Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 03 | Issue 02 | October-2020

Role of Computer Analysis Tools in Forensic Science

Preeti Kiran[1]

Available online at: www.xournals.com

Received 03rd October 2020 | Revised 10th October 2020 | Accepted 16th October 2020

Abstract:

As the world is entering into the digital era and the entire information about a person could be found online, so the reporting of computer crimes are increasing daily. To solve computer crimes, it is necessary to study digital forensics, which includes the methodology of retrieving and examination of content stored on digital devices, including desktops, laptops, smartphones, etc. Due to the vulnerabilities that have caused an increase in computer crime, there are numerous tools present for the analysis of these vulnerabilities. Examiners need a solution that puts all of the knowledge together and automates some of the repetitive acquisition and processing processes, freeing up time for deeper study. In this paper, various forensic tools are described which could be used for identification, collection, examination, and analysis, and reporting of digital evidence. Analysis of digital evidence includes disk imaging, memory capture, web browser history analysis, and various logs, etc., found in the system or network.

Keywords: *Digital Forensics, Computer Forensics, Cybercrime, Computer Crime, Computer Tools.*

Authors:

1. *Kurukshetra University, Kurukshetra, Haryana, INDIA*

Introduction

Digital forensic was known little regarding the methodology of retrieving and examination of content stored on digital devices, including desktops, laptops, and smartphones, etc. In recent years, however, as cybercrime is on an increasingly wide scale and digital technologies are being rapidly embraced, the digital forensic field has gained tremendous prominence, contributing to what was historically limited to the recovery and analysis of biological and chemical evidence during criminal investigations (**Pande, Jitendra, and Prasad, 2016**).

Computer forensic (branch of digital forensics) collects, preserves, analyses, and presents evidence related to computers. Digital evidence is often useful in criminal cases, civil disputes, and human resources or industrial proceedings (**Vacca and John, 2005**).

Computer crimes are criminal abuses of computer technology expertise for their actions, investigation, or prosecution. Computer-related crimes are white-collar crimes i.e., any criminal act based on computer technology may be a crime against the technology.

Computer crime cannot only include computers actively but passively as the evidence of action is stored in the data form. Computer crime victims and possible victims include anyone who uses or is influenced by computing systems and data processing systems, including those who store and process data on their computers (**Parker, 1989**).

It is difficult to assess the first or early stage of the "Computer Forensic" analysis. Yet most experts believe that more than 30 years ago, computer forensics started to evolve. The sector started primarily in the United States where police and military authorities started to see criminals getting technical. In response to possible safety breaches, government agencies responsible for securing valuable, privy, and inevitably confidential information performed forensic investigations not to investigate a particular breach, but also learn how to prevent any future violations. Ultimately, the fields of cyber management, focusing on cyber and assets safety and computer forensics focusing on responding to high-tech violations, started to intertwine.

The field is evolving over the following decades and until today. It has been introduced by both the government and private organizations and businesses-using internal information management and forensic computer practitioners and contracting these practitioners or companies as necessary. Significantly, the private legal sector has recently undergone an increase in the area of discovery and the need for computer forensic exams and civil legal disputes (**Pande, Jitendra, and Prasad, 2016**).

Objectives and Benefits of Computer Forensics

Cyber threats have been a big part of the general public's everyday lives. According to the data, 85% violation of safety has been identified among businesses and government agencies. Digital evidence analysis offered a medium on which forensic investigators could focus after an accident occurred. A computer forensic investigator's ultimate purpose is to determine the essence and circumstances of a crime and to classify the suspect in a formal investigation procedure (**Wiles, Jack, and Reyes, 2007**).

Computer Forensics aims to provide guidelines for:

- During the initial response process and after the incident access to the victim's computer.
- Plan protocols for a suspected crime scene so as not to distort digital evidence.
- Recovery and duplication of data.
- Recovery of deleted files and partitions removed from digital media to extract and validate the evidence.
- Guidelines are provided to analyze digital media for data security, analysis of logs and findings, network traffic, and log investigations for correlating incidents, wireless and web-based investigations, email monitoring, and email investigations.
- Computer forensic report that gives thorough information on the method of computer forensic investigation.
- Preservation of facts through the chain of custody.
- The use of stringent protocols to allow forensic findings to be investigated in a court of law.
- Digital forensic leads to an expert witness being presented to the court (**Pande, Jitendra, and Prasad, 2016**).

Review of Literature

Lim *et al.* (2009), emphasized that to gather critical data, we need a new process model. The Stepwise

Forensic Process Model offers a step-by-step and in-situ approach to the description, recovery, and review of incidents. It proposes a new investigative paradigm for object collection and only takes into account the relevant facts. It is based on the circumstances of the crime scene and seeks to accurately pick and examine the device, allowing the shortcomings of the conventional forensic model to be overcome.

Marrington *et al.* (2010), demonstrated the use of models in automated computer forensic analysis, and a novel model for use in the computer profiling object model was implemented and detailed. It is an information model that models a machine as objects with different attributes and interrelationships. It includes a plan for the production of forensic analysis and investigation software for automatic computers. The model encourages the representation of digital evidence; it determines computer activity and investigative reasoning.

Guo *et al.* (2010), introduced some concepts and principles relevant to computer forensics and digital evidence; but, without actually addressing the collection of evidence on the client's side, the authors researched digital evidence in a general way.

Garfinkel (2010), offered a literature review in which the author discusses the issues of existing forensics procedures and concerns soon, but there is no coverage of digital evidence from web environments.

Law *et al.* (2011), defined data privacy security, personal data that are not relevant to the topic of the analysis should be removed during computer forensic inspection to allow it. In the modern world, a large amount of private data is generated through the massive use of computers and there is a correspondingly increased expectation of understanding and upholding human rights in digital analysis.

Balogh and Pondelik (2011), retrieved a technique for decoding keys from the dump of the live image of a volatile memory has been suggested by The proposed approach works with True Crypt on windows and Linux, a free open-source tool that performs disc encryption on-the-fly. The authors also suggested a method for reducing the size of the dump image, particularly if the size can be limited to 1-2 MB only when True Crypt is used for encryption. The proposed method, however, carries a drawback that the picture for the forensic examination should be present nearby. Moreover, decoding keys are found by content search, and it becomes difficult to retrieve keys if such data degradation occurs on a disc. Advances in data encryption mechanics have made it very hard for cyber investigators to operate.

Nassif, Cruz, and Hruschka (2011), identified that hundreds of thousands of files are typically explored in computer forensic research. Most of those files consist of unstructured text, the study of which is difficult to carry out by computer examiners.

Raghavan and Raghavan (2013), verified each source of digital evidence as a binary large object is by conventional tool design, and it is up to the examiner to evaluate the relevant evidence objects. Today, a wide variety of forensic and research techniques are in use to examine digital evidence.

Simou *et al.* (2014), addressed a cloud forensics review; the authors concentrated on accessible technological solutions provided in primary studies that relate to cloud computing, specifically the SaaS service model; and offer general guidance on objects in that service model to be taken into account.

Suteva *et al.* (2014), identified the arrest of attackers due to evidence gathered from computer forensics. The victim machine typically contains some information that is then used to identify potential offenders, followed by forensic examination of their items, such as computers, laptops, tablets, and even mobile phones. The intruder and victim machine use post-mortem computer forensic analysis to locate such objects in them, which can help to identify and recover the attack, and most importantly, to gain credible proof kept in court. Traces are found on the attacker's computer in the historical archives of the server, temporary storage of the server, and bash history files. Traces in the file system and the log files are found on the victim's apparatus.

Kaur *et al.* (2016), presented a literature review on cyber forensics. Here, the authors present general specifics and summarise information on a range of digital evidence management tools.

Hatole and Bawiskar (2017), suggested an email forensics literature review that focuses on resources used to handle email data. However, the areas for general cases and objects from other web services are not included.

Coronel *et al.* (2018), proposed a literature review of cyber forensics in a systematic order from the perspective of a client. It dealt with the techniques of identification, collection, analysis, preservation, and report of digital evidence from a client's side.

Kumar (2020), presented a research article emphasizing on the trends and patterns to examine digital forensics and cybersecurity in India. He provided information on the types of cyber-crimes and tools used for analysis.

Forensic Analysis Tools

With the increasing use of digital media, the rate of commission of computer crime has increased, which leads to the study of the analysis of these types of crimes. Digital forensics includes various steps for the investigation that includes- identification, collection, examination, analysis, preservation, and reporting. There are numerous types of tools available to analyze a computer crime which is discussed below in detail:

A. Autopsy

An autopsy is an easy to use and Graphical User Interface based program used mainly for the digital forensic platform. It allows the analysis of the file system and metadata of hard drives and smartphones. It is used by cybersecurity experts, law enforcement, military, and corporate examiners to investigate the work done on the system **(Shaaban, Ayman, and Sopronov, 116).**

Features

It exhibits the following features:

- **Multi-User Cases:** It is designed for easy usage by one investigator or coordinates the work of a team.
- **Timeline Analysis:** It displays the activities performed on the system in a graphical interface.
- **Keyword Search:** It enables the indexed keyword search to find files that mention relevant terms.
- **Web Artefacts:** It extracts the browser history, cookies, bookmarks from Firefox, Chrome, and Internet Explorer.
- **Registry Analysis:** It identifies the recently accessed documents and USB devices by the use of RegRipper.
- **EXIF:** It extracts the geographical location and camera information from JPEG files.
- **Media Playback:** It can be used to view videos and images in the application itself without the use of an external viewer.
- **Thumbnail Viewer:** It displays the thumbnails of the images for a quick view.
- **File System Analysis:** It supports file systems such as NTFS, FAT, HFS+, and UFS, etc.
- **Hash Set Filtering:** Flag known bad files and ignore known good files.
- **Unicode Strings Extraction:** It extracts strings from unallocated space and unknown file types.
- **Android Support:** Extracts data from SMS, call logs, contacts, Tango, etc.
- **Data Carving:** Recovery of deleted from files from unallocated space using PhotoRec.
- **Fast:** It is fast software with the following features that allow the analysis of the evidence in a short period:
  - ○ Multiple plug-in modules run in parallel for multi-core systems.
  - ○ Investigation can be shortened by specifying the files to be analyzed.
  - ○ Results are presented as they are found and provide the details about the modules running at the time.
- **Input Formats:** It analyses the image of the drives and accepts the raw/dd or E01format for the analysis.

Reporting

It generates the report in an easy to read and understandable format such as HTML, Excel, Pdf, XML, etc.

The report generated by the software contains the information that the investigator intends to be included:

- **HTML and Excel:** They are shareable reports that contain the references, notes, and other essential information such as bookmarks, web history, documents, keywords, hash values, installed programs, devices attached, cookies, downloads and search queries.

- **Body File:** Contain the details of the timeline analysis exported in the XML format (**www.sleuthkit.org**).

B. Forensic Toolkit (FTK)

For quite some time AccessData has given the FTK Imager as a free download and updated the device over time. FTK Imager is a highly useful tool for all respondents or observers to obtain images not only from the systems but also check acquired images file systems, raw/dd or "expert witness" formats, VMWare vmdk file formats, etc. FTK Imager recognizes many files system format, not only FAT and NTFS, but ext2, ext3, and more (**Altheide and Carvey, 242**).

Features

FTK Imager has the following features:

- Creating a forensic image of local hard drives, CDs, DVDs, thumb drives, or other USB devices, whole directories, or single files from various media locations.
- Preview local hard disks, network drives, CDs and DVDs, USB devices with the files and directories.
- View forensic image content stored on a local computer or a network drive.
- Install a read-only image that takes Windows Internet Explorer into account to display the image content exactly as the user saw it on the initial drive.
- Forensic images export files and directories.
- See and retrieve files that have been removed but have not been overwritten on the disk from the recycle bin.
- Establish a file hash to track data integrity using either FTK Imager's two Hash functions: Message Digest 5(MD5) and Secure Hash Algorithm (SHA-1).
- Generate standard file/ disk image hash reports, which the investigator can later use as a checklist to prove the case evidence integrity. If an entire drive is imaged, FTK Imager will use a hash image and drive match after the image has been produced, which is unchanged since the acquisition **(www.marketing.accessdata.com)**.

Operating System Forensics (OS Forensics)

OS Forensics is a Windows-based tool used since 2010. It was developed by the company Passmark Software in Australia. It is easy to use and GUI based program. OS Forensics tool does the most work done by other software such as EnCase and FTK but it lacks some of the specialized features of those programs.

Main Features of the Tool

It is a useful tool for forensic analysis of digital evidence as most of the analysis could be done at one platform itself. The most essential features of the tool are as follows:

- **Find Files Quickly:** It searches through the entire disk to find the files of any format in any folder or subfolder. It is faster than any built-in Windows search and is not limited to any other search option. It searches for the entire contents of the files and returns to the indexing of the results simultaneously. The results are easy to read as they are present in the format of File Details, File List, Timeline, or Thumbnail View to get easy access of all the files present on the disk. File Details and File List provide the location, type, accessed date, created date, modified date, size, and attributes of the files searched through the disk. From the Thumbnail View of the result, the contents of the file could be easily accessed. The Timeline View provides the graphical representation of the dates of the files.
- **Search Within Files:** OS Forensics provide the most useful way to search files as it offers to search for the files of different file format by creating the indexes of the drives and then searching through it to get the list of all the files present in the index with the following keyword that is being searched. It offers the result according to the ranked search and the sorted date format which makes it easy to get access to the file. Except for this, it provides the exact phrase matching criteria for the search.
- **Search Emails:** After creating the index of the emails files from the archive could help in searching the desirable emails from the disk through the keyword search. It supports the emails of the format- .pst, .ost, .mbox, .mbx, .eml, .msg, .dbx and .msf. The emails of the supported formats could be also searched by To, From, Cc keywords. It searches for the emails and presents the result instantly. The contents of the searched Emails can be viewed by Email Viewer which

provides the complete insight of the message present in the Email.

- **Recover Deleted Files:** The files deleted from the drive are just removed but remains in the unallocated space of the drive till any new file uses that space. OS Forensic helps to recover those files and provide the details of the deleted files which could be recovered and make it useable on the drive. The results of deleted files could be shown in the Timeline View which provides the details of the date when the file was deleted.
- **Web Browser Activity:** It provides information about the browsing history, cookies, downloading history, and username & passwords for the different internet browsers such as Chrome, Firefox, Internet Explorer, Safari, and Opera. There are some features which are not supported by the browser or are just supported for the current user to extract the details by the tool. For Example, Internet Explorer and Edge does not provide the details of the downloading history to the tool whereas Chrome just provides the details of the username & password of the current user only.
- **Registry Activity:** OS Forensic also provides insight into the activities done on the system. It gives the details of the Most Recently Used (MRU) applications on the system as well as the details of the USBs connected to the system. It provides system information. It can be used instead of Windows Registry Viewer.
- **Collect System Information:** It provides the complete details of the system. It offers the following details of the system:
    - CPU, Motherboard, and Memory
    - BIOS
    - USB controllers or devices
    - Ports
    - Bitlocker detection
    - Recover Bitlocker keys
    - Python Scripts
    - Network adapters
- **Event Log Viewer:** OS Forensic scans the Windows logs and provides the details of the system activity present in the System, Security, and Application Logs. System Logs provides details such as login attempts, session time, and logout time, and password changes. Security logs provide installation and boot/shutdown details whereas Application Logs tells about the installation of application and time of using them.
- **Memory Viewer:** It provides the Live and Static Analysis of the Physical Memory of the system. During Live Analysis, it gives the details of the memory being used by different columns of the drive. It creates the dump of Physical Memory and provides the essential details of the column which is using the RAM in real-time analysis. In Static Analysis, it gives the details of the memory of the system for the analysis from the Physical Dump created in Live Analysis.
- **Hashing of Files:** OS Forensic helps in the creation of the Hash value of the files. It could help determine the case where the hash value of the file has to be matched with the other file to get the genuineness of the files.
- **Disk Imaging & Mounting:** OS Forensic could also be used to create the image of the disk as FTK and EnCase. Further, mounting the image to analyze the contents of the drive.
- **Generate Report:** The report generated through OS Forensic of the case involves the details of the entire analysis performed on the created case which is easy to access and read **(www.osforensics.com)**.

C. ProDiscover Forensics

ProDiscover Forensic is a powerful computer security tool that enables investigators to search for all data on the computer disks and protect evidence and produce quality evidence for judicial use.

ProDiscover is a forensic disk program offering a wide variety of recording and testing disk functions. A wide range of file systems is supported by Windows, Linux, and Mac. ProDiscover ensures that both the processes of processing and examination are carried out using forensically sound methods. The results satisfy the quality requirements of the evidence.

ProDiscover features a full-text search engine, set of the built-in viewer, and hash comparison methods, all of which provide forensic investigators with a user-friendly yet powerful toolkit. ProDiscover is designed to meet the NIST Imaging Tool Specification criteria.

Features

ProDiscover Forensics has the following features:

- Image and preview disks.

- To quickly and without changing data or metadata, display and scan suspect files.
- Creates and records the data integrity automatically with MD5, SHA1, and SHA256 evidence file hash.
- Create a bit-stream copy of the entire suspected disk to protect the original evidence, including the hidden HPA section.
- Maintains compatibility with multi-tool images in the overall UNIX.dd format by reading and writing.
- Thumbnail screen and registry app integrated graphics.
- The Registry Viewer Integrated.
- Extract EXIF data to identify file owners from JPEG formats.
- Auto-generating reports in XL format saves time, improves quality and precision.
- The integrated help function and GUI interface ensure a quick start and ease of use.
- It can analyze all the file systems of the various operating systems (**www.prodiscover.com**).

D. Belkasoft Evidence Centre

Belkasoft Evidence Centre makes it easy for an investigator to collect, scan, examine, preserve, and transfer digital evidence found inside computer and mobile devices, RAM, and cloud. This toolkit can easily retrieve digital evidence from various sources by analyzing hard drives, memory dumps, iOS, Android backups, chip-off dumps, and so on. Evidence Centre will automatically analyse the data source and set out the most forensically relevant items for investigator to study, investigate more closely, or add to the report.

Features

Belkasoft Evidence Centre (BEC) have the following features that make it available for investigation:

If the investigator has to investigate a laptop or an iPhone app, desktop computer, or Android tablet, the same BEC program will help them understand what information is held inside.

- Doesn’t matter whether data is still held in files or removed, concealed in unallocated or slack space, the software can easily expose it by searching inside existing files, carving using file or record signatures, examining Volume Shadow Copy, and many other forensically relevant areas.
- Starting from the acquisition process, where the product allows the investigator to copy a hard drive, create a smart mobile device dump, capture RAM, and even access Google Drove or iCloud, to development of reports in various formats, the product eases all daily operations of the investigation.
- BEC is the best GUI interface and is easy to use the software as it requires only a few steps to get the result which are as follows:
    - Run the software and add a device that has to be analyzed.
    - Select the artefact for analysis.
    - The result is out in few minutes.
- Automatic extraction of application data can be enough to solve the majority of cases, where the investigator investigates Internet communications, documents, or images. The software knows all common applications such as WhatsApp, WeChat, Snapchat various browsers and mail applications such as Outlook, office formats such as MSWord or Open Office Spreadsheet, so the investigator need not to learn data formats, file locations, signatures for carving files or individual documents, encryption schema and so on.
- Although in most cases automated extraction would be enough, more complicated investigations can require manual examination of devices in question. In these types of investigation, BEC provides powerful File System explorer, which displays all volumes and partitions within the system, both existing and deleted directories, VCS snapshots, current and deleted files. Each partition or file can be reviewed in Hex Viewer, the window assisting the investigator to investigate individual bytes, make automatic type conversions, create bookmarks and apply various encodings.
- The software can detect skin and faces within pictures and images, identify texts in scans, detect encryption and decrypt 280+ types of files. Strong Photo Forgery Detection module identifies images that were edited after the shot was taken. Geolocation analysis can display all geo-enabled objects on Google Maps **(www.belkasoft.com)**.

E. F. Magnet Forensics

Magnet AXIOM is a complete digital research platform that allows examiners to acquire and analyse forensic data seamlessly, as well as to share their results. It includes the various components that are:

- **AXIOM Process:** It is the essential component of Magnet AXIOM as it includes the following features: -
  - Acquire photos from smartphones, computers, and more and examine the proof.
  - To collect and prepare data for review automatically, use Single Stage Processing to save you time and help you get to your study faster.
- **AXIOM Examine:** It is the second step that examines the evidence processed in the AXIOM Process. It includes the following features: -
  - For an in-depth, integrated analysis using active links, multiple views, filters, search, and more, access file system, registry, and artefact info.
  - Share results with customizable report views quickly and easily.

Features

Magnet AXIOM has a strong new interface that has been built to feel natural and familiar. The user interface system helps to work more easily through the analysis, switching between high-level information and the source data of particular objects. It includes the following features:

- **Efficient Analysis:** Identify crucial facts easily with the Artefact Explorer from the outset. The Artefact Explorer is designed to make it simpler and quicker for examiners to review and evaluate vast quantities of digital evidence, drawing from the artefact database, which is comprised of separate artefact tables for each supported artefact form.
- **File System Explorer:** It can explore the file system tree of the proof source using File System Explorer and review additional content, such as unallocated space and volume slack. Recursive views help to navigate the structures of hierarchical data.
- **Registry Explorer:** Registry Explorer helps to access the Windows registry's complex relational hierarchy and explicitly connects objects and files to registry keys, minimizing the amount of time the investigator spends crossing the tree.
- **Source Linking:** The source link helps you to explore the relationship between the objects retrieved and the file location of the source.
- **Source Links:** leap directly to the original file source position in the file system or registry from an individual recovered artefact in Artefact Explorer.
- **Linked Proof Links:** jump to a filtered view in the Artefact Explorer of all objects found in the selected location from an individual file or folder in File System Explorer or Registry Explorer **(www.magnetforensics.com)**.

Conclusion

In this paper, we studied the procedure of analysis of computer crime and the various tools used for analysis. Digital forensics or computer forensics is known little regarding the methodology of retrieving and examination of content stored on digital devices. With the increase in cybercrime, the digital forensic field has gained tremendous prominence, contributing to what was limited to recovery and analysis of biological and chemical evidence during criminal investigations. The sole purpose of computer forensic investigation is to determine the essence and circumstances of a crime and to classify the suspect in a formal investigative procedure. There are various types of computer crimes in which computers either act as a tool or a target which includes espionage, hacking, phishing, etc. These crimes could be easily detected by the simple elements of the investigation process i.e., acquisition, authentication, and analysis. The forensic investigator must conduct a proper search on the crime scene and maintain the integrity of the evidence as digital evidence are the easiest to alter so they must be handled carefully. Since computer crimes are at peak, it is necessary to have a pre-planned structure of the investigation in case an incident occurs which is known as Forensic Readiness (which refers to an organization’s ability to make optimal use of digital evidence in a limited period and with minimal investigation costs). So, it is necessary to have a deep and structured knowledge of the tools which could be used for forensic analysis whenever the investigator is faced with digital evidence.

References:

"Evidence Search and Analysis Software for Digital Forensic Investigations and Incident Response." *Belkasoft*, Accessed Date 12th October 2020, Accessed from https://belkasoft.com/

"FTK® Imager 4.2.0." *FTK Imager 4.2.0*, Accessed Date 10th October 2020, Accessed https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager

"Introduction to Magnet AXIOM." *Magnet Forensics*, Accessed Date 10th October 2020, Accessed from www.magnetforensics.com/resources/introduction-magnet-axiom/

"OSForensics - Digital Investigation for a New Era by PassMark Software." *PassMark OSForensics - Digital Investigation*, Accessed Date 09th October 2020, Accessed from www.osforensics.com/

"Products." *ProDiscover*, Accessed Date 09th October 2020, Accessed from www.prodiscover.com/products-services

Altheide, Cory, and Harlan A. Carvey. *Digital Forensics with Open Source Tools*. Syngress, 2011.

Autopsy, Accessed Date 12th October 2020, Accessed from www.sleuthkit.org/autopsy/.

Balogh, Stefan, and Matej Pondelik. "Capturing Encryption Keys for Digital Analysis." *Proceedings of tl IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems*, 15 2011, pp. 759–763., doi:10.1109/idaacs.2011.6072872.

Coronel, Bryan, et al. "A Systematic Literature Review in Cyber Forensics: Current Trends from the (Perspective." *2018 IEEE Third Ecuador Technical Chapters Meeting (ETCM)*, Oct. 2018, pp. doi:10.1109/etcm.2018.8580266.

Garfinkel, Simson L. "Digital Forensics Research: The next 10 Years." *The International Journal of Digital Forensics & Incident Response*, vol. 7, Aug. 2010, pp. 64–73., doi:10.1016/j.diin.2010.05.009.

Guo, Hong, et al. "Research and Review on Computer Forensics." *Forensics in Telecommunications, Information, and Multimedia*, 2010, pp. 224–233., doi: 10.1007/978-3-642-23602-0_21.

Hatole, Pranali P., and Shobha K. Bawiskar. "Literature Review of Email Forensics." *Imperial Journal of Interdisciplinary Research*, vol. 3, no. 4, Apr. 2017.

Kaur, Mandeep, et al. "A Literature Review on Cyber Forensic and Its Analysis Tools." *Ijarcce*, vol. 5, no. 1, 2016, pp. 23–28., doi:10.17148/ijarcce.2016.5106.

Kumar, Mohit. "A Detailed Study to Examine Digital Forensics and Cyber Security: Trends and Patterns in India." *International Journal of Forensic Science*, vol. 5, no. 2, 1st May 2020.

Law, Frank Y.w., et al. "Protecting Digital Data Privacy in Computer Forensic Examination." *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2011, pp. 1–6., doi:10.1109/sadfe.2011.15.

Lim, Kyung Soo, et al. "Applying a Stepwise Forensic Approach to Incident Response and Computer Usage Analysis." *IEEE*, 10th Dec. 2009, doi: 10.1109/CSA.2009.5404204.

Marrington, Andrew, et al. “A Model for Computer Profiling.” *2010 International Conference on Availability, Reliability and Security*, 2010, pp. 635–640., doi:10.1109/ares.2010.95.

Nassif, Luis Filipe Da Cruz, and Eduardo Raul Hruschka. “Document Clustering for Forensic Computing: An Approach for Improving Computer Inspection.” *2011 10th International Conference on Machine Learning and Applications and Workshops*, 2011, pp. 265–268., doi:10.1109/icmla.2011.59.

Pande, Dr. Jeetendra, and Dr. Ajay Prasad. *Digital Forensics*. Uttrakhand Open University, 2016.

Parker, Donn B. Criminal Resource Justice Manual. National Institute of Justice, 1989, Accessed Date 09th October 2020, Accessed from https://www.ncjrs.gov/pdffiles1/digitization/118214ncjrs.pdf

Raghavan, Sriram, and S V Raghavan. “A Study of Forensic & Analysis Tools.” *IEEE*, 21st Nov. 2013, doi:10.1109/SADFE.2013.6911540.

Shaaban, Ayman, and Konstantin Sapronov. *Practical Windows Forensics: Leverage the Power of Digital Forensics for Windows Systems*. Packt Publishing, 2016.

Simou, Stavros, et al. “Cloud Forensics Solutions: A Review.” *Lecture Notes in Business Information Processing*, June 2014, pp. 299–309, doi: 10.1007/978-3-319-07869-4_28.

Suteva, Natasa, et al. “Computer Forensic Analysis of Some Web Attacks.” *World Congress on Inte Security (WorldCIS-2014)*, 2014, pp. 42–47., doi:10.1109/worldcis.2014.7028164.

Vacca, John R., Computer Forensics: Computer Crime Scene Investigation, Second ed., Charles River Media Inc, 2005.

Wiles, Jack, and Anthony Reyes., Cyber Crime and Digital Forensics, Elsevier Inc., 2007.