Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 03, Issue 02

DOI: 10.46523/jarssc.03.02.09
Multidisciplinary, Open Access

Emerging Paradigms of Cyber Forensic: An Analysis

Dr. S. Nuzhat Husain

Asst. Prof., Faculty of Law, Shia P.G. College, Lucknow

Dr. Ajai Veer

Asst. Prof., Faculty of Law, Shia P.G. College, Lucknow

INTRODUCTION

The emerging trends in computer crimes have given birth to a new branch of forensic science known as computer forensics. This branch of forensic science uses the tools of computer security and tools of disaster recovery with the aim of submitting the evidence generated for the scrutiny of the judiciary. The electronic crime scene that possesses digital and electronic evidence creates new challenges for the investigator. There exists uniqueness to this new environment not only because the evidence may be difficult to detect but also because of how its evidentiary value may be hidden through steganography and/or encryption. Furthermore, there is a degree of anonymity in which perpetrators can hide their true identity in the forging of certain criminal acts and endeavors. Therefore, the rapid technological advancements occurring in the society through the digitalization of data and information are presenting new challenges to investigators. This electronic evidence is both difficult to detect and quite fragile; therefore, the latent nature of electronic evidence requires very skilled investigators.[1]

Computer forensics is in the nascent stage and is different from the traditional branch of forensics science. Computer forensic is important in today's world because as the science of computer forensics has been evolving over the years, malicious users and hackers have become smarter and cleverer with their techniques to compromise computer system, steal money and confidential even national security information.[2] Forensic science is a core component for

[1] Thomas A. Johnson, "Forensic Computer Crime Investigation", Pub. Taylor& Francis, p.5.
[2] J. Jitendra N. Bhatt, " A Profile of Forensics Science in Juristic Journey", (2003) 8 SCC25

Received: 16.07.2020 **Accepted:** 18.08.2020 **Published**: 19.08.2020

This work is licensed and distributed under the terms of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any Medium, provided the original work is properly cited.

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 03, Issue 02
DOI: 10.46523/jarssc.03.02.09
Multidisciplinary, Open Access

providing principles and techniques that jubilate the investigation and prosecution of criminal offences. Generally speaking, forensic science is the application of science to law- any scientific principle or technique that can be applied to identifying, recovering, reconstructing or analyzing evidence during a criminal investigation is part of forensic science.[3]

Computer forensics deals with the preservation, identification, extraction and documentation of computer evidence. The field is relatively new to the private sector, but it has been the main stay of technology related investigation and intelligence gathering in law enforcement and military agencies since mid of the year 1980. Like any other forensics science. Computer forensic involves the use of sophisticated technology tools and procedure.[4]

Computer Forensics

Computer forensics also referred as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery computer analysis and computer examination, is the process of methodically examining computer medias (hard disk diskettes, tapes etc.) for evidence. A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user. In other words computer forensic is the collection preservation analysis and presentation of computer related evidence. Far more information is retained on a computer than most people realize. It is also more difficult to completely remove information than is generally thought for these reason and many more. Computer forensics often find evidence of or even complete recover lost or deleted information even in the information was intentionally deleted. [5]

The term computer forensics was first coined by International Association of Computer Specialists (IACIS) during first training session at Oregon in 1991. Computer forensics is that branch of forensic science, which is harnessed to identity, locate, preserve and extract digital information for a computer system to produce clinching evidence of a crime in the courts of law

[3] Dr. R.K. Tewari P.K. Shastry, "Computer Crime and Computer Forensics", Select Pub., p.11.
[4] Ibid.

Received: 16.07.2020 **Accepted:** 18.08.2020 **Published**: 19.08.2020

This work is licensed and distributed under the terms of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any Medium, provided the original work is properly cited.

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 03, Issue 02
DOI: 10.46523/jarssc.03.02.09
Multidisciplinary, Open Access

and connect the computer crime with the criminal. There has not been a consensus in the definition of the term computer forensics. However, it can be defined as that branch of forensic science, where in the computer investigation and analysis techniques are applied to determine potential legal evidence in a computer environment. [6]

Forensics science pertaining to computer could be further subdivided in to three branches

i) Computer forensics.

ii) Cyber forensics.

iii) Software forensics.

Computer Forensics

Computer forensics deals with gathering evidence from computer media seized at the crime scene by extracting hidden or deleted information from the computer disk. The computer forensics process includes making storage media, recovery deleted files searching slake and free space and preserving the colleted information for preserving in the courts of law with appointee interpretation and conclusion.[4]

Cyber Forensics

Cyber forensic sometimes also called as network forensics, is a technically more challenging activity. It deals with forensic analysis of digitally evidence that is distributed across a large computer network. This evidence is often transient in nature and is not preserved with in the permanent storage media. Network forensics primarily deals with the analysis of computer network intrusion evidence for which the currently available commercial tools are inadequate.[5] Cyber forensics is a branch of computer science that focuses on developing evidence pertaining to digital files for use in civil or criminal court proceedings. Forensic evidence would relate to a computer document, email, text, digital photograph, software program, or other digital record which may be at issue in a legal case.

[4] Dr. R.K. Tewari P.K. Shastry, "Computer Crime and Computer Forensics", Select Pub., p.212
[5] Ibid.

Received: 16.07.2020 **Accepted:** 18.08.2020 **Published**: 19.08.2020

This work is licensed and distributed under the terms of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any Medium, provided the original work is properly cited.

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 03, Issue 02
DOI: 10.46523/jarssc.03.02.09
Multidisciplinary, Open Access

The intrusion analysis includes examination of intrusion detection system, logs, firewalls logs, audit trails and network management information. Cyber forensic adds inspection of transient and other frequently overlooked elements such as contents or state of memory register, basic inputs/out puts system input/output buffers, signal receive buffers, front side and back side system each, drives and video buffers etc. Cyber forensic includes examination of data related to both the trans and post cyber attack period. Key objectives of cyber forensic includes rapid discovery of evidence estimate the potential impact of the malicious activity on the victim and assessment of intent and identity.[6]

Software Forensics

Software forensics is the science that deals with the author of the malicious code. This is the most arcane area of computer forensics and currently it is at the critical stage of development. The key to identity the author of a suspect code is selection of appropriate body of code and identification of appropriate features for comparison.[7]

Investigation of Computer/ Cyber Crimes

The world community as a whole is increasingly being dependent upon information technology in managing all its affairs in a more speedy and efficacious way has also brought in increased danger from activities of criminals and perverted persons. An analysis of the criminogenic factors shows that modern computer and communication networks have specific characteristics which are highly useful for perpetuators but which imply difficulties for potential victims and for law enforcement agencies[3]. Traditional nature of investigation and evidence collection are often useless in investigation of cyber crimes. It is transnational nature in crime. The primary function of the criminal investigator is to gather information, determination of authenticity of information, identify and locate perpetrator of the crime and provide evidence of his guilt. Clause (3) of section 80 IT Act clearly states that the provisions of Code of Criminal

6 Supra note, 6.
7 Supra note,6.

Received: 16.07.2020 **Accepted:** 18.08.2020 **Published**: 19.08.2020

This work is licensed and distributed under the terms of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any Medium, provided the original work is properly cited.

Journal of Advance Research in Science and Social Science (JARSSC) **ISSN:** 2582-2004
Official Publication of Indian Mental Health & Research Centre Volume 03, Issue 02
DOI: 10.46523/jarssc.03.02.09
Multidisciplinary, Open Access

Procedure 1973 shall subject to the provisions of this section apply so far as may be in relation to any entry, search, or arrest is made under this sections .

CONCLUSION

Capacity of human mind is immeasurable. It is not possible to eliminate cyber crime from the cyber space. It is quite possible to check them. History is the witness that no legislation has ever succeeded in totality eliminating crime from the globe. The only possible step is to make people aware of their rights of duties and further making the application of the laws more stringent to check crime. Undoubtedly the Information Technology Act, 2000 is a historical step in the cyber world with reference to India but at the same time it could not be concluded that it is complete code for regulating the cyber crimes in cyber space. The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 the many species of cyber crimes have been codified but still there are the category of crimes which are not in the ambit of the enactment. Further there are cyber crimes which are traditional but are committed in the cyber world, are still dealt under the Penal Code. Merely by making amendment in the Penal Code by inserting some words in the definition of the crimes so as to make them applicable as cyber crime have not suffice the purpose. In fact there is need to bring changes in the Information Technology Act, 2000 and to include the unattended species of cyber crime within the purview of the enactment so as to make it more effective to combat cyber crime.

Received: 16.07.2020 **Accepted:** 18.08.2020 **Published**: 19.08.2020

This work is licensed and distributed under the terms of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any Medium, provided the original work is properly cited.