YourLawArticle

Open Access Law Journal, ISSN (O): 3049-005

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher Reet Parihar

Role Of Cyber Forensic Experts In Cyber Investigation

Anand Sharma, B.A.LL.B (Hons.), Galgotias University

Published on: 5th June 2025

Abstract

Computers have become an indispensable element of our everyday life. We now work in a different method as a result of them. As a result, cybercrime is rapidly expanding. Criminals have realised that to continue their illicit activities, they must stay current with the times. Phishing is an example of a common form of cybercrime. As a result, it's crucial to figure out exactly what happened. The ability to expose is known as "cyber forensics." Cyber Penetrators have become more proficient in their tools and techniques, putting the worldwide phenomenon's activities in jeopardy. Antiforensic tactics are also being used by these attackers to conceal evidence of a cybercrime. During an investigation, computer forensic professionals collect and analyse potential evidence, such as data that has been deleted, encrypted, or destroyed. Digital forensics has unearthed crucial data that will enable cybersecurity firms to design technologies that will prevent hackers from gaining access to a network, website, or device. Hackers and hijackers are adept at breaking into a person's or company's device or network, but digital forensics has gathered information. Any steps made during this process are documented, and procedures are employed to ensure that the evidence is not tampered with, damaged, or destroyed. Cyber forensics technologies must become more resilient to combat these advanced persistent threats. This review paper looks at the basics of cyber forensics, the several phases of cyber forensics, useful tools, and emerging research trends in this fascinating field.

Keywords: *Cyber forensics, cyber investigation, Artificial Intelligence*

INTRODUCTION

Predators are always on the lookout for an opportunity to exploit innocent people at any given time. Computers and the Internet have given some of these predators a new instrument with which to carry out their nefarious plans. As a result of the continual rise in cases of cyber terrorism, Internet fraud, and on a regular basis, Computer forensics has, and will continue to evolve in response to ever-evolving viruses. Becoming a more prominent government and law enforcement focal point. To lessen the chance of becoming a victim, various precautions and procedures must be followed. In the realm of computer forensics, there is also a plethora of tools accessible for use by skilled professionals. There are also some things that can be done to instil a great deal of terror in individuals who may be the perpetrators. Cyber forensics is one such method. It is a one-of-a-kind technique for identifying, conserving, evaluating, and presenting digital evidence in a legally acceptable manner.

Computer forensics is the process of identifying, documenting, and interpreting computer material in order to use it as evidence and/or recreate a crime scene. Computer forensics, according to Garber, is described as the process of locating, gathering, conserving, evaluating, and presenting computer-related evidence in a legally admissible manner to a court. Offenders' deleted files can be recovered and used as serious evidence in court. A forensic specialist noticed that a computer can produce data in court that was previously difficult to produce by reporting. Another benefit is that a forensic doctor can look through the hard drive. It is advantageous to use diverse languages because cybercrime is readily committed. Through the Internet, you can travel across borders. It's important to remember that evidence can't be captured more than once; therefore, enlisting the help of the correct professionals is crucial.[1]

Computer forensics has recently branched into various overlapping domains, resulting in a slew of words like digital forensics, system forensics, network forensics, web forensics, data forensics, proactive forensics, email forensics, enterprise forensics, cyber forensics, and so on. On standalone machines, system forensics is carried out. Network forensics is gathering and analysing network events in order to identify the origins of security breaches. Web forensics is the name for the same procedure used on the internet. The study of volatile and

[1] *Role of Cyber Forensics in Investigation of Cyber Crimes* (IJLMH, 2023) https://www.ijlmh.com/wp-content/uploads/ROLE-OF-CYBER-FORENSICS-IN-INVESTIGATION-OF-CYBER-CRIMES.pdf accessed 5 June 2025.

non-volatile data is the main focus of data forensics. Proactive forensics is a type of forensics that is ongoing, with the ability to collect prospective evidence frequently.[2] E-mail. In forensics, one or more emails are used as evidence investigation. Cyber forensics is concerned with acquiring online evidence in real time. Identification, extraction, and reporting of data received from a computer system are all part of forensics analysis. With the increased usage of the Internet in homes and offices, there has been a growth in cyber-related crimes, and investigating these crimes is a time-consuming operation. Any criminal conduct involving computers or computer networks is commonly referred to as cybercrime. Crimes directed against computers, crimes where the computer carries evidence, and crimes where the computer is utilised to perpetrate the crime are all categorised as cybercrimes. Cybercrime is sometimes known as e-crime, computer crime, or Internet crime. A user sitting in a Net cafe in a distant place can use the Internet to conduct an attack on a computer resource in the United States, utilising a computer in Britain as a launch pad. These conditions present both technological and jurisdictional challenges. The cardinal pillars of cybersecurity are confidentiality, integrity, and availability, and they should not be compromised in any way. Anti-forensic tactics are also being used by attackers to obscure evidence of a cybercrime. They can change, edit, or modify file data, as well as hide directories, rename files, erase logs, and change, edit, or modify file data. In November 2003, the Indian government established a Cyber Forensics Laboratory to combat these types of crimes.

CRIMES AND CYBERCRIMES

Though punishment is the expected outcome of a crime, the conventional standards for establishing the crime result in a situation where the criminal's acquittal is far more common than the imposition of punishment. In India, the conviction rate, or the proportion of accused persons found guilty of crimes by the courts, is around 46.9%, implying that the vast majority of criminals get away with their crimes. In the case of cybercrime, the conviction rate is much lower, at 23.9 per cent. This trend in Indian criminal law is unhealthy because it causes responsible and honest persons to lose faith in the legal system. It motivates future criminals to enter the criminal realm, as well as urges offenders who have escaped punishment to commit more horrible crimes. This ailment may generate disruptions and upheavals in the

[2] *Role of Cyber Forensics in Investigation of Cyber Crimes* (NIRDPR Journal) https://nirdprojms.in/index.php/maj/article/view/166787/114628?__cf_chl_tk=axBOqicPCoTsH_HjIvdr0TDYNHJpFuQv9JEYDVh_944-1749022884-1.0.1.1-PGz5JO9a_tDlkrLENr6h4eCugFUjYDTjV3oCKRkVodU accessed 5 June 2025.

so-called "free market" if it is not dealt with strongly and decisively. As a result, it is critical and urgent to address the causes of acquittals. Globalisation and digitization of information have had an impact on all of us in today's information age, posing a plethora of legal, ethical, and sociological concerns. Cybercrime, a newer form of criminal activity, has had a tremendous impact on the criminal justice system. Technology advancements have not only resulted in the creation of new types of crimes, but they have also added new dimensions to crime detection and investigation.[3]

LEGAL UPDATION

Law can no longer stay unaffected by technological progress. Rather, it tends to follow them, even if it is slow to respond to technological improvements. As a result, various legal measures have been adopted to deal with cybercrimes, including amendments to the Indian Penal Code, Evidence Act, and Bankers Books Evidence Act, among others, as well as the enactment of the Information Technology Act, 2000, which is the mother legislation dealing with cybercrimes. The Indian Congress was forced to revise the Information Technology Act due to the increasing prevalence and dynamics of cybercrime. The Information Technology (Amendment) Act, 2008 was enacted with this goal in mind, as well as to bring IT law in line with the Model Law on Electronic Signatures adopted by the United Nations Commission on International Trade Law. Electronic evidence is now relevant and acceptable in Indian courts, thanks to changes to the Indian Evidence Act. However, there is still a big space where the intersection of law and computers can lead to significant advancements. The most crucial aspect of this field that has yet to be explored is criminal investigation and the use of digital evidence in courts. This is something that has been felt and emphasised. The Justice V.S. Mali Math Committee Report (2003), the Law Commission of India's 185th Report, and the Justice J.S. Verma Committee (2013) have all recommended that efforts be made in the direction of scientific criminal investigation and computer forensics. According to a study, Largescale acquittals by Indian courts are largely due to a lack of scientific research. The availability of scientific investigative methods and methodologies has resulted in a conviction rate of 80 to 90% in the United Kingdom and the United States. As a result, the Indian judicial system has achieved considerable headway in the field of scientific

[3] Satish Kumar and others, 'Cyber Forensic - A Literature Review' (ResearchGate, 2022) https://www.researchgate.net/publication/358780840_Cyber_Forensic_-A_Literature_Review accessed 5 June 2025.

criminal investigation, and it anticipates much more study and effort in this area. The achievements have been lauded.

Forensics is a term that refers to the study of crime.

CYBER FORENSICS

Cyber forensics is the process of gathering, evaluating, and presenting evidence to the courts utilising scientific knowledge. Cyber forensics is essentially a hybrid of computer forensics and network forensics. The goal of a cyber-forensic investigation is to recover evidence that can be used to support or refute a criminal action. It necessitates the investigators gathering and analysing electronic evidence. Fingerprinting, blood analysis, toxicology, DNA mapping, facial reconstruction, handwriting, paternity issues, ballistics, chemical analysis, autopsy, disputed document analysis, Brain Electrical Activation Profile, Narco, Polygraph, Sound Spectograph/Voice Print Studies, Signature verification, Cyber Forensics, and so on are some examples.[4]

Cyber Forensics Phases II Incident identification, evidence collecting, evidence analysis, and reporting with evidence storage are the four phases of cyber forensics [Cole, 2010]. Figure 2 depicts the many steps of the cyber forensics process, as well as the responsibilities of each phase. The identification phase is primarily concerned with incident identification, evidence collection, and evidence verification. The acquisition phase records the current status of a computer system so that it can be evaluated later. The data is collected and examined in the analysis phase to locate the pieces of evidence. Documentation and evidence keeping are part of the reporting step.

PHASE 1: IDENTIFICATION: The process of identifying evidence material and its likely placement is known as the identification phase. Unlike a traditional crime scene, this phase processes the incident site and documents everything that happens. Evidence must be handled with care. Evidence must be delivered without modification as a basic need in evidence collection. This criterion applies to all stages of forensic investigation. Evidence collecting necessitates a careful examination of system logs, time stamps, and security monitors. It is vital to account for the evidence once it has been acquired. To establish a chain of custody, or the documenting of the possession of evidence, investigators would

[4] *Cyber Forensics: An Overview* (IJFMR, 2023) https://www.ijfmr.com/papers/2023/5/6967.pdf accessed 5 June 2025.

require extensive forensics. The purpose of a chain of custody in computer forensics and the legal system is to maintain the integrity of evidence, hence, evidence should be physically held in a secure location, and a complete log should be kept. The evidence and chain of custody are both important during the investigation of an incident. Their computer security incident handling guide detailed how to handle particular types of incidents (Denial of Service, Malicious Code, Unauthorised Access, and so on).

PHASE 2: ACQUISITION: The acquisition phase records the current condition of evidence, which can then be evaluated further. This phase's purpose is to save all digital values. A copy of the hard disc is generated here, which is referred to as an image. Discussed the various methods of data collection and their relative benefits and drawbacks. There are three sorts of frequently acknowledged forensics acquisitions, according to the law enforcement community: mirror image, forensics duplication, and live acquisition. A mirror image, often known as a bit-for-bit copy, is a backup of the complete hard disk. In theory, creating a mirror image is straightforward, but it must be accurate to meet evidence standards. The goal of having a mirror image is to provide proof if the original system needs to be restarted for further investigation. A sector-by-sector forensic duplication is an advanced method that makes a copy of every bit without leaving any trace of the evidence. The end output may be a single huge file, but it must be an accurate bit stream representation of the original drive. Because it provides a forensic image of the e-evidence and also contains file slack, this method is the most common sort of acquisition. Surplus bytes are accessible in the file Slack if a tiny file overwrites a larger file. Tools such as the Forensic Tool Kit (FTK) imager, the UNIX dd command, and Encase can be used in the forensic duplicating process. The FTK from Access Data is one of the more capable tools on the market, and one of its most promising capabilities is the ability to detect steganography, the practice of hiding data in plain sight. It's common to want to capture volatile data that's stored in RAM because it can't be gathered after the machine has been turned off. This information may not be saved in a file system or image backups, but it could contain information about the attacker. In volatile information, all presently operating processes, open sockets, currently logged users, recent connections, and so on are available. In general, intruders take precautions to avoid being discovered. Trojans, key loggers, worms, and other malware are hidden in plain sight. Rootkits, automated packages that establish backdoors, are one such element to consider throughout the purchase process.

REASON FOR CONDUCTING A DIGITAL FORENSIC INVESTIGATION

Technology has advanced to previously unimaginable levels in the last decade, and although these advancements have benefited individuals and organisations alike, they have also become instruments for fraudsters and cyber criminals to steal money and data while avoiding discovery. Hackers utilise technology to conceal their criminal activities and transport money across borders and around the world. Their operations are intricate, and they have a significant budget to help them avoid detection. As a result, individuals responsible for investigating cybercrime have had to keep up with the times. A new generation of detectives, known as digital forensic practitioners, is emerging to track down these criminals and their actions. In combination with the digital forensics tools and procedures they employ, they provide invaluable information on attack trends, how criminal groups operate, what motivates them, and what new tactics and tools they employ, among other things. This information is useful for knowledge and best practice resources, as well as threat intelligence databases. Furthermore, once a corporation realises that a breach has occurred, the information gathered from a digital forensic investigation aids in incident response and remediation efforts. Data can also be obtained on new attack vectors and complex varieties of malware that have not been seen previously. It's also valuable for following the trail of an advanced persistent threat (APT) that uses a range of techniques and tools to accomplish its goals. APTs are highly focused and often remain unnoticed on the victim's network for months, doing reconnaissance and data exfiltration. Digital forensics also aids in tracing the origins of these assaults and determining what inspired them. Security specialists commonly employ such technologies to investigate network intrusions, not to punish the offender, but to figure out how the intruder got in and close the hole. Similar programs are used by data recovery companies to recover files from discs that have been accidentally reformatted or destroyed. Regardless of the purpose, digital forensics is the discipline of detecting, gathering, analysing, and reporting on information found on computers, mobile devices, and networks in such a way that all evidence is admissible in a judicial context. Furthermore, evidence of various types of crimes, including assault, murder, human trafficking, fraud, and drug dealing, is increasingly being discovered on digital devices used by either the perpetrator or the victim. Digital forensics is essential for law enforcement and investigations, but it can also be used in commercial, private, or institutional settings. Every action taken on a person's computer or a company network leaves digital traces, which might range from web browser history caches and cookies to document metadata, deleted file fragments, email headers, process logs, and backup files. [5]

VARIOUS BRANCHES OF DIGITAL FORENSICS

The field of digital forensics is extremely broad. As a result, it needs to be divided into specialised areas to permit a larger knowledge base in each area. When Cyber Forensics is broken into four or five divisions, it is easier to have experts in each field rather than one expert who knows everything. The following are the branches of Digital Forensics:

- Disk Forensics
- Printer Forensics
- Network Forensics
- Mobile Device Forensics
- Database Forensics
- Digital Music Forensics
- Scanner Forensics
- Multimedia Forensics

DISK FORENSICS: The science of extracting forensic evidence from digital storage media such as hard discs, USB devices, FireWire devices, CD, DVD, Flash drives, and floppy discs is known as disk forensics

PRINTER FORENSICS: Many criminals and terrorists use printed material as a direct tool. Furthermore, printed content could be used in the course of illegal or terrorist acts. The ability to identify the equipment or type of device used to print the content in question would be useful in both circumstances. Law enforcement and intelligence organisations will benefit greatly from this.

NETWORK FORENSICS: Network forensics is a subset of digital forensics that focuses on network traffic monitoring and analysis. Network forensics is the act of acquiring and examining raw network data, as well as routinely tracing and monitoring network traffic, in

[5] Satish Kumar and others, 'Cyber Forensic - A Literature Review' (ResearchGate, 2022) https://www.researchgate.net/publication/358780840_Cyber_Forensic_-A_Literature_Review accessed 5 June 2025.

order to ensure network security and the manner in which an attack took place. In most cases, traffic is intercepted at the packet level and either saved for later analysis or filtered in real time. Network data, unlike other types of digital forensics, is frequently volatile and rarely documented, making the discipline reactive. Such technologies are frequently used by security professionals to investigate network intrusions, not to punish the offender, but to understand how the criminal acquired access. It also aids in the investigation of crimes after they have occurred, determining how they occurred and identifying the accountable party or parties. A digital forensic investigator will collect network-based evidence from a specific computing device in the network in order to present it in court, completing a full digital investigation and creating a documented chain of evidence.

MOBILE FORENSICS: The science of recovering digital evidence from a mobile phone under forensically sound conditions using approved methodologies is known as mobile phone forensics. Mobile phones, particularly those with advanced capabilities, are a novel phenomenon that is rarely addressed in traditional computer forensics. Cell phones come in a variety of designs and are constantly evolving as existing technology improves and new ones emerge. Understanding the components and organisation of cell phones is necessary for success. When dealing with them forensically, it's important to comprehend the criticalities involved. Similarly, because logs of usage and other data are kept on cellular networks, they are a significant element of cell phone forensics. The study of cell phones is known as forensics.

Both the SIM card and the phone memory must be dealt with separately.

DATABASE FORENSICS: Database forensics is a subset of digital forensics that involves applying investigative techniques to database contents and metadata while following the standard forensic methodology. Cached data may also exist in a server's RAM, necessitating the use of live analytic tools. The timestamps that apply to the update time of a row in a relational table may be inspected and evaluated for correctness in order to validate the actions of a database user during a forensic analysis of a database. A forensic examination, on the other hand, could focus on discovering transactions within a database system or application that reveal proof of wrongdoing, such as fraud.

DIGITAL MUSIC DEVICE: The digital music device has become a technology that should be of interest to the cyber forensic community due to its large storage capacity and personal digital assistant (PDA) features. As a result of the digital music revolution, the digital music player has become a common household item. It will only be a matter of time before they follow in their footsteps into the criminal realm. This process has already started. Some of the hard drive-based devices can hold up to 60GB of data. With so much music storage, developers have expanded to include functionality such as a calendar and contact book (Apple iPod — Music and more). These devices are essentially portable hard drives that can hold files other than music, such as documents or photographs. Using the capabilities of a digital music device, an employee might steal important information. These types of devices could be used by suspects to keep crucial evidence. It must be assessed whether current cyber forensic science frameworks are suitable for digital music device forensics and to what degree current guidelines may be implemented.

NETWORK FORENSICS: Network forensics is a subset of digital forensics that focuses on network traffic monitoring and analysis. Network forensics is the act of acquiring and examining raw network data, as well as routinely tracing and monitoring network traffic, in order to ensure network security and the manner in which an attack took place. In most cases, traffic is intercepted at the packet level and either saved for later analysis or filtered in real time. Network data, unlike other types of digital forensics, is frequently volatile and rarely documented, making the discipline reactive. Such technologies are frequently used by security professionals to investigate network intrusions, not to punish the offender, but to understand how the criminal acquired access. It also aids in the investigation of crimes after they have occurred, determining how they occurred and identifying the accountable party or parties. A digital forensic investigator will collect network-based evidence from a specific computing device in the network in order to present it in court, completing a full digital investigation and creating a documented chain of evidence.[6]

MOBILE FORENSICS:

The science of recovering digital evidence from a mobile phone under forensically sound conditions using approved methodologies is known as mobile phone forensics. Mobile phones, particularly those with advanced capabilities, are a novel phenomenon that is rarely addressed in traditional computer forensics. Cell phones come in a variety of designs and are constantly evolving as existing technology improves and new ones emerge. Understanding the components and organisation of cell phones is necessary for success. When dealing with them forensically, it's important to comprehend the criticalities involved. Similarly, because

[6] 'Cyber Forensic Science' (LIFS) https://lifs.co.in/blog/cyber-forensic-science.html accessed 5 June 2025.

logs of usage and other data are kept on cellular networks, they are a significant element of cell phone forensics. The study of cell phones is known as forensics.

Both the SIM card and the phone memory must be dealt with separately. [7]

DATABASE FORENSICS: Database forensics is a subset of digital forensics that involves applying investigative techniques to database contents and metadata while following the standard forensic methodology. Cached data may also exist in a server's RAM, necessitating the use of live analytic tools. The timestamps that apply to the update time of a row in a relational table may be inspected and evaluated for correctness in order to validate the actions of a database user during a forensic analysis of a database. A forensic examination, on the other hand, could focus on discovering transactions within a database system or application that reveal proof of wrongdoing, such as fraud.

DIGITAL MUSIC DEVICE: The digital music device has become a technology that should be of interest to the cyber forensic community due to its large storage capacity and personal digital assistant (PDA) features. As a result of the digital music revolution, the digital music player has become a common household item. It will only be a matter of time before they follow in their footsteps into the criminal realm. This process has already started. Some of the hard drive-based devices can hold up to 60GB of data. With so much music storage, developers have expanded to include functionality such as a calendar and contact book (Apple iPod — Music and more). These devices are essentially portable hard drives that can hold files other than music, such as documents or photographs. Using the capabilities of a digital music device, an employee might steal important information. These types of devices could be used by suspects to keep crucial evidence. It must be assessed whether current cyber forensic science frameworks are suitable for digital music device forensics and to what degree current guidelines may be implemented.

SCANNER FORENSICS: Acquisition devices such as digital cameras and scanners are used to create a major amount of the digital image data available today. Scanners are employed to capture hardcopy art in more controlled circumstances, while cameras enable

[7] 'What is Cyber Forensics?' (Intellipaat Blog) https://intellipaat.com/blog/what-is-cyber-forensics/ accessed 5 June 2025.

for digital replication of natural scenes. A non-intrusive scanner model identification, which can be further expanded to validate scanned images, is required for forensic purposes. [8]

OBJECTIVE

Human expert witnesses are important because courts will not recognise software tools such as Encase, Pascovia, or Ethereal as expert witnesses. Cyber forensics is becoming a source of investigation because human expert witnesses are important, as courts will not recognise software tools such as Encase, Pasco, or Ethereal as expert witnesses. Many professionals, including the military, private sector and business, academia, and law, benefit from cyber forensics. Data protection, data collecting, imaging, extraction, interrogation, normalisation, analysis, and reporting are just a few of the requirements in these fields. It is critical for all professionals working in the burgeoning field of cyber forensics to have a working and functional lexicon of terminology, such as bookmarks, cookies, and web hits that is used consistently across the profession and industry.

The area of cyber forensics has become a prominent field of research because:

- Forensics systems enable administrators to diagnose mistakes, and cyber forensics has become a popular subject of study.
- In order to prevent cybercrime, intrusion detection systems are required.
- Change detection is achievable with proactive forensics.
- To look into complaints of digital misbehaviour.
- Conducting a root cause analysis.

CURRENT AND FUTURE NEEDS

Criminals use technology extensively to perpetrate both traditional and cybercrimes. Cyber terrorism has evolved into a global threat. Economic crimes conducted through the use of computers, the internet, mobile phones, and other computing gadgets are also on the rise. As a result, both traditional and cybercrime are on the rise; nevertheless, the conviction rate in both cases is lower, and the obvious explanation is the failure of the investigation and

[8] 'Understanding Digital Forensics: Process, Techniques and Tools' (BlueVoyant) https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools accessed 5 June 2025.

prosecution authorities to present appropriate evidence in court. It demonstrates that law enforcement agencies are unfamiliar with the use of cyber forensic techniques in criminal investigations. There is also a lack of communication between cyber forensic tool research organisations, forensic laboratories, investigation agencies, and prosecution agencies. As a result, interdisciplinary research is required to close the gap since failure to obtain a satisfactory conviction rate may have a cascade effect, resulting in societal chaos and a threat to our lives, liberties, and property. The expanding use of technology in our lives multiplies the likelihood of increased criminality in equal, if not greater, amounts. [9]

CONCLUSION

In the present trend, cyber forensics is a developing field. This paper provides an overview of the area of cyber forensics. The procedure for assessing cyber forensics differs from that of traditional forensics. We covered numerous computer forensics definitions and phases of cyber forensics and forensics methodology in this research. The several steps of cyber forensics have been described, and each phase has been investigated with its own tools. It is still evolving and will continue to be a hot topic for as long as people are interested in it. Data security can be jeopardised in a number of ways. In the end, we demonstrate in this new era of cyber forensics, current research trends. As a result, a review of the present legislative framework governing the use and admissibility of cyber forensics in criminal investigations and trials is required. Various methods and approaches utilised in disc and device forensics should be examined for this aim. These tools and approaches can be improved to make criminal investigations and trials more effective. It is also necessary to do a legal study of the provisions of legislation under which these Cyber Forensic technologies can be used by law enforcement agencies and courts. The current relationship between cyber forensics and law is one of new acquaintances that needs to be developed and brought to the level of a married couple.

[9] ‘Digital Forensics’ (Intellipaat Blog) https://intellipaat.com/blog/digital-forensics/ accessed 5 June 2025.

REFERENCES

[1] Nishesh Sharma, 'Cyber Forensics in India – A Legal perspective', Universal Law Publishing

[2] Vicky Nanjappa, 'Cyber Crime – 1600 arrested, only 7 convicted', Rediff Business News. [3] Asheeta Ragidi, 'With Only 250 convictions, India's cybercrime conviction rate remains abysmally low', Nov. 22, 2016.

[4] Kiran Kumar Akate Patil, 'Hurdles in Cyber Forensic Investigation in India', IOSR Journal of Computer Engineering

[5] Peter D. Keisler, Attorney General, 'Investigative Uses of Technology: Devices, Tools and Techniques', US Dept. of Justice, Office of Justice Programs, Washington D.C.

[6] Cameron S. D. Brown1, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice' Cameron S. D. Brown, Australian National University, Australia, International Journal of Cyber Criminology Vol 9 Issue 1 January – June 2015

[7] Waleed Halboob, Ramlan Mahmod Nur IzuraUdzirMohd TaufikAbdullah, 'Privacy policies for Computer Forenics', Computer Fraud & Security, Computer Fraud and Security, Elsevier, Vol. 2015, Issue 8, August 2015, Pages 9-13

[8] Dhwaniket Ramesh Kamble, Nilakshi Jain, Swati Deshpande, 'Cybercrimes Solutions using Digital Forensic Tools', I.J. Wireless and Microwave Technologies, 2015, 6, 11-18 Published Online November 2015 in MECS(http://www.mecs-press.net)

[9] Reza Montasari, Pekka Peltola, David Evans, 'Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations. [10] Europol News Item, 'The Relentless Growth of Cybercrime', 27 September 20