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.

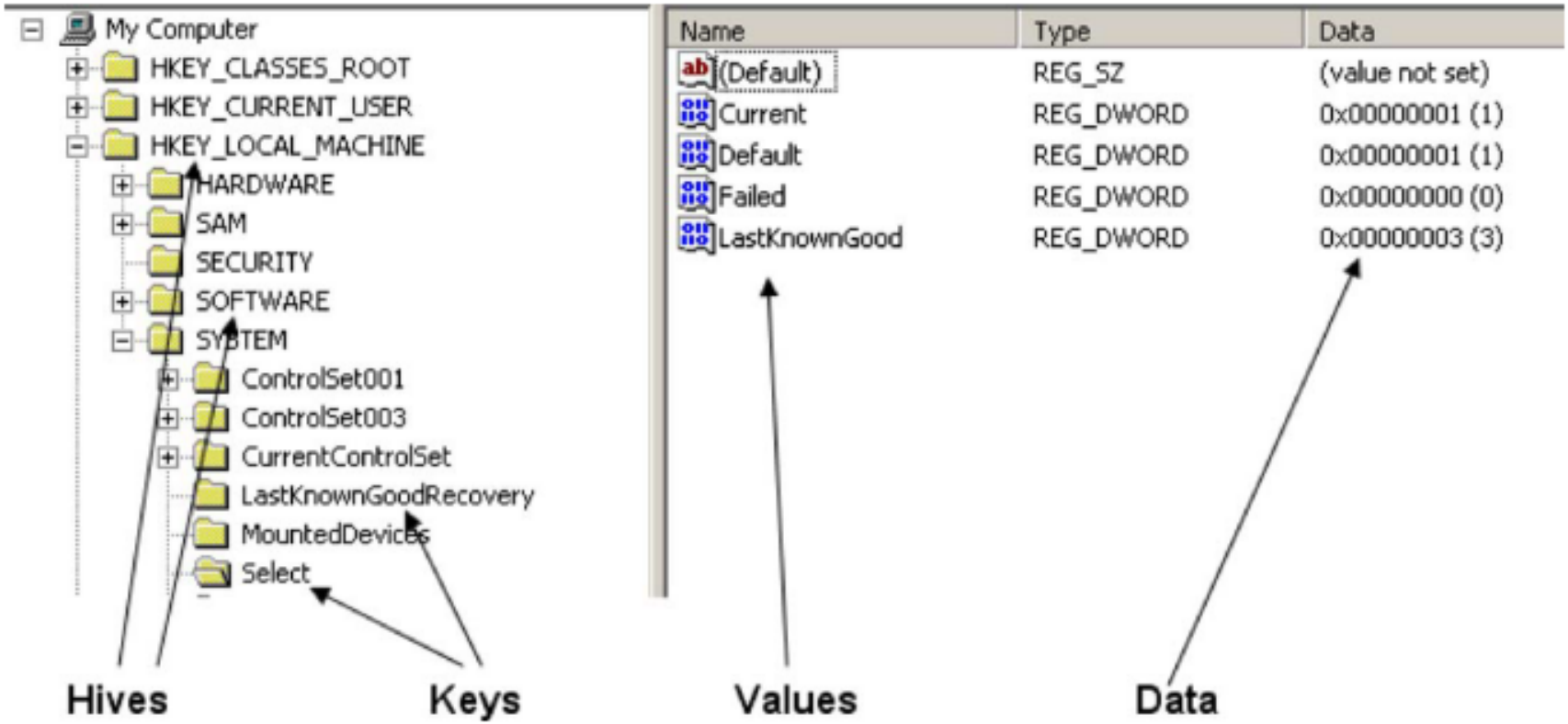
Objectives

- 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.)

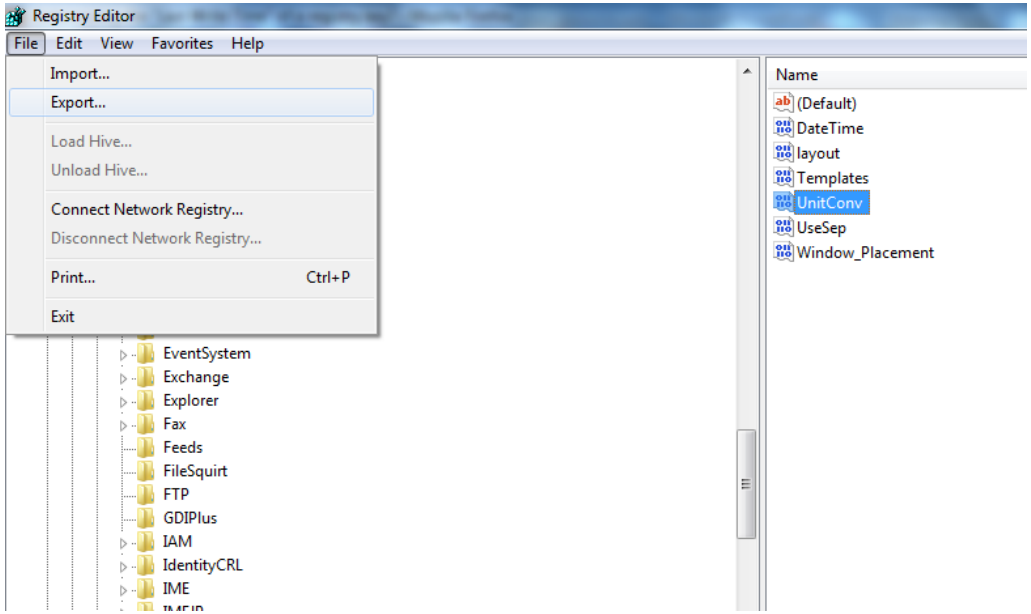
- Registry is maintained within several files on the system.
- Hives that are persistent on the system: %SYSTEMROOT%\system32\config folder.
  - HKEY_LOCAL_MACHINE\System (System folder).
- Specific user configuration:
  - Documents and Settings folder.
  - NTUSER.DAT file.

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:

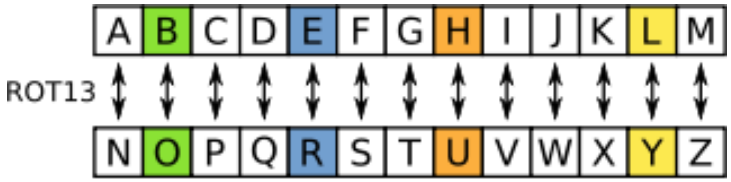


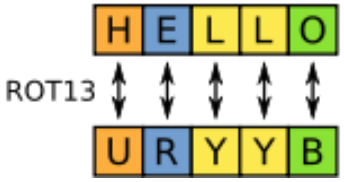
A1.txt

```
Key Name:          HKEY_CURRENT_USER\Software\Microsoft\Calc
Class Name:        <NO CLASS>
Last Write Time:   2/6/2013 - 3:08 PM
Value 0
  Name:            Window_Placement
  Type:            REG_BINARY
  Data:
00000000   2c 00 00 00 00 00 00 00 - 01 00 00 00 ff ff ff ff   ,...........ÿÿÿÿ
00000010   ff ff ff ff ff ff ff ff - ff ff ff ff ce 00 00 00   ÿÿÿÿÿÿÿÿÿÿÿÿÎ...
00000020   01 01 00 00 eb 03 00 00 - 85 02 00 00               ....ë.......
```

What's in the Registry?

- Useful forensic information within the Registry →Depends on investigator.
- Registry string search → 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.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

- 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.)

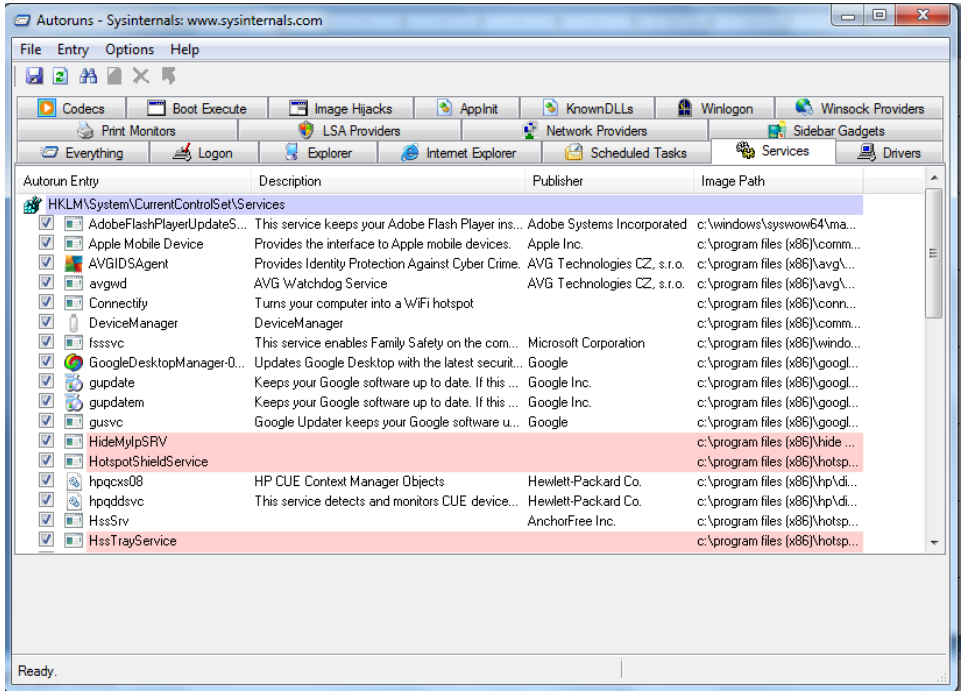
- Example 2: The key

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.

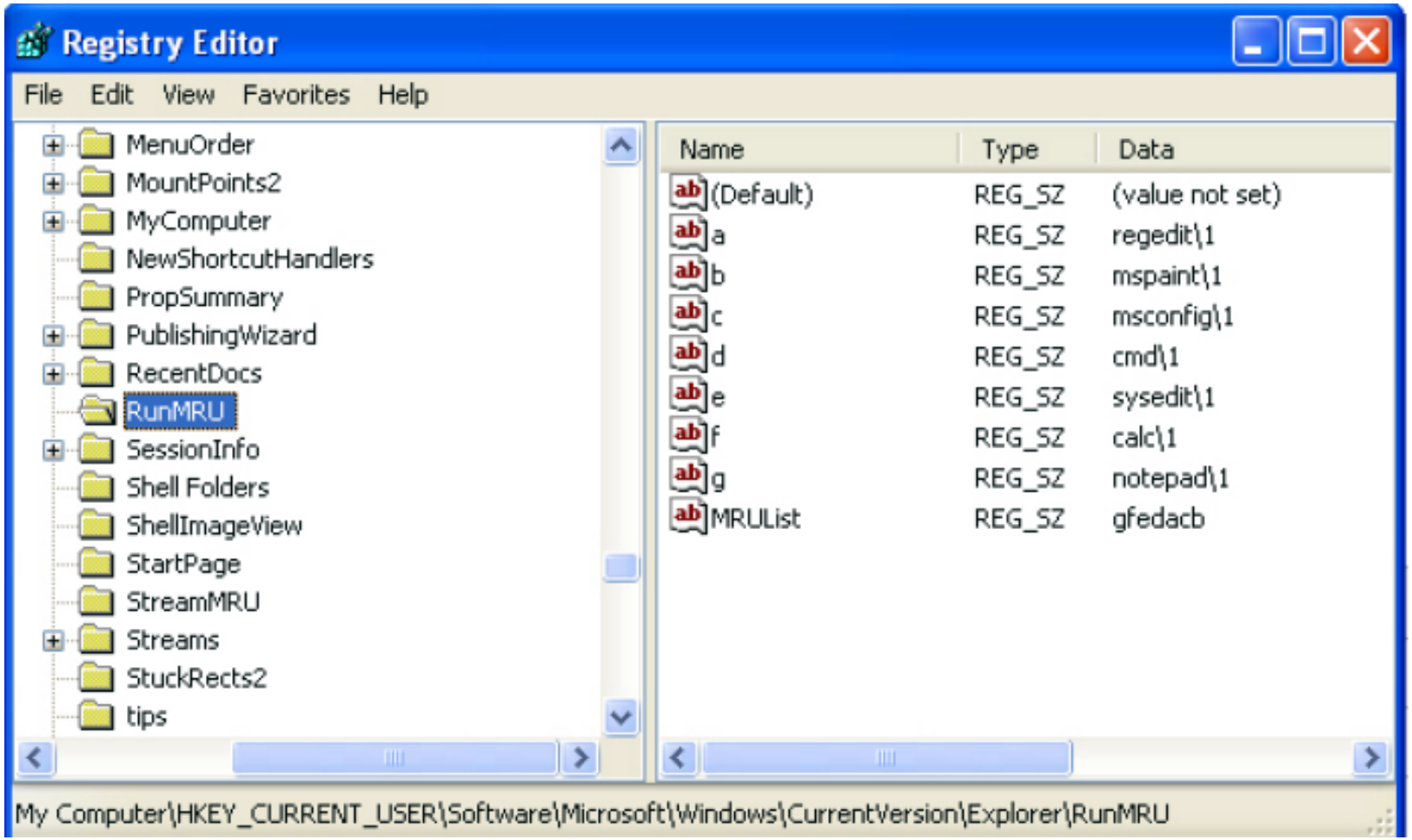
MRU Lists

- 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.)

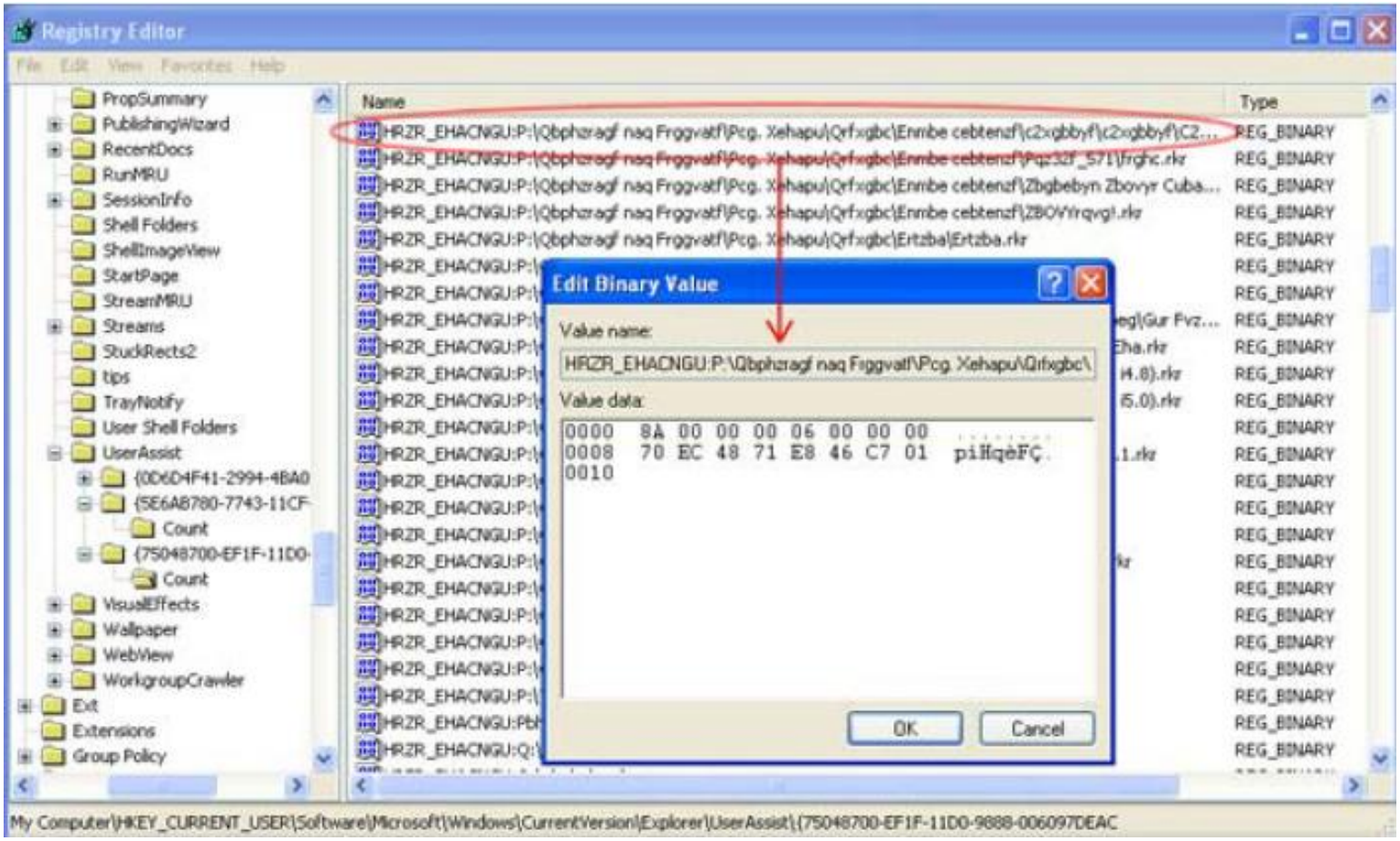
List of useful MRU lists	
XP Search Files	Software\Microsoft\Search Assistant\ACMru\5603
Internet Search Assistant	Software\Microsoft\Search Assistant\ACMru\5001
Printers, Computers and People	Software\Microsoft\Search Assistant\ACMru\5647
Pictures, music, and videos	Software\Microsoft\Search Assistant\ACMru\5604
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\Recent File List

User Assist

Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

- 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.)



Decoded Text

```
UEME_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

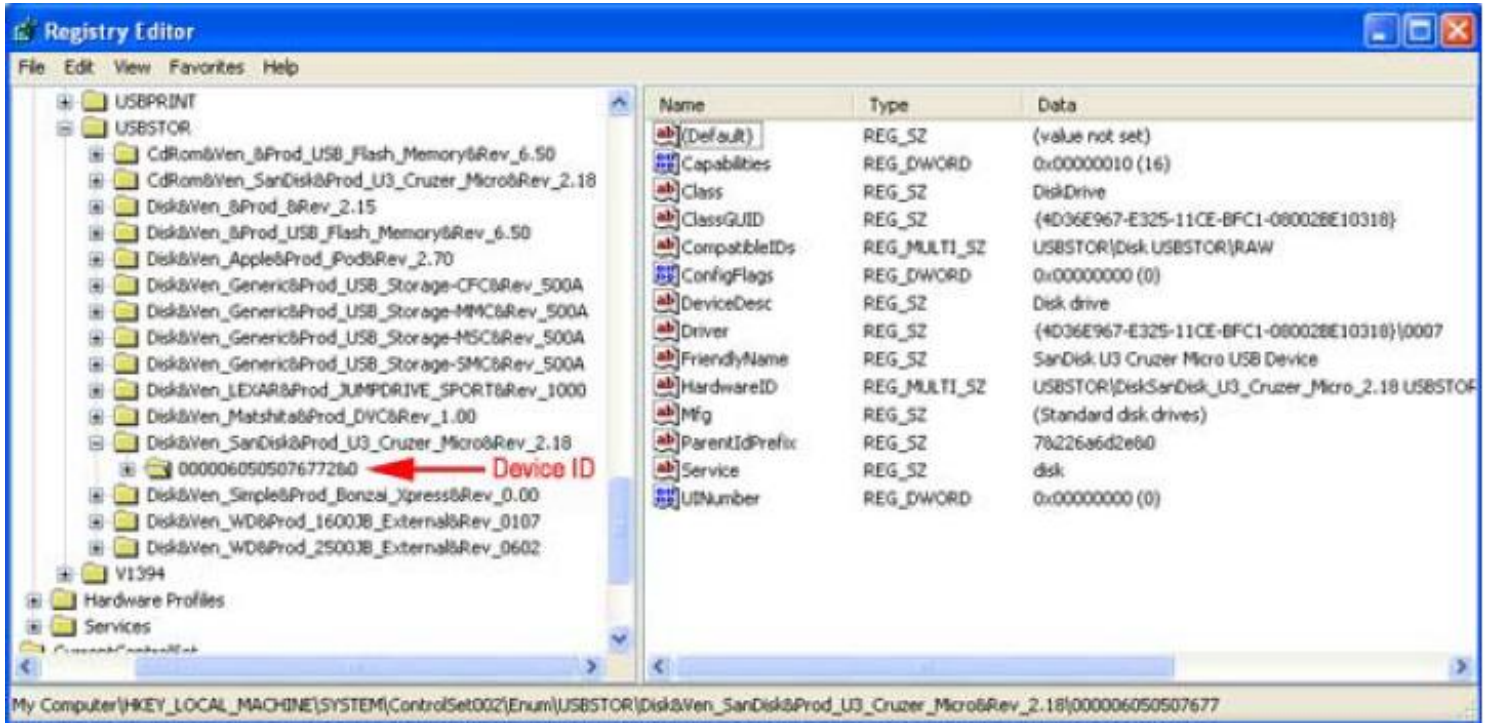
HKEY_LOCAL_MACHINE\System\ControlSet00x\Enum\USBSTOR

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

USB Removable Storage (Cont.)

- 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.

USB Removable Storage (Cont.)



Contents of USBSTOR key

No serial number case

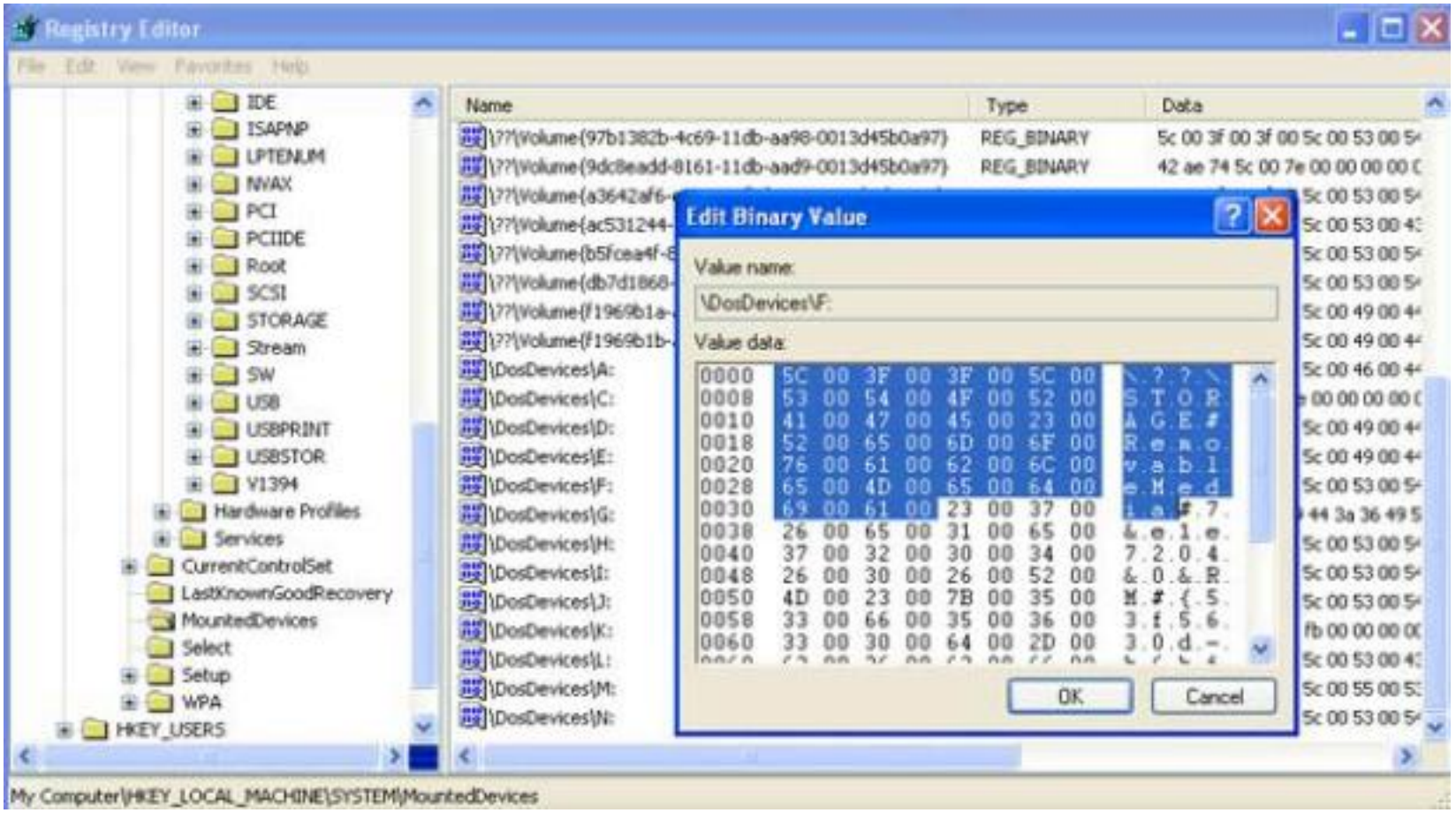
USB Removable Storage (Cont.)

- Mounted Devices:

HKEY_LOCAL_MACHINE\System\MountedDevices

- 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.

USB Removable Storage (Cont.)



Identification of volume \DosDevice\F

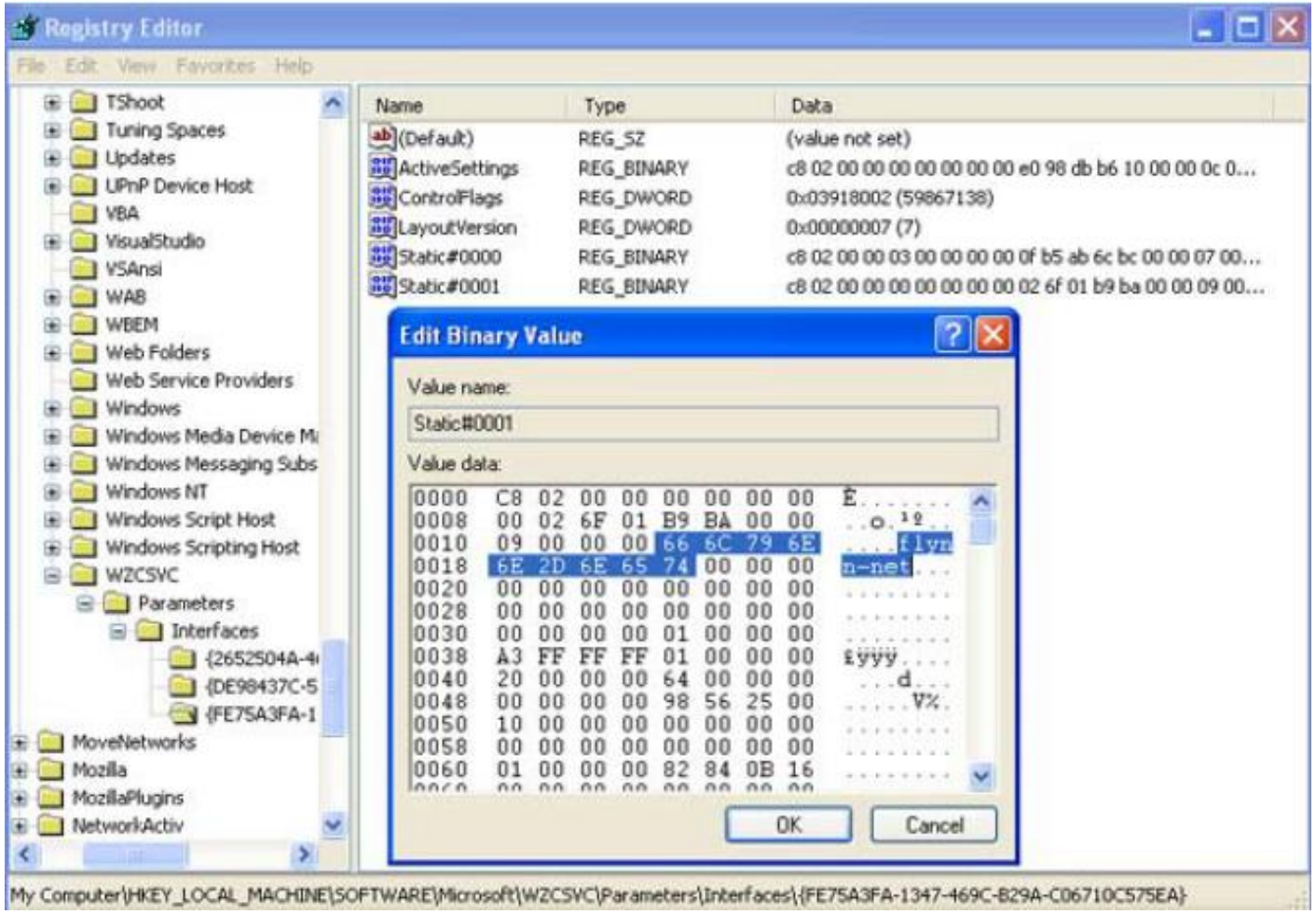
Wireless SSIDs

- 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.)



SSID example

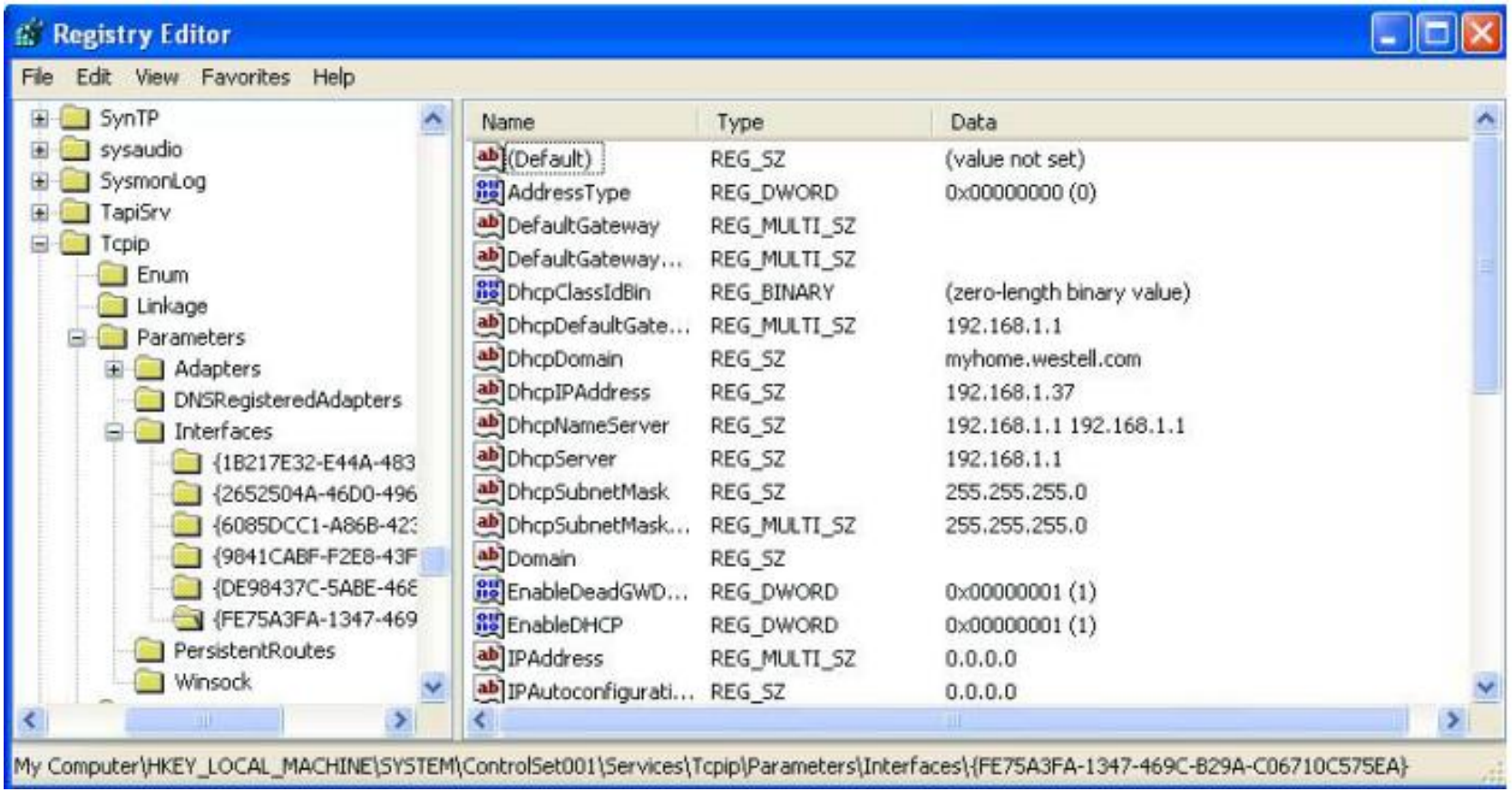
Wireless SSIDs (Cont.)

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

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TCPIP\Interfaces\GUID

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

Wireless SSIDs (Cont.)



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