Digital Forensics (IFS4102) Lab 3: Live Acquisition & Image Analyses

Lab Objectives

In this lab, you will perform a **live/volatile data acquisition** to create the **memory image/dump file** of your running target computer. You will then **inspect** the created image file, and analyse the state of the computer at the acquisition time. Subsequently, you will inspect the **disk image file** that you created in Lab 2, and start analysing the disk using **Autopsy**, including by recovering its deleted files.

More specifically, the objectives of Lab 3 are as follows:

1. To perform a live/volatile memory acquisition of a running, accessible target Windows machine using:
    a. **FTK Imager Lite**;
    b. (Optional) **FireEye's Memoryze**.
2. To access and inspect the created live/volatile memory image file of your target machine using a few available tools:
    a. **Volatility**;
    b. **FTK Imager**;
    c. (Optional) A **hex editor** like WinHex.
3. To start familiarising yourself with the GUI-based **Autopsy forensics suite** by inspecting a disk image file that you created in Lab 2, and identifying **deleted files** in the acquired disk.

Task 1-A (Win-FWS): Performing a Live/Volatile Acquisition of a Windows Machine using FTK Imager Lite

Important Notes:

- In this exercise, you are going to perform a live/volatile acquisition of a target **Windows** machine's RAM by using **FTK Imager Lite**.
- You will first use your Windows forensic workstation to **copy** the FTK Imager executable files into your prepared thumb drive. Then, you also want to use the ***thumb drive*** to store the created memory image file when possible. Due to this, the free space of your thumb drive **must be larger than the size of the RAM** of your target machine/VM. Alternatively, you can attach an external hard drive to an available USB port of your target machine. (You do *not* want to use *your target machine's hard drive* since you do not want to modify the evidence drive!)

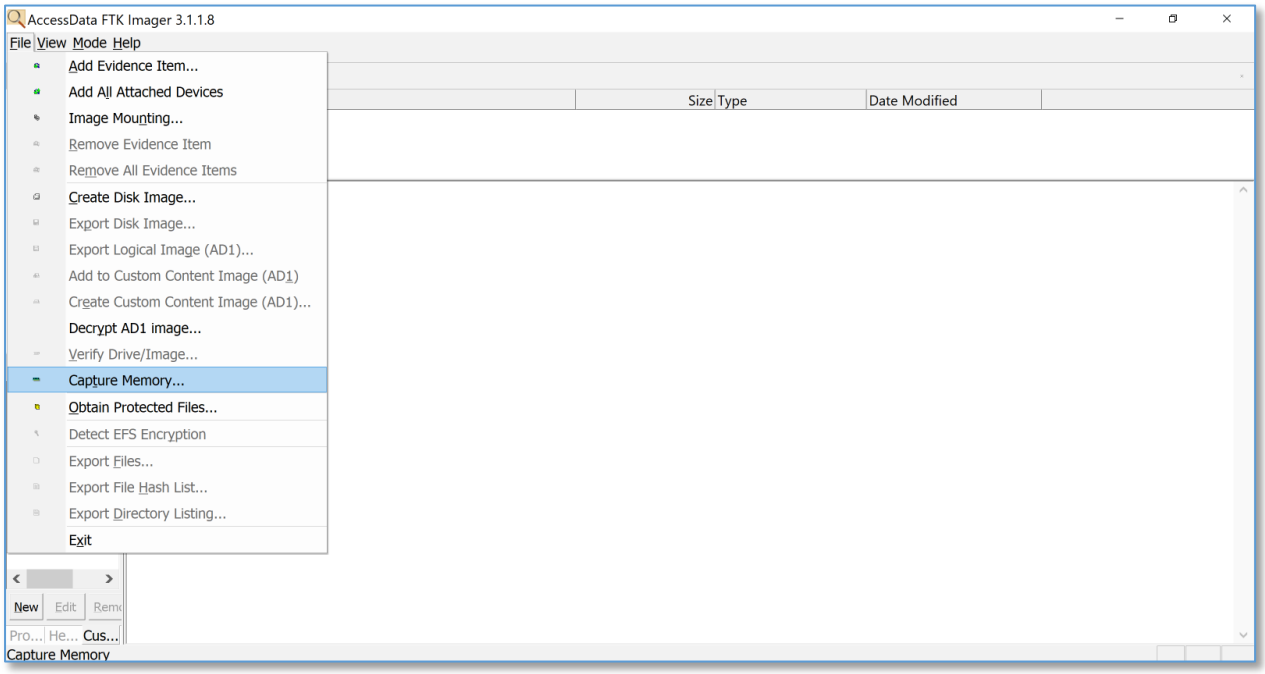
Steps:

1. You have previously downloaded and installed **FTK Imager** on your Windows forensic workstation. For this task, you need to create a portable **FTK Imager Lite** from your FTK Imager installation folder by following the steps outlined in: https://exterro.freshdesk.com/support/solutions/articles/69000765662-run-ftk-imager-from-a-flash-drive-imager-lite-.

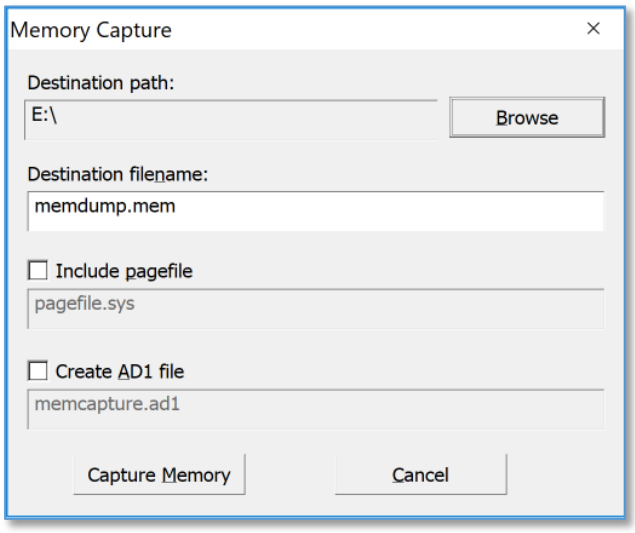
   Note that if you use a 64-bit version of FTK imager (version 3.4.3 and higher), also do the **steps in the "*Please note*" section** of the article. Otherwise, errors may occur about missing Microsoft Foundation Class (MFC) files.

2. Once your FTK Imager Lite is ready, insert your thumb drive to your target machine's USB port, and then run "FTK Imager.exe" (as Administrator).

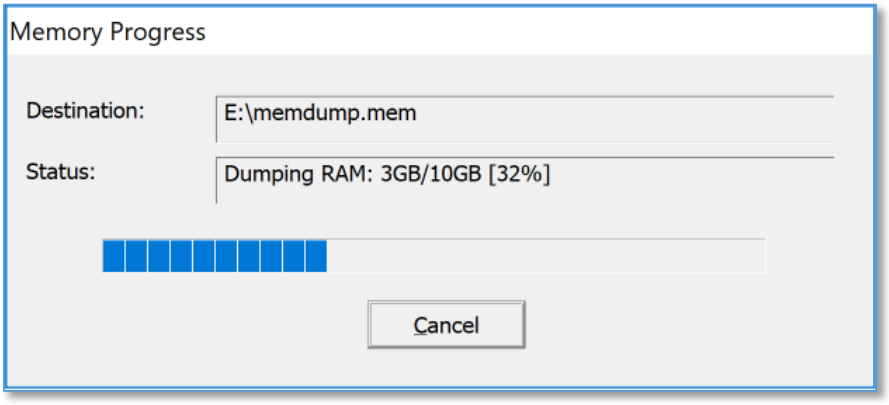
3. From its main menu, select “File” and then “Capture Memory…” as shown below (note that the UI of your latest downloaded version of FTK Imager may be slightly different from the screenshots given below):



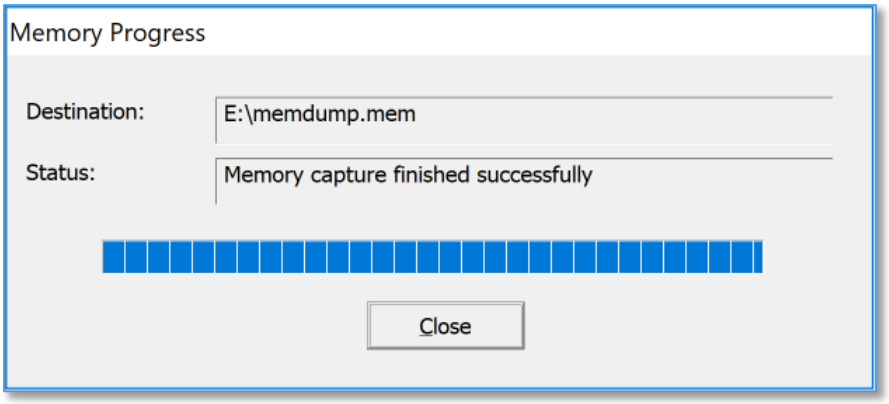
4. Set the destination path shown below. Please set it to either your thumb drive or external USB-connected storage. Then, click the “Capture Memory” button.



5. FTK Imager Lite will show the status of the memory capturing process.



6. Once the memory dump is completed, the following window will be shown:



7. Using File Explorer, verify that the memory dump file has been successfully created. Also check its file size.

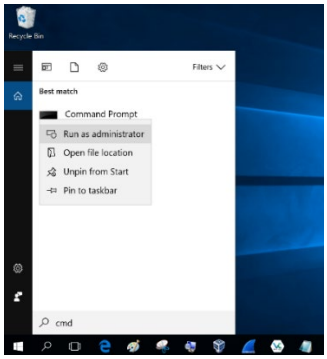
[Optional] Task 1-B (Win-FWS): Performing a Live/Volatile Acquisition of a Windows Machine using FireEye's Memoryze

Notes:

- Now, you want to do a live/volatile acquisition of the same target **Windows** machine again, but by using **FireEye's Memoryze**.
- The **User Guide** of FireEye Memoryze has been uploaded to Canvas' Files. Please refer to the PDF file for other useful functionalities of Memoryze in facilitating memory forensics.
- For this task, if you use your Windows forensic workstation as your acquisition target machine as well, then skip Steps 6 and 7 below.

Steps:

1. Connect your USB thumb drive to your Windows forensic workstation.
2. Download FireEye Memoryze's zipped installation file from: https://fireeye.market/apps/211368, and then extract the downloaded zip file into your machine's Desktop.
3. Go to your Windows' start or search button to find `cmd.exe` (Command Prompt). Right-click the Command Prompt's icon, and then select "Run as administrator" as shown below.



4. At the Command Prompt, change your directory to the Desktop where you put the downloaded file MemoryzeSetup3.0.msi, e.g.:
   `cd C:\Users\<User-name>\Desktop`.

5. At the Command Prompt, type the following command to install Memoryze executables into your USB thumb drive (by assuming **`D:`** as the drive letter assigned to your USB thumb drive, and **`\Memoryze`** as the folder that you want to create in that drive):
   `msiexec /a MemoryzeSetup3.0.msi /qb TARGETDIR=D:\Memoryze`

6. Eject the thumb drive.

7. Now, connect the prepared thumb drive to your ***target machine's*** USB port.

8. Run `cmd.exe` (Command Prompt), again by selecting "Run as administrator".

9. At the Command Prompt of your target machine, type the following batch-file command to **acquire the volatile memory** of the machine (by assuming `D:` as the drive letter assigned to your USB thumb drive, and that your target machine is a 64-bit machine):
   `D:\Memoryze\x64\MemoryDD.bat -output D:\<output-pathname>`

10. As explained in the uploaded Memoryze's User Guide, you can additionally specify the `-offset` and `-size` options if desired.

11. Please wait until the acquisition completes. (*This can take some time depending on your target computer's RAM size*.) Also notice that you may see some *warning messages* shown while Memoryze is imaging the computer's memory.

12. The image file is stored in <*output-pathname*>`\Audits\`<*machine*>`\`<*date*> folder, where: <*machine*> is the machine name, and <*date*> is a date/time stamp in the format of YYYYMMDDHHMMSS. In that folder, you should find the dumped memory image file, which is named as `memory.*.img`.

Task 2-A (Win-FWS/Lin-FWS): Inspecting a Memory Image File of a Windows Machine using Volatility

Important Notes:

- In this lab, you will use **Volatility** to inspect the *live/volatile* memory image file of your target *Windows machine*. There is recently released **Volatility 3** (Python 3 Rewrite), yet its set-up is more elaborate. For our task, let's just use **Volatility 2.6** which runs as a standalone executable.
- Volatility 2.6 is available for Windows and Linux. The steps below are to be done on a Windows machine. Yet, you can also inspect the memory image of a Linux machine using various operations/plug-ins that start with `linux_*` instead.
- Use your memory image file created in Task 1 of this lab. Alternatively, you can use a file named `memory.zip` which can be downloaded from: https://drive.google.com/file/d/14Ff2EakVS2VqWi5GV3A7VKrqQ_Ioco3/view?usp=sharing. Unzip the file to obtain the given sample memory dump file **`memory.img`**.
- A cheat sheet PDF on using Volatility has been uploaded to Canvas' Files. Please refer to the file for other commonly used commands.

Steps:

1. Download Volatility 2.6 Windows Standalone Executable (x64) from http://www.volatilityfoundation.org/26, and save it to *Path-to-folder* folder. For convenience, you can also put `memory.img` into the same folder.
2. Get some **information of the image** by invoking:
   Path-to-folder > `volatility_2.6_win64_standalone.exe -f memory.img imageinfo`

(Note that this step may take very long depending on the used image size.)
What are the image profiles suggested by Volatility?

3. With `Win7SP1x64` profile selected, print all running processes using:
   Path-to-folder > `volatility_2.6_win64_standalone.exe -f memory.img --profile=Win7SP1x64 pslist`

4. *To list the running processes in a hierarchical tree format, use:
   Path-to-folder > `volatility_2.6_win64_standalone.exe -f memory.img --profile=Win7SP1x64 pstree`

5. To print all loaded DLLs of each process, run:
   Path-to-folder > `volatility_2.6_win64_standalone.exe -f memory.img --profile=Win7SP1x64 dlllist`

6. To dump/extract DLL files of a process with pid=*pid* to drive `E:\`, invoke:
   Path-to-folder > `volatility_2.6_win64_standalone.exe -f memory.img --profile=Win7SP1x64 dlldump --pid=`*pid* `--dump-dir E:\`

7. To find out the command line arguments issued to run a process with pid=*pid*:
   Path-to-folder > `volatility_2.6_win64_standalone.exe -f memory.img --profile=Win7SP1x64 cmdline --pid=`*pid*

8. *To extract command history by scanning `_COMMAND_HISTORY`, run:
   Path-to-folder > `volatility_2.6_win64_standalone.exe -f memory.img --profile=Win7SP1x64 cmdscan`

9. To extract command history by scanning `_CONSOLE_INFORMATION`, invoke:
   Path-to-folder > `volatility_2.6_win64_standalone.exe -f memory.img --profile=Win7SP1x64 consoles`

10. To scan for network connections and sockets, run:

Path-to-folder > `volatility_2.6_win64_standalone.exe -f memory.img --profile=Win7SP1x64 netscan`

11. To discover more about the target machine from its dumped RAM memory, run other available Volatility plug-ins as listed in:
https://github.com/volatilityfoundation/volatility/blob/master/README.txt

Important Note:

- Two (2) selected steps above are marked with *, which should be run using the given sample memory dump file `memory.img`.
Please refer to the "**Graded Lab Tasks #1**" Section on **page 17**.

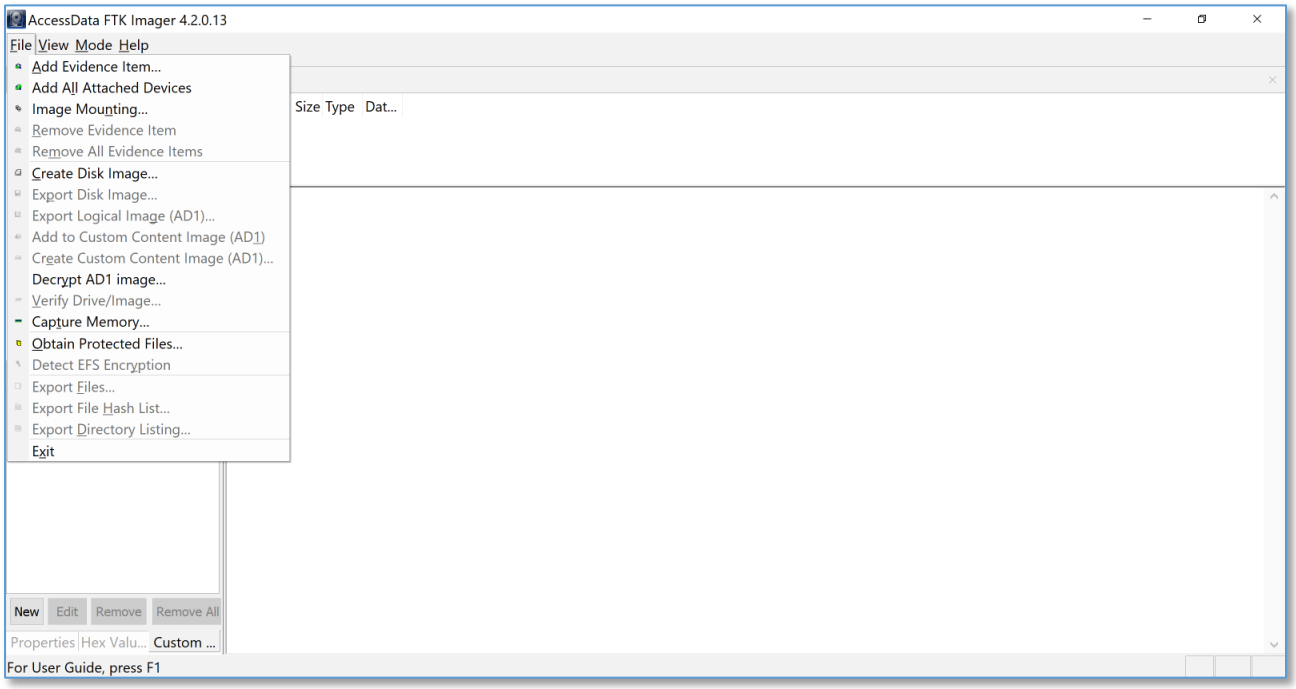
Task 2-B (Win-FWS): Inspecting a Memory Image File of a Windows Machine using FTK Imager

Important Notes:

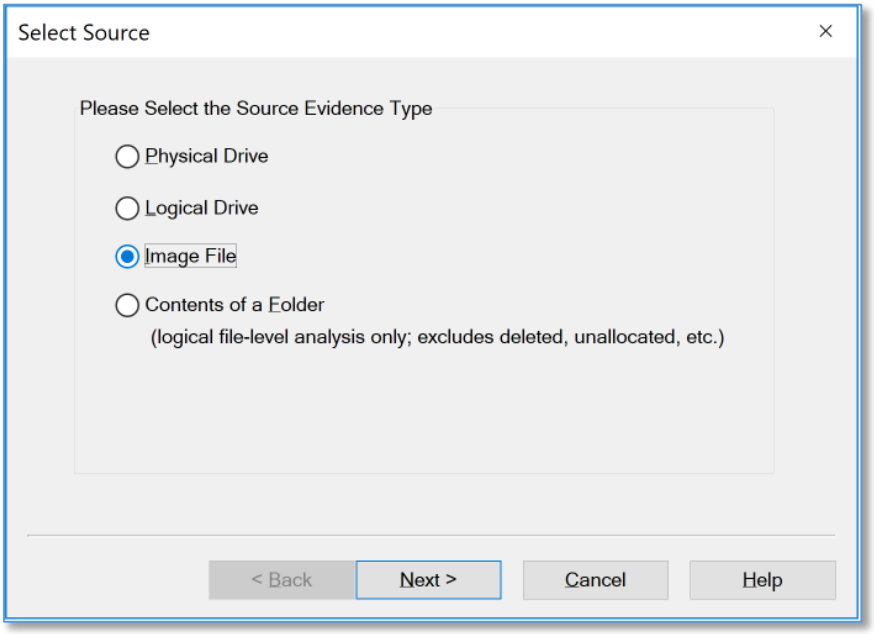
- **FTK Imager** can also be used to **manually** inspect the live/volatile memory image of a target machine. In this exercise, you want to find the occurrences of a **particular string** in the dumped memory image.
- Use the sample memory dump file "`memory.img`" given in Task 2-A.

Steps:

1. Launch FTK Imager.
2. From its main menu, select "File", and then select "Add evidence file…" as shown below:



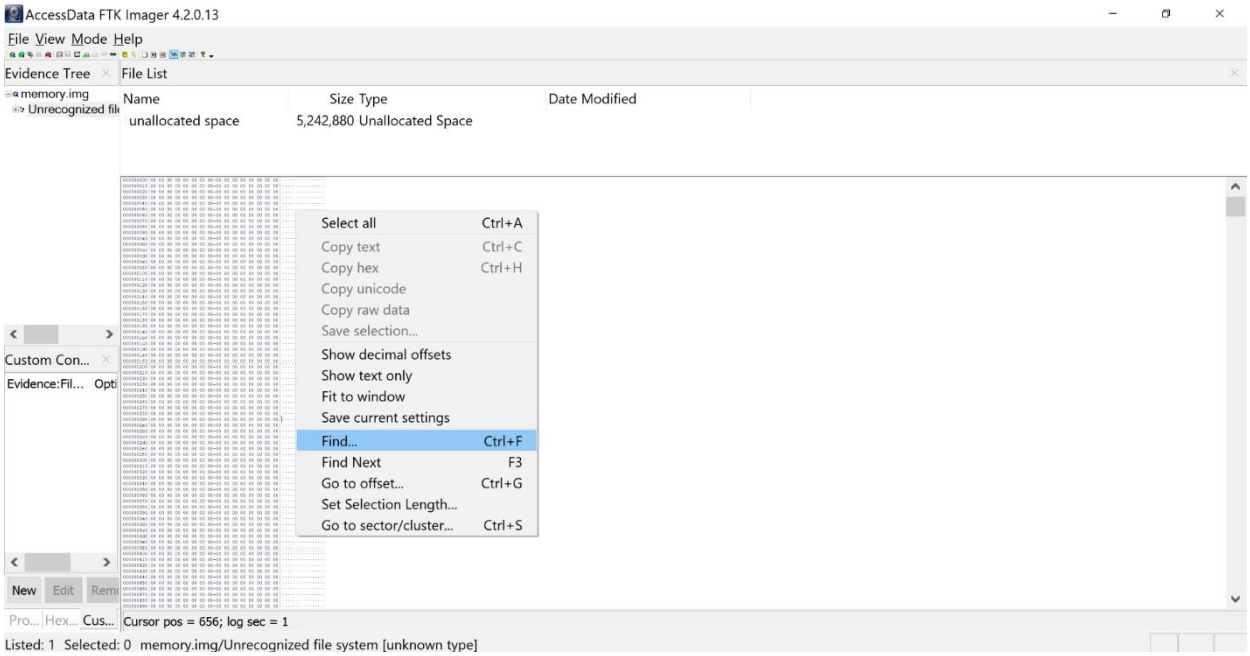
3. Select “Image File” as your source evidence type, then click the “Next” button:



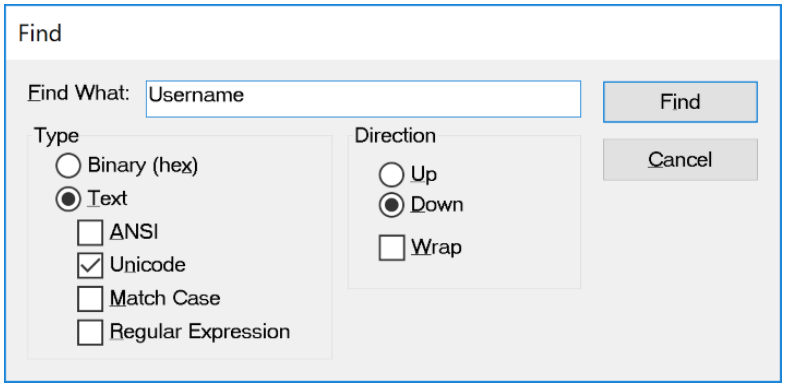
4. Browse to your image file location, and click the “Finish” button.

5. Select the added image in the “Evidence Tree”.

6. Right-click in the Viewer pane, and select “Find…” as shown below.



7. Enter a string that you want to find in dumped the memory, such as “Username” as shown below:



8. Can you find the string in the memory?

   Please find the next occurrences of the string by pressing F3 (find next).

[Optional] Task 2-C (Win-FWS): Inspecting a Memory Image File of a Windows Machine using a Hex Editor (WinHex)

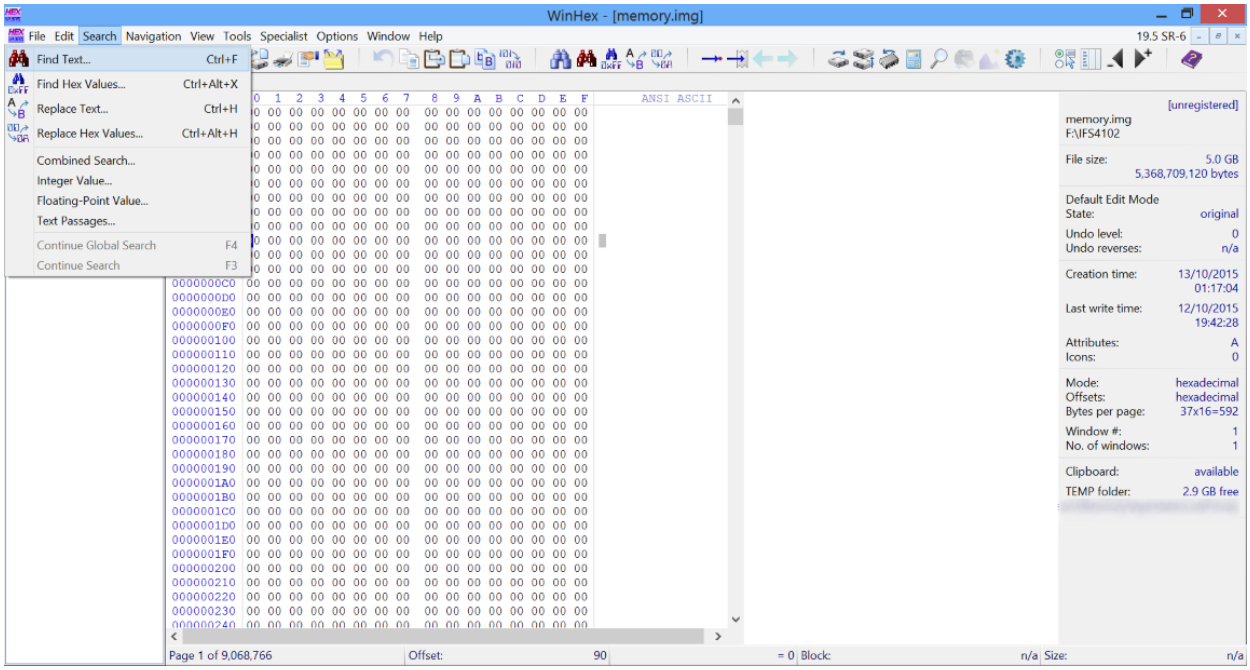
Important Notes:

- A ***hex editor*** can be used to inspect the live/volatile memory image of a target machine. In this exercise, you want to repeat Task 2-B using a hex editor, such as WinHex. **WinHex** is a handy tool, which you will use for file analysis and manipulation tasks in your subsequent labs as well. You can download WinHex from https://www.x-ways.net/winhex/. It is a fully portable application that can be executed without any installation. Launch WinHex simply by invoking its executable `WinHex.exe`.
- You can also use your other favourite hex editor, including one listed on https://en.wikipedia.org/wiki/Comparison_of_hex_editors. **010 Editor**, for instance, is also a very popular hex editor which can run on Windows, Mac and Linux. Note that 010 Editor is a commercial tool, whose trial version can be run for free for 30 days only.
- Use the same sample memory dump file "`memory.img`".

Steps:

1. Download **WinHex** from X-Ways' web site https://www.x-ways.net/winhex/.
2. WinHex is a fully portable application that can be executed without any installation. Launch WinHex simply by invoking its executable `WinHex.exe`.
3. Open the target image file.

4. Click “Search” menu, and then select “Find Text…” as shown below.



Task 3 (Win-FWS/Lin-FWS): Familiarising Yourself with Autopsy Suite by Inspecting a Disk Image File

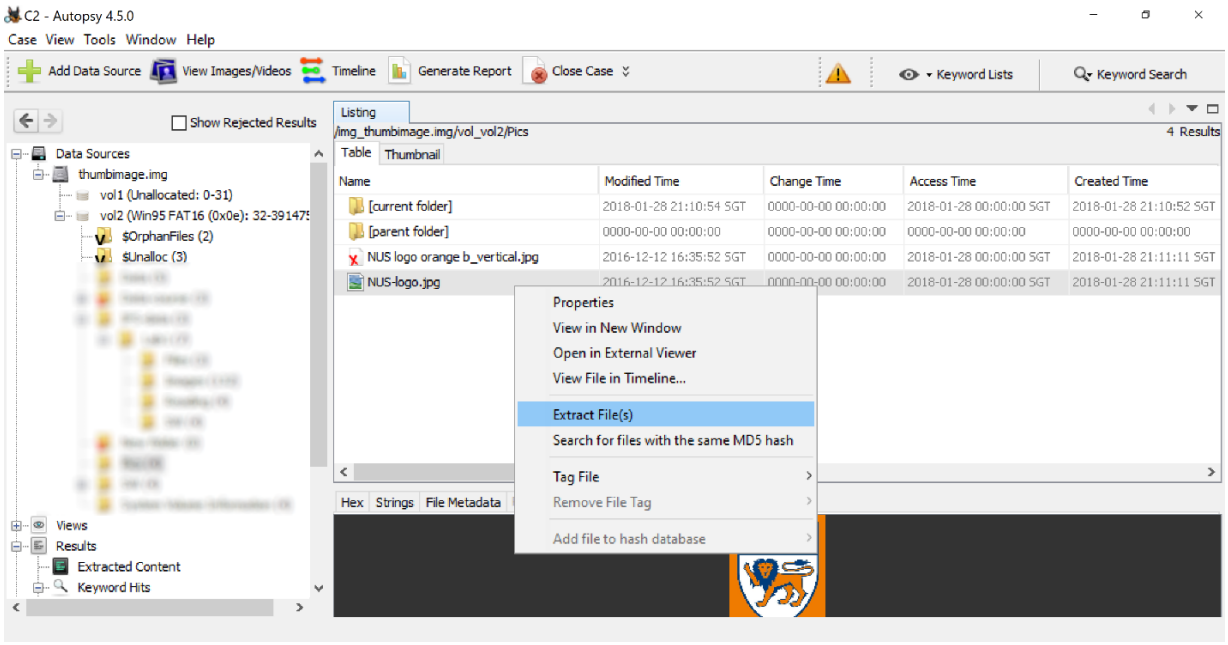
Important Notes:

- In this exercise, you want to start using **Autopsy** to inspect a created disk image file and **extract a file of interest**, including a previously deleted file. (Other tasks of employing Autopsy's available ingest modules will be done in our *next two labs*).
- Download the suitable version of Autopsy for your forensics workstation from https://www.autopsy.com/download/. The **Windows** version will be used in the steps below.
- Use the acquired **disk image file** of your thumb drive, which you created by using either FTK Imager or `dd*` tools in your Lab 2. Like before, you can alternatively use a given sample disk image named "SuspectDrive1.E01" downloadable from https://drive.google.com/file/d/1SiJOaWEmKYyXXKI-PEJP3-I2j1iOC_p3/view?usp=sharing. If you still need to verify this image, its MD5 value is b66270513117670d11ebe2191e947a6d.

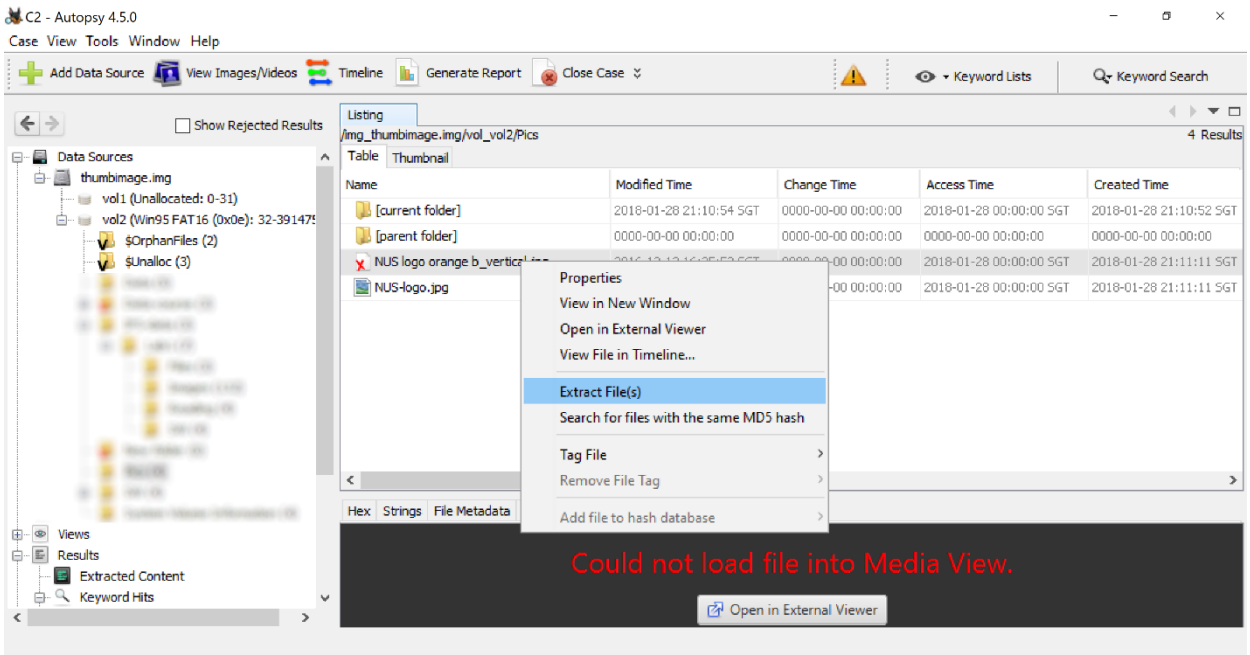
Steps:

1. Launch Autopsy, and enter your case's information.
2. Select the desired ingest modules to apply.
   For now, you may just *deselect* all.
3. Add the target image file as an evidence file.
4. Navigate the evidence tree and browse the file system.

5. Extract an *existing* target file to extract (e.g. NUS-logo.jpg) by right-clicking it as shown below:



6. Next, identify a *deleted* target file (e.g. "NUS logo orange b_vertical.jpg"), which is marked with a red cross sign on its file icon, and then extract it:



Graded Lab Tasks #1 (1 Mark)

As previously mentioned, you will be asked to answer some questions from your lab tasks for your **lab-practice marks**.

From your this Lab 3, you will need to submit **your 2 answers** using the given **sample image file** `memory.img` according to the following instructions:

- The selected **2 questions** are:
  - **Task 2-A, Step 4 (page 8)**: Please copy and paste the **first 30 lines** of the output (including *any header* included) only. If there are less than 30 lines, then just copy and paste all the lines.
  - **Task 2-A, Step 8 (page 8)**: Please copy and paste (up to) the **first 30 lines** of the output.
- From your correct 2 answers, you will earn a total of **2 * 0.75 = 1.5 marks**.
- This graded lab task assignment is an **individual** assignment.
  Hence, you MUST finish the assignment and report **independently**.
- Please prepare your answers 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-**GLT**1.pdf. Your report should also contain your name, matric number, and email address on its first page.
- Upload your PDF file using **`Graded-Lab-Tasks-1`** Canvas Assignment by **Saturday, 4 February 2023, 23:59 SGT**. Note that this deadline is a ***firm & final*** **deadline**. There will be ***no*** deadline extensions.
  As such, you are advised to submit **well before** the cut-off time so as to avoid any technical issues with Canvas or your uploading!

Have fun with your assigned lab tasks! :)