



More about the registry

Network connections
(IP and Wi-Fi)

Automated registry dumping

Notable Tracking Differences

MRU Information:

- Tracking:
 - Open / Run / Save lists
 - Printers / Find Files / Find Computers
 - Individual file types (greater numbers)

Mounted Devices:

- Indication of recently mounted and assigned devices and drive letters – may be a clue

Notable Tracking Differences

Check the SYSTEM file

→ Mounted Devices – disk signature

AccessData Registry Viewer (tm) - [system]

File Edit Report View Window Help

system

- ControlSet001
- ControlSet003
- LastKnownGoodRecovery
- MountedDevices**
- Select
- Setup
- WPA

Name	Type	Data
\\?\Volume{02b82e...}	REG_BINARY	B2 86 74 2D 00 7E 00 00 00 00 00 00
\\?\Volume{02b82e...}	REG_BINARY	B2 86 74 2D 00 9C 02 DE 01 00 00 00
\\?\Volume{02b82e...}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00
\\DosDevices\C:	REG_BINARY	B2 86 74 2D 00 7E 00 00 00 00 00 00
\\DosDevices\D:	REG_BINARY	B2 86 74 2D 00 EC 2C E2 04 00 00 00
\\DosDevices\E:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00
\\?\Volume{02b82e...}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00
\\DosDevices\F:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00
\\?\Volume{c5ea225...}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 54 00

system\MountedDevices

Notable Tracking Differences

Evidence Tree

- Evidence: \\.\PHYSICALDRIVE0
 - Partition 1 [20002MB]
 - Partition 2 [18135MB]
 - Unpartitioned Space [basic disk]

File List

Name	Size	Type	Date
unallocated space	8,516 KB	Unallocated space	
MBR	1 KB	File system met...	

Properties

General

Name	MBR
File Class	File system meta data
File Size	512

Hex Value Interpreter

Sel start = 440, len = 4; phy sec = 0

At: 0x1B8 (4 bytes) == disk signature

```
000000b0 43 f7 e3 8b d1 86 d6 b1-06 d2 ee 42 f7 e2 39 56 C.....B..9V
000000c0 0a 77 23 72 05 39 46 08-73 1c b8 01 02 b5 00 7c .w#r.9F.s.....l
000000d0 8b 4e 02 8b 56 00 cd 13-73 51 4f 74 4e 72 e4 8a .N..V...sQ0tN2..
000000e0 56 00 cd 13 eb e4 8a 56-00 60 bb aa 55 b4 41 cd V.....V...U.A.
000000f0 13 72 36 81 fb 55 aa 75-30 f6 c1 01 74 2b 61 60 .r6..U-u0...t+a`
00000100 6a 00 6a 00 ff 76 0a ff-76 08 6a 00 68 00 7c 6a j.j..v..v.j.h.lj
00000110 01 6a 10 b4 42 8b f4 cd-13 61 61 73 0e 4f 74 0b .j..B....aas.0t.
00000120 32 e4 8a 56 00 cd 13 eb-d6 61 f9 c3 49 6e 76 61 2..V.....a..Inva
00000130 6c 69 64 20 70 61 72 74-69 74 69 6f 6e 20 74 61 lid partition ta
00000140 62 6c 65 00 45 72 72 6f-72 20 6c 6f 61 64 69 6e ble>Error loadin
00000150 67 20 6f 70 65 72 61 74-69 6e 67 20 73 79 73 74 g operating syst
00000160 65 6d 00 4d 69 73 73 69-6e 67 20 6f 70 65 72 61 em.Missing opera
00000170 74 69 6e 67 20 73 79 73-74 65 61 00 00 00 00 00 ting system.....
00000180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
00000190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
000001a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
000001b0 00 00 00 00 00 2c 44 63-b2 86 74 2d 00 80 01 .....Dc....
000001c0 01 00 07 fe ff ff 3f 00-00 00 00 00 00 00 00 .....?...7.q...
000001d0 c1 ff 0c fe ff ff 76 16-71 02 08 bf 36 02 00 00 .....v.q...6...
000001e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
000001f0 00 00 00 00 00 00 00 00-00 00 00 00 00 55 aa .....U.
```

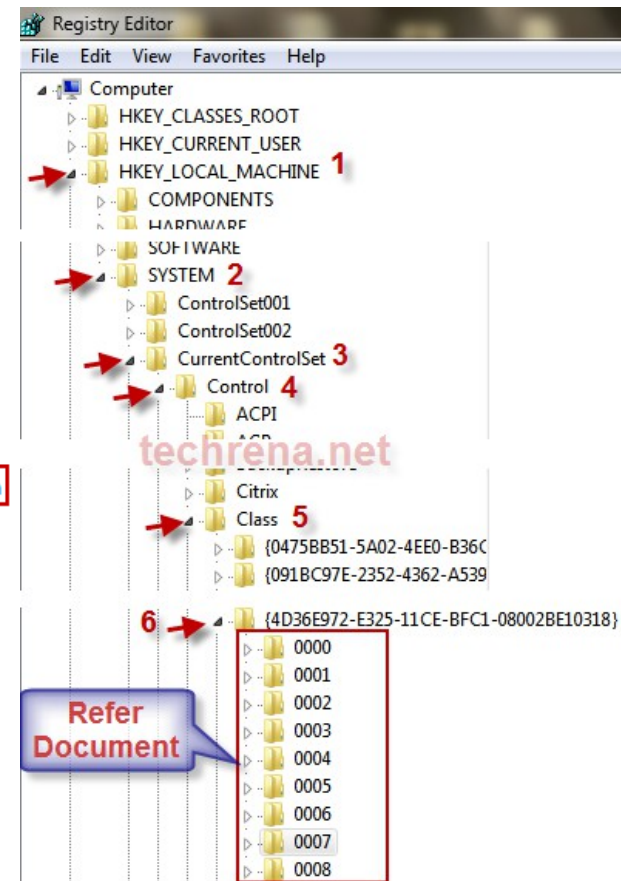
IP-adresser och NIC

- HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
 - Dvs. hive: system\ControlSet<#>\...
 - Delnycklar utgör gränssnitt mot olika NIC. Namngivna med GUID:s (Globaly Unique IDentifiers)
 - Statiska eller dynamiska adresser?
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards
 - GUID (ServiceName) och description
 - Om ett NIC tas ur datorn så är entryt kvar i registret
 - RV key property -> Last Written Time == NIC install time

Change NIC MAC address

- A Media Access Control (MAC) address is a physical address hard coded onto a network card
- HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}
- The registry key labeled "NetworkAddress" holds the MAC address setting for the adapter
- This key is however not present so you must add it yourself when you found the correct "DriverDesc" in the subkeys 001, 002, ...!

DriverDateData	REG_BINARY	00 40 b9 f1 9a 37 c8 01
DriverDesc	REG_SZ	Intel(R) PRO/100 VE Network Connection
DriverVersion	REG_SZ	8.0.47.0
EnableDynamicReducedPower	REG_SZ	1
EnablePME	REG_SZ	2
EnablePowerDownOnLinkLoss	REG_SZ	1
FlowControl	REG_SZ	3
Force10MbOnD3	REG_SZ	1
NetCfgInstanceId	REG_SZ	{902BBAEE-E2C1
NetLuidIndex	REG_DWORD	0x00000006 (6)
NetworkAddress	REG_SZ	00167670D4F6
NewDeviceInstall	REG_DWORD	0x00000000 (0)
NicCoPlugins	REG_MULTI_SZ	NicInst6.dll,NicC



WiFi Concepts

- SSID – Service Set Identifier (i.e. Network name)
- BSSID – Basic Service Set Identifier (i.e. MAC address)
- Encryption
 - WEP (Wired Equivalent Privacy)
 - TKIP (Temporal Key Integrity Protocol)
 - AES (Advanced Encryption Standard)
- Authentication
 - WPA (WiFi Protected Access – AES)
 - WPA-PSK (Pre-Shared Key)
- EAPOL = Extensible Authentication Protocol over LAN

WiFi connections – Windows XP

- All Wireless Adapters are given a unique GUID under HKLM\software\Microsoft\EAPOL\Parameters\Interfaces
- WiFi adapter description and the IP parameters etc. are on the same place in the registry as for NIC:s (follow the Interfaces > GUID)
- Entries (numbers) with SSIDs can only be removed via a direct registry edit

The screenshot shows the AccessData Registry Viewer window. The left pane displays the registry tree with the path `software\Microsoft\EAPOL\Parameters\Interfaces\{0E271E68-9033-4A25-9883-A020B191B3C1}` selected. The right pane shows a list of 14 registry values, all of type `REG_BINARY`. The data for these values is represented as hexadecimal strings. A red box highlights the 'Key Properties' section at the bottom left, which shows 'Last Written Time: 2008-04-14 12:21:57 UTC'. Another red box highlights the 'AccessData 0' entry in the SSID list at the bottom right. The status bar at the bottom shows the path `software\Microsoft\EAPOL\Parameters\Interfaces\{0E271E68-9033-4A25-9883-A020B191B3C}` and 'Offset: 0'.

Name	Type	Data
1	REG_BINARY	05 00 00 00 00 00 00 00 00 00 00 40 0D 00 00 00 07 00 ...
2	REG_BINARY	05 00 00 00 00 00 00 00 00 00 00 C0 0D 00 00 00 0D 0...
3	REG_BINARY	05 00 00 00 00 00 00 00 00 00 40 0D 00 00 00 0A 00...
4	REG_BINARY	05 00 00 00 00 00 00 00 00 00 40 0D 00 00 00 0C 00...
5	REG_BINARY	05 00 00 00 00 00 00 00 00 00 C0 0D 00 00 00 0F 00...
6	REG_BINARY	05 00 00 00 00 00 00 00 00 40 0D 00 00 00 0C 00...
7	REG_BINARY	05 00 00 00 00 00 00 00 00 40 0D 00 00 00 0A 00...
8	REG_BINARY	05 00 00 00 00 00 00 00 00 40 0D 00 00 00 0D 00...
9	REG_BINARY	05 00 00 00 00 00 00 00 00 C0 0D 00 00 00 0A 0...
10	REG_BINARY	05 00 00 00 00 00 00 00 00 40 0D 00 00 00 05 00 ...
11	REG_BINARY	05 00 00 00 00 00 00 00 00 40 0D 00 00 00 0A 00...
12	REG_BINARY	05 00 00 00 00 00 00 00 00 40 0D 00 00 00 0E 00 ...
13	REG_BINARY	05 00 00 00 00 00 00 00 00 C0 0D 00 00 00 05 00...
14	REG_BINARY	05 00 00 00 00 00 00 00 00 C0 0D 00 00 00 05 00...

Key Properties
Last Written Time: 2008-04-14 12:21:57 UTC

SSID list

WZCSVC (Wireless Zero Configuration Service)

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\
- Value: Static#0000, Static#0001, Static#0002, ...
 - The list is not a chronological description of connections
- The Data for these Values contains
 - The BSSID of the AP (Access Point) that the adapter has connected to at offset: 0x08
- The SSID of the wireless network that the adapter has connected to at offset: 0x14
- The type of encryption used at offset: 0x34
- The authentication method / protocol at offset: 0x94

WZCSVC interface values 1

- Was the AP (Access Point) secured?
- WEP, WPA, WPA2, etc.

The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of the registry path: `software\Microsoft\WZCSVC\Parameters\Interfaces\{24E2DF49-403A-47BA-9653-A6FEA1317B46}`. The right pane shows a list of registry values:

Name	Type	Data
LayoutVersion	REG_DWORD	0x00000007 (7)
ControlFlags	REG_DWORD	0x0BD18002 (198279170)
ActiveSettings	REG_BINARY	C8 02 00 00 00 40 00 00 00 13 46 C1 1F 72 00 00 0C 00 ...
Static#0000	REG_BINARY	C8 02 00 00 00 40 00 00 00 13 46 C1 1F 72 00 00 0C 00 ...
Static#0001	REG_BINARY	C8 02 00 00 00 40 00 00 00 19 CB 9E 72 FE 00 00 0A 00 ...

The 'Static#0000' value is circled in red. Below the registry list, a hex dump of the binary data for 'Static#0000' is shown with annotations:

Offset	Hex	Annotation	ASCII
000	c8 02 00 00 00 40 00 00 00 13 46 c1 1f 72 00 00	BSSID	E.....@.....FÁ.r...
010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SSIDJones Family
020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Encryptionóyyy
040	20 00 00 00 00 64 00 00 00 00 00 00 00 88 2f 25 00		...d...../;%.
050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
060	01 00 00 00 00 82 84 8b 96 00 00 00 00 00 00 00	
070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Authentication
0a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

The 'Last Written Time' property is highlighted in green, showing the value: 16/09/2009 19:33:43 UTC.

The path `software\Microsoft\WZCSVC\Parameters\Interfaces\{24E2DF49-403A-47BA-9653-A6FEA1317B46}` is highlighted in red at the bottom of the window.

WZCSVC interface values 2

- **Note!**
- **This is an incomplete list of values!**

Hex Offset	Information
0x08	BSSID
0x10	Length of SSID
0x14	Start of SSID string
0x34	Data Encryption type used (TKIP, AES, WEP, Disabled)
0x94	Network Authentication used (WPA-PSK, WPA, Shared, Open)

Encryption Type 0x34

WEP	00
Disabled	01
TKIP	04
AES	06

Network-Authentication 0x94

WPA-PSK	04
WPA	03
Shared	01
Open	00

Network connections - Windows Vista/7

- The **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList** subkey tracks general network information including wireless accounts
- Under the NetworkList key the **Profiles** and **Signatures** subkeys are the most interesting
- **Profiles** contains network information stored by GUID and may include SSID
 - **ProfileName**: SSID or server/network connected to
 - **Description**: Will usually match the ProfileName
 - **Managed**: 0 == a WiFi-router or simple network, 1 == a connection to a server/domain network
 - **DateCreated**: Subkey creation date
 - **NameType**: 0x47 == Wireless, 00x06 == Wired, 0x17 == WWAN (3G/4G)
 - **DateLastConnected**: The date the computer was last connected

Network connections - Windows Vista/7

The screenshot displays the AccessData Registry Viewer interface. The left pane shows a tree view of the registry path: `NetworkList > Profiles > {6669643B-487E-47E2-A75B-F2C5D832953C}`. The right pane shows a list of registry values for this profile:

Name	Type	Data
ab ProfileName	REG_SZ	linksys
ab Description	REG_SZ	linksys
Managed	REG_DWORD	0x00000000 (0)
Category	REG_DWORD	0x00000001 (1)
DateCreated	REG_BINARY	D8 07 02 00 05 00 0F 00 06 00 2B 00 11 00 52 01
NameType	REG_DWORD	0x00000047 (71)
DateLastConnected	REG_BINARY	D8 07 04 00 00 00 1B 00 09 00 12 00 16 00 DF 01
CategoryType	REG_DWORD	0x00000000 (0)
IconType	REG_DWORD	0x00000000 (0)

Below the registry list, a hex editor shows the binary data for the selected value: `0 | 6C 00 69 00 6E 00 6B 00-73 00 79 00 73 00 00 00 | l-i-n-k-s-y-s...`

The bottom status bar shows the full registry path: `SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{6669643B-487E-4` and the offset: `Offset: 0`.

Key Properties
Last Written Time: 2008-04-27 15:18:22 UTC

Network connections - Windows Vista/7

- **Signatures** stores Managed (domain) and Unmanaged (simple net) subkeys
 - **ProfileGuid**: Stores a GUID that points to the Profiles key
 - **DefaultGatewayMac**: MAC address to the gateway (may be 0-padded to 8 byte if length is the standard 6 byte)
- DateTime values in **Profiles** subkeys are bitstreams in 2 byte sections which can be translated as
 - d907 0a00 0500 0e00 0d00 0400 3500 af03
 - 2009 10 friday 14th - 13 : 04 : 35 ms
 - **Note! Read as little endian**

Brandväggen

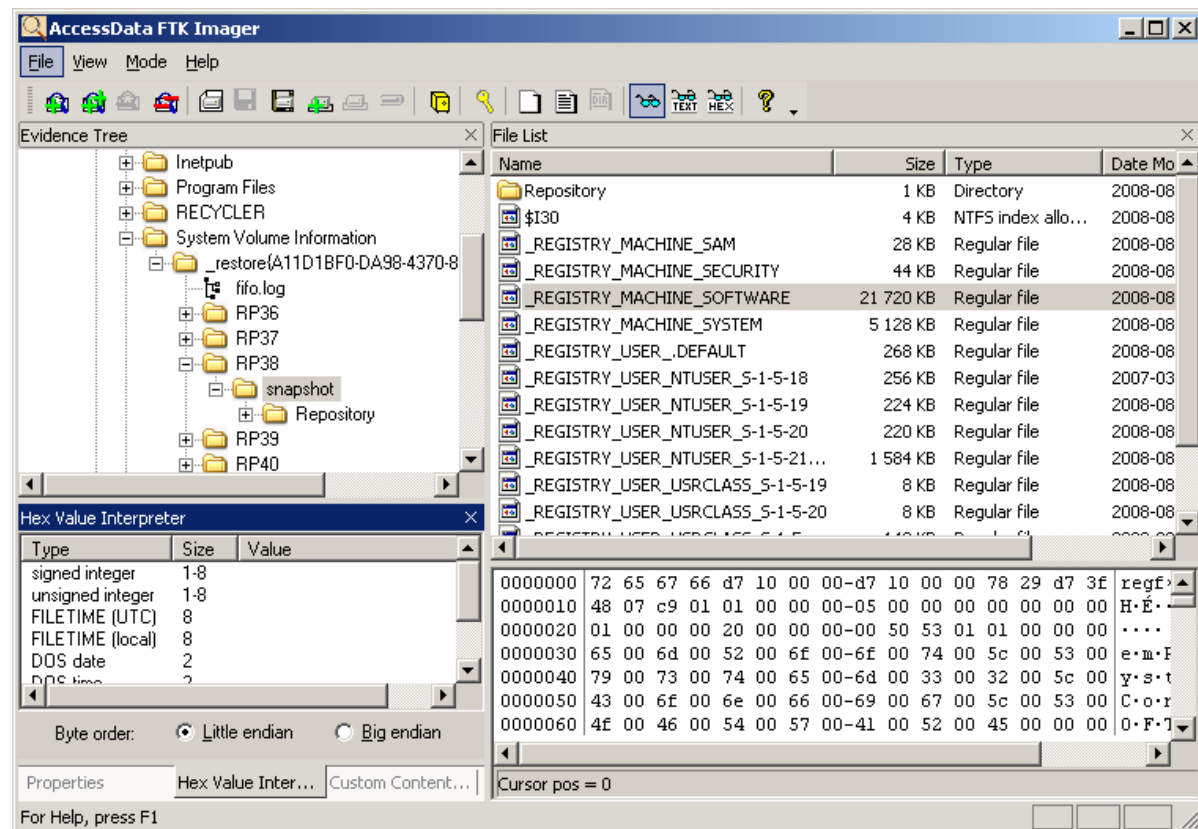
- HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy***Profile
 - Dvs. hive: system\ControlSet<#>\...
- Kontrollera värdet för EnableFirewall
 - 0 avstängd
 - 1 påslagen
- Studera delnycklarnas värden!

View the Registry as a log file

- The Registry maintains a good deal of time-based information
- Registry keys have LastWrite value
 - 64-bit FILETIME object
 - Useful when you know what actions cause the key to be updated
 - MRU Lists
- Several Registry keys maintain timestamps within their value's data
 - UserAssist keys - tracks the use of applications and shortcuts etc. by both frequency (total uses) as well as when they were last used
 - <http://accessdata.com/downloads/media/UserAssist%20Registry%20Key%209-8-08.pdf>
- All of these sources provide information useful in timeline analysis, and can be easily correlated with other sources

Registrets hive-filer sparas regelbundet!

- En Restore Point tas normalt varje dygn, sparas upp till 90 dagar!
- Normalt dock endast delar av registret som sparas i \System Volume Information\
 - Vanliga användare har ej läsrätt till katalogen
 - Exportera den med hjälp av FTK Imager!





- GUI-based (rr.exe), plugin-based approach to parsing/correlating data from within hive files extracted from an image
- Very fast, users have reported reducing data collection from DAYS to MINUTES!
- Accompanying CLI tool, rip.exe, allows for quick data extraction via a single plugin or plugin file
 - Can be included in a batch file
- Ripxp.exe is a CLI tool, similar to rip.exe and uses RegRipper plugins
 - Extract hives and Restore Points from image (FTK Imager, etc.)
 - Runs the plugin against the designated hive file, as well as the corresponding hive files in each RP

UserAssist Keys

- May have three GUIDs
 - ActiveDesktop, MS Internet Toolbar and IE7
- Value names are ROT-13 "encrypted"
- 16 byte data under ActiveDesktop GUID may contain
 - bytes 4-7; DWORD RunCount value
 - bytes 8-15; FILETIME LastRun value
- Shows that the user performed actions via the desktop
 - Logged in at console or via remote access

```
C:\hjo\cases\RegRipper032911>rip -r bilbo-NTUSER.DAT -p userassist
```

```
Launching UserAssist (Active Desktop) v.20080726
```

```
UserAssist (Active Desktop)
```

```
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
```

```
LastWrite Time Mon Jan 3 20:24:24 2005 (UTC)
```

```
Mon Jan 3 20:24:24 2005 (UTC)
```

```
UEME_UISCUT (1) UEME_RUNPATH (2) UEME_RUNPATH:AOL Instant Messenger.lnk (1)
```

```
UEME_RUNPATH:D:\Program Files\AIM\aim.exe (1)
```

```
Mon Jan 3 20:22:01 2005 (UTC)
```

```
...
```

UserAssist RV

The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of the registry, with the path `UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count` selected. The right pane shows a list of registry values, with the value `HRZR_EHACNGU:Q:\Cebtenz Svyrf\NVZ\mvz.rkr` selected. The bottom-left pane shows the properties for this value, including the value name `RC UEME_RUNPATH:D:\Program Files\AIM\aim.exe`, which is highlighted with a red box. The bottom-right pane shows the hex data for the selected value.

Name	Type	Data
HRZR_PGYFRFFVBA	REG_BINARY	91 8E 27 0E 01 00 00 00
HRZR_EHACVQY:%pfvqy2%\Jvaqbjf Zrqvn Cynlre.yax	REG_BINARY	01 00 00 00 13 00 00 00 F6 E8 1E E2 D1 F1 C4 01
HRZR_EHACVQY:%pfvqy2%\Jvaqbjf Zrffratre.yax	REG_BINARY	01 00 00 00 12 00 00 00 F6 E8 1E E2 D1 F1 C4 01
HRZR_EHACVQY:%pfvqy2%\Npprffbevrf\Gbhe Jvaqbjf KC.yax	REG_BINARY	01 00 00 00 11 00 00 00 F6 E8 1E E2 D1 F1 C4 01
HRZR_EHACVQY:%pfvqy2%\Npprffbevrf\Jvaqbjf Zbivr Znxre.yax	REG_BINARY	01 00 00 00 10 00 00 00 F6 E8 1E E2 D1 F1 C4 01
HRZR_EHACVQY:%pfvqy2%\Npprffbevrf\Fifgrz Gbbyf\Svyrf naq F...	REG_BINARY	01 00 00 00 0F 00 00 00 F6 E8 1E E2 D1 F1 C4 01
HRZR_PGYPHNPbhag:pgbe	REG_BINARY	01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
HRZR_HVFPHG	REG_BINARY	01 00 00 00 06 00 00 00 30 D2 3B 37 D2 F1 C4 01
HRZR_EHACNGU	REG_BINARY	01 00 00 00 07 00 00 00 E0 5A 58 37 D2 F1 C4 01
HRZR_EHACNGU:NBY Vafgnag Zrffratre.yax	REG_BINARY	01 00 00 00 06 00 00 00 30 D2 3B 37 D2 F1 C4 01
HRZR_EHACNGU:Q:\Cebtenz Svyrf\NVZ\mvz.rkr	REG_BINARY	01 00 00 00 06 00 00 00 E0 5A 58 37 D2 F1 C4 01

Key Properties
Last Written T: 2005-01-03 20:24:24 UTC

Value Properties

Value Name	RC UEME_RUNPATH:D:\Program Files\AIM\aim.exe
Time	2005-01-03 20:24:24 UTC
Session ID	1
Times Execute	1

Times Executed
The number of time this has been executed

bilbo-NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count Offset: 0

Issues with 64-bit Windows and Vista/7

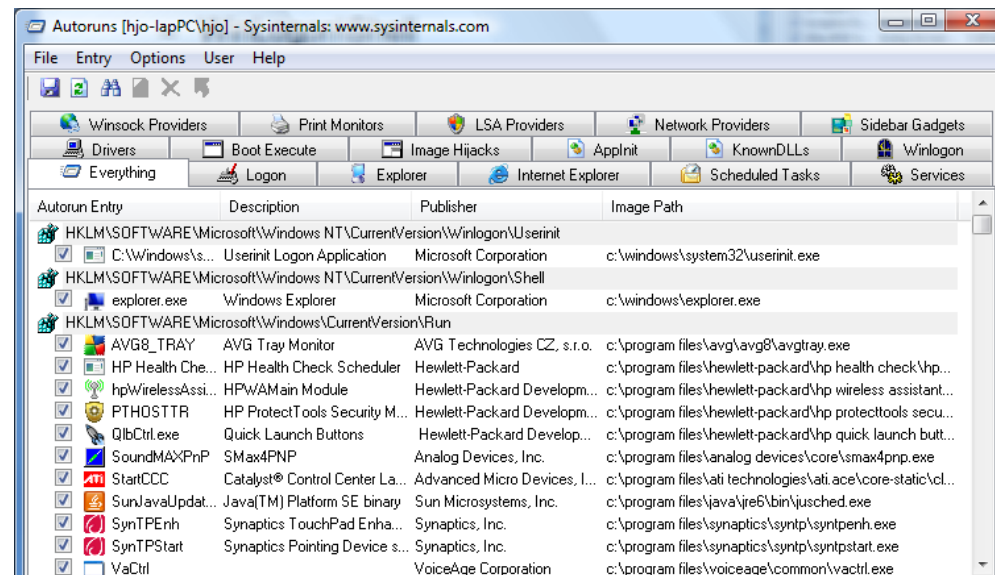
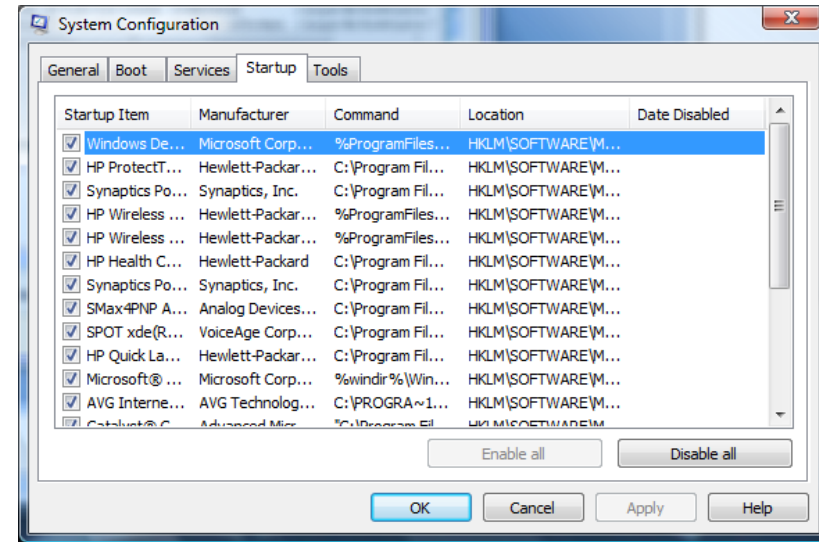
- Some redirection occurs
- Native 64-bit apps write to HKLM\Software
- 32-bit apps write to HKLM\Software\WOW6432Node
- Registry changes in x64-based versions of Windows Server 2003 and in Windows XP Professional x64 Edition
 - KB 896459 lists the keys that are shared (not redirected)
 - <http://support.microsoft.com/kb/896459>
- Vista/7 User Virtualization
 - Access to the Registry is restricted for compatibility reasons
 - Vista creates a per-user copy and subsequently redirects read/write operations
 - HKEY_CURRENT_USER\Software\Classes\VirtualStore

Platser för start av program och tjänster

- Windows har många platser där program automatiskt startas i samband med att systemet startas, användare loggar in osv.
- Enbart registret innehåller ett dussintal sådana platser
- Windows konfigurationsfiler kan också användas för att starta program
- Om du känner till programmets namn så kan du söka i registret och konfigurationsfiler
- Om inte, så använd program liknande Autoruns från Sysinternals

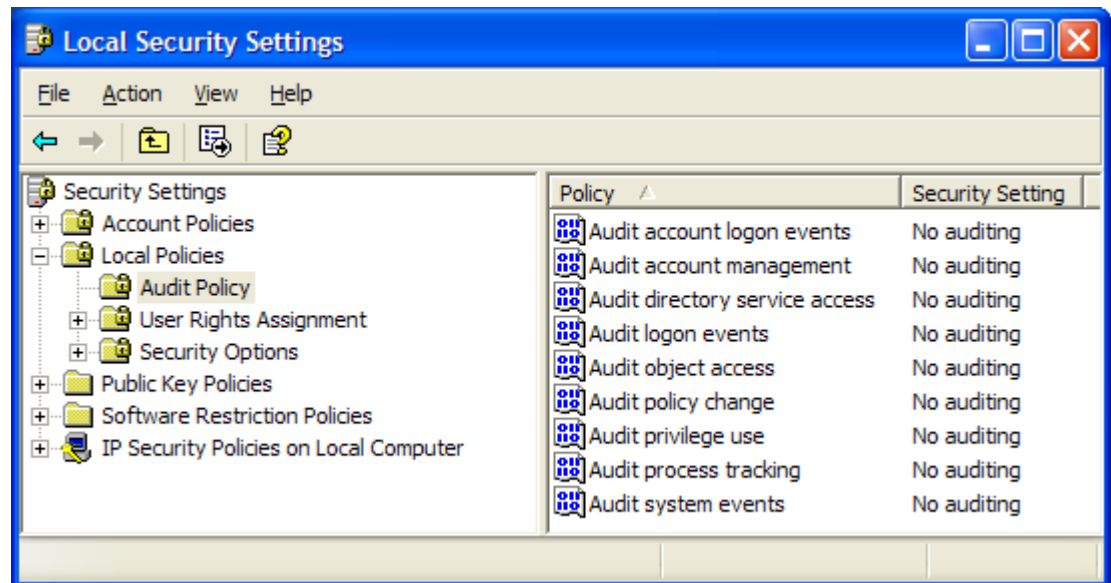
Registry nycklar och filer att kolla

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
 - Run, RunOnce, Uninstall
 - HKLM\ ... \WinLogon\Shell
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- 16 bit applikation support (liten användning, malware?)
 - System.ini
 - [Boot] sektionen – Shell
 - Win.ini
 - [Windows] sektionen – Run
- System konfigurationsverktyget
 - msconfig.exe
- Sysinternals - Autoruns



Registry auditing

- Under en undersökning kan det komma fram att en policyöverträdelse berodde på kod som körts från registry
- Att ha registry auditing påslaget kan hjälpa att se **vem som gjorde vad och när**
 - Producerar en så kallad "Audit Log" – säkerhets logg
- Samarbete med IT-support om att enabla registry auditing via grupp policy är att rekommendera!



Utforska registret!

- Ta inget för givet
- Prova först på en dator som är utrustad med likadant operativsystem som den maskin som du undersöker
- Notera förändringar med hjälp av verktyg liknande [Microsofts ProcessMonitor](#)
 - Med detta verktyg så kan du studera vad som förändras i registret vid till exempel vid installation av ett program
- Regshot, tar snapshots av registret
 - <http://sourceforge.net/projects/regshot/>
- Använd AccessDatas *Registry Quick Find Chart!*
 - <http://www.accessdata.com/supplemental.html>