CIS/ECE 387 Fall 2022 Lab5

Due: **10/31/2022**
Total points: 20

ACTIVITY: CASE STUDY WITH AUTOPSY

SOFTWARE AND DOWNLOADS

In this activity, we will use the GUI-based open-source forensic analysis tool, Autopsy, to analyze a Windows image.

- Autopsy download
- Autopsy User Guide

Download the image file, WinLabEnCase.E01, on canvas under the Files->Labs->Lab5 folder.

CASE SCENARIO

ACME Industry develops custom software for the aviation industry. Its main competitors are companies like Raytheon and Boeing, as well as a few smaller contractors.

Pat Smith has worked for ACME Industry for five years. Pat's supervisor has noted that after being passed over several times for a promotion, Pat has become quite disgruntled. The company fears that Pat may be offering proprietary company information to a competitor in exchange for a job.

An disk image of Pat's computer's hard drive has been generated. Your job is to examine the image and extract all pertinent information to support or disprove the statement of Pat may be offering proprietary company information to a competitor in exchange for a job.

INSTRUCTIONS

1. Launch Autopsy from the Toolbox folder on the desktop and follow the instruction below to create a case and add the given image into the case.
2. Select > Create New Case
3. Name the case as "ACME Case".
4. Use the default Base Directory (Desktop) to store the case data in Desktop\ACME Case\.
5. Enter the Case Number as "001" and enter your name as "Examiner."
6. Click Finish. You will see the "Add Data Source" window.

7. Select data source type: choose *Disk Image or VM File*; browse and select the path to "WinLabEnCase.E01".

8. In our case, the computer image's time zone is North American Eastern Time Zone. Select the time zone accordingly and click *Next*.

9. In the *Ingest (processing) modules* window, leave all modules checked; click *Next* and then click *Finish*.

10. Examine the files in Data Sources > WinLabEnCase.E01 and categorized data under Views and Results to identify pertinent evidence.

11. Explore the image contents and results, and answer the following questions.

    a) Data carving is the process of extracting files and objects that have been deleted or are embedded in other files. Check under Data Sources > WinLabEnCase.E01> $CarvedFiles. How many embedded files did Autopsy extract by performing the data carving process? List all the files.

    b) Autopsy lists all deleted files in Views > Deleted Files. What have you found by examining these deleted files?

    c) A file type can be determined by a header that precedes the data in the file. If a file's extension has been deliberately changed, the extension will not match with the file header. File Signature Analysis detects such mismatches by comparing the file extension with its header. Autopsy performs file signature analysis and lists these files in Results > Extracted Content > Extension Mismatch Detected. In this case, diagram.doc has a mismatched extension. What is the real file type of diagram.doc?

    d) Check cookies from \Documents and Settings\psmith\Cookies and identify the sites that stored cookies on psmith's machine during his visits.

    e) Files with the extension of .lnk are shortcuts or link files. Examine \Documents and Settings\psmith\Recent\Confidential.lnk. What is the file name and path that Confidential.lnk points to? (Hint: read its content by looking at the "result" and "File Metadata")

12. Perform a keyword search on email address: Click the Keyword Lists (on the top left corner) and Check the Email check box, then click Search

Check Results > Keyword Hits > Email Addresses. Did you find any pertinent evidence (e.g. job offers, attempt to leak company information)? Include those evidence in your report.

Note: Once you have created the case, you can reopen it at any time in Autopsy using "Open Existing Case," and choosing *Desktop\Financial Case\ACME Case.aut*.

If you are interested, you can also try other Autopsy features and examine other artifacts.

You can also try other features that Autopsy supports such as:

- View Images/Videos
- Timeline
- Tag and bookmark for reporting
- Generate Report.

  You can examine many other artifacts for this exercise. For example:

- Documents and Settings\psmith\Local Settings\History\History.IE5\index.dat
- Recycled
- Documents and Settings\psmith\ntuser.dat
- WINDOWS\system32\spool\PRINTERS.

Report

Your report should include the activity log (the steps you take or the commands you run) with some screenshots and/or outputs, answers to the questions in step 11 & 12, and a brief reflection on what you learned (one or two paragraphs).

Please submit your lab report to Canvas under the “lab5” assignment folder.