International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7, Issue-6, March 2019

An investigation into the forensic significance of the Windows 10 Operating System

Ratna Sri, M. Seetharama Prasad

Abstract: ***Digital Forensics is an emerging trend in the world of forensic investigation because of the explosion of cyber crimes and threats. As these are getting more oblique, new techniques and capabilities are developed in order to enhance the proactive cyber defence and also to conquer its challenges. Digital Forensics refers to a branch of specialised forensic science which deals with the formation of the digital information, storage and transmission of the evidence in the investigation. Formerly, most of the forensic tools and software are specialised, proprietary and expensive. But currently, they are made accessible for both the government and private sectors for investigating the digital evidence. The first part of this paper provides a brief overview of the digital forensic lifecycle, description of its phases and the features of windows 10 operating system followed by the miscellaneous investigation techniques and also the forensic analysis of the artifacts pertained on the windows 10 operating system. The outcome of this research is the evidence findings on the artifacts which correlate to the user activity by using various software, tools and mechanisms.***

Keywords: Digital Forensics, cyber crime, forensic analysis, investigation and windows 10 operating system artifacts.

I. INTRODUCTION

The branches in digital forensics are divided based on the kind of digital devices, media and the artifacts. They are computer forensics, database forensics, mobile forensics, malware forensics, network and wireless forensics. Digital forensics is used to resolve many cyber crimes and for catching criminals, confidential data recuperation, civil litigations and many more. Depending upon these, investigations in the digital forensics have a wide range of approaches. This paper is about the strategies and methodologies used for the forensic analysis of the personal computer (windows 10 operating system) and an attached pen drive to it.

Computer forensics is defined as the data created, stored and transmitted by the computers. The data acts as the source of evidence in the investigation process, legal action and its proceedings. The windows 10 OS, latest version from Microsoft came with many features like continuum, cortana, notification center, microsoft edge, multi tasking, universal apps, Xbox and windows store.

Revised Manuscript Received on 30 March 2019.
* Correspondence Author
Ratna Sri*, Student, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram (Andhra Pradesh), India.
Dr. M. Seetharama Prasad, Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram (Andhra Pradesh), India.

Apart from these, the other sources for evidence location and 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 system.

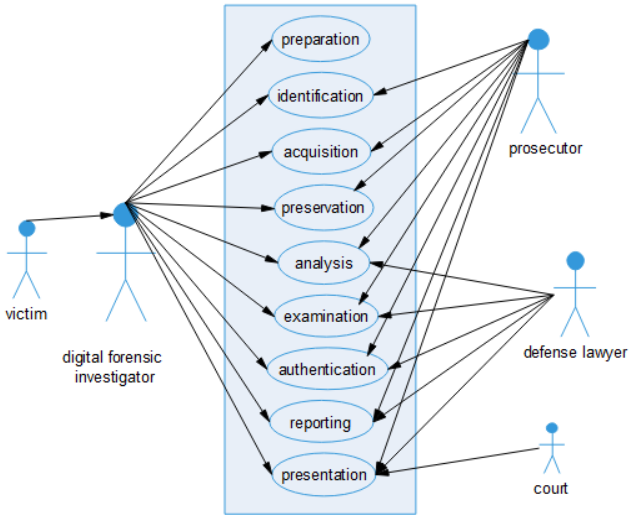

Fig.1. Use Case Diagram - digital forensics life cycle

1. **Preparation:** Before commencing the investigation, the digital forensic investigator must need to seize and retain the evidence (computer and a pen drive) from the victim. Later, forensic environment is prepared.
2. **Identification and Acquisition:** The aim is to identify what artifacts are available, where and how they are pertained on the system. After identifying and assessing, everything is acquired into custody. Hashing and forensic duplication are performed on the evidence.
3. **Preservation:** The evidence collected from the live and switched-off system is to be preserved carefully in order to prevent the tampering and altering.
4. **Analysis and Examination:** Extract the evidence from all sources, process, analyse, examine the data for evidence tracing and validating, recover deleted or hidden artifacts, reconstruct them and gather other data if needed and then interpret what kind of information is served as the real evidence.
5. **Authentication:** Hashing is to be done again on the duplicated data and it has to be compared with the initial hash values calculated on the original data. It is done to prove the integrity of the evidence.

6. **Reporting and Presenting:** Reporting means building a chain of custody form which includes documenting every step carried in the investigation and also the people associated with gathering and handling the evidence for ensuring integrity. The chronological events are to be recorded in an explicit manner so that the layperson can understand. The final step is to submit the report along with the evidence findings at the court by proving its credibility.

II. LITERATURE SURVEY

In this section, a few technological details by forensic analysts and researchers are studied.

In [2], Fabio Marturana, Simone Tacconi and Gianluigi Me have done forensics on dropbox, google documents, flickr and picasa. They extracted the related evidence of these artifacts from web browsers Mozilla Firefox and Google Chrome.

In [3], Sreeja S C, C Balan, discussed about the forensics analysis of the volume shadow copies in windows 7 OS whereas in [4], Kritarth Y. Jhala and A. Anisetti have discussed about the forensic analysis of the jump list files.

In [5], Mandeep Kaur, Suman Khurana and Navreet Kaur have conducted a literature review on the digital forensics tools.

III. FORENSIC ANALYSIS

The forensic analysis is done on the artifacts generated by windows. Evidence is extracted from the windows files and directories, file system and unallocated space in the pen drive.

A. Memory

Table I. Windows memory artifacts

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

These artifacts give a lot of information during the investigation process. Dumped RAM or 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).

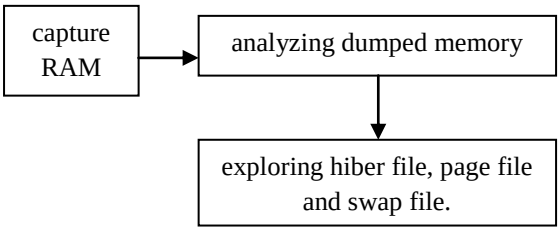

Fig.2. Procedure for forensic analysis of the windows memory

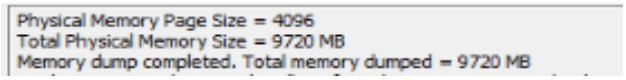

Fig.3. Acquired memory

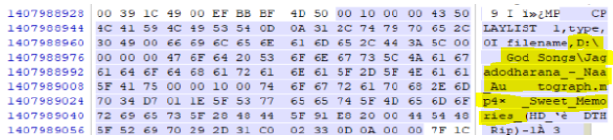

Fig.4. played songs with root folder

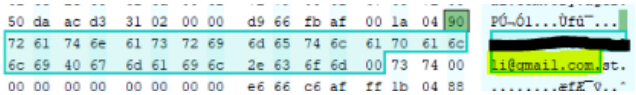

Fig.5. Found gmail address

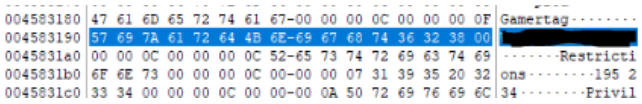

Fig.6. gamer tag (username) of Xbox live

B. Windows Drive

Table II. Windows drive artifacts

Artifacts	USB flash drive and its multimedia files (image, audio, and video).

This section is about the forensic examination of the seized pen drive. Create a forensic image of it in .E01 format with no image fragments, mount the image, export the files to a folder and examine them. For image files, conduct steganalysis. On inspecting the file signatures, the hidden files are extracted and viewed. When analysing each pixel of the image, the invisible text can be seen and obscene content is also categorised. For video forensics, break each file into multiple video fragments and concealed frames are withdrawn. And the audio files are enhanced by normalising the volume and applying the noise filters.

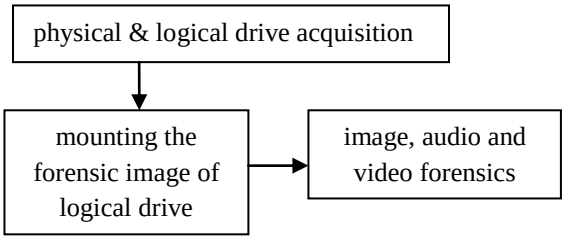

Fig.7. Steps for USB forensics.

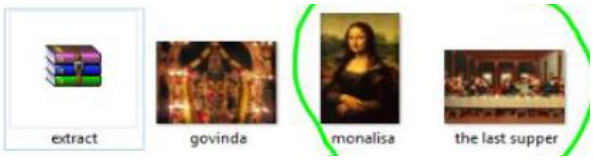

Fig.8. 'monalisa' and 'last supper' images are extracted from the zip file which is hidden behind 'govinda' image

Fig.9. concealed key frame extracted from the video fragments of 'inside tirumala temple'

Fig.10. (a) The first one is the original image where the obscured data cannot be seen.
(b) After magnifying each image pixel, the data seen on it is '333888888141414141414151515151515.'
(c) The result obtained on converting these numbers to alphabetical letters is 'C3H6N6O6' (CCCHHHHHHNNNNNNOOOOOO) which is the chemical formula for RDX.

C. File System Analysis of seized USB

Table III. File system artifacts

Artifacts	Deleted files, carved image files, file's metadata and shadow copies.

Prior to the forensic analysis on the above artifacts, identify the file system of the forensic image of the obtained USB.

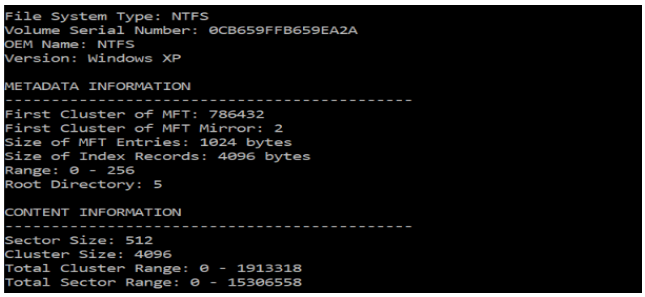

Fig.11. Master File Table (MFT) cluster records of NTFS file system through command fssat, sleuthkit command line tool kit.

Later retrieve the deleted files through the Autopsy forensics software. Next, perform file carving - the reconstruction of the files without using metadata. With carving, lost files and their fragments are recovered when the entry of a directory is corrupted or missed. Tool required here is scalpel. After carving is done, extract the metadata of the file to know the file size, signature, created, accessed timestamps and other file characteristics and also examine whether there are any shadow copies created (the backup copies of the files even when they are in use).

Fig.12. restored deleted files in USB drive.

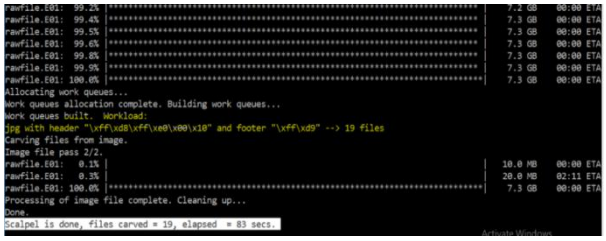

Fig.13. carving process of jpg files with header ff d8 and footer ff d9.

Fig.14. carved image files

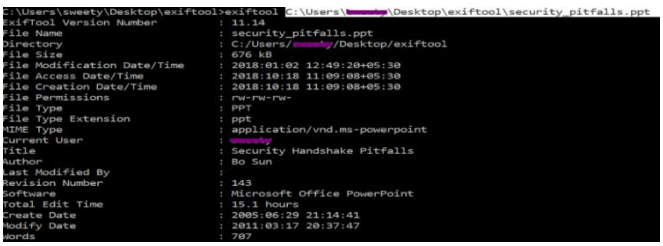

Fig.15. metadata of the security pitfalls.ppt

D. Operating System

Table IV. Operating system artifacts

Artifacts	Recycle bin data, event logs, LNK files, jumplists, prefetch files, thumbcache files and shell bag artifacts.

The vital artifacts of the windows operating system are analysed as following:-

a. Recycle bin – When a file is deleted, 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).

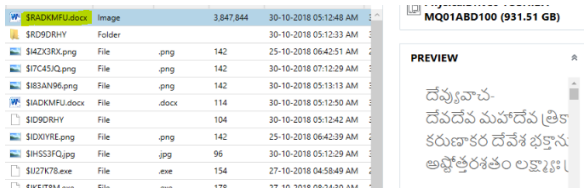

Fig.16. $R file and the content

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

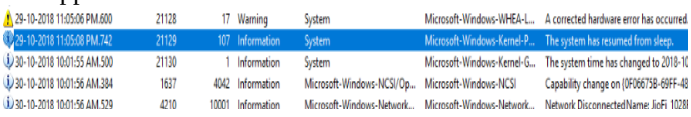

Fig.17. recorded event log when system resumed from sleep mode

c. 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.18. LNK files of desktop directory with details original .EXE path, timestamp, file size

d. Jumplist Files – They contain most recently opened (MRU) and frequently used (MFU) applications or files along with timestamp and 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.

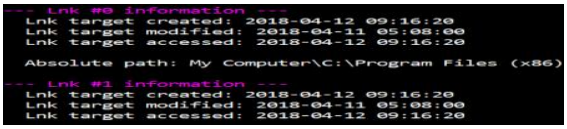

Fig.19. information in customDestination

e. Prefetch files – When an application is run for the first time from a location, prefetch file is created which helps to speed up the loading process from the next time. Location of prefetch file is C:/Windows/Prefetch.

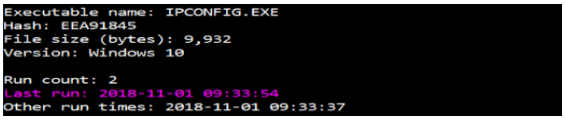

Fig.20. no. of loaded times of ipconfig.exe

f. Thumbcache – Image thumbnails are stored in thumbcache.db when the content is browsed in file explorer. Deleted images from a folder would still remain in the cache database.

Fig.21. thumbcache file with cache and data entry offset along with data and header checksum

g. Shell Bags – These store the settings of a folder (timestamp, entry number, display mode (icons, tiles)) into the registry each time when it is visited.

Fig.22. shell bags persisting information

E. Registry

Table V. registry artifacts

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, dirty shutdown events, last registry key opened, last uninstalled applications.

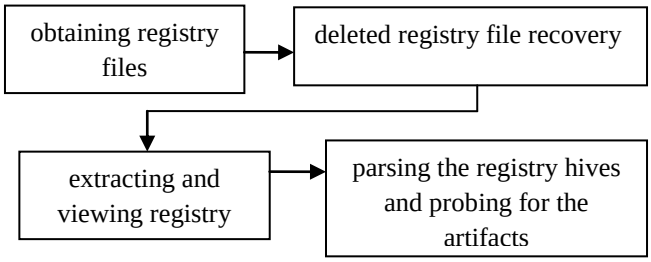

Fig.23. step by step analysis of registry

Registry files can't be examined directly, so they have to be obtained through 'FTK Imager' and restore the associated deleted registry records through 'Registry Explorer' and examine all registry hives.

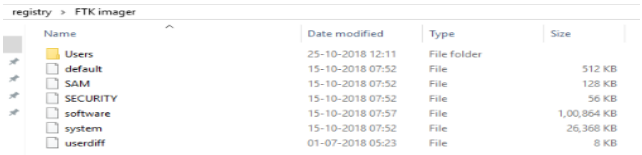

Fig.24. system protected files (registry)

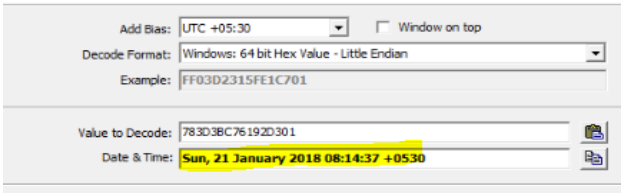

Fig.25. last password changed timestamp decoded from SAM\Domain\Accounts\Users

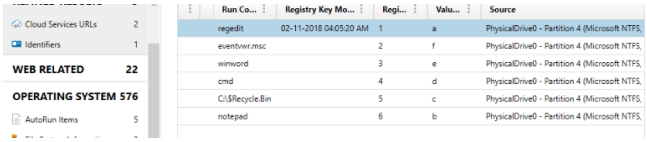

Fig.26. last password changed timestamp decoded from SAM\Domain\Accounts\Users

Fig.27. mounted USB devices along with last inserted timestamp

Fig.28. registry hive is parsed to the 'Reg Ripper' tool for dumping the last written keys.

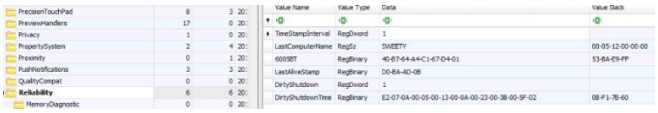

Fig.29. dirty shutdown event from HKLM\software\ microsft\windows\currentversion\reliability

Fig.30. screenshot index - last modified registry key value, extracted from regscanner tool.

F. Windows 10 Applications

Table VI. Artifacts of windows 10 features

Artifacts	Windows 10 notifications, cortana remainders and their attachments, apps searched in windows store, games played in Xbox live and their video recordings, navigated locations in windows maps, weather conditions and its location, one drive and google drive synched cloud data.

a. From wpndatabse of the windows 10 notification center – tasks, events and other system alerts are obtained.

Fig.31. stacked notification showing that K7 security update is completed

b. Windows 10 digital assistant Cortana will give about the reminders that were set, recognize the voice and handwriting.

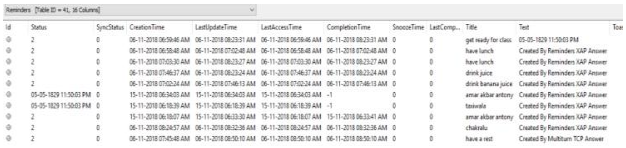

Fig.32. extracted reminders from the cortana core DB of ESE database cortana core instance

c. This is acquired from the windows store location /user_name/app_data/local/packages/microsoft_ windows_store

Fig.33. cache image of Netflix application searched in windows store

d. From XBOX live my_games_list_cache JSON file, played games are obtained.

Fig.34. BombervsDigger from the json file

e. Navigated locations are obtained from the app data/local/packages/windowsmaps/localstate/ persistentviewmodels/searchresultsitems. Also the locations are from windows weather app.

Fig.35. NTR municipal stadium location traced from windows maps

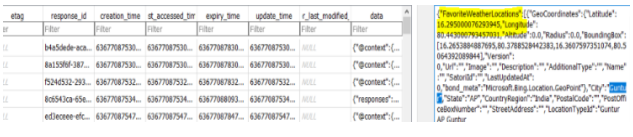

Fig.36. Favourite weather location along with the latitude and longitude coordinates from the sqlite cache db of windows weather

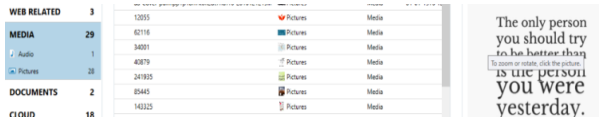

Fig.37. cloud files stored in one drive

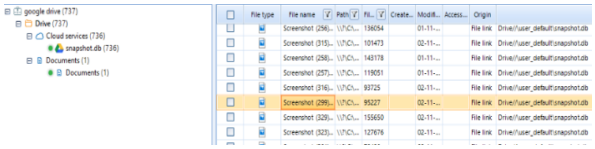

Fig.38. saved screenshots extracted from the snapshot.db of google drive

G. Web Browsers

Web browsers like Google Chrome, Mozilla Firefox, Microsoft Edge, and Internet Explorer (IE) hold the following particulars.

Table VII. Web browser artifacts

Artifacts	Downloaded files, bookmarks, cache, cookies, browser search history and passwords, images, video thumbnails.

Fig.39. 'hotstar' browsing history in Firefox

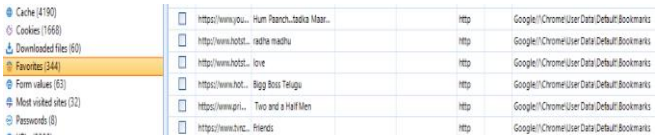

Fig.40. 'bookmarks' in Google Chrome.

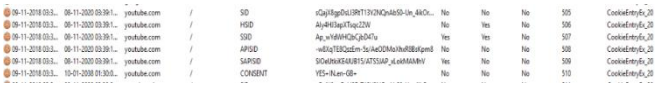

Fig.41. 'youtube' website cookies in Edge

Fig.42. 'thehindu' website cache in IE

Fig.43. browser stored usernames and passwords.

H. Emails & messaging applications

Table VIII. Email and social networking application artifacts.

Artifacts	Discovered information
Microsoft Outlook	Number of incoming and outgoing emails and the email attachments, addresses book and their contact pictures.
Thunderbird	Email messages – header, data and other content.
Skype	Chat conversations, files transmitted and received, contact pictures.
Facebook	Timeline data, post shared, messages, friends list.
Twitter	Tweets, images shared.
Instagram	Following and followers, images posted, saved videos.

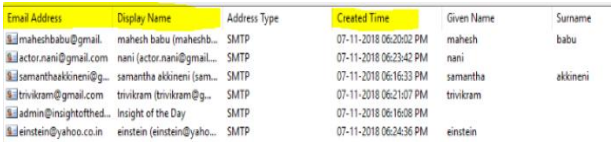

Fig.44. email contacts in microsoft outlook

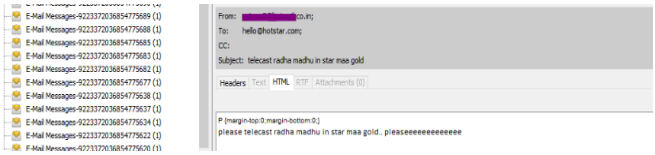

Fig.45. email extracted from thunderbird mailbox using Autopsy forensic tool.

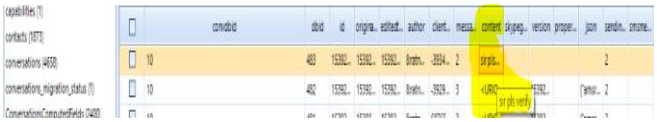

Fig.46. Extracted skype conversation from username/appdata/local/packages/microsft skype

Fig.46. facebook timeline post

Fig.47. extracted twitter tweets from location username/appdatalocal/packages/twitter

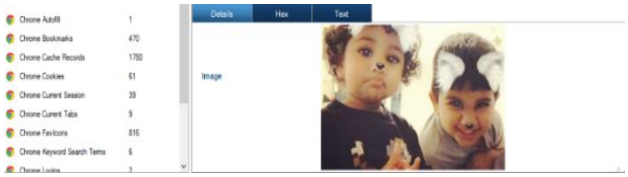

Fig.48. instagram saved pictures pulled out from chrome browser

IV. CONCLUSION

This paper is dealt with the forensic methods deployed by the forensic analyst when a computer crime related to the windows 10 arises. Based on the crime scene, these artifacts are the noteworthy part of an investigation. Also, Digital Forensics is reinforcing with the advanced methodologies and techniques in order to augment the yield of constructive evidence. Without proper gathering of it, investigation goes futile. In this manner, forensic investigation is performed right from the beginning of the crime scene to the submission of the evidence in the court.

ACKNOWLEDGMENT

We would like to express our gratitude to Kritarth Jhala and Surekha Ambati, Digital Forensic Analysts from eSF labs Ltd, Tadepalle, Vijayawada for sharing their wisdom and knowledge throughout the research work.

REFERENCES

1. S. Mehreen, B. Aslaam, "Windows 8 Cloud Storage Analysis: Dropbox Forensics," 12th International Bhurban Conference on Applied Sciences & Technology (IBCAST), IEEE, 2015.
2. Fabio Marturana, Gianluigi Me, Simone Tacconi, "A case study on digital forensics in the cloud," International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 2012.
3. Sreeja S C, C Balan, "Forensic Analysis of Volume Shadow Copy in Windows 7," International Conference on Emerging Technological Trends [ICETT], 2016.
4. Kritarth Y. Jhala, A. Anisetti, "Forensic Analysis of Jump Lists in Windows Operating System" International Journal of Engineering Research & Technology (IJERT), 2015.
5. Mandeep Kaur, Navreet Kaur, Suman Khurana, " A Literature Review on Cyber Forensic and its Analysis tools" International Journal of Advanced Research in Computer and Communication Engineering, 2016.
6. Bhupendra Singh, Upasna Singh, "Forensic Implications of Cortana Application in Windows 10", Springer, 2018.
7. Windows 10, Wikipedia - https://en.wikipedia.org/wiki/Windows_10