SABTHAGIRI A **231901044**

EXP NO: 2

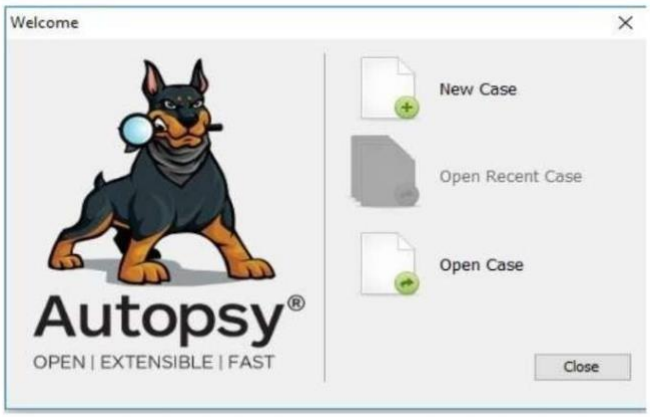
Live Forensics Case Investigation using Autopsy

Aim :

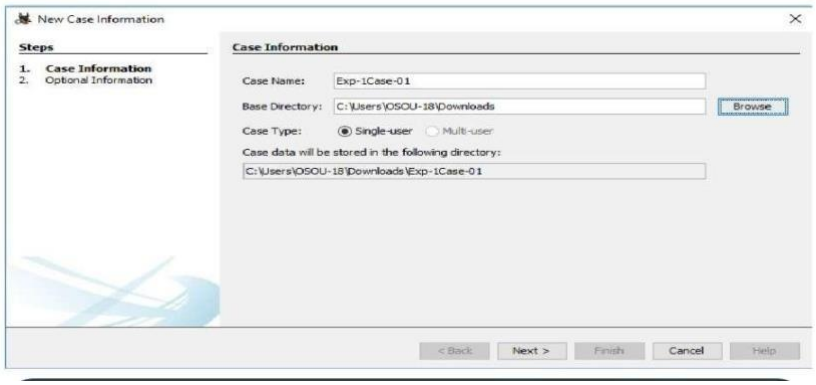
Live Forensics Case Investigation using Autopsy

Procedure :

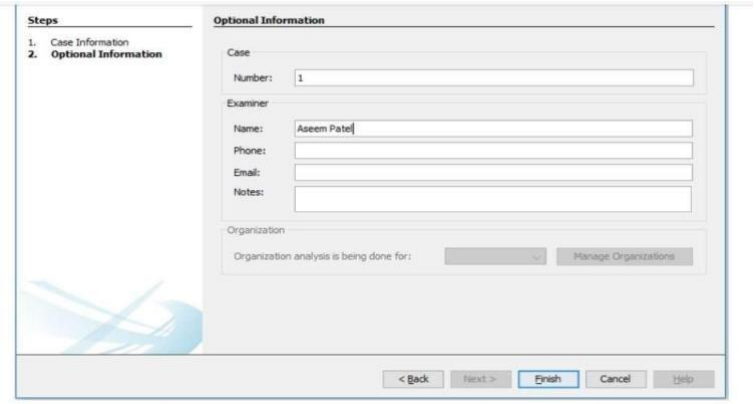
1. First Download autopsy from here and install in your pc. Click ‘New Case’ option.

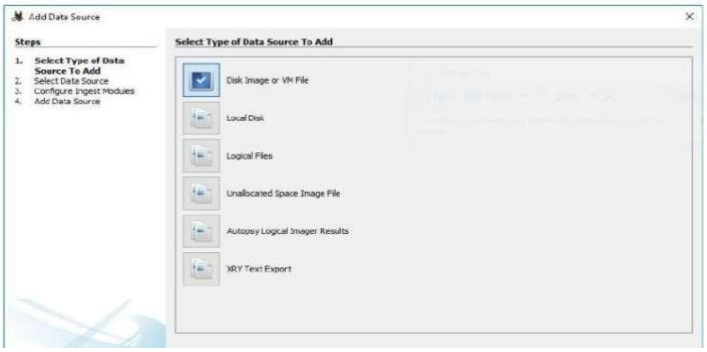


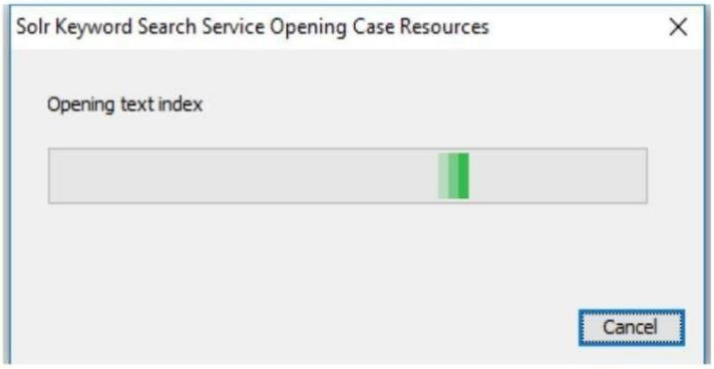
2. A new page will open. Enter the details in ‘Case Name’ and ‘Base Directory’ and choose the location to save the report e.g. :Autoreport.
3. Then click on next to proceed to the next step.



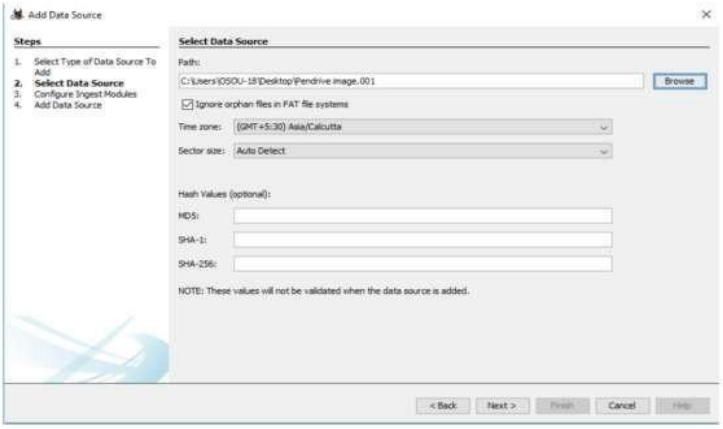
Here in the next step, you have to enter the case number and Examiner details and click on finish to proceed to the next step.



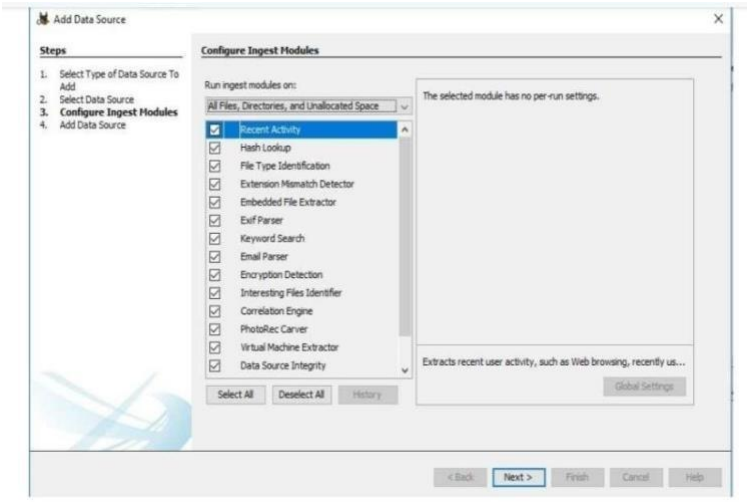




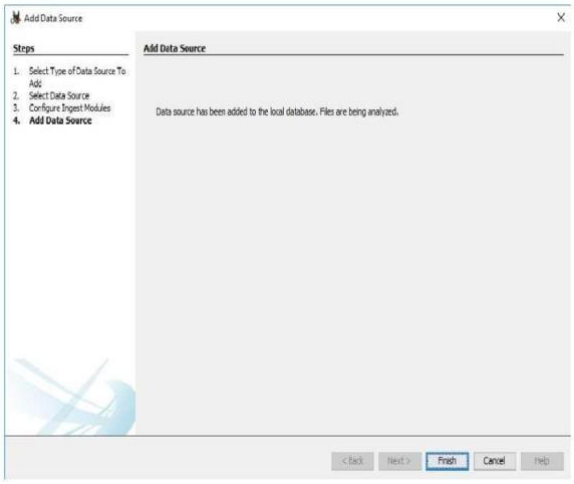
A new window will open. It will ask for the add data source in Step 1. Select source type to add & browse the file Path and click on NEXT option to proceed further.



Configure ingest Modules I have chosen all the modules as I am looking for complete information on evidence device or disk or system etc. and click next to proceed further.



In Add Data Source just click on Finish to generate the report of the device and you can perform complete investigate on the victim device or system or any other disk. It will process the data Source and add it to the local database.



- In Add Data Source just click on Finish to generate the report of the device and you can perform complete investigate on the victim device or system or any other disk.
- It will process the data Source and add it to the local database.
- After Process completion, it will show the Forensic Investigation Report.
- Now click on Devices Attached option, it will show the list of the attached device with the system.
- Now click on EXIF Metadata (Exchangeable image file format for images, sound used by Digital Camera, Smartphone and scanner), click on Installed Programs to

see the entire installed programs in the system, Click Operating System Information.

- It will show the entire operating system list, Now Select Operating System User Account Option.
- It will Display the name of all the user Accounts,
- Now click on Recent Documents Option, it will display the latest created or opened documents,
- Click Web Bookmarks Option to see all the bookmarks by system users in different
- browsers, To see web cookies, select web cookies option, To See Web Downloads,
- Click on Web Downloads option, To check internet History, click on Web History Option, To see the history of internet search, click on Web Search Option, To see the list of all email ids in the system, click on email address.

Result:

Thus, the forensic tools executed successfully, and the evidence was captured and analyzed accurately.