INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON DIFFERENT MODELS FOR DATABASE FORENSICS

ARVIND S. KAPSE[1], DR. HEMANT R. DESHMUKH[2], AVINASH S. KAPSE[3]

1. P. R. Patil College of Engg. & Tech. Amravati, Maharashtra, India.
2. Professor & Head of CSE Department, IBSS College of Engg. & Tech. Amravati, Maharashtra, India.
3. Assistant Professor, CSE Department, Anuradha Engg. College, Chikhli, Maharashtra, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Governments and private organizations are increasingly aware that vital information stored in their databases is no longer safe behind perimeter firewalls, intrusion prevention systems and other edge protections. Databases store a broad range of private and important information, making them a prime target for exploitation by wrongdoers wishing to breach confidentiality, damage the integrity of the data or make it unavailable to its users. The intricate nature and the non-stoppable critical services running in databases makes forensic examination of database difficult and challenges the forensics recovery and examination processes. This paper will present the feasibility of developing an enhanced workflow that provides insight into the challenging complexities of examining and using database evidence. It lays the foundation for the development and establishment of standards in database forensic analysis and forensic case management.

Keywords: Abstracted Digital Forensic Model, Event Based Digital Forensic Investigation Framework, Enhanced Digital Investigation Process Model, Integrated Digital Investigation Model, Systematic Digital Forensic Investigation Model Computer Forensic Investigation Process.

Corresponding Author: MR. ARVIND S. KAPSE

Access Online On:

www.ijpret.com

How to Cite This Article:

Arvind S. Kapse, IJPRET, 2015; Volume 3 (9): 857-864

PAPER-QR CODE

INTRODUCTION

Databases run the world and touch our lives daily; when we surf the web, make a phone call, swipe our credit card, use ATM, buy from a supermarket, secure a passport or driver's license, book a flight or visit a doctor. Nowadays, computer applications and databases are geographically distributed and are available to suppliers, customers and business partners who undertake business over the web.

However, the reliance on databases over time has made users highly dependent on network and information systems to complete essential operations. Whilst this technology has provided many benefits, it also has a number of vulnerabilities that has opened doors through which transgressors can target data and systems on which they depend.

Governments and private organizations according to Steven King, CTO from Data Intensity are aware that their vital information stored on databases is not completely secure in terms of confidentiality, integrity and availability behind perimeter firewalls, intrusion prevention systems and other edge protections. The current database topology is not flexible enough to differentiate between a user and a transgressor and processes all transactions by any user with a valid user name and password.

2. LITERATURE REVIEW

Yunus Yusoff et al. (2011) [1], demonstrated the CFIP (Computer Forensics Investigation Process) model proposed by Pollitt in 1984 for dealing with digital evidence examinations, so results would be scientifically reliable and legally acceptable. It comprises of 4 distinct phases.

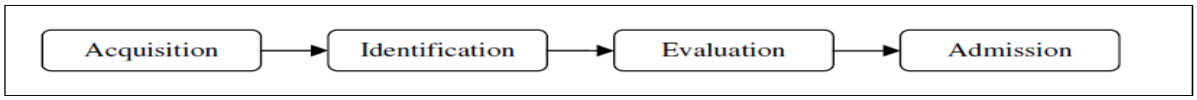

Figure 1: Computer Forensic Investigative Process [1]

Brian D. Carrier et al. (2004) [2], proposed EBDIF(event based digital investigation framework) and presented a simple framework for the digital investigation process that is based on the causes and effects of events. The phases have been organized into the basic requirements of an investigation: namely that we need to search for evidence that shows the causes and effects of an event and we need to develop hypotheses about the events that occurred at the crime scene. Each phase has a clear goal and requirements and procedures can be developed accordingly.

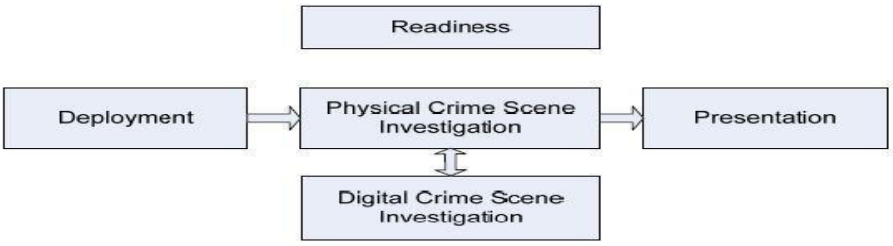

Figure 2: Five distinctive categories in the EBDFIF [2]

Baryamureeba et al. (2006) [3], proposed the Enhanced model based on the Integrated Digital Investigation Process model. It has five major phases as follows:

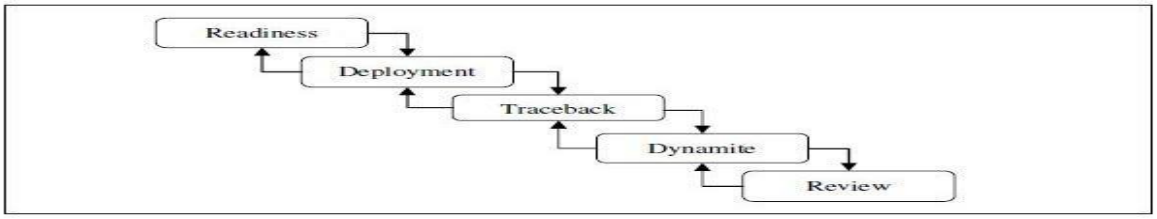

Figure 3: Enhanced Digital Investigation Process Model [3]

The U.S. Department of Justice published the FPM (Forensics Process Model) model (2008) [4] in the publication titled *'Electronic crime scene investigation: A guide to first responders'* (National Institute of Justice, 2008). This guide is oriented towards those who respond to the physical crime scene, so emphasis is placed on those requirements and little attention is paid to the analysis of the system (Carrier & Spafford, 2003). This model consists of five phases, namely Preparation phase, Collection Phase, Examination Phase, Analysis Phase and Reporting Phase.

Mark Reith et al. (2002) [1], proposed the Abstract Digital Forensic Model (ADFM) This model does well at providing a general framework that can be applied to a range of incidents. It consists of nine phases, namely Identification, Preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation, Return Evidence.

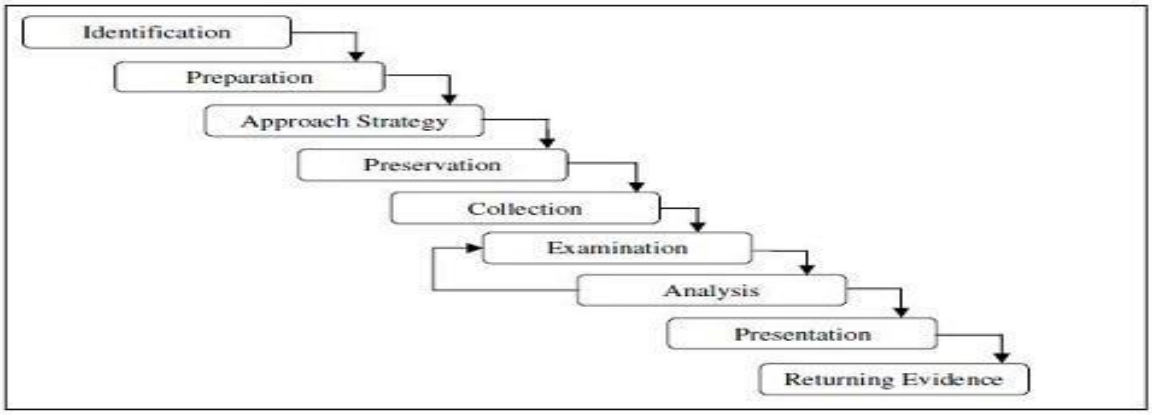

Figure 4: Abstract Digital Forensic Model [1]

Carrier et al. (2004) [2], proposed Integrated Digital Investigation Model (IDIM) (*See* An event based digital investigation framework (EBDFIF)) that has all the components from their previous model (EBDFIF) and does well at illustrating the forensic process and conforms to the cyber terrorism capabilities (National Institute of Justice, 2002).

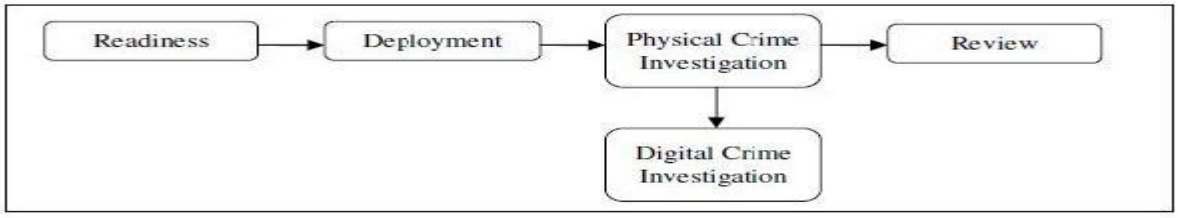

Fig. 5 Integrated Digital Investigation Model [2]

3. Comparisons of Different Models for Database Forensics:

3.1 Name Assigning for Comparison

In this section, each model that is being compared is given a short name so it can easily fit in a table. Table 1 describes the model name and the assigned short name.

Model Name	Short Name
Computer Forensic Investigative Process	CFIP
Event Based Digital Forensic Investigation Framework	EBDFIF
Enhanced Digital Investigation Process	EDIPM
Abstracted Digital Forensic Model	ADFM

Integrated Digital Investigation Model	IDIM
Digital Forensics Research Workshop Model	DFRWS
Scientific Crime Scene Investigation Model	SCSI
End to End Digital Investigation	EEDI
A Hierarchical, Objective-Based Framework for the Digital Investigations	HOBF
Framework for a Digital Forensic Investigation	FDFI
Common Process Model for Incident and Computer Forensics	CPMICF
Dual Data Analysis Process	DDAP
Network Forensic Generic Process Model	NFGP
Extended Model of Cybercrime Investigation	EMCI

Table 1. : Name Assigning for Comparison

3.2 Comparisons of Different Models

Models / Phases	CFIP	EBDFI	EDIPM	ADFMF	IDIMF	DFRWS	SCSIF	EEDI	HOBF	FDFIF	CPMICF	DDAP	NFGP	EMCI
Access												Y		
Acquisition	Y											Y		
Admission	Y													
Analysis				Y		Y		Y	Y		Y	Y	Y	
Approach Strategy				Y										
Authorization														Y
Awareness														Y
Collection				Y		Y		Y	Y				Y	Y
Deployment		Y	Y		Y									
Detection													Y	
Digital Crime Investigation		Y			Y									

Dissemination of Information														Y
Dynamite			Y											
Evaluation	Y													
Examination				Y		Y		Y					Y	Y
Hypothesis creation														Y
Identification	Y			Y		Y	Y	Y						
Incident Closure									Y					
Incident Response									Y				Y	
Individualization							Y							
Models / Phases	C F I P	E B D F I	E D I P M	A D F M	I D I M	D F R W S	S C I	E E D I	HOB F	F D F I	PM I C F	DDA P	N FGP	EMC I
Investigation										Y			Y	
Notification														Y
Physical Crime Investigation		Y			Y									
Planning														Y
Post-Analysis											Y			
Pre-Analysis											Y			
Preparation				Y					Y	Y			Y	
Presentation		Y		Y	Y	Y		Y	Y	Y			Y	Y
Preservation				Y		Y		Y					Y	
Proof & Defense														Y
Readiness		Y	Y		Y									
Recognition							Y							
Reconstruction							Y							

Report			Y	
Returning Evidence		Y		
Review	Y			
Search & Identify				Y
Traceback	Y			
Transport & Storage				Y

4. CONCLUSION

On the basis of demonstrated computer forensic investigation processes, we are able to extract the fundamental common investigation phases that are shared between all the models. The differences are in the content of each phase whereby certain scenario may require certain levels or types of details steps. Based on the grouping of the overlapping and similar phases, we have proposed, a new model, Proposed System Computer Forensic Investigation Model (PSCFIM). We hope that PSCFIM can serve as the basic and high level investigation models for any future computer forensic investigation. It should also serve as a good starting point for the development of new computer forensic investigation methodology.

REFERENCES

1. Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, “Common Phases Of Computer Forensics Investigation Models”, International Journal of Computer Science & Information Technology (IJCSIT), pp. 17 – 31, Vol 3, No 3, June 2011.

2. Brian D. Carrier, Eugene H. Spafford, “An Event-Based Digital Forensic Investigation Framework”, Digitial Forensic Research Workshop 2004, 1-12.

3. Venansius Baryamureeba, Florence Tushabe, “The Enhanced Digital Investigation Process Model”, Asian Journal of Information Technology 5(7), pp. 790-794, 2006.

4. National Institute of Justice. (2008). Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. Retrieved Apr 10, 2011, from ncjrs.gov: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

5. Ankit Agarwal, Megha Gupta, Saurabh Gupta & Prof. (Dr.) S.C. Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (1) , pp. 118-131, 2011.

6. Karen B. Alexander, "Database Forensic Analysis", Published by International Journal of Advance Research in Computer Science and Management Studies, pp. 245-251, Volume 2, Issue 3, March 2014.

7. Piyush P. Gawali, Dr. Sunil R. Gupta," Database Tampering and Detection of Data Fraud by Using the Forensic Scrutiny Technique", Published by International Journal of Emerging Technology and Advanced Engineering, pp. 439 – 446, Volume 3, Issue 2, February 2013.

8. Harmeet Kaur Khanuja1 and D. S. Adane, "A FRAMEWORK FOR DATABASE FORENSIC ANALYSIS", Published by Computer Science & Engineering: An International Journal, pp. 27- 41, Vol.2, No. 3, June 2012.

9. Martin S. Olivier, "On metadata context in Database Forensics", Published by ELSEVIER Digital Investigation, pp. 115-123, 2009.