IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

AN INVESTIGATION OF DIGITAL EVIDENCE, DIGITAL FORENSIC TOOLS AND CLOUD FORENSIC TECHNIQUES

Mr. Parveen Kumar[1], Dr.Pramod Kumar[2]

[1]M.Tech CSE Student, GITAM, Kablana, Jhajjar.

[2]Assistant Professor, Department of CSE, GITAM, Kablana, Jhajjar.

ABSTRACT

The objective of digital forensics is to follow the standardized investigation process while documenting any evidence that is stored digitally which may indicate to the person responsible for the crime. The investigators use various techniques and forensic applications to search hidden folders, retrieve deleted data, decrypt the data or restore damaged files etc. Nowadays, Cybercrimes are going on at a huge scope, and have huge dangers to the security of an individual, firm, industry and even to created nations. At long last the paper suggests the need of preparing programs for the person on call and judgment of mark based picture validation.

KEYWORDS: Cyber Crime, Computer Forensic and digital Evidence.

INTRODUCION:

Digital Forensics is the branch which deals with the crimes which happen over the computers, where a single computer system constitutes an entire crime scene or in the least it may contain some evidence or information that can be useful in the investigation. However, in technical terms it can be defined as the process of identification, acquisition, preservation, analysis and documentation of any digital evidence. A thorough examination can tell us when any document was created, edited, printed, saved or deleted There are several problems that can be faced by digital forensics examiners like the files that are encrypted take more time, the rapidly changing computer technology, and anti-forensics tools can add up to more time and money for the investigating organization However, as the crime's frequency rises so does its need to get investigated. Therefore, the process which needs to be followed must be thorough and up to its full optimization level in order to solve the case.

WHAT IS COMPUTER FORENSICS?

1. Computer criminology is the interaction of deliberately inspecting PC media (hard circles, diskettes, tapes, and so forth) for proof. At the end of the day, PC legal sciences is the assortment, protection, examination, and show of PC related proof.
2. Computer crime scene investigation likewise alluded to as PC legal examination, electronic disclosure, electronic proof revelation, computerized disclosure, information recuperation, information disclosure, PC investigation, and PC assessment.
3. Computer proof can be valuable in criminal cases, common questions, and HR/business procedures.

Digital Forensic Investigation Life Cycle

From the digital forensic definition, digital forensic investigation process involves many steps as follow as shown in Figure 2.1:

Identification: It is involved in two key phases: identification of crime and identification of digital evidence.

Collection: In this phase, an examiner gathers digital evidence from the crime scene for using in next examination phase.

Extraction: In extraction phase, the digital investigator extracts digital evidence from various types of devices such as cell phone, hard disk, and e-mail.

Analysis: In this phase, examiner interprets and correlates the extracted digital evidence to come to a summary, which can prove or disprove criminal accusations.

Examination: In the examination phase, the investigator extracts and inspects the data and their characteristics.

Report: In this process, the investigator and examiner make a prepared report to represent his/her findings from forensic analysis of crime evidence. This report should be suitable enough to present in the court of law.

Digital Evidence

Computerized proof is the source information that assistance and help advanced specialists for cybercrimes examination and assessment to carry the crooks to judgment. The advanced proof might be in different structures like content, sound, picture, and video. In the courtroom, the proof used to demonstrate and build up that cybercrime or occurrence has been carried out or can convey a connection between a crime and its casualty. Figure 2.2 shows various sorts of advanced proof.

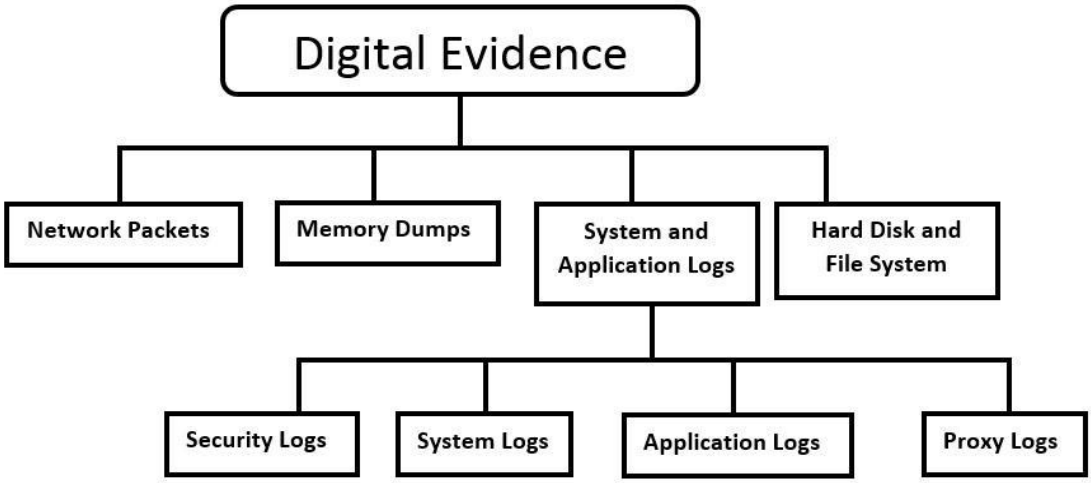

Figure : Digital Evidence Types.

Cybercrimes

In the new time, cybercrimes become more basic as dangers for breaking framework security because of creative thoughts that crooks have with respect to groundbreaking thoughts and approaches to carries out these crimes. The hoodlum's abuse weaknesses of new advances to carry out their crimes such that make it is hard to find and follow them back. The powerful idea of distributed computing adds to the issues met by specialists while separating and getting ready computerized proof for a courtroom.

Cybercrime is classified as the following [9]:

- The PC as an objective: The criminal tries to keep the authentic clients or proprietors from getting the framework admittance to their information or PCs like Denial of Service (DOS) assaults.
- The PC as an apparatus of the crime: The PC is utilized to acquire some other criminal target. For instance, a criminal may utilize a PC to take individual data.
- The PC as accidental to a crime: The PC isn't the essential instrument of the crime; it just works with it.
- Crimes related with the commonness of PCs: This incorporates crimes against the PC business, like programming theft.

Cybercrime Classification in Cloud Forensic

In the cloud computing environment, cyber-crimes divided into two main types:

- Crimes using the cloud infrastructure resources capacities to be performed the malicious attacks.
- Crimes against the cloud infrastructure**.**

CLOUD FORENSICS

The term of cloud forensics was presented by Ruan et al. [2012] to distinguish the quickly arising need for advanced forensics in the cloud. She characterized cloud forensic as a cross-control of distributed computing and computerized forensics. Likewise, referenced that in "Cloud forensics is a subset of organization forensics Organization forensics manages forensic examinations of organizations. Distributed computing depends on expansive organization access. In this manner, cloud forensics follows the principle periods of organization forensics with strategies custom fitted to distribute computing conditions".

Cloud Forensics Challenges

To understand the cloud challenges, the NIST developed a formula for a normalized sentence syntax that allows expression of all cloud forensics challenges in a format as follows:

NORMALIZED CHALLENGE [FORMULA]:

- For a [actor/stakeholder], [action/operation] appropriate to [object of this action] is testing in light of the fact that [reason]
- Entertainer/Stakeholder: This variable [a noun] distinguishes the stakeholder(s) who are influenced by the test that has been recognized. Instances of partners incorporate cloud customers, examiners, specialists on call, and so on
- Activity/Operation: This variable [a verb] recognizes the movement that the partner might want to perform. Instances of activities incorporate decoding, imaging, getting entrance, and so forth
- Object of This Action: This variable distinguishes the particular thing whereupon the activity is to be performed. Instances of items incorporate information, review logs, timestamps, proof, and so forth
- Reason: This variable recognizes the essential difficulties that the partner faces to play out the predefined activity on the item.

The standardized portrayal of certain difficulties is:

For forensic inspectors, recognizing and crediting information that is erased in the cloud to a particular client is a test in light of the fact that the sheer volume of information and clients continually working in a cloud climate restricts various reinforcements that the cloud Provider will hold.

For specialists, connection of action is a test on the grounds that there is no interoperability between cloud Providers

For all specialists and courts, reproduction of virtual pictures or capacity is testing on the grounds that these recreation calculations should be approved or created.

For agents/law authorization/examiners, the assortment and conservation of forensic proof is testing in light of the fact that there is an absence of interoperability among suppliers and there is absence of control from the client's viewpoint into the restrictive engineering and additionally the innovation utilized

For law implementation, guaranteeing legitimate chain of guardianship and security of information, metadata, and perhaps equipment is a test since it could be hard to decide possession, authority, or precise area.

For law implementation and courts, guaranteeing appropriate chain of guardianship of information is a test on the grounds that the conveyed, shared framework of distributed computing makes recognizing and approving a chain of authority troublesome.

To aid a significant investigation, the NIST classified the difficulties into the accompanying nine significant gatherings as demonstrated in Figure 2.3 while the portrayal of some cloud forensic difficulties is arranged in Table 2.1. The classes and related portrayals are summed up underneath as follows:

Engineering: In cloud forensics, the design difficulties remember managing fluctuation for cloud models between suppliers; inhabitant information compartmentalization and segregation during asset provisioning; expansion of frameworks, areas and endpoints that can store information; precise and secure provenance for keeping up and protecting chain of authority; foundation to help capture of cloud assets without upsetting different occupants; and so forth

Information assortment: Challenges of information assortment remember finding forensic antiques for enormous, dispersed and dynamic frameworks; finding and gathering unpredictable information; information assortment from virtual machines; information respectability in a multi-occupant climate where information is divided between numerous PCs in various areas and available by different gatherings; powerlessness to picture every one of the forensic relics in the cloud; getting to the information of one inhabitant without breaking the privacy of different inhabitants; recuperation of erased information in a common and appropriated virtual climate; and so on

Investigation: Analysis challenges in cloud forensics incorporate connection of forensic curios across and inside cloud suppliers; remaking of occasions from virtual pictures or capacity; trustworthiness of metadata; timetable examination of log information including synchronization of timestamps; and so forth

Hostile to forensics: Anti-forensics is a bunch of methods utilized explicitly to forestall or deceive forensic investigation. Difficulties in cloud forensics incorporate the utilization of obscurity, malware, information covering up, or different procedures to bargain the respectability of proof; malware may evade virtual machine confinement strategies; and so forth Episode people on call: Incident specialist on call difficulties in cloud forensics incorporate certainty, skill, and reliability of the cloud suppliers to go about as specialists on call and perform information assortment; trouble in performing beginning emergency; handling an enormous volume of forensic curios gathered; and so on .

Job the executives: Role the board difficulties in cloud forensics incorporate interestingly distinguishing the proprietor of a record; decoupling between cloud client qualifications and actual clients; simplicity of obscurity and making imaginary personalities internet; deciding definite responsibility for; validation and access control; and so on

Legitimate: Legal difficulties in cloud forensics incorporate distinguishing and resolving issues of locales for lawful admittance to information; absence of successful channels for worldwide correspondence and participation during an examination; information obtaining that depends on the collaboration of cloud suppliers, just as their

skill and reliability; missing terms in agreements and administration level arrangements; giving summons without information on the actual area of information; seizure and seizure of cloud assets may intrude on business coherence of different inhabitants; and so on

Principles: Standards challenges in cloud forensics incorporate absence of even least/essential SOPs, practices, and devices; absence of interoperability among cloud suppliers; absence of test and approval techniques; and so forth

Preparing: Training difficulties in cloud forensics incorporate abuse of computerized forensic preparing materials that are not relevant to cloud forensics; absence of cloud forensic preparing and skill for the two agents and teachers; restricted information by record-keeping staff in cloud suppliers about proof; and so on

Cloud Forensics Opportunities

The digital forensic investigation has various opportunities to be applied in cloud computing environment as follow:

Practical: Implement forensic assistance in distributed computing climate that permit using the immense limits of distributed computing without move the advanced proof from the cloud to the opposite side to play out the examination cycle which needs high data transfer capacity.

Information bounty: Replication of information in cloud climate presents the fundamental chance for cloud forensic for recuperate the lost and erased information from the cloud to confirmation the crime.

Versatility and adaptability: Cloud forensic administrations can use the offices of adaptability and adaptability asset use, for instance, giving limitless stockpiling, process and organization assets with the compensation per-use strategy.

Approaches and guidelines: Develop new principles and strategies for cloud forensic science because of quick difference in the innovation of distributed computing and cybercrimes against it.

Forensics as a Service (FaaS): Cloud registering gives one incredible alternative to computerized agents and inspectors called Forensic as a Service (FaaS). The forensic examiner can convey the FaaS through using the huge cloud capacities. This assistance makes advanced forensics as an "on-request" administration for permitting monstrous capacity and processor power as important to direct a computerized examination of crimes. Forensic workers will dwell on the cloud side, disconnected, until require emerges for them. Reports could be upheld into the cloud for the computerized specialists to use without upsetting typical business. Without a doubt the cloud assets could be utilized for arranging, looking, and hashing the proof information. There are numerous advantages of the Forensic as a Service as follows:

- Decrease proof securing time: If a worker in the cloud is undermined, it tends to be cloned and made promptly accessible to a cloud forensics worker.
- Diminish administration personal time: Due to the equipment deliberation in the cloud, particular equipment won't need to be gotten to proceed with the procurement of the proof in certain circumstances.
- Lessen proof exchange time: The mists conveyed record framework considers making quick piece for-bit duplicates.
- Decrease forensic picture confirmation time: Some cloud conditions utilize a cryptographic checksum or hash that can definitely diminish the time needed to hash records disconnected
- Decline time to get to secured records: The pooling of CPU power accessible in the cloud can make unscrambling a lot quicker.
- Essentially limitless log stockpiling: Cloud stockpiling arrangements will make the requirement for assessing how much plate space is required for logging superfluous, taking into account a lot of log information to be kept and utilized during an examination.
- Improve log ordering and searches: Along with limitless capacity, logs can be filed and looked through successfully progressively with cloud assets.

COMPARISON BETWEEN TRADITIONAL COMPUTER FORENSIC AND CLOUD FORENSIC

In Table, a comparison study between Classic Forensic and cloud forensic is tabulated to explain the differences between both above two types of forensics.

Table : Comparison between Computer Forensic and Cloud Forensic.

	Classic Forensic	Cloud Forensic		
		SaaS	PaaS	IaaS
Access Control	√	√	√	√
Application	√	X	√	√
Database	√	X	X	√
Operating System	√	X	X	X
Compute	√	X	X	X
Storage	√	X	X	X
Network	√	X	X	X

CONCLUSIONS

This work will worried about creating capable computerized forensic strategies for examination of cybercrimes in distributed computing climate in forensically solid and opportune way. It will present research commitments in the field of cloud forensics. They can be summed up as follows:

A writing survey will be done to investigate and recognize difficulties and openings for performing advanced forensics examination in the distributed computing climate. The ID of cloud forensic difficulties and openings, for example, secure and forensic investigation of distributed storage administrations, log information examination, plan distributed computing model to help computerized forensics, plan cloud-based forensic lab which assisted us with achieving and complete this exploration work. A cloud forensic methodology dependent on information uprightness checking for helping and aiding computerized examiners is proposed for performing programmed advanced forensics for box distributed storage as a contextual analysis. The test results showed that there are information antiques that stay in the client machine that utilizes Windows 7 about utilizing box distributed storage, for example, IP address, and client account data like a username. The proposed approach can possibly valuable device for performing cybercrimes examination identified with cloud stockpiles.

References:

1. Fiterman, E. M., and J. D. Durick. "Ghost in the machine: Forensic evidence collection in the virtual environment." Digital Forensics Magazine 2 (2010): 73-77.

2. Ezz El-Din Hemdan and Manjaiah D.H," Exploring Digital Forensic Investigation Issues For Cyber Crimes In Cloud Computing Environment", Proceeding of 1st International Conference on Computer Communication and Networks (i3CN),2015.

3. Market Research Media, "Global cloud computing market forecast 2015-2020", http://www.marketresearchmedia.com/ ?p=839, [Accessed June 25, 2015].

4. Clavister, "Clavister's new dimension in network security reaches the Cloud", http://www. clavister.com/documents/resources/white-papers/ clavister-whpsecurity-in-the-cloud-gb.pdf, Clavister White Paper, [Accessed December 27, 2016].

5. Barrett, Diane, and Greg Kipper, "Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments", Syngress, 2010.

6. P. Mell and T. Grance, "The NIST definition of cloud computing" (NIST SP 800-145), National Institute of Standards and Technology, U.S. Department of Commerce, 2011.

7. Cloud Security Alliance [CSA], "Security guidance for critical areas of focus in cloud computing", V2.1. San Francisco, California, 2009.

8. DFRWS technical report, "A road map for digital forensic research", Digital Forensic Research Workshop. G. Palmer. Utica, New York, 2001.

9. Mounir kamal (2012), "digital investigation concepts", Security Kaizen Magazine, 2(6),6-10,

10. Keyun Ruan, Joe Carthy, Tahar Kechadi and Ibrahim Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results", Elsevier, Digital Investigation vol.10, pp.34–43, 2013.

11. NIST Cloud Computing Forensic Science Working Group Information Technology Laboratory, "NIST cloud computing forensic science challenges" (NISTIR 8006), National Institute of Standards and Technology, U.S. Department of Commerce, 2014.

12. Ruan K., J. Carthy, T. Kechadi, M. Crosbie, "Cloud Forensics", 7th IFIPAdvances in Digital Forensics VII, G. Peterson and S. Shenoi (eds), vol. 361, pp. 35-46, 2011.

13. Shams Zawoad, Ragib Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems", arXiv:1302.6312v1 [cs.DC], pp. 1-15, 2013.

14. J. Dykstra and A. Sherman, "Acquiring forensic evidence from infrastructure-as-aservice cloud computing: Exploring and evaluating tools, trust, and techniques", DoD Cyber Crime Conference, January 2012.

15. R. Marty, "Cloud application logging for forensics", in Proceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011, pp. 178–184.

16. Zafarullah, F. Anwar, and Z. Anwar, "Digital forensics for eucalyptus", in Frontiers of Information Technology (FIT). IEEE, 2011, pp. 110–116.