QUBAHAN TECHNO JOURNAL
VOL. 3, NO. 3, July 2024
https://doi.org/10.48161/qtj.v3n3a41

Computer Forensics: Evolution and Its Pivotal Role in Modern Investigations

Muazam Ameer

[1] Sibling Academy of Quality Education, Bahawalpur Pakistan

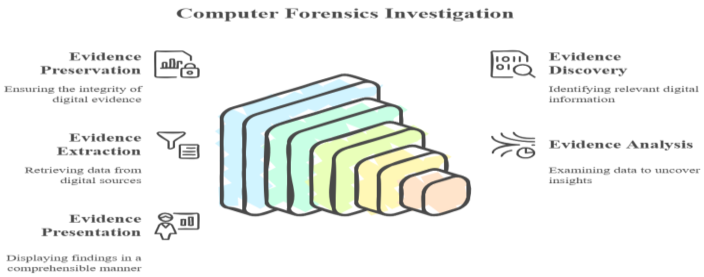
* **Corresponding author:** Muazamameer252@gmial.com.

ABSTRACT: The preservation, identification, retrieval, documentation, and evaluation of laptop facts are the honest primary goals of computer forensics. Many computer forensics guidelines and approaches that want to be described and established are tested in this have a look at. Data have to be undamaged and available for evaluation. Authenticity of the information is likewise guaranteed. As a end result, pc forensic specialists extract and take a look at facts from storage devices used on the scene of a digital crime the usage of contemporary strategies and device. Examining some of these forensic technologies is the number one objective of this take a look at. The aim of the cutting-edge take a look at is to evaluate and comparison the key variations and similarities across the extraordinary forensic equipment as a way to determine which characteristics need to be progressed for effective garage device autopsy.

Keywords: computer forensic, data retrieval, integrity of data, data analysis, forensic policies autopsy of storage devices, data evaluation.

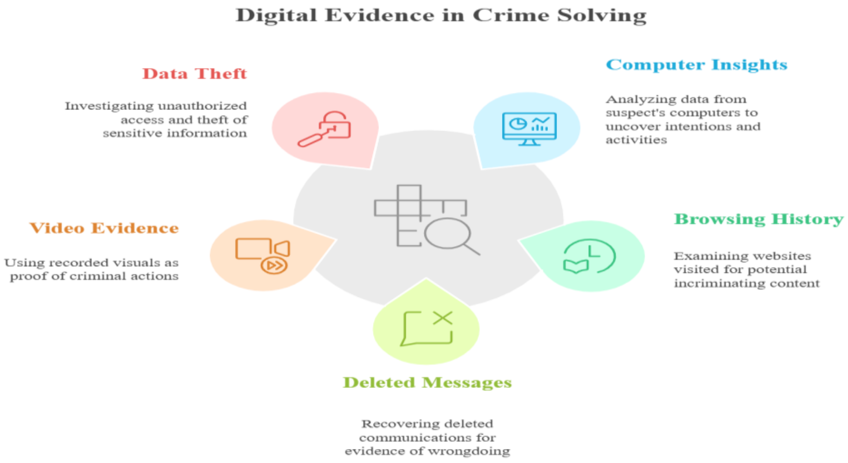
I. INTRODUCTION

In the modern world, Governments, personal organizations, and even the general human beings now have access to ever-increasing computer strength. Examples of this unexpectedly developing electricity include growing networking capacity, a huge variety of latest Internet packages, virtual distribution and e-trade systems which includes Valve Corporation's Steam, and community-on hand transportable devices which includes PDAs and cellphones. The capability for coordinated cybercrime, which may arise at any time and everywhere in the global, is big with these new equipment.[1] The introduction of what's typically referred to as a "global village" is the result of the fusion of computing era with international net connectivity. Some customers inevitably take gain of the lack of regulation in the internet's broadly speaking unregulated and moderately policed environment. This results in a range of illicit activities, including purely digital crimes, such as hacking an identity theft, as well as offences that bridge the gap between the virtual and physical worlds, such as fraud, cyber stalking, and other forms of misconduct that have tangible real-world consequences.[2]


Computer Forensics Investigation
Evidence Preservation
Ensuring the integrity of digital evidence
Evidence Extraction
Retrieving data from digital sources
Evidence Presentation
Displaying findings in a comprehensible manner
Evidence Discovery
Identifying relevant digital information
Evidence Analysis
Examining data to uncover insights

Data fraud, forbidden clothing, exploitation of babies and illegal downloading of hacking on data structures are usually some crimes that consider in the spring when we think of data -related crimes. However, the condition of digital witnesses changes more regularly, and extra common is further in crimes related to investigation and new traditional prosecution. This is the maximum important element. This is the shape, although it does not include:

- Homicides: Many carefully organized strategies are required by using virtual forensic to clean a murder case, all of which may be intended to gather virtual evidence with the intention of gaining fair insight into important crime. The purpose of this technique is to find out the substances that can be used to be aware of the suspects, rebuild opportunities and join them in Crooks. A suspect's computer can give us valuable insight into their games and intentions. Browsing history can also examine visits to websites discussing ways to kill or hide our bodies, such as emails or live messages exchanged with the victim before the crime can be probative in need of evidence.[3]
- Rape: Digital evidence also plays an important role in rape investigations. They bragged to their friends about Internet research about the rape, deleted text messages in which the suspects bragged and a video recording of an assault on them on mobile phones has also served as incriminating evidence
- Fraud: Cyber fraud is an increasing number of regularly related to standard fraud schemes, although it is regularly visible as a awesome type of crime. Computers are regularly implicated at one stage of fraud, and new forms of fraud have surfaced. These encompass identification robbery, which can be achieved by using maintaining a watch on electronic mail correspondence, and corporate information robbery, which can be as clean as connecting a small memory tool to a PC.[4]


Digital Evidence in Crime Solving
Data Theft
Investigating unauthorized access and theft of sensitive information
Computer Insights
Analyzing data from suspect's computers to uncover intentions and activities
Video Evidence
Using recorded visuals as proof of criminal actions
Browsing History
Examining websites visited for potential incriminating content
Deleted Messages
Recovering deleted communications for evidence of wrongdoing

II. THE OVERVIEW OF THE COMPUTER FORENSIC

The phrase "computer forensics" changed into at the beginning utilized in a 1991 training session held in Portland, Oregon, by way of the International Association of Computer Investigative Specialists (IACIS). The renovation, discovery, extraction, and writing on paper of virtual proof are the primary topics of this look at. It bridges the gap among clinical methodologies and prison ideas, just like other forensic disciplines. The use of scientifically established methods and methods for the protection, garage, admission, presentation, evaluation, interpretation, recording, and presentation of digital evidence from computer systems is known as pc forensics. Significant advancements had been made, leading to a boom in a variety of in your price range computing techniques that put performance and productivity first. Although it isn't unknown to unauthorized users or attackers, laptop forensics has surmounted the difficulties related to forensic equipment and methodologies and concentrated on building effective, reliable forensic centers.[5]

Because the Tool X uses similar algorithms, it can effectively remove hidden information. Therefore, the goal of this study is to check the possibility of using Tool X in forensic research to highlight the hidden information entered by other devices using similar stenographic techniques and algorithms. The study will be conducted in a real environment, and the findings should open new routes to investigate the field..[6]

III. METHODOLOGY

Cybercrime refers to the modern phenomenon which includes computer fraud, theft of intellectual property or confidential information, harassment, vandalism of websites, unauthorized or misuse of website, any crime related being about using computers They are well equipped.[7] The Internet plays an important role in modern life because of its widespread use. A wide range of internet writers developed as an important platform for business operations, including accounting, software development and hardware technique. As a result, these cyber criminals often work with impure, especially because of their reputation to the digital landscape and the regulatory structure and the current interval in the implementation. Due to the lack of oblivion and lack of solid legal examples, the internet is still exposed to the internet.[8]

Although forensic software tools have many properties available, disc photos and hashing are the main emphasis of this research. Since searching for the original archives is never appropriate, a disc image in forensic studies is an important function. The evidence is retained as imaging maintains the integrity of data on the original storage unit. The results of the investigation may not be acceptable in court if the integrity of the depot is threatened, which will enable defense lawyers to fight justice in the legal system. To ensure that the mirrored tube is a real copy, hash functions are important. These two important applications are thoroughly examined in sections that follow. [9]

IV. DISK IMAGING

Creating an accurate copy of hidden equipment during the study is the main goal of electronic forensic analysis. This illustration should be an ideal duplicate of origin. It is important to stop the suspect or the owner immediately from the computer that can put the resources of the storage unit at risk. A copy of the plate is located in each location, and the resulting image is compressed in a file for forensic reasons. In this way, disk congestion is formally described.[10] Because equipment is used, the image is guaranteed to be real and untouched. To start from a acquired image, the original geometry can be reproduced if necessary, so that the image is not to match the physical size of the original storage unit. Forensic analyzes depend a lot on accuracy, integrity and safety. Guidelines for appropriate disc methods are provided by the National Institute of Standards and Technology (NIST). This is the proposal for this guide. The program will produce an image or bit-stream copy of the original record or division..[11]

- The original plate cannot be replaced by the tool.
- The integrity of the disc image file should be tested using the tool.
- Any I/O defect must be recorded by the tool.
- Documents for the tool should be accurate and wider.

V. HASHING FUNCTIONS

A hashing function H, the variable H generates the hash value h, that is a fixed-duration string, given the input m. The integrity of the facts is assured by means of the hash cost, which serves as a completely unique identifier. The fundamental techniques hired by using forensic equipment to guarantee the renovation of the unique media and its image documents are called hash functions. The subsequent sections provide descriptions of two popular hashing algorithms: Secure Hash Algorithm (SHA) and Message Digest 5 (MD5).[12]

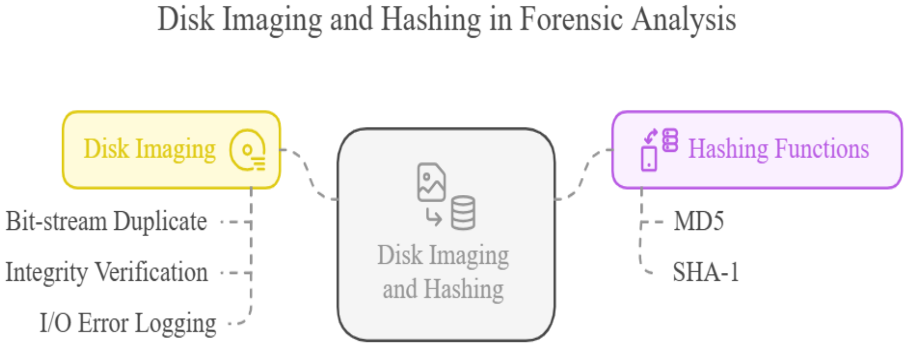
VI. MESSAGE DIGEST 5 (MD5)

MD5, which was created by using MIT Professor Ronald L. Rivest, produces a 128-bit hash cost, also known as a message encryption. Similar to how a fingerprint is particular to someone, this digest is made to be particular to an photo document. It is "computationally impossible" for two wonderful sets of enter to provide the equal hash end result, claim the Internet Engineering Task Force (IETF). Additionally, Rivest proven that searching two messages with the identical hash cost might require kind of 264 operations, while looking a message with a specific hash value might require 2128 operations. Because of these traits, MD5 is a honest hashing technique for forensic programs.[13]

VII. SECURE HASH ALGORITHM 1 (SHA-1)

Based at the same thoughts as its MD5 predecessor, MD4, SHA-1 is a lately famous hashing set of rules. When processing input information fewer than 264 bits, SHA-1 yields a 160-bit hash price. Similar to MD5, SHA-1 is regarded as stable because it's miles statistically not possible to find two awesome files that generate the equal hash or to discover facts that matches a particular hash value.[14]

The many judicial gear can be blanketed in the following sections, at the side of an analysis of the way properly they paintings to accomplish those essential duties. Because specific gadgets have distinct running systems and because mobile devices are already a part of a international social community, forensic professionals try to focus their cellular cellphone search [15]



VIII. MOBILE DEVICE FORENSICS

It is challenging to test the smartphone for forensic purposes. Due to continuous updating of data and activities, smartphones can quickly cause lost evidence. Second, most smartphones are the operating system (OS) closed sources, with a remarkable exception to the Linux-based smartphone. This makes forensic challenging to create a customized tool to restore evidence of sensors, and since smartphone providers need to release OS updates, many have made it challenging to follow the necessary tests and procedures. It is challenging to test the smartphone for forensic purposes.[16]

The processing of social networking site content on computer systems and the technology to help extract it also formed part of the scientific research. The art of the. Zellers looked at specific data tags built into several pages of Myspace source code and used them to create targeted artifact keyword searches. [17]

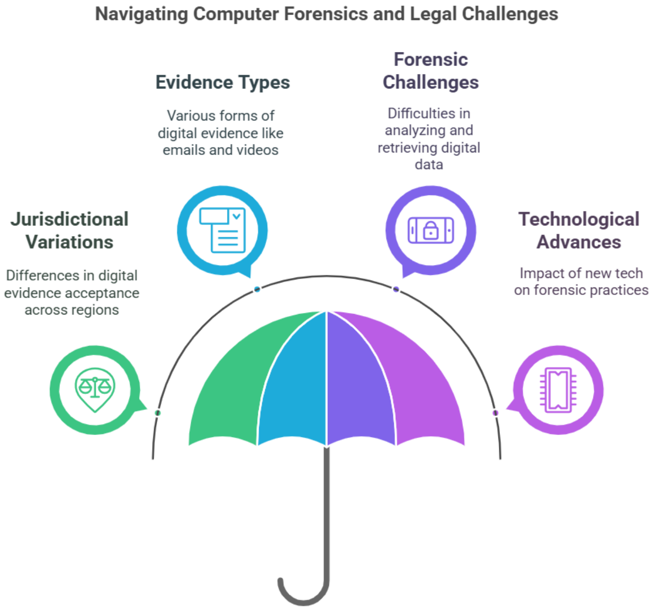
Due to the development of many social networking programs, mobile phones are used for social media today. By using web pages, forensic investigators can detect relevant data on a suspected mobile device. A database related to Facebook activity is located in RAM on the iPhone 3GS, which is in accordance with the forensic analysis that uses logical procurement. Each friend's name, ID number and phone number are included in the database.[18]

IX. IDENTIFYING LEGAL ISSUES RELATED TO COMPUTERS:

The phrase "legal" (above) is right now related to this topic. But the main cognizance of "computer drainage problems" is on the problems that stand up from differences. Judge legal guidelines had been handed in court. Commonwealth and all impartial state legal guidelines vary with regards to the presentation and access of records reviews. These effects are in a situation wherein the court's geography is assumed to be that the proof is widely wide-spread or now not. This is crucial, due to the fact some worldwide websites can receive the distribution of digital proof, others won't be. In addition, each nation has its very own set of regulations related to precise types of virtual evidence, along with e -put up, Microsoft PowerPoint displays, video recordings and registered proof.[19]

Security-associated technology and perhaps even Particularly those bearing on forensics have the ability to significantly advantage people and beautify their best of lifestyles. However, that technology can also be employed for subjection and tyranny. Computer safety and computer forensics have made considerable use of computational intelligence (CI) techniques, such as fuzzy common sense, evolutionary computing, and synthetic neural networks.[20]

X. CHALLENGES FACING IN COMPUTER FORENSIC ANALYSIS


Navigating Computer Forensics and Legal Challenges
Evidence Types
Various forms of digital evidence like emails and videos
Forensic Challenges
Difficulties in analyzing and retrieving digital data
Jurisdictional Variations
Differences in digital evidence acceptance across regions
Technological Advances
Impact of new tech on forensic practices

There are several difficulties with regards to forensic analysis of laptops and mobile gadgets. Accurately analyzing and obtaining pertinent evidence is turning into increasingly tough due to the growing availability of virtual records. Encryption, which prohibits decryption without a key or password, is any other crucial barrier.[21] When accounts are dispersed over several computers or garage web sites, report fragmentation makes restoration and reconstruction more tough. Forensic specialists need to constantly improve their statistics and gadgets because of short advancements in hardware, software, and similarly encryption processes.[22]

The technological talents and garage of cellular devices have extensively multiplied. Over the past 10 years, the capabilities and talents of cell gadgets have converted them into facts repositories that have the capacity to shop an extensive quantity of private and organizational statistics. [23] The field of cell device forensics has grown dramatically in recent years. The forensics investigator should quick get right of entry to the minimum quantity of facts that older cell phones ought to maintain. Despite the development of smartphones, forensics experts can nevertheless extract an enormous quantity of records from the device; but the strategies for doing so have grown extra intricate.[24]

XI. RESULT AND DISCUSSION

It is clear that forensic research requires a common language. One of the reasons for electronic forensic analyzes behind other forensic areas lacks between doctors and academics. Consequently, electronic forensic medicine is mostly lacking science, which is an important aspect of forensic studies. Finally, like other areas such as DNA analysis, where science and mathematics around experimental accuracy are well established, being able to express problems on both sides will help to develop a scientific process in Cyber forensic.[25]

Problems that can be resolved whilst forensic experts and computer Forensic scientists collaborate by using comprehending one another's goals, growing thorough models of rules and techniques, placing the ones policies into area, and adhering to methods:

- To what extent is the facts generated accurate?
- How specific is the analyzing technique?
- From the data, what inferences can be made?
- What presumptions are required so that you can make such claims?
- How may the quantity of assumptions required to apply data be decreased?

Forensic data processing is becoming more and more common in civil cases, especially in cases related to digital discovery, intellectual property (IP) questions, statistics security and labor law. Forensic investigators aim to understand specific concerns about the collection of records and storage of digital evidence in criminal investigation. As a result of the application being used at any time on the purpose or in a calculation system, the electronic items can be replaced or removed. Given that electronic information has been created, converted or removed during regular computer operation, a risk is that modifications may occur from an inappropriate or flawless virtual forensic technique.[26] [27] [28]

REFERENCES

[1]. Lin, X., *Introduction to Computer Forensics*, in *Introductory Computer Forensics: A Hands-on Practical Approach*. 2018, Springer International Publishing: Cham. p. 3-36.

[2]. Moore, R., *The role of computer forensics in criminal investigations*, in *Crime online*. 2013, Willan. p. 81-94.

[3]. Brady, P.Q. and W.R. King, *Technology and homicide investigation.* The handbook of homicide, 2017: p. 515-532.

[4]. Furneaux, N., *An introduction to computer forensics.* Medicine, Science and the Law, 2006. 46(3): p. 213-218.

[5]. Britz, M., *Computer forensics and cyber crime: An introduction, 2/e*. 2009: Pearson Education India.

[6]. Yari, I.A. and S. Zargari. *An overview and computer forensic challenges in image steganography*. in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 2017. IEEE.

[7]. Yusoff, Y., R. Ismail, and Z. Hassan, *Common phases of computer forensics investigation models.* International Journal of Computer Science & Information Technology, 2011. 3(3): p. 17-31.

[8]. McGrath, N., *A Computer Forensic Methodology*. 2005, Dublin, National College of Ireland.

[9]. McMillian, J., *Importance of a standard methodology in computer forensics.* Information Security Reading Room, 2000. 2.

[10]. Alazab, M., S. Venkatraman, and P. Watters, *Effective digital forensic analysis of the NTFS disk image.* Ubiquitous Computing and Communication Journal, 2009. 4(1): p. 551-558.

[11]. Al-Sabaawi, A. *Digital Forensics for Infected Computer Disk and Memory: Acquire, Analyse, and Report*. in *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*. 2020. IEEE.

[12]. Breitinger, F., et al. *Towards a process model for hash functions in digital forensics*. in *Digital Forensics and Cyber Crime: Fifth International Conference, ICDF2C 2013, Moscow, Russia, September 26-27, 2013, Revised Selected Papers 5*. 2014. Springer.

[13]. Mokhonoana, P. and M.S. Olivier. *Application of Message Digests for the Verification of Logical Forensic Data*. in *ISSA*. 2008.

[14]. Kishore, N. and B. Kapoor. *An efficient parallel algorithm for hash computation in security and forensics applications*. in *2014 IEEE International Advance Computing Conference (IACC)*. 2014. IEEE.

[15]. Pradeep, K., R. Soman, and P. Honnavalli. *Validity of Forensic Evidence using Hash Function*. in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*. 2020. IEEE.

[16]. Barmpatsalou, K., et al., *A critical review of 7 years of Mobile Device Forensics.* Digital Investigation, 2013. 10(4): p. 323-349.

[17]. Ayers, R., S. Brothers, and W. Jansen, *Guidelines on mobile device forensics (draft).* NIST Special Publication, 2013. 800(101).

[18]. Tassone, C., et al., *Mobile device forensics: A snapshot.* Trends and Issues in Crime and Criminal Justice, 2013(460): p. 1-7.

[19]. Brungs, A. and R. Jamieson, *Identification of legal issues for computer forensics.* Information Systems Management, 2005. 22(2).

[20]. Adams, C.W. *Legal issues pertaining to the development of digital forensic tools*. in *2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering*. 2008. IEEE.

[21]. Pichan, A., M. Lazarescu, and S.T. Soh, *Cloud forensics: technical challenges, solutions and comparative analysis.* Digital investigation, 2015. 13: p. 38-57.

[22]. Bennett, D., *The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations.* Information Security Journal: A Global Perspective, 2012. 21(3): p. 159-168.

[23]. Kebande, V.R. and H.S. Venter, *On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges.* Australian Journal of Forensic Sciences, 2018. 50(2): p. 209-238.

[24]. Khan, A.A., et al., *Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction.* International Journal of Electronic Security and Digital Forensics, 2022. 14(2): p. 124-150.

[25]. Noblett, M.G., M.M. Pollitt, and L.A. Presley, *Recovering and examining computer forensic evidence.* Forensic Science Communications, 2000. 2(4).

[26]. Jekot, W., *Computer forensics, search strategies, and the particularity requirement.* Pitt. J. Tech. L. & Pol'y, 2006. 7: p. 1.

[27]. Çiğdem Sıcakyüz, R. Rajab Asaad, S. Almufti, and N. R. Rustamova, "Adaptive Deep Learning Architectures for Real-Time Data Streams in Edge Computing Environments", *QTJ*, vol. 3, no. 2, pp. 1–14, Jun. 2024, doi: 10.48161/qtj.v3n2a25.

[28]. R. Asaad, R. Ismail Ali, and S. Almufti, "Hybrid Big Data Analytics: Integrating Structured and Unstructured Data for Predictive Intelligence", *QTJ*, vol. 1, no. 2, Apr. 2022, doi: 10.48161/qtj.v1n2a14.