**Forensic Analysis in Virtualization by Erfan Setork**

When analyzing such a complex topic like forensic analysis in a virtualized environment, you have to truly understand virtualization and computer forensic concepts to the core. According to Bologna and Lindquist (*Fraud Auditing and Forensic Accounting: New Tools and Technique*, John Wiley & Sons Inc., 1995), the term *forensic* means "belonging to, used in, or suitable to courts of judicature or to public discussion and debate" (Hoopes, 2009). The process of examining computer crime can be a very complex and intricate study. An important notion in computer forensics is that the evidence must be preserved. A significant practice in forensics includes making an image of all the media from a computer by copying all the data carefully without modifying the integrity of the disks data space. All the work that has been done in the investigation will then use all the forensic analysis data captured, and try to solve the case with this evidence. Virtual machines play a huge role in forensics because it allows a user to create multiple environments and provides a simulation of the original hardware. Each virtual machine ultimately performs like an independent computer with its own OS and hardware. Virtualization is an old concept that was first introduced in the 1960s in mainframes, and now its usage has increased drastically with the development of technology.

Kruse and Heiser, authors of *Computer Forensics. Incident Response Essentials*, 2001, defined computer forensics as the "coherent application of methodical investigatory techniques to solve crime cases" (Hoopes 2009). Today computer forensics is an important tool for solving crimes committed, as well as for solving crimes against people where evidence may reside on a computer (Garfinkel 2010). Where does virtualization come in to play when we talk about computer forensics? The days prior to virtualization, the way an investigation was approached was the evidence would be cloned and then put into new hardware to be booted up. Even with
that process, the investigator wasn’t guaranteed a good copy of the cloned media. This old process would cause problems for the investigators because the only option they had was to recopy the “good copy” and this would end up being a very time consuming method. The defense attorney would challenge this because all they have to prove is the potential for the data being lost, not the integrity of the clone being lost. Steve Mancini, a security professional with extensive forensic experience for Intel, says the investigator should be able to hand another investigator a copy of the image and a copy of his notes and the second investigation should lead to the same empirical results that the same assertions that were originally made about that image (Hoopes, 2009). Virtualization is a great alternative to this hard copy and booting into media because it’s ideal for working on a copy of a hard drive without the potential of altering the data. With the use of a virtual machine, the contents will be viewed in the same context as the suspect views.

“Virtualized environments can make forensic research a tough job, since this technique is widely used in companies and even nowadays integrated in operating systems, it’s a matter of time when you would face this in of your investigations” (Beek 2009). Virtualization is a tool used in forensic examination and it can be a huge advantage in an investigation. The way data is acquired sometimes occurs without fully knowing the virtual environment and what we can expect from this data. An important thing to consider would be who the data belongs to and where the location of this data is. Learning how virtual environments work is another essential element because it will provide us the knowledge of knowing what type of interesting files we are looking for in the investigation phase. Acquiring the complete hard disk is not always a guaranteed process because of things like RAID configurations and multiple data owners on the same disk. (Beek, 2009). The process of forensic sound collection of data includes the
accumulation of a bit by bit replica of a disk image using a disk duplicator or network disk duplication utility. An image of the memory is a very helpful utility in an investigation but it requires a more time consuming method of potentially freezing memory before disposing power from the host to be duplicated. “The conventional computer forensics process comprises a number of steps and it can be broadly encapsulated in four key phases: access, acquire, analyze, and report” (Bern, 2007). These methods still haven’t been proven forensically sound so there is still a lot of development coming in the future within this field.

Virtualization technology offers many advantages in the field of digital forensics because it provides investigators the capability to produce higher quality forensics in a shorter amount of time. Refreshing an image to ensure integrity isn’t a stressful method anymore because of the help tools used in today forensics. Virtualization allows us to observe the suspect’s data without worrying the data would be altered or contaminated. This makes virtualization a desirable method for forensics but it also provides more advantages like the aptitude to analyze traps and time bombs left by the suspect without affecting the evidence. You can plan for digital forensics from the start and ensure your cloud provider has the necessary tools in place and active for current state of the art perspectives” (Virtualization Forensics, 2010). A forensic investigator needs the proper tools to proceed with their work in an ideal environment which will result in an original and more systematic plan. They don’t have the essential tools to support their original plans so that causes an alternative to be created. Digital forensics needs to incorporate the modern technology by accounting for virtual and cloud environments so the future of forensics can be headed towards a potential advancement.
Works Cited


from University of Western Sydney, Australia website:
http://www.utica.edu/academic/institutes/ecii/publications/articles/1C349F35-C73B-DB8A-926F9F46623A1842.pdf

from Digital Investigation website:


The Virtualization Practice website:
http://www.virtualizationpractice.com/blog/virtualization-forensics-how-different-is-it-5126/