Chapter 11
Forensics as a Service

Jon Rav Gagan Shende
EBSL Technologies International, USA

ABSTRACT

In today's dynamic information technology system, one area of tremendous focus and recent growth has been that of the cloud-computing model in its various offerings. With this growth, however, come new challenges within the realms of e-discovery and digital forensics, as we traditionally know it. The rapid growth of cloud-computing services and the rate of acceptance and use by consumers are on the rise. Conversely, both legitimate and illegitimate activates can leverage the resources of the cloud to execute their operations. With the challenges growing to combat computer crime that utilizes the cloud ecosystem and the ease of which a criminal activity may be hidden using a cloud service, it is imperative that a cloud provider dedicate time, training, budget, and other resources to provide the facility for forensic investigators as well as law enforcement to combat this threat. The Cloud-Forensics-as-a-Service (FRaaS) model introduced later in this chapter can provide a comprehensive cloud forensics solution for creating a repeatable system. Such a system could be implemented as a standard forensics operational model for deployment within the cloud ecosystem regardless of environments and client service lines.

INTRODUCTION

This chapter will introduce a process for implementing a living Forensics-as-a-Service (FRaaS) model that could augment a cloud-computing ecosystem to meet the needs of a forensics investigation in this environment.

One of the challenges with any cloud-computing ecosystem is the lack of a repeatable environment. This may lead to a deficiency of uniformity when conducting a forensic investigation within multiple cloud ecosystems. If an investigator assumes the challenge of conducting a forensic investigation within the Cloud, there will be a constant volume of information to process, which can overload any one monitoring tool.

DOI: 10.4018/978-1-4666-2662-1.ch011

Within the forensics community, we know that for any digital forensics investigation, the factors of Volume, Evidence, and Time are of importance. We need to be cognizant of the fact that the volume of potential evidence has the potential for any evidence to be contaminated. The time to identify potential criminal activity is also critical. For example, a crime may be ongoing for an extended time unbeknownst to authorities.

Given the rise of cloud computing, we now have to contend with the volume of proportionally increasing data resulting in an increase in processes forensic investigators will have to analyze. As a result, a system needs to be implemented that can store multiple formats of data from numerous sources. Financial considerations of deploying this system as inexpensively as possible should be a priority. This system must be able to provide the option to scale out to meet needs as well as ensure that the processing capacity to support complex data analysis is made available, all within defined processes and budgetary requirements.

Additionally digital evidence must still satisfy the same legal requirements as that in a traditional forensic system. It must be *Authentic–Reliable–Complete–Believable–Admissible (ARCBA).* In this ecosystem, we also have to contend with the challenge of traceability given its assumed "vastness."

How then should we remediate such a situation? An ad-hoc data gathering process will have significant ramifications in the event that evidence retrieved is important to a future litigation process. The FRaaS model and its related tools aims to ensure that relevant evidence collected and presented will follow a defined and repeatable process when gathering, verifying and storing evidence or information.

As we traverse this chapter, we will discuss aspects of the FRaaS model, which will include a process that should be able to amalgamate relevant instance "data points." This process may then enable an investigator to concentrate on critical information that is applicable, actionable, and presentable for use in an e-discovery forum.

This model will provide a real-time tool, which should reduce the time to organize and filter information within the cloud ecosystem in which it is operating. Thus, allowing the investigator to manage instance flow and seamlessly tie relevant event data.

In summary, the FRaaS model aims to establish a cloud forensic investigative process, which can be implemented within a cloud ecosystem, integrated with tools that should ensure relevant information is gathered, verified, and stored in a manner that is forensically sound and legally defensible.

Before proceeding any further with our FRaaS model, a high-level recap on cloud computing follows. What exactly is cloud computing? Is it virtualization? Is it services that we accessed via a Web browser over the years, a new technology, or is it all of these rebranded from a marketing and revenue focused viewpoint? More importantly, how will these diverse components impact and affect a digital forensics investigation as society moves away from traditional infrastructures into a cloud ecosystem?

The industry term "Cloud Computing" started gaining notice when Google and IBM launched a university initiative to address Internet scale computing in 2007 (Google News, 2007). Some of the services that now comprise the cloud-computing ecosystem, have been evolving since the '90s. Some of its predecessors are grid computing and utility computing as well as the Software-as-a-Service offerings established a little over a decade ago.

We should leverage tested forensics methods, processes, and tools that have been in use within the traditional forensics environments where there is an alignment to a cloud system. However, there may be some challenges with this in the form of conformity, repeatability, and seamlessness of processes and techniques.

A cloud service's revenue lifecycle, simply stated, is a pay-as-you-go service. An end user can