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 processes[1].

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.

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

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 parties[2]. 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

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 reliability[5] of such evidence may be problematic[6].

Figure 1. Challenges overview