

CSEC 730 - Advanced Computer Forensics

Lab 2 - Forensic Toolkit (FTK) Lab

Please submit your answers (in PDF format) to the assignment submission folder under *MyCourses > Assignments* by the due date.

Objective

In this exercise, you will utilize FTK to analyze an incident. This project will help you tie all the pieces and techniques together so that you have a better understanding of the whole picture of forensics investigation.

Preparation

Make sure to watch the FTK videos posted in MyCourses and read the FTK User Guides as needed. You are encouraged to further explore other features of FTK that are not covered in this lab, using the FTK user guide.

Lab Descriptions

Given the forensic image, *Mantooth.E01*, you will use FTK to analyze this image and use FTK to create a report about this incident. (Note: In a real investigation, the investigator will write his/her own report using software-generated report as a reference.)

This lab uses AccessData's licensed tool, FTK software including FTK 6.2, Registry Viewer, and PRTK, installed on the Windows 11 VM on RLES. **The User Guides are located on the desktop of the VM.**

Lab Setup

You should have the Windows 11 VM deployed in Homework 3. See the lab setup instructions in Homework 3.

The Windows virtual machine is ready to use. In case you need to re-login, the Windows login credential is: Username: Student; Password: student

The evidence file, *Mantooth.E01*, is a forensic image provided by Guidance Software for FTK ACE certification training. *Mantooth.E01* is located in the ***images*** folder on the desktop.

Scenario: The first investigator has created an Encase image of *Wes Mantooth's* computer's hard drive. Your job is to examine the image using FTK and report your statement and findings based on *Mantooth's NTFS partition*. You should identify and extract pertinent evidence to support your findings.

Steps involved:

- 1) Create a new case and add the Mantooth.E01 evidence file to FTK for investigation.
- 2) Analyze the image and identify and bookmark the pertinent evidence.
- 3) Generate an FTK report. All information in your report should be verifiable and repeatable in order to be admissible in court.

DETAILED PROCEDURES THAT MAY HELP YOU TO GO THROUGH THE FTK SOFTWARE ARE SHOWN BELOW

Step 1: Starting a New Case

Launch FTK 6.2 (be patient. It takes a while) and login with **Admin, netsys**.

Create a customized evidence processing profile

Click on “Manage -> Evidence Processing Profiles...” Choose “New Profile...”.

Add the following options in addition to the default options.

- Create Thumbnails for Videos
- Language Identification
- Generate System Information

Modify “Expand Compound Files” by adding the following selections

- Chrome Bookmarks
- Chrome Cache
- Chrome SQLite
- EVTX
- IE Cookie Text
- IE Recovery
- IE WebCache

Save your new profile as “Default”, and Save. Then set “Default” as our default profile.

Create a new case named “Mantooth-FTK”

Leave the Case Folder Directory to be “C:\Users\Student\Desktop”. The “Default” profile is chosen by default. Feel free to fill in other information although there are optional.

Click on “Customize...”

Questions 1: Read the default options of “Evidence Refinement” and “Index Refinement” and list 5 default settings from “Evidence Refinement” and 5 default settings from “Index Refinement.”

- 5 “Evidence Refinement” options:
 - “Include File Slack”
 - “Include Free Space”
 - File Types:
 - Documents
 - Spreadsheet
 - Deleted, Encrypted, and From Email are in Ignore status
- 5 “Index Refinement” options:
 - “Include File Slack”
 - “Include Free Space”
 - “Include Message Headers”
 - File Types:

- Documents
- Database
- Graphics

It is safe to use all the default options. However, you should try to understand these options. Go back to the New Case Options Window, and Click OK.

Add an Image to the existing case

After the case is created, the Manage Evidence window will pop up. Add the image “Mantooth.E01” to this case.

Question 2: What are the types of evidence that can be added to a case in FTK?

- The types of evidence that can be added to a case in FTK are acquired images, All images in directory, contents in a directory, individual files, physical drive, logical drive.

Set the Time Zone

When you acquire a computer as evidence it is important to make note of the computer’s time and time zone, especially if you need to correlate evidence from different time zones (never assume the time or time zone on a computer is correct.)

In the FTK’s Manage Evidence Window, choose Eastern Time with Daylight Saving (US-New York) from the Time Zone dropdown list.

Click “OK”. Now FTK Data Processing Status window will pop up to show you the progress. For a large image, this process takes a while since FTK will process the evidence based on your setting defined in evidence processing options.

After it is done, your Mantooth-FTK case is ready for your examination. If you like, you can close the Data Processing Status window.

Step 2: Analyzing Evidence Using FTK

First, familiarize yourself with the FTK examiner’s GUI interface.

EXPLORE tab.

The Explore tab displays all the contents of the case evidence in Explorer Tree Pane, File List Pane, and File Content Viewer Pane. You can resize the panes by dragging the edges of the pane according to your need and can always reset the panes to default by choosing View -> Tab Layout -> Reset To Default.

Question 3: Expand Mantooth.E01, how many partitions are in this image, and what are the filesystems?

- There are 2 partitions in the image. The first partition is NTFS, and the second partition is Ext2.

Question 4: Find \$Recycle.Bin from Partition 1, which user (user name) once owned and then deleted the files that belong to SID=1000? How do you know?

- The user is Mantooth. The way I know this is because SID of 1000 is for the initial admin user that is created for the system. and since we are looking at the recycle bin for Mantooth, he has to be the user account with SID of 1000.

OVERVIEW tab

The Overview tab groups items into categories. It displays items in Category Pane (top-left pane by default), File list Pane (bottom), and File Content Viewer Pane (top-right).

Expand the **File Category** to examine each category and note the numbers for each category.

Question 5: Which file category (starting from File Category) does the file, *Confidential Business Letter.doc*, belong to? What is the file path for this file?

- Starting from File Category, the Confidential Business Letter.doc belongs to the Document/Microsoft Word/Microsoft Word 2003 category.
- The file path is Mantooth.e01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook.pst>Personal Folders>Top of Personal Folder>Inbox>Letter>Confidential>Confidential Business Letter.doc

Question 6: Open the Confidential Business Letter.doc, check both File Content and Properties, who was the document author, when was this document last modified, and who modified at the last time?

- The document author is Rasco Badguy. The document was last modified on 08/01/2007 at 03:04:00 PM by Nick Drehel Jr.

Bookmarks allow you to mark folders, files, or parts of a file for later reference and inclusion in reports.

Now let's bookmark the Confidential Business Letter.doc file by right clicking the file and "Create Bookmark...". Name the bookmark as "Mantooth". The "All highlighted" radio button should be chosen by default. Choose a parent directory for this bookmark, for example, Admin, and click OK.

Go to the **Bookmarks** tab to verify the bookmark you just created.

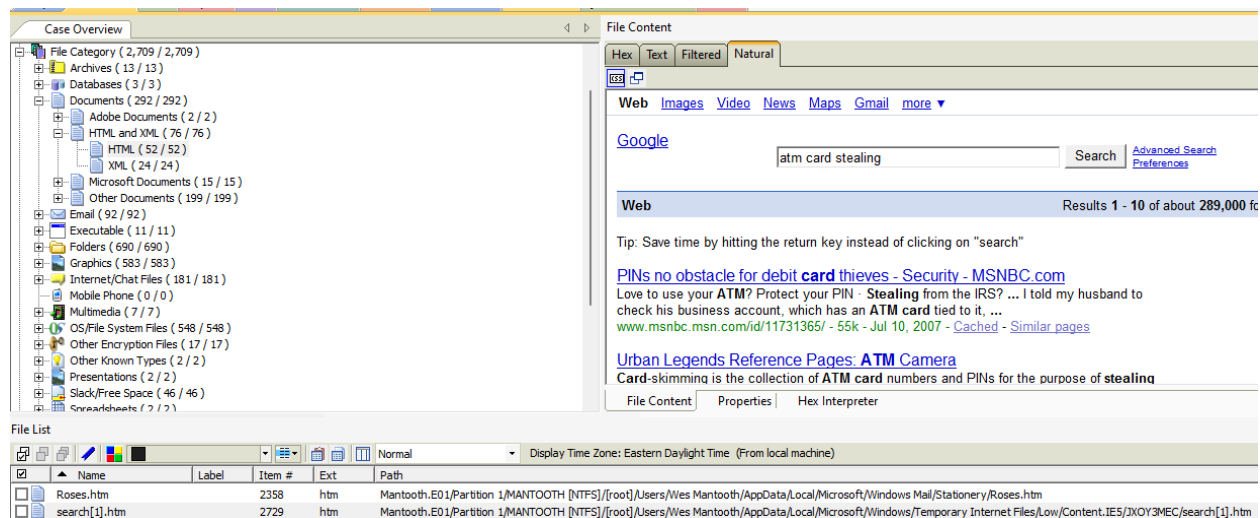
Next, check File Category > Documents > Microsoft Documents > Microsoft Word > Microsoft Word 2003 file list,

Question 7: What are the two documents that use foreign languages?

- The two documents that use foreign languages are "Arabic Text.doc" and "Japanese text.doc."

Go to File Category > Documents > HTML, and look for a Google search file that Mantooth searched "atm card stealing".

Show a screenshot below.



Bookmark this Google search file to the Mantooth bookmark by “Add to Bookmark...”.

Question 8: Go to File Category > Multimedia > Video > MPEG 2.0 Video, watch happy.mpeg, what can you tell from the video?

- From the video, I can tell that an employee was trying to do something in the office. However, it was probably not working and he got frustrated and broke the monitor and the keyboard out of anger.
-

Question 9. Go to File Category > OS/File system Files > Windows NT Registry, what is the file path of Wes Mantooth’s NTUSER.DAT? Explain what a NTUSER.DAT file is.

- The file path of Wes Mantooth’s NTUSER.DAT is Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/NTUSER.DAT. NTUSER.DAT is a file that stores user profile settings from windows registry.
-

Windows Registry

Right-click Wes Mantooth’s NTUSER.DAT and choose “Open in Registry Viewer”. (You could export the ntuse.dat and then launch the AccessData Registry Viewer to view this file in Registry Viewer.)

In the **Registry Viewer**, explore this registry file using the techniques covered in the Registry Analysis lecture. For example, you may search for the registry key, TypedURL, via Edit -> Find...

Question 10: List interesting results you found from TypedURLs, RecentDocs, and UserAssist. If you identified any other data from ntuser.dat, please also list here.

- One interesting thing for TypedURLs is that there are different search engines that seem to be used, for example, google, yahoo, hotbot, and others. There is also a path C:\Users\Mantooth\Documents\Scripts. For RecentDocs, I found some interesting .pdf and text files, for example, order851797-2007-04-12-13-17-02 (1).pdf, You Got it!.txt, Bitlocker Command.txt.txt, key.txt, and etc. For UserAssist, I found some application that ran, for example, cardchecker.exe, truecrypt.exe, remote desktop connection, FTK imager, and etc.
-

Now Expand the **File Status**

File Signatures

A file type (JPEG, Word Document, MP3 file) can be determined by the file's extension and by a header that precedes the data in the file. If a file's extension has been deliberately changed, then the only way to determine its type is by looking at its header.

Question 11: Examine the information listed under *File Status* to find out where FTK categorizes the files whose extension does not match the file type identified in the file header. List 2 Bad Extension files.

- The FTK categorizes the files whose extension does not match the file type identified in the file header in the "Bad Extensions" category. Two examples of bad extensions are "Apps.Lst", and 1rb[1].jpg.

Data Carved Files:

Data carving is the process of locating files and objects that have been deleted or that are embedded in other files.

Question 12: Check the number of Data Carved Files from File Status, what is the number?

- The number of data Carved Files is 0.
-

Now let's perform the data carving process.

From the top menu bar, click on Evidence > Additional Analysis.....

In the Additional Analysis Window, navigate to the miscellaneous tab and check Data Carve.

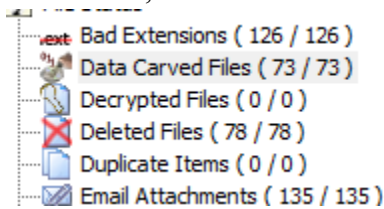
Click the carving options to select the types of files to carve.

In real cases, you should select all. Click "OK". Data carving is a time-consuming process. For this exercise, you will only choose one type (for example, jpeg) to perform data carving. A "Data Processing Status" Window will pop up to show you the status of this process. After this job is finished. Close the "Data Processing Status" Window.

The carved files should be listed in the File List Pane at the bottom by default. If you click on the file in the File List Pane, the selected file's content should be displayed in the File Content Pane. If you choose to export the data-carved file, simply right-click the file, choose "export..." and save the exported file to your desired location.

Question 13: Check the number of Data Carved Files again, have you carved out some files? Provide a screenshot.

- Yes, I have carved out 73 files.



Question 14: What interesting files do you find by performing data carving process (if you did not find any pertinent information, that is fine)? Why is this process so important?

- I found some image files that say a page of a checkbook and other images that have “invalid card number” on it. potentially showing that there were attempts to use credit card numbers and get money.
- It is important to use a data carving process because it helps to retrieve data from damaged or corrupted data resources that might potentially help with investigation.

Click the GRAPHICS tab

The Graphics tab allows you to quickly see all of the pictures contained on all of the devices in the case. Click the **Graphics** tab and green-select **Wes Mantooth** folder under root\Users. All pictures under Wes Mantooth are shown in thumbnails alphabetically.

Question 15. Find one bank check image and bookmark it in Mantooth bookmark. What is the name of this image?

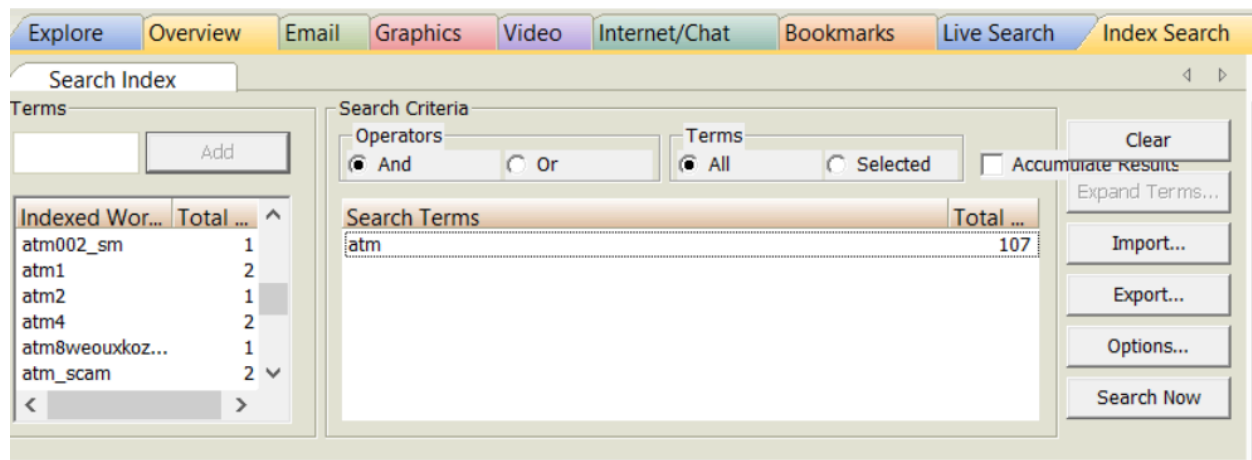
- “08-15-05_arkansas_check.gif” is the name of the image.

Keywords and Searching

Searching for evidence can be one of the most crucial steps in the examination. FTK supports two kinds of search, indexed and live searches. An indexed search uses the index file to find a search term while a live search involves an item-by-item comparison with a search term. The index file could be generated during the creation of a case or be indexed later.

Click the **INDEXED SEARCH** tab. In the Terms box, type some keywords, for example, “atm”; then click Add. If you add multiple keywords, you will use either “And” or “Or” to cumulate results.

Click “Search Now”. (If “Search Now” is hidden, you may have to pull the File Content pane down to see the “Search Now” button at the bottom of *dtSearch Index* pane.) (see the Figure below).



Check **Index Search Results** at the up-right pane and expand the search results.

Select one file and find the instances of “atm” in the file. If you find any files important, bookmark these files.

Question 16: How many files contain “atm”, and how many hits of “atm” in total?

- There are 107 hits in total in 15 files.

Click the **LIVE SEARCH** tab, then choose the **Pattern** tab.

Click the 2nd arrow to view the default regular expressions.
Select “**Visa**” to search.

Question 17: Do you find any Visa numbers? list three Visa numbers along with the expiration date.

- Yes, I found 3 visa numbers. The three visa numbers are 4805-5555-1234-5566 with Exp 10/09, 4858.2524.5456.5555 with Exp 6/09, and 4454 5588 5124 2458 with Exp 07/08.

```
[-] Live Search (Prefilter:(- unfiltered -) Query:("\<4\d\d\d[\-\. ](\d\d\d\d[\-\. ]){2}\d\d\d\d\>") (ID:1) -- performed 04/10/2024 19:12:48 -- 3 hit(s) in 1 file(s)
[-] Pattern Query: /\<4\d\d\d[\-\. ](\d\d\d\d[\-\. ]){2}\d\d\d\d\>/ <ANSI, Case Insensitive> -- 3 hit(s) in 1 file(s)
[-] Allocated Space -- 3 hit(s) in 1 file(s)
    [-] 3 hit(s) -- Item 1012 [pagefile.sys] Mantooth.E01/Partition 1/MANTOOTH [NTFS]/[root]/pagefile.sys
        Item 1012, Offset 55b43 (351043): visa <<|4805-5555-1234-5566|>> Exp 10/09 4
        Item 1012, Offset 55b62 (351074): Exp 10/09 <<|4858.2545.5456.5555|>> Exp 6/09 44
        Item 1012, Offset 55b80 (351104): 5 Exp 6/09 <<|4454 5588 5124 2458|>> Exp 07/08
    ... Unallocated Space -- 0 hit(s) in 0 file(s)
```

Question 18: What is the advantage of using indexed search vs. the live search?

- The advantage of using indexed search vs. live search is that indexed search is faster.
-

Email

Email processing is one of the most important steps in forensics investigation. FTK supports a powerful email feature to help you process emails.

Click on the **EMAIL** tab

Question 19: Check emails in Senders and Recipients under the Display Name of “wes mantooth”, do you find any important information? If so, what kind of information have you got? Bookmark some important messages to support your final report.

- I was able to find some important information. Some of the emails are about making the atm machine keep the card, or emails that have documents that talks about How To Steal Credit Number attached.
-

Click on **the INTERNET/CHAT** tab

Go to Internet Explorer Browser > Internet Explorer Files > MSIE History, check index.dat files.

Question 20: What is an index.dat file? List some pertinent information from this file.

- The index.dat files are used by windows OS to store information about internet browsing activity. Some visited websites or files paths are “file:///E:/Business Ideas/ATM_THEFTS1.ppt”, and “http://www.snopes.com/fraud/atm/atmcamera.asp”
-

Click on SYSTEM INFORMATION tab

Many important information such as Prefetch, UserAssist, URLs, Networks, SAM Users, Shell Bags are presented here.

Question 21: Choose two pieces of evidences (for example, Prefetch and SAM Users). Describe the information, and also explain why they are important for forensic investigation.

- Prefetch is important for forensics because they can provide a timeline of program execution. Using the timeline of the programs that ran one can figure out what the user was doing at a specific time and if it's relevant to the investigation. SAM Users is important because it holds information about user accounts and windows systems. By examining the SAM file, one can determine what accounts were in the windows system and what account was last used that might relate to the investigation.
-

DECRYPT ENCRYPTED FILES USING PRTK.

Part I. Attempt to recover the password for an encrypted file

Make sure to watch the PRTK video first.

Step 1. In FTK, click FTK's overview tab, select File Status > Encrypted Files, and export the encrypted file "Those who owes.xls" for decryption.

Step 2. In FTK, export the full-text index by clicking File > Export Word List. In the Select Registry Files to Be Included in the Word List window, select Wes Mantooth's NTUSER.DAT, and save it as Mantooth Wordlist Export.

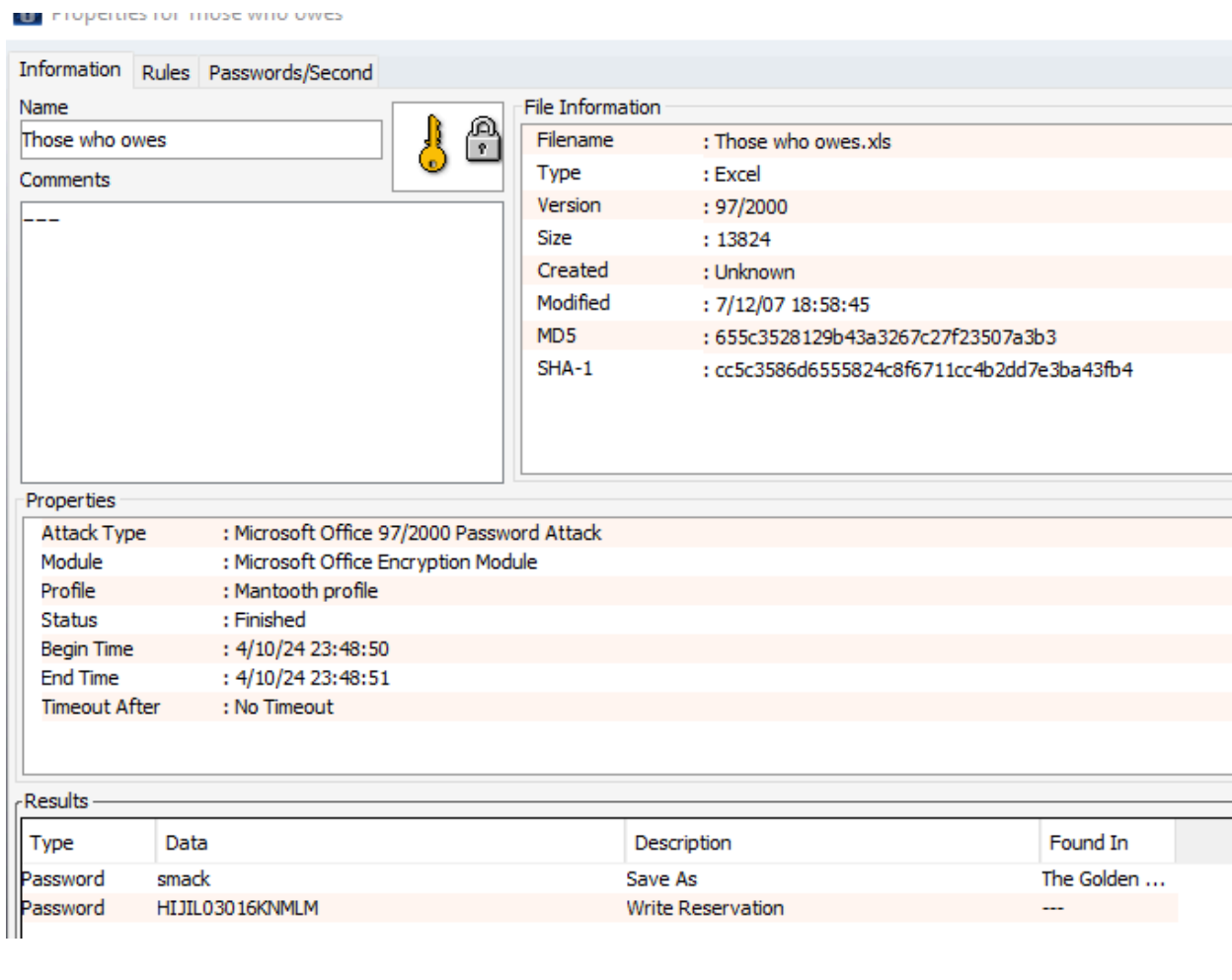
Step 3. Now start PRTK, click Tools > Dictionary Utility to generate your own Mantooth dictionary using your own Mantooth Wordlist Export list.

Step 4. In PRTK, click Edit > Profiles to create a new Profile called *Mantooth profile* using your Mantooth dictionary.

Step 5. Add the file "Those who owes.xls" in PRTK by File > Add Files... using your *Mantooth profile* to recover the password for the "Those who owes.xls" file.

Question 22: What are the passwords for the "Those who owes.xls" file? Show a screenshot of your PRTK with the passwords.

- The passwords for the "Those who owes.xls" file is smack.



Part II. Attempt to recover Mantooth's logon password to recover EFS files.

Step 1. In FTK, export registry files SAM and SYSTEM (hint: Go to Overview > File Category > OS/File System Files)

Step 2. Go back to PRTK, add the SAM file in PRTK (File > Add Files... and only check Wes Mantooth's NT hash. Also include Mantooth's SYSTEM file) to recover Mantooth's logon password.

Question 23: What is Mantooth's logon password? Show a screenshot of your PRTK with the password.

- The password is tooth



Part III. Attempt to decrypt files

Now, we try to use Mantooth's logon password to decrypt Mantooth's EFS files and also use the password of "Those who owes.xls" to decrypt "Those who owes.xls".

Return to FTK.

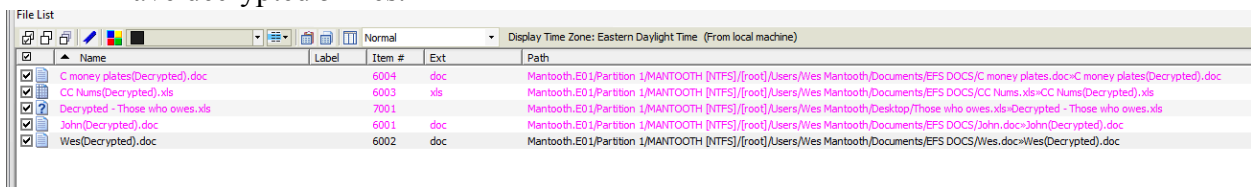
Under "Overview > File Status > Encrypted Files", check all four EFS files and "Those who owes.xls" to decrypt. On the Menu bar, click "Tools > Decrypt Files ...". Click the "Set Passwords" button, and add in both the passwords for "Those who owes.xls" and Mantooth's logon password. Leave the "Perform Automatic Decryption" and "EFS" checked. Click "Decrypt".

After the job is finished, Click the Overview tab.

Select File Status > Decrypted Files.

Question 24: How many files you have decrypted? Show a screenshot of "Decrypted Files". Include all decrypted files in your Mantooth bookmark.

- I have decrypted 5 files.



The screenshot shows the FTK File List window with the following data:

Name	Label	Item #	Ext	Path
C money plates(Decrypted).doc		6004	doc	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Documents\EFS DOCS\C money plates.doc<C money plates(Decrypted).doc
CC Nums(Decrypted).xls		6003	xls	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Documents\EFS DOCS\CC Nums.xls<CC Nums(Decrypted).xls
Decrypted - Those who owes.xls		7001		Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Desktop\Those who owes.xls<Decrypted - Those who owes.xls
John(Decrypted).doc		6001	doc	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Documents\EFS DOCS\John.doc<John(Decrypted).doc
Wes(Decrypted).doc		6002	doc	Mantooth.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes Mantooth\Documents\EFS DOCS\Wes.doc<Wes(Decrypted).doc

Step 3: Case Report (See FTK User Guide)

After performing a thorough forensic investigation, it is critical that you are able to publish and present your findings.

Question 25: Based on your investigation using FTK, provide your statement about this case regarding Wes Mantooth. Provide 3-5 evidence to support your statement.

- Based on the investigation, I was able to determine that Wes Mantooth was doing suspicious and illegal activities with drugs like and regarding stealing credit cards through ATM machines. All evidence is in the FTK generated report, especially in the Mantooth Bookmark section. To give 3 pieces of evidence to prove this investigation there have been many emails back and forth between Mantooth and others sharing how to steal credit cards through ATMs. There was a remote desktop connection, and an excel sheet that shows the name and what they need to give with the price, for example, the drug meth.

FTK has a sophisticated report wizard that allows you to assemble and publish case information. Last, let's practice how to use this built-in report wizard to generate a report.

Click File > Report

Fill in the Case information which will appear on the Case Information page of the report. Create a report to include pertinent evidence (such as pictures, bookmarked, ..., etc.) to support your statement. (Hint: To include bookmarks, make sure the boxes for Include in Report and Export Files are checked.)

Advanced Exercise (NOT REQUIRED): Using log2timeline/plaso (<https://www.youtube.com/watch?v=sAvyRwOmE10&t=2109s>) to generate a super timeline of selected Windows artifacts from the given image. Include your commands to filter your selected Windows artifacts as pertinent evidence.

Deliverables:

1. Your lab report to answer all questions from this document. (Every question is 3.5 points)
2. The PDF version of your **FTK-generated** report on this case. (12.5 points)