Autopsy

Sreekanth N

Agenda

- Introduction
- Features
- Screenshots
- Demo
- Results
- Conclusion
- References

Introduction

- **Digital Forensics**
- Autopsy

- Digital forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law.

Introduction

- **Digital Forensics**
- Autopsy

- Digital forensics activities commonly include:
  - the secure collection of computer data
  - the identification of suspect data
  - the examination of suspect data to determine details such as origin and content
  - the presentation of computer-based information to courts of law
  - the application of a country's laws to computer practice.

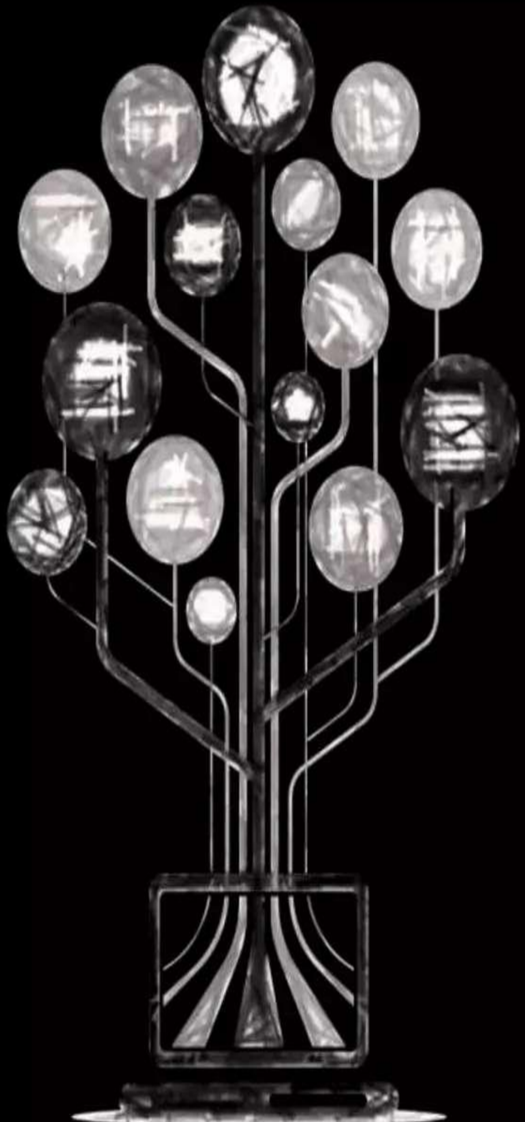
Introduction

- Digital Forensics
- **Autopsy**

- Autopsy is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-in architecture that allows you to find add-on modules or develop custom modules in Java or Python.
- It can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3, etc.).

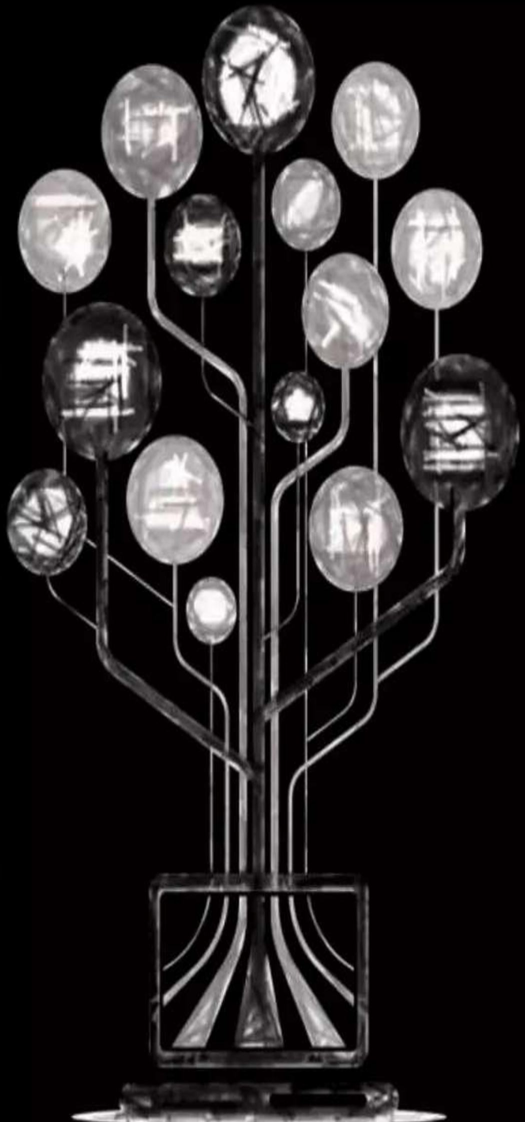
Features

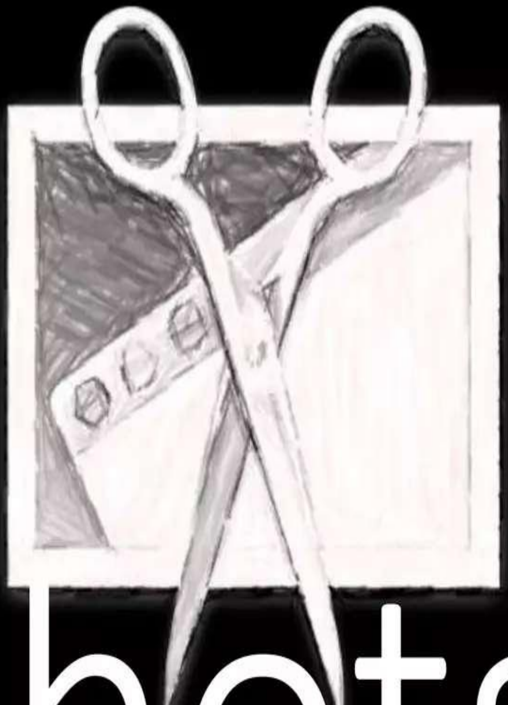
- Multi-User Cases: Collaborate with fellow examiners on large cases.
- Timeline Analysis: Displays system events in a graphical interface to help identify activity.
- Keyword Search: Text extraction and index searched modules enable you to find files that mention specific terms and find regular expression patterns.
- Web Artifacts: Extracts web activity from common browsers to help identify user activity.
- Registry Analysis: Uses RegRipper to identify recently accessed documents and USB devices.
- LNK File Analysis: Identifies short cuts and accessed documents
- Email Analysis: Parses MBOX format messages, such as Thunderbird.



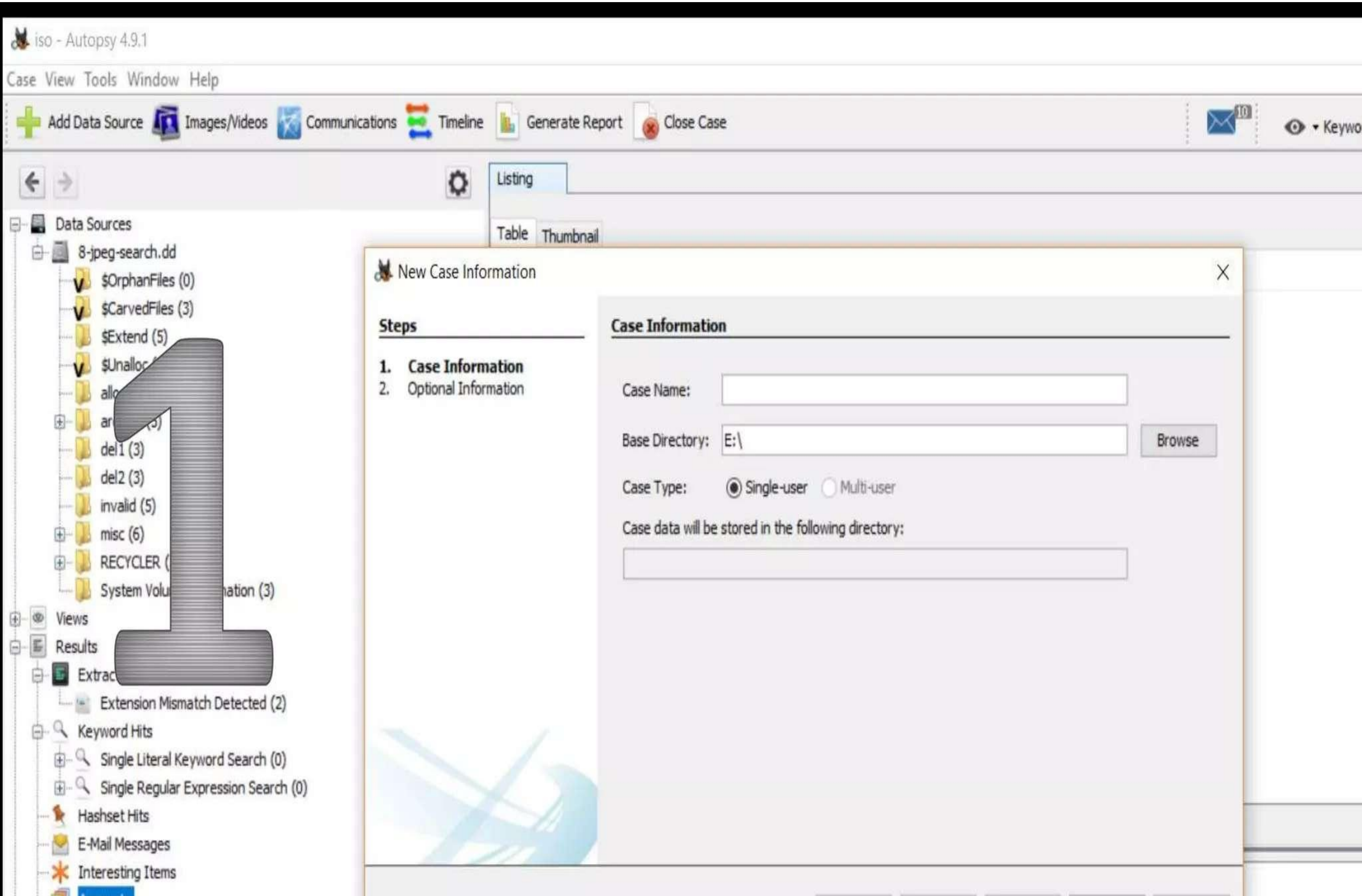
Features

- Media Playback and Thumbnail viewer.
- Robust File System Analysis: Support for common file systems, including NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2,
- Unicode Strings Extraction: Extracts strings from unallocated space and unknown file types in many languages
- File Type Detection based on signatures and extension mismatch detection.
- Interesting Files Module will flag files and folders based on name and path.
- Android Support: Extracts data from SMS, call logs, contacts, Tango, Words with Friends, and more.





Screenshots



New Case Information

Steps

1. **Case Information**
2. Optional Information

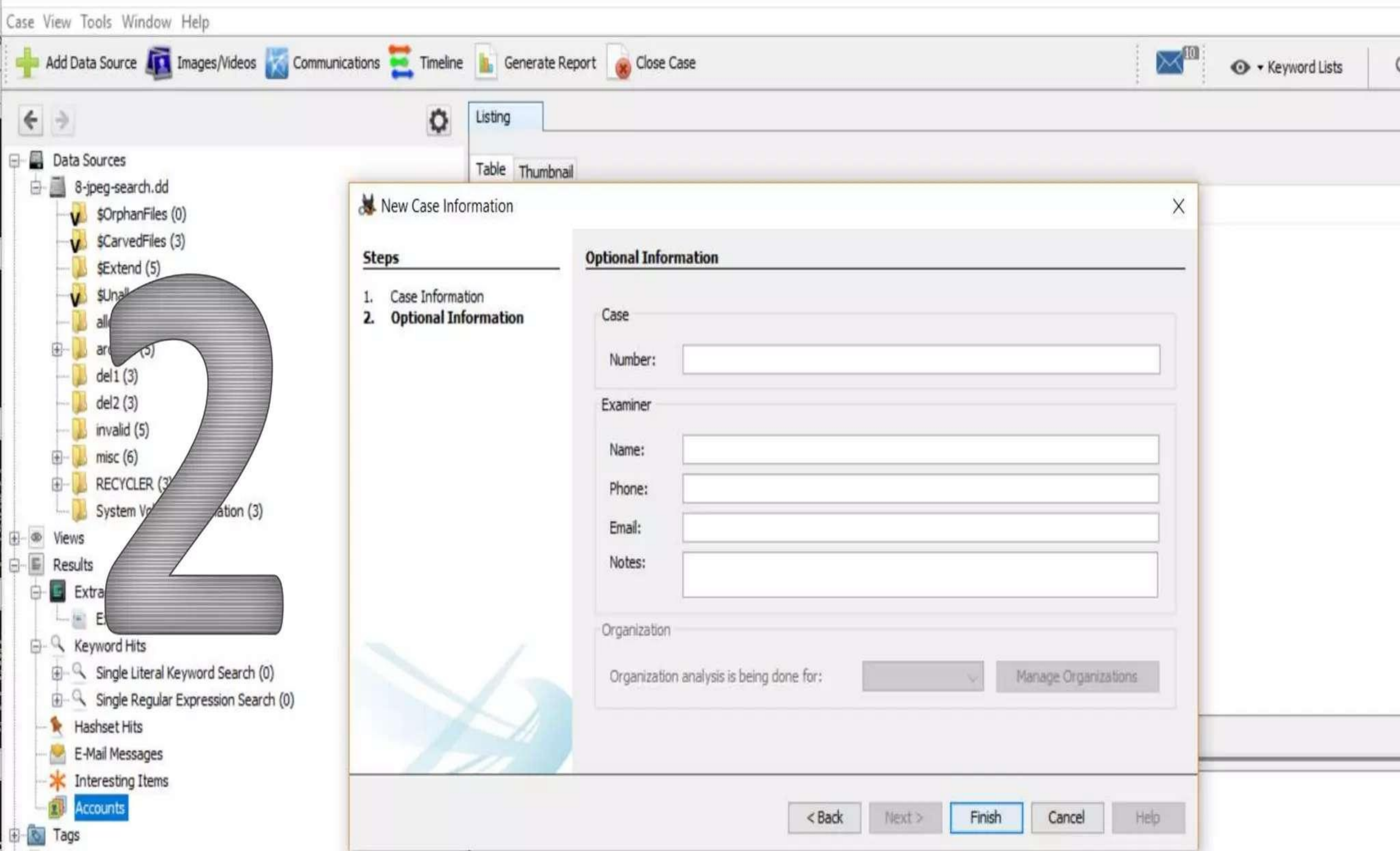
Case Information

Case Name:

Base Directory: E:\ Browse

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number:

Examiner

Name:

Phone:

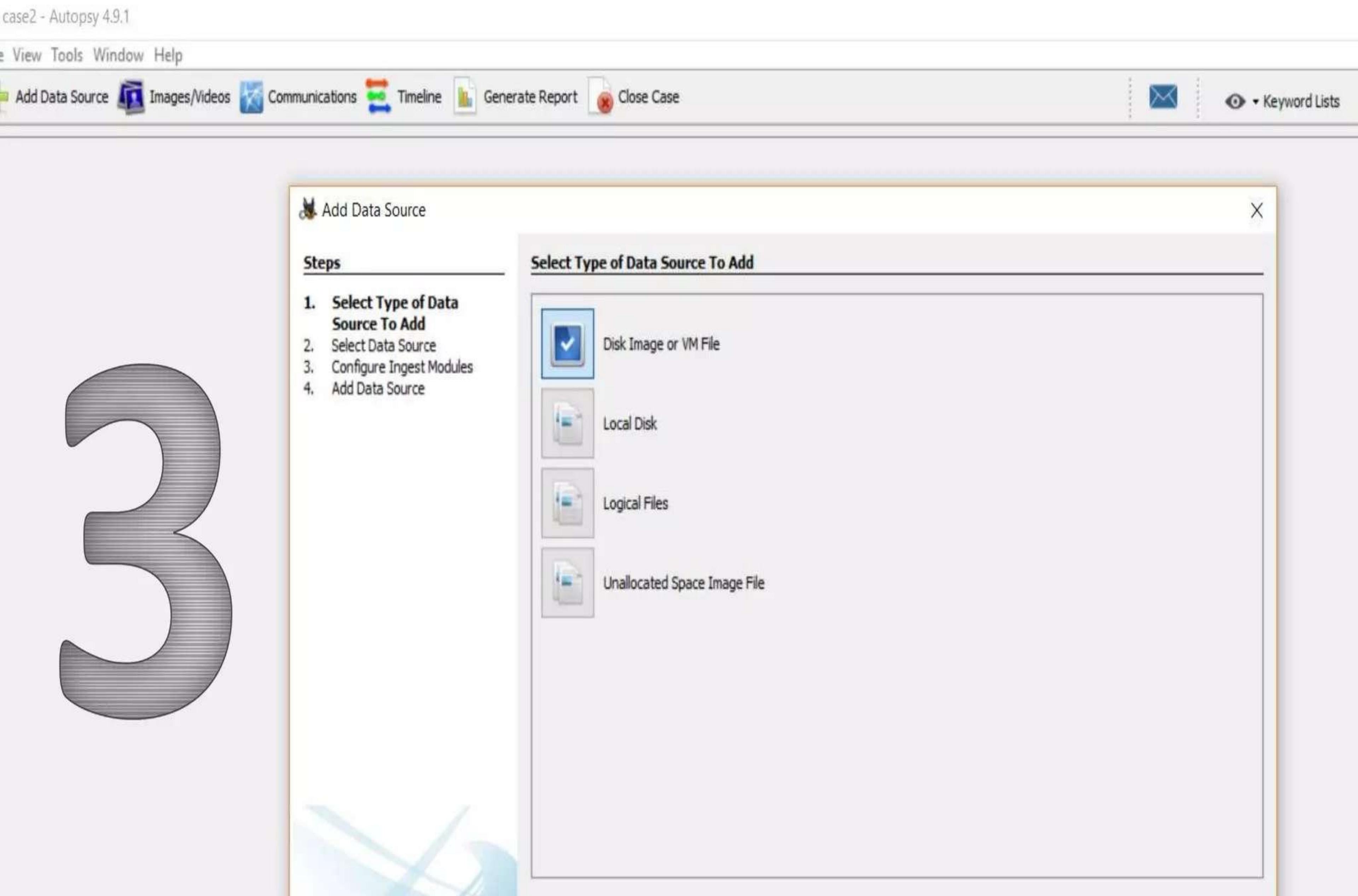
Email:

Notes:

Organization

Organization analysis is being done for:

3



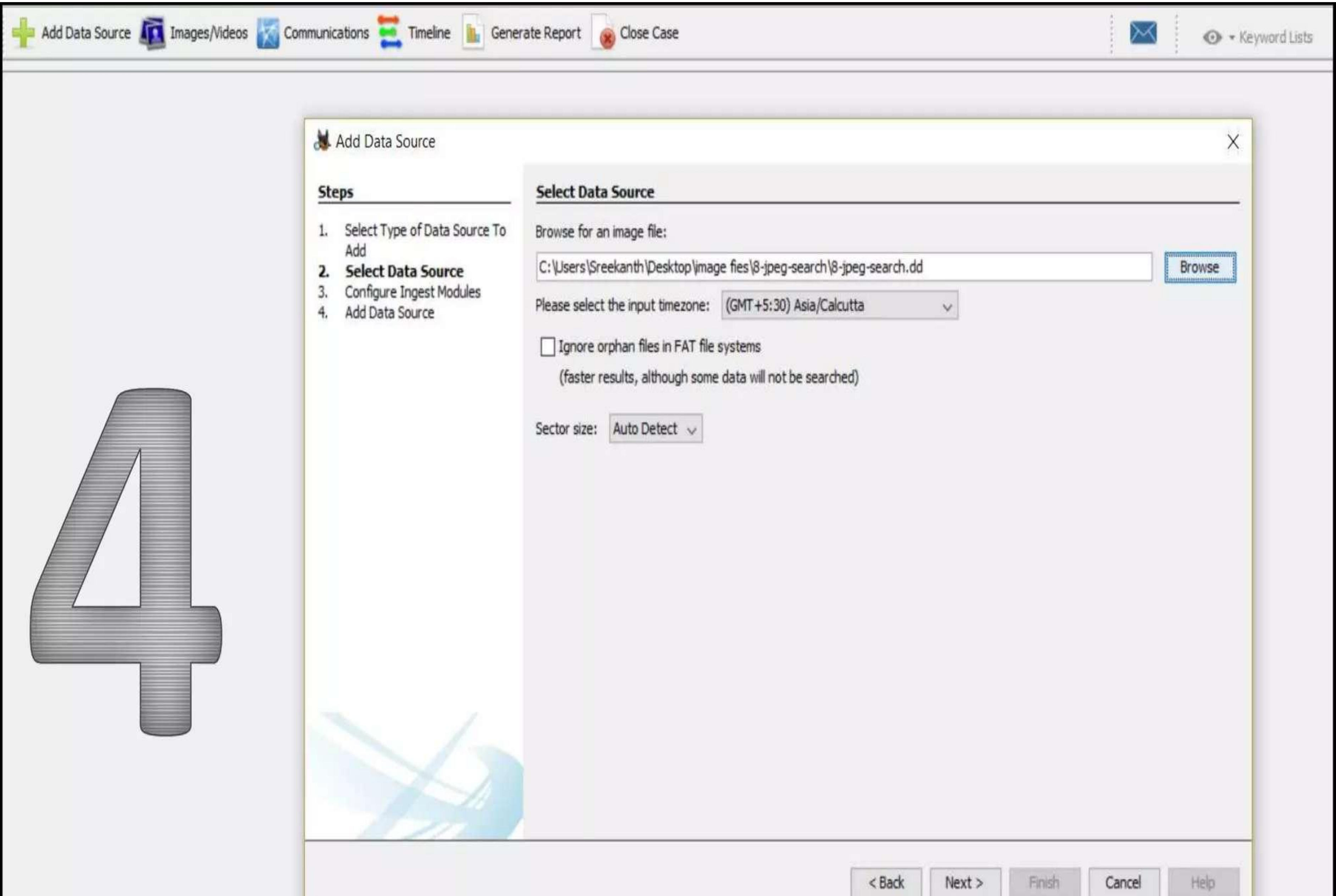
Steps

1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

- ☑ Disk Image or VM File
- Local Disk
- Logical Files
- Unallocated Space Image File

4



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Browse for an image file:

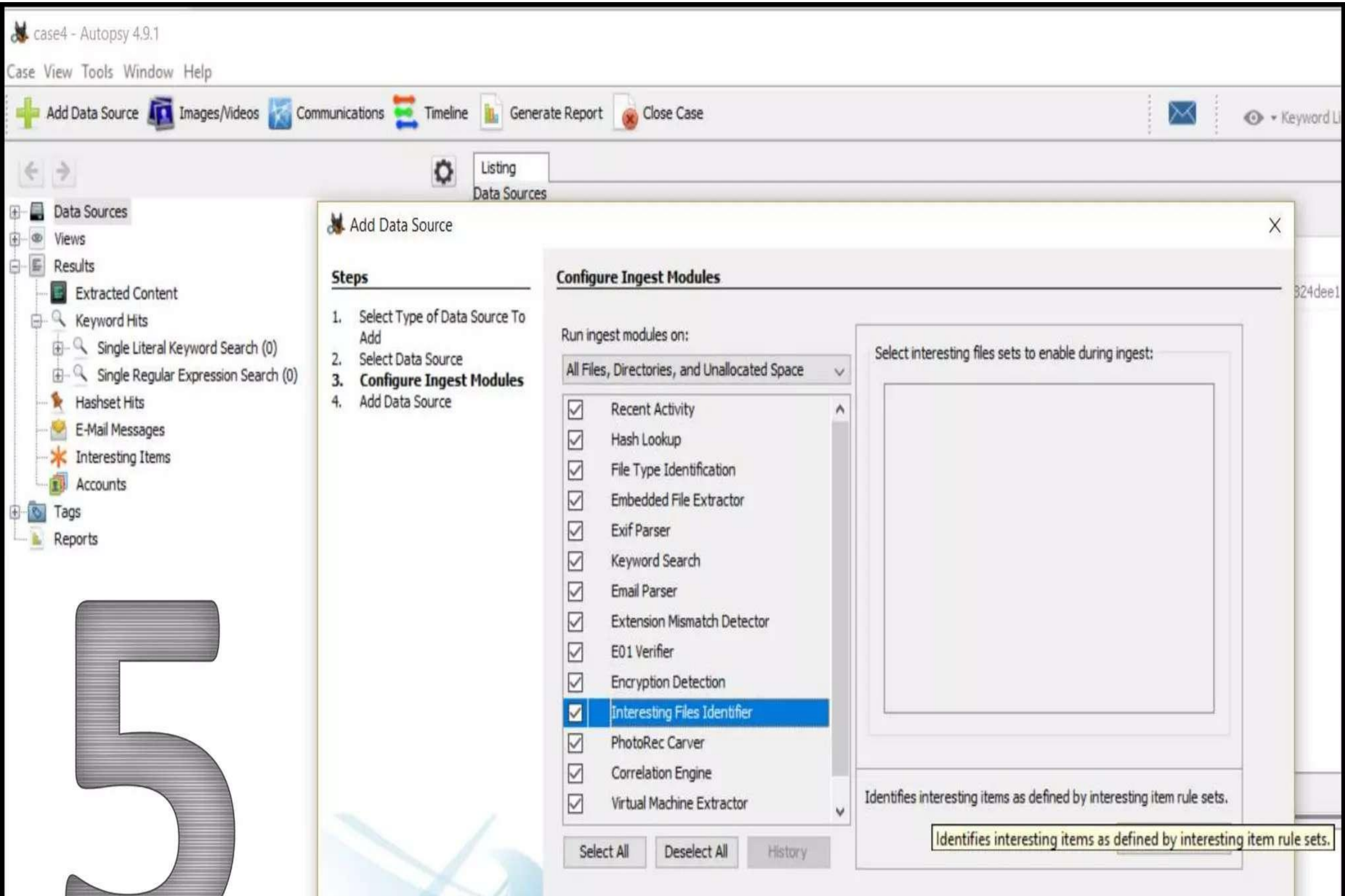
C:\Users\Sreekanth\Desktop\image fies\8-jpeg-search\8-jpeg-search.dd

Please select the input timezone: (GMT+5:30) Asia/Calcutta

☐ Ignore orphan files in FAT file systems

(faster results, although some data will not be searched)

Sector size: Auto Detect



Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

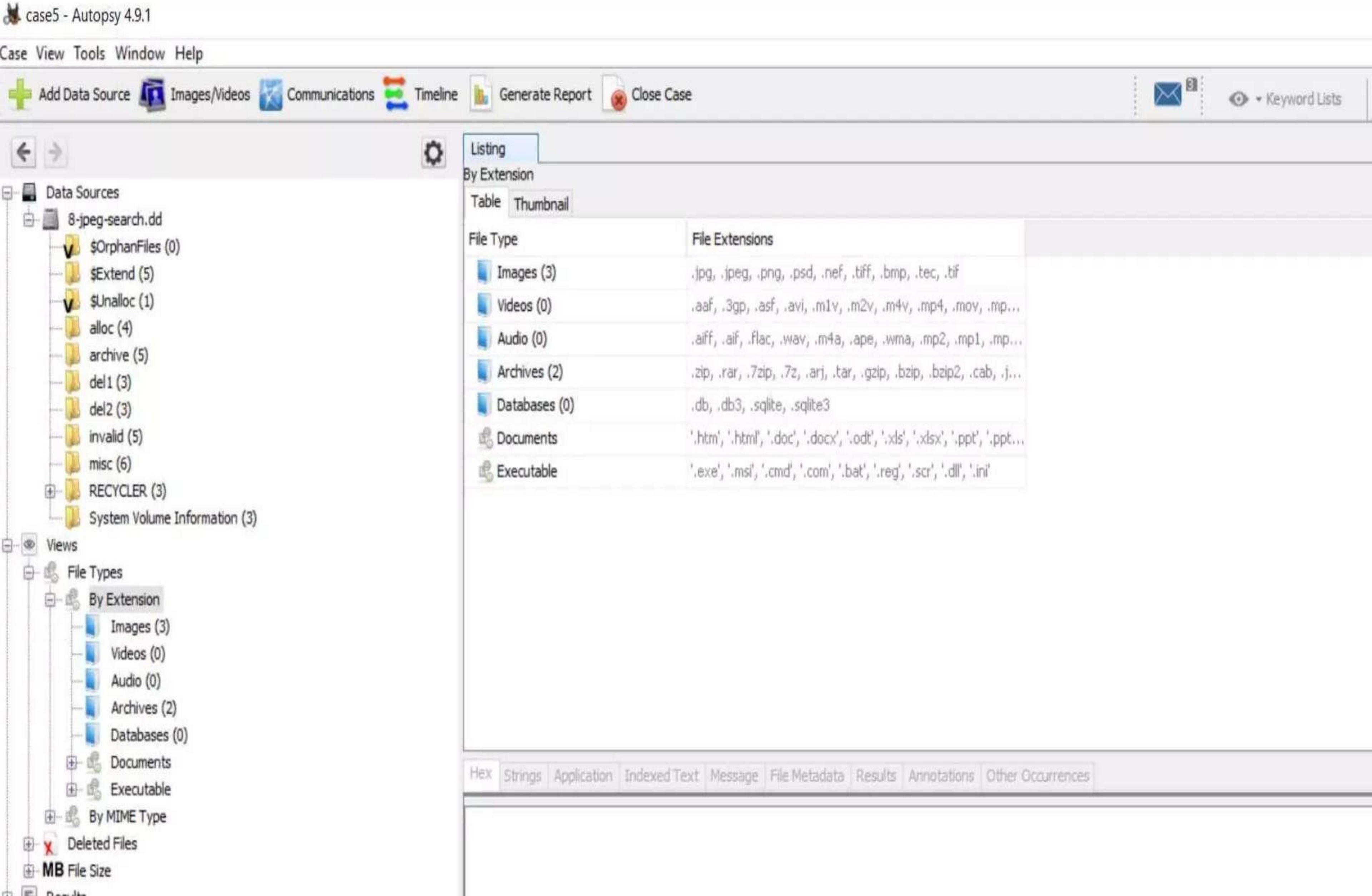
- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ Correlation Engine
- ☑ Virtual Machine Extractor

Select interesting files sets to enable during ingest:

Identifies interesting items as defined by interesting item rule sets.

Identifies interesting items as defined by interesting item rule sets.

Results



File Type	File Extensions
Images (3)	.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif
Videos (0)	.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mp...
Audio (0)	.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp...
Archives (2)	.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .j...
Databases (0)	.db, .db3, .sqlite, .sqlite3
Documents	'.htm', '.html', '.doc', '.docx', '.odt', '.xls', '.xlsx', '.ppt', '.ppt...
Executable	'.exe', '.msi', '.cmd', '.com', '.bat', '.reg', '.scr', '.dll', '.ini'

- Important Links - Hexeditor https://mh-nexus.de/en/hxd/

Assignments

- Download SuspectData.dd file from folder SuspectData and explore the same using autopsy.
- Ensure you name your folder in the following format example 001-M-DJD-S
- Inside that folder you must have the following folders
  - Autopsy - Inside this your autopsy files should go
  - Docs - maintain a txt file with the artifact name. That text file should maintain time stamps of all that you do.
  - Images – Make sure you create a folder Exhibit001 and inside that the image that you received/ created using some imaging sft (FTK Imager)
  - Reports - The reports that you generate should be in this folder
  - Temp – Temporary data should be here
- Maintain all the records anything interesting that you find accordingly

References

- https://www.sleuthkit.org/autopsy/
- https://www.autopsy.com/
- https://en.wikipedia.org/wiki/Autopsy_(software)
- https://resources.infosecinstitute.com/category/computerforensics/introduction/free-open-source-tools/autopsy-forensics-platform-overview/#gref

Thank you
danke
nandri
takk
grazie
hvala
gracias
dziękuję
děkuji
kiitos
Xièxiè
a dank
ευχαριστώ
mahalo
tänan
dank u
tack
arigatô
감사합니다
спасибо
gràcies
благодаря
köszönöm
הדות.
Mh'gōi
Շնորհակալություն
merci
ačiū
shukran
terima kasih
tak
ngiyabonga
obrigado
teşekkür ederim
paldies
Ďakujem
diolch
dhanyavād
dankie
grazzi
choukrane
Баярлалаа
bagodaram
дякую
faleminderit
хвала
mulţumesc