Live System Forensics

By: Tim Fernalld & Colby Lahaie

Patrick Leahy Center for Digital Investigation

Champlain College

2/22/12

Contents

1 Introduction

1.1 Research Statement

Many first responders and other forensic investigators are not able to view or search a computer on scene because there is little time, it might alter/change the state of the data on the computer, or the computer is off. We are aiming to create an environment where the forensic investigators are able to view the computer live, when they are off the scene and at the lab.

1.2 Field of Research

The field of research that this project falls under is live system investigation. We are researching how Live View works and how it will benefit a forensic investigator during an investigation. When conducting an investigation live, it is easier for the investigator to view the computer in its live environment because they are able to see everything that the suspect has or was doing on his/her computer. With this software, the data or md5 hash of the computer will not be affected or altered because it takes the image and creates a live virtual environment.

1.3 Research Questions

Rather than individuals questions, we are trying to answer what operating systems will run within live view and what evidence volatile and not that live view contains that may be used as evidence.

1.4 Contributions

The results from our research will contribute to the existing knowledgebase on live analysis as well as provide examiners a resource when performing live analysis of a machine.

1.5 Report Overview

The challenge is getting the live system, which was not properly shutdown, to boot so the examiner can do live analysis. We are doing baseline testing on Windows XP, Vista, 7, Server 08 with no applications/database systems installed. After we successfully completed the baseline with some of the operating systems, we added services/applications that might cause issues (database, web, etc). We will be using Live View to conduct our live analysis.

2 Overarching Methodologies

2.1 VMware

VMware is a program that allows you to create and view a virtual machine of any operating system and any size. VMware allows you to essentially use multiple operating systems on your computer without having to install the additional operating system. You are able to switch between your computer's operating system and the virtual machine. The reason why we used VMware was because we needed to create multiple virtual machines of different operating systems.

We created a virtual machine of the Windows Server 2008, Windows XP Pro, Windows Vista, and Windows 7 Operating Systems. We specifically chose these operating systems because they are the most commonly used by users and are most likely going to be found in the field when conducting an investigation.

2.2 FTK Imager Lite

FTK Imager and FTK Imager Lite allow you to create a forensic image, or an exact copy, of a hard drive, virtual or physical. We specifically chose FTK Imager Lite because it is smaller and portable. Once the image is created, you are able to view everything, files/folders/software, that is installed on the hard drive in FTK Imager. It also allows you to create multiple image types, such as raw (dd) or E01.

The reason why we used FTK Imager was because it is easier to use and it allows you to create a raw (dd) image file, which is the only image file type that Live View can open.

2.3 Live View

Live View creates a VMware virtual machine out of a raw (.dd, .001) disk image or physical disk that allows the investigator to open the forensic image and view the image live. The forensic investigator gains an interactive, graphical user interface of the environment. An image is like a snapshot and when it is open in Live View, the investigator can change and alter the data, but once the VMware virtual machine of the image is closed and then opened again, it goes back to its original state and leaves the data/image unaltered. This is a very useful tool because it is forensically sound and it allows the investigator to conduct a live investigation after they have left the crime scene.

3 Data Collection

When creating the virtual machines, we created 4 different images of each operating system; the Base Image, Image A, Image B, and Image C. To do this, we used FTK Imager Lite. The first image that we created was the base image. This image was the fresh version of the operating system as if someone had just installed the OS or obtained a new computer. It only has the basic, preinstalled software and updates and FTK Imager Lite, to image the virtual machine. We then added Firefox and iTunes to the virtual machine and then imaged it and called it Image A. We then installed Dropbox to the virtual machine and imaged it and called it Image B. We finally installed Ad-Aware antivirus and Google Chrome to the virtual machine and created Image C. We also took a screenshot of the Windows Task Manager after each image to get a list of all of the running processes.

4 Analysis

We have concluded that Live View does and will work. After you image a hard drive, in raw (dd, .001) format, you can successfully open it in Live View and you will be able to view the system of the image live.

5 Further Work

When going to the Live View website, it says that there is limited support for Linux Distribution. When researching the supported Linux Distributions that work with Live View, we were not able to find anything that would tell us. We tried imaging some Linux distros, but either we had trouble installing VMware tools on the Linux virtual machine or the image would not open in Live View. We need to figure out which Linux distros will work in Live View or we need to find a similar software that will open the images and view them live.

6 Personal Opinions

Live View is a great tool for examiners to use when wanting to boot an image as a way to see exactly what a person may have been looking at on their machine. Research into live view has been heavily documented with what it supports and does not support which was one of the goals of this project. Once the system has been successfully booted in live view an examiner would follow the same examination process as a normal computer examination. Although live view is a great tool, traditional forensics techniques and examination processes through forensic software such as EnCase should still be applied in addition and not be substituted by Live View.

For more information on this and other projects visit
WWW.LCDI.CHAMPLAIN.EDU