AN INTEGRATED DATAFLOW BASED MODEL FOR DIGITAL INVESTIGATION

Che-Pin Cheng[1], Ruey-Shiang Shaw[2], Te-Chao Liang[3], Ta-Yu Fu[4]
[1]Information Management Department, Technology and Science Institute of Northern Taiwan
[23]Information Management Department, TamKang University of Taiwan
[4]Department of Management Sciences and Decision making, TamKang University of Taiwan
[1]james@mail.tku.edu.tw; [2]rsshaw@mail.tku.edu.tw;
[3]tcliang@mail.im.tku.edu.tw; [4]dyfu@mail.mcu.edu.tw

Abstract

This study developed a highly adaptive digital forensic model, applicable to various situations, which clearly describes the digital forensic process and their purposes as well as ensuring the exactness and effectiveness of digital forensic results. It examined the viewpoint of the digital evidence process flow throughout an entire forensic process, and it hoped to provide a complete explanation of the digital forensic procedure and the details of execution. In addition, it proposed three new forensic concepts: primary, supported and comprehensive forensic procedures. The structural hierarchy constructed in the model can be expanded, then divided into its simplest forms, allowing independent task assignments. It further proposed several innovative digital forensic concepts, such as a new feedback mechanism. Finally, this model could provide a detailed list of the resources necessary for an entire forensic activity, applicable to management planning. This model provided a practical description approach and established a comprehensive and uniform digital expression form. The aim is to accumulate and to share experience and knowledge, hoping to create more mature and practical digital forensic science and to provide a reference for the practitioners of digital forensics.

Keywords: digital forensic model, digital forensic procedure, forensic data, data flow, digital forensic process, systematic decomposing

Introduction

In the past forensic process of investigating human crimes, criminals would often leave behind original evidences; these traditional forensic procedures have matured through years of scientific examination and verification procedures [8]. The lack of uniqueness makes digital crimes and their evidences easy to duplicate and alter, which renders traditional forensic procedures and experiences unable to meet the contemporary demands of digital forensics [8]. For these reasons, there is an urgent global demand for advances in digital forensic technologies. Since 2000, researchers have continuously emphasized the significance and applicability of the digital forensic procedure from the field of digital forensic science. In order to speed scientific research in digital forensics, researchers endeavor to find a universal common forensic procedure in the near future. According to Reith and Carr, the procedures followed by forensic practitioners during the collection, examination, and forensic process have not been standardized with regard to cases of digital crimes [20]. Moreover, Pollitt pointed out that, instead of publication, most digital forensic researches and experiences are either published on the Internet, or communicated in organizational seminars; therefore, these procedures and experiences are not fully accumulated and discussed. The above mentioned conditions account for the current non-standardization of the digital forensic procedure [17].

This study applied the viewpoint of the digital evidence flow throughout an entire forensic process and proposed an integrated digital forensic model. Previous digital forensic studies focused only on the digital forensic procedure or partial concepts of forensics rather than on an integrated digital forensic model, which could comprehensively describe the details and steps of execution in the forensic process and avoid that do not know how to conduct follow-up. Such a complete model has never been published in past literature. This systematic model is able to meet the above mentioned demands as well as resolving the previous model's shortcomings of excessive conceptualization and lack of detailed execution procedures.

Furthermore, there are many other contributions in this study. It proposed three new forensic concepts: primary, supported and comprehensive forensic procedures. It proposed a creative and important feedback mechanism different form previous research, which can provide many details on the execution of said feedback to satisfy various situations. In this study, through

uniform explanations of proven processes, these characteristics allow a widespread expression of collated experiences and knowledge, thus establishing a practical sharing method in knowledge management for standardized procedure groups. It also proposed a digital forensic construction dictionary, which defines requirements for personnel, technology, location, and the resources necessary to complete a complex group of digital forensic processes, allowing practical, accurate budgetary estimations in financial management.

The research of digital forensic models is given in Section 2. Section 3 describes the proposed model and Section 4 discusses the impact of the model. Lastly, Section 5 presents the conclusions.

Digital Forensics

Digital forensics is commonly defined as the preservation, collection, identification, analysis, recording, and presentation of digital evidence through scientific acquisition and scientific verification methods, with the purpose of reconstruction of discovered cases of crime [8]. Hence, a comprehensive digital forensic processing framework, which can meet the above mentioned requirements, and be operated independently from any specific technology and environment, needs to be developed [20]. Within such a framework forensic practitioners of different organizations could discuss and share their forensic methods and experiences, and digital evidence forensic results could better comply with the principles of impartiality, integrity, and correctness.

Procedure-based digital forensic model

Present literature on digital forensic models shows that some studies are concentrated on “forensic procedure” models [1] [2] [3] [4] [5] [6] [7] [8] [11] [12] [15] [18] [20] [22] [24]. These studies focus on describing the guidelines and concepts of various procedures without detailing how these procedures are implemented and developed from different executive levels and perspectives. In addition, some studies have emphasized the concepts of digital forensic implementation [3] [4] [14] [16] [19] [23] [25], namely, exploring and discussing some details of digital forensic concepts and guidelines, rather than how to implement the digital forensic model. Some studies have proposed the concepts of dividing digital forensics into different hierarchies [2] [3] [8] [16] [25], but only addressed conceptualized viewpoints without proposing substantial practices. To summarize, there is a lack of a comprehensive digital forensic model that can completely describe the details of the digital forensic process and decompose the execution steps, while detailing the personnel, technology, locations, and resources required for the digital forensic process.

After reviewing the 16 most commonly seen digital forensic models of digital forensic research, this study selected commonly used procedures of the digital forensic procedure from each piece of research, as shown in Table 1.

Digital forensic process and implementation

Although the digital forensic procedure is important, erroneous or imprecise digital forensic implementation processes and methods may occur due to lack of a thorough understanding of the subsequent details of implementation, even though good digital forensic procedural steps are available. DFRWS defined the digital forensic procedure, and briefly described the scope of these procedures [8]. Although some implementation techniques were mentioned, the study still lacked detailed explanations of the steps of execution.

Previous studies focused on certain aspects, or viewpoints, without systematic and complete description of the digital forensic model. Such a situation means that practitioners are only aware of the concepts, resulting in flawed implementation details and steps, which lead to insufficient evidential power of the forensic results. For example, the “collection” procedure is mentioned by many digital forensic procedure models, but due to the unique characteristics of digital evidence (such as alterability, dissolvability, and duplicability), the question remains of how to show and validate the collected evidences. Thus, more details of the execution steps of the collection procedure should be shown, in order to guarantee the originality and undeniability of the evidence collected.

Table 1 The common digital forensic procedure in present research
Source: This study

Writer	Year	Pre-paration	Incident response	Recording	Collection	Exami-nation	Analysis	Presen-tation	Preser-vation
Pollitt	**1995**		V		V		V	V	
Lee	**2001**		V		V	V		V	V
DFRWS	**2001**		V		V	V	V	V	V
Chris	**2001**	V	V	V		V	V	V	
NCJRS	**2001**	V		V	V	V	V	V	V
Reith	**2002**	V	V		V	V	V	V	V
Casey	**2003**		V	V	V	V			V
Carrier	**2003**	V	V	V	V		V	V	V
Stephenson	**2003**				V	V	V	V	
Mocas	**2003**		V			V		V	
Baryamueeba	**2004**	V	V	V		V	V		V
Beebe	**2004**	V	V		V		V	V	V
Carrier	**2004**	V	V	V	V			V	V
Séamus	**2004**	V	V	V	V	V	V	V	V
Erbacher	**2006**			V	V		V	V	
Kent	**2006**		V	V	V	V	V	V	

Digital Forensic Model of Dataflow Base

A key point of digital forensics is the necessity, and correctness, of the evidence data process flow, but not the invariable processing procedures. The evidence data process flow begins with the collection of digital evidence data, and then each subsequent step, or processing procedure, is precisely linked to the previous step.

Gane and Sarson proposed using a “Data Flow Diagram” (DFD) for presenting the computer system data processing flow [9]. Likewise, the digital forensic process could also be presented, and described, using the DFD. Since the DFD has well-known semantic expression modes in the field of computer software development, it is conducive to promoting and understanding the digital forensics from an evidence dataflow perspective.

Séamus proposed this new viewpoint of the cybercrime investigation model based on information flow [8]. Basically, in DFD, either term - information flow or data flow – may be exchanged as they have similar meanings. This study will still use the term “data flow” for two reasons. First, this study describes and develops the digital forensic process by applying DFD expressions, and the term of data flow has become a customary and well-known term in the field of computer software development. Second, because what digital forensic processing needs to deal with is forensic data, it is possibly more proper to use data flow when describing digital forensic details at the bottom level.

Digital Forensic Dataflow Model

This study incorporated the DFD with some adjustment to fit the expression of the digital forensic model, in order to propose a dataflow-based integrated digital forensic model, as shown in Figure 1. This model is based on the evidence data process flow, with an execution scope able to cover time-flow procedures as well as describing the relationship or processing in detail between mediate evidence in each procedure and execution steps. This model can be expanded to clearly and specifically describe when, how, where, and by whom the digital forensic is implemented, and what evidence was discovered, through which tools and methods.

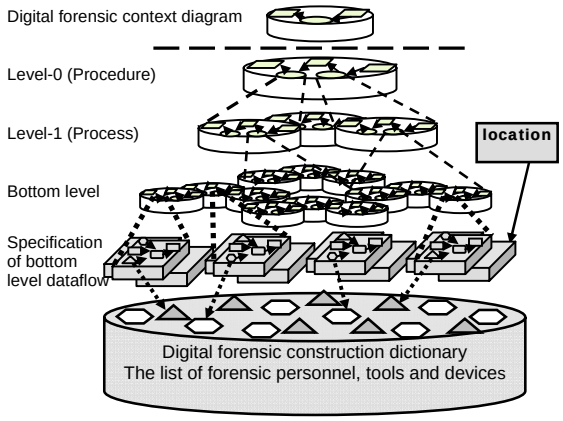

Figure 1 Dataflow-based integrated digital forensic model
Source: This study

In Figure 1, the evidence data, or mediate

evidence, is represented by a parallelogram; the procedure (or whole process) is represented by an elliptical symbol; the flow direction of evidence data is represented by an arrow; the development, or expansion, of each procedural phase is represented by a column. The digital forensic context diagram at the top of the figure is used to present the concept of the purpose of digital forensics, namely, applying forensic procedures throughout an entire process group, to collate the collection of digital evidence, which constructs a forensic evidence report.

Level-0 data flow is used to present the fully developed, or expanded, procedures necessary for the execution of an entire digital forensic activity, and explains which procedure needs to be executed, at which stage.

Level-N data flow is used to develop, and describe, which detailed steps should be taken for any given forensic procedure. This level-diagram is often used to provide more detailed task steps to the practitioners responsible for executing a forensic procedure.

Bottom-level data flow is used to further develop, and describe, the details of execution steps, as discussed in Level-N, and is aimed to develop each step into its simplest presentation form. The said "form" is simplified enough to clearly identify the personnel, locations, tools, and approaches used to carry out the forensic tasks, as well as the expected results, and can further evolve into the status of assignable units of task assignments.

After the completion of development, all bottom-level-dataflow in the digital forensic model is converted into the specifications of bottom-level-dataflow, and all resources, such as personnel, tools, devices, etc. can be listed and summarized to establish a digital forensic construction dictionary.

Level-0 Model Development

The level-0 data flow in this model is used to present the procedure perspective of fully developed digital forensics (Figure 2). Many scholars have proposed different digital forensic procedures in the past; however, no common forensic procedures have been compiled [21]. This study reviewed 16 research papers on digital forensic models (Table 1), to aggregate the eight most commonly seen procedures of research papers, and organized a complete digital forensic procedural path, which is sequentially based on the most recent forensic procedures. The proposed procedures include: preparation, incident response, recording, collection, examination, analysis, presentation, and preservation. In addition, this study add two necessary procedures, they are feedback procedure and acceptance and handover procedure.

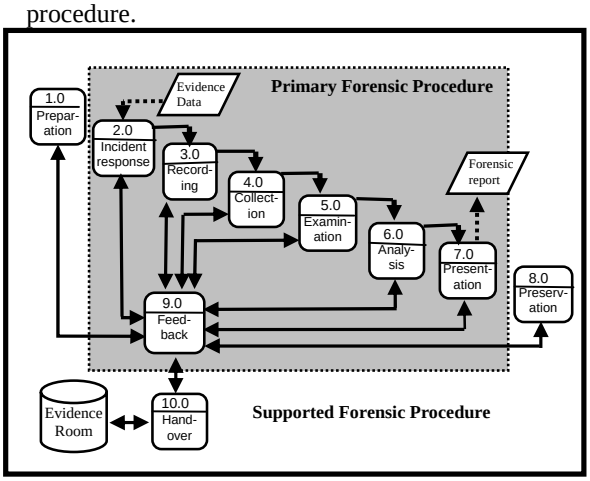

Figure 2 level-0 the comprehensive forensic procedure
Source: This study

Based on the above, the digital forensic context diagram is developed into a level-0 data flow. In this study, three new digital forensic procedure sets are proposed, which are primary, supported, and comprehensive forensic procedure. Figure 2 depicts a comprehensive forensic procedure, wherein each forensic procedure is represented by an arc block, and numbered by a recommended processing sequence. These three procedure sets are detailed below:

The primary forensic procedure

After the occurrence of criminal digital events, a series of forensic procedures are activated from the event data to achieve the goal of digital data forensics that can generate the intended forensic reports. This study summarized six primary procedures, of the primary forensic procedure, which are initial incident response, recording, collection, examination, analysis, and presentation. In addition, the feedback procedure is added to support the overall operation. As shown in Figure 2, the gray background part.

Under the primary forensic procedure, a procedure is carried out in succession to the previous one, given a normal situation. However, in the execution steps of the primary forensic

procedure, procedural feedback mechanisms must be initiated, as necessary, to reinforce and complete the specified procedure of the intended forensic mission.

The supported forensic procedure

In addition to the primary forensic procedure, the supported forensic procedure is required to ensure the smooth implementation of the primary forensic procedure. This procedure can be independently activated to provide support under any circumstances, when necessary. In this model, the supported forensic procedure is assembled by three single support procedures, which are: preparation, preservation, and acceptance and handover procedures. As shown in Figure 2, the white background part. The details are as shown below:

Preparation (1.0): the preparation procedure in digital forensics does not simply mean the preparatory actions prior to the implementation of the entire forensic process, but rather involves corresponding preparatory requirements for each procedure. Many previous studies suggested that the first step of a forensic procedure is preparation, namely the technologies, tools, and resources necessary for all forensic procedures are accurately estimated and prepared from the beginning of the entire forensic process. However, this concept has its flaws. Because of advanced technologies and continuously emerging modus operandi, special technologies, tools and resources may be required during each forensic procedure. Thus all the necessary components of digital forensics cannot be fully estimated and prepared from the beginning, but must adapted to different situations to perform the preparation procedure necessary for supporting any forensic procedure. Moreover, some preparations by forensic practitioners in real cases may not be performed at the beginning due to different schedules of budgetary allocations, so the preparation procedure may not only be performed at the beginning.

Preservation (8.0): In the digital forensic procedure, waiting periods may occur between procedures. Also, forensic personnel required by each procedure may be different. Thus, to meet actual demands, conveyance and transfer are required for evidence data. In such cases, the evidence data should be protected and preserved during procedures, and processes, to ensure the safety, integrity and evidential power of evidence data. In addition, the preservation of evidence data may not only be performed as a final procedure. It may be required when there is lack of technology, or new evidence is found during other forensic procedures, or failure of implementing the subsequent forensic procedure due to special causes.

Acceptance and handover (10.0): This model adds this procedure, which is a crucial and necessary action for when evidence data needs to be collected, preserved, and retrieved. Many forensic cases are suspended due to certain procedural issues, which arise from a lack of forensic technology, a need to collect new evidence, or other special causes. Under these situations, evidence data and mediate evidence must be properly, and safely, preserved for long periods of time, which demands complete acceptance of the integrity of evidence and handover procedures. In practice, evidence rooms are established by law enforcement units to provide long-term, suitable environments for protective and secure preservation and retrieval processes.

The comprehensive forensic procedure

The comprehensive forensic procedure is the combination of the primary forensic procedure and the supported forensic procedure. To ensure the exactness and effectiveness of digital forensic results, the comprehensive forensic procedure is strongly recommended by this study as the best forensic procedure if actual conditions and resources permit. In practice, the supported forensic procedure may not be implemented, or only implemented due to shortages of budget, resources, personnel, equipment, or economies of scale. In such cases, the primary forensic procedure at least should be built into the implementation stage so that the digital forensic report will have a basic effectiveness of evidence.

New feedback mechanism

This model proposes a creative feedback mechanism which is never shown in previous models. In this study, a new feedback procedure (9.0) is adopted as feedback mechanism, which can directly return to the procedure that is necessary to redo, but not only return to the previous procedure, as shown in Figure 2. In order to provide strict, admissible evidential forensic results, most research on digital forensics has pointed out that a feedback mechanism is required for the digital forensic procedure [1] [2] [3] [4] [5] [7] [8] [11] [15] [18] [20] [22]. To enhance the forensic requirements of

the digital forensic procedure of any given stage, the feedback mechanism is a means of returning to a previous procedure, depending on the situation or data needed.

Pervious studies have indicated that the feedback mechanism can only return to the previous procedure one by one till the initial problematic one is found rather than being return to the initial problematic procedure directly. There is a serious shortcoming to this approach that is obviously very rigid and can not meet the diverse needs of the situation. The main reason is each of the procedures with analysis and diagnosis can only return to its previous one and accept the request for its next one. For example, if the last procedure is found wrong, incomplete or without sufficient data in the very beginning of the forensic procedure occurred, it must be rigid to return to the previous procedure one by one till returning to the very beginning of the problematic procedure. This will cause waste of resources and inefficiency in forensics. Therefore, this model proposes the feedback procedure (9.0), which is very flexible and effective in solving this problem.

Level-1 model development

Previous studies have only provided conceptual explanations, lacking detailed explanations regarding expression of the execution of details. The purpose of this level is to present, and to describe, how each forensic procedure is developed and processed. Each “process” in this level is presented by an arc block, and numbered in recommended sequence. The numbering principle is based on procedure numbering used in level-0, with one more digit. For instance, “4.1” means the first procedure of the fourth forensic process.

Figure 3 depicts a reference example of collection (4.0) procedure in the forensic procedure. The processing process may be designed linearly, where applicable, or in combination with the internal feedback mechanism, if necessary, for cases such as searching (4.2).

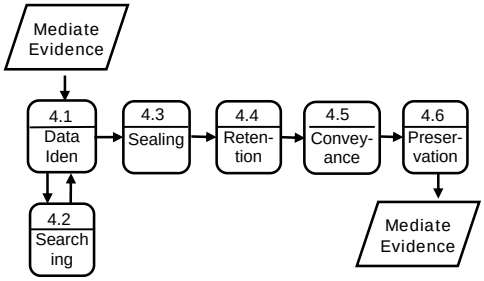

Figure 3 progression of “collection” procedure
Source: This study

Level-N model development; and continuing development until bottom-level-dataflow

This model development aims to subdivide and decompose necessary forensic tasks into their simplest presentation form, covering the simplest sources of data, implementation processes, and interim results. This form of presentation is conceptually referred to as a bottom-level-dataflow. In such cases, the simplest presentation form means that the tasks are already simplified enough for individual operation, or individual assignments. As illustrated in Figure 4, the simplest presentation form is obtained after searching (4.2) is developed.

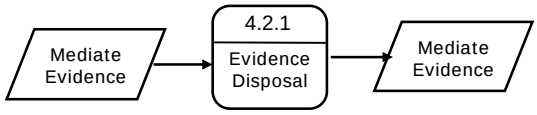

Figure 4 Forms of presentation developed into their simplest presentation form
Source: This study

The key point of the development content of level-N is the description of the processing process. If any process in level-1 is still complex, it means that it is not yet developed into its simplest presentation form, such as data identification (4.1), as shown in Figure 5. In other words, if additional sub-processes are required by any process, the development needs to continue from level-2 to the next level, until all sub-processes are decomposed into their simplest presentation form and, regardless of follow-up, would continue to develop the number of levels, such as the bottom-level-dataflow, as illustrated in Figure 4.

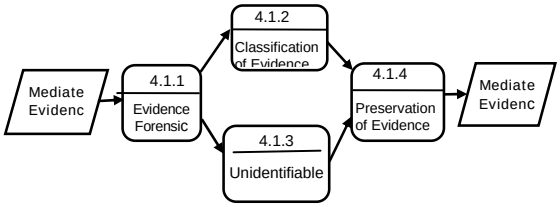

Figure 5 Decomposition diagram of sub-process
Source: This study

From level-2 to the bottom level, the source of data and interim results would use a parallelogram symbol to represent the mediate evidence. The process described herein is also represented by an arc block. Similarly, for every additional level, corresponding numbers are added

to the previous level, and the numbers in the same level are numbered sequentially.

Specifications of bottom-level-dataflow

When all procedural processes are decomposed into their simplest presentation form, the process is simplified enough to know how to execute these processes. In this level, the main purpose is to add forensic personnel, forensic tools, forensic site descriptions and forensic results to the previously developed bottom-level-dataflow, which is then converted to a presentation form of "assignable units of task assignments". In this model, this form is conceptually referred to as the specifications of bottom-level-dataflow. In other words, the process can be described as an assignable, or an executable, unit of task after the specifications of these factors are explained.

In this level, the forensic site is represented by a cubic symbol, the forensic personnel (including number of people) is represented by a triangular symbol, and the forensic tools, or method (including the quantity), is represented by a hexagonal symbol, as shown in Figure 6.

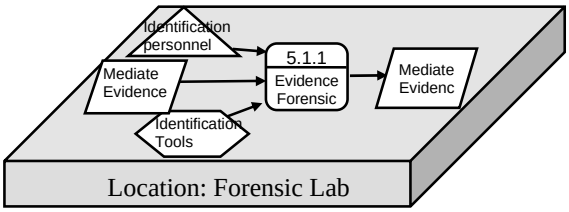

Figure 6 Specifications of bottom-level-dataflow
Source: This study

Mapping from bottom-level-dataflow to specifications, then mapping to digital forensic construction dictionary

Another important problem is realizing the amount of resources required to meet forensic demands throughout the entire digital forensic process. Namely, which area of specialty, how many professionals, specialty tools, and equipment are in need of preparation? These are factors affecting budgetary planning, staffing, training, and equipment procurement scheduling of enforcement units. Thus, this study proposes a digital forensic construction dictionary for addressing the problems faced by the digital forensic practitioners.

A digital forensic construction dictionary aims to list types, quantities of all forensic task forces, tools, and any equipment necessary for the entire digital forensic process. As discussed above, these data for each individual process can be obtained from the specifications of bottom-level-dataflow and could be statistically collected and sorted, which is the perspective of a digital forensic construction dictionary, as shown in the lowest part of Figure 7. Table 2 is an example table of a digital forensic construction dictionary.

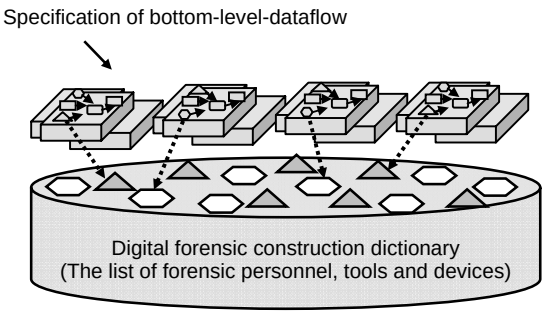

Figure 7 Conversion diagram of digital forensic construction dictionary
Source: This study

Table 2 Example table of digital forensic construction dictionary
Source: This study

Staffing requirements	XXX Table				
Task assignment / Types of personnel	4.1.4	4.2.1	…..	Total	Unit Price
Collector	X	X		X	X
Examiner				X	X
Analyst				X	X
Conveyer	X			X	X
…..	…	…	…	…	…

Equipment requirements	XXX Table				
Task assignment / Types of equipment	4.1.4	4.2.1	….	Total	Unit Price
Anti-magnet box	X			X	X
Digital sealing machine	X			X	X
Special disk drive		X		X	X
Data reproducer		X		X	X
……	…	…	…	…	…

With the use of a digital forensic construction dictionary, digital forensic practitioners can easily list and estimate the types and quantities of professionals, tools, and equipments needed, as well as the procurement time. When level-0 the comprehensive forensic procedure is fully developed, it is possible to obtain a digital forensic construction dictionary, comprised of the fullest range of resources for the digital forensic process, and is therefore, referred to as an integrative digital forensic construction dictionary. It is also recommended by this study.

However, the digital forensic practitioners in different sizes of organization may find it difficult to establish an integrative digital forensic construction dictionary due to budget restrictions or limitations of scale. Therefore, this study suggests that practitioners should select their most necessary resources, according to an integrative digital forensic construction dictionary, and build a basic resource list based on their actual budget to meet their digital forensic processing needs. The preparation of a basic list of resources can facilitate smooth budgetary planning and procurement procedures as well as the fundamental digital forensic procedure implementation. It is referred to as a fundamental digital forensic construction dictionary.

Discussion

The establishment of the digital forensic procedure can be regarded as the establishment of a forensic system. To the management level, the establishment of a “system aspect” is important; however, the practitioner is more concerned with how to handle each procedure and how to connect the processes in practice. In other words, previous researchers highlighted the discussion of the system’s aspects (procedure level: level-0 in this model), but neglected the “executive aspect” (how to develop: level-1 to bottom-level-dataflow in this model). This study proposed a solution for the above situation. Thus, this comprehensive combination of system and executive aspects could be realized to join together the feasible framework. In addition, this model proposes a digital forensic construction dictionary for a detailed description of the requirements from a “resource aspect”, making contributions to actual budgetary planning and procurement processes. The three dimensions never shown in previous models at the same time can be clearly established from this model, which offers a decisive implementation of digital forensics.

A new system of digital forensics is proposed by this study, the comprehensive digital forensic procedure. While common forensic procedures are included in the comprehensive digital forensic procedure, as proposed by this study, any study or practitioner could add, or delete procedures where necessary, according their individual needs. Therefore, this model does not conflict with other procedural models proposed by other researchers, but allows for more flexibility and degrees of inclusion.

The viewpoint of digital forensic evidence data process flow in this study, does not contradict, or exclude, the procedural model viewpoints of past studies. In contrast, the proposed viewpoint not only includes the concept of procedural models but is able to explain, in detail, the descriptions of the interactions between the procedures and digital evidence data, as well as its processing objectives. In addition to systematically linking all of the

digital forensic process activities, it is also adaptive in explaining the framework and details of digital forensic of different levels.

Conclusions

This study proposed the expandable integrated digital forensic model, not only to present new concepts of digital forensics, but also describes, in detail, the methods of execution. This model can also provide a comprehensive basis for guidance and practical implementation steps for forensic practitioners, model guidance and practical execution can be complementary. In the model every developed process can be noted in a uniform digital expression form, in order to promote understanding and facilitate sharing experiences.

Though this model seems to provide a static description method, different digital forensic practitioners can employ different procedural combinations, as based on various actual forensic missions offering different modus operandi, in order achieve dynamic descriptions. In addition, since this model is presented systematically, with straightforward symbols, almost all digital crime cases can be described, and recorded, in digital forensics, thereby establishing a digital forensic library for knowledge management and sharing.

References

[1] Baryamureeba V. and Tushabe, F. (2004), "The Enhanced Digital Investigation Process Model", *Digital Forensic Research Workshop (DFRWS) 2004, Baltimore*, MD, available at: http://www.dfrws.org/2004/bios/day1/Tushabe_EIDIP.pdf

[2] Beebe, N. and Clark, J. (2004), "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process", *Digital Forensic Research Workshop (DFRWS) 2004, Baltimore*, MD, available at: http://www.dfrws.org/2004/bios/day1/Beebe_Obj_Framework_for_DI.pdf

[3] Carrier, B. (2003), "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers", *International Journal of Digital Evidence*, Vol. 1, Issue 4, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A04C3F91-AFBB-FC13-4A2E0F13203BA980.pdf

[4] Carrier, B. and Spafford, E. (2004), "An Event-based Digital Forensic Investigation Framework", *Digital Forensic Research Workshop (DFRWS) 2004*, Baltimore, MD, available at: http://www.dfrws.org/2004/bios/day1/Beebe_Obj_Framework_for_DI.pdf

[5] Carrier, B. and Spafford, E. (2003), "Getting Physical with the Digital Investigation Process", *International Journal of Digital Evidence*, Vol. 2, Issue 2, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0AC5A7A-FB6C-325D-BF515A44FDEE7459.pdf

[6] Casey E.(2003), "Digital evidence and computer crime – forensic science", *computers and the internet. Cambridge: Academic Press*, 2003a. p265.

[7] Chris Prosise and Kevin Mandia (2001), *Incident Response: Investigating Computer Crime*, McGrawHill Osborne Media.

[8] Digital Forensic Research Workshop (2001), Research Road Map, *Digital Forensic Research Workshop (DFRWS) 2001*, Utica, NY, available at: http://www.dfrws.org/archive.html

[9] Gane, C. and T. Sarson. (1979) , *Structured systems Analysis*, Prentice-Hall.

[10] James A. O'Brien (1975), *Introduction to Information Systems: Essentials for the e-Business Enterprise*, McGraw-Hill.

[11] Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006), *Guide to Integrating Forensics into Incident Response*, Special Publication 800-86, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, available at: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

[12] Lee HC, Palmbach TM, Miller MT. (2001), *Henry Lee's crime scene handbook*, San Diego: Academic Press.

[13] Mark Reith, Clint Carr, and Gregg Gunsch (2002), "An Examination of Digital Forensic Models ", *International Journal of Digital Evidence*, Vol. 1, Issue 3.

[14] Mocas, S. (2003), "Building Theoretical Underpinnings for Digital Forensics", available at: http://www.dfrws.org/2003/presentations/Brief-Mocas.pdf

[15] National Criminal Justices Reference Service (2001), "Electronic Crime Scene Investigation: A Guide for First Responders", *National Criminal Justices Reference Service (NCJRS)*, available at: http://www.ncjrs.org

[16] Noblett, M., Pollitt, M., Presley, L. (2000), "Recovering and Examining Computer Forensic Evidence", *Forensic Science Communications*, Vol. 2, No. 4, available at: http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

[17] Pollitt, M. (2007). "An Ad Hoc Review of Digital Forensic Models", *2nd International Workshop on Systematic Approaches to Digital Forensic Engineering*

[18] Pollitt, M. (1995), "Computer Forensics: an Approach to Evidence in Cyberspace", *Proceedings (Vol. II, pp 487-491) of the National Information Systems Security Conference*, Baltimore, MD, available at: http://www.digitalevidencepro.com/Resources/Approach.pdf

[19] Pollitt, M. (2004), "Six Blind Men from Indostan", *Digital Forensic Research Workshop (DFRWS)* 2004, Baltimore, MD, available at: http://www.dfrws.org/2004/bios/day1/D1-Pollitt-Keynote.ppt

[20] Reith, M., Carr C. and Gunsch, G. (2002), "An Examination of Digital Forensic Models", International Journal of Digital Evidence, Vol. 1, Issue 3, available at: http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=article&id=A04A40DC-A6F6-F2C1-98F94F16AF57232D

[21] Ricci S.C. Ieong (2006), "FORZA-Digital forensics investigation framework that incorporate legal issues", *Digital Investigation*, S29 - S36

[22] Robert F. Erbacher, Kim Christensen, and Amanda Sundberg (2006), "Visual Forensic Techniques and Processes", *Proceedings of the 9th Annual NYS Cyber Security Conference Symposium on Information Assurance*, Albany, NY, pp. 72-80, available at: http://www.cs.usu.edu/~erbacher/publications/NetworkForensicProcesses.pdf

[23] Ruibin, G., Yun C., and Gaertner, M. (2005), "Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework", *International Journal of Digital Evidence Spring 2005*, Vol. 4, Issue 1, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A6A102-A93D-85B1-96C575D5E35F3764.pdf

[24] Séamus Ó Ciardhuáin (2004), "An Extended Model of Cybercrime Investigations", *International Journal of Digital Evidence Summer 2004*, Vol. 3, Issue 1, available at: http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=issue&id=9

[25] Stephenson, P. (2003), "Modeling of Post-Incident Root Cause Analysis", International Journal of Digital Evidence, Vol. 2, Issue 2, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0AE98D6-E1F6-1C9D-481CEE8C29401BFE.pdf