


Is a hierarchical database that stores set-up and operational details of applications, resources and users.

It's not a mandatory repository for Windows applications/executables.

It can provide a lot of details to a digital forensics investigation.

WINDOWS REGISTRY



J Vella – Digital Forensics

Rationale



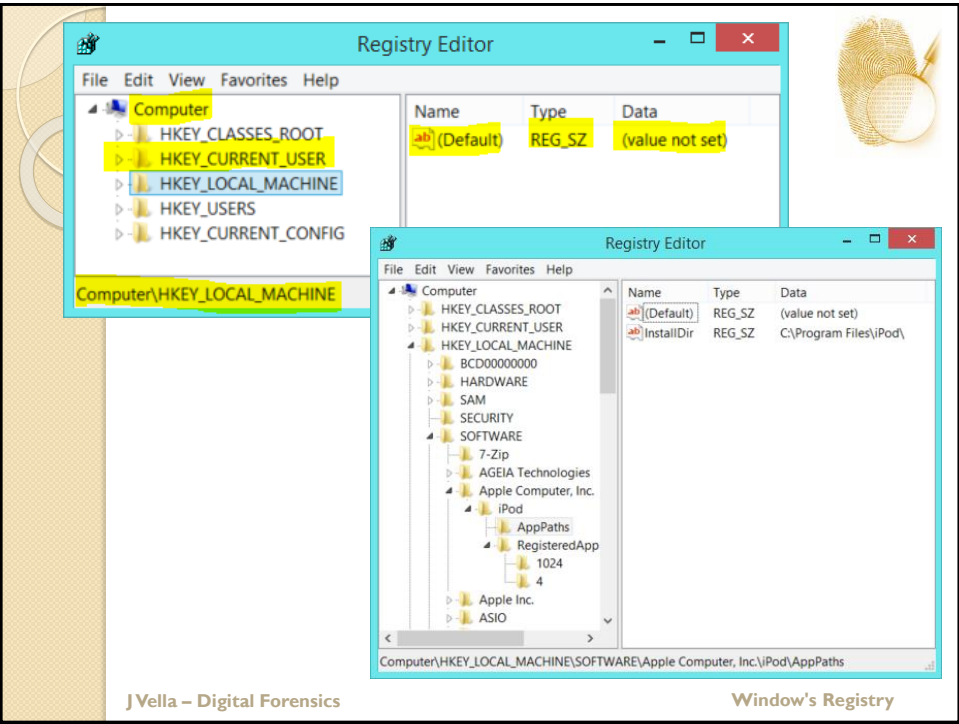
- Logical Structure
 - Entries have a standardised form (either a **Key** or a **Value**);
 - Overall structure is built by keys in a **hierarchical model**:
 - Initial levels have introduced and enforced keys;
 - Available to all application settings and preferences:
 - These are usually stored in Values (instances of **name** and **value** pairs);
 - Allows different users to share the same machine (e.g. and each have his respective preferences);
 - Provides basic *log* data on application, user and hardware usage.
- Atomic Updates
 - Since MS Windows Vista, updates to keys are through a transaction processing system.
- Number of APIs available for accessing the registry database:
 - MS Advanced Windows 32 Base API Library (advapi32.dll);
 - (Scripting languages, e.g. Python & Pearl, usually have wrapper to Window's API).

Registry Structure



- Register **keys** are containers.
Register **values** are non-containers – i.e. contain values.
- Keys can contain other keys as values – i.e. in a *hierarchic structure*.
- The registry **root** contains the following predefined sub-keys:
 - HKEY_LOCAL_MACHINE or HKLM
 - HKEY_CURRENT_CONFIG or HKCC
 - HKEY_CLASSES_ROOT or HKCR
 - HKEY_CURRENT_USER or HKCU
 - HKEY_USERS or HKU

(! The root sub-keys are also called **hives!** – see later)
- Each one of these sub-keys contain other keys.
 - Keys names, in a key container, must be unique.
- Values are found within a key and are in a name and data pair format.
 - Value names must be unique in a key container.
 - The data values can be any type but associated with a symbolic type (see next slide for these).



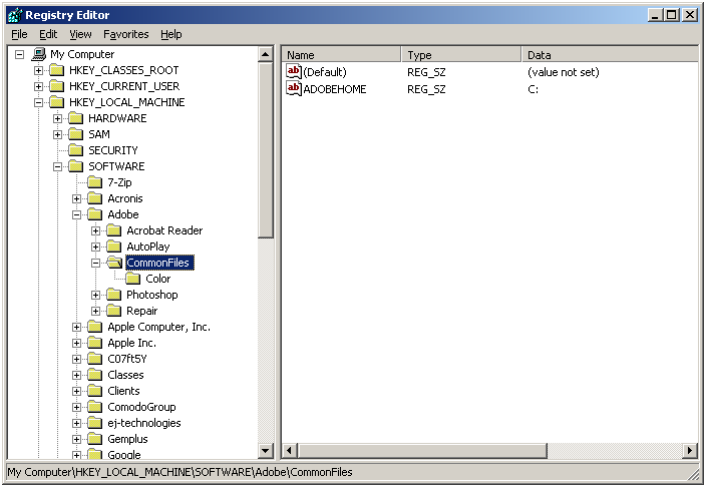
Registry Structure – Value Types		
ID	Symbolic type name	Meaning and encoding of the data stored in the Registry value
0	REG_NONE	No type (the stored value, if any)
1	REG_SZ	A value, normally stored and exposed in UTF-16LE and usually terminated by a NUL character
2	REG_EXPAND_SZ	An "expandable" string value that can contain environment variables, normally stored and exposed in UTF-16LE and usually terminated by a NUL character
3	REG_BINARY	Binary data (any arbitrary data)
4	REG_DWORD / REG_DWORD_LITTLE_ENDIAN	A DWORD value, a 32-bit unsigned integer (little-endian)
5	REG_DWORD_BIG_ENDIAN	A DWORD value, a 32-bit unsigned integer (big-endian)
6	REG_LINK	A symbolic link (UNICODE) to another Registry key, specifying a root key and the path to the target key
7	REG_MULTI_SZ	A multi-string value, which is an ordered list of non-empty strings , normally stored and exposed in UTF-16LE, each one terminated by a NUL character; the list being normally terminated by a second NUL character.
8	REG_RESOURCE_LIST	A resource list (used by the <i>Plug-n-Play</i> hardware enumeration and configuration)
9	REG_FULL_RESOURCE_DESCRIPTOR	A resource descriptor (used by the <i>Plug-n-Play</i> hardware enumeration and configuration)
10	REG_RESOURCE_REQUIREMENTS_LIST	A resource requirements list (used by the <i>Plug-n-Play</i> hardware enumeration and configuration)
11	REG_QWORD / REG_QWORD_LITTLE_ENDIAN	A QWORD value, a 64-bit integer (either big- or little-endian, or unspecified)


Window's Registry

Registry as a log

- All Registry **keys** contain a value associated with them called the “LastWrite” time, which is very similar to the last modification time of a file.
 - Creation, access, update and delete resets this timestamp;
 - It's stored as a FILETIME structure and indicates when the Registry Key was last modified.
 - Its value is in nanoseconds since 1601!
 - **Limitation:**
 - We know when a key was changed but not which of its value pairs.
 - The FILETIME value is usually compared and correlated with filing system date time stamps – e.g. MAC times.

Access to Registry – regedit.exe






The Root Sub-Keys (I-I with hives)

- **HKEY_CLASSES_ROOT** - The software settings about the **file** system, shortcut information, information on **file associations** and other **user interface** information are stored in this hive.
- **HKEY_USERS** – The **configuration settings** for each hardware and software item in the computer system, corresponding to each of the users of the computer system are stored in this hive. The information on the user's folders, user's choices of themes, colours and Control Panel settings are stored here as user's profile. This hive has a **subkey for each user** storing his/her user's profile.
- **HKEY_CURRENT_USER** - The configuration settings for each hardware and software item in the computer system, corresponding to **the currently logged-on user** are stored in this hive. This hive is **dynamic**, i.e. whenever a user logs-on into the system, the settings corresponding to the user are retrieved from the respective subkey of **HKEY_USERS** as user profile and stored in this hive. If a currently active item modifies a registry entry in its course of operation, the change will affect only the current user.
- **HKEY_LOCAL_MACHINE** - The **configuration settings for hardware and software for all users** of the computer are stored in this hive. The information stored here is computer specific and not user specific.
- **HKEY_CURRENT_CONFIG** - The **current hardware configuration** settings, pointing to **HKEY_LOCAL_MACHINE\Config** are stored in this hive. This hive is dynamic, meaning it is built at run-time.

J Vella – Digital Forensics

Window's Registry



Hives – physical parts of the Registry

- The files in the **c:\Windows\System32\config** folder and their associations with the hives are:

File Name	Associated Hive	Information Contained
Software	HKEY_LOCAL_MACHINE\SOFTWARE	Information about all the software items in the system, Windows performance parameters and the default Windows settings.
System	HKEY_LOCAL_MACHINE\SYSTEM	Information about all the hardware items in the system.
SAM	HKEY_LOCAL_MACHINE\SAM	Information about the Security Accounts Manager service.
Security	HKEY_LOCAL_MACHINE\SECURITY	Information about security. Neither of Security and SAM, can be viewed using Regedit, unless you reset the permissions.
Default	HKEY_USERS\DEFAULT	Default user settings. But the NTUSER.dat file corresponding to the currently logged-on user overrides the default user settings.
Userdiff	Not associated with any hive.	Information about the corresponding subkeys in the HKEY_USERS Hive for each registered user.

J Vella – Digital Forensics

Window's Registry

Registry Editor & .REG files



- **Regedit.exe** enables changes to the registry.
 - But also allows for access to the structures!
- Other than access, an editor is expected to:
 - Importing and exporting portions of structure (encoded in the hives) e.g. the .REG files;
 - Searching the structure for key and values (names);
 - Remote edit of registry.
- .REG files are readable extracts from the registry.
 - .REG file entries have the following syntax:

```
[<Hive name>\<Key name>\<Subkey name>]
"Value name"=<Value type>:<Value data>
```
 - For example

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Foobar]
"Value A"=<String value data with escape characters>
"Value B"=hex:<Binary data (as comma-delimited list of hexadecimal values)>
"Value C"=dword:<DWORD value integer>
"Value D"=hex(0):<REG_NONE (as comma-delimited list of hexadecimal values)>
```
- One can add content to a Registry through this syntax.

CLI access to Registry – regedit.exe



- MS Windows provides two tools to access the registry through the CLI:
 - Reg.exe and regedit.exe.
 - These tools read and write .REG files too.
- For example to export a sub-tree of the registry starting from HCE:


```
C:\> RegEdit.exe /e test.reg HKEY_CURRENT_USER[\<key>]
```
- For example retrieve a key and its values:


```
C:\>Reg.exe QUERY HKCU\Software\7-Zip\Compression

HKEY_CURRENT_USER\Software\7-Zip\Compression
Level      REG_DWORD    0x5
Archiver    REG_SZ       7z
ShowPassword REG_DWORD    0x0
EncryptHeaders REG_DWORD    0x0
ArchHistory REG_BINARY   32003000310034005F004D00
...
HKEY_CURRENT_USER\Software\7-Zip\Compression\Options

C:\>
```

°

KEYS OF FORENSIC
SOME VALUE

```
graph TD; RD((Registry Decoder)) --> UA((USB Activity)); RD --> LV((Last Visited URLs)); RD --> UA2((User Accounts)); RD --> IA((Installed Applications)); RD --> LPR((Last Programs Run)); RD --> RAF((Recently Accessed Files));
```

J Vella – Digital Forensics

Window's Registry

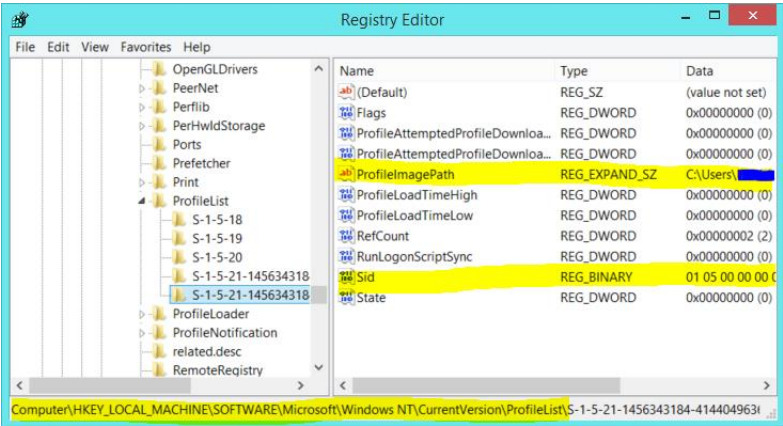
Quick Summary - Software:
Installed Applications (and Apps?)

Name	Type	Data
(Default)	REG_SZ	(value not set)
CommonFilesDir	REG_SZ	C:\Program Files\Comm...
CommonFilesDir (x86)	REG_SZ	C:\Program Files (x86)\C...
CommonW6432Dir	REG_SZ	C:\Program Files\Comm...
DevicePath	REG_EXPAND_SZ	%SystemRoot%\inf
MediaPathUnexpanded	REG_EXPAND_SZ	%SystemRoot%\Media
ProgramFilesDir	REG_SZ	C:\Program Files
ProgramFilesDir (x86)	REG_SZ	C:\Program Files (x86)
ProgramFilesPath	REG_EXPAND_SZ	%ProgramFiles%
ProgramW6432Dir	REG_SZ	C:\Program Files
SM_ConfigureProgramsName	REG_SZ	Set Program Access and...
SM_GamesName	REG_SZ	Games

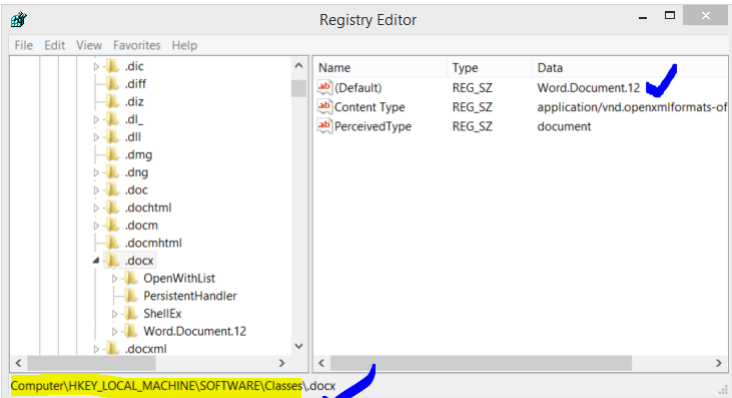
J Vella – Digital Forensics

Window's Registry

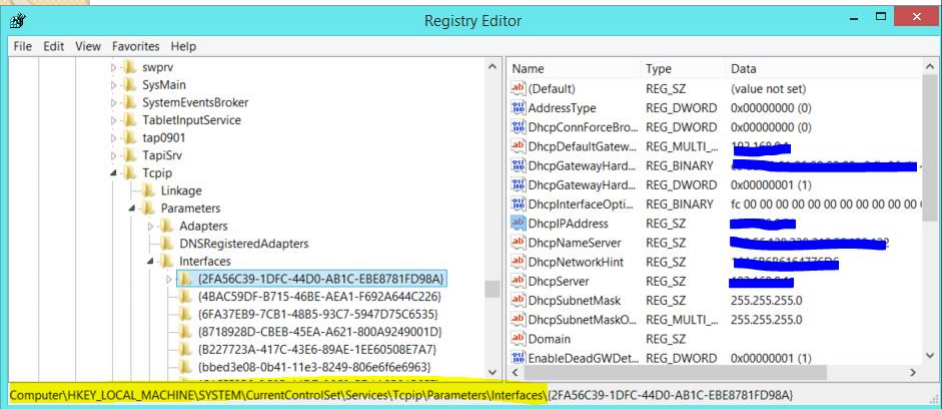
Quick Summary - Software: Installed Users?



Quick Summary - Software: Classes registered. File extensions associations?



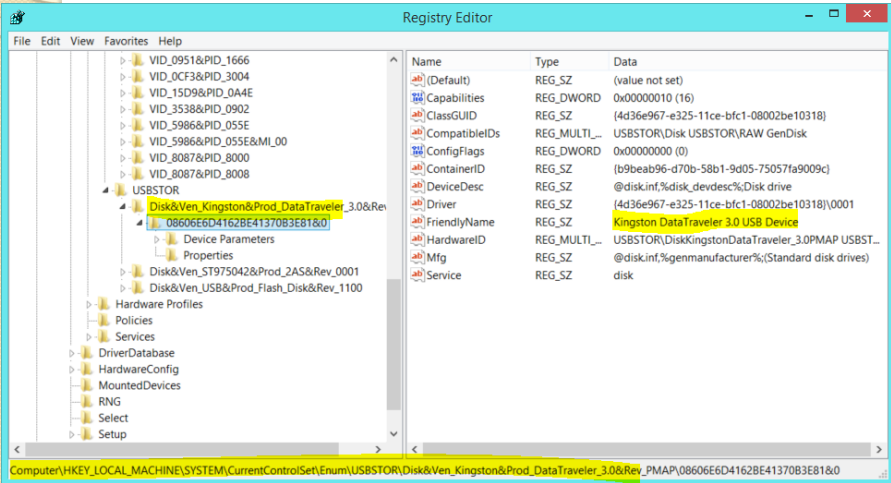
Quick Summary – Local Machine: IP addresses?



J Vella – Digital Forensics

Window's Registry

Quick Summary – Hardware: Any USB Storage Mounts?




J Vella – Digital Forensics

Window's Registry

Quick Summary:


others!?



Data Stored	Registry Key Location
Recent Docs	Windows\CurrentVersion\Explorer\Recent Docs
Recently Opened/Saved Files	Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU
Recently Opened/Saved Folders	Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
Last Visited Folder	Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRULegacy
Recently Used Apps (Non-Metro Apps)	Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU
Recently Used Apps with Saved Files	Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder
Recently Run Items	Windows\CurrentVersion\Explorer\Policies\RunMRU
Computer Name & Volume S/N	Windows Media\WMSDK\General
File Extension Associations	Windows\CurrentVersion\Explorer\FileExts
Typed URLs	Microsoft\Internet Explorer\TypedURLs
 Typed URL Time (Figure 35, Figure 36, and Figure 37)	Microsoft\Internet Explorer\TypedURLsTime

J Vella – Digital Forensics

Window's Registry

Quick Summary:




Data Stored	Registry Key Location
Current Control Set (Figure 24)	Select\Current
Last Known Good Control Set (Figure 25)	Select\LastKnownGood
Mounted Devices (Figures 26-28)	MountedDevices
Files Excluded from Restore	%CurrentControlSet%\Control\BackupRestore
Computer Name	%CurrentControlSet%\Control\ComputerName
Time Zone	%CurrentControlSet%\Control\TimeZoneInformation\TimeZoneKeyName
Last Graceful Shutdown Time (Figure 29)	%CurrentControlSet%\Control\Windows\ShutdownTime (Data stored in Windows FILETIME)
Printers	%CurrentControlSet%\Enum\SWD\PRINTENUM\FriendlyName
 Sensors & Location Devices	%CurrentControlSet%\Enum\SWD\SensorsAndLocationEnum\HardwareID
 USB Storage Devices	%CurrentControlSet%\Enum\USBSTOR

J Vella – Digital Forensics

Window's Registry

Quick Summary:

Autorun locations (e.g. boot time processes).



List of common autorun locations:

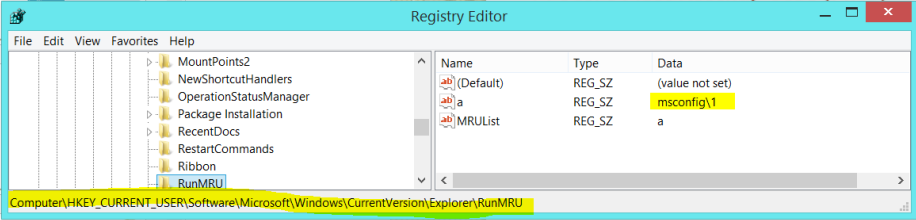
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
(ProfilePath)\Start Menu\Programs\Startup

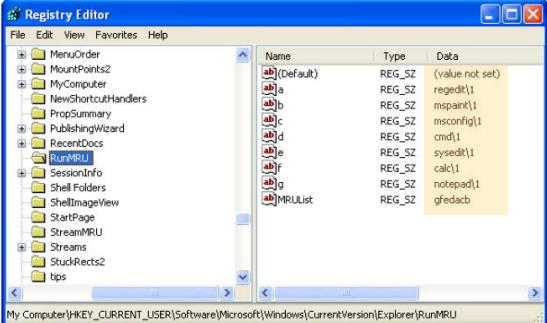
J Vella – Digital Forensics

Window's Registry

Quick Summary:

A User's Most Recently Used (MRU)





J Vella – Digital Forensics

Quick Summary:

Traces of P2P clients / connections



- The application that are allowed through the firewall are given in the registry key:

HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List

