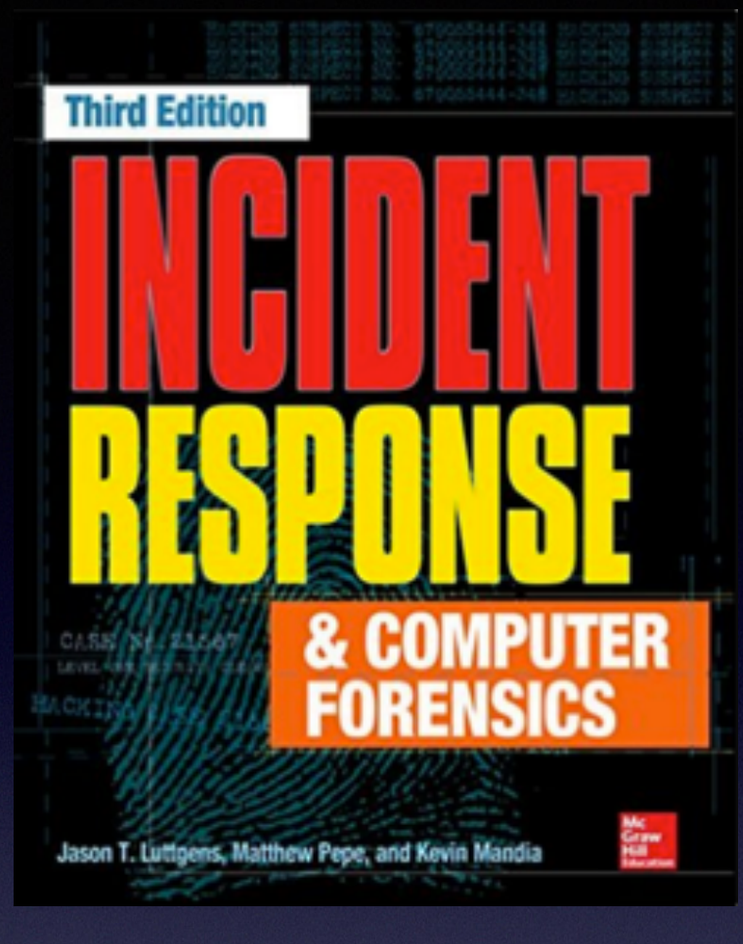
CNIT 152: Incident Response



12 Investigating Windows Systems (Part 2)

Updated 11-10-22

Ch 12 Part 2

- **The registry**

Ch 12 Part 3

- **Other artifacts of interactive sessions**
- **Memory forensics**
- **Alternative persistence mechanisms**

The Windows Registry

Purpose

- **The registry contains configuration data for the Windows operating system and applications**
- **Many artifacts of great forensic value**

Hive Files

- **Binary files that store the Registry**
- **Five main registry hives in %SYSTEMROOT%\system32\config**
  - **SYSTEM, SECURITY, SOFTWARE, SAM, DEFAULT**
- **User-specific hive files in each user's profile directory**
  - **\Users*username*\NTUSER.DAT**
  - **\Users*username**AppData**Local**Microsoft**Windows*\USRCLASS.DAT**

Windows Profiles

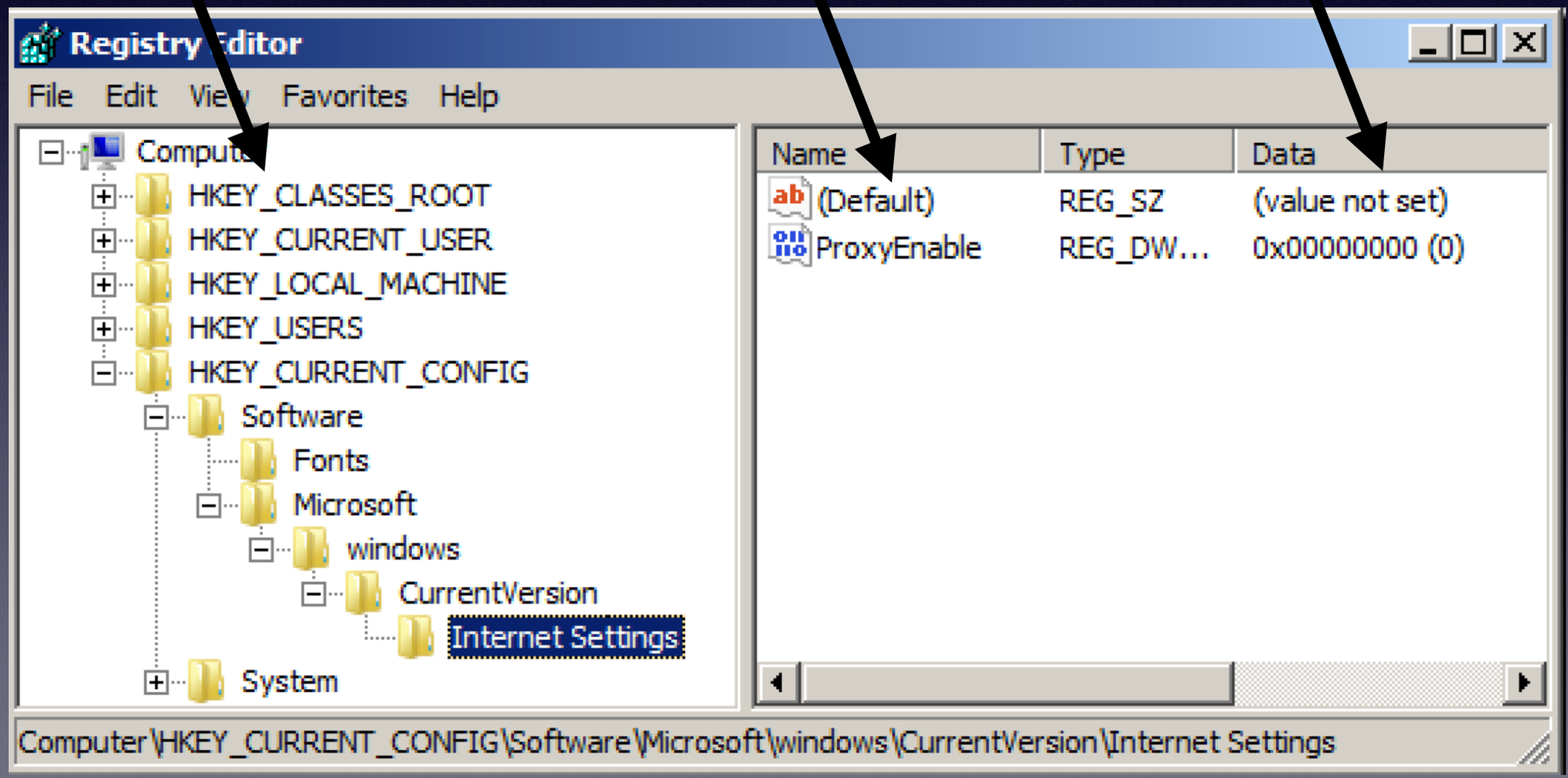
- **Created the first time a user interactively logs on to a system**
- **Users who connect over the network don't create a profile folder**

Terms

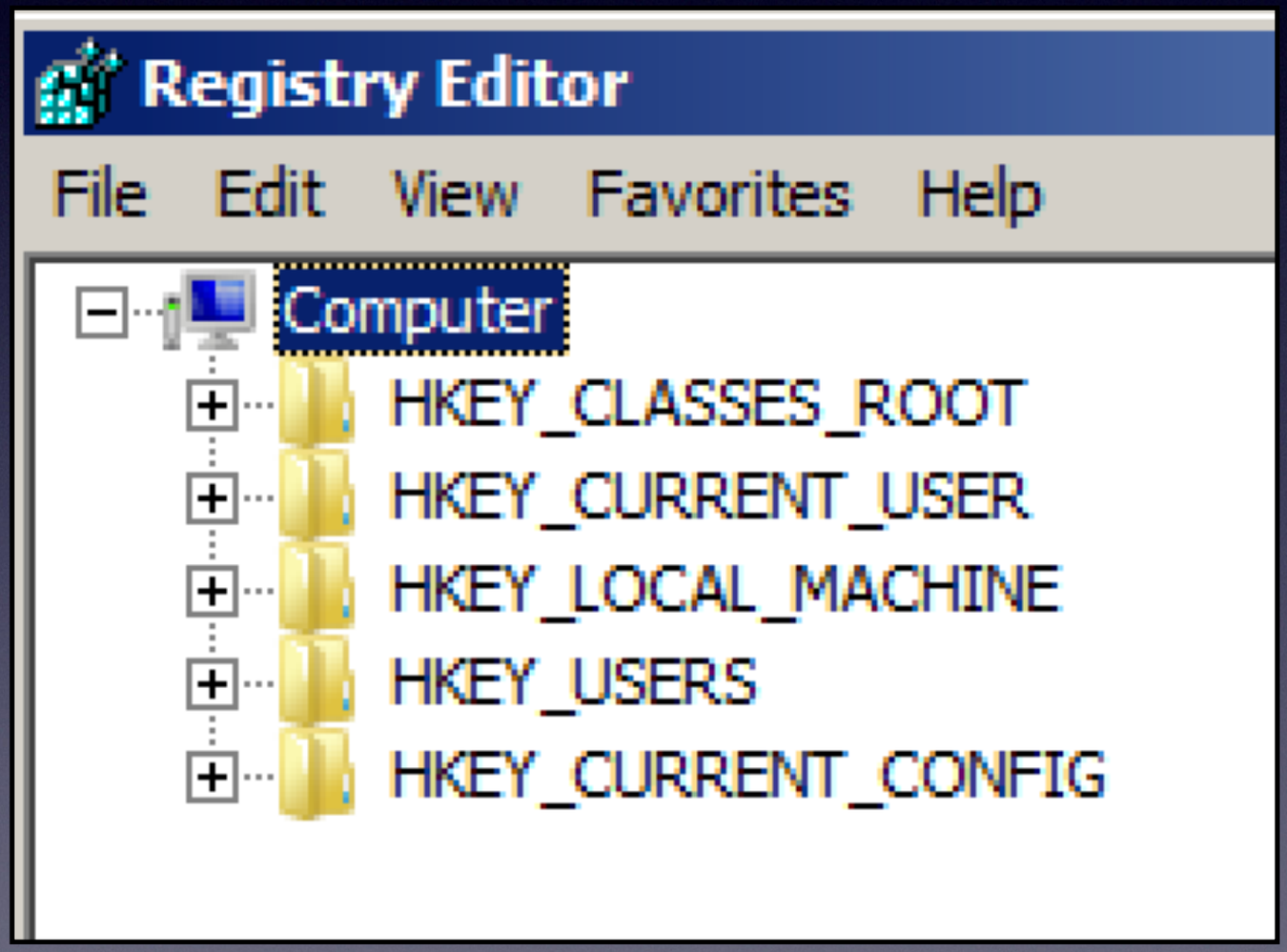
Keys

Values

Data



The Five Root Keys



HKEY_USERS

HKEY_USERS contains the following subkeys:

- **HKU\.DEFAULT maps to the DEFAULT hive.**
- **HKU\{SID} exists for each user security identifier (SID) on the system. The subkey for each SID maps to the corresponding user's NTUSER.DAT hive file.**
- **HKU\{SID}_Classes exists for each user SID on the system. The subkey for each SID maps to the corresponding user's USRCLASS.DAT hive file.**

Virtual Key Paths

- **Dynamically created in a running system**
- **Not visible on a registry capture**
- **HKEY_Current_User**
  - **Links to HKEY_USERS*{SID}***
- **HKLM\SYSTEM\CurrentControlSet**
  - **Links to HKLM\SYSTEM\ControlSet*NNN***
- **HKEY_CLASSES_ROOT**
  - **Merges two subkeys**

Registry Timestamps

- **Only one: LastWriteTime**
- **Stored on a key, not value**
- **Changed when any value under the key is added, removed, or changed**
  - **But not when subkeys' values are modified**

Example

- **Run key: programs that launch on system startup**
- **Cannot determine when these three Run items were added, without other evidence**

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\.

Value	Data	Key LastWriteTime
VMWare Tools	C:\Program Files\VMware\VMware Tools\VMwareTray.exe	2012-08-30 02:34:30
Adobe Reader Speed Launcher	C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe	2012-08-30 02:34:30
winupdat	C:\windows\addins\winupdat.exe	2012-08-30 02:34:30

More Limitations

- **Windows frequently updates the LastUpdateTime for large swaths of registry keys**
  - **During updates, and sometimes even from a reboot**
- **Attackers cannot easily change registry timestamps, although SetRegTime can do this**
  - **Link Ch 12o**

Registry Reflection and Redirection

- **64-bit Windows allows 32-bit software to run**
- **32-bit programs are redirected by the W0W64 sybsystem to alternate registry keys, like**
  - **HKLM\SOFTWARE\WoW6432Node**
- **This means 32-bit forensic software won't see the whole Registry**

Important Registry Keys

System Configuration Registry Keys

Shim Cache

Common Auto-Run Registry Keys

User Hive Registry Keys

System Configuration Registry Keys

Basic System Information

- **Computer Name**
  - **`HKLM\System\CurrentControlSet\Control\Computername`**
- **Windows Version**
  - **`HKLM\Software\Microsoft\Windows NT\CurrentVersion`**
- Time Zone
  - **`HKLM\System\CurrentControlSet\Control\TimeZoneInformation`**

Basic System Information

- **List of Installed Applications**
  - **`HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\{Appname}`**
- **Mounted Devices (with drive letters)**
  - **`HKLM\System\MountedDevices`**

USBSTOR

- **Shows every USB device that has been connected**
- **A forensic examiner should look here first, to find out what other devices should be requested for discovery, by court order or search warrant**

Network Information

- **Network adapter configuration**
- **Wireless networks previously used**
- **Shares**
- **Firewall settings**

User and Security Information

- **Audit policy**
- **Profile folder path**
- **Group membership**

Shim Cache

Shim Cache

- **Also called "Application Compatibility Cache"**
- **Used to track special compatibility settings for executable files and scripts**
- **May include:**
  - **File name, path, and size**
  - **Last modified date**
  - **Whether the file actually ran on the system**

Shim Cache

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCache

- **Maintained in memory, written to the registry on shutdown**
- **Maintains up to 1024 entries**
  - **More than Prefetch (128)**
- **includes apps that haven't executed yet**
- **Next two slides from link Ch 12a**

ShimCacheParser

- ShimCacheParser.py
  - Automatically locates AppCompatCache related keys, determines their structure type and exports the data
  - 6 types of input:

- Download at https://github.com/mandiant/ShimCacheParser

ShimCacheParser

- Output in CSV format

```
> ShimCacheParser.py -i D:\case\SYSTEM -o D:\case\output.txt
```

Last Modified	Last Update	Path	File Size	Process Exec Flag
08/27/12 19:53:26	N/A	C:\Windows\system32\sql.exe	N/A	No
08/27/12 19:52:34	N/A	C:\Users\joeuser\AppData\Local\Temp\tmp83e46c15\12345.exe	N/A	Yes
07/14/09 01:14:41	N/A	C:\Windows\system32\svchost.exe	N/A	No
08/24/12 19:19:59	N/A	C:\Windows\system32\b.exe	N/A	No
07/14/09 01:14:12	N/A	C:\Windows\system32\at.exe	N/A	No
08/24/12 19:37:47	N/A	C:\Windows\system32\msabc.exe	N/A	No
07/14/09 01:14:27	N/A	C:\Windows\system32\net1.exe	N/A	No
07/14/09 01:14:45	N/A	C:\Windows\system32\whoami.exe	N/A	No
07/14/09 01:14:27	N/A	C:\Windows\system32\NETSTAT.EXE	N/A	No
08/24/12 19:16:36	N/A	C:\Users\joeuser\AppData\Local\Temp\tmp591d39cc\12345.exe	N/A	Yes

Kahoot!

Ch 12b-1

Common Auto-Run Registry Keys

Auto-Run Keys (Auto-Start Extensibility Points)

- **Load programs on system boot, user login, and other conditions**
- **Commonly used by malware to attain persistence**
- **Windows provides hundreds of registry-based persistence mechanisms**
  - **Some are still undocumented**

Services

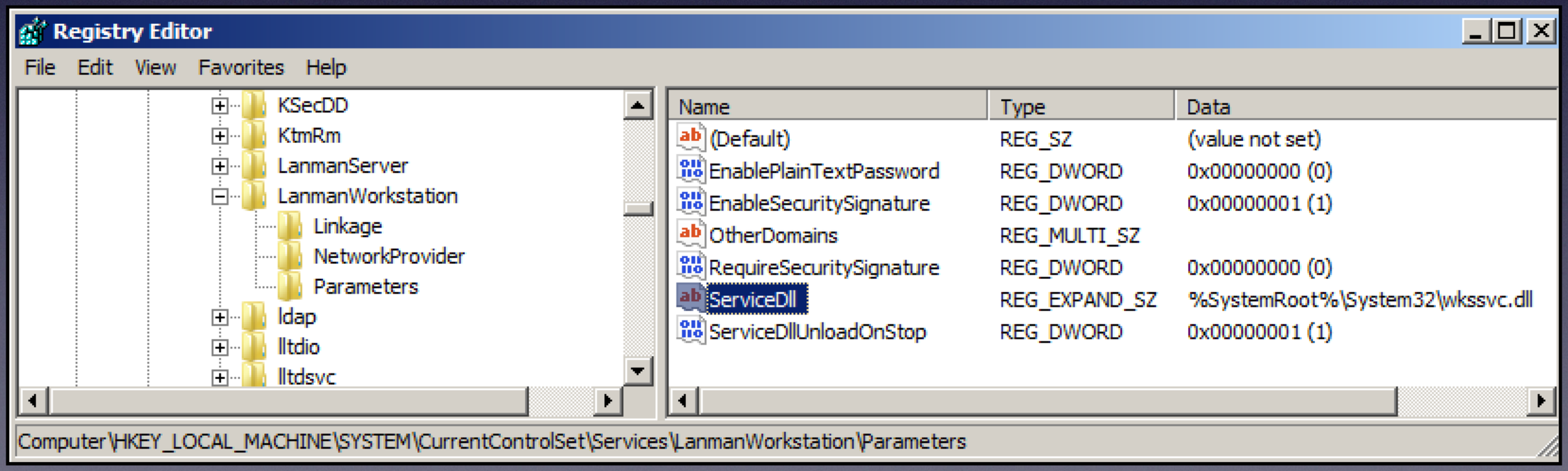
- **Most common and widely used persistence mechanism**
- **Services run in the background**
- **Usually under one of these login accounts**
  - **Local System (most powerful)**
  - **Network System**
  - **Local Service**

Services in the Registry

- **Each service has its own subkey under**
- **HKLM\CurrentControlSet\services*servicename***
- **With this information:**
  - **DisplayName and Description**
  - **ImagePath**
  - **How service starts**
  - **Type of service, such as driver or process**

ServiceDLL

- **Most services are DLL, not EXE files**



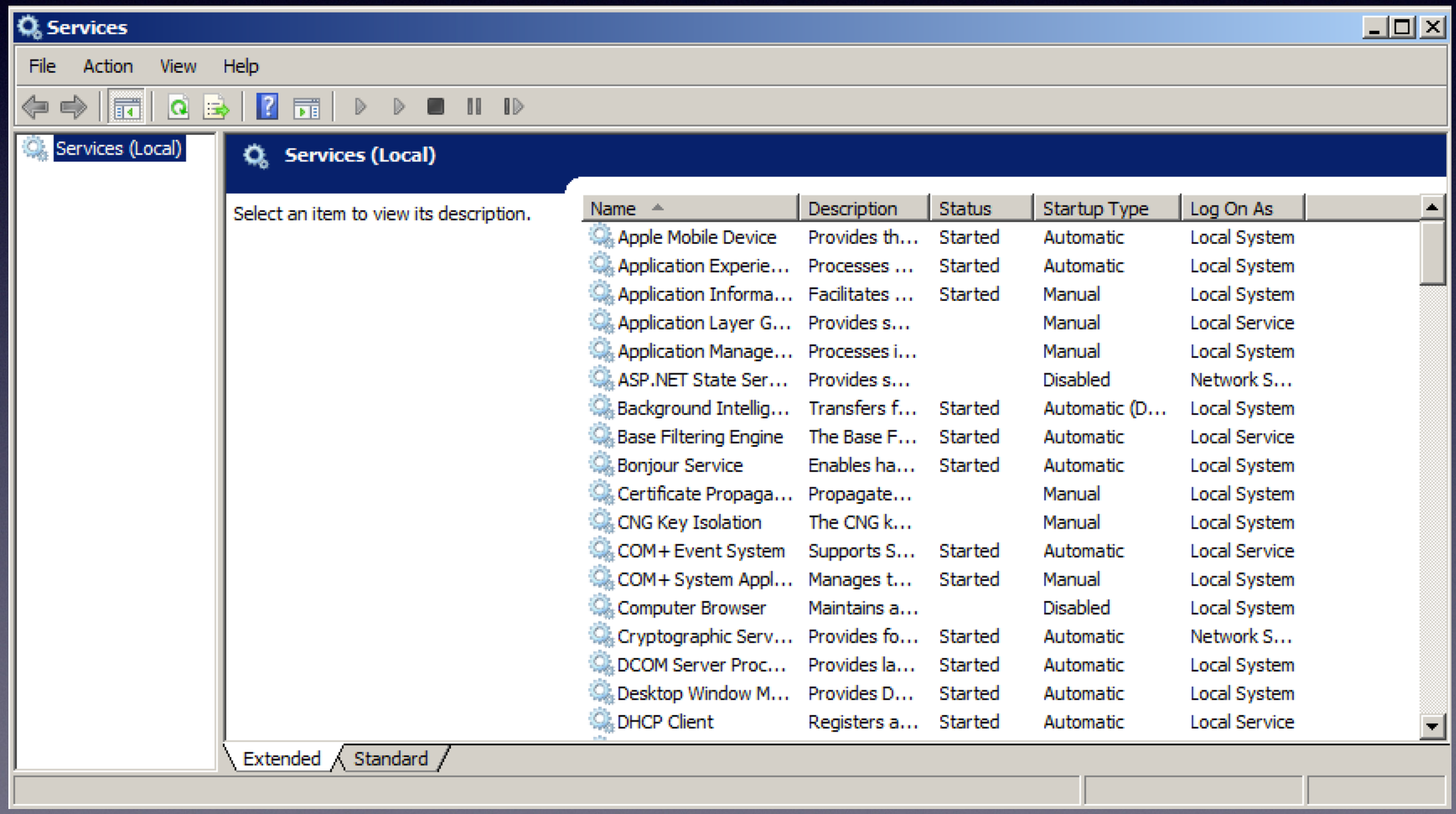
Service Control Manager

- **Services.exe**
- **Launches Windows services upon startup**
- **Command-line "sc" command lets you examine, start, stop, and create services**

sc at Command line

```
C:\Users\Administrator>sc query wuauserv

SERVICE_NAME: wuauserv
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Services GUI



One EXE Can Run Several Services

Administrator: Command Prompt

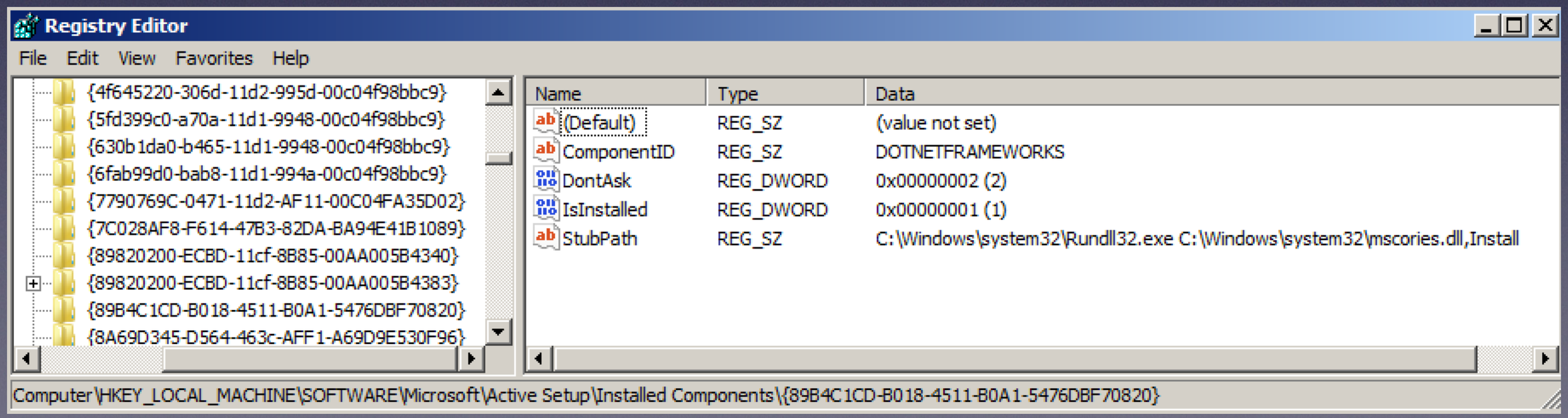
```
C:\Users\Administrator>tasklist /svc

Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       424 N/A
csrss.exe                      488 N/A
csrss.exe                      532 N/A
wininit.exe                    540 N/A
winlogon.exe                   572 N/A
services.exe                   640 N/A
lsass.exe                      648 SamSs
lsm.exe                        656 N/A
svchost.exe                    816 DcomLaunch, PlugPlay
vmacthlp.exe                   860 VMware Physical Disk Helper Service
svchost.exe                    892 RpcSs
svchost.exe                    928 Dhcp, EventLog, lmhosts
svchost.exe                   1020 gpsvc
svchost.exe                   1076 AeLookupSvc, Appinfo, BITS, IKEEXT,
                                   iphlpsvc, LanmanServer, ProfSvc, RasMan,
                                   Schedule, seclogon, SENS, ShellHWDetection,
                                   Winmgmt, wuauserv
SLsvc.exe                     1096 slsvc
```

Four Common Run Keys

- **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
- **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**
- **HKEY_USERS\{SID}\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**
- **HKEY_USERS\{SID}\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**

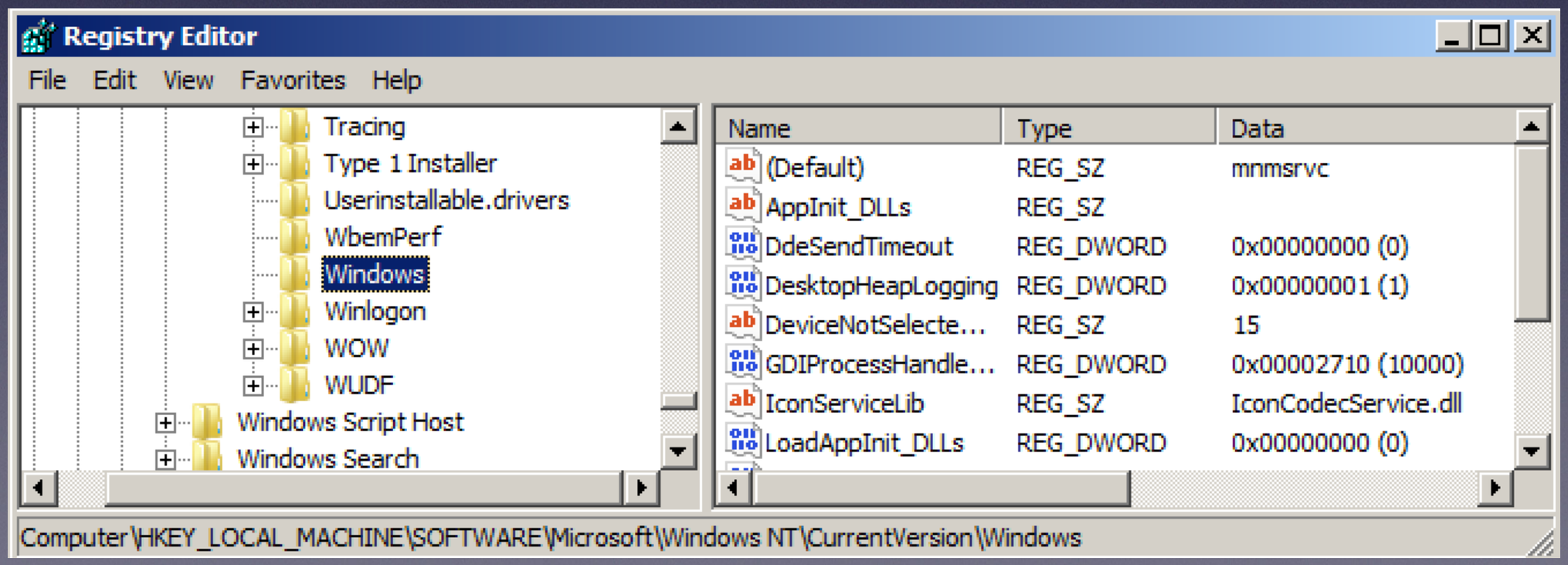
Active Setup

- **Facilitates software installation and updates**
- **Subkeys named with GUIDs (long random-looking numbers)**
- **Malware authors often re-use GUIDs so Googling them can be useful**
- **StubPath points to an EXE that will run on startup**



AppInit_DLLs

- **DLLs that will be automatically loaded whenever a user-mode app linked to user32.dll is launched**
  - **Almost every app uses user32 to draw windows, etc. (link Ch 12p)**



AppInit_DLLs

- **Starting in Windows 8, the AppInit_DLLs infrastructure is disabled when secure boot is enabled**
- **Secure boot is a UEFI protocol and not a Windows 8 feature.**

LSA (Local Security Authority) Packages

- **Load on startup**
- **Intended for authentication packages, but can be used to launch malware**

- **HKLM\System\CurrentControlSet\Control\Lsa\Authentication Packages**
- **HKLM\System\CurrentControlSet\Control\Lsa\Notification Packages**
- **HKLM\System\CurrentControlSet\Control\Lsa\Security Packages**

Browser Helper Objects (BHOs)

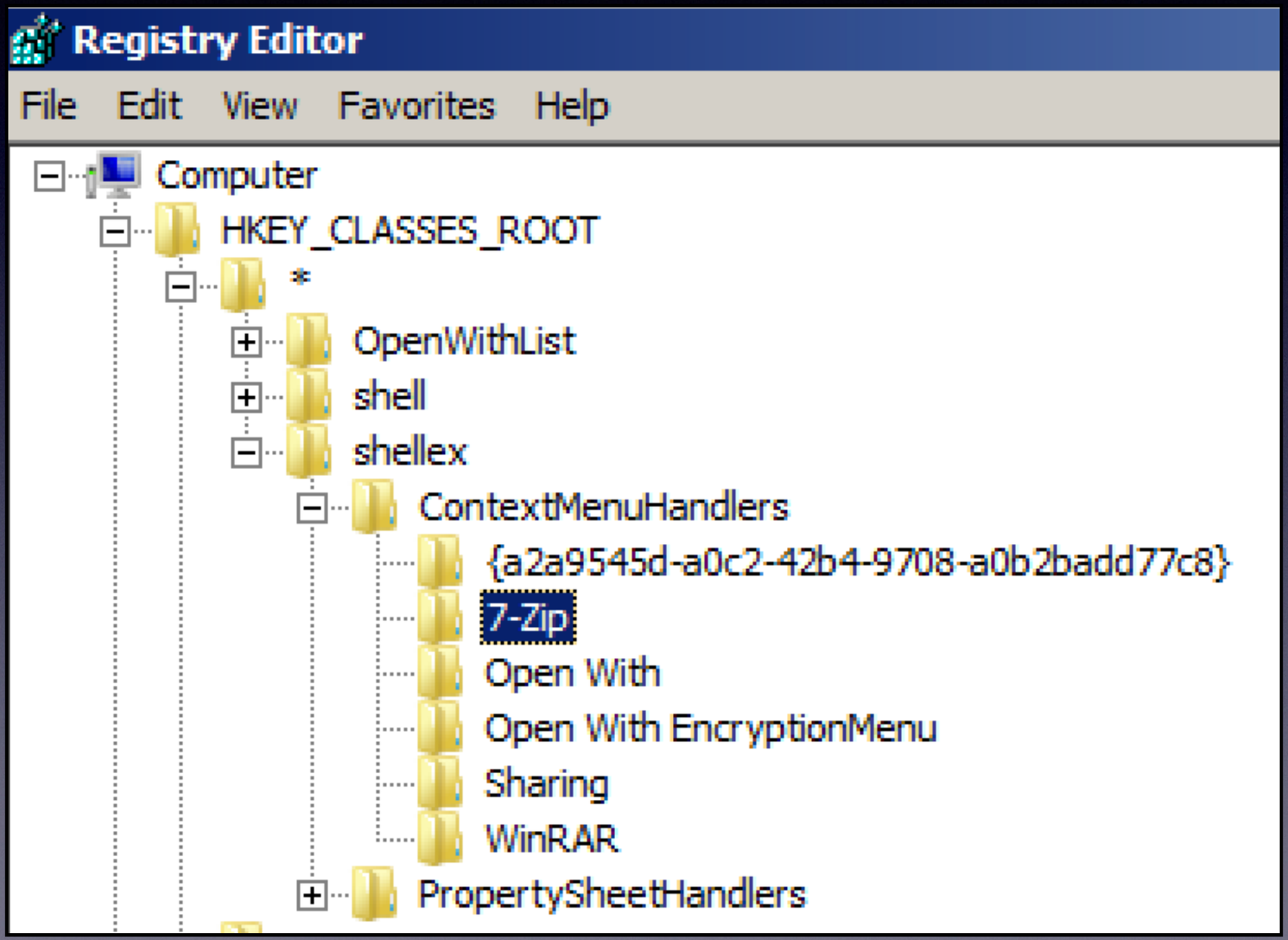
- **Add-ons or plug-ins for Internet Explorer**
- **Such as toolbars, adware, scareware**
- **No longer supported in Edge**

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{CLSID}

Shell Extensions

- **Like Browser Helper Objects, but for Windows Explorer**
- **Add context items when right-clicking a file**
- **Found at:**
  - **HKCR\CLSID\{CLSID}\InprocServer32**
  - **HKCR\{sub-key}\shellex**

Shell Extensions



Winlogon Shell

- **The shell that loads when a user logs on**
- **Normally set to Explorer.exe**
- **Can be set to any executable file**

  - **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell**
  - **HKEY_USERS\{SID}\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell**

Winlogon Userinit

- **Loads logon and group policy scripts, other auto-runs, and the Explorer shell**
- **Attackers can append additional executables to this value**

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

Identifying Malicious Auto-Runs

- **Eyeball it, looking for suspicious files or paths, spelling errors, broken English, etc.**
  - **Risky; real commercial software is often sloppily made, and some attackers are careful**
- **Next slide: which item is malicious?**

ServiceName: hpdj

Description: [none]

ImagePath: C:\Documents and Settings\johncd\Local Settings\Temp\hpdj.exe

---

ServiceName: iprip

Description: Listens for route updates sent by routers that use the Routing Information Protocol

ImagePath: C:\Windows\system32\svchost.exe

ServiceDll: C:\Windows\system32\iprinp32.dll

ServiceName: rfalert

Description: A module which sends alerts and notifications of monitered events

ImagePath: D:\Apps\RightFax\Bin\Alertmon.exe

ServiceName: synergy

Description: Allows another computer to share its keyboard and mouse with this computer

ImagePath: C:\Program Files\Synergy\synergyc.exe

ServiceName: hpdj

Description: [none]

ImagePath: C:\Documents and Settings\johncd\Local Settings\Temp\hpdj.exe

---

ServiceName: iprip

Description: Listens for route updates sent by routers that use the Routing Information Protocol

ImagePath: C:\Windows\system32\svchost.exe

ServiceDll: C:\Windows\system32\iprinp32.dll

ServiceName: rfalert

Description: A module which sends alerts and notifications of monitered events

ImagePath: D:\Apps\RightFax\Bin\Alertmon.exe

ServiceName: synergy

Description: Allows another computer to share its keyboard and mouse with this computer

ImagePath: C:\Program Files\Synergy\synergyc.exe

Recommended Steps

1. **Exclude persistent binaries signed by trusted publishers (but not all signed binaries)**
2. **Exclude persistent items created outside the time window of interest**
3. **Examine paths of remaining persistent binaries**
   - **Attackers tend to use Temp folders or common directories within %SYSTEMROOT%**
   - **Not deeply nested subdirectories specific to obscure third-party applications**

Recommended Steps

4. **Research MD5 hashes for remaining persistent binaries on VirusTotal, Bit9, etc.**
5. **Compare remaining unknowns against a known "gold image" used to install the systems**

Best Tool

- **Sysinternals AutoRuns**

Signed Malware

- **Attackers have been stealing code-signing signatures, and signing malware**
- **Also, not all legitimate persistent files, even Windows components, are signed**
- **Sometimes updates remove signatures**

Kahoot!

Ch 12b-2

User Hive Registry Keys

Personalization

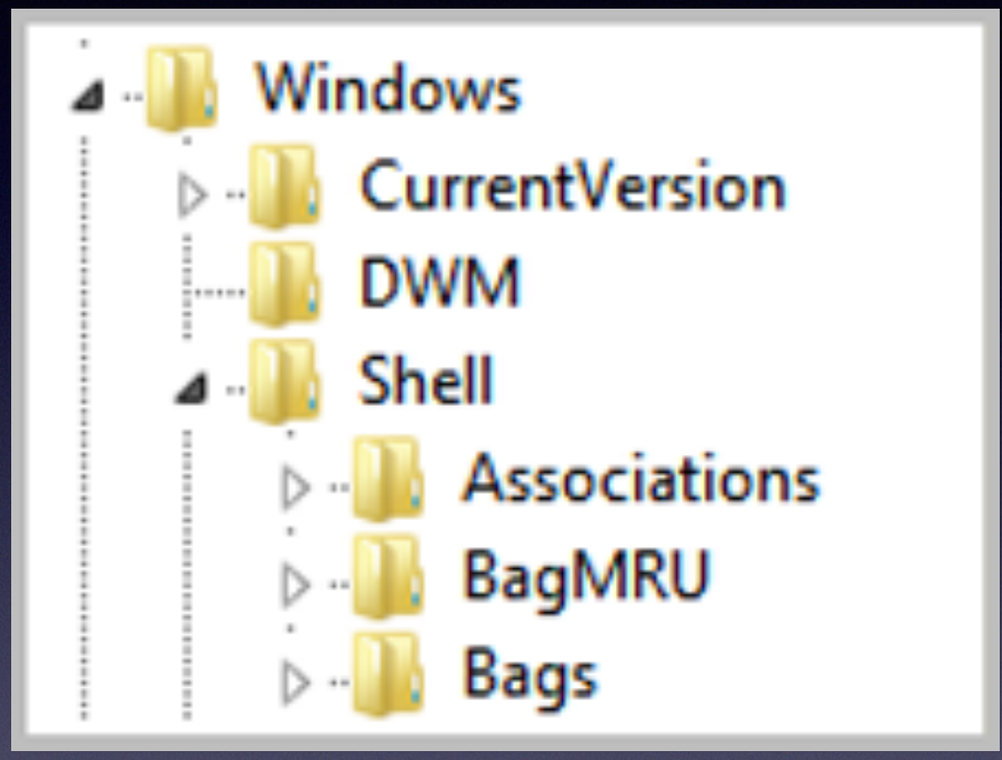
- **User hive registry keys contain personalization settings for each user**
- **First priority: examine compromised accounts**
  - **Acquire NTUSER.DAT and USRCLASS.DAT**
- **Check machine accounts, such as NetworkService and LocalSystem**
  - **May also contain evidence**

Most Helpful User-Specific Keys

- **Shellbags**
- **UserAssist**
- **MUICache**
- **Most Recently Used (MRU)**
- **TypedURLs**
- **TypedPaths**

Shellbags

- **Used to remember size, position, and view settings of windows**
- **Persist even if a directory is deleted**
- **Saved in a user's profile registry hive**



- **HKEY_USERS\{SID}_Classes\Local Settings\Software\Microsoft\Windows\Shell**

Shellbags Contain

- **Full directory paths accessed via Explorer**
- **Date and time of access**
- **Modified, Accessed, and Created times of each path *recorded when the access occurred***
- **Such historical records are very useful to track attacker actions**

Example Shellbags

	A	B	C	D	E	F	G
331	sbag - limited version ver: 0.18, Copyright (c) TZWorks LLC						
332							
333	ShellBag results for hive: C:\Users\chad\appData\local\microsoft\windows\usrclass.dat						
334							
335	UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\						
336	**bag**	**Regkey modtime [UTC]**	**folder name**	**createdate**	**ctime**	**modifydate**	**mtime**
337	1009	06/16/11 00:28:35.480	Decode	12/20/2010	15:14:06	12/20/2010	15:14:06
338	1057	06/16/11 00:28:35.480	regripper	12/20/2010	15:14:22	12/20/2010	15:14:22
339	1170	06/16/11 00:28:35.480	ADS	12/20/2010	15:14:04	12/20/2010	15:14:04
340	1197	06/16/11 00:28:35.480	web surfing forensic tools	12/20/2010	15:14:46	12/20/2010	15:14:46
341	1291	06/16/11 00:28:35.480	sleuthkit-windows	12/20/2010	15:14:26	12/20/2010	15:14:30
342	1366	06/16/11 00:28:35.480	printer tools	12/20/2010	15:14:22	12/20/2010	15:14:22
343	1587	06/16/11 00:28:35.480	memory imaging	12/20/2010	15:14:12	12/20/2010	15:14:14

UserAssist

**HKEY_USERS\
{SID}\Software\Microsoft\Windows\CurrentVersion
\Explorer\UserAssist**

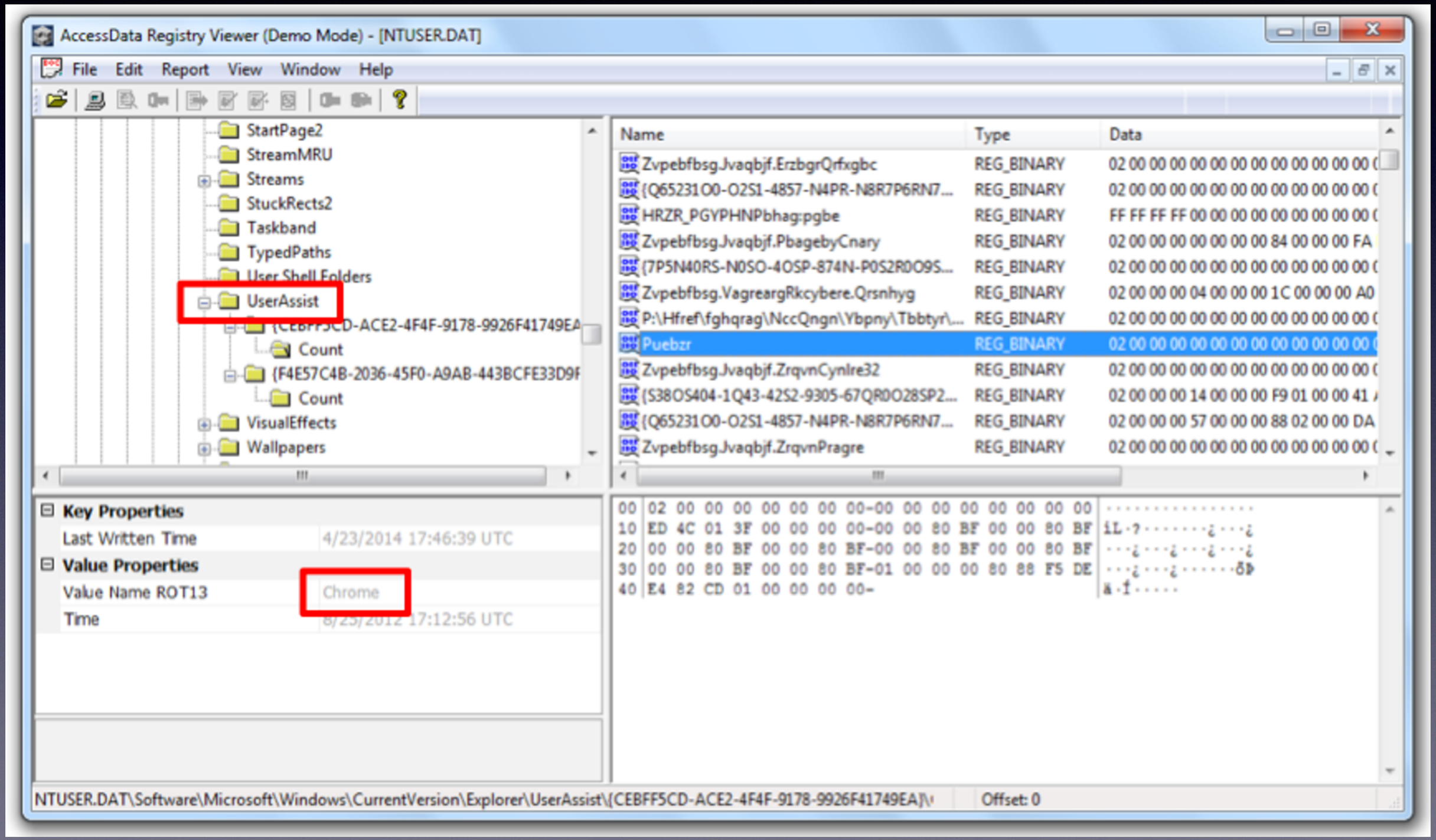
- **Tracks applications a user has launched through the Windows Explorer shell**
- **Populates Start menu with frequently launched programs**

  - **Full paths to each executable**
  - **Number of times each program ran**
  - **Last execution time**

UserAssist v. Prefetch

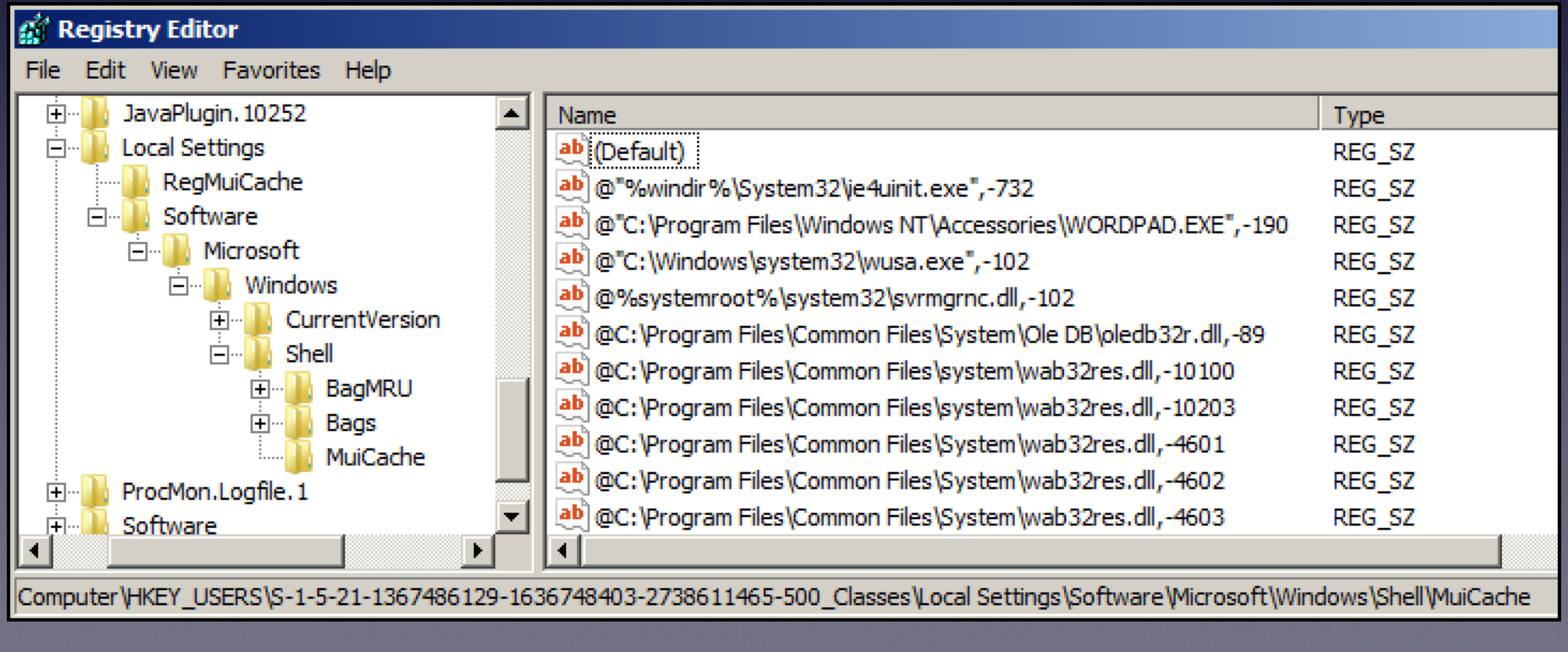
- **UserAssist only tracks items opened via Explorer**
  - **Including from the Run box and Start menu**
  - **But not from the command prompt**
- **Prefetch files don't identify which user executed a program**

Obfuscated with ROT13



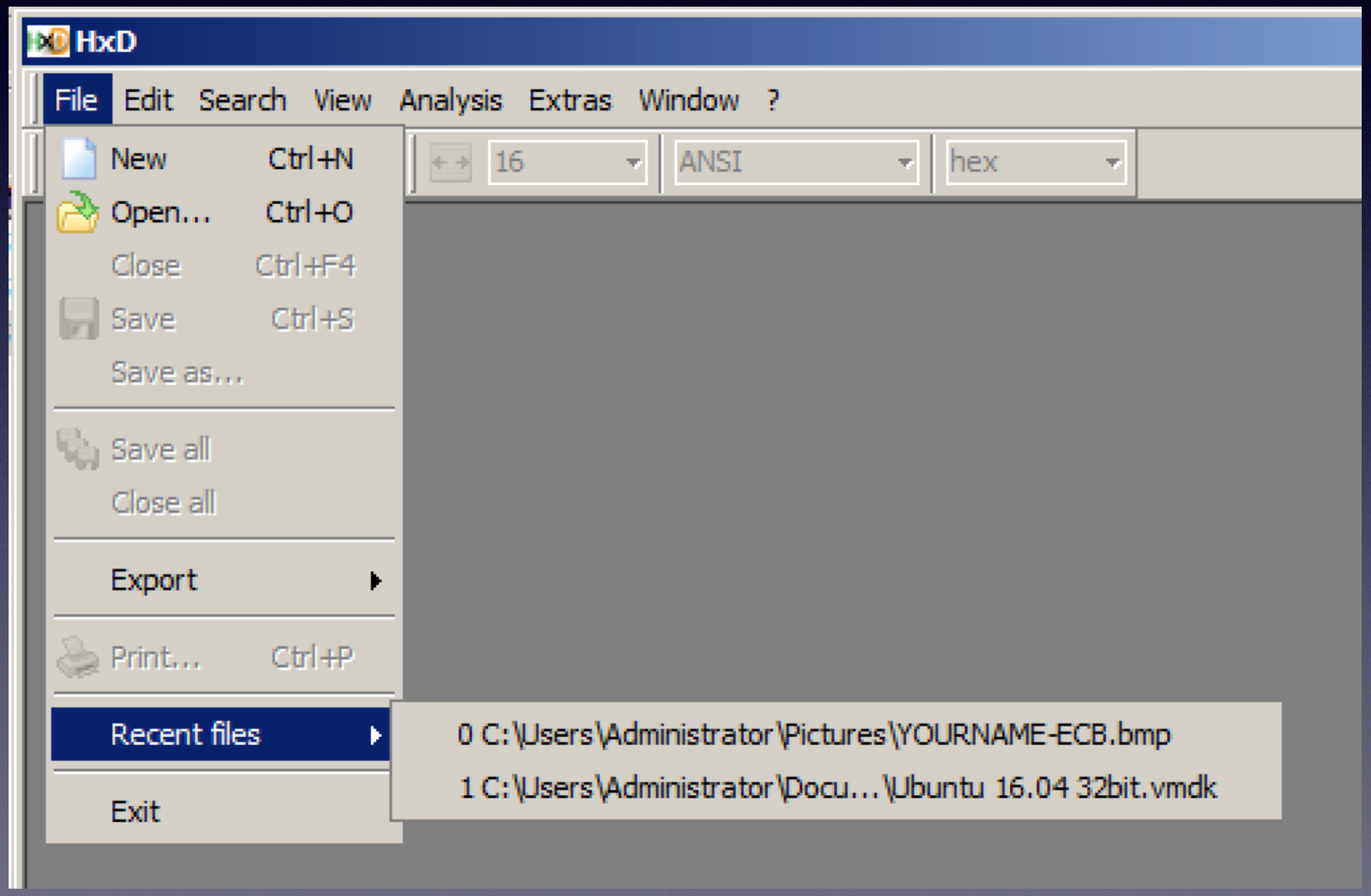
MUICache

- **Multilingual User Interface**
- **Another list of programs executed by a user**
- **HKEY_USERS\{SID}_Classes\LocalSettings\Software\Microsoft\Windows\Shell\MuiCache**



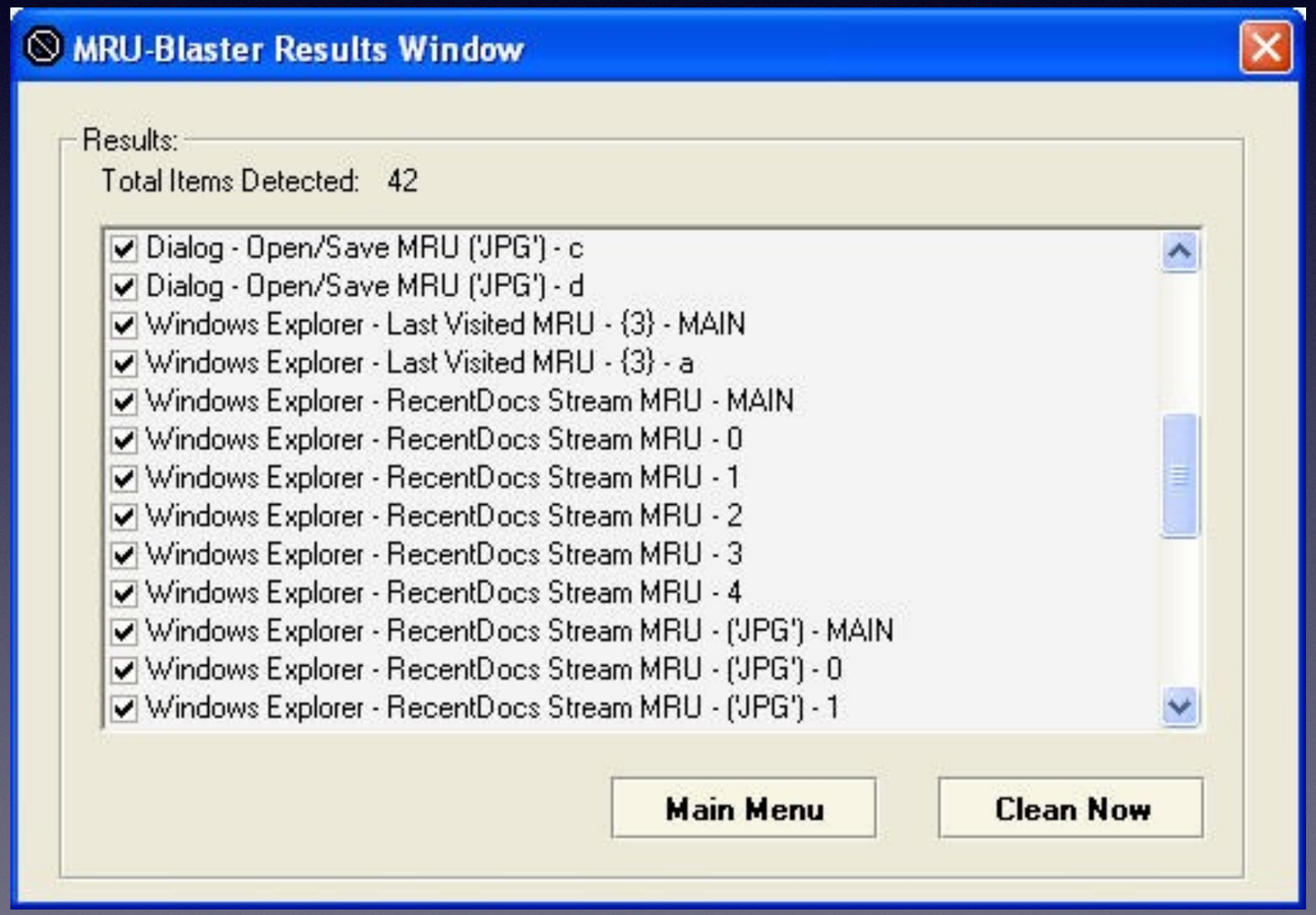
Most Recently Used (MRU) Keys

- **Used by many applications**
- **No standard registry path or value naming convention**



MRU-Blaster

- **Clears the MRU lists (link Ch 12r)**



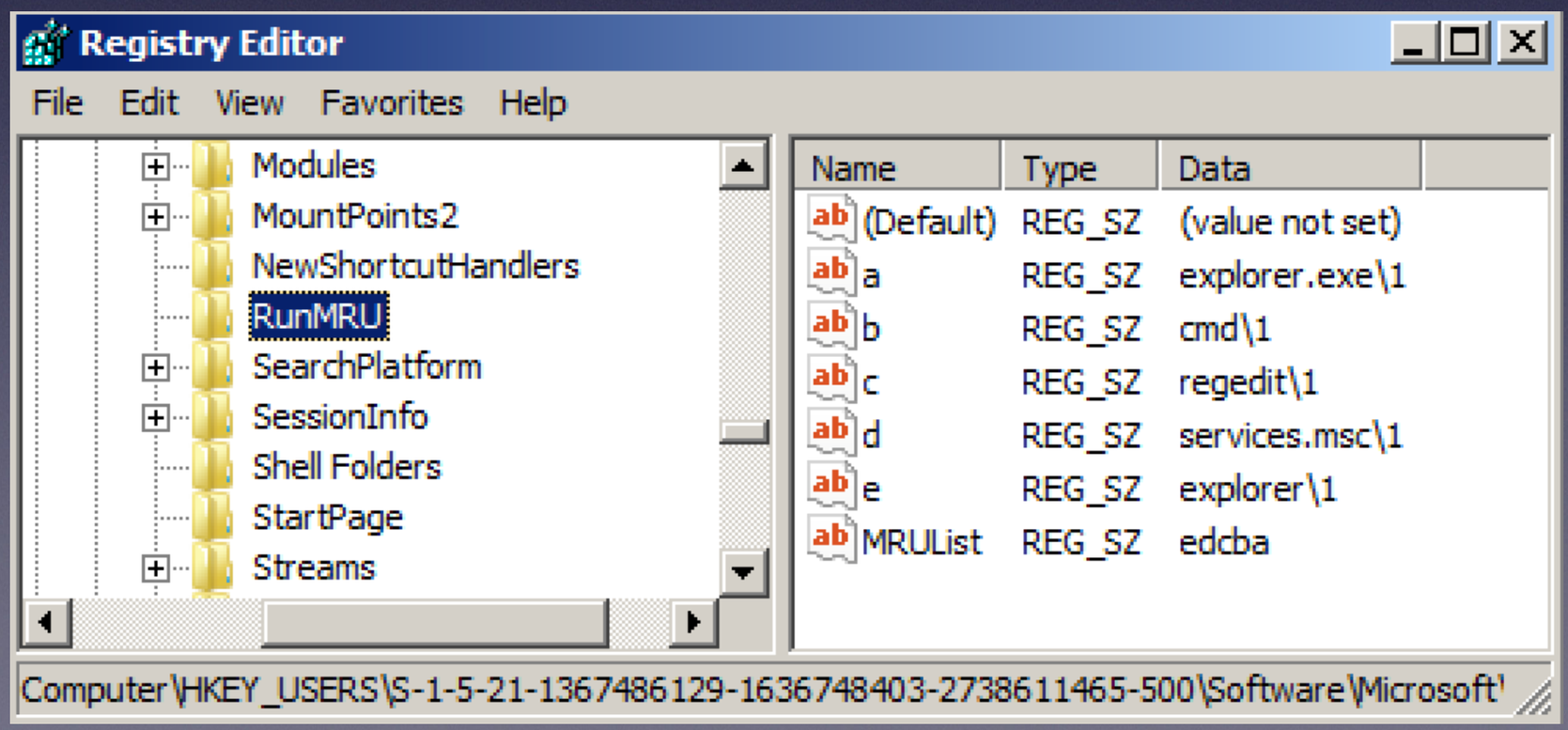
Explorer Open and Save MRU

- **Files and folders most recently accessed in the Open and Save dialog menus**
- **RegRipper can find the data**

- **HKEY_USERS\{SID}\Software \Microsoft\Windows\CurrentVersion\Explorer\ ComDlg32\OpenPidlMRU**
- **HKEY_USERS\{SID}\Software\Microsoft \Windows\CurrentVersion\Explorer \ComDlg32\LastVisitedPidlMRU**
- **HKEY_USERS\{SID}\Software\Microsoft \Windows\CurrentVersion\Explorer \ComDlg32\CIDSizeMRU**

Start Menu Run MRU

- **Programs recently launched from the Run box**
- **Human-readable**
- **\HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU**



RecentDocs

- **Recently opened documents (any file extension)**
- **Used to populate File menu of various applications**
- **HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**

Internet Explorer TypedURLs & TypedPaths

- **Used to populate the address bar drop-down list in Internet Explorer**
- **May contain URLs and paths to local files**
  - **\HKEY_USERS\{SID}\Software\Microsoft\InternetExplorer\TypedURLs**
  - **HKEY_USERS\{SID}\Software\Microsoft\InternetExplorer\TypedPaths**

Google - Windows Internet Explorer

https://www.google.com/?gws_rd=ssl

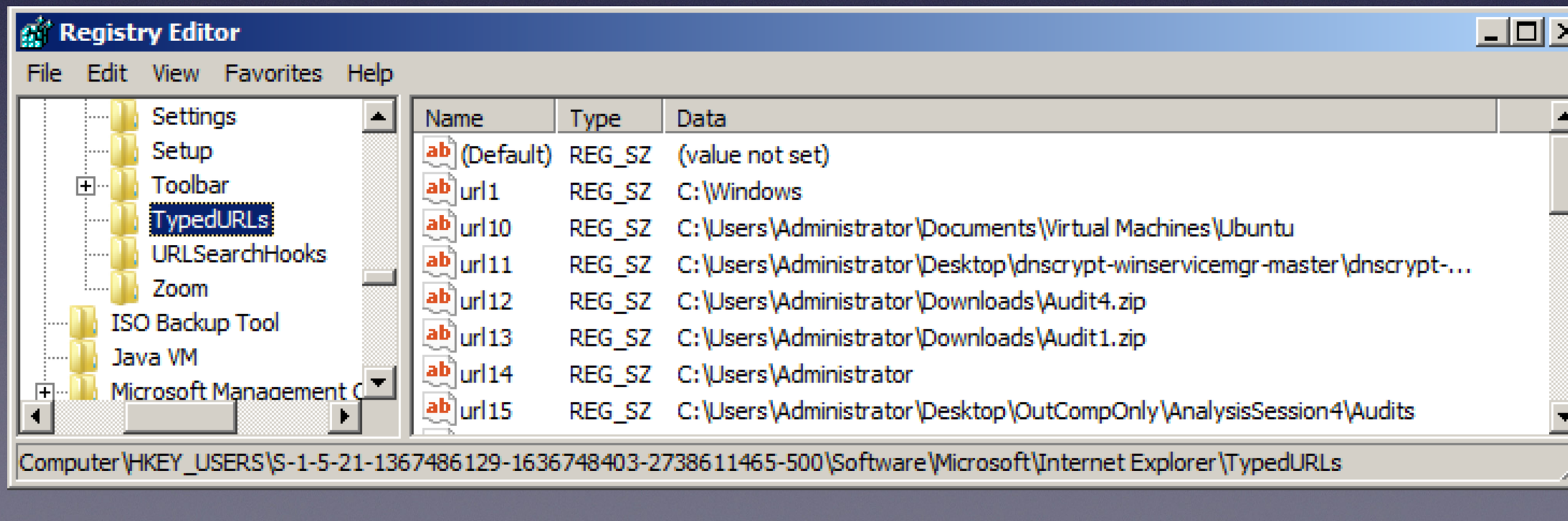
- http://google.com/
- C:\Windows
- C:\Windows\System32
- C:\Users\Administrator\Desktop\Streams
- C:\Windows\System32\0409
- F:\
- C:\Users\Administrator\Desktop\nsrllookup-1.2.3-win32
- C:\Users\Administrator\Desktop\Ub16.04\32bit
- C:\Users\Administrator\Downloads
- C:\Users\Administrator\Documents
- C:\Users\Administrator\Documents\Virtual Machines\Ubuntu
- C:\Users\Administrator\Desktop\dnscrypt-winservicemgr-master\dnscrypt-winservicemgr-n
- C:\Users\Administrator\Downloads\Audit4.zip
- C:\Users\Administrator\Downloads\Audit1.zip

Search

Google Search | I'm Feeling Lucky

Proves Intent

- **User typed (or pasted) these URLs into the address bar**
- **Didn't just click a link**



Remote Desktop MRU

- **Used to remotely control Windows machines**
- **Maintains history of recent connections and configuration data**
- **May tell you where a user connected and who they attempted to log in as**

- HKEY_USERS\{SID}\Software\Microsoft\Terminal Server Client\Default\
- HKEY_USERS\{SID}\Software\Microsoft\Terminal Server Client\Servers\

Registry Analysis Tools

All-In-One Tools

- **RegRipper (link Ch 10m)**
- **Windows Registry Decoder (link Ch 12s)**
- **AutoRuns**
- **Velociraptor**

Single-Purpose Utilities

- **ShimCacheParser**
- **Shellbags.py**
- **sbag**
- **UserAssist**
- **Nirsoft Registry Analysis Tools**

Ch 12b-3