Chapter 1
Digital Forensic Investigation and Cloud Computing

Joshua I. James
University College Dublin, Ireland

Ahmed F. Shosha
University College Dublin, Ireland

Pavel Gladyshev
University College Dublin, Ireland

ABSTRACT

This chapter aims to be a high-level introduction into the fundamental concepts of both digital forensic investigations and cloud computing for non-experts in one or both areas. Once fundamental concepts are established, this work begins to examine cloud computing security-related questions, specifically how past security challenges are inherited or solved by cloud computing models, as well as new security challenges that are unique to cloud environments. Next, an analysis is given of the challenges and opportunities cloud computing brings to digital forensic investigations. Finally, the Integrated Digital Investigation Process model is used as a guide to illustrate considerations and challenges during an investigation involving cloud environments.

INTRODUCTION

Cloud computing is a topic that has been gaining popularity with businesses and end users in recent years. A certain level of hype and inconsistent definition has lead to some confusion about what cloud computing is, and what services it can provide. Along with general confusion, some concerns have been raised about the security of cloud environments. As seen with traditional computing, a growing concern for security leads to consideration of incident response and eventually digital forensic investigation capabilities. This work endeavors to examine the implications of cloud computing on digital forensic investigations.

To accomplish this, a high-level introduction into fundamental concepts of both digital forensic investigations and cloud computing for non-experts will be given. A brief overview of

DOI: 10.4018/978-1-4666-2662-1.ch001

the history and advancement of digital forensic science, legal considerations surrounding digital forensic investigations, the current state of digital crime, types of digital forensic examinations, and an introduction into current digital forensic investigation process models will be given to build the reader's understanding of digital forensic science. Next, fundamental concepts of cloud computing, such as service and deployment models, will be covered. Once fundamental knowledge of cloud computing is established, some cloud computing security issues will be examined, followed by an analysis of the challenges and opportunities cloud computing brings to digital forensic investigations. Finally, a digital forensic investigation model will be used as a guide to illustrate digital forensic investigation challenges when applied to cloud environments.

DIGITAL FORENSIC SCIENCE

This section is a brief overview of the history and advancement of digital forensic science. Legal considerations surrounding digital forensic investigations, primarily focused on law in the United States, are discussed as well as the current state of digital crime and how digital investigators are addressing this global problem. Key digital forensic definitions, types of digital forensic examinations, and an introduction into current digital forensic investigation process models are given to build the reader's understanding of the field.

History and Advancement of Digital Forensic Science

Digital forensics[1] is a branch of the forensic sciences that deals with the analysis of digital evidence from digital sources (Palmer, 2001). Unlike traditional forensic sciences, a digital forensic analysis attempts to analyze non-physical evidence, or evidence that cannot be directly observed by humans without interpretation. It is because digital evidence cannot be directly observed that the admissibility of such evidence in court is under constant scrutiny (Casey, 2004). To help establish digital forensics as a credible forensic science, digital forensic science was defined at the first Digital Forensics Research Workshop (DFRWS) in 2001 as:

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions show to be disruptive to planned operations.

Digital investigation, however, predates this academic definition. Several notable but less developed definitions were previously proposed, such as those submitted by McKemmish (1999) and Civie and Civie (1998). Likewise, beyond academic definitions, research and digital investigations were already taking place prior to 2001. For example, Pollitt (1995) claimed that "[f]or a number of years now, law enforcement agencies have been seizing computers and other electronic devices." A growing interest in digital forensic investigation is confirmed by looking at other works of the early 1990s (Collier & Spaul, 1992a, 1992b; Clede, 1993; Spafford & Weeber, 1993). Hannan (2004) claims "forensic computing origins lay in the late 1980s…," which is when computer-based evidence was encountered more often by police (Jones, 2004), and is perhaps true for forensic computing as a field or separate science (Garfinkel, 2010), but from a legal perspective computers and computer evidence were topics of concern before then. For example, the U.S. Computer Fraud and Abuse Act was first enacted in 1984 (USDoJ, 2002), and also in the early 1980s *Computer in Court - A Guide to Computer Evidence for Lawyers and Computing Professionals* (Kelman & Sizer,