RESEARCH ARTICLE OPEN ACCESS

A New Digital Investigation Frameworks Comparison Method

Omrani Takwa*, **Chibani Rhaimi Belgacem, ***Dallali Adel
*(Macs, university of Gabes, ENIG, Tunisia
** (MACS, University of Gabes, Tunisia
*** (IRIT, university of Sfax, Tunisia)

----------**********----------

Abstract:

To understand an incident crime case and achieve the consistent electronic evidence, the investigator needs to deal with an investigation tutorial. In this paper, we study and compare some of mainly accepted digital investigation models. Then we check the investigation model accuracy by testing the main rules availability. A new model is developed which merges the former models and seeks to meet some constraints. This can help investigators to achieve electronic evidence in illegal manner and in understandable format to be presented to the court.

Keywords — **digital investigation model, digital evidence, forensic computer, electronic evidence, electronic crime**

----------**********----------

I. INTRODUCTION

.

ICTs and internet technologies provides many benefits to computer users. But, sometimes, it helped some criminals to commit fraud, intrusions and attacks that can destroy the user privacy and properties. For this, we are needed to provide a lot of effort to fight against crime events by waiting to reading and identifying the crime colours "modern." Like any act of general crime, it always resort traces helping to discover evidence; this can be realized through the electronic crime investigation process. [*1*]. The main purpose of investigation model is helping investigator to acquire, identify, extract, analyze and present digital evidence in a reasonable format to be presented in the court. Indeed, an investigative model can achieve a good level of efficiency if it can meet a set of rules.

In this paper, we present an analysis study for digital investigation model based on previous defined rules. This comparison leads to realize a new investigation model is created that can meet the constraints referred to above. This helps future work to understand the issue of forensic computer and to produce an effective investigative procedure suitable for presentation to the court. Our paper is divided into four sections; the first section focuses on some definitions related on electronic crimes. The subsequent section will discuss and compare some accepted frameworks proposed in the literature; the last section introduces the proposed forensic framework.

II. COMPARATIVE STUDY OF DIGITAL INVESTIGATION EXISTENT MODELS

In this section we study and analyse some related work of digital investigation models. Advantages and disadvantages of each methodology will be based on aggregation of different models steps [*2*], [*3*], [*4*], [*5*], [*6*], [*7*], [*8*], [*9*] which can meet evidence criteria.

A. Computer Forensic Investigative Process

The first investigation model was appeared in 1984 [*2*], composed of 4 main phases, which are acquisition, identification, evaluation and admission. Acquisition phase gives the importance of authenticity for investigation process as it will be indicated. Relevant data collection is modelled with identification phase. From all collected data, estimation and hypothesis are examined in

evaluation phase. The last phase is admission which involves the presentation of founded results and concluding evidence with understandable form before inspection by the court. However, compared with next adopted investigation framework, this methodology was not focused on securing and preserving data from intrusion during the investigation process. The second drawback of this model is its linear form .So, there will be no possibility to make correction(s) and/or updating evidence. The third drawback is that it won't be possible to report or storing an investigation scenario.

B. Digital framework investigation model

In 2001, (DFRWS) was created [*3*] for dealing with potential evidence. Compared with previous model, six phases were introduced, that are identification, preservation, collection, examination, analysis and presentation. The first phase is to plan the investigation process. This helps saving more time of investigation. Data privacy and integrity are checked in Preservation phase. The consistence has an importance in this model, this is proved by analysis and examination phase. Presentation phase involves the clarity of evidence and make it understandable by the court. However, it is impossible to return to pervious phase to correct or modify tasks. There are no preparation phases before initiating the investigation procedure. This can make a longer investigation time Furthermore; owner property is not respected at the end of investigation.

C. Abstract Digital Forensics Model (ADFM)

This model [*4*] was proposed in 2002, nine phases are introduced in this model. . Those added respectively named preparation phase, approach strategy and returning evidence phases. To do that, one must be ready to adopt them. This leads to make tools and techniques being prepared before starting the data collection. The final objective is mainly to look for minimizing the investigation time. It also focused on giving transparent evidence by designing approach strategy phase which aims to preserve data from any external event during investigation process. If results aren't validated, errors correction is possible through of a model's recursively form. A new relevant idea has been proposed by this model which is the rightful owner property. This is done in returning evidence phase which aims to ensure that evidence is safely returned to the rightful owner. Some important investigation criteria are not respected in this model. Confidentiality and integrity of data were not properly defined which can degrade the data security and proof transparency. ADFM model doesn't design steps for Storage and reporting investigation events.

D. Integrated digital investigation process (IDIP)

Created since 2003, this has been composed from five main phases [*5*] known as: Readiness phase, deployment phase, physical Crime Scene investigation phase, digital crime scene investigation and review phase. Materials and software preparation tools are involved to minimize the investigation time Preparation phase and facilitate investigation task. To contribute to investigation reliability, Evidence Analysis are divided in two virtual environments namely, *physical crime scene investigation Phase and digital crime scene investigation phase*. This makes Integrity and confidentiality well kept (deployment phase). However, owner property and security property rules are not respected during the investigation process.

E. Enhanced digital investigation model (EDIP)

In 2004, Carried and Spafford were created a model named EDIP, inspired from IDIP model [*6*]. It accords the same phases adopted by IDIP model except that it includes both of digital and physical crime investigation crime phases into one phase named Submission phase. Same advantages like those of IDIP are mentioned in this model. This model added the attribution concepts which are based on chronology time that helps to saving the investigation time and maximizes the evidence reliability. Confidentiality and integrity and owner privacy rules are not mentioned.

F. Computer Forensics Field Triage Process Model (CFFTPM)

This methodology tried to establish investigation process in a short time without using a recursive

model for correction and revision [*7*]. Six primary phases have been introduced in this model. Internet phase helps investigator to examine the internet artifact to return more relevant data. User profile phase is added to this model in order to analyze user features, his relations, his applications and his preferences. This task helps investigator to understand the incident case. Case specific phase aims to classify the incident case for becoming better clearer. For example, electronic attack incident is different from the one focused on child pornography crime. Confidentiality and integrity of collected information are not respected. Owner property is not done and investigation event is not reported.

G. Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)

In 2009 a new methodology was proposed in **[***8***]**. Based on the Malaysian investigation process, it is consisting of seven steps. A planning phase was applied to range and prepare software and hardware tools, helping to optimize the investigation time. Confidentiality and integrity rules are respected. These methodologies think to reusability of investigation process by future investigation work. So, it designed new phase named archive storage. Let's note that we must notify some points that are not respected in this model. However, some investigation criteria are not respected in this model those owner property are not respected. This model has linear form, so, returning to previous steps an impossible task which makes correction and revision difficult and often impossible. Furthermore, the protection of owner properties is not mentioned at the end of this framework.

H. A generic framework for network forensic

In 2010, P. Immanuel has proposed a new investigation framework based on network forensic **[***9***].** In this new framework, nine phases are implemented: preparation and authorization, detection of incident, collection of network traces, preservation and protection, examination, analysis, investigation attribution and presentation. As a recursive model, correction and revision are possible. Confidentiality and integrity criteria are respected in preservation phase. Data Attribution facilitates identifying data and saving time. This is done in investigation and attribution phases. This model is focusing for security properties as each investigation step is controlled and tested by many security tools. This model is applied only for network crime and not to other crime incidents. Owner property is not respected.

III. COMPARATIVE DESCRIPTORS

Before comparing different investigation models, we need to define a set of investigation criteria [10] used to discriminate a model to another one. This is described in the following table. Based on defined criteria we present a brief description of various steps focused on each of these criteria as showed in the following table.

TABLE.1 FORENSIC INVESTIGATION CRITERIA

criteria	**Appropriated phases**
Time gaining	Preparation, attribution, report, time chronology, case specific
Evidence transparence and privacy	Preservation, approach strategy, returning evidence
Evidence reliability and consistence	Preparation, Analysis, examination, presentation, evaluation, feed back
reusability	Report, review

IV. RESULT ANALYSIS

TABLE. 2 COMPARATIVE DIGITAL INVESTIGATION MODEL BASED ON RESPECTING CRITERIA

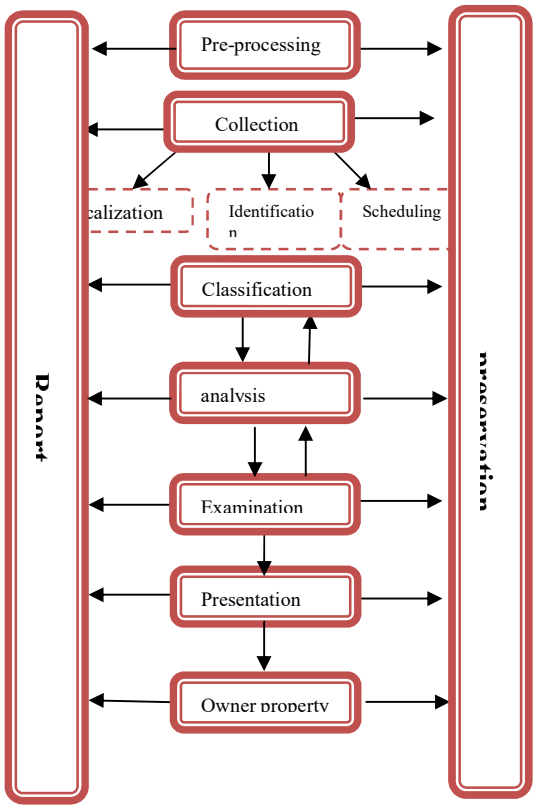
criteria	Gaining time		reusability	Evidence reliability and consistence				Evidence transparence and privacy	
Common phase	preparation	attribution	identification	Rapport	collection	Presentation	Examination	analysis	Preservation	Owner property
1984	- -	--	identificati	- -	Acquisition	admission		evaluation	-	
2001	- -		identificati	- -	collection	Presentation	examinatio	analysis	Preservatio	-
2002	preparation	--	Identificati	- -	collection	presentation	Examination	Analysis	preservation	Returning evidence
			Approch							
2003	readness	deployement	Digital crime scene investigation							
			Physical crime scene invetigation							
2004	Readness	--	deployment	Review	traceback	dynamite		--	--	
2006	planning	chronology Time	triage	- -	User profile	- -	Internet	Case specific	--	
2009	planning	-	identification	Archive	reconnaissan	Transport	Analysis	Proof	--	
2010	Preparation&	Attribution	Detection of	- -	Collection	Preservation	examination	analysis	Presentation	-

The objective of the mentioned table is to list the respected criteria of various investigation models. We present a brief comparative description of various steps constituting digital forensic models.

V. PROPOSED MODEL

Based on a review of the previous investigation framework, we will try to propose a new model within defined criteria such time saving, reusability and security property (confidentiality, integrity, Authenticity and owner property). Proposed model has numerous advantages that are distributed into many steps model below:

Fig.2 Proposed digital investigation Model



VI. DISCUSSION

Our proposed model is composed of nine main phase. The first phase is pre-processing, in which investigation software and hardware tools are prepared and checked. Furthermore, investigators capabilities and experiences need to be tested. Moreover, authorization and confirmation are given

to investigation members. This first step facilitates the achievement of relevant data and solves many investigation problems in the following steps.

The second phase is collection which is divided into three sub-phases; localization phase to identify relevant data, identification sub-phase in which, hidden information and encrypted data are also extracted this is done by using special investigation tools. Scheduling sub-phase is done to sequence collected data in the rank of their priority and reliability. The fourth phase is classification which is based on referring on previous investigation events and compares them with the current investigation. This is done by many statistic tools and data fusion technique. The aim is to understand the incident case and to quickly find the reliable solutions of investigation. The fifth phase is analysis, where many estimation, possibility and hypothesis are interpreted from given data. The result is to propose the final potential evidence. The sixth phase is examination which involves the validation analysis result. It is possible to correct and review results by returning to the former step. This makes model more flexible. In the presentation phase, electronic evidence is presented in understandable form to be presented to the court. Rapport phase is not a simple one but it covers the totality of the presented model. The output of this step is an investigation rapport which contains final potential evidence, explanation, new Policies and investigation Procedures, Evidence Disposed, investigation closed events. Preservation phase is done in order to prevent people from using the digital device or allowing other electromagnetic devices to be used within an affected range. Physical scene is recorded and pertinent data are duplicated using standardized and accepted procedures. Validity and integrity of evidence is also insured for later use. The last phase is the owner property. In fact, at the end of investigation process, owner information must be returned to their owner and authorization access must be modified. It is important to maintain owner property for later use.

VII. CONCLUSION

In this paper, a set of digital investigation models having appeared since 1984, have been reviewed. A comparative analysis has been done based on some defined criteria which are security property, reusability and time gaining. We have shown that many criteria were not explicitly processed in different investigation methodologies. A new combined digital investigation model has been defined. It aims to explicitly consider investigation issues. We hope that the new proposed framework helps future investigation actors to understand many incident cases. This offers presentable electronic evidence to the court.

REFERENCES

[1] Reith M, Carr C, and Gunsh G, "An Examination of Digital Forensics Models," *International Journal of Digital Evidence*, vol. 1, no. 3, 2002.

[2] Yusof f Yunus, Ismail Roslan, and Zainuddin Hassan, "COMMON PHASES OF COMPUTER FORENSICS INVESTIGATION MODELS," *International Journal of Computer Science & Information Technology (IJCSIT)*, vol. 3, no. 3, june 2011.

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

[4] Reith M, Carr C, and Gunsh G, "An Examination of Digital Forensics Models," *International Journal of Digital Evidence*, vol. 1, no. 3, 2002.

[5] B Carrier and H Spafford, "getting physical with digital forensic process," *www.cerias.purdue.Edu/home/carrier/forensics accessed on 20th September 2011*, 2003.

[6] Baryamereeba V and Tushabe F, "The Enhanced Digital Investigation Process Model," 2004.

[7] K, Rogers M, Goldman J, Mislan R, Wedge T, and Debrota S, "Computer Forensic Field Triage Process Model," in *Conference on Digital Forensics, Security and Law*, 2006, pp. 27-40.

[8] P. Sundresan, "Digital Forensic Model based on Malaysian Investigation Process," *International Journal of Computer Science and Network Security.*, vol. 9, no. 8, 2009.

[9] Pilli immanuelS, Joshi R.C, and Niyogi Rajdeep, "A generic Framework for Network Forensic," *International Journal For Computer Application*, vol. 1, no. 1, 2011.

[10] Aminnezhad Asou, Dehghantanha Ali, and Taufik Abdullah Mohd, "A Survey on Privacy Issues in Digital Forensics," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 4, no. 1, pp. 311-323, 2012.