ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 5, July 2012

COMPREHENSIVE STUDY OF DIGITAL FORENSICS

Jatinder kaur, Gurpal Singh

SMCA, Thapar University, Patiala-147004, India

jyoti929@gmail.com, gurpalsingh123@gmail.com

***Abstract*— This paper presenting the review about digital forensics, it consists of techniques as well as various tools used to accomplish the tasks in the digital forensic process. Network forensics is forensics and important technology for network security area. In this paper, we inspect digital evidence collection processes using these tools. From last few decades the digital forensic techniques have been improved appreciably but still we face a lack of effective forensics tools to deal with varied incidents caused by these rising technologies and the advances in cyber crime. This article discusses the tools used in network forensics , various gaps founds in these tools, and the advantages and disadvantages of these tools.**

***Index Terms*— Forensics, Digital evidence, Network forensics, computer forensics, Cyber crime , Encase, Sleuth Kit.**

I. INTRODUCTION

Forensics is use of science and technology to investigate and establish facts in criminal and civil courts of law. Internet Forensics includes techniques and methodologies to collect , preserve and analyze digital data on the internet for investigation purposes.

It is a field of research and practice that has evolved as a result of increasing internet usage and the move of criminal activity. It is also argued that internet forensics evolved as a response to the hacker community.

Digital forensics focuses on developing evidence pertaining to digital files that relate to a computer document, email, text, digital photograph, software program, or other digital record which may be at issue in a legal case. It is a branch of forensic science to monitor, analyze and examine digital media or devices. The government and the corporate security firms dedicate significant resources to investigating the insider computer attacks that continue to plague organization a worldwide. Computer forensics process consist of Preparation, Acquisition , Preservation, Examination and analysis and Reporting[1] . Among these steps, Acquisition step is a procedure that investigators collect digital evidence and garauntee integrity of evidence at incident site. Accordingly , Acquisition step most significant step for efficient investigation.

Cyber Analyst performs the following tasks while working with digital evidences:

1. Identify: Any digital information or artifacts that can be used as evidence

Figure 1 : Shows processes to collect digital data

2. Collect, observe & preserve.
3. Analyze , identify and
4. Rebuild the evidence and verify the result every time [16].

In the document describe digital evidence collection process as follows:

1. Where is the evidence? List out the systems were involved in the incident and from which evidence will be collected.

2. Establish what is likely to be relevant and admissible. When in doubt err on the side of collecting too much rather than not enough.

3.For each system, obtain the relevant order of volatility.

4. Remove external avenues for change.

5. Following the order of volatility, collect the evidence with tools

6.Record the extent of the system's clock flow.
7. Question what else may be evidence as you work through the collection steps.
8.Document each step.

9. Don't forget the people involved. Make notes of who was there and what were
they doing, what they observed and how they reacted[2].

II. WHY WE NEED FOR DIGITAL FORENSICS?

Unauthorised access : This occurs when a user/hacker deliberately gets access into someone else's network either to monitor or data destruction purposes[3].

Denial of service attack : It involves sending of disproportionate demands or data to the victims server

beyond the limit that the server is capable to handle and hence causes the server to crash.

Virus ,Worms and Trojan attacks : viruses are basically programs that are attached to a file which then gets circulated to other files and gradually to other computers in the network.

Worms unlike viruses do not need a host for attachments they make copies themselves and do this repeatedly hence eating up all the memory of the computer.

III. ENABLED STRATEGIES TO COMPUTER FORENSICS

Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data, in which computer forensics is defined as "an art of science using sophisticated methods and procedures to preserve, identify, extract, document, examine, analyze and interpret digital evidence." This methodology and basic principles are briefly stated as follows:

(1) Acquire the evidence without altering or damaging the original.

(2) Authenticate the recovered evidence as being the same as the originally seized data.

(3) Analyze the data without modifying it.

The computer forensics operating strategies below provide effective investigation procedures for cyber crime cases.

1.Preserve the evidence : Digital evidence can be changed at any time by striking the keyboard or clicking the mouse. If the evidence is not handled properly, it could result in evidence damage, inaccessible data, inability to prove that the suspect committed the crime, or even a possibility of having no evidence. Therefore, the first step upon arrival at the scene of the cyber-crime is to properly control the scene and begin to record the time, carry out the investigation and collect all significant digital evidence.
Digital evidence is, by its very nature, fragile[5].

2. **Examine the evidence**: After obtaining the evidence from the scene, the next step is to analyze it. Common computer documents, pictures and sounds can be examined by many different software programs. However, the biggest problem is deleted documents, sometimes having been deleted by the suspect, which could be the most important evidence of all. Thus, slack space in the hard drive must also be scanned; this is one of the main reasons for using the bit-stream-copy method. A software tool must be used here to do string searching and document rebuilding.

(3) **Evidence analysis**: After examination and analysis of the evidence is to recover data from deleted files, files fragments, complete files. Tools used for this process are:

1. Digital intelligence's Drive spy
2. Access Data's FTK

Drive Spy is a powerful tool that recovers and analyses data on FAT 12, FAT 16, and FAT 32disks can search for altered files and keywords[4].

FTK is an easy to use GUI application for FAT 12, FAT 16, and FAT 32 and new technology file system (NTFS) disks

1. FTK Imager
2. Registry Viewer
3. Password Recovery Toolkit

IV. VARIOUS TECHNOLOGIES USED FOR FORENSICS : TOOLS

A ENCASE **:**

This tool is Used to Analyse digital Media. It performs the following function Data acquisition , file recovery, file parsing, and hard disk format recovery.
It is a network enabled incident response system which offers immediate and complete forensic analysis of volatile and static data on compromised servers and workstations anywhere on the network, without disrupting operations. It is used for the verification of the data after verifying it gives the hash value[6]. There are three
components of Encase tool which are discussed below:

1. The first of these components is the Examiner software This software is installed on a secure system where Investigations and audits are performed.

2. The second component is called SAFE, which stands for Secure Authentication of EnCase. SAFE is a server which is used to authenticate users, administer access rights, maintain logs of EnCase transactions, and provide for secure data transmission.

3. The final component is Servlet, an efficient component installed on network workstations and servers to establish connectivity between the Examiner, SAFE, and the networked workstations, servers, or services being investigated.

ENCASE WORKING SNAPSHOTS**:**

How to recover the hard disk format data with the help of Encase tool. In these snapshots the working of the tool is discussed below :

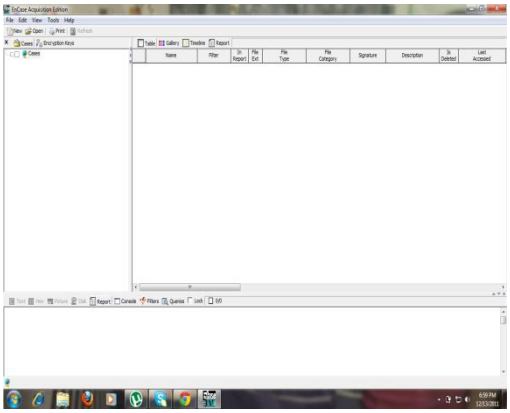

Figure:2 Interface of Encase tool

This is the main screen of the encase tool. In this we will first select the option new and then after selecting the case option and save this new case by giving the name as your choice.

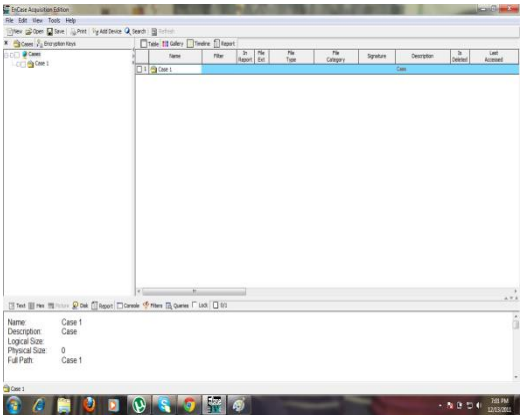

Figure:3 Interface working of tool

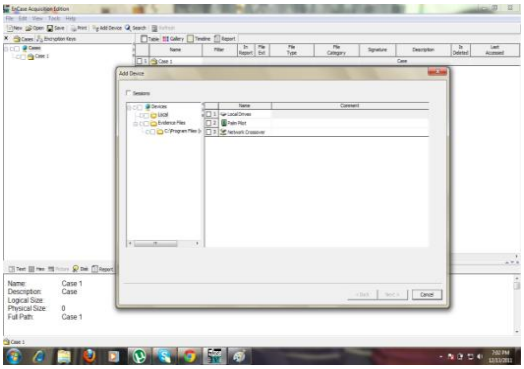

Figure:4 In this figure there is case folder presented by this screenshot .

Choose the drive from which you want to recover the data. After that click next and it will recover the deleted drive and the content of that hard drive successfully by this tool. These are the steps of Encase tool which we can use to recover hard disk deleted data.

B. FTK Explorer

- Developer : Access Data
- Operating System : Windows
- Type : Computer Forensics

Main purpose of this toolkit is to Locate deleted e-mails. Disk imaging program called FTK Imager.
FTK Imager saves an image of a hard disk in one file that may be later on reconstructed. Through this toolkit the recovery of password can be constructed. With the help of this tool from Winzip, WinRar, Gzip and compressed file data is automatically extracted.

FTK processes data faster than any other computer forensics solution. It delivers true distributed processing, allowing you to divide your processing across four workers. Furthermore, FTK is the only computer forensics solution to fully leverage multithreaded, multi-core computers. So while common forensics tools waste the potential of modern hardware solutions, FTK will fully utilize anything you throw at it[5].

- Faster more efficient processing
- Cancel/Pause/Resume functionality
- Better real-time processing status
- CPU resource throttling
- Email notification upon processing completion.

FTK delivers advanced memory and volatile analysis to aid forensic investigators and incident responders.

Memory Analysis:
Enumeration of all running Processes(Including those hidden)

1. DLL list
2. Network Sockets
3. Drivers loaded in memory
4. Device driver layering identification
5. Handles
6. Enumeration and hook detection of
7. SCT,IDT and IRP
8. Devices
9. Registry enumeration
10. VAD tree

Memory string search allows you to identify hits in memory and automatically map them back to a given process, DLL or piece of unallocated and dump the corresponding item[6].

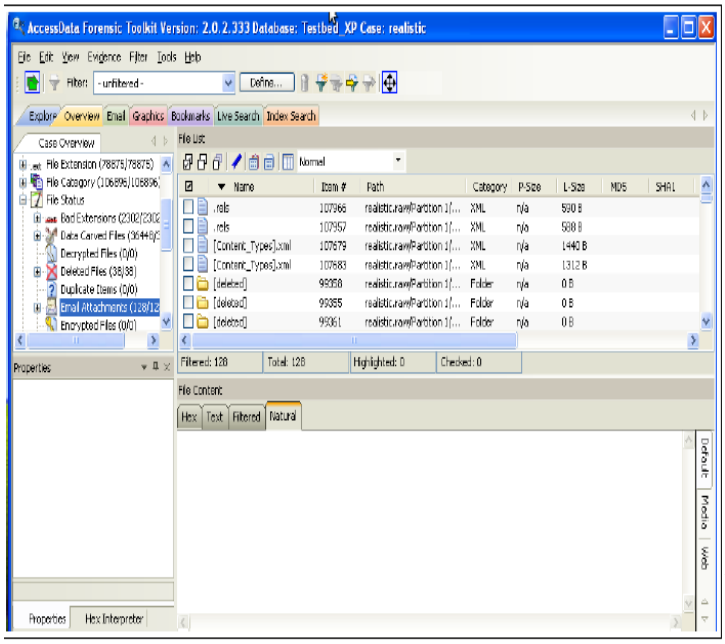

Figure:7 FTK interface

FTK runs in windows operating system and provides a very powerful tool set to acquire and examine electronic media.

C. SLEUTH KIT

Sleuth kit runs on windows and Unix system. It is the file system tool allow you to examine file systems of a suspect computer in a non-intrusive fashion. Because thetools do not rely on the operating system to process the file systems, deleted and hidden content is shown.

The Sleuth Kit is written in C and Perl . With these tools, you can identify where partitions are located and extract them so that they can be analyzed with file system analysis tools. The Sleuth Kit has been tested on[6]:

- Linux
- Mac OS X
- Windows (Visual Studio)

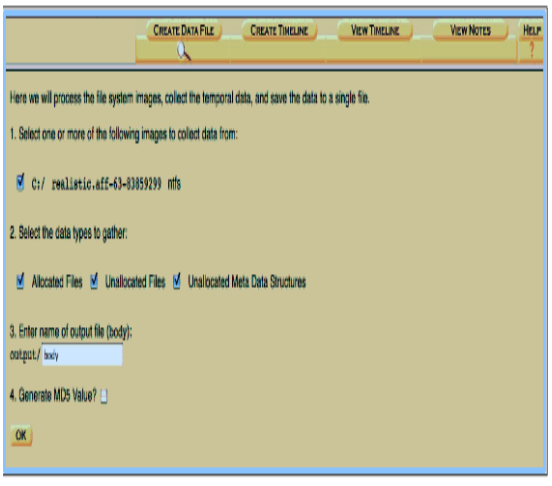

Figure:8 Interface of Sleuth kit/Autopsy browser

TSK is a collection command line tools that provides media management and forensics analysis functionality. The autopsy forensic browser is a GUI front end for the TSK product.

SLEUTH KIT CORE TOOLS

1. File System Layer
2. File Name Layer
3. Meta Data Layer
4. Data Unit Layer
5. Media Management
6. hfind
7. mactime
8. sorter

AUTOPSY BROWSER ADDS TO TSK

1. Dead Analysis
2. Live Analysis
3. Case Management
4. Even Sequencer
5. Notes
6. Image Integrity
7. Reports
8. Logging

V. CONCLUSION

Sleuth Kit along with Autopsy Browser has been selected as the best tool to implement for hands on training. The purpose of this paper is to introduce the aforementioned concepts in the cyber-crime investigations domain and the suitability of the underlying tools is studied Furthermore, a variety of digital forensics tools include digital evidence bag, automated logging – network tools in particular – which could be interfaced with the proposed system. By doing this, a more specialised system equipped with the appropriate semantics would allow further exploration of the efficiency and effectiveness of the tool.By comparing the features of these given tools in this paper in future we will give a new design and implementation framework of network forensics system for these tools with efficient results to collect the digital evidence.

VI. REFERENCES

[1] Kenneally, E.K., “The Internet is the Computer: the role of forensics in bridging the digital and physical divide”, Digital Investigation, Vol. 2, Issue 1, 2005, pp. 41-44.

[2] Chung-Huang Yang,Pei-Hua Yen ” Fast Deployment of Computer Forensics with USBs” 2010 International Conference on Broadband, Wireless Computing, Communication and Applications

[3] Hanan Hibshi Carnegie ,Timothy Vidas Carnegie ,Lorrie Cranor Carnegie Mellon University Pittsburgh, PA, USA "Usability of forensics tools: user study" 2011 Sixth International Conference on IT Security Incident Management and IT Forensics.

[4] Syed Naqvi, Gautier Dallons, Christophe "Applying Digital Forensics in the Future Internet Enterprise Systems – European SMEs' Perspective"(CETIC) Charleroi, Belgium 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering.

[5] Mario Hildebrandt, Stefan Kiltz and Jana Dittmann" A Common Scheme for Evaluation of Forensic Software" 2011 Sixth International Conference on IT Security Incident Management and IT Forensics.

[6] Guidance Software, EnCase. http://www.guidancesoftware.com

[7] Ashley Brinson*, Abigail Robinson, Marcus Rogers "A cyber forensics ontology: Creating a new approach to studying cyber forensics" d igital investigation 3 S (2 0 0 6) S 3 7 – S 4 3.

[8] Frank Y.W. Law, K.P. Chow, Michael Y.K. Kwan, Pierre K.Y. Lai "Consistency Issue on Live Systems Forensics".

[9] Yong-Dal Shin* "New Digital Forensics Investigation Procedure Model" Fourth International Conference on Computing and Advanced Information Management.

[10] Seokhee Lee, Hyunsang Kim, Sangjin Lee, "Digital evidence collection process in integrity and memory information gathering".

[11] Dan Manson, Anna Carlin, Steve Ramos, Alain Gyger, Matthew Kaufman, Jeremy Treichelt "Is the Open Way a Better Way?Digital Forensics using Open Source Tools" Proceedings of the 40th Hawaii International Conference on System Sciences – 2007".

[12] Marcus K. Rogers, Kate Seigfried" The future of computer forensics: a needs analysis survey" Received 21 November 2003; accepted 6 January 2004.

[13] Maria Karyda and Lilian Mitrou," Internet Forensics: Legal and Technical Issues" Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007).

[6] Simson L. Garfinkel," Automating Disk Forensic Processing with SleuthKit, XML and Python" 2009 Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering.

.