Microsoft | Services

Windows 7 Virtualization Technologies

Advanced Forensic Topics

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

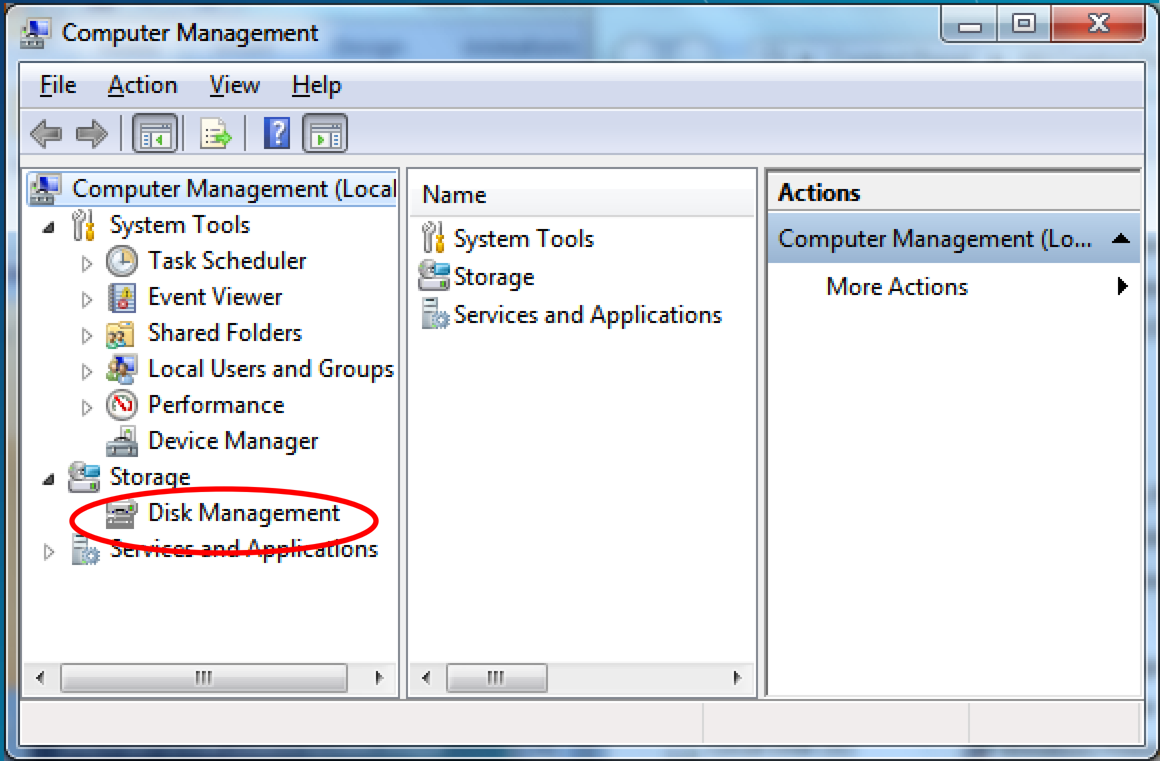
Microsoft | Services

Virtualization Technologies

- Integrated Virtual Hard Drive (VHD) Creation and Mounting
- Boot to Virtual Hard Drive (VHD)
- VHD File Use in System Image Backup
- Virtual PC 7 Technologies
  - Windows XP Compatibility Mode
  - Application Virtualization
  - Undo Disks

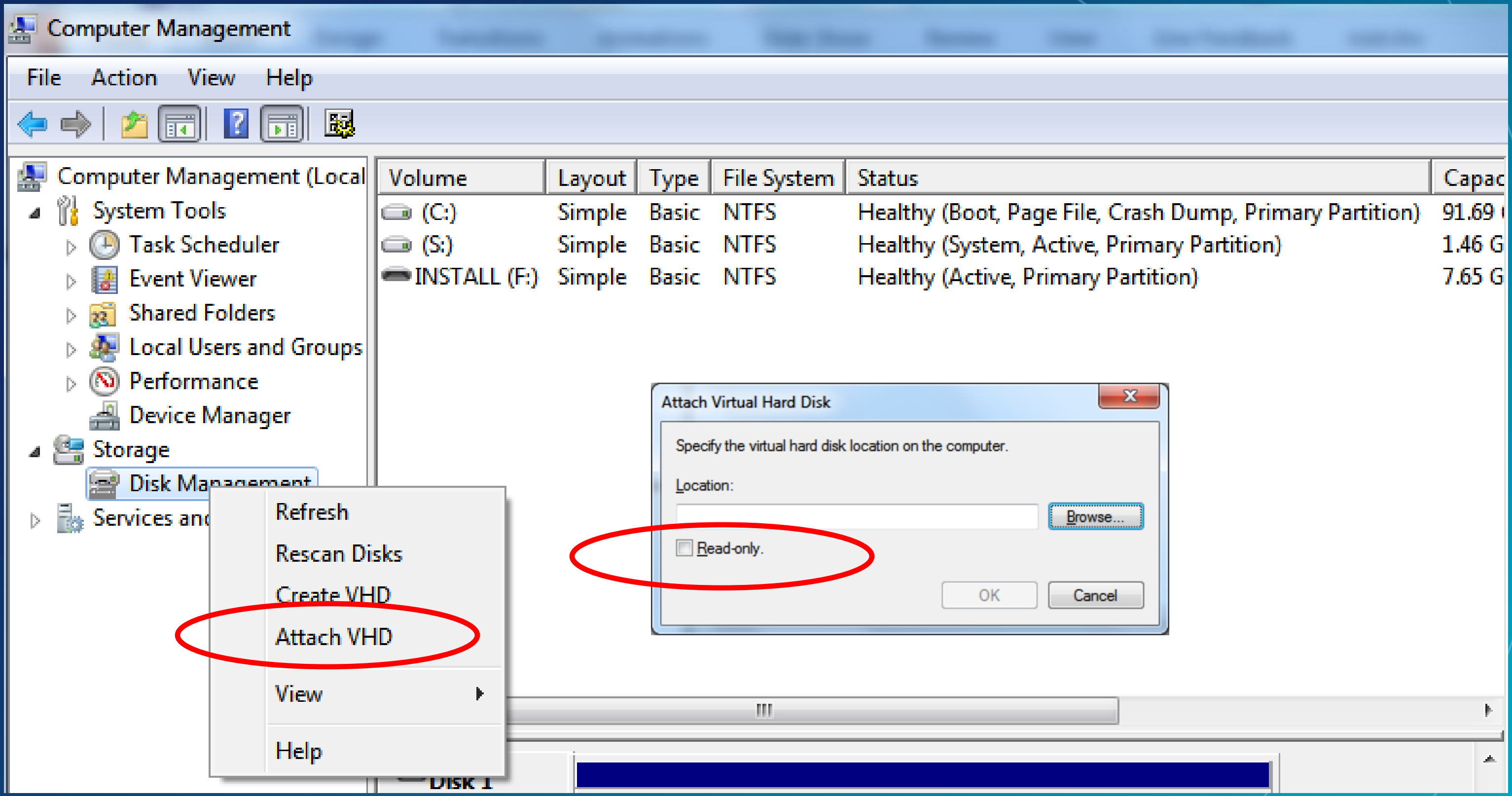
Integrated VHD Creation and Mounting

- Native in the file system
- Accessed through Control Panel\AdministrativeTools\Computer Management



Integrated VHD Creation and Mounting

- When mounting, can select “Read Only”



Volume	Layout	Type	File System	Status	Capac
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	91.69 (
(S:)	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	1.46 G
INSTALL (F:)	Simple	Basic	NTFS	Healthy (Active, Primary Partition)	7.65 G

Specify the virtual hard disk location on the computer.

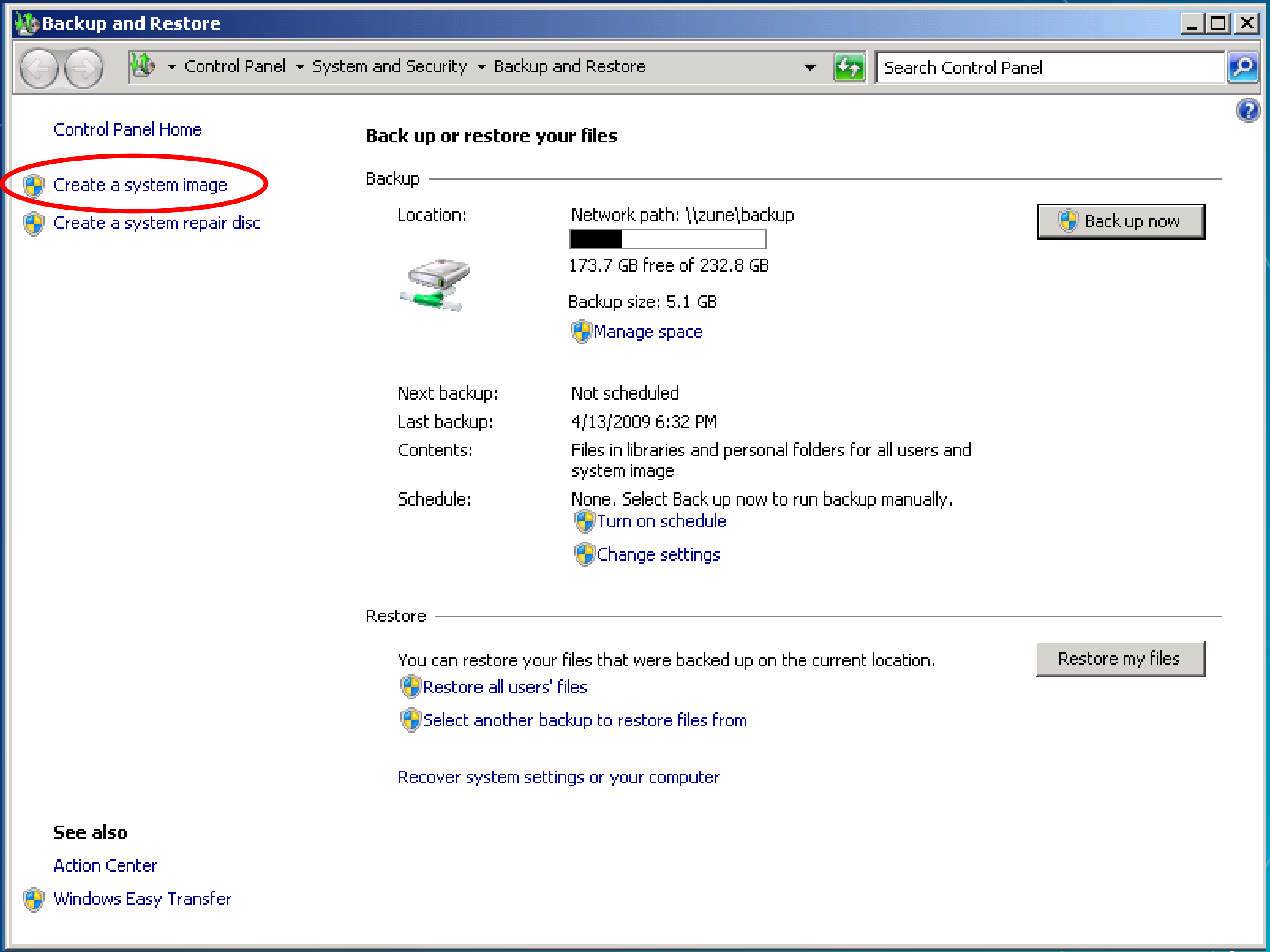
Location:

□ Read-only.

VHD File Format Used in System Image Backup

- System Image Backup (formerly Complete PC Backup in Vista)
- Backs up full hard drive, not just specific files and folders
- VHD can be stored on local USB drive or over the network
- Can be mounted natively on a Windows 7 Forensic Workstation for examination

System Image Backup



Control Panel Home

Create a system image

Create a system repair disc

Back up or restore your files

Backup

Location: Network path: \\zune\backup

173.7 GB free of 232.8 GB

Backup size: 5.1 GB

Manage space

Back up now

Next backup: Not scheduled

Last backup: 4/13/2009 6:32 PM

Contents: Files in libraries and personal folders for all users and system image

Schedule: None. Select Back up now to run backup manually.

Turn on schedule

Change settings

Restore

You can restore your files that were backed up on the current location.

Restore my files

Restore all users' files

Select another backup to restore files from

Recover system settings or your computer

See also

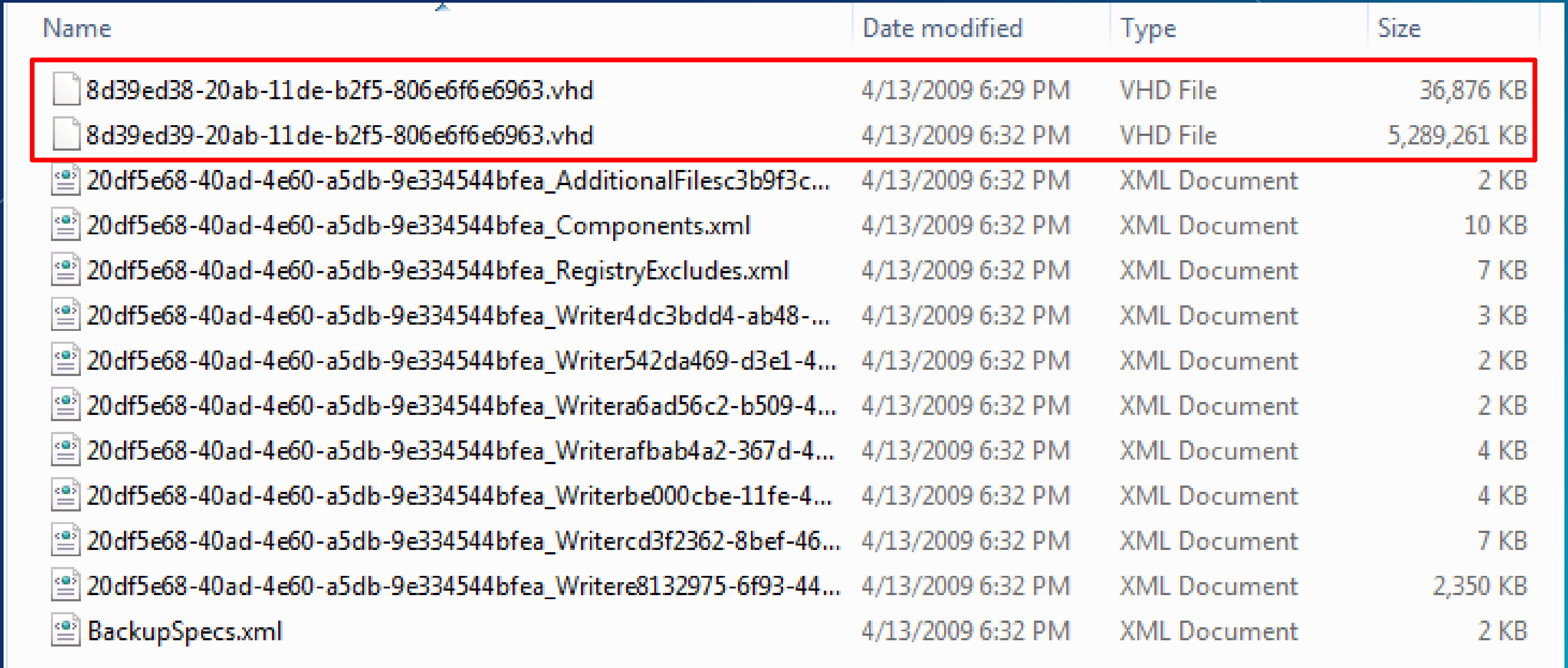
Action Center

Windows Easy Transfer

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Microsoft Services

System Image Backup



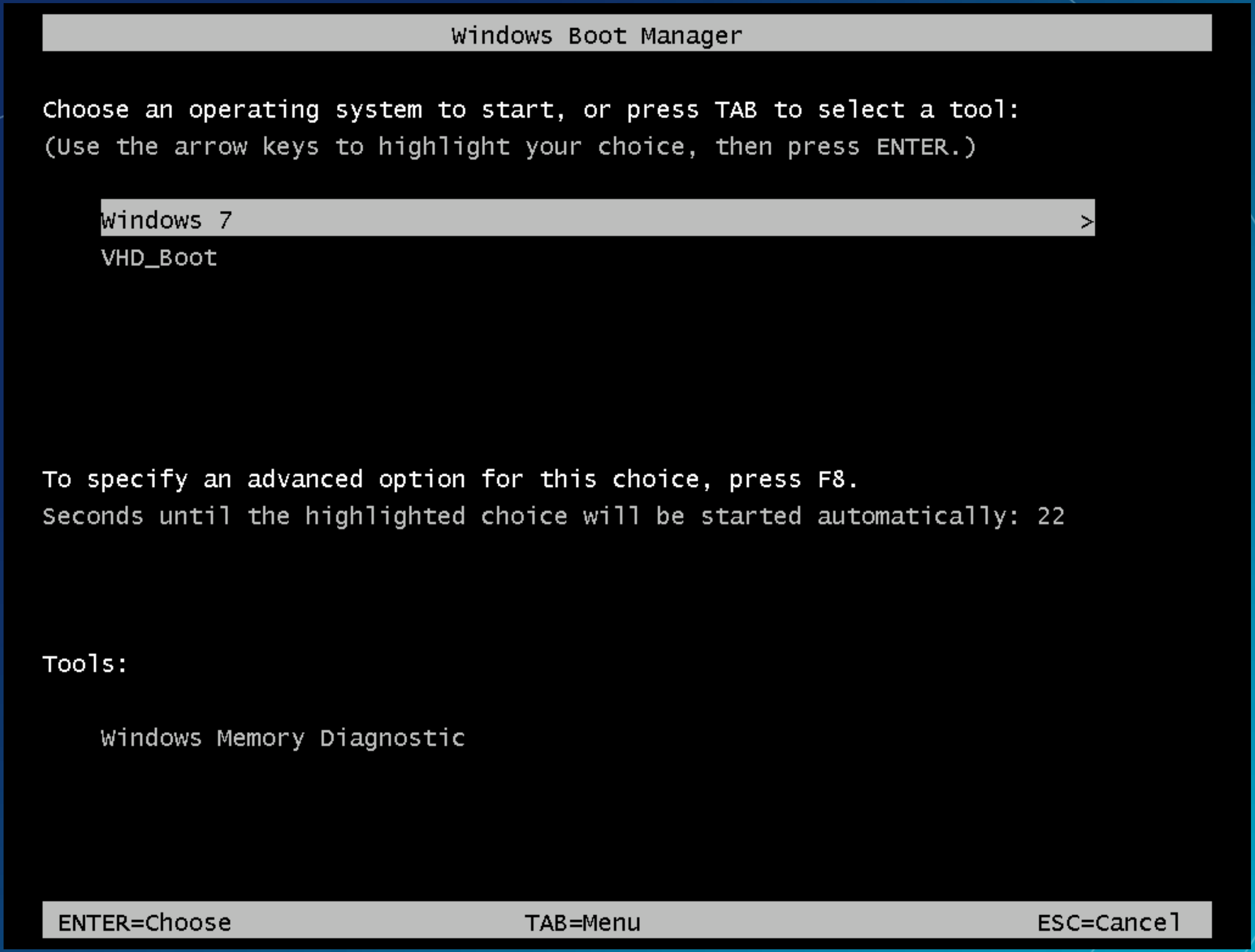
Name	Date modified	Type	Size
8d39ed38-20ab-11de-b2f5-806e6f6e6963.vhd	4/13/2009 6:29 PM	VHD File	36,876 KB
8d39ed39-20ab-11de-b2f5-806e6f6e6963.vhd	4/13/2009 6:32 PM	VHD File	5,289,261 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_AdditionalFilesc3b9f3c...	4/13/2009 6:32 PM	XML Document	2 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_Components.xml	4/13/2009 6:32 PM	XML Document	10 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_RegistryExcludes.xml	4/13/2009 6:32 PM	XML Document	7 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_Writer4dc3bdd4-ab48-...	4/13/2009 6:32 PM	XML Document	3 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_Writer542da469-d3e1-4...	4/13/2009 6:32 PM	XML Document	2 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_Writera6ad56c2-b509-4...	4/13/2009 6:32 PM	XML Document	2 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_Writerafbab4a2-367d-4...	4/13/2009 6:32 PM	XML Document	4 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_Writerbe000cbe-11fe-4...	4/13/2009 6:32 PM	XML Document	4 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_Writercd3f2362-8bef-46...	4/13/2009 6:32 PM	XML Document	7 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_Writere8132975-6f93-44...	4/13/2009 6:32 PM	XML Document	2,350 KB
BackupSpecs.xml	4/13/2009 6:32 PM	XML Document	2 KB

Boot to VHD

- Can configure Windows 7 to boot to the hard drive, OR VHD on the hard drive
- Only supported to boot Windows 7 VHD files
- Creates a boot list to select OS during system startup

How to Enable Boot to VHD

Boot to a VHD



```
                          Windows Boot Manager

Choose an operating system to start, or press TAB to select a tool:
(Use the arrow keys to highlight your choice, then press ENTER.)

    Windows 7                                                     >
    VHD_Boot





To specify an advanced option for this choice, press F8.
Seconds until the highlighted choice will be started automatically: 22



Tools:

    Windows Memory Diagnostic




 ENTER=Choose                TAB=Menu                       ESC=Cancel
```

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Microsoft® | Services

VHD Disk Investigative Impact

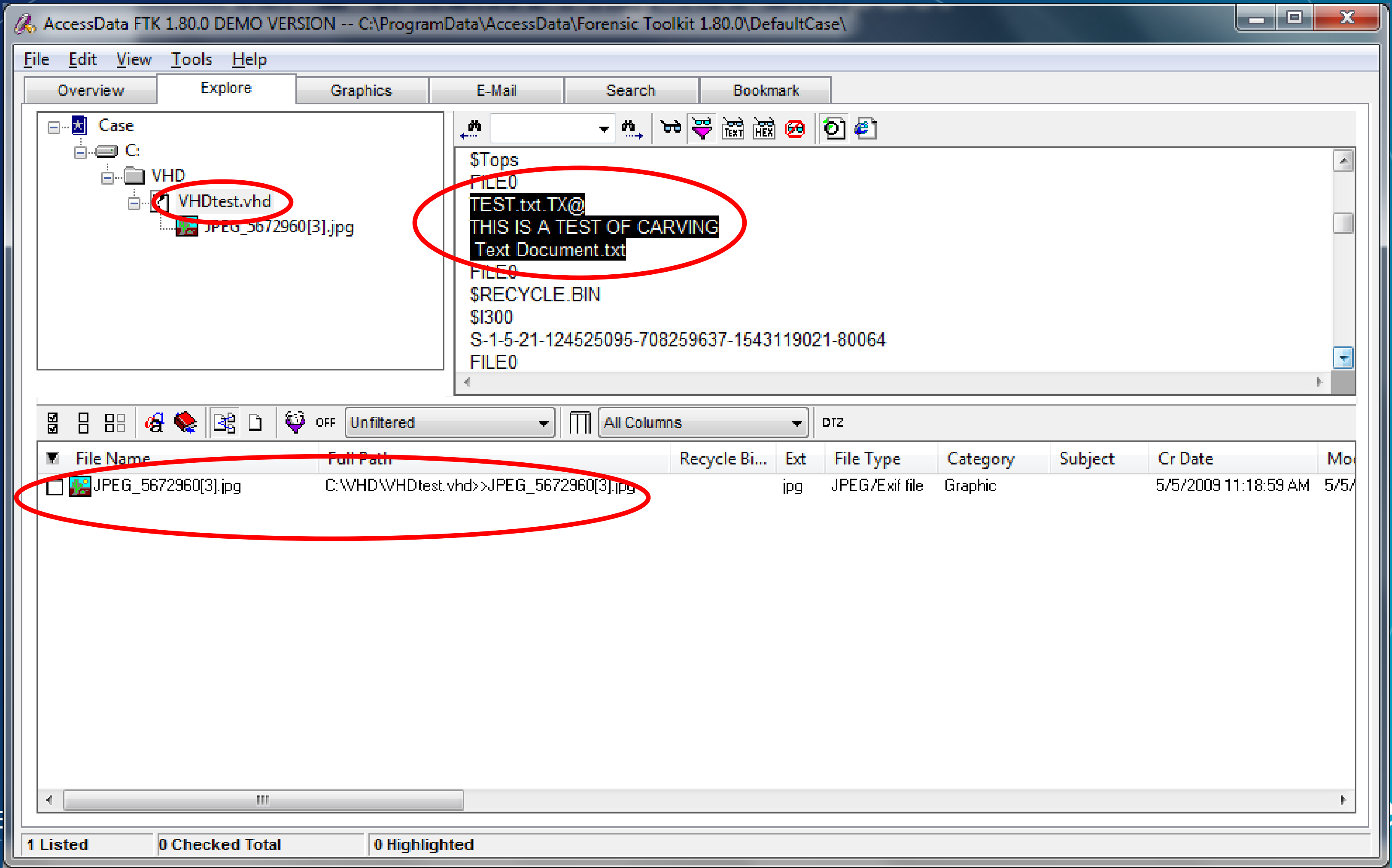
- Win7 machines may have several VHD files – backups, user created HDs, other bootable Operating systems. These may contain files critical to your case.
- Some of this data may be auto-carved via your forensic tools during examination.
- In some situations it might be useful to use the built-in ability of Win7 to mount a VHD read only to get a full view into the Virtual Hard Disk.

VHD Disk Investigative Impact

- Three methods to view data in a VHD
  - Add VHD file into FTK to be examined
  - Use built in VHD mount feature of Win7 to image the VHD after you have given it a drive letter
  - Add it into FTK as an acquired image!

VHD Disk Investigative Impact

VHD added directly into FTK



AccessData FTK 1.80.0 DEMO VERSION -- C:\ProgramData\AccessData\Forensic Toolkit 1.80.0\DefaultCase\

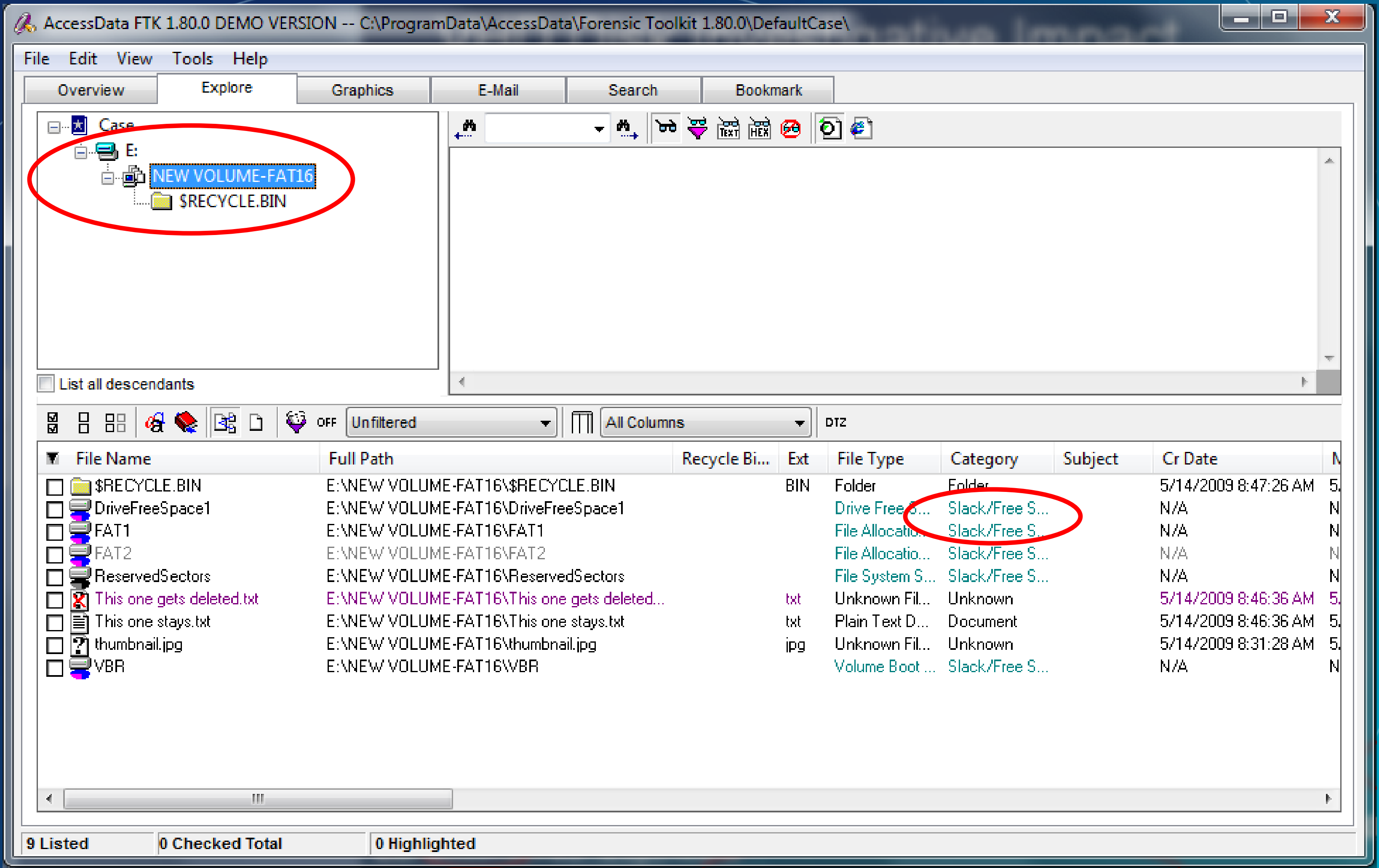
```
$Tops
FILE0
TEST.txt.TX@
THIS IS A TEST OF CARVING
 Text Document.txt
FILE0
$RECYCLE.BIN
$I300
S-1-5-21-124525095-708259637-1543119021-80064
FILE0
```

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mo
□ JPEG_5672960[3].jpg	C:\VHD\VHDtest.vhd>>JPEG_5672960[3].jpg		jpg	JPEG/Exif file	Graphic		5/5/2009 11:18:59 AM	5/5/

1 Listed | 0 Checked Total | 0 Highlighted

VHD Disk Investigative Impact

VHD mounted as a drive letter

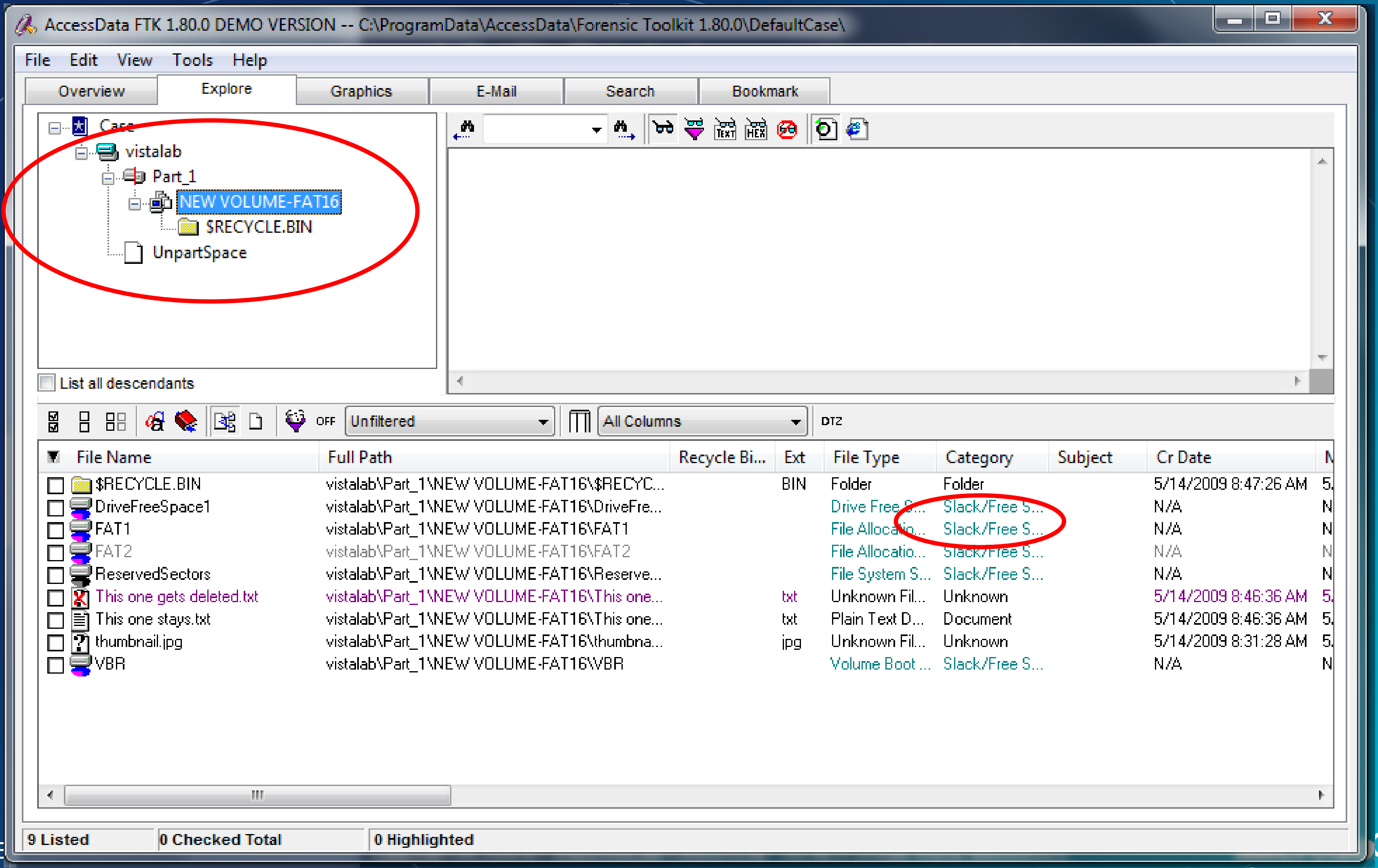


	File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	N
□	$RECYCLE.BIN	E:\NEW VOLUME-FAT16\$RECYCLE.BIN		BIN	Folder	Folder		5/14/2009 8:47:26 AM	5.
□	DriveFreeSpace1	E:\NEW VOLUME-FAT16\DriveFreeSpace1			Drive Free S...	Slack/Free S...		N/A	N
□	FAT1	E:\NEW VOLUME-FAT16\FAT1			File Allocatio...	Slack/Free S...		N/A	N
□	FAT2	E:\NEW VOLUME-FAT16\FAT2			File Allocatio...	Slack/Free S...		N/A	N
□	ReservedSectors	E:\NEW VOLUME-FAT16\ReservedSectors			File System S...	Slack/Free S...		N/A	N
□	This one gets deleted.txt	E:\NEW VOLUME-FAT16\This one gets deleted...		txt	Unknown Fil...	Unknown		5/14/2009 8:46:36 AM	5.
□	This one stays.txt	E:\NEW VOLUME-FAT16\This one stays.txt		txt	Plain Text D...	Document		5/14/2009 8:46:36 AM	5.
□	thumbnail.jpg	E:\NEW VOLUME-FAT16\thumbnail.jpg		jpg	Unknown Fil...	Unknown		5/14/2009 8:31:28 AM	5.
□	VBR	E:\NEW VOLUME-FAT16\VBR			Volume Boot ...	Slack/Free S...		N/A	N

9 Listed | 0 Checked Total | 0 Highlighted

VHD Disk Investigative Impact

VHD added as acquired image in FTK


AccessData FTK 1.80.0 DEMO VERSION -- C:\ProgramData\AccessData\Forensic Toolkit 1.80.0\DefaultCase\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
□ List all descendants
OFF
DTZ

- Case
  - vistalab
    - Part_1
      - NEW VOLUME-FAT16
        - $RECYCLE.BIN
    - UnpartSpace

Unfiltered

All Columns

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	N
□ $RECYCLE.BIN	vistalab\Part_1\NEW VOLUME-FAT16\$RECYC...		BIN	Folder	Folder		5/14/2009 8:47:26 AM	5.
□ DriveFreeSpace1	vistalab\Part_1\NEW VOLUME-FAT16\DriveFre...			Drive Free S...	Slack/Free S...		N/A	N
□ FAT1	vistalab\Part_1\NEW VOLUME-FAT16\FAT1			File Allocatio...	Slack/Free S...		N/A	N
□ FAT2	vistalab\Part_1\NEW VOLUME-FAT16\FAT2			File Allocatio...	Slack/Free S...		N/A	N
□ ReservedSectors	vistalab\Part_1\NEW VOLUME-FAT16\Reserve...			File System S...	Slack/Free S...		N/A	N
□ This one gets deleted.txt	vistalab\Part_1\NEW VOLUME-FAT16\This one...		txt	Unknown Fil...	Unknown		5/14/2009 8:46:36 AM	5.
□ This one stays.txt	vistalab\Part_1\NEW VOLUME-FAT16\This one...		txt	Plain Text D...	Document		5/14/2009 8:46:36 AM	5.
□ thumbnail.jpg	vistalab\Part_1\NEW VOLUME-FAT16\thumbna...		jpg	Unknown Fil...	Unknown		5/14/2009 8:31:28 AM	5.
□ VBR	vistalab\Part_1\NEW VOLUME-FAT16\VBR			Volume Boot ...	Slack/Free S...		N/A	N

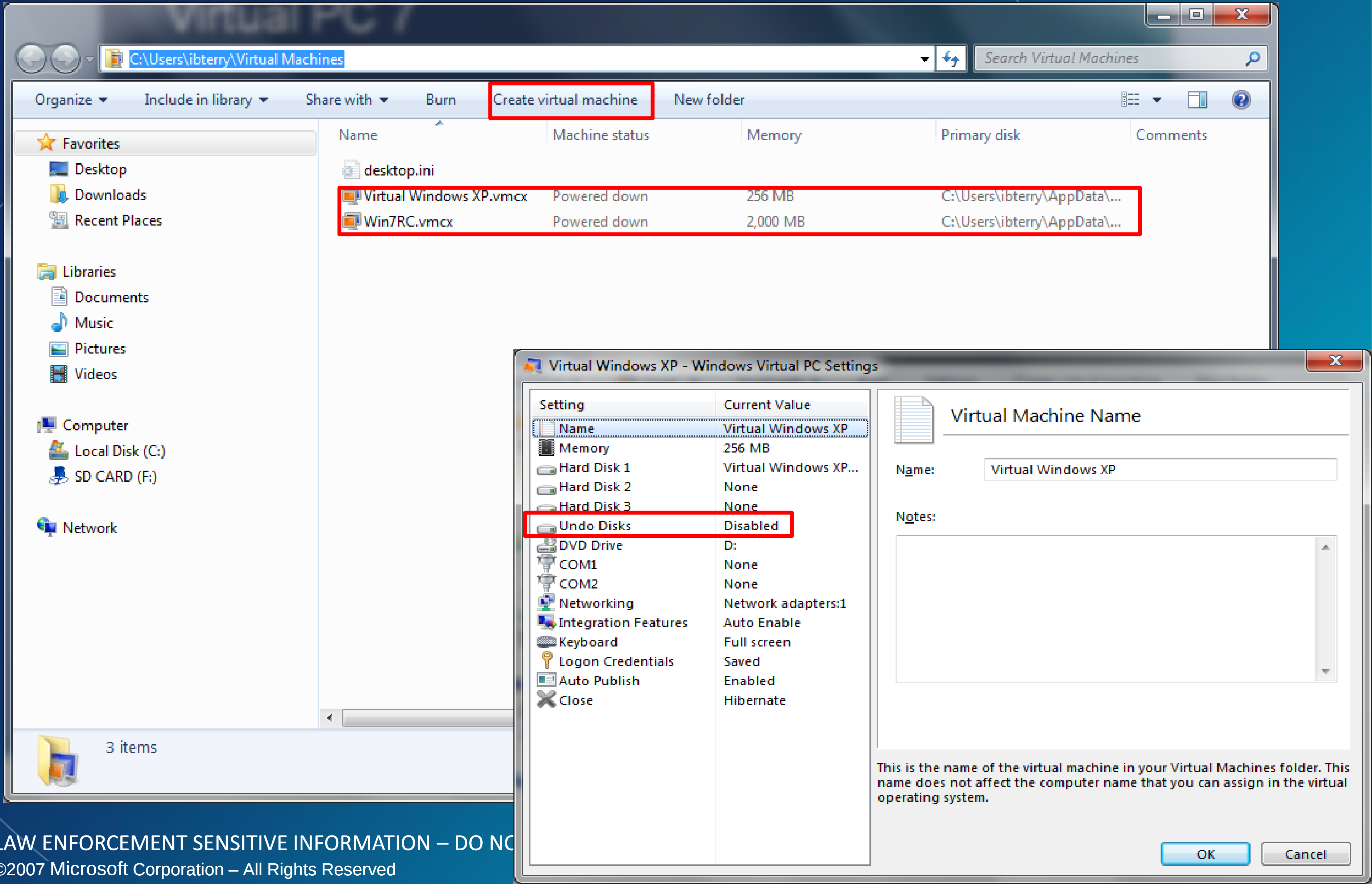
9 Listed | 0 Checked Total | 0 Highlighted

LAW E ... ces

Virtual PC 7

- Comes as separate download
- Windows 7 ONLY as host
  - Home Basic, Home Premium, Professional, Enterprise and Ultimate
- Supported GUEST operating systems
  - Windows XP, Vista and Windows 7
- Intel or AMD processor with Hardware Assisted Virtualization support required

Virtual PC 7 – User Interface



C:\Users\ibterry\Virtual Machines

Name	Machine status	Memory	Primary disk	Comments
desktop.ini				
Virtual Windows XP.vmcx	Powered down	256 MB	C:\Users\ibterry\AppData\...	
Win7RC.vmcx	Powered down	2,000 MB	C:\Users\ibterry\AppData\...	

Virtual Windows XP - Windows Virtual PC Settings

Setting	Current Value
Name	Virtual Windows XP
Memory	256 MB
Hard Disk 1	Virtual Windows XP...
Hard Disk 2	None
Hard Disk 3	None
Undo Disks	Disabled
DVD Drive	D:
COM1	None
COM2	None
Networking	Network adapters:1
Integration Features	Auto Enable
Keyboard	Full screen
Logon Credentials	Saved
Auto Publish	Enabled
Close	Hibernate

Virtual Machine Name

Name: Virtual Windows XP

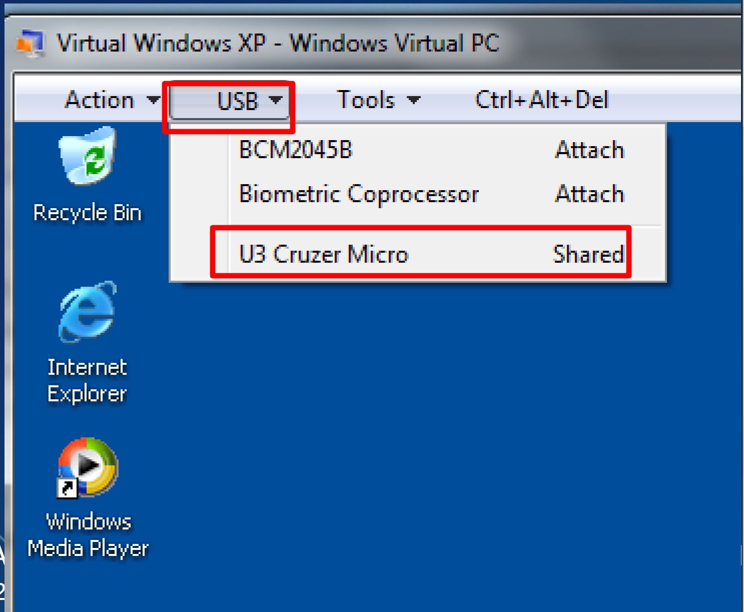
Notes:

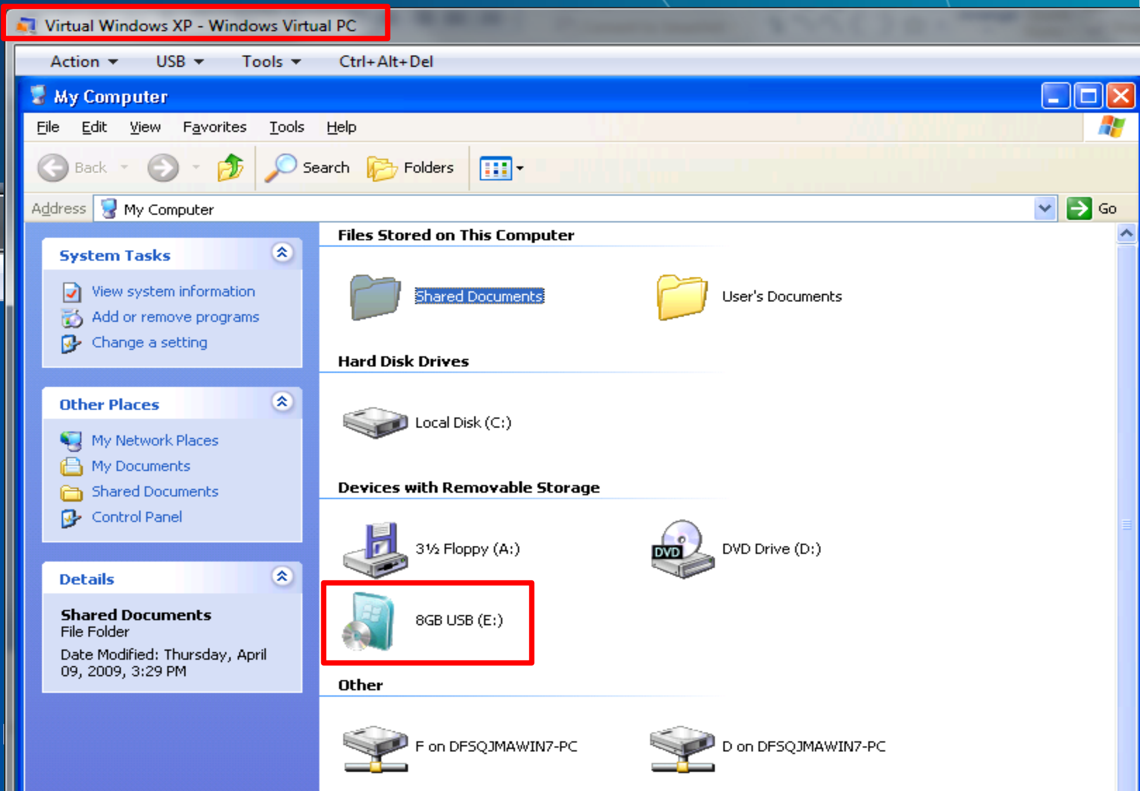
This is the name of the virtual machine in your Virtual Machines folder. This name does not affect the computer name that you can assign in the virtual operating system.

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NC

Virtual PC 7

- Allows running of multiple operating systems on host computer for testing, and compatibility
- USB Support in guest operating system!





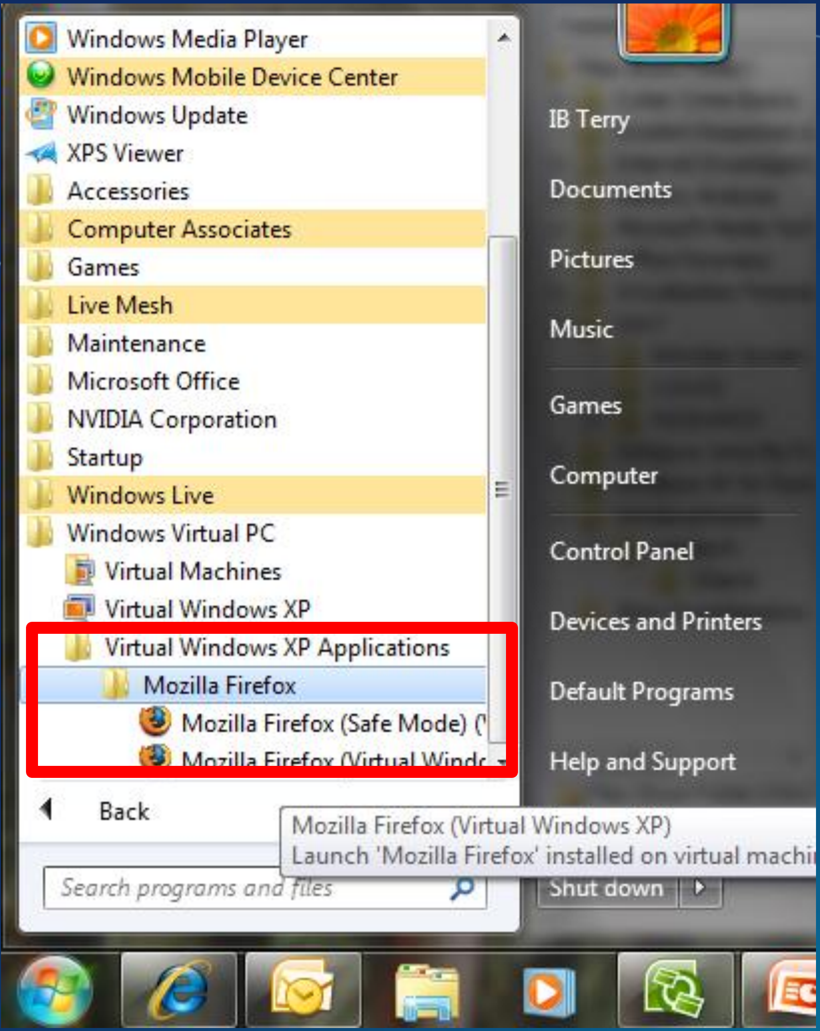
Windows XP Compatibility Mode

- Feature of Virtual PC
- Only available on Windows 7 Professional, Enterprise and Ultimate
- Guest must be Windows XP Professional SP 3

Windows XP Compatibility Mode

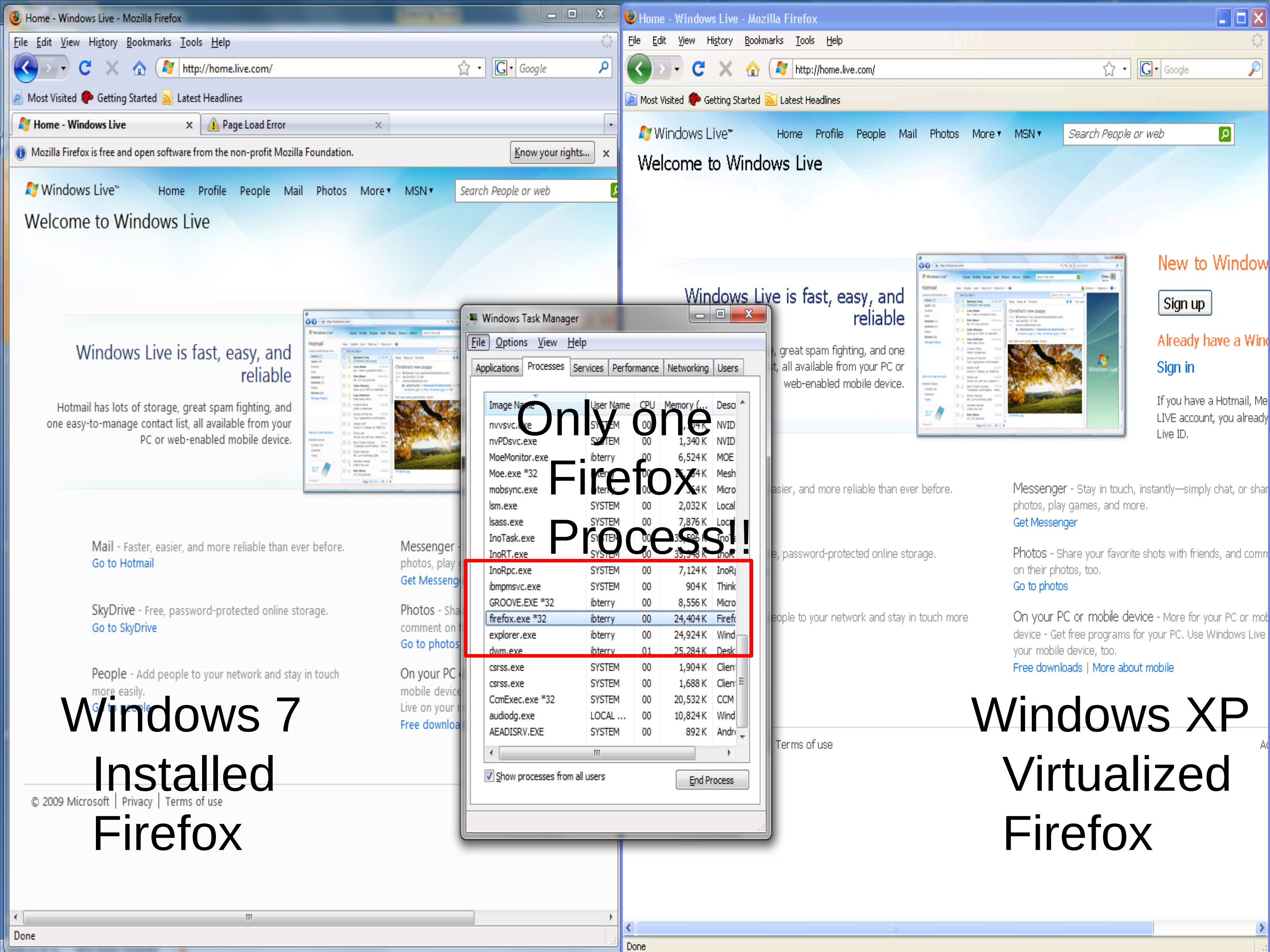
- Runs under Virtual PC 7
- Windows XP VHD you install applications into
- Application is published in the Windows 7 Start Menu
- When you run application it is running in XP VHD, BUT it appears to you to just be an application running in your Windows 7
- Allows you to run applications not compatible with Windows 7, in Windows 7

Windows XP Compatibility Mode



Mozilla Firefox (Virtual Windows XP)
Launch 'Mozilla Firefox' installed on virtual machi

- Firefox web browser was installed in guest XP virtual machine.
- Shortcut to Firefox was automatically added to the host Windows 7 machine running Virtual PC.
- Once running it looks like any other execution of Firefox



Home - Windows Live - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://home.live.com/
Google
Most Visited Getting Started Latest Headlines
Home - Windows Live
Page Load Error
Know your rights...
Windows Live
Home Profile People Mail Photos More MSN
Search People or web
Done

Mozilla Firefox is free and open software from the non-profit Mozilla Foundation.

Welcome to Windows Live

Windows Live is fast, easy, and reliable

Hotmail has lots of storage, great spam fighting, and one easy-to-manage contact list, all available from your PC or web-enabled mobile device.

Mail - Faster, easier, and more reliable than ever before.
Go to Hotmail

SkyDrive - Free, password-protected online storage.
Go to SkyDrive

People - Add people to your network and stay in touch more easily.
Go to people

Messenger - Stay in touch, instantly—simply chat, or share photos, play games, and more.
Get Messenger

Photos - Share your favorite shots with friends, and comment on their photos, too.
Go to photos

On your PC or mobile device - More for your PC or mobile device - Get free programs for your PC. Use Windows Live on your mobile device, too.
Free downloads | More about mobile

© 2009 Microsoft | Privacy | Terms of use

New to Windows

Sign up

Already have a Wind

Sign in

If you have a Hotmail, Me LIVE account, you already Live ID.

Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users

Image Name	User Name	CPU	Memory (...	Desc
nvvsvc.exe	SYSTEM	00	[illegible]	NVID
nvPDsvc.exe	SYSTEM	00	1,340 K	NVID
MoeMonitor.exe	ibterry	00	6,524 K	MOE
Moe.exe *32	[illegible]	00	[illegible]	Mesh
mobsync.exe	[illegible]	00	[illegible]	Micro
lsm.exe	SYSTEM	00	2,032 K	Local
lsass.exe	SYSTEM	00	7,876 K	Local
InoTask.exe	SYSTEM	00	[illegible]	InoT
InoRT.exe	SYSTEM	00	[illegible]	InoR
InoRpc.exe	SYSTEM	00	7,124 K	InoR
ibmpmsvc.exe	SYSTEM	00	904 K	Think
GROOVE.EXE *32	ibterry	00	8,556 K	Micro
firefox.exe *32	ibterry	00	24,404 K	Firef
explorer.exe	ibterry	00	24,924 K	Wind
dwm.exe	ibterry	01	25,284 K	Desk
csrss.exe	SYSTEM	00	1,904 K	Client
csrss.exe	SYSTEM	00	1,688 K	Client
CcmExec.exe *32	SYSTEM	00	20,532 K	CCM
audiodg.exe	LOCAL ...	00	10,824 K	Wind
AEADISRV.EXE	SYSTEM	00	892 K	Andr

☑ Show processes from all users

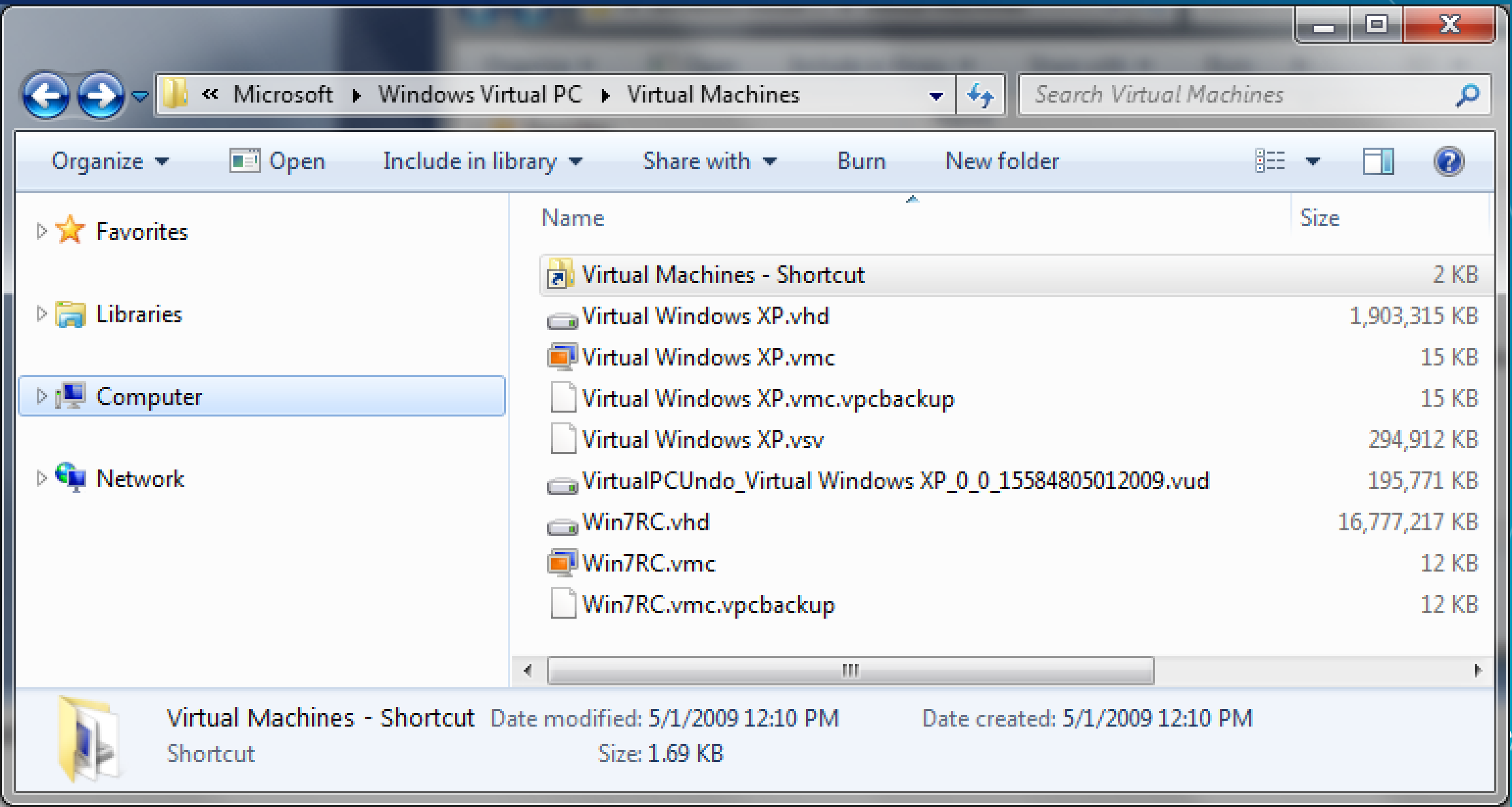
Only one Firefox Process!!

Windows 7 Installed Firefox

Windows XP Virtualized Firefox

Windows XP Compatibility Mode

- Default location for Virtual machines is
  - C:\Users\<username>\AppData\Local\Microsoft\Windows Virtual PC\Virtual Machines



Name	Size
Virtual Machines - Shortcut	2 KB
Virtual Windows XP.vhd	1,903,315 KB
Virtual Windows XP.vmc	15 KB
Virtual Windows XP.vmc.vpcbackup	15 KB
Virtual Windows XP.vsv	294,912 KB
VirtualPCUndo_Virtual Windows XP_0_0_15584805012009.vud	195,771 KB
Win7RC.vhd	16,777,217 KB
Win7RC.vmc	12 KB
Win7RC.vmc.vpcbackup	12 KB

Virtual Machines - Shortcut Date modified: 5/1/2009 12:10 PM Date created: 5/1/2009 12:10 PM
Shortcut Size: 1.69 KB

Windows XP Compatibility Mode – Undo Disks

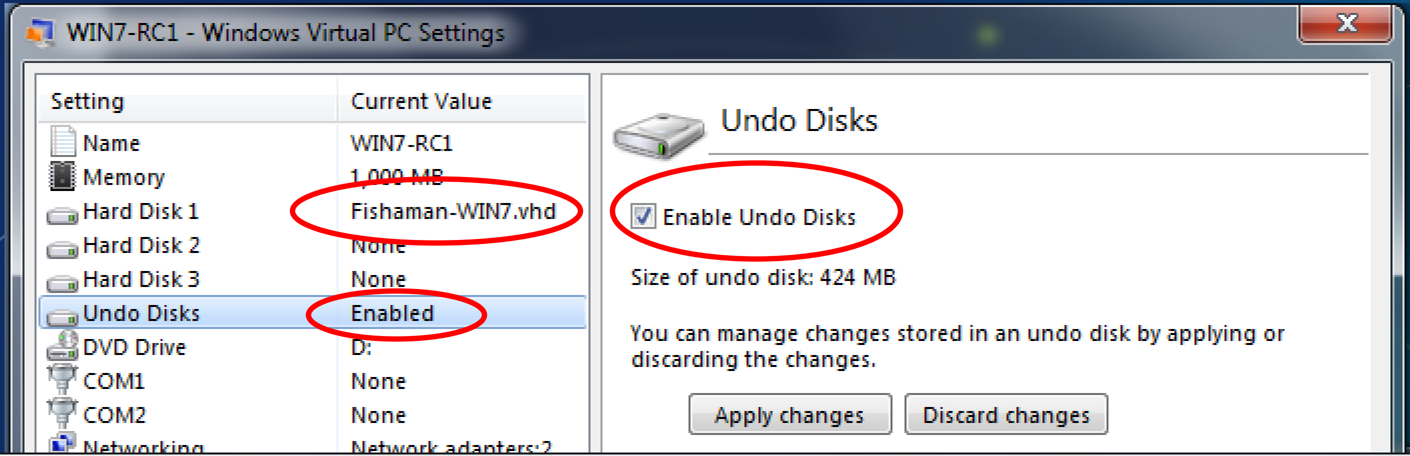
Virtual PC Undo Disks

- UNDO - to make of no effect or as if not done : make null : reverse. Merriam-Webster
- This is a great feature for Information Technology professionals – aids in testing and deployment of new services and applications
- Could potentially cause difficulties for forensic examiners.

Virtual PC Undo Disks

- If the Enable undo disks option is selected for a virtual machine, any changes made during a virtual machine session are saved to an undo disk (.vud) file. An undo disk file is a temporary file and is separate from the virtual hard disk. When the virtual machine is closed, the changes stored in the undo disk can be deleted, committed to the virtual hard disk file, or saved until a later time.

Virtual PC Undo Disks



WIN7-RC1 - Windows Virtual PC Settings

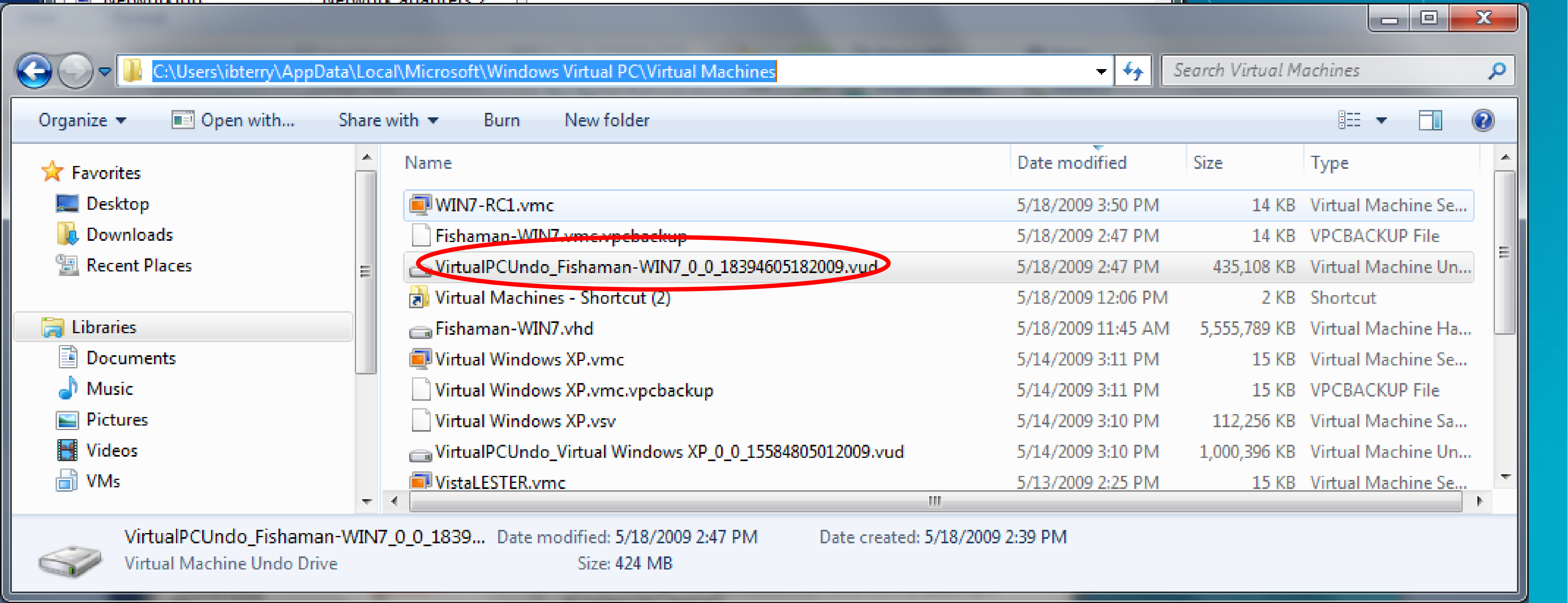
Setting	Current Value
Name	WIN7-RC1
Memory	1,000 MB
Hard Disk 1	Fishaman-WIN7.vhd
Hard Disk 2	None
Hard Disk 3	None
Undo Disks	Enabled
DVD Drive	D:
COM1	None
COM2	None
Networking	Network adapters:2

Undo Disks

☑ Enable Undo Disks

Size of undo disk: 424 MB

You can manage changes stored in an undo disk by applying or discarding the changes.

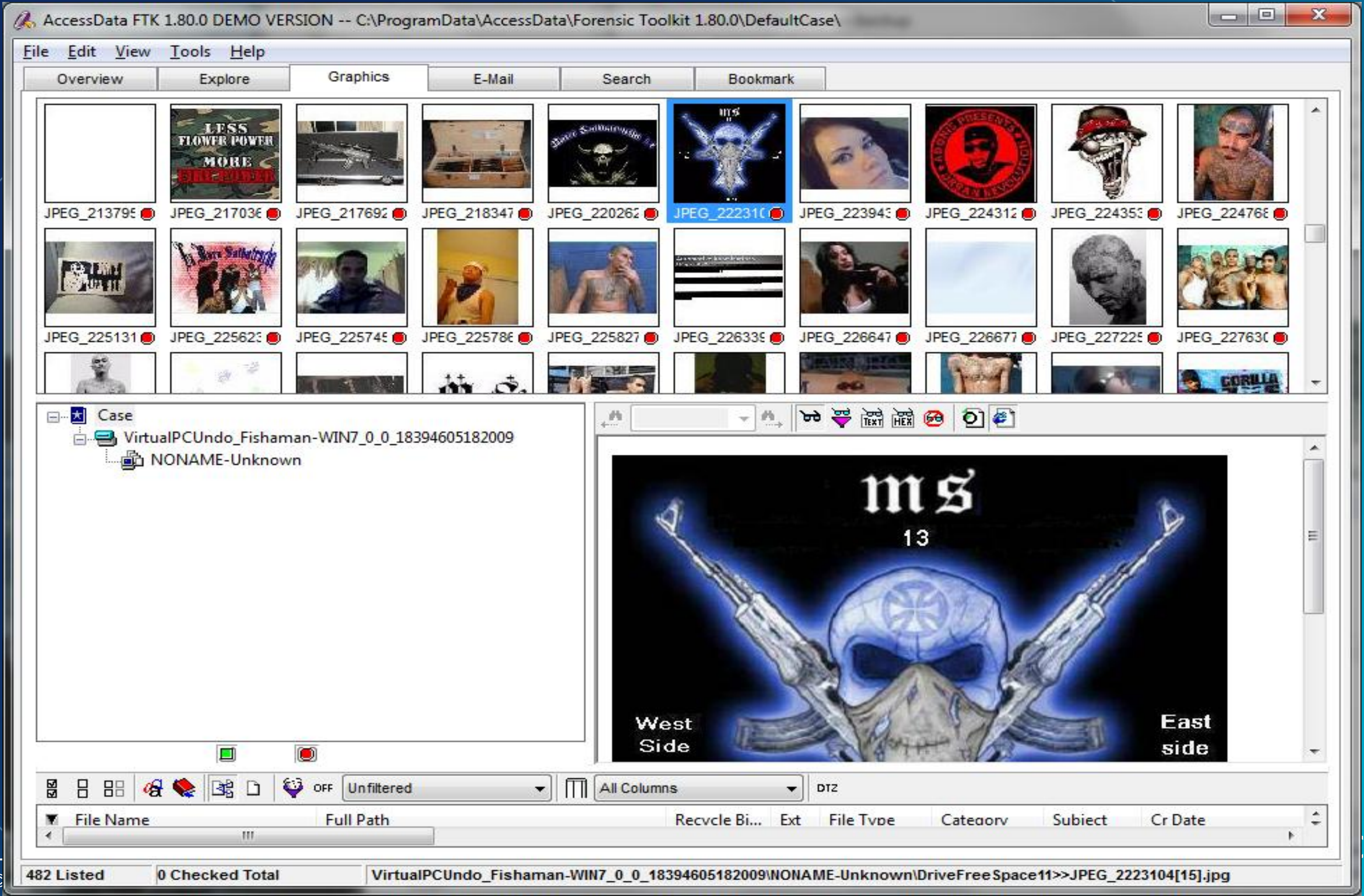


C:\Users\ibterry\AppData\Local\Microsoft\Windows Virtual PC\Virtual Machines

Name	Date modified	Size	Type
WIN7-RC1.vmc	5/18/2009 3:50 PM	14 KB	Virtual Machine Se...
Fishaman-WIN7.vmc.vpcbackup	5/18/2009 2:47 PM	14 KB	VPCBACKUP File
VirtualPCUndo_Fishaman-WIN7_0_0_18394605182009.vud	5/18/2009 2:47 PM	435,108 KB	Virtual Machine Un...
Virtual Machines - Shortcut (2)	5/18/2009 12:06 PM	2 KB	Shortcut
Fishaman-WIN7.vhd	5/18/2009 11:45 AM	5,555,789 KB	Virtual Machine Ha...
Virtual Windows XP.vmc	5/14/2009 3:11 PM	15 KB	Virtual Machine Se...
Virtual Windows XP.vmc.vpcbackup	5/14/2009 3:11 PM	15 KB	VPCBACKUP File
Virtual Windows XP.vsv	5/14/2009 3:10 PM	112,256 KB	Virtual Machine Sa...
VirtualPCUndo_Virtual Windows XP_0_0_15584805012009.vud	5/14/2009 3:10 PM	1,000,396 KB	Virtual Machine Un...
VistaLESTER.vmc	5/13/2009 2:25 PM	15 KB	Virtual Machine Se...

VirtualPCUndo_Fishaman-WIN7_0_0_1839... Date modified: 5/18/2009 2:47 PM Date created: 5/18/2009 2:39 PM
Virtual Machine Undo Drive Size: 424 MB

Virtual PC Undo Disks – Carved in FTK



AccessData FTK 1.80.0 DEMO VERSION -- C:\ProgramData\AccessData\Forensic Toolkit 1.80.0\DefaultCase\

Case
VirtualPCUndo_Fishaman-WIN7_0_0_18394605182009
NONAME-Unknown

482 Listed | 0 Checked Total | VirtualPCUndo_Fishaman-WIN7_0_0_18394605182009\NONAME-Unknown\DriveFreeSpace11>>JPEG_2223104[15].jpg

L

©

ces

Virtual PC Undo Disks

- How can you tell if a Virtual Machine has undo disk enabled?
  - Each virtual machine has a .VMC configuration file. – Located in folder with VHD usually
  - This file contains the setting for the machine such as

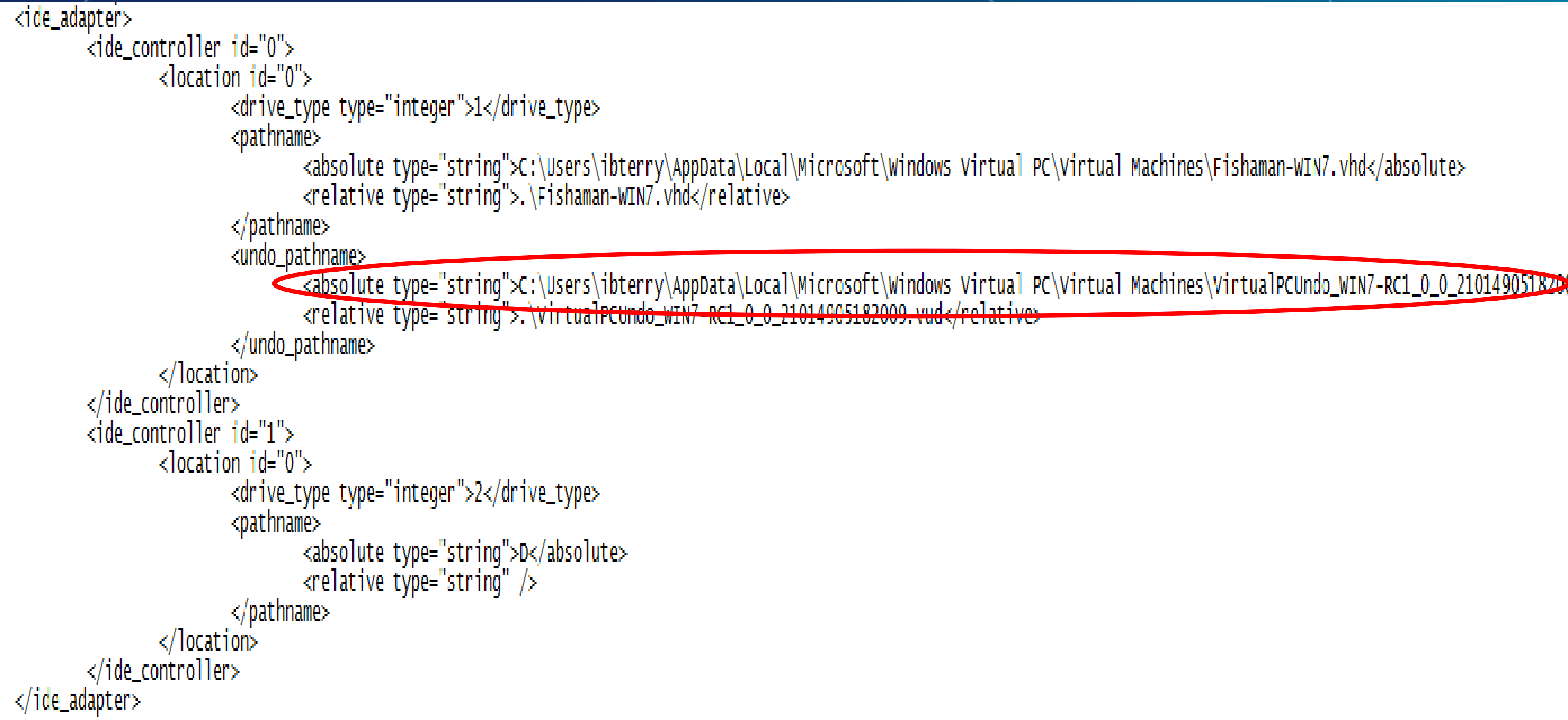
    >Memory Allocated

    >Hard Drive, Path to the VHD file

    > Network setting

    >Undo Disks!

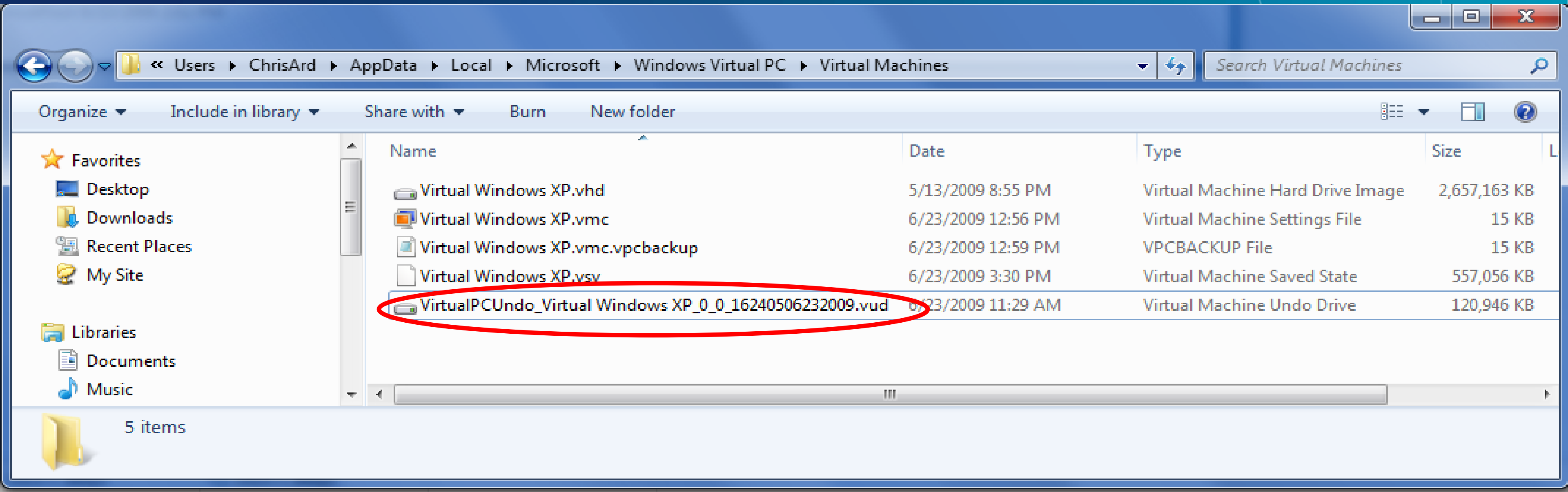
Virtual PC Undo Disks – VMC edited in notepad



```
<ide_adapter>
        <ide_controller id="0">
                <location id="0">
                        <drive_type type="integer">1</drive_type>
                        <pathname>
                                <absolute type="string">C:\Users\ibterry\AppData\Local\Microsoft\Windows Virtual PC\Virtual Machines\Fishaman-WIN7.vhd</absolute>
                                <relative type="string">.\Fishaman-WIN7.vhd</relative>
                        </pathname>
                        <undo_pathname>
                                <absolute type="string">C:\Users\ibterry\AppData\Local\Microsoft\Windows Virtual PC\Virtual Machines\VirtualPCUndo_WIN7-RC1_0_0_21014905182
                                <relative type="string">.\VirtualPCUndo_WIN7-RC1_0_0_21014905182009.vud</relative>
                        </undo_pathname>
                </location>
        </ide_controller>
        <ide_controller id="1">
                <location id="0">
                        <drive_type type="integer">2</drive_type>
                        <pathname>
                                <absolute type="string">D</absolute>
                                <relative type="string" />
                        </pathname>
                </location>
        </ide_controller>
</ide_adapter>
```

VPC Undo Disk Investigative Impact

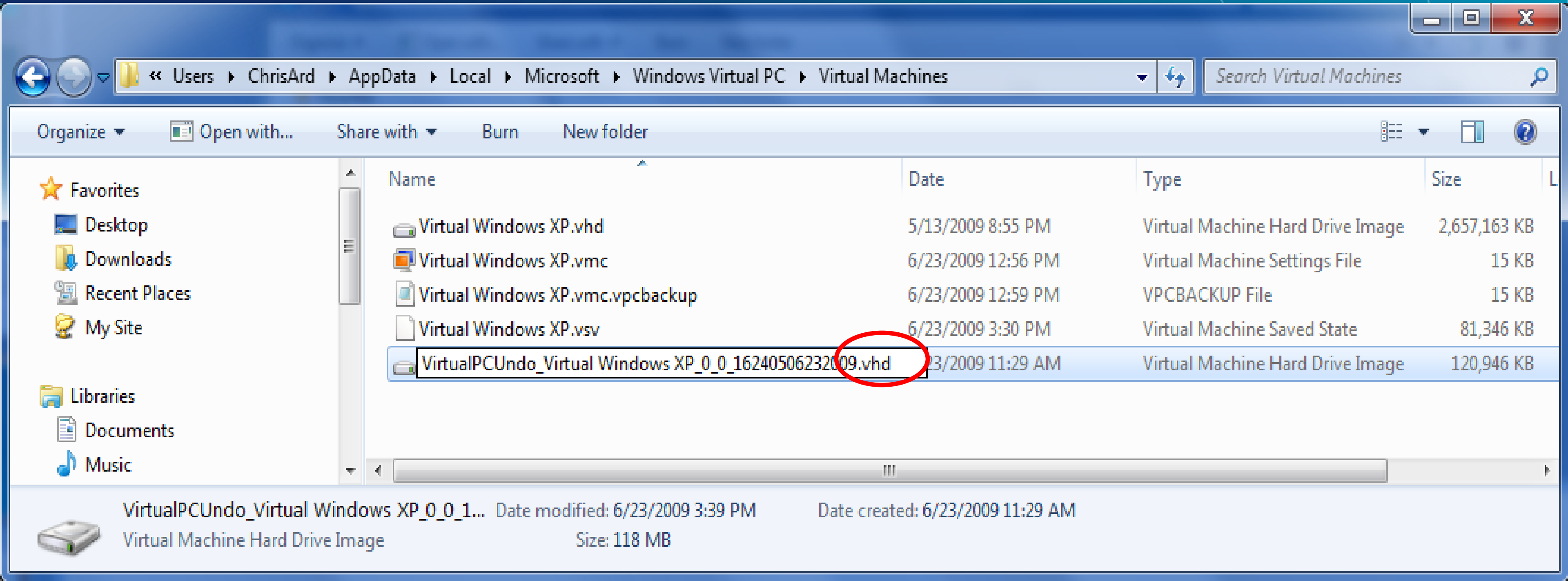
- Is there an easy way to parse or carve the contents of the VUD file?
  - Data Carving will have limited success and can be very time intensive
- What if “Discard Changes” has been selected?



Name	Date	Type	Size
Virtual Windows XP.vhd	5/13/2009 8:55 PM	Virtual Machine Hard Drive Image	2,657,163 KB
Virtual Windows XP.vmc	6/23/2009 12:56 PM	Virtual Machine Settings File	15 KB
Virtual Windows XP.vmc.vpcbackup	6/23/2009 12:59 PM	VPCBACKUP File	15 KB
Virtual Windows XP.vsv	6/23/2009 3:30 PM	Virtual Machine Saved State	557,056 KB
VirtualPCUndo_Virtual Windows XP_0_0_16240506232009.vud	6/23/2009 11:29 AM	Virtual Machine Undo Drive	120,946 KB

Parsing the VUD File

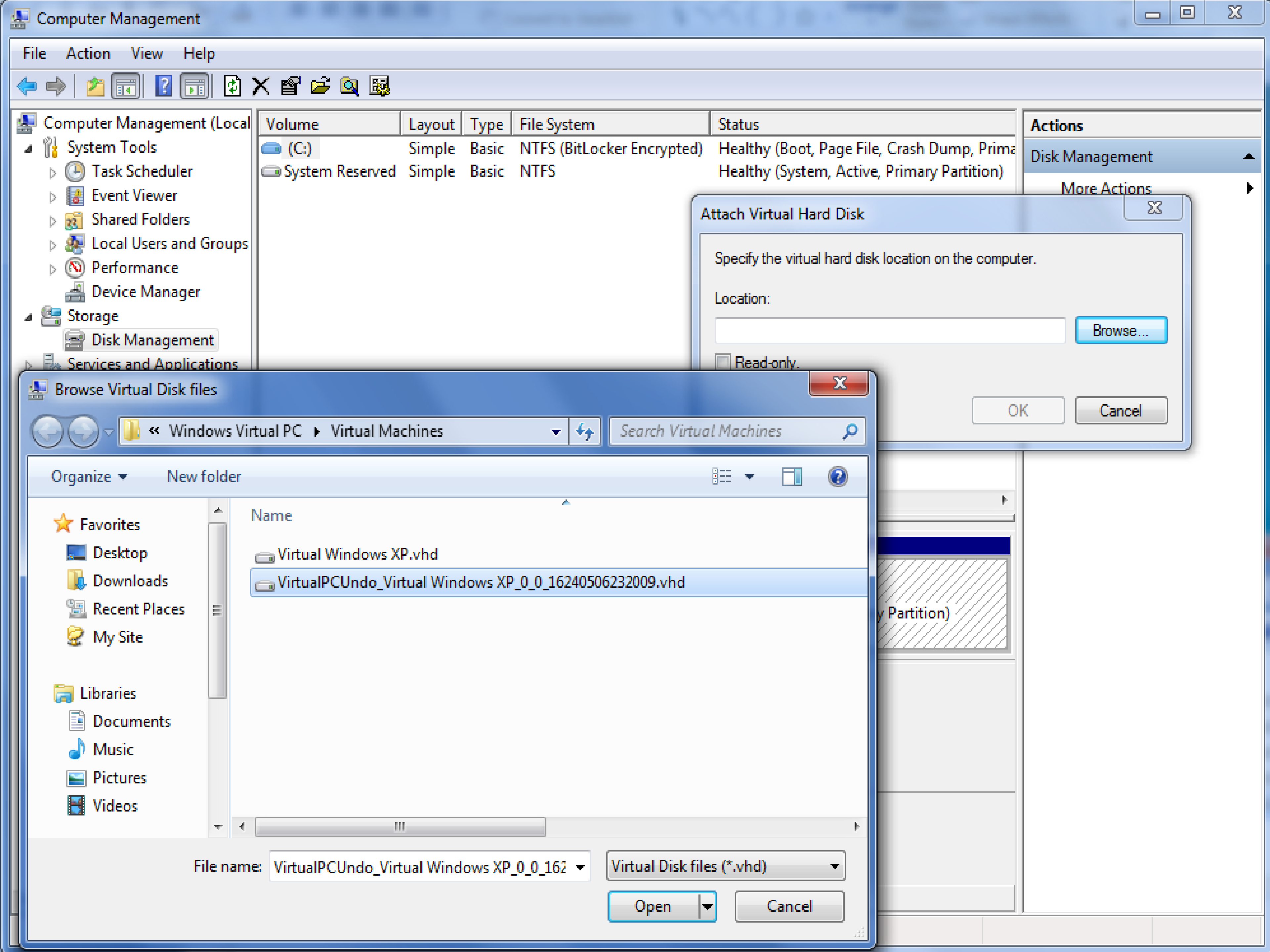
- VHD files are just files that look like disk volumes
- I wonder if VUD files are the same thing…..
- If they are, couldn't I just rename a VUD to VHD?



« Users ▸ ChrisArd ▸ AppData ▸ Local ▸ Microsoft ▸ Windows Virtual PC ▸ Virtual Machines

Name	Date	Type	Size
Virtual Windows XP.vhd	5/13/2009 8:55 PM	Virtual Machine Hard Drive Image	2,657,163 KB
Virtual Windows XP.vmc	6/23/2009 12:56 PM	Virtual Machine Settings File	15 KB
Virtual Windows XP.vmc.vpcbackup	6/23/2009 12:59 PM	VPCBACKUP File	15 KB
Virtual Windows XP.vsv	6/23/2009 3:30 PM	Virtual Machine Saved State	81,346 KB
VirtualPCUndo_Virtual Windows XP_0_0_16240506232009.vhd	6/23/2009 11:29 AM	Virtual Machine Hard Drive Image	120,946 KB

VirtualPCUndo_Virtual Windows XP_0_0_1... Date modified: 6/23/2009 3:39 PM Date created: 6/23/2009 11:29 AM
Virtual Machine Hard Drive Image Size: 118 MB



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS (BitLocker Encrypted)	Healthy (Boot, Page File, Crash Dump, Prima
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)

Specify the virtual hard disk location on the computer.

Location:

□ Read-only

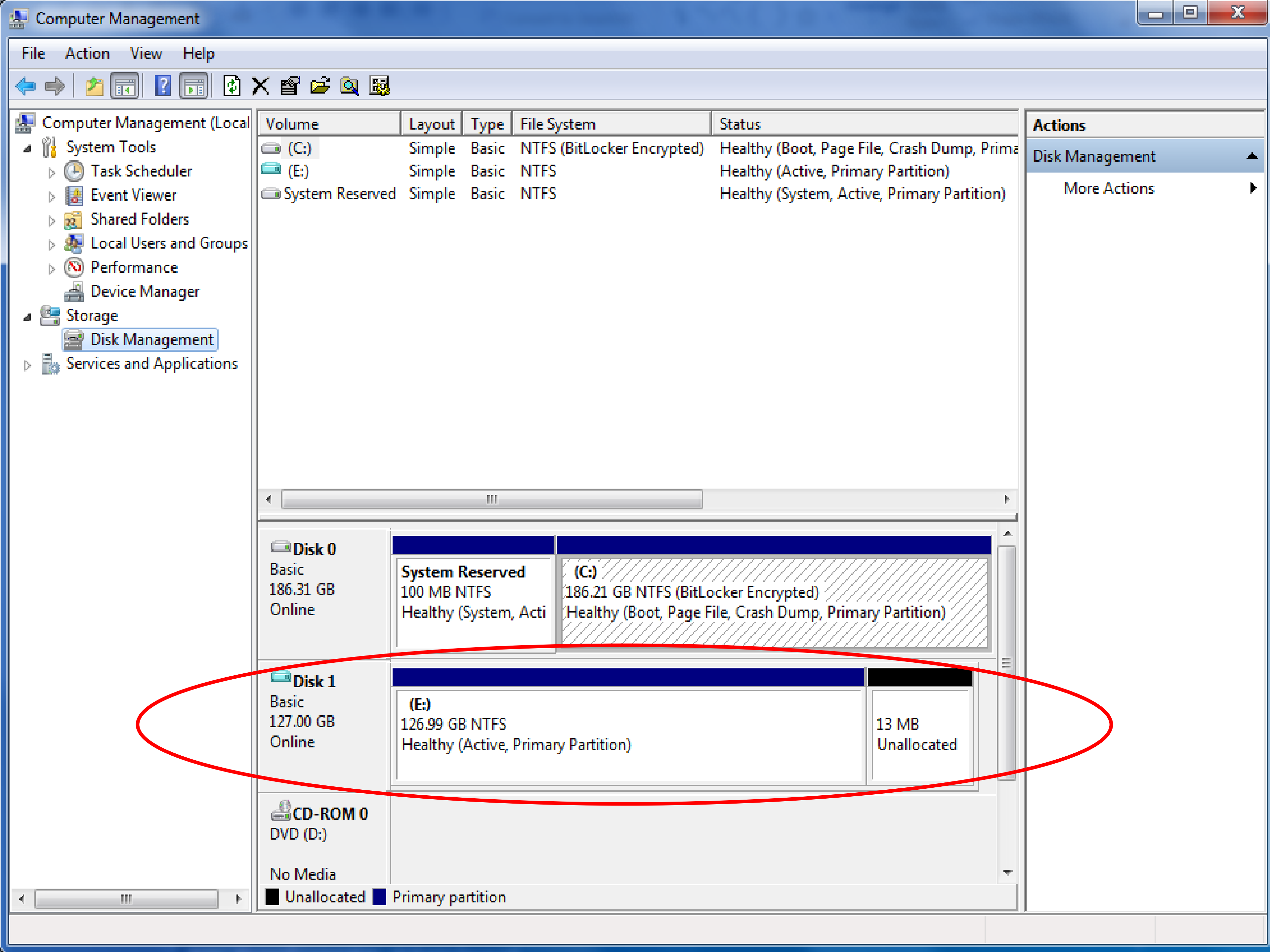
Name

Virtual Windows XP.vhd

VirtualPCUndo_Virtual Windows XP_0_0_16240506232009.vhd

File name: VirtualPCUndo_Virtual Windows XP_0_0_162

Virtual Disk files (*.vhd)



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS (BitLocker Encrypted)	Healthy (Boot, Page File, Crash Dump, Prima
(E:)	Simple	Basic	NTFS	Healthy (Active, Primary Partition)
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)

Disk 0
Basic
186.31 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Acti

(C:)
186.21 GB NTFS (BitLocker Encrypted)
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
127.00 GB
Online

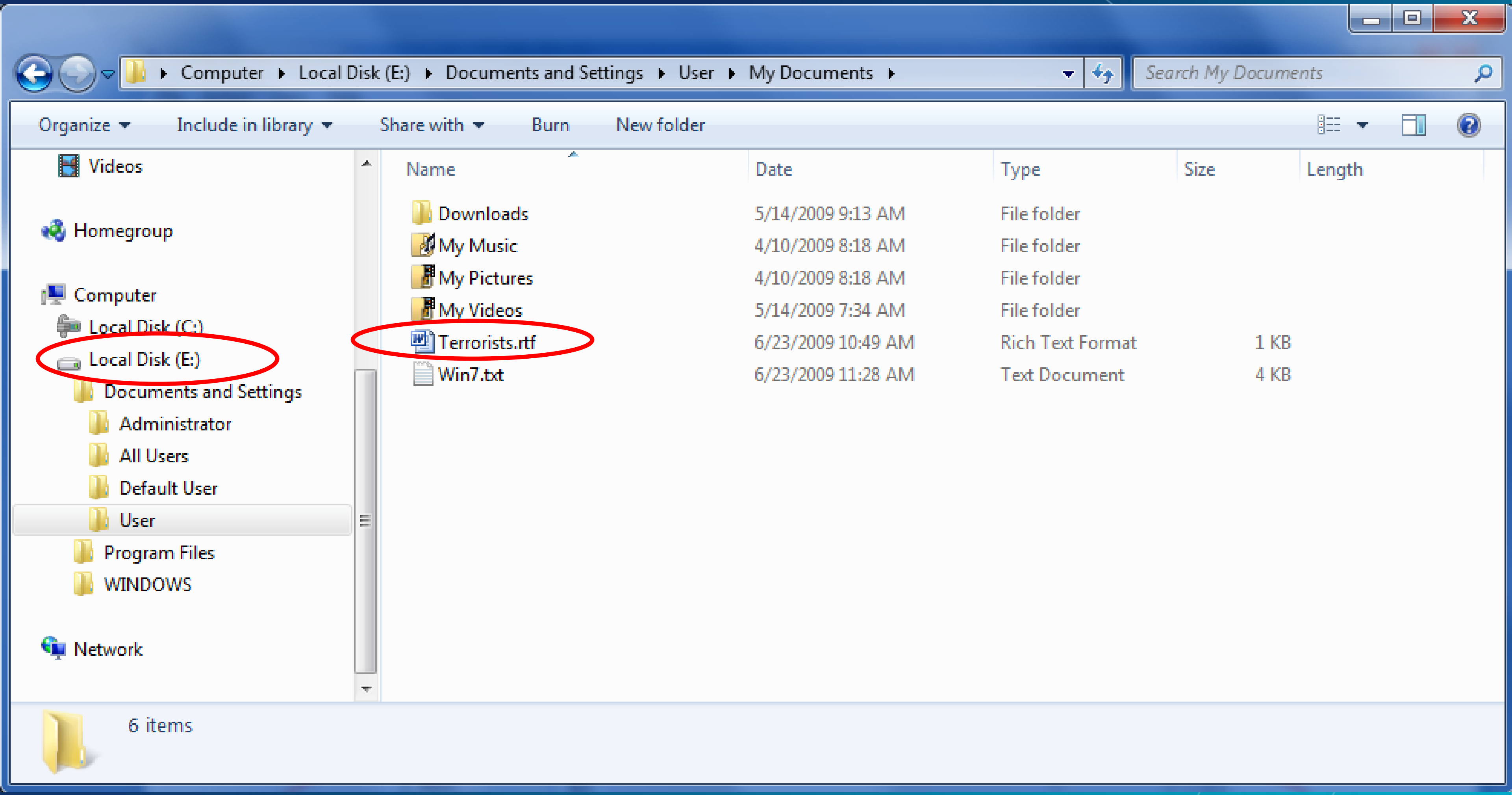
(E:)
126.99 GB NTFS
Healthy (Active, Primary Partition)

13 MB
Unallocated

CD-ROM 0
DVD (D:)

No Media

■ Unallocated ■ Primary partition



Name	Date	Type	Size	Length
Downloads	5/14/2009 9:13 AM	File folder		
My Music	4/10/2009 8:18 AM	File folder		
My Pictures	4/10/2009 8:18 AM	File folder		
My Videos	5/14/2009 7:34 AM	File folder		
Terrorists.rtf	6/23/2009 10:49 AM	Rich Text Format	1 KB	
Win7.txt	6/23/2009 11:28 AM	Text Document	4 KB	

Virtual PC Memory of hibernated virtual machines

- One feature of VPC is to allow for the state of a Virtual machine to be saved
- When the Virtual Machine is in the saved state the status information(memory) is written to a .VSV file
- These VSV files *MAY* contain information about programs that were executing when the machine was put into the saved state.

VPC Investigative Impact

Questions?

Virtulization Primer

Term	Description
VPC	Windows Virtual PC
VHD	Virtual Hard Disk. ; File containing the complete contents and structure representing a Hard Disk Drive. Used to store the virtual operating system and the associated data.
OS	Operating System
Host	The physical computer on which the virtual machine is running. It implies the OS that is installed on the physical computer.
Guest	This is the OS installed in the virtual machine
VM	Virtual Machine
Integration Features	Set of features that enable integration between Guest and the Host; namely sharing clipboard, drives, printers, smart card connected to the host, with the guest.
Integration Components	Integration Components needs to be installed on the Virtual Machine in order to enable Integration Features. It also enables seamless movement of mouse between the host and the guest. If Integration Components are not installed, the mouse pointer will get captured by the virtual machine and one needs to press Ctrl-Alt-LeftArrow to release the mouse pointer back to the Host
VM Window	This is the UI in which the Guest OS runs. This window has a toolbar of its own for common VM operations like Closing, Hibernating, Installing/Updating Integration Components etc
Saved Credentials	The user credentials of a VM can be saved. If you choose to save the credentials, then VPC will not prompt for user credentials. It will just use the saved credentials for logging-in to the VM.
Virtual Desktop	The desktop of the guest OS
Virtual Application	A guest application that is run from Windows 7 host machine and behaves like a native Windows 7 application

Virtulization Primer – Disk Terms

- ***Dynamic Disk***

  The size of the dynamic virtual hard disk expands as data is written to it. The initial size is typically less than 100 KB, but as data is written the disk size will expand until it reaches the limit specified when the disk was created.

- ***Fixed Disk***

  The size of the virtual hard disk is fixed to the size specified when the disk was created. It immediately uses the amount of space specified when it was created. The size of a fixed-size virtual hard disk cannot be changed after the virtual hard disk is created.

Virtulization Primer – Disk Terms

- ***Differencing Disk***

  The differencing virtual hard disk is a virtual hard disk associated with another virtual hard disk. One way to understand the relationship between the two disks is a parent-child analogy. The differencing disk is the child and the associated virtual disk is the parent. The differencing disk (the child) stores a record of all changes made to the parent disk and provides a way to save changes without altering the parent disk. The differencing hard disk expands dynamically as data is written to it. Microsoft recommends that you write-protect or lock the parent disk. Otherwise, if the parent disk is modified by some other process, all differencing disks related to it become invalid, and any data written to them is effectively lost.

Virtulization Primer – Disk Terms

- ***Undo Disk***

  If the Enable undo disks option is selected for a virtual machine, any changes made during a virtual machine session are saved to an undo disk (.vud) file. An undo disk file is a temporary file and is separate from the virtual hard disk. When the virtual machine is closed, the changes stored in the undo disk can be deleted, committed to the virtual hard disk file, or saved until a later time.