IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

A Literature Review on Cyber Forensic and its Analysis tools

Mandeep Kaur[1], Navreet Kaur[2], Suman Khurana[3]

Student, Department of Computer Science and Application, K.M.V., Jalandhar, India [1, 2]

Associate Professor, Department of Computer Science and Application, K.M.V., Jalandhar, India[3]

Abstract: With the advancement in cyber area, frequent use of internet and technologies leads to cyber attacks. Digital forensic is opted for acquiring electronic information and investigation of malicious evidence found in system or on network in such a manner that makes it admissible in court. It is also used to recover lost information in a system. The recovered information is used to prosecute a criminal. Number of crimes committed against an internet and malware attacks over the digital devices have increased. Memory analysis has become a critical capability in digital forensics because it provides insight into the system state that should not be represented by traditional media analysis. In this paper, we study the details of cyber forensics and also provide the vital information regarding distinctive tools operate in digital forensic process. It includes forensic analysis of encrypted drives, disk analysis, analysis toolkit, volatile memory analysis, captures and analyzes packets on network.

Keywords: Cyber Forensic, Volafox, Votality, Dff.

I. INTRODUCTION

Digital forensics is the application of examination and analysis techniques to gather and preserve evidence from an appropriate computing device in a way that is suitable for presentation in a court of law. The goal of digital forensics is to perform a careful investigation while maintaining a documented chain of evidence to find out exactly what to be found on a computing device and who was blamed for it. Digital Forensics tools are now used on a daily basis by examiners and analysts [1]. Forensic analyst typically follow a general set of procedures: After physically isolating the device in question to make sure it cannot be accidentally infected, investigators make a digital copy of the device's storage media. Once the authentic media has been copied, it is sealed in a safe or other secure facility to maintain its original condition. Analyst use a variety of techniques and recovery software forensic applications to examine the copy, searching invisible files and unloaded disk space for copies of deleted, encrypted, or damaged files. Digital Forensics is an important tool for solving crimes attached with computers (e.g. phishing and bank fraud), as well as for solving crimes against people where clue may reside on a computer (e.g. money laundering and child exploitation). Memory forensics is forensic investigation of a computer's memory dump. Its primary application is investigation of advanced computer attacks which are secret enough to avoid leaving data on the computer's hard drive.

Forensics is the process of using experimental knowledge for collecting, analyzing, and presenting evidence to the courts. Forensics deals basically with the recovery and analysis of evidence. Evidence can take many forms, from fingerprints left on a window to DNA evidence found from blood stains to the files on a hard drive. Computer forensics is the method that combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless transmission, and storage devices in a way that is admissible as evidence in a court of law [2].

The three main steps in any computer forensic analysis are acquiring, authenticating, and analysing of the data. Collecting the data mainly involves creating a bit-by-bit copy of the hard drive. Authentication is the ensuring that the copy used to perform the analysis is an exact copy of the contents of the original hard drive by comparing the checksums of the copy and the original. If deleted data could not be recovered through the use of common forensic tools, more sensitive equipment can be used to extract the data, but this is rarely done because of the high cost of the instruments. Computer forensics is essentially a means for gathering electronic evidence during an investigation. In order to use this information to litigate a criminal act, evidence must be collected carefully and legally. Computer and Network Forensics techniques are used to discover evidence in a variety of crimes ranging from theft of trade secrets. The goal of computer and network forensics is to provide satisfactory evidence to allow the criminal perpetrator to be successfully prosecuted.

For example, in a criminal case, evidence may be found such as documents related to homicides, financial fraud, drug or fraud record keeping, or child pornography. In a civil case, evidence of personal and business records related to fraud, divorce or harassment could be found. Computer Network Forensics experts are not only hired by lawyers. Computer Network Forensics techniques are sometimes needed by insurance companies to discover evidence to decrease the amount paid in an assurance claim. Individuals may also hire computer network forensics experts to support a claim of wrongful termination, sexual harassment [3, 4].

II. LITERATURE REVIEW

In [6] Bolagh and Pondelik have proposed a technique to recover the decoding keys from the dump of the live image of a volatile memory. Proposed approach works on windows and Linux with True Crypt is a free open source tool that performs on-the-fly disk encryption. The authors also suggested a method to decrease the size of dump image, especially in case when True Crypt is used for encryption, the size can be bounded to 1-2 MB only. However, the suggested technique bears a limitation that the image should be present nearby for forensic analysis. In addition, decoding keys are located through content search, and if certain data deterioration appear in a disk then it becomes impossible to extract keys. Advances in data encryption mechanics have made the job of cyber investigators really tough.

In [7] Dija et. Al. has suggested a technique to unseal encrypted drives. The suggested solution can merely decrypt only those sealed drives which are encrypted through Bit Locker using its USB only mode component. The suggested solution is primarily based on discovering "BEK" or 48-digit password file during live forensic investigation or image dump to restore Bit Locker drive. For this purpose, brute force attack can also be used to restore the drive whether on a live forensic analysis or physical memory dump file.

In[18] Govind Singh Tanwar and Dr. Ajeet Singh Poonia have described that many more corporate entities today are utilizing ICTs(information and communication technology) to identify opportunities for innovative and customer-centric, value-added products and services. Information systems have been key characteristic of any growing and successful businesses, as they utilize ICTs for business value creation. Computer Usage policy is a document that provides guidelines that classify the acceptable usage of these systems by end- users. Policies are said to be guidelines for corporate computer usage and application, Violations such as password complexity requirements, email usage, account usage, Internet usages etc. are observed violated by the sample computer users.

In [17]Natasa Suteva, Aleksandra Mileva and Mario Loleski have described that attackers are arrested due to the evidences collected by computer forensics. The victim machine usually gives some data, which are then used for identifying possible suspected, which is followed by forensic analysis of their devices, like computers, laptops, tablets, and even smart phones. Post-mortem computer forensic analysis is used by the attacker and victim machine to find some artifacts in them, which can help to identify and possible to reestablish the attack, and most important to obtain valid evidence which holds in court. On the attacker's machine, traces are found in the browser's history files, browser temporary storage and bash history file. On the victim's apparatus, traces are found in the file system and in the log files.

In [14] Luís Filipe da Cruz Nassif and Eduardo Raul Hruschka have described that, In computer forensic analysis, hundreds of thousands of files are usually investigated. Much of those files consist of unstructured text, whose analysis by computer examiners is difficult to be performed. Our experiments show that the Average Link and Complete Link algorithms provide the best results for our operation domain. If suitably initialized, partitioned algorithms can also yield to very good results. In our experiments the hierarchical algorithms known as Average Link and Complete Link presented the best results. Although their usually high computational costs, they are suitable for datasets with a few hundred documents.

In [20] Lijun Zhang, Yu Zhou and Jia Fan, have presented two scenarios of Truecrypt application: one is to enable a personal user to recover his forgotten password, the other is to provide computer forensic analysis of criminal activity. The computer forensic for Truecrypt encrypted volumes includes normal and hidden volumes. Truecrypt encryption and password verifying process is explicitly demonstrated. Digital evidence can also be obtained from the data structure residing in memory by using different tools. Chan et al suggested a tool named as 'Cafegrid' which can be used for deep analysis and recovery of data from memory in Widow and Linux. This appliance also builds a map of object systematically and tracks the use of memory design during program execution. This all is done by this tool after observe the running program and detect the allocation of dynamic memory. This tool can benefit forensic investigator in evidentiary analysis process as the data structure information can be coordinately used for offline or live analysis in digital forensics.

In[13] Andrew Marrington, George Mohay, Hasmukh Morarji and Andrew Clark, have shown the use of models in automatic computer forensic analysis and introduced and detailed on a novel model for use in computer profiling object model. It is an info model which models a computer as objects with various attributes and inter-relationships. It provides a plan for development of automatic computer forensic examination and investigation tools. The model promotes digital evidence representation; determine computer activity and investigative reasoning.

In [8] Maximilian Bielecki and Gerald Quirchmayr have described the strengths of an automated presentation and argumentation support system with a analysis of cyber criminals similar to the ones used in law enforcement work and also the description of a prototype based on an automatic forensic support system called Computer Forensic Analyzer and Advisor. Computer Forensic Analyzer and Advisor demonstrates an approach of a fully automated system that supports investigators by independently identifying malicious software and programs. In [21]Yangbin Zhou and Keyu Jiang, have presented wiping electronic evidence. The system is start with collecting the related work and analyzes the organization's security policies and strategy, finding out the security level of the computer systems, the work situation for staffs the personnel secures awareness level, and etc. With the security level of this organization, ethical programmer can test the reaction of the organization to a hacking attack. According to the system, Developer and organization's managers should clearly know their organization's insufficiency in computer forensics filed.

In[15] Jun-Hyung Park, Minsoo Kim, Bong-Nam Noh and James B D Joshi have described that with the complexity of computer systems and the composure of hacking tools and techniques, there is a crucial need for computer forensic analysis techniques. The goal of such forensic investigation is to analyze malicious executable files that hackers might have installed in a intended system. Finding such malware in a compromised system is difficult because it is hard to identify the purpose of the fragments of executable files. Using the techniques, we are able to detect any modified malicious programs without executing the program.

In [16] Frank Y.W. Law et. al. has described the protection of data privacy, personal data to enable that are not related to the analysis subject should be eliminate during computer forensic examination. In the modern world, the massive use of computers develops a huge amount of private data and there is correspondingly an increased expectation to recognize and respect human rights in digital investigation. In [23] Traditional tool design check each source of digital evidence as a binary large object and it is up to the examiner to analyze the relevant items from evidence. There are a wide range of forensic and analysis tools to investigate digital evidence in existence today. In[22]Yang and Yen have emphasize that live and dead forensic analysis can be carried out by saving the necessary scripts and different tools like Autopsy, FDumper, Scalpel, Fundl etc on a USB or DVD. Such an approach can help in performing live analysis of a running compromised system by plugging in the DVD/USB into the system. The script/tools stored on the DVD/USB when launched will collect the volatile information such as opened ports, user login history and active services etc. from the memory of victim system and store it on the USB. Similarly, the static analysis can be done by using Automated Image and Restore software. The information thus collected can be investigated by using Scalpel and Fundl software stored on a DVD/USB. Fore forensic perspective, log on/log off, date and time, kernel level information and recently executed commands including processes and network status are of much importance for a forensic analyst in making appropriate decision about the significance of the forensic evidence.

In [10] CHEN Wei and LIU Chun-mei have emphasize that the mining and analyzing the useful data of the Linux operating system has become important means and research directions of computer forensic analysis. It provides plenty of useful interfaces for the computer forensic investigation, which will be an important information-gaining tool for the computer forensics on Linux operating system.

In [11] William J. Hatt, Edward A. VanBaak and Holly B. Jimison have represented a forensics style analysis of the computer usage data that is being collected as part of a larger study of cognitive decline, and focuses on the isolation and removal of non user generated activities that are recorded by our computer monitoring software (CMS). With the eventual goal of using the computer data in conjunction with non computer measures of activity and performance, we needed to remove obvious artifacts that are left from automatic system processes. HDFS used to forensically analyze large amount of data by performing indexed searching on client-server architecture. In HDFS, the servers contain a master and a slave system, while client contains the web applications. Firstly, the forensic data is stored on a NAS (Network Access Storage), and then it is analyzed by ETL. In this process, data is extracted from NAS is transformed for the operational activities and then it is loaded into Hbase table in which multiple columns belong to a particular column family. In this approach, the encrypted data is decrypted into plain text, and data filtration and searching through index patterns are applied to reduce the amount of data for analysis. The composition of Hbase database not only improves the data sharing rate, but also enhances ease for the analysts to perform digital forensic investigations.

In [12] Kyung-Soo Lim, Seung Bong Lee and Sangjin Lee have emphasize that we need new process model to collect crucial evidence . The Stepwise Forensic Process Model provides stepwise and in-situ approach for providing incident description, recovery, analysis. It suggests a new investigational model for selecting the object and considers the relevant evidences only. It based on the crime scene circumstance and is aimed at efficiently choosing and inspecting the system, enabling one to overcome the limitations of traditional forensic model.

In [9] Louis J. Bottino has described the security policies that are important in preventing compromises of network security and risk affecting secure computer transmission. Vulnerabilities in computer networks are identified in terms of exploits. The formation of scanning technologies can discover these exploits and their affects on the integrity of the information exchanged.

In [19]Yongge Wang and Yuliang Zheng has described the computer forensic analysis, intrusion detection and disaster recovery are all dependent on the existence of trustworthy log files. Current storage systems for such log files are generally prone to modification attacks, especially by an intruder who wishes to wipe out the trail he leaves during a successful break-in. To resolve deficiencies in the current digital live forensic methods. Wang et al. Proposed a physical memory analysis model for live forensic. For forensic analysis, it is suggested to clearly separate different phases of forensic analysis such as evidence collection, examination, analysis and report generation. The proposed model underlines some aspects to maintain the credibility of forensic analysis. Firstly, authenticity tops the list as it pertains to identifying a key question about the data validity i.e., how much evidentiary data is affected by the evidence collection tools. Then integrity is considered to check whether the data gathered is complete or not. The next step is to verify that data is consistent and meet the requirement of forensic analyst besides verifying that analysis procedure is consistent. Then repeatability and applicability is assured. Finally, it is imperative to analyse that the method used for the forensic analysis is fault- tolerant i.e., method should not be interrupted if some evidentiary data is missing or tampered. A meticulous deliberation of the aforesaid aspects will assist and improve the credibility of forensic analyst.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

III. FORENSIC ANALYSIS TOOLS

There are various forensic analysis tools present that are opted for different purposed. These are discussing as follow:

A. Autopsy

Autopsy is a digital forensics platform. It based on GUI program that allows you to investigate hard disk drives and smart phones. It has a plug-in architecture that allows you to find add-on programs or develop custom programs in Java or Python. This tool helps thousands of users around the world and has community-based e-mail lists and forums. Law enforcement, military and corporate examiners use autopsy to examine what appear on a computer. You can even use it to restore photos from your camera's memory card. Autopsy refers to the process of automatically investigating the disk contents as ingest. The most common types of information abstract by ingest used in digital forensic investigation, which avoids the need to perform the tasks manually.

The Autopsy Browser helps you to conduct a digital forensic examination. Autopsy is a graphical interface, Autopsy runs as a web server, and can be accessed using an HTML browser. Autopsy presents a 'File Manager' and it shows the components of the destroyed data and architecture of the file system. Autopsy offers two analysis modes; firstly a dead investigation appears when a dedicated analysis system is used to scan data from a suspected system. In this mode Autopsy run in a reliable environment. Secondly, alive analysis mode occurs when the suspect system is being analyzed although it is running. In this mode, Autopsy run from a CD in an un-trusted environment. This mode is used as event response scenarios while the event is being accepted. When an incident is accepted, the suspect system can be captured and a dead investigation is performed. Autopsy can create ASCII details for files and other file system structures. This allows the examiner to quickly make consistent data sheets during the investigation [24].

1. Features of Autopsy

a. Timeline Analysis: Displays system events in a graphical interface to help identify activity.
b. Keyword Search: Text extraction and index searched modules enable you to find files that mention specific terms and find regular expression patterns.
c. Web Artifacts: Extracts web activity from common browsers to help identify user activity.
d. Registry Analysis: Uses RegRipper to identify recently accessed documents and USB devices.
e. LNK File Analysis: Identifies short cuts and accessed documents
f. Email Analysis: Parses MBOX format messages, such as Thunderbird.
g. EXIF: Extracts geo location and camera information from JPEG files.
h. File Type Sorting: Group files by their type to find all images or documents.
i. Media Playback: View videos and images in the application and not require an external viewer.
j. Thumbnail viewer: Displays thumbnail of images to help quick view pictures.
k. Robust File System Analysis: Support for common file systems, including NTFS, FAT12/FAT16/FAT32, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS from The Sleuth Kit.
l. Hash Set Filtering: Filter out known good files using NSRL and flag known bad files using custom hash sets in Hash Keeper, md5sum, and En Case formats.
m. Tags: Tag files with arbitrary tag names, such as 'bookmark' or 'suspicious', and add comments.
n. Unicode Strings Extraction: Extracts strings from unallocated space and unknown file types in many languages.
o. File Type Detection based on signatures and extension mismatch detection.
p. Interesting Files Module will flag files and folders based on name and path.
q. Android Support: Extracts data from SMS, call logs, contacts, Tango, Words with Friends, and more.

2. Advantages:

a. Easy to Use: Autopsy was designed to be perceptive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree.
b. Extensible: Autopsy is constructed as end-to-end platform with modules that come with it out of the box and others that are accessible from third-parties. Some of the modules provide:
1. Timeline- Advanced graphical event viewing interface.
2. Hash Filtering- Flag known bad files and ignore known good.
3. Keyword Search - Indexed keyword search to find files that mention relevant terms.
4. Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
5. Data Carving - Recover deleted files from unallocated space using PhotoRec.
6. Multimedia - Extract EXIF from pictures and watch videos.
7. Indicators of Compromise - Scan a computer using STIX.

c. Fast: Autopsy runs background functions in parallel using multiple cores and provides results to you as soon as they are found. It may take hours to fully investigate the drive, but you will know in minutes if your keywords were found in the user's home folder.

d. Cost Effective: Autopsy is free. When cost is decreasing, cost effective digital forensics solutions are essential. Autopsy offers the same core details as other digital forensics tools and offers other essential details, such as web artifact investigation and registry investigation that other commercial tools do not provide.

B. Operating system forensics

O.S. Forensics is a toolkit that provides lots of information about the use of a computer and the files stored in it. In OS Forensics you can easily manage your tasks and programs. OS Forensics you can check what your kids are doing on the system, used by a law agents in the investigation. The

program is installed directly on a memory device. Investigate the computer for certain files, recover deleted files, record recent activity or create a report with technical data about the computer. It's also very easy to use, which is good as the details don't include any documentation. If you ever need to analyze a computer in depth, OS Forensics may be the tool you're looking for. OS forensics is a complete selection of tools and its interface is neatly organized. It can also be installed on a USB device.

1. Features of O.S.

a. Discover Forensic Evidence Faster
In OS forensic, we find files faster, search by filename, size and time. File contents can be searched using the Zoom search engine through email archives from Outlook, Thunder Bird, Mozilla and more. Deleted files can be searched and recovered. Information of the system is collected. Recovery of password from web browsers and discover and reveal hidden areas in your hard disk.

b. Identify Suspicious Files and Activity
It verifies and matches files with MD5, SHA-1 and SHA-256 hashes. Drive signatures can be created and compared to identify differences. File viewer that can display streams, hex, text, images and meta data. Email viewer that can display messages directly from the archive. Browse Web browser and capture online content for offline evidence management. Prefer viewer to identify the time and frequency of applications that been running on the system, and thus recorded by the O/S's Prefer.

c. Manage Your Digital Investigation
Case management enables you to aggregate and organize results. HTML case reports provide a summary of all results and items that you have associated with a case. Drive imaging used for creating/restoring an exact copy of a storage device and rebuild RAID arrays from individual disk images. OS Forensics can be installed on a USB flash drive for more portability and maintained a secure log of the exact activities carried out during the course of the investigation.

C. RAM Forensics
Memory forensics is forensic analysis of a computer's memory dump. It investigates the advanced computer attacks which avoid leaving data on the computer's hard drive. RAM analysis is concerned with the retrieval of information, as evidence in criminal analysis. More specifically, memory management structures in computer map the abstracted files and executables resident in a computer's physical memory. These files/executables can be used to prove that a crime takes place or to trace how it came to pass. The usefulness of this type of investigation lies in the fact that any material found in RAM is recently running on the victim system. The primary method of analyzing a RAM copy was to perform a strings analysis. A variety of hardware and software solutions exist to copy the contents of physical memory to file for offline analysis. Output of such a tool is commonly referred to as an image or memory dump. The memory forensics mechanism consists of two parts. First, a copy of the target's memory called an image is written to exterior media. This requires a toolkit consisting of software to perform the capture and a USB device or network connection to preserve the image. Second, the image is analyzed on a forensic workstation using tools to extract human interpretable information [25].

D. DFF (DIGITAL FORENSICS FRAMEWORK)
Digital Forensics Framework is a Open Source computer forensics software. It is used both by professional and non-expert people in order to quickly and easily gather, conserve and admit digital evidences without compromising systems and data. It is used by both specialist and non-experts to gather, conserve, and admit digital evidence without compromising systems and data. Its command line interface enables to perform digital analysis remotely and comes with usual functionalities available in common framework such as completion, tasks management, and globing or keyboard shortcuts. Digital Forensic Framework can also run batch scripts at startup to automate repeated tasks. Advanced users and developers can also use Digital Forensic Framework directly from a Python interpreter to script their investigation.
Digital Forensic Framework is an easy to use, an open source tool which will help you in your digital forensics works, including files restoration due to error or crash, evidence research and analysis etc. The source code is written in C++ and Python, grant performances and great extensibility. Digital Forensic Framework can be installed on Linux and Windows.

E. WIRESHARK
Wire shark is free open-source packet analyzer. It is used for network damage, investigation, software and connection protocol advancement, and education .In this software we can observe all packets in network and recognize high level of traffic in our network. Wire shark is available for all OS and GUI environment which provide user friendly interface. Wire shark is the world's most suitable network analyzer. This is very powerful tool that provides network and upper layer protocols information about the data captured in a network.
Network packet analyzer is a checking device used to examine what's going on inside a network cable. Wire shark is one the best sniffers available and is being developed as a free, commercial-quality sniffer. It has great feature, a nice graphical user interface that is actively developed and managed. It runs on UNIX-based systems, Mac OS X, and windows. This is a great sniffer Wire shark includes filters, color coding and other aspects that let you dig deep into network traffic and inspect individual packets. Wire shark can be uses to checkout a large program's network traffic and scans the traffic flow on your network or trace network problems.

F. TRUECRYPT
True Crypt is an open source-available freeware utility used for encryption. It can create a virtual encrypted disk within a file or encode a partition or the entire storage device. True Crypt is a cross-platform open source record of files and full disk encryption. True Crypt can also design an encrypted hard disk partition and also on smaller

encrypted file that is easily seen by any disk service. True Crypt offers advanced encryption without hassles. True Crypt offers 'on-the-fly' encryption, which means we don't have to wait for large files to decrypt after entering the correct pass phrasing files are immediately available. True Crypt defends highly sensitive personal and business confidential information. True Crypt uses partition encryption as well as encrypted storage of files to protect sensible data from illegal access. The several combinations of encryption algorithms and hash operations are used for the key derivation. True Crypt is tool used to encode data or information. When we copy from a True Crypt drive, this procedure is duplicated from one storage disk to other storage disk. By that time information decrypts and stores in temporary storage in memory. True Crypt never saves any decrypted data to a disk; it is stores temporarily in RAM. Even when the volume is mounted, data collection in the volume is still encrypted. When you resume Windows or switch off your computer, the volume will be removed and files stored in it will be unavailable.

IV. CONCLUSION

In this paper, we examined distinctive forensic tools used for analysing security flaws in digital forensics and also the detailed review of cyber forensics. Digital evidence can also be obtained from the data structure locate in memory by using different tools. The new process model is opted to collect crucial evidence quickly and investigate the cases immediately. The Stepwise Forensic Process Model presents the stepwise and in-situ approach provides incident identification, recovery, analysis [12]. The SFPM suggest a new investigational model for selecting the target and analysing the relevant evidences only. It is based on the crime scene circumstance and is intended to quickly selecting and investigating the system, to overcome the limitations of traditional forensic model.

Network packet analyzer is opted for network troubleshooting analysis, advancement of communication protocol, and also in education. It observes network traffic and identified high level of traffic in our network. In forensic analysis, the sophisticated forensic tools are not only required to collect and analyze data, but are also needed to resolve any ambiguity or conflicts introduced due to their execution.

Due to rapid increase in the number of Internet users across the world, the frequency of digital attacks has increased [15]. Therefore, the need to devise effective methodologies and develop efficient tools to detect these attacks timely. In this paper, we have examined different tools for performing digital forensic analysis. This research provides a provisional study of the tools regarding cyber forensic analysis.

REFERENCES

[1] Simon L. Garfinkel, "Digital Forensics Research: The next 10 years", Naval Postgraduate School, Monterey, USA, 2010.
[2] "Computer Forensics", US-CERT, 2008.
[3] Alec Yasinsac and Yanet Manzano, "Policies to Enhance Computer and Network Forensics", Workshop on Information Assurance and Security, United States Military Academy, page no.289, 2001.
[4] Ahmer Umer, Kamran Ahsan and Khuram Mushtaque, "Issues In Digital Forensics Can Overcome Through Latest Technologies With Real-Time Factors", Mohammad Ali Jinnah University and Federal Urdu University of Arts, Science and Technology, Karachi, Pakistan.
[5] Muhammad Shamraiz Bashir and M. N. A. Khan, "Triage in Live Digital Forensic Analysis", The International Journal of Forensics Computer Science, 4 june 2013.
[6] Stefan Bolagh, Matej Pondelik. "Capturing Encryption Keys for Digital Analysis", In Proceedings 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems(IDAACS), pp. 759--763, Prague, 15-17 September 2011.
[7] Dija S, Balan C, Anoop V and Ramani B. "Towards Successful Forensic Recovery of BitLocked Volumes". In Proceedings 6th International Conference on System of Systems Engineering (SoSE), pp. 317--322, Albuquerque, NM, 27-30 June 2011.
[8] Maximilian Bielecki and Gerald Quirchmayr,"A prototype for support of computer forensic analysis combined with the expected knowledge level of an attacker to more efficiently achieve investigation results", International Conference on Availability, Reliability and Security, pp. no:696-701,2010.
[9] Louis J. Bottino, "Security Measures In aSecure Computer Communication Architecture", 25th Digital Avionics Systems Conference, 15 October, 2006.
[10] CHEN Wei and LIU Chun-mei, "The Analysis and Design of Linux File System Based on Computer Forensic", International Conference on Computer Design and Applications, vol. 2, 2010.
[11] William J. Hatt, Edward A. VanBaak and Holly B. Jimison, "The Exploration & Forensic Analysis of Computer Usage Data in the Elderly", 31st Annual International Conference of the IEEE EMBS Minneapolis, Minnesota, USA,2-9 September 2009.
[12] Kyung-Soo Lim, Seung Bong Lee and Sangjin Lee, "Applying a Stepwise Forensic Approach to Incident Response and Computer Usage Analysis", 2009.
[13] Andrew Marrington, George Mohay, Hasmukh Morarji and Andrew Clark, "A Model for Computer Profiling,"International Conference on Availability, Reliability and Security, page no: 635-640,2010.
[14] Luís Filipe da Cruz Nassif and Eduardo Raul Hruschka, "Document Clustering for Forensic Computing: An Approach for Improving Computer Inspection", 10th International Conference on Machine Learning and Applications,pp. no:265-268,2011.
[15] Jun-Hyung Park, Minsoo Kim, Bong-Nam Noh and James B D Joshi, "A Similarity based Technique for Detecting Malicious Executable files for Computer Forensics",pp. 188-193,2006.
[16] Frank Y.W. Law, Patrick P.F. Chan, S.M. Yiu, K.P. Chow, Michael Y.K. Kwan, Hayson K.S. Tse and Pierre K.Y. Lai, "Protecting Digital Data Privacy in Computer Forensic Examination", SADFE, 2011, Systematic Approaches to Digital Forensic Engineering, IEEE International Workshop on, Systematic Approaches to Digital Forensic Engineering, IEEE International Workshop on 2011, pp. 1-6.
[17] Natasa Suteva, Aleksandra Mileva and Mario Loleski, "Computer Forensic Analisys of Some Web Attacks", World Congress on Internet Security, pp. no:42-47,2014.
[18] Govind Singh Tanwar and Dr. Ajeet Singh Poonia, "Live Forensics Analysis: Violations of Business Security Policy", International Conference on Contemporary Computing and Informatics pp. no: 971-976, 2014.
[19] Yongge Wang and Yuliang Zheng, "Fast and Secure Magnetic WORM Storage Systems", Proceedings of the Second IEEE International Security in Storage Workshop, 2003.
[20] Lijun Zhang, Yu Zhou, Jia Fan, "The Forensic Analysis of Encrypted Truecrypt Volumes", pp. 405-409, 2014.
[21] Yangbin Zhou and Keyu Jiang, "An Analysis System for Computer Forensic Education, Training, and Awareness", International Conference on Computing, Measurement, Control and Sensor Network, page no: 48-51, 2012.
[22] Chung-Huang Yang, Pei-Hua Yen, "Fast Deployment of Computer Forensics with USBs". In Proceedings of International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), pp. 413--416, Fukuoka, 4-6 November 2010.
[23] Sriram Raghavan andS V Raghavan," A Study of Forensic & Analysis Tools", IEEE, 978-1-4799-4061-5/13,2013.
[24] Anthony Dowling, "A the Sleuth Kit v2.01 and Autopsy Forensic Browser Demonstration", June 02 2006.
[25] Andrew F. Hay and Gilbert L. Peterson," Acquiring OS x File Handles through Forensics Memory Analysis", Air Force Institute of Technology, 2011.