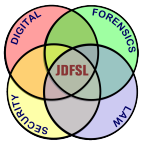

THE JOURNAL OF
DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 2 Article 9

6-30-2017

Applying a Contingency Framework to Digital Forensic Processes in Cloud Based Acquisitions

Diane Barrett
Bloomsburg University, dbarrett@bloomu.edu

APPLYING A CONTINGENCY FRAMEWORK TO DIGITAL FORENSIC PROCESSES IN CLOUD BASED ACQUISITIONS

Diane Barrett
Bloomsburg University
Mathematical and Digital Sciences
Bloomsburg, PA 17815
dbarrett@bloomu.edu

ABSTRACT

The change in business models to incorporate a wide variety of cloud computing environments has resulted in the escalation of computer crimes in the areas of security breaches and hacking. Methods to acquire evidence in a cloud computing environment are limited due to the complexity of the cloud environment. Since digital acquisition processes in cloud computing environments are still in the infancy stages, there have been no studies in the application of existing frameworks to this type environment based on traditional forensic processes.

This paper describes a qualitative study conducted to develop a robust contingency framework for deciding when to use traditional forensic acquisition practices, when to use modified processes, and when it is necessary to develop new forensic acquisition processes more appropriate to the cloud computing environment. The contingency framework was developed through the evaluation of 20 common forensic procedures by a panel of forensic and cloud computing subject matter experts.

Keywords: contingency theory, forensics, cloud computing

1. INTRODUCTION

As business models and technology evolve, information security and digital investigation practices must also change (Fiaidhi, Bojanova, Zhang, & Zhang, 2012). Information security and digital acquisition practices have come to the forefront of business concerns in light of legislation, talk of cyber war, and a Department of Homeland Security (DHS) recent public call for an army of cyber reservists equal to our military reserves (Corrin, 2016). Cloud computing technology raises questions about the effectiveness and application of traditional forensic acquisition approaches (Almulla, Iraqi, & Jones, 2014). Conditions conducive to the development of new processes are becoming more frequent in all areas of information security practices, including digital forensics (Kessler, 2011).

Although available information technology and information security research has generated many compelling theories, the

integration of these theories is inadequate (Thomas, Gupta, & Bostrom, 2008).

Carlton (2007) identified and measured 103 key forensic data acquisition processes such as turning off the computer before creating a forensic image, creating a forensic image, and verifying the created image by utilizing a panel of experts. There are 20 conventionally recognized practices (See Appendix A) that were investigated per their relevance to cloud computing and that gap was the focus of the study.

The purpose of the qualitative study was to develop a robust contingency framework for deciding when to use traditional forensic acquisition practices, when to use modified processes, and when it is necessary to develop new forensic acquisition processes through the evaluation of 20 conventionally recognized forensic acquisition processes by a panel of subject matter experts (SMEs). The main agenda in doing this research was bringing a framework based on subject matter expert opinions to the attention of forensic examiners on the applicability of current forensics evidence acquisition procedures to cloud computing environments. Since there is a lack of knowledge and understanding about the applicability of forensic evidence acquisition processes in cloud computing environments by examiners, the goal was to provide enlightenment in this area, making forensics investigations more productive and the prosecution of criminal activity more likely (Daryabar, Dehghantanha, & Udzir, 2013; Zimmerman & Glavach, 2011).

2. LITERATURE REVIEW

Contingency theory defines the response to situational variables in order to attain organizational objectives (Baird, Furukawa, & Raghu, 2012). Contingency theory also affects the initiation and adoption of change in organizations (Battilana & Casciaro, 2012). In information security, both external and internal forces shape what threatens and how to protect information systems (Pieters, 2011). Intertwined in the threat and protection landscape of information systems are people. People are both attackers and defenders of information data and systems (Dae Ham, Hong, & Cameron, 2012).

When disruptive technology such as cloud computing becomes a part of the organizational technology, there will be an information security transition period during which the security posture will need to adapt (Ngo, Zhou, & Warren, 2005). The adoption of such technology may not necessarily coincide with the ability to proactively protect and investigate the environment based on current employee skills and job tasks (Ke, Tan, Sia, & Wei, 2012). In order for contingency theory to be effective, processes must be adapted to the organizational situation (Kalchschmidt, 2011). When an organization moves to a cloud computing environment, some of the processes that need to be adapted are the cloud computing model to follow, security planning, forensic contingency planning, and collaboration across technology disciplines (Armbrust et al., 2010).

The fundamental issue in this study was the effect on information technology digital forensic acquisition processes by organizational adoption of cloud computing technology. Contingency theory allows for decision making about the relevance of traditional forensic acquisition processes to be used based on the principles that that there is not one rigid way to make decisions about conducting forensic acquisitions in cloud computing environments and provides generalizations about the best fit of different processes (Qiu, Donaldson, & Luo, 2012).

The main characteristics of information security contingency theory are parallel to the characteristics of the forensic examination of

cloud computing environments. This parallelism provided relevance to the study. Information security contingency characteristics include considering the environments both inside and outside the organization and choosing the appropriate security strategy (Tassabehji, 2005). The parallel digital forensic acquisition focus is considering both the external and internal cloud computing environment factors and choosing the appropriate forensic process strategy.

The study methodology used to develop a new forensic choice set consisting of information-contingent plans for choosing actions based on the uncertainty of information was conceptual and based on existing frameworks (Mathiassen, & Sorensen, 2008). The resulting framework offers a realistic view of cloud computing environment variables that allows forensic acquisition process decisions to be made without making prior assumptions that traditional forensic processes must apply. The contingencies examined are the NIST defined cloud computing service and deployment models applied to current forensic acquisition processes.

The basis for the underlying theoretical application associated with the research study relied on contingency theory to provide a framework for determining when to use traditional forensics acquisition processes, when to use modified processes, and when the development of new methods is required for forensic evidence acquisitions in cloud computing environments. The applicable theoretical framework used in linking this study to other information security research using contingency theory was the framework proposed by Austin and Devin (2009). The research extends the analytical framework of Austin and Devin (2009) by creating a framework for cloud computing forensic acquisition processes based on the contingency framework for determining when to use plan-based methods and when to use agile methods. The potential of digital technology makes it essential to move away from disagreements about traditional forensics versus new methods to a research-based and practical relevance dialogue that examines the related contingencies while formulating a suitable framework for when traditional, modified, and new methods are used for forensic evidence acquisitions in cloud computing environments (Austin & Devin, 2009; Garfinkel, 2010).

This new framework indicates the numerous openings for information systems (IS) research to provide a major contribution to contingency theory through theory extension and practical application (Corley & Gioia, 2011). It is a novel choice set containing information-contingent plans for making decisions based on the uncertainty of information (Austin & Devin, 2009). Although contribution to information security theory has improved over the past decade, prior to the proposed framework, contingency theory has not yet been applied to digital forensics in a manner that produces a definitive body of work that can be useful in a variety of cloud computing settings (Hurley, 2012).

Colquitt and Zapata-Phelan (2007) established that both building and testing of theory increase as concepts in literature mature. Although the information security field lacks academic theory that deals solely with managing information security, theory that does exist, mainly takes an inductive approach (Knapp, Ford, Marshall, & Rainer, 2007). Areas such as intrusion detection and digital forensics requiring theories that are more sophisticated combine both deductive and inductive research methods when contributing to theory.

Theoretically, comprehending if a prevalent theory exists allows the focusing of research

efforts and clearly indicates if a general approach to research would apply. Theory in information security spans many areas, including areas of protecting resources, detecting attacks, and forensic analysis. Ransbotham and Mitra (2009) explored a two-phase grounded approach to develop a conceptual process model for reacting to an information security compromise. The approach, using observations, interviews, and secondary data, is from the viewpoint of the compromised organization. Managing information security is critical; still there are few formal models available to provide guidance for organizations (Information Systems Audit and Control Association [ISACA], 2009).

Bayesian theory and Dempster-Shafer theory are among the few theories that have any documented research on forensic application. Current methods of application using Bayesian theory and Dempster-Shafer theory have limitations where cloud computing is concerned (Zhou & Mao, 2012). Bayesian and Dempster-Shafer approaches use the mathematics of probability theory and numerical measures of uncertainty (Chou, 2011). These theories are applicable in intrusion detection systems, data mining techniques, and data privacy, but cloud computing environments have too many variables to postulate correct hypotheses for successful mathematical calculation (Chou, 2011). Additionally, the objective of the research was to provide a framework for human use. Bayesian and Dempster-Shafer theories are machine-based applicable theories that are not conducive to human application (Zhou & Mao, 2012).

Although there is proven application of Dempster Shafer to forensic image analysis, this is a limited use application. Little is known about the application of current forensic evidence acquisition methods to cloud computing environments (Lallie & Pimlot, 2012). Prior to the current study, researchers have not sought to use contingency theory in theoretical studies used for forensic evidence acquisitions in cloud computing environments. There remains a need to explore when to use traditional forensic acquisition methods, when to use modified processes, and when the development of new methods is required for the examination of cloud computing environments (Desai, Solanki, Gadhwal, Shah, &, Patel, 2015; Pătraşcu, & Patriciu, 2014; Ruan, Baggili, Carthy, & Kechadi, 2011).

Other relevant research does not focus strictly on acquisition methods. *An Integrated Conceptual Digital Forensic Framework for Cloud Computing* by Martini and Choo emphasizes the differences in the preservation of forensic data and the collection of cloud computing data for forensic purposes. *Evidence and Cloud Computing: The Virtual Machine Introspection Approach* by Poisel, Malzer, and Tjoa describes digital forensics investigations at the hypervisor level of virtualized environments. Finally, *TrustCloud: A Framework for Accountability and Trust in Cloud Computing* by Ko, Jagadpramana, Mowbray, I. Pearson, Kirchberg, Liang, and Lee discusses challenges in achieving a trusted cloud through the use of detective controls.

3. METHODOLOGY

With the increasing crime in cloud computing environments (Berman, Kesterson-Townes, Marshall, & Srivathsa, 2012) and a lack of processes to acquire forensic evidence (Almulla, et al., 2014), the specific problem investigated was when traditional forensics evidence acquisition processes apply to cloud computing environments, when process modification is

acceptable, and when the development of new processes required.

In this study, a qualitative research methodology based on the Delphi technique was used to collect data from a sample of digital forensic subject matter experts. A modified Delphi methodology was selected due to an interest in discovering qualitative measures and a better comprehension about the application of current forensic evidence acquisition processes to cloud computing environments through querying the knowledge of digital forensics experts. The goal of the study was to use the iterative cycle of questioning and feedback to determine when traditional forensic evidence acquisition processes apply to cloud computing environments, identify when process modification is acceptable, and when the development of new processes are required. The methodology required the execution of a constant iterative process of discovery and analysis. The final goal was to extract a consensus interpretation that provided more information and sophistication for developing a contingency framework. The first part of the inquiry took on a criterion-referenced interpretive framework. The second part of the inquiry focused on processes, inquiring when to use traditional processes, when to use modified processes, and when there is a requirement for the development of new processes through the evaluation of current forensic evidence acquisition procedures. This part of the inquiry was similar to Eisner's connoisseurship model of inquiry (Willis, 2007).

3.1 Research Design

Based upon the recommendation of Hsu and Sandford, (2007) that an ideal Delphi panel consist of 10-18 members, 14 panel members and a five-member substitute pool were selected based on the extent of their knowledge and experience. Raw data were gathered from the study questionnaires completed by the 14 expert panelists from 10 preselected open-ended questions in the first online written narrative interview round. The second online written narrative interview round used the results of the first online written narrative interview round and the first 10 questions from the evidence acquisition processes identified in Appendix A, to begin gaining consensus from the panelists. The last online written narrative interview round, containing the results of the second online written narrative interview round and the remaining 10 questions from the evidence acquisition processes identified in Appendix A, provided further consensus and was analyzed to produce a robust contingency framework. The initial online written narrative interview questionnaire consisted of questions garnered from the cloud study by Ruan et al. (2011), listed in Appendix B. Using open-ended interview questions allowed the participants flexibility in relating their experiences (Snyder, 2012). The panelists responded to the open-ended questions by providing preliminary, critical perceptions on cloud computing. The first online written narrative interview round consisted of questions on cloud computing and the effect of cloud computing environments on forensics evidence acquisitions. In the initial round, the questions were limited in number to ten and required narrative answers. The SMEs provided anonymous responses to the questionnaire items and participated in a series of three evaluative rounds until reaching consensus on the specific subject item or until saturation occurred (Hsu & Sandford, 2007).

The second and third online written narrative interview rounds asked the expert panel to evaluate the responses from the previous questionnaire round and the forensic evidence acquisition processes in Appendix A. The panel experts were expected to be familiar with the 20 identified processes listed in

Appendix A. As an added measure to be sure the process definitions were clearly understood, the researcher provided an email containing contact information with each questionnaire notification for questions or clarification requests on any of the processes.

In Rounds 2 and 3, the online written narrative interview questionnaire consisted of processes from key forensic acquisition areas identified by Carlton (2007) listed in Appendices C and D in order to gain consensus on the application of traditional forensic evidence acquisition processes to cloud computing environments. The process responses were then refined in an iterative process based on panelist feedback at the conclusion of each Delphi round (Bourgeois, Pugmire, Stevenson, Swanson, & Swanson, 2011). Figure 1 shows the flow of the research design.

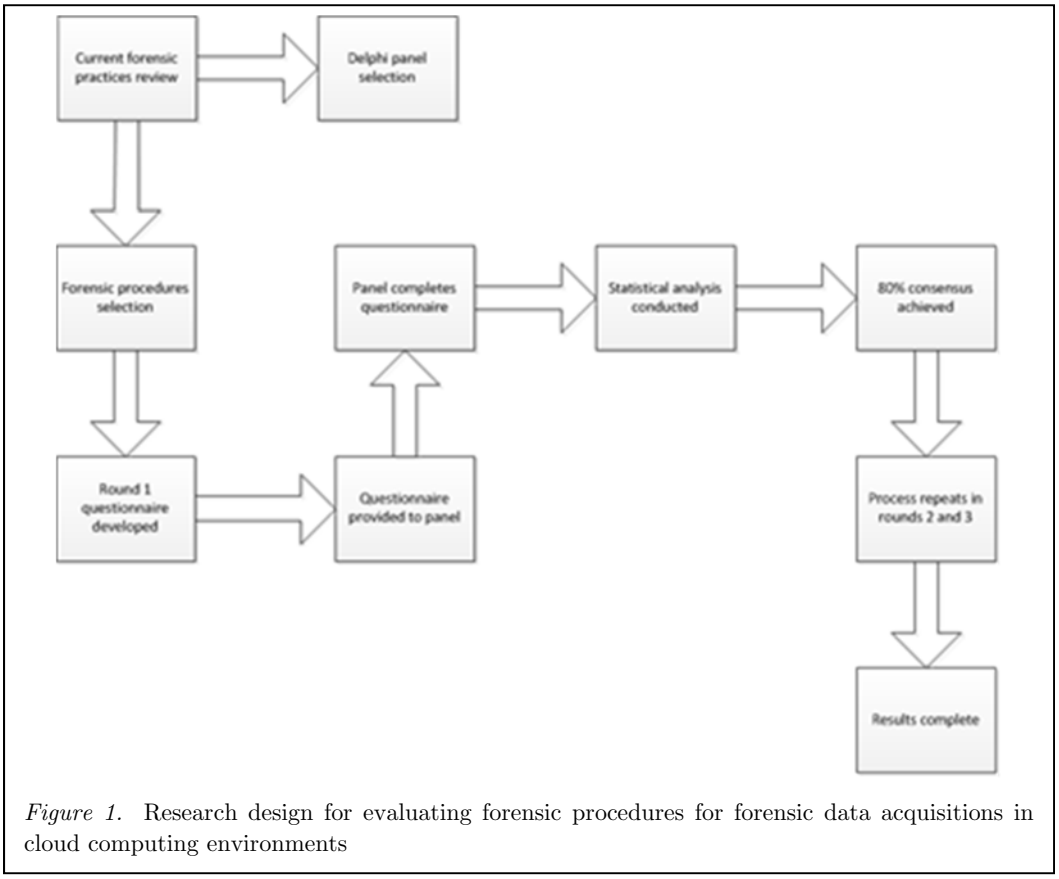

Figure 1. Research design for evaluating forensic procedures for forensic data acquisitions in cloud computing environments

After each online written narrative interview round, the questionnaires assisted in data acquisition from each panelist to reach consensus. The information gathered from the first round was organized and coded by theming the data, while the relevant processes from rounds 2 and 3 was organized into themes first and then pattern coded for qualitative analysis.

3.2 Sampling

The sampling structure characterized a purposive sample of the population. A purposive sampling is an acceptable type of sampling where specialized knowledge of the research issue is required (Neuman, 2003). Hallowell and Gambatese (2009) recommend that panelists meet at least four of the following requirements to qualify as an expert:

(a) published work in peer review journal; (b) industry presentations; (c) nationally recognized committee chair or member; (d) accredited institution of higher learning faculty member; (d) author or editor of a book or book chapter on the topic; (e) advanced degree in the field; (f) professional registration; and (e) minimum 5 years of industry experience. Using a 14-member panel and five-member substitute pool allowed for a 36% attrition rate without affecting the study results.

Study panel candidate selection was based on the criteria from the statement of qualifications based on five categories: (a) published work; (b) industry presentations; (c) organizational recognition; (d) industry recognition; and (e) years of industry experience. The solicitation responses were divided into four groups. Group 1 consisted of the candidates that only had experience documented. Group 2 consisted of the candidates that had experience documented and had one of the following: published work, industry presentations, or recognition. Group 3 consisted of the candidates that had experience documented and had published work or industry presentations, and either industry or organizational recognition. Group 4 consisted of the remaining candidates, which was those candidates that met a minimum of four qualifications. Since the pool of candidates from group 4 was not sufficient, the candidates from group 3 were added. No other candidates were in the panel member pool. In an effort to reduce any bias in expert panel selection, an independent review board reviewed the selected sampling. The expert panel contained members were from several countries.

3.3 Interview Rounds

The questions for the initial online written narrative interview questionnaire for the study were adaptations from the questions used in the study by Ruan et al. (2011). The focus of the study by Ruan et al. (2011) was to understand how digital forensic practitioners view cloud forensic concepts such the definition. Upon receipt of the responses, the researcher summarized the results and sent the response summary to the panel members with the next round questionnaire. When the panel members received the second online written narrative interview questionnaire, the panel members were permitted to modify their responses based on the provided results.

In Round 2, an online written narrative interview questionnaire consisting of 10 of forensic tasks identified in Appendix A that were extracted from 103 forensic data acquisition tasks of Carlton's (2007) survey listed in Appendix C was distributed to begin consensus building on the application of digital evidence acquisition processes. This written narrative interview questionnaire provided the results of the initial questionnaire to the participants and began the forensic evidence acquisition process area data-gathering portion of the study (Green, Armstrong, & Graefe, 2007). When the panel members received the third online written narrative interview questionnaire, the panel members were permitted to modify their responses to the second online written narrative interview questionnaire based on the provided results.

In Round 3, another online written narrative interview questionnaire consisting of results of the second questionnaire and 10 of the forensic tasks identified in Appendix A that were extracted from 103 forensic data acquisition tasks of Carlton's (2007) survey listed in Appendix D was distributed to conclude consensus building on the application of digital evidence acquisition processes.

Upon compilation of the third online written narrative interview questionnaire, the panel members were sent a one-page online questionnaire summary containing the results of each question from the third round and

permitted the panel members to modify their responses.

Consensus was based on 50% agreement of the panel members for each question. At the end of the second round, there was consensus on 70% of the round one questions, consensus on 90% of the round two questions, and consensus on 50% of the round three questions. The expert panel members were given one more chance to change responses or add additional information to any questionnaire item with the final submission.

At the end of the third round, the consensus percentages had not changed. There was consensus on 70% of the round one questions, consensus on 50% of the round two questions, and consensus on 60% of the round three questions.

4. FINDINGS

The study had two components. The first component consisted having the expert panel members respond to the questionnaires listed in Appendix B, Appendix C, and Appendix D. The second component consisted of having the members of the expert panel review and comment on the complied questionnaire responses using a Delphi methodology comprised of three rounds. This approach led to three findings regarding perceptions of cloud computing environments and the application of digital forensic evidence acquisition methods to cloud computing environments.

The first finding was that there were very diverse opinions on cloud computing, cloud forensics, and the effect cloud computing environments had on digital forensics. This area had the most changes in Delphi round responses. The high number of changes signified the various perceptions of cloud computing and cloud forensics definitions. Opinions about what constituted cloud computing diverge substantially (Zhang, Yan, & Chen, 2012). Fifty-seven percent of the panel members identified remote access as a theme; while many of the remaining members argued that cloud computing does not always involve remote access as in a hybrid cloud. The expert panel members did not agree that the NIST definition of cloud computing was the most relevant because it was cumbersome. There was not agreement on what the definition of cloud forensics encompasses. The panel members identified three main characteristics of defining cloud forensics. Verification of data integrity, working with service providers to obtain required information and legal admissibility, and international cooperation were the three main characteristics.

The second finding was that the knowledge and skill requirements for conducting acquisitions in a cloud computing environment differed from a non-cloud computing environment but there was very little guidance available for digital forensic professionals on conducting acquisitions in a cloud computing environment. Seventy-nine percent of the panel members felt the knowledge and skill requirements were different for cloud computing acquisitions and non-cloud computing forensic acquisitions. Predefining skill requirements was impossible due to the dynamically changing environment (Goodall, Lutters, & Komlodi, 2009). As an industry, digital forensics was lacking the tools, published processes, and guidance for proper acquisition of digital evidence in cloud computing environments. Twenty-nine percent of the panel members felt that there were no published processes or guidance available for forensic acquisition of evidence in cloud computing environments while the remaining panel members could identify only one resource that might be useful for published processes or guidance. Forensics tools and techniques lacked capacity to meet the progressive change

in the way data access happens in a cloud computing environment (Zhou, Cao, & Mai, 2012). Swift advances in cloud computing implementations warranted new methodologies for performing digital forensics in cloud environments (NIST, 2014). This is more than an incremental change. According to NIST (2014) cloud computing is projected to drastically alter first responder and examiner processes.

The third finding was that about half of the selected digital acquisition processes applied to cloud computing environments; the rest required modification or new process development. Approximately 55% of the 20 pre-selected traditional forensic processes were usable for the forensic acquisition of digital evidence in cloud computing environments with some limitations. Post-acquisition processes were most suited for application in cloud computing environments. Following post-acquisition processes in order of applicability were live acquisition processes. The main limitation in this area was access to the cloud server in order to perform the processes. The results analysis suggested this category of processes had solutions for digital evidence acquisitions in cloud computing environments because the processes were modeled after already established network forensic processes.

Thirty-five percent of the 20 pre-selected traditional forensic processes were modifiable for the forensic acquisition of digital evidence in cloud computing environments depending on the level of access and service provider cooperation. Pre-acquisition processes were most suited for modification in cloud computing environments. Following pre-acquisition processes in order of applicability were live acquisition processes. In the area of live acquisition processes 43% of the panel members expressed that acquisition processes required modification due to legal and technical issues.

Ten percent of the 20 pre-selected traditional forensic processes required the development of new processes for the forensic acquisition of digital evidence in cloud computing environments. The most notable observation of the study results in this area was that visions of what the new processes looked like were severely lacking. The panel experts agreed that current acquisition processes in the category of dead acquisitions did not fit into cloud computing environments and many of the processes should no longer be included because they were not applicable or modifiable. The panel members suggested that pursuing the development of new processes was moot because the processes were irrelevant.

An unexpected finding was that even a panel of experts experienced difficulty agreeing on some processes when discussing the application of digital forensic evidence acquisition methods to cloud computing environments. Overall, consensus was not reached on 30% of the processes. Panel consensus was not reached on 75% of the imaging processes and 33% of dead acquisition processes. The disagreement on imaging processes was split evenly with 36% replying that the processes were applicable, 28% replying that the processes were modifiable, and 36% replying that new processes were required.

5. RECOMMENDATIONS

The problem addressed by this study was the need for a more clear analysis of the application of digital forensic evidence acquisition methods to cloud computing environments because without comprehending the effect of cloud computing on digital evidence acquisitions, digital evidence collections and criminal prosecution are

hampered (Farina, Scanlon, Le-Khac, & Kechadi, 2015).

The findings demonstrated there were very diverse opinions on cloud computing, cloud forensics, and the effect cloud computing environments had on digital forensics. Standard evidence acquisition procedures, federal and local laws, court accepted methods, and the cooperation of the cloud provider were all factors that affected the way a successful forensic acquisition was conducted in a cloud computing environment. The areas of tools, processes, and guidance available for forensic evidence acquisitions in cloud computing were relatively immature.

Table 1 contains the contingency framework for deciding when traditional forensic acquisition processes are applicable, when modified processes are acceptable, and when the development of new methods is required. The processes are broken into categories of specific digital forensic acquisition task areas: pre-acquisition processes, live acquisition processes, dead acquisition processes, imaging processes, and post-acquisition processes. The Recommended Application is based on whether the category of Acquisition Process is applicable, modified, or if new methods are required. The Contingency Variable(s) were themed, and patterns identified in the results analysis.

Table 1
Contingency Framework

Application Process	**Recommended Application**	**Contingency Variable(s)**
Pre-acquisition processes	Modification	Fluidity of environment
Live acquisition processes	Application with limitations	Access, tools, scope
Dead acquisition processes	Partial application, modification or develop new	Cloud implementation, access
Imaging processes	Application, modification or develop new	Cloud implementation, access, scope
Post-acquisition processes	Application with limitations	Fluidity of environment, access

The digital forensic acquisition cloud contingency framework model combines the key contributions from the process design contingency model proposed by Austin and Devin (2009) and the information security management contingency model demonstrated by Tassabehji (2005). Austin and Devin's (2009) model contained elements of flexibility in software development processes that are paralleled in the digital forensic acquisition cloud contingency model. The model depicted by Tassabehji (2005) presented dynamic security levels contingent upon external variables that are integrated into the digital

forensic acquisition cloud contingency model. The new model advances existing theoretical understanding of the subject, connects the study implications to practice, and informs debate about the feasibility of flexible digital acquisition practices.

The categories for forensic evidence acquisition activity are summarized as pre-acquisition, acquisition, imaging, and post-acquisition processes. The model depicts the processes first because processes are the only constant. Once the digital forensic examiner chooses the process to be performed, the cloud computing environment uncertainty is introduced which produces the contingency. Based on the contingency, the appropriate application methodology is executed. Figure 2 represents a diagrammatical illustration of the digital evidence forensic acquisition cloud contingency model.

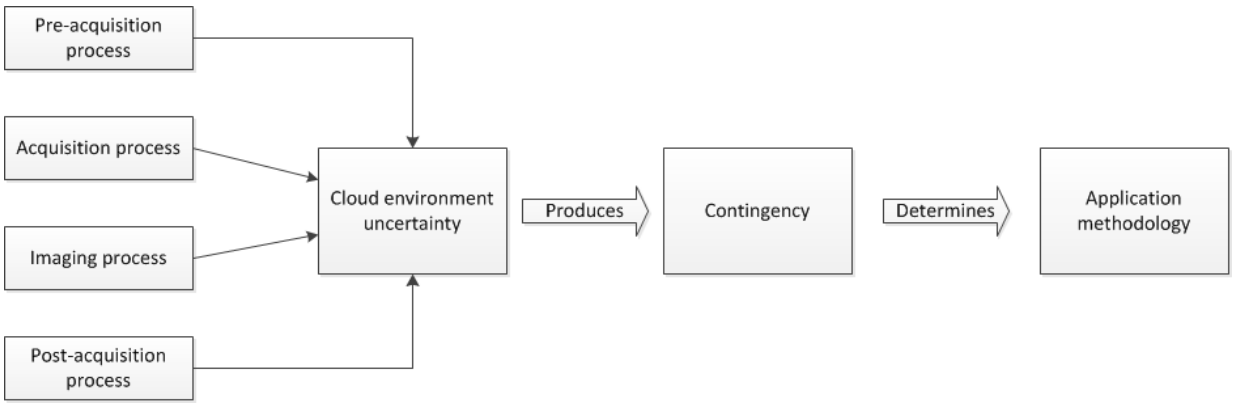

Figure 2. A diagrammatical illustration of digital evidence forensic acquisition cloud contingency model

As an example of how the model can be applied, the pre-acquisition process of performing procedures identified in a forensic acquisition checklist is used in Figure 3. The purpose of this example is to illustrate the application of the theory behind the model as an approach to guiding the relevance of the model to real-life situations. The process is the starting point because it is the constant. Three primary types of cloud environments of private, public and hybrid are used to introduce uncertainty. Based on the themes extracted from the study results, contingencies for determining if performing procedures identified in a forensic acquisition checklist include fluidity of environment, legal accessibility, and identification of the acquisition target. The contingencies then determine whether the process can be applied, requires modification, or if a new process is required to be developed.

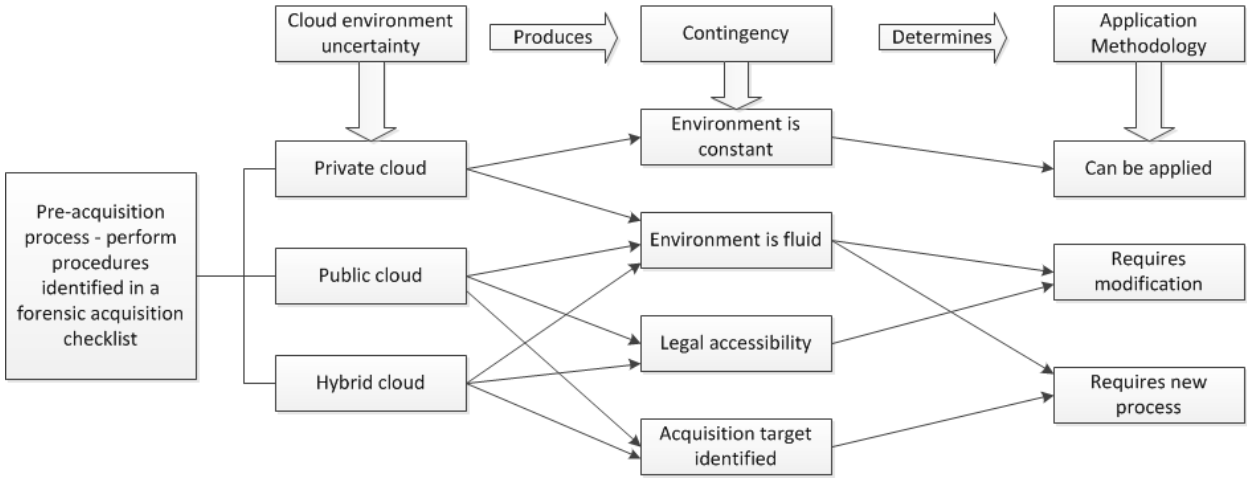

Figure 1. Application of the digital evidence forensic acquisition cloud contingency model to pre-acquisition process

The root of contingency theory is that best practices depend on the contingencies of the situation (Jacobson, 2009). The premise of the digital forensic acquisition cloud contingency model is that in order to be effective, the process application methodology must be flexible and adapt to the contingencies produced by the cloud computing environmental situation. The resulting contingency model is well suited to a wide range of cloud computing environmental applications. The contingency framework in Figure 3 used the study results as the foundation to create a digital forensic acquisition cloud contingency model, concentrating on how uncertainty and contingencies affect particular processes and guide a course of research that can support and enrich the model. When the world changes in a way that requires different functionality in a process or practice currently used, flexibility allows adjustment of the process or practice to reflect the changed world (Austin & Devin, 2009).

6. CONCLUSION

The purpose of this qualitative study was to develop a robust contingency framework for deciding when to use traditional forensic acquisition practices, when to use modified processes, and when it is necessary to develop new forensic acquisition processes through the evaluation of 20 conventionally recognized forensic acquisition processes by a panel of SMEs. Findings indicated that there were very diverse opinions on cloud computing, cloud forensics, and the effect cloud computing environments had on digital forensics. The knowledge and skill requirements for conducting acquisitions in a cloud computing environment differed from a non-cloud computing environment but there was very little guidance available for digital forensic professionals on conducting acquisitions in a cloud computing environment. About 50% of the current digital acquisition processes applied to cloud computing environments; the rest required modification or new process development. The final finding was that even a panel of experts experienced difficulty agreeing on some processes when discussing the application of digital forensic evidence acquisition methods to cloud computing environments.

The presented contingency framework used the study results as the foundation to create a digital forensic acquisition cloud contingency model, concentrating on how uncertainty of cloud computing environments and contingencies affect particular processes. The

digital forensic acquisition cloud contingency model was applied to one of the processes in the study as an approach to guiding the relevance of the model to real-life situations. The contingencies are easily ported to other evidence acquisition methods for expanding research in this area.

The findings produced potential implications for several areas of digital forensics including policymakers and those that provide guidance, digital forensic practitioners, and digital forensic educators, especially in areas related to cloud computing environments evidence acquisitions.

Recommendations for policymakers, practitioners, and educators included proper guidance pointed in solid direction, implementation of the proposed contingency framework, professional organizations taking the lead in setting forensic policy for directing practice, and improved training and education.

Recommendations for future research included expanded contingency theory application, targeting specific types of cloud computing, using a larger sample population, and expanding the number of acquisition processes examined.

REFERENCES

Almulla, S. A., Iraqi, Y., and A. Jones (2014). A state-of-the-art review of cloud forensics. *Journal of Digital Forensics, Security and Law, 9*(4), 7–28. Retrieved from http://www.jdfsl.org/

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*, 50-58. doi:10.1145/1721654.1721672

Austin, R. D., & Devin, L. (2009). Weighing the benefits and costs of flexibility in making software: Toward a contingency theory of the determinants of development process design. *Information Systems Research, 20*(3), 462-479. doi: 10.1287/isre.1090.0242

Baird, A., Furukawa, M. F., & Raghu, T. S. (2012). Understanding contingencies associated with the early adoption of customer-facing web portals. *Journal of Management Information Systems*, *29*(2), 293-324. doi:10.2753/MIS0742-1222290210

Battilana, J., & Casciaro, T. (2012). Change agents, networks, and institutions: a contingency theory of organizational

Colquitt, J. A., & Zapata-Phelan, C. P. (2007). Trends in theory building and theory testing: A five-decade study of the Academy of Management Journal. Academy of Management Journal, 50(6), 1281-1303. doi:10.5465/AMJ.2007.28165855

Corley, K. G., & Gioia, D. A. (2011). Building theory about theory building: What constitutes a theoretical contribution? *Academy of Management Review, 36*, 12-32. doi:10.5465/AMR.2011.55662499

Corrin, A. (2106, April). New Army program shifting cyber operation. *Federal Times*. Retrieved from change. *Academy of Management Journal*, *55*(2), 381-398. doi:10.5465/amj.2009.0891

Berman, S. J., Kesterson-Townes, L., Marshall, A., & Srivathsa, R. (2012). How cloud computing enables process and business model innovation. *Strategy & Leadership, 40*(4), 27-35. doi:10.1108/10878571211242920

Bourgeois, J., Pugmire, L., Stevenson, K., Swanson, N., & Swanson, B. (2011). *The Delphi method: A qualitative means to a better future (Citirano 2.11.2011).* Retrieved from http://www.freequality.org/html/knowledge.html

Carlton, G. H. (2007). A grounded theory approach to identifying and measuring forensic data acquisition tasks. *Journal of Digital Forensics, Security and Law*, *2*(1), 35-56. Retrieved from http://www.jdfsl.org/

Chou, T. S. (2011). Cyber security threats detection using ensemble architecture. *International Journal of Security and Its Applications*, 5(2), 11-15. Retrieved from http://www.sersc.org/journals/IJSIA/

http://www.federaltimes.com/story/government/cybersecurity/2016/04/04/army-cyber-operations/82621910/

Dae Ham, C., Hong, H., & Cameron, G.T. (2012). Same crisis, different responses: Case studies of how multiple competing corporations responded to the same explosion-related crises. *International Journal of Business and Social Science, 3*(20), 19-31. Retrieved from http://www.ijbssnet.com/update/

Daryabar, F., Dehghantanha, A., & Udzir, N. I. (2013). A review on impacts of cloud computing on digital forensics.

International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2(2), 77-94.

Desai, P., Solanki, M., Gadhwal, A., Shah, A., Patel, B. (2015, January) Challenges and Proposed Solutions for Cloud Forensic. *International Journal of engineering Research and Applications, 1*(5), 37-42.

Farina, J., Scanlon, M., Le-Khac, N., & Kechadi, T. (2105, August). Overview of the Forensic Investigation of Cloud Services. International Workshop on Cloud Security and Forensics (WCSF 2015).

Fiaidhi, J., Bojanova, I., Zhang, J., & Zhang, L. (2012). Enforcing multitenancy for cloud computing environments. *IT Professional Magazine, 14*(1), 16-18. doi:10.1109/MITP.2012.6 – d

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation,7, Supplement,* S64-S73. doi:10.1016/j.diin.2010.05.009

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People, 22*(2), 92-108. doi:10.1108/09593840910962186

Green, K. C., Armstrong, J. S. & Graefe, A. (2007). Methods to elicit forecasts from groups: delphi and prediction markets compared. *Foresight: The International Journal of Applied Forecasting. (8),*17-20. Retrieved from http://forecasters.org/foresight/

Hallowell, M. R., & Gambatese, J. A. (2010). Qualitative research: Application of the Delphi method to CEM research. *Journal of Construction Engineering & Management*, *136*(1), 99-107. doi:10.1061/(ASCE)CO.1943-7862.0000137

Hsu, C., & Sandford, B. A. (2007). The Delphi technique: Making sense of consensus. *Practical Assessment, Research & Evaluation*, *12*(10), 1-8. Retrieved from: http://pareonline.net/

Hurley, M. M. (2012). For and from cyberspace: Conceptualizing cyber intelligence, surveillance, and reconnaissance. *Air & Space Power Journal*, *26*(6), 12-33. Retrieved from http://www.airpower.au.af.mil/

Information Systems Audit and Control Association (2009). *An introduction to the business model for information security.* Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/An-Introduction-to-the-Business-Model-for-Information-Security.aspx

Jacobson, D. D. (2009, January). Revisiting IT Governance in the Light of Institutional Theory. In *42nd Hawaii International Conference on System Sciences, 2009.* 1-9. Retrieved from http://www.hicss.hawaii.edu/

Kalchschmidt, M. (2011). Best practices in demand forecasting: tests of universalistic, contingency and configurational theories. *International Journal of Production Economics*, *140*(2), 782-793. doi:10.1016/j.ijpe.2012.02.022

Ke, W., Tan, C., Sia, C., & Wei, K. (2012). Inducing intrinsic motivation to explore the enterprise system: The supremacy of organizational levers. *Journal of Management Information Systems*, *29*(3), 257-290. doi:10.2753/MIS0742-1222290308

Kessler, G. (2011). Judges' awareness, understanding, and application of digital evidence. *Journal of Digital Forensics,*

Security and Law, 6(1), 55-72. Retrieved from http://www.jdfsl.org/

Knapp, K. J., Ford, F. N., Marshall, T. E., & Rainer, R. K. (2007). The common body of knowledge: A framework to promote relevant information security research. *Journal of Digital Forensics, Security and Law, 2*(1), 9-34. Retrieved from http://www.jdfsl.org/

Lallie, H., & Pimlott, L., (2012). Challenges in applying the ACPO principles to cloud forensic investigations. *Journal of Digital Forensics Security and Law*, *7*(1) 71-86. Retrieved from http://www.jdfsl.org/

Mathiassen, L., & Sorensen, C. (2008). Towards a theory of organizational information services. *Journal of Information Technology*, *23*(4), 313-329. doi:10.1057/jit.2008.10

National Institute of Standards and Technology (NIST), (2014). *Cloud Computing Forensic Science*. Retrieved from http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudForensics

Neuman, W. L. (2003). *Social research methods: Qualitative and quantitative approaches* (5th ed.). Upper Saddle River, NJ: Pearson Education.

Ngo, L., Zhou, W., & Warren, M. (2005, September). Understanding transition towards information security culture change. *Proceedings of the 3rd Australian Information Security Management Conference*, 67-73. Retrieved from http://ro.ecu.edu.au/ism/

Pătraşcu, A., & Patriciu, V. V. (2014). *Digital Forensics in Cloud Computing. Advances in Electrical and Computer Engineering*, 14(2).

Pieters, W. (2011). The (social) construction of information security. *Information Society*, *27*(5), 326-335. doi:10.1080/01972243.2011.607038

Qiu, J., Donaldson, L., & Luo, B. N. (2012). The benefits of persisting with paradigms in organizational research. *The Academy of Management Perspectives*, *26*(1), 93-104. doi:10.5465/amp.2011.0125

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139,156. doi:10.1287/isre.1080.0174

Ruan, K., Baggili, I., Carthy, J., & Kechadi, T. (2011, May). Survey on cloud forensics and critical criteria for cloud forensic capability. *Journal of Digital Forensics, Security and Law, Conference Proceedings*, 55-70. Retrieved from http://www.digitalforensics-conference.org/subscriptions/proceedings_2011.htm

Snyder, C. (2012). A case study of a case study: Analysis of a robust qualitative research methodology. *Qualitative Report*, *12* (9), 661-682. doi:10.1097/00000478-198809000-00002

Tassabehji, R. (2005). Principles for managing information security. *Encyclopedia of Multimedia Technology and Networking*, (pp. 842-848). doi:10.4018/978-1-59140-561-0.ch119

Thomas, D. M., Gupta, S., & Bostrom, R. P. (2008, January). A meta-theory for understanding IS in socio-technical systems. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences, IEEE,* (pp. 451-451). doi:10.1109/HICSS.2008.28

Willis, J.W. (2007). *Foundations of qualitative research: Interpretive and critical approaches*. Thousand Oaks, CA: Sage.

Zhang, S., Yan, H., & Chen, X. (2012). Research on key technologies of cloud computing. *Physics Procedia*, *33*, 1791-1797. doi:10.1016/j.phpro.2012.05.286

Zhou, G., Cao, Q., & Mai, Y. (2012). Forensic analysis using migration in cloud computing environment. *Information and Management Engineering*, *236,* 417-423. doi:10.1007/978-3-642-24097-3_62

Zhou, X., & Mao, F. (2012, August). A semantics web service composition approach based on cloud computing. *Fourth International Conference on Computational and Information Sciences (ICCIS), 2012,* 807-810. doi:10.1109/ICCIS.2012.43

Zimmerman, S. & Glavach, D. (2011). Cyber forensics in the cloud. *IA Newsletter*, *14*(1), 4-7. Retrieved from http://iac.dtic.mil/iatac

Appendix A

Conventionally Recognized Forensic Practices Investigated

1. Perform procedures identified in a forensic acquisition checklist - Using a set checklist of documented processes in order to acquire forensics evidence.
2. Perform a RAM dump. Acquiring the RAM contents while the machine is running.
3. Collect volatile data. Acquiring data that dissipates when a computer is tuned off. This can include running processes and services.
4. Perform a live image acquisition of the computer. Acquiring an image of the computer's hard drive without turning off the computer.
5. Photograph the displayed image shown on the workstation's monitor. Using a camera to take a picture of what is currently showing in the computer screen.
6. Determine the programs currently running on the computer. Using a tool to examine what programs are running on a computer.
7. Power off the unit by using the operating system shutdown method. Turning off the computer by touching the computer itself and using the operating system to shutdown the computer.
8. Determine the current date and time from a reliable source. Using a universal time source such as atomic time or a time synchronization software.
9. Document the manufacturer, model, and serial number of all storage media attached to computer. Examining all media to identify unique markings that include the manufacturer, model, and serial number.
10. Remove the hard disk drive(s) from the system unit. Physically opening the computer to remove the hard drive for forensic imaging.
11. Document number of hard drives, size and disk geometry. Examining all hard drives removed from the computer to identify unique markings that include the capacity and disk geometry.
12. Use EnCase to obtain an image of suspect media. Using forensic software developed by Guidance Software to perform imaging of the suspect hard drive.
13. Use AccessData's FTK to obtain an image of suspect media. Using forensic software developed by Access Data to perform imaging of the suspect hard drive.
14. Identify any network connections and document findings. Categorizing all connections between the suspect computer system and networks using descriptive notations.
15. Use UNIX/Linux dd command to obtain an image of suspect media. Using a basic UNIX command included in the operating system to perform imaging of the suspect hard drive.
16. Generate a MD5/SH1 hash value of the forensic image. Performing an algorithmic calculation function to validate the image acquisition of a computer hard drive.
17. Preserve suspect media in its original condition and securely seal. Using a chain of custody procedure to secure the electronic evidence.
18. Place suspect media in a secure storage area or evidence vault. Using a chain of custody procedure to secure the electronic evidence against loss or tampering.
19. Create a clone copy of suspect media for mounting and analysis. Making a duplicate copy of the evidence hard drive for mounting to view the computer the way the suspect did.
20. Perform a visual comparison of the directory structure of the image and the suspect disk to verify that the image is readable. Loading both the forensic copy and the original evidence into forensic analysis software to verify that the directory structure is the same and that the forensic analysis image is a good working copy

Appendix B

Online Written Narrative

Interview Round One Questions

Please answer the following open ended questions based on your expert opinion:

1. What is cloud computing?
2. What is cloud forensics?
3. What impact does cloud computing have on digital forensic acquisitions?
4. What challenges does the area of cloud forensics currently face?
5. In what ways are cloud forensic acquisitions more or less complex when compared to similar non-cloud forensic acquisitions?
6. Who is responsible for the acquisition of cloud computing forensic evidence in civil and in criminal cases?
7. How are the knowledge and skill requirements different for cloud computing acquisitions from non-cloud computing forensic acquisitions?
8. What current tools are available with which to conduct forensic acquisitions in cloud computing environments?
9. What published processes are available that describe forensics acquisitions in cloud computing environments?
10. What current guidance is offered on the forensic acquisition of evidence in cloud computing environments?

Appendix C

Online Written Narrative

Interview Round Two Questions

Please answer the following open ended questions based on your expert opinion as to the applicability of the following tasks to cloud computing environments. Explain how the following traditional processes can be applied to cloud computing environments. If the process cannot be applied and the process can be modified or a new process has to be developed, please provide your opinion on what the modified or newly developed process would look like.

1. Perform procedures identified in a forensic acquisition checklist
2. Perform a RAM dump
3. Collect volatile data
4. Perform a live image acquisition of the computer
5. Photograph the displayed image shown on the computer's monitor
6. Determine the programs currently running on the computer
7. Power off the unit by using the operating system shutdown method
8. Determine the current date and time from a reliable source
9. Document the manufacturer, model, and serial number of all storage media attached to the computer

Remove the hard disk drive(s) from the system unit

Appendix D

Online Written Narrative

Interview Round Three Questions

Please answer the following open ended questions based on your expert opinion as to the applicability of the following tasks to cloud computing environments. Explain how the following traditional processes can be applied to cloud computing environments. If the process cannot be applied and the process can be modified or a new process has to be developed, please provide your opinion on what the modified or newly developed process would look like.

1. Document number of hard drives, size and disk geometry
2. Use EnCase to obtain an image of suspect media
3. Use AccessData's FTK to obtain an image of suspect media
4. Use UNIX/Linux dd command to obtain an image of suspect media.
5. Identify any network connections, and document findings
6. Generate a MD5/SHA1 hash value of the forensic image
7. Preserve suspect media in its original condition and securely seal
8. Place suspect media in a secure storage area or evidence vault
9. Create a clone copy of suspect media for mounting and analysis

Perform a visual comparison of the directory structure of the image and the suspect disk to verify that the image is readable

