Harnessing the Registry to Identify Malware

Elizabeth Schweinsberg
bethlogic@gmail.com

Why Use the Registry?

- For most malware to be useful, it needs to persist through shutdown
- The Windows Registry controls some of the most likely places for that information to be stored

Overview

- What is the Windows Registry?
- What information is available?
- What tools are there?

What is the Windows Registry?

"The repository for both system-wide and per-user settings."[1]

It is a tree structure of keys that contain subkeys and values.

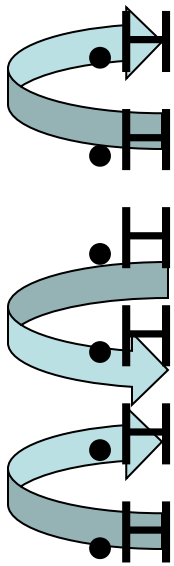
[1]Windows Internals, Fifth Edition by Mark Russinovich and David Solomon

Who uses the Registry?

- System Boot
  - Identifies device drivers and configurations for subprocesses and services
- Applications
  - Application settings are stored here
- User Preferences
  - Stores drive mappings, icon placement, wall paper, etc

The Root Keys

- HKEY_USERS
- HKEY_CURRENT_USER
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_CURRENT_CONFIG
- HKEY_PERFORMANCE_DATA



Hives

- Binary files containing the registry tree
- Root Keys are stored in different hives
- Local Machine Hives are stored in “<systemroot>\System32\config”
- User hives are stored in “Documents and Settings\<username>\NTUser.dat”

Hives, Cont.

Name	Contents
System	Boot information, hardware, services
Software	Application configurations applicable to all users
NTUser	Per-user configuration information
SAM	Local account and group information
Hardware	Inventory of active hardware
Security	System wide security policies

Hive Structure

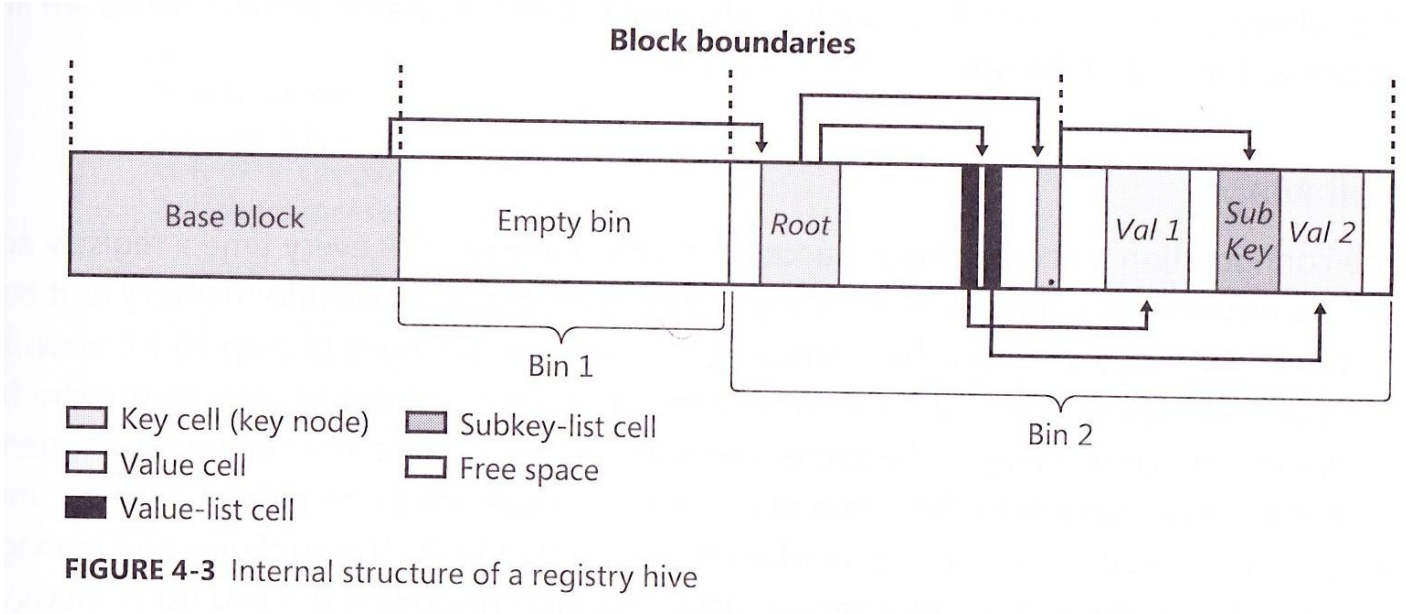


FIGURE 4-3 Internal structure of a registry hive

[1]Windows Internals, Fifth Edition by Mark Russinovich and David Solomon

Registry in Memory

- The registry is loaded into memory
  - Quick access to frequently used keys
  - To save space in memory, each hive is not loaded in its entirety
- An array tracks blocks that have been modified since the last write
  - When a write is triggered, only modified segments are written back to the file
  - Used to correct corruption due to unexpected shutdown

Registry Data Types

- There are 14 data types total, but some are more prevalent than others
  - REG_NONE
  - REG_SZ[1] – Fixed Length Unicode String
  - REG_DWord – 32-bit number
  - REG_BINARY – Arbitrary length binary data
  - REG_LINK – Unicode symbolic link
  - REG_MULTI_SZ – Array of REG_SZ

[1]Sometimes REG_SZ are ROT13 encoded for “security”. Many tools detect and counter this so it is transparent to the user.

What to Look For?

Hive	Key	Use
Software NTUser	Microsoft\Windows\CurrentVersion\Run	Programs run after boot, but before full user control
System	CurrentControlSet\Services	Services and device drivers started at or just after boot
NTUser	Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Most Recently Run programs
Software	Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler; Software\Classes\CLSID\{***}	Scheduled Tasks
System	CurrentControlSet\Control\BootVerificationProgram	Programs run to verify proper boot
Software	Microsoft\Windows NT\CurrentVersion\svchost	Services authorized to run under Svchost

Services

- Processes not tied to an interactive user
  - Web servers
  - Logon service
  - Networking

Device Drivers

- Loadable kernel modules that interface between the I/O manager and relevant hardware
- Types of Drivers:
  - Hardware
  - file systems
  - networking protocols
  - kernel streaming filters for A/V

Registry Parameters

HKLM\System\CurrentControlSet\Services

- DisplayName
- ImagePath – Path to the dll, exe, or sys (required for services)
- ObjectName (owner)
- Description
- Group (Groups services for starting order)
- Tag (Orders services within a group)

Registry Parameters, Cont.

Type	
Code	Meaning
0x001	Kernel Driver
0x002	File System Driver
0x010	Own_Process
0x020	Share_Process
0x100	Interactive

Start	
Code	Meaning
0x0	Boot Start (drivers only)
0x1	System Start (drivers only)
0x2	Auto Start
0x3	Manual
0x4	Disabled

What to highlight?

- Services cannot have a start of “Boot” or “System”
- Services without “ObjectName” that is set to:
  - Local System
  - NT AUTHORITY\LocalService
  - NT AUTHORITY\NetworkService
- Services starting under the Svchost process must have an entry in “Software\Microsoft\ Windows NT\CurrentVersion\svchost”

What to highlight? Cont.

- Drivers should be in “system32\Drivers” or in a manufacturer’s area, e.g. Dell
- Drivers should have a file extension of “sys” – look in “ImagePath”
- Drivers should not have a value for “ObjectName”

How to research?

- Don’t know what an executable does? Google it!
- ProcessLibrary.com – searchable index of Windows processes
- Create a “known good” list from your baseline
- Windows resources – Windows Internals, MSDN

Baseline Hives

- A copy of the Original Hive from installation is in “<systemroot>\System32\config\<hive>.sav”
- If System Restore is activated, then there are copies of the hive files in the Restore Points
- Retrieve the Hives from the Master Image
- Have Roaming Profiles? NTUser.dat files on other systems the user logged into

Services

<systemroot>\System32 – or as specified

- Smss.exe
  - Autochk.exe
- Csrss.exe
- Lsass.exe
  - Tbssvc.exe
  - Vssvc.exe
  - Kerberos.dll
  - Kdcsv.dll
  - Samsrv.exe
  - Samss.exe
  - Netlogon.exe
  - KeyIso.exe
  - Lsasrv.exe
  - Ntdsa.exe
- Wininit.exe
- Windload.exe

- Svchost.exe
  - Umpnpmgr.dll
  - Tapisrv.exe
  - RasMan.exe
  - RpcSS.exe
  - Netsvcs.exe
  - Netman.exe
  - Wudfsvc.exe
  - Dps.dll
  - Wlanext.exe
  - WudfHost.exe
  - Mpssvc.exe
- Winlogon.exe
- Services.exe

- Explorer.exe
- Taskeng.exe
- Audiodg.exe
- Vds.exe
- Dyn.exe
- Bus.exe
- Dns.exe
- Bfe.dll
- Dfssvc.exe
- Ntlanman.dll
- Ikeext.exe
- Lsm.exe
- Slsvc.exe

Device Drivers

<systemroot>\System32\Drivers unless otherwise specified

- Win32.sys
- Classpnp.sys
- Tpm.sys
- Hiberfil.sys
- Ecache.sys
- Clfs.sys

Ports

- Usbprint.sys
- Parport.sys
- Usbstor.sys
- Ataport.sys
- Scsiport.sys
- Storport.sys

File Systems

- Mpio.sys
- Partmgr.sys
- Volmgr.sys
- Volmgrx.sys
- Mountmgr.sys
- Fs_rec.sys
- Fvevol.sys
- Volsnap.sys
- Ntfs.sys
- Fastfat.sys
- Exfat.sys
- Udfs.sys
- Cdfs.sys
- Npfs.sys
- Msfs.sys

Networking

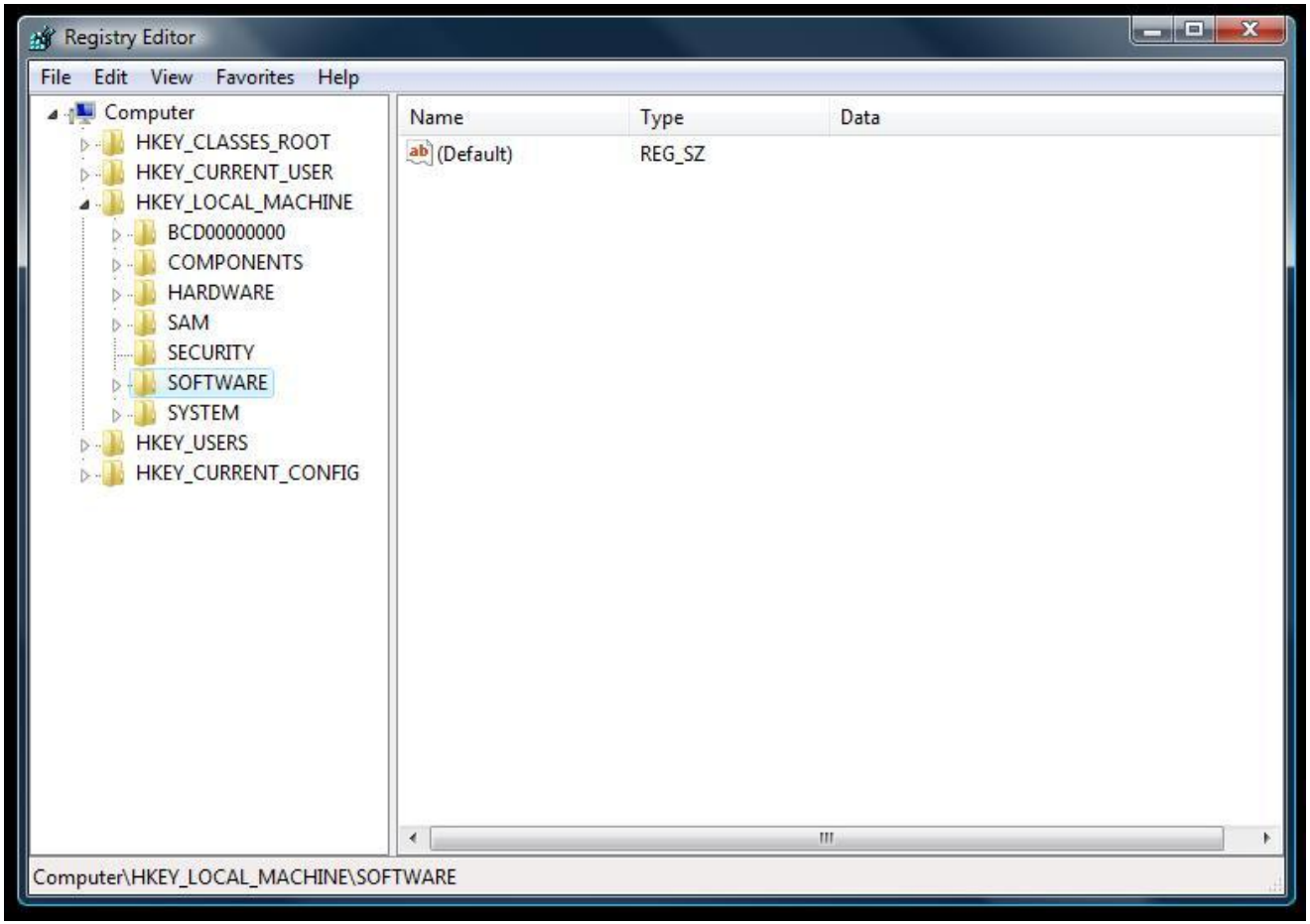
- Ndis.sys
- Afd.sys
- Netbt.sys
- http.sys
- Tcpip.sys
- Netbios.sys
- Mup.sys
- Atm.sys
- Netio.sys
- Msrpc.sys
- Rdbss.sys
- Fwpkclnt.sys
- Lpnat.sys
- Mpsdrv.sys
- Ipsec.sys

Networking, Cont.

- Rndismp.sys
- Pacer.sys
- Dfs.sys
- Dfsc.sys

Interactive Registry Tools

- Process Monitor
- RegEdit



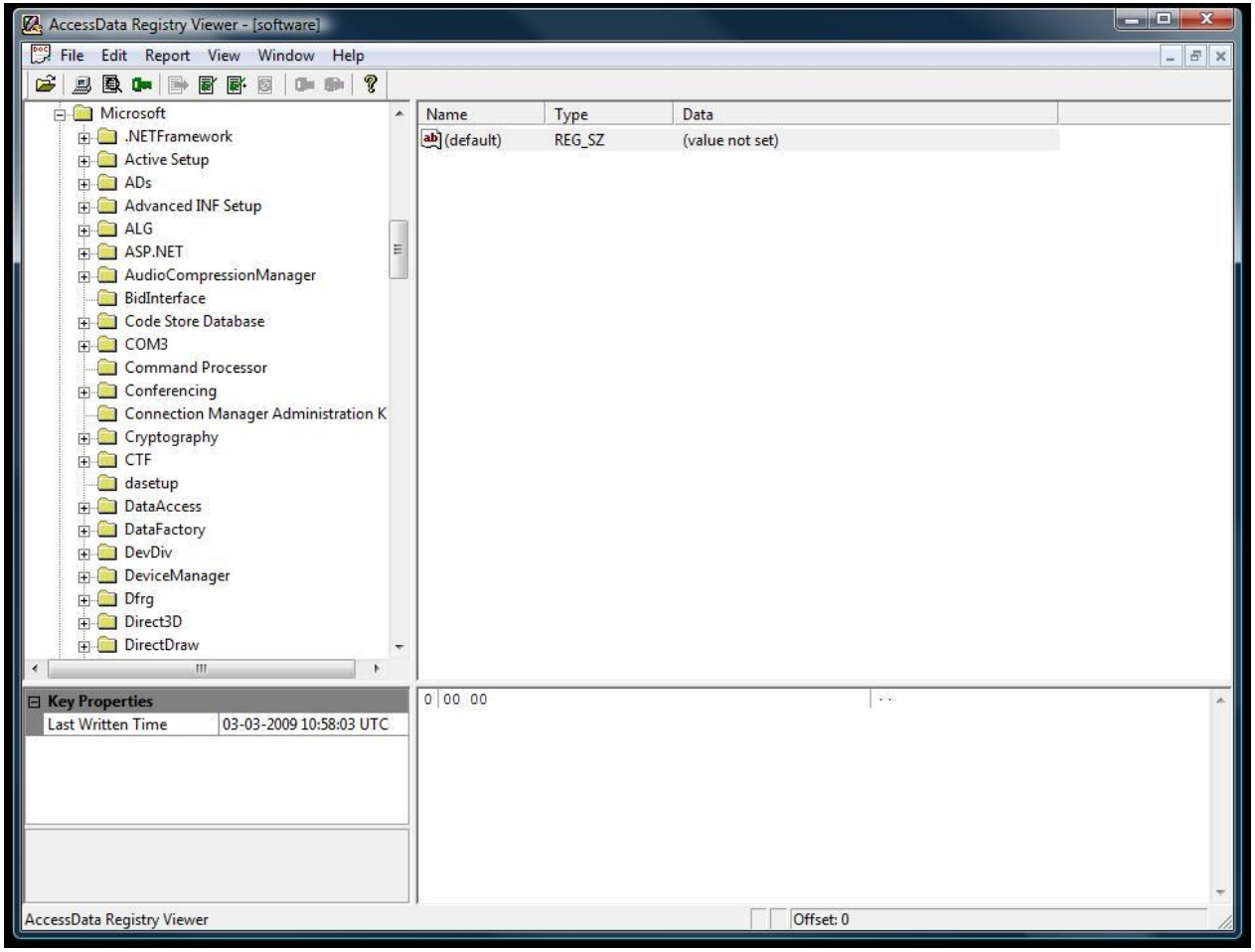
Memory Image Analysis

- Volatility – command line memory parsing tool
  - Now includes RegRipper port
  - Volatilesystems.com
- Memoryze by Mandiant
  - www.Mandiant.com/products/free_software/memoryze/

Disk Image Tools

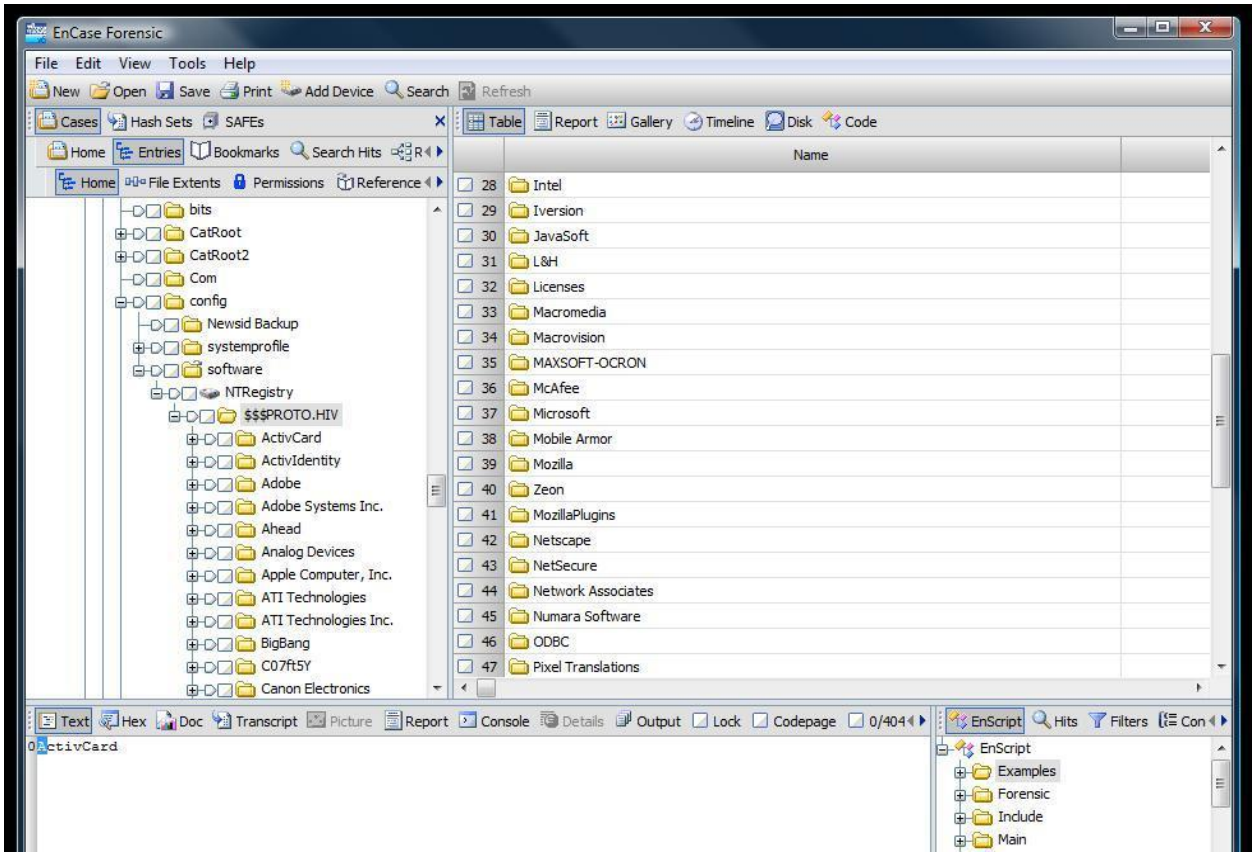
- FTK Registry Viewer
- EnCase
- RegRipper

AccessData FTK Registry Viewer



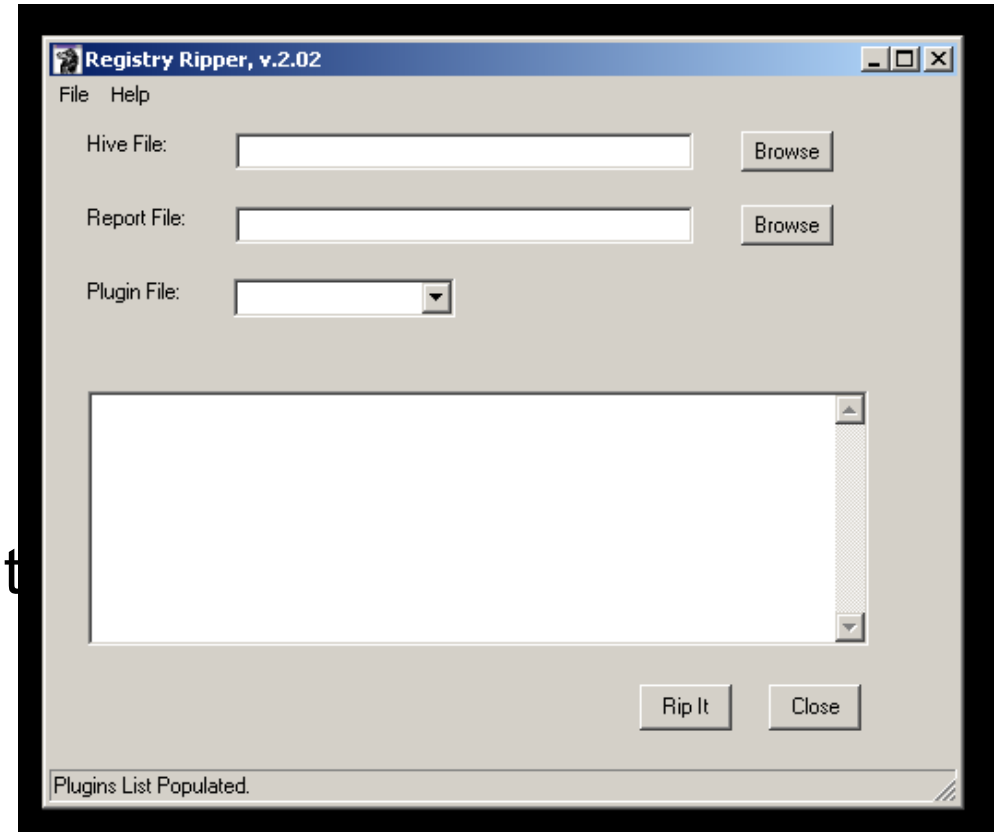
www.accessdata.com/downloads

EnCase Registry View



RegRipper

- Open Source Windows Registry analysis tool by Harlan Carvey
- www.RegRipper.net
- Perl framework with easy to use plugin architecture
- Runs on hive files extracted from an image
- Only keys from the current control set



Favorite Plugins

Plugin	Description
User_run, soft_run	User and System run keys to auto-start programs
Services, svc	All services and device drivers in the registry
Svchost	Which processes can run under svchost
User_win	Programs run when the user logs in – should be blank

RipXP

- Runs a plugin against the current hive and restore points from the same system for comparisons of registry keys altered
- Must extract the hives and restore points – in their original directory structure – before running

Acknowledgements

- Mark Russinovich and David Solomon for writing the Windows Internals book which is referenced heavily here
- Harlan Carvey for continued development of RegRipper

References

- RegRipper, RipXP: regripper.net
- Windows Processes: ProcessLibrary.com
- Windows SysInternals: microsoft.com/en-us/sysinternals/default.aspx
- Registry Viewer: accessdata.com/downloads

Elizabeth Schweinsberg: bethlogic@gmail.com