Studying the Documentation Process in Digital Forensic Investigation Frameworks/ Models

Talib M. Jawad Abbas
College of Information Engineering, Al-Nahrain University.

Abstract

With the proliferation of the digital crime around the world, there are numerous and diverse digital forensic investigation models for driving digital investigation processes. Now more than ever, it must be a criminal investigation to obtain digital evidence which wouldn't be admissible in court. Therefore, digital forensic investigation should be implemented successfully, and there are a number of significant steps that should be taken into account. Each step and phase produces documents that are essential in understanding how the investigation process is built.

The aim of this paper is to study models/ frameworks for the digital forensic investigation over a time period of ten years and find out the degree and level of attention to the process of documentation. This paper also includes definitions and descriptions of the basic and core concepts that the frameworks/ models use.

Keywords: Forensics, Digital Forensic, Framework, Models, Documentation, Digital Investigation.

Introduction

Over the past few years, a new type of crime scene has become more predominant, that is crimes committed within digital domains. Increasingly, criminals are using technology to facilitate their offenses and avoid new challenges for confinement by law enforcement agents, forensic examiners, and corporate security professionals.

Law enforcement is in a perpetual race with criminals in the application of digital technologies, and requires the development of tools to systematically search digital devices for pertinent evidence. Another part of this race, and perhaps more crucial, is the development of a methodology in digital forensics that encompasses the forensic analysis of all genres of digital crime scene investigation [1].

Although this paper focuses more on documentation of digital forensic investigation, it is recommended that all personnel involved become aware of formalized digital crime scene investigation methodologies. Therefore, the second benefit of this paper is to provide knowledge on the development of many frameworks in the field of digital forensic investigations during the ten years from 2001 to 2010.

Documentation is an essential element of crime scene investigation as well as the forensics process. Throughout this paper the reader will be alerted to and reminded of the importance of complete narrative documentation.

The paper is structured as follows: the subsequent section will clarify important terminology used in the field of forensics; the third section will briefly discuss some generally accepted models; section four will review models of digital forensic investigation, and documentation process will be confirmed in section five. Conclusions and recommendation are given in section six.

Digital Forensics

Before describing the investigation process, we need to define the basic and fundamental terms. According to the Oxford Dictionary, the word forensic is defined as "relating to or denoting the application of scientific methods to the investigation of crime" and "of or relating to courts of law" [2]. Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive [3].

In this modern age, several types of digital devices, not just computers are used on a daily basis and are constantly exploited for criminal activity. **Computer forensics** focuses on extracting evidence from a particular platform (Computer), **digital forensic** covers extracting

evidence from all forms of digital evidence. Digital forensics is the collection, preservation, analysis and presentation of digital evidence extracted from any source of digital evidence that can be used to identify criminal activities or other activity that constitutes violation [4]. Digital forensics is an investigation to answer questions [5]. One important element of digital forensics is the credibility of the **digital evidence**. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines, etc [6].

Digital forensic processes and procedures have to be followed in order to preserve and present the final evidence of an identified incident or crime. In order to achieve this, we will first introduce the term Digital Forensics, as it is defined by Kruse and Heiser [7]: "Preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/ or root cause analysis". Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity, not just computer systems [1].

The Oxford Dictionary defines a **framework** as "a supporting or underlying structure" [2]. A framework for digital forensics needs to be flexible enough so that it can support future technologies and different types of incidents [8]. The framework is an adaptation or combination of several existing forensic models. **Digital Forensic Investigation Framework (DFIF)** can be defined as a structure to support a successful forensic investigation. The purpose of digital forensic investigation frameworks is to inform, shape, and standardize digital forensic investigations. Unfortunately, there does not exist a standard or consistent digital forensic methodology, but rather a set of procedures and tools built from the experiences of law enforcement, system administrators, and hackers [1].

Existing Digital Forensic Investigation Models/ Frameworks

A good digital investigation model must be based on a consistent and standardized framework that supports every stage of the investigation (technical and non-technical) regardless of the type of crime [3]. Presently there are several digital forensic investigation methodologies developed to assist law enforcement in dealing with the digitally-based evidence. The review which will only focus on the number of forensic models that have been proposed reveals the role of documentation process in digital forensic investigation models or frameworks as in Table (1),(2),[9],[10],[11],[12],[13],[14],[15],[16],[17],[18],[19],[20] and [21].

Table (1)
Existing Digital Forensic Investigation Frameworks/Models (2001-2010).

DFRWS Palmer Model 2001 (7 class)	***Reith, Carr, and Gunsch M0del 2002 (9 phase)***	***Brian Carrier and Eugene Spafford 2003 (5 group)***	***Carrier & Spafford model 2004 (5 phase)***	***Beebe, N. l., & Clark, J. G Model 2005 (6 phase)***
Identification	identification	readiness (2 phases)	readiness (2 phases)	✓ preparation
Preservation	preparation	deployment (2 phases)	Deployment (2phases)	✓ incident response
Collection	approach strategy	physical crime scene investigation ✓ (6phases)	physical crime scene investigation ✓ (2phases)	✓ data collection
Examination	preservation	digital crime scene investigation ✓ (6phases)	digital crime scene investigation ✓ (9 phases)	✓ data analysis
Analysis	collection	review phase	Presentation	✓ presentation
✓ Presentation	✓ examination			✓ incident closure
Decision	analysis			
	presentation			
	returning evidence			

Continue

Michael Kohn, JHP Eloff, and MS Olivier Model 2006 (3 stage)	***Freiling, F. C., & Schwittay, B Model 2007 (3 phase)***	***Yong-Dal Shin M0del 2008 (10 phase)***	***Sundresan Perumal Model 2009 (7 stage)***	***Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi M0del 2010 (9 phase)***
✓ preparation	Pre-Analysis	investigation preparation	Planning	preparation
✓ investigation	Analysis	classifying cyber crime and deciding investigation priority	Identification	detection
✓ presentation	✓ Post-Analysis	investigating damaged (victim) digital crime scene	reconnaissance	incident response
		criminal profiling consultant and analysis	analysis	collection
		tracking suspects	result	Preservation
		investigating injurer digital crime scene	proof & defense	Analysis
		summoning suspect	archive storage	investigation
		additional investigation		✓ presentation
		✓ writing criminal profiling		
		✓ writing report		

Table (2)
Evaluation of Documentation Stages/Phases/Sub-phases in Those Existing Models/ Frameworks.

Code of Model	***Name of Digital Forensic Investigation Framework/Model***	***Place & Role of Documentation Found in Model/Framework***	***Evaluation Degree/Level***
M2001	Digital Forensic Research Conference (DFRWS) Investigative Model	The DFRWS report does not discuss the steps of the model in great detail but for each step a number of relevant issues are listed, e.g. for *presentation*. The relevant issues are documentation, expert testimony, clarification, mission impact statement, recommended countermeasure and statistical interpretation.	**Good**
M2002	Abstract Digital Forensic Model	The model just in *examination* phase will construct detailed documentation for analysis phase.	**Good**
M2003	Integrated Digital Investigation Process	The **Documentation Phase** of the physical crime scene (third group) involves taking photographs, making sketches, and videos of the crime scene and the physical evidence. On the other hand, the documentation Phase of the digital crime scene (fourth group) involves properly documenting the digital evidence when it is found.	**Very good**
M2004	Event-based Digital Forensic Investigation	As in framework above proposed by **Carrier and Spafford** in 2003, they put documentation phase in group three and four (physical crime scene investigation phases and digital crime scene investigation phases).	**Very good**
M2005	A Hierarchical Objective-Based Framework for the Digital Investigations Process	Proper documentation is an example of a process whose goal is to permanently (or semi-permanently as applicable) record all information relevant to and/or generated during the digital investigative process to support decision making and the legal, administrative measures, etc.	**Excellent**
M2006	Framework for a Digital Forensic Investigation	Herein, the documentation is presented in all steps.	**Excellent**
M2007	A Common Process Model for Incident Response and Computer Forensics	The *Post-Analysis* Phase is first of all concerned with documentation of the whole activities during the investigation.	**Good**
M2008	New Digital Forensics Investigation Procedure Model	This model presents a new methodology of a digital forensics procedure, but does not explicitly identify the documentation process in investigations. In this writing report phase, documentation is reviewed, summaries are written, and documentation is finalized as reports.	**Poor**
M2009	Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)	Although this model focuses on data mining in the stages of archive storage, it does not explicitly identify the documentation process in investigations.	**Poor**
M2010	Network Forensic Generic Process Model	Herein, the documentation is presented just in presentation phase and its function to meet the legal requirements and also entire case is documented to influence future investigations and to provide feedback to guide the deployment and improvement of security products.	**good**

Review of Digital Forensic Investigation Frameworks

A review is presented of the prevailing digital investigation process models proposed by various authors. Based on the observation we made some models are going to apply the process of documentation in a very specific scenario, whereas others may be applied more widely. Some of the models tend to be specified to the details and other models are very general.

It has been approved the ratings of the processes of documentation in the models presented in Tables (1 & 2) are as follows: the degree (poor) has given for the model that puts the documentation within the phase, but not within the phase stand-alone. The models that place the documentation in a single phase are evaluated (good), which is more than one phase to degrees (very good). Finally, the models that got the full mark (excellent); placed documentation facilities for all phases of investigation which is the right picture process to ensure the credibility of the investigative work.

Documentation is a continuous loop activity, required in all the stages of the investigation. Next section covers in detail the importance of the process of documentation frameworks and models presented in the previous paragraph.

Need to Apply the Process of ocumentation in the Investigation

Documentation is fundamental at all phases of dealing with and processing digital forensic investigation. To see how documentation process can be done in digital forensic investigation, we first look into definition of documentation and second explain role of documentation process in digital and physical crime scene; later, we will present preference between documentation paper and electronic in digital forensic investigation process.

Definition of Documentation

Before describing the documentation process, we need to define it. Documentation is defined as "a means of describing an existing investigation process with graphics, words, or a combination of the two". The documentation can be prepared manually or with the use of a computer, and the medium can be paper or magnetic storage [23]. Simply providing specialist forensic and court of law documentation, regardless of source, may not be enough, however. It is believed that the court of law also needs high-quality documentation. Some believe documentation should be as brief, as graphical, and as to-the-point as possible, and available when needed [24].

Documentation Process

The goal of the documentation process is to permanently (or semi-permanently as applicable) record all information relevant to and/or generated during the digital investigative process to support decision maker, and the legal, administrative, etc in processing of those decision [16]. So much of the process of forensic investigation depends on good documentation, and forensic investigation professionals can spend as much as 50-75% of their time writing up administrative and research reports. Much of the legal process depends on the careful documentation that records crucial information.

Documentation is a continuous process throughout the investigation process. It is important to precisely record location and status of computers, storage media, other electronic devices, and traditional evidence, although there are overlaps and similarities in the digital and physical forensic investigation. Many criminal investigations will include computers at some point in the case. Murder and rape suspects may, through a search warrant, have their email and Internet activities analyzed to find evidence about their motives or hiding locations. Corporations investigate computers when an employee is suspected of unauthorized actions. Fraud investigations collect transaction history evidence from servers [13]. But it is important to highlight some of the differences that distinguish implementation of the process of documentation from the process of digital and physical investigation. The laws of nature are related to the material world, while the instructions in the hardware and software are associated with the digital world. Physical crime scene investigation uses the laws of nature to find physical evidence at the crime scene and investigation of the digital code is

used to find digital evidence. The digital crime scene can be considered a secondary crime scene to the physical crime scene. So we will try in the paragraphs below, to explain each of them independently and then in the end will create a table for comparison of the increased interest.

Physical Crime Scène Documentation

The documentation of the physical crime scene involves note taking, photographs, sketches, and videos of the crime scene and the physical evidence. All four are necessary and none is an adequate substitute for another. For example, notes are not substitutes for photograph. For limitations of space two of these four referred to above will be covered. Notes as a part of the effective investigation provide written record of all activities in the crime scene. The notes are taken as the activities that are made to prevent possible memory loss if notes are made at a later date.

The objective of still photography documentation of the crime scene is to provide an honest and accurate picture record of the crime scene and physical evidence is presented. Photography is perhaps the most important form of crime scene documentation, producing a permanent visual record of the crime scene and discovered evidence [25].

The goal of documentation is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded. It could also be important to document the number and size of the hard drives and the amount of memory [13]. Examples of physical evidence that are identified in the documents contain the position of the mouse and the number and location of computers, and location of components relative to each other and also documentation of the case and the location of the computer system, etc. Similarly, in situations where there are several identical computers with identical components, documenting serial numbers and other details is necessary to specifically identify each item. Documenting the original location of evidence can also be useful when trying to reconstruct a crime. When multiple rooms and computers are involved, assigning letters to each location and numbers to sources will help keep track of item [26].

At the end of this paragraph emphasis is placed on the scientific and legal requirements, the first part of the legal requirements is not the subject of this research, but the second part, is a necessary link between notes, photographs and sketches, to achieve better results in the reconstruction of the original scene conditions and events. Also, the need for innovation and originality, for the effective translation of a crime requires not just the traditional means of documentation mentioned above, but rather it is believed to use of digital imaging technology or other sophisticated tool at the crime scene.

Digital Crime Scène Documentation

In recent years an important progress has been achieved in the digital documentation of crime scenes. Processing and documentation have been made more efficient and now provide complete, 360 degree, and even 3D documentation of the crime scene.

The documentation of the digital crime scene involves properly documenting the digital evidence when it is found. The exact copy of the system has the same role as the sketches and video of a physical crime scene. Each piece of digital evidence that is found during the analysis of the image must be clearly documented [13]. A record of all visible data must be created, which helps in recreating the scene and reviewing it at time. This is particularly important when the forensic specialist has to give a testimony in a court, which could be several months after the investigation [6]. For example, a file can be documented using its full file name path, the clusters in the file system that it uses, and the sectors on the disk that it uses. Network data can be documented with the source and target addresses at various network layers.

Finally, the need requires proper documentation of the digital crime scene and physical crime scene perspectives. And different forms of camera/video photography, graphics are used, and notes are made on the document and all relevant information relating to the crime scene. Documentation at the scene is also the starting point for the chain-custody. Table (3) gives a comparison between the physical crime scene documentation and digital crime scene documentation.

Table (3)
Comparison between Physical Crime Scene Documentation and Digital Crime Scene Documentation.

Physical Crime Scène Documentation	*Digital Crime Scène Documentation*
Physical evidence has existed for thousands of years.	Digital evidence has recently become more common.
Documentation aims at producing a permanent, objective record of the scene, of the physical evidence and of any changes that take place.	Documentation aims at producing permanent, objective of the scene of each piece of information on digital evidence found.
Physical evidence (the actual computer, hard disk, PDA, and CD-ROM).	Digital evidence (the data in memory, on the hard disk, or in a cell phone, etc).
The laws of nature bind the physical world.	The instructions in hardware and software bind the digital world.
Documenting the physical evidence by the sketches and vides and other.	Documenting the digital evidence by exact copy of the system.
All items that are used to document are non-volatile	Most items that are documented are volatile data and there is always a possibility for the perpetrator to erase them.
The time within which the evidences are secured is less important.	The time within which the evidences are secured is more important.

Differentiation between Paper and Electronic Documentation

As this research talks about documentation in forensic investigation models, it is logical to research as well in choosing the suitable medium in documentation, if the medium is paper or a medium employing modern digital technology. Therefore, the explanation in the following lines includes introduction, with a comparative table.

Historically, paper-based documentation has held several advantages over its electronic counterpart. Specifically, paper - based documentation is seen to offer superior portability, readability, availability, and ease-of-use. Electronic documentation, on the other hand, offers some important technology-based advantages including cross - referencing, indexing, and searching. Media choice is therefore largely a function of document purpose and user preference [26]. Given that technology and user preferences continue to evolve, this comparison is worth re-examining.

Table (4)
Comparison Between Paper-based Documentation and Electronic Documentation.

Paper-based Documentation	*Electronic Documentation*
It is still important.	It is becoming more important.
It is simpler to use because it is more familiar to users, especially for novice who has less computer experience.	It requires the users to learn one more set of commands.
Also is easier to flip through to gain a general understanding of its organization and topics and can be used far away from the computer itself.	Searching for information is often simpler because the user can type in a variety of keywords to view information.
It is possible in paper documentation the same information can be presented in many different formats, but the cost and size of the resulting manual make it impractical.	The same information can be presented several times in many different formats with minor additional cost.
The paper documentation significantly expensive to distribute.	It is significantly less expensive to distribute.
For good - quality documentation, process usually takes about three hours per page (single-spaced).	For electronic documentation, process takes two hours per screen.

The Table (4) leads to the conclusion that the transition to electronic documentation is one of technological change that has

significant implications for the digital forensic investigation processes. This method of documentation can assist investigator in addressing problems that occur as a result of paper-based documentation. It can also improve the accuracy and comprehensiveness of crime scene investigation information and enhance the provision of quality chain of custody.

Conclusion and Recommendation

From the digital forensic investigation perspective, the proposed models/ frameworks have clearly shown that the documentation process will lead to a fair prosecution as the very most important stages such as volatile non-volatile data acquisition is actually documented. An investigation process that does not have adequate documentation is virtually impossible to handle and maintain.

Based on the presented digital forensic investigation processes, one is able to extract the documentation process from all framework/ models.

These are offered for the purpose of models and frameworks to find out which of them pays appropriate attention to on the process of documentation in the digital forensic investigation. it has emerged from this account and detailed study, that there is a clear disparity between them, in some of them the expansion and development of documentation are implicit in all phases (they are few), in some they are placed in specific phases, but are not referred to more clearly, and the other does not refer to them closely, as previously shown in the Tables (1&2).

It is recommended those designers of frameworks/models and all the investigators focus on documentation and gives attention to the level of the parallel gathering of evidence, and not leaves the duty of documentation after completion of digital forensic investigation phases. This time is lag between development, of activities and the production of documentation of these activities leads to poor quality documentation.

Also, the quality of documentation will improve if these guidelines are followed :(1) Document Organization; the document should be clearly structured as a table of contents, and indexes…etc. (2) Document Length; make documents as short as possible. (3) Overall Appearance; make the document look as professional as possible. (4) Style and Comprehension; keep sentences short (no more than 25 words), avoid abstract and difficult words. (5) Represent Crime Scene; use pictures whenever possible to represent crime or incident. (6) Photographs; use photographs for presenting overall context.

Lastly, the documentation must be written, because judges may not be familiar with specific digital forensic technique.

References

[1] Mark Reith, Clint Carr, Gregg Gunsch, "An Examination of Digital Forensic Models", Department of Electrical and Computer Engineering, Graduate School of Engineering and Management, Air Force Institute of Technology, right-Patterson AFB, OH 45433-7765, International Journal of Digital Evidence, Fall, 1-6, 2002.

[2] Michael Kohn, JHP Eloff, and MS Olivier, "Framework for a Digital Forensic Investigation", Information and Computer Security Architectures (ICSA), Department of Computer Science, University of Pretoria, 2-6, 2006.

[3] The United States Computer Emergency Readiness Team (US- CERT), Produced, Online, www.us-cert.gov/ reading_room/ forensics.pdf 1, 2008.

[4] Sanya-Isijola, Ademuyiwa, "Models of Digital Forensic Investigation", www. scribd.com ‹ Research ‹ Science 1, 2009.

[5] Brian D. Carrier, "A Brief Introduction to the Computer History Model", www. digital-evidence.org/hist_model.١html, 1, 2008.

[6] Ankit Agarwal, Megha Gupta, Saurabh Gupta & Gupta S.C. Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security (IJCSS), (5) (1), 119, 2011.

[7] Anders Orsten Flaglien, "Cross-Computer Malware Detection in Digital Forensics", Master's Thesis, in Information Security, ECTS30, Department of Computer Science and Media Technology, Gjøvik University College, 7, 2010.

[8] Carrier, B., Spafford, E. H., "An Event-based Digital Forensic Investigation

Framework", Proceedings of Digital Forensics Research Workshop, Baltimore, MD, 2, 2004.

[9] Digital Forensics Research Workshop (2001), "A Road Map for Digital Forensics Research", DTR - T001-01 FINAL, Utica, New York, Document authored from the collective work of all DFRWS attendees by: Gary Palmer, The MITRE Corporation, www.dfrws.org, 2001.

[10] April L. Tanner & David A. Dampier, "An Approach for Managing Knowledge in Digital Forensic Examinations", International Journal of Computer Science and Security, (IJCSS), 4(5), 1, 2009.

[11] Siti Rahayu Selamat, Robiah Yusof and Shahrin Sahib, "Mapping Process of Digital Forensic Investigation Framework", Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka, Ayer Keroh, Melaka, Malaysia, IJCSNS International Journal of Computer Science and Network Security, 8, (10), 164, October 2008.

[12] Daniel A. Ray, Phillip G. and Bradford, "Models of Models: Digital Forensics and Domain-Specific Languages", Department of Computer Science, The University of Alabama, Box 870290, Tuscaloosa, AL . DanielRay@cs.ua.edu , pgb@cs.ua.edu, 2, 2007.

[13] Brian Carrier, Eugene H. Spafford, "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, 2, Issue 2, 1-11, 2003.

[14] Baryamureeba, V., Tushabe, F., "The Enhanced Digital Investigation Process Model", .Proceeding of Digital Forensic Research Workshop, Baltimore, MD, 8, 2004.

[15] Ciardhuain, S. O., "An Extended Model of Cybercrime Investigations", International Journal of Digital, Evidence, 3, Issue 1, Summer 2004.

[16] Beebe, N. l., Clark, J. G., "A Hierarchical Objectives-Based Framework for the Digital Investigations Process", roceedings of Digital Forensics Research Workshop Baltimore, MD, 2, 147-167, 2005.

[17] Kent, K., Chevalier, S., Grance, T., & Dang, H, "Guide to Integrating Forensic Techniques into Incident Response", NIST Special Publication 800-86 Gaithersburg: National Institute of Standards and Technology, 25-28, 2006.

[18] Freiling, F. C., Schwittay, B., "A Common Process Model for Incident Response and Computer Forensics", Proceedings of Conference on IT Incident Management and IT Forensics, Germany, 10-11, 2007.

[19] Yong-Dal Shin, "New Digital Forensics Investigation Procedure Model", Fourth International Conference Networked Computing and Advanced Information Management, 528-531, 2008.

[20] P. Sundresan, "Digital Forensic Model based on Malaysian Investigation Process", International Journal of Computer Science and Network Security (IJCSNS), 9, (8), citeseerx.ist.psu.edu/viewdoc/download...?, 2009.

[21] Emmanuel S. Pilli, Joshi R.C., Rajdeep Niyogi., "Network forensic Frameworks: Survey and Research Challenges", Digital Investigation, 7, Issues 1-2, October 2010, 14-27, 2010.

[22] Johan Scholtz, Ajit Narayanan, "Towards an Automated Digital Data Forensic Model with Specific Reference to Investigation Processes", Proceedings of the 8th ustralian Digital Forensics Conference, 147, 2010.

[23] Raymond McLeod, Jr, "Systems Analysis and Design", The Dryden Press, Harcourt Brace College Publishers, 730, 1994.

[24] Jeffrey A. Hoffer, Joey F. George, Joseph S. Valacich, "Modern System Analysis and Design", The Benjamin/ Cummings Publishing Company, Inc, 770, 1996.

[25] Forensic Science Central, "Crime Scene Investigation", p2, http://forensicsciencecentral.co.uk/, 2005.

[26] Eoghan Casey, "Digital Evidence and Computer Crime", Elsevier Academic Press, Second Edition, 218, 2004.

[27] Alan D, Barbara H., "System Analysis & Design", John Wiley & Sons, Inc, 417, 2000.

[28] Divinitus, "Online Versus Paper-based Documentation", published January 15, 2013. http://divinitus.ca/wp/online-versus-pap...-paper-based-documentation

الخلاصة

مع انتشار الجريمة الرقمية في جميع أنحاء العالم، ظهرت نماذج تحقيق جنائية رقمية متعددة ومتنوعة تدفع عجلة عمليات التحقيق الرقمية. الآن أكثر من أي وقت مضى، يجب أن تكون غاية التحقيق الجنائي الحصول على الأدلة الرقمية التي يمكن أن تكون مقبولة في المحكمة. ولذلك، ينبغي تنفيذ التحقيق الجنائي الرقمي بنجاح، وهناك عدد من الخطوات الهامة التي ينبغي أن تؤخذ بعين الاعتبار. وإن كل خطوة ومرحلة تنتج وثائق التي لا غنى عنها في فهم كيف يتم بناء عملية التحقيق أو سيتم بناؤها.

ان الهدف من هذا البحث هو دراسة نماذج/ أطر التحقيق الجنائي الرقمي خلال فترة عشر سنوات، ومعرفة درجة ومستوى الاهتمام بعملية التوثيق، ويتضمن أيضاً تعريفات وتوصيفات في المفاهيم الأساسية والجوهرية التي تستعملها الأطر/ النماذج.