A Comparative Analysis of Traditional Computer Forensic Tools and Cloud Forensic Tools

Arshdeep Singh, Birla Institute of Technology and Sciences, Pilani, November 30, 2022

Abstract

Digital forensics is the process of collecting evidence from any computing device and investigating, analyzing and preserving the same to present it as legally admissible evidence in the court of law. 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.

In this paper, we will be comparing traditional computer forensic and cloud forensic tools. A literature review will be provided to explain the similarities between the two types of tools and their differences. A comparison of these two types of tools will be made to determine whether they are similar or different in function and purpose. The conclusion will be made based on whether or not there are any significant differences between the two categories of tools as well as how they could be used together.

Keywords: Digital Forensic, Cyber Crime, Computer Forensic and Digital Evidence.

Introduction

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. As computer forensic tools are becoming more common in the courtroom, it is important to understand how they work and how they differ from other types of forensic tools. This paper will review the similarities between traditional computer forensic tools and cloud forensics tools. The idea of forensic computing is not new. In fact, it has been around since the 1980s when the first computer forensics tool was developed. However, its importance has never been more relevant than today due to the rapid growth of cloud computing and its impact on our lives. The two types of forensic tools are traditional computer forensic and cloud forensic tools. Traditional computer forensic is the process of collecting, preserving and analyzing digital evidence from a crime scene. Cloud forensics is the process of collecting, preserving and analyzing digital evidence from a cloud computing environment such as Amazon S3 or Microsoft Azure

Storage. The purpose of cloud forensic tools is to collect and analyze data that has been stored in a cloud computing environment. Cloud forensics differs from traditional computer forensics in several ways. First of all, the evidence you're looking for may not exist on the device itself but rather on an external storage provider such as S3 or Azure Storage. Second, there are no physical devices at the crime scene so they have to be acquired by other means such as an image-based backup from a third party provider or a snapshot from Amazon EC2 instances.

Background

Cloud forensics is a new field in forensic science. Cloud forensics is an emerging research area and it includes various techniques that can be used to analyze data stored in the cloud. The main goal of cloud forensics is to help users recover information from their devices, such as smartphones or laptops after they have been lost or stolen.

Cloud forensics tools are used by law enforcement agencies around the world to investigate cybercrimes like hacking attacks and online frauds; however, many users might not know how they work or what benefits they offer them when compared with traditional methods like hard drive recovery software or USB sticks containing encrypted files (which require specialized knowledge).

If you want to recover data from your cloud storage and are not sure how to do this, then you can use a cloud forensics tool. These tools allow users to search through their encrypted files and find out whether they contain sensitive information that could compromise their privacy.

Cloud forensics is a new field in forensic science. Cloud forensics is an emerging research area and it includes various techniques that can be used to analyze data stored in the cloud. The main goal of cloud forensics is to help users recover information from their devices, such as smartphones or laptops after they have been lost or stolen. Cloud forensics tools are used by law enforcement agencies around the world to investigate cybercrimes like hacking attacks and online frauds; however, many users might not know how they work or what benefits they offer them when compared with traditional methods like hard drive recovery software or USB sticks containing encrypted files (which require specialized knowledge).

Computer forensics

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. 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. Computer proof can be valuable in criminal cases, common questions, and HR/business procedures. Traditional Computer Forensics Tools are the tools used to investigate computer crimes. These traditional forensic tools are divided into two groups: Computer Forensics Software (or just "Forensic Tools") and Physical Hardware

Forensics tools can be classified based on their Functionality, Purpose, Application.

Forensic software is used by various individuals and organizations for different purposes, such as Data acquisition (acquiring evidence from devices) and Analysis of digital data (identifying relevant information from digital sources)

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 the next examination phase.

Extraction: In the 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, the 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.

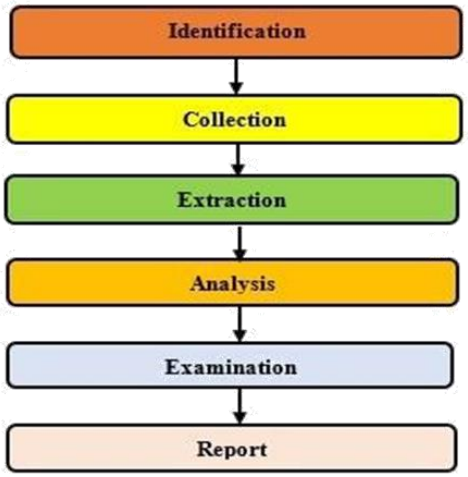

Figure 1: Digital Forensic Investigation Process.

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 shows various sorts of advanced proof.

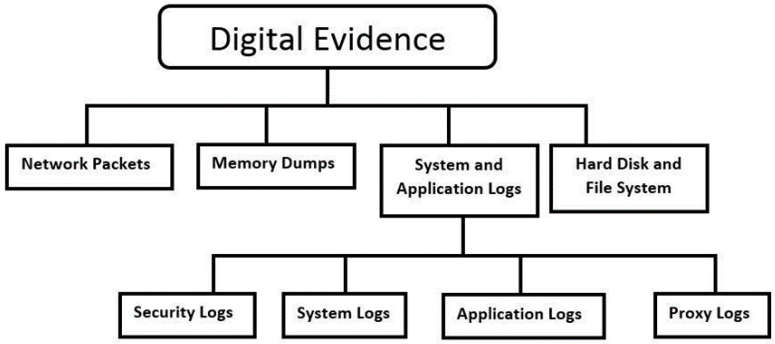

Figure: Digital Evidence Types.

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 forensic tools are used to analyze the cloud environment. Cloud forensic tools are used to perform forensic analysis on cloud environment, such as: Cloud Computing is a form of distributed computing in which shared resources (e.g., storage devices and servers) are accessed remotely over an intranet or internet connection. In contrast with traditional client/server computing, where all processing occurs locally on each computer that is accessing a shared resource, cloud computing allows clients or workers who may be far away from each other the ability to access shared resources through one central server regardless of location or device

Cloud forensics is an emerging area with tremendous potential for growth in data protection, security and privacy issues related to information stored on remote servers in the cloud (e.g., Amazon Web Services). A number of commercial products are now available that offer support for investigating these types of cases but they lack some important capabilities: they cannot handle large amounts of data nor can they operate simultaneously on multiple machines within an organization or even across organizations; they require considerable skill level from their users because they lack clear guidance on how to proceed through each step during investigation process; most importantly there is no automated way yet available today so that end users can easily perform all necessary steps required during investigation process without having any manual assistance from experts who understand what their job entails.

Cloud Forensics Challenges

Cloud forensics is a new field of forensic science that focuses on the examination of cloud computing data. It is also known as network forensics and digital evidence analysis, which refers to the examination of various types of digital media generated by a computer system or networked device.

Cloud forensics has been recognized as a discipline in its own right due to its growing importance in business environments where organizations are relying more heavily on technological systems such as mobile devices, cloud storage services like Dropbox and Google Drive (formerly called Docs), virtual machines running Microsoft Azure [6] Serverless Computing Platforms like AWS Lambda [7] etc.," says Dr Daniel Vrana who teaches at Penn State University's Department Of Computer Science.

Cloud forensics is not without its challenges, however. The first is that CSPs are not required to retain any data for a specific period of time. Therefore, the investigator must work quickly in order to analyze the evidence before it disappears forever! Another challenge is that many cloud services have different types of security measures in place such as encryption, which can make it more difficult for investigators to collect and analyze data from these sources.

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:

The normalized sentence syntax is a formula or structure developed by NIST to express cloud forensics challenges in a consistent and standardized way. This formula allows for a clear and organized representation of the specific challenges related to cloud forensics, making it easier for organizations to understand and address them.

The normalized sentence syntax formula is typically composed of several parts, including a subject, an action, and an object. It may also include additional elements, such as qualifiers or constraints. The subject of the sentence represents the entity or system being investigated, the action represents the task or challenge being addressed, and the object represents the data or information related to the challenge. Qualifiers and constraints provide additional information about the challenge, such as specific conditions or limitations.

This formula allows for clear and consistent communication of cloud forensics challenges, which can help organizations better understand and address these challenges.

It is worth mentioning that the formula of normalized sentence syntax is not only used by NIST but also in different contexts, such as in software development, where it can be used to define user stories or requirements in a consistent and easy-to-understand format.

In the context of cloud forensics, the use of the normalized sentence syntax formula helps organizations to clearly define the specific challenges they are facing and identify the data or information that needs to be preserved or analyzed. This can make it easier for organizations to develop appropriate strategies for addressing these challenges and collecting the necessary evidence.

An organization that is facing a cloud forensics challenge related to data preservation may use the normalized sentence syntax formula to clearly define the specific data that needs to be preserved, and the specific conditions or constraints related to that data, such as time limits or legal requirements. This can help the organization to develop an appropriate data preservation plan and ensure that all necessary steps are taken to preserve the relevant data.

In summary, the normalized sentence syntax formula, developed by NIST, is a powerful tool for expressing cloud forensics challenges in a consistent and standardized way, which can help organizations to better understand and address these challenges

An example of a cloud forensics challenge that can be expressed using the normalized sentence syntax formula is: "As a cloud service provider, identify and preserve all data stored in a specific cloud account associated with a specific user, within 24 hours of receiving a legal request."

In this example, the subject of the sentence is "cloud service provider" which represents the entity or system being investigated. The cloud service provider is responsible for identifying and preserving all data stored in a specific cloud account associated with a specific user.

The action of the sentence is "identify and preserve", which represents the task or challenge being addressed. In this case, the cloud service provider needs to identify all data stored in a specific cloud account associated with a specific user and preserve it.

The object of the sentence is "all data stored in a specific cloud account associated with a specific user", which represents the data or information related to the challenge. In this example, the data that needs to be preserved is all data stored in a specific cloud account associated with a specific user.

The constraint of the sentence is "within 24 hours of receiving a legal request", which provides additional information about the challenge, such as specific conditions or limitations. In this case, the cloud service provider has only 24 hours after receiving a legal request to identify and preserve the data.

This example illustrates how the normalized sentence syntax formula can be used to clearly and concisely express a cloud forensics challenge. By using this formula, the cloud service provider can understand exactly what data needs to be preserved and how to preserve it under a legal request.

It also shows that cloud forensics challenges can be complex and time-sensitive, and it's important for organizations to have clear and consistent ways of expressing them to be able to address them properly and timely.

Cloud Forensics Opportunities

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

Practical: Implement forensic assistance in a distributed computing climate that permits using the immense limits of distributed computing without moving 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 to recuperate the lost and erased information from the cloud to confirm 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 the 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 this table, a comparison study between Classic Forensic and cloud forensic is tabulated to explain the differences between both above two types of forensics.

	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

Table : Comparison between Computer Forensic and Cloud Forensic.

Conclusion

The current study has shown that traditional computer forensic tools are limited to digital evidence recovery, while cloud forensic tools are more powerful and flexible. The study also highlights the importance of using open source tools for in-depth analysis of data located in the cloud environment. This work will worry about creating capable computerized forensic strategies for examination of cybercrimes in distributed computing in a forensically solid and opportune way. It will present research commitments in the field of cloud forensics.

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 completing this exploration work.

In conclusion, it is important to note that traditional forensic tools are still useful and relevant in the investigation of cybercrime. The ability of these tools to produce high-quality evidence has been proven in various criminal cases over the years. However, as we move towards cloud computing and big data analysis, there will be an increasing need for alternative solutions that can help with this process. Cloud forensic tools offer a number of advantages over their traditional counterparts including Ability to collect data from multiple sources (e.g., servers) at once; Control over all aspects of data collection and processing; Flexible architecture allowing for faster analysis times without sacrificing accuracy or quality; High degree of automation which makes them ideal for large scale investigations where resources may not be available for manual processing

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 be a 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.

17. D. Birk and C. Wegener, “Technical issues of forensic investigations in cloud computing environments”, Systematic Approaches to Digital Forensic Engineering, 2011.

18. J. Dykstra and A. Sherman, “Understanding issues in cloud forensics: Two hypothetical case studies”, Journal of Network Forensics, vol. b, no. 3, pp. 19–31, 2011.