A Job and Significance of Digital Forensics and Digital Evidences in Detection of Cyber Crime

Jaydevsinh B. Vala[1], Dr. Vipul M. Vekariya[2]

[1] *Research scholar, Gujarat Technological University, Gujarat*
[2]*Noble Group of Institutions, Gujarat*
[1]*jaydev.vala@gmail.com,* [2]*Vekariya.vipul@gmail.com*

Abstract: The development of computerized advances brings about the development of advanced cybercrimes. Cyber-crime is a developing issue, yet the capacity law enforcement organizations to explore and effectively indict crooks for these violations are muddled. While law enforcement agencies have been leading these examinations for a long time, the recently distributed requirements evaluations all showed that there is come up short on the preparation, devices, or staff to successfully direct examinations with the volume or multifaceted nature included a large number of these cases Digital legal sciences plans to gather wrongdoing related proof from different computerized media and investigate it. This survey reviews several branches, methods, and types of evidence in the literature which extract evidence from the system and analyze them. It also discusses the challenges during the collection and analysis of low-level data from the compromised system.

Keywords: Digital forensics, Branches of digital forensics, Digital artifacts, Memory Forensics

1. INTRODUCTION

In the past days of digital forensics, intrigue and exertion were centered on tending to independent and arranged PCs. As innovation has created, the center has reached out to incorporate the recuperation of proof from any gadget that has a computerized processor or digital storage capability. Therefore, the job of digital forensics has moved from the examination of PC based wrongdoings, for example, hacking, to the examination of a wide range of wrongdoing.

Progressively, with the data that can be recovered from car engine management, satellite route frameworks, and mobile phones, the kind of proof that can be gotten has developed from the recuperation of reports, pictures, and system action records to signs of a person's developments and exercises.

Investigators of traditional crime, for example, murder, theft, shakedown, and medication managing progressively seek the computerized condition for proof and signs of suspects' exercises. In the ongoing past, specialists of traditional crimes didn't comprehend the potential estimation of advanced proof, and accordingly, they would frequently disregard it. This is as of now changing, however, there is as yet far to go before specialists of ordinary wrongdoings comprehend the potential estimation of advanced proof, and appropriate degrees of assets are accessible to address it. Here, this overview concentrated on various cybercrime scene investigation branches, strategies, and kinds of proof.

Digital forensics is the science of detection, extraction, and analysis of the pieces of evidence from the digital media, and is one of the critical requirements in cyberspace. One important goal of digital forensics is to prepare court accepted reports. Three important components of digital forensics are hard disk, memory, and network forensics which record and analyze some tracks from behaviors of cybercriminals.

2. LITERATURE REVIEW

The focal point of a significant number of the first needs evaluations on the examination of violations including advanced proof didn't ordinarily concentrate on digital crime examination unmistakably, just were viewed as the general job of digital legal sciences in the criminal examination.

As innovation has improved, so has the manner in which it is utilized in government, business, the scholarly world, and our own lives. The potential estimation of cutting edge gadgets has been perceived and their utilizations have been embraced by the two hoodlums and specialists. There has been a consistent necessity for refreshed devices, strategies, and techniques that can be utilized for computerized legal examinations to address the expanding scope of gadgets that contain either advanced processors or advanced storage media, just as to address the mind-boggling situations in which they are found.

One of the few studies conducted between 2004 and 2010 was completed by Rahul Bhaskar (2006) and was written after the negative federal, state, and local government response to the destruction caused by Hurricane Katrina. The author compared that response to the likelihood that a digital Hurricane Katrina could occur. The study found that only a small number of responding law enforcement personnel had even a basic understanding of computer forensics, and those individual organizations thought it difficult to respond to incidents because of the limited knowledge of computer forensics within law enforcement and legal personnel such as prosecuting attorneys (Bhaskar, 2006). The author identified the key elements of computer forensics as identification, preservation, analysis, and presentation, and stated that the lack of performing these tasks uniformly across agencies caused uncertainty in the ability to ensure that digital evidence would withstand the scrutiny of trials (Bhaskar, 2006).

Much research done from 2014 to 2019 discussed different digital devices, shreds of evidence present in digital devices, different methods of collection, and analysis of digital evidence, tools, and technologies used in the digital forensics process.

3. REASONS FOR CONDUCTING A DIGITAL FORENSIC INVESTIGATION

The previous decade has seen already unheard of advances in innovation, and despite the fact that those improvements have profited people and organizations the same, they have likewise become apparatuses for fraudsters and digital crooks to take cash and information, and maintain a strategic distance from the location.

Hackers use innovation to conceal their illegal exercises and to move assets across locales and around the world. Their activities are unpredictable and they have noteworthy assets to assist them with sidestepping recognition. This implies those entrusted with exploring digital crime have needed to keep pace. We are seeing another type of specialist, the advanced legal professionals, who follow these crooks and their exercises.
In combination with digital forensics tools and techniques that they use, provide incredible insight into attack trends, how these criminal groups work, what their motivations are, what new tricks and tools they are using, and so on. This evidence gives valuable input into knowledge and best practice resources, as well as threat intelligence databases.

Furthermore, the evidence collected from a digital forensic analysis helps in incident response(IR) and remediation activities, once the company realizes that a breach has happened, also data can be assembled on new attack vectors, and sophisticated types of malware that might not have been seen before.

It is additionally especially valuable in following the way of advance persistent threat(APT) which utilizes an assortment of stunts and instruments to accomplish its finishes. APTs are profoundly focused on, and for the most part remain undetected on the casualty's system for a considerable length of time, performing surveillance and exfiltration information. Advanced crime scene investigation additionally assists with following these assaults and find what roused them.

Security professionals routinely use such tools to analyze network intrusions—not to convict the attacker but to understand how the perpetrator gained access and to plug the hole. Data recovery firms rely on similar tools to recover files from drives that have been inadvertently reformatted or damaged.

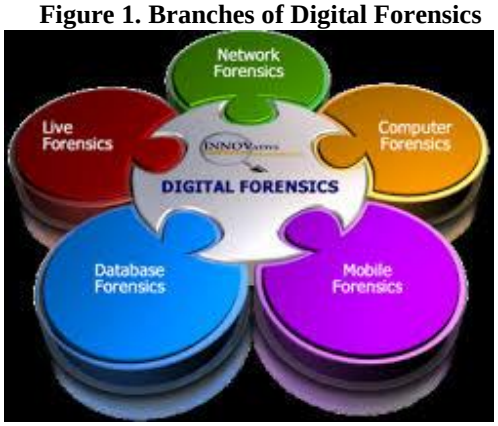
Regardless of the inspiration, the assessment, understanding, or remaking of following the proof in the digital world, forensic science is additionally practice of distinguishing, gathering, examining, and writing about data found on PCs, cell phones and systems, so that this all the proof is allowable in a legitimate setting. Moreover, proof of a wide range of crimes, for example, ambush, murder, human dealing, misrepresentation, and medication managing are progressively found in advanced gadgets that either the culprit or the casualty utilized.

Digital forensics is necessary for law enforcement and investigation, but also has applications in commercial, private, or institutional organizations. All activity conducted on an individual’s computer systems as well as on a company network leaves digital traces, which can range from the web browser history, caches and cookies, all the way to document metadata, deleted file fragments, email headers, process logs, and backup files.

4. VARIOUS BRANCHES OF DIGITAL FORENSICS

1) Network Forensics
2) Disk Forensic
3) Mobile Device Forensics
4) Database Forensics
5) Printer Forensics
6) Digital Music Device Forensics
7) Scanner Forensics
8) Multimedia Forensics
9) Memory Forensics

Figure 1. Branches of Digital Forensics



1) Network Forensics

Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time. Security professionals routinely use such tools to analyze network intrusions not to convict the attacker but to understand how the perpetrator gained access and to plug the hole.

It also helps to investigate offenses after the event, govern how they occurred, and identify the party or parties responsible. A digital forensic investigator will gather network-based evidence from a particular computing device in the network so that it can be presented in court, conducting a thorough digital investigation and building a documented chain of evidence.

2) Disk Forensics

Disk forensics deals with extracting data from storage media like Hard disk, USB devices, FireWire devices, CD, DVD, Flash drives, Floppy disks, etc; by searching deleted files, active and unallocated spaces, and slack spaces.

- **Process of Disk Forensics:**

A. Identification:

The first step in Disk Forensics is the identification of the storage devices in the crime scene. Computers may have disks like Hard disk of IDE/SCSI, CD, DVD, Floppy Disk, etc, Mobiles, PDAs, etc, may have the flashcard, SIM, USB / Fire wire disks, Magnetic Tapes, Zip drives, Jazz drives, etc.

B. Acquisition:

Once the identification of evidence is completed, it should be acquired by any of the forensic imaging tools. The acquisition is a process of bit-stream imaging. Imaging should be done with correct and complete data and also it should maintain the Disk Geometry. During this process, the source media should be write-protected.

C. Authentication:

Once the imaging has done, it should be verified with the original one. Hashing is a mechanism to prove that the copy is exact with original and it has not been altered.

D. Preservation:

Digital evidence might be altered or tampered without a trace. Once the acquisition and authentication have completed, the original evidence should be placed in secure storage. One more copy of the image should be taken and it

needs to be stored into appropriate media or reliable mass storage. Optical media can be used as mass storage. It is a reliable, fast, longer life span and reusable.

E. Analysis:

An analysis is a finding of relevant information in the digital evidence. Analysis should be in the complete evidence without leaving a single bit of information. Searching may be of files or data in normal files and folders, databases, cookies, temporary files, swap, Internet History, Registries, Pictures, passwords, etc, and ambient data area like deleted, formatted, slack, unallocated, lost.

F. Finding:

Report generation is an important task in Disk Forensics. The value of the evidence will eventually depend on the way it is presented. Technical evidence of the report should be in a simple and precise way so that the non – technical person can also understand.

3) Mobile Device Forensics

Mobile phone forensics deals with recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Mobile phones, especially those with advanced capabilities, are a relatively recent phenomenon, not usually covered in classical computer forensics. Cell phones differ in design and are continually changing as existing technologies improve and new technologies are introduced. Developing an understanding of the components and organization of cell phones is a prerequisite to understanding the criticalities involved when dealing with them forensically. Cell phone forensics includes the analysis of both SIM and phone memory, each requires a separate procedure to deal with. It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.

4) Database Forensics

Digital forensic is a branch of digital forensic relating to forensic study and applying investigative techniques to of databases and their related metadata. A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity to verify the actions of a database user. Alternatively, a forensic examination may focus on identifying transactions within a database system or application that indicates evidence of wrongdoing, such as fraud.

5) Printer Forensics

Literature is an immediate assistant to numerous hoodlums and fear-based oppressor acts. What's more, printed material might be utilized over the span of directing illegal or psychological militant exercises. In the two cases, the capacity to recognize the gadget or kind of gadget used to print the material being referred to would give an important guide to law implementation and knowledge organizations. For instance, forgers regularly carefully filter money and afterward use shading laser and inkjet printers to deliver false bills. Falsifiers utilize similar techniques to make counterfeit international IDs and different archives. Agents need to have the option to verify that a phony bill or report was made on a

specific brand and model of printer. They additionally need to recognize which model printer was utilized as well as explicitly which printer was utilized. In this way, it will be conceivable to differentiate between fake bills made on explicit printers regardless of whether they are a similar model.

First, by analyzing a document we can identify characteristics that are unique for each printer and second by designing printers to purposely embed individualized characteristics in documents. The second method is done by most of the latest printer manufacturing companies. No two printers of the same model will behave in the same pattern. This is because the mechanical parts, which make the printer, will not be 100 percent equivalent. Manufacturing such printers would reach the point where each printer would be too expensive for consumers. If, however, the printer cartridge is changed after a document is printed, the document no longer can be traced to that printer.

6) Digital Music Device Forensics

Huge storage capacities and PDA functionalities have made the digital music device a technology that should be of interest to the cyber forensic community. The advanced music unrest has additionally observed the digital music gadget become a typical family unit thing. It is just a brief timeframe until they also make a characteristic movement into the criminal world. This movement has just started. A portion of the hard drive-based gadgets have limits as much as 60GB. With this much storage space for music, developers have spread out and included highlights like a schedule and contact book (Apple iPod - Music and that's just the beginning). These gadgets are essentially a versatile hard drive and can store different kinds of records other than music, for example, reports or pictures.

A member of staff could take sensitive information by using the capabilities of a digital music device. Suspects could potentially store critical evidence on these types of devices. It must be determined if current frameworks of cyber forensics are applicable and to what extent current guidelines can be applied to digital music device forensics.

7) Scanner Forensics

An enormous bit of digital picture information accessible today is made utilizing obtaining gadgets, for example, advanced cameras and scanners. While cameras permit digital reproductions of natural scenes, scanners are utilized to catch printed copy art is progressively controlled situations. For forensic methodology, a non-intrusive scanner model distinguishing proof, which can be additionally stretched out to confirm filtered pictures is a need.

Using only scanned image samples; a robust scanner identifier should determine the brand/model of the scanner used to capture individual scanned images. A proposal for such a scanner identifier is based on statistical features of scanning noise. Scanning noise of the images can be done from multiple perspectives including wavelet analysis, neighborhood prediction, image denoising, and obtain statistical features from each characterization. The same approach can be extended to digital cameras and other imaging devices. The most significant challenge is that “analytical procedures and protocols are not standardized nor do practitioners and researchers use the standard terminology.

The technology change will result in new devices emerging in the digital world. Whenever a new digital device comes in the market a forensic methodology has to evolve to deal with it. This phenomenon will expand the field of device forensics.

8) Multimedia Forensics

Multimedia Forensics includes a set of scientific techniques recently proposed for the analysis of multimedia signals (audio, videos, images) to recover probative evidence from them; in particular, such technologies aim to reveal the history of digital contents: retrieving information from multimedia signals.

9) Memory Forensics

Memory forensics (sometimes referred to as memory analysis) refers to the analysis of volatile data in a computer's memory dump. Cyber forensics investigators conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.

5. IMPORTANT SOURCES OF DIGITAL EVIDENCE

A. Computer System

A computer system and its components can be valuable evidence in an investigation. The computer hardware, software, e-mail and attachments, databases, financial information, Internet browsing history, documents, photos, image files, chat logs, event logs, data stored on external devices, and identifying information associated with the computer system and components are all potential evidence.

B. Portable Devices

Potential evidence also named Handheld devices such as mobile phones, smartphones, PDAs, digital multimedia (audio and video) devices, global positioning system (GPS) receivers, pagers, and digital cameras may contain software applications, data, and information such as documents, e-mail messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, and financial records that are valuable evidence in an investigation or prosecution.

C. Storage devices

Storage devices like hard drives, external hard drives, removable media, thumb drives, and memory cards may have information such as e-mail messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, financial records, and event logs that can be valuable evidence in an investigation or prosecution.

D. Peripheral Devices

Peripheral devices are the devices that can be connected to a computer or computer system to enhance user access and expand the computer’s functions. The devices themselves and the functions they perform or facilitate are all potential evidence. Information stored on the device regarding its use also is evidence, like incoming and outgoing phone and fax numbers; printed documents, recently scanned and faxed documents, and information about the purpose for or use of the device. In addition, these devices can be sources of fingerprints, DNA, and other identifiers.

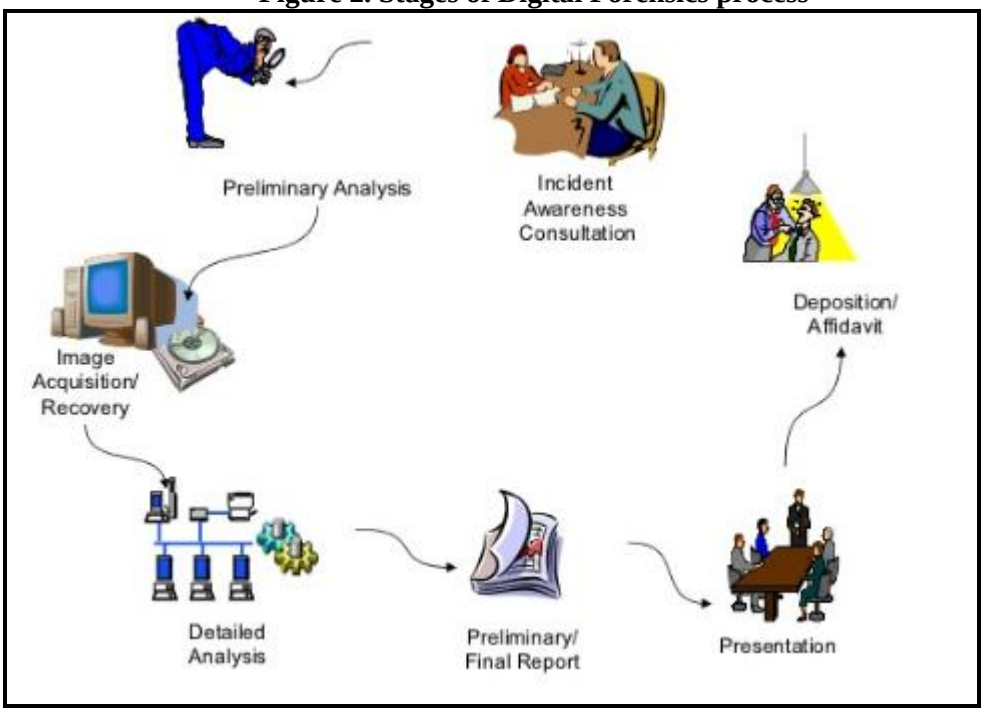
E. Computer Networks

A computer network involves two or more computers linked by data cables or by wireless connections that share or are capable of sharing resources and data. A computer network often includes printers, other peripheral devices, and data routing devices like routers, switches, and hubs. The networked computers and connected devices themselves can be evidence that is useful to an investigation or prosecution. The information present in it may also be valuable evidence and may include software, documents, photos, image files, e-mail messages and attachments, databases, financial information, Internet browsing history, log files, event and chat logs, buddy lists, and data stored on external devices. The device functions, capabilities, and any identifying information associated with the computer system; components and connections, including the Internet protocol (IP) and local area network (LAN) addresses associated with the computers and devices; broadcast settings; and media access card (MAC) or network interface card (NIC) addresses may all be useful as evidence.

6. STANDARD OPERATING PROCEDURES (SOP) OF DIGITAL FORENSICS INVESTIGATION

The Standard Operating procedure of digital forensics divided into four to five steps. Different standard organizations define it in mostly 4-5 stages.

Figure 2. Stages of Digital Forensics process



The National Institute of Standards and Technology, NIST divide any forensics investigation into four phases, which are briefly summarized below:

A. **Collection:** Identify, label, record, and acquire data from possible sources, while preserving the integrity of the data.
B. **Examination:** Use manual and automated methods to assess and extract data of particular interest, while preserving the integrity of the data
C. **Analysis:** Use legally justifiable methods and techniques to derive useful information

D. Reporting: Describe actions used, explain how tools and procedures were selected, determine what other actions need to be performed, including forensic examination of additional data sources, securing identified vulnerabilities, and improving existing security controls. Recommend improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.

7. COMPUTERS IN BUSINESS ENVIRONMENT

As often as possible have confused setups of various PCs arranged to one another, to a typical server, to organize gadgets or a mix of these. Making sure about a scene and gathering computerized proof in these situations may present difficulties to the person on call. Inappropriately closing down a framework may bring about lost information, lost proof, and potential common risk.

The person on call may locate a comparable situation in private areas, especially when a business is worked from the home.

In some instances, the first responder may encounter unfamiliar operating systems or unique hardware and software configurations that require specific shutdown procedures. Such circumstances are beyond the scope of this guide.

8. EMERGING PROBLEMS:

As challenging as the profession of digital forensics has been to date, still, more interesting problems are looming on the horizon. Computers are proliferating throughout modern society, and as their numbers grow, they change in size, shape, speed, and function. Once we gathered digital evidence from monolithic, stand-alone mainframes.
Today we have PCs, laptops, palmtops, and PDA's, supercomputers, distributed client-server networks all of which can, and do, provide digital evidence at times. We have networks that use twisted pairs, coaxial cables, fiber optic cables, radio, and infrared radiation to convey information. We have LAN's and WAN's. Digital evidence stored in one computer is readily available to a miscreant using another computer half a world, and several legal jurisdictions, away.

As PCs become littler, quicker, and less expensive, PCs are progressively implanted within other bigger frameworks in manners that are not constantly clear and permit data to be made, put away, handled, and conveyed in manners that are extraordinary. Thus, advanced proof can emerge in surprising spots and structures. Instrumentation of spaces for each reason from natural checking to intuitive control of heart rhythms will imply that computerized proof will be considerably increasingly hard to gather and investigate, and harder to introduce in manners that the trier of truth can comprehend and utilize.

Modernized control frameworks oversee banks, processing plants, retail inventories, aviation authority, medical clinics, schools, partnerships, and government associations. PCs and their product programs are installed in our vehicles, pontoons, prepares and planes, in instruments, gear, and hardware, in media communications frameworks and open exchanged systems, even in our bodies. Every one of them is a potential wellspring of advanced proof, the assortment, stockpiling, investigation, and introduction of which is and will be obliged by developing lawful measures and requirements that we neglect to comprehend at our risk.

9. CONCLUSION

As discussed above, computerized legal sciences(Digital forensics) assumes a noteworthy job in the criminal equity framework as we keep on joining a scope of innovations into our regular daily existences. Proof of all most kinds of wrongdoing is progressively found in advanced gadgets that either the culprit or the casualty utilized. Because of this potential proof that didn't exist previously, agents of regular violations progressively need to consider any advanced proof that might be accessible.

What's more, Security experts routinely utilize such instruments to investigate arrange interruptions not to convict the assailant however to see how the culprit got entrance and to plug the gap. Information recuperation firms depend on comparable instruments to restore documents from drives that have been incidentally reformatted or harmed.

In the future, digital forensics will play an increasingly significant role in the criminal justice system as we continue to incorporate a range of technologies into our everyday lives. As the digital forensic discipline continues to mature, those in the criminal justice system will more readily understand and accept the contribution it can make to the discovery and production of evidence.

10.REFERENCES

10.1. Reports
[1] The Role and Impact of Forensic Evidence in the Criminal Justice Process by Joseph Peterson, Ira Sommers, Deborah Baskin, and Donald Johnson,2010 (Joseph Peterson, 2010).
10.2. Journal Article
[2] Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies, volume 11, article 4, journal of digital forensics, security and lawby Teri A. Cummins Flory (Purdue University),2016 (Flory, 2016).
10.3 Document of SOP
[3] STANDARD OPERATING PROCEDURE OF DIGITAL EVIDENCE COLLECTION (Digital Forensics Department, Cyber Security Malaysia) (Talib, 2013).
10.4 Report
[4] Forensic Examination of Digital Evidence: A Guide for Law Enforcement (Ashcroft, 1994).
10.5 Document from website
[5] ISO/IEC 27037:2013, Guidelines for Identification, Collection, Acquisition and Preservation of digital evidence, International Standard Organization (ISO/IEC JTC 1/SC 27 Information security, 2012).
10.6 Content from website
[6] SWGDE Best Practices for Computer Forensics Version 2.1 (SWGDE, 2006).
10.7 Document in ASCLD/LAB 2011 edition
[7] Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories, 2011 edition, ASCLD/LAB-International, 2010. (Laboratories, 2010).

10.8 Content from website
[8] ISO/IEC 17025:2005, General Requirements for the Competence of Testing and Calibration Laboratories, 1st Revision, 2005, International Standard Organization. (assessmen, 2005).
10.9 Report
[9] 2019 Official Annual Cybercrime Report by Cybersecurity Ventures (Morgan, 2019).

10.10 Book
[10] DIGITAL FORENSICS :Digital Evidence in criminal investigations (Marshall, 2013).
10.11 Article from The American Archivist, volume 72
[11] Long-Term Preservation of Digital Records: Trustworthy Digital Objects By Henry Gladney,2009 (Gladney, 2009).
10.12 Article in Researchgate
[12] Systematic Digital Forensic Investigation Model by Mr. Ankit Agarwal (agarwal, 2011).
10.13 Book
[13] Digital Forensics for Legal Professionals: Understanding Digital Evidence From the Warrant to the Courtroom (Daniel, 2011).
10.14 Website
[14] National Institute of Science and Technology, Information Technology Library, NIST Computer Forensics Tool Testing Program. http://www.cftt.nist.gov(nist, 2019).
10.15 website content
[15] Best Practices In Digital Evidence (Henry, 2009).