Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.6 : 2024
ISSN : **1906-9685**

A STUDY ON DIGITAL FORENSIC: A NEW FACE TO THE DIGITAL WORLD

Dr. R. KARTHIK, ASST PROFESSOR, Department of Data Science
Ms. GOPIKA.V, Ms. SUBIKSHA.R, Department of Computer Applications
SRI KRISHNA ADITHYA COLLEGE OF ARTS AND SCIENCE, COIMBATORE

Abstract:

The risk of data misuse is growing in pace with the exponential growth in data storage and utilization in the modern world. We require a technological solution that will allow us to hold individuals accountable for attacks on computer systems all around the world accountable. This has made the information gathered by humans or robots and kept on controllers, mobile devices, or computers susceptible to several hacks. In this paper we have a comprehensive study on digital forensic process, Challenges, investigation methods, future scope and its applications.

Keywords: *Forensics, Digital evidence, exoneration, seizure*

INTRODUCTION:

Digital devices such as cell Phones, Tablets, gaming consoles, laptop and desktop computers have become indispensable part of the modern society. with the proliferation of these devices in our everyday lives, there is the tendency to use information derived from them for criminal activities. Crimes such as fraud, drug trafficking, homicide, hacking, forgery and terrorism often involve computers.

FORENSICS:

Forensic can be defined as the application of scientific methods to criminal cases. In particular forensic science deals with the analysis of evidence criminal cases.

DIGITAL FORENSICS:

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically. The main goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence and present the findings for prosecution. All processes utilize sound forensic techniques to ensure the findings are admissible in court.

HISTORY OF DIGITAL FORENSICS:

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1982 – 1911): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.
- In 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called “Best practices for Computer Forensics”.
- In 2010, Simson Garfinkel identified issues facing digital investigations.

BRANCHES OF DIGITAL FORENSICS:

- **Disk Forensics**:

It deals with extracting data from storage media by searching active, modified, or deleted files.

- **Network Forensics:**

It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

- **Wireless Forensics:**

It is a division of network forensics. The main aim of wireless forensics is to offers the tools need to collect and analyse the data from wireless network traffic.

- **Database Forensics:**

It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

- **Malware Forensics:**

This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

- **Email Forensics**

Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

- **Memory Forensics:**

It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

- **Mobile Phone Forensics:**

It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and

SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

DIGITAL FORENSIC PROCESS:

1.IDENTIFICATION OF EVIDENCE:

It includes of identifying evidences related to the digital crime in storage media, operating system, network and applications.it is the most important and basic step.

2.COLLECTION:

It includes preserving the digital evidences identified in the first step so that they do not degrade to vanish with time. Preserving the digital evidences is very important and crucial.

3.ANALYSIS:

It includes Analysing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.

4.DOCUMENTATION:

It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc… so that the case can be studied and analysed in future also and can be presented in the court in a proper format.

5.PRESENTATION:

It includes the presentation of all digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

REAL TIME EXAMPLE:

ROSS COMPTON IN 2017

In this one of a case, the data from Compton's pacemaker actually served as evidence in court. The data, which included his heart rates and pacer demand helped to prove that he had actually submitted fake medical certificates and engaged in insurance fraud and arson of his $400,000 home.

Compton claims that he was asleep when his house caught on fire. He states that when he awoke and saw the blaze, he quickly packed clothes and other belongings into bags and leaped from his bedroom window with his belongings to get to safety after breaking it with a cane. Police later found that this statement from Compton proved to be inconsistent with the evidence that they later found after collecting reports from his pacemaker before, during and after the fire took place.

According to documents provided by the court, a cardiologist who reviewed reports from Compton's pacemaker stated that is highly unlikely that Compton quickly packed numerous belongings and exited the house with several bags from a bedroom window. This is especially hard to believe at Compton's age of 60 and his heart condition. The Cardiologist was quoted as stating: "It is highly improbable Mr. Compton would have been able to collect, pack and remove the number of items from the house, exit his bedroom window and carry numerous large and heavy items to the front of his residence during the short period of time he has indicated due to his medical conditions." The case is still currently pending, as the defence is appealing the court's decision to allow the use of Compton's pacemaker data as evidence. However, if it is allowed, the use of digital forensics can be accredited with putting out the flames of Compton's insurance fraud inferno.

APPLICATION OF DIGITAL FORENSICS:

According to Forensic Control, Sometimes, it's used to prevent crime, and other times, it's used to gather evidence necessary to prosecute or exonerate someone accused of a crime.
These are some of the most important ways digital forensics can be used and applied:

- **CRIME PREVENTION:**

First, and perhaps most importantly, digital forensics can be used to prevent crimes from happening. Forensics experts, with the right tips and initial investigative direction, are able to uncover pieces of information on suspects, including messages they've sent and people they've contacted, to determine whether a crime could take place.

- **DIGITAL CRIME RECOGNITION:**

Digital forensics can also be used to reconstruct how previous events have unfolded. This is especially important in the world of accounting and banking. If someone's credit card information is stolen and used by someone else, digital forensics teams need to be able to determine where the information was stolen, when it was used, and how it was used in order to prosecute effectively.

- **SUPPLEMENTARY EVIDENCE GATHERING:**

Gathering supplementary data to build a case. In these instances, the crime is usually physical, rather than digital. For example, if someone is involved in a car accident, digital forensics can prove or disprove whether they were texting while driving, possibly Some digital forensics experts focus on leading to the crash. In a personal injury case, forensics experts can gather information on where you were and what you were doing to reconstruct the event.

- **POSITION TRACKING:**

Most of the time, you[illegible]king your locati[illegible]ovement—even if you've turned off position tracking in your settings. While this may be uncomfortable to recognize as an individual, it's a good thing for building strong cases. Being able to recognize where you were at various points in time is a must-have for high-profile cases.

- **EXONERATION:**

In some cases, evidence gathered through digital forensics can be used to exonerate someone, by proving they couldn't have taken a specific action, or that they were in a location far away from where the crime actually took place. If you're falsely accused of a crime, your phone's metadata could be all it takes to set you free.

INVESTIGATION METHODS:

The digital forensic process is intensive. First, investigators find evidence on electronic devices and save the data to a safe drive. Then, they analyse and document the information. Once it's ready, they give the digital evidence to police to help solve a crime or present it in court to help convict a criminal.

The Nine Phases of Digital Forensics

There are nine steps that digital forensic specialists usually take while investigating digital evidence.

1. First Response

As soon as a security incident occurs and is reported, a digital forensic team jumps into action.

2. Search and Seizure

The team searches devices involved in the crime for evidence and data. Investigators seize the devices to make sure the perpetrators can't continue to act.

3. Evidence Collection

After seizing the devices, professionals collect the data using forensic methods to handle the evidence.

4. Securing of the Evidence

Investigators store evidence in a safe environment. In the secure space, the data can be authenticated and proved to be accurate and accessible.

5. Data Acquisition

The forensic team retrieves electronically stored information (ESI) from the devices. Professionals must use proper procedure and care to avoid altering the data and sacrificing the integrity of the evidence.

6. Data Analysis

Team members sort and examine the authenticated ESI to identify and convert data that is useful in court.

7. Evidence Assessment

Once ESI is identified as evidence, investigators assess it in relation to the security incident. This phase is about relating the data gathered directly to the case.

8. Documentation and Reporting

This phase happens once the initial criminal investigation is done. Team members report and document data and evidence in accordance with the court of law.

9. Expert Witness Testimony

An expert witness is a professional who works in a field related to the case. The expert witness affirms that the data is useful as evidence and presents it in court.

DIGITAL FORENSIC TOOLS:

Digital forensics tools are **hardware and software tools that can be used to aid in the recovery and preservation of digital evidence**. Law enforcement can use digital forensics tools to collect and preserve digital evidence and support or refute hypotheses before courts.

With any digital forensic investigation, **EnCase and FTK** are the two most commonly used tools by law enforcement.

Some of the forensic tools are:

- The Sleuth Kit
- Wireshark
- Forensic Toolkit
- Encase
- Caine Linux
- Windows Registry
- Windows SCOPE and etc….

ADVANTAGES OF DIGITAL FORENSICS:

Some of the advantages are:

- Analysis for allowing digital evidence
- Helps to identify criminals
- Can be used to recover deleted data
- Provides insight into how crimes are committed
- Can be used to prevent future crimes.

DISADVANTAGES OF DIGITAL FORENSICS

- Time-consuming process
- Requires specialized skills and knowledge
- Can be expensive
- May require court order to obtain evidence
- Lack of technical knowledge by the investigating officer might not offer the desired result

CHALLENGES FACED BY DIGITAL FORENSICS:

Here, are major challenges faced by the Digital Forensic:

- The increase of PC’s and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions

FUTURE SCOPE OF DIGITAL FORENSIC:

Digital forensic is a type of maturing science. These are the few pointers for direction of future scope of research in this area: Application of the new model in variety of cases and improvement in light of feedback. Identification of new constraints in terms of technological advancement will require model to be updated with time. Most of the digital forensic tools are commercial version, whose costs are high and are operated by professional forensic, so we mostly use opensource forensic tools because they are easy to use and are less costly. The opensource tools for forensic investigations which reduce the cost of tools as compare to commercials tools.

CONCLUSION:

AI and deep learning in digital forensics is transforming the investigative environment, empowering organisations with the ability to access evidence faster and uncover more relevant findings. These technologies can process and analyse data within minutes making the Process of discovery and investigations more agile.

Digital forensics is a rapidly advancing field that has many challenges and crosswinds. The opportunities are endless, but they are not for the faint of heart. Frustration is a common partner, so the ability and mentality to press on through is a key characteristic an investigator should have. Someone who needs to be shown how to do everything may want to rethink their career options. A can-do attitude is essential, but the investigator does not need to do it alone. A variety of resources are available to assist, and most of the investigators who have worked through the learning curve to achieve competence are more than eager to help others do the same. Usually, they had others to lean on, so once you reach a level of expertise with the assistance of others, do not forget to return the favour.

REFERENCE:

1. Volume 7, Issue 4, April 2017 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com
2. Book: DIGITAL FORENSICS by Dr. Jeetendra Pande and Dr. Ajay prasad
3. International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.6, December 2014 DOI:10.5121/ijcsa.2014.4608 89 An Insight View of Digital Forensics Neha Kishore, Chetna Gupta
4. (15 June). Digital Forensics. Available: http://www.techopedia.com/definition/27805/digital-forensics
5. L. Garber, "Encase: A case study in computer-forensic technology," IEEE Computer Magazine January, 2001.
6. E. Casey, Digital evidence and computer crime: forensic science, computers and the internet: Academic press, 2011.
7. www.iigpi.com/5-cases-cracked-with-digital-forensics/46/2821/
8. www.digitalconnectmag.com/the-5-most-important-applications-for-digital-forensics/
9. sentreesystems.com/pros-and-cons-of-computer-forensics/