Annual ADFSL Conference on Digital Forensics, Security and Law

2007 Proceedings

The General Digital Forensics Model

Steven Rigby
BYU-Idaho, Rexburg, ID USA, rigbys@byui.edu

Marcus K. Rogers
Purdue University, West Lafayette IN USA, rogersmk@purdue.edu

Scholarly Commons Citation

Rigby, Steven and Rogers, Marcus K., "The General Digital Forensics Model" (2007). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 1.
https://commons.erau.edu/adfsl/2007/session-7/1

The General Digital Forensics Model

Steven Rigby
BYU-Idaho
Rexburg, ID USA
rigbys@byui.edu

Marcus K. Rogers
Purdue University
West Lafayette IN USA
rogersmk@purdue.edu

ABSTRACT

The lack of a graphical representation of all of the principles, processes, and phases necessary to carry out an digital forensic investigation is a key inhibitor to effective education in this newly emerging field of study. Many digital forensic models have been suggested for this purpose but they lack explanatory power as they are merely a collection of lists or one-dimensional figures. This paper presents a new multi-dimensional model, the General Digital Forensics Model (GDFM), that shows the relationships and inter-connectedness of the principles and processes needed within the domain of digital forensics.

Keywords: process model, computer forensics, expert learning, educational framework, digital forensics

1. INTRODUCTION

There is a need for students studying digital forensics to see the complete investigative picture. This is required so that connections and the linkages will be made regarding the relationships between core investigative principles and processes. Being able to see the "big picture" before teaching individual topics provides a schema that situates concepts and creates a mental structure to hang core ideas on. This paper offers a new multidimensional graphical digital forensic model (GDFM) to help to show the relationships between the interconnecting points of the forensic client, forensic processes, and the forensic elements. The model is constructed in a way that promotes the structural knowledge needed by those involved in digital forensic investigations. The creation of mental models has been a key factor for experts in their domains and these mental models can be used to increase students' expertise and problem solving abilities.

2. WHY USE GRAPHICAL MODELS?

Representing theory in a graphical model is an effective way to convey meanings of complex principles and processes, and how they interact with each other. In addition to adding to the domain literature, graphical models can also help educators' effectively present theory to students. The goal for educators is to help students evolve and acquire attributes that are exhibited by those who are considered experts in a particular domain. One of the main characteristics of experts is that they look at problems through principles and organize the problem around main ideas; while novices will immediately try to fit the problem into a solution (Chi, Glaser, & Farr, 1998). Additionally, when engaged in problem solving, experts will usually try to understand the problem more thoroughly than novices. Experts build mental models that help define the scope and constraints to the problem (Chi et al., 1998). This becomes increasingly important for problems that are ill-defined and may necessitate using previous mental models and adapting them to solve current problems.

When concepts within a specific domain are interrelated, it increases the learners' structural knowledge and helps "connect the dots". This connection is very important for problem solving (Jonassen, 2000). Learners that are only required to memorize facts may have difficulty understanding the "why?" and the "how come?" By organizing facts around principles and processes, students will better answer these questions and will start to organize a mental framework that more closely resembles that of experts (National Research Council, 2000). One way to help students create this mental framework and understand the complexity of digital forensic concepts is to provide graphical models that show these principles and processes in an inter-related way.

Creating models helps learners conceptualize systems and all of the systems sub-components in order to understand the behaviors of other systems (Lesh & Doerr, 2003). Graphical models also help learners see concepts in different representations which helps readers think at higher levels of abstraction. Research has shown that using multiple representations in instruction has been a key factor to further understanding (Ainsworth, Bibby, & Wood, 2002). All of these different representations allow the learner to derive a deeper meaning and understanding of the concept being taught. Each representation has its own vagueness and weakness, and by combining these representations a clearer picture comes into view (Ainsworth et al., 2002).

This ability to infer meanings between representations is the desired outcome of instruction. Kaput (1989, pp. 179-180) states that "cognitive linking of representations creates a whole that is more than the sum of its parts… it enables us to see complex ideas in a new way and apply them more effectively." Ainsworth (1999) suggests that this transfer can be achieved through:

a) promoting abstraction;

b) encouraging generalization; and

c) teaching relations between representations.

Additional studies have shown that the underling models or cognitive structures of experts were highly predictive of problem solving scores and activities. This suggest that "well-integrated domain knowledge is essential to problem solving" (Jonassen, 2000 p. 70).

So why do we use graphical models for representing complex systems? The reason is that graphical models help us visualize complex systems of principles and processes, and illustrate how they are related to each other. Additionally, graphic models help improve problem solving capabilities and further expertise. Expertise is the goal for students and practitioners alike and as the digital forensic domain continues to be defined, it will be increasingly important to identify the principles and the relationships between these principles. This will not only solidify the theory of digital forensic science, but it will aid in the instruction of students learning digital forensic principles, processes, and their relationships.

3. CURRRENT IA MODELS

There are many models that have been created to help explain and conceptualize Information Assurance principles. The McCumber model (which was revised to become the Information Assurance Model) uses a "cube" to represent the relationships between security services, information states, and security countermeasures (Maconachy, Schou, Welch, & Ragsdale, 2001). The representation of a cube with its many sections conveys a multi-dimensional view suggesting there are relationships between and among each section. For example, in the Information Assurance Model (Figure 1) the concept of confidentiality does not stand on its own within an organization, rather it is dependent upon technology, policy, practice, and people. At any given moment information could be in one or more of the different states of transmission, storage, or processing (Maconachy et al., 2001).

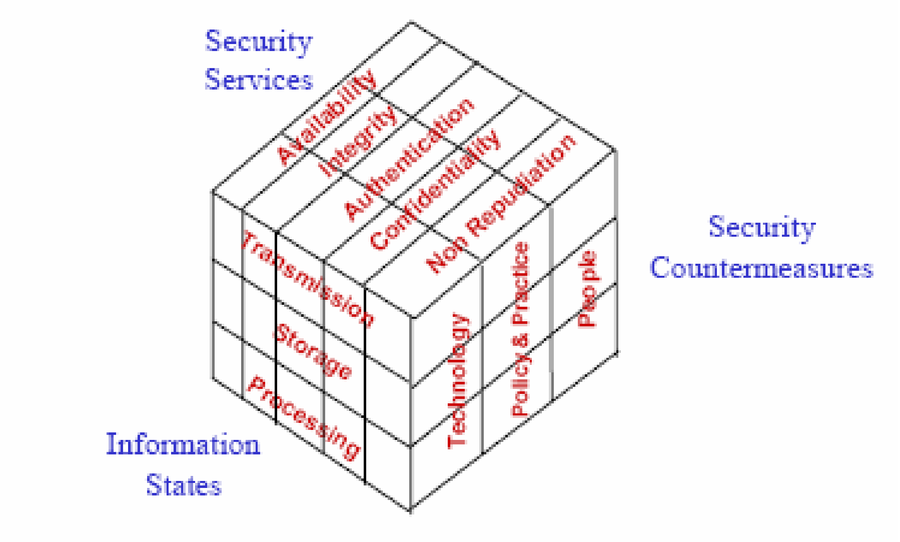

Figure 1. Information Assurance Model (Maconachy et al., 2001)

By examining the Information Assurance Model cube one can visually see the relationships between and among each concept. This becomes an important factor of instruction since much of the time spent on initial learning is developing patterns of recognition that can be recalled and applied to new experiences (National Research Council, 2000). Many textbooks and courses use this model to show the "big picture" of IA and can use this model as a launching point of discussion.

Other organizations are finding it useful to use the three dimensional matrix cube model for constructing a conceptual framework to represent theory and systems of objectives. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) used the cube (see Figure 2) for constructing a framework for integrating principles, creating a common terminology. This framework has been used to develop practical implementation guidance for risk management objectives (COSO, 2004).

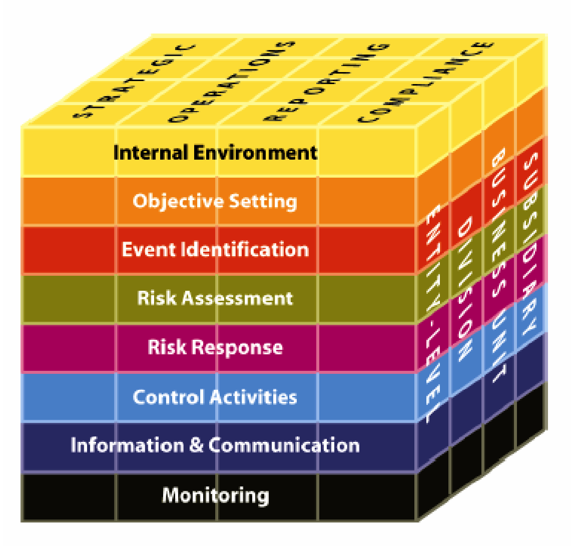

Figure 2 (COSO, 2004).

4. DIGITAL FORENSIC MODELS

With the dynamic and fast changing pace of technology, digital forensic models should be based upon core principles and processes that will continue to be relevant in the future despite the fact that tools, methods, and lists change frequently. By focusing the model on principles and concepts rather than detailed lists and procedures, the model can be applied to different environments and situations. The creation and use of tools has mainly been the focus in the past, while theory and core concepts has been relatively ignored (Rogers & Seigfried, 2004). Rogers and Seigfried (2004) state that there is a:

> …misguided belief that there is no generic conceptual approach to computer forensics (i.e., every case is so unique that standards are meaningless). Other areas of forensic science have clearly shown that this is not true, and that a common conceptual approach is not only possible but is also imperative in order to be considered a scientific discipline by the courts (p. 15).

Some of the previous academic forensic models include McKemmish (1999), Mocas (2003), Carrier & Spafford (2003) Beebe and Clark (2004), and Rogers (2006). These models have focused on core ideas that can be used as a guide for academic and practitioners alike and can be generalized to new situations. It is important to note that there are ongoing discussions concerning which models closest resemble the "real world" and which principles and processes should be included in these models; however, this is a natural evolution as the digital forensic field is still being defined (Rogers, 2006).

The work of Beebe and Clark (2004) suggest a multi-tier, hierarchical framework so that lower level objectives and processes can be represented. This is a valid point since some of the criticism of previous models is that they are "overly-broad and do not lend themselves to a practical real-world approach for dealing with an entire investigation" (Rogers, 2006 p. 606). This presents the need to create a framework of models to show how the different levels of abstraction are necessary to understand and differentiate the principles from the sub-principles. This framework can take many forms where higher level principles are more theoretical and lower-level principles are more practical.

The purpose of this paper is not to describe the principles and processes in detail, [see McKemmish (1999), Mocas (2003), Carrier and Spafford (2003), Beebe and Clark (2004), and Rogers (2006)], but rather to extract the core ideas out of the previous models and offer a graphical framework for the digital forensics discipline that presents these ideas in a multi-dimensional inter-connected view.

5. THE GENERAL DIGITAL FORENSICS MODEL

The General Digital Forensics Model (DFGM) model is based on the "cube" representation that is also used in the Information Assurance Model (see Figure 3). Not only does this structure provide consistency from the broader Information Assurance Model to the sub discipline of digital forensics but it also represents the triangulation of all of the previous models mentioned earlier including Reith, Carr and Gunsch (2002). The GDFM takes the perspective of the digital forensics practitioner showing the core principles and processes (represented by the vertical rows) involved for a specific case divided into the collection phase and the analysis phase. Although the collection and the analysis phases may be done simultaneously, there are important principles and processes that can be tied to each. In addition, the practitioner may be presented with criminal, civil, or internal cases (represented by the horizontal rows) which may cause changes to sub-principles specific to the client. For example, a forensic practitioner will need to ensure the sub-principle of "control the scene" is adhered to before entering a crime scene, and otherwise might only need to ensure the employee has left for the day before doing a forensic copy for a business. The questions that the practitioner will need to answer are along the side of the cube (the third dimension of the matrix). These represent the who, what, how, where, and when of a forensic event.

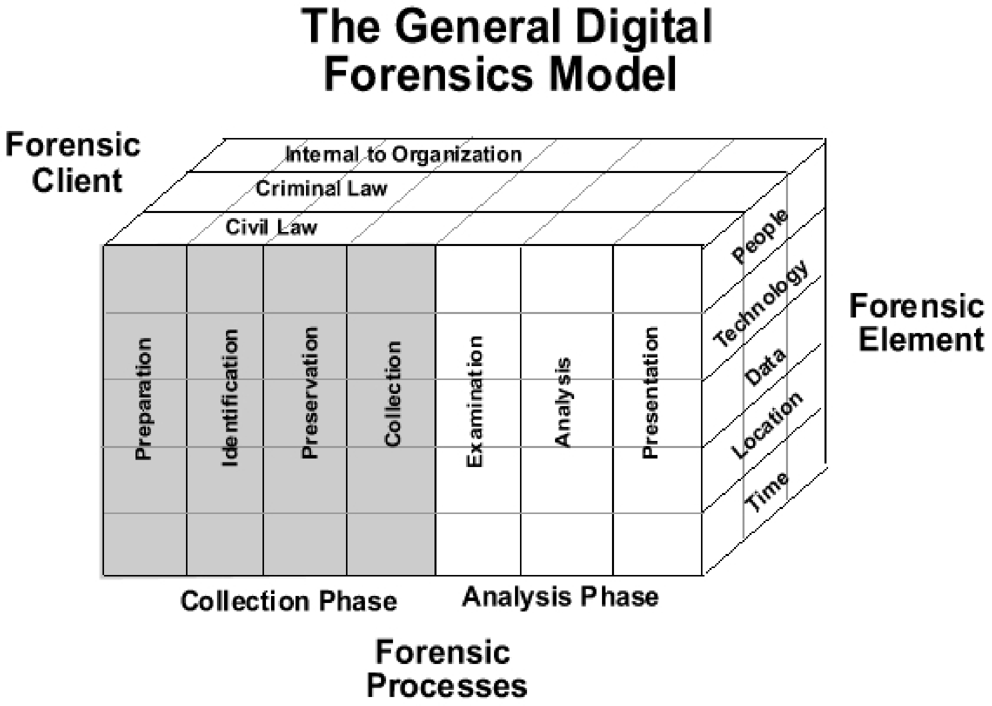

Figure 3. The General Digital Forensics Model (GDFM)

The explanatory power of the GDFM lies in the fact that the core principles and processes of digital forensics are shown in a way that stimulates the mental connections to other core principles. The principle of preparation may require search warrants in a criminal case or the approval of management for an internal investigation. Additionally, the preparation principle should also take into account what type of data may be encountered and what technologies may be involved along with whom, and when the event occurred or is occurring.

In addition to being used for instructional and training purposes, the GDFM model can be used as for evaluation in the courts to see if the forensic practitioner has performed the necessary due diligence required for the case., The Judge in a case may consider what steps were taken to ensure the collection, preservation, examination, and analysis of evidence based upon the Daubert criteria. Although the concepts and principles of the GDFM may not apply to all situations, it provides a framework for practitioners and students to consider.

6. WHAT THIS MEANS FOR EDUATION – A CASE STUDY

In order to see how the multi-dimensional view of the GDFM model can help with instruction and create the mental threads that lead to understanding and expertise, this paper offers a brief discussion of one of the intersecting points. It is not feasible to review all of the possible ideas concerning the intersecting points of the GDFM, but rather to offer some points of discussion and thought that can be incorporated into instruction. A typical classroom scenario would be to walk the students through the various intersecting points and have the students come up with situations and contexts relevant to the categories. This will allow the students to develop mental maps based on ill-defined problems that are more representative of the real world. While the model can be used for examining highly defined case scenarios (as is usually the norm), research has shown that these well-defined problems do not produce learning and skills that are transferable across situation, and thus very synthesis occurs (Jonassen, 2000).

6.1 Preparation

Preparation may be considered a principle, concept, or phase while looking through the different dimensions of the GDFM. Preparation can be applied to each of the dimensions of people, technology, data, location, and time, as well as that of whether the investigation is for a criminal, civil, or internal client

People

The forensic practitioner will need to engage the necessary people to ensure the collection and analysis phase is accurate and correct. If the practitioner knows that they will only have a limited time on location, they may need assistants to take pictures, video, and documentation and help with the labeling and collection of materials and equipment. In addition to assistants, other experts may be needed to participate if the case includes tasks outside of the practitioner's expertise. For example if the data being collected is located on a network SAN, or if the data is located in an oracle database the practitioner may need to solicit help from other experts in these areas.

Technology

The practitioner will also need to prepare the necessary hardware, and software needed to be successful in the collection and analysis process. This may include the necessary hard drives and cloning software needed for imaging disk drives as well as the appropriate technology necessary to collect data from flash, mp3, cell phones, printers, and other devices. The practitioner should also prepare an appropriate forensic field kit that includes all of the cables, labels, tape, gloves, markers, etc… that will be required for successful collection.

Data, Location & Time

The forensic data to be collected and analyzed may be in different forms and states. These data may be in a stored location, in memory or being processed. These data could be transmitting and streaming through a network, or these data could even be transmitting through the air using radio frequencies. These forensic data may not even be digital. For example these data may be analog data recorded as a tape or wave file. The forensic practitioner should be prepared ahead of time to encounter each of these different types of data with the necessary technology, and network of experts that can be drawn upon. Timing may be crucial to an investigation with the practitioner receiving limited or little advanced notice to perform the collection of digital forensic data

Criminal, Civil, & Internal

Different people may need to be contacted and different preparation may be required for criminal, civil and internal clients. One of the most important principles, when dealing with criminal cases, is to "control the scene" before entering the premise of a crime scene. This can involve communication with the police to know when it is safe for the practitioner to enter in the case of a criminal investigation. For an internal case, one area of preparation would involve communication with management and securing the appropriate clearances to be allowed on-site during off-hours. In a civil matter the preparation may include a pre-discovery meeting with the opposing organization and their counsel to go over the anticipated request for electronically stored information (ESI).

The principle of preparation is just one of many lenses that can be used to look through the GDFM. Each of the other processes of identification, preservation, collection, examination, analysis, and presentation can be used to situate classroom discussions about the forensic events and the forensic client of the case.

7. SUMMARY

This paper presented a new graphical digital forensic model (GDFM) that is multi-dimensional and thought provoking. The usefulness of this new model is its ability to help students and professionals think through how the principles and processes of digital forensics are inter-related and multi-dimensional. The GDFM shows the relationships between the interconnecting points of the forensic client, forensic processes, and the forensic elements in a way that promotes the structural knowledge needed by those studying and engaged in digital forensic investigations. By discussing these relationships we can help students create mental models which are important for problem solving and increases expertise. As the digital forensic domain continues to be defined, it will be increasingly important to identify the core ideas and the relationships between these ideas. This will not only solidify the theory of digital forensic science, but will also help students learning digital forensic principles, processes, and their inter-relations.

8. REFERENCES

Ainsworth, S., Bibby, P., & Wood, D. (2002). Examining the effects of different multiple representational systems in learning primary mathematics. *Journal of the Learning Sciences, 11*(1), 25-61.

Beebe, N., & Clark, J. (2004). *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process.* Paper presented at the Digital Forensic Research Workshop (DFRWS), Baltimore, MD, June.

Carney, M., & Rogers, M. (2004). The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction. *International Journal of Digital Evidence, 2*(4).

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence, 2*(2), 1-20.

Chi, M., Glaser, R., & Farr, M. (1998). *The Nature of Expertise*: Lawrence Erlbaum.

COSO. (2004). *Enterprise Risk Management Framework*: The Committee of Sponsoring Organizations of the Treadway Commission.

Jonassen, D. H. (2000). Toward a Design Theory of Problem Solving. *ETR&D, 48*(4), 63-85.

Lesh, R., & Doerr, H. (2003). Model development sequences. In R. Lesh, K. Cramer, H. Doerr, T. Post & J. Zawojewski (Eds.), *Beyond Constructivism* (pp. 35-58): Mahwah, NJ: Erlbaum.

Maconachy, V., Schou, C., Welch, D., & Ragsdale, D. J. (2001, June 5-6). *A Model for Information Assurance: An Integrated Approach.* Paper presented at the Proceedings of the 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, West Point, NY.

McKemmish, R. (1999). What is forensic computing? . *Trends and Issues, 118. Canberra: Australian Institute of Criminology.*

Mocas, S. (2003). *Building Theoretical Underpinnings for Digital Forensics Research.* Paper presented at the Digital Forensic Research Workshop (DFRWS), Cleveland, OH, August.

National Research Council. (2000). *How People Learn - Brain, Mind, Experience, and School* National Academy Press.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence, 1*(3).

Rogers, M. (2006). DCSA: A Practical Approach to Digital Crime Scene Analysis. In H. Tipton & M. Krause (Eds.), *Information Security Management Handbook*: (Isc)2 Press.

Rogers, M., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Computers & Security*(26).

ABOUT THE AUTHORS

Steven Rigby is a faculty member at BYU-Idaho teaching information assurance, networking, and operating system courses in the Computer & Information Technology Department. Research interests include Information Assurance & Security instructional strategies, digital forensics, and security policy.

Marcus K. Rogers PhD, CISSP, CCCI-Advanced, is an Associate Professor at Purdue University and is the Chair of the Cyber Forensics Program in the Department of Computer & Information Technology. Dr. Rogers is also a member of the research faculty at CERIAS. Dr. Rogers' research and publication interests include applied digital crime scene analysis, digital forensics, cyber criminal profiling & cyber terrorism.