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

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.

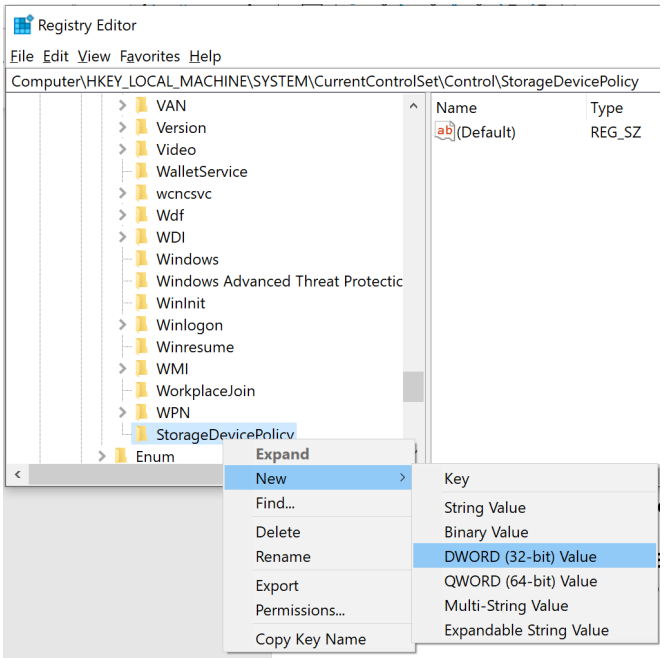
Note: For this activity and other upcoming activities, you shall use any relevant screenshots or discussions to your coursework according to your judgement. I will not be recommending Screenshots/ Recommended part to address in the coursework.

Task 1: Ensuring Integrity

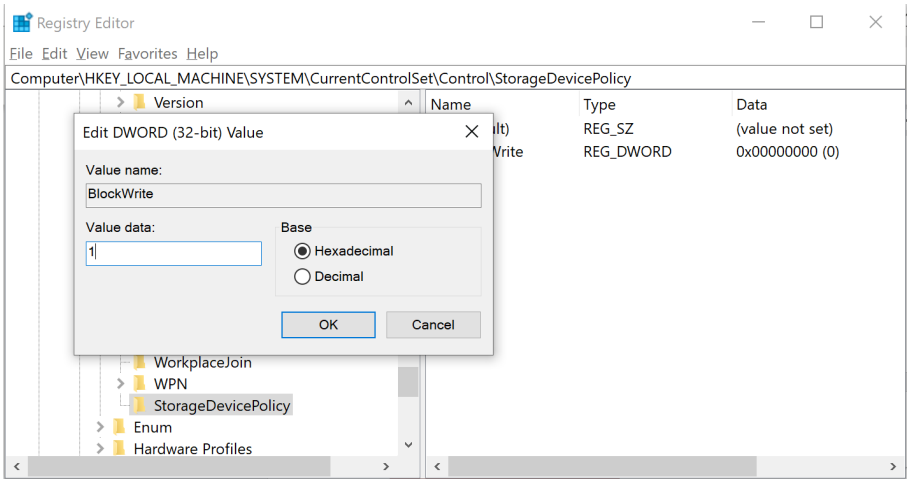
1. Discuss with your Lecturer and Classmates on what are the necessary steps to take in ensuring the integrity of the data.
    a. Document your reflection in Moodle – Discussion Forum.
2. Do you know that using Windows Registry, you can prevent data from being written to any other external storage/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

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

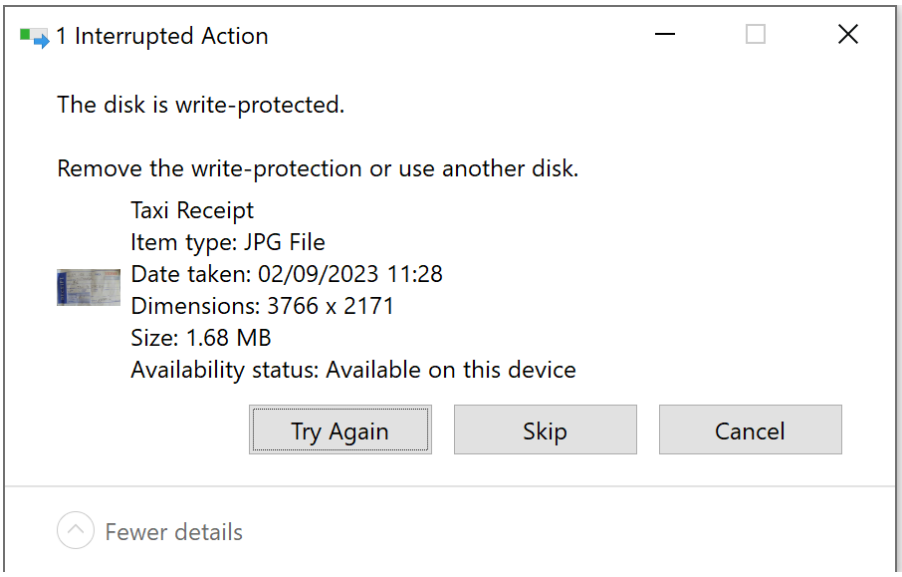
3. Review the options available in Windows Registry to accomplish the task to protect the data from being written to a USB storage/ device.
4. Open Reg Edit
    - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
    - Review the available Control Sets.
    - Create a New Key under Control and name 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 Acquistion

During your Handson Activity 1, you might have tried to acquire image from a Windows and Linux 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. Submit your reflection in Moodle – Discussion Forum
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. Submit your reflection in Moodle – Discussion Forum
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).* Submit your reflection in Moodle – Discussion Forum addressing the size of the media, sectors, serial numbers, Hashing etc.

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? Submit your reflection in Moodle – Discussion Forum
   - **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)*

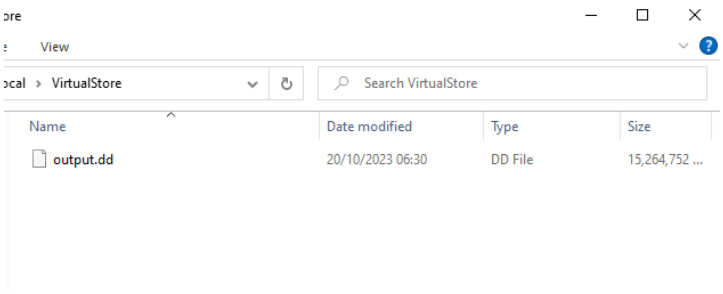
```
C:\Users\Nitheesh>cd Desktop\dd-0.6beta3

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:
```

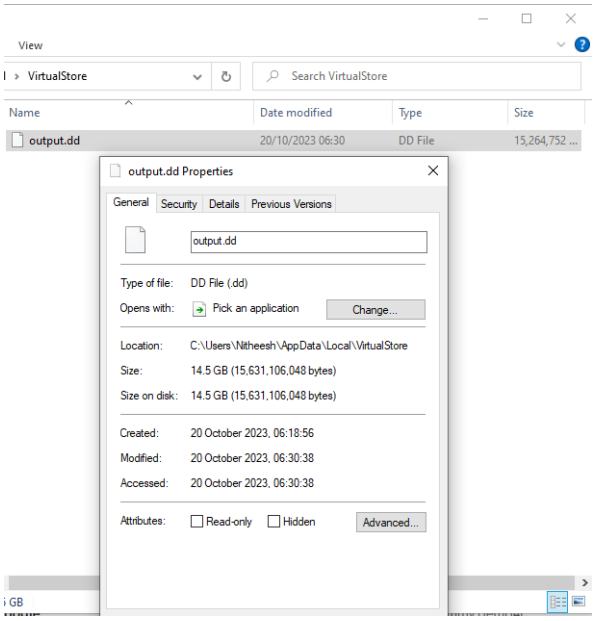
```
\\.\Volume{c75650f8-6e89-11ee-91da-18d6c704f6d7}\
  link to \\?\Device\HarddiskVolume6
  removeable media
  Mounted on \\.\e:
```

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.





vii. Try to implement Filter options and acquire the image. Discuss with your Classmates/ Team and document the outcome.

viii. Use your Virtual Topology used for Ethical Hacking Module. It is a connected Network. Use DD Tool or other relavent tool to create a Forensic image over the network using file share.

Task 3: Image Acquistion – 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.

Note that, you need to submit all the image files in a Shared folder. Link to the shared folder is available in Moodle. Always upload the image files with your name and hash file making sure, it is not altered by others.

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 corelate 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.

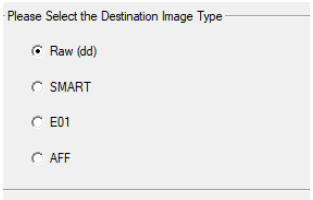
```
C:\Users\Nitheesh\Desktop\Handson Activity 2\sleuthkit-4.12.1-win32\sleuthkit-4.12.1-win32\bin>mmls output.dd
```

   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.



h. Document the outcome.

Task 4: Working on Acquired Images

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

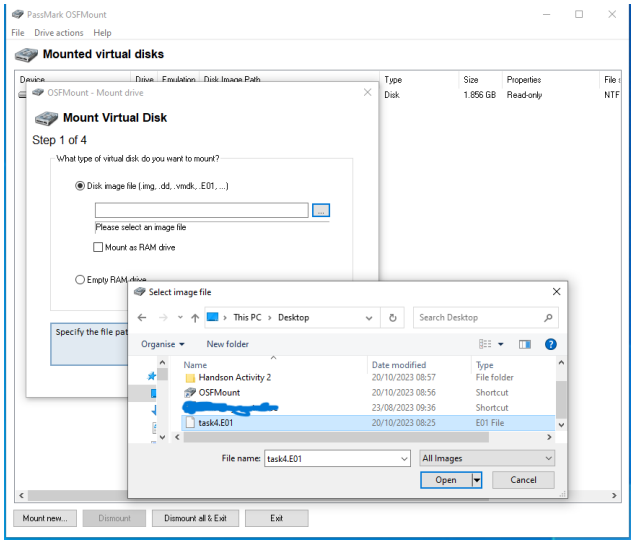
An image you are working on is likely the evidence that need to be analysed and presented to the court of law. Assuming that you have understood the purpose of imaging the evidence and ensuring its integrity during our earlier activities, we proceed ahead in analysing the acquried image.

Keep in mind:

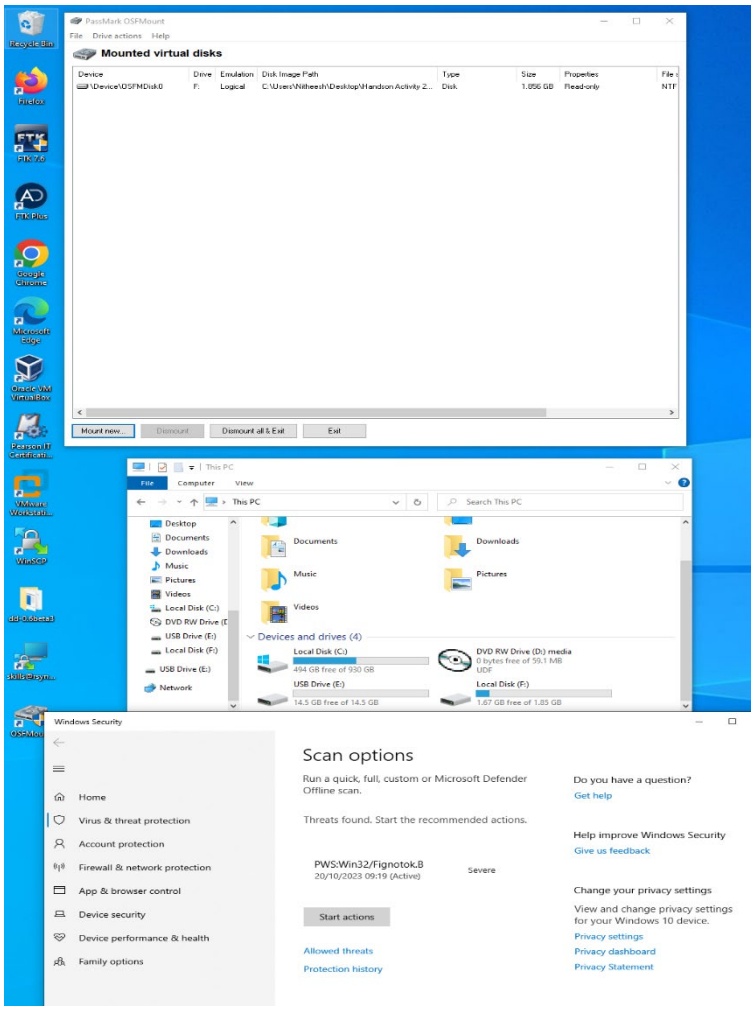
- **Always verify the file's integrity**
- **Pay attention to very discrete information.**
- **Key Factors: Hidden Files, Malwares, etc**

Warning: For this activity, we might be using image files from external sources. The image files are available to download in the Lecturer_SharedFolder. 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.

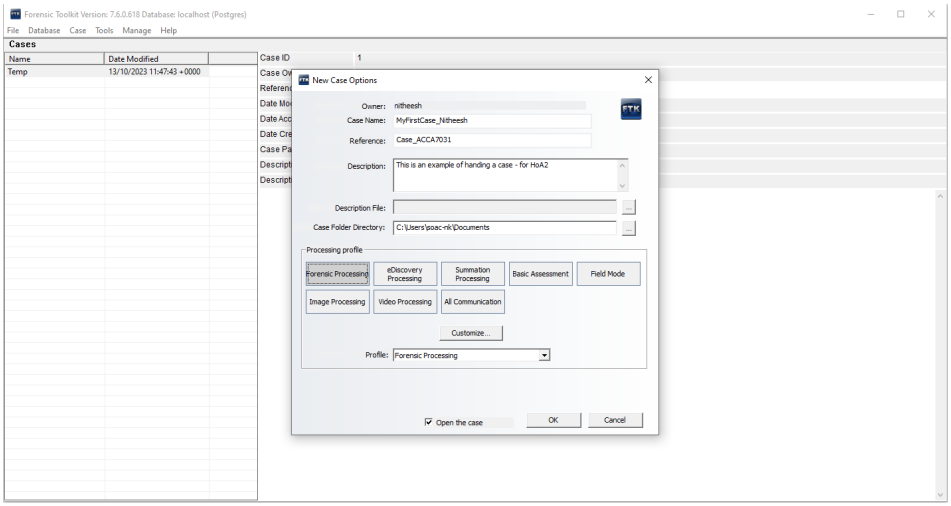
   For Autorun entries, download Sysinternals Suite and run it.

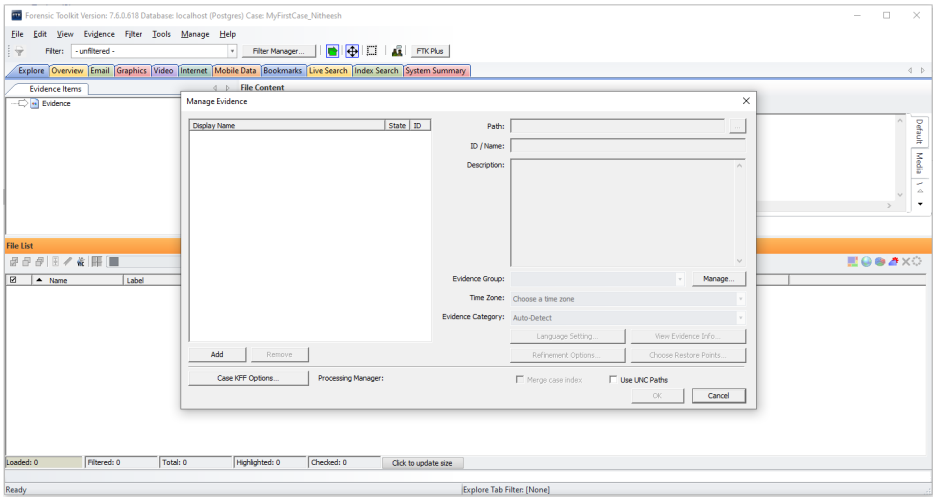
   4. Check for any security risks. Identify and mitigate risks associated with autoruns. Analyse using “Analyse Offline System”
   5. Understand your system behavior – look at how softwares and services are configured on startup.

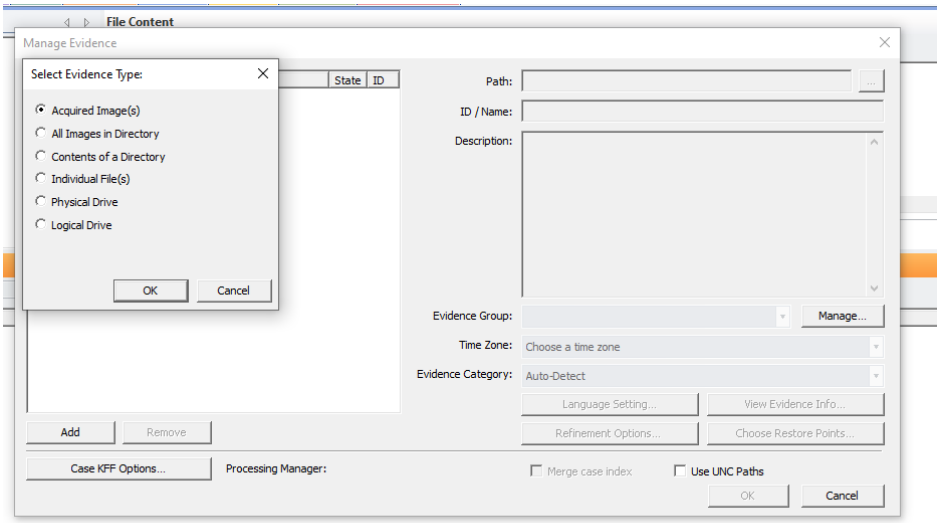
d. Mount task4_03.E01, task4_04.E01 and task4_05.E01 images from the download link and enumerate the autorun locations.
    1. Identify any malware (including virus, trojans, etc)
    2. Check if you need to remove any unwanted programs
    3. Check for autorun entries, that could eventually slow down 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.

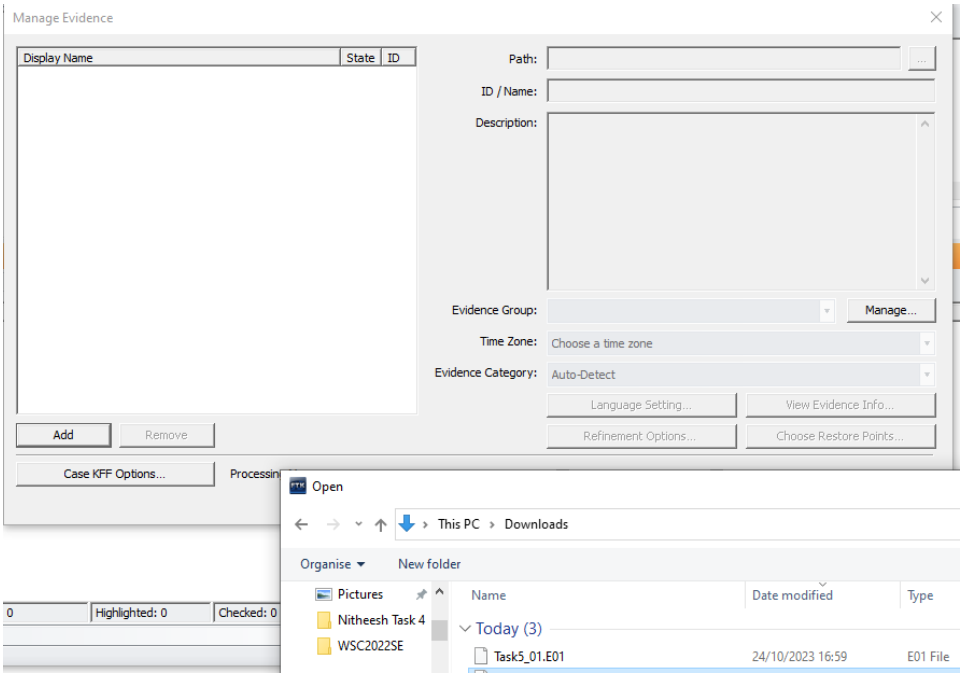
e. Mount task4_06.E01 image from the download link and enumerate the autorun locations.
    1. Identify any malware (including virus, trojans, etc)
    2. Check for autorun entries, that could eventually slow down the boot process and affect overall system performance. Identify and disable unnecessary 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.

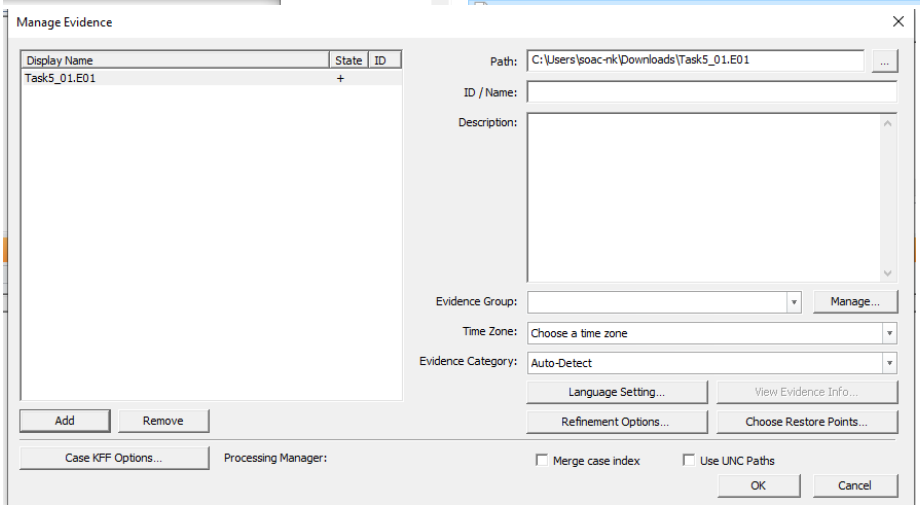
3. Working on Forensic Images
    a. Open Forensic Toolkit. Login using Cisco and Cisco. Go to File→ New User
    b. Login using your credentials.
    c. Create a New Case. Refer to the screenshot below. Open a Case.

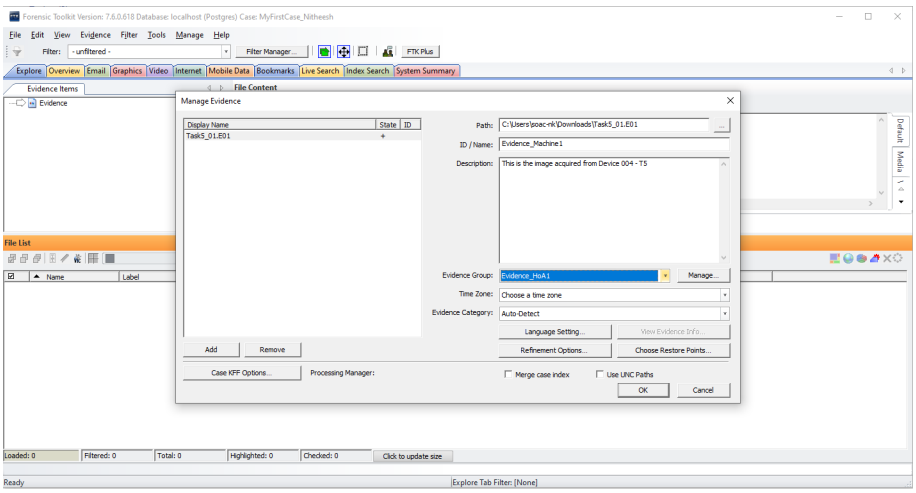

Forensic Toolkit Version: 7.6.0.618 Database: localhost (Postgres)
File Database Case Tools Manage Help
Cases
Name
Date Modified
Temp
13/10/2023 11:47:43 +0000
Case ID
1
New Case Options
Owner:
nitheesh
Case Name:
MyFirstCase_Nitheesh
Reference:
Case_ACCA7031
Description:
This is an example of handing a case - for HoA2
Description File:
Case Folder Directory:
C:\Users\poac-nk\Documents
Processing profile
Forensic Processing
eDiscovery Processing
Summation Processing
Basic Assessment
Field Mode
Image Processing
Video Processing
All Communication
Customize...
Profile:
Forensic Processing
Open the case
OK
Cancel

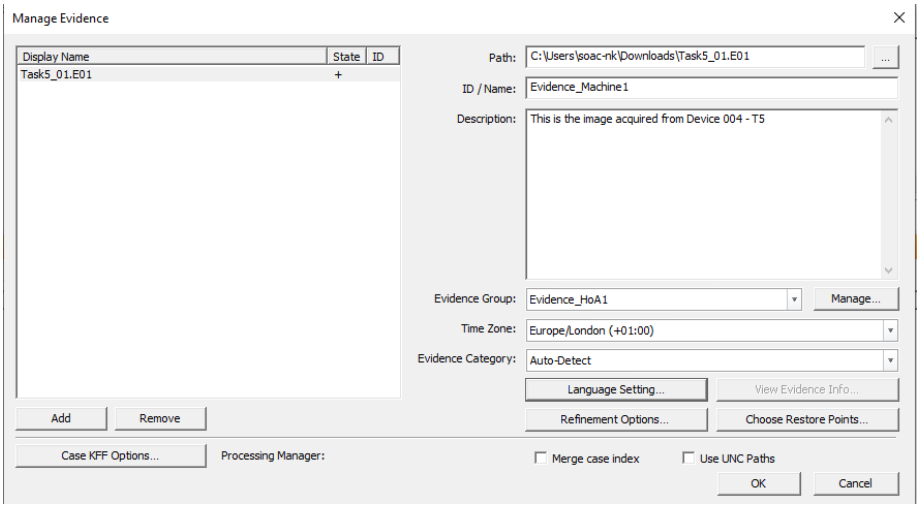

Forensic Toolkit Version: 7.6.0.618 Database: localhost (Postgres) Case: MyFirstCase_Nitheesh
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
FTK Plus
Explore Overview Email Graphics Video Internet Mobile Data Bookmarks Live Search Index Search System Summary
Evidence Items
Evidence
File Content
Manage Evidence
Display Name
State
ID
Path:
ID / Name:
Description:
Evidence Group:
Manage...
Time Zone:
Choose a time zone
Evidence Category:
Auto-Detect
Language Setting...
View Evidence Info...
Refinement Options...
Choose Restore Points...
Add
Remove
Case KFF Options...
Processing Manager:
Merge case index
Use UNC Paths
OK
Cancel
File List
Name
Label
Loaded: 0
Filtered: 0
Total: 0
Highlighted: 0
Checked: 0
Click to update size
Ready
Explore Tab Filter: [None]

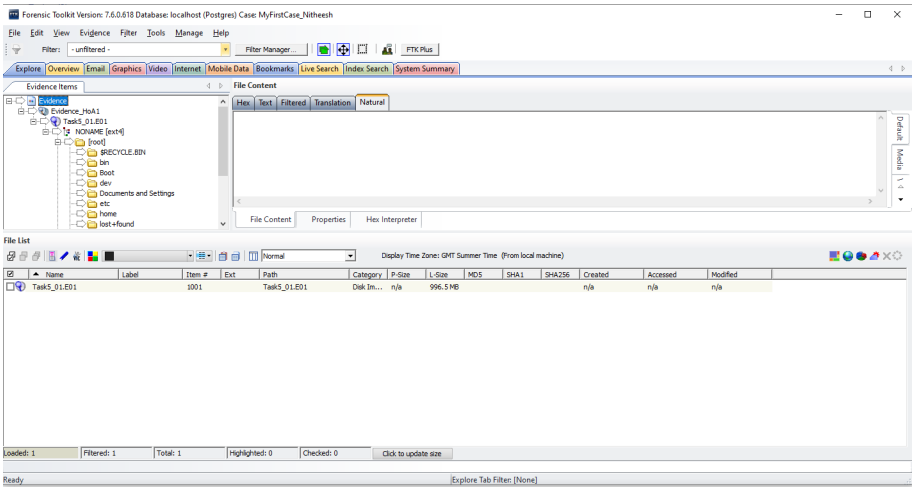

File Content
Manage Evidence
Select Evidence Type:
Acquired Image(s)
All Images in Directory
Contents of a Directory
Individual File(s)
Physical Drive
Logical Drive
OK
Cancel
State
ID
Path:
ID / Name:
Description:
Evidence Group:
Manage...
Time Zone:
Choose a time zone
Evidence Category:
Auto-Detect
Language Setting...
View Evidence Info...
Refinement Options...
Choose Restore Points...
Add
Remove
Case KFF Options...
Processing Manager:
Merge case index
Use UNC Paths
OK
Cancel

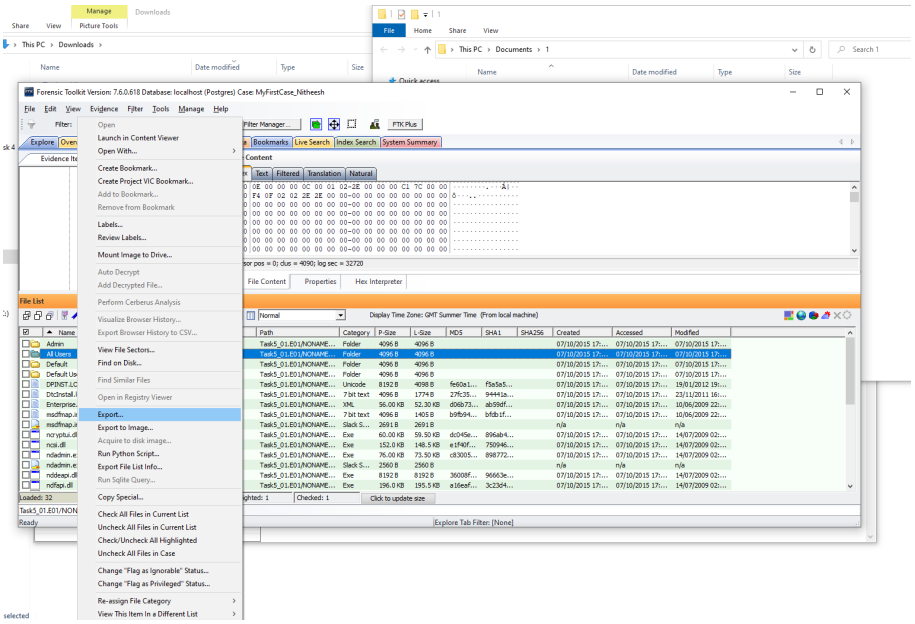

Manage Evidence
Display Name
State
ID
Path:
ID / Name:
Description:
Evidence Group:
Manage...
Time Zone:
Choose a time zone
Evidence Category:
Auto-Detect
Language Setting...
View Evidence Info...
Refinement Options...
Choose Restore Points...
Add
Remove
Case KFF Options...
Processing
Highlighted: 0
Checked: 0
Open
This PC › Downloads
Organise
New folder
Pictures
Nitheesh Task 4
WSC2022SE
Name
Date modified
Type
Today (3)
Task5_01.E01
24/10/2023 16:59
E01 File

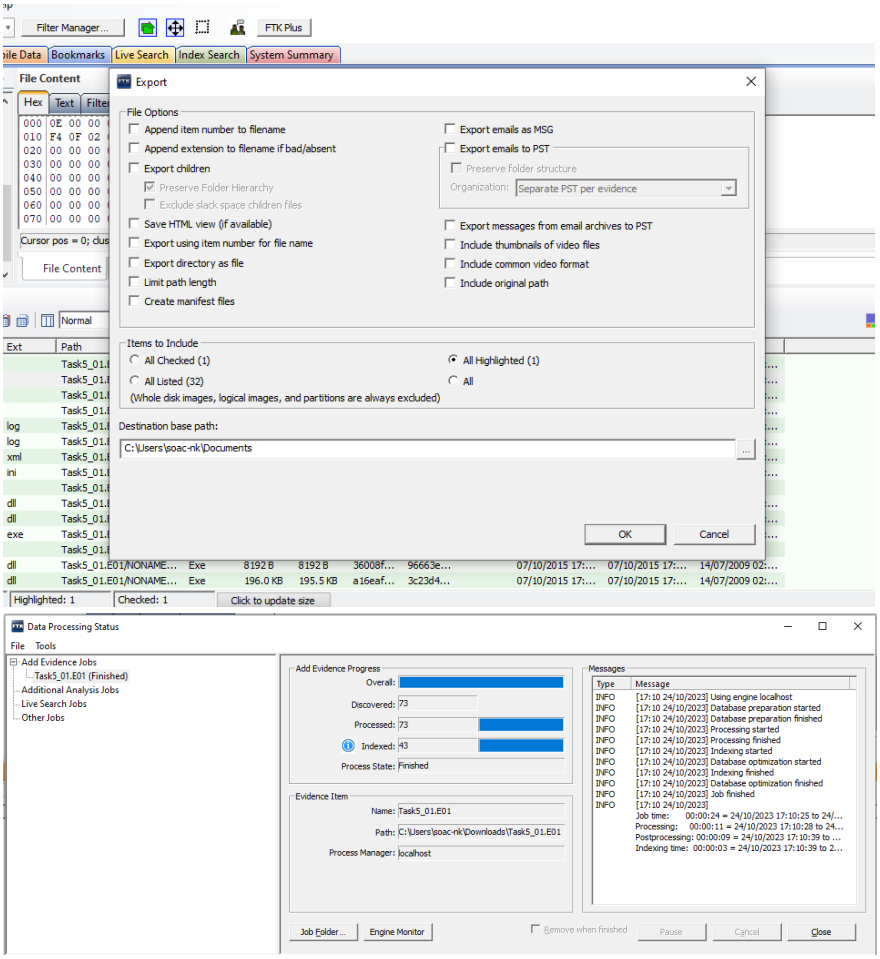

Manage Evidence
Display Name
State
ID
Task5_01.E01
Path:
C:\Users\soac-nk\Downloads\Task5_01.E01
ID / Name:
Description:
Evidence Group:
Manage...
Time Zone:
Choose a time zone
Evidence Category:
Auto-Detect
Language Setting...
View Evidence Info...
Refinement Options...
Choose Restore Points...
Add
Remove
Case KFF Options...
Processing Manager:
Merge case index
Use UNC Paths
OK
Cancel

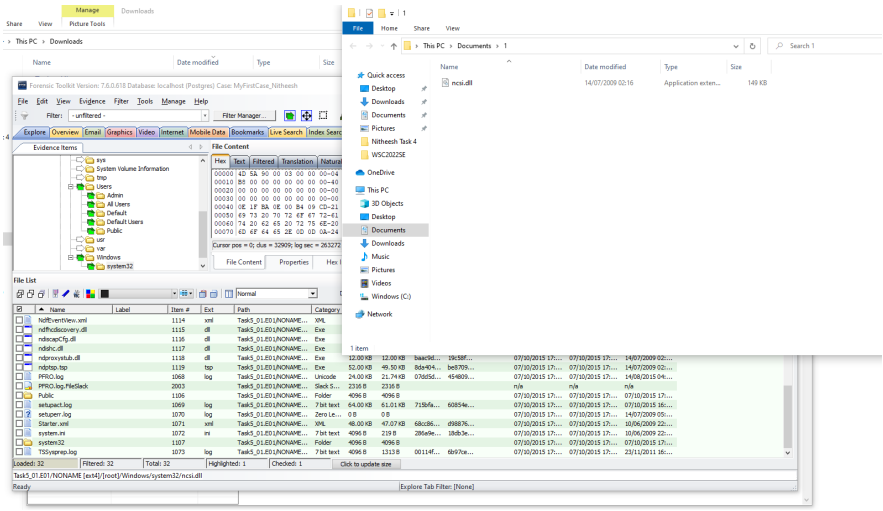

Manage Evidence
Display Name
State
ID
Task5_01.E01
Path:
C:\Users\soac-nk\Downloads\Task5_01.E01
ID / Name:
Evidence_Machine1
Description:
This is the image acquired from Device 004 - T5
Evidence Group:
Evidence_HoA1
Manage...
Time Zone:
Choose a time zone
Evidence Category:
Auto-Detect
Language Setting...
View Evidence Info...
Refinement Options...
Choose Restore Points...
Add
Remove
Case KFF Options...
Processing Manager:
Merge case index
Use UNC Paths
OK
Cancel


Manage Evidence
Display Name
State
ID
Task5_01.E01
Path:
C:\Users\soac-nk\Downloads\Task5_01.E01
ID / Name:
Evidence_Machine1
Description:
This is the image acquired from Device 004 - T5
Evidence Group:
Evidence_HoA1
Manage...
Time Zone:
Europe/London (+01:00)
Evidence Category:
Auto-Detect
Language Setting...
View Evidence Info...
Add
Remove
Refinement Options...
Choose Restore Points...
Case KFF Options...
Processing Manager:
Merge case index
Use UNC Paths
OK
Cancel









d. Analyse the Image file and try to recover evidences.
e. Download task05_02.E01and create new case. Analyse the evidence.
f. Use other tools to analyse the evidence (task05_01.E01 and task05_02.E01) to find/ gather furhter more information.
g. Document the steps with screenshots, pros and cons of each tools and additional evidences gathered. (You shall try Autopsy, EnCase etc)
h. 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?

Deliverables

1. Contribution to Discussion Forums (2.1, 2.2, 2.3, 2.4, 3a)
2. Report with Analysis (3f)
3. Documentation –File System Analysis – Using other tools (2.4 vii, 2.4 viii, 3g,3h)
4. Submit your RAW and E01 Files in "**September 2023 Student SharedFolder**". By submitting the image files, you are approving other students/ lecturers to access your image file for laboratory use. If you download other's images from the drive, you are authorised to use them with in the lab environment and not outside the lab.

Overall Reflection

Present your reflection to the class. (Note that you will have 10 minutes for presentation during the next lecture session. – Before the presentation, you must submit the documentation in Moodle)

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

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