More about the registry

Network connections
(IP and Wi-Fi)

Automated registry dumping

Notable Tracking Differences

MRU Information:

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

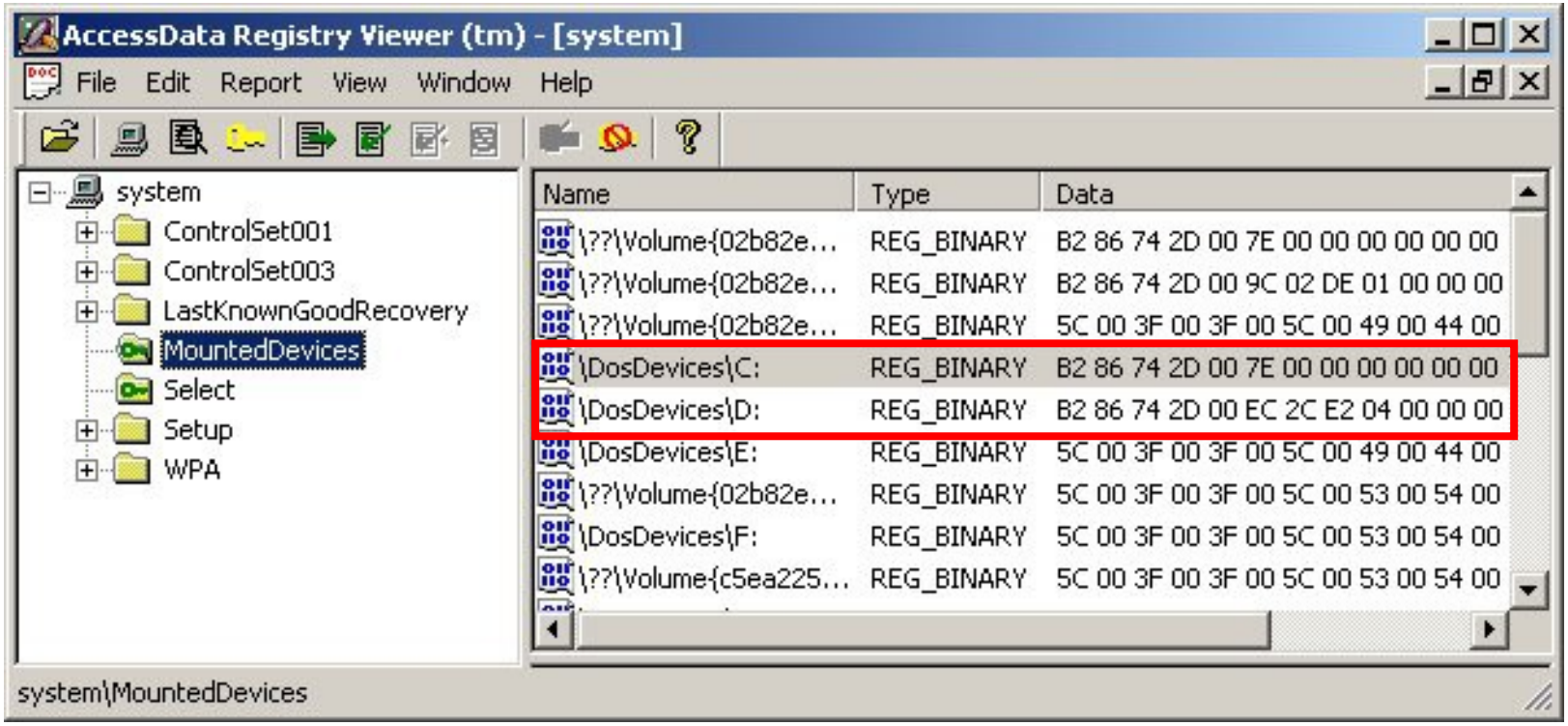
Mounted Devices:

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

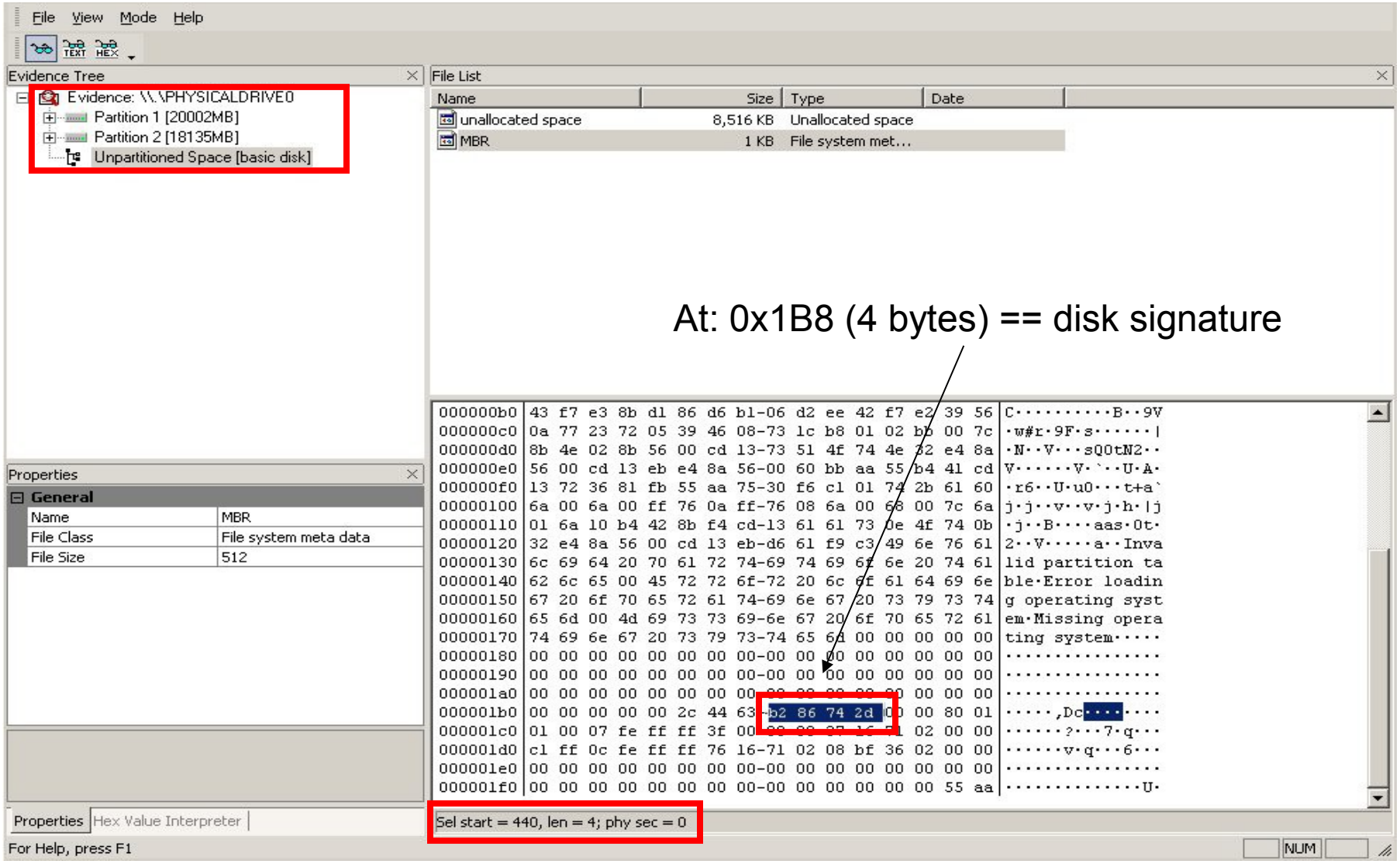
Notable Tracking Differences

Check the SYSTEM file

→ Mounted Devices – disk signature



Notable Tracking Differences

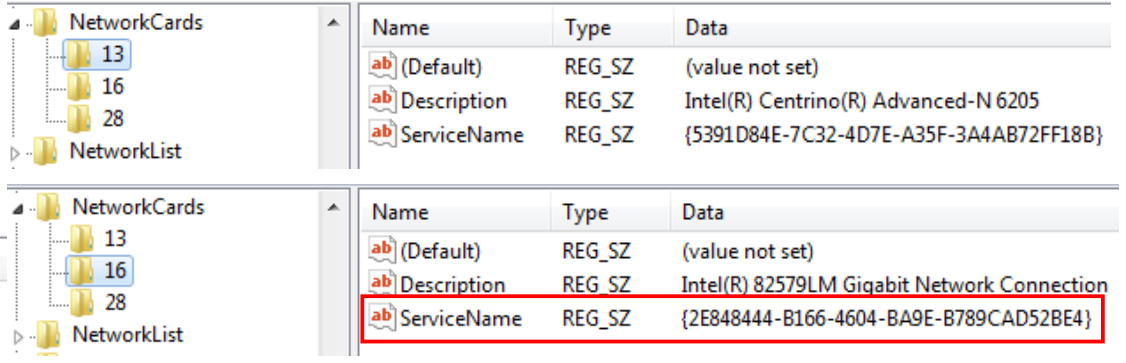


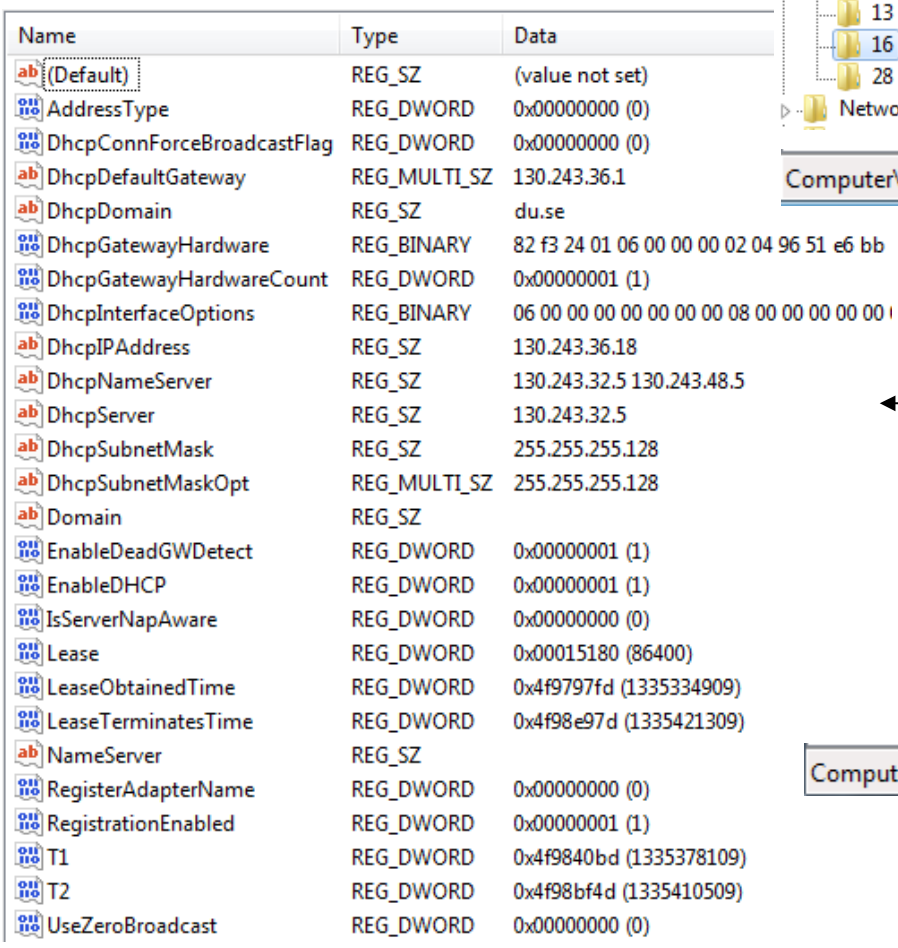
IP-adresser och NIC

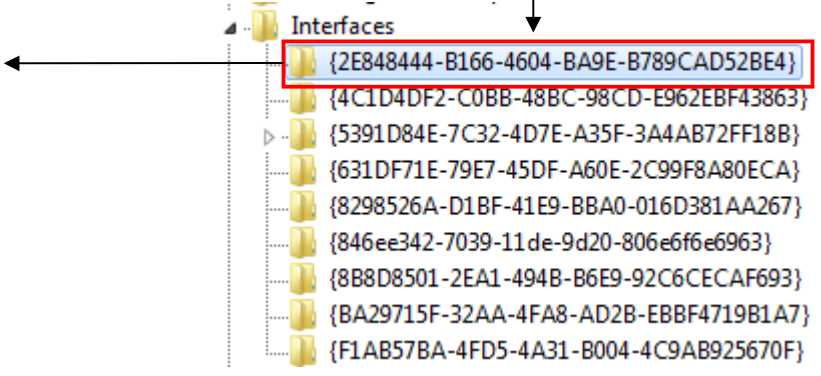
- HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
  - Dvs. hive: system\ControlSet<#>\...
  - Delnycklar utgör gränssnitt mot olika NIC. Namngivna med GUID:s (Globaly Unique IDentifiers)
  - Statiska eller dynamiska adresser?
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards
  - 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

IP-address and NIC example

- GUID to network parameters

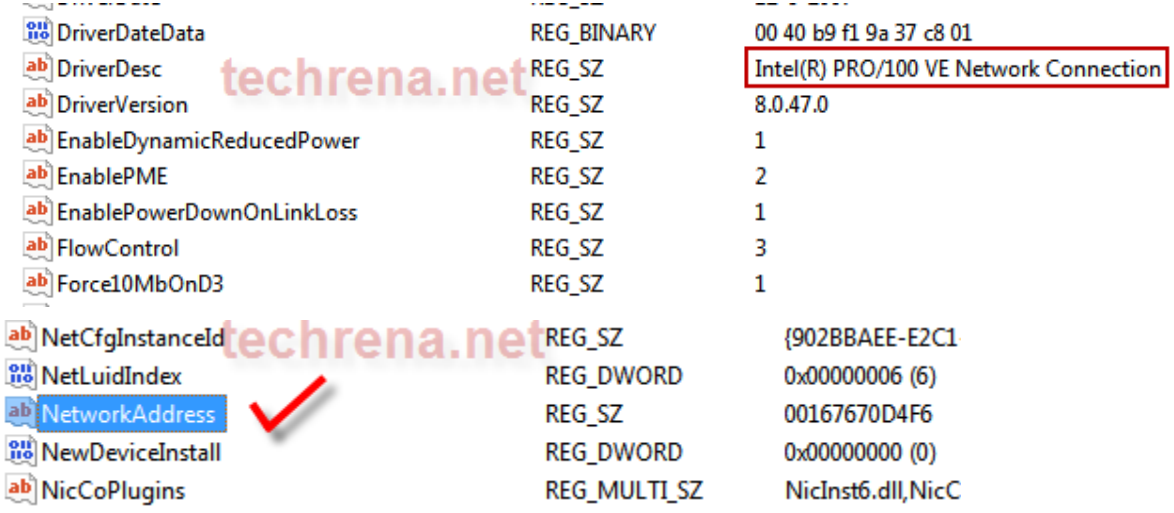


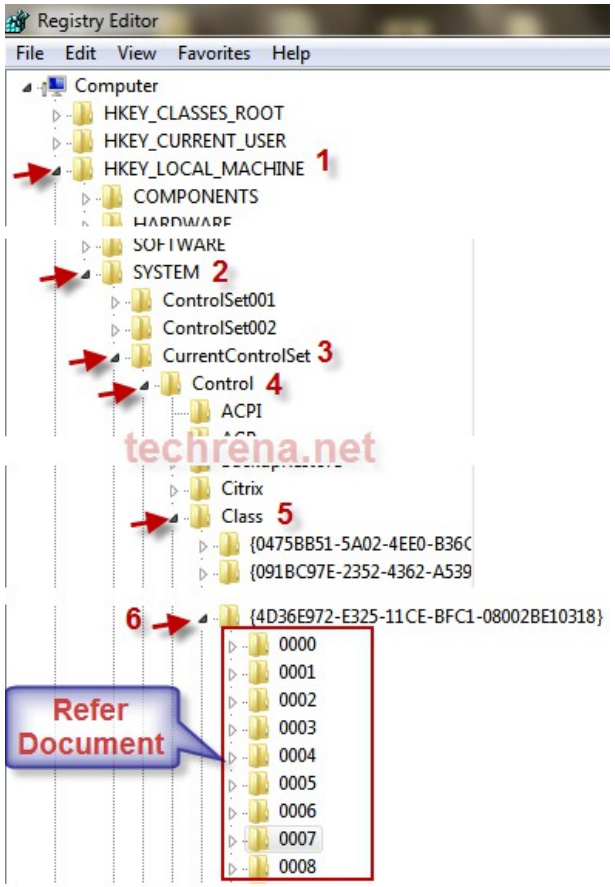




Change NIC MAC address

- 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, ...!



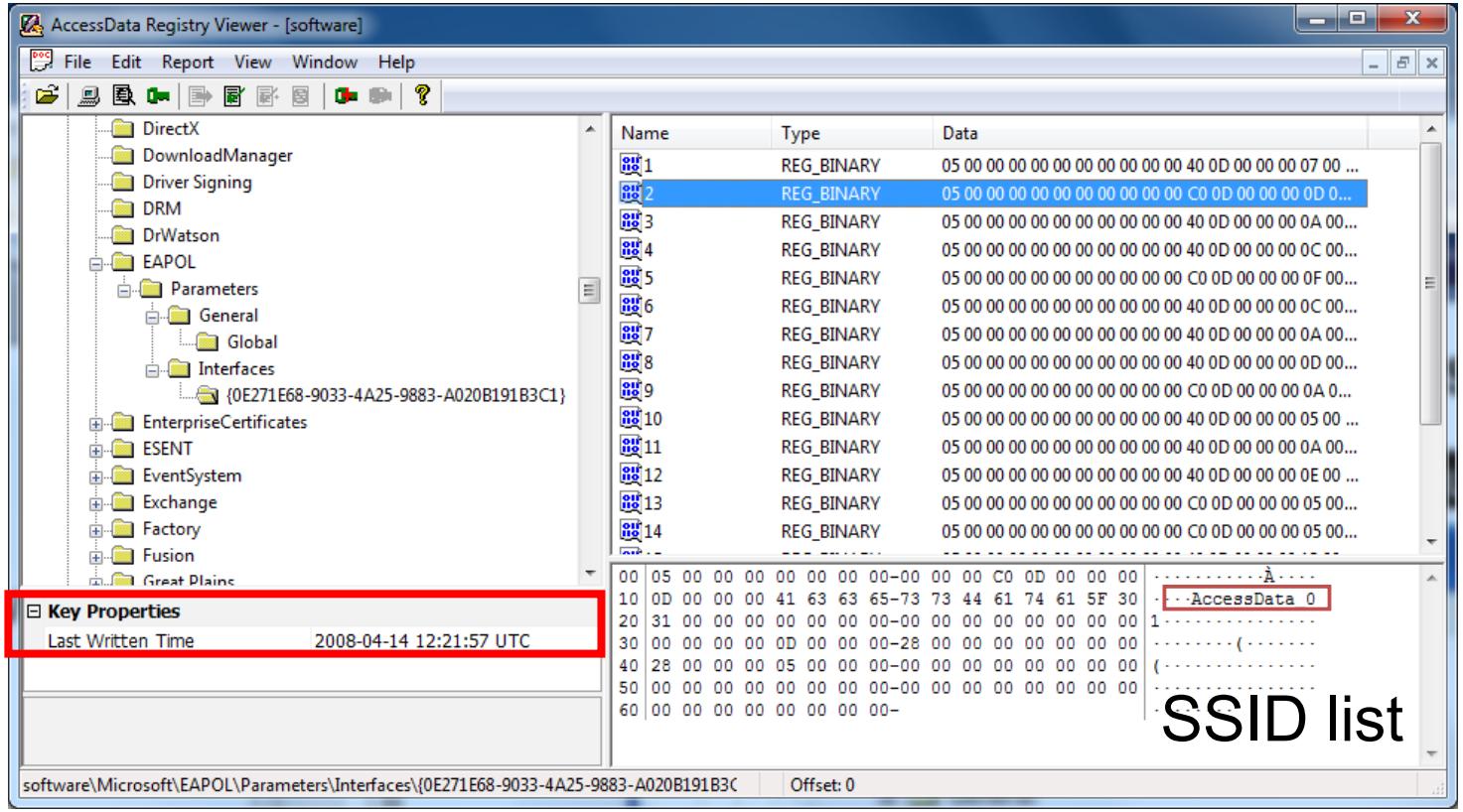


WiFi Concepts

- 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 an 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

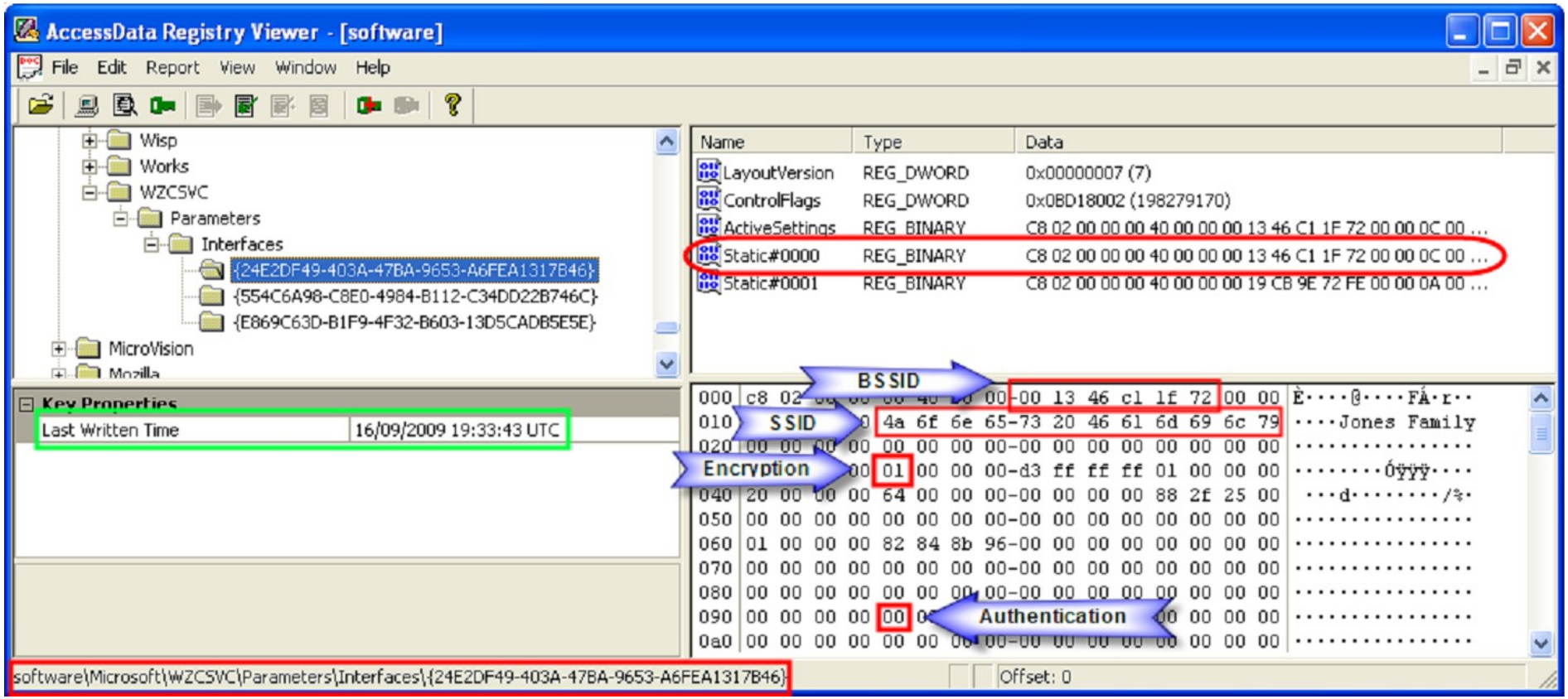


WZCSVC (Wireless Zero Configuration Service)

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\<GUID>
- Value: Static#0000, Static#0001, Static#0002, …
  - The list is not a cronological 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.



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)

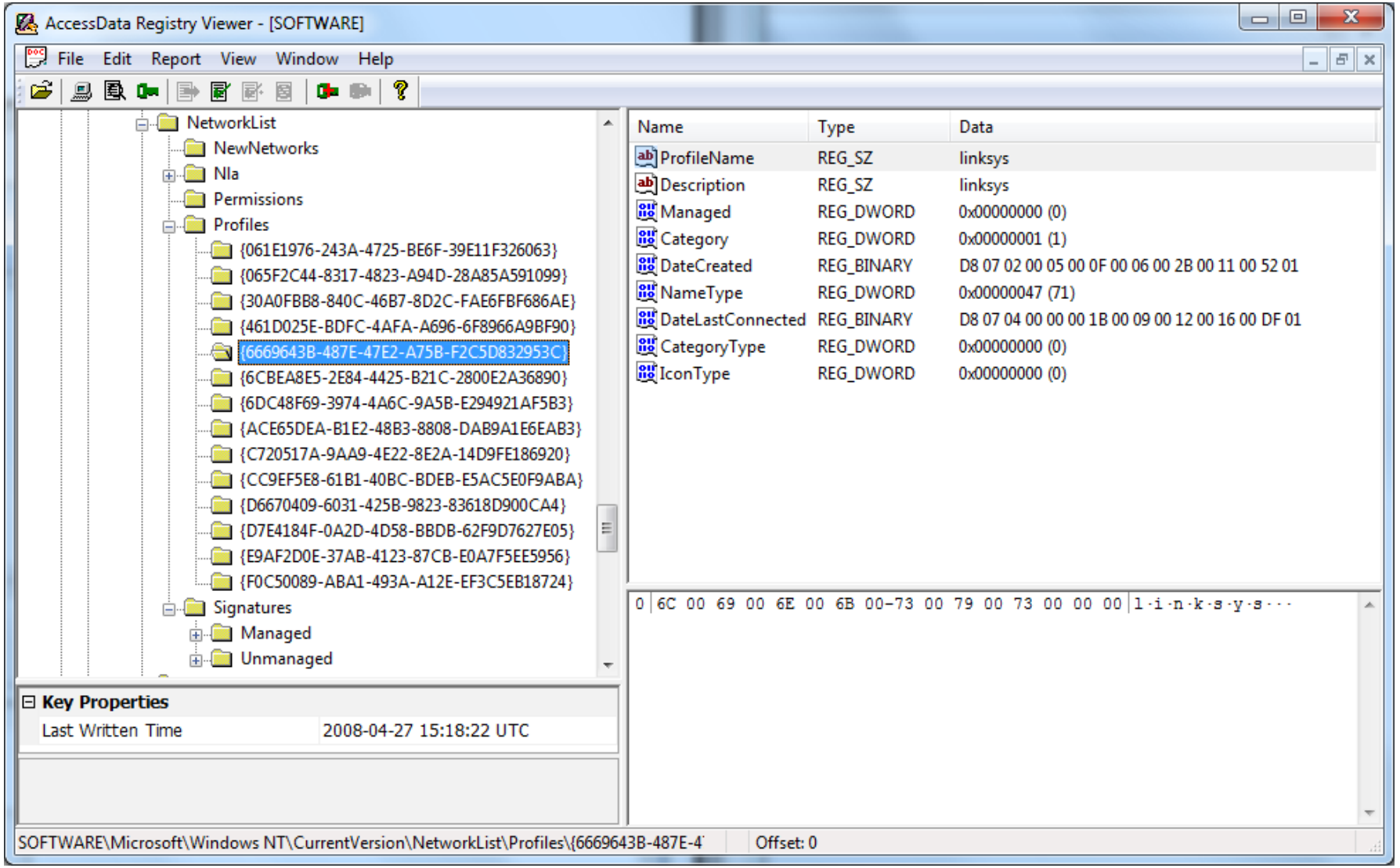
Encryption Type	0x34
WEP	00
Disabled	01
TKIP	04
AES	06

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



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

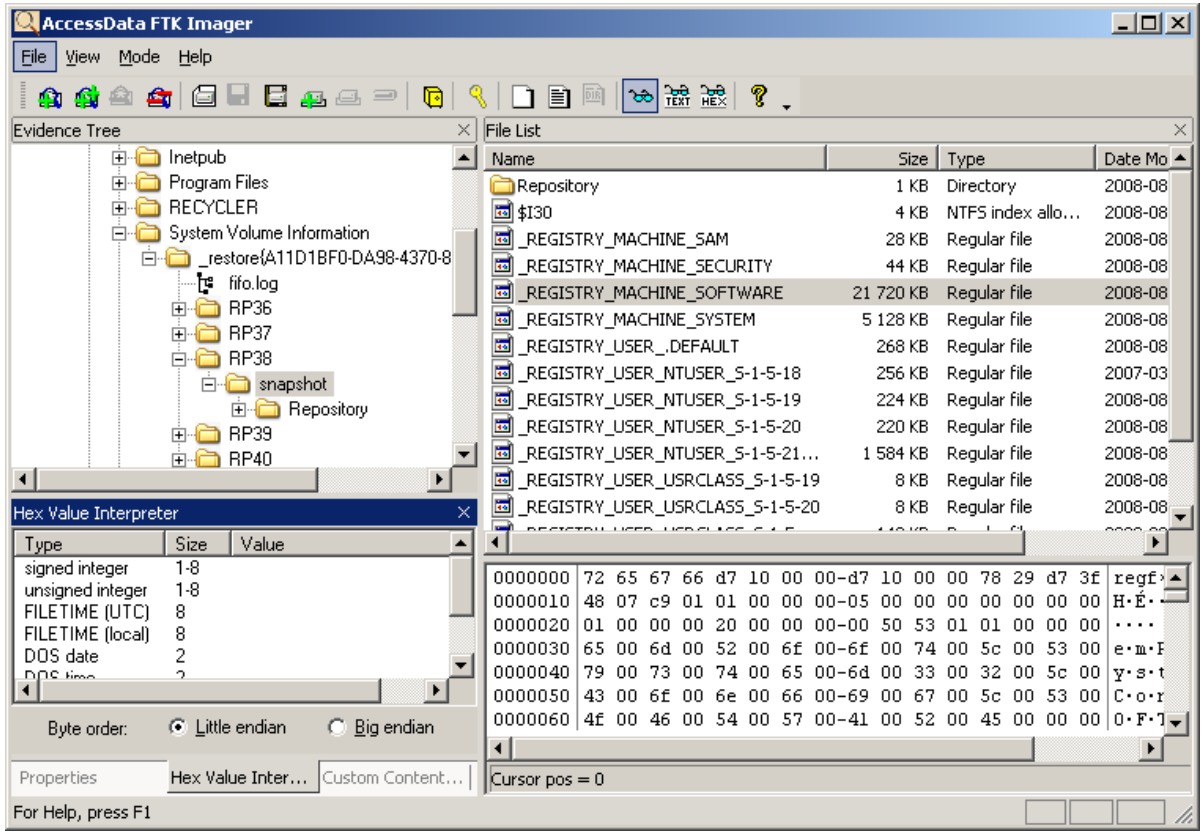
- Studera delnycklarnas värden!

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 spars regelbundet!

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



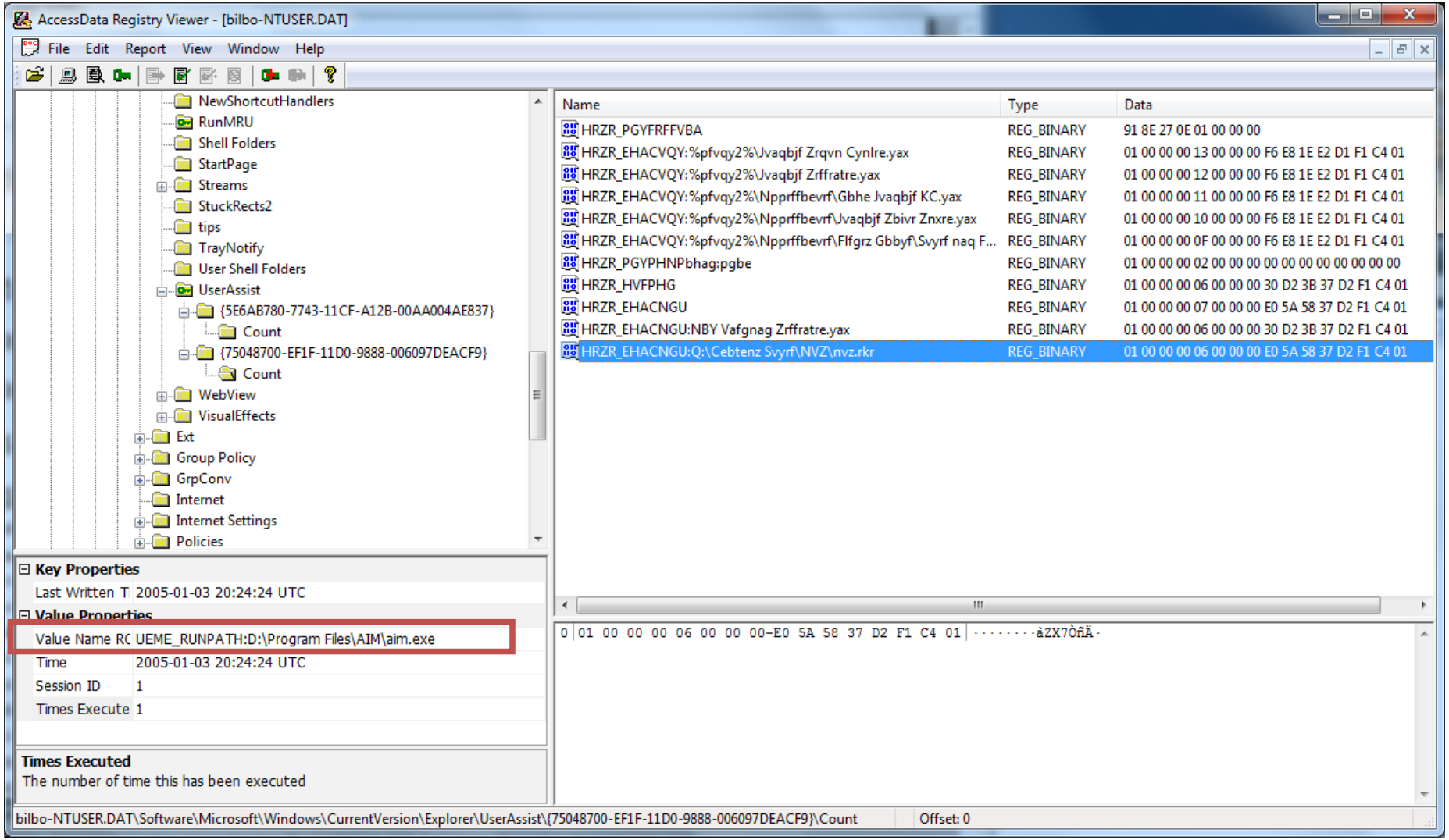
- GUI-based (rr.exe), plugin-based approach to parsing/correlating data from within hive files extracted from an image
- Very fast, users have reported reducing data collection from DAYS to MINUTES!
- Accompanying CLI tool, rip.exe, allows for quick data extraction via a single plugin or plugin file
  - 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



Issues with 64-bit Windows and Vista/7

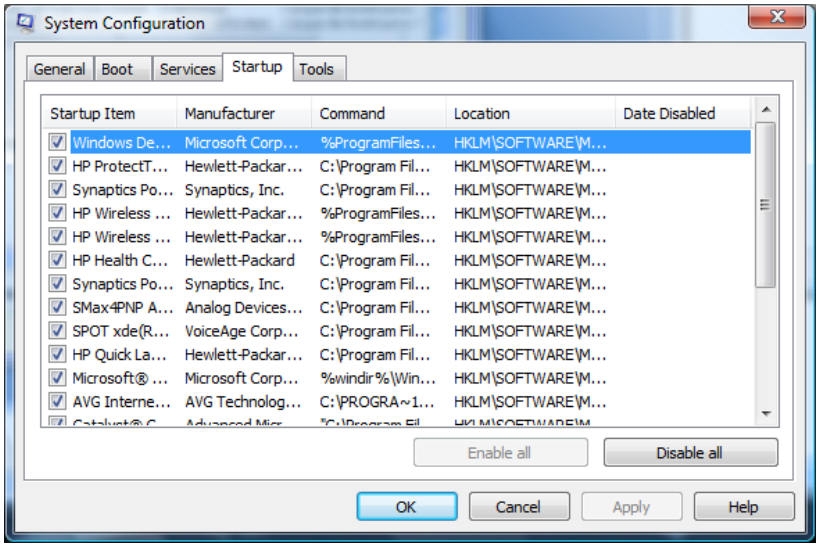
- Some redirection occurs
- Native 64-bit apps write to HKLM\Software
- 32-bit apps write to HKLM\Software\WOW6432Node
- Registry changes in x64-based versions of Windows Server 2003 and in Windows XP Professional x64 Edition
  - KB 896459 lists the keys that are shared (not redirected)
  - http://support.microsoft.com/kb/896459
- 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

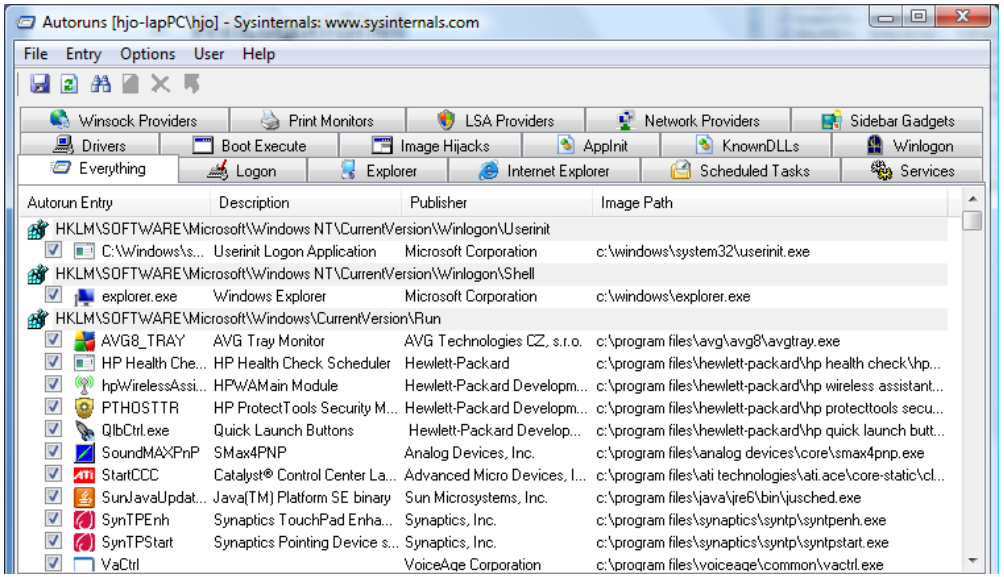
Platser för start av program och tjänster

- 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

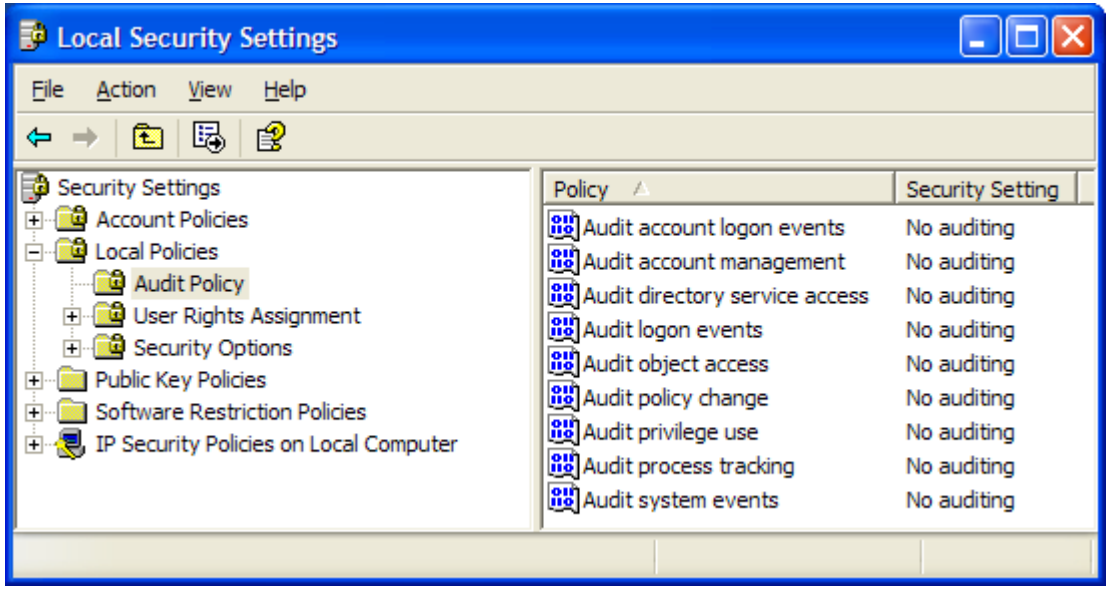
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
  - Run, RunOnce, Uninstall
  - HKLM\ … \WinLogon\Shell
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- 16 bit applikation support (liten användning, malware?)
  - System.ini
    - [Boot] sektionen – Shell
  - Win.ini
    - [Windows] sektionen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