Survey of Forensic and Analysis Tools based on Grouping of Digital Evidence using Metadata Functionality

Anubhav Kumar Vaid
School of Information Technology
RGPV, Bhopal, India

Yogendra P.S. Maravi
Professor
School of Information Technology
RGPV, Bhopal, India

Jitendra Singh Verma
Faculty
School of Information Technology
RGPV, Bhopal, India

ABSTRACT
Computer forensics can be defined as obtaining computer storage media so that data can be used as evidence in court. Traditionally the analysis of sources of digital evidences is done by examining the artefacts and metadata of artefacts for authenticating the gathered information and sequencing them in the manner they occurred. Analyzing the information acquired by forensic investigator in traditional way is a cumbersome task but it can be overcome if all the related artefacts are grouped together on the basis of metadata information they prevails. This paper is mainly focused on metadata based association of digital evidences which can simplify the task of forensic investigator and can also help in reducing human intervention making the process automatic. The main objective of this paper is to study working principal and compare different existing forensic tools on the basis of various parameters such as capability for accessing digital evidence, sources they can examine, metadata parsing capability, and analyzing them that whether they can provide grouping of different artefacts present in same or different investigating sources on the basis of metadata they contain.

General Terms
Survey of Forensic tools on the basis of metadata extraction property.

Keywords
Digital evidence, Binary abstraction, File system and schema support, Metadata, Evidence composition

1. INTRODUCTION
While performing a forensic analysis the investigator is primarily investigating for the answers of six basic questions like who, when, where, how, why and what [1]. For getting the answers of when, what and who investigator needs the knowledge of artefacts and metadata of artefacts of the source of digital evidence. Answers for where, how and why require the in depth analysis of whole systems metadata. For gaining the answers pertaining to all these six questions investigators uses tools for acquiring and analyzing the information's form the digital evidences, but the tools itself poses different challenges for investigator. Generally the tools are designed for doing specific tasks i.e. tools are highly specialized in performing a particular task, like tools named Encase and FTK can be used for computer based digital evidences only. This is so because they can retrieve data from hard drives and memory dumps only. Another that can be faced by the investigator while operating on tools is that generally tools are not inter operable because of their specialized nature which makes it difficult to integrate different functionalities of different tools..

1.1 Metadata
Metadata is a data which is structured in nature and is used for characterizing a resource. Generally metadata is defined as "data for a data" but in practical aspect it is not always true rather it should be defined as "data about data contents" or "content about contents". Metadata can provide much information like publisher of document, owner, reviewer, author, as well as information's regarding the storage place of networked activities and it may give the information of the unique identifier in the computer on which the document was created [2]. For example Timestamps can be taken as one such type of metadata which is used in the forensic investigation and its analysis plays a crucial role in digital forensics. Timestamps are used for generating a sequential timeline of activities necessary for an investigation. These Sequential timestamps generates sequenced events, and this process is referred to as digital time-lining. The main focus of the paper is to get a closer look on the metadata information on basis of which comparison among the working principles of different existing tools for forensic investigation can be done.

1.2 Digital Artifact
Another crucial area in which this paper focuses is the digital artefacts of digital evidences. It is so because an investigator uses forensic tools for gathering evidences by examining the digital artefacts. Hence the basic knowledge of which is necessary for comparing the working principals of different tools. A forensic investigator always encounters the problem pertaining to the alignment of different sources to substantiate digital evidence by finding a relation on basis of the information between them. As each and every type of digital evidence, which are not of same type, have plentiful metadata [3, 4], it can act as the common medium for finding the natural relationships that are frequently present in digital evidence. Carrier and Spafford [5] noticed that metadata can be a common link for defining the individuality of a digital object. All digital objects are evidence to a minimum of one event and the metadata of artefacts contains information which shows the state in which a digital object was at the time the crime had taken place. In this paper, a digital object is considered along with the metadata associated to it as a digital artefact. These associated metadata of digital artefacts can correspond to events and thereby can be very handy in reconstructing the events as per the sequence in which they had occurred. For clear understanding we can think of simple examples like, creating a file on a file system is a type of file-event, when we access a file it is different type of file-event, looking from different view point when we visit a web page it is a type of Internet-event and so on. This kind of abstraction

provided by digital artefact forces to focus not only on syntactic value matches but also the semantics which acts as a link between these matches. Thus by analyzing one or more digital artefacts can help in rebuilding the event sets that are responsible for generating these artefacts.

1.3 Classification and Grouping Of Artifacts

Specifically, forensic and analysis tools are capable for classifying the artefacts by utilizing the file metadata or log or network attributes being parsed, but one attribute at a time. The commonly used attributes for analyzing purposes are name of owner of file, username, last time when the file was modified or timestamp in which the events had occurred, by using IP address of source or destination. Conversely, when there is a need for in depth analysis, classification of the artefacts are done and that too is performed multiple times with different attributes. Performing the task in this way can be painstaking in few cases, chiefly, when there are unknown attribute or combination of attributes which hold the answers. This technical gap is more evident when the sources of digital evidence contain different file and log formats or different source types.

2. DIGITAL FORENSICS: A MULTI-STAGED SCIETIFIC PROCESS

According to the Digital Forensic Research Workshop (DFRWS) 2001 report [6] has defined digital forensic science as follows:

"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." Collection of various stage process initiating from identifying a digital media as an impending evidence to submitting a final analysis report in court as per the law of the country in which the crime done is under trial is known as digital forensics. The aim of a digital forensic investigation is the rebuilding of events occurred in past so that a clear knowledge of incident can be obtained which is being investigated.

2.1 Evidence Identification

The preliminary or the starting stage of digital forensic investigation process is the identifying the sources or objects which could be potential digital evidence. In this stage, one or more sources are identified as the probable source of evidence. Possible sources which could be taken as source of investigation are devices like hard disk in computer which is mainly used for storing data. Other examples of it could be random access memory card or it could be USB storage devices or it may be mobile phones PDAs etc..

2.2 Evidence Preservation

The second stage of digital forensics are evidence preservation in which the task of forensic investigator is to preserve data by using hash signatures like MD5 or SHA1 so that integrity of data collected can be maintained. Except these data investigator deal with other data also like documents stored in a computer, telephone contacts list calls made, voice and video files, email and SMS conversations, patterns of network traffic, detecting intrusion of viruses etc. Another work to be performed by the investigator is to copy all the user data and its associated metadata including activity logs and system logs to different location or storage device so that they can examine the data collected in isolation without changing the original data collected[7,8,9].

2.3 Evidence Examination

The third stage of digital forensic investigation is evidence examining stage in which the task of an investigator is to examine the data collected using one or many forensic tools which can provide them multiple file system level abstraction and can support schemas using which a forensic examiner can interpret or access raw binary data. According to Casey [1] forensic examination can be defined as the process involving extracting of information from digital evidence and making them available for analytical purpose. There may be cases, when the examination of digital evidence reveals the hidden or not-so explicit information, which has to be extracted and then analyzed. This process of finding such information is known as evidence discovery.

2.4 Evidence Analysis

The stage Evidence analysis which is the fourth stage of digital investigation starts after the sources of evidence and the data being extracted are analyzed for determining the sequence in which the events occurred leading to the reported incident under investigation. According to Casey [1] forensic analysis can be defined as the appliance of scientific methods and critical thinking to deal with the primary questions in an investigation like who, how, why, what, when and where

2.5 Documentation and Presentation

The last stage of forensic investigation is documentation and presentation stage in which the work performed in every stages are that the individual stages are methodically documented and prepared for presenting them in court as per law. Seldom there is a requirement for evidences to be presented in court and when required are presented under the guide of expert witness.

3. MODELLING THE DIGITAL FORENSIC PROCESS

The work of digital forensic investigator argues with different types of digital evidences like forensic images of disk, images of local files and folders, of file images, network packet traces and memory dumps thus making an investigator to deal with diverse nature of digital evidence examination. Except the diverse nature another obstacle for an investigator is lack of similarity in the way the evidence can be acquired, examined and analyzed. The Digital Forensic Research Workshop (DFRWS) 2001 report [6] illustrates the challenges faced in the field and called for new approach to broaden a better understanding of the digital forensic process. Several models of digital forensic process have been proposed in the journalism. Principally, these models deal with the definition of the general stages in a digital forensic investigation. The four broad stages were identified by McCamish [10] which are involved in a digital forensic investigation they are:-

1. Identifying digital evidence;
2. Preserving the digital evidence;
3. Analysing the digital evidence; and
4. Presenting the digital evidence.

The important models among the proposed forensic models are the physical investigating process model [8], hierarchal objectives framework [11], the Hadley IO model [12], the computer history model [13] and concept of digital evidence

bag model [14, 15]. Among these models the physical investigation model and the hierarchical objectives framework deals with the model the whole process whereas the Hadley model and digital evidence bags accentuate how digital evidence can be acquired. On the other hand the computer history model focuses on the process of reconstruction. Similarities among the digital investigation process on the basis of its physical twin was observed by Carrier and Spafford [5] ; which proved the cross-applicability of many techniques used in the traditional form of physical forensics adopted into its digital sibling. An objective hierarchical objectives framework based framework for digital forensic process was proposed by Beebe Clark [11] which was divided into six stages proposing a 2-tier hierarchical objectives framework. The six stages stated in this work are:-

1. Preparation,

2. Incident response,

3. Data collection,

4. Data analysis,

5. Presentation of findings; and

6. Incident closure.

The objectives of these stages are defined by sub dividing the six stages into further sub stages. Events occurring in a computer can be thought of an input and output sequenced series. According to the layered model Hadley [12] input and output in computer is the sequence of translations followed by transport of data. The Hadley model is basically a hardware model of computer which is used in identifying all input and output sources of digital evidence in a computer. This model is not used in explaining digital evidences which are generated by information flow on computer networks, external storage devices, log files and many such active devices like mobile phones, PDAs, MP3 players etc. There was an attempt made by computer history model [13] for formalizing digital evidences using a finite state automaton but at last it concluded that the task cannot be accomplished due to the size of resulting state space.. Hosmer [16] lighted the importance of data in digital world and hence stated that every operation performed on digital evidence should be audited as there is chance for data getting altered copied or erased so the following principles should be followed while conducting an investigation on the digital data. The principals to be considered are:-

1. Authentication of data under investigation,

2. Integrity property,

3. Access control, and

4. Non-repudiation,

A need for standardizing the forensic process was proposed by Myers and Rogers [17] on basis of education and certification. An automated bibliography of different forensic model was presented by Pollitt [18] in which legal constraint of various forensic process model was examined. Another independent examination of the digital forensic models and examination of its implication in the perspective of the challenges that were highlighted in the report of DRFWS 2001 was presented by Reith et al. [19]. For the advancement of digital forensic field in 2003, Mocas [20] recognized three key challenges. These challenges stated by him were:-

1. Advancing technology used in forensic and the need to accept advanced architectures;
2. The need for adopting uniform programs in certification and starting courses in digital forensics;
3. The need for changing permissibility laws in courts regarding digital evidence.

4. DATA CARVING

Evidence examination is conducted to recover the deleted or partially present file data which are used in investigation purposes and this process of recovering from such data leads to the rise of new field known as data carving. It can be defined as the process of identifying file types with the use of magic numbers which are a string of bytes. Magic numbers from a memory image are mapped with a database of known magic numbers to recover deleted or partially deleted files [21]. Magic numbers are unique to each format and hence these constant binary streams are used for identifying a file format. Carving is performed on a disk when there is a need for analyzing unallocated file system space so that files can be extracted when data cannot be identified because of missing allocation information. Carving of files is done from the dumped traffic using the same techniques. A possible shortcoming of carving process on disks or images is that file carving tools usually produces many false positives [21]; hence tests are required to be done on each of the extracted files so that tier consistency can be checked. Huge storehouse of such file types and headers are then integrated into all forensic tools which are then used in examining the portion of data that are needed to be carved with the file signatures references. A high performance file carver called Scalpel used for carving files from hard disk images was proposed by Richard and Roussev [22]

5. DATA HIDING AND STEGNOGRAPHY

Evidence discovery can be defined as discovery of new information from digital evidence. Stenographic content or hidden information discovery is an example of evidence discovery. Steganography can be defined as the art of writing hidden messages in such a way that no one, except the sender and intended recipient, can suspect the presence of any message. In digital Steganography information can be kept hidden inside document files, image files, programs or protocols. For Steganography transmission generally media files are considered ideal since media files have large size. For detecting stenographic information a saturation view technique was proposed by Hosmer and Hyde [23] and they had also discussed several challenges posed by steganography. Other contribution was made by Lee et al [24] in stenography detection. They presented an approach in which they combined computer graphics principals with AI reasoning for detecting anomalies present in image. Falsifications in image are classified under four categories, they are: deletion, insertion, montage of photos and false captioning. The approach proposed by Hosmer and Hyde works by segmenting a given image, and computing the importance map on regions of importance and employs a rule based reasoning component for determining falsified status. Other important contributions were done by Hargreaves et al. [25] when they described the challenges posed in forensics in Windows Vista format, and Park et al. [26] where they

described the detailed study on data suppression and detection in Microsoft Office 2007 files.

6. FORENSIC TOOLS

Many computer forensic tools are available for investigation both in the commercial and in the open domain. Generally used forensic toolkits for the purpose of analyzing file systems are Encase tools, FTK tools, X-Ways tools, and Nuix tools, TCT, Sleuth kit, DFF, OCFA, Snorkel and LibForensics. Among these tools Encase, FTK and X-Ways 4 are commercially available toolkits on the other hand tools like TCT, Sleuth kit [27], DFF, OCFA, Snorkel and LibForensics are available in open domain. Amongst the above mentioned tools, many commercial varieties of available tool also support the facility for examining the memory dumps and mobile device flash memories. Working principle of all forensic tools are that they take a forensic image of the "source" as input and provide necessary binary abstractions to raw data due to which it becomes possible to read entire source as a binary stream of data. In this paper these characteristics are referred as the binary abstraction. These tools can also help in distinguishing the different files along with their application formats on the file systems by using standard file signatures [28]. An addressable feature of this technology is the development of the known file filter (KFF) which helps in omitting the system files during evidence examination procedure. In this paper the characteristic of file recognition and automatically associating them with their application are used for parsing the file as file system support. The two functionalities a) file recognizing and b) automatically associating those with their applications tackle the problem of complexity in digital evidence [29]. The forensic tools can extract file system metadata which are associated with each file including the location of the file, MAC timestamps, file ownership; file size etc. In general forensic tool does not rely upon application metadata and hence cannot be used in extracting or parsing them. For availing that property investigator have to use the analysis tools.

7. ANALYSIS TOOLS

The analysis tools are used for direct access to the "source" and can parse the contents as self-governing records every record may have many attributes, together with timestamps, that are parsed for analyzing purposes. This property can also be broadly placed under the schema support, which acts as part of the file system supporting layer. The capability of parsing or extracting metadata, including the file system metadata, application metadata and all the related attributes of an artefact in a non-conflicting manner is known as metadata parsing. PyFlag, GrokEvt, libevt, Event Log Parser are few log analysers that can parse the relevant logs with their attributes. In general, the attributes present in relevant logs contains a description of events, associated user names with the event, timestamp of events etc. Wireshark and tcpdump are the tools used for parsing the analogous attributes from network packet captures. A packet sequence number, protocol for communication, source and destination IP addresses, hosts' MAC addresses, hosts 'operating systems and browser applications etc. are available in network packet captures.

8. INDEXING AND QUERRYING DIGITAL EVIDENCE

XIRAF, XML based indexing and retrieval of stored digital evidence for querying has been proposed by Alink[30]. The XIRAF architecture is indexed into raw disk images which help in storing digital evidence in an annotated XML format. The XIRAF is a framework which consists of three subsystems; the tool repository, the storage subsystem and the feature extraction manager. The work of feature extraction manager is that it handles the various feature of different extraction tools and then integrates their outputs into XML which are then stored in the storage subsystem. XQuery is a query engine which is used to query the XML database for the information of related digital evidence. Precisely it can be said that over the years, researchers have developed new ways for examining sources of digital evidence and had discovered potential sources of evidence using one or more forensic tools. However, the process of investigation has largely remained manual and labor intensive process, and the growing volumes of digital evidence had made the challenge even more complicated.

Table 1. Tabulating the Respective Functionalities of Various Forensic and Analysis ToolsThe symbol "√ "denotes presence of particular functionality and "x "denotes absence of that functionality

Forensic Tools	Digital evidence access	Sources that can be examined					Metadata parsing & extraction	Ability to Identify correlation
	Binary abstraction	File system	Main memory or RAM	Log	Network data capture	Key word search		
CAINE[31]	×	×	√	√	√	√	√ (username, device serial number etc.)	×

BKF Viewer[32]	×	√ (can view only)	√ (can view only)	√(can view only)	×	×	×	×
Browser History Capturer[33]	×	×	×	×	√(from windows computer only and supported browsers are Chrome, Firefox, IE and Edge only)	√	√	×
Wireshark[2]	√	×	×	×	√	√	√	×
PyFlag[2]	√	√	√	√	√	√	√	×
Encase[2]	√	√	√	×	×	√	Only file system metadata	×
FTK[2]	√	√	√	×	×	√	Only file system metadata	×
Sleuthkit[27]	√	√	×	×	×	√	Only file system metadata	×
AssocGen[34]	√	√	×	√	√	√	√	√

9. DISCUSSION

We have studied many research literature related to forensic tools in previous section after that we can say that binary abstraction are provided by all forensic images and memory dumps. Although some commercial toolkits can support file system images as well as memory dumps many open source forensic tools can primarily handle only file system images in different image formats .Information regarding metadata associated with file activity are available in File system which are independent of file content. Metadata are very important for identifying the owner of the file, MAC timestamps, privileges of access granted etc. but most of the tools are not able in extracting or utilizing application metadata from file which are a valuable source of information. Every forensic tools uses text indexing and searching method on the image by classifying the artefacts present in the image on the basis of the file system metadata. Although the tools are capable of supporting multiple forensic images, they cannot associate the different metadata across files and hence are not able in

alerting a forensic investigator when related metadata are found. Additionally, log files which can also be found on many file systems are processed like files by the tools thus they have to be exported for analysis. Nearly all analysis tools, with the probable exclusion of Volatility or Wireshark, cannot offer binary abstraction. The tools have the capability of interpreting the contents and processing the data as independent entries while parsing the relevant attributes for reporting. The analysis tools can usually process a single source at a time and rarely support indexing and searching. The analysis tools can classify the log on the basis of parsed attributes; yet the functionality for combining multiple attributes for deriving semantic relationships is also essential. Both forensic and analysis tools cluster their relevant contents by using two techniques, a)keyword filtering and b)attribute classification. It is a basic requirement to filter the contents on the basis of dissimilar keywords or classify them based on different attributes during analysis for determining a pattern. Obviously, these techniques are performed by human and hence if the right combination of keywords and attributes are not specified, then required pattern is likely to be missed. Some attributes may be clustered during categorization in sequential manner. The most general way of combining attributes for categorization as reported by authors Minack E and Zander S [35, 36] involves combining of the timestamps with owner for forensic images, username required for log files and IP address required for capturing network packet. After that remaining metadata and attributes are largely remains unutilized. Usually in computing environments, hard disk drives are considered as dominant source of digital evidence and analysis is mainly conducted on files. However recently, in addition to hard disks, data is also found on volatile memory, log files and network packets, in various formats due to which system and application logs, volatile memory images and network packet traces have become equally important areas of searching evidences. When diverse sources of evidence are analysed using conventional tools, redundancy in processing the evidence becomes inescapable. Digital evidence contains four parts; source, process (examination and analysis), outcome, and consolidation. Each part is required for generating related reports that are mugged up in the final step. The literatures which are discussed in previous section underlines basic requirement for analyzing dissimilar sources of digital evidence to arrive at a consolidated outcome. For overcoming the above mentioned drawbacks a tool AssocGEN[33], has been developed by Sriram Raghavan and S V Raghavan. It is an engine based on FIA architecture [37, 38h] which can integrate forensic disk images, file systems, system and application logs and network packet captures by integrating heterogeneous or diverse digital artefacts working on the principle of metadata based associations

10. CONCLUSION

In this paper, a methodical study of existing forensic and analysis tools is presented which are used for examining and analyzing digital evidences. On closely reviewing working principle of the existing tools we can say that metadata have significant role and it can be used across heterogeneous sources of digital evidence for validation and analysis. In this paper, we can compare various existing forensic tools based on various parameters and discussed their disadvantages. On the basis of this comparison we can frame a conclusion that present-day forensic tools are able to find new pieces of digital evidence but are not able to analyze evidences. Hence the analysis continues to remain largely done manually. This paper also highlights the need for consolidating the research findings into a more combined form of forensic examination providing a flawless alteration to analysis, especially with multiple sources of digital evidence. Hence we can say that metadata based forensic tools are required for handling different sources of digital evidence. The final conclusion that can be drawn from this paper is that there exist a wide range for developing capable algorithms which can be used for identifying metadata based associations in digital evidence and grouping the related artefacts.

11. REFERENCES

[1] Casey E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Academy Press Publications 3/e, ISBN 978-0-12-374268.

[2] Raghavan. And Raghavan S. V. (2013). A Study of Forensic and Analysis Tools, in Proceedings of the 2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE), IEEE 978-1-4799-4061-5, Hong Kong, China, Nov 21-22, 2013.

[3] Buchholz F and Spafford E H. (2004). On the Role of System metadata in Digital Forensics, Digital Investigations, 1(1), pp. 298-309.

[4] Garfunkel S L. (2009). Digital Forensic Research: The next 10 years, Digital Investigations, In Proceedings of the 10th Annual Conference on Digital Forensic Research Workshop (DFRWS '10), Vol. 7(2010), pp. S64-S73.

[5] Carrier, B. D., & Spafford, E. H. (2004). An Event-based Digital Forensic Investigation Framework, Paper presented at the 4th Annual Digital Forensic Research Workshop (DFRWS '04).

[6] DFRWS Technical Committee. (DFRWS) (2001). A Road map for Digital Forensic Research: DFRWS Technical Report, DTR - T001-01 FINAL

[7] Carrier B D. (2005). File system Forensic Analysis, Addison Wesley Publishers, ISBN 0-32-126817-2

[8] Casey E. (2007). What does "forensically sound" mean? Digital Investigations (Editorial), Vol. 4(1), pp. 49-50

[9] Garfunkel S L., Malan D., Dubec K., Stevens C and Pham C. (2006). Advanced Forensic Format: An Open Extensible Format for Disk Imaging, Proceedings of the Second Annual IFIP WG 11.9 International Conferences on Digital Forensics, Advances in Digital Forensics II, M. Olivier and S. Shenoi (Eds.), Springer, Boston, 2006. (ISBN: 0-387-36890-6) pp. 17-31

[10] McKemmish R. (1999). What is Forensic Computing? Australian Institute of Criminology: Trends and Issues in Crime and Justice, ISBN 0-642-24102-3, No.188, pp.1-6.

[11] Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), pp. 147-167

[12] Gerber, M., & Leeson, J. (2004). Formalization of computer input and output: the Hadley model. Digital Investigation, Vol. 1(3), pp. 214-224.

[13] Carrier, B. D., & Spafford, E. H. (2006). Categories of digital investigation analysis techniques based on the computer history model. Digital Investigation, the Proceedings of the 6th Annual Digital Forensic

ResearchWorkshop (DFRWS '06), 3(Supplement 1), pp. 121-130.

[14] Hosmer C. (2006). Digital Evidence Bag, Communications of the ACM Vol. 49(2), pp. 69-70.

[15] Pal A, Sencar H T and Memon N. (2008). Detecting File Fragmentation Point Using Sequential Hypothesis Testing, Digital Investigations, Proceedings of the 8th Annual Digital Forensic Research Workshop (DFRWS '08), Vol. 5(Supplement 1), pp. S2-S13.[29] Carrier B D., (2003),

[16] Hosmer C. (2006). Digital Evidence Bag, Communications of the ACM Vol. 49(2), pp. 69-70.

[17] Myers M and Rogers M. (2004). Computer Forensics: A need for Standardization and Certification, Intl. Journal of Digital Evidence Vol. 3(2), pp. 1-11

[18] Pollitt M. (2007). An Ad-hoc review of Digital Forensic Models, IEEE Publication, In Proceedings of the Second Intl. Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '07).

[19] Reith M, Carr C and Gunsch G. (2002). An Examination of Digital Forensic Models, Intl. Journal of Digital EvidenceVol.1 (3), pp.1-12.

[20] MocasS.(2004).Building theoretical underpinnings for digital forensics research. *Digital Investigation*, Vol. 1(1), pp. 61-68.

[21] DFRWS Technical Committee. (DFRWS) (2001). A Road map for Digital Forensic Research: DFRWS Technical Report, DTR - T001-01 FINAL

[22] Richard III, G. G., and Roussev, V. (2005). Scalpel: A Frugal High performance File Carver, Paper presented at the 5th Annual Digital Forensics Research Workshop (DFRWS '05)

[23] Hosmer C and Hyde C. (2003). Discovering Covert Digital Evidence, Paper presented at the 3rdAnnual Digital Forensic Research Workshop (DFRWS '03).

[24] Lee S, Shamma D A and Gooch B. (2006). Detecting False Captioning Using Common Sense Reasoning, Digital Investigations, Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06) 3(Supplement 1), pp. S65-S70.

[25] Hargreaves C, Chivers H and Titheridge D. (2008). Windows Vista and Digital Investigations, Digital Investigations, Vol. 5(1), pp. 34

[26] ParkB,ParkJandLeeS.(2009).Data Concealment and Detection in Microsoft Office 2007 Files, *Digital Investigation*, Vol. 5 (3-4). pp. 104-114.

[27] CarrierBD,(2003),Sleuthkit,http://www.sleuthkit.org/sleuthkit/, last retrieved on July 12, 2011

.

[28] CarrierBD.(2005).Filesystem ForensicAnalysis, *Addison Wesley Publishers*, ISBN 0-32-126817-2

[29] Carrier, B. D., (2003). Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. *International Journal of Digital Evidence (IJDE)*, Vol. 1(4), pp. 1-12.

[30] Alink, W., Bhoedjang, R. A. F., Boncz, P. A., & de Vries, A. P. (2006). XIRAF - XML-based indexing and querying for digital forensics. Digital Investigation, The Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06), 3(Supplement 1), pp. 50-58.

[31] www.caine-live.net/page11/page11.html last retrieved on March 12, 2016

[32] www.freeviewer.org/bkf last retrieved on March 12, 2016

[33] https://www.foxtonforensics.com/browser-history-capturer/ last retrieved on March 12, 2016

[34] Raghavan S. And Raghavan S. V. (2013). AssocGEN: Engine for Analyzing Metadata Based Associations in Digital Evidence, In Proceedings of the 2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE), IEEE 978-1-4799-4061-5, Hong Kong, China, Nov 21-22, 2013.

[35] Minack E., Paiu R., Cost ache S., Demartini G., Gaugaz J., Ioannou E., Chirita P-A, and Nejdl W., (2010), Leveraging personal metadata for Desktop Search: The Beagle ++ System, Journal of Web Semantics: Science, Services, and Agents on the WWW, Elsevier Science Publications, ISSN: 1570-8268, Vol. 8(1), pp. 37-54.

[36] Zander S., Nguyen T. And Armitage G. (2005)., Automated Traffic Classification and Application Identification using Machine Learning, In Proceedings of the IEEE Conference on Local Computer Networks, IEEE LCN 2005, Sydney, Australia, ISBN: 0-7695-2421-4, pp. 250-257.

[37] Raghavan S., Clark A J., and Mohay G. (2009). FIA: An Open Forensic Integration Architecture for Composing Digital Evidence., Forensics in Telecommunications, Information and Multimedia, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2009, Volume 8(1), pp. 83-94, DOI: 10.1007/978-3-642-02312-5_10

[38] Case A, Cristina A, Marziale L, Richard G and Roussev V. (2008). FACE: Automated Digital Evidence Discovery and Correlation, Digital Investigations, Proceedings of the 8 Th Annual Digital Forensic Research Workshop (DFRWS '08), 5(Supplement 1), pp. S65-S75.