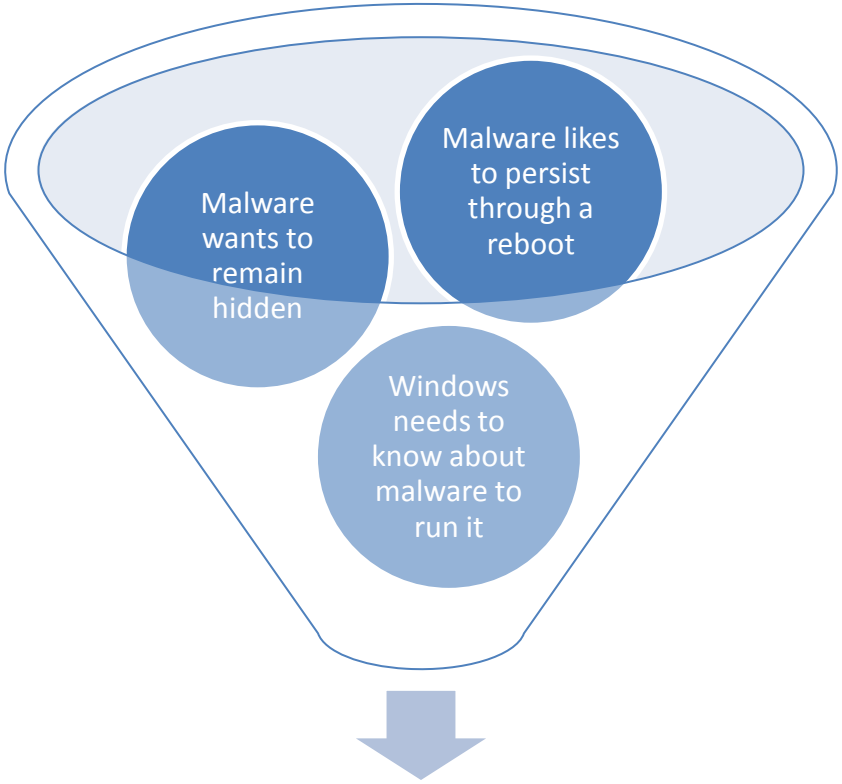
Is This Normal?
The ABCDE's of Registry Analysis

Elizabeth Schweinsberg

Why Use the Registry?

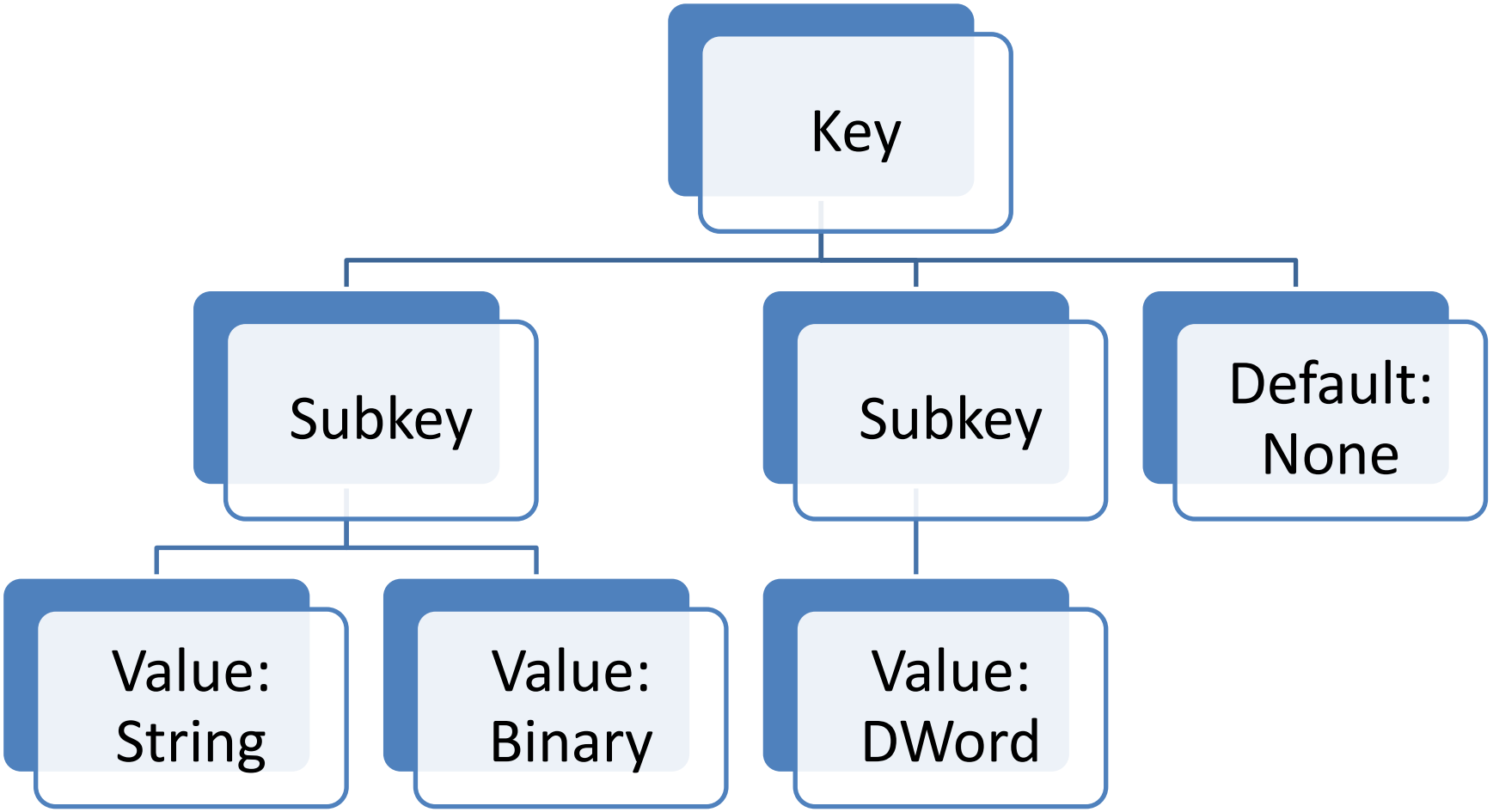


The Registry is a good place to trigger execution and find a way to hide

Overview

- Quick Overview of the Registry
- Tools to Use Right Away
- ABCDEs

What is the Windows Registry?



Who Uses the Registry?

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

Root Keys, Hives, and Files

Files

- Binary Files store the Registry Tree
- System Hives are stored in <SystemRoot>\System32\config
- User Hives are stored in “Documents and Settings\<username>\NTUser.dat”

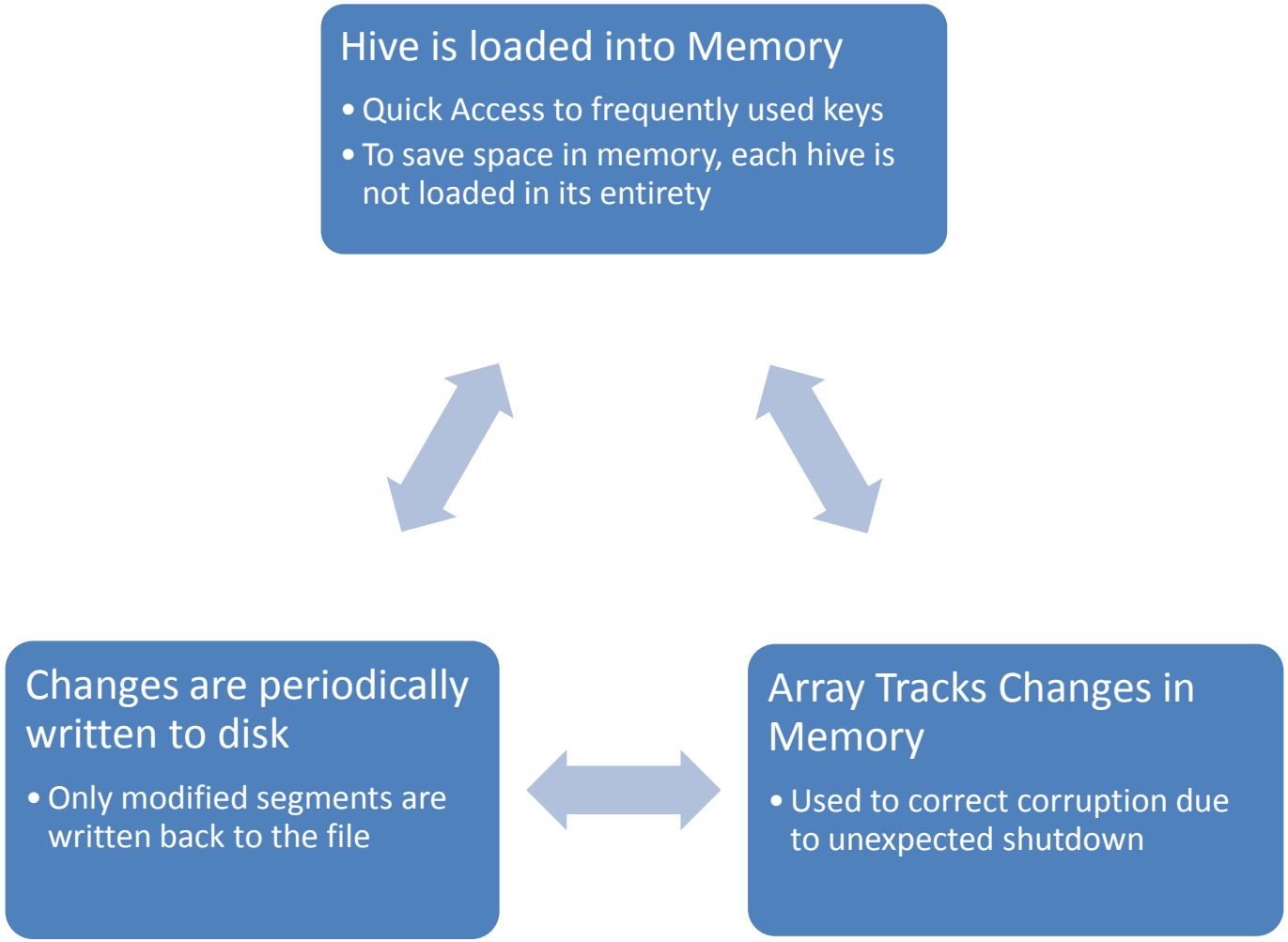
Hives

- Each Hive focuses on a different root key
- Your favorite hives are going to be: Software, System, NTUser and SAM

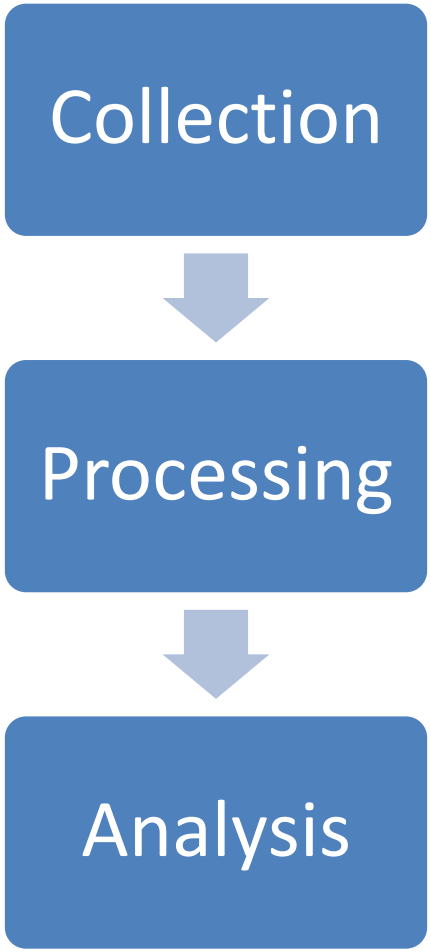
RootKeys

- HKEY_CURRENT_USER (NTUser) points to an entry in HKEY_USERS
- HKEY_CLASSES_ROOT (Software) and HKEY_CURRENT_CONFIG (System) point to HKEY_LOCAL_MACHINE

The Registry in Memory



Tools to Use Right Away



Collection

fget

- HBGary volatile forensic collection tool
- www.hbgary.com/community/free-tools

F-Response

- Live forensics access including over IP networks
- www.f-response.com

Reg.exe

- Save a registry hive from a running drive; Included in Windows
- Reg.exe SAVE HKLM\SYSTEM system.hive

Export from a drive image using your Favorite Tool

Processing

Registry Viewer

- Access Data tool, available for free use on small files
- Mostly manual processing, but one can create “highlights” for quick filtering
- www.accessdata.com/downloads.html

ProDiscover

- Forensics Platform with the ability to write Perl scripts for registry processing; Free Demo
- WFA/2e by Harlan Carvey has lots of example scripts
- Techpathways.com

RegRipper

- Open Source Registry Parsing Tool by Harlan Carvey
- Easily extensible (assuming you can read and write Perl)
- Regripper.net

Analysis

Excel/Notepad

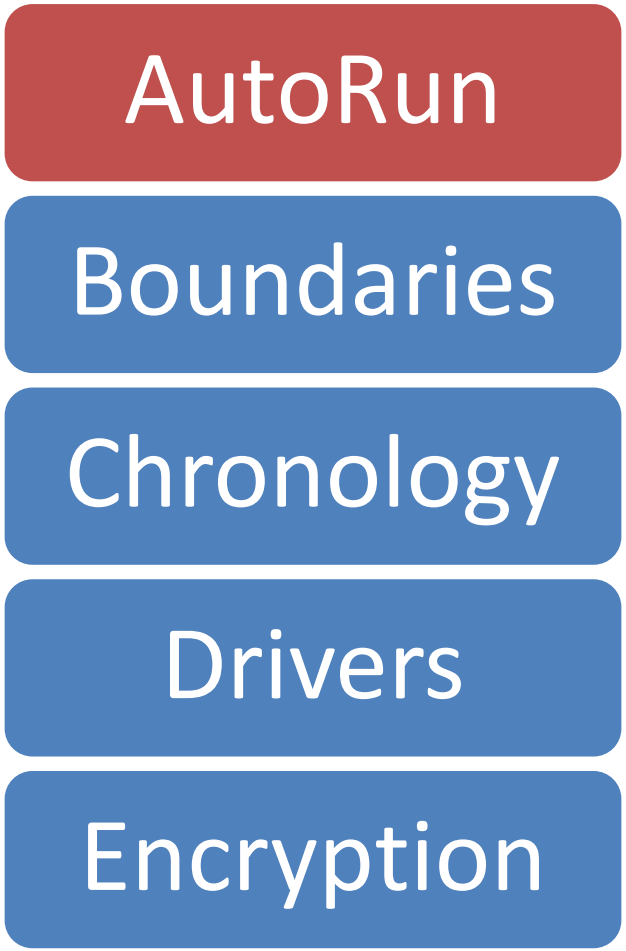
- Sifting through results by hand

SIFT from SANS

- RegRipper is built-in!

Registry Values from Memory

- Volatility has a RegRipper port for looking at registry keys that can be found in memory


AutoRun
Boundaries
Chronology
Drivers
Encryption

AutoRun

"Locations that allow applications to be launched without any interaction from the user"[1]

Services	• Processes not tied to an interactive user
User Login and Activity	• Actions when a specific users logs on • Actions when a user does something
Browser Helper Objects	• Applications Internet Explorer uses to load other programs

[1] Windows Forensic Analysis, 2nd Edition

AutoRun Details

Services

- SYSTEM\CurrentControlSet\Services
- Type is 0x10, 0x20, 0x100; Start is 2, 3, or 4 ONLY
- Services without “ObjectName” that is set to: LocalSystem, NT AUTHORITY\LocalService, or NT AUTHORITY\NetworkService
- Services starting under the Svchost process must have an entry in SOFTWARE\Microsoft\Windows NT\CurrentVersion\svchost
- RR: services (SYS) or svc (SYS); svchost (SW)

Scheduled Tasks

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shared Task Scheduler
- SOFTWARE\Classes\CLSID\{GUID}

Browser Helper Objects

- SOWFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
- RR: bho (SW)

AutoRun Details, cont.

Run, RunOnce

- SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- RR: soft_run (SW), user_run (NT), user_win (NT) – RunOnce is not checked by the plugins

Winlogin\Notify

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin\Notify
- RR: winlogon (NT), Notify must be checked manually

How files are run

- SOFTWARE\Classes\{filetype}\Shell\Open\Command
- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts
- RR: cmd_shell (SW), fileexts (SW)

AutoRun Details, cont.

Application Initialization

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
- RR: appinitdll (SW)

Actions that happen when cmd starts

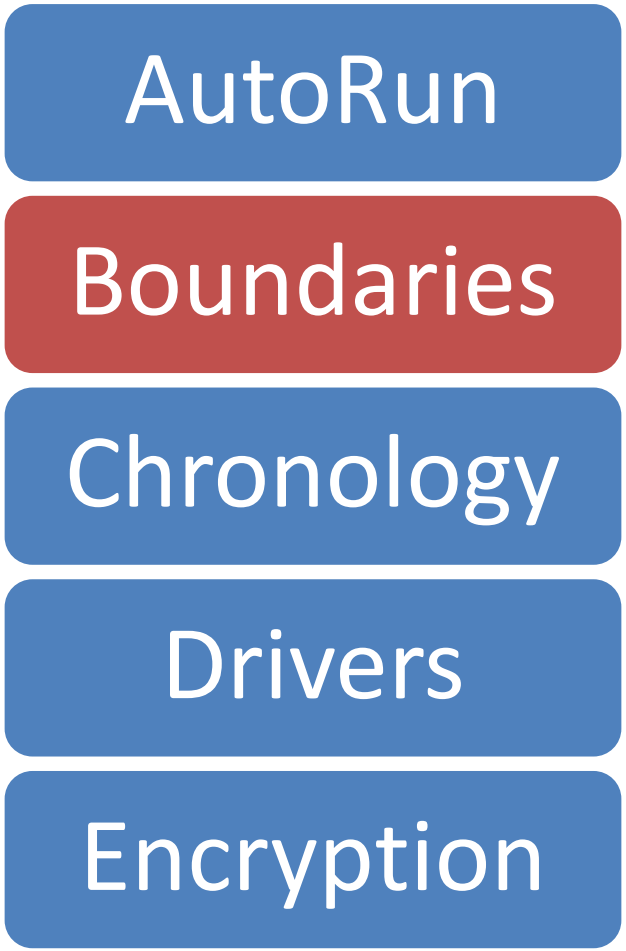
- SOFTWARE\Microsoft\Command Processor\Auto Run

Boot Verification

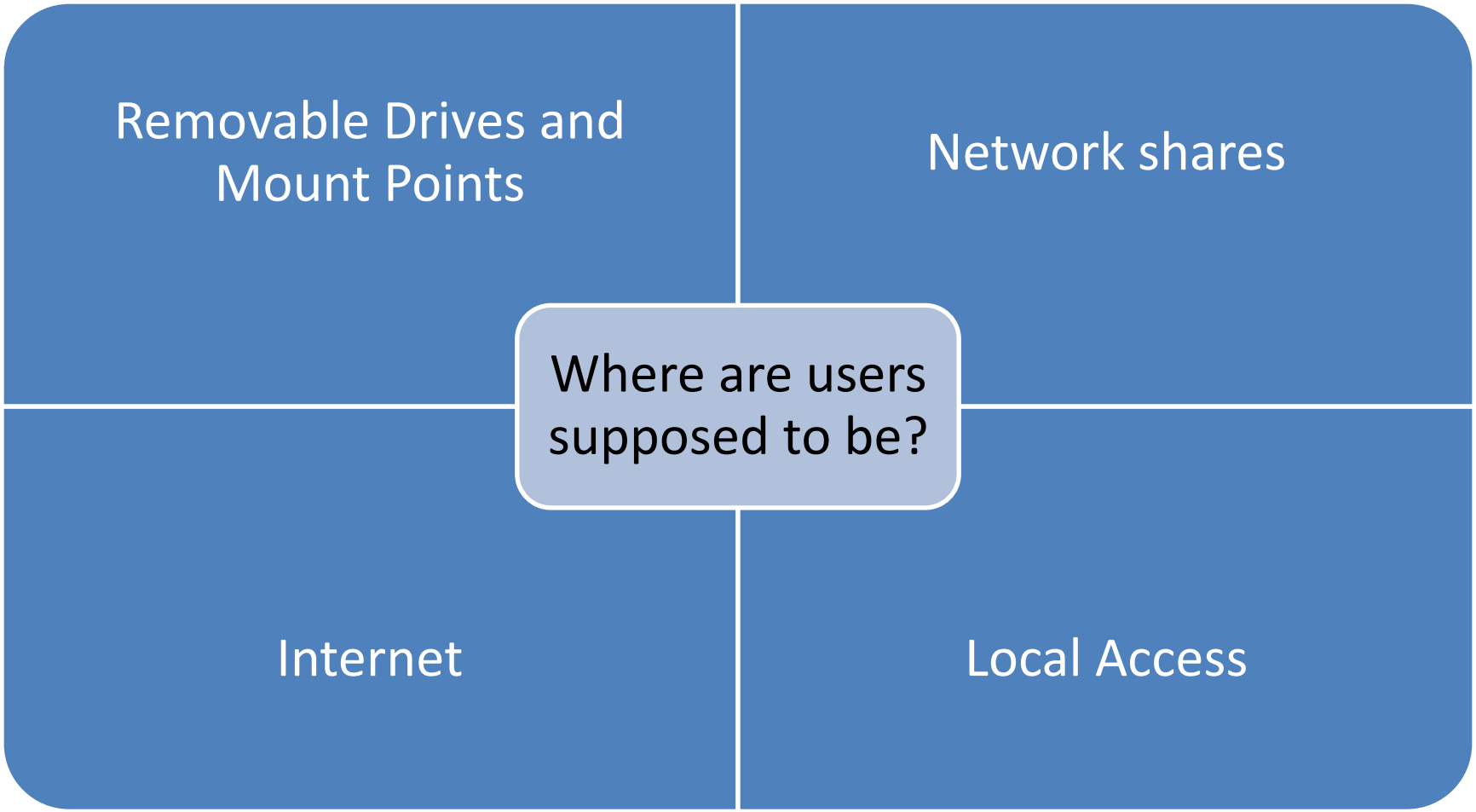
- SYSTEM\CurrentControlSet\Control\BootVerificationProgram

Execute on Boot

- SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute


AutoRun
Boundaries
Chronology
Drivers
Encryption

Boundaries


Removable Drives and Mount Points
Network shares
Where are users supposed to be?
Internet
Local Access

Boundary Details

Removable Drives

- SYSTEM\Mounted Devices
- SYSTEM\CurrentControlSet\Enumb\USBSTOR
- SOFTWARE\Microsoft\Windows Portable Devices\Devices
- RR: mountdev (SYS), usbstor (SYS), port_dev (SW)

Network Shares

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
- SYSTEM\CurrentControlSet\Services\Lanmanserver\Shares
- RR: mp2 (SW), mndmru (SW), shares (SYS)

Internet Access

- Typed URLS: SOFTWARE\Microsoft\Internet Explorer\TypedURLs (RR: typedurls (NT))
- ZoneMaps: SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\Domain
- Firewall Policies: SYSTEM\Services\Shared Access\Parameters\Firewall Policy (RR: fw_config (SW))

Boundary Details, cont.

Terminal Server Connections

- SYSTEM\CurrentControlSet\Control\Terminal Server

Recently Used Applications

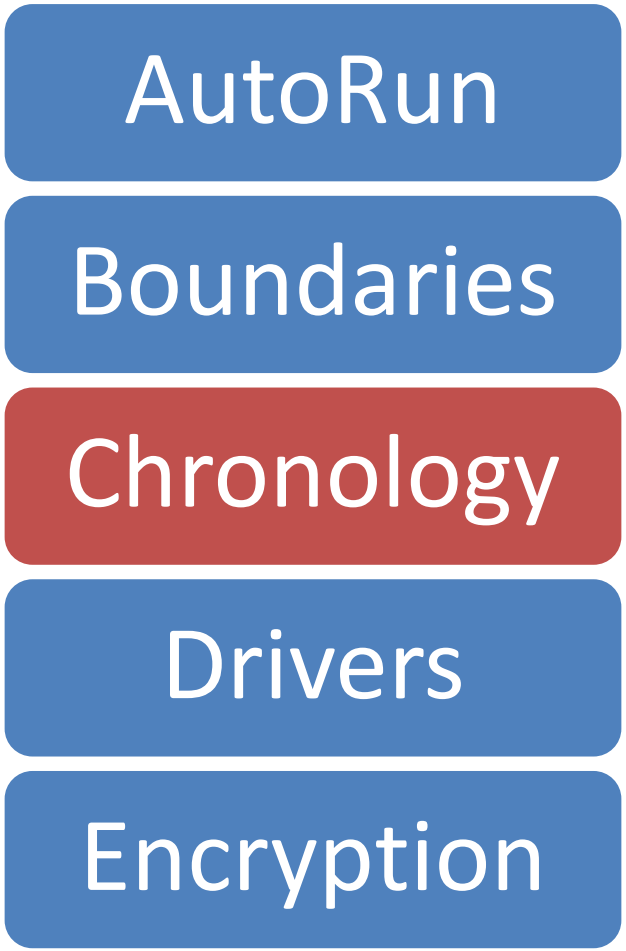
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
- RR: runmru (NT)

Searching on the drive

- HKCU\SOFTWARE\Microsoft\Search Assistant\ACMru
- RR: acmru (NT)

Recent Users

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
- RR: profilelist (SW)


AutoRun
Boundaries
Chronology
Drivers
Encryption

Chronology

System

- Installation time, Time zone, Last Shutdown
- Restore Points available?
- File Access time changed?
- Files deleted automatically?

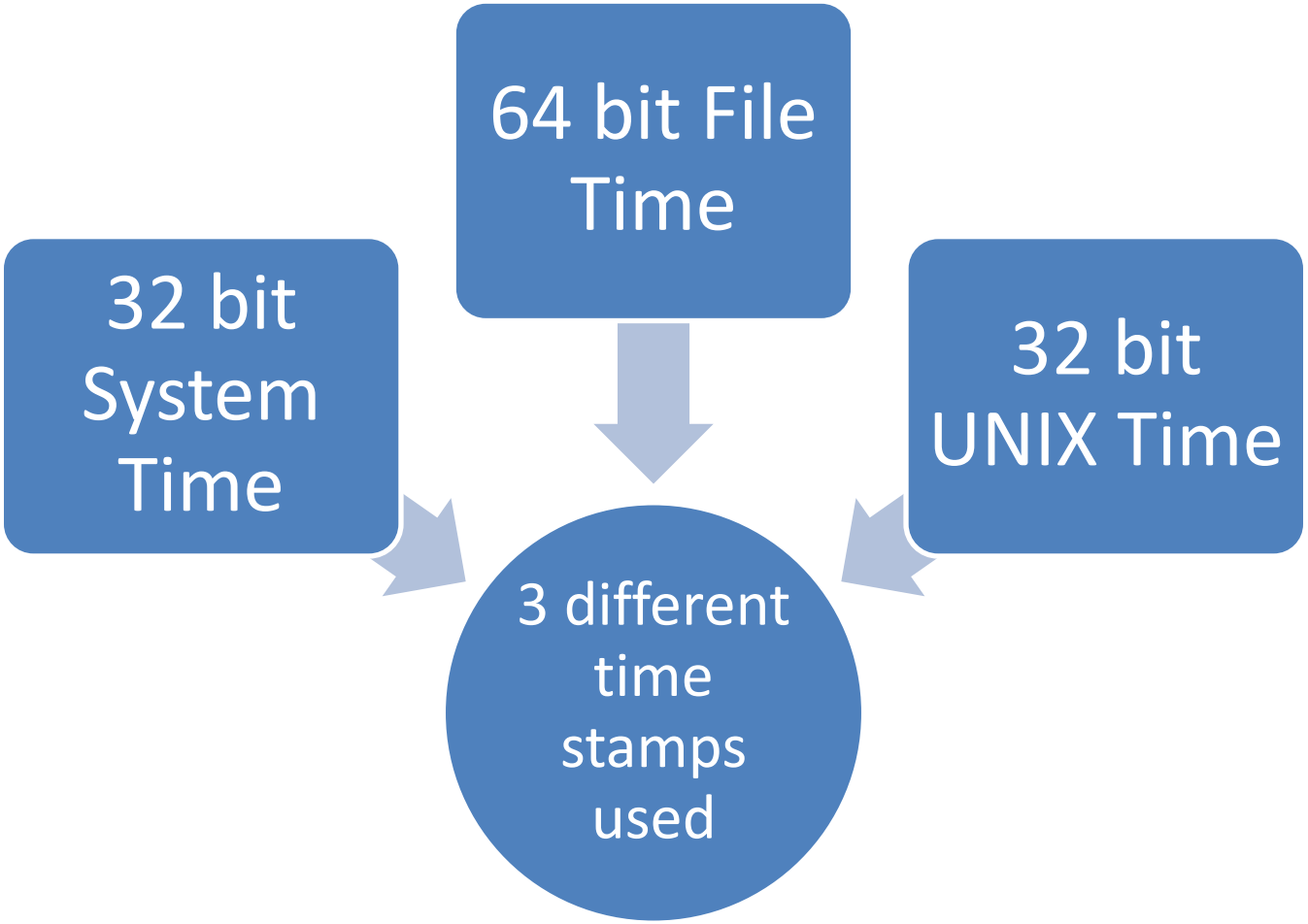
Users

- When were users created?
- When were audit policies changed?
- When did a user last access a file?
- Are there deleted registry keys?

Devices

- Mounted Devices
- USBs Installed
- Other Mount Points

A Note on Time



Chronology Details

Installation time

- SOFTWARE\Microsoft]Windows NT\CurrentVersion
- RR: winnt_cv (SW) or winver (SW)

Time zone

- SYSTEM\CurrentControlSet\Control\TimeZoneInformation
- RR: timezone (SYS)

Shutdown Time

- SYSTEM\CurrentControlSet\Control\Windows
- RR: shutdown (SYS)

Delete files?

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket
- RR: bitbucket (SW), vista_bitbucket (SW)

Disable Last Access

- SYSTEM\CurrentControlSet\Control\FileSystem
- RR: disablelastaccess (SYS)

Chronology Details, cont.

User Creation

- Stored in a binary tool; best done with a tool
- RR: samparse (SAM)

Audit Policies

- SECURITY\Policy\PolAdt\Ev
- RR: auditpol (Use the plugin)

User Actions

- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- RR: userassist (NT), runmru (NT)

Chronology Details, cont.

Mounted Devices

- The installation of USB devices is written to the file “setupapi.log” complete with timestamp
- SYSTEM\Mounted Devices
- SYSTEM\CurrentControlSet\Enum\USBSTOR
- SOFTWARE\Microsoft\Windows Portable Devices\Devices
- RR: mountdev (SYS), usbstor (SYS), port_dev (SW)

Mount Points

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
- SYSTEM\CurrentControlSet\Services\Lanmanserver\Shares
- RR: mp2 (SW), mndmru (SW), shares (SYS)

More on Time

Deleted Registry Keys

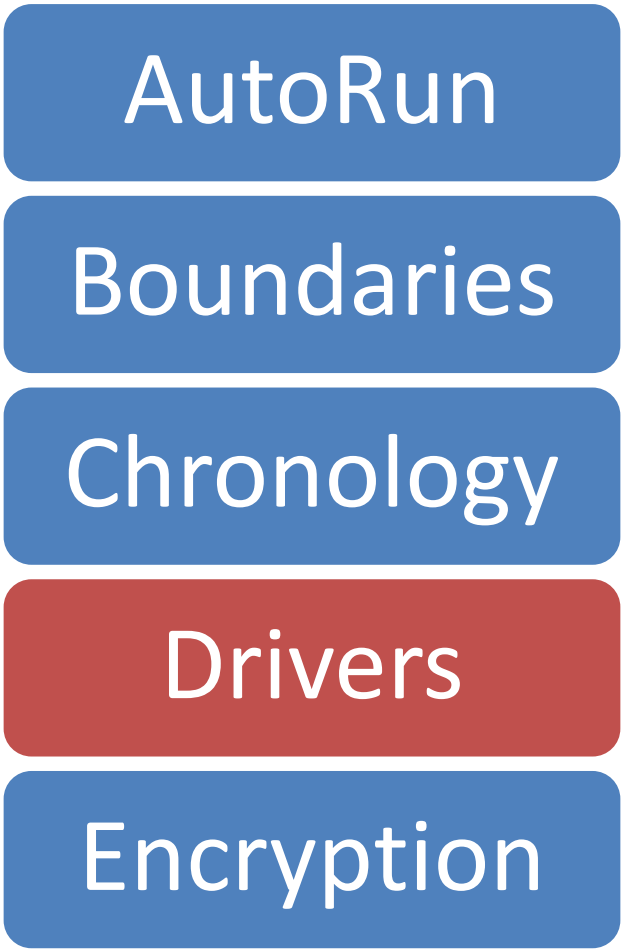
- Use regslack.exe to collect deleted registry keys

Restore Points

- RipXP will compare registry values from a collection of restore points using RR plug-ins; SAM is never stored

Comparing time?

- The RR regtime plug-in works on all the hive types and outputs the LastWritten timestamp in SleuthKit style
- Registry times can then be combined with file system times


AutoRun
Boundaries
Chronology
Drivers
Encryption

Drivers

Loadable kernel modules that interface between the I/O manager and relevant hardware

System boot

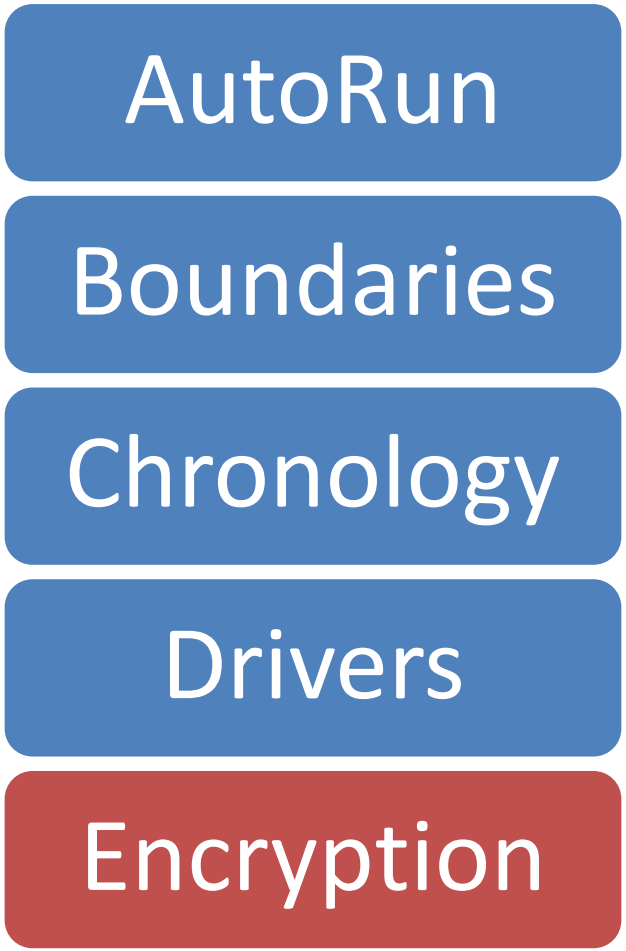
- SYSTEM\CurrentControlSet\Services
- Type is 1 or 2; Start is 0 or 1
- File extension of “sys” in “ImagePath”
- No value for “ObjectName

- RR: services (SYS) , svc (SYS)
- Driverquery – Built-in Windows program for enumerating all the currently loaded drivers

Windows File Protection

- Windows stores back up copies of important drivers in a separate space
- Backups: C:\Windows\Repair
- Drivers: C:\Windows\System32\Drivers

- WFPCheck.exe – Compares current copy to stored copy
- SigCheck – Checks drivers for their digital signatures


AutoRun
Boundaries
Chronology
Drivers
Encryption

Encryption

Intentional obfuscation or encryption of the data in the registry

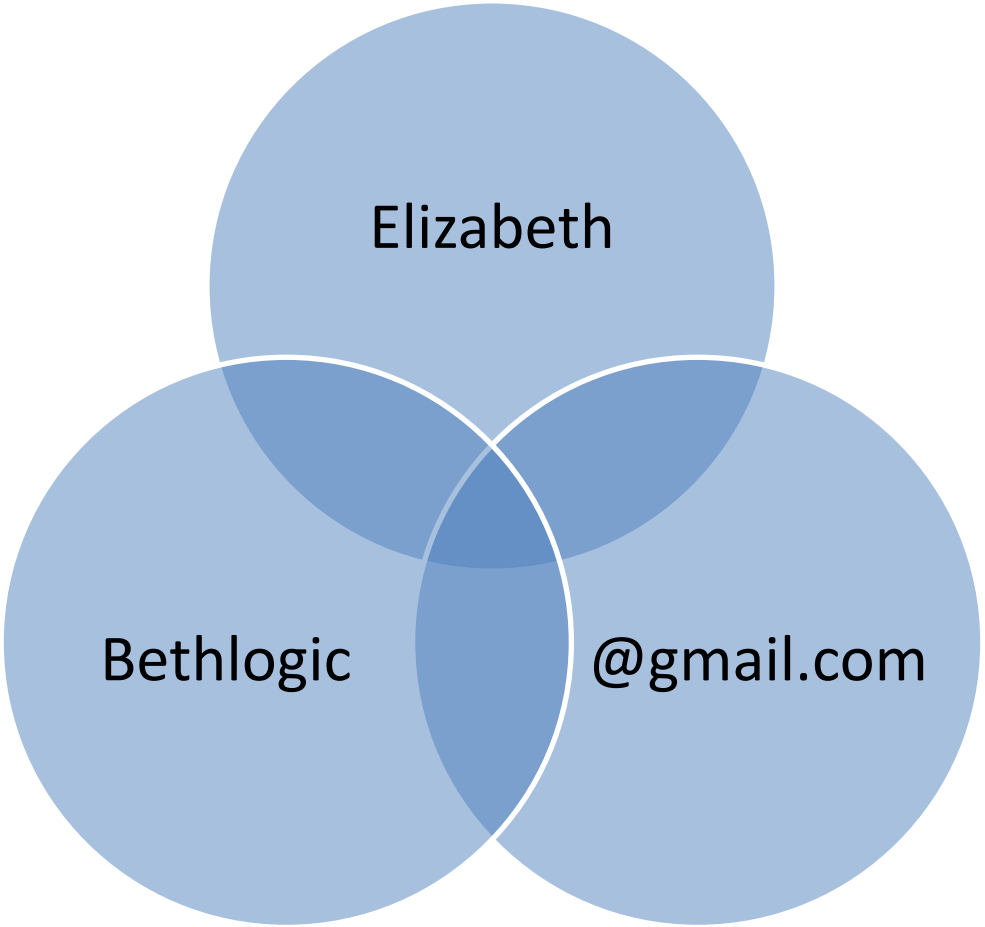
ROT 13

- UserAssist key is protected from modification by ROT 13

Look for Reg_SZ values that don’t make works

Look for large Reg_Binary values

Questions?



Further Information

- Windows Internals, Fifth Edition by Mark Russinovich and David Solomon
- Windows Forensic Analysis, 2nd Edition by Harlan Carvey
- “The Rootkit Paradox” by Jess Kornblum

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

The Root Keys

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

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

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

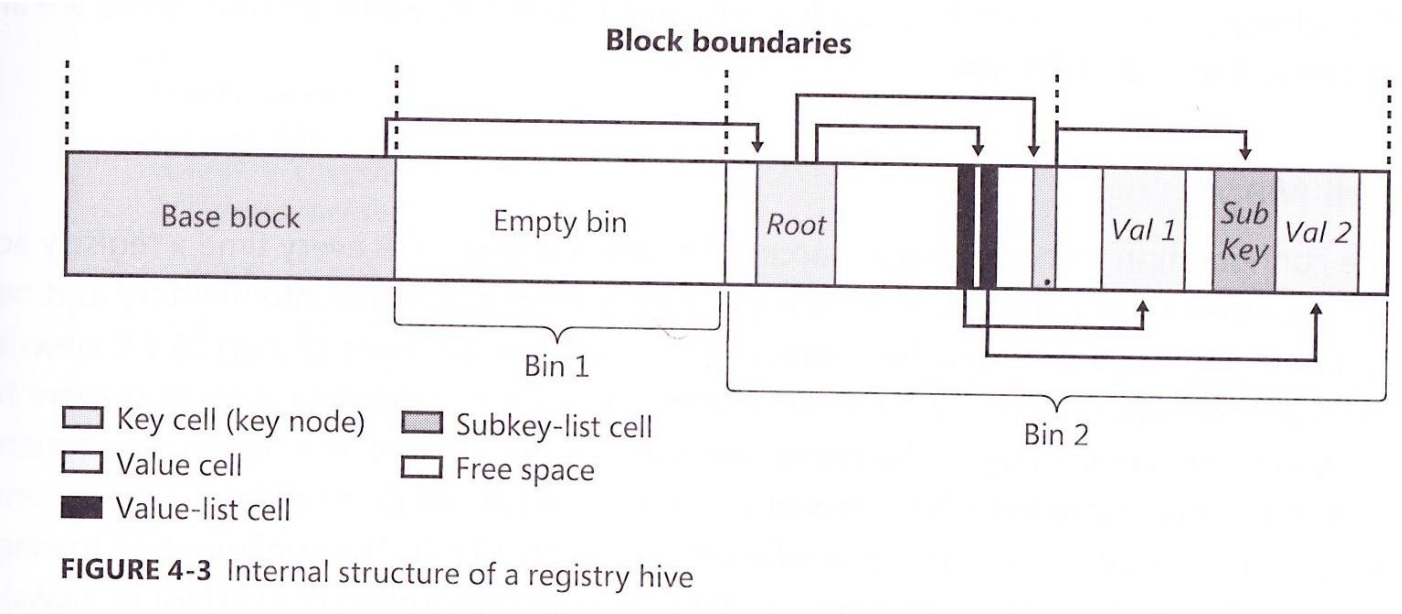


FIGURE 4-3 Internal structure of a registry hive

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

Registry 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.

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

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”