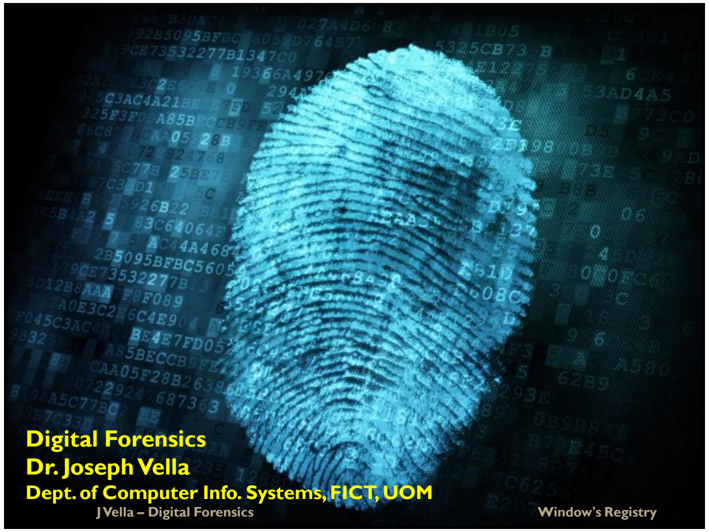
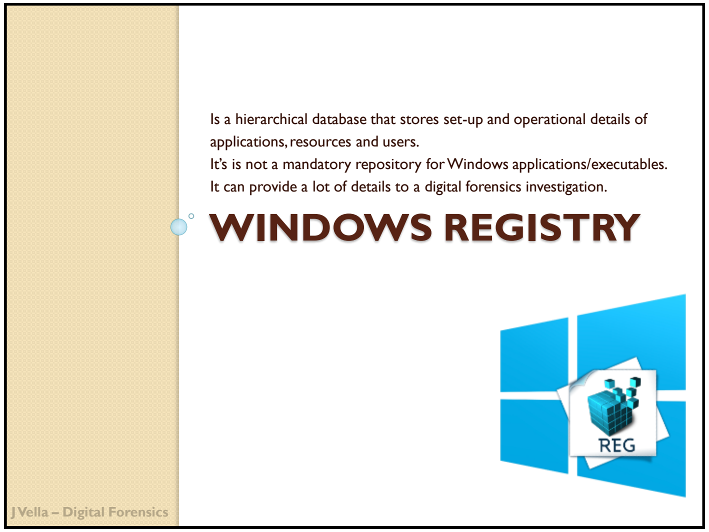
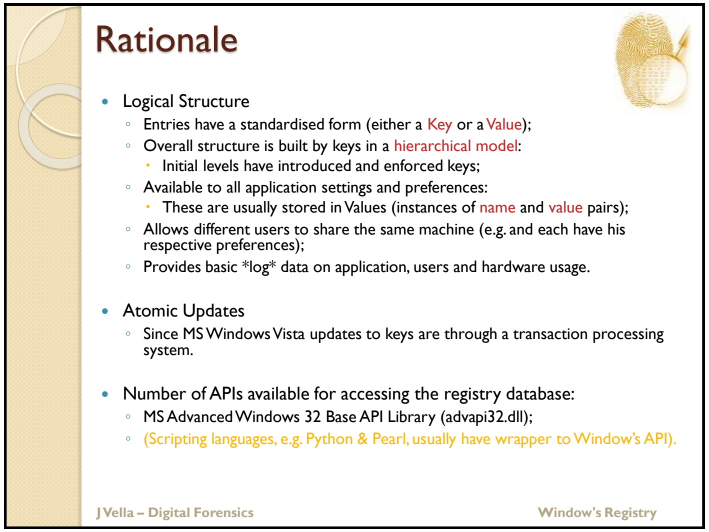


Digital Forensics
Dr. Joseph Vella
Dept. of Computer Info. Systems, FICT, UOM



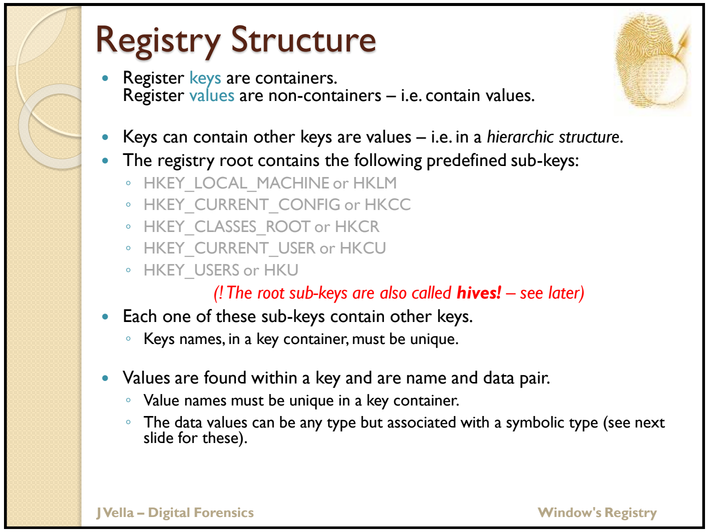
Is a hierarchical database that stores set-up and operational details of applications, resources and users.
It's is not a mandatory repository for Windows applications/executables.
It can provide a lot of details to a digital forensics investigation.

WINDOWS REGISTRY



Rationale

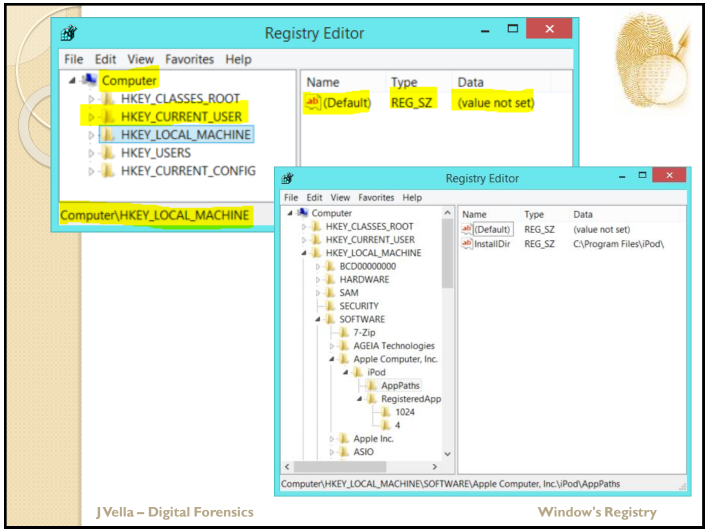
- Logical Structure
  - Entries have a standardised form (either a Key or a Value);
  - Overall structure is built by keys in a hierarchical model:
    - Initial levels have introduced and enforced keys;
  - Available to all application settings and preferences:
    - These are usually stored in Values (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, users 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 are 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 name and data pair.
  - 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 Editor

File Edit View Favorites Help

- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_CURRENT_CONFIG

Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE

Registry Editor

File Edit View Favorites Help

- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
    - BCD00000000
    - HARDWARE
    - SAM
    - SECURITY
    - SOFTWARE
      - 7-Zip
      - AGEIA Technologies
      - Apple Computer, Inc.
        - iPod
          - AppPaths
          - RegisteredApp
            - 1024
            - 4
      - Apple Inc.
      - ASIO

Name	Type	Data
(Default)	REG_SZ	(value not set)
InstallDir	REG_SZ	C:\Program Files\iPod\

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Apple Computer, Inc.\iPod\AppPaths

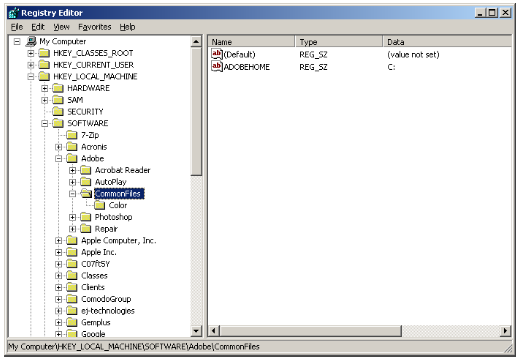
Registry Structure – Value Types

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 *Plug-n-Play* hardware enumeration and configuration)
9	REG_FULL_RESOURCE_DESCRIPTOR	A resource descriptor (used by the *Plug-n-Play* hardware enumeration and configuration)
10	REG_RESOURCE_REQUIREMENTS_LIST	A resource requirements list (used by the *Plug-n-Play* 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)

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 the 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



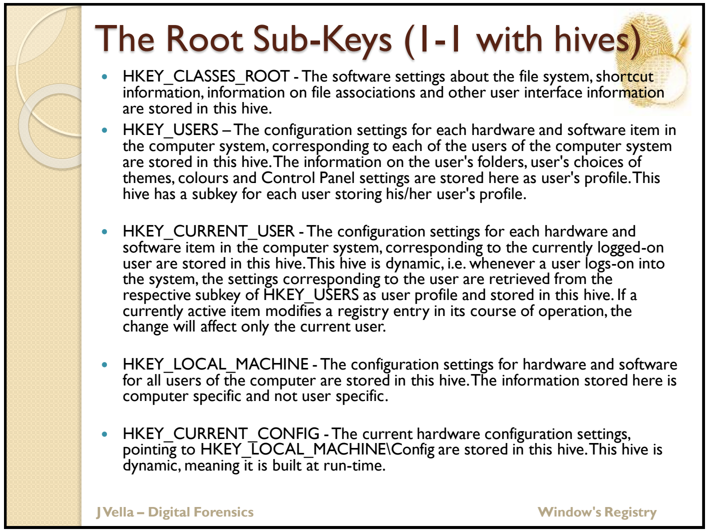
Registry Editor

File Edit View Favorites Help

- My Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
    - HARDWARE
    - SAM
    - SECURITY
    - SOFTWARE
      - 7-Zip
      - Acronis
      - Adobe
        - Acrobat Reader
        - AutoPlay
        - CommonFiles
          - Color
        - Photoshop
        - Repair
      - Apple Computer, Inc.
      - Apple Inc.
      - C07ft5Y
      - Classes
      - Clients
      - ComodoGroup
      - ej-technologies
      - Gemplus
      - Google

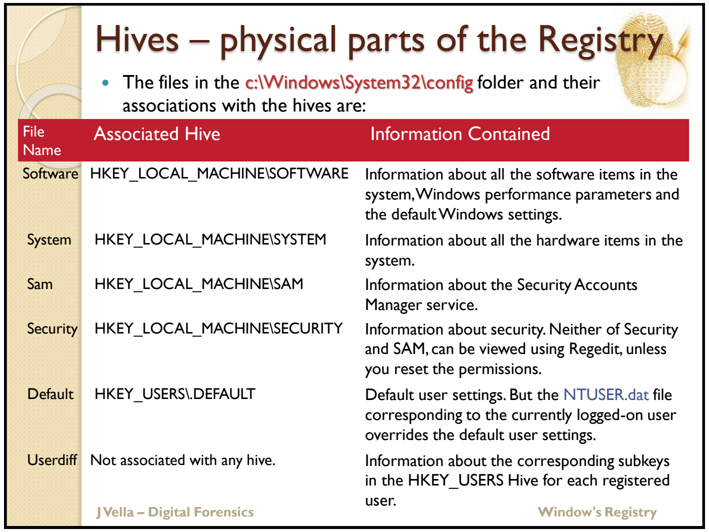
Name	Type	Data
(Default)	REG_SZ	(value not set)
ADOBEHOME	REG_SZ	C:

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\CommonFiles



The Root Sub-Keys (1-1 with hives)

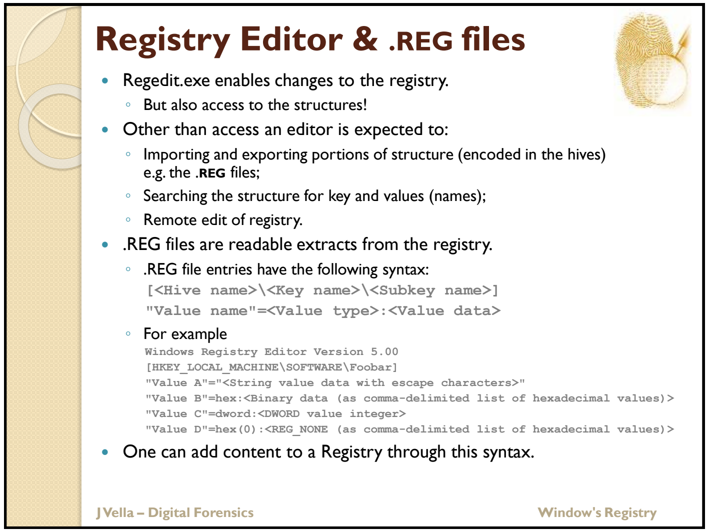
- HKEY_CLASSES_ROOT - The software settings about the file system, shortcut information, information on file associations and other user interface information are stored in this hive.
- HKEY_USERS – The configuration settings for each hardware and software item in the computer system, corresponding to 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.



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.



Registry Editor & .REG files

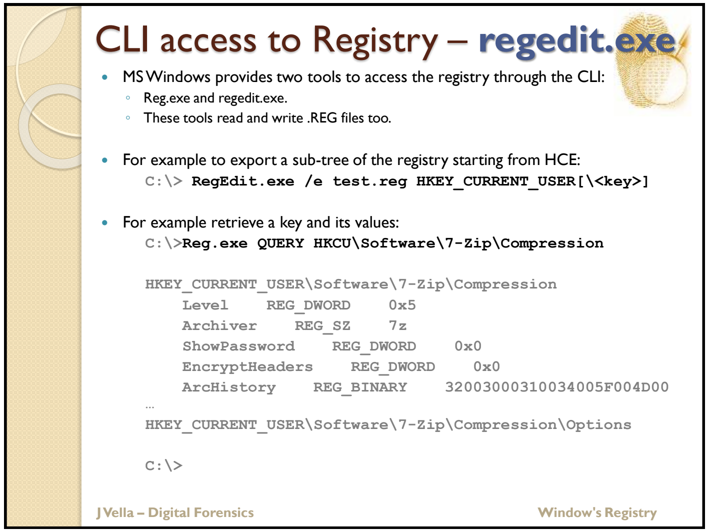
- Regedit.exe enables changes to the registry.
  - But also access to the structures!
- Other than access an editor is expected to:
  - Importing and exporting portions of structure (encoded in the hives) e.g. the .REG files;
  - Searching the structure for key and values (names);
  - Remote edit of 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>]
```

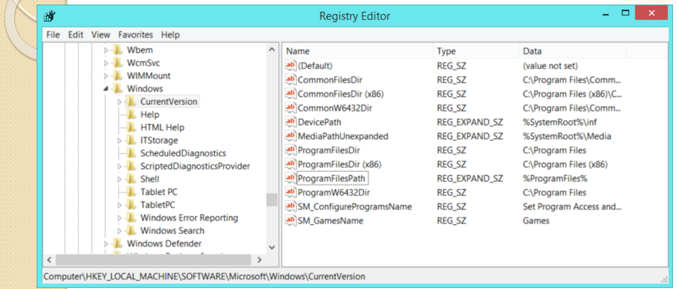
- For example retrieve a key and its values:

```
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
    ArcHistory    REG_BINARY    32003000310034005F004D00
…
HKEY_CURRENT_USER\Software\7-Zip\Compression\Options

C:\>
```

KEYS OF FORENSIC SOME VALUE

Quick Summary - Software:

Installed Applications (and Apps)?



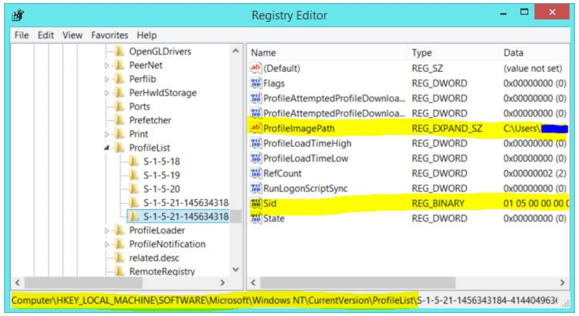
```
▷ Wbem
▷ WcmSvc
▷ WIMMount
◢ Windows
    ▷ CurrentVersion
      Help
      HTML Help
    ▷ ITStorage
      ScheduledDiagnostics
    ▷ ScriptedDiagnosticsProvider
    ▷ Shell
      Tablet PC
    ▷ TabletPC
    ▷ Windows Error Reporting
    ▷ Windows Search
▷ Windows Defender
```

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

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

Quick Summary - Software:

Installed Users?



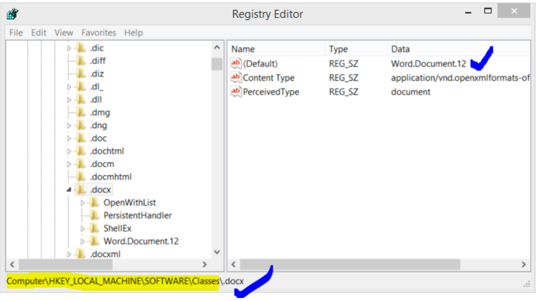
```
  OpenGLDrivers
▷ PeerNet
▷ Perflib
▷ PerHwldStorage
  Ports
  Prefetcher
▷ Print
◢ ProfileList
    S-1-5-18
    S-1-5-19
    S-1-5-20
    S-1-5-21-145634318
    S-1-5-21-145634318
▷ ProfileLoader
▷ ProfileNotification
  related.desc
  RemoteRegistry
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Flags	REG_DWORD	0x00000000 (0)
ProfileAttemptedProfileDownloa...	REG_DWORD	0x00000000 (0)
ProfileAttemptedProfileDownloa...	REG_DWORD	0x00000000 (0)
ProfileImagePath	REG_EXPAND_SZ	C:\Users\[redacted]
ProfileLoadTimeHigh	REG_DWORD	0x00000000 (0)
ProfileLoadTimeLow	REG_DWORD	0x00000000 (0)
RefCount	REG_DWORD	0x00000002 (2)
RunLogonScriptSync	REG_DWORD	0x00000000 (0)
Sid	REG_BINARY	01 05 00 00 00 (
State	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1456343184-414404963(

Quick Summary - Software:

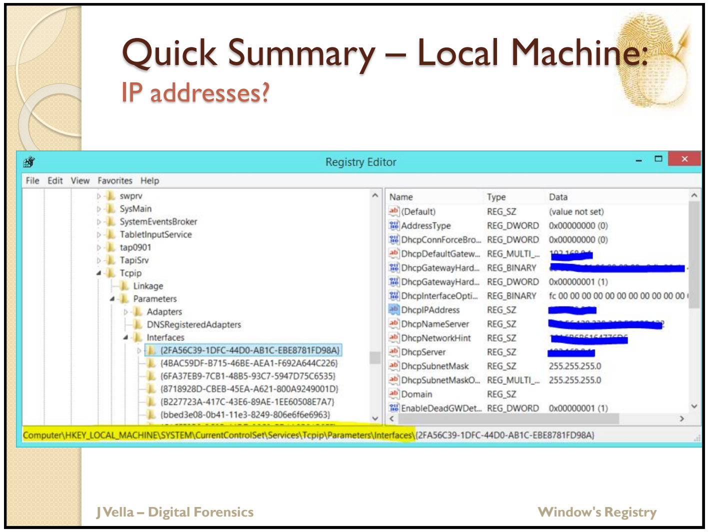
Classes registered. File extensions associations?



```
▷ .dic
  .diff
  .diz
▷ .dl_
▷ .dll
  .dmg
▷ .dng
▷ .doc
▷ .dochtml
▷ .docm
  .docmhtml
◢ .docx
    ▷ OpenWithList
      PersistentHandler
    ▷ ShellEx
    ▷ Word.Document.12
▷ .docxml
```

Name	Type	Data
(Default)	REG_SZ	Word.Document.12
Content Type	REG_SZ	application/vnd.openxmlformats-of
PerceivedType	REG_SZ	document

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.docx



Quick Summary – Local Machine:

IP addresses?

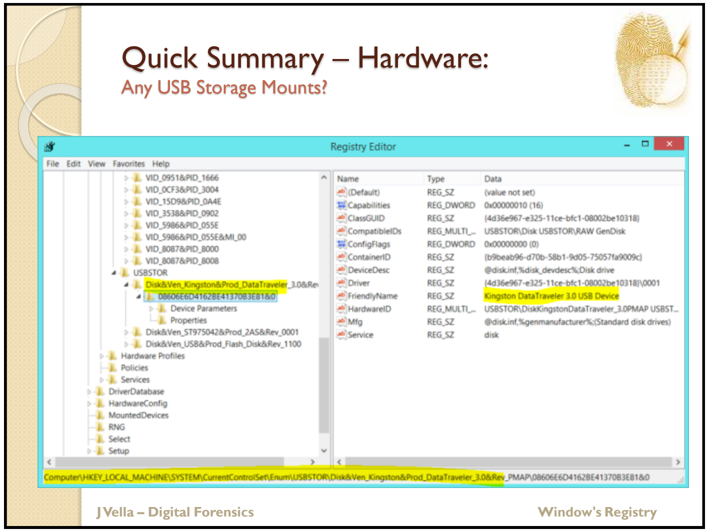
Registry Editor

```
swprv
SysMain
SystemEventsBroker
TabletInputService
tap0901
TapiSrv
Tcpip
  Linkage
  Parameters
    Adapters
    DNSRegisteredAdapters
    Interfaces
      {2FA56C39-1DFC-44D0-AB1C-EBE8781FD98A}
      {4BAC59DF-B715-46BE-AEA1-F692A644C226}
      {6FA37EB9-7CB1-48B5-93C7-5947D75C6535}
      {8718928D-CBEB-45EA-A621-800A9249001D}
      {B227723A-417C-43E6-89AE-1EE60508E7A7}
      {bbed3e08-0b41-11e3-8249-806e6f6e6963}
```

```
Name                 Type          Data
(Default)            REG_SZ        (value not set)
AddressType          REG_DWORD     0x00000000 (0)
DhcpConnForceBro...  REG_DWORD     0x00000000 (0)
DhcpDefaultGatew...  REG_MULTI_... [redacted]
DhcpGatewayHard...   REG_BINARY    [redacted]
DhcpGatewayHard...   REG_DWORD     0x00000001 (1)
DhcpInterfaceOpti... REG_BINARY    fc 00 00 00 00 00 00 00 00 00 00 00
DhcpIPAddress        REG_SZ        [redacted]
DhcpNameServer       REG_SZ        [redacted]
DhcpNetworkHint      REG_SZ        [redacted]
DhcpServer           REG_SZ        [redacted]
DhcpSubnetMask       REG_SZ        255.255.255.0
DhcpSubnetMaskO...   REG_MULTI_... 255.255.255.0
Domain               REG_SZ
EnableDeadGWDet...   REG_DWORD     0x00000001 (1)
```

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{2FA56C39-1DFC-44D0-AB1C-EBE8781FD98A}

J Vella – Digital Forensics Window's Registry



Quick Summary – Hardware:

Any USB Storage Mounts?

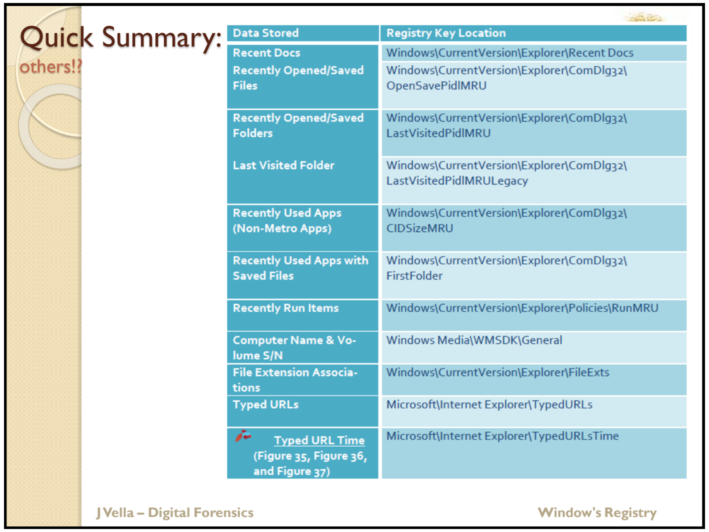
Registry Editor

```
VID_0951&PID_1666
VID_0CF3&PID_3004
VID_15D9&PID_0A4E
VID_3538&PID_0902
VID_5986&PID_055E
VID_5986&PID_055E&MI_00
VID_8087&PID_8000
VID_8087&PID_8008
USBSTOR
  Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev
    08606E6D4162BE41370B3E81&0
      Device Parameters
      Properties
  Disk&Ven_ST975042&Prod_2AS&Rev_0001
  Disk&Ven_USB&Prod_Flash_Disk&Rev_1100
Hardware Profiles
Policies
Services
DriverDatabase
HardwareConfig
MountedDevices
RNG
Select
Setup
```

```
Name            Type          Data
(Default)       REG_SZ        (value not set)
Capabilities    REG_DWORD     0x00000010 (16)
ClassGUID       REG_SZ        {4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs   REG_MULTI_... USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags     REG_DWORD     0x00000000 (0)
ContainerID     REG_SZ        {b9beab96-d70b-58b1-9d05-75057fa9009c}
DeviceDesc      REG_SZ        @disk.inf,%disk_devdesc%;Disk drive
Driver          REG_SZ        {4d36e967-e325-11ce-bfc1-08002be10318}\0001
FriendlyName    REG_SZ        Kingston DataTraveler 3.0 USB Device
HardwareID      REG_MULTI_... USBSTOR\DiskKingstonDataTraveler_3.0PMAP USBST...
Mfg             REG_SZ        @disk.inf,%genmanufacturer%;(Standard disk drives)
Service         REG_SZ        disk
```

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP\08606E6D4162BE41370B3E81&0

J Vella – Digital Forensics Window's Registry

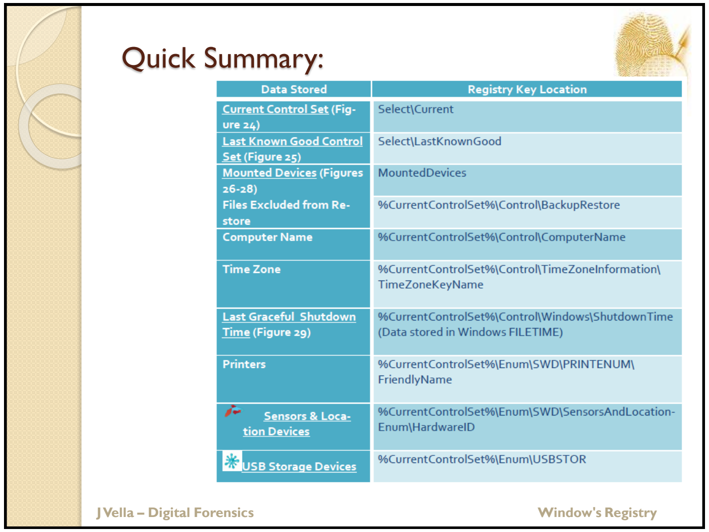


Quick Summary:

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:

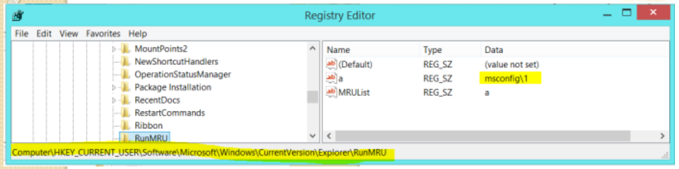
Autorun locations (e.g. boot time processes).

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

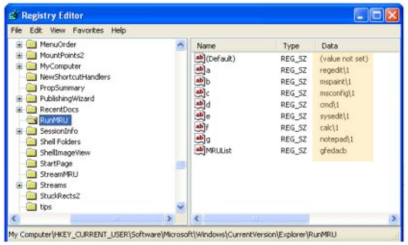
Quick Summary:

A User's Most Recently Used (MRU)



Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	msconfig\1
MRUList	REG_SZ	a

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



Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	regedit\1
b	REG_SZ	mspaint\1
c	REG_SZ	msconfig\1
d	REG_SZ	cmd\1
e	REG_SZ	sysedit\1
f	REG_SZ	calc\1
g	REG_SZ	notepad\1
MRUList	REG_SZ	gfedacb

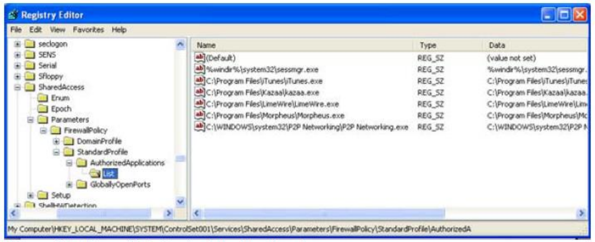
My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

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
```



Name	Type	Data
(Default)	REG_SZ	(value not set)
%windir%\system32\sessmgr.exe	REG_SZ	%windir%\system32\sessmgr.
C:\Program Files\iTunes\iTunes.exe	REG_SZ	C:\Program Files\iTunes\iTunes
C:\Program Files\Kazaa\kazaa.exe	REG_SZ	C:\Program Files\Kazaa\kazaa.
C:\Program Files\LimeWire\LimeWire.exe	REG_SZ	C:\Program Files\LimeWire\Lim
C:\Program Files\Morpheus\Morpheus.exe	REG_SZ	C:\Program Files\Morpheus\Mc
C:\WINDOWS\system32\P2P Networking\P2P Networking.exe	REG_SZ	C:\WINDOWS\system32\P2P N

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedA