



AccessData[®]

Registry Viewer

Registry structure

Searching the registry

Reports

Windows registret

- Innehåller inställningar och data om bland annat
 - Operativsystemet, hårdvara och installerade program
 - Användarnas inställningar
- De vanliga användarna har inte direkt access till registret
- Det går att ändra värden i registret via regedit
 - OBSERVERA! Det går dock inte att ångra sådant som man har gjort!
Ctrl-z existerar inte registrets värld!
- Registret innehåller information som ofta är viktiga för en forensisk utredning
- AccessDatas Registry Quick Find Chart
 - <http://accessdata.com/supplemental-class-material>
- Mera info:
 - <http://msdn.microsoft.com/en-us/library/ms724871.aspx>
 - <http://support.microsoft.com/kb/256986/sv>

Windows registry...

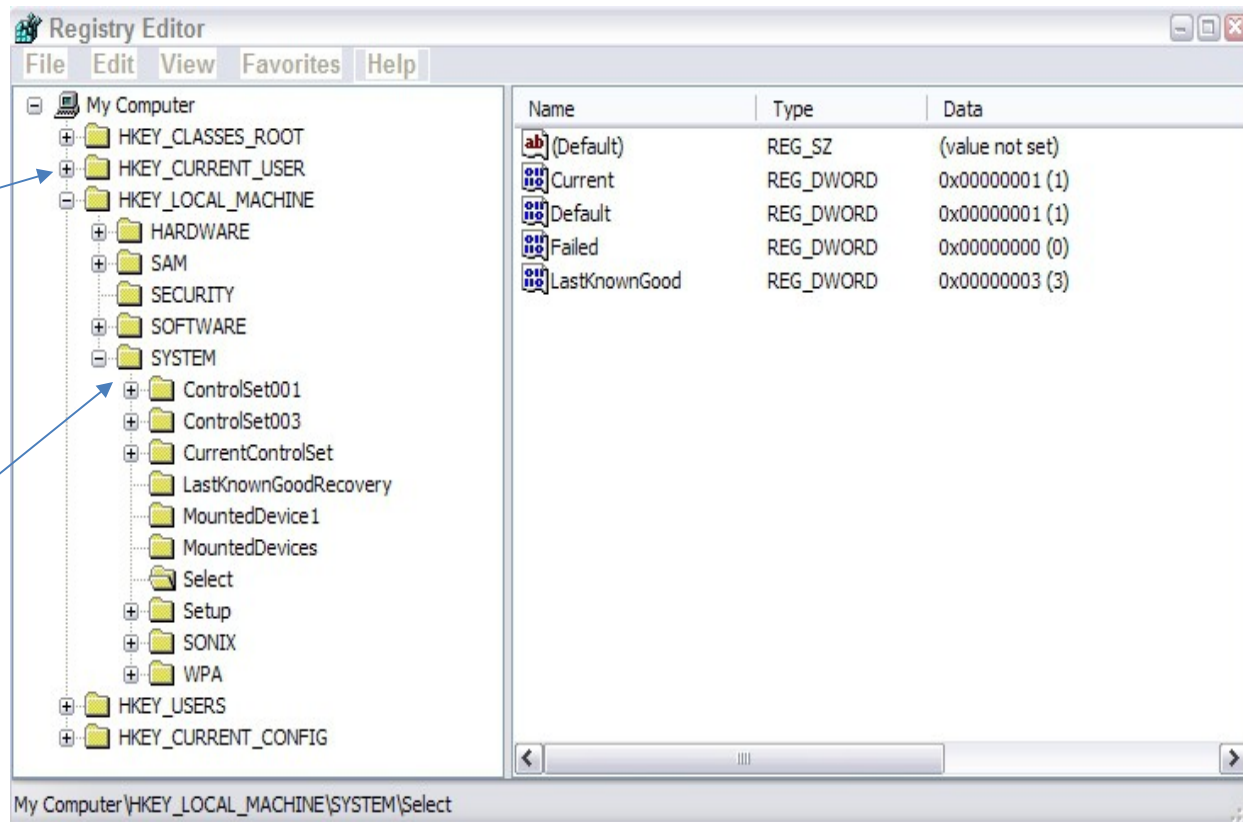
Some Available Information

- *Recent Document Lists
- *Recent File Run Lists
- *Registered Owner Information
- *Internet Explorer Typed URLs
- *Media Player History Lists
- *Mounted Devices / Drives
- *Protected Storage System Provider (PSSP)
- *IM Contacts
- *File Share Info
- *Chat Room Info
- *ID Alias Info
- *Time Bias Info
- *Profile Info
- *OS Version Info

(that's barely scratching the surface)

Registrets struktur (regedit.exe)

- Registret existerar endast i datorns internminne (RAM)!
- Registret är uppbyggt av rotmappar, olika nycklar och värden
- Varje värde består av ett namn, en datatyp och data



Rotmapp

Nycklar och
Undernycklar

Värden

Rotmapparna

- HKEY_CLASSES_ROOT (HKCR)
 - Associerar filtyper till olika program (CLSID)
 - Består av information från **HKCU\Software\Classes** (user-specific settings) och **HKLM\Software\Classes** (system-wide settings)
- HKEY_CURRENT_USER (HKCU)
 - Innehåller aktuell konfiguration/profil för nuvarande inloggad användare
 - Består av information från **HKU\<USER SID>**
- HKEY_CURRENT_CONFIG (HKCC)
 - Innehåller aktuell konfiguration/profil för hårdvaran vid systemstart
 - Informationen är hämtad från **HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current**
- HKEY_LOCAL_MACHINE (HKLM)
 - Innehåller **MÅNGA** system-inställningar, inklusive inställningar för mjukvara och hårdvara
- HKEY_USERS (HKU)
 - Innehåller miljöinställningar för systemets aktiva användare samt för konton som representerar local system, local service och network service

Huvudnycklar eller härledda nycklar?

- Endast HKEY_LOCAL_MACHINE (HKLM) och HKEY_USERS (HKU) innehåller ett antal delnycklar med egen ursprunglig information
- Resten av rotnycklarna och dess undernycklar härleds från andra nycklar och är volatile (flyktiga)
- På fysisk nivå så lagrar de båda huvudnycklarna (eller rotmapparna) HKLM och HKU det mesta av sin data i hive-filer

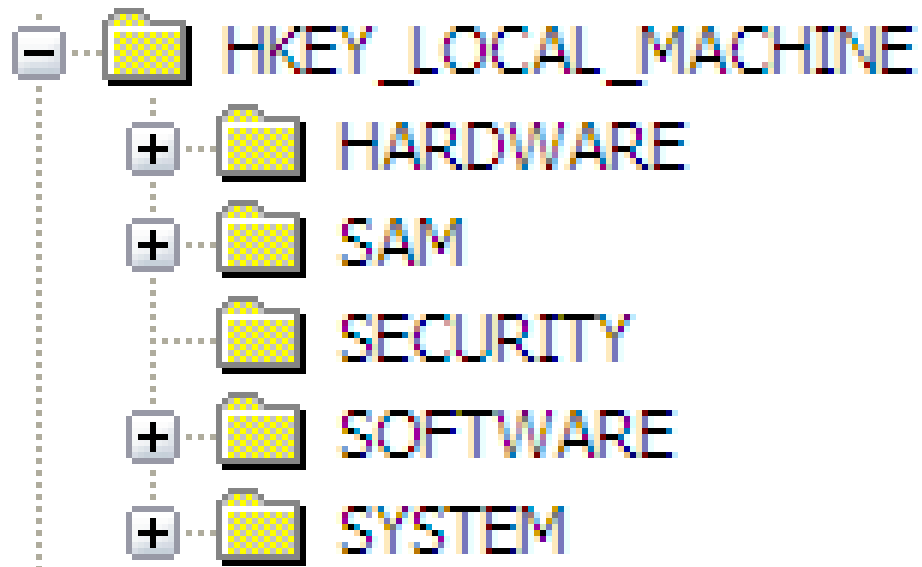
HKLM Keys > Hive Files

- En *hive* är en logisk grupp av nycklar, undernycklar och värden i registret, som har stödande filer i vilken dess värden sparas

HIVE KEY	HIVE FILE
HKLM\SAM	%SYSTEMROOT%\System32\config\SAM
HKLM\SECURITY	%SYSTEMROOT%\System32\config\SECURITY
HKLM\SOFTWARE	%SYSTEMROOT%\System32\config\software
HKLM\SYSTEM	%SYSTEMROOT%\System32\config\system

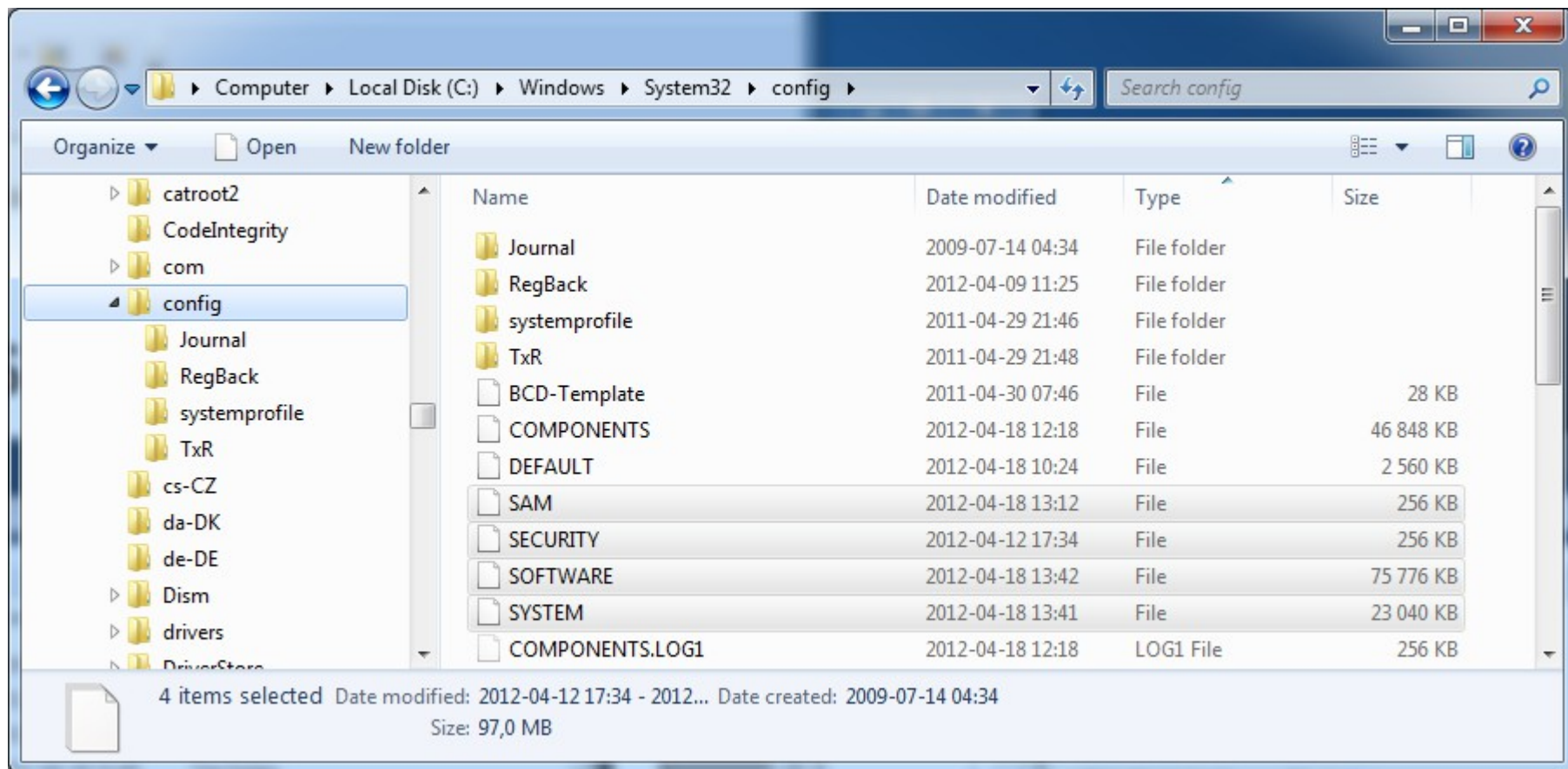
HKLM\Hardware

- Created during boot up
- Tracks attached dynamic hardware settings
- Volatile - not stored as a file!



Hive-filernas plats för HKLM

Ibland kan man hitta kopior av registry filer i **c:\Windows\repair** mappen i XP eller för Vista/7 i **c:\Windows\System32\config\RegBack**



Registry/hive files

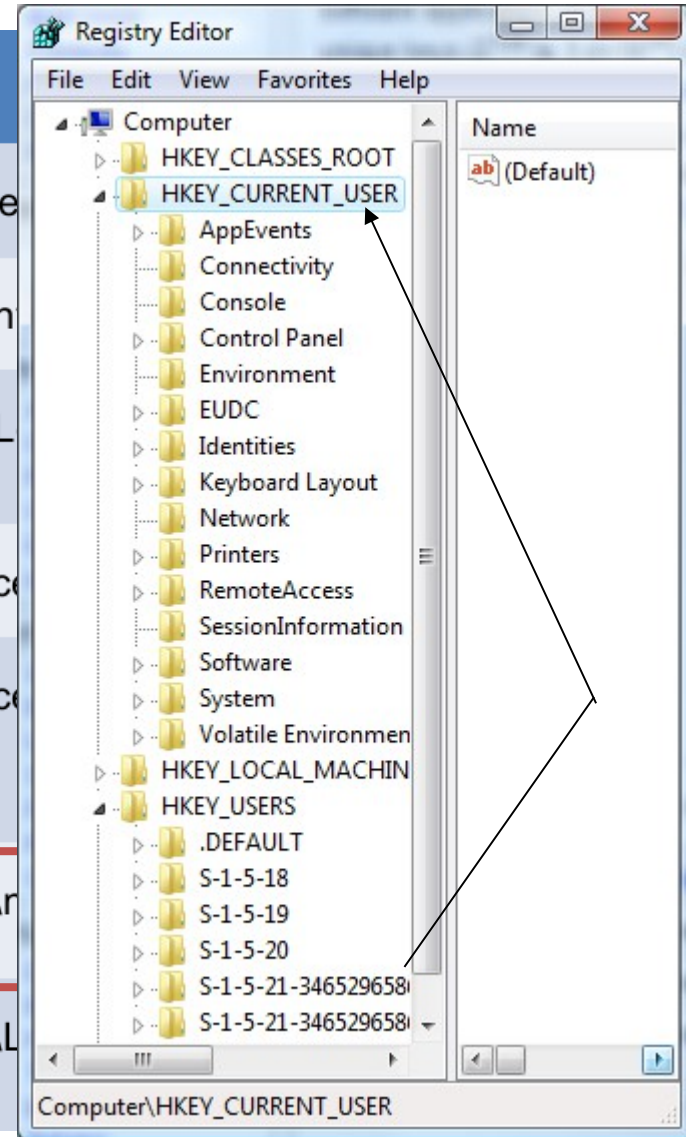
- **SAM** - HKLM\SAM
 - Account information for users and groups on the system
 - Logon passwords (crypted hash)!
- **SYSTEM** - HKLM\SYSTEM
 - Device drivers, computer name, system config, time zone
- **SECURITY** - HKLM\SECURITY
 - Local security policy, user and group rights, network security info
- **SOFTWARE** - HKLM\SOFTWARE
 - Program settings (system-wide), Classes (CLSID:s, file associations)
 - Current version settings (OS, owner, etc.)
- **NTUSER.DAT** - HKU\SID
 - User preferences/settings, desktop layout, wallpaper/screen savers
 - Opened and saved files, entered URL:s and commands, etc...

NTUSER.DAT

- HKU
 - Contains actively loaded user profiles and settings
 - Stores information from all users who have logged on to the computer in Security IDs (SIDs)
 - Default user profile .DEFAULT
 - Generates HKCU, and parts of HKCC and HKCR
- HKCU
 - Contains the active current logged on user profile data from NTUSER.DAT
 - Preferences, profile areas, mapped drives, MRU..., etc.
 - Copied from HKU upon logon
 - HKU\
 - The Software subkey is the most interesting one which contains the majority of the information about the user

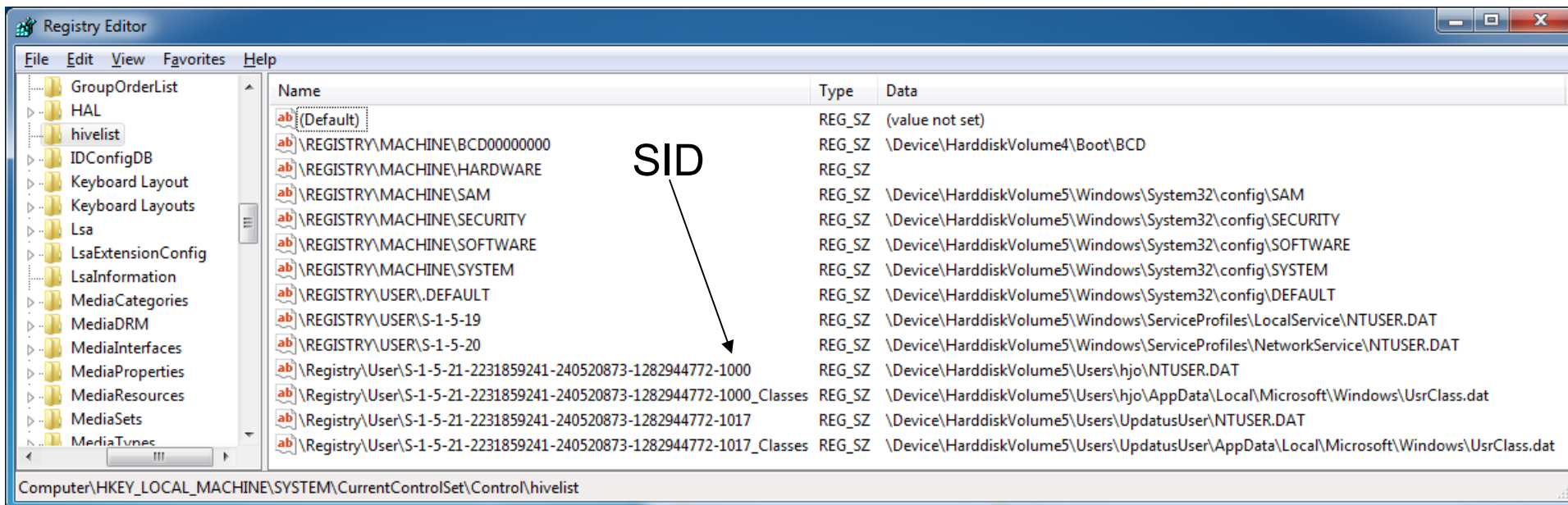
HKU Keys > Hive Files

HIVE KEY	HIVE FILE
HKU\DEFAULT	%SYSTEMROOT%\System32\config\de
HKU\S-1-5-19	Documents and Settings\LocalService n
HKU\S-1-5-19_Classes	Documents and Settings\LocalService\L Data\Microsoft\Windows\UsrClass.dat
HKU\S-1-5-20	Documents and Settings\NetworkService
HKU\S-1-5-20_Classes	Documents and Settings\NetworkService Data\Microsoft\Windows\UsrClass.dat
HKU\SID	Documents and Settings\ <username>\n </username>\n or for Vista/7 Users\ <username>\ntuser.dat< td=""> </username>\ntuser.dat<>
HKU\SID_Classes	Documents and Settings\ <username>\l </username>\l Data\Microsoft\Windows\UsrClass.dat



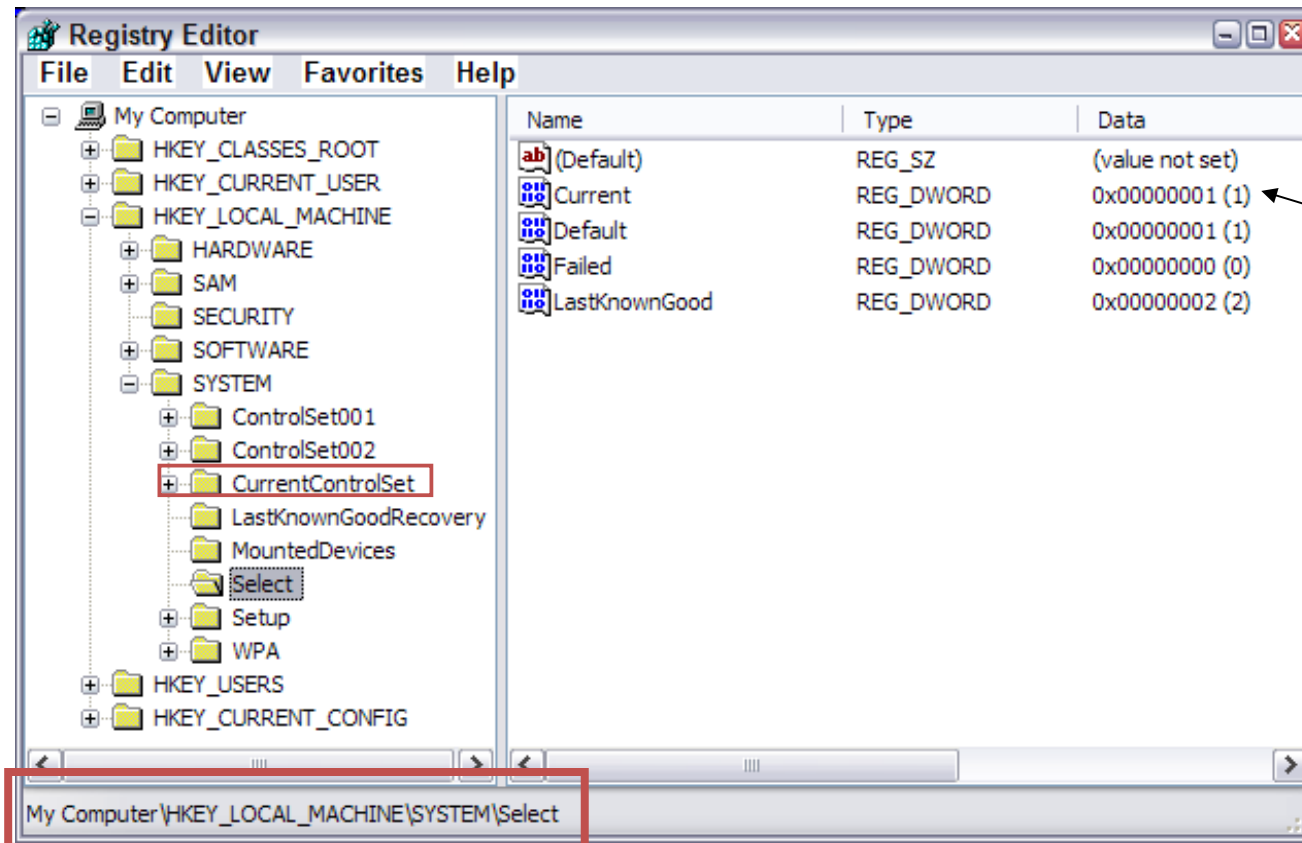
Sökvägar till hive-filerna

- Sökvägar till hive-filerna är listade i
 - HKLM\SYSTEM\CurrentControlSet\Control\hivelist



HKLM\System\CurrentControlSet

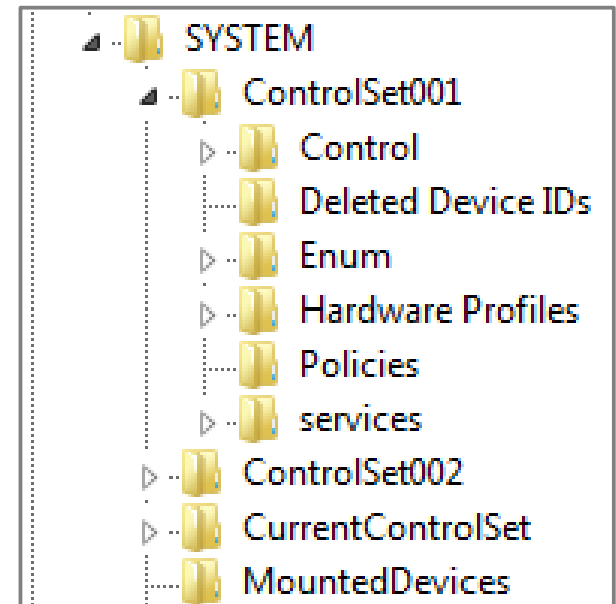
- Är härlett från ett annat ControlSet, men vilket?



I det här fallet från ControlSet001

The Select subkey

- The Select subkey defines which control set is active
- The Select subkey contains the values
 - **Default**, defines which control set will be used
 - **Current**, which of the two control sets that was used to boot last time
 - **LastKnownGood**, the control set for the last successful logon
 - **Failed**, the control set that last failed to boot
- The CurrentControlSet
 - Is a symbolic link to the ControlSet that are used of the live machine
 - The CurrentControlSet only exist in the living registry - RAM



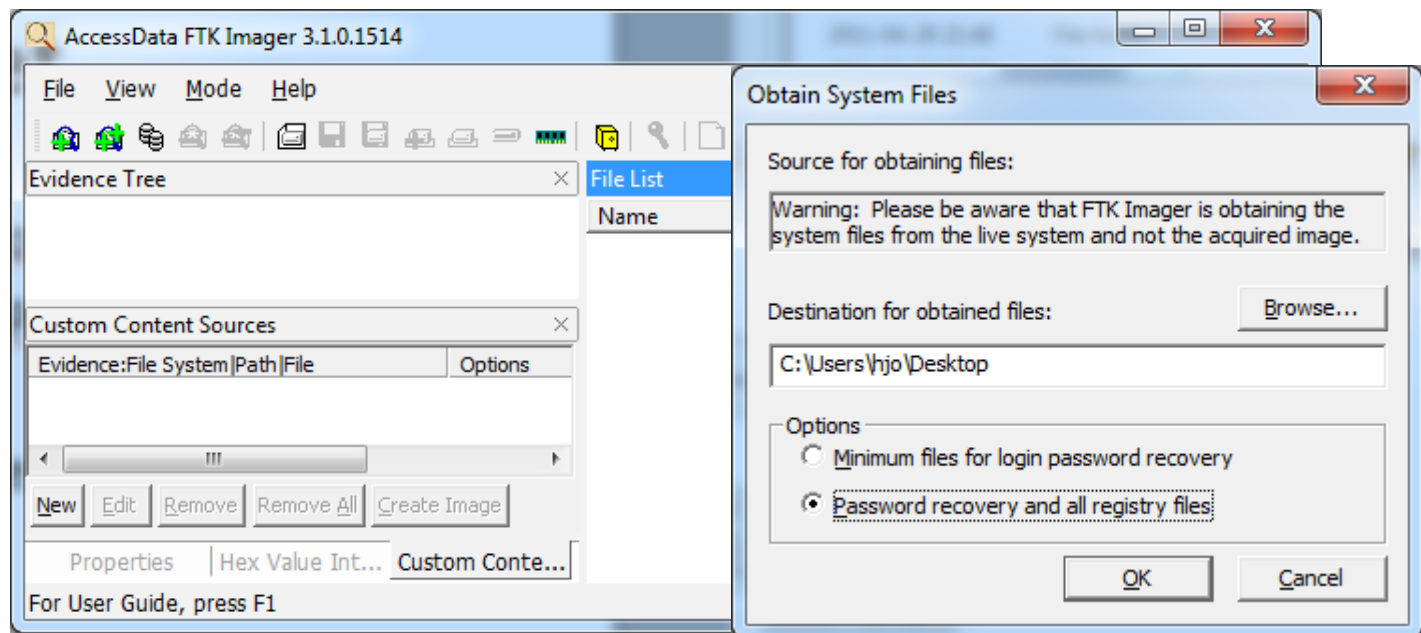
Registry data types

Programs may use any data type it wants for storage!

DATA TYPE	NUMBER	DESCRIPTION
REG_NONE	0	Data type is not defined
REG_SZ	1	Fixed length text string expressed in user-friendly format, which is often used to describe components
REG_EXPAND_SZ	2	Variable or expandable length data string
REG_BINARY	3	Binary data that is displayed in editor as hex
REG_DWORD	4	32-bit double word values and the most common data type found in the registry
REG_DWORD_LITTLE_ENDIAN	4	32-bit double word values with bytes in reverse order. As Intel already store data in this format, this term is synonymous with REG_DWORD and they have the same numeric value
REG_DWORD_BIG_ENDIAN	5	32-bit double word value with bytes in normal order with the highest bit appearing first
REG_LINK	6	An internal-use only data type for Unicode symbolic link
REG_MULTI_SZ	7	Multiple string field in which each string is separated by a null (00h) and with two nulls (00 00) marking the end of the list of strings
REG_RESOURCE_LIST	8	Listing of resource lists for devices or device drivers (REG_FULL_RESOURCE_DESCRIPTOR). You can view, but not edit these lists.

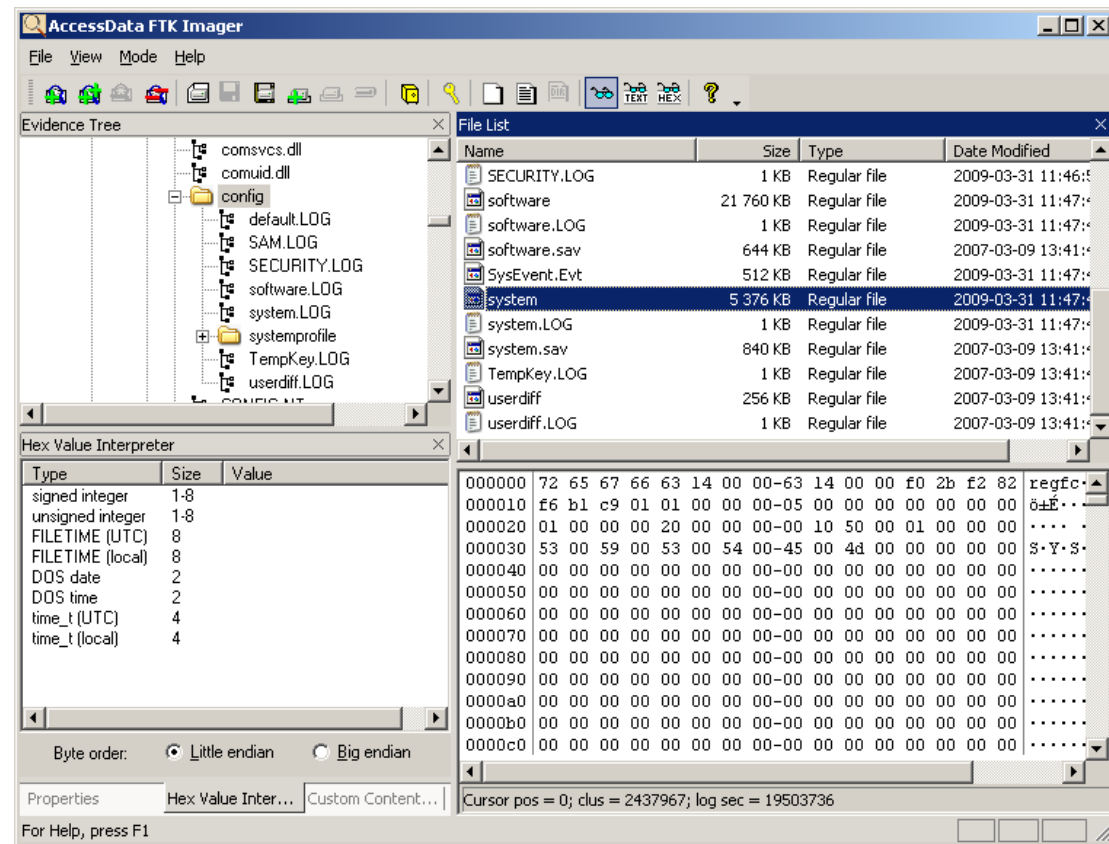
Att ta en kopia av maskinens hive-filer, det enkla sättet

- Starta FTK Imager
- Klicka på det lilla gula skåpet, "Obtain protected files"
- Ange var hive-filerna ska sparas och välj Password recovery and registry files
- Nackdel, den dator vars register ska undersökas måste vara igång...



Att kopiera hive-filer från en image

- Starta FTK Imager
- Välj File > Add Evidence Item... >
- Sök rätt på hive-filerna och exportera dem



File Menu

The screenshot shows the AccessData Registry Viewer application window. The title bar reads "AccessData Registry Viewer (tm) - [2K.DAT]". The menu bar includes "File", "Edit", "Report", "View", "Window", and "Help". The "File" menu is open, showing options: "Cascade", "Tile", "Arrange Icons", and "1 2K.DAT". The left sidebar shows a tree view of registry paths, with "2K.DAT" selected. The main pane displays a table of registry values:

Name	Type	Data
TEMP	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Temp
TMP	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Temp

Below the table is a hex dump of the selected value's data:

```
00 25 00 55 00 53 00 45 00-52 00 50 00 52 00 4f 00  %U·S·E·R·P·R·O·
10 46 00 49 00 4c 00 45 00-25 00 5c 00 4c 00 6f 00  F·I·L·E·%·\·L·o·
20 63 00 61 00 6c 00 20 00-53 00 65 00 74 00 74 00  c·a·l· ·S·e·t·t·
30 69 00 6e 00 67 00 73 00-5c 00 54 00 65 00 6d 00  i·n·g·s·\·T·e·m·
40 70 00 00 00                                     p·...
```

The bottom status bar shows "Offset: 0".

Tool Icons and Common Areas (Favorites)

The screenshot shows the AccessData Registry Viewer application window. The title bar reads "AccessData Registry Viewer - Education - [Common Areas]". The menu bar includes File, Edit, Report, View, Window, and Help. A red box highlights the toolbar, which contains icons for File Explorer, Home, Print, Copy, Paste, Undo, Redo, Refresh, and Help. The left pane shows a tree view of "Common Areas" with sub-items: CurrentVersion (selected), ProfileList, Run, System, Windows NT, and Winlogon. The main pane displays a table of registry values:

Name	Type	Data
CurrentVersion	REG_SZ	6.0
CurrentBuildNumber	REG_SZ	6000
CurrentBuild	REG_SZ	6000
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x4671BF9D (1181859741)
RegisteredOrganization	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	Dustin
SystemRoot	REG_SZ	C:\Windows

Below the table, there is a hex view of the data: 0 | 36 00 2E 00 30 00 00 00- | 6 .. .0 ...

The bottom-left pane shows "Key Properties" for the selected "CurrentVersion" value:

- Last Written Time: 2008-02-15 13:51:
- OS Install Date (Local): Thu Jun 14 22:22:
- OS Install Date (Local): Fri Jun 15 00:22:2:

The bottom-right pane shows "OS Install Date (Local)" with the text: "This indicates the time when the operating system was installed."

The status bar at the bottom reads "AccessData Registry Viewer" and "C Offset: 0".

Properties and Interpreters

The screenshot shows the Windows Registry Editor with the SAM hive selected. The left pane shows the tree structure: SAM > Domains > Account > Users > 000003F3. The right pane shows the 'Values/Data' table with two entries: 'F' (REG_BINARY) and 'V' (REG_BINARY). A 'Hex Interpreter' dialog box is open, showing the interpretation of the selected data. The 'Key Properties' pane is also visible, showing details for the selected key.

Values/Data Table:

Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 C6 32 62 00 ED 24 C8 01 00 00
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 0C 00

Hex Interpreter Dialog:

Type	Size	Value
signed integer	1-8	128393189712343750
unsigned integer	1-8	128393189712343750
FILETIME (Stored)	8	11/12/2007 5:29:31
FILETIME (As Local)	8	11/12/2007 7:29:31
DOS date	2	-
DOS time	2	-
DOS date/time	4	-
time_t (Stored)	4	-
time_t (As Local)	4	-
Unicode string	2+	ibll

Key Properties Table:

Last Written Time	11/12/2007 5:29:31 UTC
SID unique identifier	1006
User Name	Dustin
Logon Count	756
Last Logon Time	11/12/2007 5:29:31 UTC
Last Password Change Time	9/18/2005 5:54:57 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	11/12/2007 5:29:28 UTC
Account Disabled	false
Password Required	true
Country Code	0 (System Default)
Has LAN Manager Password	true
Has NTLMv2 Password	true

Hex Viewer values:

```

00 02 00 01 00 00 00 00 00 00 c6 32 62 00 ed 24 c8 01 .....E2b·içE·
10 00 00 00 00 00 00 00 00 00 c6 91 ad 7f 15 bc c5 01 .....E·...WA·
20 ff ff ff ff ff ff ff 7f 3a 7f e9 fe ec 24 c8 01 yyyyyyy··épiçE·
30 ee 03 00 01 02 00 00 00 10 02 00 00 00 00 00 00 i·.....
40 00 00 f4 02 01 00 00 00 00 00 00 e7 77 00 00 09 00 ..ô.....çw....
    
```

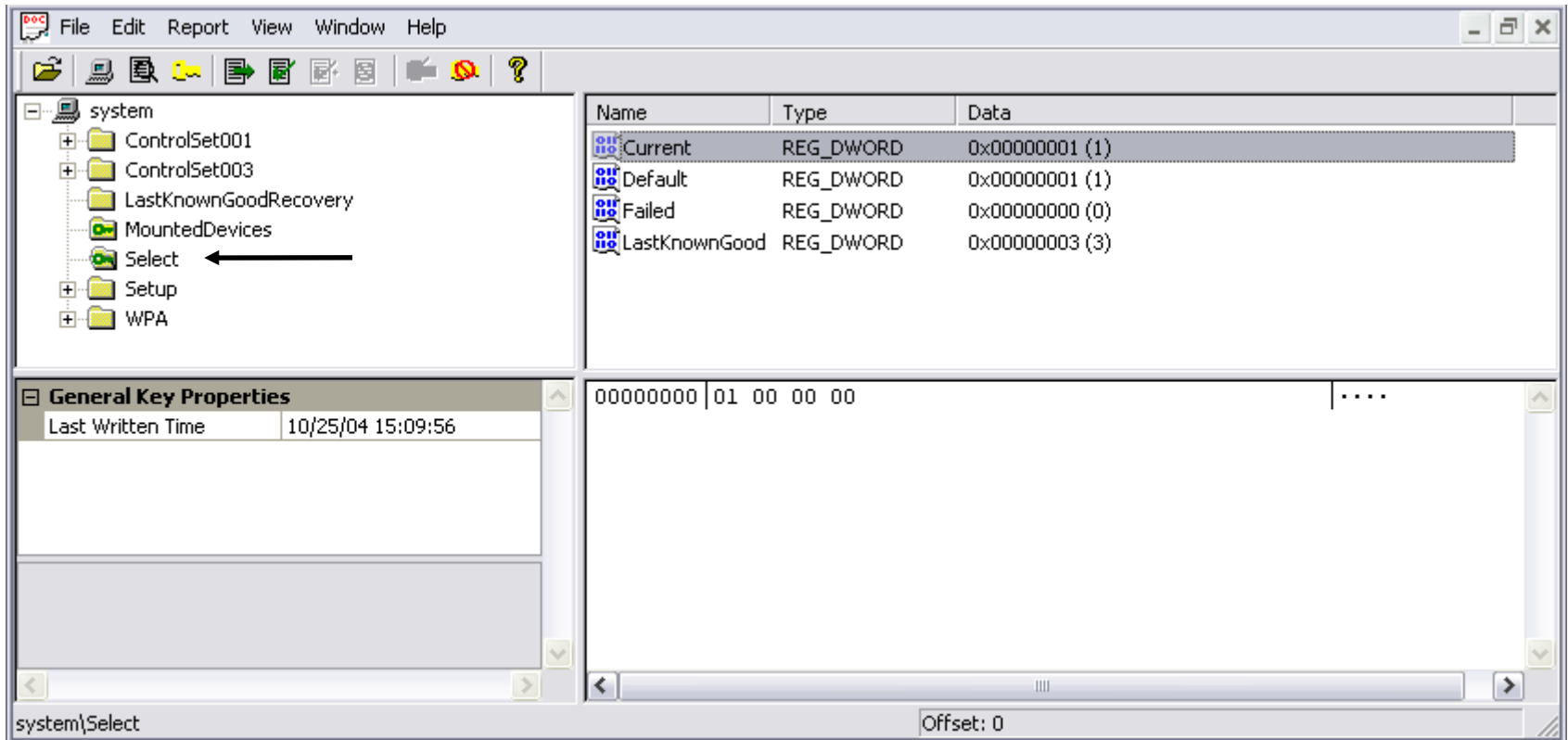
Right click > Show! Hex Interpreter...

Properties pane

Hex Viewer values

Select Key

- CurrentControlSet key is missing in RV?



Get the volatile "CurrentControlSet"
(for Vista/7 and XP: SYSTEM)

Most Recently Used (MRU) Lists

- Ntuser.dat för en viss användare (SID)
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
- HKCU\Software\Google\NavClient\1.1\History
- HKCU\Software\Yahoo\Companion\SearchHistory
- HKCU\Software\Microsoft\Internet Explorer\TypedURLs
- ...
- Check out common areas in Registry Viewer!

Chronological MRU Lists

The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of registry paths, with 'RunMRU' selected under 'Software\Microsoft\Windows\CurrentVersion\Explorer'. The right pane shows a list of registry values for 'RunMRU', sorted chronologically. The values are:

Name	Type	Data
ab MRUList	REG_SZ	qponmlkjihgfedcba
ab q	REG_SZ	regedt32\1
ab p	REG_SZ	explorer\1
ab o	REG_SZ	devmgmt.msc\1
ab n	REG_SZ	calc\1
ab m	REG_SZ	www.sourceforge.net\1
ab l	REG_SZ	www.bigbadandugly.com\1
ab k	REG_SZ	www.hellokitty.com\1
ab j	REG_SZ	regedt32 12:23 /interactive\1
ab i	REG_SZ	defrag\1
ab h	REG_SZ	notepad\1
ab g	REG_SZ	mmc\1
ab f	REG_SZ	c:\gdisk32.exe\1
ab e	REG_SZ	msconfig\1
ab d	REG_SZ	mspaint\1
ab c	REG_SZ	www.google.com\1
ab b	REG_SZ	mstsc\1
ab a	REG_SZ	cmd\1

Below the list, the 'Key Properties' section shows:

- Last Written Time: 2008-02-12 19:28:02 UTC
- Class Name: Shell

The 'ntuser.dat' file is highlighted in the bottom left. The bottom status bar shows the path: Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU and the offset: C Offset: 0.

RecentDocs MRU list

The screenshot shows the AccessData Registry Viewer (tm) - [Common Areas] window. The left pane shows the tree structure of the registry, with 'RecentDocs' selected under 'Explorer'. The right pane shows a list of registry values for 'RecentDocs', all of which are REG_BINARY. The data column shows hexadecimal values representing the MRU list. A callout box labeled 'Unicode' points to the data column. The bottom status bar shows the path 'Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs' and 'Offset: 0'.

Name	Type	Data
MRUListEx	REG_BINARY	07 00 00 00 14 00 00 00 ...
7	REG_BINARY	4D 00 79 00 20 00 50 ...
20	REG_BINARY	62 00 6C 00 6F 00 6E ...
6	REG_BINARY	4E 00 65 00 77 00 20 0...
17	REG_BINARY	4D 00 61 00 70 00 73 ...
19	REG_BINARY	4D 00 61 00 70 00 20 ...
18	REG_BINARY	43 00 6F 00 70 00 79 0...
14	REG_BINARY	4D 00 61 00 70 00 20 ...
12	REG_BINARY	61 00 72 00 77 00 65 0...
11	REG_BINARY	66 00 72 00 6F 00 64 0...
16	REG_BINARY	44 00 5F 00 41 00 6D ...
15	REG_BINARY	65 00 72 00 72 00 6F 0...
2	REG_BINARY	73 00 61 00 75 00 72 0...
13	REG_BINARY	6D 00 79 00 6C 00 6F ...
10	REG_BINARY	74 00 65 00 61 00 73 0...
9	REG_BINARY	62 00 75 00 73 00 68 0...

Key Properties:
Last Written Time: 2006-01-03 20:39:09 UTC

Value Properties:
MRU ordered list: 7, 20, 6, 17, 19, 18, 14, 12, 16, 15, 2, 13, 10, 9

ntuser.dat

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Unicode

Offset: 0

Tidzoner

- NTFS lagrar tider i GMT (UTC)
- Windows visar dessa tider omräknade till motsvarande lokala tider utifrån inställd tidszon
- Tidzonens inställningar finns i
 - HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
 - Dvs. hive: system\ControlSet<#>\...

Time Zone Settings

Vista/7, and XP: SYSTEM

***"Current Control Set"*\Control\TimeZoneInformation**

The screenshot shows the AccessData Registry Viewer application. The left pane displays a tree view of the registry, with the path `Control\TimeZoneInformation` selected. The right pane shows a list of registry values:

Name	Type	Data
Bias	REG_DWORD	0x000001A4 (420)
StandardName	REG_SZ	Mountain Standard Time
StandardBias	REG_DWORD	0x00000000 (0)
StandardStart	REG_BINARY	00 00 0A 00 05 00 02 00 00 00 00 00 00 00 00 00
DaylightName	REG_SZ	Mountain Daylight Time
DaylightBias	REG_DWORD	0xFFFFFFFFC4 (4294967236)
DaylightStart	REG_BINARY	00 00 04 00 01 00 02 00 00 00 00 00 00 00 00 00
ActiveTimeBias	REG_DWORD	0x000001A4 (420)

Below the main table, there is a hex dump of the binary data for StandardStart and DaylightStart:

00000000	4d 00 6f 00 75 00 6e 00-74 00 61 00 69 00 6e 00	M-o-u
00000010	20 00 53 00 74 00 61 00-6e 00 64 00 61 00 72 00	.S-t
00000020	64 00 20 00 54 00 69 00-6d 00 65 00 00 00	d. .7

Evidence in the software hive

- Installed software
 - HKLM\SOFTWARE
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- Last user logged in and last logon time
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Default UserName
 - HKLM\SAM\Domains\Account\Users\F Key

SID och användare

- En SID kan knytas till sin användare med hjälp av HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

AccessData Registry Viewer - [software]

File Edit Report View Window Help

ProfileList

- S-1-5-18
- S-1-5-19
- S-1-5-20
- S-1-5-21-1801674531-1177238915-725345543-1004
- S-1-5-21-1801674531-1177238915-725345543-1005
- S-1-5-21-1801674531-1177238915-725345543-1007
- related.desc
- SeCEdit
- ServicePack
- Setup
- SvcHost
- SystemRestore
- Terminal Server

Name	Type	Data
ProfileImagePath	REG_EXPAND_...	%SystemDrive%\Documents and Settings\Sam
Sid	REG_BINARY	01 05 00 00 00 00 00 05 15 00 00 00 23 5F 63 6B 83 3D 2B 46 07 E5 3B 2E
Flags	REG_DWORD	0x00000000 (0)
State	REG_DWORD	0x00000104 (260)
CentralProfile	REG_SZ	(value not set)
ProfileLoadTimeLow	REG_DWORD	0xB0B006AE (2964326062)
ProfileLoadTimeHigh	REG_DWORD	0x01C4F1D2 (29684178)
RefCount	REG_DWORD	0x00000000 (0)
RunLogonScriptSync	REG_DWORD	0x00000000 (0)

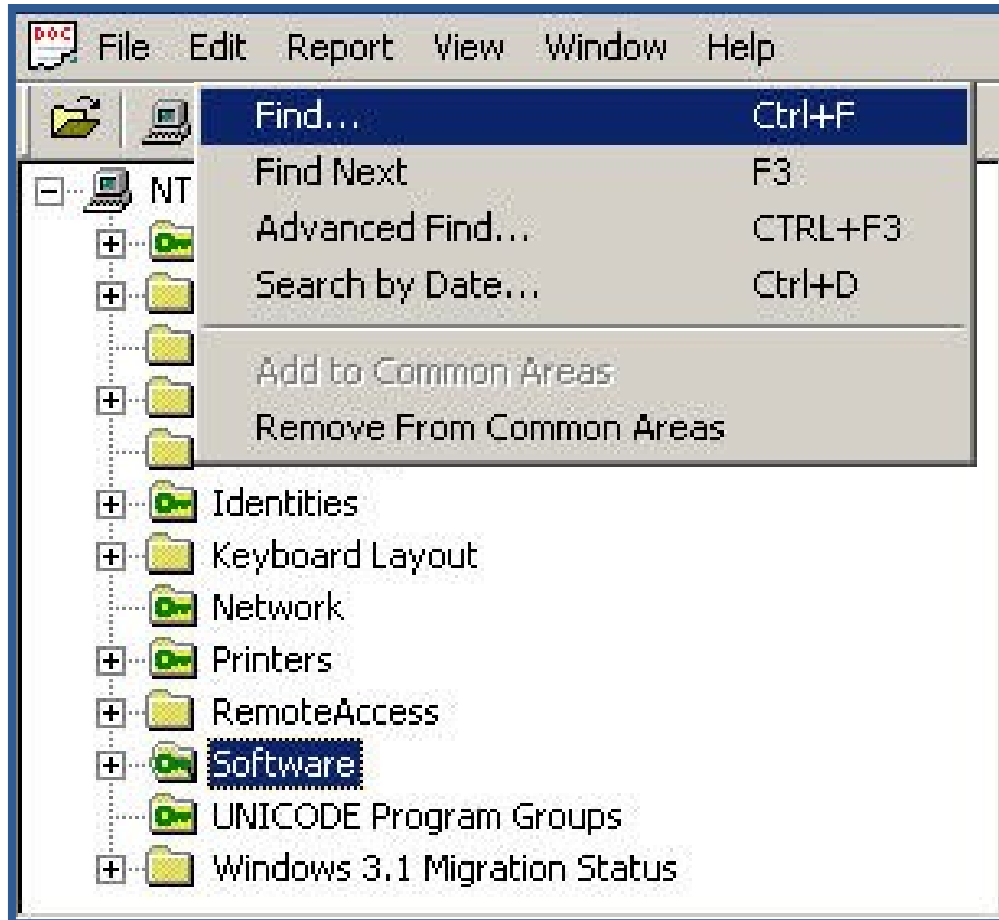
Key Properties

Last Written Time: 2005-01-03 20:28:04 UTC

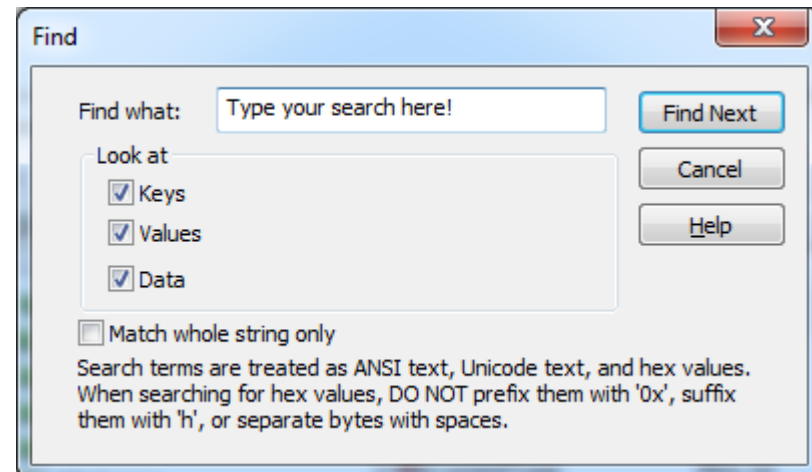
00 25 00 53 00 79 00 73 00-74 00 65 00 6D 00 44 00 | §-S-y-s-t-e-m-D-
10 72 00 69 00 76 00 65 00-25 00 5C 00 44 00 6F 00 | r-i-v-e-§-\-D-o-
20 63 00 75 00 6D 00 65 00-6E 00 74 00 73 00 20 00 | c-u-m-e-n-t-s-
30 61 00 6E 00 64 00 20 00-53 00 65 00 74 00 74 00 | a-n-d-§-e-t-t-
40 69 00 6E 00 67 00 73 00-5C 00 53 00 61 00 6D 00 | i-n-g-s-\-S-a-m-
50 00 00 | ..

software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1801674531-117723 Offset: 0

Quick Find

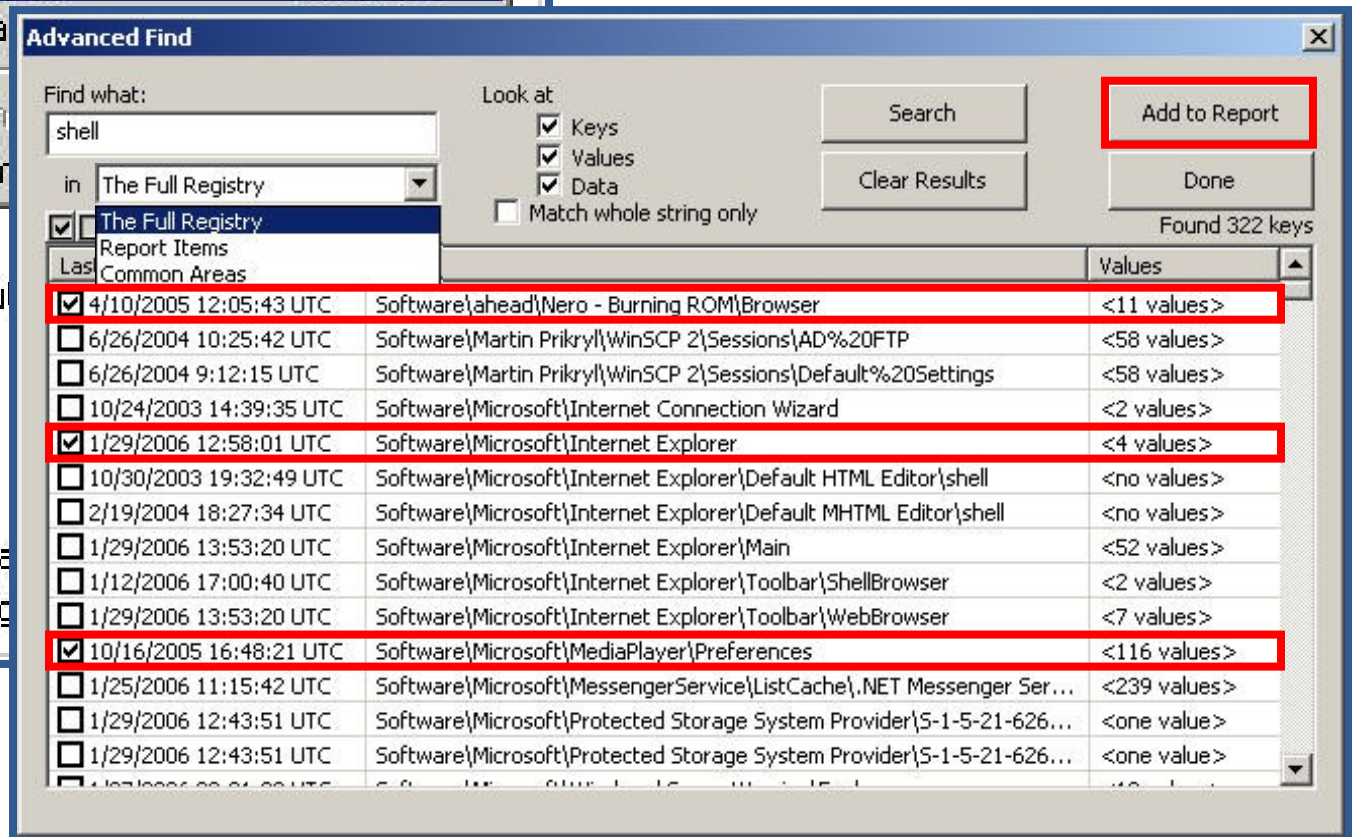
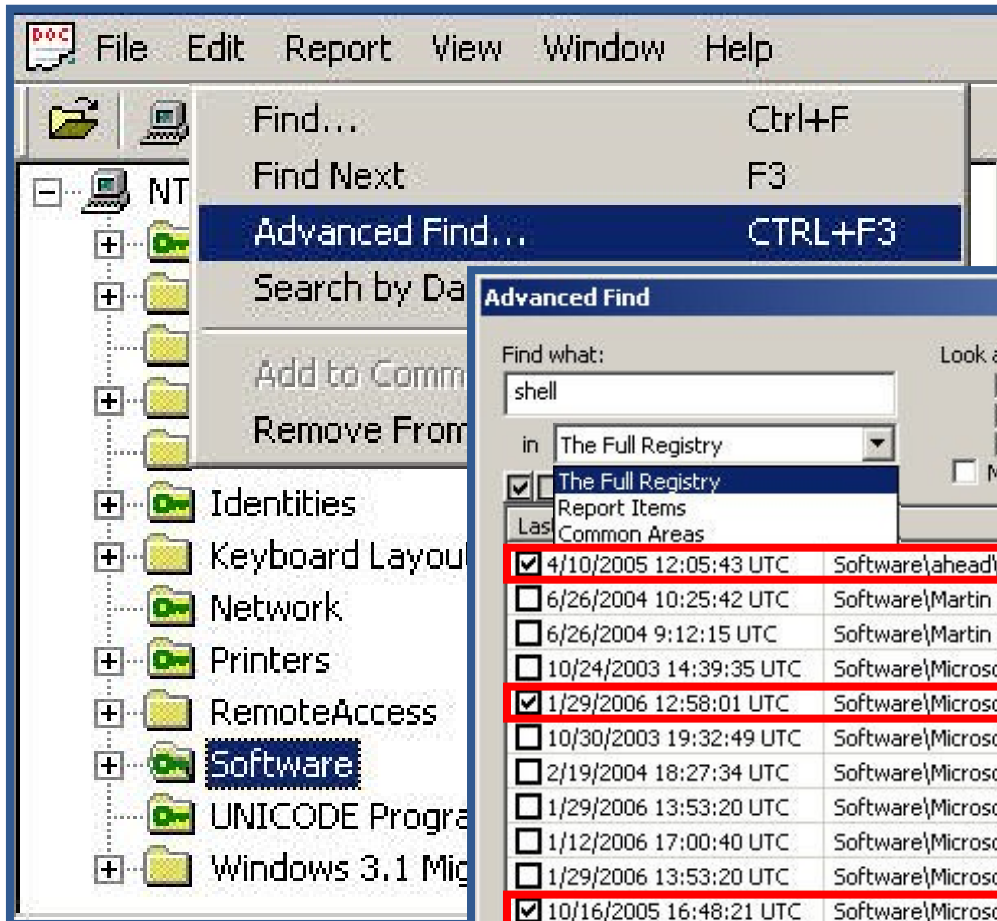


Searches in the
selected key
and its children



Advanced Find

Select search type



Searching by Date

The screenshot shows the Active Setup console with a search for keys modified on 12/24/03. The search results table is highlighted with a red box, and a red arrow points from the 'Last Written Time' field in the 'General Key Properties' pane to the search results.

Name	Type	Data
Account Name	REG_SZ	bad@evil.com
Connection Type	REG_DWORD	0x00000003 (3)
POP3 Server	REG_SZ	bad@evil.com
POP3 User Name	REG_SZ	Bad Person
POP3 Password2	REG_BINARY	01 02 62 00 61 00 64 00 40 00 65 00 76 00 69 00 6C 00 ...
POP3 Use Sicily	REG_DWORD	0x00000000 (0)
POP3 Prompt for Pas...	REG_DWORD	0x00000000 (0)
SMTP Server	REG_SZ	bad@evil.com
SMTP Display Name	REG_SZ	Bad Person
SMTP Email Address	REG_SZ	Bad@Evil.Com

Search by Modification Date

Search for keys modified during a date range: 12/22/2003 - 12/26/2003

Found 594 keys

Modification	Key	Value
12/24/03 17:09:27	Software\Microsoft\EventSystem	<no>
12/24/03 17:09:27	Software\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}	<no>
12/24/03 17:09:27	Software\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subs...	<no>
12/24/03 17:09:26	Software\Microsoft\Fax	<no>
12/24/03 17:09:26	Software\Microsoft\Fax\Setup	<4 v>
12/24/03 17:09:26	Software\Microsoft\Fax\UserInfo	<10>
12/24/03 17:09:26	Software\Microsoft\File Manager	<no>
12/24/03 17:09:26	Software\Microsoft\File Manager\Settings	<no>
12/24/03 17:10:06	Software\Microsoft\IEAK	<no>
12/24/03 17:12:39	Software\Microsoft\Internet Account Manager	<4 v>
12/24/03 17:10:00	Software\Microsoft\Internet Account Manager\Accounts	<4 v>
12/24/03 17:11:10	Software\Microsoft\Internet Account Manager\Accounts\00000001	<10>
12/24/03 17:12:39	Software\Microsoft\Internet Account Manager\Accounts\00000002	<10>

General Key Properties

Last Written Time: 12/24/03 17:11:10

2K.DAT\Software\Microsoft\Internet Account Manager\Accounts\00000001 Offset: 0

HTML Reports

Create Report

Report Title:
Registry Report

Report Location:
C:\Program Files\AccessData\AccessData f

Report Filename:
ID THEFT DUDE - SAM File (.htm)

Reduce excess data output
 Show key properties only
 Also show DWORD values as timestamps
 View Report when created

Buttons: OK, Cancel, Help, Browse...

Registry Report

SAM\Domains\Account\Users\000003EF

Last Written Time	9/26/2003 23:07:30 UTC
SID unique identifier	1007
User Name	ID THEFT DUDE
Full Name	ID THEFT DUDE
Logon Count	8
Last Logon Time	9/26/2003 23:07:30 UTC
Last Password Change Time	Never
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	true
Country Code	0 (System Default)
Has LAN Manager Password	false
Has NTLMv2 Password	false

C:\Program Files (x86)\AccessData\Registry Viewer\report

Defined Summary Reports

Individual
key values
vs.
Entire keys

Including
wildcard
abilities !

Define Summary Report

Summary Report Title:
SAM

Summary Key:

Section Information

Section: 1 Section Title: User Information

Active key: SAM\Domains\Account\Users[*]

Available items: Match any item

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

Included Items:

Name	Key Name
[AD_WildCard]	SAM\Domains\Account\Users[*]

Wildcard Key

Match all immediate children the entire subtree of:

SAM\Domains\Account\Users

Use Currently Selected Key Clear

Remove Value Remove All

Save and Close Cancel Help Preview Report

Integration – PRTK

The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of registry keys, with 'http://www.usair.com/:StringIndex' highlighted in a red box. A context menu is open over this key, listing options such as 'Generate Report...', 'Add to Report', and 'Export Word List...'. The right pane shows a table of registry values for the selected key:

Name	Type	Data
Item Data	REG_MULTI_SZ	Wed Dec 24 18:19:52 2003 ---- badperson Wed Dec 24 ...

A 'Multiple String Values' dialog box is open, displaying the 'Value Name' as 'Item Data' and the 'Data' as:

```
Wed Dec 24 18:19:52 2003 ---- 8822  
Wed Dec 24 18:19:52 2003 ---- badperson
```

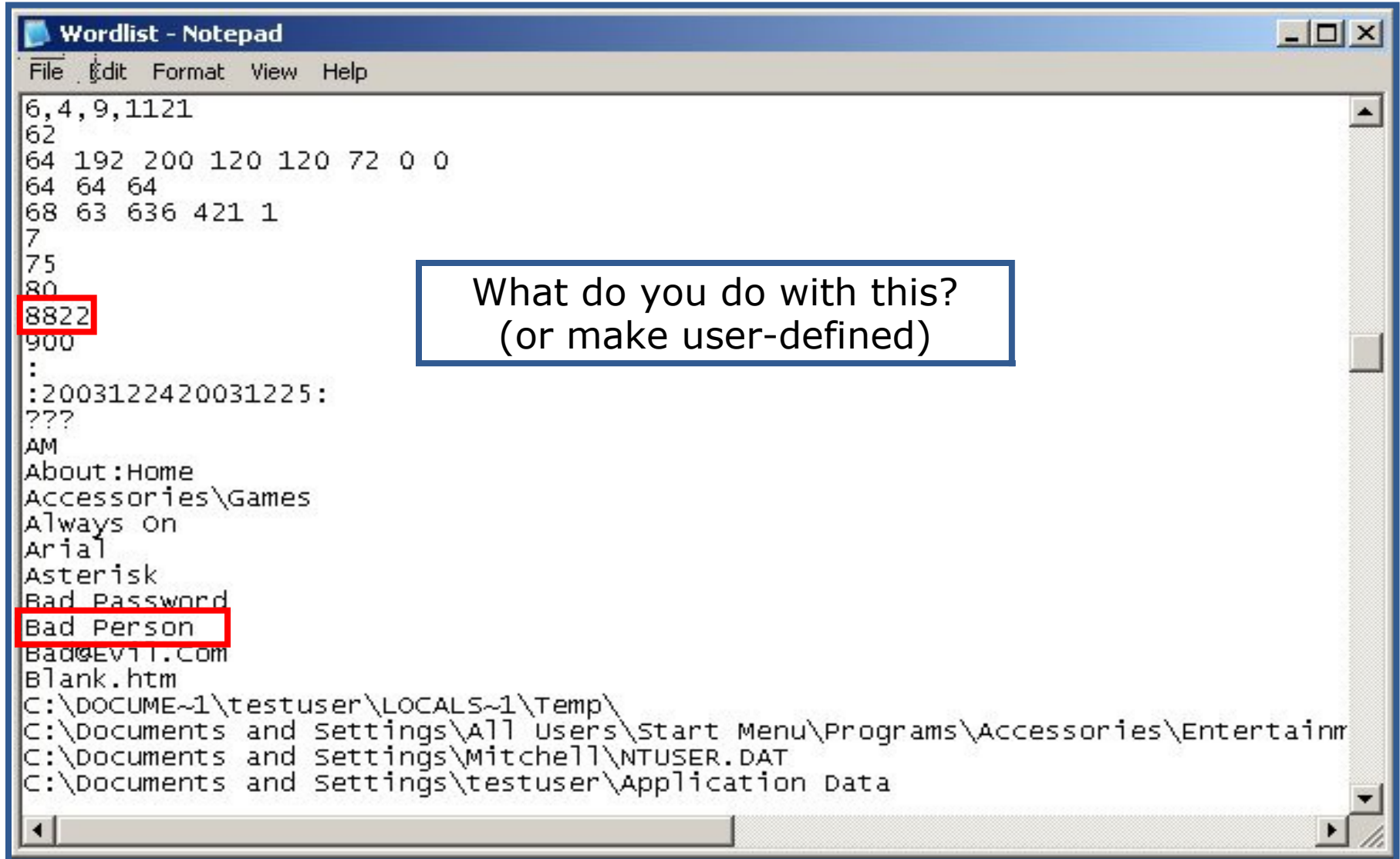
The bottom pane shows the 'General Key Properties' for the selected key, with 'Last Written Time' set to '12/24/03 12:19:54'. A red box highlights the text 'Decrypted Passwords!' in the bottom left corner, with a red arrow pointing from it to the 'Multiple String Values' dialog box.

Decrypted Passwords !

AccessData Registry Viewer

Offset: 0

Integration – PRTK



```
Wordlist - Notepad
File Edit Format View Help
6,4,9,1121
62
64 192 200 120 120 72 0 0
64 64 64
68 63 636 421 1
7
75
80
8822
900
:
:2003122420031225:
???.
AM
About:Home
Accessories\Games
Always On
Arial
Asterisk
Bad Password
Bad Person
Bad@EVTT.com
Blank.htm
C:\DOCUME~1\testuser\LOCALS~1\Temp\
C:\Documents and Settings\All Users\Start Menu\Programs\Accessories\Entertainr
C:\Documents and Settings\Mitchell\NTUSER.DAT
C:\Documents and Settings\testuser\Application Data
```

What do you do with this?
(or make user-defined)

Demo limitations

- In Demo mode, the following program features are disabled
 - Common Areas view, Report view, Generate Report function
 - Decryption and interpretation of protected storage areas (PSSP)

The screenshot shows the AccessData Registry Viewer application window. The title bar reads "AccessData Registry Viewer - [Common Areas]". The menu bar includes "File", "Edit", "Report", "View", "Window", and "Help". The toolbar contains various icons for file operations and help. The left pane shows a tree view of registry paths, with "Common Areas" selected and highlighted with a red box. Below the tree view is a "Key Properties" section, also highlighted with a red box, containing a table of metadata:

Key Properties	
Last Written Time	2004-12-31 21:52:08 UTC
OS Install Date (UTC)	Mon Oct 25 18:58:20 2004
OS Install Date (Local)	Mon Oct 25 20:58:20 2004

Below the properties is a section titled "Last Written Time" with explanatory text. The main pane displays a table of registry values:

Name	Type	Data
SubVersionNumber	REG_SZ	(value not set)
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
InstallDate	REG_DWORD	0x417D4CCC (1098730700)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganization	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	ADXP
SoftwareType	REG_SZ	SYSTEM
CurrentVersion	REG_SZ	5.1
CurrentBuildNumber	REG_SZ	2600
BuildLab	REG_SZ	2600.xpsp_sp2_rtm.040803-2158
CurrentType	REG_SZ	Multiprocessor Free
CSDVersion	REG_SZ	Service Pack 2
SystemRoot	REG_SZ	D:\WINDOWS
SourcePath	REG_SZ	F:\ENGLISH\WINXP\PRO_SP1A\I386
PathName	REG_SZ	D:\WINDOWS
ProductId	REG_SZ	55274-337-8535232-22871
DigitalProductId	REG_BINARY	A4 00 00 00 03 00 00 00 35 35 32 37 34 2D 33 33 37 2D ...
LicenseInfo	REG_BINARY	33 E9 EA 36 F9 DA 7A F8 03 BF 7D 0E 26 1A 47 81 E4 7...

At the bottom of the window, the path "Microsoft\Windows NT\CurrentVersion" is visible, along with a hex dump of the selected value and its ASCII representation "ILJA".