Creating & Accessing Forensic Images

How to Access Multiple Image Types Using Various Forensic Techniques

e3Discovery
electronic evidence experts

Brett Shavers

Topics

- Forensic Image Creation Applications
- Forensic Image Types
- Accessing the Forensic Images
- Converting the Forensic Images into Different Forensic Image Types

Forensic Images

- Basically, a *forensic image* is an exact, bit for bit copy of an original electronic media. This includes all the deleted files also (unallocated/slack/free space).
- A *mirror image* is not the best way to describe a forensic image (do you look exactly the way you do in a mirror or is instead an opposite view of you?). A forensic image is an EXACT copy, not an opposite copy.

Forensic Images

- When you ask for an image, make sure you know what you are asking for.
- A Ghost image may not be a forensic image (unless you ask for a forensic Ghost image, and even then, it may not be)
- An image may not be a complete forensic image.
- A copy may not be a forensic image at all.
- Ask for a FORENSIC IMAGE. There is no mistake as to what that means. It's every single ONE and ZERO on the media.

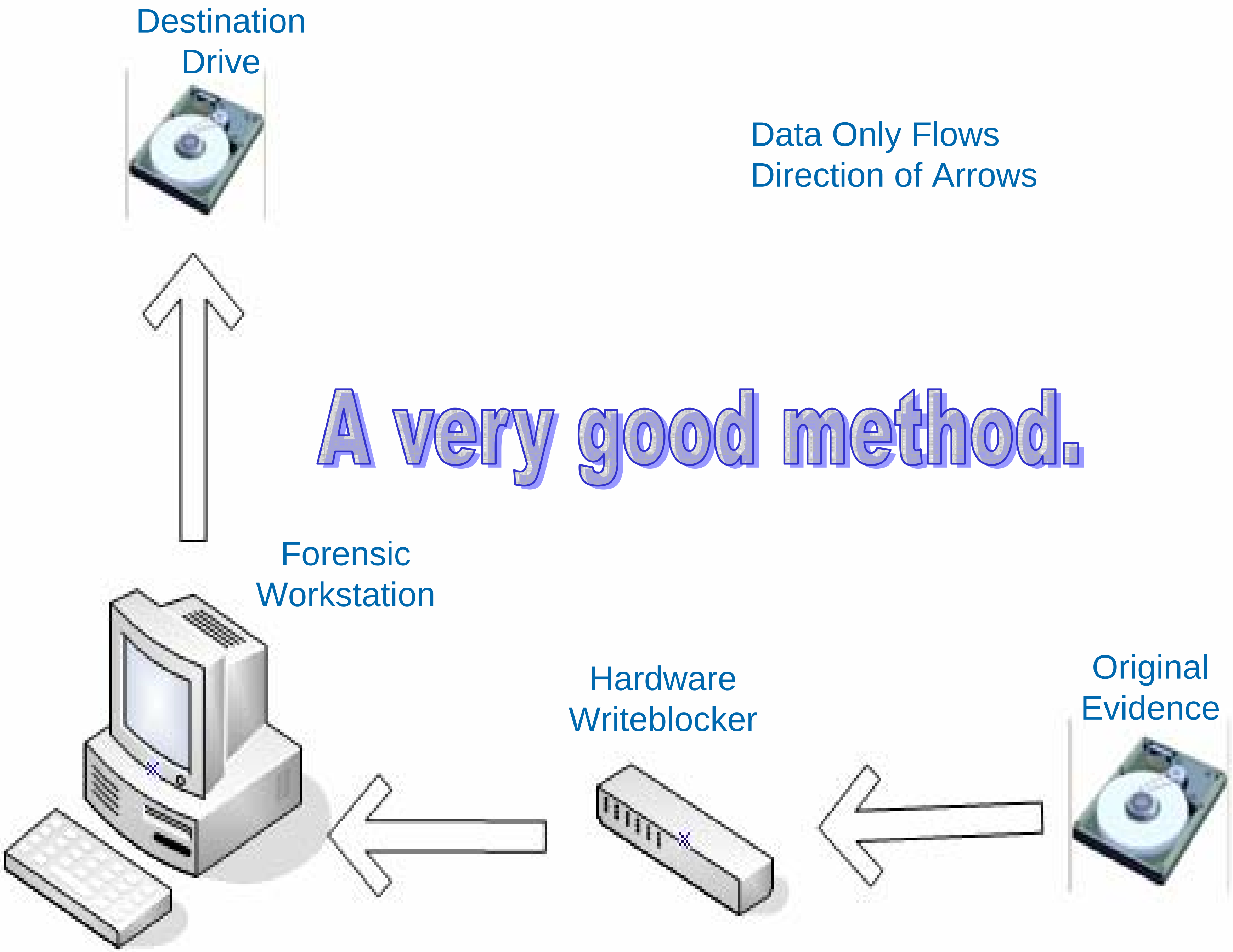
Purposes of Creating Forensic Images

Purposes of Creating Forensic Images

- Evidence preservation
- Working “copy” of the original to examine
- Multiple image copies for multiple examiners to decrease the amount of time to complete examinations.
- Prove/Disprove Allegations such as the “Trojan Defense” in virtual environments. Forensic images can be booted virtually and tests can be run on the running image.

Creating Images

1. **Ideal World Example:**
   - Write blocked evidence source (hardware or software)
   - Scrubbed/wiped destination drive
   - Forensic boot CD (DOS or Linux), forensic boot floppy (DOS), Linux OS, Windows OS, or Apple OS
2. **Non-ideal World Examples:**
   1. Using suspect machine
   2. Using Windows
   3. No hardware write blocker
   4. Using Software write blocker
   5. Using no write blockers at all



Destination Drive

Data Only Flows Direction of Arrows

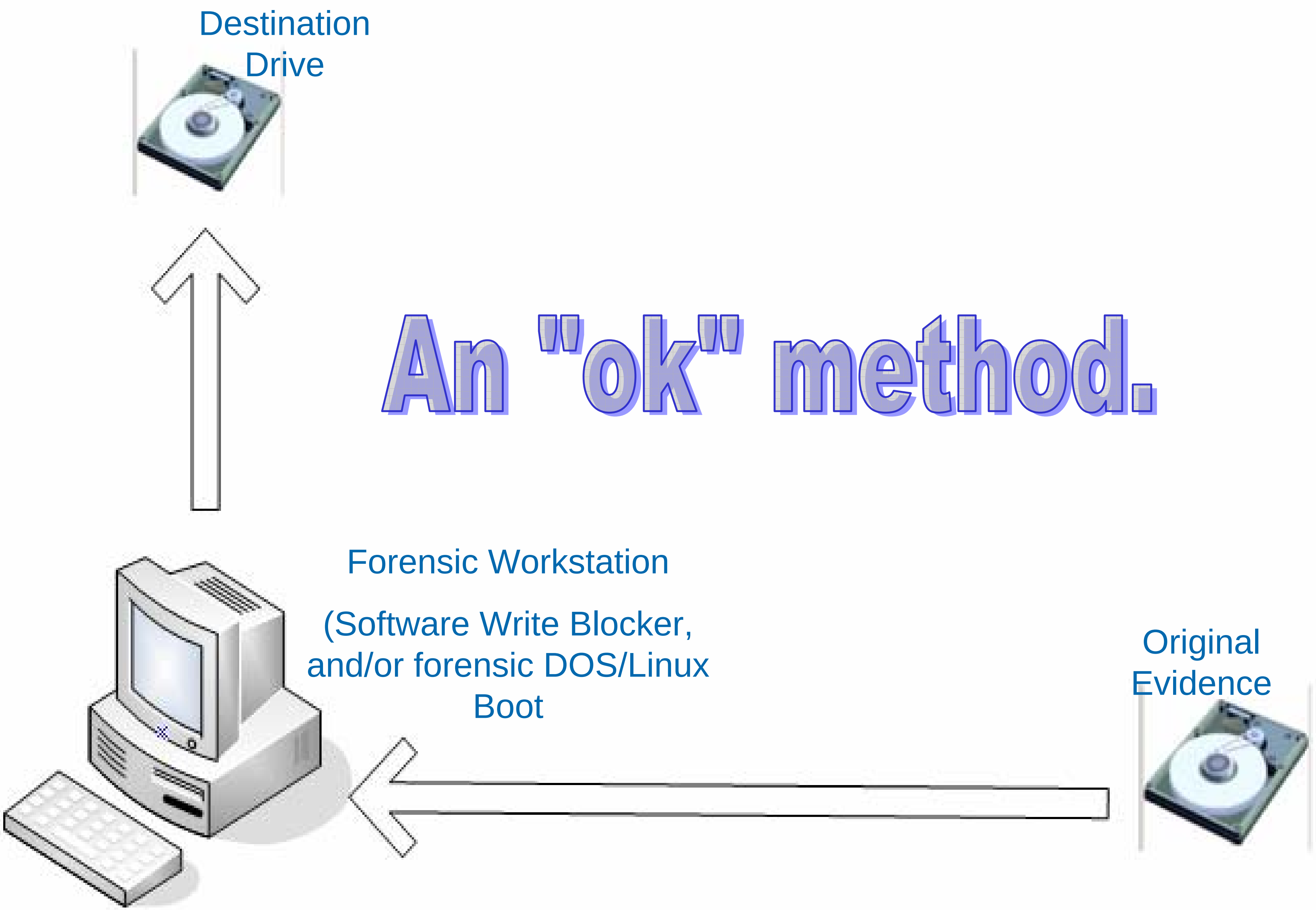
A very good method.

Forensic Workstation

Hardware Writeblocker

Original Evidence

An "ok" method.



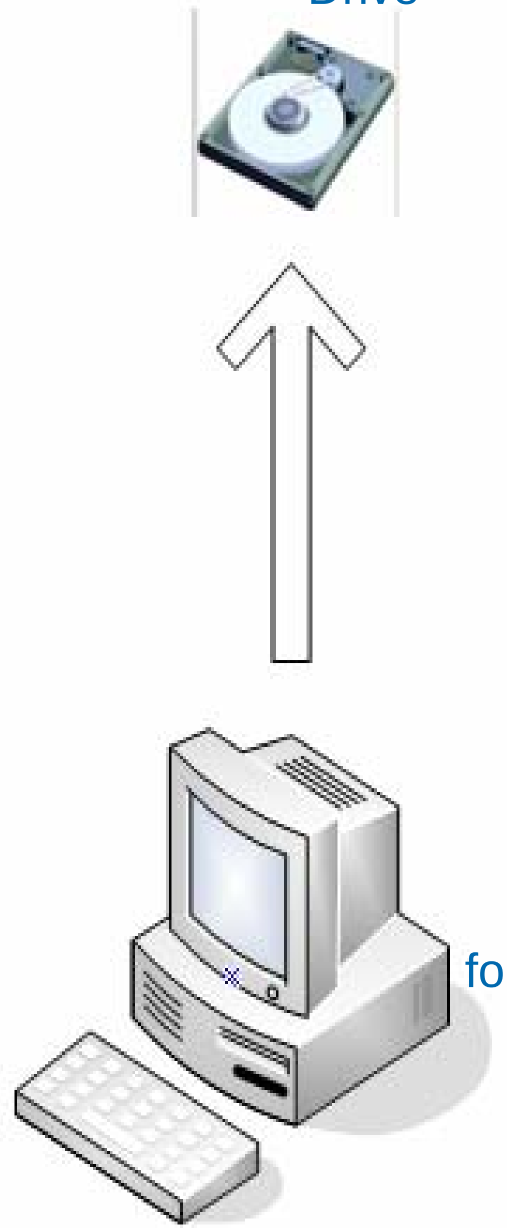
Destination Drive

Forensic Workstation

(Software Write Blocker, and/or forensic DOS/Linux Boot

Original Evidence

Destination
Drive

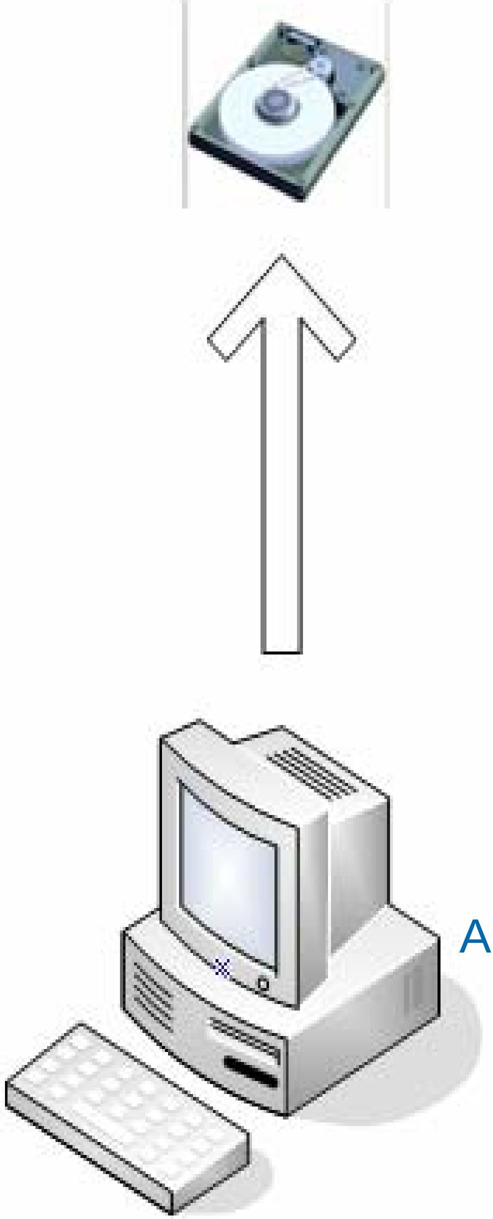


A risky method.

Suspect Machine

Software write blocker,
forensic boot with CD/Floppy
to DOS or Linux

Live Method.



Destination Drive

Suspect Machine

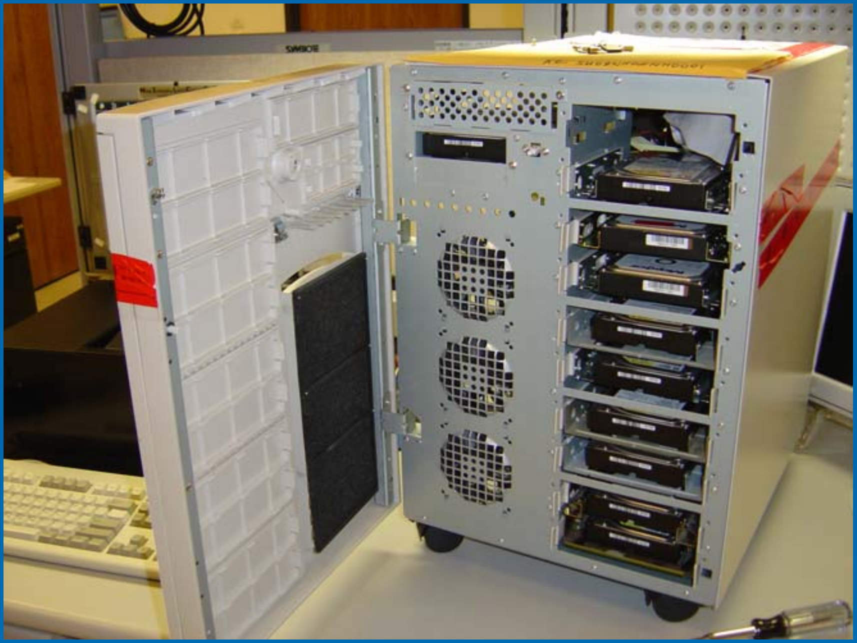
Acquisition tool running from operating system.

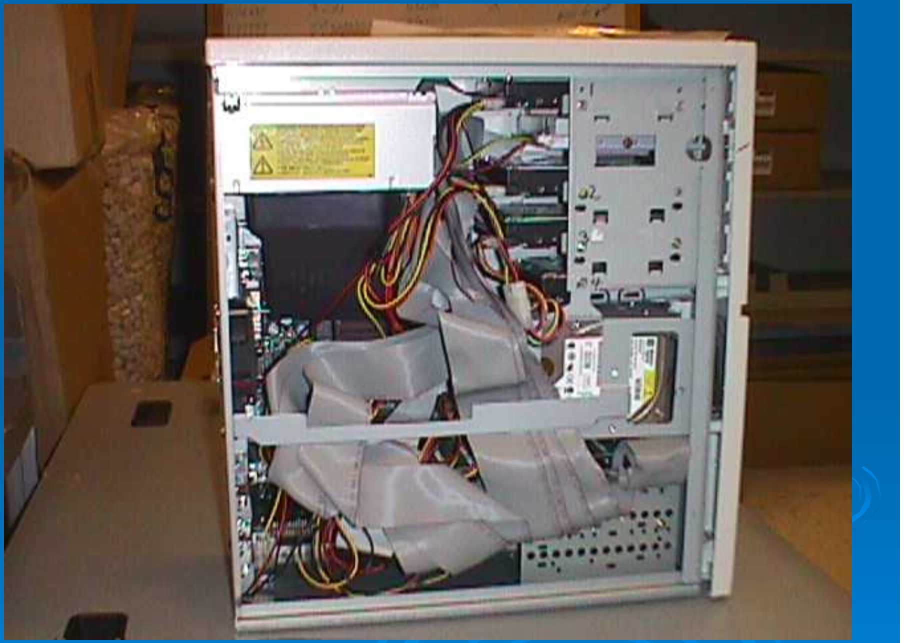
Types of Problems

Types of Problems

- RAIDs
- Whole Disk Encryption
- Vista BitLocker
- Apple computers
- Hard to remove hard drives
- Servers
- NETWORKS-Windows Server, Netware, Novell, Unix, Linux, and “I NEED A MOTRIN!

Normal on the Outside





Over a half dozen hard drives!!! Is it a RAID or not?
This is important as it can determine *how* to image.

Types of Image Formats

Types of Forensic Images

- Encase/Expert Witness (GUIDANCE SOFTWARE)
- SMART (ASR DATA)
- Safeback (NTI)
- WinHex (X-WAYS FORENSICS)
- DD
- ProDiscover File Format
- SDI32 (VOGON)
- ILook Image (IRS)
- AFF-Advanced Forensic Format
- Gfzip
- Sgzip
- Paraben Forensic Image Format
- GHOST
- Others (?) and others to come I'm sure.

Imaging Software Applications

Our Imaging Applications and Examples

X-Ways Forensics	*(WinHex backup)*
Encase	*(Encase E01)*
FTK	*(SMART)*
NTimage	*(dd)*
NTI	*(Safeback image)*
Ghost	*(be careful, as it may not be a forensic image…)*
Exact clone	*(not really an image, but an exact copy)*

We will be conducting an experiment during this presentation.
The evidence sample will be a 7GB Windows XP system
Our evidence file will be "evidence.txt" on the evidence hard drive.

A brief on some tools

- There are many tools you can use to create forensic images.
- You need to know the strengths and limitations of each tool in order to choose the best for the task at hand.
- Even when on site for one job, you may be using several different tools to handle different computer configurations.

Guidance Software™

EnCase Forensic

- Maybe the most widely used format (.e01)
- Compressible and searchable
- Proprietary format with additional information placed inside the image (header information, CRC's every block of 64 sectors, plus a footer with a hash for the entire image (INTEGRATED HASH)
- DOS and Windows acquisition

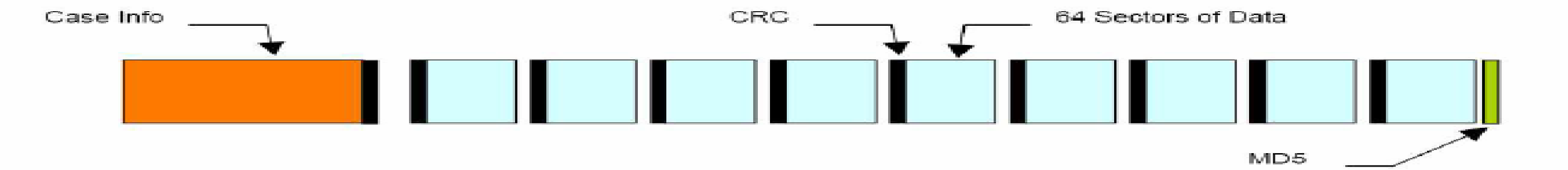
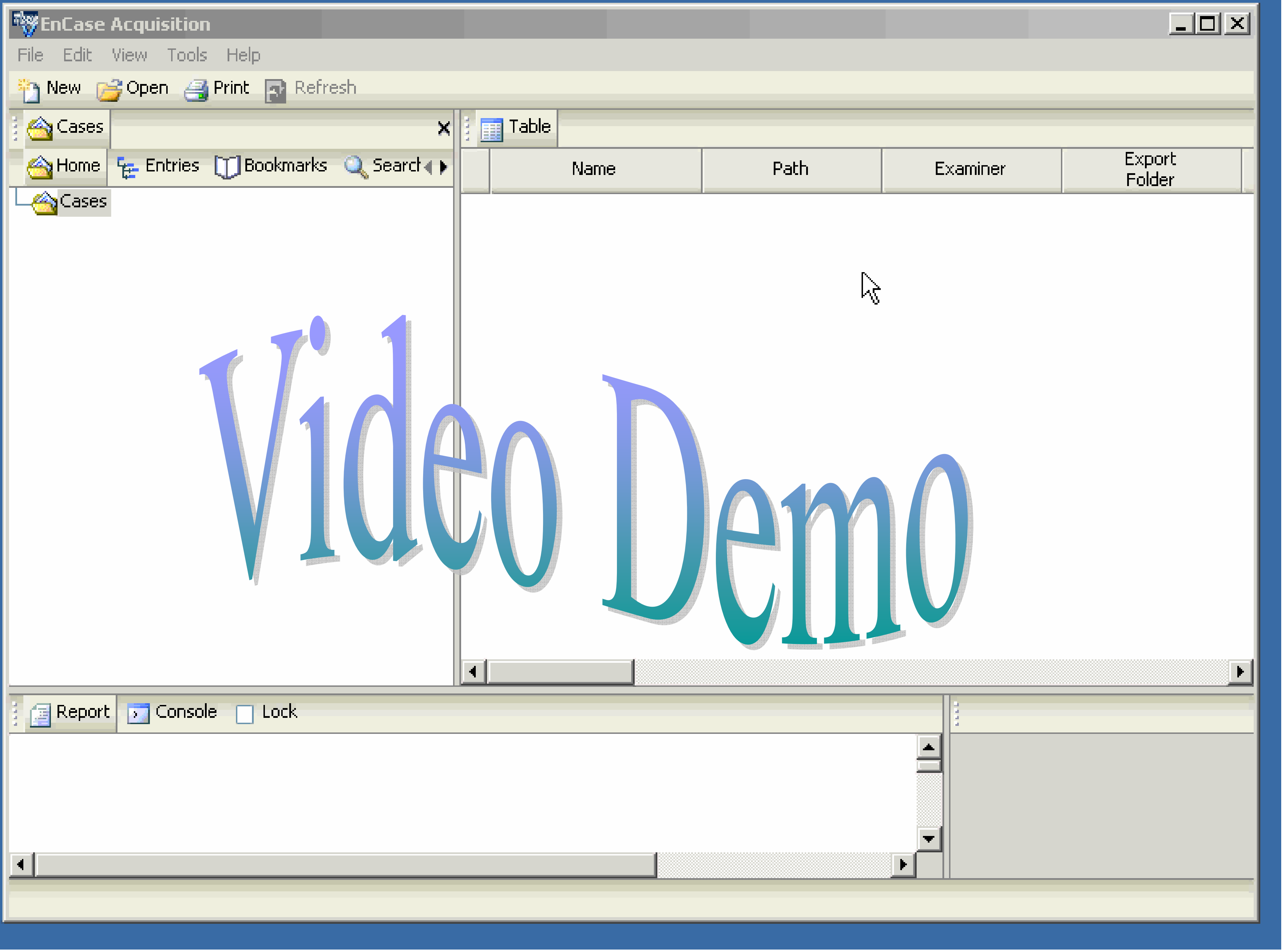


Figure 1. EnCase format.

http://guidancesoftware.com/


EnCase Acquisition
File
Edit
View
Tools
Help
New
Open
Print
Refresh
Cases
Home
Entries
Bookmarks
Searcl
Cases
Table
Name
Path
Examiner
Export Folder
Report
Console
Lock

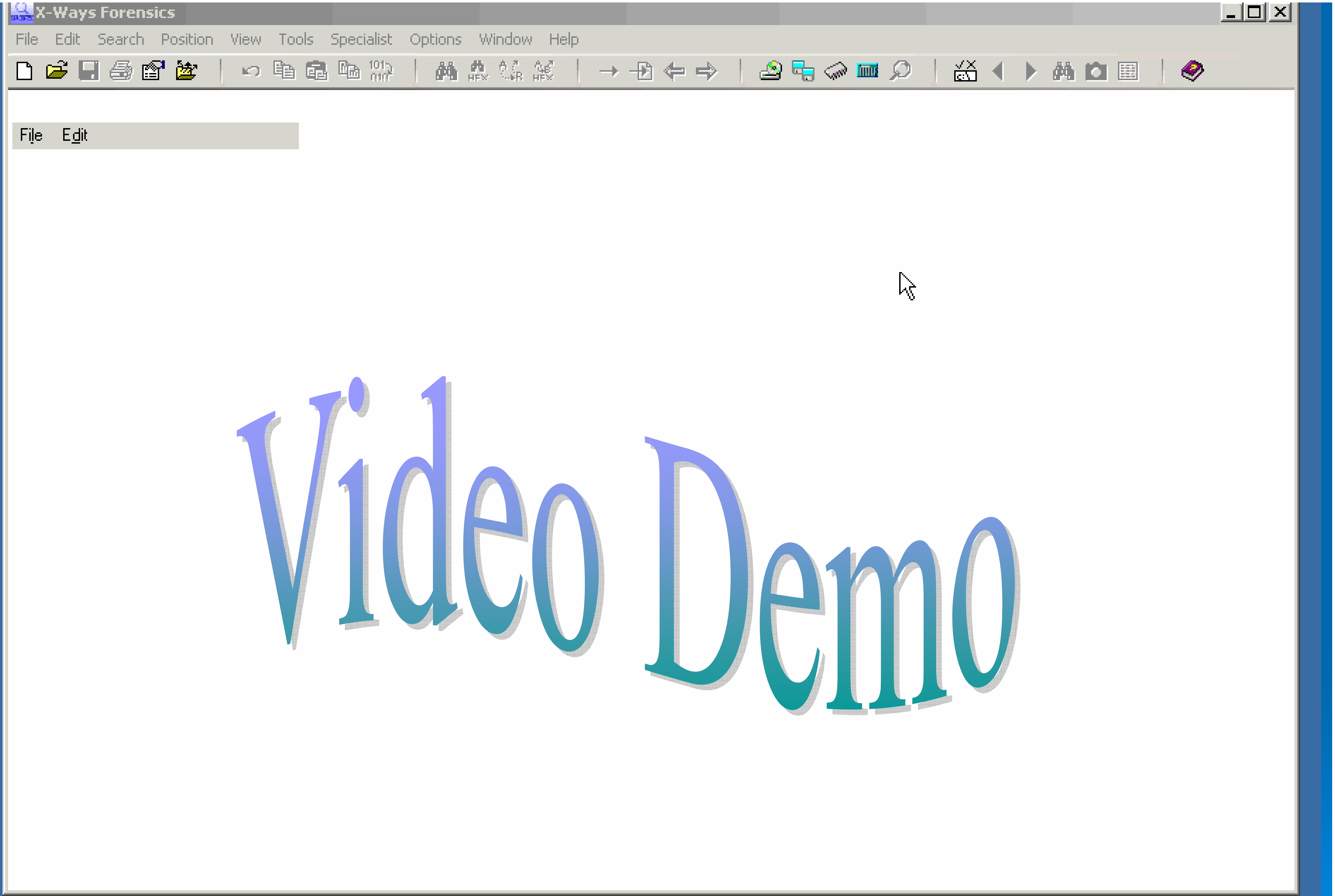
Video Demo

X-Ways Software Technology AG

X-Ways Forensics: Integrated Computer Forensics Software

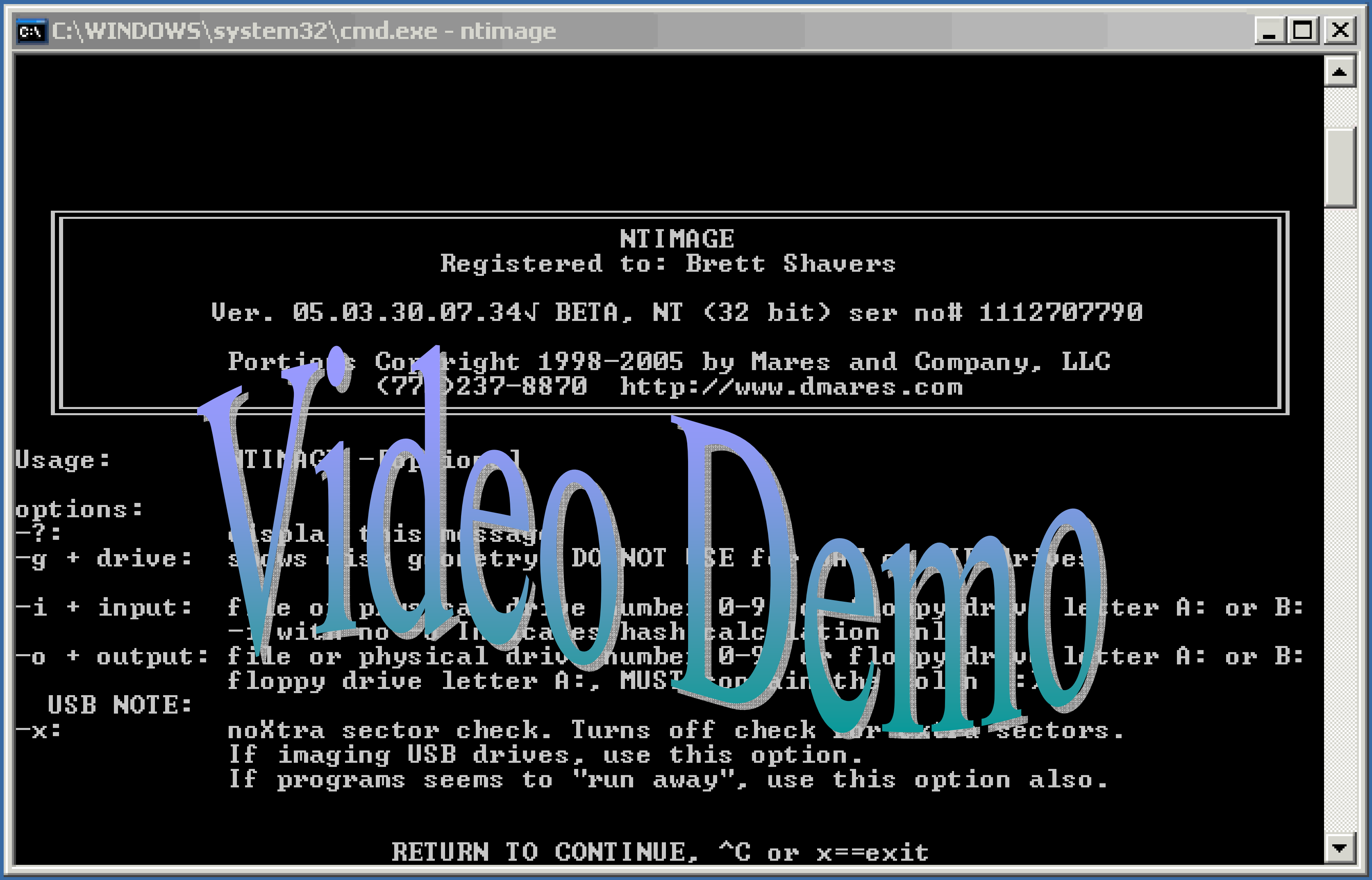
- Not interpretable as a disk-(Winhex backup)
- Not accessible by other applications
- Internal hash
- DOS (using the imaging application known as Replica) and Windows Acquisition
- However, it can also create other formats as well (dd, Encase, clone)

http://x-ways.net/forensics/index-m.html


X-Ways Forensics
File Edit Search Position View Tools Specialist Options Window Help
File Edit

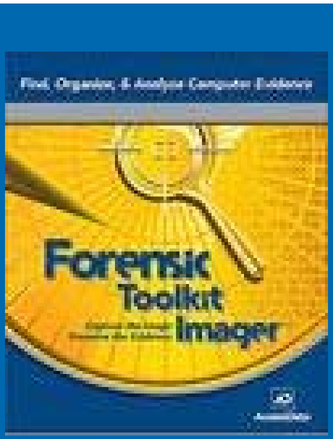
Video Demo

- Interpretable by many applications
- No internal hash (separate file)
- Not compressed (if it is compressed, it must be decompressed for forensic examinations)
- Not restricted to the 2GB size restriction of the Encase format
- Format: Raw image, compressed raw image



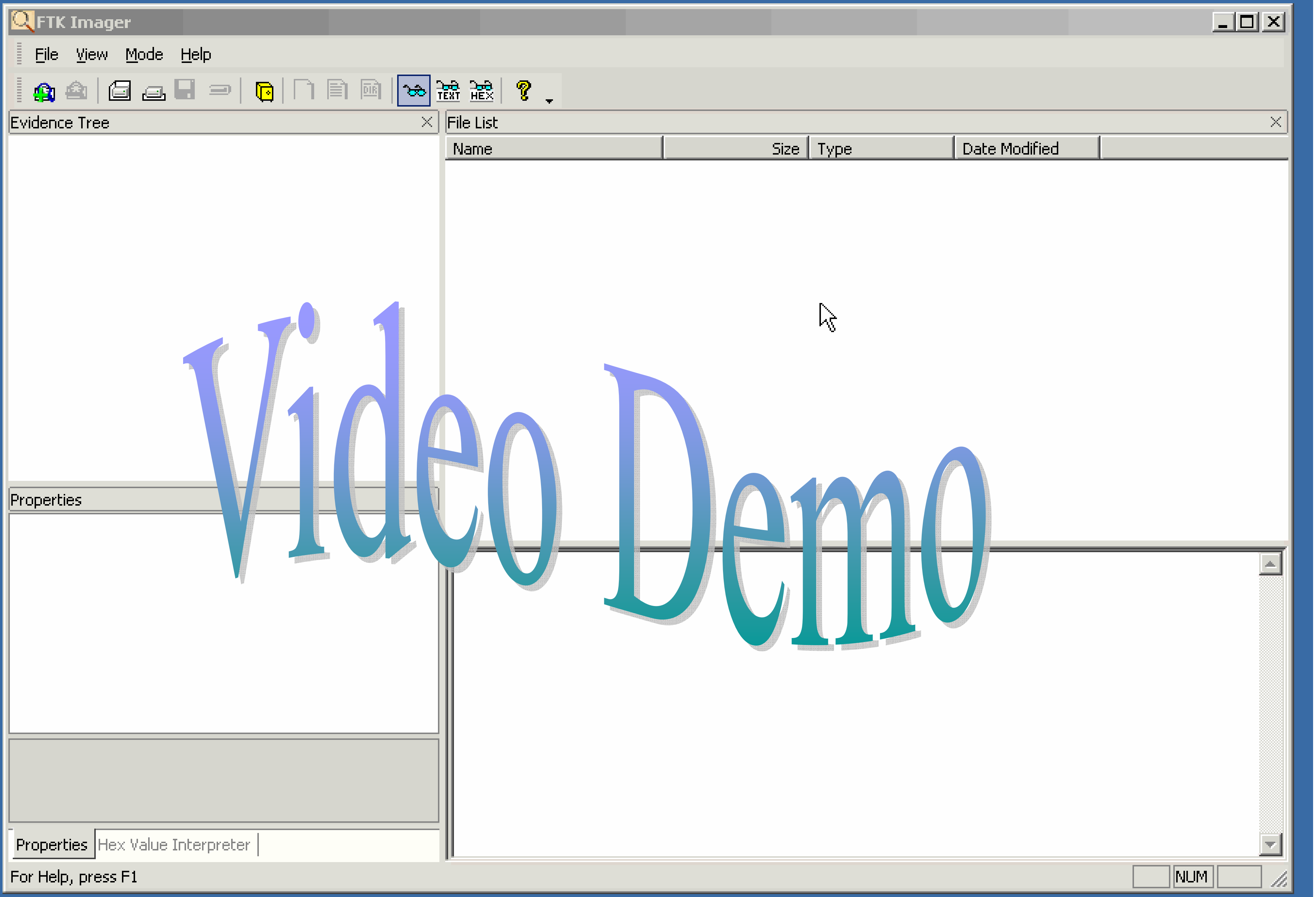
```
                               NTIMAGE
                      Registered to: Brett Shavers

         Ver. 05.03.30.07.34√ BETA, NT (32 bit) ser no# 1112707790

          Portions Copyright 1998-2005 by Mares and Company, LLC
                 (770)237-8870  http://www.dmares.com

Usage:       NTIMAGE -[options]

options:
-?:          display this message
-g + drive:  shows disk geometry. DO NOT USE for [illegible] drives
-i + input:  file or physical drive number 0-9 or floppy drive letter A: or B:
             -i with no -o indicates hash calculation only
-o + output: file or physical drive number 0-9 or floppy drive letter A: or B:
             floppy drive letter A:, MUST contain the colon (:)
  USB NOTE:
-x:          noXtra sector check. Turns off check for extra sectors.
             If imaging USB drives, use this option.
             If programs seems to "run away", use this option also.


                    RETURN TO CONTINUE, ^C or x==exit
```

Video Demo



- Windows based acquisition
- Able to run from CD, Flashdrive or from the destination media (external hard drive as an example)
- Ability to create multiple image types onto multiple destination drives at the same time
- Formats: Encase, SMART, dd

http://www.accessdata.com


FTK Imager
File
View
Mode
Help
TEXT
HEX
Evidence Tree
File List
Name
Size
Type
Date Modified
Properties
Properties
Hex Value Interpreter
For Help, press F1
NUM

Video Demo

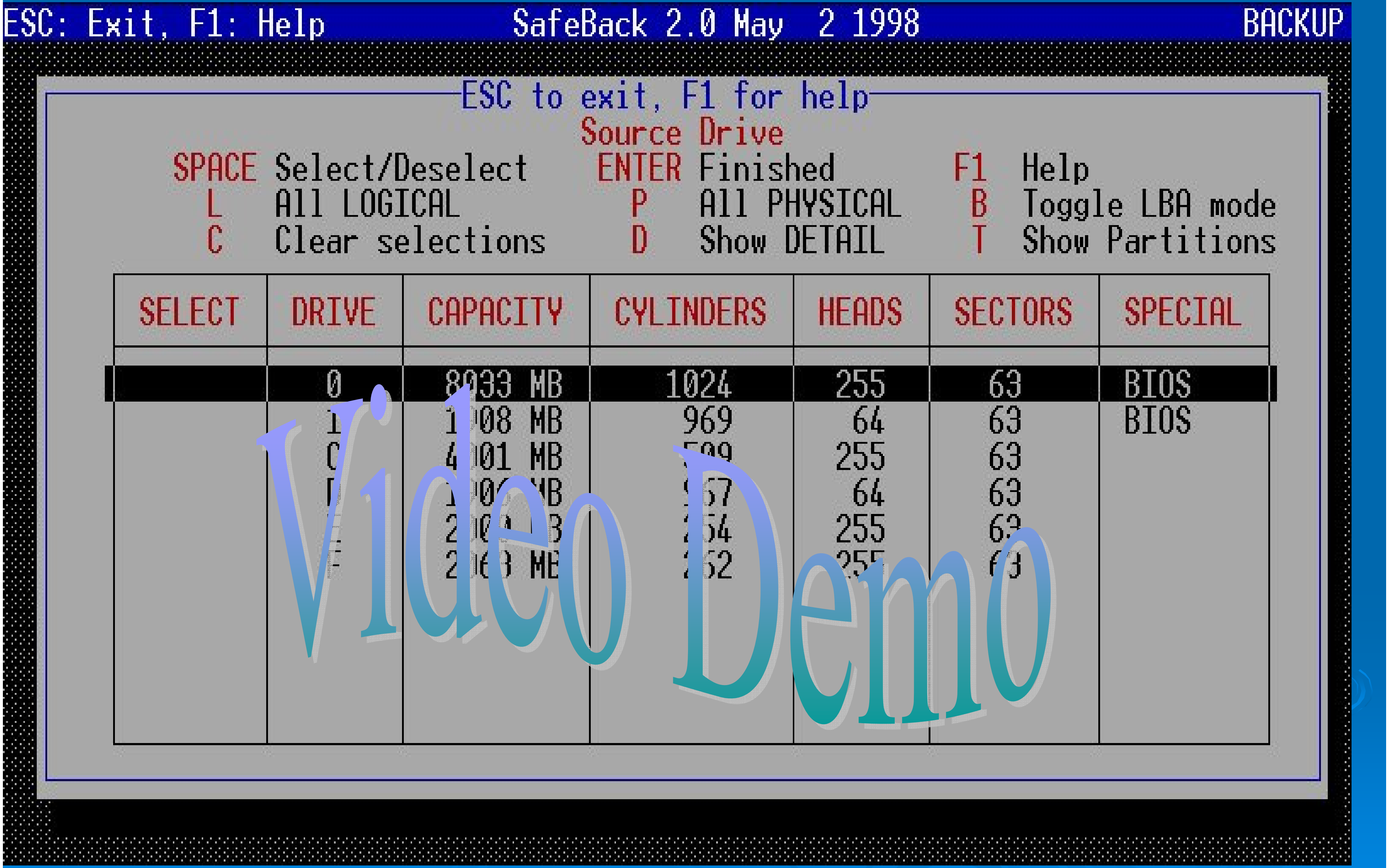
Linux

- Many bootable CD’s that can create several variants of images (Encase image, dd)
- There are many free forensic versions of Linux bootable CD’s that contain other tools in additional to imaging applications.

Safeback

Safeback Image

- The latest release of Safeback creates an image that isn't accessible by the majority of forensic tools…
- This is a serious drawback to this format.



```
ESC: Exit, F1: Help            SafeBack 2.0 May  2 1998                BACKUP

                         ESC to exit, F1 for help
                              Source Drive
     SPACE Select/Deselect      ENTER Finished          F1   Help
       L   All LOGICAL            P   All PHYSICAL       B   Toggle LBA mode
       C   Clear selections       D   Show DETAIL        T   Show Partitions
```

SELECT	DRIVE	CAPACITY	CYLINDERS	HEADS	SECTORS	SPECIAL
	0	8033 MB	1024	255	63	BIOS
	1	1908 MB	969	64	63	BIOS
	C	4001 MB	509	255	63	
	D	[illegible]	967	64	63	
	E	[illegible]	254	255	63	
	F	2063 MB	262	255	63	

Video Demo

Live Imaging

- There are times when you can’t shut the computer down and need to create a forensic image. This is when you make an image of that running computer by running a forensic application on that computer! This is not something to try without testing and training!

- Data on the computer will change, there is nothing you can do about it.
- However, you can image the RAM.
- You can create a logical or physical image using different tools.

Some Live Imaging Tools

- FTK Imager
- X-Ways Capture
- Helix (dd) and NetCat
- Enterprise editions of forensic applications (Encase EEE, ProDiscover IR/IN
- Nearly any tool that can run from either an external device such as a USB drive or CD can be used on running machines to create an image. It is NOT a good idea to use an application that must be installed on the suspect machine.

Forensic Boot Disks

- Boot floppy (to DOS)
  - Make it a FORENSIC boot floppy!
  - Non-forensic boot floppies WILL access the drive and then you will have explaining to do.

- Linux Bootable CD
  - Make sure the distribution you choose doesn't automatically MOUNT the drives!

Converting Images from One Format to Another

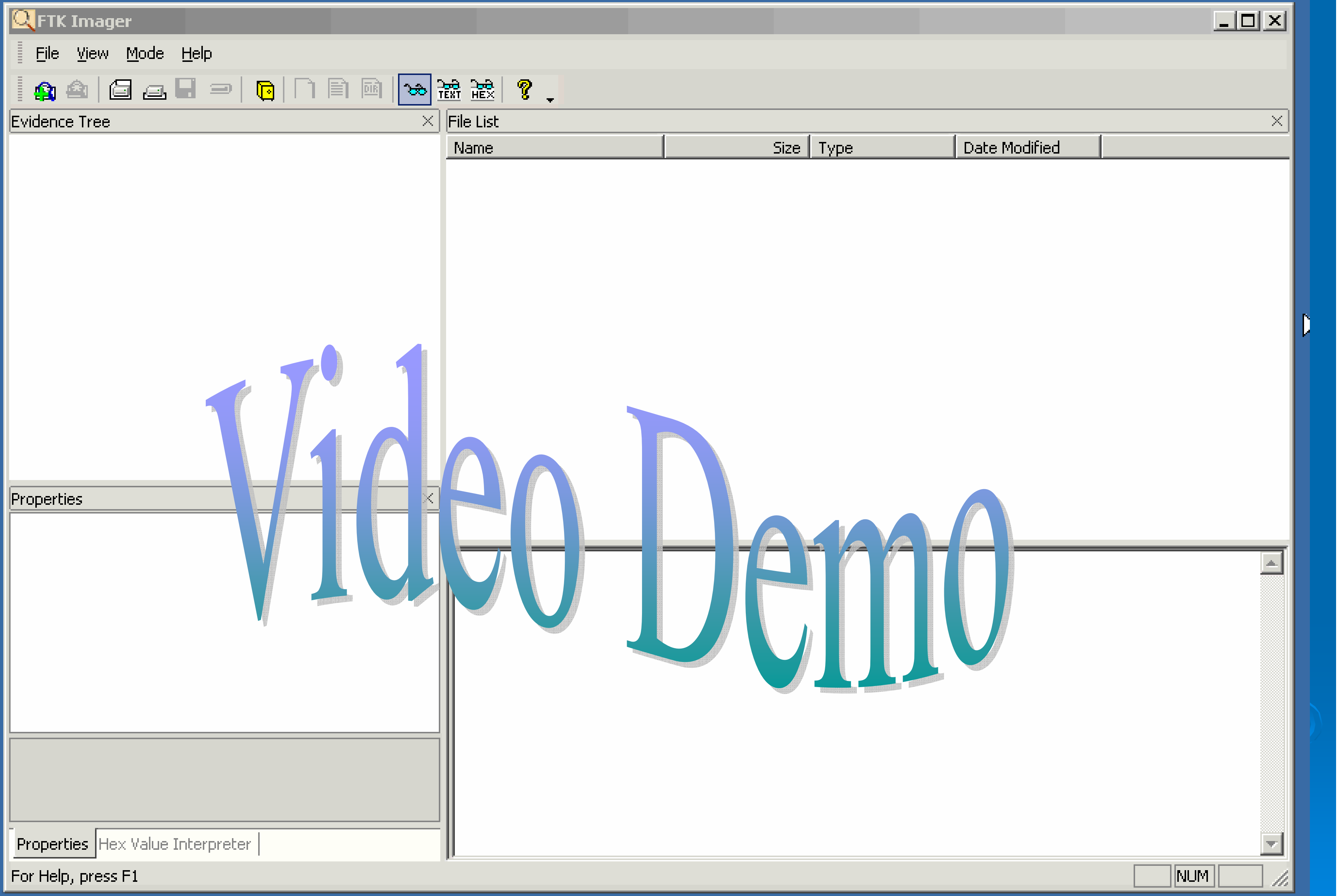
Practical Exercises

- No matter which image format you create, there is always the request of providing a copy of your image in a format that is different than what you created.
- Additionally, when you employ different forensic applications on one image, you may need to convert one format to another to access it with different tools.
- For this, we are going to convert some images!

Image Conversion Examples

We are going to convert the following:

- Original to Encase (using FTK, Encase, & Winhex)
- Encase image to dd (using FTK)
- dd to Restored Clone (using Winhex)
- Clone to dd (using FTK, WinHex)
- Encase to Restored Clone (using Winhex, Encase)
- SMART to Encase (using FTK)
- SMART to dd (using FTK)
- Any of the above to vmware to boot to a live machine!



For Help, press F1

Video Demo

Recap

- **We created Various Image Types…**
  - dd format
  - Encase format
  - WinHex backup
  - SMART format
- **…Using Various Applications**
  - Encase
  - FTK
  - X-Ways Forensics
  - Ntimage
- **And converted one image format to another**

Accessing the Images

Accessing the Images

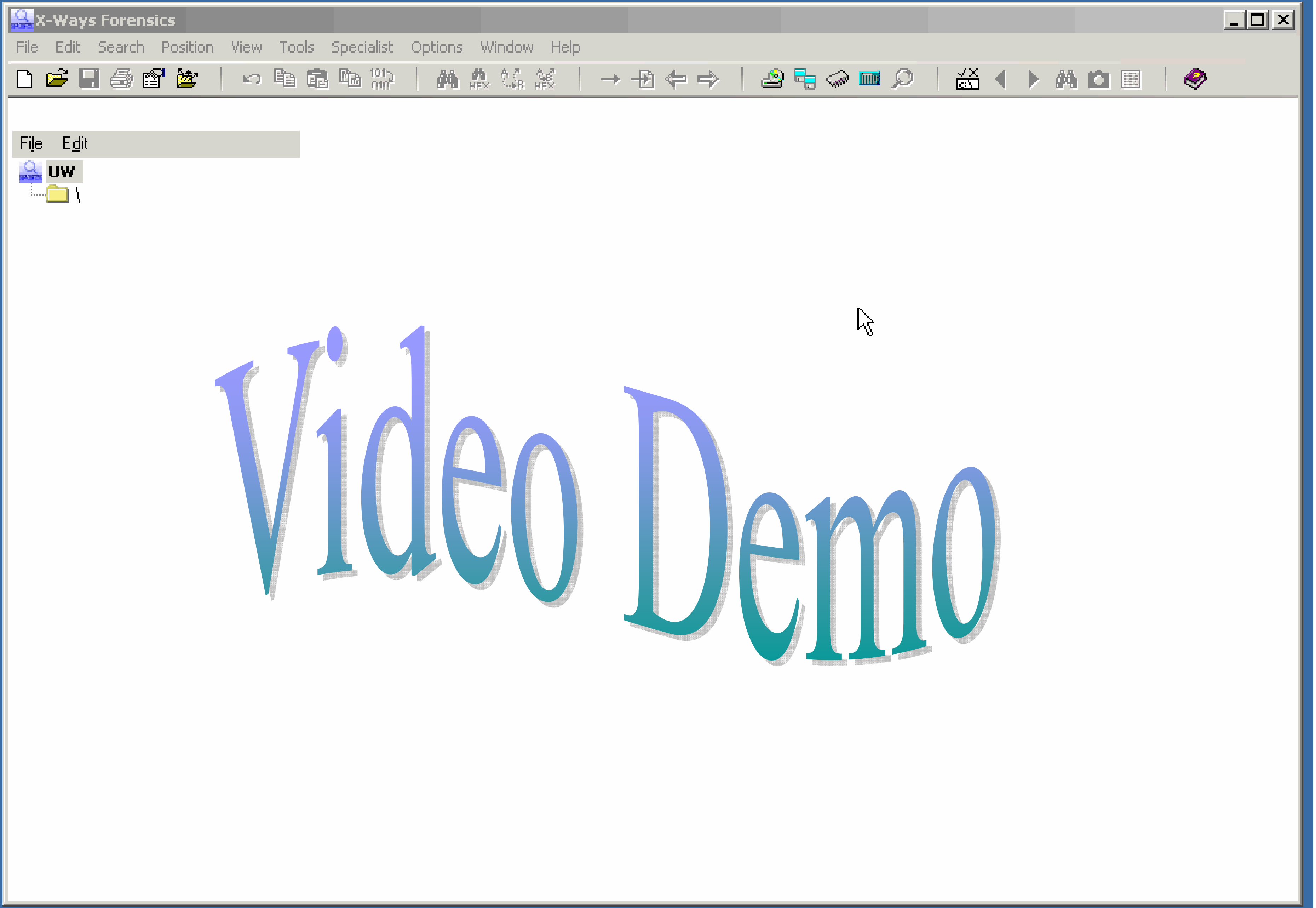
- **Forensic Applications**
  - Guidance Software "Encase"
  - Accessdata "Forensic Tool Kit"
  - X-Ways "X-Ways Forensics"
  - Other misc forensic applications
- **Other Non-Forensic Applications**
  - Mount Image Pro
  - LiveView
  - Vmware

But first, a word about GHOST

- Ghost was NOT designed as a forenisc collection utility. It’s great at what it does (clones active data)
- You *can* set it to capture all data space, but you will be limited to the forensic tools that can access it. You also risk not doing it correctly and losing your only chance to capture an original image.
- If you truly need a forensic image, use an application that has been designed and tested solely for forensic images. Don’t make due with anything less, or you risk your forensic image.

Forensic Applications

- **Encase, FTK, X-Ways Forensics, etc…**
  - Each can acquire the image for analysis
  - Indexing/cataloging of data
  - Searching of words, strings, etc…
  - Export of native files from the image
  - Creation of analysis reports
  - Duplication and conversion of images
  - Along with multiple other features


X-Ways Forensics
File
Edit
Search
Position
View
Tools
Specialist
Options
Window
Help
File
Edit
UW
\

Video Demo

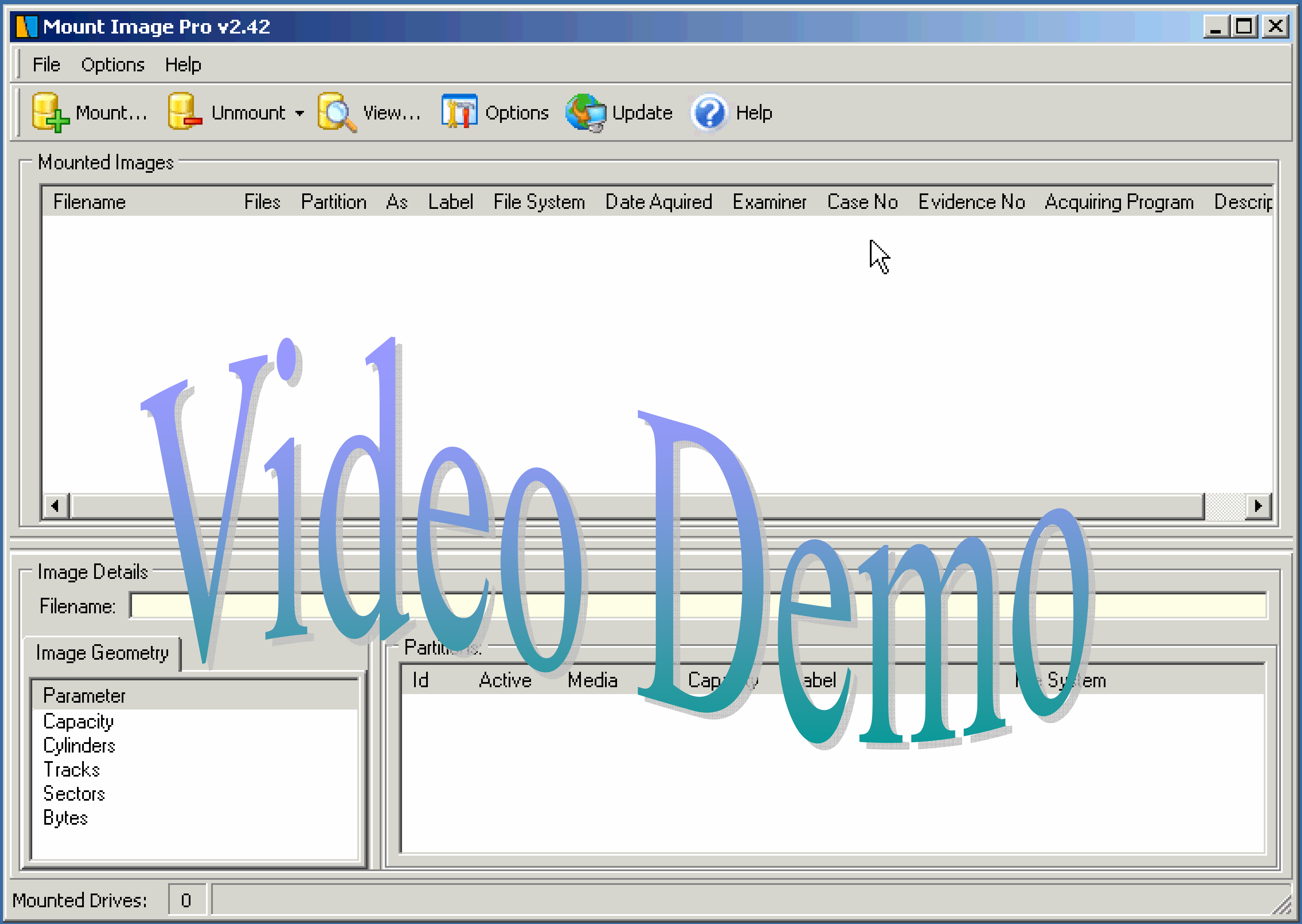
Non-Standard Applications

- Mount Image Pro
- Virtual Forensic Computing
- LiveView
- Vmware
- Symantec Ghost ***(beware!)***

- Mount Image Pro
  - Access of the image as a drive letter in Windows
  - Tools can be run against the drive letter as if it were an actual drive (anti-virus, data recovery tools, etc…)
  - No (expensive) forensic applications required to view the image
  - Native files can be extracted
  - (*Paraben's P2 Explorer is similar to MIP*)

http://www.mountimage.com/

Video Demo



Mounted Drives: 0

vmware®

Video Demo

Microsoft
Microsoft Windows 2000 Professional
Microsoft
Microsoft Windows 95
Microsoft Internet Explorer

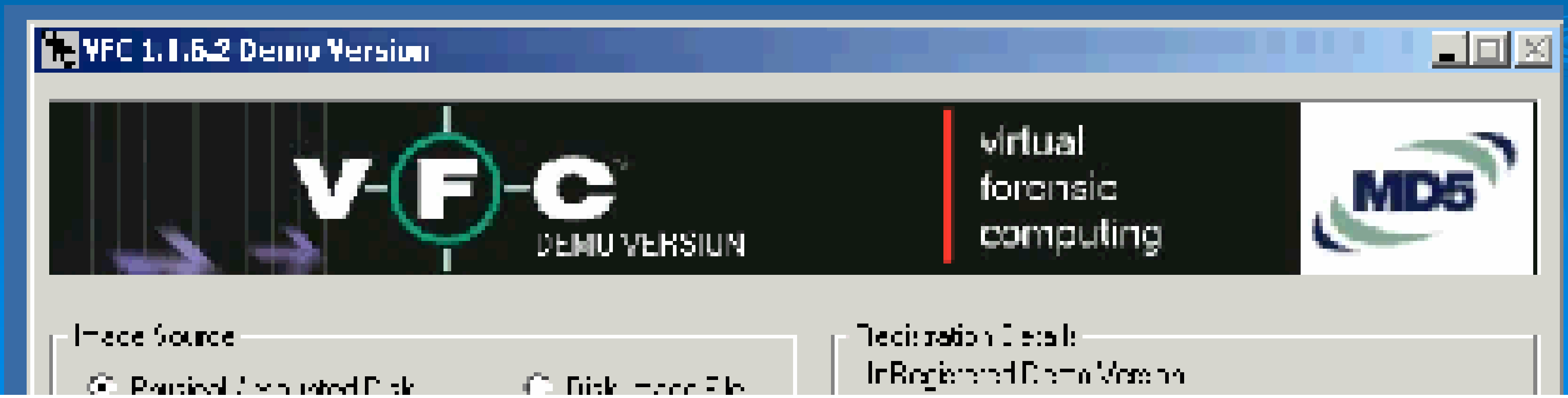
vmware

- Clone can be booted into vmware
- dd image can be booted into vmware
- Encase image can be booted into vmware
- vmware file can be accessed as a drive letter in Windows
- VMware is a versatile application that was not designed for forensic use, but clearly can be used as supplement tool in examinations.

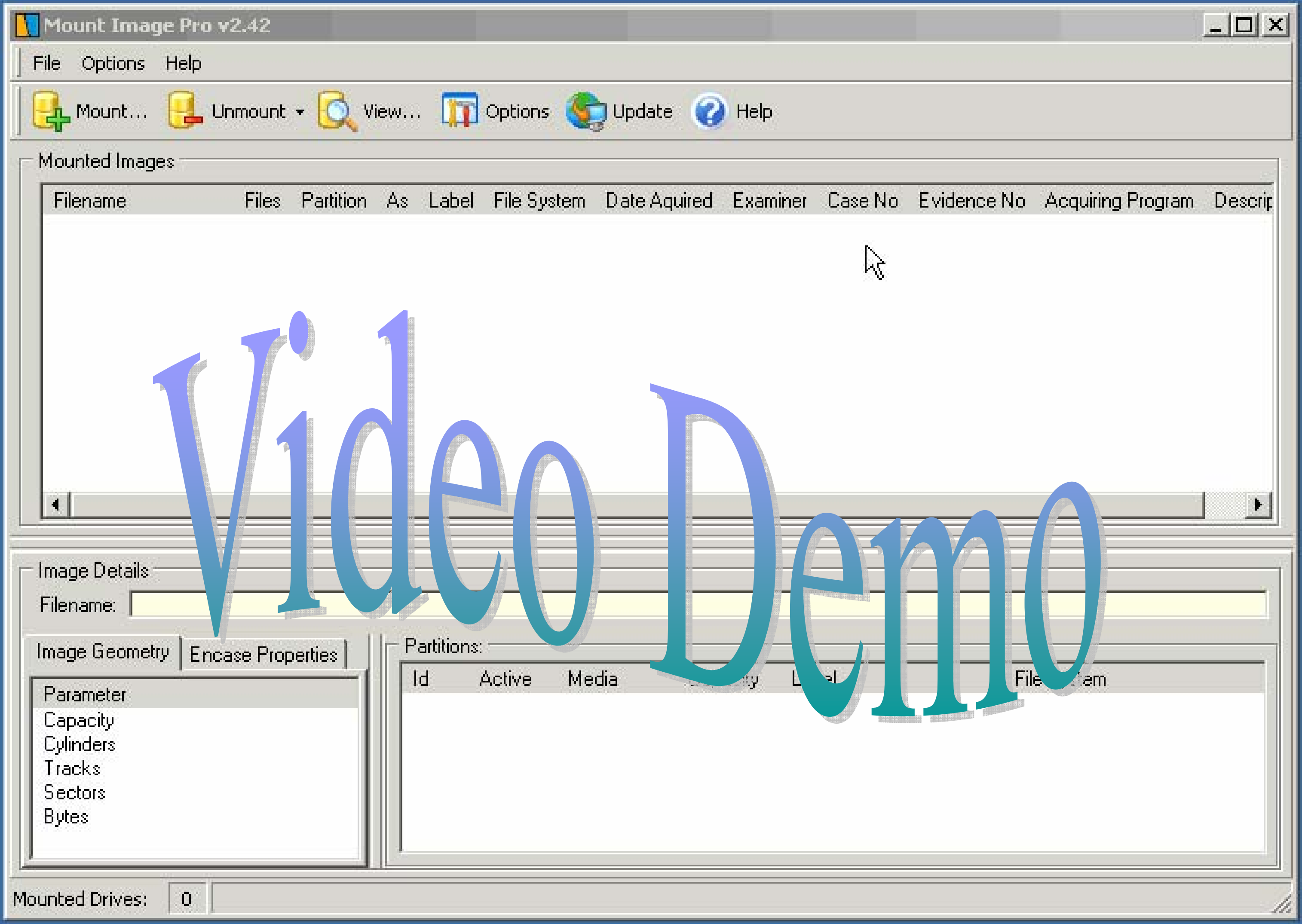
http://www.vmware.com

Booting Encase Images into vmware

- **Virtual Forensic Computing (not free)**
  - Allows an Encase image to be booted into vmware
  - Can also boot a physical drive or dd image
  - Requires Mount Image Pro (also not free)



Video Demo


Mount Image Pro v2.42
File
Options
Help
Mount...
Unmount
View...
Options
Update
Help
Mounted Images
Filename
Files
Partition
As
Label
File System
Date Aquired
Examiner
Case No
Evidence No
Acquiring Program
Descrip
Image Details
Filename:
Image Geometry
Encase Properties
Parameter
Capacity
Cylinders
Tracks
Sectors
Bytes
Partitions:
Id
Active
Media
File
Mounted Drives:
0

Booting dd Images into vmware

- **LiveView (free)**
  - Allows for dd images to be booted into vmware
  - Only requires vmware player (free) and vmware diskmount utility (free also)
  - *An Encase image can be converted to dd and then booted to vmware (a workaround to not using the Virtual Forensic Computing and Mount Image Pro applications)*

VMware Player - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Favorites
Address http://www.vmware.com/products/player/
Go Links SnagIt
VMware.com | Technology Network (VMTN) | Worldwide
Downloads | Store | Account | Help | Contact
Search
advanced search
vmware
AN EMC COMPANY
SOLUTIONS
PRODUCTS
SERVICES
SUPPORT
CUSTOMERS
PARTNERS
EVENTS
NEWS
ABOUT US
Home > Products > VMware Player
EMAIL PAGE | PRINT PAGE
VMware Player
Player
NOW
Internet

Free VMware Player

Run any virtual machine on Windows or Linux PC

Run any virtual machine

VMware Player lets you evaluate new or pre-release software contained in virtual machines, without any installation or configuration hassles. You can also share existing virtual machines with colleagues or friends—just use VMware Player to run any virtual machine

VMware Player

FAQs

NEXT STEPS

Compare Desktop Products

Download VMware Player

Download Browser Appliance

Download Virtual Appliances

VMWARE PLAYER RESOURCES

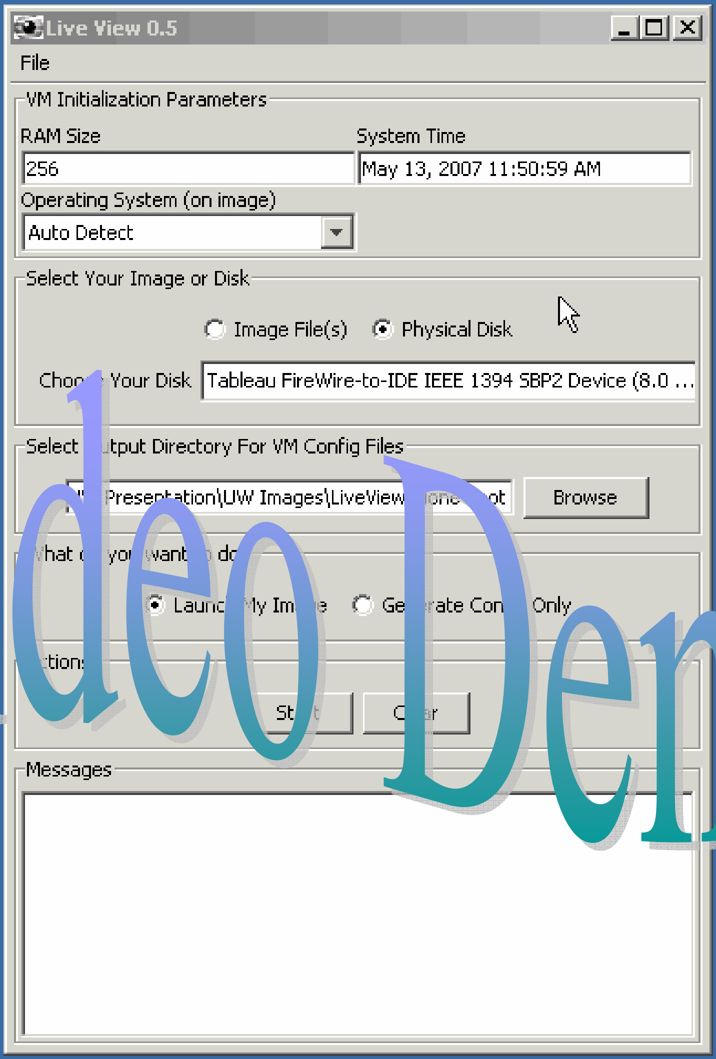
Documentation

Video Demo

Booting a Physical Drive to vmware

- LiveView can boot to vmware (after it generates the configuration files)
- Virtual Forensic Computing can boot to vmware after Mount Image Pro mounts the drive
- Our next video:
  - Cloned hard drive, attached with hardware write blocker
  - Using LiveView, we will boot it to vmware.
  - No writes to the clone, all writes go to a separate folder.

Video Demo



VM Initialization Parameters

RAM Size: 256

System Time: May 13, 2007 11:50:59 AM

Operating System (on image): Auto Detect

Select Your Image or Disk

○ Image File(s) ● Physical Disk

Choo Your Disk: Tableau FireWire-to-IDE IEEE 1394 SBP2 Device (8.0 ...

Select tput Directory For VM Config Files

Presentation\UW Images\LiveView ot

hat yo want do

● Launc y Im e ○ Ge rate Con Only

tions

Did Our Original Evidence File Ever Change with All These Images

(remember the evidence.txt we talked about in the beginning? That file has resided on each image conversion we did. We even booted the image with the file on it! Has it changed?)

Hashing, re-hashed…

- MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual.

http://WhatIs.techtarget.com/definition/0,,sid9_gci211545,00.html

Or Brett’s Definition….

A hash is a **RBN*** (really big number) that is created to give a fingerprint to a file. And actually, the strength of the hash is way stronger than any fingerprint comparison!

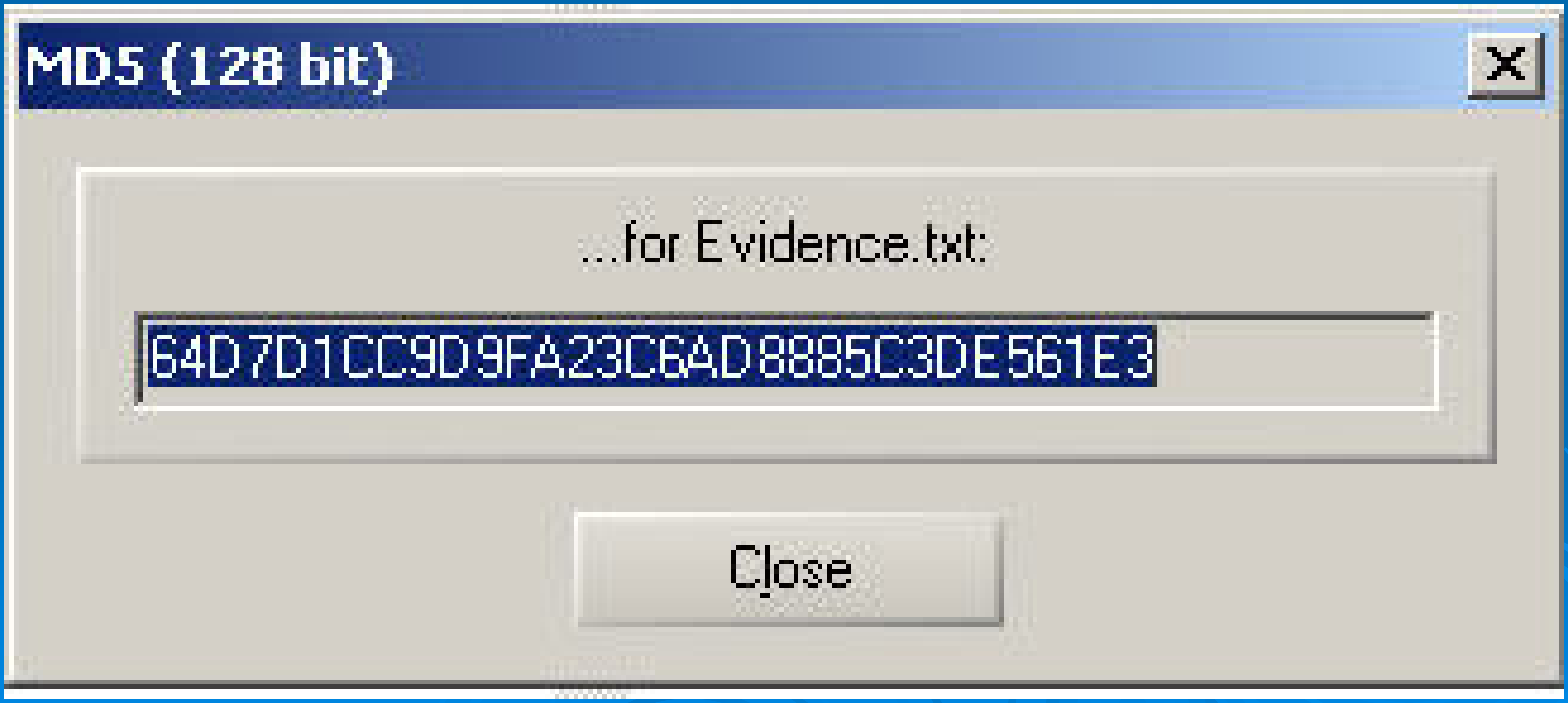
A hash is also only ‘one way’, meaning, you can take the RBN and reverse it to the original file. An analogy would be taking a pound of beef and putting it through a grinder. You can’t *ungrind* the beef to it’s original condition.

*I made up the RBN, no one in court will get it the joke….it’s actually a MD5 or SHA hash, technically…

Our evidence.txt file…

- …was created on the original evidence.
- A hash was created with the original evidence.
- The file was extracted from the Encase image with Encase and hashed.
- The file was extracted from the SMART image with FTK and hashed.
- The file was extracted from the dd image with X-Ways Forensics and hashed.
- The file was extracted from the dd that was converted from the Encase image and hashed.
- The file was extracted from the vmware restored boot session and hashed.
- The result was…

All Hashes Matched!



...for Evidence.txt:

64D7D1CC9D9FA23C6AD8885C3DE561E3

What’s the Point?

- With a true forensic image, the data is an exact bit for bit copy of the original. All files can be *hashed* to give each a very unique number.
- You can convert the images without changing the data on the images.
- You can create as many ‘originals’ as needed with one forensic image.
- If you don’t create a **forensic** image in the beginning, you may never get a second chance to capture the first original image.

Summary

- There is no ‘one’ method of creating a forensic image. The concept is to protect the original evidence and create an exact clone/bit stream image.
- Images can be converted between different formats.
- Various forensic applications can access certain image formats.
- Images can be restored and even booted into a virtual computing environment.
- Not one tool does it all, none are better than others, it all depends on the circumstances when used.

Summary

- When a forensic image is needed, it is best to have someone trained in this specific area to create the image. You only get one shot at it.
- If you even think you may need a forensic image in the future, nothing is lost by spending a little more time to create it in the beginning.
- Don’t use tools that are not designed for a purpose other than what they are marketed for. A hammer does not solve every problem, it sometimes creates more problems.

Summary

- The physical process of imaging is actually simple, but something always invariably will go wrong and problems are encountered that have to be solved.
- An experienced computer forensics examiner can pretty much image anything, solve every problem, and walk away with a perfect forensic image. Others…well, like I said, you only get one shot to capture the first original image.

Questions?

Brett Shavers

brett@e3discovery.com

www.e3discovery.com