CERIAS

The Center for Education and Research in Information Assurance and Security

Applying the OSCAR Forensic Framework to Investigations of Cloud Processing

By: Bryan R. Lee and Dr. Sam Liles

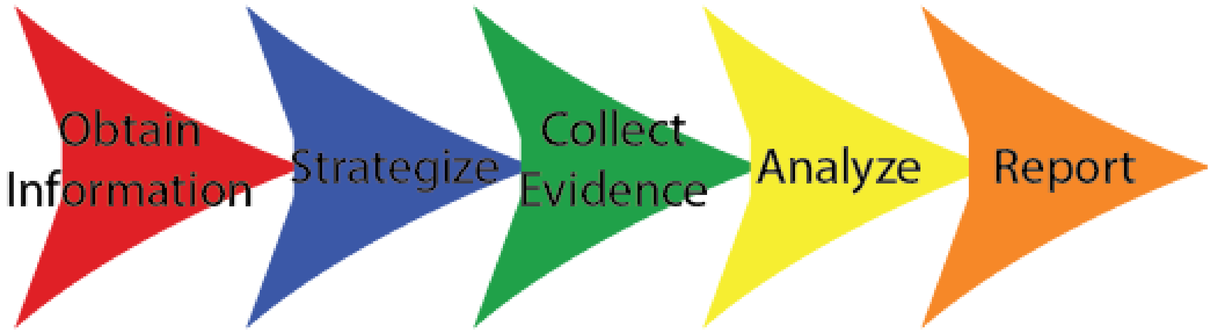
Statement of Purpose

The purpose of this research is to attempt to apply OSCAR, a forensic framework for investigating cases involving networked devices, to a cloud computing investigation. The research emphasizes the investigation of the Infrastructure as a Service (IaaS) model of cloud computing. Of particular interest is the use of cloud processing to commit an illegal act. A standard investigative model is necessary within a forensics field in order to guarantee the investigation is properly handled and repeatable. This is perhaps of more importance in the realm of cloud forensics because of the relative newness of the field and the complexity of such investigations.

Abstract

This paper examines the OSCAR network forensic investigation model and attempts to apply it to the realm of infrastructure as a service cloud computing. There are many difficulties within a forensic investigation in the cloud that must be taken into account, such as jurisdiction due to the way information is stored in the cloud and chain of evidence and trust that can be placed in evidence from the cloud. Although a forensic model of investigation cannot solve all the problems faced within an investigation of this type, a standard model can help to ensure that all investigations of this variety are handled in the same manner. This can provide a standard level of trust in evidence discovered during an investigation of this nature and provide for a standard way to deal with problems such as jurisdiction throughout the course of these investigations. The OSCAR investigation model appears to be a fairly robust model when compared with other models, such as Martini and Choo's implementation of the NIST model for use in cloud forensics.

OSCAR Forensic Investigation Framework



Comparison

The NIST model is focused on forensic investigations for the purpose of bringing criminal charges in a court of law. The OSCAR model, while forensic, is not focused solely on this. Rather, it takes into account resources available to the investigator from within the affected entity, the goals and time line of an investigation set forth by the entity, and other factors that are highly dependent on the entity or entities involved. The implementation of the NIST model does not take into account what the affected entity has to offer in terms of personnel and equipment that could be used within the investigation. It furthermore does not consider any effects that the investigation may have on the affected entity. It is not concerned with business continuity. Its goal is merely to get the evidence, analyze it, and bring it to court. In this sense, the OSCAR investigative method is broader and can be applied in more situations, from incident response to an actual forensic investigation.

Martini & Choo Proposed Framework

PURDUE UNIVERSITY