

Computer Forensics 2

Windows Registry

Dr Diane Gan

Today

- Windows Artefacts
 - Reminder of Windows XP
 - Windows 7 differences
- Registry Artifacts

Differences and similarities

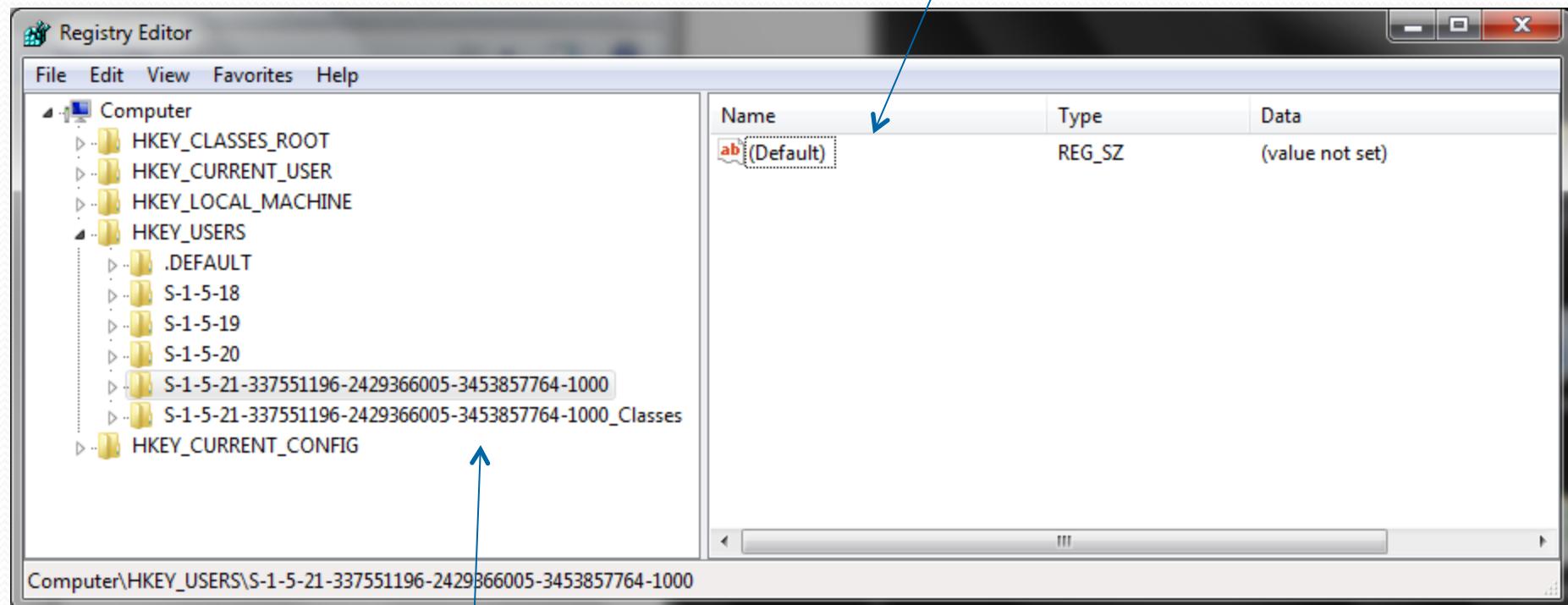
- Win 7 looks and feels very similar to Vista
- Major difference is “jump lists”
- Windows 7
 - Starter edition (SE)
 - Home Basic (HB)
 - Home Premium (HP)
 - Professional
 - Enterprise and Ultimate
 - same features just licensing differences
 - Includes Bitlocker protection
 - Ultimate is available to home users

Unchanged user artifacts

- Registry
- Shadow copy
- Folder/file structures
- Link files
- Encrypting File System (EFS)
- Spool files (except for the .SHD file format)
- Alternate data streams (unchanged from Vista)
- \$Recycle (no change between Vista and Win 7)
- Thumbcache (no change between Vista and Win 7)

Road to Central Depository - Registry

- DOS
 - config.sys & autoexec.bat
- Windows 3.0
 - INI file
- Windows 3.1
 - Start of the idea of a central repository
- Windows 95 and beyond
 - Establishment and expansion of the registry



Key

Value

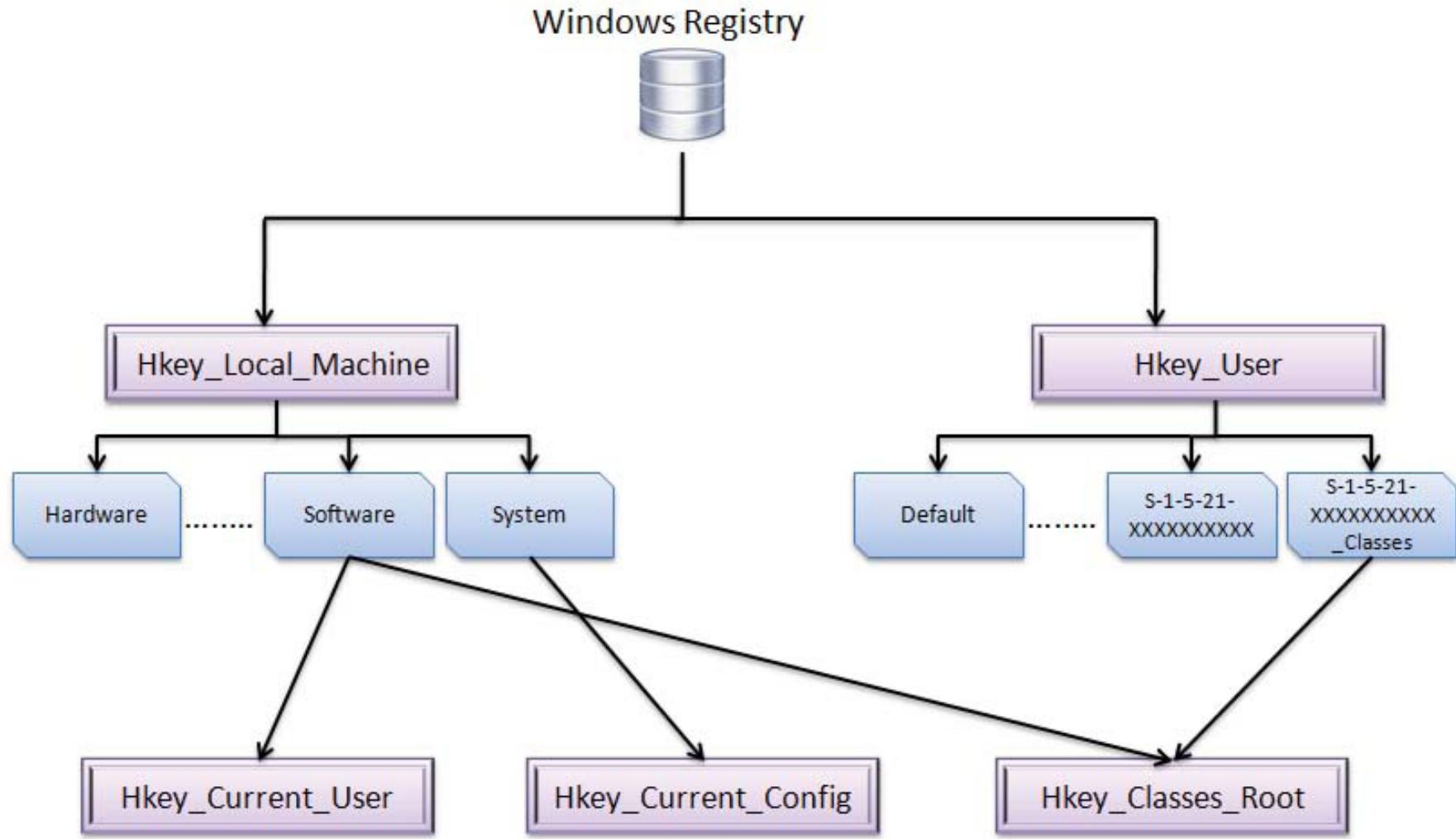
Windows 7 Registry

- Centralised hierarchical database
- Built into memory as system boots
- It is a set of system data files that enables OS to control hardware, software, user information and overall functionality
- Registry files are very useful to an investigation
- Contain information about user behaviour, loaded software and attached hardware
- Tools
 - Regedit and Regedit32
 - Accessdata FTK Imager

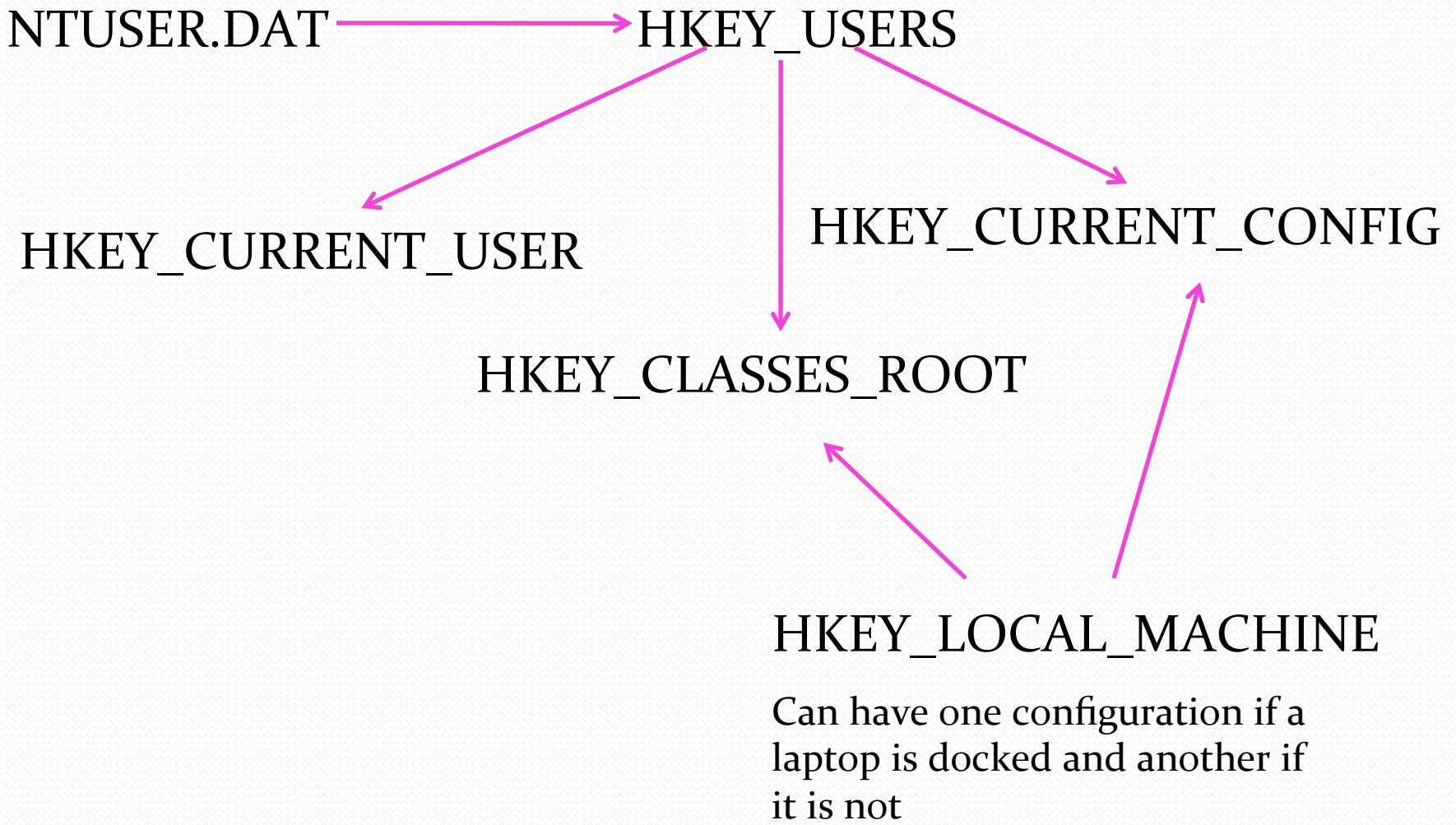
Organisation and Terminology

- At the physical level
 - Files called *hives*
 - Located in: %SYSTEMROOT%\System32\config
- Keys (analogous to folders)
- Values (analogous to files)
- Hierarchy:
 - Hive – like a root folder
 - Key: like a subfolder
 - Subkey: like a subfolder
 - Value: are like the actual data files within the subfolder

Windows 7 Root Keys



Based on who logs
into the system



Forensics benefits of Registry

- MRUs
- Typed URLs
- Installed apps
- Installed devices
- System time settings
- Registered user information
- Passwords and password hashes
- Internet search queries and form data
- Network setting and connection information
- Date and time information of Registry key updates

Important registry artefacts

- User names and passwords for programs, email and Internet sites
- Record of Internet queries (searches)
- Lists of recently accessed files (documents and images)
- List of all programs installed
- System usernames and other login information
- Hardware and system information
- Also get dates and times of registry key updates

- As user first logs on – Windows creates a unique artefact
 - In Documents & Settings (XP) – name of user
 - In Windows 7 and Vista - User/*username*/
 - Called – root user folder
 - Identifies the user by their logon name
-
- Another significant file is NTUSER.DAT
 - Contains
 - File creation = when they first logged on
 - Last update = when they logged off
-
- Recent folder – what user has created or modified

There are Five root Hives

- HKEY_CLASSES_ROOT
 - HKEY_CURRENT_USER
 - HKEY_LOCAL_MACHINE
 - HKEY_USERS
 - HKEY_CURRENT_CONFIG
-
- HKEY_CURRENT_USER and HKEY_LOCAL_MACHINE
 - Contain information that is used to create the other hives
 - HKEY_LOCAL_MACHINE – generated at startup and holds configuration info about the local machine
 - Includes hardware and software settings

HKEY_USERS

- Generated at startup from the individual NTUSER.DAT file
- Contains information on every user on the system

HKEY_CURRENT_USER

- HKEY_USERS is used to generate HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG and HKEY_CLASSES_ROOT

HKEY_CURRENT_CONFIG

- Contains the hardware profile the system uses at startup

HKEY_CLASSES_ROOT

- Contains configuration info relating to which application is used to open various files
 - This hive is subclassed to both HKEY_CURRENT_USER\Software\Classes\ (user specific settings)
HKEY_LOCAL_MACHINE\Software\Classes\ (system wide settings)

Hives in the live registry

1. SAM
2. SECURITY
3. SOFTWARE
4. SYSTEM

- Four main hive files stored in
C:\Windows\System32\config
- HARDWARE – this hive is not stored in the file system
- Created on startup and discarded on shutdown

NTUSER.DAT

- Logged on user's registry file associated with HKEY_CURRENT_USER and HKEY_USERS

BCD

- Boot Configuration Data – contains boot config params
- These used to be in the boot.ini file

UsrClass.dat

- Secondary user profile that stores Class info for each user
- Includes the users MUICache – stores executable file initiation by filename

- Tools to view registry
 - FTK imager
 - EnCase – view file structure
 - Regedit
- 99.9% of all data associated with a user is in NTUSER.DAT
- If you want information from the HKEY_CURRENT_USER open NTUSER.DAT in a registry viewer
- Windows locks live Registry files – gives a sharing violation
- SAM and SECURITY are found in
- Windows\system 32\config

- Registry entries are updated in different ways
 - Registry intensive
 - File intensive
- Some entries update as soon as a task is completed
- Some do not update until the application closes normally
- Examples
- newly created user will appear in the SAM registry file immediately
- IE browser entries for the TypedURLs MRU list do not update until the browser is closed
- How will pulling the plug affect your case?

Closing a Mounted Registry Hive

- If you don't need it then close it
 1. If you mount all the registry hives and save your case, it will take a long time to open the case again
 2. If you select the Set Include Option or select all files in your case it will include the mounted registries
 3. A mounted hive does use extra RAM on your computer
- A quick way to see mounted hives – select the Devices tab
- Then select disk view in the tree pane
- Right click a select Close

Forensic Analysis - Hardware

The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under 'Computer'. The 'BIOS' key under 'CentralProcessor\0' is selected. The right pane shows a table of registry values for this key.

Name	Type	Data
(Default)	REG_SZ	(value not set)
BaseBoardManu...	REG_SZ	ASUSTeK Computer INC.
BaseBoardProdu...	REG_SZ	P5N32-E SLI
BaseBoardVersion	REG_SZ	1.XX
BiosMajorRelease	REG_DWORD	0x000000ff (255)
BiosMinorRelease	REG_DWORD	0x000000ff (255)
BIOSReleaseDate	REG_SZ	08/22/2007
BIOSVendor	REG_SZ	Phoenix Technologies, LTD
BIOSVersion	REG_SZ	ASUS P5N32-E SLI ACPI BIOS Revision 1205
ECFirmwareMaj...	REG_DWORD	0x000000ff (255)
ECFirmwareMin...	REG_DWORD	0x000000ff (255)
SystemFamily	REG_SZ	
SystemManufac...	REG_SZ	System manufacturer
SystemProduct...	REG_SZ	System Product Name
SystemSKU	REG_SZ	
SystemVersion	REG_SZ	System Version

Computer\HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS

AccessData Registry Viewer - [SAM[40497].tmp]

File Edit Report View Window Help

SAM[40497].tmp

SAM

Domains

Account

Aliases

Groups

Users

000001F4

000001F5

000003E9

Key Properties

Last Written Time	07/06/2010 16:22:21 UTC
SID unique identifier	500
User Name	Administrator
Description	Built-in account for administering the computer/domain
Logon Count	1
Last Logon Time	14/07/2009 04:53:58 UTC
Last Password Change Tim	14/07/2009 04:55:45 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	true
Password Required	true
Country Code	0 (System Default)
Hours Allowed	Anytime
Has LAN Manager Passwor	false
Has NTLMv2 Password	true

Forensic Analysis – User ID

- SID (security identifier)
 - Well-known SIDs
 - SID: S-1-0 Name: Null Authority
 - SID: S-1-5-2 Name: Network
 - S-1-5-21-2553256115-2633344321-4076599324-1006
 - S string is SID
 - 1 revision number
 - 5 authority level (from 0 to 5)
 - 21-2553256115-2633344321-4076599324 - domain or local computer identifier
 - 1006 RID – Relative identifier
- Local SAM resolves SID for locally authenticated users (not domain users)
 - Use recycle bin to check for owners

Forensic Analysis - Software

Registry Editor

File Edit View Favorites Help

JavaSoft
JreMetrics
Kronos
Linksys
McAfee
Microsoft
MozillaPlugins
NeoSmart Technologies
Network Associates
NVIDIA Corporation
ODBC
Policies
RegisteredApplications
Software
Sonic
VMware, Inc.
Volatile
WinRAR
Wow6432Node
SYSTEM
HKEY_USERS

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications

Name	Type	Data
ab(Default)	REG_SZ	(value not set)
abGoogle Chrome	REG_SZ	Software\Clients\StartMenuInternet\Google Chrome\Capabilities
abInternet Explorer	REG_SZ	SOFTWARE\Microsoft\Internet Explorer\Capabilities
abMicrosoft Office...	REG_SZ	Software\Clients\Mail\Microsoft Outlook\Capabilities
abPaint	REG_SZ	SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\Paint\Capabilities
abSkype	REG_SZ	SOFTWARE\Clients\Internet Call\Skype\Capabilities
abWinamp	REG_SZ	Software\Clients\Media\Winamp\Capabilities
abWindows Addre...	REG_SZ	Software\Clients\Contacts\Address Book\Capabilities
abWindows Disc I...	REG_SZ	Software\Microsoft\IsoBurn\Capabilities
abWindows Media...	REG_SZ	Software\Clients\Media\Windows Media Center\Capabilities
abWindows Media...	REG_SZ	Software\Clients\Media\Windows Media Player\Capabilities
abWindows Photo ...	REG_SZ	Software\Microsoft\Windows Photo Viewer\Capabilities
abWindows Search	REG_SZ	Software\Microsoft\Windows Search\Capabilities
abWinRAR	REG_SZ	Software\WinRAR\Capabilities
abWordpad	REG_SZ	Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Capabilities

Windows Security and Relative ID

- The Windows Registry utilizes a alphanumeric combination to uniquely identify a security principal or security group.
- The Security ID (SID) is used to identify the computer system.
- The Relative ID (RID) is used to identity the specific user on the computer system.
- The SID appears as:
 - S-1-5-21-927890586-3685698554-67682326-1005

Forensics Analysis - NTUSER.DAT

- Internet Explorer
 - IE auto logon and password
 - IE search terms
 - IE settings
 - Typed URLs
 - Auto-complete passwords

Forensics Analysis - NTUSER.DAT

IE explorer Typed URLs

The screenshot shows the Windows Registry Editor window. The title bar reads "Registry Editor". The menu bar includes "File", "Edit", "View", "Favorites", and "Help". The left pane displays a tree view of registry keys under "My Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer". The "TypedURLs" key is selected and highlighted with a red border. The right pane contains a table with three columns: "Name", "Type", and "Data". The "Name" column lists entries from "(Default)" to "ab:url19". The "Type" column shows all entries as "REG_SZ". The "Data" column lists various URLs, such as "http://www.ucsc.edu", "http://129.210.114.76/hello.cgi", and "http://www.google.com/".

Name	Type	Data
ab(Default)	REG_SZ	(value not set)
ab:url1	REG_SZ	http://www.ucsc.edu
ab:url10	REG_SZ	http://129.210.114.76/hello.cgi
ab:url11	REG_SZ	http://localhost/hello.cgi
ab:url12	REG_SZ	http://localhost/test.cgi
ab:url13	REG_SZ	http://localhost/
ab:url14	REG_SZ	http://hotmail.com/
ab:url15	REG_SZ	http://httpd.apache.org/docs/2.2/mod/core.
ab:url16	REG_SZ	http://www.google.com/
ab:url17	REG_SZ	http://adm.lnpu.edu.ua/
ab:url2	REG_SZ	http://www.amazon.com/
ab:url3	REG_SZ	http://www.voroem.com/
ab:url4	REG_SZ	http://www.msdevey.com/
ab:url5	REG_SZ	http://www.scu.edu/
ab:url6	REG_SZ	http://www.hotmail.com/
ab:url7	REG_SZ	http://www.expedia.com/
ab:url8	REG_SZ	http://www.cnn.com/
ab:url9	REG_SZ	http://cnn.com/

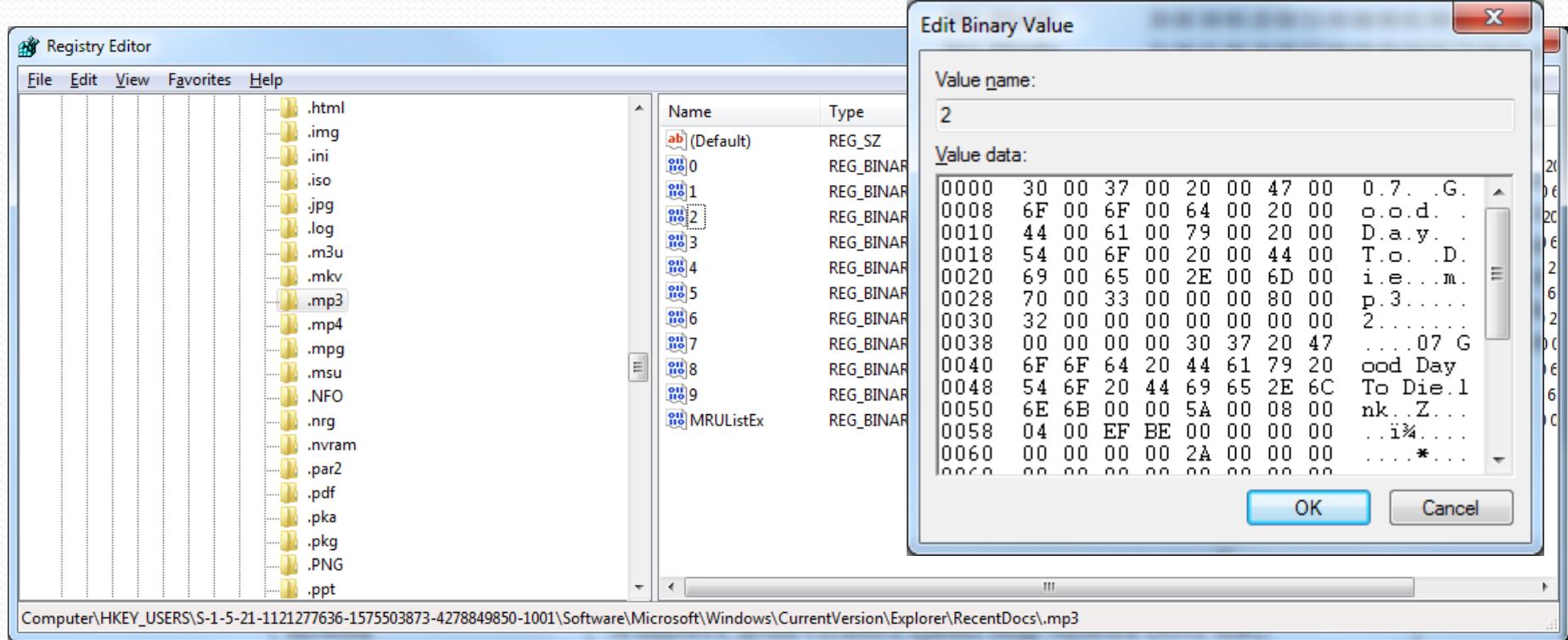
My Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Forensic Analysis – MRU List

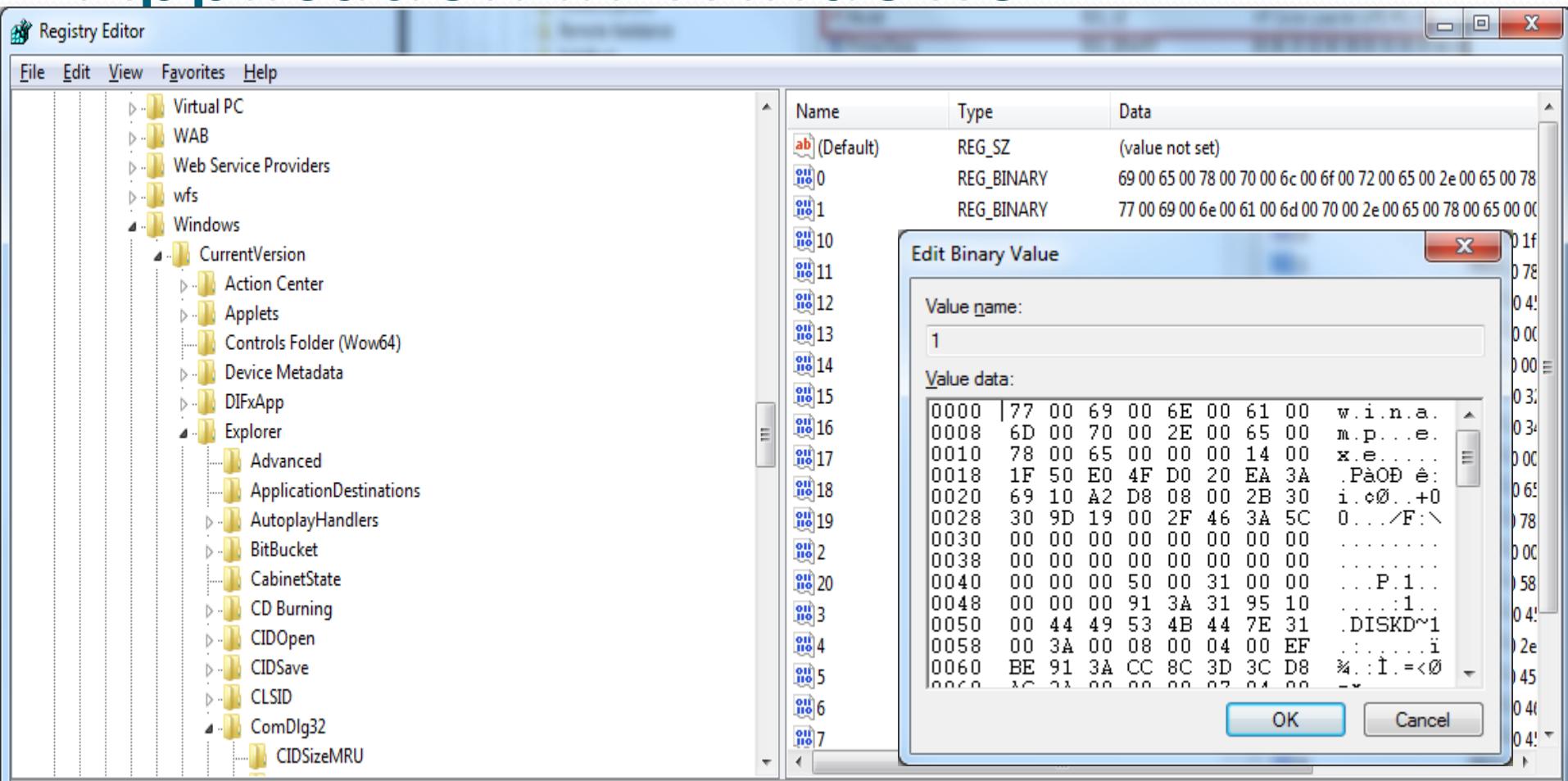
A “Most Recently Used List” contains entries made due to specific actions performed by the user. There are numerous MRU list locations throughout various Registry keys.

These lists are maintained in case the user returns to them in the future.

Essentially, their function is similar to how the history and cookies act in a web browser.



Forensic Analysis – Last Opened Application in Windows



Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidMRU

Forensic Analysis – USB Devices

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Verbatim&Prod_STORE_N_GO&Rev_2.00\0000000000001D58&0

The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under the path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR. The right pane shows a detailed table of registry key values for a selected key.

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{a55fc8de-7617-5b34-9ab1-deefcd5483cda}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0011
FriendlyName	REG_SZ	Verbatim STORE N GO USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskVerbatimSTORE_N_GO____2.00 USBSTOR\Disk
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk

Registry Forensics

Case Study

(Chad Steel: Windows Forensics, Wiley)

Department manager alleges that individual copied confidential information on DVD.

No DVD burner was issued or found.

Laptop was analyzed.

Found USB device entry in registry:

PLEXTOR DVDR PX-708A

Found software key for Nero - Burning ROM in registry

Therefore, looked for and found Nero compilation files (.nrc). Found other compilation files, including ISO image files.

Image files contained DVD-format and AVI format versions of copyrighted movies.

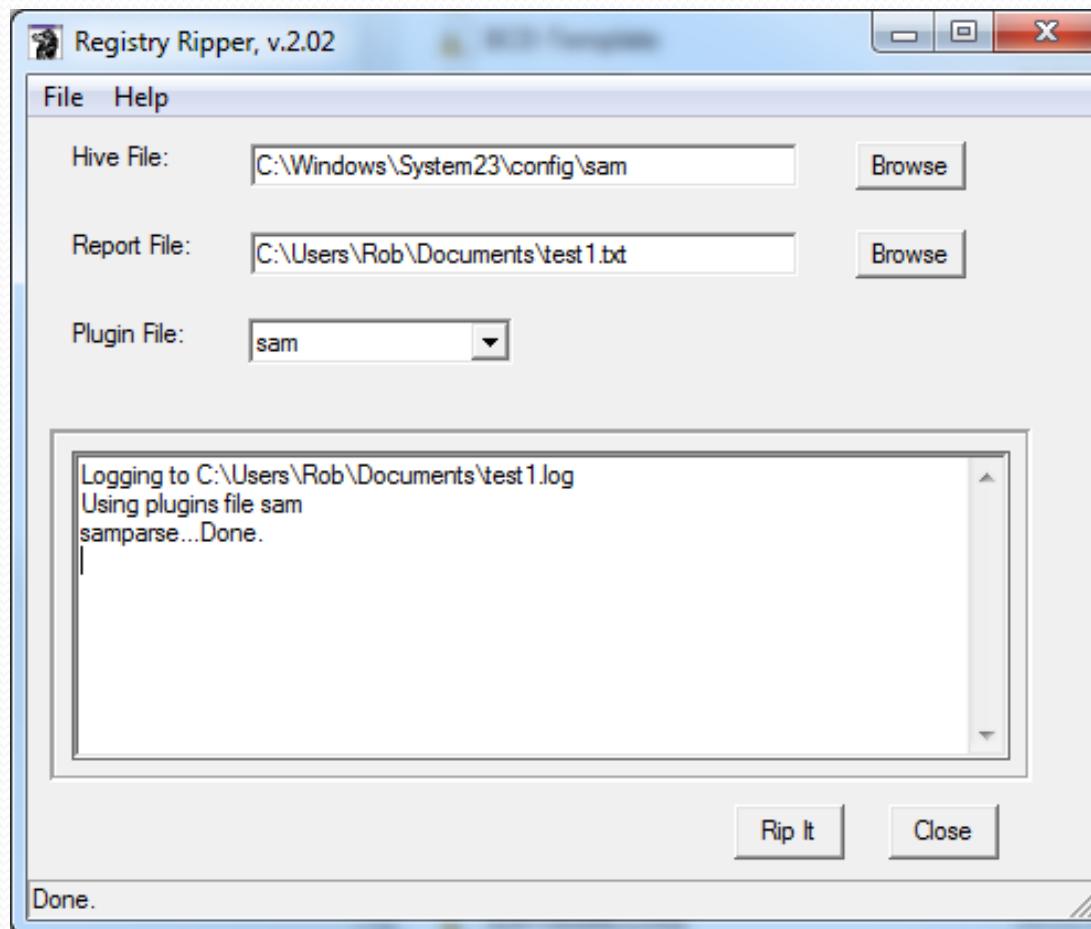
Conclusion: No evidence that company information was burned to disk. However, laptop was used to burn copyrighted material and employee had lied.

Monitoring the Registry

- The registry is highly complex, and there is not one single point of reference
- Experimentation allows you as an investigator to find out for yourself what has occurred
- Real time experimentation helps with post-mortem analysis
- Regmon (Replaced by Procmon) from Microsoft
 - Monitors the registry in real time

RegRipper

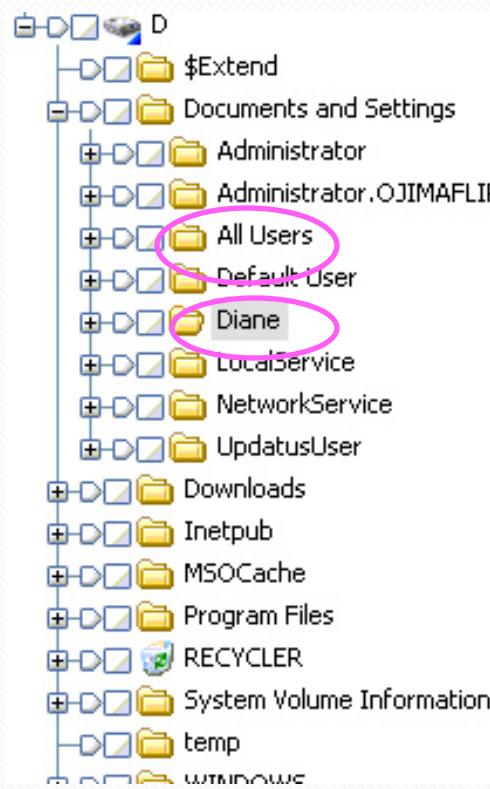
The RegRipper is an open-source application for extracting, correlating, and displaying specific information from Registry hive files from the Windows NT (2000, XP, 2003, Vista and 7) family of operating systems.



Windows 7 Registry Artifacts

- All Users – should also be investigated
- Not user specific – more global
- Each user gets a specific named account folder
- Root named after the user's login name
- NTUSER.DAT
- Specific settings for the user
 - Updated when the user logs out

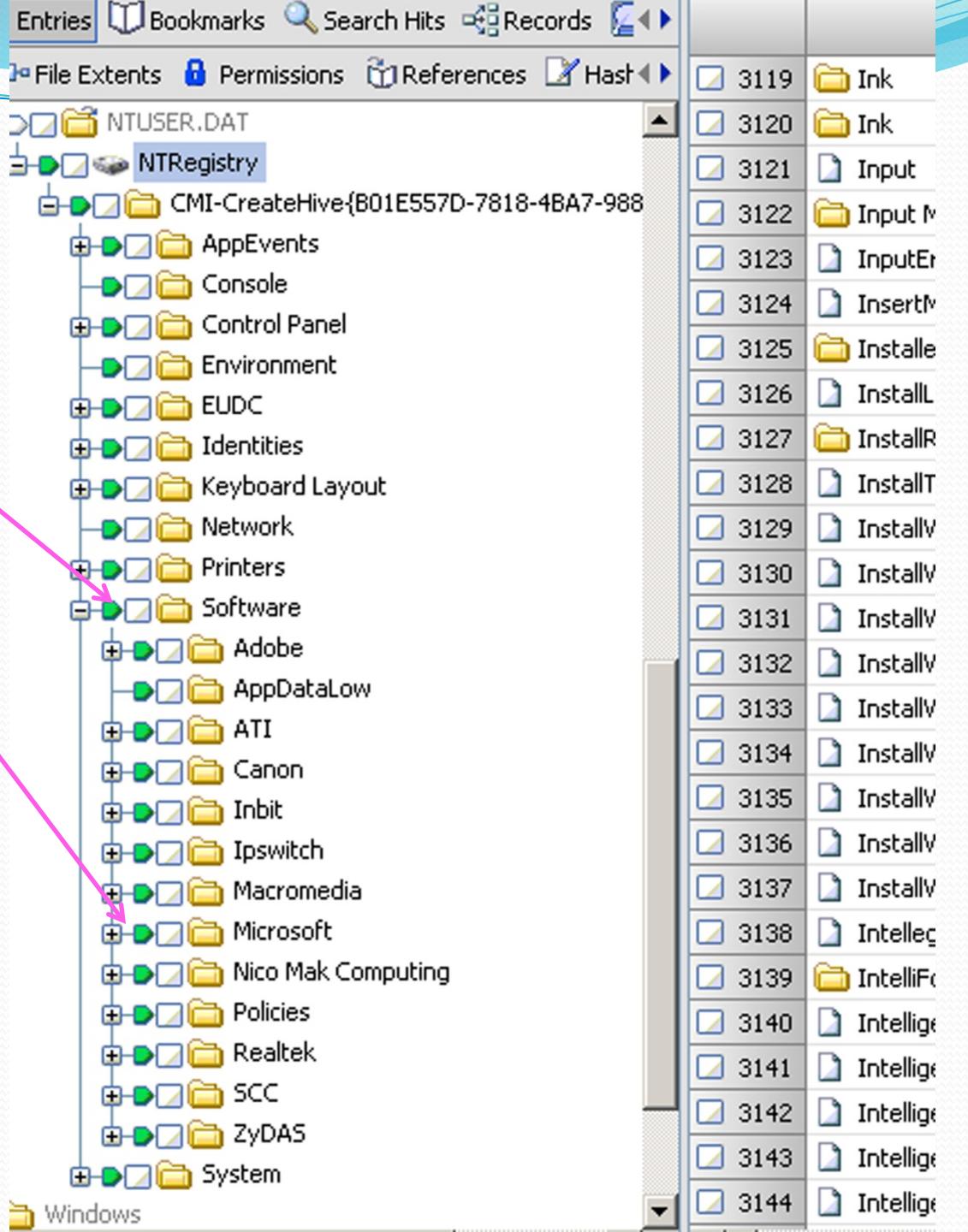
XP view



3	Desktop
4	Favorites
5	IECompatCache
6	IETldCache
7	Local Settings
8	My Documents
9	NetHood
10	NTUSER.DAT
11	ntuser.dat.LOG
12	ntuser.ini
13	PrintHood
14	PrivacIE
15	Recent
16	SendTo
17	Start Menu
18	Templates
19	UserData

- NTUSER.DAT
- Software
- Microsoft
- Internet Explorer
- TypedURLs
- TypedPaths
- Most recently used docs (MRU)
- Mounted and mapped drives
- Search history (IE)

For Win XP to Win 7



NTUSER.DAT\Software\Microsoft\Internet Explorer

\TypedURLs

The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under 'Microsoft\Internet Explorer\Software'. The 'TypedURLs' key is selected and expanded, showing ten entries labeled 'url1' through 'url10'. The right pane is a table with two columns: 'Name' and 'Value'. The 'Name' column lists the URL names, and the 'Value' column shows their corresponding binary data. The bottom pane shows the raw hex and ASCII values for the selected URL entry.

	Name
1	url1
2	url2
3	url3
4	url4
5	url5
6	url6
7	url7
8	url8
9	url9
10	url10

Hex View:

```
00 70 00 3A 00 2F 00 2F 00 77 00 77 00 77 00 b·t·t·p···//·w·w·w·  
00 6D 00 6D 00 61 00 2E 00 63 00 6F 00 6D 00 .·m·a·m·m·a·c·o·m·  
/....
```

- tracks up to 25 URLs
- not updated until IE browser has been exited appropriately
- changed with IE8
- forensically important because it demonstrates user behaviour

NTUSER.DAT\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

- RecentDocs
- Stored by extension
- Stores the last 10 of each extension type (0-9)
- Creates new extension subkey if new file type
- Notice MRUListEx
- Lists chronological order of access

The screenshot shows a Windows registry editor window with the following details:

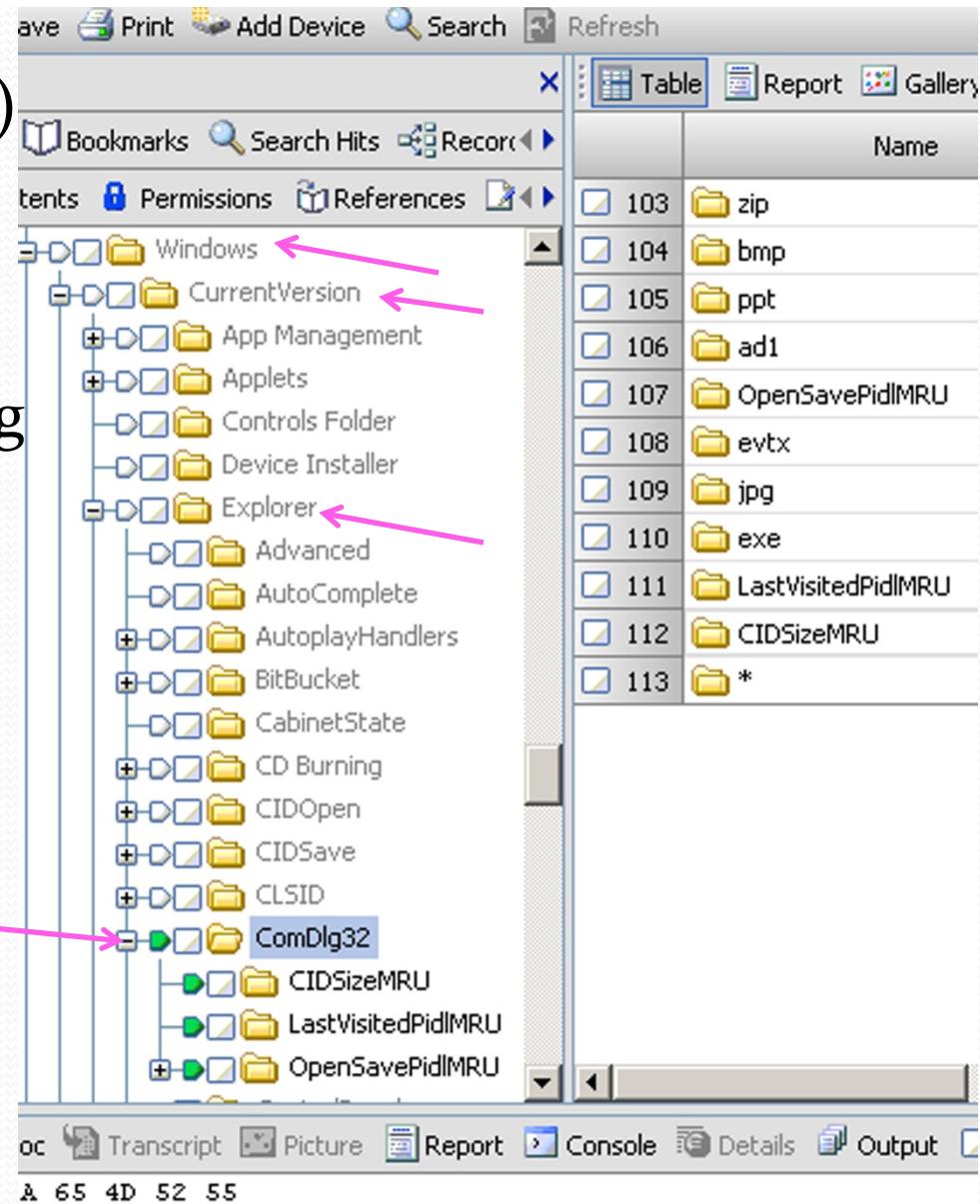
- Left pane (Tree View):** Shows the structure of the registry key:
 - RecentDocs
 - .ad1
 - .bek
 - .bmp
 - .doc
 - .evtx
 - .fang
 - .gif
 - .htm
 - .html
 - .ini
 - .jpg
 - .log
 - .mht
 - .pdf
 - .pf
 - .png
 - .ppt
 - .rtf
 - .tooth
 - .txt
 - .xar
 - .xls
 - .zip
 - Folder
- Right pane (List View):** A table showing the names of recent documents, their extensions, and their access counts.

Name	Extension	Access Count
98	3	0
99	6	0
100	7	0
101	8	0
102	9	0
103	1	0
104	4	0
105	5	0
106	0	0
107	7	0
108	MRUListEx	0
109	0	0
110	MRUListEx	0
111	MRUListEx	0
112	0	0
113	1	0
114	0	0
115	MRUListEx	0
116	1	0
117	2	0
118	0	0
119	3	0
120	0	0
121	MRUListEx	0
122	3	0

A pink arrow points from the text "Lists chronological order of access" to the "Access Count" column in the list view table.

NTUSER.DAT\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32

- Common Dialog (ComDlg32)
- Tracks user behaviour for Open and Save As
- Recorded here if a program uses Windows standard dialog box to access documents
- In Vista and Win 7 more binary data is stored here
- In Win 7
 - CIDSizeMRU
 - FirstFolder
 - LastVisitedPidlMRU
 - LastVisitedPidlMRULegacy
 - OpenSavePidlMRU



EnCase Law Enforcement

File Edit View Tools Help

New Open Save Print Add Device Search Refresh Find

Cases Entries Bookmarks

Table Report Gallery Timeline Disk Code

Home Entries Bookmarks

File Extents P

OpenSavePidMRU

- *
- ad1
- bek
- bmp
- evtx
- exe
- ...c

Name Last Written Filter In Report File Ext

	Name	Last Written	Filter	In Report	File Ext
1	0			No	
2	MRUListEx			No	
3	1			No	
4	2			No	
5	3			No	
6	4			No	
7	5			No	
8	6			No	

Text Hex Doc Transcript Picture Report Console Details Output EnScript Hits F

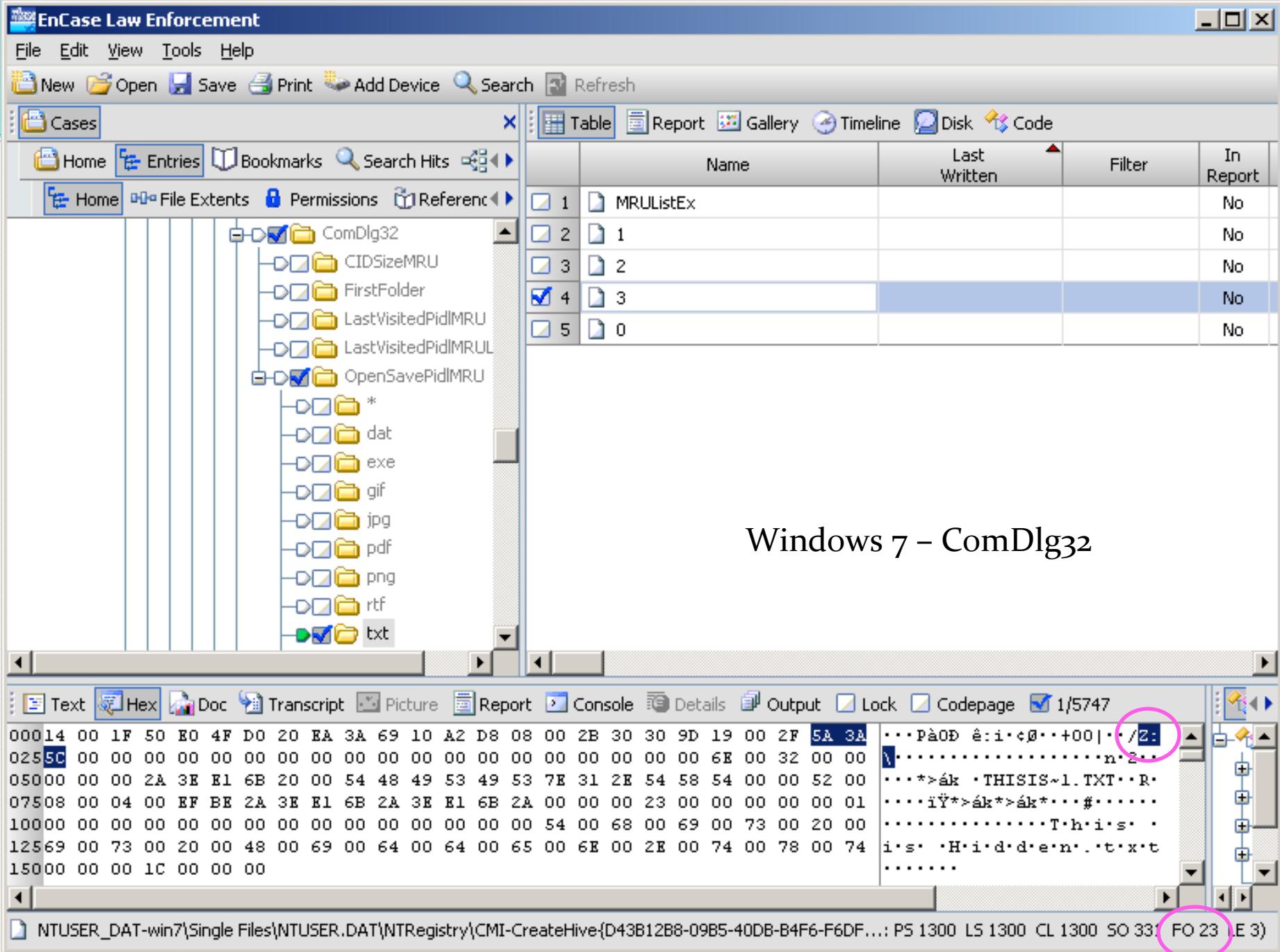
00014 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 ...Pa0D 8:i<@...+0
01830 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 00 00 00 0|.../C:\.....
03600 00 00 00 00 00 00 00 84 00 31 00 00 00 00 00 00 EC0-1.....i
05436 A7 9D 11 00 50 52 4F 47 52 41 7E 31 00 00 6C 00 07 680...PROGRA~1..1..
07200 04 00 EF BE 62 35 51 5A BC 36 A7 9D 26 00 00 00 3D ...iYb5QZi6\$04....=br/>09000 00 00 00 00 01 00 00 00 00 00 00 00 00 00 42 00 50B-P
10800 72 00 6F 00 67 00 72 00 61 00 6D 00 20 00 46 00 69 .r.o.g.r.a.m..F-i
12600 6C 00 65 00 73 00 00 00 40 00 73 00 68 00 65 00 6C .l.e.s...@s.h.e.l
14400 6C 00 33 00 32 00 2E 00 64 00 6C 00 6C 00 2C 00 2D .1.3.2..d.1.1.,--
16200 32 00 31 00 37 00 38 00 31 00 00 00 18 00 62 00 31 .2.1.7.8.1....b.1
18000 00 00 00 00 91 36 04 BB 10 00 4D 49 43 52 4F 53 7E06...>..MICROS~

EnScript Examples Forensic Include Main Source Processor

NTUSER.DAT\Manooth 30 Decrypted\Users\Wes Manooth\NTUSER.DAT\NTRegistry\CMICr...: PS 3246 LS 3246 CL 3246 SO 179 FO 23 LE 2)

ComDlg32

At offset 23 - you can see the drive letter



Windows 7 – ComDlg32

- Different functions are being tracked by LastVisitedPidlMRU and OpenSavePidlMRU
- This means that data can't be correlated between the two keysets
- Also using Windows Save As dialog box means that the data can't be correlated with the RecentDocs subkey
- CIDSizeMRU subkey
- Tracks applications used to access files
- Only records that say IE browser was used
- Show the application name but not the associated documents

Windows 7 – ComDlg32

- FirstFolder subkey (new)
- Stores default paths
- It can be useful forensically to show that an application was accessible to the system
- May be an instance of proving that uninstalled software had been on the system
- Entries are not removed from ComDlg32 when an application is removed
- Also the accessed files will also still be recorded

Windows 7 – ComDlg32

- LastVisitedPidlMRU
- Tracks applications that are used to open documents using the Open/Save dialog box
- Not all applications appear here
- Why?
- Difference between this and FirstFolder is
 - FirstFolder tracks the application used and installation location
 - LastVisitedPidlMRU tracks the application name and path on which it acted
- If drive is external or unknown then the drive letter will be included
- Else it will be referenced by GUID

Windows 7 – ComDlg32

- LastVisitedPidlMRULegacy
- New keyset to reference 32 bit applications
- 64 bit applications are stored in LastVisitedPidlMRU
- OpenSavePidlMRU
- Of great forensics interest
- References individual files accessed by the user
- Again it is dependent on it using the Open/Save dialog box
- Similar to RecentDocs – tracked on an extension basis
- Stores last 20 items (0 to 19₁₀)
- However, there are some inconsistencies regarding where a document is stored

OpenSavePidlMRU

- Type of data seen depends on the location of the document
- Example – doc opened or saved on an external drive
 - The drive letter will appear at offset 23
 - Path in both ASCII and unicode are separated by binary data
 - However, known paths to Windows are not displayed
- Pidl = Pointer to an Item Identifier List
- This artifact gives a good overview of user behaviour on the system
- Shows applications accessed and saved documents

NTUSER.DAT\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

- The RunMRU subkey
- Tracks user entries from the Start > Run command
- Alphabetical order - a to z
- If user mistypes then this is not stored
- But a mistyped URL will be stored, as it invokes IE
- Order is tracked using the MRUList value
- Last one used is first on list

Summary

- Significant changes in Windows 7
- Artifacts left behind are very useful to our investigation
- Knowing where to look is the key