A Review on Forensic Significance of Windows 10 Operating System

[1]Sakshi Pandey
M.Sc. Forensic Science
Galgotias University
Greater Noida, 203201, India.

[2]Dr Mamta Pal
Associate Professor,
Division of Forensic Science ,
School of Basic and Applied Science,
Galgotias University,
Greater Noida, 203201, India.

ABSTRACT- In this modern era of computers and mobile phones, where every hand has reach to digital world, we all are very much vulnerable to cyber-crimes and as computer technology continues to evolve, the task of managing and handling personal and sensitive information has become more and more challenging with each passing day. Therefore, with the increasing demand of computer security in recent times, it has become more important than ever to look-up to digital forensic technology. Digital Forensics is referred to a branch of forensic science that deals with the digital information, storage and carrying of evidence in the investigation. It can be categorized into different domains depending on the type of investigation required, one such domain is Windows forensics, which is popular now-a-days due to newly released and latest operating systems. At present, Windows 10 is one of the most popular windows having different types of features, and is the most extensively used operating system today that contains many programs and mechanisms for managing computer hardware and software. In the world of forensic science, such records are known as windows artifacts, which can be described as a system generated records of the user activities that have forensic value. In this review paper, we have discussed about the details of Windows Forensic, its artifacts and its vital information involving different tools. Therefore, this paper provides solution for investigating the artifacts left by user, which can correlate to the criminal or malicious activities of users.

KEYWORDS - Windows 10, Operating System, Windows Artefacts, Cyber Forensic, Cyber forensic tools.

INTRODUCTION

Crimes are increasing day by day. The criminals are freely committing crimes without the fear of hold because they know we don't have enough resources to grab them easily. Crimes are increasing in every directions. Now, Criminal has entered to the Computer world .As we know that computer has become the essential part of daily day- to- day life. It's importance has increased in all directions like in Institution, in Offices, in Industries and etc. Computers are used in scientific research vastly and it is an important tool. Research process can also be done with the help of computers. It has lots of storage devices like floppy discs, compact discs and auxiliary memories. Data can be used from these storage devices. This storage data can be used for singular phases of research process(1). In this present time computer systems have become additional and essential part of our life. Its access in personal and organizational level has increased quickly in last couple of years. As we know that we are living in digital World as well as Digital India so the crime related to digital forensic is also increasing very fast. Now, Criminals have also entered in the Digital forensic and therefore, the crime related to Computer is increasing very fast. Digital Forensics is a branch of forensic science, which is concerned with the acquisition and analysis of materials that are found on computer devices which can be used for illegal purposes like hacking, cyber stalking, impersonification, fraud and the production and attainment of child exploitation material. Bulk of data is now present in digital form that includes personal data like photos & videos, government documents, secrete and confidential reports of organizations, etc (7). Digital forensics has been developed in such a way of forensics methologies based on scientific discoveries. According to the individuality of evidence, digital forensics can be divided into two types of evidences like

static and dynamic forensics evidence. The static evidence is stored in the computer system with independent disks and other storage media. In the case of the cyber attacks, it analyses the computer systems which have been attacked using a variety of technologies and methods (14). As day- by- day technology has developed the focus has extensive to include the recovery of evidence from any device that has a digital storage capability. That is why, the role of digital forensics has stimulated from the investigation of computer-based crimes such as hacking, cyber attacks, cyber stalking, frauds and etc. In the recent past, investigators of conventional crimes did not understand the latent value of digital evidence (9). This is really important to understand the value of digital forensic as well as digital evidence too. There are common types of digital evidence investigated including images, text, video and audio files in code. For the criminal investigations, digital forensic investigation techniques are adopted for the purpose of security incident response and management of business-critical systems. The captured binary data was more commonly known as digital evidence. Forensic analysis of computer systems can performed with specialized computer forensic tools to find the integrity of the evidence. In this paper we have to study about the forensic significance of Windows 10 artefacts. Windows 10 was launched in July 2015 and it was reformed version of Windows 7 and Windows 8. Windows 10 is the operating system, which consists the features of the windows that have released in last previous years so it has become the series of all operating systems. With Windows 10 the most notable change from previous versions was the idea of having single platform for smartphones tablets and desktops. The windows 10 operating system is the latest version from Microsoft, which comes with many features like continuum, cortana, notification center, Microsoft edge, multi tasking, universal apps etc(6). Artefacts was found changed in the Windows 10 when it was compared with the previous versions of Windows like windows 7 and windows 8. Each version of Windows operating systems contained many different artifacts that Windows 10, forensic investigators must examine it in order to determine the changes implemented from Windows 8.1 and the addition of new artefacts. . Windows 10 has become the most usable windows operating system that is very easy to use because it has found there are lots of similar features when it is compared with windows 7. It starts and works fast in the comparison of previous windows that was time taken and windows 10 has more security features that keeps safe our information , personal details and some important files also. Windows 10 has released new features like Task View that is a virtual desktop system, Microsoft Edge web browser and other new applications and additional support for fingerprint as well as face recognition login, new security features for undertaking environments and for the rectification of operating system's graphic capabilities for games, it has also introduced DirectX 12 and WDDM 2.0. Windows 10 education edition is meant for educational institutions, students, teachers, and administrators (5). The tools used in Windows 10: VMware Fusion, FTK Imager, Process Monitor, Process Explorer, ESEDatabase View and Registry Explorer. The other sources for evidence location for forensic analysis are random access memory (RAM), memory files, connected pen drive and its file system, valuable artifacts of windows operating system, windows registry hives, web browsers, email and social networking applications installed on the systems. Jump Lists was the feature which was released with windows 7 in July 2009 and this feature is still continued with the latest version of windows which is windows 10. Jump Lists are the features those are created with the help of software applications with which a user can find or jump directly to the recent opened files and folders.

Material and Methodology- For the examination of windows artefacts there are different types of tools used Like-

1. AccessData FTK- FTK Imager is a Windows acquisition tool that includes in various forensics toolkits, such as Helix and the SANS SIFT Workstation. With the help of this tool, we try to obtain a forensic image of a USB drive with FTK Imager. As we know that in every forensic investigation , should never work with the real evidence, so we should never use USB drive and its content. But we should work with a copy of the real evidence, which can be an exact replica of the original means we need a bit by bit copy of the original evidence.

2. Autopsy- Autopsy, tool which is used for gathering the information about the user which can be used as evidence in criminal cases. Gathering information about the users is known as Cortona which means 'storing information'.Autopsy is an open source forensics tool that allows forensics investigators to analyze disk images and report many types of information. Autopsy is build upon 'The Sleuth Kit' set of command line tools. By using Autopsy, we can conduct keyword searches, file artifacts and fragments of files in common locations etc. And also write custom Java and Python modules that can be easily added and shared with others.

3.RegEdit-Windows registry is an important hierarchical database for the configuration of operating system and most of programs. It contains abundant information which have potential evidential value in Forensic analysis. Windows registry is one that can be used as editor to access windows registry. The Registry tool is like a wealth of information for both the administrator as well as forensic investigator. The attacker or hacker of the Computer System performs various activities on it such as software installation, device connections, putting a malicious code, accessing documents programs and network connections.

4.**Magnet Axiom**-Magnet Axiom is a complete digital investigation platform which allows examiners to acquire and analyze data, as well as share findings. This can be help to learn about capabilities and features of live systems and it can also analyse the cloud/drive .So it is 'all in one' tool.

5. **Encase Forensic**- EnCase Forensic is a tool that enables to collect data and conduct complex large scale investigations from beginning to end. EnCase Forensic was designed to be used for collecting evidence. This software comes in several designed for Forensics, Cyber security, security analystics and for e- discovery use.

6. **OSForensic**-This tool opens the mistake, Security Account Manager(SAM), software, security, system hives for the investigation. One of the most important features of this tool is that it provides the last modification date of a key. OSForensic is a tool having complete features to provide the potential for memory view, raw disk view, deleted file search, recent activity, the junkyard of physical memory and it also verifies hash.

Forensic Analysis- The forensic analysis is done on the artifacts generated by windows registry artifacts, windows memory artifacts and operating system artifacts.

1.Registry -Registry files cannot be examined directly that is why they have to obtained through 'FTK Imager' and restore with the associated deleted registry records through 'Registry Explorer' and examine all registry hives.

Artifacts- Last logon timestamp, Last password changed timestamp, Last opened and visited folders, Recently opened files, Auto-run & start-up apps, Mounted USB devices, Last modified registry hives, Hardware configuration, Installed software applications, Connected printers, windows account username, password hint and profile pictures etc.

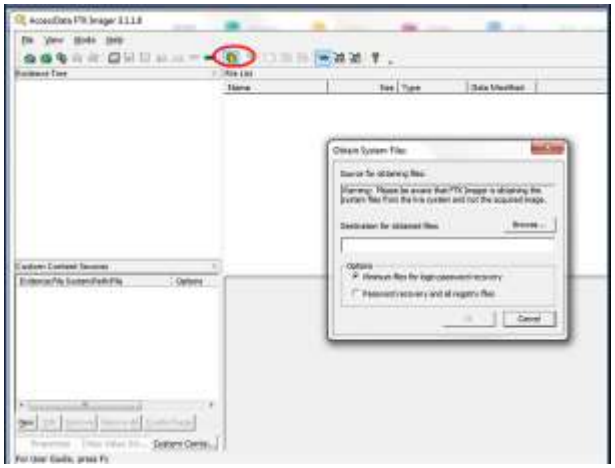

Fig.1 system protected files (registry)[online (https://www.litigationsupporttipofthenight.com/single-post/2017/01/30/FTK-Imager---Copying-Protected-Registry-Files**)]**

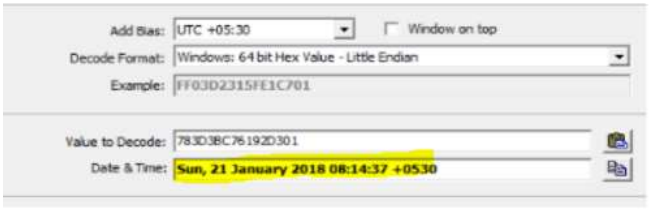

Fig2-last password changed timestamp decoded from SAM\Domain\Accounts\Users(Ratna Sri, M. Seetharama Prasad(2019) An investigation into the forensic significance of the Windows 10 Operating System ISSN: 2277-3878, Volume-7

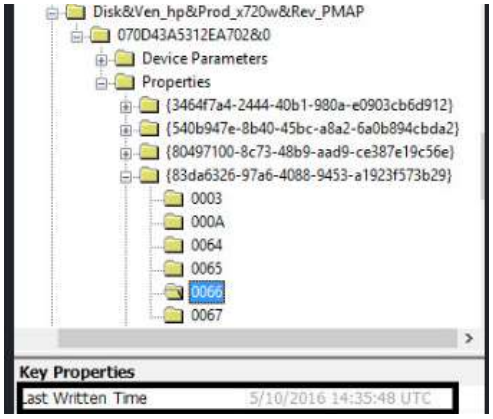

Fig.3mounted USB devices along with last inserted timestamp [online (**https://doi.org/10.1111/1556-4029.13596**)]

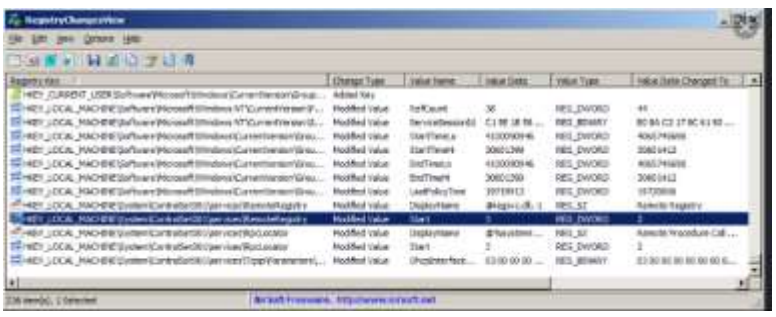

Fig4-screenshot index - last modified registry key value, extracted from regscanner tool [Online (https://www.computerhope.com/jargon/r/registry.htm)]

2. Windows memory artifacts-

Artifacts-RAM, hiber file, page file, swap file.

These artifacts have given a lots of information during the investigation process. Random access memory contains evidence like username, passwords, URLs visited. Hiber file gives data like played songs on windows OS, opened images and movies. Page file gives email id, IP addresses, voice mail messages, downloaded torrents and swap file contains information like screenshots captured, inserted pen drives and the opened files from it. It also records the traces of forensic investigations carried out. Capturing RAM is done using the forensic tool 'RAM Capturer' by Belkasoft whereas hiber, page and swap files are analysed using the Magnet AXIOM (commercial).

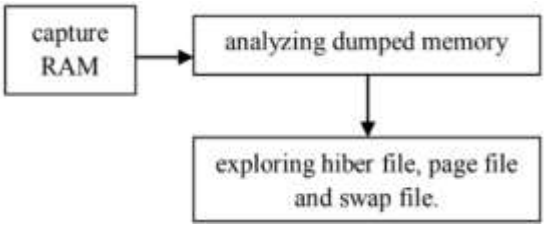

Fig-Procedure for forensic analysis of the windows memory

3.Operating System

Artifacts- Recycle bin data, event logs, LNK files, Jumplists, Prefetch files, Thumbcache files and etc.

Recycle bin– When a file is deleted from the system, it will be moved to the security identifier folder (SID). These files will either begin with $R and $I. $R contains the actual content of a deleted file, $I comprises the metadata (0 to 7 bytes is the header, 8-15 deleted file size, 16-23 deleted file timestamp, 24-27 file name and the rest is the file path).

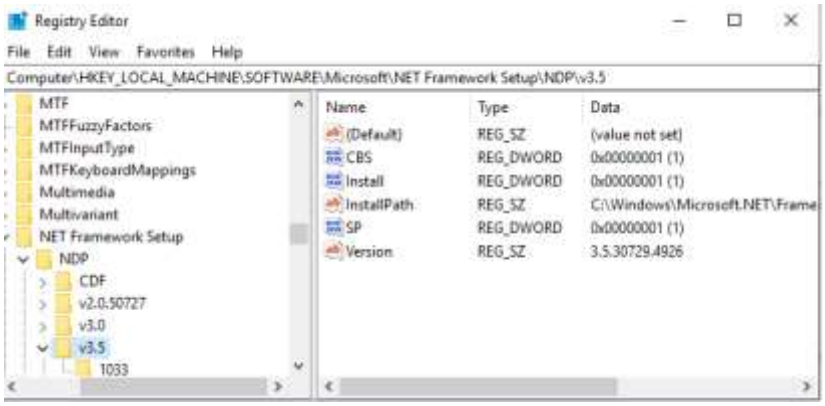

Fig.. $R file and its content[online (https://richardlent.github.io/post/rstudio-as-a-research-and-writing-platform/)]

Event logs – This log book record maintains the information like account lockouts, logon and logoff sessions, recently executed programs, blocked application events etc**.**

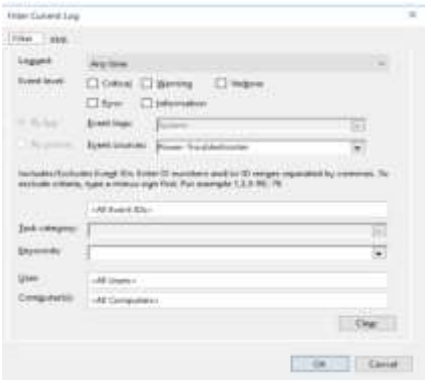

Fig- recorded event log when system resumed from sleep mode[online(http://techgenix.com/computer-wakes-up-at-the-wrong-time/)]

LNK files – These are the shortcut files with LNK extension will directly link to an application rather navigating to the executable file every time.

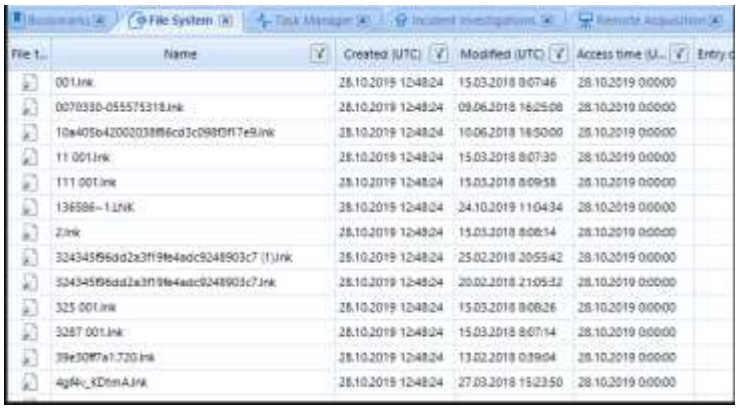

Fig- LNK files of desktop directory with details original ,EXE path, timestamp, file size [online (https://belkasoft.com/forensic-analysis-of-lnk-files**)]**

Jumplist Files – They contain most recently opened (MRU) and frequently used (MFU) applications or files along with time stamped stored under automatic and custom destination files. The former one has MRU/MFU entries while the latter contains LNK files for jumplists and also the metadata.

Fig- Information in custom Destination [Prasanna Amruthavakkula (2018) Push Notifications – Implementing Custom Destinatination]

Discussion-

In this digital world where crimes related digital forensic is increasing day by day, the forensic tools played an important role to catch the criminal who commit crimes related to windows artifacts.With the help of different digital tools we can find the evidence which may help to identify the criminals. Many digital tools like open-source tools and licensed tools are used to identify the artefacts of windows 10.These digital tools can help to find hidden data in unallocated space or in hidden partitions.

Conclusion- As there is rapid increase in the number of internet users across the world, the frequency of digital attacks has been increased.Therefore, there is a need of effective devices, methodologies and development of essential tools to detect these attacks timely. In the present review article, we have examined different tools to identify the windows artifacts. In addition, it has been seen that by using different tools we can identify the criminals easily based on the crime scene. Hence, these artifacts are the worthy part of an investigation. Moreover, we can say that Digital Forensics is reinforcing with the advanced methodologies and techniques in order to find the constructive evidences. Therefore, in this manner, forensic investigation can performed right from the beginning to the end of the crime scene, till the submission of the evidence in the court and can helped in criminal justice system.

References-

1.Aryan Singh. 2016. Role of Computer in Research ISSN:2277128X [online (www.ijarcsse.com)]

2.Arjun Chetry, Uzzal Sharma. 2019 Memory Forensics Analysis for Investigation of Online Crime - A Review Corpus ID: 211210920

3. A. Đuranec Hausknech, D. Topolčić ,K. Hausknecht ,D. Delija. 2016. Investigating file use and knowledge with Windows 10 artifacts MIPRO 2019/ISS

4.Bhupendra Singh, Upasna Singh. 2016. Digital Investigation 1e13

6.Diana Hintae, Robert Birl, Michael Green. 2017. An Investigation into the forensic implications of the Windows 10 operating system: Recoverable artefacts and Significant changes from Windows 8.1 DOI: 10.1504/IJESDF.2017.087394

7. David Mugisha. 2019. Role and Impact of Digital Forensics in Cyber Investigations

8..DigbijayGuha, Shameek Mukhopadhyay, Sayak Konar ,Juin Banerjee.2015.Windows 10 ISSN: 2320-5288

9.Gavin Philips. 2019. what is Registry and How do I edit it? Online (https://www.computerhope.com/jargon/r/registry.htm)

10.Premchand Ambhore , Archana Wankhade and B.B.Meshram.2018.Disk based Forensics Analysis DOI: 10.14741/ijcet/v.8.2.33

11.Juan Manuel Castelo Gómez, José Roldán Gómez,, Javier Carrillo Mondéjar and José Luis Martínez. 2019.Non-Volatile Memory Forensic Analysis in Windows 10 IoT Core ; doi:10.3390/e21121141

12.Milind G. Meshram, Prof. Deepak Kapgate.2015.Investigating the Artifacts Using Windows Registry and Log Files ISSN 2320–088X

13.Palwinder Singh , Amarbir Singh.2016.Computer Forensics: An Analysis on Windows and Unix from data recovery perspective e-ISSN: 2395 -0056 p-ISSN: 2395-0072

14.Ratna Sri, M. Seetharam Prasad. 2016. An investigation into the forensic significance of the Windows 10 Operating System ISSN: 2277-3878, Volume-7

15. Umesh Timalsina. 2018.Acquiring Disk Image with FTK ImagerDOI: 10.13140/RG.2.2.33881.62564

16. Dinesh Patil.2016. RegForensic Tool: Evidence Collection and Analysis of Windows Registry DOI: 10.17781/P002064

17. FTK imager- Copying Protected Registry Files. 2017. online (https://www.litigationsupporttipofthenight.com/single-post/2017/01/30/FTK-Imager---Copying-Protected-Registry-Files)

18. Shawn Brink. 2017. Show Current Refresh Custom Recovery Image in Windows 10

19. Rui YanG, Jiang- Chun REN, Shuai BAI and Tian TaNG. 2017.A digital forensic framework for cloud based on VMI ISBN: 978-1-60595-461-5