Cloud Based Evidence Acquisitions in Digital Forensic Education

Diane Barrett
Bloomsburg University of Pennsylvania
dbarrett@bloomu.edu
Bloomsburg, PA

Abstract

In a cloud computing environment, traditional digital forensic processes (such as turning off the computer to image the computer hard drive) can be disruptive to businesses because the data of businesses may be co-mingled with other content. As technology changes, the way digital forensics acquisitions are conducted are also changing. The change in methodology affects the way this subject matter is taught in programs and institutions. Methods to teach digital forensic acquisition methods in a cloud computing environment are limited due to the complexity of the cloud environment. This paper explores how a panel of expert practitioners viewed evidence acquisitions within the cloud environment, the implications for digital forensic education, and suggestions on how the education field can prepare students for technological changes in digital forensic acquisition processes where cloud computing environments are concerned and also help develop new methodologies. The paper offers a classroom case scenario as an example on how new methodologies and tools can be used in the classroom.

Keywords: digital forensics, cloud forensics, digital forensic acquisition methods

1. INTRODUCTION

The definition of digital forensic processes has been in existence for many years. Digital forensic processes consist of crime scene evidence collection, evidence preservation, evidence analysis, and presentation of the analysis results (Zimmerman, 2012). Traditional digital acquisition processes include maintaining chain of custody control of forensic evidence data. This chain of custody control occurs in the evidence collection phase through the imaging of a system (Decker, Kruse, Long, & Kelley, 2011). Cloud computing technology disrupts this initial step in conducting a digital forensic investigation and presents a problem for digital forensic investigators because it is not possible to take down and create a forensic image of such a large environment (James, Shosha, & Gladyshev, 2013).

As business models have changed to incorporate a wide variety of cloud computing environments, the escalation of computer crimes from hacking and security breaches related to cloud computing environments has steadily increased. Methods to investigate crime in a cloud computing environment are limited due to the complexity of the cloud environment. Cloud related criminal activity is likely to present security and forensic challenges for an extended period, spanning well into the future (Robinson, 2012). As institutions evaluate their curriculum in preparing students for entering the workforce, digital forensic teaching methodologies must encompass the acquisition of cloud computing related data.

2. BACKGROUND

The science behind digital forensics requires repeatable processes producing consistent results (Decker et al., 2011). Traditional forensic evidence acquisition processes do not fit well into cloud computing because of the way

cloud computing works (Desai, Solanki, Gadhwal, Shah, & Patel, 2015).

Traditional forensics focuses on acquiring a complete image of the environment. Current digital acquisition processes include controlling forensic evidence data to maintain an unaltered state through the imaging of a system. With cloud computing environments, such an acquisition is not feasible.

Traditional digital forensic acquisition processes focus on individual computers and isolated environments, while cloud computing forensic acquisition processes include the intricacies of complex infrastructures including virtual servers, applications, and diverse operating platforms that may be located in foreign countries (James et al., 2013).

Cloud computing systems consist of multiple user environments, using a variety of services. Shutting down a cloud computing system disrupts services to all the user environments hosted on the system (Pătraşcu, & Patriciu, 2014). The common forensic procedure of shutting down the system in order to take a forensic image of the system cannot apply to hosted cloud services due to disruption of service to a wide scope of users.
Cloud computing systems using distributed file systems have large volume storage areas distributed physically across many geographic locations. The application of current forensic methods cannot be used because it is impossible to image and reconstruct separate replications of each disk node (Farina, Scanlon, Le-Khac, & Kechadi, 2015). The time, storage, and labor required to forensically collect and reassemble this environment is extremely extensive and quite unmanageable.

Many of the key aspects of proper evidence acquisition and handling such as evidence control, acquisition skills, and forensics tools need further development to meet the requirements to properly acquire digital evidence in cloud computing environments (Lallie & Pimlott, 2012). Prior research from a 14-member expert panel survey shows that eleven (79%) of the panel members felt the knowledge and skill requirements for cloud environments were different for cloud computing forensics acquisitions and non-cloud computing forensic acquisitions.

Predefining skill requirements where cloud computing environments are concerned is impossible due to the dynamically changing environment (Goodall, Lutters, & Komlodi (2009). The nature of such expertise makes transferring those skills to other examiners problematic (Goodall et al., 2009). New analysts cannot properly validate the information in the reports without extensive knowledge. Network security tool creators and vendors must recognize the vital role human expertise plays in report validation.

3. PRACTIONER VIEWS

In order to garner opinions on cloud forensics and the application of traditional forensic acquisition methods to cloud forensic environments, an expert panel survey was conducted. 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. Expert panel member selection was based on the criteria from a submitted statement of qualifications. Only digital forensic investigators with at least five years of relevant field experience, published work, industry presentations, and recognition were eligible to participate in this study. The expert panel consisted of 14 members from several countries.
Fourteen panel members were selected because an ideal Delphi panel consists of 10-18 members. The 14 panel members were selected based on the extent of their knowledge and experience.

An online written narrative interview questionnaire for the study began with 10 open-ended written questions on cloud computing based on the cloud study by Ruan Baggili, Carthy, & Kechadi (2011) as defined in Appendix A. Panel members were then asked to evaluate 20 common forensic procedures for applicability to cloud computing environments. The common forensic procedures selected are listed in Appendix B.

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.

A recap of the responses to the evaluation of the 20 common forensic procedures for applicability to cloud computing environments indicated several key points. Only eleven (55%) of the 20 pre-selected traditional forensic processes were usable for the forensic acquisition of digital evidence in cloud computing environments and the usability of those processes had some limitations. Post-acquisition processes were most suited for application in cloud computing environments. Seven (35%) 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. One (5%) 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. Table 1 depicts these findings. The panel members suggested that pursuing the development of new processes in some cases was moot because the processes were irrelevant to cloud computing environments.

4. IMPLICATIONS FOR DIGITAL FORENSIC EDUCATION

According to NIST (2014), cloud computing is projected to drastically alter first responder and examiner processes. Practitioners agree that the knowledge and skill requirements for cloud are different for cloud computing acquisitions and non-cloud computing forensic acquisitions. In order to prepare digital forensic professionals for this change in processes, practitioner education will be needed (Holt & Bossler, 2011). This will require additional funding for new program development that will accommodate the projected alteration of first responder and examiner processes. Education on acquisition procedures will be in need the most.

Cloud forensics is a relatively new area of digital forensic practices with few industry professionals capable of providing required training (Ruan et al., 2011). The organizations and universities that build and deliver curriculum in digital forensic areas that involve cloud computing acquisitions need to participate in the advancement of the digital forensics field. Academia and the digital forensic training community will need to create and encourage the development of new training programs so that practitioners may better respond to situations where the acquisition of cloud computing environments are required. The expert panel study results provide compelling reasons for individuals currently involved in cloud forensics research to provide direction and advice for those implementing training programs, courses, or curriculum including education for law enforcement and industry professionals for the advancement of the profession in the ability to pursue cybercriminals.

Academia and the digital forensic training community need to create and encourage the development of new training programs so that practitioners may better respond to situations where the acquisition of cloud computing environments are required. The development of training programs, courses, or curriculum is dependent on existing knowledge. The panel research produced a contingency framework connecting the study results to practice as shown in Figure 1, Appendix C. This represents an illustration of the 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 2. 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 and is illustrated in Figure 2 of Appendix C.

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 general framework presented is populated with specific digital forensic acquisition process categories, a recommendation as to the applicability, and the contingency variables upon

which the process application is dependent. This format makes it an ideal starting point for training or education in this area. The applicable forensics processes that ported over well to cloud computing environments occurred because similar processes are used in current live analysis and network forensics methods. This provides a basis for expanding network forensics to either include cloud forensics as part of this domain or develop new training and education based on the domain. The base of forensic knowledge is expanded by researching information and incorporating the ideas of others into training and education programs.

5. AVAILABLE TOOLS

Representatives of the Cloud Security Alliance and forensics practitioners agree that there is a need for additional research to create a framework of methodologies and establish processes that will hold up when challenged in a court of law (Zimmerman & Glavach, 2011). There is a need to develop a forensic architecture for cloud computing environments. Many of the key aspects of proper evidence acquisition, handling, and analysis such as evidence control, acquisition skills, and forensics tools need further development to meet the requirements to properly acquire digital evidence in cloud computing environments (Lallie & Pimlott, 2012).

Digital forensic investigators must broaden digital forensic practice tools and expertise to include cloud computing environments. The current mature tools, processes, and expertise for digital investigations focus on small, individual environments (Svetcov, 2011). There is still an emphasis on imaging all devices in the environment and a belief that if there are any changes to the media where the data is stored during the acquisition process, the data is not reliable where the courts are concerned (Cohen, 2011).

Cloud computing environments make it extremely impractical to conduct in-depth analysis on each bit of storage media (James et al., 2013). Forensic labs do not have the capacity required to process large quantities of media in a timely manner. Forensic tools become unstable when case files become too large and weeks or months of work is negated if the created case file consistently becomes unresponsive because the data capacity is too large for the tool to handle (Svetcov, 2011).

Cloud computing forensic evidence acquisitions pose challenges at a more rudimentary level, the acquisition itself. In a cloud environment, the examiner has few options to image the virtual machine remotely, and deploying a remote forensic agent requires administrative credentials. In some instances, there may be a willingness to conduct an internal acquisition by the provider (Dykstra & Sherman, 2011). However, in many cases the information is proprietary and confidential so the provider is reluctant to turn over any raw data.
Tools will gradually become outdated and computer forensic practitioners will no longer be able to rely on forensic analysis results, unless the forensic community formulates a vibrant strategy for developing methods that build upon each other. Garfinkel (2010) argued that the digital forensic investigative practice has been in a golden age and that golden age is rapidly ending and proposed a plan for realizing research and operational effectiveness by using forensic computation systematic approaches. Garfinkel (2012) further stated that writing digital forensic tools is difficult because of the diversity of data types that needs to be processed, the need for high performance, the skill set of most users, and the requirement that the software run without crashing.

Vital aspects of proper evidence acquisition necessitate additional development of forensics tools to meet the requirements for properly acquiring cloud computing environments (Zhou, Cao, & Mai, Y, 2012). 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. Four (29%) panel members felt there were no current tools available with which to conduct forensic acquisitions in cloud computing environments and five (36%) felt the current tools for non-cloud environments were sufficient to conduct forensic acquisitions in cloud computing environments. Four (29%) panel members identified a specific forensic tool, F-Response, as the only available tool capable of performing forensic acquisitions in cloud computing environments. One (7%) panel member indicated that current eDiscovery tools had the capability to accomplish forensic acquisition tasks in cloud computing environments.

The development of training programs, courses, or curriculum is dependent on existing knowledge. There are compelling reasons for individuals currently involved in cloud forensics

research to provide direction and advice for those implementing training programs, courses, or curriculum including education for law enforcement and industry professionals for the advancement of the profession in the ability to pursue cybercriminals.

6. EDUCATIONAL IMPLEMENTATION EXAMPLE USING A CASE SCENARIO

Cloud environments are difficult to access in a forensic manner because the environment is live and the evidence cannot be logged into directly as it violates preserving the state of data and alters the data state. This can be compared to looking through a hard drive to find evidence without first creating a forensic image of the drive. The first rule of evidence is to never work on original evidence. The scenario acquisition process combined with the VM tools produces the repeatable processes necessary for the preservation of evidence and validation required. Based on the expert panel research and the contingency model created, a class project was created.

The basis of the project was an e-Discovery factual case scenario. The case scenario is based on several work-related legal issues but is a good starting point because it encompasses many different types of cloud based evidence. The case involves an employee of a worldwide organization that became disgruntled when he was accidentally copied on an email about a promotion he was being denied. In turn, the disgruntled employee exfiltrated company data to take with him after accepting a position with a competitor. During this time, the employee began communication with an old high school girlfriend who had located him on Facebook and he confided pertinent information with her. The scenario was used to build a cloud computing scenario by creating cloud based artifacts.

The scenario includes many cloud components including cloud based email, cloud based personal storage, social media, and cloud based corporate storage. The evidence items encompass personal e-mail accounts, Facebook pages, corporate storage buckets on Amazon Web Services (AWS), and personal storage on DropBox, Box, and Google Drive. The project is broken into two parts: an initial fact finding and exploration part and an actual acquisition part. Breaking the project into two parts gives the students practice in using cloud environment acquisition tools and allows students to become familiar with the process of doing an acquisition in a cloud computing environment. Privacy and legal considerations are discussed in the scenario since some of the storage buckets are located in foreign countries.

The investigative environment consists of a virtual machine (VM) that contains several forensic tools such as Access Data's FTK imager, F-Response Universal, and Paraben's E3 DS. Paraben E3 and F-Response access the cloud environment through an authentication API. Basically the tools act as an intermediary between the forensic examiner and the cloud environment. This allows evidence to be mounted as read-only and prevents direct access by the examiner. Then standard validation processes such as hashing can be conducted. This is an acceptable process from a forensic standpoint. In the classroom, the process does not allow the student to touch the original evidence, reinforcing proper forensic procedures.

Once the environment is accessed, both F-Response Universal, and Paraben's E3 DS can compress, hash, and export the data. The evidence is preserved in a forensic manner using this process. Once the acquisition is complete, the evidence is analyzed in the same manner as any other evidence. This validates the expert panel findings that post-acquisition processes were most suited for application in cloud computing environments.

Cloud acquired evidence is analyzed in the same manner as any other acquisition. This process is supported by prior research from the 14-member expert panel survey. Post-acquisition processes were most suited for application in cloud computing environments. Following post-acquisition processes in order of applicability were live acquisition processes.

There are a few important points worth mentioning. Credentials are needed in order to access the environment. The authentication of the accounts requires logins and passwords. Authentication keys are required to access AWS storage. As long as all parties are cooperative this information will be available. If the parties are not cooperative, the process cannot be used. When parties are not cooperative, any investigation is impeded, whether it is a cloud-based or a traditional forensic based investigation. When two-factor authentication is used, the process will be difficult as currently tools are not set-up to access information when two-factor authentication is required. This difficulty is encountered whether it is a cloud-based or a traditional forensic based

investigation. Privacy and legal issues are a consideration, especially since the passage of General Data Protection Regulation (GDPR).

The case results indicate the learning methodology used was successful. Some students took the path of least resistance and logged into several of the accounts instead of thinking outside the box. This breach of forensic process resulted in lower scores for those students. Assessment results from the Fall 2019 section of the class show that overall scores improved between the initial assessment in Week 4 and the final assessment in Week 8. The average score in Week 4 was 60%, with a median grade of 72%. In week 8, the average score was 69%, with a median grade of 79%.

7. FUTURE RESEARCH AND WORK

The opportunity for researchers to make innovative contributions and substantial impact to the cloud computing industry has only just begun (Zhang, Cheng, & Boutaba, 2010). The findings from the expert panel study are a bridge to a very small body of literature. The results of the study produced a contingency framework and digital evidence forensic acquisition cloud contingency model to help guide a course of implementation that can test the model and be used in teaching methodologies.

Using contingency frameworks to address other research questions provides a different perspective on the application of digital forensic acquisition methods to cloud computing environments. Additional studies could firmly establish that the choices available for the application of digital forensic methods to cloud computing environments are ingrained in contingency frameworks. One of the significant contributions of the expert panel study is the identification of contingency factors such as available tools, access, availability, and acquisition scope as the underlying elements when choosing the application of digital forensic methods to cloud computing environments. These contingency factors are easily ported to other evidence acquisition methods for expanding teaching and research in this area.

The digital evidence forensic acquisition cloud contingency model suggests other important directions of research and teaching methodologies. Accepting a contingency perspective on how to choose digital process application in cloud computing environments can serve as a powerful theoretical lens both in interpreting the results of prior models and in shaping rigorous research models for future inquiry. Another direction for future research and teaching would be to examine the influence of multiple contingencies on the process application within individual cloud types.

The expert panel study was conducted using a 14 member expert panel, which is a very small subset of all practitioners and researchers in the digital forensics field. A similar study can be performed using a larger sample. Carlton (2007) identified 103 forensic acquisition tasks. The task identification encompassed three phases of a digital forensic acquisition based on tasks performed during investigation preparation, the actual event, and concluding tasks. This same study can be conducted on an expanded set of processes to include more than the 20 identified processes used in the study. Future study options would be to include all 103 identified processes, restrict the study to one of the phases outlined by Carlton (2007), or re-evaluate the processes identified by Carlton to identify which of the 103 processes are still relevant.

8. CONCLUSION

Educating students in a constantly changing technological environment presents challenges to the academic field. The purpose of this paper was to explore how a panel of expert practitioners viewed evidence acquisitions within the cloud environment, the implications for digital forensic education, and suggestions on how the education field can prepare students for technological changes in digital forensic acquisition processes where cloud computing environments are concerned. A case scenario project was included to show how new processes can be incorporated into the classroom.

The work contained within is based on a qualitative Delphi study used to develop a robust contingency framework through the evaluation of 20 conventionally recognized forensic acquisition processes by a panel of subject matter experts (SMEs). 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. As an industry, digital forensics is lacking the tools, published processes, and guidance for proper acquisition of

digital evidence in cloud computing environments. Pre-acquisition processes are most suited for modification in cloud computing environments while post-acquisition processes are most suited for application in cloud computing environments. The digital acquisition processes that applied to cloud computing environments were modeled after already established network forensic processes.

A sample case example was included to demonstrate validation of the expert panel findings and show how the study results can be incorporated into the classroom environment. The scenario includes many cloud based forensic evidence items. The scenario addressed the privacy and legal considerations associated with cloud-based evidence. The process used in the case example project provided students with hands-on experience using tools for cloud-based evidence acquisitions that are different from traditional digital forensic tools.

Recommendations for educators included 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. Once the research is completed porting over these processes to the educational environment is the next step to producing new teaching methodologies and forensic processes. Creating new scenarios such as the one provide in this paper furthers the development of training programs, courses, and curriculum for the existing body of knowledge.

9. REFERENCES

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/

Cohen, F. (2011). Putting the science in digital forensics. *Journal of Digital Forensics, Security and Law, 6*(1), 7-14. Retrieved from http://www.jdfsl.org/

Decker, M., Kruse, W., Long, B., & Kelley, G. (2011). *Dispelling common myths of "live digital forensics"*. Retrieved from http://www.dfcb.org/docs/LiveDigitalForensics-MythVersusReality.pdf

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.

Dykstra J., Sherman, A. T.(2012, August). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques [Supplement]. *Digital Investigation, 9,* S90-S98. doi:10.1016/j.diin.2012.05.001.

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).

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

Garfinkel, S. L., Lessons Learned Writing Digital Forensics Tools and Managing a 30TB Digital Evidence Corpus, Digital Investigation 9, 2012, pg. S80-S89.

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

Holt, T. J., & Bossler, A. M. (2011). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice, 37*(3), 396-412. doi:10.1007/s12103-011-9131-5

James, J. I., Shosha, A. F., Gladyshev, P. (2013). Digital forensic investigation and cloud computing. In K Ruan (Ed.), *Cybercrime and cloud forensics: Applications for investigation processes*. (pp. 1-41). doi:10.4018/978-1-4666-2662-1.ch001

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/

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

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

Robinson, R. (2012, July 5). *Cloud cyber crime: Hackers take to the skies*. Retrieved from: http://midsizeinsider.com/en-us/article/cloud-cyber-crime-hackers-take-to-the-s

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

Svetcov, E. (2011). *An introduction to cloud forensics*. Retrieved from http://blog.datacraft-asia.com/2011/01/an-introduction-to-cloud-forensics/

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7-18. doi:10.1007/s13174-010-0007-6

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

Zimmerman, S. (2012, February). Legal hurdles in mobile device forensics. *Digital Forensics Magazine*, (10), 28-30. Retrieved from http://www.digitalforensicsmagazine.com/

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: Online Written Narrative Interview 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 B: Online Written Narrative Questions Regarding the 20 Selected Forensic Processes

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
10. Remove the hard disk drive(s) from the system unit
11. Document number of hard drives, size and disk geometry
12. Use EnCase to obtain an image of suspect media
13. Use AccessData's FTK to obtain an image of suspect media
14. Use UNIX/Linux dd command to obtain an image of suspect media.
15. Identify any network connections, and document findings
16. Generate a MD5/SHA1 hash value of the forensic image
17. Preserve suspect media in its original condition and securely seal
18. Place suspect media in a secure storage area or evidence vault
19. Create a clone copy of suspect media for mounting and analysis
20. Perform a visual comparison of the directory structure of the image and the suspect disk to verify that the image is readable

Appendix C: Figures

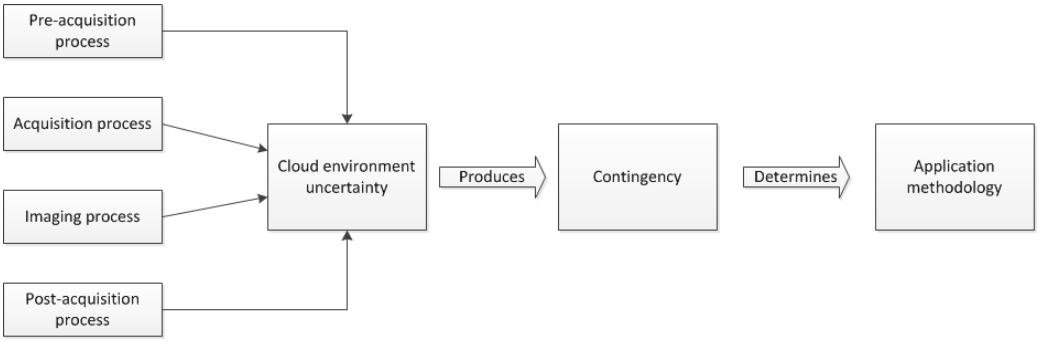

Figure 1. An illustration of the digital evidence forensic acquisition cloud contingency model

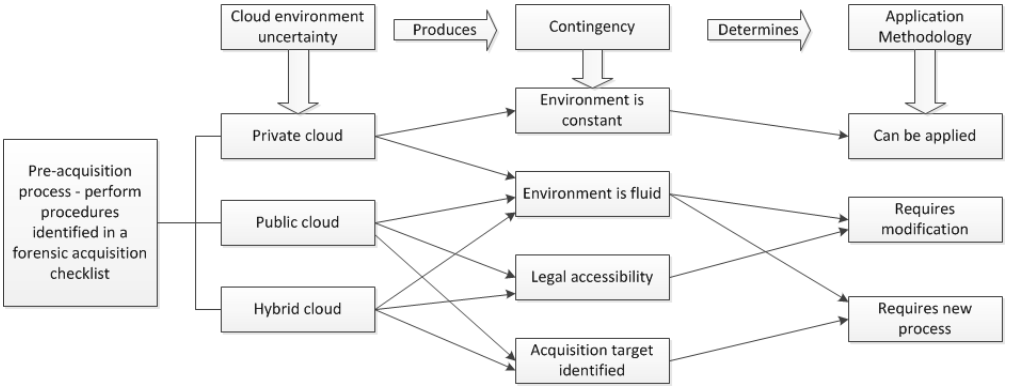

Figure 2. Application of the digital evidence forensic acquisition cloud contingency model to pre-acquisition process.

Appendix D: Tables

Table 1
Study Results of the 20 common forensic procedures for applicability to cloud computing environments

Forensic Procedure identification	Number of procedures
Traditional forensic processes usable for the forensic acquisition of digital evidence in cloud computing environment	11
Traditional forensic processes modifiable for the forensic acquisition of digital evidence in cloud computing environments	7
Traditional forensic processes required the development of new processes for the forensic acquisition	2