Digital Forensics (IFS4102) Lab 5: File and Windows Forensics

Lab Objectives

In this lab, you are going to perform additional ***file forensics tasks***, including **file carving** and some file-analysis tasks using **Autopsy**. Furthermore, you will also start performing some ***Windows forensic tasks***. More specifically, you want to:

1. Perform an ***automated*** **file carving** on a target disk image using:
    a. Carver Recovery (which utilizes Scalpel);
    b. Bulk Extractor.
2. *(Optional)* Perform a ***manual*** **file carving** of a deleted file using FTK Imager.
3. Use **Autopsy** to perform the following file-analysis tasks:
    a. Find **interesting files** using the *Interesting File Identifier* module;
    b. Perform **keyword search** using the *Keyword Search* module.
4. Extract and analyse **offline registry files** of a target Windows machine in both **manual** and **automated** fashions:
    a. Manual extraction and analysis using RegEdit;
    b. *(Optional)* Automated extraction and analysis using RegRipper.

Note: *Before* you start your lab, you may want to **download** the shared sample data files, especially a large (>1GB) sample disk image used in Tasks 1 and 2.

Task 1-A (Win-FWS): Performing an Automated File Carving on a Target Disk Image using Carver Recovery Notes:

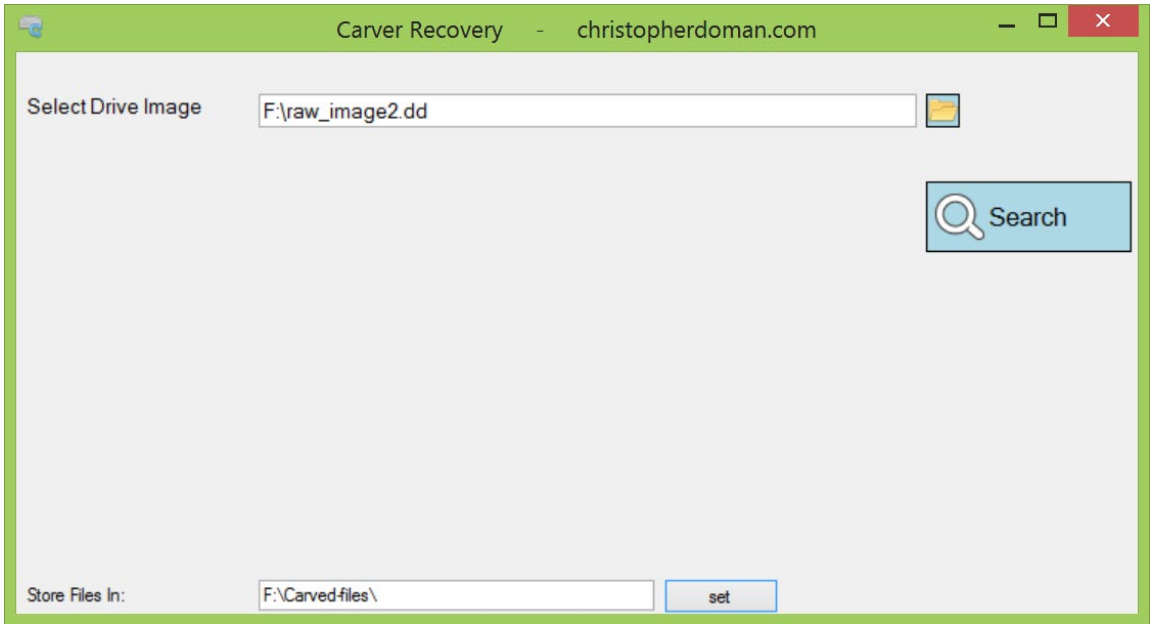
- In this exercise, you want to use an ***automated*** **file carving tool** named **Carver Recovery**, which actually utilizes **Scalpel** (https://github.com/sleuthkit/scalpel) using a customized config file.

- You can observe the automated steps first, and **compare** them later with manual file carving steps in the optional Task 2 below.
- You can use a sample disk image "raw_image2.dd" downloadable from: https://drive.google.com/file/d/1ExdsTlfrlavxgb0fTrWDxcJcybkY5PC5/view?usp=sharing. Note that the file is **slightly larger than 1GB**.
  Its MD5 value is b85ee299a11295ec8bbec95aef7c3b11.

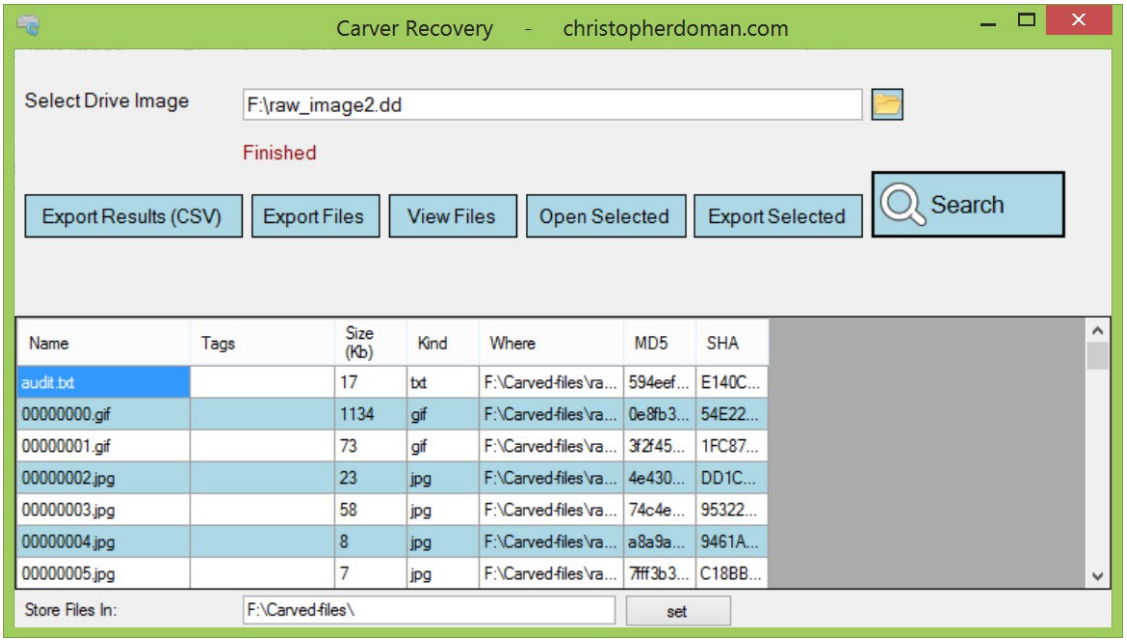
Steps:

1. Download Carver Recovery from https://code.google.com/archive/p/carver-recovery/.

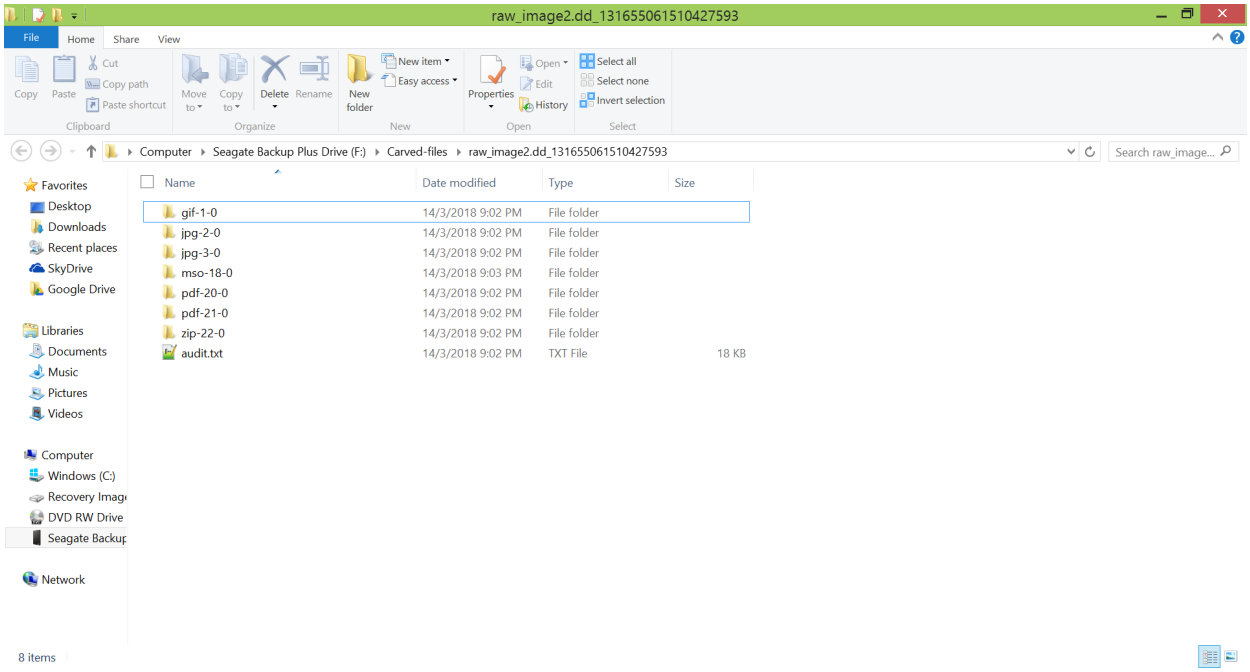
1. Launch Carver Recovery.
2. Set "Select Drive Image" to your downloaded "raw_image2.dd".
3. Create a folder, and set it as the output folder ("Store Files In") as shown below.



4. Click the "Search" button to start an automated carving.
5. The results are shown as below:



6. Now, check all the carved files in the specified folder as shown below. Note that the file "audit.txt" is the log the tool's process, and not a recovered/carved file.



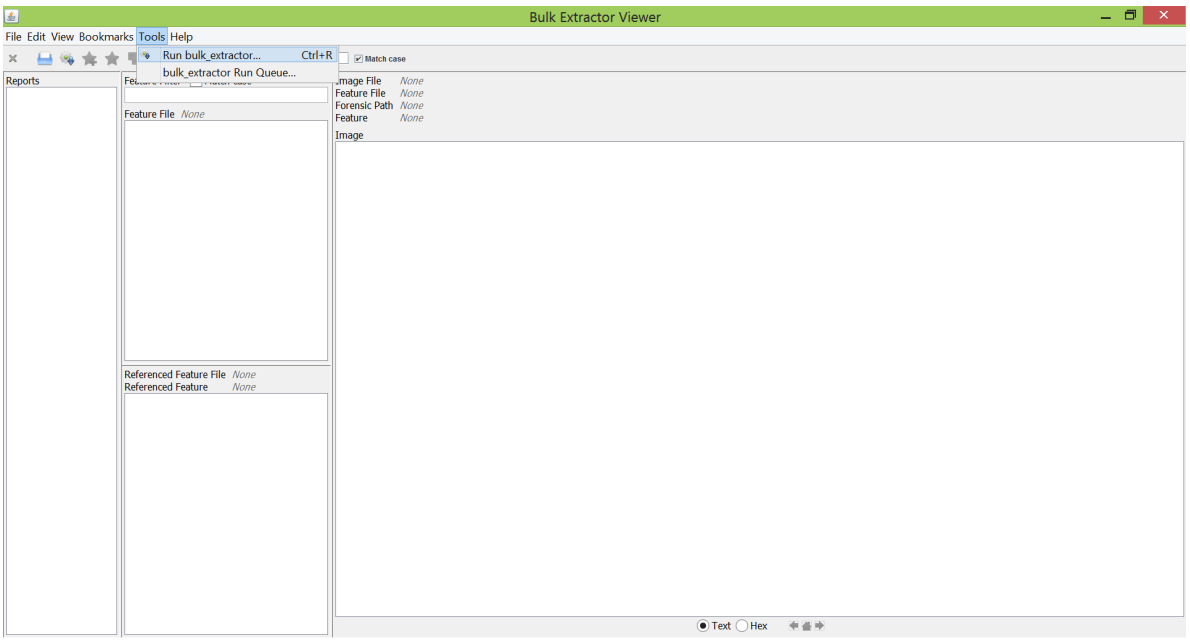
Task 1-B (Win-FWS): Performing an Automated File Carving on a Target Disk Image using Bulk Extractor

Notes:

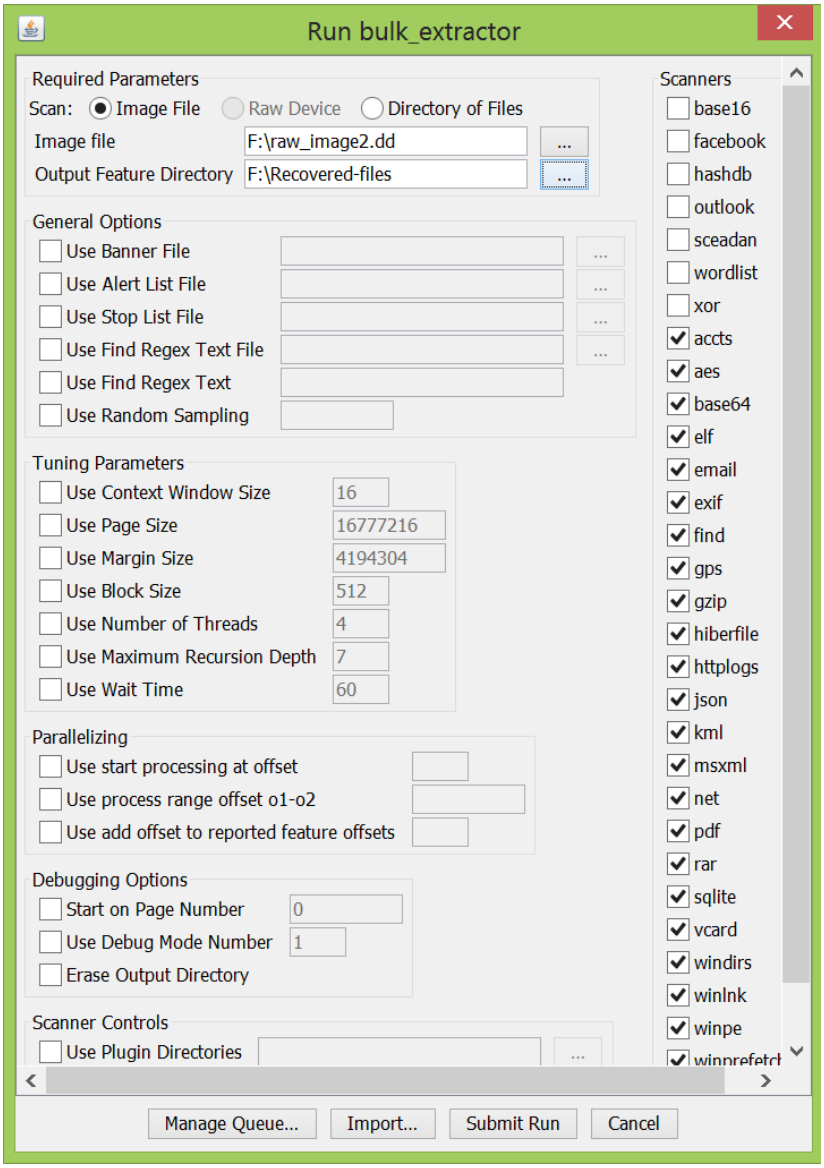
- Now, you want to use another popular **automated file carving tool** called **Bulk Extractor**. You can refer to its project site at: https://github.com/simsong/bulk_extractor. You can also download https://digitalcorpora.s3.amazonaws.com/downloads/bulk_extractor/BEUsersManual.pdf for its user manual.
- You can reuse the given sample disk image file "raw_image2.dd".

Steps:

1. Download Bulk Extractor's executable from http://downloads.digitalcorpora.org/downloads/bulk_extractor/, and install it.
2. Launch Bulk Extractor Viewer.
3. From its main menu, select "Tools" then "Run Bulk Extractor" as shown below.



4. In Bulk Extractor, set the “Image File” and “Output Feature Directory” as shown below.



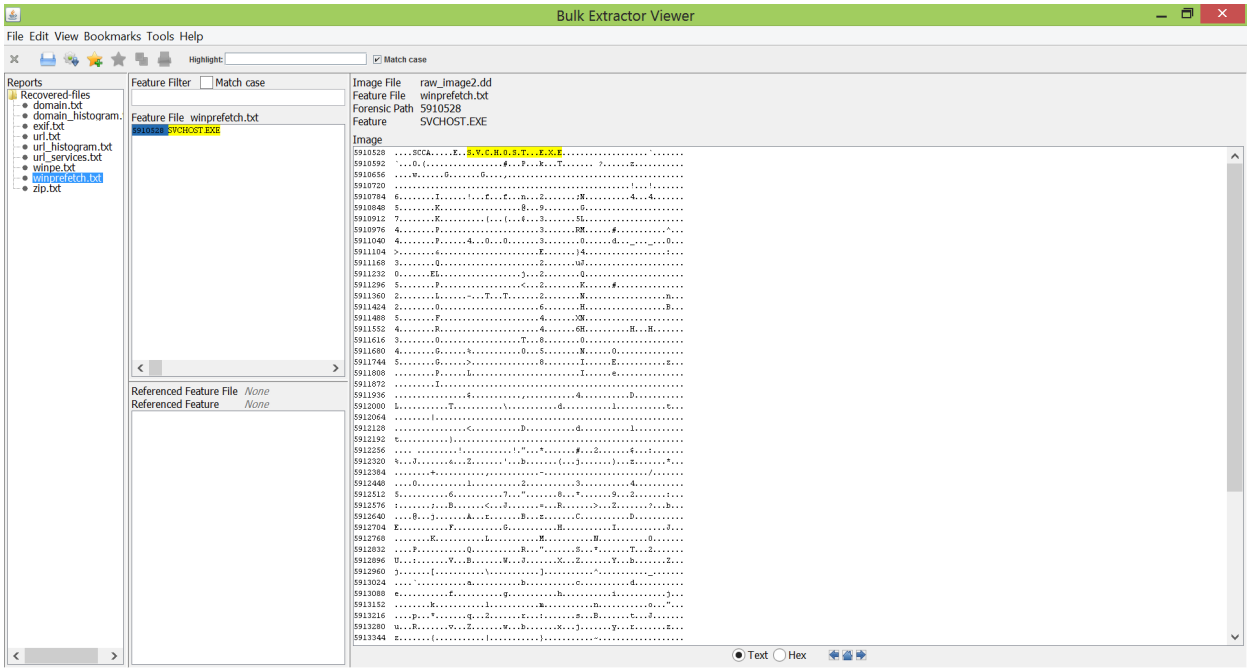
5. Click the “Submit Run” button.

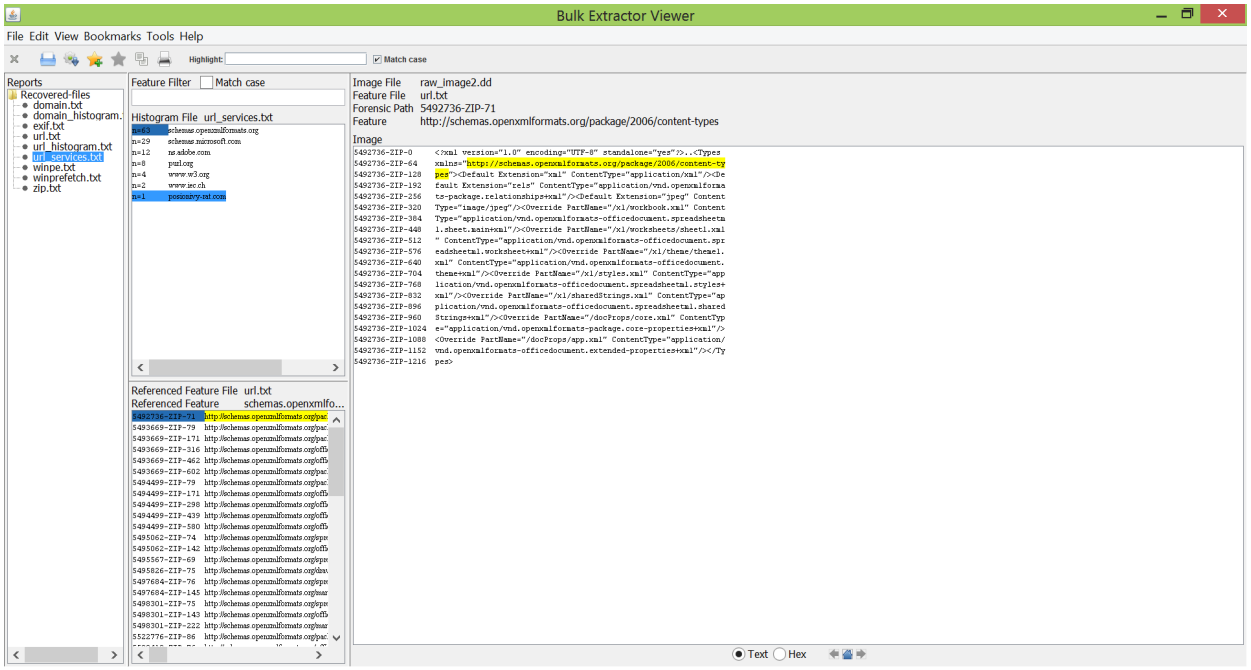
6. Now, back in the Bulk Extractor Viewer window, navigate the output folder as shown below. Check the following recovered items:

   a. winprefetch.txt

   b. url_services.txt

   c. winpe.txt


Bulk Extractor Viewer
File Edit View Bookmarks Tools Help
Highlight:
Match case
Reports
Recovered-files
domain.txt
domain_histogram.
exif.txt
url.txt
url_histogram.txt
url_services.txt
winpe.txt
winprefetch.txt
zip.txt
Feature Filter
Match case
Feature File winprefetch.txt
5910528 SVCHOST.EXE
Referenced Feature File None
Referenced Feature None
Image File raw_image2.dd
Feature File winprefetch.txt
Forensic Path 5910528
Feature SVCHOST.EXE
Image
Text
Hex


Bulk Extractor Viewer
File Edit View Bookmarks Tools Help
Highlight:
Match case
Reports
Recovered-files
domain.txt
domain_histogram.
exif.txt
url.txt
url_histogram.txt
url_services.txt
winpe.txt
winprefetch.txt
zip.txt
Feature Filter
Match case
Histogram File url_services.txt
n=29 schemas.openxmlformats.org
n=29 schemas.microsoft.com
n=12 ns.adobe.com
n=8 purl.org
n=4 www.w3.org
n=2 www.iec.ch
n=1 poesanvy-ist.com
Referenced Feature File url.txt
Referenced Feature schemas.openxmlfo...
Image File raw_image2.dd
Feature File url.txt
Forensic Path 5492736-ZIP-71
Feature http://schemas.openxmlformats.org/package/2006/content-types
Image
Text
Hex

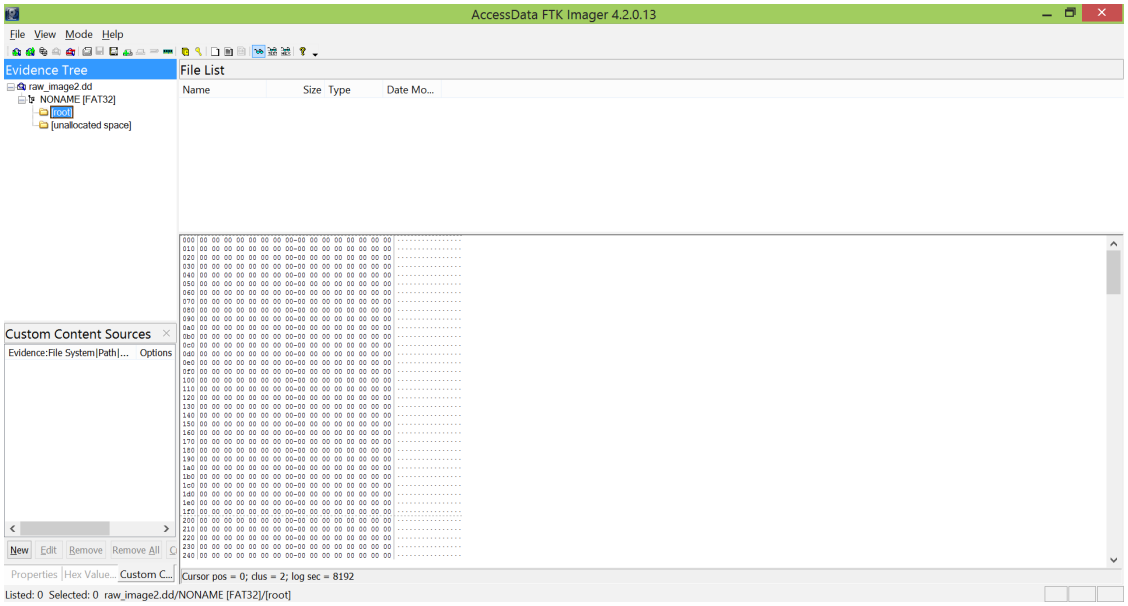
[Optional] Task 2 (Win-FWS): Performing a Manual File Carving of a Deleted File using FTK Imager

Notes:

- *If you are curious*, you can try to perform a ***manual* file carving** of a deleted file in a disk image.
- For the steps below, utilize **FTK Imager**, which you have installed and used before. You can reuse the **previously downloaded** "raw_image2.dd" disk image file. *Note that the carving steps can be pretty tedious!*

Steps:

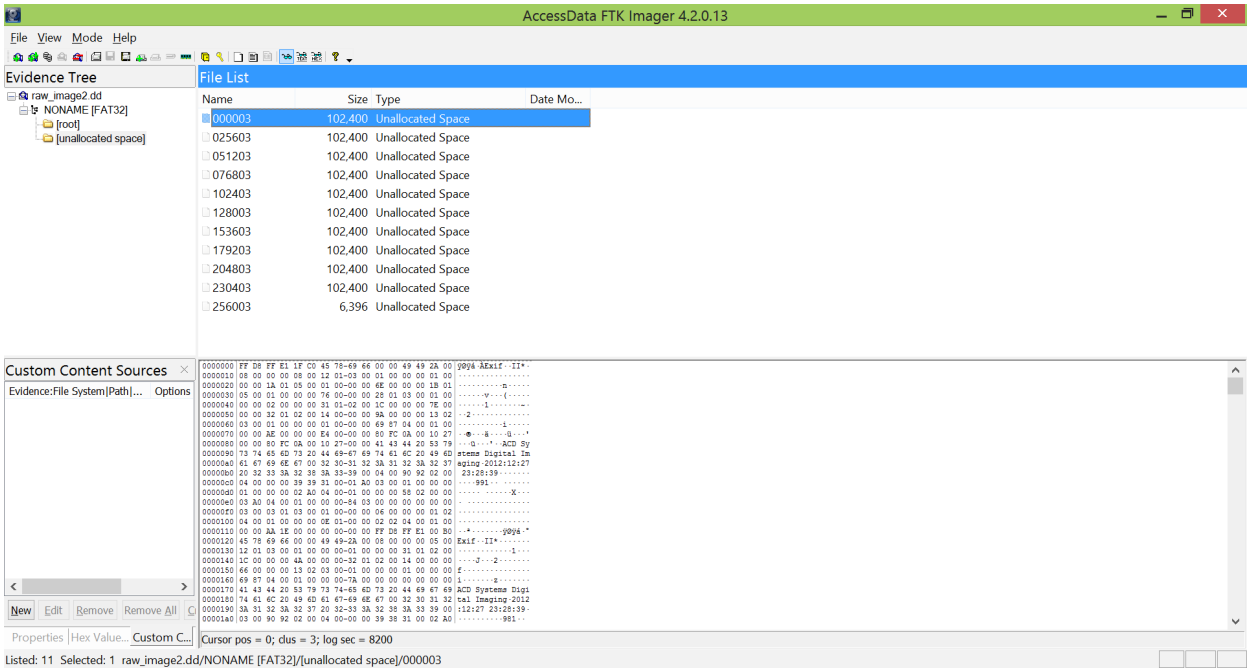
1. Launch FTK Imager.
2. From its main menu, select "File" then "Add Evidence Item…".
   In the "Select Source" dialog box, select "Image File" then the "Next" button.
3. Browse to the downloaded raw_image2.dd file.
   The following screen will be shown by FTK Imager.



4. Notice the **file system type**. What is it?

5. Can you find any files stored on the file system by clicking the item "root"?

6. Now, click on the tree item "**Unallocated space**".
   And click on the first entry shown in the File List pane as shown below.



7. Notice the content of the unallocated space, which is shown in both hex and text formats at the lower Content View pane.

8. Check the following:

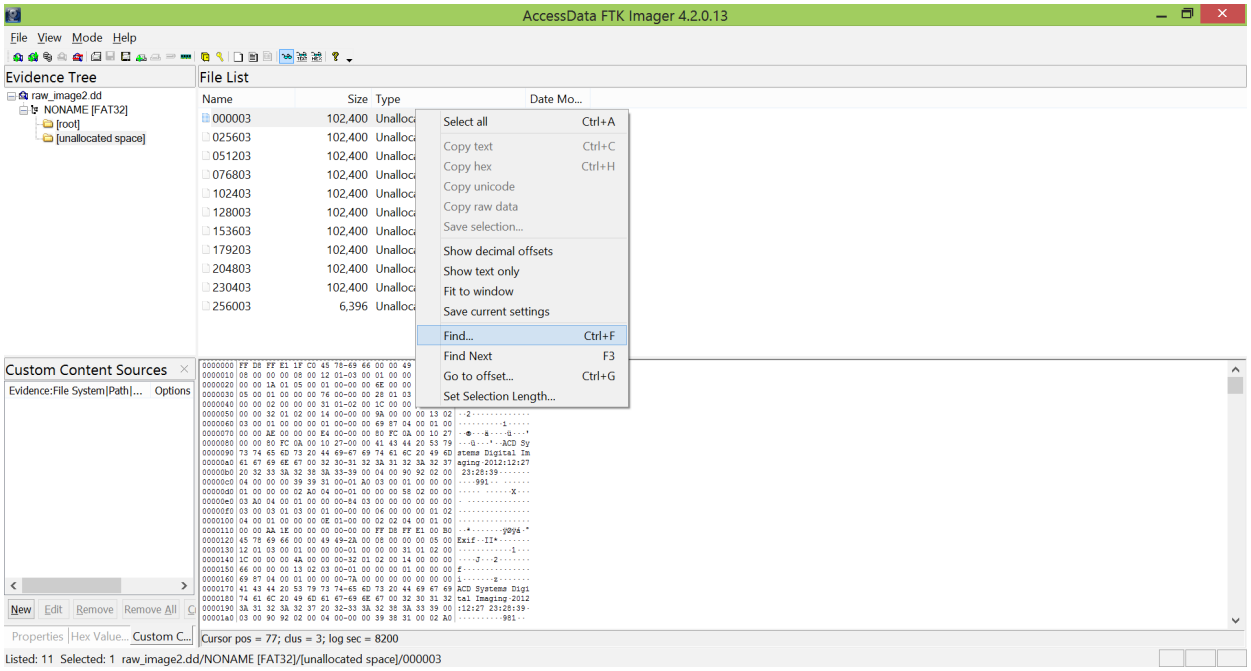
   a. What is the file signature? It is FF D8 FF E1.

   b. Visit https://www.garykessler.net/library/file_sigs.html.
      What file type is it? It is a JPG file.

   c. What is the EOF marker or file footer of a JPG file? It is FF D9.

9. To perform a manual data carving, you need to *find the occurrence* of the EOF marker. Before that, notice the **offset** associated with the start of the sector, which in this case is 0000000.

10. Now, in the Content View pane, right-click and select “Find…” as shown below.



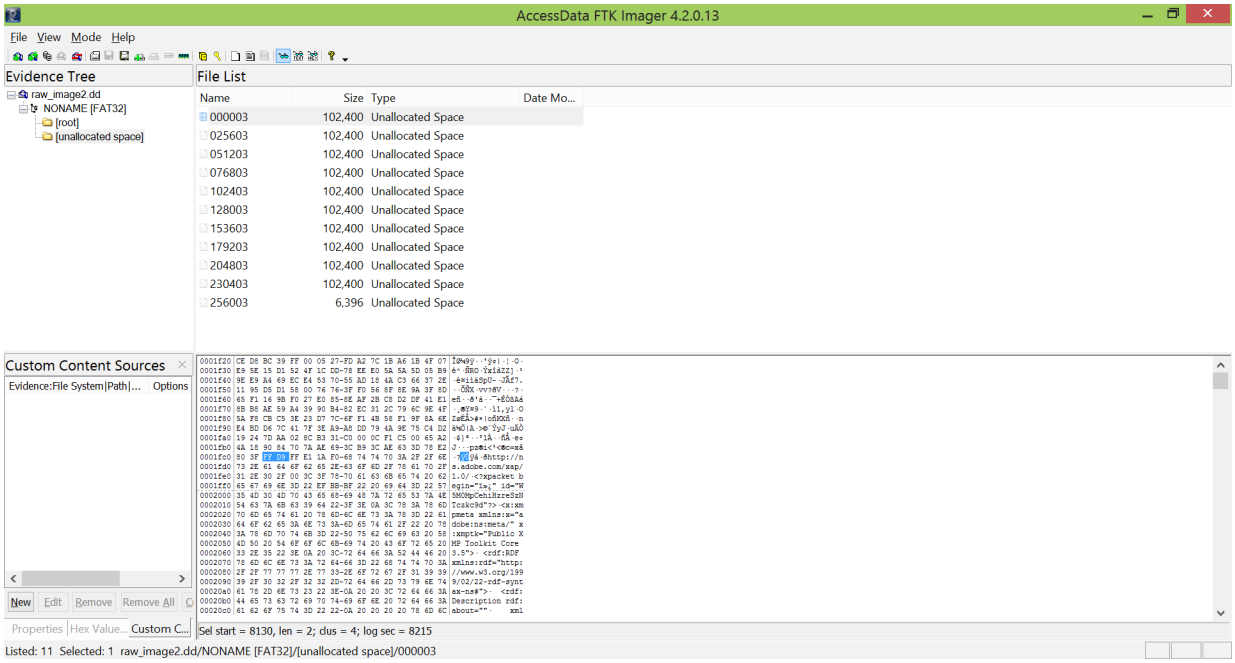
11. In the dialog box, enter the string for the EOF marker without a space (i.e. FFD9) and select “Binary (hex)” as its type as shown below.

12. Check the **first occurrence** of the string shown below. Is it a likely candidate for the file footer? Check its suitability by inspecting the following questions:

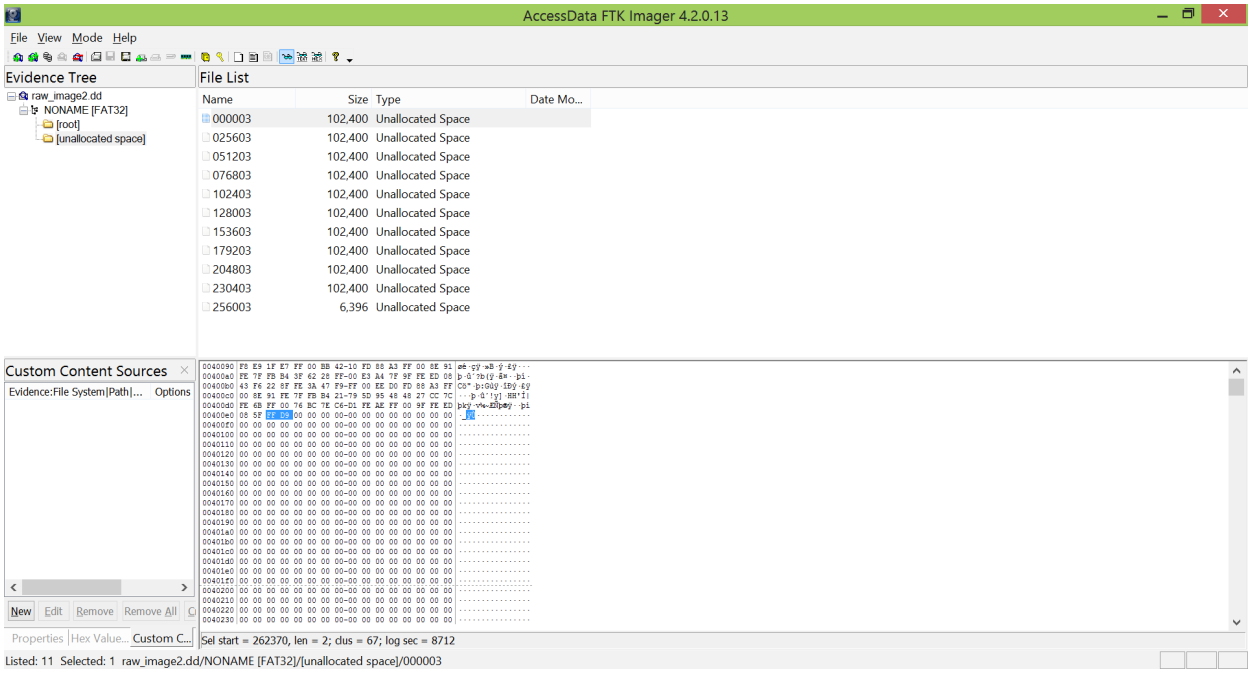
    a. Is the footer directly adjacent with the start of a new sector, which is mark by a dotted line in FTK Imager?

b. Are the characters between the EOF marker and the start of a new sector indicative of a slack space?

c. Does the start of the next sector contain a file header again? The string occurrence may ***not*** be the footer that we are looking for.



13. Press F3 to find the **next occurrence** of the string, which is shown below.



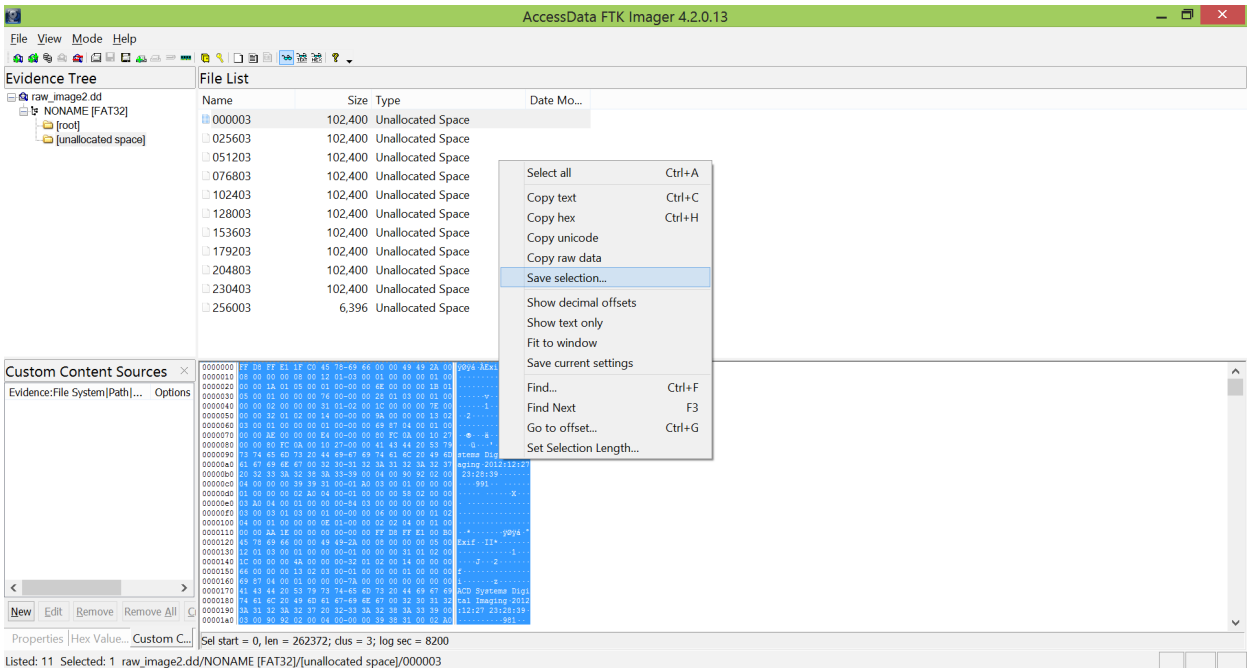
14. Check if this is a good candidate for the file footer.

    You will notice that it is, assuming that there are no fragmentations.

    The file thus starts at 0000000, and ends at 00400e3.

15. Highlight the identified file area by using the scroll bar and ***shift-clicking***.

    Then right-click, and select "Save selection…" as shown below.



16. Save the carved file to a folder location and name it with a .jpg extension.

17. Open the recovered .jpg file. What image can you see?

Task 3 (Win-FWS): File Analysis Tasks Using Autopsy

Let's now use Autopsy to perform **a few remaining file-analysis tasks** by employing the relevant ingest modules.

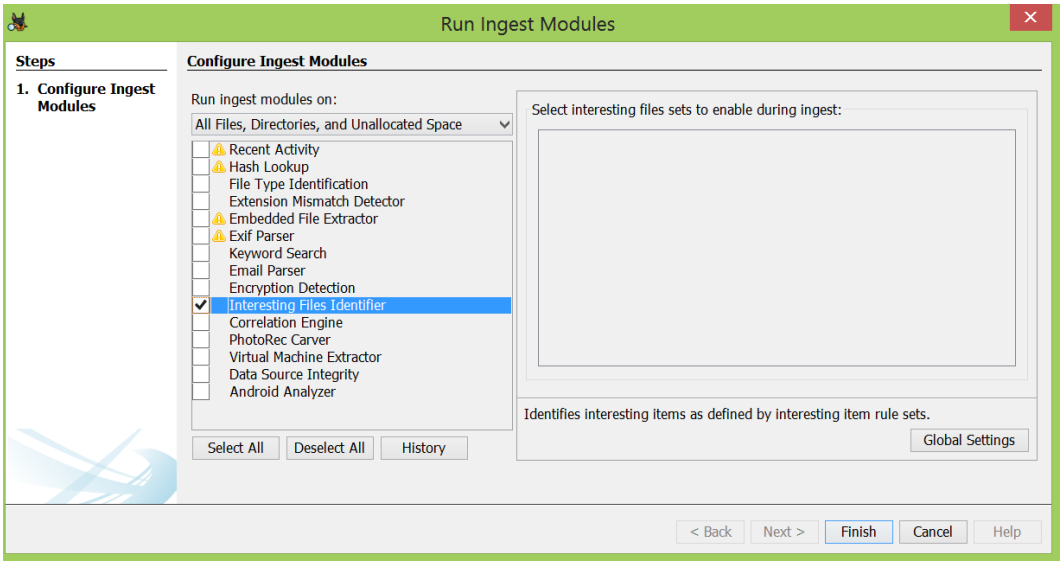
Task 3-A (Win-FWS): Finding Interesting Files based on Rule Sets using Autopsy

Notes:

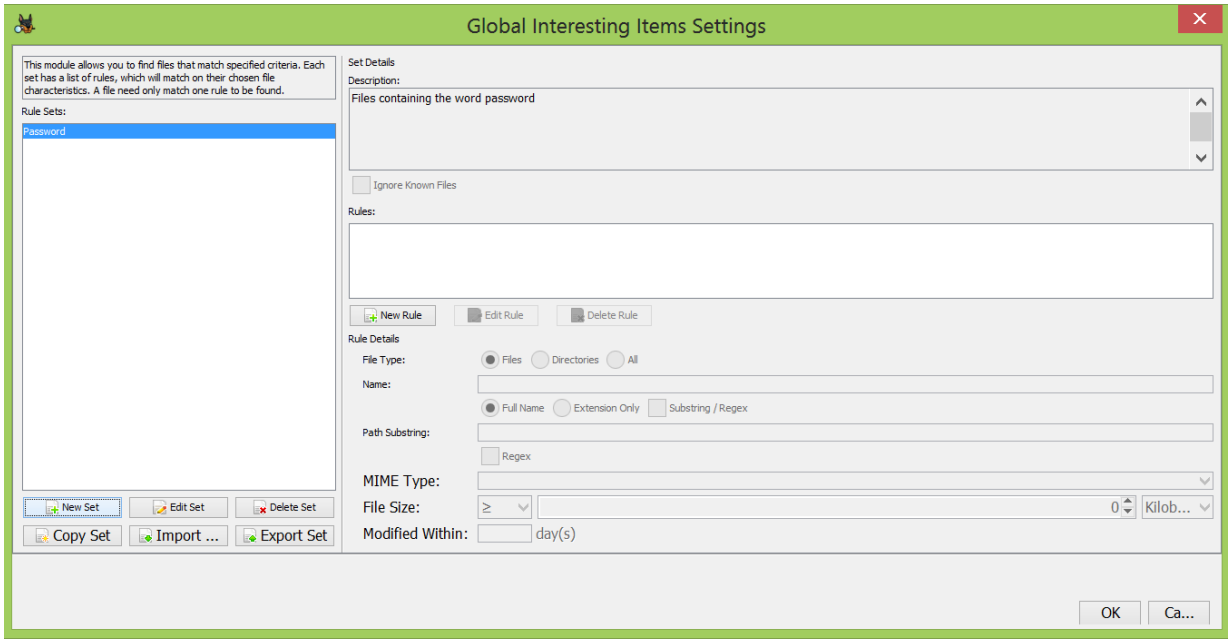
- In this task, you want to use Autopsy's ***Interesting File Identifier*** module to **find interesting files** according to some **rules sets** that you specify.
- You can use the "SuspectDrive1.E01" file that was previously used in Lab 4 if needed.

Steps:

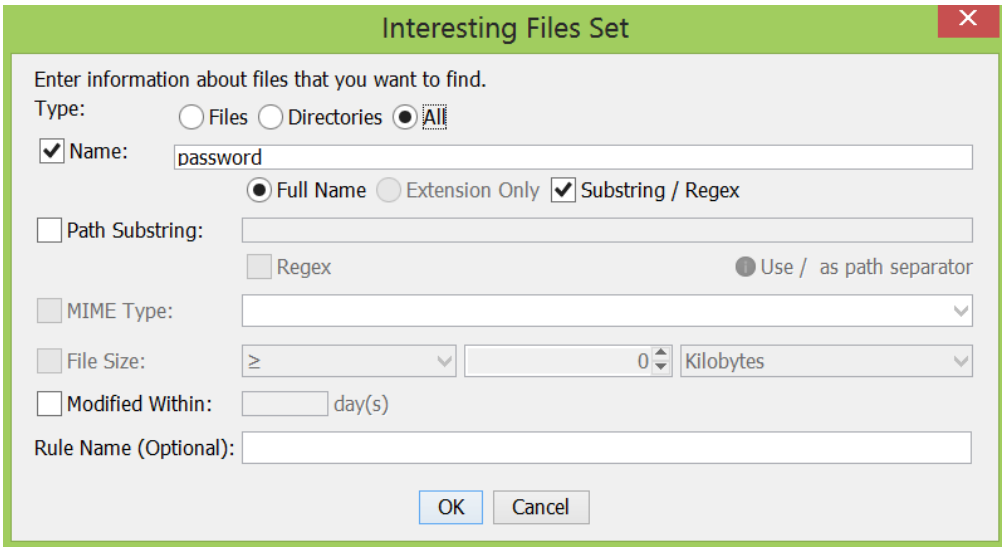
1. Launch Autopsy, and add the disk image file as a data source (if still needed).
2. Launch the "Run Ingest Modules" dialog box, then select the "Interesting File Identifier" module.



7. Click the "Global Settings" button so that the "Global Interesting Items Settings" dialog box can be shown. Create a **rule set** by clicking "New Set" and name it "Password". You can optionally give a short description like "Files containing the word password" as shown below.

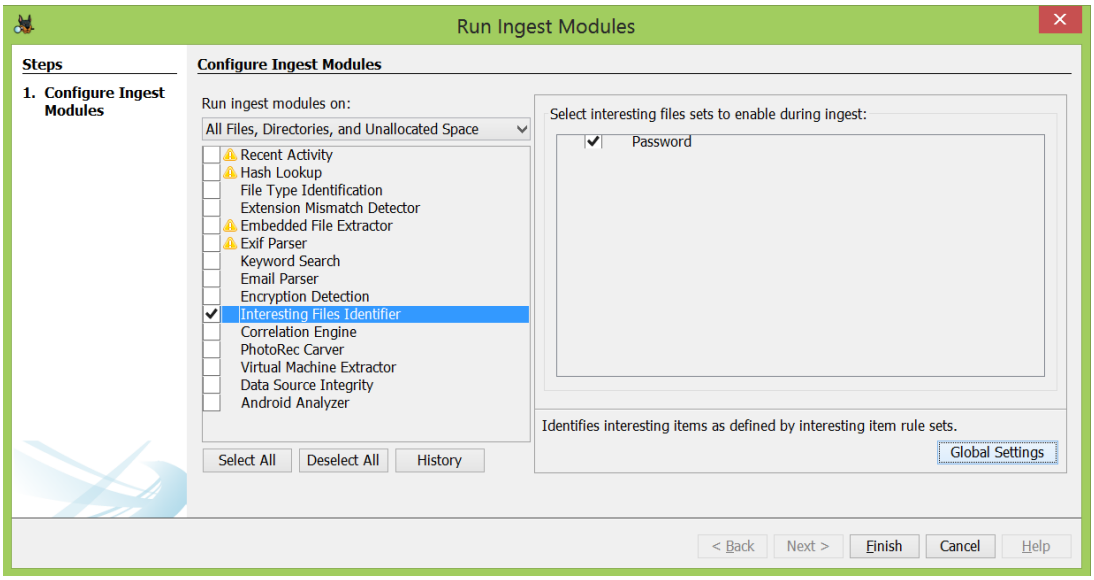


8. Create a rule in the rule set by clicking the "New Rule" button. You want to specify your new rule, for instance, by setting the options as shown below.

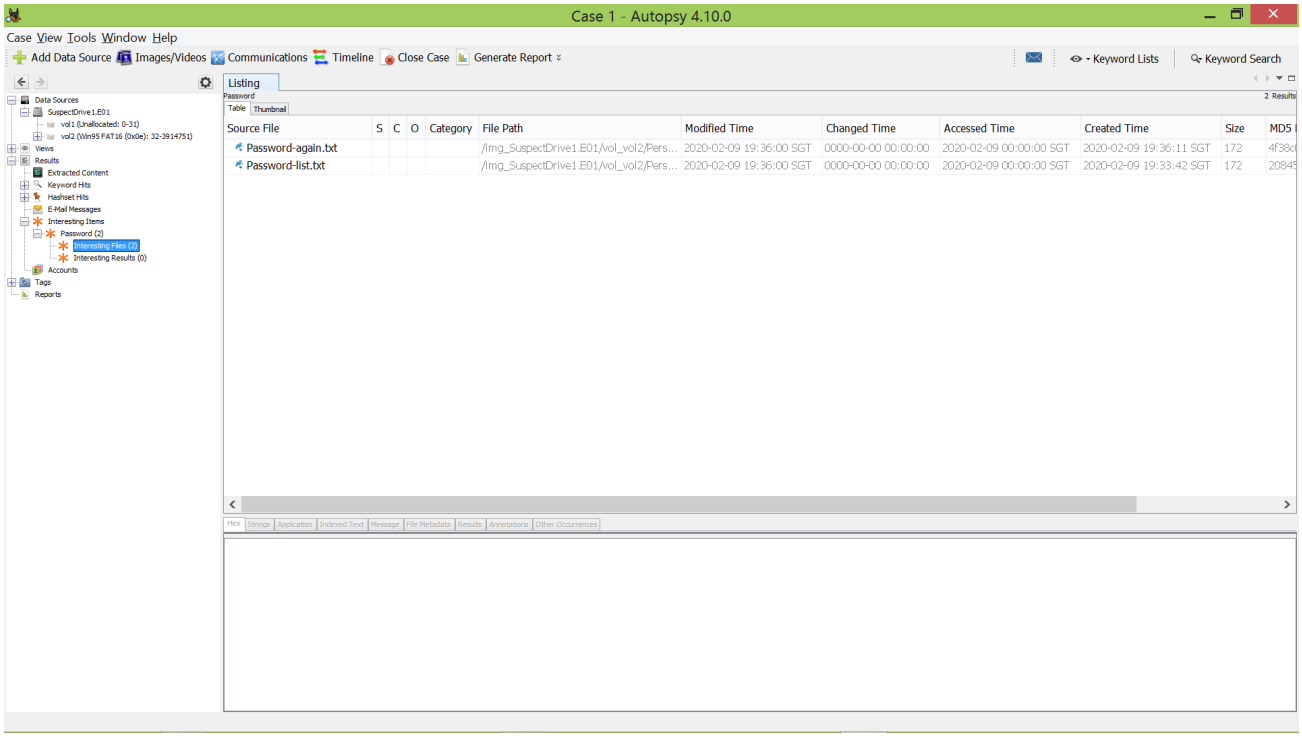


9. Click "OK" to close the "Interesting Files Set" dialog box. Click "OK" again to close the "Global Interesting Items Settings" dialog box.

10. In the "Run Ingest Modules" dialog box, you should see an entry for your created "Password" rule set. Make sure that it's selected for processing as shown below. Click "Finish" to start the module processing.



11. Once the ingest module has completed its processing, you can see the identified files under the "Results" → "Interesting Items" → "Password" in Autopsy's tree viewer.



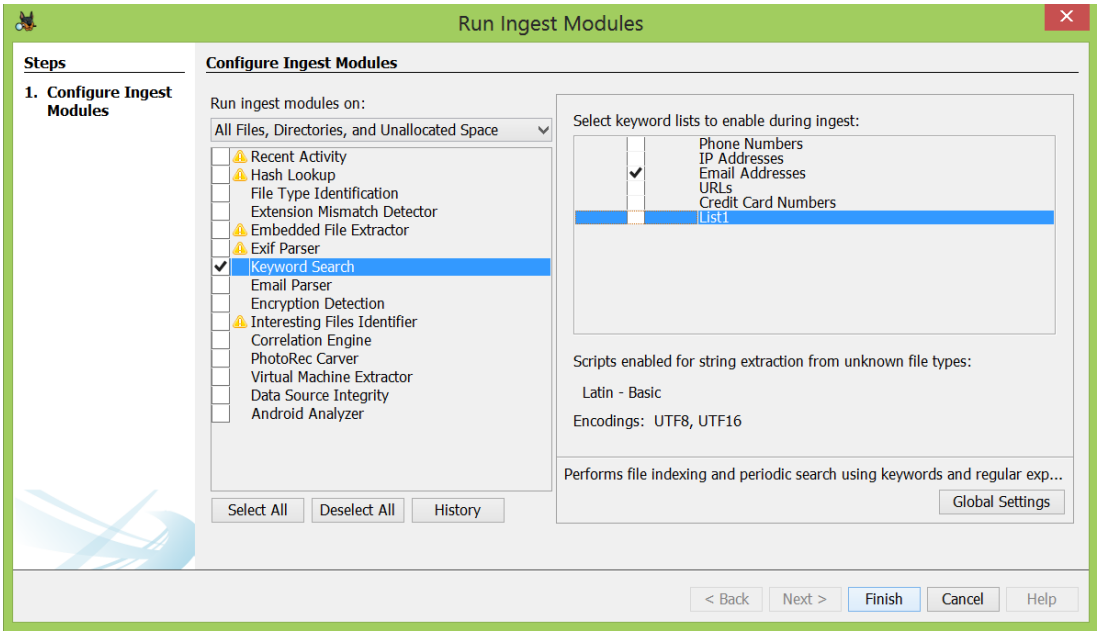
Task 3-B (Win-FWS): Performing Keyword Search in Autopsy

Notes:

- In this task, you want to use Autopsy's ***Keyword Search*** module to **find files in a target file system** that contain certain keywords of interest.
- Use the "SuspectDrive1.E01" file if needed.

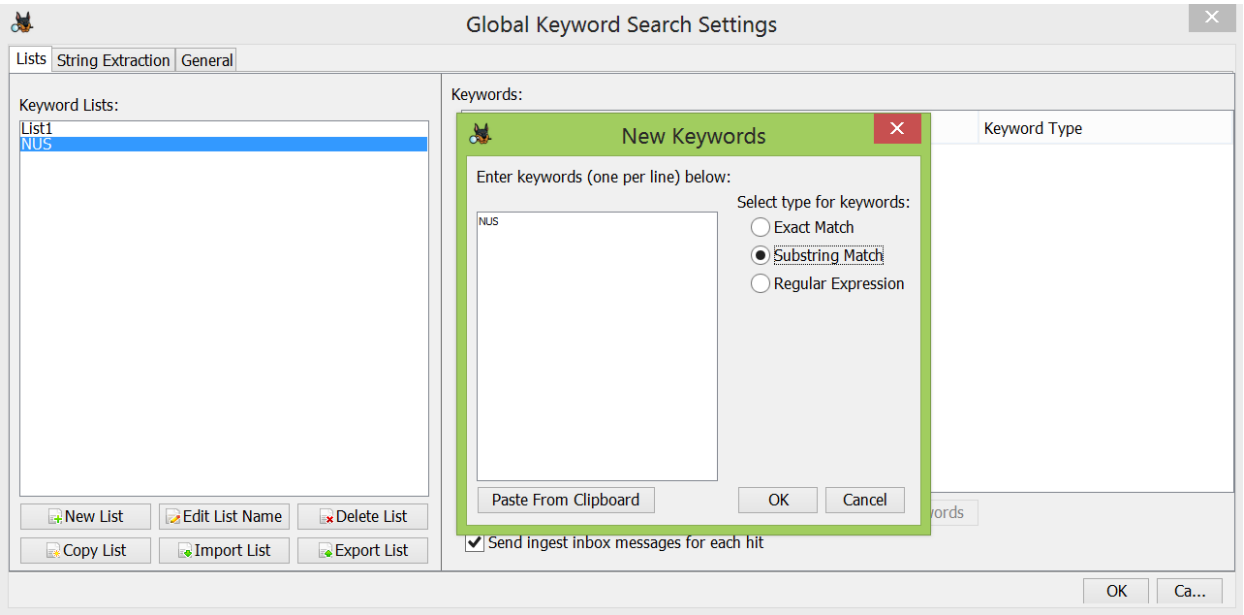
Steps:

1. Launch Autopsy, and add the disk image file (if still needed).
2. Launch the "Run Ingest Modules" dialog box, then select the "Keyword Search" module.



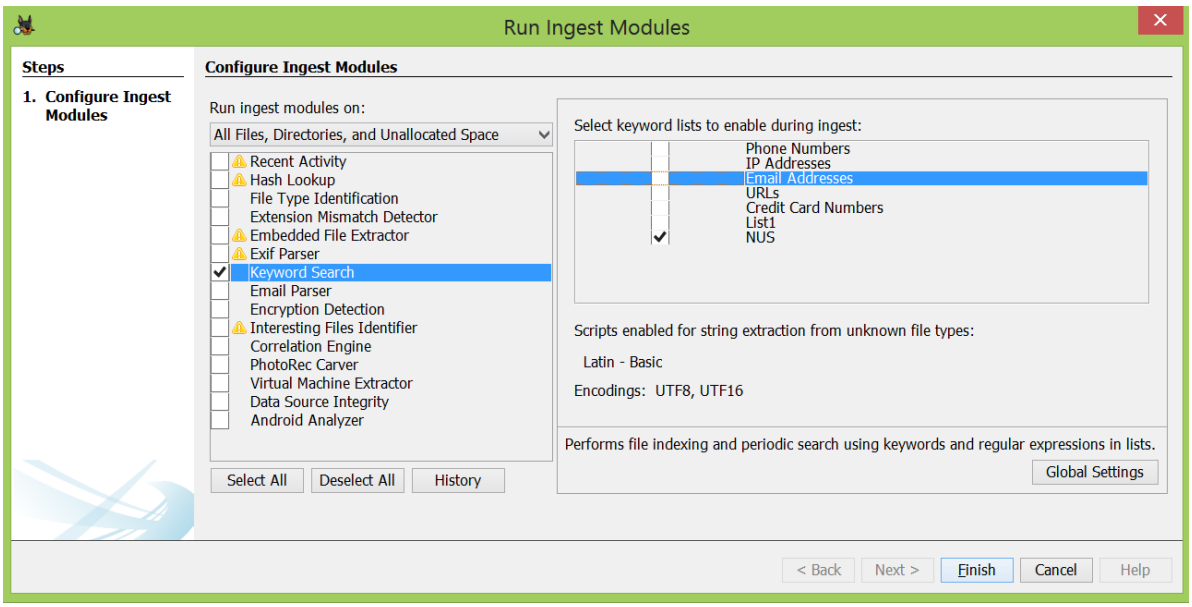
12. Notice that there are already some ***pre-defined keyword lists*** that you can select. You can select some of them if you want to.
    Let's now also add **our own keyword list**. For that, click the "Global Settings" button so that you can see the "Global Keyword Search Setting" dialog box.

3. Create a **new keyword list** by clicking "New List" and name it "NUS". Then, create keywords in the keyword list by clicking the "New keywords" button. You can specify a new keyword as shown below.

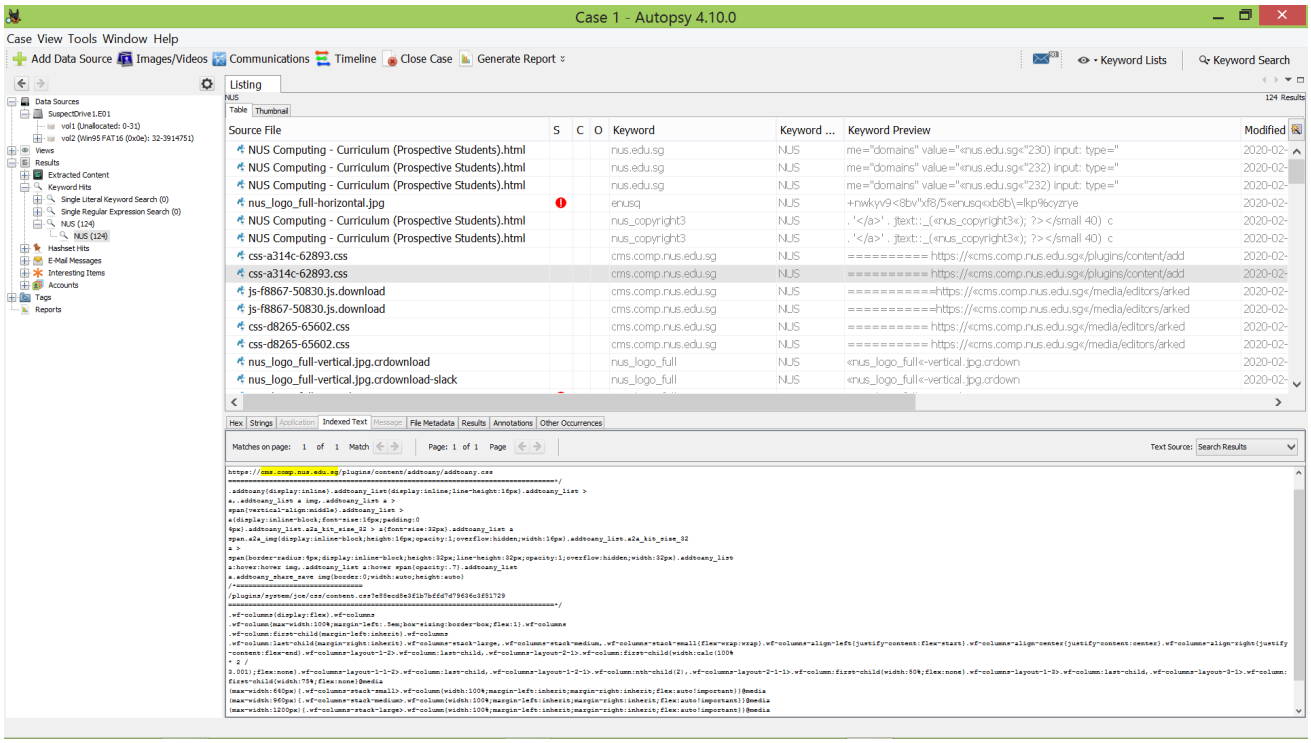


13. Click "OK" to close the "New Keywords" dialog box. Click "OK" again to close the "Global Keyword Search Settings" dialog box.

14. In the "Run Ingest Modules" dialog box, you should see an entry for your created "NUS" keyword list. Make sure that it's selected for processing as shown below. Click "Finish" to start the module processing.



15. Once the module ingest has completed its processing, you can see the matching files under the “Results” → “Keyword Hits” → “NUS” in Autopsy’s tree viewer.



16. Browse all the listed files. For each file, also check the **highlighted matching string(s)** inside the “Indexed Text” tab within Autopsy’s content viewer.

Task 4 (Win-FWS): Extract and Analyse Offline Registry Files of a Target Windows Machine

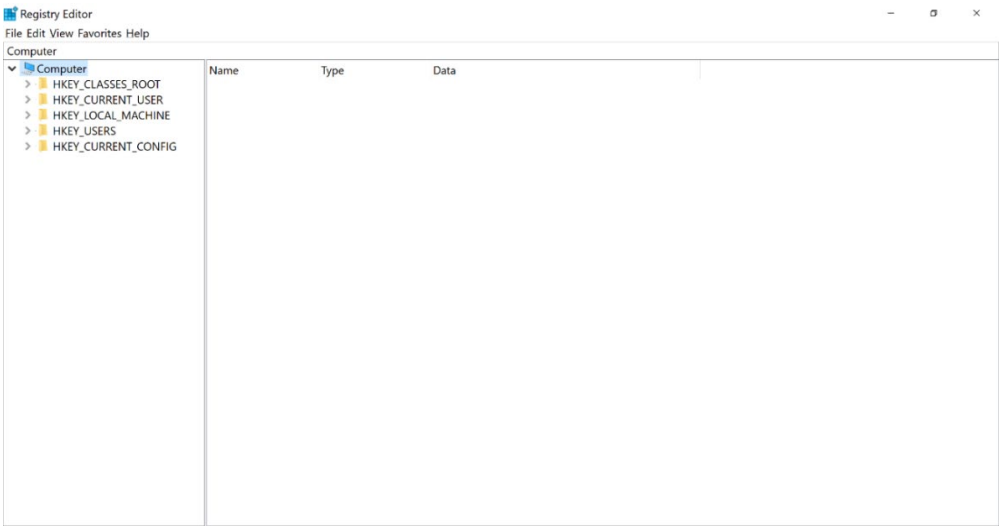
Task 4-A: Manual Extraction & Analysis using RegEdit

Notes:

- In this exercise, you will use **RegEdit**, which is already available in Windows. You can use RegEdit to manually inspect offline registry files of your target Windows machine, should the need for a manual inspection arise.
- For sample registry files, you can download a zipped file from: https://drive.google.com/file/d/133bLl7TYqDyCG9eSfuDcIKhbwqiKxJil/view?usp=sharing. Its MD5 value is b527b6a8a4a395aac8afb6c59cf4b15e.
- As usual, ***be very careful*** when using RegEdit on *your host Windows*!

Steps:

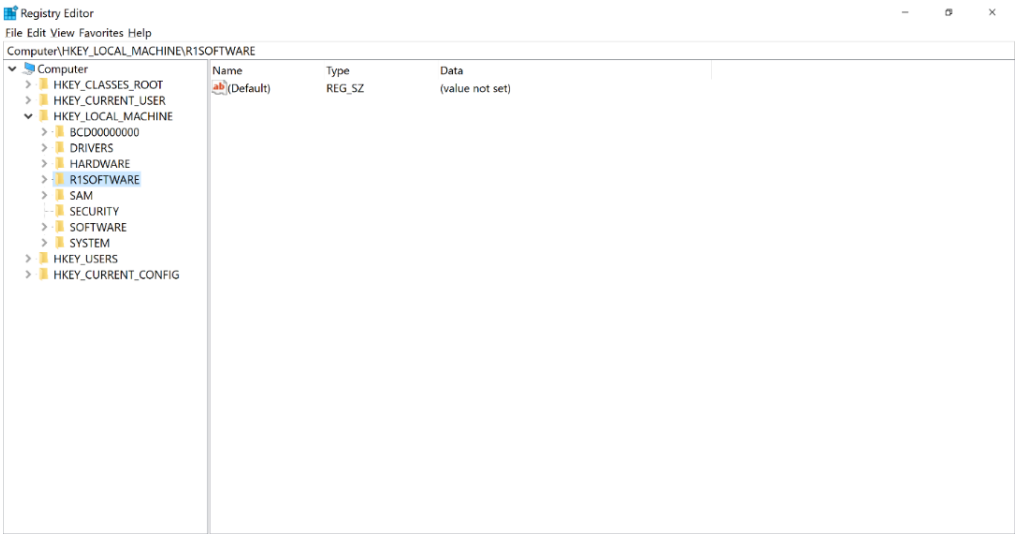
1. Open a command prompt on your Windows machine, and launch Regedit by invoking `regedit`. Regedit window should appear as shown below.



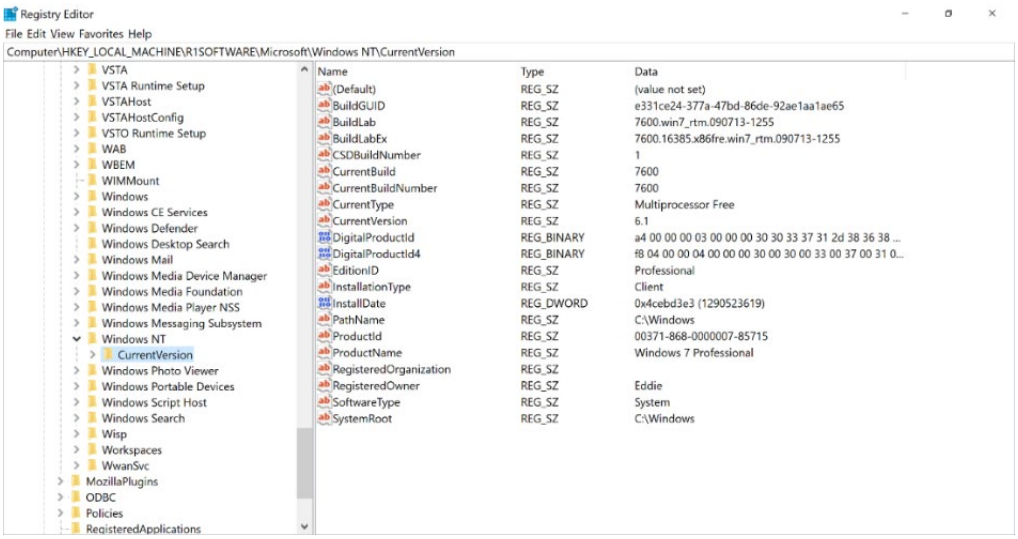
2. Expand `HKEY_LOCAL_MACHINE` hive, and notice the names of all existing key entries under it.

3. Access the main menu, select “File” menu item, and then select “Load Hive…”. Browse to the directory where the sample registry files reside, and select the file `SOFTWARE`. When prompted for a key name, just give a *different name* from existing keys under `HKEY_LOCAL_MACHINE`, such as “`R1SOFTWARE`”.

4. Now, expand `HKEY_LOCAL_MACHINE` hive (if still needed), you should be able to see an entry for “`R1SOFTWARE`” as shown below.



5. Navigate to the following key `HKEY_LOCAL_MACHINE\R1SOFTWARE\Microsoft\WindowsNT\CurrentVersion` as shown below.



6. Inspect various relevant key values and their set data.
   Answer the next few questions below.

   - Find out the target machine's **Windows version (product name)** by checking the data of the `ProductName` key value.
   - Find out the machine's **Windows product ID** by checking the data of the `ProductId` key value.
   - Find out the machine's **registered owner** and **organization** by checking the data of the `RegisteredOwner` and `RegisteredOrganization` key values, respectively.
   - Find out the machine's **installation date** by checking the data of the `InstallDate` key value.
     Note: You can easily convert the recorded timestamp (in *epoch time*) to its human-readable date version by using an online tool like https://www.epochconverter.com/. The "Date/Time" feature of CyberChef online tool (https://gchq.github.io/CyberChef/) can also be used. Alternatively, you can download and install Digital Detective's DCode (https://www.digital-detective.net/dcode/) for conversion of various timestamp formats.

7. Lastly, to finish, unload the offline registry file R1SOFTWARE. At the main menu of RegEdit, select "File" and then select "Unload Hive…".

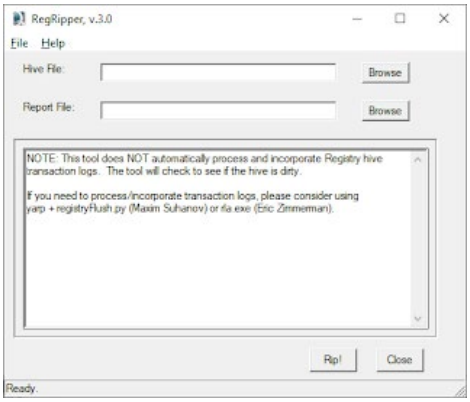
[Optional] Task 4-B: Automated Extraction & Analysis using RegRipper

Notes:

- As you can see, manual registry analysis, while powerful, is rather time consuming and inconvenient. Additionally, you will need to know the right registry keys to browse. Hence, an ***automated*** **registry analyzer** is often used to extract various registry entries that are useful for forensic purposes.
- In this exercise, you will use a popular tool called **RegRipper**. Manual registry analysis, as done in the previous sub-task, can complement an automated one using a tool like RegRipper.

Steps:

1. Download RegRipper from https://github.com/keydet89/RegRipper3.0, and extract its zipped file's contents to a folder, e.g. Desktop.
2. Launch RegRipper by double-clicking its executable file `rr.exe`.
   Its starting windows is shown below as taken from its author's blog post http://windowsir.blogspot.com/2020/05/regripper-v30.html.
   (***Note***: the previous v2.8 used to have the "Profile" dropdown list option).



3. Click the first "Browse" button (for "Hive File") in the window, and select the `NTUSER.dat` file from the registry files downloaded in Task 4-1.

4. Click the second "Browse" button (for "Report File"), and then select a file to record the registry analysis output.
5. (*In older RegRipper, e.g. v2.8*: Select the applicable profile, i.e. "`ntuser`". RegRipper version 3.0 now runs through the entire plugins folder to build a list of all plugins that apply to, and then runs them).
6. Click the "Rip It" button to start your registry extraction/ripping.
7. Once the extraction is done, open the report file.
   You can also check and open the RigRipper log file in an outputted log file (`.log`) with the same file name.
8. Analyze the report file, and find out useful information, such as the *typed URLS* of the Internet Explorer browser, which were extracted from `Software\Microsoft\Internet Explorer\TypedURLs`.
9. Now, repeat the process to rip the `SYSTEM` file from the downloaded sample registry file set. Remember to set the right profile option accordingly.
10. Open the report file, and inspect any useful information, such as the *USBSTOR information*. The USBSTOR section starts with "`USBStor ControlSet001\Enum\USB`".
    Find out the answers to the following questions regarding USBSTOR:
    a. What were the serial numbers of devices connected to the machine?
    b. When were the devices first connected?
11. Repeat using RegRipper on other registry files.
    Analyze the outputs accordingly.

Notes on RegRipper Seemingly Hanging when Importing SOFTWARE Registry File:

- Please find below some information regarding **a potential issue with RegRipper** when it is used to analyze a SOFTWARE registry file.
- When using RegRipper to analyze a SOFTWARE registry file, RegRipper may *seemingly hang* after running the `btconfig` plugin. This is actually because the subsequent plugin, `clsid`, produces **a lot of output** that may take a long time to complete. As such, you may choose to disable the `clsid` plugin if it is taking too long.
- To **disable** the `clsid` plugin, do perform the following steps:
  1. Close RegRipper if you have it opened.
  2. Open the file `plugins/software` in Notepad.
  3. Comment out the line with `clsid`, so that it looks like the following:

```
...
bitbucket
btconfig
# clsid
cmd shell
cmd shell tln
...
```

  4. Save the file, and then close it.
  5. Now you can import the SOFTWARE registry file as per normal.

Graded Lab Tasks #3 (2 Marks)

From your Lab 5, you will also need to submit **your 3 answers** as follows:

- The selected **3 tasks** in this lab are:
  - (0.75 marks) Task 3-B (pages 15-17): Run Autopsy's Keyword Search module on the "SuspectDrive1.E01" file by selecting Autopsy's **built-in "URLs" keyword list**. Please attach a screenshot of the hit results given by Autopsy as your proof-of-work.
  - (0.5 marks) Task 4-A, Step 6 (page 20): Please tell the target machine's **Windows version (product name)**.
  - (0.75 marks) Task 4-A, Step 6 (page 20): Please tell the target machine's **installation date** in **human-readable date version**.
- From your correct 3 answers, you will earn a total of **2 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-**GLT3**.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-3`** Canvas Assignment by **Saturday, 18 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 tasks in this lab! :)