



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

Applied Computing

Wales Institute of Science and Art (WISA)

Computer Forensics (ACCD5000)

Investigation



[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 2, you must have a lab setup working.	☒
So far:	
HoA1: Understand Digital Evidences - Importance of Computer Forensics – Basic Investigation	☒
HoA2: Understand the importance of ensuring DATA Integrity – Computer Forensics Virtual Lab Setup	☒
HoA3: understand Investigation Process, Ensure integrity of the evidence by calculating, comparing Hash Values	☒
Make sure the above activities are completed before starting this week's activity	
Task 1: Data Recovery	
Task 2: Hashing	
Task 3: Working with various Files	
Task 4: Handling evidence data	
Task 5: Creating Disk Image	

ICONS Used in this document:

Find out the outcome/ Answers/ Solution and record your reflection



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.

Scenario

From our previous Hands on Activity, where you had experienced the pre-investigation process by being in the crime scene, forming your investigation team, identifying evidences (*though few teams couldn't identify all the evidences 😊*) and transporting the evidences safely and securely, now during today's hands-on activity, you will further proceed in imaging the gathered digital evidence.

Task 1: Data Recovery

Insights:

A hard disk is a non-volatile data storage device used to store data or install programs on your computer.

Always, make sure to adapt Industry best practices in selecting the tools, using them, and completing the tasks. It is recommended to refer to the tool's documentation before using the tool.

Also, organise the gathered evidences in an appropriate folder, name them appropriately etc are appreciated.

Make sure, you submit concrete justification in the process you have adapted to complete the tasks. Not necessarily, you are expected to follow the instructions or same process listed below. However, keep in mind that you are free to work with only the sample data provided in an isolated lab environment (eg: your Computer Forensics Virtual Lab setup) and not outside this environment or in a real world environment or not with any real time data without proper consent/ permission.

Pre-work:

1. Login to your Windows Client Machine (in your Virtual Isolated lab environment) and create a folder with the name "HandsonActivity4" and create 5 txt files, 5 word files and browse internet to get few images downloaded to the folder.
2. In one of the text files or word file, create a flag for "If you wish to give a tag line for you, what is your tag line?". (A flag here refers to any text or numbers for the given question) For example, my tag line is – "Don't take my kindness for

weakness” or it could be something (irrelevant as well) like Jamesbond 007, 76898659 etc.

3. In other txt files and word document, create junk data.
4. Compute hashes of files and text string – Refer to Hands-on Activity 3.
5. Attach the text file you created with a flag and its hash values in moodle – Tutorial 4 Prework Submission.
 - a. You could calculate hash values using any (one or multiple) algorithms (MD5, SHA512, HMAC, CRC32 etc). Use MD5 as well.
 - b. Justify your reason to calculate the hash values using one specific or multiple algorithms other than MD5 in moodle – group discussion forum.

Research

6. Do basic search to find out the best data recovery tool available in the market. Discuss with your friends in the class to find more information about any other tools.

Shuffle & Challenge

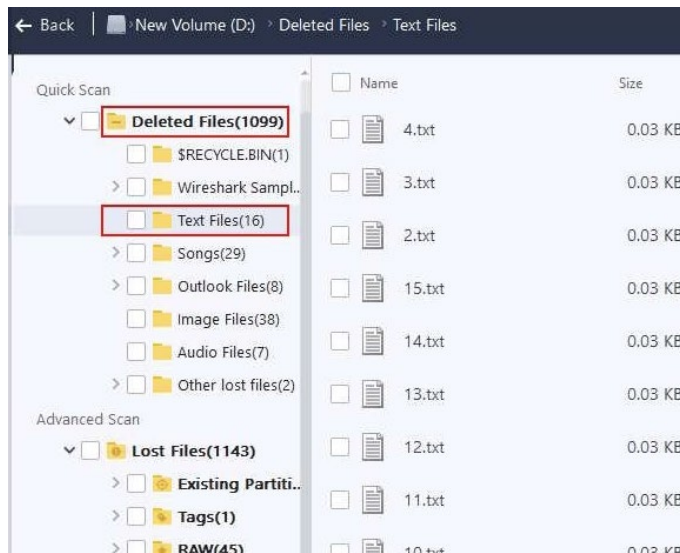
7. Delete the files (maybe not all the files – but definitely the one with the flag and few others) (Shift Delete – and confirm in recycle bin as well)
8. Ask one of your classmate, to sit in your PC (Isolated Lab environment) and challenge to recover the deleted files and find out the flag.
9. You accept the challenge from one of your other classmate as well and complete the task.

Recover and capture the flag!!!

10. For this activity, this lab works on EaseUS Data Recovery Tool. You might use any other tools you have found from Q.5.
11. If you still prefer to use EaseUS Data Recovery Tool, download it from internet or from the resource link shared with you.
12. Setup your tool.



13. During installation, it might have asked you to participate in the Customer Experience Improvement Program. Did you opt in? Yes/No. Justify.
14. The EaseUS data recovery wizard displays the Hard Disk Drives under the Devices and Drivers section. Hover the mouse cursor over the drive/location you want to scan so that the Scan button appears below the location.
15. The application runs two types of scans: Quick Scan and Advanced Scan. Upon completion of the scan, it displays the scan results under three folders: Deleted Files, Lost Files, and Existing Files.
16. The deleted files are contained within the Deleted Files directory under the Quick Scan section. You can choose either to preview these files or recover them depending on your requirement.
17. In this lab, we will be attempting to recover the deleted files from your classmates Isolated Lab environment.
18. To do that,
 - a. expand Deleted Files.
 - b. A list of files associated with this folder appears in the right pane, right-click on the files listed and select Preview.



c. The preview of the selected text file will appear



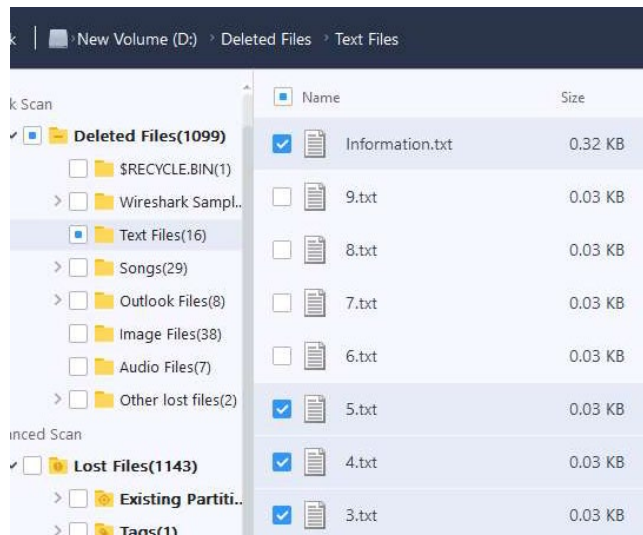
d. If you wish to recover this text file, click on Recover. Remember, you are looking for a flag to capture.

e. A Browse for Folder window appears where you need to choose the location for saving of the file.

19. On completing the recovery, a Recover Complete window will appear and the application automatically directs you to the Recovered Files folder. Close the Recover Complete window and the Preview window.

20. EaseUS auto-creates a sub-folder named Preview inside yet another auto-created sub-folder named Easeus [DD HH_MM] under the Recovered Files folder, where DD denotes the date, HH denotes the hours, and MM denotes the minutes.

21. You can also manually view this recovered file by navigating to the location Documents\Recovered Files\Easeus [DD HH_MM] \Preview (or C:\Users\Admin\Documents\Recovered Files\Easeus [DD HH_MM] \Preview).
22. To recover multiple files, select the files you want to recover, then click Recover.



23. On clicking Recover, the Browse for Folder window appears where you need to choose the location for saving of the file, like the previous case where a single file was recovered. You may either choose the Recovered Files folder created earlier to save the files or choose another location.
24. Following the same method as in the previous case, from the Browse for Folder window, expand Documents, select Recovered Files folder, and click OK. The file being recovered then gets saved to this Recovered Files folder.
25. On completing the recovery, a Recover Complete window appears as previously seen, and the application automatically directs you to the location where the recovered files are saved.
26. Close the Recover Complete window.
27. EaseUS auto-creates a series of sub-folders inside Recovered Files folder in this order: Easeus [DD HH_MM] --> New Volume(D) --> Deleted Files, where DD denotes the date, HH denotes the hours, and MM denotes the minutes.
28. To view the recovered files, open Deleted Files --> Text Files. The recovered files appear in this location.

29. In the same way, you may recover single or multiple folders, sub-folders, or even the entire Deleted Files folder.
30. If the space required for saving the files/folders is insufficient, then consider saving the data to another location such as an external hard disk with adequate space and create a backup. The recovered data may also be saved to cloud.

Task 2: Hashing

Insights:

Hashing is performed on data such as files or text to generate unique fixed-length string called hashes or checksum. The generated hashes are helpful in determining whether the given data has maintained integrity.

1. Calculate the hash values of the recovered file and test it with any database for malicious behaviour. (*Refer to Handson Activity 3*)
2. Share your hash value with your classmate who challenged you to capture the flag. – You will also get the hash value of your file from your classmate you challenged to capture your flag.
3. Compare your hash value with your classmates hash value
4. Discuss the outcomes and record your reflection
 - a. Is the hash value matching?
 - b. If yes, what is the outcome – If no, what is the outcome?
 - c. If the file integrity is under question, what will be the further actions?

Task 3: Working with various Files

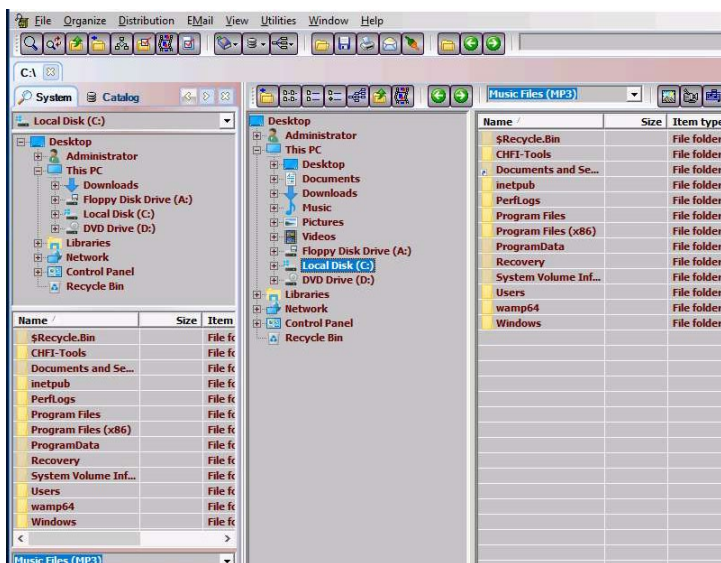
Insights:

There are various chances that a criminal could hide the file format to confuse/ hide the evidence related to crime. The investigators in general use File Viewer to recognize the format and extract its contents that led to an incident.

To be a computer forensic expert, you must have sound knowledge of various file viewing tools used for forensic investigations. This knowledge includes how to locate files quickly, view files of different formats, etc.

A file format is a layout of a file that tells a program how to display its contents. Some of the common file formats are .doc, .gif, .jpg, .png, .mp3, .pdf, .txt, etc.

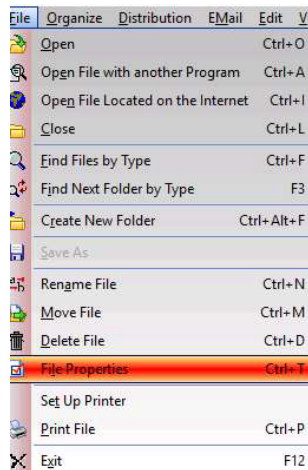
1. Do a basic search on tools that are available to view the file formats. Use any of the identified tools. Have an open discussion with your classmates. Note: These searches could be used in your Coursework.
2. Use your Windows Server Machine.
3. For this demonstration, this lab uses FileViewer. You are free to use any tools.
4. Download and install the tool.
5. Open the tool



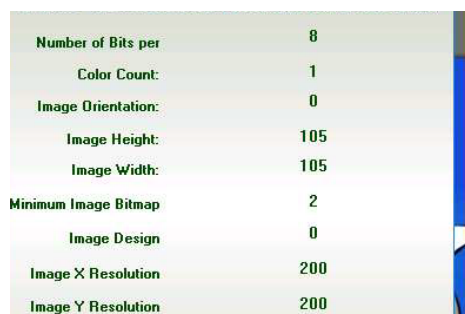
6. Go to File menu and click Open.
7. In the Open dialog box, locate the evidence file path. For this lab, we use Image files in Evidence Folder (Refer to our Resources in \\192.168.135.50\FTKToolsShare\$)
8. Select All files (.) in the File type drop-down list.
9. Select the file Friends2.jpg and then click Open
10. If a Getting Started with File Viewer dialog box appears, click Cancel.
11. The image Friends2.jpg opens in the file viewer screen, as shown:



12. Navigate to File --> File Properties to view various properties of the selected image.



13. The File Properties window will pop up showing various properties of the selected file. Click OK to close the window.



14. Now, we shall open an mp4 (520px-Biohazard_symbol_(blue).mp4) file in the application.

15. Go to File menu and click Open and select the file 520px-Biohazard_symbol_(blue).mp4 and then click Open

16. What happened?

- a. Did the file open? (yes/ no) Clarify, discuss the possibilities of the outcome.
- b. If a File Viewer pop-up appears stating LTMM Error, click OK to close the pop-up. File Viewer will try to run the mp4 file, but will fail to do so

Note: This happens when a file is either corrupt or its file extension is forcefully changed, resulting in a blank screen. Such files need to be further investigated.

Note: Before investigating, you need to identify such files that are suspicious.

Task 4: Handling Evidence Data

Insights:

Forensic evidence is obtained via bit-by-bit copying of original media such as hard drive, USB drive, etc., found at the crime scene. It contains information such as files/folders, deleted data, etc., that can serve as a potential source of evidence during investigation.

1. Do a basic search to find out tools that could be used for
 - a. data acquisition, data analysis, artifact examination and reporting.
 - b. Use the tutorial sessions to download, install and use various tools that are available.
 - c. Discuss with your classmates about the pros and cons of various tools.
 - d. Use your knowledge and understanding to support your coursework.
2. Use your Windows Server Environment.
3. For this task, this lab uses Paraben's E3. You are free to use other tools.
4. While looking at Paraben's E3, there are various products like E3 Universal, Mobile, Computer, Etc. Download the appropriate latest version of Paraben's E3 product and use it for examination based on the above scenario.
5. Make sure you sign up for trial version edition of E3 platform on <https://paraben.com/dfir-tools-trial/>, download the tool and communicate with the Paraben team in order to obtain license for activation. (if required)

6. Double-click on the Paraben installer to launch the setup and follow the wizard-driven installation steps to install the application.
7. At the end of the installation process, click Finish to exit the installation wizard.
8. If a Paraben's Driver Pack download webpage opens in the default browser, close it.
9. Double-click on the Electronic Evidence Examiner icon located on the desktop to launch the application. Alternatively, you can launch the application from the Apps screen.

If the tool has been activated earlier, then you can skip directly to the step where we create a new case in the next task and get started with the lab exercise.

10. Upon launching the tool, the main window of Paraben's E3 opens up along with a Paraben's E3 pop-up. Close the pop-up. If the activation window opens up, click Cancel. If the tool opens up Paraben's webpage in the default browser, close it. If Paraben's tutorial pop-up appears along with the main window of E3 on launching the application, close the tutorial menu pop-up.
11. Activation of the application as a trial version is highly recommended as the trial version offers full functionality of all the features of this tool, on par with its full, paid version. The free version of the tool offers only limited features and may not be suitable to run the lab. To activate the trial version, go to Case in the menu bar and from the drop-down, click on Activation. Then click the option Activate.
12. Paraben's Electronic Evidence Examiner Activation window appears listing the options for activation. Ensure that the option Internet License is selected and click on Activate button.
13. A Registration dialog box appears asking you to restart the application to finish the activation. Click OK. Close the application and restart it.
14. The Paraben's E3 trial version is valid only for 7 days.
15. Next, Connect to Web License Server window opens up and asks for user credentials to connect to the web license server. Here, you must enter the Login ID (or email ID) and Password that has been used to sign up/register for the Paraben's E3 trial setup in order to access the trial version of the tool. Upon entering the credentials, click the Connect button.

16. The main window of the application opens up along with the Paraben's E3 pop-up that we saw upon launching the application for the very first time after completing its installation. Close the pop-up.
17. Go to Case on the menu bar and click Help to check whether the tool has been activated. In the right window pane, you can find information pertaining to Paraben's E3 registration along with Registration key.
18. When the trial version of the application has been activated, you will also find that its name at the top of the window is Paraben's E3: Universal instead of Paraben's E3: Free, which will be seen only when using the free version of the tool.
19. Next, we will examine a forensically acquired digital evidence using the Paraben's E3 forensic platform. In order to examine a new evidence, go to Case on the menu bar and click Create New Case.
20. A New Case window appears which displays the Welcome section. Click Next button.
21. In the Case Properties section, provide a Case name and case Description in the respective fields. You may enter these details according to your requirement. Click Next.
22. In the Additional Information section, enter additional information related to the investigator (you may also enter your details in this section) and click the Finish button. Additional information is not mandatory and can be filled any time through the Properties pane.
23. In the New case creation window that appears next, navigate to the Desktop and create a folder named Reports. Then, go into the Reports folder by ensuring that it is selected and clicking Open. Specify a file name for the case in the File Name field and then click Save.
24. In the Add New Evidence window that appears next, select Image File under the Category section in the left pane, then select Auto-detect image under the Source type section in the right pane and click OK.
25. An Open window will appear; navigate to Evidence Files in our resource folder, look for Forensic Images and select Windows_Evidence_001.dd
26. A pop-up appears where we can specify a new name for the evidence that we added. We will retain the default name (Windows_Evidence_001) for our evidence file. Click OK.

27. An NTFS Settings window pops up. Check all the options specific to deleted data recovery and click OK.
28. If the image file uses a FAT file system, then the below window will not pop up.
29. The selected image file is added to the case (Case 1 file under the Case Content tab in the left pane of the application window).
30. Expand Case 1 --> Windows_Evidence_001 --> NTFS --> Root. You will find the data pertaining to the evidence file.
31. During forensic investigation, retrieving deleted data from the evidence image file is crucial. The information pertaining to the deleted data can be retrieved from the Trash folder. Click on the Trash folder to find deleted data.
32. To view the properties of a deleted file, select it. Its properties will then be displayed under the Properties tab in the right pane of the window.
33. To view the actual image contained in the selected file (since the selected file is of image file format), click the File View tab. The image will be displayed in the right pane of the window.
34. Apart from viewing the actual image contained in a selected file, Paraben's E3 also lets you view its Hex values.
Hex values help determine the raw and exact contents of a file even if it has been deleted or overwritten.
Hex values thus help you identify and retrieve information of forensic value that normally cannot be accessed by the operating system.
35. To view the hex values of the selected file, click the Hex View tab. The Hex values will be displayed in the right pane of the window.
36. To view the text values of a text file document, select the text file (here, we have selected the text file New Text Document.txt) and then click the Text View tab:
37. To generate an investigative report, first select the desired files that must be included in the report. Then click on Reports on the menu bar, and then click Generate Report:
38. In the Reports Wizard window that appears next, we need to select the report type to be generated and also specify a Destination folder. In this lab, we will be selecting the HTML Investigative Report type option and the default destination folder location shown by the application. Ensure to check the options Include Parsed Embedded Data and Open report on finish. Click Next.

39. If you want the report to be opened automatically at the end of the lab without having to manually open it by navigating to the location where it has been saved, then do ensure to check the option Open report on finish.
40. Add any additional investigator information, if needed, in the Investigator's Information section that appears next, and then click the Next button.
41. In the Filesystem Types section that appears next, select the file types that you want included in the report and click Next button.
42. In the File properties section that appears next, select those details under properties that you want included in the report, then click Next.
43. In the Other evidence section that appears next, select the options according to your requirement (you may also leave these options set to default). Click Next.
44. In the Sorted files section that appears next, select the Include only data checked as "Include to reports" radio button and then click Next.
45. In the Custom Report View section that appears next, you can customize the report view by adding your custom logo, custom header, and custom footer. Click Next after customizing the report view.
46. Customizing the report view is not mandatory and can be skipped by clicking Next.
47. In the Summary and Conclusion section that appears next, you can add the summary and conclusion pertaining to the evidence examination in the Examination Summary and Examination Conclusion sections respectively.
48. Click on the Edit Section buttons below the Examination Summary and Examination Conclusion sub-sections respectively. An Editing Section window (which looks similar to a word document) for each of those sub-sections will open. In the Editing Section windows for each of those sub-sections, you can respectively write a brief summary on the evidence file examined and a conclusion describing the actions performed on it and the result generated. After adding the summary and conclusion, click Next.
49. The Summary and Conclusion section is not mandatory to edit and can be skipped by clicking Next.
50. In the Logs and Supplementary files section, check the Include Case History option and click Finish.

51. A Task Status Notification window appears indicating that report generation is finished and that the generated report has been saved to the default destination. Click OK or close the window.
52. You can also manually navigate to the folder where you have saved the report file and open it from there. In this folder, you will find a sub-folder named Case 1. Open that sub-folder and double-click the Case 1.html file to open and view the report.
53. A detailed Investigative Report will open in the web browser; scroll down the browser window to examine the report in detail.
54. In this manner, you can use Paraben's E3 utility to handle evidence data.
55. Submit the report in Moodle – Handson Activity 4 Submission.

Task 6: Creating a Disk Image of a Hard Disk

Insights:

As investigators should always create duplicates of the hard disk and perform the forensics process on the copy. To be a computer forensics expert, you must have sound knowledge of the various disk imaging tools used for forensics investigation.

A disk image is a bit-by-bit copy of a hard disk or a disk partition, which includes all the files/folders, deleted files, files left in the slack space and unallocated space, file system information, etc.

1. Use Windows Client for this activity.
2. Do a basic search to find out tools that could be used for
 - a. Creating an Image.
 - b. Discuss with your classmates about the pros and cons of various tools.
 - c. Use your knowledge and understanding to support your coursework.
3. For this lab, R-drive Image tool is used. You are free to use any other imaging tools. Download R-Drive Image tool and follow the wizard-driven installation steps to install the application.
4. On completing the installation, ensure that Launch R-Drive Image option is checked and click Finish.
5. In the Action Selection window, Create an Image option is selected by default. Click Next to continue.

6. In this lab, we will be creating an image for D:. (Only do this, if you have partitioned your Windows Client Lab environment with multiple drives – and the drive D is less than or equal to 500 mb) If not, use an external hdd/ flash drive with less space to do this activity.
7. Further demonstrations assumes your D drive with 500 mb partition.
8. Select D drive to create a drive image file of the drive. Click Next.
9. In the Image Destination panel:
 - a. Expand This PC and select the Forensic Disk (F drive) to save the file in this drive
 - b. The filename will be automatically taken by the application
 - c. Select R-Drive Image files (*.rdr) in the Files of type field and click Next
 - d. In the Image Options panel, click Next. Providing a password is optional.
 - e. In the Backup Options panel, click Next.
 - f. The Processing panel displays the summary of all the processes. Click Start to start the disk partition imaging process.
 - g. The Progress bar in the Processing panel will show the percentage of task completed. Once the processing is done, a pop-up will appear displaying Image created successfully. Click OK.
 - h. In the R-Drive Image window that reads Action Selection at the top, click the Exit button to close the application.
 - i. Now, navigate to the Forensic Disk (May be F Drive – it is the source of the image created) to view the created disk partition image file.
 - j. The size of the image file depends on the space filled in the drive. If your drive is empty, the size of the generated image file is relatively less.
10. **Try to create your images (not pictures, a bit-bit copy of any evidence) and upload them in our Shared folder by creating a folder with your name. Make sure the image doesn't contain any confidential / personal/ sensitive information. Those images may be reused for other class activities.**



Overall Reflection

Record your reflection via Moodle – Group Discussion.

1. Understanding of the concepts discussed in the lecture and its relation to the activity done.
2. Understanding Investigation Process (Acquiring, Analysing Data and reporting).
3. Understanding and implementing an investigation ensuring data integrity.
4. Rate yourself (1 very low – 5 exceptional): Understanding the Investigation Process.

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