Chapter 16
Legal Process and Requirements for Cloud Forensic Investigations

Ivan Orton
King County Prosecuting Attorney's Office, USA

Aaron Alva
University of Washington, USA

Barbara Endicott-Popovsky
University of Washington, USA

ABSTRACT

For the emerging field of cloud forensics, the development of validated and repeatable scientific processes for conducting cloud forensic investigations should include requirements that establish evidence collected as legally admissible. There is currently an uncertainty in the legal requirements for cloud forensics. Forensic investigations in the cloud introduce unique issues that must be addressed, and the legal environment of the cloud must be considered. The authors will detail the process in criminal cloud forensic investigations for commanding production from cloud providers including constitutional and statutory limitations, and the civil and criminal admissibility processes. Decisions in court cases rely on the authenticity and reliability of the evidence presented. Ensuring cases involving cloud forensics follow the proper legal process and requirements will be beneficial for validating evidence when presented in court. Further, understanding of legal requirements will aid in the research and development of cloud forensics tools to aid investigations.

1.0. INTRODUCTION

Cloud forensics introduces unique legal issues beyond those encountered during traditional digital forensics cases and presents a challenge to the legal system, which is not well equipped to handle such cases. This chapter will examine issues regarding commanding and producing in court digital evidence resident in the cloud. The "commanding production" section will focus on the criminal law. The "producing in court" or admissibility section will apply to both civil and criminal practice.[1]

DOI: 10.4018/978-1-4666-6539-2.ch016

To date, there is limited guidance available from case law that can govern decisions involving admissibility of cloud-based evidence. Our analysis is founded on an extensive review of the constitutional and statutory limitations that apply to cloud forensic investigations, as well as a walkthrough of admissibility standards for digital evidence including issues unique to cloud-based evidence.

Cloud computing is in its infancy. This chapter identifies the ways in which digital evidence in the cloud differs in substance from digital evidence gathered from computer hard drives and networks under the control of parties engaged in legal actions. The material presented begins to identify the issues surrounding cloud forensics uncertainty, comparing these issues to those raised in more traditional digital forensics cases.

The authors recognize that addressing barriers to conducting effective cloud forensic investigations will require a concerted effort by stakeholders involved in the process, including the cloud provider.

Development of new tools and procedures for cloud forensics may not currently address the complex legal requirements that must be met in order for cloud-gathered evidence to be admissible in court. Incorporating the need to collect admissible evidence in system design can improve the ability of system operators to identify, collect, store and retrieve valid evidence. It is particularly important for potential cloud customers to analyze this before moving to the cloud since cloud customers lose the ability to control this process once information is moved to the cloud (Convery, 2010). Understanding the legal requirements for admissible cloud evidence allows for incorporation of those concepts into information systems, creating a forensically ready design that will improve the efficiency of valid evidence collection.

1.1. Cloud Forensics Definitions

The emerging field of cloud forensics combines the disciplines of digital forensics and cloud computing (Ruan, Carthy, Kechadi, & Crosbie, 2011b). Cloud computing is defined by the U.S. National Institute of Standards and Technology (NIST) as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011).

Digital forensics is the study of evidence from attacks on computer systems in order to learn what has occurred, how to prevent it from recurring, and the extent of the damage. This field initially was divided into digital disk forensics–retrieving admissible evidence from a computer disk–and network forensics–retrieving evidence throughout a network system wherever it may reside or flow. Based on network access and architecture, cloud forensics is a subset of network forensics (Ruan, Carthy, Kechadi, & Crosbie, 2011b).

With traditional disk forensics, the model by which investigations are conducted rely on the acquisition of physical disks, and require a clear chain of custody be maintained on the physical items (Pollitt, Caloyannides, Novotny, & Shenoi, 2004). By contrast, cloud forensics requires a different approach due to characteristics of the cloud environment where physical assets are not under the control of the user and may not be identified and located easily due to the dynamic nature of cloud provisioning.

1.2. Legal Background

Cloud forensics, like traditional digital forensics, requires that technical and legal practitioners have a strong integrated understanding of computer science and the law. U.S. courts operate through a combination of procedural rules and case law precedent as guidance when ruling on evidentiary issues (Kuntze, Rudolph, Alva, Endicott-Popvsky, Christiansen, & Kemmerich, 2012). Other countries where cloud data may reside may have a differ-