

Dealing with PC Guardians Encryption Plus Hard Drive (EPHD)

By kevenmurphy

Dealing with EPHD, or PC Guardian's Encryption Plus is not too bad provided it has been setup correctly. By being setup correctly, I mean that the PC administrators have created an account that anyone can use to get past the hard drive encryption. This account and password needs to be treated just like the admin account. Only those people who need to know it, should have the userid and password.

On a side note: If your corporation has not implemented for your laptops and mobile devices, I have to ask why not? Hard drive encryption is much cheaper to implement then letting your corporate secrets and customer data out into the public.

Before We Begin

Before doing anything talk with your management and legal with regard to how they want you to proceed with imaging the encrypted devices. They may feel that this methodology is not right for them. The other aspect to be aware of is do you image the drive in its encrypted state and then use the technique below to get a decrypted image or do you do the reverse? Either way has caveats. Let's say the hard drive fails during the imaging. If you have imaged the encrypted drive in the encrypted state, the question is will it boot up so that you can decrypt it, or do you need to find another solution to decrypt what you have? As it stands there is not much you can do with an encrypted drive. If you imaged the drive using the method below and thus have a decrypted portion of the drive, will it be good enough for court? Will it have the evidence you are looking for?

For myself, I image the encrypted drive first. Then decrypt the hard drive.

Using LiveView

LiveView will create a VMWare machine from a dd image or physical disk drive hooked up to a read-only write blocker. This allows the forensics examiner to boot up the drive and see it from a user's point of view. The big plus to this is that you can make an image of the decrypted drive. The downside is that you effectively can change data on the VMWare version of the drive while making an image. For example, Windows will start installing drivers for the "new" devices it sees after it boots up for the first time. Secondly, anything you do on the machine will change data on the VMWare version of the drive.

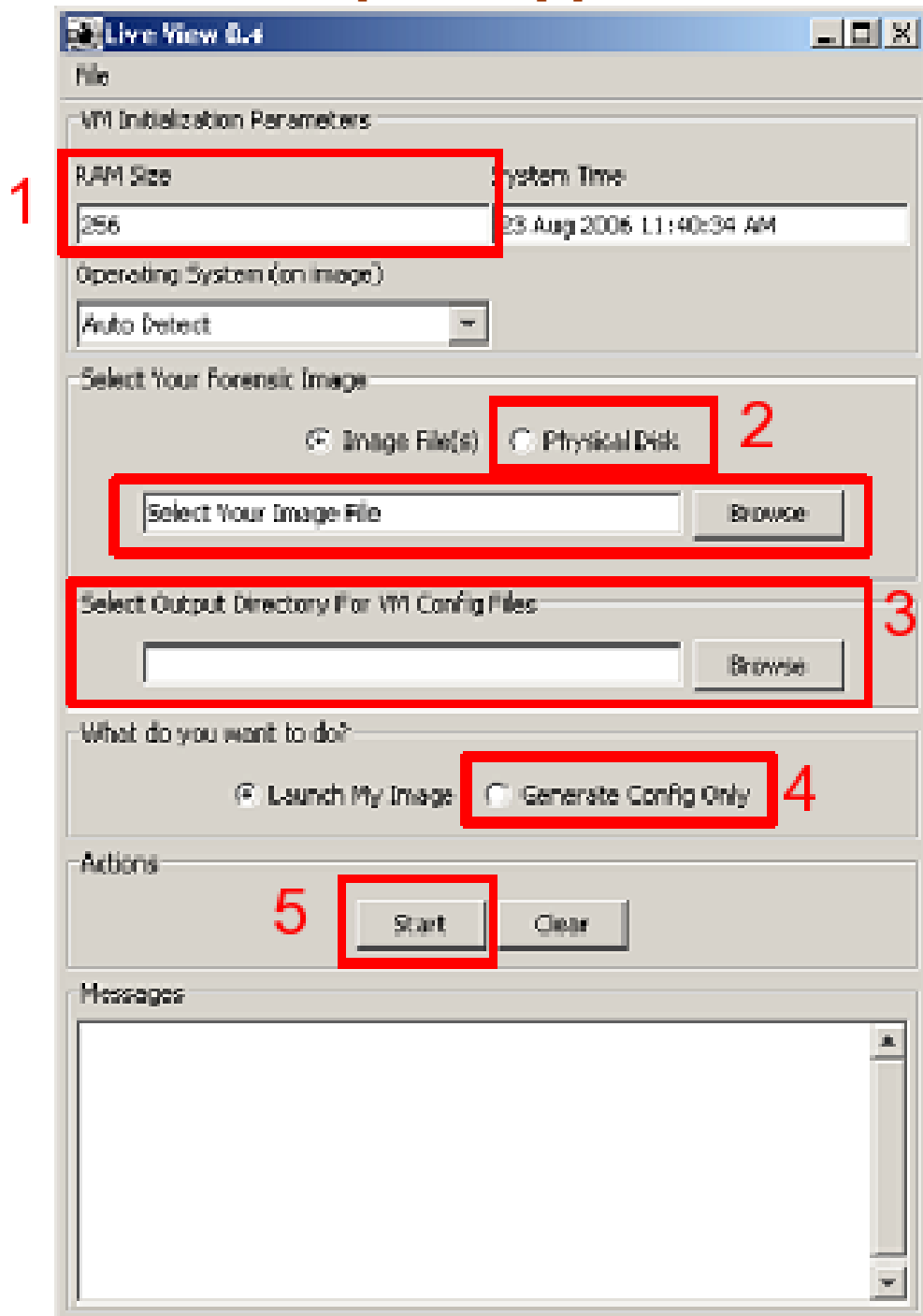
So why do it this way?

First, I have had issues getting the decrypter program that Guardian supplies to decrypt the drives to work correctly. Usually what happens is that I get a partial decryption. If I am using the original drive (a big forensic no-no), then I lost the data I need. Secondly, it takes an extremely long time to decrypt the drive. I have found that it saves some time by making a dd image of the original, then use the dd image and LiveView to get a decrypted version of the hard drive. The only thing left is to be able to explain any changes that occur while making the image.

Here is one way to configure LiveView:

Dealing with PC Guardians Encryption Plus Hard Drive (EPHD)

By kevenmurphy



1. Configure your RAM size to 512+ if you machine has it. This helps with the virtual machine speed. The more RAM it has the faster it will be to a point.

Dealing with PC Guardians Encryption Plus Hard Drive (EPHD)

By kevenmurphy

2. Select your dd image
3. Select your output directory.
4. Click on Generate Config Only to only generate the config and not autostart VMWare.
5. Lastly, click on the start button.

VMWare Configuration

Since I am using VMWare Server, I need to add in a network interface so that I can send the image through the VMWare network. To do this just bring up VMWare Server, then:

1. Click on Edit virtual machine settings
2. Click on the Add button and click on Next
3. Click on Ethernet Adapter and click on Next
4. Select Host-Only and click on Finish

You want to use Host-Only as you have no idea what kind of software will kick off when the machine boots. Doing it this way will contain any malware to just your physical box. Think of it this way, if the machine has malware on it that starts scanning the network upon starting up, it could take down network devices or worse yet start reporting what it finds to a third party. The key here is isolation. Plus for the truly paranoid, you can install tcpdump/snort on your physical machine and monitor that while you create your images.

Imaging

Once the virtual machine is up and your logged in as an Administrator, you can start imaging the hard drive. There is a variety of methods to doing this. Since I am using VMware Server here is one of the methods I use:

Physical Machine

On the physical machine bring up a DOS window and change directory into the where you want to save the image.

Execute:

```
nc -l -p {port} | dcf1dd of={image file} hash=sha512,md5 hashwindow=512  
sha512log={image file}.sha512 md5log={image}.md5 status=on
```

Virtual Machine

On the virtual machine, I use either a mounted ISO or CD-ROM with Helix on it and bring up a DOS window.

In the DOS window (assuming D: is the CD-ROM drive):

Dealing with PC Guardians Encryption Plus Hard Drive (EPHD)

By kevenmurphy

```
d:\IR\Cygwin\dcflddd if=\\.C: hash=md5 hashwindow=0 bs=512  
conv=noerror,notrunc,sync status=on | d:\IR\Cygwin\nc.exe -w30 {IP address of  
physical machine} {port}
```

Now it just a matter of waiting for the imaging process to complete. I usually screen lock the physical machine and come back the next day to check on it as I have a slow imaging machine. The time it takes to image this way really depends on the equipment you are using. For example, there have been times where the drive I am imaging is connected via a USB write-blocker and the drive I am saving the image to is USB. In that case it may take 12+ hours to do a 40 gig drive. I have found that saving the image off to a network drive via netcat/samba share to be faster than USB/Firewire.

Once the imaging is done, I take a screenshot of the VMWare session as the MD5 hash is shown in the DOS window and save it with the image. Then I compare the MD5hash from the screenshot with the MD5 hash from the image. The hashes should match.

Good luck. I know it is a slow process to decrypt the drive, but I have had good success with it.