Digital Forensic in Cyber Security

Sharanya Mohanan.C.V
Assistant Professor On Contract
Carmel College Mala

***Abstract*:- Digital Forensics could be a branch of forensic science which has the identification, collection, analysis and news any valuable digital info within the digital devices with the pc crimes, as a region of the investigation. It includes the world of study like storage media, hardware, OS, network and applications. This paper presents the importance of digital forensics within the field of security in modern world.**

keywords-cybersecurity, mobile forensic cybercrime, software.

I INTRODUCTION

"Digital forensics" could be a broad term bearing on the look for and detection, recovery and preservation of proof found on digital systems, usually for criminal or civil legal functions.

Digital forensics will typically involve the acquisition of proof regarding events within the physical world. An example, sick deleted emails that link a suspect to a murder or alternative crime. The Computers, mobile devices still play a bigger role in just about each side of society, the demand for digital forensic consultants is probably going to rise, very much like it's with cyber security consultants. Aim of pc forensics techniques is to go looking, preserve and analyze data on pc systems is to seek out potential proof as an attempt as an example simply gap a data file changes the file.

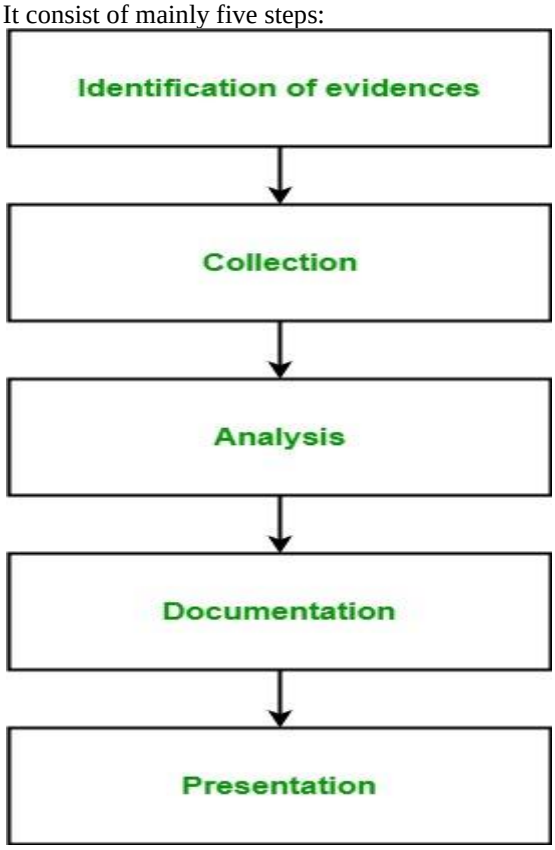
II DIFFERENCE BETWEEN FORENSIC SECURITY AND CYBERSECURITY

As a sub-domain of the cyber security field, the distinction between the duties of execs operating in digital forensics and people operating in additional ancient cyber security roles may be compared to the distinction between a detective and a patrol officer in real-world policing. The patrol officer's task is essentially to forestall offenses from occurring, or notice and take action once they're happening. The detective job is to research offenses once the event, is verified. While there could also be quite an little bit of overlap in duties with alternative cyber security occupations, digital forensic specialists specialize in past events instead of the interference of current or future happenings.

Digital forensic investigator can gather proof from a specific electronic computer in order that it may be conferred in court, conducting a radical digital investigation and building a documented chain of proof. Investigators use a range of techniques and proprietary package forensic applications to look at the copy, looking out hidden folders and unallocated space for copies of deleted, encrypted, or broken files."This proof is then verified against the first device and collated in a very finding report, that is leveraged in any later legal proceedings.

III LEVELS OF DIGITAL FORENSICS

It consist of mainly five steps:



1. Identification:

It is the distinctive evidences associated with the digital crime in storage media, hardware, package, network and/or applications. it's the foremost necessary step.

2. Collection

It includes digital evidences known within the opening move in order that they doesn't degrade to fade with time. protective the digital evidences is incredibly necessary and crucial.

3. Analysis:

It includes analyzing the collected digital evidences of the committed pc crime so as to trace the criminal .

4. Documentation:

It includes the right documentation of the total digital investigation, digital evidences, loop holes of the attacked system etc. in order that the case will be studied and

analysed in the future conjointly and might be bestowed within the court in a very correct format.

5. Presentation:

It includes the presentation of all the digital evidences and documentation within the court so as to prove the digital crime committed and determine the criminal.

IV BRANCHES OF DIGITAL FORENSICS

- ***Media forensics***

It is the branch of digital forensics which has identification, collection, analysis and presentation of audio, video and image .

- ***Cyber forensics:***

It is the branch of digital forensics which has identification, collection, analysis and presentation of digital evidences throughout the investigation of a cyber crime.

- ***Mobile forensics:***

It is the branch of digital forensics which has identification, collection, analysis and presentation of digital evidences throughout the investigation of against the law committed through a mobile devices like mobile phones,GPS device,tablet, laptop.

- ***Sofware forensics:***

It is the branch of digital forensics which has identification, collection, analysis and presentation of digital evidences throughout the investigation of against the law associated with softwares solely.

VI. NEXT GENERATION DIGITAL FORENSICS

A. Cloud Forensics

The cloud computing paradigm presents several edges each to organizations and one among such blessings relates to the style during which knowledge is managed by the cloud infrastructure. for example, knowledge is unfold between numerous knowled ge centres to enhance performance and facilitate load-balancing, measurability.

As a result, proof left by adversaries is harder to eliminate since it are often derived in numerous locations, rendering the acquisition of proof and its examination easier to perform. Despite its several edges, cloud computing poses important challenges to the LEAs and DFEs from a rhetorical perspective.

These embrace, however aren't restricted to, issues related to the absence of standardization amongst completely different CSPs, variable levels of information security and their service level agreements.

B. Network Forensics

A Network forensic Investigation (NFI) pertains to the acquisition, storage and examination of network traffic (encapsulated in network packets) generated by a bunch, associate degree intermediate node, or the complete portion of a network so as to determine the supply of a security attack. Network traffic objects that need analysis incorporates protocols used, informatics addresses, port numbers, timestamps, malicious packets, transferred files, useragents, application server versions, and OS versions, etc. This knowledge are often nonheritable from differing kinds of traffic.

C. web of Things (IoT) Forensics

The Internet of Things (IoT) that is supported by the cloud, huge knowledge and mobile computing typically connects something and everything ‘online’. The IoT represents the interconnection Some IoT devices square
measure normal things with inherent web property, hereas some square measure sensing devices developed specifically with IoT in mind. The IoT covers technologies, such as: remote-controlled aerial vehicles,good swarms,good grid,good buildings and residential appliances autonomous cyber-physical and cyberbiological systems, wearables, embedded digital things, machine to machine communications, RFID sensors, and context-aware computing, etc. every of those technologies has become a particular domain on their own advantage.

With the new styles of devices perpetually rising,the IoT has virtually reached its uttermost evolution. With associate degree calculable range of fifty billion devices that may be networked by 2020 it's calculable that there'll be ten connected IoT devices for each person worldwide.

VII CONCLUSION

The field of Digital forensics is facing numerous challenges difficult to beat because the new technologies square measure perpetually being developed, Digital forensic’s square measure given with varied challenges which will have substantial socioeconomic impact on each international enterprises and people

Evidentiary knowledge isn't longer restricted to one host however instead unfold between completely different or virtual locations, including: on-line social networks, cloud resources, and private network–attached storage devices. what is more, advances in technology and propagation of innovative services have semiconductor diode to a major rise within the quality of DFIs that DFEs should manage.Hence, to mitigate these challenges, worldwide collaboration among LEAs, tutorial establishments and corporate of dominant importance becomes . To facilitate analysis efforts that stretch each other, rhetorical analysis can lag behind, tools can become noncurrent, and law enforcements’ product are going to be incapable of counting on the results of DF analysis.

VIII REFERENCES

[1] Montasari, R. (2017, a). An Overview of Cloud Forensics Strategy: Capabilities, Challenges, and Opportunities. In Strategic Engineering for Cloud Computing and Big Data Analytics, pp. 189-205. Springer, Cham.

[2] Caviglione, L., Wendzel, S. and Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security & Privacy, (6), pp.12-17.

[3] Taylor, M., Haggerty, J., Gresty, D. and Lamb, D. (2011). Forensic investigation of cloud computing systems. Network Security, 2011(3), pp.4-10.

[4] Bojanova, I and Voas, J. (2015). 'Securing the Internet of Anything (IoA)'.

[5] Next-Generation Digital Forensics: Challenges and Future Paradigms, Reza Montasari Department of Computing and Engineering The University of Huddersfield Huddersfield, U.K.