

Practical No. 03

AIM - Forensics Case Study → Solve the Case Study (image file) provided in the lab using Encase Investigator or Autopsy.

1. Autopsy is a web based front end to the FSK. Start it and create a new case.
Open Autopsy → File → New Case → Enter the case details. Such as Investigator Name & Contact.



2. You need a sample file. Browse in directory. And also the location where study has to be created. Fill the required information → Finish.

The screenshot shows the 'New Case Information' dialog box with the 'Case Information' tab selected. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The 'Case Information' section contains the following fields:

- Case Name:** case study
- Base Directory:** C:\Users\MANGESH\Desktop\abc\ (with a 'Browse' button)
- Case Type:** ☒ Single-user ☐ Multi-user
- Case data will be stored in the following directory:** C:\Users\MANGESH\Desktop\abc\case study

At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

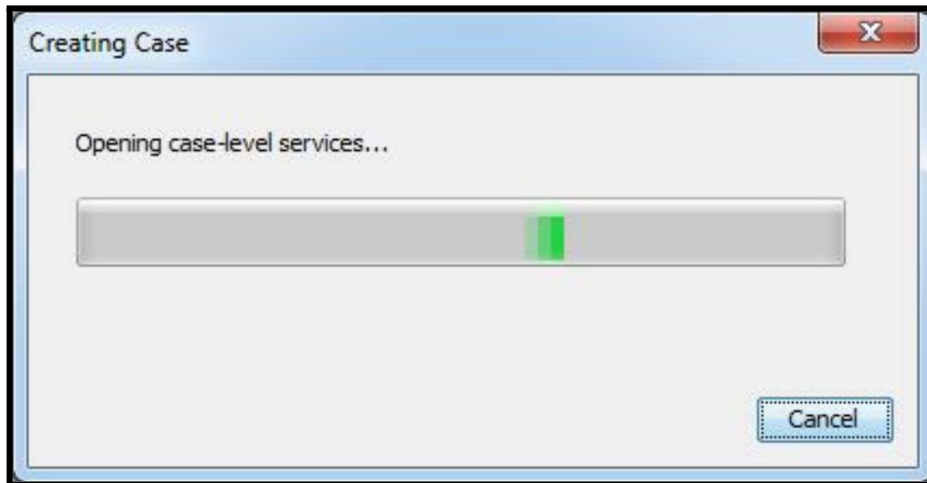
Fill the CASE Details.

The screenshot shows the 'New Case Information' dialog box with the 'Optional Information' tab selected. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The 'Optional Information' section contains the following fields:

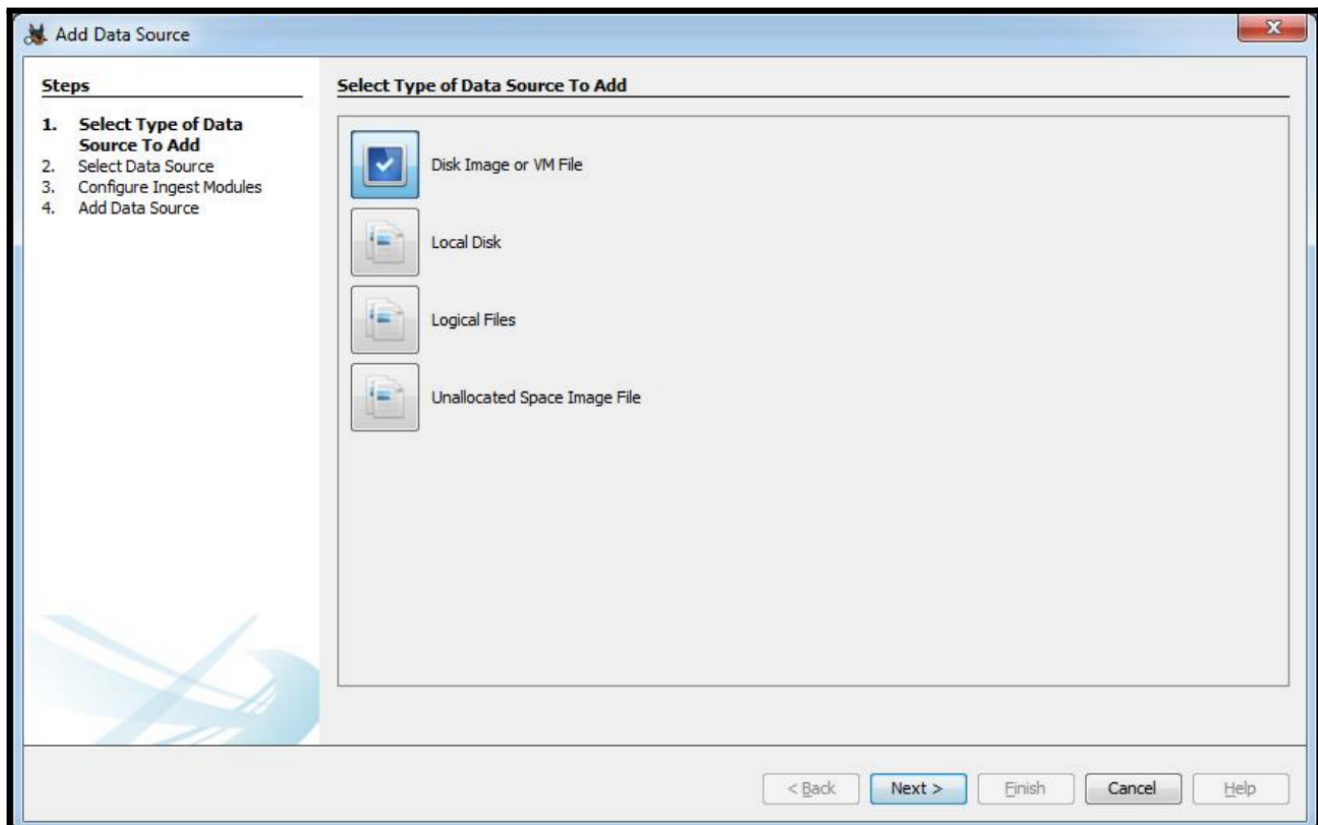
- Case Number:** 1
- Examiner:**
 - Name:** Pratibha
 - Phone:** 9920436534
 - Email:** jadhavprati2013@gmail.com
 - Notes:** Analysis of case
- Organization:**
 - Organization analysis is being done for: (dropdown menu)
 - Manage Organizations (button)

At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

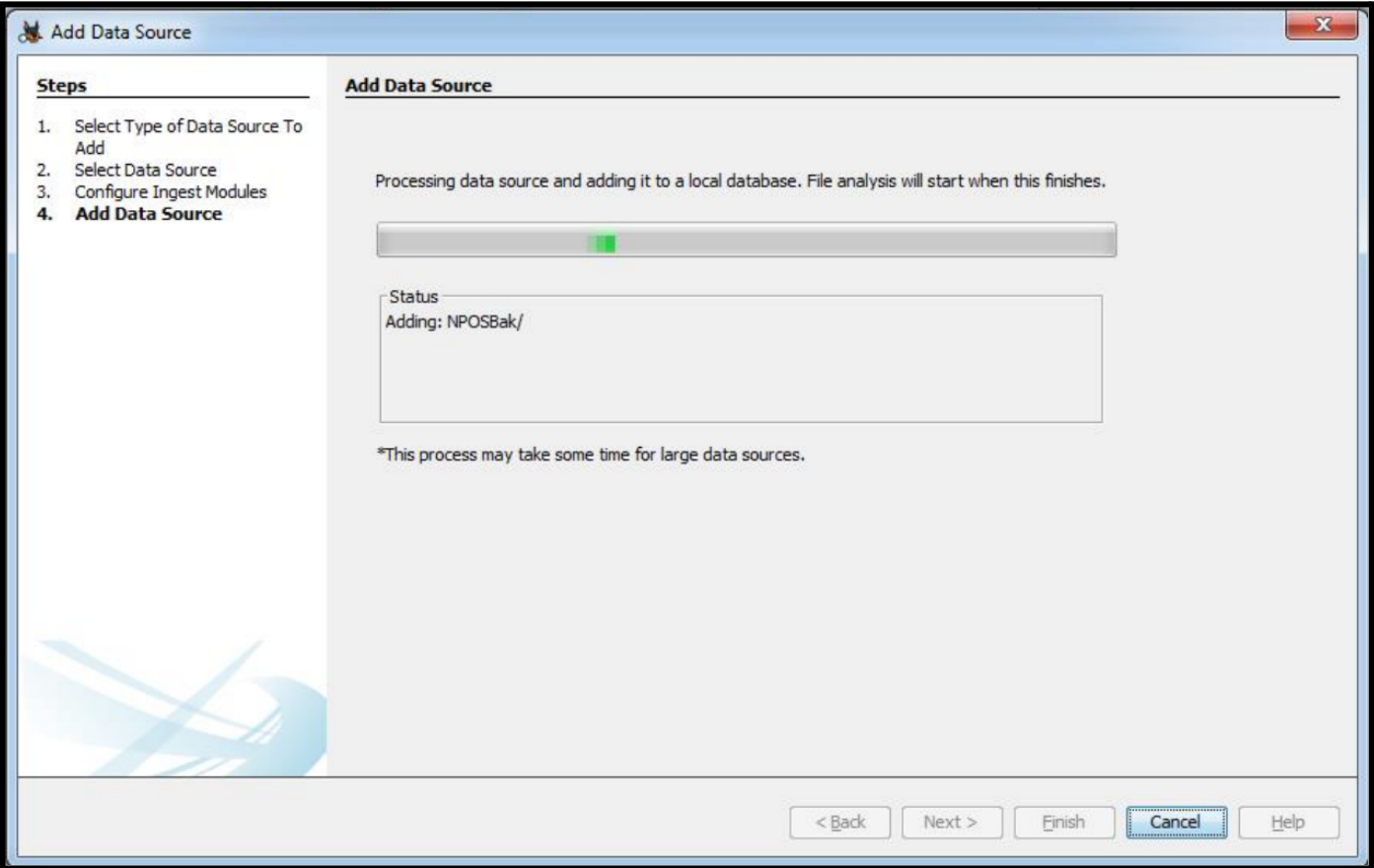
Creating a DATASOURCE →



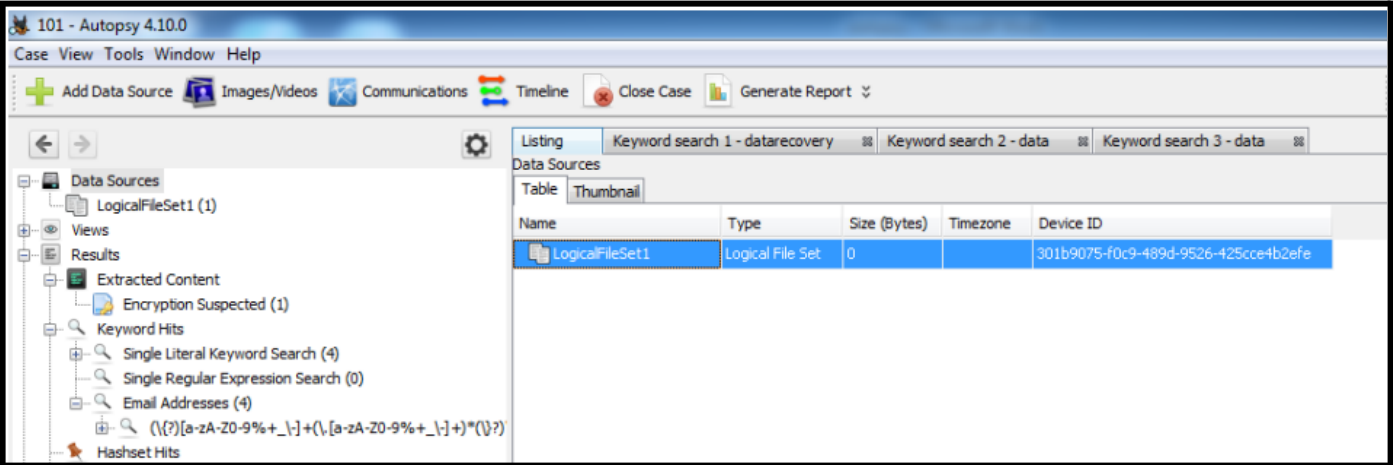
3. Select file or image →



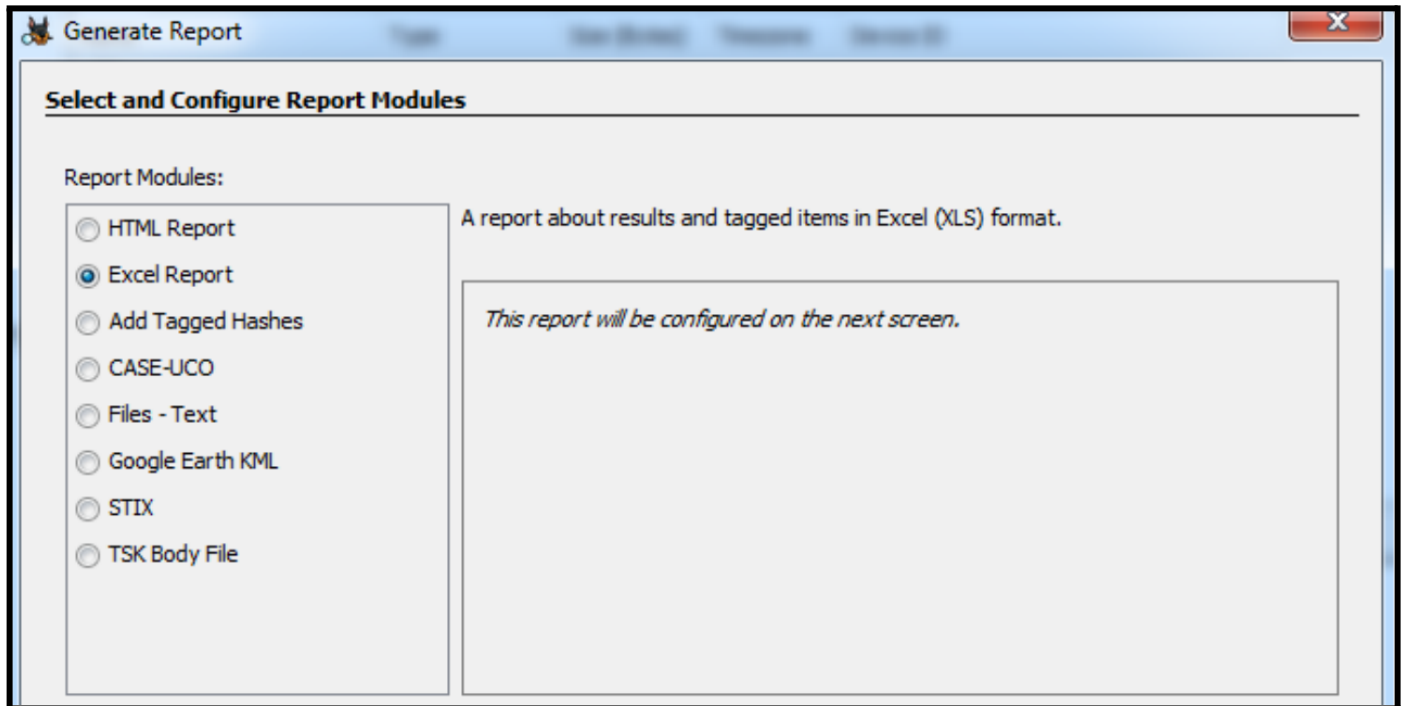
This allows us to import an image or logical file. Then it will process the Data Source.



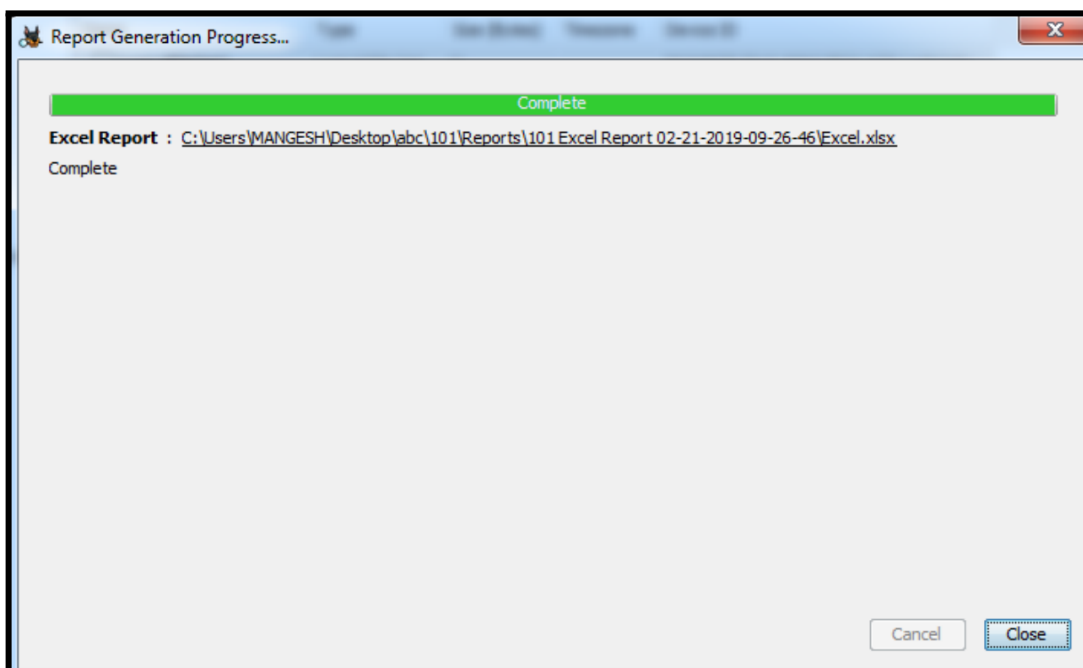
Then, it will create a Logical File →



4. For generating reports → Click on Generate Report.



It will generate report at given location →



The File will Look
as Follows →

User Searches									
A	B	C	D	E	F	G	H	I	J
1	User Searches								
2	data								
3	Preview	Source File	Tags						
4	"z2Jnu^%hiiUBIx!A	/LogicalFileSet1/st.002							
5	u^%hiiubix!a#@z"	/LogicalFileSet1/st.002							
6									
7	datap								
8	Preview	Source File	Tags						
9	v c"zu(-s\ f.z(f@«d«	/LogicalFileSet1/st.002							
10									
11	sdata								
12	Preview	Source File	Tags						
13	i>,"4'p%)@wnd: -(/LogicalFileSet1/st.002							
14									
15									
16	Email Addresses								
17	axh@c.ua								
18	Preview	Source File	Tags						
19	z%o\w~8g?xtpimc'	/LogicalFileSet1/st.002							
20									
21	b5mgj@qd.bv								
22	Preview	Source File	Tags						
23	{g\$cebx vxx^;hl?«	/LogicalFileSet1/st.002							

5. For image, Go to Image /gallery in menu → cache → thumbnails → pictures

All GroupsOnly Hash Hits

LogicalFileSet1

SampleFile

sec

Temp (2)

ModuleOutput

Embedded File Extractor

sample-files-master.zip_1109

0 (183)

sample-files-master.zip_3

sample-files-master.zip_1117

Export

Cache

thumbnails (6)


Reports

sample-files-master.zip


Category# Files

/LogicalFileSet1/SampleFile/sec/Cache/thumbnails/ -- 0 hash set hits / 6 files


Tag Selected Files:Follow UpCategorize Selected File:CAT-5: Non-pertinent




1425.png




1428.png




1430.png



1432.png

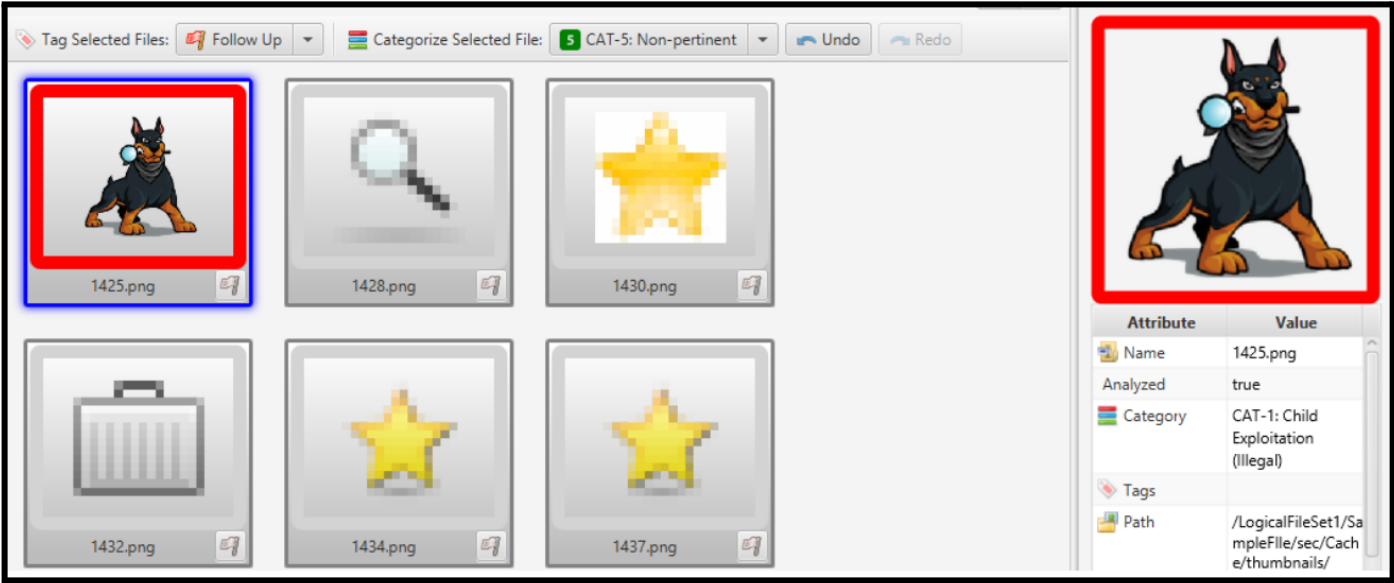


1434.png

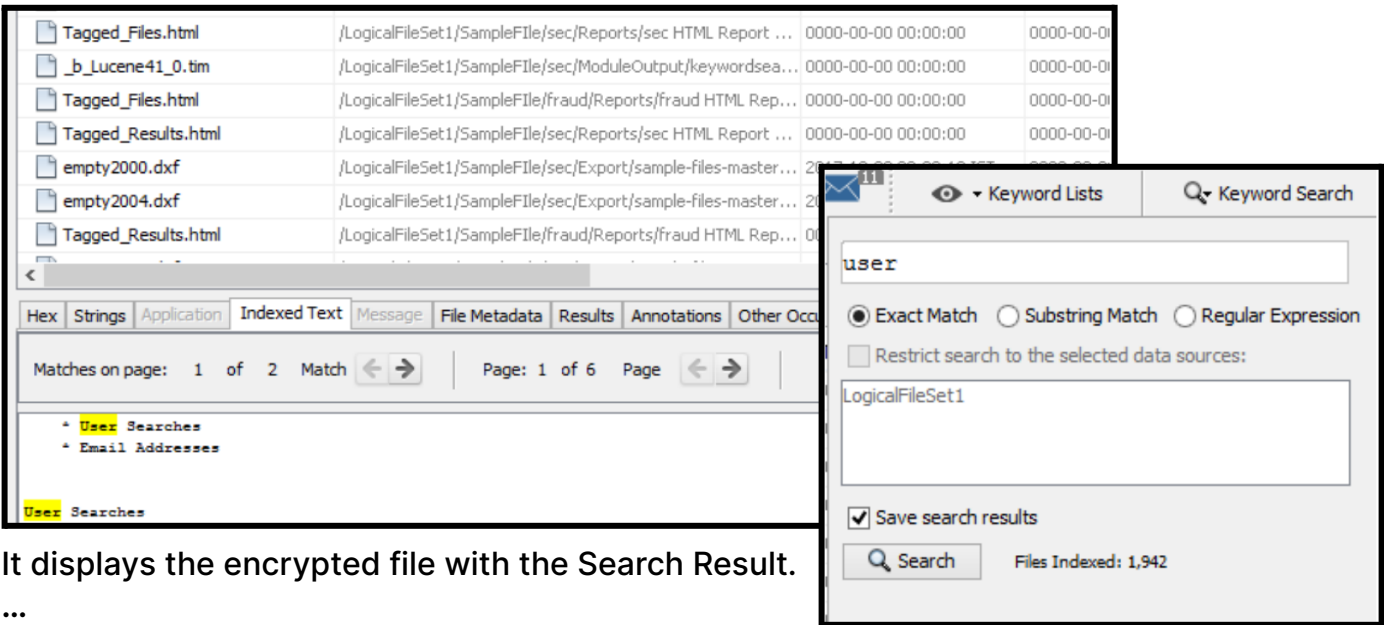


1437.png6

Right Click on image → categorized →



6. For Keyword Search, Select Keyword search at upper right corner → Type word to Search →



It displays the encrypted file with the Search Result.

...