

11. Digital Forensics

Objective: To learn the basics of digital forensics and evidence collection

Tools: Autopsy, FTK Imager

Digital forensics is the process of investigating and analyzing electronic data to uncover and present evidence in a way that is legally admissible. It involves recovering, preserving, and examining data from computers, smartphones, servers, and other digital devices to solve crimes, resolve disputes, or investigate incidents.

Here's a breakdown of what digital forensics entails:

1. **Data Collection:** Identifying and gathering data from digital devices while ensuring that the process doesn't alter or damage the evidence. This often involves creating forensic copies (or images) of the data.
2. **Data Preservation:** Ensuring that the collected data remains unchanged throughout the investigation. This involves using specialized tools and techniques to maintain the integrity of the evidence.
3. **Data Analysis:** Examining the data to identify relevant information. This can involve looking at files, metadata, logs, communications, and other types of digital information.
4. **Data Presentation:** Preparing findings in a clear and understandable format for legal proceedings or other investigations. This may involve creating reports, visualizations, or expert testimony.
5. **Incident Response:** In some cases, digital forensics is used in real-time to respond to and manage ongoing security incidents or breaches.

Autopsy

Autopsy is a widely used open-source digital forensics platform that helps investigators analyze and examine digital evidence. It provides a suite of tools for processing and investigating data from various types of digital devices, including computers, smartphones, and external storage media. Here's a closer look at what Autopsy offers:

Key Features of Autopsy:

1. **Case Management:** Allows investigators to organize and manage cases, including setting up case files and tracking evidence.
2. **Data Analysis:** Provides tools for analyzing file systems, recovering deleted files, and examining file contents. It supports a variety of file systems and can extract data from different types of devices.
3. **Search and Filtering:** Includes powerful search capabilities to find specific files or data within a case. Investigators can use keywords, file types, and other criteria to narrow down their search.
4. **Timeline Analysis:** Helps in creating and analyzing timelines based on file system activities, such as file creation, modification, and access times.
5. **File Carving:** Capable of recovering deleted or fragmented files from raw disk images.
6. **Metadata Extraction:** Extracts and analyzes metadata from files, which can provide insights into file origins, modifications, and other relevant details.
7. **Visualization:** Offers graphical representations of data, such as file trees, directory structures, and timeline charts, to aid in understanding and interpreting the evidence.

8. **Reporting:** Generates detailed reports summarizing the findings of the investigation, which can be used for legal proceedings or internal documentation.

How Autopsy Works:

- **Data Ingestion:** Forensic images of disks or individual files are imported into Autopsy. These images are often created using other forensic tools to ensure that the original data remains unaltered.
- **Analysis:** Autopsy processes the data, applying various analysis modules to identify and examine relevant evidence. Investigators can explore the data through a user-friendly interface.
- **Reporting:** After analysis, investigators can compile their findings into comprehensive reports that detail the evidence and support investigative conclusions.

Steps: Windows

1. Download the Autopsy from Google: <https://www.autopsy.com/download> **autopsy Sluthkit (64 Bit)**

1. Getting Started

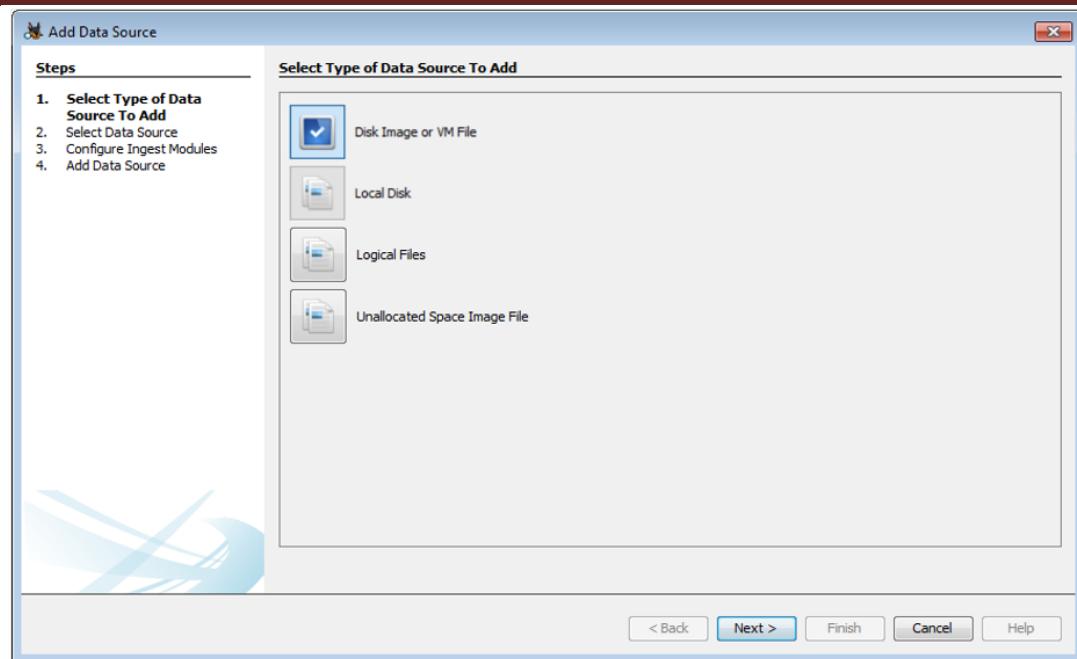
Open Autopsy and create a new case.



Click on **Finish** after completing both the steps.

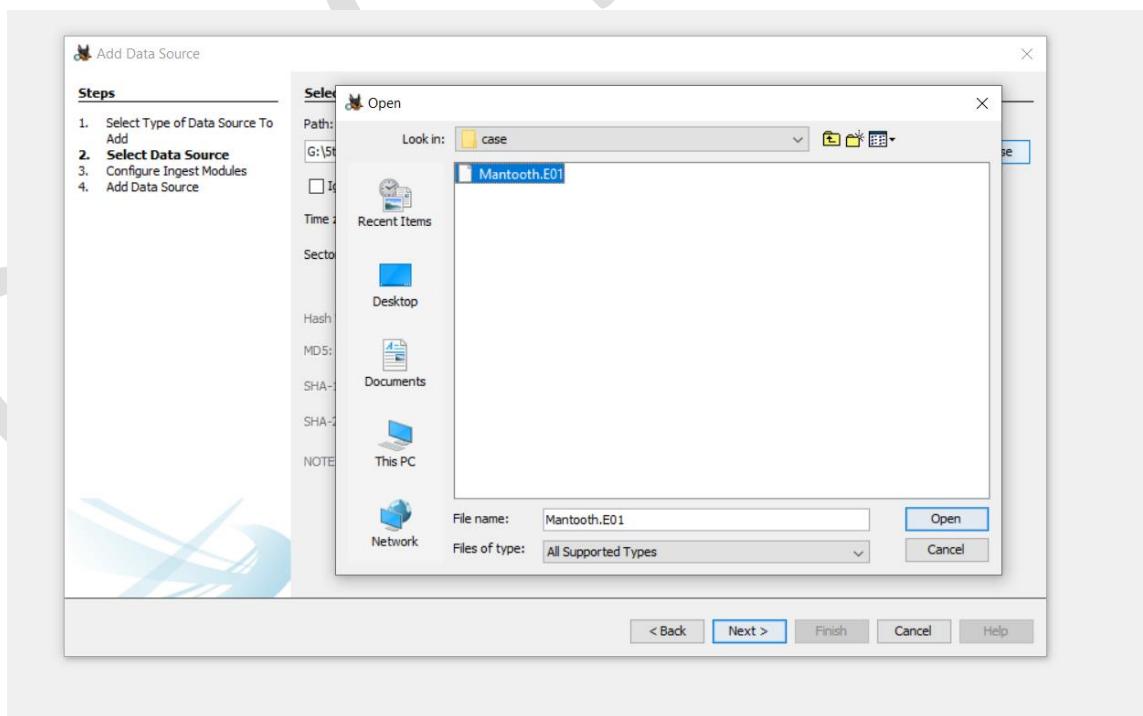
2. Add a data source.

Select the appropriate data source type.

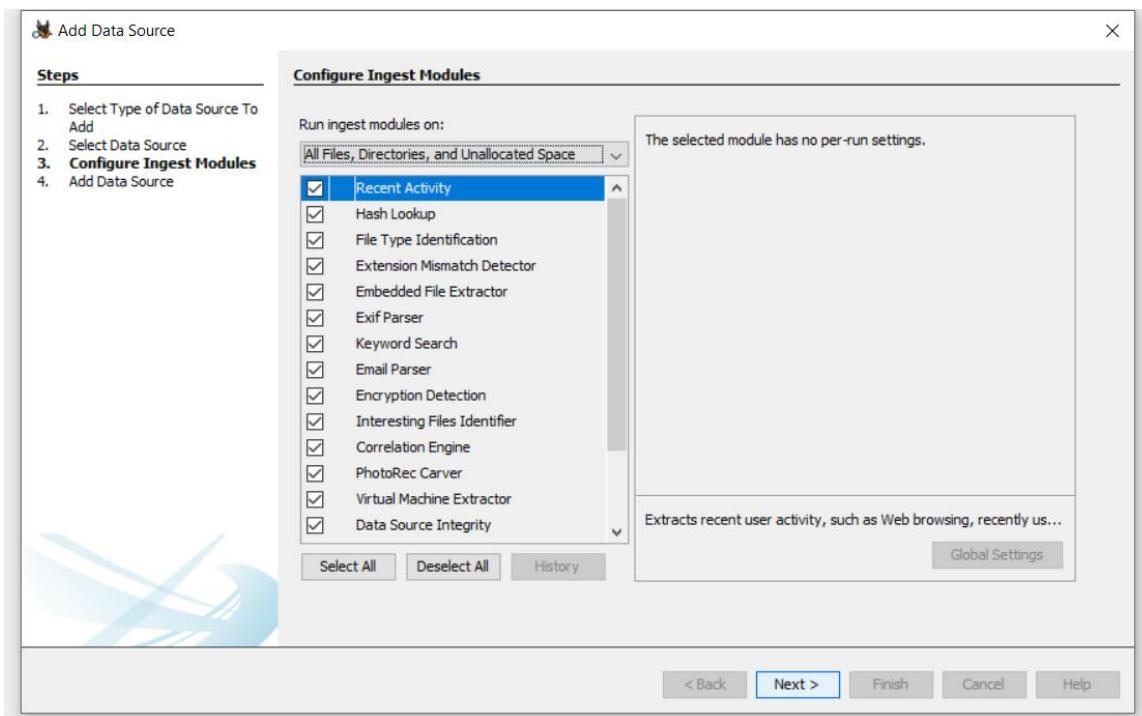


- **Disk Image or VM file:** Includes images that are an exact copy of a hard drive or media card, or a virtual machine image.
- **Local Disk:** Includes Hard disk, Pendrive, memory card, etc.
- **Logical Files:** Includes local folders or files.
- **Unallocated Space Image File:** Includes files that do not contain a file system but need to run through ingest.

The data source used here is a disk image. Add the data source destination.



Configure ingest modules.

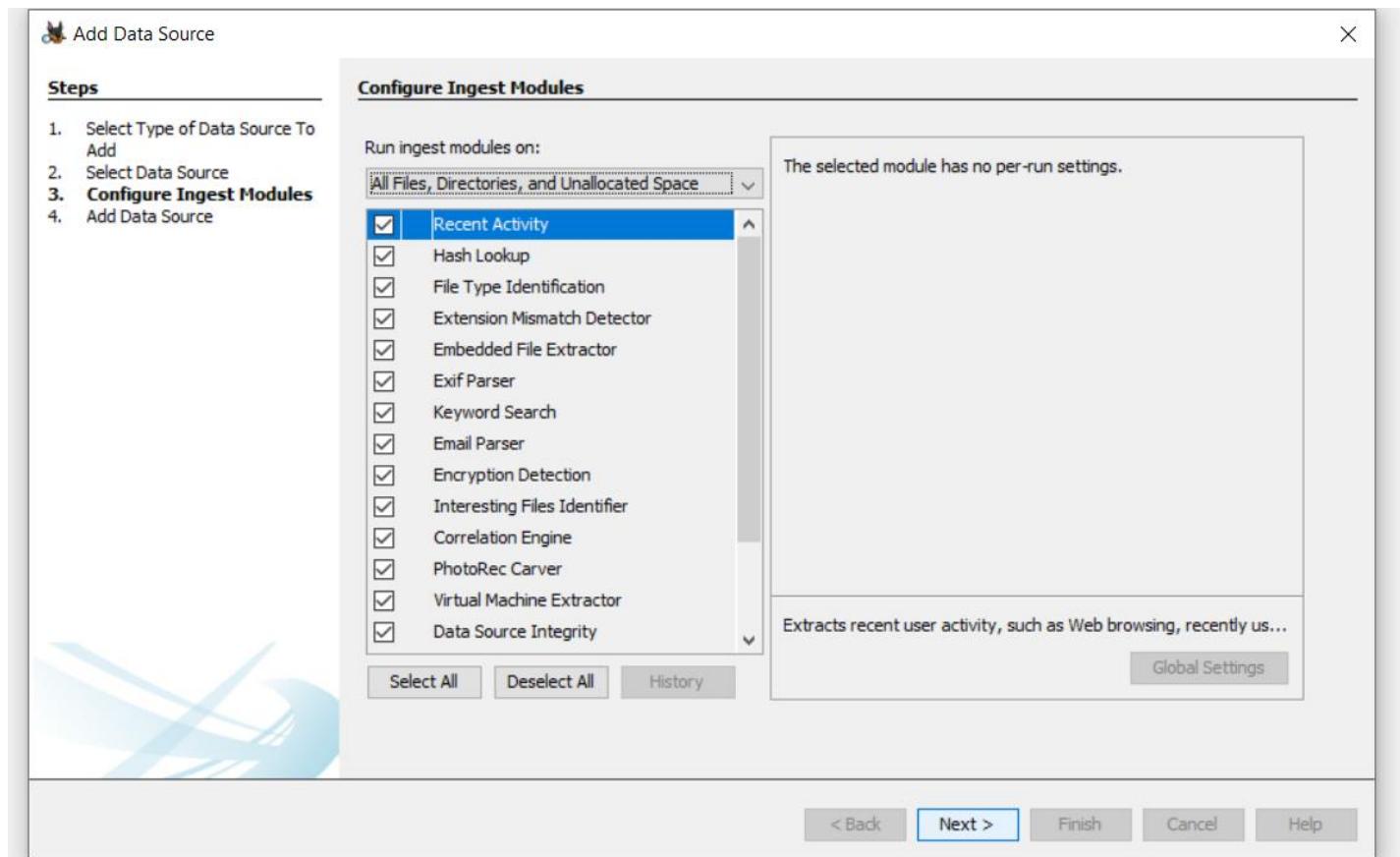


The ingest modules determine factors for which the data in the data source is to be analyzed. Here is a brief overview of each of them.

- **Recent Activity:** Discover the recent operations performed on the disk, for example, the files that were last viewed.
- **Hash Lookup:** Identify files using hash values.
- **File Type Identification:** Identify files based on their internal signatures rather than just file extensions.
- **Extension Mismatch Detector:** Identify files whose extensions are tampered with/changed possibly to hide evidence.
- **Embedded File Extractor:** It extracts embedded files such as .zip, .rar, etc. and uses the derived file for analysis. Another example could be a PNG image saved inside a doc to make it appear as a document and thus hide crucial information.
- **EXIF (Exchangeable Image File Format) Parser:** It is used to retrieve metadata about the files, for example, date of creation, geolocation, etc.
- **Keyword Search:** Search for a particular keyword/pattern in the data source.
- **Email Parser:** If the disk holds any form of email database, for example, pst/ost files of outlook then information from these files can be extracted using an email parser.
- **Encryption Detection:** Detects and identifies encrypted / password-protected files.
- **Interesting File Identifier:** Let's set custom rules regarding the filtering of data. Examiner is notified when results pertaining to these rules are found.
- **Correlation Engine:** Allows saving properties in and then retrieved from the central repository. It helps in displaying correlated properties.
- **PhotoRec Carver:** Recover files, photos, etc. from the unallocated space.
- **Virtual Machine Extractor:** Extract and analyze any Virtual machine found on the data source.

Advanced Cyber Security

- **Data Source Integrity:** Calculates the hash values and stores them in the database in case they aren't already present. Otherwise, it will verify the hash values associated with the database.
- **Plaso:** Extract timestamp for various types of files.
- **Android Analyzer:** Analyze SQLite and other files retrieved from an Android device.



Select all that will serve the purpose of your investigation and click Next. Once the data source is added, click Finish. It will take some buffer time to extract and analyze the data depending upon the size of the Data Source.

3. Exploring the data source:

The Data Source information: Here the basic metadata is shown. A detailed analysis is displayed in the bottom section. These details can be extracted in the form of Hex values, Results, File Metadata, etc.

Advanced Cyber Security

The screenshot shows the Autopsy 4.15.0 interface. The left sidebar contains a tree view of data sources, views, file types, deleted files, results (including extracted content like EXIF metadata, encryption detected, installed programs, etc.), keyword hits, email messages, interesting items, accounts, and tags. The main area is titled 'Listing' under 'Data Sources' and shows a table with one entry: 'Mantooth.E01' (Image, 128450048 bytes, 512 sector size, Asia/Calcutta timezone, Device ID 7a1c6fb8-4b18-4921-9ac2-cca49ebc88a1). Below this is a hex viewer window. The tabs at the top of the hex viewer are 'Hex', 'Text', 'Application', 'Messages', 'File Metadata' (which is highlighted with a green oval), 'Results' (also highlighted with a green oval), 'Annotations', and 'Other Occurrences'. The hex dump shows binary data starting with 0x00000000. The results tab below the hex viewer displays several lines of text, likely file metadata or search results.

The disk image is then broken down based upon its volume partitions.

This screenshot shows the volume structure of the disk image 'Mantooth.E01'. The tree view on the left lists 'Data Sources' (Mantooth.E01) which contains four volumes: 'vol1 (Unallocated: 0-62)', 'vol2 (NTFS / exFAT (0x07): 63-224909)', 'vol3 (DOS FAT12 (0x01): 224910-240974)', and 'vol4 (Unallocated: 240975-250878)'. The 'Views' section includes 'File Types' and 'Deleted Files'.

Each volume can be browsed for its contents, results for which are displayed in the section at the bottom. For example, the content shown below belongs to Data Sources -> Mantooth.E01 -> MSOCache-> [Parent Folder].

Advanced Cyber Security

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location
[current folder]				2007-07-08 02:38:29 IST	2007-07-08 02:38:29 IST	2008-07-03 02:37:00 IST	2007-07-08 02:38:29 IST	256	Allocated		unknown	/img_Mantooth.E01/vol_vo2/MSO
[parent folder]				2008-02-13 06:23:18 IST	2008-02-13 06:23:18 IST	2008-07-03 02:23:08 IST	2007-07-07 04:52:55 IST	56	Allocated	Allocated	unknown	/img_Mantooth.E01/vol_vo2/MSO
All Users				2007-07-07 06:36:21 IST	2007-07-07 06:36:21 IST	2008-07-03 02:36:59 IST	2007-07-08 02:38:29 IST	48	Allocated	Allocated	unknown	/img_Mantooth.E01/vol_vo2/MSO

Views (Determines the factor of file classification)

- File Type:** Here the files are categorized based upon their type. The classification can be done either on the basis of file .extension or MIME type. While both of these provide a hint about how to deal with a file, file extensions are commonly used by the OS to decide what program shall be used to open a file and MIME types are used by the browser to decide about how to present the data (or by the server on how to interpret the data received). Files displayed here also include the deleted files.

Name	Type	MIME Type	Size	File Name Allocation	Metadata Allocation	Modified	Accessed	Created	Changed
/img_Mantooth E01/vol_vo2/MSOCache/	File System	null	56	Allocated	Allocated	2008-02-13 06:23:18 IST	2008-07-03 02:23:08 IST	2007-07-07 04:52:55 IST	2008-02-13 06:23:18 IST

- Deleted Files:** Here information about the files that were specifically deleted can be found. These deleted files can be recovered as well: Right-click on the file to be recovered -> click on Extract File(s). -> Save the file in an appropriate destination.

Advanced Cyber Security

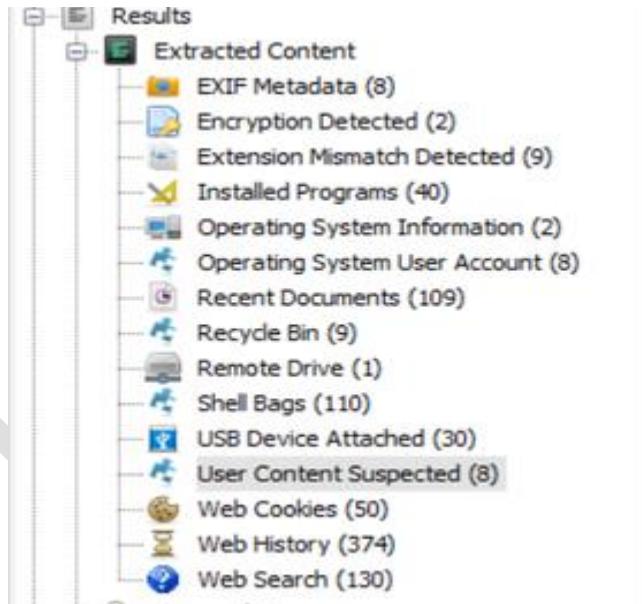
The screenshot shows the Autopsy 4.15.0 interface. On the left, the 'Data Sources' tree shows a mounted volume 'Martooth.E01' with several partitions. The 'Results' pane on the right displays a table of extracted files from 'vol_2'. A context menu is open over a file named 'conn', with the 'Extract File(s)' option highlighted. Other options include 'Properties', 'View File in Directory', 'View in New Window', 'Open in External Viewer Ctrl+E', and 'View File in Timeline...'. Below the table, there's a detailed view of the selected file 'conn'.

MB Size Files: Here files are classified based upon their size. The range starts from 50MB. This enables the examiner to determine exclusively large files.

Results:

All the extracted data is viewed in **Views/ Data Source**. In **Results**, we get the information about this data.

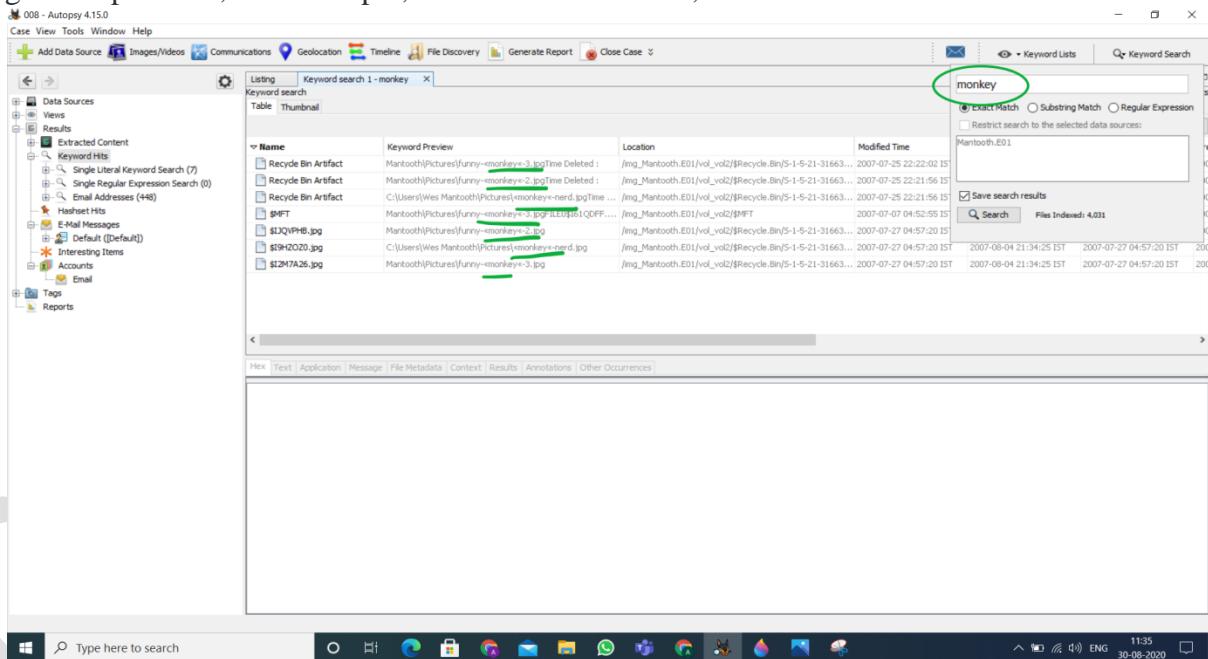
- **Extracted Content:** Each Extracted Content displayed below can be further explored. The following briefly explains each of them.



- **EXIF Metadata:** It contains all the .jpg images that have EXIF Metadata associated with them, this Metadata can be analyzed further.
- **Encryption Detection:** It detects files that are password protected/ encrypted.
- **Extension Mismatch Detection:** As explained above, it Identifies the files whose extensions do not match their MIME types and thus they may be suspicious.
- **Installed Programs:** It gives details about the software used by the user. This information is extracted with the help of the Software Registry hive.

Advanced Cyber Security

- **Operating System Information:** It gives information about the OS with the help of the Windows Registry hive and the Software Registry hive.
- **Operating System User Account:** It lists information about all the user accounts, for example, accounts belonging to the device are extracted from the Software Hive and the accounts associated with the Internet Explorer using index.data files.
- **Recent documents:** Lists all the documents that were accessed nearby the time the disk image was captured.
- **Recycle Bin:** Files that are temporarily stored on the system before being permanently deleted are visible here.
- **Remote Drive:** Shows information about all the remote drives accessed using the system.
- **Shell bags:** A shell bag is a set of registry keys that stores details about a folder being viewed, such as its position, icon, and size. All the Shell bags from the system can be viewed here.
- **USB Device attached:** All the information about the external devices attached to the system is displayed here. This data is extracted from Windows Registry which is actually a maintained database about all the activities taking place on the system.
- **Web Cookies:** Cookies saves the user information from the sites and thus provide a lot of information about the user's online activities.
- **Web History:** All the details about the browser history is shown here.
- **Web Searches:** Details about the web searches made are displayed here.
- **Keyword Hits:** Here specific keywords can be looked for in the image of the disk. Multiple data sources can be selected for the lookup. The search can be restricted to Exact match, Substring match and Regular expression, for example, emails/ IP Addresses, etc.



- **HashSet Hits:** Here the search can be made using hash values.
- **E-mail Messages:** Here all the *outlook.pst* files can be explored.

Advanced Cyber Security

The screenshot shows a digital forensics tool interface with a main menu bar (Case, View, Tools, Window, Help) and a toolbar with various icons (Add Data Source, Images/Videos, Communications, Geolocation, Timeline, File Discovery, Generate Report, Close Case). The left sidebar displays a tree view of the data source structure, including 'Data Sources' (Mantooth.E01), 'Views', 'File Types', 'Deleted Files', 'MB File Size', 'Results' (Extracted Content, Keyword Hits, Hashset Hits, E-Mail Messages, Interesting Items), 'Accounts' (Email, Tags, Reports), and 'Information Themes'. The main pane is titled 'Listing' and shows a table of extracted emails. The table has columns: Source File, S, C, O, Account Type, ID, and Data Source. The table contains several rows of Outlook.pst files from the 'Mantooth.E01' data source, detailing subjects like 'Rasco Badguy!', 'dollarhyde66@comcast.net', and 'Wes Mantooth', along with their respective message IDs, paths, and thread IDs.

Source File	S	C	O	Account Type	ID	Data Source
Outlook.pst	3			EMAIL	dollarhyde66@comcast.net	Mantooth.E01
Outlook.pst	3			EMAIL	oleteam@microsoft.com	Mantooth.E01
Outlook.pst	3			EMAIL	chkwisher@comcast.net	Mantooth.E01
Outlook.pst	3			EMAIL	tblidd@vibell.net	Mantooth.E01
Outlook.pst	3			EMAIL	molarmart20@hotmail.com	Mantooth.E01
Outlook.pst	3			EMAIL	skinnerm27@hotmail.com	Mantooth.E01
242D0208-00000003.eml	3			EMAIL	ppg_corporation_laura_lee@mail.vresp.com	Mantooth.E01
165D65F6-00000004.eml	3			EMAIL	mailer-daemon@comcast.net	Mantooth.E01
242D0208-00000003.eml	3			EMAIL	dollarhyde66@comcast.net	Mantooth.E01
165D65F6-00000004.eml	3			EMAIL	dollarhyde66@comcast.net	Mantooth.E01
20465154-00000001.eml	3			EMAIL	mail-noreply@oncile.com	Mantooth.E01

- Interesting Items:** As discussed before, these are the file results based upon the custom rules set by the examiner.
- Accounts:** Here all the details regarding the accounts present on the disk are shown. This disk has the following EMAIL accounts.

The screenshot shows a digital forensics tool interface with a main menu bar (Case, View, Tools, Window, Help) and a toolbar with various icons (Add Data Source, Images/Videos, Communications, Geolocation, Timeline, File Discovery, Generate Report, Close Case). The left sidebar displays a tree view of the data source structure, including 'Data Sources' (Mantooth.E01), 'Views', 'Results' (Extracted Content, Keyword Hits, Hashset Hits, E-Mail Messages, Interesting Items), 'Accounts' (Email, Tags, Reports), and 'Information Themes'. The main pane is titled 'Listing' and shows a table of accounts. The table has columns: Source File, S, C, O, Account Type, ID, and Data Source. The table contains several rows of Outlook.pst files from the 'Mantooth.E01' data source, detailing account types like 'EMAIL' and 'FMAIL' along with their respective IDs and data sources.

Source File	S	C	O	Account Type	ID	Data Source
Outlook.pst	3			EMAIL	dollarhyde66@comcast.net	Mantooth.E01
Outlook.pst	3			EMAIL	oleteam@microsoft.com	Mantooth.E01
Outlook.pst	3			EMAIL	chkwisher@comcast.net	Mantooth.E01
Outlook.pst	3			EMAIL	tblidd@vibell.net	Mantooth.E01
Outlook.pst	3			EMAIL	molarmart20@hotmail.com	Mantooth.E01
Outlook.pst	3			EMAIL	skinnerm27@hotmail.com	Mantooth.E01
242D0208-00000003.eml	3			EMAIL	ppg_corporation_laura_lee@mail.vresp.com	Mantooth.E01
165D65F6-00000004.eml	3			EMAIL	mailer-daemon@comcast.net	Mantooth.E01
242D0208-00000003.eml	3			EMAIL	dollarhyde66@comcast.net	Mantooth.E01
165D65F6-00000004.eml	3			EMAIL	dollarhyde66@comcast.net	Mantooth.E01
20465154-00000001.eml	3			FMAIL	mail-noreply@oncile.com	Mantooth.E01

- Reports:** Reports about the entire analysis of the data source can be generated and exported in many formats.

Advanced Cyber Security

The screenshot shows the Autopsy 4.15.0 interface with a 'Generate Report' dialog open. The left sidebar contains navigation links like 'Data Sources', 'Views', 'Results', 'Extracted Content', 'Keyword Hits', 'Hashed Hits', 'E-Mail Messages', 'Interesting Items', 'Accounts', 'Tags', and 'Reports'. The main area displays a tree view of data sources, including 'Manboot.E01' with volumes 'vol1' through 'vol4'. A 'Generate Report' button is highlighted. The 'Select and Configure Report Modules' section lists 'Report Modules' such as 'HTML Report', 'Excel Report', 'Text', 'Tagged Hashes', 'TSK Body File', 'Google Earth KMZ', 'STIX', 'CASE-UCO', and 'Portable Case'. A tooltip for 'Excel Report' explains it generates a report about results and tagged items in Excel (XLS) format. The 'File Path' column on the right lists various output paths for different report types.

Report Name
Created Time
Report Path

Generate Report
X

Configure Report

Select which data to report on:

- All Results
- All Tagged Results
- Specific Tagged Results

Advanced Cyber Security

The screenshot shows a Microsoft Excel spreadsheet titled "Excel - Microsoft Excel". The data is organized into two main columns, A and B. Column A contains a list of approximately 60 email addresses, mostly from Comcast.net and Gmail domains. Column B contains the content of the emails, which include various subjects such as "Welcome to Microsoft Office Outlook 2003", "Re: Whats up in D town?", "A trade", "Sweet Info", "Forgot photo", "Girlfriend", "Letter", "Re: Stuff", "RE: New Venture", "Welcome to Windows Mail", "HEY", "New Venture", "Gmail is different. Here's what you need to know.", "It's easy to switch to Gmail!", "Hey Mom", and "PGP Trial Software Order Confirmation: 851797 ::EW49TU6IB". The bottom of the Excel window shows a ribbon with tabs like FILE, HOME, PAGE LAYOUT, FORMULAS, DATA, REVIEW, and VIEW.

Additional Features:



- Add a Data Source:** Each case can hold multiple Data Sources.
- Images/Videos:** Images/ Videos in the data source can be viewed in Gallery View. The information here is displayed in the form of attribute-value pairs.

This screenshot shows a file management interface with a sidebar and a main content area. The sidebar on the left shows a tree view of file groups and categories, with "Documents (10)" expanded. The main area displays a grid of 12 image files, each with a preview thumbnail and a file name below it. To the right of the grid, there is a "Details" panel showing specific attributes for one of the files. A green arrow points from the "Attribute" column to the "Value" column for the "Name" attribute, which is listed as "gift_certif_sample.j". Other visible attributes include "Analyzed" (true), "Category" (CAT-0: Uncategorized), "Tags", "Path" (/img_Mantooth.E01/vol.vol2/Users/Wes Mantooth/Documents), "Created Time" (2007-03-06 07:22:34 IST), "Modified Ti...", and "MD5 Hash" (b8b19afe6d2abf6e d8b91b0b29e3d29).

- Communications:** All the communications made using the source device are displayed here. This device had communications only in the form of emails.

Advanced Cyber Security

The screenshot shows the 'Communications Visualization - Editor' window. On the left, there are filtering options for 'Account Types' (Device, Email), 'Devices' (Mantooth.E01 selected), and a 'Date Range (Asia/Calcutta)' set to 28 February, 2007. The central area is titled 'Browse' and 'Visualize' and contains a table of accounts:

Account	Device	Type	Items
dollarhyde86@comcast.net	Mantooth.E01	Email	19
chkwasher@comcast.net	Mantooth.E01	Email	13
txkidd@swebbell.net	Mantooth.E01	Email	8
smee.rox@gmail.com	Mantooth.E01	Email	8
skimmerman27@hotmail.com	Mantooth.E01	Email	2
pgp_corporation_laura_lee@mail.vresp	Mantooth.E01	Email	2
mail-noreply@google.com	Mantooth.E01	Email	2
molarman420@hotmail.com	Mantooth.E01	Email	1
mailer-daemon@comcast.net	Mantooth.E01	Email	1
trialsoftwareorder@pgp.com	Mantooth.E01	Email	1
trialwareorderconfirmation@pgp.com	Mantooth.E01	Email	1
msoe@microsoft.com	Mantooth.E01	Email	1
toothfairy@mentaldental.com	Mantooth.E01	Email	1

The right side of the window has tabs for 'Summary', 'Messages', 'Call Logs', and 'Media Attachments'. Below these are fields for 'From', 'To', 'CC', and 'Subject', and a large text area for message content.

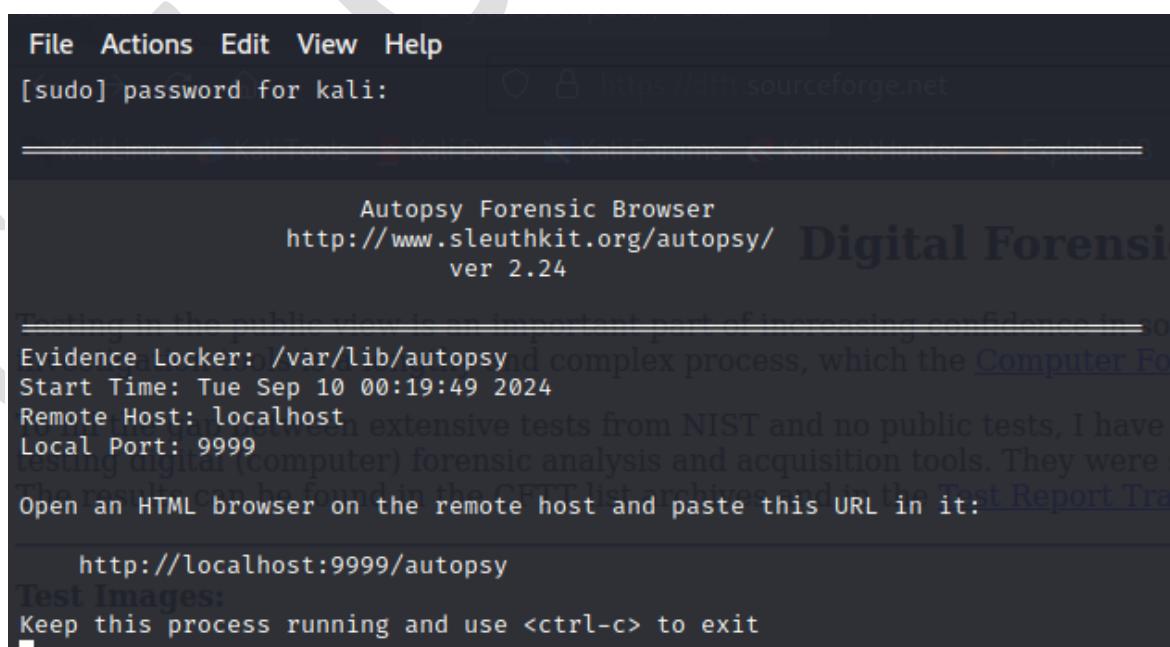
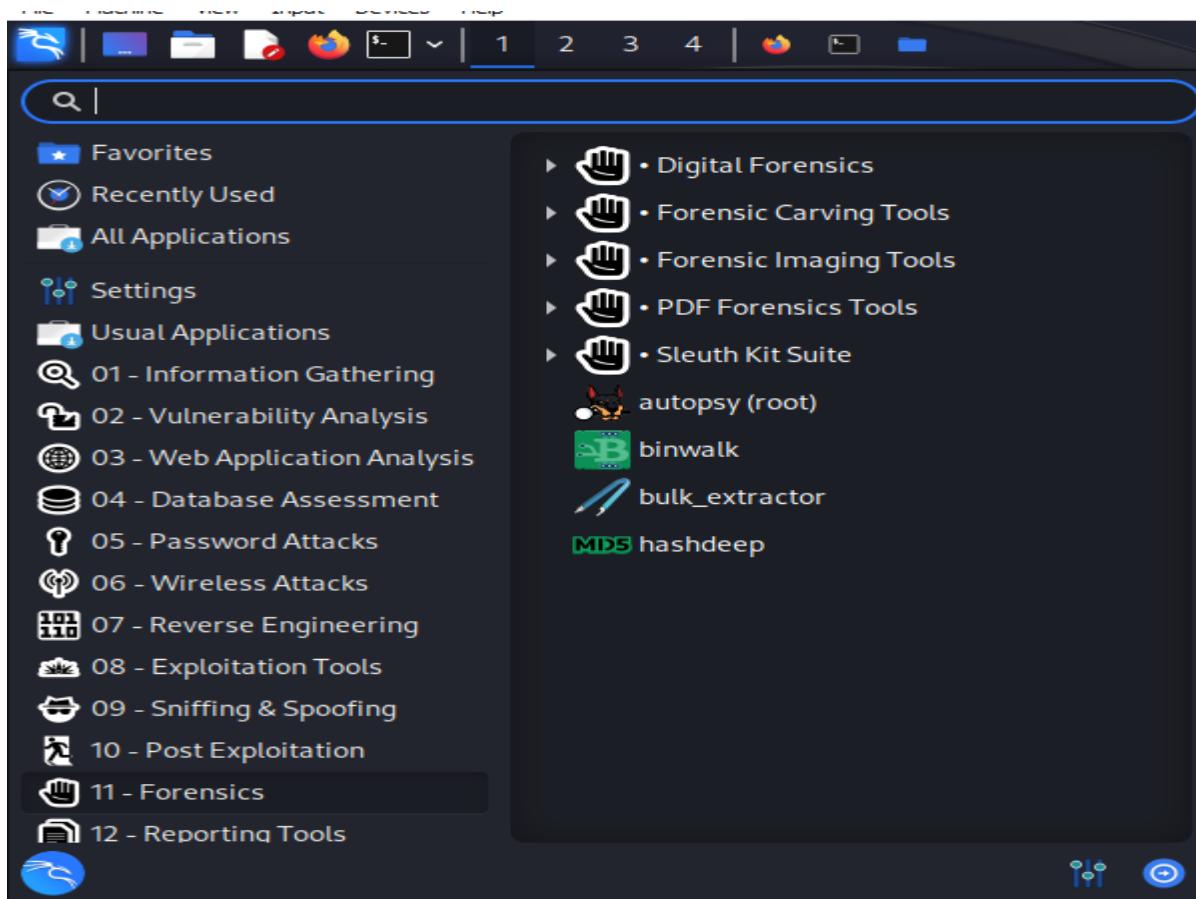
- Geolocation:** This window displays the artifacts that have longitude and latitude attributes as waypoints on a map. Here the data source has no waypoints.
- Timeline:** Information about when the computer was used or what events took place before or after a given event can be found, this greatly helps in investigating events near about a particular time.



Almost all the basic features and how actually Autopsy works have been discussed in this article.

Autopsy Using Kali

Download the images from: <https://dfft.sourceforge.net/> in that select (8) [JPEG Search Test #1](#) (Jun '04), extract in one folder and select the file with extension .dd



Copy the local host URL into the browser



Select New Case

The screenshot shows the "CREATE A NEW CASE" form. The title "CREATE A NEW CASE" is centered at the top. The form consists of several input fields and dropdown menus:

- 1. Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.
Input field: 100
- 2. Description:** An optional, one line description of this case.
Input field: Investigation of JPEG
- 3. Investigator Names:** The optional names (with no spaces) of the investigators for this case.
List of dropdown menus:
 - a. X
 - c.
 - e.
 - g.
 - i.
 - b. Y
 - d.
 - f.
 - h.
 - j.

At the bottom of the form are three orange buttons: "NEW CASE", "CANCEL", and "HELP".

Click on new case

Creating Case: 100

Case directory (/var/lib/autopsy/100/) created
Configuration file (/var/lib/autopsy/100/case.aut) created

We must now create a host for this case.

Please select your name from the list: X ▾

ADD HOST

Click on add host

Provide host name

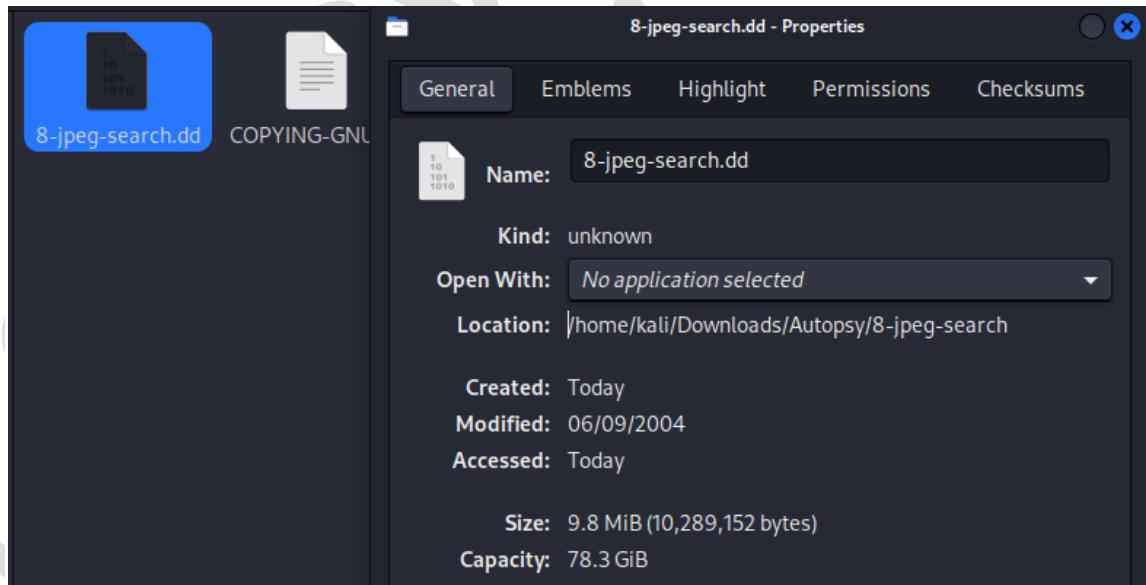
Adding host: host1 to case 100

Host Directory (/var/lib/autopsy/100/host1/) created

Configuration file (/var/lib/autopsy/100/host1/host.aut) created

We must now import an image file for this host

ADD IMAGE



ADD A NEW IMAGE

1. Location

Enter the full path (starting with '/') to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

Downloads/Autopsy/8-jpeg-search/8-jpeg-search.ddl

2. Type

Please select if this image file is for a disk or a single partition.

Disk Partition

3. Import Method

To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink Copy Move

NEXT

Warning: Autopsy could not determine the volume system type for the disk image (i.e. the type of partition table). Please select the type from the list below or reclassify the image as a volume image instead of as a disk image.

Disk Image

Volume Image

Volume System Type (disk image only):

OK

Image File Details

Local Name: images/8-jpeg-search.dd

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- Ignore the hash value for this image.
- Calculate the hash value for this image.
- Add the following MD5 hash value for this image:

Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ntfs)

Mount Point: C:

File System Type: ntfs

ADD

CANCEL

HELP

Case: 100
Host: host1

Select a volume to analyze or add a new image file.

CASE GALLERY		HOST GALLERY		HOST MANAGER
mount	name	fs type		
<input checked="" type="radio"/> C:/	8-jpeg-search.dd-0-0	ntfs	details	

ANALYZE **ADD IMAGE FILE** **CLOSE HOST**

FILE ACTIVITY TIME LINES **IMAGE INTEGRITY** **HASH DATABASES**

VIEW NOTES **HELP** **EVENT SEQUENCER**

Click on details, and click on analyze. It will provide the details and make analysis.

Autopsy:

https://www.youtube.com/watch?v=2PhJ4bCopGo&list=PLx2aAxxVN1NVk9JwAQwCNA159FrSXQ5Hn&ab_channel=SridharIyer

FTK Imager: https://www.youtube.com/watch?v=TkG4JqUcx_U&ab_channel=DFIRScience