B13 Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies

Josiah Dykstra, MS, 1739 Carriage Lamp Court, Severn, MD 21144; and Alan T. Sherman, PhD, University of Maryland, 1000 Hilltop Circle, Baltimore, MD 21250*

After attending this presentation, attendees will understand how cloud computing poses unique forensic challenges that require new methods of forensic acquisition, evidence preservation and chain of custody, and open problems for continued research.

This presentation will impact the forensic science community by laying out the significant issues associated with digital forensics for cloud computing and preparing the way for forensic investigation of the inevitable criminal targeting of cloud environments.

Crime committed using cloud computing resources and against cloud infrastructures is inevitable. Though real incidents have already taken place against cloud providers including Google, an absence of documentation indicates that no crimes using the cloud or targeting it directly have been publicized nor litigated thus far. Forensic investigators must understand that current tools and techniques are inadequate in the cloud environment where acquisition, examination and analysis will be in practice executed very differently than is done today. To illustrate these issues, two hypothetical crimes are fabricated and the forensic investigation is deconstructed against them.

Companies are embracing cloud technology to offload some of the cost, upkeep, and growth of equipment that they would otherwise have purchased themselves. Cloud infrastructure, with exceptional bandwidth, storage and computing power, offers an attractive prize for hackers. While many people have lamented how the users of the cloud and their data are protected, few of these discussions have considered the difficulty of responding to security breaches, including forensics and criminal prosecution. Furthermore, no case law exists on which to extrapolate the desire of the courts on the matter. Garfinkel recently suggested that "cloud computing in particular may make it impossible to perform basic forensic steps of data preservation and isolation on systems of forensic interest."[1]

To provide an update about the state of digital forensics for cloud-related crimes, the investigative response and forensic process of two hypothetical, but plausible, case studies of crimes tied to cloud computing are considered. While fictional, they describe computer crimes that are not uncommon today. Case Study one uses the cloud as an accessory to a crime. In this case, a criminal stores and distributes child pornography using the cloud. Case Study two targets the crime against the cloud. In this case, a criminal hacks into a cloud-based website and installs malicious code. These common crimes require a reinterpretation when set in a cloud computing environment. In both scenarios, the following themes emerge that differentiate these investigations from traditional digital forensics:

- Acquisition of forensic data is more difficult.
- Cooperation from cloud providers is paramount.
- Current forensic tools appear unsuited to process cloud data.
- Cloud data may lack key forensic metadata.
- Chain of custody is more complex.

These two case studies illustrate larger issues that exist beyond the scope of the specific examples. Forensic acquisition is a renewed challenge, one unsuited for today's tools, which will possibly be addressed by a combination of technological and legal approaches. We have begun to evaluate the ability of popular forensic tools to obtain evidence from a cloud environment. Cooperation with providers will empower consumers to understand their risks and give them leverage to prosecute crimes. The preservation and availability of forensically relevant metadata remains an open problem.

The issues of common crimes that vary from today only in their use of the cloud have been evaluated. This technology alone introduces peculiarities and open problems that demand immediate attention. Shown in this presentation are deficiencies in both law and technology can be addressed with proper advances.

Reference:

[1.] Garfinkel, Simson, "Digital Forensics Research: The Next 10 Years", DFRWS 2010, Portland, OR, August 2010

Cloud Computing, Digital Forensics, Case Studies

 ** Presenting Author*