**CIS-387: Digital Forensics (4 credits)**

**With Dr. Jinhua Guo**

**Lab 5**

**Demetrius Johnson**

**October 26, 2022**

# ACTIVITY: Disk Image Analysis with ACME Autopsy Tool (GUI version of Sleuthkit)

## 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.

Graphical user interface, text, application

Description automatically generated

## 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\.

Graphical user interface, text, application, email

Description automatically generated

## 5. Enter the Case Number as “001” and enter your name as “Examiner.”

Graphical user interface, text, application, email

Description automatically generated

## 6. Click Finish. You will see the "Add Data Source" window.

Graphical user interface, text, application

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

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

Graphical user interface, text, application, email

Description automatically generated

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

Graphical user interface, application

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

## 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.

Text

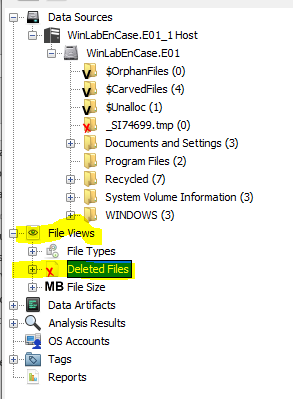
Description automatically generated

Notice 4 files have been extracted by the data carving process:

Graphical user interface, text, application

Description automatically generated

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



Graphical user interface, text, application, email

Description automatically generated

Here are all the deleted files:

Graphical user interface, text, application, email

Description automatically generated

Here are the deleted system files, a subset of all deleted files:

Graphical user interface, text, application, email

Description automatically generated

* Raytheon, Boeing, and \_P62 were all directories which were small enough that their file data was able to be stored as attributes in the MFT table.
* There were also two .gif files with diagrams and a .pdf file which contained a research paper or abstract.
  + Graphical user interface

    Description automatically generated
  + Diagram

    Description automatically generated
  + Graphical user interface, text, application, email

    Description automatically generated

### 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?

* Graphical user interface, text, application, email

  Description automatically generated
  + Above, I am showing diagram.doc file that is found to have extension mismatch.
* Here is the detected actual file type:

Graphical user interface, text, application, email

Description automatically generated

It is really a image/.gif file type.

* Here is the gif file:
* Diagram

  Description automatically generated
* Notice it is a schematic of some sort.
* This is potential evidence that he is hiding data inside of this file and sending it somewhere or downloading it.

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

Graphical user interface, application

Description automatically generated with medium confidence

Above are listed the websites that the user has visited and logged in to according to the cookies stored on their drive. I noticed he visited and logged into a site called **rayjobs.com**; thus, this is some evidence that Pat Smith is searching for a job.

Also as a side note, I notice two deleted folders named **Boeing** and **Raytheon** were found on the disk under his profile:

A picture containing graphical user interface

Description automatically generated

Here is what google search for rayjobs brings up:

Graphical user interface, text, application, email

Description automatically generated

Notice **rayjobs.com** is the name for their career application site. His machine stored login cookies for that site, so there is good reason to believe that Pat created a profile and logged into the site to apply for a job.

### 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”)

Graphical user interface, text, application, email

Description automatically generated

The shortcut file contains a data segment showing that the file stores a pointer to the path as highlighted 🡪 documents and settings\psmith\my documents\Confidential.

Here are the contents under that directory:

Graphical user interface, application, Word

Description automatically generated

Notice that diagram.doc is under this directory and has the mismatch extension. Also, the project238x and 47x is property of ACME industries and is confidential. This is not yet incriminating however because he is only doing this within the company and has not been proven at this point in this investigatory document to have sent this information to anyone not authorized to receive it.

## 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.Graphical user interface, text, application Description automatically generated

Table

Description automatically generatedGraphical user interface, application, table

Description automatically generated

* Graphical user interface, application

  Description automatically generated
  + Notice he sent and received mail from Raytheon.com to email users Lucy Flynn, B Conrad, and Norman Krim
  + Here is one of the email exchanges where Pat sent a request to Ben from RAYTHEON asking for a position in the company in exchange for information from ACME company:
  + Graphical user interface, text, application, Word

    Description automatically generated

# Summary/Reflection

Include a brief reflection on what you learned (one or two paragraphs).

I learned that the ACME graphical user interface tool is very powerful for analyzing the contents of a disk. It automatically finds deleted files and directories that have not yet been overwritten with contents from a new file, it analyzes the meta data of the file system and all files and allows you to get the true file types. The auto-analysis feature is probably the most powerful feature because it allows you to quickly and effectively (although not as complete) audit a drive to find important or key information. According to my investigation, it is clear that there is good evidence Pat is trying to get a job at Raytheon, and there is even evidence that he sent an email offering company information in exchange for a job.