The Windows Registry as a forensic resource

Harlan Carvey Digital Investigation (2005)

> Presented By: Azzat Ahmed

Outline

- Introduction.
- Objectives.
- Windows Registry.
- Registry Structure.
- Registry as a Log File.
- What's in the Registry?
- Summary.

Introduction

- Forensic investigators may use several analysis mechanisms on the system image.
- Comparing hashes of files: MD5 or SHA-1.
- Examining the file system alone:



- No comprehensive picture of activities.
- Weak case.

Introduction (Cont.)

- Analysis of Windows system can go much deeper.
- Windows Registry is treasure of information.



- Correlation of system file and Registry information:
 - Strong case.

Objectives

- Briefly discuss the structure of the Windows Registry.
- Examples of registry information.
- Methods for determining Registry "footprints".



Windows Registry

- Hierarchical database stores system information.
- First introduced with Windows 95.
- Some slightly differ between versions.
- Replaces config.sys and autoexec.bat files.
- Replaces text-based initialization (.ini) in windows 3.0.

Registry Structure



Registry Structure (Cont.)

- Five main hives.
- Begin with (HKEY) Handle to a Key.
- 1. HKEY_CLASSES_ROOT
 - Open programs, drag and drop and shortcuts.
- 2. HKEY_CURRENT_USER
 - User's folders, screen colors, and Control Panel settings for the current user.
- 3. HKEY_LOCAL_MACHINE
 - Hardware-specific information, drives mounted, installed hardware.

Registry Structure (Cont.)

- 4. HKEY_USERS
 - Configuration information of all user profiles, application configurations, and visual settings.
- 5. HKEY_CURRENT_CONFIG
 - information about the systems current configuration.

Registry Structure (Cont.)

- Registry is maintained within several files on the system.
- Hives that are persistent on the system: %SYSTEMROOT%\system32\config folder.
 - HKEY_LOCAL_MACHINE\System (System folder).
- Specific user configuration:
 - Documents and Settings folder.
 - NTUSER.DAT file.

Registry as a Log File

- Registry keys have a value indicate "LastWrite" time. → FILETIME.
- Indicates Registry key last modification.
- FILETIME records 100 nanosecond intervals since midnight, 1 January 1601.

Registry as a Log File (Cont.)

Finding FILETIME example:



What's in the Registry?

- Useful forensic information within the Registry →Depends on investigator.
- Registry string search \rightarrow little data.
 - Data may be kept in binary.
 - ROT-13 "encryption".







Autostart Locations

- Allow applications to be launched without any direct user Interaction.
- Most popular: "Run" key.

• Used by many pieces of malware.

Autostart Locations (Cont.)

- Many other Registry keys launch applications and depend on actions:
 - System starts up.
 - User logs in.
- Example 1: The key



 $Software \Microsoft \CommandProcessor \AutoRun$

 Found in both the HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER hives
 launch application whenever cmd.exe is launched.

Autostart Locations (Cont.)

• Example 2: The key

HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

- Allow administrator to designate a debugger for a specific application.
- Attackers use this key to redirect an application to a Trojaned copy.



Autostart Locations (Cont.)

• Autostart locations provide the investigator with clues whether the activity initiated by the user or by malware or an attacker.



Autoruns tool from sysinternals

User Activity

- NTUSER.DAT file holds all of the Registry settings specific for a particular user.
- Its content mapped to the HKEY_USERS\SID.
- when the user logs in:
 - -HKEY_CURRENT_USER hive is created.
- Helps forensic investigators regarding actions taken by the user.



MRU Lists

- MRU: Most Recently Used
- Consist of entries made due to specific actions taken by the user.
- Keep track of items the user may return to in the future.
- Example:

 $HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU$

Maintains a list of commands that the user types into the Start → Run box

MRU Lists (Cont.)



MRU List example

MRU Lists (Cont.)

List of useful MRU lists					
XP Search Files	Software\Microsoft\Search Assistant\ACMru\5603				
Internet Search Assistant	Software\Microsoft\Search Assistant\ACMru\5001				
Printers, Computers and People	Software\Microsoft\Search Assistant\ACMru\5647				
Pictures, music, and videos	Software\Microsoft\Search Assistant\ACMru\5604				
XP Start Menu Recent	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs				
Run dialog box	Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU				
Mapped Network Drives	Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU				
WordPad - Recent Files	Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Re cent File List				

User Assist

 $Software \Microsoft \Windows \Current Version \Explorer \User \Assist$

- Contains two sub-keys globally unique identifiers(GUID).
- Each one records specific objects on the system that the user has accessed.
- Entries are "encrypted" using ROT-13.
- Not associated with a specific date and time.
- Only information if user has accessed a particular file or object. User may access malware.

User Assist (Cont.)

PropSummary	Name	Type
Propumnary PublishingWzard RecentDocs RunMRU SessionInfo Shell Folders ShellmageView StartPage StreamMRU Streams StuckRects2 tips TrayNotfy User Shell Folders User Shell Folders	Name HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Pcg. Xehapu\Qrfxgbc\Enmbe cebtenzf\c2xgbbyf\c2xgbbyf\c2xgbbyf\ HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Pcg. Xehapu\Qrfxgbc\Enmbe cebtenzf\2bgbebyn Zbovyr Co HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Pcg. Xehapu\Qrfxgbc\Enmbe cebtenzf\2bgbebyn Zbovyr Co HRZR_EHACNGU:P:\ HRZR_EHACNGU:P:\ HRZR_EHACNGU:P:\ HRZR_EHACNGU:P:\ HRZR_EHACNGU:P:\ HRZR_EHACNGU:P:\ HRZR_EHACNGU:P:\ HRZR_EHACNGU:P:\ HRZR_EHACNGU:P:\ Wake data 0000 8A 00 00 00 05 00 00 00 0008 70 EC 48 71 E8 46 C7 01 piHgèFC. 1.4k	Type IC2 REG_BUNARY Y REG_BUNARY REG_BUNARY REG_BUNARY REG_BUNARY REG_BUNARY REG_BUNARY REG_BUNARY Y REG_BUNARY Y REG_BUNARY REG_BUNARY REG_BUNARY REG_BUNARY REG_BUNARY REG_BUNARY REG_BUNARY
OD6D4F41-2994-4BA0 (5E6AB780-7743-11CF Count (75048700-EF1F-11D0 Count VisualEffects Walpaper WebWew WorkgroupGrawler Exit Extensions Group Policy	HRZR_EHACNGU:P:) 0010 HRZR_EHACNGU:P:) HRZR_EHACNGU:P:) HRZR_EHACNGU:P:) HRZR_EHACNGU:P:) HRZR_EHACNGU:P:) HRZR_EHACNGU:P:) HRZR_EHACNGU:P:) HRZR_EHACNGU:P:) HRZR_EHACNGU:P:) OK Cancel	REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_BINARY REG_BINARY

Decoded Text

UIME RUNPATH:C:\\Documents and Settings\\Cpt. Krunch\\Desktop\\Razor programs\\p2ktools\\p2ktools\\P2KTools.exe

USB Removable Storage

• Connecting USB removable storage to windows system initiated an entry under

 $HKEY_LOCAL_MACHINE \ System \ ControlSet00x \ Enum \ USBSTOR$

- Stores the contents of the product and device ID values of USB devices.
- Devices could be cameras or thumb drives.

- Device ID could be the serial number (unique).
- Not all USB thumb drives have serial numbers.
- If the 2nd character of the ID had "&' → device has no serial number.
- Other registry locations provides more details to the investigator.



Cok view ravorkes nep	inser		112235	
USBPRINT USBSTOR GdRomälven_äProd_USB_Flash_Memory&Rev_6.50 GdRomälven_SanDiskäProd_U3_Cruzer_Micro@Rev_2.18 Oiskälven_BProd_BRev_2.15 Diskälven_BProd_USB_Flash_Memory&Rev_6.50 Diskälven_Apple&Prod_Pod&Rev_2.70 Diskälven_Generic&Prod_USB_Storage-CFCBRev_500A Diskälven_Generic&Prod_USB_Storage-MMC&Rev_500A Diskälven_Generic&Prod_USB_Storage-SMC&Rev_500A Diskälven_Generic&Prod_USB_Storage-SMC&Rev_1000 Diskälven_Generic&Prod_USB_Storage-SMC&Rev_2.18 Diskälven_Matshta&Prod_UVC&Rev_1.00 Diskälven_Matshta&Prod_UVC&Rev_1.00 Diskälven_Matshta&Prod_USB_Storage-SMC&Rev_0.00 Diskälven_Simple&Prod_Bonzal_Vipress&Rev_0.00 Diskälven_WD&Prod_250038_External&Rev_0.002 V1394 Hardware Profiles Services	Name (Default) Capabilities Capabilities Cass Cass CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs Priver PriverdyName CompatibleIDs PriverdyName CompatibleIDs PriverdyName CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs CompatibleIDs Comp	Type REG_SZ REG_DWORD REG_SZ REG_SZ REG_DWORD REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_DWORD	Data (value not set) 0x00000010 (16) DiskDrive (4D36E967-E325-11CE-BFC1-080028E10318} USBSTOR\Disk USBSTOR\RAW 0x00000000 (0) Disk drive (4D36E967-E325-11CE-BFC1-080028E10318}\0007 SanDisk U3 Cruzer Micro U58 Device USBSTOR\DiskSanDisk_U3_Cruzer_Micro_2.18 U585TOF (Standard disk drives) 76226a6d2e80 disk 0x00000000 (0)	Contents of USBSTOR key



No serial number case

26

• Mounted Devices:

 $HKEY_LOCAL_MACHINE \ System \ Mounted Devices$

- View each drive associated with the system.
- Stores a database of mounted volumes used by NTFS.
- The investigator may indicate that the user removed the drive if:
 - a device is in the list of MountedDevices and it is not physically in the system.

* DE	Name		Turne	Data	
B ISAPNP B ISAPNP B IPTENUM B IPTENUM	177/Volume(97b1382b-4	17/Wolume(97b1382b-4c69-11db-aa96-0013d45b0a97) 17/Wolume(9dc8eadd-8161-11db-aad9-0013d45b0a97) 17/Wolume(a3642af6-		5c 00 3f 00 3f 00 5c 0 42 ae 74 5c 00 7e 00 1 5c 0	0 53 00 54 00 00 00 C 0 53 00 54
H PCI H PCIIDE H Root H SCSI	1/7?(Volume(ac531244- 1/7?(Volume(b5fcea4f-6 1/7?(Volume(db7d1868- 1/7?(Volume(f1969b1a-	Edit Binary Value 100 \77ac531244- Edit Binary Value 100 \77\Wolume{b5fcea4f-8 Value name: 100 \77\Wolume{db7d1868- Value name: 100 \77\Wolume{f1969b1a- \DotDevices\F:		2 X 5c0 5c0 5c0 5c0	5: 00 53 00 43 5: 00 53 00 54 5: 00 53 00 54 5: 00 53 00 54 5: 00 49 00 44
STORAGE Stream Stream SW USBPRINT USBPRINT USBSTOR USBSTOR V1394 Hardware Profiles Services Services USBSTOR USBSTOR Services Services Select Select Select Setup WPA HKEY_USERS	Volume (f1969b1b-)DosDevices (A:)DosDevices (C:)DosDevices (D:)DosDevices (E:)DosDevices (F:)DosDevices (F:)DosDevices (H:)DosDevices (H:)DosDevices (I:)DosDevices (I:)Dos	Value data: 0000 50 00 3F 00 3 0008 53 00 54 00 4 0010 41 00 47 00 4 0010 41 00 47 00 4 0018 52 00 65 00 6 0020 76 00 61 00 6 0030 63 00 61 00 2 0038 26 00 65 00 3 0048 26 00 30 00 2 0050 4D 00 23 00 77 0058 33 00 66 00 3 0060 33 00 30 66 67	00 5C 00 00 52 00 00 62 00 00 6F 00 00 6C 00 00 64 00 00 37 00 00 65 00 00 34 00 5 00 35 00 5 00 36 00 4 00 2D 00 5 00 6K	St 00 S T 0 R A G E # S T 0 R A G E # S 00 S 00	0 49 00 44 0 46 00 44 00 00 00 0 0 49 00 44 0 53 00 54 0 55 00 55 0 53 00 54

Identification of volume \DosDevice\F

Wireless SSIDs

• Service set identifiers (SSIDs) are stored In the wireless card.

HKEY_LOCAL_MACHINE\Software\Microsoft\ WZCSVC\Parameters\Interfaces



- Different sub-keys (GUID).
- SSID name in binary data format.

Wireless SSIDs (Cont.)

🗑 🧰 TShoot 🛛 👩			
 Tuning Spaces Updates UPnP Device Host VBA VisualStudio VSAnsi WA8 WBEM Web Folders Web Service Providers Windows Media Device Mi Windows Media Device Mi Windows Script Host Windows Script Host Windows Scripting Host Mozella MozellaPlugins 	Name (Default) ActiveSettings ControlFlags LayoutVersion Static#0000 Static#0001 Value name: Static#0001 Value data: 0000 C8 00 0018 6E 2 0020 00 0 0018 6E 2 0020 00 0 0038 A3 F1 0040 20 0 0058 00 0 0058 0 00 0 0058 0 00 0 0058 0 00 0 000 0 0000 0 000	Type REG_SZ REG_BINARY REG_DWORD REG_DWORD REG_BINARY REG_GONONON REG_GONONONON	Deta (value not set) c8 02 00 00 00 00 00 00 e0 98 db b6 10 00 00 0c 0. 0x03918002 (59867138) 0x00000007 (7) c8 02 00 00 00 00 00 00 00 c6 f01 b9 ba 00 00 09 00 C8 02 00 00 00 00 00 00 02 6f 01 b9 ba 00 00 09 00 C8 02 00 00 00 00 00 00 00 02 6f 01 b9 ba 00 00 09 00 C8 02 00 00 00 00 00 00 00 00 02 6f 01 b9 ba 00 00 09 00 C8 02 00 00 00 00 00 00 00 00 02 6f 01 b9 ba 00 00 09 00 C8 02 00 00 00 00 00 00 00 00 00 02 6f 01 b9 ba 00 00 09 00 C8 02 00 00 00 00 00 00 00 00 00 02 6f 01 b9 ba 00 00 09 00 C8 02 00 00 00 00 00 00 00 00 00 00 00 00

SSID example

Wireless SSIDs (Cont.)

• Additional information such as IP address, DHCP domain, subnet mask.

HKEY_LOCAL_MACHINE\System\Current ControlSet\Services\TCPIP\Interfaces\GUID

• IP addresses and durations will be more helpful for investigators.



Wireless SSIDs (Cont.)

💣 Registry Editor				
File Edit View Favorites Help				
🕀 🧰 SynTP 🛛 📉	Name	Туре	Data	~
 sysaudio SysmonLog TapiSrv Tcpip Enum Linkage Parameters Adapters DNSRegisteredAdapters Interfaces {1B217E32-E44A-483 {2652504A-46D0-496 {6085DCC1-A86B-423 {9841CABF-F2E8-43F {9841CABF-F2E8-43F {DE98437C-5ABE-466 {FE75A3FA-1347-469 PersistentRoutes Winsock 	(Default) AddressType DefaultGateway DefaultGateway DefaultGateway DhcpClassIdBin DhcpDefaultGate DhcpDefaultGate DhcpIPAddress DhcpIPAddress DhcpSubnetMask DhcpSubnetMask DhcpSubnetMask DhcpSubnetMask DhcpSubnetMask DhcpSubnetMask DhcpSubnetMask DhcpSubnetMask Domain EnableDeadGWD EnableDHCP DhcpSubnetMask	REG_SZ REG_DWORD REG_MULTI_SZ REG_MULTI_SZ REG_BINARY REG_MULTI_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_DWORD REG_DWORD REG_MULTI_SZ	(value not set) 0x00000000 (0) (zero-length binary value) 192.168.1.1 myhome.westell.com 192.168.1.37 192.168.1.1 192.168.1.1 255.255.255.0 255.255.255.0 0x00000001 (1) 0x00000001 (1) 0.0.0	
< × ×	<	REG_52	0.0.0.0	>
My Computer\HKEY_LOCAL_MACHINE\SYSTEM	ControlSet001\Services\1	cpip\Parameters\Inte	erfaces\{FE75A3FA-1347-469C-B29A-C067	10C575EA}

Network settings of SSID

Summary

- Windows Registry is a significant forensic resource.
- Provides a comprehensive picture of the case.
- An investigator need to know where to look.
- This paper presents some Registry information but there are more.

Thank You

