**Nwachukwu Edumanichukwu**

**CYBR 440 - Incident Detection and Response  
Module 7 Lab – Analyzing System Storage**

In this seventh lab, we will spend some time becoming familiar with the open-source forensics investigation tool Autopsy. You may have used this tool in your digital forensics course or another tool like it called FTK. While your previous course focused on investigative elements common to criminal investigations, forensic tools can also be used for malware investigation and analysis as well as corporate investigations into things like fraud or corporate espionage.

**You will be required to submit the following graded items as part of this lab:**

* Answer all questions listed in **BOLD**
* Provide screenshots when asked

Accessing the Lab

This lab is hosted in the university's IS Lab and requires special instructions to access it. If you are not familiar with accessing the IS Lab, please see the document in this course that walks you through accessing the Cybersecurity Desktop. You can access the Cybersecurity Desktop through the Web or using VMWare’s Horizon client. You should use the native Horizon client when possible as it provides better performance. The web client can be accessed at <https://workspace.bellevue.edu>. Make sure you log into this interface with your Bellevue student ID and password.

After accessing workspace.bellevue.edu and selecting the IS Lab desktop, open a browser and navigate to <https://10.98.100.11>. The first time you access this site you will see a warning in the browser. Make sure to click advanced and then Proceed to 10.98.100.11 (Unsafe). You should see the following remote access page.

Graphical user interface, application, Word

Description automatically generated

After accessing Bellevue Bank and Trust’s Remote Management Portal, login in using the following information:

* Username: analyst# - Where # is the number provided to you by your instructor
* Password: An@lyst#!! - Where # is the number provided to you by your instructor

After logging in you should see the following page:

Graphical user interface, application

Description automatically generated

You should have three available connections, RDP Kali #, RDP Workstation#, and SSH Kali #. These your three analyst tools you will use throughout this course.

You will be using the Windows 10 RDP Workstation# connection for this lab. You should open each new RDP or SSH connection in a new tab.

Part 1 - Analyzing System Storage with Autopsy

In this lab we will become familiar with Autopsy and how it can be used to examine a disk image. The image used in this lab comes from the NIST Computer Forensics Reference Data sets (CFREDS). Before you continue, please read through the scenario overview for this case here: <https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html>.

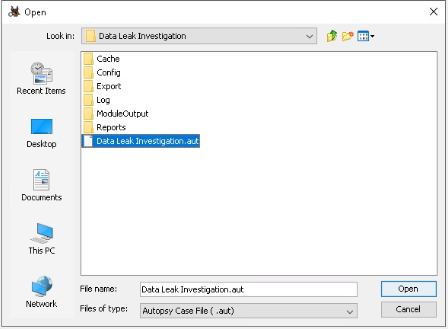
Note: Due to the time the virtual machines take to process the image, a completely analyzed image is already provided. It is recommended that you follow the steps below and then skip to step 11 as the analysis can several hours.

1. Start by opening Autopsy. Double click the Autopsy icon on the desktop. The following Window appears. Select Open Case:

Graphical user interface, text, application

Description automatically generated

1. Navigate to C:\CYBR 440\Data Leak Investigation and open Data Leak Investigation.aut.



1. Start by opening Autopsy. Double click the Autopsy icon on the desktop. The following Window appears. Select New Case:

Graphical user interface, text, application

Description automatically generated

1. On the next screen fill out the case information. The Case Name should be Data Leak Investigation and Base Directory C:\CYBR 440.

Graphical user interface, text, application, email

Description automatically generated

1. On the next screen, fill out that information as follows:
   1. Number: Incident-2021-0145
   2. Examiner:
      1. Name: Your Name
      2. Phone: Your Phone Number
      3. Email: Your Bellevue Email
      4. Notes: A brief set of notes based on your reading of the scenario.

Graphical user interface, text, application, email

Description automatically generated

1. Click Finish and wait a few minutes for Autopsy to create your case. On the next screen, leave the default of Generate new host name based on data source name selected and click Next>.
2. On the Select Data Source Type, leave Disk Image or VM File selected and click Next>.
3. On the Select Data Source click Browse and then navigate to C:\CYBR 440\Data Leakage Case. Select cfreds\_2015\_data\_leakage\_pc.E01, the click Open. Click Next>.
4. On the Configure Ingest, leave the default selected and click Next>.
5. The Add Data source page will begin processing the image file. Wait for it to finish processing and then click Finish.
6. At this point, Autopsy will begin analyzing the files from the disk image. This process can take some time, up to several hours.
7. Repeat steps 4 -9 for each of the removable media files rm#1-3.E01. You do not have to do pc.E01-E04 as those are all imported as part of the initial import. Note, that on step 4, make sure you select the existing host listed at the bottom of page 4 instead of generating a new hostname for each of the removable media. rm#3 will fail as it uses encryption.

Graphical user interface, text, application

Description automatically generated

1. Click on the Web History on the left-hand side of the page and examine the web history entries under Data Artifacts, then answer the following questions.

**Which Cloud Storage websites/services were accessed on this computer?**

Apple iCloud - <https://www.apple.cpm/icloud/>   
Google Drive - <https://www.google.com/drive/>

1. Scroll to the top of the left pane and open Data Sources -> Host Name (should resembled cfreds\_2015\_data\_leakage\_pc.E01\_1 Host) -> vol3 (NTFS / exFAT (0x07): 206848-41940991) -> Windows -> System32 -> config. Make sure config is selected/highlighted then highlight the file named SYSTEM in right hand pane. This is the SYSTEM hive, a database that holds part of the registry settings for the computer. You will notice a registry browser window open on the Application tab underneath the List pane.

Graphical user interface

Description automatically generated with medium confidence

1. In the registry windows (Application), navigate into the ControlSet001 -> Control -> TimeZoneInformation key. Make sure TimeZoneInformation is select/highlighted. Read the keys on the right side of the Application screen.

**What was the timezone set on this computer?**

Eastern Standard Time.

1. In the Listing pane, locate and select the file SOFTWARE. This is another part of the system registry. When performing a forensics investigation for malware, you will often find yourself looking in this location for evidence of malware. Malware entries are often found in but not limited to the following locations:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

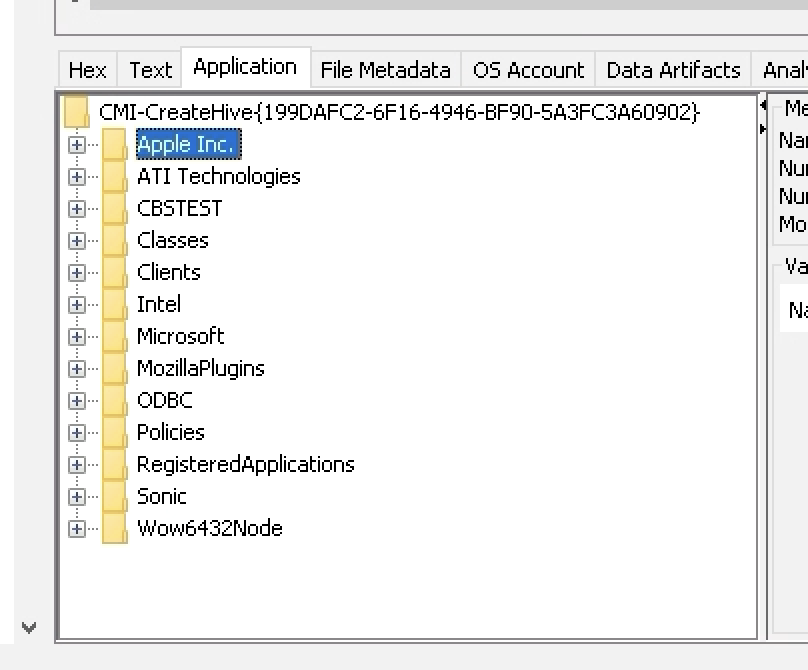
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

HKEY\_CURRENT\_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager

While you will not be required to check these locations, it is important to know where they are. The file SOFTWARE that your examining corresponds to the HKEY\_LOCAL\_MACHINE\Software entry in the registry.

**Take a screen shot of the Application pane and paste it below.**

1. Under the Data Sources -> Host Name (should resembled cfreds\_2015\_data\_leakage\_pc.E01\_1 Host) -> vol3 (NTFS / exFAT (0x07): 206848-41940991) file system, navigate to Users -> informant. Select/highlight informant and then, in the right Listing pane, highlight NTUSER.DAT. This file corresponds to the HKEY\_CURRENT\_USER registry hive. Every user on the system will have their own NTUSER.DAT file. As seen in step 14. there are also values in this database that will often be modified by malware.

**Take a screen shot of the Application pane and paste it below.Graphical user interface, application

Description automatically generated**

1. Collapse the vol3 NTFS volume and navigate to Data Artifacts -> Communication Account -> Email on the left side of the screen. Email and the Web are the two most common vectors for malware, social engineering, and other attacks.

**What is the name of the primary email account on this system?**

spy.conspirator@nist.gov

1. Navigate to Data Artifacts -> E-Mail Messages -> Default -> Default. Make sure the second Default is selected. Email messages contain indicators of compromise such as email addresses, domain names, and malicious files that can be hashed.

**Who is** [**iaman.informant@nist.gov**](mailto:iaman.informant@nist.gov) **primarily communicating with?**

Iaman

**Why are they communicating?**

To share sensitive data.

1. Navigate to Data Artifacts -> Operating System Information. Make sure Operating System Information is selected/highlighted.

**What is the operating system installed on the computer that this image was taken from?**

Windows 7 Ultimate Service Pack 1

1. Navigate to OS Accounts. Make sure OS Accounts is selected.

**Which user accounts are on this computer? Ignore systemprofile, NetworkService, temporary, LocalService, Administrator, and Guest.**

admin11, ITechTeam, informant.

1. Navigate to Data Artifacts -> Web Downloads. Make sure Web Downloads is selected/highlighted. This is another important place to check for malware and indicators of compromise.

**Which two clients for cloud storage were downloaded?**

Apple and Google

**What two programs were downloaded that could help an informant cover their tracks?**

Eraser 6.2.0.2962.exe and ccsetup504.exe

1. Navigate to Data Artifacts -> Run Programs. Make sure Run Programs is highlighted/selected.

**When was ccleaner first run?**

2015-03-25 10:15:50 CDT

**Which cloud drive program was definitely run on this system?**

Google Drive

1. Navigate to Data Artifacts -> USB Device Attached. Make sure USB Device Attached is selected/highlighted. Though less common, USB drives are another vector for malware and other malicious activity.

**What were the device Make and Model of the two USB drives connected to this system?**

SanDisk Corp. – Cruzer Fit

VMware, Inc. – Virtual Mouse

**How many times were the USB drives connected to this computer and what dates/times were they connected?**

On 2015-03-25 08:05:36 CDT, Virtual Mouse connected to the system 6 times.

On 2015-03-25 08:38:00 CDT, Cruzer Fit connected to the system twice.

On 2015-03-25 14:38:09 CDT, Cruzer Fit connected to the system twice.

This lab is a very brief introduction to Autopsy and the information that can be obtained from a forensic image. Special attention was given to some of the places you will look for malware and other malicious indicators. Though the tools and processes between malware investigations and criminal investigations are similar, the goals of each investigation are often very different. Keep the things you checked and could check in mind as we go through a brief introduction to malware analysis in Module 11.