

# DIGITAL FORENSICS

## DEFT:

*DEFT* is a household name when it comes to digital forensics and intelligence activities. The Linux distribution *DEFT* is made up of a GNU/Linux and DART (Digital Advanced Response Toolkit), a suite dedicated to digital forensics and intelligence activities.

*DEFT* is touted as a top choice among security and law enforcement agencies for computer forensic investigations.

\*When client give evidence copy we will receive and make two copies of that, one Master copy and other one will be Working copy in which he/she will start his/her investigation\*.

There are two tools use for imaging purpose in deft:

1. FTKmager (use for specific file imaging and storage device too)
2. Guymager (use for storage device imaging only)



# DIGITAL FORENSICS



# DIGITAL FORENSICS

**Acquire image of /dev/sdb**

☐ Linux dd raw image (file extension .dd or .xxx)  
☒ Expert Witness Format, sub-format Guymager (file extension .Exx)  
☐ Advanced forensic image (file extension .aff)

☒ Split image files  
Split size  GiB

Case number   
Evidence number   
Examiner   
Description   
Notes

**Destination**

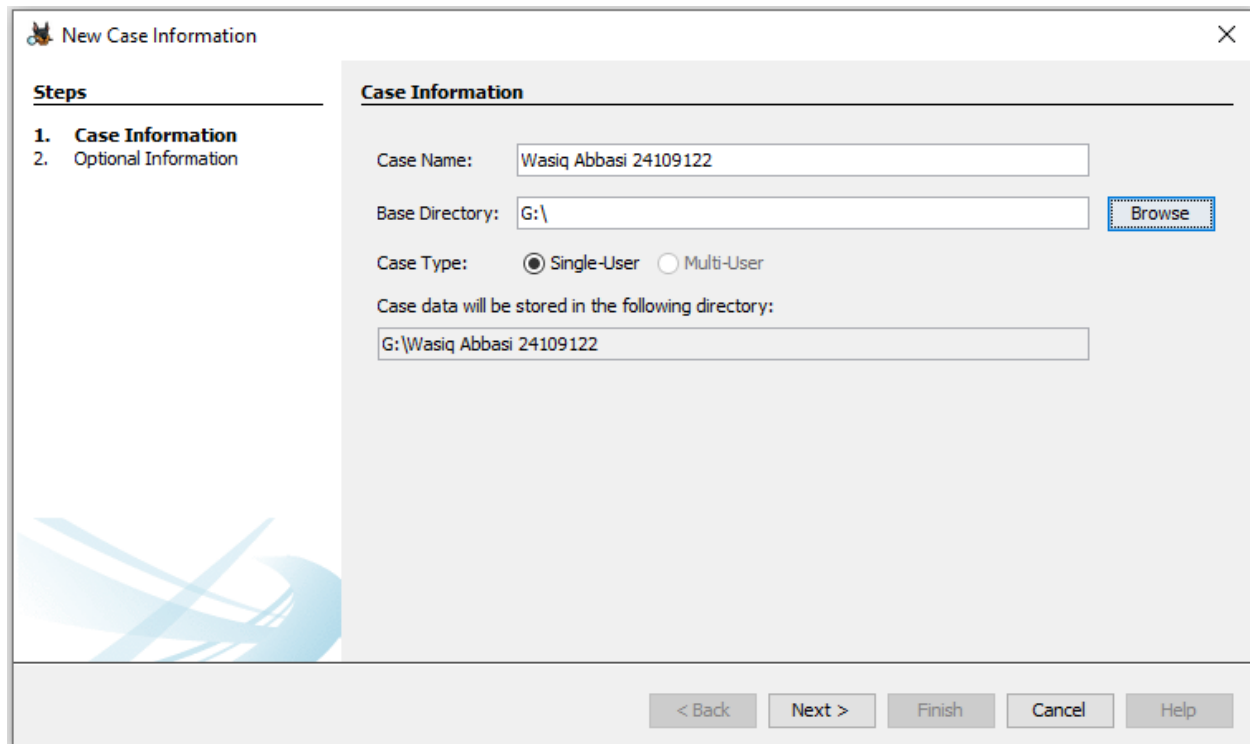
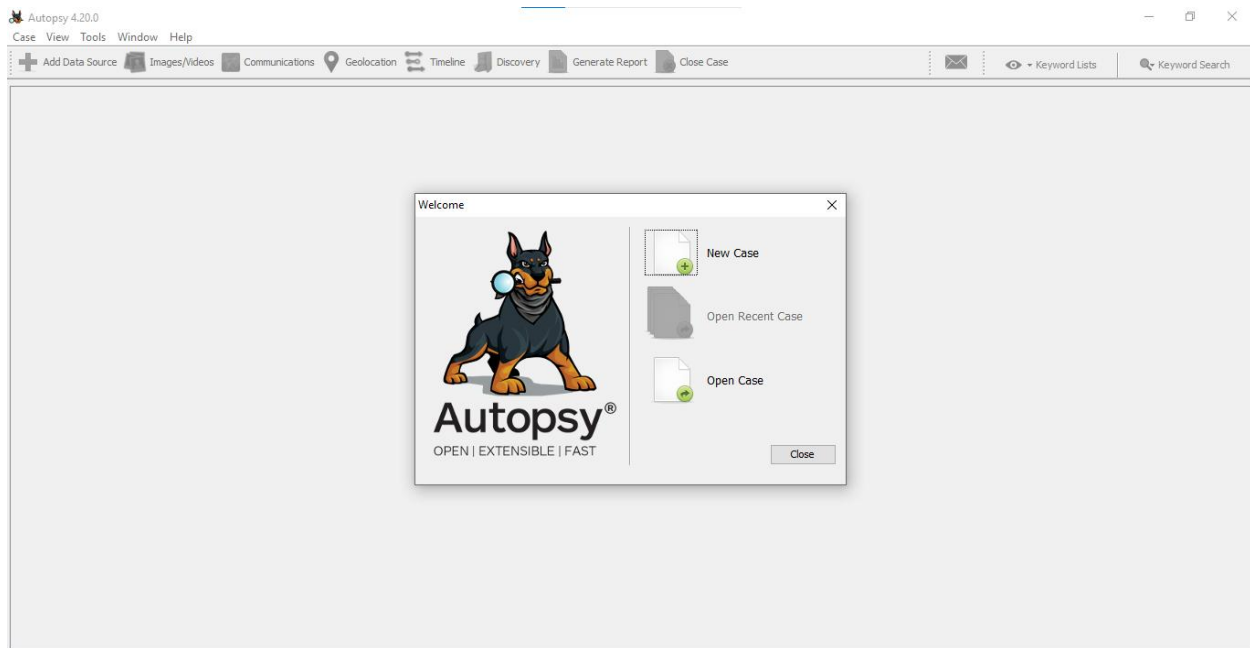
Image directory    
Image filename (without extension)   
Info filename (without extension)

**Hash calculation / verification**

☒ Calculate MD5 ☐ Calculate SHA-1 ☐ Calculate SHA-256  
☐ Re-read source after acquisition for verification (takes twice as long)  
☒ Verify image after acquisition (takes twice as long)

Size 7,823,458,304 bytes (7.29GiB / 7.82GB)  
Sector size 512  
Image file /root/Desktop/WasiqAbbasImaging.Exx  
Info file /root/Desktop/WasiqAbbasImaging.info  
Current speed 4.26 MB/s  
Started 2. May 08:55:28 (00:00:09)  
Hash calculation MD5  
Source verification off  
Image verification on

# DIGITAL FORENSICS



The image shows the "New Case Information" dialog box. The title bar reads "New Case Information" and has a close button. The dialog box is divided into two main sections: "Steps" and "Case Information".

**Steps**

1. Case Information
2. Optional Information

**Case Information**

Case Name:

Base Directory:

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

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

# DIGITAL FORENSICS

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:

< Back

Next >

Finish

Cancel

Help

Add Data Source



## Steps

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

## Configure Ingest

Run ingest modules on:

- ☒ 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

Select All

Deselect All

History

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

< Back


Next >

Finish

Cancel

Help

# DIGITAL FORENSICS

 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

Processing data source and adding it to a local database. File analysis will start when this finishes.

Status

\*This process may take some time for large data sources.


< Back

Next >

Finish

Cancel

Help

 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

Data source has been added to the local database. Files are being analyzed.

< Back

Next >

Finish

Cancel

Help

# DIGITAL FORENSICS

Listing  
Wasiq.E01\_1.Host

Table Thumbnail Summary

Save Table as CSV

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
Wasiq.E01	Image	4871301120	512	Asia/Karachi	656cba27-e3f7-48d6-b3ec-8500b6d665cf

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

05/02/25 15:20:00 PKT Read Error: revolution[1].htm  
Error encountered while calculating the hash value for /Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/JIRVY9X/revolution[1].htm (Allocated File).

Analyzing files from Wasiq.E01 3% (3 more...) 17

Listing  
/img\_Wasiq.E01/vol\_vol2/My Documents

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2004-08-20 20:21:05 PKT	2004-08-20 20:21:05 PKT	2004-08-20 20:21:09 PKT	2004-08-18 21:55:24 PKT	56	Allocated
[parent folder]				2004-08-26 20:46:18 PKT	2004-08-27 20:08:18 PKT	2004-08-27 20:08:05 PKT	2004-08-19 21:57:43 PKT	168	Allocated
ARCHIVE				2004-08-20 20:18:09 PKT	2004-08-20 20:18:09 PKT	2004-08-20 20:18:09 PKT	2004-08-20 20:18:07 PKT	440	Allocated
COMMANDS				2004-08-20 20:18:16 PKT	2004-08-20 20:18:16 PKT	2004-08-20 20:18:16 PKT	2004-08-20 20:18:12 PKT	176	Allocated
DICTIONARIES				2004-08-20 20:18:41 PKT	2004-08-20 20:18:41 PKT	2004-08-20 20:18:41 PKT	2004-08-20 20:18:16 PKT	56	Allocated
ENUMERATION				2004-08-20 20:18:41 PKT	2004-08-20 20:18:41 PKT	2004-08-20 20:18:41 PKT	2004-08-20 20:18:41 PKT	232	Allocated
EXPLOITATION				2004-08-20 20:19:12 PKT	2004-08-20 20:19:12 PKT	2004-08-20 20:19:12 PKT	2004-08-20 20:19:09 PKT	232	Allocated
FOOTPRINTING				2004-08-20 20:19:49 PKT	2004-08-20 20:19:49 PKT	2004-08-20 20:19:49 PKT	2004-08-20 20:19:49 PKT	232	Allocated

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

05/02/25 15:21:00 PKT Read Error: wmlibrary\_v\_0\_12.db  
Error encountered while calculating the hash value for /Documents and Settings/All Users/Application Data/Microsoft/Media Index/wmlibrary\_v\_0\_12.db (Allocated File).

Analyzing files from Wasiq.E01 9% (3 more...) 61