



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Digital Forensics (ACCA7031)

Investigative Process



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Lab Activities are based on

TryHackMe, EC Council – CHFI, Digital Forensics Workbook and other Industry Digital Forensic Curriculum

Objectives

In continuation to our lectures, this hands-on Activity helps in providing you an overview of digital forensic investigation process.

ETHICAL STATEMENT

As discussed during our lectures, it is very important to adhere to Personal Ethics, Professional Ethics, Computer Ethics and Business Ethics.

We, the participants and stakeholders in the digital forensics laboratory, recognize the significance of ethical conduct when using digital forensics tools and processes for academic purposes. Our commitment to ethical standards is grounded in the principles of integrity, privacy, and responsible handling of digital data.

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various digital forensic activities. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using these tools for educational purposes on an outside environment, you should contact your lecturer prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Based on Activity 1, you must be clear on the process of identifying digital evidence, and secure them, acquiring data from its original sources ensuring its integrity using various tools. In continuation to Activity 1, and based on the lecture discussions, complete the following tasks to further understand the process involved in Investigation.

Task 1: Ensuring Integrity of the data

Task 2: Image Acquisition (Alternative Methods)

Task 3: Image Acquisition – Deep Dive

Task 4: Working with Acquired Images

Task 5: Investigating Digital Evidences - 1

ICONS Used in this document:

Find out the outcome/ Answers/ Solution



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.



Recommended Screenshot (with Timestamp) for your Coursework.



Recommended to address this part in your Coursework.

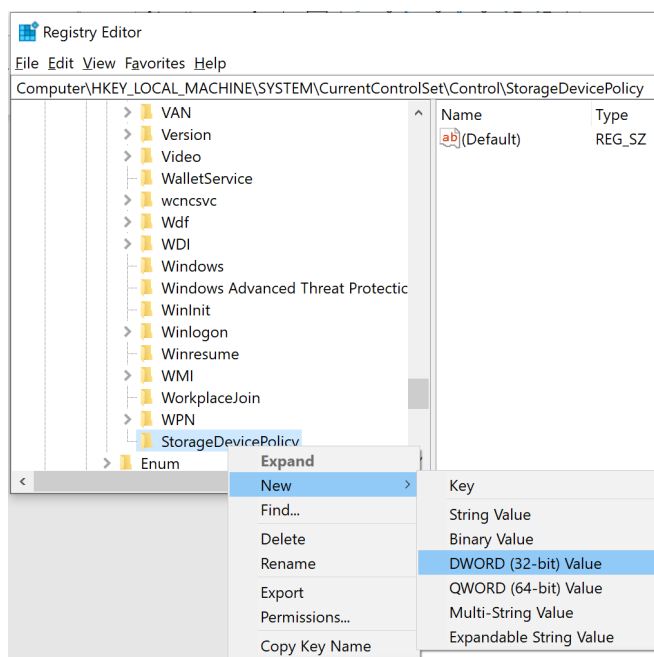
Note: For this activity and other upcoming activities, you shall use any relevant screenshots or discussions to your coursework according to your judgement. I will not be recommending Screenshots/ Recommended part to address in the coursework.

Task 1: Ensuring Integrity

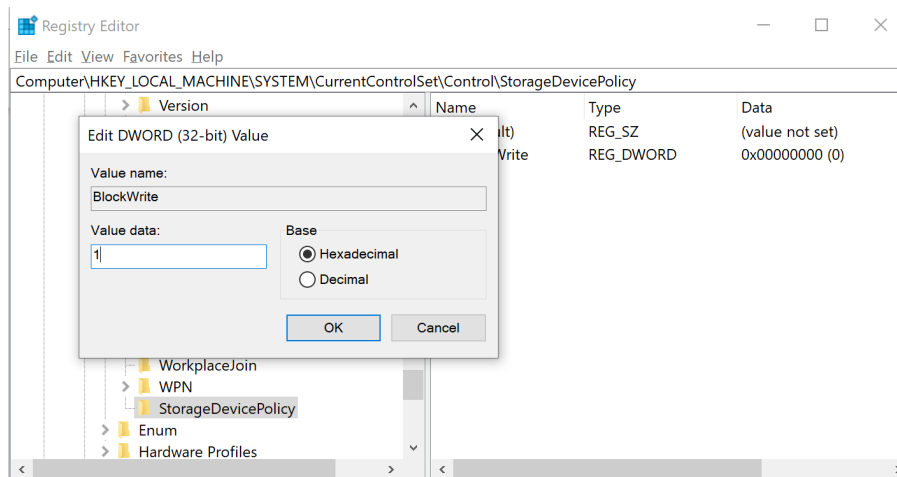
1. Discuss with your Lecturer and Classmates on what are the necessary steps to take in ensuring the integrity of the data.
 - a. Document your reflection in Moodle – Discussion Forum.
2. Do you know that using Windows Registry, you can prevent data from being written to any other external storage/ device?

Login to your Virtual Lab → Windows Client: Make sure your Windows Client in your Virtual Lab could access USB Port.

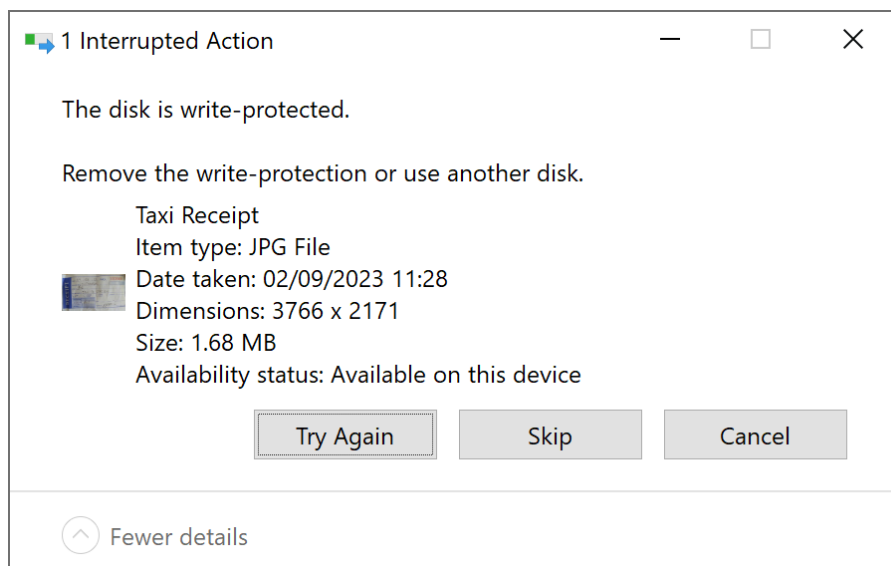
3. Review the options available in Windows Registry to accomplish the task to protect the data from being written to a USB storage/ device.
4. Open Reg Edit
 - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
 - Review the available Control Sets.
 - Create a New Key under Control and name it appropriately. I named it as StorageDevicePolicy.
 - Click New: What are those options? Research and discuss with your Team



- Create a DWORD and name it appropriately. Change the value to 1.



- Check the outcome by connecting a Flash Drive/ HDD and copying data to it.



Task 2: Image Acquisition

During your Handson Activity 1, you might have tried to acquire image from a Windows and Linux OS/MAC OS using FTK Imager. On that note,

1. During acquiring the images, you might have come across different file formats. A brief discussion about file formats like E01, RAW was done during the Lecture session with your Lecturer. Based on your activity and understanding, discuss with your classmates/ team about those available file formats and their purposes.
2. Based on the research done during Handson Activity 1, about the tools for acquiring the image, list out and briefly summarize the pros and cons of the tools you identified.
3. In continuation with the Handson Activity 1, did you manage to acquire the image?
 - a. Did you reach a point where FTK Imager verified the image/ results? Discuss the importance/ key aspects of that verification with your classmates/ team. *(Note: If you have not done this, I strongly recommend you to complete this activity before continuing this).*
4. Try to acquire image with a Command Line Tool
 - a. What are the possible tool options to acquire image using CLI? Did you come across tools during your Handson Activity 1 research?
 - b. Lets try dd tool from chrysocome.net. Have a overview of the tool in the given website and download it. Make sure you download the correct version.
 - i. Download DD (Appropriate version)
 - ii. Open Command Prompt and change directory to the current path where DD is stored. (cd Desktop)
 - iii. Use dd –list to check the mounted devices
 - iv. Image a small folder/ file to a specific destination. *(I would possibly recommend to connect a flash drive with minimal data to get more information)*

```

C:\Users\Nitheesh>cd Desktop\dd-0.6beta3

C:\Users\Nitheesh\Desktop\dd-0.6beta3>dd --list
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

Win32 Available Volume Information
\\.\Volume{247d81de-07ca-470f-b8a8-e1ef59573a7d}\
  link to \\?\Device\HarddiskVolume3
  fixed media
  Mounted on \\.\c:

\\.\Volume{72ba58c2-e79d-4d13-b8ab-039d4e18d353}\
  link to \\?\Device\HarddiskVolume4
  fixed media
  Not mounted

\\.\Volume{4d4d752f-470a-42df-8027-0171080ca43a}\
  link to \\?\Device\HarddiskVolume1
  fixed media
  Not mounted

\\.\Volume{2a287635-402a-11ee-91ce-806e6f6e6963}\
  link to \\?\Device\CdRom0
  CD-ROM
  Mounted on \\.\d:

\\.\Volume{c75650f8-6e89-11ee-91da-18d6c704f6d7}\
  link to \\?\Device\HarddiskVolume6
  removeable media
  Mounted on \\.\e:

```

v. Create the image specifying the source and the destination.

```

C:\Users\Nitheesh\Desktop\dd-0.6beta3>dd if=\\.\e: of=c:\output.dd bs=1m --size --progress
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

Unknown suffix m
Invalid block size

C:\Users\Nitheesh\Desktop\dd-0.6beta3>dd if=\\.\e: of=c:\output.dd bs=1M --size --progress
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

14,906M
14906+1 records in
14906+1 records out

```

vi. Check the dd image file.

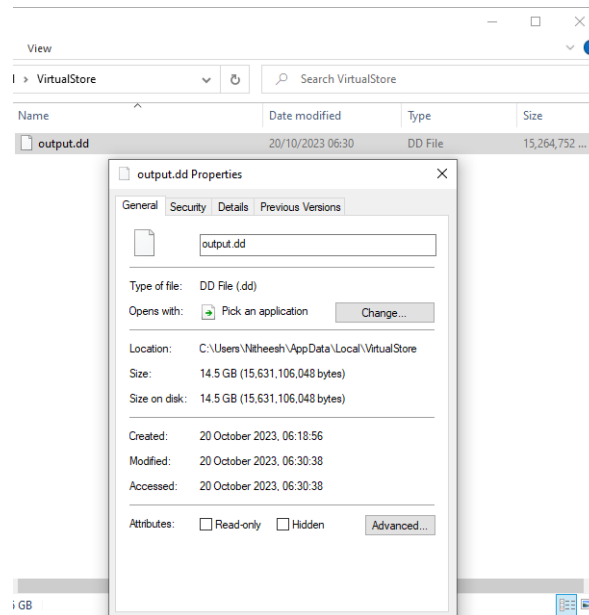
ore

View

VirtualStore

Search VirtualStore

Name	Date modified	Type	Size
output.dd	20/10/2023 06:30	DD File	15,264,752 ...



- vii. Try to implement Filter options and acquire the image and document the outcome.
- viii. Build your Virtual Topology. Use DD Tool or other relevant tool to create a Forensic image over the network using file share.

Task 3: Image Acquisition – Deep Dive

Pre-requisite: Handson Activity 1 and Handson Activity 2 (Task 2)

Checkpoint: Based on the discussions about the image formats during the lectures and discussions with your classmates/ team, you must now be very clear on what's the purpose and scope of these different formats. If you are not clear, please discuss again with your Team and Lecturer.

Use the FTK imager (Refer Handson Activity 1), and create an Image with partitions in a E01 Format.

On completing Task 2 above, you must have a DD (RAW) image Format.

Keep all the images you acquire safe. You will be using in the future Handson Activities as well.

1. Deep dive to look at the image acquired to understand the file system. Always, a file system stores the data in a logical way in any media. The Operating Systems uses the logical methods to retrieve the data when required. A lot of algorithms involved in this process. However, as a Forensic Analyst, understanding the file system will help you to correlate the manner in which the data is arranged, leveraging an option to identify the meta data.
 - a. What are the possible tool options to identify and analyse the file system of the image you acquired? Research, discuss with your Classmates/ Team and identify tools. Submit your reflection in Moodle – Discussion Forum
 - b. We will be using The Sleuth Kit. Go to the website and look at the available documentation. Did you come across Autopsy? Have an overview of this tool. We might be using in our future activities.
 - c. Download the Sleuth Kit for your Operating System and save it.
 - d. Check the details of DD (RAW) File. You have to make sure you give the correct path of the file. Set your path to the bin folder of Sleuth Kit.

```
c:\Users\Nitheesh\Desktop\Handson Activity 2\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32\bin>mmls output.dd
```
 - e. Check the details of E01 File. You have to make sure you give the correct path of the file. Set your path to the bin folder of Sleuth Kit.

```

C:\Users\Nitheesh\Desktop\Handson Activity 2\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32\bin>fsstat -i ewf myimage.E01
FILE SYSTEM INFORMATION
-----
File System Type: FAT32

OEM Name: MSDOS5.0
Volume ID: 0x1881387d
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 10440
Free Sector Count (FS Info): 2058552

Sectors before file system: 0

File System Layout (in sectors)
Total Range: 0 - 2068991
* Reserved: 0 - 4165
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 4166 - 6178
* FAT 1: 6179 - 8191
* Data Area: 8192 - 2068991
** Cluster Area: 8192 - 2068991
*** Root Directory: 8192 - 8199

METADATA INFORMATION
-----
Range: 2 - 32972806
Root Directory: 2

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 2 - 257601

```

- f. From the outputs after analysing DD File and E01 File, what details could you analyse as a Forensic Analyst? Write a report and submit it individually. However, you could discuss with your team/ classmates before submitting. (Hint: Analyse Metdata, Directory Structure, File System, File Signature, etc)
- g. Try analysing other file formats. Do a research on tools and procedures to analyse the file system of other formats listed below.

Please Select the Destination Image Type

☒ Raw (dd)

☐ SMART

☐ E01

☐ AFF

- h. Document the outcome.

Task 4: Working on Acquired Images

Pre-requisite: Handson Activity 1 and Handson Activity 2 (Task 2, 3)

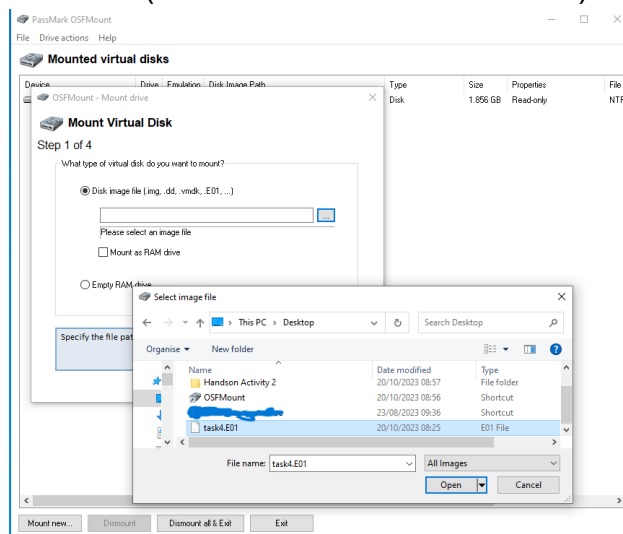
An image you are working on is likely the evidence that need to be analysed and presented to the court of law. Assuming that you have understood the purpose of imaging the evidence and ensuring its integrity during our earlier activities, we proceed ahead in analysing the acquired image.

Keep in mind:

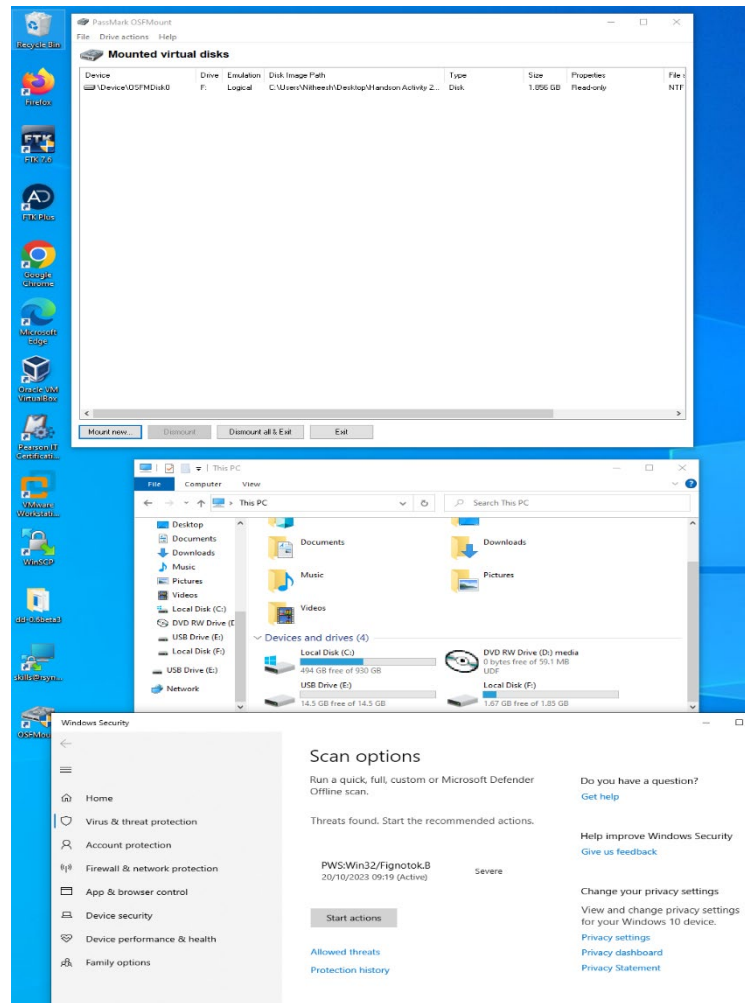
- + **Always verify the file's integrity**
- + **Pay attention to very discrete information.**
- + **Key Factors: Hidden Files, Malwares, etc**

Warning: For this activity, we might be using image files from external sources. The image files are available to download from your Lecturer. The download may contain malicious files. Don't attempt to do anything other than instructed (even in a virtual network)

1. Do a research and discuss with your classmates/ team about available tools to mount the acquired images. Note: You must have your own RAW File and E01 file. In addition to those two files, download another file from the link above. Read the warning before downloading. Submit your reflection in Moodle – Discussion Forum
2. For demonstration, OSFMount is used here. You shall use any other mount tools as you pick during the discussion.
 - a. Install OSFMount. It is a Free Tool from Pass Mark Software.
 - b. Mount the images and analyse the details:
 1. Mount E01 Image and analyse the details
 2. Mount DD Image and analyse the details
 3. Mount task4.E01 image from the download link and analyse the details. (It contains Malicious Files in it)



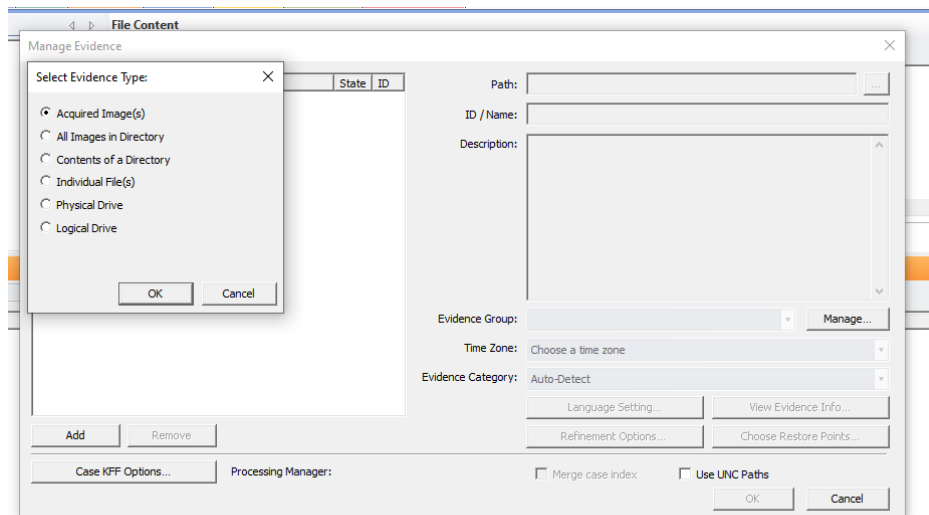
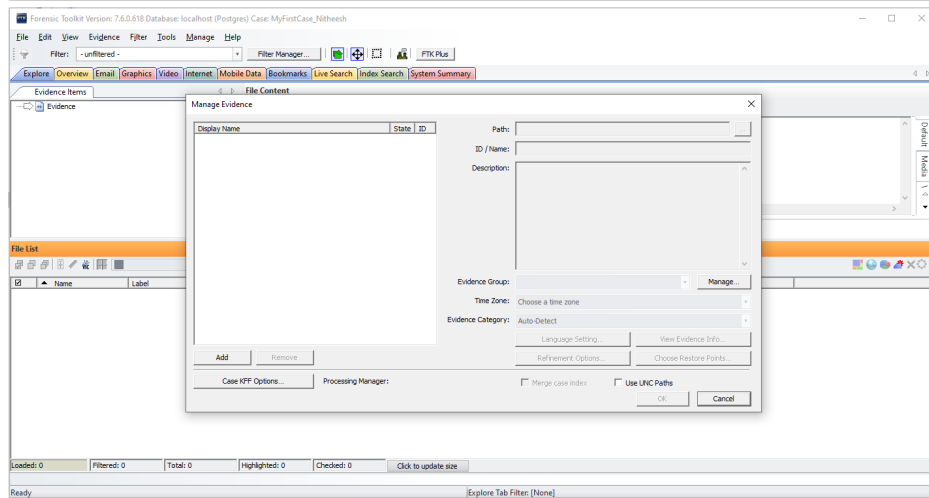
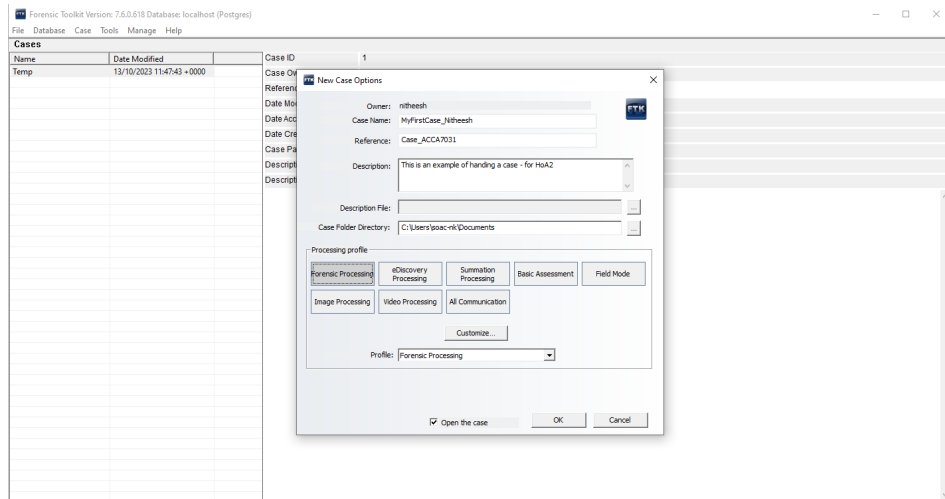
4. Scan the drive to check:

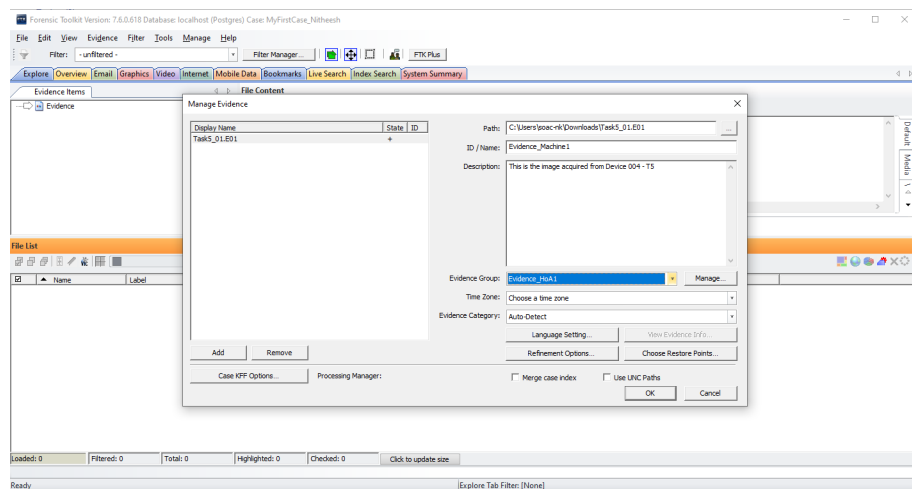
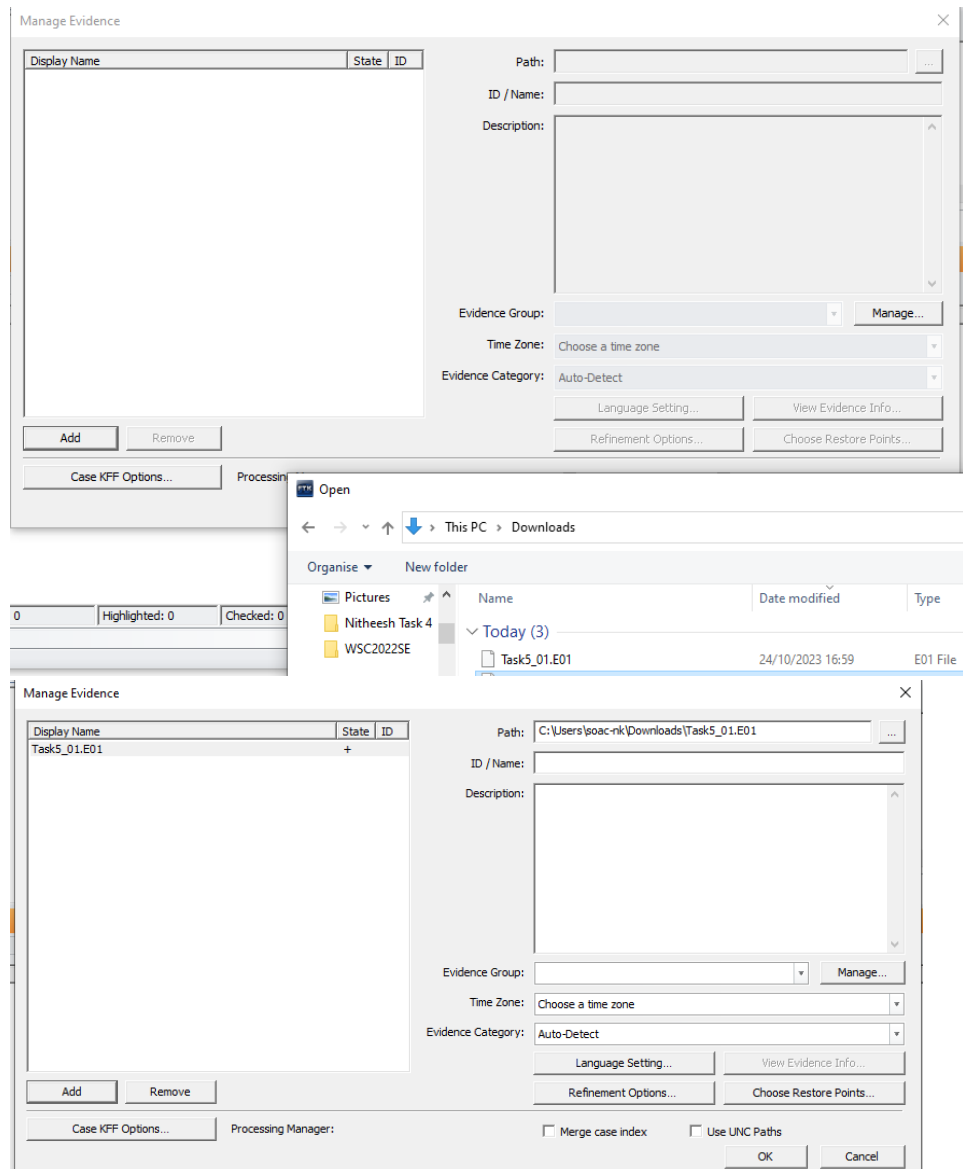


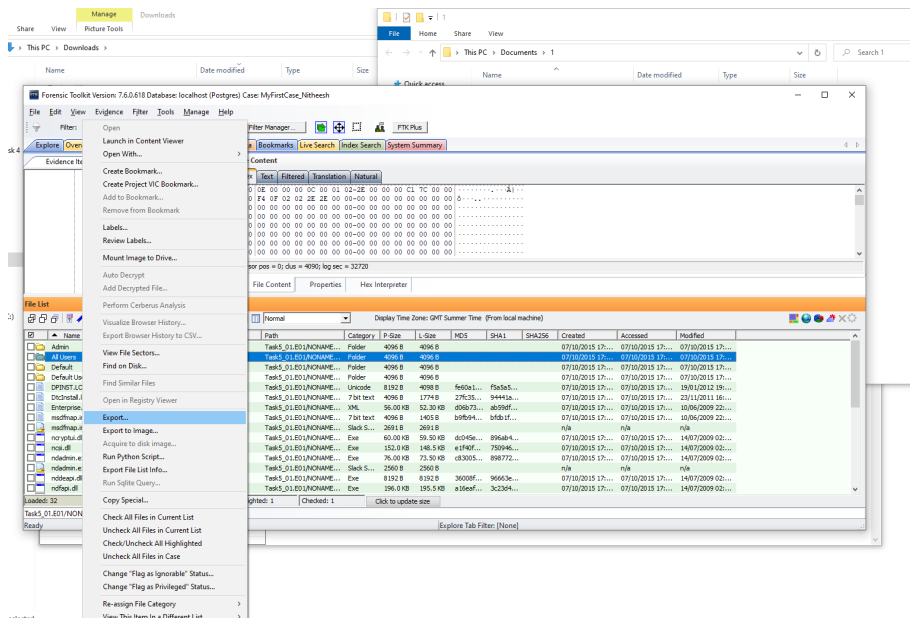
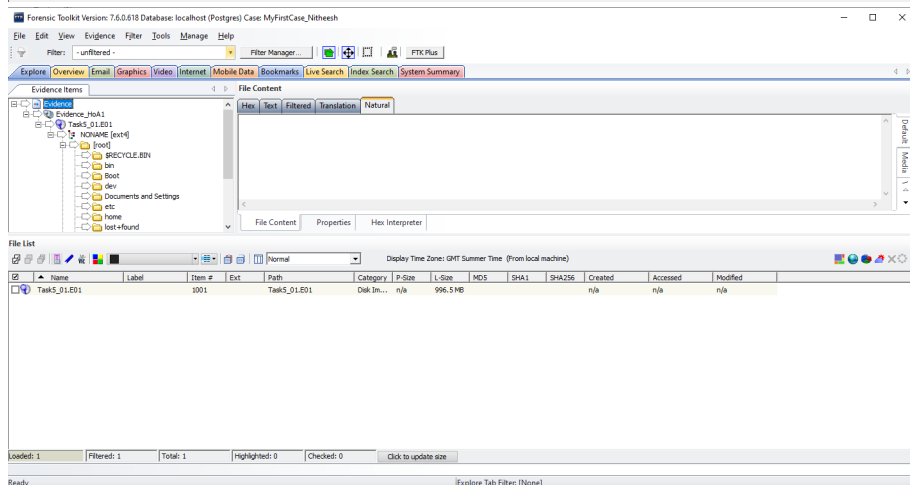
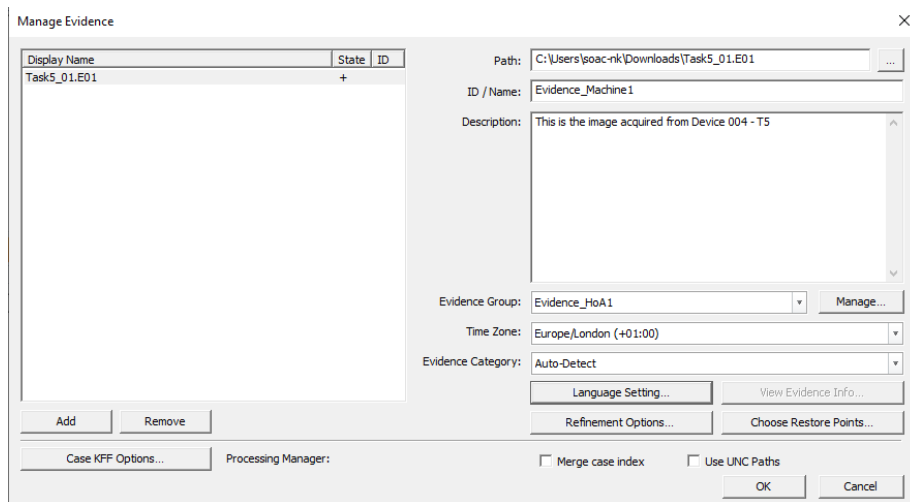
5. Could you discuss this situation:

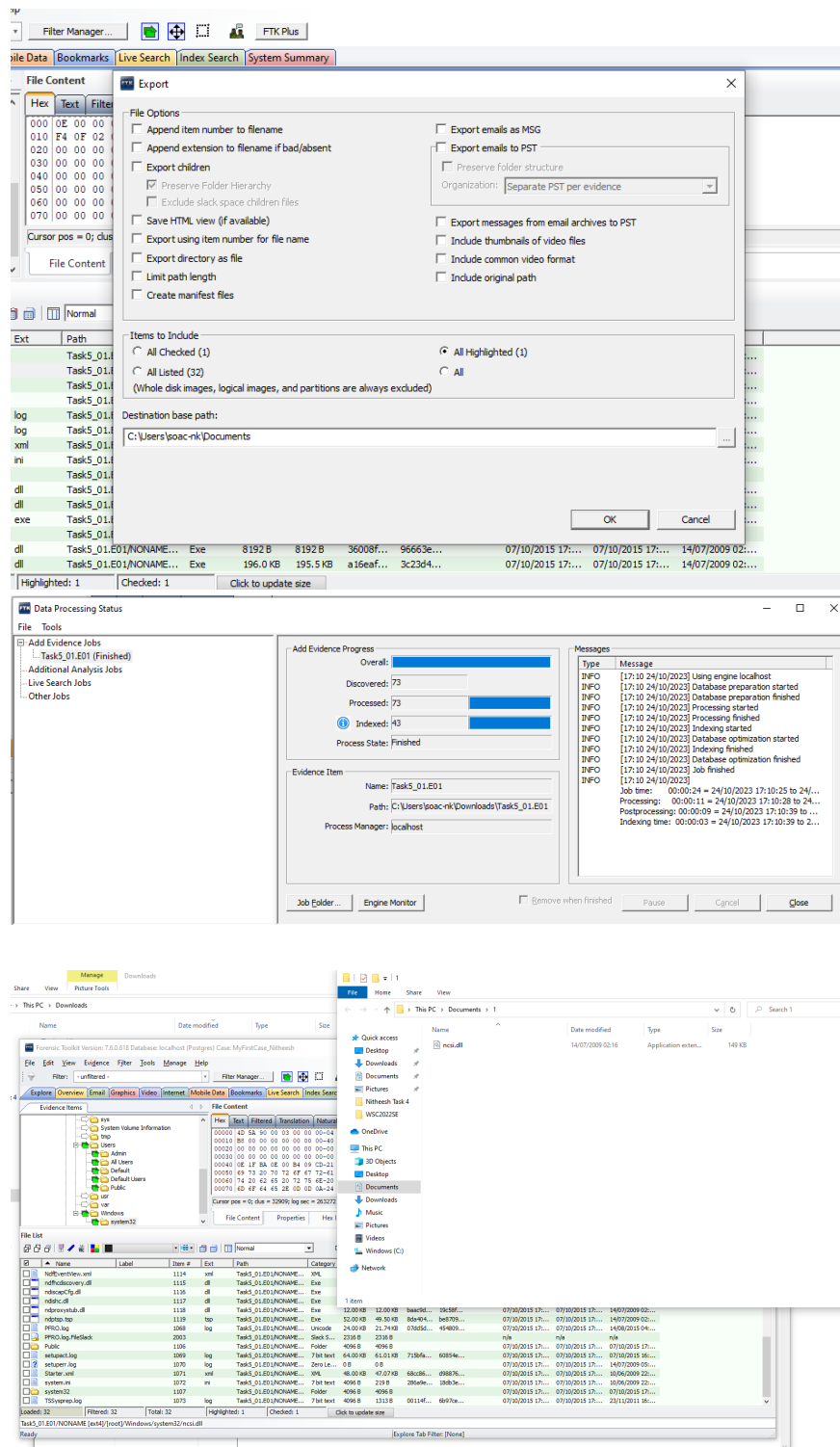
1. What if you acquire an image, mount it and see some malicious files in it? What actions would you take?
 2. What was the threat identified in the task4.E01 image? Could you deep dive and identify the location of the threat and find more information on the threat?
- c. Mount task4_02.E01 image from the download link and enumerate the autorun locations.
1. Identify any malware (including virus, trojans, etc)
 2. Check if you need to remove any unwanted programs
 3. Check for autorun entries, that could eventually slow down the boot process and affect overall system performance. Identify and disable unnecessary autoruns.
- For Autorun entries, download Sysinternals Suite and run it.**
4. Check for any security risks. Identify and mitigate risks associated with autoruns. Analyse using "Analyse Offline System"
 5. Understand your system behavior – look at how softwares and services are configured on startup.

- d. Mount task4_03.E01, task4_04.E01 and task4_05.E01 images from the download link and enumerate the autorun locations.
 1. Identify any malware (including virus, trojans, etc)
 2. Check if you need to remove any unwanted programs
 3. Check for autorun entries, that could eventually slow down the boot process and affect overall system performance. Identify and disable unnecessary autoruns.
 4. Check for any security risks. Identify and mitigate risks associated with autoruns. Analyse using “Analyse Offline System”
 5. Understand your system behavior – look at how softwares and services are configured on startup.
 - e. Mount task4_06.E01 image from the download link and enumerate the autorun locations.
 1. Identify any malware (including virus, trojans, etc)
 2. Check for autorun entries, that could eventually slow down the boot process and affect overall system performance. Identify and disable unnecessary autoruns.
 3. Check for any security risks. Identify and mitigate risks associated with autoruns. Analyse using “Analyse Offline System”
 4. Look at HKEY_Current_User\SOFTWARE\Microsoft\CurrentVersion\Run. What is your observation?
 5. How many browser helper objects exists on the computer?
 6. Understand your system behavior – look at how softwares and services are configured on startup.
3. Working on Forensic Images
- a. Open Forensic Toolkit. Login using Cisco and Cisco. Go to File→ New User
 - b. Login using your credentials.
 - c. Create a New Case. Refer to the screenshot below. Open a Case.









- Analyse the Image file and try to recover evidences.
- Download task05_02.E01 and create new case. Analyse the evidence.
- Use other tools to analyse the evidence (task05_01.E01 and task05_02.E01) to find/ gather further more information.
- Document the steps with screenshots, pros and cons of each tools and additional evidences gathered. (You shall try Autopsy, EnCase etc)
- Review: From the task05_02.E01 image,

1. Did you manage to recover Microsoft word document? If yes, how many documents?
2. Did you manage to recover exe files? If yes, how many files? And what are the details?
3. Did you manage to recover spreadsheets? If yes, how many documents?
4. Any details you could gather from the collected/ gathered evidences?

Task 5: Investigating Digital Evidences - 1

Pre-requisite: Handson Activity 1 and Handson Activity 2 (Task 2, 3, 4)

With all the lectures done so far, and completing the above tasks, you should be confident in

➔ **Knowledge and Understanding:**

- **The Digital Forensics Process and Methods**
- **Importance of ensuring Integrity of the evidence**

➔ **Cognitive, Intellectual and Practicals:**

- **Acquire the evidence**
- **Verify the integrity of the evidence**
- **Working on the evidence**

This activity focuses on analysing the digital evidence OF M57 Company. Refer to M57.biz Files in your Virtual Machine (S-DC). Use them to Analyse and record the findings.

Note: You are allowed to use the reflection on the findings for this activity in your coursework assessment.

Case Background:

A functioning workstation originally belonging to m57.biz was purchased on the secondary market. The buyer (Aaron Greene) realizes that the previous owner of the computer had not erased the drive and finds illegal digital images and videos on it. Aaron reports this to the police, who take possession of the computer.

Police forensics investigators determine the following:

- The computer originally belonged to m57.biz
- The computer was used by Jo, an M57 employee, as a work machine.

Police contact Pat McGoo (the CEO). Pat authorizes imaging of all other computer equipment onsite at M57 to support additional investigation. Police further pursue a warrant to seize a personal thumb drive belonging to Jo.

Tasks

1. Launch the evidence to Investigate:
 - a. Launch FTK and Add your evidence. Import the followin:

1. "jo-2009-12-11-002.E01" (Jo's workstation)
 2. "jo-favorites-usb-2009-12-11.E01" (Jo's USB drive).
- b. Process the evidence with default options, ensuring "File Signature Analysis" and "MD5 Hash" are enabled.
 - c. Navigate to the "Explore" tab in FTK and filter for image and video files (e.g., *.jpg, *.mp4).
 - d. Examine metadata (e.g., file creation/modification timestamps, user profiles) for files Eg: Files containing "cat" in the filename.
 - e. Check the "Internet/Chat" tab for browser history or saved passwords linking Jo to these files.
 - f. Analyze the Recycle Bin ("\$Recycle.Bin") for deleted files or folders.
 - g. Record your Analysis. Export a screenshot of a relevant file's metadata and note its hash value.
2. Reflect on how reliable is the metadata (e.g., timestamps) in linking Jo to the illegal files? What factors could affect its accuracy? (If any)
 3. Reflect on challenges you faced when analyzing this image. How did you overcome them?

Overall Reflection

Note: Make sure you make snippets of the work with timestamp (Timestamp on the Host Machine and not the virtual environment) to use them for Demonstration as part of your Assessment

1. Understanding on the concepts discussed in the lecture and its relation to the activity done.
2. Understanding about various tools used and various frameworks available for DF Investigation process.
3. Rate yourself: Understanding Image Acquisition and Analysis

-----End of Activity-----