e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

LIVE CYBER FORENSICS

Priya Godse[*1], Suyog Deshmukh[*2], Aayushi Godiya[*3]

[*1,2,3]Department of Engineering, Ajeenkya D.Y. Patil University, Charholi Budruk, Pune, India

DOI : https://www.doi.org/10.56726/IRJMETS38098

ABSTRACT

Live digital forensics, otherwise called live investigation or live reaction, is a basic interaction for gathering and analyzing digital evidence from an effectively running or as of late closed-down framework. Customary digital forensics procedures are not generally sufficient to deal with the development of innovation and the refinement of cyber-attacks. This research project investigates the fields of cloning, information recovery, and steganography with regard to cyber forensics, meaning to give productive and dependable techniques for gathering digital evidence. The system includes an exhaustive writing survey and the examination of true contextual analyses to comprehend the functional utilization of these procedures in the field of cyber forensics. The concentrate additionally investigates the difficulties and constraints looked at by digital forensics experts, including the requirement for cutting-edge specialized abilities and the restrictions of current innovation. The proposed arrangements intend to upgrade the productivity and unwavering quality of digital forensics examinations and add to the general progression of the field.

KEYWORDS: Imaging/Cloning, Data recovery, Steganography. Hash value, Report

I. INTRODUCTION

Digital forensics is the process of collecting, preserving, and analyzing digital evidence in a way that is admissible in an official courtroom. Digital forensics is used in different contexts, including incident response, regulatory compliance, internal investigations, and e-discovery. However, digital forensics presents unique challenges that require skilled forensic experts with deep technical and legal knowledge to do investigations effectively. Live digital forensics, otherwise called live examination or live response, is a basic process for collecting and analyzing digital evidence from an actively running or recently shut down the system. In live digital forensics, the forensic examiner should collect and analyze information in real time, which presents unique challenges and requires advanced technical skills.

II. LITERATURE REVIEW

Digital forensics is a rapidly evolving field, with new technologies and techniques arising to meet the steadily changing landscape of cybercrime. In this segment, we will analyze the current literature on cloning, data recovery, and steganography with regard to digital forensics.[4]

Cloning

Cloning is the most common way of making a precise copy of a hard drive or other digital stockpiling media. This procedure is ordinarily utilized in digital forensics examinations for protecting proof and guaranteeing that the first data stays in salvageable shape. A few studies have analyzed the effectiveness of different cloning techniques in digital forensics examinations. For instance, Casey and Stellatos (2006) looked at three changed techniques for plate cloning and found that a hardware-based approach gave the best outcomes with regard to speed and found that a hardware-based approach gave the best outcomes concerning pace, and accuracy.[4]

Data Recovery

Data recovery is the method involved with recuperating data that has been lost or erased because of hardware disappointment, programming blunders, or deliberate erasure. This technique is fundamental for digital forensics examiners to recuperate important proof from harmed or undermined digital capacity media. A few studies have inspected the effectiveness of different data recovery techniques in digital forensics examinations. For instance, Kessler and Dreyfus (2000) fostered a novel data carving technique that had the option to recuperate more than 80% of erased documents from a harmed hard drive.[4]

Steganography

Steganography is the act of concealing data inside other data in a manner that isn't effectively detected. This technique is usually utilized by cybercriminals to conceal delicate data, for example, passwords, Mastercard

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

numbers, and other personal data. Several studies have analyzed the effectiveness of different steganography detection techniques in digital forensics examinations. For instance, Fridrich et al. (2002) fostered a steganalysis tool called Stegdetect that had the option to detect the presence of steganographic satisfaction with a serious level of accuracy.Overall, the literature recommends that cloning, data recovery, and steganography are crucial techniques for digital forensics agents to gather and analyze digital proof successfully. Be that as it may, the studies also feature the requirement for proceeding with research and improvement here to stay aware of the advancement of innovation and the developing sophistication of cybercrime.[4]

III. PROBLEM DEFINITION

The increasing demand for efficient and reliable methods for cloning, information recovery, and steganography in the digital forensics space has led to a need for continued research and development in these areas. Cloning is the process of creating an exact replica of a hard drive or other digital storage media. Information recovery is the process of recovering information that has been lost or deleted due to hardware failure, software errors, or intentional deletion. Steganography is the practice of concealing data inside other data in a manner that isn't easily detected. These techniques are essential for digital forensics investigators to collect and analyze digital evidence effectively.[3]

IV. METHODOLOGY

The methodology for this research project includes an exhaustive literature review and analysis of certifiable case studies to investigate the functional use of cloning, information recuperation, and steganography techniques with regards to live digital forensics. The literature review includes a quest for pertinent research articles, books, and different distributions connected with cloning, information recuperation, and steganography techniques in digital forensics. The articles are screened in light of their importance to the subject, the nature of the research, and the validity of the writers. The chose articles are then investigated to extricate applicable data, for example, the strategies utilized, the outcomes got, and the impediments of the techniques. Genuine case studies are likewise to analyzed comprehend the practical application use of the techniques in the field of digital forensics. The case studies are chosen in view of their pertinence to the research questions and their quality. The analysis of the case studies includes distinguishing the techniques utilized, the difficulties looked by the measurable inspectors, and the results of the examinations.[6] The review investigates the difficulties and constraints looked by digital forensics experts, including the requirement for cutting edge specialized abilities and the restrictions of current innovation. The proposed arrangements expect to improve the proficiency and unwavering quality of digital forensics examinations and add to the general progression of the field. Generally, the methodology includes a thorough and orderly way to deal with gathering and breaking down data from pertinent sources to give dependable and important experiences into the reasonable use of cloning, information recuperation, and steganography techniques in live digital forensics[6]

V. TOOLS

ACCESS DATA FTK IMAGER

You'll discover how to swiftly and precisely gather and analyse evidence as part of a computer-related investigation using the Access Toolkit (FTK) Imager. An important tool in forensic inquiry is the Data FTK Imager, which you will first learn how to install and configure. AccessData Forensic FTK Imager is covered in this course.

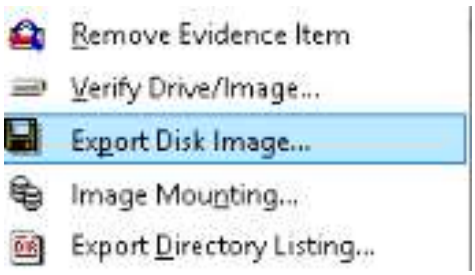
Steps for Creating Image:

- Step 1: Download and install the FTK imager on your machine.
- Step 2: Click and open the FTK Imager, once it is installed. You should be greeted with the FTK Imager dashboard.
- Step 3: In the menu navigation bar, you need to click on the File tab which will give you a drop-down, like given in the image below, just click on the first one that says, Add Evidence Item.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

- Step 4: A pop-up window asking you to choose the source of evidence will then appear. You should choose the Physical Drive option if a physical hard drive is connected to the laptop or computer you are using to create the forensic image. Select Next. Select the physical drive you want to use right now. To avoid wasting time while exporting a forensic picture of your OS drive, please double-check the drive you are choosing.
- Step 5: The forensic pictures will now be exported.

1) In the FTK Imager window, right-click the Physical Drive that you want to export. Here, click on Export Disc Image.



1) Select the Image Destination and click the Add button.

2) Decide what kind of forensic image you want to export. Click Next after selecting.E01.

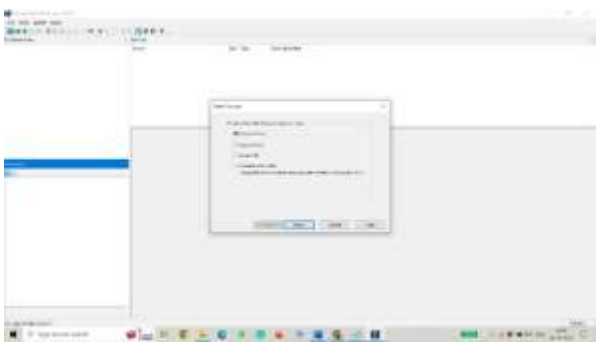
3) Following that, you must now enter case-related information. This element is entirely up to you; you can either leave them blank or keep them general.

4) After that, you must name the image and select the destination to which you want to export the forensic image. Finally, we must wait until the Forensic Image has been created and has been verified. Depending on your hardware, the forensic picture creation process will go differently quickly.

Process of Verifying Disk Image:-

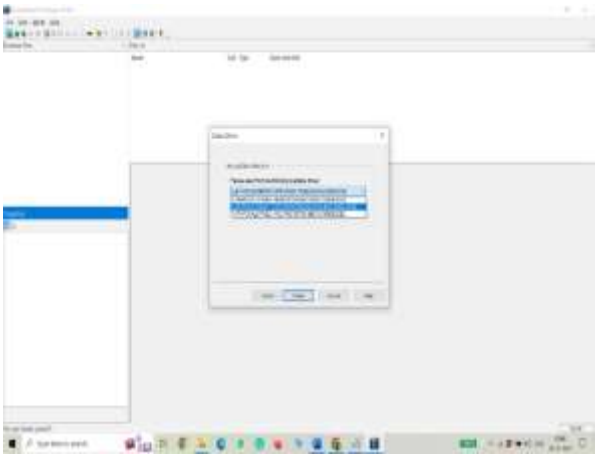
1) Step 1:

2) Step 2:

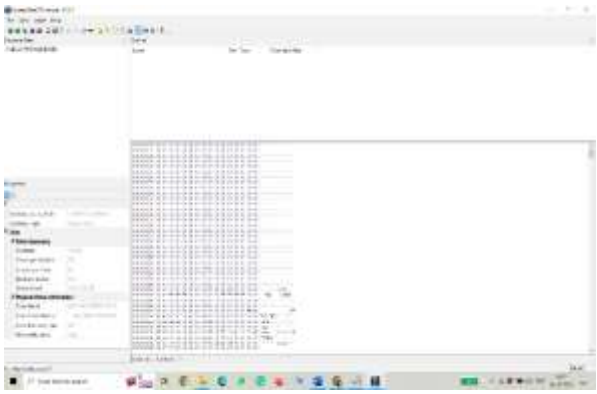


e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

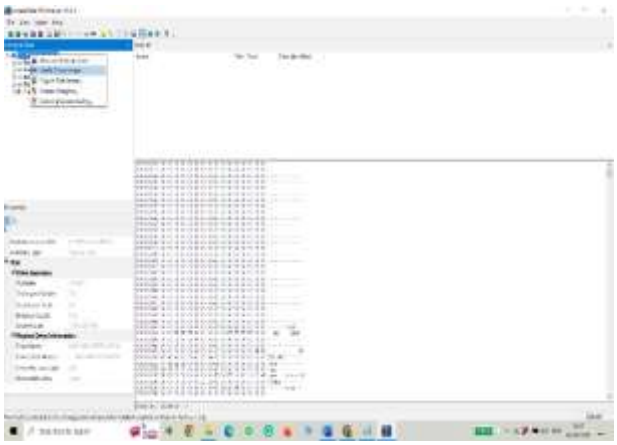
3) Step 3:



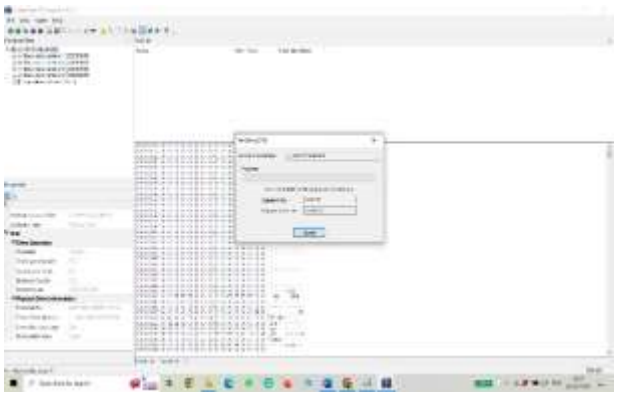
4) Step 4:



5) Step 5:



6) Step 6:



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

1. LOGICUBE TALON ULTIMATE (Hashing, Cloning, Wiping)

The Talon® Ultimate offers cutting-edge, high-performance forensic imaging at an affordable price and is designed for use in the field or forensic lab. The Talon Ultimate has been designed exclusively for digital forensic investigators and satisfies all your needs for forensic imaging, hashing, and wiping. It has a small footprint, easy navigation, and unmatched imaging speed.

- The Talon® Ultimate is an extremely fast forensic imaging solution, achieving speeds of over 40GB/min.
- Image and verify to multiple image formats; native copy, dd image, .dmg image, e01, and ex01. The Talon Ultimate provides SHA1, SHA256, and dual hash (MD5+SHA1) authentication at extremely fast speeds.
- Talon Ultimate formats destination drives to NTFS, EXT4, FAT 32 or exFAT file systems. The unit supports imaging from source drives formatted to any major file system.
- Concurrent Image+Verify. Imaging and verifying concurrently take advantage of destination hard drives that may be faster than the source hard drive. The duration of the total image process time may be reduced by up to half.
- The targeted imaging/logical imaging tool enables you to construct a logical image by capturing only the necessary files using pre-set, custom filters, file signature filters, and/or keyword searches. A list of potentially deleted files can be included in an MFT report. L01, LX01, ZIP, or directory tree output formats are available. Users can browse and see content directly on the Talon Ultimate display or use a web browser on their laptop or desktop to manage and view content on a networked Talon Ultimate. requires the Targeted Imaging option to be purchased.Write-Blocked Drive Preview. Preview drive content directly on the Talon Ultimate. The file browser feature provides logical access to source or destination drives connected to Talon Ultimate. Users can view the drive's partitions and contents, and view text files, jpeg, PDF, XML, and HTML files.
- Solid-state drives, as well as SATA/USB3/FireWire storage devices, are supported natively by the Talon Ultimate. When a software option is purchased, SAS devices are supported. Talon Ultimate comes with an adaptor that supports 2.5"/3.5" IDE drives. With optional adapters, PCIe, 1.8" IDE, 1.8" ZIF, mSATA, Micro SATA, SATA, and flash drives are supported.
- Encrypt the entire drive using AES 256-bit to protect important evidential data. VeraCrypt, TrueCrypt, or FreeOTFE are a few examples of open-source software tools that can be used for decryption.
- Network Push Functionality. Push evidence files from Talon Ultimate repository or from destination drives attached to the Talon Ultimate to a network site. By completing an MD5 or SHA hash during the push procedure, the Push function offers a more secure technique than merely copying and pasting to the analysis machine.
- Using the FireWire port, users can capture from a MAC system that is booted in target disc mode. For MACs with a Thunderbolt port, an aftermarket Thunderbolt to FW connection is necessary. Supports the use of images taken from MACs with USB-C ports and the MacBook Pro.

2. MOBIL edit (Mobile Phone Extraction)

A Digital forensics tool by Compelson Labs called MOBILedit Forensic searches, evaluates, and generates reports on data from GSM/CDMA/PCS cell phone handsets. Through an Infrared (IR) port, a Bluetooth connection, WiFi, or a cable interface, MOBILedit can connect to cell phone devices. The phone model is

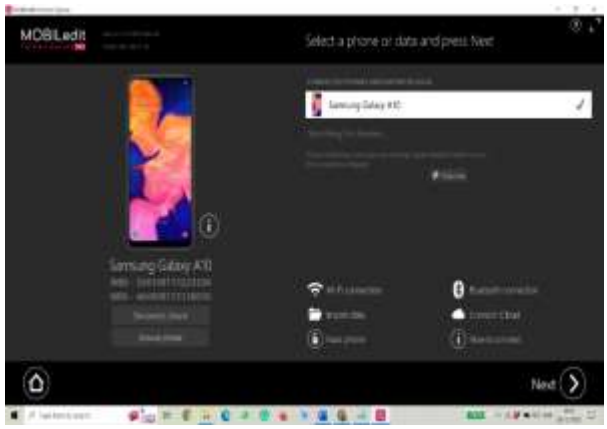
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

identified by its manufacturer, model number, serial number (IMEI), and a related image of the phone after connectivity has been established. The MOBILedit platform examines the contents of the phone through a folder structure like to MS Outlook and is compatible with a number of phones and smartphones (a complete list of supported handsets is available on the manufacturer's website).

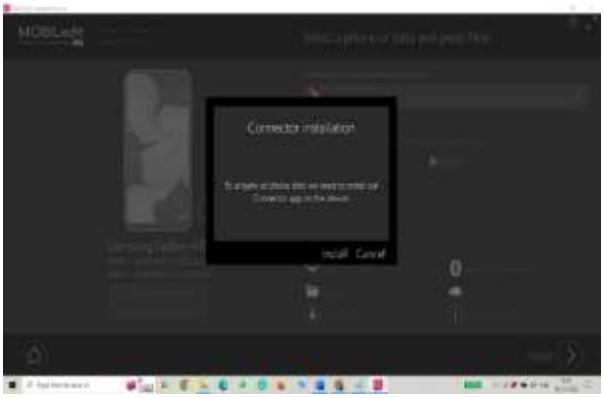
Step 1: Home page of MOBILedit application. Click on the start button.

Step 2: Connect the Phone, note(switch on the developer mode and USB debugging)

Step 3:The phone will be detected and details of the phone will be displayed.

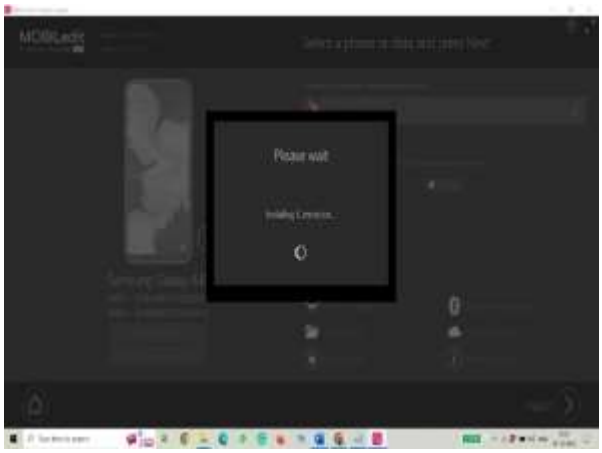


Step 4: Now it will show a popup for installing a forensic connector on the phone click on install.



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

Step 5: Now the forensic connector will be installed wait till the connector is installed.



Step 6: Now it will be reconnected after giving access to all on phone for forensic connector

Step 7: Now we have to choose what we exactly want to extract.

Step 8: Now enter the details as asked below.

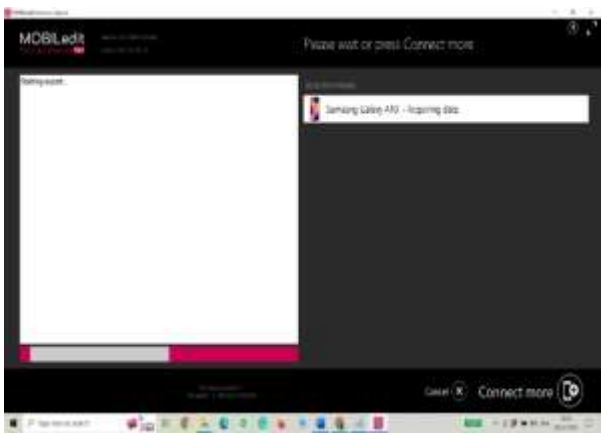
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:05/May-2023 Impact Factor- 7.868 www.irjmets.com

Step 9: Now enter the details as asked below.

Step 10: Now choose the report format in which format you want the report.

Step 11: Now give the destination as per required.

Step 12: Now the exporting will start to wait till the complete exporting.



Last but not the least, phones will be exported to the given destination. We can access the report after completing the extraction

VI. RESULTS AND DISCUSSION

The literature review reveals that cloning, information recovery, and steganography are vital techniques for digital forensics investigators to collect and analyze digital evidence effectively. However, the concentrate likewise identifies challenges and restrictions, like the need for accurate and effective information recovery techniques, and the challenges posed by steganography techniques in uncovering hidden information. The project team has proposed answers for these difficulties, including the use of advanced cloning techniques, information recovery calculations, and steganalysis methods. These arrangements plan to enhance the efficiency and reliability of digital forensics investigations and contribute to the overall advancement of the field. Given timeline only. Suppose, If the engineer is unable to solve the query, then, the query gets passed on to the other engineer of the same specialization. Other engineer of the same specialization takes down the work of solving the query which isunresolved.

VII. CONCLUSION

In conclusion, this research project features the increasing importance of live digital forensics and the unique challenges it presents. The project focuses on the fields of cloning, information recovery, and steganography, and explores their useful application in the context of cyber forensics.Through a comprehensive literature review and examination of real-world case studies, the project team has identified the need for efficient and reliable methods for cloning, information recovery, and steganography in digital forensics investigations. The concentrate additionally sheds light on the challenges faced by digital forensics professionals, including the need for advanced technical skills and the restrictions of current technology.During the research process, the team encountered difficulties, for example, the need for accurate and effective information recovery techniques and the challenges posed by steganography in uncovering hidden information. However, the team proposed answers for these difficulties, including the use of advanced cloning techniques, information recovery calculations, and steganalysis methods.Overall, this research project provides valuable bits of knowledge into the importance of live digital forensics and the need for advanced techniques and skilled forensic examiners in doing successful investigations

VIII. REFERENCES

[1] Casey, E., & Stellatos, G. (2014). Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer. Elsevier.

[2] Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional. Casey, E., & Stellatos, G. (2014). Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer. Elsevier.

[3] Garfinkel, S. L., & Shelat, A. (2003). Remembrance of data passed: A study of disk sanitization practices. IEEE Security & Privacy, 1(1), 17-27. Kruse, II, W. G., & Heiser, J. G. (2002). Computer forensics: incident response essentials. Addison-Wesley Professional.

[4] Casey, E. (2011). Digital evidence and computer crime: forensic science, computers, and the internet. Academic Press. Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional.

[5] Quick, D., & Choo, K. K. R. (2014). Principles and practice of forensic investigation of digital devices. Springer. Kessler, G. C. (2005). Digital forensics: new paradigms in digital evidence and electronic crime investigation. Springer.

[6] Casey, E. (2011). Digital evidence and computer crime: forensic science, computers, and the internet. Academic Press. Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional.