Introduction to AccessData Forensic Toolkit

Introduction

In this practical you will use the AccessData FTK ToolKit to examine a case

By the end of this lab you will be able to

- Use the basic functionalities within the FTK Toolkit environment

Task 1: Introduction to AccessData FTK ToolKit

Scenario:

Wes Mantooth was found to be in possession of fraudulent checks. When Mantooth was questioned he stated that he had obtained the checks from an associate of his. Mantooth refused to give any further details to the people questioning him about his accomplice or accomplices were. When asked how Mantooth created the checks he said: "With a computer, you figure the rest out". Since Mantooth was living in Phoenix, his computer may be set to Mountain Time.

Create a new case by using the Mantooth.E01 image and answer the following questions

Gather basic information about the Image

1. Verify the image first; Tools Verify Image Integrity what is the result from the verification process?

2. What is the MD5 hash of the Mantooth image?

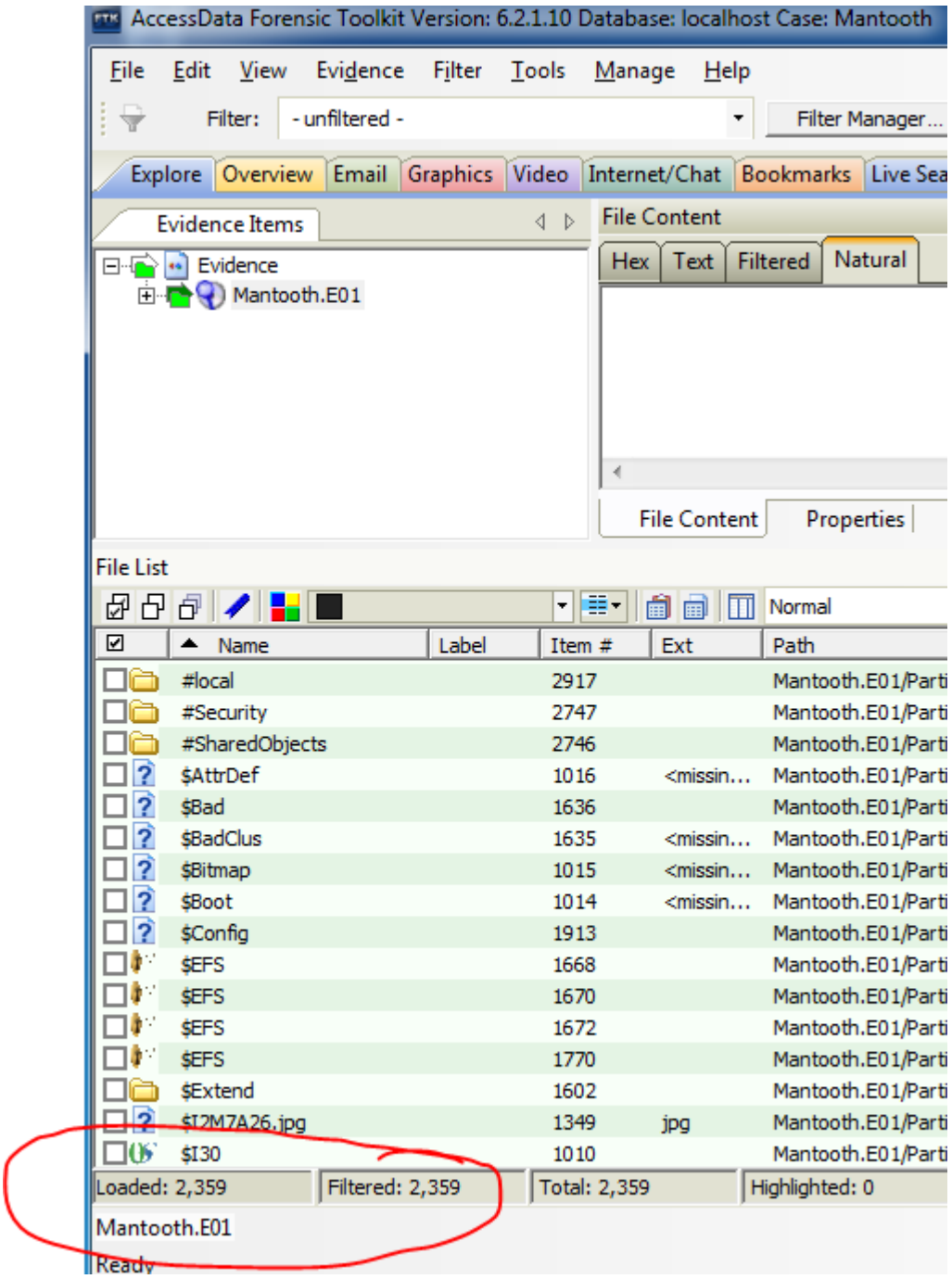
31217210a1a69f272079a3bde3d9d8fc

3. What is the SHA1 hash of the Mantooth image?

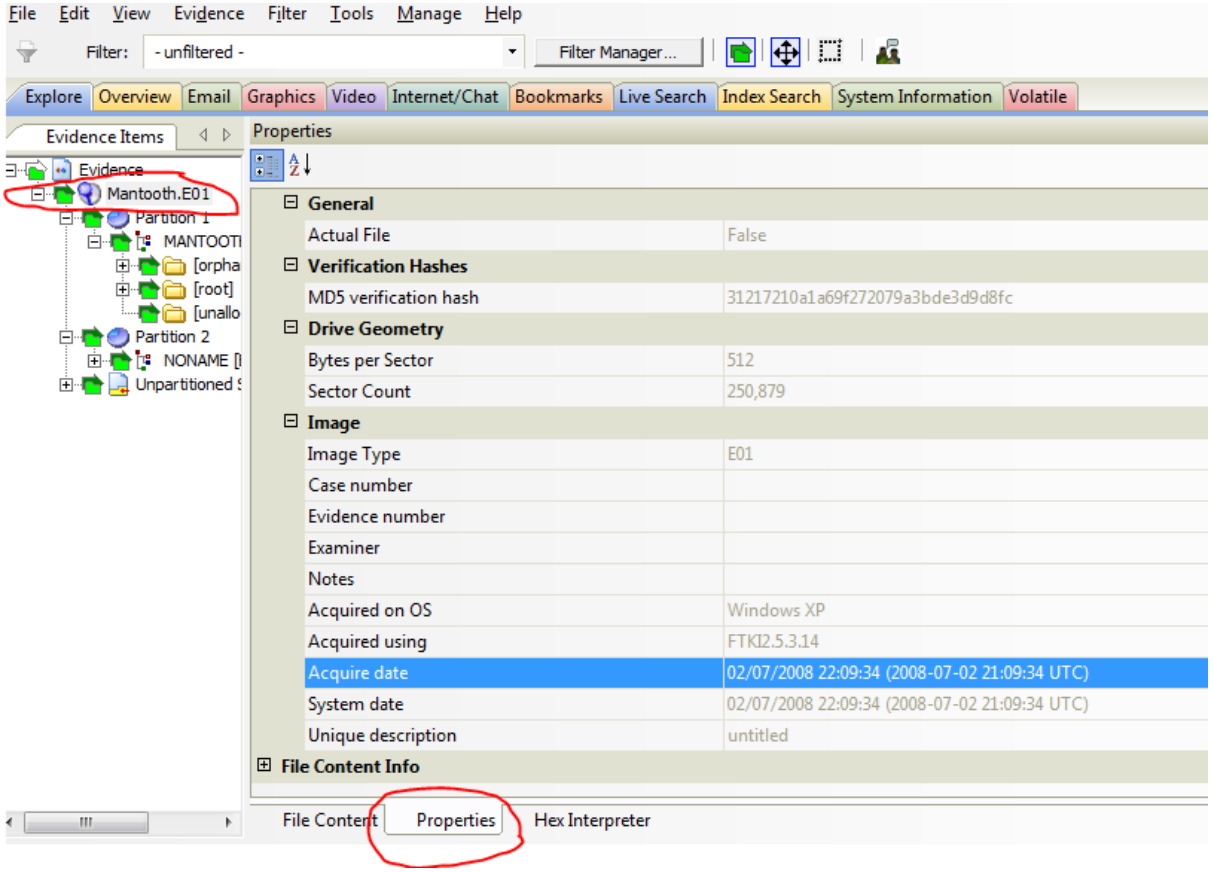
12e4ac047e328ca2bd63a4d65df25b3ecba55769

4. How many evidence items (i.e. the files and folders) are in the case?

2,359

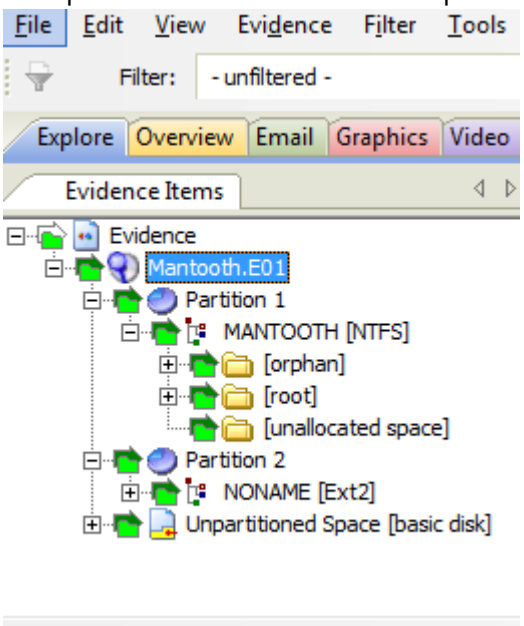


5. Find additional information regarding the image, including sector size, total sector count, acquisition date etc
    a. Sector size: 512 bytes
    b. Total sector count:250,879
    c. Acquisition time: 02/07/2008 22:09:34 (2008-07-02 21:09:34 UTC)



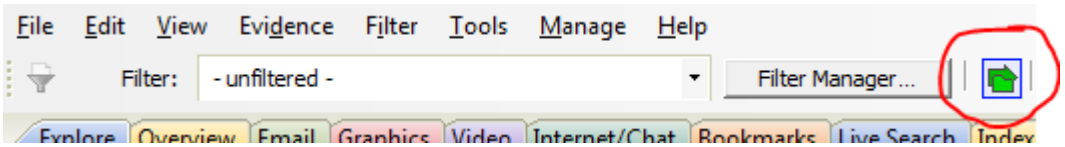
6. How many partitions are on the evidence image and what are they?

Two partitions – one is an NTFS partition and the other one is an EXT2 partition

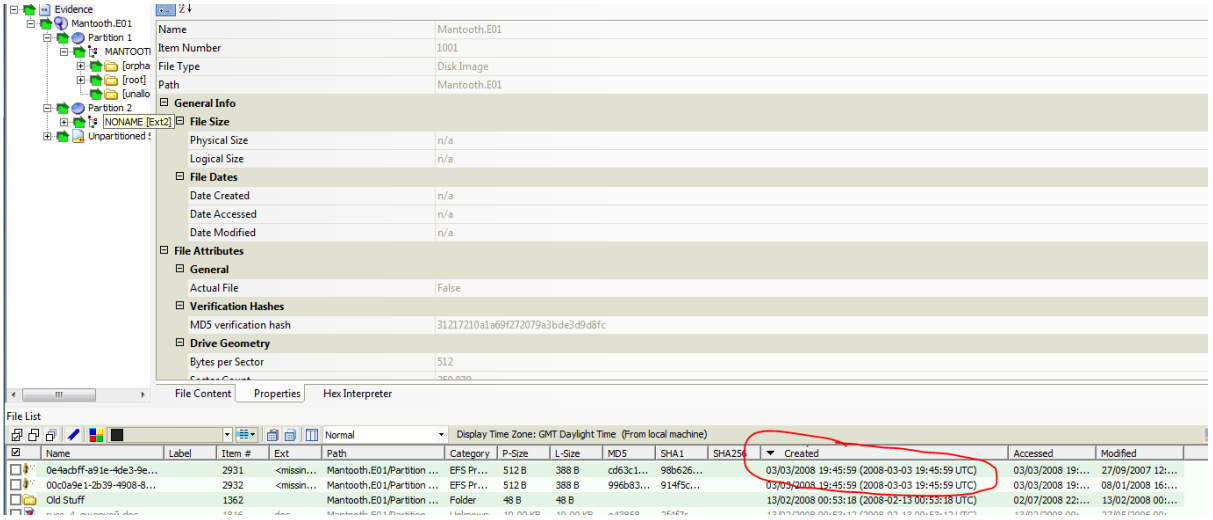


Changing Time Zone Settings

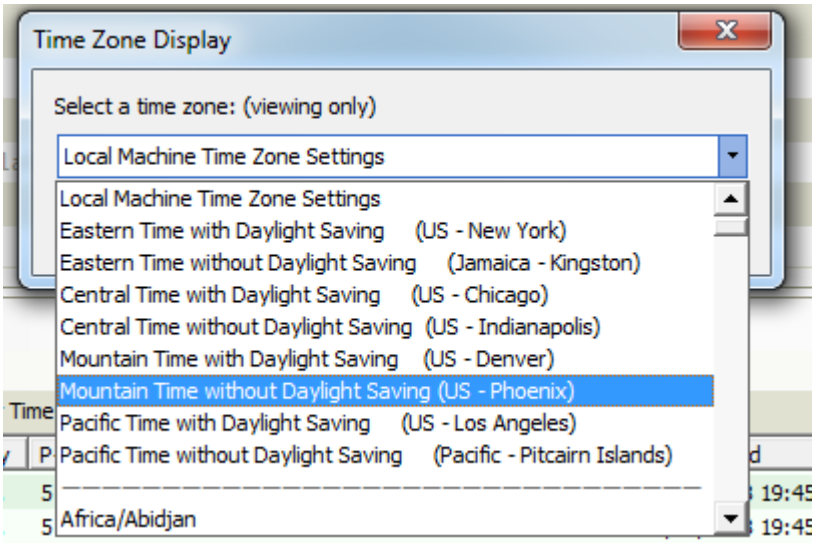
7. Click on the **Explore** tab, select **Evidence** at the top of the file list tree, click the **QuickPicks** (see the caption below) icon at the root of the evidence tree to list all of the files in the case



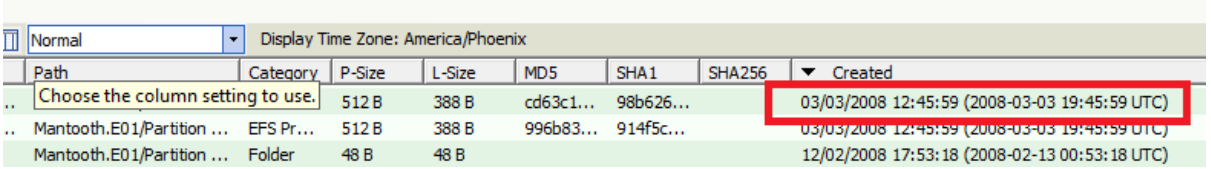
8. Click the column heading **Created** (twice) to sort by the created date; note down the date and time information



9. Click **View > Timezone Display**, then select the proper time zone for the given image



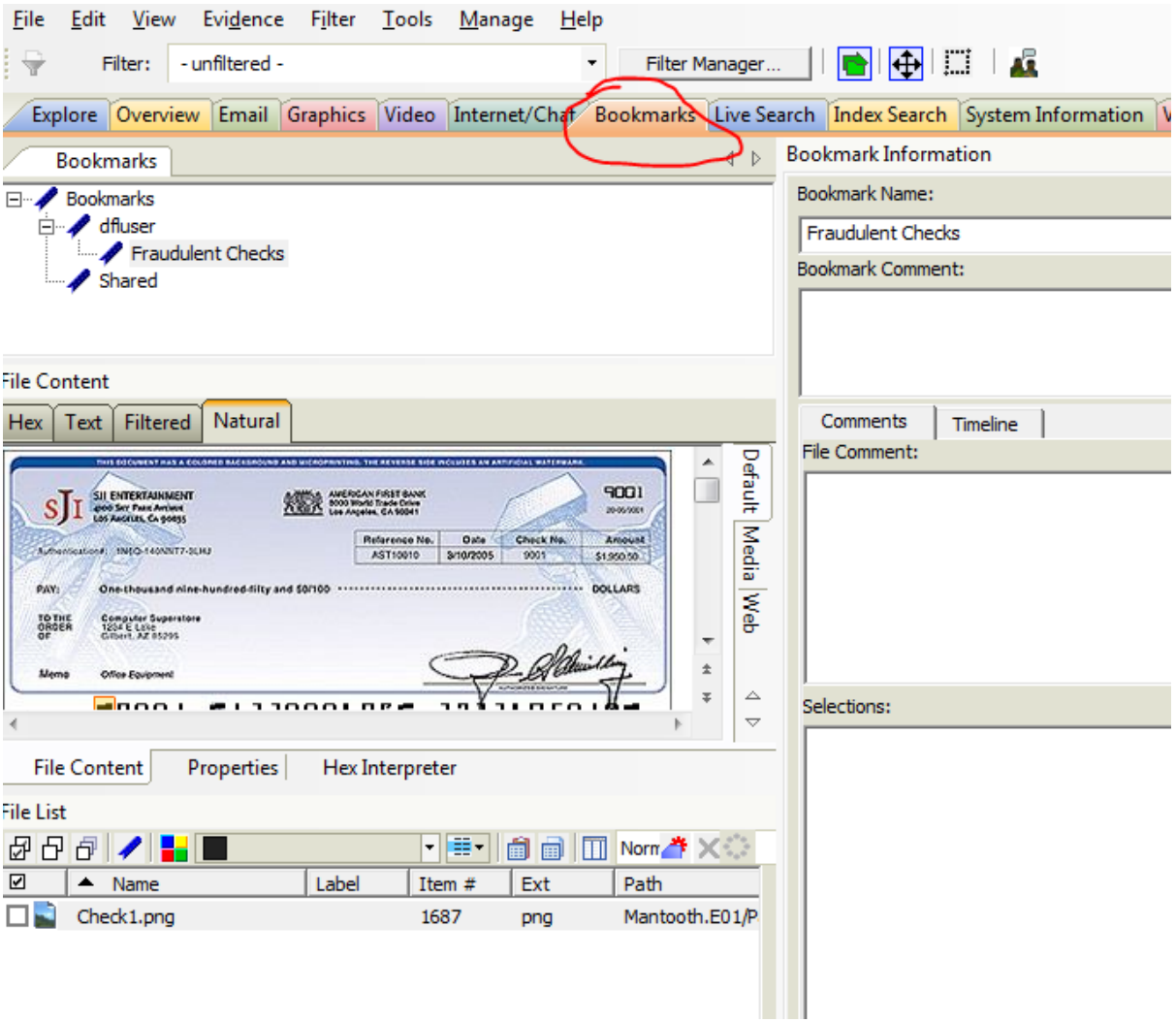
10. Repeat step 8 and ***discuss the difference***



Creation of a Basic Bookmark

11. Navigate to the "Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/Checks" folder; right click on the "Check1.png" file -> choose the option "Create Bookmark" -> Name the bookmark "Fraudulent Checks" -> click on the dfluser as a Bookmark parent -> click on "OK"

12. Click on the **Bookmarks** tab to check your newly created bookmark.

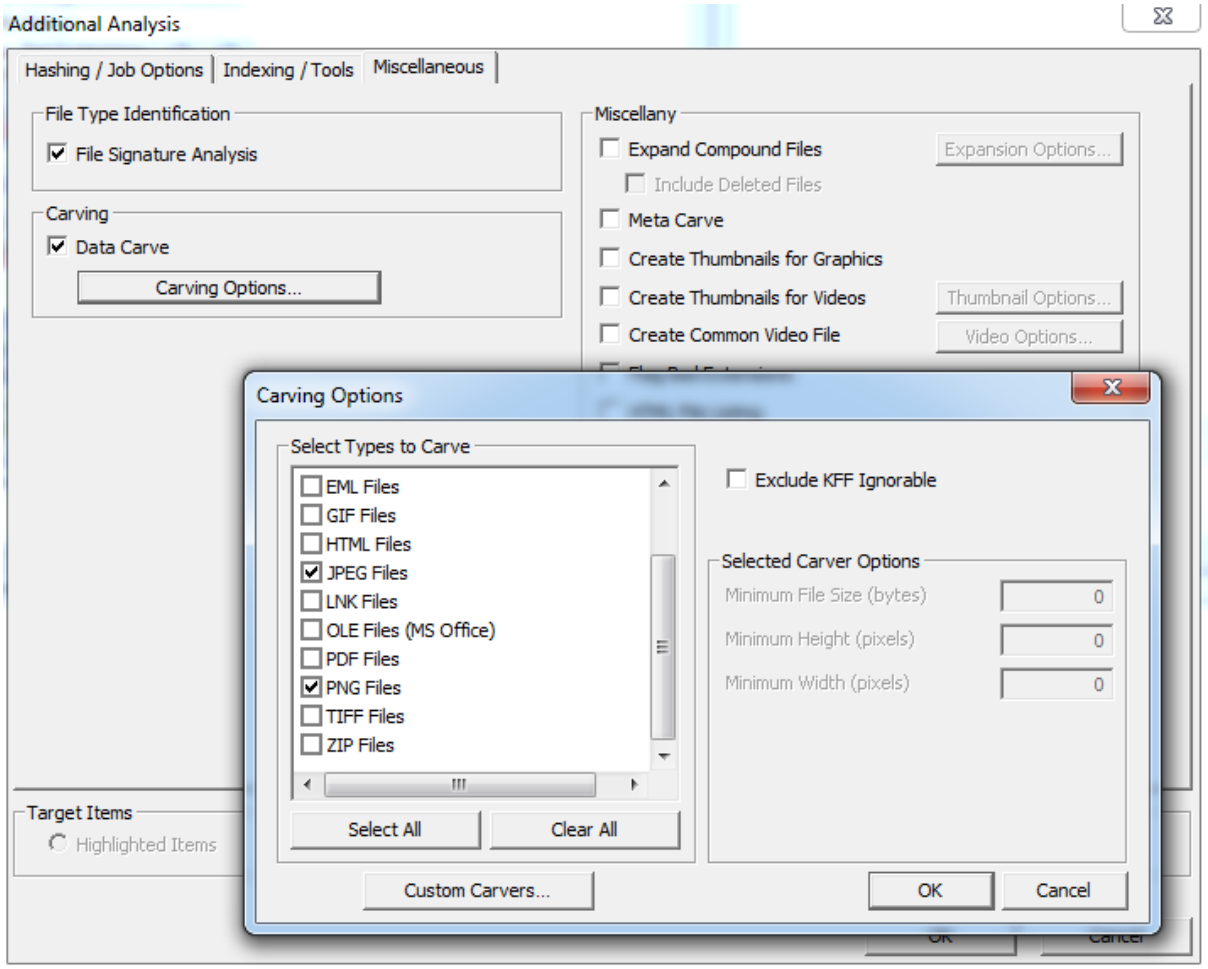


If possible, bookmark additional suspicious files/items within the case

Data carving

13. Click on the **Overview** tab -> **File Status** -> note down the number of data Carved Files [at this stage, the total number of data carved files is zero]

14. Go to **Evidence** -> **Additional Analysis**; within the new popup window click on the **Miscellaneous** tab, under the **Carving** section, tick the box for **Data Carve**; click on the Carving Options then choose JPEG files and PNG Files [additional questions: what happens when other file types are also selected? How do we know which file types should we select?], click OK twice.



15. Note down the total number of Data carved files; Click on the **Overview** tab -> **File Status** -> [90]

16. Check how many evidence items (i.e. the files and folders) are in the case now? Is it the same as the result from **step 4**? What is the difference? ***The difference is the 90 carved jpeg and png files.***

17. Find the "Carved [237152].jpeg", note down its path Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[unallocated space]/093637»Carved [237152].jpeg

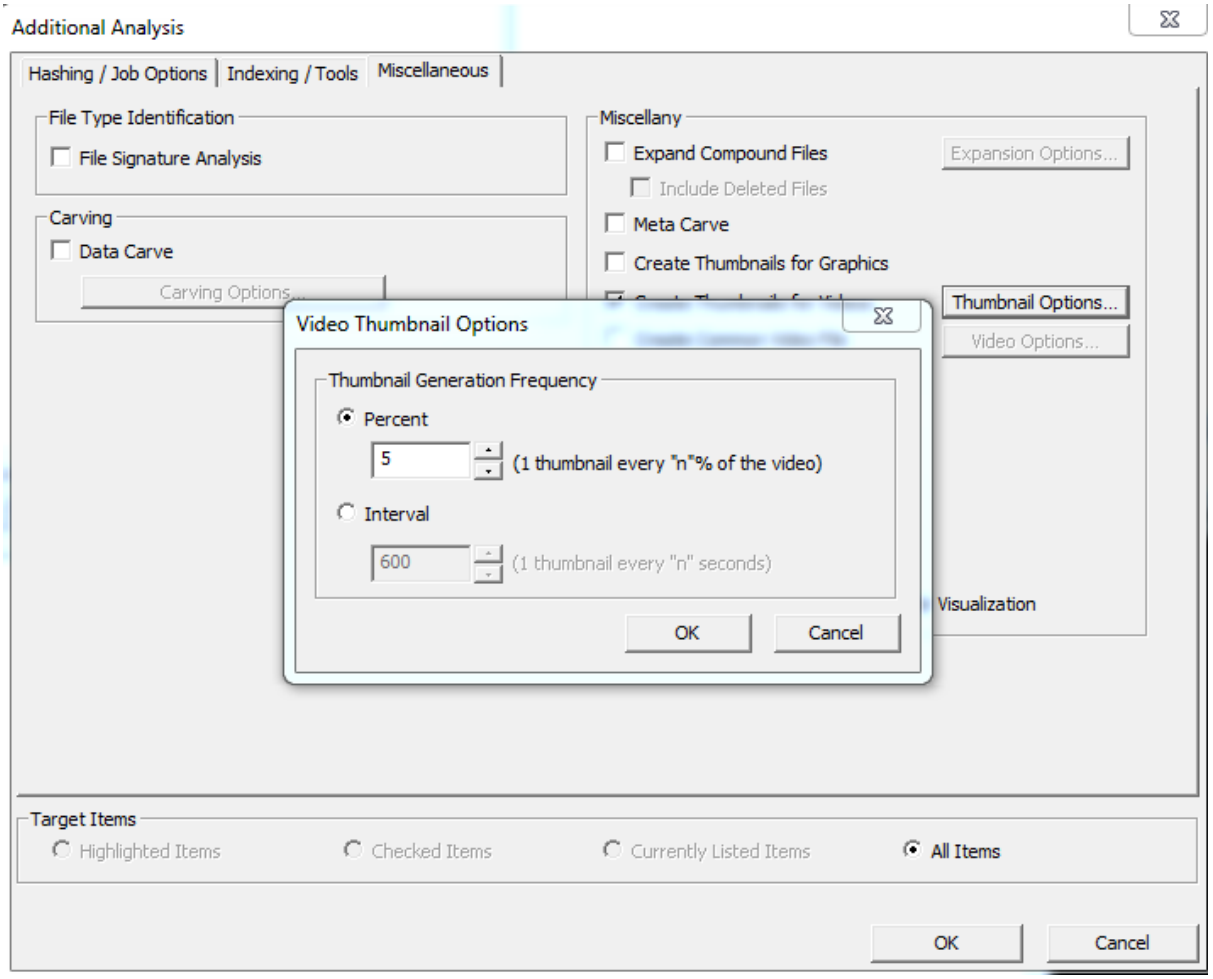
18. Find the "093637" file within Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[unallocated space] folder then go to the offset location "237152" note down the next two bytes in hexadecimal. What do the hex values represent?

Video Files

19. Click on the **Video** tab; note down the number of Multimedia files

20. Go to **Evidence** -> **Additional Analysis**; within the new popup window click on the **Miscellaneous** tab, under the **Miscellany** section, tick the box for **Create**

Thumbnails for Videos; click on the Thumbnail Options then select **percent**, click OK twice.[You can try the "Interval" option as well]



21. On the Video Tab, Open Multimedia->Video->MPEG 2.0 Video
22. Click on Happy.mpg in the File List window; note down the total number of thumbnail images created of the video; what is the 14th thumbnail showing?

The man standing up

23. Click on the play button, and see what happens.

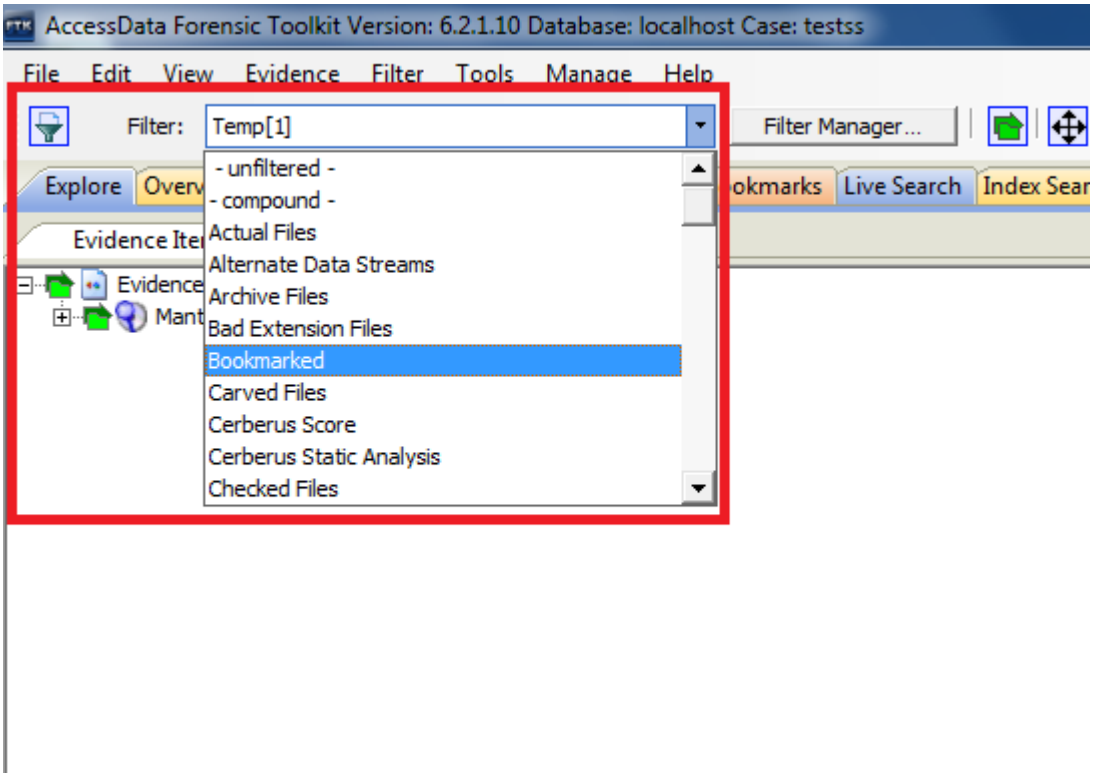
The video plays at spot of the thumbnail

24. Discuss the pros and cons of using video thumbnails for digital forensic investigations

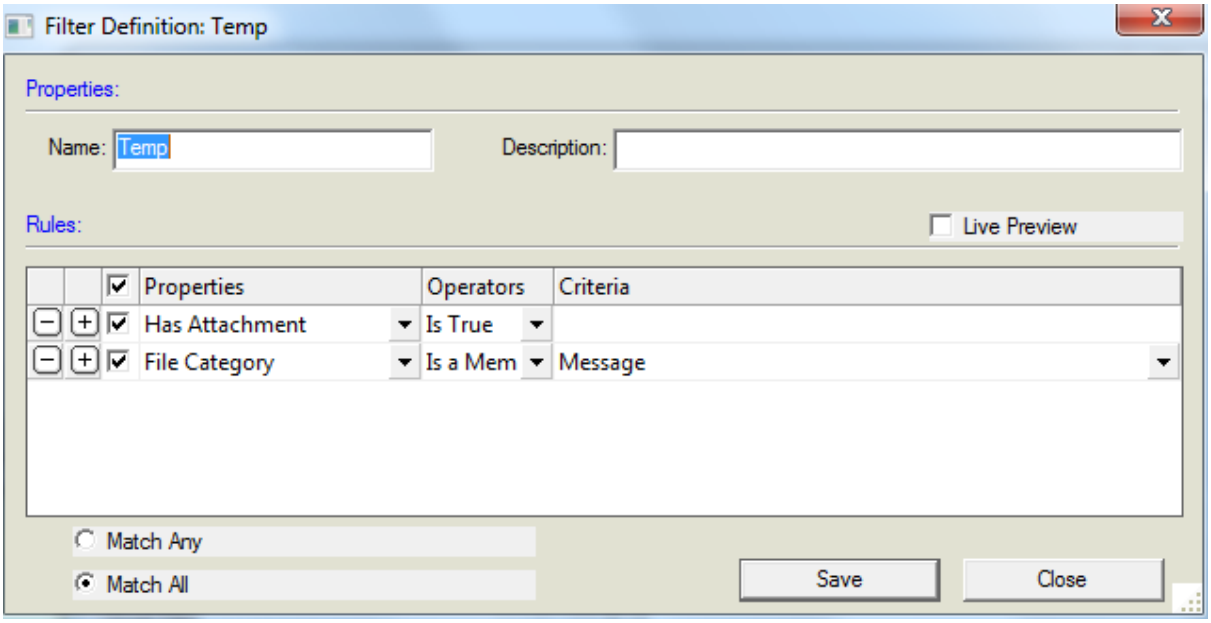
Pros: save investigator's time
Cons: if not configured properly, evidence could be overlooked

Filtering

25. Click on Filter -> New; in the pop up window, create a filter for email messages with attachments. Match all. Apply the filter by choosing it from the filter dropdown list as shown below How many email messages are listed?

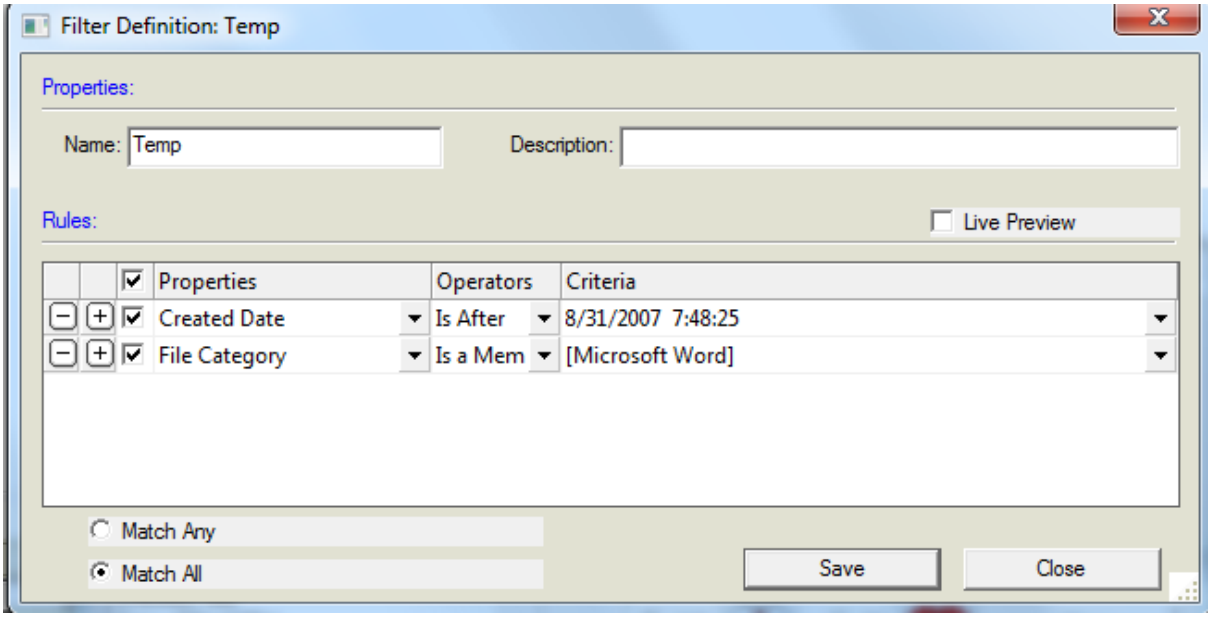


10



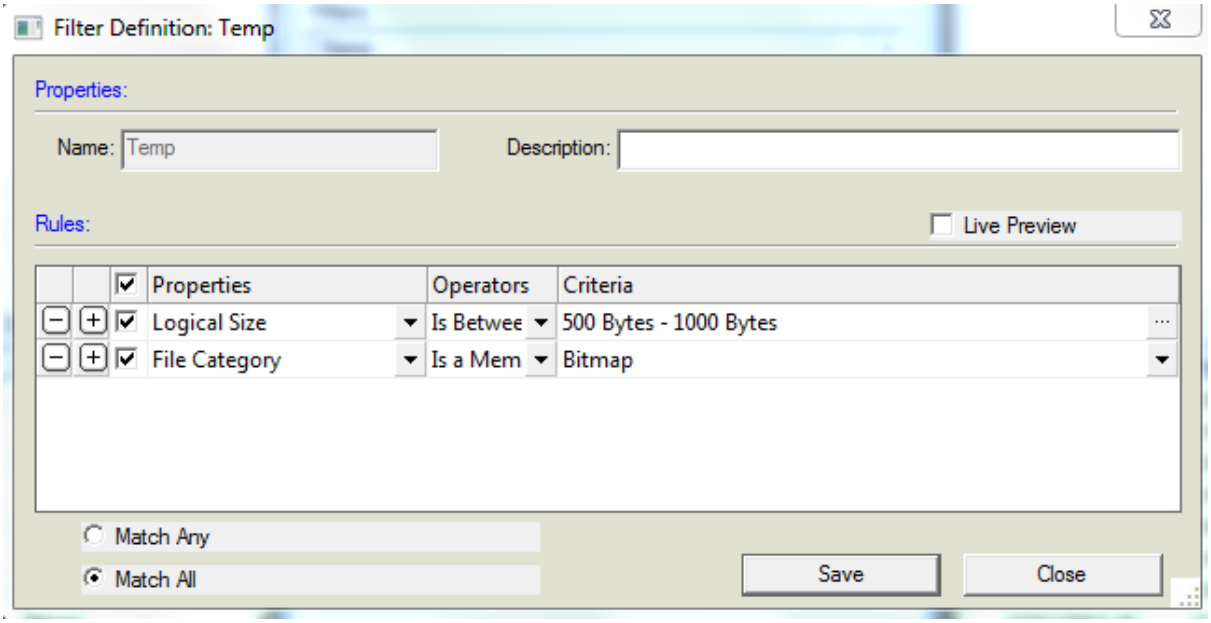
26. Click on Filter -> New; in the pop up window, create a filter for all Microsoft Word document created after August 30, 2007. Match all. How many word document are listed? [additional question, what happens when the date is changed to August 1, 2007]

8

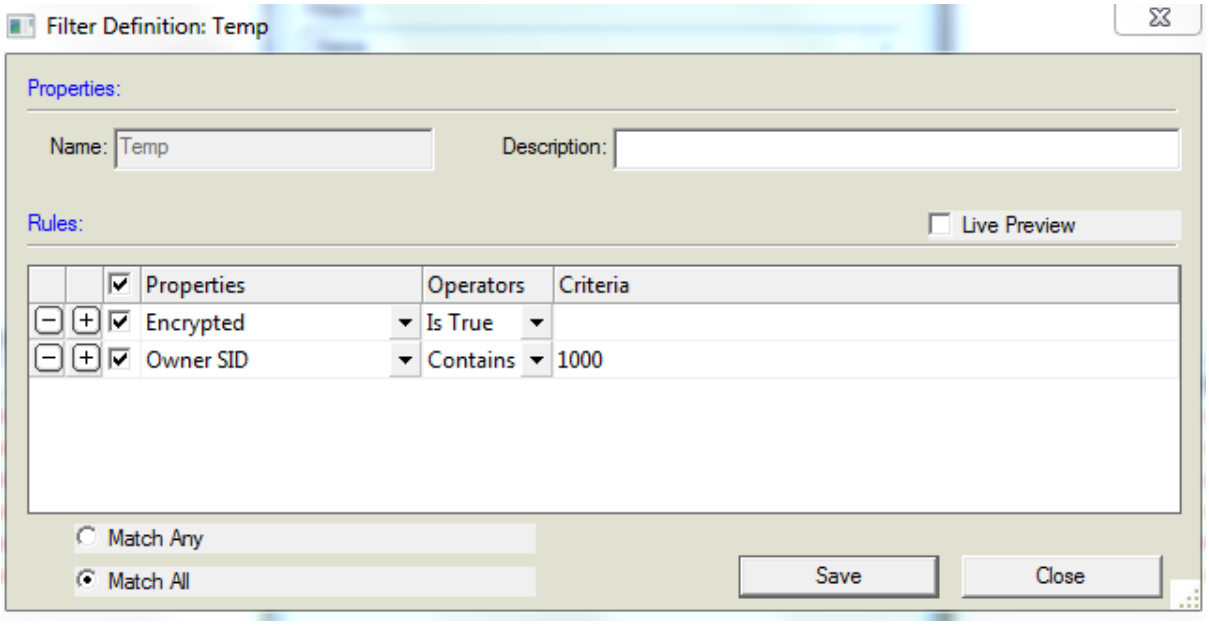


27. Click on filter -> New; in the pop up window, create a filter for all bitmap graphics with a file size of 500 to 1000 bytes. Match all. How many files are there?

21



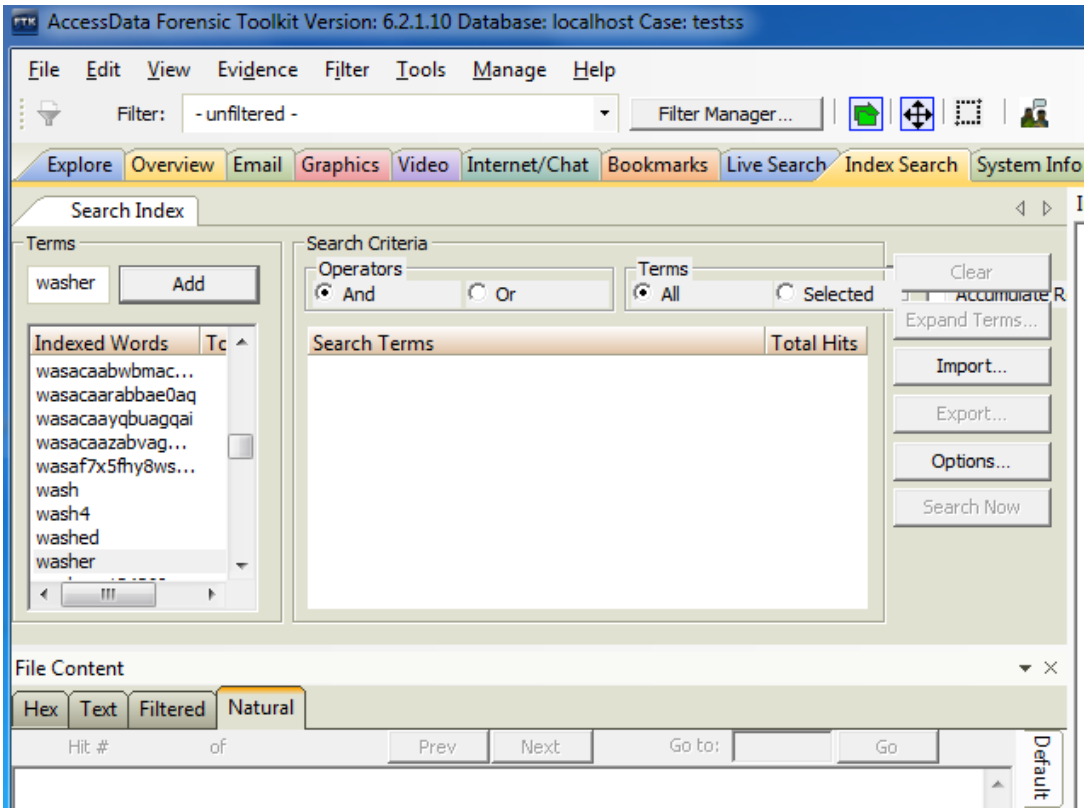
28. Click on filter -> new, in the pop up window, create a filter for all encrypted files for the user with a SID of 1000. Match all. How many files are there?



Searching

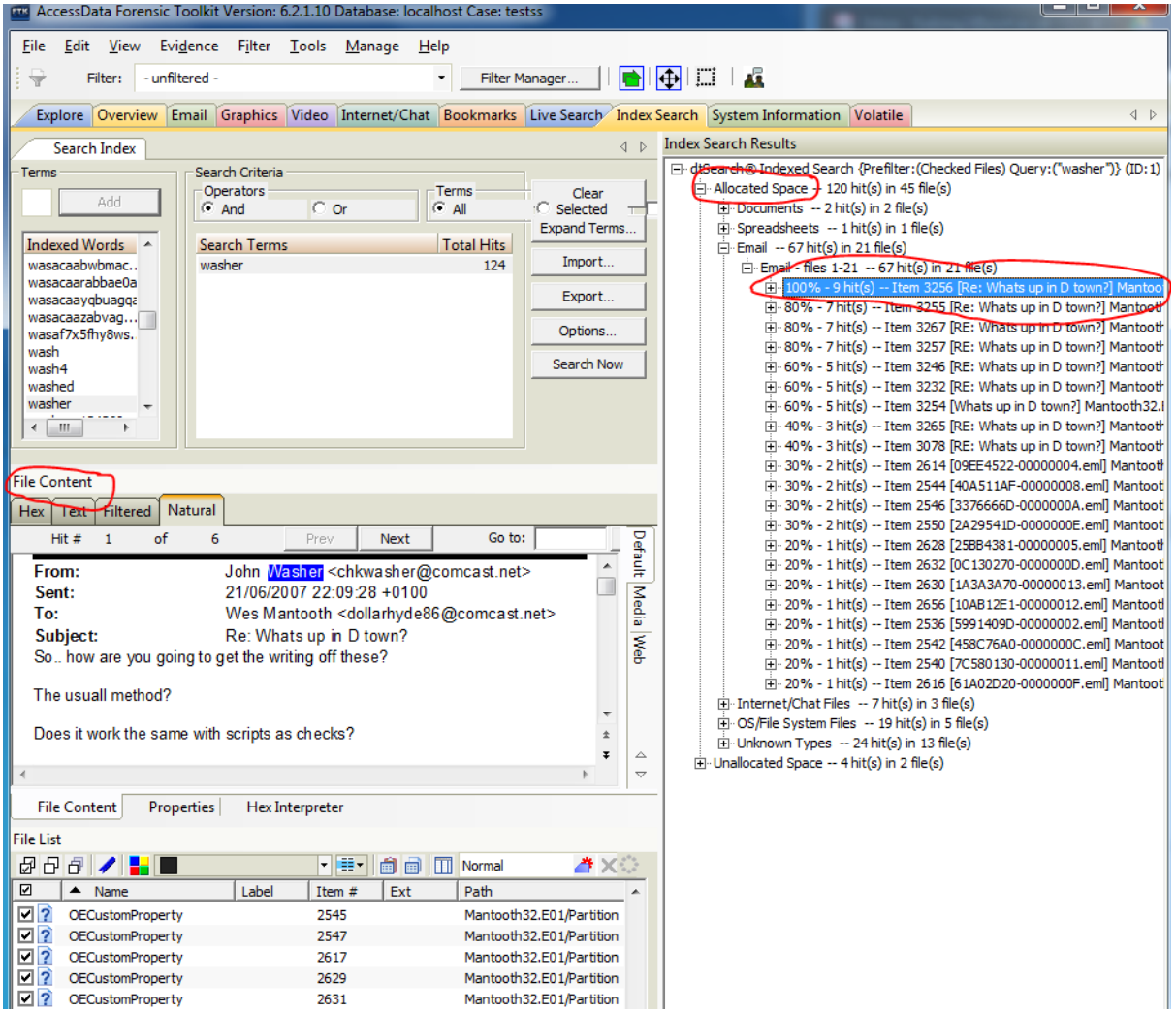
Index search

29. Start on the **Explore** tab; quick pic the Mantooth image; checkmark all Mantooth files by selecting the **double check icon** in the **file list**;
30. Click the **Index search** tab, in the Search Term box, type "**Washer**", then click add.



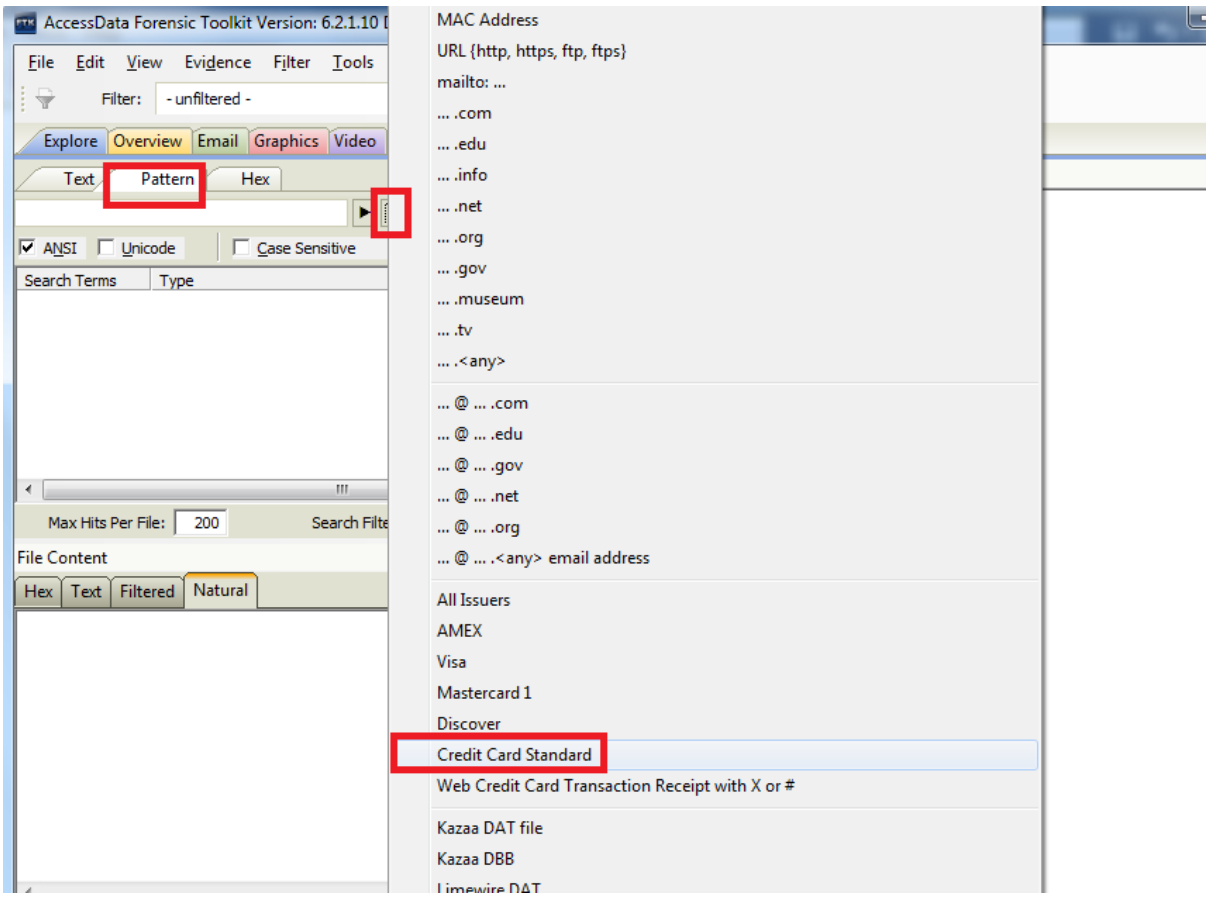
31. Note how the Indexed words list grows as you type the first string.
32. Click Search now.

33. In the Index Search filter option dialog, select **Checked Files**, then click OK. **[if the "included all files" option was selected, the result should be the same]**
34. In the Index Search Results window, expand the search results.
35. Note that the hits are divided into Allocated Space and Unallocated Space.
36. Expand the Allocated Space hits and the Email category.
37. Select the hits "[Re: Whats up in town]"
38. Select the first hit, then view the highlighted this in the **File Content** viewer

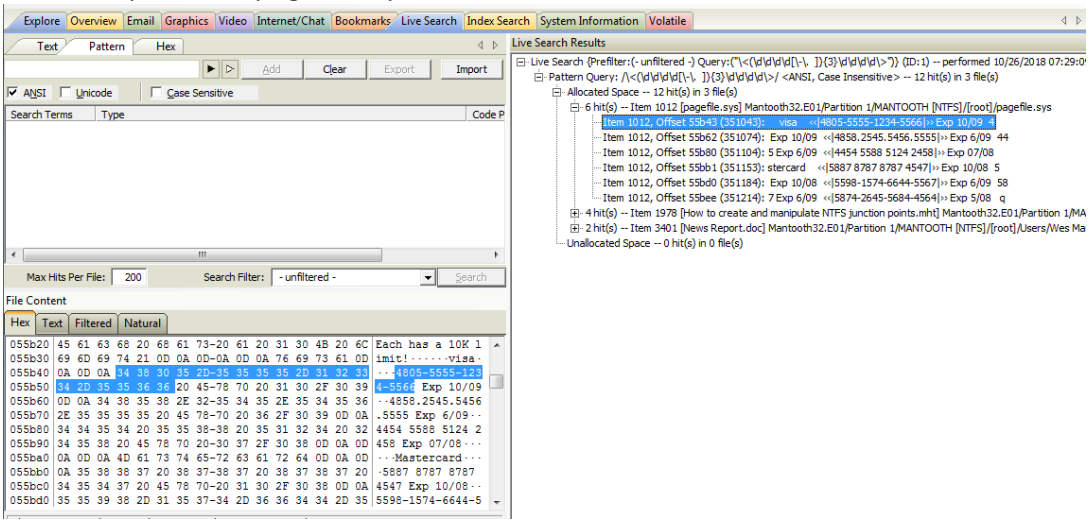


Live search

39. Start on the **Explore** tab; quick pic the Mantooth image; checkmark all Mantooth files by selecting the **double check icon** in the **file list**;
40. Click on **Live Search** tab; [note how the options differ from Index Searching]; select the Pattern search sub-tab; have a look at the available regular expressions; then select "**Credit Card Standard**", click Add.

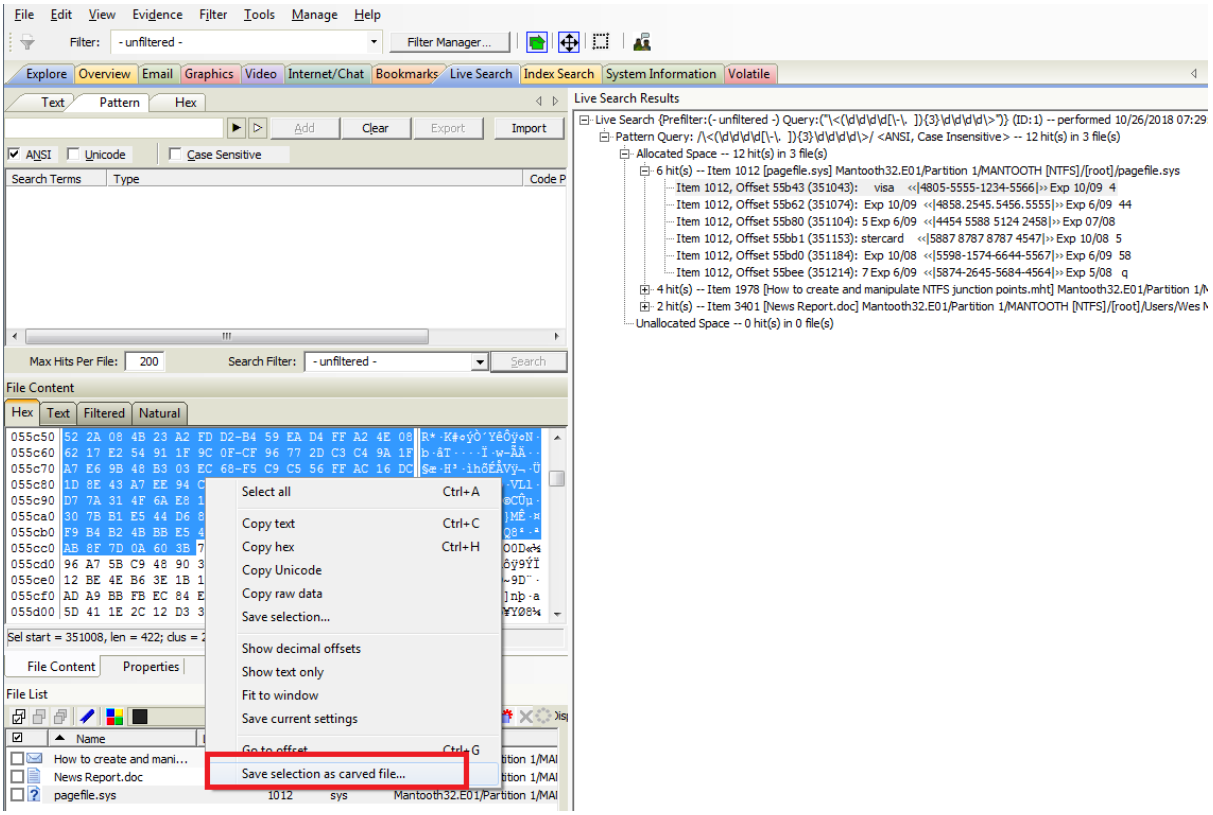


41. At the bottom of the Pattern Search Terms window, select Checked Files from the Search Filter pull-down menu. Click on search.
42. In the Live Search Results pane, expand Live Search > Pattern Query > Allocated
43. Expand the pagefile.sys hits and review the data results.



44. In the File Content Viewer, scroll up to locate the beginning of the text fragment.
45. Click-and-drag in the Hex view to highlight the recovered data (approximately 234bytes)

46. Right-click the highlighted data, then click Save Selection as a Carved File.



47. In the Save Carved File As window, name the carved file with a proper name.
48. Find the saved carved file from previous step -> **Overview** tab -> File Status -> Data Carved Files.