**ANALYSIS AND STUDY ON DIGITAL FORENSIC TOOLS AND TECHNIQUE FOR CRIME INVESTIGATION**

Stuti Mohan Srivastava1 Vasudev Gupta2 Karthikeyan P3

[stutimohan.srivastava2019@vitstudent.ac.in](mailto:stutimohan.srivastava2019@vitstudent.ac.in) [vasudev.gupta2019@vitstudent.ac.in](mailto:vasudev.gupta2019@vitstudent.ac.in) [pkarthikeyan@vit.ac.in](mailto:pkarthikeyan@vit.ac.in)

19MCA0014 19MCA0011

**SITE, Department of Computer Applications, Vellore Institute of Technology (VIT), Vellore**

**ABSTRACT**

This paper is all about Digital Forensics Computer Forensics) which comprises the study of many forensics like: Computer and memory Forensics, Mobile Forensics, Network Forensics and data recovery.

Specific forensic cybersecurity and

Computer (Digital) technologies will construct the investigation procedure much simpler, accurate and reliable. They can be any tools like: software or hardware or a both which can be used in the process of investigation for a information gathering, analysis of data, report preparation, enquiry to provide a direction, and then identify some of the hardest aspects for a human being to a deal with it.They can be open source tool or proprietary tool. Some come with hardware and software packages, and some may be as an application. Few forensic tools may be required an active Internet surfing connection while others can work without.

Analyzing and preventing crime is a systematic approach for identifying and analyzing criminal methods and trends. Our system can predict areas that are most prone to crime, and visualize areas that may be prone to crime.

Some of the Digital Forensic tools are:

* Hashing Tools,
* Disk Imaging Software,
* File Recovery Program,
* Encryption Decoding Software,
* Password Cracking Software, etc.

The proposed case study was carried out on the Linux system and includes: Analysis of storage devices. Therefore, it aims to show a full criminal investigation so that end users can easily create the steps described in this work. In this review article we provide a list and description of a various tools that are helpful for digital forensic investigation procedure. This case study will be helpful in designing new strategies for crime forecasting and analysis.

**INTRODUCTION**

Computer forensics is the basically proved method for considering fragmentary and digital sayings in order to provide a credible person in line with cybercrime operations. We need digital forensic tools to successfully solve these types of crimes.

**Process of Computer Forensics:**

* *Collection:* This is a procedure which is used for gathering information and evidence with a purpose of protect the resources.
* *Examination:* This step is related to the process of detecting the crimes, related data as a proof (evidence) for the investigation.
* *Psychoanalyze:* In this process the data that is gathered in the earlier phase is analyzed with the purpose of finding a link with the person who has committed it.
* *Reporting:* It provides a result to understanding of what happened in that, and how the evidence work against the crime committer and also what the evidence meant for that.

We are looking for evidence in the crime scene investigation, which means we can find corpus delicti, crime scene and other evidence. It’s essential to know that evidence extracted in cybercrime is not always physical, as in other crime work such as fire or assault or some other crime. Evidence obtained may be inherent in the situation or may be digital. Digital proofs are basically in the form of bits and shapes of bytes. Some digital credentials cannot be accessed by opening the system. Now this important resource can be restored with the help of some accessible tools.

**Categories of Digital Forensics:**

* *Computer & Memory Forensic Tools:* Computer forensic or what we call them as digital forensic tools are used to retrieve data from a computer. They are basically used to obtain logs and encrypted data from the system. Whereas memory forensic tools are used to obtain and analyze RAM. These tools are also used to preserve resources in memory that are vanished when the system (computer) is shut down. They examine the OS and also the software which are running in memory. They run on various platforms such as Windows, Unix, Linux, DOS and Mac.
  + *Windows:* Window is sequential graphical interface OS that Microsoft has developed & sells.
  + *UNIX:* This is a multi-client PC work framework that comes in many variants. Unix is ​​made using the C-programming language.
  + *Linux:* This is a computer operating system like Unix, which is assembled under the model of free and open source software. Users may modify, create and sell their own version of the OS for its own benefit.
  + *Distributed OS:* It is an OS that provides the summary and management of secondary storage devices and the information on them.
  + *MAC:* This is a GUI based operating system developed by Apple Inc. for their Macintosh line of computers.
* *Mobile Forensic tools:* These tools include both hardware and software devices. Mobile phones come with a variety of connectors; Hardware devices support a wide variety of cables and perform the same role as a write blocker on computer devices. Mobile devices contain important personal data that can be used as a source. Data obtained from mobile phones continues to be used as evidence in criminal, civil and even high-profile cases. Mobile operating systems investigated using these tools include Android, iOS, BlackBerry OS, Windows.
  + *Android:* This is Google Incorporation which comes under the category of open source OSs.
  + *Blackberry:* This comes under the category of proprietary based operating systems.
  + *IOS:* It was developed by Apple Incorporation. It is closed source and proprietary. Apple iPhone, iPod Touch and iPad all use iOS.
  + *Windows:* It was developed by Microsoft and is a closed and proprietary source.
* *Network Forensic Tools:* These type of tools has multiple monitors that are has being installed at different locations in the network and used for network monitoring. These tools combine data from various monitors and gives a whole view of network performance.

**Types of Forensic Digital Tools:**

Forensic tools are categorized as Open Source Tools or Proprietary Tools.

* *Open Source Tools:* It is a phrase used to refer to a program that performs a specific task or operation, in which the source code is distributed freely and can be modified from its original design. These type of tools are usually developed as a joint venture in where a developer improves the code and share the changes. These tools are available at no cost under the license ltd.
  + *Tools for Computer & Memory Forensics*
    - *Categorizer Four Pictures:* This makes it possible to quickly and efficiently classify forensics segmented images. It is a mixture of forensic encryption & a complete windows application. http://www.freedownload-scenter.com/Mhttp://www.ultimedia\_and\_Graphics/Graphics\_Viewers/ Categorizer\_ Download.html
    - *The sleuth kit:* These tools are used to retrieve and analyze all delete content, hashing database, a sort based on file type and runs on Windows.

<http://www.sleuthkit.org/sleuthkit/>

* + - *Test Disk:* This tool is used to verify and remove partitions on the system. This tool runs on the Windows operating system.

http://www.cg-security.org/wiki/TestDisk\_Down-load

* + *Tools for Mobile Forensics*
    - *Oxygen Forensic Suite:* This tool is used to check mobile phones forensically and the best part of this software is that it does not transfer any sort of data into the phone’s memory plus this software runs on windows platform.

http://www.oxygen-forensic.com/en/down-load/freeware

* + - *Sim Manager:* This software is used for the purpose of retrieving phone’s contact details and the text messages.

http://www.sourceforge.net/projects/agsm/

* + *Network Forensic tools*
    - *Net-Sleuth:* It enables network hosts and devices to identify and fingerprint files from Packet Capture files stored from Ethernet or wireless fidelity data. It also consists of a live mode, which silently identify the host and the device without need of sending any packets or to a put network adapter in precise mode. It runs on both Windows & Unix operating systems.
    - *TCP-FLOW:* It captures sent data as part of transmission control protocol (TCP) connection and saves information to facilitate protocol analysis or debugging. It runs on Unix operating system.

http://www.source-forge.net/projects/tcpflow/

* *Proprietary Tools:* Tools or programs owned by owners are proprietary tools. This software has no control over any use, troubleshooting, copying or modification of the product. They can also be called *closed-source software*. They are tools charged by the seller or seller. The software is valid for active tools. The user license must be renewed when valid.
  + *Computer and Memory Forensics*
    - *Elcomsoft Password Recovery Bundle:* This software is used to protect disks, settings and encrypts folder as well as files and documents with famous applications. The tool is efficient to use in case of cost and time. It runs on Windows operating system.
    - *FTK:* This tool is used in the cases of encryption and recovery. This allow the GUI filtering functionality. The software also runs on the Windows operating system and is best tool for email inquiry.
    - *NUIX / Proof Finder:* This tool was developed with the purpose of forensic analysis and fraud prevention. It also consists of Full Text Search, IP Addresses, URLs and runs on both Windows and Linus operating systems.
  + *Tools for Mobile Forensics*
    - *ACESO KIOSK:* This helps prevent network access. Sim as well as memory card in the phone helps one to retrieve information, this also provides metadata access and stores all the information in an advanced encryption standard encrypted file.

* + - *Cellebrite Mobile Forensic Toolkits:* This is basically a mobile forensics solution based software. It includes USB and RJ45, SIM Clone and Device Extraction. The best part of this software is that it can be used in almost all type of mobile phones with various operating systems.
  + *Tools for Network Forensics*
    - *Paraben Net Analysis:* This tool works by querying we browser’s cached memory and history with a powerful search, filtering & resource identification. It runs on windows operating systems.
    - *DT-Search:* It searches for terabyte text on desktop, network, internet as well as intranet sites. It consists of special forensic search options which supports public & secure, static & dynamic web data. It also runs on Windows operating system.

**LITERATURE SURVEY**

1. *Data analysis of file forensic investigation*: [Priyanka Salunkhe](https://ieeexplore.ieee.org/author/37085849215), et.al[] presented this paper. This paper puts light on how decision tree allows the system to analyze the log information obtained through various file analysis methods effectively as well as efficiently. Finding a criminal investigator for such a crime must use a variety of methods and a logical structure to recover data. There are different types of FTK namely freeware Applications, techniques which are available for pre-file analysis.
2. *A complete study on tools and techniques for digital forensic analysis*: [Abirami Sivaprasad](https://ieeexplore.ieee.org/author/38244527400), et.al [] presented this paper, outlining the methods that can be used to detect crime in the area of ​​crime and where important information is hidden, can be sent and obtained from the captured computer network. This also presents the gifts of other tools and methods of analyzing digital crime.
3. *Digital Forensic analysis for enhancing information security*: Abdulmalik Yunusa Ade, et.al [] presented this paper for the purpose of this project to illustrate the nature of digital crime and pre-existing research and anti-crime behavior to improve security. To continue this project, the project uses various technologies and anti-forensic devices and techniques. The data analyzed were based on the simulation experiments. The findings suggest that while detecting digital crime can be difficult, it can be done with the help of forensic software / anti forensics.
4. *The Governance of Digital Forensic Investigation in Law Enforcement Agencies*: [Da Yu Kao](https://ieeexplore.ieee.org/author/37410195200), et.al[] presented this paper presenting a novel application of the TEAR-class of THOR magnitude in digital forensics. Enables efficiency and effectiveness in creating clear investigations. The amount of data on cybercrime investigations continues to increase at levels of transparency and challenge for the law enforcement agency. It poses a major threat to law enforcement agencies. Submitting digital evidence to a court of law requires a thorough consideration of all relevant information at the crime scene or lab.
5. *Digital Forensics and Crime Investigation: Legal Issues in Prosecution at National Level*: Ayaz Khan, et.al [] presented this paper introducing a modern regional model that incorporates digital technologies and similar national criminal investigations involving digital information that focus on the legal system and cyber. The paper also addresses the case of re-issue by the Hawala, as well as concerns related to the prosecution of borders and the many challenges of prosecution of these cases due to litigation and legal issues.
6. *Digital Evidence Analytics Applied in Cybercrime Investigations*: [Chia-Yang Huang](https://ieeexplore.ieee.org/author/37086608996), et.al [] explained everything about the increase in the number of cybercrime, law enforcement officials are required to investigate more cases than ever in the area of ​​technology. forensics. Due to the nature of digital activities, various types of research have been undertaken to provide different perspectives on engineering methods, concrete applications, or functional metals. The combination of these points of view is less discussed. Therefore, this study proposes an open source framework for the four sectors to solve these problems.
7. *From biometric to forensic hashing: Challenges in digital crime scene trace analysis*: [Claus Vielhauer](https://ieeexplore.ieee.org/author/37269934600), et.al [] In this paper, we present two cases of criminal use: (a) a Bio-Hash investigation obtained during the technological engineering and (b) the use of Bio-Hash in the last trace of crimes that have arisen in the domain of digital numbers. First, we emphasize the Bio-Hash architecture in two known mode of operation with their important parameter settings. Second, we analyze what ancient information can be accessed and translated into publicly available data by presenting four research objectives. Bio-Hash can be used to search for the preservation of privacy or to improve the re-appearance of features unique to criminal offenders.
8. *Electronic mail forensic algorithm for crime investigation and dispute settlement*: [Dawson Ladislaus Msongaleli](https://ieeexplore.ieee.org/author/37085500118), et.al [] explained everything about electronic mail (email) that has replaced traditional postal mail. The email service is widely used in the worldwide distribution of text and multimedia messages. The high confidence of the email service has prompted criminals to use email apps to spread malicious messages. This study presents an e-mail search algorithm for criminal investigations and conflict resolution. We introduce a three-tiered algorithm that can be used by law enforcement and other investigative agencies to identify the cause of the proliferation of malicious and defamatory emails. In opposition to existing publications, our research looks at email topics, email logs, and local device analysis. Existing publications are investigating this problem by looking at ways to analyze email headers.
9. *Data Hierarchy and Analysis for Digital Forensic Application Using Data Mining*: [Latesh G. Malik](https://ieeexplore.ieee.org/author/37294244700), et.al [] shows everything about this paper focusing on data collection from the cyber system and web browser. In cybercrime, big log data is made up of transaction data, which usually stores and analyzes large amounts of data. It is difficult for forensic investigators to spend too much time tracking and analyzing information. Network forensic analysis includes network tracking and attack detection.
10. *A Review and Comparative Study of Digital Forensic Investigation Models***:** Dale Lindskog, et.al [] this paper presents a review and comparative study of existing digital research models and proposes an improved model based on the Program for the Formal Digital Investigation Process. The paradox in digital investigations is that they often do not place enough emphasis on the admissibility of collected evidence. The model is not a waterfall model, but iterative in nature contributes to effective research and effective prosecution. The outcome of this study is expected to improve throughout the investigation process including potential litigation.
11. *Forensic Investigation Processes for Cyber Crime and Cyber Space*: B. B. Meshram, et.al [] introduced that this is about Forensic tools and resources that are an integral part of the criminal investigation used to investigate victim systems, collect and store evidence, rebuild or impersonating an event, as well as checking the current status of an event. In this paper we discuss two points; first, various types of cyber-crime and various sources of cyber-attacks, and secondly, investigative procedures for various cyber-attacks with the help of digital tools such as Win-Hex.
12. *Analysis of Digital Forensic Tools and Investigation Process*: Jayant Shekhar, et.al [] presented in this paper, we have proposed a model of investigation process for any type of digital crime. This model is simple and gives the right result for any type of digital crime and the best way to improve the duration of the investigation. We describe both the type of forensic commercial tool and the open source and the comparison between them. We also categorize digital forensic and digital crimes according to their active investigations.
13. *Computer Crime Investigations – Computer Forensics*: Joseph Migga Kizza [] introduced this paper; Understand the sciences of digital crime investigation and basic steps in digital crime investigation, understand digital evidence, learn how to manage digital evidence, find the techniques needed in digital crime investigations, find the difficulties you encountered in time for digital crime investigations.
14. *Detection of Hidden Information in Forensic Tools***:** [Jewan Bang](https://ieeexplore.ieee.org/author/37390983900), et.al[] introduced this paper, which tells us that Criminal tools are used to generate sensitive evidence in computer-related criminal investigations. Evidence has a bearing on the judgment of the court and requires the validation of pre-existing tools. Validation should require the agreement of law enforcement agencies. The Computer Forensic Tool Testing (CFTT) certification project provides assurance that the tools used in the investigation produce the correct results. The CFTT proposes requirements, verification and documentation of test cases to validate forensic tools. There are hidden details in the image obtained however CFTT is not compatible with hidden data discovery tests. Detection technologies that rely on cover management, such as images, audio, text or digitally encoded code, capture encrypted data. This paper proposes a preliminary approach to the acquisition of hidden information whether or not it is available through advance governance tools.

**REFERENCES**

[1] Ramesh Vardhan, Vimal shetty, "Digital Forensics using Data Mining", *International Journal of Computer Trends and Technology (IJCTT)*, vol. 22, April 2015.

[2] "ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification Collection Acquisition and Preservation of Digital Evidence" in, ISO Office, 2012.

[3] P. Stephenson, Official (ISC) 2® Guide to the Certified Cyber Forensics Professional (CCFP) Common Body of Knowledge (CBK), Auerbach Publications, pp. 293-404, 2014.

[4] Marrington Andrew et al., "CAT Detect (computer activity timeline detection): A Tool for Detecting Inconsistency in Computer Activity Timelines", *digital investigation*, vol. 8, pp. S52-S61, 2011.

[5] Inoue Hajime, Frank Adelstein, Robert A. Joyce, "Visualization in testing a volatile memory forensic tool", *Digital Investigation*, vol. 8, pp. S42-S51, 2011.

[6] "Dutch Police Shut down Bredolab Botnet", *Technology News Analysis Comments and Product Reviews for IT Professionals*, [online] Available: http://www.zdnet.com/blog/security/dutch-police-shut-down-bredolab-botnet/7573.

[7] Casey Eoghan, "Tool review-WinHex", *Digital Investigation*, vol. 1, no. 2, pp. 114-128, 2004.

[8] Simson, L., Garfinkel: Digital forensics research: The next 10 years. Digital Forensic Research Workshop in Science Direct, digital investigation 7, 64–73 (2010) http//doi: 0.1016/j.diin

[9] Nance, K., Hay, B., Bishop, M.: Digital Forensics: Defining a Research Agenda. In: Proceedings of the 42nd Hawaii International Conference on System Sciences, pp. 1–6. IEEE computer society, Los Alamitos (2009)

[10] Aggarwal, S., Duan, Z., Kermes, L., de Medeiros, B.: E-Crime Investigative Technologies. In: Proceedings of the 41st Hawaii International Conference on System Science in IEEE, pp. 1–10 (2008)

[11] Abdul A. A. Ghani, Mohd A Zain, Mohd Taufik Abdullah, Ramlan Mahmod, S AbuBakar Md, "Review on Advanced features of Digital Forensics", *International Journal of Computer Science and Network Security*, vol. 8, no. 2, February 2008.

[12] John R. Vacca "Computer forensics: computer crime scene investigation" 2nd ed., vol. 1. Charles River Media River media, 2005.

[13] Hamid Jahankhani, David Lilburn Watson, Gianluigi Me "Handbook of Electronic Security and Digital Forensics" world scientific publishing co. pvt. Ltd 2009.

[14] Muzammil M. Baig, W. Mahmood 1,2Muzammi M. Baig, W. Mahmood, Al- Khawarzmi Institute of Computer Science, University of Engineering & Technology, Lahore, Pakistan. "A Robust Technique of Anti Key-Logging using Key-Logging Mechanism" Inaugural IEEE International Conference on Digital Ecosystems and Technologies, 2007.

[15] L. Changwei, S. Anoop, W. Duminda, "A Model Towards Using Evidence from Security Events", *A Model Towards Using Evidence from Security Events*, vol. 10, pp. 103-122, 2014.

[16] M. Balogun, Y. Z. Shao, "Privacy Impacts of Data Encryption on the Efficiency", *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 5, pp. 36-40, 2013.

[17] A. Benjamin, "Modelling and refinement of forensic data acquisition", *Digital Investigation*, vol. 11, no. 2, pp. 90-101, 2014.