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

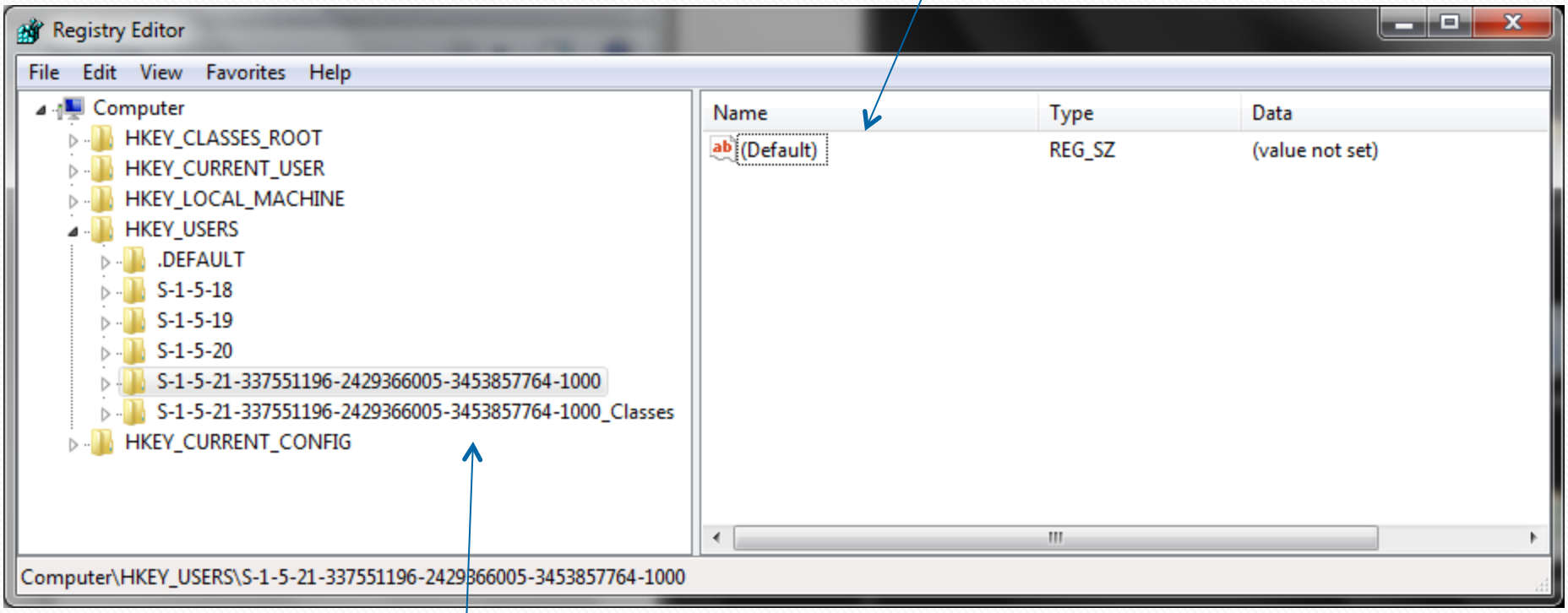
Unchanged user artifacts

- 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

Value


Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
.DEFAULT
S-1-5-18
S-1-5-19
S-1-5-20
S-1-5-21-337551196-2429366005-3453857764-1000
S-1-5-21-337551196-2429366005-3453857764-1000_Classes
HKEY_CURRENT_CONFIG
Name
Type
Data
(Default)
REG_SZ
(value not set)
Computer\HKEY_USERS\S-1-5-21-337551196-2429366005-3453857764-1000

Key

Windows 7 Registry

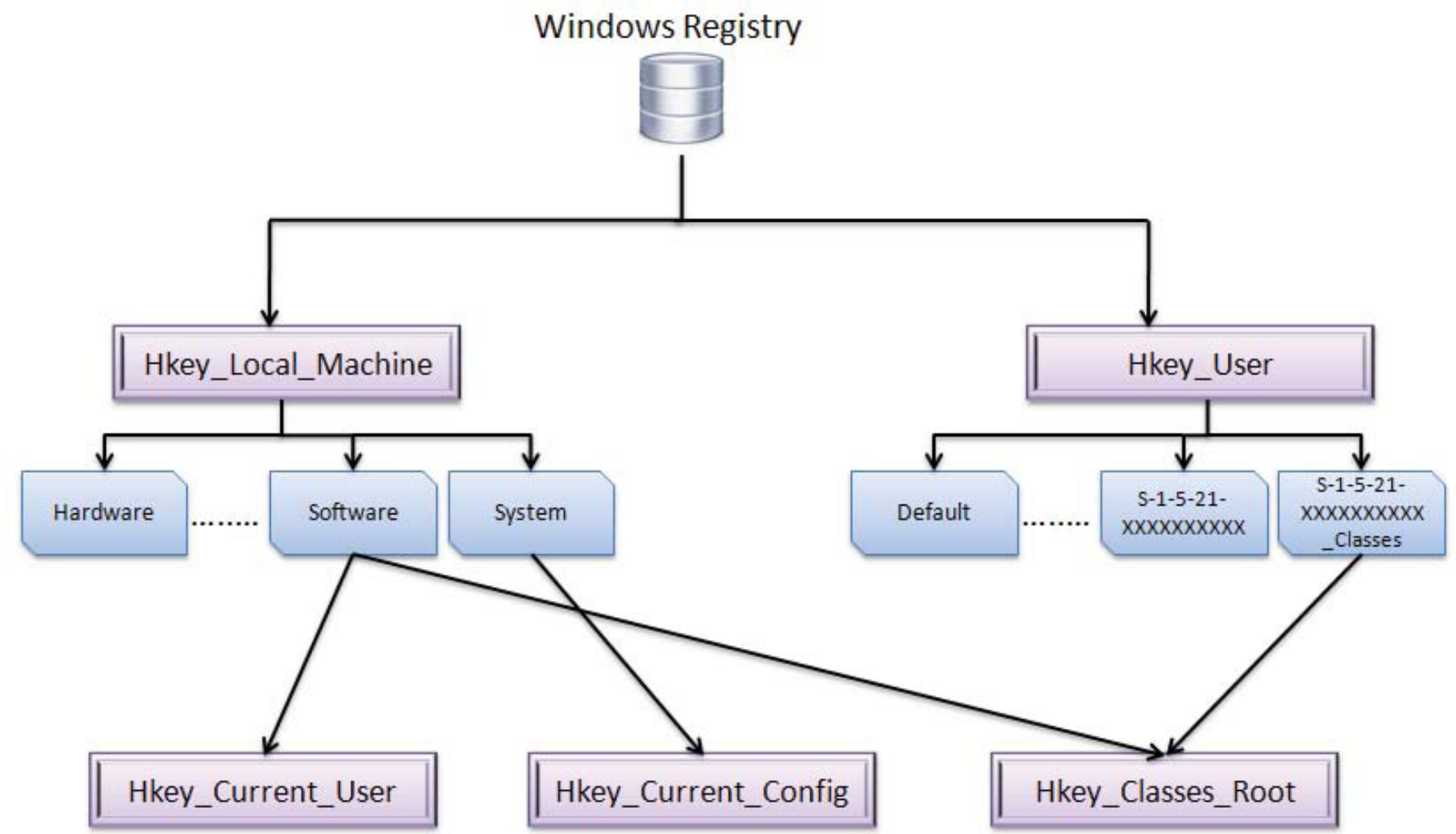
- Centralised hierarchical database
- Built into memory as system boots
- It is a set of system data files that enables OS to control hardware, software, user information and overall functionality
- Registry files are very useful to an investigation
- Contain information about user behaviour, loaded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

- Tools
  - Regedit and Regedit32
  - Accessdata FTK Imager

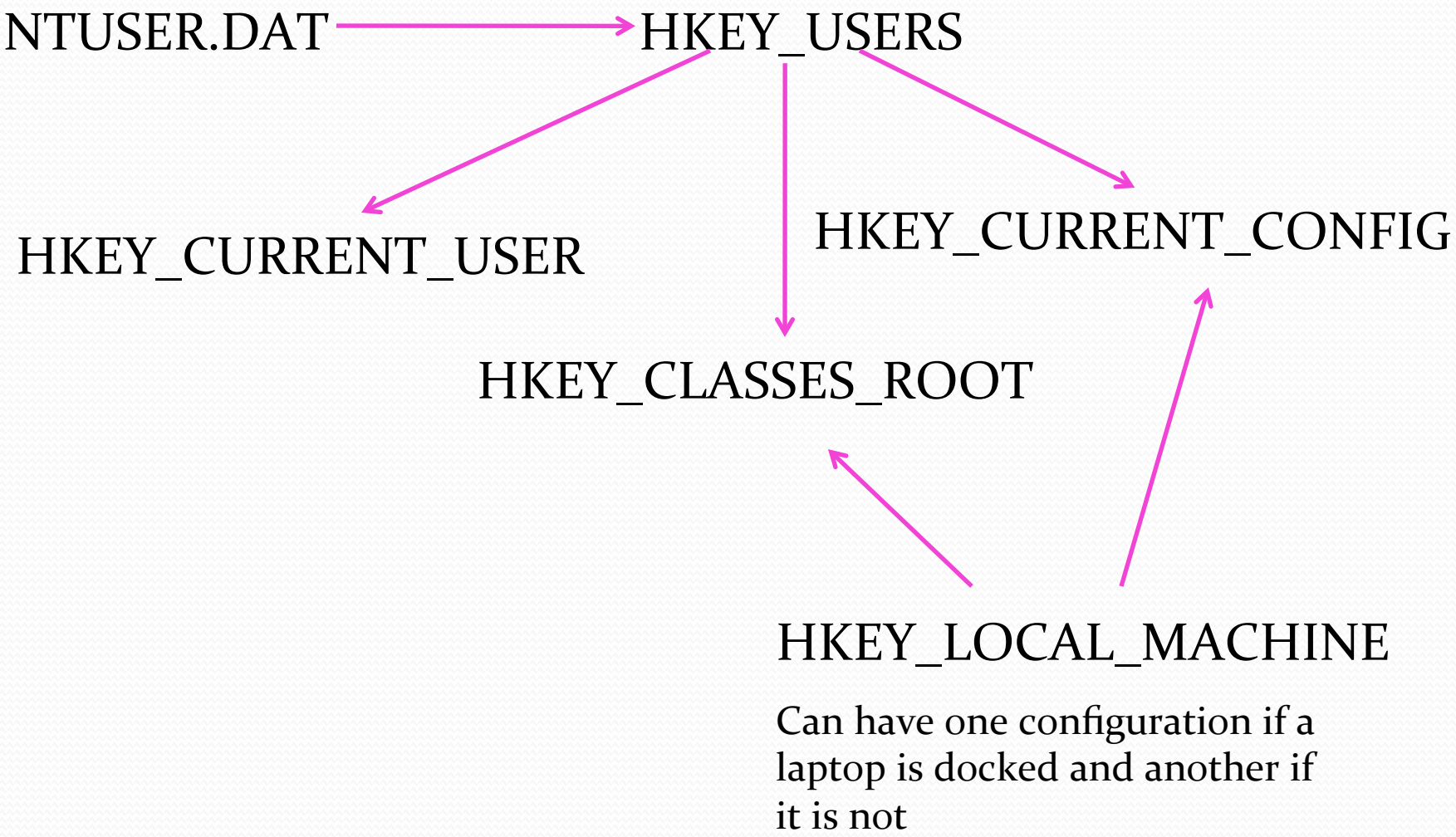
Organisation and Terminology

- 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



Can have one configuration if a laptop is docked and another if it is not

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

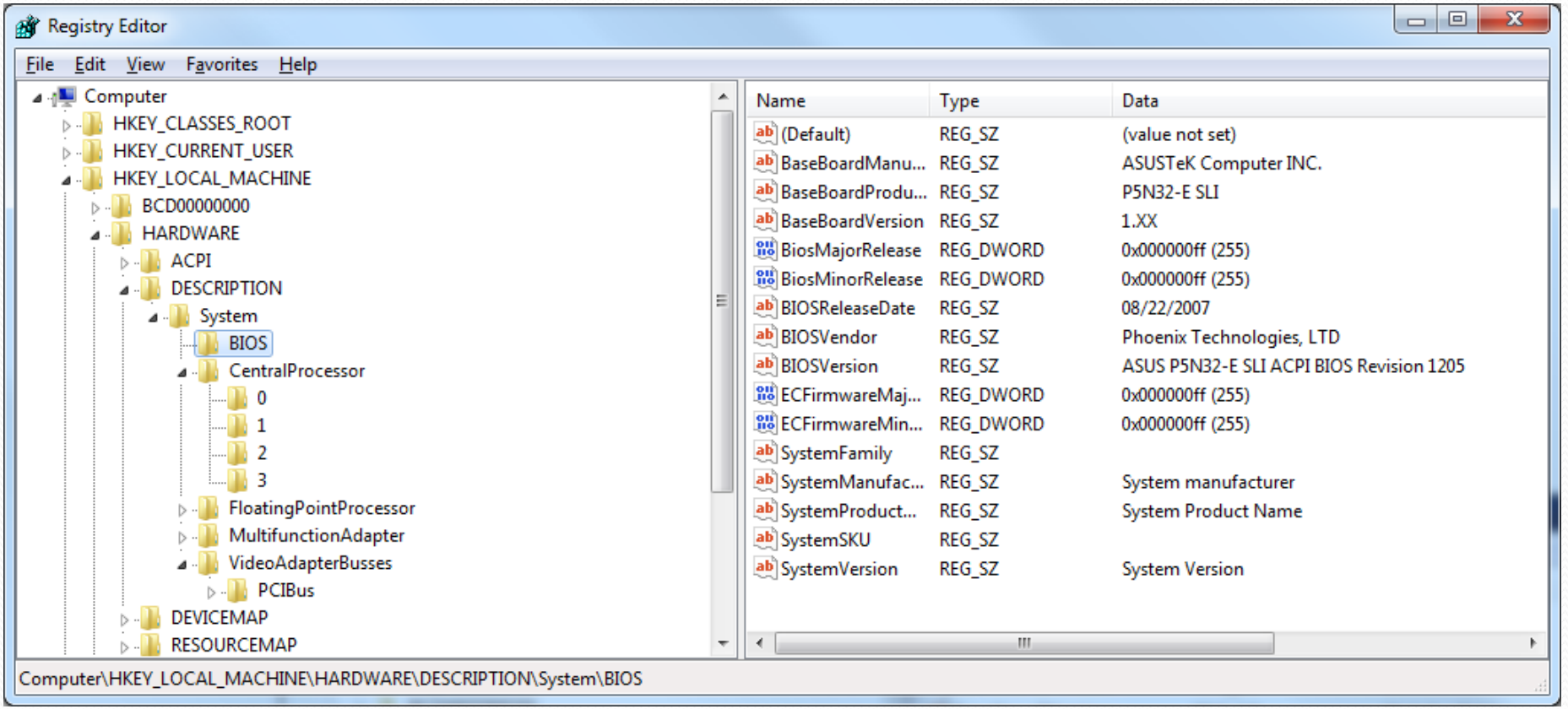
- Examples
- newly created user will appear in the SAM registry file immediately
- IE browser entries for the TypedURLs MRU list do not update until the browser is closed
- How will pulling the plug affect your case?

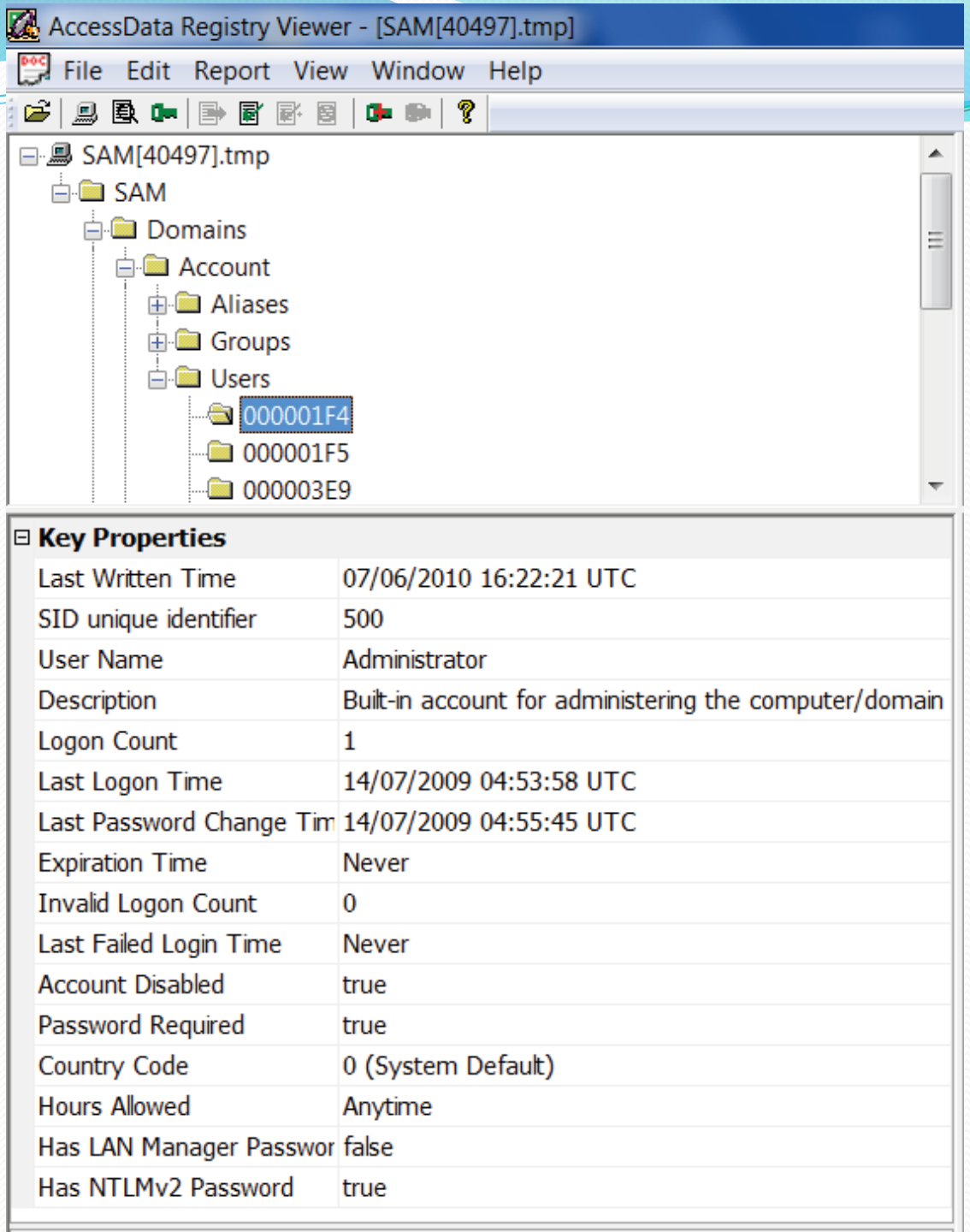
Closing a Mounted Registry Hive

- 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

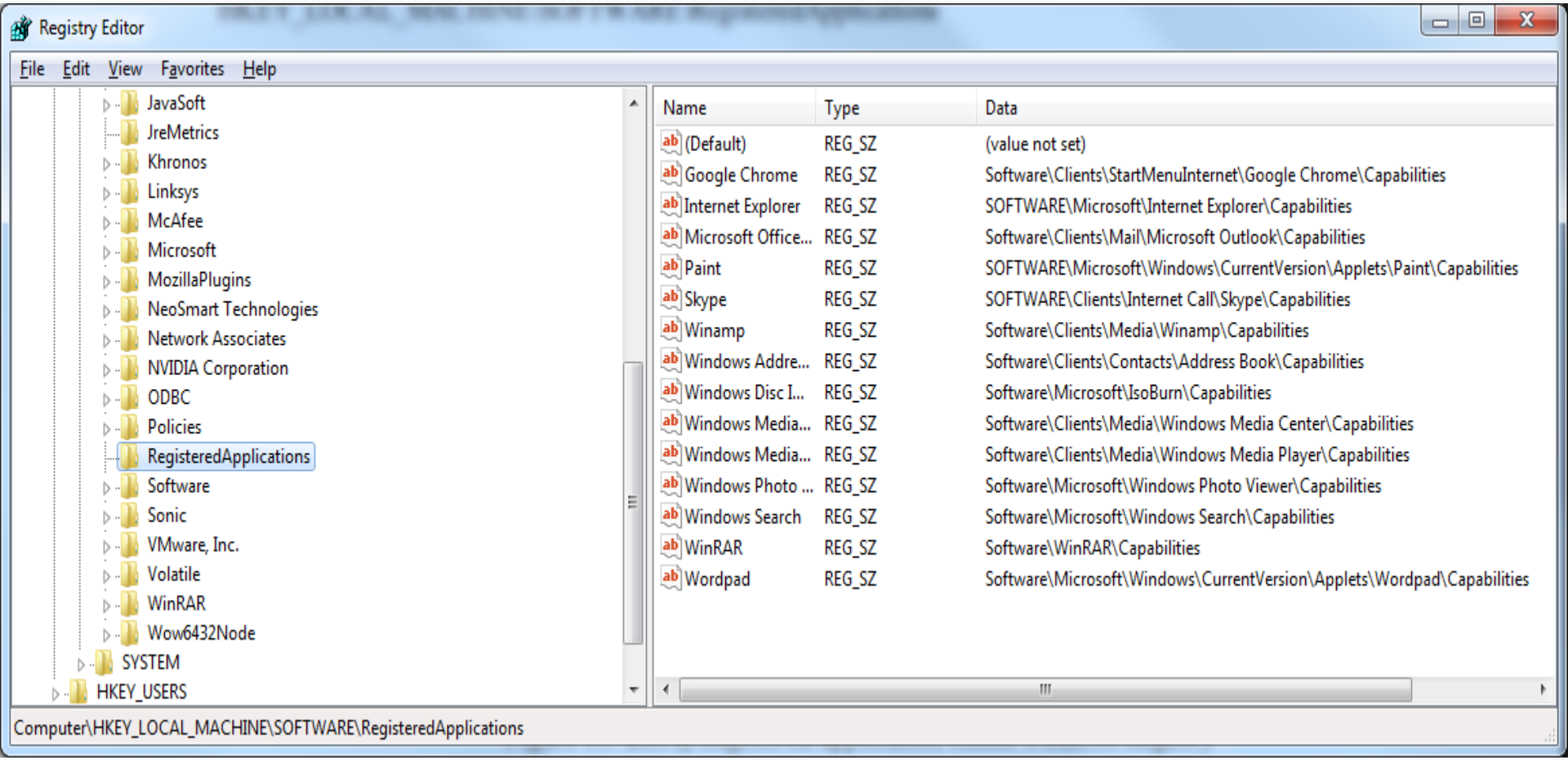



AccessData Registry Viewer - [SAM[40497].tmp]
File Edit Report View Window Help
SAM[40497].tmp
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000003E9
Key Properties
Last Written Time 07/06/2010 16:22:21 UTC
SID unique identifier 500
User Name Administrator
Description Built-in account for 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



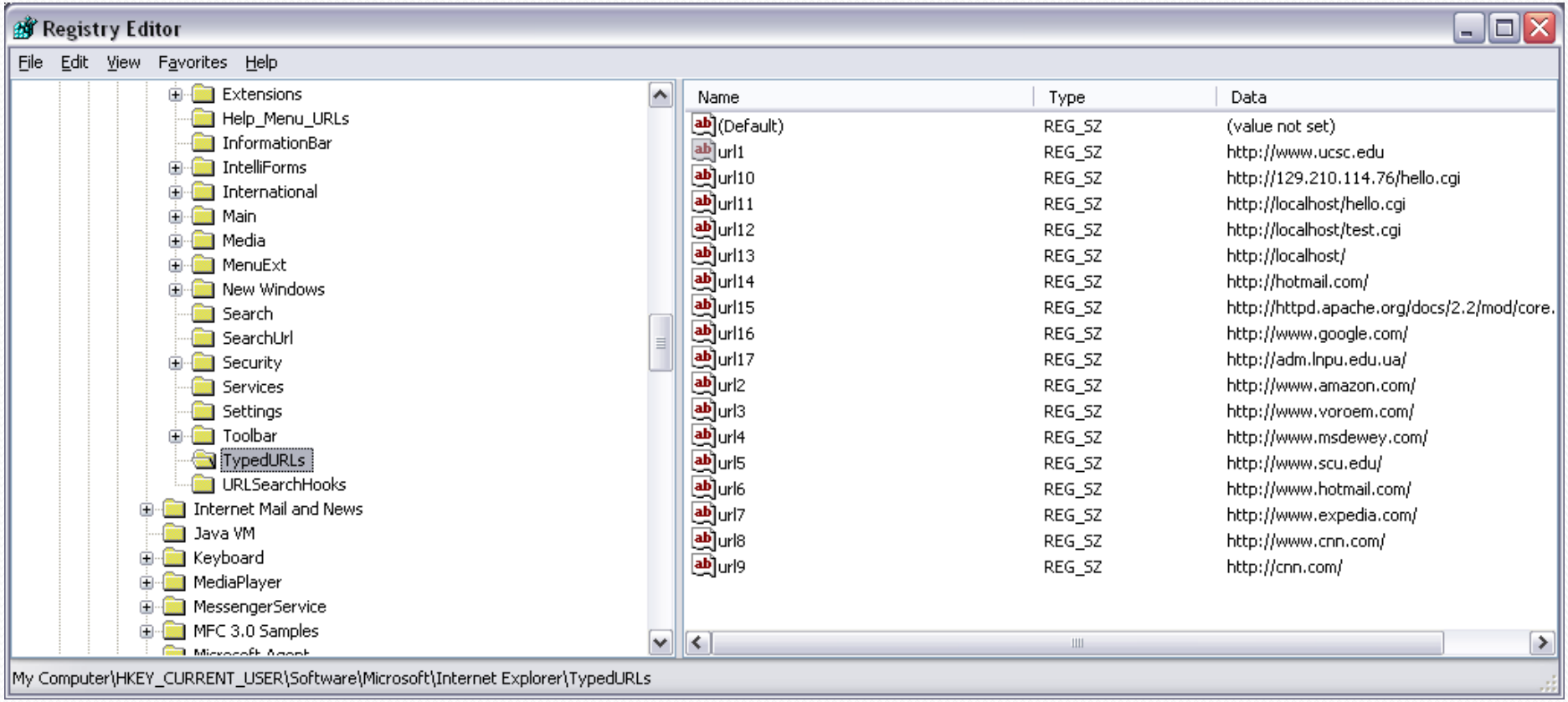
Windows Security and Relative ID

- 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

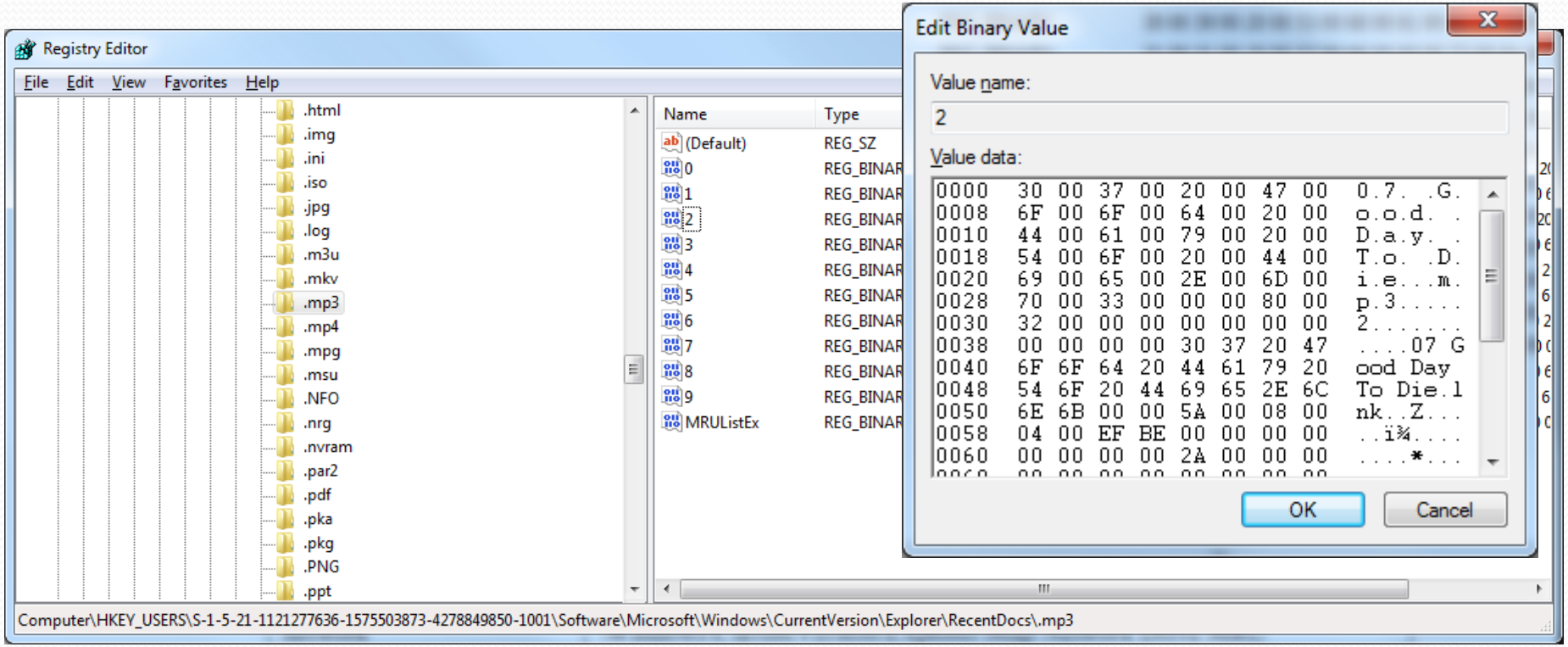
Forensics Analysis - NTUSER.DAT
IE explorer Typed URLs



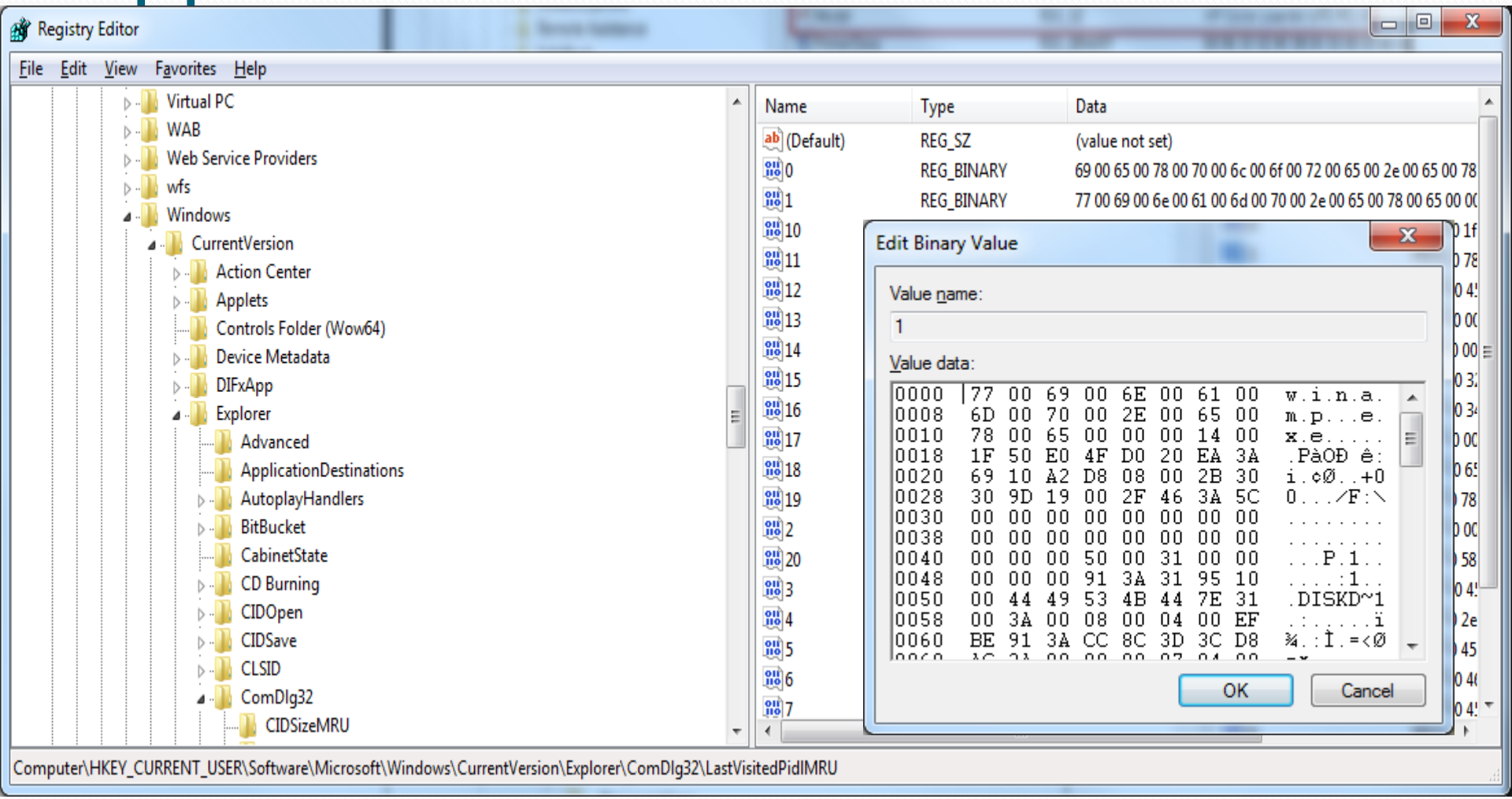
Forensic Analysis – MRU List

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.

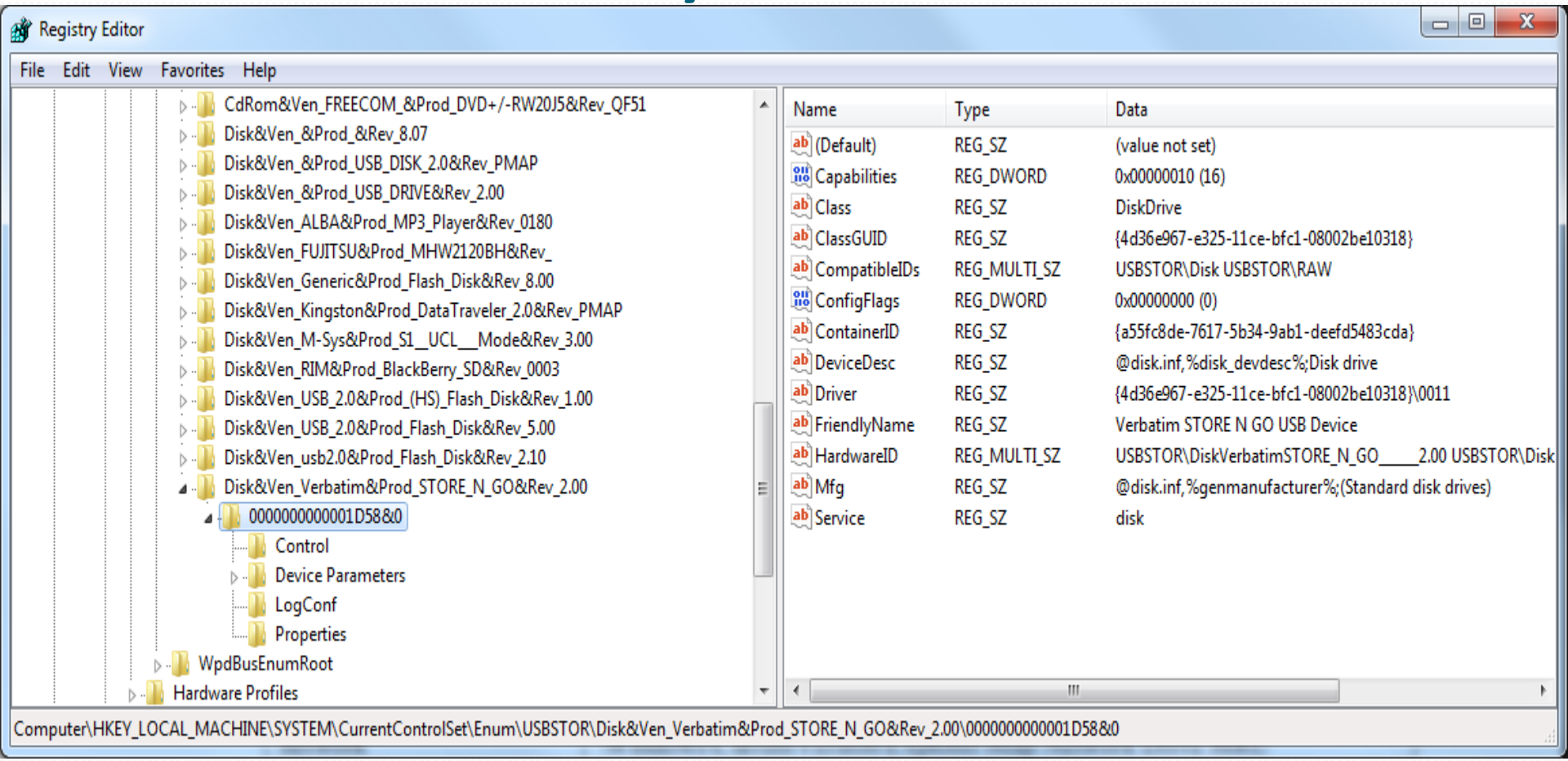
These lists are maintained in case the user returns to them in the future. Essentially, their function is similar to how the history and cookies act in a web browser.



Forensic Analysis – Last Opened Application in Windows



Forensic Analysis – USB Devices



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.

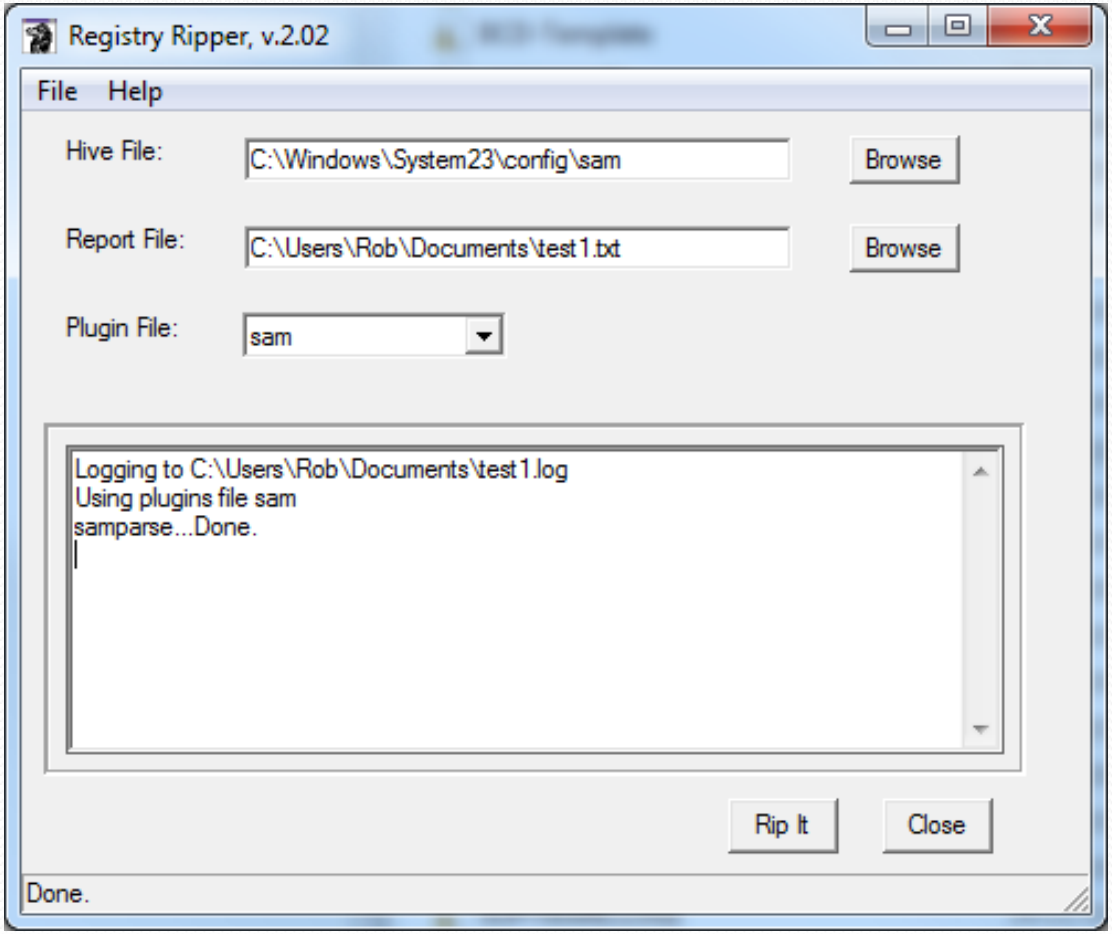
Conclusion: No evidence that company information was burned to disk. However, laptop was used to burn copyrighted material and employee had lied.

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

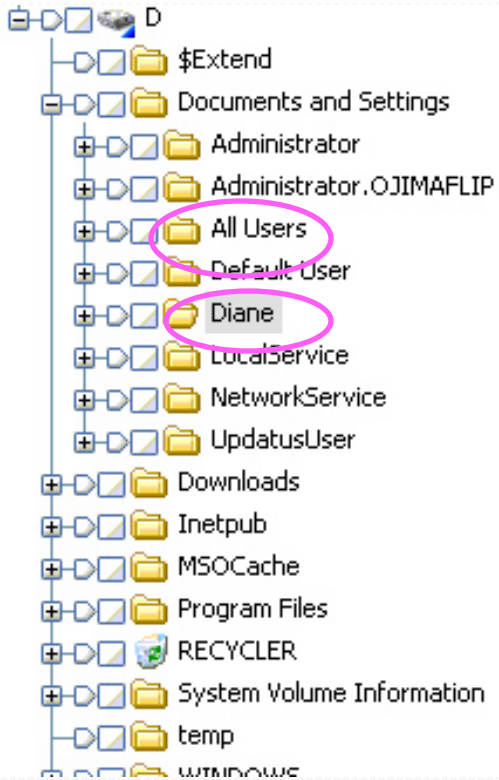
RegRipper

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.

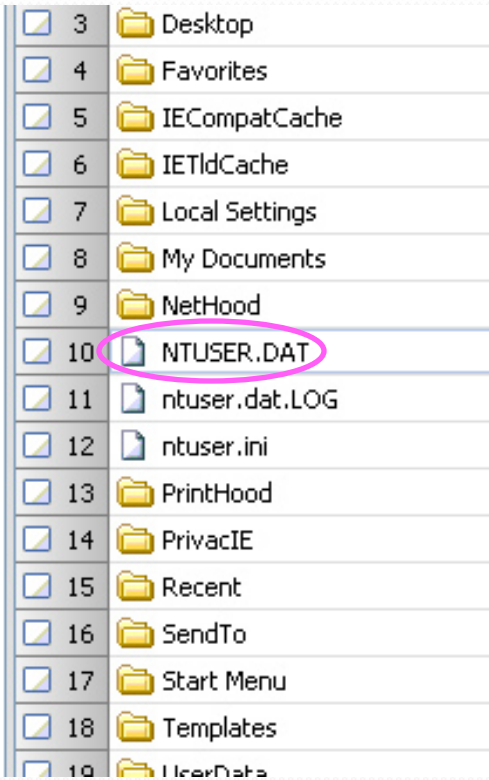


Windows 7 Registry Artifacts

- 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



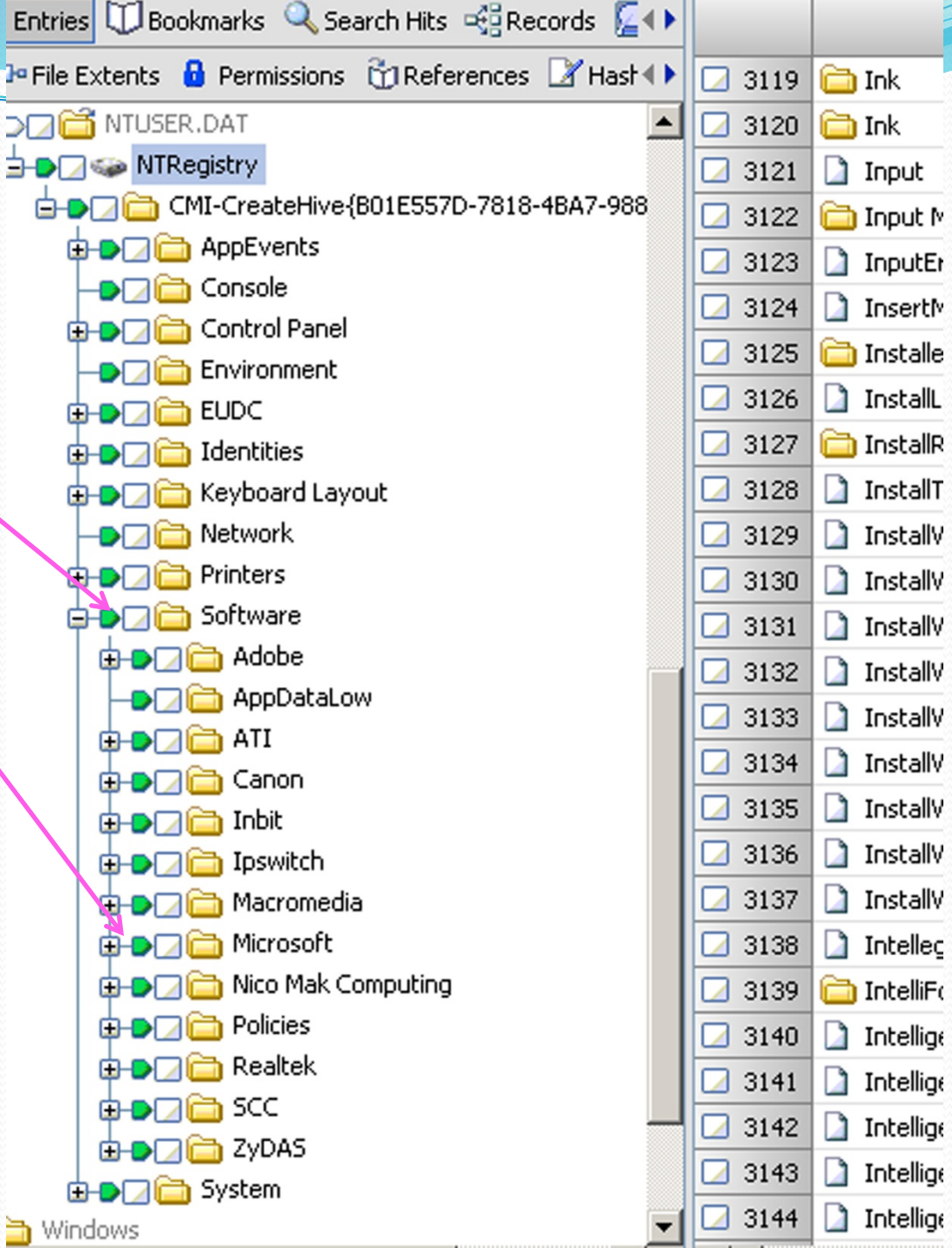
XP view



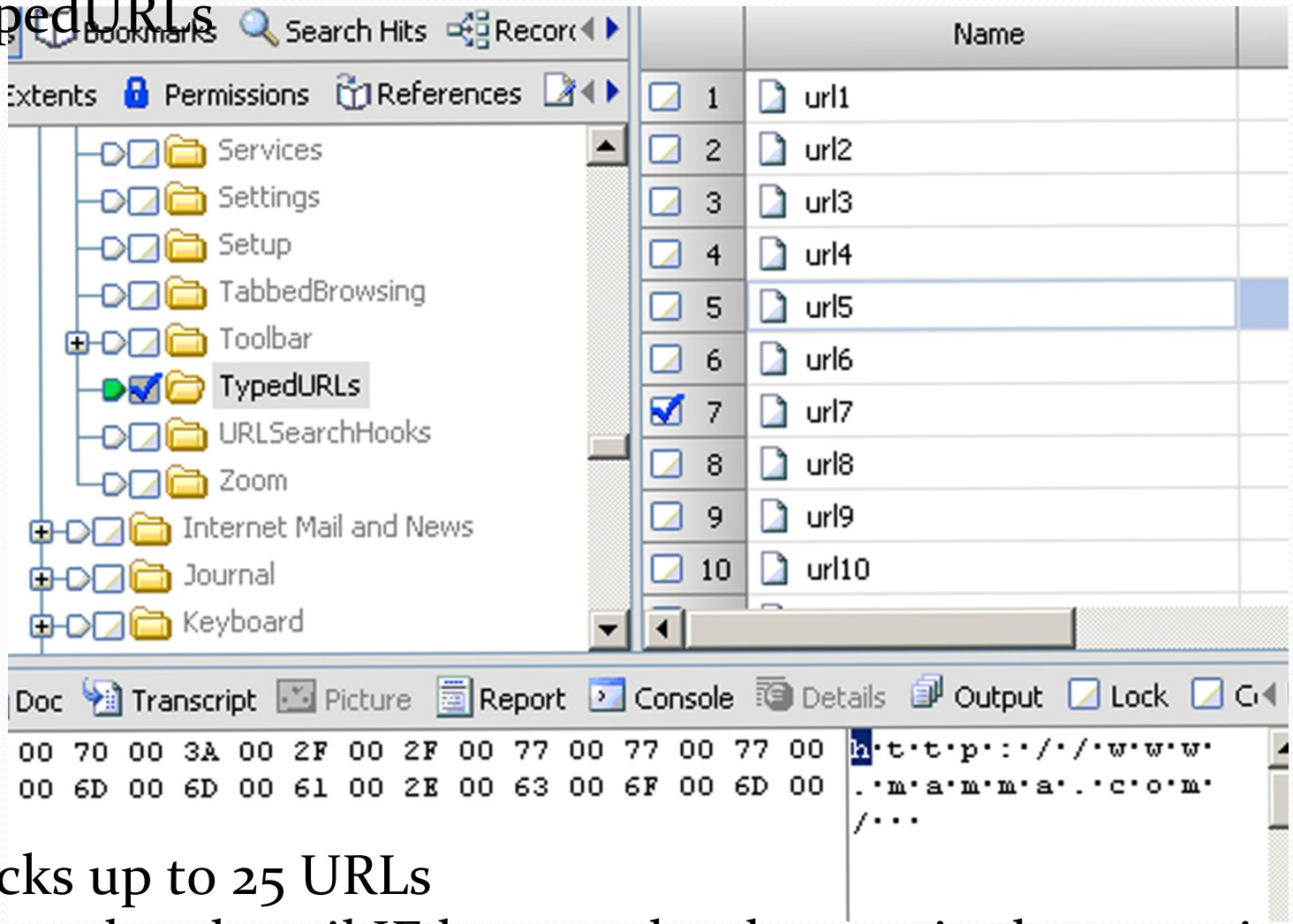
- NTUSER.DAT
- Software
- Microsoft

- 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

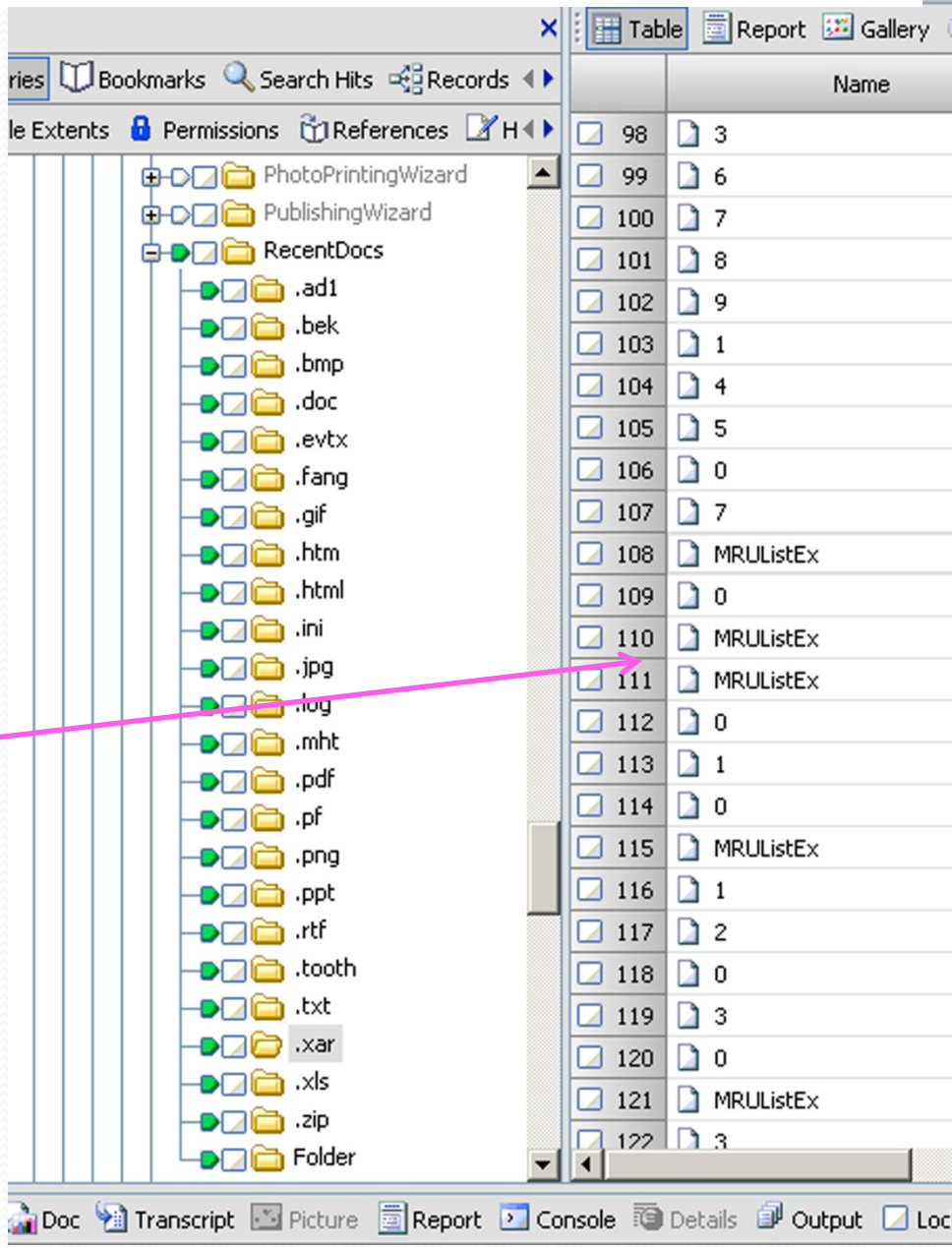


- tracks up to 25 URLs
- not updated until IE browser has been exited appropriately
- changed with IE8
- forensically important because it demonstrates user behaviour

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

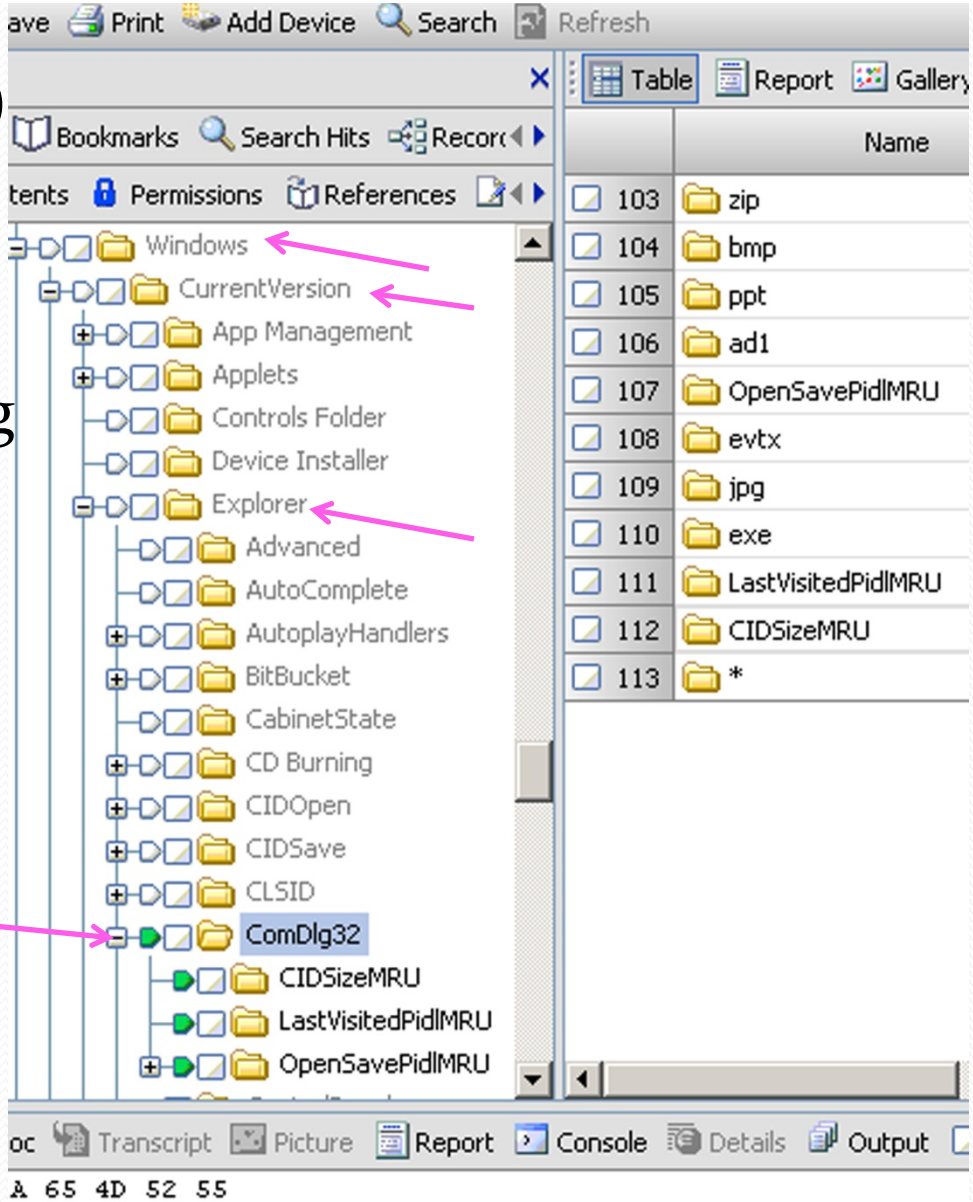
- RecentDocs
- Stored by extension
- Stores the last 10 of each extension type (0-9)
- Creates new extension subkey if new file type

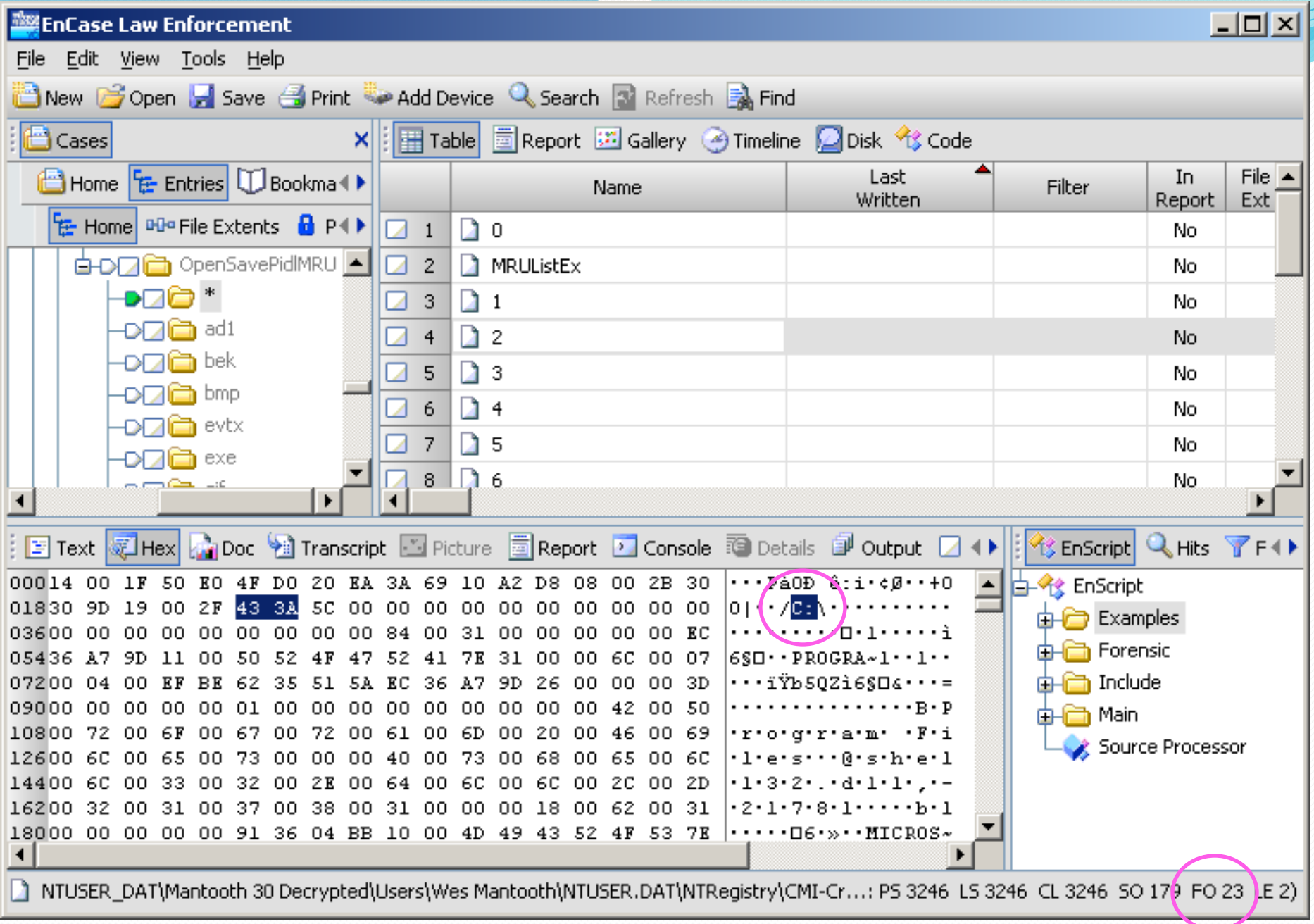
- Notice MRUListEx
- Lists chronological order of access



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

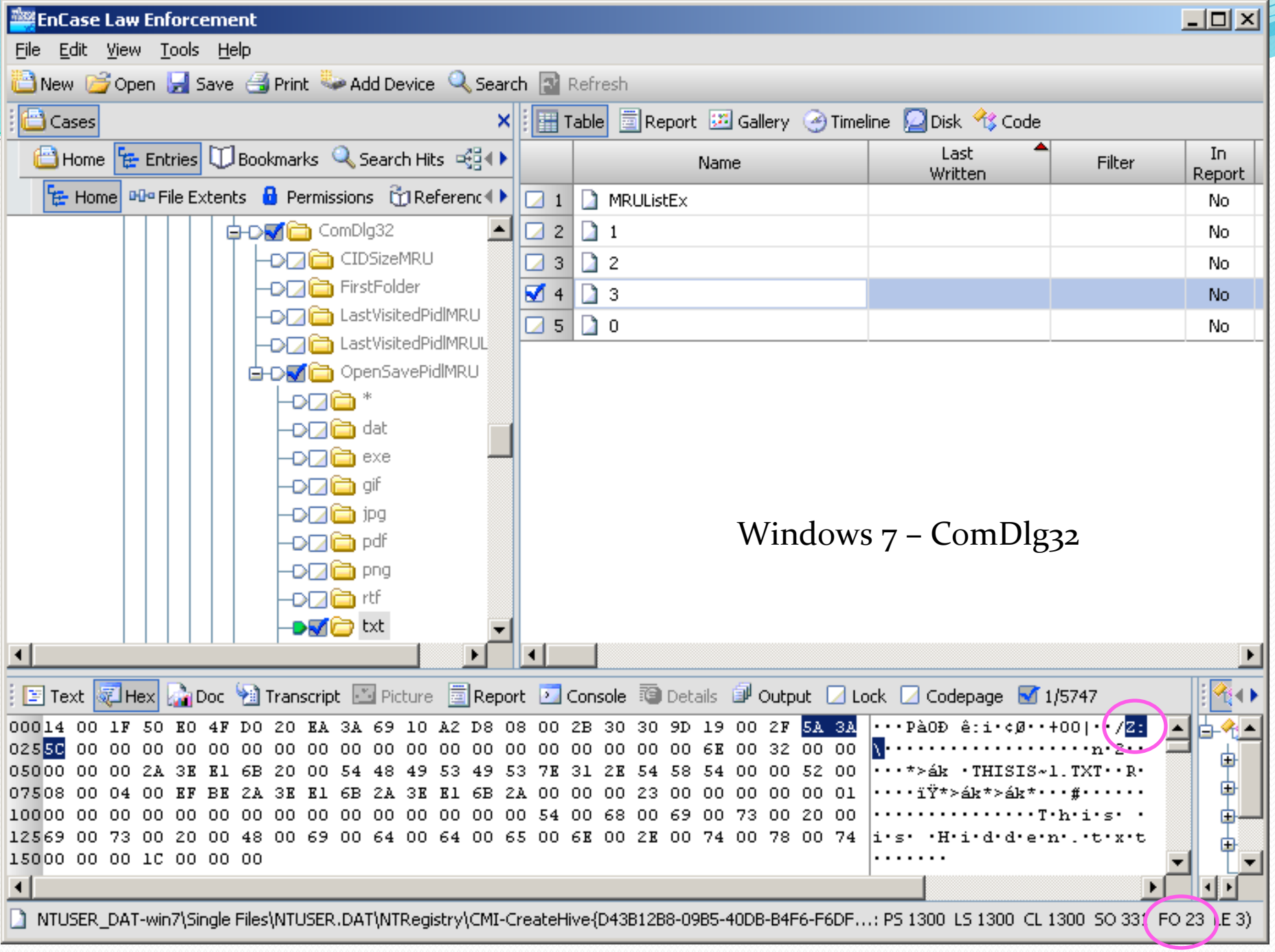
- Common Dialog (ComDlg32)
- Tracks user behaviour for Open and Save As
- Recorded here if a program uses Windows standard dialog box to access documents
- In Vista and Win 7 more binary data is stored here
- In Win 7
  - CIDSizeMRU
  - FirstFolder
  - LastVisitedPidlMRU
  - LastVisitedPidlMRULegacy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





ComDlg32

At offset 23 – you can see the drive letter



Windows 7 – ComDlg32

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 19_{10})
- 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 entires 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