

DISK IMAGE ANALYSIS

USING AUTOPSY



MoTech IT Articles
NOEL MOSES MWADENDE

INTRODUCTION.

This is our last part of device forensic, after doing USB write protection, creating disk image, now it is time to retrieve all contents of USB drive and make analysis of it.

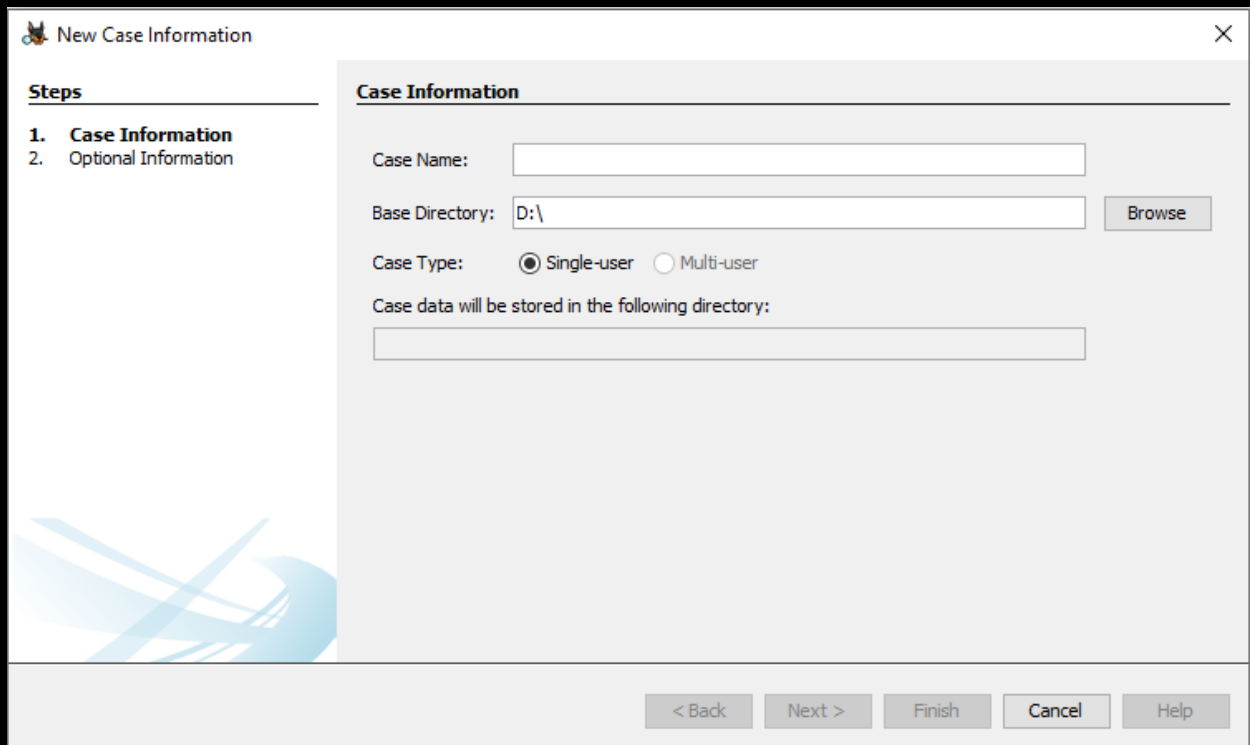
Below are the steps

After opening autopsy, it should look as shown in the figure 1.



Fig. 1.

In the new case click addition sign to create new case as shown in the figure 1.



The image shows a 'New Case Information' dialog box. On the left, a 'Steps' pane lists '1. Case Information' and '2. Optional Information'. The main area is titled 'Case Information' and contains the following fields: 'Case Name' (empty), 'Base Directory' (set to 'D:\' with a 'Browse' button), 'Case Type' (with 'Single-user' selected and 'Multi-user' unselected), and 'Case data will be stored in the following directory:' (empty). At the bottom, there are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Steps

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

Case Information

Case Name:

Base Directory:

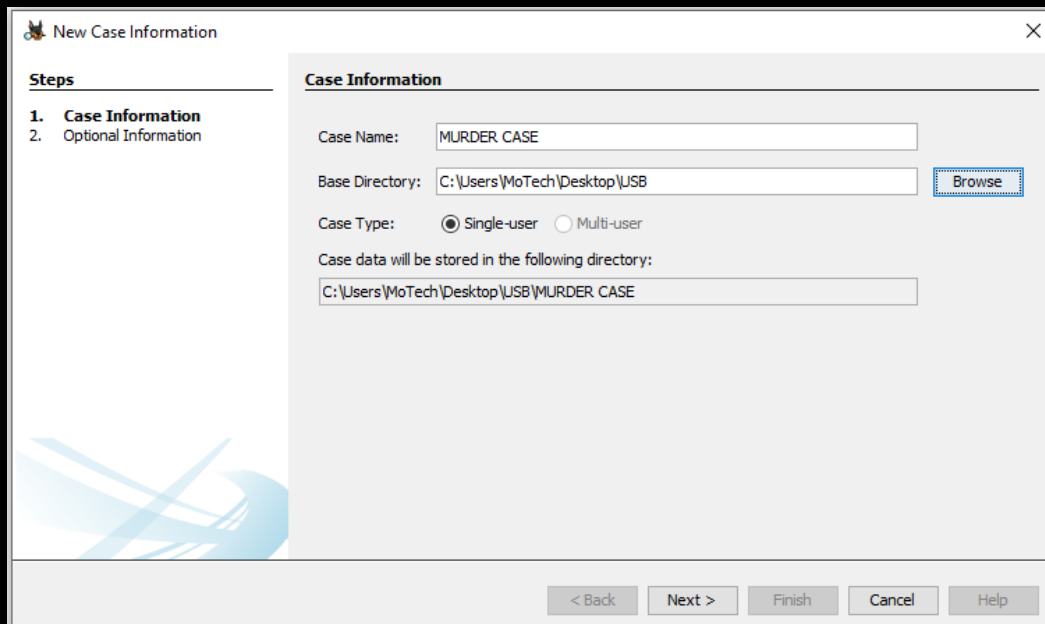
Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

Fig. 2.

After clicking new case in the figure one, new window will open as shown in the figure 2. In the case name field, fill it with the name of the case, make sure single user is marked.



This image shows the same 'New Case Information' dialog box as Figure 2, but with the fields filled out. 'Case Name' is 'MURDER CASE', 'Base Directory' is 'C:\Users\MoTech\Desktop\USB' (with a 'Browse' button), 'Case Type' is 'Single-user', and the storage directory is 'C:\Users\MoTech\Desktop\USB\MURDER CASE'. The 'Next >' button is now highlighted.

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:

< Back Next > Finish Cancel Help

Fig. 3.

In the figure 3, Base Directory is the directory for the case to be written and the name of our case is MURDER CESE, so inside folder called USB in the desktop case name will be written, fill all information as shown in the figure 2 above and then click next.

New Case Information

Steps

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

Optional Information

Case

Number: 01

Examiner

Name: moses

Phone: 12345

Email: moses@gmail.com

Notes: This is murdercase

Organization

Organization analysis is being done for: [Dropdown] Manage Organizations

< Back Next > **Finish** Cancel Help

Fig. 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

Path: C:\Users\MoTech\Desktop\USB\usbIMAGE.E01 Browse

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-8:00) America/Los_Angeles

Sector size: Auto Detect

Hash Values (optional):

MD5: [Field]

SHA-1: [Field]

SHA-256: [Field]

NOTE: These values will not be validated when the data source is added.

< Back Next > Finish Cancel Help

Fig. 5.

In the figure 5 we can see the data source file which is the image created by using FTK.

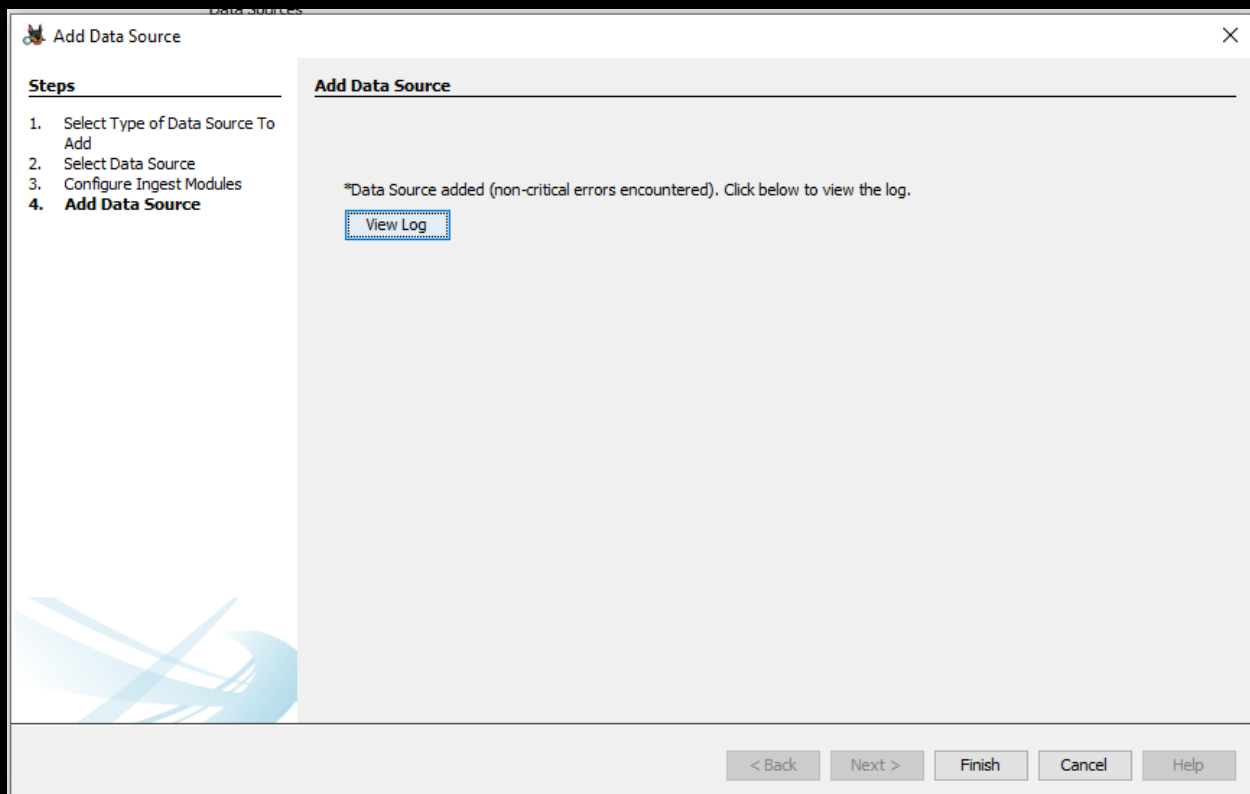


Fig. 6.


Listing				
Data Sources				
Table Thumbnail				
Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone
 usbIMAGE.E01	Image	2382266368	512	America/Los_Angeles

Fig. 7.

Figure number 7 shows the detected USB which contain retrieved files.

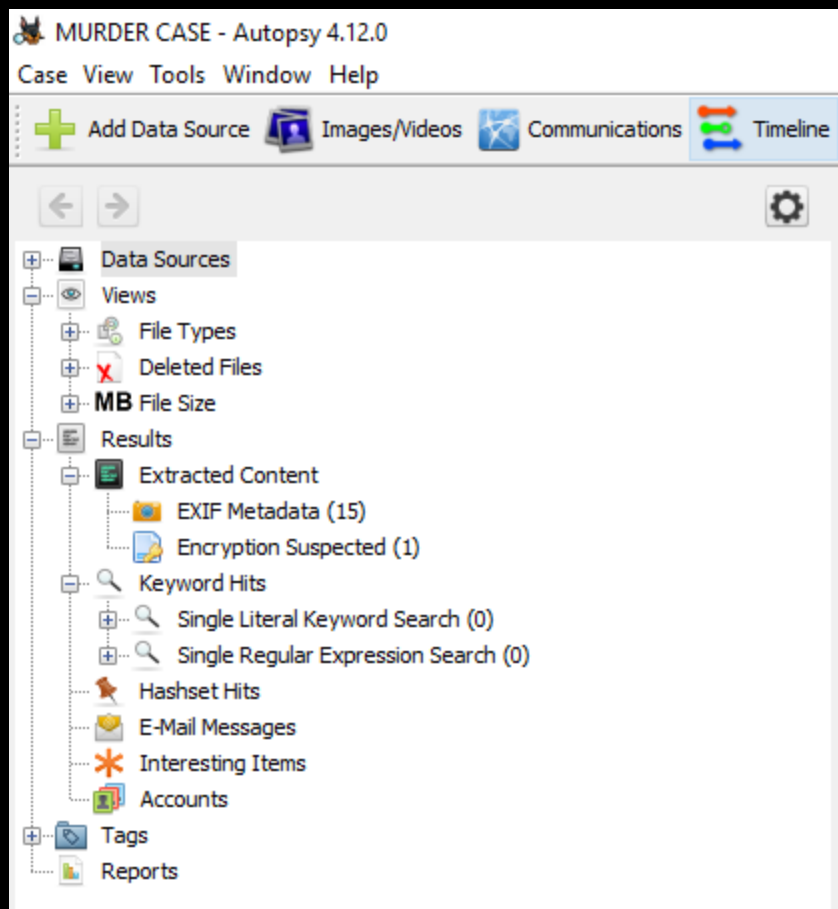


Fig. 8.

Figure number 8 shows the tree structure of contents retrieved.














Source File	S	C	Date Created	Device Model	Device Make	Data Source
 f0592696.jpg			2012-07-31 11:23:51 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0583624.jpg			2012-07-31 10:08:38 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0572672.jpg			2012-07-31 09:55:42 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0563720.jpg			2012-07-31 09:53:04 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0553216.jpg			2012-07-31 09:46:19 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0544296.jpg			2012-07-31 09:43:51 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0536064.jpg			2012-07-31 09:43:34 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0525048.jpg			2012-07-31 09:41:18 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0515504.jpg			2012-07-31 09:39:11 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0504448.jpg			2012-07-30 19:21:54 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0493152.jpg			2012-07-30 19:20:50 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0481328.jpg			2012-07-30 19:20:25 PDT	Canon EOS 450D	Canon	usbIMAGE.E01
 f0471136.jpg			2012-07-30 19:08:10 PDT	Canon EOS 450D	Canon	usbIMAGE.E01

Fig. 9.

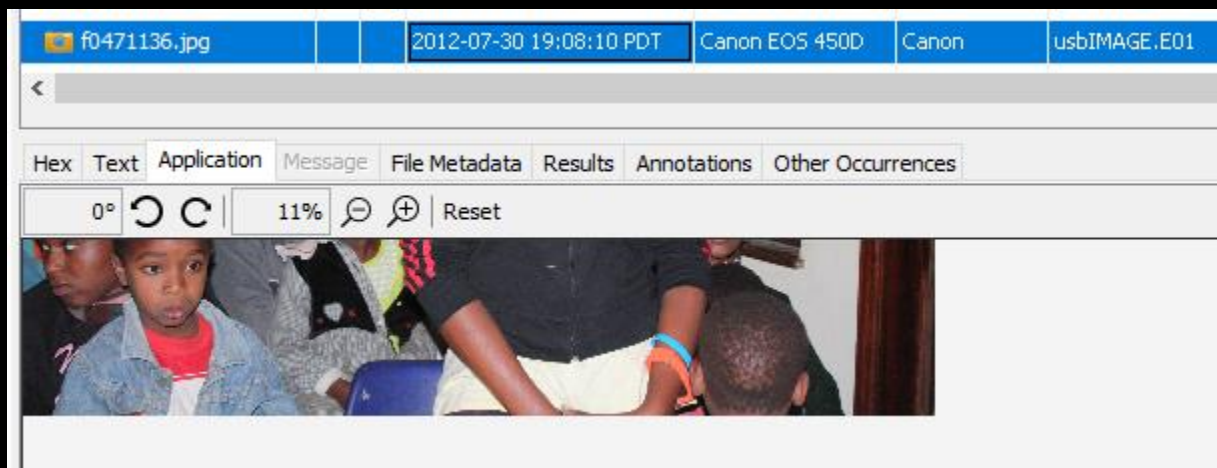


Fig. 10.

Figure number 9 and number 10 shows deleted files which is recovered.

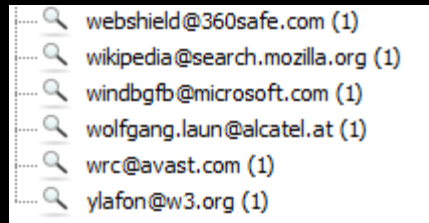


Fig. 11.

Figure number 11 shows retrieved emails, these tools are working fine, if victim deleted files all files are retrieved, if user refuse that he or did not used any email in computer, all emails are retrieve.

CONCLUSION.

If all evidences are found, in the USB of user then according to laws user should be held responsible, thank you that is the end of Device Forensic, thank you for being with me from the start till the end.

WAYS TO GET IN TOUCH WITH MoTech.

Linkedin.com

<https://www.linkedin.com/in/motech-inc-720261191/>

YouTube.com

<https://www.youtube.com/channel/UCtuaigKZF3okQnKON5RM1qQ>

Amazon.com

https://www.amazon.com/s?k=noel+moses+mwadende&ref=nb_sb_noss

Github.com

<https://github.com/MoTechStore/>

Scribd.com

<https://www.scribd.com/user/470459684/MoTech>

SlideShare.com

https://www.slideshare.net/MoTechInc?utm_campaign=profiletracking&utm_medium=sssiteref&utm_source=ssslideview