



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)

Data Acquisition



[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 analysis 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	✓
HoA4: Understand Investigation Process – Copying Evidences and ensuring integrity	✓
HoA5: Understand File Systems – Linux, Windows Images and Deleted Files	✓
Make sure the above activities are completed before starting this week's activity	
Task 1: Creating a dd Image	
Task 2: E01 to DD Format	
Task 3: Mount the Image	
Task 4: Acquiring RAM from Windows and Linux	
Task 5: Creating Customized Images from an Image Containing NTFS File System	
Task 6: Viewing Contents of Forensic Image File	
Task 7: Coursework Milestone (Important) – Acquire your Image Copy	

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.

Task 1: Creating a DD Image

1. Use Windows Client Machine.

Note: Physical acquisition of the suspect disk/drive usually requires an external data storage medium, such as a hard disk or a pen drive, to collect the image generated during physical acquisition process.

1.1. You are free to use your own flash drive/ pen drive or Hard Disk – Consider the size!!!

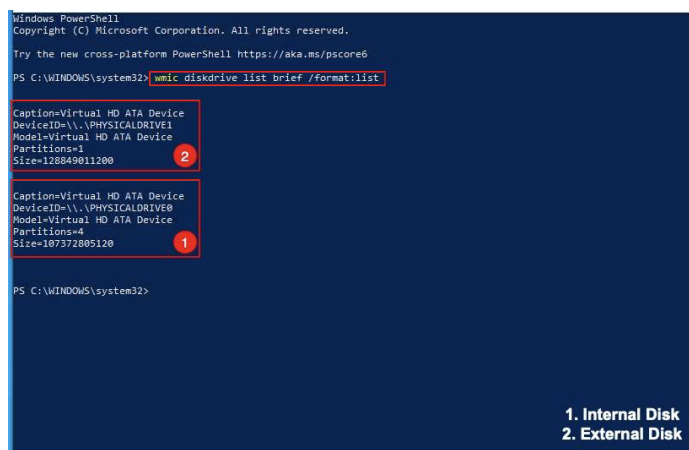
1.2. If not, For this lab, we will be performing physical acquisition of the primary disk/internal disk (PHYSICALDRIVE0) of the Windows 10 virtual machine using dd command.

1.3. Acquisition usually requires an external data storage device for storing the image. However, since this is a lab environment, we are using a secondary physical disk (PHYSICALDRIVE1, created during the lab setup – if you haven't created a secondary physical disk, try to create one now) assuming it as an external storage device to store the image. Therefore, we will be treating this disk as an external disk for this lab.

2. To obtain information about the available drives on Microsoft Windows, we will issue the wmic command in Windows PowerShell.

3. To launch PowerShell as an administrator, right-click on the Windows icon and select Windows PowerShell (Admin).

4. Type the command wmic diskdrive list brief /format:list and press Enter.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> wmic diskdrive list brief /format:list

Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE1
Model=Virtual HD ATA Device
Partitions=1
Size=128849011200 2

Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE0
Model=Virtual HD ATA Device
Partitions=4
Size=107372805120 1

PS C:\WINDOWS\system32>
```

1. Internal Disk
2. External Disk

4.1.

```
PS C:\WINDOWS\system32> wmic diskdrive list brief /format:list

Caption=NVMe KXG80ZNV1T02 NVMe KIOXIA 1024GB
DeviceID=\\.\PHYSICALDRIVE0
Model=NVMe KXG80ZNV1T02 NVMe KIOXIA 1024GB
Partitions=5
Size=1024203640320
```

4.2.

Note: You may be getting an output of either one of the images above. 1st one is with 2 disk, where you use one as external and the other as internal. 2nd one is with 1 disk. Either consider re-creating secondary physical drive or use pen drive or HDD

5. From this point, you need to make necessary amendments to your work based on the available disk drives. The instructions are given for 4.1.

5.1. Copy DD Folder from our resources to the Desktop

5.2. Now, use cd command to navigate to the directory C:\Users\Admin\Desktop\dd

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> wmic diskdrive list brief /format:list

Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE1
Model=Virtual HD ATA Device
Partitions=1
Size=128849011200

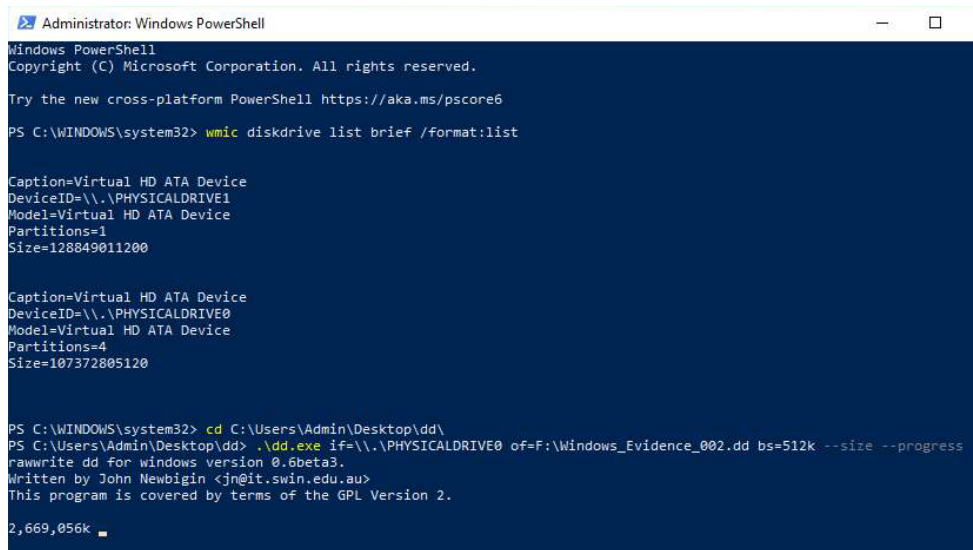
Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE0
Model=Virtual HD ATA Device
Partitions=4
Size=107372805120

PS C:\WINDOWS\system32> cd C:\Users\Admin\Desktop\dd\
PS C:\Users\Admin\Desktop\dd>
```

5.3. Next, type the command `.\dd.exe if=\\.\PHYSICALDRIVE0 of=F:\Windows_Evidence_002.dd bs=512k --size --progress` and press Enter.

5.4. This begins to create a physical image of the drive PHYSICALDRIVE0 in the Forensic Disk (F:\ in this lab) as shown in the following screenshot: The drive letter of the forensic disk may vary in your lab environment.

You need to enter the letter that is associated with the forensic disk.



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> wmic diskdrive list brief /format:list

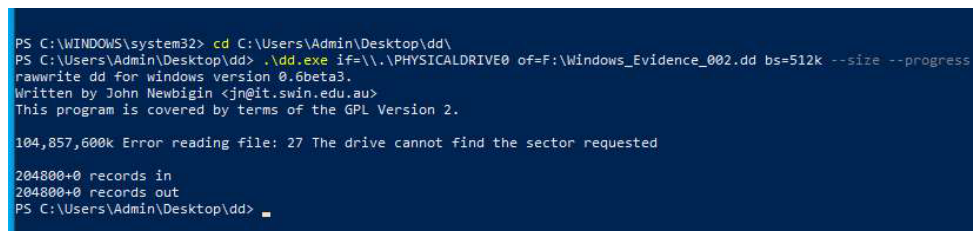
Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE1
Model=Virtual HD ATA Device
Partitions=1
Size=128849011200

Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE0
Model=Virtual HD ATA Device
Partitions=4
Size=107372805120

PS C:\WINDOWS\system32> cd C:\Users\Admin\Desktop\dd\
PS C:\Users\Admin\Desktop\dd> .\dd.exe if=\\.\PHYSICALDRIVE0 of=F:\Windows_Evidence_002.dd bs=512k --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.

2,669,056k
  
```

5.5. It takes some time for the tool to create the image. Upon successfully creating the image, it displays the number of records in and the number of records out, as shown in the following screenshot:



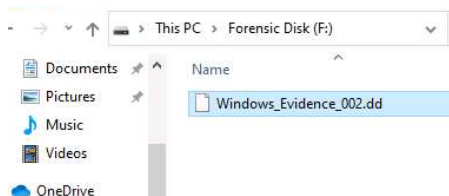
```

PS C:\WINDOWS\system32> cd C:\Users\Admin\Desktop\dd\
PS C:\Users\Admin\Desktop\dd> .\dd.exe if=\\.\PHYSICALDRIVE0 of=F:\Windows_Evidence_002.dd bs=512k --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.

104,857,600k Error reading file: 27 The drive cannot find the sector requested

204800+0 records in
204800+0 records out
PS C:\Users\Admin\Desktop\dd>
  
```

5.6. Navigate to the Forensic Disk (F:) drive in this lab) to see the captured dd image file, as seen in the screenshot below:



This image becomes the main source of examination for investigators in real-time. Depending on the type of forensic workstation and the investigator's requirements, these images are either examined directly through forensic tools or further converted into other forensic tool formats and bootable images.

Delete this image file, in case you are running short of space for the upcoming labs. This way, you can create a dd image of system drive during investigation process.

Task 2: Converting Image File from E01 Format to dd Format

Note: You are asked to examine an E01 format forensic image file on a Linux workstation. But forensic examination of E01 image file works perfectly only when the forensics workstation is Windows-based, not Linux-based. To examine E01 file format image file on a Linux workstation, you need to convert the E01 image file to dd file format.

Note 2: E01 and dd are forensic image file formats to store bit-by-bit copy of storage devices such as hard disks, USB drives, etc.

1. Use Ubuntu Machine for this lab.
2. Click on the Files icon in the Launcher panel to launch the File Manager.
3. Go to Evidence Files --> Forensic Images. You will be able to view the Windows_Evidence_001.E01 file in the images.
4. In this lab, we are going to convert an image file with E01 file format to dd file format. To do this, we need to install xmount tool. You are free to use any available/ preferable tools – based on your research task for your coursework.
5. Click on the Terminal icon from the launcher panel to launch the command line terminal.
6. Command line terminal launches. You require root privileges in the terminal to install an application.
7. So, type `sudo su` and press Enter. You will be prompted to enter the password.
8. Now, you will enter the root terminal as shown in the following screenshot:
9. To install xmount, type the command `apt-get install -y xmount` and press Enter.
Note: If you face any issues with the internet connectivity, run the commands `ifdown -a` followed by `ifup -a`; and then run the command `apt-get install -y xmount`.
10. The `apt-get install -y xmount` command will not execute in case another process is using the apt command.
11. In this scenario, restart the Ubuntu Forensics virtual machine and then run the command for xmount so that it executes successfully.
12. It is not possible to mount the evidence file from the shared directory; therefore, copy the Windows_Evidence_001.E01 file from the shared directory into the Home directory of Ubuntu.

13. To convert the E01 file using xmount and mount it, execute the command `xmount --in ewf Windows_Evidence_001.E01 /home/jason/Documents` in the terminal. This command converts the E01 file to dd file and mounts it onto Documents folder..
14. Make sure that the mount directory is empty before executing the command. You may also create a new empty folder and provide the location of the created empty folder for mount directory.
15. The mounted drive (here, Documents) will be created on the system.
16. Click on the mounted Documents directory to find `Windows_Evidence_001.dd` file:
17. This way, you can convert the E01 file into dd file format for further examination.

Task 3: Mounting Images on a Linux Forensic Workstation

You generated the image file of the evidence gathered from a hard drive to conduct investigation. In order to access and examine the files present in the image file, you should mount the image file using different tools.

In some cases, you end up in a situation where you cannot use your preferred tool. Therefore, you should know how to mount different forensic file image formats on different workstations using different tools.

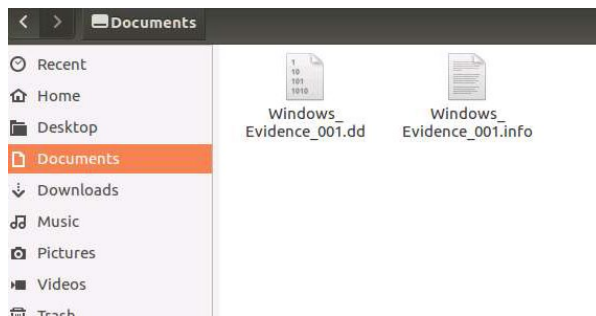
In this scenario, we consider mounting image files on a Linux forensic workstation.

Linux workstations can support various file systems and contains advanced tools that can help conduct forensic investigation.

Forensic image files are mounted on a drive to access and analyze files/folders present within the image file.

1. Use Ubuntu Machine for this activity.
2. This lab is a continuation of the previous task. In the previous task, we saw how to convert an E01 image to dd image. In this task, we will see how to mount this converted image to view its contents.
3. So, click on the Terminal icon from the launcher panel to launch the command line terminal.

4. Command line terminal launches. You require root privileges in the terminal to install an application.
5. Therefore, type `sudo su` and press Enter. You will be prompted to enter the password.
6. If you have not shut down the Ubuntu forensics virtual machine, and the `Windows_Evidence_001.dd` file is still mounted on Documents directory, skip to Step no 8.
7. If you have rebooted the machine, the mounted image would disappear, and you need to again convert the E01 file using `xmount` and mount it. (Refer previous task)
8. The `Windows_Evidence_001.dd` file appears in the Documents directory, as shown in the following screenshot:



9. Next, we will mount this image. In this lab, we are going to create a directory named `dd` within the `/mnt` directory and mount the image on this directory.
10. To create the directory, issue the command `mkdir /mnt/dd`.
11. To mount the image located at `/home/name/Documents/` onto `/mnt/dd` in read-only mode, type the command `mount -o ro /home/name/Documents/Windows_Evidence_001.dd /mnt/dd/` and press Enter.
12. Now the image is successfully mounted on the `dd` directory. To view the contents of the image through the command line terminal, type `ls -la /mnt/dd/` and press Enter.
13. A list of all the files pertaining to the image appears:
14. To view these files in the file manager, click on the Files icon in the Launcher panel to launch the File Manager.
15. File manager window will appear pointing to Home directory. Click on Computer from the left pane.
16. Now navigate to the directory, `mnt --> dd` to view the files.

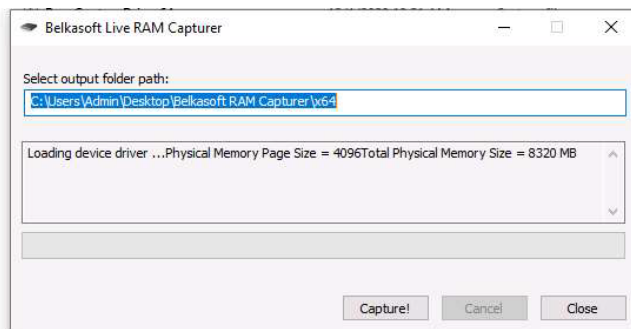
17. Our next task is to mount a dd image that contains Apple File System. (If you are not interested to work with Apple File System, ignore the below task) – This is not within your scope of your coursework.
18. To begin the task, navigate to the shared directory Forensic Images and copy MAC_Evidence_001.dd. Paste the image file in the Home folder.
19. Next, we shall mount an image by attaching it to a loop device. Before attaching it, you need to find a free loop device.
20. Clear the terminal screen by issuing clear command and continue to next step.
21. The losetup -f command helps you identify the first unused loop device. Therefore, issue this command to view the unused loop devices.
22. The unused loop device returned in the output might vary in your lab environment.
23. In this lab, we will be considering loop1 as the unused device. To attach the image to the loop device, type losetup -r /dev/loop1 MAC_Evidence_001.dd in the command line terminal and press Enter.
24. This mounts the image file (MAC_Evidence_001.dd) to the loop device loop1.
25. The mounted image (named Evidence Image) can be seen on the Launcher Panel.
26. Click on the mount icon to see Evidence Image folder that contains the contents of the image file:
27. Sometimes, images may contain hidden files and folders. To view them, press Ctrl+H on the keyboard.
28. This way, you can mount an image file using mount and losetup commands. These images form the base of the investigation and help gain crucial insights related to the investigation.

Task 4: Acquiring RAM from Windows and Linux Workstations

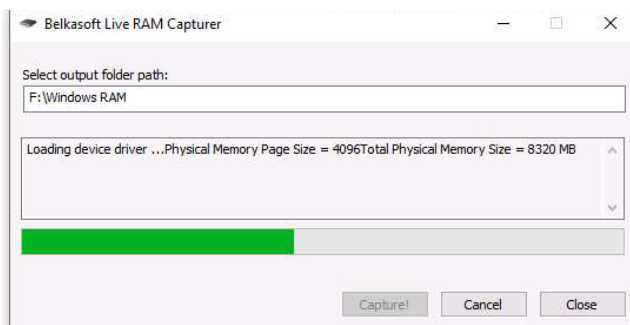
You are performing live analysis on a suspect's computer. In this process, you need to primarily capture the RAM dump of the machine as RAM contains volatile data that is lost when the machine loses power. In this scenario, you are performing RAM acquisition on both Windows and Linux workstations.

Note: RAM (Random Access Memory) is a volatile-memory storage found in computing devices that temporarily holds the data your device needs to access.

1. Use Windows 10 virtual machine
2. Before beginning this lab, navigate to the shared directory, Data Acquisition Tools, copy Belkasoft RAM Capturer folder and paste it onto Desktop. Alternatively, you can use any other relevant tools based on your research for your coursework.
3. Install and Launch RamCapture64.exe



4. If an Open File - Security Warning pop-up appears, click Run. If a User Account Control pop-up appears, click Yes.
5. You need to assign a folder to store the captured RAM. Therefore, create a folder named Windows RAM.
6. Now, enter the path for the output under Select output folder path field and click Capture!
7. The application begins to capture the RAM, as shown in the following screenshot:



8. Once the memory dump is successfully created, click Close to close the application.
9. Navigate to the folder to view the created memory dump. The dump is saved in the yyyyymmdd.mem format, where yyyy refers to the year, mm refers to the month, and dd refers to the date.

10. This way, you can capture the memory dump of a suspect Windows machine. These dumps act as important source of evidence for you while investigating volatile memory.
11. Now, we shall see how to dump RAM on Ubuntu machines.
12. Click on the Files icon in the Launcher panel to launch the File Manager.
13. File manager window will appear pointing to Home directory.
14. Now, go to Data Acquisition Tools, copy fmem and LiME folders and paste them in the Home directory.
15. Now, click on the Terminal icon from the launcher panel to launch the command line terminal.
16. Command line terminal launches. You require root privileges in the terminal to install an application.
17. Before you start acquiring RAM on this machine, you need to install fmem.
18. In terminal, type `cd fmem/` and press Enter.
19. You need to make sure that all the dependencies are met before installing fmem. Therefore, type `apt install -y build-essential` in the terminal and press Enter.
20. If the `apt install -y build-essential` command is not executing, then restart the Ubuntu Suspect virtual machine, acquire root privileges, run the command `cd fmem/`, and then run the above command so that it executes successfully.
21. If you are experiencing issues with internet connectivity, then run the commands `ifdown -a` followed by `ifup -a`, and then run the command `apt install -y build-essential`.
22. Type `make` and press Enter to build all the necessary libraries associated with fmem from the source code.
23. Now, type `bash run.sh` and press Enter to install the fmem tool.
24. In this lab, we are going to acquire RAM using local acquisition and remote acquisition methods. We will be using dd and LiME to acquire RAM locally, and dd to acquire RAM remotely.
25. To acquire RAM locally, type `dd if=/dev/fmem of=/home/james/ubuntu_local_ram.dd bs=1MB` and press Enter.
26. This begins to dump RAM of the machine in the Home folder with the name `ubuntu_local_ram.dd`.

27. It takes some time to complete the acquisition procedure. Upon dumping the RAM successfully, you will see the stats of the operation:
28. Now, navigate to the Home folder to view the created `ubuntu_local_ram.dd` file.
29. Next, we shall install LiME tool on the machine to use it for acquiring RAM. Therefore, type `cd /home/james/LiME/src/` in the command prompt and press Enter.
30. Now, type `make` and press Enter to build all the necessary libraries associated with LiME from the source code.
31. To acquire RAM locally, type `insmod lime-4.15.0-45-generic.ko "path=../../ubuntu_local_ram.mem format=lime"` and press Enter. This begins to dump the image of the RAM in lime format with the name `ubuntu_local_ram.mem` in the Home directory.
32. The kernel module version varies depending on the Ubuntu OS version installed on the suspect machine.
33. LiME takes a considerable amount of time to acquire the image. Navigate to Home directory to see the RAM dump.
34. We have successfully completed how to acquire RAM locally on an Ubuntu suspect machine using `dd` and LiME.

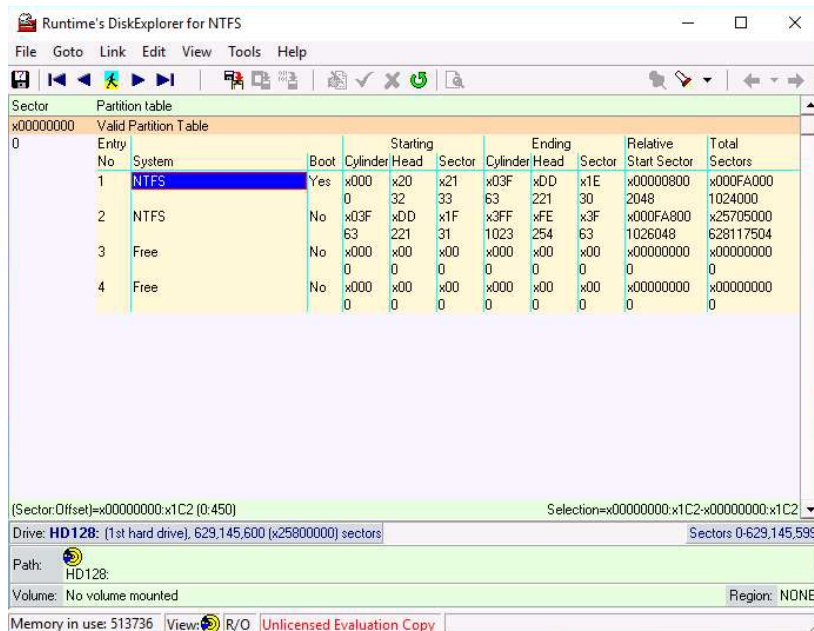
Task 5: Creating Customized Images from an Image Containing NTFS File System

NTFS has become the default storage format across various devices. It supports features such as compression and encryption, which help users hide data. Therefore, you need a deep knowledge of how the format works.

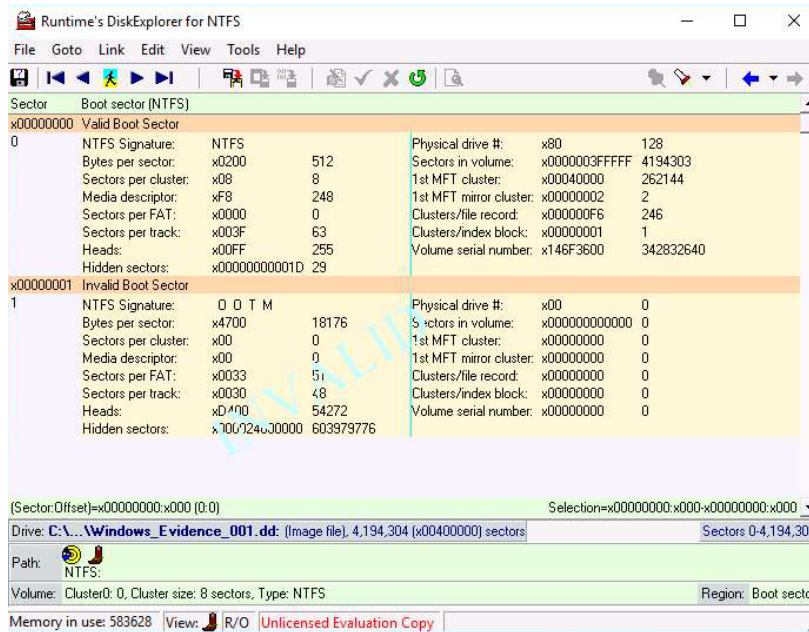
NTFS (New Technology File System) is the file system used by the Windows NT Operating system for storing and retrieving files on a hard drive.

1. Use Windows Client
2. Navigate to Resource Folder → Data Acquisition Tools\DiskExplorer for NTFS. Double-click `Setup.exe` to launch the setup and follow the wizard-driven installation steps to install the application. You can use other alternative tools as well.

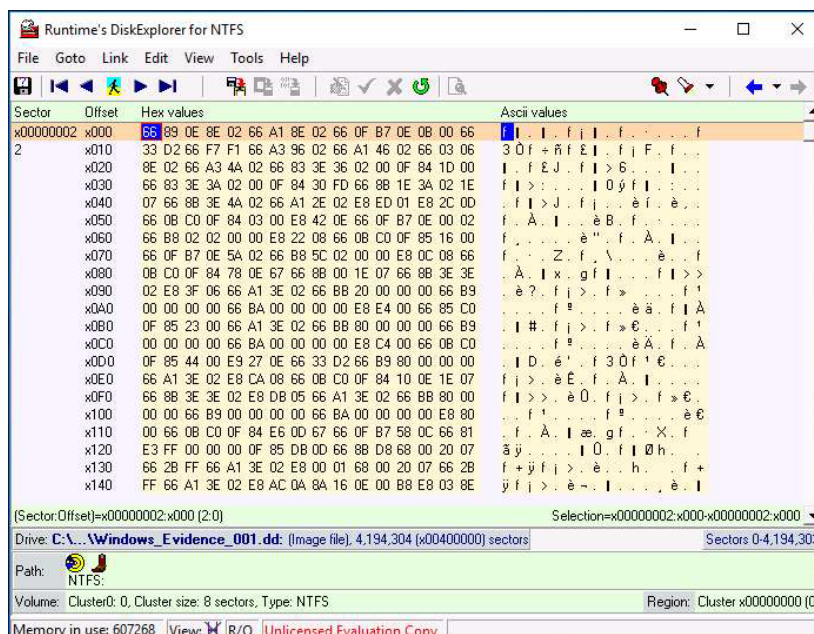
3. If an Open File - Security Warning pop-up appears, click Run.
4. To launch the application, double-click the DiskExplorer for NTFS shortcut icon located on the Desktop.
5. The main window of DiskExplorer for NTFS appears, as shown in the screenshot:



6. Now, we will import a forensic image into this application. Go to File and select Image....
7. Select file to open as a drive... window appears; in the Files of type drop-down list, select All files (.), navigate and select Windows_Evidence_001.dd, and click Open. It will display the complete details of the image file in two sectors, Valid and Invalid Boot Sector, as shown in the figure below:



8. Now, click the Sector icon on the toolbar or navigate to Goto --> Sector to view a specific sector.
9. In the Goto sector... wizard, enter a hex value of your choice (Here, we gave hex value as 00000002 in the Sector section) in the Sector or Byte section, to jump to a new position, and then click OK.
10. It will display the specified sector:
11. Click View --> as Hex, or alternatively you can press F3 to view the hex values of the selected sector.
12. The screenshot below shows the Hex view of the selected sector:



13. You can copy the entire/required hex data for future reference. To copy the entire data, go to Edit --> Select All.
14. The entire Hex data will be highlighted:
15. Navigate to Edit and click Copy to file... to copy the evidence file for further processing.
16. In the Copy pop-up window, select the destination location to save the file, and specify the name for the image file. At the top of the prompt, it will display the size of the image about to be created. Click Save.
17. In this lab, we are creating a folder named Runtime Disk Explorer Image on the Desktop, and saving the file to this location with the name RDEM.img.
18. In the Confirm pop-up, click No to save the image to a single file.
19. The application will start copying the image file:
20. Navigate to the directory, Desktop --> Runtime Disk Explorer Image to see the customized image (here, RDEM.img) created from the image file (here, Windows_Evidence_001.dd) containing NTFS file system.
21. Close all open windows.

Task 6: Viewing Contents of Forensic Image File

As part of investigation you are asked to scan all the systems using the AccessData FTK Imager tool to know if the deleted files on the systems contain any information of evidentiary value. The tool saves your time as it eliminates the hectic process of recovering every deleted file from the system.

After acquiring the forensic image of the hard disk, you need to preview the contents of the image file to see if it contains any evidence useful for investigation or any additional analysis is required.

1. Use Windows Server machine.
2. Navigate to Shared Resources and install AccessData FTK Imager. Alternatively, you can download from Internet as well.
3. At the end of the installation process, ensure that the Launch AccessData FTK Imager option is checked in the setup wizard and then click Finish.
4. The main window of AccessData FTK Imager appears:
5. Click File --> Add Evidence Item... to add evidence.

6. Alternatively, you may also click on the Add Evidence icon from the toolbar to add evidence.
7. A Select Source window opens. Select the Image File option and click Next.
8. In this lab, we will be examining a dd image; therefore, select the Image File radio button
9. Click the Browse button to specify the image file path Windows_Evidence_001.dd and then click Finish.
10. The evidence file (Windows_Evidence_001.dd) appears in the left pane of the main window under the Evidence Tree section. Expand the evidence file and its contents so that it appears in the form of a tree:
11. Select any file or folder (here, we selected images folder) from the Evidence Tree to view the file list in the Right pane under File List.
12. Apart from viewing the contents of a file or folder, AccessData FTK Imager also lets you view the hex values of files. 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 that normally cannot be accessed by the OS.
13. To view the Hex value of a file, select a file (here we selected 1200px-Peace_sign.svg.png) from the File List.
14. Click the Hex icon on the toolbar and Hex values of the selected file will be displayed in the bottom-right pane.
15. Click the Properties tab in the lower-left pane to view the properties such as file class, size, date, start cluster, etc. of the selected file.
16. Click the Hex Value Interpreter tab in the lower-left pane to view the properties such as signed integer, DOS date, etc. of the selected file.
17. This way you can examine the contents of the forensic image file using AccessData FTK Imager tool.
18. Close all open windows.

Task 7 (Coursework Task) – Acquire your Image Copy

This is a Group Activity. Form 2 Groups. The groups are not necessarily to continue in future. So, form groups based on the available members in the class.

1. Total time for each group: 30 Minutes
2. Form into Groups (Group 1 and Group 2)
3. Group 1 and Group 2 – 15 Minutes – Planning Phase
 - a. Setup your Lab System
 - b. Plan and assign roles
Make sure that each member in your group are aware of every process in this activity.
 - c. Document every steps done – Use these documentation during your coursework presentation.

Image Acquisition:

4. Group 1:
 - a. Collect the evidence from the Lecturer.
 - b. Make a image of the evidence. (Determine the type of image you need for this investigation and make image)
5. Group 2: Observe Group 1 and add critics in your presentation.

Ensuring Integrity:

6. Group 2: Once the image is acquired by Group 1 and you observed the process, check the integrity of the acquired image and confirm the same.
7. Circulate the copies to all members
8. Group 1: Observer Group 2 and add critics in your presentation.

Deliverables:

Make sure, all the student have a copy of the image to begin your investigation as a part of your coursework task.

Hint: Before you begin your investigation, check the integrity of the image file.



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 Image acquisition Process (Tools, Formats, Process etc).
3. Understanding and implementing data acquisition ensuring data integrity.
4. Rate yourself (1 very low – 5 exceptional): Understanding the Investigation Process.

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