UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

SCHOOL OF COMPUTING AND INFORMATICS

WINDOWS REGISTRY FORENSIC ARTIFACTS; SHELLBAGS FORCOMPUTER SECURITY

By

MUTINDA PETER MBATHA

P53/73184/2014

Supervisor:

MR. ERIC M. AYIENGA

A project report submitted in partial fulfillment for the Award of a Master of Science Degree in Distributed Computing Technology

NOVEMBER, 2016

DECLARATION

I, Mutinda Peter Mbatha do here by declare that this project is my original and own work, with reference where other individuals work and contributions have been cited and that to the best of my knowledge it has not been presented for the award of any degree in any other university.

Signature …… **Date……**

MUTINDA PETER MBATHA

Supervisor;

This project has been submitted in partial fulfillment of the requirement for the Masters of Science Degree in Distributed Computing Technology of the University of Nairobi with my approval as the University supervisor.

Signature …….... **Date ……**

MR. ERIC M. AYIENGA

DEDICATION

I dedicate this work to the digital forensics practitioners and more so to the investigators who carry out their duties each day to see a cyber-secure working environment, to the students so that they may find information worth learning whenever they go to their libraries.

ACKNOWLEDGEMENTS

I wish to convey my appreciation and special thanks to Mr. Eric M. Ayienga my supervisor for his dedication and assistance throughout the research process, the members of the panel whose knowledge and experience in this field has been of great help to my research and the whole School of Computing and Informatics for their support that made me deliver in this work.

Special thanks to my family for their love, encouragement and support towards delivery. Lastly, I would like to appreciate my colleagues at work and school who supported me to deliver this research project.

ABSTRACT

Computers have become part of every one's modern life for it's the tech world that's shaping all that is happening around us. They are not only used for office work but also as tools for achieving other interests both in office and outside as we try to achieve the digitization dream. Criminals too have not been left behind in the same and have perfected the art of their daily business by inventing tech ways so as to hit on this high end fast growing business environment. This has led to the use of computers to do their job (enhance crime activities) which has seen them leverage in an environment that's friendly and very few people in the society suspect. Still, they have created an uneasy atmosphere for those yet to adopt tech in their institutions because they fear being lured and in return become victims. This has led to forensics growth amongst all institutions that have adopted the tech devices available in the market hence the need to venture in to forensics so as define the underlying issues. Still forensics can help define what and how these criminals managed to get authentication, gain access and steal from our systems. Most forensic analysis tools recover the information that might have been deleted from systems and probably show what has been stolen but fail to provide factual evidence relating to these crimes. This has in return informed the need to study forensics artifacts that can be retrieved from the operating system of the given computers leading to identification of Shellbags as the artifacts that provide the wealthiest information relating to these activities that took place on the system. However, less study has been done regarding them leading to limited knowledge on the Shellbags as artifacts. Through the use of exploratory research, this study demonstrates how the use of Shellbags forensics artifacts information can inform the professional practitioners on the use of the available artifacts to enhance security for our computer systems and further advance their skills on forensics. This is because the right interpretation of forensic artifacts is vital for any investigation thus eliminating the instance of false accusations.

KEY WORDS

Computer Security, Shellbags, Windows Registry, Digital Forensics Analysis, Forensic Artifacts, Registry Hives.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CSV – Comma Separated Value

DFI – Digital Forensic Investigator

DWORD – Double Word (A Microsoft Windows definition of a data type)

HKCU – HKEY –CURRENT-USER

HKLU – HKEY-LOCAL-USER

LNK Files – Link Files

MRU – Most Recently Used

NTUSER.DAT – a registry file that stores content of personal documents for the local user

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.0 Study Background

Microsoft window has developed new operating systems that are in use in the current time whose release is based on the success of the previous versions. This has seen the progressive release of the new and different operating systems by Microsoft up to the current Windows8, 8.1 and not to mention the latest release Windows 10 (Microsoft, 2015a) Each of these operating systems versions brings in a varied challenge to the forensic community which they need to overcome in order to perform their duties (Pulega, 2013, Wilson, 2013).

Windows operating system has the capability to record desktop and folder view preference such that when these are visited again by a user logged on into the system; the location, view and position is remembered (Lo, 2014, Key, 2015). These view preferences are stored within the registry hives called the Shellbags in the Windows Operating system. Therefore, Shellbags are an accumulation of registry keys and values that permit the Windows working framework to track client window by showing the users view preference particular to Windows Explorer (Ligh et al. , 2014) that hold a wealth of information particular to the user for forensic investigation.

This information that can be retrieved from Shellbags include: files a user accessed, files that a user should not access, files deleted by a user either on the network or locally on a desktop, the current user who accessed a computer and the folders they accessed before an incident happened, timestamps, etc (Lo, 2014).

There are characteristics that make Shellbags outstanding in forensic investigations according to studies by (Ligh et al. , 2014) some of these are that:

i. Entries for the SHELLITEMS remain in the registry even after these files have been deleted
ii. There is never any update of timestamps associated with the SHELLITEM entries despite there being a modification or access of the file later.
iii. Moving, deleting or access of files updates the ITEMPOS entries

iv. If a user is not logged on to the system at the time memory sample is taken, that user's hives are not available in memory and therefore the Shellbags data is not processed.

The wealth of the information retrievable from Shellbags and the variance each and every new windows operating system has from its predecessor informs my research. The study explores and examines different studies on Shellbags and the forensic artifacts available in the windows registry that are useful towards enhancing computer security.

1.2 Statement of the Problem

Thorough measures for curbing forensics and anti-forensics activities have been implemented by the respective institutions and concerned parties. Whenever an instance relating to these activities takes place, as noted in many victim institutions and by the regulating bodies both locally and internationally and as noted in different works by (Cheboi J, E. Abade, 2016) and (kilungu M., E. Abade, 2015), they hopelessly lead to events which end up destroying the possibly available evidence or distorting it fully. At times, the tools they use are not standardized or fail to work out for them because of limited skills on the same (Cheboi J, E. Abade, 2016). With the fear of not knowing what eventualities took place, how they happened, why they happen, who did them, when did they took place and what they need to do next as established in the research conducted by (kilungu M., E. Abade, 2015), there comes in the need to substantially evaluate the available evidence to prove behold doubts that the fears are cleared. Despite the huge investment in ICT security both in infrastructure, mechanisms, technical skills and tools towards achieving every day dream of a cyber-secure environment; this has not been achieved because of the inability to unearth these adventures (forensic and anti-forensic). This research will be focusing on evaluating studies done on Shellbags so as to enhance the different models applied in this exercise and how they can be employed in any digital forensics investigations towards delivering a cyber-secure environment by the ability to generate valuable forensics reports and proof of factual digital evidence in any litigation proceedings.

1.3 Justification of the Study

The adoption of technology by institutions globally implies the growth of forensics data and thus the need to grow the knowledge on how to usefully retrieve all evidence that exists on these tech-devices employed in delivering their objectives and realizing their dreams for they are subject tools for execution of crimes both internally and externally. Each device runs an

operating system that ensures its operability at any given moment ranging from UNIX, MAC OS, LINUX, and WINDOWS among others. The windows registry in itself holds wealthy artifacts that contain forensic information useful to an analyst during their investigations. Categorically, more detailed and reliable findings that can be used to reveal whether an instance happened, how it happened, who did it that is the system user and many others. The retrieval of such details will be valuable for any forensics investigation towards assuring a cyber-secure territory and their incorporation in the models already in place will foster a developed forensics society.

1.4. Research Objectives

1.4.1. General Objective

Primarily, the main objective for this study is to explore Shellbags information available on windows registry artifacts towards ensuring cyber-crime free society.

1.4.2. Specific Objectives

i. To establish Shellbags artifacts available in the windows registry useful to a digital forensic investigator.
ii. To determine the forensic information that can be retrieved from Shellbags artifacts during forensics analysis.
iii. To incorporate Shellbags analysis skills to digital forensic models employed by forensic analysts.

1.5 Research Questions

i. What forensic artifacts do forensics investigators look for when doing an investigation?
ii. Which information do the artifacts hives (Shellbags) hold for a cyber-crime free society?
iii. How can Shellbags as an artifact be used to carry out investigations?
iv. How adequate is the information retrieved from Shellbags artifacts in forensics?
v. How can investigators incorporate Shellbags artifacts during forensics analysis exercise?

1.6 Limitations of the Study

This research is built on previous assumptions on forensics investigation of windows Shellbags artifacts (Carvey, 2012, Pulega, 2013) who did note that this exercise is encountered with the challenges of having different tools for parsing the Shellbags that are not featured on any defined model. These tools employ different technologies and therefore none of the tools provide similar results as the other. The deleted folders within any given system that is under investigations with Shellbags data can be updated if new folders shared the same names and paths. MAC times contained in a systems Shellbags entry cannot be updated after the folders first exploration. MRU times for the folders that were explored and have Shellbags entries within them and have only one direct subfolder will not get updated. If folders had not been previously explored and are explored, this updates the root BagMRUsubkey's last write time thus causing direct subkey's to report an updated MRU time. This calls for caution to be exercised whenever analyzing Shellbags artifacts. As noted by (Cheboi J, E. Abade, 2016), it is difficult to obtain data from institutions performing digital forensics and thus the scope covered is limited.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

There has been a shift from the use of traditional devices to the use of new tech devices and modern ways of sharing files that has informed the diversity of the available devices being used, emergence of new technologies that are being employed in our day today life activities, the rapid growth of data and the entire world being in the tech-run towards discovering devices that can accommodate more data.

This in return has informed the Cyber-criminal activities and attacks that involve both insiders and the outside (with access rights or without) and are being executed through different ways. These activities and attacks have become sophisticated and stealth, with the advancement in technology; the possibility of an intruder being able to edit or delete the audit trails in a computer and the emergence of tools that can dynamically modify the kernels of the Operating Systems (running) so as to hide what is happening or produce false results.

There are also Anti-forensics tools and techniques (Guan, 2007, Bilby, 2006, Garfinkel, 2007) being employed by the cyber-criminal perpetrators to do a number of things that help them get away with their criminal activities. These include Steganography, Evidence elimination tools, Encryption (File or whole drive). These tools are used to erode factual forensic evidence that can be used within a legal system to carry out prosecution in a criminal case where the majority of cyber criminals never get caught or prosecuted even after definition and identification.

Whenever an investigator is conducting an investigation (McQuaid, 2014a), it is recommended that they don't lose sight of the fact that they are investigating the actions of a person and not that of a computer. Each and every action on the computer (McQuaid, 2014a) is as a result of doing something or not doing it at a particular time for the event to be created thus the need for the investigator to understand how these events on the system correlate to the actions of a user. These Events are kept in the operating system registry keys/hives which analysts use for any activity they are undertaking.

2.2 Categories of Windows Registry Artifacts

These are the different types of artifacts found in the windows registry as a result of the user activities with the operating system of the given machine (McQuaid, 2014a).

i. Shellbags

These are registry entries/keys according to (Ballenthin, 2014) that record the users preferences according to the folder display in the windows explorer by showing every directory a user accesses whether the user opened a file or not.

ii. File System Information

This is information (WikiInformation, 2012) showing how data is stored and retrieved within a given system for each individual file. This information includes structure and logic rules used to manage the group of information regarding any given file in the system.

iii. Jump Lists

These are lists according to (Microsoft, 2015b)that hold a record of the recently opened items like files, folders, websites etc. and are organized in order by the program that a user open them with. Therefore they are used to open items and also pin favorites for quick access to those items one uses frequently on their machine.

iv. LNK - Files

These are extension for an alternate route record (Rouse, 2010) that is utilized by Microsoft windows to indicate an executable file instead of navigating to the executable file location in the system. The acronym LNK stands for LiNK.

v. Network Share Information

This is information about files shared across a network or that can be remotely available from another device regarding the subject network they are running in (Microsoft, 2015c).

vi. Operating System Information

This is the information about the software that manages the computer hardware and software resources and also the provision of common services for computer programs. This includes time sharing information for tasks, memory allocation for processes, hardware input and output information too (wikimedia, 2015).

vii. Startup Items

These according to (Phelps, 2011) in his article, these are specialized package whose code is executed amid the final phase of the boot process and during other predetermined times and contains shell scripts along with other configuration information used by the system to determine the execution order for all startup items.

viii. Time-Zone Information

These are the time zone data available in the Windows registry (microsoft, 2015d) where by the time zones installed in the computer are stored in the time zone registry hive with each having a unique key. These hives store information about the time such as display name, standard name, daylight name and optimal daylight start and daylight end times.

ix. Windows Event Logs

These are special files (Microsoft, 2015e) found in Windows that record significant events on our computer such event provider and the sessions it logs, when a program running encounters an error. In the event this occurs, Windows records this in the event log that can be read using the event viewer.

x. Windows Pre-fetch Files

These are small files in Windows according to (McQuaid, 2014c) where information is saved in them within the Pre-fetch folder. Where the information stored in these files is then used the next time a user is switching on their computer for reference so as to help speed the start process.

2.3 Why Study Shellbags

This study has been motivated by the wealth of information available in Shellbags unlike other artifacts found in the Windows Registry. The information available in Shellbags keys/hive according to (Tilbury, 2011) in his article on "computer Forensics Artifact; Windows 7 Shellbags" include; Bag Number, Registry key last write time, name of the folder, it's path, creation date and time, the modify date and time, access date and time all as embedded. These Shellbags contain information of forensic value according to (Pulega, 2013);-

i. Shellbags data is able to define which files were accessed by a certain user using the windows explorer either from the local machine, through the network or from a detachable drive i.e. USB drive, external hard disk or any other drive.

ii. The availability of evidence for previously existing folder files either after overwriting or deletion.
iii. The different users who might have had access to certain folders through the system.
iv. The means through which a certain folder was navigated to which is either through a shortcut or via the root over the windows explorer.
v. When certain folders in the given system were accessed using the file explorer.
vi. The historical MAC times of the folders corresponding to the time these folders were first accused in the system.

2.4 History of Shellbags

Since Windows XP, Shellbags have existed only that they were not popular (McQuaid, 2014b). They have become popular as Forensic Investigators understand their potential in regards to value for the information these artifacts contain and their advantage to an investigation. They have since been available in all latest versions of Windows Operating Systems. According to (Pulega, 2013) they are used to trace the activities of a user on a Windows Operating System that is in question, to define the availability of an attacker or an intruder through the explorer navigation activities or the use of removable devices by the users of the subject system.

2.5 Structure for the Shellbags

The Shellbagsartifacts information is made up of main two registry keys that include the BagMRU and Bags (Lo, 2014). The keys BagMRU represents is the desktop except the ordinary BagMRU because the child keys do not have any assignment to specific folders (Lo, 2014). This keys store the names and the paths for the folder by creating a similar tree structure while in the Bags keys, the view preferences for the location, mode of view and size of a window are stored. The study by (Lo, 2014 and McQuaid, 2014b) narrates that the registry keys that are found in BagMRU and have an MRUListEx registry value that is binary does the recording of the order of the recent child folders that had been accessed. Besides that keys under BagMRU have a DWORD value called NodeSlot which has a number slot that point to the registry key which is in the Bags and that it holds the view preferences for different users.

According to (Lo, 2014) windows Shellbags structure has undergone an evolution whereby for each version of the Windows Operating System released there have been changes in the location of the of registry keys and the value files. In Windows XP (McQuaid, 2014b and Lo, 2014), indicate that both the Shell and the ShellNoRoam keys store the Shellbags

information. As of Windows 7, (McQuaid, 2014b and Lo, 2014) have found out that the ShellNoRoam is no more employed and hence these Shellbags information are stored only under Shell keys. Thus the keys are stored in the BagMRU Keys in the same way and order of access as it is in the windows explorer.

2.6 Insights on Shellbags

The Shellbags according to the works by (McQuaid, 2014b) are stored in the BagMRU Keys in the same way and order of access as it is in the windows explorer where each folder represents the child or the parent folder as it is in the previous one. All these folders contain the following keys MRUListEx, NodeSlot, and NodeSlots as (Key, 2015 and McQuaid, 2014b) define it:

i. The MRUListEx keyhas a 4-byte value that shows the order in which each of the child folders under the BagMRU listing was lastly accessed. This is for an instance where a given folder that has three child folders labeled as 0, 1, and 2 and we have folder 2 asthe one that had been accessed recently; the MRUListEx will now list folder 2 as the first record then the order of access for folders 0 and 1 will come next.
ii. The NodeSlot is a value that corresponds to the Bags key and the specific view setting which is stored there for the specific folder. Therefore combining the data from these locations, investigators will be able to group together the several information that pertain a given folder and how the specific folder was viewed by the subject user.
iii. Finally the NodeSlots which is available in the root within the BagMRUSubKeys.This keys only update at any instance a new Shellbags is created in the system.

2.7 Analyzing Shellbags

Shellbags data as (McQuaid, 2014b)states is kept in a raw hex format and therefore they need to be formatted so as to understand the path and all other additional details relating to them. An analyst is required to bring together all the data collected from each subject in the progression order so as to piece together the path of the folder. This will then lead him to the use data found in the available Bags key so as to get the extra details within the icons, the position, and finally that of the timestamp as (Pulega, 2013) elaborates in his work. According to (Key, 2015) analysis of Shellbags can be used to define what shell folders were accessed and when mostly those folders that have since been deleted or that were located on a removable disk.

According to (Tilbury, 2011) the information an investigator finds in Shellbags hive has each folder having the following information:

i. The Bag number which identifies the Bags SubKeys that contains the user preferences also referred to as the NodeSlot
ii. The registry key last write time defines the first access time of the given folder or the last preference change of the folder in subject.
iii. The name of the folder as it is in the system.
iv. The full path for the folder location.
v. The attached creation date and time as stored at the time that the BagMRU key was created.
vi. The attached modify date and time as stored at the time the BagMRU key was created.
vii. The attached access date and time as stored at the time the BagMRU key was created.

2.8 Use of Shellbags for Investigation

The study on incident response on windows by (Carvey, 2012) demonstrates how Shellbags are used in carrying out an investigation by a forensic examiner. This is because Shellbags are able to demonstrate the user's activity ranging from the access to the systems folders, different files, the external devices used for storing data and finally all the attached network resources to the subject system (Carvey, 2012). The users access to these stated resources is ideally recorded and remains even after these resources that were accessed cease to exist i.e. were deleted or cannot be accessed over the system (Carvey, 2012). Shellbags are very useful when finding answers to queries on data enumeration in an intrusion case as subject. They are also important in that an investigator can use them to define the contents of removable device which an intruder used and the left with it long way ago. None the less Shellbags can define the details held in a previously encrypted storage device that had been mounted to the system, and the information pertaining to all folders deleted. Finally, it is also possible to retrieve the invaluable reference for the items that are no longer part of the file system as (Tilbury, 2011) defines in his studies. In his publication (Yuandog et al. , 2009) proposed a method that could be used to analyze user activities by tracing their actions in Shellbags information within the registry snapshots. This method was used by the investigator to define that there were no association of the user and the subject system and that the interaction should have or should

not have taken place in a window of a defined time period. Incorporating this method with other ordinary forensics analysis tools provided detailed information on the subject user activities according to (Yuandog et al. , 2009), they were overly able to observe and analyze the casual links amongst the actions of the specific users and the update patterns on the Shellbags information. An institution that has adopted a policy for its users can utilize the Shellbags data to exhibit the infringement of its predefined policy by ordinarily showing access to file paths with flawed names or an infringement of worthy the policy use so as to get to another worker's PC without their assent (Carvey, 2012). Shellbags analysis can also exhibit how users add and handle files (i.e. The .zip files) within their systems, access to removable devices which can be attached to their systems (i.e. smart phones, flash disks, external hard drives, cameras, SD cards etc.) and are embedded in the Registry Keys. This also entails the access by the user to specific resources on these devices (Carvey, 2012). The understanding of the actual data structures for the Shellbags is very valuable for any analyst or investigator because they use these structures knowledge to parse other artifacts like windows shortcut/LNK files (Carvey, 2012).

2.9 View/Location of Shellbags

Shell bags can be viewed in a live environment using Registry Editor available in operating system. They though cannot be parsed not unless a Shellbags parser is used to decode their contents. A user can also modify these contents of the Shellbags depending on the action that they perform on them and thus requiring an investigator to exercise caution so as to define what possible action could have been performed before they start the action on the suspects' machine.

In Windows Xp (McQuaid, 2014b), stated that Shellbags artifacts are stored in the NTUSER.dat registry hive as shown below:

i. HKCU SoftwareMicrosoftWindowsShell
ii. HKCUSoftwareMicrosoftWindowsShellNoRoam

In Windows Vista (Key, 2015), Shellbag data is stored in NTUSER.dat and UsrClass.dat registry hive:

i. HKCU SoftwareMicrosoftWindowsShell
ii. HKCU SoftwareMicrosoftWindowsShellNoRoam

While in Windows 7 they are found in the UsrClass.dat hive (McQuaid, 2014b):

i. HKCULocalSettingsSoftwareMicrosoftWindowsShellbags
ii. HKCULocalSettingsSoftwareMicrosoftWindowsShellNoRoamShellBagMRU

In the latest releases, both Windows 8, 8.1 and 10, the diagram below shows elaborately the location for the UsrClass.dat hive as viewed using the Registry Editor

i. HKCULocalSettingsSoftwareMicrosoftWindowsShellbags
ii. HKCULocalSettingsSoftwareMicrosoftWindowsShellBagMRU

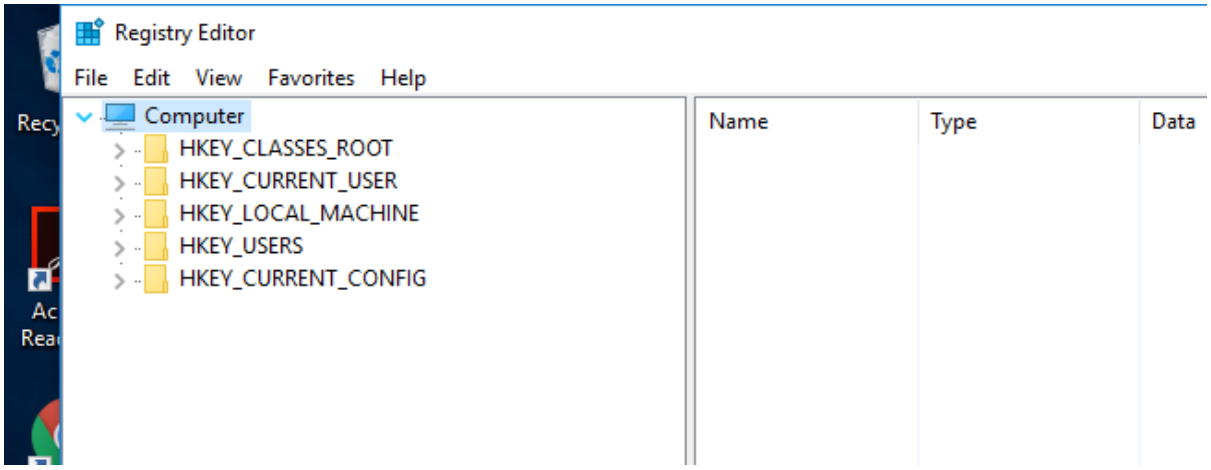


Figure 2.1 Showing Windows Registry

Windows10 registry view using Registry Editor on a live machine showing the location of HKCU (HKEY_CURRENT_USER)

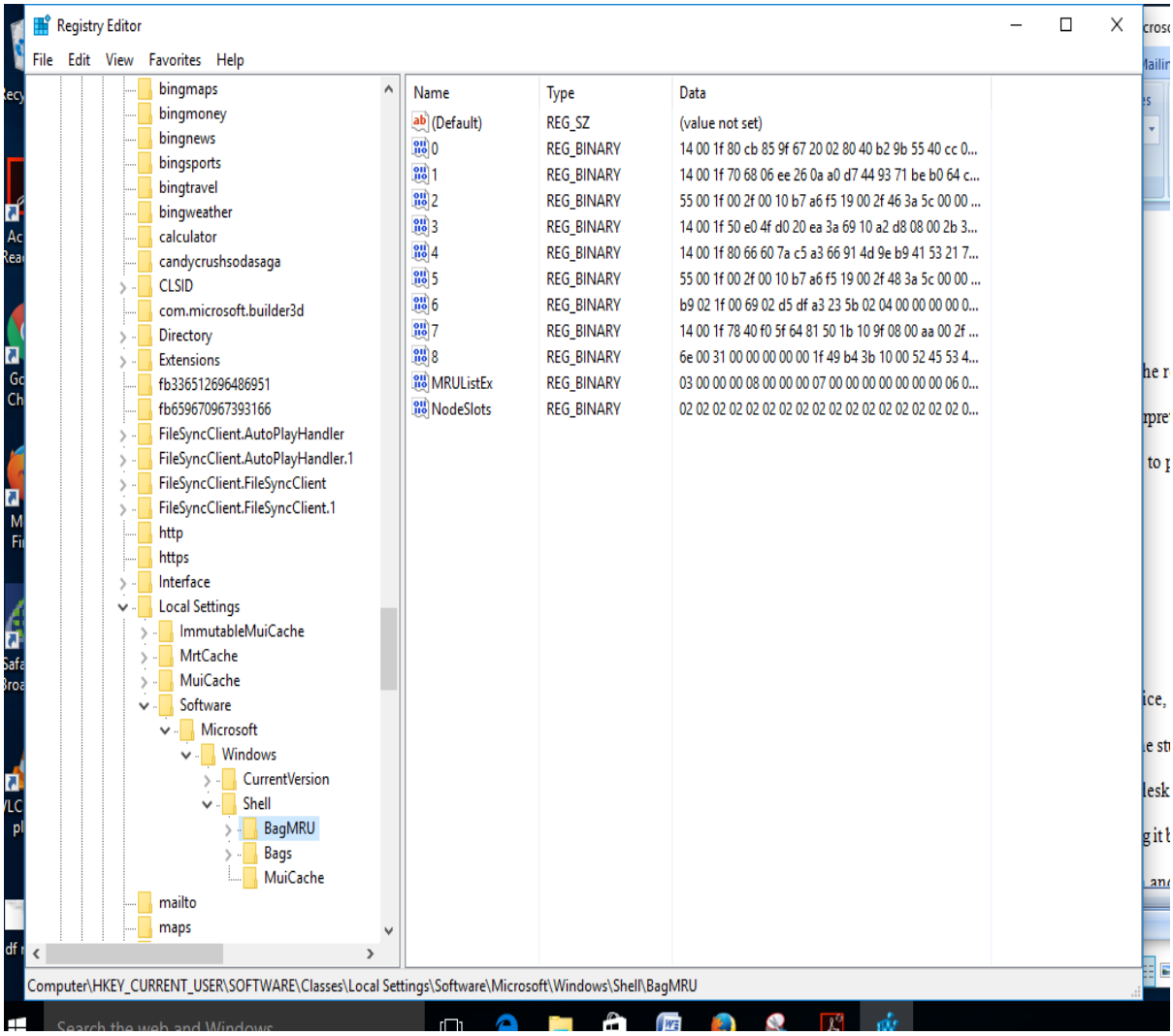


Figure 2.2 Showing the Location of Shellbags

Shellbags location view in Windows10 Using Registry editor on a live machine (showing both Shellbags and ShellbagsMRU)

By employing analysis tools on these hives, the NTUSER.dat and UsrClass.dat according to (McQuaid, 2014b) an examiner is able to define the files and folders that were accessed on a system using the Windows Explorer and also find out what action might have been performed on the subject investigation machine as defined below.

i. The file name.
ii. The size of the physical file.
iii. The size of the logical file.
iv. Modified timestamps.
v. Accessed timestamps.
vi. Created timestamps.

vii. Last write timestamps for the Register Keys(BagMRU and the Bags)

viii. The location of the folder being analyzed using its path.

The timestamp details are also available where an investigator is able to define the last access times for folders being examined.

2.10. Events on a Desktop of the Local Machine

This table defines how Shellbags artifacts are created and modified when exploring files and folders within any given computer that is running.

Table 2.1 Showing Events on a Local Machine

Actions/no.	**User action/event**	**Shellbags tool output**
1.	On clean machine	No Shellbags artifacts created.
2.	Create a folder	No Shellbags artifacts created.
3.	Navigate the folder	Shellbags entries are created.
4.	Create more folders and add items inside the already existing folder	New Shellbags entries are created for each new created folder and entry.
5.	Close all the folders	The action close does not change Shellbags entries – this is because the BagMRU does not update when there is no action to update details in the directories.
6.	Repeat process No. 3 for all folders	This Updates the MRU time for the Shellbags artifacts.
7.	Click the back button in the windows explorer	This does not update the BagMRU time artifacts.
8.	Close the opened window	This does not update the BagMRU time artifacts.
9.	Navigate the folders again using the windows explorer	Additional entries are created for the folders that had not been accessed and have been accessed.
10.	Close and or delete the folder	No updates for Shellbags artifacts
11.	Explore the folders again	There is creation of Shellbags artifacts

In the above table we see how Shellbags artifacts are created and modified when exploring files and folders in a computer.

2.11. Events on a Removable Media - Flash disk/Hard Drive

This is used to show that Shellbags artifacts can be used to identify explored files and folders from media that is no longer available to an investigator. For instance, someone stealing

documents by copying them to the removable media and later explores the device to confirm that what they copied exists in their device before removing it.

Table 2.2 Table showing how Shellbags artifacts are created and modified when exploring files on a removable device

Action S/No.	User action/event	Shellbags tool output
1.	Insert and open drive	No change on Shellbags already existing
2.	Drag and drop the folder at the desktop inside the removable media	The MRU time is updated but no Shellbags are updated
3.	Navigate the folder on desktop from the removable media	Update of the MRU time for the two folders in both locations
4.	Change the location of the folder on the desktop and close the window, navigate the folders backwards forth and close it	Position change updates the Bags subkeys but no updates for BagMRU for all events
5.	Navigate the folders via explorer	New entries are created, MRU times are updated but no updates to the Shellbags artifacts
6.	Close, and delete the folder via cmd	No updates to Shellbags artifacts
7.	Explore the drive	Update to Shellbags MRU time takes place
8.	Close the window and remove the drive from the device	No updates to the Shellbags artifacts and no changes

2.12. Tools and Techniques for Analyzing Shellbags

There are several tools available for the above subject and they each differ in the approaches used for decoding and presenting information available in Shellbags. According (Garfinkel, 2007) these tools were not developed for typical computer security issues that are committed with computers or otherwise against computers but rather these tools were developed with the sole purpose to solve issues and crime related cases perpetrated in opposition to the people where the evidence exists on the subject computer. Also these tools are developed to help examiners to single out the specific pieces of evidence that are not in any way going to assist in the investigation or analysis being carried out. These tools include the following:

2.12.1. RegRipper

This tool was developed by (Carvey, 2014) for the extraction of Windows Registry data towards Shellbags analysis which offers flexibility according to the examiners needs because

it allows customization through the use of plugins or the user writing their own plugins to suit their needs. This tool cannot be used on live hives files thus indented for use on file hives that have been extracted from required images or those accessible by mounting their images as a file system. The tool has been archived (RegRipper, 2014) because better tool have been developed by borrowing this tools concepts as we will envisage below.

2.12.2. RegistryDecoder

This tool was developed for acquisition analysis and reporting of registry contents (DFS, 2015). Being a free and open source tool, it exists in two components: online acquisition component and the offline acquisition component. These components functionality is exposed to a graphical user interface and provides investigators with powerful analysis capabilities. The tools development (DFS, 2015) was inspired by other registry analysis projects that include:

- Access Data's Registry Viewer (AccessData, 2015) used for browsing specific hives,
- RegRipper (RegRipper, 2014) used for the plug-in based analysis system and the
- RegLookup (Sentinel, 2010) for automated registry analysis.

Registry Decoder does a unified registry analysis and provides a new registry-related research useful for all skills level of an investigator (DFS, 2015).

2.12.3 TZWorkssbag

According to the developers of TZWorksSbag (TZWorks, 2015), this tool was developed to work either as a standalone or on a command-line platform. It is used to parse and retrieve Shellbags artifacts from the windows user account registry hives available in the given system. TZWorksSbag as a tool targets the Shellbags SubKeys and pulls out the important artifacts available in the directory and file so as to help in the identification of the user activities in the system. This tool works on both running target registry hives (computer that is already in use) and on already secured registry hives (Imaged storage devices for analysis) where all the available artifacts are dumped in one of the three formats that are parsed and then included together with other forensics artifacts (TZWorks, 2015).

These formats include;-

- The default output format where all the record is placed in a separate line and field then they are separated by a pipe character (TZWorks, 2015).
- Format two is the Sleuth Kit body-file format as it is elaborated by (SleuthKit, 2012)

- Finally this log2time line CSV(Comma Separated Value) value as in (Log2timeline, 2015)

2.13. Shortcomings when Examining Shellbags

When an examiner is analyzing timestamps in Shellbags, caution should be taken because most of the timestamps may or may not update in every given case according to (McQuaid, 2014b and Pulega, 2013). It is advised that an analyst should ensure the validity of the given Shellbags value and the use of the MRUListEx key is highly recommended so as to tell the child folder that had the most views previously.

2.14. Conceptual Framework

The digital forensic business model by (Choo et al. , 2013) provides a clear conceptual framework that fully distinguishes electronic evidence from physical evidence and defines the components involved in the digital forensics activities like the humans conducting the activity, the digital evidence which is the major object then finally the procedure which is the authority for the activities being undertaken. This does not suggest that the other existing models and frameworks are not sufficient as (Yusoff et al. , 2011) notes in his works. This is because of administering electronic evidence on any litigation process may be limited by the legislation of different countries in the world thus the need to widen the scope for the digital forensics activities. (Prayudi et al. , 2015) In their studies recommend that handling both digital and physical evidence be treated similarly. These are the phases involved and they include the readiness and deployment phase, the investigating the physical and digital crime scenes then finally the review phases as well. The trio according to their work also did note the magnificent difference exhibited in the real and current practice also noted are the models in place in respect to storing and maintaining the digital evidence which require harmonization so as to embrace the models in place fully.

The importance of this model in a digital forensics investigation environment is that is incorporates both physical (manual) and digital forensics investigation processes that may be employed by an investigator.

The above model incorporates how digital forensics should be carried out which entails the steps noted below and demands that one; -

i. Identifies the main purpose for the digital investigation that they are conducting
ii. Identifies the fundamental standards held as reference for the treatment of the forensic evidence

iii. Identifies and defines the objects involved in the activity of digital forensics and investigation who are human beings.

iv. Recognize nature and how the advanced crime scene investigation action goes about.

v. Finally, construct business models that will explain the connection between the items in the work place of the digital forensics investigation.

For the above exercise to be a success, the following is recommended of the investigator to observe and includes: preserve and overview of the collected digital evidence, documentation of evidence proof and the scene, searching for the available evidence, reconstructing the digital crime scene and then finally presenting the digital scene theory.

Based on this framework provided, Digital Forensics Investigations(DFI) revolves around five phased exercise that include the Pre-Process, acquisition and preservation of the acquired evidence, analysis, presentation and post process towards delivery of reports on the whole exercise as noted by (Yusoff et al. , 2011) in their concluded studies. The crime tools employed in execution, the investigation tools too and the level of expertise skills for the investigators vary thus requiring one to revisit the previous phases they had done towards rectifying the challenges that might be encountered in the whole exercise.

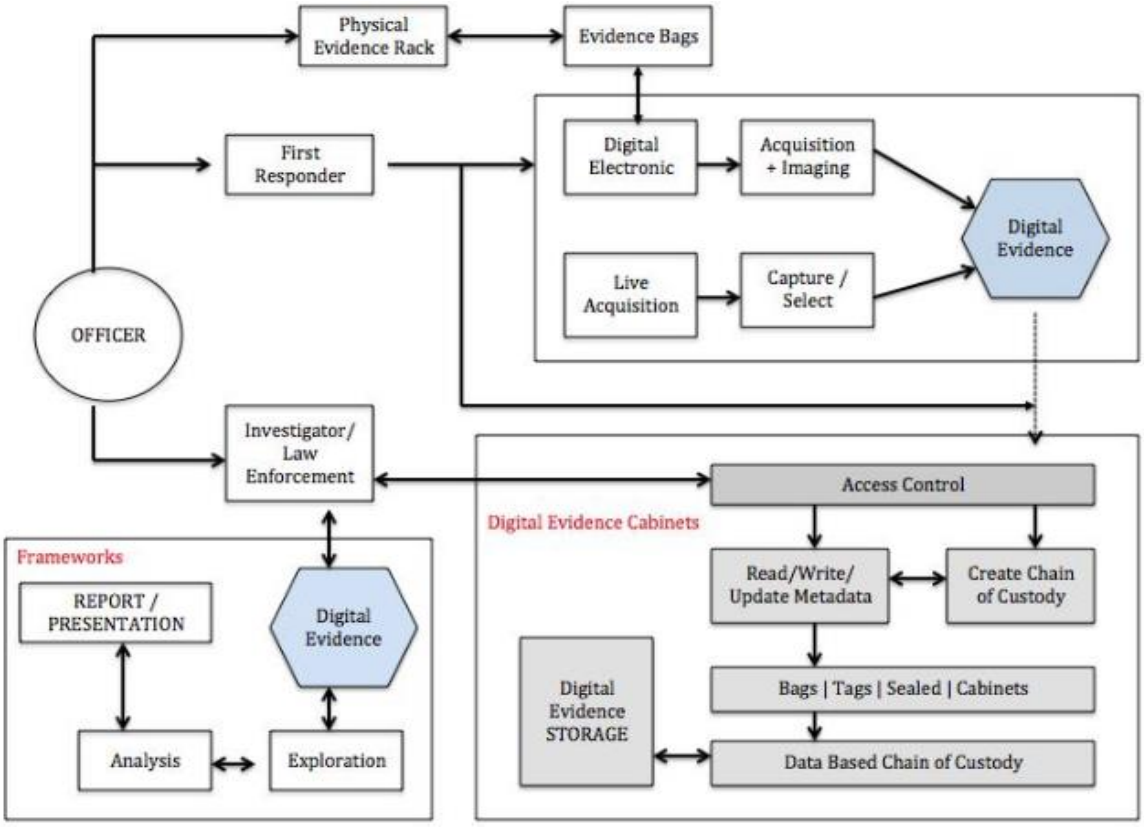


Figure 2.1 Digital Forensics Business Model (Prayudi et al. , 2015)

CHAPTER THREE:

RESEARCH METHODOLOGY

3.1 Introduction

This refers to the system of explicit rules and procedures upon which the research is based. It mainly consists of; research design and approach procedures, tools and techniques to be employed in data collection analysis and interpretation together with research validation and justification. (Kothari, 2004)in his studies underlines that researchers shouldn't only understand how to develop certain indices or tests, but rather how to apply the specific research expertise, but it's much needful for them to know which of these expertise are relevant and which aren't, and what they would refer to and indicate and why that. He (Kothari, 2004) focuses on the need to comprehend the suppositions hidden different systems and more so the need to know the criteria by which the researchers can choose the specific strategies and methodology relevant to specific issues and others won't. In this manner the requirement for every researcher to outline his approach for his issue as the same may vary from issue to issue. By descriptive study we will ensure that systematic and organized exercise.

3.2 Research Design and Approach

Exploratory and descriptive research study design will be used as there are few earlier studies that have been done and thus the need for the researcher to link the collected data to the original problem and the conclusions drawn at the end. The study will be accomplished by doing experiments and also by reviewing the existing literature so as to understand the information on Shellbags by both professionals and academia personalities. A pre study will be done to help inform on Shellbags so as to understand them fully and later an actual study so as to describe the findings on Shellbags as per the findings.

The actual study design shall involve an experiment process which shall provide data which can be manipulated by controlling the factors which are irrelevant to the research objective. Too reviewing works on Shellbags using Shellbags analysis tool Registry Decoder available in Open Source so as to establish the validity of the artifacts available towards building evidence so as to enhance computer security.

3.3 Data Sources and Collection Method/ Tools

For the useful incorporation of Shellbags artifacts in Digital Forensics investigations towards enhancing computer security we will review the tools used to carve Shellbags hives against their capability. The review of available literature from the developers and users of these tools against the evidence will provide the required data which will be sampled and analyzed towards achieving our sole objective of our study. This study is however limited to Windows Operating System and will not touch on any other Operating system. Practical experiments will also be conducted on these tools against DFI (Digital Forensic Image) acquire to justify the findings of the above study by the researcher as (Kothari, 2004) defines it. This choice has been selected due to the limited samples of inquiry towards the completion of this study.

This study is going to use secondary data sources which include literature review of frameworks, models, previous research works, journals, books and reports both from the internet and library while the primary data sources will include the expert views as data sources and the results that will be retrieved from the tools subjected to the same test environment.

It is critical to consider all the applicable factors before the last data collection arrangement is affirmed with a specific end goal so as to augment trust in the last results. The whole data collection exercise considered these four important variables that include background, primary, constant and uncontrollable variables.

i. Being able to identifying the background variables and their measure although they cannot be regulated but they fully impact the outcome of the experiment taking place.
ii. The ability to define the primary variables which are of interest to the researcher and entail the treatment and structure designs thus are referred to as factors. They are guided by the background variables and are a possible source of variation in the outcome of the experiment tool.
iii. The constant variables can be measured and are controlled but for this study they are held constant so as to increase the validity of the results as it reduces the strenuous cause of variation from being subject to the data. In this data collection plan, there are some of the variables that were held constant and they include:
    a. Restricting the experiment to one operator for each measuring device
    b. Doing all the required measurements at specific times and locations

iv. Uncontrollable variables they are evident in existence but cannot be manipulated due to conditions underlying. They create experimental errors which may result to less precise evaluations of both primary and background variables.

In the exercise, the following variables were held constant for all forensic and analysis tools on the source of digital evidence: - the successful load, the read and interpretation of binary data, recognition of different file systems, identifying the individual digital artifacts, parsing of the metadata from individual digital artifacts, grouping many digital artifacts based on the metadata and in an unrestricted way and finally understand the meaning of the metadata associated to a digital artifact.

In order to examine these proposition, we will conduct an experiment that will be discussed generally and then apply that to each of the Digital forensic and analysis tools and the Shellbags tools in turn so as to determine the outcome.

3.4 Data Collection Procedure

This involved the setting up of a Digital Forensic and Analysis Tool in an open environment which is subject to control parameters by the user that involved the forensic laptop which has the software running in it and the source drive which host the source image to be analyzed by the user. The same procedure was repeated for the Shellbags Analysis tools setup for the experiment. This exercise was repeated on the images that were used for analysis on both DFI and Shellbags analysis tools.

3.5 Data Analysis Method

Data collected will be reviewed, interpreted, tabulated, and presented in form of tables to help in drawing conclusions and doing recommendations after the end of study. This process will involve a practical analysis of computer images by applying the procedures and major steps defined in digital forensics investigation models and processes. They include the following:-

i. Pre-investigation (planning and authorization).
ii. Evidence identification and acquisition.
iii. Evidence transportation and storage.
iv. The analysis of evidence.
v. Studying results, documentation and reporting.
vi. Post-investigation and archiving of the results.

vii. Then the adoption of digital forensic results.

3.6 Research Validation and Test Parameters

In the evaluation of digital evidence and validation of the results, respective matrices need to be employed so as to provide accurate results despite the little information towards defining the matrices as (Flavien et al., 2014) found. This research will be justified using the results gathered by defining how the information acquired from a Digital Analysis exercise will be effective in addressing the study objective and answers to the raised research questions.

3.7 Experiment Setup

The environment for the investigation which is the test bed was setup whose specifications are as predefined in the figure below

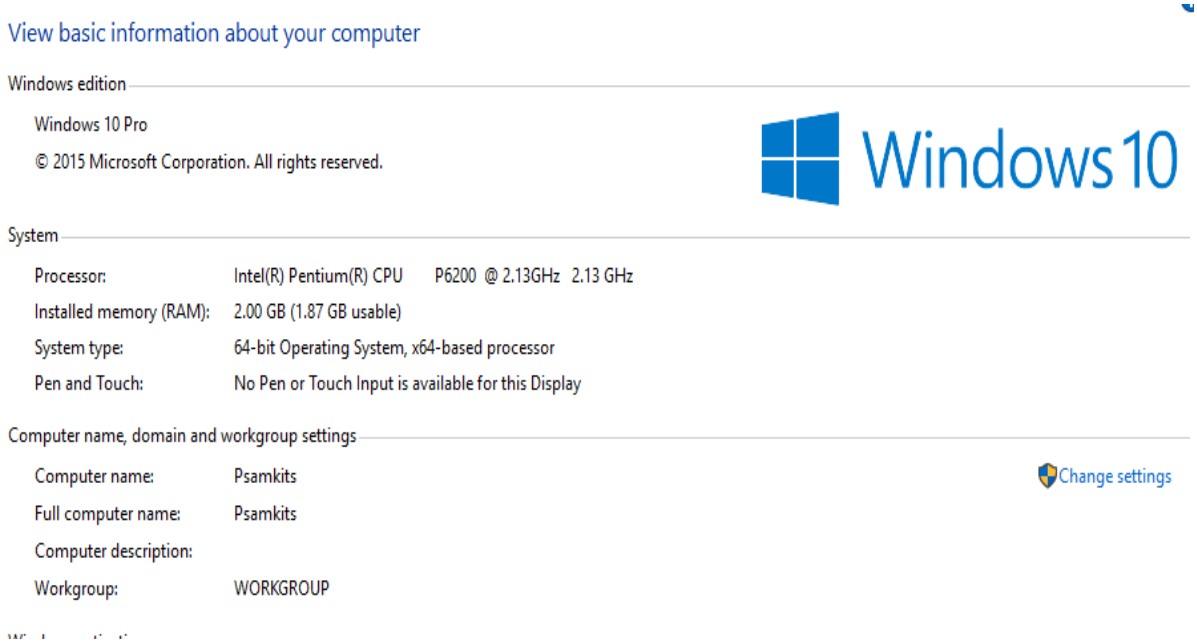


Figure 3.1 Experiment Setup

On the exercise a generic procedure on evidence acquisition was followed for the digital forensic tools to be used. The following is a description of the test drive that were carried out on the forensic tool.

Table 3.1 Defining matrices used for the exercise

S/No	Item Description	What Is Being Tested
1.	User profiles	Presence/Absence
2.	Email address/messages	Presence/Absence
3.	Activity timeline	Presence/Absence
4.	Hidden files	Presence/Absence
5.	Deleted files	Presence/Absence
6.	Recent documents	Presence/Absence
7.	Pictures and videos	Presence/Absence
8.	Downloads	Presence/Absence
9.	Web history	Presence/Absence
10.	Cookies	Presence/Absence

Note: test cases are set up and configured differently.

3.8 Limitations and Assumptions

The assumption is that different activities on the system by user result to different Shellbags artifacts being created. The limitation is that registry values have varying extensions that keep records of any changes made in the registry and thus this calls for the analysis of a Shellbags structure so as to provide a way to parse the data and convert it in to formats that are readable before analysis.

Any interference on the digital forensic tool at this point interrupts the whole process and thus renders the results inaccurate and irrelevant.

CHAPTER FOUR

DATA ANALYSIS

4.1 Introduction

In this chapter, we are summarizing and reporting on the findings from the performance of the DFI and Shellbags carving tools used. It includes the analysis of data as it is stipulated in the research methodology, then the presentation of the findings and a summary with the interpretations on the findings in relation to windows registry Shellbags information in reference to computer security. The literature review and the methodology offer guidance on the approach towards the objectives.

4.2 The Evaluation Tool in Action

The tests being done involved two universal images obtained from two drives and ensured the standard file extension .E0 file which is the standard image file that can be supported by major forensic tools and able to provide hash values that are realistic. The images used are as named

i. Nps-2008-Jean.E01
ii. Nps-2008-Jean.E02

These images are evaluated using a forensic tool whose selection was based on effectiveness on its performance based on accuracy and precision rates, absolute and relative speed and lastly reliability. Later on the same image were evaluated using a Shellbags carving tool whose selection was based on performance too.

The Digital forensic tool used for the exercise here is Autopsy – The sleuth Kit. This was based on its availability on the open source and its ability to analyze a Digital Forensic Image. On the other hand, the Shellbags carving tool experimented choice was the ability to acquire and analyze a Forensic component both on a live machine and offline in an image already acquired and carve the archives available.

Table 4.1 showing Image Nps-2008-jean.E01

Artifact	Autopsy (Freeware)	Registry Decoder (Freeware)
User Profiles	1	1
Email Address/Messages	1	1
Activity Timeline	1	1
Hidden Files	0	1
Deleted Files	1	1
Recent Documents	1	1
Pictures And Videos	1	1
Downloads	1	1
Web History	1	1
Cookies	1	1
Error detection	0	1
Date accessed	1	1
Bag path	0	1
Child Bags	0	1
Date created	1	1
First explored	0	1
Last explored	0	1
Last write time	1	1
MFT entry and number	0	1
MRU	0	1
Value	0	1

The analysis of Image Nps-2008-jean.E01using the Sleuth Kit Autopsy against Registry decoder

Key: 1 – means present 0 – means absent

Table 4.2 showing Image Nps-2008-jean.E02

Artifact	Autopsy (Freeware)	Registry Decoder (Freeware)
User Profiles	1	1
Email Address/Messages	1	1
Activity Timeline	1	1
Hidden Files	0	1
Deleted Files	1	1
Recent Documents	1	1
Pictures And Videos	1	1
Downloads	1	1
Web History	1	1
Cookies	1	1
Error detection	0	1
Date accessed	1	1
Bag path	0	1
Child Bags	0	1
Date created	1	1
First explored	0	1
Last explored	0	1
Last write time	1	1
MFT entry and number	0	1
MRU	0	1
Value	0	1

The analysis of Image Nps-2008-jean.E01 using the Sleuth Kit Autopsy against Registry decoder

Key: 1 – means present 0 – means absent

The events being presented include the after image acquisition exercise where and Investigator engages in evidence profiling to deliver on the predefined objectives. After the device which had Digital evidence has been extracted and run through a digital forensic tool, Shellbags parser is induced so as to retrieve and compile the user activities as held at the archives.

4.2.2. Retrieving Artifacts

This is meant for us to confirming forensic facts available in windows artifacts that can be retrieved using Shellbags tools unlike normal forensics tools. In this scenario we are able to define the forensics information available in Shellbags that cannot be retrieved using the normal forensics tools available and hence the reason why we should implement the use of forensics tools that can parse Shellbags for their advantage as they are highly rich in evidence that can support any forensics investigation outcome.

CHAPTER FIVE:

SUMMARY CONCLUSION AND RECOMMENDATION

5.1 Summary

Objective 1: To establish Shellbags artifacts available in the windows registry useful to a digital forensic investigator.

The experiment set up has been able to predefine the artifacts available in the windows registry after parsing them using the Shellbags forensics parsing tool as listed in the table 4.2.1 and 4.2.2 of this study and also in the appendices attached at the bottom of this document.

Objective 2: To determine the forensic information that can be retrieved from Shellbags artifacts during forensics analysis.

From the experiment we have conducted, it is evident that not all the information contained in the Shellbags hives is fundamental for any forensics investigation. Any forensics investigator is therefore required to filter the data retrieved from the Shellbags artifacts and retrieve all that information that is magnificent to the study towards delivering a sustainable secure and cyber free world as elaborated during the experiment that we carried out.

Objective 3: To incorporate Shellbags analysis skills to digital forensic models employed by forensic analysts.

As we conclude this study and achieved the above two objectives, it has been noted that Digital Forensics Investigators who are actively practicing do not carry out preventive forensic examination. This is because most cases where they are involved, entails the cross examination to retrieve forensic data that a certain investigator is looking for. This in return has been challenged in this study where by the experiment whereby we have defined that despite the security level we are undertaking the investigations. Shellbags have proved to provide very vital information that proves facts on any investigation which the ordinary forensic tools have been unable to retrieve thus making the whole exercise faster and robust. In this, it is very important for the practitioners to adopt the use of Shellbags artifacts for their exercises and this can be achieved by implementing models that appreciate their value in investigation.

It is evident that Shellbags parsing towards retrieving the artifacts available is not an easy task because we have seen the challenges that come with them thus care is required when

handling them because they are not the only thing one need to rely on for any forensics investigation. Also it is noted that the Shellbags parsing tools are not standardized and are developed with different capabilities and so is the data that they can retrieve during a given study. This means that the results retrieved are as a result of the tools capability and knowing how to use different tools, one knows their limitations and so they are able to make choices towards their deliverables. The study is revolving on the Shellbags artifacts leaving all other available artifacts being unexamined.

5.2 Conclusion

Digital forensic analysis and the parsing of Shellbags is not a difficult exercise, the shell parsing tools available online as open source and are easy to use, the important thing is to have interest to learn what the tool does, be able to interpret the output from the exercise fully and make use of the findings effectively towards being a good investigator.

This study concludes that digital forensic investigation is not all about the retrieval and production of electronic documents for analysis only after any subject investigations, but doing that extra mile of finding facts that can support the evidence retrieved for presentation towards strengthening the evidence available for a compound and strong case towards serving justice for computer and cyber security crimes that take place in the current digital age.

Digital forensic investigators poor assumption of forensic artifacts available in Shellbags has failed the field due to improper interpretation thus insincerity hence improper investigations by the practitioners. This in return does not serve justice to the victims of computer security breach and violations.

The knowledge of the digital forensic investigator to use Shellbags parsing tools may be limited. The limited knowledge hinders the investigators from being able to interpret the output and using the information effectively.

Bias of the study is on windows operating system environment leaving out the other available operating systems environments thus one is not able to tell whether Shellbags do exist on them or not and if they do, how they should be handled.

5.3 Suggestions and Recommendations for Further Research

Shellbags artifacts are not the only ones in the windows registry that have forensic information with value, there are other artifacts that exist and can work together with Shellbags. The study of Shellbags as forensic artifacts can help enrich the field of digital forensics.

Shellbags data structures are complicated and a lot of knowledge is required in this field so as to enhance the understanding, we therefore encourage forensic investigators to dig deep and study them for better understanding.

Shellbags parsing tools are not standardized, more work needs to be done on the models adopted towards their development so as to ensure standard operation procedures towards delivering standard results despite the parsing too used. There is also the need to develop forensic models that implement Shellbags analysis in them so as to deliver computer security services to our clients with no bias.

Most of the DFIs lack knowledge and are not eager learn how to use Shellbags parsing tools thus unable to interpret their output whereas learning how to use it makes one reliable and improves their investigation skills for these artifacts work together.

REFERENCES

AccessData. (2015). *Registry viewer.* Retrieved 2015, from www.accessdata.com/product-download/digital-forensics/registry-viewer-1-8-0-5

Ballenthin, W. (2014). *Windows Shellbag Forensics*. Retrieved 2015, from http://www.williballenthin.com/forensics/shellbags/

Bilby, D. (2006). Low Down and Dirty: Anti-forensic Rootkits. JAPAN: security-assesment.com.

Carvey, H. (2012). ShellBag Analysis. Windows Incidence Response.

Carvey, H. (2013). *Windows incident REsponse; Shell Item Artifacts, Reloaded*. Retrieved 2015, from http://windowsir.blogspot.ca/2013/10/shellitem-srtifacts-reloaded.html

Carvey, H. (2014). Registry Analysis. *Windows Forensic Analysis*.

Cheboi J, E. Abade. (2016). *Comparative evaluation of the effecivens of digital forensic tools used in kenya.* Nairobi: sci.uonbi.ac.ke.

DFS, D. F. (2015). *Registry Decoder.* Retrieved 2015, from www.digitalforensicssolutions.com/registrydecoder

Dr. Kim-kwang Raymond Choo, Ben Martin, Dareen Quick. (2013). Forensic and incidence response in the cloud. *Cloud Security Alliance.* Singapore: University of South Australia.

Flavien F,William J.B. ,Richard M, Bruce R, Adrian S. (2014). *Evaluating Digital Forensic Tools(DFTs).* Edinburgh: School of Computing, Edinburgh Napier University.

Garfinkel, S. L. (2007). Anti-forensics: Techniques, Detection and Countermeasures. nNaval Postgraduate School.

Guan, Y. (2007). *Digital Forensics; Research challanges and open problems*. Retrieved 06 28, 2015, from http://www.eng.iastate.edu/~guan

Key, S. (2015). *Digital Forensics Today; Parsing Windows ShellBags Using the ShelBags Parser EnScript*. Retrieved July 10, 2015, from http://encase-forensic-blog.guidancesoftware.com/2015/03/parsing-windows-shellbags-using.html

kilungu M., E. Abade. (2015). *An Investigation of Digital Forensic Models Applicable in the Public Sector (A case of Kenya National Audit Office).* Nairobi: sci.uonbi.ac.ke.

Kothari, C. (2004). *Research Methodology; Methods and Techiniques(secon d revised edition).* New Delhi: New Age International (P) Limited.

Ligh, Case, Levy, Walters. (2014). The Art of MEMORY FORENSICS. In C. Long (Ed.), *Detecting malware and threats in windows*, linux*, and mac* memory.* Indianapolis, Indiana-USA: John Wiley & Sons, Inc.

Lo, V. (2014). *Windows Shellbag Forensics in Depth.* Retrieved 2015, from http://www.sans.org/reading-room/whitepapers/forensics/windows-shellbags-forensics-in-depth-34545

Log2timeline. (2015, June 25). *Log2timeline CSV format.* Retrieved 2015, from http://log2timeline.net/

McQuaid, J. (2014a, June 18). *Investigating User Activity with Windows Artifacts in IEF*. Retrieved 2015, from www.magnetforensics.com/computer-forensics/investigating-user-activity-with-windows-artifacts-in-ief

McQuaid, J. (2014a, June 18). *Investigating User Activity with Windows Artifacts in IEF*. Retrieved 2015, from www.magnetforensics.com/computer-forensics/investigating-user-activity-with-windows-artifacts-in-ief

McQuaid, J. (2014b, August 7). *Forensics Analysis of Windows Shellbags.* Retrieved July 17, 2015, from http://www.magnetforensics.com/computer-forensics/forensic-analysis-of-windows-shellbags

McQuaid, J. (2014c). *Forensic analysis of prefetch files in windows*. Retrieved 2015, from http://www.magnetforensics.com/computer-forensics/forensic-analysis-of-prefetch-files-in-windows

Microsoft. (2015a). *Windows features and app; A History of Windows Features*.

Microsoft. (2015a). Windows features and app. *A History of Windows Features*.

Microsoft. (2015b). *Using Jump Lists to open programs and items*. Retrieved 2015, from http://windows.microsoft.com/en-us/windows7/using-jump-lists-to-open-programs-and-items

Microsoft. (2015b). *Using Jump Lists to open programs and items*. Retrieved 2015, from http://windows.microsoft.com/en-us/windows7/using-jump-lists-to-open-programs-and-items

Microsoft. (2015c). *Windows Registry files for network share*. Retrieved 2015, from https://social.technet.microsoft.com/Forums/windows/en-US/1ca8a9d3-6d78-4d9c-a97b-74484ef0ab69/windows-registry-file-for-network-shares

microsoft. (2015d). *Time zone Information Structure*. Retrieved 2015, from https://msdn.microsoft.com/en-us/library/windows/desktop/ms725481%28v=vs.85%29.aspx

Microsoft. (2015e). *Windows event log*. Retrieved 2015, from https://msdn.microsoft.com/en-us/library/windows/desktop/aa385780%28v=vs.85%29.aspx

Phelps, J. (2011). *PC World*. Retrieved 2015, from http://www.pcworld.com/article/241049/how_to_disable_windows_startup_programs.html

Pulega, D. (2013). *Shellbags Forensics: Addressing a misconception(Interpretation, step-by-step testing, new findings and more)*. Retrieved July 10, 2015, from http://www.4n6k.com/2013/12/shellbags-forensics-addressing.html

RegRipper. (2014). *RegRipper*. Retrieved 2015, from https://regripper.wordpress.com

Rouse, M. (2010). *LNK File Format*. Retrieved 2015, from http://whatis.techtarget.com/fileformat/LNK-Shortcut-file-Microsoft-Windows-9-x

Sentinel. (2010). *Sentinel Chiken Networks; RegLookup*. Retrieved 2015, from www.projects.sentinelchiken.org/reglookup/

SleuthKit. (2012). *Body file format.* Retrieved 2015, from http://log2timeline.net/

Tibury, C. (2011). *Computer Forensics Artifacts: Windows 7 Shellbags*. Retrieved 2015, from http://www.dfrws.org/2009/proceedings/p69-zhu.pdf

Tilbury, C. (2011). *Windows & Shellbags*. Retrieved 2015

TZWorks. (2015, Feb 7). *yaru-TZWorks ShellBag Parser (sbag) Users Guide.* Retrieved July 17, 2015, from http://www.tzworks.net/prototype_page.php?proto_id=14

WikiInformation. (2012). *File System*. Retrieved 2015, from https://en.wikipedia.org/wiki/File_system

wikimedia. (2015). *Operating System*. Retrieved 2015, from https://en.wikipedia.org/wiki/Operating_system

Wilson, P. J. (2013). *A Forensic Comparison: Windows 7 and Windows 8.* Retrieved 2015, from http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1974&context=theses

Yuandog, Gladyshev, Joshua. (2009). Using Shellbag information to reconstruct user Activities. Dublin: Elsevier.

Yudi Prayudi, Ahmad Ashari, Tri K Priyambodo. (October 2015). a Proposed digital forensic business model to support cybercrime investigaion in Indonesia. *I.J Computer Network and Information Security*, 1-8.

Yunus Yusoff, Roslan Ismail & Zainuddin Hassan. (June 2011). Common Phases of Computer Forensics Investigatiom Models. *Intrenational journal of computer science & information technology, Vol 3,* 1-3.

APPENDICES

ON THE LAUNCH

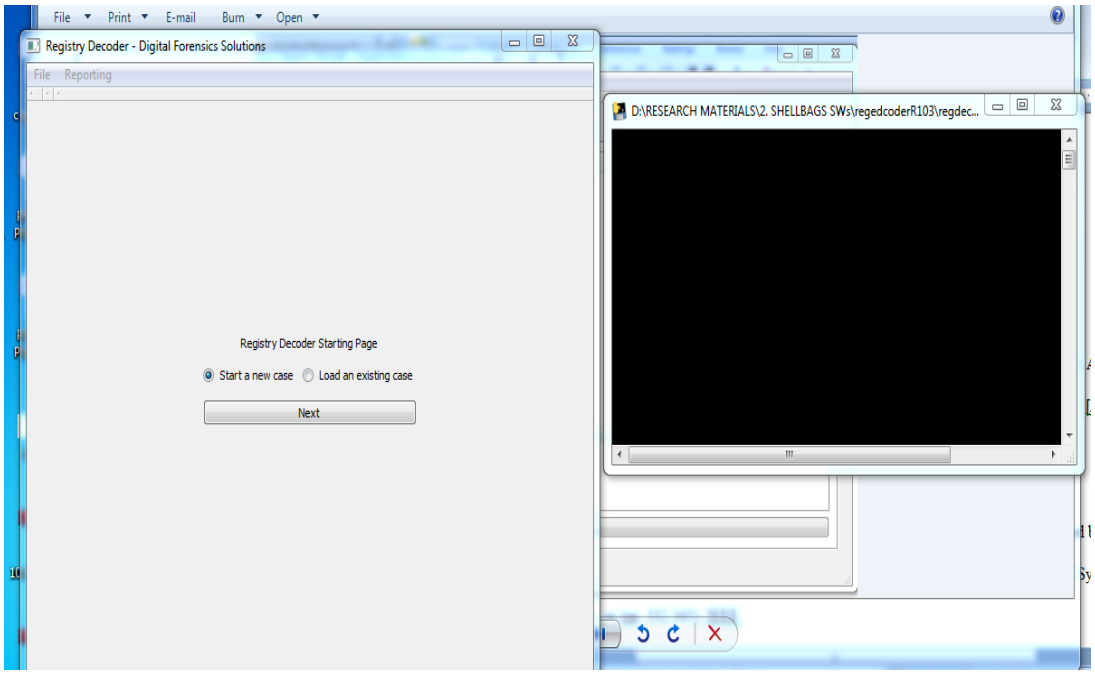
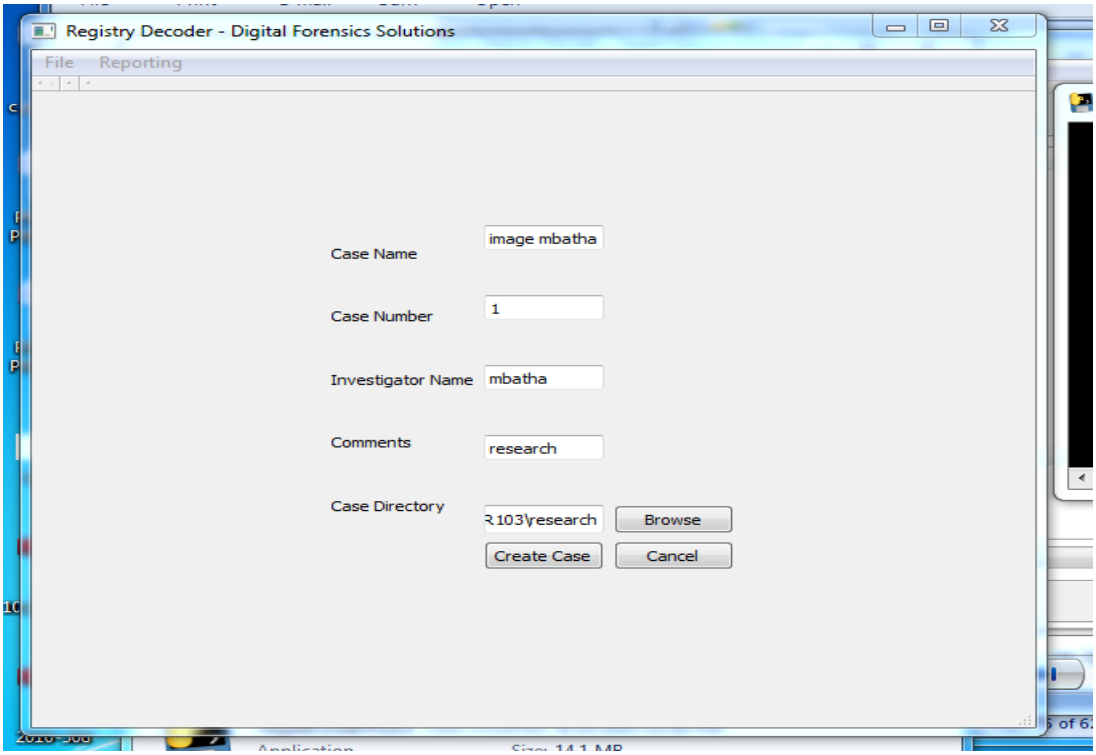
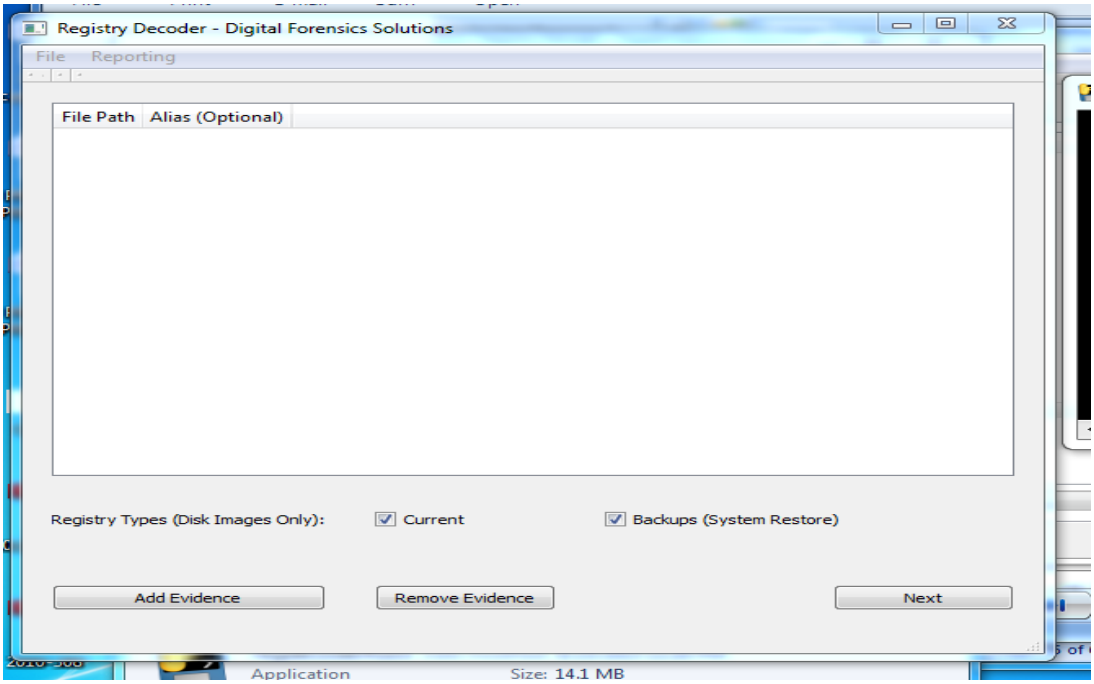


Figure 6.1 on the launch of a Shellbags analysis tool

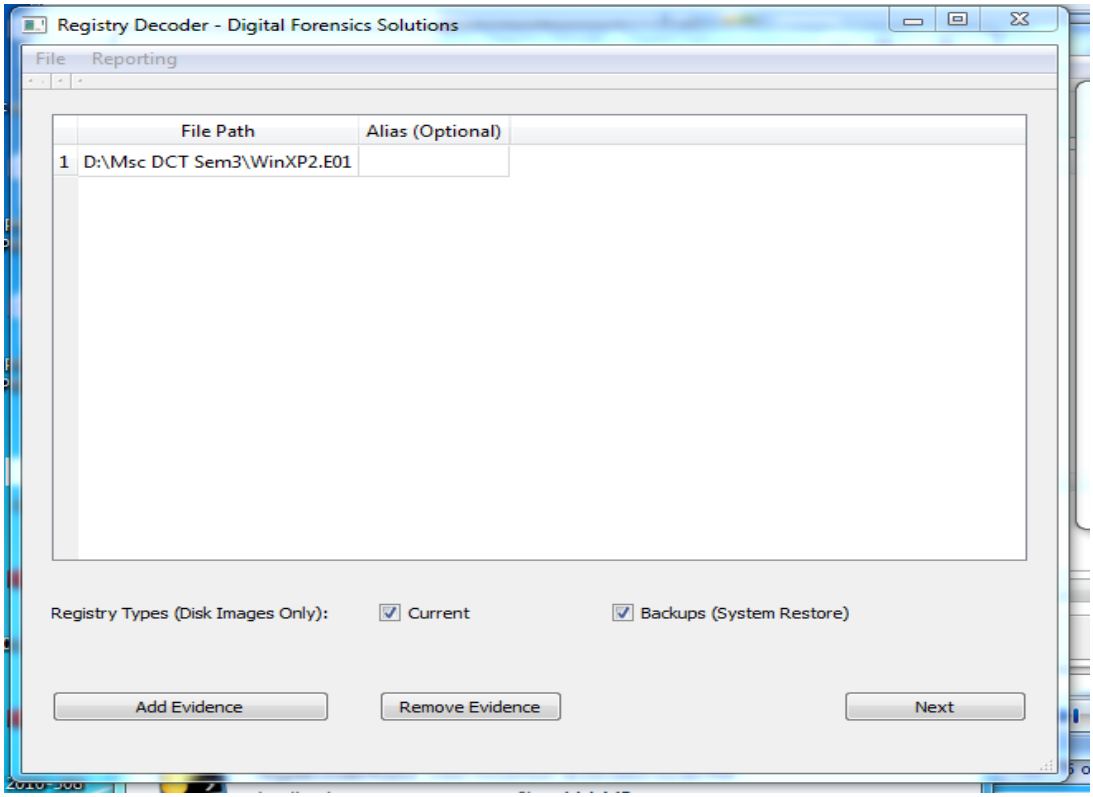
CREATING A NEW CASE



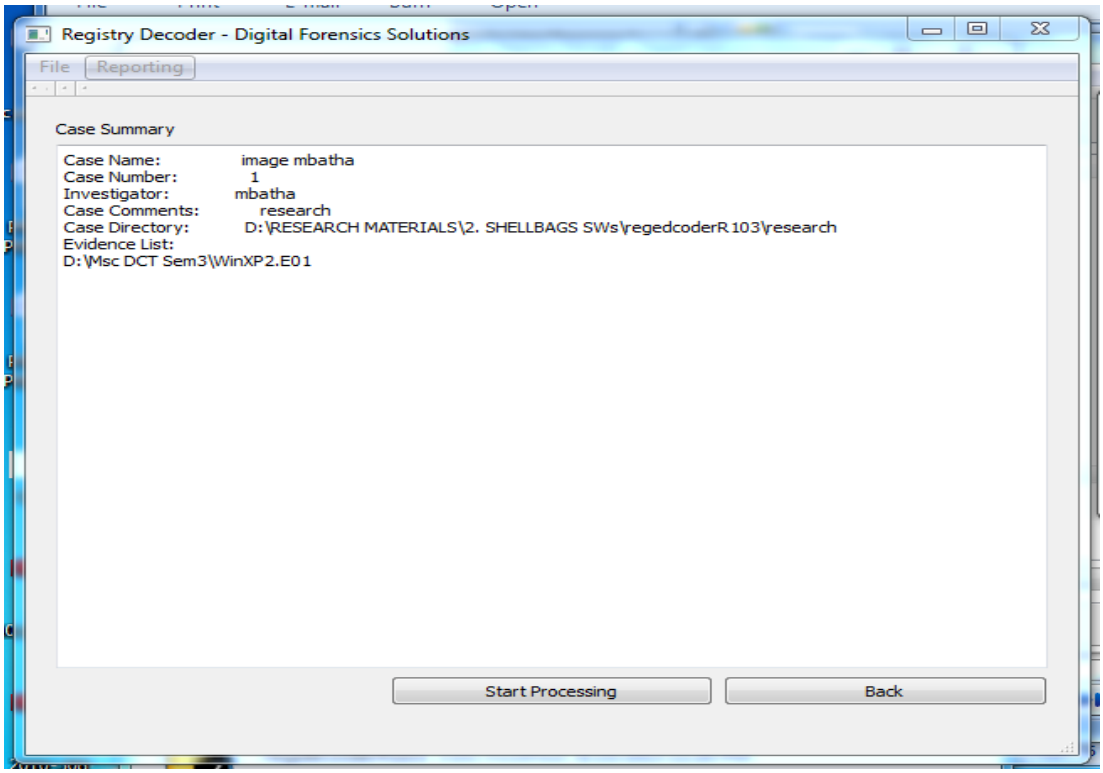
ADDING AND REMOVING EVIDENCE IN A TOOL



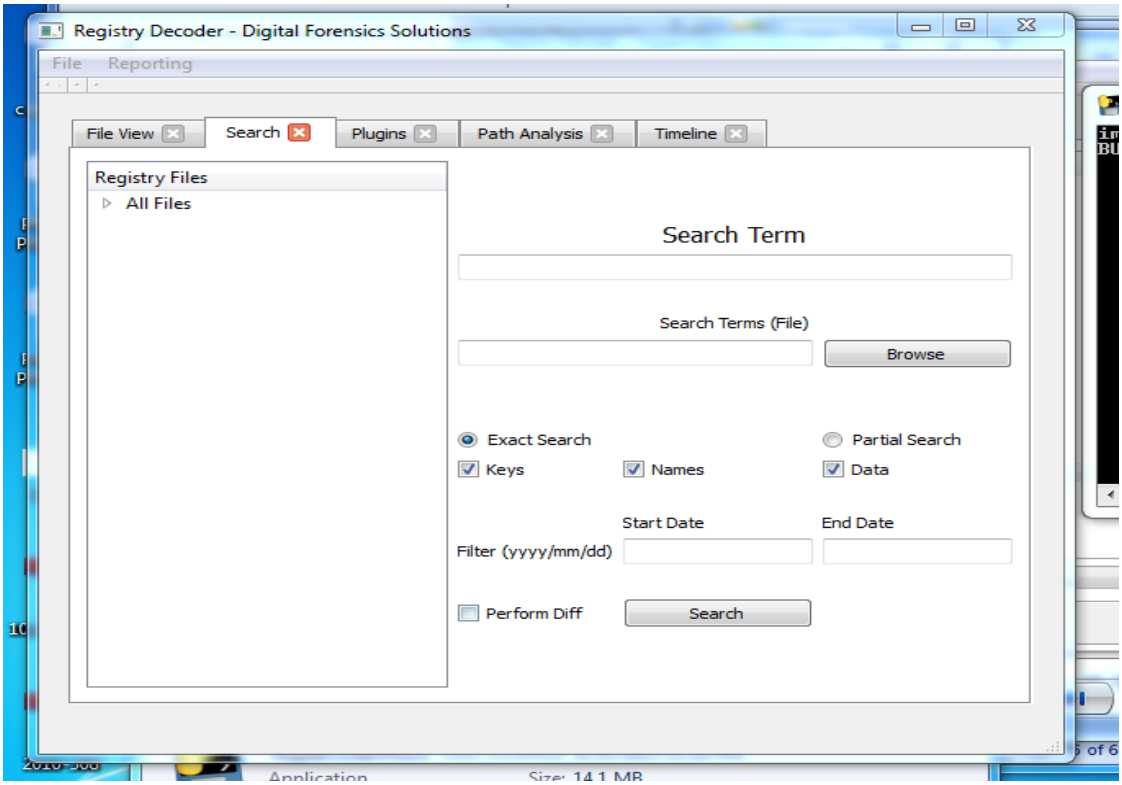
EVIDENCE ADDED



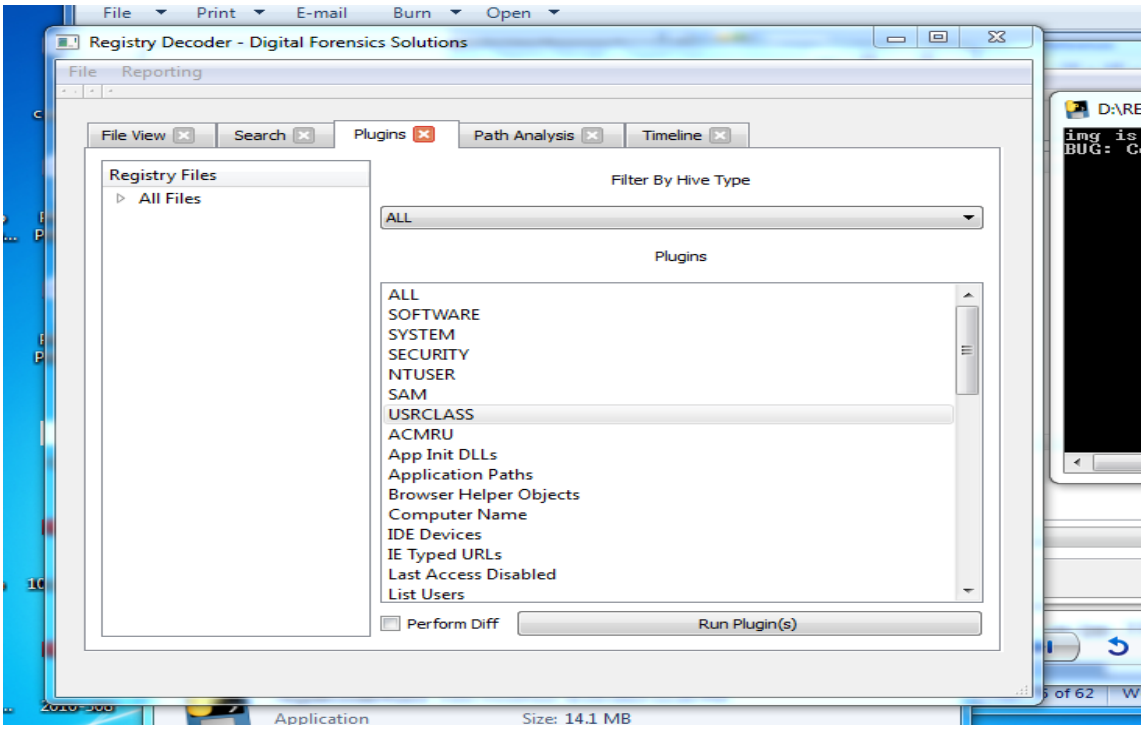
READY TO START



SEARCHING THE HIVES



PARSING THE HIVES PLUGINS



PARSING THE EVIDENCE PATH