B30 A Proposed Cloud Computing Forensic Interface

Ernesto F. Rojas, MBA, PO Box 597, Seabrook, TX 77586*

After attending this presentation, attendees will be able to understand the need for a common interface that enables forensic practitioners to extract data, metadata, and other log files and to conduct an investigation of the events related to a particular case. This presentation is a proposal to the forensic cloud computing community to consider development of a common interface to facilitate training, consistency of results, and commonality of forensic collections among multiple cloud providers.

This presentation will impact the forensic science community by encouraging discourse among members of the forensic cloud computing community to recognize the difficulty that investigators have in learning multiple forensic interfaces from one provider to another and the time savings created by a common user interface for forensic collections.

At the present time, Cloud Computing providers have either developed a method or interface for the collection of evidence from their cloud environment and in many cases there is no interface provided to the user community for evidence collection. This disarray is rapidly becoming a major obstacle for cloud users, law enforcement, the legal community, the courts, and government agencies to collect information to support an investigation, when cloud applications and storage are employed as part of the computing environment storing data related to a legal dispute or incident. This presentation proposes a model that has a common user interface to effect the collection of evidence, with the back-end of the model customized to interface with the provider's existing software architecture, so that when files are collected they are presented in a forensically sound format, with their metadata intact in a similar manner as files collected by current digital forensic processes available today.

This proposal is based on foundational work done by Dykstra and Sherman for the FROST interface developed and the experience in forensics of the presenter.[1] A list of items that should be part of the interface will be offered as a starting point from which to develop the menu for the interface, along with a proposed method by which to have a back end that will be easy to connect to the cloud providers existing software architecture. In addition the use of existing forensic evidence formats will be suggested as a way of standardizing the output of the interface.[2] In conclusion, this presentation proposes to stimulate the conversation to adopt a common format for the collection of evidence from cloud providers.

References:

1. Dykstra, J. and Sherman, A.T.; Design and Implementation of FROST: Digital Forensic Tools for the OpenStack Cloud Computing Platform; Cyber Defense Lab, Department of CSEE, University of Maryland, Baltimore County; April 12, 2013.
2. Brown, C.L.T.; Computer Evidence Collection and Preservation; Charles River Media Inc., Chapter 12; 2006

Cloud, Forensic, Interface

** Presenting Author*