# Image Restoration

CSC 485/585

1

## Objectives

- Understand the situations in which an examiner may need to restore a forensic image.
- Understand the variety of options available for restoring and booting the image of a hard drive.
- Be able to successfully restore and boot a forensic image of a seized hard drive.

2

## Why restore?

- Traditional CF tools are used for searching, viewing, extracting and reporting of standard file types and many forensic artifacts.
- But what about…
  1. "non-standard" file types from proprietary software that only display in it's native software application
  2. data that can not be understood without, or is better understood in, it's native environment or device
  3. for jury presentation, when "a picture is worth a thousand words"
  4. when you need a clone of the original seized drive

Let's look at each of the above in more detail…

3

## "Non-standard" file types

When a data file can only be opened, viewed, printed, etc. in the native application that created the data file, you have a limited number of options:

1. Purchase the software application, extract the files from your forensic image and load them into your copy of the software.
2. Contact the software vendor and obtain a "loaner" copy of the software, extract the files from your forensic image and load them into your copy of the software.
3. For some applications, you may be able to extract the C:\Program Files\application\ folder for the specific software program, to your forensic workstation and run the software. Without a complete software install, any application requiring registry entries and shared .dll and other files will not run.
4. Restore the forensic image of the seized HD containing the proprietary software and run the seized copy of the software.

4

## Native environment needed

- There are hundreds of "embedded" devices designed for anything from game consoles, to point-of-sale cash registers, to video surveillance systems, and any other type of custom computing purpose.
- Many of these employ operating system that do not run on standard Intel-based PCs (or virtualization software) and store data on file systems that your forensic tools do not know how to read and parse.
- The only method of analysis may be to run the original hardware system and manually browse through the data stored within, using the OS of the device……but this is done with a restored copy of the HD (i.e. a clone) in place of the original HD, so you are not modifying original evidence when performing this type of "live" analysis.

5

## Xbox 360


- Social Networking
- Photos/Videos/Music
- Internet Browser History
- Peer-to-Peer
- Movie Rentals
- File Storage & more…

6


## CCTV Systems

NAS Devices
& many other
proprietary systems

7

## Native environment needed - cont.

- You may just need to run a software or system you are not familiar with, to study it's behavior or see what remnants it leaves behind.
- External scanning (for network traffic, anti-virus, malware, etc.) of a restored Virtual Machine copy of a subject's computer can be used to debunk the "Trojan Defense."
- Restorations of multiple computers and/or servers allow you to run client/server network applications in a virtual restoration of a seized network.

8

## Jury presentation

Which of the following slides would be the easiest for the 70 year old grandmother sitting on the jury to understand and watch you demonstrate and explain?

- Complex Forensic Reports showing deconstructed .lnk and .url files from c:\Users\%username%\Favorites?

or

- A running duplicate of the Subject's computer showing the subject's "Favorites" list in Internet Explorer?

9

## HD clones

1. You need to make a clone of one or more HDs to place the clone(s) back in the seized computer/device, while you seize the original HD(s).
2. You already made an image of the original and then did "live" analysis of the computer…..time to restore the computer back to it's original state.
3. Defense wants cloned drives instead of .e01 forensic images

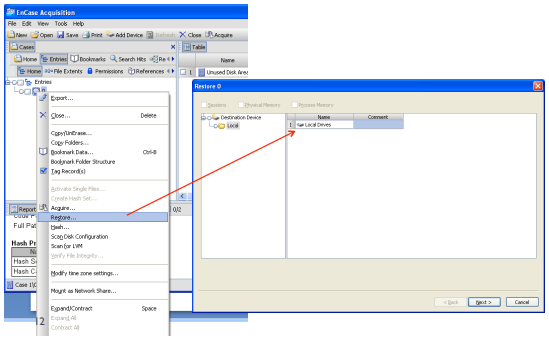
10

## How do we restore?

- This depends on what you are starting with.
  - .e01 image
  - .dd image (Raw Bit Stream = RBS)
  - Physical drive
- When working with an .e01 forensic image, you will typically restore using EnCase.
  - Some 3rd-party tools can also restore an .e01 image.
- When restoring a RBS image, you will typically use Linux "dd" to restore the image.
- When restoring from a physical drive to another physical drive (a.k.a. cloning) and can use EnCase, Linux "dd", a forensic drive duplicator, and other 3rd-party tools.

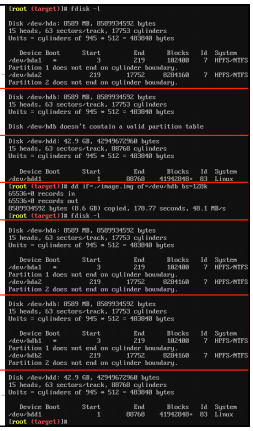
11

## Restoring or Cloning with EnCase



## Restoring with Linux "dd"

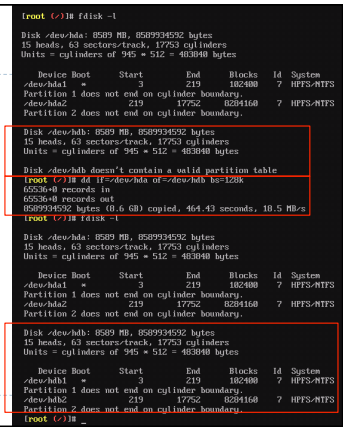
1.
2.
3.



13

## Cloning with Linux "dd"

1.
2.
3.



14

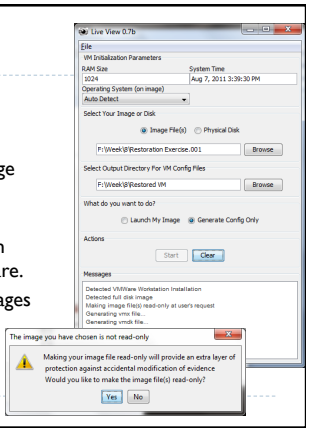
## Restoring and booting

- In many cases, the reason you will be restoring a forensic image is for the purpose of booting the OS contained on the original seized HD.
- This restoration may be to write out the data onto a physical disk or a virtual disk for use in VMWare or other virtualization software.
- VMWare has the ability to utilize a physical disk, virtual disk, or a raw (i.e. "dd") image of a disk within a virtual machine.
  - This means that if you have a "dd" image of a seized HD, you can utilize tools to boot the image in a read-only state as if the image were an actual hard drive, without needing to restore it.
  - If your forensic image is an .e01 or other non-raw format, you may be able to use 3rd-party tools such as Mount Image Pro or Physical Disk Emulator to mount the image file and present it to your forensic machine as a physical disk, which VMWare can then boot from.

15

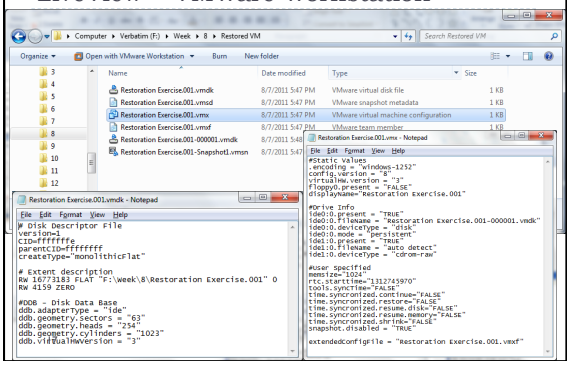
## LiveView

- Will create VMWare configuration files for booting the selected image or physical disk.
- Helps with some disk geometry issues common with restores into VMWare.
- Only works with RBS images or Physical Disks.

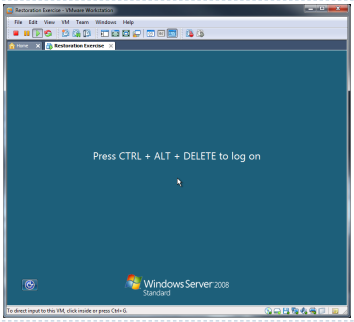



16

## LiveView > VMWare Workstation



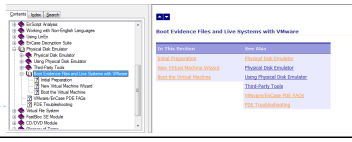
## LiveView > VMWare Workstation




18

## .e01 > Disk Emulation > VMWare

- Using some 3rd party tools, you may be able to mount your .e01 forensic image, emulate the image as a disk and boot with VMWare.
- Physical Disk Emulator – add-on module for EnCase.
  - LiveView used to create VM from PDE emulated disk.
  - Detailed explanation of PDE and booting with VMWare is available in EnCase help file.
- Mount Image Pro in conjunction with &VFC.

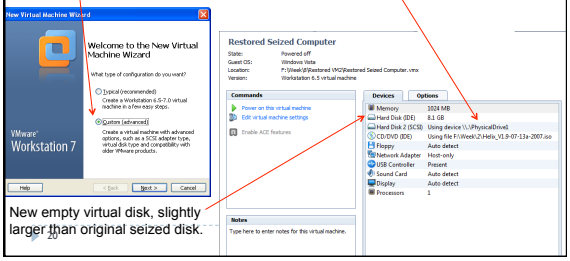


19

## VMWare Workstation (without LiveView)

Use the Wizard to configure a new Custom VM to contain the restored data and become a virtual replica of the subject's machine.

After the wizard, temporarily add a new physical hard disk, selecting the disk containing the images you wish to restore.

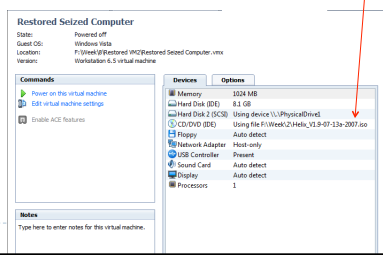



New empty virtual disk, slightly larger than original seized disk.

20

## VMWare Workstation (without LiveView)

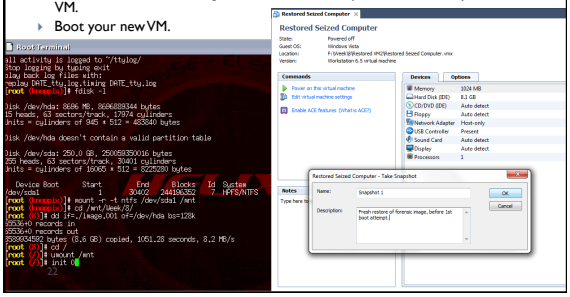
- To restore a "dd" image, boot your newly configured VM with your Linux CD (or .ISO) and perform your restoration with "dd."
- To restore an .e01 image, boot your VM with your SAFE CD and perform your restoration with EnCase (installed on a SAFE Tools Disk).




21

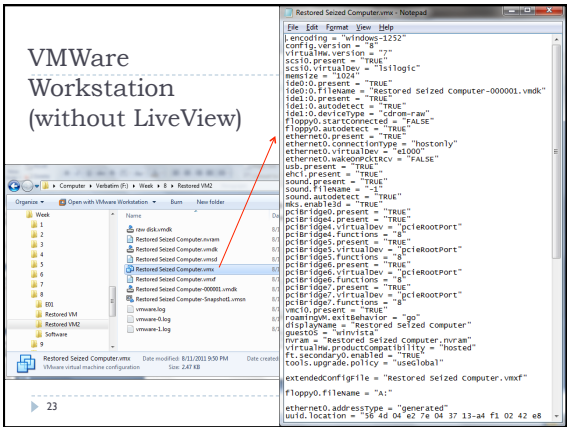
## VMWare Workstation (without LiveView)

- After restoring your image to the new virtual disk, shutdown, remove both your Boot CD and the physical disk containing the images you just used to restore from the VM configuration, and take a snapshot of the freshly restored VM.
- Boot your new VM.




22

## VMWare Workstation (without LiveView)




23

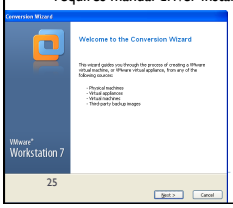
## Boot problems

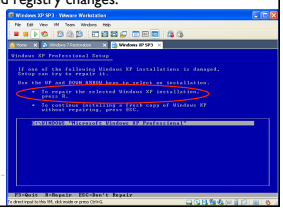
- Anytime you restore an OS that was installed configured for other hardware (physical or virtual) and try to boot it on dis-similar hardware (physical or virtual), you may experience boot problems.
  - Incompatible device drivers and HAL related settings & files.
  - Installed software apps that look for hardware that doesn't exist now.
  - Drive geometry problems going from physical to virtual HD.

24

## Boot problems

- LiveView handles the correction of some drive geometry issues.
- Built-in VMWare Conversion Wizard fixes some device driver and HAL issues.
- For Windows 2003, XP and earlier, a "Repair Installation" takes care of many boot problems. No "Repair Installation" option in Vista or later, requires manual driver installation and registry changes.



25

Questions ???

…as usual, use the discussion board!

26