Booting up evidence E01 image using free tools (FTK Imager & Virtualbox)

Being able to boot an acquired evidence image (hard drive) is always helpful for forensic and investigation. If you would do a Google search, you would find most methods or discussions are referring to usage of Vmware Workstation. As Vmware Workstation is not free, not a good news if you are on low budget or do not have one at all.

Don't worry....I will show you how you could boot an acquired E01 image using freely available tools.

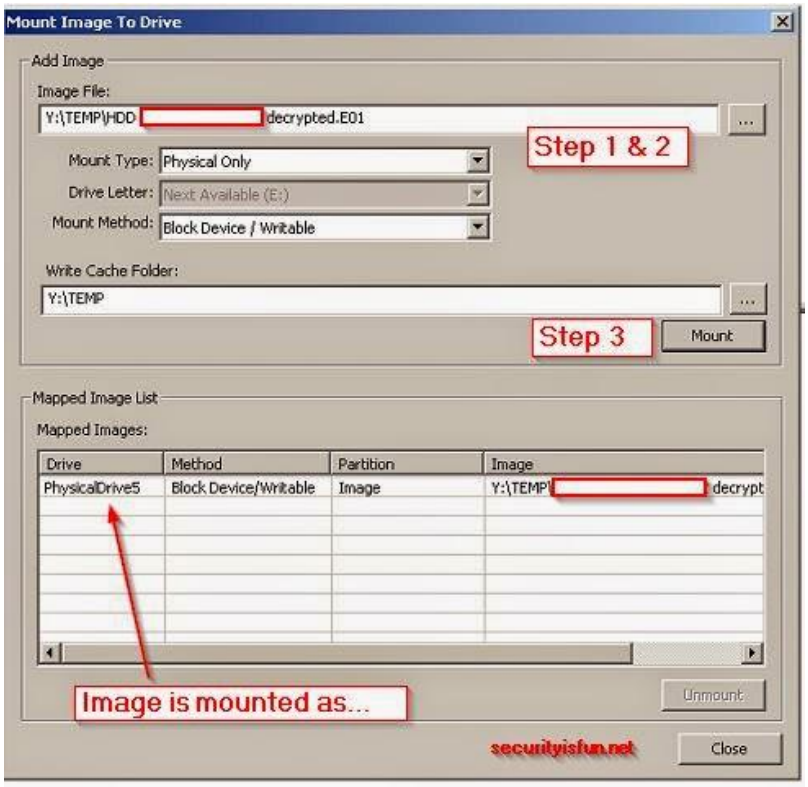
What you will need:
1. FTP Imager
2. Virtualbox and Virtualbox expansion pack-
3. Admin right (do not have one? You're joking right???)

I'm not going to detail down how you should install FTK and Virtualbox.... those are really easy.

Here are the steps:
1. Open FTK Imager. Go to File -> Image Mounting.

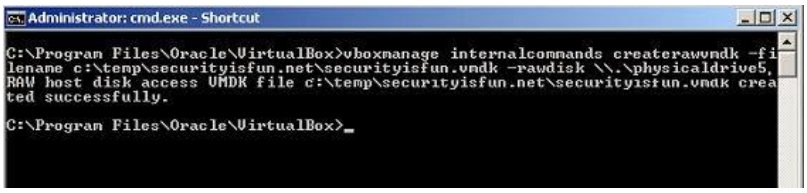
2. Select the E01 image you want to mount.
a) Mount Type: Physical Only
b) Mount Method: Block Device / Writeable (I know what you are thinking.... do not worry about tampering the evidence file. FTK Imager will create a cache file that will temporarily store all the "changes" you made)
c) Write Cache Folder: Take the default or point it to any folder that would make you happy :)

3. Click "Mount". You will see which physical drive the image is mapped to.



4. Create a new folder (for storing the virtual disk file later) e.g. c:\temp\securityisfun.net
5. Open a command prompt as administrator. Go to c:\Program Files\Oracle\VirtualBox. Run following command: **vboxmanage internalcommands createrawvmdk -filename*c:\temp\securityisfun.net\securityisfun.vmdk* -rawdisk \\.*physicaldrive5***

NOTE: Replace **the path**, **file name to be created** and **physical drive** as accordingly.



5. Run Virtualbox as administrator. Create a new virtual machine matching the OS of the image e.g. Windows XP or Windows 7.
a) RAM - set it to any amount you like. For me, normally I will set it to 2GB
b) Hard Drive - point it to the virtual disk file you just created in step 5 above

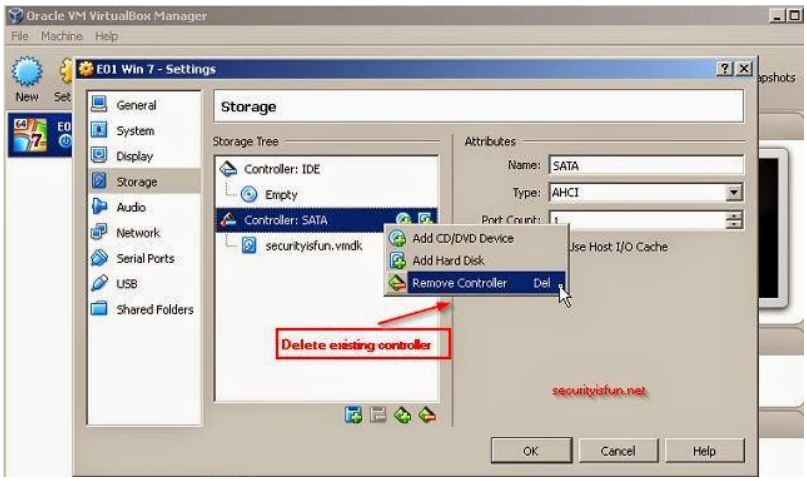
6. Well, start the virtual machine. It should run now.

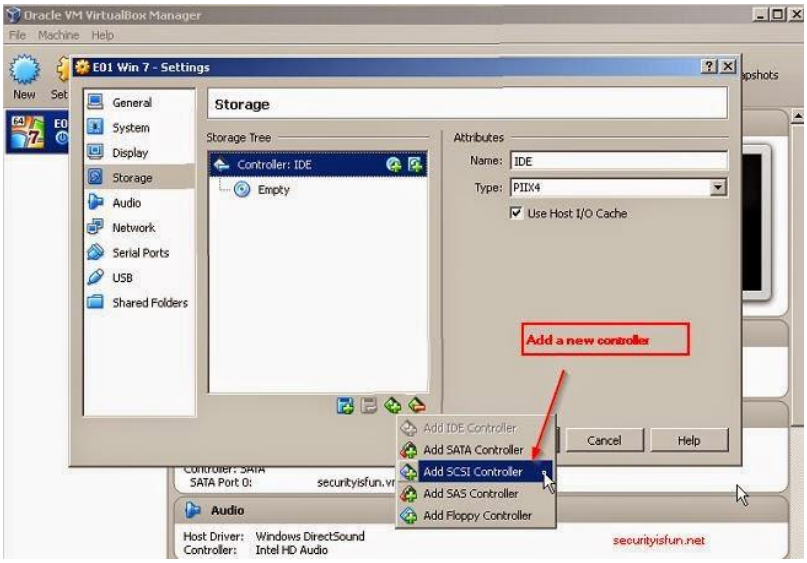
7. In case you get a blue screen.. which is not uncommon. Try changing the HDD controller type, which is IDE by default, to SATA, SCSI or SAS. You can change this by editing the settings of the virtual machine:

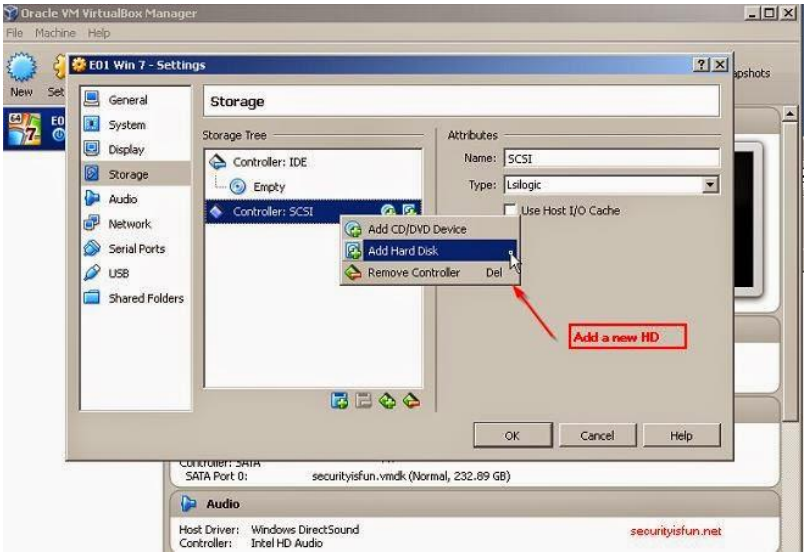
a) Delete the existing HDD controller

b) Add a new controller e.g. SATA

c) Add a new disk. Select "Choose an exiting disk". Point it to the virtual disk file you created (e.g. securityisfun.vmdk)







8. If you still get the blue screen... this might be due to Windows could not see the drive. Try following steps which involve editing the registry to enable SCSI and SAS drivers on boot:

a) Unmount the image you mounted with FTK Imager

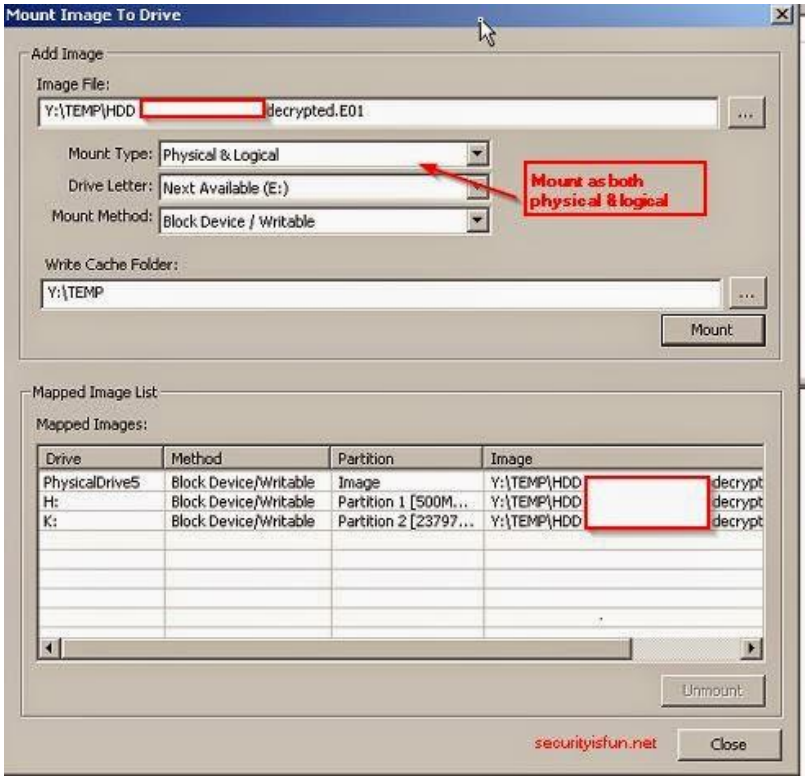
b) Mount the same image with FTK Imager but now with the option:

Mount Type: **Physical & Logical**

Drive Letter: Take the default

Mount Method: Block Device / Writable

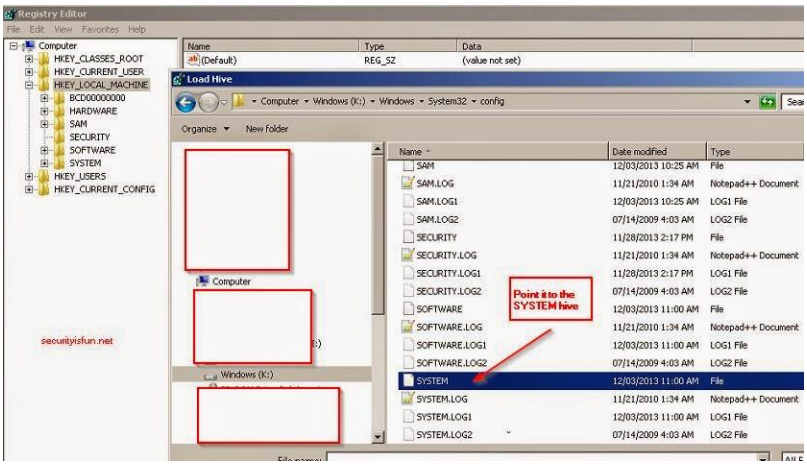
c) You should see the partitions of the image are now mounted and accessible



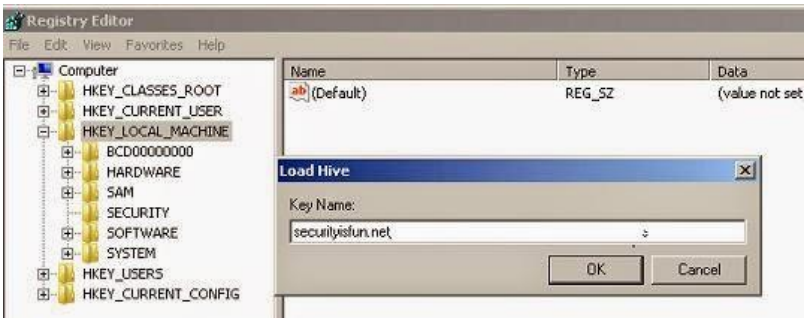
d) Run "regedit.exe" as administrator.

d) Expand "HKEY_Local_Machine".

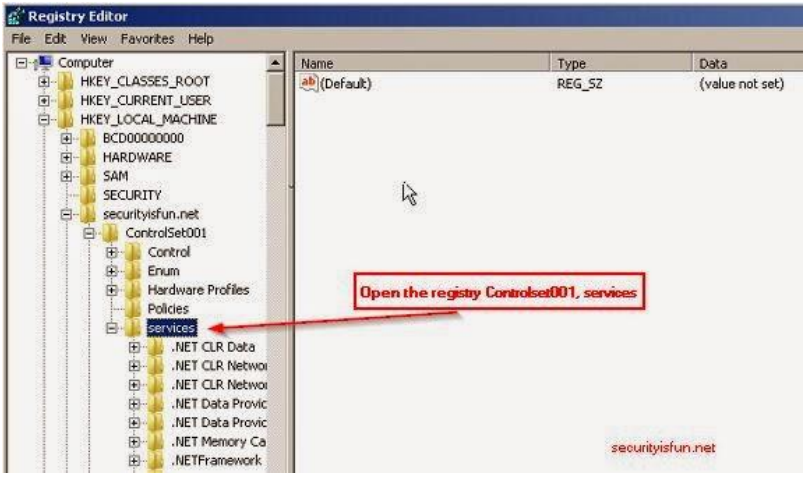
e) Select "Load Hive". Point it to the SYSTEM hive of the Windows partition of your mounted image. For example, if the image's Windows partition is mounted by FTK as K:, point it to K:\Windows\system32\config\SYSTEM



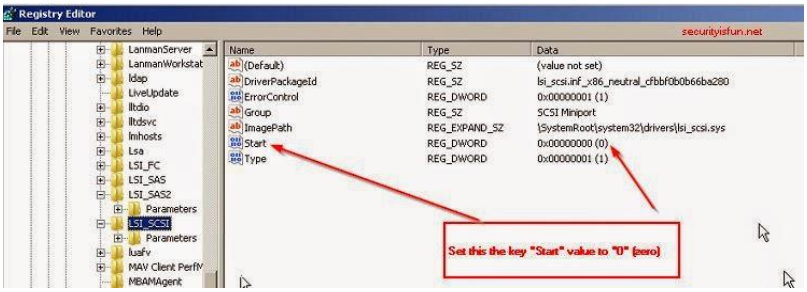
d) Enter any name when prompted e.g. securityisfun.net (sorry, a bit of marketing here :)). You should now see additional registry key with the name you typed appeared.



e) Navigate to securityisfun.net\ControlSet001\Services



f) Look for "LSI_SCSI". Click on it and set the key "Start" value to "0" (zero). Setting it to "0" means Windows will start/load this driver at boot time. Repeat the same for "LSI_SAS, LSI_SAS2".



g) Point to the "securityisfun.net" hive once you finish editing. Select "File, Unload Hive". Click "Yes". Close regedit.

h) Now try to boot your virtual machine again. Try using difference controllers e.g. SAS, SATA, SCSI if you still getting the blue screen.

9) If you are still getting the blue screen despite doing all this..... two words for you - bad luck! At this moment, I don't have any other solutions or workarounds. I will update this blog post if I (ever) come across something new :)

Have fun!

27/06/2014

KienEng Chan