Chapter 109
A Forensic-as-a-Service Delivery Platform for Law Enforcement Agencies

Fabio Marturana
University of Rome "Tor Vergata", Italy

Simone Tacconi
Postal and Communications Police, Italy

Giuseppe F. Italiano
University of Rome "Tor Vergata", Italy

ABSTRACT

With the global diffusion of cybercrime, the ever-growing market penetration of high-performance and low-cost personal digital devices, and the commercial success of cloud computing, the area of digital forensics is faced with various new challenges that must be taken seriously. In this chapter, the authors describe a novel approach to digital investigations based on the emerging "Forensics as a Service" (FaaS) model. This model attempts to optimize Law Enforcement Agency's (LEA) forensic procedures, reduce complexity, and save operational costs. Inspired by previous work on distributed computing for forensic analysis, this chapter provides the reader with design guidelines of a FaaS platform for secure service delivery. The proposed FaaS platform should be able to support investigators and practitioners in their daily tasks (e.g. digital evidence examination, analysis, and reporting) once implemented by a cloud forensic provider or internally by a LEA. In this chapter, the authors also present the architecture components, interfaces, communication protocols, functional and non-functional requirements, as well as security specifications of the proposed framework in detail.

INTRODUCTION

The pervasiveness of the Internet and the large availability of low-cost, sophisticated and heterogeneous digital devices (i.e. PDAs, laptops, tablets, mobiles, and smartphones, etc.) characterized by large storage capacity and broadband network connections have contributed to the global diffusion of cyber threats and cybercrimes.

DOI: 10.4018/978-1-4666-6539-2.ch109

As technology penetrating to all works of life, cybercrime is also evolving at an astonishing pace. Whilst society is inventing and evolving, at the same time, criminals are deploying a remarkable adaptability in order to derive the greatest benefit from it (National Gendarmerie, 2011). According to McAfee (2012), the first part of 2012 has seen an impressive increase of cyber threats and malware. According to Federal Bureau of Investigation (FBI) 2008 statistics, in the United States, the size of the average digital forensic case is growing at the rate of 35% per year–from 83 GB in 2003 to 277 GB in 2007. With storage capacity growth outpacing network bandwidth and latency improvements, forensic data is not only getting bigger, but is also growing significantly larger relative to the ability to process them in a timely manner (Roussev, et al., 2009).

Under such circumstances, we believe that ever-growing amount of disk storage and bandwidth available to ordinary computer users will soon overwhelm forensics practitioners accustomed to handle digital evidence on a stand-alone workstation. Performing simple preprocessing operations, such as keywords indexing and image thumbnail generation, against a captured image will therefore consume vast amount of time before an investigation can even begin. Non-indexed "live" searches, such as those involving regular expressions, are already time-consuming and will become completely infeasible. Even worse, it will be impossible to raise the level of sophistication of digital forensics analysis because single forensics workstations will simply not be up to the task. As a consequence, forensic investigation tools will have to employ a pool of distributed resources in order to make investigations manageable (Roussev & Richard, 2004).

The Digital Forensic Research Workshop (DFRWS) has defined digital forensics as "the application of scientifically derived and proven methods aiming at preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence extracted from high-tech devices, maintaining a documented chain of evidence, for presentation in courts" (Digital Forensic Research Workshop, 2001). Huge efforts have been made in the last decade to improve digital forensic techniques and capabilities in order to develop new tools and procedures to support LEAs investigations. Following this trend, practitioners and researchers have developed new ideas and methods for retrieving evidence more effectively as it happened in the field of digital triage and machine learning-based automated analysis of evidence (Marturana, et al., 2012a, 2012b).

According to NIST (Mell & Grance, 2009), cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimum management effort or service provider interaction." Cloud computing has four deployment models (i.e. public, private, hybrid and community cloud) and three service models, i.e., Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

Cloud computing is radically changing the way information technology services are created, delivered, accessed, and managed. Cloud computing is bringing a new wave of innovation, and enabling tasks formerly carried out by well-rounded computers and servers to be performed on a pocket device such as a smartphone. According to Perry et al. (2009), this new service delivery paradigm has the potential to become one of the most transformative developments in the history of computing, following the footsteps of mainframes, minicomputers, PCs (Personal Computers), and smart phones.

Cloud-based document and photo sharing, calendar and address book synchronization, image and word processors are scalable, platform-independent, and accessible from anywhere on demand. Cloud computing benefits also include