UDGAM VIGYATI, Volume 2, 2015, (November)
Online ISSN 2455-2488
Page No. 144- 149

"ANALYSIS OF THE DIGITAL FORENSIC INVESTIGATION MODELS"

Prof. (Dr.) Umesh Singh
Director, School of Engineering and Technology,
Vikram University, Ujjain

Ms.Neha Gaud
Institute Of Computer Science,
Vikram University, Ujjain

ABSTRACT
Digital Forensic is a new and fast growing field that involves carefully study of collecting and examining electronic evidences that not only asses that damage to computer as a result of an electronic evidences attack but also to recover lost information from such a system to prosecute criminals. For those several investigations process models have been proposed from different investigators .The focus of this paper is to study different models and the steps that have been proposed by the investigators in order to implement those models, the steps that are involved in the investigation process and finally makes a complete analyzing study of the different phases of the respective models.

Keywords*: Digital Forensic models, DFA, digital evidences.*

INTRODUCTION

Today we are living in the world of technology, as the number of people is growing; the numbers of digital devices or assets such as computers, mobiles are growing rapidly. These assets are interconnected with each other in the form of networks and exchanging huge amount of data. These assets are emerging as a main reason for cyber crime.

In order to emphasis on such digital crime in 1984, the FBI laboratory and other law enforcement agencies began developing programs to examine computer evidences. The process or procedure adopted in performing the computer forensic investigation has a direct influence to the outcome of the investigation. Choosing the inappropriate or missing evidence, bypassing one step or jumping any of the steps lead to invalid conclusion

So it is very crucial for the computer forensic investigator to conduct their work properly as all of their actions are subjected to scrutiny by the judiciary should the case be presented in the court. Over the years there were a number of investigation models being proposed by various investigators based on our assumptions and observations some of the models tend to be quite detail and others may below general .So it is has becoming a bit difficult one even confusing, especially to the new comer forensic investigators to adopted the correct appropriate investigation model. So it is our efforts to analysis to all the phases combinely and focuses on their shortcomings.

NEED OF THE DIGITAL FORENSIC MODELS

To redevelop the digital evidences from digital sources a technique called digital Forensic has been developed, the digital forensic Models have been constructed So that step wise or well ordered inspection procedure of digital evidences can be made through it .The models can provide digital evidences

UDGAM VIGYATI, Volume 2, 2015, (November)
Online ISSN 2455-2488
Page No. 144- 149

examiners or investigators with the detailed and relevant true informations about particulars aspect or phase to be considered during the process of digital forensic investigation.

Existing digital forensic investigation model based on the chronological order ensuring at least one model proposed per year

Year	Investigators name	Name of the proposed model
2001	Henry lee	Scientific crime scene Investigation
2001	Kruse and heiser	Digital Forensic Investigation model
2001	Dfrws	Digital forensic research workshop model
2002	Reith,Care and Gunush	Abstract digital forensic model
2003	Carrier and spafford	Integrated digital investigation process model
2004	Casey 2004	Relevance information investigation
2004	Ciardhuain	Extended model of cyber crime
2004	Baryamureeba	Enhanced digital model

PROCESS REPRESENTATION THROUGH SEQUENTIAL LOGIC

To represent all the phases of models we are using sequential logic. The sequential logic used in this paper to represent phase is mealy machine .The mealy machine is a sequential logic circuit where the output is developed on the input and the current internal state.

The sequential logic circuit is given as follows:

<x> = <x1, x2, x3…… xn > where xi is either 0 or 1.xi is the set of conditions part of the circuit evaluating either true or false.

Lee (2001) [1]

Process

Lee = {Recognise=>identify=>Indivisualise=>Reconstruct}

Where,

Recognise = {Document=>Collect=>preserve}

Identify = {Evaluate=>Interpret}

Individualise = {evaluate=>interpret}

Reconstruct = {Report and present}.

Kruse and Heiser (2001) [2]

Process

Kruse and Heiser = {Acquire=>Authenticate=>Analyse}

Where,

Acquire = Collect the evidences without making any changes (original)

Authenticate = in this the evidences are checking against the original image.

Analyze = evidences are analyzed.

Digital Forensic Research Workshop Groups DFRWS (2001) [3]

UDGAM VIGYATI, Volume 2, 2015, (November)
Online ISSN 2455-2488
Page No. 144- 149

Process
DFRWS = {Identify=>preserve =>Collect=>Examine=>analysis=>Present=>Decide}

Reith (2002) [4]
Process
Reith =
{Identify=>Prepare=.ApproachStrategy=>preserve=>collect=>Examine<=>Analysis=>Presentation=>Returning Evidence}

Carrier and Safford (2003) [5]
Process
Carrier and Spafford= {Readiness=>Deployment=>physical Investigation||Digital Investigation=>Review}

Casey (2004) [6]
Process
Casey = {Incident Recognition=>Assessment=>Identification and Seizure=>Preservation=>Recovery=>Harvesting=>reduction=>Classification=>Analysis=>Reporting}
Where,
Preservation = {Collect=>Document}
Classification = {Organize=>Compare=>Individualize}

Ciardhuain (2004) [7]
Process
Ciardhuain = {Awareness=>Authorize=>Plan=>Notify=>Search/identify=>Collect=>Transport =>store=>examine=>Hypothesis=>present=>Prove/Defend=>Disseminate}

Baryamureeba (2004) [8]
Process
Baryamureeba= {Readiness<=>Deployment<=>Trace back <=> Dynamite< => Review}
Where,
Readiness= {Operational Readiness=>Infrastructure Readiness}
Deployment= {Detection and notification=>physical Crime Scene Investigation=>Digital Crime Scene Investigation=>Confirmation=>Submission}
Trace back= {Digital Crime scene Investigation=>Authorization}
Dynamite= {physical crime Scene Investigation=>Reconstruction=>Communication}

The below table consists of all the Phases of the Investigation Models discussed respectively where each row indicating to phases of the models and each column referring to each investigators respectively

UDGAM VIGYATI, Volume 2, 2015, (November)
Online ISSN 2455-2488
Page No. 144- 149

Name of phases	**Henry lee**	**Kruse and heiser**	**Dfrws**	**Reith**	**Casey**	**Carrier and Spafford**	**Ciardh -uain**	**Baryamureeba**
recognize	1				1			
document	1.1				4.2	3.2		
collect	1.2		3	5	4.1	3.5	6	
preserve	1.2		2	4	4	3.1		
identify	2		1	1	3		5	
classify	2.1				8			
compare	2.2				8.2			
individualize	3				8.3			
evaluate	3.1							
interpret	3.2							
reconstruct	4				4	3.6		4.3
report	4.1				10			
present	4.1		6	8		3.7	11	
acquire		1						
authenticate		2						
analyse		3	5	7	9			
examine			4	6			9	
assess					2			
seizure					3			
recover					5			
harvest					6			
reduce					7			
organise					8.1			
decide			7					
prepare				2				
Approach strategy				3				
return				9				
readiness						1		1

UDGAM VIGYATI, Volume 2, 2015, (November)
Online ISSN 2455-2488
Page No. 144- 149

operational						1.1		1.1
infrastructure						1.2		1.2
deployment						2		2
Physical investigation						3		2.3/4.1
Digital investigation						3		2.4/3.1/4.2
review						4		5
detect						2.1		
notify						2.1	4	2.5
confirm						2.2		8
authorise						2.2	2	3.2
survey						3.2		
search						3.4	5	
trace back								3
dynamite								4
submit								2.6
communicate								
Become aware							1	
plan							3	
Prove/ defend							12	
disseminate							13	
Transport							7	
Store							8	
hypothesise							10	

There is however instances where the listed terms are actually synonyms of terms tested in other. According to Thesaurus [9] it should not be avoided and investigators must put endeavors to develop the models consisting with features like cyclic .scene reconstruction, time limitations.

CONCLUSION

The high number of duplicity and the great degree of variability among different stages of models signifies complexity In spite of developing a new model it would be more relevant to remove the shortcomings in phases. Digital evidence must be admissible precise authenticated and accurate in order

UDGAM VIGYATI, Volume 2, 2015, (November)
Online ISSN 2455-2488
Page No. 144- 149

to be accepted in the court a detailed digital forensics procedure provides important assistance to forensic investigators in gathering evidences admissible in the court of law.

REFERENCES

1. Brian Carrier and Eugene H Spafford, (2003) Getting Physical with the Investigative Process International journal Of Digital Evidence. Fall 2003, Volume 2, Issue 2.
2. Casey, E., State of the field: growth, growth. Digital Investigation,2004.
3. Digital Forensic Research Workshop (DFRWS) Research Road Map, Utica, NY. (2001)
4. Henry lee, Timothy Palm Bach, and Marilyn Miller. Henry Lee's crime Scene Handbook. Academic Press, 2001.
5. Mark Reith, Clint Carr and Gregg Gunsh. (2002) an Examination of Digital Forensic Models International Journal of Digital Evidence, fall 2002, Volume 1, Issue 3.
6. S. Ciardhuain, (2004)" An Extended Model of Cyber crime Investigation ", International Journal of Digital Evidence, Vol.3, no. 1, pp.1-22.
7. V. Barymereeba & F. Tushabe, (2004) "The Enhanced Digital Investigation Process Model". In proceeding of Digital Forensic Research Workshop, Baltimore, MD.
8. **W**arren Kruse and jay heiser.*Computer Forensic*: *Incident Response Essentials*. Addison Wesley, 2001.
9. Thesaurus.com. Thesaurus. http://thesaurus.com/,october 2011.