Oct 20th, 1:00 PM - 1:25 PM

Using Project Management Knowledge and Practice to Address Digital Forensic Investigation Challenges

Steven S. Presley
University of South Alabama, ssp1521@jagmail.southalabama.edu

Jeffrey P. Landry
University of South Alabama, jlandry@southalabama.edu

Michael Black
University of South Alabama, mblack@southalabama.edu

Presley, Steven S.; Landry, Jeffrey P.; and Black, Michael, "Using Project Management Knowledge and Practice to Address Digital Forensic Investigation Challenges" (2018). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 1.
https://digitalcommons.kennesaw.edu/ccerp/2018/practice/1

Abstract

The management of digital forensics investigations represents a unique challenge. The field is relatively new, and combines the technical challenges of Information Systems with the legal challenges of forensics investigations. The challenges for the Digital Forensics Investigators and the organizations they support are many. This research effort examines the characteristics and challenges of Digital Forensics Investigations and compares them with the features and knowledge areas of project management. The goal was to determine if project management knowledge, as defined in a common body of knowledge, would be helpful in addressing digital forensics investigation challenges identified in the literature. The results indicate that there are parallels between the two areas.

Location

KC 462

Disciplines

Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

Digital Forensics is a relatively new field but one that is very prevalent in today's world. Reports of security breaches and criminal misconduct can be seen daily in major news sources. As a result, interest in digital forensics research is high. Most of the research in this field has been focused on specific vulnerabilities and forensic data collection, as well as the specific challenges of new technologies. Digital Forensics research is also beginning to find that these challenges can have a huge influence on the success of an investigation in the short term, and on an organization's overall ability to conduct digital forensics investigations (Karie & Venter, 2015). For the field of digital forensics to grow and flourish, these challenges must be addressed.

This study provides a new perspective—project management—to address the emerging challenges of digital forensics. This research effort will investigate whether it is appropriate to consider project management research and practices to support digital forensics challenges. To make this determination, it will compare the characteristics of digital forensics investigations with the standard definition of a project. It will then review the challenges being reported in recent research related to digital forensics investigations (DFI) and attempt to map them to areas within the Project Management Body of Knowledge (PMI, 2013). If there is sufficient similarity between the digital forensics challenges reported in the literature with the knowledge areas and processes described in the PMI Project Management Body of Knowledge (PMI, 2013), this may be a good indicator that digital forensics investigations can be viewed as a specialized type of information systems project.

In summary, this research is expected to show that many of the characteristics of digital forensics investigations are similar to the traditional definitions of a project and that many digital forensics challenges are potentially addressed by project management practices and knowledge areas.

The research questions posed by this paper are:

R1 – Do Digital Forensics Investigations (DFI) share many of the same characteristics and processes as traditional projects as defined by a common standard?

R2 – Do the practices and knowledge areas in this project management standard contain information that may be useful for addressing challenges in the Digital Forensics field?

This study expects to make a contribution by identifying which knowledge areas in project management pertain to digital forensic challenges. Each connection found between a DFI challenge and a PMBOK area presents an opportunity for problem-solving. As an outcome, this could suggest that further research on applying project management practices and knowledge areas in the context of digital forensics investigations may be beneficial to organizations and stakeholders in digital forensics investigations.

BACKGROUND

Before we can address the linkages between digital forensics and project management, the relevant literature in each area will be reviewed. In the following sections, we will define the characteristics of a digital forensics investigation. This section will include common definitions and descriptions of the digital forensics process. Similarly, the characteristics of a project will also be defined, according to a widely accepted ANSI standard. A framework of knowledge areas based on this standard will be introduced, and the project management process will be described.

Digital Forensics Investigation Definitions and Characteristics

For this effort, the research team relied upon a widely cited digital forensics framework by Carrier and Spafford (2004). Among other important contributions, this framework provided a foundational set of definitions for the following terms:

Digital Data – data represented in numerical form, whether binary or another numbering system.

Digital Object – a discrete collection of digital data, such as a file, hard drive sector, or memory *contents*

Digital Event – An occurrence that changes the state of one or more digital objects. If the object state changes, this is an *effect* of the event.

Evidence of an Event – Generally, this is an indicator that an event occurred –an object can become evidence of an event if the state of the object changes during the event.

Digital Incidents and Crimes – one or more digital events that violate a policy (an incident) or a law (a crime).

Investigation – process which develops and tests hypotheses about events: for example, did an event occur, what caused it, and when did the events occur.

Digital evidence of an incident - Any digital data that contains reliable information that supports or refutes a hypothesis about the incident

Forensics Investigation – A process that uses science and technology to develop and test theories, which can be entered into a court of law, to answer questions about events that occurred.

The previous definitions, therefore, lay the foundation for the activities being described:

Digital Forensic Investigation (DFI) – (A) process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred.

Digital Forensics Investigation Phases

There have been many attempts to define digital forensics models (Lutui, 2016; Selemat et al., 2008). DFI models focus on the tasks required to directly perform the digital investigation tasks, specifically the "process of identifying, preserving, analyzing, and presenting evidence in a manner that is legally acceptable" (Selemat et al., 2008). More recent models also consider the management of this process at a higher level and the readiness of the organization to perform investigations to meet specific challenges (Lutui, 2016; Karie & Venter, 2015). Another parallel with project management can also be seen in the digital forensics literature. DFI, like projects, were originally described as having consecutive phases. Recent research in DFI supports Agile processes as being potentially useful to speed time to completion, reduce costs, and improve outcomes (Grispos et al., 2014).

For simplicity and generality, the research team opted to use a widely-cited framework suggested by Carrier and Spafford (2004), which was based on crime scene procedures and extended to the digital domain (Carrier and Spafford, 2003). It consists of the following broad categories of phases, as shown in Figure 1:

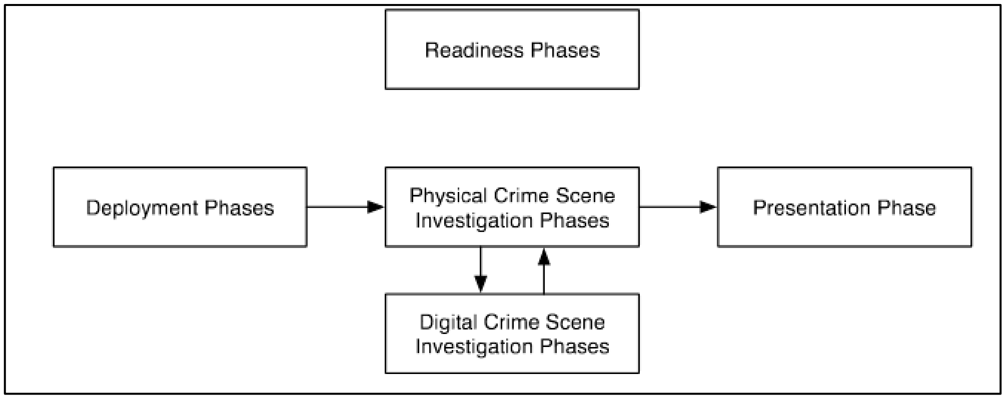
Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Presentation Phase
Digital Crime Scene Investigation Phases

Figure 1 – Major categories described by Carrier and Spafford (2004)

Readiness Phases – include training the people and testing the procedures and tools needed to perform the investigation.

Deployment Phases – include the detection and notification of an event which triggers an investigation. Also includes confirmation and authorization phases where the approval to conduct the investigation and the scope of the investigations are defined.

Physical Crime Scene Investigation Phases – After authorization, physical devices are collected and physical evidence that could link suspects to the data.

Digital Crime Scene Investigation Phases – examines the digital data for evidence. Each device represents a separate investigation. Reconstruction of digital evens is included, and hypotheses are formed and tested leading to conclusions, which are the products of the investigation.

Presentation Phase – the results of the investigations are presented to courts or corporate audiences.

These phases appear similar to project management processes described in the PMI Project Management Body of Knowledge (PMI, 2013) as shown in the next section.

Project Definitions and Characteristics

The PMI Project Management Body of Knowledge (PMI, 2013), currently in its fifth edition, represents the combined efforts of hundreds of project management professionals and has been peer-reviewed by countless practitioners in almost every industry. It is an ANSI standard (ANSI/PMI 99-001-2013), whose stated purpose is to document that subset of the project management body of knowledge that is generally recognized as good practice. It is intended to apply as broadly as possible to a broad range of project applications and has widely been used in the computing field.

According to the Project Management Body of Knowledge (PMBOK), projects have the following characteristics:

- Occur for a limited duration: a temporary endeavor, having a beginning and an end
- Create a unique product, service, or result
- Have a set of objectives which may vary in maturity (deterministic versus iterative)
- Have clients, customers, and stakeholders
- Results are intended to be permanent, but may also be used for temporary objectives

- Have the potential for social, economic, and environmental impacts
- Can involve single or multiple individuals and organizations

As part of the effort to capture the organize the practices of project management, the PMI PMBOK is organized using Project Management Knowledge Areas. It is believed that these Knowledge Areas contain information which may be useful in Digital Forensics Investigations (DFI). These knowledge areas include the broad category of Organization Influences and Project Lifecycle, and the ten PMBOK areas: project integration, scope, time, quality, human resource, communications, cost, risk, procurement, and stakeholder management.

The research team noted that digital forensics investigations vary widely in the amount of time needed. Simple cases may take only an hour or so, while the most complex cases may require many person-years of work. Therefore, the effort needed to manage the project-related challenges of an investigation would likely be commensurate with the size and duration of the overall investigation; for the simplest investigations, the need for these practices may be negligible.

Despite the similarities, few research efforts to date have attempted to look at the challenges of digital forensics from the broader perspective of project management. However, many challenges identified by current research are very similar to the challenges encountered in general information systems projects. This observation seems to indicate the potential for applying project management research and practices to digital forensics investigations.

There are many examples of digital forensics challenges in the literature which are similar to general project management challenges. These include the impact of applying ethical standards and codes of conduct (Sharevski, 2015; National Research Council, 2009), the need to develop standardized processes (National Research Council, 2009; Lutui, 2016), the emergence of new technologies and paradigms such as cloud computing (Grispos, Storer, & Glisson, 2012; Lutui, 2016), and the changing legal environment and jurisdictional concerns (Karie & Venter, 2015; National Research Council, 2009). Resource shortages, including trained digital forensics practitioners and hardware required to handle increasingly large amounts of data, can further impact an organizations ability to successfully perform digital forensics investigations (Karie & Venter, 2015; National Research Council, 2009; Quick et al., 2014).

There is a precedent for the line of reasoning proposed in this paper. Recent research has suggested that Agile practices, a strategy commonly used for software projects, also may also useful for security response teams (Grispos, Glisson, & Storer, 2014). This research focused on the tasks directly involved in the investigative process - specifically in suggesting a useful methodology to support the activities of the security response teams during an incident. As security responses are a common type of digital forensics, this seems to indicate that other project management approaches may also be useful.

Digital forensics research has pointed to organizational and environmental factors (Karie & Venter, 2015) as challenges which may affect the success of an investigation. Despite this, there is little research which considers the supporting processes and organizational features needed. Project Management professionals have long realized that these broader factors are just as critical to the success of the project as the technical and procedural details of the actual implementation (PMI, 2013). The Project Management Body of Knowledge, a widely accepted standard model, goes well beyond the specific technical details of the project, and considers these additional factors, such as: environmental impacts and constraints; organizational characteristics; resource requirements; scope identification and control; resource needs and procurement; and budgetary management (PMI, 2013).

METHODOLOGY

A two-step process will be used to accomplish the goals of this effort. Each step will be used to support each of the two research questions presented in the introduction. First, to address research question 1, the concept of a digital forensic investigation will be compared to the characteristics of a traditional project to establish whether it is reasonable to consider project management approaches as applicable to DFI efforts.

Next, to address research question 2, an existing taxonomy of DFI Challenges (Karie & Venter, 2015) and challenges found in other literature will be compared to the Knowledge Areas from the Project Management Body of Knowledge (PMI, 2013). A list of current challenges in digital forensics investigations will be compiled based on a review of recently published journal articles and conference proceedings which reference open DFI challenges which are still in need of additional research. An attempt will be made to match the identified DFI challenges with knowledge areas in the project management body of knowledge.

Three mappings were made by the research effort to examine whether the Project Management Body of Knowledge (PMBOK) is potentially useful for DFI challenges. First, the researchers created a mapping between project characteristics and the characteristics of digital forensics investigations. Second, the phases of typical projects were compared with the phases of DFI. Finally, challenges in DFI were mapped to sections of the Project Management Knowledge areas, and examples of possible activities were given.

The methodological approach used in this paper is knowledge mapping and has been used in prior work. Mapping is a useful technique for exploring the linkages between separate but related knowledge taxonomies. Prior work in information systems education led to the development of an information systems exit exam whose test items were created based on linkages between curriculum knowledge areas and exit skills (Daigle et al., 2004; Reynolds et al., 2004). Another effort involved having IS education professionals using an approach similar to this research effort to map IS model curriculum learning objectives to specific objectives of IS courses taught at their institutions (Presley et al., 2006).

Recent work has also linked the project management body of knowledge used in this study to cybersecurity frameworks. One study mapped PMBOK risk management activities to a U.S. Department of Defense cybersecurity risk management framework (Presley and Landry, 2016). Subsequent studies (Presley, Landry & Shropshire 2018a and 2018b), built on the first study to create a project meta-phase framework used to model the early presence and impacts of cybersecurity events in projects. Although the conceptual model relationships suggested by the prior work is different, the proximity between DFI and project management further suggested to the researchers that the PMBOK Knowledge Areas may also be useful studying the challenges of digital forensics investigations.

Mapping Project Characteristics to the Characteristics of Digital Forensics Investigations

Using a qualitative review of both models, the researchers compared the characteristics of a project as defined in the PMI Project Management Body of Knowledge (PMI, 2013) to the characteristics of DFI (Carrier and Spafford, 2004; National Research Council, 2009; Selemat et al., 2008). See Table 1. To further develop the idea that DFI could be considered a specialized IT project, additional characteristics from an IT project management text (Marchewka, 2015) will also be considered which deals with specific roles and tasks.

Table 1 – Comparison of Project and Digital Forensic Investigation Characteristics

PMI and IT Project Characteristics (PMI, 2013; Marchewka, 2015)	**Do Digital Forensic Investigations (DFI) have these characteristics?**
Occur for a limited duration. The project represents a temporary endeavor, having a beginning and an end.	**Yes –** DFI are temporary, have limited durations, but may be part of the ongoing detection and prosecution process (Carrier & Spafford, 2004, Grispos et al. 2014).
Creates a unique product, service, or result.	**Yes -** the results of each DFI are potentially unique (Carrier & Spafford, 2004; Bulbul et al., 2013).
Have a set of objectives, which may vary regarding their maturity (deterministic versus iterative)	**Yes -** DFI have objectives, which may change based on testing of hypotheses (Carrier & Spafford, 2004).
Have stakeholders.	**Yes –** DFI have many stakeholders (Bulbul et al., 2013).
Results are intended to be permanent, usually, but may also be used for temporary objectives.	**Yes –** DFI results are often intended to prevent, discourage or reduce the ability to inflict further harm (National Research Council, 2009 pp. 1-35).
Have the potential for social, economic, and environmental impacts to a greater or lesser degree	**Yes** - DFI are performed in response to criminal activities, terrorism, cybersecurity events, and national security concerns (National Research Council, 2009 pp. 1-35).
Can involve single or multiple individuals and organizations	**Yes –** DFI can include one or more organizations (National Research Council, 2009 pp. 1-35, 201-204)**.**
Composed of interdependent phases, tasks, and subtasks (often described as a “work breakdown structure”)	**Yes –** DFI are comprised of related and dependent phases, tasks, and subtasks (Ieong, 2006; Bulbul et al., 2013)
Contain roles for Project Sponsor, Project Manager, Subject Matter Experts, and Technical Experts	**Yes –** Each of these roles can be mapped to similar roles in DFI (Ieong, 2006).

Following is a more detailed discussion of the qualitative factors – for simplicity, some characteristics in the PMI model are grouped and discussed together.

PMI Project Characteristics Set 1

The PMBOK (PMI, 2013) describe projects as having the following characteristics:

- *Occur for a limited duration. Projects represent a temporary endeavor, having a beginning and an end*
- *Creates a unique product, service, or result*

This description is also consistent with the nature of digital forensics investigations. Digital forensics investigations are primarily done to test hypotheses about specific events that occurred. (Carrier & Spafford, 2004). The investigation is a temporary effort with a defined beginning and end, and it will "create a unique result" (i.e., the results of testing the hypothesis). These results and outcomes can be as diverse as the prosecution of a criminal case, evidence in a civil case, or prevention of a national security event (National Research Council, 2009 pp. 201-204).

PMI Project Characteristics Set 2

The PMBOK (PMI, 2013) describe projects as having the following characteristics:

- *Projects have a set of objectives, which may vary regarding their maturity (deterministic versus iterative)*

Digital forensics investigations have specific objectives, which may change over time as the investigation matures. In the definition of forensics investigations, the objectives are described as being "to develop and test theories, which can be entered into a court of law, to answer questions about events that occurred." (Carrier & Spafford, 2004)

The fact that digital forensic investigations develop and test theories about events which occurred also suggests a clear variance in maturity and potential scope, which can range from deterministic activities (e.g., a limited scope investigation of one single device) to iterative processes (e.g., a full-scale investigation where all the actors and devices are not known initially). Variability in scope is also consistent with the description of projects found in the project management literature (PMI, 2013)

PMI Project Characteristics Set 3

The PMBOK (PMI, 2013) describes projects as having the following characteristic:

- *Projects have stakeholders*

Digital forensics investigations have stakeholders with unique interests and requirements (Ieong, 2006). For example, there are frequently two at least two main groups involved in a DFI - investigators and legal personnel. Each of these groups has a different perspective and requirements. Examples of stakeholders in a DFI include:

Courts – rely upon evidence, which "can be entered into a court of law" (Carrier & Spafford, 2004). The is a central focus in literature related to improving all forensics capabilities, including digital forensics (National Research Council, 2009 pp. 1-35).

Policy or law-making bodies – often the DFI investigations are centered around "one or more digital events that violates a policy (an incident) or a law (a crime)." (Carrier & Spafford, 2004). Again, this is a major concern for the government (National Research Council, 2009 pp. 1-35).

Affected parties/victims of an event – government literature identifies society, criminals, and litigants as all being stakeholders of investigations in general, including DFI (National Research Council, 2009 pp. 1-35). Other academic literature also implicitly or explicitly considers the interests of various stakeholders (Ieong, 2006; Bulbul et al., 2013)

Public– government-sponsored research includes the need to protect the public from wrongful prosecution or imprisonment and cites improper forensics techniques as a possible source of risk (National Research Council, 2009 pp. 1-35). Privacy concerns are also a significant source of recent public attention.

Digital Forensics Investigators and Organizations – active participants in conducting the digital forensics investigation. Costs, training, availability of resources are examples of reasons why participants are impacted by and have an interest in the investigations they conduct (Ieong, 2006; National Research Council, 2009 pp. 1-35).

PMI Project Characteristics Set 4

- *Results are intended to be permanent, usually, but may also be used for temporary objectives*
- *Have the potential for social, economic, and environmental impacts to a greater or lesser degree*
- *Can involve single or multiple individuals and organizations*

Digital forensics investigations, like all forensics activities, can have a profound impact on society and the stakeholders of an investigation, when they are part of a criminal or civil process. Similarly, they can affect national security. These impacts are described extensively in government-sponsored research (National Research Council, 2009 pp. 1-35).

DFI is often used to establish a hypothesis about (and therefore culpability for) criminal and civil digital events, which may end up in a court of law (Carrier & Spafford, 2004). DFI then may produce permanent results (e.g., a conviction or other legal sanctions) and have wide potential impacts.

PMI Project Characteristics Set 5

According to both PMI PMBOK (PMI, 2013) and a referenced text (Marchewka, 2015), a defining characteristic of projects is:

- *Projects are composed of interdependent phases, tasks, and subtasks (often described as a "work breakdown structure")*

This description is also consistent with DFI literature. Phases are commonly used to group DFI activities into a hierarchy, with many different models for doing so proposed over the last 20 years (Carrier and Spafford, 2004; Selemat et al., 2008). Recent research efforts describe how digital forensics investigations are comprised of related and dependent phases, tasks, and subtasks (Ieong, 2006; Bulbul et al., 2013).

IT Project Characteristic Roles

According to a widely used text on managing IT projects, these projects are typically comprised of phases, tasks, and subtasks. They also have typical roles including Project Sponsor, Project Manager, Subject Matter Experts, and Technical Experts (Marchewka, 2015)

In the DFI process, it is straightforward to map these common project roles to the stakeholders in a digital forensics investigation. The following list contains common DFI roles identified in an academic research effort (Ieong, 2006) which map to the project roles listed above:

Project Sponsor**:** responsible for initiating the DFI and defining procedures, standards, and guidance. May include corporate security officers, law enforcement leadership, or prosecutors who would make decisions on charges and whether to proceed. Corresponding DFI roles (Ieong, 2006) may include the system/business owner. To a limited degree, this may also be the Case Leader.

***Project Manage*r**: In the DFI world, this would likely be a lead investigator or actual position entitled "Forensics Project Manager" – as of this writing, a search through several job sites returned multiple job opportunities with similar titles. Corresponding DFI role (Ieong, 2006) would be the Case Leader.

Subject Matter Experts and Technical Experts – In DFI, these are the resources with the technical skills and experience to perform the extraction and analysis of digital data in a forensically sound matter. This category also includes legal experts. The corresponding DFI roles (Ieong, 2006) would include the Legal Advisor, Security/System Architect/Auditor, Digital Forensics Specialist, Digital Forensics Investigator/System Administrator/Operator, and Digital Forensics Analyst.

Mapping PMI Project Phases to DFI Phases

As noted in the prior section, both digital forensics investigations and projects are composed of phases, which include tasks and subtasks which represent activity. The next stage for this research effort was to consider whether typical project phases would map to typical phases of digital forensics investigations.

Using the PMI PMBOK model, projects can be mapped to a generic lifecycle (PMI, 2013), along with the relevant process groups. As with DFI, projects are often organized into stages – and it is common for these phases to overlap. (PMI, 2013). Project processes may be predictive or iterative. A predictive process requires that most of the activities needed to meet the goals of the project are known up front. Iterative project activities involve processes where the end product is not fully known.

A recent effort by the research team recommended a high-level approach using project meta-phases to considering project activities (Figure 2). The project meta-phases are presented as a "wide lens" to consider project activities, and are intended to capture better the preparation and project selection process (called the "Project Conception" meta-phase) and the consequences of project outcomes (called the "Deliverable Use" meta-phase). It was thought that this would also be useful for describing digital forensics investigations, as the DFI readiness of organizations is a recurring theme in recent DFI literature (Reddy & Venter, 2013). The actual DFI investigation would correspond to the "Project Execution" Metaphase, as shown in Figure 2.

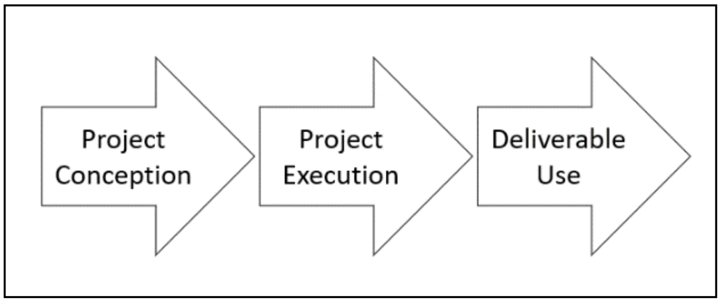

Figure 2 – Project Meta-phases (Presley, Landry, & Shropshire, 2018b)

The Carrier and Spafford (2004) model was used to represent DFI phases. The following table (see Table 2 below) shows at a high level how these models can be compared based on similar activities:

Table 2 – Comparison of DFIs to Projects by Temporal Phase

DFI Phases (Carrier & Spafford, 2004)	**Related PMI Phase(s) (PMI, 2013)**	**Project Meta-Phase (Presley, Landry, and Shropshire, 2018a)**	**Similar activities**
Readiness	Pre-condition to Starting the Project	Project Conception	Ensuring that resources are available, both human expertise and equipment, to ensure that the project will meet objectives.
Deployment	Starting the Project Organizing and Preparing	Project Execution	Identifying the need for the project, getting authorization for the project and use of resources, defining goals and scope
Physical Crime Scene Investigation	Carrying out the project	Project Execution	Performing tasks to achieve project / DFI objectives. May include iterative refinement
Digital Crime Scene Investigation	Carrying out the project	Project Execution	Performing tasks to achieve project / DFI objectives. May include iterative refinement
Presentation	Closing the Project	Project Execution (closeout) / Deliverable Use (after effects)	Delivery of outputs to stakeholders, which may include presenting findings in a court of law, releasing project / DFI resources, and formal closeout.

Mapping Project Management Knowledge Areas to DFI Challenges

The final phase of this research effort involved considering whether the project management knowledge areas would be useful in addressing challenges which were identified in the DFI literature.

A key component of the PMI project management body of knowledge is the idea of knowledge areas. At a high level, these knowledge areas represent the types of knowledge that are key to successful projects. All descriptions that follow are consistent with the PMI Project Management Body of Knowledge, Fifth Edition (PMI, 2013). During the research effort, a more recent edition of the PMI Body of Knowledge was released, which will be revisited in a future effort.

These knowledge areas are specifically designed to address and prevent potential problems from occurring that would threaten the outcome of the project. If DFI is considered to be a specialized type of information systems project, it should be possible to suggest specific DFI challenges which may occur in the context of these knowledge areas and find examples in the current literature.

This effort looked at each of the Project Management Knowledge Areas and proposed possible challenges in a DFI context that may occur if there are shortfalls in the knowledge of these areas by digital forensics teams. Appendix 1 captures this initial mapping effort, which is expected to be useful as a framework for further expert validation and in suggesting research efforts.

The following section summarizes the types of challenges that are currently being discussed in the literature which may be addressable using the project management knowledge areas. These challenges may benefit from further research through the lens of the project management literature in each area.

Organizational Influences and Project Lifecycle

This knowledge area deals with the effect of organizational characteristics on the project. These characteristics map to the concept of DFI organizational readiness, which has been seen in the DFI literature (Reddy & Venter, 2013). Government and academic research efforts have also suggested the following areas as concerns for DFI and forensics investigations in general (Reddy & Venter, 2013; National Research Council, 2009 pp. 1-35 and 201-204; Lutui, 2016)

Another consideration is the organizational and individual efforts that have been put in place to plan for DFI readiness. One study considered the cognitive approaches for the formation of DFI plans (Pooe & Labuschagne, 2012)

Some examples of DFI challenges that may be related to this area include:

- Availability of resources needed to conduct DFI – hardware, software, storage, or subject matter experts
- Definition of standards, expectations, and oversight – such as evidence handling, chain of evidence
- Clarity of organizational goals related to DFI investigations
- Policies or laws which impact the effective collection of data needed for a digital forensics investigation
- Jurisdictional problems and challenges

Project Management Processes

This knowledge area deals with all the processes required to manage the project: Initiating, Planning, Executing, Monitoring, and Closing. Recent literature has recognized that DFI efforts are comprised of many phases, with interdependent tasks and subtasks (Ieong, 2006; Bulbul et al., 2013; Reddy and Venter, 2013). These relationships can become quite complex, especially when differences between various technologies are taken into account (Grispos et al., 2012; Bulbul et al., 2013; National Research Council, 2009 pp. 1-35 and 201-204).

Possible DFI challenges related to this area include:

- Clarity of goals related to a specific DFI investigations
- Processes or standards for investigation
- Planning for typical DFI management functions
- Monitoring of investigation progress
- Closeout procedures, preventing loss of information that might help prevent future digital events (e.g., intrusions)

Integration Management

This knowledge area deals with the actions associated with defining and creating and integrating all the parts of a project plan, along with project resources. A project plan usually includes the project charter and a plan for directing and controlling work, performing change control, and facilitating close out phases. Typically these are actions performed by the project manager.

In the DFI literature, the role which is most closely associated with these activities is called case leader (Ieong, 2006). The case leader is seen as the overall "planner and conductor" of the DFI process. Cooperation and coordination between disciplines are also described as important (Lutui, 2016).

Possible DFI challenges related to this area could include:

- Availability of a plan for the investigation in enough detail, regularly adjusted
- Clarity of roles and responsibilities
- Change processes for scope changes, such as when new evidence becomes available

Scope Management

This knowledge area deals with planning the project scope management process, collect requirements, defining scope according to the stakeholder needs and the triple constraints (schedule, budget, scope). Creation a work breakdown structure, validation that the scope has been achieved, and controlling project scope changes during execution are also part of this process.

Typically the project manager works closely with project stakeholders to define and maintain the overall scope. Scope, along with quality and time, are the three legs of the triple constraint of project management (PMI, 2013).

DFI efforts similarly have to consider all of these areas – scope is balanced by time constraints, legal authority and privacy concerns, which is described by both academic (Ieong, 2006) and government-sponsored research (National Research Council, 2009 pp. 1-35). Other considerations may include problems with cost and available resources associated with storing and processing large amounts of data, which can be caused when the investigation scope is very broad or includes certain types of evidence (Grispos et al., 2012; Quick et al., 2014)

Examples of possible DFI challenges related to this area include:

- Avoiding the use of resources on irrelevant or out-of-scope activities
- Defining when to stop investigation activities based on legal and ethical guidelines (e.g., whether to stop once there is sufficient evidence to convict, or conversely whether to consider possible exculpatory scenarios)
- Rising costs associated with storing increasingly large amounts of data, such as in cloud services scenarios when the scope is not well defined

Time Management

This knowledge area deals with scheduling, task definition, sequencing, estimation of resources needed, task durations, and ongoing efforts to monitor and control the schedule during project execution. DFI literature describes these as being relevant – specifically the overall cost and time required to perform the investigations (Ieong, 2006).

Possible DFI challenges related to this area include:

- Preventing investigations from extending too long – failure to achieve the desired results.
- Ability to provide forensics data promptly to legal teams
- Avoiding resources shortages due to incorrect prioritization of investigation tasks
- Estimation of time required to perform DFI tasks

Quality Management

This knowledge area deals with the need to plan for quality and test for quality assurance to control the quality of project outputs. Regarding DFI efforts, government research expresses the need for quality in terms of both positive outcomes (e.g., a dangerous criminal is apprehended and prevented from harming others) and avoiding negative outcomes (e.g., an innocent person is improperly convicted of a crime). It is considered a critical issue in this context (National Research Council, 2009 pp. 1-35). Academic literature also describes the many roles and interdisciplinary processes that are required for producing quality (defined in terms of efficiency and effectiveness) in DFI efforts (Lutui, 2016; Ieong, 2006)

Possible DFI challenges related to this area include:

- Ensure support for proper investigation results
- Proper techniques to avoid dismissal of evidence
- Proper oversight of investigator processes
- Avoiding successful challenges by defense counsel leading to failures to convict.
- Avoiding wrongful convictions due to misapplied techniques or incorrect attribution
- Processes and coordination to optimize the use of DFI resources

Human Resource Management

This knowledge area deals with the processes needed to plan, acquire, develop, and manage the human resources needed to complete project tasks. In a DFI context, this includes training and recruiting investigators to handle rapid changes in technology (Grispos et al., 2012; Bulbul et al., 2013; Lutui, 2016) Several sources in the DFI literature discuss this topic as a key concern for organizations, either directly or by describing the need for competent multi-disciplinary expertise (Ieong, 2006; National Research Council, 2009 pp. 201-204; Lutui, 2016; Karie and Ventor, 2015; Cleveland and Cleveland, 2018)

Possible DFI challenges related to this area include:

- Ensuring sufficient resources to meet schedules and workload
- Reducing backlogs
- Avoiding case dismissal due to time limitations/expirations
- Ensuring sufficient personnel to detect and prevent intrusions to protect sensitive information

Communications Management

This knowledge area deals with all required communications between project stakeholders. Communication is considered one of the essential project processes (PMI, 2013). Similarly, DFI literature describes challenges in communications between the DFI roles (Ieong, 2006; Lutui, 2016), and suggests that improvements are needed, especially between the technically-oriented forensics investigators and the legal community.

Examples of possible DFI challenges related to this area include:

- Preventing unauthorized release of information
- Protecting private data
- Protecting security-sensitive information (e.g., logs with server addresses)
- Keeping the investigation team informed of key information or directions from legal team
- Ensuring legal team members are informed of key DFI results affecting the case

Cost Management

This knowledge area involves all financial controls in a project that are used to plan, estimate, budget, and control costs. Cost management is discussed in academic (Ieong, 2006; Bulbul et al., 2013; Reddy et al., 2011) and government-sponsored research (National Research Council, 2009 pp. 201-204). Finally, academic research has described how technology changes are driving investigation costs (Grispos et al., 2012; Quick et al., 2014; Lutui, 2016; Karie and Venter, 2015)

Possible DFI challenges related to this area include:

- Creating budgets for resources needed to support digital forensics teams
- Funding to procure needed equipment or specialized knowledge
- Controlling DFI costs to prevent exceeding the budgets of organizations and departments
- Forecast and plan for increased storage and processing costs associated with data quantity and workload increases

Risk Management

This knowledge area deals with the formulation of a risk management plan, identification, and analysis of risks (qualitative and quantitative), formulation of risk responses, and ongoing efforts to control risks. Government literature, in particular,, has been concerned with the risks of improper and inaccurate forensics efforts, including digital forensics (National Research Council, 2009, pp. 1-35 and 201-204). Many academic sources have also considered risk as an important factor, as well as the need to reduce risk and improve overall outcomes (Bulbul et al., 2013; Karie & Venter 2015; Lutui, 2016)

Possible DFI challenges related to this area include:

- Creation of risk assessments and mitigation strategies
- Establish controls and standards to reduce the risk of wrongful prosecutions
- Evaluate and mitigate risks to life and property using forensics techniques and capabilities

Procurement Management

This knowledge area deals with the acquisition of needed resources – planning, conducting the procurement process, controlling costs, and all close-out activities, including the disposition of project assets as required. DFI literature describes the procurement of resources as an important consideration of DFI efforts (Grispos et al., 2012; Reddy et al., 2011)

Possible DFI challenges related to this area include:

- Procure additional hardware to perform investigations due to increased storage and processing power needed
- Identify and procure additional forensics software to address new technology and standards, based on an evaluation of the investigation environment
- Ensure procurement of resources and specialists in time to support investigation tasks

Stakeholder Management

This knowledge area deals with the management of all stakeholders in a project. Stakeholders in project terms are defined as people and organizations with interest in the outcome of a project, both positive and negative. Both PMI (2013) and Marchewka (2015) identify stakeholder management as key to project success. Key activities in this area include the identification of stakeholders, planning for stakeholder management, and managing and controlling stakeholder engagement.

As mentioned in the prior sections, DFI efforts can be shown to have multiple stakeholders with unique interest, which can potentially conflict. A prior research effort described DFI efforts usually having eight typical roles, and identifying the common key questions that each role would typically consider (Ieong, 2006).

Possible DFI challenges related to this area include:

- Avoiding conflicts with stakeholder interests, including resource demands from other investigations
- Establish regular channels of communication between stakeholders (e.g., between forensic analysts and legal prosecutors)
- Controlling the impact of political influences on investigations
- Preventing or resolving conflict of interest scenarios
- Identification of stakeholder requirements as early as possible

Mapping Digital Forensics Challenges to Project Management Knowledge Areas

With this mapping, the next logical step was to consider whether recent research is identifying challenges that may be helped by considering the practices described in the PMI Project Management Knowledge Areas. A review of the literature was conducted to determine if challenges were being mentioned that could be mapped to the framework produced in Section 3.2

Karie and Venter (2015) presented a taxonomy of current challenges they identified during an extensive review of the literature. Their taxonomy includes four categories, as follows, with the number of challenges given in parentheses: technical challenges (12), legal systems and law enforcement challenges (6), personnel-related challenges (5), and operational challenges (4) for a total of 27 digital forensics challenges.

Based on the researchers' review of the digital forensics literature, and considering each DFI challenge in the taxonomy, individually, it was possible to map all of these challenges to the Project Management Knowledge areas. The challenges were considered one-by-one from the taxonomy. For each challenge, it was decided which of the PMBOK areas would be potentially relevant as having the potential to address the challenge. Where a linkage was identified, we wrote a description of the expected connection between the DFI challenge and the PMBOK area. In future work, this description will provide a starting point for validation by experts and motivate a search for solutions to the challenges. See Tables 3 through 6 below for a breakdown of the mapping detail for each of the four DFI challenge sets.

Table 3 – Technical Challenges Mapping Detail

Challenge	PMI Knowledge Areas Impacted	Examples
Encryption	Procurement Management	Procurement of hardware and software needed to defeat encryption
	Project Risk Management	Manage risks that some evidence may be encrypted and look for mitigation strategies.
Vast Volumes of Data	Procurement Management	Procure hardware and software needed to store large data
	Project Risk Management	Manage risk that volume will be too large to analyze, and find mitigation strategies
	Project Cost Management	Planning for increases in the cost of storage and processing hardware to accommodate increased data
Incompatibility Among Heterogeneous Forensic Tools	Procurement Management	Ensure that the tools purchased are interoperable. Procure tools that may be useful in managing the interfaces needed
	Project Risk Management	Manage risk of incompatibility of data from other agencies and form a mitigation plan to convert data.
Volatility of Digital Evidence	Time Management	Manage the schedule for the investigation to coordinate the collection of the data (e.g., raids, warrants are timed to reduce the risk of data destruction)
	Quality Management	Create a quality plan to ensure processes are understood and measured.
Bandwidth Restrictions	Procurement Management	Ensure that the bandwidth needed is sourced from telecom providers
Limited Lifespan of Digital Media	Time Management	Actively manage the schedule to reduce the risk of data loss.
Sophistication of Digital Crimes	Human Resource Management	Ensure that the project team or PMO has appropriate resources and training to handle sophisticated crimes
	Organizational Influences and Project Lifecycle	Ensure the organization is aware of and able to respond to sophisticated cyber attacks.

	Project Risk Management	Create a risk management plan and processes to identify and respond to advanced threats.
Emerging Technologies and Devices	Procurement Management	Plan for the acquisition and analysis of new devices that emerge on the market
	Human Resource Management	Hiring and training of technical experts who can perform the analysis
Limited Window of Opportunity to Collection of Potential Digital Evidence	Time Management	Actively manage the investigation schedule to ensure data is collected and reduce the risk of data destruction.
The Antiforensics	Project Risk Management	Analyze the risk and possible mitigation strategies for each type of antiforensics method – for example, provide a Faraday evidence bag to investigators to reduce the risk of remote cell phone wiping.
Acquisition of Information from Small-Scale Technological Devices	Human Resource Management	Ensure that the investigation team and PMO have personnel who are trained and experienced in data collection from all devices commonly encountered
	Procurement Management	Ensure that budget and a process for acquiring new devices is part of the procurement plan for the investigating organization
Emerging Cloud Computing or Cloud Forensic Challenges	Organizational Influences and Project Lifecycle	Ensure that senior management is focused on the importance and requirements for supporting the procurement, risk management, and resource needs required to manage new challenges
	Procurement Management	Ensure that budget and a process for acquiring new devices is part of the procurement plan for the investigating organization
	Project Risk Management	Identify the risks associated with new challenges, and form strategies to respond to these challenges in a methodical, organized manner.
	Human Resource Management	Ensure that the investigation team and organization have access to subject matter experts capable of analyzing and responding to new challenges.

Table 4 – Legal Systems and Law Enforcement Challenges Mapping Detail

Challenge	Relevant PMI Knowledge Areas	Examples
Jurisdiction	Integration Management	Analyze the possible conflicts between jurisdictions and the impacts on the investigation team
	Scope Management	Define the scope of the investigation such that jurisdictional concerns are factored it – if an investigation leads to a source that is inaccessible then the scope may be limited to focus on more accessible data.
	Time Management	Consider jurisdiction issues, such as the time needed to acquire evidence, as part of the investigation schedule
	Communications Management	Ensure that a channel of communication and contacts are defined for each jurisdiction
Prosecuting Digital Crimes (Legal Process)	Communications Management	Ensure that the communications and contacts are defined between the legal team or prosecutors and the investigation team.
	Human Resource Management	Plan for personnel who are knowledgeable of legal issues to be available for the investigation team and the organization in general.
Admissibility of Digital Forensic Tools and Techniques	Communications Management	Ensure that the chain of custody requirements are defined and properly communicated and that the channel between the investigation team and legal team is defined.
	Human Resource Management	Ensure that team members are trained properly.
	Quality Management	Create a plan for oversight and monitoring the proper use of tools.
Insufficient Support for Legal Criminal or Civil Prosecution	Integration Management	Ensure that the organization senior leadership is informed and is in agreement with the overall goals and requirements needed to support the investigation team.
Ethical Issues	Communications Management	Define a communication plan, such as a hotline, for team members to report ethical concerns
	Human Resource Management	Provide training in ethical and legal compliance in DFI
	Project Management Processes	Ensure that the project management plan includes ethical training and oversight as part of the project plan.

Privacy	Integration Management	Define and communicate the organization's privacy policy and get buy-in from senior officials
	Scope Management	Ensure that the DFI complies with the legal and ethical limitations such that they do not extend the scope to include prohibited information sources.

Table 5 – Personnel-related Challenges Mapping Detail

Challenge	Relevant PMI Knowledge Areas	Examples
Lack of Qualified Digital Forensic Personnel (Training, Education, and Certification)	Human Resource Management	Plan for the recruiting, hiring, and training of DFI qualified team members
Semantic Disparities in Digital Forensics	Communications Management	Publish a common lexicon as part of the communications plan
Lack of Forensic Knowledge Reuse among Personnel	Project Management Processes	Ensure the investigation project plan includes the time needed to research previous efforts, and document the work done on the current effort.
	Organizational Influences and Project Lifecycle	Communicate the need for reuse to senior management, and make sure that efforts to accomplish this will be funded and supported.
Lack of Formal Unified Representation of Digital Forensic Domain Knowledge	Project Communication Management	Create standard descriptions and resumes to be used internally for task descriptions and C.V.s
Forensic Investigator Licensing Requirements	Human Resource Management	Manage the training and processes needed to achieve certifications and licenses

Table 6 – Operational Challenges Mapping Detail

Challenge	Relevant PMI Knowledge Areas	Explanation
Incidence Detection, Response, and Prevention	Organizational Influences and Project Lifecycle	Ensure that the organizational processes are in place to initiate and scope digital investigation efforts. Monitoring and response planning must be part of the organization's strategic plans

Lack of Standardized Processes and Procedures	Organizational Influences and Project Lifecycle	Ensure that standards and processes for DFI are defined at the organization level.
	Stakeholder Management	Ensure that stakeholders are identified and are able to participate in the creation and revision of DFI standards and processes
Significant Manual Intervention and Analysis	Human Resource Management	Ensure that qualified specialists are available to handle the work needed to complete an investigation
	Procurement Management	Identify and procure tools that will reduce the need for manual efforts.
Digital Forensic Readiness Challenge in Organizations v. Trust of Audit Trails	Stakeholder Management	Identify and solicit input from stakeholders who have an interested in DFI readiness
	Organizational Influences and Project Lifecycle	Create awareness and seek support from senior leadership with regards to DFI requirements, processes, and standards

DFI Challenges to Project Management Knowledge Area: Mapping Results Summary

The following tables summarize the results of the mapping effort. In the left-most column (x-axis), the DFI Challenges (Karie & Venter, 2015) are listed. Across the top (y-axis) are each of the Project Management Knowledge Areas (PMI, 2013). A value of “1” in a cell represents a successful mapping between a DFI challenge set and a Project Management Knowledge Area. In the right-most column (“Total”) the total number of successful mappings is indicated.

Table 7 shows the mapping between the DFI technical challenges and the PM areas. The technical challenges mapped heavily to two PM areas: risk and procurement management. A total of 13 of the 24 mappings were to these two areas.

Table 8 shows the mapping between two DFI challenge sets--legal system and personnel-related—against PM areas. As these DFI areas are people-related, it is no surprise that project human resource and communications management areas are heavily mapped, accounting for 11 of the 21 total mappings.

Table 9 illustrates the Operational DFI challenges mapped to PM areas. Four PM areas touched the operational challenges: organizational influences, HR management, procurement management, and stakeholders. In the summary row, the total counts of mapping intersections across all tables are provided. There were a total of 51 DFI-PM pairs.

Table 7 – Technical Challenges to PM Areas

	Organizational influences & project lifecycle	project management process groups	project integration mgmt	project scope mgmt	project time mgmt	project quality mgmt	project human resource mgmt	project communication mgmt	project cost mgmt	project risk mgmt	project procurement mgmt	project stakeholder mgmt	Total
1. TECHNICAL CHALLENGES													
i. Encryption										1	1		**2**
ii. Vast Volumes of Data									1	1	1		**3**
iii. Incompatibility Among Heterogeneous Forensic Tools										1	1		**2**
iv. Volatility of Digital Evidence					1	1							**2**
v. Bandwidth Restrictions											1		**1**
vi. Limited Life span of Digital Media					1								**1**
vii. Sophistication of Digital Crimes	1						1			1			**3**
viii. Emerging Technologies and Devices							1				1		**2**
ix. Limited Window of Opportunity to Collection of Potential Digital Evidence					1								**1**
x. The Antiforensics										1			**1**
xi. Acquisition of Information from Small-Scale Technological Devices							1				1		**2**
xii. Emerging Cloud Computing or Cloud Forensic Challenges	1						1			1	1		**4**

Table 8 – Legal System and Personnel Challenges to PM Areas

	Organizational influences & project lifecycle	project management process groups	project integration mgmt	project scope mgmt	project time mgmt	project quality mgmt	project human resource mgmt	project communication mgmt	project cost mgmt	project risk mgmt	project procurement mgmt	project stakeholder mgmt	Total
2. LEGAL SYSTEMS AND/OR LAW ENFORCEMENT CHALLENGES													
i. Jurisdiction			1	1	1			1					**4**
ii. Prosecuting Digital Crimes (Legal Process)							1	1					**2**
iii. Admissibility of Digital Forensic Tools and Techniques						1	1	1					**3**
iv. Insufficient Support for Legal Criminal or Civil Prosecution			1										**1**
v. Ethical Issues		1					1	1					**3**
vi. Privacy			1	1									**2**
3. PERSONNEL-RELATED CHALLENGES													
i. Lack of Qualified Digital Forensic Personnel (Training, Education, and Certification)							1						**1**
ii. Semantic Disparities in Digital Forensics								1					**1**
iii. Lack of formal Unified Representation of Digital Forensic Domain Knowledge								1					**1**
iv. Lack of Forensic Knowledge Reuse among Personnel	1	1											**2**
v. Forensic Investigator Licensing Requirements						1							**1**

Table 9 – Operational Challenges to PM Areas and Total Mapping Results

	Organizational influences & project lifecycle	project management process groups	project integration mgmt	project scope mgmt	project time mgmt	project quality mgmt	project human resource mgmt	project communication mgmt	project cost mgmt	project risk mgmt	project procurement mgmt	project stakeholder mgmt	**Total**
4. OPERATIONAL CHALLENGES													
i. Incidence Detection, Response, and Prevention	1												**1**
ii. Lack of Standardized Processes and Procedures	1												**1**
iii. Significant Manual Intervention and Analysis							1				1		**2**
iv. Digital Forensic Readiness Challenge in Organizations	1											1	**2**
v. Trust of Audit Trails													
TOTALS	**6**	**2**	**3**	**2**	**4**	**3**	**9**	**6**	**1**	**6**	**8**	**1**	**51**

RESULTS

It was possible for the researchers to map the characteristics and phases of projects to equivalent characteristics and phases of digital forensics investigations, as identified in the literature. The researchers were also able to provide qualitative support for each intersection between the two models: in most cases, peer-reviewed literature was found describing the challenges that the project management literature describes in the context of digital forensics investigations.

Based on a review of the content of the descriptions of challenges in the digital forensics' literature, the research team was able to map all 27 Digital Forensics challenge areas identified in the taxonomy (National Research Council, 2009; Karie and Venter, 2015) to the PMI Project Management Knowledge Areas.

The research effort provided results which address the two research questions as follows:

R1 – Do Digital Forensics Investigations (DFI) share many of the same characteristics and processes as traditional projects as defined by a common standard?

Results: By mapping the characteristics and processes between DFI and project management, it was shown that they share many of the same characteristics and processes. A digital forensic investigation was shown to be unique, purposeful, temporary endeavor with stakeholders and carried out by an interdependent team in temporal phases.

R2 – Do the practices and knowledge areas in this project management standard contain information that may be useful for addressing challenges in the Digital Forensics field?

Results: In mapping the project management knowledge areas to common DFI challenges, it was shown that each of 27 DFI challenges mapped to at least one project management knowledge area, and each PMBOK area mapped to at least one DFI challenge. A total of 51 DFI-PMBOK pairs were identified, and for each, a descriptive explanation of that connection was provided. The PMBOK areas with the most linkages to DFI challenges were project human resource management (9 linkages), and project procurement management (8 linkages), followed by project risk management and project communication management (6 each).

SUMMARY OF CONCLUSIONS

The team found that the project management literature closely describes the same types of characteristics and challenges that are found in the digital forensics investigation literature. These findings appear to support the idea that digital forensics investigations could be described and further researched as a specialized type of information systems project.

This effort was intended to be a first attempt at mapping the project management literature to digital forensics investigations. The mapping as described in the results section was based on the experience and knowledge of the research team and is not meant to be the final word on this topic. It is however very suggestive that future research in this area may be fruitful. A similar strategy was used in the development of curriculum models to demonstrate how expected learning units were being implemented in actual Information Systems courses (Daigle et al., 2004; Presley et al., 2006). This effort can similarly be thought of as the first mapping attempt of digital forensics investigation challenges to project management knowledge areas. More mappings by both digital forensics and project management researchers will be needed to confirm the results.

The overall implication of this study is that the challenges of digital forensic science can be addressed by project management knowledge and practice. Viewing digital forensic investigations as projects, we found 51 potential solution vectors for further exploration. For instance, the technical DFI challenge presented by the presence of vast volumes of data can be linked to the project procurement management knowledge area. This could point to a possible solution such as a project procurement strategy which might include the acquisition of computer hardware and software to store and process large data sets and procuring other resources from outside the organization. Each connection between DFI challenge and PMBOK area is valuable as it serves as a potential research question for further exploration, or as a suggested avenue for finding practical solutions to DFI problems.

A limitation of these results is that the mapping taxonomy represents the interpretations of the authors only, and have not been validated using, for example, a panel of experts. These limitations are expected to be addressed in future research.

SUGGESTIONS FOR FUTURE RESEARCH

There is much more research that is needed to develop the ideas presented in this effort. First, to address the major limitation of this study, the results of should be validated with a larger group of experts in the fields of project management and digital forensics. A Delphi method might be employed to determine whether the mapping suggested by this effort is accepted. As previously discussed, further use of the mapping methodology similar to that used in curriculum development may prove useful (Daigle et al., 2004), along with a software-supported approach (Presley et al., 2006).

Next, a method needs to be developed for considering additional challenges and appropriate responses. A potential approach could use this effort as a starting point, and evaluate additional challenges against the taxonomy, and determine whether the specific recommendation in project management literature is potentially helpful.

Researched focused on the application of project management principles to digital forensics investigations, either real or simulated, would be the next step to determine whether PM practices would definitively benefit DFIs. Risk management is a critical (and often overlooked) part of project management (Marchewka, 2015), and is expected to be an underlying concern for many challenges described in the digital forensics investigation literature (Reddy & Venter, 2013; Bulbul et al., 2013; Karie and Venter, 2015; Grispos et al., 2014).

Finally, the project management body of knowledge needs to be enhanced or expanded through future research to include unique requirements of digital forensics investigations – both within the context of the project management practices as applied to the investigations and in the context of the forensics characteristics of deliverables produced by information systems projects.

REFERENCES

Bulbul, H. I., Yavuzcan, H. G., & Ozel, M. (2013). Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). *Forensic Science International*, 233(1–3), 244–256. https://doi.org/10.1016/j.forsciint.2013.09.007

Carrier, B. D., & Spafford, E. H. (2004). An Event-Based Digital Forensic Investigation Framework, *Digital Forensic Research Workshop (DFRWS).*

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

Cleveland, M. and Cleveland, S. (2018). Cybercrime Post-incident Leadership Model. *Proceedings of the Thirteenth Midwest Association for Information Systems Conference*, Saint Louis, Missouri May 17-18, 2018 https://works.bepress.com/simon_cleveland/29/

Daigle, R. J., Longenecker, H. E., Landry, J. P. & Pardue, J. H. (2004). Using the IS 2002 Model Curriculum for Mapping an IS Curriculum. *Information Systems Education Journal*, 2(1). http://isedj.org/2/1/

Grispos, G. Glisson, W. B., & Storer, T. (2014). Rethinking Security Incident Response: The Integration of Agile Principles. *20th Americas Conference on Information Systems (AMCIS 2014)*, Savannah, Georgia.

Grispos, G., Storer, T., & Glisson, W.B. (2012). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. *International Journal of Digital Crime and Forensic*s, 4(2), 28-48.

Karie, N. M. & Venter, H. S. (2015). Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences*, 60(4), 885–893.

Ieong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 3, 29–36. https://doi.org/10.1016/j.diin.2006.06.004

Lutui, R. (2016). A multidisciplinary digital forensic investigation process model. *Business Horizons*, 59(6) 593-604. http://dx.doi.org/10.1016/j.bushor.2016.08.001

Marchewka, J. (2015). *Information Technology Project Management*, Fifth Edition, Hoboken, NJ: John Wiley and Sons.

National Research Council (2009). *Strengthening Forensic Science in the United States: A Path Forward*. (2006-DN-BX-0001 No. 228091). Washington DC: US Department of Justice. Pp. 1-35, 201-204. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf

PMI – Project Management Institute (2013). *A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Fifth Edition*. Newtown Square, PA: Project Management Institute.

Pooe, A., and Labuschagne, L. (2012). Cognitive Approaches for Digital Forensic Readiness Planning. *9th International Conference on Digital Forensics (DF)*, Jan 2013, Orlando, FL, United States. Springer, IFIP Advances in Information and Communication Technology, AICT-410, pp. 53-66, 2013, Advances in Digital Forensics IX. <10.1007/978-3-642-41148-9_4>. <hal-01460620>

Presley, S. S. & Landry, J. P. (2016*)*. A Process Framework for Managing Cybersecurity Risks in Projects (1st ed., vol. 8). *SAIS 2016 Proceedings*. 8. http://aisel.aisnet.org/sais2016/8

Presley, S. S., Landry, J. P., & Shropshire, J. D. (2018a). Cybersecurity Threats in the Context of Project Meta-Phases. *Americas Conference for Information Systems (AMCIS 2018)*, New Orleans, LA.

Presley, S. S., Landry, J. P. & Shropshire, J. D. (2018b). Three Meta-Phases of a Project. *SAIS 2018 Proceedings*. 5. https://aisel.aisnet.org/sais2018/5

Presley, Longenecker, Pardue, and Landry (2006). Suggested Characteristics of User Interfaces in Support of IS 2002 Curriculum Model Implementation and Program Accreditation. *Information Systems Education Journal*, 4 (97). http://isedj.org/4/97/. ISSN: 1545-679X. (Also appears in The Proceedings of ISECON 2005: §3372. ISSN: 1542-7382.) http://isedj.org/4/97/

Quick, Darren, and Choo, Kim-Kwang Raymond (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation* 11; 273-294. http://dx.doi.org/10.1016/j.diin.2014.09.002

Reddy, K., & Venter, H. S. (2013). The architecture of a digital forensic readiness management system*. Computers & Security*, 32, 73–89. https://doi.org/10.1016/j.cose.2012.09.008

Reddy, K., Venter, H. S., and Olivier, M. S. (2011). Using time-driven activity-based costing to manage digital forensic readiness in large organizations. *Inf Systems Frontiers*. 14(5):1061–1077. DOI 10.1007/s10796-011-9333-x

Reynolds, J., Longenecker, H. E., Landry, J. P., Pardue, J. H., & Applegate, B. (2004). Information Systems National Assessment Update: The Results of a Beta Test of a New Information Systems Exit Exam Based on the IS 2002 Model Curriculum. *Information Systems Education Journal*, 2(24). isedj.org/2/24/.

Selemat, S. R., Yusof, R., & Shaib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. *IJCSNS International Journal of Computer Science and Network Security*, 8 (10), 163-169.

Sharevski, F. (2015). Rules of professional responsibility in digital forensics: A comparative analysis. Journal of Digital Forensics, *Security and Law*, 10(2), 39–54.