FORFUN

Week 6 Registry Forensics
Soraya Harding & Rahim Taheri

Session Content

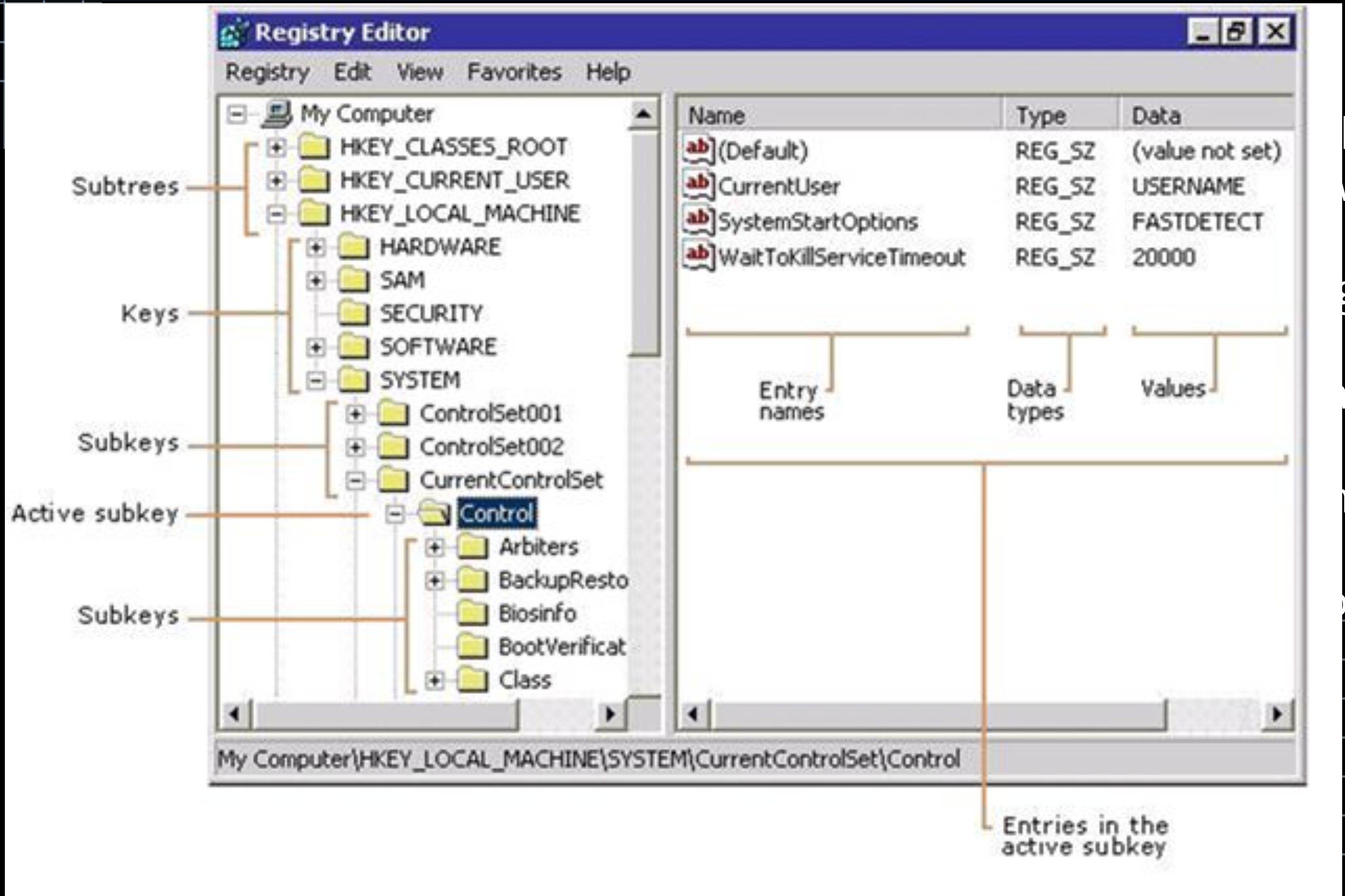
- Introduction to Windows Registry
- Registry Forensics
- Interesting Registry Settings
- Conclusions

Introduction to Registry

Windows Registry

- The Windows Registry is a hierarchical database that contains all of the configurations and settings used by components, services, applications, and pretty much everything in Windows.
- Information can be recovered from registry, such as files opened, programs executed, users, passwords, devices that are connected to the computer

Registry Organization



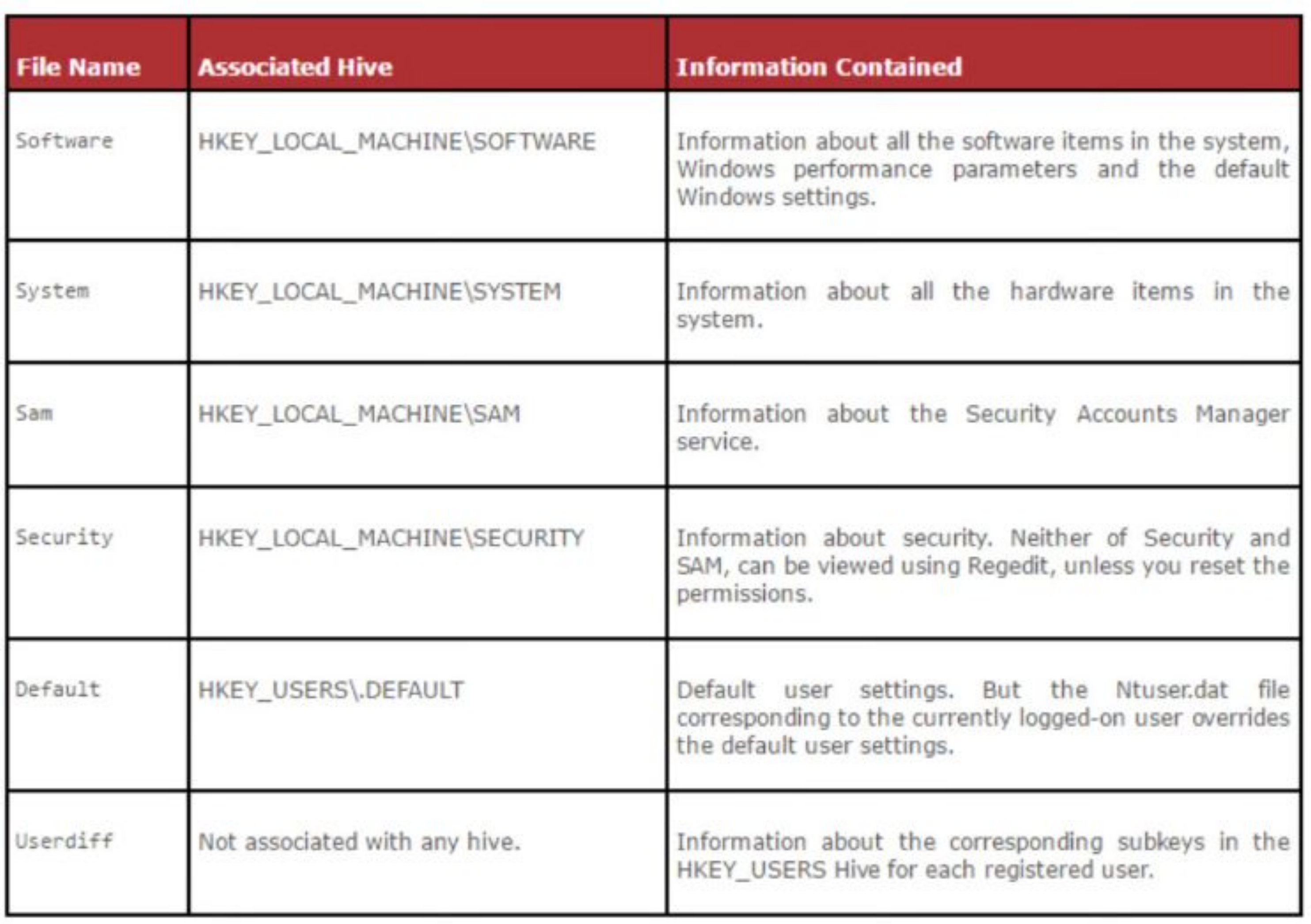
- My Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
    - HARDWARE
    - SAM
    - SECURITY
    - SOFTWARE
    - SYSTEM
      - ControlSet001
      - ControlSet002
      - CurrentControlSet
        - Control
          - Arbiters
          - BackupResto
          - Biosinfo
          - BootVerificat
          - Class

Name	Type	Data
(Default)	REG_SZ	(value not set)
CurrentUser	REG_SZ	USERNAME
SystemStartOptions	REG_SZ	FASTDETECT
WaitToKillServiceTimeout	REG_SZ	20000

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

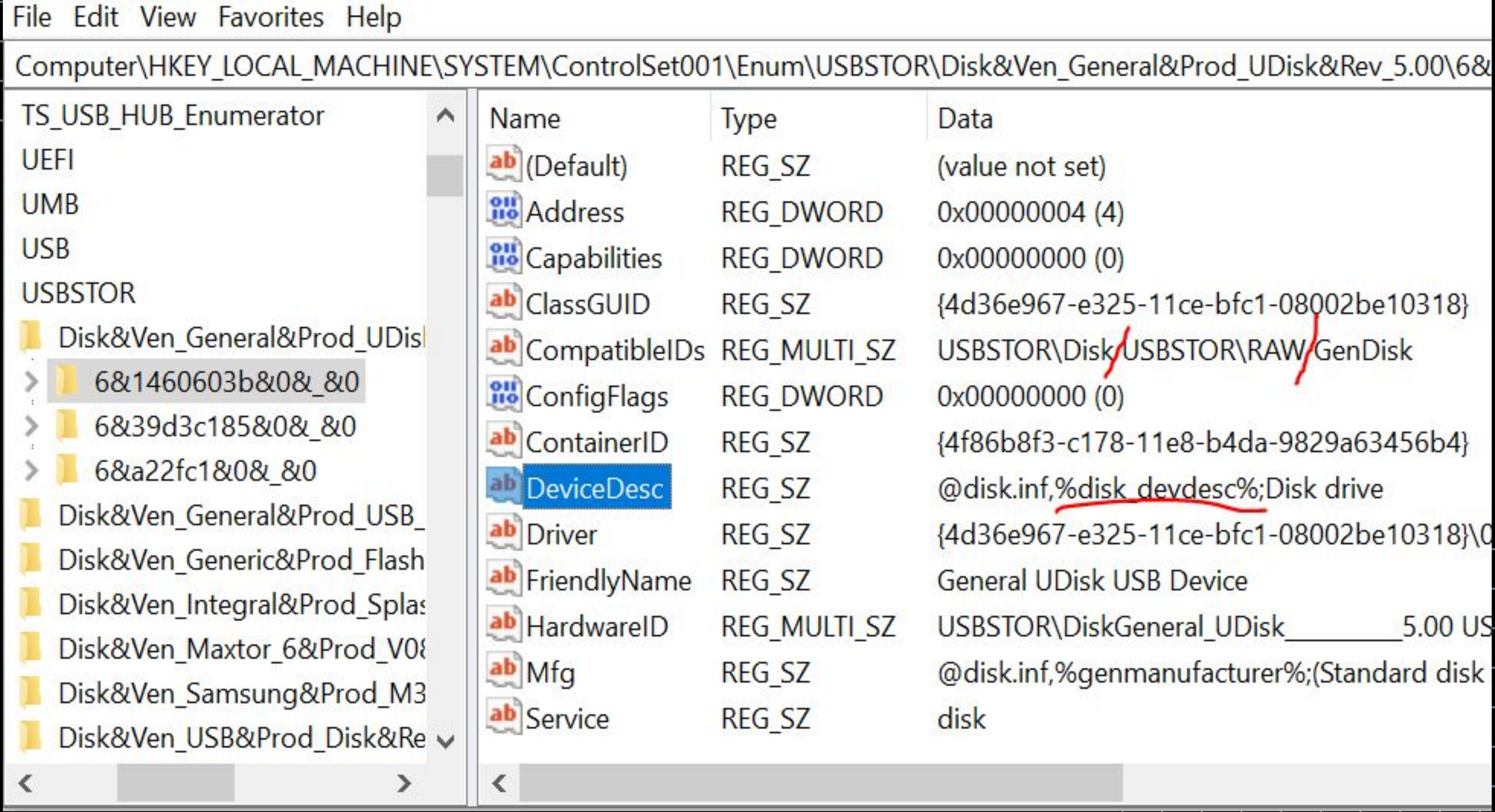
he
ws
gs,
re
nat
out
at

Local Machine



File Name	Associated Hive	Information Contained
Software	HKEY_LOCAL_MACHINE\SOFTWARE	Information about all the software items in the system, Windows performance parameters and the default Windows settings.
System	HKEY_LOCAL_MACHINE\SYSTEM	Information about all the hardware items in the system.
Sam	HKEY_LOCAL_MACHINE\SAM	Information about the Security Accounts Manager service.
Security	HKEY_LOCAL_MACHINE\SECURITY	Information about security. Neither of Security and SAM, can be viewed using Regedit, unless you reset the permissions.
Default	HKEY_USERS\.DEFAULT	Default user settings. But the Ntuser.dat file corresponding to the currently logged-on user overrides the default user settings.
Userdiff	Not associated with any hive.	Information about the corresponding subkeys in the HKEY_USERS Hive for each registered user.

Registry Value Types



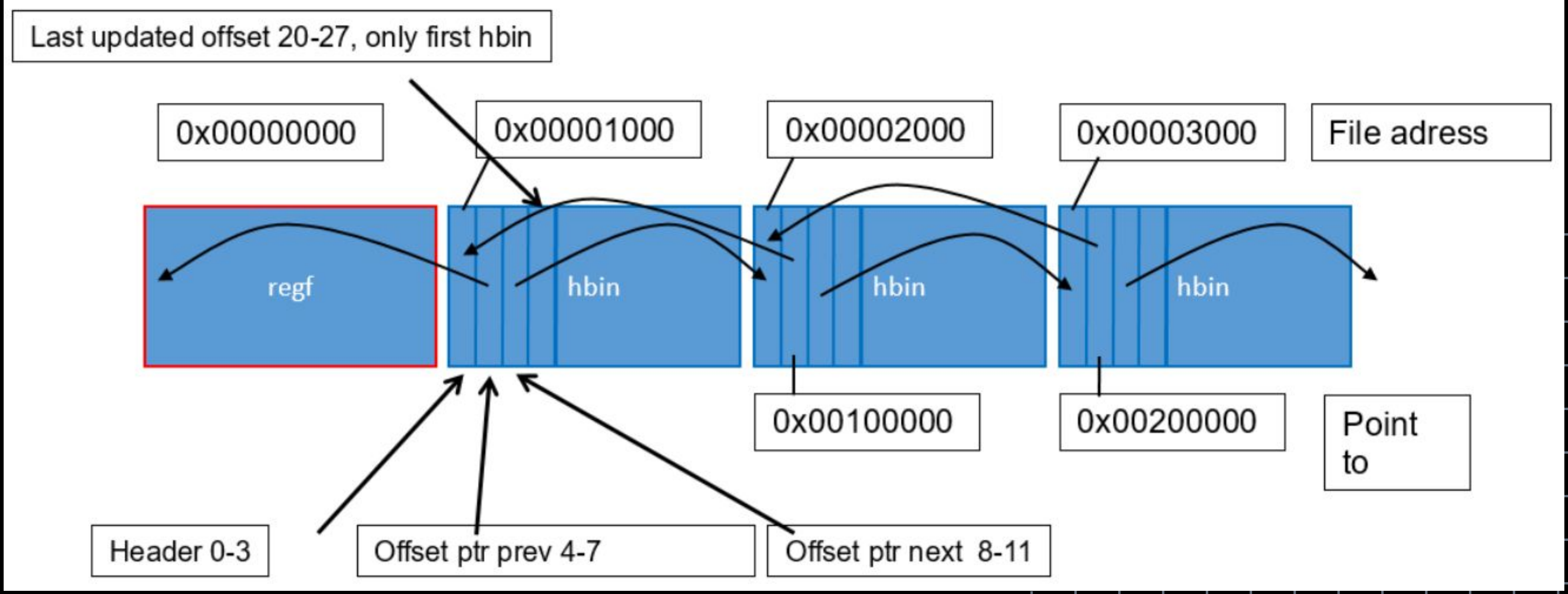
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_General&Prod_UDisk&Rev_5.00\6&

TS_USB_HUB_Enumerator
UEFI
UMB
USB
USBSTOR
Disk&Ven_General&Prod_UDisl
6&1460603b&0&_&0
6&39d3c185&0&_&0
6&a22fc1&0&_&0
Disk&Ven_General&Prod_USB_
Disk&Ven_Generic&Prod_Flash
Disk&Ven_Integral&Prod_Splas
Disk&Ven_Maxtor_6&Prod_V0
Disk&Ven_Samsung&Prod_M3
Disk&Ven_USB&Prod_Disk&Re

Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000004 (4)
Capabilities	REG_DWORD	0x00000000 (0)
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	{4f86b8f3-c178-11e8-b4da-9829a63456b4}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0
FriendlyName	REG_SZ	General UDisk USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskGeneral_UDisk________5.00 US
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk
Service	REG_SZ	disk

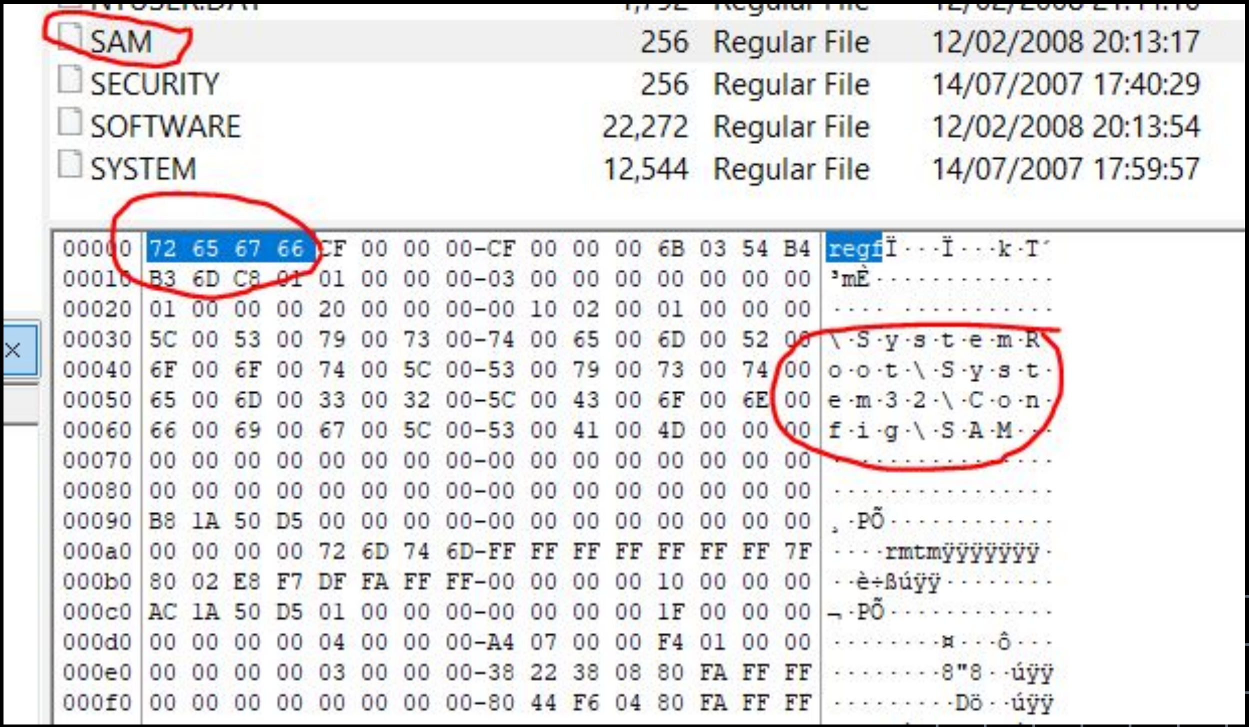
Hives

- Registry root files, contain subkeys; Made up of 4KiB sections or “bins”
- starts with regf block followed by many hbins



Regf block

- regf block: contains regf signature (offset 0-3), last updated date and time (offset 12-19) and file name and path information (variable size from offset 48)

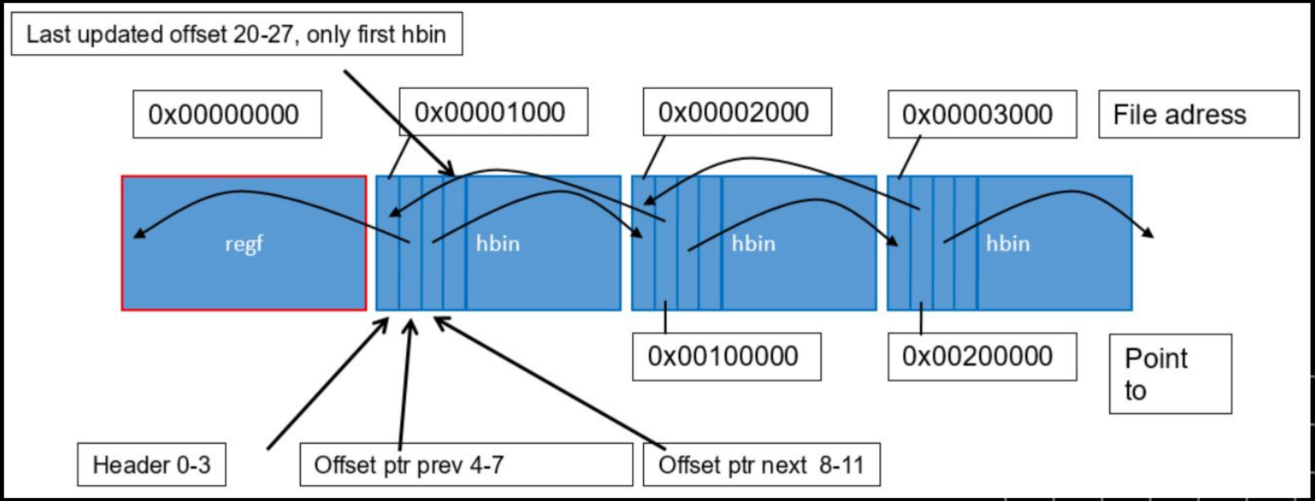


SAM	256	Regular File	12/02/2008 20:13:17
SECURITY	256	Regular File	14/07/2007 17:40:29
SOFTWARE	22,272	Regular File	12/02/2008 20:13:54
SYSTEM	12,544	Regular File	14/07/2007 17:59:57

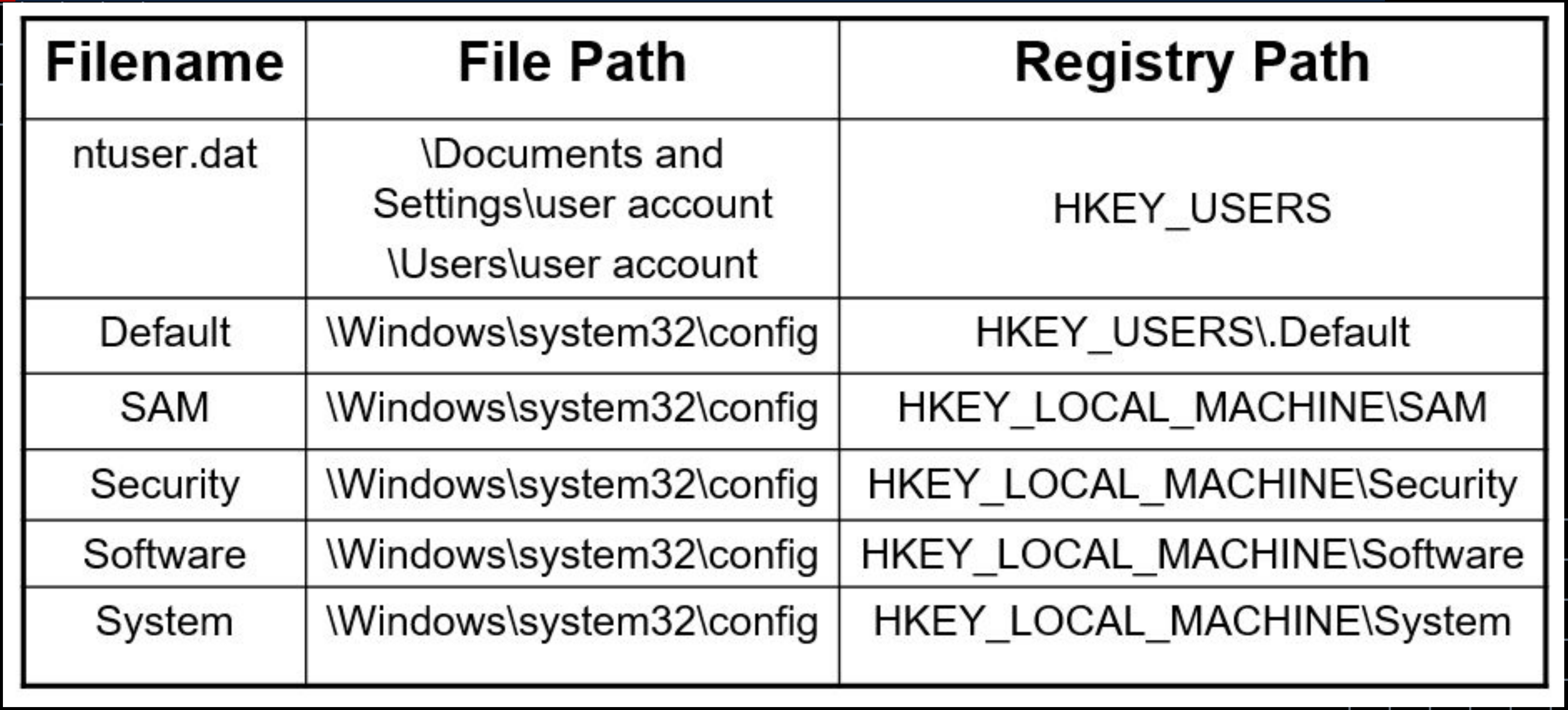
```
00000 72 65 67 66 CF 00 00 00-CF 00 00 00 6B 03 54 B4 regfÏ···Ï···k·T´
00010 B3 6D C8 01 01 00 00 00-03 00 00 00 00 00 00 00 ³mÈ·············
00020 01 00 00 00 20 00 00 00-00 10 02 00 01 00 00 00 ················
00030 5C 00 53 00 79 00 73 00-74 00 65 00 6D 00 52 00 \·S·y·s·t·e·m·R·
00040 6F 00 6F 00 74 00 5C 00-53 00 79 00 73 00 74 00 o·o·t·\·S·y·s·t·
00050 65 00 6D 00 33 00 32 00-5C 00 43 00 6F 00 6E 00 e·m·3·2·\·C·o·n·
00060 66 00 69 00 67 00 5C 00-53 00 41 00 4D 00 00 00 f·i·g·\·S·A·M···
00070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00090 B8 1A 50 D5 00 00 00 00-00 00 00 00 00 00 00 00 ¸·PÕ············
000a0 00 00 00 00 72 6D 74 6D-FF FF FF FF FF FF FF 7F ····rmtmÿÿÿÿÿÿÿ·
000b0 80 02 E8 F7 DF FA FF FF-00 00 00 00 10 00 00 00 ··è÷ßúÿÿ········
000c0 AC 1A 50 D5 01 00 00 00-00 00 00 00 1F 00 00 00 ¬·PÕ············
000d0 00 00 00 00 04 00 00 00-A4 07 00 00 F4 01 00 00 ········¤···ô···
000e0 00 00 00 00 03 00 00 00-38 22 38 08 80 FA FF FF ········8"8··úÿÿ
000f0 00 00 00 00 00 00 00 00-80 44 F6 04 80 FA FF FF ·········Dö··úÿÿ
```

hbin block

- 32 bytes header size;
- Each hbin points to the previous hbin block (offset 4-7) and to the next hbin block (offset 8-11).
- When one hbin block is filled system will make a new hbin block. The space will not be removed and data is recoverable even after deleting

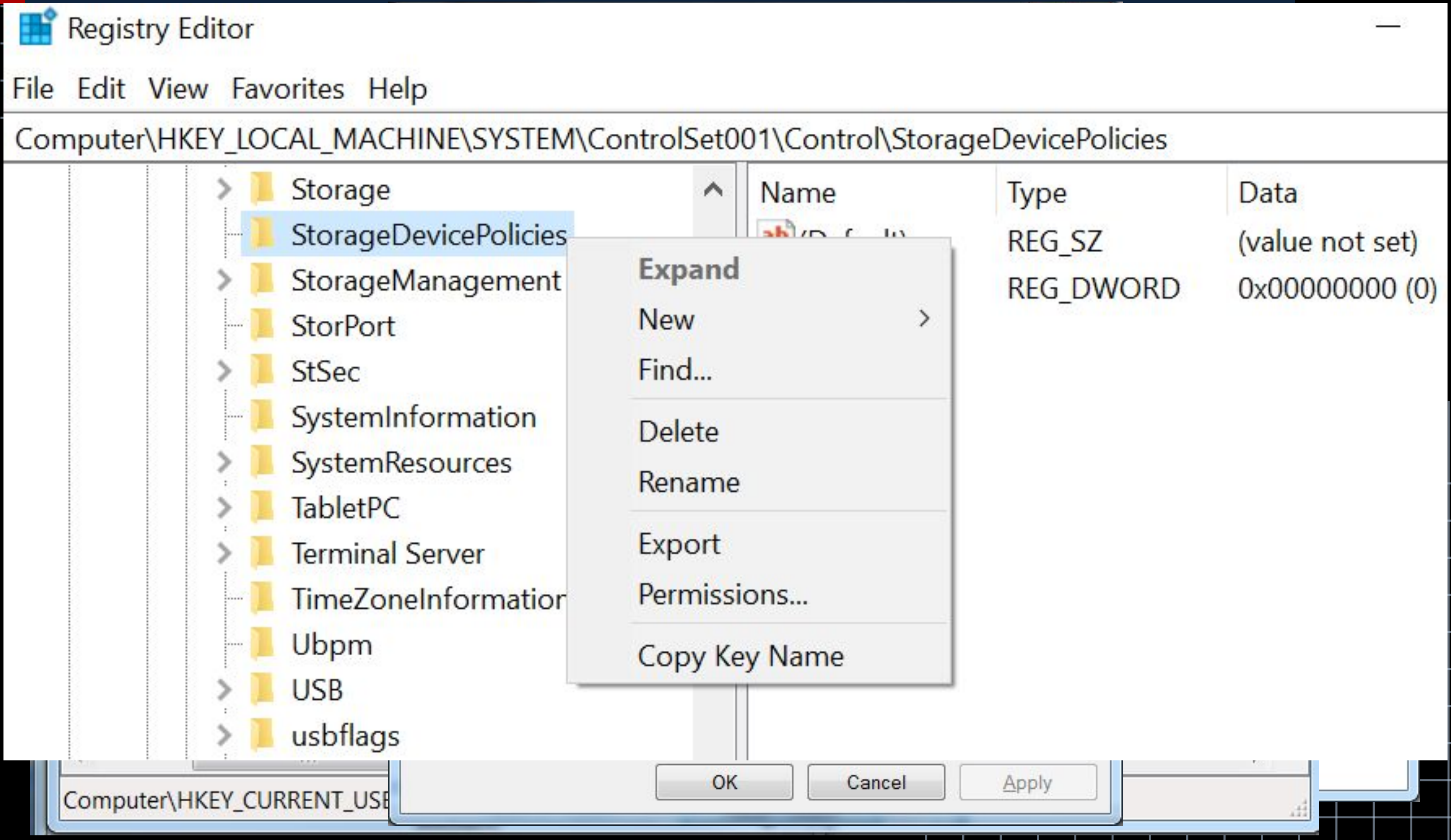


Registry Files Location



Filename	File Path	Registry Path
ntuser.dat	\Documents and Settings\user account \Users\user account	HKEY_USERS
Default	\Windows\system32\config	HKEY_USERS\.Default
SAM	\Windows\system32\config	HKEY_LOCAL_MACHINE\SAM
Security	\Windows\system32\config	HKEY_LOCAL_MACHINE\Security
Software	\Windows\system32\config	HKEY_LOCAL_MACHINE\Software
System	\Windows\system32\config	HKEY_LOCAL_MACHINE\System

Registry Modifications



Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\StorageDevicePolicies

Name	Type	Data
(Default)	REG_SZ	(value not set)
	REG_DWORD	0x00000000 (0)

Computer\HKEY_CURRENT_USE

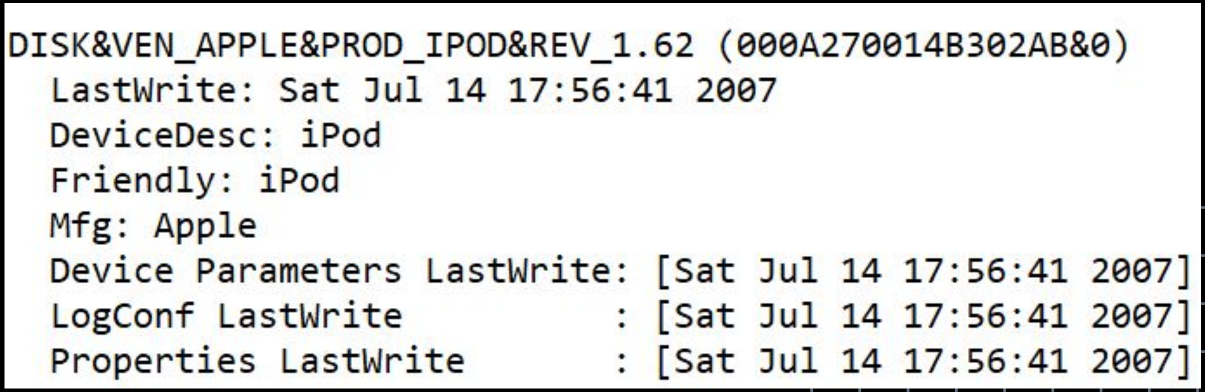
Registry Forensics

Forensic Benefits

- MRUs (most-recently-used)
- Typed URLs
- System users
- Installed devices
- Registered user information
- Passwords and hashes
- Internet search queries and form data
- Date and time information of registry keys updates
- Network and wireless setting and connection information

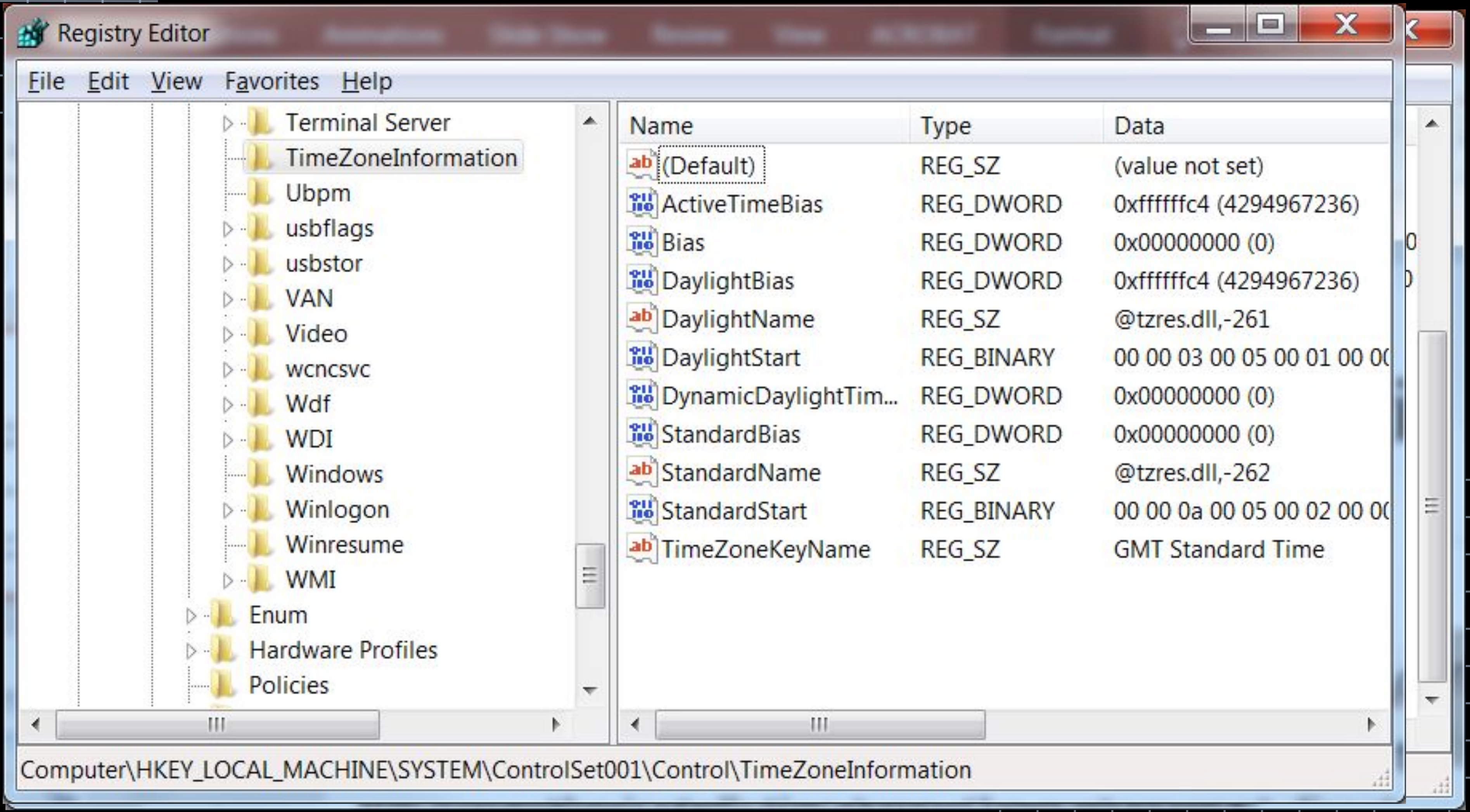
Registry as a Log File

- Registry keys have the last modified timestamp; similar to the last modification time associated with files and directories; the timestamp is updated to the current local system time when the registry key or any of its values are created, altered, or deleted.
  - Not accessible through regedit but accessible in binary, or via various tools (e.g. RegRipper, FTK's Registry Viewer)



```
DISK&VEN_APPLE&PROD_IPOD&REV_1.62 (000A270014B302AB&0)
  LastWrite: Sat Jul 14 17:56:41 2007
  DeviceDesc: iPod
  Friendly: iPod
  Mfg: Apple
  Device Parameters LastWrite: [Sat Jul 14 17:56:41 2007]
  LogConf LastWrite          : [Sat Jul 14 17:56:41 2007]
  Properties LastWrite       : [Sat Jul 14 17:56:41 2007]
```

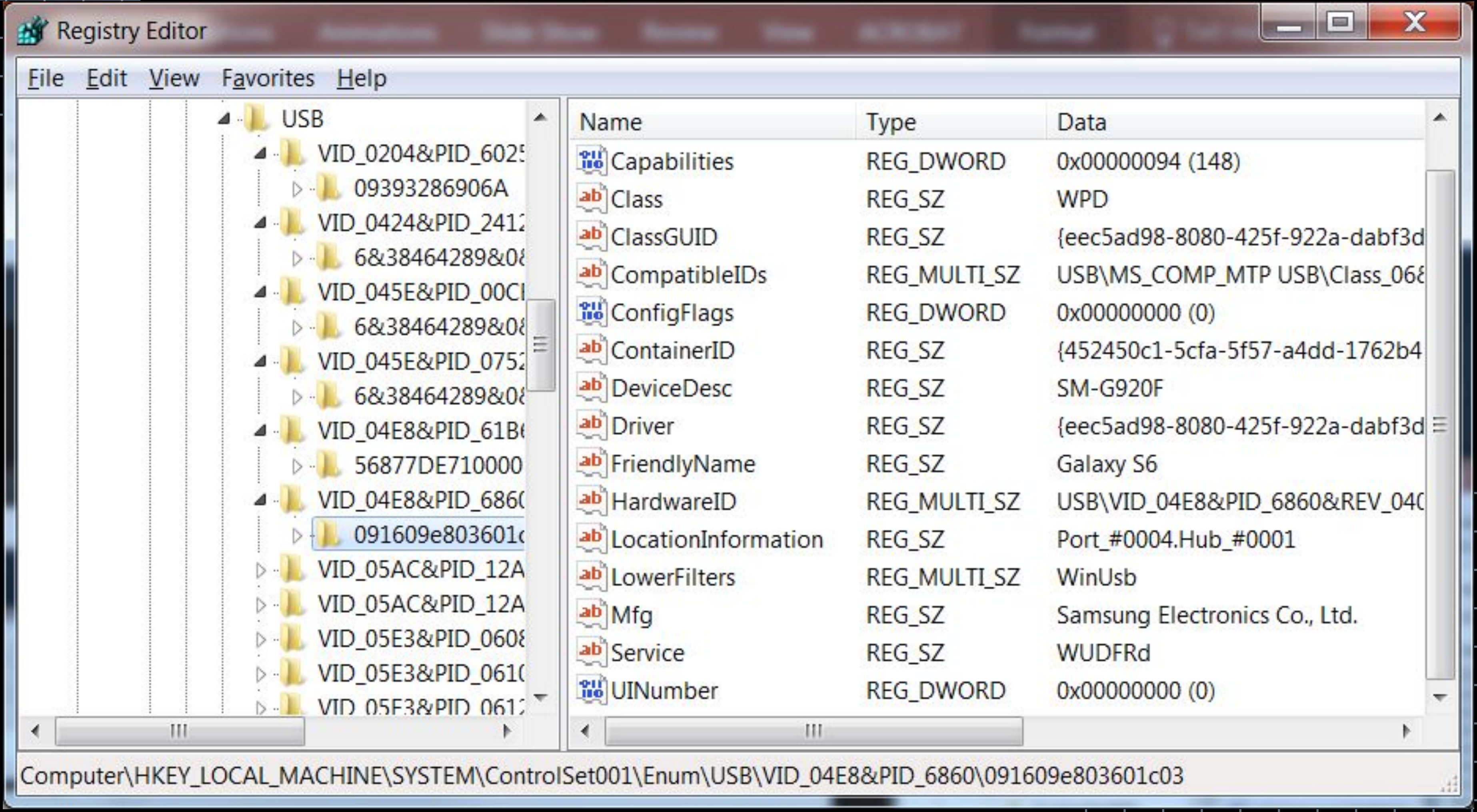
System Information



Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveTimeBias	REG_DWORD	0xffffffc4 (4294967236)
Bias	REG_DWORD	0x00000000 (0)
DaylightBias	REG_DWORD	0xffffffc4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-261
DaylightStart	REG_BINARY	00 00 03 00 05 00 01 00 0(
DynamicDaylightTim...	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-262
StandardStart	REG_BINARY	00 00 0a 00 05 00 02 00 0(
TimeZoneKeyName	REG_SZ	GMT Standard Time

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation

Attached Devices/Connected Networks

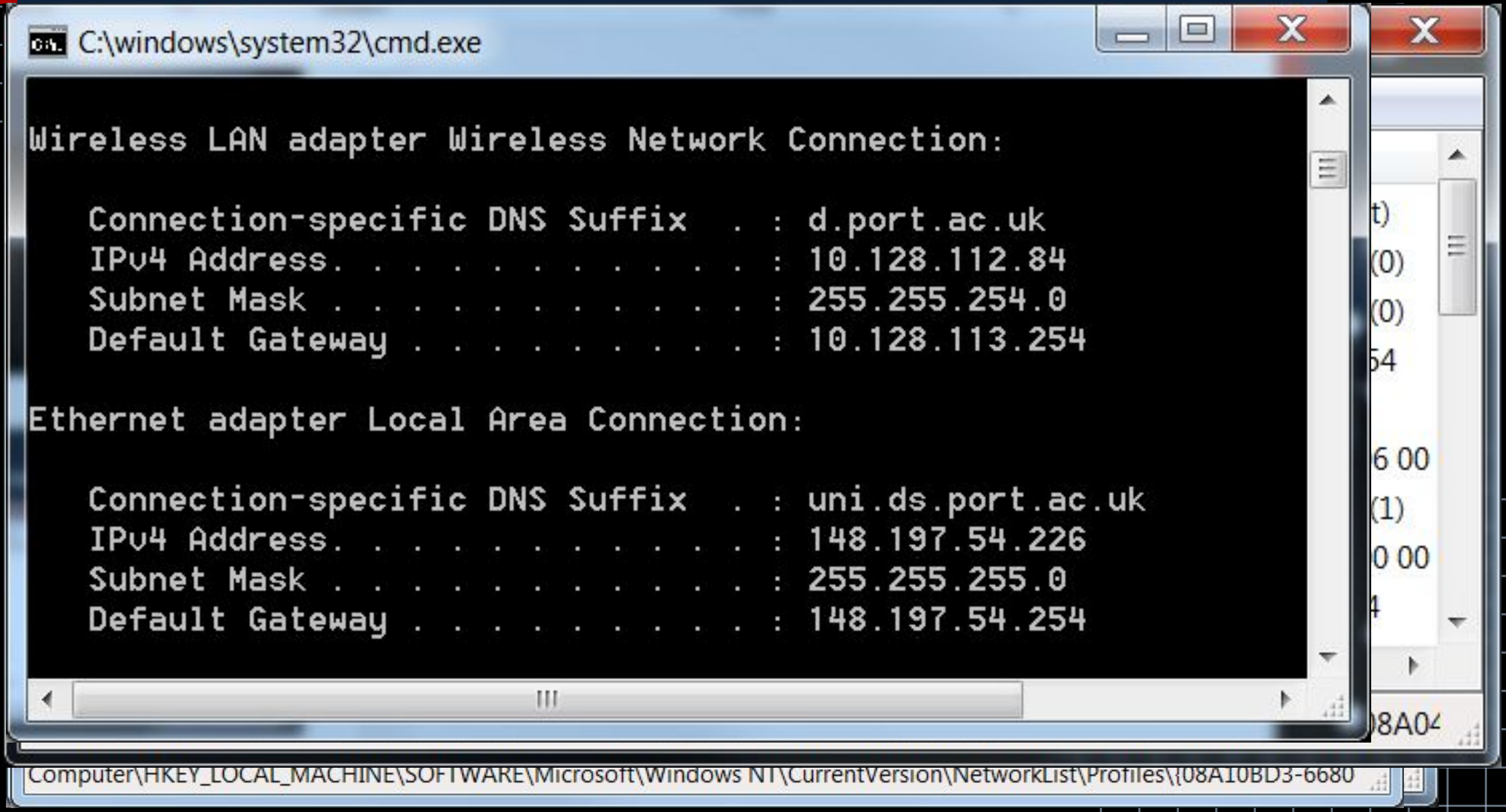


```
USB
  VID_0204&PID_6025
    09393286906A
  VID_0424&PID_2412
    6&38464289&08
  VID_045E&PID_00CI
    6&38464289&08
  VID_045E&PID_0752
    6&38464289&08
  VID_04E8&PID_61B6
    56877DE710000
  VID_04E8&PID_6860
    091609e803601c
  VID_05AC&PID_12A
  VID_05AC&PID_12A
  VID_05E3&PID_0608
  VID_05E3&PID_0610
  VID_05E3&PID_0612
```

Name	Type	Data
Capabilities	REG_DWORD	0x00000094 (148)
Class	REG_SZ	WPD
ClassGUID	REG_SZ	{eec5ad98-8080-425f-922a-dabf3d
CompatibleIDs	REG_MULTI_SZ	USB\MS_COMP_MTP USB\Class_068
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{452450c1-5cfa-5f57-a4dd-1762b4
DeviceDesc	REG_SZ	SM-G920F
Driver	REG_SZ	{eec5ad98-8080-425f-922a-dabf3d
FriendlyName	REG_SZ	Galaxy S6
HardwareID	REG_MULTI_SZ	USB\VID_04E8&PID_6860&REV_040
LocationInformation	REG_SZ	Port_#0004.Hub_#0001
LowerFilters	REG_MULTI_SZ	WinUsb
Mfg	REG_SZ	Samsung Electronics Co., Ltd.
Service	REG_SZ	WUDFRd
UINumber	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB\VID_04E8&PID_6860\091609e803601c03

Network Interfaces

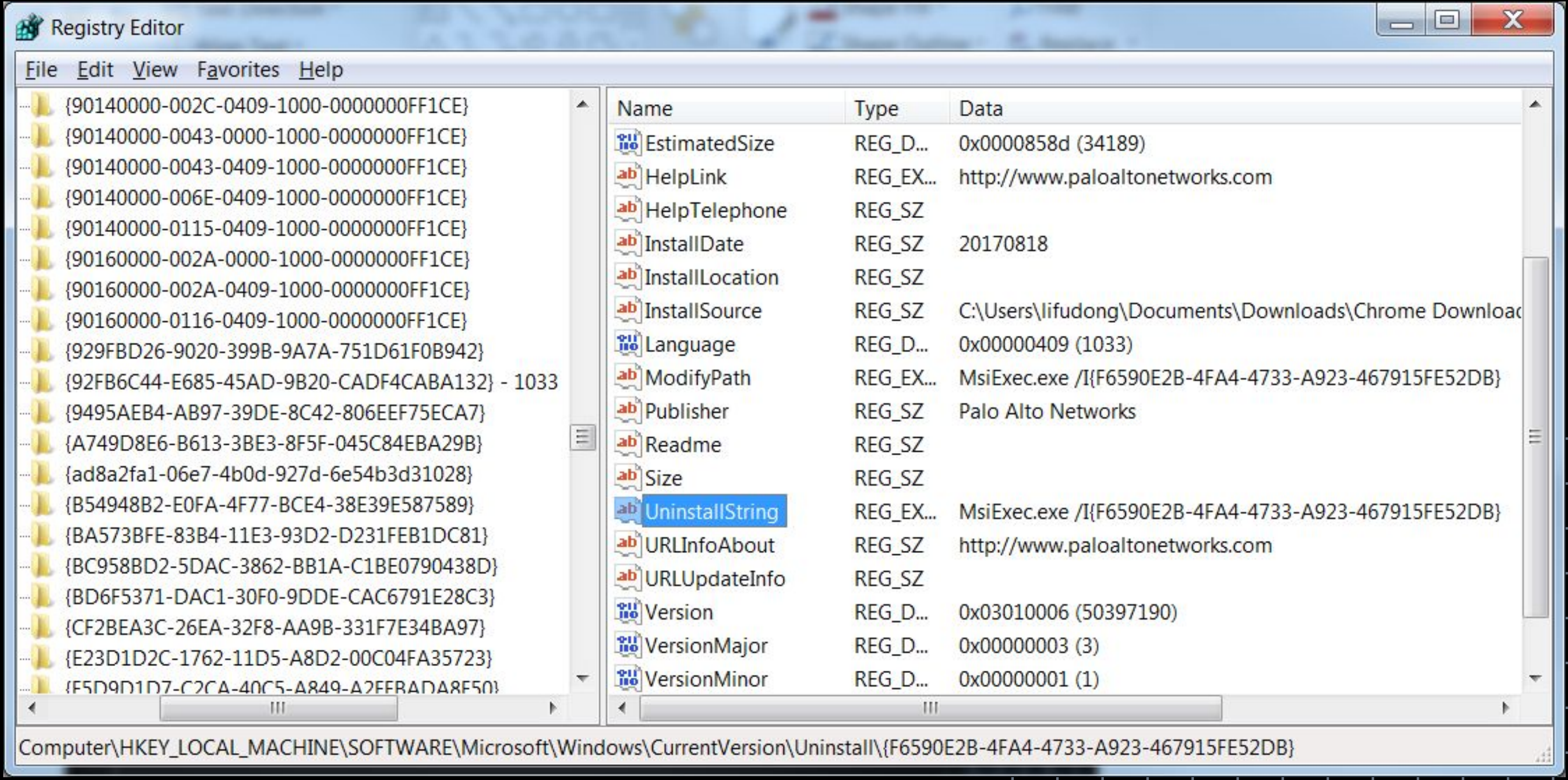


```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : d.port.ac.uk
   IPv4 Address. . . . . . . . . . . : 10.128.112.84
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 10.128.113.254

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : uni.ds.port.ac.uk
   IPv4 Address. . . . . . . . . . . : 148.197.54.226
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 148.197.54.254
```

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{08A10BD3-6680
```

Installed Software

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

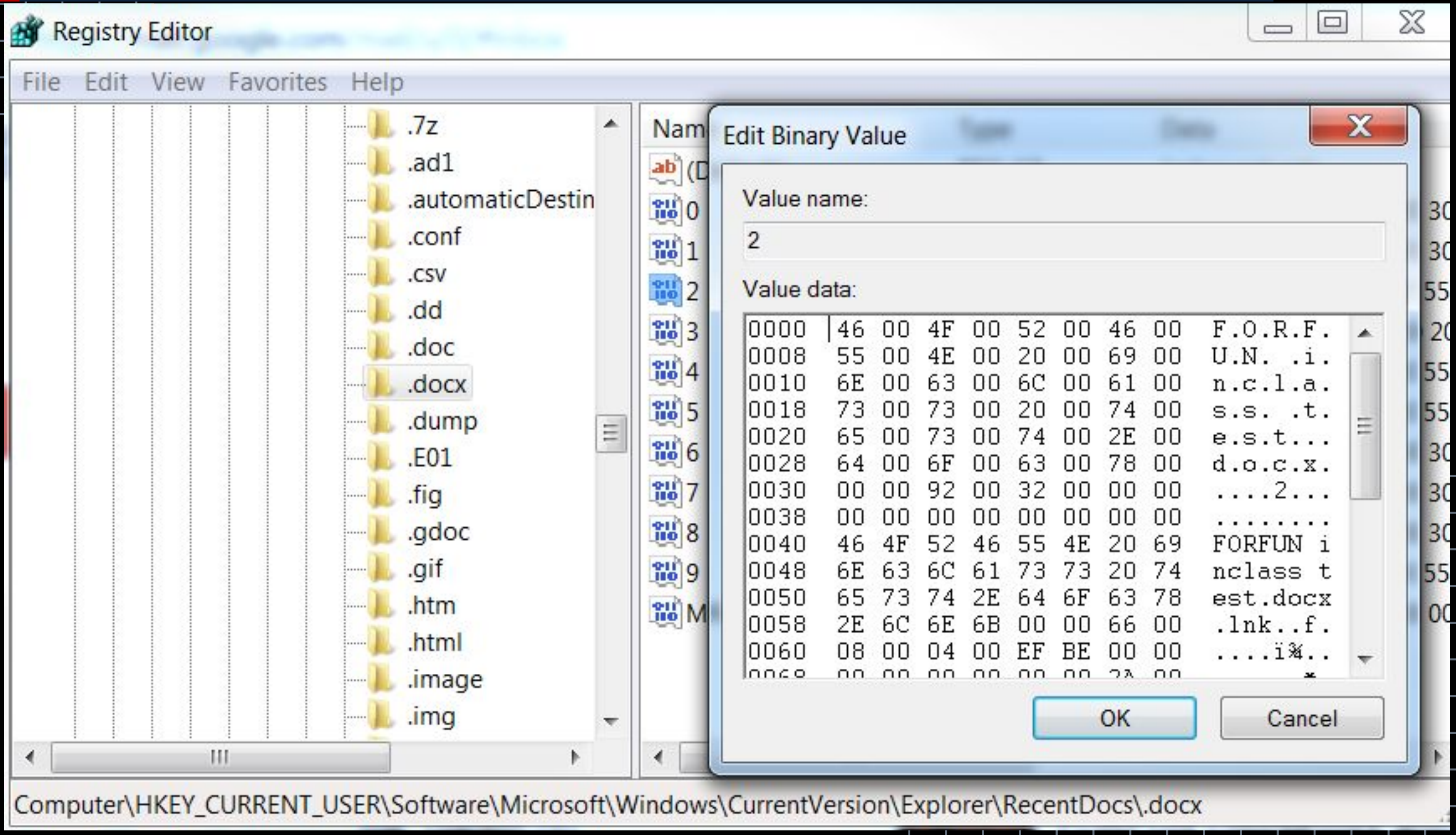


```
{90140000-002C-0409-1000-0000000FF1CE}
{90140000-0043-0000-1000-0000000FF1CE}
{90140000-0043-0409-1000-0000000FF1CE}
{90140000-006E-0409-1000-0000000FF1CE}
{90140000-0115-0409-1000-0000000FF1CE}
{90160000-002A-0000-1000-0000000FF1CE}
{90160000-002A-0409-1000-0000000FF1CE}
{90160000-0116-0409-1000-0000000FF1CE}
{929FBD26-9020-399B-9A7A-751D61F0B942}
{92FB6C44-E685-45AD-9B20-CADF4CABA132} - 1033
{9495AEB4-AB97-39DE-8C42-806EEF75ECA7}
{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}
{ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}
{B54948B2-E0FA-4F77-BCE4-38E39E587589}
{BA573BFE-83B4-11E3-93D2-D231FEB1DC81}
{BC958BD2-5DAC-3862-BB1A-C1BE0790438D}
{BD6F5371-DAC1-30F0-9DDE-CAC6791E28C3}
{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}
{E23D1D2C-1762-11D5-A8D2-00C04FA35723}
{E5D9D1D7-C2CA-40C5-A849-A2FFBADA8F50}
```

Name	Type	Data
EstimatedSize	REG_D...	0x0000858d (34189)
HelpLink	REG_EX...	http://www.paloaltonetworks.com
HelpTelephone	REG_SZ	
InstallDate	REG_SZ	20170818
InstallLocation	REG_SZ	
InstallSource	REG_SZ	C:\Users\lifudong\Documents\Downloads\Chrome Downloac
Language	REG_D...	0x00000409 (1033)
ModifyPath	REG_EX...	MsiExec.exe /I{F6590E2B-4FA4-4733-A923-467915FE52DB}
Publisher	REG_SZ	Palo Alto Networks
Readme	REG_SZ	
Size	REG_SZ	
UninstallString	REG_EX...	MsiExec.exe /I{F6590E2B-4FA4-4733-A923-467915FE52DB}
URLInfoAbout	REG_SZ	http://www.paloaltonetworks.com
URLUpdateInfo	REG_SZ	
Version	REG_D...	0x03010006 (50397190)
VersionMajor	REG_D...	0x00000003 (3)
VersionMinor	REG_D...	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F6590E2B-4FA4-4733-A923-467915FE52DB}

User Activities



Value name:

2

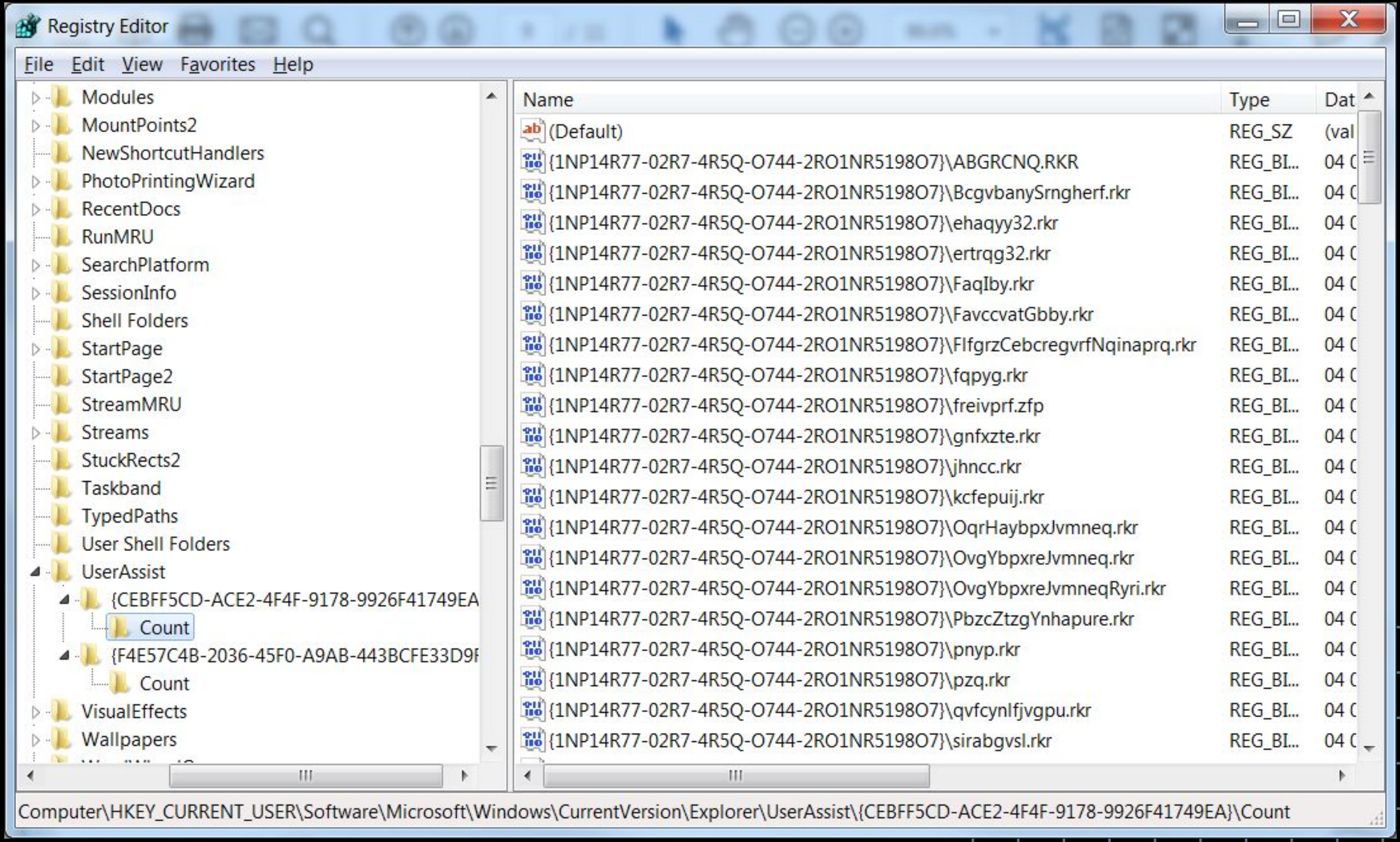
Value data:

```
0000  46 00 4F 00 52 00 46 00   F.O.R.F.
0008  55 00 4E 00 20 00 69 00   U.N. .i.
0010  6E 00 63 00 6C 00 61 00   n.c.l.a.
0018  73 00 73 00 20 00 74 00   s.s. .t.
0020  65 00 73 00 74 00 2E 00   e.s.t...
0028  64 00 6F 00 63 00 78 00   d.o.c.x.
0030  00 00 92 00 32 00 00 00   ....2...
0038  00 00 00 00 00 00 00 00   ........
0040  46 4F 52 46 55 4E 20 69   FORFUN i
0048  6E 63 6C 61 73 73 20 74   nclass t
0050  65 73 74 2E 64 6F 63 78   est.docx
0058  2E 6C 6E 6B 00 00 66 00   .lnk..f.
0060  08 00 04 00 EF BE 00 00   ....ï¾..
0068  00 00 00 00 00 00 2A 00   ......*.
```

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx

UserAssist (1)

- UserAssist holds information on programs being used by the user, including program name, the last execution date and time, and number of usage.



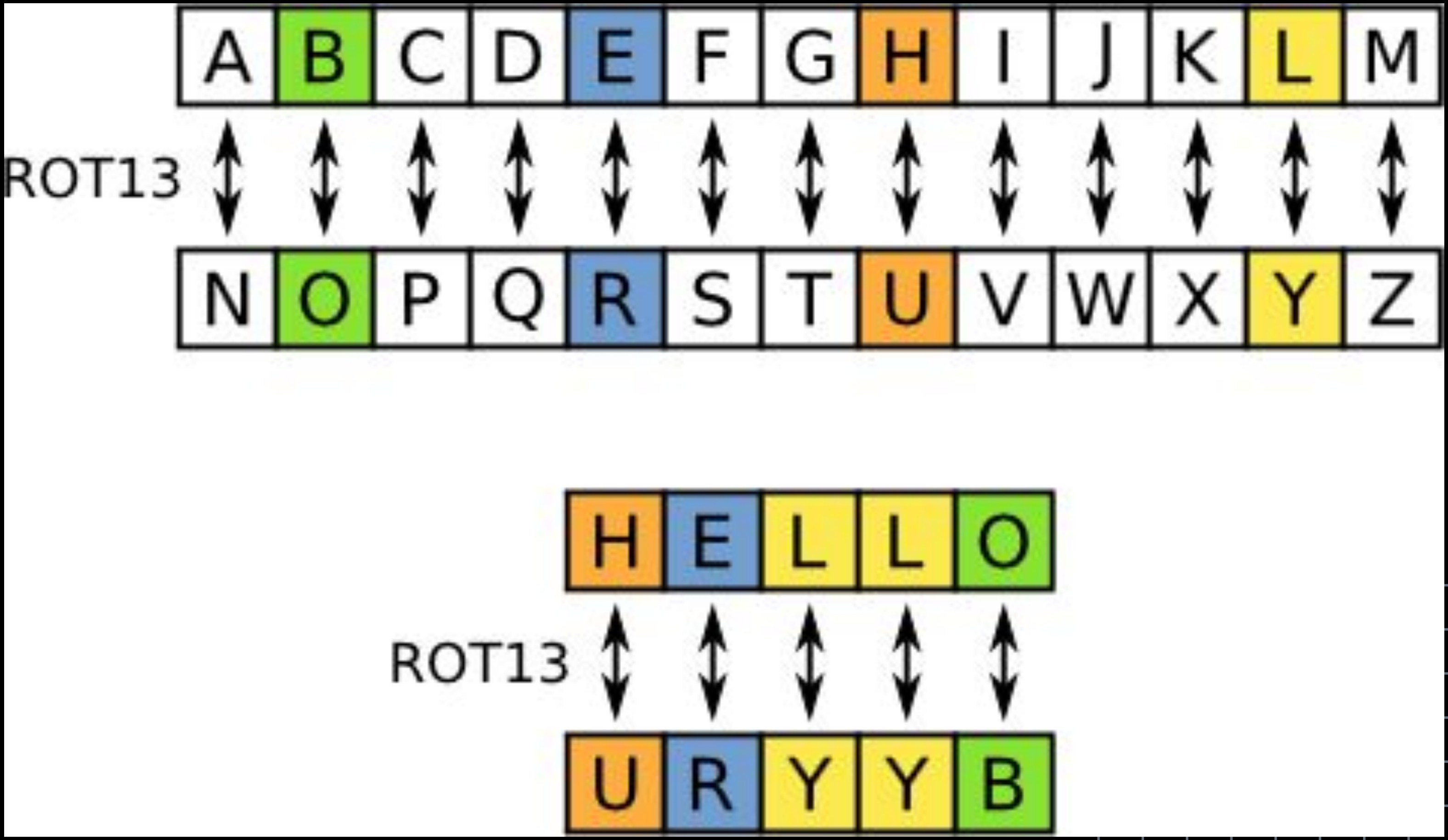
Modules
MountPoints2
NewShortcutHandlers
PhotoPrintingWizard
RecentDocs
RunMRU
SearchPlatform
SessionInfo
Shell Folders
StartPage
StartPage2
StreamMRU
Streams
StuckRects2
Taskband
TypedPaths
User Shell Folders
UserAssist
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA
Count
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F
Count
VisualEffects
Wallpapers

Name	Type	Dat
(Default)	REG_SZ	(val
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\ABGRCNQ.RKR	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\BcgvbanySrngherf.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\ehaqyy32.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\ertrqg32.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\FaqIby.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\FavccvatGbby.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\FlfgrzCebcregvrfNqinaprq.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\fqpyg.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\freivprf.zfp	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\gnfxzte.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\jhncc.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\kcfepuij.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\OqrHaybpxJvmneq.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\OvgYbpxreJvmneq.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\OvgYbpxreJvmneqRyri.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\PbzcZtzgYnhapure.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\pnyp.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\pzq.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\qvfcynlfjvgpu.rkr	REG_BI…	04 (
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\sirabgvsl.rkr	REG_BI…	04 (

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count

UserAssist (2)

- Data is encrypted with ROT13 (Rotate 13) by default.



A B C D E F G H I J K L M

ROT13

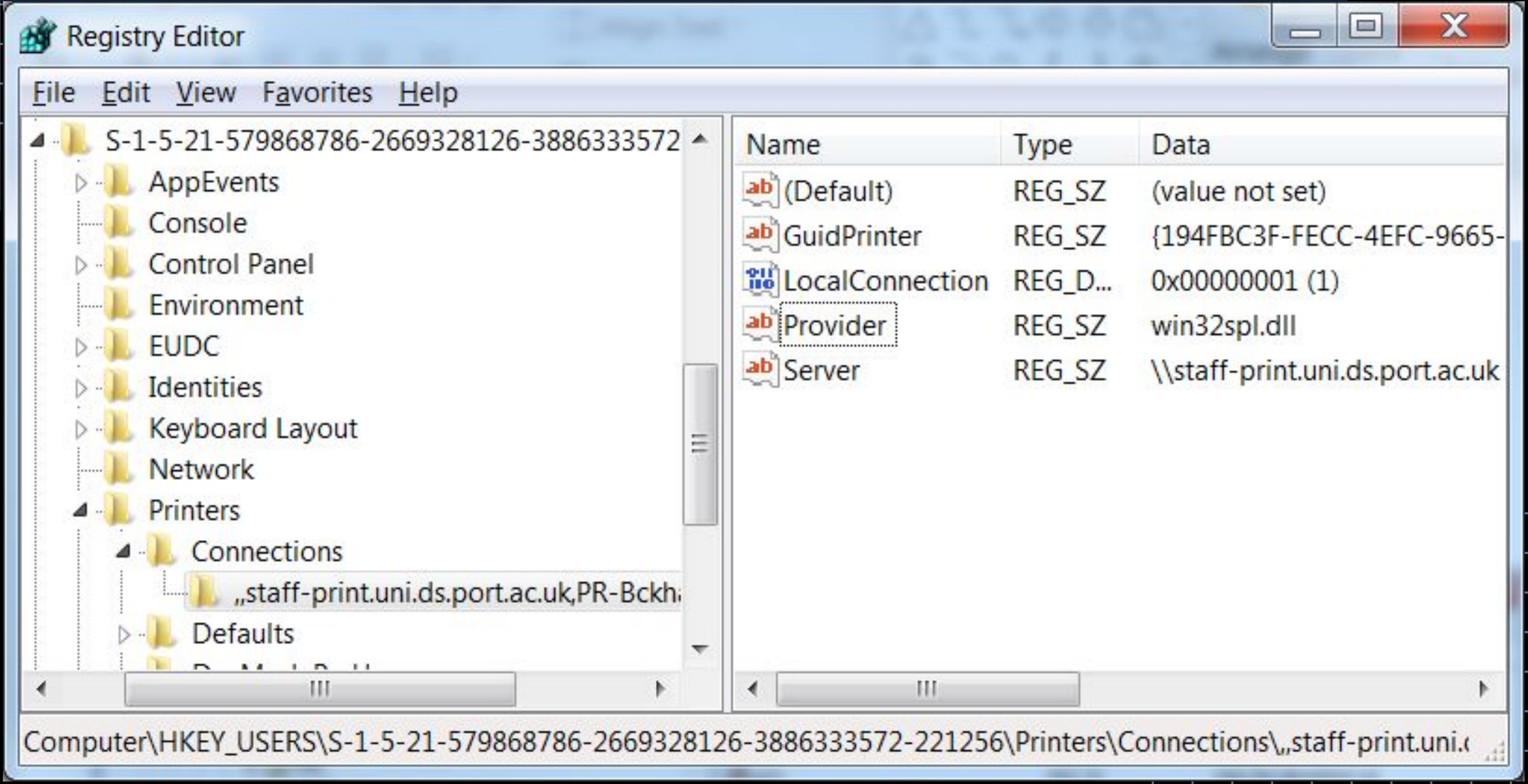
N O P Q R S T U V W X Y Z

H E L L O

ROT13

U R Y Y B

Printers

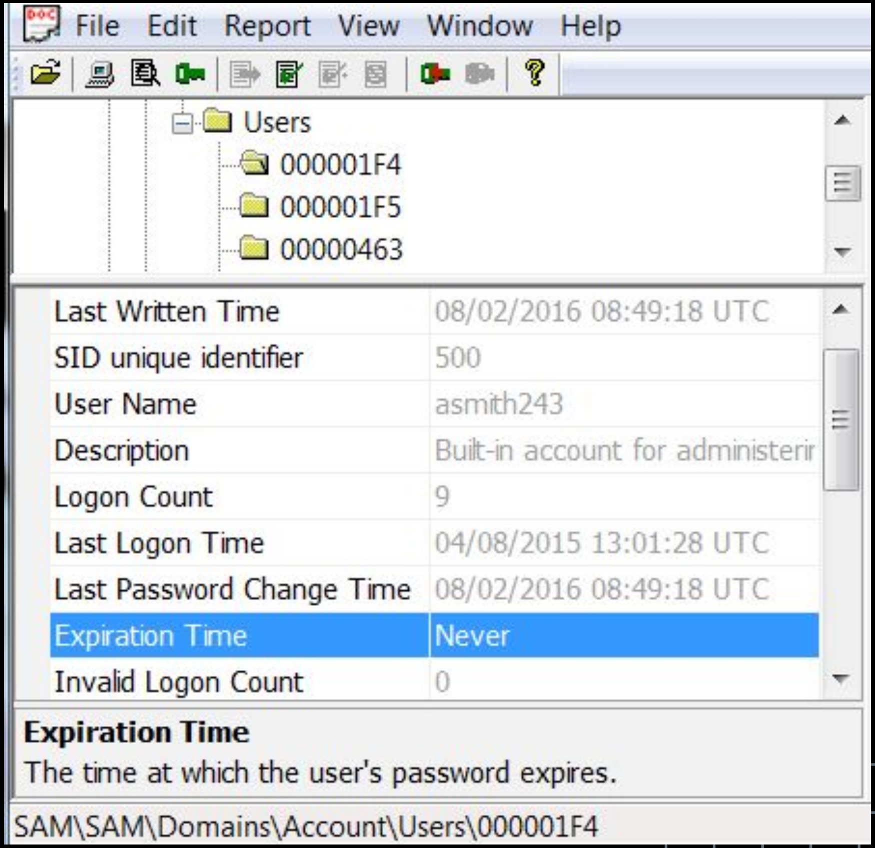


Name	Type	Data
(Default)	REG_SZ	(value not set)
GuidPrinter	REG_SZ	{194FBC3F-FECC-4EFC-9665-
LocalConnection	REG_D...	0x00000001 (1)
Provider	REG_SZ	win32spl.dll
Server	REG_SZ	\\staff-print.uni.ds.port.ac.uk

Computer\HKEY_USERS\S-1-5-21-579868786-2669328126-3886333572-221256\Printers\Connections\,,staff-print.uni.

User Accounts

- Includes user name, logon count, last logon time, last password change, password hashes…



Last Written Time	08/02/2016 08:49:18 UTC
SID unique identifier	500
User Name	asmith243
Description	Built-in account for administerir
Logon Count	9
Last Logon Time	04/08/2015 13:01:28 UTC
Last Password Change Time	08/02/2016 08:49:18 UTC
Expiration Time	Never
Invalid Logon Count	0

Expiration Time
The time at which the user's password expires.

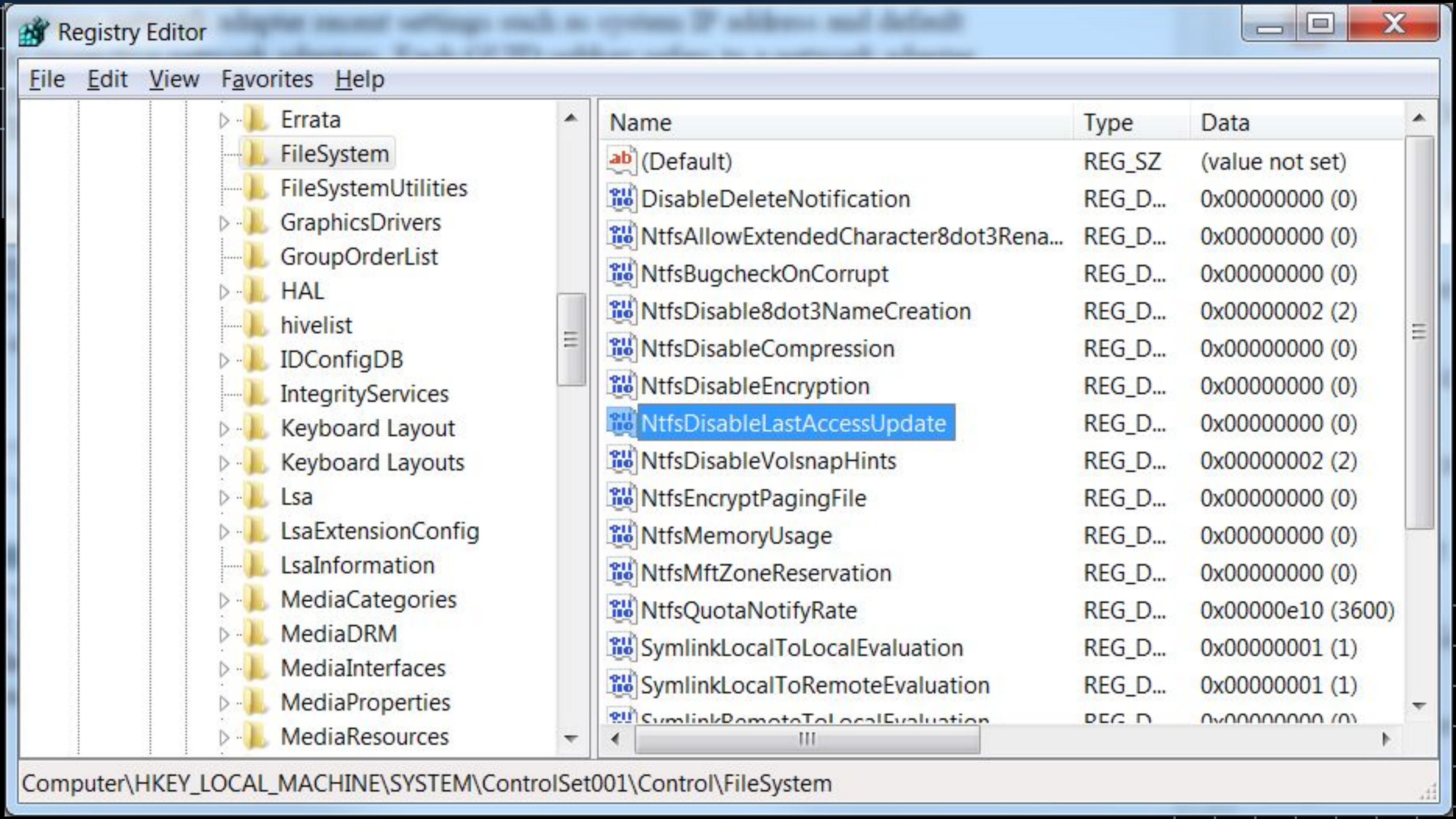
SAM\SAM\Domains\Account\Users\000001F4

Passwords

- Security Accounts Manager (SAM): contains user account details including the password in hashed form
  - HKLM\SAM\Domains\Account\Aliases\Members
  - HKLM\SAM\Domains\Account\Users
- Windows protected storage
  - HKCU\Software\Microsoft\Protected Storage System Provider
- Internet Explorer remembered passwords
  - HKCU\Software\Microsoft\Internet Explorer\IntelliForms

Interesting Registry Settings

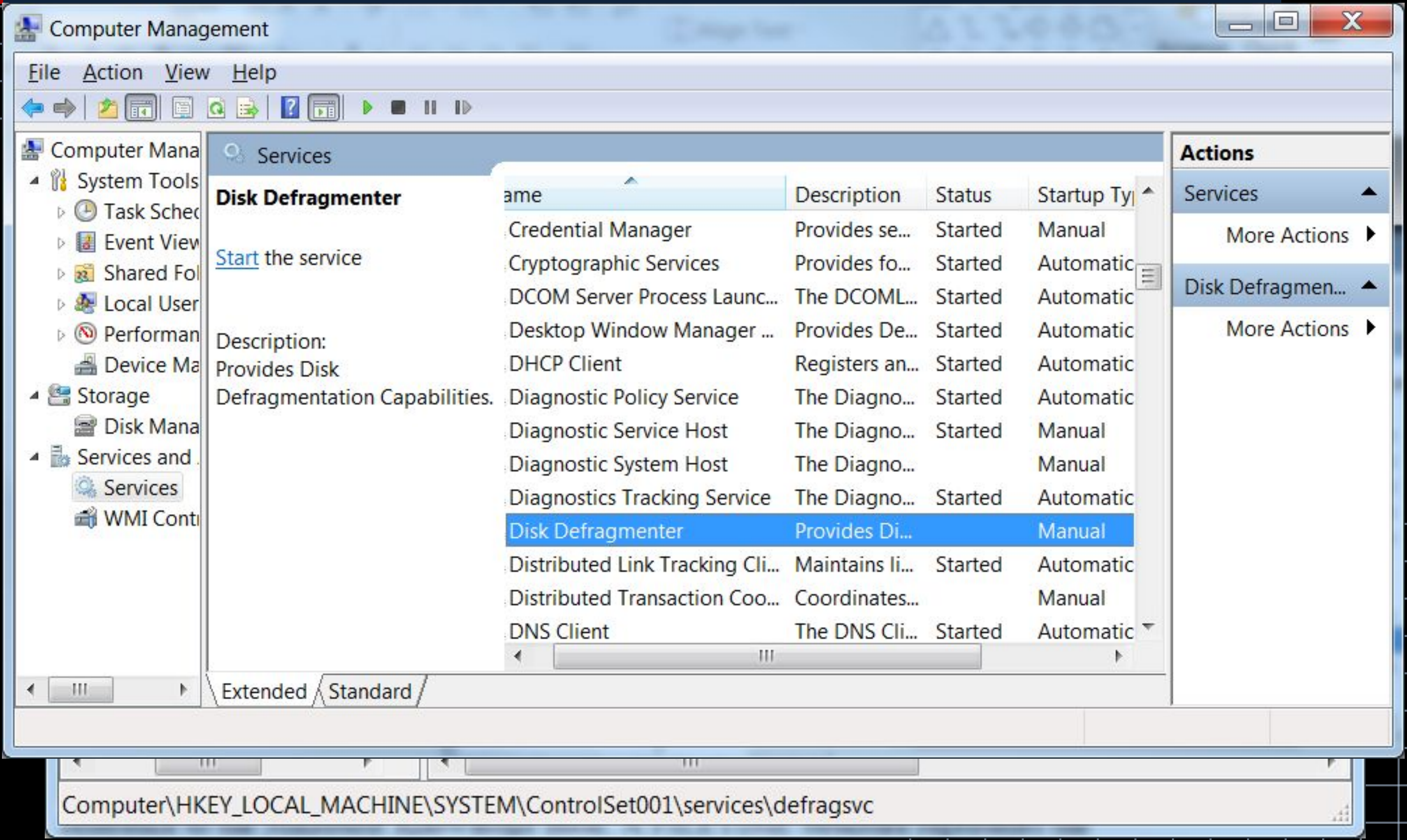
Last Access Timestamps



Name	Type	Data
(Default)	REG_SZ	(value not set)
DisableDeleteNotification	REG_D...	0x00000000 (0)
NtfsAllowExtendedCharacter8dot3Rena...	REG_D...	0x00000000 (0)
NtfsBugcheckOnCorrupt	REG_D...	0x00000000 (0)
NtfsDisable8dot3NameCreation	REG_D...	0x00000002 (2)
NtfsDisableCompression	REG_D...	0x00000000 (0)
NtfsDisableEncryption	REG_D...	0x00000000 (0)
NtfsDisableLastAccessUpdate	REG_D...	0x00000000 (0)
NtfsDisableVolsnapHints	REG_D...	0x00000002 (2)
NtfsEncryptPagingFile	REG_D...	0x00000000 (0)
NtfsMemoryUsage	REG_D...	0x00000000 (0)
NtfsMftZoneReservation	REG_D...	0x00000000 (0)
NtfsQuotaNotifyRate	REG_D...	0x00000e10 (3600)
SymlinkLocalToLocalEvaluation	REG_D...	0x00000001 (1)
SymlinkLocalToRemoteEvaluation	REG_D...	0x00000001 (1)
SymlinkRemoteToLocalEvaluation	REG_D...	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\FileSystem

Defragmenter service



Disk Defragmenter

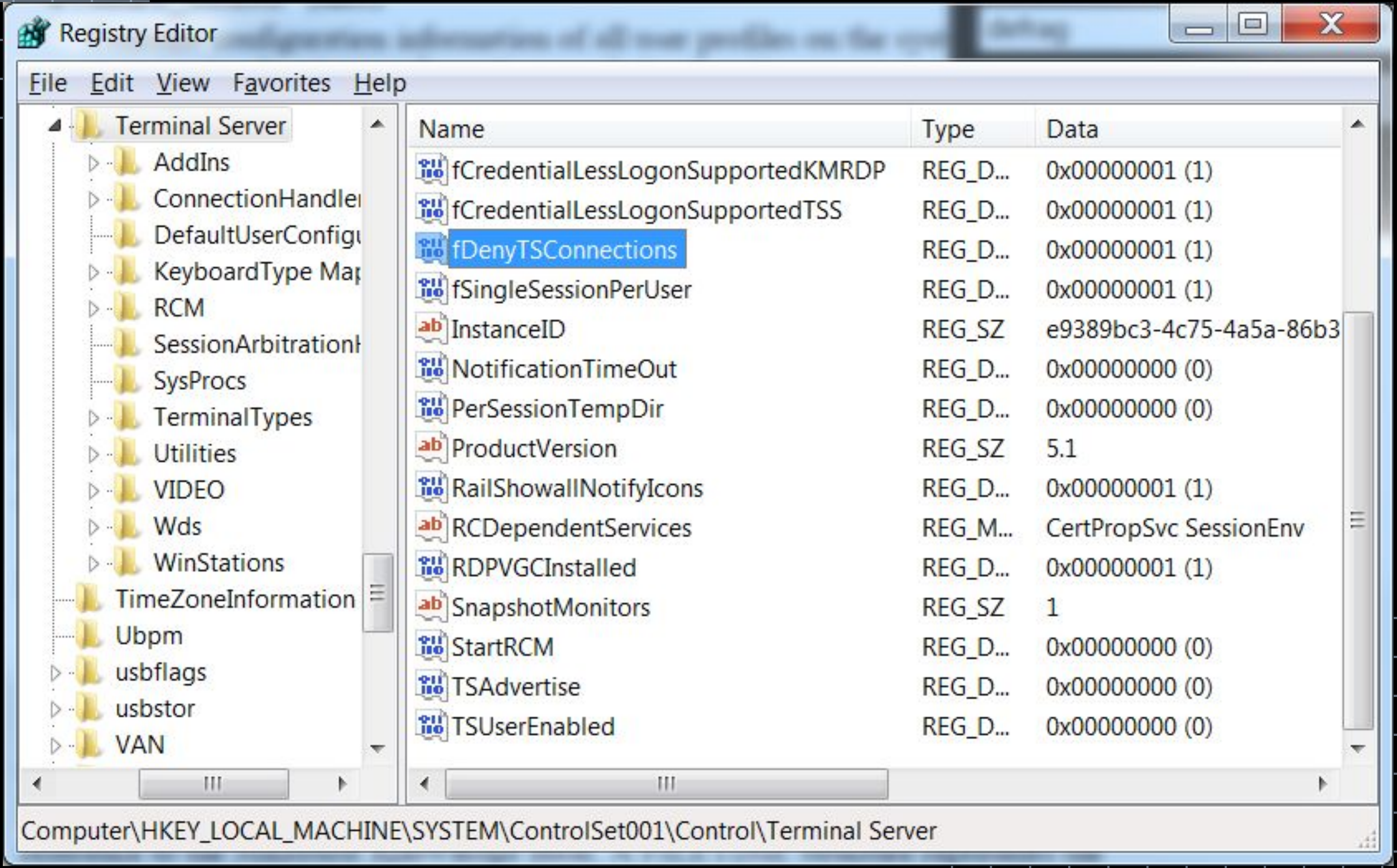
Start the service

Description:
Provides Disk Defragmentation Capabilities.

ame	Description	Status	Startup Ty
Credential Manager	Provides se...	Started	Manual
Cryptographic Services	Provides fo...	Started	Automatic
DCOM Server Process Launc...	The DCOML...	Started	Automatic
Desktop Window Manager ...	Provides De...	Started	Automatic
DHCP Client	Registers an...	Started	Automatic
Diagnostic Policy Service	The Diagno...	Started	Automatic
Diagnostic Service Host	The Diagno...	Started	Manual
Diagnostic System Host	The Diagno...		Manual
Diagnostics Tracking Service	The Diagno...	Started	Automatic
Disk Defragmenter	Provides Di...		Manual
Distributed Link Tracking Cli...	Maintains li...	Started	Automatic
Distributed Transaction Coo...	Coordinates...		Manual
DNS Client	The DNS Cli...	Started	Automatic

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\defragsvc

Remote Desktop

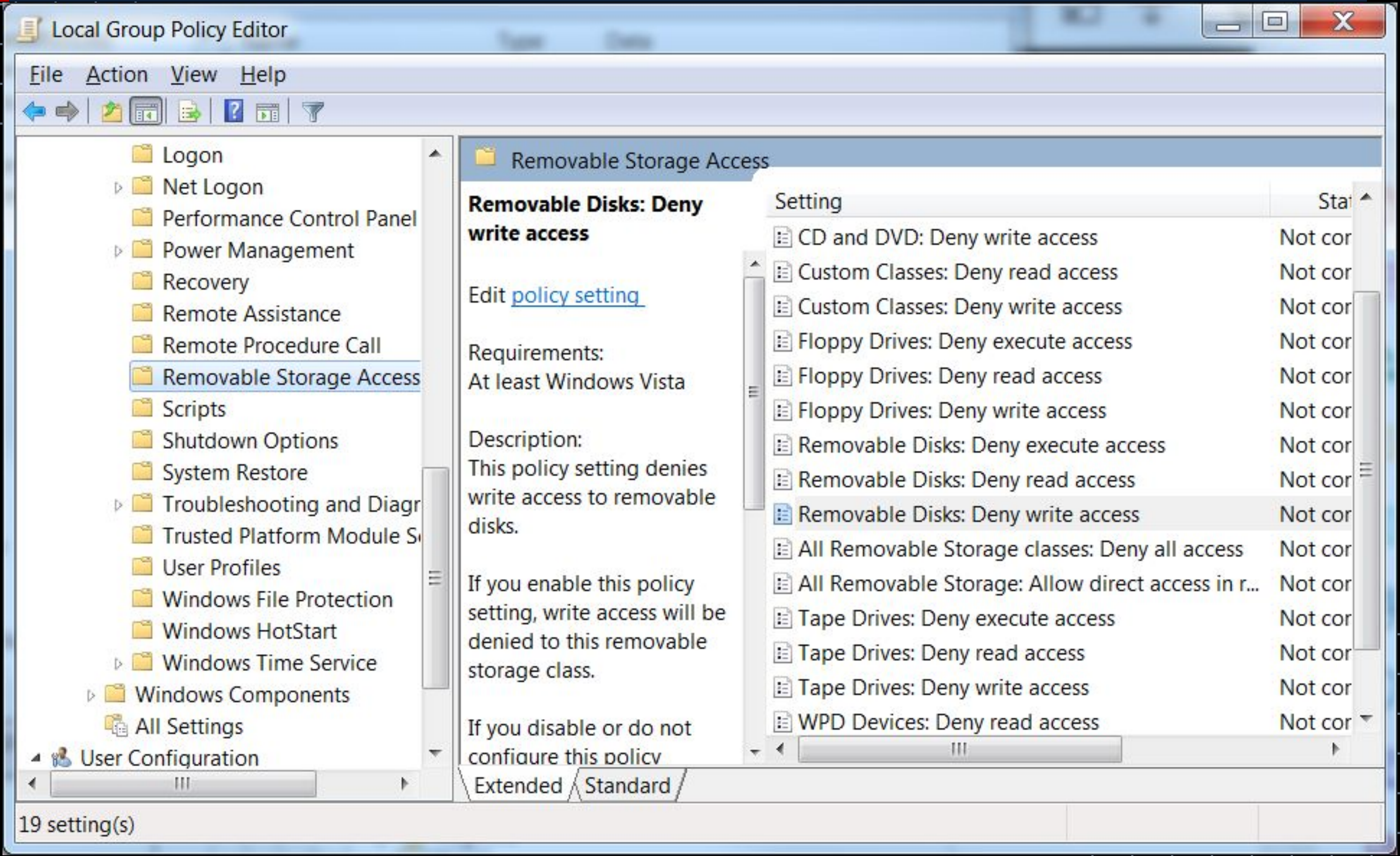


- Terminal Server
  - AddIns
  - ConnectionHandle
  - DefaultUserConfig
  - KeyboardType Ma
  - RCM
  - SessionArbitration
  - SysProcs
  - TerminalTypes
  - Utilities
  - VIDEO
  - Wds
  - WinStations
- TimeZoneInformation
- Ubpm
- usbflags
- usbstor
- VAN

Name	Type	Data
fCredentialLessLogonSupportedKMRDP	REG_D...	0x00000001 (1)
fCredentialLessLogonSupportedTSS	REG_D...	0x00000001 (1)
fDenyTSConnections	REG_D...	0x00000001 (1)
fSingleSessionPerUser	REG_D...	0x00000001 (1)
InstanceID	REG_SZ	e9389bc3-4c75-4a5a-86b3
NotificationTimeOut	REG_D...	0x00000000 (0)
PerSessionTempDir	REG_D...	0x00000000 (0)
ProductVersion	REG_SZ	5.1
RailShowallNotifyIcons	REG_D...	0x00000001 (1)
RCDependentServices	REG_M...	CertPropSvc SessionEnv
RDPVGCInstalled	REG_D...	0x00000001 (1)
SnapshotMonitors	REG_SZ	1
StartRCM	REG_D...	0x00000000 (0)
TSAdvertise	REG_D...	0x00000000 (0)
TSUserEnabled	REG_D...	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server

Removable Storage Access



Removable Storage Access

Removable Disks: Deny write access

Edit policy setting

Requirements:
At least Windows Vista

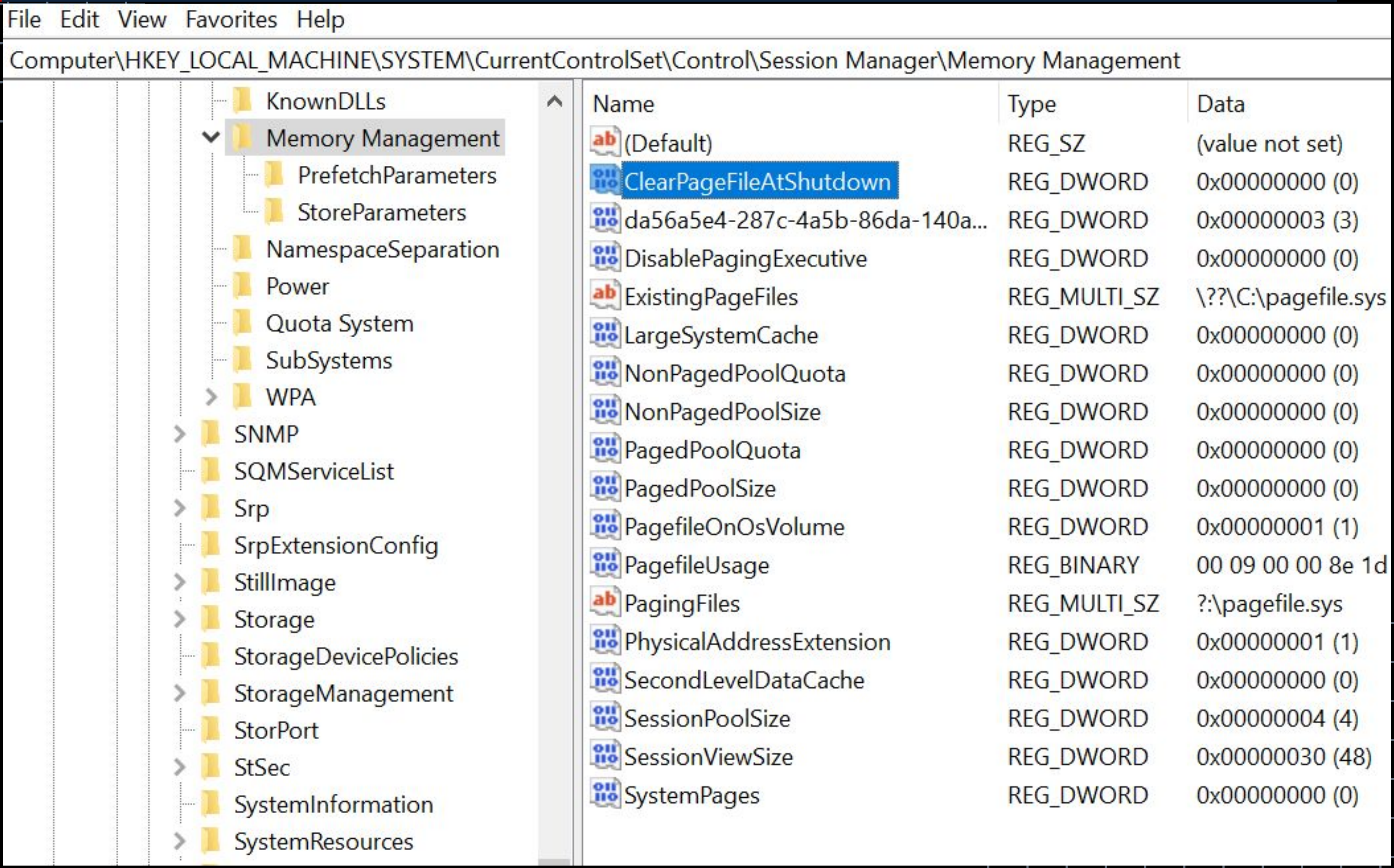
Description:
This policy setting denies write access to removable disks.

If you enable this policy setting, write access will be denied to this removable storage class.

If you disable or do not configure this policy

Setting	Stat
CD and DVD: Deny write access	Not cor
Custom Classes: Deny read access	Not cor
Custom Classes: Deny write access	Not cor
Floppy Drives: Deny execute access	Not cor
Floppy Drives: Deny read access	Not cor
Floppy Drives: Deny write access	Not cor
Removable Disks: Deny execute access	Not cor
Removable Disks: Deny read access	Not cor
Removable Disks: Deny write access	Not cor
All Removable Storage classes: Deny all access	Not cor
All Removable Storage: Allow direct access in r...	Not cor
Tape Drives: Deny execute access	Not cor
Tape Drives: Deny read access	Not cor
Tape Drives: Deny write access	Not cor
WPD Devices: Deny read access	Not cor

Swap/Page files

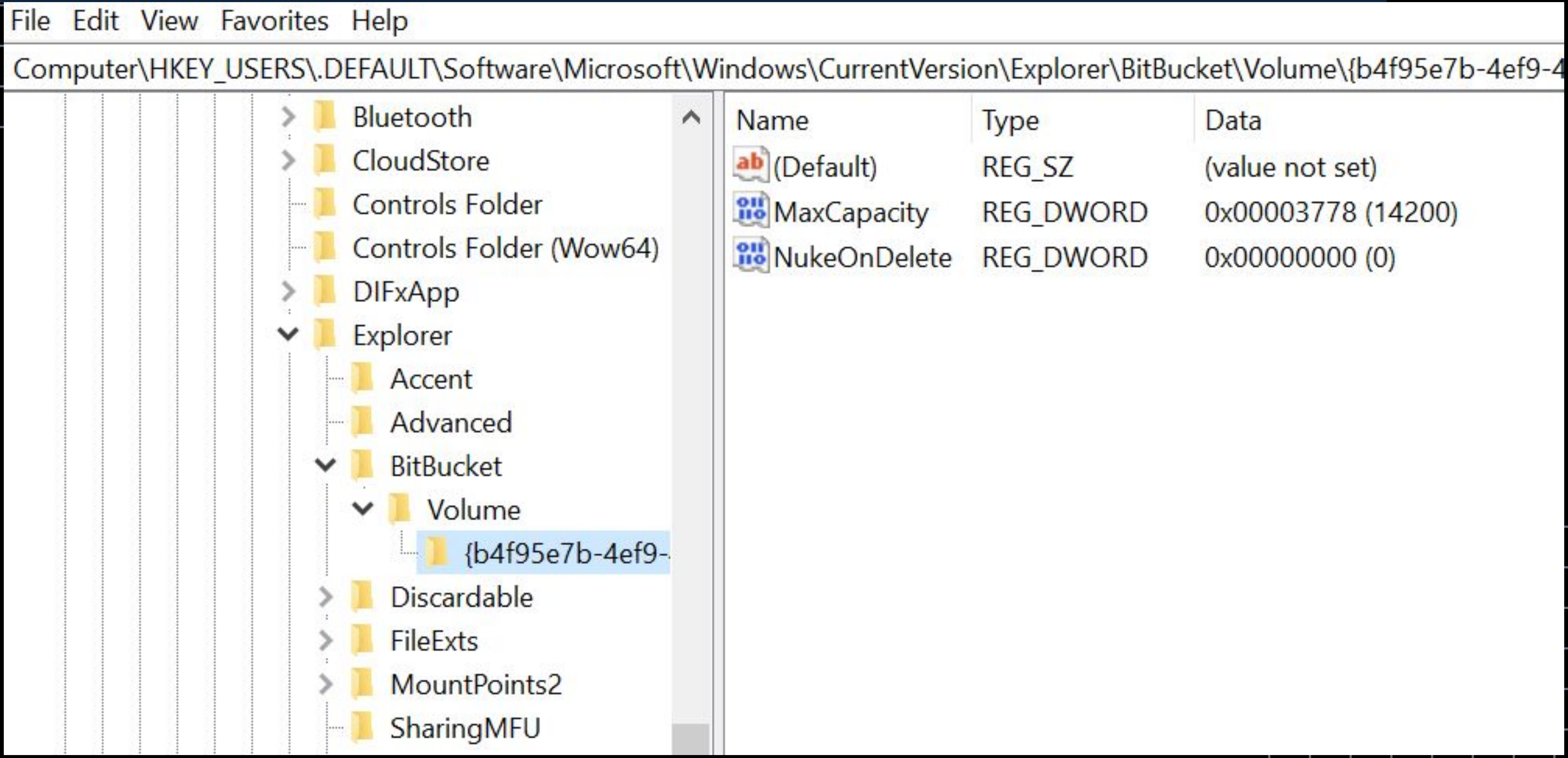


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

```
KnownDLLs
Memory Management
    PrefetchParameters
    StoreParameters
NamespaceSeparation
Power
Quota System
SubSystems
WPA
SNMP
SQMServiceList
Srp
SrpExtensionConfig
StillImage
Storage
StorageDevicePolicies
StorageManagement
StorPort
StSec
SystemInformation
SystemResources
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
ClearPageFileAtShutdown	REG_DWORD	0x00000000 (0)
da56a5e4-287c-4a5b-86da-140a...	REG_DWORD	0x00000003 (3)
DisablePagingExecutive	REG_DWORD	0x00000000 (0)
ExistingPageFiles	REG_MULTI_SZ	\??\C:\pagefile.sys
LargeSystemCache	REG_DWORD	0x00000000 (0)
NonPagedPoolQuota	REG_DWORD	0x00000000 (0)
NonPagedPoolSize	REG_DWORD	0x00000000 (0)
PagedPoolQuota	REG_DWORD	0x00000000 (0)
PagedPoolSize	REG_DWORD	0x00000000 (0)
PagefileOnOsVolume	REG_DWORD	0x00000001 (1)
PagefileUsage	REG_BINARY	00 09 00 00 8e 1d
PagingFiles	REG_MULTI_SZ	?:\pagefile.sys
PhysicalAddressExtension	REG_DWORD	0x00000001 (1)
SecondLevelDataCache	REG_DWORD	0x00000000 (0)
SessionPoolSize	REG_DWORD	0x00000004 (4)
SessionViewSize	REG_DWORD	0x00000030 (48)
SystemPages	REG_DWORD	0x00000000 (0)

Recycle Bin



Computer\HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{b4f95e7b-4ef9-4

- Bluetooth
- CloudStore
- Controls Folder
- Controls Folder (Wow64)
- DIFxApp
- Explorer
  - Accent
  - Advanced
  - BitBucket
    - Volume
      - {b4f95e7b-4ef9-
  - Discardable
  - FileExts
  - MountPoints2
  - SharingMFU

Name	Type	Data
(Default)	REG_SZ	(value not set)
MaxCapacity	REG_DWORD	0x00003778 (14200)
NukeOnDelete	REG_DWORD	0x00000000 (0)

Conclusions

- Windows Registry contains a wealth of information, holding keys to confirm or refute a claim.
- Hence it is mission critical that forensic investigators can extract valuable information from it.