# Project report

# On

# An Overview of Opportunities & Challenges in Forensic Analysis of Artifacts in Windows 10 OS using Open Source & Licensed Tools: A Comparative Approach

Submitted for the fulfillment of the Requirement for the Degree of M.Sc. Forensic Science


Submitted by

**Sakshi Pandey**

M.Sc. Forensic Science (4th Semester)

Under the Supervision of

**Dr Mamta**



Division of Forensic Science
School of Basic and Applied Science
Galgotias University

Uttar Pradesh


**May 2019**

# CANDIDATE DECLARATION

I hereby declare that dissertation entitled ‘An Overview of Opportunities & Challenges in Forensic Analysis of Artifacts in Windows 10 OS using Open Source & Licensed Tools: A Comparative Approach’’ submitted by me in partial fulfillment for the degree of Forensic Science, School of Basic and Applied Science, Galgotias University, Greater Noida , Uttar Pradesh . It has not been submitted in part or full to this University of any other Universities for the award of diploma or degree.

Sakshi Pandey
Enroll No. 18022010007
M.Sc. Forensic Science (4th semester)
Division of Forensic Science
School of Basic and Applied Science
Galgotias University
Greater Noida
Uttar Pradesh, India

## Acknowledgement-

Firstly, I would like to express my sincere gratitude to my advisor Prof. Dr Mamta (Associate Professor of School of Basic and Applied Science, Galgotias University) for the continuous support of my thesis, for her motivation, for her patience and immense knowledge. Without whom I would not have been able to complete this report, and without whom I would not have made through my masters degree! Her guidance helped. And then I would like to Thank HOD of School of basic and applied science, Dr Lalit Chandravanshi whose insight and knowledge into the subject matter steered me through this project.

**Sakshi Pandey**

**M.Sc. Forensic Science**

**4th semester**

## List of Abbreviation-

- **OS**- Operating system
- **Xbox**- Microsoft video game Console
- **.lnk**- Link
- **MAC**- Media Access Control
- **Cmd**- Command
- **PE**- Portable Executable
- **RAM**- Random Access Memory
- **X**- Extension
- **RAM**- Random Access Memory

## List of Contents-



## Project summary-


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 private and sensitive information has become more and more challenging with each passing day. In my project, described about the artifacts of Windows10. And how these artifacts can be used as a evidence to link a suspect to the crime scene. We can identify the artifacts by using different types of Forensic tools. We took Forensic tools like FTK imager, OS Forensic, Autopsy and etc. These tools help to identify the artifacts of Windows 10. On the basis of the previous research we found that there are different artifacts which have studied before like Jump lists, Recycle bin, Registry analysis and etc. Every digital evidence can be found by using four steps ,

Identification, Acquisition Collection and Preservation .We did imaging in the project. We took a 'PEN-DRIVE' and then using 'acquisition' process we imaged the 'PEN-DRIVE' by using FTK Imager Forensic tool. FTK imager is a forensic tool which helps in imaging the storage device or system. We used FTK imager version 4.2.0.13.

## Title – An Overview of Opportunities & Challenges in Forensic Analysis of Artifacts in Windows 10 OS using Open Source & Licensed Tools: A Comparative Approach

## Introduction-

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 .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 .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 . 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 . 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. 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 . 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.

**Artifacts:** Artifacts are the areas or region within a computer system which consists an important information about to the activities which is performed by the computer user/ computer operator. The type and location of this information depends upon the operating system. At the time of forensic analysis, these artifacts play a very important role in sympathetic or harsh the investigator's observation.

Windows artifacts accept importance due to the following reasons –

Around 90% of the traffic in world occurs from the computers and it's operating system. So Artifacts are important for digital forensics examiners.

The Windows operating system stores different types of evidences related to the user activity on computer system. This is the second reason which shows the importance of Windows artifacts for digital forensics.

Several times the Due to increase in cyber-crime in recent years reason that Windows artifacts are important.

## OS Artifacts:

- File System
- Registry Hives
- Event Logs
- Prefetch Files
- Recycle Bin
- Cortana(Search)
- Notification Centre
- Picture Password
- LNK Shortcuts
- Thumb Cache

Investigator rotates the investigation around old and traditional areas like user crated data. Windows artifacts can help in the investigation towards non-traditional areas like system created data or the artifacts. Great abundance of artifacts is provided by Windows which are helpful for investigators as well as for companies and individuals performing informal investigations.

**OS Artifacts**: Windows 10 operating system's artifacts are following:

## LNK Files Forensics:

**"Link"** files are the shortcut files of Windows. That link or point to other files or executables for ease of access.
On the basis of Computer Forensic , these files contain a personal set of information that can help during an investigation or an incident response.
There are some of the information carried inside of ".lnk" files.

- Original path of the target file.
- Timestamp of both the target and the ".lnk" file (Created, Modified, Accessed).
- File Attributes (System, Hidden…etc.)
- Details about the disk.
- Remote or local execution.
- MAC address of the machines.
- Etc.

To extract and parse the contents of these files you'll require some tools, fortunately we're not short on those. Here a two of them.

- **LECmd**
- **LNK parsing Utility**

To understand more about "**.lnk**" files I suggest you read Magnet Forensics's blog post titled **"**Forensic Analysis of LNK files" and watch this introductory video tutorial by 13 Cubed titled "Jump lists and LNK files".

## Jump List Forensics :

Jump Lists are a windows feature introduced with Windows 7. They contain information about recently accessed applications and files.
Two forms of jump lists can be created in windows.

- **"AUTOMATIC DESTINATIONS-MS"** These are jump lists which are created automatically when any users opens a files or an application. They are situated in the subsequent directory.
  **C:\User\xxx\App Data\Roaming\ Microsoft\Windows\Recent\Automation Destinations**
- **"CUSTOM DESTINATIONS-MS"**: As the name suggested these are custom -made jump lists which are created when the users pins a file or an application. They are positioned in the next directory.
  **C:\User|xxx\App Data\Roaming\Microsoft\Windows\Custom Destinations**

To make sense of the information found inside these files we can use many tools. Below are two of my favorites.

JLECmd by Eric Zimmerman
Jump List Explorer by Eric Zimmerman

Windows Jump List Parser

Also you can check the resources listed below to understand a bit more about this topic.

- LNK Files and Jump Lists
- Forensics Wiki Jump Lists
- Windows 10 Jump List Forensics

## Prefetch Files Forensics:

There are Prefetch Files which are very valuable set of artifacts for anyone doing forensics analysis. These files contain a fruitful information about the applications that have been run on a system such as

- Application name
- Application path
- Last execution timestamp
- Creation timestamp
- Etc.

Prefetch files can be created with the help of directory which is mentioned below:

**C:\Windows\Prefetch**

To make sense of these files and the information available within. We require some tools. Fortunately we have just that.

Below are some tools that can help us parse these files.

- **PECmd**
- **Windows Prefetch Parse**
- **Win Prefetch View**

I highly encourage you to read more about Application Perfecting and Prefetch Files as they are truly great forensic artifacts.

Below are some resources to get you started.

- Forensic investigation of Prefetch Files Windows Operating System– Magnet
- Forensics WiKi – Prefetch Files in Windows
- Digital Forensics Prefetch Artifacts
- Prefetch Forensics

## Windows Forensic Analysis involves:

Collection of Volatile and Non- Volatile information
Windows memory & Registry analysis
Windows Operating System File analysis
Forensic Investigation of event logs & Windows password issues

**Volatile Information:** Volatile information is any information which is stored in memory that will be vanished when the computer loses power supply or in the case of when it is turned- off. Volatile information are hold in physical memory or RAM (Random Access Memory), and it also consists data or details about the processes, network connections, open files and etc. Volatile information gives the specific details information about the condition of the system while it was at the active mode .

There are particular types of Volatile information which are always investigated by the investigator during the investigation:

- Logged –On user
- Open Files
- Network Connections
- Process Information
- Process-to-port mapping
- Process memory
- System time
- Command history
- Mapped drives
- Service/ Driver information
- Network issues
- Shares

**Non Volatile Information:** Nonvolatile information is a type of digital information that is determinedly stored within a file system in the form of electronic medium. It is stored in the form of electronic medium so that it can store information even after the even after the plug is OFF state when power is removed. It is perpetual and it can be collected after the collection of volatile information .

There are particular types of Volatile information which are always investigated by the investigator during the investigation:

- Swap Files
- Index.dat files
- Hidden ADS( alternate data streams)
- Windows Search Index
- Unallocated clusters
- Connected devices
- Registry setting
- Event logs
- Unused partitions

**Windows Registry Analysis:** 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.

**Windows File Analysis**: It maintains several number of files those are useful from a forensic viewpoint. An Investigator who investigates the different locations during the investigation ,he finds the fruitful l information in which possibility of finding data is more , they collect information from that particular areas and then they do analysis of uncertainty . There are different aspects those are attached together by the fact that they all reside within files or the file system.

**Event Logs**: This contains the full information related to the system, security and application notifications stored by the Windows operating system. The process is only used is only used by the Investigator to identify system problems and it also analyse the future issues. There are many applications and the operating system (OS) which use these event logs to record significant hardware and also there are many software actions that are only used by the administrator can use to short out the problem issues with the operating system. This log book record maintains the information like account lockouts, logon and logoff sessions, recently executed programs, blocked application events etc**.** The Windows operating system locates the exacting events in its log files, such as security management, application installations, , system setup operations on initial startup, and problems or errors. The elements of a Windows event log:

There are different information contain by Event log given following

- **Time**: The time in which the event is occurred.
- **Date**: The date on which the event occurred.
- **Computer:** The name of the computer using by the operator.
- **Event ID**: Windows identification number that specifies the type of an event .
- **User**: The username of the user at that particular time when logged onto the machine.

**Cyber tools**- Cyber Forensic Investigators investigates the incarcerate Analysis of digital data to prove that Internet was related to fraud or not. In previous years Computers were only used for storing large volume of data and perform many operations on it but now a days as the crime related to Digital Forensic is increasing so the use of Computer has been also increased. To solve the problems related to Cyber crime, selection of Forensic tools are very important, For better and fast research investigation, the Investigator had created many cyber forensic tools. Corporate Agencies and investigation agencies select the tools based on the basis of their budget and availability. By the study of different crimes we can know the importance of computer forensics & its tools which can help Investigator to Investigate the crime scene during the investigation.

There are different types of Cyber Forensic tools which may help to analyse the artifacts of Windows Forensics:

**1.AccessData FTK**- FTK Imager is a Cyber tool which helps in Acquisition which includes various forensic toolkits such as Helix and SANSSIFT. With the help of this tool, we try and obtain a forensic image of a USB drive with by using FTK Imager. As we know that in every forensic investigation we should never work with the real evidence that in our case. So we should never USB drive and its content, but rather work with a copy of the real evidence, which can be an exact replica of the original evidence, means we need a by degrees copy of the original evidence.

**2. Autopsy**- Autopsy is a tool which is used for collecting the information about the user which can be used as an evidence in criminal cases. Gathering information about the users is known as Cortona which means 'storing information'. Autopsy is a Free tool that allows forensics investigators to analyze disk images and also report many types of information. Autopsy is build upon 'The Sleuth Kit' set of command line tools. Autopsy works as 'Multi- purpose' tool which is used in mobile clouds and Windows both. With the help of this tool we can analyse the live system and also we can analyse the cloud/drive .

**3. RegEdit**-It is an important hierarchical database for the configuration of operating system and most of the different programs. It contains relevant information which have potential evidential value in Forensic analysis. It is a tool which can be used to access windows registry. This tool helps to extract the useful information which can help for both Administrator as well as Investigator. The hackers of the Computer System performs various activities on it such as software installation, putting a malicious code, device connections ,accessing documents and programs.

4. **Magnet Axiom-** It is a complete digital tool for the investigation platform which allows Investigators to acquire and analyze data, as well as share findings. This tool helps to learn about capabilities and features of Axiom- the evolution of Magnet IEF. It also helps 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 Digital evidence and conduct large scale investigations from beginning to end during the investigation. This tool 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 default, SAM, software, security, system hives for the investigation. One of the most important features of this tool that it provides the last variation date of a key. OSForensic is a complete toolkit which is also known as 'Multi-tasker' that provides the facilities for memory view, raw disk view, recent activity.

## Review of Literature-

**Ning Zhang *et al.*(1997)** discussed about the increment of Cyber-attacks which are increasing very fast day-by-day .Forensic investigators could find very easily that what happened on a system by acquiring the memory data. In this , they studied about possibility of malicious software which misusing architectural features to damage memory forensics. There are two types of architectural feature those are misused named physical address layout and secure containers. The first architectural feature was physical address layout which was used by the north bridge to route memory access to either physical memory or Input devices on x86 platforms. They proposed Hidden location in input Space (Hives), which can change CPU registers to alter the physical address layout to cover memory. A novel Input investigation technique is used to lock a memory region named Hives memory into I/O address space to prevent access. There were two different novel techniques first technique name was Black box write and the second one was TLB Camouflage those were developed to protect the unlocked Hives memory against memory forensics while it was allowing access for attackers. And the second architectural feature was explored named hardware-aided secure execution technology. More importantly, they proposed countermeasures and mitigations these two features for the latest discovered attacks .On the basis on these features their aim was to raise the awareness of the potential risks of misusing hardware architectural features to demonstrate the risk.

**Grant Osborne(2015)** discussed about the general techniques which was used in the acquisition and analysis of a system's volatile memory. Memory forensics
Comes from obscurity in 2005 in response to a challenge issued by the Digital Forensics
Research Workshop (DFRWS). Then the Researchers and Investigators started to understand the importance and role of memory for the forensic analysis. He also discussed about the Volatile memory which contains a useful information regarding the current state of device. Memory forensics techniques examined RAM to remove information such as, encryption keys, passwords, open files, network activity, open files and etc within an operating system. These information could help investigators to reconstruct the events surrounding criminal use of technology.

**Richard M. Stevens (2010)** discussed about the current memory forensic tools like processes and sockets. Due to the number of having forged data ,there was a need for more memory forensic techniques which was used to dig out user-entered data retained in various Microsoft Windows applications. There was a key named Command history which was best source of evidence in computer crimes which reveals important details about an offender's activities on the subject system.

**Johannes Stuttgen and Michael Cohen (2013)** discussed memory analysis had gained popularity in recent years proving to be an effective technique . There were different unique evidentiary challenges are acquired due to the different challenging acquisition technique which was presented by the Memory acquisition process .They also used a number of simple anti-forensic techniques which were current commercial and free memory acquisition tools. They found that current tools were not as much useful t to very simple anti-forensic measures. They presented a unique and convenient acquisition technique named ' novel memory acquisition technique' that was based on direct page table manipulation and PCI hardware introspection.

**Brain D. Carrier and Joe Grand (2003*)*** discussed that it is very difficult to perform acquisition of volatile memory from a compromised computer again and again because the acquisition procedure should not works on un trusted code, such as the operating system or applications executing on top of it. They also presented a procedure for acquiring volatile memory with the use of a hardware expansion card that can make replica of memory to an external storage device. The memory card could not easily be detected by an attacker and it also had a specialty that the acquisition procedure did not works on untrusted resources

**Bhupendra Singh and Upasna Singh (2016)** discussed about the Jump lists and they said a Jump list could have records which could be work as evidence during the investigation and it could also give the information about the activity of user and his/her

details. Artifacts recorded by Jump Lists had been widely discussed in various forensic Investigators since its debut in Microsoft Windows 7. However, this feature had more capabilities to reveal evidence in Windows 10, due to its modified structure. In this paper, they have identified the structure of Jump Lists in Windows 10 and they compared it with Windows 7 and windows 8. After many years a tool was introduced called Jump List Ext (Jump List Extractor) that was developed on the basis of identified structure that can parse Jump Lists in Windows 10 individually as well as collectively. There were number of experiments which were used to detect anti forensic efforts like evidence destruction, evidence modification and evidence forging carried out on the records of Jump Lists.

**Bernard Allen Sabernick III (2016*)*** discussed Forensic tools were a critical component of forensic investigators job. As new features were added in operating systems, those tools need to adapt and be updated to analyze those new features. Microsoft recently released its Windows 10 operating system with a new voice activated personal digital assistant called Cortana.. Cortana is capable of storing information about a user which could be used as evidence in criminal cases. Using the open source forensic tool Autopsy, this information was currently not being gathered in an effective manner. In order to address this problem, their paper proposed enhancements to the Autopsy tool to allow forensic investigators to collect the needed information about Cortana and analyze it more quickly.

**Diana Hintea *et al*. (2017)** discussed about the latest version of Microsoft operating system,. Windows 10 was the latest Microsoft operating system on which Forensic investigators examined the artifacts .Forensic investigators must examined to determine the changes they compared it with windows 8.1 and with their artifacts also . They analysed Windows 10 and their new features so that they can differentiate its artifacts to the other windows systems. The tools which helped: FTK Imager, Process Monitor, ESE Database View and Registry Explorer. They also found that the artefacts were changed in Windows 10 in comparison to the previous version of Windows. When they compared windows 10 with Windows 8.1 , there were a number of artifacts found similar to the Windows 10.

**Haoyang Xie *et al.(2012)*** discussed the importance of Windows Registry forensics which were an important branch of computer and network forensics. Windows Registry was considered as the heart of Windows Operating Systems because it was contained all of the Groups, Windows Registry configuration setting of specific users, hardware, and software. Therefore, it was viewed as a gold mine of forensic evidences which could be used in courts. They also introduced the basics of Windows Registry.

**Derrick J. Farmer (2007)** discussed about the Microsoft Windows Registry database and explain how critically important a registry examination is to computer forensics experts. He discussed in his paper about the various types of Registry 'footprints' and

delve into examples of what crucial information that can be obtained by performing an efficient and effective forensic examination. Many of the Registry keys that are imperative and relevant to an examination will also be discussed.

**Amir Najafi Amin *et al.*(2019)** discussed that mostly Microsoft Word was used as a primary tool of the computer which created ,and accessed and modified the associated digital documents. Due to the rapid increase in the usage of digital devices, Digital Investigations became vital while dealing with deleted, hidden, modified, tempered or stolen documents either in case of an incident or a digital crime. In their paper, a novel study is carried out specifically on Microsoft Word to figure out its forensics artifacts in Windows 10 registry.

**Harlan Carvey (2005)** discussed the Windows Registry contains a wealth of information that can prove to be very valuable to the forensic investigator. The key to accessing this information is to know where the information exists within not only the file system, but also within the structure of the Registry itself.

**Graeme Harsman *et al.* (2019)** discussed that computing desktop market was dominated by the the Microsoft Windows operating system. Examination of digital device and artifacts was the essential part of Forensic investigation.. This examination provided examination of Windows 10 Timeline feature and also ability to know the activity of the user. Within the database log files. It also given the information regarding the Timeline feature of Windows 10.

**Narasimha Shashidhar and Dylan Navak (2005)** discussed that from the digital forensic perspective , Prefetch files like any other file in a system can be investigate for the investigation purpose. With the help suitable tools a Digital Forensic examiner can investigate the Prefetch files within the system. These tools help to find the rapidly files so they take less time during the investigation. Windows Prefetch files were made to less the starting time which is taken by the applications of windows and it also help to consume data within less time. In another way , Prefetch files help to avoid fault . This folder contains prefetch files for user and system applications as well as a ReadyBoot folder, a layout.ini file, and several database files. They investigated the process behind the creation and management of prefetch files on a Windows machine.

**Timothy D.Morgan (2008)** discussed the for getting fruitful information , Investigator should investigate the Windows registry serves as a primary storage location . There were a number of Researcher worked on the fact but they did not find something that can help during the investigation process but also they were unavailable to find how Windows deletes registry data structures under NT-based systems. He also explained the topic and provided an algorithm for improving deleted keys, values, and other structures in the context of the registry as a whole.

**Enlyn Butterfield (2014)** discussed that the Window registry is a database which can store setting for a computer user like applications, and hardware installed in a system and many other associated settings. The registry was stored in such a format that requires decoding to be read; there are several tools that can help to do this. Once these are opened it provides a wealth of information including, but is in no way limited to, evidence of the applications and files a user has opened.

**Nihad Ahmad Hassan and Rami Hijazi (2017)** Registry files cannot be examined directly that is why they should achieved with the help of 'FTK Imager' and also it should be restored with the associated deleted registry records which should be identified with the 'Registry Explorer' and also examine all registry hives .Registry key is a consists an object that plays the exact same role as a folder in normal naming Windows® . A Registry key that can contain another keys and subkeys in addition to data values. To work the function keys help to work any application .

**Hong Guo *et al* (2012)**.- discussed that the use and development of Internet is increasing and new technologies are increasing with the passage of time. Computer forensics is a region of research that helps to investigator for the investigation process and also analysis techniques to help detection of these crimes to present in the court. They provided basic concept of computer forensics and also outlines various principles of computer forensics.

**Research-** The previous Research was done in Windows Forensic

**1.Registry -**Registry files cannot be examined directly that is why they should achieved with the help of 'FTK Imager' and also it should be restored with the associated deleted registry records which should be identified with the 'Registry Explorer' and also examine all registry hives.

**Artifacts-**, Last password changed timestamp **,**Last logon time stamp Last opened and visited folders, Recently opened files and etc.

## 2. Windows memory Artifacts:

**Artifacts-** These are the artifacts namely Hiber file, RAM, Swap file, Page file.

These artifacts give a number of information during the investigation process. This memory involves evidence like passwords, username, URLs visited. Hiber file gives data like played songs on windows OS, opened images and movies and etc. It also records

the outlines 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).

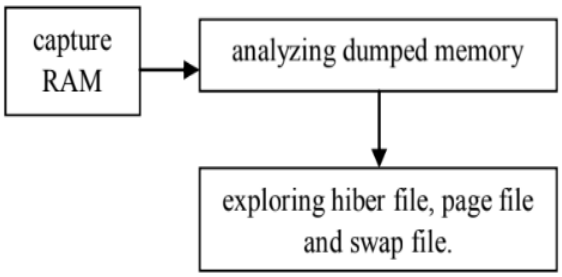


**Fig- Procedure for forensic analysis of windows**

## Operating System:

**Artifacts-** It involves artifacts namely Event logs, Recycle bin data, LNK files, Prefetch files, Jumplists and etc.

My Research was based on the artifacts related to Windows Operating system by using different Forensic Tools. I have done Imaging part of storage but its analysis was left.

## Methodology-

The important role of digital forensics Investigator is to gathering data from a suspect's device,

The process of gathering information from a digital evidence

**Identification:** This is the process of documenting and detecting the digital evidence. During this step of Identification, the DEFR (digital evidence first responder) must examine the all devices which are used in the perpetration of a crime as well as those devices that seem irrelevant. The DEFR should take practical components like cloud computing into consideration .

**Collection:** After the process of Identification , all devices which are identified should be transferred to the laboratory for analysis. The DEFR or Investigator should also look other materials which can help to link crime to the crime scene such as glass, hairs, or any other substances.

**Acquisition:** After the collecting and identifying the evidence ,Acquisition process should be done In the process digital evidence from an electronic media should be analysed. There are four fundamental methods for acquiring data, disk-to-image file:, disk-to-disk copy,, logical disk-to-disk file, and sparse data copy of a file or folder. Acquisition process is performed where there is a large amount data are

gathered from RAID drives or large drives. While collecting the digital evidence, an investigator must remember the rule of e “Order of Volatility” that defines the order or sequence in which the digital evidence should be collected. This order for collecting evidence is maintained from highly volatile to less volatile data. The suitable tool must be used for acquisition purposes and it should always performed on test rather than on suspect drive so that real evidence can not be destroyed..Validate acquisition with built-in tools such as hexadecimal editor with SHA-1 or MD5 hashing functions. For Acquisition we use FTK imager or Encase imager .We used ‘ PENDRIVE’ as a evidence then we done imaging with the version of FTK Imager 4.2.0.13. We followed several steps foe imaging which are given as follows:

## Create image disk – Physical drive- Finish – Add Raw (dd)- Image destination Folder-Browser- This PC- Disk E- Create Folder-Image file Name – Start

## Preservation:

After the Acquisition process, evidence should be preserved now. It should be preserved at physical site so that it cannot be altered or changed. . Only well-preserved evidence can be presented for court proceedings.

**Result** - With the help of FTK imager , imaged the ’Pen-drive’.

**Discussion**- We made image of a pen-drive successfully but we haven’t make image of system with the help of FTK imager. For the investigation purpose we should follow these four steps of digital forensic like Identification, Aquisition, Collection and Identification with the help of different Forensic tools By using different Forensicf tools we can identify artifacts of Windows Forensic easily. And these digital evidence which are followed by digital tools can help to relate suspect to the crime scene .After Acquisition the admissibility of evidence in court is valid. Due to the Covid-19 my work is not completed.

## Conclusion-

As the Crime related Computer Forensics are increasing very fast .Therefore, it is

necessary to have knowledge of Computer Forensic. The demand of Digital Forensic knowledge is increasing in every field like government sector, banking Sectors, International companies and etc In this present time everyone possesses mobile phones , laptops , tablets and etc so, online frauds are also increasing very fast. Windows Forensic and it's artifacts can be identified with the of different Digital Forensic tools. 'Acquisition' is the step of Computer evidence which can be recognized with the help of FTK or Encase imager. FTK imager helps to imaged the storage devices.

## Future scope

As the crimes related Computer Forensics are increasing day-by-day. The importance of Digital Forensics is increasing very fast in this present time. Digital Forensic is playing an important role in every field of area like Banking Sectors, Multinational companies, Cyber Securities, Government sectors and etc. By seeing the increment of cyber crime, I would say that it is one that can play an important role and also it can hold the future of IT industry. We are seeing that cyber crimes are increasing day by day and to catch these breaches or stop this crime , we need cyber forensics to detect mitigate and analyse them. Attacks have no limitation for the country, area or any other geographical region. These attacks can come from any direction so we need to be positive against cyber crimes. As the technologies are increasing , crimes are also increasing . To contest these crimes, digital forensic has become essential part for the criminal investigation in the purpose of court of law. Computer forensics defines the crime which is related to the computer and network. There are two types of crimes which are related to it firstly a computer is used to commit a crime and secondary the computer itself is the target of a crime. Digital Forensics do post and pre-digital forensics investigations. In this present time as the technologies are increasing very fast , everyone has mobile phones and they are using it from Online transactions , social media and etc. We can build our own task core. Employees working in International companies and IT sectors stole the data of the company and sell it to other companies as they are doing fraud so we can catch them easily with the knowledge of Digital Forensics. We get Details which are very much crucial to link a suspect to the crime scene. As the jobs through linkedin and indeed are increasing so frauds are also increasing so it will also help in Online jobs Fraud.

## References:

[1] Hong Guo, Bo Jin, and Daoli Huang https://link.springer.com/chapter/10.1007/978-3-642-23602-0_21 ' Research and Review on Computer Forensics'

[2] B. V. Prasanthi( 2016) online[http://www.ijettjournal.org/archive/ijett-v41p249 ]

doi 10.14445/22315381/IJETT-V41P249

[3]N. Beebe, “Digital forensic research: The good, the bad and the unaddressed,” in Advances in digital forensics V, pp. 17–36, Springer, 2010.

[4] N. R. Council, “Strengthening Forensic Science in the United States: A Path Forward.” https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf, 2010.

[5] D. Bilby, “Low down and dirty: Anti-forensic rootkits,” BlackHat Japan, 2013.

[6] S. L. Garfinkel, “Digital forensics research: The next 10 years,” Digital Investigation, vol. 7, pp. S64–S73.

[7] B. D. Carrier and J. Grand, “A hardware-based memory acquisition procedure for digital investigations,” Digital Investigation, vol. 1, no. 1, pp. 50 – 60, 2010.

[7]J. Wang, F. Zhang, K. Sun, and A. Stavrou, “Firmware-assisted memory acquisition and analysis tools for digital forensics,” in Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on, pp. 1–5, IEEE, 2011.

[8] E. Chan, S. Venkataraman, F. David, A. Chaugule, and R. Campbell, “Forenscope: A framework for live forensics,” in Proceedings of the 26th Annual Computer Security Applications Conference, pp. 307–316, ACM, 2010.

[9] R. Harris, “Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem,” digital investigation, vol. 3, pp. 44–49, 2012.

[10] T. Haruyama and H. Suzuki, “One-byte modifications for breaking memory forensic analysis,” Black Hat Europe, 2012.

[11] J. Rutkowska, “Subverting vistatm kernel for fun and profit,” Black Hat Briefings, 2014.

[12] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar, “Innovative instructions and software model for isolated execution.,”

in HASP@ ISCA, p. 10, 2013.

[13] “ARM Security Technology, Building a Secure System using TrustZone Technology,” April 2010.

[14] A. Kharraz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, “Unveil: A large-scale, automated approach to detecting ransomware,” in USENIX Security 16, pp. 757–772, 2016.

[15] A. Dinaburg, P. Royal, M. Sharif, and W. Lee, “Ether: malware analysis via hardware virtualization extensions,” in Proceedings of the 15th ACM conference on Computer and communications security, pp. 51–62, ACM, 2012.

[16] T. Fischer, “Private and public key cryptography and ransomware,” 2014.

[17] E. Kirda, “Cutting the gordian knot: A look under the hood of ransomware attacks,” in Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings, vol. 9148, p. 3, Springer, 2015.

[18] D. Bovet and M. Cesati, Understanding the Linux kernel. O’reilly, 2010.

[19] “Advanced Micro Devices. Amd64 Architecture Programmer’s Manual,” vol. Vol. 2, may 2013.

[20] “Intel 64 and IA-32 Architectures Software Developer’s Manual,” sep 2013..

[21] T. Muller, F. C. Freiling, and A. Dewald, “Tresor runs encryption ¨ securely outside ram,” in USENIX Security Symposium, 2011.

[22] P. Simmons, “Security through amnesia: a software-based solution to the cold boot attack on disk encryption,” in Proceedings of the 27th Annual Computer Security Applications Conference, pp. 73–82, ACM, 2011.

[23] J. Pabel, “Frozencache: Mitigating cold-boot attacks for full-diskencryption software.,” in 27th Chaos Communication Congress, 2010.

[24] L. Guan, J. L. amd Bo Luo, and J. Jing, “Copker: Computing with Private Keys

without RAM.," in In Network and Distributed System Security Symposium (NDSS), 2014.

[25] "Memory Forensic Challenges under Misused Architectural Features." http://memoryforensic.weebly.com/.

[26] N. Zhang, K. Sun, W. Lou, and Y. T. Hou, "Case: Cache-assisted secure execution on arm processors," in Security and Privacy (SP), 2016 IEEE Symposium on, pp. 72–90, IEEE, 2016.

[27] A. Baumann, M. Peinado, and G. Hunt, "Shielding applications from an untrusted cloud with haven," OSDI'14, 2014.

[28] H. Taylor, "Ransomware spiked 6,000% in 2016 and most victims paid the hackers, IBM finds." https://goo.gl/8afou8.

[29] V. Kotov and M. Rajpal, "Understanding crypto-ransomware," Bromium whitepaper, 2014.

[30] Intel, Intel 64 and IA-32 Architectures Software Developer's Manual, System Programming Guide, Sep 2016.

[31] "Dumpit." https://zeltser.com/memory-acquisition-with-dumpit-for-dfir-2/.

[32] D. G. Lunde, "What is the average size of an office document?." https://blogs.technet.microsoft.com/dangl/2012/10/18/ what-is-the-average-size-of-an -office-document/.

[33] L. Martignoni, A. Fattori, R. Paleari, and L. Cavallaro, "Live and trustworthy forensic analysis of commodity production systems," in Recent Advances in Intrusion Detection, pp. 297–316, Springer, 2010.

[34] M. Yu, Q. Lin, B. Li, Z. Qi, and H. Guan, "Vis: virtualization enhanced live acquisition for native system," in Proceedings of the Second Asia Pacific Workshop on Systems, p. 13, ACM, 2011.

[35] D. Kaplan, J. Powell, and T. Woller, AMD MEMORY ENCRYPTION, Apr 2016.

[36]Grant Osborne (2013) Memory Forensics: Review of Acquisition and Analysis

Techniques DSTO–GD–0770

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

[38]Brent Muir – 2015 windows 10 Forensics  Version 1.5 (Build 10240)

[39]Pooja Salave, Atisha Wakdikar (2017). Memory Forensics: Tools Comparison. International Journal of Science and Research (IJSR). 6, 6, p5-8.

[40].Aryan Singh(2016) Role f Computer in Research ISSN:2277128X

[41] David Mugisha (2019) Role and Impact of Digital Forensics in Cyber Investigations

[42]Digbijay Guha, Shameek Mukhopadhyay, Sayak Konar ,Juin Banerjee(2015)Windows 10 ISSN: 2320-5288

[43] Umesh Timalsina (2018) Acquiring Disk Image with FTK ImagerDOI: 10.13140/RG.2.2.33881.62564