




Jun 10th, 11:15 AM

## On Resolving the Cloud Forensics Conundrum

John Bagby

*The Pennsylvania State University, Pennsylvania, USA, jbagby@ist.psu.edu*

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

---

### Scholarly Commons Citation

Bagby, John, "On Resolving the Cloud Forensics Conundrum" (2013). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 6.

<https://commons.erau.edu/adfsl/2013/monday/6>

This Presentation is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).

**EMBRY-RIDDLE**  
Aeronautical University™  
SCHOLARLY COMMONS

(c)ADFSL



## **ON RESOLVING THE CLOUD FORENSICS CONUNDRUM** **(Invited Paper/Presentation)**

John Bagby  
The Pennsylvania State University  
Pennsylvania, USA  
[jbagby@ist.psu.edu](mailto:jbagby@ist.psu.edu)

### **ABSTRACT**

The “cloud” is idiom for an ill-defined set of online services. The cloud simultaneously offers IT savings and promises advances in functionality (e.g., ubiquity). However, the cloud also imposes poorly understood burdens on security and it may provoke injustice. Thus, the cloud presents a durable and seemingly irreconcilable conundrum for the digital forensics communit(ies). First, cloud proponents make efficiency promises for cloud services (SaaS, IaaS, PaaS). These translate well into the digital forensics domain. Indeed, the cloud may enable crowd sourcing of investigatory data vastly lowering costs of dispute resolution. For example, cloud-based litigation war rooms may reduce electronic discovery costs substantially. Furthermore, expansion of cloud-based evidence repositories could encourage settlements on litigation claims theretofore considered infeasible. Second, however, the current architecture of many cloud services arguably undermines justice. Proliferation of cloud services arguably undermines several due process presumptions made to support litigants’ needs in their case preparation. For example, the cloud increases opacity complicating forensics because file and directory structures are unstable and in constant flux. Indeed, cloud practices may compromise the forensic quality of evidence due to the (1) off-shoring of data and (2) practices that result in persistent file rotation with frequent metadata modification (e.g., activity logs). Many other nations that typically host cloud services have generally under-developed laws regulating privacy, security and litigation process rights. Therefore, these prevailing international practices erect barriers of cost, reliability, and access (lack of reciprocity) to accurate forensics. Indeed, all these conditions are inconsistent with U.S.-style litigation expectations. This paper attempts provisional resolution of this conundrum by recommending better deployment of existing standards from the ISO, NIST, GARP, GAAP, GAAS and other sources. Proposals are evaluated for the development, diffusion and implementation of new standards that would address the likely evolution in cloud architectures. This analysis proposes to restore traditional expectations for evidence transparency as data continues its migration into the cloud.

