Internet Security Systems

The Secrets Of Registry Analysis Revealed

Obligatory Joke

There are 10 kinds of people in this world…those who understand binary, and those who don't.

“Allow myself to introduce…myself”

- **Admin Stuff**
  - Why are we here?
  - Expectations
- **Please…ask questions**
- **Breaks, as necessary**

Purpose

Discuss the structure of the Windows Registry, and the details of Registry Analysis

- What secrets does the Registry hold?
- What do we mean by calling the Registry a “log file”?

Key Concepts

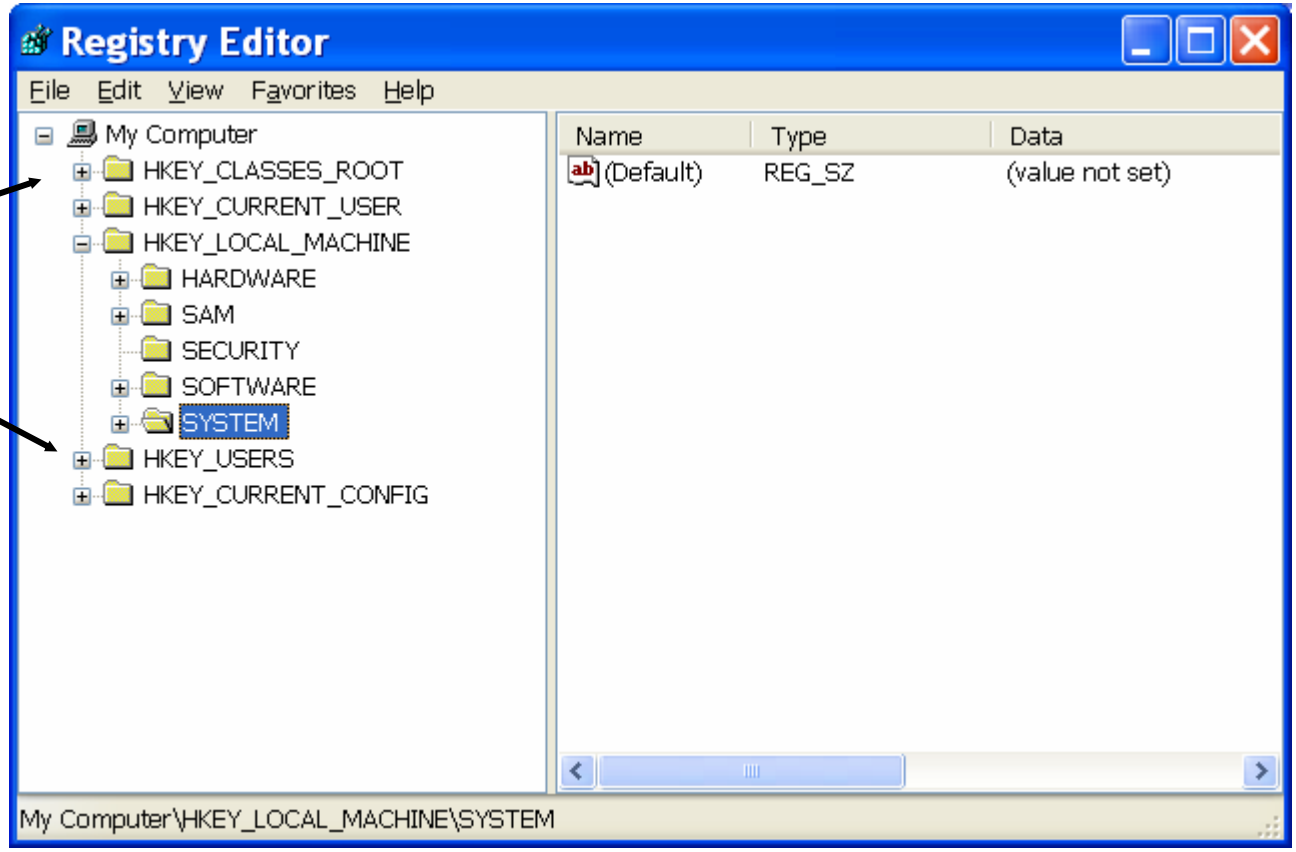
- **Locard's Exchange Principle**
  - Applies to intruder, but also to investigators interacting with live systems
  - Where we do leave "footprints"?
- **Artifacts**
  - The key is to know/understand how artifacts (Registry keys, values, data) are created and/or modified
  - We know where to look for artifacts
  - We know that ***the absence of an artifact is itself an artifact***
- **Focus will be on Registry for Windows 2000, XP, 2003, and to some extent, Vista**

What is the Registry?

- **Binary hierarchal database**
  - Based on nodes (key, value) and pointers to other structures
- **Replaces INI files from Win3.x**
- **Consists of several hives**
  - HKEY_LOCAL_MACHINE\System
  - HKEY_LOCAL_MACHINE\Software
  - HKEY_LOCAL_MACHINE\SAM
  - HKEY_LOCAL_MACHINE\Security
  - HKEY_USERS\.Default
- **Hives exist as files on the system (system32\config)**

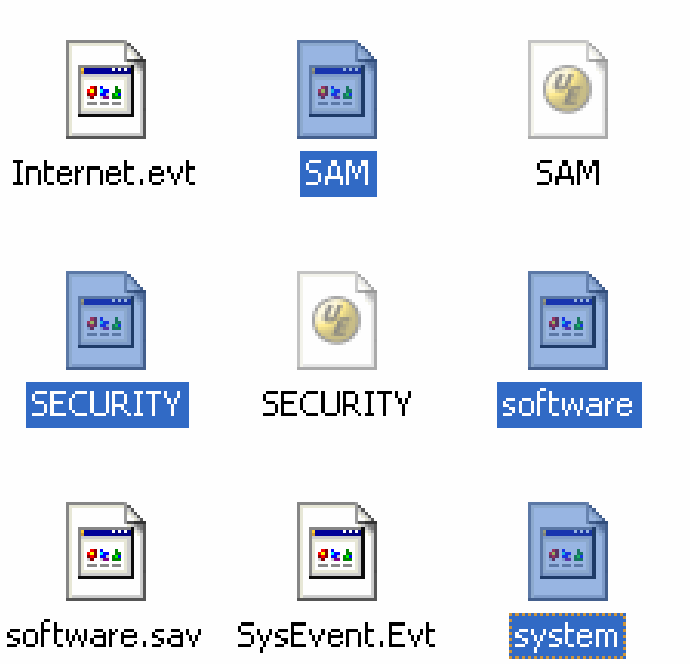
Registry Hives

Hives

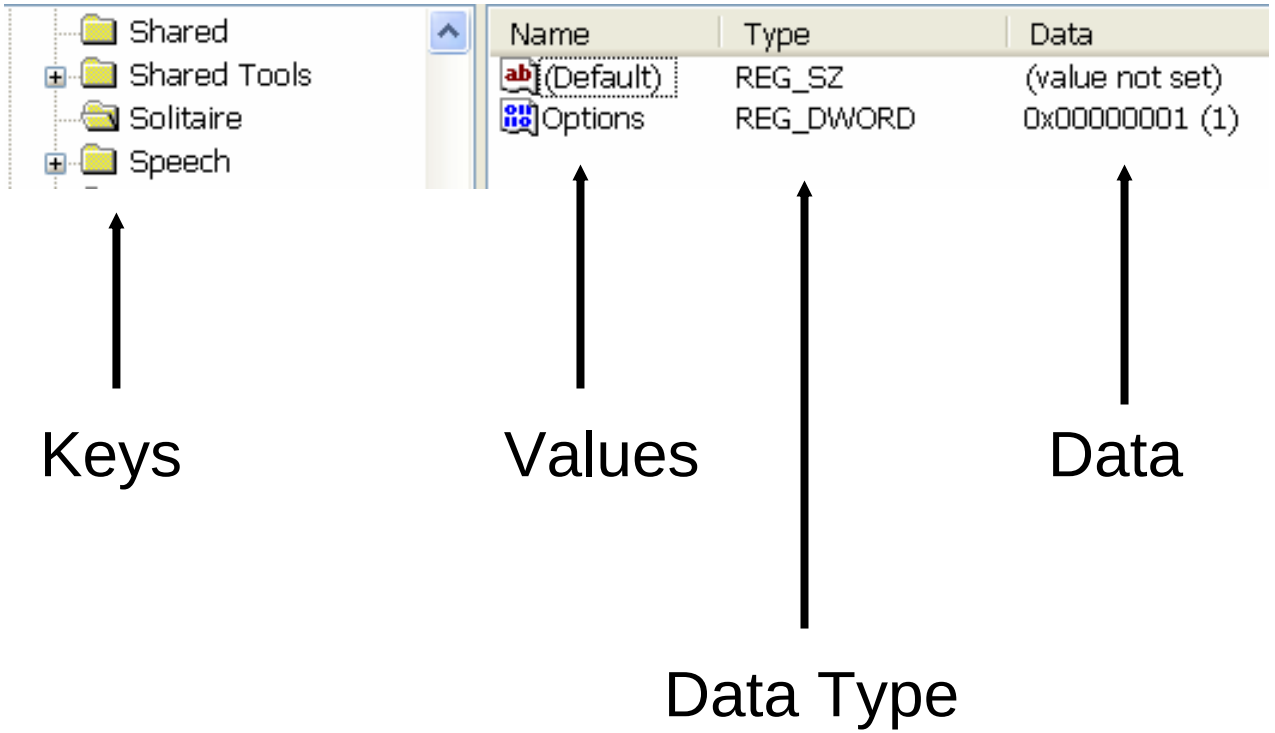


What is the Registry?

- **Hives can be found on disk**
  - system32\config dir; System, Software, SAM, etc.
  - NTUSER.DAT file in the user's profile
  - Does not include "volatile" hives, such as "CurrentControlSet", HKLM\Hardware, HKEY_CURRENT_USER, etc.



Registry Structure Nomenclature



Registry Key – Binary Structure

```
12 00 00 00 0D 0A 00 00 A0 FF FF FF 6E 6B 20 00 ; ........ ÿÿÿnk .
3C A8 E1 E7 98 84 C4 01 00 00 00 00 20 00 00 00 ; <¨áç˜„Ä..... ...
04 00 00 00 00 00 00 00 B0 1F 0A 00 FF FF FF FF ; ........°...ÿÿÿÿ
00 00 00 00 FF FF FF FF 18 02 00 00 FF FF FF FF ; ....ÿÿÿÿ....ÿÿÿÿ
24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; $...............
00 00 00 00 0D 00 00 00 43 6F 6E 74 72 6F 6C 53 ; ........ControlS
65 74 30 30 31 63 BF 81 E0 FE FF FF 73 6B 00 00 ; et001c¿□àþÿÿsk..
E8 21 21 00 28 E9 06 00 4F 10 00 00 04 01 00 00 ; è!!.(é..O.......
01 00 04 84 E8 00 00 00 F8 00 00 00 00 00 00 00 ; ...„è...ø.......
```

Key “header” is 76 bytes long, followed by the name of the key

LastWrite Time: 3C A8 E1 E7 98 84 C4 01

Number of Subkeys: 4

Number of Values: 0

Key Name: ControlSet001 (length = 0x0D, or 13 characters)

Registry Value – Binary Structure

```
F8 FF FF FF 28 1A 00 00 D0 FF FF FF 76 6B 18 00 ; øÿÿÿ(...Ðÿÿÿvk..
0C 00 00 00 18 04 00 00 01 00 00 00 01 00 00 00 ; ................
57 61 69 74 54 6F 4B 69 6C 6C 53 65 72 76 69 63 ; WaitToKillServic
65 54 69 6D 65 6F 75 74 F0 FF FF FF 32 00 30 00 ; eTimeoutðÿÿÿ2.0.
30 00 30 00 30 00 00 00 F0 FF FF FF 18 E9 07 00 ; 0.0.0...ðÿÿÿ.é..
```

Value “header” is 20 bytes; followed by name (length 0x18 or 24 bytes)

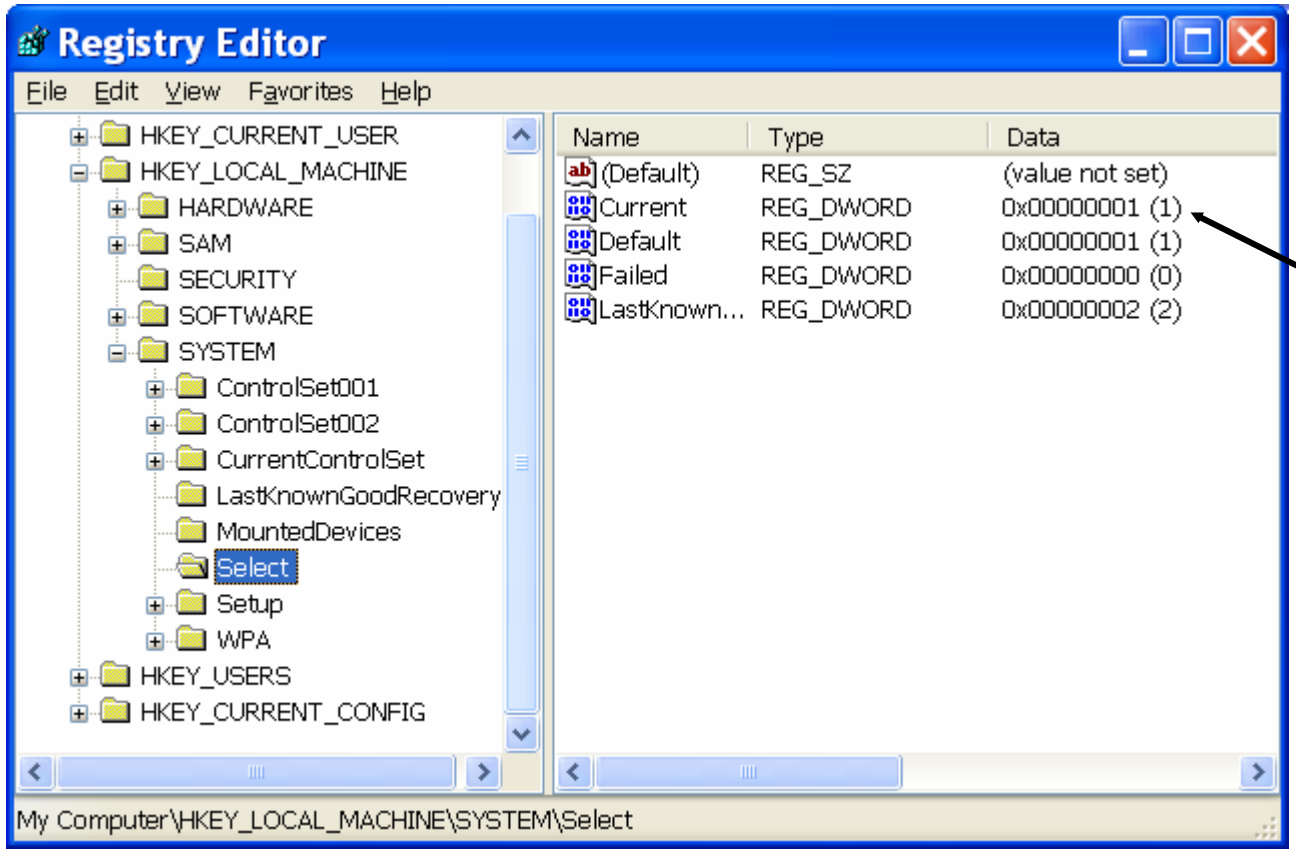
No timestamp value

Data type: 0x01, or REG_SZ

What can we find in the Registry?

- **System Stuff - configuration settings**
  - Application settings
    - Download directories (P2P applications)
    - Recently accessed files (images, movies, etc.)
  - AutoStart locations
    - Applications that start w/ little or **NO** user interaction
- **User Stuff**
  - Attached USB devices (thumb drives, ext HDD, digital cameras, etc.)
  - User activity
    - MRUs
    - Viewed documents or images
    - Applications installed or launched (UserAssist keys)

NOTE: Locating the CurrentControlSet



Current

Extracting/correlating data from the Registry

- **Access Methods/Scenarios**
  - Live response
    - Reg.exe, Perl (Win32::TieRegistry)
    - F-Response, RegRipper
  - Post-mortem in forensic analysis tool
    - ProDiscover/ProScripts
  - Post-mortem, raw files
    - RegRipper/rip.exe!!
    - RFV from MiTec
- **Method used depends on your needs**
- **Correlation and analysis depend on your needs and goals**
  - RegRipper is awesome when it comes to correlation!

The Registry as a log file

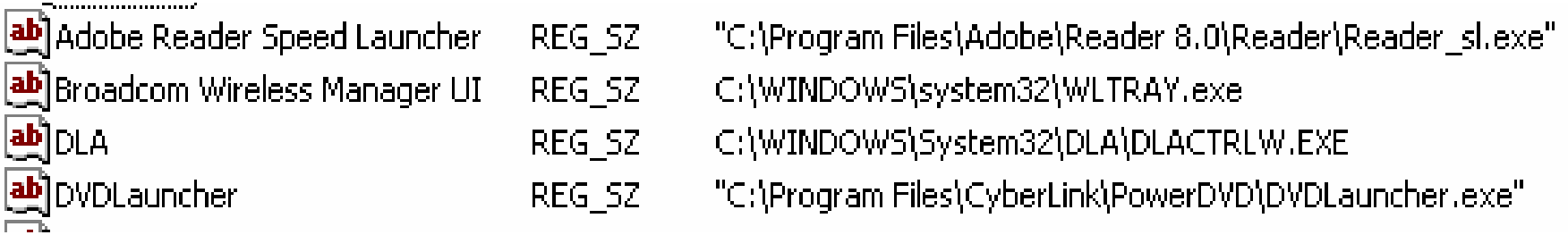
- **The Registry maintains a good deal of time-based information**
- **Registry keys have LastWrite value**
  - 64-bit FILETIME object
  - Useful when you know what actions cause the key to be updated
    - MRULists
- **Several Registry keys maintain timestamps within their value's data**
  - UserAssist keys
- **All of these sources provide information useful in timeline analysis, and can be easily correlated with other sources**

AutoStart Locations

- **Mostly in Software file, some in System file**
- **Traditional locations**
  - HKLM\..\Run, RunOnce, etc.
  - Services keys (great place to find kernel-mode rootkits)
- **Great source of autostart keys is AutoRuns from SysInternals (MS)**
- **Mostly straightforward queries for values, no correlation required**
- **Where does most of the documentation regarding autostart locations come from? The vendor?**

The “Ubiquitous” Run key

- **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
  - Lists command to be run each time a user logs on (*not* at boot)
  - No specific order to startup
  - Exists in both HKLM and HKCU hives



AppInit_DLLs Value

- **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows**
  - Specifies a DLL to be loaded by a Windows GUI application
  - Used by malware

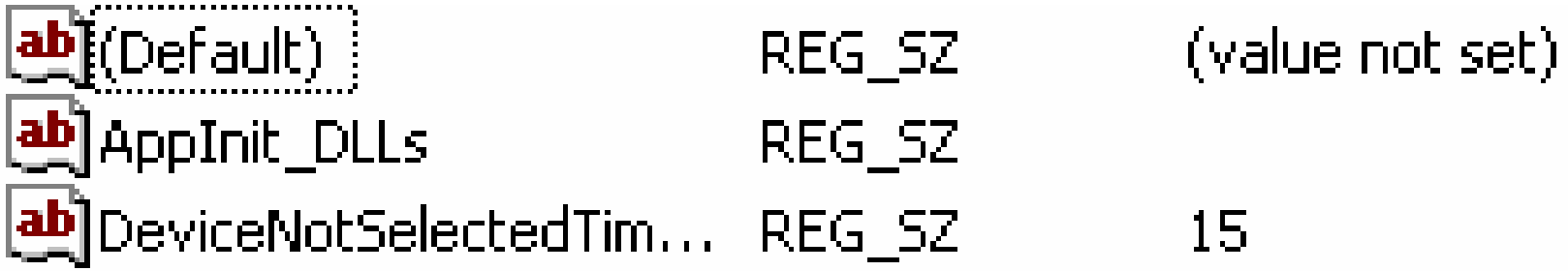
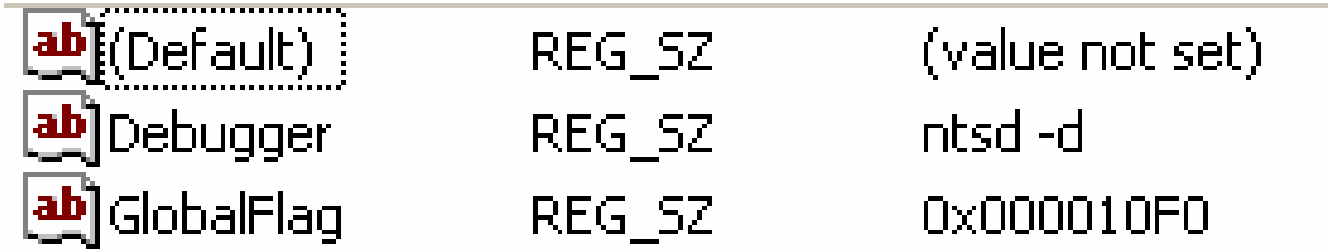


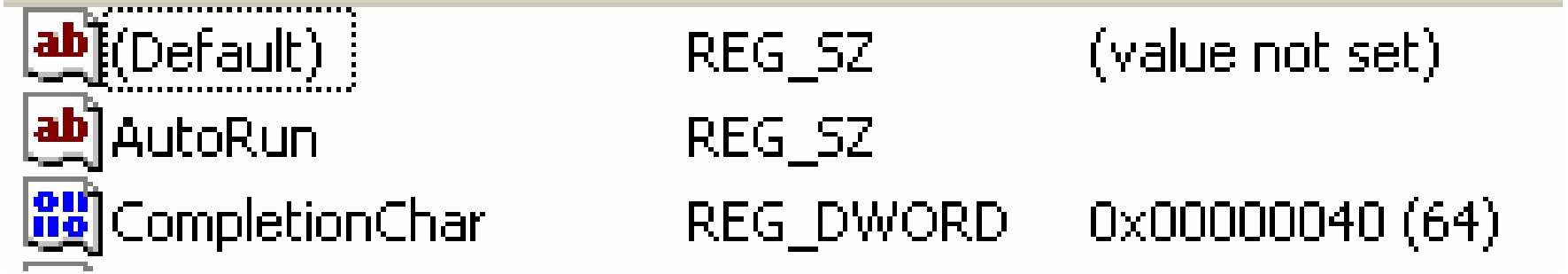
Image File Execution Options

- **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options**
  - Add a value named “Debugger” to redirect the application, point to another executable
  - Identified as an “attack vector” on Windows; *no* verification that the value points to an actual debugger
  - I have seen this one in the wild!!



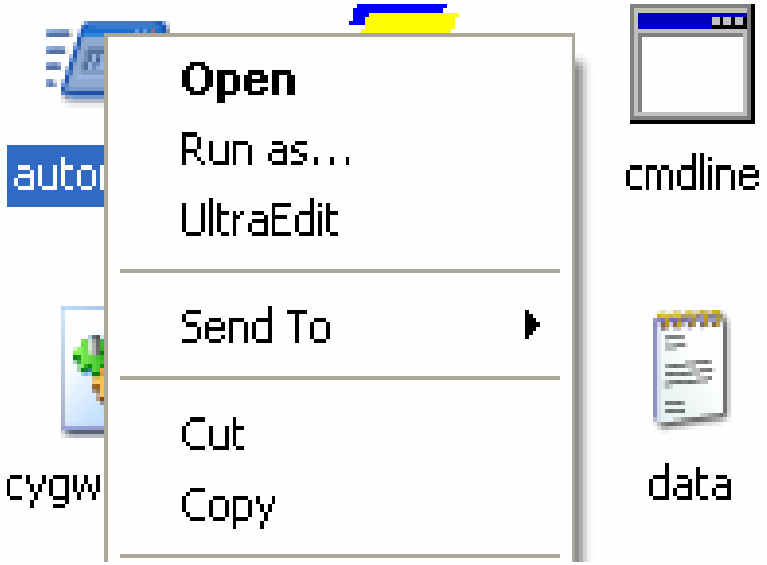
Command Processor\Autorun

- **HKLM\SOFTWARE\Microsoft\Command Processor**
  - Lists command to be run each time cmd.exe is run
  - Change via “cmd /d”
  - Exists in both HKLM and HKCU hives



exefile\shell\open\command

- **HKLM\Software\Classes\exefile\shell\open\command**
  - Also HKCR\exefile\shell\open\command
  - Default entry should be ‘ “%1” %* ‘
  - Automatically run when exe file is opened (applies to comfile, batfile, etc.)
  - Used by malware (ie, Pretty Park)



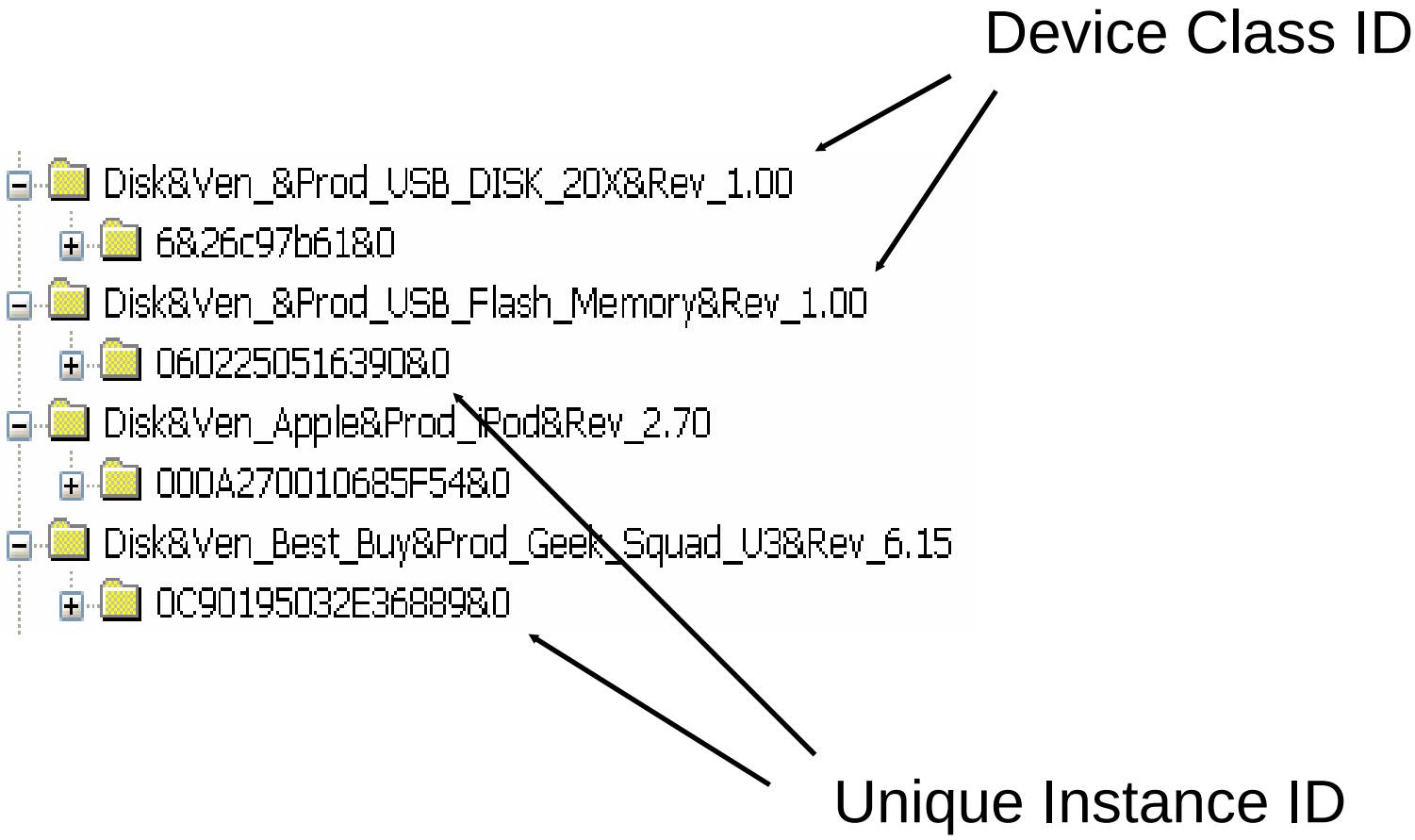
Other Registry keys/values of interest

- **May affect your follow-on analysis**
  - NukeOnDelete
    - Bypass the Recycle Bin on deletion
  - DisableLastAccess
    - Disable updating of last access times on files
    - Disabled **by default** on Vista
  - ClearPageFileAtShutdown
    - Clear the pagefile during a normal shutdown

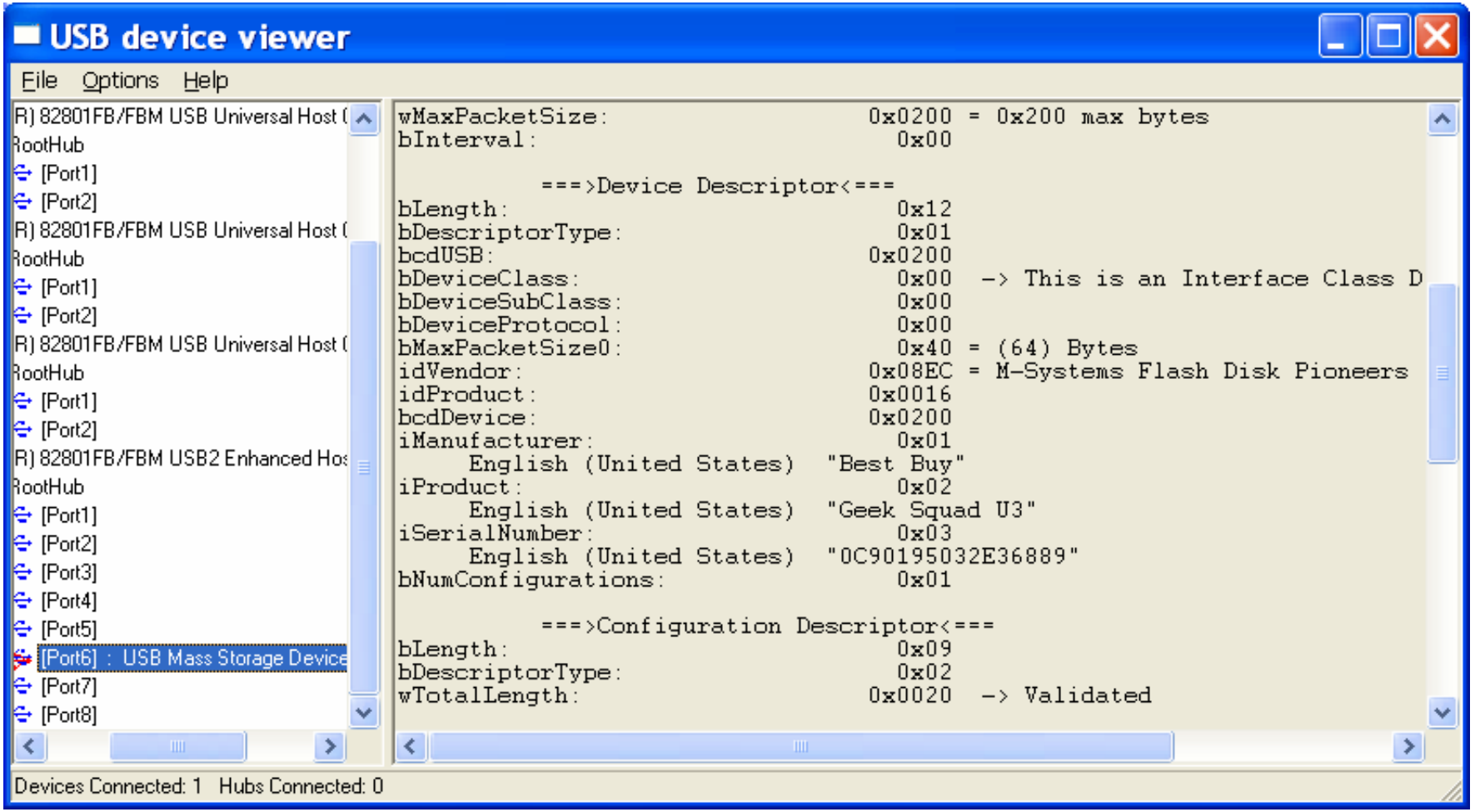
USB Devices

- **Found in the System file**
- **USB removable storage**
  - Thumb drives, iPods, digital cameras, ext HDD
- **Can determine through correlation:**
  - Type/class of device
  - Serial number (if device has one) or drive signature (for ext. HDDs)
  - Date/time device was last disconnected (DeviceClasses keys)
  - Drive letter the device was mapped to (MountedDevices key)
- **See setupapi.log for first time the device was connected**

USB Devices



USB Devices - UVCView

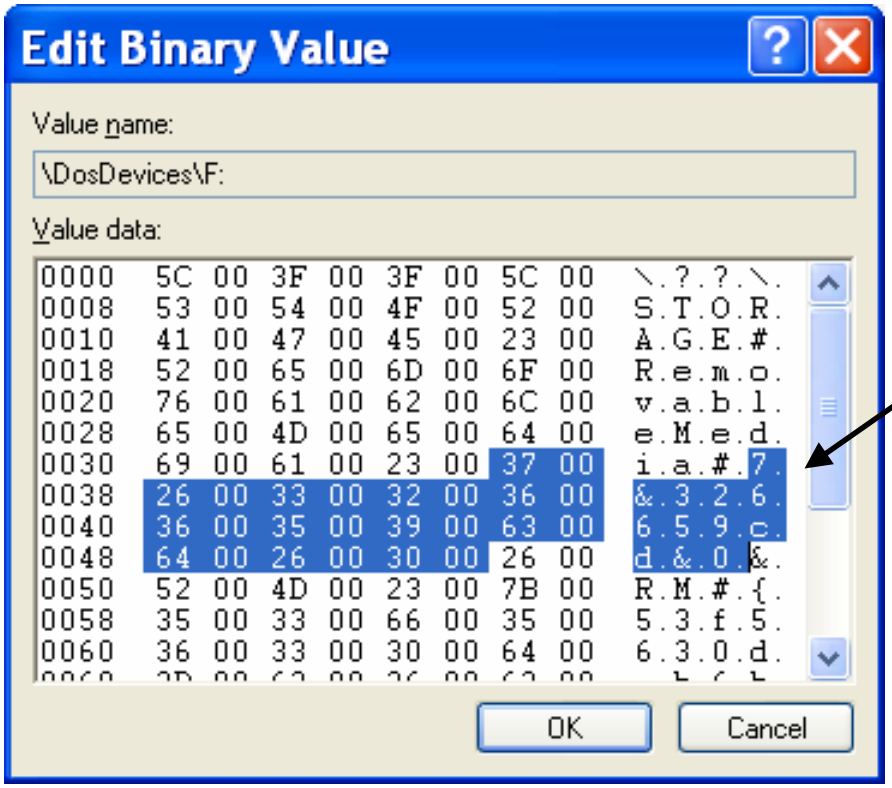


USB Devices - ParentIDPrefix

FriendlyName	REG_SZ	Best Buy Geek Squad U3 USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskBest_BuyGeek_Squad_U3___6.15 US
Mfg	REG_SZ	(Standard disk drives)
ParentIdPrefix	REG_SZ	7&326659cd&0

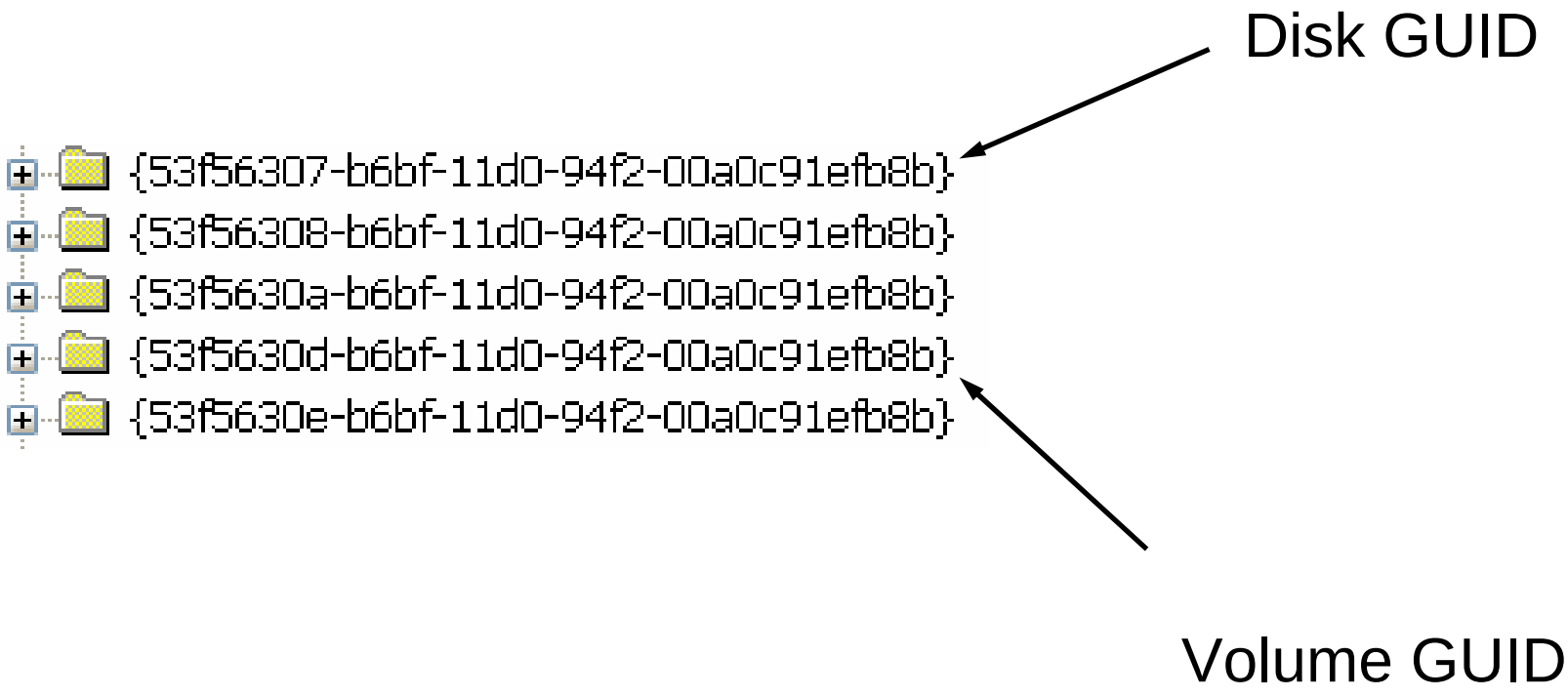
ParentIDPrefix

USB – MountedDevices key



ParentIDPrefix

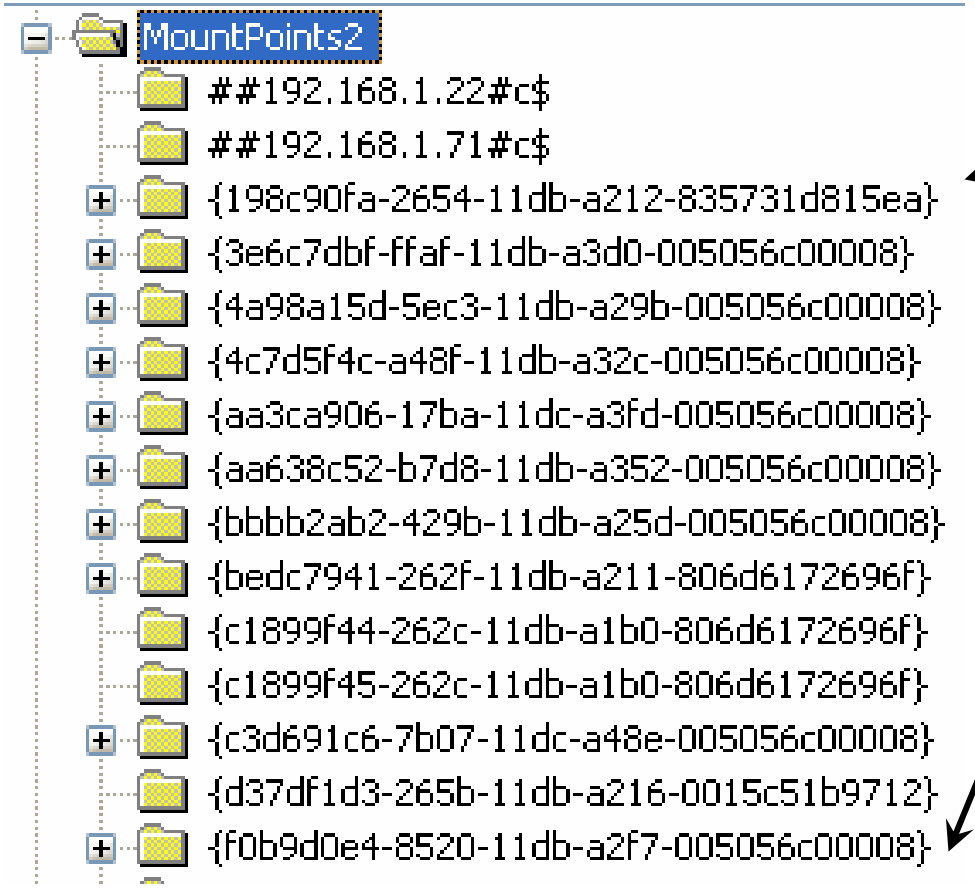
USB – DeviceClasses Key



USB – DeviceClasses Key

- **Disk GUID**
  - \##?#USBSTOR#Disk&Ven_Apple&Prod_iPod&Rev_2.70#000A270010685F54&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
  - Serial number
- **Volume GUID**
  - \##?#STORAGE#RemovableMedia#7&326659cd&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  - ParentIDPrefix
- **LastWrite time on key == last time the device was connected**
- **To get the first time the device was connected to the system, you need to go to the setupapi.log file**

USB – User's MountPoint2 Key



These entries are found in the MountedDevices key, as well…so they will tell you which device the user had access to.

Using these entries, we can tie an external storage device to a user.

SAM File

- **Local user account information**
- **Local group membership**

Guest
Built-in account for guest access to the computer/domain
Key LastWrite Time = Tue Aug 17 20:27:13 2004 (UTC)
Last Login = Never
Login Count = 0
Pwd Reset Date = Never
Pwd Failure Date = Never
Account Flags:
--> Password does not expire
--> Account Disabled
--> Password not required
--> Normal user account

SAM File

Harlan
Key LastWrite Time = Mon Sep 26 23:37:51 2005 (UTC)
Last Login = Mon Sep 26 23:37:51 2005 (UTC)
Login Count = 35
Pwd Reset Date = Wed Aug 18 00:49:42 2004 (UTC)
Pwd Failure Date = Mon Sep 26 23:37:47 2005 (UTC)
Account Flags:
--> Password does not expire
--> Normal user account

Administrators
Administrators have complete and unrestricted access to the computer/domain
Key LastWrite Time = Wed Aug 18 00:46:24 2004 (UTC)
Administrator
Harlan

Security File

- **Extract the audit policy, similar to what you get with auditpol.exe on a live system**
  - Tells you what you should expect to see in the Event Logs
  - LastWrite time on the Registry key will tell us when this was modified

```
C:\Perl\forensics>secparse d:\cases\security
LastWrite: Fri Sep  9 01:11:43 2005 (UTC)
Auditing was enabled.
There are 9 audit categories.

Privilege Use                 None
Object Access                 None
Account Logon Events          Both
System Events                 Both
Policy Change                 Both
Logon Events                  Both
Account Management            Both
Directory Service Access      None
Process Tracking              None
```

Tracking User Activity via the NTUSER.DAT Registry Hive file

User Activity

- **User activity recorded in the NTUSER.DAT file located in the user's profile directory**
  - Files accessed
  - Searches
  - Network connections
  - Applications launched

MRU Lists

- **Most Recently Used**
- **Applies to Windows; other apps also maintain their own MRU lists**
- **Mostly in user's NTUSER.DAT**
  - Software\Microsoft\Windows\CurrentVersion\Explorer key
  - RecentDocs (binary data)
  - RunMRU
  - Map Network Drive MRU
  - ComDlg32\LastVisitedMRU
  - ComDlg32\OpenSaveMRU (ASCII data)

RecentDocs Key

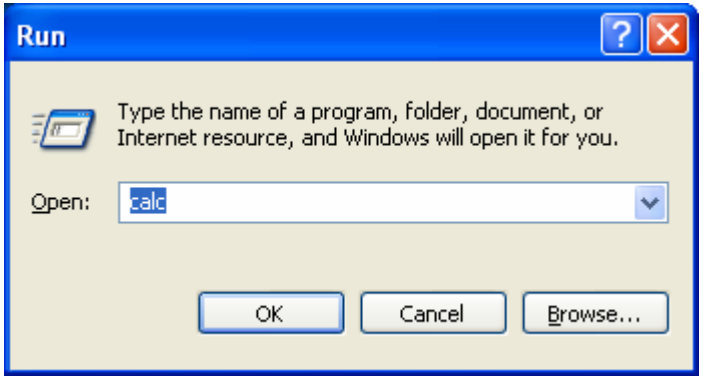
- **Which documents did the user recently access?**
  - Key's LastWrite time tells us when the most-recent document was accessed
  - Binary data type, must be translated
  - Key includes MRUListEx value showing order of accesses

Excerpt:

12 honeynet_papers
13 cover.jpg
14 USB DISK (E:)
15 fspconfig.jpg
16 fru.jpg
17 test.txt
18 c$ on '192.168.1.22' (Z:)
19 2k3_usb.log
20 c$ on '192.168.1.71' (X:)
MRUListEx 20,19,18,17,14,16,15,13,12,11,8,10,9,7,1,6,0,4,5,3,2

RunMRU

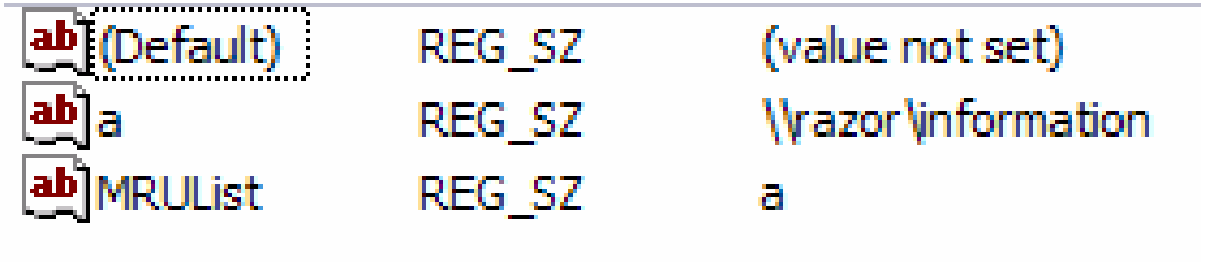
- **What did the user type into the Run box?**



(Default)	REG_SZ	(value not set)
a	REG_SZ	notepad\1
b	REG_SZ	calc\1
c	REG_SZ	regedit\1
d	REG_SZ	sol\1
e	REG_SZ	drwtsn32\1
f	REG_SZ	wscui.cpl\1
g	REG_SZ	wbemtest\1
h	REG_SZ	c:\windows\system32\restore\srdiag.exe\1
i	REG_SZ	winver\1
MRUList	REG_SZ	acbgdihfe

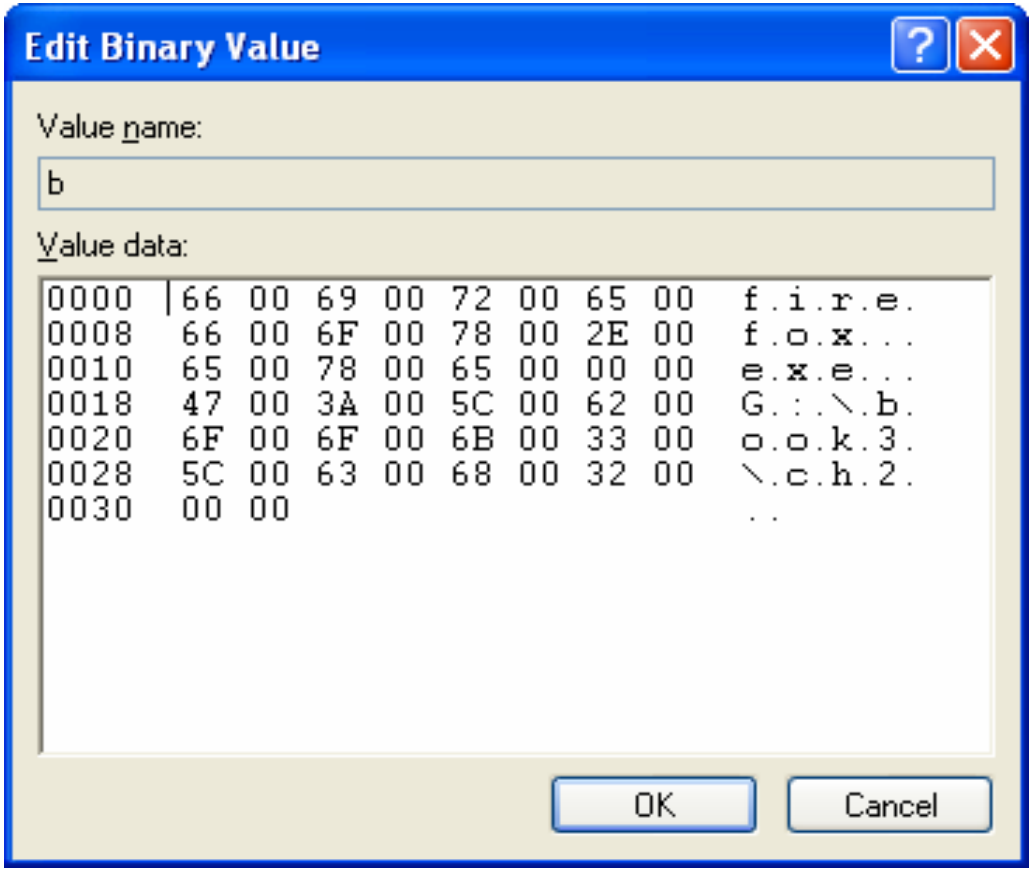
Map Network Drive MRU

- **Maintains a list of the drives that a user mapped to via the Map Network Drive Wizard**
  - Key LastWrite time can tell us when the MRU drive was mapped



ComDlg32 LastVisitedMRU

- **Files listed as binary data…must be translated**



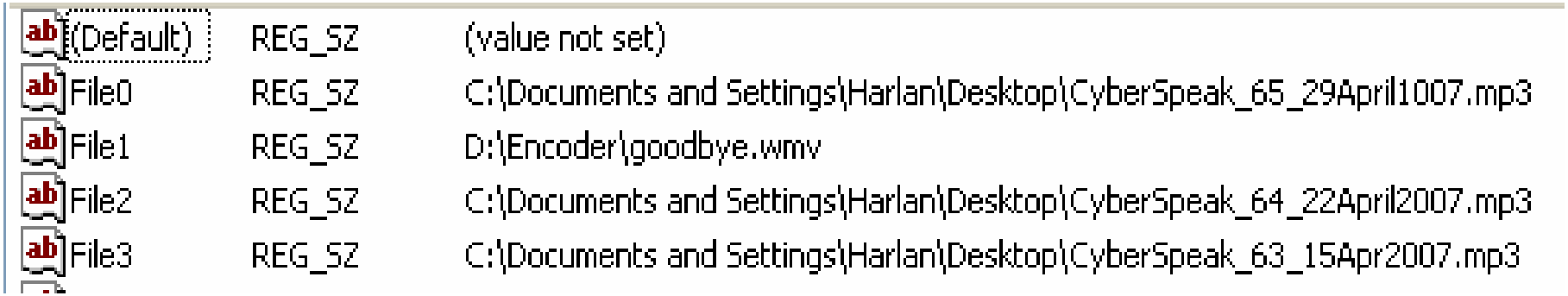
ComDlg32 OpenSaveMRU

- **Files listed by extension**

(Default)	REG_SZ	(value not set)
a	REG_SZ	D:\ubuntu-6.06.1-desktop-i386.iso
b	REG_SZ	D:\vista_5600.16384.060829-2230_x86fre_client-lr1cfre_en_dvd.iso
c	REG_SZ	D:\Helix_V1.7-03-07-2006.iso
d	REG_SZ	D:\Helix_V1.8-10-05-2006.iso
e	REG_SZ	D:\bt20061013.iso
f	REG_SZ	C:\Documents and Settings\Harlan\Desktop\Helix_V1.9-07-13-2007.iso
g	REG_SZ	D:\KNOPPIX_V5.1.1CD-2007-01-04-EN.iso
h	REG_SZ	D:\bt2final.iso
i	REG_SZ	F:\ubuntu-7.10-desktop-i386.iso
MRUList	REG_SZ	ihgfedcba

Media Player

HKCU\Software\Microsoft\MediaPlayer\Player\RecentFileList

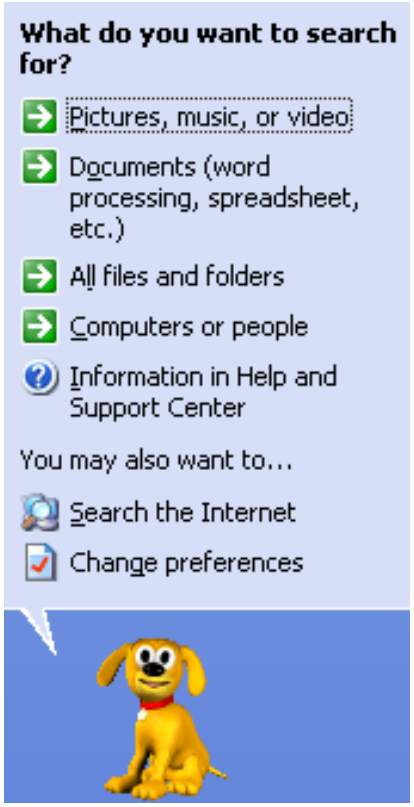


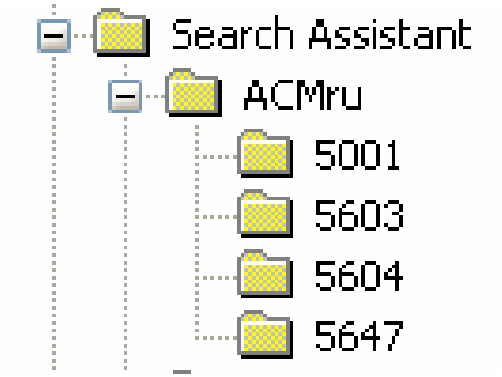
(Default)	REG_SZ	(value not set)
File0	REG_SZ	C:\Documents and Settings\Harlan\Desktop\CyberSpeak_65_29April1007.mp3
File1	REG_SZ	D:\Encoder\goodbye.wmv
File2	REG_SZ	C:\Documents and Settings\Harlan\Desktop\CyberSpeak_64_22April2007.mp3
File3	REG_SZ	C:\Documents and Settings\Harlan\Desktop\CyberSpeak_63_15Apr2007.mp3

ACMru

- **Start -> Search**
  - 5001 – Internet Search Assistant
  - 5603 - Search for Documents (or Files and Folders), particularly in the "All or part of document name" textfield
  - 5604 - Search for Files and Folders, particularly the "A word or phrase in a file" textfield
  - 5647 - Search for Computers
  - HKCU\Software\Microsoft\Search Assistant

ACMru





Other MRU Lists

- **TypedURLs – URLs typed by the user into the IE Address bar**
- **Microsoft Management Console\Recent File List – most recent .msc files opened**
- **Sonic – burn ISOs**
  - \Software\Sonic\MediaHub\Preference\Plugins\{BBD5C82E-73E5-42F8-835B-5F1C61472F30}\ImageList
- **Adobe -** \Software\Adobe\AcrobatReader\8.0\AVGeneral\cRecentFiles\c*n*
- **Word docs -** \Software\Microsoft\Office\11.0\Common\Open Find\Microsoft Office Word\Settings\File Save\File Name MRU
- **Many applications maintain MRU lists of some kind…if you see it in the GUI, it's probably maintained in the Registry!**
  - Even RegEdit maintains the last key accessed by the user

Other MRU Lists

- **Archive utilities, such as WinRar and WinZip maintain lists of archives accessed**

Network Connections – Remote Desktop

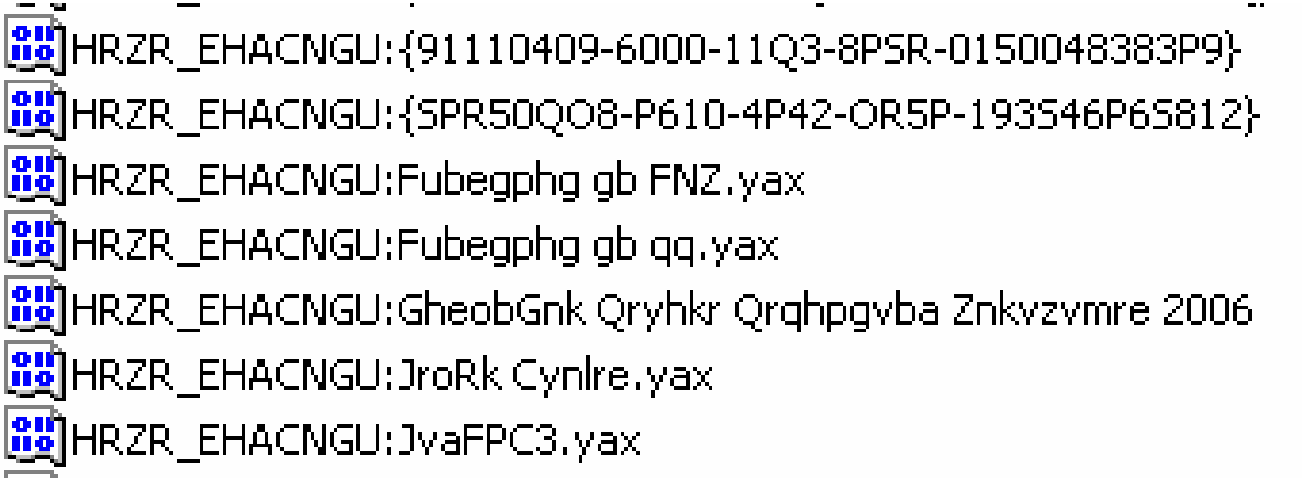
- **\Software\Microsoft\Terminal Server Client\Default**
- **Maintains a list of systems connected to via Remote Desktop**
- **Case Study**

UserAssist Keys

- **Three GUIDs**
  - ActiveDesktop
  - MS Internet Toolbar
  - IE7 (new)
- **Value names are ROT-13 “encrypted”**
- **16 byte data under ActiveDesktop GUID may contain**
  - bytes 4-7; DWORD RunCount value (starts at 5 – easy to remember; “Gates” has 5 letters)
  - bytes 8-15; FILETIME LastRun value
- **Shows that the user performed actions via the desktop**
  - Logged in at console, or via remote access (i.e., Terminal Services, etc.)

UserAssist Keys

- **Value names are ROT-13 “encrypted”**



- **Easily parsed and translated**
  - Didier Stevens UserAssist Tool
  - Perl → tr/N-ZA-Mn-za-m/A-Za-z/

UserAssist Keys – parsing NTUSER.DAT w/ Perl

```
C:\Perl\forensics>uassist.pl d:\cases\ntuser.dat
UserAssist\Settings subkey not found.
UserAssist (Active Desktop) [Mon Sep 26 23:33:06 2005 (UTC)]
Mon Sep 26 23:33:06 2005 (UTC)
        UEME_RUNPATH;22
        UEME_RUNPATH:C:\WINDOWS\system32\notepad.exe;10
Mon Sep 26 23:26:43 2005 (UTC)
        UEME_RUNPATH:Z:\WINNT\system32\sol.exe;6
Mon Sep 26 23:16:26 2005 (UTC)
        UEME_RUNPATH:C:\Program Files\Morpheus\Morpheus.exe;6
Mon Sep 26 23:16:25 2005 (UTC)
        UEME_RUNPATH:Morpheus.lnk;6
Mon Sep 26 23:04:08 2005 (UTC)
        UEME_RUNPATH:d:\bintext.exe;6
```

RegRipper

- **GUI-based, plugin-based approach to parsing/correlating data from within hive files extracted from an image**
- **Very cool, very slick; users have reported reducing data collection from DAYS to MINUTES!!**
- **Accompanying CLI tool, rip.exe, allows for quick data extraction via a single plugin or plugin file**
  - Can be included in a batch file

RegRipper Demo

Rip.exe – Batchin' it!

Command for one run of rip.exe to parse USB removable storage device information:

C:\forensics>rip.exe –r system –p usbstor2 [> usbstor.csv]

Command to run rip.exe across multiple systems, putting all info into a spreadsheet for correlation and analysis:

C:\forensics>rip.exe –r <file1> –p usbstor2 > usbstor.csv

C:\forensics>rip.exe –r <file2> –p usbstor2 >> usbstor.csv

Result is a spreadsheet that can be used to correlate devices connected across several systems, etc.

XP System Restore Points

- **XP maintains Restore Points for system recovery**
- **By default, an RP is created every day**
  - Specific RPs created for software install/uninstall, etc.
- **Each RP retains pertinent *portions* of Registry files**
  - Registry files are not completely backed up
- **Examining RP Registry files can provide insight into:**
  - “Historical” data
  - When a user was added to the Administrators group
  - Was data deleted at one point?

RipXP.exe

- **CLI tool, similar to rip.exe**
- **Uses RegRipper plugins**
- **Extract hives and Restore Points from image (FTK Imager, etc.)**
- **Runs the plugin against the designated hive file, as well as the corresponding hive files in each RP**

RipXP.exe Demo

Unallocated Space in Hive Files

- **Within hive files, structures are deleted and become part of unallocated space within the file**
- **Locate deleted keys (LastWrite times) and attempt to locate their associated values**
- **Work done by Jolanta Thomassen (thesis student) and Tim Morgan (DFRWS 2008 presentation)**
- **Registry “cleaning” tools will remove this unallocated space**

Issues w/ 64-bit Windows

- **Some redirection occurs**
  - Native 64-bit apps write to HKLM\Software
  - 32-bit apps write to **HKLM\Software\WOW6432Node**
  - KB 896459 lists the keys that are shared (not redirected)

Vista User Virtualization

- **Access to the Registry is restricted**
- **Vista creates a per-user copy and subsequently redirects read/write operations**

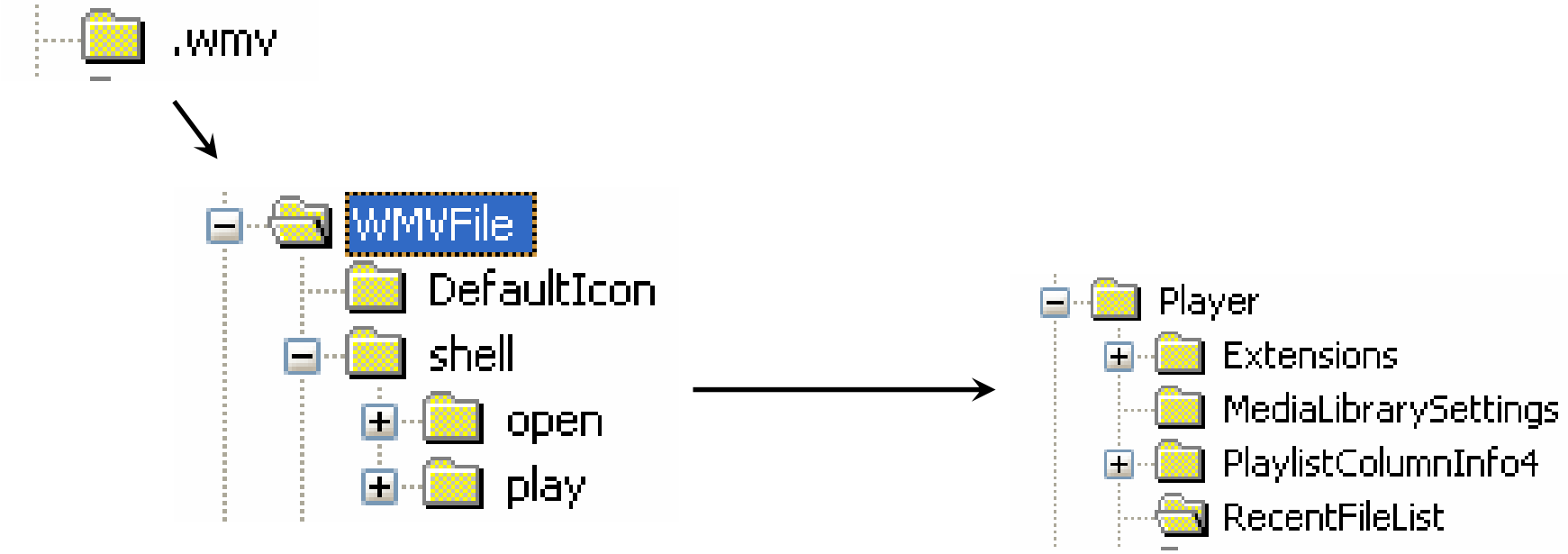
HKEY_CURRENT_USER\Software\Classes\VirtualStore

Case Study 1

- **User logged in via remote access**
  - UserAssist key showed that Cain.exe had been installed, launched, and uninstalled
  - Resulting *.lst files still on the system; MAC times corresponded to when cain.exe was launched

Case Study 2

- **User connects digital camera or other removable storage to system**
- **Views content from the storage device**
- **Files not on system; removable storage not confiscated**



Case Study 2

- **Start at RecentDocs key in user's Registry hive file, notice ".wmv" file extension (note LastWrite time on the key)**
- **HKEY_CLASSES_ROOT key holds file association info**

```
C:\>assoc .wmv
.wmv=RealPlayer.wmv.6

C:\>ftype wmvfile
wmvfile="C:\Program Files\Windows Media
  Player\wmplayer.exe" /prefetch:7 /Open "%L"
```

- **Now we know that Windows Media Player is used to view files with .wmv extension; go check out the RecentFileList key**

Methodology

- **Whenever you find something of interest in one investigation, document it and add it to a script**
- **Whenever working on a new case, or if you get unusual results, import the hive file into RegEdit, and "poke around"**
  - Find something new, document it, add it to a script…

Questions?

Harlan Carvey

hcarvey@us.ibm.com