



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



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 stödjande 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

ganize 🔻 📄 Open 🛛 N	ew folder				•= •
🛛 🍌 catroot2	*	Name	Date modified	Туре	Size
CodeIntegrity		Journal	2009-07-14 04:34	File folder	
> 📕 com	_	🔒 RegBack	2012-04-09 11:25	File folder	
4 🍌 config		🔒 systemprofile	2011-04-29 21:46	File folder	
Journal		Jan TxR	2011-04-29 21:48	File folder	
RegBack		BCD-Template	2011-04-30 07:46	File	28 KB
systemprofile			2012-04-18 12:18	File	46 848 KB
JI TxR		DEFAULT	2012-04-18 10:24	File	2 560 KB
s-CZ		SAM	2012-04-18 13:12	File	256 KB
da-DK		SECURITY	2012-04-12 17:34	File	256 KB
de-DE		SOFTWARE	2012-04-18 13:42	File	75 776 KB
Dism		SYSTEM	2012-04-18 13:41	File	23 040 KB
Image: Second	-	COMPONENTS.LOG1	2012-04-18 12:18	LOG1 File	256 KB

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 <u>NTUSER.DAT</u>
 - Preferences, profile areas, mapped drives, MRU..., etc.
 - Copied from HKU upon logon
 - HKU\<User SID>
 - 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>\r or for Vista/7 Users\<username>\ntuser.dat</username></username>
HKU\SID_Classes	Documents and Settings\ <username>\L Data\Microsoft\Windows\UsrClass.dat</username>



Sökvägar till hive-filerna

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

💣 Registry Editor		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>H</u> e	elp	
	Name T	Type Data
⊳ • HAL	ab (Default)	REG_SZ (value not set)
hivelist		REG_SZ \Device\HarddiskVolume4\Boot\BCD
Keyboard Layout		REG_SZ
Keyboard Layouts	AREGISTRY\MACHINE\SAM	REG_SZ \Device\HarddiskVolume5\Windows\System32\config\SAM
⊳ - Lsa =	AREGISTRY\MACHINE\SECURITY R	REG_SZ \Device\HarddiskVolume5\Windows\System32\config\SECURITY
▶ - 1 LsaExtensionConfig	A REGISTRY\MACHINE\SOFTWARE R	REG_SZ \Device\HarddiskVolume5\Windows\System32\config\SOFTWARE
LsaInformation	REGISTRY\MACHINE\SYSTEM	REG_SZ \Device\HarddiskVolume5\Windows\System32\config\SYSTEM
MediaCategories	AREGISTRY\USER\.DEFAULT	REG_SZ \Device\HarddiskVolume5\Windows\System32\config\DEFAULT
🖟 📲 MediaDRM	REGISTRY\USER\S-1-5-19	REG_SZ \Device\HarddiskVolume5\Windows\ServiceProfiles\LocalService\NTUSER.DAT
MediaInterfaces	REGISTRY\USER\S-1-5-20	REG_SZ \Device\HarddiskVolume5\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
MediaProperties	bill and the set of th	REG_SZ \Device\HarddiskVolume5\Users\hjo\NTUSER.DAT
MediaResources	kegistry\User\S-1-5-21-2231859241-240520873-1282944772-1000_Classes R	es REG_SZ \Device\HarddiskVolume5\Users\hjo\AppData\Local\Microsoft\Windows\UsrClass.dat
MediaSets	(Registry\User\S-1-5-21-2231859241-240520873-1282944772-1017	REG_SZ \Device\HarddiskVolume5\Users\UpdatusUser\NTUSER.DAT
MediaTunes	العلى الجار الحري ا 	es REG_SZ \Device\HarddiskVolume5\Users\UpdatusUser\AppData\Local\Microsoft\Windows\UsrClass.dat

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist

HKLM\System\CurrentControlSet

Är härlett från ett annat ControlSet, men vilket?

gradition Registry Editor	_			
Pile Edit View Favorites He Image: My Computer Image: My Computer Image: My Computer Image: My Computer <t< td=""><td>Name (Default) Current Default Failed LastKnownGood</td><td>Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD</td><td>□ Data (value not set) 0x00000001 (1) 0x00000000 (0) 0x00000000 (2)</td><td>l det här fallet från ControlSet001</td></t<>	Name (Default) Current Default Failed LastKnownGood	Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD	□ Data (value not set) 0x00000001 (1) 0x00000000 (0) 0x00000000 (2)	l det här fallet från ControlSet001
MountedDevices			>	
My Computer (HKEY_LOCAL_MACHINE \SYSTEM	Select		.:	

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...

Q AccessData FTK Imager 3.1.0.1514				J
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp		Í	Obtain System Files	×
🕼 🎲 🗣 🗠 🚖 🖾 日 🖬 🚑		e List	Source for obtaining files:	
	N	ame	Warning: Please be aware that FTK Imager is obtainin system files from the live system and not the acquired	g the image.
Custom Content Sources	X		Destination for obtained files:	wse
Evidence:File System Path File	Options		C: \Users \hjo \Desktop	
•	4		Options <u>Minimum files for login password recovery</u>	
New Edit Remove Remove All Create	Image		• Password recovery and all registry files	
Properties Hex Value Int Cust	com Conte		ОКС	ancel
For User Guide, press F1				

Att kopiera hive-filer från en image

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

🔍 AccessData F	TK Imager																	_	
<u>File View M</u> ode																			
🏥 🏩 🏩 🖴	t 🖾 🖬 🖬 4	e e = 🖻 🤇		<u>a</u>	2	گ آ	EXT	HEX	ା 💡	' -									
Evidence Tree		×	File List																×
	comsvcs.d		Name								Size	Туре				Dat	e Mod	dified	
	comuid.dll		🗐 Secu	RITY.L	.OG						1 KB	Regu	lar fi	le		200	9-03-	-31 11	:46:5
	🖃 🧰 config		🖻 softw	are						21 7	60 KB	Regu	ılar fi	le		200	9-03-	-31 11	:47:4
	C default	.LOG 📃	🗐 softw	are.LC	G						1 KB	Regu	llar fi	le		200	9-03-	-31 11	:47:4
	SAM.L	OG	🖻 softw	are.sa	N.					6	44 KB	Regu	lar fi	le		200	7-03-	-09 13	:41:4
	E SECUR	RITY.LOG	🗟 SysEv	ent.Ev	vt					5	12 KB	Regu	lar fi	le		200	9-03-	-31 11	:47:4
	t softwar	re.LUG	syster	m _						53	76 KB	Regu	lar fi	le _		200	9-03-	-31 1 <u>1</u>	:47:
	🖂 🖂 🖂	LUG	🗐 syste	n.LOG							1 KB	Regu	lar fi	le		200	9-03-	-31 11	:47:4
	H- C system	profile	🚾 syste	m.sav						8	40 KB	Regu	lar fi	le		200	7-03-	-09 13	:41:4
	L Iempr	ley.LUG	🗐 Templ	Key.LC	DG						1 KB	Regu	ılar fi	le		200	7-03-	-09 13	:41:4
			🔟 userd	iff						2	56 KB	Regu	ılar fi	le		200	7-03-	-09 13	:41:4
 			🗐 userd	iff.LOC	3						1 KB	Regu	lar fi	le		200	7-03-	-09 13	:41:
Hex Value Interpret	er	×	•																ЪĒ
Туре	Size Value		000000	72	<u> </u>	67	66	62	1.4	00	00-62	1.4	00	00	£0	2h f	2 02	rec	fart
signed integer	1-8			f6 1	63 - 61 -	07 69	00	03	14	00	00-05	14	00	00	00	20 L 00 0	5 02 N NN	L Ö+R	
unsigned integer	1-8		000020	01	00 1	00	00	20	00	00	00-00	10	50	00	01	00 O	0 00		
FILETIME (UTC)	8		000030	53	00	59	00	53	00	54	00-45	00	4d	00	00	00 0	0 00	5.1	·s.
DOS date	2		000040	00	00	00	00	00	00	00	00-00	00	00	00	00	00 0	0 00		
DOS time	2		000050	00	00	00	00	00	00	00	00-00	00	00	00	00	00 0	0 00		•••
time_t (UTC)	4		000060	00	00	00	00	00	00	00	00-00	00	00	00	00	00 0	0 00	•••	•••
time_t (local)	4		000070	00	00	00	00	00	00	00	00-00	00	00	00	00	00 0	0 00	! •••	••••
					00	00	00	00	00	00	00-00	00	00	00	00	00 U 00 0	0 00		
			000090		00 0	00	00	00	00	00	00-00	00	00	00	00	00 U 00 0	0 UU D DO		
•		•	0000000	00	00 1	00	00	00	00	00	00-00	00	00	00	00	00 0	0 00		
Bute order:	I little endian	C Big endian	0000c0	00	00	00	00	00	00	00	00-00	00	00	00	00	00 0	0 00		••••
byte order.	S Endo chaian	S big crititan	•																ЪĒ
Properties	Hex Value Inter	Custom Content	Cursor po	s = 0;	; clus	5 = 2	2437	967	; log	sec :	= 19503	3736							
For Help, press F1																			
																			//

File Menus

AccessData Registry Viewer (tm) - [2K.DAT]		
Cascade 8		그러즈
2K.DAT AppEvents Console Control Panel Environment Environment	Name Type Data Image: Temp REG_EXPAND_SZ %USERPROFILE%\Local Settings\Temp Image: Temp REG_EXPAND_SZ %USERPROFILE%\Local Settings\Temp	
General Key Properties Last Written Time 12/24/03 17:09:26	00 25 00 55 00 53 00 45 00-52 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 ff:U:S:E:R:P:R:O: 20 63 00 61 00 6c 00 20 00-53 00 65 00 74 00 r::::::::::::::::::::::::::::::::::::	
	Offset: 0	1.

Tool Icons and Common Areas (Favorites)

🧟 AccessData Registry Viewer - Educatio	n - [Common Areas]					×			
📴 <u>F</u> ile <u>E</u> dit <u>R</u> eport <u>View</u> <u>W</u> indow <u>H</u> elp									
🕞 🚊 🖳 📭 📑 🗑 📓 💷	B ?								
Common Areas	Name	Туре	Data			-			
	DurrentVersion	REG_SZ	6.0						
ProfileList	DurrentBuildNumber	REG_SZ	6000			Ξ			
Run	ab CurrentBuild	REG_SZ	6000						
Windows NT	■ SoftwareType	REG_SZ	System						
winlocon	ab CurrentType	REG_SZ	Multiprocessor Free						
	👸 InstallDate	REG_DWORD	0x4671BF9D (118185974	41)					
	(a) RegisteredOrganization	REG_SZ	(value not set)						
Key Properties	and RegisteredOwner	REG_SZ	Dustin						
Last Written Tin 2008-02-15 13:51:	မာ့် SystemRoot	REG_SZ	C:\Windows			-			
OS Install Date (Thu Jun 14 22:22:	0 36 00 2E 00 30 00 0	0 00-		60		~			
OS Install Date (Fri Jun 15 00:22:21									
OS Install Date (Local)									
This indicates the time when the									
operating system was installed.						$\overline{\mathbf{v}}$			
AccessData Registry Viewer			C Offset: 0						

Properties and Interpreters

File Edit Report View	Window Help		[
😂 🚊 🖪 🖬 📑 🖥	🖻 🖻 🛑 🖦 💡	50.		Valu	es/D	ata				
🖃 🗐 SAM 🔺 👘		Name	Туре		Data	э				
🖻 🧰 SAM	Hive	88 F	REG_	BINARY	02 0	0 01 00 0	00 00 00	00 C6 32	: 62 00 ED 24 C8 01 00	0 00
Domains		88 V	REG_	BINARY	00 0	00 00 00 0	3C 00 00	00 02 00	01 00 BC 00 00 00 0C	: 00
		1000								
	Kay a lay history			and the state					w l	
E Groups	Keys/subkeys		Hex Incer	precer						
	00154		Type		Size	Value				
	00165		signed inte	eger	1-8	128393	31897123	343750		
	00250		FILETIME	(Stored)	1-0	120333	2007 5.2	943730		
	003ER		FILETIME	(As Local)	8	11/12/	2007 7:2	9:31		
	003ED		DOS date		2	10.000				
	003EE		DOS time		2					
	003F1		DOS date	/time	4	32453				
🛅 000	003F2		time_t (Sto	l ocal)	4	10.00				
	003F3 🔫		Unicode s	trina	2+	ю				
E Key Properties						1000				
Last Written Time	11/12/2007 5:29:31 UTC		Byte	order:	 Little 	endian	C	Big endia	n	
SID upique identifier	1006	3					4			
User Name	Dustin	1 1	Right	click	> S	how	/Ho	v Inf	tornrotor	
Logon Count	756		Ngin	CIICK	- 0	110 1			ler preter m	-
Last Logon Time	11/12/2007 5:29:31 UTC	00 02 00 0	01 00 00	00 00 00)- <mark>c6 3</mark> ;	2 62 00) ed 24	4 c8 01	E2b·íş	ŧÈ۰
Last Password Change Time	9/18/2005 5:54:57 UTC	10 00 00 0	00 00 00	00 00 00)-c6 9.	l ad 71	15 bo	c c5 01	E	٩Å٠
Expiration Time	Never	20 ff ff f	f ff ff	ff ff 7f	5-3a 71	f e9 fe	e ec 24	4 c8 01	. ÿÿÿÿÿÿÿ ∵∵éþì\$	۶E・
Invalid Logon Count	0	30 ee 03 0		02 00 00)-10 0;	2 00 00	00 00	0 00 00) 1	••••
Last Failed Login Time	11/12/2007 5:29:28 UTC	40 00 00 1	4 02 01	ου ου οι	J-00 01	Je/ /.	r 00 00) 09 OC) oĉm	
Account Disabled	false									
Password Required	true		He	y Viev	wer v	value	S			
Country Code	0 (System Default)									
Has LAN Manager Password	true									
Has NTLMv2 Password	true									

Properties pane

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

🥵 AccessData Registry Viewer - Education - [Common A	(reas]		
Eile Edit Report View Window Help			_ & ×
i 🖆 🚇 🖳 🖛 📄 🗃 🐼 📓 💷 🛸 🤶			
Common Areas	Name	Туре	Data
🔒 💼 Adobe	ab MRUList	REG SZ	gponmlkijhgfedcba
🖶 💼 AppEvents	ചിപ	REG SZ	renedt32\1
ia comDlg32	ചിച്ച	REG SZ	explorer\1
E CurrentVersion	ഷീം	REG SZ	devmant msc/1
Explorer	ഷീം	REG SZ	calc/1
i	ഷീന	REG SZ	www.sourceforge.pet\1
i ⊡ ⊡ Identities	ച്ച	REG_SZ	www.sourcerorge.net/1
i IntelliForms ≡	abl L	REG_SZ	www.bigbadandugiy.com\1
⊡ Internet Explorer	abl:	REG_SZ	regenter2212:22 (interactive)1
	le≕]) [ab]:	REG_SZ	defrag\1
Map Network Drive MRU	ալ	REG_SZ	
E Intwork	eein labha	REG_SZ	notepad\1
	2019 1910	REG_SZ	mmc\1
H De Printers		REG_SZ	c:\gdisk32.exe\1
Protected Storage System Dravider	e e	REG_SZ	msconfig\1
Protected Storage System Provider	i i i i i i i i i i i i i i i i i i i	REG_SZ	mspaint\1
RecentFileList	en c	REG_SZ	www.google.com\1
RecentFileList	in p	REG_SZ	mstsc\1
	[ab)]a	REG_SZ	cmd\1
RunMRU			
	00 77 00 77 0	0 77 00 28 00 4	68 00 65 00 6C 00 6C 00 11 11 11 10 10 10 10
E Key Properties	10 6F 00 6B 0	0 69 00 74 00-7	74 00 79 00 2E 00 63 00 o.k.i.t.t.vc.
Last Written Time 2008-02-12 19:28:02 UTC	20 6F 00 6D 0	0 5C 00 31 00-0	00 00 o·m·\·1···
Class Name Shell			
ntuser.dat			-
Software\Microsoft\Windows\CurrentVersion\Explorer\R	unMRU		C Offset: 0

RecentDocs MRU list

AccessData Registry Viewer (tm) - [Common	ı Ar	eas]			
Eait Report View Window Help					- 0'
🚰 🔜 🖹 🖛 🖶 🗑 🐼 💷 🛸 🎗					
🖃 🗐 Common Areas	^	Name	Туре	Data	
🕂 📴 AppEvents		10 MRUListEx	REG BINARY	07 00 00 00 14 00 00 0	
🕀 📴 ComDlg32		88 7	REG BINARY	4D 00 79 00 20 00 50	
🕀 📴 CurrentVersion		20	REG BINARY	62 00 6C 00 6F 00 6E	
🗄 🖸 Explorer		886	REG BINARY	4E 00 65 00 77 00 20 0	
		17	REG BINARY	4D 00 61 00 70 00 73	
ICQ		88 19	REG BINARY	40 00 61 00 70 00 20	
		88 18	REG BINARY	43 00 6E 00 70 00 79 0	
	≣	80 14	DEC BINARY	40.00.61.00.70.00.20	
🕀 🖻 Internet Explorer		80 10	REG_DINART	40 00 01 00 70 00 20	
🕀 🗠 Kazaa		00 11 00 11	REG_DINART	65 00 72 00 77 00 65 0	
Map Network Drive MRU			REG_DINART		
• Network		00 10 00 10	REG_BINARY	44 00 5F 00 41 00 6D	
		00 15	REG_BINARY	65 00 72 00 72 00 6F 0	
Hand Printers			REG_BINARY	/3 00 61 00 /5 00 /2 0	Lln
🛨 🔤 profiles		13 000	REG_BINARY	6D 00 79 00 6C 00 6F	011
Protected Storage System Provider		10 000-	REG_BINARY	74 00 65 00 61 00 73 0	
		<u>100</u> 9	REG_BINARY	62 00 75 00 73 00 68 0	
		00 07 00 00 0	0 14 00 00	00-06 00 00 00 11 00 00	00
Run		10 13 00 00 0	0 12 00 00	00-0e 00 00 00 0c 00 00	00
RunMRU	~	20 06 00 00 0	0 10 00 00	00-0£ 00 00 00 02 00 00	00
		30 0d 00 00 0	0 0a 00 00 I	00-09 00 00 00 08 00 00	00
E Key Properties		40 03 00 00 0	0 01 00 00 I	00-05 00 00 00 04 00 00	00
Last Written Time 2006-01-03 20:39:09 UTC		SULL IL IL I	I		1 AAAA
Value Properties					
MRU ordered list 7, 20, 6, 17, 19, 18, 14, 12	4, 1				
	=	<			>
	-				

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\TimeZ oneInformation
 - Dvs. hive: system\ControlSet<#>\...

Time Zone Settings

Vista/7, and XP: SYSTEM

"Current Control Set"\Control\TimeZoneInformation

File Edit Report View Window Help Image: PriorityControl PriorityControl PriorityControl PriorityControl Image: PriorityControl PriorityControl PriorityControl PriorityControl PriorityControl Image: ProductOptions StandardName REG_DWORD 0x00000000 (0) 0x0000000 (0) Image: Providers SecureProviders PriorityControl PriorityControl PriorityControl Image: Provider PriorityControl PriorityControl PriorityControl PriorityControl PriorityControl Image: Providers PriorityControl PriorityControl PriorityControl PriorityControl PriorityControl Image: Provider PriorityControl	🔀 AccessData Registry Viewer (tm) - [system]					
Image: Security Providers Name Type Data Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Providers Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider Image: Security Provider S	File Edit Report View Window Help					
Print Name Type Data PriorityControl PriorityControl ProductOptions 0x000001A4 (420) SafeBoot StandardName REG_SZ Mountain Standard Time ScsiPort StandardStart REG_DWORD 0x0000000 (0) ScsurePipeServers Scaure/PipeServers StandardStart REG_SZ Mountain Daylight Time Secure/PipeServers Secure/PipeServers DaylightName REG_SZ Mountain Daylight Time Secure/Providers Secure/PipeServers DaylightStart REG_DWORD 0xFFFFFFC4 (4294967236) ServiceGroupOrder ServiceFrovider DaylightStart REG_DWORD 0x000001A4 (420) Session Manager Setup 00000000 4d 00 6f 00 75 00 6e 00-74 00 61 00 69 00 6e 00 M·o··· SystemResources 00000000 4d 00 20 00 54 00 69 00-6d 00 65 00 00 00 ·s·t Mudate UsbFlags Video Video ·s·t	🗳 🚇 🕰 😓 📑 🗑 🖉 🦉	<u>K</u> . 1	• ?			
PriorityControl ProductOptions ProductOptions StandardName REG_SZ Mountain Standard Time SafeBoot StandardStart REG_BINARY 00 00 00 00 00 00 00 00 00 00 00 00 00	庄 - 🧰 Print		Name	Туре	Data	
ProductOptions StandardName REG_SZ Mountain Standard Time B	PriorityControl		Bias	REG_DWORD	0x000001A4 (420)	
SareBoot StandardBias REG_DWORD 0x00000000 (0) ScsiPort ScsiPort StandardBias REG_BINARY 00 00 A0 00 50 00 20 00 00 00 00 00 00 00 00 00 00 00			DistandardName	REG_SZ	Mountain Standard Time	
Setup 00000000 4d 00 6f 00 75 00 6e 00-74 00 61 00 69 00 6e 00 M·o·l▲ Stillmage 00000000 20 00 53 00 74 00 61 00-6e 00 64 00 61 00 72 00 ·S·t Terminal Server 000000020 64 00 20 00 54 00 69 00-6d 00 65 00 00 00 ·S·t Update ·S·that ·S·t ·S·t Video ·S·tillitude ·S·t ·S·t Video ·S·t ·S·t ·S·t Video ·S·t ·S·t ·S·t Video ·S·t ·S·t ·S·t Video ·S·t ·S·t ·S·t ·S·t ·S·t ·S·t	 ⊕ · · · · · · · · · · · · · · · · · · ·		StandardBias StandardStart DaylightName DaylightBias DaylightStart ActiveTimeBias	REG_DWORD REG_BINARY REG_SZ REG_DWORD REG_BINARY REG_DWORD	0x00000000 (0) 00 00 0A 00 05 00 02 00 00 00 00 00 00 00 00 00 Mountain Daylight Time 0xFFFFFFC4 (4294967236) 00 00 04 00 01 00 02 00 00 00 00 00 00 00 00 00 0x000001A4 (420)	
	Setup StillImage StillImage SystemResources Terminal Server TimeZoneInformation Update SystemResources Update Update StillImage Update UsbFlags Video		00000000 4d 00 00000010 20 00 00000020 64 00	0 6f 00 75 00 0 53 00 74 00 0 20 00 54 00	6e 00-74 00 61 00 69 00 6e 00 M·o·1▲ 61 00-6e 00 64 00 61 00 72 00 ·S·t 69 00-6d 00 65 00 00 00 d· ·1 d· ·1	

Evidence in the software hive

- Installed software
 - HKLM\SOFTWARE
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ap p Paths
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Un install
- 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	*	Name	Туре	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	0x0000000 (0)	
S-1-5-21-1801674531-1177238915-725345543-1005		👭 State	REG_DWORD	0x0000104 (260)	
S-1-5-21-1801674531-1177238915-725345543-1007		a CentralProfile	REG_SZ	(value not set)	
		🔀 ProfileLoadTimeLow	REG_DWORD	0xB0B006AE (2964326062)	
🛅 SeCEdit		🔀 ProfileLoadTimeHigh	REG_DWORD	0x01C4F1D2 (29684178)	
ServicePack		ut RefCount	REG_DWORD	0x0000000 (0)	
💼 Setup		🔀 RunLogonScriptSync	REG_DWORD	0x0000000 (0)	
🛅 SvcHost					
🛅 SystemRestore					
- Terminal Server	Ŧ				
I → 100 × 100	_			4	
Key Properties		00 25 00 53 00 79 00	73 00-74 00 6	5 00 6D 00 44 00 %·S·y·s·t·e·m·D·	
Last Written Time 2005-01-03 20:28:04 UTC		10 72 00 69 00 76 00 20 63 00 75 00 6D 00) 65 00-25 00 5) 65 00-68 00 7	C 00 44 00 6F 00 r·i·v·e·\$·\·D·o·	
		30 61 00 6E 00 64 00) 20 00-53 00 6	5 00 74 00 74 00 a n d · Sett	
	_	40 69 00 6E 00 67 00	73 00-5C 00 5	3 00 61 00 6D 00 i·n·g·s·∖·S·a·m·	
		50 00 00		••	
				*	
software\Microsoft\Windows NT\CurrentVersion\ProfileList	t\S-:	L-5-21-1801674531-117723	Offset: 0		

Quick Find

📴 File Edit	Report View Window	Help				
	Find	Ctrl+F				
	Find Next	F3				
	Advanced Find	CTRL+F3				
÷	Search by Date	Ctrl+D				
±	Add to Common Areas Remove From Common Are	eas				
🗄 📴 Ide	entities					
🗄 🛅 Ke	yboard Layout					
🔜 Ne	💮 Network					
🕂 📴 Pri	nters					
🗄 📄 Re	🗄 🧰 RemoteAccess					
庄 😇 🚾 So	ftware					
🖳 💽 UN	IICODE Program Groups					
🗄 🛄 Wi	ndows 3.1 Migration Status					

Searches in the selected key and its children

Find		×
Find what:	Type your search here!	Find Next
Look at		Cancel
Values		<u>H</u> elp
🔽 Data		

Match whole string only

Search terms are treated as ANSI text, Unicode text, and hex values. When searching for hex values, DO NOT prefix them with '0x', suffix them with 'h', or separate bytes with spaces.

Advanced Find

File E	Edit Report View	w Window Help		Sel	ect sea	arch
	Find	CtrlH	FF			
	Find Next	F3	-		type	
÷	Advanced Find	i CTRI	L+F3			
÷.	Search by Da	Advanced Find				×
	Add to Comm	Find what:	Look at	Keys	Search	Add to Report
	Remove From	in The Full Registry	<u>v</u>	Values Data	Clear Results	Done
	Identifies			ch whole string only	() () () () () () () () () () () () () (Found 322 keys
		Las Common Areas				Values 🔺
±	Keyboard Layou	☑ 4/10/2005 12:05:43 UTC	Software\ahead\Ne	ro - Burning ROM\Browse	er	<11 values>
	Network	6/26/2004 10:25:42 UTC	Software\Martin Pri	kryl\WinSCP 2\Sessions\A	D%20FTP	<58 values>
		6/26/2004 9:12:15 UTC	Software\Martin Pri	kryl\WinSCP 2\Sessions\D	efault%20Settings	<58 values>
±	Printers	10/24/2003 14:39:35 UTC	Software\Microsoft	Internet Connection Wiz	ard	<2 values>
मि 🦳	RemoteAccess	✓ 1/29/2006 12:58:01 UTC	Software\Microsoft	Internet Explorer		<4 values>
		10/30/2003 19:32:49 UTC	Software\Microsoft	Internet Explorer\Defaul	t HTML Editor\shell	<no values=""></no>
E	Sortware	2/19/2004 18:27:34 UTC	Software\Microsoft	Internet Explorer\Defaul	t MHTML Editor\shell	<no values=""></no>
O-	UNICODE Progra	1/29/2006 13:53:20 UTC	Software\Microsoft	(Internet Explorer\Main		<52 values>
÷ 👝	THE ALL OF MARK	1/12/2006 17:00:40 UTC	Software\Microsoft	Internet Explorer\Toolba	r\ShellBrowser	<2 values>
	WINDOWS 3.1 Mig	1/29/2006 13:53:20 UTC	Software\Microsoft	Internet Explorer\Toolba	r\WebBrowser	<7 values>
		✓ 10/16/2005 16:48:21 UTC	Software\Microsoft	(MediaPlayer\Preferences	5	<116 values>
		1/25/2006 11:15:42 UTC	Software\Microsoft	MessengerService\ListCa	ache\.NET Messenger Ser	<239 values>
		1/29/2006 12:43:51 UTC	Software\Microsoft'	Protected Storage Syste	m Provider\S-1-5-21-626	<one value=""></one>
		1/29/2006 12:43:51 UTC	Software\Microsoft	Protected Storage Syste	m Provider\S-1-5-21-626	<one value=""></one>
		LE La localecer de los une	1 - 0 1 - 0	or the second		

Searching by Date

📴 File Edit Report View Window Help				_ 8 ×
Active Setup	Name	Туре	Data	1
📮 🧰 Installed Components	Account Name	REG_SZ	bad@evil.com	
	Connection Type	REG_DWORD	0×00000003 (3)	
>{60B49E34-C7CC-11D0-8953	POP3 Server	REG_SZ	bad@evil.com	
2179C5D3-EBEE-11CE-B6ED-C	POP3 User Name	REG_SZ	Bad Person	
{22d6f312-b0f6-11d0-94ab-00	POP3 Password2	REG_BINARY	01 02 62 00 61 00 64 00 40 00 65 00 76 00 69 00 6C 00	
(44BBA840-CC51-11CF-AAFA-I	POP3 Use Sicily	REG_DWORD	U×00000000 (0)	
44BBA842-CC51-11CF-AAFA-	ab SMTP Server	PEG_DWORD	bad@evil.com	
448BA848-CC51-11CF-AAFA-1	SMTP Display Name	REG_SZ	Bad Person	
{7790769C-0471-11d2-AE11-0	SMTP Email Address	REG_SZ	Bad@Evil.Com	
Optional Component Sync				
Advanced INF Setup	Search by	Modification Dat	P	
Clock				
EventSystem	Search for k	eys modified	12/22/2003	Report
E Fax		ing a date range		Tropore
Setup		ing and arter a give ing and before a give	en date 12/26/2003 👻 Clear Results Do	ne
UserInto		ing and before a gr	Foundate , Foundate	d 594 keys
	Modification	[Key	Value 🔺
🖃 🦲 Internet Account Manager	12/24/03	17:09:27	Software\Microsoft\EventSystem	<no< td=""></no<>
Accounts	12/24/03	17:09:27	Software\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}	<no< td=""></no<>
	12/24/03	17:09:27	Software\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subs	<no< td=""></no<>
	12/24/03	17:09:26	Software\Microsoft\Fax	<no< td=""></no<>
🖻 General Key Pronerties 📃 📥	00 62 12/24/03	17:09:26	Software\Microsoft\Fax\Setup	<4 v
Last Written Time 12/24/03 17:11:10	10 2e 12/24/03	17:09:26	Software(Microsoft)Eile Mapager	<10
	12/24/03	17:09:26	Software(Microsoft)File Manager	<00
	19/24/03	17:10:06	Software\Microsoft\IEAK	
	12/24/03	7:12:39	Software\Microsoft\Internet Account Manager	<4 v
	12/24/03	17:10.02	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
	4	17.10.10		
				*
2K.DAT\Software\Microsoft\Internet Account Manager\Accoun	ts\00000001		Offset: 0	1.

HTML Reports



Registry Report

SAM\Domains\Account\Users\000003EF

Last Written Time	0/26/2002 22:07:20 ITC
Last written Time	9/20/2003 23.07.30 UIC
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
Logon Count Last Logon Time Last Password Change Time Expiration Time Invalid Logon Count Last Failed Login Time Account Disabled Password Required Country Code Has LAN Manager Password Has NTLMv2 Password	8 9/26/2003 23:07:30 UTC Never 0 Never false true 0 (System Default) false false

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

Defined Summary Reports

Individual key values vs. Entire keys

Including wildcard abilities !

minda y report relot	-Section Information		
AM	Section: Sect	tion Title:	
P.		er Information	
mmary Key:		er miormadon	
🚊 🛅 Domains 📃 📃	Active key: SAM\Domains	<pre>s\Account\Users\[*]</pre>	
	C Available items:		Match any item 💿
🕀 🧰 Aliases	Name	Type	Data
	nu E	REG BINARY	02 00 01 00 00 00 00 00 00 00 00
	nit V	REG BINARY	00 00 00 00 BC 00 00 00 02 00 01
0000013			
🎦 000003EA	10		
<u>*</u> 1000003EB	•		<u> </u>
	Included Items:	Add Unlisted Valu	Le Add Value(s) Select All
	Included Icents.		
	Name	Key Name	
🛨 🚵 Names 📃 🔪		CAMI Domoinel Ac	couptil lears [*]
	[AD_WildCard]	SAMOUNIAINS(AU	codictosers([]
⊕- Names ⊕- Builtin RXACT	[AD_WildCard]	COAMUDOINIAINS (AU	conicioseis([]
⊕-/ Mames ⊕-/ Builtin RXACT ✓	[AD_WildCard]	SAMUDOMAINS (AU	
	[AD_WildCard]	SAMUDUMAINS(AU	condoseis(L]
	[AD_WildCard]	SAMUUUIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	count/oscis/[]
	[AD_WildCard]	SARIUUUIIIIIIIIIIIIIIIII	count(osois([]

Integration – PRTK

AccessData Registry Viewer (tm) - [2K]						
File Edit Report View Window Help						<u>_B×</u>
🗁 🗐 🖳 Generate Report						
Add to Report Add to Report with Children Remove from Report	▲ 0284298-1000	Name Miltem Data	Type REG_MULTI_SZ	Data Wed Dec 24 18:19:52 : ing Values	2003 badperson Wed Dec 24	
Manage Summary Reports Define Summary Report			Value Name: Item Data			
https://webmail.pas.earth	ngData ink.net/wam/login.jsp:StringData		Data: Wed Dec 24 1 Wed Dec 24 1	3:19:52 2003 8822 3:19:52 2003 badpe	rson	
a http://www.usar.com/isti	ingindex inkinet/wam/login.jsp:StringIndex					
RegEdt32 RegEdt32 Schedule+ SystemCertificates H- WAB H- Windows Windows Help				Close		
Mindows NT						
Decrypted Passwords	:19:54 5 !	00000000 57 0 00000010 32 0 00000020 3a 0 00000030 20 0 00000040 62 0 00000050 6e 0 00000050 63 0 00000050 30 0 00000080 30 0	0 65 00 64 00 0 34 00 20 00 0 35 00 32 00 0 20 00 24 00 0 61 00 64 00 0 00 00 57 00 0 20 00 32 00 0 39 00 3a 00 0 33 00 20 00	20 00-44 00 65 00 31 00-38 00 3a 00 20 00-32 00 30 00 24 00-2d 00 2d 00 70 00-65 00 72 00 65 00-64 00 20 00 34 00-20 00 31 00 35 00-32 00 20 00 38 00-32 00 32 00 38 00-32 00 32 00	63 00 20 00 W-e-d- 10-e 31 00 39 00 2-4- 1-8-e 30 00 33 00 :-5-2- 2-(0) 20 00 20 00 73 00 6f 00 b-a-d-p-e-1 44 00 65 00 nW-e-4 38 00 3a 00 c2-4 32 00 30 00 1-9-::5-2- 2d 00 2d 00 0-3-: 00 00	2. C
AccessData Registry Viewer				Offset: 0		

Integration – PRTK

[Wordlist - Notepad	
File gdit Format View Help	
6,4,9,1121 62 64 192 200 120 120 72 0 64 64 64 68 63 636 421 1 7	0
75 80 8822 900	What do you do with this? (or make user-defined)
: :2003122420031225: ??? AM About:Home Accessories\Games Always On Arial Asterisk Bad Password Bad Person Bad@Evil.Com Blank.htm	
C:\Documents and Setting C:\Documents and Setting C:\Documents and Setting C:\Documents and Setting	TALS~1\Temp\ gs\All Users\Start Menu\Programs\Accessories\Entertainm gs\Mitchell\NTUSER.DAT gs\testuser\Application Data
•	

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)

🧏 AccessData Registry Viewer - [Common Areas]					
📴 File Edit Report View Window Help			_ 8 ×		
2					
🖃 🗐 Common Areas	Name	Туре	Data		
CurrentVersion	SubVersionNumber	REG_SZ	(value not set)		
	(LurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)		
ter system	瞪 InstallDate	REG_DWORD	0x417D4CCC (1098730700)		
Windows NT	(a) ProductName	REG_SZ	Microsoft Windows XP		
Winloaon	a) RegDone	REG_SZ	(value not set)		
	RegisteredOrganization	REG_SZ	(value not set)		
	and RegisteredOwner	REG_SZ	ADXP		
Key Properties	SoftwareType	REG_SZ	SYSTEM		
Last Written Time 2004-12-31 21:52:08 LITC	CurrentVersion	REG_SZ	5.1		
OS Install Date (UTC) Mon Oct 25 18:58:20 2004	CurrentBuildNumber	REG_SZ	2600		
OS Install Date (Local) Mon Oct 25 10:50:20 2004	(a)BuildLab	REG_SZ	2600.xpsp_sp2_rtm.040803-2158		
OS INSLAIL DALE (LOCAL) MOIT OCC 25 20:58:20 2004	(a)CurrentType	REG_SZ	Multiprocessor Free		
Last Written Time	(a) CSDVersion	REG_SZ	Service Pack 2		
This indicates the last time this key was written. This is	(a) SystemRoot	REG_SZ	D:\WINDOWS		
available only in Windows NT-based registry files (NT, XP,	(a) SourcePath	REG_SZ	F:\ENGLISH\WINXP\PRO_SP1A\I386		
2000, etc)	ab)PathName	REG_SZ	D:\WINDOWS		
	ProductId	REG_SZ	55274-337-8535232-22871		
	DigitalProductId	REG_BINARY	A4 00 00 00 03 00 00 03 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		
	0 CC 4C 7D 41		ÌL}A ♀		
Microsoft\Windows NT\CurrentVersion	C Offse	t: 0	at the second		