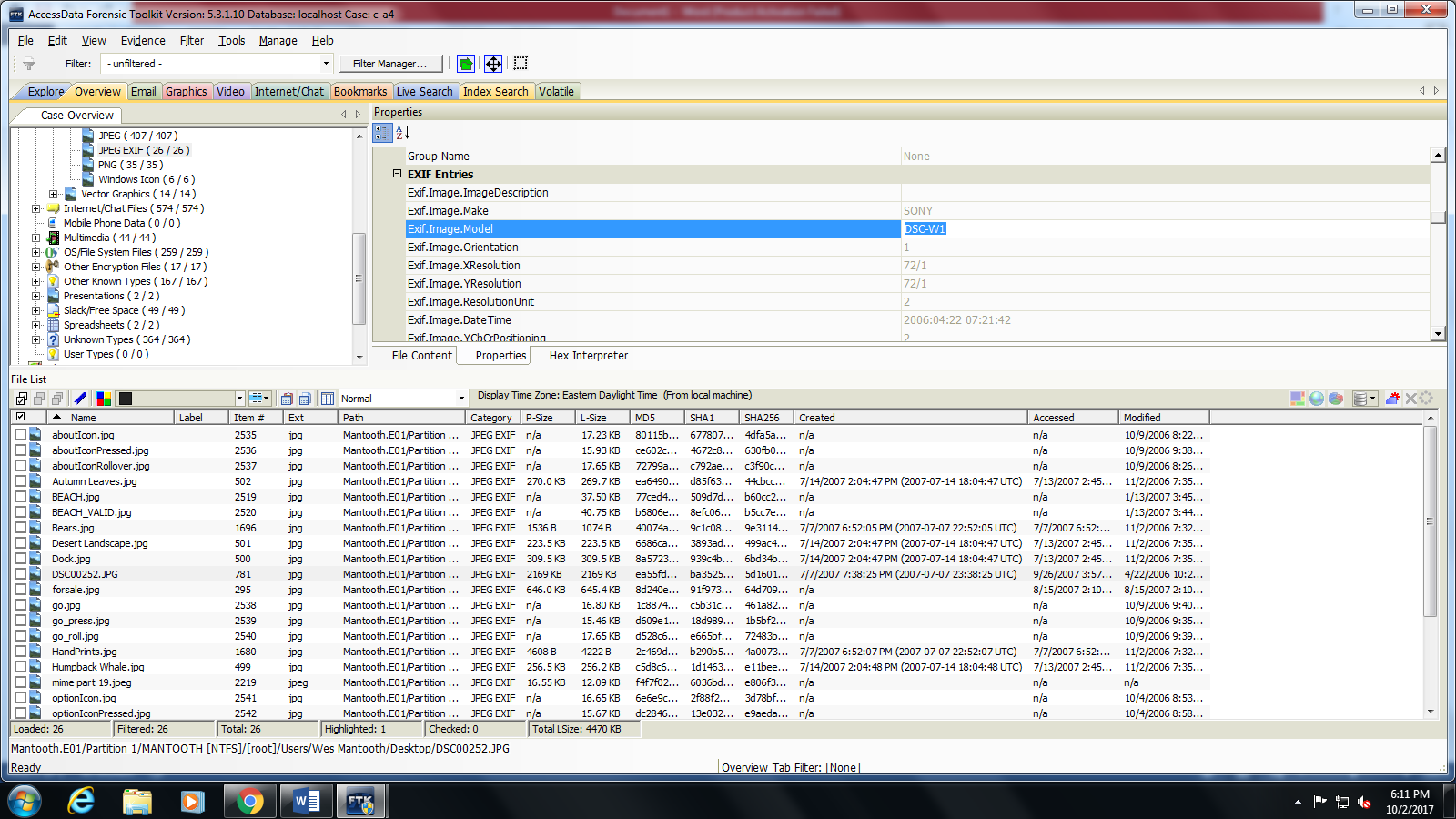
1. Click on the Overview tab. Navigate to File Category > Graphics > Raster Graphics > JPEG EXIF container. Select the file named DSC00252.JPG and view the files EXIF data. Note: EXIF data is data in the “exchangeable image file format.” This is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras. What make and model of camera took this picture? [5 points]

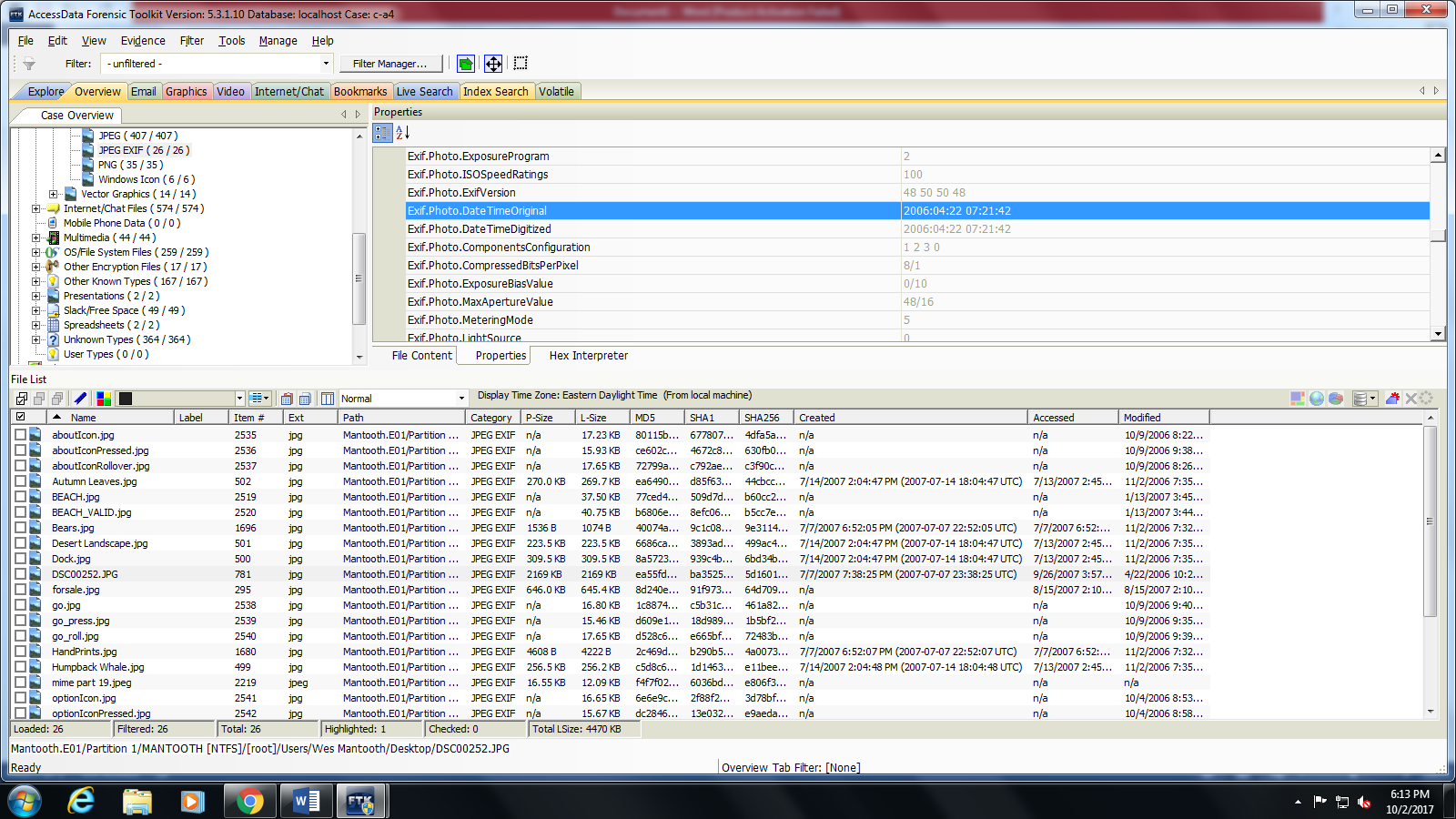


2. Notice that the DSC00252.JPG picture’s EXIF data states the picture has an “Orientation” value of 1. What does an orientation value of 1 mean? (Use the Internet to find your answer.) [5 points]

The [Exif specification](http://park2.wakwak.com/~tsuruzoh/Computer/Digicams/exif-e.html) defines an Orientation Tag to indicate the orientation of the camera relative to the captured scene. The orientation value of 1 indicates that the image’s 0th row is on top and the 0th column is on the left side.

(http://sylvana.net/jpegcrop/exif\_orientation.html)

3. On what day and at what time was the DSC00252.JPG picture taken? [5 points]



4. Review the evidence tree within FTK. Notice that within the Graphics container there are sub-containers for “raster graphics” and “vector graphics.” What are raster graphics and what are vector graphics? (You may have to Google this answer.)

Raster images are created with pixel-based programs or captured with a camera or scanner. They are more common in general such as jpg, gif, png, and are widely used on the web. Vector graphics are created with vector software and are common for images that will be applied onto a physical product. Also used in CAD, engineering, and 3D graphics which we do not provide information nor services for.

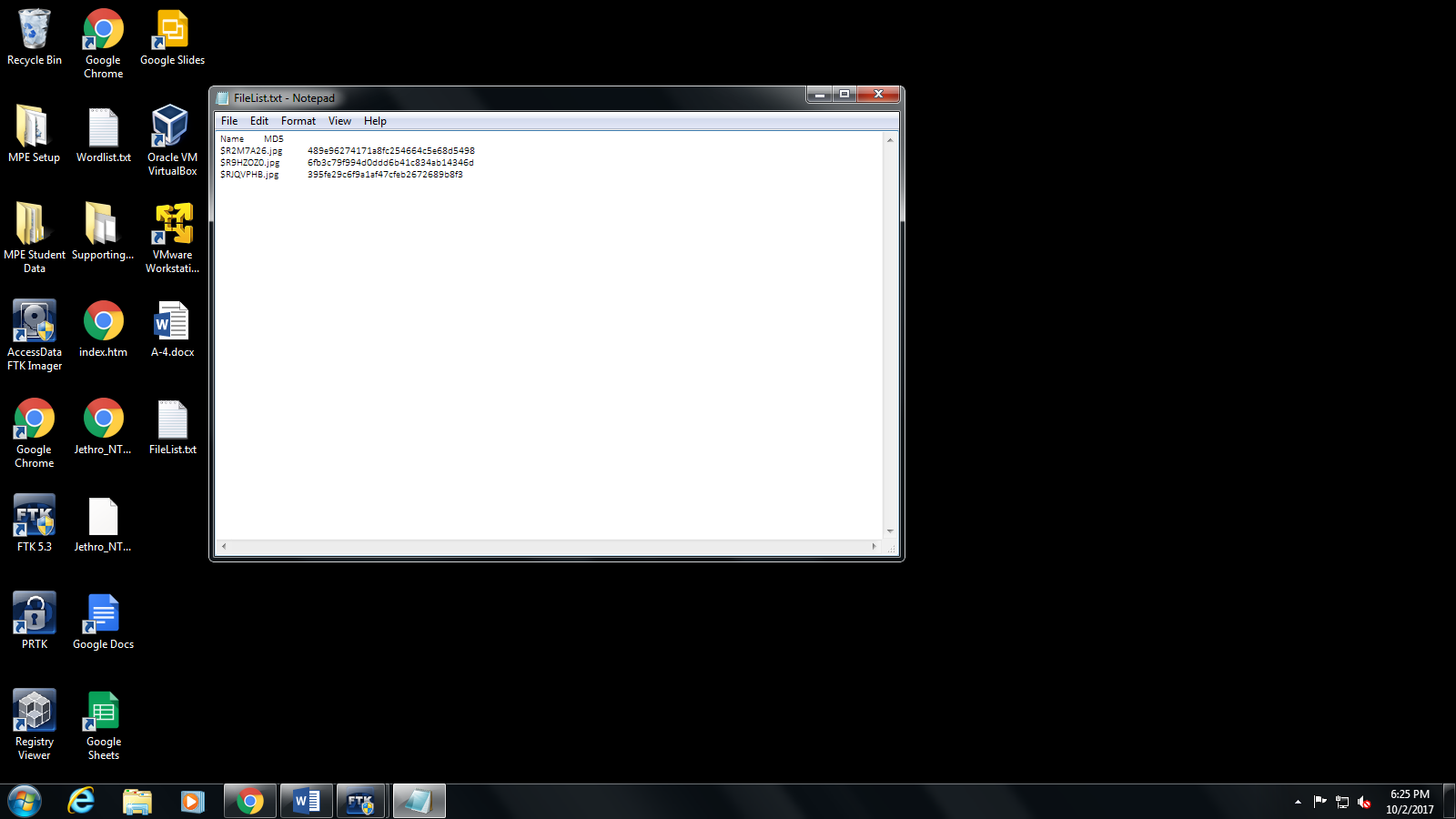
When using a raster program you **paint** an image and it's similar to dipping a brush in paint and painting. You can blend colors to soften the transition from one color to another. When using a vector program you **draw the outline of shapes**: and it's similar to creating an image with tiles of all different shapes and sizes. E.g. an eye shape, a nose shape, a lip shape. These shapes called objects display one single color each.

(http://vector-conversions.com/vectorizing/raster\_vs\_vector.html)

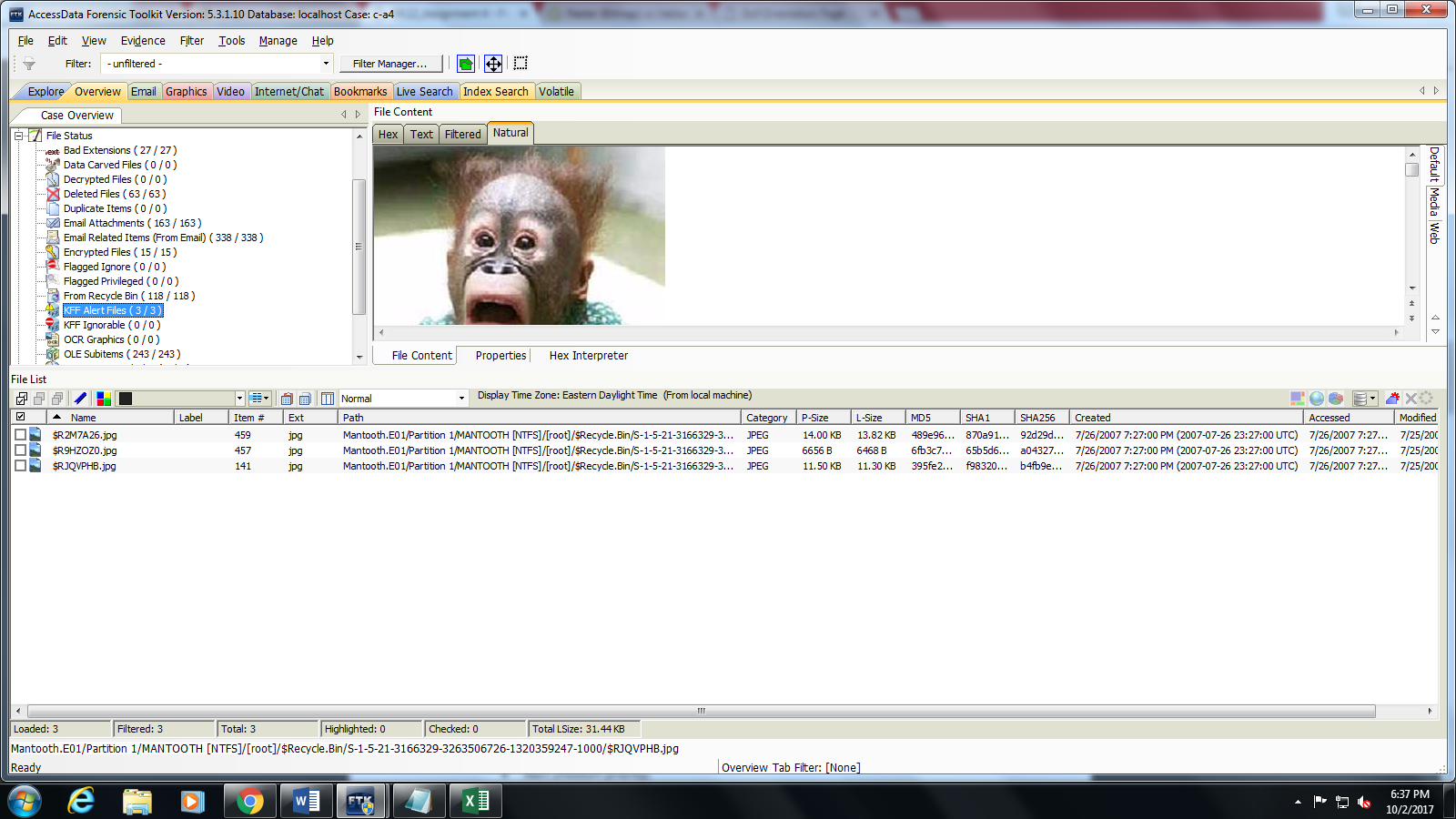
5. Locate the three (3) files listed below. Check each one and export a file list that just includes the file name and the MD5 value.

$R2M7A26.jpg, $R9HZOZ0.jpg, $RJQVPHB.jpg

Provide a print-screen image of the list of three files names with MD5 values. [5 points]



6. Navigate to the “Overview” tab > “File Status” > “KFF Alert Files” container. What are the names of the files within this list? [10 points]



7. By default, what three hash groups does FTK have to categorize files based on their importance or “priority”? [10 points] (Hint: The answer is not MD5, SHA1, and SHA256. These are hash algorithms, not “hash groups”.)

ANSWER PROVIDED

Ignore (lowest priority)

Alert (medium priority)

Disregard (highest priority)

(p. 501, Training Manual)

8. Name four (4) sources (agencies) for the information that is maintained within the AccessData Known File Filter (KFF)? [10 points]

ANSWER PROVIDED

National Drug Intelligence Center (NDIC)

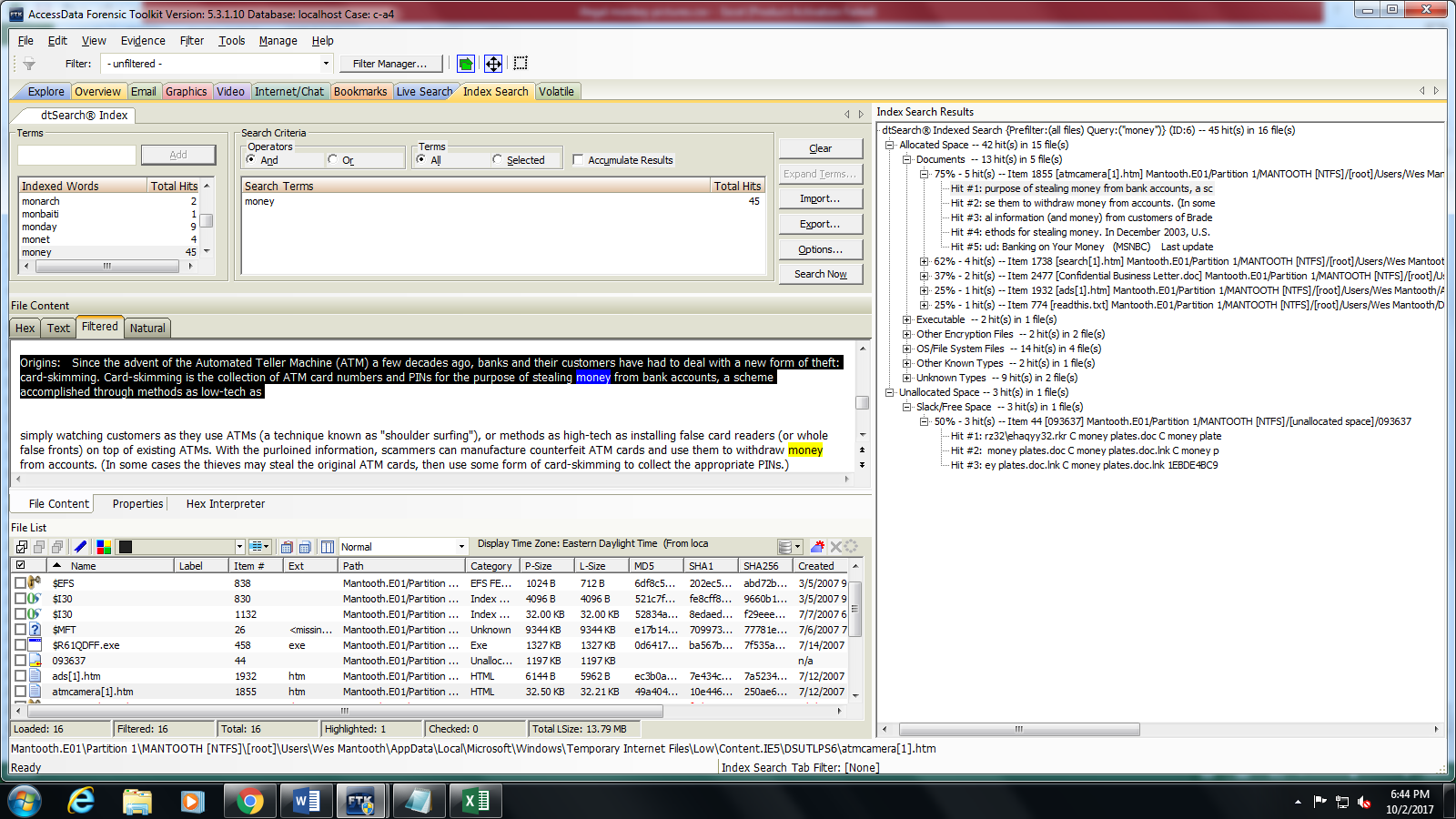
National Institute of Standards and Technology (NIST)

National Software Reference Library (NSRL)

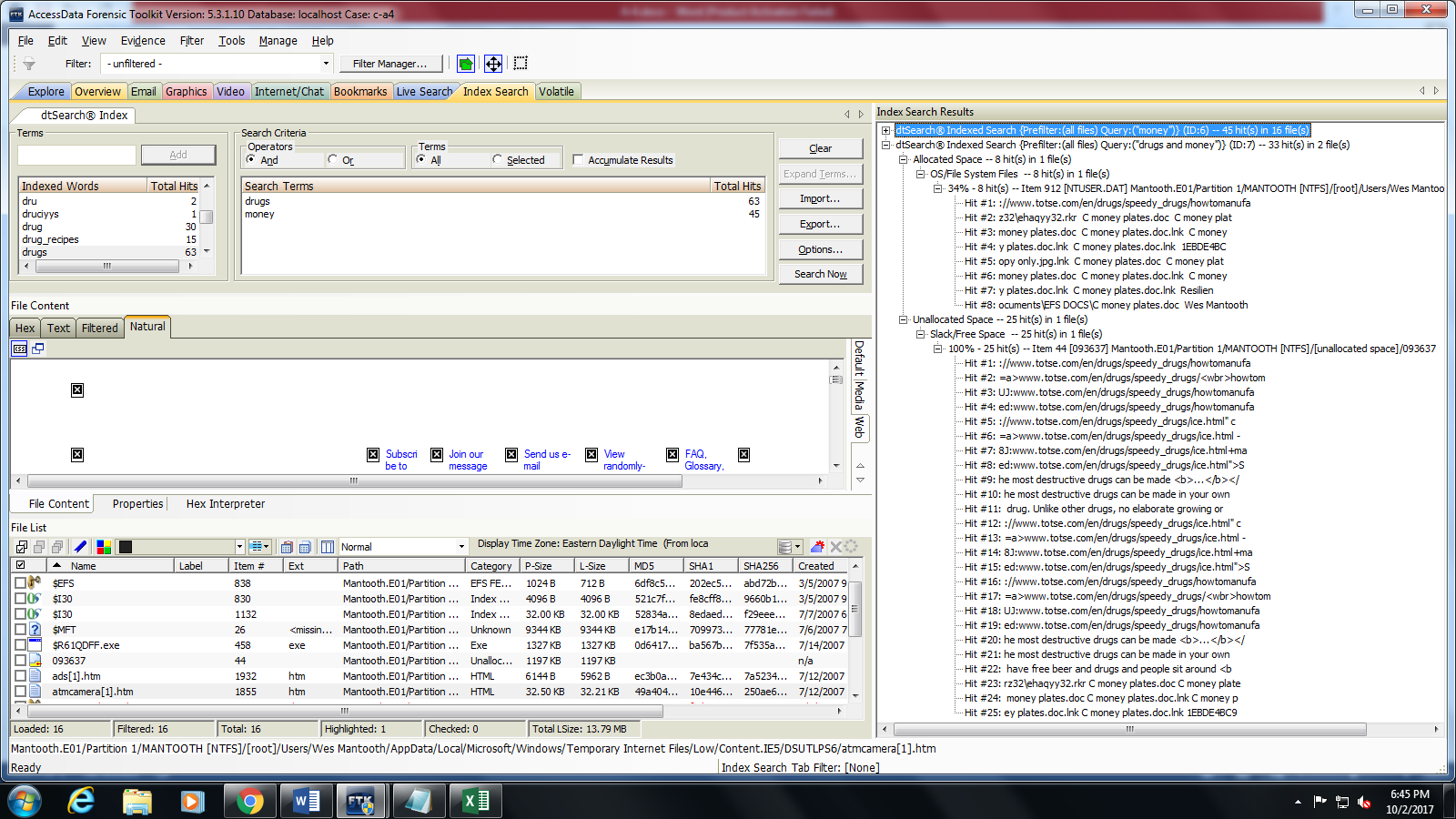
Department of Homeland Security (DHS)

(p. 503, Training Manual)

9. Conduct an “Index Search” for the word “money”. Notice that you get 45 “hits”, in 15 files. Notice that 3 hits are in “unallocated” space. Navigate to the file tree in the “Index Search Results”. View the “File Content” associated with the first hit associated with the first file in the list. Note, the list looks like the picture below. Notice “Hit #1” is associated with the sentence fragment “purpose of stealing money from bank accounts, a sc…” What is the complete sentence that this fragment comes from? (Well, it’s not actually a complete sentence. It’s technically a longer sentence fragment.) [5 points]



10. Conduct an “Index Search” for the term “drugs”. Notice that you get 65 hits. Notice in the FTK interface there is an option to do “And” and “Or” operations. If your only searches are for “money” (done previously) and “drugs”, and you select “Or”, the search will return any “hit” that has either or both terms, “money” and “drugs”. However, If you select “And” and you conduct a search, the search result only returns those “hits” that include both terms, “money” and “drugs”. When you do a search for “money” AND “drugs”, how many hits in allocated space do you receive and how many files are involved with these hits? (Hint: Do not include hits from “Unallocated space”) [5 points]

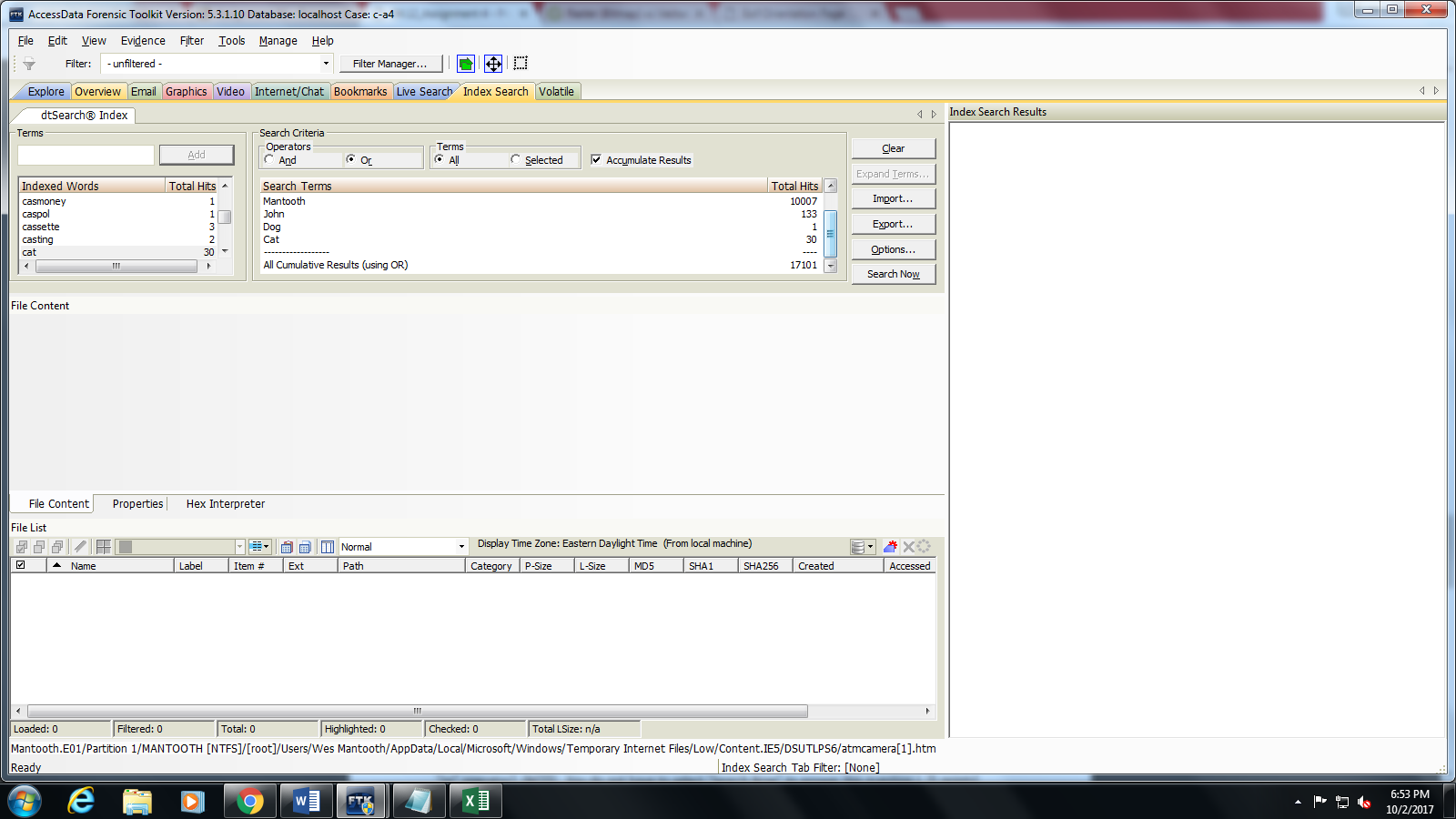


Number of hits from Allocated Space: 8 Hits in 1 file

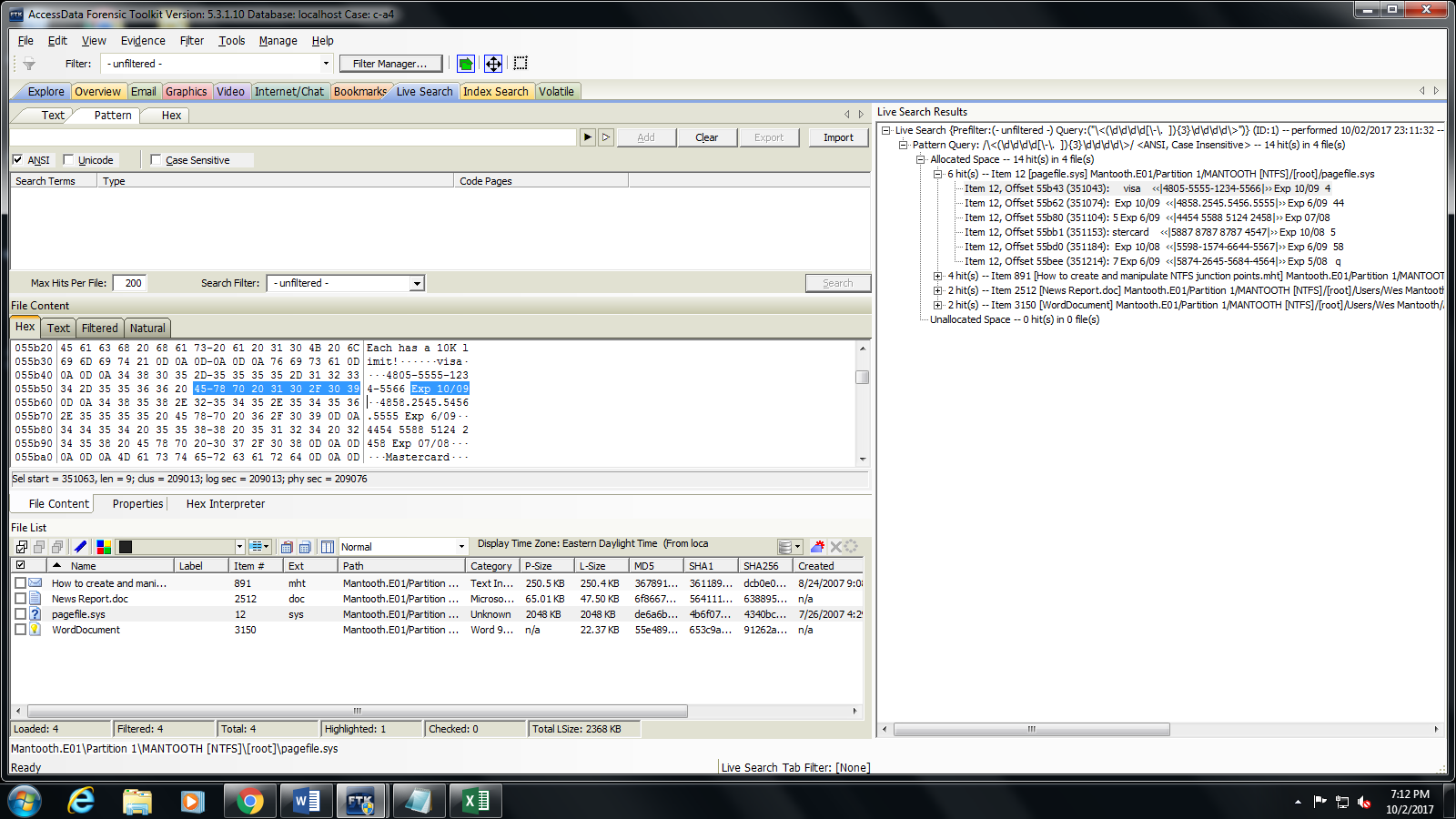
11. Within the Index Search tab, right-click any query and click “Delete All Search Hits.” In the Search Terms section, click “clear” multiple times to clear all of the search terms. On the Desktop, create a new text file named “SearchImport.txt” and add the following terms.

* Wes
* Washer
* Mantooth
* John
* Dog
* Cat

Notice that if you select the “and” operator, you get “0” hits. How many hits do you get if you use the “or” operator? (NOTE: You do not have to select “Search Now” to answer this question.) [5 points]



12. Conduct a “Regular Expression” search for a “pattern” that is in the “Credit Card Standard” format. You should get 14 hits. One of the hits is for the credit card number 4805-5555-1234- 5566. What is the expiration date for this credit card? [5 points]



13. Wes Mantooth sent an email to his mom. What is her email address? [5 points]

[toothfairy@mentaldental.com](mailto:toothfairy@mentaldental.com)

14. What is the meaning of the term “fuzzy hashing” as the term is applied to a word search within FTK? [5 points]

Fuzzy hashing is a concept which involves the ability to compare two distinctly different items and determine a fundamental level of similarity (expressed as a percentage) between the two.

(http://www.shadowserver.org/wiki/uploads/Information/FuzzyHashing.pdf)