



Internet Security Systems

Registry Analysis

SANS Forensic Summit 2009

“Allow myself to introduce...myself”



What is “Registry Analysis”??

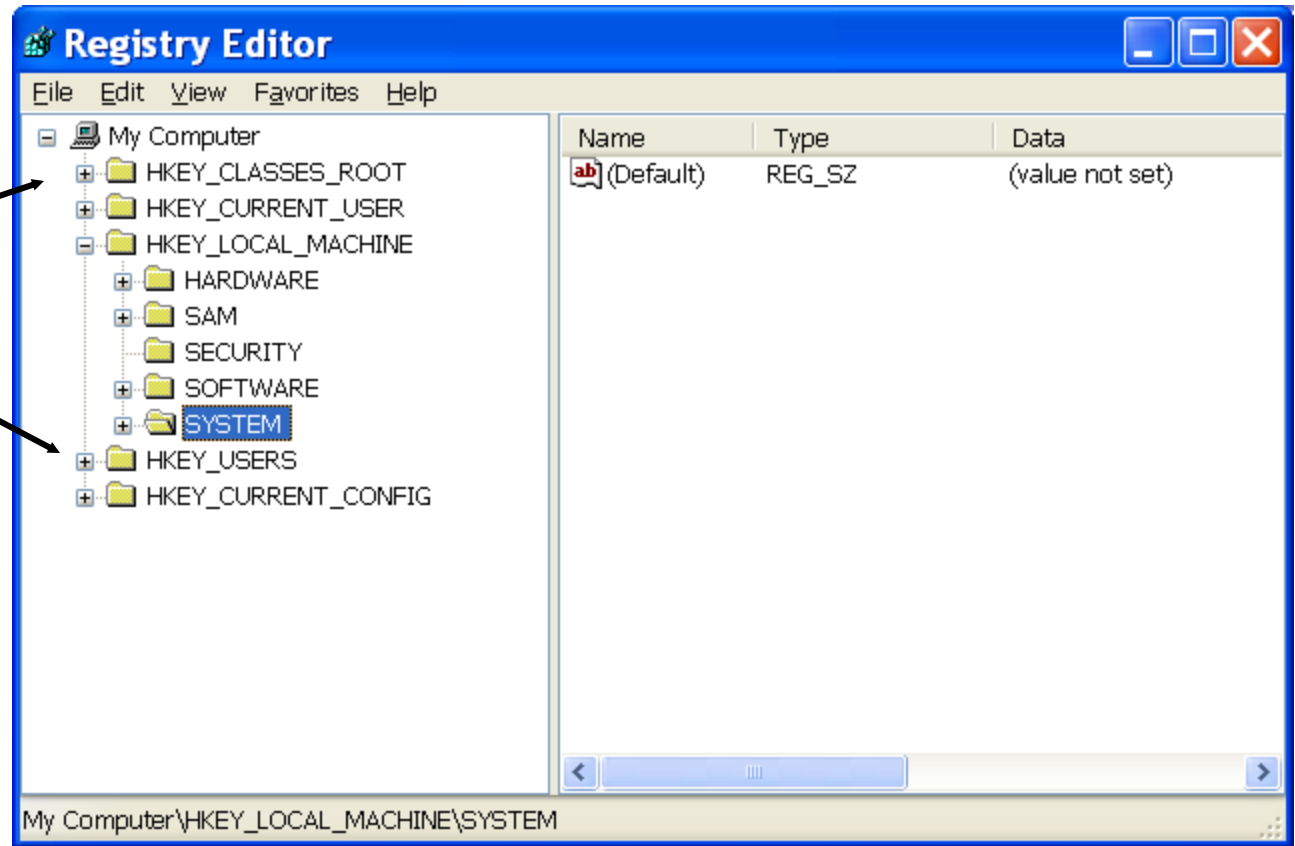
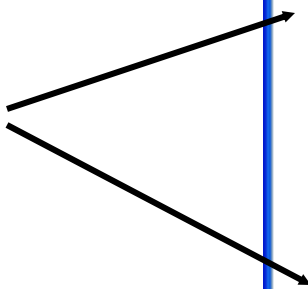
- **More than just opening Registry files in a viewer and finding values**
- **Registry analysis involves:**
 - Extracting information and *context* from a largely untapped source of data
 - Extracting relevant information only (Dan Purcell, CEIC 2009)
 - Knowing the *context* which creates or modifies Registry data, as that you do find can significantly impact your overall analysis

What is the Registry?

- **Binary hierarchal database**
 - Based on nodes (key, value) and pointers
- **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)**

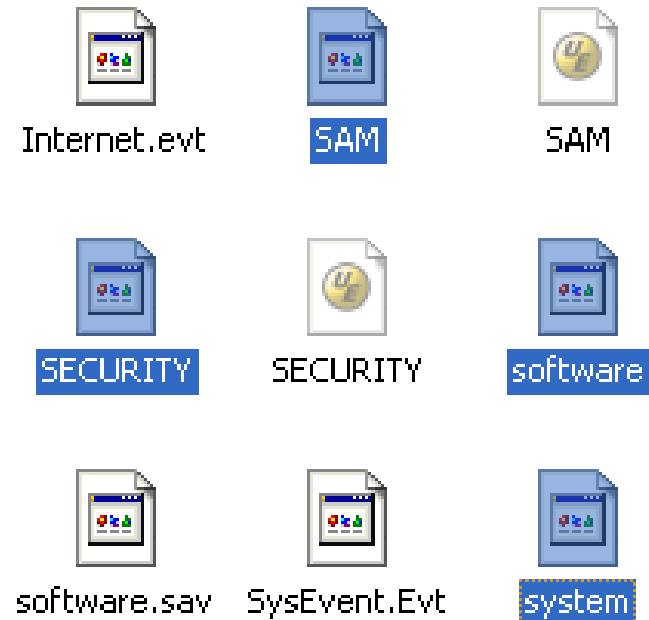
Registry Hives

Hives



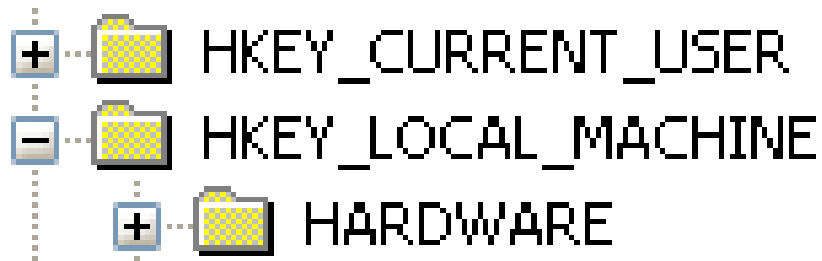
What is the Registry?

- **Hives can be found in files**
 - system32\config dir; System, Software, SAM, etc.
 - NTUSER.DAT file in the user's profile

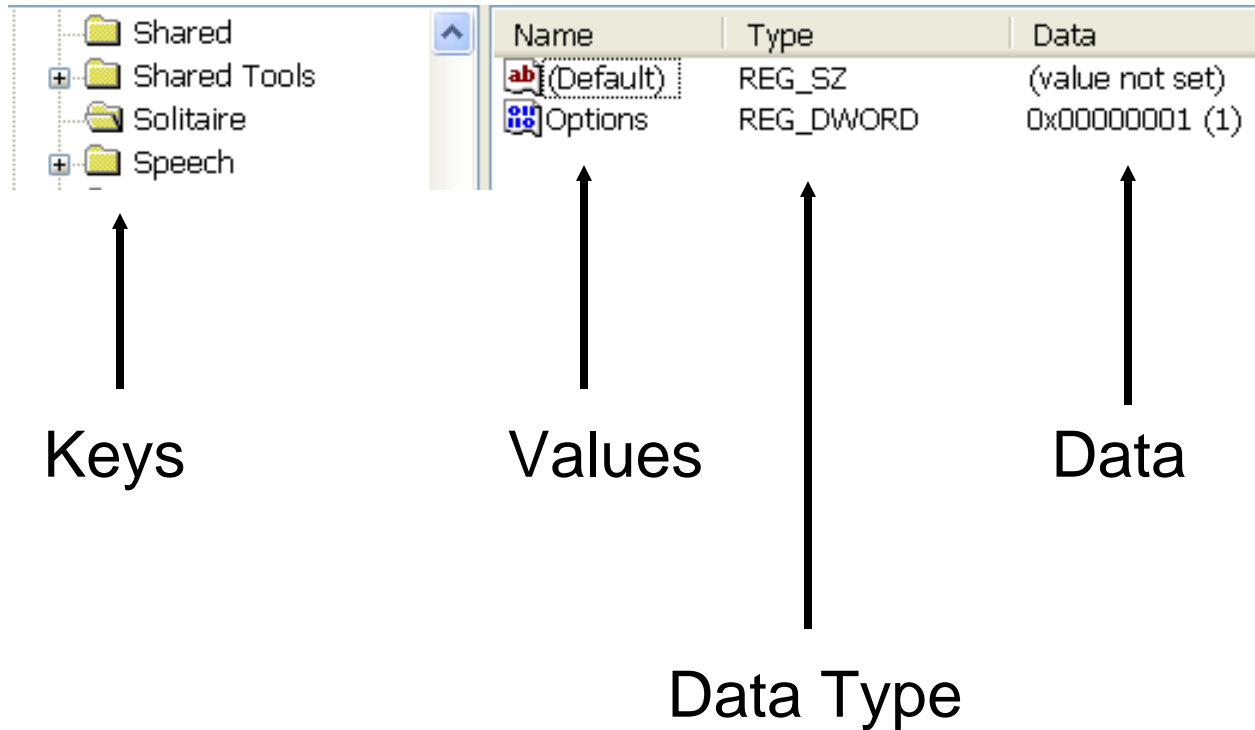


What is the Registry?

- **Some hives are volatile, created when the system starts or user logs in**
 - HKEY_LOCAL_MACHINE\System\CurrentControlSet
 - HKEY_CURRENT_USER
 - HKEY_LOCAL_MACHINE\Hardware



A Bit of Registry Nomenclature



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
 - Some timestamp data is maintained a 32-bit *nix epoch time
- **All of these sources provide information useful in timeline analysis, and can be easily correlated with other sources**

Registry Structure

- **Tim Morgan**
- **Jolanta Thomassen**
 - Regslack.pl
- **Brendan Dolan-Gavitt**
 - Volatility modules
- **Pete Norris**
 - Thesis

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"„ÿ.....
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¿Dàpÿÿsk..
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 ; eTimeout&ÿÿÿ2.O.
30 00 30 00 30 00 00 00 F0 FF FF FF 18 E9 07 00 ; 0.0.0...&ÿÿÿ.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?

- **Configuration settings**

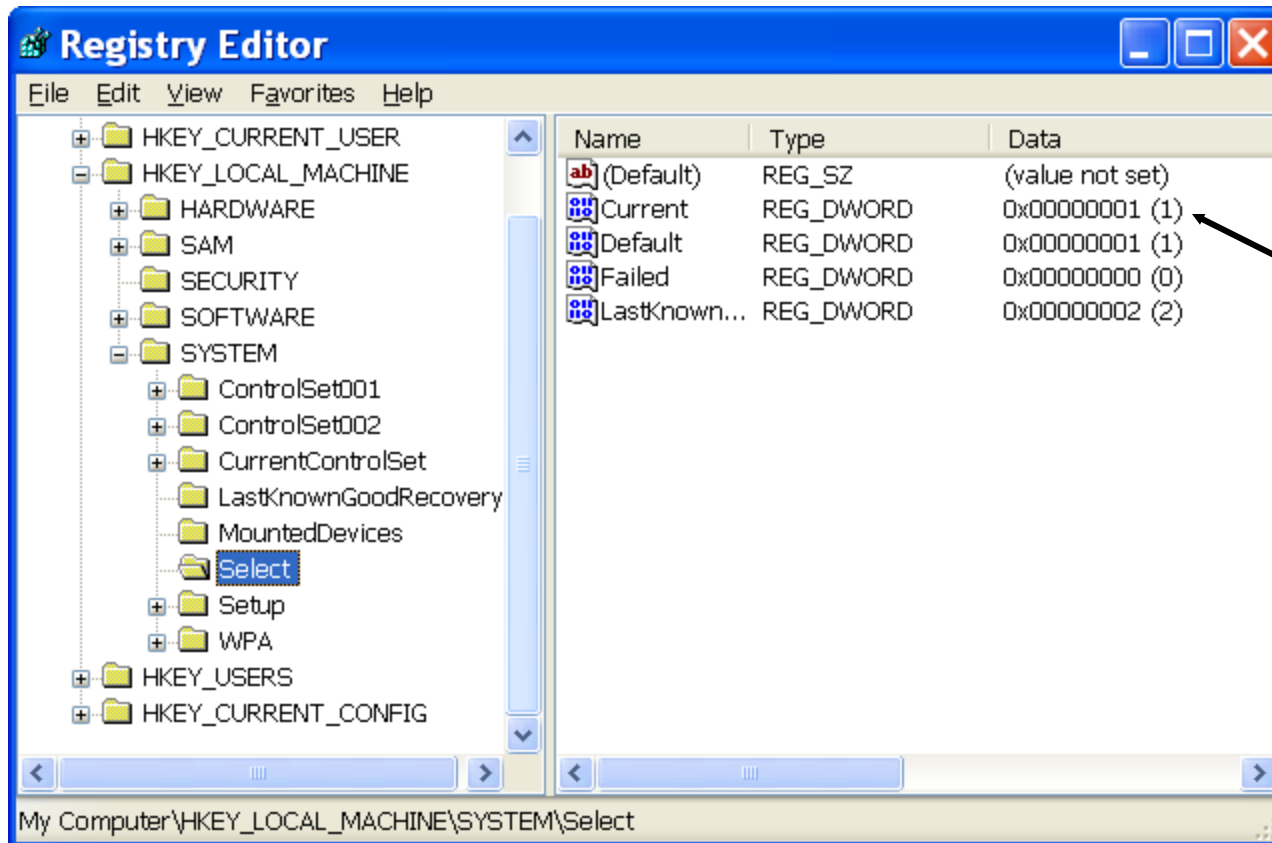
- Application settings
 - Download directories (P2P applications)
 - Recently accessed files (images, movies, etc.)
- AutoStart locations
 - Applications that start w/ little or **NO** user interaction

- **Tracking info**

- Attached USB devices (thumb drives, ext HDD, digital cameras, etc.)
- User activity
 - MRUs
 - Viewed documents or images
 - Applications installed or launched (UserAssist keys)

- **Context**

NOTE: Locating the *CurrentControlSet*







Current

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

 Adobe Reader Speed Launcher	REG_SZ	"C:\Program Files\Adobe\Reader 8.0\Reader\Reader_sl.exe"
 Broadcom Wireless Manager UI	REG_SZ	C:\WINDOWS\system32\WLTRAY.exe
 DLA	REG_SZ	C:\WINDOWS\System32\DLA\DLACTRLW.EXE
 DVDLauncher	REG_SZ	"C:\Program Files\CyberLink\PowerDVD\DVDLauncher.exe"

AppInit_DLLs Value

- **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows**
 - Specifies a DLL to be loaded by a Windows GUI application
 - Used by malware
 - <http://support.microsoft.com/kb/197571>







 (Default)	REG_SZ	(value not set)
 AppInit_DLLs	REG_SZ	
 DeviceNotSelectedTim...	REG_SZ	15




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

 (Default)	REG_SZ	(value not set)
 Debugger	REG_SZ	ntsd -d
 GlobalFlag	REG_SZ	0x000010F0

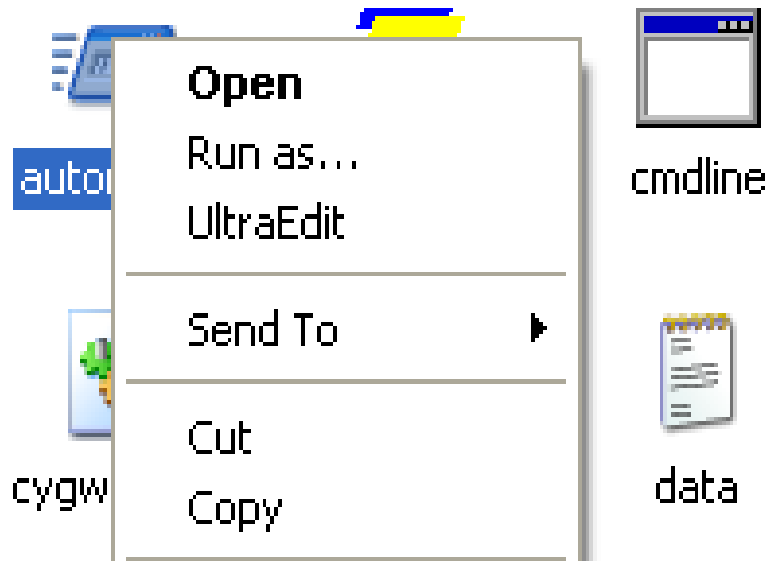
Command Processor\Autorun

- **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

 (Default)	REG_SZ	(value not set)
 AutoRun	REG_SZ	
 CompletionChar	REG_DWORD	0x00000040 (64)

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**
 - NeedtoPurge (XP) & NukeOnDelete (Vista)
 - Bypass the Recycle Bin on deletion
 - NtfsDisableLastAccessUpdate
 - 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
 - External hard drives
 - iPods
 - Digital Cameras
- **Can determine:**
 - Type/class of device
 - Serial number (if device has one) or drive signature (for ext. HDDs)
 - Date/time device was last connected
 - Drive letter the device was mapped to
- **See setupapi.log for first time the device was connected**

USB Devices

Device Class ID

- [-] [+] Disk&Ven_&Prod_USB_DISK_20X&Rev_1.00
 - [+] [+] 6&26c97b61&0
- [-] [+] Disk&Ven_&Prod_USB_Flash_Memory&Rev_1.00
 - [+] [+] 0602250516390&0
- [-] [+] Disk&Ven_Apple&Prod_iPod&Rev_2.70
 - [+] [+] 000A270010685F54&0
- [-] [+] Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15
 - [+] [+] 0C90195032E36889&0

Unique Instance ID

USB Devices - UVCView

The screenshot shows the 'USB device viewer' application window. The left pane displays a tree view of USB devices, with '[Port6] : USB Mass Storage Device' selected. The right pane displays the details for this device, including the Device Descriptor and Configuration Descriptor.

```

File  Options  Help
R) 82801FB/FBM USB Universal Host (
RootHub
[Port1]
[Port2]
R) 82801FB/FBM USB Universal Host (
RootHub
[Port1]
[Port2]
R) 82801FB/FBM USB Universal Host (
RootHub
[Port1]
[Port2]
R) 82801FB/FBM USB2 Enhanced Hos
RootHub
[Port1]
[Port2]
[Port3]
[Port4]
[Port5]
[Port6] : USB Mass Storage Device
[Port7]
[Port8]

wMaxPacketSize:      0x0200 = 0x200 max bytes
bInterval:           0x00

===>Device Descriptor<===
bLength:              0x12
bDescriptorType:     0x01
bcdUSB:               0x0200
bDeviceClass:         0x00  -> This is an Interface Class D
bDeviceSubClass:     0x00
bDeviceProtocol:     0x00
bMaxPacketSize0:     0x40 = (64) Bytes
idVendor:             0x08EC = M-Systems Flash Disk Pioneers
idProduct:            0x0016
bcdDevice:            0x0200
iManufacturer:       0x01
                    English (United States) "Best Buy"
iProduct:             0x02
                    English (United States) "Geek Squad U3"
iSerialNumber:        0x03
                    English (United States) "0C90195032E36889"
bNumConfigurations:  0x01

===>Configuration Descriptor<===
bLength:              0x09
bDescriptorType:     0x02
wTotalLength:        0x0020  -> Validated
  
```

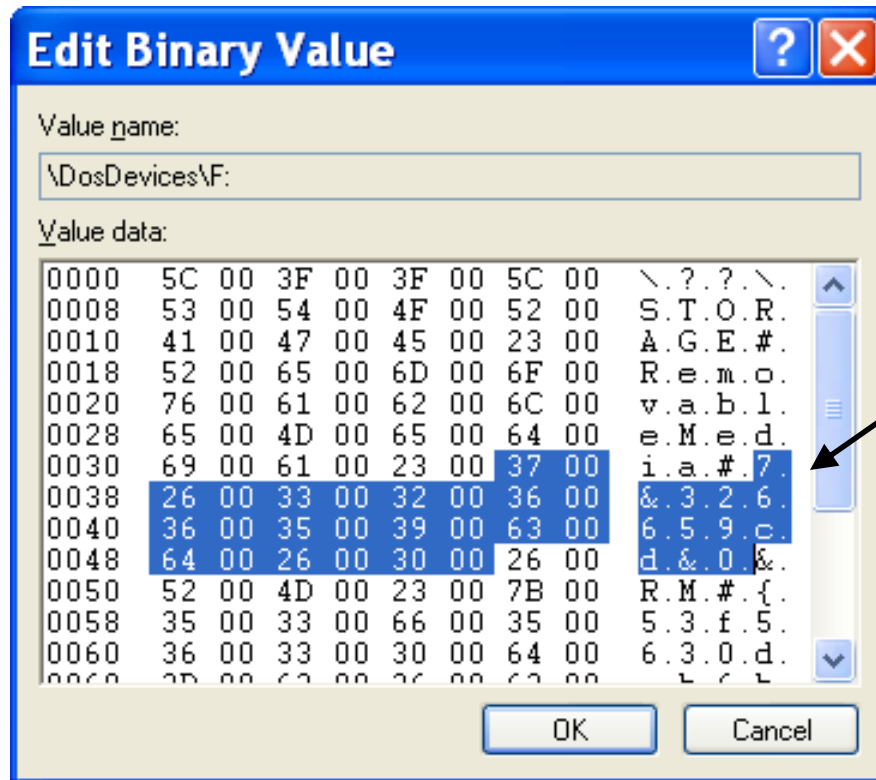
Devices Connected: 1 Hubs Connected: 0

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

Disk GUID

- + {53f56307-b6bf-11d0-94f2-00a0c91efb8b}
- + {53f56308-b6bf-11d0-94f2-00a0c91efb8b}
- + {53f5630a-b6bf-11d0-94f2-00a0c91efb8b}
- + {53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
- + {53f5630e-b6bf-11d0-94f2-00a0c91efb8b}

Volume GUID

USB – DeviceClasses Key

- **Disk GUID**

- \###?#USBSTOR#Disk&Ven_Apple&Prod_iPod&Rev_2.70#000A270010685F54&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
- Serial number

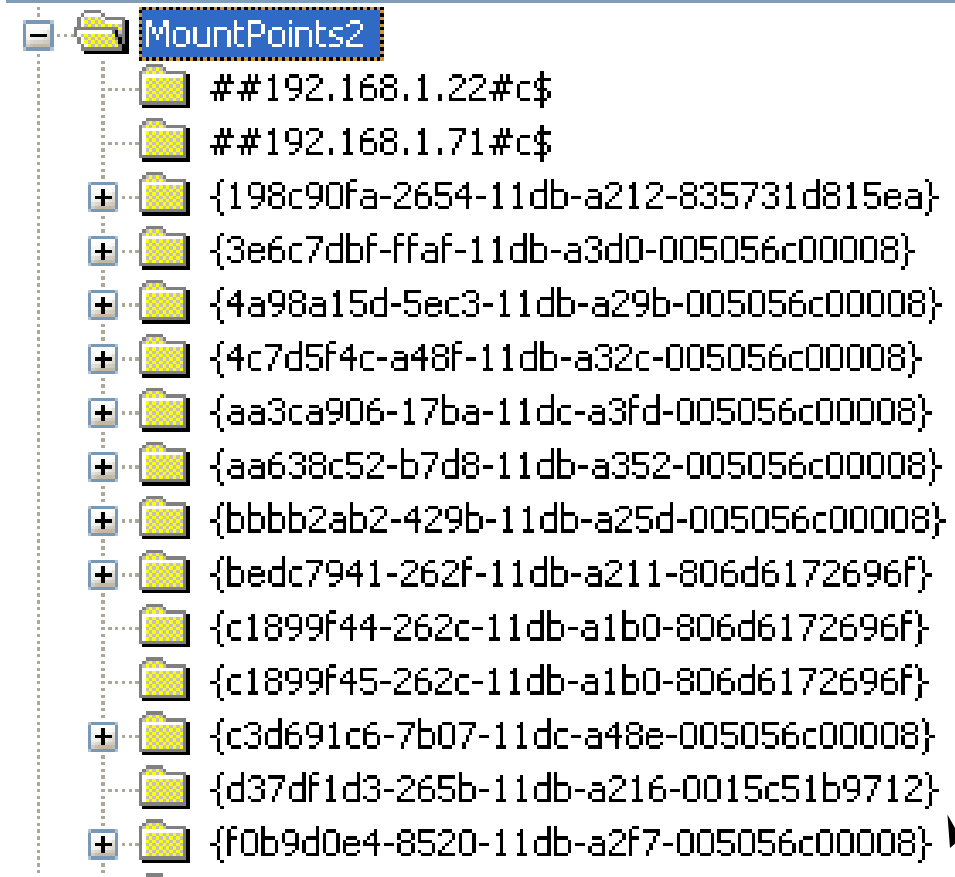
- **Volume GUID**

- \###?#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.

Vista's Portable Devices key

- **Appears to maintain a history of portable devices connected to the system**
- **Based on new driver framework provided with Vista**

Device : DISK&VEN_APPLE&PROD_IPOD&REV_1.62

LastWrite : Fri Sep 21 01:42:42 2007 (UTC)

SN : 000A270018A0E610&0

Drive : IPOD (F:)

Device : DISK&VEN_BEST_BUY&PROD_GEEK_SQUAD_U3&REV_6.15

LastWrite : Thu Feb 7 13:26:19 2008 (UTC)

SN : 0C90195032E36889&0

Drive : GEEKSQUAD (F:)

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, and applications 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

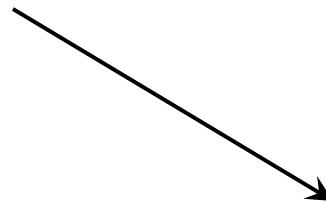
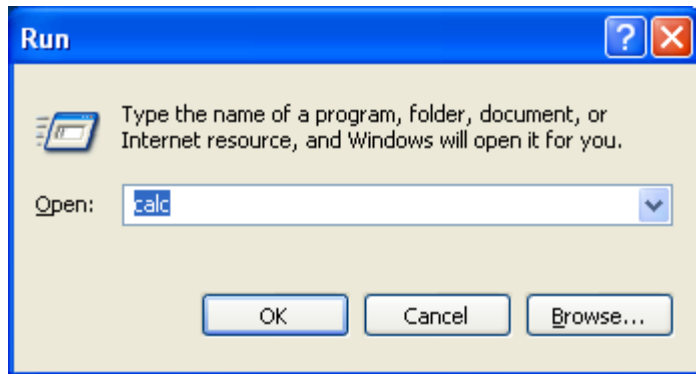
Excerpt:










```
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\srdiaq.exe\1
 i	REG_SZ	winver\1
 MRUList	REG_SZ	acbgdihfe

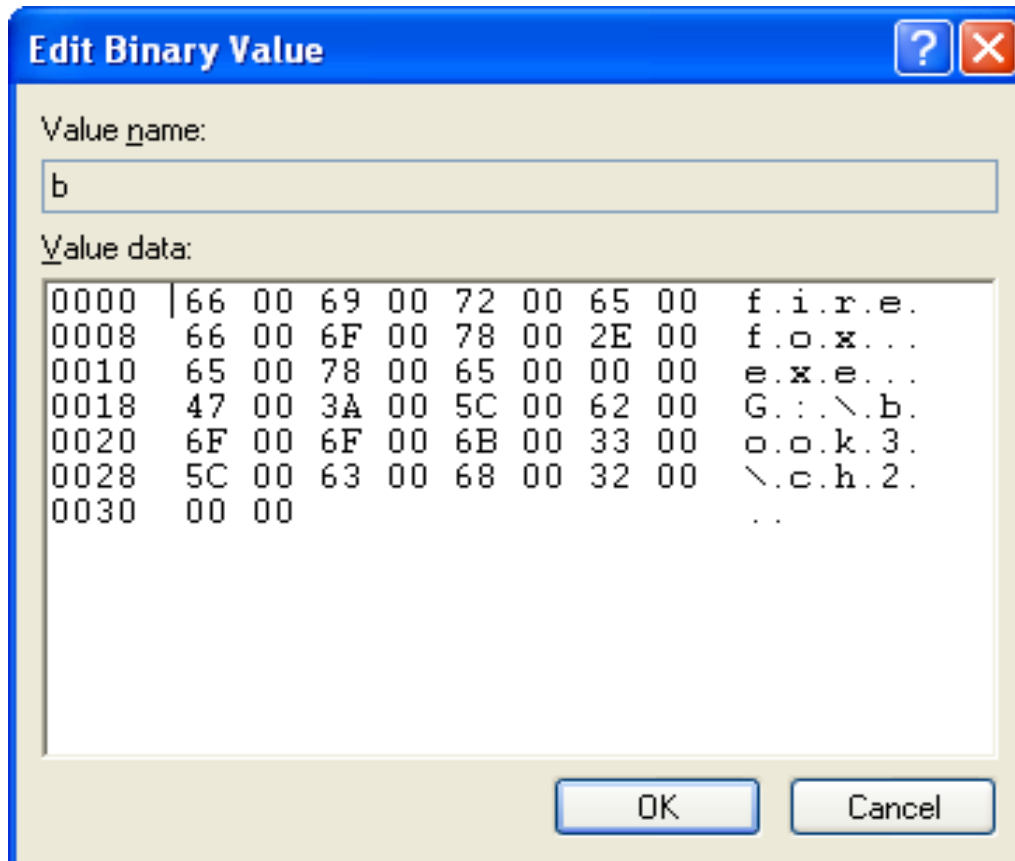
Map Network Drive MRU

- **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

 (Default)	REG_SZ	(value not set)
 a	REG_SZ	\\razor\information
 MRUList	REG_SZ	a






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


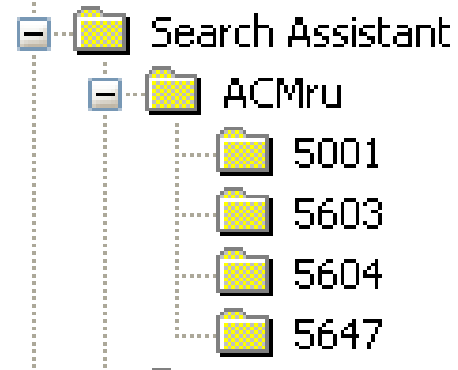
ACMru

What do you want to search for?

- Pictures, music, or video
- Documents (word processing, spreadsheet, etc.)
- All files and folders
- Computers or people
- ⓘ Information in Help and Support Center

You may also want to...

- 🔍 Search the Internet
- 📄 Change preferences

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\cn
- **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

Network Connections – Remote Desktop

- **\Software\Microsoft\Terminal Server Client\Default**
- **Maintains a list of systems connected to via Remote Desktop**
- **<http://support.microsoft.com/kb/312169>**

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”

```
HRZR_EHACNGU:{91110409-6000-11Q3-8PSR-0150048383P9}  
HRZR_EHACNGU:{SPR50QO8-P610-4P42-OR5P-193546P65812}  
HRZR_EHACNGU:Fubegphg gb FNZ.yax  
HRZR_EHACNGU:Fubegphg gb qq.yax  
HRZR_EHACNGU:GheobGnk Qryhkr Qrqhpgvba Znkqvzvmre 2006  
HRZR_EHACNGU:JroRk Cynlre.yax  
HRZR_EHACNGU:JvaFPC3.yax
```

- 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>rip.pl -r d:\cases\ntuser.dat -p userassist
```

```
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.Ink;6
```

```
Mon Sep 26 23:04:08 2005 (UTC)
```

```
    UEME_RUNPATH:d:\bintext.exe;6
```

Correlating Registry Data

■ Correlation Sources

- Registry itself (USB devices)
- Files
 - SetupAPI.log
 - Shortcut (LNK) files
 - XP Prefetch files
- Event Log
- Other Files

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?

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)

XP vs. Vista

- **Basic binary structure is the same**
- **Some entries remain the same**
- **Some functionality added, other functionality moved to different key**
- **MS maintaining XP until 2014, including a virtual XP install in Windows 7**

Demos

- **RegRipper**
- **RipXP**
- **Regslack**

Questions?

Harlan Carvey
hcarvey@us.ibm.com