10 19:23:45 MESZ	2022-04-10 19:23:45 MESZ	2022-04-10 19:23:45 MESZ	32768	Unallocated	Unalloc
EventStore.db-wal				2022-04-10 20:02:14 MESZ	2022-04-10 20:02:14 MESZ	2022-04-10 20:02:14 MESZ	2022-04-10 19:23:44 MESZ	1048576	Unallocated	Unalloc
EventStore.db-shm				2022-04-10 19:23:44 MESZ	2022-04-10 19:23:44 MESZ	2022-04-10 19:23:44 MESZ	2022-04-10 19:23:44 MESZ	32768	Unallocated	Unalloc
unghfrvc				2022-04-10 19:24:45 MESZ	2022-04-10 19:24:45 MESZ	2022-04-10 19:24:45 MESZ	2022-04-10 19:24:45 MESZ	48	Unallocated	Unalloc
[current folder]				2022-04-10 19:24:45 MESZ	2022-04-10 19:24:45 MESZ	2022-04-10 19:24:45 MESZ	2022-04-10 19:24:45 MESZ	48	Unallocated	Unalloc
[parent folder]				2022-04-10 20:02:18 MESZ	2022-04-10 20:02:18 MESZ	2022-04-10 20:02:18 MESZ	2022-04-10 13:00:34 MESZ	48	Unallocated	Allocat
MicrosoftOffice2013Office365Win64_xml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unalloc
Microsoft.Macrofficekub_18.1903.1152.0_neutral				2022-04-10 12:57:55 MESZ	2022-04-10 12:57:55 MESZ	2022-04-10 19:58:43 MESZ	2022-04-10 12:57:55 MESZ	48	Unallocated	Unalloc
[current folder]				2022-04-10 12:57:55 MESZ	2022-04-10 12:57:55 MESZ	2022-04-10 19:58:43 MESZ	2022-04-10 12:57:55 MESZ	48	Unallocated	Unalloc
[parent folder]				2022-04-10 19:58:56 MESZ	2022-04-10 19:58:56 MESZ	2022-04-10 19:58:56 MESZ	2019-12-07 10:14:52 MEZ	296	Unallocated	Allocat
Microsoft.Macrofficekub_18.1903.1152.0_x64_sh				2022-04-10 19:58:43 MESZ	2022-04-10 19:58:43 MESZ	2022-04-10 19:58:43 MESZ	2022-04-10 12:57:55 MESZ	48	Unallocated	Unalloc
[current folder]				2022-04-10 19:58:43 MESZ	2022-04-10 19:58:43 MESZ	2022-04-10 19:58:43 MESZ	2022-04-10 12:57:55 MESZ	48	Unallocated	Unalloc
[parent folder]				2022-04-10 19:58:56 MESZ	2022-04-10 19:58:56 MESZ	2022-04-10 19:58:56 MESZ	2019-12-07 10:14:52 MEZ	296	Unallocated	Allocat
ActivationStore.dat				2022-04-10 12:57:55 MESZ	2022-04-10 12:57:55 MESZ	2022-04-10 19:58:43 MESZ	2022-04-10 12:57:55 MESZ	32768	Unallocated	Unalloc
ActivationStore.dat.LOG1				2022-04-10 12:57:55 MESZ	2022-04-10 12:57:55 MESZ	2022-04-10 12:57:55 MESZ	2022-04-10 12:57:55 MESZ	32768	Unallocated	Unalloc
ActivationStore.dat.LOG2				2022-04-10 12:57:55 MESZ	2022-04-10 12:57:55 MESZ	2022-04-10 12:57:55 MESZ	2022-04-10 12:57:55 MESZ	0	Unallocated	Unalloc
Microsoft.Macrofficekub_18.1903.1152.0_neutral				2022-04-10 19:58:42 MESZ	2022-04-10 19:58:42 MESZ	2022-04-10 19:58:42 MESZ	2022-04-10 12:57:55 MESZ	48	Unallocated	Unalloc
[current folder]				2022-04-10 19:58:42 MESZ	2022-04-10 19:58:42 MESZ	2022-04-10 19:58:42 MESZ	2022-04-10 12:57:55 MESZ	48	Unallocated	Unalloc
[parent folder]				2022-04-10 19:58:56 MESZ	2022-04-10 19:58:56 MESZ	2022-04-10 19:58:56 MESZ	2019-12-07 10:14:52 MEZ	296	Unallocated	Allocat
S-1-5-71-1631604977-30160163-1851836032-1001-?				????-04-10 14:45:44 MF??	????-04-10 14:45:44 MF??					

15. Search for communication accounts

The screenshot shows the Autopsy 4.19.3 interface. On the left, the 'Data Sources' tree is expanded to 'Communication Accounts (8)', which includes 'Email (8)' and 'Phone (1)'. The main pane displays a table of search results for 'Web Data'.

Source Name	S	C	O	Account Type	ID	Data Source
Web Data				PHONE	017690784998	Windows10.iso

Below the table, the 'Accounts' section shows details for the selected account:

Type	Value	Source(s)
Account Type	PHONE	
ID	017690784998	
Source File Path	img_windows10.iso\vol_1\06\Users\BadGuy\AppData\Local\Microsoft\Edge\User Data\Default\Web Data	
Artifact ID	923372036854775403	

16. Read emails

The screenshot shows the Autopsy 4.19.3 interface. On the left, the 'Data Sources' tree is expanded to 'E-Mail Messages (7)', which includes '[Gmail] (Alle Nachrichten)' and 'Default (5)'. The main pane displays a table of search results for 'E-Mail Messages'.

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)
INBOX				no-reply@accounts.google.com	badguy12345asd@gmail.com	Sicherheitswarnung	2022-04-10 19:34:57 MESZ	[Image: Google] Windows wurde zugr...
INBOX				googlecommunityteam-noreply@google.com	badguy12345asd@gmail.com	Bad, Einrichtung Ihres neuen Google-Kontos beenden	2022-04-10 19:31:41 MESZ	Hallo Bad, willkommen bei Google. H...
INBOX				no-reply@accounts.google.com	badguy12345asd@gmail.com	Sicherheitswarnung	2022-04-10 19:39:54 MESZ	[Image: Google] Mozilla Thunderbird...
INBOX				no-reply@mail.instagram.com	badguy12345asd@gmail.com	967304 is your Instagram code	2022-04-10 19:46:50 MESZ	
INBOX				security@mail.instagram.com	badguy12345asd@gmail.com	New login to Instagram from Edge on Windows	2022-04-10 19:47:19 MESZ	

Below the table, the 'E-Mail Messages' section shows details for the selected email:

From: security@mail.instagram.com; 2022-04-10 19:47:19 MESZ
To: badguy12345asd@gmail.com;
CC:
Subject: New login to Instagram from Edge on Windows

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Hide Images

Instagram

We noticed a new login,
badguy101420

We noticed a login from a device you don't usually use.

Windows - Edge - Blaubeuren, Germany
April 10 at 10:47 AM (PDT)

17. Installed Software

TestCase - Autopsy 4.19.3

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

Installed Programs

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page:

Save Table as CSV

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	Mozilla Maintenance Service v.91.8.0	2022-04-10 17:39:17 MESZ	Windows10.iso
SOFTWARE			0	Mozilla Thunderbird (x64 de) v.91.8.0	2022-04-10 17:39:16 MESZ	Windows10.iso
SOFTWARE			0	VMware Tools v.11.3.5.18557794	2022-04-10 12:41:43 MESZ	Windows10.iso
SOFTWARE			0	Microsoft Visual C++ 2019 164 Additional Runtime - 14.28....	2022-04-10 12:40:59 MESZ	Windows10.iso
SOFTWARE			0	Microsoft Visual C++ 2019 164 Minimum Runtime - 14.28.2....	2022-04-10 12:40:58 MESZ	Windows10.iso
SOFTWARE			0	DIM_Runtim	2019-12-07 14:54:53 MEZ	Windows10.iso
SOFTWARE			0	MPlayer2	2019-12-07 09:17:28 MEZ	Windows10.iso
SOFTWARE			0	AddressBook	2019-12-07 09:17:28 MEZ	Windows10.iso
SOFTWARE			0	Connection Manager	2019-12-07 09:17:28 MEZ	Windows10.iso
SOFTWARE			0	DirectDrawEx	2019-12-07 09:17:28 MEZ	Windows10.iso
SOFTWARE			0	Fontcore	2019-12-07 09:17:28 MEZ	Windows10.iso
SOFTWARE			0	IE40	2019-12-07 09:17:28 MEZ	Windows10.iso
SOFTWARE			0	IE4Data	2019-12-07 09:17:28 MEZ	Windows10.iso
SOFTWARE			0	IESBAEX	2019-12-07 09:17:28 MEZ	Windows10.iso
SOFTWARE			0	IESData	2019-12-07 09:17:28 MEZ	Windows10.iso

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

Result: of Result

18. Recent opened documents

TestCase - Autopsy 4.19.3

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

Recent Documents

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page:

Save Table as CSV

Source Name	S	C	O	Path	Date Accessed	Data Source
8684_2.Link				C:\Users\BadGuy\Downloads\8684_2.webp	2022-04-10 19:28:36 MESZ	Windows10.iso
BecomeAHacker.Link				C:\Users\BadGuy\Downloads\BecomeAHacker.pdf	2022-04-10 19:55:10 MESZ	Windows10.iso
Cat03.Link				C:\Users\BadGuy\Downloads\Cat03.jpg	2022-04-10 19:28:29 MESZ	Windows10.iso
Downloads.Link				C:\Users\BadGuy\Downloads	2022-04-10 19:28:30 MESZ	Windows10.iso
Herunterladen.Link				C:\Users\BadGuy\Downloads\Herunterladen.jpg	2022-04-10 19:29:14 MESZ	Windows10.iso
How To Become A Hacker.Link				C:\Users\BadGuy\Downloads\How To Become A Hacker.pdf	2022-04-10 19:55:18 MESZ	Windows10.iso
https-go.microsoft.com-fvlink-linkid=2060958.Link				No preferred path found	2022-04-10 14:45:08 MESZ	Windows10.iso
Internet.Link				No preferred path found	2022-04-10 14:44:29 MESZ	Windows10.iso
ms-gamingoverlay-igcheck-.Link				No preferred path found	2022-04-10 14:44:29 MESZ	Windows10.iso
Password.Link				C:\Users\BadGuy\Desktop>Password.txt	2022-04-10 19:30:18 MESZ	Windows10.iso
8684_2.webp.Link				C:\Users\BadGuy\Downloads\8684_2.webp	0000-00-00 00:00:00	Windows10.iso
Password.txt.Link				C:\Users\BadGuy\Desktop>Password.txt	0000-00-00 00:00:00	Windows10.iso
How To Become A Hacker.pdf.Link				C:\Users\BadGuy\Downloads\How To Become A Hacker.pdf	0000-00-00 00:00:00	Windows10.iso
No preferred path found.Link				No preferred path found	0000-00-00 00:00:00	Windows10.iso
BecomeAHacker.pdf.Link				C:\Users\BadGuy\Downloads\BecomeAHacker.pdf	0000-00-00 00:00:00	Windows10.iso

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

Strings Indexed Text Translation

Page: 1 of Page Go to Page:

Script: Latin-Basic

19. Analyze web Accounts

TestCase - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

Web Accounts

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Source Name	S	C	O	URL	Date Created	Decoded URL	Username	Realm	Domain	Program Name	Date
Login Data				https://accounts.google.com/signup/v2/webcreateaccount	2022-04-10 19:31:49 MESZ	google.com	badguy12345asd	https://accounts.google.com/	google.com	Microsoft Edge	Win

Web Accounts (1)

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

Result: 1 of 1 Result: Web Accounts

Time	Value	Source(s)
URL	https://accounts.google.com/signup/v2/webcreateaccount	Recent Activity
Date Created	2022-04-10 19:31:49 MESZ	Recent Activity
Decoded URL	google.com	Recent Activity
Username	badguy12345asd	Recent Activity
Realm	https://accounts.google.com/	Recent Activity
Domain	google.com	Recent Activity
Source File Path	/img_Windows10.iso/vol_vols/Users/BadGuy/AppData/Local/Microsoft/Edge/User Data/Default/Login Data	Recent Activity
Artifact ID	-9223372036854775406	

20. Analyze web cookies

TestCase - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

Web Cookies

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Source Name	S	C	O	URL	Date Accessed	Name	Value	Program Name	Domain	Data Source
Cookies				man.com	2022-04-10 19:50:07 MESZ	_ss		Microsoft Edge	man.com	Windows10.iso
Cookies				rtp.man.com	2022-04-10 19:50:07 MESZ	msaoptout		Microsoft Edge	rtp.man.com	Windows10.iso
Cookies				rtp.man.com	2022-04-10 19:50:07 MESZ	sptmarket		Microsoft Edge	rtp.man.com	Windows10.iso
Cookies				de.indeed.com	2022-04-10 15:04:21 MESZ	CHP_YTISITED		Microsoft Edge	de.indeed.com	Windows10.iso
Cookies				.indeed.com	2022-04-10 15:04:09 MESZ	CTK		Microsoft Edge	indeed.com	Windows10.iso
Cookies				de.indeed.com	2022-04-10 15:04:09 MESZ	CTK		Microsoft Edge	de.indeed.com	Windows10.iso
Cookies				www.berliner-sparkasse.de	2022-04-10 15:04:17 MESZ	IF_SPWDE_CHECK		Microsoft Edge	www.berliner-sparkasse.de	Windows10.iso
Cookies				www.ariva.de	2022-04-10 15:04:21 MESZ	ISSE		Microsoft Edge	www.ariva.de	Windows10.iso
Cookies				de.indeed.com	2022-04-10 15:04:21 MESZ	LV		Microsoft Edge	de.indeed.com	Windows10.iso
Cookies				www.indeed.com	2022-04-10 15:04:09 MESZ	LV		Microsoft Edge	www.indeed.com	Windows10.iso
Cookies				www.onvista.de	2022-04-10 15:04:09 MESZ	OAID		Microsoft Edge	www.onvista.de	Windows10.iso
Cookies				.indeed.com	2022-04-10 15:04:20 MESZ	OptanonConsent		Microsoft Edge	indeed.com	Windows10.iso
Cookies				.royalgames.com	2022-04-10 15:04:13 MESZ	OptanonConsent		Microsoft Edge	royalgames.com	Windows10.iso
Cookies				.ikea.com	2022-04-10 15:31:46 MESZ	OptanonConsent		Microsoft Edge	www.ikea.com	Windows10.iso

Web Cookies (343)

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

Strings Indexed Text Translation

Page: 1 of Page: Go to Page: Script: Latin - Basic

21. Browse “encryption suspected” files

The screenshot shows the Autopsy 4.19.3 interface. On the left sidebar, under 'Analysis Results', 'Encryption Suspected (2)' is highlighted. The main pane displays a table of files suspected of encryption.

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment	File Path
mpenginedb.db			0	File	Likely Notable			Suspected encryption due to high entropy (7,981510).	Suspected encryption due to high entropy (7,981510).	[img_Windo
iconcache_256.db			0	File	Likely Notable			Suspected encryption due to high entropy (7,926102).	Suspected encryption due to high entropy (7,926102).	[img_Windo

22. Analyze OS Accounts

The screenshot shows the Autopsy 4.19.3 interface. On the left sidebar, under 'Analysis Results', 'OS Accounts' is highlighted. The main pane displays a table of OS accounts.

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-80-956008885-3418522649-1831038044-185329			0		Windows1...	Local		
S-1-5-18			0	systemprofile	Windows1...	Local		
S-1-5-80-3028837079-3186095147-955107200-370196			0		Windows1...	Local		
S-1-5-19			0	LocalService	Windows1...	Local		
S-1-5-21-1163160977-3019039153-1851826052-1001			0	BadGuy	Windows1...	Local		2022-04-10 14:34:43 MESZ
S-1-5-20			0	NetworkService	Windows1...	Local		
S-1-5-21-1163160977-3019039153-1851826052-1000			0		Windows1...	Local		
S-1-5-80-2620923248-4247863784-3378508180-26591			0		Windows1...	Local		
S-1-5-21-3933942852-973373972-2766786355-1032			0		Windows1...	Local		
S-1-5-21-1163160977-3019039153-1851826052-501			0	Guest	Windows1...	Local		2022-04-10 13:00:30 MESZ
S-1-5-21-1163160977-3019039153-1851826052-500			0	Administrator	Windows1...	Local		2022-04-10 13:00:30 MESZ
S-1-5-21-1163160977-3019039153-1851826052-504			0	WDAGUtilityAccount	Windows1...	Local		2022-04-10 13:00:30 MESZ
S-1-5-21-1163160977-3019039153-1851826052-503			0	DefaultAccount	Windows1...	Local		2022-04-10 13:00:30 MESZ

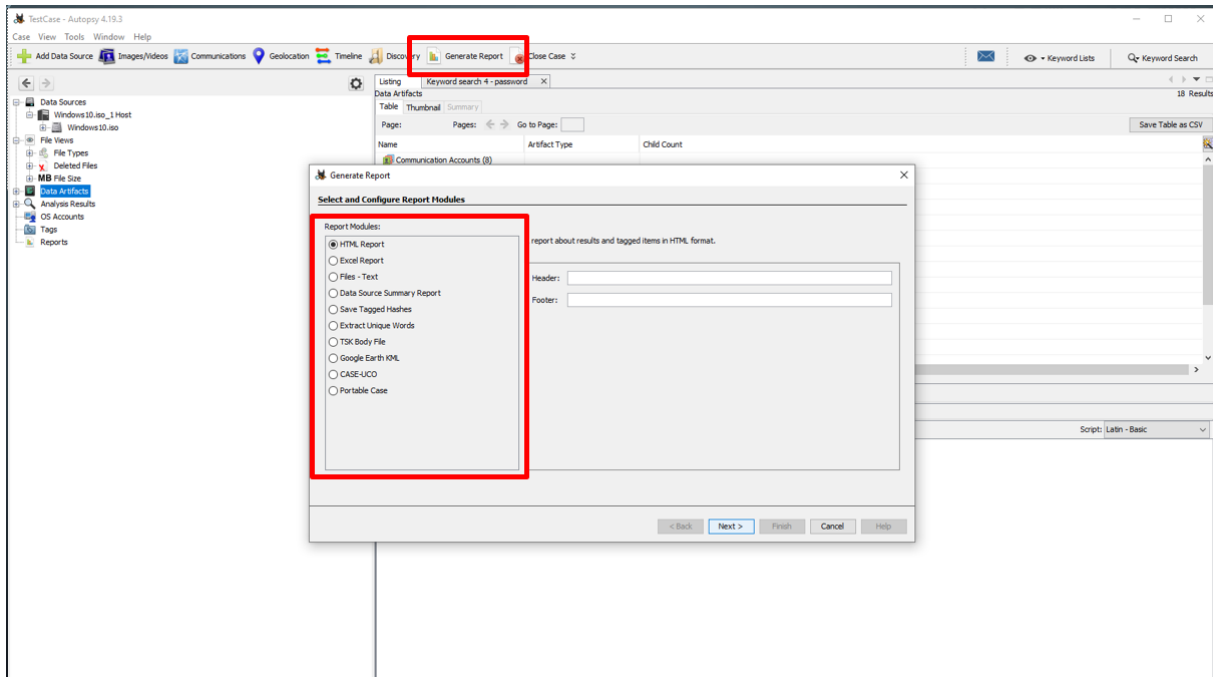
Below the table, the 'Basic Properties' for the selected account 'BadGuy' are shown:

Basic Properties
Login: BadGuy
Full Name: S-1-5-21-1163160977-3019039153-1851826052-1001
Address: S-1-5-21-1163160977-3019039153-1851826052-1001
Type: Password Hash
Creation Date: 2022-04-10 14:34:43 MESZ

Windows10.iso_1 Host Details
Last Login: 2022-04-10 19:24:30 MESZ
Login Count: 8
Password Hash: 123456
Password For Date: 2022-04-10 14:45:56 MESZ
Password Settings: Password does not expire, Password not required
Flags: Normal user account
Home Directory: C:\Users\BadGuy

Realm Properties
Name: Unknown
Address: S-1-5-21-1163160977-3019039153-1851826052
Scope: Local
Confidence: Inferred

23. Create Report using the “Generate Report” Button



24. Example of a report

Report Navigation

- Case Summary
- Accounts: Email (8)
- Accounts: Phone (1)
- Data Source Usage (1)
- E-Mail Messages (7)
- EXIF Metadata (7)
- Encryption Suspected (2)
- Extension Mismatch Detected (37)
- Installed Programs (39)
- Keyword Hits (296800)
- Metadata (99)
- Operating System Information (2)
- Recent Documents (22)
- Run Programs (1091)
- Shell Bags (6)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- USB Device Attached (6)
- User Content Suspected (7)
- Web Account Type (1)
- Web Accounts (1)
- Web Bookmarks (6)

Autopsy Forensic Report

HTML Report Generated on 2022/04/27 21:59:50

Case: TestCase
Case Number: 001
Number of data sources in case: 1
Examiner: Thomas

Image Information:

Windows10.iso

Timezone: Europe/Berlin
Path: D:\Eigene Dateien\Dokumente\VirtualBoxGemeinsamerOrdner\Windows10.iso

Software Information:

Autopsy Version: 4.19.3
Android Analyzer Module: 4.19.3
Android Analyzer (aLEAPP) Module: 4.19.3
Central Repository Module: 4.19.3
DJI Drone Analyzer Module: 4.19.3
Data Source Integrity Module: 4.19.3
Email Parser Module: 4.19.3
Embedded File Extractor Module: 4.19.3
Encryption Detection Module: 4.19.3
Extension Mismatch Detector Module: 4.19.3
File Type Identification Module: 4.19.3
GPX Parser Module: 1.2