International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

A Computer in Digital Forensic: Computer Forensic

KAVYA SHREE J[1]

Post Graduate Student, Department of Master Computer Applications, D.S.C.E., Bangalore, India

ABSTRACT

The report focuses on computers' roles in digital forensics. All of these industries are implementing digitalization into their operations as the globe progresses toward digitalization. As a result of digitalization, working methods are becoming more productive and convenient. To employ digitalization, all we need is a computer or a system. Some forensics software tools are available, but they must be loaded on computers in order to complete the operation. It gives us the advantage of being able to operate quickly. Crimes committed have grown increasingly frequent in electronic or digital worlds, particularly cyber. Technology is being used by criminals to commit crimes, providing new obstacles for law enforcement agents, lawyers, magistrates, army members, and security experts.

i)INTRODUCTION

The term "digital forensics" refers to the process of detecting and comprehending electronic data. Mobile phones, tablet devices, video game systems, pcs, and home computers are all becoming indispensable in modern society. Because these devices are so widely adopted in our daily lives, there really is a possibility that information gathered from them will be misused. Fraud, drug trafficking, homicide, phishing, forgery, and terrorist acts are all crimes that involve computers.

Digital forensics (DF) was originally utilised in law of enforcement agencies, cybersecurity, and civil defence to combat computer crimes. Digital forensics is being included into the architecture of law enforcement organisations, finance companies, and investing firms

- Hans Gross (l847-l9l5) was the first to use a technical study in a criminal investigation.
- Since l990, what we used to call digital forensics has been referred to as "computer forensics."

II) TYPES OF DIGITAL FORENSIC:

l)Computer-forensic

2)mobile-forensic

3)network-forensic

4)live-forensic

5)email-forensics

III) INTRODUCTION TO COMPUTER FORENSIC:

Computer forensics is the process of collecting and preserving testimony from a specialized computer system in a way that may be submitted as evidence in court using investigation and analysis tools. Computer forensics aims to conduct an organized investigation and preserve a recorded chain of forensic evidence in order to determine precisely what happened on a system and who was to blame. A computer forensics examination covers a wide range of topics; consequently, the case's success relies on meticulous documenting of facts that is educational, cohesive, and correct.

iv) COMPUTER FORENSIC TECHNOLOGY TYPES

4.l) Disk forensic

Disc forensics is the study of retrieving information from digital storage devices for forensic purposes includes hard-drives/secondary memory, Universal Serial Bus-device, FireWire adaptors, Compact disc, Digital versatile disc, Flash Drivers, and floppy disk drives.

The process of Disk Forensics is:

l. Detect digital evidence

2. Take the proof and keep it.

3. Ensure the proof is legit.

4. Maintain the evidence preserved.

5. Examine the evidence

6. The findings should be reported.

7. Documenting

4.2) The Disk forensic tools:

4.2[a]) ADS locator

Alternate Data Streams (ADS) are a method of storing data on machine that is not easily available to consumers. Files created with ADS are not easily accessible by Windows and do not appear in any file directory. windows create ads files on its own, and most p2p software does as well This software will only find ADS items that have the customer type "alternative/option," which is occasionally used by spyware, infections and malware.

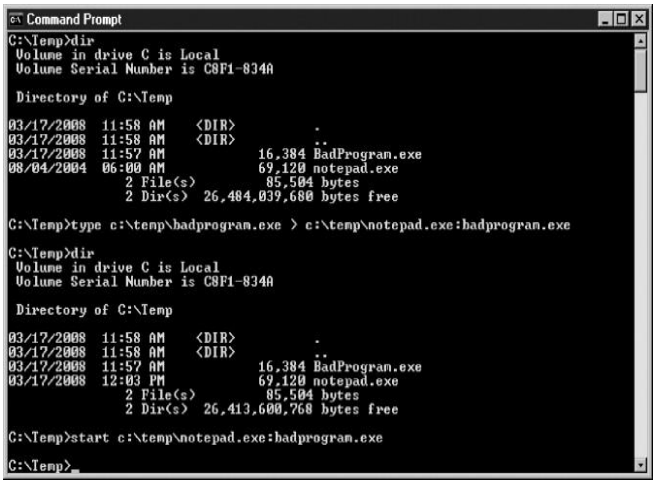

Fig l: ADS locator

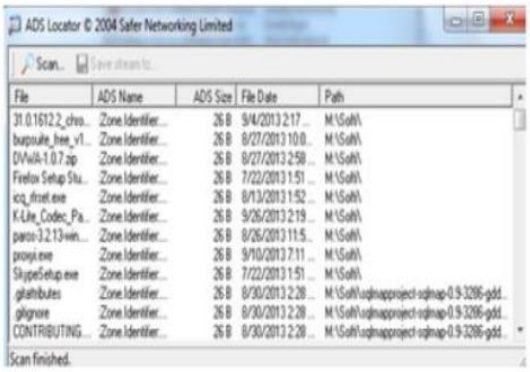

Fig 2: Data forensics

4.2[b]) Disk investigator:

Disk Investigator is a programme that allows you to find out what's on your system's hard drive. It can also help you recover data that has been lost. bypassing the OS in favour of viewing the bare sectors of the hard drive, you can see the true drive contents. Raw directories/folders, documents, groups(clusters), and system sectors may all be viewed and searched more easily. Examine the program's efficacy in erasing files and discs. Restore previously deleted files

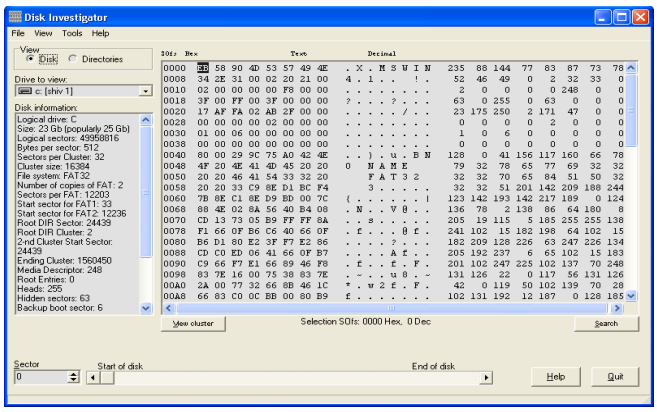

Fig 3:Disk investigator

4.2[c]) RECUVA

RECUVA tool to restore files for free that can recover files from both local and external discs that have been lost or erased. The built-in wizard walks users through the entire recovery procedure step-by-step. Smart cards encrypted Digital-cards, Memory stick, Digital cameras, Flash cards, and many other removable media can all be used.

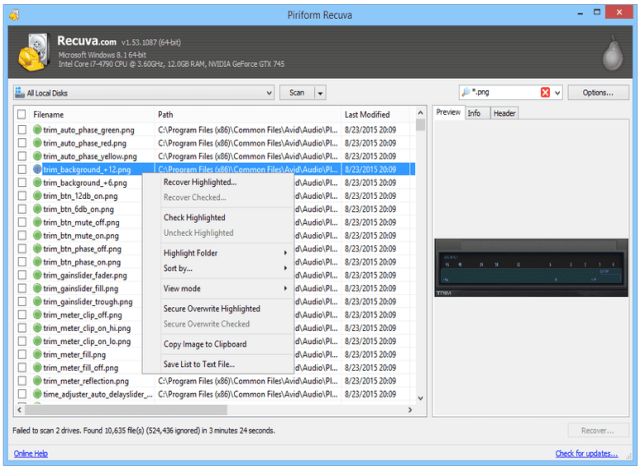

Fig 4: RECUVA

4.2[d]) Encrypt disk detector

ENCRYPTED DISK DETECTOR is a command-line application that checks for encoded files encrypted with encryption software True-crypt, Pretty Good Privacy, or Bit locker on an internal physical disc of the system. If no disc encryption signatures are found in the Master boot record, Enhanced disk drive displays the Original Equipment Manufacturer ID and, if appropriate, the volume label for divisions on that disc, in addition to checking for Bit locker volumes. During an incident response, Encrypted Disk Detector can also be used to search for encoded folders on a computer system quickly and discreet the judgement can then be made to

look into it further and see if a to protect your data, you'll need to acquire it live. and collect evidence that would otherwise destroy if the plug had been yanked.

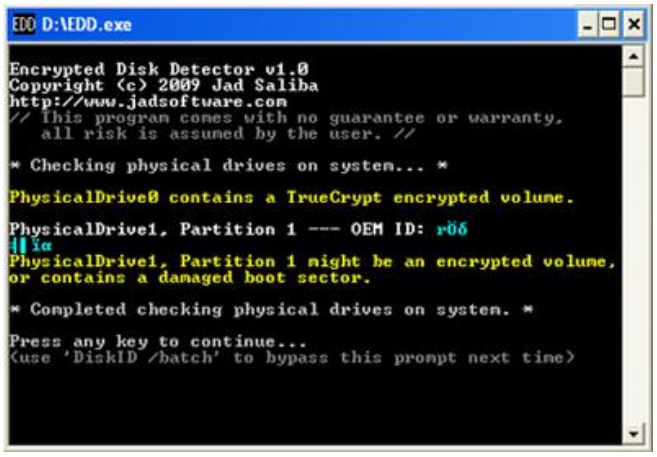

Fig 5: EDD

4.2[e]) password encryption manager

This application looks for password-protected and encoded files on a computer and shows the encoding difficulty and Each one has its own set of decoding possibilities You get access to all credential recovery and decryption methods for the records and hard disc pictures in the situations you're looking into when you work with EA.

V)NETWORK FORENSIC:

Data that is both unstable and changeable is investigated in network investigations. Network forensics is typically a proactive analysis since network communication is usually sent and subsequently lost. Network forensic specialists are used by insurance companies and lawyers to locate evidence to cut down on the amount paid in an insurance company. Users can also employ Network Forensic specialists to back up claims of wrongful termination, sexual assault, or racism

The two main applications for network forensics. The first is network security, which includes keeping an eye out for odd traffic and intrusion detection. An attacker will be able to remove all log files on a hijacked system, leaving only internet proof. law enforcement is the second form of network forensics. Wiretapped network traffic (data transmission) can be utilised for Reattaching transferred data, searching for keywords, and translating human communication such as e - mails and chatrooms are all jobs that need to be completed.

vi)FORENSIC SYSTEM USED TOOLS

Various software tools are utilised in the field of computer forensics. The people who work in this field are known as investigators. They had to look for the encrypted file among the tasks they had to do. As a computer forensics expert, your primary goal is to not only retrieve data, but also to solve cases. Investigators can use computer forensics technologies to process all of this data in order to find a solution and close the case.

6.l) Disk analysis: autopsy/sleuth kit

The sleuth kit is a command- line tool for forensic photography analysis from hard drives (secondary memory) and mobile. The Sleuth Kit is making use of behind the scenes in Post-mortem examination, a graphical user interface-based system [6].
Because the tools are built on a flexible and plug-in architecture, users can quickly add new functions [7]. Business service and training are provided regardless of the fact that both software's are free and open source [7].

6.2) Image creation: FTK imager

Due to Post-mortem's inability to generate photos, another approach must be used. While the majority of the Access Information Forensics Toolkit's components are paid. FTK Imager is a data viewing and imaging feature that lets you quickly analyse digital evidence to evaluate if it warrants further investigation with a methodological tool like Forensic Toolkit [6]. Create digital evidence of internal hard discs, Compact discs, Digital versatile disc and other universal serial bus devices, whole directories, or isolated documents from a wide range of media sources [6]

6.3) Memory forensic: volatility

Whereas the Sleuth Kit focuses also on hard disc, it's not the only place on a computer where forensic data and evidence can be found. Important forensic data could be kept in RAM, and it needs to be retrieved quickly and correctly and being forensically valid and relevant [6].
Volatility analysis is a well-known and commonly utilised technique for examining volatile memory. Volatility is free, open-source, and extensible with third-party plugins, just like The Sleuth Kit [6]. In fact, Every year The Volatility Foundation is holding a challenge for consumers to come up with the most useful and unique framework extension. [6].

6.4) Linux distribution: CAINE

Most of those tools listed here are open source and free. While this makes them easy to buy, installation and configuration can be challenging. To make things simple, a variety of Linux computer forensic distribution are accessible as virtual PCs. These virtual PCs come equipped with a number of pre-installed and customised utilities. The Computer Assisted Investigative Environment is a great example of such a tool (CAINE). This Linux edition includes third party plugins for tools like Autopsy, including several of the much more popular computer forensics software

6.5) Network analysis: Wireshark

Regardless of the fact that several forensics tools concentrate solely on endpoints, endpoints are not the primary data source in

a forensics study. Network traffic records can assist in the detection of viruses and the retrieval of data that has been lost or overwritten just on endpoint, and this is where the majority attacks take place. Wireshark is the most well-known and widely used network traffic analytical technique.
Wireshark is a free and open-source network traffic analyzer that includes dissectors for a variety of network traffic types, simple and straightforward UI for traffic monitoring, as well as a lot of power behind the hood. It may either record or examine network capture files in real time [6].

VII) CONCLUSION

As a conclusion we've determined that digital forensics is vital to our civilization, and it's become lot easier to perform with just computers. The evidence has grown out of hand for a single host. This is spread across a number of physical and virtual sites, including resources stored in cloud, social networking sites, and storage units connected to personal networks. As a result, exact and comprehensive evidence reconstruction demands more expertise, time, and resources.
As a result, computers play a significant and useful part in digital forensics. There have been various examples of computer crime and hacking in the recent past. Computer forensics is required to investigate such situations as well as to educate users on how to protect themselves from such assaults or to improve understanding. Every person is at risk of being a victim of cybercrime. Everything is becoming more electronic, and the security of information transmitted via the internet is becoming more of a problem. As a result, as previously said, there are excellent job chances in practically every profession. To summarise, computer forensics is a field with a lot of research potential as well as a tough vocation with no limitations to learning.

REFERENCE:

[l] Computer Forensic Technology Bharat Bhushan#l , Yashpal Singh*2 Joni Birla3 l,2,3Department of Computer Science &Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, India
[2] Darshan University of Mysore, Role of The Computers In Digital Forensics IJSART
[3] Digital Forensics Matthew N. O. Sadiku, Mahamadou Tembely, and Sarhan M. Musa Roy G. Perry
College of Engineering, Prairie View A&M University, Prairie View, TX 77446 United State
[4] Computer Forensics, Cybercrime and Steganography Resources http://www.forensics.nl/links/
[5] S. C.Gupta, (20l7). Systematic digital forensic investigation model. International Journal of Computer Science and Security (IJCSS), 5(l), ll8-l3l
[6]http://www.forensics-research.com/index.php/computer-forensics/computer-forensics-history/
[7]https://www.sleuthkit.org/
[8]https://resources.infosecinstitute.com/topic/7-best-computer-forensics-tools/
[9] https://www.exterro.com/ftk-imager