IT Forensic Workshop 7

Topics:

- Windows Registery
- Live search
- NTFS Volume Shadow Copies

Covered Learning Outcomes:

- explain the motivations and landscape of forensic investigations in an IT context;
- explain the relevant legal definitions and frameworks that apply to digital forensic investigations;
- select appropriate tools and algorithms to perform forensic investigations and acquire relevant evidence;

Instructions:

- Individual activities.
- Install a free demo mode of Registry Viewer

Required Files:

- Volume Shadow Copies.E01
- Washer17.E01

ACTIVITY A.1: Exporting Registry Files

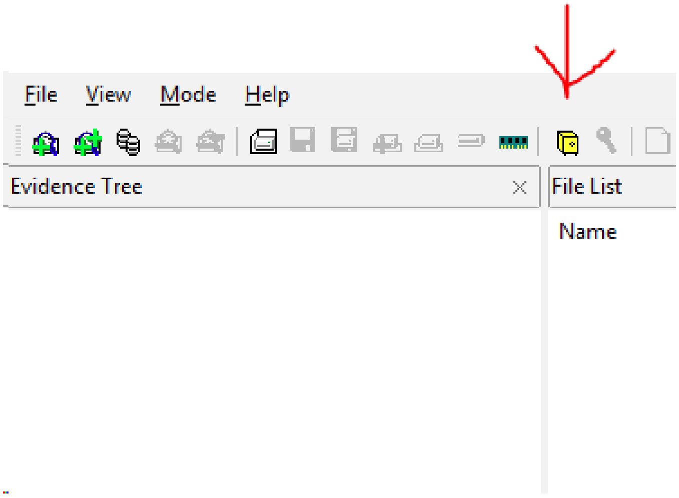
Export registry files from an image:

1. Prepare Washer 17.E01.
2. Export all registry files to a folder under your (authcate) directory.
3. Explore various registry files as the result of the operation.

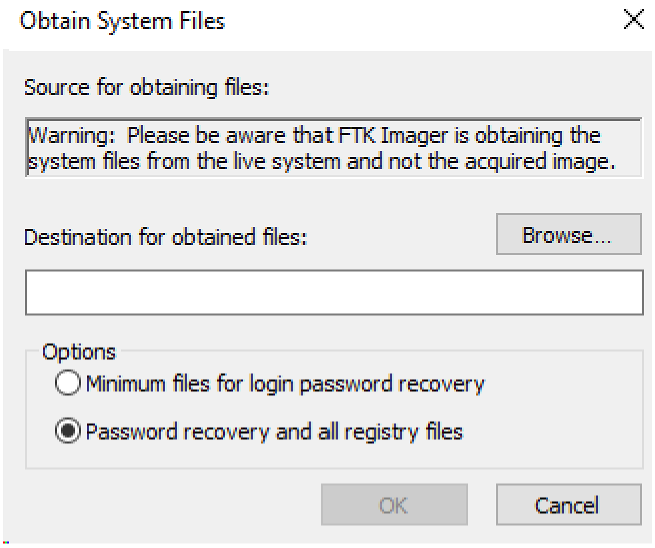
Export registry files from a live machine

NOTE: only do this **on your own machine**. If you are using computer lab, **skip** the activity.

1. Open your FTK Imager.
2. Click the “Obtain Protected Files” button in the FTK Imager.



3. There will be a window popup.



Obtain System Files

Source for obtaining files:

Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.

Destination for obtained files: Browse...

Options

○ Minimum files for login password recovery

● Password recovery and all registry files

OK Cancel

4. Destination for obtained files is the folder you have created before. Choose “Password recovery for login password recovery”, then click OK.
5. Open the Data folder and explore the folder. Explore various registry files as the result of the operation.

ACTIVITY A.2: System, SAM, Software, NTUR Registry

This activity registry files to determine some important forensic related information.

Question 1: What are “Control Set” and “LastKnownGood” in System Registry? Where do you find them?

Security IDentifier

Windows manages users and login information from the Security Accounts Manager (**SAM**). The SAM stores user information such as login information, login password hashes, and group information. When a user account is created, the user account name is created in the

SAM file. Additionally, each user is given a unique **Relative IDentifier** (RID) number. This number is not duplicated or reissued if a user account is deleted.

Windows tracks files on the computer using the Security IDentifier (SID). When a user creates a new file or doing other activities, Windows assigns the logged-on user’s SID to the file. This information may play a vital role during the investigation.

Question 2: What are the three main components of SID?

Question 3) What is the user name of the user with SID = 1003 in the Washer Image?

The SOFTWARE registry file contains information about software installed on the computer. This includes the operating system and registered owner (if supplied by the user at installation).

Question 4) What “Software” file may contain?

Each user will have his/her own NTUSER.DAT file found in the root of his home directory.
Export the NTUSER.DAT files from Washer image and use them in the activity. Exploring NTUSER.DAT

Task 5) Take one user at random. Find all unique information (activities, etc) you can find from the files regarding this user. The file may reveal the following:

- MRU (Most Recently Used)
- Typed URLs
- Internet search queries and form data
- Recent Documents
- Internet Explorer Start Page
- Printer information

ACTIVITY B: Volume Shadow Copies

In NTFS partitions, the Volume Shadow Copy Service (VSS) maintains a copy of every 16 KB block that is changed. These blocks are packaged up at predetermined times (which differ depending on the operating system being run) as a Volume Shadow Copy (VSC) or restore point.

Question 1: Why VSS/VSC might be of importance for a digital forensic examiner?

Question 2: What might be the limitations of VSC in digital forensic examinations?

With reference to Page 132 of FTK Manual, add VSC.e01 as the evidence file **with all its available restore points.**

Question 3: Can you spot a “secret” folder that is not in the current VSC? What files are inside the “secret” folder?

Refer to page 352 to find out how to examine metadata from Microsoft Office and Adobe documents.

Question 4: Examine “Steps for successful password Recovery.pdf” in the “First” folder. Who is the author? When are the created and modified Metadata?

ACTIVITY C: Live Search using Regular Expression

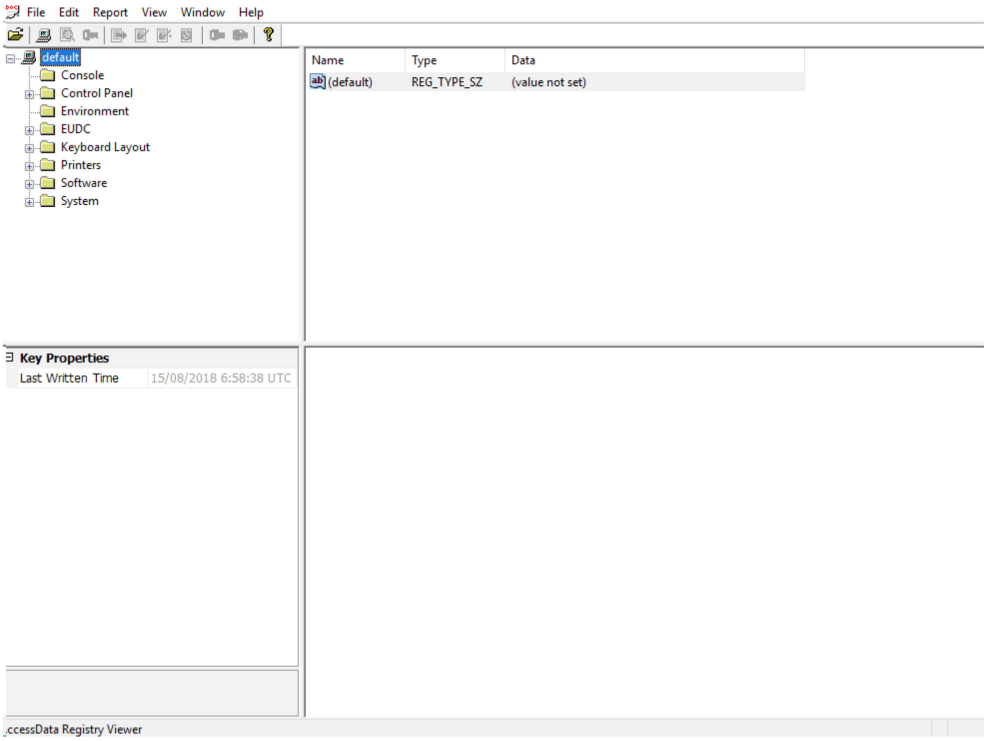
This exercise is to familiarize you with the Live Search in FTK. Refer to Page 366 (Chapter 26) of FTK User Guide.

Question:

1. Try new queries by using various regular expression statements and describe your findings.
2. You have now determined that viewing the documents is your next best course of action. Mantooth and Washer may have shared documents and you might want to test this theory.

Appendix for Activity A.1:

Load one of the registry files to Registry Viewer and explore the menus.



Name	Type	Data
(default)	REG_TYPE_SZ	(value not set)

Key Properties

Last Written Time	15/08/2018 6:58:38 UTC

The registry Viewer is divided into four panes: Key Tree, Value, Properties, and Hex Viewer. There are menus available (several options are disabled on the free demo)

File Menu

Option	Description
Open	Opens a registry file.
Close	Closes the currently open registry file.
MRU List	Shows the last four opened registry files.
Exit	Shuts down the program

Edit Menu

Option	Description
Find	Performs a find for a requested key or value string.
Find Next (F3)	Finds the next value matching the search string.
Advanced Find	Searches for and view all instances of a specific string.

Search by Date	Searches for a string value for: - During a date range - During and after a given date - During and before a given date
Add to Common Areas	Adds a key or subkey to the Common Areas
Remove from Common Areas	Removes a key or subkey from the Common Areas

Report Menu

Option	Description
Generate a Report	Creates a report.
View Existing Report	Displays an existing report.
Load Existing Report	Loads an existing report.
Regenerate Index.htm	Re-creates the index.htm portion of the report.
Add to Report	Adds only the values from the highlighted subkey.
Add to Report with Children	Adds the values from the highlighted key or subkey and all of the subkeys below the parent.
Remove from Report	Removes the selected subkey from the report.
Clear All Report Entries	Removes all of the areas marked to include in the report.
Manage Summary Reports	Executes or modifies existing Registry Summary Reports.
Define Summary Reports	Creates a new Registry Summary Report.
Export Word List	Export all of the string values from the registry in a text file. This file can be used to create a custom dictionary in PRTK.
Generate File Types Report	Creates an HTML report based on the file associations in the Classes subkey in the Software registry.

View Menu

Option	Description
Full Registry	Displays the full registry in the Key Tree pane.
Report Items	Displays only the keys and subkeys marked for the report in the Key Tree pane.
Common Areas	Displays only keys and subkeys marked as Common Areas.
Toolbar	Turns the Toolbar on or off.

Status Bar	Turns the Status Bar on or off.

Appendix for Activity A.2:

1. Go to the Explore tab.
2. Click the icon on the file list toolbar to uncheck (deselect) all files in the case.
3. Set the QuickPicks focus on the top of the evidence tree so that all items in the case are visible.
4. (Conditional) If not already done, sort the file list by Name.
5. Using the typedown feature, locate the Pagefile.sys files.
6. Check (select) both of the Pagefile.sys files in the case.
7. Click the Live Search tab.
8. Note how the options differ from Index Searching.
9. Select the Pattern search sub-tab.
10. Click the icon to view the available regular expressions.
11. Click Edit Expressions to open the default regular expressions in Notepad.
12. Close Notepad.
13. Click the icon, then select Credit Card Standard.
14. Click Add.
15. At the bottom of the Pattern Search Terms window, select Checked Files from the Search Filter pull-down menu.
16. This is not a tab filter.
17. Click Search.
18. In the Live Search Results pane, expand Live Search > Pattern Query > Allocated.
19. Expand the pagefile.sys hits and review the data results.
20. In the File Content Viewer, scroll up to locate the beginning of the text fragment.
21. Click-and-drag in the Hex view to highlight the recovered data (approximately 422 bytes).
22. Right-click the highlighted data, then click Save Selection as a Carved File.
23. In the Save Carved File As window.
24. In the Save Carved File As window, name the carved file “Recovered CC Numbers.txt”.
25. Select Create a Bookmark and Assign Type as Text.
26. Click Add to Case.
27. In the Create New Bookmark window, name this bookmark “Recovered Text”, then select Username as the Bookmark Parent.
28. Navigate to the Bookmarks tab to view this new bookmarked item.
29. Reset the Search Filter on the Live Search tab to Unfiltered and clear all search results.
30. Uncheck all files in the case.

(FIT3168 post-class) ACTIVITY D: Wireshark

Files required:

- Lubuntu virtual machine (username/password: user/user).

PREPARATION

1. Download the Lubuntu virtual machine from the following link https://s.id/2c0rP. There will be two files to download:
    - Lubuntu.vbox (6KB)
    - Lubuntu.vdi (6GB)
2. Download both files and store the files in a new folder under your Authcate folder.
3. Double-click the Lubuntu.vbox file and it will be automatically shown in VirtualBox or VMware application.
4. The Lubuntu virtual machine will be used to do Activity A and Activity B.

Wireshark is used to capture network traffic from a selected network interface. Follow the instructions below to conduct a live capture. Do all of the following steps using Lubuntu virtual machine.

1. Run the Wireshark from the desktop. Choose enp0s3 or other network interface, whichever has any network activities. After a network interface is , the Wireshark starts recording.chosen
2. Access the following URL from a web browser: http://users.monash.edu/~guidot/test.html. Note that if you have accessed the URL, the web browser will show the cache, hence Wireshark will record different network packets.
3. Once the URL is fully loaded, stop the Wireshark.

Observe and answer the following questions:

1. Source address + port and destination address + port of captured packets related to accessing the URL.
    a. The request packet(s)
    b. The response packet(s)
2. Describe how the client and the server establishes a connection.
3. Describe how the client and the server terminates a connection.
4. Observe how Wireshark helps the users to read the network packets.
    a. Display filter.
    b. Search (hex value, string, regular expression).
    c. Related network layers for each network packet. Find the difference.
    d. Show a specific TCP session in one page.