C32 The Acquisition and Analysis of Evidence From Cloud and Internet of Things (IoT) Services

Vassil Roussev, PhD, Computer Science, 2000 Lakeshore Drive, 308 Mathematics Bldg, New Orleans, LA 70148*

After attending this presentation, attendees will better understand the qualitative differences between working with traditional and cloud-based evidence sources. Attendees will also gain methodological insight into the inherent limitations of the currently prevalent client-side analysis of cloud services as well as a preliminary notion of how IoT forensics is likely to take place.

This presentation will impact the forensic science community by clearly demonstrating: (1) the need to develop new approaches to investigating cloud services; (2) a summary of early results in the field, including new data sources that are not available on client devices; and, (3) several new types of capabilities that forensic tools already need.

The rapid transition to a cloud-centric delivery of Information Technology (IT) services is having a profound, and currently underappreciated, impact on the acquisition and analysis of digital evidence. Namely, the switch from deploying "software as a product" to using it "as a service" changes both the legal environment and the technical requirements for search, seizure, and evidence analysis operations. Considering the technical side, it is shown that digital forensics needs to move away from the idea that physical acquisition is the gold standard and transition to the concept of acquiring evidence from an authoritative source, such as a cloud service. It is argued that digital forensics, as a whole, is on the verge of transitioning to a new mode of operation in which large-scale automated data analysis will dominate and mainstay data recovery and reconstruction techniques will rapidly diminish in importance.

Several case studies of cloud acquisition and analysis tools that work with cloud drive and online collaboration services to illustrate both the limitations of client-side analysis and the new opportunities presented by rich historical data collected by services will be discussed. Examples include direct acquisition from Dropbox™, Box, Google® Drive™, and Microsoft® OneDrive®, and analysis of native Google® Docs artifacts, including the extraction of user biometric signatures based on keyboard dynamics.

This presentation will also briefly consider the forensic analysis of IoT devices, which are placed in several capability classes. The argument will be made that for a large class of low-end devices, the only meaningful forensic analysis will be based on the data acquired from the cloud service backing the devices.

Based on the above reasoning and experiences, the argument is made that the next generation of forensic tools will be primarily focused on working with network Application Programming Interfaces (APIs) and the forensic community will need to develop completely new capabilities for (semi-) automated reverse engineering and will describe the semantics of network protocols and data APIs.

Cloud Forensics, Cloud Evidence, IoT Forensics