International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Disk based Forensics Analysis

Premchand Ambhore †, Archana Wankhade† and B.B.Meshram#

†Information Technology Government College of Engineering, Amravati, India
†Computer Science and Engineering Department V.J.T.I. Mumbai, India

Received 12 Feb 2018, Accepted 15 April 2018, Available online 19 April 2018, **Vol.8, No.2 (March/April 2018)**

Abstract

Today computer systems have become integral part of our life. Its penetration in personal and organizational level has increased rapidly in last couple of years. Majority of data is now present in digital form which includes personal data like photos & videos, government documents, secrete and confidential reports of organizations, etc. This change in technology is also adopted by criminals to perform their illegal activities. Use of computers for performing crimes has increased therefore it has become necessary for investigator to collect and process evidences from suspect's computer. Windows 7 has become mainstream operating system for users and thus its forensics investigation is becoming important. There are various places in Windows 7 which can be used in forensics analysis; some of the areas of interest are windows registry and the underlying NTFS file system. Registry contains valuable information that can be helpful for the forensics analysis. Registry contains the basic information like date when Operating System installed, owner name and the advanced information such as the software installed on system, history of recently used documents and so on, which will help the analyst to decide the way of further analysis of system depending on the its environment. The NTFS file system is native file system for Microsoft's Windows 7 which is used to manage files present on disk. Suspect can hide data in the file system using its Alternate Data Streams feature. He/She can also remove evidence present on disk by deleting files containing evidences. It is important for forensic investigator to get back the evidences from hidden and deleted files by suspect. In this paper we have proposed and implemented tool that will be useful for performing forensics analysis of windows 7 registry, underlying NTFS file systems Alternate Data Streams and recovery of deleted files. This tool will helps in saving efforts and time of investigator in its investigation.

Keywords: *Ntfs, Windows OS, Data, Collecting, Preserving, Analyzing.*

1. Introduction

This paper includes the basic overview of computer forensics and its need in current world, the background and motivation behind the windows 7 forensics analysis followed by the statement of problem and important modules with their description.

2. What is Computer Forensics?

Computer Forensics is the investigation of computer system that is suspected to being involved in committing criminal activity (or victim of criminal activity) by extracting useful and related information that is important for the case under study and can be presented as evidence in court of law. It is the art and science of applying computer science knowledge and skills to aid the legal process. Collecting, Preserving, Analyzing, and presenting digital artifacts are the primary goals of Computer Forensics. To goals are achieved efficiently by using various software and tools are used according to pre-defined procedures, to extract and protect computer related crime evidence.

Need for Computer Forensics

Today computer systems have become integral part of our life. Its penetration in personal and organizational level has increased rapidly in last couple of years. Majority of data is now present in digital form which includes personal data like photos & videos, government documents, secrete and confidential reports of organizations, etc. This change in technology is also adopted by criminals to perform their illegal activities. Criminals use computer systems to commit crimes and may also try to destroy evidences to avoid detection of their illegal activity, therefore there is a need to analyze and utilize evidences stored on and transmitted using computer

*Corresponding author's ORCID ID: 0000-0002-3776-582X
DOI: https://doi.org/10.14741/ijcet/v.8.2.33

system to catch the criminal. Computer forensics helps in gathering and processing of digital evidences in a way that their integrity will not be compromised. Without proper knowledge of computer forensics the data may get accidently corrupted or destroyed and will not be accepted in law of court as evidence

3. Background and Motivation

Operating systems provides user a way to interact with the computer system. There are various operating systems exists for computer system, such as Macintosh OS X and Ubuntu, Microsoft's Windows operating systems, but windows operating systems remain the most popular and used by majority of users across the world. There are various versions of Microsoft's windows operating system available to choose from some of which (Windows 95, Windows 98, Windows XP) are outdated and/or they are no longer supported by Microsoft. Windows Vista and Windows 7 are the currently being supported and Microsoft's latest operating system Windows 8 is not released at the time of writing. Windows Vista was not a major success for Microsoft and most of the users migrated to Windows 7 after its launch. Today Microsoft's Windows 7 operating system is the mainstream operating system for majority of users in home as well as organizations. Thus is it more likely that it is involved in or victim of computer related crime and the forensics investigator will come across its forensic analysis. The various changes in the structure and working of this new operating system have impact on collecting and analyzing data from this operating system. These changes in operating system produce opportunities and challenges for forensic investigator to gather digital evidences. Windows registry is one of the places which contain a lot of useful information that can be used in forensics analysis, but is overlooked because of its complex structure and lack of proper documentation. Another place is Microsoft's Windows 7 underlying NFTS file system which is used to store user's data. Both of these are very important in forensics analysis of windows 7 machine. This motivates us to do research in this field of Windows 7 forensics analysis and its underlying NTFS file system to develop tools which will help in the investigation process.

4. Statement of Problem

There are various places of evidences in Windows 7 Operating system. For proper forensic analysis of windows 7 system we need proper understanding of NTFS file system, the 'artefacts' generated by Windows 7 with their location and use of good tool. Our aim is to provide a tool that will help in forensics investigation of windows 7machine. In this paper we have proposed and implemented tool for forensics analysis of windows 7 registry and its NTFS file system. This paper has five important modules: A.RegAnalyzer Module, B.Clone Disk Module,C.ADS Examiner Modul D.True Recovery Module Detail description of each module is given below: E.Activity Module

RegAnalyzer Module

Most of the users are ignorant about the wooing of the system, therefore leaving footprints of their activity on the system and mainly in the registry. Analysing that info gives forensic investigator initial information about the system environment and direction for further analysis. Due to registry's complex structure it is very difficult and time consuming to extract required evidences. To overcome these difficulties, this module will automate task of windows 7 Registry analysis for forensics investigator. This will supplement traditional registry analysis can give investigator an edge in forensic analysis by hiding unrelated information and highlighting the important information from registry and will reduce the large amount investigation time spent on analysis of Windows Registry.

Clone Disk Module

It is important to make multiple copies of evidence which will be used later in dead forensics analysis. This module helps in acquisition process by allowing making of raw copy/image of Hard Disk, USB Pen Drives which can be used later for forensics analysis.

ADS Examiner Module

NTFS file system's Alternate Data Streams feature allows the user to hide data in the file system, thus the forensic investigator cannot neglect this fact while doing forensic investigation of windows machines having NTFS file system. The Alternate Data Streams present in deleted file are also having the same importance, but may get overlooked as it is less known in forensic experts. This module helps to find out data hidden in Alternate Data Streams at various Locations like file, folder, partition, as well as the data present in Alternate Date Streams of deleted files.

True Recovery Module

Data stored in the files is the main source of evidence in computer forensics. The file system is used to manage these files present on disk. A suspect can remove evidence present on disk by deleting files containing evidences. It is important for forensic investigator to get back the evidences deleted by suspect. This module helps forensics investigator to recover deleted files on hard disk or USB pen drives formatted using NTFS file system.

Activity Module

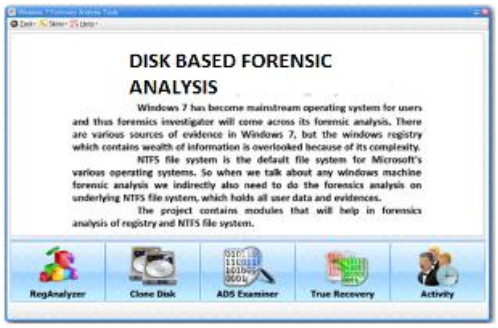
Analysing the time when computer system is ON and the user who is logged in at that time can provide

useful information that can be correlated to other evidences. Example: Deleted file time of file on NTFS file system can be correlated with user who was logged in at that time to identify which user has deleted the files. This module helps forensics investigator to analyse user activity on the system by displaying time line of user log on and log off events.

Conclusion

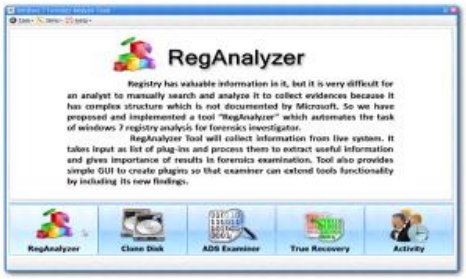
Computer forensics is needed in today's world as it is involved in number of cybercrimes. As windows 7 is widely used operating system it is important to analyse its artefacts like registry, log files and its NTFS file system in forensics investigation. Tools speed up the process of analysis, so there is need develop tools that will help in forensics investigation. So we have proposed and implemented tool for forensics analysis of windows 7 system. Our project will help the forensic investigator for saving time & effort in performing computer forensic investigation of windows 7 registry and NTFS file system on windows 7 machine. Manually searching artifacts to find evidences which are related to case under consideration is very time consuming and inefficient way to performing forensic analysis on large amount of data. Good tools make this job easier by automating the process of finding related evidences. In this chapter we have shown the implementation of the tool that we have proposed and implemented, with the help of tool's screen shots and by describing how to use the tool.

Screen shots of Windows 7 Forensics Analysis Tool



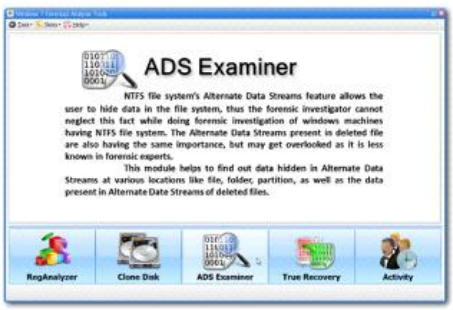
Screen shot 1: Main GUI for Forensics Analysis Tool

Screen shot 2: Information of RegAnalyzer Module



Screen shot 3: Information of Clone Dis

Screen shot 4: Information of ADS Examiner Module



Screen shot 5: Information of True Recovery

Screen shot 6: GUI of Plugin Creator

To create plugging first choose the registry hive in which the desired information is located. Then enter the registry key path whose values are to be processed. If possible give particular values as comma separated list. If not enter 'Process All' in the Value field. This will process all the values present under particular registry key. Give the description about the plugin so that it will be easier to understand its forensics

importance. Finally click on 'Create Plugin' button, this will ask for the location where the plugin will be saved and kept for future use.

References

R. D. Pittman and D. Shaver, Windows Forensic Analysis, in Handbook of Digital Forensics and Investigation,

H. Carvey, Windows Forensic Analysis DVD Toolkit 2E, Burlington, MA, Syngress Publishing, Inc., 2009, pp. 299-320.

Paul McFedries, Microsoft Windows 7 Unleashed (United States of America,Library of Congress Cataloging-in-Publication Data, 2009) 225-244.

B. Carrier, File System Forensic Analysis, Addison Wesley Professional, 2005.

Philipp, D. Cowen and C. Davis, Hacking Exposed Computer Forensics, 2nd ed., McGraw-Hill, 2005.

B. Sheldon, Forensic Analysis of Windows Systems, in Handbook of Computer Crime Investigation Forensic Tools and Technology, E. Casey, Ed., Great Britain, Academic Press, 2003, pp. 133-166.

Brendan Dolan-Gavitt, Forensic analysis of the Windows registry in memory, Digital Investigation 5, 2008, S26-S32.

Timothy D. Morgan, Recovering deleted data from the Windows registry, Digital Investigation 5, 2008, S33-S41.

Huebner, D. Bem and C. K. Wee, Data hiding in the NTFS filesystem, Digital Investigation the International Journal of Digital Forensics & Incident Response, vol. 3,no. 4, pp. 211-226

D. D. Hayes, V. Reddy and S. Qureshi,(2010) The Impact of Microsoft's Windows 7 on Computer forensics examinations, in Applications and Technology Conference (LISAT), Long Island Systems,

Darren Hayes, Vijay Reddy, (2010) Shareq Qureshi, The Impact of Microsoft's Windows 7 on Computer Forensics Examinations, Proc. Applications and Technology Conference, Farmingdale, NY, 1-6.

Muhammad Yasin, Muhammad Arif Wahla, Firdous Kausar,(2009) Analysis of Download Accelerator Plus (DAP) for Forensic Artefacts, Proc. Fifth International Conference on IT Security Incident Management and IT Forensics, , 142-152.

Z. Kai, C. En and G. Qinquan,(2010) Analysis and Implementation of NTFS File System Based on Computer Forensics, in the Second International Workshop on Education Technology and Computer Science, Wuhan, Hubei, China.

J. Davis, J. MacLean and D. Dampier,(2010) Methods of Information Hiding and Detection in File Systems, in SADFE 2010, Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA,.

I. Martini, A. Zaharis and C. Ilioudis,(2008) Detecting and Manipulating Compressed Alternate Data Streams in a Forensics Investigation, in WDFIA, Third International Annual Workshop on Digital Forensics and Incident Analysis, Malaga, Spain,.

Mirza,(2008.) Looking for Digital Evidence in Windows, in Biometrics and Security Technologies, ISBAST

Yoo, J. Park, J. Bang and S. Lee(2010) A Study on a Carving Method for Deleted NTFS Compressed Files, in Human-Centric Computing (HumanCom), 3rd International Conference, Cebu, Philippines, 2010.

L. Naiqi, W. Zhongshan, H. Yujie and Q. Ke, (2008) Computer Forensics Research and Implementation Based on NTFS File System, in ISECS International Colloquium on Computing, Communication, Control, and Management, Guangzhou,.

J. Bang, B. Yoo, J. Kim and S. Lee,(2009) Analysis of Time Information for Digital Investigation, in Fifth International Joint Conference on INC, IMS, and IDC, Saut, Korea,.

Muhammad Yasin, Muhammad Arif Wahla, Firdous Kausar,(2009) Analysis of Download Accelerator Plus (DAP) for Forensic Artefacts, Proc. Fifth International Conference on IT Security Incident Management and IT Forensics, ,pp 142-152.

Ronald C. Dodge, (2008) Skype Fingerprint, Proc. 41st Hawaii International Conference on System Sciences,