iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40867

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

A Study of Minimization of Cybercrimes by the Implementation of Cyber Forensics Tool Kit

Danish Rehman[1], Er. Jasdeep Singh[2]
[1]*M. Tech Scholar,* [2]*Assistant Professor, Department of Computer Science and Engineering, RIMT University, Mandi Gobingarh, Punjab, India*

Abstract: ***To identify whether the victim has committed a crime, both criminal and forensic investigators need the help of digital forensics. As a result, an investigator must use an adequate, accurate, affordable, and trustworthy cyber forensic tool for forensics investigations related to crimes. Digital forensics, also known as computer forensic analysis, computer analysis, and computer inspection, is the practise of painstakingly evaluating computer media (hard discs, diskettes, cassettes, and so on) for evidence. A comprehensive inspection by a qualified examiner may result in the reorganisation of a computer's operations. It's a step-by-step technique for investigating crimes utilising digital evidence employing scientific methodologies and processes. While many amazing solutions have been developed to protect our information communication networks, these devices require much more frequent updating. Individuals with both research abilities and a professional grasp of how the internet works, as well as those who know how to examine PC network security problems, are in great demand. This gives an attack-resistant investigative framework, as well as understanding of how the internet operates and the skills to assess cybercrime apparatus to discover who, what, when, why, and how. The study's findings led to the development of Digital Forensic tool solutions for investigators looking to expand their capabilities in using these tools.***

Keywords: Forensic, Cybercrime, investigation, toolkit

I. INTRODUCTION

Weapons, life, and money will be in short supply on the planet. An electron with zeros, or little sources of evidence, will oversee the planet. As a result of the least quantity of shooting in the world wars. Information is key in a world war, as it determines what people will believe, see, and hear, as well as how they will act (Sneakers, 1765). Computer crime is referred to as cybercrime. Cybercrime is the illegal flow of data across the internet, networks, and computer systems. In a roundabout way, cybercrime involves the control, access, and misuse of data, as well as persons. Trustworthy thieves are on the search for new and vulnerable PC improvements to exploit as computer crime becomes the world's most ubiquitous criminal trend. These cybercriminals range in age, sexual orientation, identity, social status, and financial status, to mention a few traits, demonstrating that cybercriminals may be anybody. Nonetheless, most cybercriminals have similar perspectives and objectives for their crimes. People engage in cybercrime because it is so simple to hide behind technology. A typical motive for information technology crimes is the compromise of the "Deficient Legal Jurisdiction," and it is also prevalent for the guilty parties. If developing or maintaining processing equipment is prohibitive while remote processing is possible, the issue has been included into the computer encryption system. Individuals routinely spread dangerous computer programmes such as worms and viruses in order to cause harm to another person or company. Such assaults are designed to destroy or put to the test a person's aspirations in order to gain personal enjoyment from seeing them persevere. The thrill, popularity, and difficulty of abusing a computer framework are what motivate some computer thieves to conduct cybercrime. Cybersecurity will cost the world $6 trillion a year by 2021, up from $3 trillion just a year ago, according to the digital security organisation and the mainstream media Global expenditure on digital security goods and services is predicted to reach $1 trillion over the next five years, from 2017 to 2021. By 2020, Microsoft predicts that four billion people will be online, more than doubling the present amount. By the end of 2017, the cost of ransomware damage is estimated to surpass $5 billion. In the next five years, cybercrime may become the greatest threat to everyone, everywhere, and everything on the planet. Forensic investigators of computer crimes must design a strategy that incorporates the use of specialised equipment as well as the use of systems to handle the obstacles. Depending on the type of PC equipment and the sort of automated proof, experts may pick one instrument over another.

The application of precisely derived and proven methods to the preservation, endorsement, proof of identity, scrutiny, elucidation, documentation, and appearance of digital evidence derived from digital sources for the purpose of enabling or broadening the reestablishment of criminal events or assisting in the prediction of unapproved actions that are troublesome to prearranged tasks is defined as digital forensics [1].

The Internet is becoming an inextricable feature of our life. The internet presents us with practically limitless chances, but it also gives fraudsters with a depressingly enormous number of opportunities. They break into our computers every day, taking personal and confidential information and sending forged financial messages. This sort of crime is known as cybercrime. Cybercrime has the potential to damage governments, companies, and the general population. Botnets are networked computers infected with computer viruses that are used to commit cybercrime. Several Digital Forensic technologies should be employed to lessen system vulnerability to prevent being a victim of cybercrime. Several Digital Forensic technologies have been released thus far. Using Digital Forensic technology streamlines and explains the investigation process while also lowering the investigation's complexity. It assists in the finding of digital evidence from a range of digital sources that may be important in the conduct of a computer crime.

II. LITERATURE REVIEW

Cyber-attacks are operations carried out by governments to enter a country's or other nations' systems or computer networks to cause harm or disruption. Clark, Richard: (Motsch et al., 2020). According to the analysis and critique of this notion, the three parts of the assault, namely the criminal, the objective, and the purpose of the attack, have been used as criteria without addressing the forms of interruption (Cao et al., 2019) Furthermore, only countries are discussed in terms of the attack's guilty party in general; however, if an attack is carried out in the background and field work under the command and regulation of a home nation (cyberspace of systems under control of regions of the world) by individuals and pro and private groups against a third country, it will come under the scope of the process mentioned and will not be included, leaving a gap. Given this situation, it is plausible to infer that the definition is entirely insufficient, since it excludes a significant number of assaults committed by commercial and non-governmental organisations, leaving a gaping hole (Zhang, 2017)

According to Michael Hayden, any deliberate attempt to harm or destroy another country's computer networks is illegal (Robinson et al., 2015). Furthermore, this phrase is quite wide and does not differentiate between cybercrime, cyber-attacks, and cyber warfare, and the boundary between their detection is blurry. Observers and policymakers will surely be influenced by the lack of such a distinction. The broad scope of the rules of war leaves the internet open, which can have damaging and bad consequences for the evolution of war and nation-state belligerence (Edgar and Manz, 2017). This definition of cyber-attacks excludes a wide range of potential threats to a country's national security if its cyber infrastructure has been attacked but has not yet reached the level and scope of major attacks.

III. OBJECTIVES

The computer attack and cyber extortion component typically provides coverage for loss directly arising from a computer attack or cyber extortion.

1) The main objective of this study is to examine the numerous Digital Forensic technologies that play a crucial role in locating forensic evidence from digital sources based on several criminal cases.
2) The digital forensic tools are iSafe, USB Deview, Recuva, and WinHex.
3) To show the diversity of subjects indicates the field's scope and relevance, as well as potential areas for future advancement in cybercrime kit tools.
4) To develop a study which gives solutions for investigators who want to improve their serviceability in using Digital Forensic technologies.

IV. METHODOLOGY

The hazards posed by cybercrime to businesses have expanded faster than potential victims or digital security experts can respond, putting a wide spectrum of companies at risk (Khari et al., 2017). The threat of cybercrime has developed at a quicker rate than the threat of other forms of digital security. In the present, digital thieves are growing increasingly skilled at acquiring unnoticed access while maintaining a low profile. Various types of discernment are used by different analyzers. As more attacks and attack systems become linked to such marketplaces, dark and shadow markets for hacking tools, hacking services, and hacker items are attracting a lot of attention (Albom et al., 2014). Reconnaissance Tools, Scanning Tools, Access and Heightening Tools, Exfiltration Devices, Sustainment Devices, Assault Devices, and Obfuscation Devices were all classified as Reconnaissance Tools, Scanning Tools, Availability and Heightening Tools, Exfiltration Devices, Sustainment Devices, Assault Devices, and Obfuscation Devices by a group of analysts in 2013. (Andres et al., 2013). In his study, Harbawi (2016) recognizes the gap between creating brilliant discoveries and generating quantified instruments.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

A. Computer Vs. Crimes

Computers may be used as a target for criminal conduct as well as a source of information about illicit activity (Casey et al., 2001). Computer and network crimes in which a computer may have played a part in the commission of the crime (www.studymode.com). Although the term "cybercrime" refers to computer-related crime, some people believe that computer crime is a subclass of cybercrime that requires its own definition and explanation. The topic of computer crime will create a dizzying quantity of papers as more scientists and professionals utilize the term cybercrime as an umbrella phrase for all crime, including computing and advancements.

1) *Computer Crime Technology PC:* This crime is shown as an enlargement of a criminal act that incorporates the knowing of a product's result in order to execute, test, and prosecute it (C. Laudon, 2004; P.Laudon, 2004). The fundamental purpose of information and connection development was to enhance connection capacity and quantity. In any case, when charlatans mishandle automated measurement for great qualities, the goal of revenue and sufficient serves to encourage even more gloomy objectives (Pichard, 2009). Any illegal display supplied using PC advancements or the employment of such breakthroughs as tactics in the execution of the offence is referred to as a PC offence, a PC-related offence, or a technology offence.
2) *Computer Crime on the Interne:* The internet is one of the most wonderful sensations of our time. It has become a symbol of human innovation and delivers a dazzling exhibition of advantages to mankind (Wall et al., 2003). The term "web offence" refers to both cybercrime and computer crime. It has been described as a "two-edged blade" that presents several chances for illicit conduct on the internet (Gottschalk, 2010). On a worldwide scale, online crime has evolved into a global issue that requires complete collaboration and participation from both developing and developed countries. Snap coercion has become a difficult issue for Google and other sites that participate in pay-per-click internet advertising. Several organizations hire misfits to falsely tap into a competitor's achievements to undercut them by increasing their public relations expenditures (S. Pickett, 2002; M. Pickett, 2002). The online adaptations of real-world crimes like hacking and virus spread are another important aspect of cybercrime. People can organize classic sorts of cybercrime using current principles, as well as embrace new, digital-specific rules for emergent types of cybercrime. The issue is with the format in which requirements are written (Jewkes et al., 2013).
3) *Financial Crime on the Internet:* Monetary crime is described as a crime against assets, which includes the illegal transfer of another's property for one's own use and advantage (Larsson, 2006). Some scientists describe financial crime as the use of deceit for the aim of acquiring illicit gain, which often entails a breach of trust and the hiding of the actual objective of the activity. According to some forecasters, financial crime includes a wide range of crimes against assets, such as extortion, racketeering, perversion, illegal tax avoidance, misuse of funds, insider trading, assess intrusion, and digital assaults, as well as extortion, bribery, defilement, illegal tax avoidance, misuse of funds, insider trading, assess intrusion, and digital assaults (Henning, 2009). Financial and creative crimes such as cash fabrication, tax evasion, economic espionage, installments card extortion, computer virus assaults, and cyber warfare may harm all levels of civilisation. Financial crime is usually carried out by well-organized criminal networks that are enticed by the prospect of huge riches. Law enforcement officers must move quickly and with a specific goal in mind, such as gaining confirmation or securing and seizing unlawfully obtained assets. Nevertheless, a variety of reasons make tracking down illegitimate or unlawful resources difficult, if not impossible (Interpol, 2017).
4) *White Collar Computer Crime PC:* White-collar crime refers to a specific sort of financial crime. Cubicle misbehavior can be defined by the offences, the guilty party, or both. Theft of assets for personal or institutional gain is what white-collar crime is classified as. If one of the property categories has a flag that conveys communication, concealment, or misdirection (Simpson,2009). When it comes to the offender, white-collar crime refers to crimes perpetrated by high-ranking members of society for personal or organizational gain. If white-collar crime is depicted and held accountable, it suggests that the crime was committed by members of high society or for organizational gain. That is, people who are well-off, knowledgeable, and socially active, and who are regularly employed by and in actual organizations (Hansen, 2009). The most economically challenged members of society are by no means the primary criminals. People from a certain financial class are also involved in the suspect lead. Lower classes may be distinguished by this type of violation, such as legitimate advocates supporting criminal customers in laundering their cash and managers justly compensated open experts to fulfil open or accounting contracts that govern the accountant interconnection to save money. The most criminal kind is significantly more resistant to being welcomed or reproached because of their financial wealth, which is a fundamental distinction between both responsible groups (Brightman, 2011).

B. Cybercrime Cases

More lately, digital hoodlums have broadened their horizons and guided by monetary and political thought processes, have perpetrated a wide range of crimes, and caused substantial financial and human suffering throughout the world. A rising number of lawsuits have been filed in court because of the change in power. Prosecutors and courts have encountered some well-known issues because of these cases, and more may be on the way (Smith, Grabosky, & Urbas, 2004). Man has become dependent on the Internet for all his needs as technology has progressed.

Man may now access anything from a single area thanks to the Internet. Personal communication, online shopping, data storage, gaming, web-based testing, and online jobs, among other things The Internet is widely utilized. The notion of cybercrime rose in popularity as the internet and its attendant advantages expanded in popularity.

Cybercrime may take many different forms. There was minimal anxiety a few years ago about wrongdoings that may be disclosed on the internet. In terms of cybercrime, India isn't far behind other countries, where the incidence of occurrence is likewise steadily growing. Cybercrime may be described as illegal demonstrations that involve the use of a computer as a tool or a target. Phishing, credit card fraud, bank robbery, illegal downloading, modern surveillance, child obscenity, kidnapping through chat rooms, traps, digital fear-based authoritarianism, production, and a scattering of viruses, spam, and other forms of infringement are just a few examples. Cybercrime is a wide term that refers to any illegal activity that involves the use of computers or computer systems as a tool, a purpose, or a site for criminal growth, and can range from electronic theft to administrative assaults. It also covers the normal wrongdoings involving the use of computers or systems to aid illicit development. Allow us to talk about the many forms of cybercrime cases.

1) *Fake Websites:* Culprits develop fake websites that look legitimate to fool customers into providing personal information such as usernames, passwords, credit card numbers, and social security numbers. These sites often seem identical to authentic ones, and they may even utilize similar web addresses to entice customers in. A fictional bank site, for example, might be made to seem like a true bank site simply altering the URLs. The con artist now has the client's bank account details after they enter their information on the fake website. Fake websites are becoming more difficult to detect, earning billions of dollars in false revenue at the cost of innocent internet users. Due to their style and appearance, clients may find it difficult to recognize these sites as phony (Abbasi, Zhang, Zimbra, Chen, & Nuna-maker, 2010).
2) Money Laundering: Tax evasion is the concealment and integration of unlawful earnings into the actual blue cash system. It's riskier for gang bangers to spend unlawful money before laundering the proceeds of crime since they won't know where it came from, and it'll be harder to trace it back to the crime. After being laundered, it is difficult to tell the difference between cash and legitimate monetary assets, and the assets might be utilized by criminals without being identified. Money can be distributed in a variety of ways. Tax evasion is sometimes broken down into three parts.

a) *Incorporation:* Incorporation is the process of introducing unlawful monies into the financial system.
b) *Layering:* A technique for shielding assets from their source, which may include the employment of unknown shell firms.
c) *Integration:* The money is returned to the offender from what appears to be a reliable source. Tax evasion is a steady stream of assets. There is a location where money is created and a place where money is laundered. This type of veiled confidence is evident even in the strongest findings on unlawful tax evasion.

3) *Bank Fraud:* Extortion from a bank or other financial institution is a criminal conduct that happens when a person obtains money or resources through illicit means (legaldictionary.net). As a result of the growing impact of banks and monetary institutions on today's society's financial outlook, criminals have new opportunities to prey on people's rights, amidst any great achievements they could have on the improvement of credit intermediaries; as an outcome, we might see more extremely complicated and new types of crimes is been devoted in bank and economic structures areas, which are not the same as their traditional forms (Hidarimanesh & Esfahani, 2016). Various organizations have been concerned about money-related deceit; billions of dollars are lost each year because of this extortion (Duhart). Fixed deposits, loans, or expanding credit privileges for bribery, phishing, and other web/ATM-based fakes are among the current misrepresented events in India that have been reported in the media. Recent high-profile examples show that fraud not only jeopardizes benefits, operational efficiency, and continuous client satisfaction, but it may also harm an organization's brand. Regardless of any administrative fines, it is possible that it will have a negative influence on employee morale and financial expert confidence.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

V. SYSTEM ARCHITECTURE

A. Cybercrime Tools

Computer crime detectives require a variety of special tools such as the use of about certain tactics. Small equipment can also be selected by dealers based on the kind of computer device and the type of automated display. A prevalent misconception concerning the use of PC criminological instruments is that they are solely used to prosecute cybercrime. This is incorrect. While cybercrime is rapidly growing to levels unfathomable only ten years ago, computer legal sciences are not restricted to this sort of crime. Indeed, cybercrime is only a minor part of the issues settled by PC legal specialists. Methods, Techniques, and Issues in Digital Evidence Up to 93 percent of all data is never retrieved from the digital environment... As a result, the great majority of statistics are generated and created in a virtual setting. Automated pictures, electronic email, online meetings, and messaging are all impossible without a computer. For researchers, this implies that more and more data is being available in digital format. Many types of affirmation, like as the truth, are only effective in automation. The usage of specific gear is required for reviving automated proof in the direction of quantifiable exams. PC quantifiable investigators can retrieve data that has been erased, encrypted, or concealed in the folds of mobile phone innovation; they may be called to testify in court and recount the evidence revealed during examinations. They might be utilised in circumstances like assessing the arguments of guilty parties, probing Internet misuse, exploiting computing resources, and leveraging the system to develop PC-related threats. In real-life situations that included data loss, disruptions, or any other type of incident, forensic experts can be called in to help. Using methods and unique programming criminological applications to assess framework gadgets or stages, they may be able to supply significant disclosures to stick who was/oversaw an examined crime.

B. Hardware Tools

There is a wide range of cybercrime-specific devices available. Cloning devices, composition blocks, easy capacity devices, connections, linkages, and that's only the beginning are just a few of the devices available. Without computers, any cybercrime lab would be incomplete. You'll need the best computer workstation you can get your hands on as an inspector. Cybercrime assessments need a great deal of mental acrobatics. Many, multicore CPUs, as much RAM as you can get 40 (the more, the better), and pricy, short hard drives make up a fantastic examination gadget. Producers of legal programmes provide details about the bare minimum and proposed equipment requirements. Cybercrime is no longer only a "PC-based" activity. Mobile phones and GPS gadgets, for example, are filling labs all over the world. . Cellebrite's UFED supports over three thousand phones. Over 4,000 phones, PDAs, and GPS devices are supported by the Paraben organisation, a rival of Cellbrite. It is critical to have the right connection while operating telephones. Unlike PCs, cell phones need a significant amount of infrastructure in terms of ports and connectivity. Labs require a high number of connections close by to accommodate the wide assortment of handsets that come through the doors. Fortunately, many of the necessary connections are provided by the producers of instrumentation for mobile phones. Only a few firms manufacture copying equipment. A forensic clone is a "bit stream" duplicate of a piece of media, such a hard disc. These gadgets can considerably increase the pace of the process.

C. Software Tools

A wide number of cybercrime programming tools are now available. A few examples of common tools that may be used for a range of tasks. Rest is more focused, meeting a genuine need. Such programmes tend to focus on a certain sort of proof, such as email or web, when considering whether to develop the programme using open-source resources or a professionally generated item. Both have their benefits and drawbacks. Cost, usefulness, capacity, and support are just a few of the factors to consider while making this selection. Forensic Toolkit (FTK) from Access Data and Encase from Guiding software are the most well-known general programs for enterprises. These two programmes are amazing, and they have the potential to make exams go much more easily and effectively. These applications are equivalent to a "Swiss Army Knife" in terms of functionality. They conduct things like "searching," "e-mail research," "sorting," "reporting," and "password cracking," among other things. These goods' investigation features are particularly impressive, allowing investigators to easily dig down to the details they're looking for. Here's a brief rundown of some of the information you could find: Some of the phrases utilised include "Email addresses," "Names," "Phone Numbers," "Keywords," "Web addresses," "File sorts," and "Data ranges."

D. Brief Study on Digital Forensic Tools

To understand how these tools work to mitigate cyber threats, four Digital Forensic technologies must be studied. The four Digital Forensic tools are iSafe, USBDeview, Recuva, and WinHex.

1) ISafe

ISafe is a networked and system-monitoring digital forensic tool [2] that records keystrokes, takes system snapshots, shows which apps are running on the system, records mouse click events, analyses the network, and displays information on the websites visited.
Some of the advantages of iSafe are as follows:

a) ISafe records most activity, such as websites viewed, print jobs, attached drives, microphones, and file sharing [3].
b) ISafe offers AES 1,024-bit encrypted log files as well as activity restriction features.
c) The ISafe tracking programme is simple to install and use, even for those with no prior IT experience.
d) It keeps track of almost every activity and blocks them based on their content [3].
e) The unintended effect of I Safe is:
f) ISafe lacks features that many IT organisations desire, such as bandwidth use warnings and port monitoring.

2) USB Deview

The USB Deview data recovery tool identifies and analyses all USB devices attached to a system, and report based on device type, serial number, date manufactured, and last plug/unplug date, among other factors [4].
USB Deview also allows you to deactivate and facilitate USB devices, as well as remove previously used USB devices, detach USB devices that are presently connected to our computer, and remove previously used USB devices.
If the admin user is used to log in, the USBDeview can be utilised on a remote machine.
Some of the advantages of USB Deview are as follows:

a) The main advantage of USBDeview is that it allows us to handle tainted USB device information, such as USB flash drives, so that we may repair it using the updating process once we've detected the tainted flash drive information.
b) USBDeview is user-friendly and easy to use.

The following are USBDeview's disadvantages: • USBDeview does not allow you to activate or disable USB devices on a 32-bit system.

- The 'Created Date' column on Windows 7/8/Vista/2008 does not provide exact principles.
- If a USB device has a bad driver, USBDeview may be disabled [4].

3) Recuva

Recuva is a well-known file recovery tool for recovering mistakenly deleted data from a Windows PC, recycle bin, or MP3 player [5]. All of our data, files, photographs, and media files are restored. It aids in the upkeep of our computers, as well as memory cards, USB flash drives, and iPods.

Some of Recuva's advantages are as follows:

a) Recuva retrieves all the important papers we'd written in our word document during the past 5 hours.
b) The programme is particularly effective for retrieving word file write-ups that have not been saved.
c) The procedure is straightforward, and if we require a backup on a device other than our own, we may do it without having to configure anything on that device.
d) It offers information about the electronic message before we can truly erase it. It is constructed using the most recent material stored, resulting in the omission of the file that restores our data.
e) When we use Recuva to recover emails, it recovers them as.ZIP files.

The following are some of Recuva's drawbacks: • The lack of filters is Recuva's worst flaw.

- Recuva will not recover files erased using Ccleaner.
- Takes around 6 hours to scan an 80GB partition (C:).
- There aren't many layouts in Recuva, and it can't look at portable media.
- It has a proclivity for crashing at inopportune times.
- Some of the photographs are impossible to find using Recuva.

4) Winhex

Winhex is a global hexadecimal editor that is used in digital forensics [6][7]. Winhex assists with digital forensic elements such as includes motivating, uninformed processing, and IT security measures. [6][7]. Winhex examines and revises all forms of data, as well as recovering deleted files from hard drives and damaged files retrieved from any digital source.

Some of Winhex's advantages are as follows:

a) Only cargo ships data that is expressly targeted, omitting data that is not, as may be needed by law or the client.

b) Quick to create, especially when using F-Response [8] to retrieve remote hard discs over a weak network connection.

c) Full access to all critical file system data.

d) If correctly prepared, the output serves as a straight raw image of the disc for all projection purposes, with the original offsets and comparative distances between data structures preserved.

The following are some of Winhex's flaws:

- The expense of each treatment's license may have been decreased.
- WinHex does not hinder the contents of System Console.
- WinHex is not supported on Macintosh or Linux PCs.

5) Pro Discover Basic

The instrument includes an advanced legal inspection mechanism that allows us to photograph and validate the disc's cover. When the criminological image is included, users may see a database by looking at the content and observing groups that store such data. Similarly, a client inspects knowledge as information in the context using the Search focus point, depending on the criteria specified.

Create a heap of the meander and a fuse show from the "Include" focus to begin utilising Pro Discover Basic. To analyse data, use the 'Substance View' and 'Group View' centre points, as well as the Tools menu to do exercises on the data. Tap a "Report" centre point to see important information.

Figure 1 Pro discover tool

6) FTK Imager

Analysts can utilise the FTK Imager to quickly assess the contents of logical photographs or memory dumps, as well as local hard discs, arrange drives, and CDs/DVDs. The FTK Imager is a tool for data and imaging. Analysts can use FTK Imager to create SHA1 or MD5 hashes of archives, transport records, and envelopes from criminological pictures, as well as circle, review, and recover records that have been deleted from the Recycle Bin (provided their data pieces haven't been overwritten) and mount a quantifiable picture in Windows Explorer to see its substance.

To begin, select "Record >Include Supporting Item" to add a piece of proof to the survey.

Go to "Document > Create Disk Image" to create a forensic image that the investigators may use.

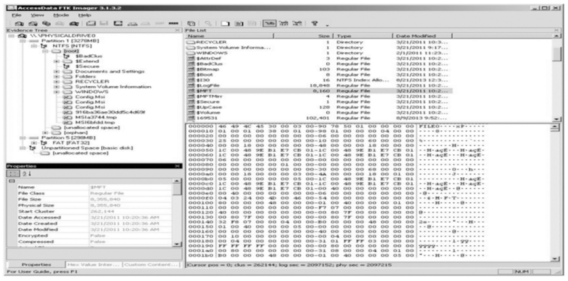


Figure 2 FTK imager

7) Linux 'dd'

dd is now halting various Linux divisions (e.g., Ubuntu, Fedora). The Linux 'dd' software may be used for a number of difficult legal activities, such as forensically wiping (zeroing) a drive and generating a rudimentary image of a disc. dd is a strong tool that, if misused, may result in terrible results. It is suggested that you test this device in a secure setting before using it in the real world.
Simply open a terminal window and type dd followed by a list of order parameters to utilise dd. The following dd language syntax is necessary for forensically wiping a disc:

VI. RESULTS

Solutions for Digital Forensic Tools: ISafe, Recuva, USBDeview, and WinHex are supplied and described from the attacker's perspective based on numerous criminal incidents, including how to identify the theft and how to eradicate the threat.

A. Case 1

In a brokerage case, the defendant pleads guilty to stealing money [9]. One of three defendants in a computer fraud scheme that used Trojans to steal money from brokerage accounts pled guilty to federal charges in New York. The three persons, according to an outcome that did not describe how they accomplished it, placed key logger Trojans on the victims' computers [9].
The defendants obtained the victims' passwords when they logged onto their brokerage accounts and used them to gain access to the accounts. [9]
In this case, ISafe was employed as a tool.
Steps:

1) Install ISafe on the victim's computer.
2) Click Start to begin monitoring the victim's computer.
3) After hitting the start button, restart the computer.
4) On the victim's computer, the software will be completely concealed, and unhiding it will involve hitting a shortcut key that only the attacker knows.
5) The attacker acquires every detail about the victim's actions by the photo he receives in his email.

The Security Task Manager from Neuber is a piece of software that gives us background information about our computer's current visible and hidden activities. Our antivirus product misses malware and rootkits, but Security Task Manager identifies them.

B. Case 2

Cyber crooks have emptied ATMs that ran on Windows XP and were robbed using infected USB sticks (most ATMs still run Windows) [10]
In 2013, cyber hackers targeted many cash machines belonging to an unknown European bank, stealing money from the devices with a simple USB stick [10]. The attackers, who were well-versed in the technical details of the ATMs, drilled holes in them to allow them to install a USB drive with specially built malware. [10]
The case was examined using USBDeview..

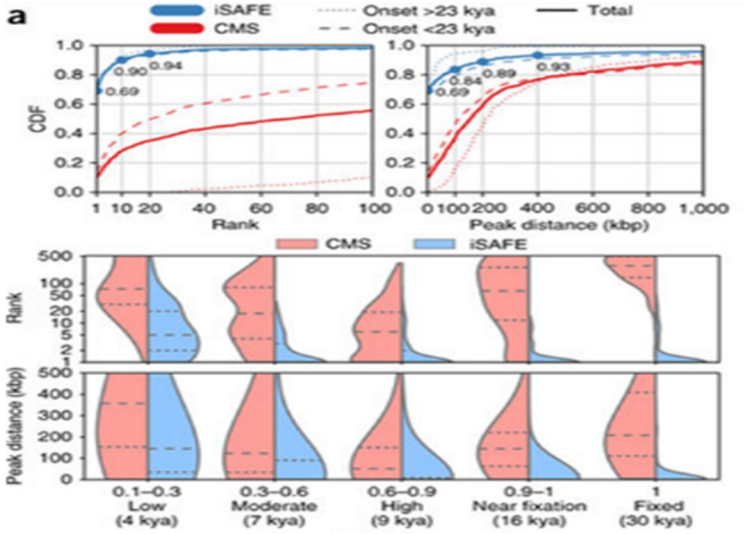


Figure 3 Performance of isafe

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Solution:

1) Install USBDeview on your PC and run it.
2) Examine the date and time of the occurrence, as well as any USB devices connected now, using the USBDeview Interface.
3) Check to determine whether the USB drive has been used previously.
4) Locate the files created in the system on each disc based on the incident date and time.
5) Check the files for dates and times that match the incident on the system, then delete them since the attacker must have installed the malicious application to attack and take the money.
6) Examine the CCTV camera footage by the time and date of the incident.
7) Use technology to track down the offender and capture him.

C. Case 3

Hurricane Katrina taught us a valuable lesson [11].

Hurricane Katrina caused a slew of problems for Gulf Coast businesses, the most serious of which was data security [11]. While some companies deployed remote data backup services or planned to ensure their backups were secure, others were left with flooded systems and no backups [11]. Katrina showed how natural disasters can ruin even the best-laid plans, thus data recovery became a must-have option when all other choices were exhausted [11]. Unfortunately, for many small businesses, high-level data protection is too expensive, placing them in a tough position [11]. Some businesses faced the prospect of losing all their vital data, even putting them out of business, if they didn't have established backup systems in place [11].

Recuva was used in this situation.

1) Open the Recuva software application by downloading it and running it.
2) After selecting the option you want to recover, click Next.
3) After choosing the location where the files were deleted, click Next.
4) Click Start after selecting Enable Deep Scan from the drop-down option.
5) From the context menu, right-click the file we want to restore and select Recover Highlighted.
6) Use the same disc location where the file was deleted to recover it; otherwise, there's a chance it won't work.
7) After a successful recovery, the task reports are produced, and the file is recovered to the target disc.

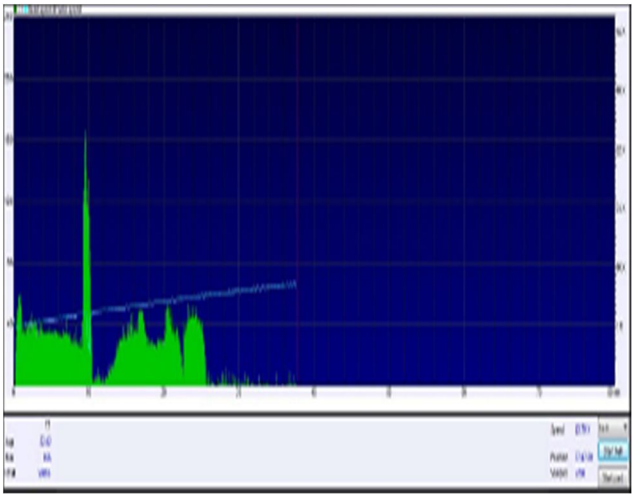


Figure 4 Working of Recuva

D. Case 4

Video games are targeted by hackers for several purposes, including amusement, profit, and greater scoring [12].

Last year, Nintendo said that it had been the target of a hacking incident in which hackers acquired unauthorised access to a Nintendo members reward site 23,000 times after 15 million attempts [12].

Hackers attempted 4 million times to get access to Konami's networks, with 35,000 of those efforts succeeding [12]. Crytek, a game firm, also revealed a compromise. Bohemia Interactive, a Czech gaming firm, confessed that it, too, had been hacked after the source code for their DayZ game surfaced on a game-hacking site [12].

In this case, WinHex was utilised.

Solution:

1) Install and run both the WinHex software package and the game we want to alter simultaneously.
2) Visit 'webcheats.com.br' and copy the WinHex registration code.
3) Select Register from WinHex's Help menu, then paste the copied code from the website and select Ok.
4) Select Tools, then Open RAM from the WinHex menu to see the processes presently running on the system.
5) Click Ok after selecting the memory size from the game process that says Point Blank.
6) Now that the game's hex values are available, go to the website 'webcheats.com.br' and copy the hex value we want to edit.
7) Select the Search option on WinHex's menu bar, then 'Find Hex Values,' paste the copied hex value, and then click Ok.
8) Change the game's hex value to allow endless ammo.
9) You'll see that the ammunition remains the same when you start the game and pick any shooting weapon.

Table 1 Features of the Tools

Tools	Cost	Operating System	Function
I safe	Free	Windows/Linux/Mac/ Android	The software can run a mining technique for mobile and has an ability to examine several types of memory dumps [15]
Recuva	Free	Windows/Linux	Useful in finding the possible location from raw location data of android application [16]
USB Deview	Paid	Windows XP/Vista/7/8	Software utility; can crack lock screen, decode communication, files and database of devices [17]
CMS	Paid	Windows	Able to perform secure forensic extraction on many type of mobile

This is how hex values are utilised to change a game.
We should back up our company's confidential data and then use a hard drive cleansing method to protect our personal privacy. Because cybercrime is expanding and increasing at such a rapid rate, the tools used to counteract it are evolving and growing at the same rate.

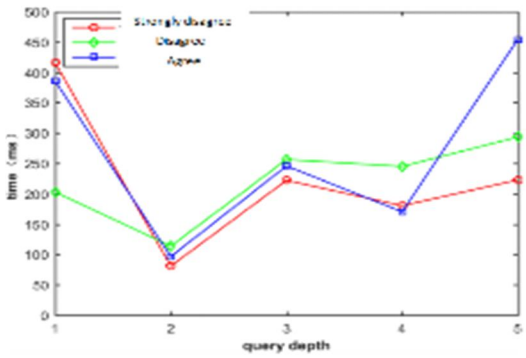


Figure 5 Database Opinions

VII. CONCLUSION

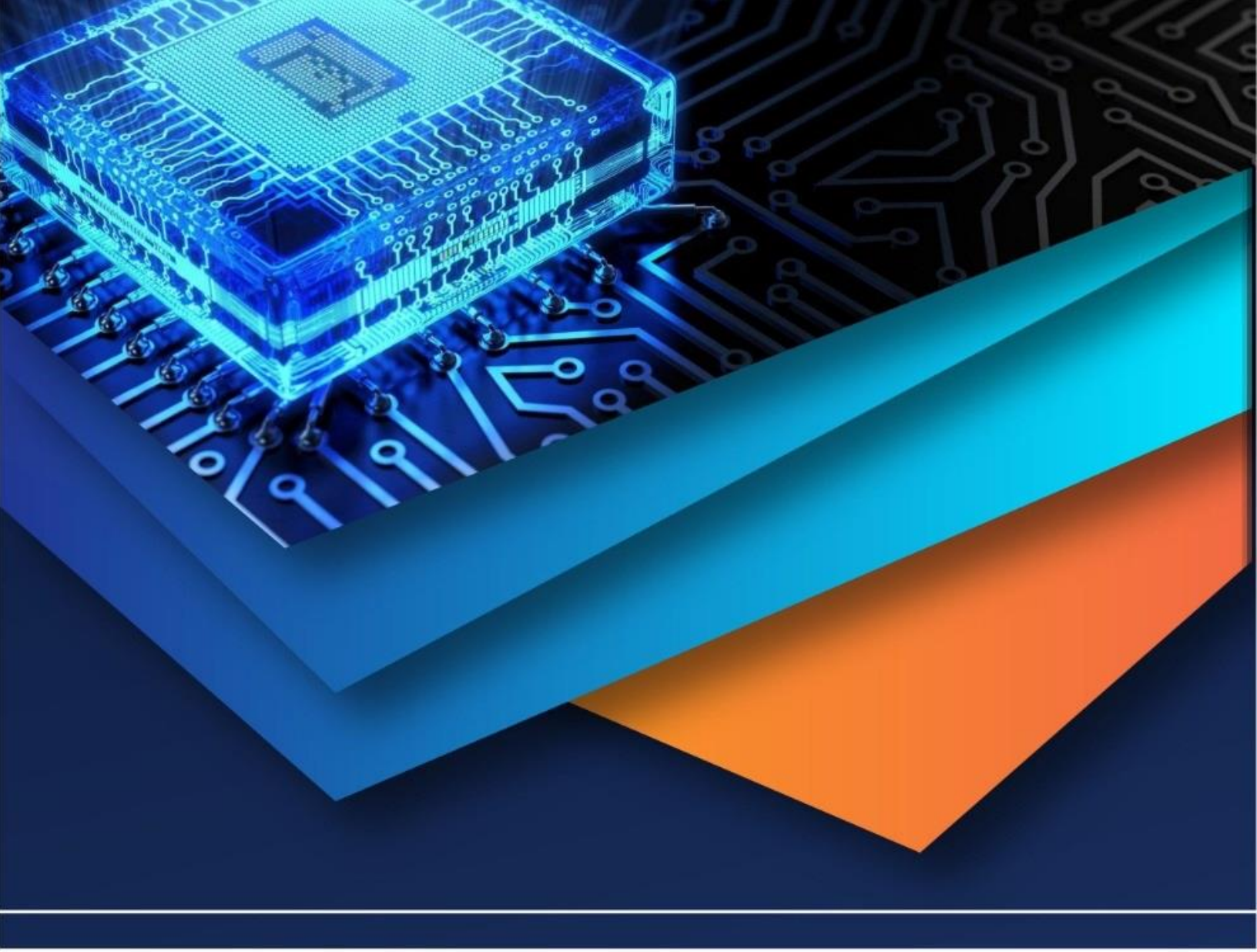
In the face of wrongdoers and conventional clients, the Internet's future remains uncertain. Fears of a more sophisticated Apocalypse are alive and well, and the potential for broad extortion to wreak devastation is practically endless. We looked at computer crimes, cybercrime cases, and a variety of hardware and software tools. There is no such thing as a single device that can do everything or does everything well. Regardless, keeping many instruments on hand is a good habit to have. Using a variety of gadgets to verify your results is also a great way to go.
We investigated the various Digital Forensic tools that play a critical role in locating digital evidence from digital sources, and we discovered that isafe is always better to use in a few or other areas to investigate offences, considering the rise in the number of computer-related crimes. Because We believe that digital forensic methods are valuable in cybercrime investigations and will become more successful in identifying vital digital evidence in the future shows that 88.88% of the database agree that they “can pre-process data into vector space model formats for use in machine learning applications” as shown in Figure 5.

As a result, Digital Forensic technologies are necessary to build solutions with the purpose of detecting and deducing theft.

Future work will involve improving the library and adding more modules. Possible future data sets and modules that can be added include web security data, phishing data, steganography data, etc. Additionally, we will provide more use cases of how to use the library in various other applications.

REFERENCES

[1] K. Inman and N. Rudin, Principles and Practice of Criminalistics: The Profession of Forensic Science. Florida, USA: CRC Press LLC, 2000.
[2] K.K. Sindhu and B.B. Meshram. (2012, April). "Digital Forensics and Cyber Crime Datamining." Journal of Information Security [Online]. vol. 3, no. 3. Available: https://www.scirp.org/html/3- 7800083_21340.htm [Accessed: 21-Aug- 2020].
[3] J. Jones and L. Etz Korn, "Analysis of digital forensics live system acquisition methods to achieve optimal evidence preservation," in Southeast on 2016, Norfolk, VA, USA, 2016, pp. 1-6.
[4] E. Casey, Handbook of Computer Crime Investigation: Forensic Tools and Technology. London, UK: Academic Press, 2002.
[5] A. K. Mohan and P. Selwin, "Digital forensic investigation using sleuth kit autopsy," in National Conference on Information, Communication and Cyber Security, India, 2016, pp. 43-48.
[6] K.K. Arthur and H.S. Venter, "An Investigation into Computer Forensic Tools," [Online]. Available: https://pdfs.semanticscholar.org/1636/195399eeeca73911458c41acaa96f 98d292a.pdf [Accessed: 20-Aug-2020].
[7] "Volatility." GitHub [Online]. Available: https://github.com/volatilityfoundation/volatility [Accessed: 20-Aug2020].
[8] "Mail Viewer." MITEC [Online]. Available: https://www.mitec.cz/mailview.html [Accessed: 21-Aug-2020].
[9] C. Sanders, Practical Packet Analysis, 3rd ed. San Francisco, CA, USA: No Starch Press. Inc., 2017.
[10] Xplico. [Online]. Available: https://www.xplico.org/ [Accessed: 21-Aug2020].
[11] INFOSEC. (2019). Computer Forensics: Network Forensics Analysis and Examination Steps [Online]. Available: https://resources.infosecinstitute.com/category/computerforensics/introdu ction/areas-of-study/digital-forensics/network-forensics-analysis-andexamination-steps/#gref [Accessed: 21-Aug-2020].
[12] "XRY – Extract." MSAB [Online]. Available: https://www.msab.com/products/xry/ [Accessed: 21-Aug-2020].
[13] G. Suciu, C. Istrate , R. I. Răducanu , M. Dițu , O. Fratu and A. Vulpe, "Mobile devices forensic platform for malware detection," in. 6th International Symposium for ICS & SCADA Cyber Security Research 2019 (ICS-CSR), Athens, Greece, 2019, pp. 59-66.
[14] R. Ahmed and R. V. Dharaskar, "Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective," in 6th International Conference on E-Governance, New Delhi, India, 2008, pp. 312-323.
[15] "SQLite Forensics Browser." Revove. [Online]. Available: https://www.revove.com/database-forensics/sqlite-forensics-browser/ [Accessed: 22-Aug-2020].
[16] E. C. Cankaya and B. Kupka, "A survey of digital forensics tools for database extraction," in 2016 Future Technologies Conference (FTC), San Francisco, CA, USA, 2016, pp. 1014-1019.
[17] Noori, Roman. (2021). Network Security Attacks and Countermeasures on Layer 2 and Layer 3 Network Devices. International Journal for Research in Applied Science and Engineering Technology. 9. 1173-1185. 10.22214/ijraset.2021.33462.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY