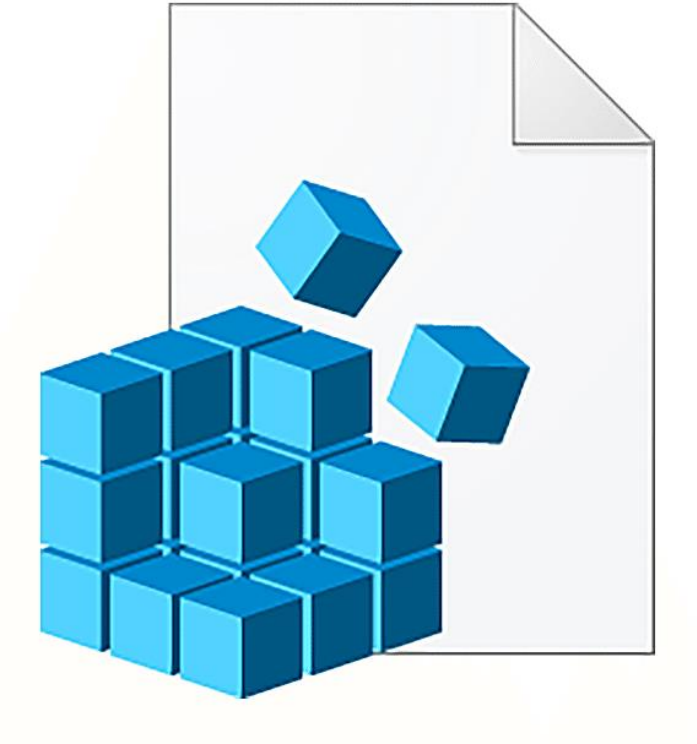
Digital Forensics Notable Artifacts

Dr Hanan Hindy
hanan.hindy@cis.asu.edu.eg

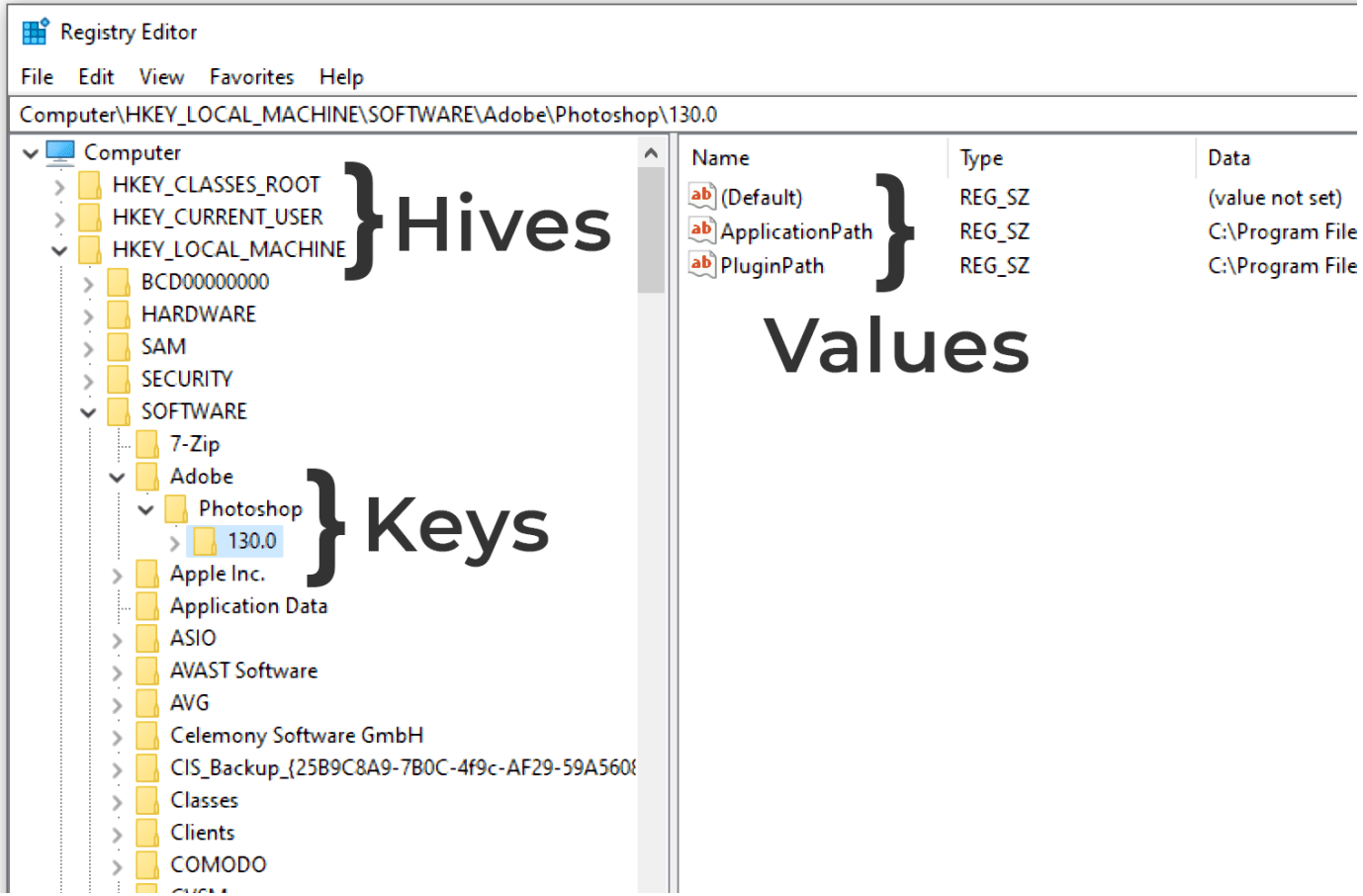
Agenda

- From Last Time:
  - Windows Registry
  - Page file
- Windows Artifacts
  - Metadata
  - EXIF Data
  - Prefetch
  - .LNK Files
  - MRU-Stuff
  - Thumbcache
- Windows Event Viewer
- Program Log Files
- Browser Artifacts

Windows Registry



Windows Registry



Windows Registry

The Windows registry is a **hierarchical database** that stores information about users, installed application, and the Windows system itself.

Windows registry is a **tree structure** where each node in the tree is called a key and every key may have a value or sub-keys.

A registry tree can be as deep as **512** keys.

Windows Registry

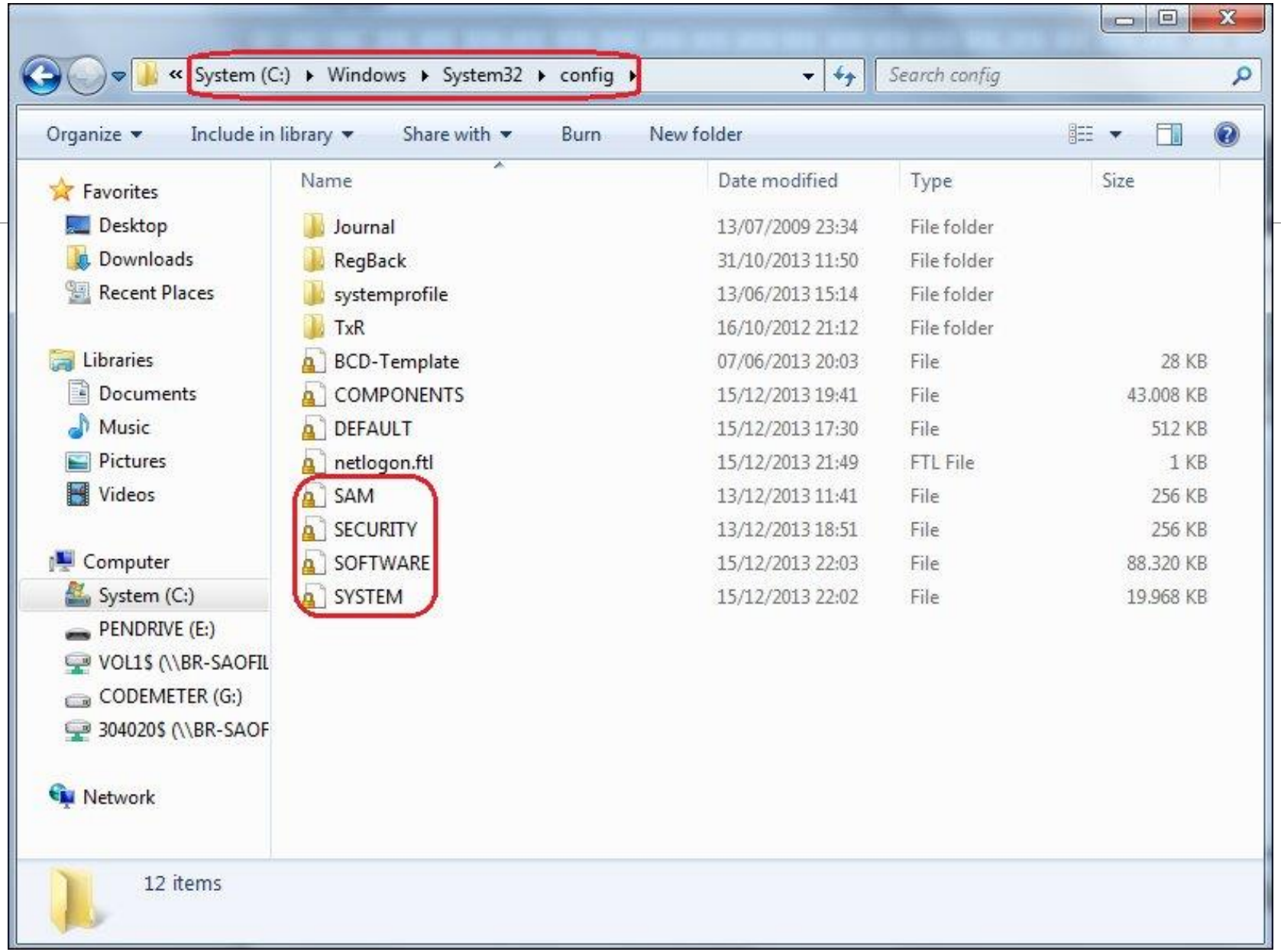
The values that a key can contain are just arbitrary data, and it is up to the application that stored the value to decide the format and how it is to be interpreted.

The registry is made up of several files, so-called **hives.**

Windows Registry

The hives that are most commonly of interest to a forensic examiner are (located in [root]/windows/system32/config):

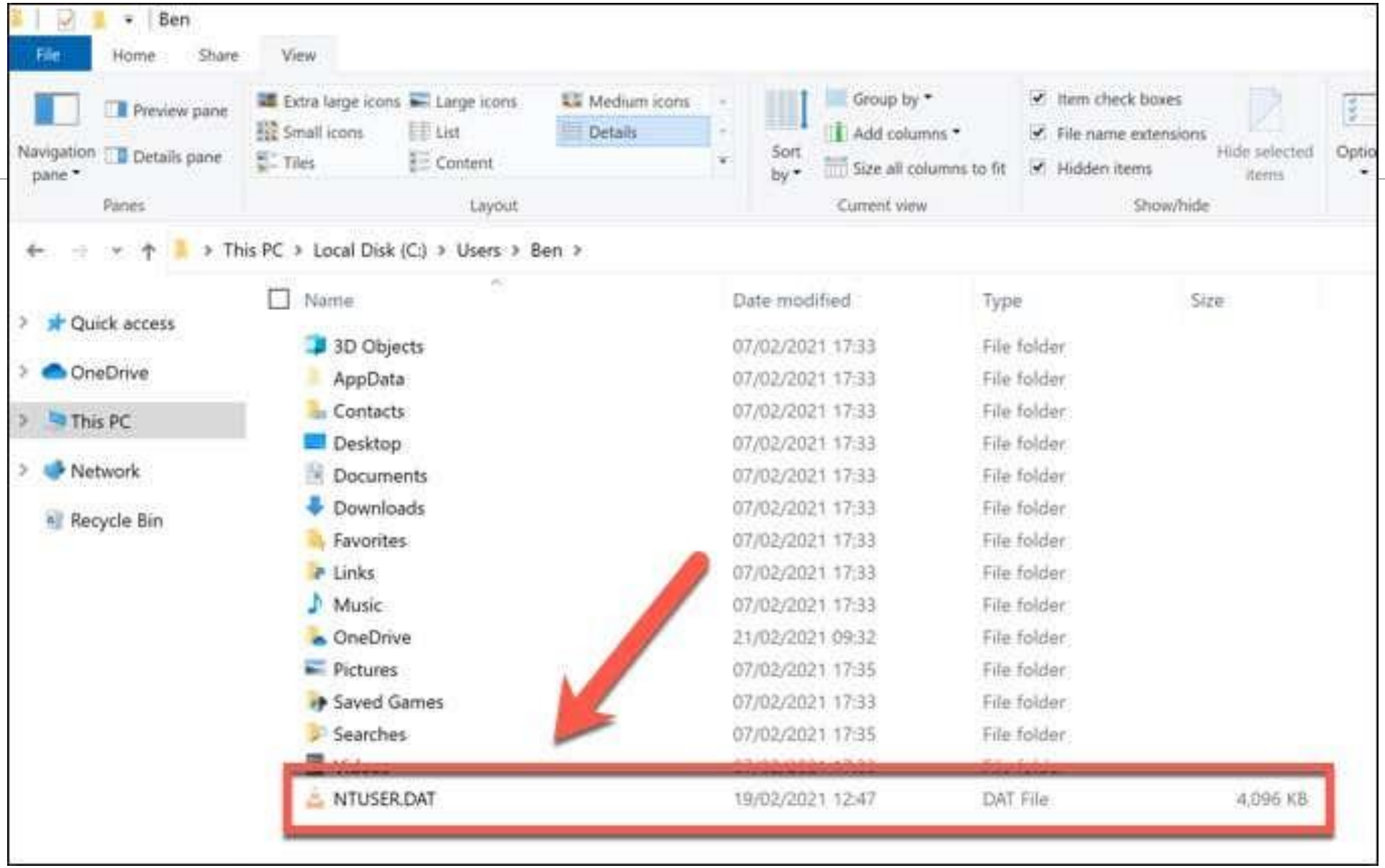
- SAM,
- SECURITY,
- SYSTEM,
- and SOFTWARE.

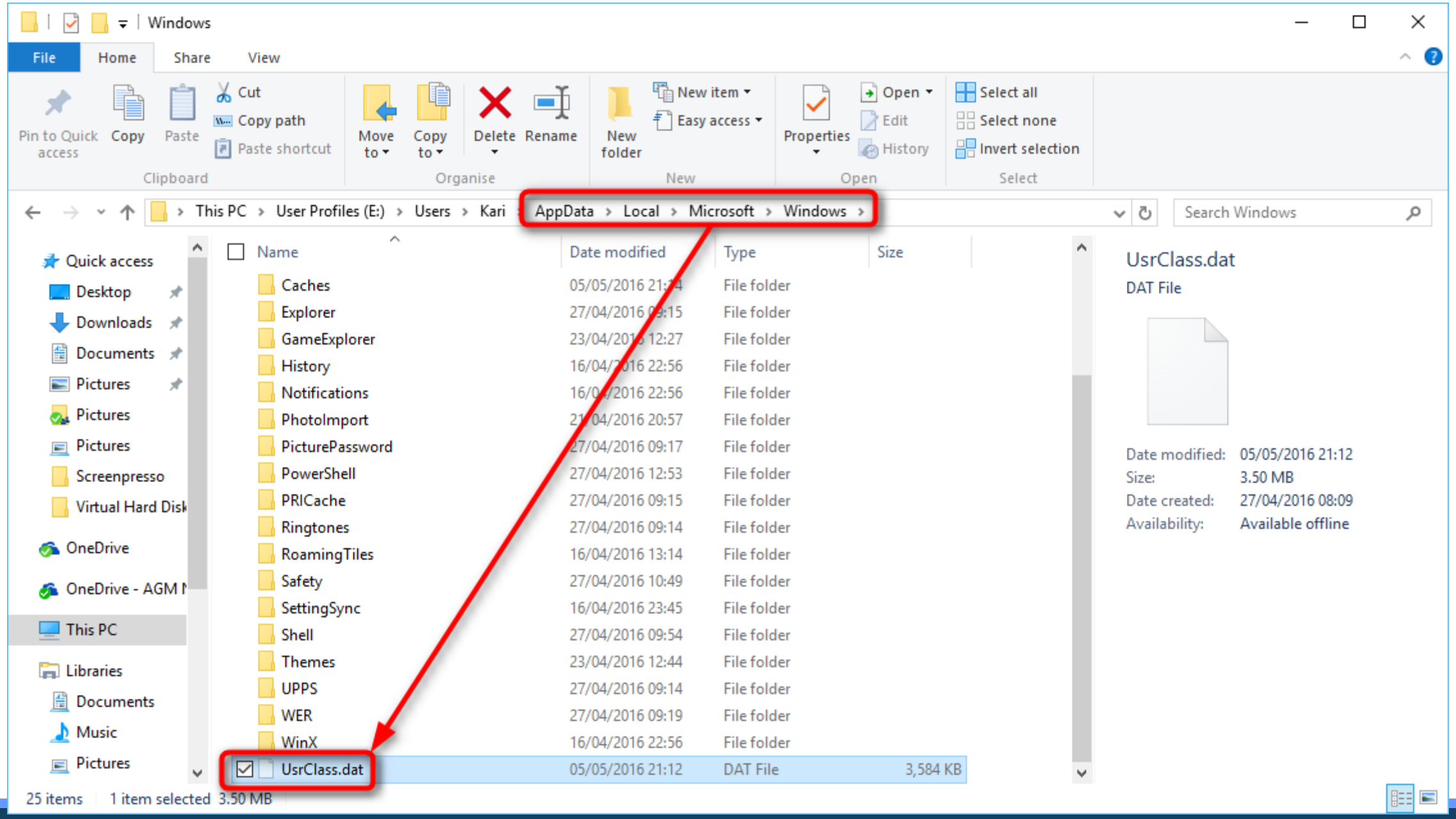

System (C:) ▸ Windows ▸ System32 ▸ config
Search config
Organize
Include in library
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
System (C:)
PENDRIVE (E:)
VOL1$ (\\BR-SAOFIL
CODEMETER (G:)
304020$ (\\BR-SAOF
Network
Name
Date modified
Type
Size
Journal 13/07/2009 23:34 File folder
RegBack 31/10/2013 11:50 File folder
systemprofile 13/06/2013 15:14 File folder
TxR 16/10/2012 21:12 File folder
BCD-Template 07/06/2013 20:03 File 28 KB
COMPONENTS 15/12/2013 19:41 File 43.008 KB
DEFAULT 15/12/2013 17:30 File 512 KB
netlogon.ftl 15/12/2013 21:49 FTL File 1 KB
SAM 13/12/2013 11:41 File 256 KB
SECURITY 13/12/2013 18:51 File 256 KB
SOFTWARE 15/12/2013 22:03 File 88.320 KB
SYSTEM 15/12/2013 22:02 File 19.968 KB
12 items

Windows Registry

There is also a hive for each user:

- NTuser.dat, located in the user's home folder
- usrClass.dat, located in ..\AppData\Local\Microsoft\Windows\


Ben
File
Home
Share
View
Preview pane
Navigation pane
Details pane
Panes
Extra large icons
Large icons
Medium icons
Small icons
List
Details
Tiles
Content
Layout
Sort by
Group by
Add columns
Size all columns to fit
Current view
Item check boxes
File name extensions
Hidden items
Hide selected items
Show/hide
This PC › Local Disk (C:) › Users › Ben ›
Quick access
OneDrive
This PC
Network
Recycle Bin
Name
Date modified
Type
Size
3D Objects 07/02/2021 17:33 File folder
AppData 07/02/2021 17:33 File folder
Contacts 07/02/2021 17:33 File folder
Desktop 07/02/2021 17:33 File folder
Documents 07/02/2021 17:33 File folder
Downloads 07/02/2021 17:33 File folder
Favorites 07/02/2021 17:33 File folder
Links 07/02/2021 17:33 File folder
Music 07/02/2021 17:33 File folder
OneDrive 21/02/2021 09:32 File folder
Pictures 07/02/2021 17:35 File folder
Saved Games 07/02/2021 17:33 File folder
Searches 07/02/2021 17:35 File folder
NTUSER.DAT 19/02/2021 12:47 DAT File 4,096 KB

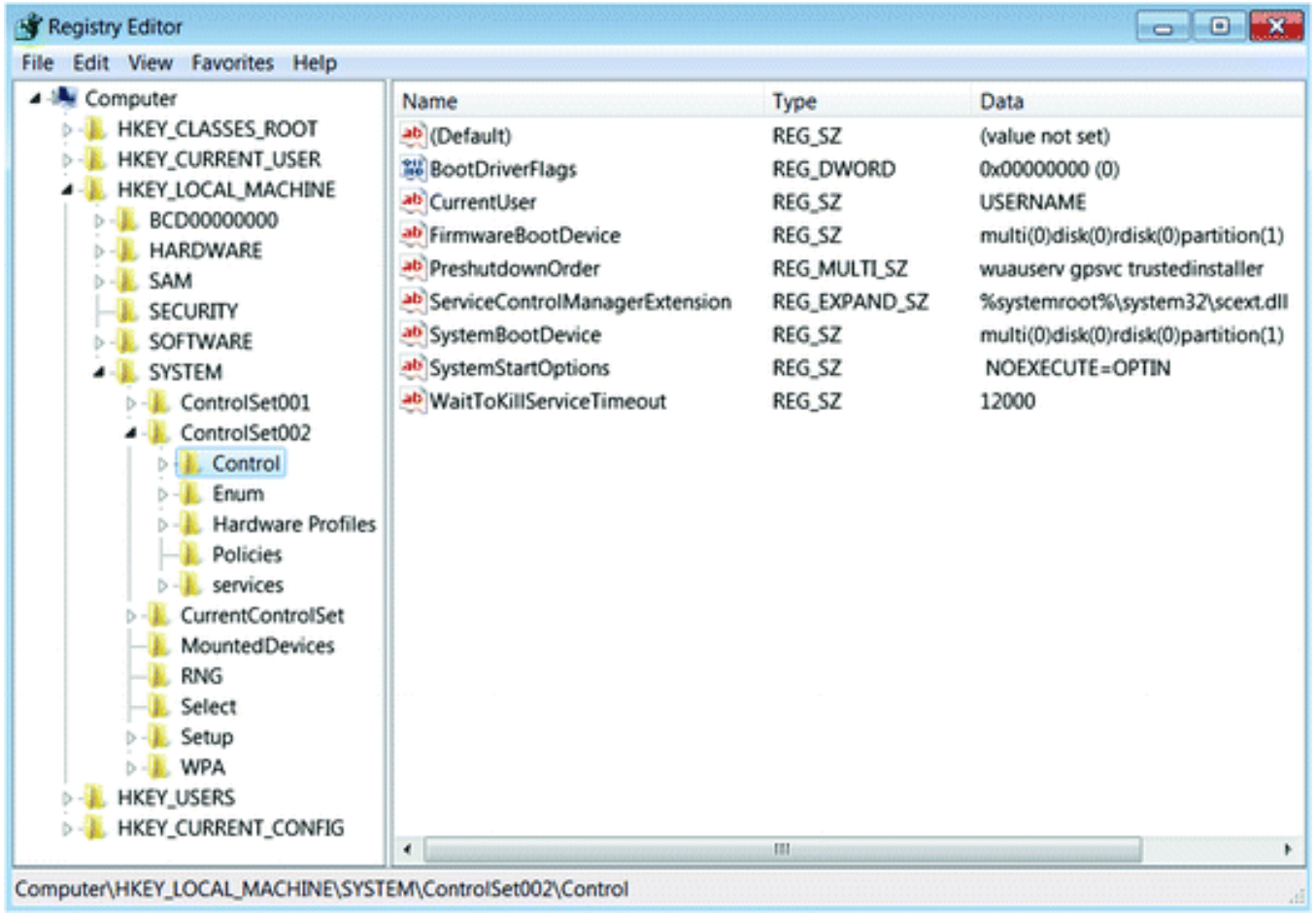

Windows
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organise
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › User Profiles (E:) › Users › Kari › AppData › Local › Microsoft › Windows ›
Search Windows
Quick access
Desktop
Downloads
Documents
Pictures
Pictures
Pictures
Screenpresso
Virtual Hard Disk
OneDrive
OneDrive - AGM
This PC
Libraries
Documents
Music
Pictures
Name
Date modified
Type
Size
Caches
Explorer
GameExplorer
History
Notifications
PhotoImport
PicturePassword
PowerShell
PRICache
Ringtones
RoamingTiles
Safety
SettingSync
Shell
Themes
UPPS
WER
WinX
UsrClass.dat
05/05/2016 21:12
DAT File
3,584 KB
UsrClass.dat
DAT File
Date modified: 05/05/2016 21:12
Size: 3.50 MB
Date created: 27/04/2016 08:09
Availability: Available offline
25 items
1 item selected 3.50 MB

Windows Registry

The experiments show that:

- The NTUSER.DAT stores the ShellBag information for the Desktop, Windows network folders, remote machines and remote folders.
- The UsrClass.dat stores the ShellBag information for the Desktop, ZIP files, remote folders, local folders, Windows special folders and virtual folders.

Registry Editor



Typical registry hive:	Supportive files:
HKEY_CURRENT_CONFIG	System & System.alt, System.log & System.sav
HKEY_CURRENT_USER	Ntuser.dat & Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam & Sam.log & Sam.sav
HKEY_LOCAL_MACHINE\SECURITY	Security & Security.log & Security.sav
HKEY_LOCAL_MACHINE\SOFTWARE	Software & Software.log & Software.sav
HKEY_LOCAL_MACHINE\SYSTEM	System & System.alt & System.log & System.sav

Transaction Logs

Transaction logs are used when registry hives **cannot** directly be written due to locking or corruption.
Transaction logs are written to files in the same directory as their corresponding registry hives.

SOFTWARE	9/30/2020 9:33 PM	File	69,376 KB
SOFTWARE.LOG1	12/7/2019 12:03 PM	LOG1 File	0 KB
SOFTWARE.LOG2	12/7/2019 12:03 PM	LOG2 File	17,396 KB
SYSTEM	9/16/2020 10:26 AM	File	10,496 KB
SYSTEM.LOG1	12/7/2019 12:03 PM	LOG1 File	1,216 KB
SYSTEM.LOG2	12/7/2019 12:03 PM	LOG2 File	0 KB

Windows Registry

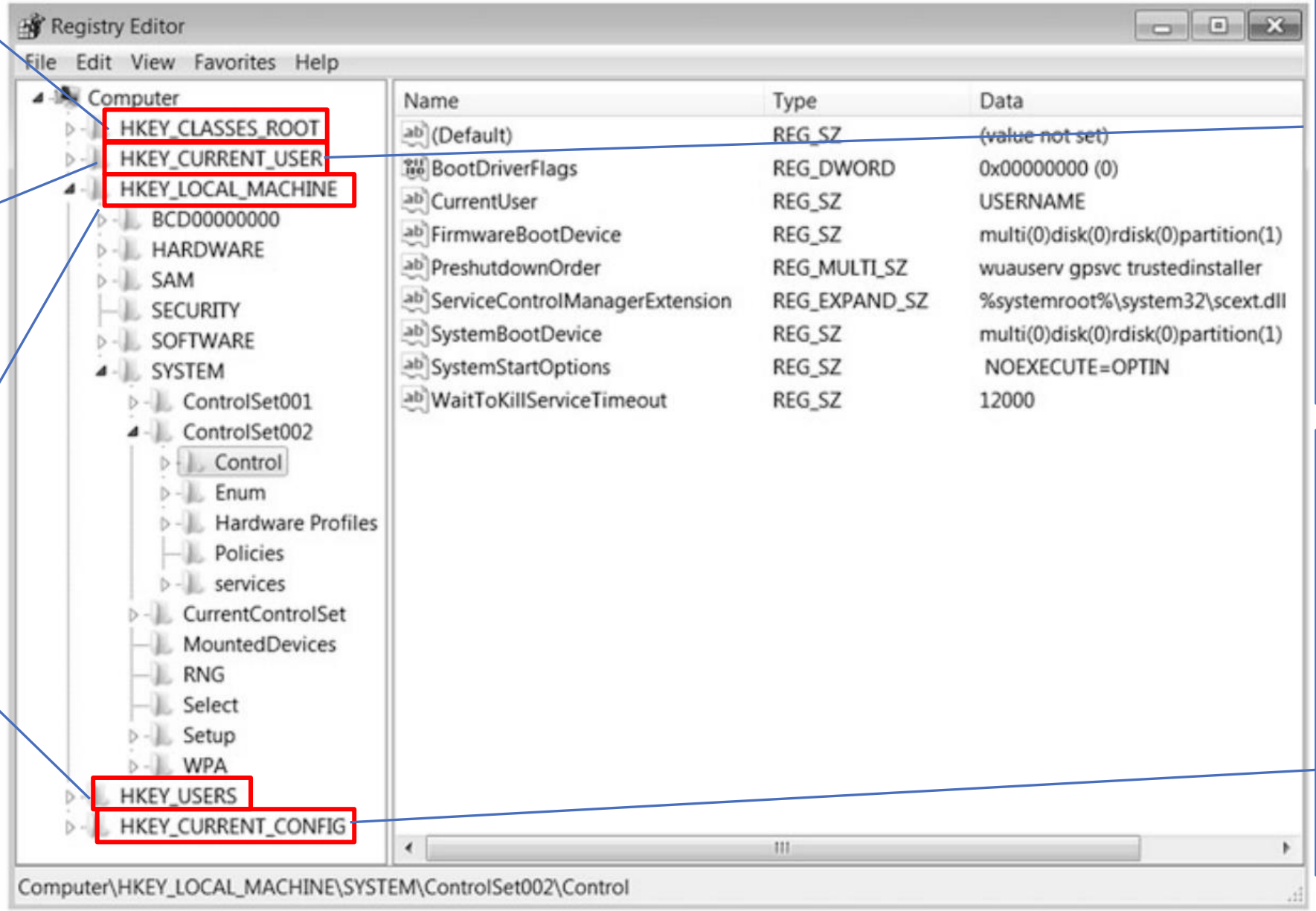
What is each hive used for?

Contains information about registered applications.

Contains the data stored for the current user

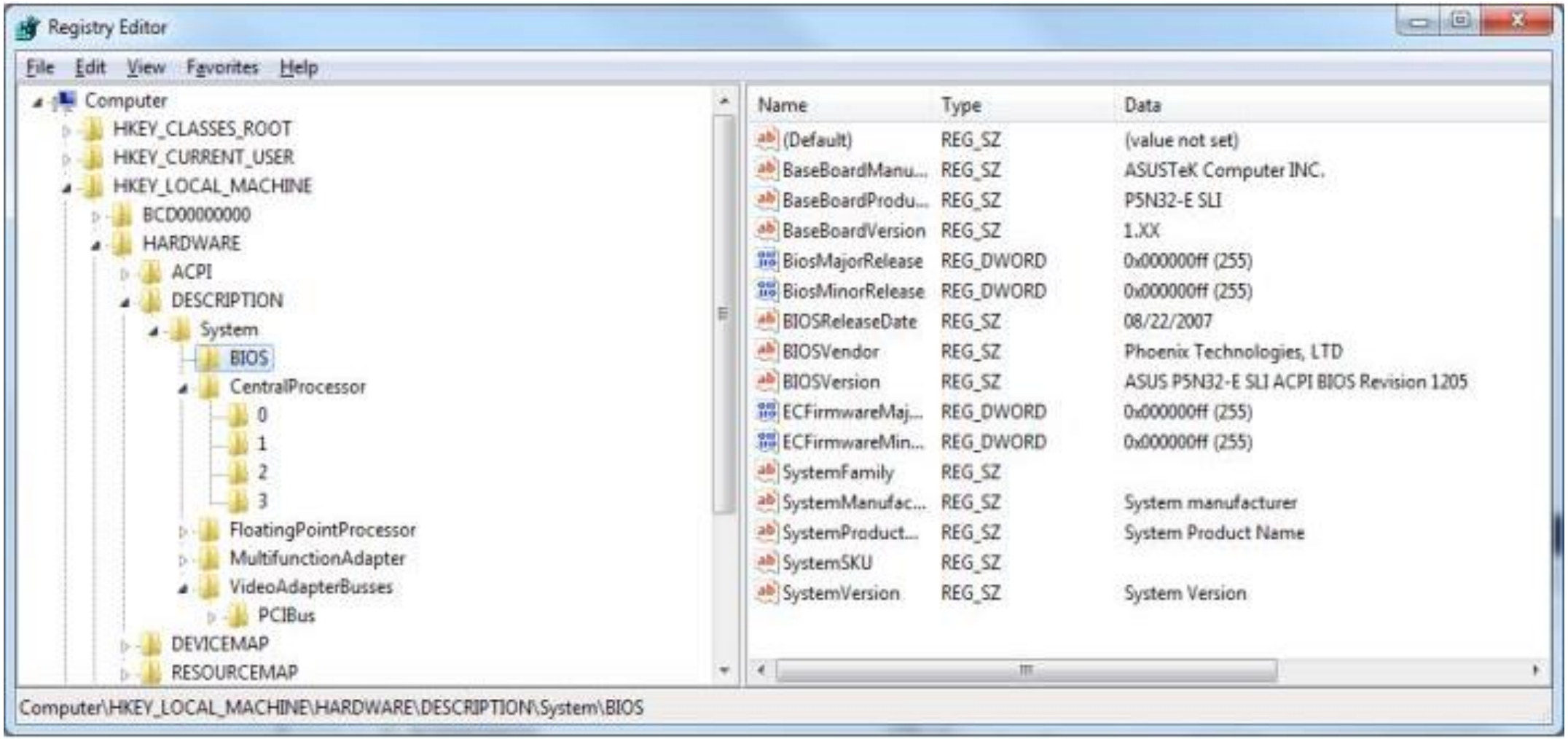
Contains settings that are specific to the local computer.

Contains subkeys corresponding to the HKEY_CURRENT_USER keys for **each user profile** actively loaded on the machine.



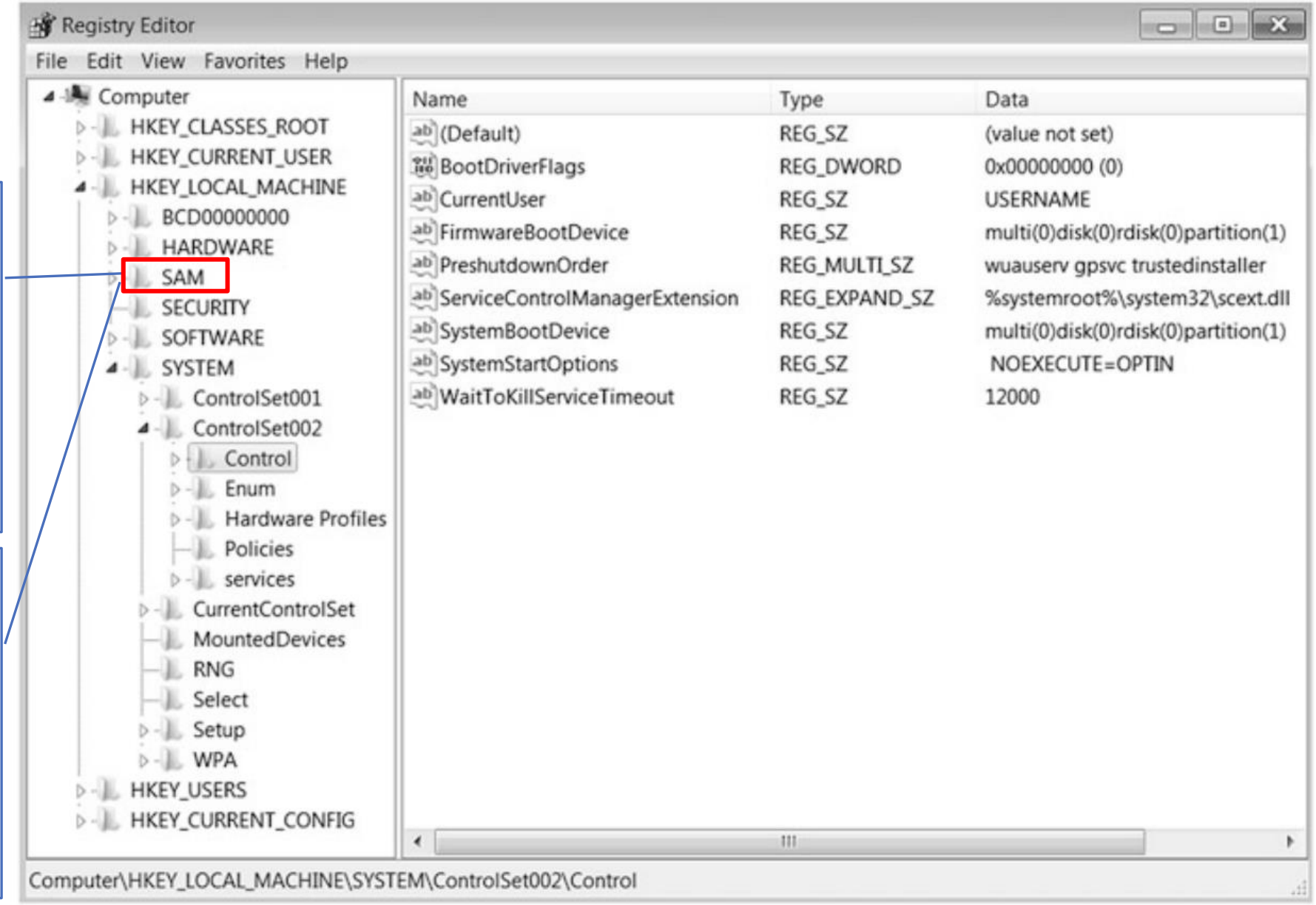
Stores information about a specific user account. This hive can contain information such as the user's browser settings and history and data related to user applications.

It doesn't store any information itself but instead acts as a pointer, or a shortcut, to a registry key that keeps the information about the hardware profile currently being used.


Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
ACPI
DESCRIPTION
System
BIOS
CentralProcessor
0
1
2
3
FloatingPointProcessor
MultifunctionAdapter
VideoAdapterBusses
PCIBus
DEVICEMAP
RESOURCEMAP
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

Security Accounts Manager. It stores credentials and account information for local users.

SAM is protected, not edited through Regedit

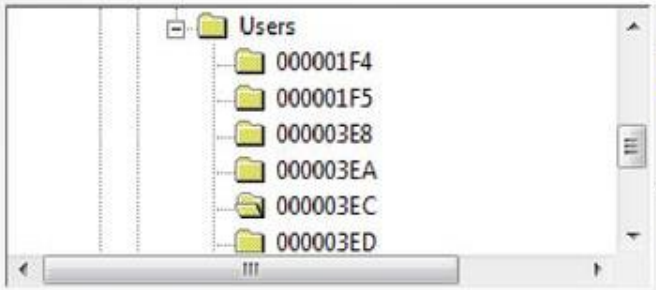


File Edit Report View Window Help

- SAM
  - SAM
    - Domains
      - Account
        - Aliases
        - Groups
        - Users
          - 000001F4
          - 000001F5
          - 000003EA
          - 000003EB
          - 000003EC
          - 000003ED
          - 000003EE
          - Names
            - Administrator
            - dunno
            - Evil_1
            - Evil_2
            - Evil_User
            - Guest
            - sansforensics408
      - Builtin
    - LastSkuUpgrade
    - RXACT

Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 00 00 00 00 00 00
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 0
ForcePasswordReset	REG_BINARY	00 00 00 00

- The F value in each users subkey contains <u>login info</u>



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 D6 B3 9E 88 E2 F0 C4 01 00 00 00 00 00 0...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 1A 00 00 00 00 0...

```
00 02 00 01 00 00 00 00 00-d6 b3 9e 88 e2 f0 c4 01 ........Ö³··âðÄ·
10 00 00 00 00 00 00 00 00-ee a2 b1 59 8e 0d c6 01 ........î¢±Y··Æ·
20 00 00 00 00 00 00 00 00-46 38 13 84 e2 f0 c4 01 ........F8··âðÄ·
30 ec 03 00 00 01 02 00 00-10 02 00 00 00 00 00 00 ì···............
40 00 00 4d 00 01 00 00 00-00 00 ff ff eb 06 91 7c ··M·......ÿÿë··|
```

Key Properties

Last Written Time	2005-01-02 15:48:41 UTC
SID unique identifier	1004
User Name	Frodo Baggins
Full Name	Frodo Baggins
Logon Count	77
Last Logon Time	2005-01-02 15:48:41 UTC
Last Password Change Time	2005-12-30 22:14:06 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	2005-01-02 15:48:34 UTC
Account Disabled	false
Password Required	true
Country Code	0 (System Default)
Hours Allowed	Anytime
Has LAN Manager Password	false
Has NTLMv2 Password	true

Description	Offset
Last logon time	8-15
Last password set time	24-31
Account expiration	32-39
Last failed logon time	40-47
Relative Identifier	48-51
Account status (LN)/password set (RN)	56
Country code	60-61
Invalid logon count	64-65
Logon count	66-67

LN= 0 = Account active
1 = Account not active

RN= 0 = Active and password set
1 = Not active (?)
4 = Password not set

- The V value stores the password hash (LM &/or NTLM)

Key Properties

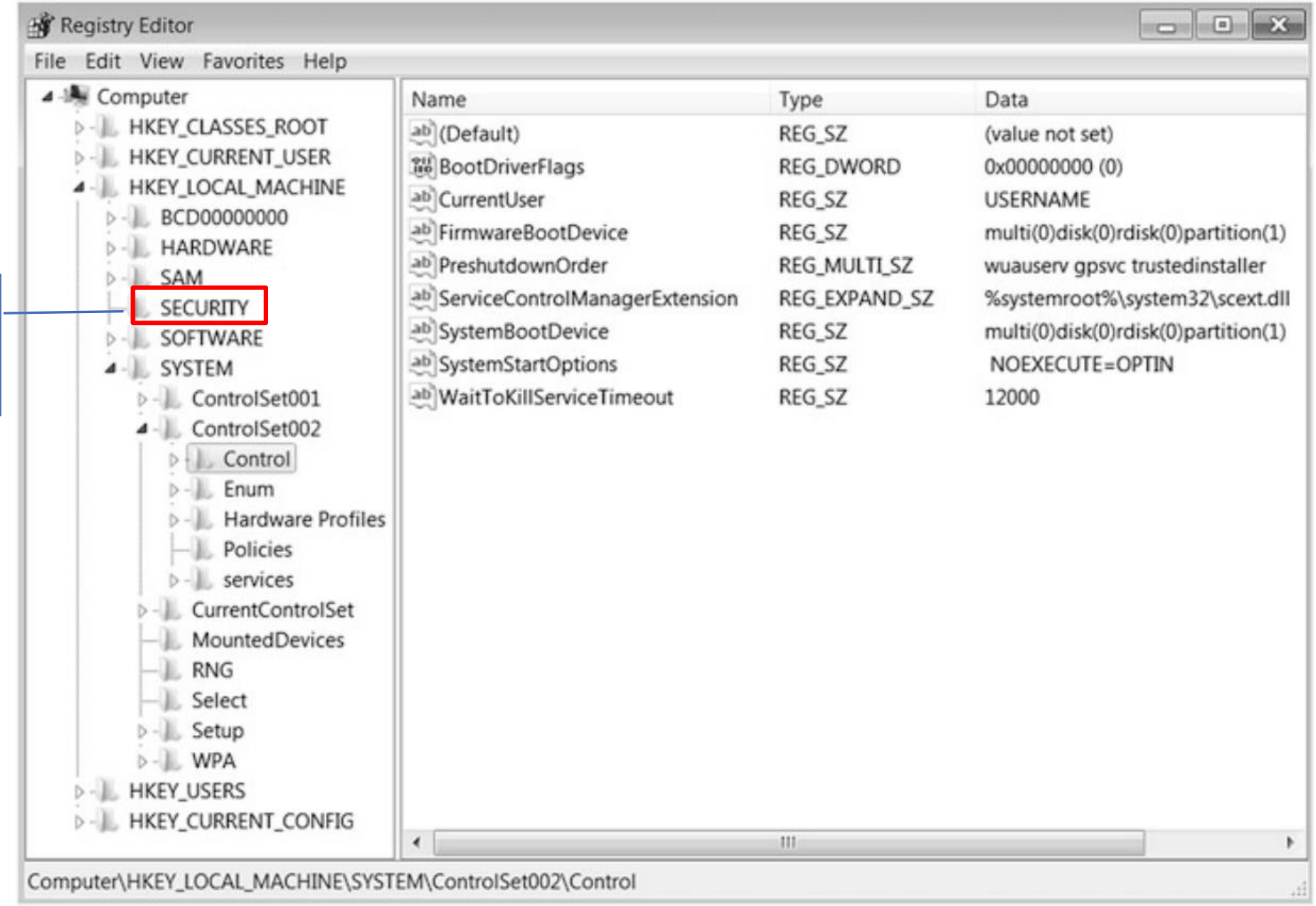
Last Written Time	2005-01-02 15:48:41 UTC
SID unique identifier	1004
User Name	Frodo Baggins
Full Name	Frodo Baggins
Logon Count	77
Last Logon Time	2005-01-02 15:48:41 UTC
Last Password Change Time	2005-12-30 22:14:06 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	2005-01-02 15:48:34 UTC
Account Disabled	false
Password Required	true
Country Code	0 (System Default)
Hours Allowed	Anytime
Has LAN Manager Password	false
Has NTLMv2 Password	true

Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 D6 B3 9E 88 E2 F0 C4 01 00 00 00 00 00 0...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 1A 00 00 00 00 0...

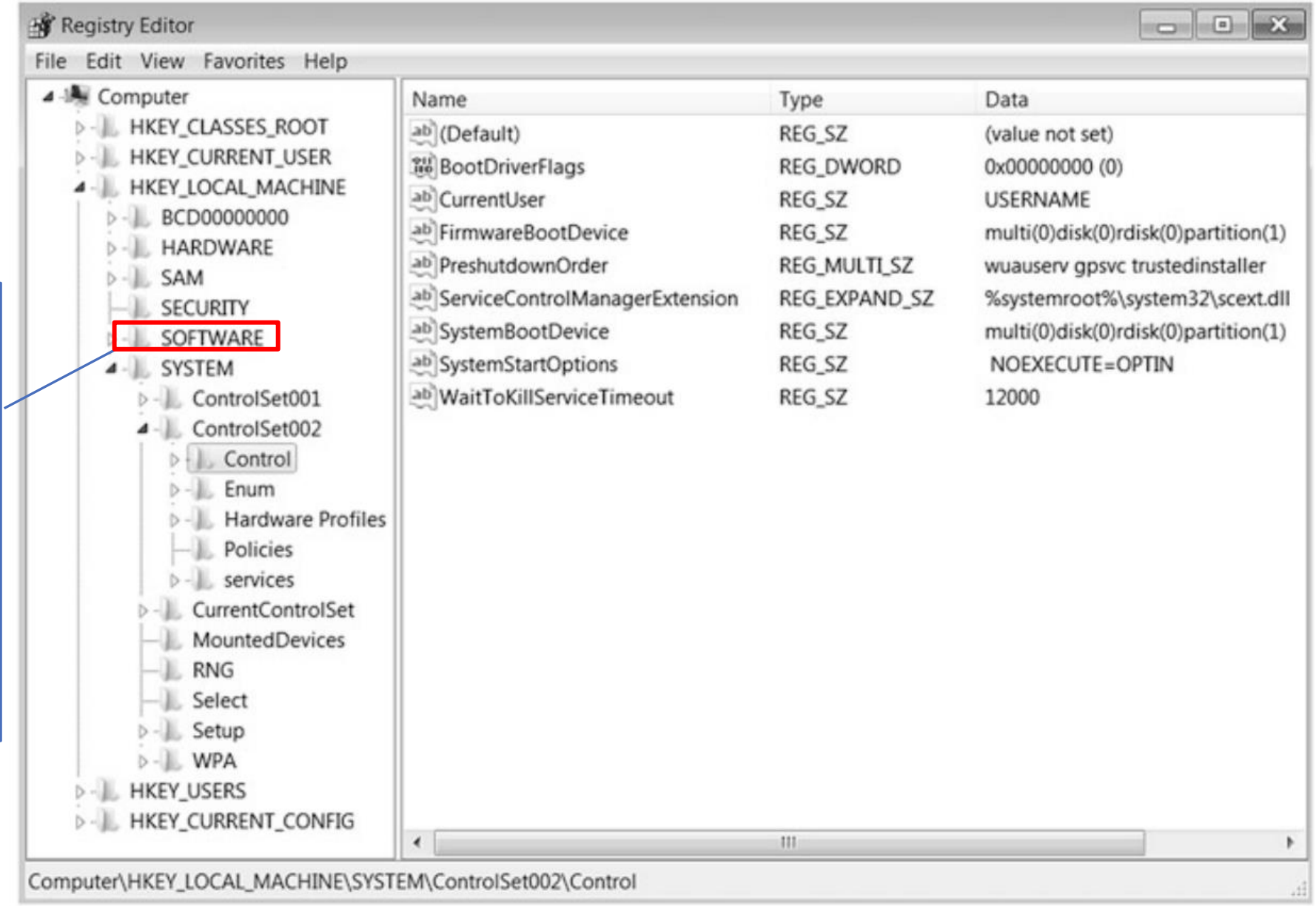
```
000  00 00 00 00 bc 00 00 00-02 00 01 00 bc 00 00 00  ····¼·····¼···
010  1a 00 00 00 00 00 00 00-d8 00 00 00 1a 00 00 00  ·····Ø·····
020  00 00 00 00 f4 00 00 00-00 00 00 00 00 00 00 00  ····ô·····
030  f4 00 00 00 00 00 00 00-00 00 00 00 f4 00 00 00  ô·····ô···
040  00 00 00 00 00 00 00 00-f4 00 00 00 00 00 00 00  ·····ô·····
050  00 00 00 00 f4 00 00 00-00 00 00 00 00 00 00 00  ····ô·····
060  f4 00 00 00 00 00 00 00-00 00 00 00 f4 00 00 00  ô·····ô···
070  00 00 00 00 00 00 00 00-f4 00 00 00 00 00 00 00  ·····ô·····
080  00 00 00 00 f4 00 00 00-15 00 00 00 a8 00 00 00  ····ô·····¨···
090  0c 01 00 00 08 00 00 00-01 00 00 00 14 01 00 00  ······· ·····
0a0  04 00 00 00 00 00 00 00-18 01 00 00 14 00 00 00  ····· ·····
0b0  00 00 00 00 2c 01 00 00-04 00 00 00 00 00 00 00  ····,·····
0c0  30 01 00 00 04 00 00 00-00 00 00 00 01 00 14 80  0·····€····
0d0  9c 00 00 00 ac 00 00 00-14 00 00 00 44 00 00 00  ····¬·····D···
0e0  02 00 30 00 02 00 00 00-02 c0 14 00 44 00 05 01  ··0·····À··D···
0f0  01 01 00 00 00 00 00 01-00 00 00 00 02 c0 14 00  ·····À··
100  ff 07 0f 00 01 01 00 00-00 00 00 05 07 00 00 00  ÿ·····
110  02 00 58 00 03 00 00 00-00 00 24 00 44 00 02 00  ··X·····$·D···
120  01 05 00 00 00 00 00 05-15 00 00 00 23 5f 63 6b  ·····#_ck
130  83 3d 2b 46 07 e5 3b 2b-ec 03 00 00 00 00 18 00  ·=+F·å;+ì·····
140  ff 07 0f 00 01 02 00 00-00 00 00 05 20 00 00 00  ÿ·····  ···
150  20 02 00 00 00 00 14 00-5b 03 02 00 01 01 00 00  ·····[·····
160  00 00 00 01 00 00 00 00-01 02 00 00 00 00 00 05  ·····
170  20 00 00 00 20 02 00 00-01 02 00 00 00 00 00 05  ···  ·····
180  20 00 00 00 20 02 00 00-46 00 72 00 6f 00 64 00  ···  ···F·r·o·d·
190  6f 00 20 00 42 00 61 00-67 00 67 00 69 00 6e 00  o· ·B·a·g·g·i·n·
1a0  73 00 00 00 46 00 72 00-6f 00 64 00 6f 00 20 00  s···F·r·o·d·o· ·
1b0  42 00 61 00 67 00 67 00-69 00 6e 00 73 00 00 00  B·a·g·g·i·n·s···
1c0  ff ff ff ff ff ff ff ff-ff ff ff ff ff ff ff ff  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
1d0  ff ff ff ff ff c3 48 d6-01 02 00 00 07 00 00 00  ÿÿÿÿÿÃHÖ·····
1e0  01 00 01 00 01 00 01 00-41 11 24 b5 10 3f 4d 25  ·····A·$µ·?M%
1f0  05 e1 74 f2 f3 53 15 89-01 00 01 00 01 00 01 00  ·átòóS·····
```

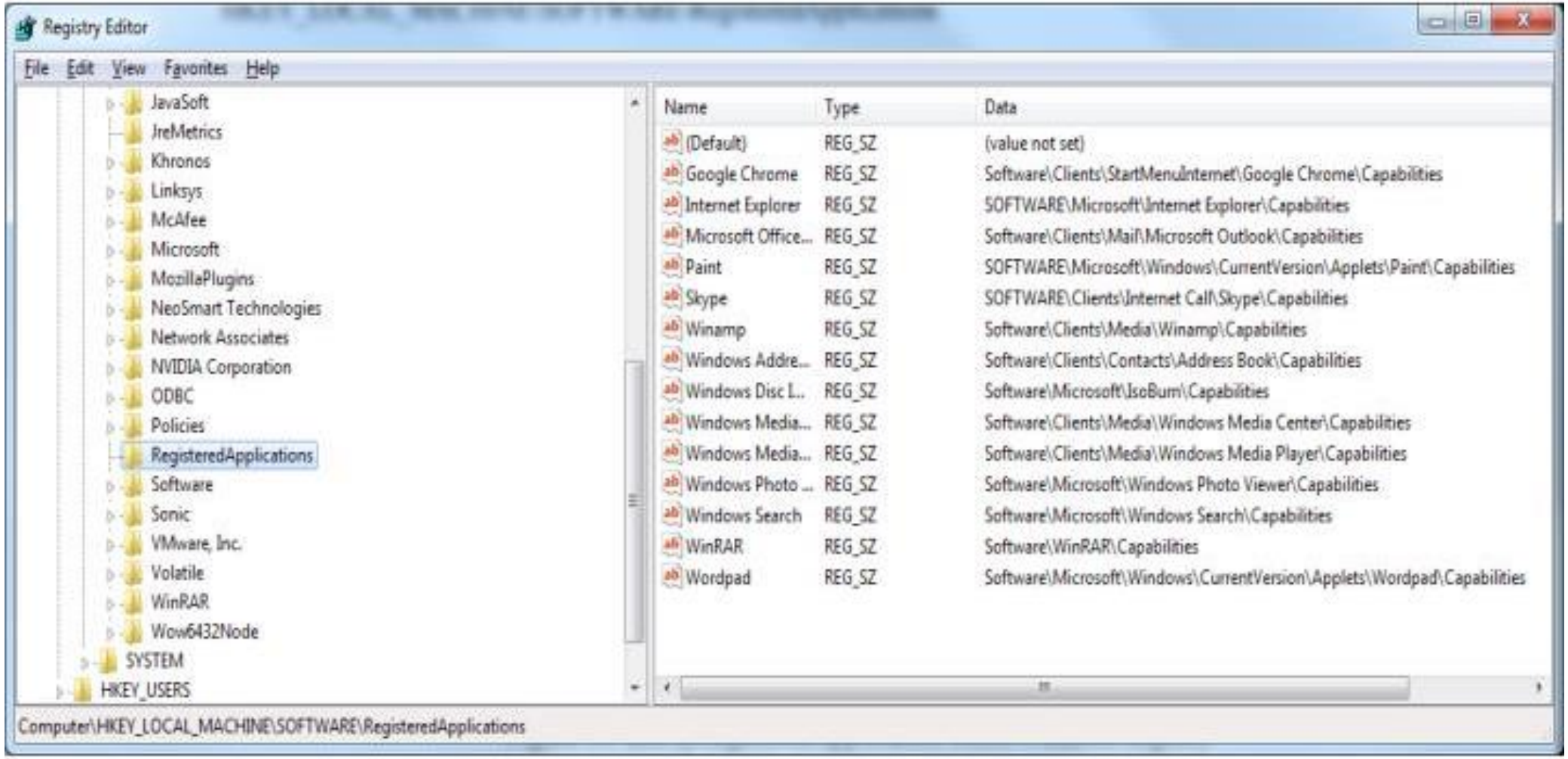
Hash(es) are stored at end.
If not logged in or no password entered when created, it's empty.

Mainly stores security policy.



Contains information related to applications. This includes data stored by Windows and data stored by other applications.




Registry Editor
File Edit View Favorites Help
JavaSoft
JreMetrics
Khronos
Linksys
McAfee
Microsoft
MozillaPlugins
NeoSmart Technologies
Network Associates
NVIDIA Corporation
ODBC
Policies
RegisteredApplications
Software
Sonic
VMware, Inc.
Volatile
WinRAR
Wow6432Node
SYSTEM
HKEY_USERS
Name Type Data
(Default) REG_SZ (value not set)
Google Chrome REG_SZ Software\Clients\StartMenuInternet\Google Chrome\Capabilities
Internet Explorer REG_SZ SOFTWARE\Microsoft\Internet Explorer\Capabilities
Microsoft Office... REG_SZ Software\Clients\Mail\Microsoft Outlook\Capabilities
Paint REG_SZ SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\Paint\Capabilities
Skype REG_SZ SOFTWARE\Clients\Internet Call\Skype\Capabilities
Winamp REG_SZ Software\Clients\Media\Winamp\Capabilities
Windows Addre... REG_SZ Software\Clients\Contacts\Address Book\Capabilities
Windows Disc L... REG_SZ Software\Microsoft\IsoBurn\Capabilities
Windows Media... REG_SZ Software\Clients\Media\Windows Media Center\Capabilities
Windows Media... REG_SZ Software\Clients\Media\Windows Media Player\Capabilities
Windows Photo ... REG_SZ Software\Microsoft\Windows Photo Viewer\Capabilities
Windows Search REG_SZ Software\Microsoft\Windows Search\Capabilities
WinRAR REG_SZ Software\WinRAR\Capabilities
Wordpad REG_SZ Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Capabilities
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Registry Editor

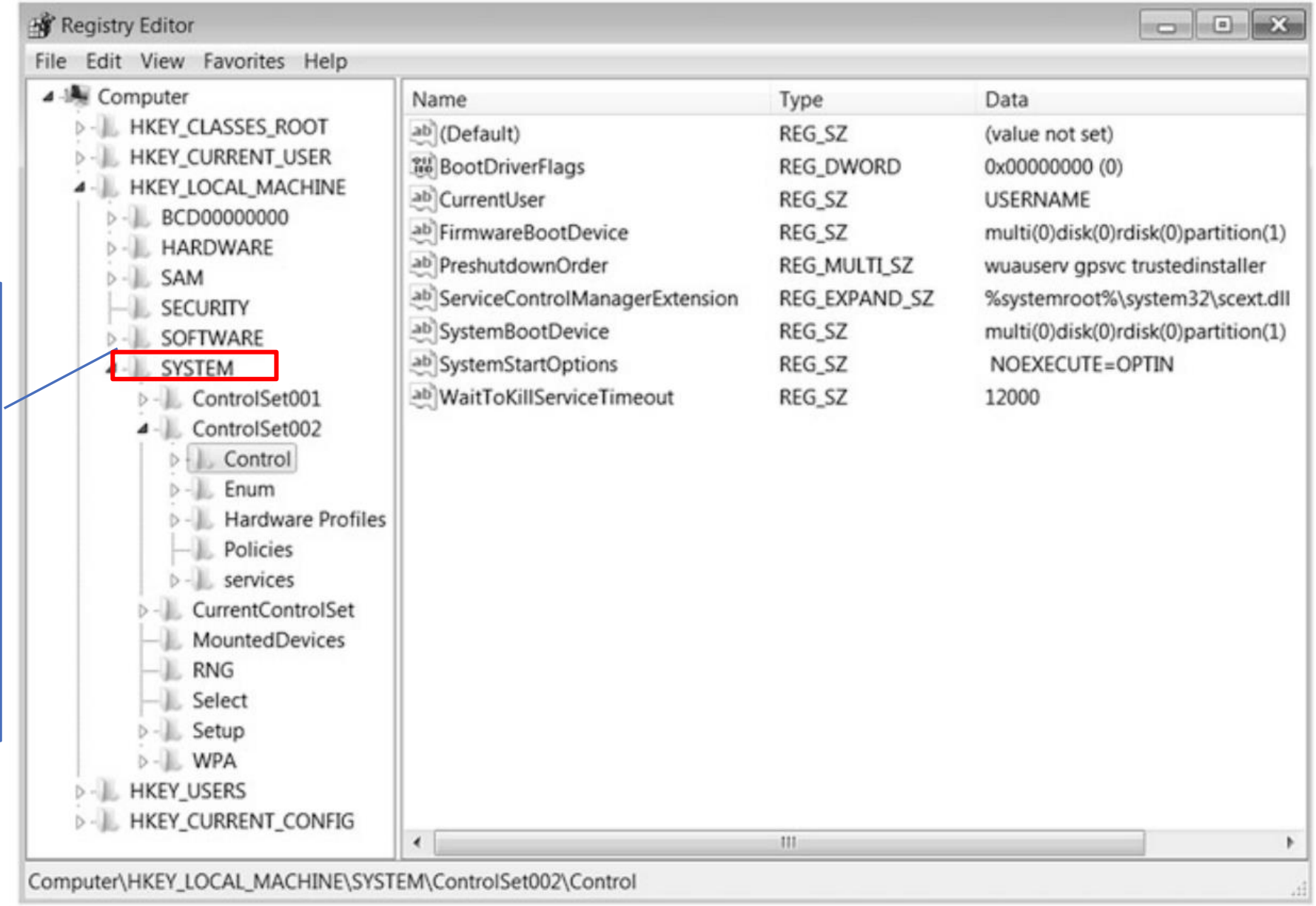
File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

- VisualStudio
- WAB
- Wallet
- Wbem
- WcmSvc
- WIMMount
- Windows
- Windows Advanced Threat Protection
- Windows Defender
- Windows Defender Security Center
- Windows Desktop Search
- Windows Embedded
- Windows Mail
- Windows Media Device Manager
- Windows Media Foundation
- Windows Media Player NSS
- Windows Messaging Subsystem
- Windows NT
  - CurrentVersion
- Windows Phone
- Windows Photo Viewer
- Windows Portable Devices
- Windows Script Host
- Windows Search
- Windows Security Health
- WindowsRuntime
- WindowsSelfHost
- WindowsStore
- WindowsUpdate
- Wisp
- WlanSvc
- Wlpasvc
- Wow64
- WSDAPI

Name	Type	Data
(Default)	REG_SZ	(value not set)
BuildBranch	REG_SZ	rs5_release
BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLab	REG_SZ	17763.rs5_release.180914-1434
BuildLabEx	REG_SZ	17763.1.amd64fre.rs5_release.180914-1434
CompositionEditionID	REG_SZ	Enterprise
CurrentBuild	REG_SZ	17763
CurrentBuildNumber	REG_SZ	17763
CurrentMajorVersionNumber	REG_DWORD	0x0000000a (10)
CurrentMinorVersionNumber	REG_DWORD	0x00000000 (0)
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.3
DigitalProductId	REG_BINARY	[redacted]
DigitalProductId4	REG_BINARY	[redacted]
EditionID	REG_SZ	Enterprise
EditionSubManufacturer	REG_SZ	
EditionSubstring	REG_SZ	
EditionSubVersion	REG_SZ	
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x5d8b656e (1569416558)
InstallTime	REG_QWORD	0x1d573a1823ef39e (132138901589390238)
PathName	REG_SZ	C:\Windows
[redacted]	[redacted]	[redacted]
ProductName	REG_SZ	Windows 10 Enterprise
RegisteredOrganization	REG_SZ	
RegisteredOwner	REG_SZ	Windows User
ReleaseId	REG_SZ	1809
SoftwareType	REG_SZ	System
SystemRoot	REG_SZ	C:\WINDOWS
UBR	REG_DWORD	0x00000325 (805)

Contains information about the Windows system setup



Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Memory Management

- Environment
- Executive
- FileRenameOperations
- I/O System
- kernel
- KnownDLLs
- Memory Management
  - PrefetchParameters
  - StoreParameters
- NamespaceSeparation

Name	Type	Data
(Default)	REG_SZ	(value not set)
ClearPageFileAtShutdown	REG_DWORD	0x00000000 (0)
DisablePagingExecutive	REG_DWORD	0x00000000 (0)
ExistingPageFiles	REG_MULTI_SZ	\??\C:\pagefile.sys
FeatureSettings	REG_DWORD	0x00000000 (0)
LargeSystemCache	REG_DWORD	0x00000000 (0)
ModifiedWriteMaximum	REG_DWORD	0x00000004 (4)
NonPagedPoolQuota	REG_DWORD	0x00000000 (0)
NonPagedPoolSize	REG_DWORD	0x00000000 (0)

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows

- VAN
- Video
- WalletService
- wcncsvc
- Wdf
- WDI
- Windows
- WinInit
- Winlogon
- Winresume
- WMI
- WorkplaceJoin
- WPN
- Enum

Name	Type	Data
(Default)	REG_SZ	(value not set)
ComponentizedBuild	REG_DWORD	0x00000001 (1)
CSDBuildNumber	REG_DWORD	0x000008eb (2283)
CSDReleaseType	REG_DWORD	0x00000000 (0)
CSDVersion	REG_DWORD	0x00000000 (0)
Directory	REG_EXPAND_SZ	%SystemRoot%
ErrorMode	REG_DWORD	0x00000000 (0)
FullProcessInformationSID	REG_BINARY	01 06 00 00 00 00 00 05 50 00 00 00 5e f3 0f b1 8...
NoInteractiveServices	REG_DWORD	0x00000001 (1)
ShellErrorMode	REG_DWORD	0x00000001 (1)
ShutdownTime	REG_BINARY	2c b9 2c 6f a3 fb d9 01
SystemDirectory	REG_EXPAND_SZ	%SystemRoot%\system32

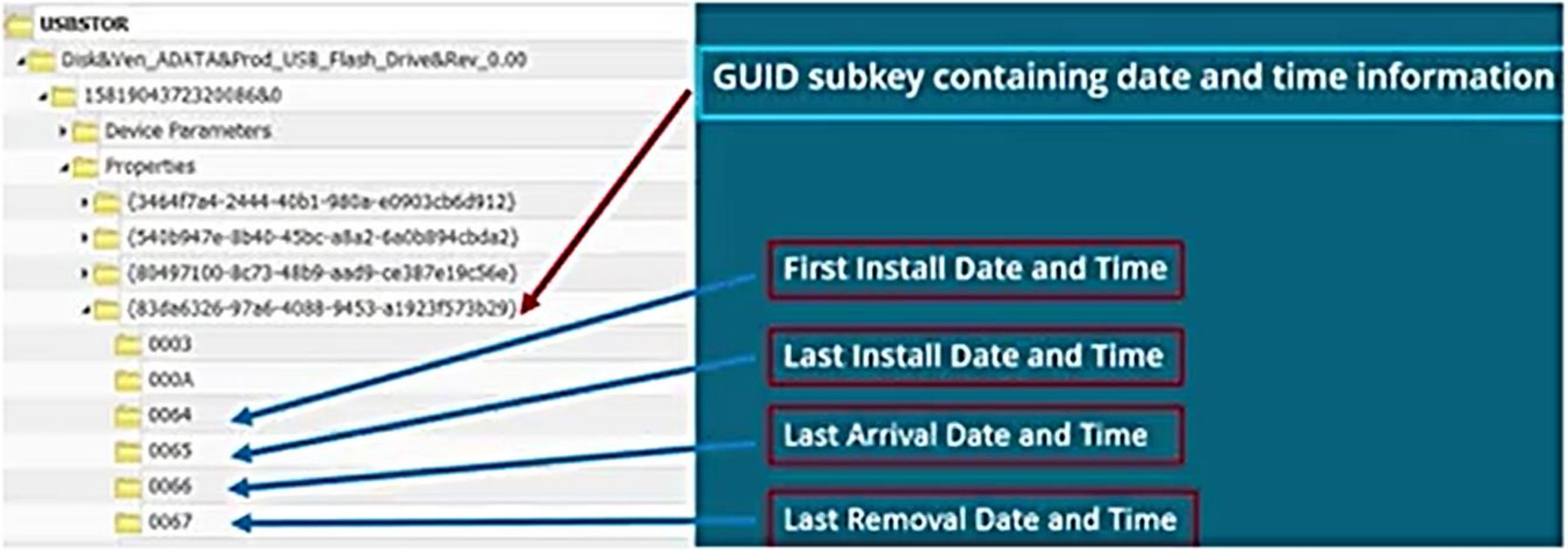
Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_VendorCo&Prod_ProductCode&Rev_2.00\0285681276815618279&0

- USB
- USB4
- USBPRINT
- USBSTOR
  - Disk&Ven_Generic&Prod_Flash_Disk&Rev_
    - 7AD35455&0
  - Disk&Ven_Generic-&Prod_MicroSD/M2&R
    - 058F64596479&1
  - Disk&Ven_Generic-&Prod_Multiple_Reader
    - 058F64596479&0
  - Disk&Ven_SanDisk&Prod_Cruzer_Blade&R
    - 00009619021521130922&0
  - Disk&Ven_VendorCo&Prod_ProductCode&
    - 0285681276815618279&0
- Hardware Profiles
- Policies

Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000003 (3)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{8175d4e2-8cfa-508e-811a-a602f517afa1}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0003
FriendlyName	REG_SZ	VendorCo ProductCode USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskVendorCoProductCode____2.00 USB...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk


USBSTOR
Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00
15819043723200866&0
Device Parameters
Properties
{3464f7a4-2444-40b1-980a-e0903cb6d912}
{540b947e-8b40-45bc-a8a2-6a0b894cb5a2}
{80497100-8c73-48b9-aad9-ce387e19c56e}
{836a6326-97a6-4088-9453-a1923f573b29}
0003
000A
0064
0065
0066
0067
GUID subkey containing date and time information
First Install Date and Time
Last Install Date and Time
Last Arrival Date and Time
Last Removal Date and Time

Windows Registry

The **SAM** and **SECURITY** hives are protected by the Windows system and cannot be browsed using regedit on a running computer.

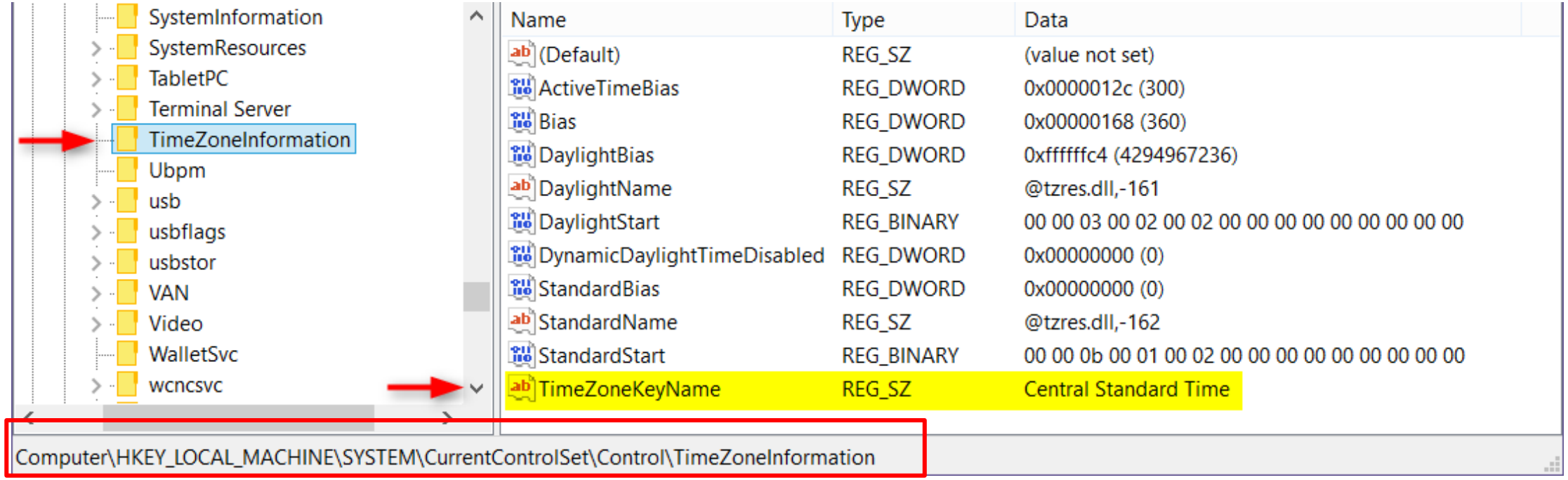
However, extracting them from a forensic image and browsing them using a forensic tool is no problem.

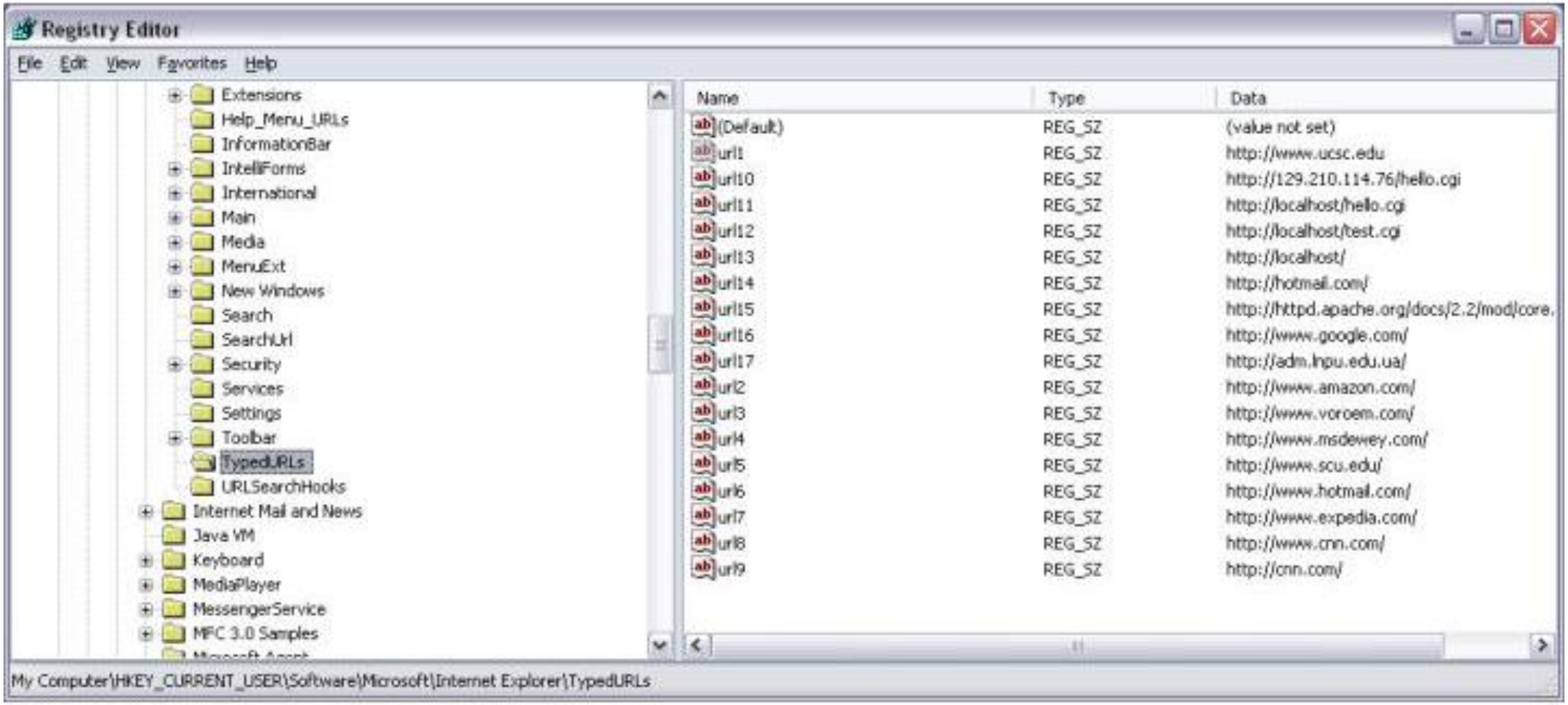
SAM hive stores information about users.

- Find the users on the local machine,
- Find information about when they last logged on, when each account was created, and password hashes.
- This hive contains the information you need to map a RID to a username, located in the key SAM \Domains\Account\Users\Names.

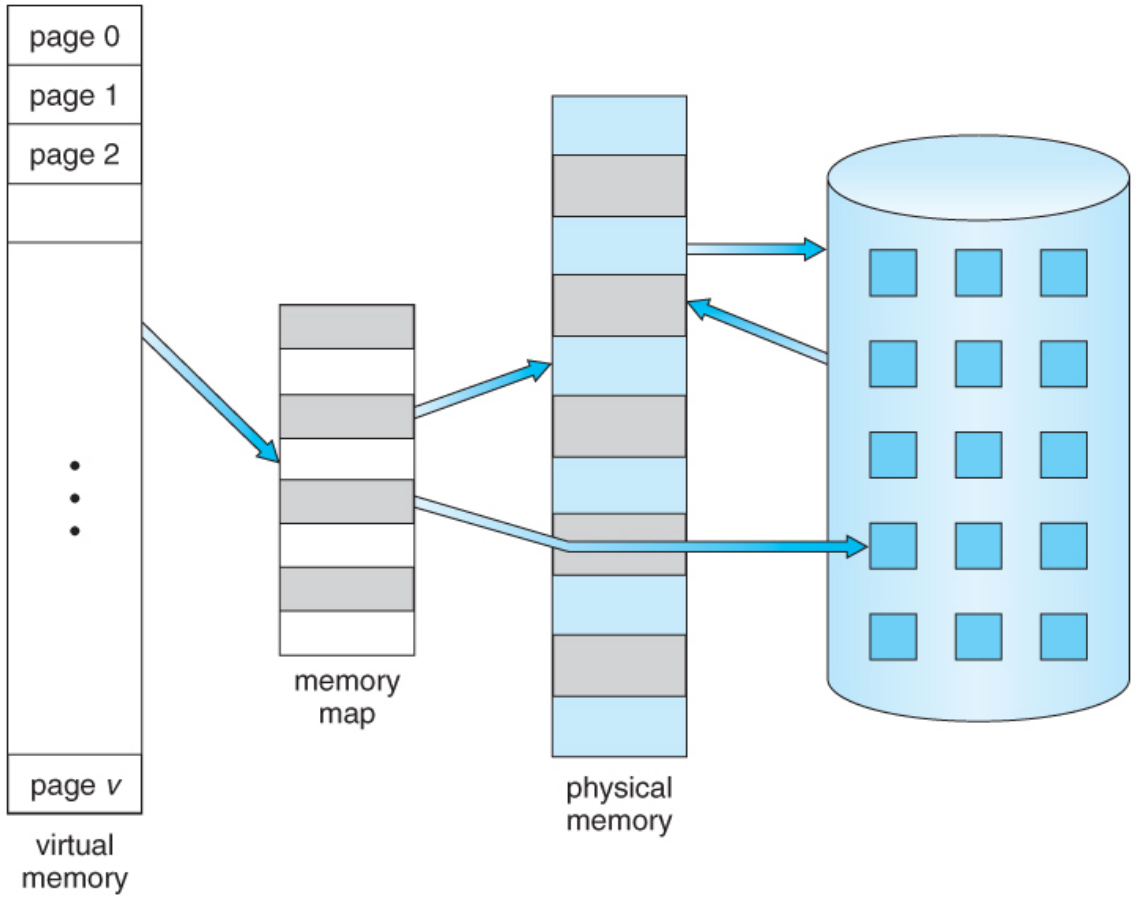
SECURITY hive stores some information about the system, perhaps mainly the system audit policy, and the Syskey that you will need in addition to the SAM hive if you need to crack user passwords.

Time Zone


SystemInformation
SystemResources
TabletPC
Terminal Server
TimeZoneInformation
Ubpm
usb
usbflags
usbstor
VAN
Video
WalletSvc
wcncsvc
Name
Type
Data
(Default)
REG_SZ
(value not set)
ActiveTimeBias
REG_DWORD
0x0000012c (300)
Bias
REG_DWORD
0x00000168 (360)
DaylightBias
REG_DWORD
0xffffffc4 (4294967236)
DaylightName
REG_SZ
@tzres.dll,-161
DaylightStart
REG_BINARY
00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
DynamicDaylightTimeDisabled
REG_DWORD
0x00000000 (0)
StandardBias
REG_DWORD
0x00000000 (0)
StandardName
REG_SZ
@tzres.dll,-162
StandardStart
REG_BINARY
00 00 0b 00 01 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName
REG_SZ
Central Standard Time
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation


Registry Editor
File Edit View Favorites Help
Extensions
Help_Menu_URLs
InformationBar
IntelliForms
International
Main
Media
MenuExt
New Windows
Search
SearchUrl
Security
Services
Settings
Toolbar
TypedURLs
URLSearchHooks
Internet Mail and News
Java VM
Keyboard
MediaPlayer
MessengerService
MFC 3.0 Samples
Name Type Data
(Default) REG_SZ (value not set)
url1 REG_SZ http://www.ucsc.edu
url10 REG_SZ http://129.210.114.76/hello.cgi
url11 REG_SZ http://localhost/hello.cgi
url12 REG_SZ http://localhost/test.cgi
url13 REG_SZ http://localhost/
url14 REG_SZ http://hotmail.com/
url15 REG_SZ http://httpd.apache.org/docs/2.2/mod/core.
url16 REG_SZ http://www.google.com/
url17 REG_SZ http://adm.lnpu.edu.ua/
url2 REG_SZ http://www.amazon.com/
url3 REG_SZ http://www.voroem.com/
url4 REG_SZ http://www.msdewey.com/
url5 REG_SZ http://www.scu.edu/
url6 REG_SZ http://www.hotmail.com/
url7 REG_SZ http://www.expedia.com/
url8 REG_SZ http://www.cnn.com/
url9 REG_SZ http://cnn.com/
My Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

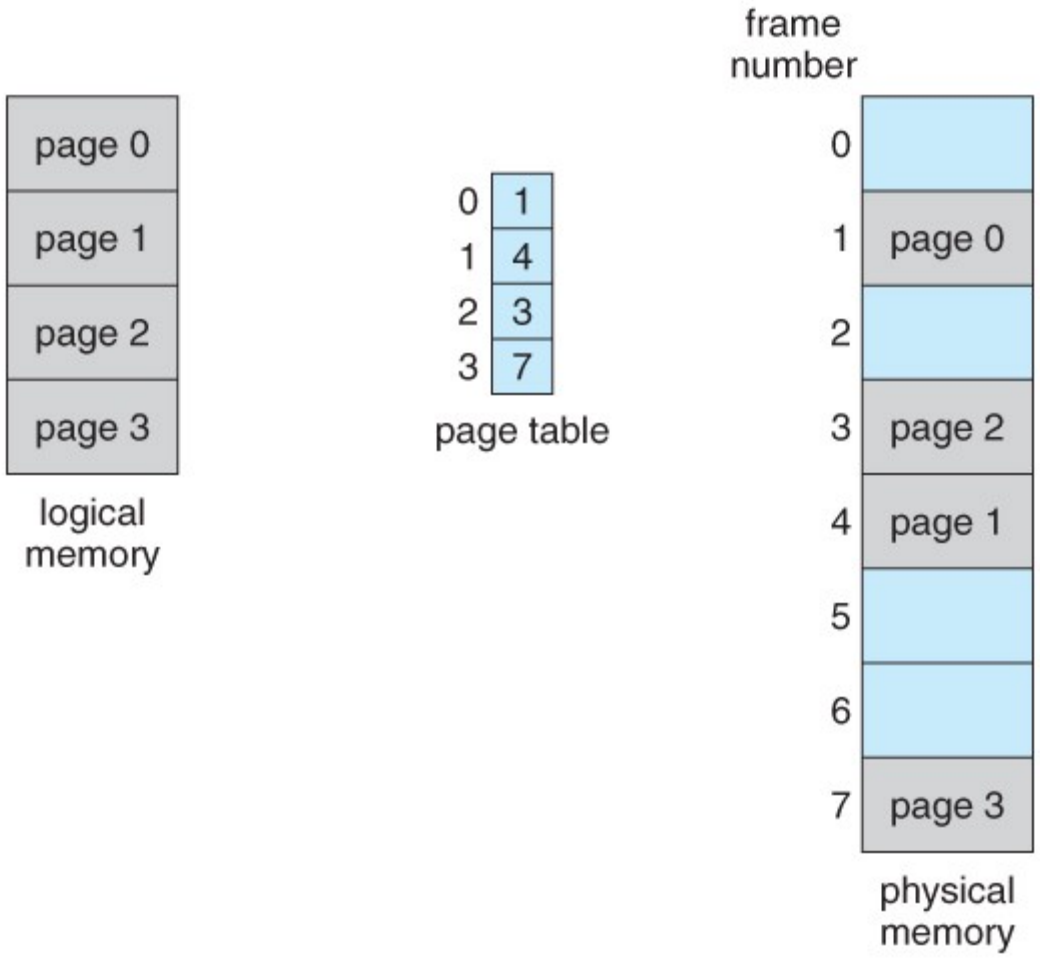
Memory

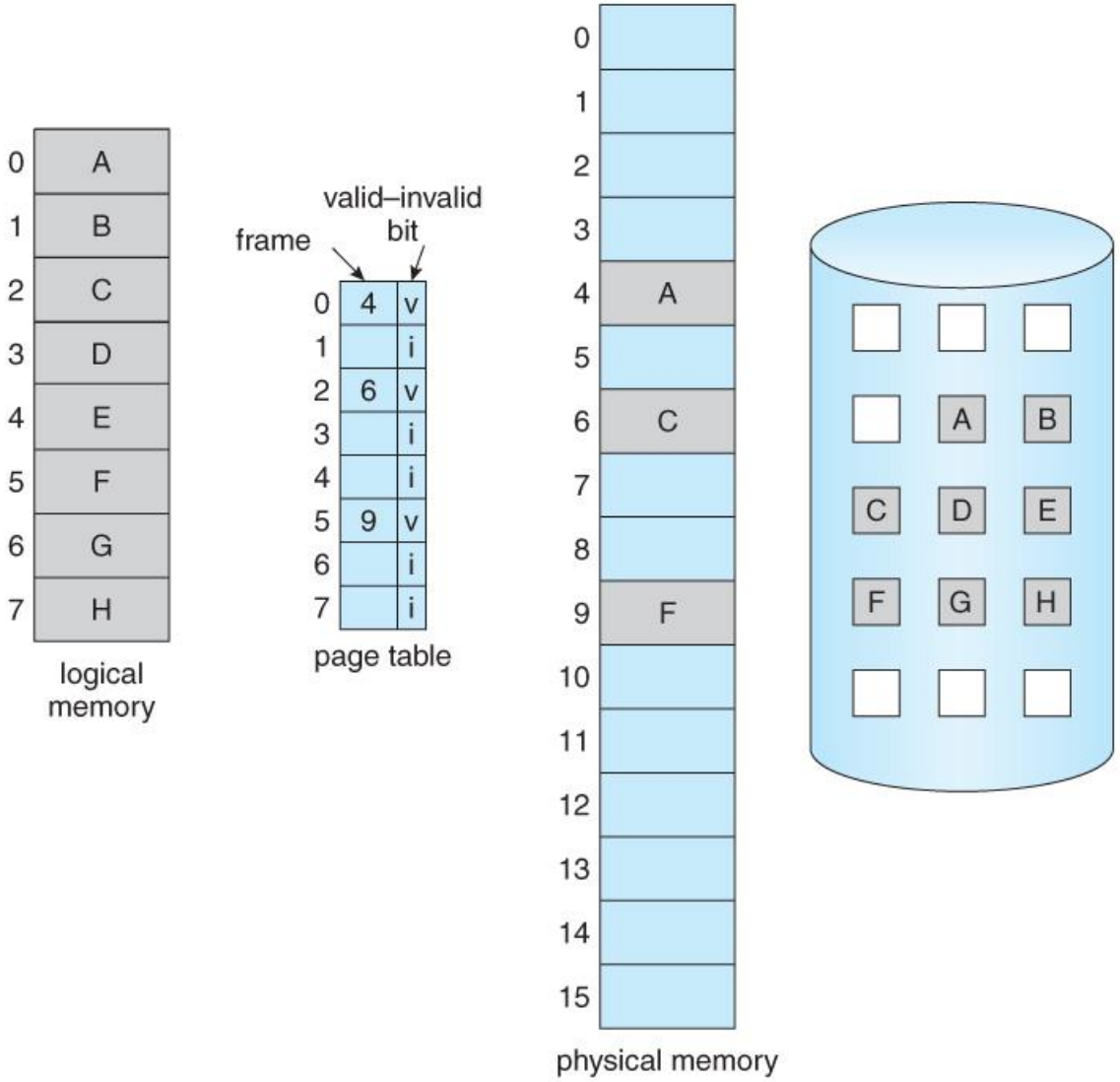

page 0
page 1
page 2
page v
virtual memory
memory map
physical memory

Why is Memory Valuable?

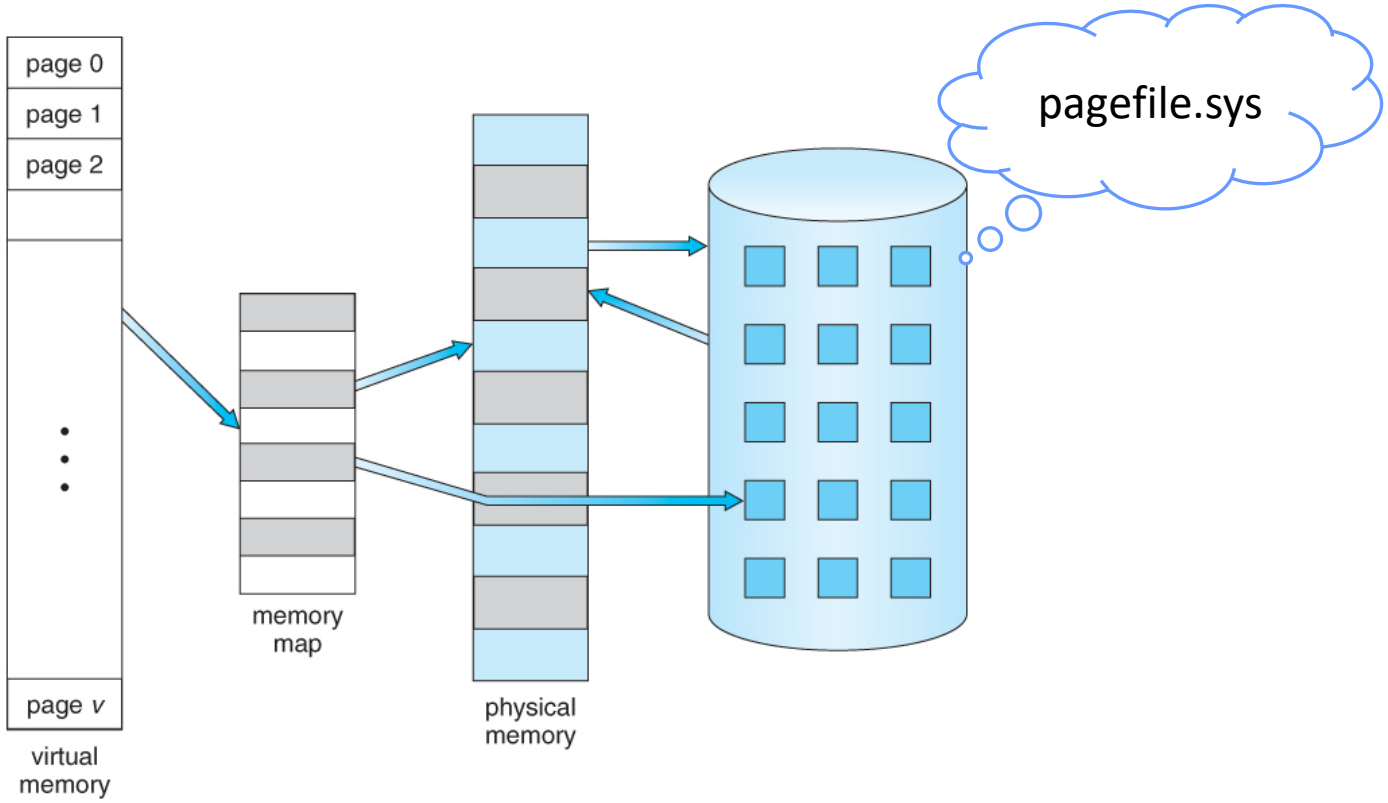
It is hard for a suspect that was arrested sitting in front of his computer to claim that some one else was responsible for the information found in the computer memory.

When viewing encrypted data in a decrypted format, the decrypt ed version of the data is temporarily stored in memory— this makes the memory a good place to find encrypted information in a decrypted state.

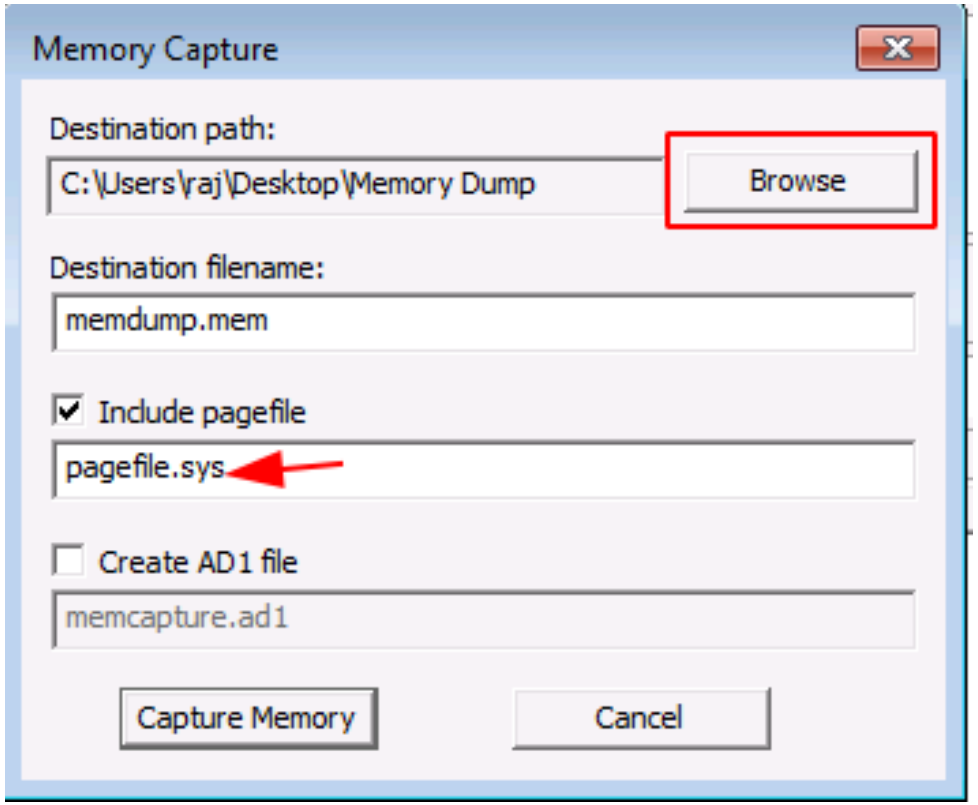

page 0
page 1
page 2
page 3
logical memory
0 1
1 4
2 3
3 7
page table
frame number
0
1 page 0
2
3 page 2
4 page 1
5
6
7 page 3
physical memory


0 A
1 B
2 C
3 D
4 E
5 F
6 G
7 H
logical memory
frame
valid–invalid bit
0 4 v
1 i
2 6 v
3 i
4 i
5 9 v
6 i
7 i
page table
0
1
2
3
4 A
5
6 C
7
8
9 F
10
11
12
13
14
15
physical memory
A B
C D E
F G H

Memory and Paging



Pagefile.sys



Notable Forensic Artifacts

A forensic artifact is basically a piece of **information** that holds **forensic value**, meaning that it can be used to answer the question or aim of the examination.

Artifacts include pictures, word documents, text messages, or some other information where the importance is quite evident.

Notable Forensic Artifacts

What is interesting, and often **problematic**, about those artifacts is the fact that Microsoft (and other providers) provide **little or no documentation** about how those pieces of information actually work.

It is important that a forensic expert ensures that he/she understand the artifacts used to draw conclusions.

- Research is necessary if you are uncertain.

Metadata

Metadata is basically **data about data**, and most objects such as files and folders on any computer system will have metadata.

On a computer running Windows and the NTFS file system, the file system will record metadata for every file created on the computer.

This metadata will include information such as:

- Creation date,
- Last modified date,
- Author (who created the file),
- Etc.

Three Types of Metadata

Descriptive	Descriptive metadata is basic information, who, what, when and where.	Time and date of creation. Creator or author of the data Location on a device where the data was created File size
Structural	Metadata about containers of data and indicates how compound objects are put together	Types, Versions, Relationships How pages are ordered to form chapters
Administrative	Owners, Rights, Licenses	
	Permissions	

Metadata

Several file types will store additional metadata.

For instance, Microsoft Office files will store information about:

- The author's name,
- Title of the document,
- How many times it has been modified,
- Etc.

EXIF Data

EXIF data is metadata stored in **pictures**

EXIF data was originally developed to help photographers record when they took a certain picture, what camera they used, and what settings they used.

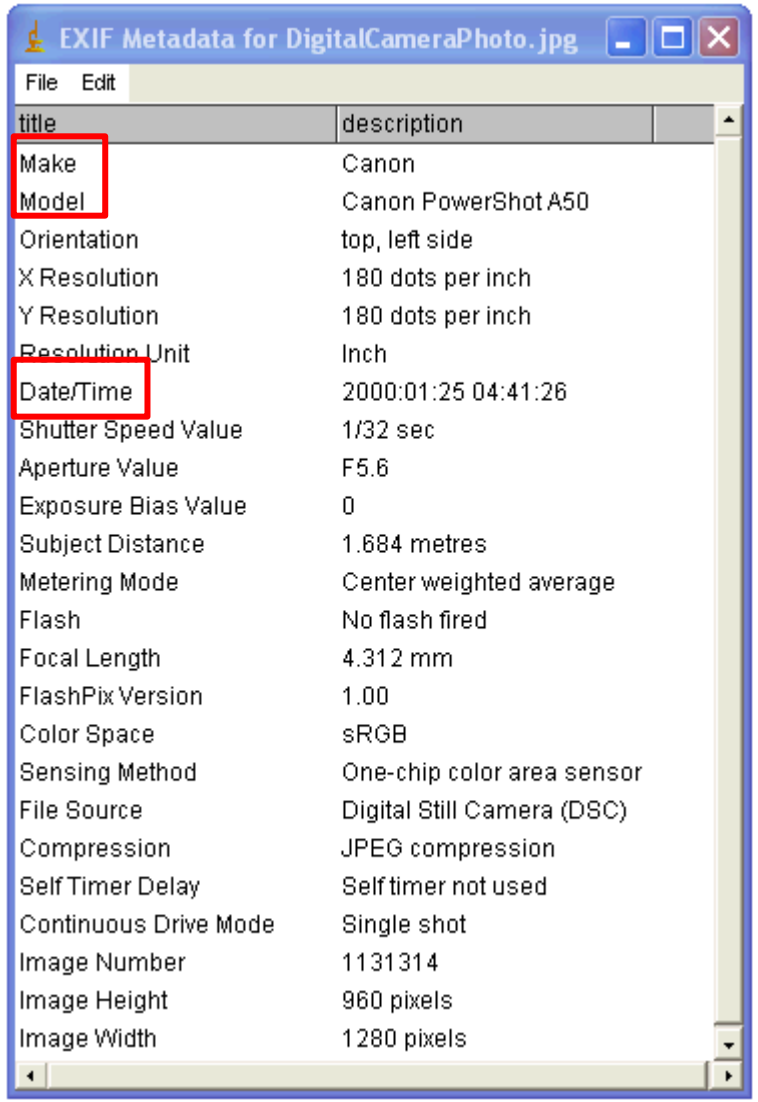
The data stored as EXIF data is also very valuable to a forensic examiner.

Camera manufacturer	Canon
Camera model	Canon EOS 1200D
Author	Praveen. P
Exposure time	1/60 sec (0.016666666666667)
F-number	f/11
ISO speed rating	200
Date and time of data generation	22:29, 22 November 2018
Lens focal length	41 mm
Show extended details	

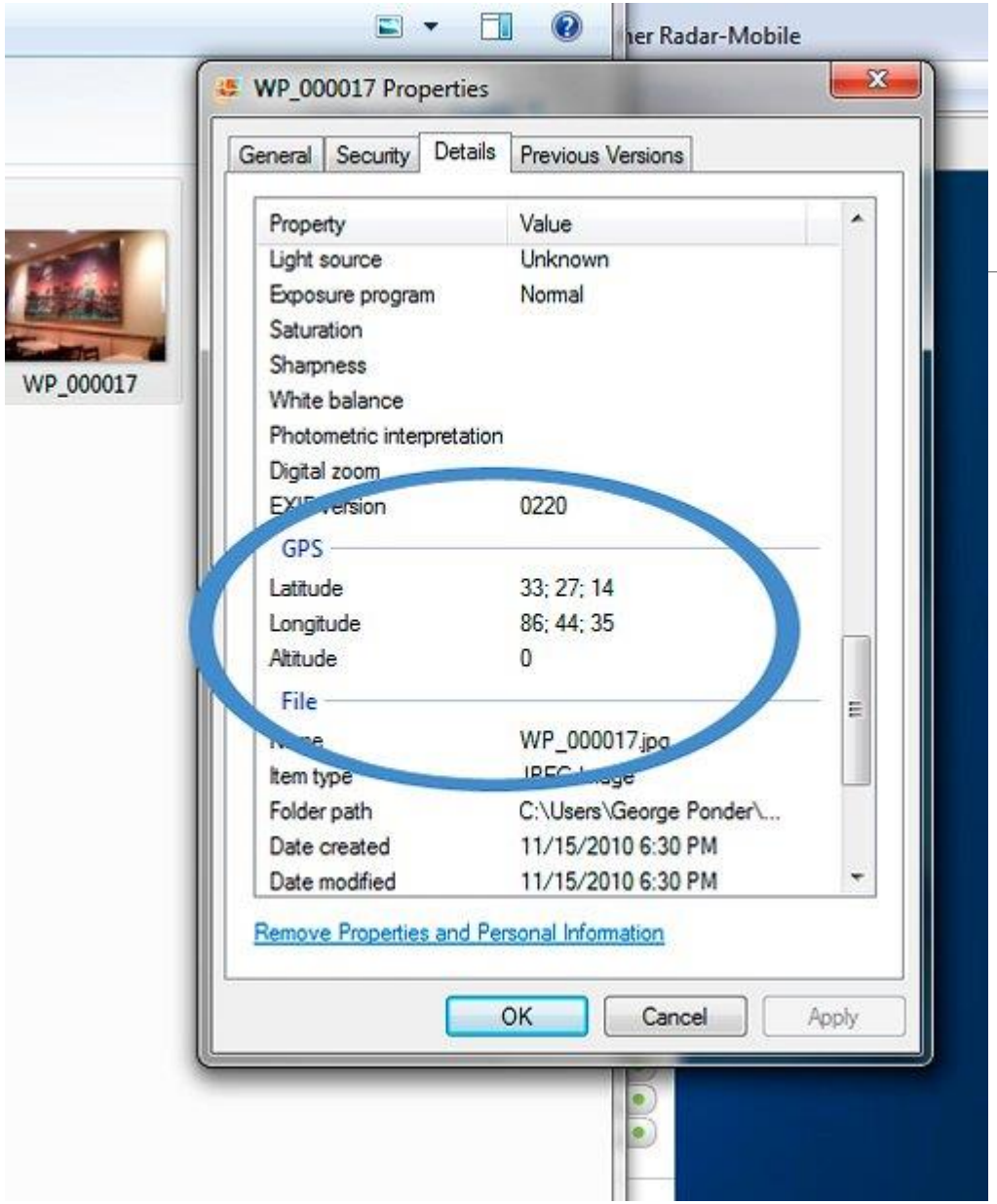
Hold on

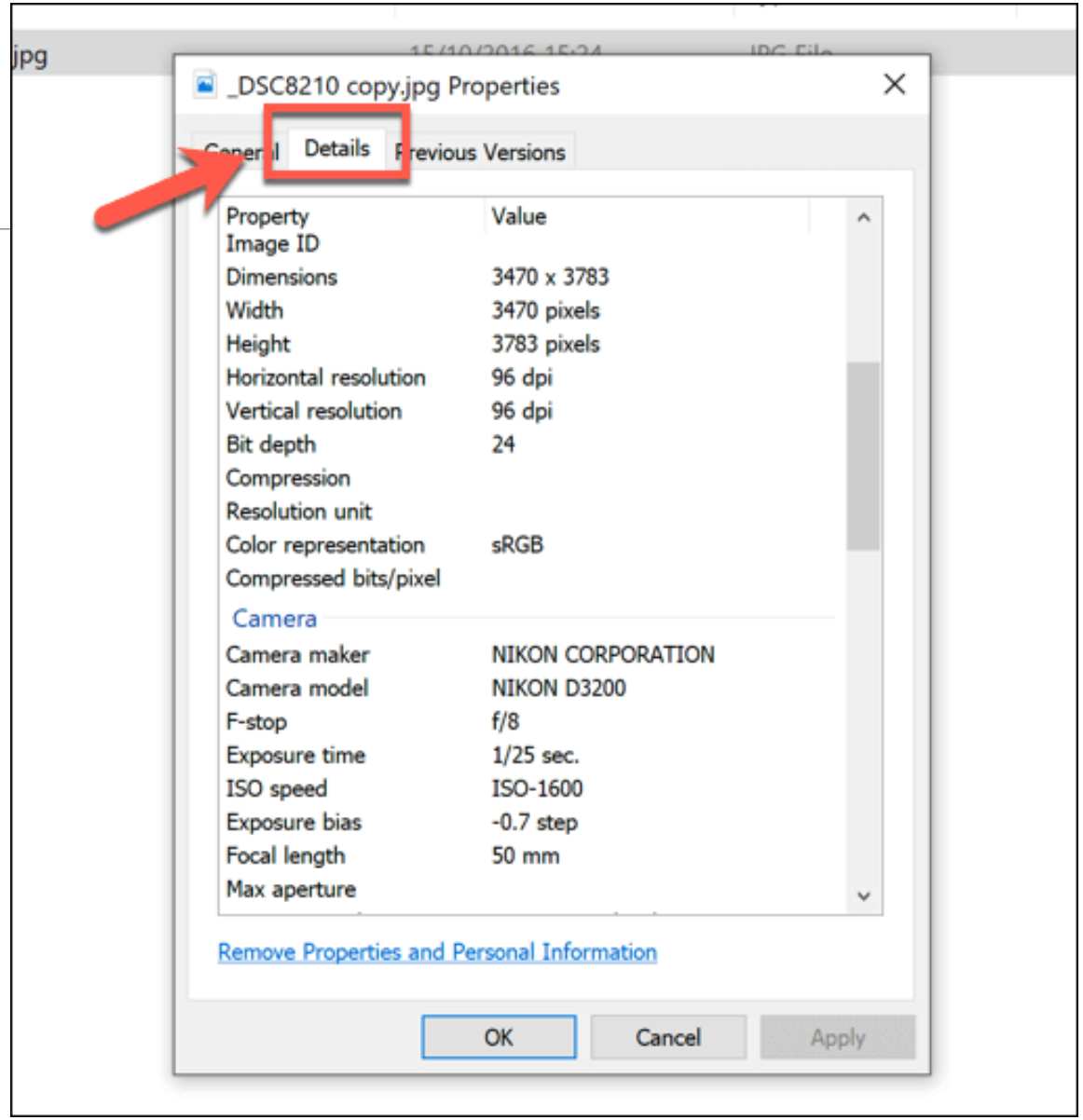
It is up to the camera manufacturer to decide what information to store as EXIF data, and it is often possible for a user to turn off the storage of this information.

Also, web sites commonly exclude EXIF data when pictures are published online.



title	description
Make	Canon
Model	Canon PowerShot A50
Orientation	top, left side
X Resolution	180 dots per inch
Y Resolution	180 dots per inch
Resolution Unit	Inch
Date/Time	2000:01:25 04:41:26
Shutter Speed Value	1/32 sec
Aperture Value	F5.6
Exposure Bias Value	0
Subject Distance	1.684 metres
Metering Mode	Center weighted average
Flash	No flash fired
Focal Length	4.312 mm
FlashPix Version	1.00
Color Space	sRGB
Sensing Method	One-chip color area sensor
File Source	Digital Still Camera (DSC)
Compression	JPEG compression
Self Timer Delay	Self timer not used
Continuous Drive Mode	Single shot
Image Number	1131314
Image Height	960 pixels
Image Width	1280 pixels


WP_000017 Properties
General
Security
Details
Previous Versions
Property
Value
Light source
Unknown
Exposure program
Normal
Saturation
Sharpness
White balance
Photometric interpretation
Digital zoom
0220
GPS
Latitude
33; 27; 14
Longitude
86; 44; 35
Altitude
0
File
WP_000017.jpg
Folder path
C:\Users\George Ponder\...
Date created
11/15/2010 6:30 PM
Date modified
11/15/2010 6:30 PM
Remove Properties and Personal Information
OK
Cancel
Apply
WP_000017


_DSC8210 copy.jpg Properties
Details
Previous Versions
Property
Value
Image ID
Dimensions
3470 x 3783
Width
3470 pixels
Height
3783 pixels
Horizontal resolution
96 dpi
Vertical resolution
96 dpi
Bit depth
24
Compression
Resolution unit
Color representation
sRGB
Compressed bits/pixel
Camera
Camera maker
NIKON CORPORATION
Camera model
NIKON D3200
F-stop
f/8
Exposure time
1/25 sec.
ISO speed
ISO-1600
Exposure bias
-0.7 step
Focal length
50 mm
Max aperture
Remove Properties and Personal Information
OK
Cancel
Apply

Prefetch

Prefetching, in Windows terminology, is the process of bringing data and code pages into memory **before** it is needed.

The idea is to track normal application usage and load the data that an application usually needs during runtime when the application is loaded.

This process was implemented to increase performance of applications that are used in a similar manner every time they are used.

How can this be used?

Prefetch data is stored in prefetch files located in the “Prefetch” folder under the system root (commonly c:\Windows).

The most significant function of the prefetch files, from a forensic perspective, is that they contain information about

- **how many** times an executable was run,
- and **when** it was **last** run.

Windows › prefetch ›

Search prefetch

Name	Date modified	Typ
ReadyBoot	19-03-2020 20:20	File
_IU14D2N.TMP-4C0C1AF7.pf	26-03-2020 05:21	PF
AACT_NETWORK_X64.EXE-1B75573B.pf	19-03-2020 23:29	PF
ACCOUNTSCONTROLHOST.EXE-110FD91...	09-04-2020 04:04	PF
ANYDESK.EXE-9B0515A7.pf	27-04-2020 00:46	PF
APPLICATIONFRAMEHOST.EXE-CCEEF75...	26-04-2020 20:54	PF
ASWOFFERTOOL.EXE-D136F81F.pf	26-04-2020 20:51	PF
AUDIODG.EXE-BDFD3029.pf Winosbite	27-04-2020 03:53	PF
AVAST FREE - 3RD APRIL 2020.E-6A82179...	03-04-2020 07:03	PF
AVAST_FREE_ANTIVIRUS_SETUP_ON-3B17...	03-04-2020 06:59	PF
AVASTBROWSERUNINSTALL.EXE_{5A-ED5...	04-04-2020 05:00	PF
AVASTUI.EXE-56B29A0A.pf	26-04-2020 21:56	PF

The file name of a prefetch file begins with the **name of the executable** followed by a hash of the location; where the executable is stored.

2487E885.pf	12/17/2016 10:40 PM	PF File	3 KB
E-5349D2D7.pf	12/28/2016 9:37 PM	PF File	7 KB
ME.EXE-5349D2D8.pf	12/28/2016 9:50 PM	PF File	10 KB
OME.EXE-5349D2D9.pf	12/16/2016 9:34 PM	PF File	20 KB
ROME.EXE-5349D2DA.pf	12/28/2016 9:26 PM	PF File	15 KB
CHROME.EXE-5349D2DD.pf	12/28/2016 12:18 AM	PF File	7 KB
CHROME.EXE-5349D2DE.pf	12/28/2016 9:37 PM	PF File	7 KB
CHROME.EXE-5349D2DF.pf	12/28/2016 9:37 PM	PF File	9 KB
CITRIXONLINELAUNCHER.EXE-73AE6288.pf	12/14/2016 11:40 AM	PF File	14 KB
CLEAR.EXE-34BAE403.pf	12/25/2016 3:35 PM	PF File	3 KB
CLEAR.EXE-F98CBA81.pf	12/17/2016 10:40 PM	PF File	4 KB
CMD.EXE-0BD30981.pf	12/24/2016 6:16 PM	PF File	4 KB
CMD.EXE-6D6290C5.pf	12/28/2016 6:19 PM	PF File	5 KB
CMP.EXE-D222ADA0.pf	12/17/2016 11:23 AM	PF File	3 KB

Prefetch

There will be a "**modified**" time stamp for the prefetch file, and that time stamp reflects the last runtime of the application, as the prefetch file is updated when the application is executed.

The data in the prefetch file contains information about how many times the application was used, what hard drive it resides on, and what files and directories it referenced.

The data format is somewhat cumbersome to read, but there are several good and free to use parsers available.

Prefetch Viewer

Help

Drive Drive-C:\

Application Name	Run Count	Last Run Time	File size	Prefetch File	Prefetch Hash
WMIPRVSE.EXE	278	May-12-14, 12:19:46 PM	31.84 KB	WMIPRVSE.EXE-8DDA8D43.pf	8DDA8D43
CONSENT.EXE	419	May-12-14, 10:11:32 AM	87.96 KB	CONSENT.EXE-1A8D0661.pf	1A8D0661
CSRSS.EXE	3381	May-09-14, 11:17:43 AM	19.51 KB	CSRSS.EXE-5B81FB65.pf	5B81FB65
MT.EXE	729	May-12-14, 1:30:26 PM	22.13 KB	MT.EXE-4FAC4D28.pf	4FAC4D28
NOTEPAD.EXE	31	May-12-14, 10:10:26 AM	23.55 KB	NOTEPAD.EXE-9FB27C0E.pf	9FB27C0E
NTOSBOOT	86	March-28-14, 9:10:35 AM	3.02 MB	NTOSBOOT-B00DFAAD.pf	B00DFAAD
SEARCHFILTERHOST.EXE	24376	March-28-14, 5:08:33 PM	16.49 KB	SEARCHFILTERHOST.EXE-44162447.pf	44162447
SEARCHFILTERHOST.EXE	4276	May-12-14, 1:41:41 PM	16.50 KB	SEARCHFILTERHOST.EXE-DDB228B1.pf	DDB228B1

Mapped Files | Mapped Directories

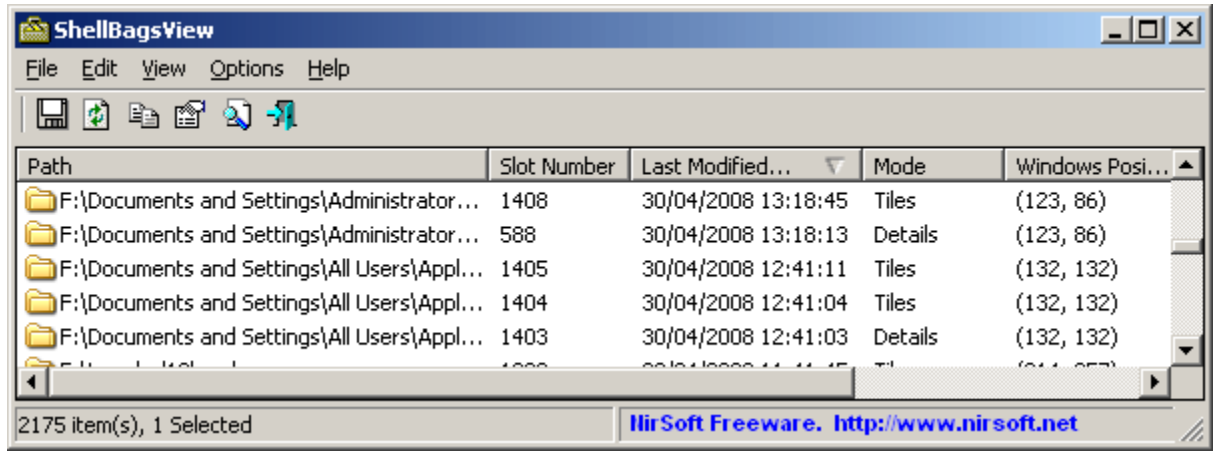
File Name	File Path
$MFT	\DEVICE\HARDDISKVOLUME5\$MFT
ADVAPI32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\ADVAPI32.DLL
APISETSCHEMA.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
BASEBRD.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\BRANDING\BASEBRD\BASEBRD.DLL
BROWCLI.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\BROWCLI.DLL
CFGMGR32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CFGMGR32.DLL
CIMWIN32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\WBEM\CIMWIN32.DLL
CLBCATQ.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CLBCATQ.DLL
CREDSSP.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CREDSSP.DLL
CRYPT32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CRYPT32.DLL
CRYPTBASE.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CRYPTBASE.DLL
CRYPTSP.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CRYPTSP.DLL

```
PS C:\Users\joaki\Downloads\PECmd> .\PECmd.exe -f .\CMD.EXE-4A81B364.pf
PECmd version 0.9.2.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f .\CMD.EXE-4A81B364.pf

Keywords: temp, tmp

Processing '.\CMD.EXE-4A81B364.pf'

Created on: 2018-03-14 11:12:48
Modified on: 2018-03-14 11:09:56
Last accessed on: 2018-03-14 11:12:48

Executable name: CMD.EXE
Hash: 4A81B364
File size (bytes): 6 292
Version: Windows 10

Run count: 2
Last run: 2018-03-14 11:09:56
Other run times: 2018-03-14 11:09:56

Volume information:

#0: Name: \VOLUME{01d3bb8869f25d67-5c6a9abc} Serial: 5C6A9ABC Created: 2018-03-14 11:34:29
 Directories: 3 File references: 11

Directories referenced: 3

0: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS
1: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM~2
2: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM 2\EN-US

Files referenced: 8

0: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM32\NTDLL.DLL
1: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM32\CMD.EXE
2: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM32\KERNEL32.DLL
3: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM32\KERNELBASE.DLL
4: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM32\LOCALE.NLS
5: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM32\MSVCRT.DLL
6: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM32\EN-US\CMD.EXE.MUI
7: \VOLUME{01d3bb8869f25d67-5c6a9abc}\WINDOWS\SYSTEM32\EN-US\KERNELBASE.DLL.MUI

Processed '.\CMD.EXE-4A81B364.pf' in 0.03577850 seconds
```

Shellbags

Shellbags are used to store information about GUI settings for explorer that is used to browse files and folders on a Windows-based computer.

That means that they store information about what **preferences** a user sets for **viewing** certain directories. This can, for instance, be how to list files in the directory.



Shellbags

The forensic significance of these artifacts comes from:

- A shellbag for a certain folder is created when a user is **actually viewing** that folder. Thus, the **existence** of a shellbag for a certain folder is a very good indication that the user in question has visited that particular folder.
- The shellbags are stored in NTUser.dat and another user-specific file called UsrClass.dat, located in . . ./AppData/Local/Microsoft/Windows/UsrClass.dat. That makes the shellbag data **user specific**.
- It is known that shellbags are not deleted and can therefore serve as **evidence of deleted folders.**
- Can provide information about network shares, mounted encrypted volumes, and removable media.


Thank
you!