Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

Digital Forensics: Collection and Analysis of Digital Evidence to Create Stronger Security Measures

Kiran Tomar[1], Rishiraj Singh Rajawat[2], Dr. Umang Garg [3]
[1,2,3]Amity School of Engineering and Technology, Amity University Madhya Pradesh, Gwalior,
[1]kiran.tomar87@gmail.com, [2]rishirajrajawat02@gmail.com, [3]umangarg@gmail.com

Abstract— **Digital forensics (DF) or computer forensics is important when discussing and examining cyber surveillance. Nowadays, with the great advancement and progress of technology, cybercrimes are becoming more serious and our dependence on them is increasing. This is especially true during epidemics. At the end of 2020, the number of patients increased by 31 people. More people moving from offline to online has made connectivity worse. Criminals have used the opportunity to target the lack of influence and potential impact resulting from the control environment. Systems and processes that lead to cybersecurity issues. Cybercrime incidents, such as cyberattacks, can lead to the loss of important data or information, resulting in financial losses in the form of subsidies fines, or insurance from non-profit organizations.**

***Keywords*—Digital Forensics, Cybercrimes, Chain of Custody, Digital Evidence, Data Breach.**

I. INTRODUCTION

It's ineluctable that as technology advances, so will cybercrime. People who use electronic bias leave behind a variety of vestiges, traces, and imprints, just like they do in real life. These fictitious or digital vestiges may take the form of train fractions, exertion logs, timestamps, metadata, and more. Discovering substantiation from digital media, such as computers, mobile phones, or networks, is the focus of the arising field known as" digital forensics." To prop in the disquisition of crimes using technology, forensic brigades examine, identify, and save digital substantiation.

Experts in data forensics can help in figuring out how an attack passed, what damages were caused, and, in numerous situations, who was responsible for it, whether data has been compromised by a hack or lines have been translated by ransomware. Computer-related crimes were handled under laws before the 1970s. In the preceding times, regulations were created to address brand, sequestration/ importunity (like cyberbullying, happy slapping, cyberstalking, and online bloodsuckers), and child pornography as well as the variety of computer crimes that were being committed.

II. GOALS OF DIGITAL FORENSICS:

Property damage and fraud. Generally, digital evidence is created in the event log. The main purpose of digital forensics is to analyze digital media to find, recover, evaluate, and communicate facts and insights about information. The purpose of planning and enforcement is not to prevent crimes when they occur but to detect victims and perpetrators after an attack or incident layer of the system or network, thoroughly investigate and record them for future use (e.g. crime).

Computer forensics is defined as "the use of computer detection and analysis to identify legal evidence." According to Bennett (2011), legal evidence can find many types of computer crime or abuse, including viewing pornographic images of children, use of abusive language, audio or

Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

video, theft of trade secrets, and theft of applications and operating software. < br>In today's work, every application process will be run in a closed environment and the work will ensure that the application has minimal information about other application processes running on the system. Therefore, by definition, evidence generated by application activities (such as event logs) does not complete the view. The information found can be used for analysis and analysis by collecting logs or data to solve various computer crimes. Computer experts have many ways to recover data stored on a computer or retrieve data from deleted, locked, or damaged files. Therefore, the most important thing here is to determine the best way to collect digital crime evidence. The distribution of digital certificates, including the verification function, is shown in the figure.

III. TAXONOMY OF DIGITAL FORENSICS.

The growing number of CC cases has presented unique challenges to the digital forensics community. culprits are chancing innovative ways to exploit digital technology, making it extremely delicate, if not insolvable, to describe and break technology-grounded crimes. The main thing of digital forensics is to develop and apply scientific styles grounded on the conditions of interpreters to find focused short-term results. In the long term, results should be considered being paradigms but shouldn't be limited by them. introductory questions about substantiation in the digital world begin with," Can digital data itself ever give suggestions about the motives behind a crime or incident?" How do you expand your view of digital forensics from standalone computers to the web as a continuum? Profiling, relating, tracking, and arresting cyber suspects are crucial exploration questions, but can digital forensics answer the questions" Who? What? Why? Where? and when?" Will cybercrime ever have cyber substantiations?

These are some of the questions that need to be delved into to give useful results for short- and long-term use. Other factors relate to the desirable characteristics of the digital forensics ways themselves. Properties like trustability, delicacy, scalability, delicacy, irrefutability, security, thickness, inflexibility, and affordability make up a short list. All of them should be considered as generalities, designs, senses, trials, and prototypes of digital forensics tools. The below questions give sufficient provocation for serious exploration into digital forensics.

IV. DIGITAL FORENSIC READINESS:

As previously mentioned, a successful digital forensics (DFR) plan is an organization's ability to improve the evidence collection process while trying to reduce collection costs. Therefore, to achieve DFR, digital evidence must be collected before an incident occurs. DFR is one of the best digital forensics methods that can be more efficient and effective in the long run. To adopt DFR in an organization, business activities must be clearly defined and understood because each organization's business will be different.

These international guidelines set stricter standards for advanced digital search methods as well as traditional digital search methods. preparation process. This includes five processes: planning, initiation, purchasing, research, and integration. It is also linked to the research life cycle shown in Figure 1, including planning, purchasing, storage, analysis,

Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

advertising, distribution, and supply chain. Most studies focus on evidence collection and analysis, but little was done to protect the priest and his integrity. There are no good standards or recommendations for preserving the integrity of evidence, especially regarding digital forensic methods. Although it includes evidence preservation, which describes recommendations for physical storage and preservation of evidence, honest preservation of evidence is not sufficient.

Digital forensic readiness is a vital component of any organization's cybersecurity strategy. By establishing comprehensive policies, providing adequate training, and maintaining up-to-date technological infrastructure, organizations can effectively respond to cyber incidents, preserve evidence integrity, and ensure compliance with legal and regulatory requirements. Prioritizing digital forensic readiness is a proactive step toward bolstering cybersecurity and protecting valuable digital assets.

V. METHODOLOGY

Several actions need to be taken to make sure the CoC is as legitimate as feasible.

Step 1: Collect evidence of the crime or investigation in the form of a DNA analyzer, video, audio, text, images, or even recordings, along with the date and time the evidence was collected to determine the time.

Step 2: Use the saved data to update the data to help save the information. The URL is generated based on the file uploaded to it. The generated URL is extracted and used in the hashing process of the blockchain.

Step 3: The captured URL is treated as a string and hashed using a hashing technique. For added integrity, the timestamp is hashed along with the URL. The block itself contains the hashed value.

Step 4: The block and timestamp are produced. The timestamp makes it easier to determine when the proof was added to the blockchain. It will alter if there is any tampering, which results in the chain breaking. If the chain is intact, it guarantees that the block is in good condition.

Step 5: PoW is a technique to check for evidence of tampering because the connection between the blocks would have been destroyed after a given amount of time. Rehashing the existing blocks will allow you to cross-reference them with the most recent data.

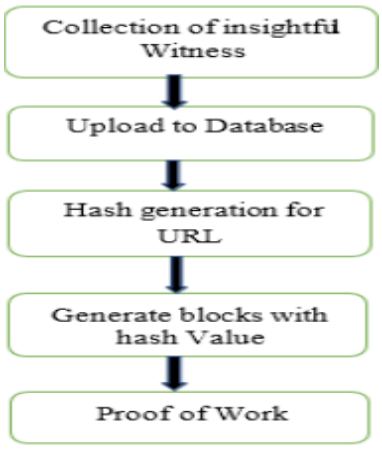

Figure 1. Flowchart of COC

Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

VI. CONCLUSION

This article provides a detailed analysis of digital evidence and reviews of digital evidence. Fields such as criminology, law, ethics, computer engineering, information and communication technology (ICT), computer science, and forensic science are included in many disciplines. teaching and coordination of digital studies. Figure 1 [8] shows the disciplines involved in the approach. It is a method of searching and analyzing electronic data to preserve evidence in its purest form. Although digital forensics is an important field among young people, more and more people are interested in this field due to their knowledge of digital forensics. It is going through a transition from a purely technical product to a scientific discipline that must be held to higher standards. Many systems are now being developed for background screening. There are now colleges and universities all over the world. All forensic science is new, and digital forensics is the newest. The discipline of digital forensics is about to transform as new technologies and trends emerge. As our world becomes digital, the importance of digital certificates in law enforcement and occupational security continues to increase. The discipline is evolving rapidly as new models and strategies are developed to meet the digital revolution.

There are also many updates available that can improve the experience and reduce the delay of results. Various developments are mentioned in this section. Therefore, testers can help improve the proposed process and ensure that the trust model meets the legal requirements of the courts. Special procedures should be thoroughly checked and checked before use. The implicit flaws and limitations of this model should be understood before use, allowing for further experimentation with the color scheme. Likewise, thinking about the truth of truth requires careful testing and verification of truth. Therefore, the only way to guarantee the growth and sustainability of digital forensics is to adopt a very good model based on good research methods and foundations. Fortunately, thanks to the power of pall computing, digital forensics for most crimes can be loaded with events such as log analysis, file indexing, and multimedia processing.

One of the most interesting aspects of pallor, in this view, implies the adoption of a new paradigm in forensic science given in mils.

REFERENCES

[1]. ” Digital Forensics Review Of Issues in Scientific Validation of Digital Evidence” BY Humaira Arshad, Aman Bin Jantan, and Oludare Isaac Abiodun, J Inf Process System, April 2018

[2]. The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security by Michael M. Losavio K. P. Chow Andras Koltay Joshua James, 3 December 2017

[3]. Digital forensics using blockchain by Dr. S. Harihara Gopalan, S. Akila Suba, C. Ashmithashree, A. Gayathri, V. Jebin Andrews, September 2019

[4]. “Improving the collection of digital evidence” available on: https://nij.ojp.gov/

[5]. “Digital Forensics” available on: https://www.packetlabs.net/

[6]. FORZA – Digital forensics investigation framework that incorporates legal issues. Author links open overlay panel by Ricci S.C. Ieong, September 2006

[7]. Studies on digital forensics for detection of computer frauds and cyber crimes by Gaurav Gupta, Mazumdar, Chandan, and Rao, M. S.,2008.

Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

[8]. "Data forensics and future visualization" available on:: https://www.sciencedirect.com/.

[9]. "The need for digital forensics, why digital forensics is important" available on: https://financialcrimeacademy.org