International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-10 Issue-3, September 2021

Maintaining and Evaluating the Integrity of Digital Evidence in Chain of Custody

Devesh Banwani, Yatin Kalra

Abstract*: *The Chain of Custody is an intrinsic part of any inspection. Maintaining and evaluating the integrity of evidence procured from a crime scene is an important part that needs to be done properly by following a certain set of protocols to make the evidence admissible in the court. Keeping track of the evidence right from the moment it was collected from the crime scene till the time it reaches court is also a major task. It is important for the investigator to know how, where and who handles the evidence during analysis at each phase in order to safeguard the integrity of the evidence. Over a period of time, various tools and technologies have been created to handle evidence. Researchers from across the globe have presented various techniques on how evidence should be handled. Many researchers have even incorporated blockchain technology with the chain of custody or life cycle of evidence to make the process stronger. The growth in this domain has been at a rapid pace. This paper presents a method on "Maintaining and Evaluating the Integrity of a Digital Evidence in Chain of Custody" using a global positioning system. The methodology focuses on the use of global positioning system tags or chips which when embedded with the collected evidence enables an investigator to track the evidence throughout its life cycle. The proposed methodology aims to help the investigators to keep track of the evidence throughout its life cycle using very basic tools like FTK Imager and technology like a global positioning system.

Keywords*: *Cyber Security, Autopsy, Forensic, Evidence, Chain of Custody (CoC)

I. INTRODUCTION

The rate of crime committed per day is increasing at a rapid pace across the world. Hackers have been attacking computers and networks at a rate of one attack every 39 seconds [16] and 81 percent of surveyed organizations were affected seriously by these attacks [16]. Over a span of a decade people have started adopting technology more and more, people find it convenient to store important documents on their laptops, phones or tablets as compared to old ways of making notes on a paper because storing information on devices becomes handy as compared to making a note on paper.

Manuscript received on September 09, 2021.
Revised Manuscript received on September 13, 2021.
Manuscript published on September 30, 2021.
* Correspondence Author
Devesh Banwani*, Department of Computing Sciences and Engineering, Vellore Institute of Technology, Bhopal (M.P), India. Email: deveshbanwani30@gmail.com
Yatin Kalra, Department of Computing Sciences and Engineering, Vellore Institute of Technology, Bhopal (M.P), India. Email: yatinkalra.vit@gmail.com

Technology has eased some processes like storing important documents but at the same time the risk factor has increased because technology is being used as an attack weapon as well by a group of people who are known as hackers and hence the cybercrime rate has increased drastically. Broadly hackers are classified into three categories.

1 Black Hat Hackers: These hackers perform illegal activities using various tools in order to steal data, destroy data or manipulate data of particular organization or organizations for money or a directed motive.
2 White Hat Hackers: These hackers are trained professionals who do the work similar to that of black hat hackers i.e., hacking into a system but these hackers have permission to do so. They are also referred to as" Penetration Testers". They perform risk assessment on organizations in order to find exploits, loopholes or vulnerabilities and report these to the concerned organization so that they can fix these and make themselves secure from attacks.
3 Grey Hat Hackers: These hackers are a mixture or hybrid between Black Hat Hackers and White Hat Hackers. They perform hacking but not with a motive of stealing, destroying or manipulating. In most cases they inform the system owner or administrator with the loopholes, vulnerabilities and exploits present in their systems. Sometimes these hackers are awarded with Bug Bounty.

It is seen that in any criminal case, digital evidences collected from a crime scene play a major role in getting to the root of the crime. To get the criminal a chain of authority must be kept up with, without keeping up with the trustworthiness in the chain of care of advanced proof, the entire examination goes to no end and consequently keeping up with the chain of guardianship of proof has turned into an indispensable part to make the proof acceptable in the court. Chain of care is the method involved with approving the number of sorts of confirmations have been assembled, followed, and secured enroute to a courtroom Maintaining chain of care implies that the proof gathered ought not be gotten to by unapproved individual and ought to remain carefully designed. It assumes continuous accountability. If accountability is not maintained it may not be admissible in the court. Nowadays law firms use chain of custody software, earlier chain of custody forms were filled (who handled the evidence, dates and times) Along with maintaining the integrity of evidence in chain of custody, two more parameters known as confidentiality and availability also need to be maintained.

Together these are referred to as CIA Triad.

1 Confidentiality: Confidentiality of an evidence is done by allotting access levels to the authorized personnel. Particular evidence is accessible to only some specific people who are working on the particular case.

For example: Evidence" A" was collected from a crime scene" B" by" Team C" and evidence" D" was collected from a crime scene" E" by" Team F". Suppose a person from" Team F" asks for evidence" A" then S/He would be denied as only" Team C" is authorized to work on that evidence and vice - versa.

2 Integrity: Integrity is the most important part of the triad as it involves protecting of data from unauthorized addition, modification or deletion.

3 Availability: Availability of the evidence collected and analyzed should be flexible. Proper reports along with the evidence should be made available whenever demanded by authorized personnel or the court.

According to [8] a proper procedure needs to be followed while maintaining the CoC. [13] proposed a framework that incorporates the use of digital evidence cabinets in order to maintain the integrity of an evidence. Use of blockchain technology [1]4 along with PoC Hyperledger [12] and Ethereum blockchain [11] is also being used to maintain the CIA Triad of an evidence in CoC. Evidence is analyzed in forensic labs by trained and expert forensic scientists who perform various experiments on evidence in order to reach closer to the criminal and finally catch him/her. During analysis a cloned copy of the evidence is used in order to maintain the integrity of the evidence, time stamp [7] is also maintained so as to keep the record of an evidence from the time it was collected from the crime scene till the point it reaches to the court. The main problem that occurs while maintaining the chain of custody for evidence is due to the lack of availability of tools and techniques used for analysis of an evidence. One of the proposed frameworks [4] works only on specific hardware which becomes difficult while implementing on other hardware. Moreover, hackers are coming up with new attack patters daily and hence sometimes use of multiple tools is required in order to defend and analyses the attack origin which is yet another challenge. To overcome such challenges new technologies like blockchain are being incorporated in the traditional tools and techniques to make the evidence analysis procedure stronger and more reliable. Use of GPS tags is the area which if embedded with existing technologies can proof to be very useful as it will allow us to track and maintain the integrity of the evidence throughout till the time it reached and becomes admissible in the court.

II. PROBLEM STATEMENT

Chain of custody is an integral part that has to be maintained in all types of crime, when it comes to cybercrime, the criminals tend to use various tools and techniques in order to commit a crime. In such cases evidences play a major role and to deliver justice to the victim evidence need to handled properly in which chain of custody plays a major role. As per the existing research, various tools and techniques have been developed. Cusic and Baca [6] have given deep insights and had even proposed a solution that used GPS technology to track the evidence. Bonomi et al. [3] and Lone and Mir [11] used blockchain technology in order to maintain the integrity of the evidence throughout the chain of custody. The existing works somewhere lack in the implementation of the proposed solutions and offer the theoretical knowledge of the subject. In this research, the researcher has offered an algorithm of the proposed technique that will allow and make the evidence admissible in the court.

III. RELATED WORKS

Cusic et al. [8] gave deep insights about the proper procedure and protocol on what needs to be followed while maintaining Chain of Custody in order to make the evidence admissible in the court. The paper lacks the technical aspect on how the chain of custody can be maintained. Handling evidence and tracking the evidence is a major aspect in order to maintain the chain of custody. Prayed et al. [13] proposed and gives a framework on how evidence can be tagged and handled once it is collected from the crime scene. The paper lacks the technical aspect how the evidence can be tracked and monitored during the transportation of it from the crime scene to forensic labs wherein analysis is done and finally it is sent for admissibility in court.

Cusic and Baca [6] proposed a framework which uses basic hash functions along with encryption techniques like asymmetric encryption, cyclic redundancy checks etc. They mention the importance of GPS technology and compare it with RFID (Radio Frequency identification) to track the location of the evidence and how they can be useful to maintain the chain of custody. The paper lacks the implementation part of the proposed technology and the framework. Ahmad et al. [1] integrates blockchain technology and stores the evidence metadata in a secure manner using a framework which furthermore adds integrity to the evidence. The research makes use of physical boxes to store the digital evidence using encryption algorithms. Since physical boxes are being used, it is possible that the integrity may be compromised or tampered as it is easily accessible. Bonomi et al. [3] used private permissible blockchain and smart contracts to increase the integrity of the digital evidence in order to make the evidence admissible in the court. The research is currently applicable only when validator nodes are fixed and validators who are willingly ready to sacrifice their privacy. Cusic and Baca [5] presented the challenges that investigators face while they maintain the chain of custody. The authors have been successful in delivering the theoretical knowledge to the readers about the process of handling the evidence. The paper fails to give solutions to these challenges and further research is needed on how technology can be integrated to maintain the chain of custody. Bradford and Ray [4] developed a framework that allowed generating specialized hash values based on time stamp using a new algorithm and existing Jakobsson's Algorithm. The hashes that are generated using these algorithms works on a specialized hardware and hence it is difficult to implement it on any other hardware. Colenso et al.

[10] delivered a framework for both Digital Forensic Investigation and Digital Evidence handling which increases the integrity and authenticity.

The paper restricts the investigating of evidence to only specific people and hence workload may increase and feature of anonymity may be lost. Cusic and Cusic [9] focused on the possible problems that may occur in chain of custody which further hampers the integrity of the evidence. As a result, if these problems arise then the evidence won't be admissible in the court. The paper fails to give a framework on how these problems or challenges can be overcome and hence decreasing the integrity and authenticity. The authors fail to answer certain answers and give the same definition. Lone and Mir [12] used Hyperledger composer to maintain the CIA Triad using Blockchain, use of this reduces the work that happens in months to weeks. The model strengthens the integrity and hence it helps in maintaining the forensic chain. The process of generating the hash values and smart contracts is manual and hence there can be a possibility of human error. Fully automated software could be more beneficial and error free. Cusic and Baca [7] focused on logging in the time stamp at each phase of forensic evidence chain i.e., right from the point of collection till the time it reaches court, a timestamp is generated using SHA/MD algorithms in order to track the digital evidence all the time. The timestamp is generated using a third-party system and hence there is a chance of data theft or errors. A more secure framework for logging in the time stamp could have been a better option instead of using a third-party system. Prayed et al. [14] focused on common problems and challenges faced while maintaining the chain of custody and gives very basic solutions on what can be done to partially manage these problems. The paper still has a scope to develop a technical framework that can be practiced in order to overcome the challenges more deeply and hence making the evidence more credible and acceptable by the court that can support the investigation process as well. Lone et al. [11] used Ethereum based blockchain i.e., each digital evidence is encrypted in various blocks and each block is linked to one another and hence integrity of the evidence is preserved till the time it reaches to the court. Loss of any block may result in losing the evidence permanently and hence integrity will be lost and chain of custody would be broken. Shah et al. [15] developed an automated tool that corrects the problems and challenges faced in FTK Imager and EnCase while evaluating the integrity of the digital evidence. The proposed tool has a drawback that the data is stored only in RAW format and hence it becomes difficult to handle for an investigator to use RAW data. Baidya and Menezes [2] gave a theoretical explanation of what "Chain of Custody" means. The paper lacks the implementation part on how evidences should be handled in order to maintain the chain of custody and hence just focuses on the clinical approach of handling the evidence using chain of custody.

Table 1: A comparison of existing research papers (R1: Uses Blockchain, R2: Satisfies Confidentiality, R3: Satisfies Integrity, R4: Satisfies Availability, R5: Framework/Tools Used)

Paper Topic	R1	R2	R3	R4	R5
An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence	No	Partially	Partially	Partially	No
Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody	No	Partially	Partially	Partially	Yes
A Framework to Improve "Chain of Custody" in Digital Investigation Process	Yes	Yes	Yes	Yes	Yes
Blockchain-based Chain of Custody	Yes	Yes	Partially	Yes	Yes
B-CoC: A Blockchainbased Chain of Custody for Evidences Management in Digital Forensics	Yes	Yes	Yes	Yes	Yes
Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?	No	-	-	-	No

IV. BACKGROUND RESEARCH

With the use of technology crimes like cyber theft and cyber terrorism have increased which cause destruction ten times more than the physical crimes. Criminals have adapted the technology and attempt different types of crime using it. Any crime that happens leave some evidences, be it log files in case of cyber-crime or a weapon in case of a physical crime. Proper investigation becomes a key parameter in order to catch the criminal. The science which deals with examining the evidences collected from the crime is known as Forensic Science.

Dr. Edmond Lockard's Principle of exchange states "every crime leaves a trace", any person entering and leaving the crime scene leaves traces behind, these traces can be DNA particles, skin cells, weapon fingerprints, gunshot residues, bullet shell or anything. All these things come under evidence which need to be collected in order to catch a criminal. Most people think that there must be a weapon involved whenever they hear the word crime, but some crimes are executed with the help of the tools and technology. In such cases the type of evidence varies. Broadly we can specify the evidence into two categories which are as follows: Physical Evidence: A physical evidence is a type of evidence that comes from anon-living background, it may include weapons like gun, knife and so on. Digital evidence is basically a type of physical evidence but contains digital information in it. Hard drives, USB flash drives and computers or laptops if found on a crime scene are termed as digital evidence. The process of analyzing digital evidence varies as compared to other evidences. In order to make digital evidence admissible in the court, one must maintain the "Chain of Custody".

Chain of custody involves various parameters and protocols that need to be followed: -

a) Collection of evidence: The collection of evidence/data needs to be done in a procedural manner i.e., once evidence is recovered from the crime scene it should be labelled and put into the evidence bag. Proper recording using a digital camera should be done along with

b) taking the photographs of the evidence. A file should also be maintained stating the number of people who handled the evidence throughout the collection phase of the evidence. It is done in the process to maintain the integrity of the evidence.

c) Examination: This process involves the examination of the evidence to check if its integrity has been maintained or not. Capturing of screenshots throughout the process is important to shoe that the tasks are completed in a proper manner and evidence is uncovered.

d) Analysis: This is the most important step as it involves analysis of the evidence and fragments of data using various tools and technologies in order to draw a conclusion so that justice is served to the victim. The process is tedious and time consuming as various tools are used in the process. The investigator also has to ensure that the integrity of the evidence is managed throughout this whole task.

e) Reporting: This phase involves the documentation and analysis of the evidence. Reporting involves:

- Statements: These involve statements from the people present around at the time of crime scene. These also involve statements made by the forensic scientist once S/he is done with the analysis of the evidence.
- Tools and techniques: The names of tools and techniques used for the analysis of the evidence are stated under this section of the report.
- Description of the data sources referred to: Detailed description of the data sources used for the analysis of the evidence need to be listed in this section.
- Issues/loopholes found: The weaknesses found during analysis on the evidence are mentioned here.
- Vulnerabilities, exploits identified: Names of the vulnerabilities and the exploits along with a detailed report of the same need to be mentioned under this heading.

1 Digital Evidence: Digital evidence or digital information may include MD5 hash, filename, hard disk, serial number, host name etc. In order to maintain Chain of Custody the evidence should be properly bagged and tagged containing information like investigator name, evidence type, collection time, collection place, case id and date of collection. It should be also containing the information on where the evidence was stored and how it was transported to the forensic lab for further analysis. Moreover, information of how and by whom the evidence was transported should also be documented. A proper report should be hence generated containing all the above-mentioned protocols. Every time the evidence is handed off to someone, then report should be updated in order to maintain the chain of custody.

System to build up the chain of guardianship should be continued to keep up with the validness and uprightness of the proof. Keeping up with the uprightness of the proof is simpler than keeping up with the chain of guardianship. To break down computerized proof after conventions ought to be drilled:

- Save the original evidence, never work on the original evidence.
- Create an image of the evidence procured from the crime scene using tools available like FTK Imager in case of hard drive analysis
- Perform a hash test analysis to authenticate the image of the evidence created.
- The original evidence should be sterilized in order to ensure that the digital evidence is not infected with any malware or any other thing.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 2: Types of Digital Forensics used based on the type of digital evidence (R1: Evidence Type, R2: Type of Forensic, R3: Explanation)

R1	R2	R3
Storage Media Devices	Disk Forensics	deals with extracting data from storage media by searching active, modified, or deleted files.
Routers, Modem, Network Devices	Network Forensics	monitoring and analysis of computer traffic is done and collection of important data and legal evidence is done.
Wireless Networking Devices	Wireless Forensics	Data from wireless devices is collected such as log files.
Database	Database Forensics	Examination of databases and their related metadata is collected and analyzed.
Malicious code, viruses, payloads, worms etc.	Malware Forensics	Identification of malicious code, payloads, viruses, worms etc. is carried out.
Emails, calendars, contacts	Email Forensics	Recovery of important emails including deleted emails, calendars and contacts is done.
System Memory	Memory Forensics	Collection of data like system registers, cache, RAM is done.

There are pros and cons for digital forensics:
Pros/benefits of Digital forensics:

- To keep up with the trustworthiness of the proof or PC framework.
- In request to make proof acceptable in the court computerized crime scene investigation is utilized
- Helps evaluate the security of the organization if their PC frameworks or organizations are compromised
- Helps get the offender which besides serves equity to the person in question.

Cons/disadvantages of Digital forensics:

- Digital evidence is admissible in the court but to present it in the court, it is necessary to prove that evidence has not been tampered. • Producing and storing electronic records and data is an extremely costly affair.
- The tools used to carry out digital forensics must be of the standards specified by the court, if not found then evidence will be dismissed.
- A skilled investigator officer is needed to carry out the desired results, lack of technical knowledge may give us fulfilling results.

V. IMPLEMENTATION

The current model proposes an addition to the existing m1ethod of maintaining the chain of custody of digital evidence. In the previously proposed models, a detailed procedure of how to maintain the chain of custody has been explained. In the above model, various steps have been implemented. The initial step in order to maintain the chain of custody is that a crime needs to be reported. Due to the nature of crime, many crimes go unreported. Investigation is done for the crimes which are reported. The next step for any investigator is to reach and seal the crime scene so that the crime scene doesn't gets contaminated by foreign substances. Securing the area containing the equipment or the crime scene is an important part of the investigation. Following steps should be followed:

- Secure the entrances and exits to the digital scene.
- Move people away from computer and power supply as it may lead to contamination if anyone touches anything.
- Preventing changes in possible computerized proof, including network disconnection, gathering unpredictable information, and replicating whole
- Description of the evidence
- Case number or identification number
- Date and location of the collection
  Evidence that are found on or around the crime scene need to be bagged and tagged properly. The label that is used for tagging the evidence must contain
- Description of the evidence
- Case number or identification number
- Date and location of the collection
- Investigator name
- Any serial number or information on the evidence

Once the evidences are collected and labelled properly, they are sent for further analysis in the laboratory. Before analysis the evidences are distinguished based on their nature. Evidence is classified broadly in two categories – physical evidence and digital evidence. Physical evidence has a different procedure for analysis and digital evidence has a different procedure. The proposed model focuses on maintaining the chain of custody for digital evidence. Following are the steps that should be taken: • Acquire the e-evidence from the equipment by using forensically sound methods and tools to create a forensic image of the e-evidence.

- Keep the first material in a safe, gotten area.
- Design your audit procedure of the e-proof, including arrangements of watchwords and search terms.
- Examine and investigations legal pictures of the e-proof (never the first!) as indicated by your technique.
- Interpret and draw deductions dependent on realities accumulated from the e-proof.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- Describe your investigation and discoveries in a straightforward and obviously composed report.
- Give declaration having sworn to tell the truth in a statement or court.

Digital evidence is analyzed using various forensic tools and techniques. The first and foremost step is to create a digital clone of the original evidence.

In order to create a clone of the original evidence various tools. Copying and pasting the files is not same as forensic cloning, Cloning involves creating a bit-to-bit image of the data which includes both the active and latent data. The further analysis is done on the cloned image and not on the original evidence. Original evidence should be preserved and used only if necessary.

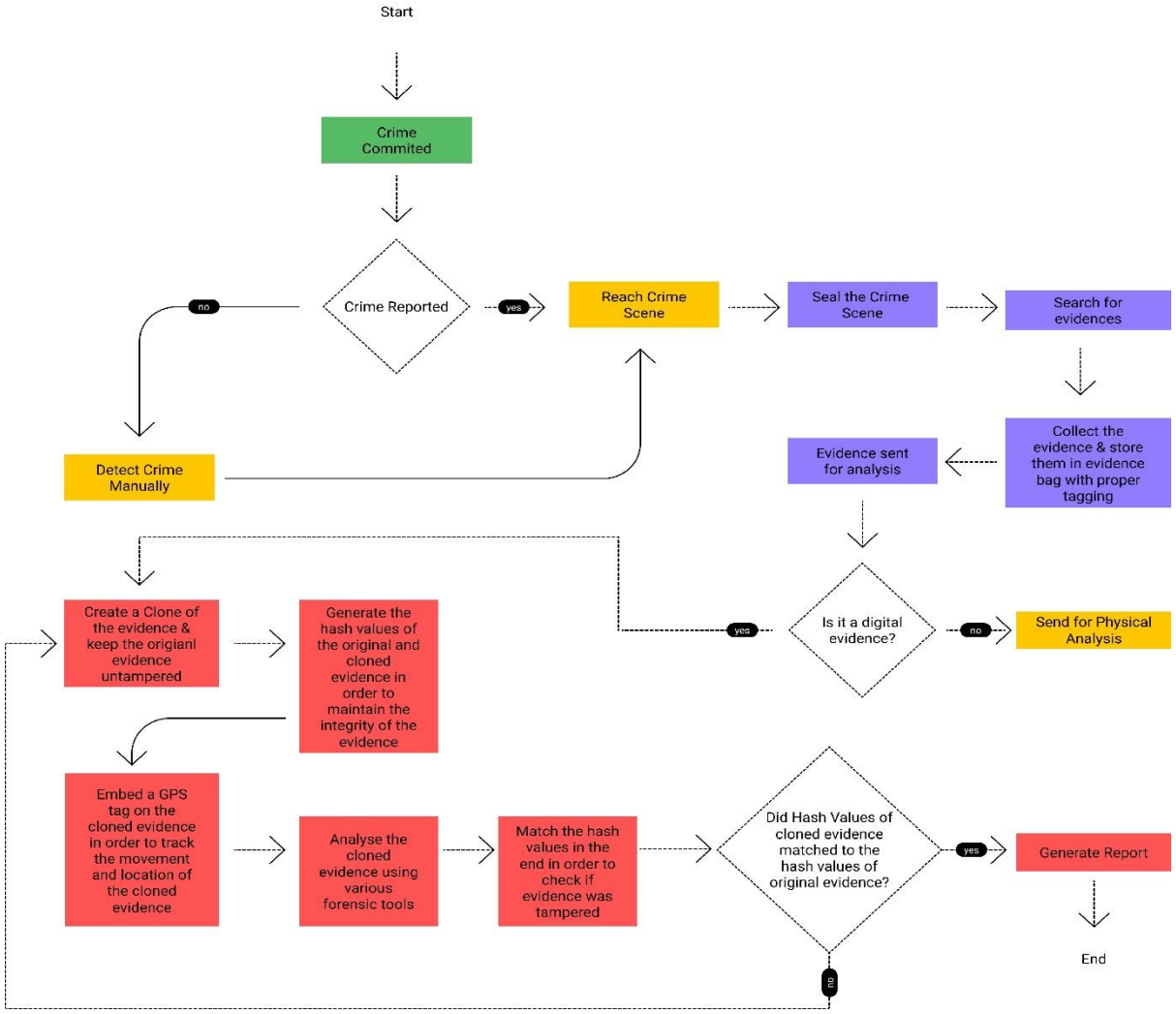

Figure 2: Proposed Model Flow Chart

VI. RESULT AND DISCUSSION

the examination is engaged and situated towards the objective to accomplish the respectability of an advanced proof for the duration of its life cycle till the time it arrives at the court. this space of examination is taken to help and assist the agents with keeping a track on the proof all through the course of chain of authority. the principal step to guarantee the honesty of a proof is to try not to alter of the proof. here and there during the investigation period of the advanced proof, it needs to go through different tests which give numerous outcomes that at long last go about as a proof that can additionally be utilized against a convict in the court to verification his/her wrongdoing.

VII. CONCLUSION AND FUTURE WORKS

The research is focused and oriented towards the goal to achieve the integrity of a digital evidence throughout its life cycle till the time it reaches the courtroom. This area of research is taken in order to assist and help the investigators to keep a track on the evidence throughout the process of chain of custody. The foremost step to ensure the integrity of an evidence is to avoid tampering of the evidence. Sometimes during the analysis phase of the digital evidence, it has to undergo various tests which give multiple results that finally act as a proof that can further be used against a convict in the courtroom to proof his/her crime. Another challenge that an investigator faces is tracking of the evidence, since the evidence is analyzed by different forensic scientists, there always stays a chance that evidence may get tampered due to any circumstantial reason or a motive which can affect the integrity of the evidence and make it inadmissible in the courtroom.

The proposed research uses available tools like FTK Imager and technology like global positioning system to aid the investigator with proper tracking of the evidence right from the moment it was collected from the crime scene till the time

Figure 3: Steps to be followed in order to create an image in FTK Imager

It reaches the court room. The proposed method describes the usage of GPS technology in the process chain of custody of digital evidence which helps the investigator to maintain and evaluate the integrity of the evidence throughout the life cycle of the digital evidence. The method uses GPS tags and chips embedded with a hash value which would be matched at the end once the analysis on the evidence is done in order to check if the evidence was not tampered and integrity was maintained throughout. This helps the investigator and eases his/her task of maintaining and evaluating the integrity of the digital evidence. The proposed research has provided an algorithm to the approach with the required tools and technologies. though a lot more needs to be researched like on how to embed the process of hiding the metadata of the digital evidence collected from the crime scene, making custom size gps chips as per the nature of the evidence and making the process fully automated and smoother. the future work would be more oriented towards the above stated problems which will help and reduce the task of investigators while ensuring the integrity of the digital evidence throughout the chain of custody making sure that the evidence becomes admissible in the court, thereby ensuring justice to the victim or victim group.

REFERENCES

1. L. Ahmad, S. Khanji, F. Iqbal, and F. Kamoun. Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In Proceedings of the 15th International Conference on Availability, Reliability and Security, pages 1–8, 2020.
2. A. Badiye and R. G. Menezes. Chain of custody. StatPearls [Internet], 2020.
3. S. Bonomi, M. Casini, and C. Ciccotelli. B-coc: A blockchain-based chain of custody for evidences management in digital forensics. arXiv preprint arXiv:1807.10359, 2018.
4. P. G. Bradford and D. A. Ray. Using digital chains of custody on constrained devices to verify evidence. In 2007 IEEE Intelligence and Security Informatics, pages 8–15. IEEE, 2007.
5. J. Cosic and M. Baca. Do we have full control over integrity in digital evidence life cycle? In Proceedings of the ITI 2010, 32nd International Conference on Information Technology Interfaces, pages 429–434. IEEE, 2010.
6. J. Cosic and M. Baca. A framework to (im) prove" chain of custody" in digital investigation process. In Central European Conference on Information and Intelligent Systems, page 435. Faculty of Organization and Informatics Varazdin, 2010.
7. J.´Cosi´c and M. Ba˘ca. (im) proving chain of custody and digital evidence integrity with time stamp. In The 33rd International Convention MIPRO, pages 1226–1230. IEEE, 2010.
8. J.´Cosi´c, Z.´Cosi´c, and M. Ba˘ca. An ontological approach to study and manage digital chain of custody of digital evidence. Journal of Information and Organizational Sciences, 35(1):1–13, 2011.
9. J. Cosic, Z. Cosic, J.´Cosi´c, and Z.´Cosi´c. Chain of custody and life cycle of digital evidence. Computer Technology and Aplications, 3:126–129, 2012.
10. R. Koleoso, O. Ajayi, F. Oladeji, and C. Uwadia. A digital forensics investigation model that incorporates digital chain of custody for its integrity, and authenticity. COMPUTER NETWORKS, INFRASTRUCTURE MANAGEMENT AND SECURITY (CoNIMS), page 55.
11. A. H. Lone and R. N. Mir. Forensic-chain: Ethereum blockchain based digital forensics chain of custody. Scientific and Practical Cyber Security Journal, 1(2):21–7, 2018.
12. A. H. Lone and R. N. Mir. Forensic-chain: Blockchain based digital forensics chain of custody with poc in hyperledger composer. Digital Investigation, 28:44–55, 2019. 16
13. Y. Prayudi, A. Ashari, and T. K. Priyambodo. Digital evidence cabinets: A proposed framework for handling digital chain of custody. International Journal of Computer Applications, 107(9), 2014.
14. Y. Prayudi and A. Sn. Digital chain of custody: State of the art. International Journal of Computer Applications, 114(5), 2015.
15. M. S. M. B. Shah, S. Saleem, and R. Zulqarnain. Protecting digital evidence integrity and preserving chain of custody. Journal of Digital Forensics, Security and Law, 12(2):12, 2017.
16. A. ZAHARIA. 300+ terrifying cybercrime cybersecurity statistics [2021 edition] 2021
17. Y Kalra, PS Patheja, S Upadhyay, Advancements in Cyber attacks in Security, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9, Issue-4, February 2020

AUTHORS PROFILE

Devesh Banwani, is currently pursuing Bachelor of Technology in Computer Science and Engineering with specialization in Cyber Security and Digital Forensics from Vellore Institute of Technology, Bhopal. Research Area Includes Cyber Security, Digital Forensics and Cyber Laws. Email: deveshbanwani30@gmail.com

Yatin Kalra, is currently pursuing Bachelor of Technology in Computer Science and Engineering from Vellore Institute of Technology, Bhopal. His research area interest includes OS Hardening, security analysis in cybersecurity. Email: yatinkalra.vit@gmail.com