Design and Development of CLI for SleuthKit: A Cyber Forensics Framework

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Technology

In

Computer Science and Application

Submitted By
Dilpreet Singh Bajwa
651203002

Under the supervision of
Gurpal Singh Chhabra
Lecturer

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004
July-2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "Design and Development of CLI for SleuthKit: A Cyber Forensics Framework", in partial fulfillment of the requirements for the award of degree of Master of Technology in Computer Science and Application submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Gurpal Singh Chhabra and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Dilpreet Singh Bajwa

651203002

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Gurpal Singh Chhabra

Lecturer,
Computer Science &
Engineering Department.

Countersigned By:

(Dr. Deepak Garg)

Head

Computer Science and Engineering Department

Thapar University, Patiala

(Dr. S. S. Bhatia)

Dean (Academic Affairs)

Thapar University, Patiala

ACKNOWLEDGEMENT

Firstly, I would like to express my sincere gratitude to my guide Mr. Gurpal Singh Chhabra, Lecturer, Computer Science and Engineering Department for his immense help, guidance, stimulating suggestions and encouragement all the time with this thesis work. This work would have not been possible without his constant encouragement. He always provide motivating and enthusiastic work environment to work with; it was a great pleasure and learning experience to do this thesis work under his supervision. The successful completion of this thesis is a direct consequence of his moral and material support throughout this thesis.

I am equally grateful to Dr. Deepak Garg, Head, Computer Science and Engineering Department. My sincere thanks also goes to Dr. Maninder Singh, Associate Professor and Head, CITM for their insightful comments and encouragement. I am also very thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct-indirect help, cooperation and love which made my stay at Thapar University memorable.

Last but not the least, I would like to thank my family: my parents who bestowed ability and strength in me to complete this thesis work, brother, sister and my wife for supporting me spiritually throughout writing of this thesis and my life in general.

Dilpreet Singh Bajwa

(651203002)

ABSTRACT

With growing advancement in computer technology, the usage of computer and internet is increased day by day; in turn the crime related to computers is also increased gradually. So Computer forensics is a new field which incorporates procedure, tools and techniques to find the evidence against cyber criminals and prove it in court of law. The Computer forensics follow the investigation with some predefined general steps in any forensic investigation i.e. identification, preservation, extraction, interpretation, documentation and presentation.

There are many cyber forensic tools available for extraction, making copy of original media and for analysis. Tools are inherent part of any cyber forensic investigation and they must be based on proven methodology and techniques admissible under legal procedure. The cyber forensic tools broadly categorized as commercial and open source tools. Each has their own advantage and disadvantage. Open source tools are not so user friendly but as efficient as commercial tools and can be authenticated because their code is available, further we can expand it according to our requirement. The Sleuth Kit (TSK) is a popular open source cyber forensic tool constitutes a library and collection of command line tools that allow you to investigate disk images. These command line tools are difficult to use and you have to use each one independently. Your output is also not saved for future reference and analysis.

In this thesis work we created a command line common user interface for these command line tools of sleuthkit and automate the process. Some other tools for hash calculation are also incorporated in the system to make it more efficient. Guidance and help is provided while we are executing these command line tools further your output just not shown on screen, in addition it is saved for further analysis. Secondly your whole session and steps you follow as a cyber forensic expert is also saved for future reference.

LIST of FIGURES

Table of Contents

1. Introduction

From last few years, computer forensics plays a major role in prosecuting criminals. Cyber forensics has come to front as an important field to investigate cyber crimes, identification of cyber criminals and proves their crime in court. Before using any cyber forensic investigation techniques and tools, lots of cases of crime related to computer were left unsolved.

Due to integration of computer and communication technology and the fast development of digital technology have made significant changes to computer world. Firstly, the effectively and efficiently processing capability of computer made it most important tool for data processing. With the new technology storage capacity is also increased day by day. As a result, more and more data are processed and stored in computer systems. Secondly, the internet influence is so much in our daily life from simple email communication to banking transactions, online shopping, surfing, social networking etc. Gradually, our society is in a state of transformation toward a "virtual society," where people's daily activities, such as shopping, communication, and particularly sharing of information, can be accomplished without face-to-face contact with others. Although information technology has enabled world to flourish, it also becomes one of the major interested area for unscrupulous individuals to commit crime and escape apprehensions by law enforcement agencies.

1.1 Cyber Forensics:

Cyber forensics is defined as "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations
[1]".

1.2 Need of Cyber Forensics:

The crime related to computers is also increased gradually. So Computer forensics is a new field which incorporates procedure, tools and techniques to find the evidence against cyber criminals and prove it in court of law. The Computer forensics follow the investigation with some predefined general steps in any forensic investigation i.e. identification, preservation, extraction, interpretation, documentation and presentation.

The identification and preservation refers to identify the digital devices or computer related to crime and preserves the original media or data before analysis. Documentation refers to record everything from start to end during investigation like, what tools, techniques, procedure and steps which are also legally admissible follow during investigation, it will be helpful and necessary while presenting case in court. Presentation refers to present your evidence against culprit in court of law and prove or relate the evidence with culprit under legal procedure. Extraction and interpretation are two very important steps which we used to extract or collect evidence from the copy of media or digital device under consideration and interpretation refers to analyze and relate the evidence to crime and culprit, so that it can be prove in court.

1.3 Main goal of Cyber forensics is:

- Identification of criminal activities and unauthorized access.
- Acquiring, storing, preserving, processing and analysing the evidences and present it under legal procedure.
- To use the experience and information gained during cyber forensic investigation to protect computer systems and networks and also to prosecute culprits [2].

To achieve these goals digital Investigations must be perform in a structured and standardized manner so that the data collected and details to be produce as evidence in a court during criminal prosecution of the culprit [2]. There are many reasons why an cyber forensic investigation might not lead to success, but the most important one is

non- availability of right set of tools and lack of preparation. The agencies investigating the crime often deficient in carrying right tools, techniques and correct skill set. Thus, computer forensics needs to focus on consistency and cohesion to the field of acquiring and interpreting evidences collect from a digital device at a crime scene. Specifically, the gathering of evidence from a computer is takes place in such a way that the original evidence is not compromised.

1.4 Steps in Cyber Forensic Investigation:

It is observed that cyber crime investigation & forensics is the biggest challenge for law enforcement agencies in this 21st century. Digital Forensics or Cyber Forensics has grown to an important part of many investigations related to cyber crime.

Cyber Forensics generally follows these steps:

- Identification
- Preservation
- Extraction
- Interpretation
- Documentation and
- Presentation of computer data in such a way that, it can be legally admissible.

Identification

In the starting phase, the identification of containers and devices which are possible containers of computer crime evidences is very important. This phase take care of identifying devices, such as hard drives, floppy disks, and log files to name a few which might be contain crucial evidence. Understand that a computer or hard drive itself is not evidence - it is a possible container of evidence.

Preservation

Before performing a computer forensics analysis, we must take care to preserve the original media and data. Typically this involves making a forensic image or forensic copy of the original media, and conducting our analysis on the copy versus the original.

Extraction

Any information/data which is of our interest and can be consider as evidence relevant to the situation at hand will need to be extracted from the working copy media and then must saved to another form of media as well as printed out for further analysis.

Interpretation

Some of the tools available make forensic analysis extremely easy but being able to find evidence is one thing and interpret it properly and relate it to crime is another story. This is the most important part as we have to analyze and interpret the evidence properly so that it can be proved in the court of law Results from any tool should always be thoroughly checked by someone expert in the underlying technology. Differences in interpretation may also arise and was due to the experience, tools used and education levels of the experts.

Documentation

Documentation needs to be done from beginning till end. This includes what is commonly referred to as a **chain of custody** form, as well as documentation pertinent to what cyber forensic expert do during your analysis. When involved in a situation where conducting a computer forensics analysis, it is recommended that keep in mind that the case or situation is going to end up in court. If proper documentation is done and recorded the steps follow for analysis than it will be great help to prove and authenticate the work done during analysis. Take it in to consideration that analyst will be questioned on every aspect of the case, and everything he do.

Presentation

Final findings and reports needs to be based on proven techniques, tools and methodology, and any other competent forensic examiner should be able to duplicate and reproduce the same results. Analyst may have to prove or relate his results and opinions in a court of law or any other type of legal or administrative proceeding.

An important legal challenge faces cyber- investigators: not only must they find incriminating evidence they must also produce it in a lawful manner. Otherwise, the

evidence will not be admissible in court. One of the most important aspects of introducing computer forensic evidence in a court or trial is the **Chain of Custody** by assuring court that the computer or peripheral such as an external hard drive, flash drive or other electronic media device has not been tampered with, the computer forensic professional must keep a detailed log of how the device or devices were obtained and who may have had access to the files in question during the trial.

1.4 Role of Tools in Cyber Forensic Investigation

Cyber Forensics tools are now used on a daily basis by examiners and analysts within local, state and National law enforcement agencies. Separate Cyber forensic cells are also established by the government for research and analysis of cyber related crime and evidences. Several private organizations are also contributing in developing software for cyber forensics from extraction of evidence to analysis of digital devices. Developments in forensic research, tools, and process over the last decade have been very successful and many government and private agencies are relying on it. Moreover, there seems to be a widespread belief, that advanced tools and skillful practitioners can extract actionable information from practically any device that a government, private agency, or even a skillful individual might encounter.

So right kind of tool is in your hand to create a best sculpture, similarly right kind of tools are required to properly investigate the case. Several commercial and open source tools are available for cyber forensics investigation but not always a single software or tool is enough for all types of cyber crimes. You need a different set of tools for different type of investigation depending upon the digital devices and type of crime.

1.5 Commercial Vs Open Source Forensics Tools:

From the above discussion it is clear that Interpretation/Analysis and documentation are two important steps to find the evidence and to prove it in court of law. For analysis of digital devices several commercial and open source forensic tools are

available. Commercial tools are software products provided by different organizations. Law enforcement agencies are using these tools for cyber forensics. Education institutes which running course in cyber forensics also use these proprietary tools. These commercial tools are very expensive and can be purchased on license for particular duration. After expiry you again have to renew the license. They are easy to use and proper documentation and support is available for these commercial tools usage.

On the other hand open source cyber forensic tools are also available which are also equally efficient. But these tools are difficult to use and not proper documentation and support is available for these open source tools. But there are several benefits attached in using open source cyber forensic tools: You don't have to purchase them, No license fee is required, and you can use them anywhere i.e outside the licensed lab, for students, educationist and the organizations who don't afford commercial tools, the open source tools are the best bet. Further the code is available for these open source forensic tools, you can optimize and modify them according to your requirement, you can also understand the internal working and code and how results are produced which is not possible with commercial tools. You authenticate in court of law that particular tool is work in this way and using this algorithm and produce the right result.

As many commercial tools are available with proper manual, guidance and support but you have to pay a heavy price for it. Secondly not a single tool is enough so you have to pay more. In the scenario to learn, to experiment, to understand internal working and code, open source cyber forensic tools are the best bet. Open source tools with proper combination also provide all features provide by any commercial tool. The disadvantage of using an open source tools is lack of support and proper documentation. It is also finding difficult to use these tools. The Sleuth Kit (TSK) is an open source cyber forensic tool constitutes a library and collection of command line tools that helps in investigating disk images. These command line tools are difficult to use and you have to use each one independently. Your output is also not saved for future reference and analysis.

1.6 Slight Overview of Thesis Work:

In the thesis work we created a common interface for some of these command line tools and automate the process. Some other tools for hash calculation are also incorporated in the system to make it more efficient. Guidance and help is provided while we are executing these command line tools further your output just not shown on screen, in addition it saves in a file for further analysis. Secondly your whole session and steps you follow as a cyber forensic expert is also saved. Figure: 1.1 given below helps to understand the idea.

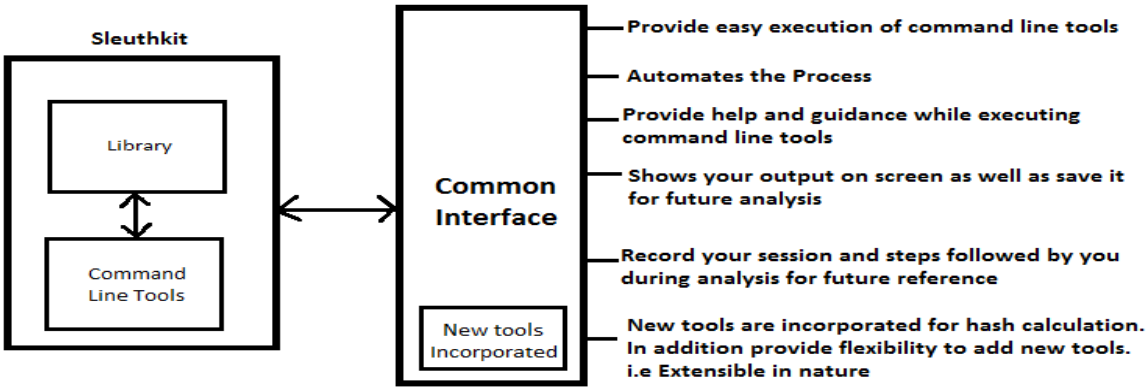


Figure: 1.1: Higher Level Model of CUI for Sleuthkit

So, the interface created provides easy execution of command line tools, automate the process, saves your output, record your session, and provide flexibility to add new tools other than TSK. Thus making environment more user friendly, optimize it and make it more useful at user end.

2. Literature Review

Whenever we have to take some problem in hand and also want to find its solution, its background knowledge is very necessary. As much you know from the basics to the current trends of the problem in hand, more easily you can resolve and find the better solution and also you can emphasize on the significance of your work. So for all this we first have to do a literature survey. As much time you spent on literature survey, less time we have to spend on resolving the problem. Here in this section we mention the main papers, publications and conference proceedings which we go through to complete this work.

2.1 Role of Cyber Law and Survey of Cyber Crime in India:

"A Survey of Cyber Crime in India" In this paper the author discusses various aspects of cybercrime and case studies in support of the same. It is concluded that cybercrime is a crucial threat and disastrous in comparison to the other conventional crimes and it also depend upon geographical boundaries and presence of criminal on crime site. In the current scenario of technology advancement which is strictly dependent on computers, every nation and the national will have knowledge of cybercrime, criminal psychology and threats or associated with it[3].

"Role of Cyber Law and its Usefulness in Indian IT Industry" This paper discuss cyber crime is not limited to geographical space, group and time of occurrence. Now with time more and more people are using internet so more tendency to commit and become victim of cyber crime. Around 500 million people using the internet and this figure gradually increasing with time. Until recently, IT professional and even law enforcement officers lacked in knowledge about cyber criminal behavior and activities and how to counter them. They don't have adequate tools, techniques, procedures and laws to prove the crime and put the criminals behind bars. Old laws are not so powerful and not fit the type of crimes happening in today's world and even new ones are not up to the mark in punishing the culprits. Furthermore, there was certain amount of lack of coordination between two maint players in countering cyber

criminals: computer professional or experts and law enforcement agencies but the close interaction and operation is necessary between these two players to tackle cyber crime because law enforcement agencies understands the criminal mind set and also they are responsible for making law and policies to counter cyber crime, whereas computer professional or experts have knowledge of computers, computer networks, information gathering and analysis of digital devices. So both must be work in tandem to counter cyber criminals[4].

2.2 Research and Challenges in Digital Forensics:

"A Road Map for Digital Forensic Research" The aim of the workshop was to constitute a forum for a recently born community of researchers, practitioners and academics so that they can share their experience and knowledge on Digital forensics Science. The targeted audience is law enforcement agencies, civilian and military who use forensic procedure, technique and tools to gather evidences against criminal from digital devices. This workshop is an initiated effort to bring together the best persons and practices in the field of digital forensics [1].

"Challenges to Digital Forensics: A Survey of Researchers & Practitioners Attitudes and Opinions" In this paper, the author focuses on Digital forensics and consider it is really important to investigate computer related and cyber crimes. Research is being undertaken and many tools are also exists, many questions regarding domain future also exists simultaneously. Author specifies that literature regarding challenges exist within domain. However, not much effort is focused upon getting knowledge about reality of these challenges. This paper focus on research that try to quantify, prioritize and identify these real challenges so that in future we focus on real domain. To overcome these challenges author proposed that there is need of improving communication between practitioners and researchers and also to develop methodology to identify and gather significant data [5].

"Digital Forensics Best Practices and Managerial Implications" This paper discusses main points to be followed in analysis of digital evidences and cyber forensic investigation process. It also focuses on best practices followed in forensics

investigation process**.** Author states that the reliability and authentication of evidence acquired is also depend on the cyber forensic tools used during investigation. If the tools used for investigation are not reliable and authenticate the collected evidence, the results are also not considered reliable and authentic [2].

"Framework for a Digital Forensic Investigation" The main aim of paper is to create a proper guideline of what steps must be followed in a cyber forensic Investigation. According to paper, the author wants to specify clearly a framework which is used in cyber forensic investigation process. Overview taken from proposed frameworks prescribed previously disclose that a many phases or steps overlapped with each other and the main difference resides in terminology. New steps are not added to the proposed framework instead similar tasks were grouped in to single stage. This framework is extensible and uses to incorporate any number of additional phases needs in the future[6].

"Digital forensics research: The next 10 years", this paper states that good days of computer forensics is rapidly vanishing. In deficiency of a standard strategy for research efforts, research work of forensics will fall lack in getting pace according to market trend, tools will get obsolete with time and computer professional, analyst, experts and forensics products will not rely on the forensic analysis results. Author gives overview of current forensic research directions and focus on modular and standardized approaches for forensic processing and date representation. This paper provides details of requirement to make research of digital forensics more efficient by creating new abstractions. With considerable attention the cyber forensics research community can simultaneously lower costs of development and quality of research efforts can be improved [7].

2.3 Tools and Techniques for Digital Forensics:

"Computer Forensic First Responder Tools" This paper provides an important although limited details of the nature of computer forensic first responder tools. Author shown that open source tools may also more concisely and comprehensively meet the guidelines and requirements than would closed source tools [8].

“The Need to Adopt Agile Methodology in the Development of Cyber Forensics Tools” As we know that cyber forensics is the process of identification, gathering and analysis of digital devices. This paper states that it is challenging to develop cyber forensics tools in scenario of rapidly change in digital device format and new techniques to commit crime. If the traditional development method is followed and time for development is long than there is chance that tool will be obsolete when released. So agile development methods can be used by development teams to manage change and quick release of tools [9].

“Hacktivism Trends, Digital Forensic Tools and Challenges: A Survey” states that there is always a race between the development of forensics and anti forensics tools. The speed of the criminals making anti forensic tools is similar to speed of the ethical hackers which makes the process of gathering of evidences difficult from digital devices. The main difficulty being faced by the digital forensics is the lack of cyber policy and cyber laws which makes very easy for criminals to commit crime without any fear of being caught. While analyzing devices for digital devices following things take in to consideration: During examination of any evidence, also make chain of custody which contains proper documented reports regarding hardware examined and the tools, techniques , procedure followed and the results found during investigation[10].

“Hash-algorithms Output for Digital Evidence in Computer Forensics” This paper states that Hash-algorithm is, basically used to check message integrity. One of its applications in the area of computer forensics is to provide authentication of originality for evidence collected from digital device.. In this paper, the author reviews the property of hash calculation and discusses the related computer forensics

application to increase the reliability of digital evidence while investigating cyber crime. The MD5 and SHA-1algorithms for hash calculation has been applied to many areas due to quickness and reliability they provide. The researchers conclude that SHA-1 many times weaker than thought. This result cannot have quick effect on security of cyber space, but this point is really important from information security

point of view. The evidence of computer crime, its originality and completeness is crucial to prove the crime under law. Author analyzes the basic hash property and explains to which extent it is secure. The cracking of MD5 and SHA-1 may not have instant effect in the area of computer forensics. Therefore, we can use available substitute algorithms like SHA-224, SHA-256, SHA-384, and SHA-512 [11].

"Developing Forensic Computing Tools and Techniques within a holistic framework: an Australian Approach" This paper presents work-in-progress in the development of conceptual framework within which to accommodate diverse approaches to forensic computing investigations. By use of this framework a suite of cyber forensic computing tools and investigative procedures is produced to help police and intelligence agencies. These tools provide help in detection of online computer misuse and provide technical also. The accompanying integrated procedures will take care that digital evidence is acquired methodologically and is presented in a manner that is legally admissible [12].

"Integrating Forensic Investigation Methodology into e-Discovery" The paper has two purposes; to give introduction on the e-Discovery process for analysts and also to provide information regarding forensic investigative methodology to said process. This paper proposes that forensic analyst and legal professionals can take advantage when they combine their processes; forensic tools and techniques have been used in the collection, analysis and presentation of evidence in the legal system for years. This paper will also provide information regarding how the work and scope of a forensic expert during the e-Discovery process different from a typical forensic investigation.

2.4 Open Source Forensic Software

"Is the Open Way a Better Way? Digital Forensics uses Open Source Tools" This paper discusses the tools used in computer forensics; it compares an open source tool with two commercial tools, and in academic environment advantages and disadvantages of all three tools are also compared. It suggests that we can also consider open source forensic tools other than commercial tools for forensic

investigation. Open source tools are most widely used tools in computer forensics. While one tool like Sleuth kit/Autopsy is very good at performing disk analysis, it is of great importance to be able to copy the steps taken with it in obtaining evidence with another forensic program because credibility and authentication cannot be built by only one program. It is important that both open and closed source tools works in collaboration to validate each other's results.. This means that closed source users must also try other open source tools to validate their results. If an open source tool produces the similar evidence as a closed source tool, then the open source tool's code which is available freely can be analyzed and proved that it works correctly. Therefore the closed source tool's source code can also be assumed that it works correctly because of similar results produce by both [13].

"Preliminary Acquisition Information Gathering on Computer Data Storage: Open Source Software (OSS) vs. FIRST DiskImager" This paper states that acquisition of data and its analysis is important in cyber forensics investigation. The output from this process will help cyber forensics experts to obtain accurate specific information on device partitions, hidden partition metadata, unknown and deleted file systems and data sectors. Generally, computer forensics investigator will be using open source software (OSS) such as DD, FDISK, DISKTYPE and SLEUTHKITS to capture this daunting process but using these tools is quite difficult for most forensic investigators. Poor result documentations, confusing analysis and not user friendly are some of weakness faced by experts. This paper discussed the experiment results produced by the FIRST DiskImager and the adopted OSS tools when conducting acquisition and information gathering [14].

"Building Open and Scalable Digital Forensic Tools" The main part of this paper is to analyze current approaches used for building integrated digital forensic tools and to propose alternatives. The author showed that current approaches, both commercial and open source tools currently available, are not data and cost scalable in the face of fast data growth; they does not support extensibility much to incorporate new tools and standards and also have inadequate user interface. Specifically, our analysis leads us to the following conclusions: On conclude, the author believe that it cannot be possible to build all of its tools from the ground up. Instead, it must gain leverage by opportunistically aligning itself with technologies that are being openly developed for

the Web by big technology providers. This allows for reusing developed solutions and focusing most of the development effort on forensic-specific problems [15].

"Using Open Source for Forensic Purposes" This paper states that for acquisition and analysis of digital devices similar results can be shown by open source tools in the broad field of analysis of digital evidence, There are huge varieties of open source tools available which are characterized by multiple specifications, most of the tools are certified and validated and are in no way less reliable and efficient than commercial or proprietary tools. Commercial tools are more user friendly and easy to use but it is not always possible to evaluate their reliability and also licensing cost is very high. So open source tools provides a good alternative [16].

2.5 Open Source Forensic Software: The SleuthKit :

"Automating Disk Forensic Processing with SleuthKit, XML and Python" The author states that in recent years many important applications for computer forensic tools have been found that extend from traditional boundaries of law enforcement and e-discovery. Many research are interested to work on disks, USBs and other digital devices without go in to much details about disk image formats and partitions and other things. Due to such needs, the standard approach is to write programs that run SleuthKit command line tools in background and process the results. But SleuthKit's interface is not well suited to this task, so working applications using sleuthkit requires good forensic knowledge. To assist users who wanted to create programs that can automatically process disk images, author has developed a methodology for automating the processing of forensic data using Sleuthkit, XML and python [17].

"Framework for the Design of Web-based learning for Digital Forensics Labs" The author discusses that many open source forensic software are available in the market. Teaching a student or learner, how to use every tool is impractical. However, the students must get the thorough knowledge and basics so that it builds a strong foundation for them. The author had identified several tools that are user friendly. Computer Forensics has one main goal and that is acquired or extracts evidence from digital devices, including computers, cell phones, PDA's etc. Forensic tools are

available there to safely assist in the process. One of the tool that may use for learning purpose is Sleuthkit, It create timeline of file activity , Sorts files based on their file type and performs extension checking and hash database lookups , Analyze image partition structures process data units at content location brief description [18].

"Sleuthkit:http://www.sleuthkit.org/sleuthkit/docs.php" As mentioned above that open source cyber forensic tools are also popular for cyber forensic investigation specially in education and research community and they are as efficient as commercial tools but these open source forensic tools has some limitation also like they are difficult to use, don't have proper documentation and support. In our problem we had taken "sleuthkit" open source forensic tool in to consideration. The reason to choose this tool is that it is very popular among cyber crime experts and it has vast potential to expand its library, further its command line tools are efficient to conduct disk and volume analysis when used properly and in right way.

Following are the main Command Line Tools available in Sleuthkit[22]:

- **fsstat:** Shows file system details and statistics including layout, sizes, and labels.
- **ffind:** Finds allocated and unallocated file names that point to a given meta data structure.
- **fls:** Lists allocated and deleted file names in a directory.
- **icat:** Extracts the data units of a file, which is specified by its meta data address (instead of the file name).
- **ifind:** Finds the meta data structure that has a given file name pointing to it or the meta data structure that points to a given data unit.
- **ils:** Lists the meta data structures and their contents in a pipe delimited format.
- **istat:** Displays the statistics and details about a given meta data structure in an easy to read format.
- **blkcat:** Extracts the contents of a given data unit.
- **blkls:** Lists the details about data units and can extract the unallocated space of the file system.

- **blkstat:** Displays the statistics about a given data unit in an easy to read format.
- **blkcalc**: Calculates where data in the unallocated space image (from blkls) exists in the original image. This is used when evidence is found in unallocated space.
- **jcat**: Display the contents of a specific journal block.
- **jls**: List the entries in the file system journal.
- **mmls**: Displays the layout of a disk, including the unallocated spaces.
- **mmstat**: Display details about a volume system (typically only the type).
- **mmcat**: Extracts the contents of a specific volume to STDOUT.
- **img_stat:** tool will show the details of the image format
- **img_cat:** This tool will show the raw contents of an image file.
- **hfind:** Uses a binary sort algorithm to lookup hashes in the NIST NSRL, Hashkeeper, and custom hash databases created by md5sum.
- **mactime:** Takes input from the fls and ils tools to create a timeline of file activity.
- **sorter:** Sorts files based on their file type and performs extension checking and hash database lookups.
- **sigfind:** Searches for a binary value at a given offset. Useful for recovering lost data structures.

These tools perform some specific function and we can execute them independently. We can also use many arguments with these command line tools which make their function more specific. So sleuthkit contains rich set of these command line tools which are used for disk analysis.

So above we discussed literature review studied or followed, Firstly we understand what is cyber forensics and what are different cyber types of cyber forensics exists like Digital Forensics, Computer forensics, Network Forensics and Mobile Forensics. From these forensics we choose to work on Computer forensics and specifically disk and volume analysis. So we studied papers and books related to these, There are several Commercial and Open Source forensic tools are available for disk and volume system analysis but commercial tools are available at very high cost second their code is not available to understand their working. So we choose to work on open source

software. Sleuthkit is the open source software which is very popular for collection of its command line tools but the problem we observed with these command line tools is that it is very difficult to use them without any help. So we try to automate the process of execution of these command line tools and also provide flexibility in our frame work to incorporate new tools other than sleuthkit.

Although more than mentioned paper and sources are studied to clear background knowledge and to get direction of work but the mentioned papers are more suitable in reference to thesis work that's why only they are mentioned.

Problem Statement:

As it is clear from above discussion that open source tools provide a good alternative for computer forensics. The Sleuthkit (TSK) is open source cyber forensic software and constitutes a C library and collection of command line tools for file and volume system forensic analysis. The file system tools are used to examine file systems of a suspect computer. It works on both Windows and Unix platform. The volume system (media management) tools are used to examine the layout of disks and other media. The Sleuth Kit supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT disks. With these tools, you can identify where partitions are located and extract them so that they can be analyzed with file system analysis tools. When performing a complete analysis of a system, we all know that command line tools can become tedious to use and you must know how to use them. The basic idea behind working of sleuthkit command line tools is given below in Figure 2.1:

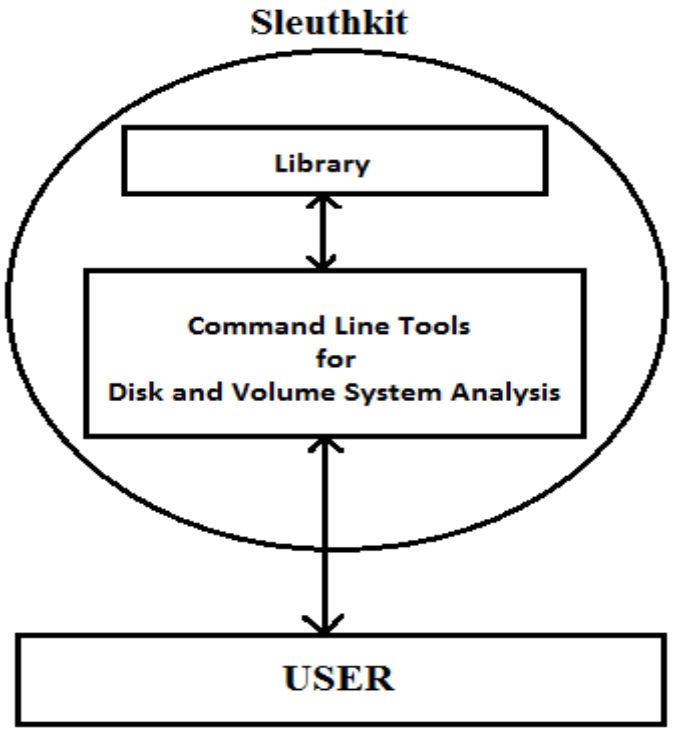


Figure: 3.1: User Interaction Scenario with Sleuthkit

The user can execute command line tools directly and perform disk and volume system analysis.

We observed following problems while using these command line tools:

- Each one can only be executed independently.
- Lack of help and support while executing these command line tools.
- Output is shown on screen only, not saved for further analysis.
- No case management is available or facility for session record while executing these command line tools.
- Not a common interface available for all command line tools to show these are the tools available to use and you can select one of them according to your requirement at particular time.
- We can only use command line tools available with TSK.

The problem is that it is difficult to use these command line tools directly without any prior knowledge. Secondly you have to execute each command line tool independently and also the output is shown on terminal only, further what steps you are performing in sequence is not recorded or saved for future reference and analysis. In our thesis work we optimize this direct interaction of user with sleuthkit and provide a common user interface to access these command line tools in easy way and automate the process. The output is saved for further analysis and whole session is also recorded for future reference. You may also incorporate new tools also other than TSK in the framework. Around 700- 800 lines of code is written in Linux to provide required functionality.

4. Design and Implementation

4.1 Proposed Design

After considering the points mentioned in problem statement, we proposed and develop a common user interface which overcome all above limitations and provide us following benefits:

- Commands can be executed in collaboration.
- While you are executing command, at each step you get the help.
- Output is not only shown on screen but it can also save for later analysis.
- Case Management is available, you can record your whole session i.e what commands and what steps you follow while doing analysis.
- Common interface is provided for command line tools.
- We can also incorporate other tools in to the system and use them.

According to our proposed solution, we design a framework that is used to access sleuthkit command line tools through a common interface and we can also add more tools which are not part of sleuthkit. This framework is useful in sense as it is simple provides user help at each step while executing the tools and automates the process. Secondly the results are saved in different files corresponding to each tool you execute and you can see them later on for analysis and other purposes. One step ahead this framework provides you case management that is your whole session records for future reference and documentation. It records what steps you follow and commands you execute and their corresponding output for a complete session i.e. until you exit from the system.

Figure 4.1 given on next page shows block diagram of our proposed Framework.

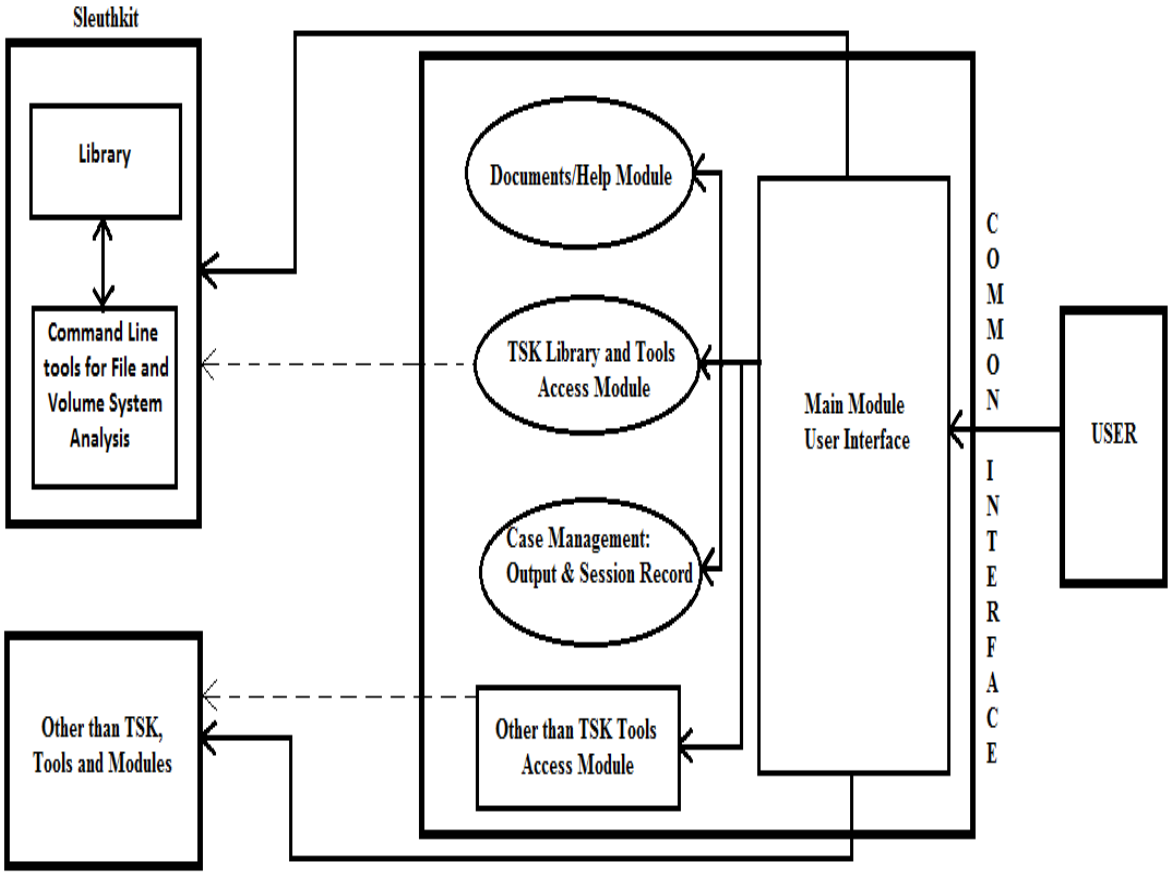


Figure 4.1: Block Diagram of proposed CLI for SleuthKit

4.2 Implementation:

For implementation of our proposed Command Line Common User Interface for Sleuthkit we use Shell Programming Language of Linux. The reason to choose this scripting language is that firstly sleuthkit command line tools are meant to execute on Linux platform, Secondly it is easy to use and implement shell programming, it has vast variety of features and commands of Linux further we can use powerful features like pipeline, redirection, regular expression and combination of Linux commands which makes it unmatchable specifically for purpose like cyber or computer forensics..

Currently we implement following command line tools of sleuthkit and in future all command line tools present in sleuthkit will be implemented:

- **img_stat**
- **mmls**
- **mmstat**

- **fsstat**
- **fls**

In addition to these tools we also incorporate tools used for Hash Calculation and these tools are not part of sleuthkit. We can also calculate SHA-224, SHA-256, SHA-384 and SHA-512 hash values corresponding to some file or image in addition to MD5 and SHA-1. The interface further provides you flexibility to add more tools when required.

The Interface also provides you a very important functionality which is necessary from point of view of cyber forensic investigation. It provides you complete case management which help in documentation of your case investigation automatically and also in future reference and analysis. For a complete session i.e. from invoking of this common interface up to exiting, it records everything from steps you follow to commands you execute, all are saved. Separately when you execute commands their output is also saved in different file corresponding to each command.

It also makes execution of these commands easy for a beginner as well as professional by providing help and guidance at each step. You can also get complete description of tools and their various arguments before using them or while using them. So it provides a user friendly environment for users.

Broadly we divide our interface in to five modules:

First module (Main Module) is main module corresponding to this module a script file main.sh is used and all other modules are directly connected to it and it is also responsible for start and providing first interface to user.

Second module (TSK Library and Tool Access Module) is very important; it is used to provide access to user for command line tools of sleuthkit through the interface. It provides you option to choose between available list of tools, you want to use at particular time. Corresponding to each command line tool there is separate script file to access it. For e.g if you want to use img_stat tool of sleuthkit then corresponding to it script file imgstat.sh is available which works in background to help in accessing the tool and providing the options which you can use with the

command. it also responsible for providing help during execution in collaboration with Document/Help Module.

Third Module (Document/Help Module) is responsible for providing documentation and complete description regarding tools available for use when required. It also provide help and description regarding various arguments/options you can use with command line tools while executing the tool in collaboration with corresponding script file of tool.

Fourth Module (Session Record Module) is responsible for case management. It records your complete session and saved it for future reference. It also saves output of all command line tools you used in separate file corresponding to each tool. It works simultaneously with scripting file available for each tool.

Fifth Module (Other Than TSK Access Module) is used to provide access to user for tools (which are not part of TSK) through the interface. It provides you option to choose between available list of tools, you want to use at particular time. Corresponding to each command line tool there is separate script file to access it. It provides you flexibility to add new tools and access to them. This module is expandable and you can incorporate new tools when required.

So it is clear from our module description that how our modules in interface work together and specifically what they do. Figure 4.2 given on next page shows interaction and integration of these modules:

Flowchart Working is described as: Now we show how control of out framework flows from start to end with the help of flowchart diagram Figure: 4.3.1 to 4.3.4 which is helpful in getting to know about the flow of control and working of our interface in depth.

In actual the flowchart from Figure 4.3.1 to 4.3.4 is complete one flow chart for whole interface. So all are connected with each other at different point and can be consider as a single flowchart while observing flow of our interface.

Flowchart is divided in to four parts, First part shown in Figure 4.3.1 shows flow of our main module and what options it provide at start. It has main three option. Option

1 is choose to get Help and Description about all Sleuthkit command line tools. 2nd option is the main option chosen by user to see list of all available tools under this frame work and from there it choose to execute them. 3rd option is used to exit from the interface. Whenever you choose to exit during session at any stage, the whole session is saved for future analysis and reference.

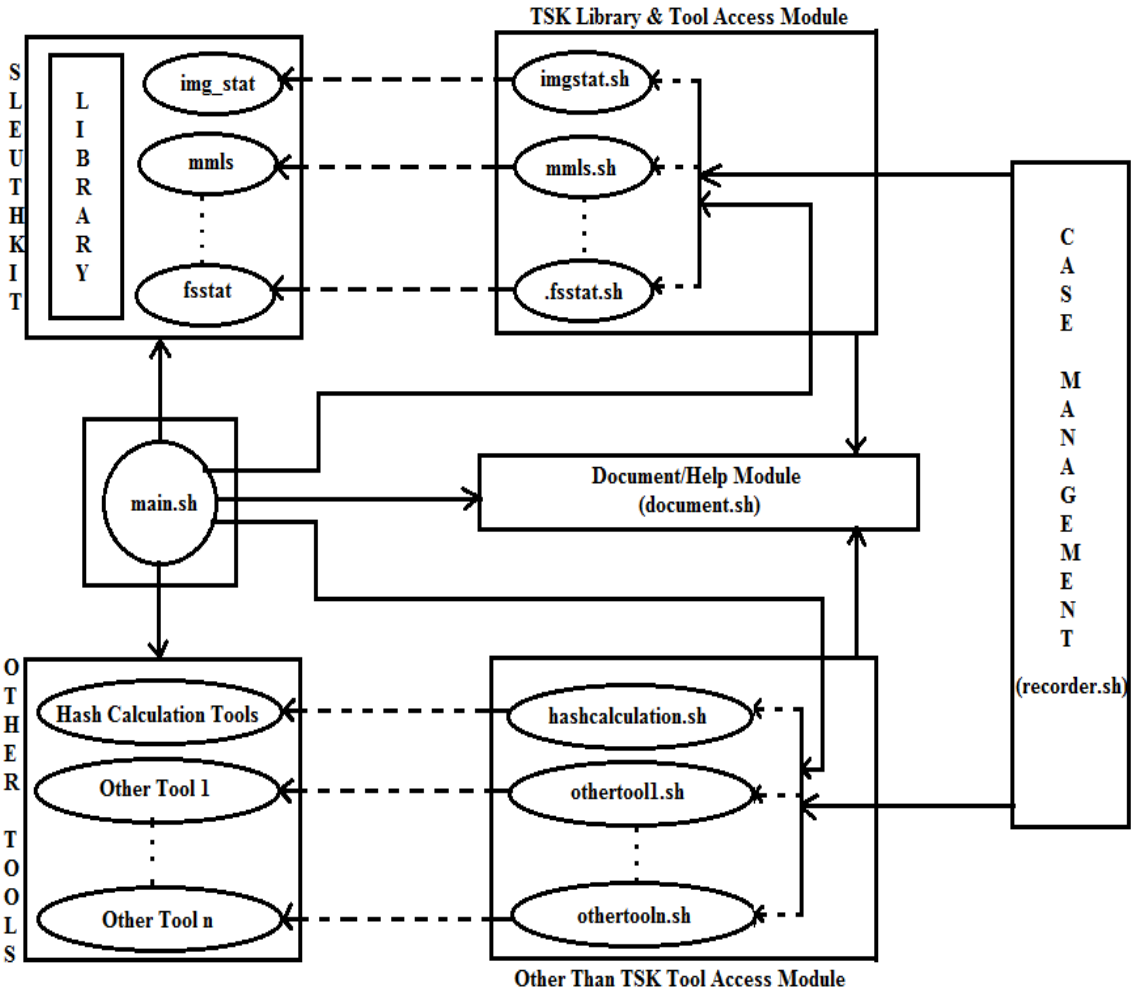


Figure 4.2: Interaction and Integration of Main Script Modules

Second part and Third part is demonstrated in Figure 4.3.2 and Figure 4.3.3 which shows the most important part of our frame work i.e. selection of tool of your choice and their execution. When you select option 2 from main page interface i.e. you choose to use the tools then the system follow the control mention in this flowchart. Before moving forward it asks you for case name. Your whole session now records under this case name. After providing case name, the interface shows all the tools

which are available for use, you can select one if want to run otherwise also select exit. When you choose any tool then options corresponding to selected tool are shown. Corresponding to each command line tool of sleutkit these options are shown. The options are if you want to run the tool then select 1, 2nd option is also important here as it provides you to build your command line and directly run it on command prompt, if you select 3rd option then you get complete description about the tool and various arguments you can use with this tool to make it more specific,4th option take one step back to see again list of available tools and from there you again continue to choose same or any other tool, 5th option takes you to home screen and 6th takes to exit point. If the user select wrong option than error checking mechanism display message regarding wrong option and again takes you to the same screen to select the right option.

If you select to choose run any command line tool then first it asks about image full path i.e the image on which you want to apply forensic investigation and also arguments are shown which can be used with the tool and also asking whether you want to use one of these argument or not. If user select no than in that case tool is run with default arguments otherwise if user select yes than interface asks for the argument user want to use and prepare command line according to that and execute the tool. When you execute some command, the output is shown on screen and also message is displayed that your output is also saved and storage location is also specified.

If user select option 6 in Figure 4.3.2, It shows all available tools which are not part of sleuthkit but incorporated in to framework to provide more functionality during cyber forensic investigation. Now your control goes to Figure 4.3.4, Currently Hash calculation tools are incorporated in to framework so they are shown with corresponding options. Either you choose to use tools for hash calculation or move back to see list of all tools or select 3rd option to go back to home or choose 4th option to exit. If user can't choose the options given above then error handling mechanism display message wrong option chosen and again prompt to same screen so that user choose the right option.

If in Figure 4.3.4 user selects option 1 and chooses to run hash calculation tools then interface shows all available options of hash calculation from md5 to sha-512. User

can either select one of the hash calculation tool or choose option 6 to apply all hash calculation algorithm and calculate all hash values but before executing one or all tools system prompts user for name of file or image for which user wants to calculate hash. User can also select option 7 which takes user back to see all available tools again or user can also choose 8^{th} and 9^{th} option for moving back to home or to exit. If user can't choose the options given above then error handling mechanism display message wrong option chosen and again prompt to same screen so that user choose the right option.

Refer to Figure 4.3.4, if we choose to calculate hash than interface ask for file or image name on which user want to perform hash calculation and after giving image or file name, it gives you output on screen and also saves it, further message is also displayed that your output is saved and where it saved.

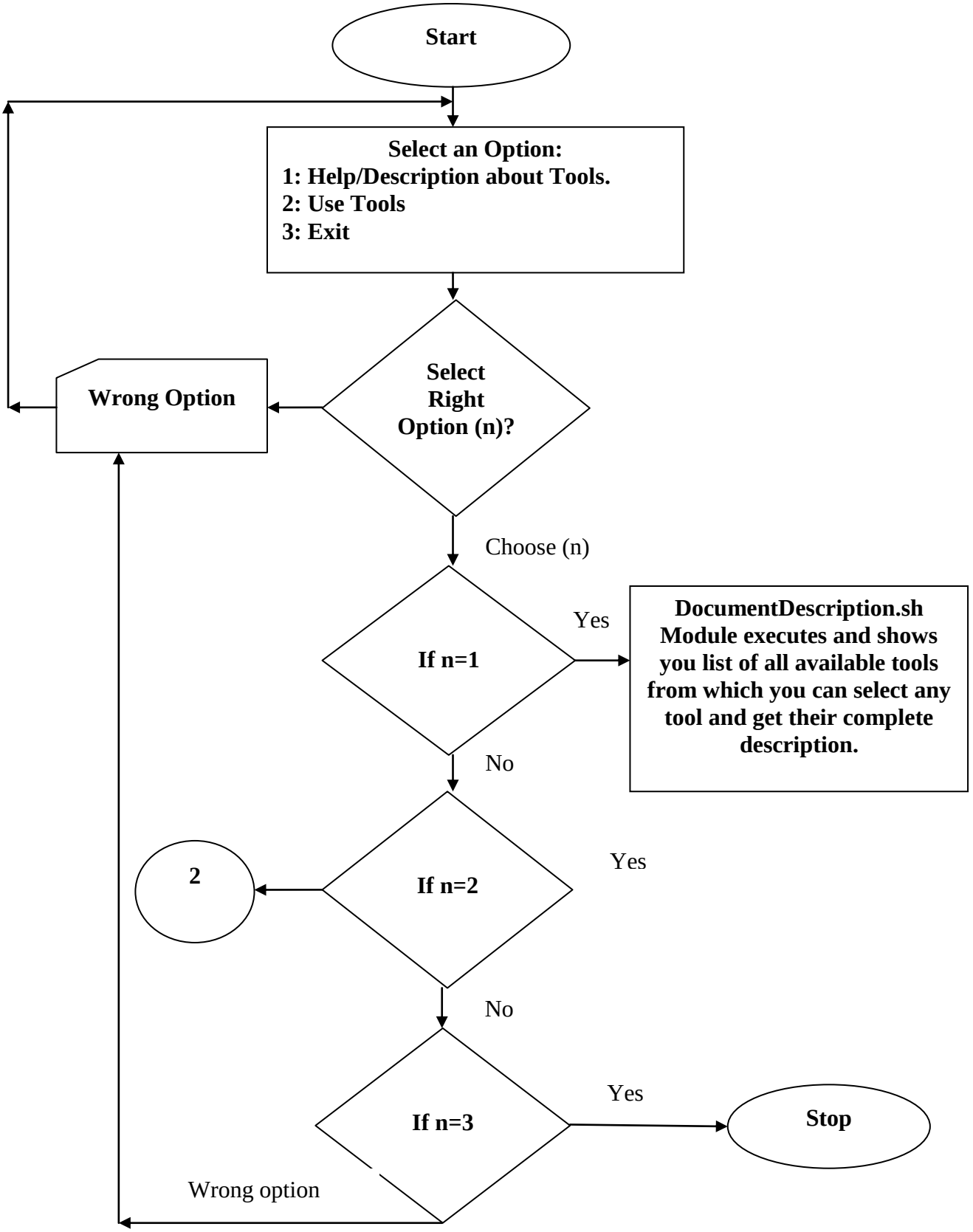


Figure 4.3.1: Flowchart for Main Interface

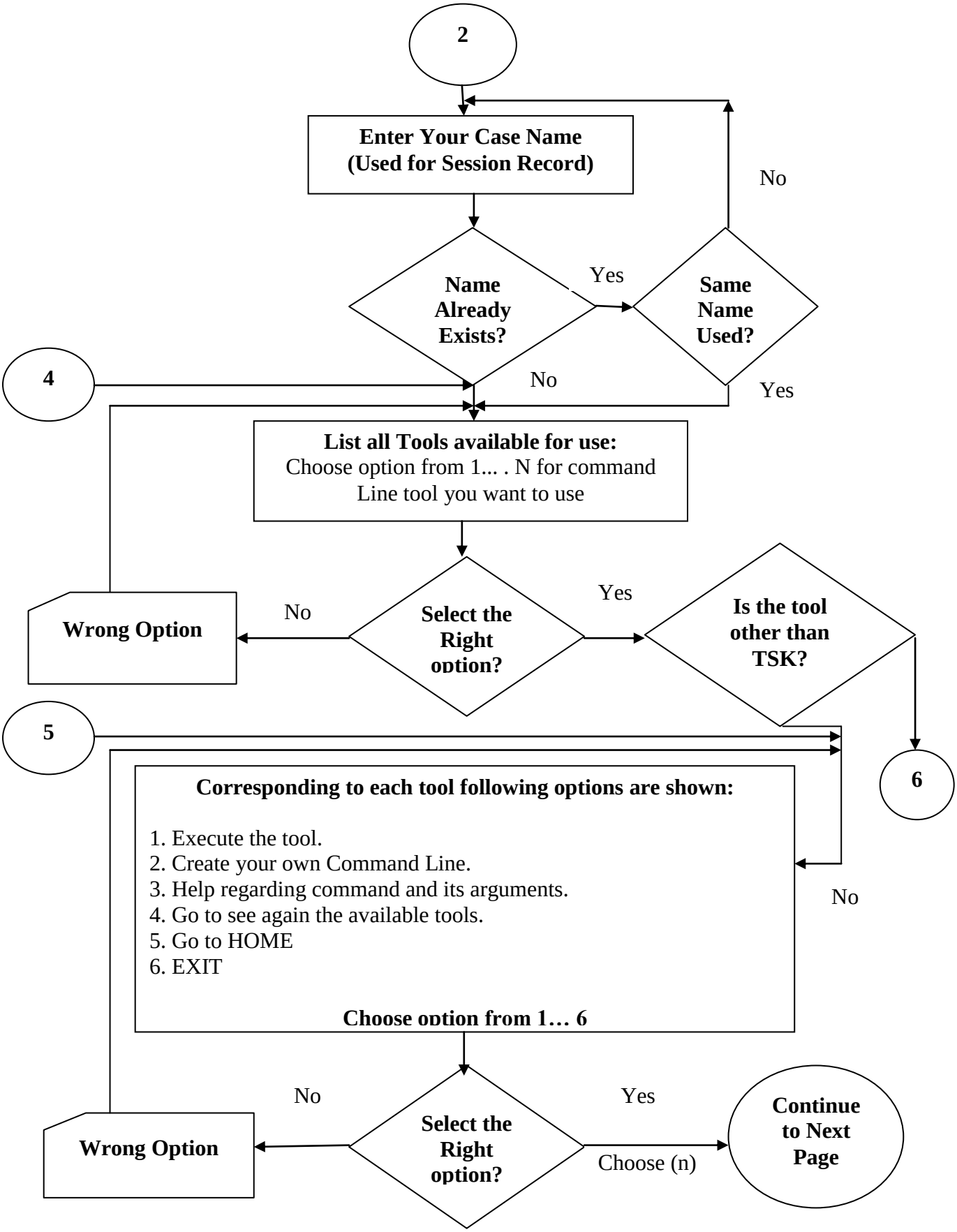


Figure 4.3.2: Flowchart for Interface of Tools available for Use and Command Execution-1

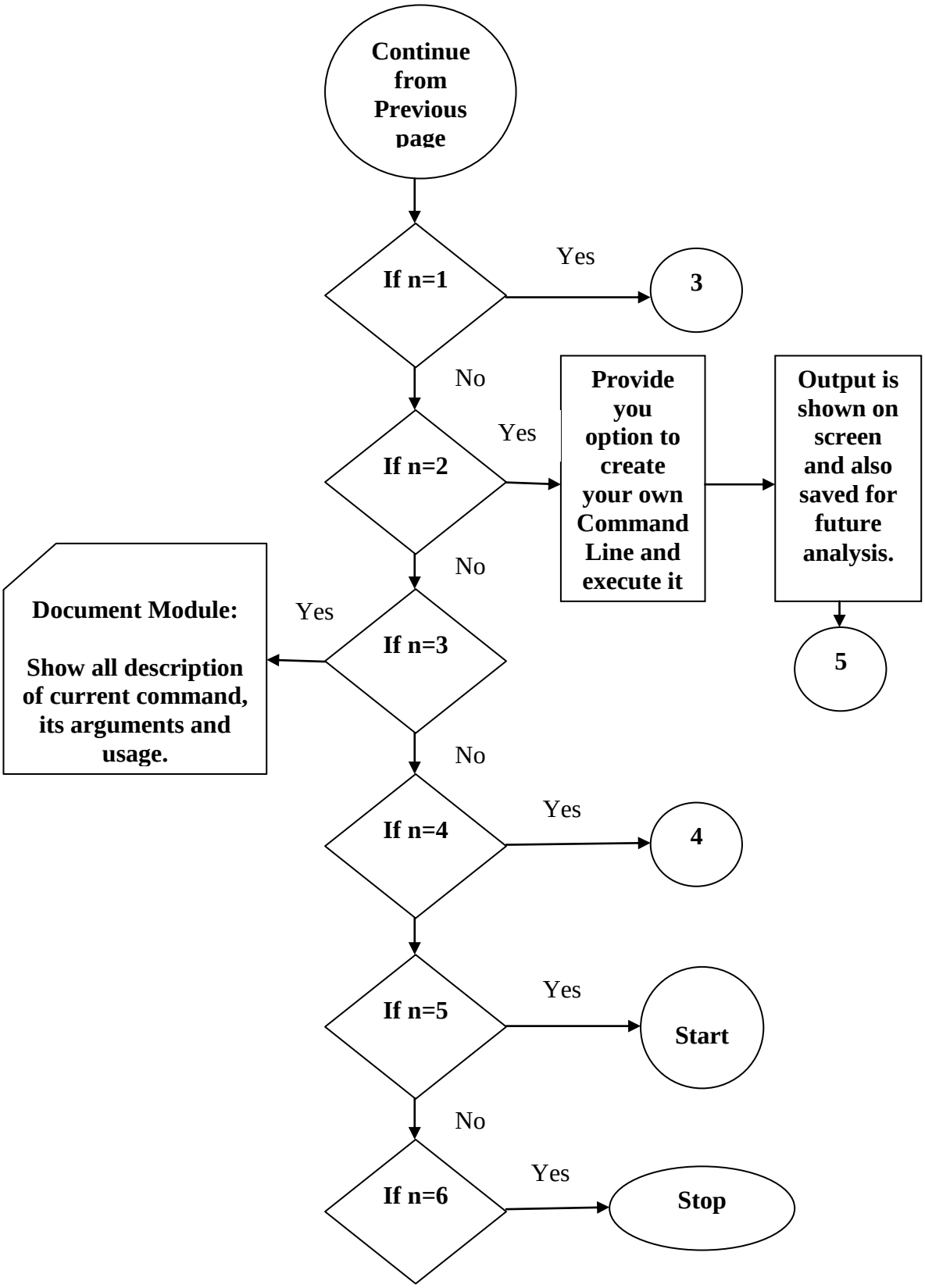


Figure 4.3.3: Flowchart for Interface of Tools available for Use and Command Execution-2

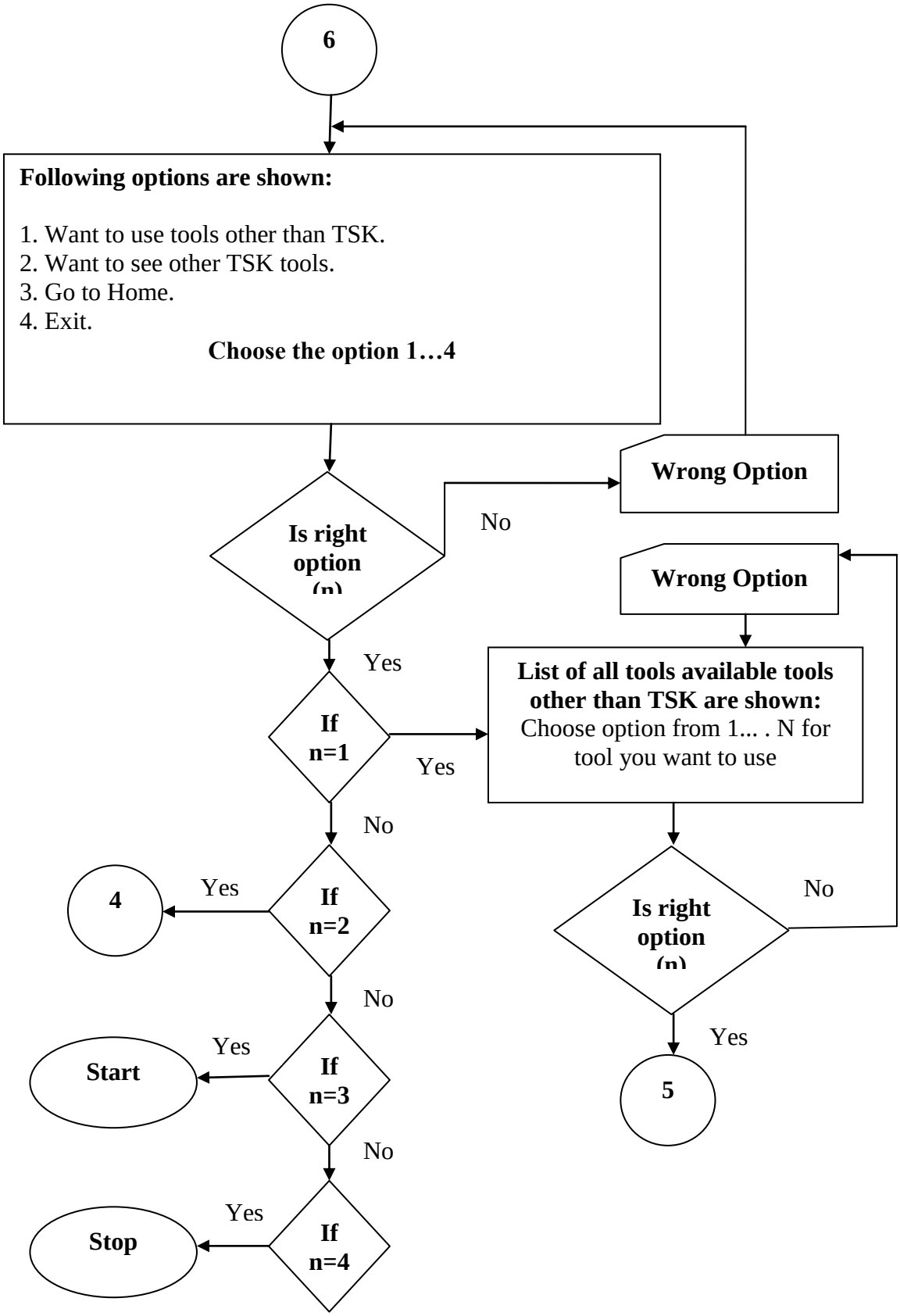


Figure 4.3.4: Flowchart for Interface of Tools Other Than TSK available for Use and their execution.

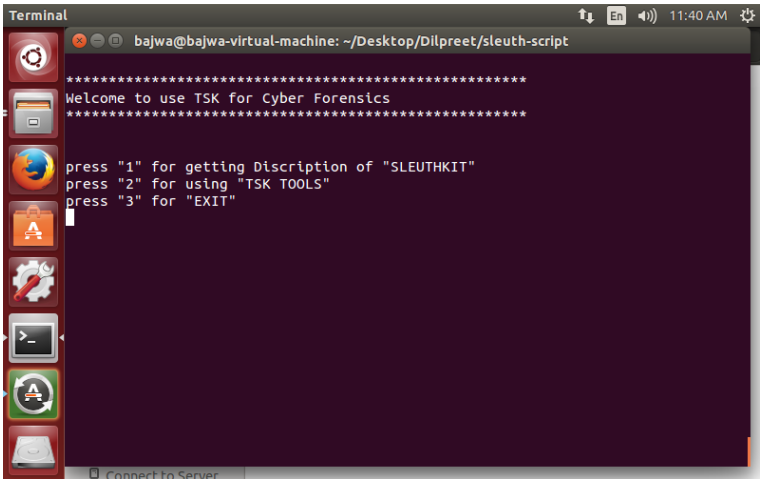
5.1 Experimental and Test Results:

After coding ant integration of our Common CLI for sleuthkit is used and it is observed that interface is working properly corresponding to the command line tools which are implemented. Results are shown and also saved, commands are executed successfully, and session is recorded. All the options shown in interface are working correctly and flow of control is also following the valid path.

We here in this section show the screenshots of our interface to support our point. As shown in screen shorts our interface is working quite well. It provides all features and overcome all limitations which we described earlier. We also observed that we can also incorporate more features and make it more user friendly by adding more functionality which we will definitely incorporate in near future. Not all screen shots included corresponding to all tools. Only limited screen shots are included but all the screen interfaces and implemented tools are working correctly.

5.2 Screen Shots:

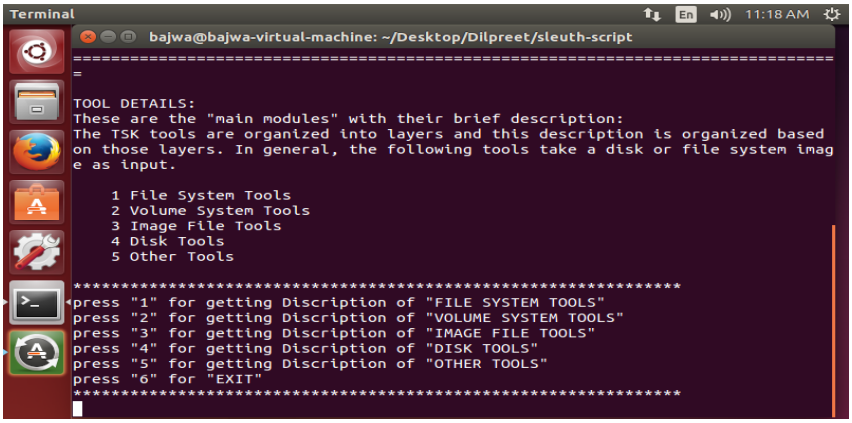
Screen Shot 5.2.1: HOME



Above screen shot is our first main home page, Here it provides us three options regarding getting description of sleuthkit, want to use tools or want to exit, You have

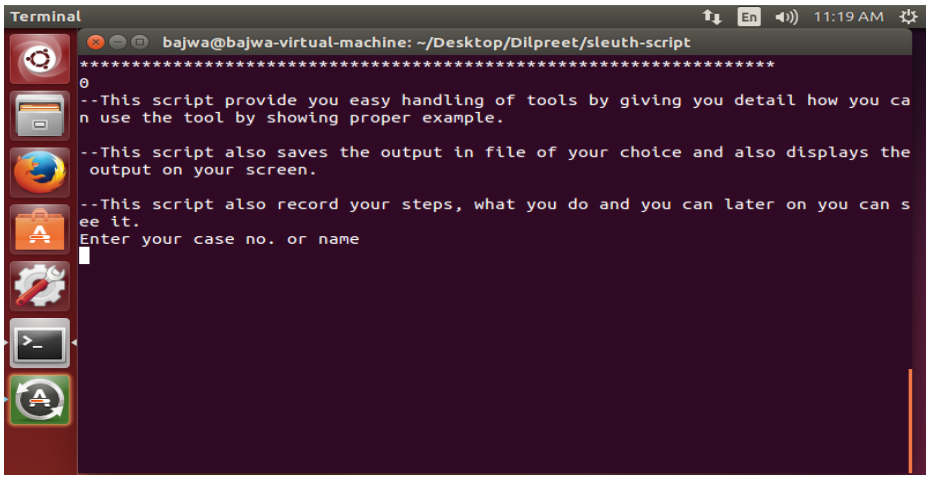
to choose only one option by pressing corresponding number. After that it takes you to next level.

Screen Shot 5.2.2: Description/Help for Tools



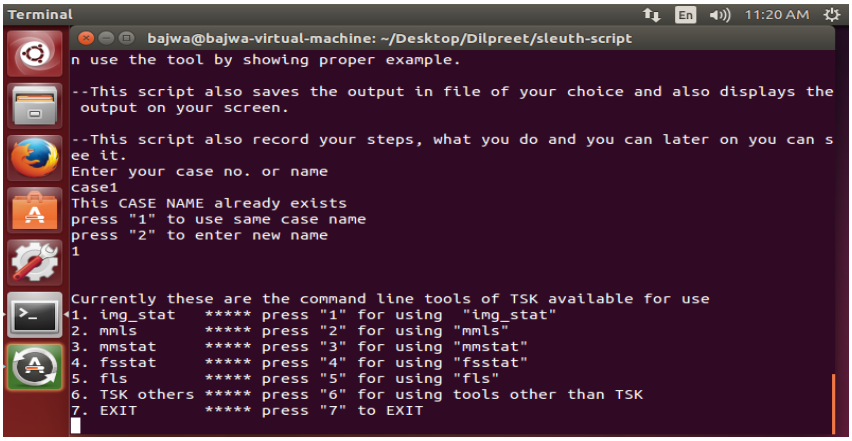
After choosing option 1 from home page, you move to this screen which provides you link for complete description of sleuthkit command line tools category wise. To move forward and to get complete description of tools again you have to select option from the given ones.

Screen Shot 5.2.3: Asking for Case Name for Session Record



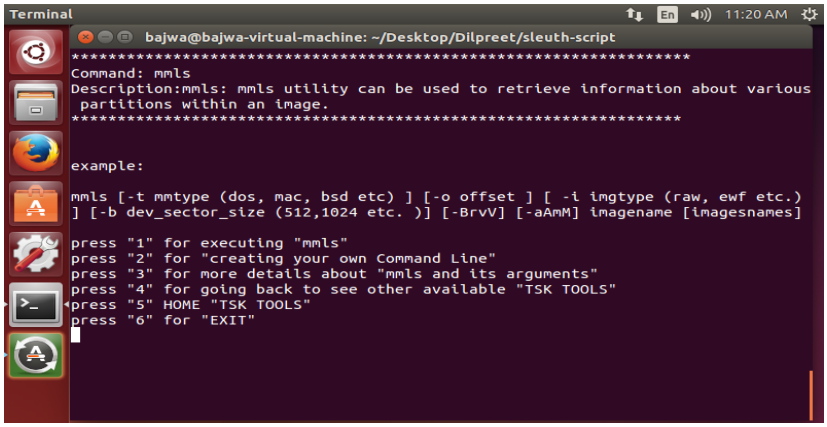
When you select option 2 i.e. you choose to use the tools then you move to this screen. Before moving forward it asks you for case name. Your whole session now records under this case name.

Screen Shot 5.2.4: Shown Tools available to execute



This screen shows all the tools which are available for use, you can select one if want to run otherwise also select exit. Currently img_stat, mmls, msstat, fsstat and fls are implemented, so they are shown. At 6th option there is choice to select tools other than TSK and currently Hash calculation tools are implemented.

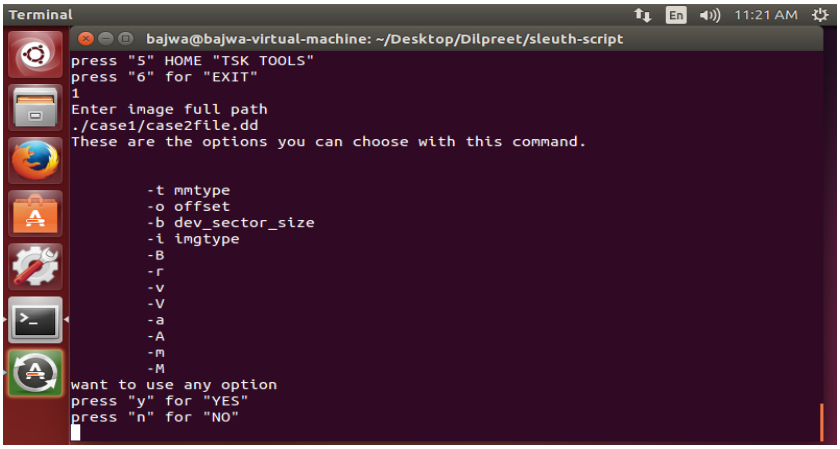
Screen Shot 5.2.5: Asking for execution of Command Line tool mmls and also shown how it will be used.



From above screen if we select one tool then this type of screen appears. Here we choose the mmls tool so options corresponding to mmls are shown. Corresponding to each command line tool of sleutkit these options are shown. The options are if you want to run the tool then select 1, 2nd option is also important here as it provides you to build your command line and directly run it on command prompt, if you select 3rd option then you get complete description about mmls tool and various arguments you can use with this tool to make it more specific,4th option take you to screen no-4 to

see again list of available tools and from there you again continue to choose same or any other tool, 5th option takes you to home screen and 6th takes to exit point. If the user select wrong option than error checking mechanism display message regarding wrong option and again takes you to the same screen to select the right option.

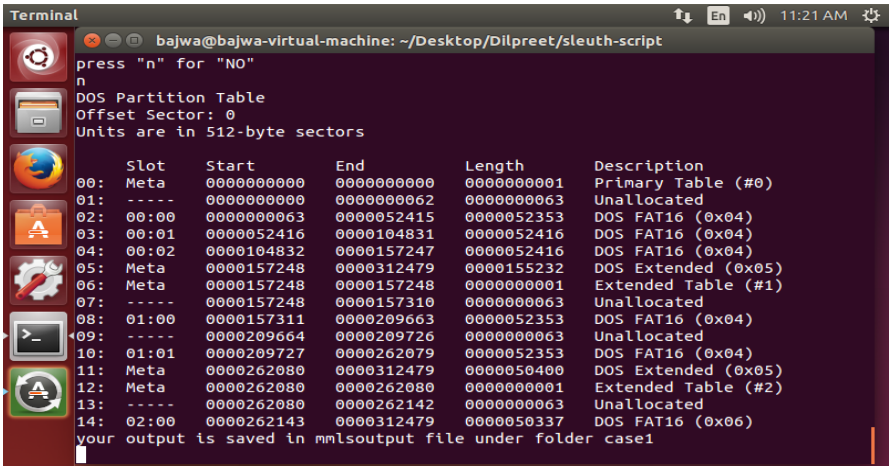
Screen Shot 5.2.6: Asking for image full path on which command is applied, also shown the no. of options you can use with the command and asking for whether you want to use any option.



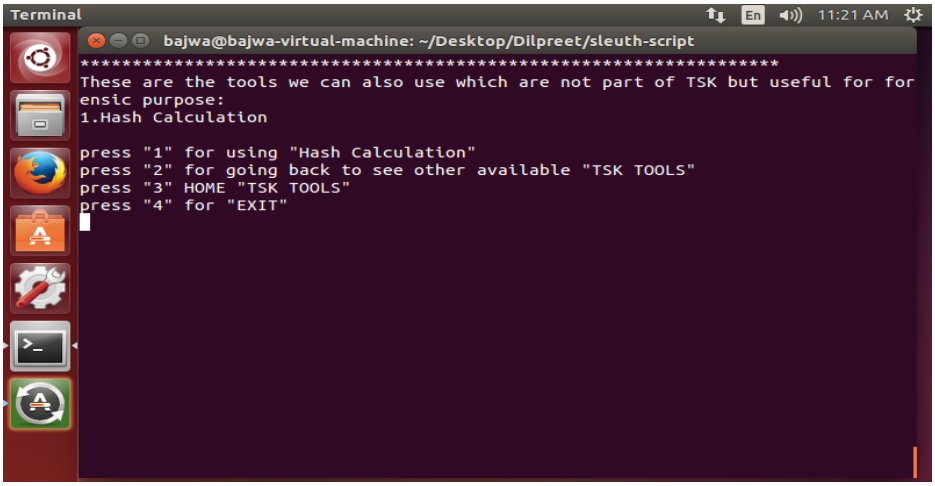
If you select to choose run any command line tool then screen smilar to this appears, Here in previous screen we choose to run mmls tool so this screen appears corresponding to mmls tool. First it asks about image full path i.e the image on which you want to apply forensic investigation and also arguments are shown which can be used with the tool. Here arguments for mmls tools are shown and also asking whether you want to use one of these argument or not. If user select no than in that case tool is run with default arguments otherwise if user select yes than interface asks for the argument user want to use and prepare command line according to that and execute the tool.

Screen shot 5.2.7: Output is shown corresponding to execution of command mmls and also told that where your output is saved.

This is output screen, when you execute some command, the output is shown on screen and also below message is displayed that your output is also saved and storage location is also specified. Above screen shows the output corresponding to execution of mmls tool.

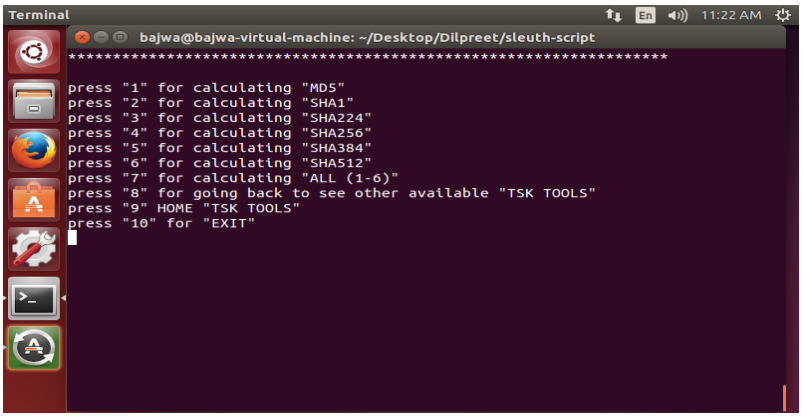


Screen Shot 5.2.8: This screen shows the tools available within this frame work other than TSK and also provides various options you can choose.



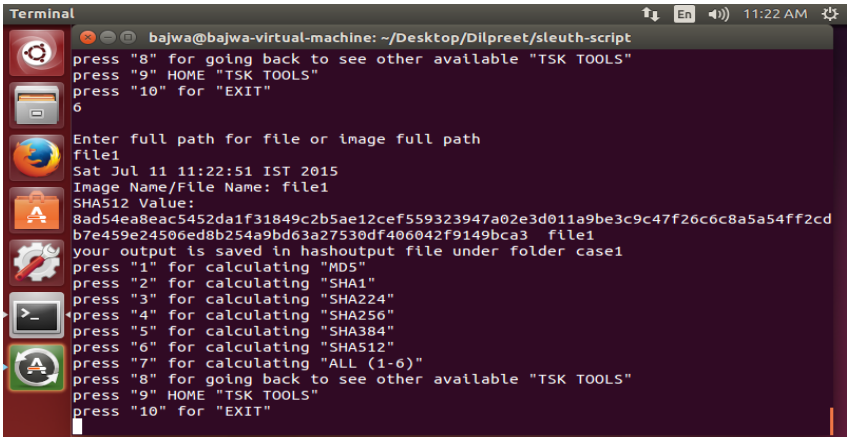
Above screen appears when user selects to use tools other than TSK. It shows all available tools which are not part of sleuthkit but incorporated in to framework to provide more functionality during cyber forensic investigation. Currently Hash calculation tools are incorporated in to framework so they are shown with corresponding options. Either you choose to use tools for hash calculation or move back to screen no.-5.2.4 to see list of all tools or select 3rd option to go back to home or choose 4th option to exit. If user can't choose the options given above then error handling mechanism display message wrong option chosen and again prompt to same screen so that user choose the right option.

Screen Shot 5.2.9: Shows Hash Calculation tools available within this framework.



If from previous screen 5.2.8, user selects option 1 and chooses to run hash calculation tools then following screen appears. It shows all available options of hash calculation from md5 to sha-512. User can either select one of the hash calculation tool or choose option 6 to apply all hash calculation algorithm and calculate all hash values but before executing one or all tools system prompts user for name of file or image for which user wants to calculate hash. User can also select option 7 which takes user to screen 5.2.4 to see all available tools or user can also choose 8th and 9th option for moving back to home or to exit. If user can't choose the options given above then error handling mechanism display message wrong option chosen and again prompt to same screen so that user choose the right option.

Screen Shot 5.2.10: Asking for File or image name for which hash will be calculated, Result is also shown and also shown that where your output is saved.



From previous screen if we choose to calculate hash than this screen appears asking for file or image name on which user want to perform hash calculation and after giving image or file name, it gives you output on screen and also saves it, further message is also displayed that your output is saved and where it saved. Currently from previous screen we choose to calculate sha-512 so corresponding output is shown.

So from above screen shots it is clear that our common CLI for sleuthkit is working properly and efficiently. In addition to this the framework also check errors, if any wrong argument is passed or any wrong option is chosen by user and corresponding message is displayed. Second, the whole session from start to end (until user choose to exit) is recorded under the case name provided by user.

Above small set of screen shots are shown, for each tool there are around 5-6 main screen shots are available, so it is not possible to include all screen shots but from above screen shots you get an idea how actually this interface is working.

6. Conclusion

Several Forensic framework, investigation procedures, policies, tools and techniques are available and we also use them to prove the role of criminals in crime and put them behind bars. Not a standard procedure or technique is available for all types of crimes. For different types of crimes, we use different set of tools, techniques and procedures for forensic analysis. So its responsibility of cyber forensic expert to choose right set of tools to find the culprit. In addition to cyber experts normal internet users or person using computers also have knowledge about cyber crime and related threats so that they can be prone to cyber attacks.

In spite of several measures taken by law enforcement agencies, researchers and cyber experts the cyber crimes takes place so it is must for us to tackle these crimes, if crime happened then it is must to do forensic investigation and found the evidence against the culprits. In forensic investigation cyber forensic tools plays a very important rule and generally they are available as commercial and open source forensic tools. Each has their own advantage and disadvantage. Commercial tools are easy to use, easy to handle and more user friendly further they also provide proper documentation and support. They are efficient and based on proven techniques. The only main disadvantage of using a proprietary tool is that you have to pay a heavy price for it in form of licensing fee for particular time period and after expiring of time period again you have to renew it. Open source tools are also widely used and popular among cyber experts, researchers, students and professionals. They are also equally efficient as commercial tools but the main disadvantage is that not a single tool provides you all functionality secondly they are not so user friendly. Output is complex and it takes time to command open source forensic tool.

In our thesis work we focus on open source forensic tool because they are freely available and their code is also available which you can study, modify, expand according to your requirement, further you can authenticate the working of software because code working is transparent to you. We choose to work on sleuthkit, which is very popular tool for disk and volume system analysis in forensic investigation. It constitutes set of command line tools. As we mentioned earlier these tools are not so

user friendly, it is difficult to use them without any prior knowledge. We developed a common interface for users who want to use these command line tools easily. Actually we automate the process and each step we provide options to users and user can easily select one of them. At the backend we are handling the command line tools for user. When we are using these tools through our interface at each step you get help about how to use these tools and what arguments you can use with the command. The sleuthkit command line tools only show the output on screen but when you are using it through our common interface it not only shown the output on screen but simultaneously saved it for future analysis further from start to end your whole session is recorded that is what steps you follow, what command line tools you used and what is the output corresponding to each tool including timestamp is saved for future analysis and reference. This interface also provides flexibility to incorporate and use tools other than TSK under the same common framework which further enhance the functionality of investigation process.

Future Scope:

Some tools of sleuthkit are not implemented in our interface, in our future work we try to implement all remaining tools of sleuthkit and also add more tools other than TSK to enhance the functionality of our framework as well as cyber forensic investigation. Currently it is available on linux, we try to create interface for windows on same pattern and there is also possibility of showing the output in graphical forms so we try to implement this thing also.

References

1. Gary Palmer et al. ,"A Road Map for Digital Forensic Research", Report From the First Digital Forensic Research Workshop (DFRWS),Utica, New York, August 7-8, 2001.
2. Khidir M. Ali, "Digital Forensics Best Practices and Managerial Implications" Presented at Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012, IEEE.
3. Vinit Kumar, Gunjan, Amit Kumar , Sharda Avdhanam "A Survey of Cyber Crime in India", 15th International Conference on Advanced Computing Technologies (ICACT), IEEE, Sept-2013.
4. Apurba Kumar Roy, "Role of Cyber Law and its Usefulness in Indian IT Industry," Presented at 1st Int'l Conf. on Recent Advances in Information Technology , RAIT-2012 IEEE.
5. M. Al Fahdi, N.L. Clarke & S.M. Furnell, "Challenges to Digital Forensics: A Survey of Researchers & Practitioners Attitudes and Opinions", Information Security for South Africa, IEEE 2013.
6. M Kohn, JHP Eloff and MS Olivier, "Framework for a Digital Forensic Investigation," in HS Venter, JHP Eloff, L Labuschagne and MM Eloff (eds), Proceedings of the ISSA 2006 from Insight to Foresight Conference, Sandton, South Africa, July 2006 (Published electronically) Available: http://mo.co.za.
7. Garfinkel L. Simson, "Digital Forensics Research: The next 10 Years ", digital investigation, pp S64-S7 3, Science Direct, Aug-2010.
8. A.Sankara Narayanan, M.Mohamed Ashik, Computer Forensic First Responder Tools, International Conference on Advances in Mobile Network, Communication and Its Applications, 2012.
9. C.Balan, Dija S, Divya S. Vidyadharan, "The Need To Adopt Agile Methodology In The Development Of Cyber Forensics Tools", International Conference on Computational Intelligence and Computing Research (ICCIC), IEEE, 2010.
10. Mohammad Wazid, Avita Katal, R H Goudar, Sreenivas Rao, "Hacktivism Trends, Digital Forensic Tools and Challenges: A Survey", Proceedings of

IEEE Conference on Information and Communication Technologies (ICT 2013), 2013.

11. Hung-Jui Ke, Jonathan Liu, Shiuh-Jeng Wang, Dushyant Goyal, "Hash-algorithms Output for Digital Evidence in Computer Forensics", International Conference on Broadband and Wireless Computing, Communication and Applications, pp 399-404,Barcelona, IEEE, Oct-2009.
12. Dr Jill Slay, Member, IEEE, Mathew Hannan, Vlasti Broucek and Dr Paul Turner, "Developing Forensic Computing Tools and Techniques within a holistic framework: anAustralian Approach", Proceedings of the 2004 IEEE Workshop on Infonnation Assurance United States Military Academy, West Point, NY 10-11 June.
13. 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", 40th International Conference on System Sciences, Hawaii – 2007.
14. Azril Azam, Raja Mariam Ruzila, "Preliminary Acquisition Information Gathering on Computer Data Storage: Open Source Software (OSS) vs. FIRST DiskImager", International Symposium on Information Technology, 2008. (Volume:1), Kualalumpur Aug-2008.
15. Vassil Roussev, "Building Open and Scalable Digital Forensic Tools", IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), 2011.
16. Manuel Delgado, Manuela Aparicio, Carlos Costa, "Using Open Source for Forensic Purposes",Proceedings of the Workshop on Open Source and Design of Communication, PP 31-37, ACM, New York,USA-2012.
17. Simson L. Garfinkel, "Automating Disk Forensic Processing with SleuthKit, XML and Python", Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, 2009.
18. Kevin R. Lawrence, Hongmei Chi, " Framework for the Design of Web-based Learning for Digital Forensics Labs", 47th Annual Southeast Regional Conference, ACM, NY USA-2009.
19. Sultan Al Sharif, Mohamed Majed Al Ali, Naser Salem, Farkhund Iqbal, May El Barachi, and Omar Alfandi, "An Approach for the Validation of File

Recovery Functions in Digital Forensics' Software Tools", 6th International Conference on New Technologies, Mobility and Security (NTMS), 2014.

20. Erik E. Northrop, Heather Richter Lipford, "Exploring the Usability of Open Source Network Forensic Tools", Proceedings of the 2014 ACM Workshop on Security Information Workers, SIW-14.
21. D.J. Bennett and P. Stephens, "A Usability Analysis of the Autopsy Forensic Browser", Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008).
22. Sleuthkit: http://www.sleuthkit.org/sleuthkit/docs.php
23. Gong Ruibin, Chan Kai Yun, Tony, Mathias Gaertner, "Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework", International Journal of Digital Evidence, Spring 2005, Volume 4, Issue 1.
24. Olga Angelopoulou University of Glamorgan, "ID Theft A Computer Forensics' Investigation Framework", Originally published in the Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2007. This Conference Proceeding is posted at Research Online.
25. Reith, M., Carr C. and Gunsch, G. "An Examination of Digital Forensic Models", IJDE Fall 2002 Volume 1, Issue 3.
26. Eric Katz, "The Fascinating World of Digital Evidence", Purdue, Cyber Forensics Lab Dept. of Computer & Information Technology, Available at: http://www.cyberforensics.purdue.edu.
27. Ayaz Khan,Uffe Kock Wiil and Nasrullah Memon,"Digital Forensics and Crime Investigation: Legal Issues in Prosecution at National Level", Presented at IEEE Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, 2010.I-Lon
28. g Lin 1 Tai-Kuo Woo 2 Yen-Chun Chen3 Tsung-Lin Lu 4 Ian-Sue Shu 5, "Study on Constructing Forensics Mechanism of Digital Evidence Based on Information security Governance Using Digital Evidence Forensic System as an Example", The International Journal of FORENSIC COMPUTER SCIENCE, Volume 7, Number: ISSN:1809-9807, 2, 2012.

29. Agreeka Saxena, Gulshan Shrivastava, Kavita Sharma, “Forensic Investigation in Cloud Computing Environment”, The International Journal of FORENSIC COMPUTER SCIENCE, Volume 7, Number: ISSN: 1809-9807, 2, 2012.
30. Nathan Balon, Ronald Stovall, Thomas Scaria, “Computer Intrusion Forensics Research Paper”, CIS 544.
31. Xuena Peng, Hong Zhao”, “A Framework of Attacker Centric Cyber Attack Behavior Analysis”, This full text paper was peer reviewed at the direction of IEEE communications Society subject matter experts for publication in the ICC 2007 proceedings.
32. Ziming Zhao, Gail-Joon Ahn and Hongxin Hu”, “Automatic Extraction of Secrets from Malware”, 2011 18th Working Conference on Reverse Engineering IEEE Computer Society, pages 159-169.
33. Tameem Chowdhury, Dr. Stilianos Vidalis”, “Collecting evidence from large-scale heterogeneous virtual computing infrastructures using Website Capture”, 2012 Third International Conference on Emerging Intelligent Data and Web Technologies IEEE, pages: 211-217.
34. Kim-Kwang Raymond Choo, “The Cyber Threat Landscape: Challenges and future Directions”, Computer and Security, Science Direct, Elsevier, pp-719-731, 2011.
35. Olalekan Adeyinka, “Internet Attack Methods and Internet Security Technology”, Second Asia International Conference on Modeling & Simulation, May-2008.
36. Manuel Delgado, Manuela Aparicio, Carlos Costa, “ Using Open Source for Forensic Purposes”, Proceedings of the Workshop on Open Source and Design of Communication, pp-31-37, ACM, NY, USA-2012.
37. AccessData, “FTK – Forensic Toolkit”, AccessData. Retrieved from http://www.accessdata.com/products/digital-forensics/ftk.
38. M. Rogers, K. Seigfried, “The future of computer forensics: a needs analysis survey”, Computers & Security, vol. 23, no. 1, 2004, pp. 12-16.
39. N. Beebe, J. Clark, “Dealing with terabyte data sets in digital investigations, Advances in Digital Forensics, vol. 194, 2005, pp. 3-16.
40. Ipsita Mohanty, R. LeelaVelusamy, “Information Retrieval from Internet Applications for Digital Forensic”, International Journal of Security, Privacy and Trust Management (IJSPTM),Vol. 1, No 3/4, August 2012.

41. HananHibshi, Timothy Vidas, Lorrie Cranor, “Usability of Forensics Tools: A User Study”, IEEE Sixth International Conference on IT Security Incident Management and IT Forensics 2011.
42. YinghuaGuo, Jill Slay, Jason Beckett, “Validation and verification of computer forensic software tools-Searching Function”, Digital Investigation: The International Journal of Digital Forensics & Incident Response Volume 6, September, 2009 Pages S12-S22.
43. Eoghan, Casey “Digital Evidence and Computer Crime”, Second Edition: Elsevier ISBN 0-12-163104-4 2004.
44. Computer Forensics Available at: http://newyorkcomputerforensics.com/learn/index.php
45. Digital Forensics Tools & Identification Available at:http://www.vascan.org/
46. Memory forensics details Available at: http://www.dfinews.com/article/memory-forensics-where-start.
47. Jan Kallberg, Bhavani Thuraisingham, “Towards Cyber Operations The New Role of Academic Cyber Security Research and Education” International Conference on Intelligence and Security Informatics (ISI), Arlington, VA, pp 132-134, IEEE 2012.
48. Geer, Dan. A New Cybersecurity Research Agenda (In Three Minutes or Less). https://threatpost.com/en_us/blogs/new-cybersecurity-researchagenda-three minutes-or-less-110711.
49. Jean West, Ulf Lindqvist, Peter J. Vasquez, Sr., “Panel: Technical, Social and Legal Frameworks for Digital Forensics and CyberInfrastructure Security” Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, 2009.
50. M. Karyda and L. Mitrou, “Internet Forensics: Legal and Technical Issues,” Second International Workshop on Digital Forensics and Incident Analysis, 2007.
51. S.J. Wang, “Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crime,” International Journal Computer Standards & Interfaces, Vol. 29, No. 2. pp. 216-223, Jan., 2007.
52. R. Golden & R. Vassil, “Digital Forensics Tools: The next Generation”, Idea Group Inc, 2006, p. 76-91, Chapter IV.

List of Papers Published/Accepted/Communicated

1. Gurpal Singh Chhabra, Dilpreet Singh Bajwa, "Review of E-mail System, Security Protocols and E-mail Forensics", July 2015.
   Status: Accepted in International Journal of Computer Science and Communication Networks

2. Gurpal Singh Chhabra, Dilpreet Singh Bajwa, "Design and Development of CLI for SleuthKit: A Cyber Forensics Framework", July 2015.
   Status: Communicated in International Journal of Latest Trends in Engineering and Technology.