International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 09 Issue 10 ǁ 2021 ǁ PP. 01-10

Computer Forensics: An Overview

Reshma H.M &Remya.B.Joy
Diploma in Computer Engineering, Students
GOVT WOMEN'S POLYTECHNIC COLLEGE
Kaimanam,TRIVANDRUM

Abstract
Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.Forensic investigators typically follow a standard set of procedure. After physically isolating the device in question to make sure it can't be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition.

Date of Submission: 09-10-2021 Date of acceptance: 23-10-2021

I. INTRODUCTION

1. What is computer forensics?

The goals of computer forensics is to retrieve the data and interpret as much information about it as possible as compared to data recovery where the goal is to retrieve the lost data. The main experts of computer forensics is not only to find the criminals but also to find out the evidence and the presentation of the evidence in a manner that leads to legal action of the criminals. It is most often associated with the investigation of a wide variety of computer crimes it may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create legal audit trail

- It is a branch of digital forensic science pertaining to legal evidence found in computer and digital storage media.
- Computer forensics is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable
- Evidence right be required for a wide range of computer crimes and misuses
- Information collected assists in arrests, prosecution, termination of employment and preventing future illegal activities .

II. CHARACTERISTICS

IDENTIFYING
PRESERVING
ANALYSING
PRESENTING

1. IDENTIFYING

This is the process of identifying the things such as what evidence is present, where and how it is stored, and which operating system being used. From this information the investigator can identify the appropriate recovery methodologies, and the tools to be used.

2. PRESERVING

This is the process if preserving the integrity of digital evidence, ensuring the chain of custody is not broken. The data need to be preserved on stable media such as CD-ROM, using reproducible methodologies. All steps taken to capture the data must be documented. Any changes to the evidence should be documented, including what the change was and the reason for the change. You may need to prove the integrity of the data in the court of law.

3.ANALYSING

This is the process of reviewing and examining the data. The advantage of copying this data onto CD-ROMs is the fact it can be viewed without the risk of accidental changes. Therefore maintaining the integrity and examining the changed.

4.PRESENTING

This is the process of presenting the evidence in a legally acceptable and understandable manner. If the matter is presented in court who may have little or no computer experience, must all be able to understand what is presented and how it relates to the original, otherwise all efforts could be futile.

NEEDS OF COMPUTER FORENSICS

- To produce evidence in the court that can lead to the punishment of the actual.
- To ensure the integrity of the computer system.
- It is also efficient where in the data stored in a single system for the backup.
- To focus on the response to hi-tech offenses, started to intertwine.
- The importance of computer forensics is evident in tracking the cases of the child pornography and email spamming.
- It is the threat against the wrong doers and the people with negative mind sets.

HISTORY OF COMPUTER FORENSICS

- Began to evolve more than 30 years ago in US when law enforcement and military investigation started seeing criminals get technical.
- Over the next decades and up to today the field has exploded, law enforcement and the military continue to have a large presence in the information security and computer forensics field at the local, states and federal levels.
- Now a days software companies continue to produce newer and more robust forensic software programs. And law enforcement and the military continue to identify and train more and more of their personal in the response to crimes involving technology.

GOALS OF COMPUTER FORENSICS

The goals of computer forensics is to retrieve the data and interpret as much information about it as possible as compared to data recovery where the goal is to retrieve the lost data.

The main experts of computer forensics is not only to find the criminals but also to find out the evidence and the presentation of the evidence in a manner that leads to legal action of the criminals.

It is most often associated with the investigation of a wide variety of computer crimes it may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create legal audit trail.

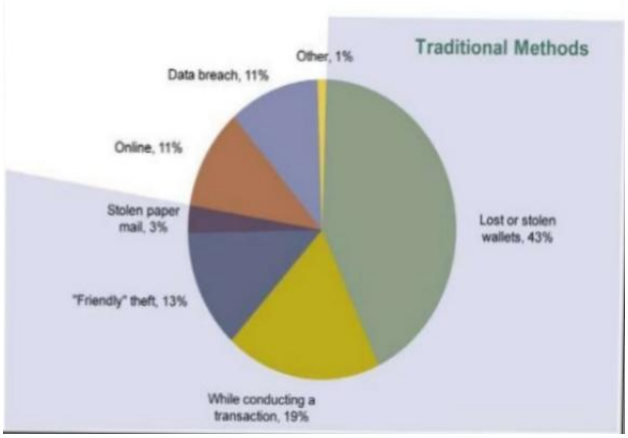
2. CYBER CRIMES & EVIDENCE

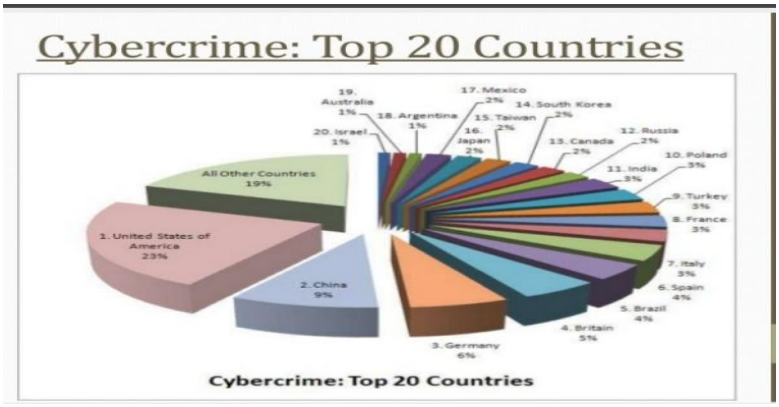
i. What are cybercrimes?

Cybercrimes occurs when information technology is used to commit or conceal an offence.

ii. TYPES OF CYBER CRIMES

1. Forgery
2. Breech of computer security
3. Fraud /Theft
4. Copyright violation
5. Identify theft
6. Threats
7. Burglary
8. Homicide
9. Administrative investigation
10. Cyber terrorism
11. Sales and investment fraud
12. Electronics fund transfer fraud





ii. EVIDENCE& DIGITAL EVIDENCE

EVIDENCE :

An item does not become officially a piece of evidence until a court admits it.

Much of forensics practice concerns how to collect preserve and analyse these items without compromising their potential to be admitted as evidence in a court of law.

DIGITAL EVIDENCE :

Any data that is recorded or preserved on any medium in art by a computer system or other similar device, that can be read or understand by a person or a computer system or other similar device. It includes a display, print out or other output of the data."

iii. **TYPES OF DIGITAL EVIDENCE**

1. PERSISTENT DATA (Non-volatile data)

Data that remains intact when the computer is turned off. Eg: Hard drives, Disk drives and Removable storage devices (Such as USB drives or flash drives)

2. VOLATILE DATA

Data that would be lost if the computer is turned off

Eg: Deleted files, Computer history, The computer's registry, Temporary files and Web browsing history.

iv. RULES FOR HANDLING EVIDENCE

1. ADMISSIBLE :Must be able to be used in court or elsewhere.
2. AUTHENTIC : Evidence relates to incident in relevant way.
3. COMPLETE : (No funnel vision) Exculpatory evidence for alternative suspects.
4. RELIABLE : No question about authenticity and veracity.
5. BELIEVABLE : Clear, easy to understand and believable by jury.

v. TOP 10 LOCATION FOR EVIDENCE

1. Internal history files
2. Temporary internet files
3. Slack / Unallocated space
4. Emails
5. File storage dates
6. New groups / Club lists / Posting
7. Software / Hardware added
8. Files sharing ability
9. Setting, Folder structure, File names
10. Buddy lists, Personal chat rooms records, other saved areas

3. ABOUT THE PROBLEMS

The problem basically behind the computers is the attacks. But a general question arises what are attacks in relation to a computer network or simply a computer system? An attack is defined as any kind of malicious activity targeted against computer system resources, including (but not limited to) a break-in (any unauthorized access), virus infestation, data alteration or destruction or distributed denial of service attacks.

i. GENERAL PROBLEMS

Computers systems may crash, files may be accidentally deleted, disks may accidentally be reformatted, viruses may corrupt files, file may be accidentally overwritten, disgruntled employees may try to destroy your files. All of this can leads to loss of your critical data. Your sensitive records and trade secrets are vulnerable to intentional attacks from, for eg: Hackers, disgruntled employees, viruses etc.. Also unintentional loss of data due to accidental deletion, hardware and software crashes are equally threatening.

ii. CRIMINAL PROBLEMS

The criminal element in society learn to use computers for personal and professional activities, police departments at all

level will most likely increase their hiring of computer forensics report and on the other hand the number of computer forensics experts might not be large.
Crimes involving a computer can range across the spectrum of criminal activity, from child pornography to theft of personal data to destruction of intellectual property. Files may have been deleted, damaged or encrypted, and the investigator must be familiar with an array of methods and software to prevent further damage in the recovery process.

iii.GLOBAL PROBLEMS

The world is becoming a smaller place in which to live and work. A technological revolution in communication and information exchange has taken place within business, industry, and our homes.

In the information technology age, the need of law enforcement are changing as well. Some traditional crimes especially those concerning finance and commerce continued to be upgraded technologically. Paper trails have become electronic trails. Crimes associated with the theft and manipulation of data are detected daily. Crimes of violence also are not immune to the effects of the information age. A serious and costly terrorist act could come from the internet instead of a truck bomb. The diary of the serial killer may be recorded on a floppy disk or hard disk drive rather than on paper in a notebook. Gradually the evidence converted to physical information. In which evidence exists only electronically, and investigators are conducted online.

iv. DNA ANALYSIS

DNA analysis attempt to develop specific identifying information relative to an individual. To support the conclusions, forensics DNA scientists had to gather extensive statistical data on the DNA profiles from which they base their conclusions but the absence of computer forensics led to its failure in the past. The purpose of the computer examination is to find information related to the case but without computer forensics it was not fully possible. To support this computer forensics examination was introduced, for which procedures are needed to ensure that only the information exists on the computer storage media, unaltered by the examination process. Forensic DNA analysis and other forensic disciplines, were not so accurate, reliable or discriminating power of the actual data or information.

v. IGNORANCE

what happens if you ignore computer forensics or practice it badly? You risk destroying virtual evidence or having forensic evidence ruled inadmissible in a court of law. Also you or your organization may run afoul of new laws that mandatory regulatory compliance and assign liability if certain types of data are not adequately protected. Recent legislation makes It possible to hold organizations liable liable in civil or criminal court if they fail to protect customer data.

vi. TRADITIONAL & COMPUTER FORENSIC SCIENCE

Beyond the forensic product and the case related information needed to efficiently perform the work there is another significant difference between most traditional forensic science and computer forensic science. Traditional forensic analysis can be controlled in the laboratory settings and can progress logically, incrementally and in concert with widely accepted forensic practices. In comparison ,computer forensic science is almost entirely technology and market driven, generally outside the laboratory settings, and the examinations present unique variations in almost every situation.

4. SOLUTIONS

i. Deciding How to Respond to an Attack

In the event of a suspected attack on a computer system, the first step in preparing for the investigation is deciding how to respond to the attack. Your organization has a range of response to consider, including :

- Do nothing.
- Performing an analysis as fast as possible so that the compromised system can be required and put back into production , allowing business process to resume.
- Performing as detailed an analysis as possible, properly collecting and preserving all evidence in anticipation of possible prosecution
- Your organization must decide its response in a case by case basis. However, this article marked the following recommends:
- Whenever possible, perform as detailed and comprehensive an investigation as possible.
- Your organization should assume that the information gathered during the investigation will, sometimes into the future, need to be admitted as evidence in account of law for the criminal prosecution of the person participating in the attack.

Once your organization has decided on how to approach an investigation, investigators can take any of the following specific actions to conduct the investigation :

A. Do Nothing

we do not consider this is to be a viable option and strongly recommended any other approach instead. Nonetheless, this approach is taken more often than it should be, with victims of attacks hoping that attackers will get bored and go away. Many home users use this tactic, thinking they have real value on their subsystem or wireless access points, thus they do not consider it much of an issue. The negative consequence to this approach is that your site might be used as a staging point to attack others. You might be the one who receives the knock on the door by the local police department with a search warrant because your system was used to stage attacks upon other system. There might be legal ramifications that can leave your organization liable, if one of its systems was, in fact, used for illegal purposes

B. Reinstall And Move On

This approach is probably the fastest way to recover from an incident with minimal interruption to system operations. Unfortunately, it has become the de facto way in which most computer incidents are handled. In this case, an organization just chalks up the intrusion to the cost of doing business, reinstalls the OS and gets the system back into production as soon as possible. Often, little or no negative publicity about the incident becomes public. The negative consequence of this approach us that it emboldens attackers. They might attack again, and one can't be certain to have closed all the holes. Intruders often leave backdoors that are removed by reinstalling the IS. However, most often, during the initial break in an attacker will gather and retain enough information about your organization to be able to attack more efficiently again. Eg :Attackers might have already sniffed or cracked passwords that will allow them back into your system

C. Investigate For Yourself

The positive aspects of this approach is that no outsider needs to be contacted. Depending in the level of expertise that is available from in-house resources, your organization might be able to complete the investigation in a timely and efficient manner. The downside of this approach is the, even if the investigation is successful, others do not know about the attack scenario and do not benefit from the results of the investigation.

D. Call For Help

Calling for outside help is the most practical of the four options, and it is the approach that we recommended for most scenario. Many sites are not able to have an onsite specialist who knows computer forensic methodology. Computer forensic is a discipline that can take years to really understand intimately. Incan be a daunting task to know all of the different techniques required to perform an investigation on all of the different types of operating system.

Bringing in a trustworthy confidential investigator, when needed, might be less expensive than trying to keep a resident expert on the payroll. A hired consultant who knows computer forensic techniques will often be able to detect, isolate, and help your organization recover from attacks in a timely manner.

ii. DNA Examination

Forensic science discipline have affected countless criminal investigations dramatically and have provided compelling testimony in scores of trials. To enhance objectivity and to minimize the perception of bias, forensic science traditionally has remained at arm's length from much of the actual investigation. It uses only those specific details from the investigation that are necessary for the examination. These details might include possible sources of contamination at the crime scene or fingerprints of individuals not related to the investigation who have touched the evidence. Forensic science relies on the ability of the scientists to produce a report based on the objective result of a scientific examination. The actual overall case may play a small part in the examination process. As a case in point, a DNA examination in a rape case can be conducted without knowledge of the victim's name, the subject, or the specific circumstances of crime..

iii. Forensic Results

Forensic science has historically produced results that have been judged to be both valid and reliable. For example, DNA analysis attempts to develop specific identifying information relative to an individual. To support their conclusion, forensic DNA scientists have gathered extensive statistical data on DNA profiles from which they base their conclusions. Computer forensic science, by comparison, extract or produce information. The purpose of the computer examination is to find information related to the case. To support the results of a computer forensic examination, procedures are needed to ensure that only the information exists on the computer storage media, unaltered by the examination process. Unlike forensic DNA analysis or other forensic

disciplines, computer forensic science makes no interpretive statement as to the accuracy, reliability, or discriminating power of the data or information.

iv. Recovery

System administrators and security personal must also have a basic understanding of how routine computer and network administrative tasks can effect both the forensic process (the admissibility of evidence at court) and the subsequent ability to recover data that may be critical to the identification and analysis of a security incident.

5. FORENSIC TOOLS & ITS TYPES

• Forensic Tools

.The forensic took are the software and hardware used for gathering data from the media storage devices of the computer that is believed to be used to commit any crime

• Types of Forensic Tools

A. Basic Forensic Tools

a. Registry Recon
b. SAN'S Investigative tool kit

B. Other types of Forensic Tools

a. Memory Forensic Tools
b. Mobile Device Tools
c. Network Forensic Tools
d. Database Forensic tools

Memory Forensic Tools	Mobile Forensic Tools	Network Forensic Tools	Database Forensic Tools
• CMAT	• Cellebrite Mobile Forensic	• Wire shark	• Hashkeeper
• Memorize	• Microsystemation XRV	• TCP Flow	• Arbutus

6. METHODOLOGY USED

The basic methodology consists of what you can think of as the three A's:

• Acquire the evidence without altering or damaging the original.
• Authenticate that your recovered evidence is the same as the originally seized data.
• Analyse the data without modifying it.

We expand on each of these three topics in the sections that follows; they are the framework of every forensic game plan. The details of your specific game plan will depend upon the circumstances and your goals, but the plan will always follow these same three steps

i. Forensic Process

Computer forensic investigation usually follow the standard digital forensic process (acquisition, analysis and reporting). Investigations are performed on static data (i.e. acquired images) rather than " live " systems. This is a change from early forensic practices which, due to a lack of specialist tools, saw investigations commonly carried out on live data.

A portable Tableau write-blocker attached to a Hard Drive

ii. Techniques:
A number of techniques are used during computer forensic investigation

• **Deleted files :**A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Mist operating system and file system do not always delete physical file data, allowing it to be reconstructed from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials
• **Cross-drive analysis :**A forensic technique that correlates information found on multiple hard drives. The process, which is still being researched, can be used for identifying social networks and for performing anomaly detection.
• **Live analysis :**The examination of computers from within the OS using custom forensics or existing system administration tools to extract evidence. The practice is useful when dealing with Encrypting file system. For example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged(known as a live acquisition) before the computer is shut down.
iii. Analysis tools
A number of open source and commercial tools exist for computer forensics investigation. Typical forensic analysis includes a manual review of material on the media, reviewing the windows registry for suspect information, discovering and cracking passwords, keyboard searches for topics related to the crime, and extracting e-mail and pictures for review.
iv. Methodology for an investigator
The application of science and education to computer related crime forensics is still largely limited to law enforcement organizations. Building a suitable workforce development program could support the rapidly growing field of computer and network forensics. We propose some generic requirements, resources, and pedagogical approaches for developing and implementing a forensics program in higher education. We don't expect our results to be implemented directly, but we do intend them to stimulate thoughtful discussions, as did the workshop at which many of these ideas originated (the enter for Secure and Dependable Software Forensics investigation methodology is basically the approach that an investigator follows to retrieve possible evidence that may exit on a subject's computer system. For example, the following steps should take :-
1.Shut down the computer.
2.Document the hardware configuration of the system.
3.Transport the computer system to a secure location.
4.Make a bit stream Backup of hard disks and floppy disks.
5.Mathematically verify data on all storage devices.
6.Document all system date and time.
7.Make a list of key search words.
8.Evaluate the windows swap file.
9. Evaluate file slack.
10.Evaluate unallocated space (Erased Space).
11.Search files, file slack and unallocated space for key words.
12.Document file names, dates and times.
13.Identify file, program and storage anomalies.
14.Evaluate program functionality.
15.Document your findings.

7. APPLICATIONS OF COMPUTER FORENSICS
1. Financial fraud detection
2. Criminal prosecution
3. Civil litigation

4. " Corporate security policy and violation "

8. USERS OF COMPUTER FORENSICS

CRIMINAL PROSECUTION

Rely on evidence obtained from a computer to prosecute suspects and use as evidence.

CIVIL LITIGATION

Personal and business data discovered on a computer can be used in fraud, harassment or discrimination.

LAW ENFORCEMENT OFFICIALS

Rely on computer forensics to backup search warrants and post –seizure handling

PRIVATE CORPORATION

Obtained evidence from employee computer can be used as evidence in harassment, fraud and embezzlement cases.

INDIVIDUAL / PRIVATE CITIZENS

Obtain the services of professional computer forensic specialists to support claims of harassment abuse or wrongful termination from employment.

9. SKILLS REQUIRED FOR COMPUTER FORENSICS

- Programming or computer related experience.
- Board understanding of OS and applications.
- Strong analytical skills.
- Strong computer science fundamentals.
- Strong system administrative skills.
- Knowledge of the latest intruder tools.
- Knowledge of cryptography and steganography.
- Strong understanding of the rules of evidence and evidence handling.
- Ability to be an expert witness in a court of law.

10. ADVANTAGE & DISADVANTAGE OF COMPUTER FORENSIC

A. ADVANTAGES

- Ensure the overall integrity and continued existence of an organization computer system are network infrastructure.
- Help the organization capture important information if their computer system or network are compromised.
- Efficiently tracks down cyber criminals and terrorists from different part of the world.
- Tracks complicated cases such as child pornography and email spamming.

B. DISADVANTAGES

- Cost
- Increasing storage space
- New technologies
- Anti-forensics
- Legal issues
- Administrative issues

11. CONCLUSION

- Cybercrimes are increasing in number day to day
- The forensic department has been efficiently delivering its duties by controlling the crime rate of the digital side
- All most in all cases the persons involved have been found out
- On the other hand it is the duty of judiciary to resolve any disputes and punish the accused

REFERENCES

[1]. www.google. Com
[2]. A Yasinsac; RF Erbacher, DG Marks, MM Pollitt (2003)."Computer forensics education".IEEE Security & Privacy.
[3]. Michael G. Noblett; Mark M. Pollitt,Lawrence A. Presley (October 2000)."Recovering and examining computer forensic evidence".
[4]. P.Sommer, "Intrusion Detection Systems as Evidence," Computer Netwoks,vol. 31,nos.23-24, 1999,pp. 2477-2487.
[5]. K. Rosenblatt,"High Technology Crime",KSK Publications,1995.
[6]. D. Icove, K. Seger, and S. VonStorch, "Computer Crime: A Crimefighter's Handbook",O'Reilly & Associates,1995.

[7]. R. McKemmish,"What is Forensic Computing,"Trends and Issues in Crime and Criminal Justice, no.118, Australian Inst. Of Criminology ; www.aic.gov.au/publications/tandi/index3.html.
[8]. C.E. Irvine,S.K Chin and D.A Frincke,"Integrating Security into the Curriculum,"Computer,vol.31,no. 12,1998,pp.25-30.
[9]. C.E. Irvine,"Amplifying Security Education in the Laboratory,"Proc. 1st World Conf.Information Security Education(IFIP TCII WC 11.8),1999,pp. 139-146.
[10]. A. Yasinsac,"Information Security Curricula in Computer Science Departments:Theory and Practice,"5th Nat'l Colloquium Information Systems Security Education 2001:A Security Odyssey,NCISSE Colloquium Press,2001.
[11]. A. Yasinsac, J. Frazier and M.Bogdonav,"Developing an Academic Security Laboratory,"Proc.6th Nat'l Colloquim Informaion Systems Security Education,NCISSE Colloquium Press,2002.
[12]. J.E. Anderson and P.H Schwager,"Security in the information Systems Curriculum;Identification & Status of Relevant Issues,"J.Computer Information Systems,vol.32,no.3,2002,pp. 16-24.
[13]. G. Shpantzer and T.Ipsen,"Law Enforcement Challenges in Digital Forensics,"Proc.6th Nat'l Colloquium Information Systems Security Education ,NCISSE Colloquium Press,2002.
[14]. S.L. Garfinkel and A.Shelat,"Remembrance of Data Passed:A study of Disk Sanitization Practices,"IEEE Security and Privacy ,vol.1,no.1,2003,pp.17-27.
[15]. Y. Manzano and A. Yasinsac , "Policies to Enhance Computer and Network Forensics,"Proc. 2nd Ann.IEEE Systems,Man, and Cybernetics Information Assurance Workshop,IEEE CS Press,2001,pp.289-295.
[16]. Noblett , M.G Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence .In:Proceedings of the 11th INTERPOL.Forensic Science Symposium,Lyon,France.The Forensic Sciences Foundation Press,Boulder,Colorado,1995.
[17]. Pollitt,M.The Federal Bureau of Investigation report on computer evidence and forensics.In: Proceedings of the 12th INTERPOL Forensic Science Symposium,Lyon,France.The Forensic Sciences Foundation Press,BoulderColorado,1998.