FORENSIC COMPUTING MODELS: TECHNICAL OVERVIEW

Gulshan Shrivastava, Kavita Sharma, Akansha Dwivedi

Department of Information Technology,
Dronacharya College of Engineering, Gr. Noida, U.P., India
gulshanstv@gmail.com,
kavitasharma_06@yahoo.co.in,
akansha.dwivedi11@yahoo.com

ABSTRACT

In this paper, we deal with introducing a technique of digital forensics for reconstruction of events or evidences after the commitment of a crime through any of the digital devices. It shows a clear transparency between Computer Forensics and Digital Forensics and gives a brief description about the classification of Digital Forensics. It has also been described that how the emergences of various digital forensic models help digital forensic practitioners and examiners in doing digital forensics. Further, discussed Merits and Demerits of the required models and review of every major model.

KEYWORDS

Digital Forensics, Computer Forensics, Digital Forensic Model, Digital Forensic History, Digital Evidence.

1. INTRODUCTION

Today in the computers world along with the computers, its user is also increasing very rapidly. Now the time has come in which organization are strongly dependent on the computers and internet for taking their business to the crest. A large package of information is being sent or received at one click. The large numbers of computers are connected in a cob-web like network, which is necessary for dispatching and receiving information. Along with boom, these computers are also responsible for cyber frauds and cybercrimes (CFCC).the first computer crime was approximately 85% of 66 million U.S dollar was last by organizations due to digital related crime in 2007.The technique named "Digital Forensics" has been started from a basic level and extended up to level, that it has occupied an untouched and influence able place in almost every field related to the computers. Its birth is stated in 1970's almost forty years back. In the initiating days of digital forensics it was primarily used for data recovery and the technique was only performed by the computer professionals. This research emphasizes on a techniques through which the clues after crime can be constructed i.e. a uniform approach of digital forensic models

David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 207–216, 2012.
 DOI : 10.5121/csit.2012.2222

for digital forensic investigation. The research is about the postulates of the different digital forensic models and their limitation. The research will conclude to a new digital forensic model.

1.1 History and Previous Work

Mark Reith et al. concluded that "digital forensic is the use of scientifically derived and proven methods toward the identification, preservation, collection, validation, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the reconstruction of events". Digital forensics is a wide branch comprising of branch like computer forensics, digital forensics not only cover the evidences reconstructed after the crime committed by or through a stand-alone computers , the evidences reconstructed from any of digital sources can be interpreted by using digital forensics. Digital forensics investigation has three phases to go through.

Table 1 :(History Evolution of digital forensic) [2]

Year	History
1978	First computer crime in Florida which involved unauthorized modification and deletion of data on a computer system.
Prior 1980	Computer crimes were solved using existing laws. No federal laws for computer crimes.
1983	Canada – The first country to pass legislation dealing with computer crimes.
1984	United States passed Federal Computer Fraud & Abuse Act
1990	United Kingdom passed British Computer Misuse Act.
1992	Collier & Spaul wrote a paper 'A forensic methodology for countering computer crime.'
2002	Scientific Working Group on Digital Evidence (SWGDE) produced a paper 'Best practices for computer forensic'.
2005	Publication of an ISO standard (ISO 17025, General requirements) for the competence of testing & calibration laboratories.
2005 Onwards till now	Various dimensions related to computer crimes are being discussed.

1.2 Process of Digital Forensic Investigation

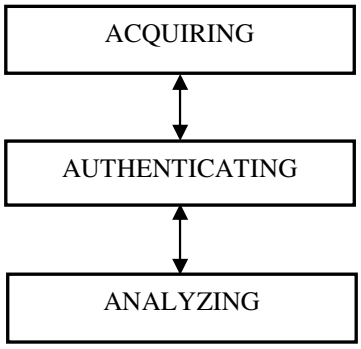

Figure 1 :(Process of Digital Forensic) [1]

1.2.1 Acquiring

It is the process of conquering the digital evidences carefully, so the integrity of evidence can be maintained.

1.2.2 Authenticating

The process of examining the validation of evidence, whether it is valid to use or not.

1.2.3 Analyzing

The close examination of data to sort out the case.

2. DIGITAL EVIDENCES AND IT'S CHARACTERISTICS

Digital evidence is defined as the clues which can be recovered from digital sources and helps in digital forensic investigation. Digital evidence is very delicate to deal with. If it is handed improperly, its integrity can be spoiled. Digital evidence is hidden evidence just like any biometric evidence [3].

2.1 Classification of Digital Forensics

It is stated that there are various types of digital forensics. Some of them are:-

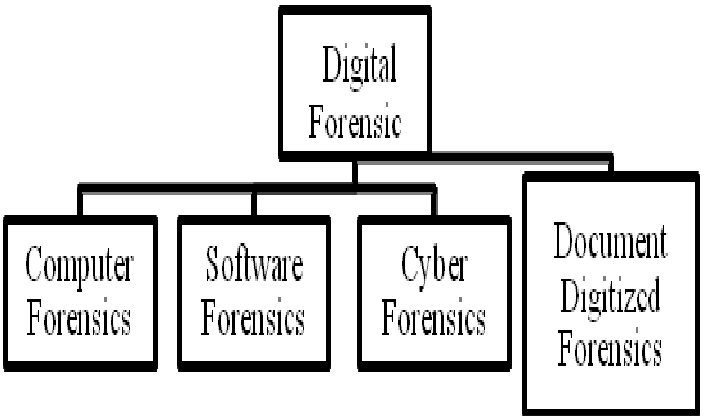

Figure 2 :(Types of Digital Forensics)

i. Computer Forensics

It has been defined that this branch of digital forensics deals with the reconstruction of evidences from the suspected computer which is found from the location of crime. It has also been called as 'media forensics.

ii. Software Forensics

It has been called as 'code analysis. In this branch it has been discussed about the identification of the developer of unauthorized code, or of any e-mail document.

iii. Cyber Forensics

It is also called as 'network forensics. This technique is used to identify, collect, examine the digital evidences reconstructed from various digital sources or to measure the amount of unauthorized activities meant to disrupt, corrupt the particular system.

iv. Document Digitized Forensics

It is being considered as upcoming branch of digital forensics to develop the procedures for detecting the decepted data and its solution. Usually frauds committed through printers and scanners will be resolved by this technique.

3. NEED OF DIGITAL FORENSIC MODEL

To reconstruct the digital evidences from digital sources a technique called digital forensics has been developed. The digital forensic models have been constructed so that step wise or ordered inspection procedure of digital evidences can be made through it. The models can provide digital evidence examiners or investigators with the detailed and transparent information's about particular aspect or phase to be considered during the process of digital forensic investigation.

4. EXISTING DIGITAL FORENSIC INVESTIGATION MODEL

Table 2 :(Existing digital forensics models)

Year	Model	Description
2001	The forensic process model proposed by Ashcroft the U.S National Institute of Justice(NIJ)	It serves as a guide for first responders. This guide is used by enforcement & other for protecting , recognition , can of digital evidence
2002	Abstract digital forensic model proposed by Reith , Carr & Gunsch	It is based on traditional strategy of forensic evidence collection.
2003	The integrated digital investigation process model (IDIP) proposed by Carrier and Spafford.	In this model digital investigative process is converted into physical investigation process.
2004	Extended model of cyber crime investigation proposed by Ciardhuain	It emphasizes on the management aspect.
2005	Case-relevance information investigation proposed by Ruibin, Yun & Gartner.	In this model computer intelligence will assist in investigation procedures. The degrees of case-relevance are defined.
2009	Digital forensic model based on Malaysian investigation process proposed by Perusal	The acquiring of static & dynamic data is included in this model.
2011	The systematic digital forensic investigation model (SRDHM) proposed by Ademu, Imafidon and Preston.	It helps forensic examiner & organization in a proper manner.

4.1 The Forensic Process Model [4]

This model was proposed by NIJ for electronic crime scene investigation. It comprises of four phases:

1. COLLECTION: in this process evidences are searches, felicitated and get collected.

2. EXAMINATION: it is done to make the evidences transparent & find the base of its origin.

3. ANALYSIS: the inspection of the outcome of the examination phase.

4. REPORTING: outlining the outcomes and conclusion of all the phases and information gathered.

Disadvantage: The analysis phase of this model is improperly defined and ambiguous [9].

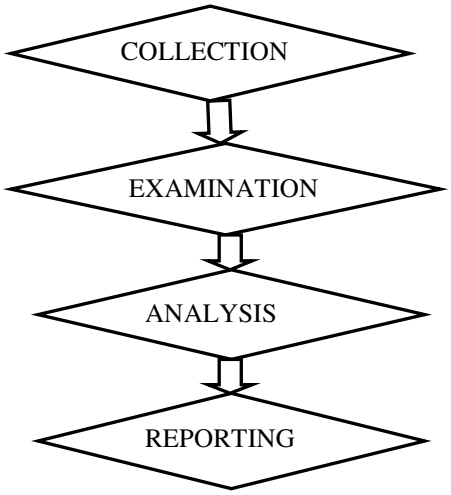

Figure 3 : (Forensic Process Model)

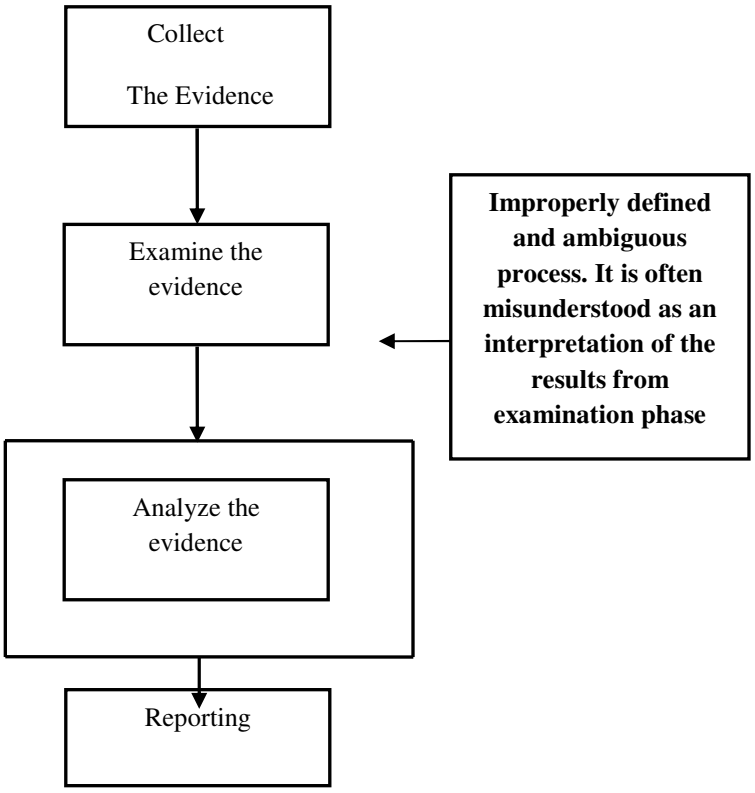

Figure 4 : (Disadvantage in Forensic Process Model)

4.2 The Abstract Digital Forensic Model [5]

This model comprises of nine components.

1. IDENTIFICATION: It helps in recognizing & identifying the type of the incident. It has a influence on other steps or phases of this model.

2. PREPARATION: The preparation of procedure, techniques, search warrants.

3. APPROACH STRATEGY: It is the formulation of procedures and approach to be used in the collection of evidences.

4. PRESERVATION: It deals with securing and preserving the evidences.

5. COLLECTION: The collection is done using the standardized procedures to record the physical scene.

6. EXAMINATION: It deals with searching evidences of the related suspect of the crime.

7. ANALYSIS: The inspection of importance of examined product.

8. PRESENTATION: The explanation of all the phases involved.

9. RETURNING EVIDENCE: Returning the digital sources back to the right owner.

Disadvantage: In this model third phase is to an extent a duplication of its second phase. This is because the preparation wile selecting tools directly depends on strategy selected.

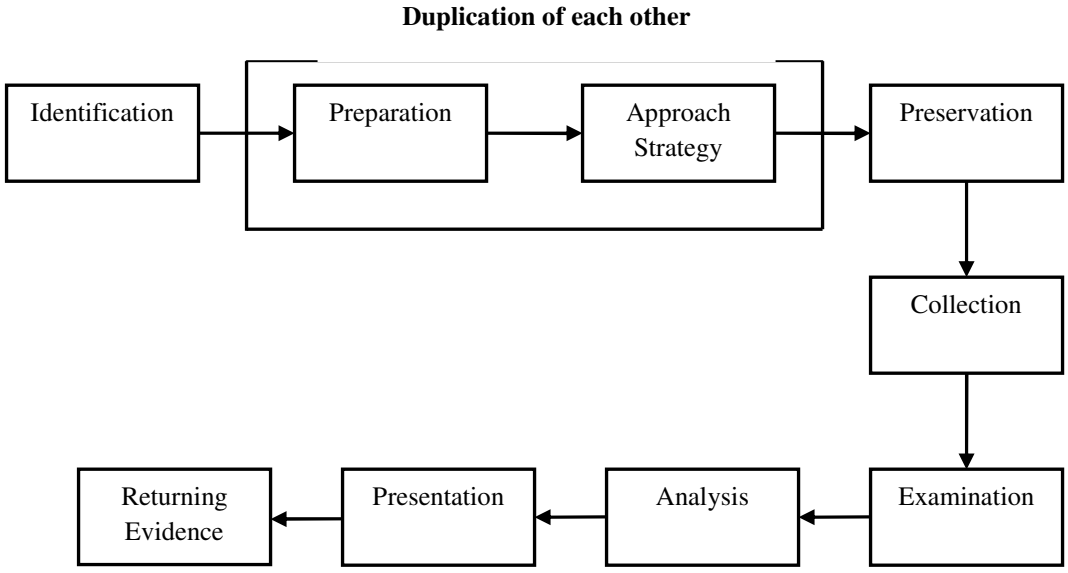

Figure 5 : (Disadvantage of the Abstract Digital Forensic Model)

4.3 The Integrated Digital Investigation Model (2003) [3]

The previous work has been reviewed and digital investigation process is transformed into the physical investigation process. Brian Carrier and Eugene Spafford proposed model that manages the process into five groups.

1. READINESS PHASES: The goal of this phase is to ensure that the operations and infrastructure are able to fully support an investigation.

2. DEPLOYMENT PHASE: The motive of this phase is to provide a mechanism for an incident to be detected and confirmed.

3. PHYSICAL CRIME SCENE INVESTIGATION PHASE: The goal of this phase is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident.

4. DIGITAL CRIME SCENE INVESTIGATION PHASE: The goal is to collect and analyze the digital evidence that was obtained from the physical investigation phase and through any other future means. It includes same process as physical evidence phase; however the main focus is to collect digital evidence.

5. REVIEW PHASE: This includes a review of the whole investigation and identifies areas of improvement.

Disadvantage: The deployment phase of this model deals with the confirmation of the incidents. But in practice it is impossible to confirm the digital or computer crime before proper investigation.

4.4 Extended Model Of Cyber Crime Investigation (2004)[6]

It was stated that the previous models were concentrated only to the processing of cyber crime evidences in cyber crime investigation. This model emphasizes on the management aspect of digital evidences.

4.5 Case – Relevance Information Investigation(2004)[7]

The requirement of computer intelligence technology has been explained in this model it emerges as an assistant to the investigation procedures it is used to describe the degrees of case-applicability and to distinguish between the forensics and the computer security.

4.6 Digital Forensic Model Based On Malaysian Investigation Process (2009)[8]

It was proposed by Perusal in 2009. It is defined that this model has been proved as an important phase to acquire static and dynamic data. This model emphasis more on delicate digital evidence.

4.7 The Systematic Digital Forensic Investigation Model (2011)[1]

This was proposed by Ademu, Imafidon and Preston. This model helps the forensics practitioners, examiners to set accurate procedures techniques in a proper manner.

5. CONCLUSIONS

In order to be revealed or accepted in the court, digital evidences must be precise and accurate and its integrity should not be spoiled by heedlessness. The process of digital forensics is to aid the digital forensic investigation and practitioners in reconstructing the evidences the association of digital forensics needs to form a guide line for the swift development of digital forensic procedure so that evidences can be easily elucidated, examined and processed.

ACKNOWLEDGEMENTS

We are grateful to Prof. M.P.S. Bhatia (Dean of Student Welfare, Netaji Subhas Institute of Technology), Dr. Vishal Bhatnagar (Associate Professor, Ambedkar Institute of Communication Technologies and Research), & Mr. Parbal Partab (Scientist, DRDO) for taking time to read carefully drafts of this paper and provide us with valuable comments.

The authors are also grateful for thoughtful comments from reviewers who improved the content of the paper. The authors would like to thank everyone, just everyone!

REFERENCES

[1] Inikpi O.Ademu, Dr. Chris.O.Imafidon, Dr.David S. Preston (2011)"A new approach of digital forensic model for digital forensic investigation" vol 2, no. 12, 2011.

[2] Kruse II, Warren and Jay, G. Heiser (2002) Computer Forensics: Incident Response Essentials.Addison-Wesley.

[3] Carrier, B.Spafford, H.(2006),getting physical with digital forensics process vol. 2(2)available online: http://www.cerias.purdue.Edu/ homes/carrier/forensics accessed on 20th September 2011.

[4] National institute of Justice.(July 2001) Electronic Crime Scene Investigation A guide for first responders http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

[5] Reith, M.Carr.c.Gunsch, G. (2002) an examination of digital forensic model. Department of electrical and computer engineering Air force institute of technology.Wright-Patterson.available (online): http://www.utica.edu/academic/institutes/escii/ijde/articles.cfm?action accessed on the 7th October 2011.

[6] Ciardhuain, S.(2004) an extended model of cyber-crime investigation Accessed on 20th October 2011 available (online): www.ijde.org/citeseerx.ist.psu.edu/view doc/download? doi=10.1.180.....Accessed on 11th august 2011

[7] Ruibin, G.Gaertner, M.(2005)case-relevance information investigation process : binding computer intelligence to the current computer forensics frame work. Vol. 4(1) available (on line): http://www.utica.edu/academic/institutes/ecii/publications/article/B4A6A102-A93D-85B195C575D5E35F3764.pdf Accessed 15th September 2011.

[8] Perumal,S.(2009) digital forensics model based on Malaysian investigation process vol. 9(8) available (on line): http://paper.ijcsns.org/o7_book/200908/20080805 pdf Accessed on 7th august 2011.

[9] Baryamureeba, V.Tushabe, F. (2004) The Enhanced digital investigation process (2004) Available (online):http//www.dfrws.org/2004/bios/day1/tushabeEIDIP.pdf Accessed on 15th June 2011.

Authors

Gulshan Shrivastava, working as Assistant Professor in Dronacharya College of Engineering, Greater Noida (U.P.). He has obtained a degree of M.Tech. (Information Security) from Ambedkar Institute of Communication Technology and Research, New Delhi and MBA (IT) from Punjab Technical University, Jalandhar, Punjab after completing B.E. (Computer Science Engineering) from Hindu College of Engineering, Sonipat, Haryana. He has rich experience in teaching the classes of Graduate and Post-Graduate in India and Abroad. He is a Sun Certified Java Programmer (SCJP 5.0). He has been continuously imparting corporate training to the experienced professionals of multinational IT giants in the area of Java Programming & Information Security. He has participated in many National & International Workshop and Technical Fest. He has contributed to numerous International journal & conference publications in various areas of Computer Science. He published more than 10 Research Paper in International Journals and Conferences. He has also written an International book Titled as "*Java Programming & Website Design"* (ISBN 81-87201-25-8), which is published by Suhavi Publication, India. He is also holding position in editor team of various International Journals and magazines of high repute. He is member of The Society of Digital Information and Wireless Communications (SDIWC), Internet Society, Institute of Nanotechnology, Life Member, International Association of Engineers (IAENG), Life Member, International Association of Computer Science and Information Technology (IACSIT), Computer Science Teachers Association (CSTA), International Association of Online Engineering (IAOE). His area of interest includes Java Programming, Website Designing, Data Mining, Information Security and Forensic Investigation.

Kavita Sharma, working as Assistant Professor in Dronacharya College of Engineering, Greater Noida (U.P.). She received the M.Tech. (Information Security) from Ambedkar Institute of Technology, New Delhi, India, Affiliated by G.G.S. Indraprastha University after completed her B.Tech. Degree in Information Technology from the I.M.S. Engineering College, Ghaziabad, India. She has published more than 9 research papers in International Journals and Conferences of high repute. She has also written an International book ISBN as "81-87201-25-8", which is published by Suhavi Publication, India. She is also holding position in editorial team of various International Journals and magazines of high repute. She is member of The Society of Digital Information and Wireless Communications (SDIWC), Internet Society, Life Member, International Association of Engineers (IAENG), Life Member, International Association of Computer Science and Information Technology (IACSIT), Computer Science Teachers Association (CSTA), International Association of Online Engineering (IAOE). She has actively participated in different faculty development programs. She has participated in different National & International Workshop. Her area of interest includes Digital Forensic Investigation, Data Structure and Algorithm, Web Mining, Programming Language, Cryptography and Data Security.

Akansha Dwivedi, pursuing Bachelor of Technology Degree in Information Technology from Dronacharya College of Engineering, Greater Noida, U.P. India, Affiliated by Gautam Buddh Technical University (GBTU). She has participated in different National Workshop. Her areas of interest include Computer Forensic Investigation, Ethical Hacking & Information Security etc.