
Introduction to Computer Forensics and Security

6G7Z1009

Windows Artifacts

Objectives

- Conduct efficient and effective investigations of Windows systems
- Find user data and profiles in Windows folders
- Locate system artifacts in Windows systems

Introduction

In many cases you may have gigabytes or even terabytes of data that must be searched for evidence. Maximize efficiency of the search by showing default locations of file storage.

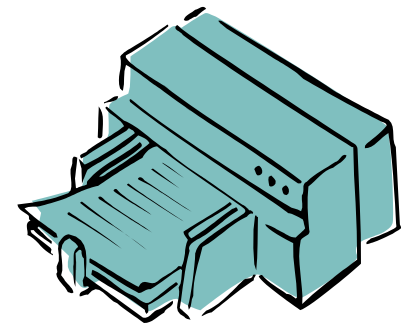


Investigating Windows Systems

- Activities of the user result in user data
 - User profiles
 - Program files
 - Temporary files (temp files)
 - Special application-level files

Investigating Windows Systems (Cont.)

- System data and artifacts are generated by the operating system
 - Metadata
 - Windows system registry
 - Event logs or log files
 - Swap files
 - Printer spool
 - Recycle Bin



Investigating Windows Systems (Cont.)

- Identify the operating systems of a target hard drive by:
 - Operating system folder names
 - The folder for the Recycle Bin
 - The construction of the user root folders because of the differences in the way user data is kept

Finding User Data and Profiles in Windows Folders

- Documents and Settings / Users folders
 - Contains a *user root folder* for each user account created on the computer
 - Windows NT and above automatically install
 - Administrator
 - All users
 - Default user (hidden)



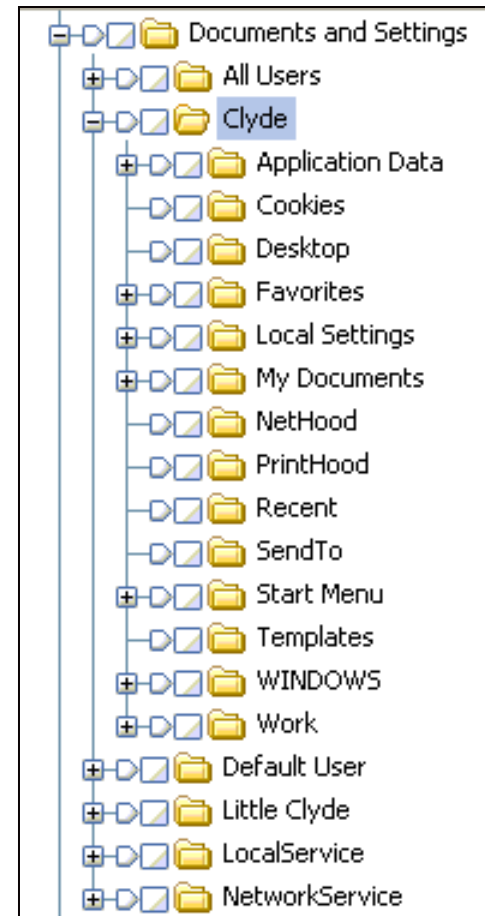
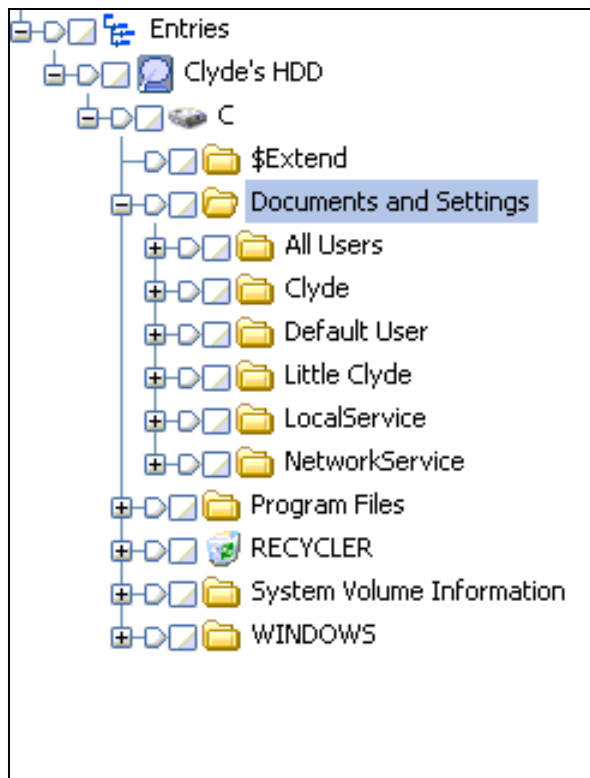
Finding User Data and Profiles in Windows Folders (Cont.)

- Data stored in the user root folder:
 - ❑ Desktop settings, such as wallpaper, screensavers, color schemes, and themes
 - ❑ Internet customizations, such as the homepage, favorites, and history
 - ❑ Application parameters and data, such as e-mail and upgrades
 - ❑ Personal files and folders, such as My Documents, My Pictures, and so on

Finding User Data and Profiles in Windows Folders (Cont.)

- Some of the subfolders in the user root folder include:
 - Application data (hidden)
 - Cookies
 - Desktop
 - Favorites
 - Local Settings (hidden)
 - My Documents
 - NetHood (hidden)

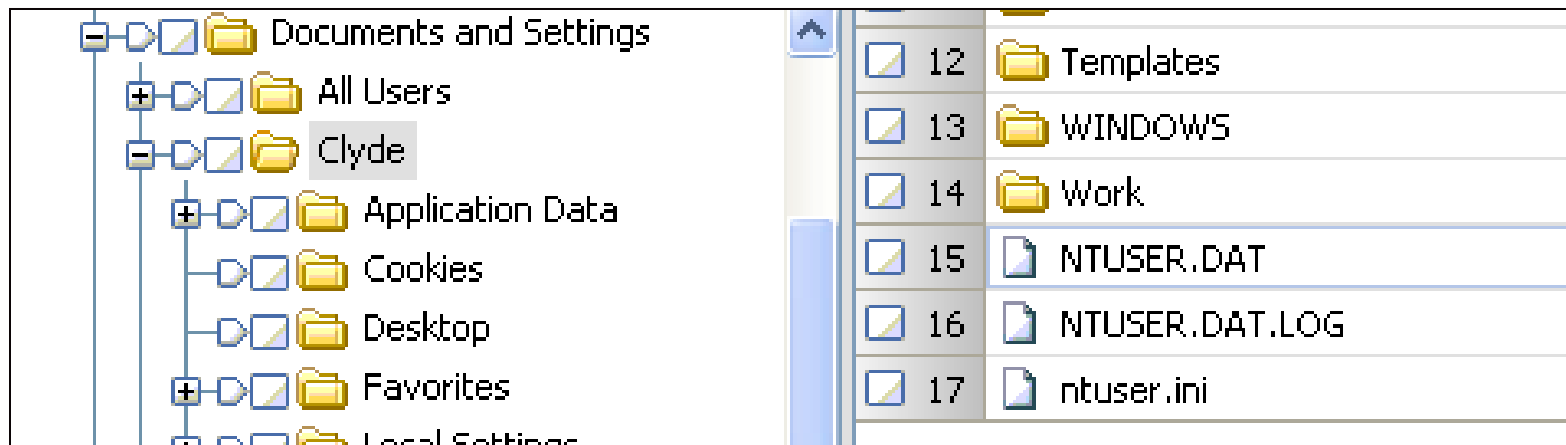
Finding User Data and Profiles in Windows Folders (Cont.)



Location of User Root Folders

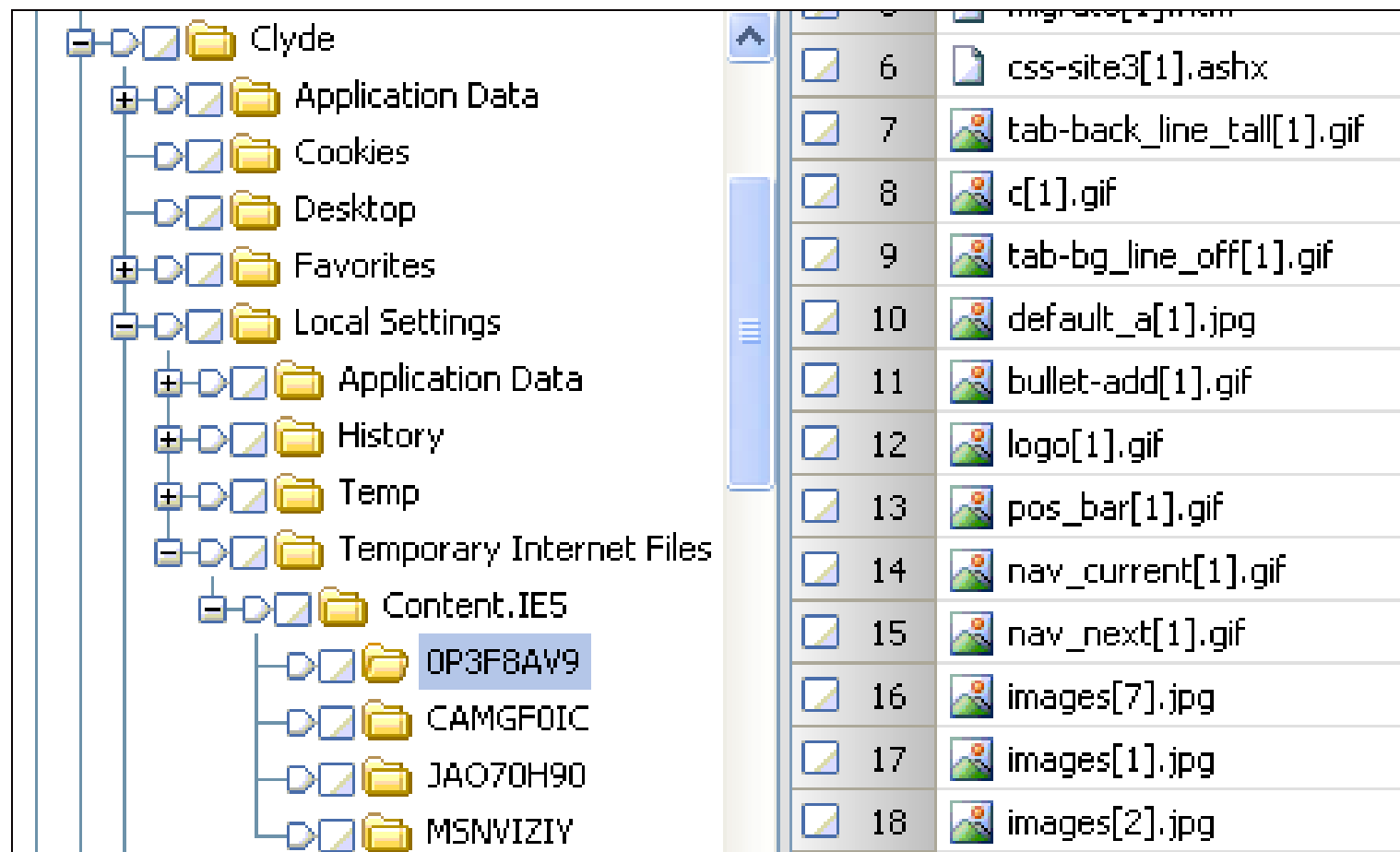
Operating System (Platform)	User Root Folder	Location
Windows 9x	<partition>:\WINDOWS\Profiles\userid	USER.DAT file
Windows NT	<partition>:\WINNT\Profiles\userid	NTUSER.DAT file
Windows 2000 and Windows XP	<partition>:\Documents and Settings\userid	NTUSER.DAT file
Windows 7	<partition>:\Users\userid	?

Location of User Root Folders



In Practice: Temp Internet Files Provide Valuable E-Evidence

Next Term



Investigating System Artifacts

■ Types of metadata

- ❑ Descriptive: describes a resource for purposes such as discovery and identification
- ❑ Structural: indicates how compound objects are put together
- ❑ Administrative: provides information to help manage a resource, such as when it was created, last accessed, and modified

Investigating System Artifacts

(Cont.)

■ Registry

- ❑ Can reveal current and past applications, as well as programs that start automatically at bootup
- ❑ Viewing the registry requires a registry editor

■ Event logs track system events

- ❑ Application log tracks application events
- ❑ Security log shows logon attempts
- ❑ System log tracks events such as driver failures

Investigating System Artifacts (Cont.)

■ Swap file/page file

- Used by the system as virtual memory
- Can provide the investigator with a snapshot of volatile memory

■ Print spool

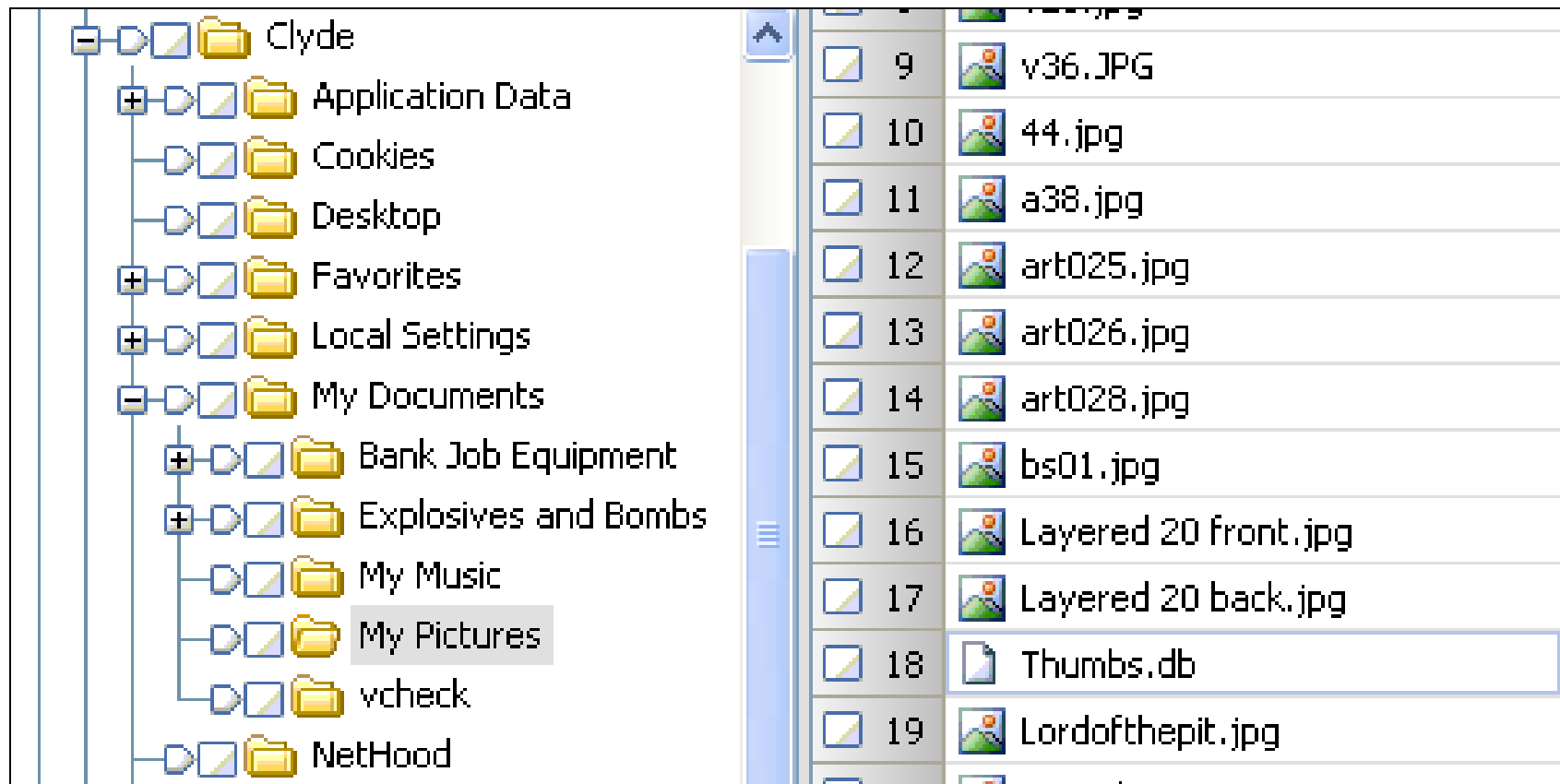
- May contain enhanced metafiles of print jobs

■ Recycle Bin/Recycler

- Stores files the user has deleted

Investigating System Artifacts

(Cont.) - Thumbs.DB



Investigating System Artifacts

(Cont.) - Print spool

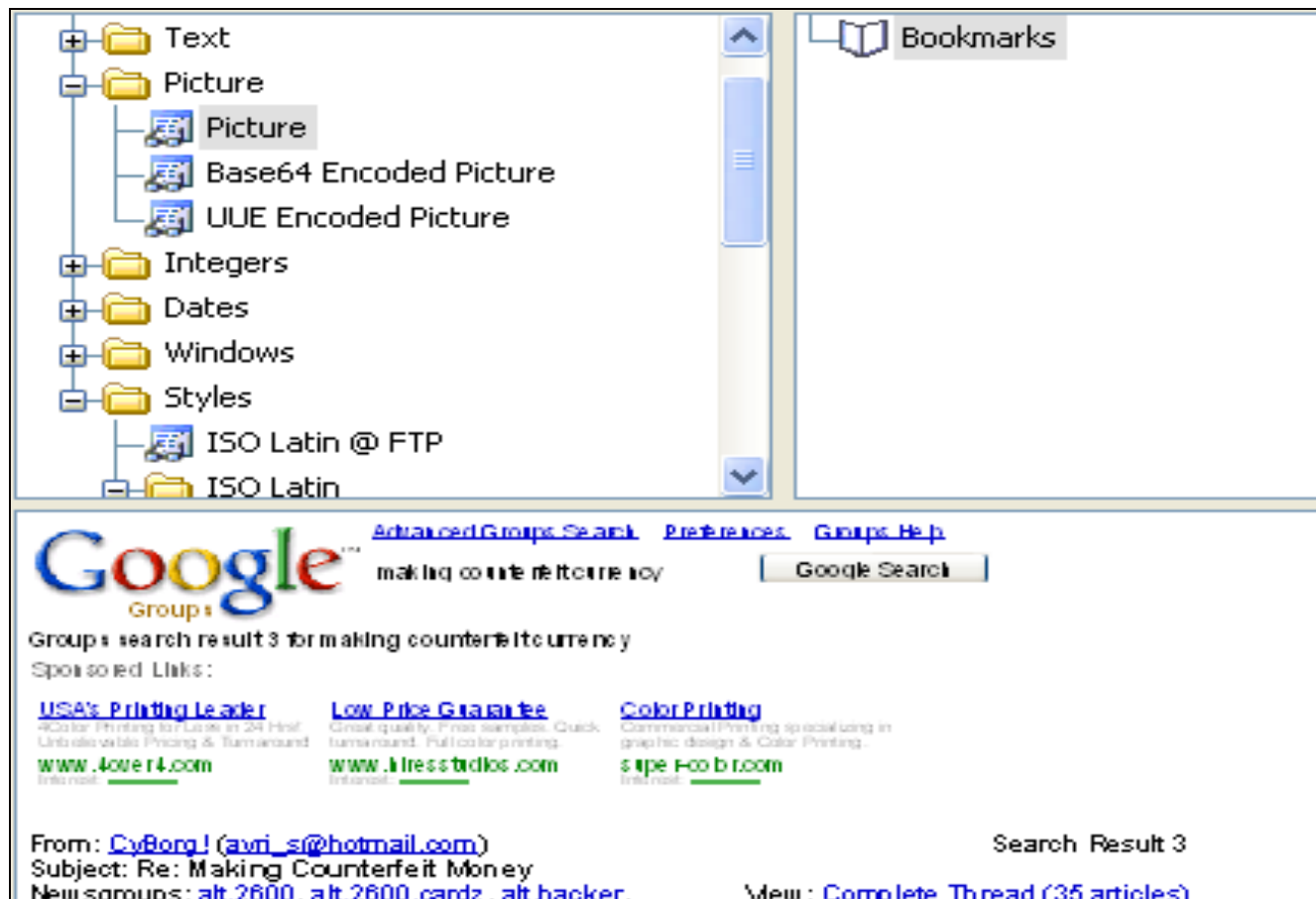
The screenshot displays a file explorer interface. The left pane shows a tree view with folders: spool, drivers, PRINTERS, prtprocs, and System84. The right pane shows a list of files: FP00001.SPL, FP00001.SH, FP00002.SPL, FP00002.SH, FP00004.SPL, FP00004.SH, FP00003.SPL, and FP00003.SH. The bottom pane shows a hex dump of a file, with a selection of 41 bytes highlighted in blue. A red box with an arrow points to the selection and contains the text "Select 41 bytes".

000000h.t.t.p.:././g.r.o.u.p.s..g.o.o.g.l.e..c.o.m./g.r.o.u.p.s.?
000080 q'=m.a.k.i.n.g.+c.o.u.n.t.e.r.f.e.i.t.+c.u.r.r.e.n.c.y.&h.....T+...
000160L0...g...EMF...T÷...l.....x...l.....À...□...È...
000240(...P.r.i.n.t...t.e.s.t...□□ConvertEmfToWmf.m.f.3.2.1.6...□□\f.
000320 o.n.t.s...□□\s.y.s.t.e.m...P.i.e.o□□Ñ.□"..'q* ÿ..ä□Ñ.□á. É.)"O.ôÝ
000385 iD.®¶.².À□>á□¥.¶pD.□□.².»j@+±¥]Ñ.□İ.À□Ñ.À.ÖiçID.□□.².»jÁ.ÖiçID.□□.².»j/k@Z
000465 >Ñ.¶@.².;ùjÀ.ÖiçID.□□.².»j□□□□.....□%.....□%.....□.....

Select 41 bytes

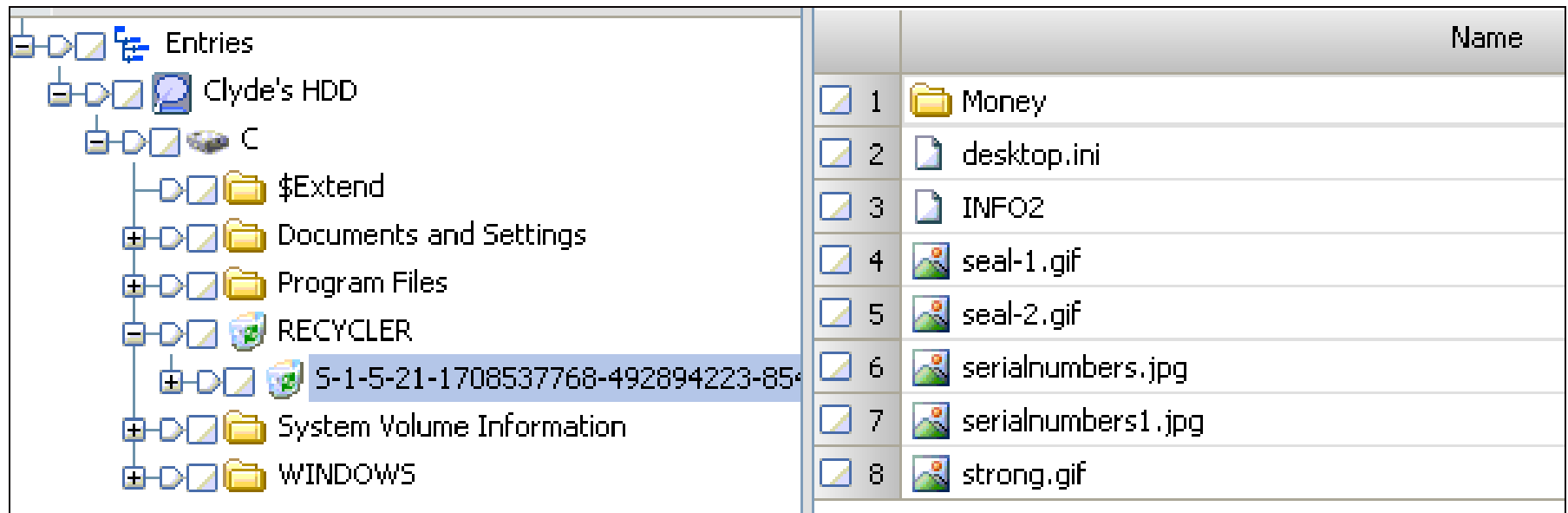
Investigating System Artifacts

(Cont.) - Print spool



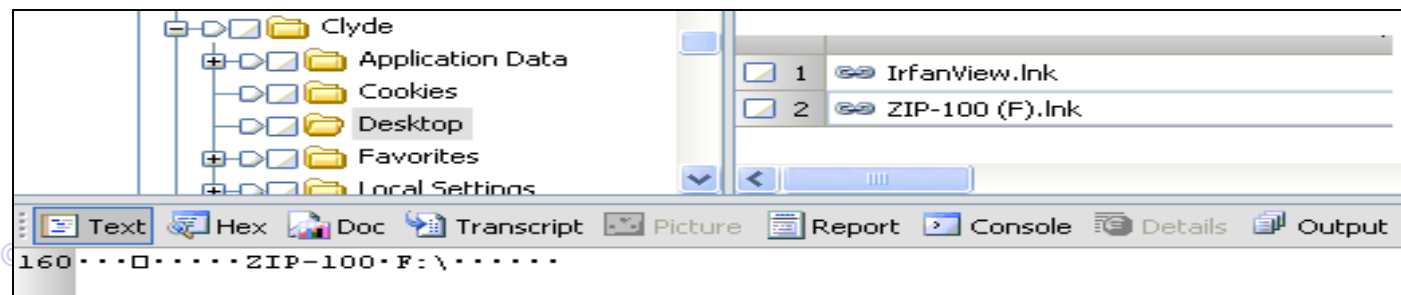
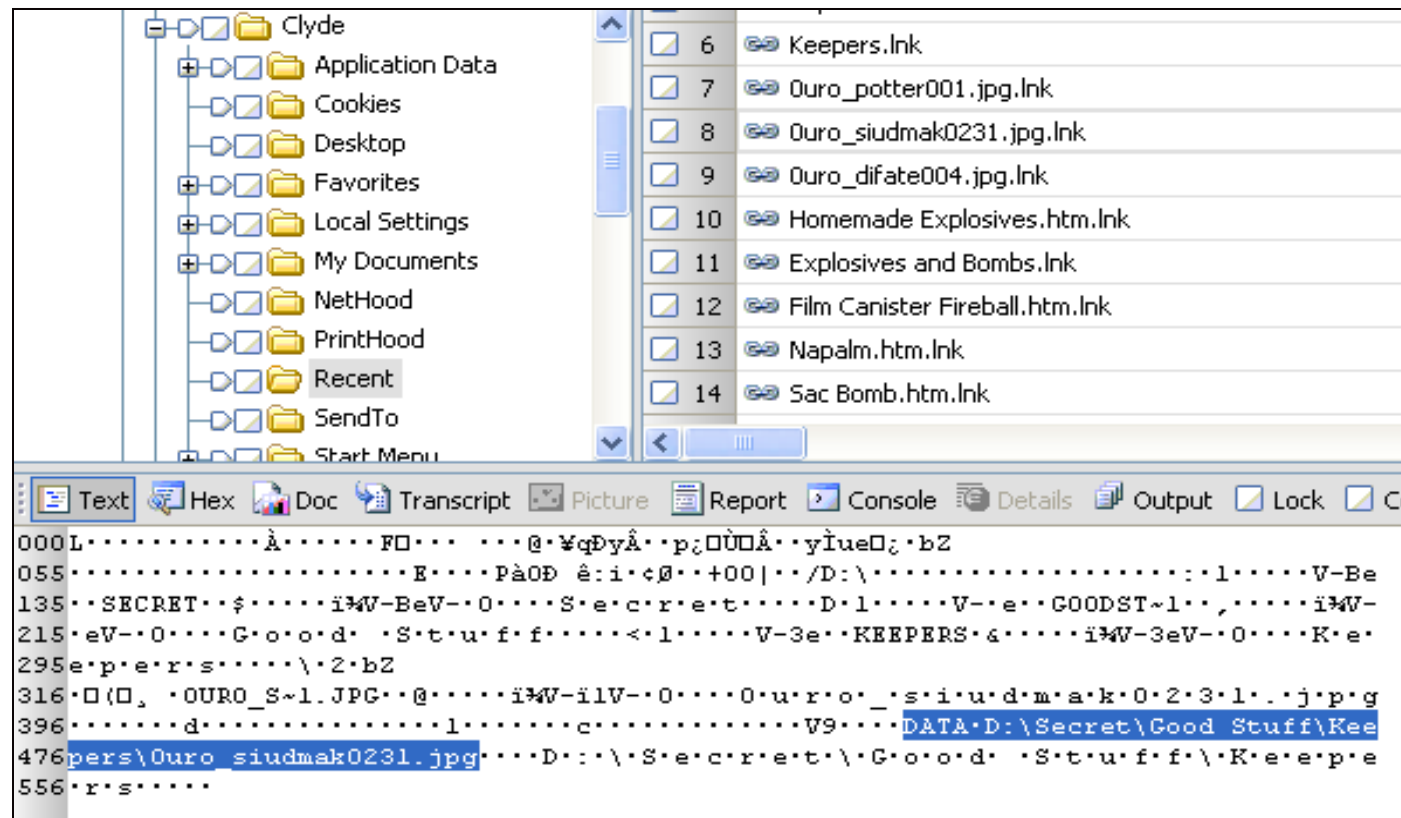
Investigating System Artifacts

(Cont.) - Recycle Bin/Recycler



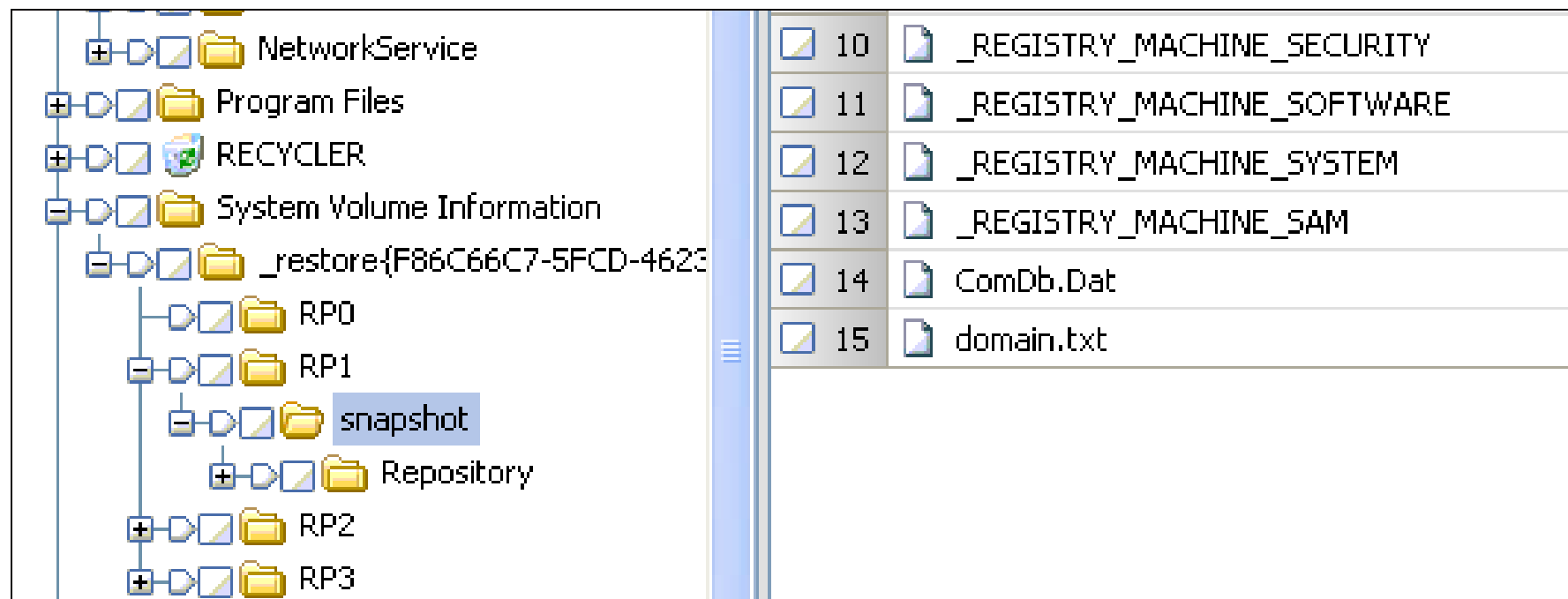
Investigating System Artifacts

(Cont.) – link files & recent used files



Investigating System Artifacts

(Cont.) – Store points



The screenshot displays a Windows Explorer window. The left pane shows the folder hierarchy: NetworkService, Program Files, RECYCLER, and System Volume Information. Under System Volume Information, the folder _restore{F86C66C7-5FCD-4623} is expanded, showing subfolders RP0, RP1, RP2, and RP3. The RP1 folder is further expanded, showing a 'snapshot' folder and a 'Repository' folder. The right pane shows a list of files, including _REGISTRY_MACHINE_SECURITY, _REGISTRY_MACHINE_SOFTWARE, _REGISTRY_MACHINE_SYSTEM, _REGISTRY_MACHINE_SAM, ComDb.Dat, and domain.txt.

Index	File Name
10	_REGISTRY_MACHINE_SECURITY
11	_REGISTRY_MACHINE_SOFTWARE
12	_REGISTRY_MACHINE_SYSTEM
13	_REGISTRY_MACHINE_SAM
14	ComDb.Dat
15	domain.txt

Investigating System Artifacts

(Cont.) – Logs

Windows NT, 2000, XP maintain log files

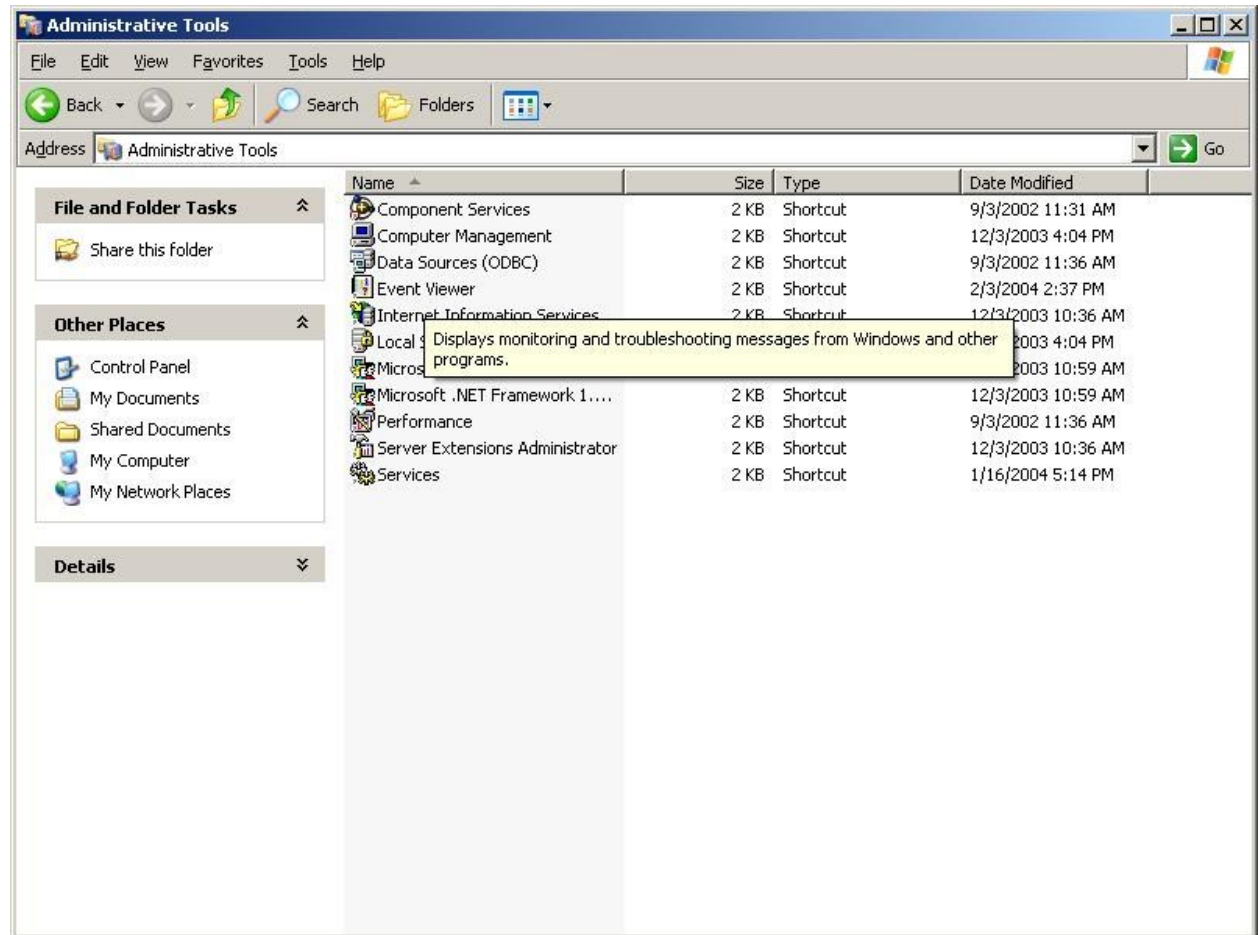
- System Log
- Application Log
- Security Log

Investigating System Artifacts

(Cont.) – Logs

Live System:

- Use Event Viewer



Investigating System Artifacts (Cont.) – Logs Event Viewer

■ Event Viewer

Type	Date	Time	Source	Category	Event	User	Computer
Information	2/3/2004	1:32:33 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	1:21:16 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	1:21:16 PM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/3/2004	1:00:05 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:57:07 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:42:38 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:42:38 PM	Removable Storage Se...	None	98	N/A	BOBADILLA
Information	2/3/2004	12:40:35 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:40:35 PM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/3/2004	12:40:34 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:40:34 PM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/3/2004	12:40:33 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:40:33 PM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/3/2004	12:40:33 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:40:33 PM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/3/2004	12:39:11 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:39:11 PM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/3/2004	12:33:30 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:22:44 PM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	12:22:44 PM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Warning	2/3/2004	10:01:44 ...	W32Time	None	36	N/A	BOBADILLA
Error	2/3/2004	7:43:29 AM	MrxSmb	None	8003	N/A	BOBADILLA
Information	2/3/2004	3:23:54 AM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	3:23:54 AM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/3/2004	3:23:46 AM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	3:23:42 AM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/3/2004	3:23:24 AM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	3:23:24 AM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/3/2004	3:23:24 AM	Service Control Manager	None	7036	N/A	BOBADILLA
Information	2/3/2004	3:23:24 AM	Service Control Manager	None	7035	SYSTEM	BOBADILLA
Information	2/2/2004	9:14:30 PM	Application Popup	None	26	N/A	BOBADILLA
Information	2/2/2004	8:39:10 PM	Application Popup	None	26	N/A	BOBADILLA

Investigating System Artifacts

(Cont.) – Logs from forensics duplicate
(Windows/System32/Config/)

- SecEvent.evtx
- AppEvent.evtx
- SysEvent.evtx

Investigating System Artifacts

(Cont.) – \$ Logfile

- \$Logfile entry in the MFT contains the log of all file system transactions
- Deletion of a file leaves several entries in \$Logfile
- Not unusual to find files that are no longer on the disk
- Shows that file was used by the system

Investigating System Artifacts

(Cont.) – Temporary Files

- Temporary files
 - Files with extension tmp
 - Created by many applications
- Emails with large attachments:
 - Attachments are probably stored as temp files.
(Depends on email system.)
- Look for file extensions .tmp

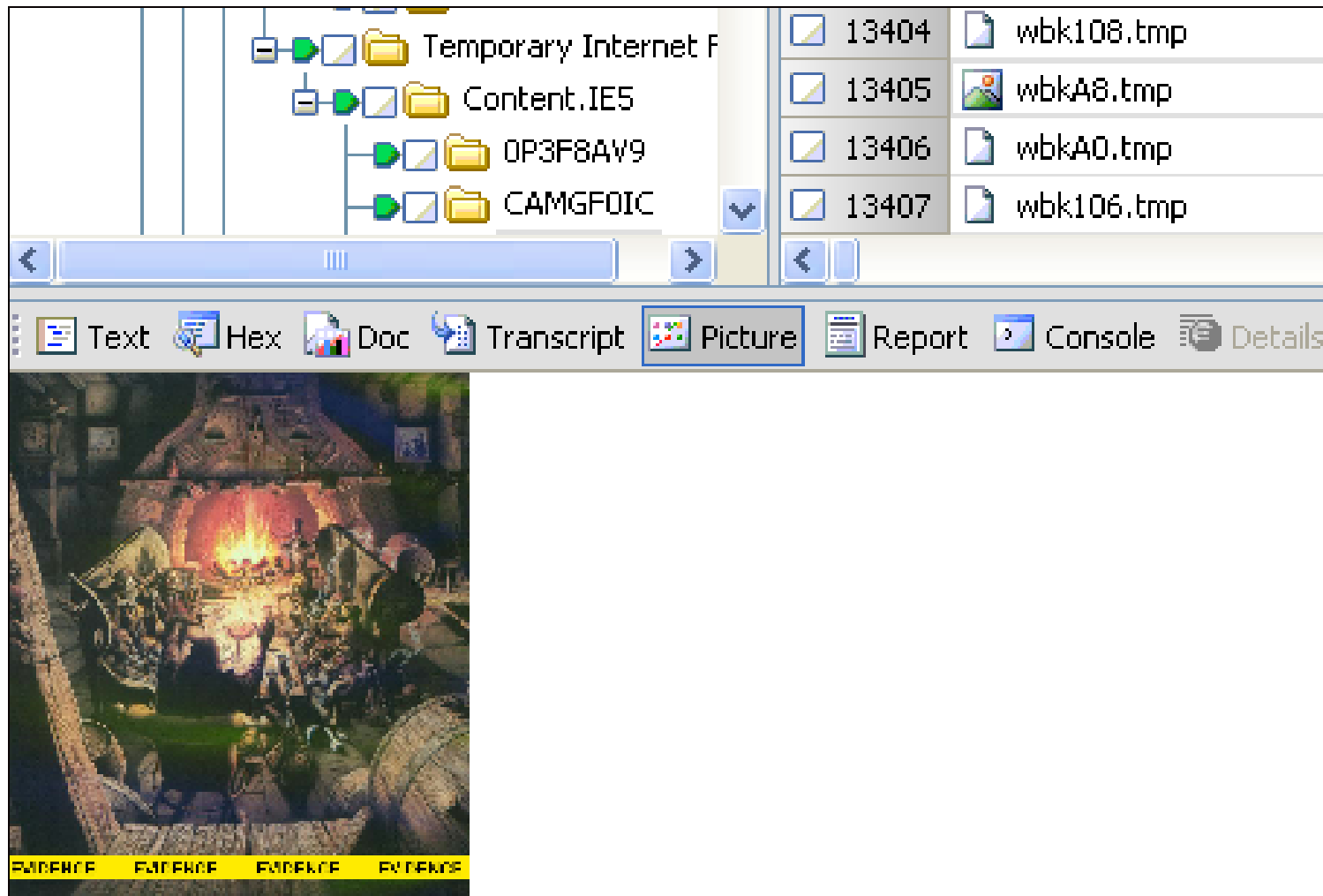
Investigating System Artifacts

(Cont.) – Internet Explorer

- Internet Explorer (as well as other browsers) use a cache.
- index.dat contains internet explorer cached websites.

Investigating System Artifacts

(Cont.) – Temporary Files



Investigating System Artifacts

(Cont.) - Recycle Bin/Recycler

Entries		Name
Clyde's HDD		
C		
\$Extend		
Documents and Settings		
Program Files		
RECYCLER		
S-1-5-21-1708537768-492894223-854		
System Volume Information		
WINDOWS		
1	Money	
2	desktop.ini	
3	INFO2	
4	seal-1.gif	
5	seal-2.gif	
6	serialnumbers.jpg	
7	serialnumbers1.jpg	
8	strong.gif	

Investigating System Artifacts

(Cont.) – Swap Files

- Windows 2000 & WinXP
 - Pagefile.sys
- Windows 98
 - Win386.swp

Investigating System Artifacts

(Cont.) - Registry

- Database that stores settings and options for 32b MSWin OS
- Contains information and setting for
 - Hardware
 - Software
 - Users
 - Preferences

Investigating System Artifacts (Cont.) - Registry

- Registry contains information about
 - ❑ Usernames and passwords for programs, e-mail, and Internet sites
 - ❑ A history of Internet sites accessed, including date and time
 - ❑ A record of Internet queries (i.e., searches performed on Internet search engines like Google*, Yahoo*, etc.)
 - ❑ Lists of recently accessed files (e.g., documents, images, etc.)
 - ❑ A list of all programs installed on the system

Investigating System Artifacts

(Cont.) - Registry

Win95, Win98

- USER.DAT, SYSTEM.DAT in Windows

WinME

- USER.DAT, SYSTEM.DAT, CLASSES.DAT

WinNT, 2000, XP

- In %SystemRoot%\System32\Config

Win vista / 7 / 8

- .DAT files

Investigating System Artifacts (Cont.) – Registry – Win XP

Filename	Location	Purpose
ntuser.dat	\Document and Settings\ <i>user account</i>	<ul style="list-style-type: none">■ Protected storage for this user■ Most Recently Used list of files (MRU)
Default	\Windows\system32\config	System settings
SAM	\Windows\system32\config	User account management and security information
Security	\Windows\system32\config	Security settings
Software	\Windows\system32\config	All installed programs, their settings, any associated usernames and passwords
System	\Windows\system32\config	System settings

Investigating System Artifacts

(Cont.) - Registry

- Use RegEdit to access.
- Before experimentation, make a backup of the registry.



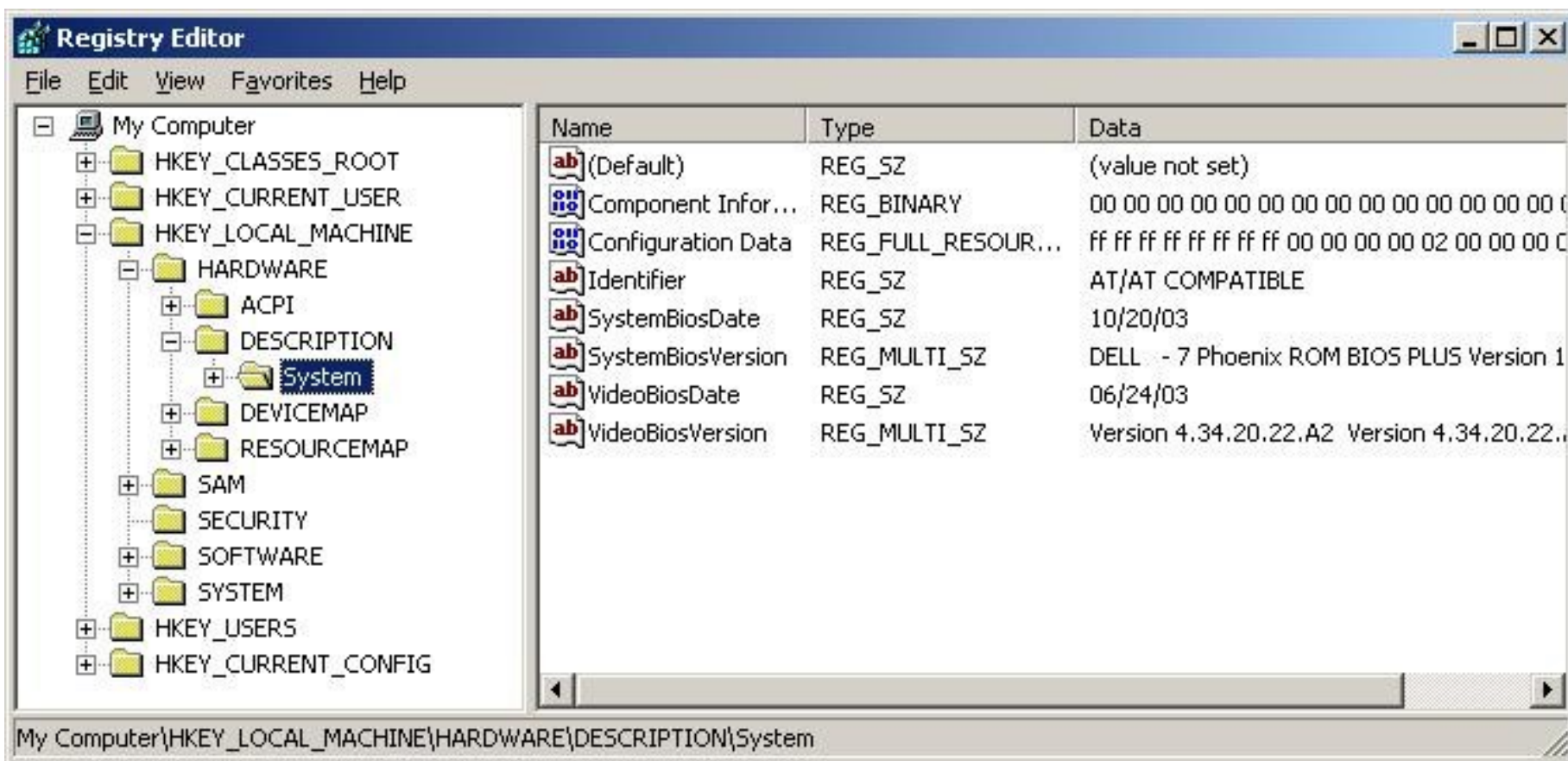
Investigating System Artifacts

(Cont.) – Registry Structure

- Hierarchical structure
- Main branches are Hives
- Hives contain keys.
- Keys can contain subkeys and values

Investigating System Artifacts

(Cont.) - Registry



Investigating System Artifacts

(Cont.) - Registry

- Six main branches
 - **HKEY_CLASSES_ROOT** - This branch contains all of your file association mappings to support the drag-and-drop feature, OLE information, Windows shortcuts, and core aspects of the Windows user interface.
 - **HKEY_CURRENT_USER** - This branch links to the section of HKEY_USERS appropriate for the user currently logged onto the PC and contains information such as logon names, desktop settings, and Start menu settings.

Investigating System Artifacts

(Cont.) - Registry

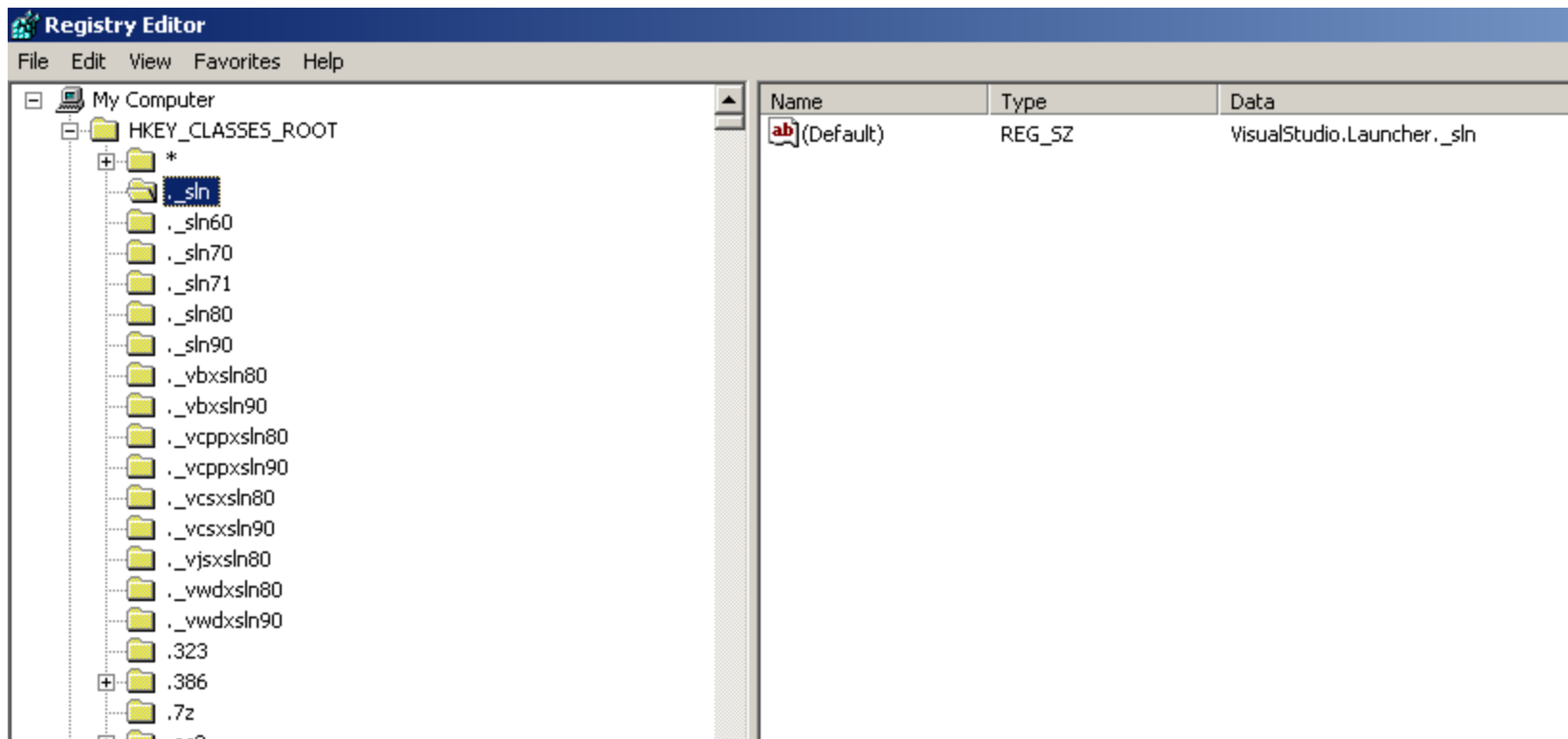
- ❑ **HKEY_LOCAL_MACHINE** - This branch contains computer specific information about the type of hardware, software, and other preferences on a given PC, this information is used for all users who log onto this computer.
- ❑ **HKEY_USERS** - This branch contains individual preferences for each user of the computer, each user is represented by a SID sub-key located under the main branch.

Investigating System Artifacts

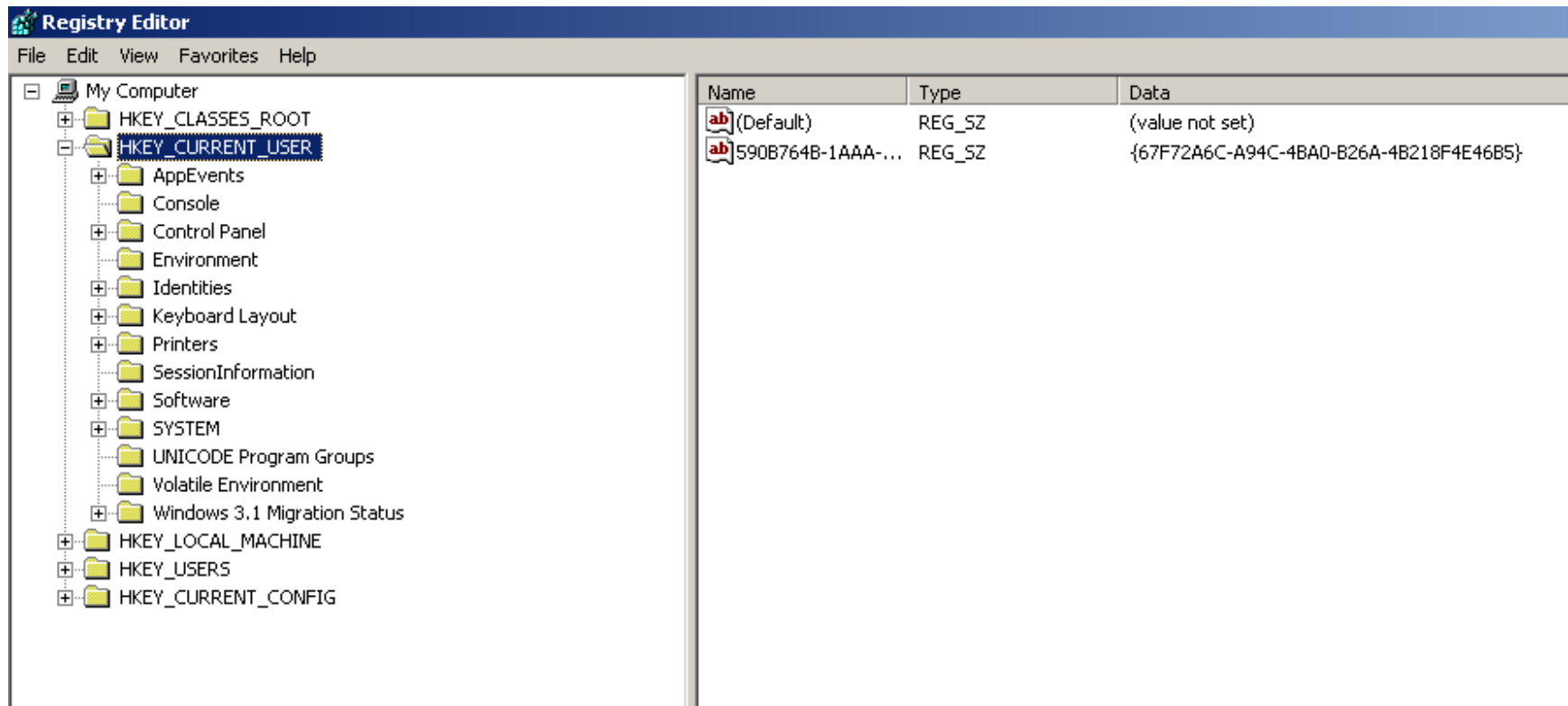
(Cont.) - Registry

- ❑ **HKEY_CURRENT_CONFIG** - links to the section of HKEY_LOCAL_MACHINE appropriate for the current hardware configuration.
- ❑ **HKEY_DYN_DATA** - points to the part of HKEY_LOCAL_MACHINE, for use with the Plug-&Play features of Windows, this section is dynamic and will change as devices are added and removed from the system.

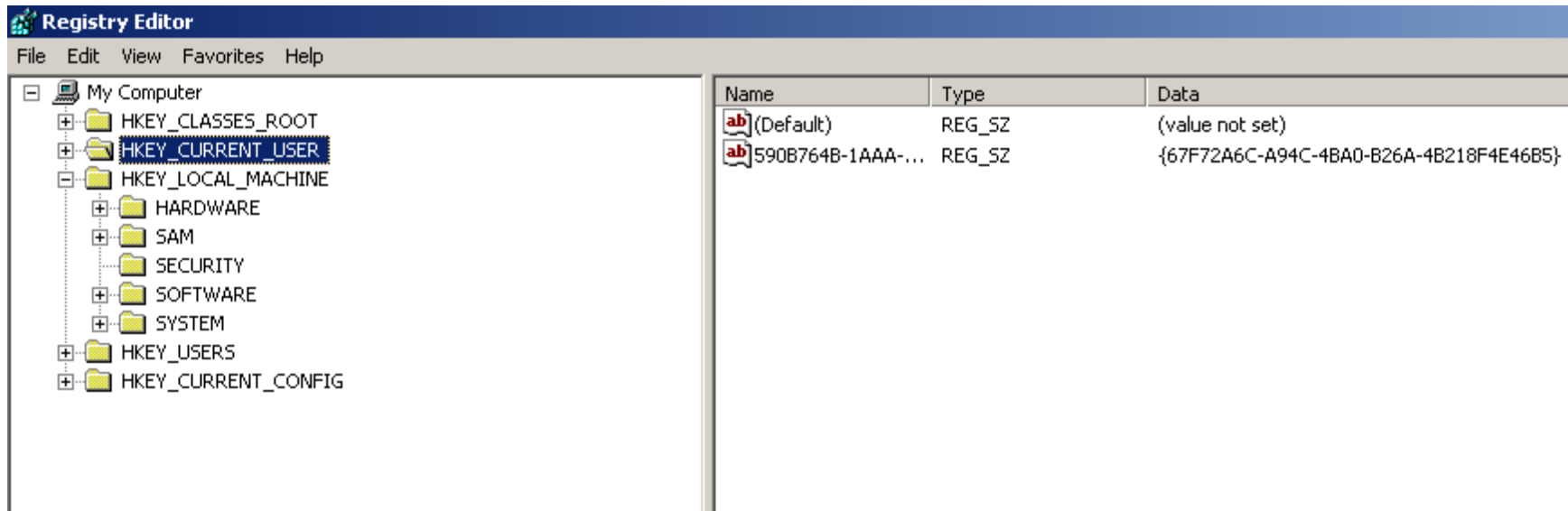
Investigating System Artifacts (Cont.) – Registry - Classes



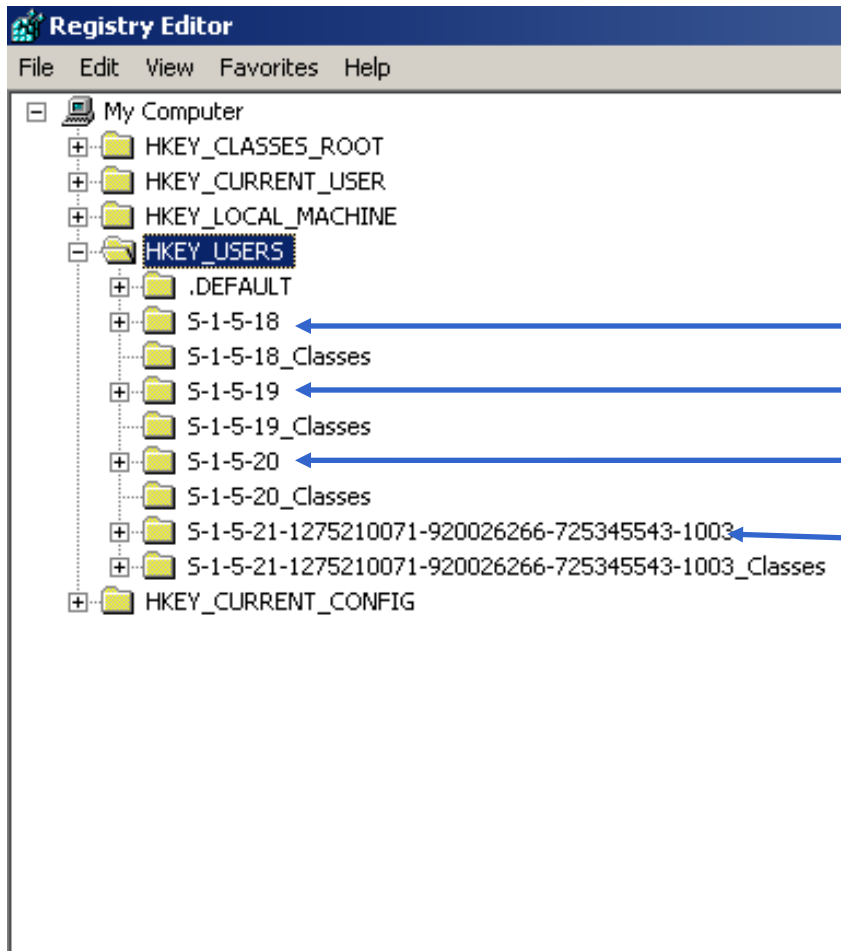
Investigating System Artifacts (Cont.) – Registry – Current User



Investigating System Artifacts (Cont.) – Registry – Local Machine



Investigating System Artifacts (Cont.) – Registry – Documents and Settings Folder Users



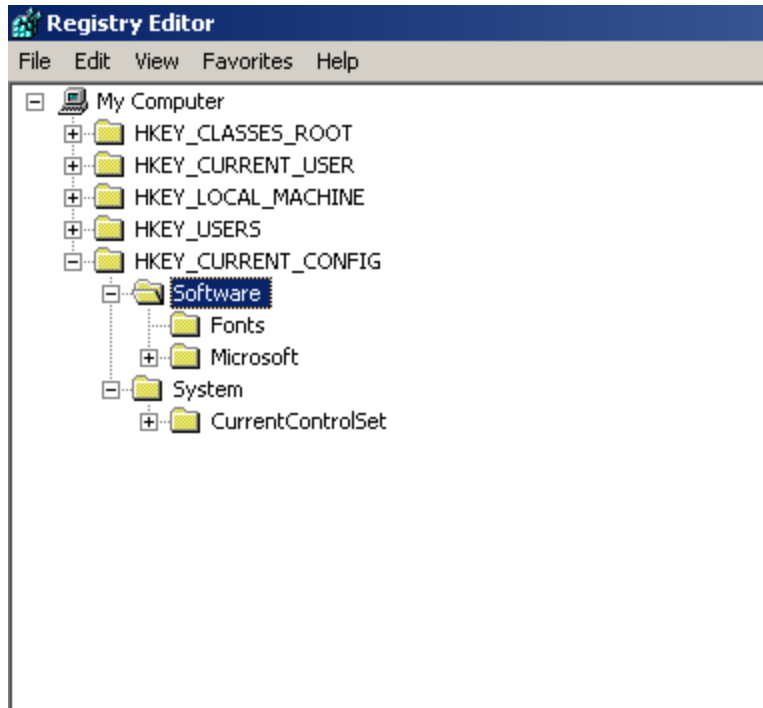
Local System (Default)

Local Service (NTUSER.DAT)

Network Service (NTUSER.DAT)

User 1 (NTUSER.DAT)

Investigating System Artifacts (Cont.) – Registry – Current Config



Investigating System Artifacts

(Cont.) - Registry

- Registry Editor can import and export registry settings to / from a text file.
- Copy registry hive files from the forensic duplicate to your forensic work station.
- Import them into regedit.

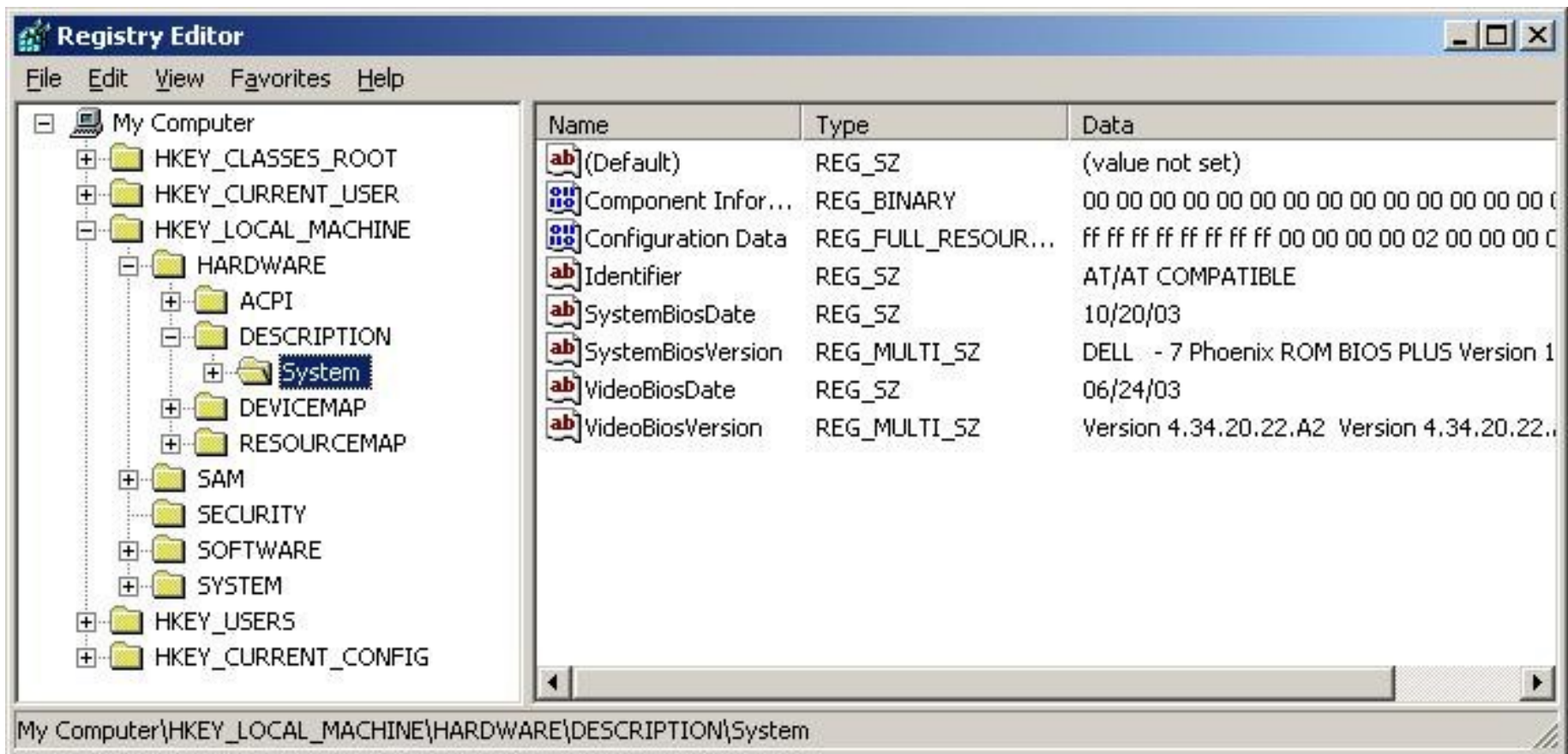
Investigating System Artifacts

(Cont.) - Registry

- Use the registry to
 - ❑ obtain listing of applications that are set to run automatically
 - ❑ obtain registry entries that have been modified lately
 - ❑ User accounts

Investigating System Artifacts

(Cont.) – Registry - Data types



Windows Registry Data Types

- REG_BINARY

- Raw binary data displayed in hex format

- REG_DWORD

- 4-byte (32-bit) integer
 - REG_DWORD_LITTLE_ENDIAN
 - Least significant byte at lowest address
 - REG_DWORD_BIG_ENDIAN
 - Least significant byte at highest address

Windows Registry Data Types

- REG_EXPAND_SZ
 - Variable-length string
- REG_MULTI_SZ
 - Multiple string
 - Values that contain lists
 - Entries usually separated by spaces, commas, or other marks

Windows Registry Data Types

- REG_SZ
 - Fixed-length text string
- REG_NONE
 - Data with no particular type
- REG_LINK
 - Unicode string naming a symbolic link
- REG_QWORD
 - 64-bit integer

Windows Registry Data Types

■ REG_RESOURCE_LIST

- ❑ Nested array
- ❑ Designed to store a resource list used by a device driver

■ REG_RESOURCE_REQUIREMENTS_LIST

- ❑ Nested array
- ❑ Designed to store a device driver's list of possible hardware resources

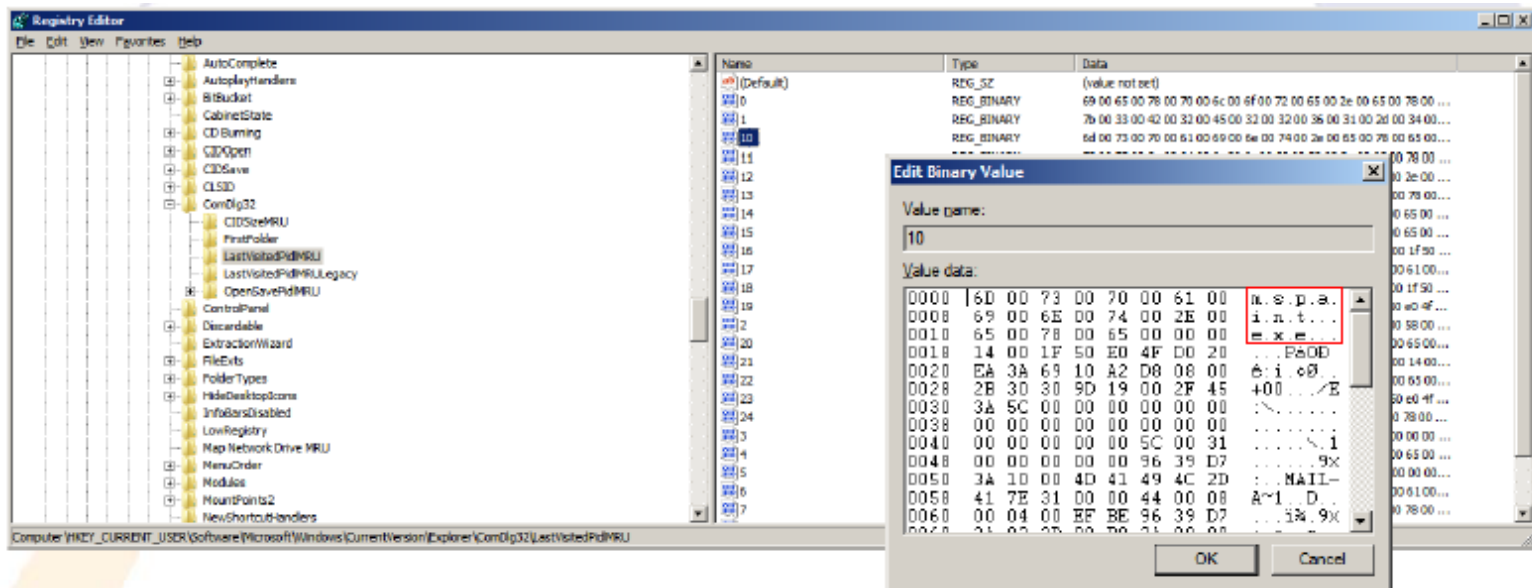
Windows Registry Data Types

- REG_FULL_RESOURCE_DESCRIPTOR
 - Nested array
 - Stores a resources list used by a physical hardware device

Used Files

- These are usually stored within the registry
 - Old windows versions: INI-files in windows/program directory
- Common lists include:
 - Start menu: HKCU
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
 - » Equivalent of %USERPROFILE%\Recent
="My Recent Documents"
 - » Includes both local and network files!
 - Run box: HKCU
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
 - » In order of most recently added (not: Used)!
 - Files (Common dialog box): HKCU\Software
Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
 - Typed URLs in IE: HKCU
Software\Microsoft\InternetExplorer\TypedURLs

Last Opened Application



- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidMRU (<Vista: LastVisitedMRU)
 - Applications last used to access the files listed in OpenSavePidMRU (OpenSaveMRU)
 - Contains path information as well

USB Devices History

- When a USB device is connected to a computer, this is "logged" within the registry
 - I.e., configured and appropriate driver, if necessary, loaded
 - This information remains when the device is disconnected!
- Note: Most USB storage device have unique serial numbers
 - This means, the exact item can be recognized!
 - » Software: UVCView from Microsoft
- Registry key: HKLM\System\ControlSet00?\Enum\USBSTOR
 - Subkey: Vendor, Producer and Revision
 - Sub-Subkey: Serial number (if existing; else generated)
 - ParentIdPrefix: Corresponds to HKLM\System\MountedDevices
 - » Binary value!
- In C:\Windows\setupapi.log the first installation is logged

Owner Information

- Owner/Organization: HKLM\Software\Microsoft\Windows NT\CurrentVersion
 - RegisteredOwner: Owner name
 - RegisteredOrganization: Organization name
 - ProductId: Product ID
 - DigitalProductId: Contains encr. license key (Bytes 52-66)
 - InstallDate: Installation date (UNIX timestamp)
 - SystemRoot: Windows installation directory
- Last user: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
 - DefaultUserName: Last logged in user
 - » When? → Timestamp of key!
 - DefaultDomainName: Last domain logged into
 - DontDisplayLastUserName: Don't store information above

Summary

- Search times can be reduced through the use of default folders and operating system artifacts
- The skill level of the user will determine whether this is an effective use of time in the case

Questions?

m.owda@mmu.ac.uk