ISSN: 0067-2904

# Identifying Digital Forensic Frameworks Based on Processes Models

**Talib M. Jawad Abbas*, Ahmed Salem Abdulmajeed**
Department of Systems Eng., College of Information Eng., Al-Nahrain University, Baghdad, Iraq.

**Abstract:**
Digital forensic is part of forensic science that implicitly covers crime related to computer and other digital devices. It's being for a while that academic studies are interested in digital forensics. The researchers aim to find out a discipline based on scientific structures that defines a model reflecting their observations. This paper suggests a model to improve the whole investigation process and obtaining an accurate and complete evidence and adopts securing the digital evidence by cryptography algorithms presenting a reliable evidence in a court of law. This paper presents the main and basic concepts of the frameworks and models used in digital forensics investigation.

**Keywords:** Advance Encryption Standard, Digital Evidence, Digital Forensic, Digital Investigation, Hash Function.

## Introduction:

Digital technology development has resulted an upturn in the use of computers / internet as instruments used to increase productivity and effectiveness in government sectors and businesses, educational institutions, and in all economies. It has strengthened in the same manner the use of computers as a means of offender's ability to carry out and conceal illegal or unethical activities.
Statistics show that the computer crimes are increasing and in parallel it is obvious a high rise of products and companies specialized in producing computerized law enforcement tools in determining the who, what, where, when, and how of crimes. Consequently, "computer and network forensics has evolved to assure proper presentation of computer crime evidentiary data into court" [1]. The law enforcement against criminals is an continuously challenge, to succeed in this challenge using methodologies based on deep forensic analyses of digital crime investigation and tools development are necessary. Studying and overviewing a wide range of digital forensic investigation models it will possible to conclude a digital investigation process [2]. We will review a set of digital forensic investigation models/frameworks that is introduced during the last decade to identify the commonly shared processes and develop it to adopt a secure procedure.

The structure of paper is as follow: section two presents the definitions of main terms in the field of forensics; in section three, some of investigation models of digital forensic are discussed slightly; the fourth section suggests a forensic framework from the common phases of an analysis on various available models. Section five presents' cryptography algorithms and defines a method to secure the digital evidence Conclusions are given in section six.

Definitions:

The key words in this field are interpreted in a various ways, to avoid confusion the main terms of process will be defined. Forensics "is defined in the Merriam Webster's dictionary as belonging to, or suitable to courts of judicature or to public discussion and debate and relating to or dealing with the application of scientific knowledge to legal problems, it comes from the Latin of the forum"[3]. The main aim of forensics implementing is to gain a better understanding of the event by finding and analyzing the facts related to this event.

*Email: talib_altaleb@yahoo.com

Digital Forensics is a proven scientific method that extracts from a digital source, contributions of a digital evidence as a collection, presentation, validation, preservation, interpretation, identification and analysis in detecting a crime or unauthorized actions. Digital Evidence is generated/collected from electronic machines such as mobile phones, desktop and laptop computers and any digital audio/video device, etc. [4]. Therefore, it's obvious any digital component in the daily life could be considered through the digital forensics. The process of answering questions regarding a digital event is called Digital Investigation. Where, a Digital Forensics Investigation is a type of digital investigation based on techniques and procedures that leads to the acceptance of detected findings in a court of law[5].

Framework is a defined structure based on disciplines where a digital forensic framework has to cover all subjects related to in this field. A more powerful term than framework is Model it is based on classifying and grouping entities with a particular specification [6]. Digital Forensic Investigation Framework (DFIF) aim is to present a successful investigation process by defining standardize digital forensic investigations. The known methodologies are contributed from law enforcements, cybercriminal actions, etc., experiences based on procedures and tools. [7]

Summary to Some Digital Forensic Investigation Models/Frameworks:

This paper aims to identify the commonly shared processes through the published frameworks and models in a period of ten years by reviewing the published papers during 2001/2010 from a wide range of adopted procedures for digital forensics investigations. It is obvious that a perfect model is a well-structured framework that covers all aspects (non-technical and technical) of a digital investigation.

Digital Forensic Research Working Group (DFRWS):

In the first meeting of (DFRWS) in 2001, a document was created by consensus, which outlined the state of digital forensics at that time [8]. It consists of the following classes (The primary function is highlight):

A. Identification: Clarify how investigator is notified of a potential incident or crime.
B. Preservation: An acceptable chain of custody.
C. Collection: The use of various techniques to recover relevant data.
D. Examination: Deal with the techniques used to examine evidence.
E. Analysis: The analysis of an evidence that is collected, identified and extracted from a gross data collection.
F. Presentation: Tasks of this phase is documentation, expert testimony, etc.
G. Decision: This includes the confession of the suspect or accused person.

It is obvious that the captured data are collected and passed to the next phase.

Abstract Digital Forensics Model (ADFM):

This model introduced by Reith, Carr and Gunsch, in 2002, operates based on a traditional strategy of collecting forensic evidence as implemented by law enforcement [7]. They offer a model comprised of nine steps:

Identification, Preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation, Returning Evidence.

This model and the previous one (DFRWS) contain many of the same ideas, but differ in the categories. This model includes Identification, Preservation, Collection, Examination, and Analysis classes similarly defined as those of the DFRWS. In the two models the emphasize is on the chain of custody at the phase of preservation. Both DFRWS and ADFM care about record or the physical crime scene and documentation of electronic evidence. Third and fourth phases, which include examination and analysis, are similar in the two models in dealing with the tools and techniques used in the examination of evidence. Lastly, they include return of evidence to place of decision.

Integrated Digital Investigation Process (IDIP):

In 2003, Brian Carrier and Eugene Spafford [9], proposed a model called the Integrated Digital Investigation Process (IDIP). This model is implemented in 17 phases, which could be grouped into five classes as follow:

- Readiness: this phase clarifies and ensures the ability to process an investigation.
- Deployment: implements a procedure to detect and confirm a crime or criminal event.

- Physical Crime Scene Investigation: reconstruction of crime scene and criminal action through collecting and analyzing physical evidences.
- Digital Crime Scene Investigation: It is the same as previous step where the concentration in this phase is on the digital evidence from digital sources.
- Review: aims to find gaps where it could be possible to improve the investigation.

This model studies and solves the case by a different perspective in comparison with the previous models even though that it is using many parts of the same phases.

It is clear that the function of readiness in the current model, which necessarily includes all the preparations, for example, training people, and the composition and the establishment of the infrastructure of the investigation is approximately similar to the functions of the preparation phase in the previous model. Therefore, as the rest of the other stages it is also able to find participants.

Enhanced Digital Investigation Process Model (EDIP):

In 2004, Baryamueeba and Tushaba have introduced a modification on IDIP Model (2003), they have added two extra phases to the previous model, which are trace back and dynamite [10]. In this section based on the comparison Table1 in [11] we aim to illustrate the commonalities between the phases of the two models IDIP & EDIP.

**Table 1 -** Comparison Between Phases Between IDIP and EDIP Models

| Phase | IDIP | EDIP |
|---|---|---|
| Readiness phases | ▪ Operations<br>▪ Infrastructure | ▪ Operations<br>▪ Infrastructure |
| Deployment phases | ▪ Detection and notification<br>▪ Confirmation and Authorization | ▪ Detection and notification<br>▪ Phy crime scene Inv<br>▪ scene inv Dig crime<br>▪ Confirmation<br>▪ Submission |
| Physical Crime Scene phases Investigation / Trace back phases | ▪ Presentation<br>▪ Survey<br>▪ Documentation<br>▪ Search and Collection<br>▪ Reconstruction | ▪ Dig crime scene Inv<br>▪ Authorization |
| Digital Crime Scene phases Investigation / Dynamite phases | ▪ Presentation<br>▪ Survey<br>▪ Documentation<br>▪ Search and Collection<br>▪ Reconstruction<br>▪ Presentation | ▪ Phy crime scene Inv<br>▪ Dig crime scene inv<br>▪ Reconstruction<br>▪ Communication |
| Review | ▪ Review | ▪ Review |

**A Hierarchical, Objectives-Based Framework:**

In 2005 Beebe and Clark have defined a framework based on hierarchical thematic structure in compare with the traditional single tier higher order process models. The defined model in the first level (tier) presents common phases with previous models the difference is that each phase has sub-phases getting deep in specifications to provide quality and granularity, based on disciplines and classifications [12]. The six phases [13]:

**Preparation:** Includes support deterrence, detection, response, investigation, and prosecution.

**Incident Response:** detecting an electronic crime in a related incident and starting a pre-investigation.

**Data Collection:** Collect digital evidence in support of the response strategy and investigative plan.

**Data Analysis:** Confirmatory analysis (to confirm or refute allegations of suspicious activity) and/or event of reconstruction, etc.

**Presentation of Finding:** Communicate relevant findings to a variety of audiences, including management, technical personnel, legal personnel, and law enforcement.

Incident Closure: As the name implies, it focuses on closure of the investigation.

As mentioned at the beginning, the goal of the research primarily is to find commonalities between the activities of phases in a range of models, not the detailed view of every stage. Therefore, we will schedule similarity between the phases of the current model and some previous models that have been presented. Table-2 [13] shows the similarity between the present model and some of the previous models. As shown, each of the previous frameworks/models addresses most or all of phases of current framework.

**Framework for a Digital Forensic Investigation:**

In 2006, Kohn have introduced a framework including a number of finite steps and to make it a more adaptable framework it's being classified into three groups. These steps a defined as follow [14]:

Preparation: are rules and procedures defined as a standard to be implemented for assisting in the investigation, training, etc. process.

Investigation: is the process of interrogation and research to gather digital evidence from electronica devices.

Presentation: Presenting the analysis, and proving it.

All the phases making up previous frameworks can be incorporated into this framework.

**Common Process Model for Incident and Computer Forensics:**

It is introduced by **Freiling** in 2007, to investigate computer security crime cases, and the aim from this model is to achieve an improvement in the investigation process through the combination of Computer Forensics and Incident Response concepts. It's based on three main phases [15]:

Pre-Analysis: is all the implemented procedures and actions before starting the actual analysis.

Analysis: is analyzing the collected data from the computer system that is as a target while it is on and running, starting with Live Response, data concerning the incident.

Post-Analysis: After finishing collecting and analyzing the digital evidence this phase starts and it is concentrated on documenting all the procedures and actions during the investigation.

This model presents a common model for both Incident Response (including seven phases or steps) and Computer Forensics processes (including twelve phases or steps) which combine their advantages in a flexible way. In fact, the Common Model somewhat resembles a Computer Forensic investigation which is embedded into an Incident Response procedure.

**Table 2**- The similarity between the present model and some of the previous models

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| DFRWS Palmer *Model 2001* | Class | | | | | | | | |
| | Identification | Preservation | Collection | Examination | Analysis | Presentation | Decision | | |
| | 2 | 3 | 3 | 4 | 4 | 5 | 6 | | |
| Reith, Carr, and Gunsch M0del 2002 | Phases | | | | | | | | |
| | identification | preparation | approach strategy | preservation | collection | examination | analysis | presentation | returning evidence |
| | 2 | 2 | 2 | 3 | 3 | 4 | 4 | 5 | 6 |
| Brian Carrier and Eugene Spafford *2003* | Groups | | | | | | | | |
| | readiness 2 phases | deployment phases 2 | physical crime scene investigation phases 6 | digital crime scene investigation phases 6 | review phase | | | | |
| | 1 | 2 | 3 | 4 | 6 | | | | |
| Beebe, N. l., & Clark, J. G | Phases | | | | | | | | |
| | preparation | incident response | data collection | data analysis | presentation | incident closure | | | |

**New Digital Forensics Investigation Procedure Model:**

In 2008, Yong-Dal Shin, have introduced a new ten stage model and these phases are: Investigation Preparation, Classifying Cyber Crime and Deciding Investigation Priority, Investigating Damaged (victim) Digital Crime Scene, Criminal Profiling Consultant and Analysis, Tracking Suspects, Investigating Injurer Digital Crime Scene, Summoning Suspect, Additional Investigation, Writing Criminal Profiling, Writing Report [16]. This current model can be approximated and participates in some phases belonging to the Brian Carrier model, which does not includes Classifying Cyber Crime and Deciding Investigation Priority, Psychological Profiling Investigation Method, and so on. This model cannot be adopted with the aim of the search in finding commonalities.

**"Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)":**

Perumal suggested model that the investigation process based on a fragile evidence will improve the prosecution by including all important stages, static data and live data acquisition [10]. This model is a 7-stage framework which are as follow: **planning, identification, reconnaissance, analysis, result,**

**proof and defense, and archive storage.** Compering the this model with DFRWS [17] it is obvious there is a complete similarity in five out of seven stages, as shown in Table-3 below.

**Table 3 -** Comparison of the stages task in the DFMMIP model with DFRWS model.

| DFMMIP | Planning | Identification | Reconnaissance | | | Analysis | Result | Proof & Defense | Archive Storage |
|---|---|---|---|---|---|---|---|---|---|
| DFRWS | | Identification | preservation | collection | examination | Analysis | presentation | decision | |

**Network Forensic Generic Process Model:**

Lastly in 2010, **Emmanuel S. Pilli, R.C. Joshi, and Rajdeep Niyogi proposed** this model which has been formulated from a specialized methodology for investigations on the network. The phases in this model are similar to the previous mentioned models with a difference where network forensic is considered slightly in the above models. NFGP model phases are as follow:

**Preparation** phase: This phase is applicable only to environments of network forensics where network security tools and others are deployed at various strategic points on the network.

**Detection**: The presence and nature of the attack are determined from various parameters.

**Incident response**: The response to crime or intrusion detected is initiated based on the information gathered to validate and assess the incident.

**Collection**: Data is acquired from the sensors used to collect the traffic data.

**Preservation**: digital evidence logs and traces collected from original data will be saved as read only in storage devices.

**Examination**s: The traces obtained from various security sensors are examined.

**Analysis**: Statistical, soft computing and other tools are used to analysis data.

**Investigation**: This phase aim is to find out the attack source from the victim device through the communication routs and networks.

**Presentation**: is to outline the observations and considered procedures in the conclusions (12).

**Recognition Phases Shared:**

Of the existing frameworks or models referred to in paragraph 3, each model, despite its differences, has quite a lot in common with other models. It is obvious that each suggested framework builds on the previous experience; where some of them define similar approaches and other focuses on the different aspects of the investigation.

Consequently, all of these frameworks results are the same even if in some stages the procedures are different.

"In order to recognize the common phases shared by all the presented models, in Table4 we have sorted the mentioned models based on naming them according to the issue year.

The next step is to extract all of the common phases within each of the investigation processes". It is clear that some of the phases do include duplication or overlap each other. "Bearing in consideration functions performed in each of the phases, and not depending only on the real naming", we have detected that these phases can be assembled in five groups (rows). These activities may not always be in this grouping assign one to another between them in the current models proposed in paragraph 3. In some cases, despite the fact that a similar process and the terms used in current models differ, Table-5shows how they share phases

**Table 4**-Existing Digital Forensic Investigation Models/Frameworks (2001-2010)

| Code of Model | Name of Model/Framework | Authors | No of Phases |
|---|---|---|---|
| M2001 | DFRWS Investigative Model | Palmer | 7 classes |
| M2002 | Abstract Digital Forensic Model | Reith, Carr, & Gunsch | 9 phases |
| M2003 | Integrated Digital Investigation Process | Carrier & Spafford | 17 phases |
| M2004 | Enhanced Digital Investigation Process Model | Baryamureeba & Tushabe | 21 phases |

| | | | |
|---|---|---|---|
| M2005 | A Hierarchical Objectives-Based Framework for the Digital Investigations Process | Beebe & Clark | 6 phases |
| M2006 | Framework for a Digital Forensic Investigation | Michael Kohn, JHP Eloff, and MS Olivier | 3 stages |
| M2007 | A Common Process Model for Incident Response and Computer Forensics | Freiling & Schwittay | 3 phases |
| M2008 | New Digital Forensics Investigation Procedure Model | Yong-Dal Shin | 10 phases |
| M2009 | "Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)" | Sundresan Perumal | 7 stages |
| M2010 | Network Forensic Generic Process Model | **Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi** | 9 phases |

The rows from the analysis shown in Table5 reveals, most of the frameworks/models in the first row consist of the **preparation** phase. Functions are performed in this phase for all actions that are required to be implemented before the effective investigation and official data collection, management support and monitoring authorization is obtained authorization to conduct the investigation, etc. Having a thorough preparation phase increases the quality of evidence and minimizes the risks and threats associated with an investigation.

The second row, the **collection and preservation** is dominant and represents the largest percentage of the phases entering in the models. This phase consists of extracting evidence from external storage media. In addition, it prevents the people from the use of electronic devices and machines digital device or allowing the use of other electromagnetic devices within a radius affected.

The third row highlights the **examination** and **analysis** phase clearly in six of the existing models. It is the core of the digital forensic investigation processes. This phase reveals information extracted from the available evidence by examining its contents, which is very important to establish the case. The contributed results from analyzing the collected physical and digital evidence are organized and analysis repetitions are eliminated. The results of analysis should be completely and accurately documented.

"The fourth row has the greatest number of phases in the groups, thus the focus of most models reviewed is indeed on the **presentation and documentation** phase". Documentation is included with the presentation because the third phase in the model of 2007 referred to above gives great importance to documentation, lets call this phase **documentation** phase. The importance of this phase is due to that it satisfies the key requirement specification defined by the word 'forensic' [18]. Presentation phase of the investigation should prove the validity of the hypothesis reached during the investigation. The physical and digital evidence must be clarified, documented and submitted to the court.

Even though it does not have in the last row represents the largest percentage, or prevailing also note the presence of a few phases in this row, but possible be shared with **review** and returning, and we chose the first term. The outcome of this phase could be new measures, new training, or nothing if all gone according to plan actually. In addition, the review of the investigation is to determine areas for improvement now and in the future.

"Therefore, a good framework should consist of all-important phases: Preparation, Collection and Preservation, Examination & Analysis, Documentation, and Review".

**Table 5-**Common Process with Different Phases &Models

| M2001 | M2002 | M2003 | M2004 | M2005 | M2006 | M2007 | M2009 | M2010 |
|---|---|---|---|---|---|---|---|---|
| | **Preparation & Approach Strategy** | **Readiness** | **Readiness** | **Preparation & Incident response** | **Preparation** | **Pre-Analysis** | **Planning** | **Preparation& incident response** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Preservation& Collection & Identification** | **Preservation& Collection & Identification** | **deployment** | **Deployment** | **Collection** | | **Pre-Analysis** | **Identification & Result** | **Preservation& Collection** |
| **Analysis & Examination** | **Analysis & Examination** | **Digital crime scene Investigation & Physical crime scene Investigation** | **Trace back & Dynamite** | **Analysis** | **Investigation** | **Analysis** | **Analysis & Reconnaissance** | **Analysis & Examination** |
| **Presentation& Decision** | **Presentation** | | | **Presentation** | **Presentation** | **Post-Analysis** | **proof & defense** | **Presentation** |
| | **Returning Evidence** | **Review** | **Review** | **Incident closure** | | | **Archive storage** | |

**Securing Phase:**

We have recognized that all the considered models do not consider any security procedure in securing the collected evidence (data), as it's important to deliver a reliable evidence in the court. Consequently, as the title of this study is including digital forensic therefore we will introduce a robust implementation of evidence (data) securing based on cryptography libraries.

Mentioning cryptography there are a wide variety of cryptography algorithms (DES, 3DES, AES) Hash functions (MD4, MD5, SHA1, SHA2 family) combining some we aim to provide the court with reliable evidence. In case to detect if, the evidence has been modified or manipulated.

Using timestamp, location, data file log are some file data's that are considered in the securing procedure [19].

The Data Encryption Standard (DES) works based on 56 bit block, in 1997 by a group of computer scientists have been cracked within 24 hours and the 3DES is encrypting each block of data with DES algorithm three times where the Advanced Encryption Standard (AES) adopts key lengths of 128, 192 and 256 bits which leads to a higher robustness. Bruce Schneier's states that breaking 11 rounds out of 14 full rounds of AES by having the related multiple keys of encrypted plain text takes $2^{70}$ time therefore we consider AES algorithm for encrypting [20].

Another method is Hash function, which produces a fingerprint of the data. By this function it is easy to detect if a single bit of the evidence file has been modified that is because a different fingerprint will be generated. There are different algorithms of HASH, which are based on the block size of operation and number of characters for the output. Some of these algorithms are MD5, SHA1, SHA2 family (SHA224, SHA256, SHA384 and SHA512) operates respectively on block size 128, 160, 224, 256, 384, 512 and the number of output characters respectively are 32, 40, 56, 64, 96 and 128, where through the different available methods we consider the SHA 512 as it offers a wider range of possible unique outputs for each input which supports avoiding collision and rainbow tables,

Another encryption/decryption system that supports both symmetric and asymmetric is Gnu Privacy Guard (GnuPG) where it adopts Public and Private Key that uses AES for encryption/decryption and RSA for key exchange protocol.

Based on this section we suggest that the framework includes the digital evidence protection through the following procedure.

Evidence (data file – any type) (1) Hash (File), (2) HASH (File HASH + Timestamp + GPS), (3) Encrypting + signing using Gnupg.

In this procedure to robust the evidence from manipulation we consider the timestamp and location GPS (Global Position System) then Hashing, encrypting and signing it.

In Figure-1 we presents the diagram of the flow of evidence data being secured considering the mentioned algorithms above. Figures-(2), (3), (4) presents the outlook of data passing throw the defined securing procedure.

**Evidence Hash file content:**

Line 1,2- Evidence file hash
Line 4- Timestamp
Line 5, 6- GPS

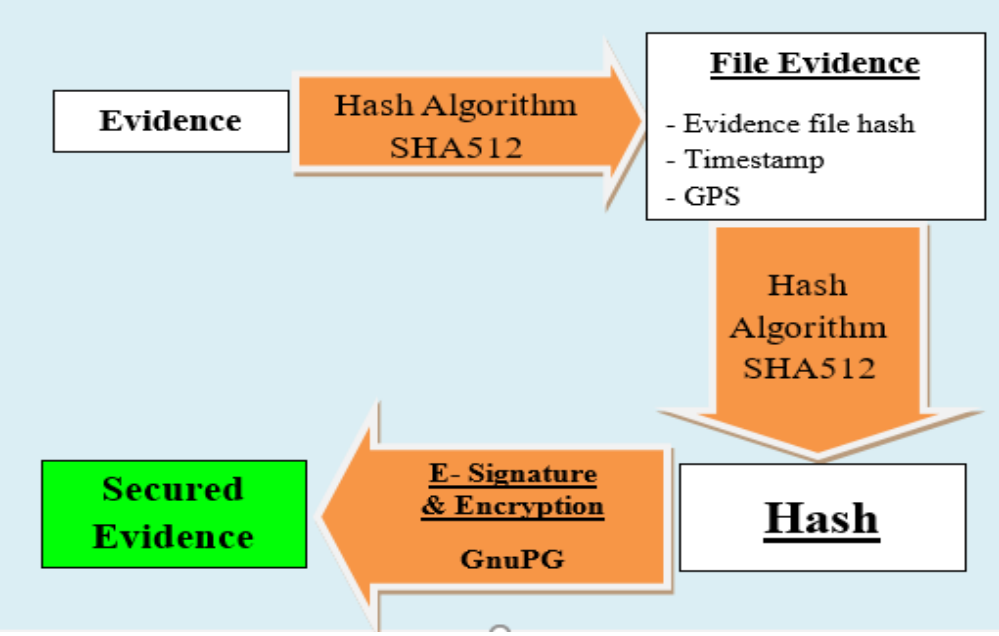


**Figure 1**-Evidence Securing Diagram

```
1 c56ef8473c6aee95607e921287d8aa6b9d8abf6d94ea4d9645fc4a104ba8e879
2 9ca07a85982adffc79c89d3124f1aa1da1d1a610a1b58f7f9d951a8c5fa0b1cf
3
4 Oct  1  2014 2014.09.29
5 Latitude: 33.28183917738964
6 Longitude:44.38163280737058
```

**Figure 2**-Evidence hash file content

**62ea1c8f38b131b8d62c570cef356eb631d530b77f6835fdc264816a0528643bbe8c5e3986c32cff6c783e2209046b50eeb55cab776892d48801d3e5f5e47735**

**Figure 3**- Hash (Evidence Hash file)

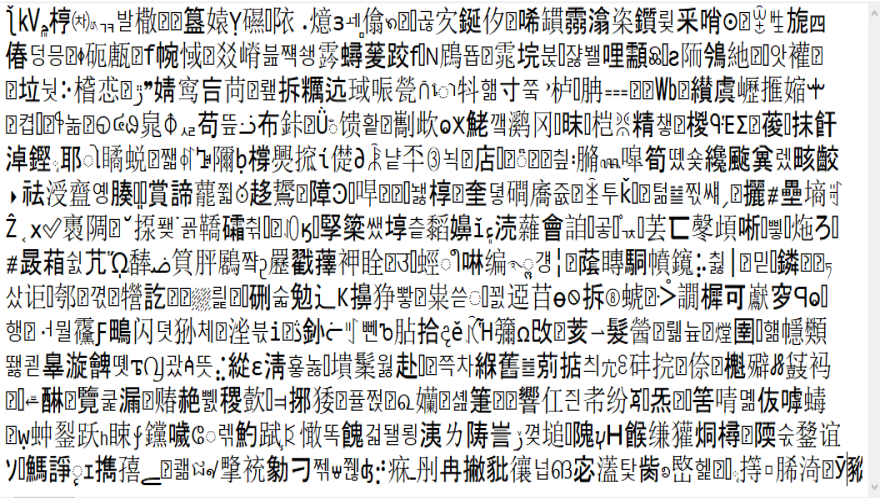

**Figure** 4-Signed and Encrypted by GnuPG

**Conclusions:**

The digital crimes are increasing each year in worldwide. Technology and sciences development, including users computerized knowledge increments and software changes has lead the criminal users to commit sophisticated crimes.

"In practices related to digital forensic investigation, there are more than hundreds of digital forensic investigation models developed all over the world. Most organizations have to develop their own models where some are focused on the technology aspects such as data acquisition or data analysis. Most defined and developed models are introduced to tackle the technologies used in the inspected device. Consequently, when devices technology changes, new models are required to be developed".

It has been more than 10 years that the paper related to (DFRWS) has been published and it is obvious that working in this field is getting more difficult and challenging.

The presentation to many models in section three it was introduction to discussion which done in section four to find a process common which occurs inside different models. Each model, despite their differences, has quite a lot in common with other models.

In this paper the aim is to merge all the phases with similar procedure and output result and we have contributed a six phase model. "Based on the analysis, most of the frameworks consist of some critical phases which are: Phase 2 – Collection and Preservation, Phase 3 – Examination and Analysis, and Phase 4 – presentation and documentation except Phase 1 and Phase 5 or except Phase 1 and Phase 4. Even though, Phase 1 and Phase 5 are not included in some of the framework, to guarantee that the investigation process is done completely both of these phases are important".

Some frameworks aim to define a model that could be capable of linking some particular procedures, it is known that major issue in this field is the gap between judicial process and technical aspects of digital forensics where the existing procedures are not able to deal with this

Studying the previous proposed frameworks reveals there is an overlap between some of the stages where the terminology is the main reason of difference. There may not always be a one-to-one mapping between the activities in the mentioned models. In some existing models there is a difference between the used terms but there is similarity in the process.

So far, we can say with confidence that these models are basically ad hoc, and there is much to be done in this particular field.

Based on our finding we contribute the following framework that adopts a new phase not existing in other frameworks which is located as Phase 3. This framework is consist of six phases as follow in Table-6

**Table 6**-Digital Forensic Framework considering securing Evidence

| Phase | Name |
|---|---|
| 1 | Preparation |
| 2 | Collection and Preservation |
| 3 | Securing evidence |

| | |
|---|---|
| 4 | Examination and Analysis |
| 5 | Documentation |
| 6 | Review |

**References:**


1. Kent K., Chevalier S., Grance T. and Dang H. **2006**. Guide to integrating forensic techniques into incident response. *NIST Special Publication*. 2006 Aug; **10**(14): 800-6
2. Aanya-Isijola A. **2009**. Models of Digital Forensic Investigation. 2009; Available from: www.scribd.com.
3. McCombie S. and Warren M. **2003**. Computer Forensic: An Issue of Definitions. In Australian Computer, Network & Information For .ensics Conference 2003 Nov
4. Shin YD. **2011**. New Model for cyber crime investigation procedure. *Journal of Next Generation Information Technology*. Volume. 2011 May; **2**(2).
5. Selamat SR., Yusof R., Sahib S., Hassan NH., Abdollah MF. and Abidin ZZ. **2011**. Traceability in digital forensic investigation process. In2011 IEEE Conference on Open Systems 2011 Sep 25 .IEEE .(106-pp. 101)
6. Johan S. **2012**. Towards an Automated Digital Data Forensic Model with specific reference to Investigation Processes MSc. Thesis, Department of Computing and Information Science, Auckland University of Technology.
7. Reith M., Carr C. and Gunsch G. **2002**. An examination of digital forensic models. *Int. J. Digit. EVid.* **1**(2002):1-12.
8. Pollitt MM. **2007**. An ad hoc review of digital forensic models. Conference: Second .IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2007 ,12-Seattle, Washington, USA, April 10 ,2007.
9. Carrier B. and Spafford EH. **2003**. "Getting Physical with the Digital Investigation Process." *Int. J. Digit. EVid*. **2**(2): 1-22.
10. Ademu IO., Imafidon CO. and. Preston DS. **2011**. A new approach of digital forensic model for digital forensic investigation. *Int. J. Adv. Comput. Sci. Appl*. 2011; **2**(12): 175-.8
11. Schmid JA. **2001** . Guard Architecture for Application Portability. Fuentez Systems Concepts Inc Fairfax VA; 2001 Jun.
12. Pilli ES., Joshi RC. and Niyogi R. **2010**. Network forensic frameworks: Survey and research challenges. *Digital Investigation*. 2010 Oct 1; **7**(1-2): 14-27.
13. Beebe NL. And Clark JG. **2005**. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, **2**(2): 147-167.
14. Köhn, Michael, M. Olivier and J. Eloff. **2006**. "Framework for a Digital Forensic Investigation." *ISSA* (2006). In ISSA (pp. 1-7).
15. Freiling F. and Schwittay B. **2007**. A common process model for incident response and digital forensics. Proceedings of the IM.F2007. 2007 Sep
16. Shin YD. **2008**. New digital forensics investigation procedure model. 2008 Fourth International Conference on Networked Computing and Advanced Information Management, pp. 528-531, Sep. 2008.
17. Perumal, S. **2009**. Digital Forensic Model Based on Malaysian Investigation Process International Journal of Computer Science and Network Security, **9**(8): 38-44
18. Abbas TM. **2015**. Studying the Documentation Process in Digital Forensic Investigation Frameworks/Models. .162-153:(4)**18** ,*Nahrain University-Journal of Al*
19. Talib MJA. **2018**. Adoption of Chain of Custody Improves Digital Forensic Investigation Process. *Iraqi Journal of Information and Communications Technology*(IJICT), **1**(2): 12- 21.
20. Altaher AS. And Taha SM. **2017**. Personal authentication based on finger knuckle print using quantum computing, *International Journal of Biometrics*, **9**(2).