Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Forensic Procedures in Electronic Crime Scene Management and Police Investigations

Nagendar Rao Koppolu[1], Vishnu Murthy Gunda[2]

[1]Research scholar, Department of Computer Science and Engineering, Anurag University, Telangana, India.
[2]Professor, Department of Computer Science and Engineering, Anurag University, Telangana, India.
Email: knagenderrao@yahoo.com

The advancements in digital communication technology and internet services have brought a paradigm shift in the lives of people and, in no time, became part of their lives. Their ubiquitous nature provides ample opportunities for those with criminal intentions. Growing cyber threats such as data thefts, phishing scams, online financial crimes, and other electronic crimes are affecting people's lives more than ever before. These incidences are harming the nation's strategic and competitive advantages as well as its economic growth. The increasing use of the Internet and Social Media Applications by people and organizations for various activities made it imperative for Law Enforcement Agencies to rise to the challenges and protect their privacy, assets, and critical information. The police require new investigation techniques and digital forensic procedures to effectively respond to these electronic crimes. The goal of this research paper is to give a thorough review of the forensic techniques used in managing electronic crime scenes and conducting police investigations. This paper addresses the value of digital forensics, the procedures involved in the forensic process, challenges faced by the investigators, and new developments in the field in line with the requirements of the Investigating Officers. It presents an approach that makes collecting and analyzing electronic evidence easier and increases the effectiveness of police investigation. It also discusses the gap areas in existing digital forensic frameworks and assess the need for police investigators to concentrate on non-traditional areas of the electronic systems to collect and analyze electronic evidence. In order to effectively address electronic crimes, it concludes by underlining the significance of cooperation among law enforcement agencies, forensic specialists, and other stakeholders.

Keywords: Artifacts, chain of custody, crime scene, cyber kill chain, digital forensics, electronic evidence, forensic analysis, investigation, law enforcement, operating system.

1. Introduction

1.1. Background

Cyberspace has made inroads in our day-to-day life with affordable and accessible internet and other communication mediums. Due to the quick proliferation of cyber technology, using computers, smartphones, and other electronic devices for daily tasks has now become the standard. With such a degree of penetration and usage of cyberspace, electronic crimes and victimization of women and children are also increasing. Incidences of hacking, cyberstalking, harassment on social media and online fraud are increasing at an alarming rate across the globe affecting the business and individuals like never before. The new-age crimes require novel ways to investigate and collect electronic evidence.

1.2. Objective

The objective of this research paper is to provide a thorough understanding of how to handle electronic crime scenes and conduct police investigations using digital forensic techniques. Also, to counteract the growing threat of electronic crimes, to emphasize the crucial role that digital forensics play in modern law enforcement and the necessity for continued study, training, and collaboration.

With the evolution of cutting-edge technologies, collection and analysis of electronic evidence has become complex and understanding the intricacies involved in it constantly bothering the police investigators than before as they are responsible for protecting public property and maintaining law and order. For police investigations and prosecutions to be effective, investigators must have a thorough awareness of the many facets of electronic evidence. It is necessary for police investigators to have a solid understanding of various aspects of electronic evidence to be successful in police investigations and prosecutions. In this regard, the field of digital forensics aids the prosecutors and jurors in understanding complex data more easily and identifying relationships between crime data for reconstruction of historical events and better understanding of crime based on its merits. During the investigation and prosecution of both civil and criminal cases, many digital forensic procedures, and techniques aid in determining and validating the electronic evidence [1].

2. Literature Review

The purpose of a literature review is to provide an outline of the current research on the collection and analysis of electronic evidence. The examination of the artifacts can yield crucial information about the actual events in the criminal and civil cases. As such, researchers have explored various methods for the collection and analysis of artifacts related to the operating system, browser, social media applications etc.

In [2], Asma Majeed and Shahzad Saleem discussed how the development of technology has made it difficult for digital forensic analysis to carry out its tasks. The knowledge of various artifacts of frequently used applications might help solve various types of police cases. The authors of this research have examined the behavior of the social media applications like Twitter, Facebook, Viber and Skype on Windows 10 system. The forensic examination of the artifacts left by social media applications on Windows 10 system has been detailed in detail,

along with how these artifacts can serve as a valuable source of information for investigators examining social media-related cases. As a part of future work, the authors proposed analysis of deleted artifacts in unallocated space, social media applications on live system, and comparing the artifacts' locations of Windows 8.1 and Windows 10 versions to understand the behavior of applications.

In [3], Silpa M. L. described how to use cyber forensic tools to collect online evidence from various locations of internet-related artifacts by forensic investigation of Windows systems. Using of Internet has become an inalienable part of one's life for performing daily chores. As a result, the information generated out of user's activities in cyberspace is of great use to the crime investigation. Internet artifacts including Browser Cache, Cookies, Downloads, Restore points, Hiber file, and Page file have been discussed in this paper with regard to the Firefox, Internet Explorer, and Google Chrome browsers. For use in digital investigations, the author also recommended a few open-source programs and cyber forensic tools, including Pasco, Galleta, Net Analysis, Cache back, and Internet Evidence Finder to collect internet-related evidence spread across the Windows system.

In [4], Ming Sang Chang explored digital forensic analysis of Facebook using artifacts left behind by user activity on a Windows 10 system. Because of the Facebook application's popularity, criminals have used it to carry out unlawful activities such as hacking, malware attacks, cyberbullying, and stalking. It is crucial for the police investigator to identify the evidence generated by the user activities using the proper forensic tools and procedures in order to identify the offender and bring him or her to justice. The author's study concentrated on hard disk drive and volatile memory artifacts. To collect desired evidence from digital footprints left behind by the users, the author has conducted various experiments using several virtual machines created on Windows 10 system. The experiments were carried out while preserving the integrity of the data being studied and under forensically acceptable conditions. Multiple scenarios were studied with different browsers including Mozilla Firefox, Internet Explorer, and Google Chrome. For each browser, forty-two virtual machines were created to replicate different scenarios. The result shows that user's activity on Facebook with Windows 10 system leaves significant evidence on hard disk drive and other locations.

In [5], Ming Sang Chang, Chih Yen Chang have explained how to conduct Twitter forensic analysis on Windows 10 system. The way people communicate with each other have undergone radical changes as a result of social networking sites like Twitter. Such popular sites can also be used for perpetrating crimes such as identity theft and cyber stalking among others. It's essential to locate the evidence on the Windows system in order to properly combat such crimes. During the study, both volatile memory and hard disk drive artifacts were considered. For this purpose, the authors used a virtual machine on a windows system with the VM ware software. To better understand various scenarios and potential outcomes, eight sub-experiment systems based on Twitter activities such as Login, Post Text, Reply Text, Delete Text, Post Image, Delete Image, and Send Message and Delete Message were created. These systems used various modes of Internet Explorer and Google Chrome. The authors concluded that, the activities of user on Twitter on a Windows 10 system leaves useful evidence on memory dumps and hard disk drive.

In [6], Dija S, Indu V, Sajeena A, Vidhya J A proposed a structure for Browser Forensics in

Live Windows Systems. Since this type of information is lost when the computer system is turned off, doing live forensics is essential for collecting volatile data from a functioning computer system at the crime scene. In Live Forensics, it is essential to analyze suspects' internet activities by way of examining browser files. A framework for acquisition and analysis of browser file was proposed by the authors. This framework enables the police investigator in identifying important leads in investigation and allows him to understand cybercrime in the suspect's computer. The authors recognized that use of portable web browser presents certain challenges as there won't be any traces once the browsing is completed. since browser-related files are created on portable devices. The second difficulty is when the suspect browses the internet in private mode, which temporarily stores information. The third challenge is encoding where the information can be decoded using known algorithms. Owing to these types of challenges investigators find it difficult to extract evidence from browsers. One of the major issues is also the use of anti-forensic techniques by criminals to remove evidence from computer systems.

In [7] Mandeep Kaur, Navreet Kaur and Suman Khurana describes how to use digital forensics to collect and analyze data from various storage devices that can be admissible in court and to prosecute criminals. They have explained Stepwise Forensic Process Model (SFPM) to identify, collect, and analyze evidence during investigation of cases. Also, authors emphasized the need to develop effective methodologies and develop better forensic tools to detect the cases in a timely manner. The authors provided a fundamental study on digital forensics and use of forensic tools like Autopsy and Network Packet analyzer in investigation. Finally, researchers have stressed the use of significant windows artifacts such as the Windows Registry, Windows Event Logs, Restore Points etc., to collect and analyze Windows Operating System artifacts. In a nutshell, the collection and analysis of Windows Operating System artifacts related to social media applications is an area of growing importance for police investigations. The digital forensic tools and techniques are crucial for the successful investigation of criminal and civil cases as they provide insightful information related to the events that transpired.

2.1. Digital Forensic Models

Digital forensic models [8,9] help in collection and analysis of electronic evidence in a way that is both legally acceptable and scientifically reliable. These models are important because they help to establish a standard and consistent methodology for conducting electronic crime investigations and serve to ensure the accuracy and integrity of the electronic evidence during its analysis. Additionally, they aid in facilitating communication and collaboration among different parties involved in the investigation, such as police investigators, forensic experts, and judges.

Some of the existing digital forensic frameworks are:

2.1.1. Systematic Digital Forensic Investigation Model (SRDFIM)

With the support of Systematic Digital Forensic Investigation Model (SRDFIM) Police Investigators, Forensic Experts and Organizations can design suitable policies and procedures for the forensic investigation process. This model can be used to investigate various incidents of electronic crime. Integrity and admissibility of electronic evidence can be attained using

this model. Preparation, Deployment, Physical Crime Scene Investigation, Digital Crime Scene Investigation, Traceback, Dynamite, Presentation, Review, Archiving, Feedback and Training are the stages that make up this model.

2.1.2. Integrated Digital Forensic Process Model (IDFPM)

Integrated Digital Forensic Process Model (IDFPM) permits investigators and forensic practitioners to follow a same approach in investigation of electronic crimes. This model helps the investigators in overcoming certain challenges of present digital investigation methods. The steps included in this model are Preparation, Incident, Digital Forensics Investigation and Presentation.

2.1.3. National Institute of Standards and Technology (NIST) model

National Institute of Standards and Technology (NIST) model is based on the ISO/IEC 27037 standard and provides guidelines for identification, collection, acquisition, and preservation of electronic evidence. This model contains four phases, namely Collection, Examination, Analysis and Reporting. It acts as a compass for the investigators in conducting various digital investigations.

2.1.4. Cyber Forensic Field Triage Process Models (CFFTPM)

Investigative models known as "Cyber Forensic Field Triage Process Models (CFFTPM)" are used during the early stages of an investigation, suspect interviews, and search execution phase. These models consist of four phases – Preparation, Identification, Prioritization and Acquisition. At the scene of a crime, CFFTPM can help police investigators to collect critical information quickly and efficiently, such as suspect identification, suspect motivation, suspect activities, and suspect associates. It can also help crime investigators to preserve volatile or perishable electronic evidence that may be lost or altered if not collected immediately, like memory contents, network connections, and running processes.

2.2. Research Gaps

The literature review revealed that adequate research work has been done on windows system and social media applications. The nature and quantity of artifacts vary among themselves due to the diversity of operating systems and browsers. Currently, the crime investigators are focusing mostly on “traditional areas” (user protected data, user-created) like active files, deleted files, password/encrypted files etc., but not on “non-traditional areas” (System created artifacts/data). For successful investigation of the case, there is an imminent need to concentrate on non-traditional areas especially by the police investigators while working on electronic evidence.

Various research papers have described different operating system artifacts, the information contained in them and the use of such information for investigations. While some free literature is available to aid police investigators in triaging incidents, determine whether a system is relevant for further investigation, and make quick decisions, there isn't much literature available that can help in successful collection and analysis of evidence from electronic media. The majority of the research to date has focused on specific operating system, social media, and browser artifacts. Now, to guide the investigation in a right direction, there is a need to probe further from police investigator’s point of view as to which case-specific artifacts reveal

more information about the system and user activity than the others. In this regard, extensive research on artifacts of operating system, browser and other related areas is necessary. A more in-depth study of threads and processes of the system is essential to understand the locations of electronic evidence left over by the suspects' acts in crime investigation and uncover previously hidden evidence.

The current forensic frameworks differ in their scope, granularity, terminology, and applicability. They also have some similarities, such as following a general sequence of identification, collection, analysis, and presentation of electronic evidence. The phases of collection and analysis of data are not much elaborated from Law Enforcement perspective in these existing frameworks. The phase of collection is more focused towards gathering secondary storage media and/or dumping the data. This impacts the successive phase of analysis more tedious and time-consuming, which in turn affects the investigation process and its outcome. In light of this, a better framework for collection and analysis of evidence can be proposed for Law Enforcement Agencies in order to improve the effectiveness of police investigations. Such frameworks must take into account the SANS artifacts and Cyber Kill Chain (CKC) process for better investigative outcomes.

3. Digital Forensics

The new-age crimes require novel methods and procedures to investigate and collect electronic evidence. In this regard, the discipline of digital forensics emerged as a front-runner and dependable prescription to investigators and forensic experts for identification, collection, and analysis of the electronic evidence from various devices. Computer and mobile device artifacts play a decisive role in finding the traces of evidence during the investigation.

Digital Forensics encompasses the systematic examination of electronic devices, networks, and digital data to extract relevant information and reconstruct past events. It involves the use of specialized tools and methodologies to identify, collect, and analyze electronic evidence such as documents, emails, chat logs, images, videos, and metadata. The primary goal of digital forensics is to uncover facts, establish truth, and provide reliable evidence from various devices in order to link the suspect to the crime scene and to aid in the investigation, and prosecution of electronic crimes.

3.1. Significance of Electronic Evidence

Electronic evidence plays a vital role in modern criminal investigations for several reasons:

i) In today’s digital age, individuals and organizations generate and store vast amounts of data. Electronic evidence can be found in computers, mobile devices, cloud services, social media platforms, and other electronic systems. It provides valuable information about a person’s activities, communications, financial transactions, and interactions, making it a crucial source of evidence.

ii) Electronic evidence can provide comprehensive insights into a crime. It can establish timelines, identify suspects, corroborate, or refute alibies, and provide contextual information to reconstruct events. It can also reveal hidden or deleted information, uncovering critical details that may not be apparent through traditional investigative methods.

iii) Electronic evidence can carry inherent attributes that can prove the authenticity and integrity of data or actions. For example – timestamps, digital signatures, and cryptographic hashes can establish the origin and integrity of digital files or communications, making it difficult for individuals to deny their involvement.

iv) Electronic evidence has the potential to persist indefinitely unless deliberately destroyed or overwritten. Unlike physical evidence that can be degraded or be lost overtime, electronic evidence can be stored, analyzed, and retrieved long after the crime has occurred. This provides investigators with an extended window of opportunity to gather crucial evidence. Often, factors like the variety of electronic devices, cloud storage, encryption, damaged & password-protected devices and finding appropriate digital forensic tools for the collection and analysis of evidence present a significant challenge to the crime investigator. To plan future course of action during the investigation process, it is essential for the investigator to understand the nature and the type of data available at crime scene. Considering these varied spectra of challenges will pave the way for the successful collection and analysis of digital data. This paper explains the procedures required in collecting and analyzing electronic evidence from the point of view of police investigation and offers suggestions to strengthen the investigation process.

Irrespective of nature of crime, collecting and analyzing electronic evidence has now become an integral aspect of police investigations [10]. Emails, text messages, digital images and videos are all examples of this. In addition to providing investigators with more sources of evidence to consider, electronic evidence can also help to uncover facts and evidence that may have otherwise been overlooked. In other words, electronic evidence can be used to build a more comprehensive picture of an incident or crime, making it an asset in police investigations to solve different types of crimes and cement the existing evidence.

4. Role of Digital Forensics in Crime Investigation

Digital forensics plays a critical role in investigations by enabling the steps of identification, extraction, analysis, and interpretation of evidence. Its key roles are-

i. Crime Scene Management – Digital forensics helps investigators effectively manage electronic crime scenes. It provides guidelines and procedures for identifying, collecting, and preserving evidence to ensure its admissibility in court. This involves securing the crime scene, protecting digital devices, and maintaining the chain of custody.

ii. Evidence Collection – Digital forensics enables the recovery of valuable evidence from electronic devices and systems. It employs specific tools and techniques to extract data from computers, mobile devices, network logs, cloud services and other sources. This process involves preserving the integrity of the evidence that can be analyzed and presented in court.

iii. Evidence Analysis – Digital forensics facilitates the analysis of electronic evidence to uncover relevant information. It involves examining data, identifying patterns, reconstructing events, and drawing conclusions on findings. Keyword searching, data recovery, file carving, meta data analysis, and forensic timeline reconstruction are a few examples of analysis approaches.

iv. Suspect Identification – Digital forensics helps in identification of suspects by linking electronic evidence to individuals or entities. It enables investigators to establish connections, trace communications, and attribute actions.

4.1. Digital Forensics Process

The person who commits the crime using modern technology makes the job of the police investigator difficult. To deal with such situations professionally, the investigator should approach the electronic crime scene with adequate caution and preparation. In this, the discipline of digital forensics helps the investigator in identifying, collecting, analyzing, and reporting the electronic data while maintaining the integrity of the data's source [11]. The following are the major steps suggested commonly in digital forensic models discussed above are:

a. Identification: Identifying the electronic media used to store data

b. Collection: Forensic acquisition of data while maintaining the source device's integrity

c. Analysis: Different forensic tools and techniques are used to analyze the collected evidence based on the inputs

d. Reporting: Evidence obtained is compiled in the form of report and submitted before the court or competent authority

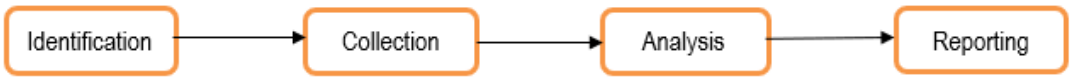

Fig.1. Phases of Digital Forensics Process

While collecting evidence systematically, various factors are to be considered, such as its nature and location. The data obtained from various devices should be 'forensically sound', which means that it should be error-free, meaningful, and transparent. Maintaining the integrity of the case data is essential for successful investigation and its trial process in the court. Further, the methods employed to collect and analyze the data are to be well accepted by the courts, and forensic community. This helps the investigators in successfully bringing those responsible to justice.

5. Guidelines for Electronic Crime Investigation

It is essential to identify and seize all the possible electronic and physical evidence at the crime scene. For traditional investigators with limited knowledge of current cyber trends would face difficulties in investigation of electronic crimes [12]. To help investigators and forensic practitioners, international organizations like National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Scientific Working Group of Digital Evidence (SWGDE) standards and Interpol have provided certain guidelines to Law Enforcement Agencies (LEAs) on how to seize various types of evidence and conduct electronic crime investigations at crime scene and in the computer forensic lab [13]. These guidelines' main objective is to help the investigator understand various options for conducting

electronic crime investigations.

5.1. Best Practices

When dealing with the electronic evidence during an investigation, general forensic and procedural principles should be followed, such as -

a. Collection, preservation and transportation of electronic evidence process should not alter the evidence

b. Only specially trained professionals should examine electronic evidence

c. Everything done during the seizure, transportation and storage of electronic evidence should be documented, preserved and available for examination by third parties

d. The investigator should never work with the original evidence

5.2. Locard's Principle of Exchange

Locard's principle of exchange states that when an object comes into contact with another object, a cross-transfer of evidence can occur. In other words, every contact leaves a trace. The exchanged materials indicate that the two objects were in contact, and the traces can be found on both objects. Similar considerations apply to digital information. Using this principle, the user of the digital data can be traced in the act of cyber-related crimes.

5.3. Daubert's Standard

The Daubert's Standard is a rule of evidence regarding the admissibility of expert witness testimony. It states that "Any scientific evidence presented in a trial has to have been reviewed and tested by the relevant scientific community." Likewise, in digital forensics, any tools, techniques, or processes used in an investigation should be widely accepted in the cyber forensic community.

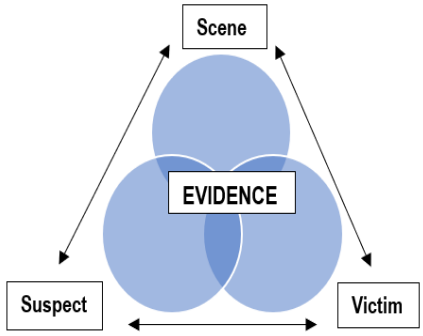

Fig.2. The Evidence Linkage Triangle

5.4. Evidence Linkage Triangle

The Evidence Linkage Triangle explains that items of evidence are used to establish specific links or relationships between the suspect(s), the victim(s), and the scene(s). At the center of triangle is evidence that ties all the three corners together as well as the evidence itself. The same thing can be considered for electronic crimes.

5.5. Integrity of Evidence

The integrity of the electronic evidence is one of the important factors which determines the outcome of the police case i.e., conviction or acquittal. Hence, it is very important that the Investigating Officer (IO) or First Responder to the electronic crime scene must collect evidence with utmost care by following the cyber forensic best practices and forensic tools accepted by the courts and forensic community.

The following are some of the important factors which influence the integrity of the electronic evidence:

a. Forensics Software: Software helps to analyze and maintain the integrity of electronic evidence

b. Guidelines: International guidelines aids in proper collection, preservation, analysis and presentation of electronic evidence

c. Chain of Custody: Chain of custody safeguards the integrity of evidence

d. Secure Evidence Storage: Electronic evidence is secured to prevent tampering and unauthorized access using encryption/hashing techniques.

e. Authentication: Authentication protocols help to verify the identity of users who access evidence and log activity associated with it.

f. Hashing: Hashing helps in validation, and authentication of electronic evidence maintained throughout its life cycle:

6. Electronic Crime Scene Management

The term "electronic crime scene" refers to the environment where potential evidence may be recovered from a mobile phone, pen drive, hard disk, or any other digital storage media. This place might be anything, including a person’s house, workplace, or the scene of a serious crime. Electronic crime scene management is necessary to preserve the integrity of the evidence. Because each crime is unique, and each investigative process is distinct. The main objective of electronic crime scene management is to provide situational awareness to Investigating Officer (IO) about identification, collection, and analysis of electronic evidence to facilitate time-critical decision making during the investigation.

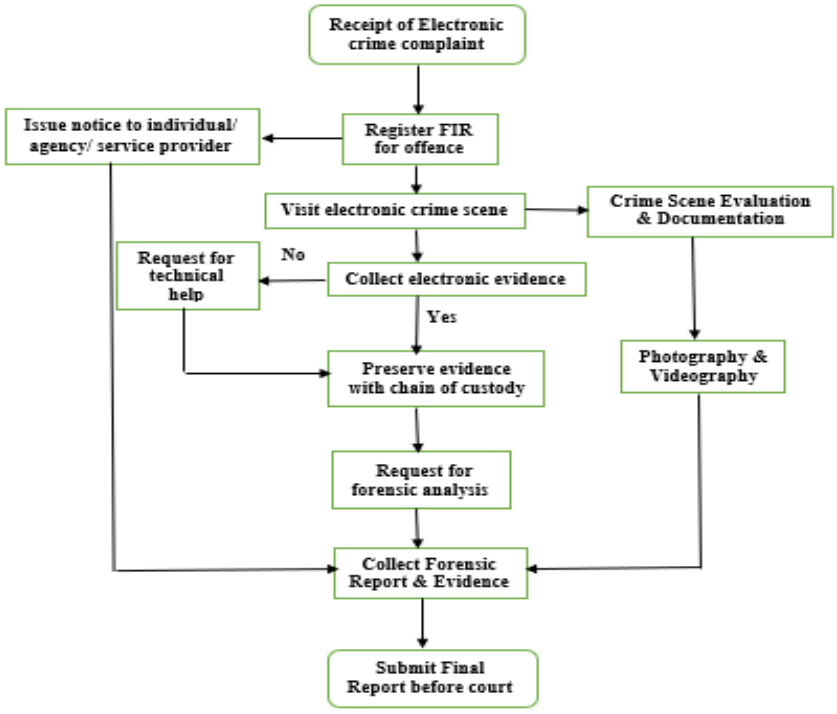

Fig.3. Flow chart of Electronic Crime Scene Management

6.1. Investigating Officer's Role

From the time a case is registered to the time it is prosecuted, the role of the police Investigating Officer (IO) is crucial. It is essential for the IO to have a thorough understanding of every element of the crime for successful investigation and bring it to a logical conclusion. That is,

- Firstly, after registration of FIR, the IO must secure the crime scene to prevent evidence tampering
- Secondly, based on the crime scene requirements, IO may submit a valid request for the assistance of the digital forensic expert to carry out a forensic procedure.
- Thirdly, before finalization of the case, the IO must consider inputs from victims and relevant stakeholders and obtain a forensic report from the expert.
- Finally, the evidence collected during the electronic crime investigation must be presented to the court in conformity with the applicable laws. Fig.3. Flow chart of Electronic Crime Scene Management

Each electronic crime scene has potential to educate the police investigator, forensic practitioner or anyone associated with the case. Therefore, electronic crime scene management is one of the important factors for LEAs in crime investigation and subsequent trial process in the court.

6.2. Chain of Custody (CoC)

The Chain of Custody (CoC) is a sequential documentation of evidence showing its seizure, custody, transfer, and disposition. The main aim of CoC is to establish that the evidence collected is linked to the crime. It is a procedure of validating the evidence and plays a vital role in bringing the culprits to justice. Conversely, if the investigator fails to show evidence integrity and proper CoC in any case, the evidence presented before the court becomes inadmissible.

The following are some of the key elements of CoC:

- Name of the Law Enforcement Agency (LEA)
- Details of the incident
- Time, date, and location of collection of items
- Identity and signature of the investigator
- Description of the items submitted for the examination
- Details of steps carried out during the forensic process and
- Details of the custodians of evidence

6.3. Digital Investigation Challenges

During the process of evidence collection and analysis, LEAs encounter many challenges in electronic crime scene management. Some of the important challenges are: 1) Lack of expertise in LEAs, 2) Old-fashioned forensic equipment, 3) Anti-forensic methods, 4) Encryption of data, 5) Hidden files and hidden storages, 6) Password protected devices, 7) Presence of non-essential persons at the crime scene, 8) Different sizes and shapes of storage media, and 9) Advanced storage techniques.

Each crime scene is distinct in its own way, thus suitable methods to be used to manage it properly. In addition, the approach employed in the process must be in-line with the established and widely accepted forensic norms so that the evidence submitted in court is admissible. Therefore, proper preparation is required before approaching the crime scene for collection and analysis of electronic data. This work will become crucial at a later stage especially during the court's trial process and, often decides the outcome of the case i.e. conviction or acquittal.

7. Digital Artifacts

Digital artifacts [14,15] play an important role in investigation of the crime by finding the traces of evidence in electronic devices. They record or log evidence of various user activities on the computer system/device. The entries in the majority of these artifacts are formed as a by-product of user action, and the user may or may not be aware of them [16,17]. They provide information about system configuration, installed applications, suspect's activity, location, and intent. The Operating System (OS) contains dozens of artifacts that store important evidence about the user's activities in the system. Exploring digital artifacts from a tainted electronic

system will facilitate investigators to get important clues swiftly for framing the future steps in investigation process [18,19].

Some examples of different types of digital artifacts are given below:

Table 1 Types of Digital Artifacts

Sr. No.	System/Device	Important artifacts
1	Operating System	**Windows:** Registry, Recycle Bin, Prefetch files, Event Logs, Jump Lists, Windows Error Reporting (WER), User Assist, RecentApps, ShimCache, System Resource Usage Monitor (SRUM), Restore points, Master File Table (MFT), Timeline activity, Link Files **Linux**: Bash History, Network Interfaces, Recent Files, System Logs, SSH activity, OS information
2	Mobile device	Call logs, SMS, MMS, Contacts, Browser History, Location Data, Photos, Videos, Apps Data (WhatsApp, Facebook, Gmail etc.)
3	Browser	History, Cookies, Cache, Bookmarks, Password files, Downloads, Extensions, Add-ons, Plug-ins

7.1. SANS Artifacts

SANS artifacts [20,21] are digital evidence that can be used in electronic crime investigation. They are categorized by the type of evidence they provide, such as Evidence of Execution, Evidence of File Opening, Evidence of Communication, Evidence of Persistence and Evidence of Data Exfiltration. These artifacts can help electronic crime investigators to reconstruct the past events, actions and intentions of the suspects or attackers by providing relevant information about their activities and behaviors on the tainted system. Further, SANS artifacts can also help to identify the source and destination of the attack, the tools and techniques used, and the impact and damage caused.

7.2. Cyber Kill Chain (CKC)

The Cyber Kill Chain (CKC) process is a security defense model that describes the stages of a cyberattack and how to prevent or disrupt it. CKC consists of seven steps - Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Actions on Objectives. The CKC process can help electronic crime investigators to identify and analyze the evidence of a cyberattack by mapping the digital artifacts to each step of the attack. For example, network logs can reveal the source, destination of the delivery and command-and-control channels; malware analysis can reveal the payload's functionality and indicators of compromise (IOCs); file system analysis can show the installation and actions taken in response to the payload's objectives, etc. Thus, digital artifacts can help investigators in reconstructing the timeline of events, identifying the motive and means of the crime, linking the suspect to the crime scene or the victim, and confirming or disproving alibis. From digital forensic point of view, artifacts produce valuable data of user activities having significant forensic value [22] that can be used as reliable and objective evidence in the court of law.

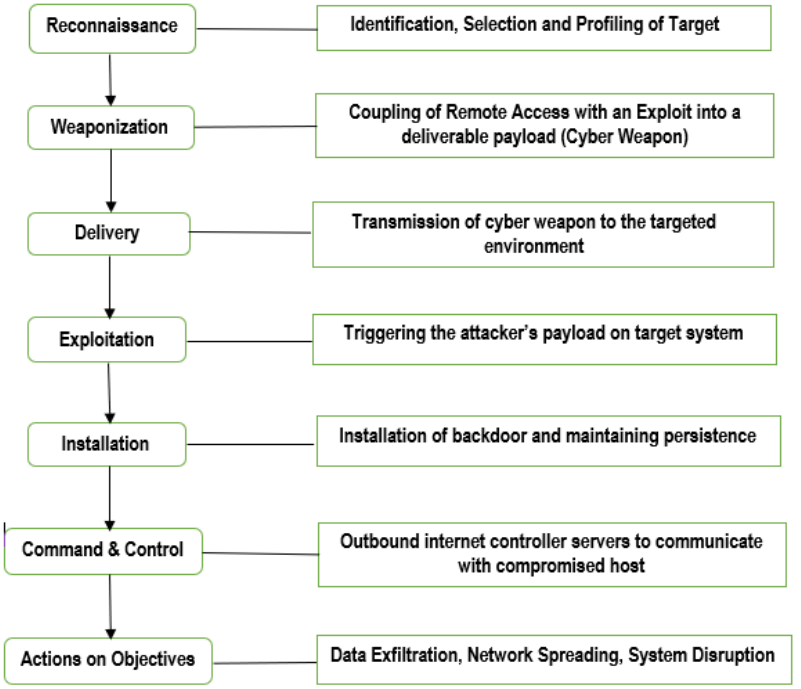

Fig.4. Cyber Kill Chain (CKC) Process (Existing)

8. Digital Forensic Tools

Digital forensic tools are both in the form of hardware and software [23]. Law Enforcement Agencies (LEAs) frequently employ them for imaging, collecting, and analysis of digital data from various types of electronic devices like hard disk drives, pen drives, MMC cards, mobile phones, browsers, drones, IoT devices, CCTVs, networks, and other electronic media. They help the Law Enforcement Agencies (LEAs) in identifying the perpetrators and connecting them to crimes [24]. Based on their mode of service, digital forensic tools are categorized as commercial and open source. The following are some of the well-liked digital forensic tools for different types of investigations is given in Table 2.

Table 2 Types of Digital Forensic Tools

Sr. No.	Type of Forensics	Popular Tools
1	Disk Forensics	Encase Forensics, Exterro FTK, Prodiscover, Magnet Axiom, OS Forensics, MCMS Detego, Atola Forensics, Belkasoft BEC X, X-Ways Forensics, Autopsy, SIFT, Sleuth Kit.
2	Mobile Forensics	UFED 4PC, Oxygen Detective, XRY Forensics, MOBILedit, MD-NEXT, Paraben E3
3	Video Forensics	DVR Examiner, AMPED FIVE, Video Investigation Portable, Foclar Impress
4	Social Media Forensics	X1 Social Discovery, Page Vault Browser, Maltego Enterprise, Voyager Labs, S2T DeepWebInt
5	Network Forensics	Wireshark, Nmap, Xplico, Network Minor
6	Drone Forensics	CFID, MSAB Drone forensics, Hancom MD-Drone

7	IoT Forensics	Paraben IoT Forensics
8	Vehicle Forensics	Berla Blackthorne, Bosch Crash Data Recorder
9	Damaged Forensics	Teeltech, ACE Lab
10	Audio Forensics	Speech Lab, Ikar Lab, AnuBhooti Solution

9. Proposed Methodology

The prevailing forensic methods include phases of evidence identification, collection, analysis, and reporting from the time of its discovery at crime scene and the forensic tools used for analysis and interpretation. This ensures the integrity of the electronic evidence and enables the investigator to present the court with relevant evidence. The main purpose of this paper is to facilitate the investigators to analyze electronic system and mobile phone artifacts using a tried-and-true method recognized by the digital forensic community and the legal system [25].

The proposed forensic methodology contains following steps:

9.1. Identification

This phase involves identification of artifacts depending on the nature of electronic crime, the type and versions of the operating system, the number of systems involved, and the case history provided to the Investigator. Sometimes, quick preview of the system is required to identify what artifacts are relevant for investigation and to separate innocent systems from tainted systems using digital forensic tools. The Police Investigator managing the electronic crime scene must be well trained in the use of digital forensic tools in order to identify and collect the relevant electronic evidence.

9.2. Collection

a. Existing Method: The identified data needs to be collected during the forensic process while ensuring the integrity of the evidence. This involves collecting the volatile data first, followed by the contents of hard disk and external media. Chain of custody (CoC) compliance and maintaining relevant documentation at each step are important parts of the collection process. Based on the requirements of the case, the collecting of data can be physical, or logical. The forensic collections can be authenticated by taking hash values which are like digital fingerprints to prove collected data's integrity in court [26].

b. Proposed Method: Depending on the nature of the case, data collection can be targeted by duly considering the SANS artifacts and Cyber Kill Chain Process during the management of electronic crime scene. In the proposed method, the collection of evidence phase can be streamlined as follows:

Table 3 SANS Artifacts

Sr. No.	SANS Artifacts	Type of evidence
1	Evidence of Execution	Prefetch files, Shimcache, UserAssist
2	Evidence of File Opening	LNK files, RecentDocs, Shell bags
3	Evidence of Communication	Web browser history, email files, chat logs
4	Evidence of Persistence	Registry Run Keys, Scheduled Tasks, Services
5	Evidence of Data Exfiltration	USB devices, cloud storage, network shares

The proposed method will allow the Police Investigator to manage the crime scene more effectively and stay focused while collecting relevant artifacts for a specific case.

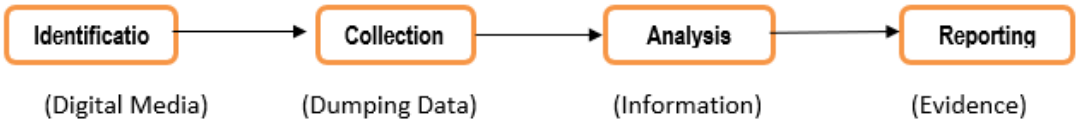

Fig.5. Existing Phases of Digital Forensics Process

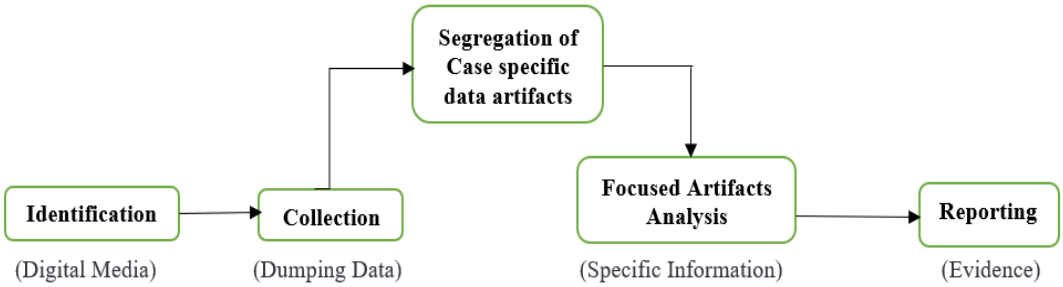

Fig.6. Proposed Phases of Digital Forensics Process

9.3. Analysis

a. Existing Method: Traditionally, the data collected needs to be parsed and analyzed to identify evidence that is relevant to the case. Verifying the evidence, mounting the evidence, performing timeline activity, network activity analysis, external devices connected, software installed/uninstalled, keyword searches, browser/internet activity are all part of the analysis process. The findings of analysis must be properly documented and presented in a forensic report. In this phase, the evidence's data is examined, processed, interpreted and the deleted data is recovered.

b. Proposed Method: The analysis phase will only be focused on the specific artifacts collected during the collection phase resulting in lesser turnaround time, increased efficiency and decreased financial outlays. The proposed method will quickly help the Police Investigator to understand how the crime has occurred, reconstruct the past events and focus on the relevant evidence to strengthen case.

9.4. Reporting

The analysis observations and findings must be well documented during this phase so that even non-technical people may understand them. In other words, the report should include a brief summary of the facts of the case, information about the evidence collected, the method used to collect it, hash values, and the analysis's findings. With the help of the proper proof, such as screenshots, file listings, exported data, etc., it can be presented in an easy way.

The success of the electronic crime investigation and the outcome of the case will ultimately depend on how well the investigating officer (IO) chooses the digital forensic tools and techniques used for data collection and analysis while conducting the forensic procedures at crime scenes and forensic labs [27].

10. Discussion

Electronic crime becomes more sophisticated and widespread with the development of technology. As a result, LEAs are finding it difficult to tackle these crimes with the available resources, expertise, and infrastructure. Many a times, the Investigating Officer (IO) in-charge of the case is solely responsible for collecting, and analyzing all relevant evidence during the investigation process, including the electronic evidence from numerous devices that were seized from the crime scene. Due to the significance of electronic evidence and the potential it holds to influence the outcome of the case, IO must make greater efforts to collect and preserve it. The ability to collect and analyze electronic evidence from multiple sources makes it possible for the IO to build a more complete picture of an incident or crime, reconstruct past actions/events, and identify the perpetrator of a crime with relative ease. The sufficient evidence collected during the forensic procedures enables the IO to present a fit case before the court and set the legal wheels in motion.

Digital forensics is a discipline that is useful primarily to support the IO's efforts during the investigation process. It mainly focuses on the investigation of electronic evidence collected from electronic systems such as computers, mobile phones, network devices, and other electronic media [28]. It entails identifying, collecting, analyzing, and reporting evidence in a manner that is legally admissible. It can aid investigators with access to electronic evidence that would otherwise be difficult or impossible to retrieve. In addition, digital forensics can assist in correctly locating the origin of cybercrime and allowing the police to focus their resources on the investigation in a more professional and sensible way. Until now, Law Enforcement Agencies (LEAs), due to lack of awareness on collection of case-specific data, are using information gathering digital forensic tools to collect information from the suspect/tainted devices for investigative purposes. In light of this, it is essential for LEAs to shift from obsolete to space-age technologies in order to effectively combat the challenges posed by electronic crimes and potential consequences, if any.

The authors of the literature review, in this paper, focused mostly on limited electronic artifacts of the operating system, and social media applications. These artifacts only represent a chunk of the evidence; The remaining evidentiary artifacts located in different areas of the electronic system, which are often ignored, could be vital in the prosecution of the case. To bridge this gap, the investigation needs a thorough approach that can collect data from both traditional and non-traditional areas of the electronic systems and such data needs to be analyzed vertically, laterally and in a timely manner. For efficient collection and analysis of crime related data, LEAs may use a blend of both commercial and open-source digital forensic tools subject to the validation of forensic community and courts.

In view of the challenges discussed in this paper vis-à-vis effective collection and analysis of electronic evidence from various artifacts of operating systems, social media applications, browsers, and other electronic media, the LEAs require a new method. The proposed method discussed in this paper for effective evidence collection and analysis may be incorporated with up-to-the-minute technologies. For instance, Machine Learning (ML) algorithms could be utilized to automatically identify, collect, and analyze case-specific evidence more quickly and accurately; Artificial Intelligence (AI) may be used to precisely identify patterns and links within electronic evidence that could prove to be vital in criminal investigations; Blockchain

Technology could be used to securely store electronic evidence and to ensure its integrity and authenticity.

Keeping in view the requirements of IOs, a professional automated forensic framework capable of identifying, collecting, analyzing, and reporting electronic evidence may be developed with the support of cutting-edge technologies like Artificial Intelligence, Machine Learning and Block Chain [29]. This framework will arguably reduce workload, enhances critical decision-making ability, and helps in alleviation of the technology-driven crimes more efficiently. Finally, to effectively address the issues of technology enabled crimes, it is important to have unwavering collaboration among various LEAs, forensic experts, and other stakeholders. This will allow them to share resources, expertise, and intelligence in order to neutralize the growing challenges presented by electronic crimes.

11. Challenges & Future Work

The ultramodern technologies showcase a variety of challenges to the police investigators while collecting, analyzing electronic evidence and managing an electronic crime scene. Firstly, the latest versions of operating systems (OS) have a different file structure than previous versions, which makes it more difficult to locate and collect relevant electronic evidence. Second challenge is that collecting evidence from cloud-based applications like One Drive, Google Drive may be tough. Third challenge is that the newest operating systems like Windows 11 contain certain security features that could limit investigator's access to the electronic evidence under investigation. Fourth challenge is that data collection through digital forensic tools may be difficult due to their incompatibility with modern operating systems. Finally, present-day encryption techniques may limit investigator's access to electronic evidence stored in multiple locations of operating system, browsers etc.

To meet the investigative demands of LEAs, there is a dire need for the creation of talented pool of workforce and state-of-the-art infrastructure. Also, future research must be oriented towards better identification, collection, analysis, and reporting of electronic evidence to achieve desired investigative results [30]. In this direction, the police fraternity must work diligently with an aim to mitigate the challenges posed by the electronic crimes.

12. Conclusion

This research paper provides a thorough overview of digital forensic procedures for managing electronic crime scenes and conducting police investigations. The paper also highlights the crucial role digital forensics plays in modern law enforcement by exploring its importance in electronic crime investigation, the steps in the forensic process, and the challenges faced by investigators. This paper aims to educate the LEAs as to how to approach crime scenes scientifically and target case-specific data needed for electronic evidence collection and analysis. This paper also emphasizes the need for ongoing research, training and cooperation among the various LEAs, and stakeholders to keep pace with rapidly evolving technologies and combat the growing danger posed by electronic crimes. In a nutshell, this paper signifies the role of digital forensic methods and techniques in contemporary law enforcement.

References

1. Khushboo Rathi, Umit Karabiyik, Temilola Aderibigbe, Hongmei Chi, "Forensic Analysis of Encrypted Instant Messaging Applications on Android", 978-5386-3449-3/18 © 2018 IEEE [DOI:10.1109/ISDFS.2018.8355344]
2. Asma Majeed, Shahzad Saleem, "Forensic Analysis of Social Media Apps in Windows 10", NUST Journal of Engineering Sciences, Vol.10, No. 1, 2017, pp. 37-45 [URL: https://www.researchgate.net/publication/320556174_Forensic_Analysis_of_Social_Media_Apps_in_Windows_10]
3. Silpa M L, "Forensic Analysis on Windows System for Internet Evidences", CDAC, Trivandrum, Kerala, India [DOI: 10.20247/IJARTET.2016.S03020012]
4. Ming Sang Chang, "Digital Forensic Investigation of Facebook on Windows 10", IJournals: International Journal of Software & Hardware Research in Engineering, ISSN- 2347-4890, Volume 4, Issue 10, October, 2016 [URL: https://ijournals.in/wp-content/uploads/2017/07/1.41002-Ming.compressed.pdf]
5. Ming Sang Chang, Chih Yen Chang, "Twitter Social Network Forensics on Windows 10", IJISET – International Journal of Innovative Science, Engineering & Technology, Vol. 3, Issue 9, September 2016, ISSN (Online) 2348-7968 [URL: https://ijiset.com/vol3/v3s9/IJISET_V3_I9_09.pdf]
6. Dija S, Indu V, Sajeena A, Vidhya J A, "A Framework for Browser Forensics in Live Windows System", C-DAC, Thiruvananthapuram, India [DOI:10.1109/ICCIC.2017.8524412]
7. Mandeep Kaur, Navreet Kaur, Suman Khurana, "A literature Review on Cyber Forensic and its Analysis tools", IJARCCE- International Journal of Advanced Research in Computer and Communication Engineering, Vol.5, Issue 1, January 2016, ISSN (Online) 2278-1021 [DOI:10.17148/IJARCCE.2016.5106]
8. Sara Sarwar Mir, Umar Shoaib, Muhammad Shahzad Sarfraz, "Analysis of Digital Forensic Investigation Models", -Academia.edu.[URL: https://www.academia.edu/30916517/Analysis of Digital Forensic Investigation Models]
9. Athanasios Dimitriadis, Nenad Ivezic and others, "D4I - Digital forensics framework for reviewing and investigating cyber-attacks", Elsevier Ltd. [URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9074801]
10. Michael B. Mukasey, Jeffrey L. Sedgwick, David W. Hagy, "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition" [URL: https://www.ojp.gov/pdffiles1/nij/219941.pdf]
11. Zubair A. Baig, Patryk Szewczyk and others, "Future challenges for smart cities: Cyber Security and digital forensics", 1742-2876 © 2017, Elsevier Ltd. [https://doi.org/10.1016/j.diin.2017.06.015]
12. Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, "Guide to Integrated Forensic Techniques into Incident Response", ["URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf]
13. Interpol, "Guidelines for Digital Forensics First Responders", [URL: https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders V7.pdf?inLanguage=eng-GB]
14. "Understanding Digital Evidence - Law Enforcement Cyber Center", [URL : https://www.iacpcybercenter.org/investigators/digital-evidence/understanding-digital-evidence/]
15. Christa Miller , "Digital Forensic Evidence And Artifacts: Recent News And Research" Forensic Focus, [URL: https://www.forensicfocus.com/articles/digital-forensic-evidence-and-artifacts-recent-news-and-research]
16. Vivienne Mee, Theodore Tryfonas, Iain Sutherland, "The windows Registry as a forensic artefact: Illustrating evidence collection for Internet usage", Digital Investigations 3 (2006)

166-13, Elsevier Ltd. [DOI:10.1016/j.diin.2006.07.001]
17. A. Duranec, D. Topolcic, K. Hausknecht, D. Delija, "Investigating file use and knowledge with windows 10 artifacts, MIPRO 2019, May 20-24, Opatija Croatia [DOI:10.23919/MIPRO.2019.8756877]
18. Farshund Iqbal, Zainab Khalid, Andrew Marrington, Babar Shah, Patrick C.K. Hung, "Forensic investigation of Google Meet for memory and browser artifacts", DFRWS 2022 APAC – Proceedings of the Second Annual DFRWS APAC, Elsevier Ltd. [DOI:10.1016/j.fsidi.2022.301448]
19. Rich Murphey, "Automated Windows event log forensics", 1742-2876 © 2007 DFRWS, Elsevier Ltd [https://doi.org/10.1016/j.diin.2007.06.012]
20. SANS Institute, "Digital Forensics and Incident Response - SANS Institute", [URL: https://www.sans.org/digital-forensics-incident-response]
21. Sri Parvathi Kota, Vijaya Sri Kompalli, "Automated Collection of Artifacts from a Live Windows System using e-Triage Tool", International Journal of Advanced Trends in Computer Science and Engineering, volume 9, No.1, January-February 2020 [DOI:10.30534/ijatcse/2020/03912020]
22. Jisung Choi, Jungheum Park, Sangjin Lee, "Forensic exploration on windows File History", Forensic Sience International Digital Investigation 36 (2021) 301134, 2666-2817 © Elsevier Ltd [https://doi.org/10.1016/j.fsidi.2021.301134]
23. Kambiz Ghazinour, Deep M Vakharia, Krishna Chaitanya Kannaji, Rohit Satyakumar, "A study on Digital Forensic Tools", IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017), 978-1-5386-0814-2 © 2017, IEEE [DOI:10.1109/ICPCSI.2017.8392304]
24. Rodrigo Fernando, Morocho Román, Nancy Magaly, Loja Mora, "Digital Forensic tools.", International Journal of Applied Engineering Research 11.19 (2016): 9754-9762 [URL:https://www.researchgate.net/publication/319332740_Digital_Forensics_Tools]
25. Dasaka Sameer, "A Synopsis on Digital Forensics and its investigative strategies", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 8.2 (2019) [URL: https://www.academia.edu/42907825/A_SYNOPSIS_ON_DIGITAL_FORENSICS_AND_ITS_INVESTIGATIVE_STRATEGIES]
26. Arshad Humaira, Aman Iantan and Esther Omolara, "Evidence Collection and forensics on social networks: Research challenges and directions." Digital Investigation 28 (2019): 126-138 [DOI:10.1016/j.diin.2019.02.001]
27. Ghazinour, Kambiz, et al. "A study on digital forensic tools" 2017 IEEE international conference on power, control, signals, and instrumentation engineering (ICPCSI), IEEE, 2017 [DOI:10.1109/ICPCSI.2017.8392304]
28. Richard Apau, Felix N. Koranteng, "An overview of the digital forensic investigation infrastructure of Ghana", Forensic Science International: Synergy 2 (2020) 299-309, Elsevier Ltd.[DOI:10.1016/j.fsisyn.2020.10.002]
29. Raj Shree, Ashwani Kant Shukla, Ravi Prakash Pandey, Vivek Shukla, "A contiguous cybercrime investigation framework to deal with the cyber dependent-cum-cyber enabled crimes", 2214-7853 © 2021 Elsevier Ltd [URL: https://doi.org/10.1016/j.matpr.2020.12.428]
30. Ayse Okutan, Yalcin Cebi, "A Framework for Cybercrime Investigation", 3rd World Conference on Technology, Innovation and Entrepreneurship (WOCTINE), 1877-0509 © 2019 Elsevier Ltd. [DOI:10.1016/j.procs.2019.09.054]