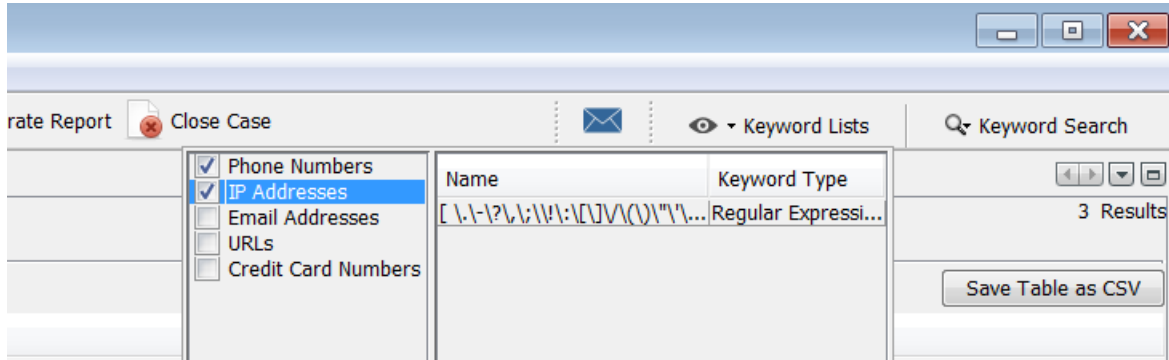


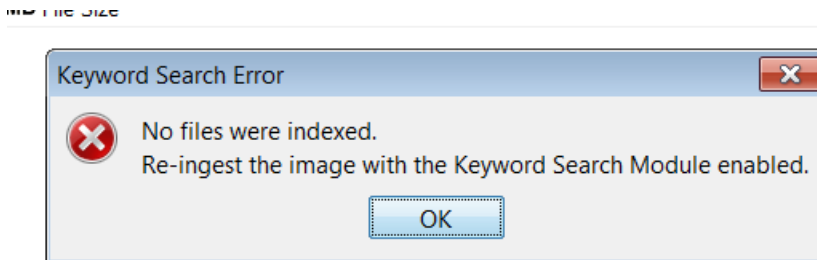
Kịch bản 1

Ổ đĩa lựa chọn là ổ D trong máy ảo Win7

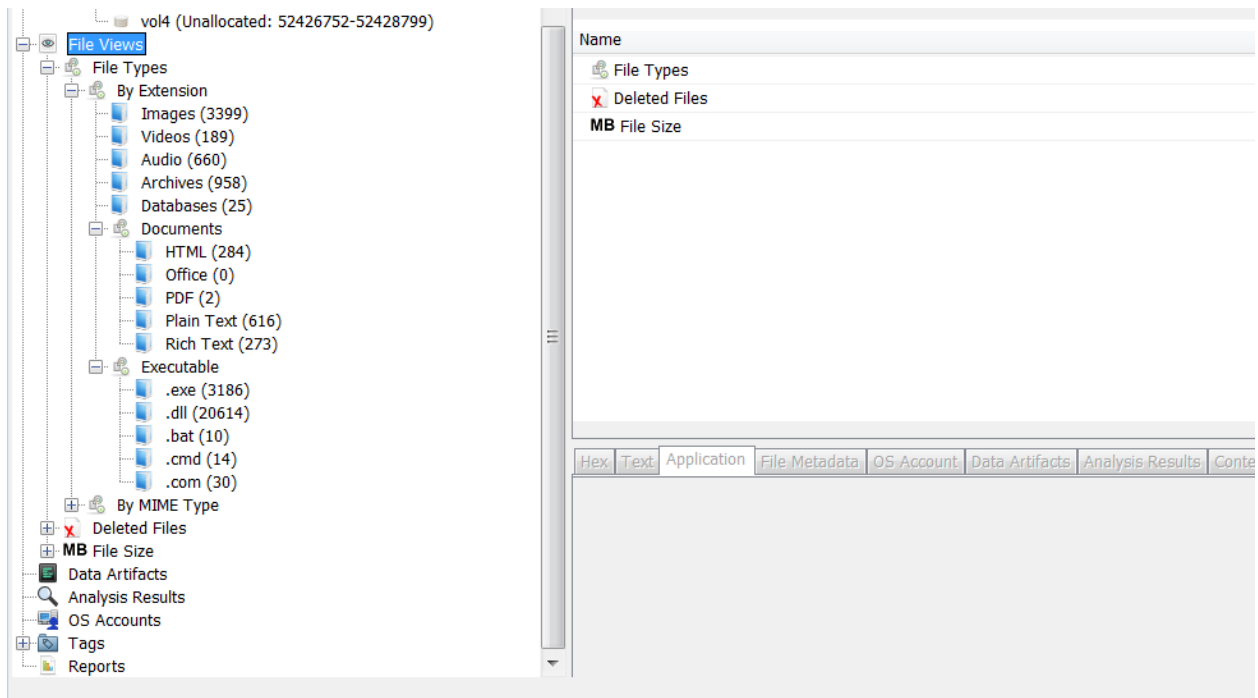
- Chọn tìm các số điện thoại và địa chỉ IP có trong Filesystem.



Kết quả: Không tìm kiếm được gì

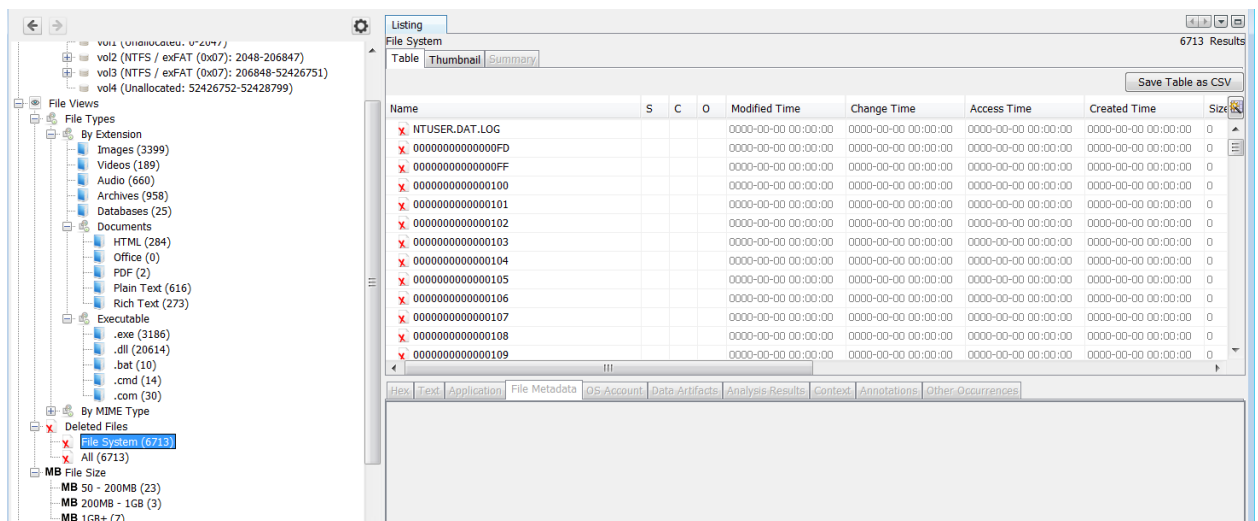


- Thực hiện việc xem xét toàn bộ Filesystem, xem xét các lựa chọn nằm ở phía bên trái của màn hình.



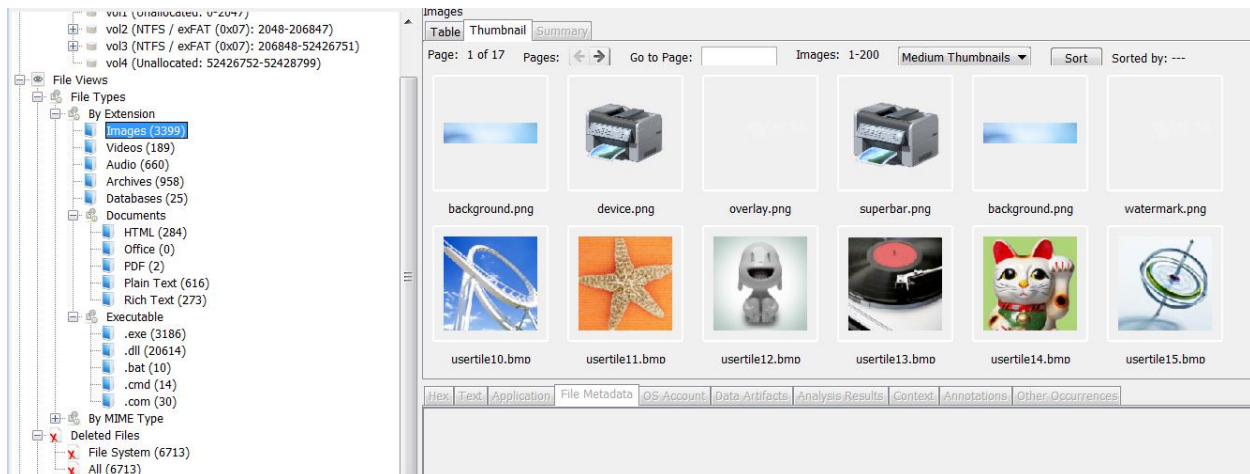
- **Tìm thư mục có nhiều File nhất trong Filesystem.**

Thư mục File System và All đều chứa 6713 files



- **Xem các file hình ảnh chứa trong Filesystem bằng chế độ view Thumbnail. Xác định số lượng các files dạng doc và pdf chứa trong Filesystem.**

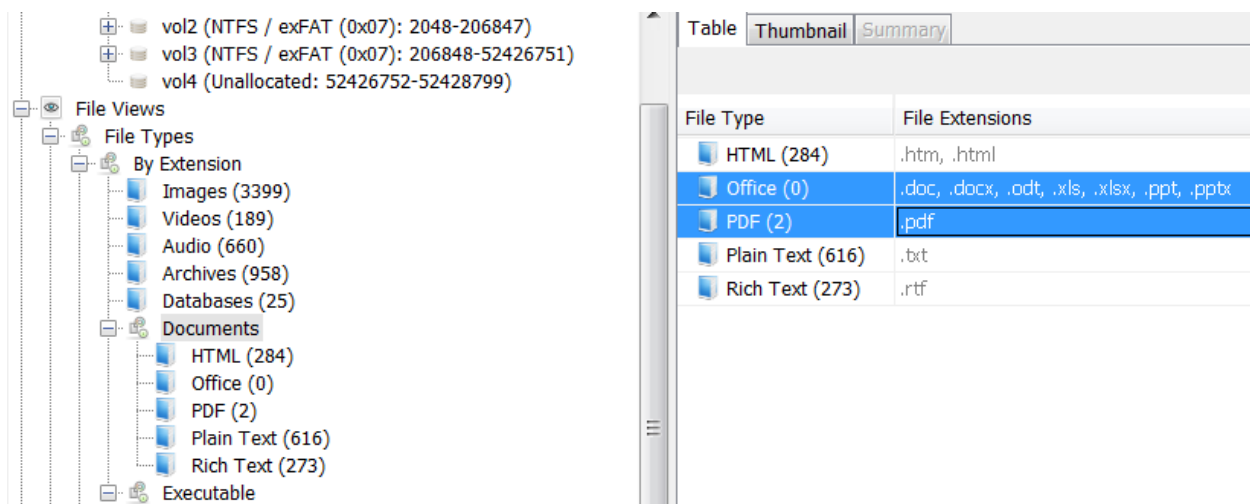
Xem file hình ảnh bằng Thumbnail



Xác định số lượng files doc và pdf

Doc: 0

Pdf: 2



- Sử dụng nút "Generate Report" để tạo ra báo cáo dạng HTML và Excel, xem nội dung báo cáo trong mục Report. Nêu nhận xét, kết luận về nội dung của báo cáo.

HTML Report: Bản tóm tắt các thông tin chính bao gồm các thông tin về case name, số lượng data source, thông tin hình ảnh, múi giờ, đường dẫn tới ổ cứng khai thác, phiên bản ứng dụng và ingest history (theo tìm hiểu thì đây là lịch sử truy cập dữ liệu để phân tích hoạt động của người dùng)

Report Navigation

- Case Summary
- ★ Tagged Files (0)
- ★ Tagged Images (0)
- ★ Tagged Results (0)

Autopsy Forensic Report

HTML Report Generated on 2023/04/19 15:01:13

Case: kb01
Number of data sources in case: 1

Image Information:

PhysicalDrive0

Timezone: Asia/Bangkok
Path: \\.\PhysicalDrive0

Software Information:

Autopsy Version: 4.20.0

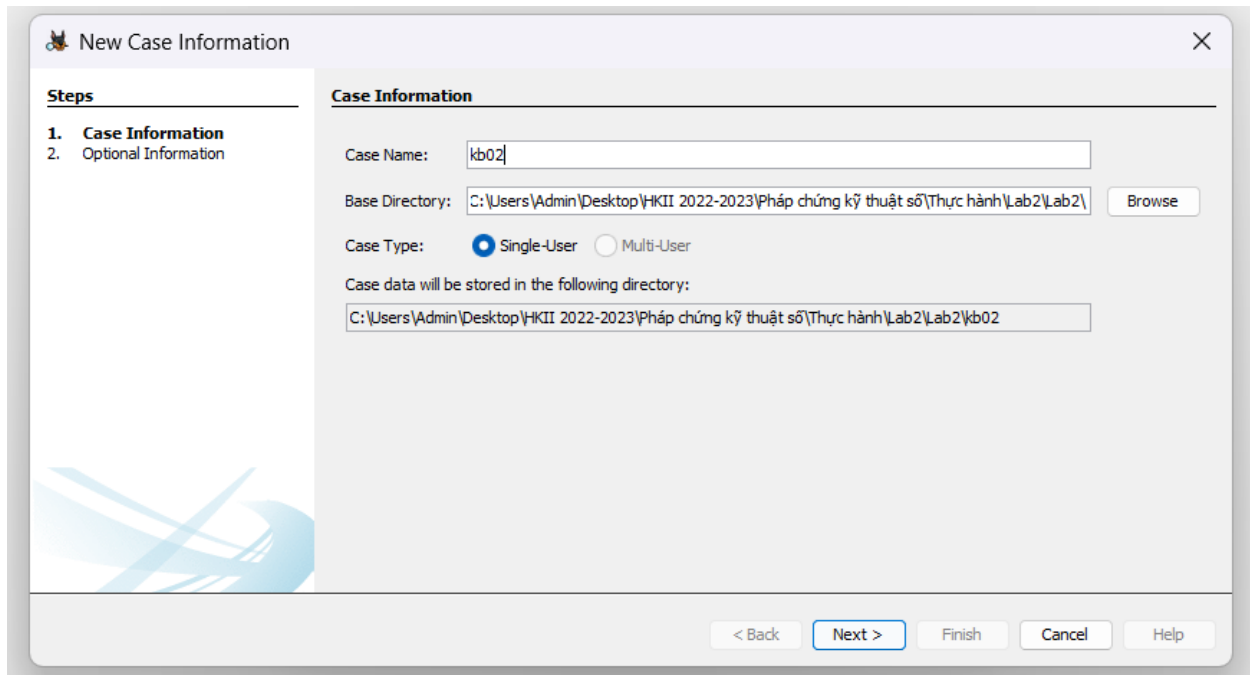
Ingest History:

- Excel Report: Chỉ gồm 2 thông tin là Casename và số lượng data sources trong case này

	A	B	C	D
1	Summary			
2				
3	Case Name:	kb01		
4	Number of data sources in case:	1		
5				
6				
7				

Kịch bản 2

- Mở Autopsy -> New Case -> set case name để tạo case mới

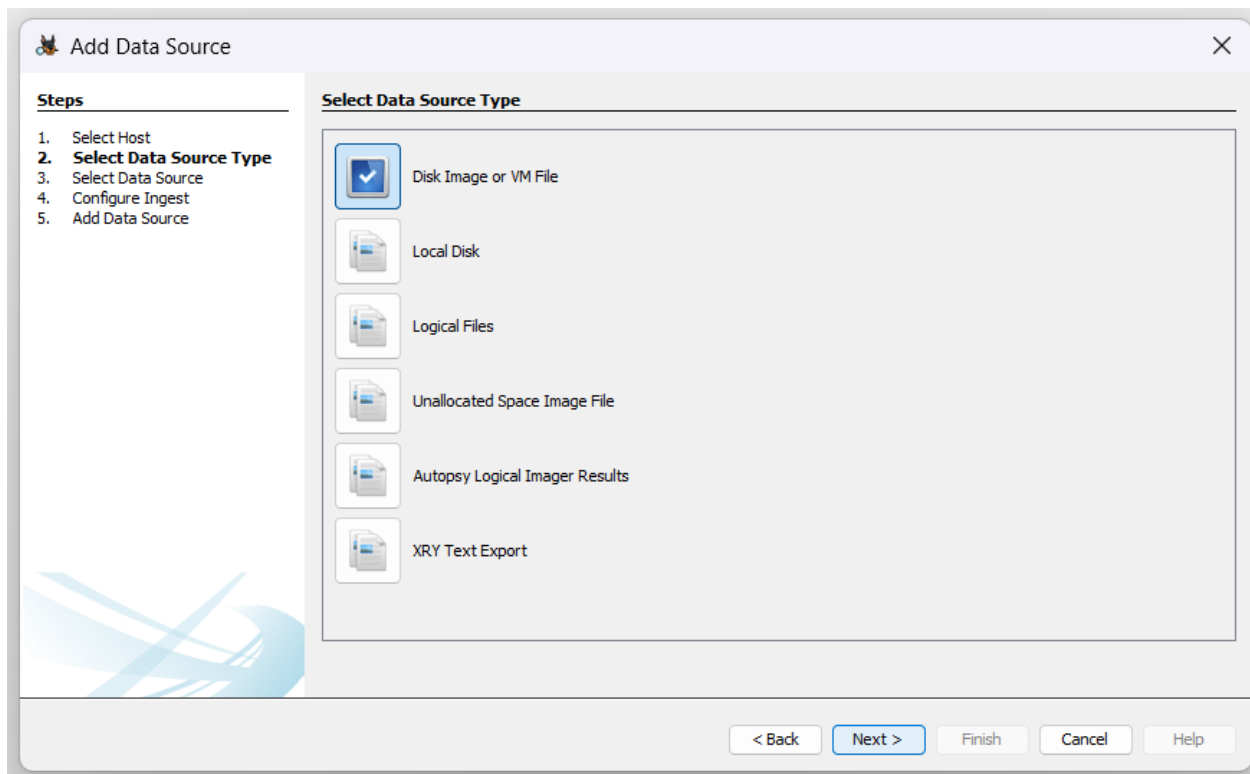


The 'New Case Information' dialog box is shown. It has a 'Steps' sidebar on the left with two steps: '1. Case Information' (selected) and '2. Optional Information'. The main area is titled 'Case Information' and contains the following fields:

- Case Name:** A text box containing 'kb02'.
- Base Directory:** A text box containing 'C:\Users\Admin\Desktop\HKII 2022-2023\Pháp chứng kỹ thuật số\Thực hành\Lab2\Lab2\'. To the right is a 'Browse' button.
- Case Type:** Two radio buttons: 'Single-User' (selected) and 'Multi-User'.
- Case data will be stored in the following directory:** A text box containing 'C:\Users\Admin\Desktop\HKII 2022-2023\Pháp chứng kỹ thuật số\Thực hành\Lab2\Lab2\kb02'.

At the bottom, there are five buttons: '< Back', 'Next >' (highlighted), 'Finish', 'Cancel', and 'Help'.

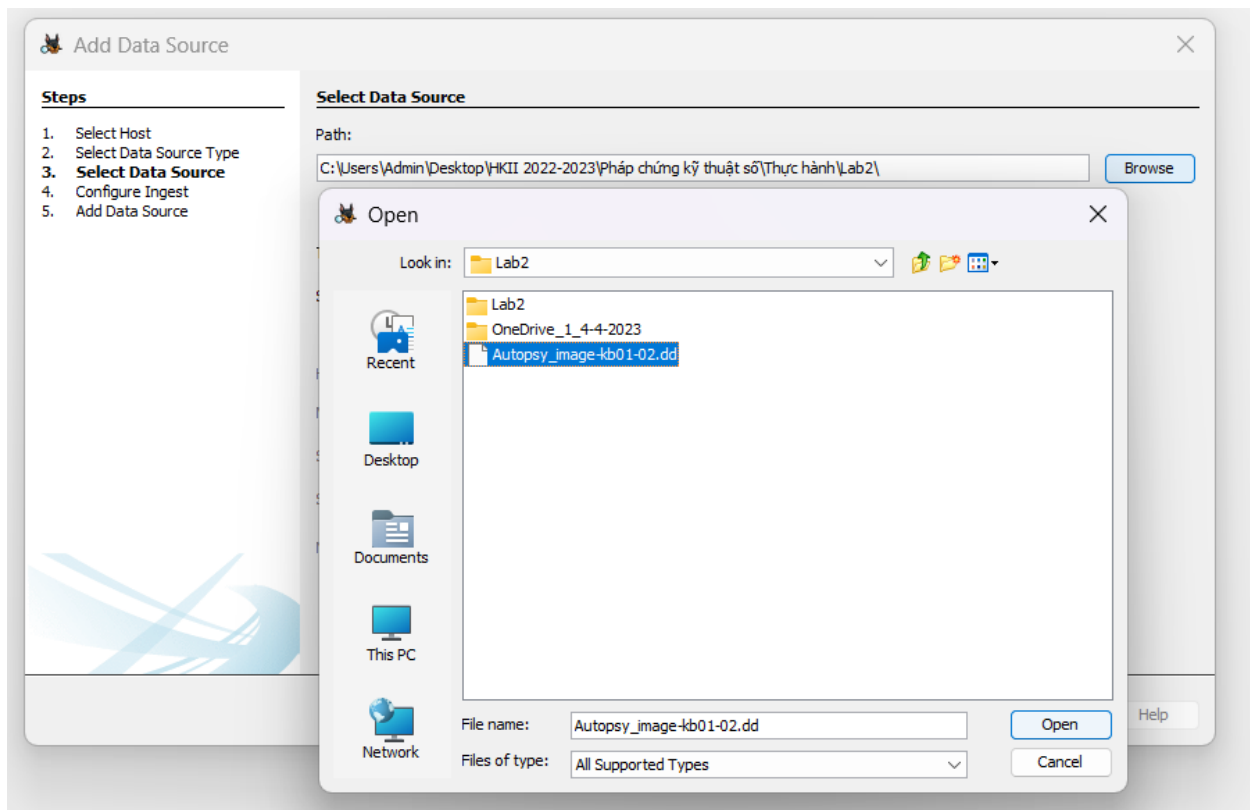
- Tại Add data source, chọn **Disk Image or VM File** và chọn path tới file tài nguyên cho sẵn



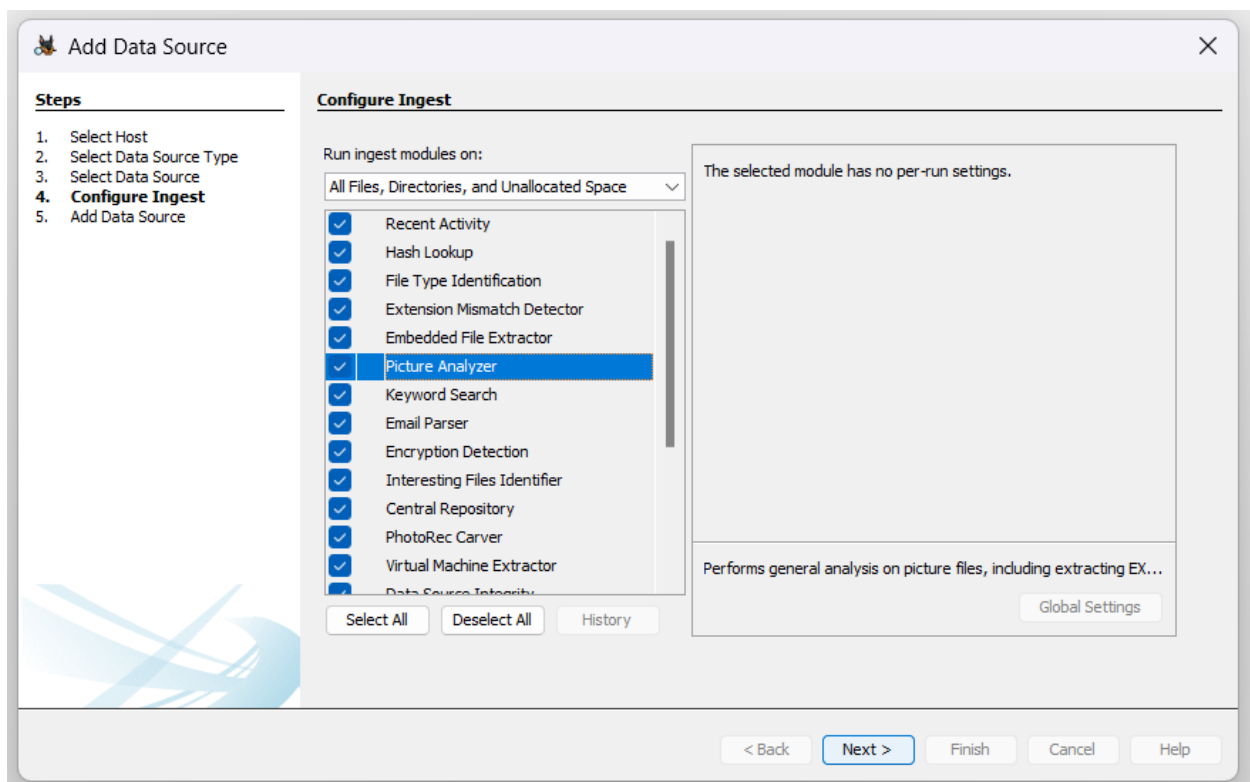
The 'Add Data Source' dialog box is shown. It has a 'Steps' sidebar on the left with five steps: '1. Select Host', '2. Select Data Source Type' (selected), '3. Select Data Source', '4. Configure Ingest', and '5. Add Data Source'. The main area is titled 'Select Data Source Type' and contains a list of options, each with a folder icon and a text label:

- Disk Image or VM File** (selected with a blue checkmark icon)
- Local Disk
- Logical Files
- Unallocated Space Image File
- Autopsy Logical Imager Results
- XRY Text Export

At the bottom, there are five buttons: '< Back', 'Next >' (highlighted), 'Finish', 'Cancel', and 'Help'.



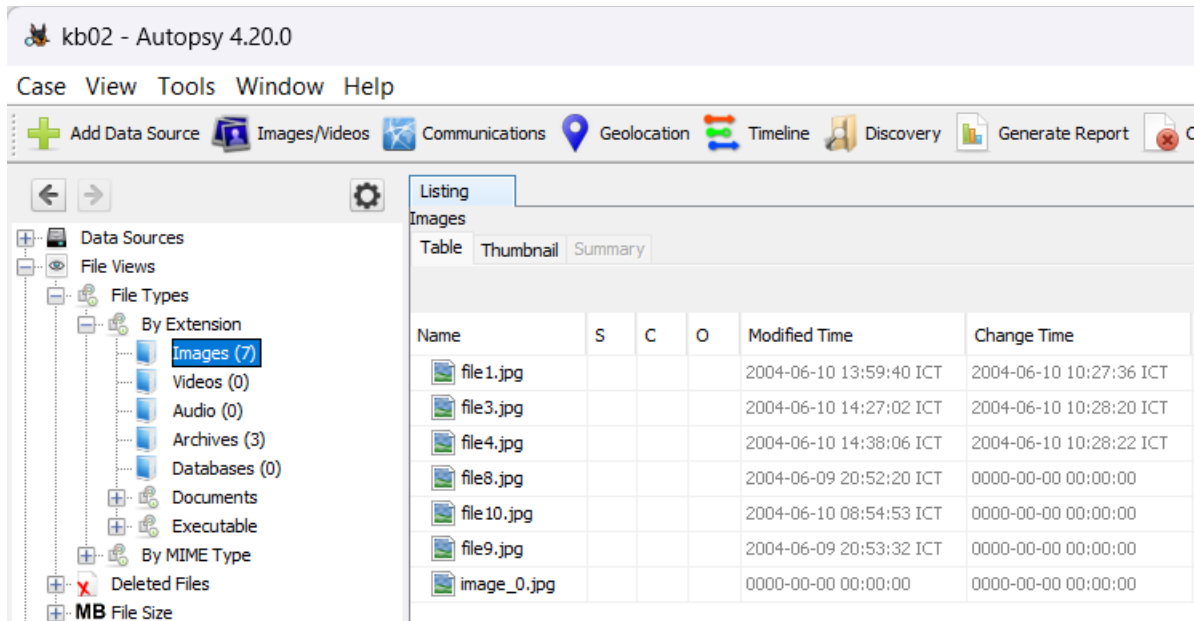
- Chọn các module cần phân tích



- Vào File Views, nơi hiển thị các thông tin chi tiết thông tin của các file chứa trong Filesystem.

Tìm tất cả các hình ảnh

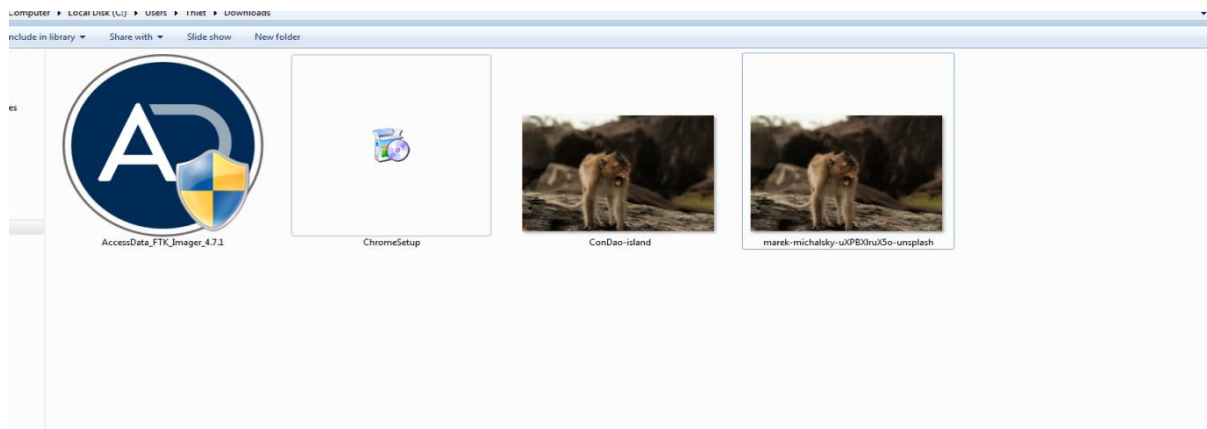
File Views -> File Types -> By Extension



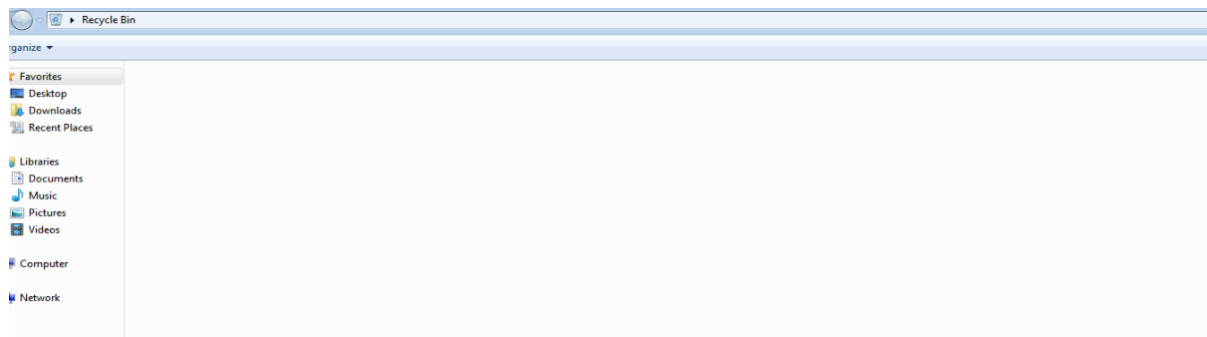
Liệt kê thông tin liên quan tới các file ảnh tìm được

Listing														
Images														
Table Thumbnail Summary														
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash
file4.jpg				2004-06-10 14:38:06 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:28:22 ICT	2004-06-10 10:28:20 ICT	199021	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.d\invalid\file4.jpg		
file3.jpg				2004-06-10 14:27:02 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:28:20 ICT	2004-06-10 10:28:20 ICT	214228	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.d\invalid\file3.jpg		
file1.jpg				2004-06-10 13:59:40 ICT	2004-06-10 10:27:36 ICT	2004-06-10 10:27:36 ICT	2004-06-10 10:27:36 ICT	274260	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.d\alloc\file1.jpg		
file8.jpg				2004-06-09 20:52:20 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	337653	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.d\archive\file8.zip\file8.jpg		
file10.jpg				2004-06-10 08:54:53 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	209919	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.d\archive\file10.tar.gz\file...		
file9.jpg				2004-06-09 20:53:32 ICT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	292813	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.d\archive\file9-bon\file9.jpg		
image_0.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	110373	Allocated	Allocated	unknown	/img_Autopsy_image-kb01-02.d\misc\file12.doc\image_0....		

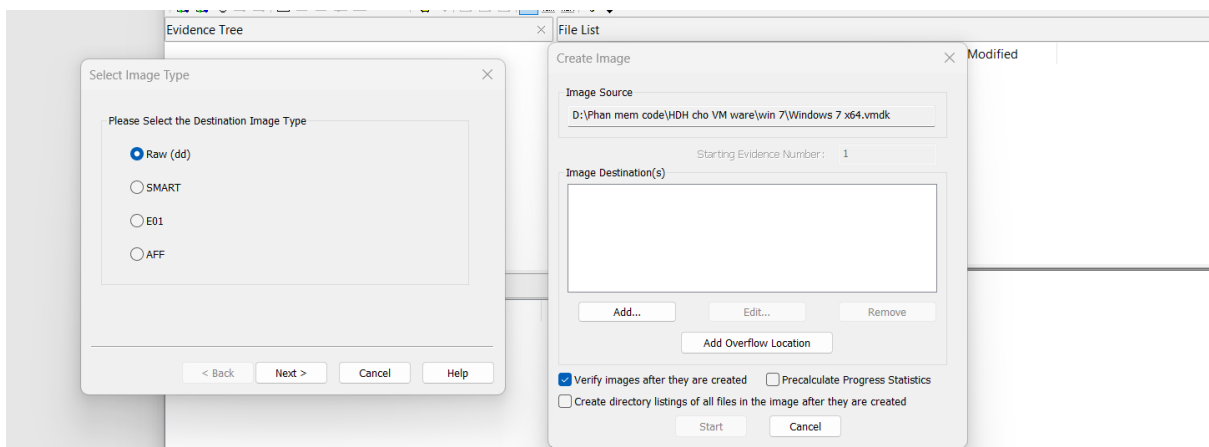
Kịch bản 3



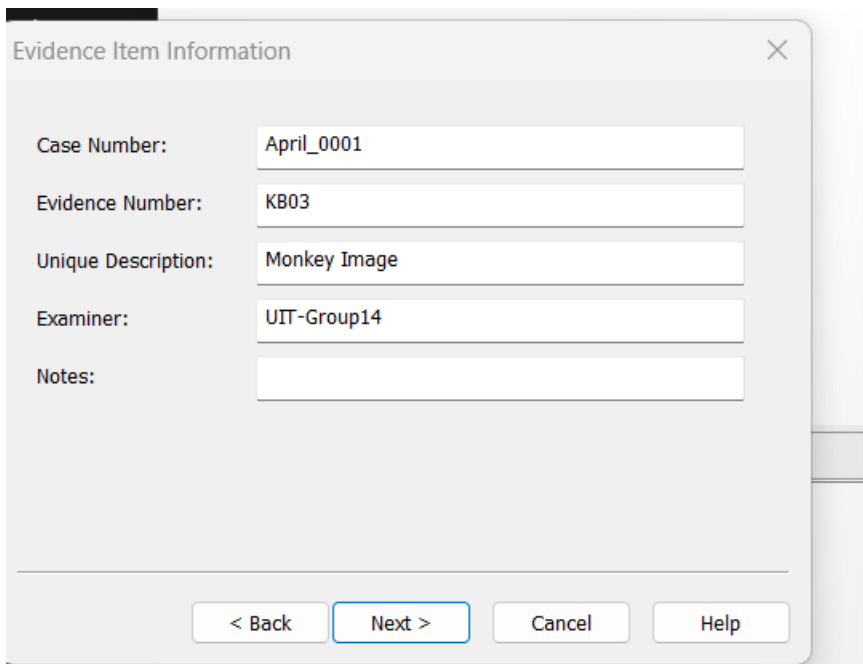
- Trên máy ảo win 7 ta tải file ảnh về sau đó đổi tên “ConDao-island”



- Ta thực hiện xóa ảnh, Xóa luôn trong recycle bin



- Tạo một ảnh đĩa -định dạng Raw (dd) sau khi xóa file ảnh trên



Evidence Item Information

Case Number: April_0001

Evidence Number: KB03

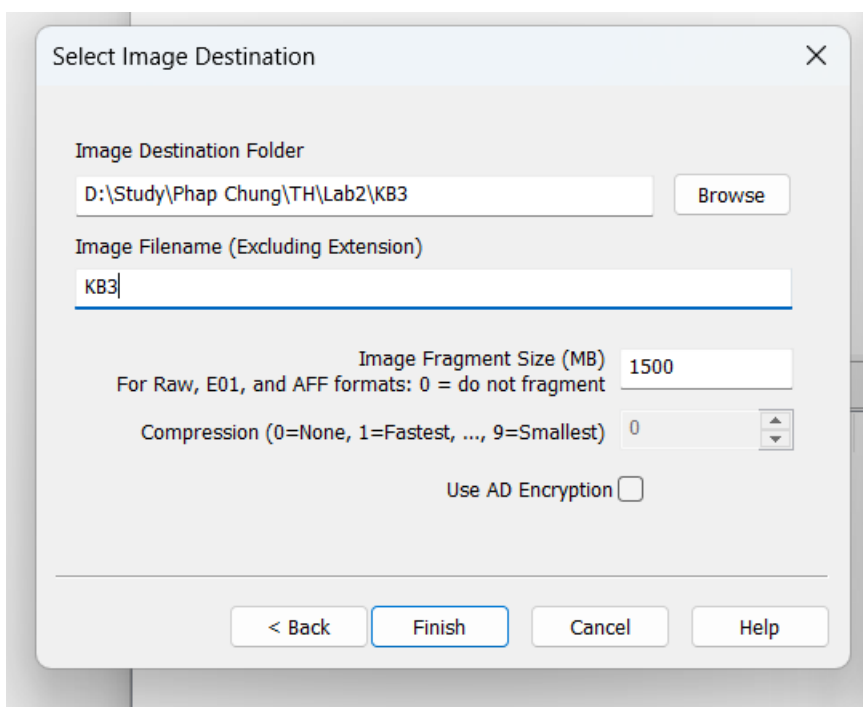
Unique Description: Monkey Image

Examiner: UIT-Group14

Notes:

< Back Next > Cancel Help

- Đặt tên theo yêu cầu



Select Image Destination

Image Destination Folder
D:\Study\Phap Chung\TH\Lab2\KB3 Browse

Image Filename (Excluding Extension)
KB3

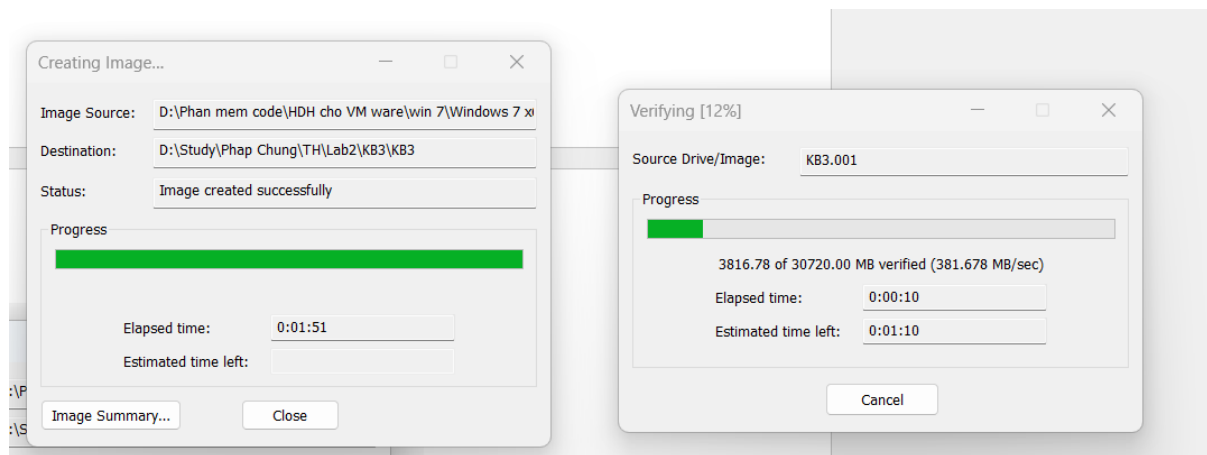
Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

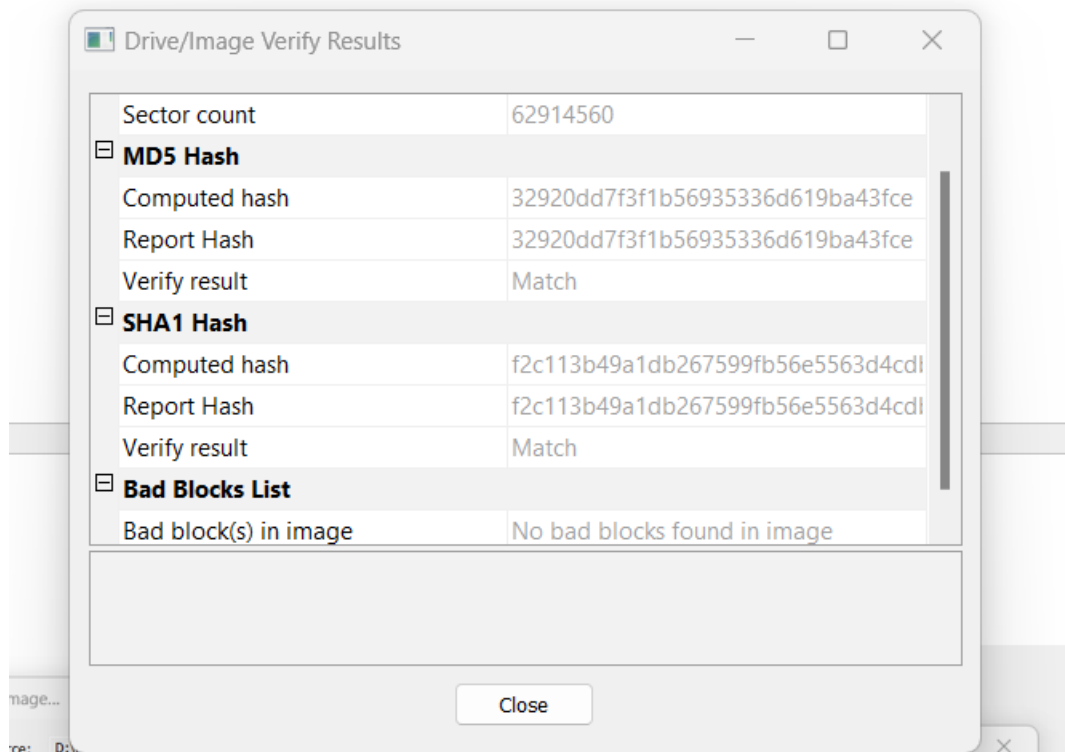
Use AD Encryption ☐

< Back Finish Cancel Help

- Ta lưu vào 1 folder và đặt tên là KB3



- Đợi quá trình tạo disk image hoàn tất

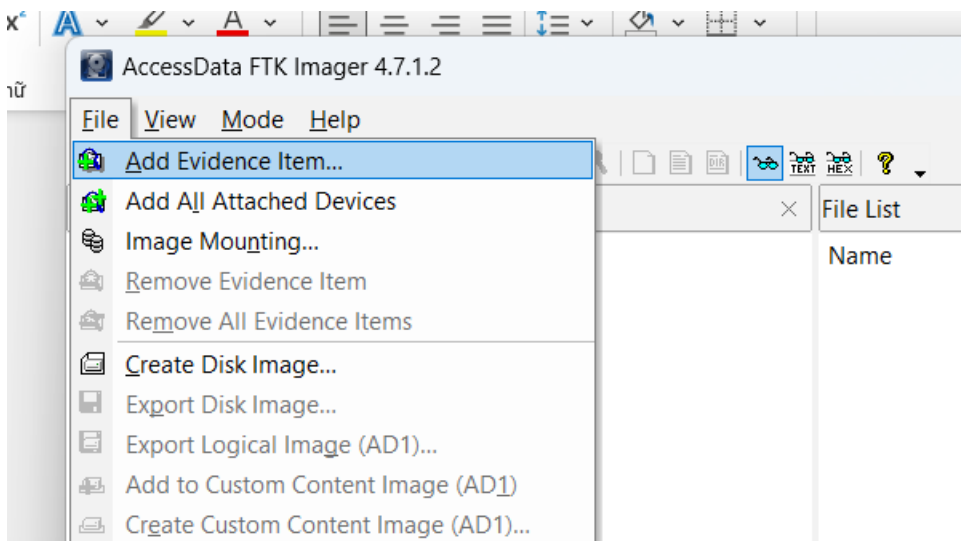


- Sau khi hoàn tất thì ta có bảng tóm tắt disk image vừa tạo

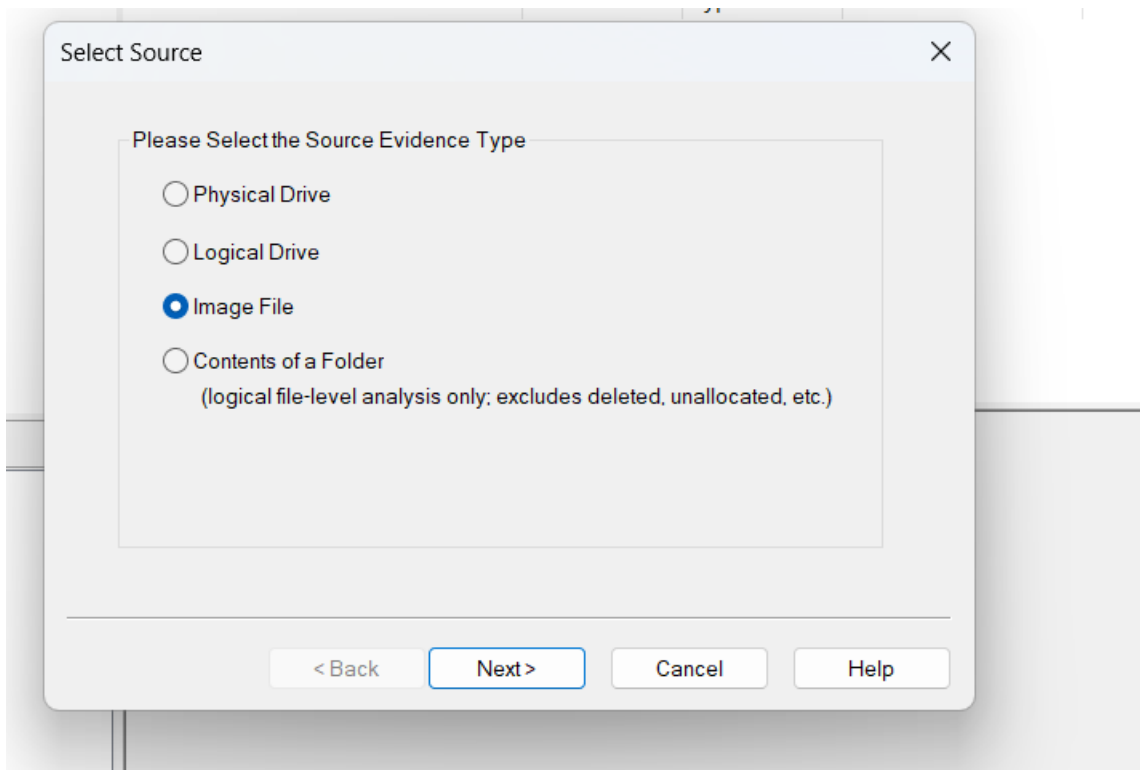
↑ > This PC > Data (D:) > Study > Pháp Chung > TH > Lab2 > KB3

Name	Date modified	Type	Size
KB3.001	4/19/2023 1:52 PM	WinRAR archive	1,536,000 ...
KB3.001.txt	4/19/2023 1:55 PM	Tài liệu văn bản	3 KB
KB3.002	4/19/2023 1:52 PM	002 File	1,536,000 ...
KB3.003	4/19/2023 1:52 PM	003 File	1,536,000 ...
KB3.004	4/19/2023 1:53 PM	004 File	1,536,000 ...
KB3.005	4/19/2023 1:53 PM	005 File	1,536,000 ...
KB3.006	4/19/2023 1:53 PM	006 File	1,536,000 ...
KB3.007	4/19/2023 1:53 PM	007 File	1,536,000 ...
KB3.008	4/19/2023 1:53 PM	008 File	1,536,000 ...
KB3.009	4/19/2023 1:53 PM	009 File	1,536,000 ...
KB3.010	4/19/2023 1:53 PM	010 File	1,536,000 ...
KB3.011	4/19/2023 1:53 PM	011 File	1,536,000 ...
KB3.012	4/19/2023 1:53 PM	012 File	1,536,000 ...

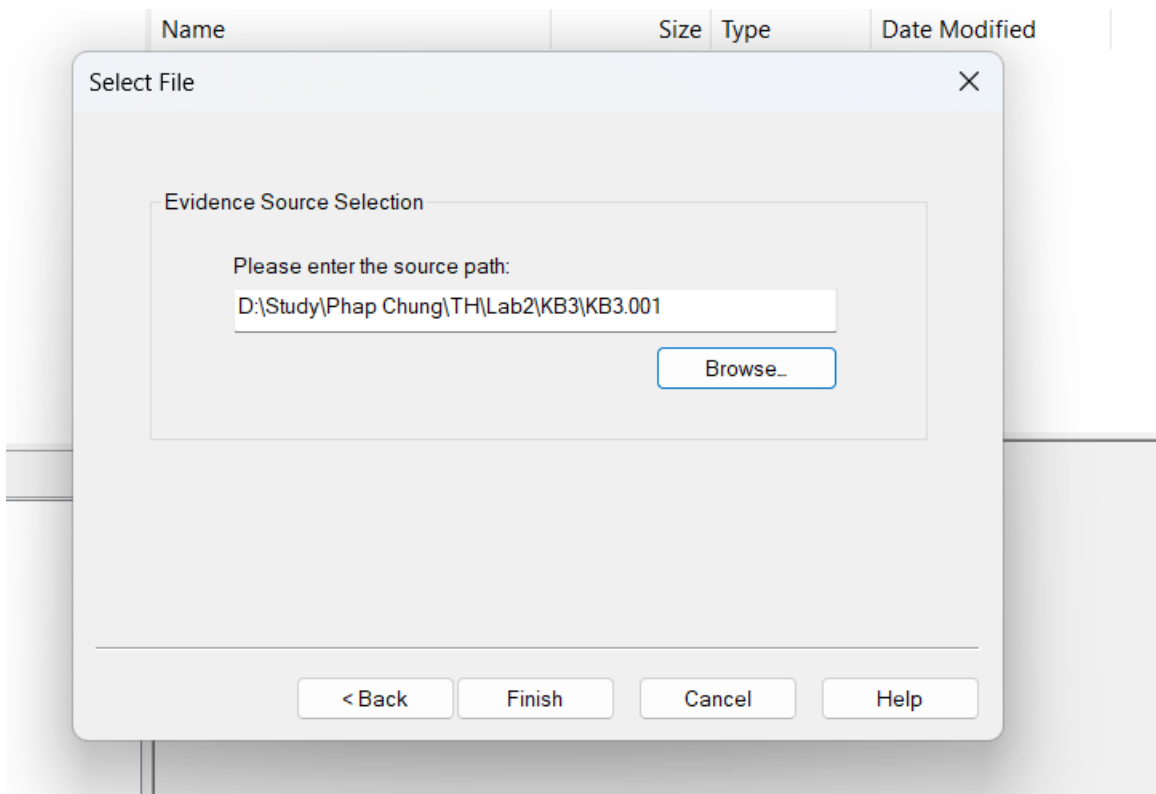
- Trong thư mục KB3 vừa tạo chứa disk image ta vừa tạo



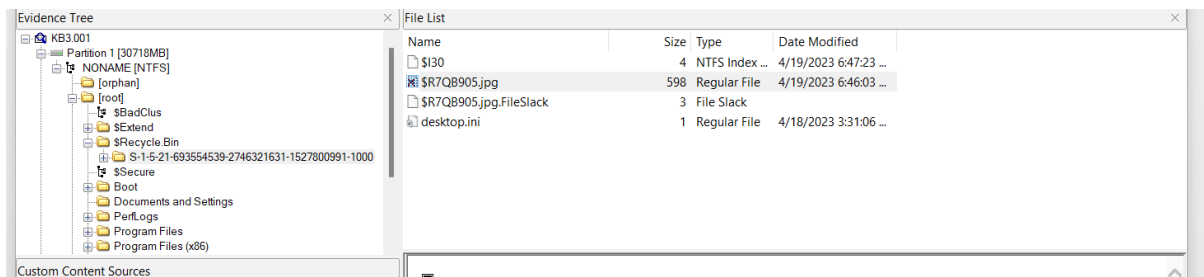
- Để thêm bằng chứng ta chọn file -> add evidence item



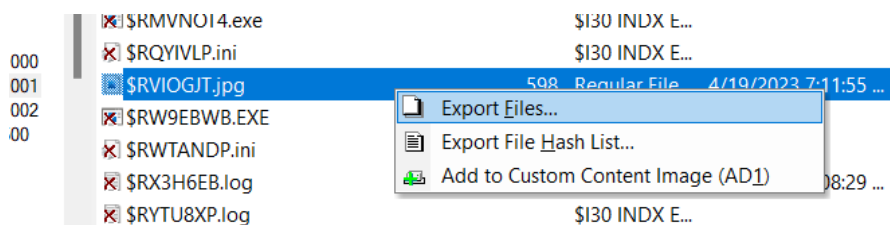
- Chọn image file



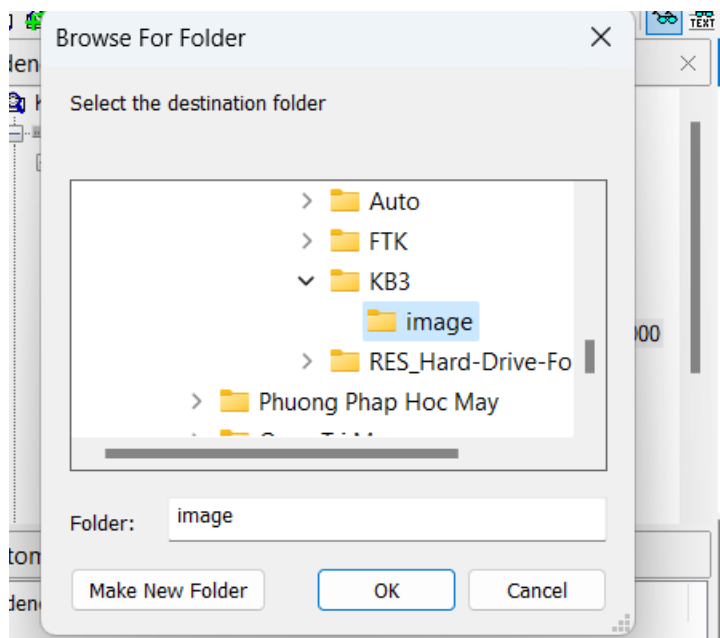
- Ta chọn disk image vừa tạo trong folder KB03



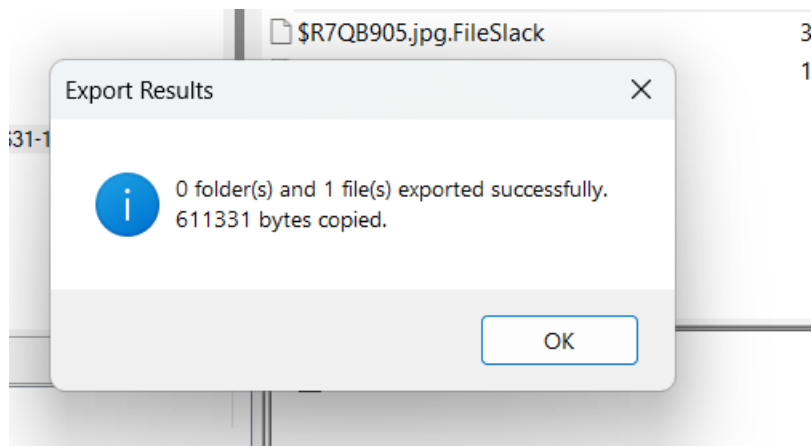
- Sử dụng tính năng phục hồi file ảnh đã bị xóa (tính năng Export Files), lưu trữ file này trong thư mục KB03\images.
- Ta để ý file ảnh của ta có kích thước 598kb trùng với kích thước file ảnh ta tải về



- Sử dụng tính năng export file để phục hồi



- Lưu vào thư mục KB3/image



- Ta phục hồi thành công

MD5 File Checksum

MD5 online hash file checksum function

\$RVIOGJT.jpg

Hash

☒ Auto Update

9ee18830b6c7d85abcc9c570686463e6

MD5 File Checksum

MD5 online hash file checksum function



Hash

☒ Auto Update

9ee18830b6c7d85abcc9c570686463e6

- Mã MD5 hash giống nhau vậy là cùng 1 file

```
C:\Users\Thiet>dir "D:\Study\Phap Chung\TH\Lab2\KB3\image" | findstr "ConDao-island"
04/19/2023  02:06 PM                611,331 ConDao-island.jpg

C:\Users\Thiet>date /t
Wed 04/19/2023

C:\Users\Thiet>echo "Group14-UIT"
"Group14-UIT"

C:\Users\Thiet>
```