Win74n6

or, "Shh - It's Vista"

Justin Hall
CBTS

Meet the new boss...

Lots of hype about Windows 7 - "Safer, Simpler, More Stable"

Rave reviews from geek media

Businesses plan to jump straight from Windows XP to 7

Image Acquisition

Encase, FTK and F-Response all ***claim*** to acquire images from Windows 7 machines

All will run from Windows 7 except FTK Enterprise - Oracle DB component doesn't support 7 yet (v3.02 will)

Filesystem

Windows 7 continues to use NTFS 5.1, adds support for exFAT

NTFS 5.1 is the 'same' as XP and Vista - basic structure remains the same

Backwards compatible, but OS adds layers of features, such as...

Volume Shadow Copy

Introduced in Windows Server 2003

Incremental backups of files, folders, even entire drives - changes archived daily

Allows investigators to access earlier copy of data - including deleted / modified files

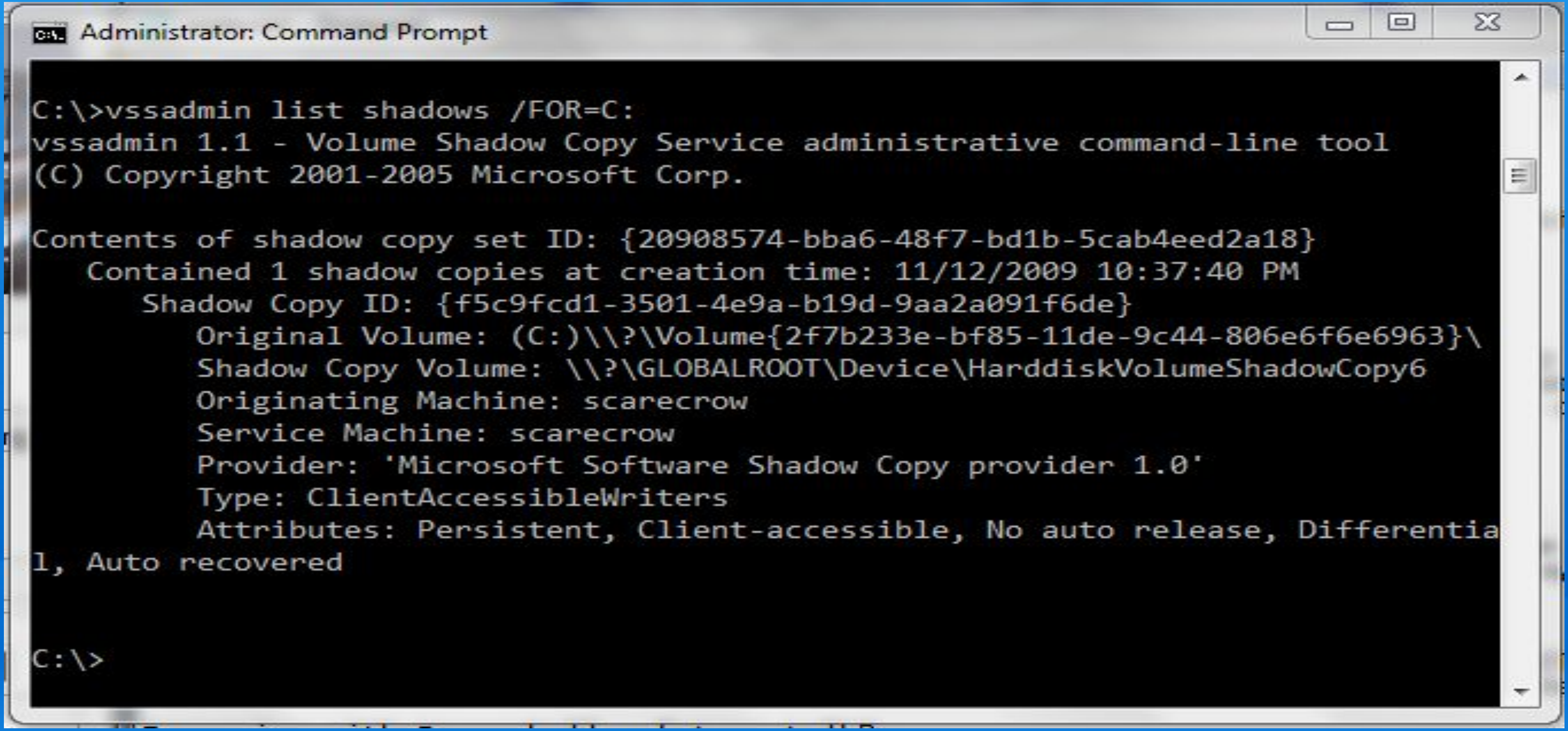
Requires physical drive - standard image of volume will not contain shadow data

Use vssadmin tool to get access to shadow data

Vssadmin

List shadow copy data available

Mount or duplicate image of shadow data like you would a standard volume



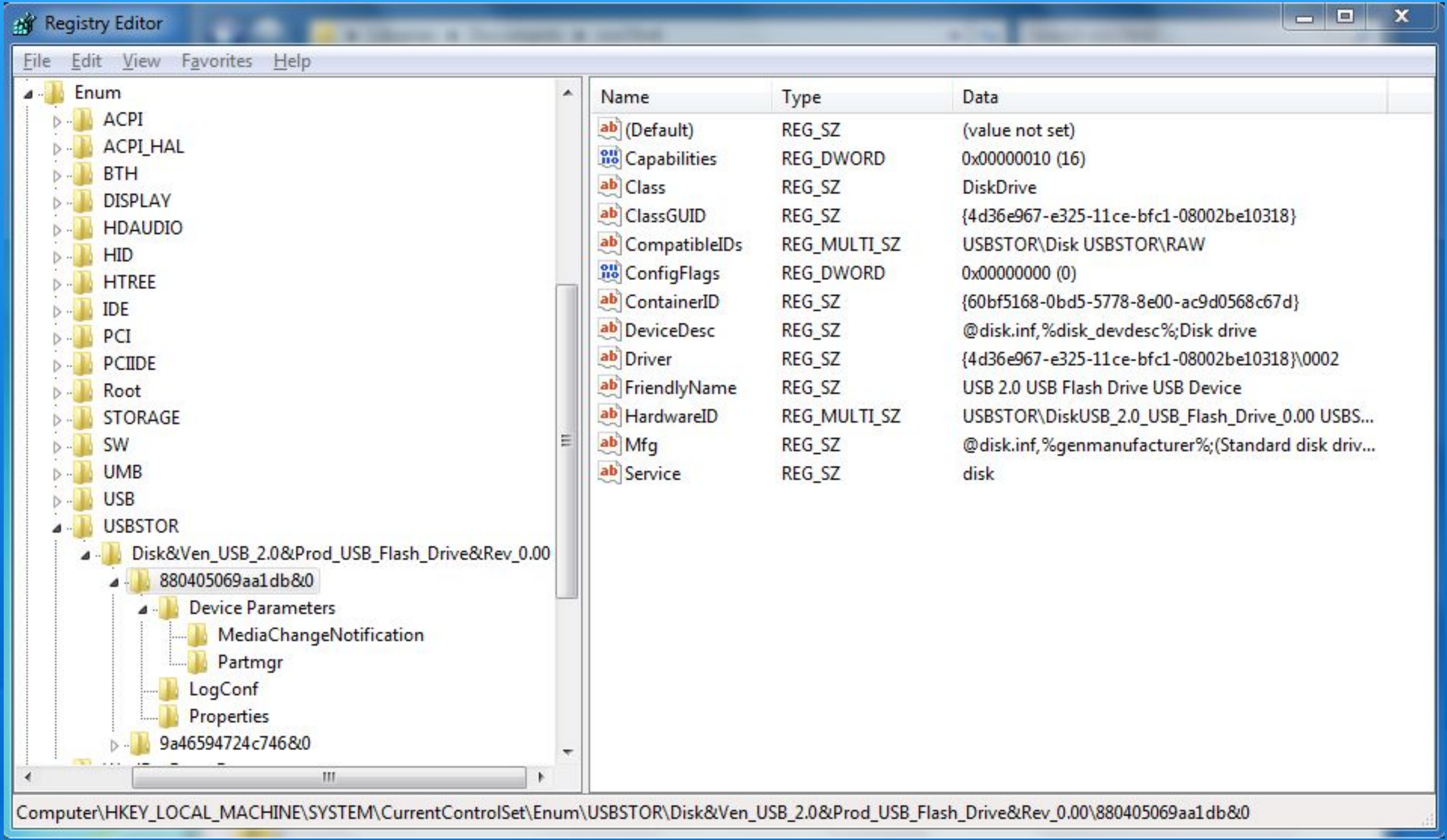
```
C:\>vssadmin list shadows /FOR=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Contents of shadow copy set ID: {20908574-bba6-48f7-bd1b-5cab4eed2a18}
   Contained 1 shadow copies at creation time: 11/12/2009 10:37:40 PM
      Shadow Copy ID: {f5c9fcd1-3501-4e9a-b19d-9aa2a091f6de}
         Original Volume: (C:)\\?\Volume{2f7b233e-bf85-11de-9c44-806e6f6e6963}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6
         Originating Machine: scarecrow
         Service Machine: scarecrow
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-accessible, No auto release, Differentia
l, Auto recovered


C:\>
```

USB Removable Media

No substantial changes from Vista's architecture



```
Enum
  ACPI
  ACPI_HAL
  BTH
  DISPLAY
  HDAUDIO
  HID
  HTREE
  IDE
  PCI
  PCIIDE
  Root
  STORAGE
  SW
  UMB
  USB
  USBSTOR
    Disk&Ven_USB_2.0&Prod_USB_Flash_Drive&Rev_0.00
      880405069aa1db&0
        Device Parameters
          MediaChangeNotification
          Partmgr
        LogConf
        Properties
      9a46594724c746&0
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{60bf5168-0bd5-5778-8e00-ac9d0568c67d}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0002
FriendlyName	REG_SZ	USB 2.0 USB Flash Drive USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskUSB_2.0_USB_Flash_Drive_0.00 USBS...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk driv...
Service	REG_SZ	disk

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_USB_2.0&Prod_USB_Flash_Drive&Rev_0.00\880405069aa1db&0

USB Removable Media

What USB devices are on the system?

HKLM\SYSTEM\CurrentControlSet\Enum\USBStor

HKLM\SYSTEM\CurrentControlSet\Enum\USB

What user used the devices?

HKCU (or HKU)\Software\Microsoft\Windows\CV\Explorer\MountPoints2

When was the device installed?

%WINDIR%\inf\setupapi.dev.log

Browsing

Windows 7 ships with Internet Explorer 8

Includes InPrivate - browsing mode that doesn't record history
Can be disabled using GPO or Registry key
HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Privacy\EnableInPrivateMode = "00000001"

By default IE runs in "Protected" mode - prevents code from web (and exploits) from executing with elevated privileges

Browsing

Browser artifacts retrieved in Protected mode are stored in "Low" folders

%USERPROFILE%\AppData\Local\Microsoft\Windows\History\Low\History.IE5

Caveats - Protected mode must be enabled (duh)
- UAC must be enabled
- User cannot be local administrator

Live Analysis

Sysinternals - supported, most tools re-released w/Windows 7 support since public beta in January
Logparser - logs from Windows 7 are supported
GNU Win32 ports - supported

Memory analysis - dd, kntdd, mdd, win[32,64]dd, Memoryze, FastDump PRO, winen, nigilant32
(Limitations on access to \Device\PhysicalMemory after Windows Server 2003 SP1)

Netstat, Reg, Tasklist, SC, netsh, diskpart, etc are bundled with OS

WMIC and Powershell pre-installed for advanced queries

References

SANS Forensics Blog - forensics.sans.org

Forensics Wiki - forensicswiki.org

Harlan Carvey's Blog - windowsir.blogspot.com

WFA/2e (not updated for Windows 7 but a good list of tools)

Questions?

Thanks for listening!
justin.hall@cbts.cinbell.com