Ilkogretim Online - Elementary Education Online, 2020; Vol 19 (Issue 4): pp. 5030-5037
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2020.04.764911

Role Of Digital Evidence And Cyber Forensic In Criminal Justice System

Prof. Mahesh Koolwal, Dean & Professor, Faculty of Law JECRC University.

Ms. Bhanu Gangwal, Ph.D. Scholar, JECRC University, Jaipur**.** bhanugangwal9328@gmail.com

Abstract

In today's globalized world, computers are frequently used for committing crime, and, thanks to the burgeoning science of digital evidence, and law enforcement now uses computers to fight crime. Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card. Cyber Forensic is the process through which evidence has been gathered and processed for the proceedings in the court of law. However, digital evidence is now used to prosecute all types of crimes, not just electronic crime. In an effort to fight electronic crime and to collect relevant digital evidence for all crimes, law enforcement agencies are incorporating the collection and analysis of digital evidence, also known as computer forensics. However, Law enforcement agencies are challenged by the need to train officers to collect digital evidence and keep up with rapidly evolving technologies such as computer operating systems. The research paper deals with the problems regarding the collection of electronic evidence and their role in the court of law.

Introduction

While digital evidence exploitation may be a relatively new tool forenforcement investigations,enforcement relies extensively ondigital evidence for important information about both victimsand suspects. Due to the potential quantity of digital evidenceavailable, cases where such evidence is lacking are harderto develop leads and solve.

Section 65-B of the Evidence Act deals with admissibility of electronic records as digital evidence in the court of law.The computer holding the primary evidence does not got to be produced in court. A printout of the record or a copy on a CDROM, hard disk, floppy, etc. can be produced in the court. However, some conditions required to meet and a certificate needs to be provided.[1]

Law enforcement agencies face a novel challenge in handling cyber- crimes. Criminal acts are being committed and therefore the evidence of those activities is recorded in electronic form. Besides, crimes are being committed in cyberspace. Evidence in these crimes is almost always recorded in digital fashion. It is important that computer security professionals remember of a number of wants of the legal system and understand the developing field of computer forensics.[2]

The reality of the information age is that it has a big impact on the legal establishment. One major area in which this is being felt is that of the **acquisition, authentication, evaluation and legal admissibility of information** stored on magnetic and other media. This information

[1]Rohas Nagpal, Cyber Crime & Digital Evidence-Indian Perspective (Asian School of Cyber Laws, 2008).

[2]H.C. Catherine, Organizing for Computer Crime Investigation and Prosecution (National Institute of Justice, Washington DC 1989).

isoftenmentioned as digital evidence.[3] Computer forensics is that the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law.[4]

In the paper-based world, law assumes a process which is mutually understood and observed by all the parties. Almost without thinking, a four-part process takes place, involving acquisition, identification, evaluation and admission. When we attempt to apply this process to digital evidence, we see that we have a novel set of problems.

Digital evidence, by its very nature is imperceptible to the eye. Therefore, the evidence must be developed using tools aside from the human eye. It is only logical that the method utilized in the case of digital evidence mimic the method that is used for paper evidence. Because each step requires the utilization of tools or knowledge, the method must be documented, reliable and repeatable. The process itself must be understandable to the court.

Digital Evidence

Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device. This evidence can be acquired by when electronic devices are seized and secured for examination.

Data obtained online and/or extracted from digital devices can provide a wealth of information about users and events. For instance, gaming consoles, which operate like personal computers, store personal information about users of the devices (e.g., names and email addresses), financial information (e.g., credit card data), Internet browsing history (e.g., websites visited), images, and videos, among other data.

Cyber Forensic

The term forensics, in its literal sense, stands for an established scientific process to collect, analyze, and present evidence collected from an investigation.
Cyber forensics are used for identifying, preserving, analyzing and recovering data from computers and various digital media storage.

The data can be from any digital asset or data storing entity, which includes a computer system, mobile device, cloud service, and so on.

Criminal Justice System

Criminal Justice refers to the agencies of government charged with enforcing law, adjudicating crime, and correcting criminal conduct. The criminal justice system is essentially an instrument of social control: society considers some behaviours so dangerous and destructive that it either strictly controls their occurrence or outlaws them outright. It is the job of the agencies of justice to prevent these behaviours by apprehending and punishing transgressors or deterring their future occurrence.

The main objectives of the criminal justice system can be categorized as follows:

1. To prevent the occurrence of crime.
2. To punish the transgressors and the criminals.

[3]George Garner, â€oeForensic Acquisition Utilitiesâ€• http://users.erols.com/ gmgarner/forensics.
[4] Basic Considerations in Investigating and Proving Computer-Related Federal Crimes (United States Deptt. of Justice,U.S. Govt. Printing Office, Washington DC 1988).

3. To rehabilitate the transgressors and the criminals.
4. To compensate the victims as far as possible.
5. To maintain law and order in the society.
6. To deter the offenders from committing any criminal act in the future.

DIGITAL EVIDENCE

Many departments are behind the curve in handling digital evidence. There are a number of explanations for this, including the rapid changes and proliferation of digital devices, budgetary limitations, and lack of proper training opportunities.

Performing digital forensics can be an expensive proposition involving licenses, equipment and significant personnel costs. Demonstrating cost effective return on investment is crucial to securing command staff buy in. Funding these efforts can involve a complicated mix of local, state and federal budgets, and this can be particularly challenging for smaller departments. Regional models and other forms of collaboration can help, provided officers know where to turn for help.

Advanced digital evidence training is not yet part of the core curriculum for police academies, yet officers of all levels of experience may have contact with digital evidence that is sufficient to affect the resolution of the case.

Departments face large digital evidence backlogs, limited equipment, and potential turnover of examiners. Contributing to the backlog is the lack of personnel trained in digital evidence extraction. A growing backlog prevents training opportunities since classes would take examiners out of the workplace, and a backlog can undermine requests to replace inadequate, antiquated, or under-funded technology and licenses due to budget constraints of units perceived to be performing slowly.

What is Digital Evidence?

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, among other places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud.

Digital evidence is "information and data of value to an investigation that is stored on, received, or transmitted by an electronic device" (National Institute of Justice [NIJ], 2008).[5]

Digital evidence:-

- Is latent (hidden), like fingerprints or DNA evidence
- Crosses jurisdictional borders quickly and easily
- Can be altered, damaged or destroyed with little effort
- Can be time sensitive

Sources of Digital evidence:-

- Internet- based,
- Stand-alone computers or devices, and
- Mobile- devices

[5]Alvarez, L. (2011, July 18). Software designer reports error in Anthony trial. *New York Times*, p. A14.

When and Why Digital Evidence is Used?

Digital evidence may come into play in:-

- Any serious criminal investigation such as murder, rape, stalking, car-jacking, burglary, child abuse or exploitation, counterfeiting or extortion, gambling or piracy, property crimes and terrorism.
- Pre and Post crime information.
- Fully Digitalized crimes such as Computer hacking, economic fraud or identity theft.

Evidence that May be Gathered Digitally

- Computer documents
- Emails
- Texts and instant messages
- Transactions
- Images
- Internet Histories
- Mobile Locations

Who Conducts the Analysis?

- Certified Digital Media Examiners are the investigators.

How Digital Devices are Collected?

- On the scene
- Seizing Mobile Devices
- Seizing Stand Alone Computers and Equipment

Limitations Regarding the Digital Device Evidence

- Encryption and proprietary systems that require decoding before data can even be accessed
- Both, Legal and Technical limitations (Critical Law Enforcement Issue)
- Data ownership
- Wiretapping laws
- Privacy laws (Internet and personal device privacy laws)

CYBER FORENSIC

Cyber Forensics is the application of investigation and analysis of techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of cyber forensic is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.The term forensics, in its literal sense, stands for an established scientific process to collect, analyze, and present evidence collected from an investigation.

Cyber forensics are used for identifying, preserving, analyzing and recovering data from computers and various digital media storage.

The data can be from any digital asset or data storing entity, which includes a computer system, mobile device, cloud service, and so on.

Objectives:-

- To gather facts, to know what occurred and, if possible, to know how and when it occurred.
- To collect data in a manner that is acceptable for a court.

Phases of Cyber/ Digital Forensic[6]

- **Policy and procedure development-**As the primary aim of any digital forensics investigation, is to allow others to follow the same procedures and steps and still end with same result and conclusions, considerable effort must be spent on developing policies and standard operating procedures (SOP) in how to deal with each step and phase of the investigation.
- **Evidence Assessment-**All sources of possible digital evidence should be thoroughly assessed with respect to the scope of the case. This will help establish the size of the investigation and determine the next steps.Special attention should be given to reviewing the scope of search warrant(s) and other legal authorisations to establish the nature of hardware and software to be seized, other potential evidence sought together with the circumstances surrounding the acquisition of the evidence to be examined.
- **Evidence Acquisition-**Digital evidence is fragile and can be easily altered, damaged, or destroyed by improper handling or examination. Even the act of opening files can alter timestamp information destroying information on when the file was last accessed. So special precautions are needed to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.
- **Evidence Examination-**The same general forensic principles apply when examining digital evidence as they do to any other crime scene. However, different types of cases and media may require different methods of examination. Only trained personnel should conduct an examination of digital evidence.

It is important to make a distinction:-

- **Extraction** refers to the recovery of data from whatever media the data is stored on.
- **Analysis** refers to the interpretation of the recovered data and placement of it in a logical and useful format, answering such questions as how did it get there, where did it come from, and what does it mean?

Separating the forensic examination this helps the examiner in developing procedures and structuring the examination and presentation of the digital evidence.

Step 1 Preparation

Prepare working directory/directories on separate media to which evidentiary files and data can be recovered and/or extracted. These should be checked to make sure they

[6]http://cybersecurity.jhigh.co.uk/digitalForensics/phasesOfInvestigation.html

are **'forensically clean'** so that investigators can be sure any evidence belongs to case being investigated, rather than leftover from other cases.

Step 2 Extraction

This is the actual process of extracting the data from digital devices. There are two different types of extraction, physical and logical.

- **Physical Extraction-**Data is extracted at the physical level without regard to any file systems present on the drive. Essentially, any image is made and then subjected to the following methods: keyword searching, file carving, and extraction of the partition table and unused space on the physical drive.

- **Logical Extraction-** Data is from the drive is based on the file system(s) present on the drive. This will involve an examination of active files, recovering deleted files, looking at file slack (i..e unusual space between files) and unallocated file space: May contain remnants of deleted files not found during the recovery process.

Step 3 Analysis

Analysis is the process of interpreting the extracted data to determine their significance to the case. Various analytical methods exist, examples of which include :-

- Timeframe,
- Data hiding,
- Application and file,
- Ownership and possession.

Step 4 Conclusion

Single pieces of evidence from one source will probably be insufficient to reach a definite conclusion. Conclusions have to be based on all evidence in the round, including the associations between each part of the evidence.

- **Reporting-**The investigator must document completely and accurately their each step in their investigation from the start to the end. The aim is to allow others following the steps outlined in the documentation to reproduce the investigation and reach the same conclusions.

Importance of Cyber Forensic

- Prevents hackers and hijackers
- Prevent Viruses
- Recover deleted Information
- Identifying areas of Weaknesses and Vulnerabilities
- Improves the Cyber Security

Importance of Digital Evidence and Cyber Forensic in Criminal Justice System

- Proactive investigation now considers how digital evidence might be exploited for non-computer crimes as well.
- Many computer crimes that get reported may or may not exceed thresholds for investigation and/or prosecution. As victims of such crimes increasingly turn to law enforcement for assistance, adequate processes for responding need to be in place not

only to assist the victim, but also to capture digital evidence and information that might otherwise be lost.

- In many cases, considerable jurisdictional challenges exist when the digital evidence required for an investigation does not exist on a physical device at the crime scene, but rather on a server many countries, states, or countries away.
- Issues relating to cloud-based information and legal challenges associated with the proper scope for searching portable electronic "microcomputers" may shape the future of digital evidence processing.
- Ultimately, abiding by the scientific method will help forensic examiners to avoid egregious errors. Carefully exploring potential sources of error, hypothesis testing and qualifying conclusions with appropriate uncertainty will protect forensic examiners from overstating or misinterpreting the facts.

CONCLUSION

1. Maintaining the integrity of digital evidence throughout the process of examination presents different problems from those encountered when handling traditional physical or documentary evidence.
2. Mistakes in interpretation and analysis can be reduced by rigorous application of the scientific method.
3. Digital evidence should trigger new rules of criminal procedure because computer-related crimes feature new facts that will demand new law.
4. The law of criminal procedure has evolved to regulate the mechanisms common to the investigation of physical crimes, namely, the collection of physical evidence and eyewitness testimony.
5. Existing law is naturally tailored to law enforcement needs and privacy threats they raise. The new ways of collecting evidence are so different that the rules developed for the old investigations often no longer make sense for the new.

REFERENCES

1. The Role and Impact of Forensic Evidence in the Criminal Justice Process by Joseph Peterson, Ira Sommers, Deborah Baskin, and Donald Johnson,2010 Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory (Purdue University),2016
2. Renuka Sane(2019), "The way forward for personal insolvency in the Indian Insolvency and Bankruptcy Code", No. 251, National Institute of Public Finance and Policy, January-2019
3. R Kaur, A Kashyap, D Kumar," Computer Vision Detection Of Submerged Object Through Machine Learning", Elementary Education Online, Vol:20,Issue:5, Pg: 5013-5019, 2021/5, doi:10.17051/ilkonline.2021.05.560.
4. Forensic Examination of Digital Evidence: A Guide for Law Enforcement
5. Halil Ibrahim Bulbul, Yavuzcan, Mesut Ozel, 'Digital Forensics: An Analytical Crime Scene Procedure Model', Forensic Science International, Elsevier, 2013.
6. Justice Singh, Yatindra (2nd Ed.), Cyber Laws, Universal Law Publishing Co. Pvt. Ltd.
7. R Kaur A Jain, S Kumar," Optimization classification of sunflower recognition through machine learning", Materials Today Proceedings, Volume 46, Part 8, Science Direct, Elsevier, 26 May 2021, https://doi.org/10.1016/j.matpr.2021.05.182.
8. Kiran Kumar Akate Patil, 'Hurdles in Cyber Forensic Investigation in India', IOSR Journal of Computer Engineering
9. M. Al. Fahdi, Clarke, Furnell, 'A suspect-oriented intelligent and automated computer forensic analysis', Digital Investigation, Elsevier, 2016.

10. M.M. Kohn, M.M. Eloff, J.H.P Eloff, 'Integrated Digital Forensic Process Model', Computers and Security, Elsevier 2013.
11. A Tulchhia, R Kaur, A Kashyap," The Degradation Technique of Randomization through Convolution Neural Network for Submerged Object", International Journal of Advanced Science and Technology, Volume:29, Issue: 5s, Pages:1341-1347, May 2020, sersc.org/journals/index.php/IJAST/article/view/8163
12. Justice Singh, Yatindra (2nd Ed.), Cyber Laws, Universal Law Publishing Co. Pvt. Ltd
13. Dr. Rupinder Katoch (2017), Insolvency and Bankruptcy Code,2016:Features,Mechanism and Challenges in implementation, International Journal of Management, IT & Engineering Vol. 7 Issue 9, September 2017, ISSN: 2249-0558, pp 71-89
14. Rakesh Dubbudu, 'Conviction Rate of Sec 498-A cases is among the lowest of all IPC Crimes', Report 'Crime in India', National Crime Records Bureau, July 2017
15. Supplemental Requirements for the Accreditation of Forensic Science Testing
16. Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories, 2011 edition, ASCLD/LAB-International, 2010
17. Barbara Guttman; James R. Lyle; Richard Ayers, Ten Years of Computer Forensic Tool Testing, 8 Digital Evidence & Elec. Signature L. Rev. 139, 147 (2011).