Lab Assignment 1A – Data Acquisition and Triage

Background

The Shield SOC received a network alert for a download for BitTorrent and a Privacy Cleaner utility over the weekend. Both tools are in violation of the company's Acceptable Use Policy (AUP) and may be potentially unwanted programs (PUPs). The incident response team identified the system of interest and requested that the forensic team image the system and perform an analysis.

Note: Students will setup their forensic Virtual Machine (VM) and install forensic applications required for the course. You may use a host Windows system for course materials, but a VM is recommended (See Lab Assignment 0).

Objectives

- Ensure initial tools are installed on student forensic workstations (physical or virtual)
- Create a Custom Content Image using FTK Imager to collect Windows triage artifacts
- Learn how to mount a physical and logical evidence image to interact with a source drive natively

Exercise Preparation

1. **Forensic Workstation Preparation**
   Install required forensic software on your host **Windows system or guest VM**. Some of these steps may have been completed in Lab 0, but are listed here for completeness which allows for exercises and labs to stand on their own.
   a. Download and unzip FTK Imager on a host system or FTK Imager Lite on an external drive (See Lab Assignment 0).
   b. Download and unzip Arsenal Image Mounter (v.3.4.141) on a host system and install the application. https://northeastern-my.sharepoint.com/:u:/g/personal/e_booker_northeastern_edu/EUQKvzfFtIVFrhsLyX-SuPwBWOPu85DCZ6TWyuFFfPiWEQ?e=0Vzm5M
   c. Download and unzip the Assignment Lab 1A contents from OneDrive or obtain them from the instructor in class ("Imaging and Triage Lab.zip" archive for Case Study 1).

   OneDrive Link:
   https://northeastern-my.sharepoint.com/:f:/g/personal/e_booker_northeastern_edu/EgjF7jqB2m1MgHBQxMMm1fYBha6WztkXrFt6_d9IrAJzwg?e=XZYVew

2. **Create a Custom Content Image**

Extract relevant forensic artifacts for additional analysis, which will include creating a **Custom Content Image** AND exporting relevant files from the image for additional analysis. Typically the custom image is created as a container to maintain timestamps and send artifacts to another analyst or archive the evidence in accordance with a data retention policy.

a. Start FTK Imager Lite from an external drive or local analysis system (or FTK Imager client-side application if installed)
b. Load the .E01 image by clicking the **"Add Evidence Item"** toolbar icon or the menu bar option **"File" > "Add Evidence Item…"**
c. Choose **"Image File"** as the source evidence type and select **Next**
d. Navigate to the unzipped "Imaging and Triage Lab" folder and select the **Triage Acquisition.E01** evidence file > **Open** > **Finish**
e. Add artifacts to the custom content image (AND/OR select them individually) and export them to a case file as highlighted in Module 2 demonstrations. The custom image will preserve timestamps. Make sure you select the following folders/files in accordance with a standard Windows triage collection checklist (core artifacts for this course):

I. **NTFS Files**
- NONAME [NTFS]/[root]/$MFT
- NONAME [NTFS]/[root]/$LogFile

II. **Registry Hives *(Required for this lab)***
- NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM
- NONAME [NTFS]/[root]/Windows/System32/config/SECURITY
- NONAME [NTFS]/[root]/Windows/System32/config/SAM
- NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
- NONAME [NTFS]/[root]//Users/srogers/NTUSER.DAT
- NONAME [NTFS]/[root]//Users/srogers/AppData/Local/Microsoft /Windows/UsrClass.dat

II. **Log Files**
- NONAME [NTFS]/[root]/Windows/System32/winevt/Logs (folder)

III. **Optional Memory/Analysis Files (for end of semester)**
- NONAME [NTFS]/[root]/pagefile.sys
- NONAME [NTFS]/[root]/hiberfil.sys (not enabled in this image due to size limitations)

IV. **Additional Shellbag Items**
- NONAME [NTFS]/[root]/Windows/Prefetch (folder)
- NONAME [NTFS]/[root]/Users/srogers/AppData (folder)
- NONAME [NTFS]/[root]/Users/srogers/Recent (folder)

V. **User's Profile (Specific Data)**
- Typically include entire profile for triage, however
- NONAME [NTFS]/[root]/Users/srogers/Desktop (folder)
- NONAME [NTFS]/[root]/Users/srogers/Documents (folder)

- NONAME [NTFS]/[root]/Users/srogers/Downloads (folder)
- NONAME [NTFS]/[root]/Users/srogers/Dropbox (folder)

VI. **Additional Artifacts**

- NONAME [NTFS]/[root]/$Recycle.Bin (folder)
- NONAME [NTFS]/[root]/Windows/INF/setupapi.dev.log

Custom Content Sources

Evidence:File System|Path|File	Options
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|$MFT	Exact
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|$LogFile	Exact
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Windows|System32|config|SYSTEM	Exact
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Windows|System32|config|SECURITY	Exact
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Windows|System32|config|SAM	Exact
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Windows|System32|config|SOFTWARE	Exact
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Users|srogers|NTUSER.DAT	Exact
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Users|srogers|AppData|Local|Microsoft|Windows|UsrClass.dat	Exact
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Windows|System32|winevt|Logs|*	Wildcard,Consider C..
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|pagefile.sys	Exact
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Windows|Prefetch|*	Wildcard,Consider C..
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Users|srogers|AppData|*	Wildcard,Consider C..
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Users|srogers|Recent|*	Wildcard,Consider C..
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Users|srogers|Desktop|*	Wildcard,Consider C..
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Users|srogers|Documents|*	Wildcard,Consider C..
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Users|srogers|Dropbox|*	Wildcard,Consider C..
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Users|srogers|Downloads|*	Wildcard,Consider C..
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|$Recycle.Bin|*	Wildcard,Consider C..
IP_CaseStudy.E01:Basic data partition (4) [60824MB]:NONAME [NTFS]|[root]|Windows|INF|setupapi.dev.log	Exact

f. Once all items are added to the Custom Content Image (19 in this case – will vary in future exercises), select "**Create Image**"

g. Ensure boxes **"Verify images after they are created"** and **"Create directory listings of all files in the image after they are created"** are checked

h. Under Image Destination(s) select "**Add**" and complete the following fields

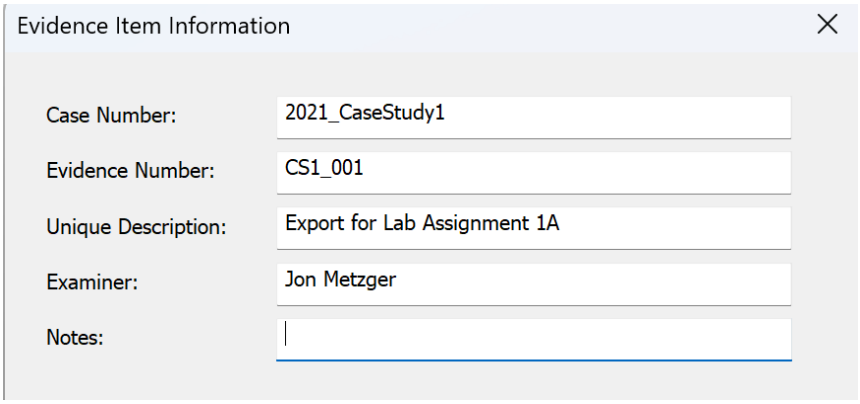
I. **Case Number:** 2021_CaseStudy1

II. **Evidence Number:** CS1_001

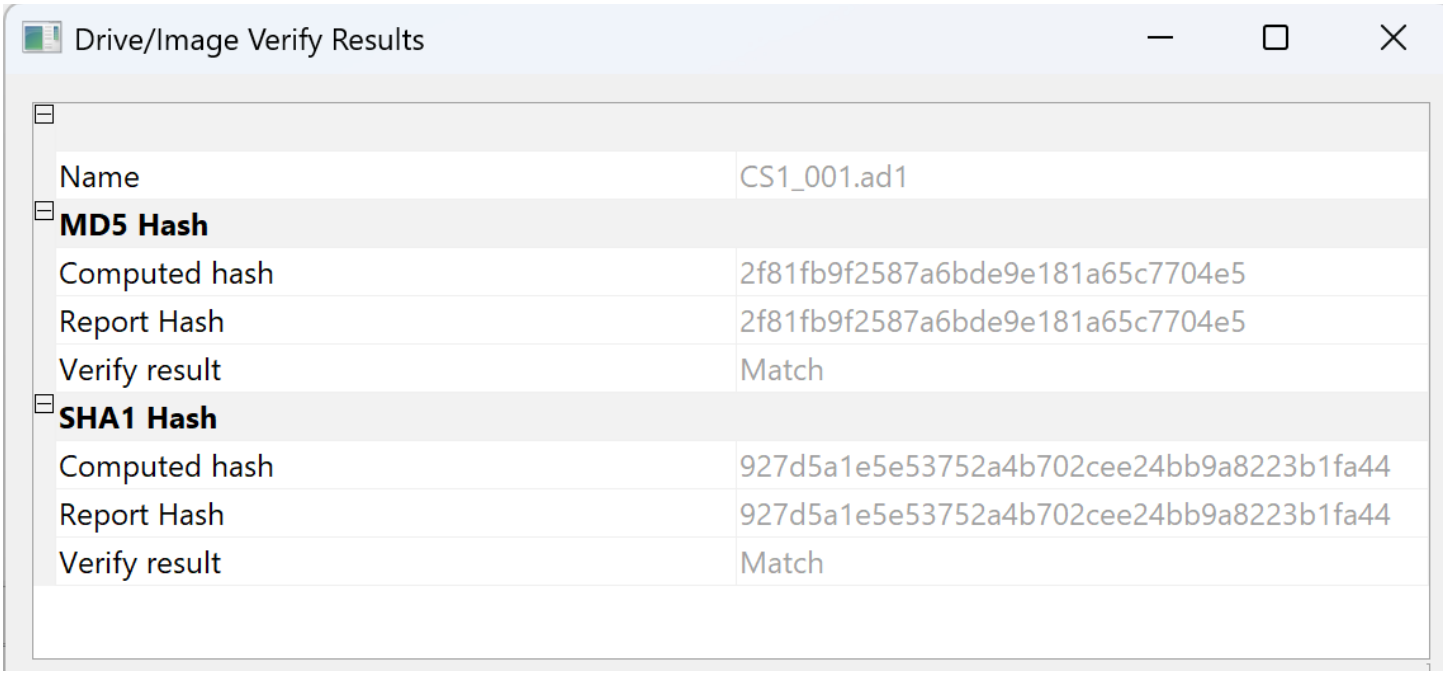
III. **Unique Description:** Export for Lab Assignment 1A

IV. **Examiner:** YOUR NAME

V. **Notes:** Leave Blank



i. Select **Next**
j. A **"Select Image Destination"** splash screen will pop-up; select Browse and choose your case folder or create a new folder (example: Case_Study_1), and click "**OK**"
k. Under "Image Filename (Excluding Extension)" add **CS1_001** and leave the defaults and select **Finish**
l. Select **Start**



DONE

3. **Image Mounting (FTK Imager)**

   Practice the basic concept of mounting an image in FTK Imager or FTK Imager Lite to access the image as a physical drive or share. This allows an analyst to interact with the device using specific tools and run antivirus scans against the image.

   a. Start FTK Imager Lite from an external drive or local analysis system (or FTK Imager client-side application if installed)
   b. Select the **"Image Mounting"** toolbar icon (third from the left) OR select **"File > Image Mounting…"** from the menu bar
   c. Select **"Image File:"** and select the **Triage Acqusition.E01** file. You may also alternatively right-click the root of a loaded evidence file (in the previous custom content image step) and select "Image Mounting…" from the context menu and select the following options defined in the lecture material:
      a. Set **Mount Type:** Physical & Logical
      b. Set **Drive Letter:** Next Available (#:)
      c. Set **Mount Method:** File System / Read Only
   d. Select "**Mount"**
   e. After answering the following questions, you may "Unmount" the volumes or close the application when the lab is completed

Getting the following error when mounting: "Installation of drive mapping drivers failed"

4. **Image Mounting (Arsenal Image Mounter)**

Arsenal Image Mounter (AIM) is a free tool (a commercial version is also available) that can be used to mount disk images that have been collected. AIM can mount .E01, raw disk images, and virtual disks (VMDKs). AIM mounts the contents of a disk image as complete disks in Windows, not as shares or partitions that other products do. This feature is also useful for obtaining access to special artifacts like volume shadow copies.

a. Start Arsenal Image Mounter on a host system
b. Once the license splash screen is presented, select **OK**
c. Select **Mount disk image**
d. Navigate to and select the Case Study 1 image ("Triage Acquisition.E01") and select **Open**
e. Select the **Write temporary disk device** in the **Mount options** window and select **OK**
f. After selecting OK in the Write Temporary disk device selected, students might see the following pop-up about the **write overly file**. Select **No** to remove the existing file.
g. Once mounted, students should be returned to the **Arsenal Image Mounter** main window
h. **Double-click** the mounted drive shown to see the Mount points (mounted drive letter) and **take a screenshot of the entire window** (number of mount points will vary based on the particular evidence)

BELOW

i. In Windows Explorer the mounted partition(s) will be displayed
    i. Students might need to show hidden folders to see all protected files by selecting the **View tab > Show/hide > and checking "Hidden items"**
j. Browse to the **\Users\srogers** folder (students might need to "grant" permission to access the folder). This might take a short while and students may see an access denied dialog, since Windows does not like when NTFS permissions from other file systems (mounted evidence partition(s)) do not match the current file system. Selecting **Continue** might complete this requirement
k. **Take a screenshot** of the Windows explorer folder showing the **NTUSER.DAT** file under the "srogers" user account

BELOW

l. In the main AIM window, you can highlight the mounted evidence and select **Remove** or close the application

DONE

Note: These files will be further analyzed during Lab Assignment 2, 3, and required to complete Case Study 1.

Exercise – Questions

1. **Forensic Workstation Preparation**
    a. Not applicable

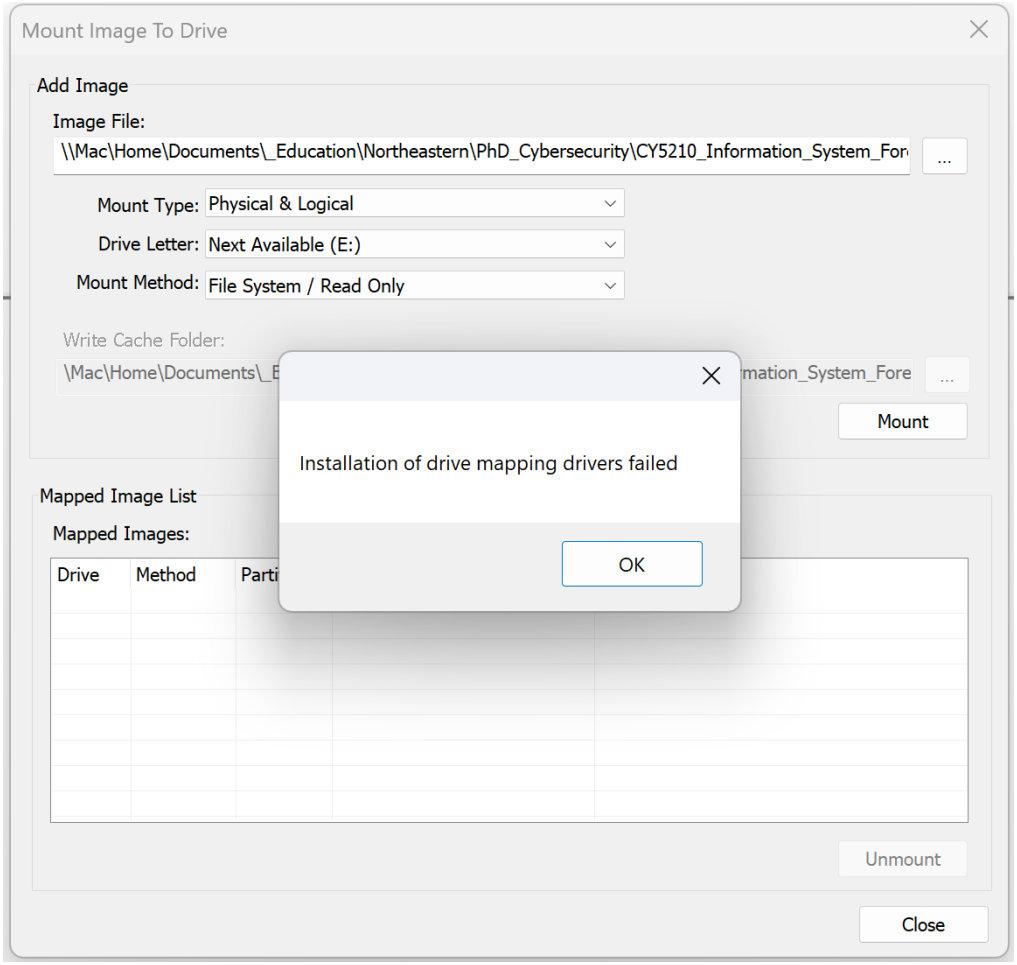
2. **Create a Custom Content Image**
    a. When was the original image acquisition finished (see text file of the evidence image – this is not the text file for the custom collection)?
        i. **Original Image Acquisition Finished: Mon Jan 21 15:17:18 2019**
    b. What are the MD5 and SHA1 hashes of the original image?
        i. **MD5 checksum: ed8faefff8b27232b542a17a08208742**
        ii. **SHA1 checksum: 6226f14c9a2ad69f213548ecc08ccefdde903891**
    c. What is the drive geometry of the original source drive (see text file)?
        i. **Bytes per Sector: 512**
        ii. **Sector Count: 125,829,120**
    d. Review the $Recycle.Bin and the directory for Steve Rogers' SID. What deleted files, if any, might be of interest given the scope of this case?
        i. **NTuser***
        ii. **NTUSER***
        iii. **S-1-5-21-263698462-3103634936-1936700066-1001/*.exe**

        Need to list down the files of interest. Its strange that you found ntuser to be deleted

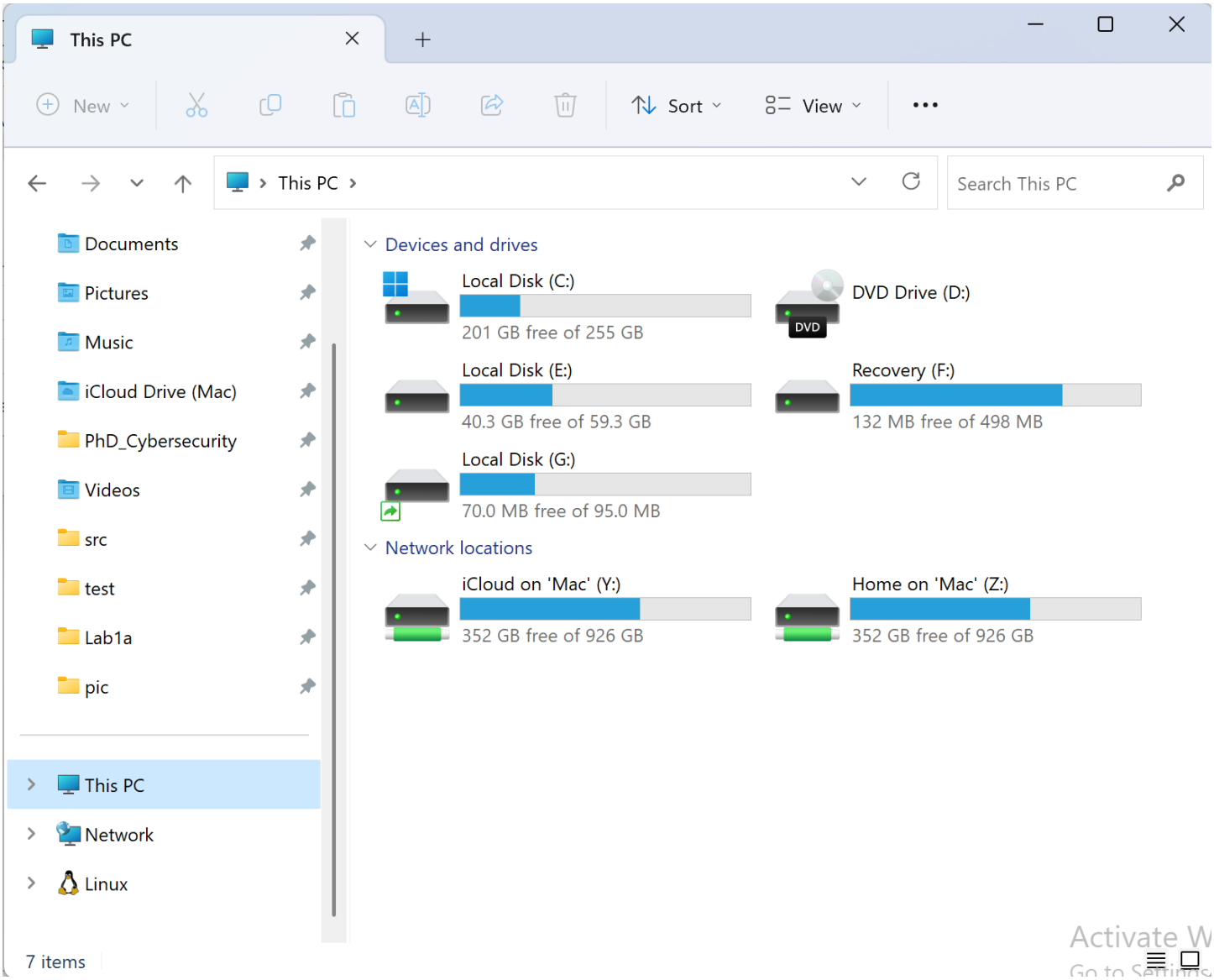
    e. Review the "srogers" Desktop folder. Do you see any files of interest from an investigation perspective?
        i. **BitTorrent.lnk**
        ii. **BitTorrent.lnk.FileSlack**
        iii. **Privacy Erased.lnk**
        iv. **Privacy Erased.lnk.FileSlack**
        v. **Dropbox**
        vi. **TOR files**
    f. Review the "srogers" Download directory. Do any files warrant further investigation? If so, what are their filenames and when were they most likely downloaded?
        i. **BitTorrent.exe 1/20/2019 7:24:37 PM**
        ii. **Installer.exe 1/21/2019 5:30:19 AM**
    g. When was the Tor browser downloaded (Created timestamp)?
        i. **torbrowser-install-win64-8.0.4_en-US.exe 1/20/2019 7:19:48 PM**
    h. Were there any intellectual property files that may have been exfiltrated or stored on a non-corporate SHIELD system?
        i. **Confidential Alloy Expense Accounts.xlsx Because it holds confidential sensitive material that can be harmful towards the organization if exposed.**

3. **Image Mounting (FTK Imager)**
    a. Take a screenshot of the mounted physical and logical drives in the "Mount Image to Drive" dialog box in FTK Imager

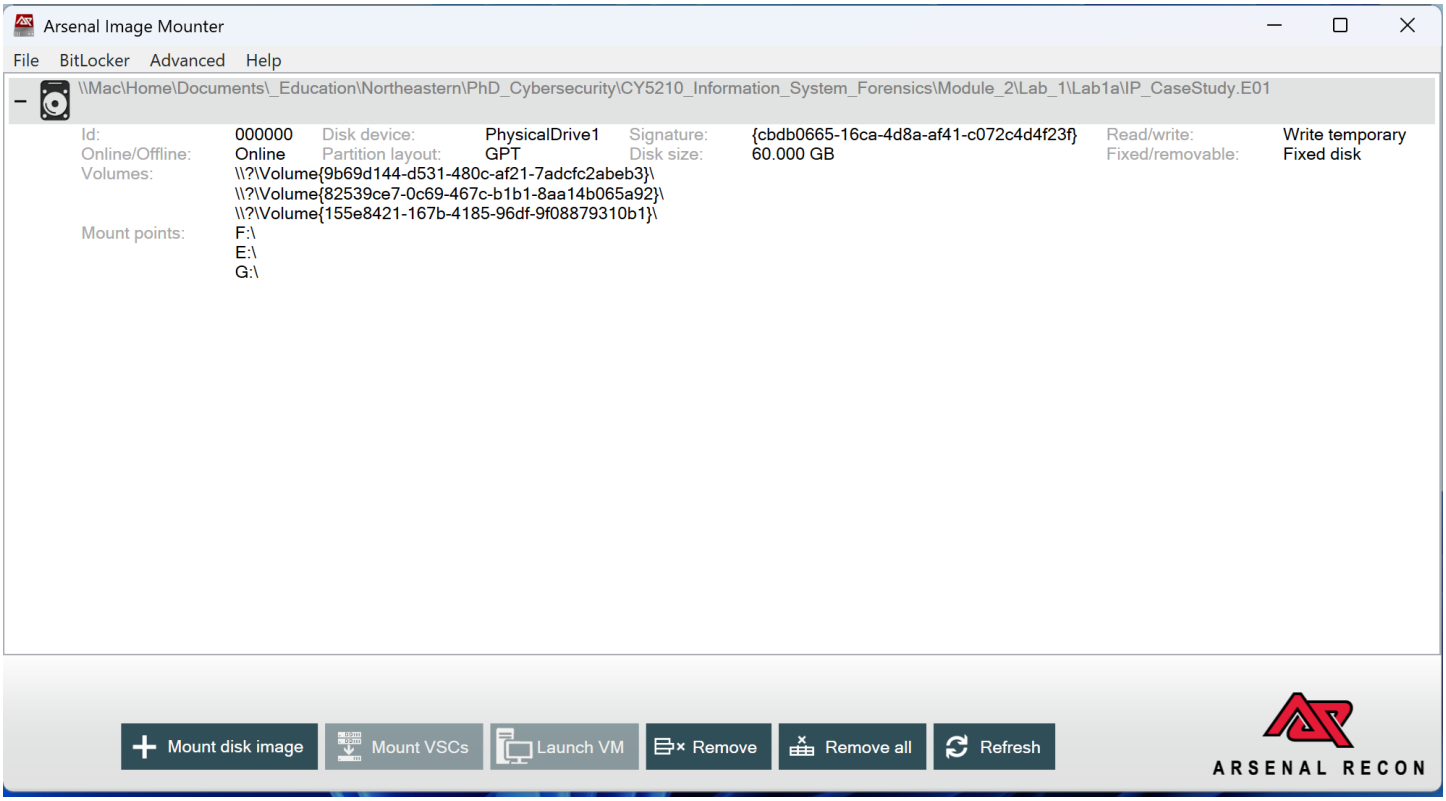
    Mounting wasn't working so I used Arsenal Image Mounter.



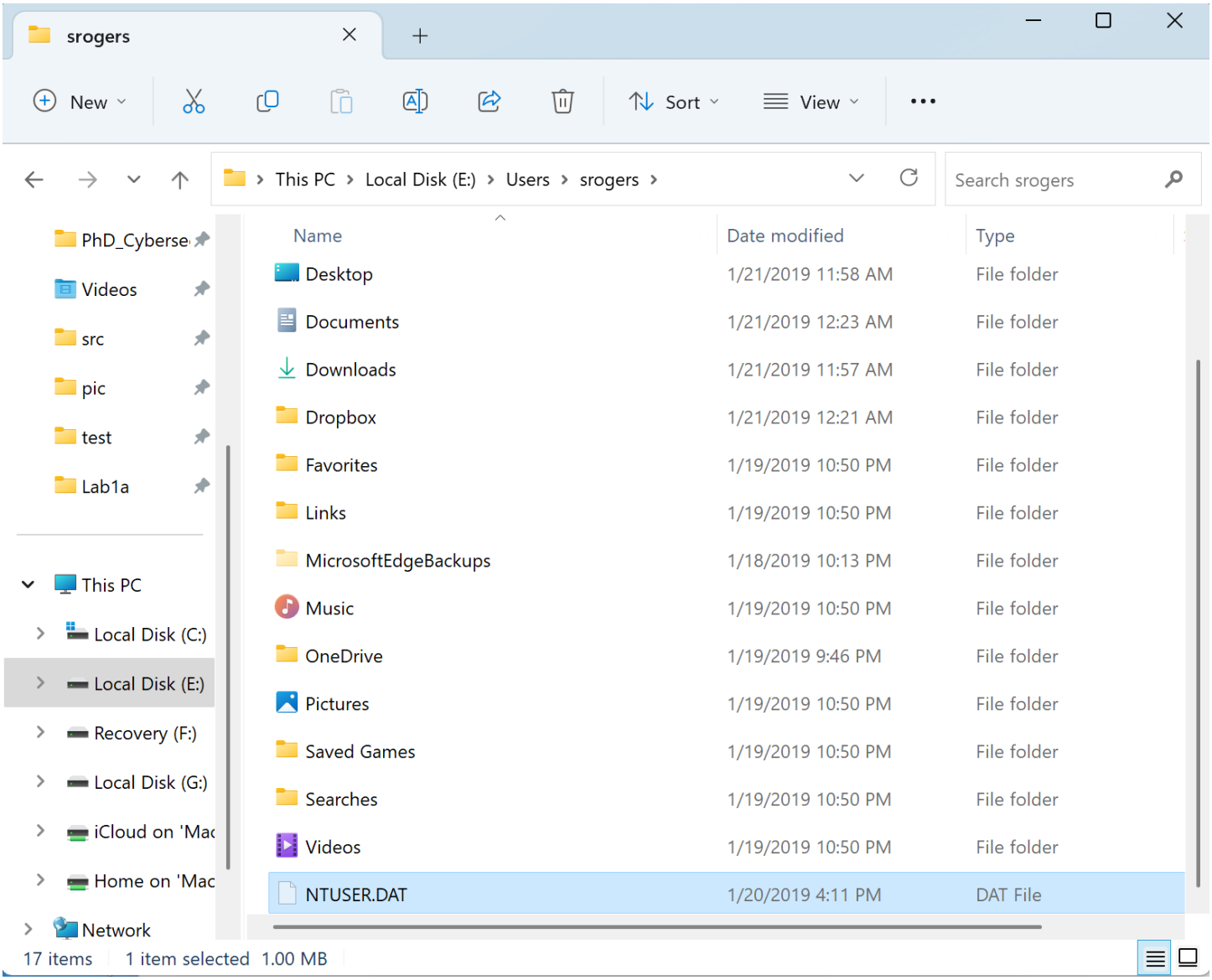
b. Take a screenshot of "This PC" to show the drives connected in Explorer – you can now navigate the file structure in Windows natively and run command-line tools and scripts against the available folders in addition to viewing them with native tools.



4. **Image Mounting (Arsenal Image Mounter)**
    m. Take a screenshot of the entire AIM window (number of mount points will vary based on the particular evidence) that will show that the image(s) are mounted.



n. Take a screenshot of the Windows explorer folder showing the NTUSER.DAT file under the "srogers" user account once the image is mounted and you're "granted" permissions to the protected Users directory.



Exercise—Key Takeaways

- Analysts and investigators should follow the order of volatility when preserving and acquiring data
- A Custom Content Image can preserve data and timestamps while containing evidence of interest
- An evidence image may be mounted physically and/or logically for native OS interaction

***Please submit the final assignment as a single .PDF and any applicable reports as a .ZIP file.**
**Screenshots may also be added to this document when appropriate.