International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume X, Issue III, March - 2023

Research and Implementation of the Digital Evidence Object Model and Enforcement Protection Program for Situation Awareness

Mohamed Imdhiyaz I
Computer Science and Engineering
Cyber Forensics Applied Lab Student
Francis Xavier Engineering College
Tirunelveli
mohamedimdhiyazi.ug20.cs@francisxavier.ac.in

Godwin Lasaras P
Computer Science and Engineering
Cyber Forensics Applied Lab Student
Francis Xavier Engineering College
Tirunelveli
godwinlasarasp.ug20.cs@francisxavier.ac.in

Logeshwaran S
Computer Science and Engineering
Cyber Forensics Applied Lab Student
Francis Xavier Engineering College
Tirunelveli
logeshwarans.ug20.cs@francisxavier.ac.in

Arun Kumar V
Computer Science and Engineering
Cyber Forensics Applied Lab Student
Francis Xavier Engineering College
Tirunelveli
arunkumarv.ug20.cs@francisxavier.ac.in

Dr. R. Ravi
Prof/ Computer Science and Engineering
Cyber Forensics Applied Lab In Charge
Francis Xavier Engineering College
Tirunelveli
fxhodcse@gmail.com

***Abstract*—*Digital forensics technology is a crucial weapon in the battle against cybercrime and computer crime. To avoid violations of the rules governing the use of digital evidence in court proceedings,*

Protecting data evidence from inadvertent changes to the evidence is a key guideline throughout the entire process of digital forensics. There are issues with the currently used techniques for purposefully securing digital evidence, such as the risk of clandestine data alteration. In this work, we presented a software for the enforcement protection of digital evidence based on third party notary in order to overcome the limitations in digital evidence consciously protection. Before discussing the program's security, we looked at its execution and method methods.

Keywords — *crucial weapon, violations, limitations, clandestine data, Protection, third party notary.*

I. INTRODUCTION

Considering how frequently computers and the Internet are used in social and business settings, network connectivity

Many elements of modern life have been impacted by high-tech computer crime. For the fight against computer commercial crime, to maintain the security of businesses and public property, and to purge the Internet environment, digital forensics technology is an invaluable and effective tool. Perfect digital forensics techniques and powerful digital forensics tools may find evidence of a crime, locate perpetrators swiftly, and stop likely criminal motivations.[1]

Digital evidence can take many various shapes, including evidence that is stored on hard drives, networks, and portable storage devices. Data evidence is high-tech, easy to change, easy to destroy, and easy to hurt, in contrast to traditional physical evidence[2][3]. In most cases, forensics experts take deliberate steps to safeguard digital evidence, such as write-protecting, copying, backing up, computing the checksum, and taking further measures to prevent data evidence[4] from being accidently corrupted. It is extremely unsafe and dangerous to keep hard disc and other media evidence even if there are deliberate precautions in place to prevent tampering with and deleting digital evidence.[7]

Sensor networks, cloud and fog endpoints, cell phones, social networks, etc. are all becoming more disorganized, putting users' communication systems and private data at risk. As a result, there is an increase in the quantity, variety, speed, and reliability of digital data that can be used in forensic investigations, which collect, preserve, analyze, and present evidence of attacks from various heterogeneous digital sources, including mobile devices, networks, big data in the cloud, etc.[5][6]Digital forensics inquiry cannot be totally automated since it requires human expert knowledge to make accurate determinations.

II. DIGITAL FORENSICS AND DIGITAL PROTECTION CONCERNS

A. Digital Forensics

Digital Forensics Addresses All Legal and Network Issues Digital forensics is a broader idea than computers in the realms of security and data recovery.

International research focuses on forensics and network forensics. DFRWS is thinking on what constitutes digital forensics:

"Method of derivation and verification via storage, collection, ascertainment, identification, analysis, interpretation, and documentation of digital evidence from digital sources, to aid

and facilitate criminal reconstruction; or Aids in the prediction of disruptive and unlawful activity." Definitions are clear sources of evidence; His research and the study of digital forensics were both digital. Data processing, evaluation, collection, and storage are the goals.

B. Data protection concerns

To comply with litigation's demands for digital evidence. Using forensics to prevent unforeseen changes in the evidence workers gather and examine evidence to avoid accidental evidence of damage, and take conscious protection of digital evidence measures such as read-only, copy, save, and calculate checksum. actions taken by to prevent Evidence that they have been maliciously modified, add written records, digital signatures, timestamps, and a back-up piece of evidence referred to as Force Protection Measure.

How to Activate Digital Evidence Protection

Normally: Turn off your computer, copy the contents of your hard drive, and calculate hash values using less-technical methods.

Your data might not be lost when you turn off your computer, which could be used by both law enforcement and criminals. the goal of the primary hard drive is safeguarded by a forensic hard drive copy, and analyze the data from the disk copy.

III. USING A THIRD-PARTY REVIEW, PROTECT YOUR DIGITAL EVIDENCE PROGRAM DELIBERATELY

A. The Goal of the Program:

To develop proof-aware security programs to reach the objective of making evidence irrefutable Irrefutability and No repudiation by Parties technology. irreversibility of the evidence. should be used wisely means of inspection for tampering with evidence. However, you ought to examine it. an example of infallibility. Use a digital signature to prohibit the creation of the same digital signature after the collecting of the evidence. Parties' no repudiation. Detectives and law enforcement officials cannot dispute the validity of the data source's evidence and field data collecting.

B. Relevant technology:

The Digital Evidence Preservation Project is something we are aware of.

Asymmetric Cryptographic Algorithms, Digital Signatures, Biometrics Authentication, Security Time stamping, and Security Notarization Services, together with the hash function presented in this article cryptography. Big computations are made via hash functions.

The resulting data is known as a hash value when it is combined with a tiny quantity of input data from a dataset.

Encrypted Asymmetric encryption is used to encrypt data

using a private key.

With the use of your public key, the algorithm must be decoded. because asymmetric encryption methods' public keys are also public used to encrypt the file's hash value using the private key.

Digital signatures, which may be validated by each individual has a public key. to possess just private key signature designed to prevent tampering without a secret signing key.

C. The Force Protection Program for the Digital

Evidence Process:

a) Hard disc for data acquisition: Copies of disc data

make the hash using a forensic disc copy machine value of

the disc. the initial data gathered proof-sealed named master

copy with confirmation message prohibited. This master copy is safeguarded as official documentation. The second copy may be duplicated once more. Additional copies have been encrypted for upcoming research.

b) Forensic Protocol: This process establishes the case name and the name of the forensic log. Evidence gathering details, including dates, locations, and activities; Forensic computer, computer owner employees; Info about disc copy errors.

c) Sound data: To capture sound, the owner of a forensic computer must be asked to sign approval, which is a step in the procedure needed to get speech data. The case name should contain this information.

d) Evidence-based Security Timestamp

A security notary offers services through a network connection after building a block and calculating its hash value H. Next, the timestamp containing the hash value is submitted to the security notary.

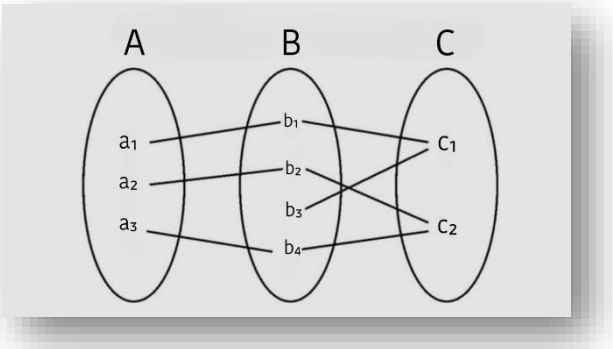
A security notary H together with server time form a digital signature. identifying information for this timestamp, including the date, the time, the hash, digital certificates, and digital signatures.

e) Digital signature: software for digital signatures

Create a digital signature using the private bailiff's key and the hash value. Digital certificates and signatures are considered Evidence of the Evidence Verification message block by the PKI standard.

Introduction Into Category Theory:

A category is described as a group of related things and arrows. It is possible to formalize various items into groups that can be linked. A category is made up of the objects A, B, and C and the specified arrows that connect them (functions)



C. Demo Model

We suggest the DEO model, which is based on an analysis of data obtained through proper forensic procedures.

Concentrating on the forensic investigation cases suggested in Miranda Lopez et al.'s publication. We employ the category

theory because it has a strong foundation in computer science and supporters in a number of other disciplines. Because it is particularly well adapted to modeling open, autonomous, and networked dynamical systems, its formalism can also be used to represent digital objects.

The suggested DEO model's objectives are to minimize the amount of data from the examination phase of the digital forensic investigation process, formalize the examination phase of a computer system or digital gadget to expedite the collecting of digital evidence. The concept is based on the U.S. Department of Justice's 45 forensic process handbook, which identified the four basic stages as collection, examination, analysis, and reporting. Documentation (which involves describing the substance and state of the evidence overall) and data reduction make up the two sections of the examination phase. Due to the enormous amount of data and information that is saved in computer systems, the data reduction step of the examination phase is crucial.

IV. CASE STUDY

Preliminaries:

The forensic inquiry is broken down into five steps in the NIST and ISO/IEC forensic guidelines20:

1) Recognition.

2) Acquisition and/or collection.

3) Maintenance.

4) Inspection and evaluation.

Five) Reporting.

Starting with a copy of the confiscated device, the investigation and analysis process unearths digital evidence using the necessary forensic tools and established criteria. Here, we show how to use the programmed. of our model for the inspection and analysis (stage 4) of the forensic inquiry.

In our case study, the major goal of the digital forensic inquiry was to compile a valid and trustworthy set of DEOs that would be useful to forensic investigators in their search for evidence.

To do this, the set of all feasible sets of DEOs—the n-ary Cartesian product—is determined.

The case study's environment. Due to alleged hacking activities, an information system (IS) that manages the electricity cogeneration plant system has malfunctioned. As a result, on March 22, the power plant caught fire. causing the plant's owners to suffer severe material losses. The power plant's insurance provider launched an investigation to ascertain what caused the catastrophe. There was a possibility that the IS's logs had been altered between March 21 and April 1, 2016.

The case study's subject. The picture of the 40 GB Samsung hard drive (HDD) that was taken from the suspicious computer by law enforcement officers looking into a possible fraud offence. The photograph was prepared for the fourth step of the forensic investigation—examination and analysis—by mounting it in the expert computer.

Premise for Inspection and Analysis. The confiscated HDD is equipped with a cogenerated energy information system (CEIS), which the forensic expert was aware of.

The installed CEIS's primary duty is to regulate the output of cogenerated energy. The system either failed to provide accurate data or did not function properly for some reason (perhaps fraud intended to conceal the quantity of cogenerated energy produced) the theory put forth by the expert. With the intention of harming CEIS, suspicious activity was carried out, possibly altering OS traces as well as log information. The range of probable suspicious behavior is set between 2016-03-21 and 2016-04-01. The expert has chosen the 2016-01-08 to 2016-04-08 timeframe for his investigation.

The equipment that the expert utilized. Forensic Toolkit 5 (FTK) and Autopsy 4.9 (Basis Technology, Cambridge, MA, USA) (Access Data, Orem, UT, USA).

V. CONCLUSION

In this piece, we examined the drawbacks of digital. When

using digital evidence, consciously protect the evidence.

Describe the collecting method and go through the dangers and risks involved. Make a difference to secure digital evidence on purpose.

Winkle displayed evidence preservation in digital form a software that offers fundamental security for public key

digital signatures on the Notarization server. The project employs an asymmetric encryption method, digital signatures, biometrics, security timestamps, and the highest level of security notary service technologies.

Irreversibility, non-repudiation, and irreversibility objectives using hard hash value components for digital proof disk data, a computer owner's voice, a hash calculation, and digital signatures all at once. For digital forensic inquiry, we suggested a novel DEO paradigm and discussed its use. The suggested DEO model is utilized for digital investigation analysis in relation to the 5Ws (Why, When, Where, What, and Who). It is founded on the fundamental ideas of the category theory. The methodology facilitates intelligent situation-aware time-critical decision making and automates knowledge discovery in the field of digital forensics.

We presented a real-world case study for aiding a computer forensics expert in the digital evidence investigation process of the fraud created with the intention of concealing the quantity of produced cogenerated energy by the power plant to show the model's applicability. Our findings demonstrate that the suggested DEO model can formalize the inspection stage of the digital forensic investigation process, reduce the amount of time that the amount of data from a computer system or digital device for analysis, hasten the gathering of digital evidence, and enhance cyber security. A forensic investigator can use the DEO model to reduce the amount of data that has to be examined, then evaluate and extract digital evidence from a smaller dataset. The digital forensics professional can perform more quickly and with less error by focusing on the tiny amounts of information and data from a computer system.

The proposed model will be expanded in the future to handle the semantics of events for integrated forensic acquisition on social media, and the proposed DEO model will be used to quickly locate evidence of harmful activity in social networks.

REFERENCES

[1.] V. Mancuso, S. McGuire, and Dr. R. Ravi, "Human centered cyber situation awareness," in Proc. Adv. Hum. Factors Cybersecurity, 2019, pp. 69–78.

[2]. S. Jajodia, P. Liu, V. Swarup, and Dr. R. Ravi, Cyber Situational Awareness (Advances in Information Security). New York, NY, USA: Springer, 2010.

[3]. S. K. Alamgir Hossain, M. Anisur Rahman, and Dr. R. Ravi, "Edge computing framework for enabling situation awareness in IoT based smart city," J. Parallel Distrib. Comput., vol. 122, pp. 226–237, 2018.

[4]. Z. Yang, T. Li, and Dr. R. Ravi, "Situation awareness for cyber-physical system: A case study of advanced metering infrastructure," in IEEE Int. Conf. Prognostics Health Manage., 2018, pp. 1–6.

[5]. M. H. Bazrafkan, H. Gharaee, and Dr. R. Ravi, "National cyber situation awareness model," in Proc. 9th Int. Symp. Telecommun., Emphasis Inf. Commun. Technol., 2018, pp. 216–220.

[6.] I. A. Cooke et al., Toward robust models of cyber situation awareness, 2019. doi:10.1007/978-3-319-94782-2_13

[7]. S. Jajodia and Dr. R. Ravi, An Integrated Framework for Cyber Situation Awareness (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2017, vol. 10030, pp. 29–46.