SLEUTH KIT

Aim:

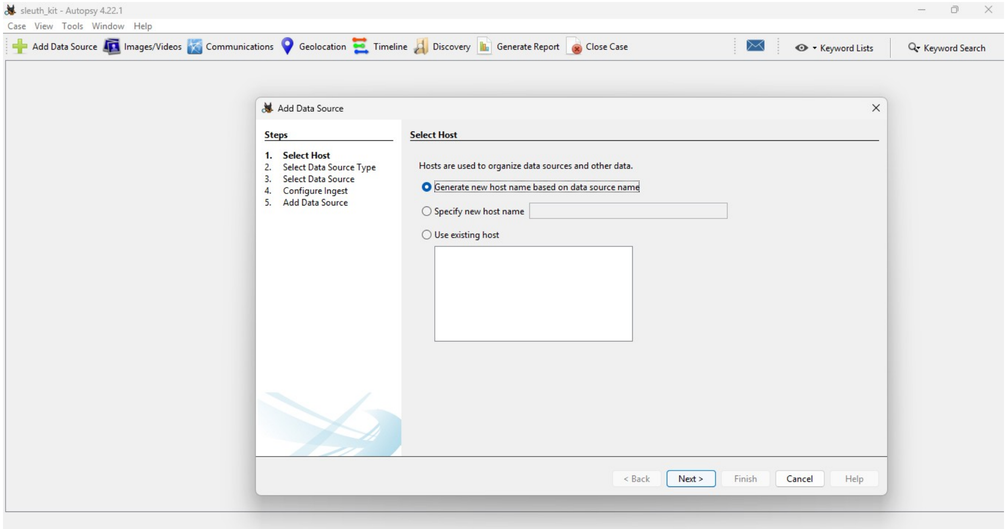
To analyze a digital evidence disk image using **Autopsy (GUI for The Sleuth Kit)** in order to extract file system information, recover deleted files, examine metadata, and generate a forensic investigation report.

TOOL DESCRIPTION:

The Sleuth Kit (TSK) is a collection of command-line forensic tools used to investigate disk images. It supports file system analysis, timeline creation, and evidence recovery. Autopsy uses Sleuth Kit internally to perform these analyses through a graphical interface. The toolkit helps in locating deleted files, partitions, and file attributes for forensic reporting. It is useful for learning both manual and automated evidence examination. This experiment showed how Autopsy builds on TSK to deliver efficient forensic results.

Steps involved in Autopsy (GUI for the Sleuth Kit):

Create a new case in Autopsy



Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

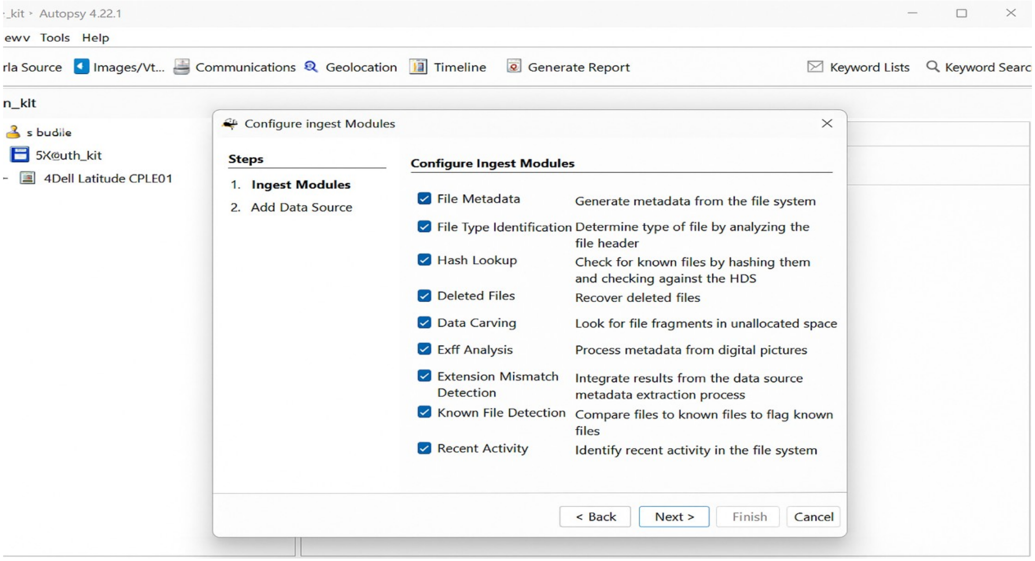
Select Host

Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host



Configure ingest Modules

Steps

1. **Ingest Modules**
2. Add Data Source

Configure Ingest Modules

☑ File Metadata — Generate metadata from the file system

☑ File Type Identification — Determine type of file by analyzing the file header

☑ Hash Lookup — Check for known files by hashing them and checking against the HDS

☑ Deleted Files — Recover deleted files

☑ Data Carving — Look for file fragments in unallocated space

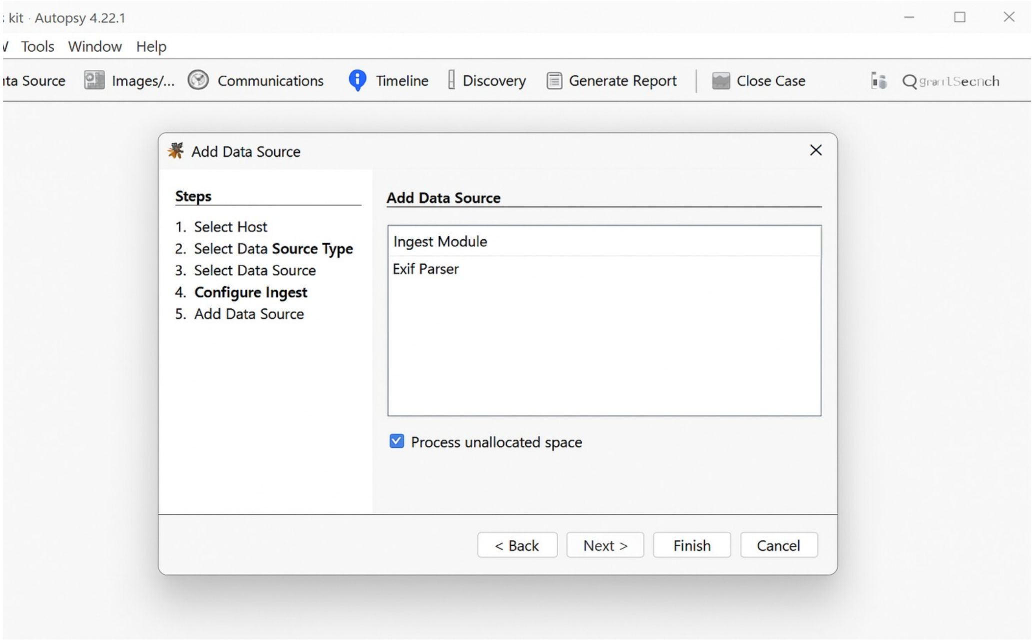
☑ Exff Analysis — Process metadata from digital pictures

☑ Extension Mismatch Detection — Integrate results from the data source metadata extraction process

☑ Known File Detection — Compare files to known files to flag known files

☑ Recent Activity — Identify recent activity in the file system

RESULT:



Add Data Source

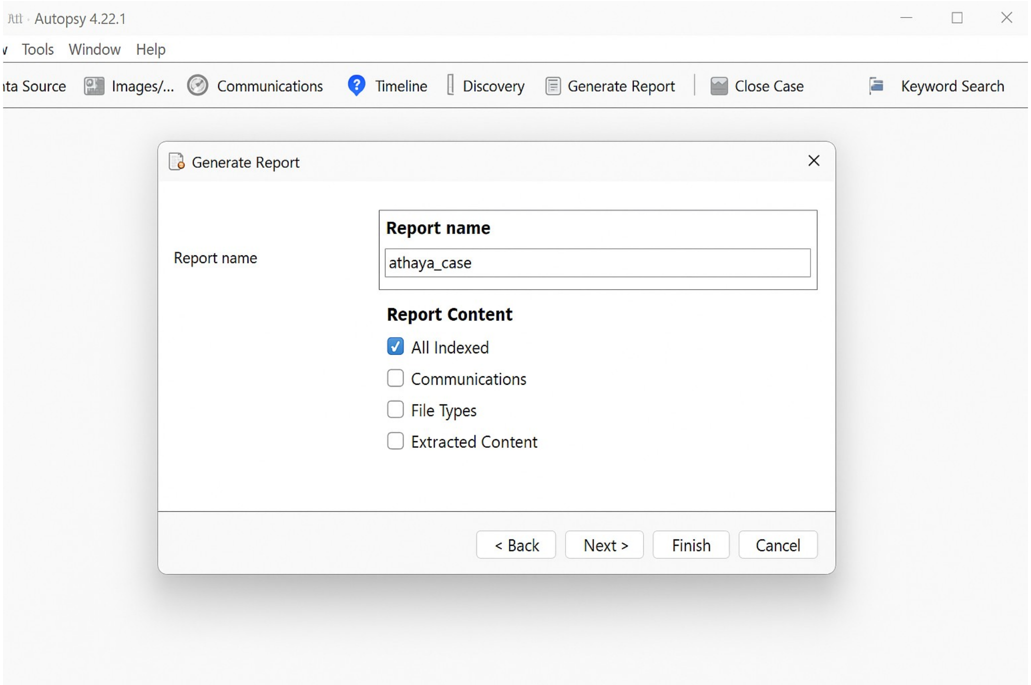
Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Add Data Source

Ingest Module
Exif Parser

☑ Process unallocated space



Report name

Report name

athaya_case

Report Content

☑ All Indexed

☐ Communications

☐ File Types

☐ Extracted Content