ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2013

COMPARATIVE DIGITAL FORENSIC MODEL

Dr.DhananjayKalbande[1], Nilakshi Jain[2]

Head of Department, Dept. Of CSE, SPIT/ Mumbai University, Mumbai, Maharastra, India [1]

Assistant Professor, Dept. Of IT, SAKEC/ Mumbai University, Mumbai, Maharastra, India[2]

Abstract: The computer forensic is the about evidence finding from computer or services using its reliability and justification which can be proved in court or in management. To accomplish this task various digital forensic model has been introduced till now. The proposed model ,Comparative Digital Forensic Model (CDFM) provides the authenticate evidence using less efforts because it based on required output only. Initially all models has been reviewed and listed advantages and disadvantages of all finally the CDFM has been developed, using that model very initial user can also understand the basic concept of digital forensic model.

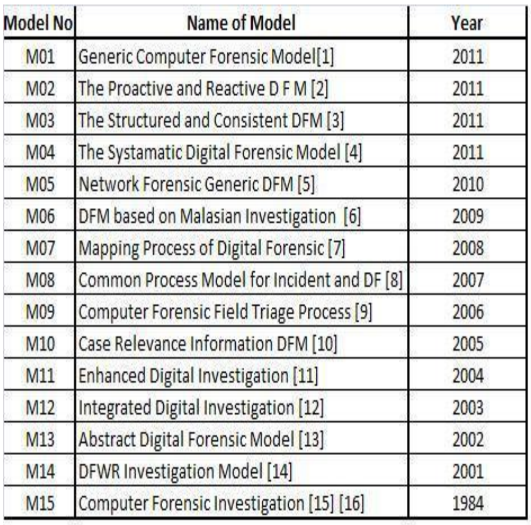
Keywords:Digital forensic, DFA, digitalevidences, Investigation model**.**

I. INTRODUCTION

Since 1984 when the initial digital forensic model has been introduced ,after that too many models has been described efficient methods to investigate a digital crime Scene[1].Now a days when crime takes place in form of digital devices it has been very crucial to identified the crime and justified the crime.

Although authors has been proposed very effective model or a framework to identify the crime level and digital evidence or digital data .It can be review that some models may be very reliable to take in practical approach and some may not be. At the very initial knowledge as a digital forensic investigator it has been experienced that it is so confusing to select the best model among them. Hence we have reviewed various latest digital forensic models, named given in TABLE 1,and then found that based on desired output we can summarized so many phases into some very effective and efficient phases .Using the comparison approach we have developed a Comparative Digital Forensic Model which is based on bottom up approach. Using desired output from each and every phase of reviewed models ,we have grouped the output and then identified the required phases to achieve those output.

Table 1:Digital Forensic Models



Model No	Name of Model	Year
M01	Generic Computer Forensic Model[1]	2011
M02	The Proactive and Reactive D F M [2]	2011
M03	The Structured and Consistent DFM [3]	2011
M04	The Systamatic Digital Forensic Model [4]	2011
M05	Network Forensic Generic DFM [5]	2010
M06	DFM based on Malasian Investigation [6]	2009
M07	Mapping Process of Digital Forensic [7]	2008
M08	Common Process Model for Incident and DF [8]	2007
M09	Computer Forensic Field Triage Process [9]	2006
M10	Case Relevance Information DFM [10]	2005
M11	Enhanced Digital Investigation [11]	2004
M12	Integrated Digital Investigation [12]	2003
M13	Abstract Digital Forensic Model [13]	2002
M14	DFWR Investigation Model [14]	2001
M15	Computer Forensic Investigation [15] [16]	1984

II. REQUIREMENT OF DIGITAL FORENSIC MODEL

As in the computer world growing with new technologies but it also gives facilitate the digital crime .So there should be some proper way to find out the digital crime .Digital Forensic models describe the systematic way to do so .Some basic requirement of digital forensic models are:

- It provide future security of further crime events for the same target.
- It ensures the identification for all malicious events that has been occurred and also determination of involved different parties.
- To justify the crime investigation .
- To improve the current prevention methodology so that crime rate can be decrease.
- To provide a better standards for companies and organization so that better security can be achieve.

III.COMPARATIVE DIGITAL FORENSIC MODEL

The Comparative Digital Forensic Model based on the comparison of previous Digital Forensic Models. We have reviewed various models as shown in table 1.Based on desired output required for different phases we have proposed a new model with five phases. The flow chart of desired output is given below :

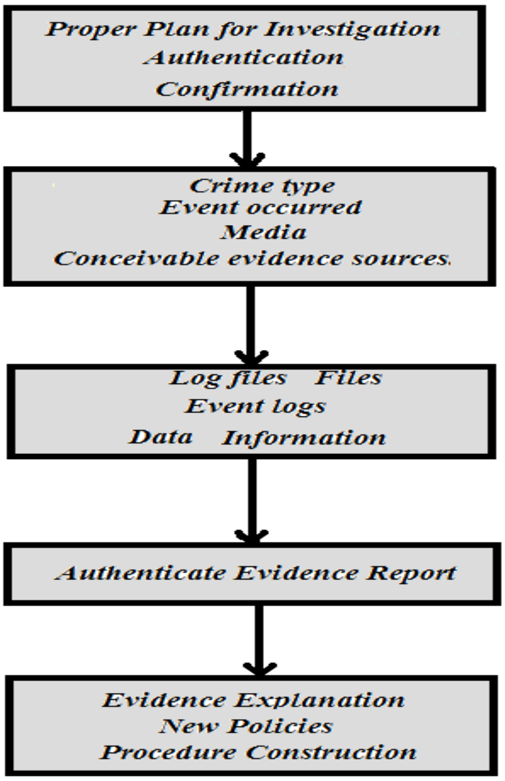


Fig. 1 : Desired Output from each phase

According to desired output we have construct therequired phases. The CDFM is having 5 phases as given in figure 2.Figure 2 describes the complete flow of the model like first phase Foundation which will establish a systematic plan for investigation , Secondly Accumulation & Conservation which will produce the crime type and level. The third phase is Inspection and Analysis which generate the authenticate evidence. Fourth phase is Presentation and

Documentation which will explain proof to justify the case. And finally the Justification and Disseminating the case which will generate the result. The next portion of paper describes the detail working of model.

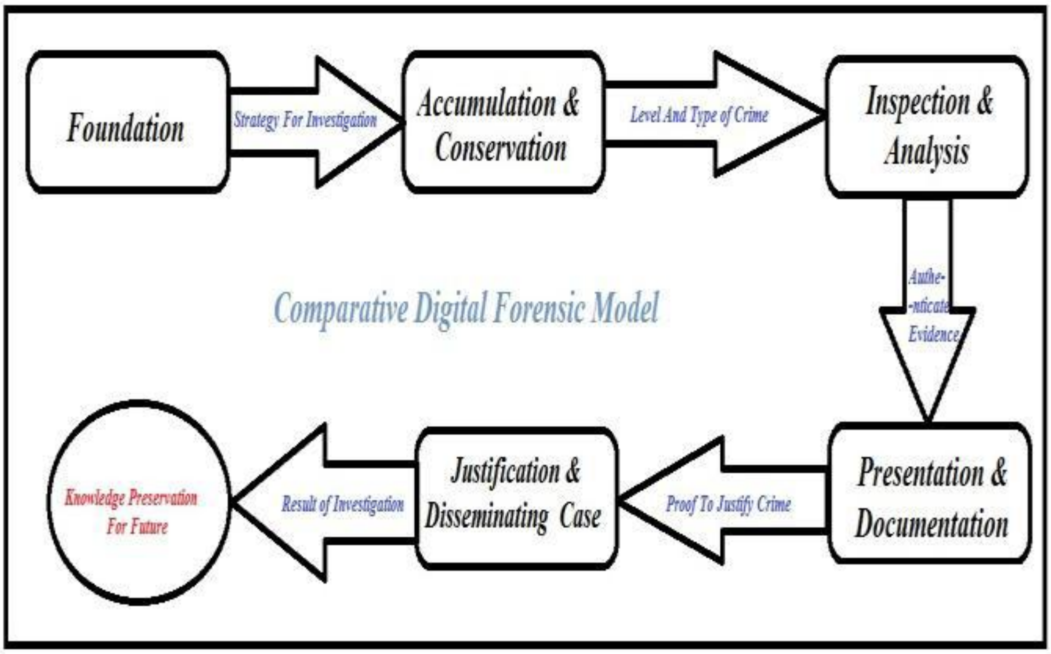

Foundation
Strategy For Investigation
Accumulation & Conservation
Level And Type of Crime
Inspection & Analysis
Authe- -nticate Evidence
Comparative Digital Forensic Model
Presentation & Documentation
Proof To Justify Crime
Justification & Disseminating Case
Result of Investigation
Knowledge Preservation For Future

Fig. 2: Comparative Digital Forensic Model

A. *Foundation*

This is initial phase of CDFM ,which includes different process and activities .The first activity is monitoring authorization and to obtain authorization so that the investigation can start .Secondly testing of infrastructure and operations take place to support an investigation .Based on this requirement and mechanism will be produced for the investigation.

With the complete verified and an efficient plan the investigator will decide all policies and will alert all concerned parties regarding investigation.

Hence at the finish stage of this phase the investigator will get following output:

- Proper Plan for Investigation
- Authentication, and
- Confirmation

B. *Accumulation & Conservation*

The major task of this phase to identify the digital evidence and all sources of data. This phase involves following activities like choosing any digital evidence or source of data for examination and then the investigator starts with finding its physical location. Then the investigators convert all encrypted or any form data to readable format. But the converted data should not lose its integrity and authenticity. During this all activity the investigator should conserve all digital evidence from outside environment. After completing above activity the investigators should take image snapshot of all produced digital evidence.

The output of this phase will be :

- Crime type,
- Event occurred
- Media
- Conceivable evidence sources.

C. Inspection & Analysis

At this stage the investigators are having physical and digital evidence which will be analyse and examine by them .This phase involves following activities : From evidence identification of data that how it was produced and when and using which technique. Then investigator will start with extracting data , all hidden data and all pattern matches.

After extraction of evidence data the investigator should simultaneously construct a detailed documentation for analysis and note down all conclusion and related theory based on inspection. At the end hypothesis should be developed which can justify the investigation.

Output of this phase will be :

- Log files
- Files
- Event logs
- Data
- Information

D. Presentation and Documentation

The task of this phase is to present and prepare a report using output of previous phase. The phase having following activities : retrieving all relevance issues of the information and its reliability. Then this issues will be tested to the availability and summarize all explanations , conclusions with documentation.

After completing Documentation a proper presentation should be made which can be present in the court .There should be final confirmation on every evidence and proof of the validity of the hypothesis created before and finally defend it against criticism and challenge.

The output of this phase will be :

- Authenticate Evidence Report

E. Disseminating the Case & Justification

After presenting all evidence and documents to the audience (Management, Law enforcement, Technical Person) ,it should be ensure that physical and digital evidence are returned to proper owner and find out the problems associated with the investigation if any .So that the investigators can do improvement in the future. The next step is disseminating the information from the investigation and close out the investigation. The knowledge gained should be preserved for future investigation.

IV. BENEFITS OF THE WORK

The proposed model is having very less and effective phases which provides better learning for new user .Some more benefits are as follows :

- The proposed model will help in evidence capturing and reconstruction of process or event by providing the properties of reliability, authenticity and testability in indentify the computer crimes and fraud.
- It will serve a standard and reference for investigate the computer crime and fraud for computer forensic team.
- Not only a systematic way but also it will provide a complete solution for computer crime which is very important need of the current changeable world.
- Using this model the authenticity and integrity can be achieved by providing different software tools.

V. CONCLUSION

The major requirement is that the digital evidence must be accurate so that it can present the case in court and the investigator should have enough knowledge to justify with the case. To accomplish this task the digital forensic model provide better approach to get the complete path for investigation.

After doing the survey of various models and with the proposed theory model our emphasis will be on how to achieve high quality result and satisfy with the output .The proposed model which is having comparative approach is more useful in this field. We hope the proposed model will be serve a better output to the new learning investigators.

ACKNOWLEDGMENT

We extend our sincere acknowledgements to all the faculty members of our institutes and other contributors for providing us the technical assistance for carrying out the study. Our truthful appreciation is to all the persons who were there to provide the facilities and help us for preparing this research review paper.

REFERENCES

[1] Yusoff,Ismail, Hassan,(2011),“Common Phases of Computer Forensic Investigation Model”, International Journal of Computer Science &Information Technology, Vol 3, No. 3..

[2] Alharbi,Jens,Issa(2011),“The Proactive and Reactive Digital Forensic Investigation Process: A Systematic Literature Review”, International Journal of Security and its Applications, Vol 5, No. 4.

[3] FC Freilling(2011),“The Structure Digital Forensic Investigation Process: A Systematic Literature Review”, International Journal of Security and its Applications, Vol 5, No. 4.

[4]Agrawal, A. Gupta, M. Gupta, S. Gupta, C. (2011) Systematic digital forensic investigation model Vol. 5 (1)

[5] E. S. Pilli, R. C. Joshi, & R. Niyogi, (2010) “Network Forensic frameworks: Survey and research challenges,” Digital Investigation, Vol. 7, pp. 14-27.

[6] SundresanPerumal (2009), “Digital Forensic Model Based on Malaysian Investigation Process”, International Journal of Computer Science & Network Security,Vol 9 No 8.

[7] SitiRahayu,RobianYusof ,ShahrinShaib,(2008) “Mapping Process of Digital Forensic Investigation Framework”, International Journal of Computer Science & Network Security,Vol 8 No 10.

[8] F. C. Freiling& B. Schwittay, (2007) “Common Process Model for Incident and Computer Forensics”, in Proceedings of Conference on IT Incident Management and IT Forensics, Stuttgard, Germany, pp. 19-40.

[9] M. K. Rogers, J. Goldman, R. Mislan, T. Wedge & S. Debrota, (2006) “Computer Forensic Field Triage Process Model”, presented at the Conference on Digital Forensics, Security and Law, pp. 27-40.

[10] Ruibin G Garrtner,M (2005) “Case relevance Information Investigation : Binding Computer Intelligence to the Current Computer Forensic Framework” Proceeding of Digital Forensic Research Workshop, Baltimore, MD.

[11] V. Baryamereeba& F. Tushabe, (2004) “The Enhanced Digital Investigation Process Model”, in Proceeding of Digital Forensic Research Workshop, Baltimore, MD.

[12] B. Carrier & E. H. Spafford, (2003) “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, Vol. 2, No. 2.

[13] M. Reith, C. Carr & G. Gunsh, (2002) “An Examination of Digital Forensics Models”, International Journal of Digital Evidence, Vol. 1, No. 3.

[14] G. Palmer, (2001) "DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research", Digital Forensics Workshop (DFRWS), Utica, New York.

[15] M. M. Pollitt, (1995) “Computer Forensics: An Approach to Evidence in Cyberspace”, in Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II, pp. 487-491.

[16] M. M. Pollitt, (2007) “An Ad Hoc Review of Digital Forensic Models”, in Proceeding of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE’07), Washington, USA.

BIOGRAPHY

Dr.DhananjayRamraoKalbande is currently a Associate Professor and Head in Department of Computer Engineering, Sardar Patel Institute of Technology, Andheri (West),Mumbai, India. He has completed B.E. in Computer Technology from Nagpur University in 1997 and Master of Engineering in Information Technology in May 2005, from Vivekanand Education Society's Institute of Technology(VESIT), Mumbai University, Mumbai, India.He has obtained Ph.D. in Technology from University of Mumbai, Mumbai in Jan 2012. With over 15+ Years experience in teaching & research, he is the author of several journal/conference/book chapter/ paper publications. His Research interests include Computer Network, Soft Computing, ERP Application development using Dot Net Technologies, Human Computing Interaction, Mobile device applications and Decision making and business intelligence.

Ms Nilakshi Jain is currently an Assistant Professorin Information Technology Department, Shah And Anchor Kutchhi Engineering College, Chembur (West),Mumbai, India. She has completed B.E. in Computer Technology from MLSU University in 2008 and Master of Technology in Computer Technology in 2012, from Pacific University.She is pursuingPh.D. in Digital Forensic (Computer Technology) fromPacific University . With over 5+ Years' experience in teaching & research, she is the author of one journal and 3 paper publications.