**Cybersecurity 401**

**Module 7 - Threat Hunting**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

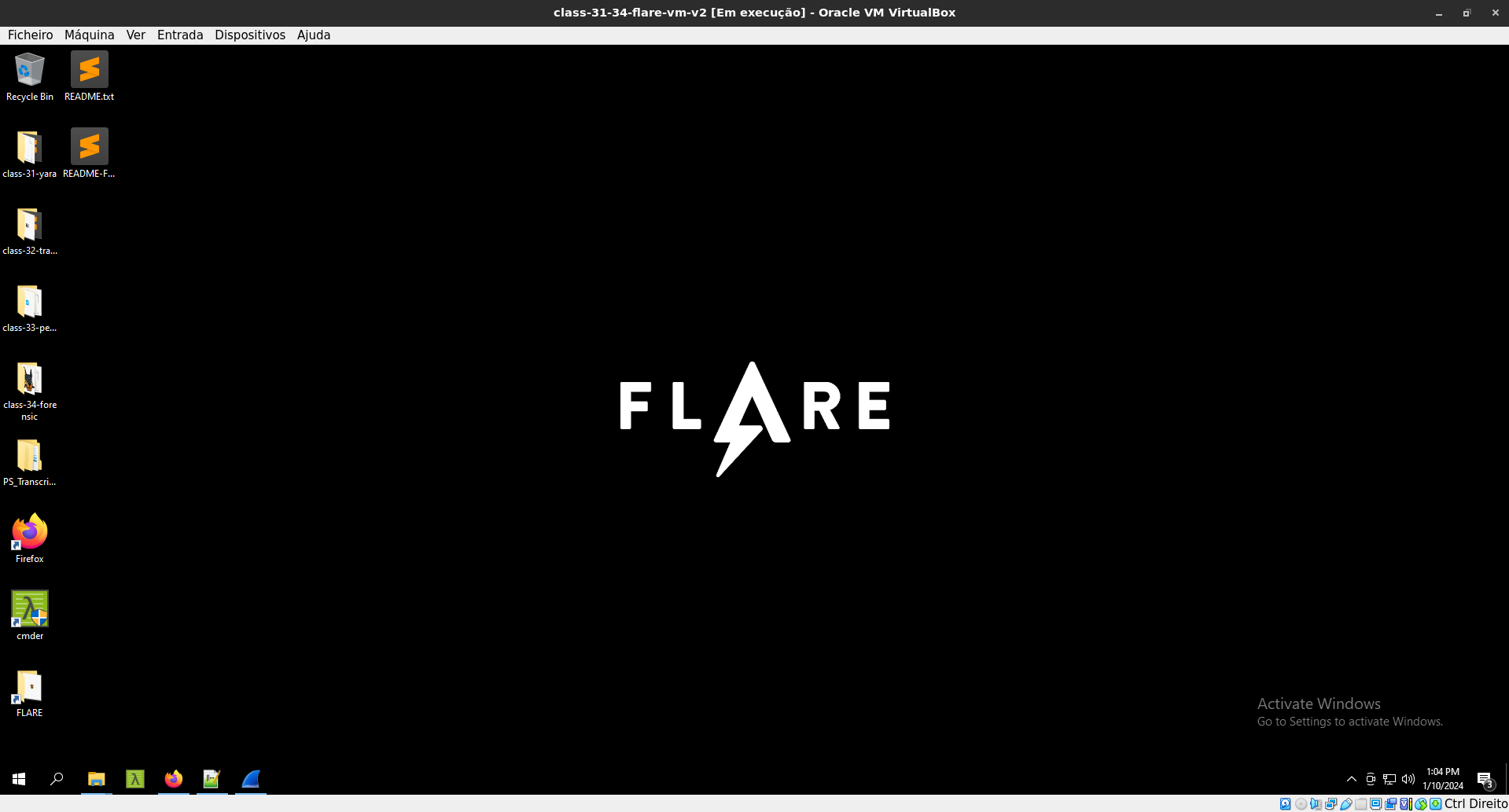
## **Lab 34 - Forensic Investigation with Autopsy**

## 

**| Rodrigo Brasil 12/2023 |**

### Part 1: Staging

You will need FLARE VM for this lab.



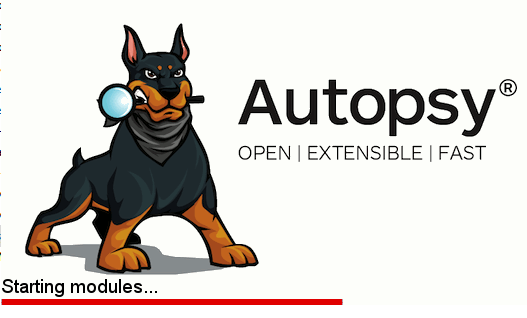
### 

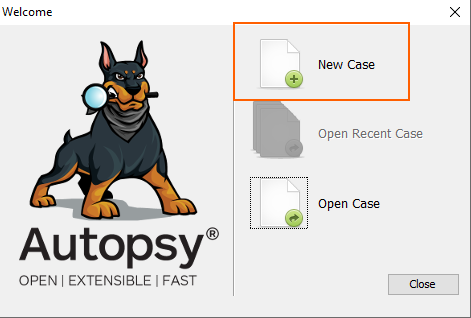
### Part 2: Investigating with Autopsy

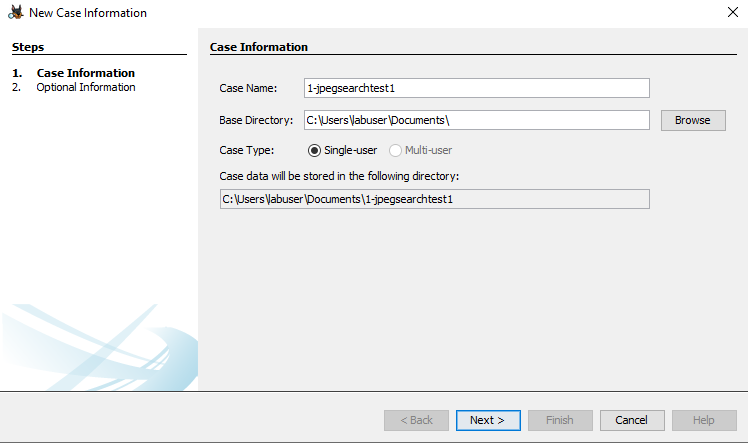
In today’s folder you’ll see twelve different scenarios you can investigate using Autopsy.

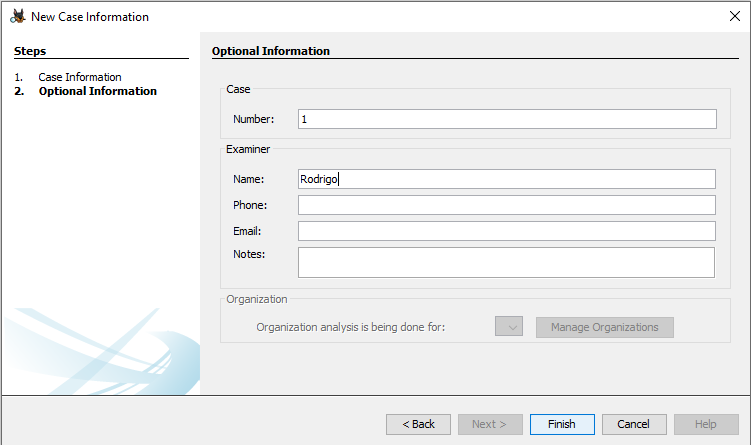
Complete at least three different scenarios using Autopsy.

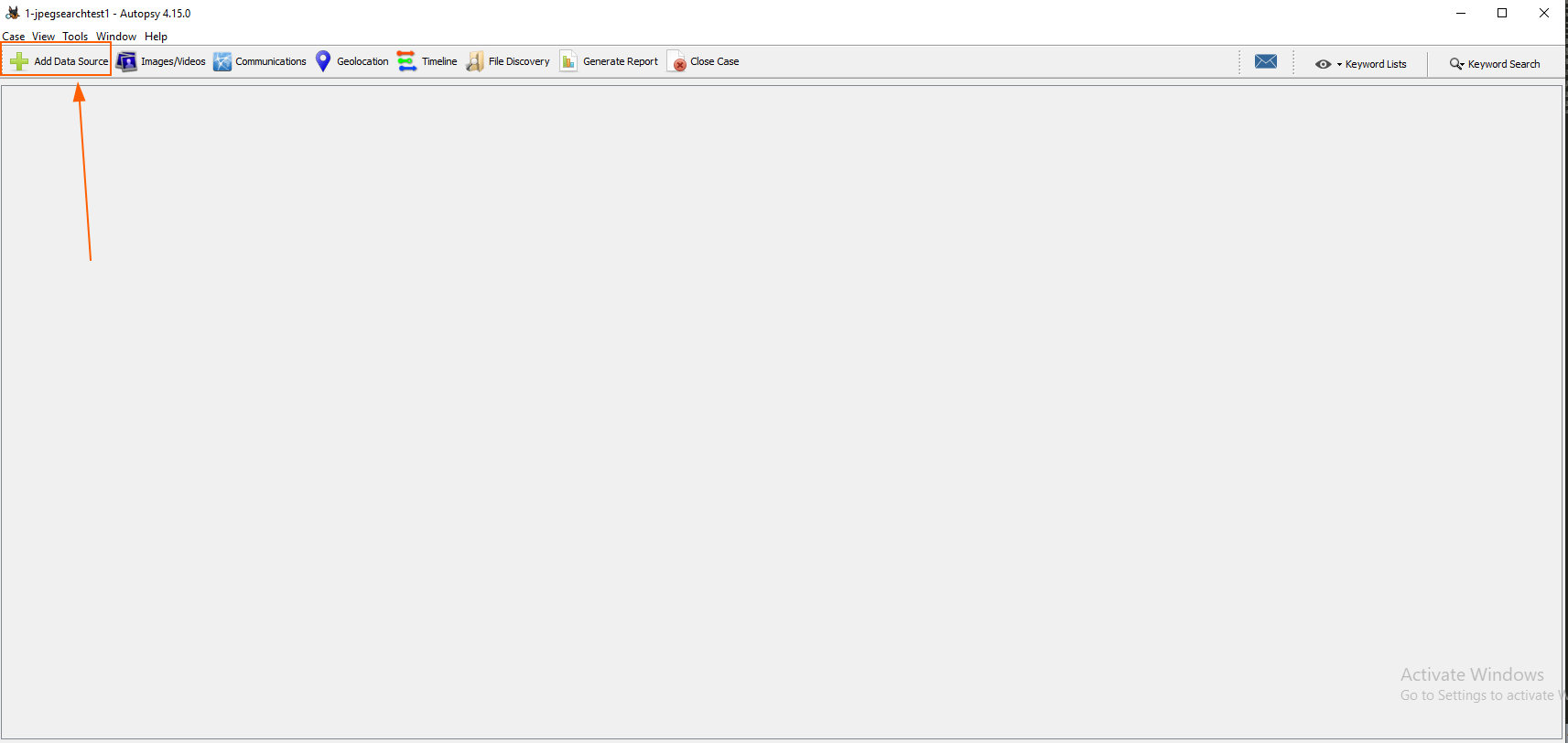
If a results.txt file is present for the scenario, copy its text over to your Google Doc submission and fill out your findings using this as a template. Otherwise, document your own findings in your submission today.

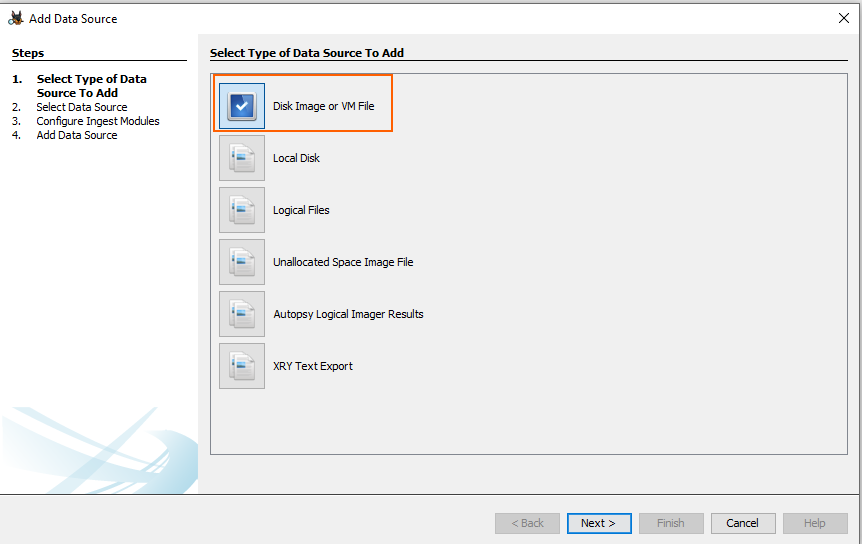


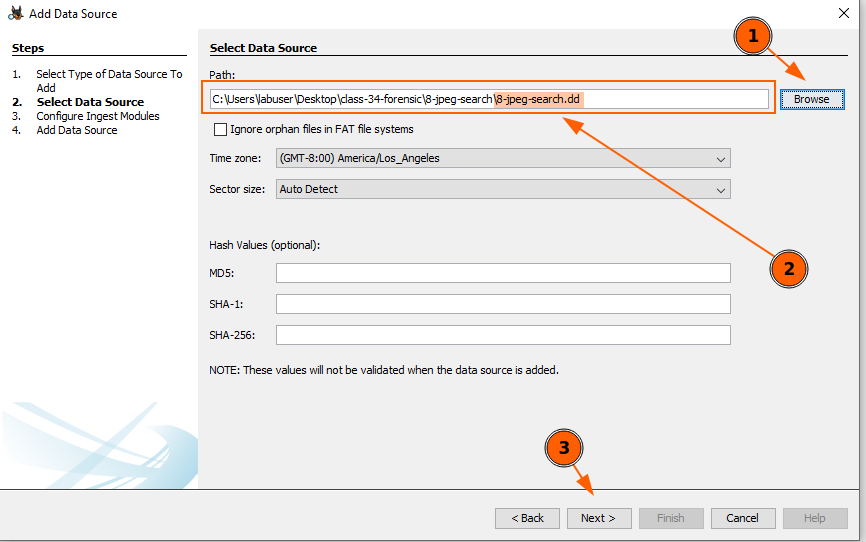


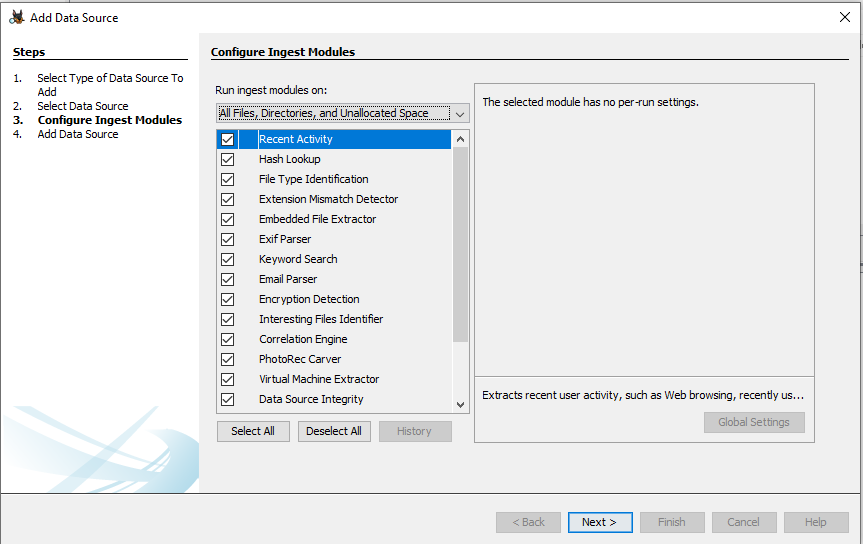


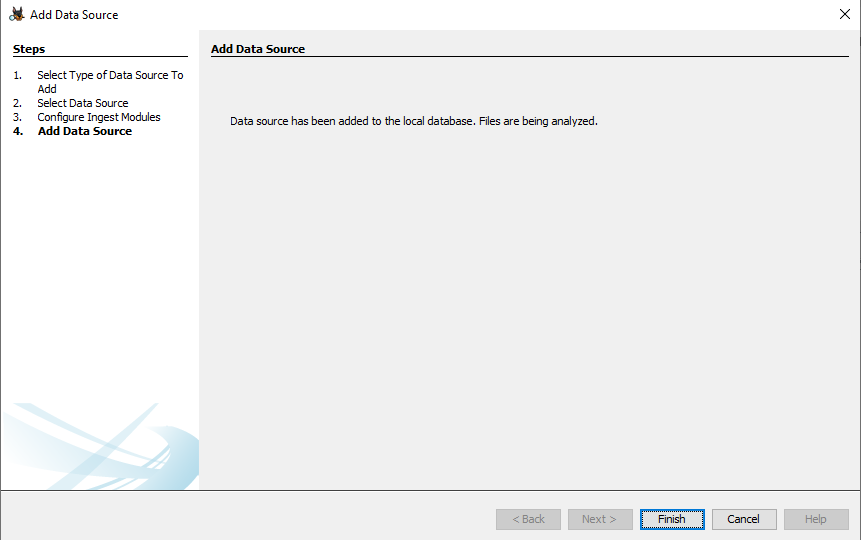


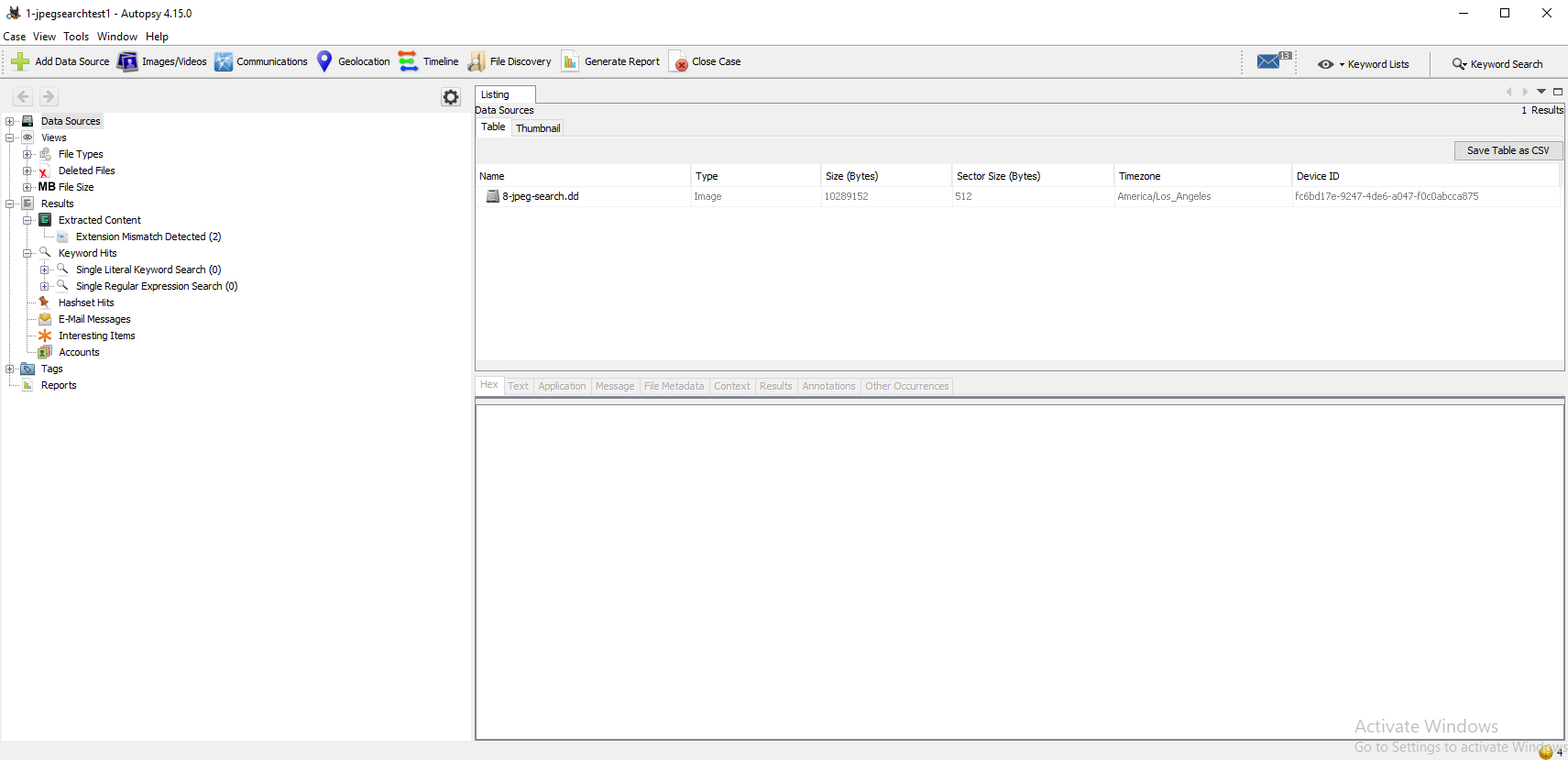












#### 

#### 8-jpeg-search

JPEG Search Test #1

Tool: Autopsy

Version: 4.15.0

1. What search procedure(s) were used to obtain the following

results? The procedure was running an automated search

tool called autopsy

The following apply to the results from running an automated search

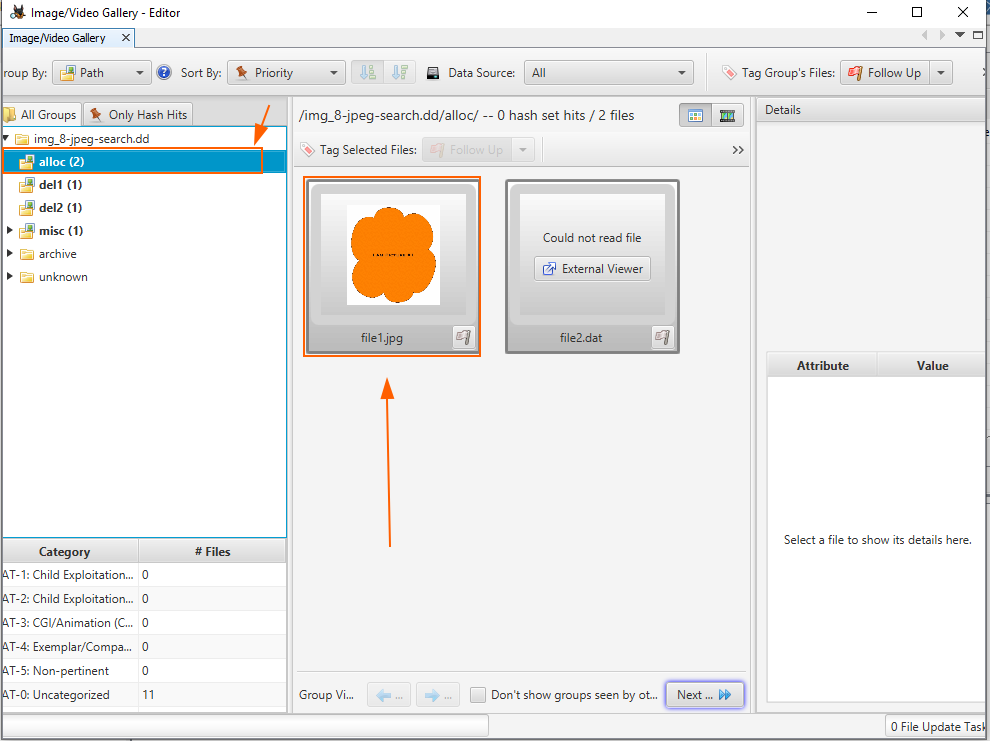
tool for JPEG pictures. If more than one procedure was used to

find the images, please note the procedure that was used to find

each. Note that this was not designed to test data carving tools.

2. Did the search results include the alloc\file1.jpg picture?

Yes the search results include the alloc\file1.jpg

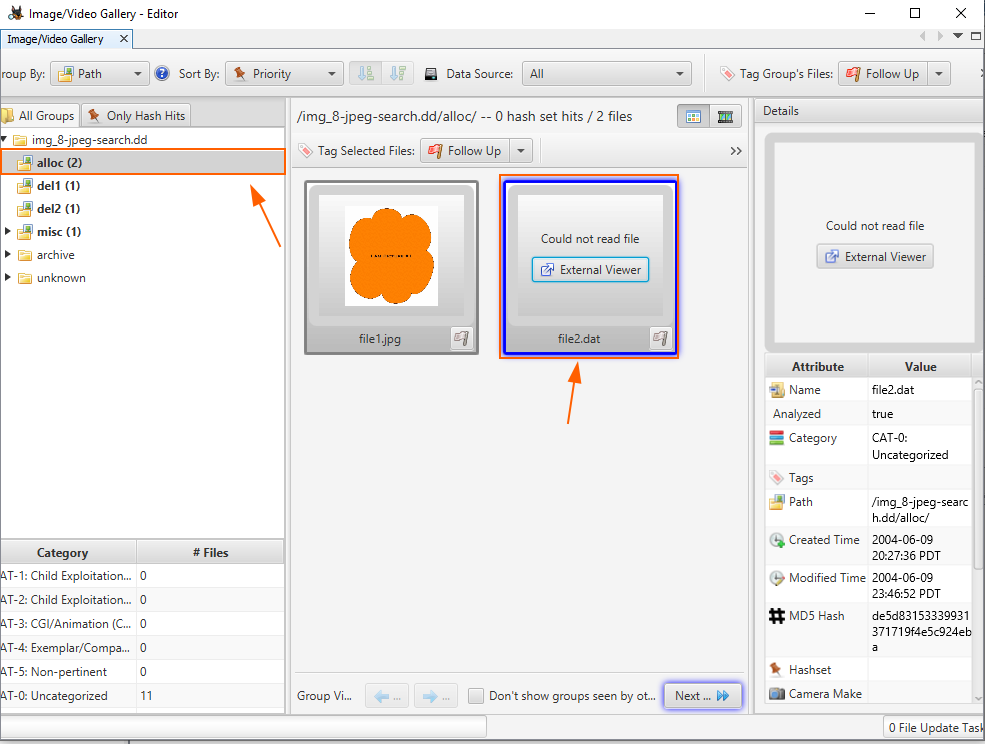


3. Did the search results include the alloc\file2.dat picture? If

not, then is it documented that JPEGs are found using only the

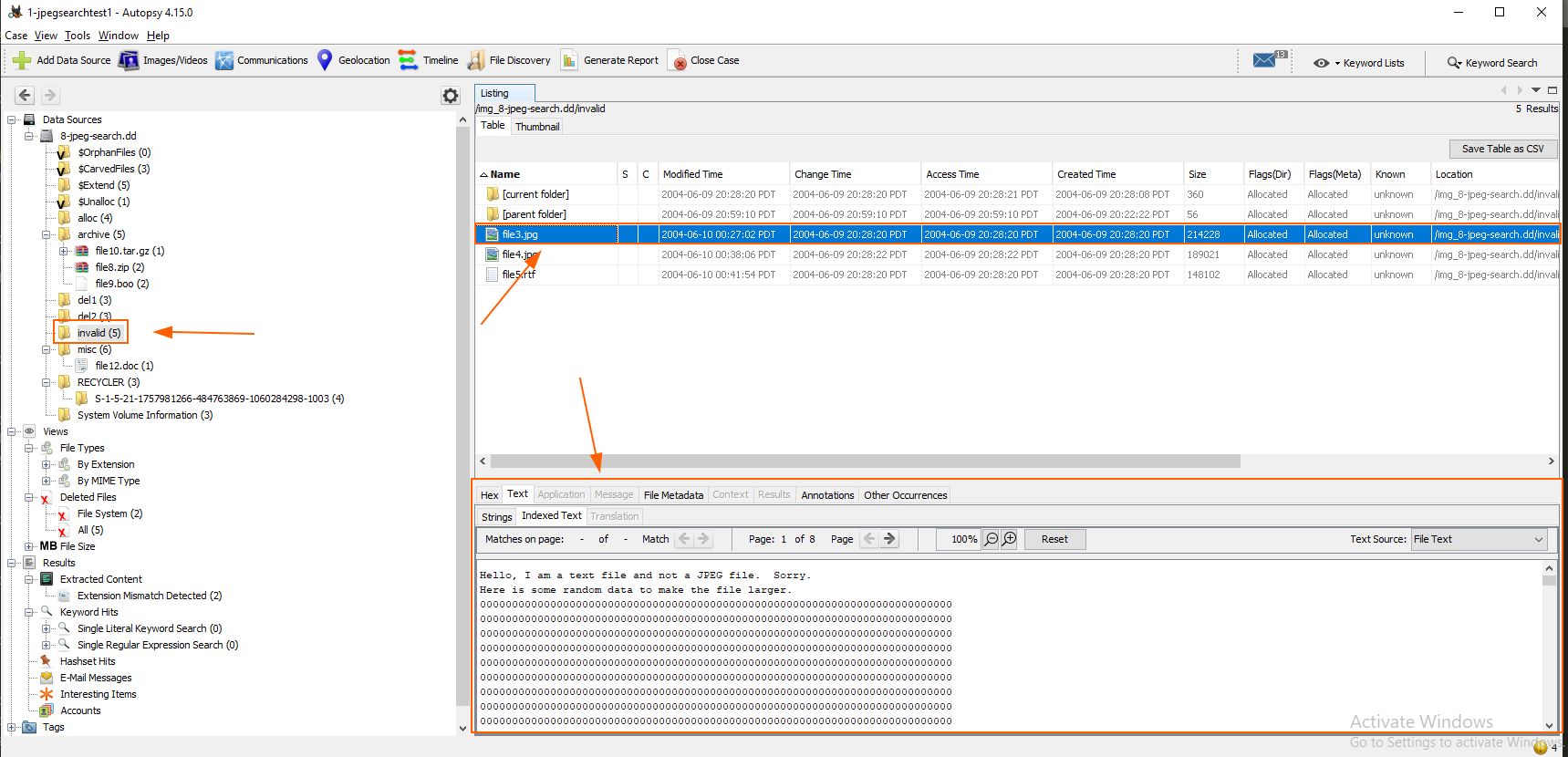
extension?

Yes the search results include the alloc\file2.dat



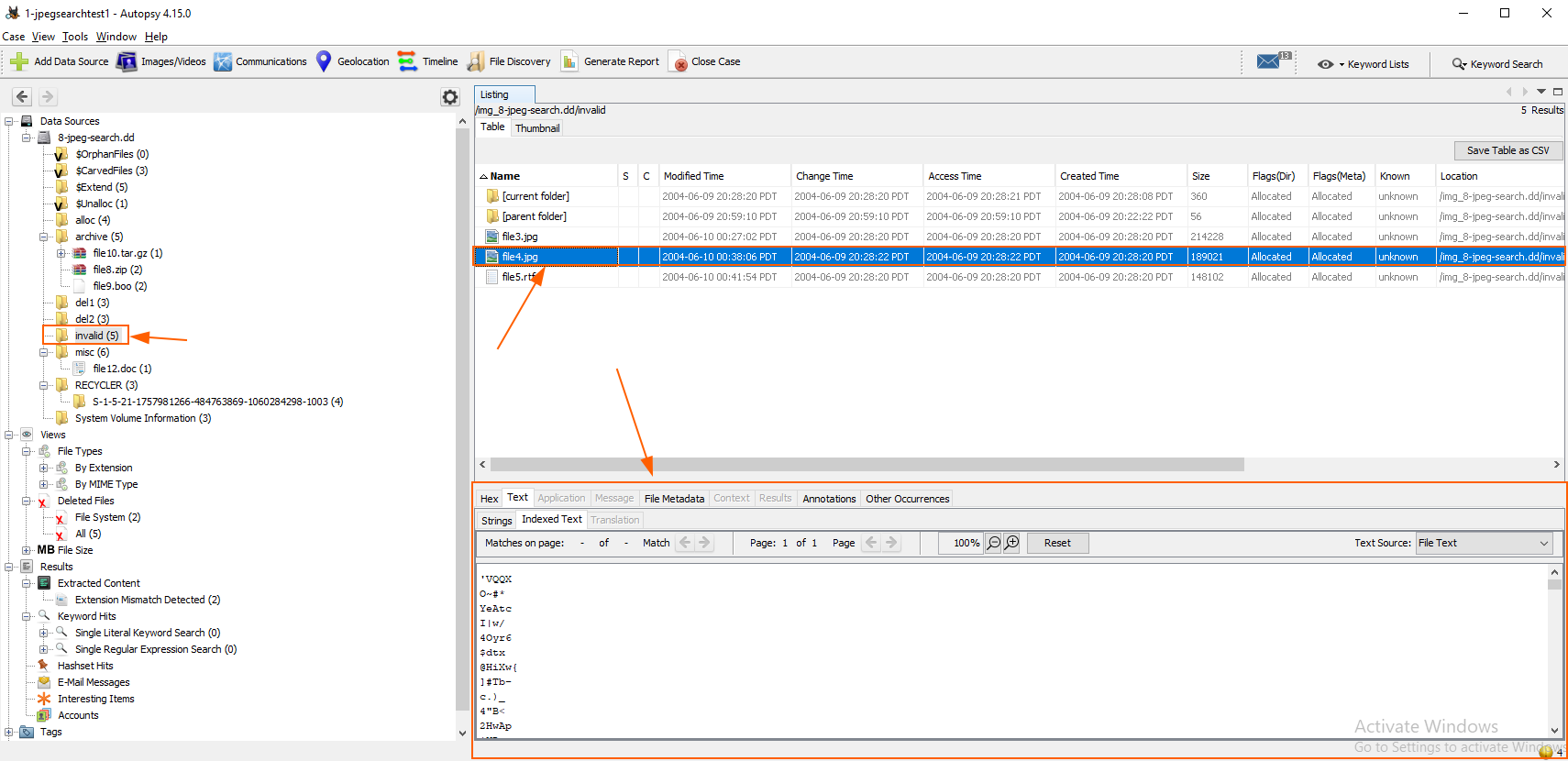
4. Did the search results include the invalid\file3.jpg file?

Yes the search results included the invalid\file3.jpg



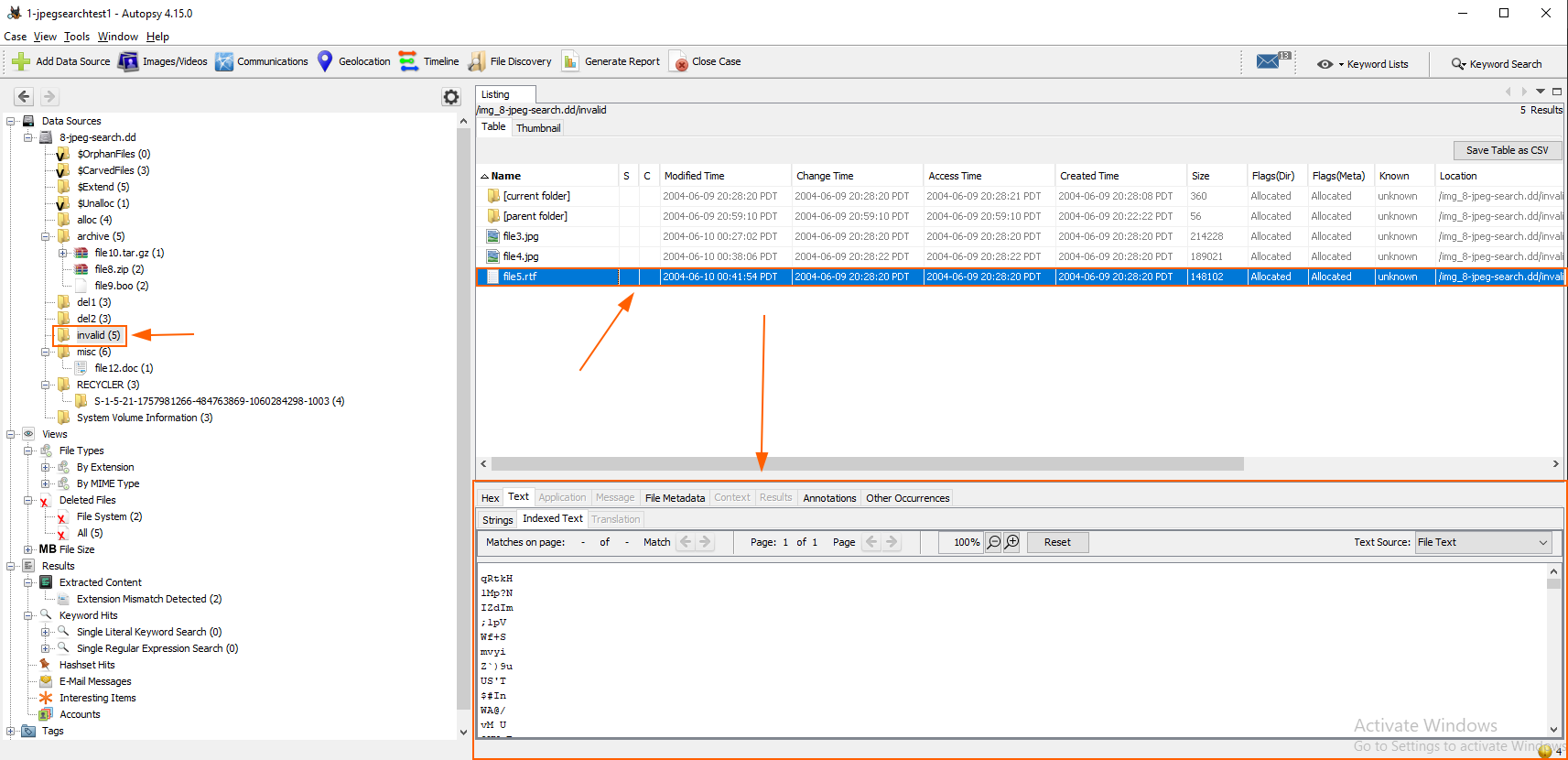
5. Did the search results include the invalid\file4.jpg file?

Yes the search results include the invalid\file4.jpg



6. Did the search results include the invalid\file5.rtf file?

Yes the search results include the invalid\file5.rtf file

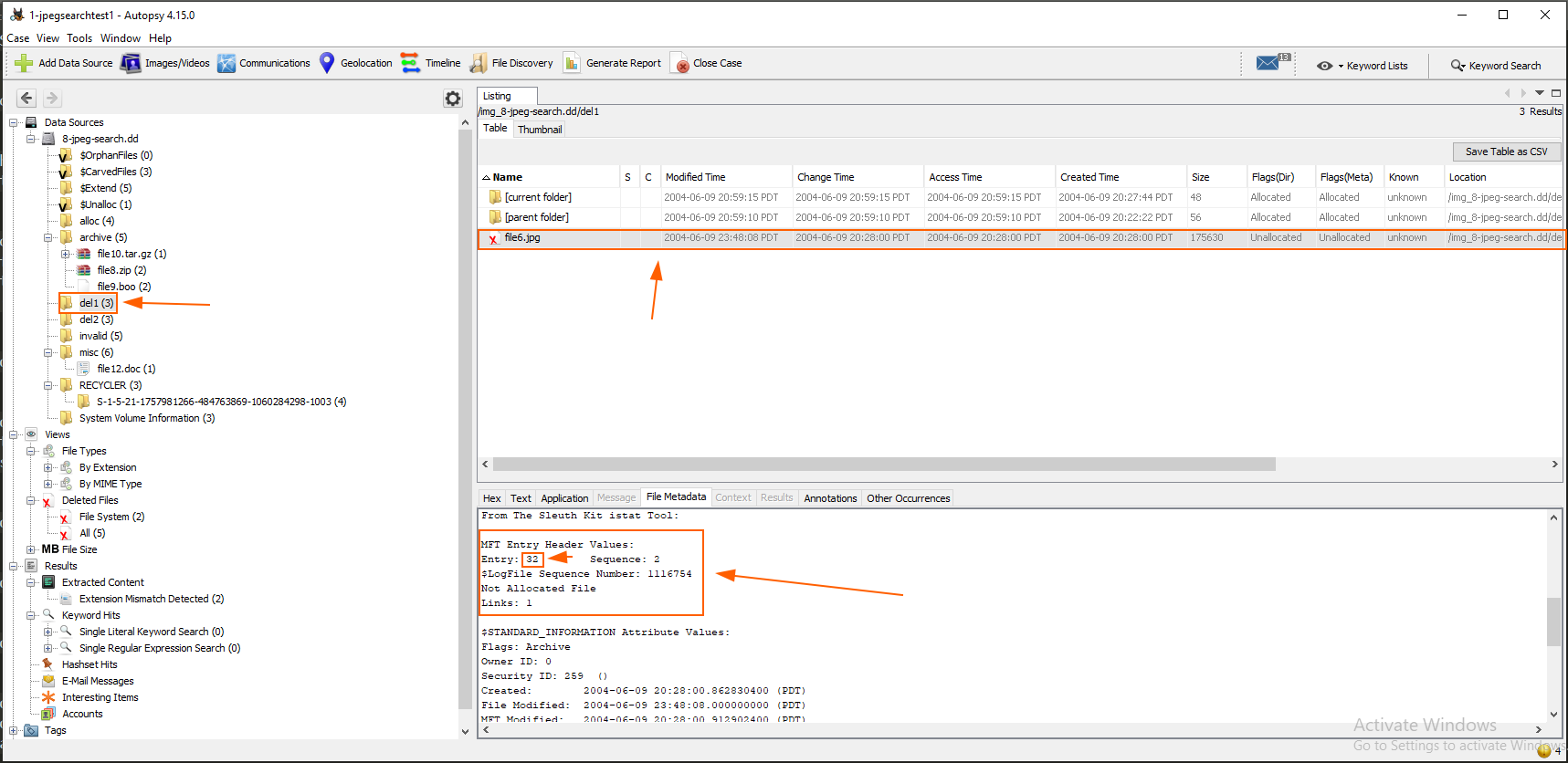


7. Did the search results include the deleted picture in MFT entry

#32 (del1/file6.jpg)? If not, then is it documented that only

allocated JPEGs will be found?

Yes the search results included the deleted picture in MFT entry #32 del1/file6.jpg



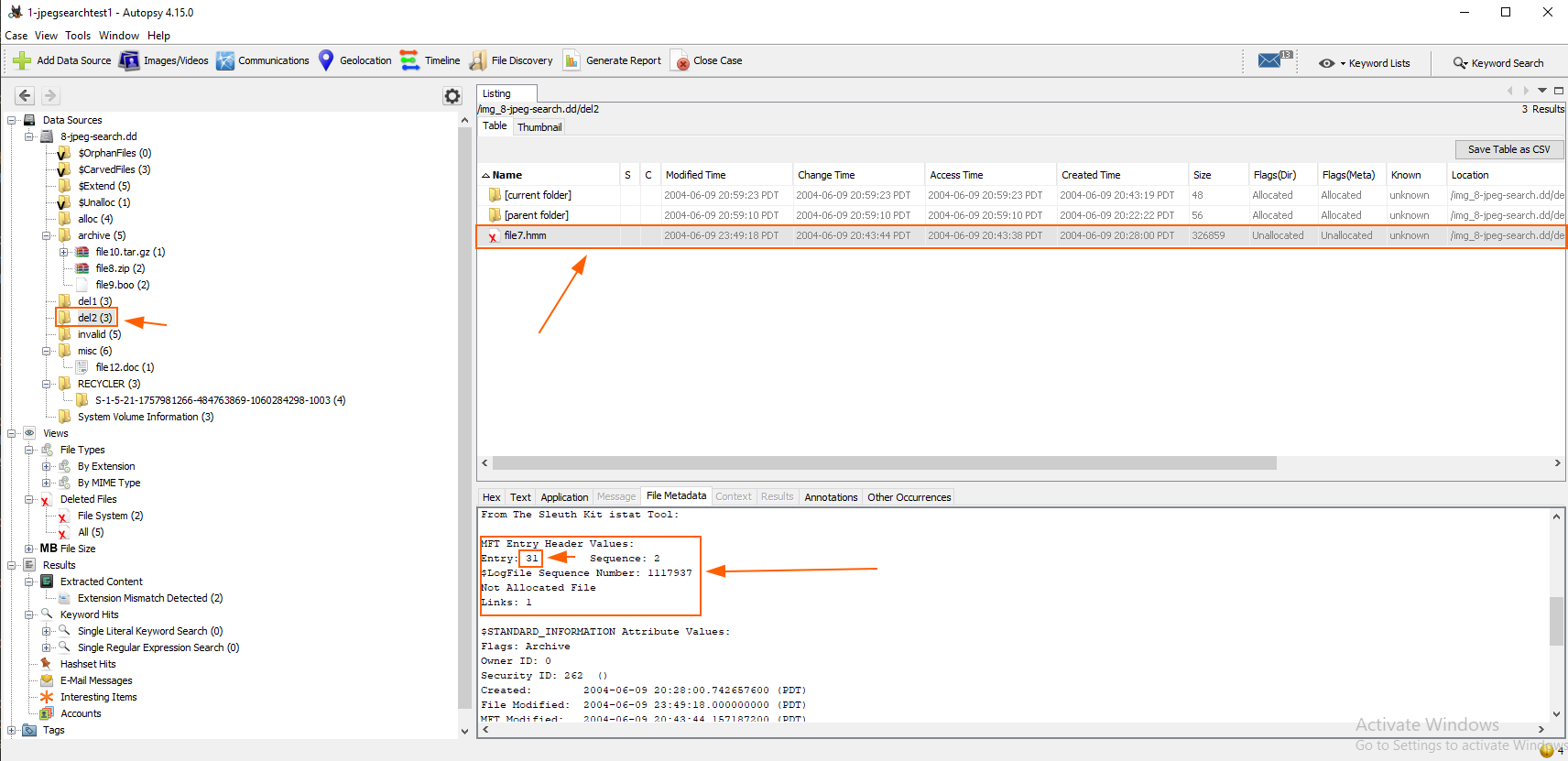
8. Did the search results include the deleted picture in MFT entry

#31 (del2/file7.hmm)? If this file was not found, but the file in

step #7 was found, then is it documented that only JPEGs with a

proper extension will be found?

Yes the search results included the deleted picture in MFT entry #31 del2/file7.hmm



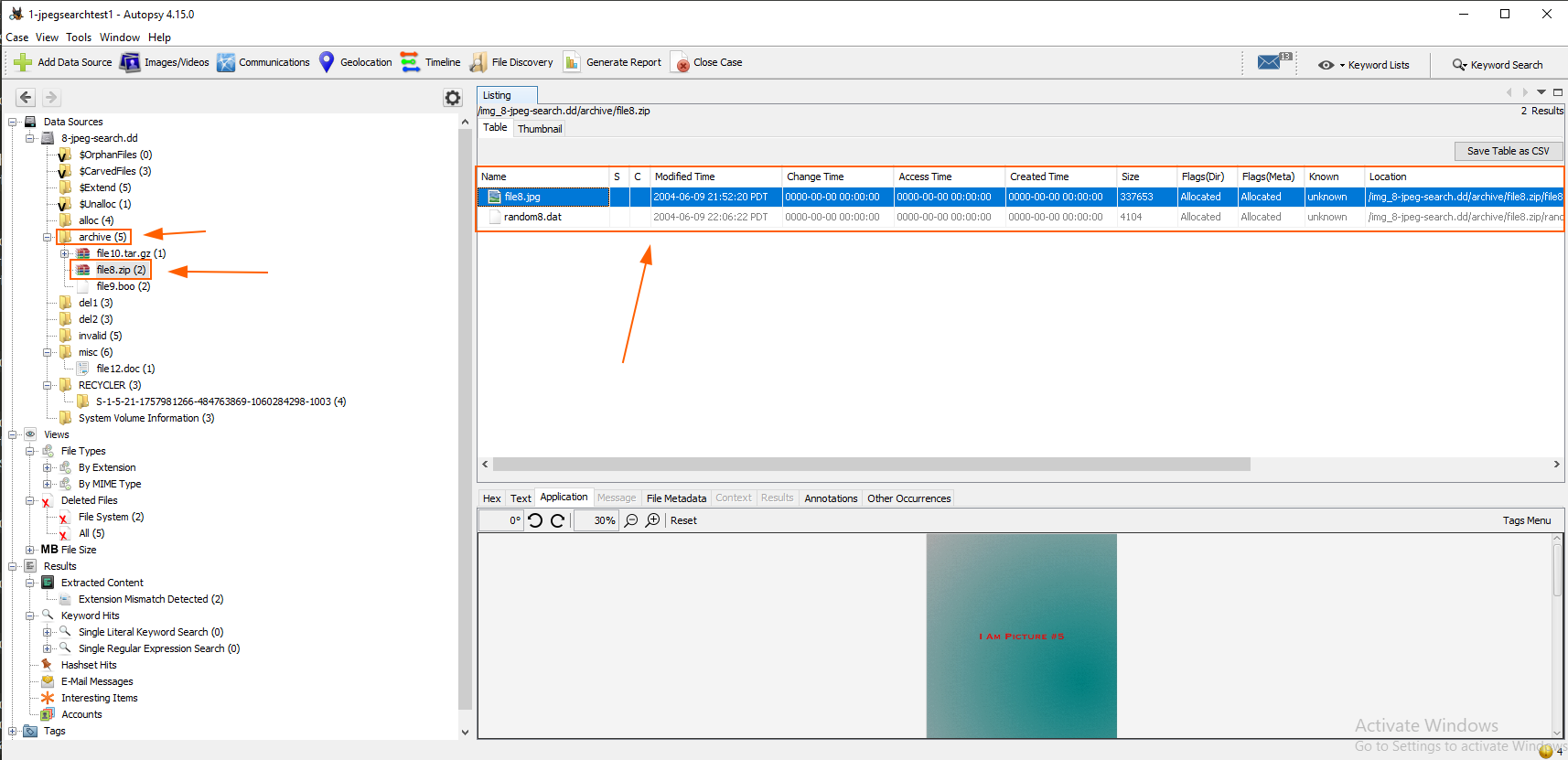
9. Did the search results include the picture inside of archive\file8.zip?

If not, then is it documented that JPEG files will be found and

that JPEG images that are embedded inside other file types will

not?

Yes the search results include the picture inside of archive\file8.zip



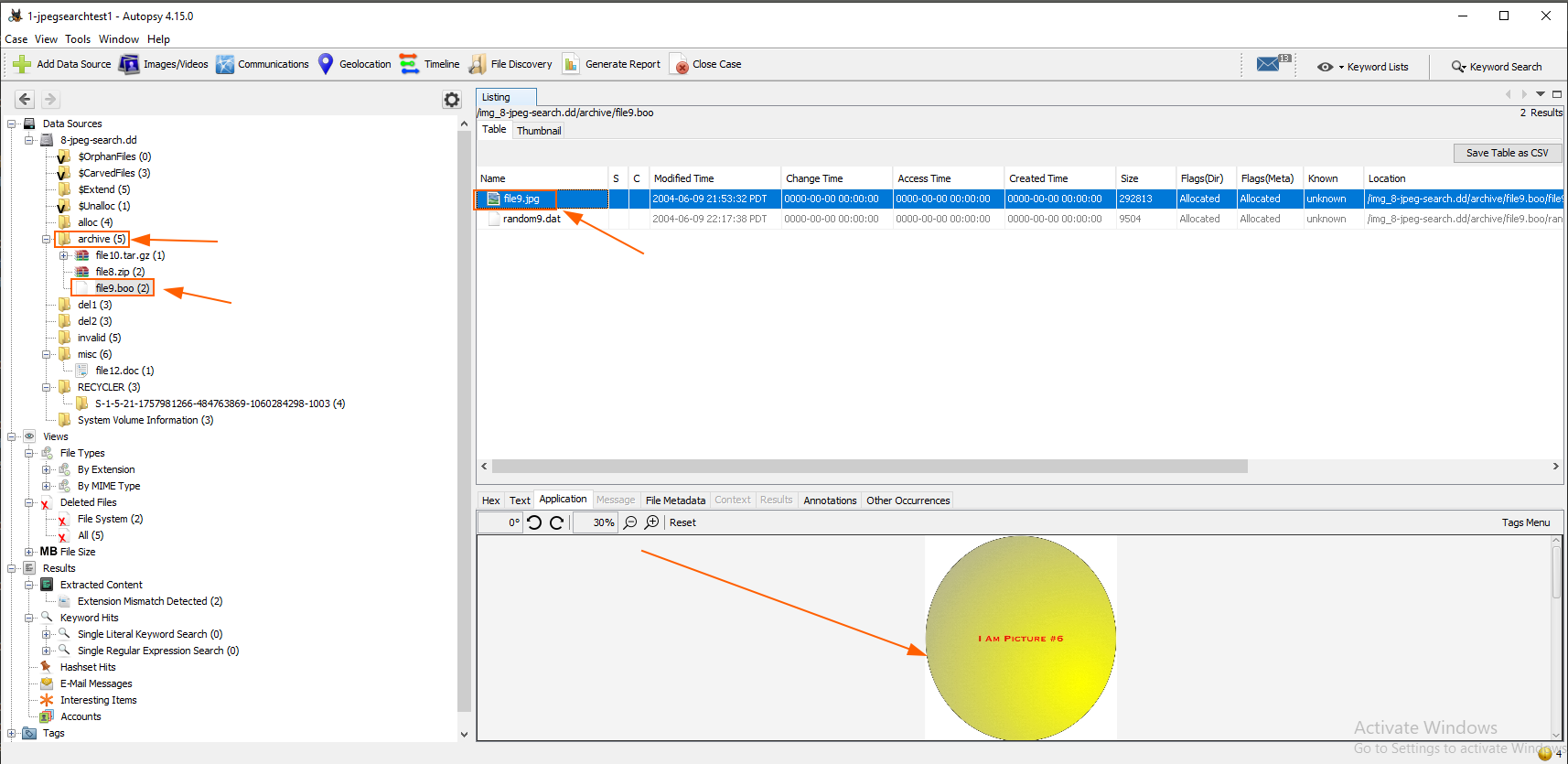
10. Did the search results include the picture inside of

archive\file9.boo? If not, then is it documented that JPEG files

will be found and that JPEG images that are embedded inside other

file types will not?

Yes the search results include the picture inside of archive\file9.boo



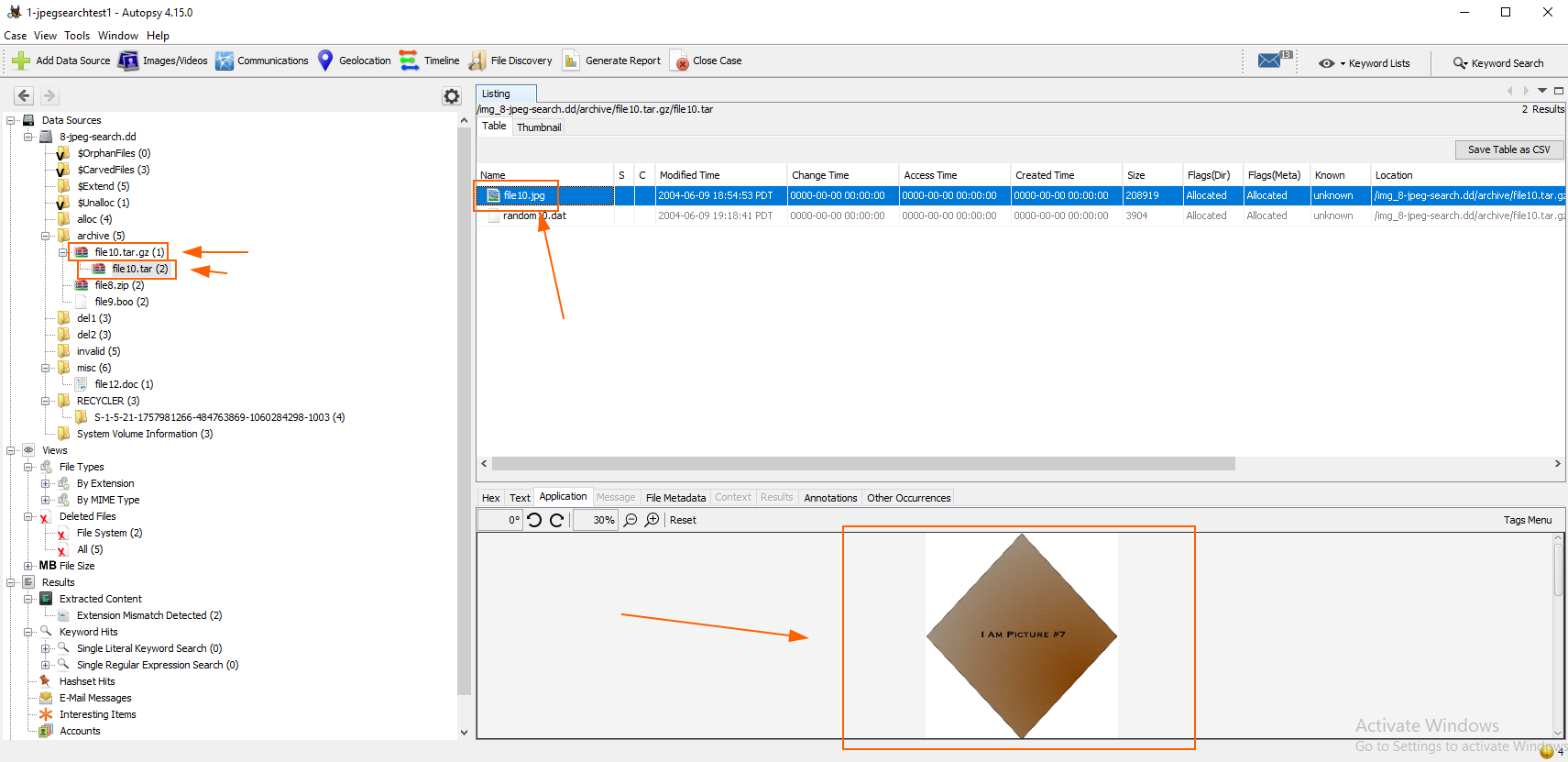
11. Did the search results include the picture inside of

archive\file10.tar.gz? If not, then is it documented that JPEG

files will be found and that JPEG images that are embedded inside

other file types will not?

Yes the search results include the picture inside of archive\file10.tar.gz?

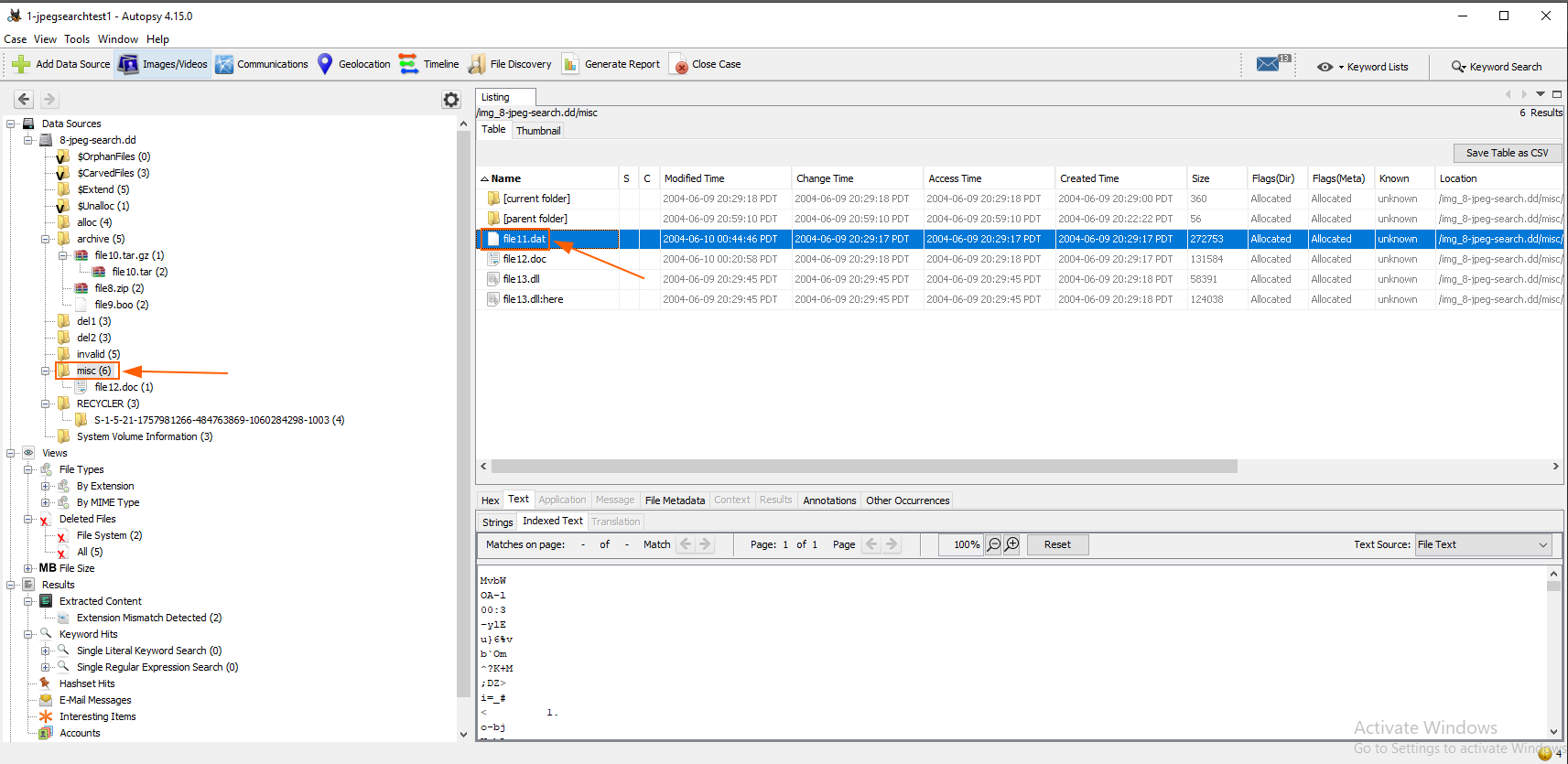


12. Did the search results include the misc\file11.dat file? If

not, then is it documented that JPEG files will be found and that

JPEG images that are embedded inside other file types will not?

Yes the search results include the misc\file11.dat file

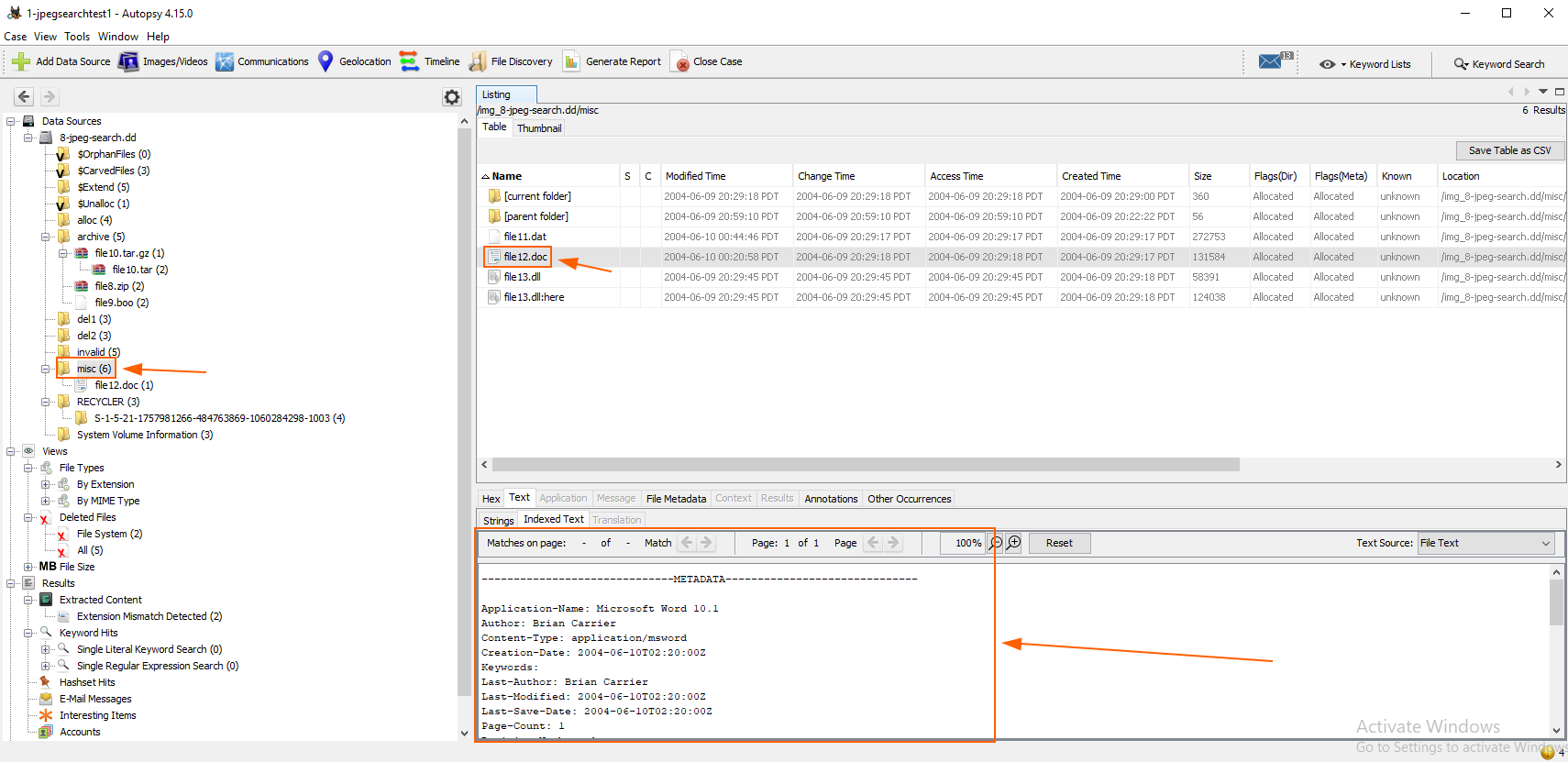


13. Did the search results include the misc\file12.doc file? If

not, then is it documented that JPEG files will be found and that

JPEG images that are embedded inside other file types will not?

Yes the search results include the misc\file12.doc file

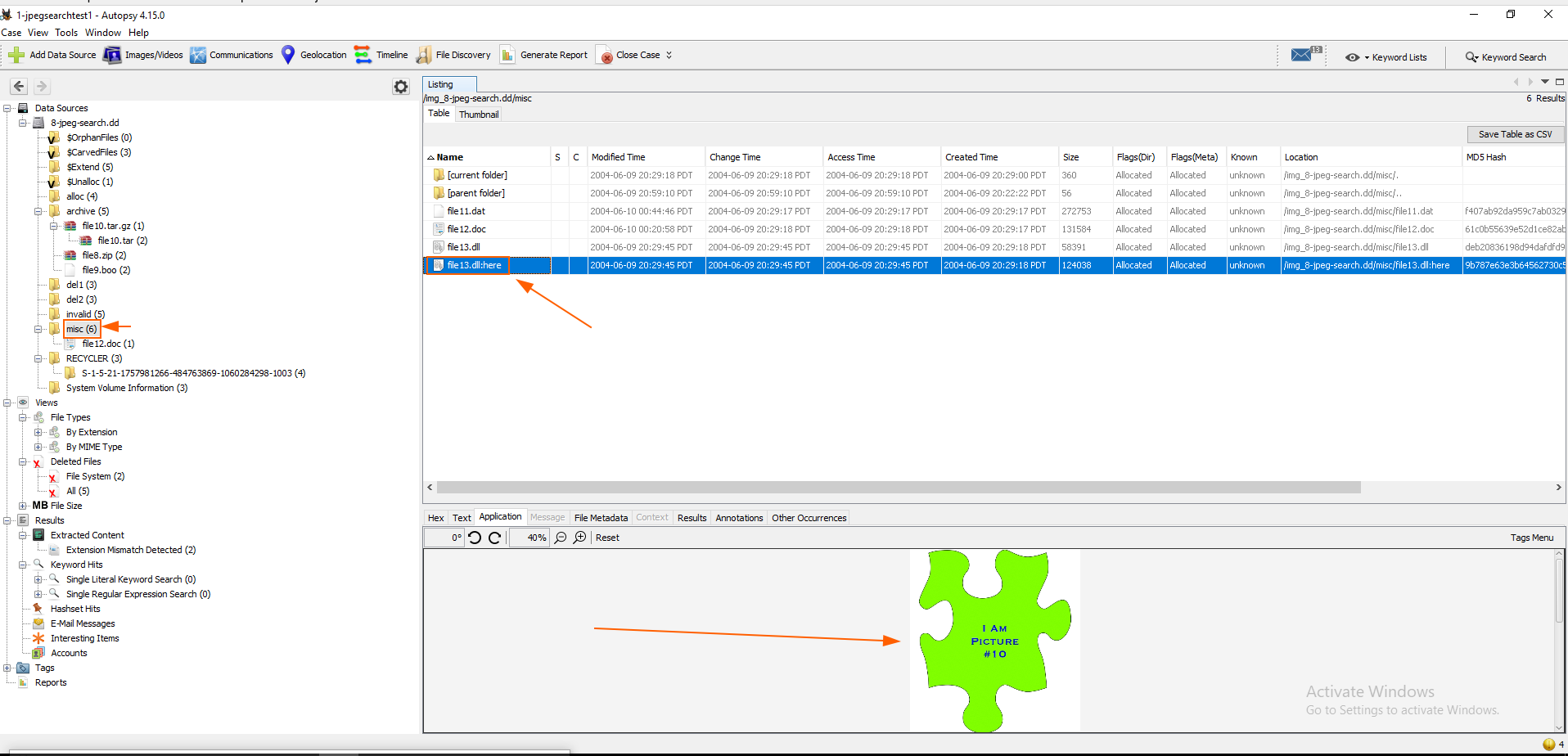


14. Did the search results include the misc\file13.dll:here picture?

If not, then is it documented that pictures in alternate data streams

will not be found?

Yes the search results include the misc\file13.dll:here picture



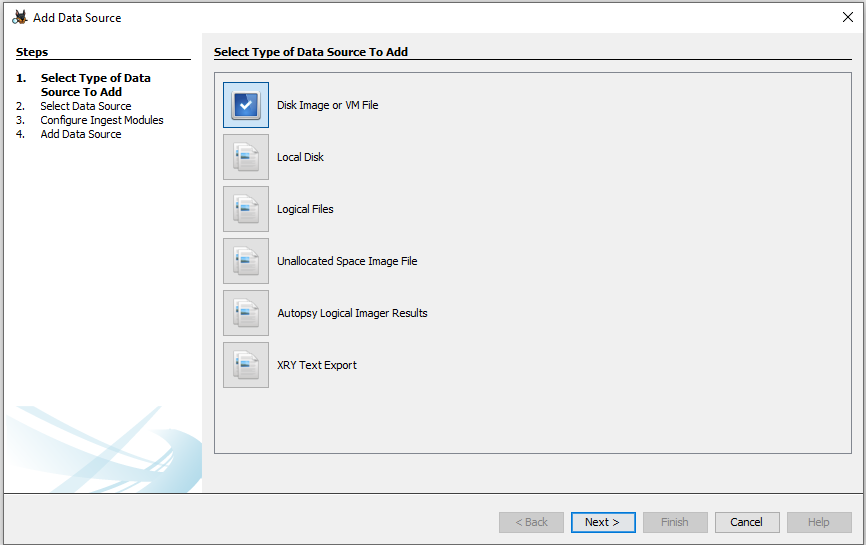
#### 10-ntfs-autodetect

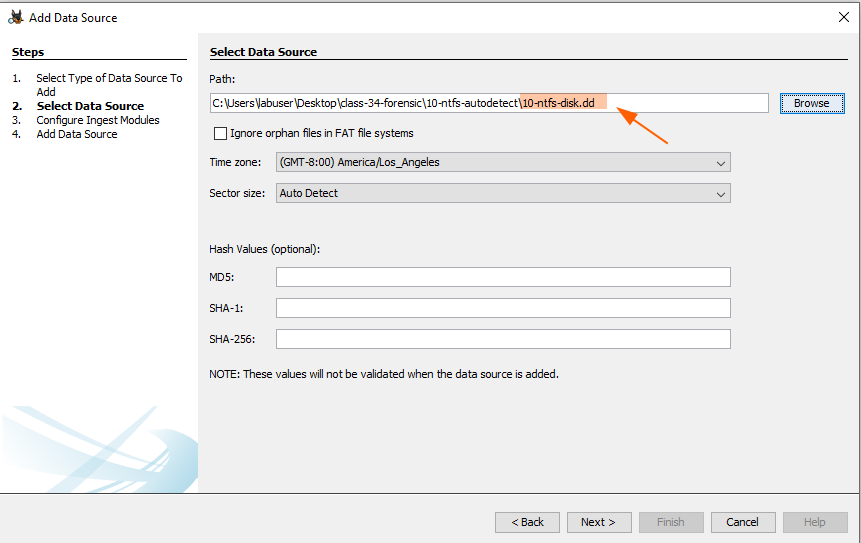
NTFS Autodetect Test #1

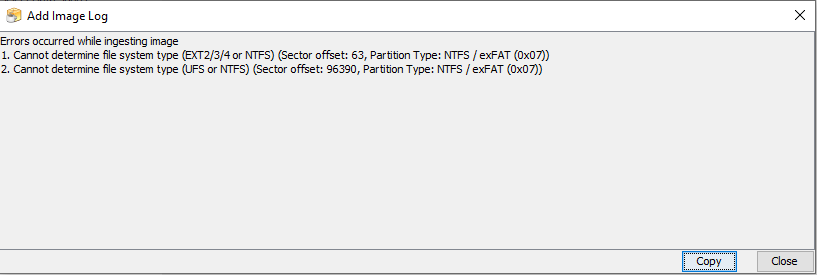
Tool: Autopsy

Version: 4.15.0

1. Import the 10-ntfs-disk.dd image into your analysis tool.





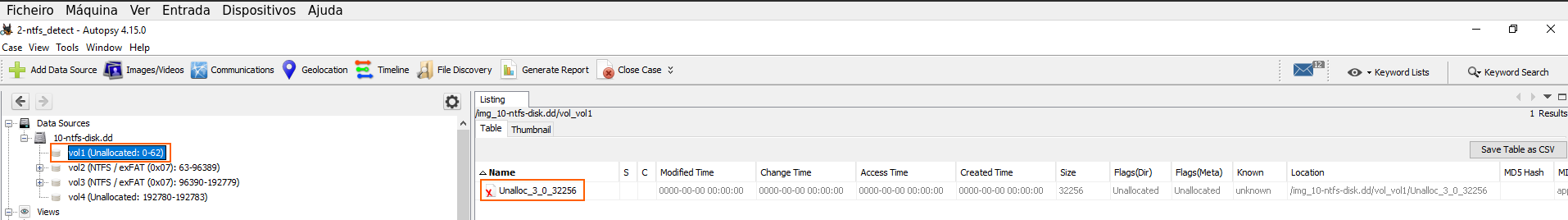


1a. Does the tool warn you that multiple file systems exist in the

first partition? If not, which file system is shown (you can easily

determine this based on the name of the file in the root directory)?

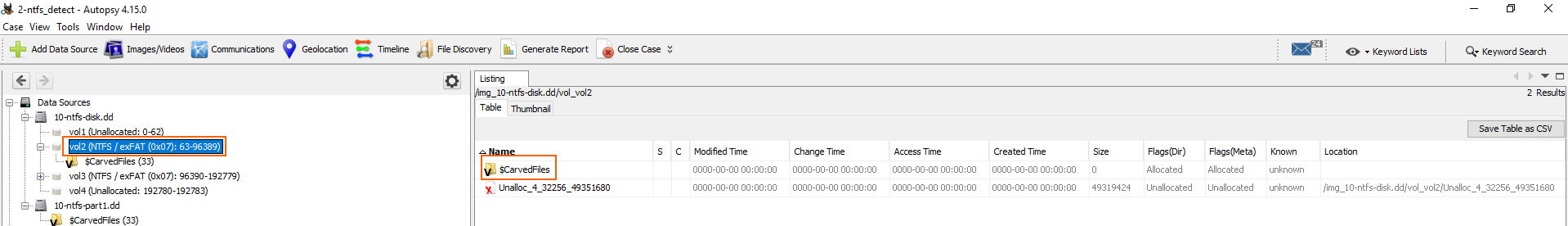
No it did not warn about multiple file systems existing in the first partition. the first file shown is **Unaloc\_3\_0\_32256**



1b. Does the tool warn you that multiple file systems exist in the

second partition? If not, which file system is shown?

Yes it warns me that multiple file systems exist in the second partition

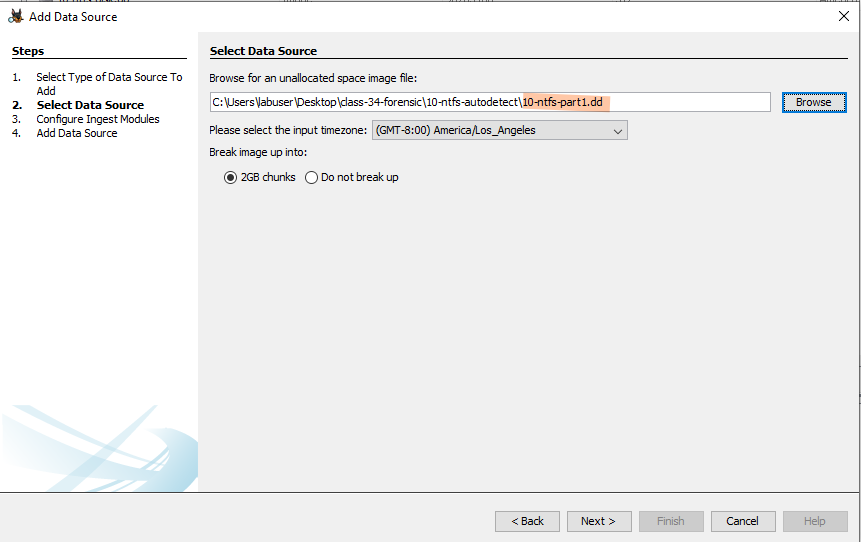


2. Import the 10-ntfs-part1.dd image into your analysis tool. Does

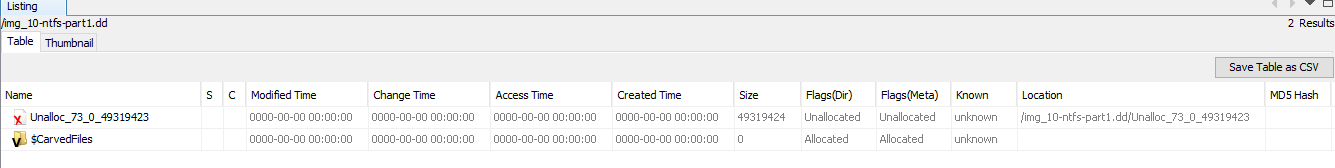
the tool warn you that multiple file systems exist in the partition?

If not, which file system is shown?

Yes the tool warns me that multiple file systems exist in the partition





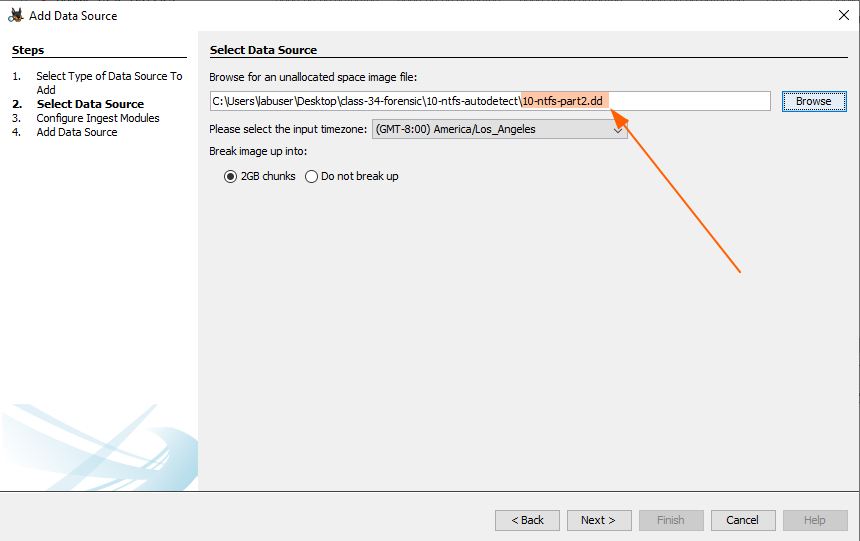


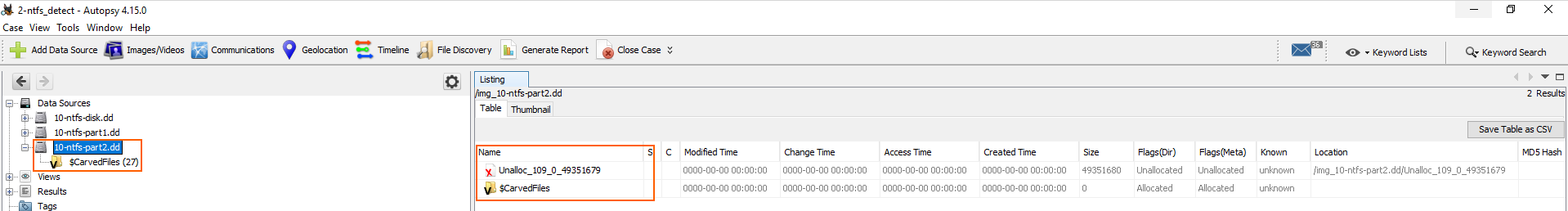
3. Import the 10-ntfs-part2.dd image into your analysis tool. Does

the tool warn you that multiple file systems exist in the partition?

If not, which file system is shown?

Yes the tool warns me that multiple file systems exist in the partition



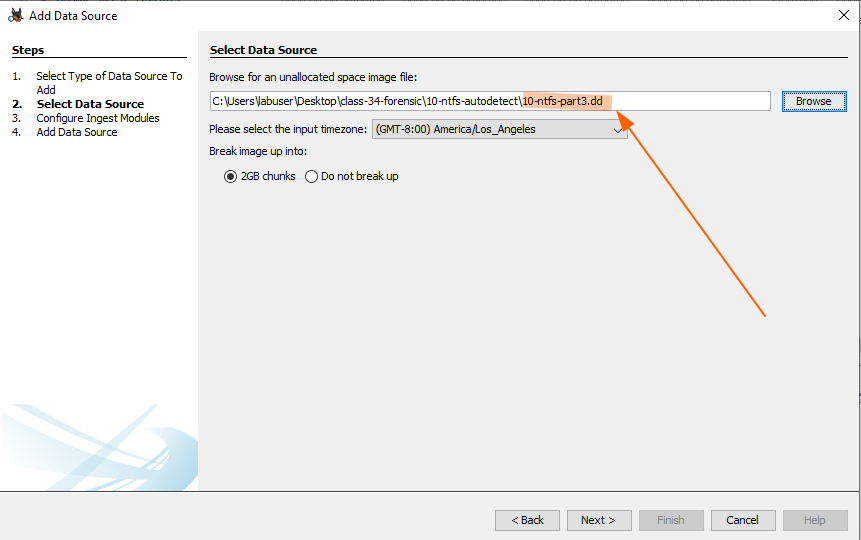


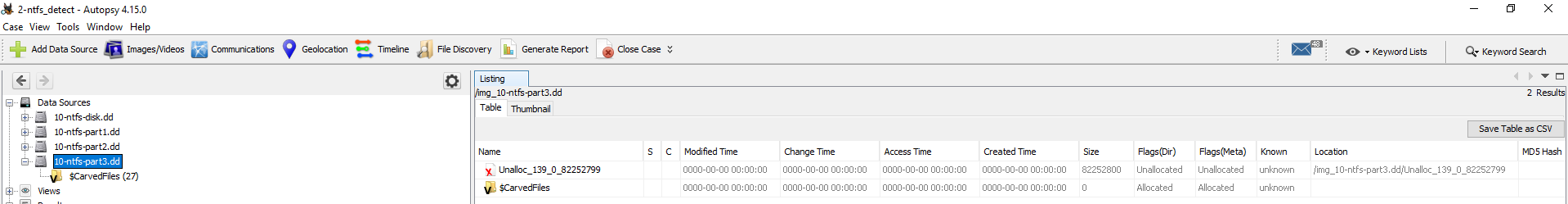
4. Import the 10-ntfs-part3.dd image into your analysis tool. Does

the tool warn you that multiple file systems exist in the partition?

If not, which file system is shown?

Yes the tool warns me that multiple file systems exist in the partition





#### 

#### 5-fat-daylight

This is a FAT test image for Daylight savings time. There are two

files on the image. The 'winter.txt' file was created at 2:00PM

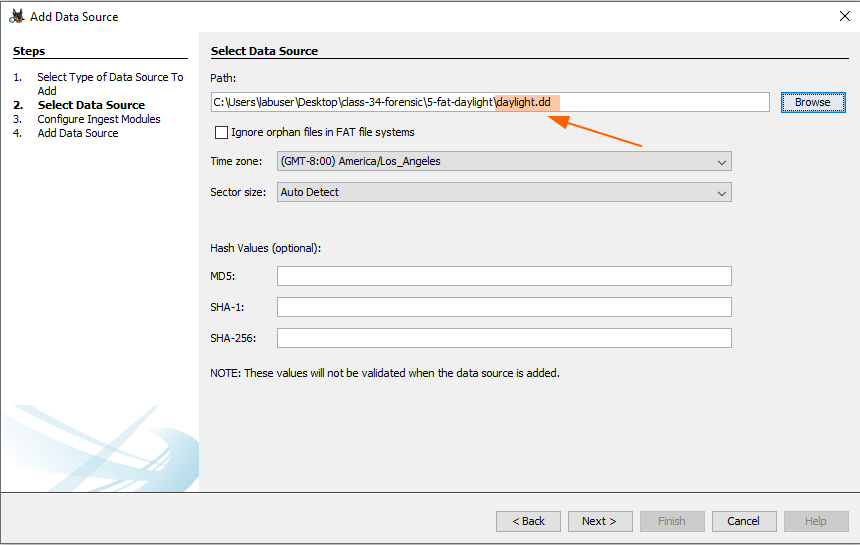
on January 1, 2004. The 'summer.txt' file was created at 3:00PM

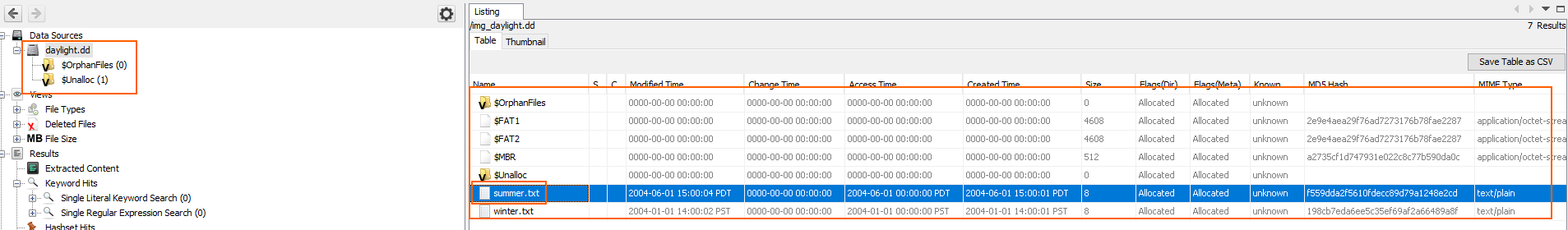
on June 1, 2004. The contents of each file contain the creation

time.

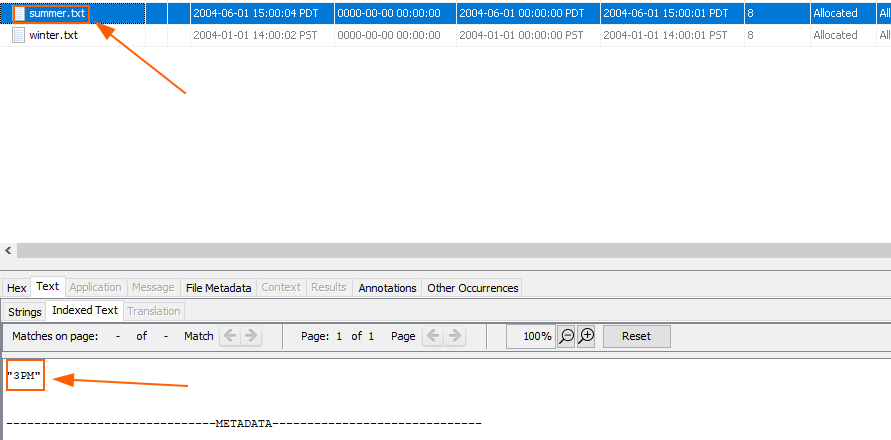
The files were created on a Windows XP system by setting the date

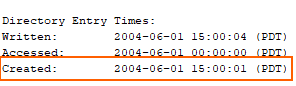
and then creating the file.

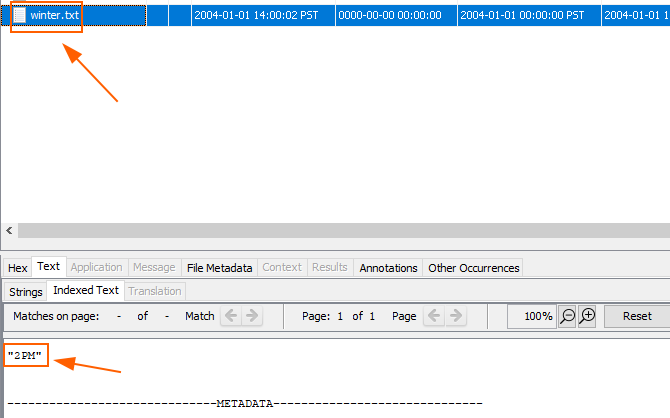


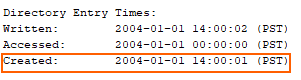












### 

### Part 3: Reporting

Answer these discussion prompts:

* How can Autopsy accelerate your ability to find important data on a hard disk image?
  + Autopsy can accelerate my ability to find important data on a hard disk image by organizing the files, showing metadata, keywords searching and more.
* Why might the Autopsy timeline view be relevant in an investigation?
  + To know the exact time and date a file was created or modified and to filter it
* How does Autopsy compare to manually searching a hard disk in something like Windows Explorer?
  + Autopsy makes it easier than windows explorer because it organizes the files in a certain manner like only showing files by extension or contents inside them while windows does something similar but more simplified