Using Linux
VMware and SMART
to
Create a Virtual Computer
to
Recreate a Suspect's Computer

By:

Senior Special Agent Ernest Baca
United States Customs Service
Office of Investigations
Resident Agent in Charge
3010 North 2nd Street, Suite 201
Phoenix, Arizona
erniebaca@msn.com

Introduction:

Since beginning my endeavors with computer forensics, I have always wanted the ability to boot up a suspects computer just to see what the user saw when he was using the computer. So many times I have done computer forensic exams in which proprietary software is used. Simply looking at directory structures sometimes just doesn't cut it. Also, how many times did I make case agents go out and buy accounting software in order to run the target's data, not to mention figuring out which files to extract.

The old method of booting the target's machine consisted of cloning the target's drive with Safeback, then installing it into a sterile computer or the suspect's computer. I never liked the former method because of hardware issues and I never liked the latter because I like to touch the target machine as little as possible. All this hassle, not to mention I would still have to image the suspect's computer again in order to do my forensic examination.

Is there a solution? I have found a solution that simplifies and speeds up the process. I am utilizing Linux, VMware for Linux, and SMART. Just what is Linux, VMware for Linux, and SMART? Well, as you all know, Linux is an operating system. What few people realize is just how powerful this operating system is when it comes to computer forensic work. VMware for Linux is a software package that enables you to create a virtual computer within your Linux operating system. SMART is a graphical computer forensic tool written for the Linux operating system. Why SMART? You will see later in this paper when I discuss the imaging capabilities of SMART. These capabilities make it probably the best imaging tool I've seen to date, not to mention the computer forensic tools built in to SMART.

I will present a step-by-step procedure on how to create a virtual computer out of your suspect's machine and image your suspect's machine at the same time for forensic analysis. It's a system I call SMART Forensics.

Equipment:

Skytek Datasucker Computer (Computer Forensics Box)
PIII 750mhz
512MB, PC100 RAM

Dual Boot running Windows XP and SUSE Linux 8.0
(I know, not the hottest machine. What can I say, I work for the Government. It takes 4 years before I see an upgrade. But it does the trick.)

2 or 3 Hard Drives
Must be bigger than suspect's Hard Drive, 1 IDE mandatory.
I usually format one of the drives with the FAT32 file system which enables me to run my Windows based forensic tools on my Image.

Vmware Software for Linux -
Installed as per companies instructions.
Available at www.vmware.com .

SMART Software - Installed as per companies Instructions.
Available at www.asrdata.com .

Procedure:

1. Attach suspect's drive to computer as you normally would to image the drive for forensic processing. Also, attach your 2 or 3 evidence drives to the computer. I personally utilize 3 drives. The first drive will be my cloned drive. The second drive is a Linux formatted drive that I use to do Forensic processing in Linux. The third drive is a FAT32 drive that I use to create an image in 2gig chunks in order to run my Windows forensic tools. If I'm running low on hard drives, I scrap the Linux drive. I can still do Forensics in Linux utilizing the chunked image and SMART.
Note: It is very important that the cloned drive be an IDE drive. VMware will not work with a cloned SCSI or firewire drive.

2. Boot up the computer into Linux, log in as root and load KDE.
Note: You must be logged in as root in order for SMART to work. VMware also tends to work better when logged in as root. Also note that by default, Linux does not mount your suspect's drive on initial boot and therefore the file system and disk are not written to. This is one of the great things about Linux. You don't have to spend extra money for a hardware write blocker to boot into a GUI.

3. Start up SMART.

4. At this point, I personally like to do some initial interrogation of the suspect's hard drive. I utilize SMART to gain basic information about the device, partitions and what operating system(s) and file system(s) are present (if not already known).

5. Next, highlight the drive to be cloned and imaged. Now this is one of the awesome abilities that SMART has. You will now be able to Clone, create a chunked image and a raw image... all at one time (Can your software do that?). Just imagine the time I save by doing it all at once. It reduces my work by 3 days. This is one of the many advantages to this method. The old method required extra time, which in many cases I don't have. Once I highlight the drive, I right click on the drive to be cloned and imaged. Go to the "Acquire" option in the dropdown menu. You will notice it has two options: one for cloning and one for imaging. An option is given as to how many images you would like to create and how many drives you would like to clone to. I select one drive in the cloning section and 2 drives in the imaging section. You will notice tabs will appear for each image and each clone. Go to each tab and select a destination for each image and the clone. On one of the images, I set the option to split the image into 2 gig chunks. I usually choose "Ewcompress" as a compression option. This compression can be read by all the leading Windows forensic software packages. I usually compress my Linux image using the Gzip option. When I am more concerned with speed and not so concerned with hard drive space, I usually don't compress at all. This procedure is pretty straightforward in SMART and due to the GUI nature of SMART you should be able to figure it out. If I have the hard drive space I usually don't worry about compression. No compression speeds up the imaging time.

6. Next, I start the acquisition process and wait.

7. Once acquisition is finished, I power down the computer and disconnect my suspect's drive along with the two drives that contain the images. I preserve the suspects drive according to our evidence procedures and stow away the other 2 drives for later forensic analysis. I leave the cloned drive attached to the computer.

8. Next, I boot up the computer once again in to Linux, log in as root, and run KDE. At my office I have a Linux box with a removable drive bay and VMware installed that I use for Agents that want to sit at the suspect's virtual computer. In this case, I place the cloned drive in to the removable bay and boot up in to Linux.

9. Once Linux and KDE are running, load up the VMware software.

10. Once you're in Vmware, configure a new computer using the configuration wizard. This wizard will go through several steps. The steps are as follows:

a.) Welcome dialog: At this point just hit the next button.

b.) Select Configuration Type Dialog: Choose the *Create Standard Virtual Machine* option then choose the next button.

c.) Guest Operating System Dialog: Select the operating system that your suspect had on their computer. This is where the interrogating comes in handy. If I can't figure it out I usually just choose Windows XP. Once you have chosen your Operating system choose the next button.

d.) Virtual Machine Display Name Dialog: I usually change the default name to a name I will recognize. This helps if you're doing multiple cases and computers. You must also select a path for your virtual computer to run in. Usually the default path is fine. I sometimes change it for the sake of housekeeping. Once the path is selected, choose the next button.

e.) Disk Type Setting Dialog: Now this is the most important setting. This is where you point your virtual machine to use the cloned drive. At this point you choose the *Use Physical Disk* option. You will see a list of available IDE hard drives. Your cloned drive should be in that list. Choose the cloned drive then choose the next button.

f.) Disk permission setting Dialog: The defaults are always set to read only. I usually change everything but the MBR to read write access. That's right... the cloned drive will be read and written to. This is why it is important to do a parallel forensic examination with the images you took. Any files you may see on the virtual machine still need to be extracted forensically from the images and NOT THE VIRTUAL COMPUTER unless you just want a work copy. This method is not a forensic procedure. It is only used to assist the examiner or agent in getting an idea what to look for. Sort of like the saying, “a picture is worth a thousand words.”

g.) CDROM dialog: I keep it as is and choose the next button.

h.) Floppy Device Setting Dialog: I also keep this setting as is and choos the next button.

i.) Networking Setting Dialog: I usually set this setting to no networking. Once in a while I will set it to bridged networking if I want the virtual machine to access the Internet. In this case, I usually have my machine connected to a DSL line. Once finished choose the next button.

j.) Confirmation Dialog: Here choose the done button.

k.) Now your ready to start your virtual computer.

l.) Hit the power on button at the main dialog box and you've done it. At this point you should see a virtual computer pop up and load your suspect's computer.

m.) Let the operating system boot as normal. You will notice that the OS will find all sorts of new hardware like in the old days. Just let it try to install all the new hardware. It may even ask you to reboot. Go ahead and say yes to reboot. Once this process is complete, go to "Tools" on the VMware menu bar then install VMware tools. This will install the VMware drivers to your guest computer. Once installed, change your video settings and there you are, on your suspect's computer! The coolest thing I ever saw when I tried it for the first time!

Known Issues:

When restoring some laptops and some desktops to the VMware environment you may get an error warning. Go ahead and press "ok". If the computer boots, cool. If not, you will get an error message with a website link. This error message has to do with power management features that the suspects computer may have had. Go to that link and follow the instructions. Don't do this procedure on your machine as in the instructions. Do the procedure on the cloned drive and it should work.

Disclaimer:

This procedure has worked for the writer of this article on many occasions. The writer does not guarantee that it will work in every case. The world of computer forensics presents many different scenarios that cannot be guaranteed by this process. This is also a method that should only be utilized by experienced computer forensic examiners. The writer also takes no responsibility as to any damage that this procedure may cause. It is recommended that you have good backups of your computer before attempting this. The opinions of this author are his sole opinions. The author and the United States Customs Service are in no way associated with VMware, SUSE, or ASR Data. This paper is not an endorsement for those products.

Legalities:

All trademarks are the property of their respective owners.

About the Author:

The Author of this paper graduated from the University of Texas Pan American with a Bachelors of Science in Computer Science in 1989. My emphasis during my college studies was systems programming and data communications (Back in the days of the 2400 baud modem, the Internet was called Bitnet and consisted of only educational institutions and large corporations. Boy am I ancient) . Upon graduation I began my career in Federal Law Enforcement as a Criminal Investigator for the United States Marshals Service. In 1997, I transferred to the United States Customs Service as a Special Agent. I have been involved as a computer forensic examiner since the year 2000. I have just recently begun to relearn and apply my prior Unix knowledge to computer forensics. I hope this article helps out. If it did or you have any suggestions on revising this paper or new paper ideas, please send me an email or you can find me on the Linux Forensics listserv.