# Chapter 6
# Security Architecture and Forensic Awareness in Virtualized Environments

**Diane Barrett**
*American Military University, USA*

## ABSTRACT

*Just about every technology magazine and article published today mentions virtualization or cloud computing. Technically, the two are different but very much intertwined. When environments use virtualization, there are artifacts an investigator can request that may provide valuable information. The content of this chapter explores the virtualization process, types of virtualized environments, and the part virtualization plays in cloud computing. A section will be included that presents case scenarios to demonstrate the type of evidence gathered in each environment for forensic investigations. A final section will include recommendations for additional areas of research in the area of investigating environments containing virtualization integration with cloud environments.*

## INTRODUCTION

With more emphasis placed on going green and power becoming more expensive, virtualization offers cost benefits by decreasing the number of physical machines required within an environment. A virtualized environment offers reduced support by making testing and maintenance easier. On the client side, the ability to run multiple operating environments allows a machine to support applications and services for an operating environment other than the primary environment (Barrett, 2010). Since most organization look to maximize machine utilization while reducing administrative costs, virtualization decreases upgrade costs and allows more uniformity in desktop environments.

In the third quarter of 2011, roughly 40% of all servers were virtualized with 80% of surveyed organizations planning to increase virtualization in the next year (Veeam, 2011). According to Gartner, the global desktop virtualization market will reach 65.7 billion unit sales, equivalent to about 40% of the worldwide business desktop market, in 2013 (Gartner, 2011). At the 2011 Gartner

DOI: 10.4018/978-1-4666-2662-1.ch006

Symposium IT/Expo, managing vice president and infrastructure teams, chief of research, David Cappuccio, said that virtualization would ultimately drive more companies to treat IT like a business. Virtualization is a critical component in increasing density and vertically scaling data centers. When utilized properly, average server performance can reach 40% to 50%, yielding huge benefits in floor space and energy savings (Cooney, 2012). 4- and 8-core processors are common in regular systems, with 16 and 32 core processors common in higher end systems. This provides a very conducive environment for virtualization.

According to Gartner, in 2011 more than 20 percent of organizations began storing customer-sensitive data in hybrid architecture and by 2016, more than 50 percent of Global 1000 companies will have stored customer-sensitive data in the public cloud (Gartner, 2011). The venture into virtualization has encouraged the use of this technology to extend as far as mobile devices. Estimates are that in 2012, more than half of all new smartphones shipped will include virtualization support. One such example is VMware's Horizon Mobile. An installed guest operating system in a virtual machine keeps the users work and personal environments, applications, and data isolated. LG and Samsung have both agreed to build phones containing VMware's mobile hypervisor. In late 2011, Verizon entered into an agreement with VMware to sell the virtualized Android smartphones. The phones, expected to hit the market shortly, include a virtualized SIM (Higgenbotham, 2011).

These predictions along with the fast pace as which technology is moving, means encountering a virtualized environment during a forensic investigation will become the norm as opposed to the exception. The relationship between virtualization and cloud computing is a complex one. Not all virtualized environments are cloud environments but generally cloud computing includes virtualized components. Virtualized components include everything from servers to routers.

Technological advances in virtualization, cloud computing and portable desktop environments leave very little trace on the host system. Locating pertinent evidence is no longer as simple as examining the local hard drive. Often the investigator finds only small traces of evidence on the host machine, provided the investigator knows how to recognize virtualization products. Virtualization, in-memory computing, and cloud computing will all affect the current forensics investigative processes, forcing the community to produce new methods and procedures for investigations in this type of environment.

There is not a lot of literature published on examining virtual environments. The first published text to address the examination of virtualized environments is Barrett and Kipper's (2010) Virtualization and Forensics. While the book does not go into detail about the examination of more complex environments, it does provide a forensic investigator with basic information needed to recognize various environments and the associated files.

Fiterman and Durick (2010) delved into the examination of ESXi environments by co-authoring an article published in Digital Forensics Magazine titled 'Ghost in the Machine.' In addition to the article, Durick maintains a blog where he posts additional virtual machine examination research. Bares (2009) presented a paper at the IEEE International Conference on Security and Intelligence Informatics that explored how the physical memory of a machine is actually allocated in the use of virtual machines.

To emphasize the issue with lack of research in this area, Haletky (2009) observed that despite the increasing number of critical applications and secure data on virtual infrastructures, few forensics tools exist to be sure a VM is locked down, or find out why it wasn't once it's been compromised. Although there is some published research on the examination of virtual environments, a need exists for conducting more research especially in more complex environments. Peppered throughout the