|  |
| --- |
| **INTEGRATED USB TOOLKIT FOR DIGITAL FORENSICS**      A project report submitted to the Bharathiar University in the partial fulfilment  of the requirements for the award of the degree of    **B.Sc., DIGITAL AND CYBER FORENSIC SCIENCE**  Submitted by  **X. JOHN BOSCO ANTONY**  **(Reg.No 2128A0021)**    Under the guidance of  **Mr.A. KAMALRAJ M.C.A., (Ph.D).,**  (Assistant Professor & Head, Department of Digital and Cyber Forensic Science)    **DEPARTMENT OF DIGITAL AND CYBER FORENSIC SCIENCE**  **AJK COLLEGE OF ARTS AND SCIENCE**  (Affiliated to Bharathiar University, Re-Accredited with A+ Grade by NAAC)    **NAVAKKARAI, COIMBATORE – 641 105.**  **MARCH 2024** |
| **INTEGRATED USB TOOLKIT FOR DIGITAL FORENSICS**    A project report submitted to the Bharathiar University in the partial fulfilment  of the requirements for the award of the degree of    **B.Sc., DIGITAL AND CYBER FORENSIC SCIENCE**  Submitted by  **X. JOHN BOSCO ANTONY**  **(Reg.No 2128A0021)**    Under the guidance of  **Mr.A. KAMALRAJ M.C.A., (Ph.D).,**  (Assistant Professor& Head, Department of Digital and Cyber Forensic Science)        **DEPARTMENT OF DIGITAL AND CYBER FORENSIC SCIENCE**  **AJK COLLEGE OF ARTS AND SCIENCE**  (Affiliated to Bharathiar University, Re-Accredited with A+ Grade by NAAC)    **NAVAKKARAI, COIMBATORE – 641 105.**  **MARCH 2024** |

# PROJECT WORK

**INTEGRATED USB TOOLKIT FOR DIGITAL FORENSICS**

Bonafide Work Done by

**X. JOHN BOSCO ANTONY**

**(Reg.No.2128A0021)**

The project submitted in partial fulfilment of the requirements for the award of **BSc** .,**Digital and Cyber Forensic Science**, of Bharathiar University, Coimbatore – 641 046



**GUIDE HEAD OF THE DEPARTMENT**

**Submitted for the Viva-Voce Examination held on**

**INTERNAL EXAMINER**      **EXTERNAL EXAMINER**

**MARCH 2024**

# DECLARATION

## DECLARATION

I, **JOHN BOSCO ANTONY X (2128A0021)** hereby declare that the project entitled **“INTEGRATED USB TOOLKIT FOR DIGITAL FORENSICS ”** is my project work carried out during the second year B.Sc., Digital and Cyber Forensic Science at AJK College of Arts and Science, Coimbatore, under the guidance of **Mr.A. KAMALRAJ M.C.A., (Ph.D).,**  Assistant professor & Head, Department of Digital and Cyber Forensic science, AJK College of Arts and Science, and has not submitted previously for the award of any other degree or diploma by me to any institution or university ac-cording to the best of my knowledge.

**SIGNATURE OF THE CANDIDATE**

**Place:** Coimbatore

**Date:**

# ACKNOWLEDGEMENT

## ACKNOWLEDGEMENT

I express my sincere thanks to all those who have provided us valuable guidance towards

the completion of this system as part of the syllabus of the Second Year BSc Digital and Cyber

Forensic Science Course.

I am deeply indebted to my guide **Mr.A. KAMALRAJ M.C.A., (Ph. D).,** Assistant Professor & Head, Department of Digital and Cyber Forensic Science, for making available his intimate knowledge and experience in making **“INTEGRATED USB TOOLKIT FOR DIGITAL FORENSICS”.**

I am deeply thank to **Mr.A. KAMALRAJ M.C.A.,(Ph.D).,** Head of the Department, Department of Digital and Cyber Forensic Science for his effective guidance and constant encouragement, which let this information work to its successful completion.

I extend my gratitude to **Dr. S. RAJU M.Sc., MBA., Ph.D.,** Principal, AJK College of Arts and Science, whose primary aim is to establish and promote educational institutions of excellence and eminence in all fields so as to initiate and equip the youth with the originality of thinking, selfreliance and technological expertise.

I strive to the almost of my sincerity to repay a millionth of my indebtedness with profound gratitude by acknowledging the inestimable support and extensive guidance by our management members, **AJK College of Arts and Science**, whose dedicated care has come down a long way not only in competing support and venture but also in making our dreams into reality.

I would like to express my heartfelt thanks to my parents for their blessings, my dear friends, classmates and all faculties for their help and wishes for the successful completion of this project.

## CONTENTS

|  |  |  |
| --- | --- | --- |
| **S.NO** | **TITLE** | **PAGE No** |
|  | **SYNOPSIS** |  |
| **1** | **INTRODUCTION** |  |
|  | 1.1 About the Project |  |
| **2** | **SYSTEM STUDY AND ANALYSIS** |  |
|  | 2.1 Proposed System |  |
|  | 2.1.1 Advantages of the Proposed System |  |
| **3** | **SYSTEM CONFIGURATION** |  |
|  | 3.1 Hardware Configuration |  |
|  | 3.2 Software Configuration |  |
|  | 3.2.1. Static Analysis tool |  |
|  | 3.2.2. Dynamic Analysis tool |  |
|  | 3.2.3. Operating system |  |
| **4** | **SYSTEM TESTING AND IMPLEMENTATION** |  |
| **5** | **CONCLUSION** |  |
| **6** | **FURTHER SCOPE OF THE PROJECT** |  |
| **7** | **BIBILIOGRAPHY** |  |
| **8** | **APPENDIX** |  |
|  | 8.1 Project Design |  |
|  | 8.2.1 Extract Coding |  |
|  | 8.3.1Report |  |

# SYNOPSIS

## SYNOPSIS

The objective of the project is **“INTEGRATED USB TOOLKIT FOR DIGITAL FORENSICS”** aims to offer a comprehensive software package that is simple to use and in-corporates many of the tools and capabilities required to conduct digital forensics investigations.

This project is aimed to create an integrated toolkit for digital forensics designed for the Linux operating system.

The proposed system of the project is to create a portable Forensics Toolkit compatible with Linux and housed in a USB device. This system simplifies digital investigations with a user-friendly interface, allowing investigators to swiftly select and execute various tools.

This project consists of four modules. The first module is **Tool launcher** is to makes it possible for investigators to choose and use digital forensics tools with ease, improving accessibility. The second module is **Forensic tool** collection contains a wide range of forensics tools in the USB toolkit, providing a complete answer for many investigation requirements. The third module is **Auto run** streamlines forensic analysis by automating predefined tasks upon USB insertion. The fourth module is **Reporting** which simplifies the creation of reports by using standardized templates to communicate forensic results in an efficient manner.

# INTRODUCTION

1. **INTRODUCTION**

The objective of the project is **“INTEGRATED USB TOOLKIT FOR DIGITAL FORENSICS”** aims to offer a comprehensive software package that is simple to use and in-corporates many of the tools and capabilities required to conduct digital forensics investigations.

The Integrated USB Toolkit for Digital Forensics aims to provide forensic investigators and cybersecurity professionals with a comprehensive suite of tools and techniques specifically tailored for the analysis of USB devices.

* 1. **ABOUT THE PROJECT**

The Integrated USB Toolkit for Digital Forensics represents a comprehensive solution for streamlining the investigation process of USB devices. By integrating automated identification, data extraction, malware detection, and timeline reconstruction capabilities, this toolkit empowers forensic professionals to efficiently collect and analyze evidence from USB drives.

Its user-friendly interface and robust feature set enable investigators to navigate the complexities of digital forensics with ease, ultimately enhancing the accuracy and speed of forensic examinations in both criminal and corporate investigations.

# SYSTEM STUDY AND ANALYSIS

**2.SYSTEM STUDY AND ANALYSIS**

**2.1 PROPOSED SYSTEM:**

The proposed system of the project is to create a portable Forensics Toolkit compatible with Linux and housed in a USB device. This system simplifies digital investigations with a user-friendly interface, allowing investigators to swiftly select and execute various tools.

This system aims to streamline the forensic examination process, enabling investigators to efficiently extract evidence from USB drives while maintaining data integrity and adhering to forensic best practices.

**2.1.1. Advantages of proposed system:**

**Efficiency and Time Saving:**

Automated device identification and data extraction streamline the investigation process. Reduces manual effort and accelerates the collection of evidence from USB devices.

**Enhanced Security:**

Malware detection and removal capabilities safeguard investigators' systems from potential threats. Protects against the risk of malware infection when analysing USB devices.

**Improved Analysis and Understanding:**

Timeline reconstruction feature aids in understanding the sequence of events related to USB device usage. Facilitates the reconstruction of digital scenarios, providing context to forensic findings.

**User-Friendly Interface and Accessibility:**

Intuitive design and user-friendly interface make the toolkit accessible to forensic professionals of varying expertise levels. Simplifies the navigation of complex forensic tools and techniques, allowing for efficient utilization by investigators.

# SYSTEM CONFIGURATION

## 3.SYSTEM CONFIGURATION

**3.1 HARDWARE CONFIGURATION**

* **3.1. Model:** Dell optiplex 5490 All in one
* **Processor:** Intel core i5 – 11500
* **Chipset:** Intel Q570
* **Memory:** 16GBDDR4
* **Network:** Integrated realtek Ethernet LAN 10/100/1000
* **Intel WI-FI** 6 AX201+Bluetooth 5.1
* **Hard Drive:** 512GB NVMe class 35 SSD
* **Chassis:** AIO – 13.54”\*21.26”\*2.07”
* **Display:** “23.8” FHD Non-Touch Anti-Glare
* **Keyboard:** Dell KB216 Wired Multimedia USB Keyboard  **Mouse:** Dell MS116 optical Mouse .

**3.2. SOFTWARE CONFIGURATION**

**Operating System:** Kali Linux Operating System

* + 1. **Operating System: Kali Linux Operating system**



Linux is a versatile and robust open-source operating system kernel renowned for its stability, security, and flexibility. Developed by Linus Torvalds in the early 1990s, Linux powers a wide array of computing devices, from servers and desktops to mobile devices and embedded systems.

Its modular design and customizable nature make it suitable for diverse applications, while its strong security model ensures data integrity and protection.

|  |  |
| --- | --- |
| **OS family** | Linux |
| **Source model** | open-source |
| **Initial release** | 13 march 2013 |
| **Latest release** | 23 August 2023 |
| **Platforms** | x86, x86-64, armel, armhf |
| **Kernel type** | Monolithic |
| **Official website** | [https:www.kali.org/](https://www.kali.org/) |

# SYSTEM TESTING AND IMPLEMENTATION

## 4.SYSTEM TESTING AND IMPLEMENTATION

## 

**FLASHING AN ISO FILE ONTO A USB DRIVE**

**Step 1:**

**I)Download the MX Linux ISO File:**

Obtain the MX Linux ISO file from the official MX Linux website or another trusted source.

**II)** **Download and Launch balenaEtcher:**

Get balenaEtcher from its official website and install it. Launch the application.

**III)Insert USB Drive:**

Plug in your USB drive into an available USB port.

**IV)Select MX Linux ISO File:**

In balena Etcher, click on "Flash from file" and select the MX Linux ISO file you downloaded.

**V)Flash to USB Drive:**

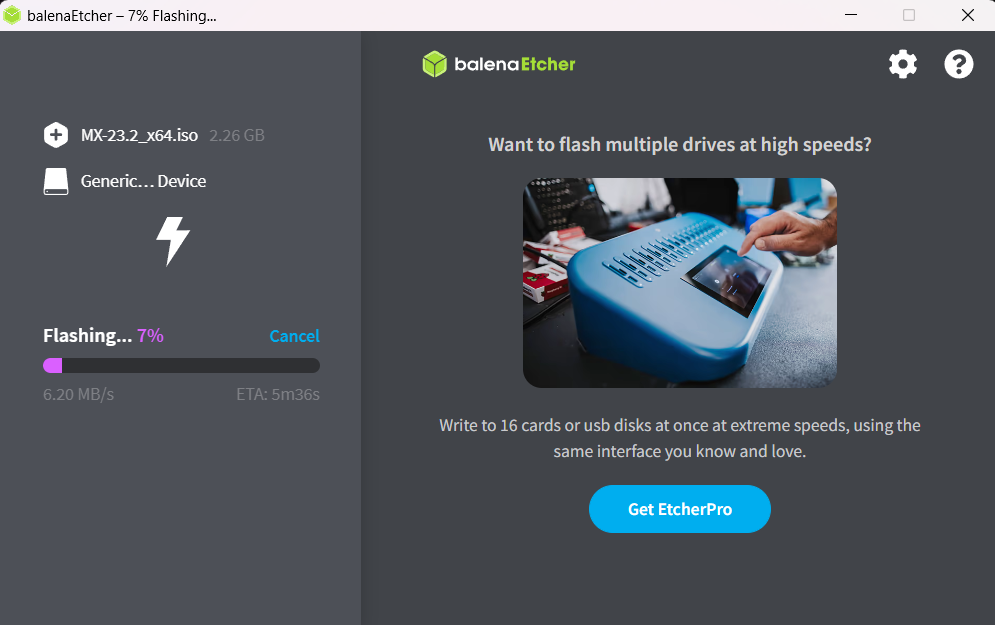
 Select your USB drive as the target, then click "Flash!" to start the process.

Fig4.1: Booting of Linux onto USB.

**Step 2:**

**Verify Flashing Process:**

Once balenaEtcher has finished flashing the MX Linux ISO file, it will display a "Flash Complete!" message. Verify that there are no errors reported during the flashing process.

**Eject USB Drive:**

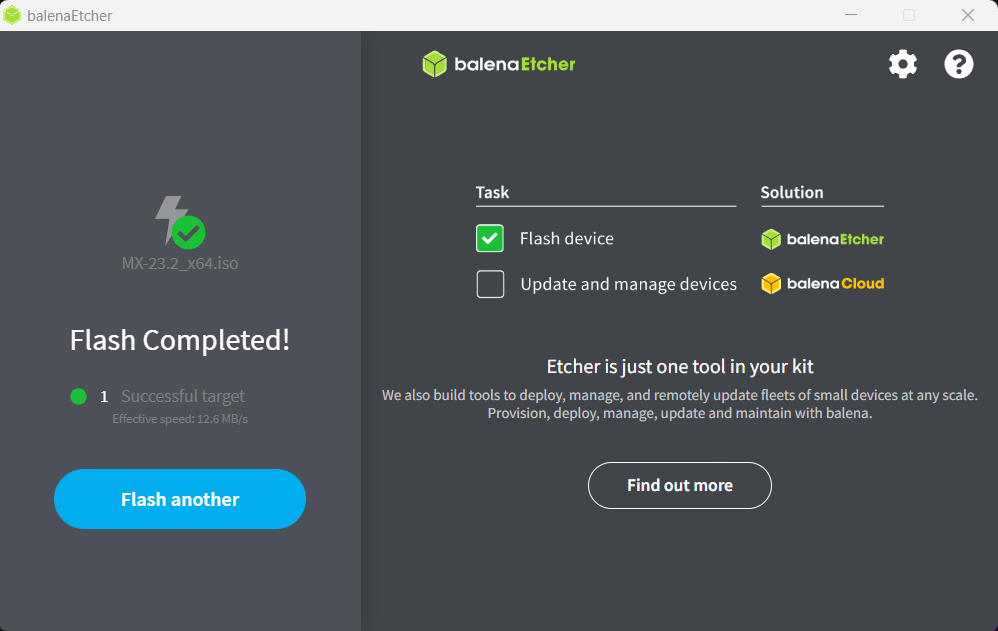
Safely eject the USB drive from your computer using the appropriate method for your operating system.

Fig4.2: The workspace of the Ghidra is opened.

**STEP 3: GUI Interface Overview: MX Linux**

The accessibility and simplicity of the interface, emphasizing its user-friendly design tailored to various skill levels.

Showcase the intuitive layout of the desktop environment, featuring familiar elements such as the applications menu, taskbar, and system tray.

****

Fig4.3: GUI of MX Linux

**STEP 4: Automated Network Scanning with Nmap on MX Linux:**

Automated network scanning with Nmap on MX Linux offers a powerful solution for discovering devices, services, and vulnerabilities within a network environment.

Begin by launching Nmap through the terminal or utilizing a graphical user interface (GUI) frontend for ease of use. Configure the scan parameters, including target IP addresses, scan types (such as SYN, UDP, or comprehensive scans), and desired output format.

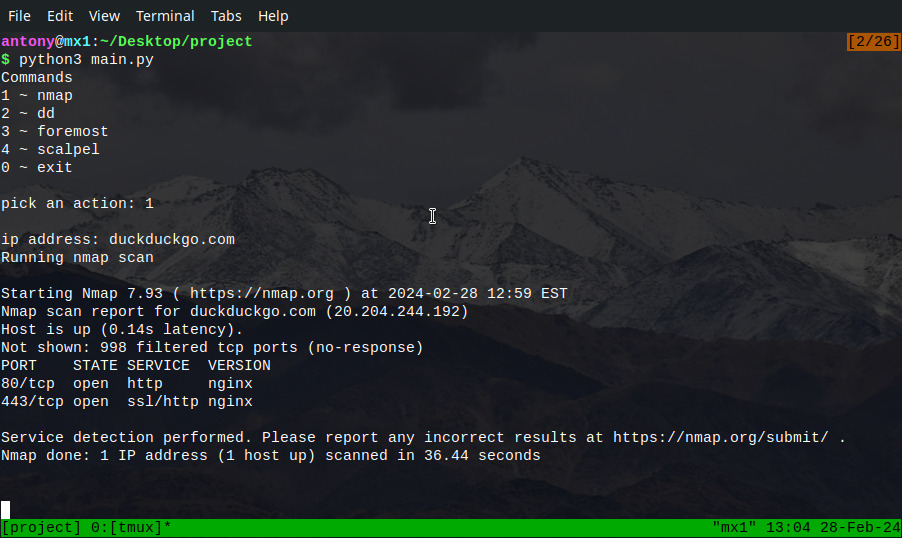


Fig4.4: Nmap automated Run.

**STEP 5: Analysing Nmap Scan Results in Text Format on MX Linux:**

To begin the analysis, users can open the text file using a text editor or terminal-based tools like grep, awk, or sed.

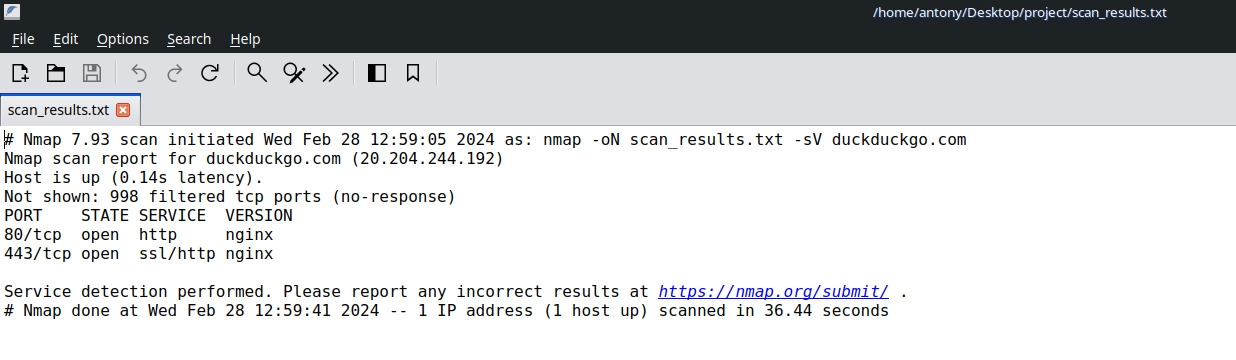
Within the file, each host and associated information are typically delineated, allowing for easy navigation and extraction of relevant data.

Fig4.5: Text results of nmap.

**STEP 6: Disk Cloning and Imaging with the dd Tool on MX Linux:**

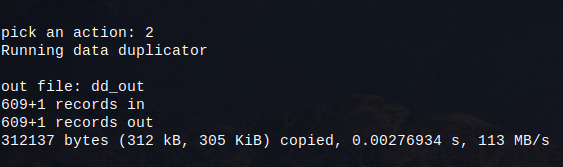
To initiate a disk cloning or imaging process, users launch the dd tool from the command line interface (CLI) of MX Linux. They specify the input source, typically denoted as the 'if' parameter, and the output destination, represented by the 'of' parameter. These parameters designate the source and target devices or files involved in the cloning or imaging operation.

Fig4.6:DD automated results.

**STEP 7: Data Recovery with Foremost Tool on MX Linux:**

To initiate a data recovery process with Foremost on MX Linux, users execute the tool from the command line interface (CLI) and specify the target disk image or device to be scanned.

Additionally, users can customize the recovery process by specifying file types or extensions to focus on during the scan**.**

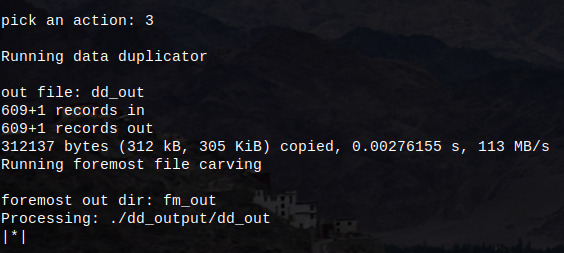


Fig4.7: Foremost automated run.

**STEP 8: Saving Foremost Data Recovery Results to Text File on MX Linux:**

When utilizing the Foremost tool for data recovery on MX Linux, users can save the results of the recovery process to a text file for easy reference and analysis.

By saving the recovery results in a text file format, users can document the recovered files, their metadata, and any relevant information for further investigation or archival purposes.

# Fig4.8: Text results of Foremost.

**STEP 9: File Carving with Scalpel Tool on MX Linux:**

To initiate file carving with Scalpel on MX Linux, users execute the tool from the command line interface (CLI) and specify a configuration file that defines the file types to be carved.

This configuration file contains rules for identifying file signatures, specifying file extensions, and indicating the maximum file size for extraction.

# 

# Fig4.9: Scalpel automated results.

**STEP 10: Concluding Processes on MX Linux with "Action=0":**

By selecting "Action=0," users signify their decision to end the current process or session gracefully. This action ensures that all pending tasks are completed, resources are properly managed, and any necessary cleanup actions are performed before concluding the session.

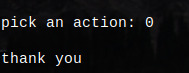
"Action=0" provides users with a straightforward and efficient way to bring processes to a close on MX Linux, promoting a smooth and seamless user experience.

Fig4.10:Thank you

**STEP 11: Cataloging Installed Tools on MX Linux from a List:**

When provided with a list of files, users can catalog installed tools on MX Linux efficiently by cross-referencing the filenames with the system's directory structure. By employing terminal commands to search specific directories where executable files are stored, users can identify the installed tools corresponding to the filenames in the list.

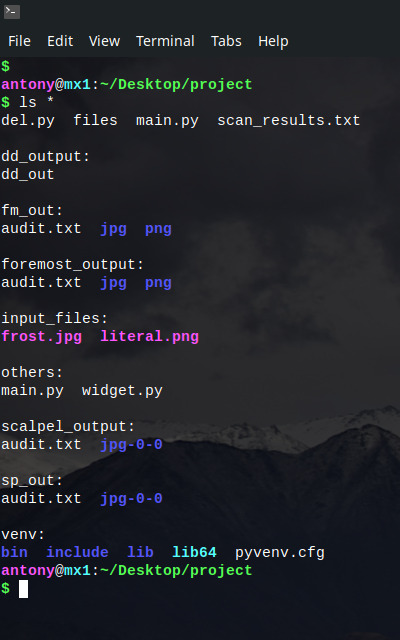
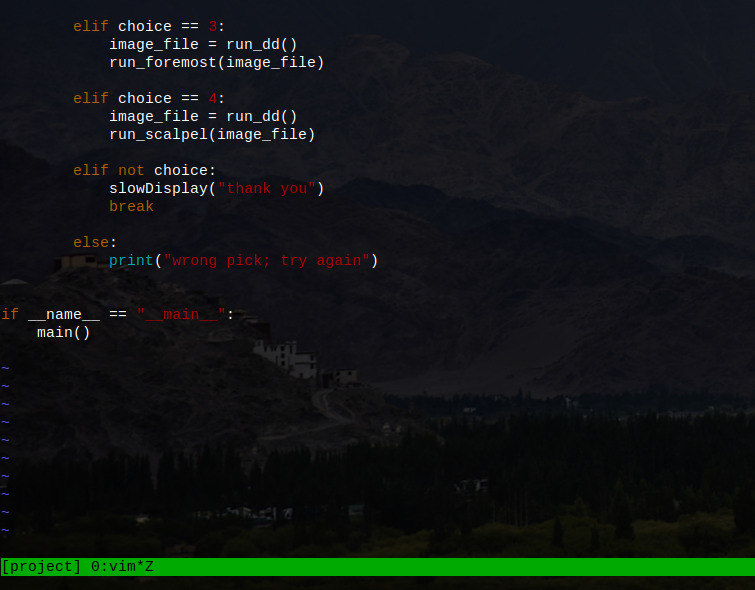
This process ensures a comprehensive overview of the tools available on the system, facilitating management, troubleshooting, and utilization of software resources on MX Linux.

Fig4.11: Listing of all Tools.

# STEP 12: Python Script Integration for Task Automation:

Within this project, Python scripts are integrated to automate and streamline various tasks on MX Linux. These scripts serve as instrumental tools, enabling the automation of repetitive processes, enhancing productivity, and optimizing system management.

Fig4.12: Python code

Fig4.13: Python code.

# CONCLUSION

## 5. CONCLUSION

The project entitled as **“INTEGRATED USB TOOLKIT FOR DIGITAL FORENSICS”**. It is a process of continuous innovation and adaptation that propels the Integrated USB Toolkit for Digital Forensics to the forefront of forensic investigation.

With its comprehensive suite of tools and functionalities, the toolkit has redefined the way USB device analysis is conducted, empowering forensic professionals with efficiency and precision. As the digital landscape evolves, so too must the toolkit, with opportunities for further development and expansion. By embracing these opportunities and remaining dedicated to excellence, the toolkit will continue to play a pivotal role in advancing the field of digital forensics, ensuring the integrity of investigations and the pursuit of justice in an increasingly interconnected world.

**FURTHER SCOPE OF THE PROJECT**

**6. FURTHER SCOPE OF THE PROJECT**

The further scope of the **Integrated USB Toolkit for Digital Forensics** encompasses several key areas aimed at expanding its capabilities and increasing its effectiveness in forensic investigations.

**Enhanced Compatibility:**

Expand compatibility to support a wider range of USB devices, including newer models and emerging technologies such as USB Type-C and Thunderbolt.

**Integration with Cloud Forensics:**

Incorporate capabilities to analyse USB devices connected to cloud storage services, allowing for comprehensive digital forensic investigations in cloud environments.

**Mobile Device Integration:**

Extend the toolkit's functionality to include analysis of USB-connected mobile devices, such as smartphones and tablets, enabling investigators to extract and analyse data from a broader range of digital devices.

**Cross-Platform Support:**

Develop versions of the toolkit for different operating systems, including Windows, macOS, and Linux, to ensure compatibility with diverse forensic investigation environments.

**Community Collaboration and Feedback:**

Foster a community of forensic professionals to provide feedback, suggestions, and contributions to the project, facilitating continuous improvement and innovation in USB device forensics.

**Expanded Forensic Capabilities:**

Enhance the toolkit to cover a broader range of digital devices and data types, including computers, mobile devices, IoT devices, cloud storage, and social media platforms.

**Automation and Efficiency:**

Develop features to automate repetitive tasks and streamline the digital forensic process, such as evidence acquisition, analysis, and reporting, to improve efficiency and reduce manual effort.

**Customization and Extensibility:**

Allow users to customize and extend the toolkit according to their specific requirements and workflows, such as adding custom analysis modules, integrating with proprietary tools, or adapting to new technologies and forensic techniques.

**Continuous Improvement and Updates:**

Commit to ongoing development, maintenance, and updates to keep the toolkit up-to-date with evolving technologies, forensic methodologies, and emerging threats in the digital landscape.

# BIBLIOGRAPHY

**7.BIBLIOGRAPHY**

**BOOKS REFERRED**

* USB Forensics: Using USB Devices for Evidence Collection" by Ron L. Meyers.
* "Digital Forensics with Opensource Tools" by Cory Altheide and Harlan Carvey.
* "Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 10" by Harlan Carvey.
* "File System Forensic Analysis" by Brian Carrier.

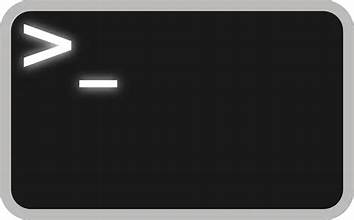
**WEBSITE REFERRED**

* <https://www.sans.org/in_en/>
* <https://www.forensicfocus.com/>
* <https://www.digitalforensicsmagazine.com/>
* <https://www.exterro.com/digital-forensics-software/forensic-toolkit>

## APPENDIX

### 8. APPENDIX

8.1 PROJECT DESIGN



The Terminal in Linux stands as a fundamental gateway for users to engage directly with the operating system through command-line interactions. It serves as a versatile tool, easily accessible through the applications menu or keyboard shortcuts, enabling users to execute commands swiftly and efficiently.

With basic navigation commands and essential functionalities such as file management and system administration, it empowers users to perform a wide range of tasks seamlessly. Moreover, its simplicity belies its power, offering features like tab completion and command history for enhanced productivity.

Embracing the Terminal not only fosters a deeper understanding of the Linux environment but also opens doors to endless possibilities for customization and automation.

It stands as a testament to the flexibility and adaptability inherent in the Linux ecosystem, catering to both novice users and seasoned professionals alike.

** BalenoEtcher:**

BalenaEtcher is a user-friendly software tool designed for flashing disk images to SD cards or USB drives, commonly used for creating bootable media for operating systems like Linux distributions or Raspberry Pi OS.

Its intuitive interface makes it easy to select the desired image file, target drive, and initiate the flashing process with just a few clicks. BalenaEtcher supports various image formats and offers validation features to ensure the integrity of the flashed media.

Its reliability and cross-platform compatibility make it a popular choice among users seeking a hassle-free solution for creating bootable drives.

**TOOLS:**

**I)Nmap:**

* + - Firstly, I chose Nmap as the cornerstone for automating network scanning tasks, recognizing its widespread adoption and robust feature set for network exploration and security assessment. Leveraging Python's versatility and Nmap's command-line interface.
    - I crafted a streamlined script to automate the execution of Nmap scans, simplifying the process of probing hosts, identifying open ports, and assessing potential vulnerabilities.

**II)Dd:**

* Secondly, I chose the dd tool for my project integrated toolkit for digital forensics due to its unparalleled ability to create forensic disk images and perform low-level data acquisition tasks.
* By integrating dd into the toolkit, I aim to empower forensic investigators with a versatile and powerful toolset for acquiring evidence in a forensically sound manner.
* Leveraging dd's capabilities, the toolkit enables investigators to perform tasks such as disk imaging, data carving, and disk wiping with precision and efficiency. Moreover, by incorporating features for logging, error handling, and hash verification, the toolkit ensures the integrity and admissibility of acquired evidence in legal proceedings.

**III)Foremost:**

* + - Foremost stands out as a robust open-source tool in the realm of digital forensics, serving the critical purpose of recovering lost or deleted files from storage media.
    - With its adept ability to identify files based on their headers, footers, and internal structures, it emerges as a formidable solution for data recovery in scenarios ranging from accidental deletions to disk formatting mishaps.

**IV)Scalpel:**

* + - Scalpel is a top-tier tool in digital forensics, essential for recovering lost or deleted files from various storage media. Its knack for piecing together fragmented or damaged data makes it indispensable for situations ranging from accidental deletions to system glitches.
    - This versatile tool covers a wide range of file formats, from everyday ones like JPEG and PNG to more complex formats like PDF and DOC.