IFS4102 (Digital Forensics) Assignment 1:
Memory, Disk and File-System Forensics

Due Date: Thursday, 2 March 2023, 23:59 SGT

Introduction & Assigned Mission

In this assignment, you will play the role of a Digital Forensic Investigator. Your **mission** is to investigate your target computers by analyzing the given captured **memory & disk image files**. To this end, you will need to use forensics tools that have been covered in **Labs 1-5**, including Volatility, TSK, and Autopsy.

Instructions and Deadline

This is an **individual** assignment. You MUST finish the assignment and report **independently**. Note that your report may be checked by the available anti-plagiarism service.

Please prepare your report in a self-contained **PDF file** by using your name and matric number as part of your file name. For example, Jack Lee with Matric No A001 should submit the filename JackLee-A001-A1.pdf. (*Note*: If you submit multiple files to the Canvas' assignment, a counter suffix is automatically added for version tracking purposes. We will take your latest submission there.) Your report should also contain your name, matric number, and email address on its first page.

Do upload your PDF file to Canvas' `Assignment-1` by **Thursday, 2 March 2023, 23:59 SGT**. There will be **no deadline extensions**, and there will be following **penalties for late submissions**:

- Late up to 5 hours: 10% penalty to your obtained marks.
- Later than 5 hours but no later than 1 day: Maximum possible marks are capped at 80%.
- Later than 1 day (*subject to approval only*): Maximum possible marks are capped at 60%.

Grading Scheme

By correctly answering all the questions asked in this assignment, you will get the possible **30 marks**. This assignment is worth **15%** of your final score.

In addition to answering the questions, your must also succinctly describe the ***methods*** that you have used to find the answers: by giving **the whole command lines invoked (including all their arguments)** and/or attaching **some screenshots of your GUI-based tools** as requested. Note that giving the correct answers but without providing the complete commands or screenshot(s) will give you **partial marks** only!

Good luck, and have fun with your mission!

Challenge 1: Analyzing a Memory Dump File of a Target Windows Machine (10 marks)

Given Scenario and Task:

- You are given a **mystery memory dump file** named `memory-dump.img`. Its zipped file, named `memory-dump.zip`, can be found in the `Assignments / Assignment-1` folder of our Canvas' Files. The MD5 hash value of the .img file is `8caa17c3d30aadff223f044ee7cf60f0`. Please ensure the integrity of your extracted image file before you start analyzing it.
- Your **task** is to analyze **the state of the target machine** when its memory was acquired by answering all the questions below (**1 mark** for each question). ***Please remember again to include your invoked full commands or attach screenshot(s) of GUI-based tools together with your answers***.

Questions:

1. What was the OS version of the target computer from which the memory was captured?
   List the 2 most-likely version profiles as reported by Volatility.
2. What was the address-space type of the machine reported by Volatility?
   Based on the value given, mention the processor type used and whether it was a 32 or 64-bit machine.
3. List the PID and executable name of all active processes that were running when the memory was captured.
   Note: You can copy and paste the output of the command that you run.
4. There was a text-editor application running at the acquisition time.
   Mention the executable name associated with that application and also its PID (process ID).
5. You also want to find out how the text editor was invoked in the first place.
   Tell the PID of a process that was used to spawn the text-editor's process, its executable name, and when the process was started.
6. At the acquisition time, what DLLs were loaded by the text-editor application's process?
   Note: You can copy and paste the output of the command that you run.
7. What were the user name and Windows domain of the user running the text-editor application?
8. What were the files that the text editor had access to at the acquisition time?
   List the full pathname of the files.
   Note: You can just list *unique* file pathnames reported.
9. List the executable name, PID, and exit time of processes that *had terminated* (became inactive) before the acquisition time.
   Note: Do not include processes that were *still active* at the acquisition time.
10. At the acquisition time, the machine had a UDP port open for Network Time Protocol (NTP) communication.
    Tell the UDP port number used, PID and executable name of the process related to the port.

Challenge 2: Analyzing a Disk Image File of a Target Machine (10 marks)

Given Scenario and Task:

- You are given a **mystery disk image file** named `disk-dump.E01`, which can also be found in the `Assignments / Assignment-1` folder of the Canvas' Files. The MD5 hash value of the file is `96e8b80bef70b15bc1192515ad0994aa`. Please ensure the integrity of your downloaded image file before you start analyzing it.
- Your **task** is to analyze **the media & file system of the machine** by answering the questions below (**1 mark** for each question). ***Again, please remember to include your invoked full commands or attach screenshot(s) of GUI-based tools together with your answers***.

Questions:

1. What are the allocated and unallocated partitions contained in the acquired disk?
   Also specify the total number of sectors in each listed partition.
2. What is the file-system type of an accessible partition contained in the disk?
3. What are the volume ID and named volume label of the file system?
4. What are the sector size (in bytes) and cluster size (in bytes) of the file system?
5. How many sectors are allocated to the *data area* of the file system?
6. Name the deleted and undeleted *user-created* directories/folders that reside at the root directory of the file system.
7. List all *deleted* files and directories (in their full pathnames) in the whole file system.
   Note: You can copy and paste the output of a suitable tool that you can use. However, do *not* include any undeleted files/directories.
8. What is the file metadata no (similar to inode no in UNIX/Linux) allocated to a directory named `Personal` that resides at the root directory?
9. What is the file name associated with the file metadata no 190?
   If you use TSK, use a *single* TSK command (without using any additional Linux text-filtering commands) that directly gives you the required file name.
10. What are the recorded MAC times of a folder named `Home` that resides at the root directory according to the times recorded within its file metadata?

Challenge 3: Automatically Analyzing the Files in a File System of a Target Disk (10 marks)

Given Scenario and Task:

- You still want to use the disk image file named `disk-dump.E01` given for Challenge 2. Again, the MD5 hash value of the file is `96e8b80bef70b15bc1192515ad0994aa`.
- Your **task** is to analyze **the files contained in the file system of the machine** by answering the questions below (**2 marks** for each question) using **Autopsy** (with the appropriate ingest modules).
  Please remember to attach ***screenshots of Autopsy as your proof-of-work*** *together with* ***your requested answers*** *to the given questions below!*

Questions:

1. Do use Autopsy to find out all deleted text files (with .txt extension).
   Tell the full pathnames of the files and the last time they were modified.
   Also attach **a screenshot of your Autopsy** listing all the identified files.

2. Use Autopsy to find files in the file system (including those inside an archived/zip file) that match the following listed *hash values/digests*:

   - a2a8da835c7341b606f10805fba26687
   - ea2ef30c99ececb1eda9aa128631ff31

   Tell the full pathnames of the files (relative to the root directory of the file system).
   Also attach **a screenshot of your Autopsy** listing all the identified files.

3. Use Autopsy's *Interesting Find Identifier* module to find all files (either with existing or deleted status) in the file system, whose **file name** contains the *substring* "`tool`".
   Tell the full pathnames of the files.
   Do attach **a screenshot of your Autopsy** listing all the identified files.
   Also tell which among them are already deleted by giving their MD5 value as well.

4. Use Autopsy's *Keyword Search* module to mine all **email addresses** in all the files.
   List the email addresses together with their respective associated file(s).
   Note: You can omit the folder part of the pathnames in you answer, but do include all files with the same name but located in different folders.

5. Use Autopsy's *Keyword Search* module again to list all text files (with .txt extension) whose **content** contains the *substring* "`password`".
   For each file listed, mention all the matching keywords (full words) as reported by Autopsy.

— End of Assignment —