C17 Cloud Computing Forensic Science Challenges

Josiah Dykstra, PhD, Department of Defense, 8080 Greenmead Drive, College Park, MD 20740; Lon Gowen, PhD, United States Agency for International Development, 2733 Crystal Drive, Ste 11-510, Two Potomac Yard, Arlington, VA 22202; Martin Herman, PhD, 100 Bureau Drive, Mail Stop 2000, Gaithersburg, MD 20899; Michaela Iorga, PhD, National Institute of Standards and Technology, Information Technology Laboratory, 100 Bureau Drive, Gaithersburg, MD 20899; Robert Jackson, MS, SphereCom Enterprises Inc, 7900 Sudley Road, Ste 416, Manassas, VA 20109; Otto Scot Reemelin, MS, CBIZ, Inc, 3101 N Central Avenue, Ste 300, Phoenix, AZ 85012; Ernesto F. Rojas, MBA, PO Box 597, Seabrook, TX 77586; Keyun Ruan, PhD, Espion Group, Corrig Court, Corrig Road, Sandyford Industrial Estate, Dublin 18, Dublin, IRELAND; A. Michael Salim, MS, American Data Technology, Inc, PO Box 12892, Research Triangle Park, NC 27709; Ken E. Stavinoha, PhD, Cisco Systems, 170 W Tasman Drive, San Jose, CA 95134; Laura P. Taylor, MS, Relevant Technologies, 10440 Little Patuxent Parkway, Ste 900, Columbia, MD 21044; and Kenneth R. Zatyko, MS, Ernst & Young LLP, 1101 New York Avenue, NW, Washington, DC 20005*

After attending this presentation, attendees will have a better understanding of some of the main challenges faced by forensic investigators attempting to identify, collect, analyze, and interpret digital evidence residing in cloud computing environments.

This presentation will impact the forensic science community by describing research performed by the National Institute of Standards and Technology (NIST) Cloud Computing Forensic Science Working Group, which was established to aggregate forensic science challenges in the cloud environment and to develop plans for measurements, standards, and technology research to mitigate the challenges that cannot be handled with current technology and methods.

The cloud exacerbates many technological, organizational, and legal challenges already faced by digital forensics examiners. Several of these challenges, such as those associated with data replication, location transparency, and multi-tenancy, are somewhat unique to cloud computing forensics.

The Group plans to prioritize the challenges enumerated. For high-priority challenges, gaps in technology and standards will be determined, resulting in a roadmap for addressing the challenges.

The challenges this study has aggregated are categorized into the following groups:

Architecture (e.g., diversity, complexity, provenance, multi-tenancy, data segregation, etc.) — Architecture challenges in cloud forensics include dealing with variability in cloud architectures between providers; tenant data compartmentalization and isolation during resource provisioning; proliferation of systems, locations, and endpoints that can store data; accurate and secure provenance for maintaining and preserving chain of custody; infrastructure to support seizure of cloud resources without disrupting other tenants; etc.

Data Collection (e.g., data integrity, data recovery, data location, imaging, etc.) — Data collection challenges in cloud forensics include locating forensic artifacts in large, distributed, dynamic systems; locating and collecting volatile data; data collection from virtual machines; data integrity in multi-tenant environments where data is shared among multiple computers in multiple locations and accessible by multiple parties; inability to image all the forensic artifacts in the cloud; accessing data of one tenant without breaching the confidentiality of other tenants; recovery of deleted data in a shared and distributed virtual environment; etc.

Analysis (e.g., correlation, reconstruction, time synchronization, logs, metadata, timelines, etc.) — Analysis challenges in cloud forensics include correlation of forensic artifacts across and within cloud providers; reconstruction of events from virtual images or storage; integrity of metadata; timeline analysis of log data including synchronization of timestamps; etc.

Anti-Forensics (e.g., obfuscation, data hiding, malware, etc.) — Anti-forensics are techniques used specifically to prevent or mislead forensic analysis. Challenges in cloud forensics include the use of obfuscation, malware, data hiding, or other techniques to compromise the integrity of evidence; malware may circumvent virtual machine isolation methods; etc.

Incident First Responders (e.g., trustworthiness of cloud providers, response time, reconstruction, etc.) — Incident first-responder challenges in cloud forensics include confidence, competence, and trustworthiness of cloud providers to act as first responders and perform data collection; difficulty in performing initial triage; processing a large volume of forensic artifacts collected; etc.

Role Management (e.g., data owners, identity management, users, access control, etc.) — Role management challenges in cloud forensics include uniquely identifying the owner of an account; decoupling between cloud user credentials and physical users; ease of anonymity and creating fictitious identities online; determining exact ownership of data; authentication and access control; etc.

Legal (e.g., jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy, ethics, etc.) — Legal challenges in cloud forensics include identifying and addressing issues of jurisdictions for legal access to data; lack of effective channels for international communication and cooperation during investigations; data acquisition that relies on the cooperation of cloud providers, as well as their competence and trustworthiness; missing terms in contracts and service level agreements; issuing subpoenas without knowledge of the physical location of data; seizure and confiscation of cloud resources may interrupt business continuity of other tenants; etc.

Standards (e.g., Standard Operating Procedures (SOPs), inter-operability, testing, validation, etc.) — Standards challenges in cloud forensics include lack of even minimum/basic SOPs, practices, and tools; lack of inter-operability among cloud providers; lack of test and validation procedures; etc.

Training (e.g., forensic investigators, cloud providers, qualification, certification, etc.) — Training challenges in cloud forensics include misuse of digital forensic training materials that are not applicable to cloud forensics; lack of cloud forensic training and expertise for both investigators and instructors; limited knowledge by record-keeping personnel in cloud providers about evidence; etc.

Digital Forensics, Cloud Computing, Forensics Challenges