

# 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.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

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.

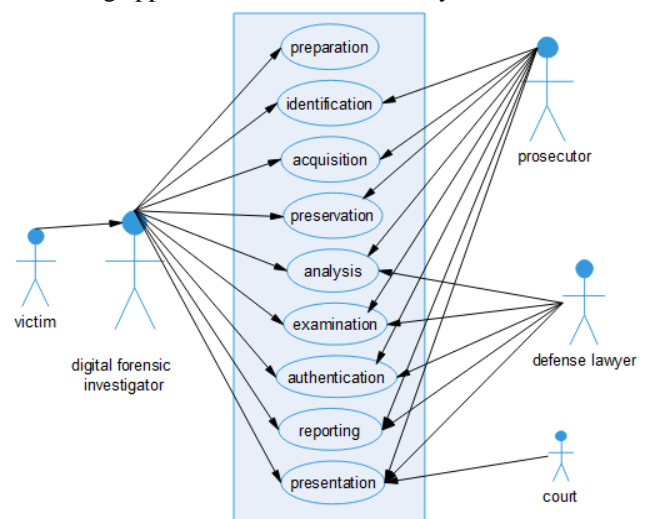


Fig.1. Use Case Diagram - digital forensics life cycle

- 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

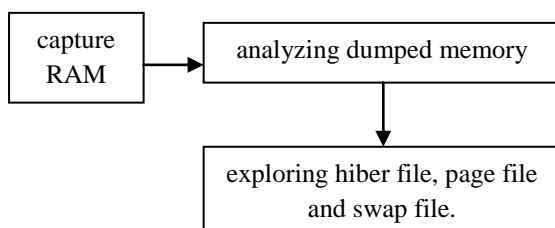
The forensic analysis is done on the artifacts generated by windows. Evidence is extracted from the windows files and directories, file system and unallocated space in the pen drive.

### A. Memory

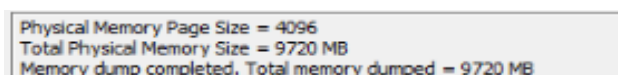
**Table I. Windows memory artifacts**

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

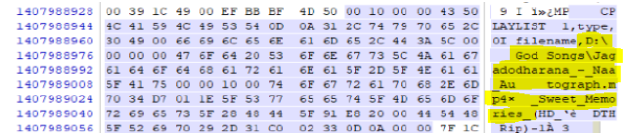
These artifacts give a lot of information during the investigation process. Dumped RAM or random access memory contains evidence like username, passwords, URLs visited. Hiber file gives data like played songs on windows OS, opened images and movies. Page file gives email id, IP addresses, voice mail 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).



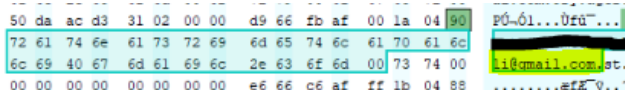
**Fig.2. Procedure for forensic analysis of the windows memory**



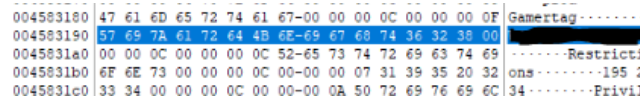
**Fig.3. Acquired memory**



**Fig.4. played songs with root folder**



**Fig.5. Found gmail address**



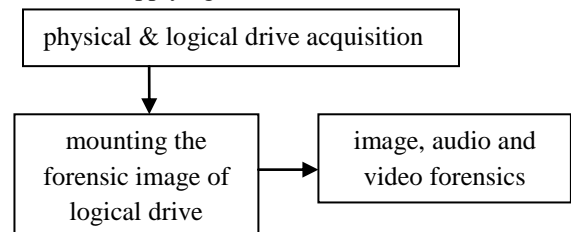
**Fig.6. gamer tag (username) of Xbox live**

### B. Windows Drive

**Table II. Windows drive artifacts**

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

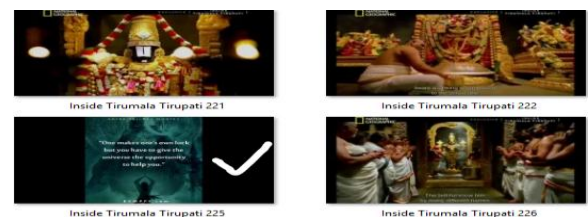
This section is about the forensic examination of the seized pen drive. Create a forensic image of it in .E01 format with no image fragments, mount the image, export the files to a folder and examine them. For image files, conduct steganalysis. On inspecting the file signatures, the hidden files are 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'**

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



- 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 '3338888888141414141414151515151515.'  
 (c) The result obtained on converting these numbers to alphabetical letters is 'C3H6N6O6' (CCCHHHHHNNNNNNNOOOOOO) 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.

```
File System Type: NTFS
Volume Serial Number: 0CB659FFB659EA2A
OEM Name: NTFS
Version: Windows XP

-----
METADATA INFORMATION
-----
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 256
Root Directory: 5

-----
CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 1913318
Total Sector Range: 0 - 15306558
```

**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.**

```
resfile.E01: 99.1% ..... 7.2 GB 00:00 ETA
resfile.E01: 99.4% ..... 7.3 GB 00:00 ETA
resfile.E01: 99.5% ..... 7.3 GB 00:00 ETA
resfile.E01: 99.6% ..... 7.3 GB 00:00 ETA
resfile.E01: 99.8% ..... 7.3 GB 00:00 ETA
resfile.E01: 99.9% ..... 7.3 GB 00:00 ETA
resfile.E01: 100.0% ..... 7.3 GB 00:00 ETA
Allocating work queues...
Work queues allocation complete. Building work queues...
Work queues built, verified.
Jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" -> 19 files
Carving files from image.
Image file pass 2/2.
resfile.E01: 0.1% ..... 10.0 MB 00:00 ETA
resfile.E01: 0.3% ..... 20.0 MB 02:11 ETA
resfile.E01: 100.0% ..... 7.3 GB 00:00 ETA
Processing of image file complete. Cleaning up...
Data.
Scalpel is done, files carved = 35, elapsed = 83 sec.
```

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



**Fig.14. carved image files**

```
C:\Users\seewy\Desktop\exiftool>exiftool C:\Users\seewy\Desktop\exiftool\security pitfalls.ppt
ExifTool Version Number : 11.14
File Name : security_pitfalls.ppt
Directory : C:\Users\seewy\Desktop\exiftool
File Size : 676 kB
File Modification Date/Time : 2018:01:02 12:49:20+05:30
File Access Date/Time : 2018:10:18 11:09:08+05:30
File Creation Date/Time : 2018:10:18 11:09:08+05:30
File Permissions : rwx-rwx-rwx
File Type : ppt
File Type Extension : ppt
MIME Type : application/vnd.ms-powerpoint
Current User : seewy
Title : Security Handshake Pitfalls
Author : Bo Sun
Last Modified By : seewy
Revision Number : 143
Software : Microsoft Office PowerPoint
Total Edit Time : 15.1 hours
Create Date : 2005:06:29 21:14:41
Modify Date : 2011:03:17 20:37:47
Words : 787
```

**Fig.15. metadata of the security pitfalls.ppt**

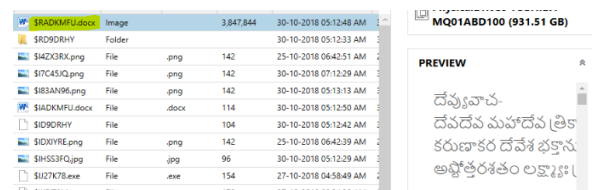
## D. Operating System

**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.

28-10-2018 11:05:06 PM.620	21128	17	Warning	System	Microsoft-Windows-WHEA-L...	A connected hardware error has occurred
28-10-2018 11:05:08 PM.742	21129	107	Information	System	Microsoft-Windows-Kernel-P...	The system has resumed from sleep.
30-10-2018 10:01:55 AM.500	21130	1	Information	System	Microsoft-Windows-Kernel-G...	The system time has changed to 2018-10-
30-10-2018 10:01:56 AM.384	1637	4042	Information	Microsoft-Windows-NCSC/Op...	Microsoft-Windows-NCSC/	Capability change on (0F0675B-60FF-4B
30-10-2018 10:01:56 AM.529	4210	10001	Information	Microsoft-Windows-Network...	Microsoft-Windows-Network...	Network disconnectedName: SicFi 10289

**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.

FileModifiedDate	FileAccessDate	FileCreateDate	FileLinkFileName	FileLinkPath	FileMOS	LinkModifiedDate	LinkAccessDate	LinkCreateDate	FileSize
11-10-2017 07:11 AM	07-07-2018 05:02 PM	07-07-2018 05:02 PM	CableLink YouCamLink	C:\Users\seewy\Desktop	3F98C08BCE5A54	23-10-2017 03:37 PM	15-10-2017 07:11 AM	23-10-2017 03:37 PM	992562
11-10-2018 06:46 AM	11-10-2018 05:46 AM	11-10-2018 05:46 AM	Edwin Mayh	C:\Users\seewy\Desktop	62222226077602	17-07-2018 10:36 AM	11-10-2018 05:46 AM	11-10-2018 05:46 AM	7580032
07-07-2018 05:24 PM	07-07-2018 05:24 PM	07-07-2018 05:24 PM	Microsoft Edge.lnk	C:\Users\seewy\Desktop	8A2AC025F95946	27-04-2018 04:37 PM	27-04-2018 04:37 PM	24-12-2017 08:31 AM	8192
01-11-2018 11:24 AM	01-11-2018 11:25 AM	01-11-2018 11:25 AM	perito - Shortcuts.lnk	C:\Users\seewy\Desktop	E0D0E6E959E0C3	01-10-2018 08:24 AM	01-10-2018 08:24 AM	01-10-2018 08:24 AM	384704

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



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

- 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.

```
-- Lnk #0 information --
Lnk target created: 2018-04-12 09:16:20
Lnk target modified: 2018-04-11 05:08:00
Lnk target accessed: 2018-04-12 09:16:20
Absolute path: My Computer\C:\Program Files (x86)

-- Lnk #1 information --
Lnk target created: 2018-04-12 09:16:20
Lnk target modified: 2018-04-11 05:08:00
Lnk target accessed: 2018-04-12 09:16:20
```

**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.

```
Executable name: IPCONFIG.EXE
Hash: EEA91845
File size (bytes): 9,932
Version: Windows 10

Run count: 2
Last run: 2018-11-01 09:33:54
Other run times: 2018-11-01 09:33:37
```

**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.

ST	RNAseq ID	Gene	Chromosome	Start	End	Strand	RefSeq ID	RefSeq Name	RefSeq Description
31	ENR001101237.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
32	ENR001101238.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
33	ENR001101239.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
34	ENR001101240.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
35	ENR001101241.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
36	ENR001101242.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
37	ENR001101243.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
38	ENR001101244.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
39	ENR001101245.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
40	ENR001101246.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
41	ENR001101247.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
42	ENR001101248.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
43	ENR001101249.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
44	ENR001101250.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
45	ENR001101251.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
46	ENR001101252.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
47	ENR001101253.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
48	ENR001101254.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
49	ENR001101255.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
50	ENR001101256.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
51	ENR001101257.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
52	ENR001101258.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
53	ENR001101259.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
54	ENR001101260.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
55	ENR001101261.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
56	ENR001101262.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
57	ENR001101263.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
58	ENR001101264.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
59	ENR001101265.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
60	ENR001101266.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
61	ENR001101267.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
62	ENR001101268.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
63	ENR001101269.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
64	ENR001101270.gcg	SRFBP1	618	587010	618	587010	SRFBP1	SRFBP1	SRFBP1
65	ENR001101271.gcg	SRFBP1	618						

**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.

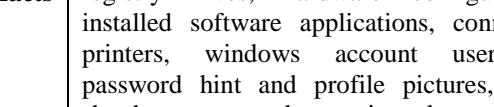
Path	Size	Stat	Last Modified Time	Mode	Type	Soft Key	Stat Modified Time
D:\Songs	654	14-08-2017 10:22:04 PM	Details	ShellHIcon (File)	Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\154		07-07-2017 10:41:11
D:\Songs	75	07-07-2017 10:40:59 PM		ShellHIcon (File)	Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\154		07-07-2017 10:41:11
D:\Songs\Full	124	14-08-2017 10:22:07 PM	Details	ShellHIcon (File)	Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\154		07-07-2017 10:41:11
D:\Songs\Full	1192	08-08-2017 11:03:13 PM		ShellHIcon (File)	Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\154		07-07-2017 10:41:11
D:\Songs\Old Songs	631	08-08-2017 10:45:42 AM		ShellHIcon (File)	Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\154		07-07-2017 10:41:11
D:\Songs\Old Songs\New folder	802	08-08-2017 10:57:45 AM	Details	ShellHIcon (File)	Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\154		07-07-2017 10:41:11

**Fig.22. shell bags persisting information**

### E. Registry

### Table V. registry artifacts

<b>Artifacts</b>	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.
------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

```

graph TD
    A[obtaining registry files] --> B[deleted registry file recovery]
    A --> C[extracting and viewing registry]
    B --> C
    C --> D[parsing the registry hives and probing for the artifacts]
  
```

The flowchart illustrates the process of registry recovery. It begins with 'obtaining registry files', which leads to 'deleted registry file recovery' and 'extracting and viewing registry'. 'deleted registry file recovery' also leads to 'extracting and viewing registry'. Finally, 'extracting and viewing registry' leads to 'parsing the registry hives and probing for the artifacts'.

**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.

	Name	Date modified	Type	Size
	Users	25-10-2018 12:11	File folder	
	default	15-10-2018 07:52	File	512 KB
	SAM	15-10-2018 07:52	File	128 KB
	SECURITY	15-10-2018 07:52	File	56 KB
	software	15-10-2018 07:57	File	1,00,864 KB
	system	15-10-2018 07:52	File	26,368 KB
	userdiff	01-07-2018 05:23	File	8 KB

**Fig.24. system protected files (registry)**

Add Bias: UTC +05:30 ☐ Window on top

Decode Format: Windows: 64 bit Hex Value - Little Endian

Example: FF03D2315FE1C701

Value to Decode: 783D3BC75192D301

Date & Time: Sun, 21 January 2018 08:14:37 +0530

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

	Run Co...	Registry Key Ma...	Regist...	Value...	Source
	regedit	02-11-2018 04:05:20 AM	1	a	PhysicalDrive0 - Partition 4 (Microsoft NTFS)
	eventvwr.msc		2	f	PhysicalDrive0 - Partition 4 (Microsoft NTFS)
	windows		3	e	PhysicalDrive0 - Partition 4 (Microsoft NTFS)
	cmd		4	d	PhysicalDrive0 - Partition 4 (Microsoft NTFS)
	C:\\$Recycle.Bin		5	c	PhysicalDrive0 - Partition 4 (Microsoft NTFS)
	notepad		6	b	PhysicalDrive0 - Partition 4 (Microsoft NTFS)

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

Known DLLs	31	YD_04E8A9C0_6860	330971ef4630e321	First Install Date/Time	08-08-2018 04:13:02 AM
Network Interfaces (Registry)	1	YD_04E8A9C0_6860	630004e04640a247		
Shm Cache	1,024	YD_04E8A9C0_6860	c0170370-cda3393	Last Install Date/Time	26-09-2018 11:51:07 AM
System Services	623	YD_04E8A9C0_6860&ADB	68338414640460	Last Removal Date/Time	26-09-2018 1:24:29 PM
USB Devices	38	YD_04E8A9C0_6860&ADB	68c7e78a60	Description	7804x7804
		YD_04E8A9C0_6860&Modem	68c7296c2780		

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

```
Thu Oct 25 06:39:24 208Z ROOT/ControlSet\Enum\STORAGE_VolumeSnapshot_HarddiskVolumeSnapshot\Properties\{3da2e317-27d4-4622-a309-3cfe4b700493}
Thu Oct 25 06:39:24 208Z ROOT/ControlSet\Enum\STORAGE_VolumeSnapshot_HarddiskVolumeSnapshot\Properties\{3da2e317-27d4-4622-a309-3cfe4b700493}
Thu Oct 25 06:39:23 208Z ROOT/ControlSet\Services\VSS_Diag\FPP
Thu Oct 25 06:39:23 208Z ROOT/ControlSet\Services\VSS_Diag\SystemRestore
ROOT/ControlSet\Services\WinSxS\Usersettings\S-1-y-2-a90f8756-13737031-23876f4215-1001
Thu Oct 25 06:34:52 208Z ROOT/ControlSet\Enum\PCI/VEN_8086DEV_d07H3C/SUBSYS_96820804REV_21_jk81m3j69v8z8m8FBV)
Thu Oct 25 06:34:34 208Z
```

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

			Value Name	Value Type	Data	Value Stack
Present/Outdated	8	3: 20:				
Present/Outdated	17	0: 20:				
Privacy	1	0: 20:				
Property/System	2	4: 30:				
Proximity	0	1: 20:				
Publish/Notifications	3	3: 20:				
Quality/Compat	0	0: 20:				
Reliability	6	6: 20:				
			TimeStamp/Interval	RegWord	1	
			LastCompensation	RegDz	SWEETY	
			600587	RegBinary	40-67-64-A4-C1-67-D4-01	09:05:12:00:00:00
			LastModTimeStamp	RegBinary	D0-6A-4D-08	53-6A-FF-FF
			DirtyShutdown	RegWord	1	
			DirtyShutdownTime	RegBinary	E2-07-0A-05-00-13-00-0A-00-23-00-38-00-9F-02	08:17:36:40

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

Microsoft Software Microsoft Office 12.0 Word File MRU	Item 6	REG_SZ	{F0000000}77... 28-10-2018 01...	108
Microsoft Software Microsoft Office 12.0 Word File MRU	Item 25	REG_SZ	{F0000000}77... 28-10-2018 01...	108
Microsoft Software Microsoft Windows Current Version Explorer	Screenshots	REG_DWORD	0x00000039 (9)	28-10-2018 02... 4

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

## F. Windows 10 Applications

**Table VI. Artifacts of windows 10 features**

<b>Artifacts</b>	Windows 10 notifications, cortana reminders 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.
------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

- a. From wpndatabase 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. BombersDigger 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.





Email Address	Display Name	Address Type	Created Time	Given Name	Surname
maheeshbabu@gmail.com	maheesh babu (maheeshb...)	SMTP	07-11-2018 06:20:02 PM	maheesh	babu
actor.nani@gmail.com	nani (actor.nani@gmail.com)	SMTP	07-11-2018 06:23:42 PM	nani	
samanthaakkineni@gmail.com	samantha akkineni (sam...)	SMTP	07-11-2018 06:16:33 PM	samantha	akkineni
trivikram@gmail.com	trivikram (trivikram@...)	SMTP	07-11-2018 06:21:07 PM	trivikram	
admin@insightsthehindu.com	Insight of the Day	SMTP	07-11-2018 06:16:08 PM		
einstein@yahoo.co.in	einstein (einstein@yaho...	SMTP	07-11-2018 06:24:36 PM	einstein	

Fig.44. email contacts in microsoft outlook

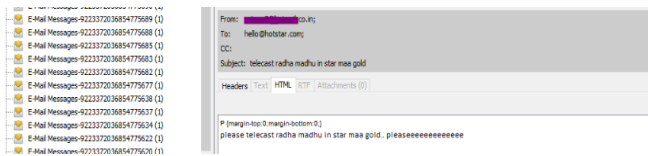


Fig.45. email extracted from thunderbird mailbox using Autopsy forensic tool.

contacts (107)	convos (403)	conversations_migration_data (1)	Conversations/ConversationsFields (1403)
10	403	1	1403

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



Fig.46. facebook timeline post



Fig.47. extracted twitter tweets from location username/appdata/local/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," 12<sup>th</sup> 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. Aniseti, "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](https://en.wikipedia.org/wiki/Windows_10)