Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/



Research Paper Open Access

A Framework for Rapid Acquisition and Secure Transfer of Disk-Based Digital Evidence During the Golden Hour

Shubham Sangwan[1], Naveen Kumar Chaudhary[2]

[1]Forensic Sciences University, Sector 9, Gandhinagar, Gujarat. crshubhamsangwan@gmail.com, https://orcid.org/0009-0007-2786-2785
[2]National Forensic Sciences University, Sector 9, Gandhinagar, Gujarat. naveen.chaudhary@nfsu.ac.in, https://orcid.org/0000-0002-5851-6996

ABSTRACT
The "Golden Hour" following a crime incident is critical for the acquisition and preservation of digital evidence to ensure successful forensic investigations. This study presents a practical methodology combining a custom-built remote acquisition script, automated cryptographic hashing for integrity verification, and secure cloud storage to enable timely and tamper-resistant collection and transfer of digital evidence from the crime scene. Unlike traditional approaches that rely on physical transportation of devices to forensic laboratories, the proposed framework supports on-scene forensic imaging with controlled remote transfer, reducing delays and associated risks. Experimental evaluation using an 8 GB USB storage device demonstrates that imaging, hashing, and secure transfer can be completed within approximately 2-3 hours, with integrity confirmed through matching hash values before and after transfer. The results indicate that the methodology improves the efficiency and reliability of disk-based digital evidence handling during the Golden Hour while remaining consistent with established forensic principles.

Keywords: Disk Duplication, Digital Forensics, Forensic Duplication, Forensic Acquisition, Forensic Imaging, Golden Hour

Introduction

This short but crucial phase of every crime immediately following the event - typically labelled as the 'Golden Hour' of forensics - provides an opportunity which requires the most accurate collection and protection of digital data in order to maximize chances of success. The digital data produced is relevant to various criminal enquiries including sexual crimes, human traffickers, homicides, suicides, children at risk from harm or exploitation, class 1 drug cases, and fraud [1]. However, in comparison to our methods for both physical and electronic evidence there is clearly a void within the current methods of evidence identification and collection which do not incorporate the distinct difficulties encountered when considering digital data during this precarious window. Simply put: The more promptly the investigator reaches the crime scene the greater possibility to find and retrieve valuable and better-quality evidence and investigative leads. [2] OR The "Golden Hour" of forensics,a term indicating the limited period immediately after a criminal offence where collection procedures are most effective-encompasses a critical point when, unless evidence is gathered and examined thoroughly, critical information could be erased or contaminated.

Among these reasons, you can also find a remote possibility to get lost, get corrupt or even be deleted or wiped completely. As for now, the official manuals which have a structured methodology for processing each type of evidence either U.S. Department of Justice [2] and even NIST [1], do recommend us to collected evidence physically, send it to forensic center, etc. Currently, the on-site, and the investigation Van there can be quite some tests in an early stage of process for any type of evidences, so you can differentiate your physical-bio-chemical analysis on any evidence at site, the phenolphthalein test for any sample which looks like blood ,ELITE Cards for explosive examination [3], However; there is lack of support system in current available methods to

support for real-time data or information during the "Golden Hours" in distributed, mobile or remote cases where it is required to preserve our precious digital forensic evidence. With rising digital threats, globalization of crimes it becomes necessary to have a robust system for handling real-time crime and information with remote acquisition capability and secure evidence trail. [4]
To overcome this issue, the research herewith is presenting an end-to-end approach that helps digital evidences during the golden hours by developing an integrated framework consist of a specially developed remote acquisition script, automated script for cryptographic hash-based verification, and secure file transfer directly into the cloud environment that allows forensics team to perform acquisition of digital evidence on-scene. This version tightly links the urgency and specific challenges of the Golden Hour to the research objectives and clearly defines the paper's contribution in addressing a critical gap in digital forensics.

The contributions of this work are summarized as follows:

- Proposes a practical framework for rapid disk evidence acquisition during the Golden Hour.
- Demonstrates secure network-based transfer of forensic images with integrity verification.
- Evaluates feasibility using low-cost hardware suitable for field deployment.
- Aligns the methodology with existing digital forensic guidelines and chain-of-custody requirements.

The flow of paper goes like this:
Section 2 covers the background of digital forensics, its evolution, and different fields of digital forensics. Section 3 covers various guidelines and frameworks used by different organizations and institute for handling digital evidence and its acquisition, analysis, examination, and reporting. Section 4 describes the lacunas and challenges in existing infrastructure with respect to the Golden Hour of crime incidents. Section 5 covers the proposed methodology that describes the framework step by step and practical implementation under available resources (open source and free).

Background

Digital forensics can be described as a discipline whose technology components seem to change constantly. Nearly everyone agrees; the meaning of the term digital today is changing from year to year, as smart watches, cellphones, rings, and glasses become overnight ubiquities. Needless to say, it is natural that due to these changes, defining and implementing digital forensic investigation approaches also changed along with them.
Figure 1 reveals that digital forensics already extends and branches out over several sub-disciplines. Indeed, the swift progress of technology demands that both researcher and law enforcement rethink their investigative approaches to digital evidence. Fakhouri et al. Highlighted this need as, "The function of digital forensic investigation of extracting, Analyzing and scrutinizing the electronic content device has also developed into one of central significance as we grow more digitally intertwined with every facet of life [5]."
As the majority of the scholars agree, "The digital forensic investigation processes consists of a series of steps; involving identification, collecting, and acquiring electronic evidence from a source; subsequently to examination, analysis and then report writing which generally involve a number of scientific procedures and protocols and methods [6–10]." Nikkel stated that Digital investigations were entirely science and based on prove that techniques were used [11]. Most typically the traditional conventional forensics processes contain Six Steps [2]: Identification, Collection, Acquisition, Examination, Analysis and Report writing. Of all the six steps, the first three (Identification, Collection and Acquisition) occur generally at the scene of incidence, whereas the remaining steps (Examination, Analysis and Report writing) occur at the forensics lab. In the study our main focus is acquisition from mobile devices during Golden Hour, when is the best time to seize incriminating evidence so the evidence stays free of further corruption till the point it goes in court of justice which is an unexplored issue for research. As mentioned previously in Fig.1, we focuses in to the issue of Disk forensic and acquiring electronic data from storage devices like smartphones, laptops, tablets or PC's. Smart Phones etc most of devices store their useful information either internal or external memory, from which data transfer processes called either taking an image of either logical or full disk data (entire physical bitstream) from the source. But this data must remain free of being alter so in order to overcome these challenges technical and procedural control must be implement to ensure the data integrity through all procedures by investigators that will also prevent loss of evidence, Photographing or videography the storage media when collecting the evidence; sealing the drive, labeling it carefully and maintain all-round a Chain of Evidence Documentation and by applying and using some Hash value technique through hashing which ensure the evidence never to alter.

Existing Infrastructure

Disk forensics plays an increasingly important role in most criminal investigations, as most digital devices

(whether computers, mobile phones, or portable storage media) store indispensable and often irreplaceable information on internal or external storage media, like disks and USBs. In today's society, people often possess these portable storage media, forcing law enforcement officers to collect, store and analyze the data from them at different points of time during the criminal investigation. As a storage medium often contains sensitive information, log data and user traces, it is crucial to collect data very quickly and securely, especially during the first 60 minutes after discovery of an incident, where this information is likely to be lost, deleted or altered. Thus, the following research is primarily intended to provide solutions to the first responders facing problems with the acquisition of disk-based evidence. The author conducted literature review on available guidelines and procedures for first responders to act upon the discovery of any digital evidence at crime scene, however have narrowed down my scope to digital forensics in regards to the disk and USB storage.



Figure 01: Different streams of Digital Forensics

Many guidelines are available to address this problem but fail to meet the immediate needs in a highly time-critical 'Golden Hour' situation of acquiring disk-based evidence. Most of the available procedures describe fundamental processes, are generic regarding electronic evidence, or primarily focus on the post-incident collection and transportation protocols, which do not fully satisfy the demands of immediate action under difficult circumstances.

In 2008, The "Electronic Crime Scene Investigation: A Guide for First Responders" was published by the U.S. Department of Justice which highlighted critical phases in collection and transfer of digital evidence. Divided into seven chapters, the guideline touches upon electronic devices, different types of crime scenes and key principles related to electronic evidence, which include ensuring that evidence does not get modified during the collection, transportation or storage and is handled by only trained and professional persons, and also that it is properly documented to ensure the chain of custody. This guide strongly emphasis on use of correct procedures and tools to maintain the data integrity, to conduct a thorough investigation at the forensic lab [12] But, this guide like most others mainly focuses on physical preservation and post-collection processes with inadequate attention to technical and logistical challenges associated with immediate collection of disk and USB drive at crime scene in relation to a very strict time constraint.

In 2015, The Digital Evidence Guide for First Responders, published by Massachusetts Police Department, guides on appropriate handling of electronic devices in the crime scene to make evidence admissible in court. It guides on photographing/sketching of evidence, disconnecting devices from network by Airplane Mode or using Faraday bags, maintaining the physical and digital integrity of the evidence, securing passwords, chain of custody, and transfer of evidence to the Digital Forensic lab for analysis. Author also recommends obtaining help from certified forensic experts for further investigation[13].However, this guide also doesn't fully address the issue of speed and potential for alteration at this stage with respect to disk-based evidence or any network attacks.

In March 2021, INTERPOL Guidelines for Digital Forensics First Responders was launched as an overarching set of guidelines to be followed for the secure handling of digital evidence. It briefs how to find, collect and preserve digital evidence to assure its admissibility in the court. Following are some of the critical recommendations to use in case of any electronic evidence found; use of certified and authorized tools, maintain chain of custody,

documenting each step involved in collection, etc. They also recommend to use highly skilled personnel for handling the evidence during the transfer to the lab[14].Even then, the issue remains about transfer of physical evidence to centralized labs which could increase the response time further.
In 2023, the UN Practical Guide for First Responders, published with details on effective forensic procedures on handling and collection of electronic devices at crime scenes under challenging situations divided the crime scene procedures in four parts (Stage 1 - Arrival at the Scene, Stage 2 - Triage of digital devices, Stage 3 - Collection and packaging of digital devices and Stage 4 - Transportation). In every phase, it emphasizes on maintaining chain of custody, integrity of evidence, adapting best practices in forensic investigations, preventing tampering of evidence using Faraday bags, proper documentation and safe transfer of devices for analysis[15].Despite all these features, it primarily deals with handling any digital device and doesn't emphasize any specific methods for imaging disk or USB at the crime scene.

By 2024, SWGDE aka Scientific Working Group on Digital Evidence, came out with "Considerations for Required Minimization of Digital Evidence Seizure" which focuses on best practices for limiting the seizure of digital evidence during investigations. It talks about balancing of privacy concerns and the need to preserve legally relevant information and other critical evidence as well as the need for efficient utilization of resources and legal and ethical standards.16 It also does not address the crucial aspect of fast and forensically sound disk imaging at the crime scene as it mainly focuses on reducing the amount of evidence taken.
Another method by Samus Ciardhuin[17] involved 13 steps intended for law enforcement agencies. These steps were designed to facilitate the transfer of digital evidence via network rather than traditionally because it was assumed to be "more feasible in case of digital devices and more faster and safer to transfer the digital evidence compared to traditional method". This approach foreshadowed the demand for network-based evidence transfer currently highlighted as an important aspect for disk imaging, however it was never applied as a standard procedure. Immediately following, Rogers et al.18 proposed the Cyber Forensic Field Triage Process Model (CFFTPM) which would efficiently reduce the overall investigation time through an effective on-site triage method of the digital evidence. The pragmatism and the inclusion of a chain of custody are some of the major advantages to the mentioned process.
In 2017, Formal Two Stage Triage Process Model (FTSPTM) by Montasari [19] was introduced. It divided the process in two major phases: The planning phase and the on-site examination phase. In the planning phase, there were a variety of considerations mentioned before heading to a crime scene, like legal, data constraints and physical constraints (divided into sub-phases), and after a plan is devised, you are ready to visit the scene for the on-site procedure which resembles the CFFTPM, emphasizing on the importance of acting quickly at this critical "Golden Hour" in order to bring significant changes in the speed of the investigation. Both mentioned models emphasize on the criticality of early on-site action but, due to the specialized nature of disk data, more work has been conducted with regards to what and how should it be transferred at the crime scene under specific time constraints.
In 2018, Dimpe et al. Introduced a set of Generic Digital Forensic Requirements consisting of ten phases as shown in Figure 02. The acquisition and collection phase are discussed and evidence transportation is given as a task[20]. The digital forensic findings must be recoverable for producing admissible results in the court[21].
In 2021, The NGDFIM framework was proposed by Akash et al[22] it was designed to cater forensics of any kind of devices and also addressing the extra tasks of big data analysis and privacy protection in the entire procedure.In summary, while many well-established guidelines and models exist to guide evidence handling at crime scenes, clear limitations persist in their ability to deliver timely, secure, and forensically robust acquisition of disk evidence during the Golden Hour. Existing protocols tend to prioritize general process over device-specific needs, and often lack the practical tools and frameworks necessary for first responders to quickly image, validate, and preserve disk-based data before it is lost or compromised. Addressing these gaps through innovative methods for disk acquisition forms the central objective of this research

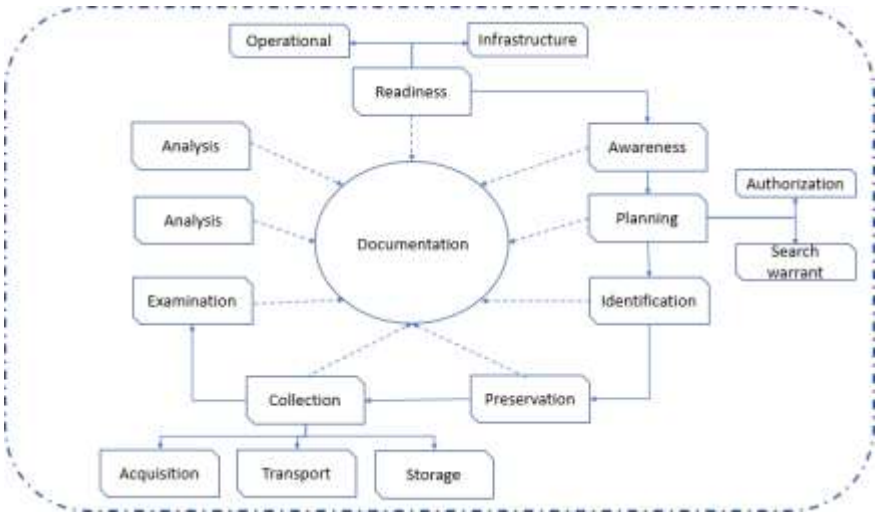


Figure 02: Generic Digital Forensic Framework

Challenges in existing infrastructure

Even after having many different guidelines around the globe, Dubey et al. asserted that DF faces key challenges, including the complexity of data and its volume, a lack of standardization, and inadequacies in the power of existing tools to support investigations and issues related to timelines. [23]

Standardization in digital forensics holds considerable importance, affecting the consistency, reliability, and legal admissibility of forensic findings. Despite the progress made in establishing professional practices, the field worldwide still lacks universally accepted standards that can guide investigators and ensure the quality of forensic outputs. [24]

Digital forensics has undergone a significant transformation, evolving from a specialized field into a comprehensive discipline encompassing various subdomains. Each sub-discipline addresses unique challenges within specific digital environments by; employing tailored methodologies and tools. An overview of these subdomains is provided below

For instance, Unmanned Aircraft Systems (UAS) are electronic devices that first responders might be directed to retrieve on a battlefield. Terrorists can rig a UAS with explosives to target first responders attempting to handle the device at a combat scene, or may use it for a secondary strike once responders arrive at a blast location. In 2016, a UAS detonated when military personnel attempted to examine it after it reportedly crashed, resulting in the deaths of two soldiers and injuries to two other soldiers. First, responders need to be aware of the potential dangers linked to digital devices abandoned on the battlefield, such as explosion risks, adversaries' tracking capabilities, and other factors that could endanger their safety. [15]

4.1) Risk during transportation:

UN Guidelines highlights risk of transferring digital evidence from crime scene to lab, it mentioned "While in transit, the transport team should be aware of the risks of transmitting digital devices. The transport team MUST never unpack the collected digital devices because they can expose themselves to terrorists, who might continue to track the devices. Unpacked digital devices can transmit signals, expose transport locations, record conversations, and transmit data to an unknown hostile location. In turn, this can lead to targeted attacks, exposure to the transport route, and facility location.

Unpacking cell phones; that have not been concealed can record the team's faces and transmit this data to the cloud. The transport team should also be aware of the risk of self-exploding devices such as batteries, powerbanks, cellular phones, and take necessary precautions." [21]

Séamus Ó Ciardhuáin [17] conducted participation activities of Police and Law enforcement officers in Ireland and asked them to rate the relevance of 13 steps as per their Investigative Techniques. Two steps that he was unable to define well were "Transport" and "Storage." He even stated that " The transport and storage activities were considered to be of no relevance, because at present they are essentially trivial, consisting of the removal and storage of PCs, disks, and similar material. Currently there is no use of network transport for possible digital evidence at present. However, the participants agreed that this was likely to become an issue of concern in the future as the scope of the investigations became larger. "

4.2) Time is a crucial factor during Golden hour of investigation

The golden hour of investigation—the initial phase after a crime is discovered—is critical for preserving digital evidence. Digital artifacts such as volatile memory (RAM), network logs, and live sessions are often transient and can disappear with system shutdowns or overwrites. In addition, delays increase the risk of data tampering, encryption, or erasure by perpetrators. Acting promptly ensures evidence integrity, supports chain-of-custody requirements, and aids in timely investigation. The golden hour is crucial for forensic investigators to effectively secure actionable insights.

4.3) Man-Power Requirements

Almost all existing frameworks show one common issue:- the requirement of skilled personalities at crime scenes, and recruiting professionals is troublesome for organizations. This issue can be diminished by hiring professionals or by providing specific technical training to current employees.

Proposed Methodology

The earliest stages of forensic investigation are crucial for preserving evidence integrity and ensuring a successful outcome. Securing, documenting, and maintaining the chain of custody are essential steps. Without these early actions, evidence can be altered, destroyed, or inadmissible in court, thereby compromising the investigation. Organizations must anticipate digital threats, have up-to-date knowledge, and have well-defined procedures in place. Regular training, quick access to forensic experts, and the latest tools and techniques are essential steps for preparing for potential incidents. This allows organizations to act swiftly and decisively, increasing the chances of a successful outcome while minimizing the impact of the organization. Section 5 outlines the proposed methodology, "Next Generational Digital Forensic Imaging Framework." The proposed methodology has been designed after extensive research and comparison of various frameworks available on the Internet and Research Repositories, as well as with studies of various SOPs and frameworks used by several law enforcement agencies across the country. The author has found few lacunae in all studies that are constrained by various circumstances or the availability of resources. The proposed Methodology focuses specifically on digital evidence (disk/storage media). An elaborate graphical representation is shown in Fig.5.

The methodology is strongly helpful in the Golden Hour of any crime scene investigation.

The golden hour of a crime scene refers to the critical time window immediately following an incident, during which digital evidence is most vulnerable to loss, modification, or encryption. Rapid and forensic sound acquisition of digital evidence is essential to ensure legal admissibility and integrity. This methodology provides a structured approach by integrating forensic imaging, cryptographic verification, secure cloud transfer, and chain-of-custody management, ensuring that the evidence remains unaltered and court-admissible.

This framework aims to provide an investigation method where digital devices are involved, to perform fast, reliable data acquisition in the golden hour, transfer the forensic image via the network channel, and upload them to secure cloud storage where a forensic expert can access it through proper authentication, post analysis, and examination; a report has to be made and it will remain attached to forensic images on the cloud server. The same case file, along with the report, can also be accessed by Higher Police Officials and the judiciary system via secure authentication, leading to a fast and secure process overall. This methodology is quite resilient in investigations in which there is an acute shortage of time. It is divided into two main parts: 1) at the crime scene, and 2) at the command and control centre.

At the crime scene

The most critical and intense period of any investigation is the Golden Hour, which includes reaching the crime scene, understating the nature of the crime, exploring the possibilities of evidence found at crime scenes, and its relevance to the crime committed.

The presence of digital evidence, if combined with the presence of biological evidence, makes the case stronger in the court room; thereof, whenever we search for any digital evidence, wet evidence must be collected before seizures of electronic devices.

Even after seizure and acquisition of digital evidence, the process itself becomes so long that it may consume a critical time period and intensive labor. The authors believe that, in the era of this technology, this can be reduced with the application of 5G integration, as it provides good connectivity between the two digital entities. With the integration of systems such as the Raspberry or Jetson Nano Kit, the cost can also be reduced significantly.

At the command and control centre

The second part involves examination, analysis and reporting components of any investigation.

The methodology begins with preparedness, which includes a basic setup such as sanitized hard drives for evidence imaging, sophisticated forensic imaging tools, and other peripherals that will be required. In the

proposed methodology, the author used an in-house experimental setup based on programming languages and Raspberry Pi, and the motivation for the same has been taken from (Brick-Fire Project). The use of Raspberry and in-house programming will promote a safer and more efficient alternatives for all the law enforcement agencies that prioritize confidentiality while lowering costs.

NGDIF Workflow:

The proposed methodology is a systematic multi-step process that ensures the basics of digital forensics. A Raspberry Pi enabled by a Unix-based OS is topped with many fine scripts and secure codes that enable it to create an exact image/replica of any USB storage device connected to it irrespective of its file type. (NTFS, FAT32, EXT4).

In workflow step1 demonstrates the preparedness of digital kit (charging batteries that will be used to run Raspberry Pi in remote locations, keeping buffer sanitized digital storage devices, such as (hard drives or sophisticated SSDs).

Whenever any relevant storage media (here, source drive) is found at the crime scene, it can be directly connected to Raspberry Pi, which will enable the operations and a screen to appear with the calculation of metadata of the source drive.

Post calculation, it will ask for the destination location of Forensic Imaging:

1. Legacy (ofline data storage), which is a conventional method used to date, and eventually the Destination Hard Drive, can be sent to the forensic lab via the traditional method.
2. Command and Control Database (Secure Cloud Platform)

In this case, the imaging process will begin, the Raspberry Pi will create a secure tunnel to the cloud platform, the image will be created in chunks to maintain bandwidth, and real-time forensic images can be created in various formats such as E01 (Expert Witness Format),DD (Raw Image), or Advanced Forensic Format (AFF). This stage confirms that all files, hidden partitions, deleted records, and unallocated spaces we are preserved for further analysis.

As soon as the imaging is completed, the software checks for its integrity by verifying the hash values. Upon successful verification of the hashes, the file was saved with case details on the cloud platform.

An analyst from the C&C team can take up the case at any time, as the availability of the cloud platform is 24 x 7. In this case, the forensic image is downloaded to the PC of the analyst with case details, and further examination and analysis can be conducted according to the requirements of the investigation. Post Analysis a Forensic report will be created by an analyst that will be required in the courtroom. This forensic report can then be attached to the original Forensic Image file saved in the C&C database. A separate web portal serviced with authentication can be used to log remotely for the relevant police officials as well as for the judiciary system, even the same can be archived for future perspectives.

This methodology will not only save crucial time of investigation, but also timely acquisition, examination, and analysis can be helpful in saving human lives in cases of terrorism, and human trafficking.

The use of a secure cloud system will reduce the risk of any physical damage, data tampering, or unauthorized access, with electronic evidence providing a sense of security to law enforcement agencies. The entire process can be documented with a timestamp that will facilitate the chain of custody for future reference

The whole methodology is explained in Figure 000 for a better understanding, it is divided into 7 steps, briefing of each step is given here:

Step 1: System readiness and detection of evidence on the crime scene (Step 1):

The system is kept prepared before any event by charging its battery and wiping the high storage hard disk/SSD.

When crime information is received, the potable system is brought on the crime scene and looks for digital evidences.

If wet evidences like fingerprints or biological evidences are present on the digital device, they are collected by the on-site investigator.

Photography and videography of the crime scene is done by the on-site investigator.

Step 2: Device connection and imaging (Step 2):

The digital device containing the evidence is connected to the system of the present invention through USB and the case details are filled in through the user interface of the system.

This is followed by initiation of imaging of the digital device for which the source drive, which is to be imaged, is chosen.

If source drive isn't found, the digital device is again connected to the system to search for the source drive,

following which the destination drive is chosen.

Step 3: Choosing the destination drive (Step 3):

After choosing the source drive, the destination drive is chosen, which may be any among:

Legacy/Conventional Method/Ofline imaging – wherein imaged data will be saved in external connected hard drive/storage for later analysis

Command and Control Centre - wherein imaged data will be saved to online secure cloud storage portal along with hash verification

Step 4: Data imaging (Step 4):

The source data in both the cases is imaged with metadata and hash calculation and the user can change the data format (DD, E01) as per requirement, following which the
image is ready.

Step 5: Hash calculation and verification (Step 5):

The images of data for both the destination drives are hash calculated and the hash is verified.

In both the types of data storage if the image isn't hash verified, the digital device is re-connected and the steps of data acquisition and imaging are repeated.

The hash verified image of data is saved to the hard drive and is ready to be transported for analysis, in cases where the imaging is done ofline, while the hash verified image of data is saved in the central database with desired format, in cases where the imaging is done online by the command and control centre.

Step 6: Forensic image analysis (Step 6):

The data image saved on the central database in the desired format is accessed by the digital forensic analyst, which if not ready for analysis, is again accessed by the analyst for analysis.

When the data image is ready for forensic analysis, it is downloaded in the local drive and is hash verified.

If the hash verification isn't done, the image is again downloaded and is hash verified.

After hash verification, the digital forensic analyst examines and analyzes the image.

Step 7: Reporting (Step 7):

After forensic image analysis, its report is generated, which if not generated, again image analysis is done and report is generated.

The generated report is saved with respective forensic image in the central database.

This central database portal has access for higher police officials, judiciary officials and archived cases.

Experimental Set-up:

We used various hardware and accessories to implement the proposed methodology. Setup begins with A Raspberry Pi 4 B Model, a single board computer equipped with 4GB RAM, 15 W USB C-type power supply, 1 Gigabit Ethernet Port, 2 x USB 3.0 Ports, 2 x USB 2.0 Ports, 2 x Micro HDMI ports that support two 4K displays along with 40 GPO Pin attachment slots for small on-board screen attachments.

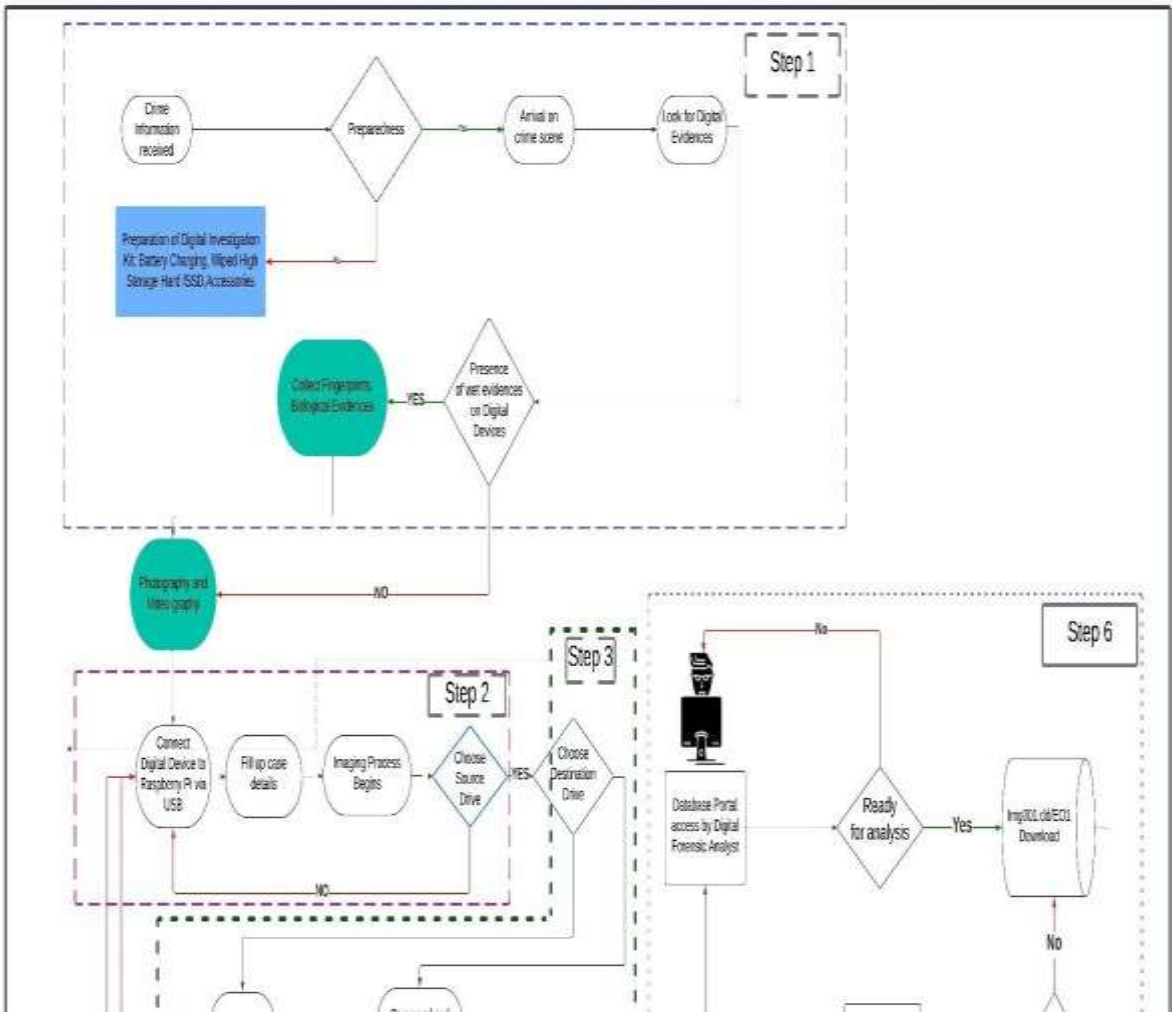


Figure 03: 7 step work flow NGDIF framework.

There are a variety of single-board computers available, such as Jetson Nano Kit and Odroid XU-4, which can be used as good alternative options, but here we use Raspberry Pi 4 because of community support, price (to keep it low cost), and features such as additional connectivity ports and direct support for display.

Hardware Accessories:

1. 32 GB SanDisk Memory Card
2. A multi-USB port hub.
3. 3.5 Inches touch screen
4. Internet Dongle
5. 20000 Mah Battery Power Bank
6. 1 x 8 GB SanDisk USB Pen drive
7. 1 x 1TB SanDisk SSD
8. 1 x Bluetooth Keyboard and Mouse Pair

Software:

1. Ubuntu 24.04 LTS (nicknamed as Noble Numbat)
2. 1 x Google drive account.

Testing Framework:

A 32GB SanDisk Memory card was wiped using sophisticated software, and a customized Ubuntu Linux (with minima resource pack to keep it light weight) was installed as an operating system.
Python-based code was written to call out different open-source libraries and handle all the operations of the process.

A known data-set was created with 2 x WEBP files, one MP4 Video file, one MS Word Document, one MS Excel document, one PDF file, three-JPG Images, one BMG File, and one GIF file, constituting a total of 11 files.

After creating the dataset, all files were hashed, and the data were saved separately.
To simulate a crime scene, an 8 GB SanDisk Pendrive is considered a Digital Device that can be found at any crime scene. To begin with the acquisition, one has to simply power the Raspberry Pi equipped with a 32GB memory card running a customized Linux and 1TB SSD in the Destination port.
All USB ports are classified as either source or destination to avoid any confusion. As soon as we plug in a USB in the source port and run the program, it shows us multiple options for image acquisition.(dd, E01,RAW, dmg). Note: The proposed framework is designed to be format-agnostic at the conceptual level and can be applied to common forensic image formats such as RAW (dd), AFF, and DMG. However, the current prototype implementation and experimental evaluation focus exclusively on RAW (dd) and e01 disk images.
As soon as the user selects the desired format for image acquisition, it starts calculating hashes of the entire source drive in SHA1 and MD5 formats. The program always checks for available storage in the Destination Disk as shown in Figure 04.

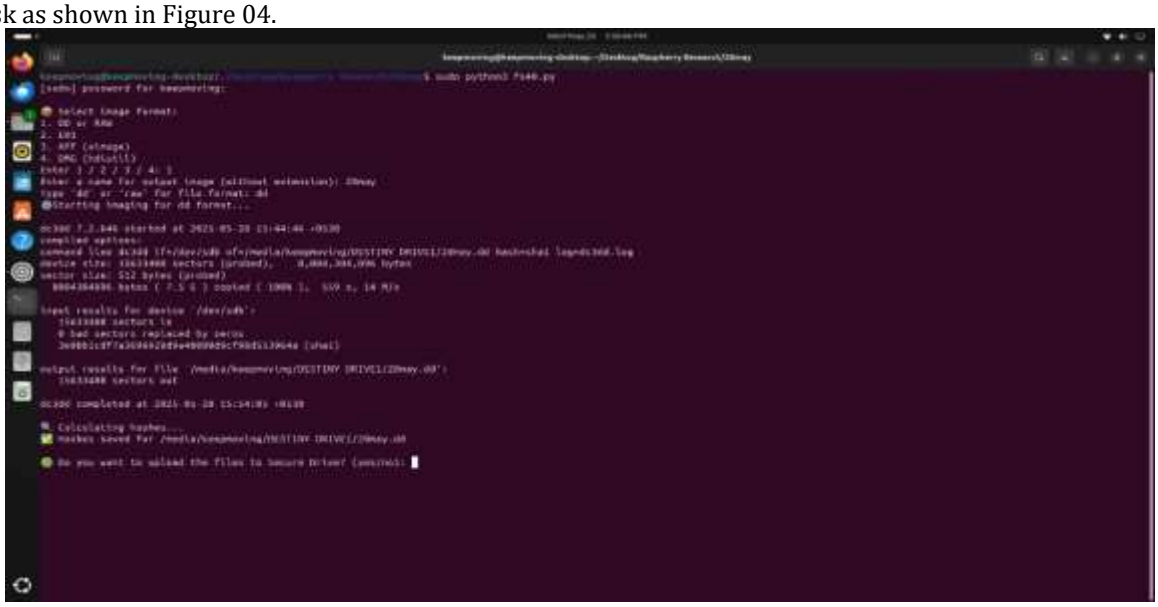


Figure 04: Screenshot of the forensic imaging interface showing prompt for image format.

The moment image acquisition is completed, the program again asks the user to secure upload to cloud storage. Upon approval, it authenticates a secure connection with a cloud storage and uploads the forensic image to a remote server, as shown in Figure 05. Completion of data transfer can be seen in Figure 06. Upon completion of the data transfer, it can again verify the hashes of the image stored in the drive. Figure 07 shows the presence of an uploaded forensic image at the cloud portal, where an analyst can download the forensic image and can verify the integrity by checking on hash values on his/her local workstation and can perform analysis.

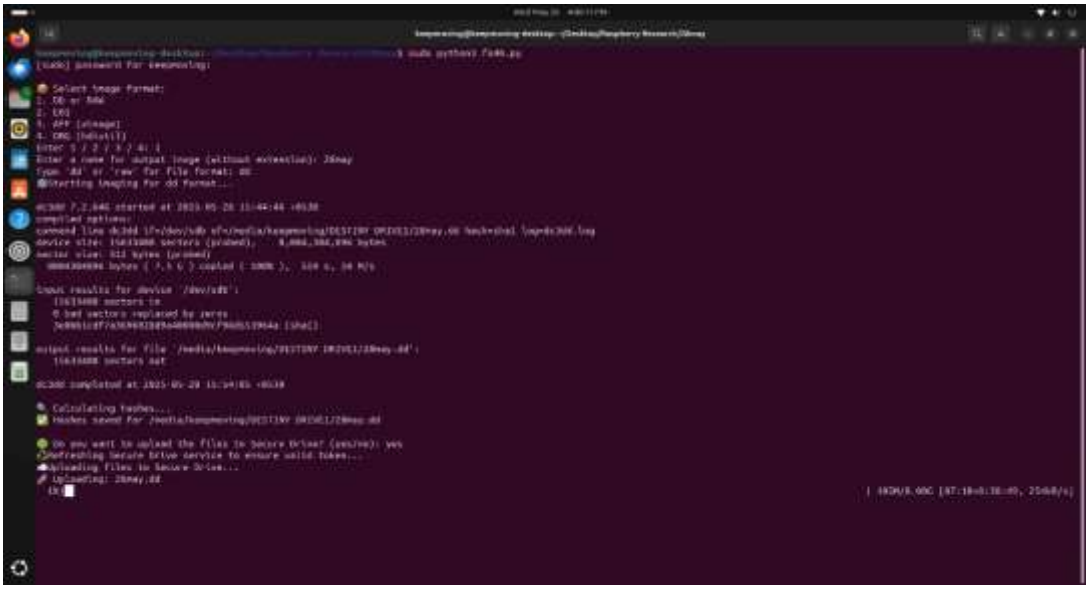


Figure 05: Screenshot of the forensic imaging interface showing prompt for secure cloud transfer and upon approval it starts uploading the forensic image with live status progress bar.

The author tested forensic images for their integrity and found that the hashes that were calculated before imaging, and after imaging (saved in cloud storage, were the same. Various software packages were used to calculate the hashes like FTK and Quickhash.

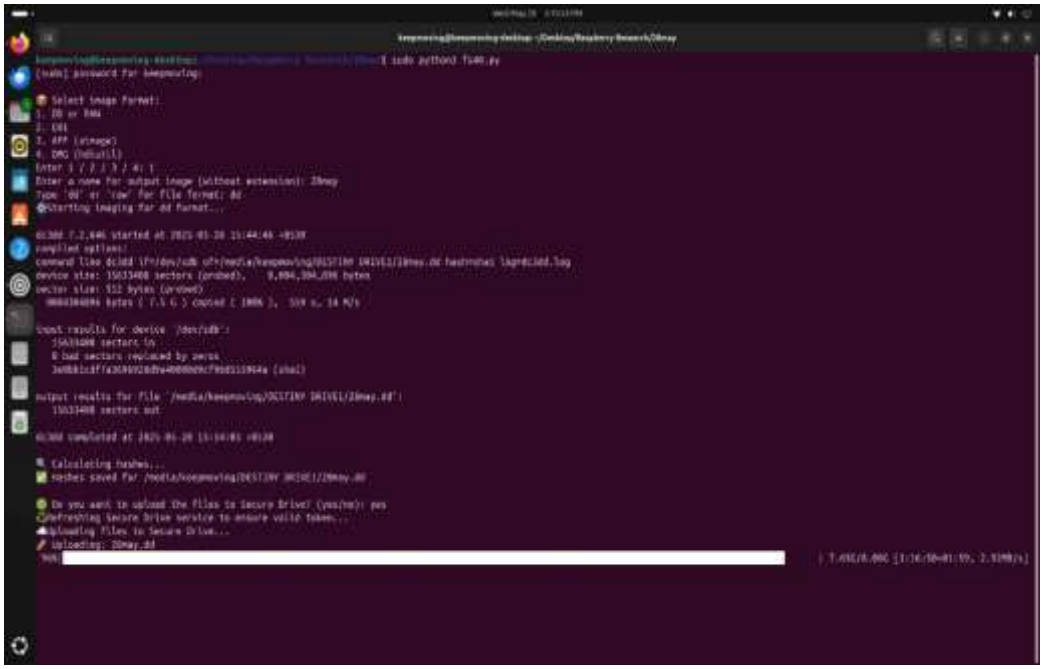


Figure 06: Screenshot of the forensic imaging interface showing completion of data transfer with live progress bar.

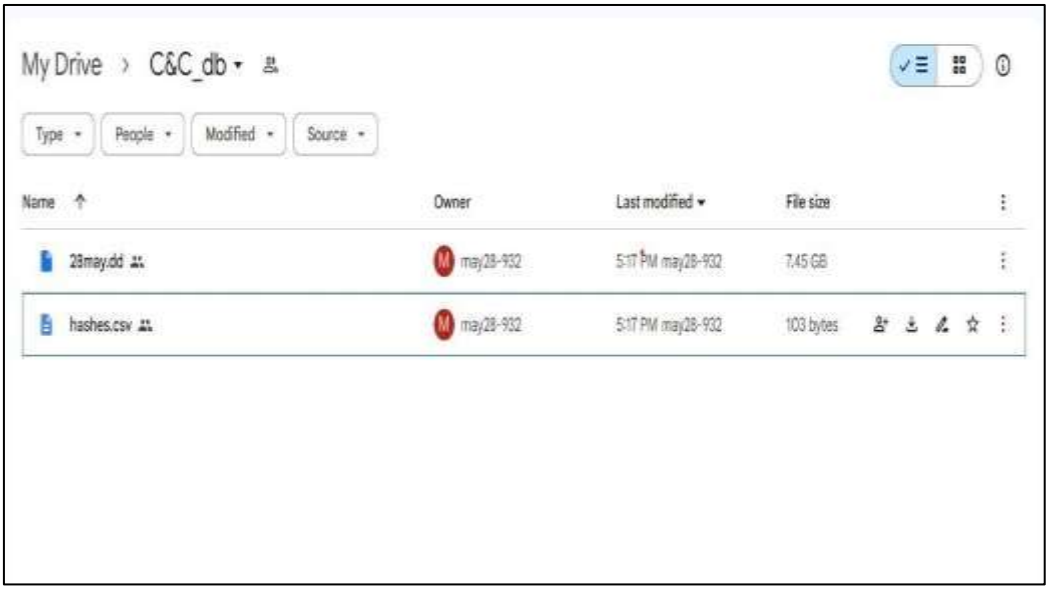


Figure 07: Screenshot showing uploaded image along with hashes stored in csv file at secure cloud storage named as C&C_db.

Similarly, it can be done for image format e01, which is one of the most advanced forensic image formats and widely accepted by tools for analysis. Figure 08 shows the selection of the e01 format rather than dd format. E01 format files can be chunked into desirable sizes (by default 1.4gb) and the hash value of each chunk will be calculated and saved for further references.

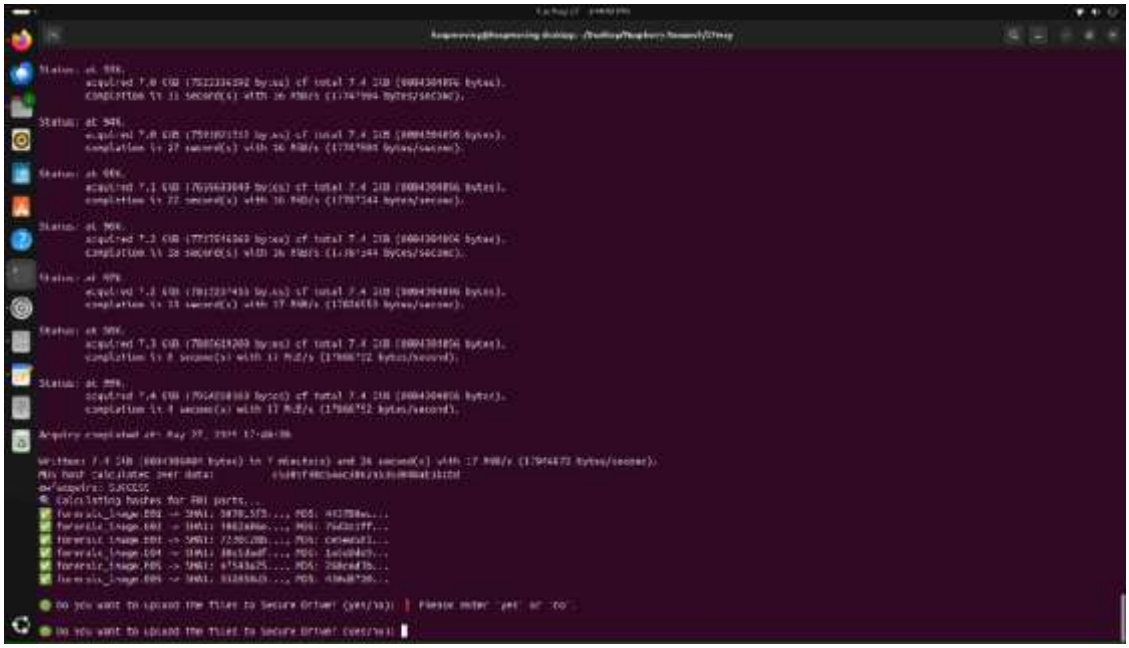


Figure 08: Screenshot showing uploaded image along with hashes stored in csv file at secure cloud storage

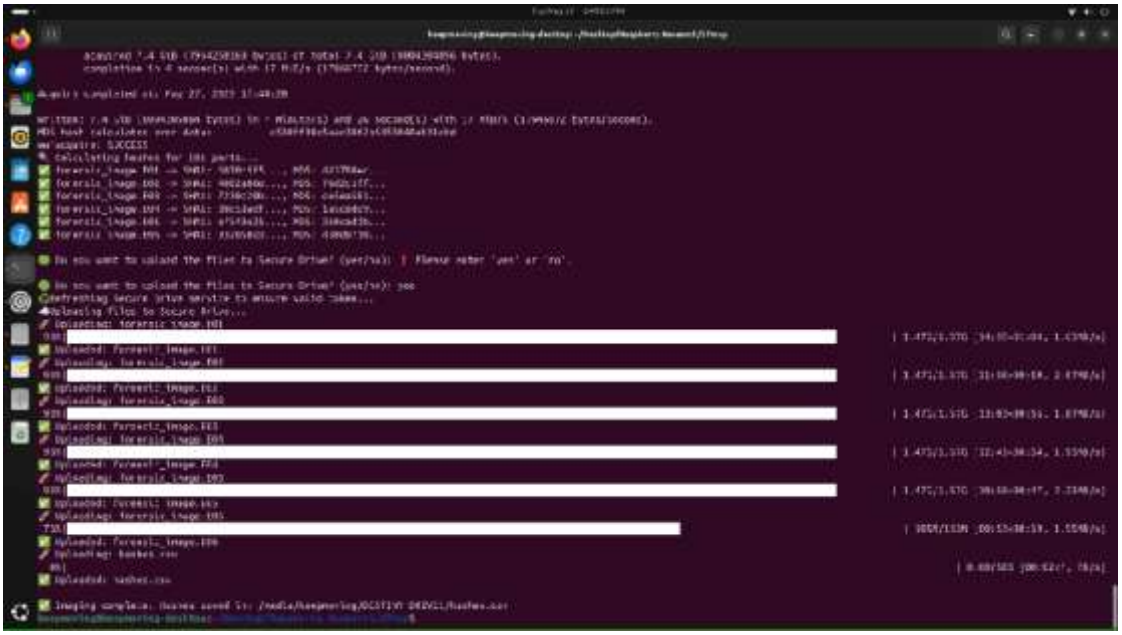


Figure 09: Screenshot showing uploading of chunked e01 images and hash file to cloud portal with progress bar.

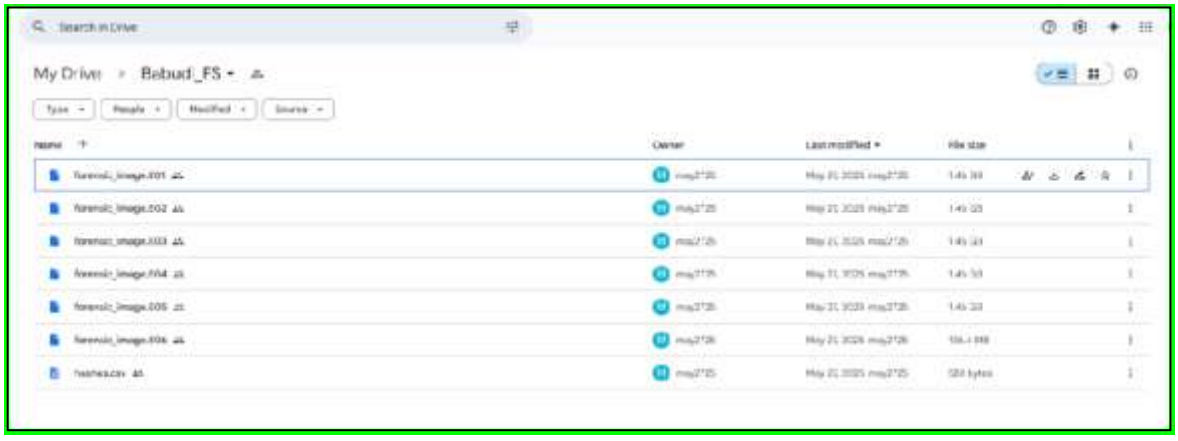


Figure 10: Screenshot showing uploaded image along with hashes stored in csv file at secure cloud storage named as Babudi_FS.



Figure 11: Screenshot showing side by side comparison chart of hashes derived from different software (Proposed methodology, FTK Imager, and Quickhash in order).

Conclusion

This study presents a comprehensive approach to digital evidence acquisition and secure transfer during the Golden Hour. The proposed methodology provides a structured, scalable, and legally compliant approach to digital evidence acquisition in the Golden Hour. By integrating indigenous forensic imaging tools, cryptographic verification, secure cloud storage, and proper chain-of-custody procedures, this methodology ensures that digital evidence is collected efficiently within the golden hour while maintaining forensic integrity and supporting the judicial system. Future work will include expanding the framework to IoT devices and encrypted storage systems to further enhance forensic capabilities.

The entire process consumes around 2-3 hours (may vary as per internet connectivity), whereas traditional methods may take up to 2-3 days, providing an edge while working in the golden hour of any crime scene.

Future Work

Future advancements such as AI-driven forensic analysis, blockchain-based chain-of-custody management, AI-based triage with considerations of privacy issues, and real-time remote imaging will further enhance digital forensic capabilities in crime investigations. The proposed framework can be enhanced by integrating 5G technology with new digital devices. Extending the implementation to additional forensic image formats such as AFF and DMG is identified as future work and can be achieved without modification to the core acquisition and secure transfer workflow."

Acknowledgement

The authors would like to express their gratitude to the Centre of Excellence in Digital Forensics at the National Forensic Sciences University, India, for providing the technical environment and equipment utilized to create and test the solution.

Declarations

All authors declare that they have no conflicts of interest.

References

1. Eoghan Casey. 2011. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd. ed.). Academic Press, Inc., USA.
2. Anni Pues, Towards the 'Golden Hour'? A Critical Exploration of the Length of Preliminary Examinations, Journal of International Criminal Justice, Volume 15, Issue 3, July 2017, Pages 435–453, https://doi.org/10.1093/jicj/mqx024
3. https://www.llnl.gov/sites/www/files/2020-05/elite-STR-Oct-06.pdf (accessed on 60
4. June 2025)
5. https://www.exterro.com/resources/white-papers/filling-the-void-the-importance-of-remote-

digital-forensics-in-contemporary-cyber-investigations. (accessed 20 March 2025)
6. H. N. Fakhouri, M. A. AlSharaiah, A. k. Al hwaitat, M. Alkalaileh and F. F. Dweikat, "Overview of Challenges Faced by Digital Forensic," 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2024, pp. 1-8, doi: 10.1109/ICCR61006.2024.10532850.