

Chapter 3

Challenges to Digital Forensic Evidence in the Cloud

Fred Cohen
All.Net, USA

ABSTRACT

Digital forensic evidence is subject to a variety of challenges, and these challenges apply in the Cloud as anywhere else. This chapter is an overview of these issues specifically oriented toward the Cloud Computing environments of today.

INTRODUCTION

Digital forensic evidence is identified, collected, transported, stored, analyzed, interpreted, attributed, reconstructed, presented, and destroyed through a set of processes. Challenges to this evidence may come through challenges to elements of this process. These processes, like all other processes and the people and systems that carry them out, are imperfect. That means that there are certain types of faults that can occur in these processes¹.

The emerging cloud-computing environment has three distinct features of note related to these issues: (1) distributed computing implies that evidence may exist in and reflect activities on many computers, (2) those computers may be at

many locations, and (3) the computers may not be owned by the same entities as the content at issue. This chapter covers these differences in context of the previous work in the digital forensics area.

Faults and Failures

Faults consist of intentional or accidental making or missing of content, contextual information, the meaning of content, process elements, relationships, ordering, timing, location, corroborating content, consistencies, and inconsistencies. In the cloud context, the faults and failures may extend to multiple computers in multiple locations under control of multiple parties². Thus, the opportunities for faults and failures are extended.

Not all faults produce failures, but some may. While it may be possible to challenge faults, this generally does not work and is unethical if failures

DOI: 10.4018/978-1-4666-2662-1.ch003

are not demonstrable. Certain things turn faults into failures, and it is these failures that legitimately should be and can be challenged in legal matters.

Failures consist of false positives and false negatives. False negatives are items that should have been found and dealt with in the process but were not, while false positives are things that should have been discarded or discredited in the process but were not.

Legal Issues

In the United States, at the Federal level, evidence is admitted or rejected based on the relative weights of probative and prejudicial value. Other standards apply in different jurisdictions, but this standard is fairly common worldwide. Probative value is the extent to which potential evidence supports a legal claim. Prejudicial value is the extent to which that evidence potentially influences the trier of fact (usually a judge or jury). If more probative than prejudicial, evidence is admissible^{3,4}.

Part of the issue of probative value is the quality of the evidence. If the process that created the

evidence as presented is flawed, this reduces the probative value. Impure evidence, evidence presented by an expert who is shown to lack expertise in the subject at hand, evidence that has not been retained in a proper chain of custody, evidence that fails to take into account the context, or evidence falling under any of the other fault categories shown in Figure 1, all lead to reduced probative value. If the effect of these faults is wrong results, the probative value may go to zero.

In the cloud context, these issues may be greatly complicated. For example, establishing a chain of custody is potentially problematic if evidence comes from or through many jurisdictions and providers, is gathered without direct physical access, was under the control of third parties, is stored in and moved between systems with a history of breaking, accessible from anywhere by anyone, or was protected only by a password that was one of millions of such passwords stolen in the last 6 months. Attesting to the reliability⁵ of such evidence may be problematic⁶.

Figure 1. Challenges overview

Process	Faults	Failures
Identification	Make / Miss	False positive
Collection	Content	False negative
Transport	Context	
Storage	Meaning	
Analysis	Process	
Interpretation	Relationship	
Attribution	Ordering	
Reconstruction	Time	
Presentation	Location	
Destruction	Corroboration	
	Consistency	
	Accident/Intent	

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/challenges-digital-forensic-evidence-cloud/73958

Related Content

An Effective Selective Encryption Scheme for H.264 Video based on Chaotic Qi System

Fei Peng, Xiao-wen Zhu and Min Long (2013). *International Journal of Digital Crime and Forensics* (pp. 35-49).

www.irma-international.org/article/an-effective-selective-encryption-scheme-for-h264-video-based-on-chaotic-qi-system/83488

Trust Management in Mobile Ad Hoc Networks for QoS Enhancing

Ryma Abassi (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 131-161).

www.irma-international.org/chapter/trust-management-in-mobile-ad-hoc-networks-for-qos-enhancing/131401

Measuring Crime in and around Public Housing Using GIS

Harold R. Holzman, Robert A. Hyatt and Tarl Roger Kudrick (2005). *Geographic Information Systems and Crime Analysis* (pp. 311-329).

www.irma-international.org/chapter/measuring-crime-around-public-housing/18831

Multilevel Visualization Using Enhanced Social Network Analysis with Smartphone Data

Panagiotis Andriotis, Zacharias Tzermias, Anthi Mparmpaki, Sotiris Ioannidis and George Oikonomou (2013). *International Journal of Digital Crime and Forensics* (pp. 34-54).

www.irma-international.org/article/multilevel-visualization-using-enhanced-social-network-analysis-with-smartphone-data/103936

Named Entity Recognition Method of Chinese Legal Documents Based on Parallel Instance Query Network

Rui Lu and Linying Li (2024). *International Journal of Digital Crime and Forensics* (pp. 1-19).

www.irma-international.org/article/named-entity-recognition-method-of-chinese-legal-documents-based-on-parallel-instance-query-network/367470