

Disk Memory Forensics

Analysis of Memory Forensics Frameworks Flow

T.Prem, V.Paul Selwin, Ashok Kumar Mohan

TIFAC-CORE in Cyber Security,

Amrita School of Engineering, Coimbatore

Amrita Vishwa Vidyapeetham,

Amrita University – INDIA

Email: mr.premgowtham@gmail.com, paul.selwin@gmail.com, m_ashokkumar@cb.amrita.edu

Abstract - We have heard of Cyber Espionage where a spy was able to hide data and go unnoticed virtually. Using some forensics frameworks we can able to hide and retrieve data in any format both in Windows and Linux operating systems. Whatever the data are made to be hidden in the disk, some frameworks are very good at its carving technique which it analyze and give all the parts of the disk or any other memory devices. In this paper I have clearly explained how memory forensics frameworks analyze the memory of the hard disk drives. Some specific utilities are capable and designed specifically only for windows Operating system and at the same way some forensics frameworks are designed specifically for Linux based distributions. Here I have analyzed few frameworks that are currently good in conducting a digital forensic investigation. These frameworks are for a human resources internal investigation where unauthorized investigation into the server, or to select frameworks to conduct new investigation and these frameworks and suits will assist to conduct analysis of memory forensic, forensic analysis of hard drive, forensic imaging, forensic image exploration, forensic imaging and mobile forensics. Such that, they all designed in such a way that it has the features to bring back in whole depth analyzed report of its merits in its technique flow and about what's under the system hood.

Keywords - Anti-forensics, Disk Forensics, Offset, Hidden data, Frameworks, Slack Space, Investigation, Digital Evidences, Documentation

I. INTRODUCTION

The process of Disk forensics is the extraction of forensic data from digital storage devices like Hard disk, USB devices, CD, DVD, Flash drives, Floppy disks etc. Commonly the overall process of Disk Forensics comprises of Identifying digital evidence, Seizing & Acquiring the digital evidence, authenticating the digital evidence, preserving the digital evidence, analyzing the got Digital evidence, reporting the complete findings and as finally making a Document of it. Disk Forensics is identification of some source of digital evidences such as hard disks with interfaces like SATA/SCSI, Compact Disks, Digital Video Disks, Floppy disk, Mobiles, flash drives, PDAs, SIM Cards, USB storage, Magnetic Tapes, Zip media drives etc. After seizing the digital evidence at the crime scene. In this step, hash of the storage media that was seized will be computed using appropriate Cyber forensics framework. Based on the storage media content hash value with unique signature

is generated. After generating the hash value, storage device is completely sealed and took for further process of available digital investigation. Main core rules of Cyber Forensics is never work with original evidence. To make sure of this, original data was taken a copy as evidence for digital evidence collection and its analysis. Then the acquisition process of creating this exact copy, where original storage will be kept write protected and copying is made to conform that the complete data is copied into the destination directory of the media. This process of acquisition will be done in a Cyber Forensics centers or laboratories. Then the authentication of the digital evidence is done in Digital Forensics centers. Both the source media and destination media hash will be compared to ensure that both are similar, which make sure that the information of source device is an exact copy of the destination respectively. All Electronic evidences might be tampered or altered without any trace. Once the authentication along with acquisition have been completed, the original digital evidence need to be placed in secure manner keeping aside from radiation sources and highly magnetic areas. Another copy of the image will be taken and it should be stored into another reliable mass storage or any other appropriate media. Since optical media is fast, reliable and has longer span of life, it may be used as a mass storage. The process of analysis of collecting digital evidence involves searching for picture analysis, keywords, cookies, temporary, time line analysis, mailbox analysis, registry analysis, Internet history files analysis, database analysis, deleted item recovery, data carving and its analysis process, partition analysis after recovery, format analysis after its recovery, etc. Report of analyzed case need to be prepared with respect to the nature of examination as requested by investigation agency. It should have nature of the case, details of respective hash values, details of examination requested, evidence verification results, collected digital evidence and details of analysis conducted and examiner observation report and conclusion. The presentation of the report must be in easy terms and crispy way so that any non-technical persons can able to understand the case report. In Forensic the very important part is Documentation processing. Everything should be documented clearly to submit the case report in a court of law. Documentation need to be initiated from the plan of the case investigation and continues along searching in crime scene, seizing of material objects with Chain of Custody(COC), acquisition and authentication of

evidence, analysis and verification of evidence, collecting digital data evidence and reporting, preserving the material and till the closing of the taken case. In this paper I have made a report how most of the best forensics framework deals with disk memory forensics. Also I have observed its working and collected its relative merits.

II. NTFS DIGITAL DATA RECOVERY TOOLS IN RECOVERY FRAMEWORKS

What was renamed, what was deleted, Ignore known files and finding fragments among old files?

NTFS Recovery framework has relevant specific working category to help in both the investigation of corrupted and good New Technology File System disks. Compressed and Deleted files can be seen, along with all respective dates. Clusters with sectors used along with all data process get stored in the form of log file and both data with its respective directory of slack space can recovered [1]. If the disk was corrupted or attempted reformat, then the disk will be scanned to get rest of Master File Tables.

A. Sector to Examine

In every Operating Systems, NTF Systems has many areas that can be investigated in the disk. These investigation includes,

- Identifiable good known files
- OS files - checked with its hash values so that which may be skipped
- Deleted or removed files
- ADS - Alternate Data Streams
- Area of the data and area of the directory which is known as Slack Space
- Scanning all Master File Tables
- Unallocated sector or clusters
- Compressed area
- Files with respective dates

Added entanglement can include compression of data by the OS, sparse files and encrypted files. Framework can restore encrypted files, but external frameworks needed to be used for decryption. There exists operating system files and data files as a combination on every disks. To increase the speed of any digital investigation, it is necessary to neglect any files of Operating systems, fortunately to implement this, investigator must be completely sure about the evidence that it was not edited in any way known and for this Hashed verification shall be used. If a file is found with a hash that exactly matches a released file, having Windows operating system as a part or an antivirus package, then the further investigation is not necessary on it, as it is unchanged.

B. Identifiable good files

Among some investigations, the initial point will be the known good files that are identifiable. These are files that can

be read along the Operating Systems. And one particular import area of data will be respective dates that relate to the files. If any files are analyzed [6] with the OS, the date of last accessed will be altered. Recovery Framework will not alters anything on the device, but it will log all details of the dates and time as it is found. The information for any working file is the MFT which exists as a separate file in the main file log, also matched with its respective index files.

C. Deleted or removed files

Many people even now wonder about how a deleted file can be often recovered and read. Users unfortunately delete any file, they are delighted but this is not a good news for those who try to hide a file. Recovering deleted files normally will not depend on happenings about disk image after the alteration or removal. Any file gets deleted by flag allowed in the Master File Table and developing the table that shows the usage available. Fortunately, the pointers of the data into Master table not gets deleted. Files can be written again to the disk once deleted and there exists a possibility of the original file to get overwritten.

Digital Framework shows that investigating the recovered file is worth but such data should be handled with more care. Framework can restore all files that are found as removed or deleted into a separate tree of subdirectory which will be marked deleted.

D. Slack space as in Digital Forensics

Every NTFS disk will have two areas where this slack space is available, first in the main data area and second is at the place of directory. It is due to the reason that information on device can only be written which to be in are fixed sized sector blocks or clusters. If the data size is small than a cluster, then there will be an area of free space of non-defined raw data. This will be interesting, as this can contain data from an already removed memory of system at the time of input. Default cluster size for an NT File System formatted disk is in the format of 4K.[5] The main reason for the directory may have slack space is due to the small file size normally not more than 400-700 bytes are written to the end of an Master File Table rather than to take complete whole cluster. Forensic framework will then restore the slacks for next level of digital investigation. The slack directory is stored in a single file with individual header having tags, like

```
mft:sssss-mmmm .
...../...../mft
```

The shown two numbers are the physical sector (sssss), and the Master File Table's (mmmm) logical value [4]. For slack space that are found at the cluster end are stored as another second file. Now the data will be completely surrounded by the tags with its current structure. It need to be declared that no process is carried to enlarge slack area that was compressed in it.

cluster:sssss-cccc ...
...../ .../clust

sssss will be the sector value of the starting of the cluster, and ccccc is the respective cluster number value. The result file can be analyzed with suitable file viewer or other editing frameworks.

E. ADS - Alternate Data Streams

NTFS drives have the compatibility to store multiple data for any file. Secondary streams are hidden normally and Windows Explorer and DOS let not to show these streams. The streams are used to store special information or version details, but they may store complete data also. They can be interesting as a normal structured file that could have a secondary file with main information or more illegal images as possible. The utility kit will extract them after finding those. To differentiate the data, the name of the file will be corrupted by adding #- string at first and the extra stream name. The framework's log also gives the number of streams present in a file as a part of its file flag.

F. Unallocated space

Disk have unallocated space which is currently not used by the files that is they are full whole clusters that are presently left free. The reason behind interest will be due to the information from already deleted files. Recovery utility will analyze the clusters available and extract all the logical files. Scanning the space left unallocated and old files which are compressed with NT File System will be found decompressed. Thus Recovery process will be able to carve New Technology FS compressed disks.

G. Analyzing for all Master File Tables

Each file on any NT File system will have Master File Table entry. They will be stored in the _\$MFT file. When a disk been formatted or changes made to partitions, then the location of MFT also get change. So it is very useful to scan the whole disk area for available MFTs. This process may be little slow, but will help in identifying files that are not otherwise be able to get recover.

H. Files available in Master File Tables

As explained above on slack, it was shown that small files are written to the end of the Master File Table, rather than the original data part of the device. The default MFT size is 1024 bytes in length and files less than that will be 600 bytes. If the size of the file increases, the complete file is then allowed to store in a single normal cluster or more clusters. It must be noticed, that if a file then reduces in its size, it is then won't reallocated to the MF Table. The short file that may have written to the MF Table can be taken back as directory of slack data.

I. Orphan - Support file

While analyzing for complete MF Tables, it is usual to find files which exists no longer as a portion of the OS and also have no default PDS - Parent Directory Structure. This may also occurs when the disk structure got failure. The final solution occurred is mainly to create fake directories and finding them with the number of respective lost parent Master File Table. For example it can be dir_54379. All files related to that are stored in the respective directory, also including subdirectories. These fake directories will be in log as the final forensics report.

J. Logs

Important feature of digital forensic analysis is having a proper organized log of details which was found. With many forensic utilities of the program enabled, complete log will be provided which includes HASH (MD5 normally) for every file. Some results for respective tests are stored within forensic report even though much details is portion of the file of standard log. It includes complete dates, size of the files and attributes of the files along with exact position on the disk. If the directory of Scan Stubs is used then the log would act as a report of all file tables on that device.

K. Forensic report of XML

Forensic summary of XML of many logs directing to dissimilar stages of any recovery of disk. It comprises extension matching and signature of files and also mismatching respectively.

L. File respect to Sector

It is useful to control the file where a specific sector is present. If a disk was completely read, the data gets stored inside in the form of a log. For accessing this, we can use the normal search and add the number of the respective sectors while it gets prompted. The log file can be searched and the displayed files will be those files that the sector relates. Related attribute is the area of fragments of the log file. This shows all number of fragments which any file gets stored into. If the value gets checked twice, a list of all location of fragments and size of sectors are then shown. This feature is used when any damaged or bad sector is identified, finding which of the file is affected or any key word is identified in any raw partition discovery search, where was it get originated.

III. FORENSIC ANALYSIS OF FAT DISKS

Recovery done with many frameworks has reports for assisting investigation of FAT systems also. Most reports are Digital Forensic Report's part which are included in the options of Forensic framework.

A. FAT Analysis

Previous to the program attempt to read disk drive of FAT, then it is analyzed and some discrepancies are founded normally which are mostly related with its respective cluster pointers. Once the FAT is upgraded automatically, then the log file will store the changes.

- Difference among FAT Family The fat elements will be either considered or assumed to be correct only if the fat element points directly to the next cluster.
- Clusters points to itself. This may initiate the program to get looped on the same single cluster.
- The value then will be overwritten or rewritten with the following respective cluster location.
- For any valid file of FAT, there should consist an individual entry for every cluster.

From the directory of FAT, the following dates are fetched.

- Date and Time it's created.
- Date and time it gets modified.
- Accessed time - The time will not be a part of the FAT directory.

IV. UNALLOCATED PARTITION DATA RECOVERY

On most of the disks there will be data present in unallocated area. These are spaces which the operating system directs as empty space and it can be used to create new files. The answer for how much such type of data present is based upon the file that has been removed or deleted, with respect to the directory entry which has been cleaned, but to reduce the time taken, the number of sectors and clusters used to save data are not initialized first. Another way in which data can present in unallocated area is as the final result of the error on disk or program corrupt or crash.

Forensics framework recovery has two ways to recover data from unallocated space.

- By fetching entries of file that has been deleted.
- By fetching complete or some part of the disk and looking for start of the files.
- File entries are read that have been deleted.
- Looking for file starts by reading all parts of the disk.

The initial approach will be with an option within the recovery menu and is normally depend on the OS used. NT File System (NTFS) helps in great way at recovering most of the files deleted, as the Master File Table is just targeted as deleted and all the file location remain intact. Where available files are marked as overwritten if few of all of the data region has been used for other different file. A FAT system may point to the start of a file, but then it is just a guess on which where the file got saved. If it got fragmented then recovery is little bit harder. Next approach will be raw partition read. This can analyses the whole disk in which it can examine every parts of the device that has never used by the operating system. Files

are identified by analyzing the very first initial part for signature of known files but it will be always believed that the file must be clearly sequential. For big files the case is not same. As a advantage, on NTFS compressed blocks should be handled correctly. A final part where data may be available is in slack space. Slack space is the area found at the end of a cluster, left unused by the respective current file. It may have data from any previous file deleted in that location or the memory of the computer during writing. The process of data carving is the combining file fragments into a single file. The need is when an operating system has not succeeded in its attempt and a file exists but as many fragments in multiple places on the device. There are some ways to find the beginning and end of the file based upon the signatures and to know continuation of bytes. The problem in extracting a file correctly is discovering the slacks in-between the file. File beginning can be identified and for many types of file, the file is evaluated. This depends on pointers that are found throughout the file or may be just having a target pointer at the beginning, and evaluating the file end. For many file types, when the file extracted from beginning signature is invalid, the carving tools need to be applied by marking the fragments option. This operation method is different for each logical support format, but it is different when comes to overall scheme.

Once the Data carving is performed, all the sectors taken are portions of good known files that are marked as used. It is very important portion of the data carve function many file types are verified. Next approach will be raw partition read. This can analyses the whole disk in which it can examine every parts of the device that has never used by the operating system. Files are identified by analyzing the very first initial part for signature of known files but it will be always believed that the file must be clearly sequential. For big files the case is not same. As an advantage, on NTFS compressed blocks should be handled correctly. A final part where data may be available is in slack space. Slack space is the area found at the end of a cluster, left unused by the respective current file. It may have data from any previous file deleted in that location or the memory of the computer during writing.

V. ADVANCED DATA CARVING TOOLS BUILT INTO FRAMEWORKS

A. Processing fragmented files

Combining file fragments into a single file is known to be data carving. The need is when an operating system has not succeeded in its attempt and a file exists but as many fragments in multiple places on the device. There are some ways to find the beginning and end of the file based upon the signatures and to know continuation of bytes. The problem in extracting a file correctly is discovering the slacks in-between the file.

B. More than just file signature

File beginning can be identified and for many types of file, the file is evaluated. This depends on pointers that are found throughout the file or may be just having a target pointer at the beginning, and evaluating the file end. For many file types, when the file extracted from beginning signature is invalid, the carving tools need to be applied by marking the fragments option. This operation method is different for each logical support format [3], but it is different when comes to overall scheme. Once the Data carving is performed, all the sectors taken are portions of good known files that are marked as used. It is very important portion of the data carve function many file types are verified. When any file is shown as incomplete it is analyzed to show how much of the file is invalid or valid. This can be the first few KB or around 90%. Routines are used to find parts of the device that are not used apparently. The data in this respective sections are then analyses to find if they have any data that is suitable. For instance, if a JPG file was repaired, a section of pure text could be skipped. Also, to increase the chances of most favored recovery, starting sectors of each files that are recovered are analyzed. This is used to conclude the cluster location and size of the files. By looking at all clusters, fragments of files can be verified successfully for its suitability.

C. Forensic implications

Forensically, one need to be cautious on automatic data carving but for most of the users, the end results are highly useful. A test on a corrupted or sector damaged 2 GB memory chip will produce about 120 files that are good and corrupted will be 60. Once the data carving routine was run, up to 40 files that are corrupted can be reconstructed.

D. Carving Data on NTFS disks that are compressed

A significant characteristic of respective framework is that it processes NTFS cluster that are compressed and can carve files from the same NTFS compressed disks.

VI. RECOVERY FRAMEWORKS WILL HAVE SEVERAL FEATURES TO HELP FORENSIC INVESTIGATION OF CD'S

For multi-session ISO9660 each session is displayed as an individual track. A user can only see the end or track that is final but the recovery displays each track. All track can be restored independently which let any investigator to view how files were included and possibly how it were deleted. The log file also shows the time and date which every track was enabled after created to track down the complete history of the Compact Disk. The option is also available same way for DVDs and UDF CDs. Having this format, every session will have a virtual allocation table (VAT) saved at the end of the disk session. By making a search all over the disk and finding

the sessions, the files available on every session can be structured again and reconstructed. This will show files that can be deleted in future sessions or modified. To make it enable to scan all sessions the Scan all sessions feature will be available to proceed. Once recovery is undergone, all the sessions will gets displayed as a separate track and differences will be clearly detected. Also, the log file for this feature can be utilized to remove similar copies allowing files that have been modified or unique. For any situation of straight recovery, it is including a session that can make the device unreadable. By attempting to recover just the session of Penultimate and good recovery of whole files up to that current date may be reached and achieved. Different techniques will then be induced to the rest of the portion of the device and the sector range can be calculable from the data in the log file.

VII. VIEWING DVD PROPERTIES FROM UNSEEN AREAS OF THE DISK

There exists multiple portions of a DVD which are not visible to usual data command. The properties allows these parts to be investigated, with which it can be a useful portion of all forensic DV Disk investigation. The other information in this field is decoded actually and included as a portion of the forensic optional report. The function available relate to many different aspects and once selected the data associated is shown in Fig.1. Not every drives will show all features. Values are Big Endian with which it is high byte first.

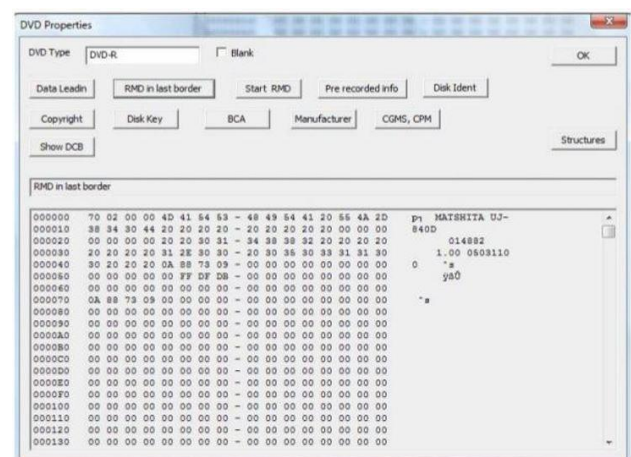


Fig 1. DVD Properties

A. Data Leadin

This area included the beginning and end of physical sector of the data part. The beginning sector will be often 0x30000 or 0x31000. Other fields contains size [2] and type of the disk as well as the count of layers.

B. RMD in last border

This contains information such as owner or manufacturer of the device. The information will be similar to

the Compact Disk RID code but will be in a different structure. By checking this data it is possible to show exactly which Digital Video Disk writer was used to create a disk.

VIII. LOCATING FILES THAT USE SELECTED SECTORS AND OVERWRITTEN FRAGMENTS

While undergoing a recovery, time comes there when some deleted file are overwritten. It is very useful to find when was that occurred and on what type of file. Frameworks inside the logged file support and give important solutions to these queries but it should also be marked that when a file was removed or deleted, the OS can utilize all the sector and entries of directory as it need and delete useful data. For tracking all the sectors, first it is must to perform a complete disk restoration that includes files that are deleted. This will store mandatory information inside the logged file that can be analyzed with having a search of sector and display of fragments.

A. Fragments display

Once the Frags available in the log column is selected, a fragment began to popup and also length of the run is also displayed. Up to now more than 60 fragments are made to display in this respective way on any forensic frameworks.

B. Sector Search

The search selection point in the log need a sector value and then it shows all file names which contains this sector. More files may present if the position has been taken by one or more files which have been deleted. Using two frameworks, it can be seen how a file that got deleted has corrupted and the time, dates and file names that was written into the sectors.

C. Overwritten files - Recovery

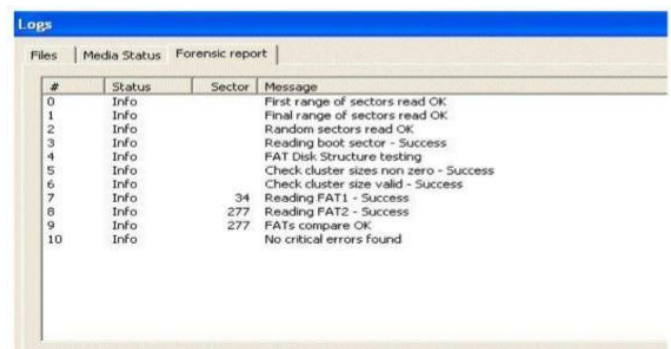
When any sector or cluster is overwritten it is fixed that the whole data that is available previously is lost or overwritten. With old drives, maybe before 2001, there exists possibility with government abled budgets for recovering any data from few sector that are overwritten and this might cause a big law of folk on such type of recovery. With a latest device with density higher this is now not possible and any framework or tool that tells it is possible is being really creative. The only helpful way to recover any overwritten file easily is through identifying other similar copy – that is backup.

IX. SCANNING AND ANALYSIS OF CONTENTS OF A DISK

When beginning to analyze a new device it is very useful to find an idea of what will be on the disk and also about its location. The Disk Scanning will helps with the problem by providing a visual content display of the device. This feature provides a visual display on the disk how it has

been utilized and so displays portions that has used and an indication of the data types. To bring analysis simpler, different layers of the drive may be categorized separately [8]. The functions can be done on all disk type even it is totally corrupted file system. It is possible to zoom in some particular areas of the drive for detailed display. By viewing parts of the disk that has been used, it can isolate unallocated parts of the device and also check if the sector or cluster exists blank. The bitmap screen points the sector that present on the device and they can be picked and analyzed. When the sector is checked with the mouse, the displayed screen will provide sector numbers and explains how sectors has been identified. The display has some limited count of listed status lines and each line of status will represent more than one sector. This happens when the color would be chosen for the important summary, this file line will be displayed rather than an empty line sector. By altering the boxes each and every layer can be made to seen separately. As the analysis doesn't dependent on analyzing the disk, every types of device can be scanned and analyzed. It will detect prescribed sectors of the system and sector directories from all known available types of devices.

X. FORENSICS REPORT



#	Status	Sector	Message
0	Info		First range of sectors read OK
1	Info		Final range of sectors read OK
2	Info		Random sectors read OK
3	Info		Reading boot sector - Success
4	Info		FAT Disk Structure testing
5	Info		Check cluster sizes non zero - Success
6	Info		Check cluster size valid - Success
7	Info	34	Reading FAT1 - Success
8	Info	277	Reading FAT2 - Success
9	Info	277	FATs compare OK
10	Info		No critical errors found

Fig 2. Log report

The forensic final report is the feature that plays a portion of the Fig.2 Forensic logging option. It is structured to keep track every actions that have been taken over the disk, [7] full description of errors and also tests so far taken.

XI. CONCLUSION

In general, having the disk memory forensics steps, we have analyzed the data collected from social network account backups and successfully analyzed its file type with its security and protection parameters that are stored into different disk formats such as NTFS and FAT. Even though the data that are backed up from social sites are mapped using semantic matching algorithm for ensuring link establishment, they can be easily figured out its file systems and recovered when comes to carving methodology from disk clusters. In a digital world, all scene of crime will be initiated with lot of

evidence that can be reliably and also validly analyzed. Every part of digital evidence will be perfectly targeted, gathered, stored, analyzed till it admitted to court and it given its proper value by finding facts. Limitations occurs each step of the process from the scene of crime to court preventing the system from getting perfect justice. Science isn't only the perfect and all forensic science methods and disciplines affected with shortcomings. Finding where the limits occurs and by knowing how to increase the efficiency of the complete procedure are very important skills for each forensic scientist. Similarly, clearly knowing the limitations of all relevant technology is also important for both evidence examiners and legal professional experts facing court discussions of digital investigation reports.

REFERENCE

- [1] John, J. L. (2012). Digital forensics and preservation. Digital Preservation Coalition.
- [2] Amritha, P. P., Sethumadhavan, M., & Krishnan, R. (2016). On the Removal of Steganographic Content from Images. *Defence Science Journal*, 66(6), 574.
- [3] Kaur, M., Kaur, N., & Khurana, S. A Literature Review on Cyber Forensic and its Analysis tools.
- [4] Barakat, A., & Hadi, A. (2016, August). Windows Forensic Investigations Using PowerForensics Tool. In *Cybersecurity and Cyberforensics Conference (CCC)*, 2016 (pp. 41- 47). IEEE.
- [5] Larson, S. P. (2009, January). Concerning File slack. In *Proceedings of the Conference on Digital Forensics, Security and Law* (p. 103). Association of Digital Forensics, Security and Law.
- [6] Alazab, M., Venkatraman, S., & Watters, P. (2009). Effective digital forensic analysis of the NTFS disk image. *Ubiquitous Computing and Communication Journal*, 4(3), 551-558.
- [7] Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of digital evidence*, 1(4), 1-12.
- [8] Gohel, H., & Upadhyay, H. (2017). Cyber Threat Analysis with Memory Forensics. *CSI CommunIcatlonS*, 5.