



First Responder Handbook- Computer System Acquisition

(August, 2021)

NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)

Modernization Division
BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India



First Responder Handbook- Computer System Acquisition

National Cyber Crime Research & Innovation Centre (NCR&IC)

**Modernization Division
Bureau of Police Research & Development
New Delhi**

Disclaimer -

- ✓ This document is not a substitute for existing manuals available in the various States/UTs. It is only for awareness purpose. In case of any conflict, local manual/practice may prevail.
- ✓ BPR&D does not promote any tools/ software. All the mentioned tools and software in this manual are for demonstration purpose only.
- ✓ Wherever any Image/graphic/flowchart is taken from other sources, the same has been duly acknowledged

वरुण सिंधु कुल कौमुदी, भा.पु.से.

महानिदेशक

VSK Kaumudi, IPS

Director General

Tel. : 91-11-26781312 (0)

Fax : 91-11-26781315

Email : dg@bprd.nic.in



पुलिस अनुसंधन एवम् विकास ब्यूरो

गृह मंत्रालय, भारत सरकार

राष्ट्रीय राजमार्ग-8, महिपालपुर,

नई दिल्ली-110037

Bureau of Police Research & Development

Ministry of Home Affairs, Govt. of India

National Highway-8, Mahipalpur,

New Delhi-110037

Message



The setting up of the National Cyber Crime Research & Innovation Centre (NCR&IC) at the BPR&D Hqrs. and its branch, the National Cyber Crime Research, Innovation and Capacity Building, at the CDTI, Hyderabad, has been a major technological milestone in the cyber research and training capabilities of the BPR&D. The NCR&IC, as part of the umbrella scheme of the Indian Cyber Crime Coordination Centre (14C), MHA, has been striving continuously to strengthen and augment the capacity of Law Enforcement Agencies (LEAs) in their efforts of Cyber Crime prevention and investigation.

I am happy that NCR&IC professionals have come up with the following four booklets to address the urgent need for awareness related to Cyber Crimes, keeping in mind the skill set required by the police officers in the investigation of Cyber Crimes:

- Emerging Cyber Crimes in India - A Concise Compilation
- First Responder Handbook - Computer System Acquisition
- SOP on Investigative Process/Methodologies for Cryptocurrency related Cyber Crimes
- Manual on Social Media Intelligence (SOCMINT) for LEAs

The above manuals/SOPs are result of the sincere efforts of Dr. Karuna Sagar, IPS, IG (Modernization), Sh. B. Shanker Jaiswal, IPS, DIG (Mod), Dr. M. M. Gosal, SSO (T) and NCR&IC professionals/experts, namely, Dr. Pankaj Choudhary, Sh. Gourav Chaurasia, Sh. M. Krishna Chaitanya and Sh. Farhan Sumbul, BPR&D. I record my deep appreciation for their hard work.

I believe, these booklets will guide the police officers in understanding the Cyber Crimes of various categories, including the modus operandi of cyber criminals, Data Acquisition in different scenarios, Methodology for Investigating Cryptocurrency and Social Media Platform, etc.

(V.S.K. Kaumudi)

Place: New Delhi

नीरज सिन्हा, भा.पु.से.
अपर महानिदेशक

Neeraj Sinha, IPS
Additional Director General

Tel.: + 91 11 26781341 • Fax: 91 11 26782201
Email: adg@bprd.nic.in • Website: www.bprd.nic.in



पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Message



Technology is often value neutral. It can be used effectively by friends and foes alike. On occasions, the rapid strides by technology, especially in the domain of cyber-space, threatens to outpace the skills of inadequately trained professionals, especially at the cutting edge.

BPR&D, with its motto of 'Promoting Good Standards and Practices', has often bridged the information gap for the LEAs, with its thoughtful seminars and publications. It gives me great pleasure that the National Cyber Research & Innovation Centre (NCR&IC) professionals are putting together 04 significant compilations, including 'Emerging Cyber Crimes in India - A Concise Compilation'; 'First Responder Handbook - Computer System Acquisition'; 'SOP on Investigative Process/Methodologies for Crypto-currency related Cyber Crimes'; and 'Manual on Social Media Intelligence (SOCMINT) for the LEAs'.

The team of the Modernization Division of the BPR&D, led by Dr. Karuna Sagar, IPS, IG, Shri B S Jaiswal, IPS, DIG, Dr. Manjunath M Gosal, SSO (T), Dr. Sarabjit kaur, Dr. Pankaj Choudhary, Sh. Gourav Chaurasia, Sh. M. Krishna Chaitanya and Sh. Farhan Sumbul, are deserving of our appreciation for the publications.

I trust the Investigating Officers, particularly at the cutting edge, would find these compilations useful in their day to day professional lives.

(Neeraj Sinha)

Place: New Delhi.

डॉ. करुणा सागर, भा.पु.से.
महानिरीक्षक/निदेशक (आधुनिकीकरण)

Dr. Karuna Sagar, IPS
Inspector General/Director (Modernisation)

Tel. : 91-11-26782023
91-11-26782030 (F)
Email : igmod@bprd.nic.in



पुलिस अनुसंधन एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Executive Summary



Data Acquisition Systems impact a wide range of activities of day-to-day life. These Systems are widely used today in home automation systems, industrial monitoring and control as well as in a variety of other time-critical applications. Installation of Data Acquisition Solutions in Industries is a flexible and cost-effective measurement solution. Today, Data Acquisition Systems along with “Internet of Things” have led to the development of many applications.

The Central Government has initiated several measures for spreading awareness on cyber crimes, those include issuing cyber-related alerts/ advisories, capacity building/ training of law enforcement officers/ judges/ prosecutors and improving cyber forensics facilities etc. to prevent cyber crime and expedite investigations. States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of the law against reported cyber crimes.

This booklet ‘First Responder Handbook - Computer System Acquisition’ may be useful for the cyber crime investigating officers as a ready reckoner. It carries a step by step procedure for acquisition of computer system images from a crime scene. The step by step guide provided for the acquisition process from bitlocker encrypted computer systems makes this booklet more interesting.

My sincere congratulation goes to Sh. Gourav Chaurasia, Cyber Crime Investigator/Researcher, NCR&IC, who actively took part in compiling and publishing this booklet.


I hope that this booklet will assist all the Investigating officers across the country towards better preparedness in handling the acquisition process of a computer system with various scenarios.

(Dr.Karuna Sagar)

Place: New Delhi.

Table of Contents

| | |
|---|----|
| List of Tables | 10 |
| List of Figures | 11 |
| List of Flowcharts | 13 |
| List of Abbreviations | 14 |
| 1. Introduction | 15 |
| 2. Collection of Computer System | 16 |
| 2.1 Preparation stage | 16 |
| 2.2 Activities at the crime scene | 19 |
| 2.3 System Acquisition | 20 |
| 2.3.1 Windows System | 20 |
| 2.3.2 Mac system | 44 |
| 2.3.3 Linux System | 47 |
| 2.3.4 Stand Alone Storage device | 53 |
| 3. Packaging and transport of Electronic Evidence | 54 |
| Summary- | 56 |
| References- | 57 |



List of Tables

| | |
|--|----|
| Table 1: Write blockers web-links | 24 |
| Table 2: Steps for the Packaging process | 54 |

List of Figures

| | |
|--|----|
| Figure 1: Indicative Tools & Material Used at Scene of Crime | 17 |
| Figure 2: Evidence Duplicators & Extractors | 19 |
| Figure 3: Computer Management. | 25 |
| Figure 4: Computer Management Console. | 25 |
| Figure 5: Disk Management Console. | 26 |
| Figure 6: FTK Interface. | 26 |
| Figure 7: Source Evidence selection. | 27 |
| Figure 8: Image destination selection. | 27 |
| Figure 9: Image destination selection. | 28 |
| Figure 10: Destination drive selection. | 28 |
| Figure 11: Provided image filename and other setting. | 29 |
| Figure 12: Imaging process started. | 29 |
| Figure 13: C drive image file along with image log. | 30 |
| Figure 14: Detailed Image log. | 30 |
| Figure 15: Computer management console. | 31 |
| Figure 16: Computer management console. | 31 |
| Figure 17: Disk management console. | 32 |
| Figure 18: Decryption process on C, D and E drive. | 32 |
| Figure 19: Decryption status. | 33 |
| Figure 20: FTK Imager Interface. | 34 |
| Figure 21: Source evidence selection. | 34 |
| Figure 22: Select the Source disk. | 35 |
| Figure 23: Image destination selection. | 35 |
| Figure 24: Image type selection. | 36 |
| Figure 25: Evidence information. | 36 |
| Figure 26: Providing image name and other information. | 37 |
| Figure 27: Create image. | 37 |
| Figure 28: Image progress status. | 38 |
| Figure 29: Image hash verification results. | 38 |
| Figure 30: Add Evidence. | 39 |
| Figure 31: Image file selection. | 39 |

| | |
|---|----|
| Figure 32: Browse image file. | 40 |
| Figure 33: Evidence image preview. | 40 |
| Figure 34: FTK imager creates disk image. | 42 |
| Figure 35: Evidence image preview. | 42 |
| Figure 36: Linux terminal. | 48 |
| Figure 37: Attached hard disk information. | 48 |
| Figure 38: Dcfldd Command. | 49 |
| Figure 39: Steps for Linux machine acquisition. | 51 |
| Figure 40: Steps during the transport evidence. | 55 |

List of Flowcharts

| | |
|---|----|
| Flowchart 1: Detailed process for system acquisition – Powered ON Stage. | 20 |
| Flowchart 2: Detailed process for system acquisition – Power OFF Stage. | 22 |
| Flowchart 3: Detailed process for system acquisition with MacAfee Endpoint enabled. | 41 |
| Flowchart 4: Detailed process for RAID system acquisition – Power ON Stage. | 43 |
| Flowchart 5: Detailed process for Linux system acquisition – Power ON Stage. | 48 |
| Flowchart 6: Detailed process for Linux system acquisition – Power OFF Stage. | 52 |
| Flowchart 7: Detailed process for SAD acquisition. | 53 |

List of Abbreviations

| | |
|-------|---|
| LEA's | Law Enforcement Agencies |
| IO | Investigating officer |
| VM | Virtual Machine |
| VMDK | Virtual Machine Disk |
| USB | Universal Serial Bus |
| NTFS | New Technology File System |
| HFS | Hierarchical File System |
| SSD | Solid-State Drive |
| SAD | Standalone device |
| RAID | Redundant Array of Independent Disks |
| MB | Megabyte |
| AVML | Acquire Volatile Memory for Linux |
| BPRD | Bureau of Police Research and Development |
| NCRIC | National Cyber Crime Research Innovation Centre |
| I4C | Indian Cyber Crime Coordination Centre |

1. Introduction

Dependence on the internet has increased manifold in the last decade and is increasing exponentially in the daily life of mankind. Though the use of the internet has eased access to several channels of information in the life of an individual, it has also invited many ill effects; many of those are reported as typical Cyber Crime cases.

Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cyber-crime. The term digital forensics was first used as a synonym for computer forensics.¹

Digital forensic investigation has many steps data collection, acquisition, process, analysis, preservation, presentation.

Data acquisition in many of the cases is one of the major challenges where LEAs face many challenges i.e., Disk encryption, password, MacAfee disk encryption, File-vault, T2 Security and many more.

This booklet cover procedure to be followed for the onsite retrieval, transport and handling of digital evidence, including situations where evidence is seized from individuals or companies.

They furthermore contain procedures for the live acquisition of suspect system data onsite, while the identified computer systems are turned on/running, as accessing them later might be prevented by passwords or encryption.

Finally, this booklet procedures for the acquisition of data from a computer system in where the physical collection of a computer system is not feasible.

The objective is to create this booklet for LEAs for a better understanding of the data acquisition process so that The First Responder² can easily take a decision at the crime scene and do the proper data acquisition.

As per the National Crime Records Bureau Report (NCRB 2019), cyber-crimes in India have 63.5 % increased dramatically in the year 2019 as compared to previous years. It is anticipated that such crimes will become epidemic unless they are effectively and promptly dealt with and the perpetrators are convicted and punished.

The National Cyber Crime Research and Innovation Center (NCR&IC) under the I4C scheme of the MHA set up at the **Bureau of Police Research and Development (BPR&D)** has compiled this booklet, viz., *“First Responder Handbook - Computer System Acquisition”* to provide a comprehensive Best Practice to Investigation Team to deal more effectively with the cyber-crime cases where the computer system is under study. The step-by-step approach towards such cases would help LEAs build effective and foolproof cases against culprits leading to the conviction.

1 <https://www.eccouncil.org/what-is-digital-forensics/>

A first responder in a computer forensic scenario is the individual who is first to find out about the situation and start to address it.W

2 A first responder in a computer forensic scenario is the individual who is first to find out about the situation and start to address it.

2. Collection of Computer System

2.1 Preparation stage

The process of collecting digital evidence has both technical and judicial effects and should be viewed in its entirety, starting from the initial steps of collecting computer systems or storage devices made available voluntarily or acquire through searches of premises.

Gathering as much data as possible on the location to be searched for seizing computer systems or storage devices is key and provides relevant Investigation Officers with insights that will help them in their work.

Section 79A Information Technology (Amendment) Act 2008 defines the electronic form of evidence as “any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cellphones and digital fax machine”.

The main feature of digital evidence is that it can be transmitted beyond borders with ease and speed, is highly fragile and can be easily altered, damaged, destroyed and also time-sensitive. Owing to this reason special precautions should be taken while documenting, collecting, preserving and examining digital evidence.

Digital evidence especially related to crime are to be collected immediately as early as possible and should be preserved scientifically because digital evidence is highly volatile. Any delay or laps in collection and preservation of digital evidence will result in unavailability or deterioration of valuable evidences. So ultimate care and diligence should be used for collection of digital evidences so that all available evidences are collected and the victim does not suffer any miscarriage of justice.³

Before reaching the search scene, the Investigation Officer must obtain as much information about the offence/Crime as possible. The type of crime investigated may influence preparations before arrival at the Crime Scene. Since sources of digital evidence typically need special handling, the Investigation Officer should ensure that appropriate tools and equipment are taken to the scene (Premises).

65B. Admissibility of electronic records. -- (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

The conditions referred to in sub-section (1) in respect of a computer output are mentioned in The Indian Evidence Act, 1872. For further reference, an officer can refer to the below link-

³ Digital Evidence Related to Crimes against Women and Children – SOP, Kerla police

Crime scene management is an extremely sensitive task where the best practices and relevant toolkits must be used. In addition to the tools for processing crime scenes in general, first responders should have the following items as shown in Figure 1 in their digital evidence collection toolkit:



Figure 1: Indicative Tools & Material Used at Scene of Crime

List of things to be carried by the Investigation Team at the Crime Scene:

- Cameras (photo and video)
- Cardboard boxes
- Notepads
- Gloves
- Evidence tape
- Paper evidence bags
- Evidence stickers, labels, or tags
- Crime scene tape
- Antistatic bags
- Permanent markers
- Nonmagnetic tools
- First responding officers
- Crime scene personnel
- Consent/search forms
- Crime scene barricade tape
- First-aid kit
- Flashlight and extra batteries
- Markers
- Notebook

- Paper bags
- Personal protective equipment (e.g., gloves)
- Camera (plus memory cards, back up battery, remote flash, tripod and remote cord)
- Evidence seals/tape
- Blank papers, pen & pencils
- Labels / Scales for Photography
- Physical Evidence collection containers
- Evidence identifiers
- Extension cords
- Fingerprint ink pad and print cards for elimination prints
- Pocket knife
- Volatile Data Collection Kit – New/Sterilized CDs, DVDs, USB drives and hard disk etc.
- Digital Evidence Storage Containers – Anti-static bags, Faraday bags, Plastic bubble wraps etc.
- Cables – RJ45, Cross over, USB cables, mobile charging/sync cables etc.
- Physical Acquisition Units/Imaging Tools – Logicube Neo / Tableau etc. for disk duplication
- Hardware Write Blockers & Cables (USB / SCSI / SATA / Firewire etc.)
- Digital Workstation – Laptop with at least i7 processor, 32 GB RAM, 512 GB SSD For operating system and 2 TB Hard drives for data storage, 4 GB Graphics Processor etc.
- Forms (seizure memo, chain of custody, forwarding letter, 65-B certificate)
- IO & Police station seal & stamp & wax
- Magnifier
- Staplers, pin and paper clips
- A Laptop of good configuration, installed with all software tools (For hashing, imaging & analyzing disk, mobile, network & live system data)
- CDs/DVDs/pen drives with portable software tools can be used for hashing, imaging & analysis of data.
- Hardware / Software write blocker to protect the suspect media from tampering with the data while doing the hashing, imaging and analysis (if needed)

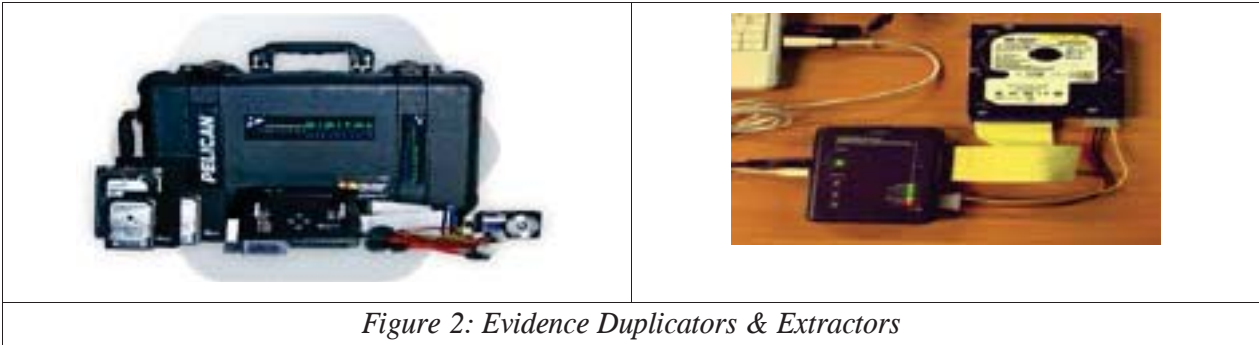


Figure 2: Evidence Duplicators & Extractors

- Disk imaging hardware or software tools for taking a copy of original storage media (suspect media)
- External Sterile Media to store the image (file) of a suspect media

2.2 Activities at the crime scene

The first responder plays a crucial role at the crime scene. While searching premises (any location where the search is in progress), to eliminate the risk of discarding/destroying important evidence or of suspects leaving the scene where computer systems, computer data and digital devices are to be seized, all location access routes need to be secured well in advance to the search.

Digital data is extremely volatile and hence consideration must be taken about the speed of entry to the scene. It is prudent to prevent the suspect from deleting/wiping/destroying data at the time of entry and steps should be taken to isolate the suspect from any device which may contain digital evidence.

The following activities are carried out immediately after entering a location where computer systems, computer data and digital devices are to be seized from:

- 1 Identify and determine the number of computer systems available on site, their type, whether they are connected to a network and can access the Internet.
- 2 Forbid access to computer systems/data and digital devices or other electronic equipment as well as to power supply sources, of persons identified at the location where the activity/search is to be conducted.
- 3 Document the scene, all sources of digital evidence that might be a target of seizure and their status and connections.
- 4 Check the operational status of each of the identified computer systems whether they are power On or Off.

If a large number of computer systems or storage devices are to be seized, one should use automated tools for filtering all seized electronic evidence, passing only the most relevant artefact for further analysis by digital forensic Investigation Officers. The users (Investigation Team) of these tools should be appropriately trained for their usage and lawfully authorized to operate them. Training should incorporate an understanding of the relevance of items to be seized and prioritization to avoid the seizure of unnecessary items. The principle of record-keeping should be maintained throughout the process.

All actions taken at the scene should be documented/recorded and this report should remain with the case file for further examination.

2.3 System Acquisition

The Crime scene might throw different challenging scenarios at the premises (home/office). A broad list of possible scenarios with examples for the IO along with the Investigation Officer is listed below to help them correctly perform the system acquisition.

2.3.1 Windows System

Scenario 1 - Computer system with powered On stage



Flowchart 1: Detailed process for system acquisition – Powered ON Stage.

Note –

- a.) RAM Dump – RAM dump is also known as the memory dump. It is the process of taking all the information content in RAM and writing it to a storage drive.
- b.) FTK Imager – FTK imager is the free software/ application. FTK imager helps in various activities such as Forensic Imaging, Image Mounting, Data Exportation, RAM Dump, Registry Extraction etc.
- c.) Magnet Acquire – Magnet Acquire is to be used for extracting RAM dump and is a free application.
- e.) Disk Encryption – Encryption is the method in which information is converted into secret code that hides the actual information.
- f.) BitLocker - BitLocker secures data by encrypting it. Encryption secures data by scrambling it, so it can't be read without decryption using a Decryption Key. BitLocker differs from most other encryption programs because it uses Windows

login to secure your data and no extra password is needed. Once you're logged in, your files look just like they would otherwise, and once you log out everything's secured.

- g.) VM – Virtual machine (VM) is a virtual environment that functions as a virtual computer system with its CPU, memory, network interface, and storage, created on a physical hardware system (located Off or On-premises). VM might be created and run using the VMware, Oracle virtual box and Hypervisor.

The Investigation Team must check the different attributes of the VM in the suspected system.

VMDK - This is a virtual disk file/Image of the VM which stores the contents of the virtual machine's hard disk drive. It is a virtual machine disk file format, and an open format developed by VMware. These files have a .vmdk extension and are used by VMware and Virtual Box virtual machines.

- h.) Source drive – Source drive is also known as Source Disk/Hard disk which is the suspect system's internal disk.

In the current generation of Systems, computer manufacturing companies install two separate hard disks in the systems to speed up the system. One is a dedicated SSD for the operating system and the other is for data storage. The Investigation Team must carefully verify all the installed Hard Drives in the suspect's system.

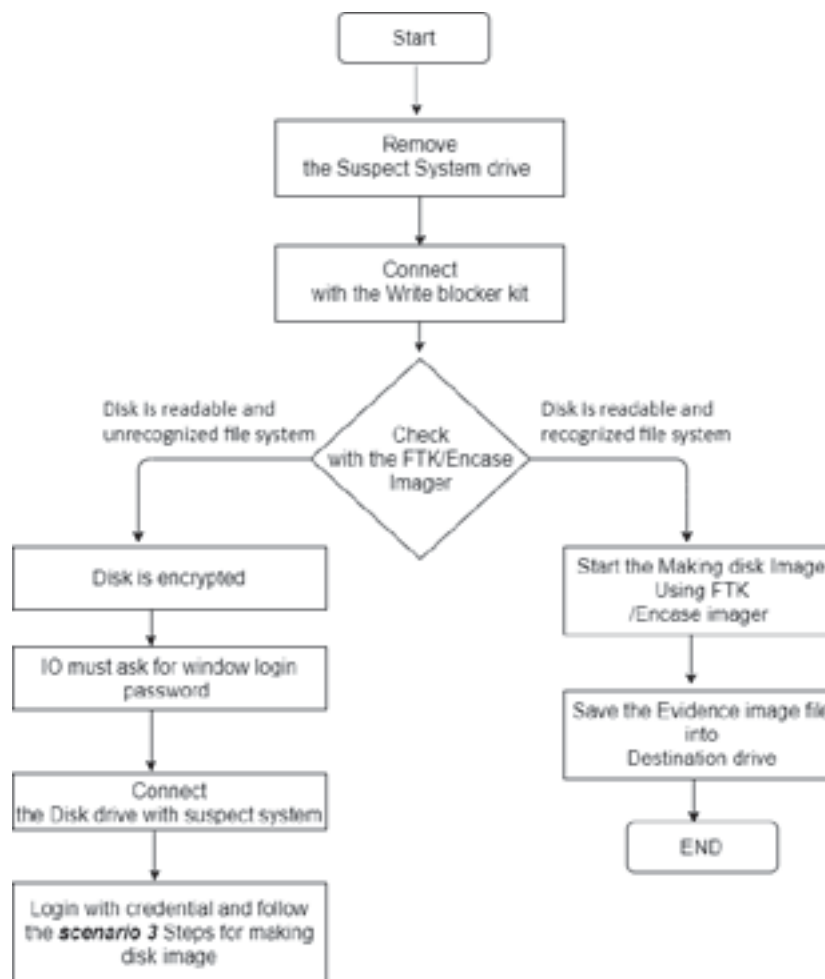
- i.) Destination drive – During the disk imaging process, a disk is used for storing the image file which is known as destination drive/disk/hard disk. Keep in mind always to choose the destination disk larger than the source disk.
- j.) Forensic Image File – A Forensic Image is a comprehensive duplicate of electronic media such as a hard disk drive. Artefacts (information or data created as a result of the use of

an electronic device that shows past activity) such as deleted files, deleted file fragments, and hidden data may be found in slack (unused space that is created between the end-of-file marker and the end of the hard drive cluster in which the file is stored and unallocated space (an unused portion of a hard drive). This exact duplicate of the data is referred to as a bit-by-bit copy of the source media and is called an Image.

The investigation officer must check all the installed applications so that they have an idea about the types of applications present in the suspect's computer system.

Scenario 2 - Computer system with Powered Off stage

When the First responder has no idea about the source evidence disk as to whether it is encrypted or not, there are two methods to check encryption and making the disk image of the suspect's system.



Flowchart 2: Detailed process for system acquisition – Power OFF Stage.

Note –

- a.) Write blocker - A write blocker is a tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker when used properly, can

guarantee the protection of the data integrity. Some write blocker is also in-built with the Forensic imager.

Some examples of write blockers are as below –

Use the pocket-size USB 3.1 Write Blocker for fast forensic access to USB storage devices. It packs incredible performance into a tiny package and is an essential device in any digital Investigation Officer's toolkit.



The Forensic ComboDock is a professional hard drive write blocker with read/write capabilities. Switching from write blocker mode to read/write mode is easy, but it's impossible to unintentionally turn off write blocking.



The WriteProtect-DESKTOP provides digital forensic professionals with fast, secure, read-only write-blocking of suspect hard drives. The only portable write-blocker that provides support for 6 different interfaces in one device. The WriteProtect is the ideal write-block solution for lab or field acquisitions.



Tableau Comprehensive Write Block Kit



Coolgear USB 3.0 / 2.0 to IDE/SATA Adapter

**Table 1: Write blockers web-links**

| Name | Link |
|--|---|
| USB 3.1 WriteBlocker | https://www.cru-inc.com/products/wiebetech/usb-3-1-writeblocker/ |
| Forensic ComboDock | https://www.cru-inc.com/products/wiebetech/forensic-combodock-v5-5/ |
| WriteProtect-DESKTOP | https://www.logicube.com/shop/writeprotect-desktop/?v=c86ee0d9d7ed |
| Tableau write blocker | https://security.opentext.com/tableau/hardware |
| Coolgear USB 3.0 / 2.0 to IDE/SATA Adapter | https://www.coolgear.com/product/usb-3-0-sataide-adapter-with-write-protection |

Scenario 3 - Computer system with Bit Locker (Powered On stage)

“Before making the disk image, Investigation Team must check the Bit locker Encryption status.”

Step 1 - Right-click on the This PC icon and click on the Manage tab as shown in the below Figure 3.

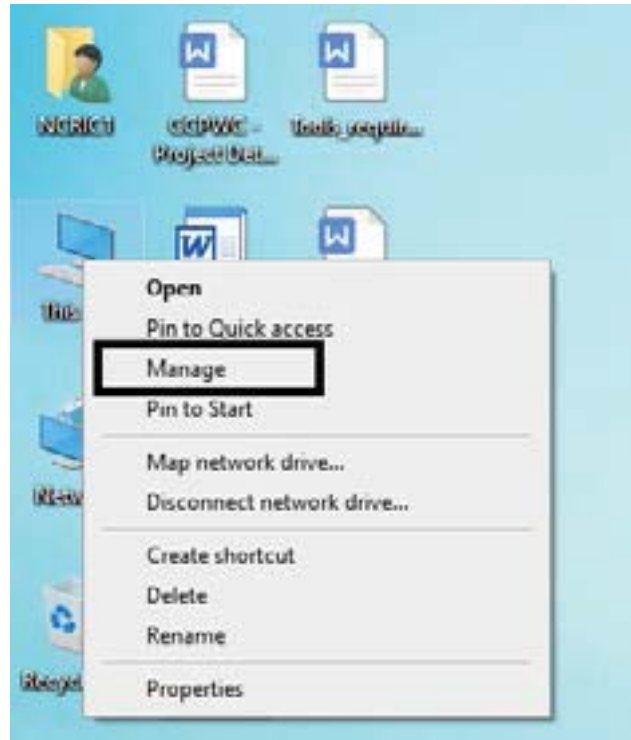


Figure 3: Computer Management.

Step 2 - In the Computer management option, click on the disk management as shown in Figure 4.



Figure 4: Computer Management Console.

Step 3 – Suspect’s system internal disk is Bit-locker encrypted as shown in the below Figure 5.

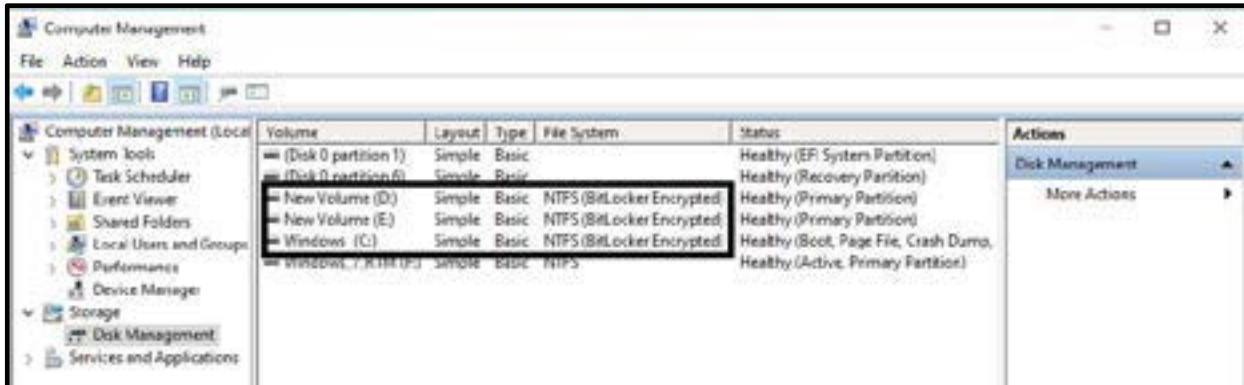


Figure 5: Disk Management Console.

Perform the logical acquisition with the help of FTK Imager of all the highlighted disk volumes as shown in the above Figure.

Step 4 - Launch the FTK Imager and select the Create Disk Image Option as shown in Figure 6.

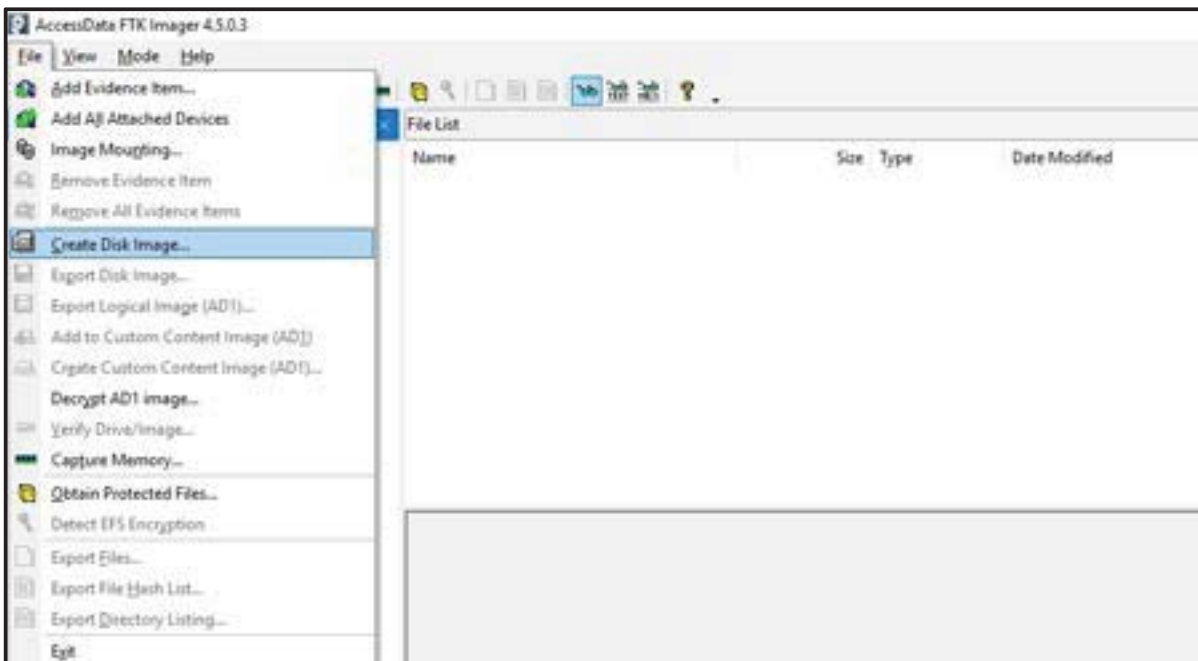


Figure 6: FTK Interface.

Step 5 - Next, select the Logical drive option as highlighted in below Figure 7.

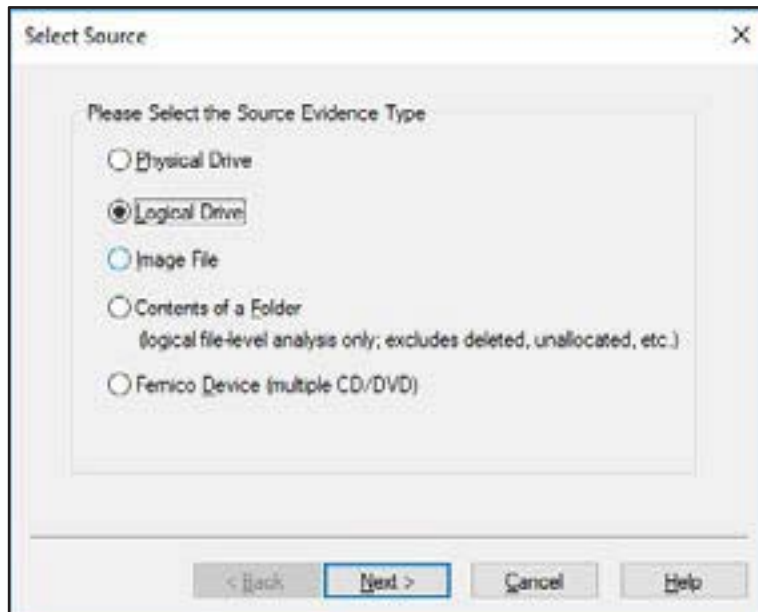


Figure 7: Source Evidence selection.

Step 6 - Select the image source as shown in Figure 8.

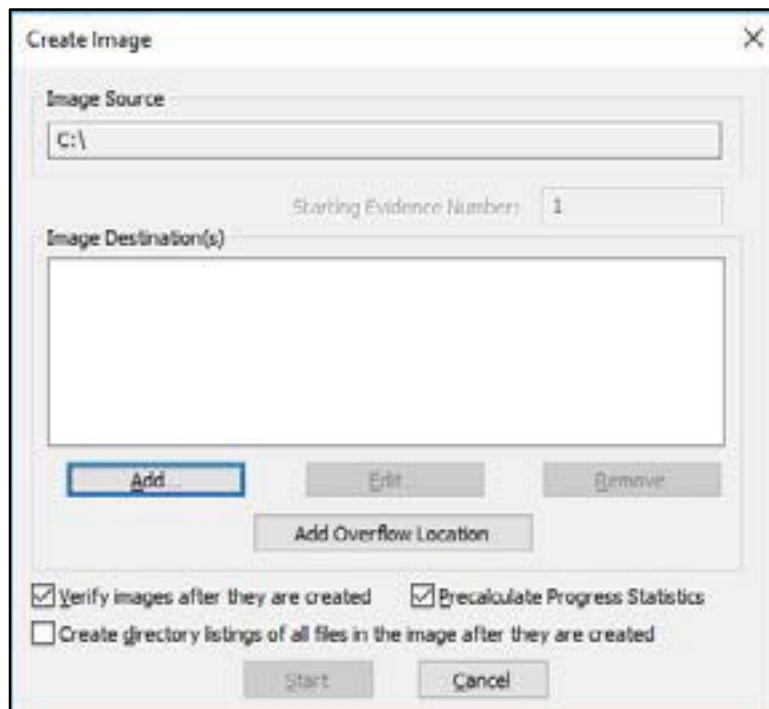


Figure 8: Image destination selection.

Step 7 - Click on the Browse button and select the Image destination Path for storing the image file as shown from Figures 9 to 11.

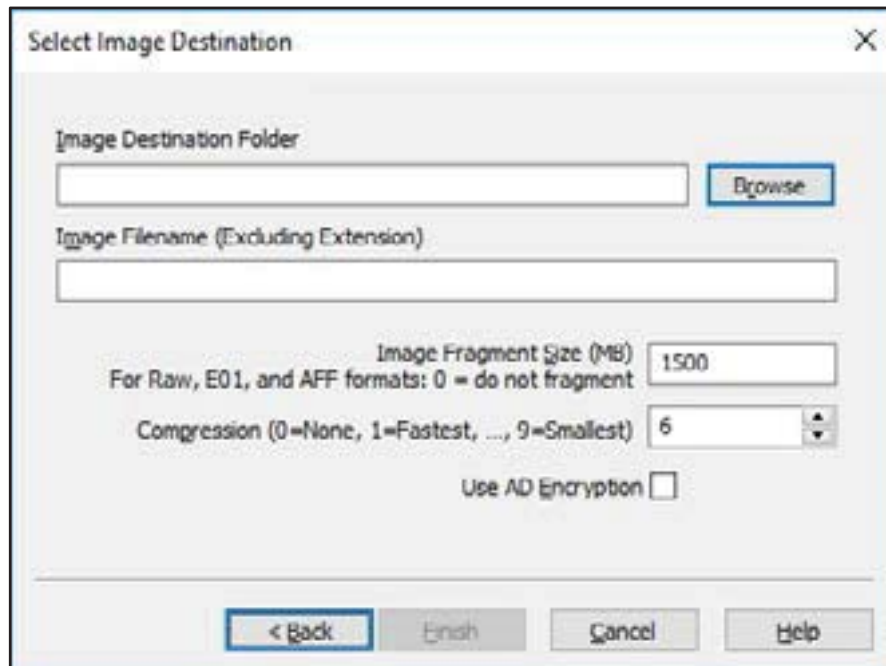


Figure 9: Image destination selection.

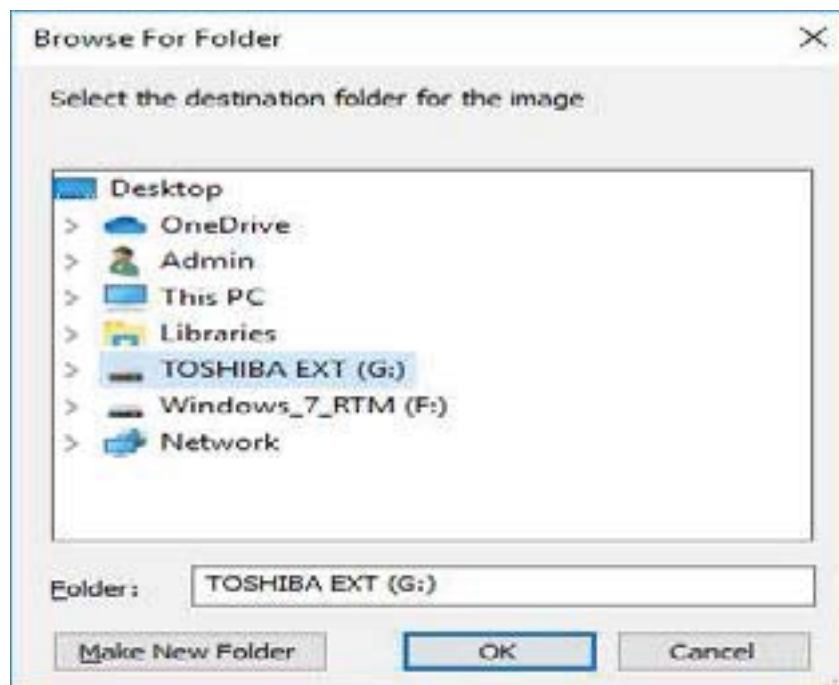


Figure 10: Destination drive selection.

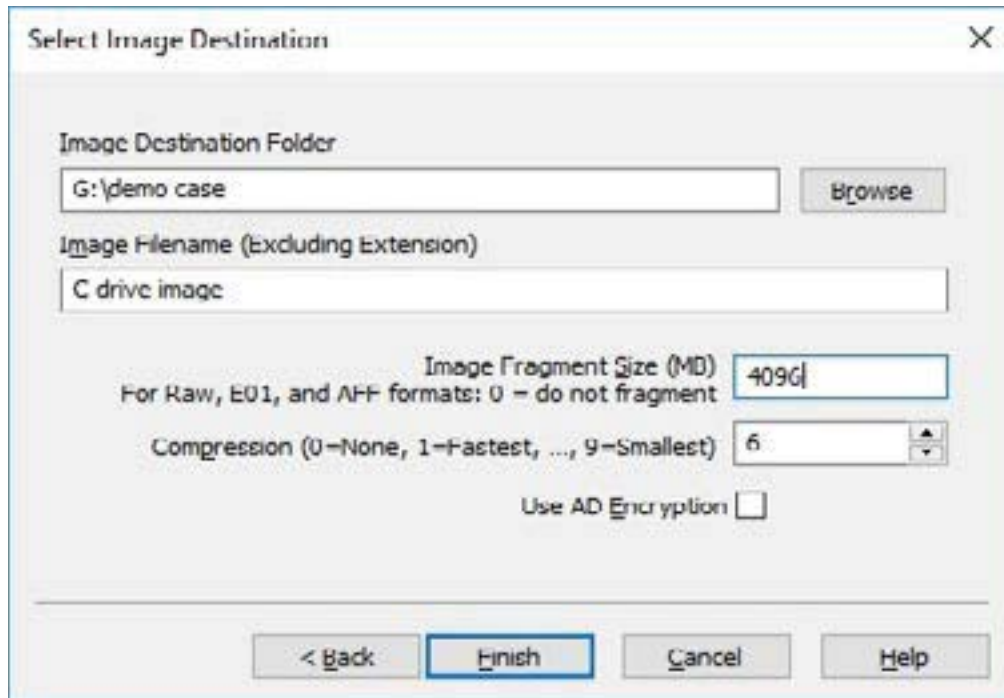


Figure 11: Provided image filename and other setting.

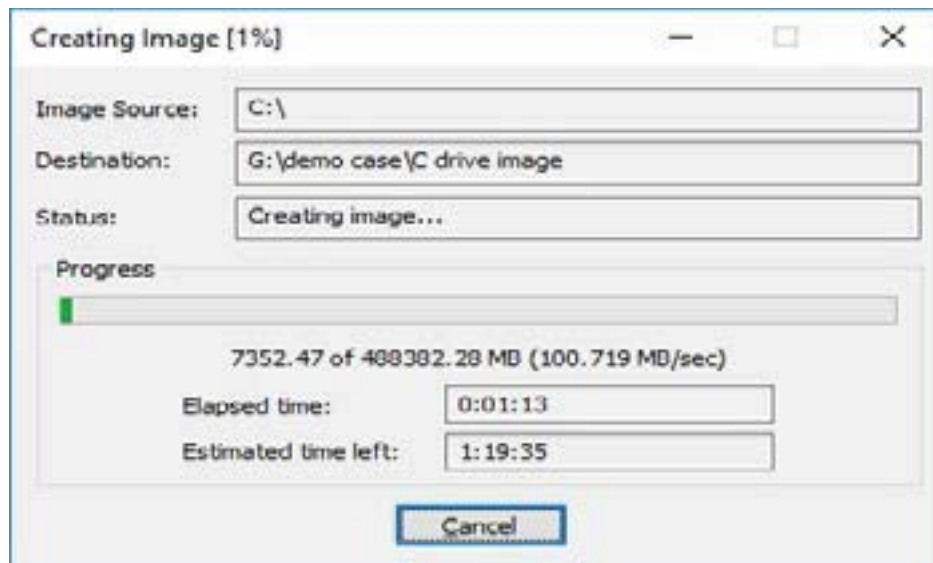


Figure 12: Imaging process started.

Step 8 - Then Imaging Process will be started as shown in Figure 12.

Step 9 - Once the process is finished, a log file will be generated and saved into the location as highlighted in Figure 13.

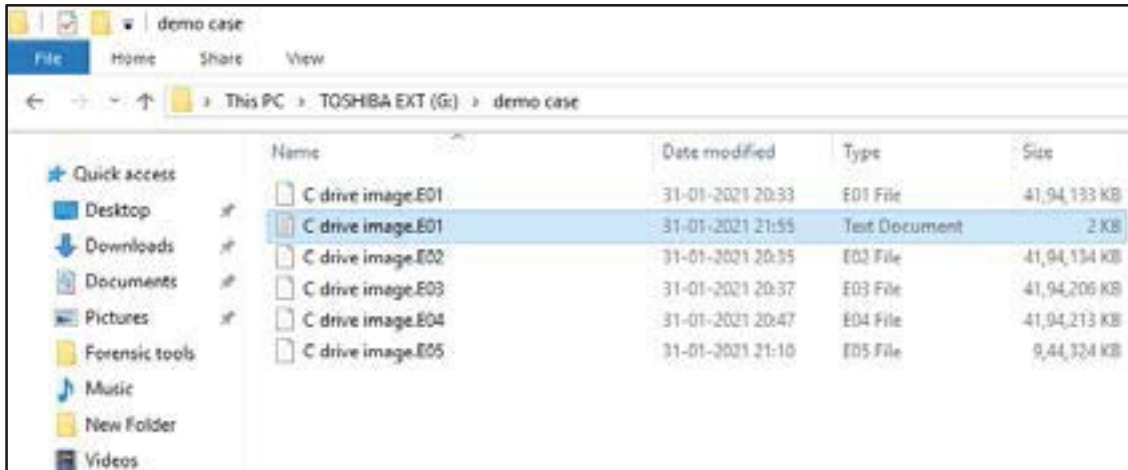


Figure 13: C drive image file along with image log.

Step 10 – Further, the Investigation Team can check the logical image along with the log report



Figure 14: Detailed Image log.

Similarly, create the logical images of D and E drives.

Scenario 4 – Computer system with bit locker enabled by default

“Before creating the disk image, Investigation Team must verify the Bit locker Encryption status as below.”

Step 1 - Right-click on the This PC icon and click on the manage tab as shown in Figure 15.

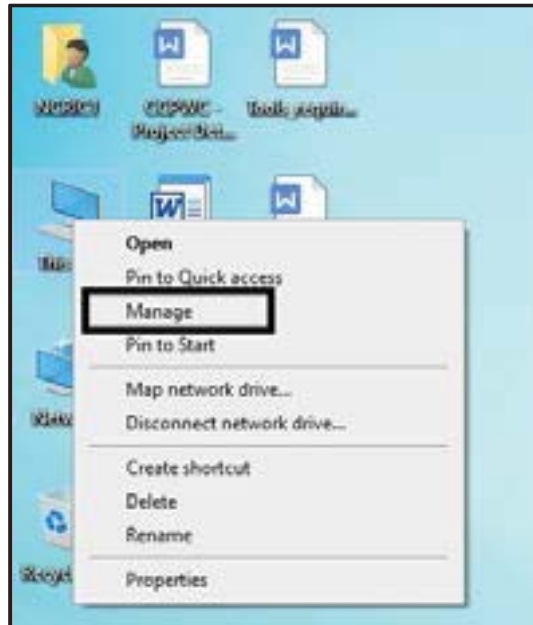


Figure 15: Computer management console.

Step 2 - In the computer management Console, click on the disk management option as shown in Figure 16.



Figure 16: Computer management console.

Step 3 – The highlighted portion in Figure 17, shows that the suspect’s system internal disk is BitLocker encrypted as shown.

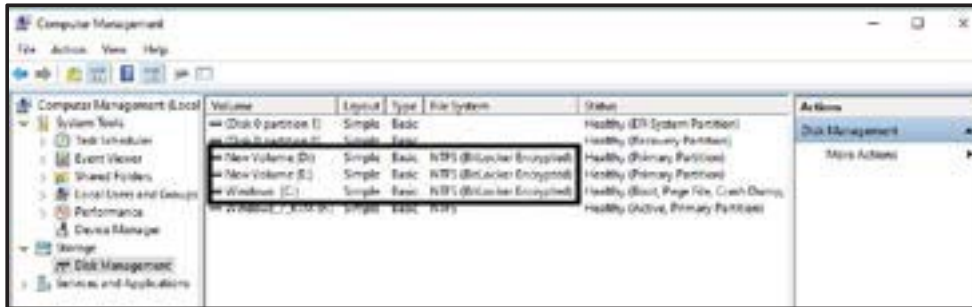


Figure 17: Disk management console.

As shown in Figure 17, there are 3 partitions C, D, and E having the BitLocker encryption enabled. The Investigation Team should use the `manage-bde`⁴ command to disable the bitLocker as shown in Figure 18.

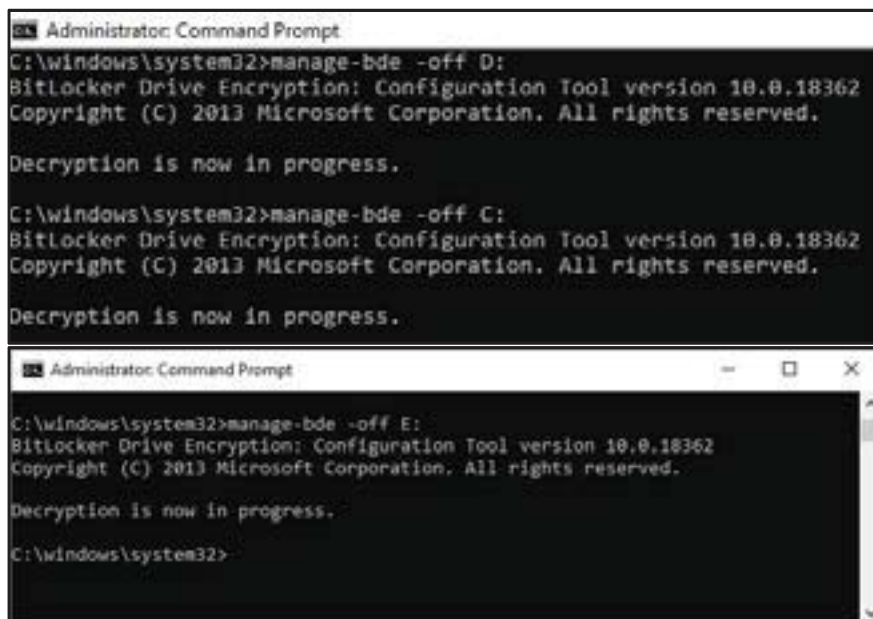


Figure 18: Decryption process on C, D and E drive.

Note – this process may take some time depending on the data size and hard disk type.

Next, use the “`manage-bde -status`” command to verify the bitLocker status on each partition as shown in Figure 19.

⁴ Manage-bde is a command-line tool that can be used for scripting BitLocker operations. For this operation administrator permission is required.

Conversion Status = Fully Decrypted

Encryption method = None, along with some other parameters.

```
Administrator: Command Prompt
C:\windows\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.18362
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: [Windows ]
[OS Volume]

    Size:                298.73 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Key Protectors:       None Found

Volume D: [New Volume]
[Data Volume]

    Size:                338.86 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Automatic Unlock:     Disabled
    Key Protectors:       None Found

Volume E: [New Volume]
[Data Volume]

    Size:                292.97 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0.0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Automatic Unlock:     Disabled
    Key Protectors:       None Found
```

Figure 19: Decryption status.

Note – Default encryption does not ask for a key/password during the decryption operation.

Step – Once the bit locker has been disabled from all the partitions, create the disk image as shown in Figure 20.

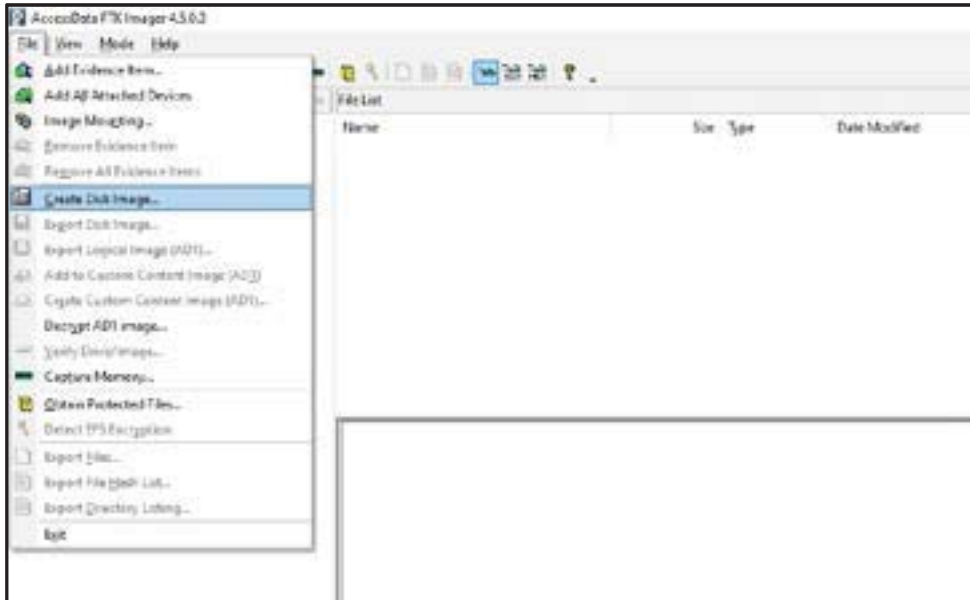


Figure 20: FTK Imager Interface.

Select the Physical drive option and click Next as shown in Figure 21.

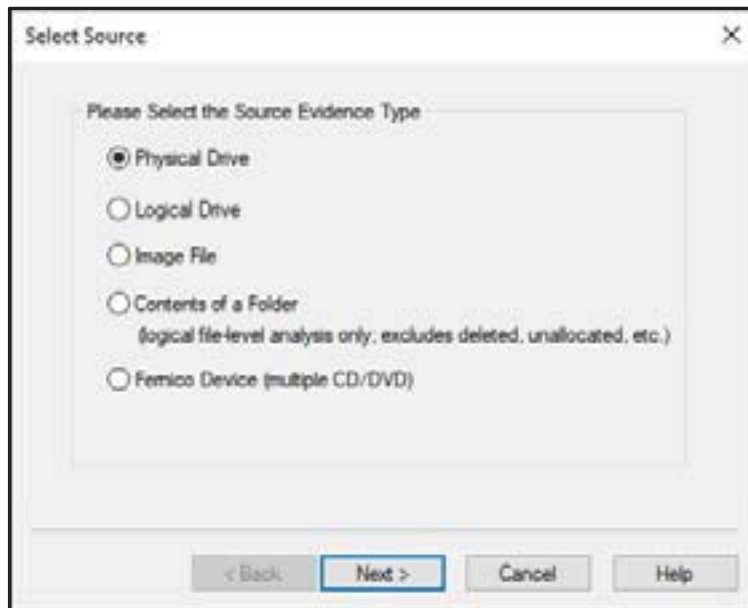


Figure 21: Source evidence selection.

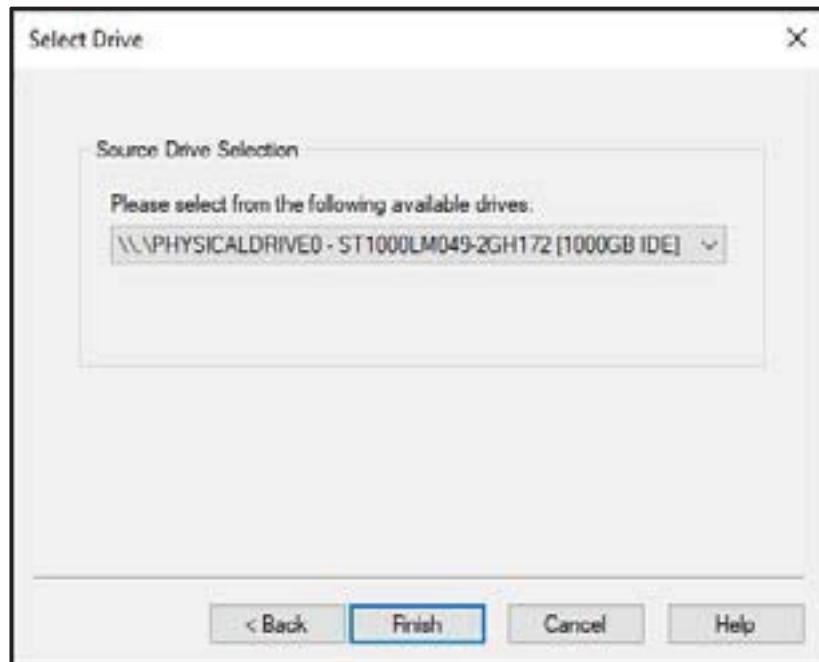


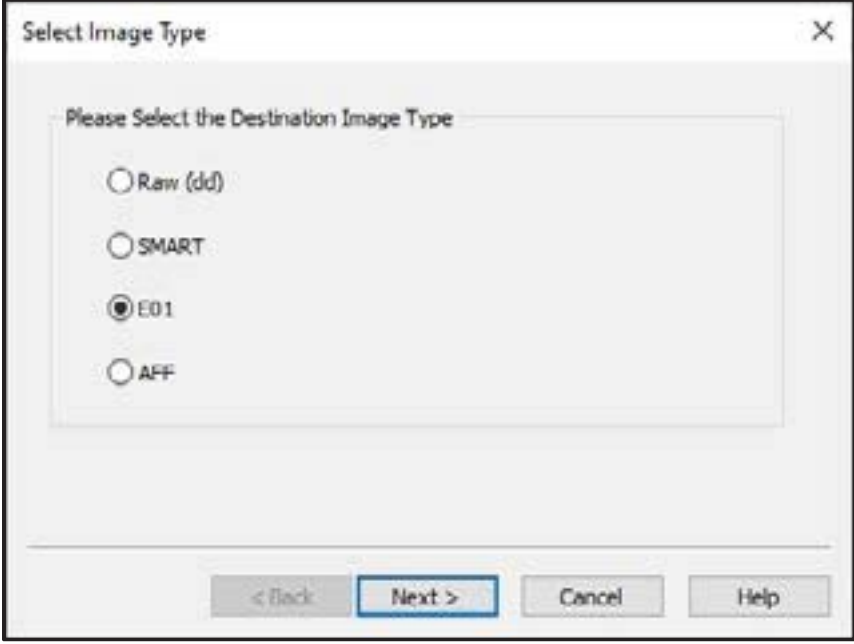
Figure 22: Select the Source disk.

As shown in Figure 22, select the Source Drive and click the Finish button.



Figure 23: Image destination selection.

Select the image type as shown in Figure 24 (Type E01 in the example)



Select Image Type

Please Select the Destination Image Type

Raw (dd)

SMART

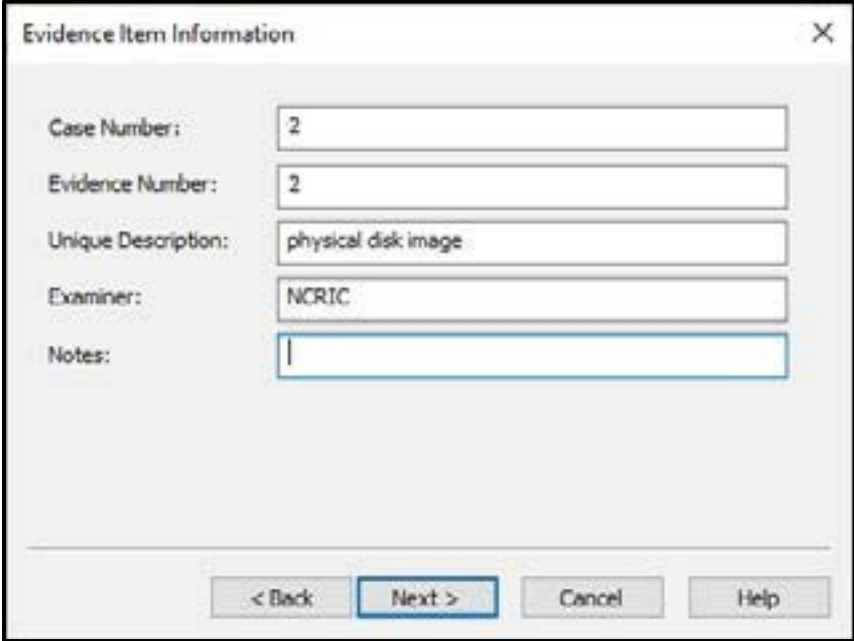
E01

AFF

< Back Next > Cancel Help

Figure 24: Image type selection.

Next, provide the case information as shown in Figure 25.



Evidence Item Information

Case Number: 2

Evidence Number: 2

Unique Description: physical disk image

Examiner: NCRIC

Notes:

< Back Next > Cancel Help

Figure 25: Evidence information.

Then select the image destination as shown in Figure 26. The image fragment size is editable and the Investigation Team can change the size if they want. (The default size is 1500 MB)

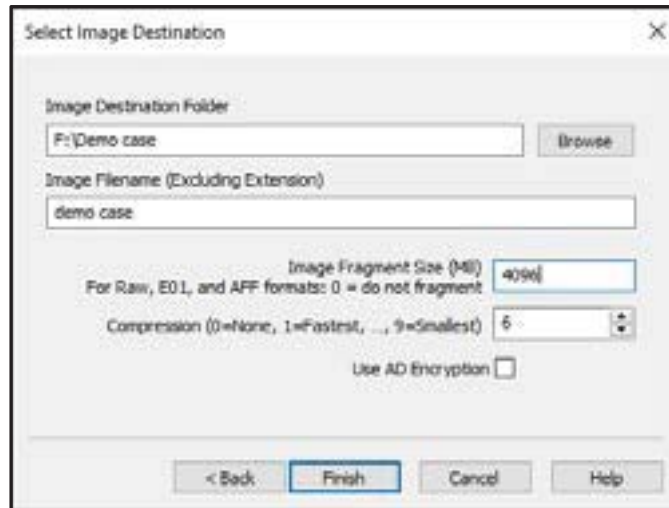


Figure 26: Providing image name and other information.

Once image source and image destination have been selected, click on both the checkboxes (Verify the image after they are created⁵ and Precalculated progress statistics⁶) as shown in Figure 27. Then click on the start button.



Figure 27: Create image.

⁵ Verify Images after they are created to check the image hash signature. This detects whether the content of the original data has changed since it was copied to the image.

⁶ Precalculate Progress Statistics to see approximately how much time and storage space creating the custom image will require before you start, and as the imaging proceeds.

Image successfully created as shown in Figure 28.

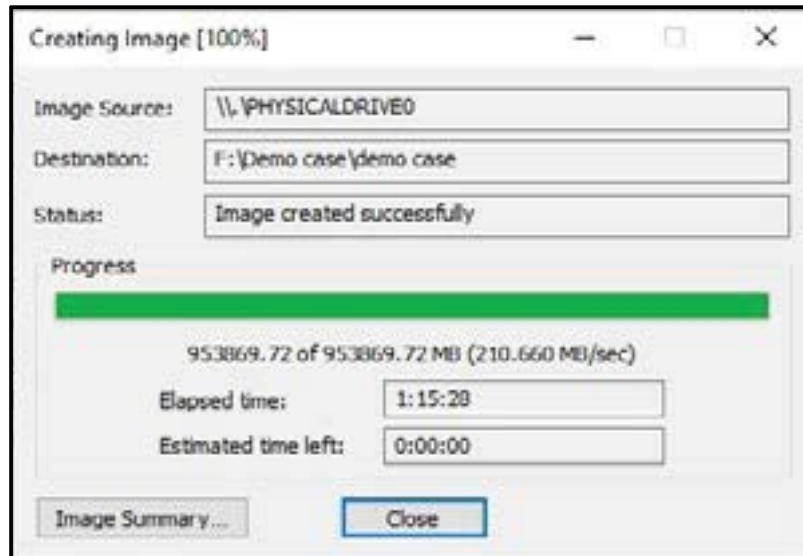


Figure 28: Image progress status.

Figure 29 shows the Image hash verification result.

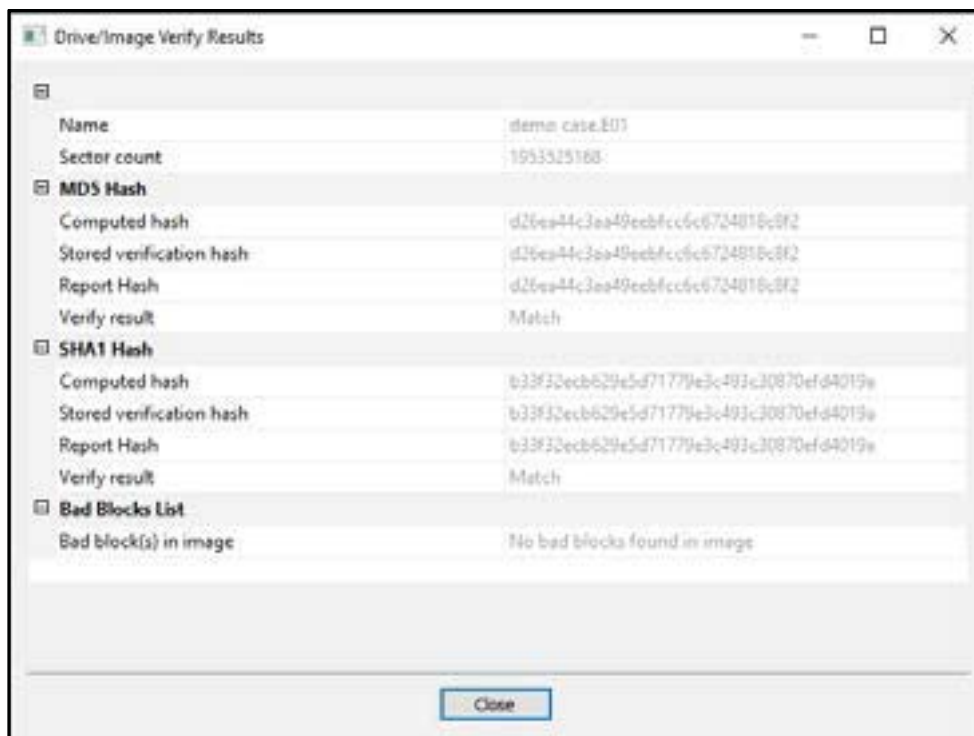


Figure 29: Image hash verification results.

After creating the image, the Investigation Team must verify the image file with the help of FTK

Imager as shown from Figures 30 to 32.

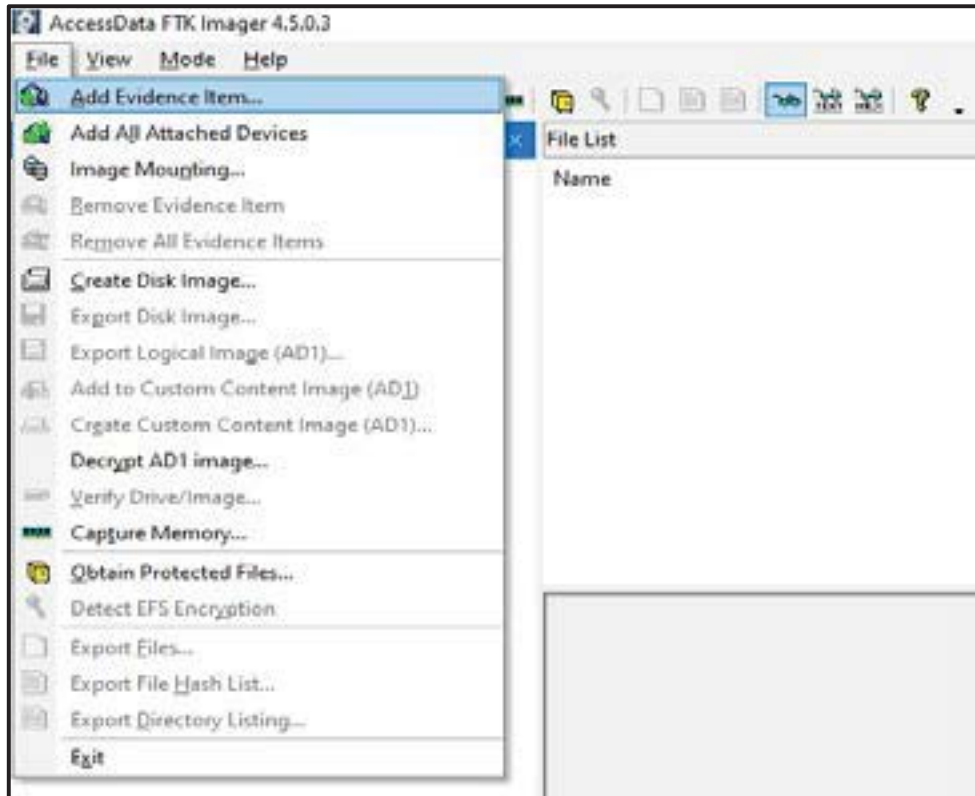


Figure 30: Add Evidence.

Next, select the image file.



Figure 31: Image file selection.

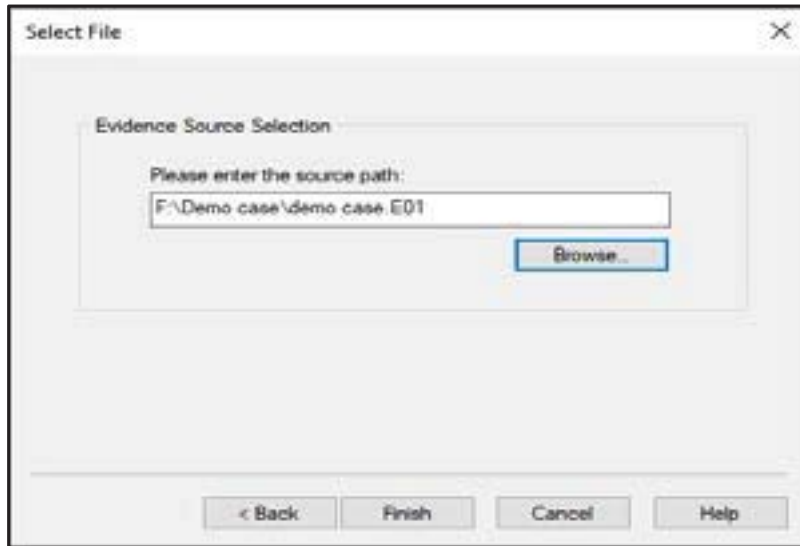


Figure 32: Browse image file.

After adding the image in the FTK imager, see all the partitions along with the Root Folder as shown in Figure 33, hence the evidence image file can be viewed without any bit locker decryption key.

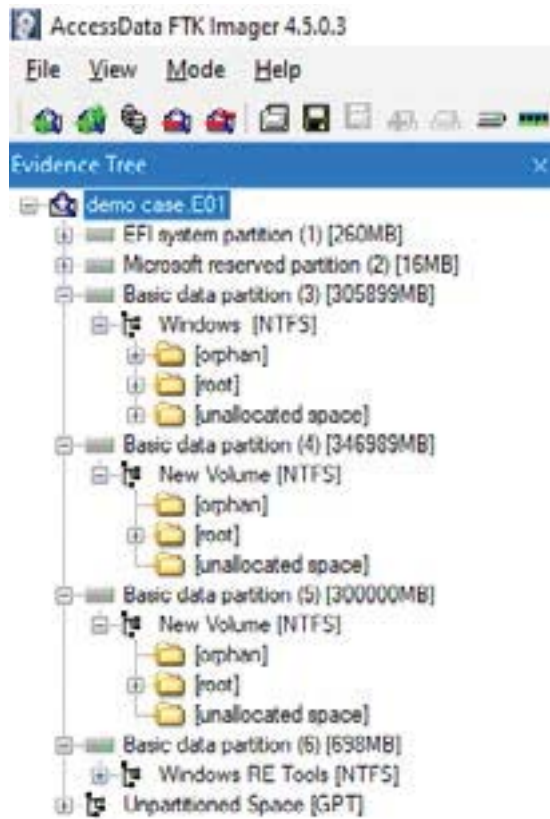
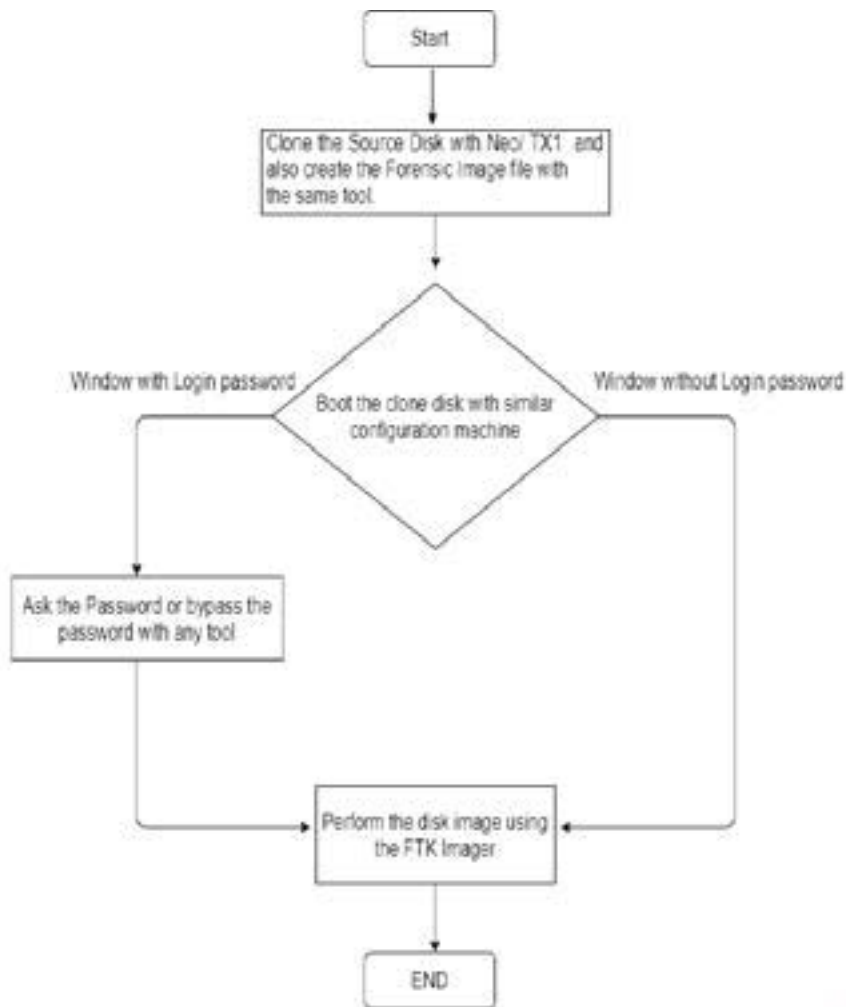


Figure 33: Evidence image preview.

Scenario 5 - Computer system with MacAfee Endpoint Security



Note -

- I) Check whether the disk is enabled with bit locker encryption or not ? if disk is encrypted then Perform the steps of **Scenario 3**
- II) This method was tested on window 7 environment.
- III) Investigation officer make sure to maintain chain of custody form along with the all necessary form.

Flowchart 3: Detailed process for system acquisition with MacAfee Endpoint enabled.

Scenario 6 - Windows server with RAID Configuration

RAID stands for Redundant Array of Independent Disks. It's a bunch of hard drives, matching in capacity, size, speed and model, which are assembled and with the means of software or hardware or both, they may be configured for drive redundancy. In case, any of the drives fail, the data can still be recovered.

Since RAID servers have multiple hard disks and by combining all-disk drives, logical volumes are created, no disks should be removed from the server which is RAID enabled. The process to acquire the disk image in live mode is detailed in Flowchart 4.

- Step 1 - Estimate the source disk size along with the data size and select the appropriate destination disk for storing the server image file.
- Step 2 - Copy the disk imaging tool to the USB drive (Investigation Officer can use any Imaging tool either FTK Imager/Encase Imager)
- Step 3 - Insert the destination disk drive along with imaging tool USB drive into the server (make sure to connect in USB 3 for better speed. Using the USB 2.0 option, takes a longer time as compared to the USB 3)
- Step 4 - Launch the FTK Imager and click on create Disk Image as shown in the below Figure 34.

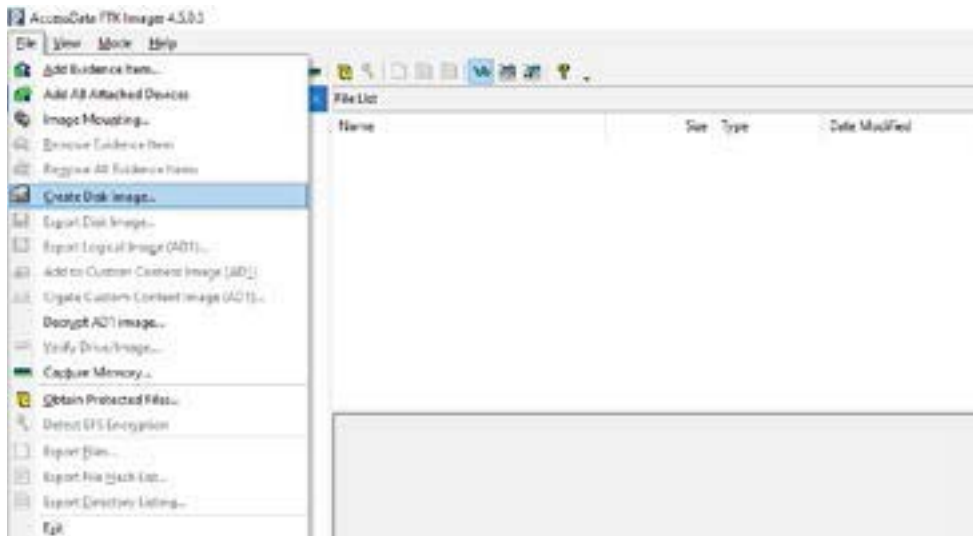


Figure 34: FTK imager creates disk image.

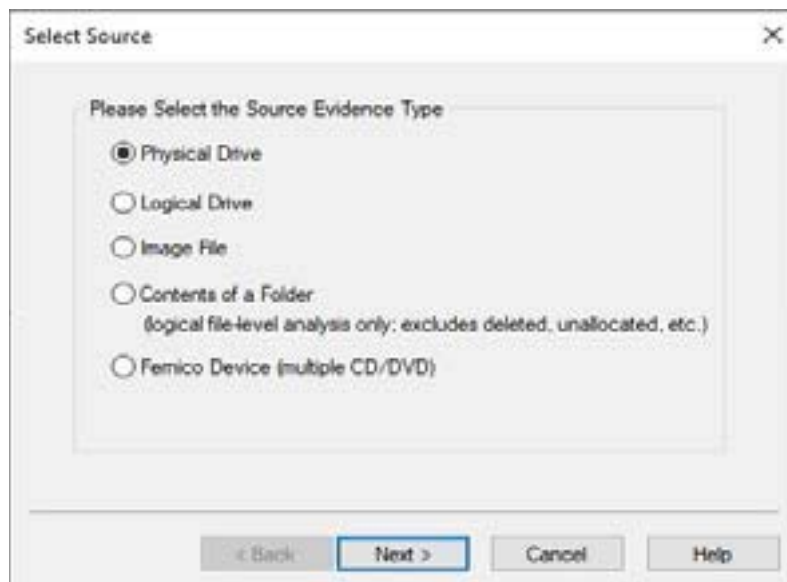


Figure 35: Evidence image preview. Step 5 – Select the Physical Drive option as shown in Figure 35.

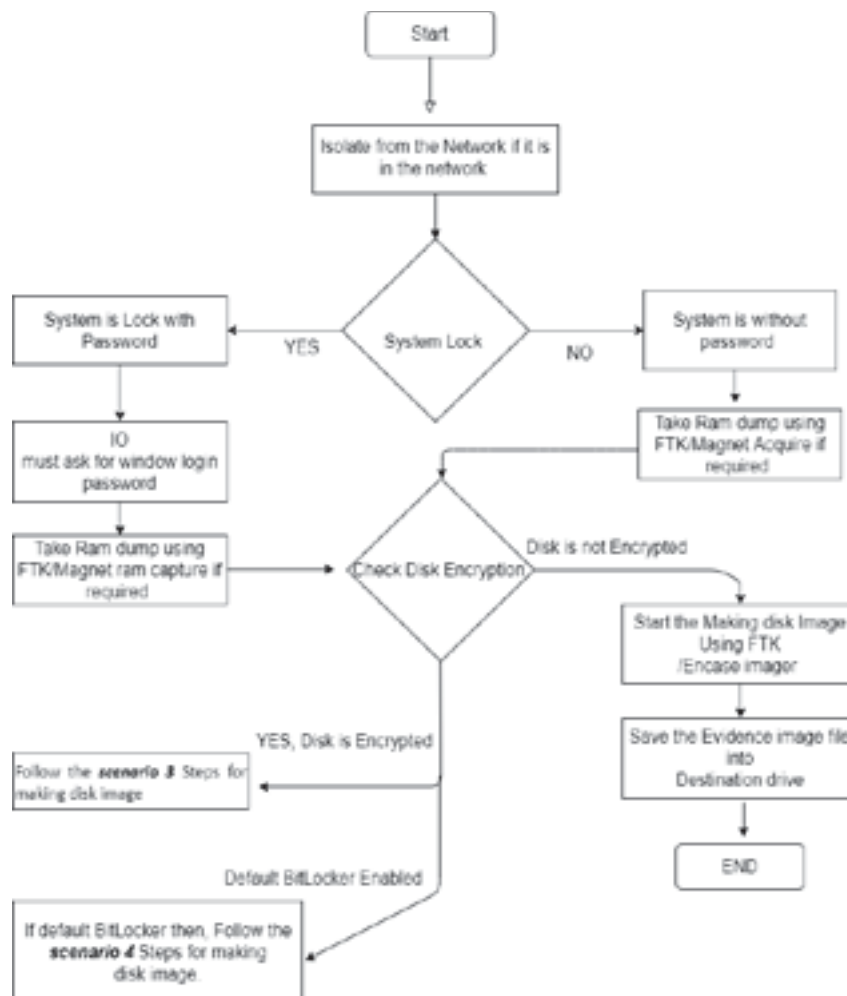
Step 6 - Select the source Hard Disk then select the E01 as image type.

Step 7 - Provide the case details such as Case Number, Evidence Number etc. and Image destination path where the Server image will be saved.

Step 8 - Give the name for the Image file to be created and click on the Finish button.

Note –

- Image processing is a time taking activity as it depends on the size of the hard disk, data size, type of hard disk, and USB type etc.
- In some cases, there is not enough time for acquiring the image file at the crime scene. Hence, in such scenarios, the Investigation officer can acquire relevant files only.
- During the acquisition, the Investigation officer must maintain the chain of custody, Digital evidence collection form and form 65b.



Flowchart 4: Detailed process for RAID system acquisition – Power ON Stage.

2.3. 2 Mac system

Step 1- PRE-SEARCH INTELLIGENCE

Find out as much as you can about your target:

- Number and types of Macs (MacBook, iMac or Mac Pro).
- Operating System Version (for collecting/processing volatile data and Copy Over Procedure).
- Type/s and the number of ports.
- Does it contain a T2 chipset with Secure Boot?
- Is File Vault Active?
- Can passwords be obtained

Step 2 - ISOLATE

Assign one trained Digital Evidence Collection Specialist to handle the electronic evidence to minimize contamination and the Chain of Custody. Prohibit anyone else from handling the devices.

Step 3-ALWAYS ASK FOR THE PASSWORD

Most newer Macs have enhanced security features such as T2 Security Chipsets, APFS File Systems, Secure Boot, File Vault and more. Anyone or a combination of these security features can stop you from getting the data. ALWAYS ASK FOR THE PASSWORD.

STEP-4: IF COMPUTER IS ON - LOCK SCREEN ACTIVE Options are:

- Ask for the Password - Confirm the password and proceed to Step-6.
- Restart to Image RAM - Connect a RAM Imaging Utility to the Mac such as

RECON IMAGER. Conduct a soft-restart (do not power off if possible and image the RAM).

****Note - This will not work with Macs with T2 Chipsets with Secure Boot enabled.****

STEP-5: COMPUTER IS OFF

Collect the computer using best practices for the collection of electronic evidence. Prepare for imaging (refer to Step-12).

STEP-6:

COMPUTER IS ON - DESKTOP IS ASSESSABLE - LOOK FOR DESTRUCTIVE PROCESSES

Look for signs of destructive processes such as wiping utilities, erasing free space, etc. If destructive processes are running, options are:• Attempt to stop the destructive process. Use Force Quit, if possible (Command + Option/Alt + Esc keyboard combo).

STEP-7:

COMPUTER IS ON - DESKTOP IS ASSESSABLE - COLLECT VOLATILE INFORMATION using a trusted and validated tool (not the source computer's tools)

Collect Volatile Data such as running processes, network connections, and unsaved documents.

RECON ITR has automated Volatile Data collection features.

STEP-8:

COMPUTER IS ON - DESKTOP IS ASSESSABLE - CHECK FOR HIDDEN DESKTOPS OR RUNNING VIRTUAL MACHINES

Check for running virtual machines and open files on other desktops

(macOS supports up to 16).

If a Virtual Machine is found running use the VM software to "Save a snapshot"

(keep in mind they will create a new file or could overwrite an existing snapshot).

Treat the VM as a new computer follow the best practices for responding to a live system for that OS.

STEP-9:

COMPUTER IS ON - DESKTOP IS ASSESSABLE - CHECK FOR ENCRYPTION

When the user is logged in, data on any mounted encrypted volumes are accessible.

Check to see if any of the mounted volumes are encrypted (Command + I). If encrypted, copy the data from the encrypted volumes to an HFS formatted volume to preserve metadata (can use "rsync" command) or Live Imaging built into RECON ITR.

Using System Preferences -> Security and Privacy -> FileVault, check to see if FileVault is ON or OFF. If found ON, copy the data from the encrypted home directory to an HFS formatted volume to preserve metadata.

RECON ITR includes Live Imaging and Triage tools to assist with this

STEP-10: COMPUTER IS ON - DESKTOP IS ASSESSABLE - IMAGE RAM

Image RAM using a tool that supports the running macOS version such as RECON ITR.

****Special Note - imaging Mac RAM can sometimes cause a kernel panic and requires the admin password. Make sure that you image Mac RAM last.****

STEP-11: COMPUTER IS ON - DESKTOP IS ASSESSABLE - SHUTDOWN

Once you have completed collecting your data, perform a hard or soft shutdown (unless you are restarting to image Mac RAM with the bootable version of RECON ITR).

STEP-12: OBTAINING SYSTEM DATE AND TIME With the system OFF,

power on the system holding down the Option/ALT key to check for the presence of a Firmware Password (boot level password). If you do not see a lock, power off the system by holding down the power key.

If the Mac does not contain a T2 Chipset, power on the system again this time holding the (Command + S) keys. Once you see text, you can let go. This is a Single User Mode.

If the Mac does contain a T2 Chipset you will need the password to enter Single User Mode. At the command prompt type: date Power off the system by holding down the power key until the system turns off.

STEP-13: IMAGING macOS Extended (RECON IMAGER included with RECON ITR)

Image the Mac by booting to RECON ITR USB. RECON ITR automatically interprets the Core Storage volume. Depending on your case you can create an image of the physical disks, individual volumes or the derived Core Storage Volume.

- DMG format - .dmg is recommended for mounting and processing on a Mac natively. The .dmg image made by RECON IMAGER is also a RAW image that can be imported into any forensic tool.

STEP-14: IMAGING - FUSION DRIVE RECON IMAGER included with RECON ITR)

Fusion Drives are seen by most tools as two separate drives (usually a combination of an SSD, spinning hard disk or an additional SSD).

RECON ITR will automatically interpret any synthesized file systems properly which are derived from the two individual disk volumes.

STEP-15:**IMAGING (PALADIN)**

Image the Mac using PALADIN (non-T2 Chipset Mac).

- DMG format - .dmg is recommended for mounting and processing on a Mac natively. The .dmg image made by PALADIN is also a RAW image that can be imported into any forensic tool.

Step 16 - IMAGING - FUSION DRIVE (PALADIN)

Fusion Drives are seen by most tools as two separate drives (usually a combination of an SSD, spinning hard disk or an additional SSD). Create an Image of both drives individually using PALADIN using a .dmg format.

These images can be recombined on a Mac into a single volume. Remember to mount the SSD drive first.

RECON LAB can automatically recombine Fusion drives that have been imaged separately.

STEP-17:

IMAGING - MACS WITH T2 CHIPSET AND SECURE BOOT ENABLED

Newer Macs with T2 security chipsets have secure Boot enabled preventing booting from any external devices.

To image Mac with Secure Boot enabled put the source Mac into Target Disk Mode by holding down the “T” key on start-up.

Connect the source Mac to your forensic computer with the proper cable (ex. Thunderbolt) and boot your forensic computer with RECON ITR to image.

Additionally, you can use RECON ITR running from the examiner’s Mac live. Use RECON ITR’s Disk Manager to disable Disk Arbitration, connect the source Mac in Target Disk Mode, open RECON IMAGER to create an image.

Optionally, if you know the password, you can enter the Mac’s Recovery Mode and disable the Secure Boot and Booting from External Media to allow booting. Image the source Mac with the bootable version of RECON ITR.

2.3.3 Linux System

Scenario 1 – The Computer system is in an ON state.

Step 1 - The Investigation Officer must check the system carefully at the crime scene. If it is in the network, then disconnect immediately.

Step 2 - Open the terminal and type the following command as shown in Figure 36.

A screenshot of a Linux terminal window. The prompt is 'ncric@ubuntu: ~'. The command 'sudo fdisk -l' has been entered and is followed by a cursor. The terminal background is dark with light-colored text.

Figure 36: Linux terminal.

For checking the source disk size and accordingly attaching the external disk for storing the image file as shown in Figure 37.

```

ncric@ubuntu:~$ lsblk
Disk /dev/sda: 50 GiB, 53687091200 bytes, 104857600 sectors
units: sectors of 1 = 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x5eb725f9

Device      Boot      Start        End    Sectors  Size Id Type
/dev/sda1   *                2048 100665343 100663295  48G 83 Linux
/dev/sda2                100667390 104855551  4188162    2G  5 Extended
/dev/sda5                100667392 104855551  4188160    2G  B2 Linux swap / Solaris

Disk /dev/sdb: 1.8 TiB, 2000398933504 bytes, 3907029167 sectors
units: sectors of 1 = 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 33553920 bytes
Disklabel type: dos
Disk identifier: 0x17fa3c00

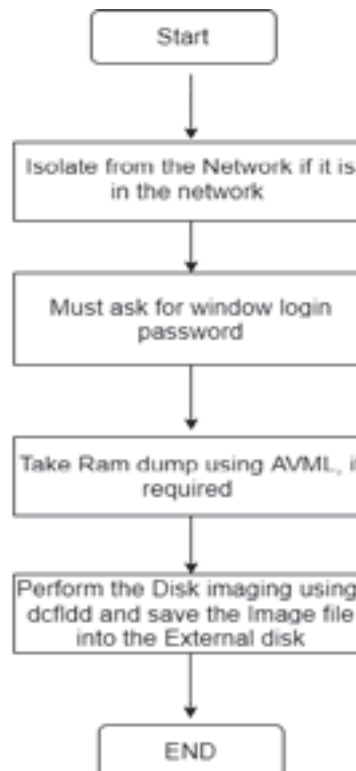
Device      Boot      Start        End    Sectors  Size Id Type
/dev/sdb1   *                64 3907024128 3907024065  1.8T  7 HPFS/NTFS/exFAT
ncric@ubuntu:~$

```

Figure 37: Attached hard disk information.

Source hard disk is indicated in white mark and destination hard disk marked yellow as shown in the above Figure.

Step 3 - Change directory (provided the external disk location where the image will be saved) and use the `dcfldd` command for making the disk image.



Flowchart 5: Detailed process for Linux system acquisition – Power ON Stage.

Note -

- ✓ Always take the larger disk as Destination Disk when compared to the source disk (For example - if the source disk size is 500 GB then destination disk size must be 1 TB).
- ✓ Ask the Root password for performing the disk imaging activity.
- ✓ If the disk imaging process takes longer than usual time there may be various factors resulting in it such as hard disk condition, hard disk speed, data size.
- ✓ For demonstration purpose, using the dcfldd command instance of dd because dcfldd is an enhanced version of dd with features useful for forensics and security.
- ✓ In case of RAID disks, perform the partition wise image creation with the help of dcfldd command.
- ✓ (dcfldd --h) is a command used for help purpose. There are some parameters for the same and the Investigation Officer can select the desired parameters as per the requirement.

| | | |
|-------------|-----|---|
| if | = > | input file |
| /dev/sdb | = > | source /suspect drive (whole disk) |
| hash | = > | Definition of hash algorithms |
| hashwindows | = > | Will hash data chunks of 2 GB |
| md5log | = > | Saves all md5 hashes in a file called md5.txt |
| sha256log | = > | Saves all sha hashes in a file called sha256.txt |
| hashconv | = > | Hashing AFTER or BEFORE the conversion |
| bs | = > | block size (default is 512) |
| 4k | = > | block size of 4 kilobyte |
| conv | = > | conversion |
| noerror | = > | will continue even with read errors |
| sync | = > | if there is an error, NULL fill the rest of the block |
| split | = > | Split image file in chunks of 2 GB |
| splitformat | = > | the file extension format for split operation |
| of | = > | output file sdb_image.img => name of the image file |
| log | = > | Path of the log file |

progress

= >

view progress of acquisition

- ✓ During this process, the Investigation Team must fill the Chain of custody form and mention all the commands and tool names that have been used to create the disk image.
- ✓ Root Password along with the other credential if any, also must be mentioned in the Chain of custody.
- ✓ For demonstration in the above snapshots, we have used Ubuntu 16 along with VMware player.

Scenario 2 - Computer system in Powered Off stage

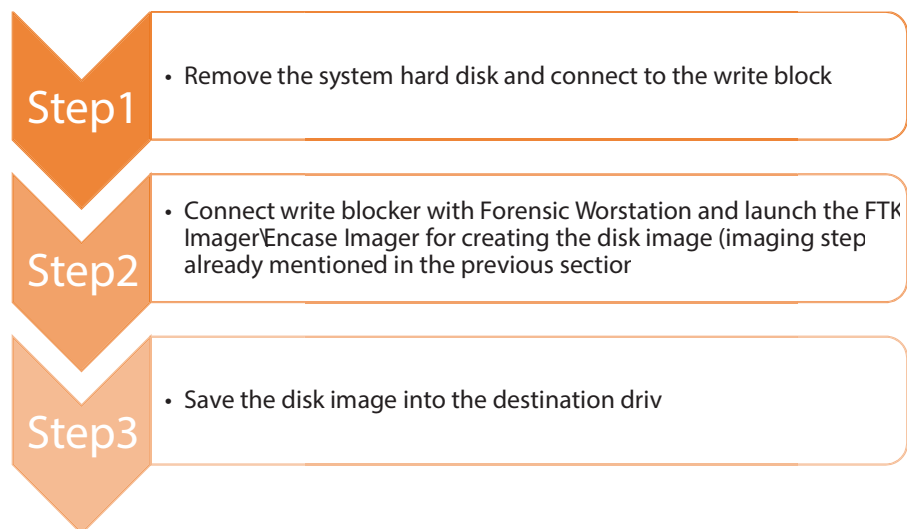


Figure 39: Steps for Linux machine acquisition.

Note –

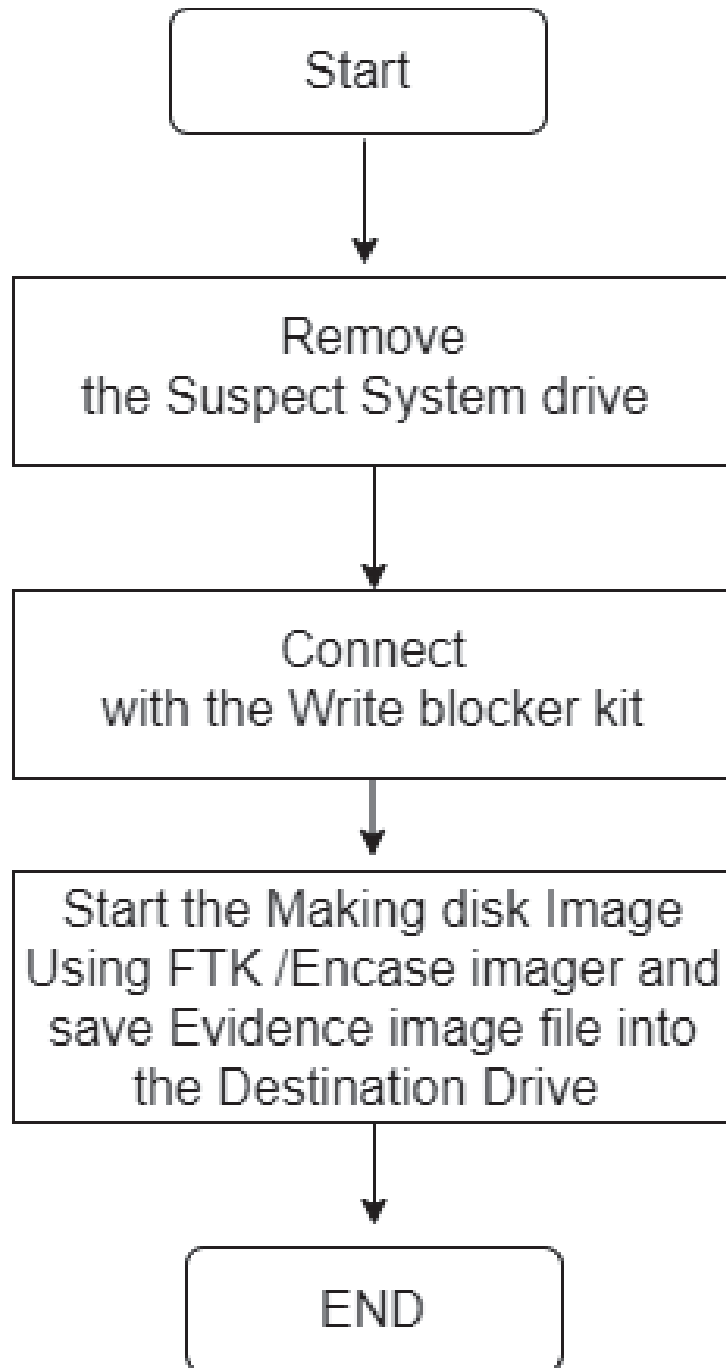
- ✓ In Figure 39, when the system is in Powered Off mode, the Investigation Officer may use Logicube Forensic Neo, Tableau TX1, Tableau TD2U, hardware devices for creating the disk images.
- ✓ If IO doesn't have the above mentioned tools, then they may use other alternatives such as PALADIN EDGE, Parrot OS, Kali Linux.

Link for downloading these Tools are as follows –

<https://sumuri.com/product/paladin-edge-64-bit/>

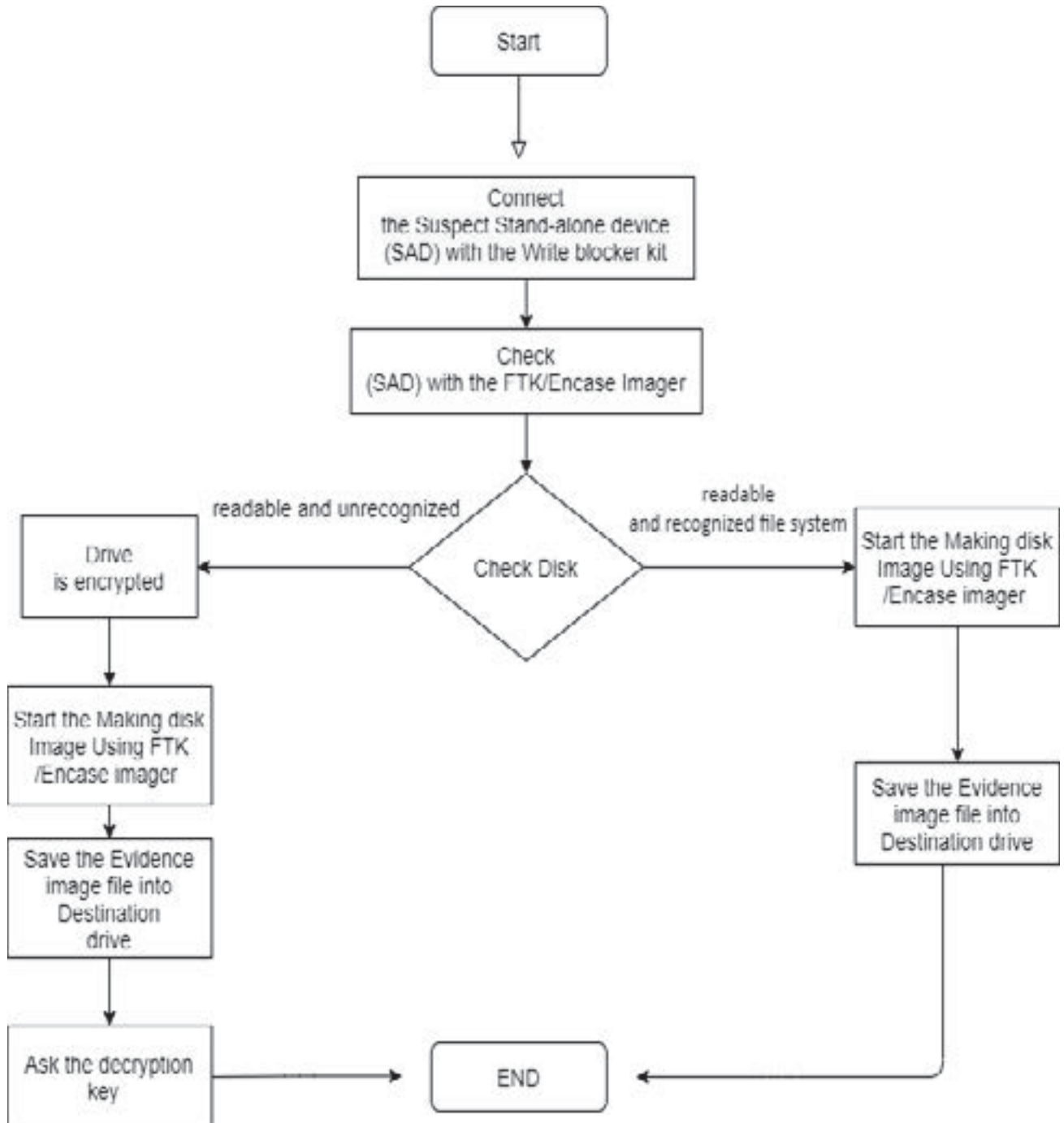
<https://www.parrotsec.org/download/>

<https://www.kali.org/downloads/>



Flowchart 6: Detailed process for Linux system acquisition – Power OFF Stage.

2.3.4 Stand Alone Storage device – At the Crime scene, standalone storage devices such as Memory cards, Pen-drives, USB devices can be found and are very relevant. Following are the steps for the Forensic imaging of these standalone devices.



Flowchart 7: Detailed process for SAD acquisition.

3. Packaging and transport of Electronic Evidence

Digital evidence and the computers and electronic devices on which it is stored are fragile and sensitive to parameters such as Temperature, Moisture, Physical fright, Static electricity, and Magnetic fields.

Hence, the Investigation officer must take precautions when documenting, photographing, packaging, transporting, and storing digital evidence to avoid altering, damaging, or destruction of the electronic data.

When packaging digital evidence for transportation, the Investigation officer must follow below steps:

Table 2: Steps for the Packaging process.

| | |
|---------------------|--|
| Packaging process - | 1. Ensure that all digital evidence collected is properly documented, labelled, marked and photographed before i packaged. |
| | 2.Pack all the digital evidences in antistatic wrapping |
| | 3.Plastic equipment should not be used when gathering digi evidence since plastic can generate static electricity and l moisture and condensation to develop which may spoil or destr the evidence |
| | 4.Make sure that all digital evidence is tied together in a way s that it averts them from being turned, dented, or otherwi deformed |
| | 5.Label all containers used to package and store digital evidenc clearly and properly gather all power supply cables and adapte of all the electronic devices seized |

When transporting digital evidence, the Investigation Officer should follow the below steps:

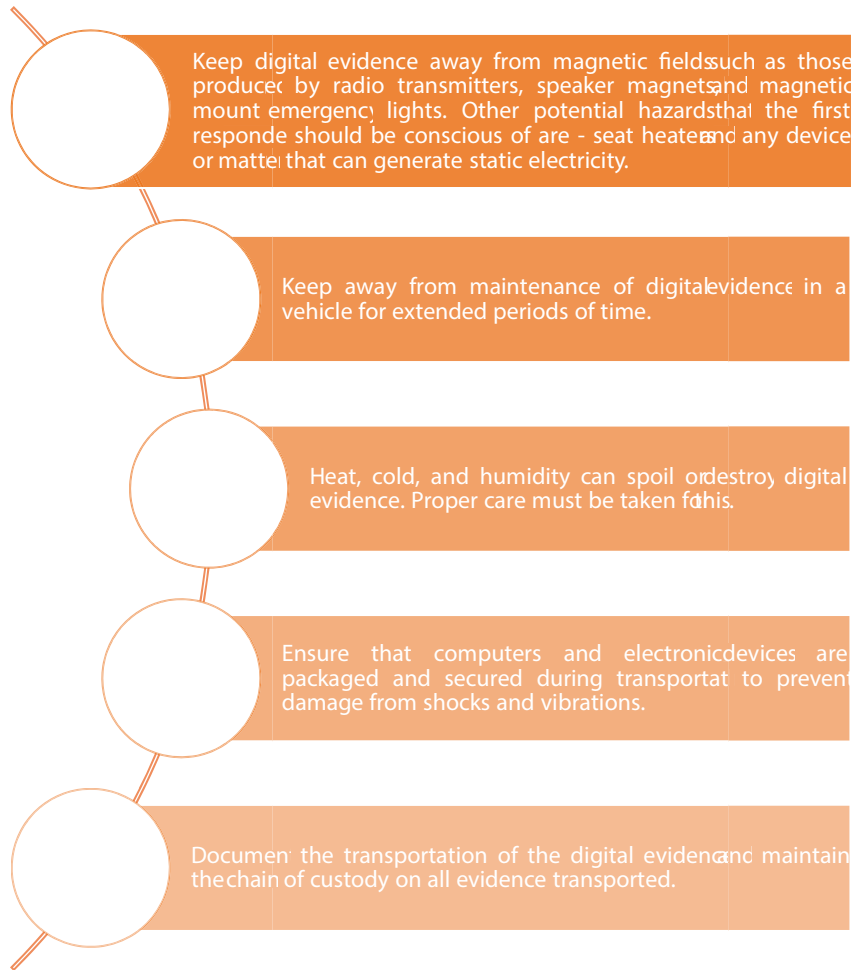


Figure 40: Steps during the transport evidence.

Storage Procedures

When storing digital evidence, the investigating officer should —

- ✓ Ensure that the digital evidence is stored in a secure, climate-controlled atmosphere or a place that is not subject to great temperature or humidity.
- ✓ Ensure that the digital evidence is not exposed to magnetic fields, moisture, dust, vibration, or any other elements that may spoil or ruin it.

If more than one computer system are detained as evidence, all computers, cables, and devices linked to them should be appropriately labelled to enable possible reassembly if necessary.

Subsequently seized computers can be labelled in alphabetical order. The corresponding connections and cables can be labelled with the letter designation for the computer and a unique number to ensure proper reassembly.

The role of electronic devices as evidence has become so important that an effective law enforcement officer can't complete his/her investigation without them. From a common phishing fraud to even a murder and nearly everything in between, all such crimes include some or the other form of involvement of electronic devices, which can be utilised by LEAs in investigating the crime scene. Though the ideal scenario demands that the investigation team should have a well trained professional forensic specialist, the luxury is not available to everyone. In such cases LEAs themselves have to handle the acquisition of electronic devices from crime scene for intelligence/evidence gathering. Any investigation officer who may follow the steps provided in this manual should be able to successfully acquire electronic evidence.

Summary–

The data acquisition process for different operating system flavours such as Windows, Linux and MAC systems have been described in detail with various scenarios throughout the document.

During the image acquisition phase, the procedures demonstrated above for the collection of evidence from the computer systems FTK imager has been used throughout the document.

Linux testing environment was set up with the help of VMWare Player and Forensic imaging has been performed using the 'DCFLDD' command in this document. The testing environment has been configured based on the scenarios conducted in Chapter 2.

The research resulted in the observation that, the default bit locker is not that big a challenge for the LEAs. This booklet will guide across all challenging scenarios along with practical demonstrations (See Chapter 2).

References–

- ✓ <https://sumuri.com/mac-forensics-best-practices-guide/>
- ✓ <https://www.servercase.co.uk/blog/article/tech-help---raid---what-is-it-and-how-does-it-work/>
- ✓ http://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/forensic_science/16._digital_forensics/33._digital_crime_scene_investigation/et/6317_et_6317_et_et.pdf
- ✓ <https://caseguard.com/articles/proper-handling-of-electronic-evidence/>
- ✓ <https://whatis.techtarget.com/definition/memory-dump#:~:text=A%20memory%20dump%20is%20the,it%20to%20a%20storage%20drive.&text=Memory%20dumps%20save%20data%20that,error%20in%20Microsoft%20operating%20systems.>
- ✓ <https://community.windows.com/en-us/stories/what-is-bitlocker-windows-10>
- ✓ <https://www.redhat.com/en/topics/virtualization/what-is-a-virtual-machine>
- ✓ <https://www.solarwindssp.com/blog/cloning-vs-imaging#:~:text=Once%20the%20process%20of%20cloning,placing%20it%20on%20another%20drive.>
- ✓ <https://capsicumgroup.com/2-key-differences-between-digital-forensic-imaging-and-digital-forensic-clone-and-how-they-can-affect-your-legal-case/>
- ✓ <http://www.cyber-forensics.ch/acquiring-data-with-dd-dcfldd-dc3dd/>
- ✓ <https://www.forensics-matters.com/2020/10/20/simple-forensics-imaging-with-dd-dc3dd-dcfldd/>
- ✓ https://www.google.com/url?sa=i&url=https%3A%2F%2Fresources.infosecinstitute.com%2Ftopic%2Fcomputer-forensics-tools%2F&psig=AOvVaw3q9_AzKLzFQf0l4dTxu9tu&ust=1618030589387000&source=images&cd=vfe&ved=2ahUKEwjgrPlr_DvAhXwhXIEHeagBIYQjRx6BAgAEAc
- ✓ Investigative Workflow Manual on Cyber Harassment Cases- I4C, BPR&D
- ✓ https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D8HTPTtEfChA&psig=AOvVaw1g3DPKO745aC5mpuAMHWDx&ust=1618491543466000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCNCyjKzl_e8CFQAAAAAdAAAAABAF



officialBPRDIndia



BPRDIndia



Bureau of Police Research & Development India



bprdIndia



www.bprd.nic.in



Cyberdost



www.cybercrime.gov.in



**NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)
BUREAU OF POLICE RESEARCH AND DEVELOPMENT**

Ministry of Home Affairs, Government of India
NH-8, Mahipalpur, New Delhi-110037