RegForensicTool: Evidence Collection and Analysis of Windows Registry

Article · January 2016

DOI: 10.17781/P002064

1 author:

Dinesh Patil
Veermata Jijabai Technological Institute, India, Mumbai
8 PUBLICATIONS **8** CITATIONS

SEE PROFILE

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(2): 94-105
The Society of Digital Information and Wireless Communications, 2016 (ISSN: 2305-0012)

RegForensicTool: Evidence Collection and Analysis of Windows Registry

Dinesh N. Patil[1], Bandu B. Meshram[2]
Veermata Jijabai Technological Institute
Matunga, Mumbai, India
dinesh9371@gmail.com[1], bbmeshram@vjti.org.in[2]

ABSTRACT

The Registry works as a configuration database, maintaining the information needed for the running of the Computer System. In addition to this, the Registry is a source of evidence against the cyber crime as the details of the activity on the system is maintained in it. Therefore investigating the Registry can help to collect information relevant to the case. After considering existing research and tools, the paper suggests a new evidence collection and analysis methodology, RegForensicTool to aid in the process of Digital Forensic Investigation of Registry.

KEYWORDS

Registry, Registry key, Hives, Integrated analysis, Timeline

1 INTRODUCTION

The Registry is a wealth of information for both the administrator and the forensic investigator. The attacker of the Computer System performs various activities on it such as software installation, device connections, putting a malicious code, accessing documents and programs, network connections; the entries of their activities are made in the Registry. The investigator can get clues about the incident from these entries. The investigator has to perform the careful search in the Registry to find the potential evidence about the crime, analyzing that evidence can lead in finding the criminal, the time of the crime, the devices or software used in the crime.

The Microsoft operating system stores configuration data in the Registry. The Registry is a hierarchical database, which can be described as a central repository for configuration data or as a configuration database [1]. As the Windows was built on the MS-DOS, it becomes quite essential to discuss how the Registry comes into existence in Windows Operating Systems. MS-DOS does not have Registry and it got its configuration data from Config.sys and Autoexec.bat. The primary purpose of Config.sys was to load device drivers, and the primary purpose of Autoexec.bat was to run programs, set environment variables, and more, to prepare MS-DOS for use. Every application that ran on MS-DOS was responsible for managing its own settings. Neither of these configuration files is useful in Windows.

Windows 3.0 somewhat alleviated the limitations of Autoexec.bat and Config.sys by providing .INI files for storing settings [2]. .INI files are text files that contain one or more sections with one or more settings in each section. The main problems with .INI files are that they provide no hierarchy, storing binary values in them is cumbersome, and they provide no standard for storing similar types of settings. .INI file causes other subtle problems, all related to the configuration files inability to build complex relationships between applications and the operating system. Windows 3.1 introduced the Registry as a tool

for storing OLE (object linking and embedding) settings, and Windows 95 and Microsoft Windows NT 3.5 expanded the Registry into the configuration database that Windows XP and future versions of Windows use. A comparative study of some of the features introduced in the subsequent versions of Windows operating system and their associated keys in the Registry are listed in table1.

Table 1. Comparative Study of Registry

Features	**Operating Systems**			**Registry Key**	**Purpose**
	Windows 7	*Windows 8*	Windows 10		
Data Collection	X	X	✓	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\WMI\AutoLogger\AutoLogger-Diagtrack-Listener	Collect Users data and transfer to Microsoft
Start-up delay	X	✓	✓	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Seriali	Adding timing delay to start application
Internet User name	X	✓	✓	HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users\InternetUserName	To secure Microsoft account
Change User folder name	X	✓	X	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	Rename the user folder name
Hide Folder	X	✓	✓	HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer \ FolderDescriptions \ <FOLDER-GUID> \ PropertyBag\ThisPCPolicy	To remove default folders such as Documents, Pictures
Hibernate Disable	X	✓	✓	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power	To disable or enable hibernation
Hidden Files Display	✓	✓	✓	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced	To show the hidden files

Aside from being a central place to store settings, the Registry by its very nature allows complex relationships among different parts of Windows, applications, and the user interface. The user can access the Registry through graphical user interface (GUI) Registry editor such as regedit.exe or regedt32.exe. The GUI Registry editor can be opened by clicking on start and then typing run in the search dialog box and then typing regedit.exe or

regedt32.exe in the open dialog box of the run utility.

The forensic examiner needs to access the Registry in order to find out the forensic evidence of the various activities performed on the computer system. But the process of searching the Registry through regedit.exe or regedit32.exe consumes lots of time since the examiner is needed to search the entire Registry in order to find out the meaningful forensic information. Therefore, there is the need of a tool which can extract the required information from the Windows Registry along with the timeline and provide them to the forensic examiner in a presentable manner. The information thus extracted can help in convicting the cyber criminal. The expert user on accessing the system may modify or delete the information in the Registry to avoid from being caught this raises the need to identify if any changes to the Registry has been caused by the user. A study on the available existing tools which extract forensic data from the Registry has been performed. Based on the study of the existing tools, a new standalone, portable tool RegForensicTool has been proposed which overcomes the limitations in the existing tools.

This paper is organized as follows: A study of the existing research and tools which extract the forensic information's from the Registry has been performed in section 2. The detailed Registry analysis using proposed tool is performed in section 3. The software architecture, investigation procedure of the Registry implemented in the proposed tool along with the salient features of the tool is covered in section 4. To highlight the advantages of the proposed tool, a comparison is performed with the existing tools in section 5.The conclusion and the future work to be carried out are discussed in section 6.

2 RELATED RESEARCH

This section details out existing research on the Registry and the Registry tools which have been carried out to perform the forensic investigation of Registry.

2.1 Existing Research

Carvey H. [3] has provided the Windows Registry structure and performed the Registry analysis. The RegRipper tool to perform the forensic investigation of Registry is developed. Hipson P. [4] provided the detailed description of each and every key, sub key and their purpose in the Windows XP Registry. Jones A. et al. [5] discussed some of the keys in the Windows 7 Registry that are helpful to the forensic examiner. The forensic elements were categorized into five groups which are system, application, networks, attached devices, and the history lists. Based on these forensic elements a tool was proposed which can extract the forensic information specific to the category. Morgan T. [6] has provided an algorithm for recovering deleted keys, values, other structures in the context of the Registry as a whole. Russinovich M. [7] has provided the internal details of the Windows Registry. Saidi R. et al. [8] performed the analysis of the Registry focused on detecting unwanted applications or unauthorized access to the machine with regard to the user activity via the VNC connection for the potential evidence of illegal activities. Carvey H. [9], [10] have identified the potential location for the forensic information within the Registry.

2.2 Existing Tools

The various Registry tools and their features are as follows:

Autoruns

This utility provided as part of the Windows Sysinternals by the Microsoft gives the information about the programs which start running during system bootup or login and

when you run various Windows applications. These programs and drivers information are extracted from the Run, RunOnce, services Registry keys.

Autorunsc

This utility provided as part of the Windows Sysinternals gives the information about the programs which run automatically based on the information extracted from the Run key. It does not provide GUI to the user.

ProDiscoverBasic

This tool provides the facility of viewing the Registry. The selection of the evidence has to be done manually.

OSForensic

This tool opens the ntuser.dat, default, SAM, software, security, system hives for the investigation. The evidence is needed to find out manually. One of the features of this tool is that it provides the last modification date of a key. OSForensic is a complete toolkit providing the facilities for memory view, deleted file search, raw disk view, recent activity, the dump of physical memory, verifying and creating a hash.

MuiCacheView

The tool automatically extracts the newly installed application name and its executable file path from a Registry key MuiCache. This helps the forensic examiner in knowing about any erroneous programs running on the system.

USBDEVIEW

This utility provides the information about the USB devices that are currently connected to your Computer System and the USB devices whichever previously connected. It also provides the facility for enabling or disabling a USB device.

Regshot

This utility allows taking the snapshot of a Registry and compares it with another snapshot earlier taken. This helps in detecting any changes to a particular key.

KUSTAR

This tool covers five user's activity on the system as mentioned in [5]. The evidence about the activity are extracted from the Windows Registry and displayed on the GUI.

The summary of the above Registry tool is as in table 2.

Table 2. Registry Tool Summary

Tool	**Function**					
	Integrated Analysis	Timeline Analysis	Activity Analysis	Registry Compare	GUI support	Any other feature
RegForensicTool (Proposed)	✓	✓	✓	✓	✓	Running process, service, dll
AutoRun	X	✓	✓	X	✓	Only covers autorun activity
AutoRunsc	X	✓	✓	X	X	Only covers autorun activity
ProDiscoverBasic	X	X	X	X	✓	Registry view
OSForensic	X	✓	✓	X	✓	Registry view
MuiCacheView	X	X	✓	X	X	Only covers MuiCache Registry key
USBDEVIEW	X	X	✓	X	X	Only covers USB devices
Regshot	X	X	X	✓	✓	
KUSTAR	X	X	✓	X	✓	

3 EVIDENCE COLLECTION USING PROPOSED TOOL

The forensic investigator should be able to analyze the activities of the user when performing the investigation and in doing so the timing of the activities is needed to be considered to establish the correlation between the time and the activity. As the details of the user's activities are recorded in the Registry of the Windows based Computer System; the user with technical knowledge may delete the traces of his or her activity in the Registry. In such a situation, the forensic investigator should find out if the Registry hive files were modified. In addition, the investigator should be able to investigate the Registry hive files stored in the seized hard disk of the computer system which was used to commit the crime.

However, the previous Registry forensic tools provided limited facilities for performing the forensic analysis of Windows Registry. For these reasons a new evidence collection and analysis methodology is required. This methodology performs integrated Registry analysis, timeline analysis and extracts the information that is useful for the digital forensic analysis of the Registry

3.1 Integrated Analysis

As discussed in section 2.2, no tool is found to be robust for the entire Registry forensic. The cyber crime cell generally used to seize the hard disk of the computer which is used for crime purpose. The forensic investigator has the responsibility to find out the possible traces of evidence against the criminal. The Windows based computer system stores the Registry hive files in the location SystemRoot%\System32\Config\ of the hard disk. During the booting process of the computer, the configuration manager uses these hive files to construct the hierarchical database called as Registry.

The proposed RegForensicTool provides the facility for extracting the forensic evidence from the hive files stored in the external hard disk. This hard disk is needed to be connected to the computer system having RegForensicTool which loads the external Registry hive in the Registry of the running system to extract the evidence.

The proposed tool also performs Local Registry forensic which involves extracting the information from the Registry about the various activity performed by the user on the system, on which the tool is running.

The forensic investigator will be able to examine and extract the forensic evidence from the Registry of various operating systems using this tool. The tool has been tested on Windows XP, Windows 7, and Windows 8.

3.2 Analysis of User Activity

The existing tools provide a few number of functionality in extracting the forensic information from the Registry. A facility which is found in one tool may not be available in another tool. It means that the forensic examiner will have to use a different tool for different purposes, increasing the time and cost of doing the forensic investigation. This has stimulated the need of having a Registry forensic tool which can extract the forensic data from the Windows Registry based on the various activities being performed by the user and generate a report of the evidence for further use.

The proposed RegForensicTool covers the various activities as discussed in [11], which are

performed on the Computer system. These activities include:

- Autorun programs running on the system
- Recently accessed documents/programs,
- Applications installed on the system
- Network connected
- Devices connected to the system
- Last login activity of the user
- Malware activity

The detail of these activities is as follows:

The Autorun programs running on the system

The program which gets run automatically when the operating system is booted is stored in the Run key. This key helps in identifying any unknown autorun programs running on the system. The Run key path is as below:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Recently Accessed documents and programs

The Recent Docs key provides the Information about the documents that the user has recently accessed, the forensic examiner can know about the documents in which the user has interest. The RecentDocs path is shown below:

HKEY_CURRENT_USER\SoftwarenMicrosoft\Windows\CurrentVersion\Explorer\RecentDocs

The RunMRU key provides the information about the recently used programs by the user. The path for this key is as below:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Applications installed on the system

The uninstall key provides the information about the software installed on the system. It also provides the information about the installation location and the location where the traces of the files that are created when the application is uninstalled gets stored. The RegisteredApplications key provides the list of the application that is registered with the Window Operating system. This key helps in identifying if there are any unregistered applications installed in the system. Below is a path to the Uninstall key and RegisteredApplications.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications

Network connected or accessed

The information about the network used by the user is maintained in the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles

The details of the network connections currently active can also be obtained by the netstat command.

Devices connected to the System

The list of the hardware devices attached to the system is available with the following keys. The devices that have been used by the malicious insiders to commit a crime can be known.

HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System

HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP

The USBSTOR key provides the list of various USB devices that have been connected to the system. If a particular device subkey is exported as a text file then we can get the last connection time of the USB device. In addition to this USB device information such as vendor, version information can be known.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

Last Login Activity of the user

The date and time of the last logon performed by the user can be obtained using last logon

command. This command is executed using cmd.exe. The last logged in user information is stored in the LogonUI key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI

Malware Activity

When a malware run, the operating system creates a value in the MuiCache, as a result of how the malware was being launched within the testing environment. And some malware run as a service. Their presence can be identified by the services key:

HKEY_CURRENT_USER\SoftwarenClasses\LocalSettings\MuiCache\31\52C64B7E

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

3.3 Comparison of Registry Hive files

The malicious user after performing the crime, in order to clear the traces of activity, may delete or alter the values, key or sub keys from the Registry. It stresses the importance of having the comparison between the current Registry hive file and the backup hive file to identify the potential location in the Registry that was affected.

The tool such as RegShot provides only the facility of comparison between hives. The methodology used by the RegForensicTool is to compare the backup of the Registry hive file such as ntuser, software, system, default, SAM, security one by one with the respective hive file in the current working Registry. For each comparison, the dissimilarity if any is identified. If dissimilarity is found then the forensic investigator can predict the approach used by the criminal to commit the crime.

3.4 Timeline Analysis

The digital forensic investigator should detect the activity being performed by the suspect along a timeline. By performing the timeline analysis, the investigator can trace the sequence of events that were performed by the suspect. For instance, if the suspect had accessed a word document by logging using a login Id, the date and time of these activities can be correlated to convict the suspect. The forensic report obtained as in Figure 1 shows LAB_3_one user had logged in at 03:01PM on 02/07/2016 and accessed the .doc file 'Advanced Evidence Collection and Analysis of Windows Registry' at 03:05PM. This forensic information can be evidence against the LAB_3_one user for accessing the .doc file as the .doc file was accessed after the login time by LAB_3_one user and before the shutdown of the system. The forensic report thus obtained using the RegForensicTool underlines the importance of performing the timeline analysis of the activities.

4 TOOL DEVELOPMENT

The RegForensicTool is built using QT4, a cross-platform application frame-work that is widely used for developing application software that can run on various software and hardware platforms with little or no change in the underlying code base while having the power and speed of native applications. Qt uses standard C++ with extensions including signals and slots that simplify handling of events, and this helps in the development of both GUI and server applications which receive their own set of event information and should process them accordingly. The RegForensicTool uses QSetting class and its methods to extract the informations from the Windows Registry.

The software architecture of the RegForensicTool is illustrated in Figure 2. The analysis of local Registry and the external hard disk hive file can be performed using RegForensicTool. The evidence and time of the activity are extracted and the report is generated for correlating the sequence of events and their

timings. The comparison of Registry performs the comparison between backup Registry hive files and the current Registry hive files of the running system.

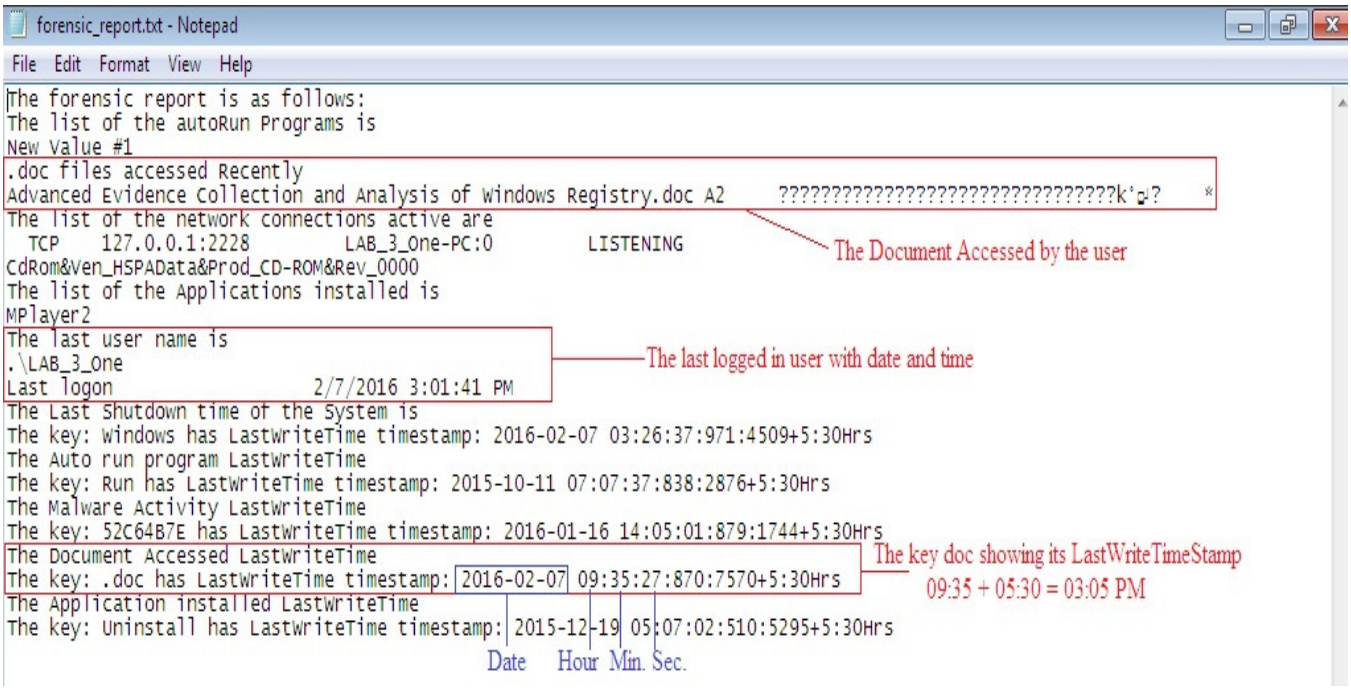

Figure 1. A snapshot of the forensic report using RegForensicTool

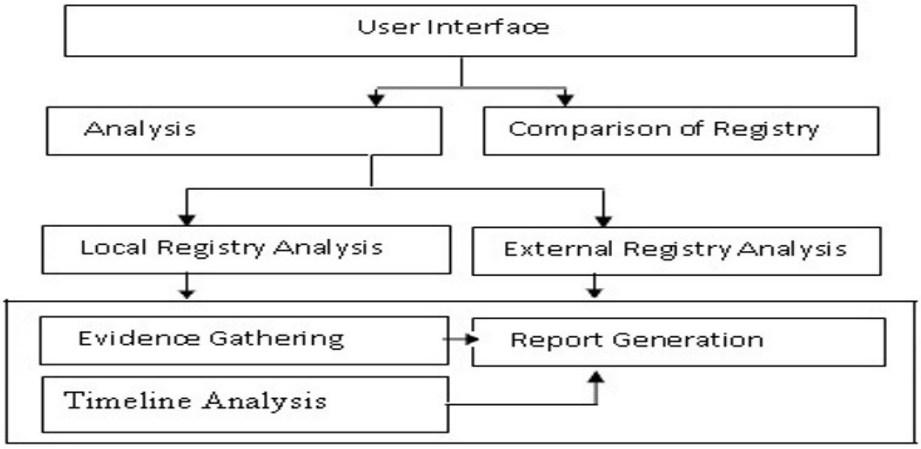

Figure 2. RegForensicTool Software Architecture

The screenshots of the RegForensicTool is shown in Figure 3 and 4.

The salient features of the RegForensicTool are as follows:

- Portable

- Standalone Application
- Ease to use
- GUI support
- Inter process communication
- Covers most of the forensically important activity such as Autorun program, recent Accessed documents/programs, network accessed or connected, devices connected, applications installed, login activity, malware activity.
- Facility for drag and drop of evidence for a user activity extracted from the Registry key
- Facility for backup of individual Registry hives and entire Registry.
- Facility for obtaining information about running processes, services and dlls on the system.
- Facility for timestamp generation of Registry key.

The overall process of investigating the Windows Registry that is achieved using RegForensicTool is summarized in Figure 5.

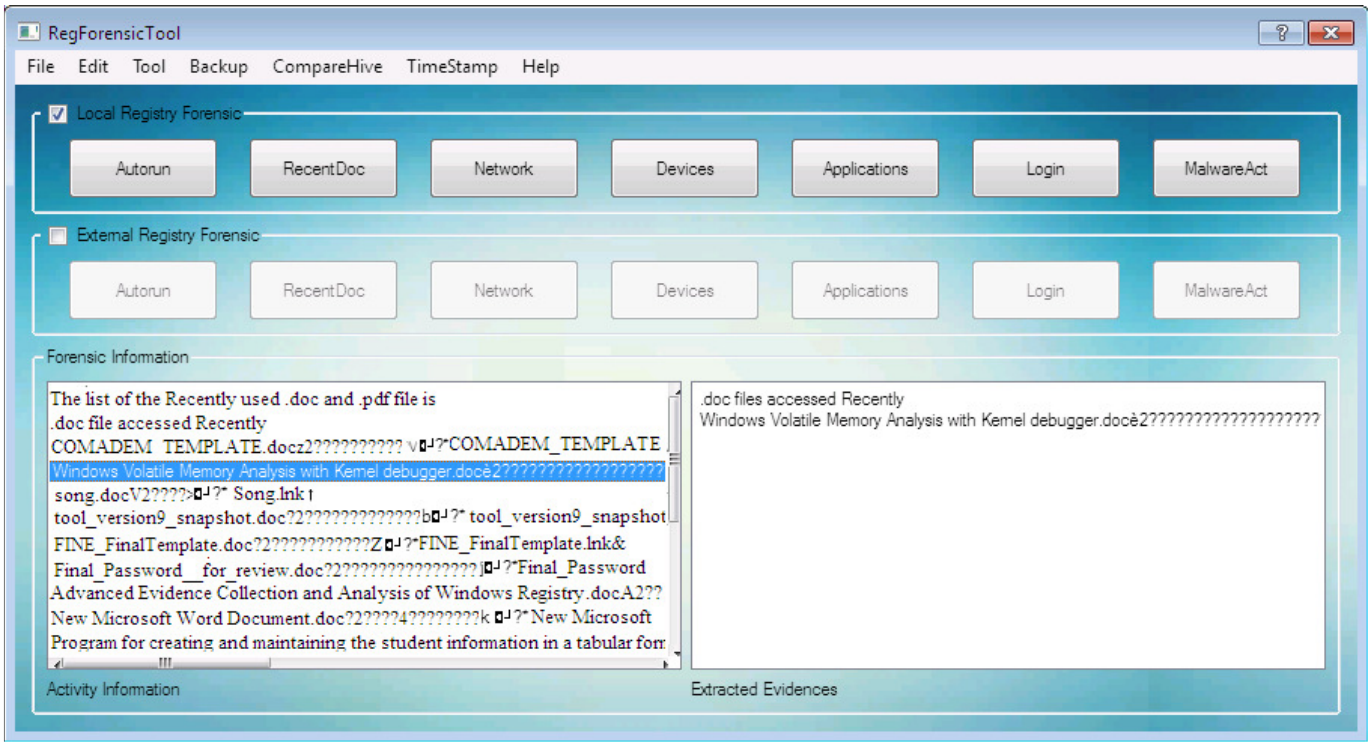

Figure 3. RegForensicTool showing recent accessed document

In addition to the forensic information about the various activities as discussed above, the forensic investigator can extract the information about the running processes, services, DLL, on the host machine of the RegForensicTool and generate the report about the evidence if any from the various user activities in the .txt file.

5 FUNCTIONAL COMPARISONS WITH EXISTING TOOLS

The comparison between the existing Registry forensic tools and the RegForensicTool is performed. The results are shown in table 2.

The functions for comparison were selected based on the advanced requirements mentioned in this paper. The tools such as Autorun, Autorunsc provides the details about the autorun programs. ProDiscoverBasic, OSForensic tool gives the entire Registry view but these tools do not have the features for extracting specific forensic information. USBDEVIEW lists the USB devices connected to the system. RegShot compares the Registry hives. The existing tools do not cover most of the user's activity for extracting the forensic evidence. Also, none of the tools have provided the facility for performing the forensic investigation of Registry hive files on the external hard disk.

The proposed RegForensicTool provides the improvement over the shortcoming of the existing tools. This tool extracts the forensic evidence for most of the user's activities on the system along with the timeline. The tool also provides the facility for extracting the evidence from the Registry hive files present in the external hard disk. It also identifies if any changes have occurred to the current Registry using the backup of the Registry.

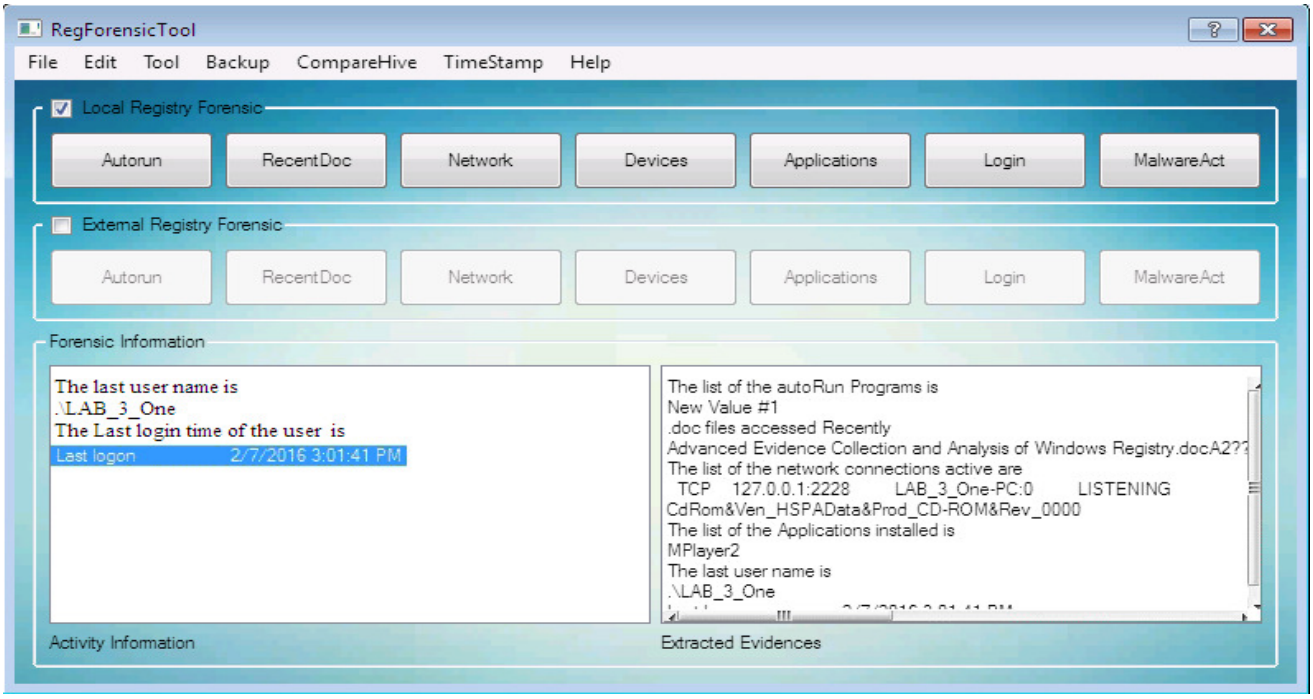

Figure 4. RegForensicTool showing extracted evidences

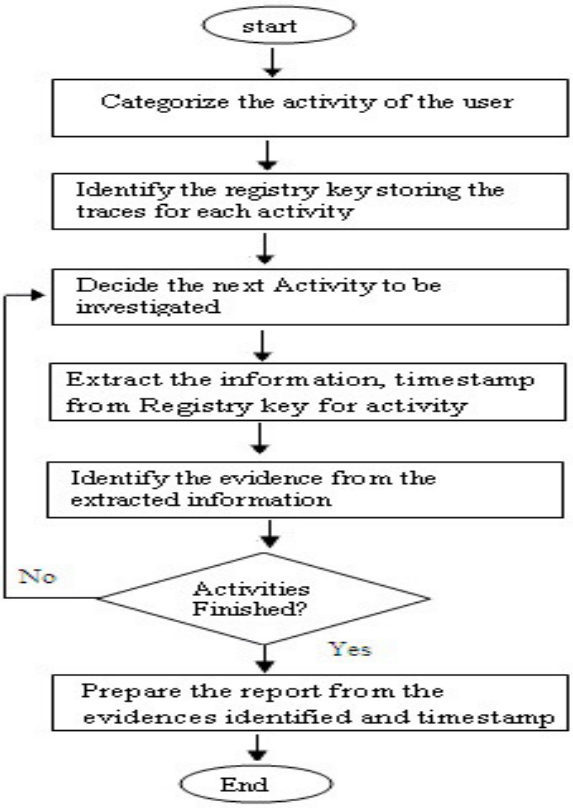

Figure 5. Registry Investigation Procedure

6 CONCLUSIONS

The Registry maintains historical information about user activity. All of this information can be extremely valuable to a forensic analyst, particularly when attempting to establish the timeline of activity on a system. It is essential to perform the analysis of Registry and use timeline analysis to detect the suspicious activities of the suspect. A wide range of cases would benefit greatly from information derived or extracted from the Registry.

A survey on the existing Registry forensic tools revealed that they extract very little forensic information from the Registry. Comparatively, the RegForensicTool provides more evidence from the Windows Registry as that of the existing tools; saving the cost, time and effort in searching the evidence. The RegForensicTool also covers forensic analysis of the hives files on the external hard disk, thus enabling the forensic investigator to conduct the forensic investigation without changing the setup.

This work has focused on some of the activities that are being performed on the system and extraction of the evidence about these activities. In the future, more activities will be identified and the key for these in Windows10 Registry will be located in order to get more evidences against cyber crime and the criminal.

7 REFERENCES

1. Microsoft: Windows registry information for advanced users, http://support.microsoft.com/kb/256986 (2013).
2. HoneyCutt, H.: Microsoft windows registry guide, 2nd ed. Microsoft Press (2005).

3. Carvey, H.: Windows forensics analysis, Syngress publication (2011).
4. Hipson, P.: Mastering windows xp registry, SYBEX Inc.,(2002).
5. Alghai, K., Jones, A., Martin T.: Forensic analysis of the windows7 registry, In Proc. 2010 8th Australian digital Forensic conference, pp. 8-24, SECAU, Perth (2010).
6. Morgan, T.: Recovering deleted data from the windows registry, Digital Investigation (2005).
7. Russinovich M..: Inside the registry, WindowsItPro Magazine (1999).
8. Saidi R., Ahmad S., Noor N., Yunos R.: Windows registry analysis for forensic investigation, IEEE (2013).
9. Carvey H.: The windows registry as a forensic resource, Digital Investigation, 2(3), pp. 201-205 (2005).
10. Carvey, H.: Windows forensics and incident recovery, Addison Wesley (2004).
11. Patil, D., Meshram, B.: Forensic investigation of user activities on Windows7 and Ubuntu12 operating system, IJIET, 5(3) (2015).