An Algorithm for Crime Detection in Digital Forensics

Arpita Singh
Amity Institute of Information Technology, Amity University, Lucknow, India, arpita.singh5@s.amity.edu

S. K. Singh
Amity Institute of Information Technology, Amity University, Lucknow, India

Nilu Singh
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation

Sandeep K. Nayak
Department of Computer Science & Application, Integral University, Lucknow, India

Abstract

Digital forensics is a collection of pre-defined processes or tasks used in the course of a criminal investigation, with some technical implementation specifics shared with traditional forensics for managing and collecting technical evidence information. Although a variety of digital forensic investigation frameworks have been offered by numerous researchers and practitioners. The inquiry procedure becomes hard due to numerous technical and legal details. To break down the technological barriers that exist between investigators, information technologists, and legal practitioners, the researcher must present a technical-independent framework that can bring all of these duties together. This study emphasized a critical principle of digital forensics investigations (Obtaining authorization, documentation, information flow, preservation, collection of evidence, and evidence analysis). Based on this technique, the author defines five questions for digital forensic inquiry. An expert in digital forensics A digital forensics investigation algorithm is created by incorporating these five sets of queries. We'll go over how this new algorithm can work with legal counsel as part of a larger digital forensics investigation framework.

Keywords: *Crime detection, Cyber-crime, Digital forensics, Algorithm, Digital evidence.*

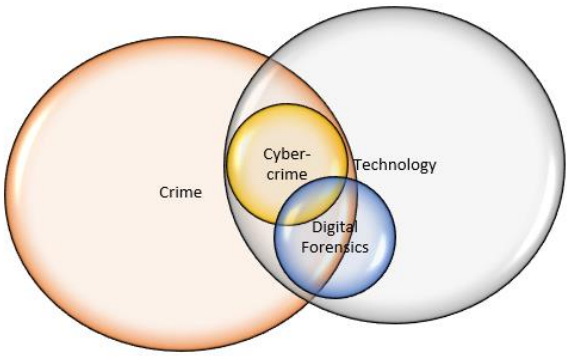
I. INTRODUCTION

When the world was combating the COVID pandemic in 2020, the world was put on lockdown, with all workplaces shut down. "Work from home" was the only choice for speeding up work. Individuals' need for digital gadgets grew as a result of this predicament. According to a study, the number of IoT connections will reach over 26.9 billion in 2026, which is more than double the number of IoT connections reported in 2020 [1]. Students, office employees, teachers, and others all have increased screen time as a result of this. A lot of information is circulating around on the internet, which these people can access using these internet devices [2]. With mobile device forensics, network forensics, cloud forensics, and computer forensics, component (hardware, software, and services), geography, and end-user vertical, the digital forensics market is expected to grow from USD 4.49 billion in 2020 to USD 8.21 billion by 2026. During the anticipated period of 2021-2026, the compound growth rate is 10.97 percent [3]. This makes

clear the photo of the future that IoT applications and devices are also becoming more prevalent on the market.

The proliferation of digital and multimedia technologies is influencing the field of digital forensics. Furthermore, the number of cases where digital evidence is relevant to investigations is increasing [5]. Due to the huge amount and volume of data available, forensic practitioners find it challenging to analyze digital evidence [5]. Furthermore, the scattered nature of cloud computing makes evidence collection problematic [7]. Law enforcement agencies around the world are experiencing substantial digital evidence backlogs as a result of the rising number of cases requiring digital forensic expertise [5]. Criminals, on the other hand, have realized that conducting cybercrime is faster and easier than traditional crime because of technology [8]. In this dynamic context, the purpose of this study is to identify the success factors as well as the key difficulties in digital forensics for law enforcement. This is performed by contrasting and comparing the research community's success elements and challenges with those recognized by digital forensic practitioners. The main goal is to find connections between them. This topic is being offered as part of a collaboration agreement between the University of Skövde and the Swedish Police's Forensic Department in Västra Götaland to conduct forensic methods research. A systematic literature review was planned, with current and available scientific literature linked to the topic of interest published between 2015 and 2021 serving as the major source of information. Similarly, the results of a survey of Swedish Police forensic practitioners will be used to triangulate the findings of the systematic literature review.

Fig 1: Relationship between cyber-crime and digital forensics



Cybercrime, digital forensics, criminality, and technology are all linked in Figure 1. It demonstrates that cybercrime is a crime that can be solved through digital forensics. This research presents a response, mitigation, and recovery plan in the event of cybercrime. The proposed solution addresses the following issues:

1. What should be the incident response approach before, during, and after the cybercrime is identified?

2. What information security policies should be implemented during an incident response?

3. What should be done right now (for example, should the investigation team will need any kind of warrant)?

4. What should be done with volatile data?

5. How might forensically sound prospective digital evidence be obtained and preserved (for example, should the computer be left on to preserve the potential digital evidence in memory)?

6. What are the options for restoring and recovering the database system while investigating?

The rest of the manuscript is organized as follows: the first section contains the problem

description as well as some basic background information on digital forensics and related keywords. The study's second section focused on the proposed Digital Forensic guiding algorithm's details, while the third section discussed legal elements of digital forensic inquiry, evidence processing, and future research for research academics.

Digital Evidence-

The use of virtual gadgets is crucial with the advent of the virtual proof. According to Vincze [8] and Kävrestad [2], each tool that shops virtual statistics may be utilized in an investigation, and virtual proof may be observed in nearly any sort of crime. The author divides offenses into 3 categories, as follows:

- Crimes with virtual proof: These are offline crimes in which virtual gadgets aren't used to facilitate the crime, however, they are able to preserve a few lines of the virtual proof. Those lines may be beneficial to tie the proprietor of a tool with a devoted crime.

- Cyber-aided crimes: Crimes are defined via way of means "the antique type of crimes thru virtual means." These are conventional crimes that employ virtual devices and the Internet as useful resource.

- Cybercrimes: Denial of provider assaults or intrusions are examples of cybercrimes wherein computer systems are used to perpetrate crimes in opposition to different computer systems.

These are some categories of crime where digital evidence can play a vital role while investigating and solving the case.

II. PROBLEM STATEMENT

The author can clearly assert that several digital forensic investigation models have been established by researchers to identify, gather, evaluate, preserve, document, and recreate evidence obtained in digital devices based on a literature review that has been mentioned in the study. The phases, language, techniques, and actions of these models may differ, but the end aim of each framework is always the same. As a result, previous research has not focused on addressing basic and critical criteria that can be effective in establishing a baseline for database occurrences. Rather, these studies have primarily focused on specific technological techniques and ideas that address specific difficulties. As a result, there is a lack of a standardized and unified incident response model that can meet the demands, report, or data sharing requirements of forensic domain practitioners. Furthermore, current models primarily overlooked the forensic soundness of any prospective evidence that could be found to support investigation assertions. Many scholars are interested in digital forensics as it has become more sophisticated. Due to the increment in technology and IoT devices, the amplified structural complexity, quantity, diffusion, and diversity of digital evidence [9], make it tougher for practitioners and investigators to identify and collect objects (which can further use as digital evidence) that can be used in a court of law [10]. Furthermore, developing technology has a significant impact on the field of digital forensics [10] asserts that the digital era's rapid transition provides both obstacles, and opportunities for forensic research?

III. PRINCIPLES OF DIGITAL FORENSIC

Digital forensic is a new category of forensic science which helps in covering all data found in digital devices while investigating and recovering that data, often in cybercrimes is known as digital forensic science [12]. There are many applications such as solving criminal

cases reported like murder, theft, kidnapping, assault against humans, robbery, etc. where digital forensics is used. It is basically six stages of investigation:

1) Obtaining authorization

2) Documentation

3) Information flow

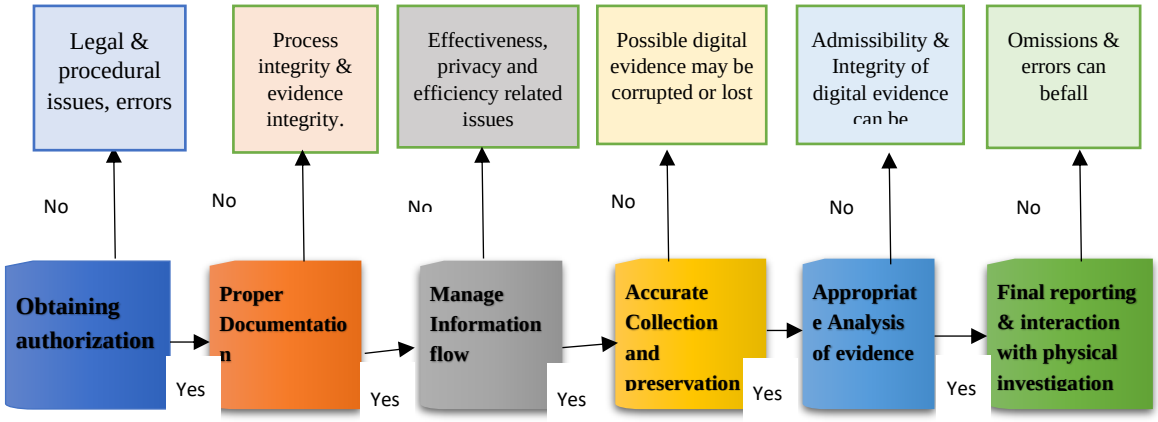
4) Preservation and collection of evidence

5) Evidence analysis

6) Final reporting (demonstration of evidence in the court of law) and interaction with the physical investigation

Investigation analysts complete their investigation with the help of available techniques which must follow all the underlying principles of forensic science and digital forensics. Collection and preservation of evidence involve all evidence collected during the investigation. And this evidence is further analyzed by forensic experts this principle will involve all stakeholders like judges, jury, lawyers, investigation officers, accused, and prosecutors. The final report will be presented in court so it must be getting organized in that manner [11].

Fig: 2 Tactic of principles of the digital forensic investigation process



• According to the first principle of digital forensics, every organization that intends to examine a crime scene must first seek authorization before proceeding. Otherwise, legal and procedural concerns may arise, and other errors may emerge during the investigation.

• The second digital forensic principle is proper documentation. Any entity that has been granted permission to conduct a digital forensic investigation must keep track of the authorization document as well as any other evidence discovered during the investigation; otherwise, questions about the investigation's accuracy and integrity may arise.

• If the digital forensic investigation team does not sustain and accomplish information flow throughout the investigation process, a privacy and efficiency conflict may arise in court.

• The investigation team must pay close attention while collecting evidence and preserving it according to the next principle, or the digital evidence that is recovered may get corrupted, or significant evidence may be destroyed.

- Digital evidence discovered during an investigation must be properly analyzed so that the results of the analysis can be presented to a court of law for justice, as per the next principle of digital forensic investigation, if the admissibility and integrity of digital evidence is called into question.

- After all of the investigation and analysis, a final report should be made, and the digital forensic expert team should engage with the physical investigation team, and data should be shared between them if errors and omissions are to be avoided.

Embedded computer systems, audio/video recording devices, communication systems, and other digital storage devices may include digital evidence. Digital evidence can be faithfully reproduced from digital devices, making manipulation or removal of evidence extremely difficult [11]. Flash drives, hard drives, phones, routers, mobile phones, GPS, CCTV cameras, tablets, pen drives, hand cameras, printers, and other digital evidence will be accepted in a court as evidence for justice, and this evidence must be credible and relevant.. During the collection of digital evidence, there have been some legal challenges for digital forensic investigators like the authentication of pieces of evidence and relevancies [11].

IV. THE PROPOSED DIGITAL FORENSIC GUIDANCE ALGORITHM DETAILS

The initial understanding of the problem, as well as the appropriate tools, are all part of the preparation phase. This step is used to get authorization and approval, as well as a search warrant and legal notification to people who have expressed concern, before developing a suitable plan. Here's a rundown of the steps involved in the planning phase. During this phase, we identified all activities/processes aimed at maximizing an organization's potential while lowering investigation costs. The investigation phase entails activities and processes involving the study and inspection of digital evidence utilizing various forensic techniques in order to determine the cause of the crime. The presentation phase includes all activities/processes that comprise disseminating the investigation's results so that a decision can be made. The algorithm steps for all these processes are given below :

Input: All 7 Phases of Proposed Digital forensic framework.

Output: Accurate and efficient reported case solution.

Begin:

//Algorithm for preparation phase

Step 1. Start Preparation Phase

Step 2. Identify /detect incidence

Step 3. Calculate possible risk assessment

Step 4. Actuate CERT & assign responsibilities

Step 5. If required to obtain search warrant go to step 6 else go to step 6

Step 6. Formulate Paperwork & onsite plan

Step 7. Select appropriate approach

Step 8. Determine the suspect’s operating system & hardware

Step 9. If got information about the suspected check with case files & move to step 10 else go to step 11.

Step 10. Determine software/ hardware required for investigation with a database of software & hardware available.

Step 11. If more information is required go to step 2 else move to the next step.

Step 12. Move to the next phase.

//Algorithm for the Extraction phase

Step 1. Start extraction phase

Step 2. Secure the crime scene's physical environment

Step 3. Secure all correlated logs, data, and volatile evidence. Laptops, hardware, and secure narrative description

Step 4. Analyze and find similar previous investigations.

Step 5. If found a similar case goes to step 6 else go to step 9.

Step 6. Study similar investigation & follow the footprint of that investigation.

Step 7. Investigation result

Step 8. End.

Step 9. Identify potential evidence and other electronic evidence.

Step 10. Try to evaluate objects on the crime scene as evidence.

Step 11. If an object is found as evidence goes to step 13 else go to step 12.

Step 12. Inscribe object & return. Go to step 23.

Step 13. Place labels over all the drive slots & Power connections.

Step 14. Take preliminary photographs of the crime scene.

Step 15. Select narration technique (written, audio or video) to delineate the search area and detect unauthorized activity.

Step 16. Validate the damage/ impact of incidence and ensure the protection of non-digital evidence like fingerprints.

Step 17. Evaluate whether any movement appears in evidence, determine devices on the network and make a complete evolution sheet.

Step 18. Observe & document physical scene, position of devices, location of devices relative to each other, condition of devices include power status.

Step 19. Check whether digital evidence has screen. If yes go to step 20 else go to step 20.

Step 20. Take written notes on what appears on screen, take snapshots of the screen and active program should videotape.

Step 21. Take photograph before and after examination of evidences. Label properly each evidence.

Step 22. Maintain and seize evidence log that include brief description and photographic log. Prepare chain of evidence.

Step 23. Start Identification & collection.\

//Algorithm for Identification & collection Phase

Step 1. Firstly check to be collected evidences are physical or electronic, If physical go to step 2 else for electronic go to step 3.

Step 2. Apply tag on Identified object & go to step 4.

Step 3. If device is running, go to step 5 else step 14.

Step 4. Fill evidences collection form & go to step 18.

Step 5. If volatile data of device required go to step 6 else go to step 6.

Step 6. If non-volatile data is required go to step 7 else go to step 12

Step 7. Perform live acquisition of volatile data else go to step 12

Step 8. If found device data is stable go to step 9 else go to step 10.

Step 9. Remove power source & go to step 11.

Step 10. Perform normal system shutdown& go to step 11.

Step 11. Decide the most appropriate way to acquire data to acquire data.

Step 12. Make duplicate copy of the acquire data and verify.

Step 13. If all required data has been acquired then go to step 14 else go to step 5.

Step 14. Seize found device if done go to step 16 else go to step 15.

Step 15. Record and return connection of device go to step 18.

Step 16. Label the evidences found then pack and pack and transport the evidences.

Step 17. Store the evidences.

Step 18. Maintain and preserve chain of custody.

//Algorithm for Examination and Analysis

Step 1. Collect unprocessed data and devices from related investigation.

Step 2. Identify operating systems used in incidence & choose data extraction techniques for examination & analysis of evidences.

Step 3. Check documents obtain by related investigation with condition of device.

Step 4. Perform physical, logical extraction and dead acquisition on data from collected devices.

Step 5. Make duplicate copies of all acquired data from electronic devices.

Step 6. Authenticate duplicate data with original one in their time stamp

Step 7. Reconstruct the extracted data from devices.

Step 8. Choose the analysis technique - Data hiding analysis, log analysis, Timeframe analysis, Application & file analysis etc.

Step 9. Reconstruct sequence of crime to produce a clear picture & try identify missing links

Step 10. Compare acquired evidence with proven facts and with physical forensic results

Step 11. Documentation & Preserve chain of custody in storage

Step 12. Store evidences in secure custody room.

//Algorithm for Reporting & presentation

Step 1. Write a comprehensive report which can understand by lay man as well

Step 2. Determine target audience and Put together evidences and preserve chain of custody.

Step 3. Present evidences according to rules of law enforcements.

Step 4. Preserve evidence for further requirement.

Step 5. Handover closer Documents, with time & date of release, to whom & by whom released.

V. LEGAL ASPECTS

Evidence dictates the truth of an issue, but its weight is difficult to assess and verify using current forms of court debate [14]. Lack of attention to the court principles governing the acquisition and use of virtual proof could render the evidence useless and expose investigators to liability in countersuits [14]. Virtual forensic proof must be taken into account within the jail situation, according to Cohen [15]. The virtual forensics technique and the work of those who use it are driven by these jail contextual issues. It is really difficult to complete the exercise properly without them. These phases of the digital forensic investigation process can be extended to correspond to the ISO/IEC 27043 digital forensic ready phase [15]. Before an incident occurs, forensic readiness, as stated in the literature, could bring a consistent strategy to prospective evidence dependability and extraction (post-mortem). Digital forensic investigation approaches and steps are being formalized and standardized for decades after the technology came into existence. ISO/IEC 27037:2012 is the International Organization for Standardization which predefine set of rules for handling digital evidence (found during the digital forensic investigation process) during specific activities such as identification, collection, acquisition, and preservation; and the NIST (National Institute of Standards and Technology) provides hands-on guidance on "how to perform computer and network forensic activities from an IT perspective" [16]. Furthermore, information and standards used by law enforcement organizations for digital forensic processes and procedures are disseminated by the NCJRS (National Criminal Justice Reference Service) [17]. Chain of custody is an important aspect of digital forensic investigation which could not be mistreatment by the investigator.

Any finding that demonstrates that the proof's information has been tampered with has a negative impact on the research and the prison processes [18]. Chain of custody is critical since it's a way to assess the quality, authenticity, and validity of the evidence gathered [18]. The chain of custody is a proof document that covers the moment it was accumulated until it reached the courts of law [19]. There is no way to assure that an object submitted to the courthouse docket is the same thing that was discovered on the crime scene, and there is no way to ensure that the expert's testimony pertains to proof without a chain of custody [20].

VI. CONCLUSION AND FUTURE WORK

This study addressed what is needed while doing a digital forensic investigation. Understanding what's required within the digital forensic investigation and having a preference that specifies that makes the investigator's job easier for investigators. The author of this work discussed digital forensic fundamental concepts by assessing some of the concerns generated by the literature review. The author presented a digital forensic investigation algorithm based on fundamental principles that can aid investigators in every circumstance. This research is based on scientific data from primary studies that addressed the research topics provided in this study. The review was conducted using a scientific technique to ensure that the results are transparent and repeatable. Finally, the scientific impact of this work is dependent on the ability to steer future research by highlighting the difficult areas that are most relevant to practitioners. In the domain, more effort needs to be done in terms of identifying success factors and opportunities. Concerning the obstacles, findings highlight the importance of taking practitioners' perspectives into

account when doing research in the field. Human-related difficulties are a topic that demands more attention and research.

Reference

Ericsson (2020, November). Ericsson Mobility Report. [Online]. Retrieved January 6, 2021 from https://www.ericsson.com/4adc87/assets/local/mobilityreport/documents/2020/november-2020-ericsson-mobility-report.pdf.

Kävrestad, J. (2020). Fundamentals of digital forensics: Theory, methods, and real-life applications (2nd ed.). Springer International Publishing. https://doi.org/10.1007/978-3-030-38954-3.

Mordor Intelligence (2021). DIGITAL FORENSICS MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2021 - 2026). Retrieved April 16, 2021 from https://www.mordorintelligence.com/industry-reports/digital-forensics-market.

Institute of Electrical and Electronics Engineers. (2016). Proceedings of the 19th International Conference on Computer and Information Technology : 18-20 December 2016, North South University, Dhaka -1229, Bangladesh., 213–217.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. Proceedings of the 11th Annual ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, Florida, 24-26 May 2016, pp. 24-26. https://doi.org/10.13140/rg.2.2.34898.76489.

National Institute of Standards and Technology (NIST) (2020, June 02). NIST to Digital Forensics Experts: Show Us What You Got. [Online]. Retrieved January 6, 2021 from https://www.nist.gov/news-events/news/2020/06/nist-digital-forensics-experts-show-uswhat-you-got.

Neware, R., & Khan, A. (2018). Cloud Computing Digital Forensic challenges. Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29-31 March 2018, pp. 1090-1092. https://doi.org/10.1109/ICECA.2018.8474838.

Vincze, E. A. (2016). Challenges in digital forensics. Police Practice and Research, 17(2), pp. 183-194. https://doi.org/10.1080/15614263.2015.1128163.

Casey, E. (2019). The chequered past and risky future of digital forensics. Australian Journal of Forensic Sciences, 51(6), pp. 649-664. https://doi.org/10.1080/00450618.2018.1554090.

Roux, C., Ribaux, O., & Crispino, F. (2018). Forensic science 2020 – the end of the crossroads? Australian Journal of Forensic Sciences, 50(6), pp. 607-618. https://doi.org/10.1080/00450618.2018.1485738.

Matthew N. O. Sadiku, Mahamadou Tembely, and Sarhan M. Musa "Digital Forensics" Volume 7, Issue 4, April 2017 ISSN: 2277 128X International journal of advanced research in computer science and software engineering

Bartosz Inglot & Lu Liu (2014) Enhanced Timeline Analysis for Digital Forensic Investigations, Information Security Journal: A Global Perspective, 23:1-2, 32-44, DOI: 10.1080/19393555.2014.897401

L. Prasad, A. Gupta and S. Badoria, "Measurement of Software Reliability Using Sequential Bayesian Technique," in in Proceedings of the World Congress on Engineering and Computer Science, 2009.

W. Chung, H. Chen, W. Chang and S. Chou, "Fighting cybercrime: a review and the Taiwan experience," in Decision Support Systems, The Netherlands, Elsevier Science Publishers, 2006, pp. 669-682.

ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes. Available at : https://www.iso.org/standard/44407.html (Access on 10 may 2022).

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST SP 800-86; 0 ed., p. NIST SP 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86.

Montasari, R., & Hill, R. (2019). Next-Generation Digital Forensics: Challenges and Future Paradigms. Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), United Kingdom, 16-18 January 2019, pp. 205-212. https://doi.org/10.1109/ICGS3.2019.8688020.

K. N. Nithesh, U. Agarwal and H. Faizal, "Use of AFF4 “Chain of Custody”-Methodology for Foolproof Computer Forensics Operation," International Journal of Communication and Networking System, vol. 1, no. 1, pp. 49-57, 2012.

J. McMillan, "Importance of a standard methodology in computer forensics," Information Security Reading Room, 2000.

S. L. Garfinkel, "Providing cryptographic security and evidentiary chain-of-custody with the advanced forensic format, library, and tools," International Journal of Digital Crime and Forensics , vol. 1, pp. 1-28, 2008.