ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

Role Of Computers in Digital Forensics

Hameem Mohammed[1], Vipin Vasu A. V[2]

P. G. Student, Dept. of Computer Engineering, College of Engineering, Thiruvanandhapuram, Kerala[1]

Associate Professor, Dept. Of Computer Engineering, College of Engineering, Thiruvanandhapuram, Kerala[2]

Abstract: The report focuses on computers' roles in digital forensics. As the world moves toward digitalization, all of these industries are incorporating digitalization into their operations. Working procedures are becoming more efficient and effective as a result of digitalization. We only need a computer or a system to use digitalization. There are some forensics software tools available that must be installed on computers in order to perform the task. It provides us with the advantage of quick operations. The use of the Internet and information communication technology is rapidly increasing in the modern world. Almost all valuable and confidential information is stored in computers or computer-based systems, and the majority of people share their personal information on social networks like Facebook. Because of the advancement of information and communication technology, there has been a significant increase in the number of computer-based or online criminals all over the world. Criminals who commit murder, kidnapping, sexual assault, extortion, drug dealing, economic espionage & cyber terrorism, weapon dealing, robbery, gambling, economic crimes, and criminal hacking, such as web defacements and computer file theft, keep files containing convicting evidence on their computer.

Keywords: Computer forensics, computer crime, digital evidence, Digital Forensic.

I. INTRODUCTION

The use of the Internet and information technology has grown rapidly throughout the world in the twenty-first century. The increased number of criminal activities involving digital crimes or e-crimes worldwide is directly related to this growth. These digital crimes present new challenges for the prevention, detection, investigation, and prosecution of related offences.

Because of the highly technical nature of digital crimes, a new branch of forensic science known as computer forensics has emerged. Computer forensics is a new field of study that employs computer investigation and analysis techniques to aid in the detection of these crimes and the collection of digital evidence suitable for presentation in court. This new field combines knowledge of information technology, forensic science, and law, and it gives rise to a number of intriguing and challenging computer security and cryptography problems that have yet to be solved [1].

Many local law enforcement agencies have recently become interested in computer forensics. It is now used for judicial expertise in almost every type of enforcement activity. However, it lags behind other methods, such as fingerprint analysis, due to fewer efforts to improve its accuracy. As a result, the legal system is frequently in the dark about the legitimacy, or even the significance, of digital evidence [2].

Digital Forensics is a method of using scientific knowledge and cutting-edge technology in a court of law. The primary goal of digital forensics is to present a structured inspection while organising a documented series of proof and evidence to determine exactly what happened on a digital device. It is the great evolution of technology; digital forensics devices must be updated. Forensics is based on the assumption that every criminal leaves a trace of himself behind-when two things are linked to each other, they are transferred between them, and one criminal can be linked to the crime through evidence conveyed from the scene of the crime [3].

The digital forensics operation is a well-known factual and forensics action in digital forensics examination.

Digital Forensics operation has the following five basic steps:

1.Identification:

It is the first stage of a digital forensic investigation. The Identification operation entails determining what proof is present, where it is gathered, and finally how it is gathered (in which arrangement). It identifies potential sources of relevant evidence, as well as key conservators and data positions. Personal mobile phones, computers, and PDAs are examples of computerised storage media.

2. Preservation:

It is the process of storing relevant computerised data. Data is currently secluded or isolated. It entails preventing people from using the electronic device so that the digital confirmation is not satisfied.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

3. Analysis:

At the moment, inspection agents are restoring data fragments and drawing conclusions based on witnesses discovered. However, it may take several examination repetitions to support a specific crime thesis. A thoroughly systematic search for evidence related to the event under consideration.

4. Documentation:

The History of all detectable data must be designed during this phase. To begin, documents are built around demonstrating technique and methodology. It aids in the regeneration and evaluation of the crime scene. It includes proper evidence and crime scene documentation, as well as snapshots and crime-scene retailing.

5. Presentation:

The operation of outline, summarization, and clarification of opinions is completed in this final phase. Digital forensics is more than just gathering, processing, and presenting data. It is all about current research and staying up to date, so one forensics must first be a scientist before entering the field of digital forensics.

Digital forensics is a multidisciplinary and inter-disciplinary field that includes criminology, law, ethics, computer engineering, information and communication technology (ICT), computer science, and forensic science. Figure 1 [4] depicts a typical way of depicting these related disciplines.

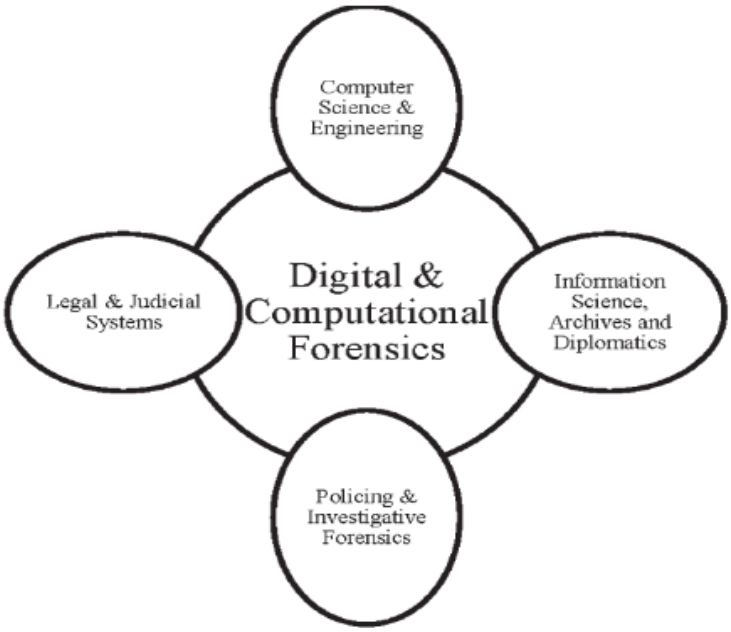

Figure 1: Multiple domains of digital forensics

It is the process of locating and interpreting electronic data in order to preserve any evidence in its most authentic form. Although the field of digital forensics is still in its infancy, increased public awareness of DF has drawn many to it. It is transitioning from a relatively obscure tradecraft to a scientific field that must constantly be held to higher standards. Several next-generation forensic analysis systems are in the works. Colleges and universities all over the world have begun to include DF courses in their information security curricula at the undergraduate and graduate levels.

Computer Role In Digital Forensics:

The job of PC criminology in wrongdoing will simply become more sought after as the need for assistance with recovering data that can be used as evidence becomes increasingly difficult for law enforcement. This developing field of study now, more than ever, requires IT experts who are the best at this type of information recovery for law implementation. According to Forbes Magazine, the top job opening for 2015 is for IT experts, and this is only for established types of IT positions. IT aptitude in law implementation isn't a simple position, but it is one that changes the essence of law authorization with method and dominance to illuminate examples and have unrivalled ramifications.

Computer Forensics Tools:

Various software tools are used in the field of computer forensics. Individuals who work in this field are referred to as investigators. They must perform operations such as searching for the encrypted file. The term is "live box," and other new tools are available for investigation purposes. That is why they are the best in the business. In most cases, common operations such as recovering deleted files, recovering deleted passwords, and recovering from raw data are performed.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

The evidence gathered during the investigation processes will be sent as proof to lawyers, judges, and police for further action. The main task of computer forensics is not only to recover data, but it is also important to solve cases. Computer forensics tools enable investigators to process all of this data in order to find a solution and close the case [5].

Computer Forensics Tools:

There are numerous free computer forensics tools available, which can be classified into the following categories:

- Disk and data capture tools
- Email analysis tools
- File viewers
- File analysis tools
- Application analysis tools
- Registry analysis tools
- Internet analysis tools
- Mac OS analysis tools
- Mobile devices analysis tools
- Network forensics tools
- Database forensics tools

Objectives:

- Creating a computer forensic detail that contains comprehensive information about the exploration process.
- Creating policy at a suggested wrongdoing scene that assists you in ensuring that the digital confirmation obtained is not manipulated.
- It helps to suggest the motive for the crime and the similarity of the main offender.
- It can assist in retrieving, exploring, and storing computer and familiar data in such a way that it allows the inspection agency to represent them as witnesses in court.
- Retrieving deleted files and documents from digital media in order to substance and authenticate them.

II. REVIEW OF LITERATURE

Computer forensics is defined as "the preservation, identification, extraction, interpretation, and documentation of computer evidence, including the rules of evidence, legal processes, evidence integrity, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found," according to Steve Hailey, Cyber security Institute. [6].

Computer forensics, network forensics, mobile device forensics, memory forensics, and email forensics are the five branches of digital forensics (Kumari, N. et al., 2016). [7]

The science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media is known as computer forensics (M. G. Noblett, 2010). [8]

Network forensics is defined as "the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyse, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success, of unauthorised activities intended to disrupt, corrupt, or compromise system components, as well as providing information to assist in response to or recovery from such activities" (Gary Palmer, 2001). [9]

Mobile device forensics is a subfield of digital forensics concerned with recovering digital evidence from mobile devices under forensically sound conditions and using accepted methods (Kevin Curran, 2010). [10]

III. RESULT AND DISCUSSION

Because of the rapid evolution of information technology, almost everything is now computerised or electronic-based, such as e-banking, e-learning, e-commerce, and so on. Due to their hectic schedules, people are always looking for quick and easy ways to complete their day-to-day activities using technology. As a result, computer or cybercrime has recently been reported as the world's second most prevalent crime. According to the 19th CEO survey, 32% of organisations have been affected and 34% expect to be affected in the next two years. Most businesses are still not adequately prepared for or understand the risks they face. Only 37% of businesses have a cyber incident response plan in place. Although 61% of CEOs are concerned about cyber security, less than half of the board is. [11]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

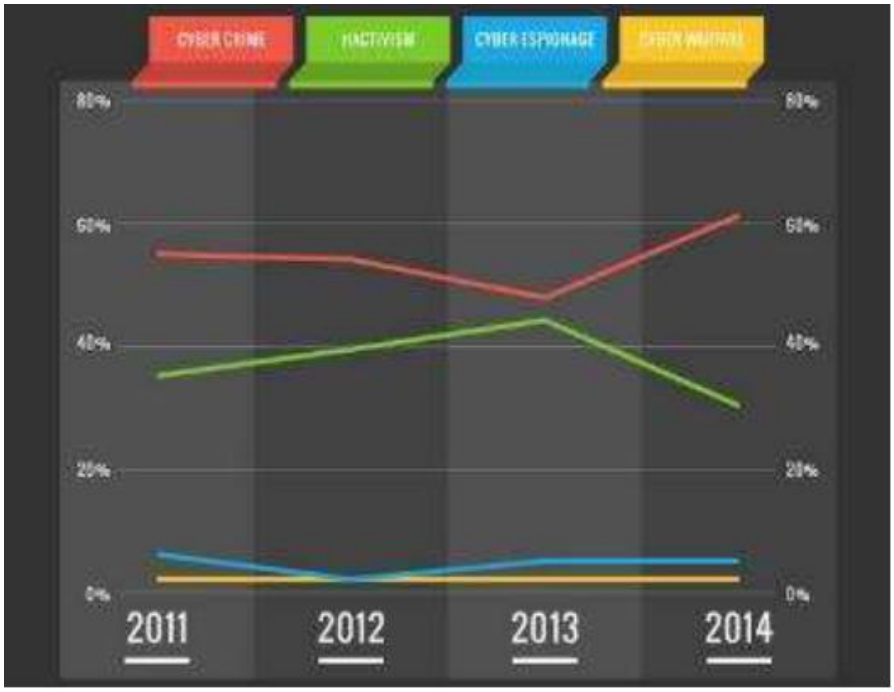

Figure 2: Motivation behind cyberattacks over the years

Cyberwarfare - when a cyber-attack is used as a form of terrorism against a government Figure 2 depicts the motivation behind cyberattacks from 2011 to 2014.

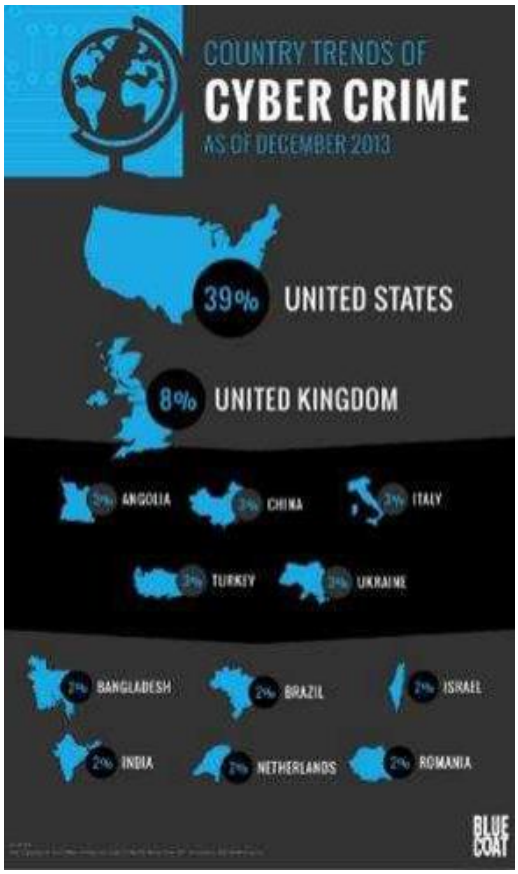

Figure 3: Country trends of cybercrimes according to the Blue Coat website

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

According to the Blue Coat website, Figure 3 depicts the country trends in cybercrime. As of December 2013, 39% of cybercrimes were reported in the United States, while 8% were reported in the United Kingdom. China, Italy, Turkey, Ukraine, and Angola reported 3%, while India, Bangladesh, Brazil, Israel, the Netherlands, and Romania reported 2%. [12]

IV. CONCLUSION

A person in charge of investigating a crime should be familiar with the basic technologies involved in gathering information, how to properly gather data, and how to confirm that the information will be valid as evidence during the investigation. It is critical to acquire, authenticate, and analyse data stored in electronic devices, regardless of whether they run Microsoft or Linux operating systems. Furthermore, an experienced investigator should be familiar with the technologies used in tracing and identifying a specific computer user's actions. The main goal of this paper is to bring together the use of computer forensics, digital forensics tools, and issues facing computer forensics, as well as legal aspects of computer forensics and its application; however, it is not intended to be a comprehensive description of the computer forensic field. Furthermore, computer forensics is a growing field that will only expand as laws evolve and computer technology becomes more prevalent. Finally, it is critical to avoid becoming a criminal while investigating criminal activities.

REFERENCES

[1] Hui, L.C.K., Chow, K.P., Yiu, S.M.: Tools and technology for computer forensics: research and development in Hong Kong. In: Proceedings of the 3rd International Conference on Information Security Practice and Experience, Hong Kong (2007)
[2] Wagner, E.J.: The Science of Sherlock Holmes. Wiley, Chichester (2006)
[3] B.Carrier and E. Spafford, An event-based digital forensic investigation framework. Digital Investigation. (2015)
[4] M. Losavio, K. C. Seigfried-Spellar, and J. J. Sloan III, “Why digital forensics is not a profession and how it can become one,” Criminal Justice Studies, vol. 29, no. 2, 2016, pp.143-162.
[5] B. Martini, An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71-80. (2016).
[6] Hailey, S.: What is Computer Forensics (2003)
[7] N. Kumari and A. K. Mohapatra, An insight into digital forensics branches and tools, Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies, 2016.
[8] Michael G. Noblett, Mark M. Pollitt, Lawrence A. Presley. Recovering and examining computer forensic evidence, 2010
[9] Gary Palmer, A Road Map for Digital Forensic Research, Report from DFRWS 2001, First Digital Forensic Research Workshop, Utica, New York, August 7 – 8, 2001, Page(s) 27–30.
[10] Curran K., Robinson A., Peacocke S., Cassidy S., Mobile Phone Forensic Analysis, International Journal of Digital Crime and Forensics, Vol. 2, No. 2, 2010.
[11] Legal Methods of Using Computer Forensics Techniques For Computer Crime Analysis and Investigation-Daphyne Saunders Thomas, Karen A. Forcht
[12] Digital Crime and Forensics - Prashant Mahajan & Penelope Forbes