iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67302

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

A Non-Destructive Technique for Extraction of Digital Data in Forensic Analysis

Kiran R Dodiya[1], Dr. Kapil Kumar[2], Kashyap Joshi[3], More Aditya Rajesh[4], Bhumika Doshi[5], Dr. Parvesh Sharma[6]
[1, 3, 4]*Research Scholars, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, India*
[2]*Coordinator, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, India*
[5]*TRA (Cyber Security), Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, India*
[6]*Assistant professor (Forensic Science) NSIT-IFSCS (Affiliate to NFSU) Jetalpur, Ahmedabad, Gujarat, India*

Abstract: ***The rapid growth of digital devices and technological advancements has led to a surge in data storage across hard drives, pen drives, and cloud platforms. Digital data retrieval has become crucial for criminal investigations, enabling offender identification and evidence-based judicial decisions.***
However, the ability to erase, alter, or corrupt data poses significant challenges for forensic investigators, particularly in preserving data integrity during extraction.
To address these challenges, developing non-destructive methods for data extraction is essential for maintaining the authenticity and reliability of digital evidence.
This research proposes a novel, non-destructive technique to extract specific data from storage devices while safeguarding both the integrity of the data and the media.
The approach enhances forensic analysis by facilitating evidence acquisition without jeopardizing its admissibility in court. Advancing forensic methodologies is vital to overcoming the evolving complexities of digital investigations and ensuring effective, reliable outcomes.
Keywords: Digital forensics, Data integrity, Non-destructive extraction, Evidence preservation, Criminal investigations.

I. INTRODUCTION

A. Data

Data saved on virtual gadgets performs an important position in forensic analysis, as it serves as the cornerstone of evidence in criminal investigations.
The number one objective of forensic evaluation is to acquire, method, and interpret data to aid investigative outcomes and ultimately present it as admissible evidence in a court of regulation. Unlike different sorts of proof, virtual information possesses the specific function of last unchanged if it is not intentionally up to date or altered.
However, forensic analysts and safety engineers face considerable challenges due to the restrained availability of appropriate tools and specialized information for efficaciously investigating modern digital gadgets. As using the internet and digital structures continues to enlarge, so too does the attention to the price of the information saved on those systems. Unfortunately, this cognizance is regularly exploited by cybercriminal companies, which understand that focusing on virtual platforms can yield sizable private and commercial enterprise records.
Digital statistics is increasingly vulnerable to diverse sorts of cyber threats, such as malware, Trojans, viruses, and different malicious software, that could compromise its protection and integrity[1].

B. Challenges in Data Extraction

For digital proof to be diagnosed in a court docket of regulation, it is imperative to keep both its authenticity and chain of custody. The forensic technique necessitates creating a precise reproduction or disk photo of the unique evidence to make certain the statistics stay unaltered at some point of analysis.
Maintaining the integrity of authentic statistics while allowing green extraction and analysis is a key undertaking in virtual forensics. To deal with those boundaries, this research proposes a unique, non-destructive approach for extracting unique records from virtual storage structures. This method goals to conquer cutting-edge obstacles by using ensuring records integrity and facilitating the acquisition of reliable forensic proof for investigative and felony purposes[2].

©IJRASET: All Rights are Reserved

Figure 1: Computer Forensic Process Model

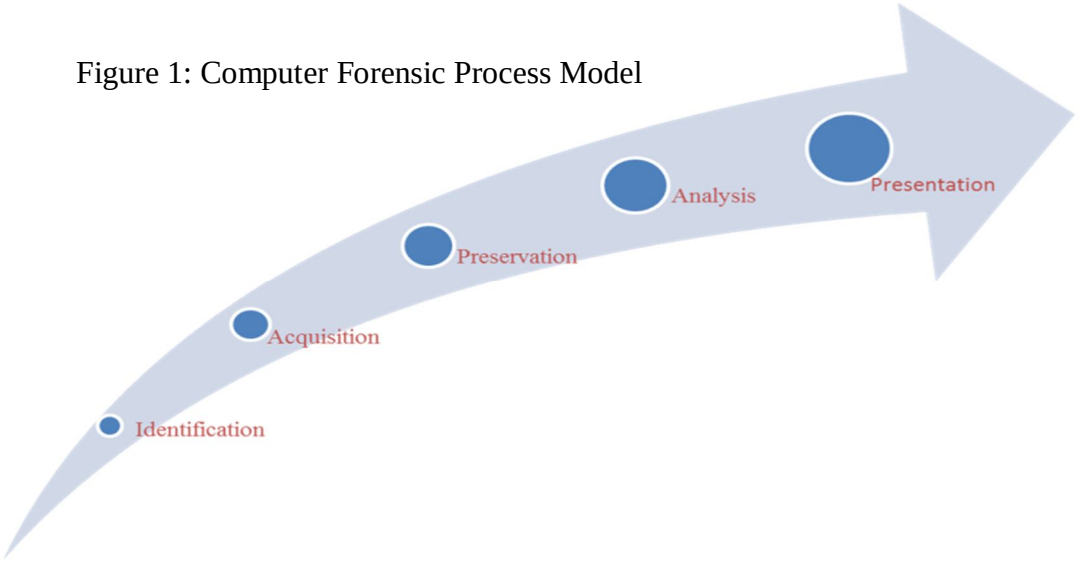


Figure 1 shows a Computer Forensic Process Model for the digital evidence[13].

1) Identification

Digital proof can exist in both logical and tangible paperwork. Tangible evidence refers back to the bodily shape, design, and final shape of gadgets that save or procedure digital information. Logical evidence, alternatively, consists of records saved in binary layout, accessible through unique tools or procedures. During the identification segment, virtual garages and processing gadgets which could contain applicable proof are identified and documented. With the growing adoption of cloud computing, Network-Attached Storage (NAS), and Storage Area Networks (SAN), the identification technique has grown more complicated, introducing virtualized components. Consequently, first responders and digital forensic examiners have to have radical know-how of those structures to identify and document evidence efficaciously[3].

2) Acquisition

The acquisition phase includes growing an actual image of potential virtual proof or the information contained within virtual gadgets whilst meticulously documenting the equipment and strategies used. The resulting picture has to be verified to make certain it's far a piece-by-bit, actual reproduction of the authentic statistics, proven via hash fee comparisons. Any discrepancies between the original evidence and its reproduction render the acquisition invalid. Depending on the requirements, virtual forensic examiners may additionally appoint logical acquisition, which makes a speciality of extracting unique varieties of facts, documents, or directories. The integrity of the facts ought to stay uncompromised at some point in this manner, as that is critical for ensuring the admissibility of evidence in a court of regulation[4].

3) Preservation

The preservation degree ensures that capability virtual proof is safeguarded from tampering, destruction, or alteration. Preservation techniques cognizance on preserving each the physical and logical integrity of the proof, consisting of metadata and related facts fragments. Any shape of spoliation, whether intentional or unintentional, can compromise the evidentiary price of virtual artefacts. To achieve this, virtual proof should be saved in a secure environment where confidentiality and integrity are assured. Best practices contain growing write-covered copies of the original evidence and ensuring no alterations occur for the duration of subsequent forensic tactics[5].

4) Analysis

The Analysis level includes a detailed exam of the acquired records to uncover relevant information and reconstruct activities. This step is crucial for deciphering the internal shape of information and identifying styles or anomalies that aid investigative conclusions. Through iterative analysis, fragmented records are reconstructed, hypotheses are tested, and findings are substantiated. Depending on the complexity of the records, forensic analysis may additionally require specialised gear and knowledge. However, collaborative efforts and iterative examination techniques often enable more comprehensive information on the evidence[6].

5) Presentation

The presentation level involves compiling the findings of the forensic research right into a clean, concise, and structured document. This report needs to detail each step taken through the investigative manner, along with protocols followed, equipment used, and techniques hired to acquire, analyze, and keep proof. The record needs to additionally provide a transparent description of the conclusions drawn and the assisting proof. To ensure reliability, the findings have to be supplied in a way that is comprehensible to non-professional stakeholders, which include judges, lawyers, and jurors, even adhering to clinical and felony requirements[7].

II. RELATED WORK

Digital evidence incorporates binary records stored, transmitted, or processed on digital gadgets. This evidence can take diverse formats, inclusive of audio, video, photographs, and files. However, virtual proof possesses specific traits that distinguish it from traditional types of proof: it may be without difficulty copied, altered, or deleted; figuring out its original supply can be difficult; and it frequently calls for technical procedures to make it human-readable[8]. The discipline of digital forensics specializes in uncovering, retaining, and analyzing electronic facts to reconstruct past activities. As conventional proof will increasingly change to digital proof, ensuring the non-damaging and legally admissible acquisition of virtual artefacts has emerged as a key difficulty[9]. Digital forensics encompasses numerous strategies of statistics acquisition, consisting of guide acquisition, logical acquisition, hex dump evaluation, chip-off strategies, and micro-examine strategies. With the growing prevalence of cybercrimes such as network intrusions, records fabrication, and unauthorized content distribution, digital forensics plays a pivotal role in crook investigations[9]. Specialized gear, along with Guidance Software's EnCase, Access Data's FTK, and ASR Data's SMART, Permits investigators to identify, preserve, and analyze statistics successfully[10]. However, usability problems with these tools can now and then prevent investigations, leading to capacity miscarriages of justice or incomplete analyses. A substantial undertaking in digital forensic investigations is the recovery of deleted or hidden information. Hard drive pictures regularly consist of allocated and unallocated spaces, the latter of which can also incorporate remnants of deleted documents or temporary records. While string searches may additionally recover sure text documents, identifying significant information in compressed documents, pictures, or encrypted formats requires superior strategies[11]. Password safety and encryption in addition exacerbate the complexity of virtual proof healing, necessitating sophisticated tools and expertise. The National Institute of Standards and Technology (NIST) outlines a structured forensic process comprising 4 key stages: seizure, acquisition, exam, and reporting. Maintaining the integrity of proof during those stages is critical. Additionally, ensuring the chain of custody and preventing adjustments to the unique data stays a cornerstone of forensic fine practices. As cybercriminals adopt more and more state-of-the-art methods to hide or obfuscate data, improvements in forensic equipment and methodologies are important to keep pace with evolving challenges [12].

III. METHODOLOGY

Figure 2 describes the whole process of cloning and extraction of data using FTK and Autopsy software.

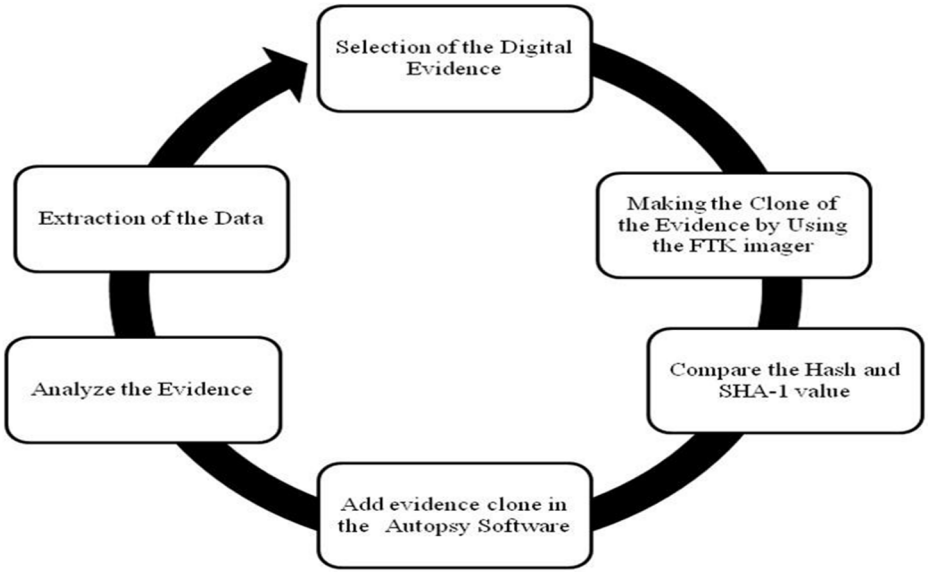


Figure 2 Methodology Of Research

A. Selection of the Evidence

The selection procedure involves figuring out and reading digital evidence along with difficult disks, memory cards, pen drives, or other storage media. These gadgets are imported into a forensic software program which includes FTK (Forensic Tool Kit) for additional analysis. The number one goal of this stage is to decide the series of occasions, investigate their significance, and compare the probative value of the evidence to the case. Practitioners ought to cautiously take a look at the available virtual artefacts to avoid misinterpretation or unfounded assumptions. This phase is a truth-locating system that objectives to reconstruct events correctly and expand doable know-how of the records.

B. Making the Clone of the Evidence

Hard pressure cloning refers to developing an actual replica of the records stored on a tough disk with the use of a specialised forensic device. This method, also referred to as bitstream imaging, replicates every bit of facts for various functions consisting of machine backups, provisioning, healing, and legal investigations. A forensic picture is created in controlled surroundings, typically in a forensic examiner's laboratory. The examiner connects the hard power to a write blocker to save you from tampering and guarantee the integrity of the facts. Using a specialized software program, the examiner generates a bitstream photograph, that is then transferred to an outside garage tool. In certain instances, a couple of forensic snapshots may be stored on an unmarried outside drive for redundancy and further analysis.

Difference between Cloning and Forensic Imaging:

1) Cloning: Creates an exact reproduction that allows for direct exploration and report access.
2) Forensic Imaging: Captures all facts, including deleted and hidden documents, to maintain the evidence for investigative purposes. It acts as a virtual fingerprint of the authentic disk. Forensic photographs aren't immediately reachable through popular software programs and might only be tested with the use of specialised forensic tools.

C. Compare the Hash Value

Hash values play a crucial position in validating the integrity and authenticity of forensic pics. A hash feature generates a unique cryptographic fingerprint (e.g., MD5, SHA-256) for the unique records. The contrast of pre-acquisition and submit-acquisition hash values ensures that the forensic image is an actual reproduction of the supply media. Any mismatch would indicate tampering or corruption at some point in the purchase manner. Additionally, hash comparisons help verify the reliability of the hardware and software program gear hired at some stage in imaging. Factors inclusive of differences in media sizes or disasters in forensic gear for the duration of acquisition necessitate rigorous hash validation processes to ensure the admissibility of proof.

D. Add Evidence in the Autopsy Software

Autopsy, an open-supply forensic platform, is used to investigate and get better digital proof. The software supports external devices and mobile storage media, permitting investigators to import forensic photos or raw facts for additional examination.

The Autopsy User's Guide gives step-through-step commands for importing proof, the same time the Developer's Guide gives equipment for extending Autopsy’s capability through custom modules. By including evidence in an Autopsy, examiners can leverage its complete analysis functions to extract, classify, and interpret virtual artefacts systematically.

E. Analyzing the Evidence

The scope of proof has multiplied to encompass virtual artefacts, aligning with definitions supplied inside the Indian Evidence Act and the Information Technology Act. Under those criminal frameworks, virtual evidence—which includes emails, documents, or logs—may be admissible without supplying the bodily tool in the courtroom. Instead, forensic investigators might also post hard-pressure copies, revealed records, or test reports as proof. However, the admissibility of virtual evidence calls for compliance with positive conditions, consisting of submitting a certificate underneath applicable prison provisions. The evaluation section includes scrutinizing digital proof to extract actionable insights and generate precise forensic reviews. These reviews report findings comprehensively and support felony complaints by organising the relevance and integrity of the evidence.

F. Extraction of Digital Evidence

Following the import of evidence into the Autopsy software, the extraction technique entails categorizing and retrieving precise document types based on their extensions. Evidence together with pics, documents, audio, and video files are systematically prepared under their respective report extensions, allowing green evaluation.

To extract virtual artefacts, investigators can:

1) Select the desired file types or extensions within Autopsy.

2) Use the "Extract" characteristic to isolate and export applicable proof for addition examination.

This prepared extraction process guarantees that all vital facts are correctly retrieved, documented, and organized for inclusion in forensic reviews or presentations in the courtroom.

IV. RESULT AND DISCUSSION

A. Results of FTK Clone

The forensic cloning system is executed using FTK Imager, a widely recognized device for growing forensic pix. Figure three demonstrates the exact similarity to the virtual evidence of the usage of the FTK Imager. A bitstream picture of the original statistics was created to ensure that everyone's active, deleted, and hidden documents had been captured without changing the supply. This non-destructive procedure preserved the integrity of the authentic virtual proof for further forensic analysis**.**

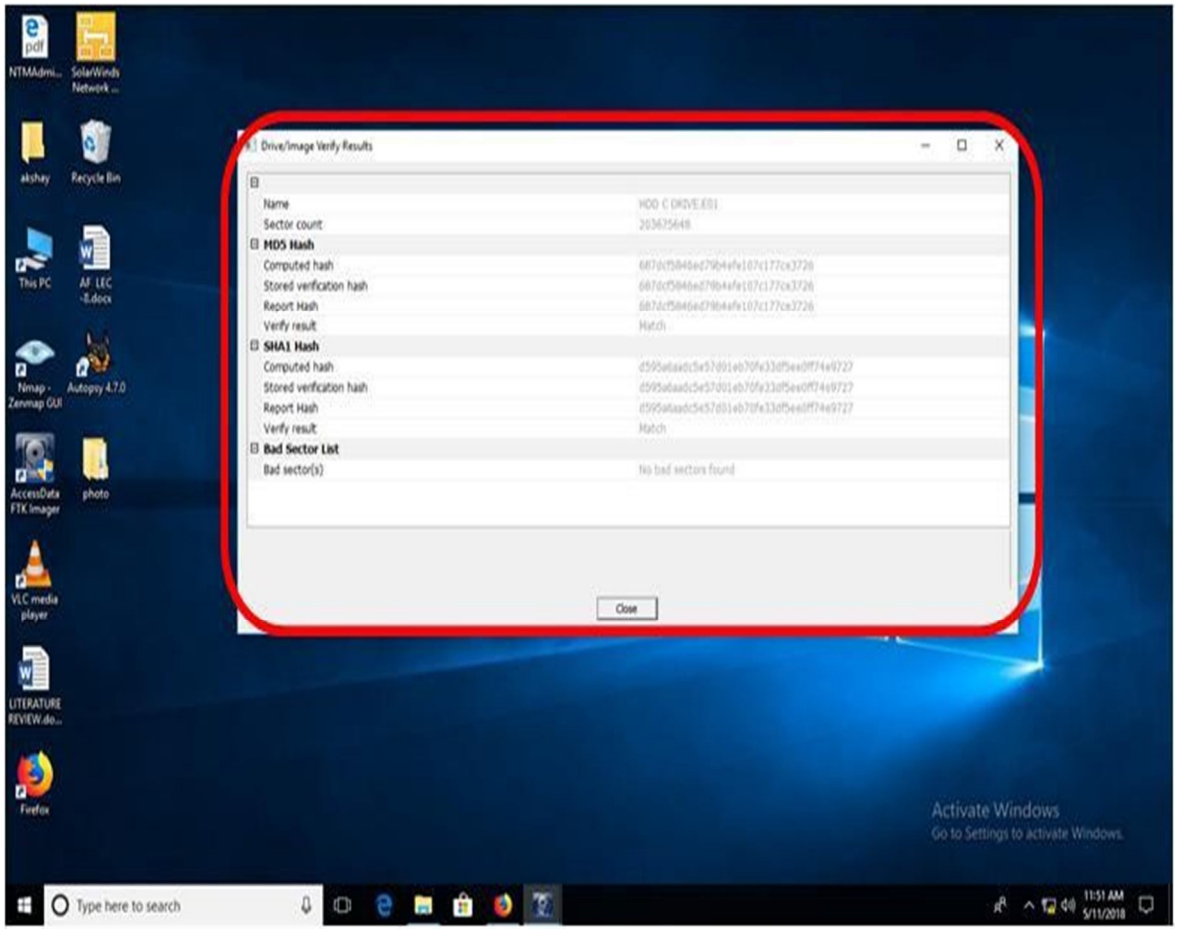


Figure 3: clone of digital evidence using FTK Imager

Figure 3: Exact similar to digital evidence of the usage of FTK Imager. Addition of Evidence in Autopsy and File Separation

Following the cloning method, the forensic image is imported into Autopsy, an open-supply forensic evaluation tool. Figure four illustrates the addition of virtual evidence into the Autopsy software. The software program systematically separates the documents primarily based on their extensions, allowing easy admission to unique classes which include:

- Images (e.G., .Jpg, .Png, .Gif)
- Documents (e.G., .Doc, .Pdf, .Txt)
- Audio Files (e.G., .Mp3, .Wav)
- Video Files (e.G., .Mp4, .Avi)

The report on business enterprise in Autopsy simplifies the technique of finding and analyzing digital artefacts applicable to the investigation. This step is critical for correctly retrieving actionable proof without compromising record integrity.

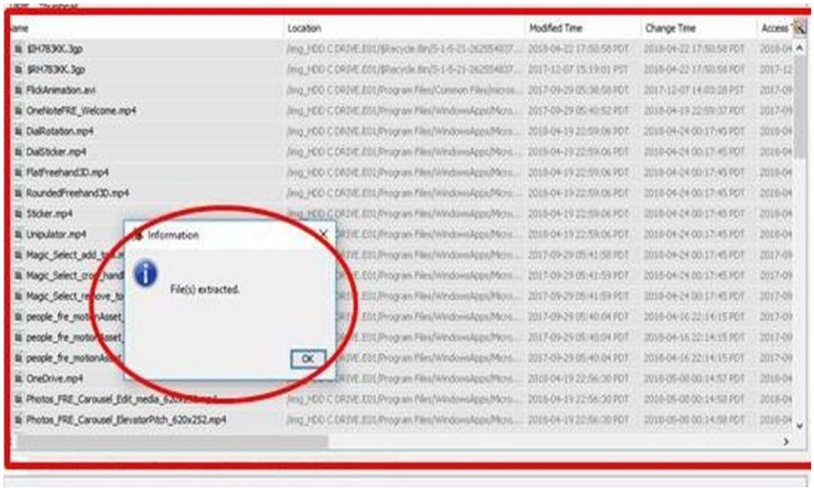


Figure 4: The addition of the evidence in the Autopsy gives the separation of the file by extension

Figure 4 shows the addition of digital evidence into Autopsy, where files are automatically categorized based on their extensions. The software organizes the extracted data into folders, such as documents, images, audio, video, and system files, enabling efficient analysis and retrieval of relevant artefacts for forensic investigation.

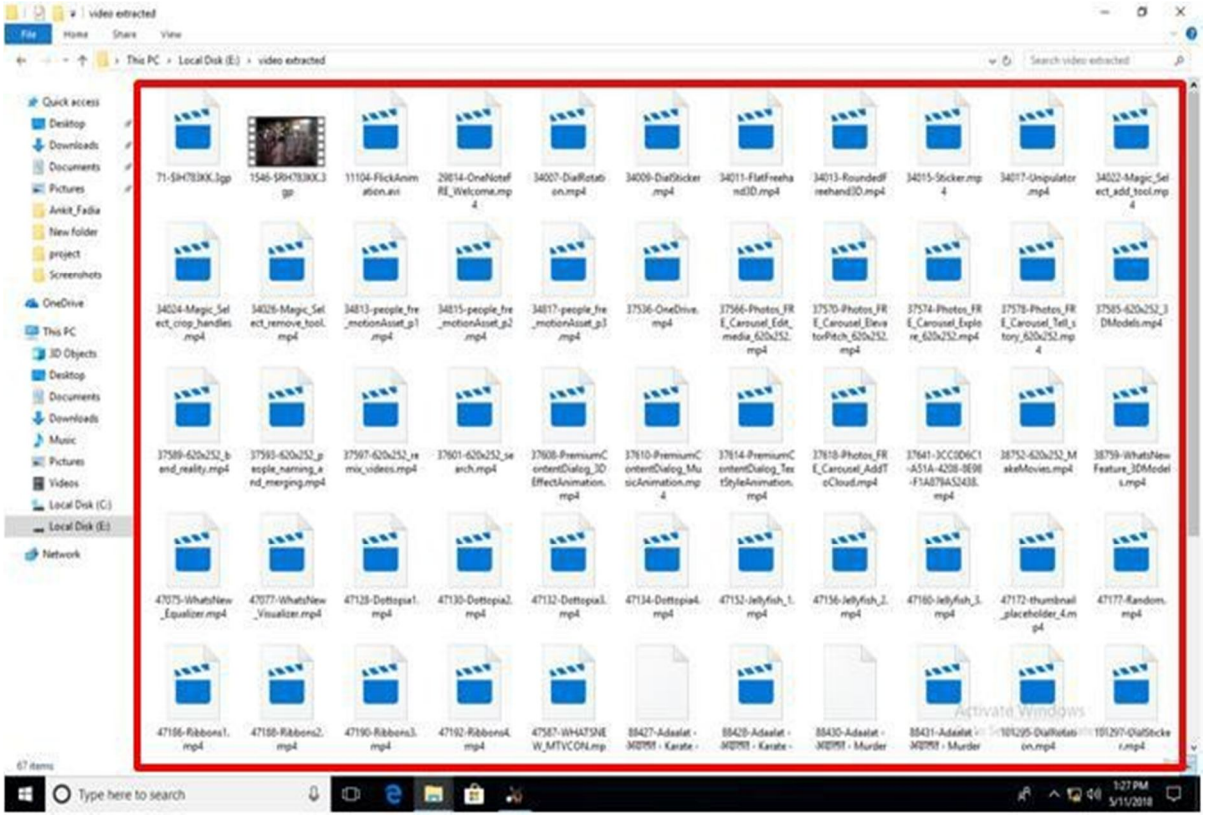


Figure 5: Extracted Data Organized in a Folder

Figure 5 illustrates the outcome of the forensic data extraction system, in which the retrieved information has been systematically prepared into specific folders. This enterprise is finished after uploading the proof into Autopsy, an open-supply forensic evaluation device. The software allows the examiner to categorize files based on their kinds and extensions, making sure that each extracted virtual artefact is smartly stored for further evaluation.

The extracted information may additionally encompass numerous report sorts together with:

1) Documents: Files with extensions along with .Docx, .Pdf, .Txt that could incorporate important textual information.
2) Images: Visual evidence in formats like. JPG, . PNG, and . GIF that would provide insights or links to occasions or people concerned.
3) Audio and Video Files: Multimedia files in formats like. MP3, . WAV, .Mp4, and .Avi which can function as helping evidence for criminal investigations.
4) Logs and Metadata: Files containing gadget or user interest logs which could reconstruct the sequence of occasions up to the incident.

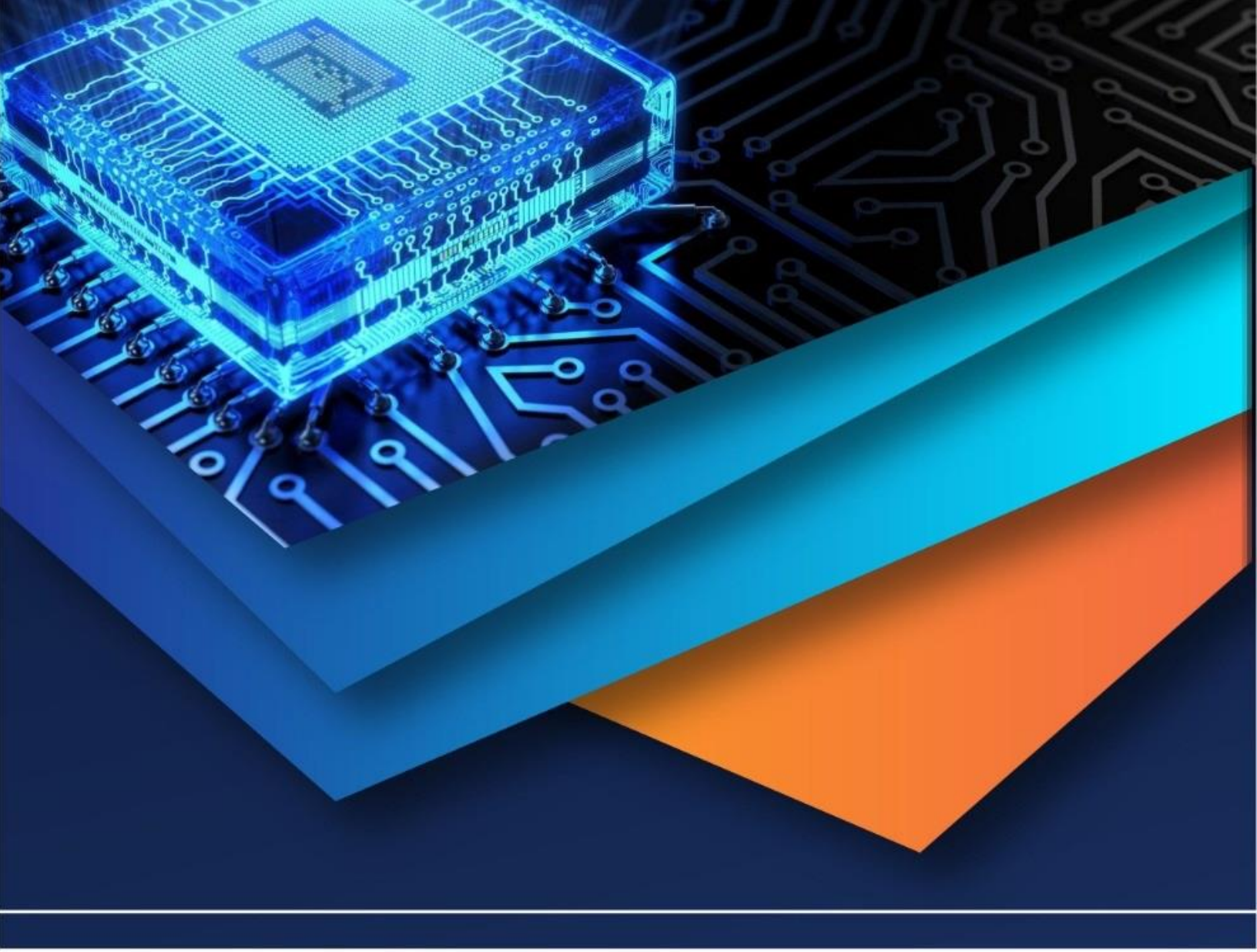
By systematically organizing these documents into folders, investigators can successfully navigate through the statistics, awareness of applicable artefacts, and analyze them without dropping track of important facts. This structured approach minimizes the complexity of coping with large amounts of extracted records and aids in the timely identification of evidence. Furthermore, the prepared folders make certain that all statistics are preserved in their original nation, preserving their integrity and admissibility in felony lawsuits. The extracted and categorized statistics serve as the inspiration for drawing conclusions and reconstructing the timeline of activities, which is vital in assisting forensic evaluation and presenting findings in the courtroom. In the end, Figure 6 highlights the effectiveness of digital forensic gear in retrieving and structuring facts from evidence assets, ensuring a streamlined and systematic manner for forensic investigations.

V. CONCLUSION

The consequences reveal that records extraction from digital garage gadgets is successfully facilitated via forensic gear like FTK Imager and Autopsy, offering a non-unfavorable approach to retrieving energetic, deleted, and hidden information from tough drives, USB flash drives, and memory playing cards. FTK Imager efficaciously created an exact forensic similar to the original digital proof while maintaining facts integrity through the use of a write blocker to prevent modifications. Autopsy correctly categorized the extracted information using record sorts and extensions, permitting investigators to easily discover and analyze crucial artefacts, which include photos, films, files, and audio documents, which were systematically organized into folders for detailed examination. This manner offers giant applications in virtual forensic investigations, allowing investigators to get better precious evidence from crime scenes without compromising its integrity, keep statistics for criminal court cases, and uncover unexpected leads primarily based on the recovered artefacts. Overall, the study highlights the effectiveness of FTK and Autopsy as systematic, green, and reliable gear for records extraction and protection in virtual forensic evaluation.

REFERENCES

[1] Expert Data Forensics | Las Vegas, Nevada Digital Forensics. https://expertdataforensics.com/. Accessed 18 Dec 2024
[2] The Admissibility And Challenges of Digital Evidence In Court. https://www.legalserviceindia.com/legal/article-14633-the-admissibility-and-challenges-digital- evidence-in-court.html. Accessed 18 Dec 2024
[3] (PDF) An Examination of Digital Forensic Models. https://www.researchgate.net/publication/2589967_An_Examination_of_Digital_Forensic_Mod els. Accessed 18 Dec 2024
[4] Montasari R (2017) A standardised data acquisition process model for digital forensic investigations. International Journal of Information and Computer Security 9:229–249. https://doi.org/10.1504/IJICS.2017.085139
[5] AlKhanafseh M, Surakhi O (2024) Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography. Electronics 2024, Vol 13, Page 3729 13:3729. https://doi.org/10.3390/ELECTRONICS13183729
[6] Stakia A, Dorigo T, Banelli G, et al (2021) Advances in Multi-Variate Analysis Methods for New Physics Searches at the Large Hadron Collider. Reviews in Physics 7:100063. https://doi.org/10.1016/J.REVIP.2021.100063
[7] Write a Forensic Report Step by Step [Examples Inside]. https://www.salvationdata.com/work- tips/write-a-forensic-report/. Accessed 18 Dec 2024
[8] Digital & Multimedia Evidence | National Institute of Justice. https://nij.ojp.gov/topics/forensics/digital-multimedia-evidence. Accessed 18 Dec 2024
[9] Digital Forensics Fundamentals: Successful Preservation of Evidence. https://www.ftitechnology.com/resources/blog/digital-forensics-fundamentals-successful- preservation-of-evidence. Accessed 18 Dec 2024
[10] Sarkar G, Shukla SK (2023) Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology 2:100034. https://doi.org/10.1016/J.JECONC.2023.100034
[11] Reedy P (2020) Interpol review of digital evidence 2016 - 2019. Forensic Sci Int 2:489–520. https://doi.org/10.1016/J.FSISYN.2020.01.015
[12] Simou S, Kalloniatis C, Gritzalis S, Mouratidis H (2016) A survey on cloud forensics challenges and solutions. Security and Communication Networks 9:6285–6314. https://doi.org/10.1002/SEC.1688
[13] (PDF) Evaluation of Digital Forensic Process Models concerning Digital Forensics as a Service. https://www.researchgate.net/publication/318981575_Evaluation_of_Digital_Forensic_Process_ Models_with_Respect_to_Digital_Forensics_as_a_Service. Accessed 18 Dec 2024



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)