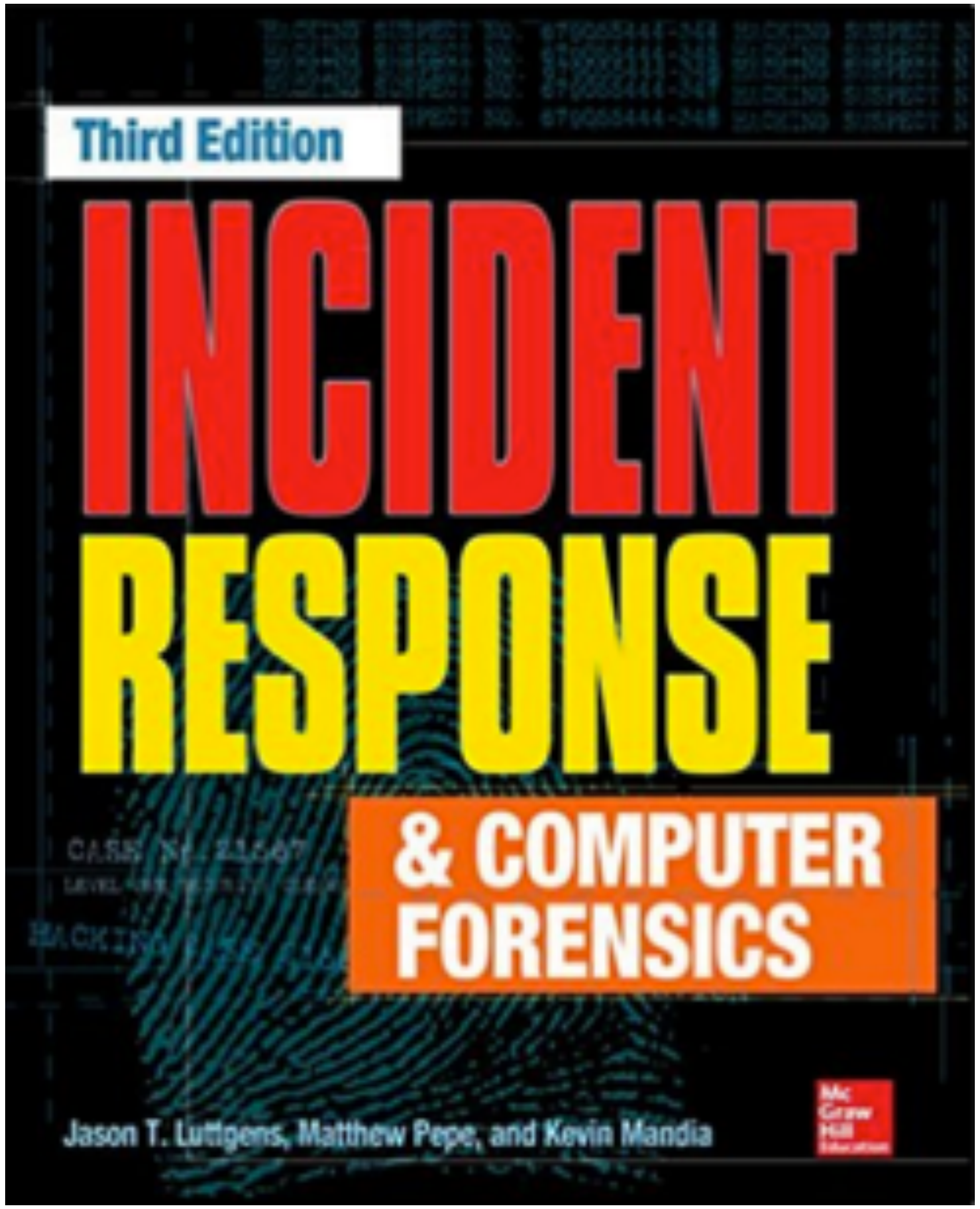
CNIT 121: Computer Forensics



12 Investigating Windows Systems (Part 2)

- The registry
- 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**

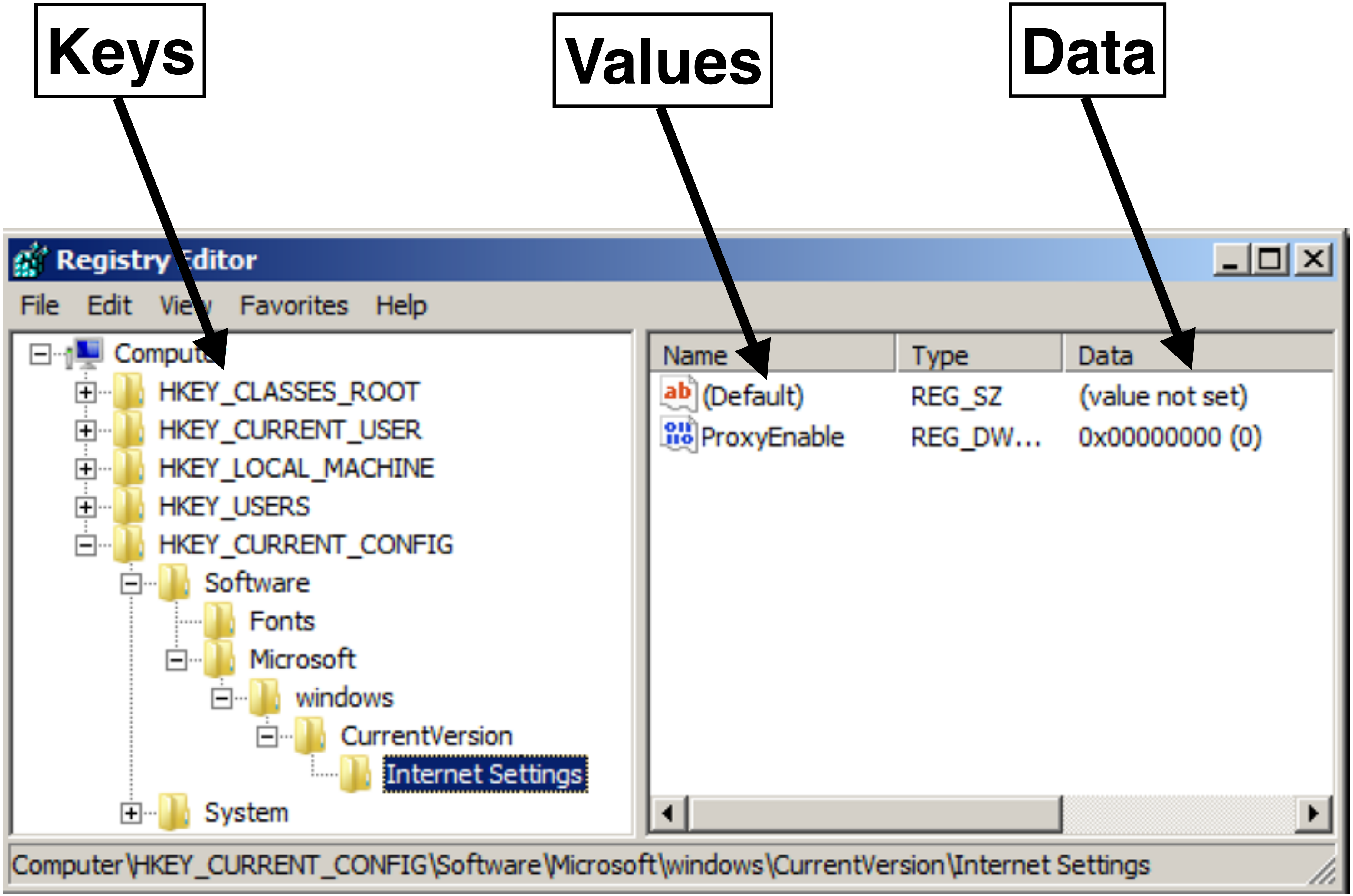
Hive Files

- **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

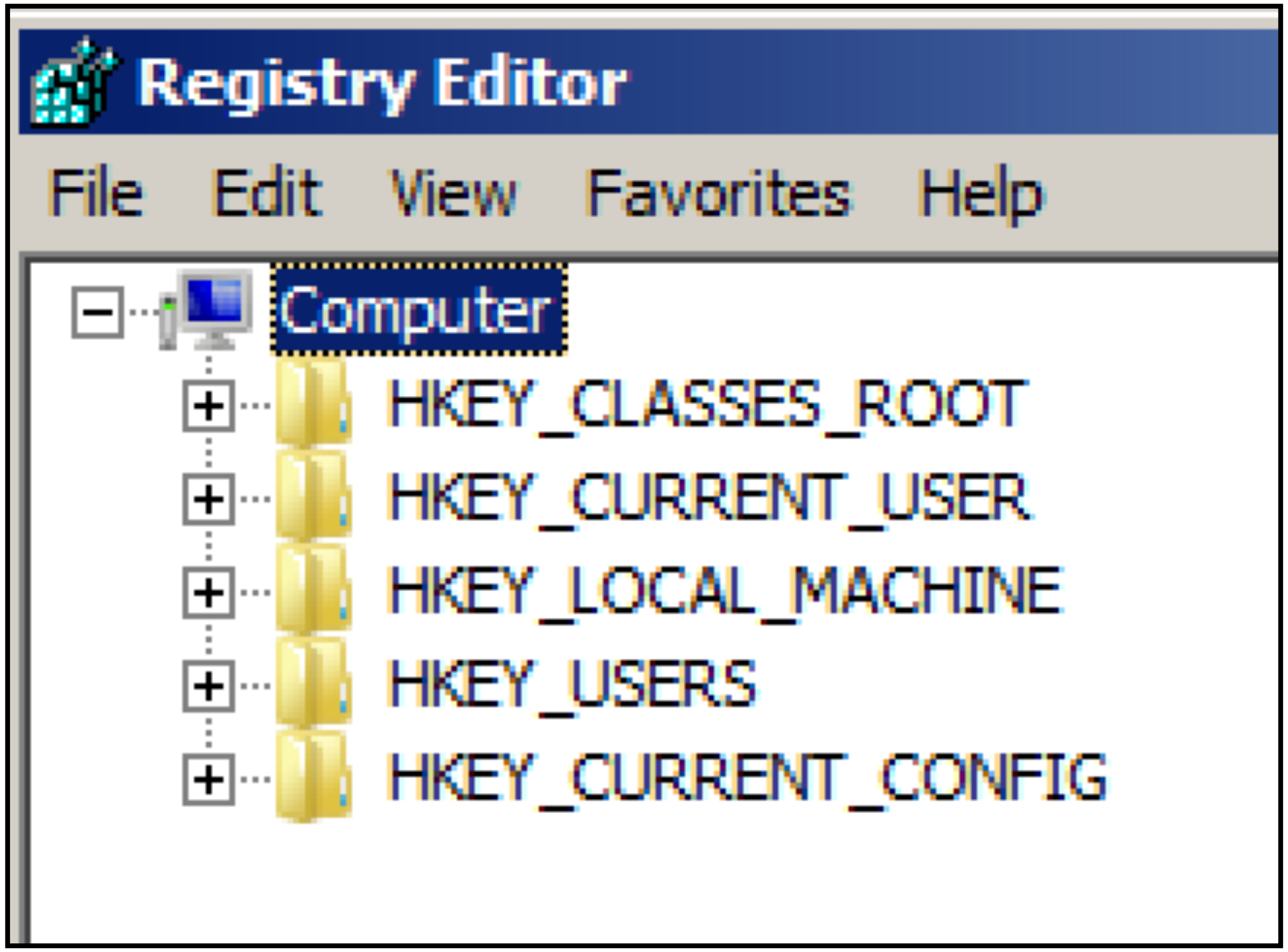
Data

```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
  HKEY_USERS
  HKEY_CURRENT_CONFIG
    Software
      Fonts
      Microsoft
        windows
          CurrentVersion
            Internet Settings
    System
```

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ProxyEnable	REG_DW...	0x00000000 (0)

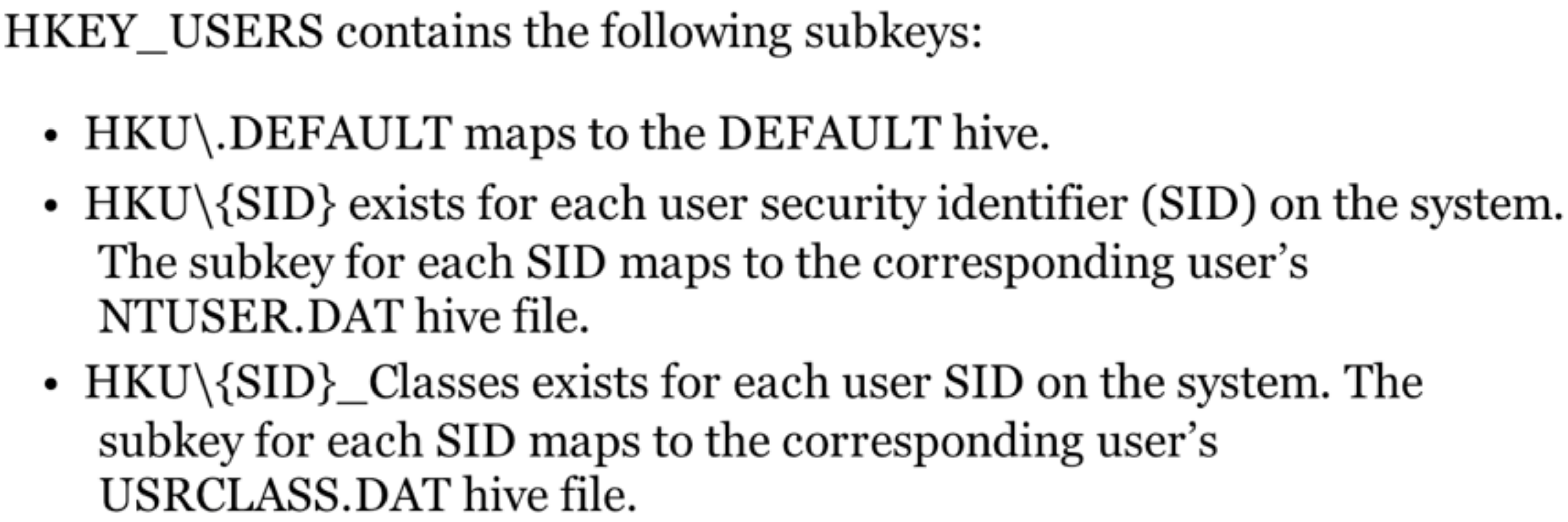
Computer\HKEY_CURRENT_CONFIG\Software\Microsoft\windows\CurrentVersion\Internet Settings

The Five Root Keys



HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG

HKEY_USERS

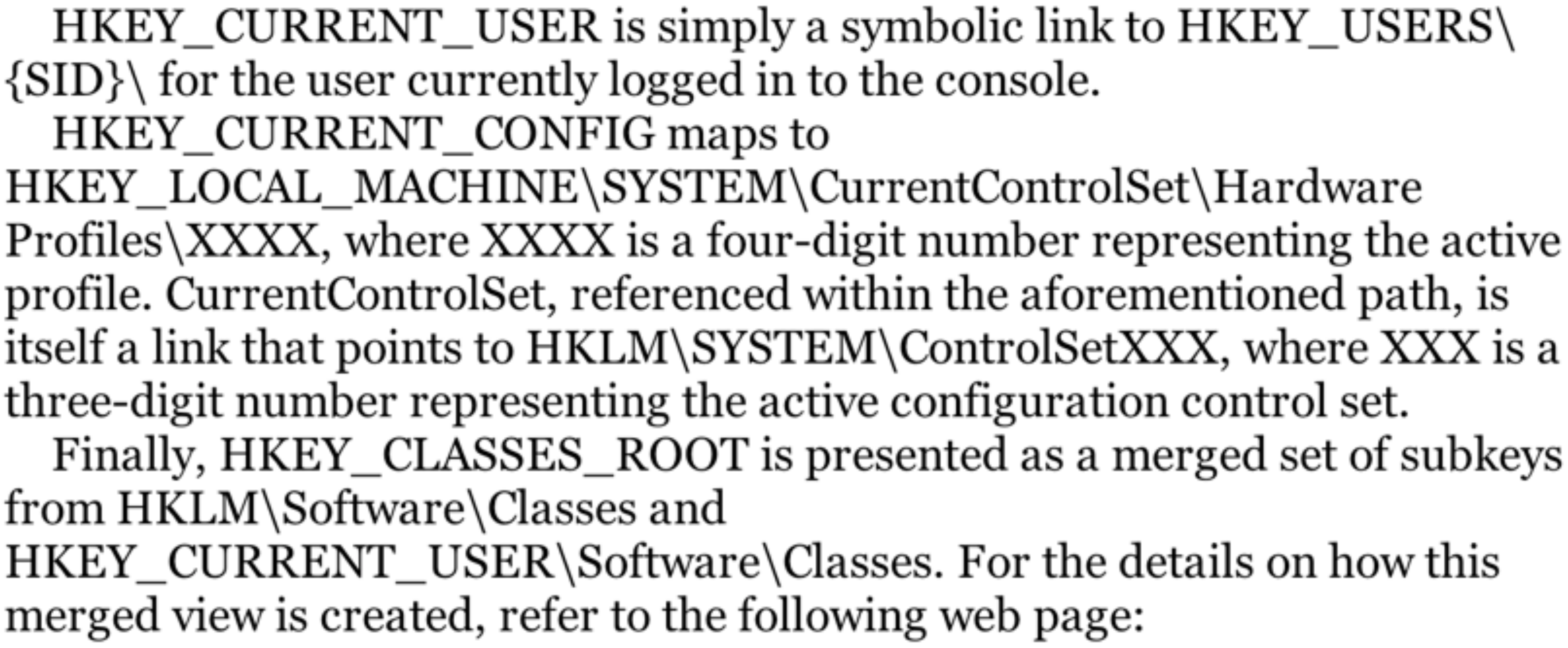


HKEY_USERS contains the following subkeys:

- 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 is simply a symbolic link to HKEY_USERS\{SID}\ for the user currently logged in to the console.

HKEY_CURRENT_CONFIG maps to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\XXXX, where XXXX is a four-digit number representing the active profile. CurrentControlSet, referenced within the aforementioned path, is itself a link that points to HKLM\SYSTEM\ControlSetXXX, where XXX is a three-digit number representing the active configuration control set.

Finally, HKEY_CLASSES_ROOT is presented as a merged set of subkeys from HKLM\Software\Classes and HKEY_CURRENT_USER\Software\Classes. For the details on how this merged view is created, refer to the following web page:

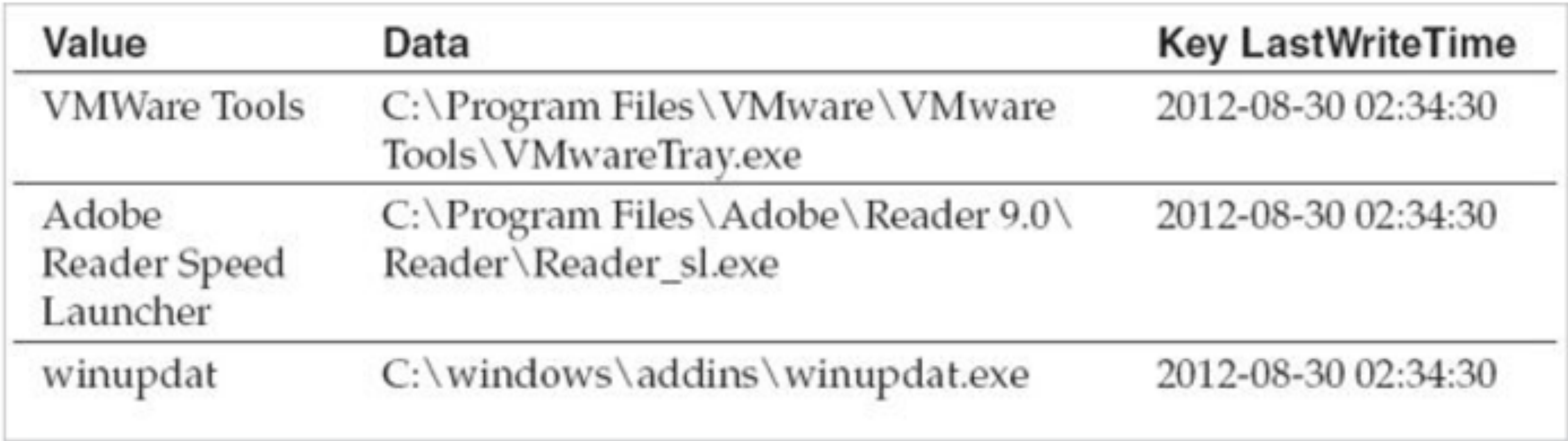
Registry Timestamps

- **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

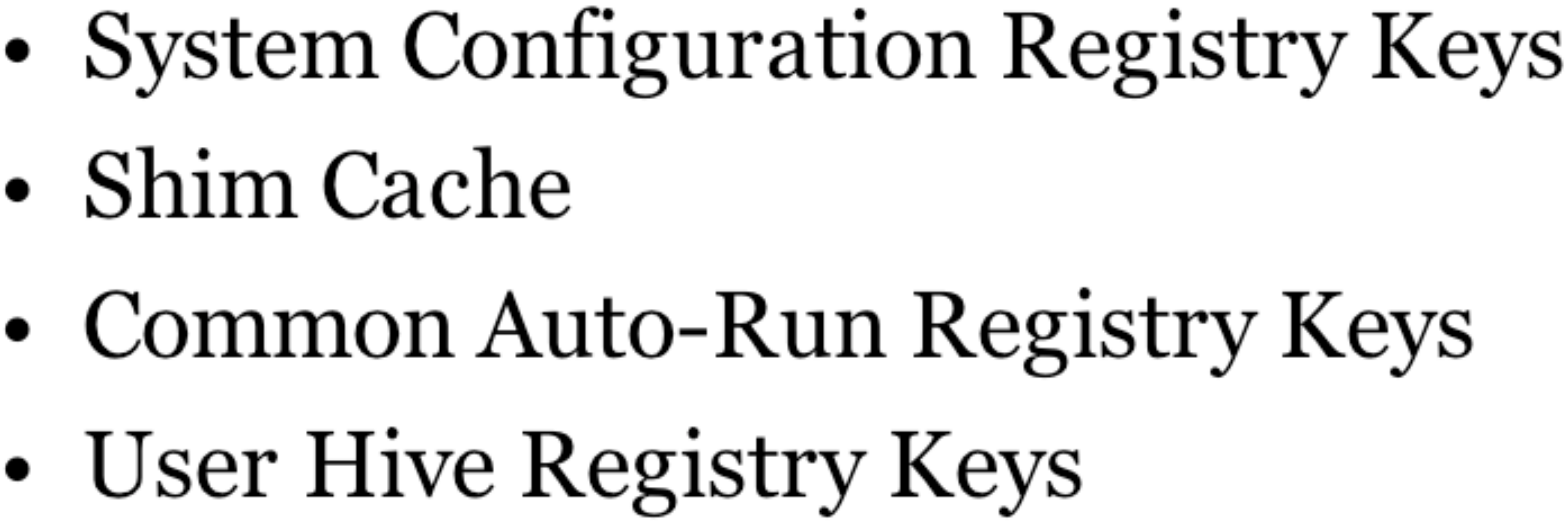
More Limitations

- **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

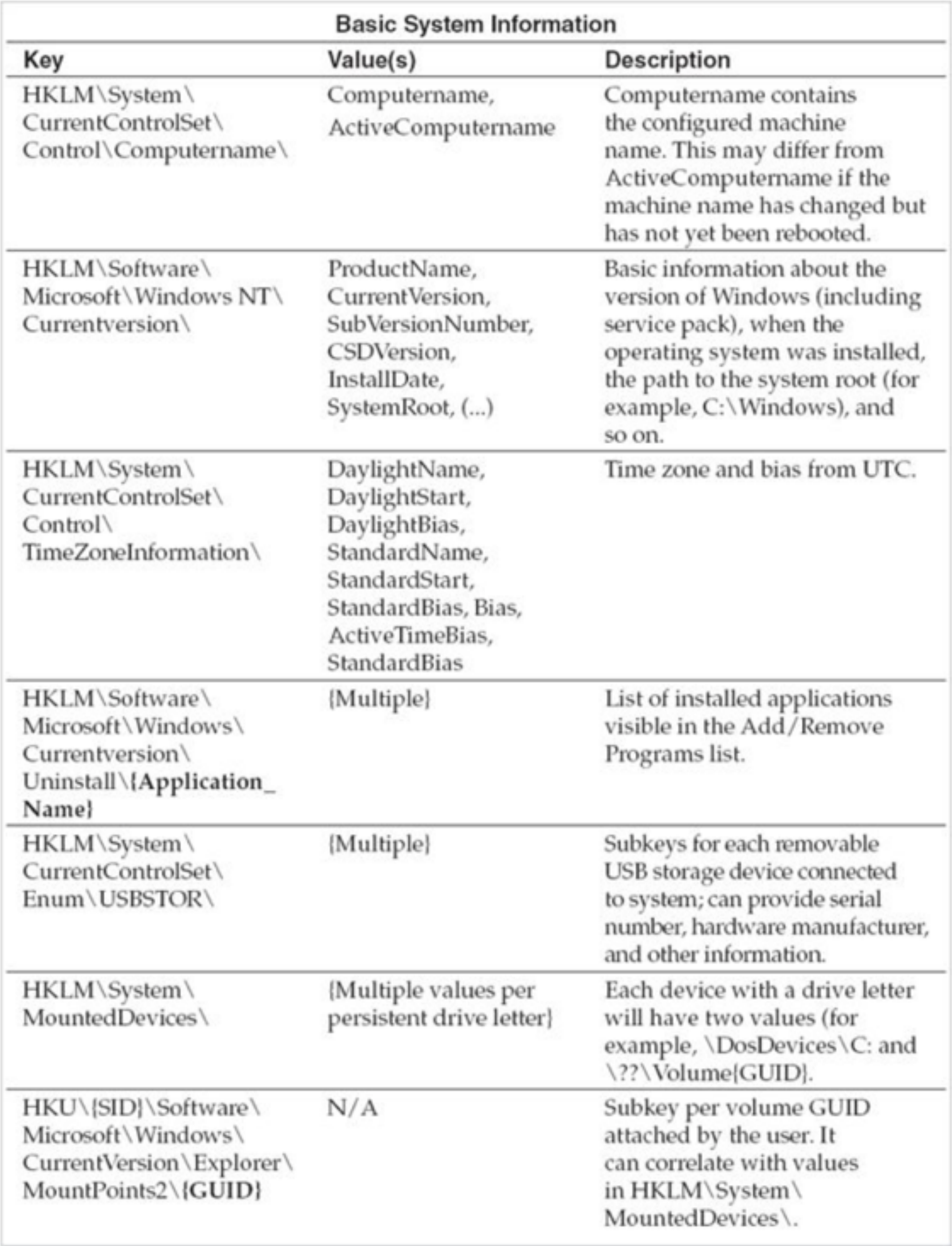
- **64-bit Windows allows 32-bit software to run**
- **32-bit programs are redirected by the W0W64 sybsystem to alternate registry keys, like**
  - **HKLM\SOFTWARE\WoW6432Node**
- **This means 32-bit forensic software won't see the whole Registry**

Important Registry Keys



- System Configuration Registry Keys
- Shim Cache
- Common Auto-Run Registry Keys
- User Hive Registry Keys

System Configuration Registry Keys



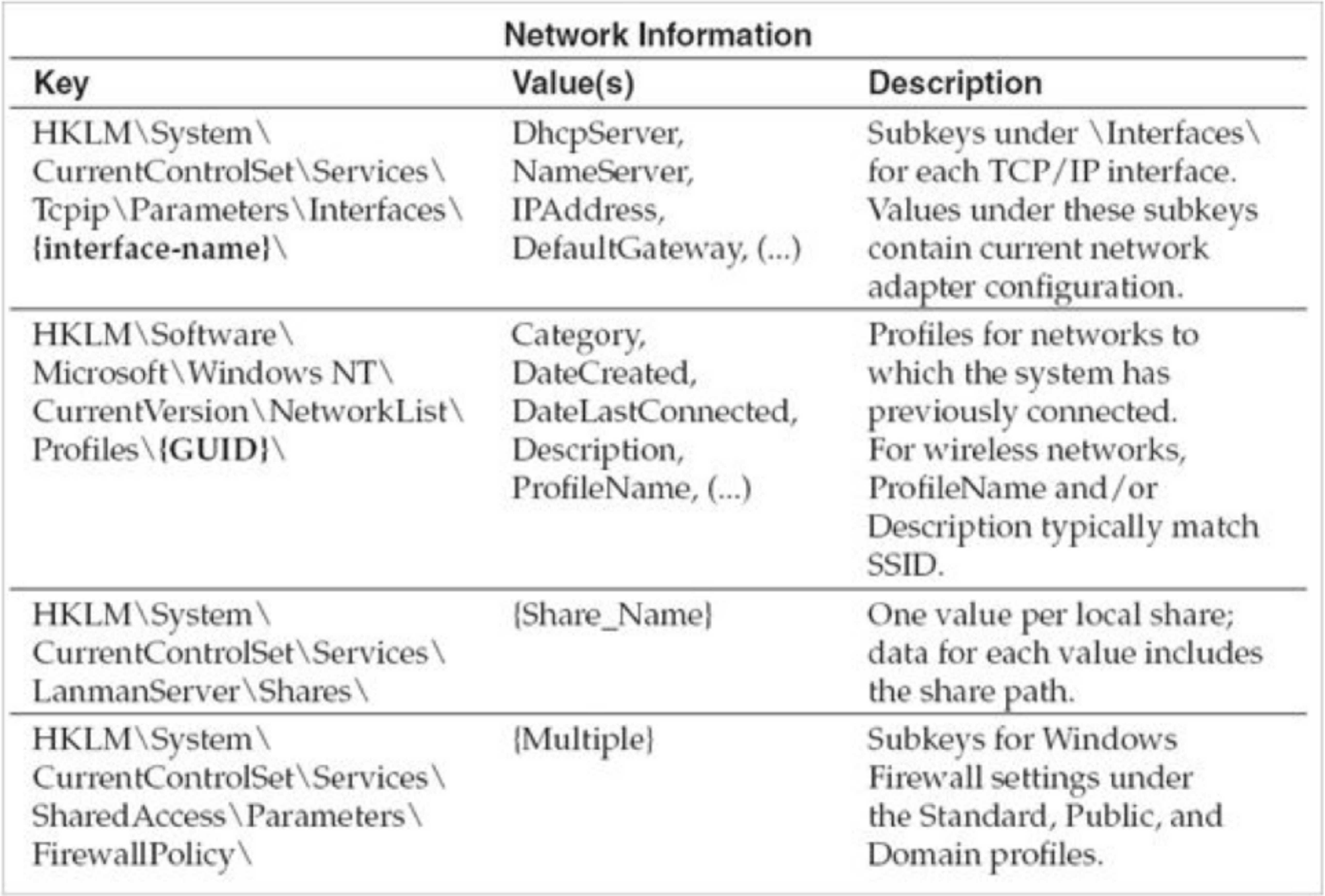
Basic System Information

Key	Value(s)	Description
HKLM\System\CurrentControlSet\Control\Computername\	Computername, ActiveComputername	Computername contains the configured machine name. This may differ from ActiveComputername if the machine name has changed but has not yet been rebooted.
HKLM\Software\Microsoft\Windows NT\Currentversion\	ProductName, CurrentVersion, SubVersionNumber, CSDVersion, InstallDate, SystemRoot, (...)	Basic information about the version of Windows (including service pack), when the operating system was installed, the path to the system root (for example, C:\Windows), and so on.
HKLM\System\CurrentControlSet\Control\TimeZoneInformation\	DaylightName, DaylightStart, DaylightBias, StandardName, StandardStart, StandardBias, Bias, ActiveTimeBias, StandardBias	Time zone and bias from UTC.
HKLM\Software\Microsoft\Windows\Currentversion\Uninstall\**{Application_Name}**	{Multiple}	List of installed applications visible in the Add/Remove Programs list.
HKLM\System\CurrentControlSet\Enum\USBSTOR\	{Multiple}	Subkeys for each removable USB storage device connected to system; can provide serial number, hardware manufacturer, and other information.
HKLM\System\MountedDevices\	{Multiple values per persistent drive letter}	Each device with a drive letter will have two values (for example, \DosDevices\C: and \??\Volume{GUID}.
HKU\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\**{GUID}**	N/A	Subkey per volume GUID attached by the user. It can correlate with values in HKLM\System\MountedDevices\.

USBSTOR

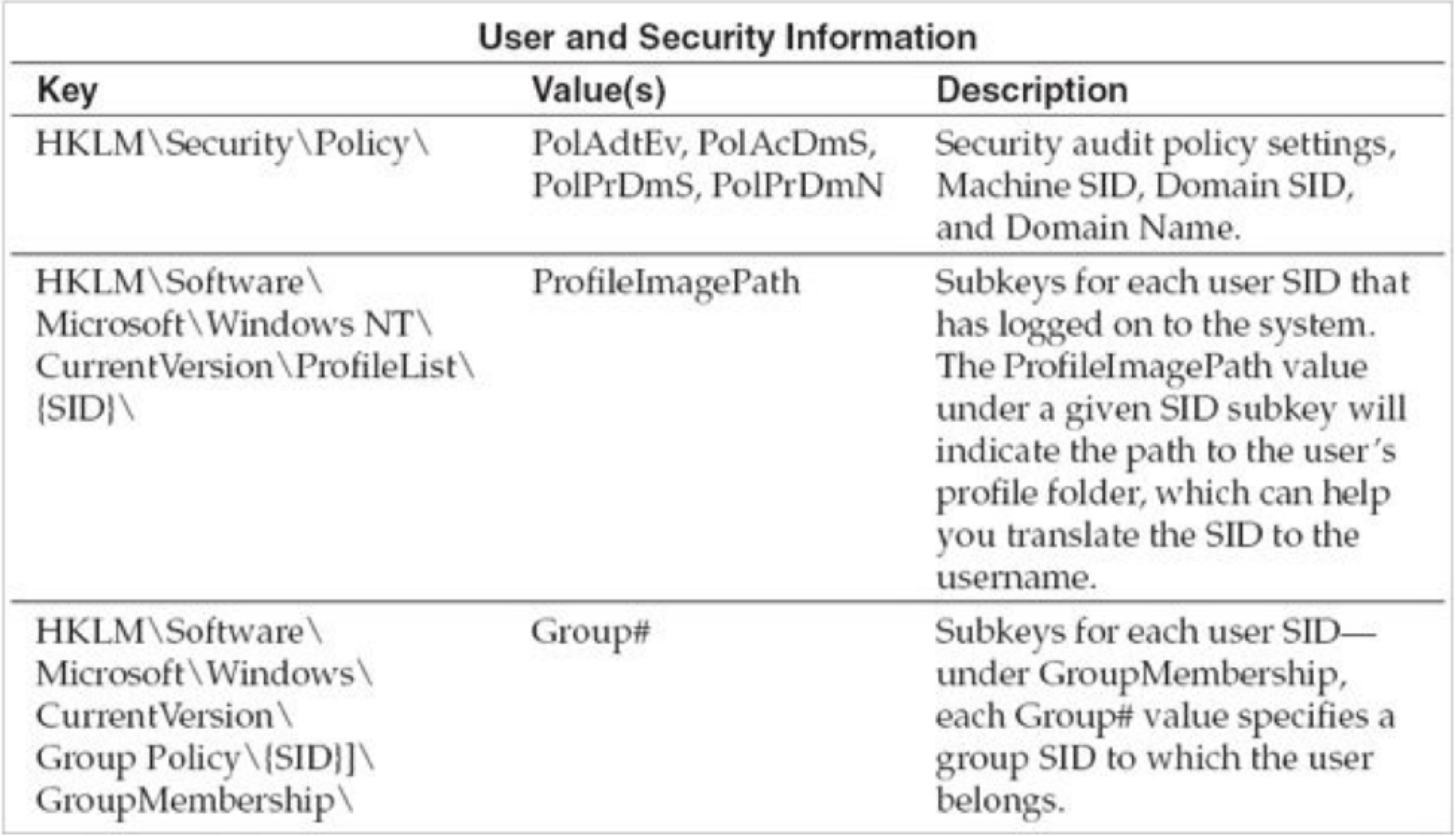
- **Shows every USB device that has been connected**

- **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

Key	Value(s)	Description
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\ **{interface-name}**\	DhcpServer, NameServer, IPAddress, DefaultGateway, (...)	Subkeys under \Interfaces\ for each TCP/IP interface. Values under these subkeys contain current network adapter configuration.
HKLM\Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\ **{GUID}**\	Category, DateCreated, DateLastConnected, Description, ProfileName, (...)	Profiles for networks to which the system has previously connected. For wireless networks, ProfileName and/or Description typically match SSID.
HKLM\System\CurrentControlSet\Services\LanmanServer\Shares\	{Share_Name}	One value per local share; data for each value includes the share path.
HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\	{Multiple}	Subkeys for Windows Firewall settings under the Standard, Public, and Domain profiles.



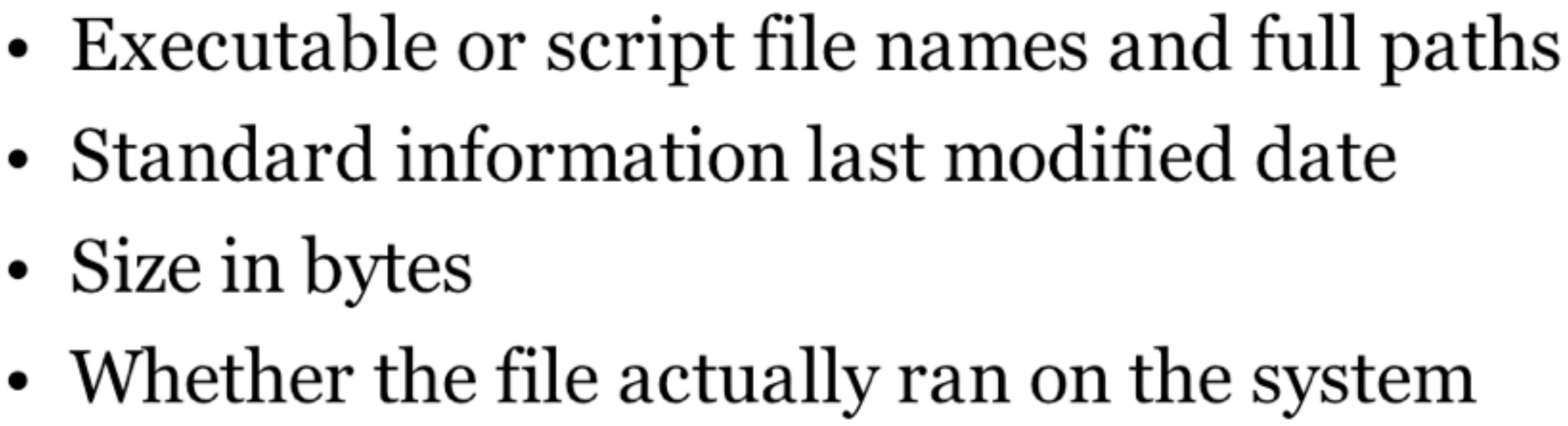
User and Security Information

Key	Value(s)	Description
HKLM\Security\Policy\	PolAdtEv, PolAcDmS, PolPrDmS, PolPrDmN	Security audit policy settings, Machine SID, Domain SID, and Domain Name.
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\{SID}\	ProfileImagePath	Subkeys for each user SID that has logged on to the system. The ProfileImagePath value under a given SID subkey will indicate the path to the user's profile folder, which can help you translate the SID to the username.
HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\{SID}]\GroupMembership\	Group#	Subkeys for each user SID—under GroupMembership, each Group# value specifies a group SID to which the user belongs.

Shim Cache

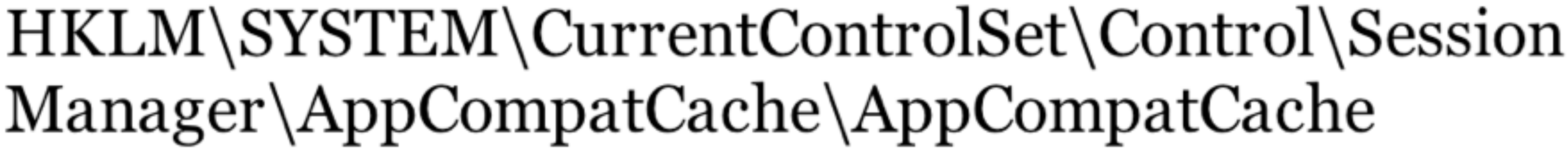
Shim Cache

- **Also called "Application Compatibility Cache"**
- **Used to track special compatibility settings for executable files and scripts**
- **May include this data:**



- Executable or script file names and full paths
- Standard information last modified date
- Size in bytes
- Whether the file actually ran on the system

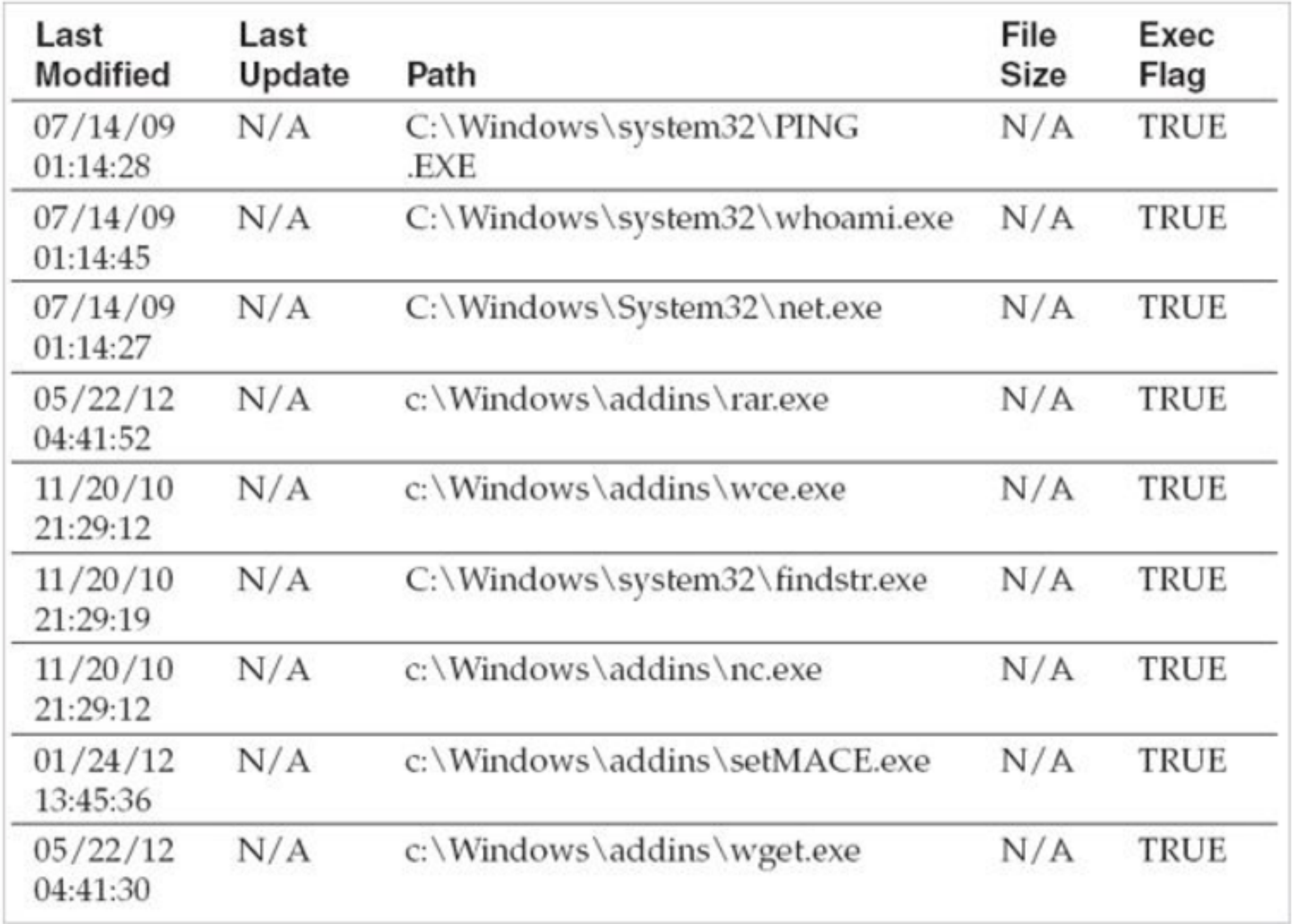
Shim Cache



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**

ShimParser.py



Last Modified	Last Update	Path	File Size	Exec Flag
07/14/09 01:14:28	N/A	C:\Windows\system32\PING .EXE	N/A	TRUE
07/14/09 01:14:45	N/A	C:\Windows\system32\whoami.exe	N/A	TRUE
07/14/09 01:14:27	N/A	C:\Windows\System32\net.exe	N/A	TRUE
05/22/12 04:41:52	N/A	c:\Windows\addins\rar.exe	N/A	TRUE
11/20/10 21:29:12	N/A	c:\Windows\addins\wce.exe	N/A	TRUE
11/20/10 21:29:19	N/A	C:\Windows\system32\findstr.exe	N/A	TRUE
11/20/10 21:29:12	N/A	c:\Windows\addins\nc.exe	N/A	TRUE
01/24/12 13:45:36	N/A	c:\Windows\addins\setMACE.exe	N/A	TRUE
05/22/12 04:41:30	N/A	c:\Windows\addins\wget.exe	N/A	TRUE

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

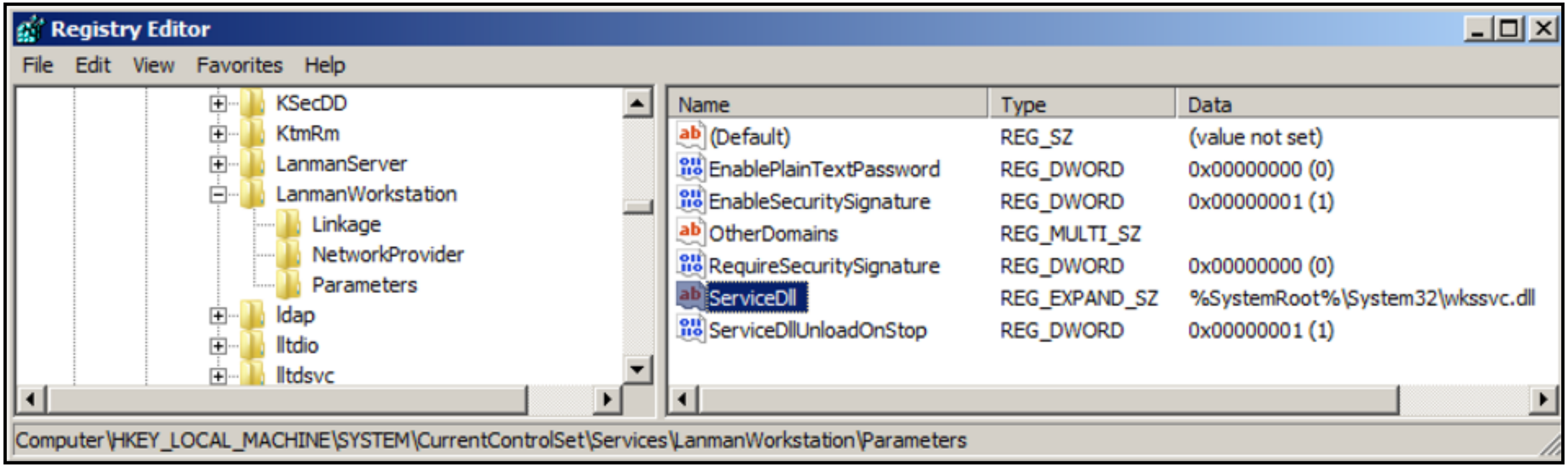
- **Each service has its own subkey under**
- **HKLM\CurrentControlSet\services\*servicename***

- **DisplayName** A “long-form” descriptive name for the service. Can be up to 256 characters and include spaces and mixed case.
- **Description** A comment that may describe the functionality or purpose of the service.
- **ImagePath** The path to the executable file (for a service) or .sys file (for a driver) to be executed.
- **Start** How and when the driver or service should be loaded. The data for this key is in the range 0–4. For most malware, this will be set to 2 (Automatic).
  - **0x0** Boot (by kernel loader—drivers only)
  - **0x1** System (by I/O subsystem during kernel initialization—drivers only)
  - **0x2** Automatic (by Service Control Manager upon startup—for services)
  - **0x3** Manual (user or application must explicitly request that the service be started)
  - **0x4** Disabled

- **Type** Specifies one of several service types, most commonly the following:
  - **0x1** Driver
  - **0x2** File system driver
  - **0x10** Service that runs in its own process
  - **0x20** Service that shares a process
- **DependOnGroup or DependOnService** Specifies other service groups and individual services that must start before the service can load and run.
- **Group** Specifies a group to which this service belongs. Services in the same group will start up together.

ServiceDLL

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



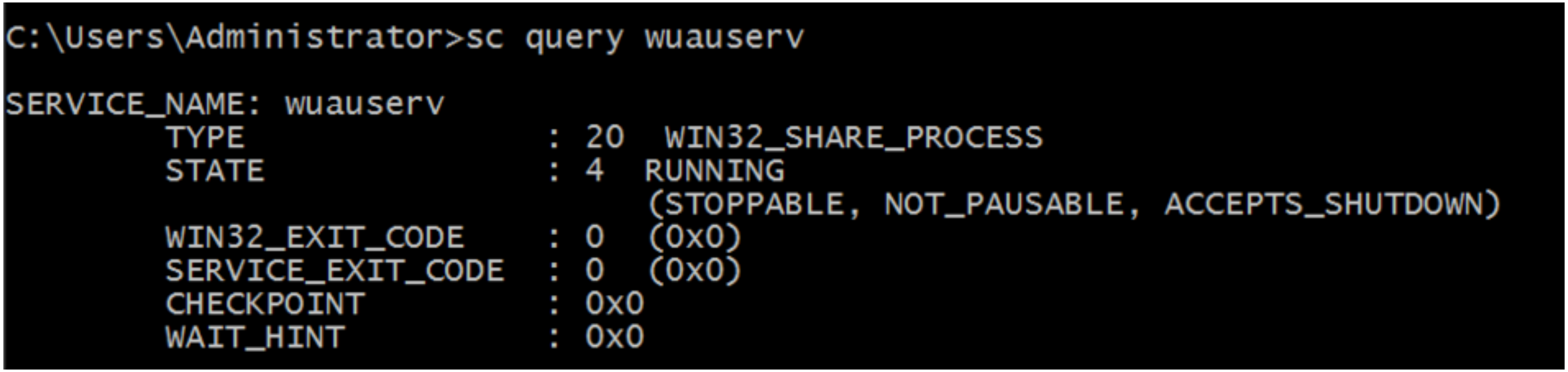
Name	Type	Data
(Default)	REG_SZ	(value not set)
EnablePlainTextPassword	REG_DWORD	0x00000000 (0)
EnableSecuritySignature	REG_DWORD	0x00000001 (1)
OtherDomains	REG_MULTI_SZ	
RequireSecuritySignature	REG_DWORD	0x00000000 (0)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\wkssvc.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters

Service Control Manager

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

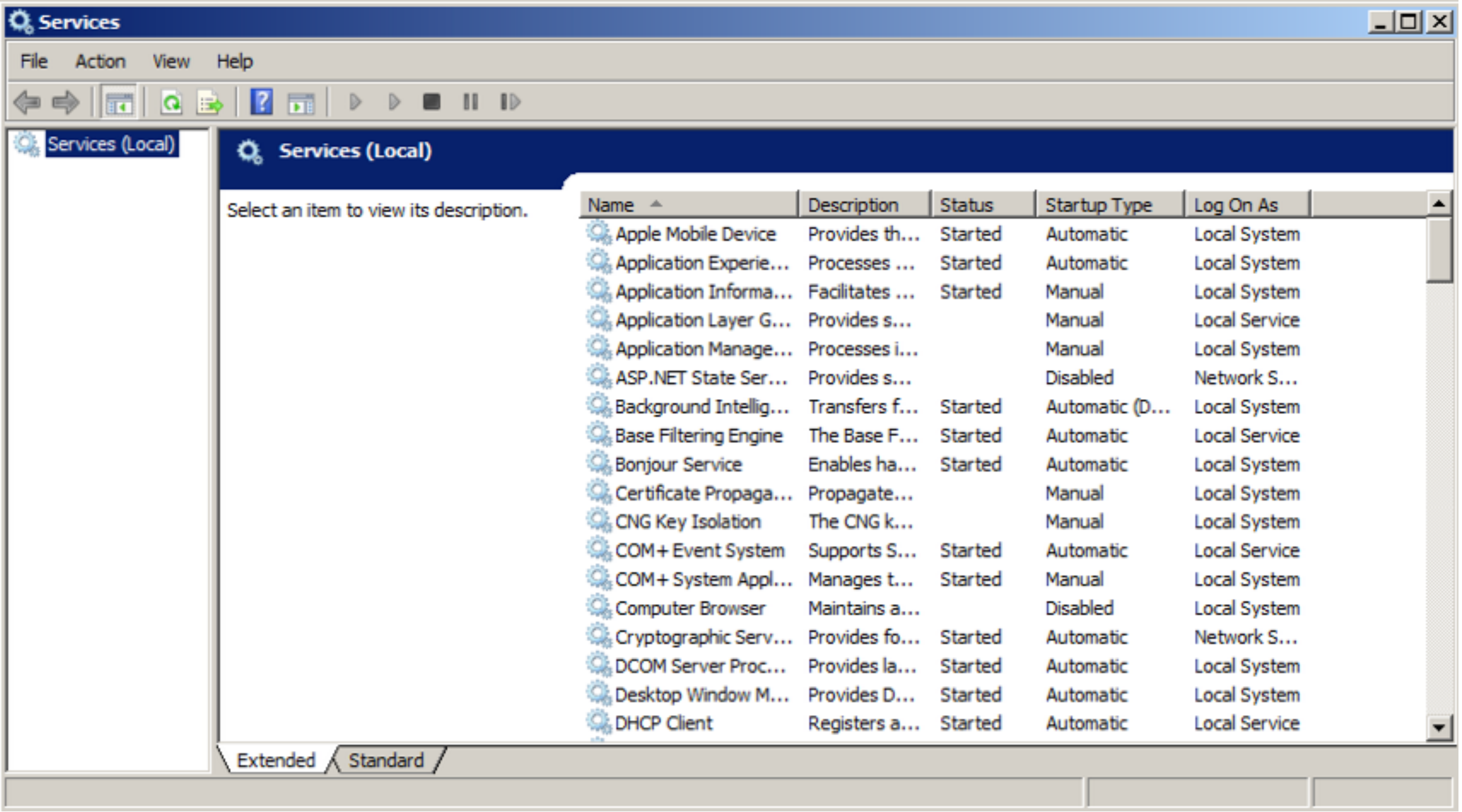
sc at Command line



```
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
```

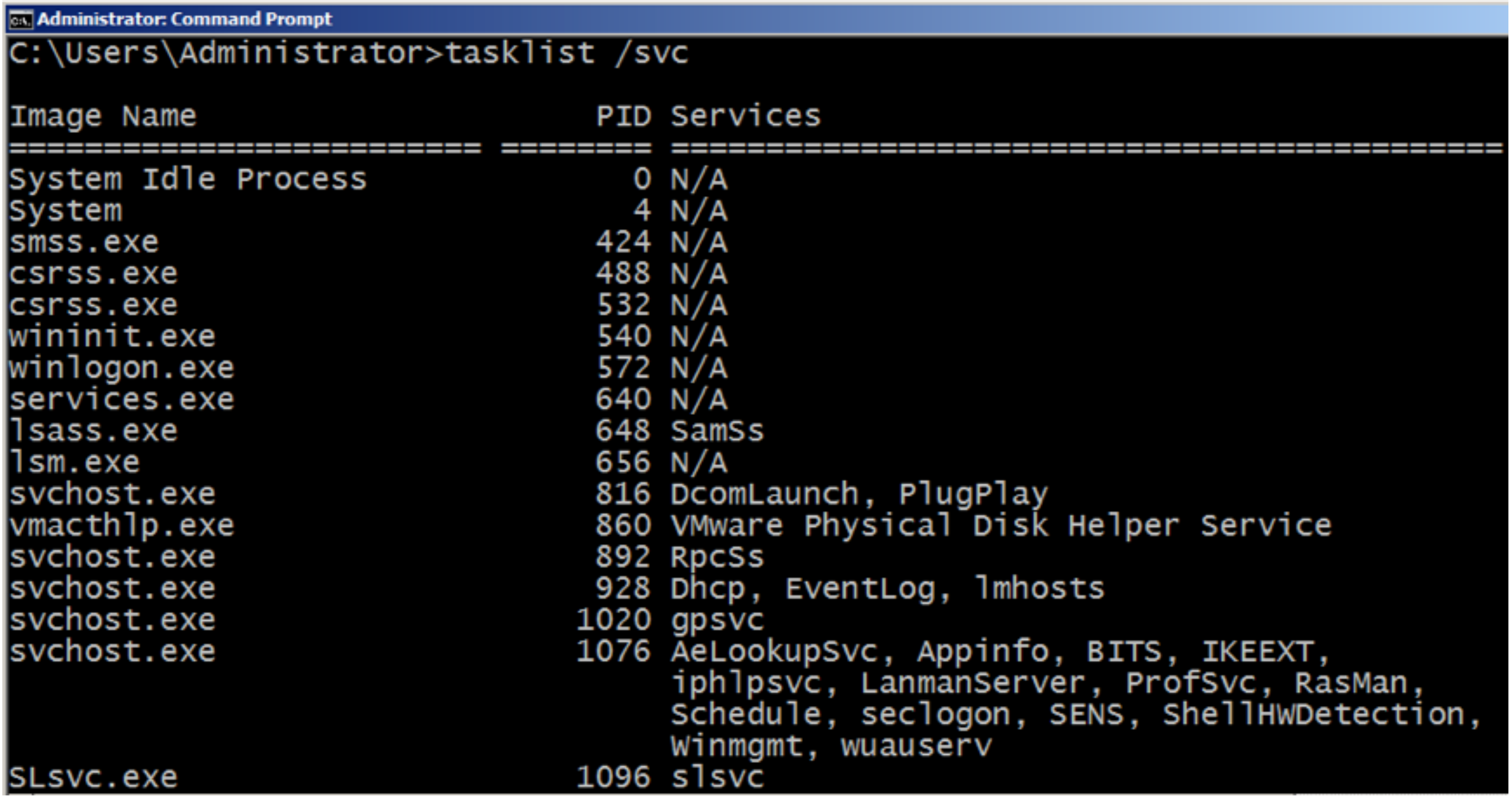
Services GUI



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Apple Mobile Device	Provides th...	Started	Automatic	Local System
Application Experie...	Processes ...	Started	Automatic	Local System
Application Informa...	Facilitates ...	Started	Manual	Local System
Application Layer G...	Provides s...		Manual	Local Service
Application Manage...	Processes i...		Manual	Local System
ASP.NET State Ser...	Provides s...		Disabled	Network S...
Background Intellig...	Transfers f...	Started	Automatic (D...	Local System
Base Filtering Engine	The Base F...	Started	Automatic	Local Service
Bonjour Service	Enables ha...	Started	Automatic	Local System
Certificate Propaga...	Propagate...		Manual	Local System
CNG Key Isolation	The CNG k...		Manual	Local System
COM+ Event System	Supports S...	Started	Automatic	Local Service
COM+ System Appl...	Manages t...	Started	Manual	Local System
Computer Browser	Maintains a...		Disabled	Local System
Cryptographic Serv...	Provides fo...	Started	Automatic	Network S...
DCOM Server Proc...	Provides la...	Started	Automatic	Local System
Desktop Window M...	Provides D...	Started	Automatic	Local System
DHCP Client	Registers a...	Started	Automatic	Local Service

One EXE Can Run Several Services

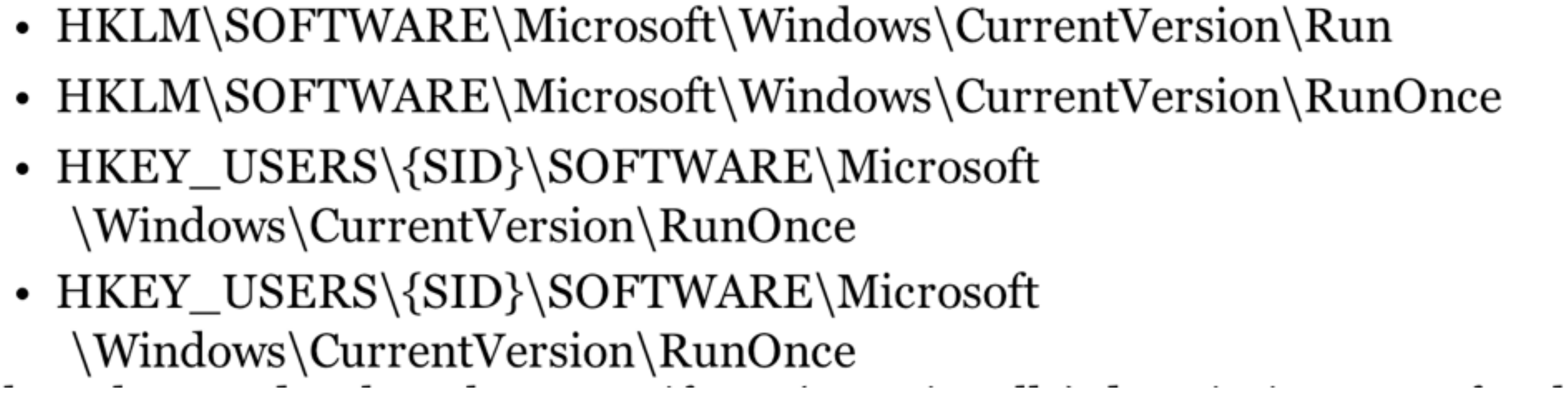


```
C:\Users\Administrator>tasklist /svc

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
```

Run Keys

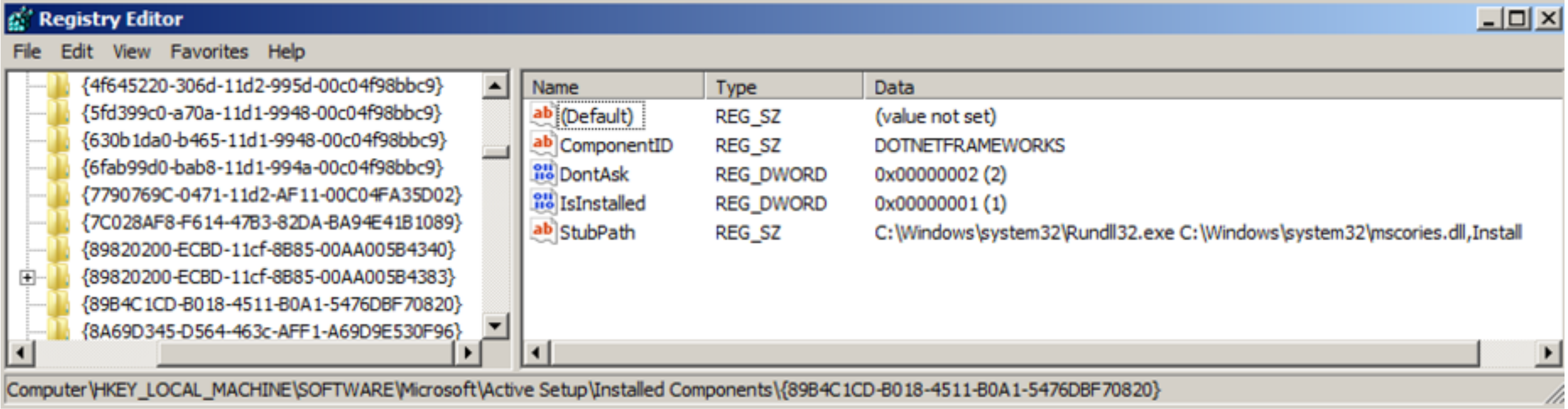
- **Files in HKLM\SOFTWARE run on startup**
- **Files in HKEY_USERS run on login**



- 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

- **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**



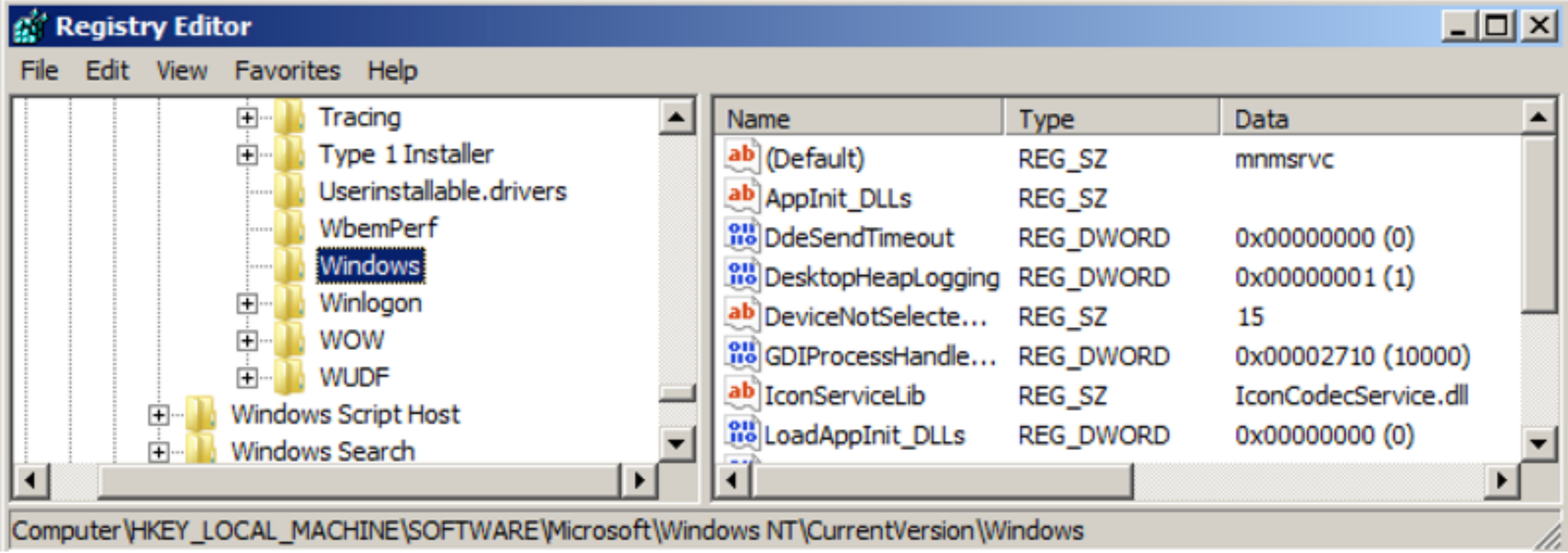
```
{4f645220-306d-11d2-995d-00c04f98bbc9}
{5fd399c0-a70a-11d1-9948-00c04f98bbc9}
{630b1da0-b465-11d1-9948-00c04f98bbc9}
{6fab99d0-bab8-11d1-994a-00c04f98bbc9}
{7790769C-0471-11d2-AF11-00C04FA35D02}
{7C028AF8-F614-47B3-82DA-BA94E41B1089}
{89820200-ECBD-11cf-8B85-00AA005B4340}
{89820200-ECBD-11cf-8B85-00AA005B4383}
{89B4C1CD-B018-4511-B0A1-5476DBF70820}
{8A69D345-D564-463c-AFF1-A69D9E530F96}
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
ComponentID	REG_SZ	DOTNETFRAMEWORKS
DontAsk	REG_DWORD	0x00000002 (2)
IsInstalled	REG_DWORD	0x00000001 (1)
StubPath	REG_SZ	C:\Windows\system32\Rundll32.exe C:\Windows\system32\mscories.dll,Install

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{89B4C1CD-B018-4511-B0A1-5476DBF70820}

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)**

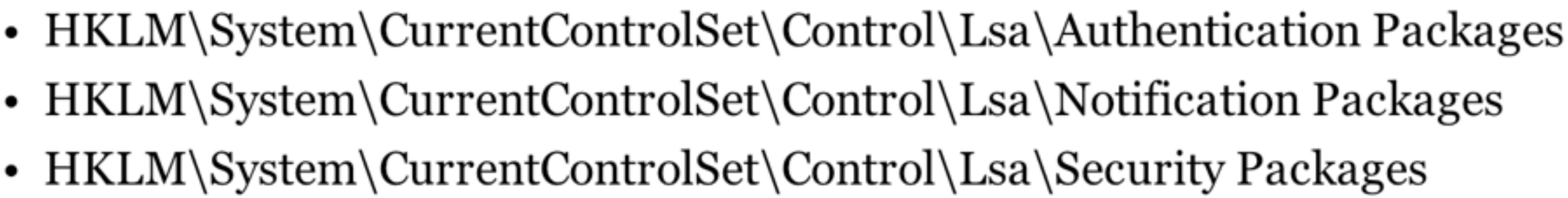


Name	Type	Data
(Default)	REG_SZ	mnmsrvc
AppInit_DLLs	REG_SZ	
DdeSendTimeout	REG_DWORD	0x00000000 (0)
DesktopHeapLogging	REG_DWORD	0x00000001 (1)
DeviceNotSelecte...	REG_SZ	15
GDIProcessHandle...	REG_DWORD	0x00002710 (10000)
IconServiceLib	REG_SZ	IconCodecService.dll
LoadAppInit_DLLs	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

LSA (Local Security Authority) Packages

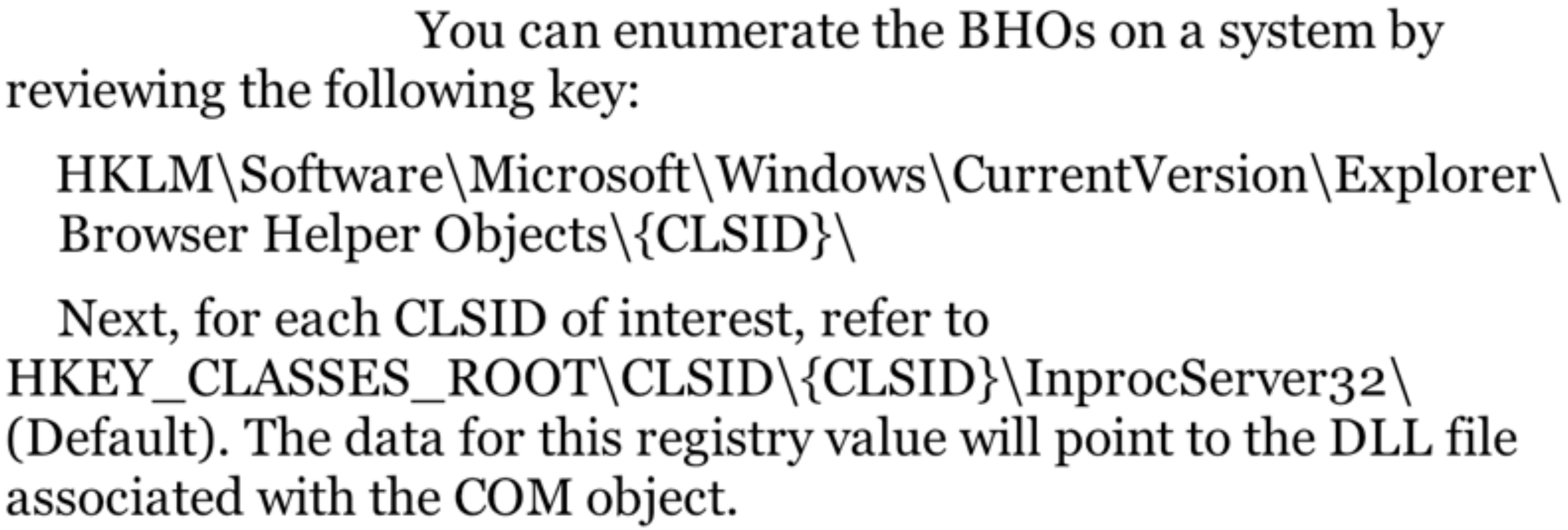
- **Load on startup**
- **Intended for authentication packages, but can be used to launch malware**



- 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**



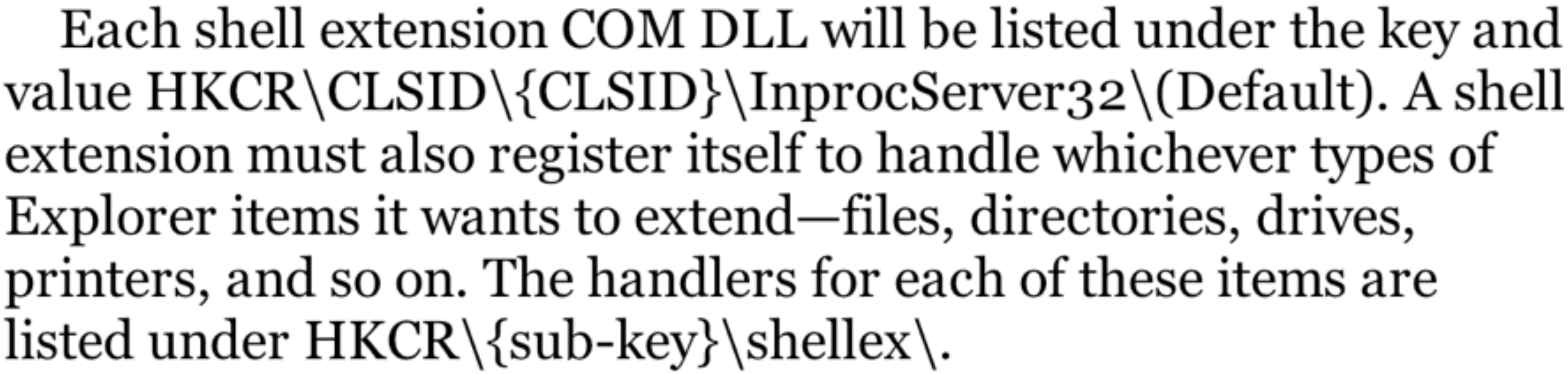
You can enumerate the BHOs on a system by reviewing the following key:

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

Next, for each CLSID of interest, refer to HKEY_CLASSES_ROOT\CLSID\{CLSID}\InprocServer32\(Default). The data for this registry value will point to the DLL file associated with the COM object.

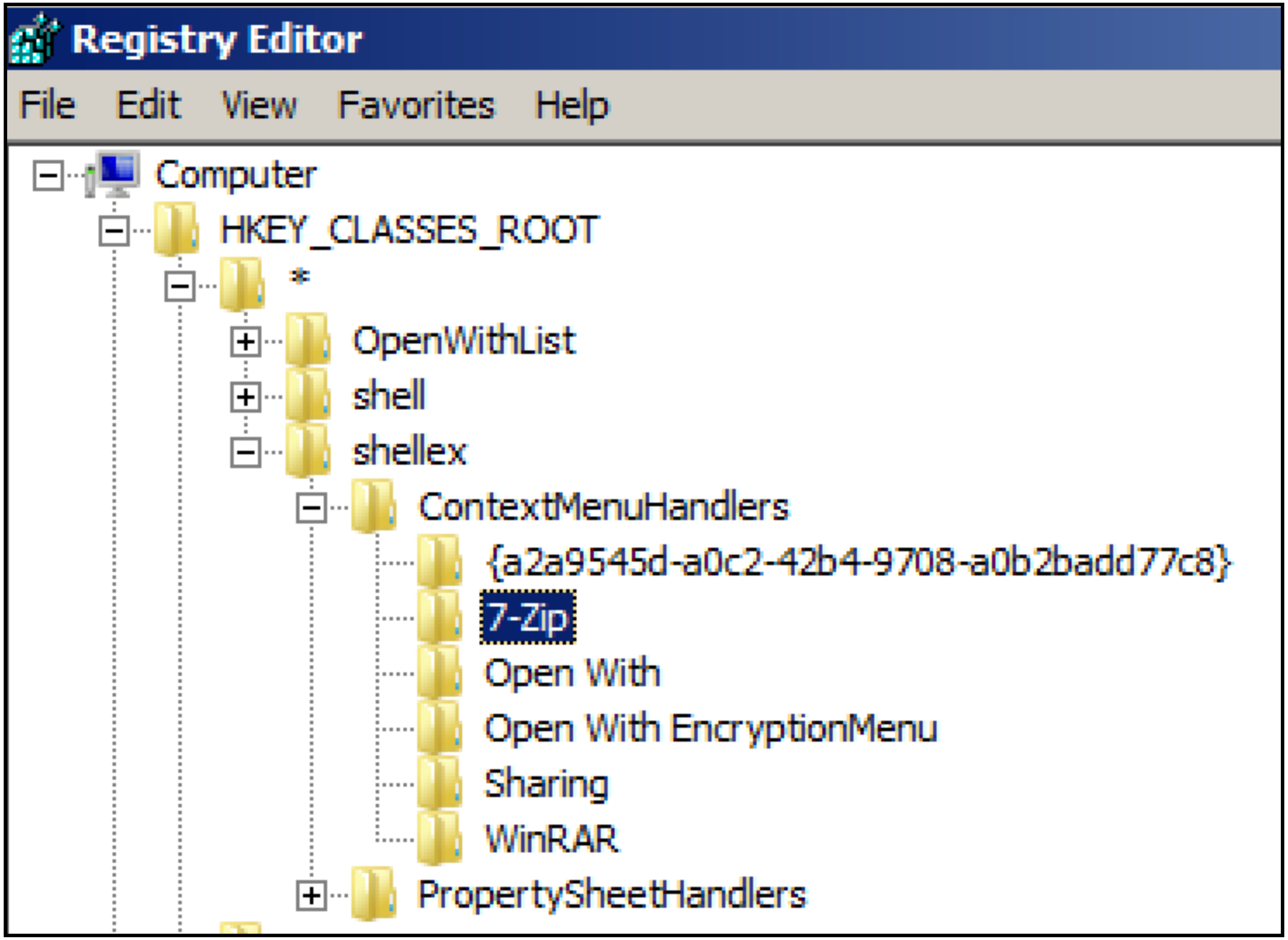
Shell Extensions

- **Like Browser Helper Objects, but for Windows Explorer**
- **Add context items when right-clicking a file**



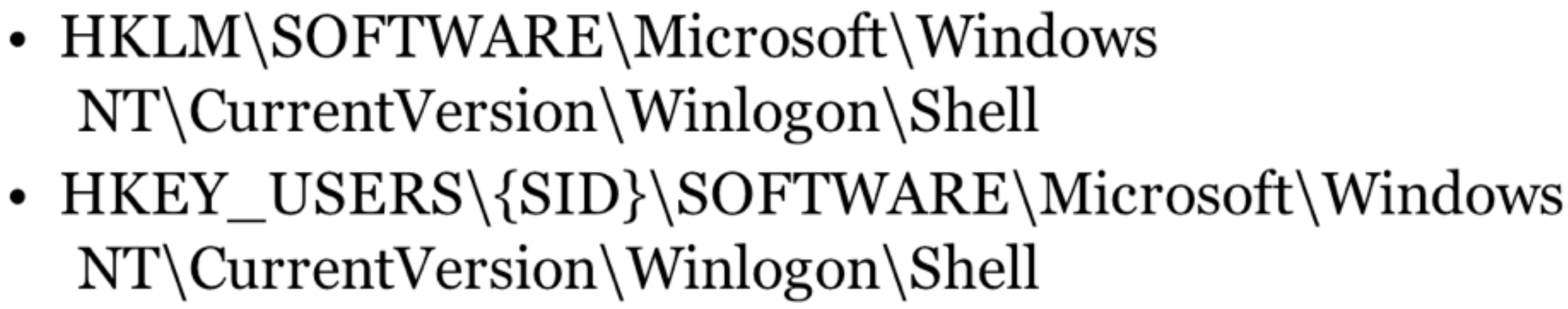
Each shell extension COM DLL will be listed under the key and value HKCR\CLSID\{CLSID}\InprocServer32\(Default). A shell extension must also register itself to handle whichever types of Explorer items it wants to extend—files, directories, drives, printers, and so on. The handlers for each of these items are listed under HKCR\{sub-key}\shellex\.

Shell Extensions



Winlogon Shell

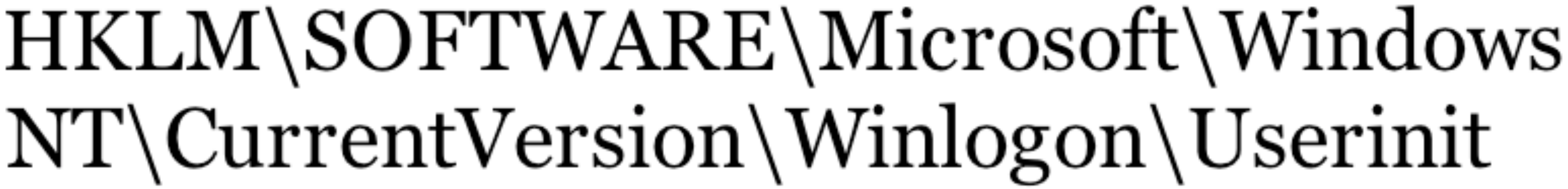
- **The shell that loads when user logs on**
- **Normally set to Explorer.exe**
- **Can be set to any executable file**



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

Winlogon Userinit

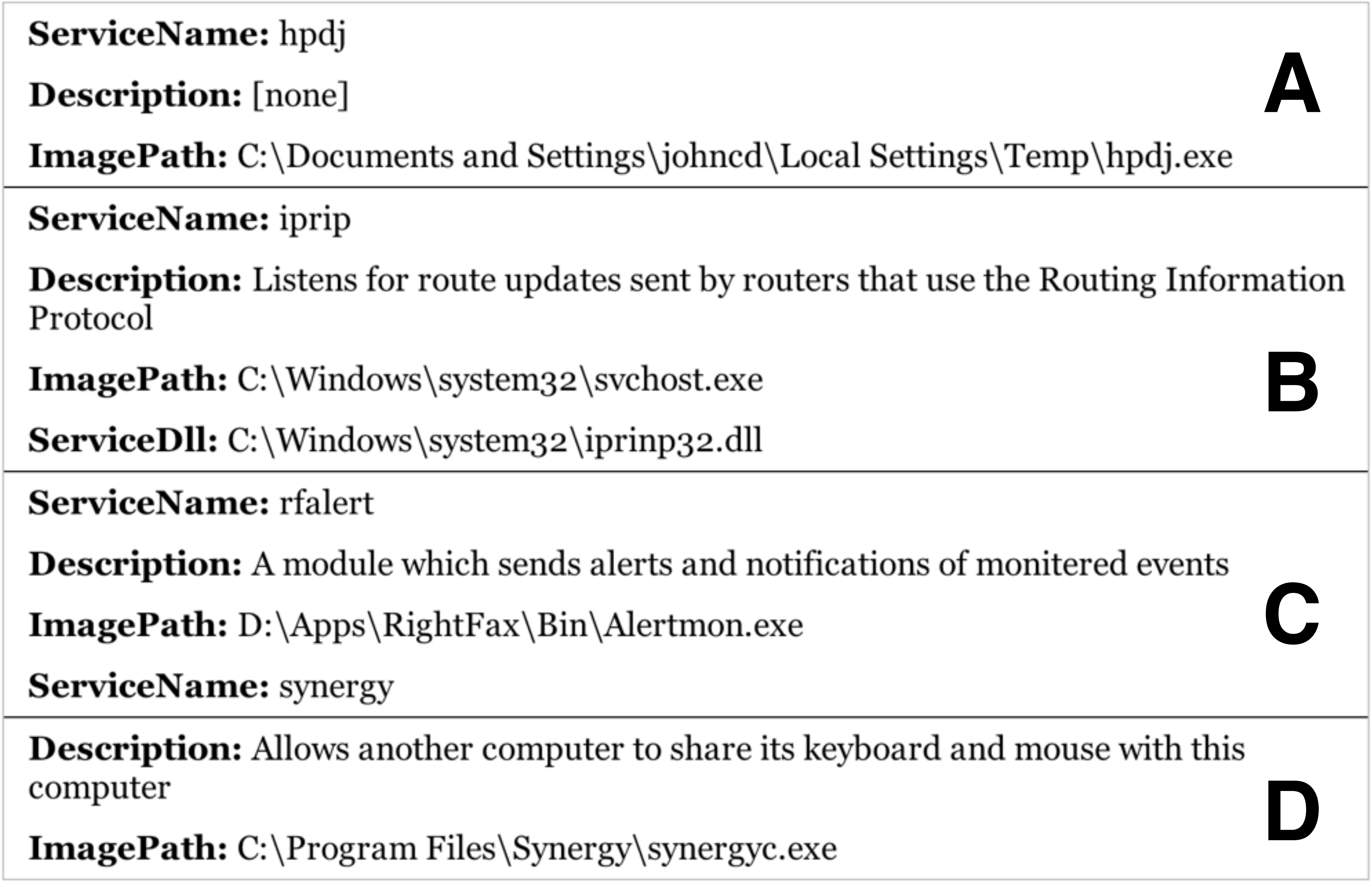
- **Loads logon and group policy scripts, other auto-runs, and the Explorer shell**
- **Attackers can append additional executables to this value**



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

Identifying Malicious Auto-Runs

- **Eye-ball 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

A

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

B

ServiceName: rfalert

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

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

ServiceName: synergy

C

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

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

D

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**

Tools

- **Sysinternals AutoRuns**
- **Mandiant Redline**

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**

User Hive Registry Keys

Personalization

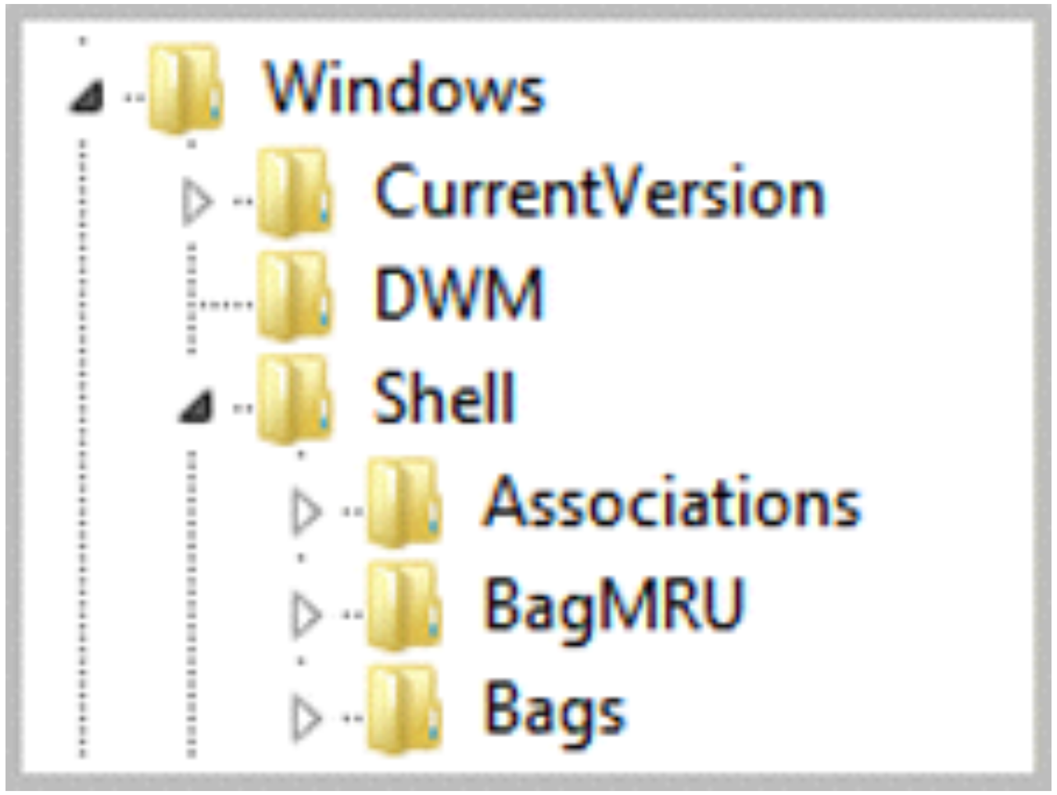
- **User hive registry keys contain personalization settings for each user**
- **First priority: compromised accounts**
  - **Acquire NTUSER.DAT and USRCLASS.DAT**
- **Check machine accounts, such as NetworkService and LocalSystem**
  - **May also contain evidence**

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**



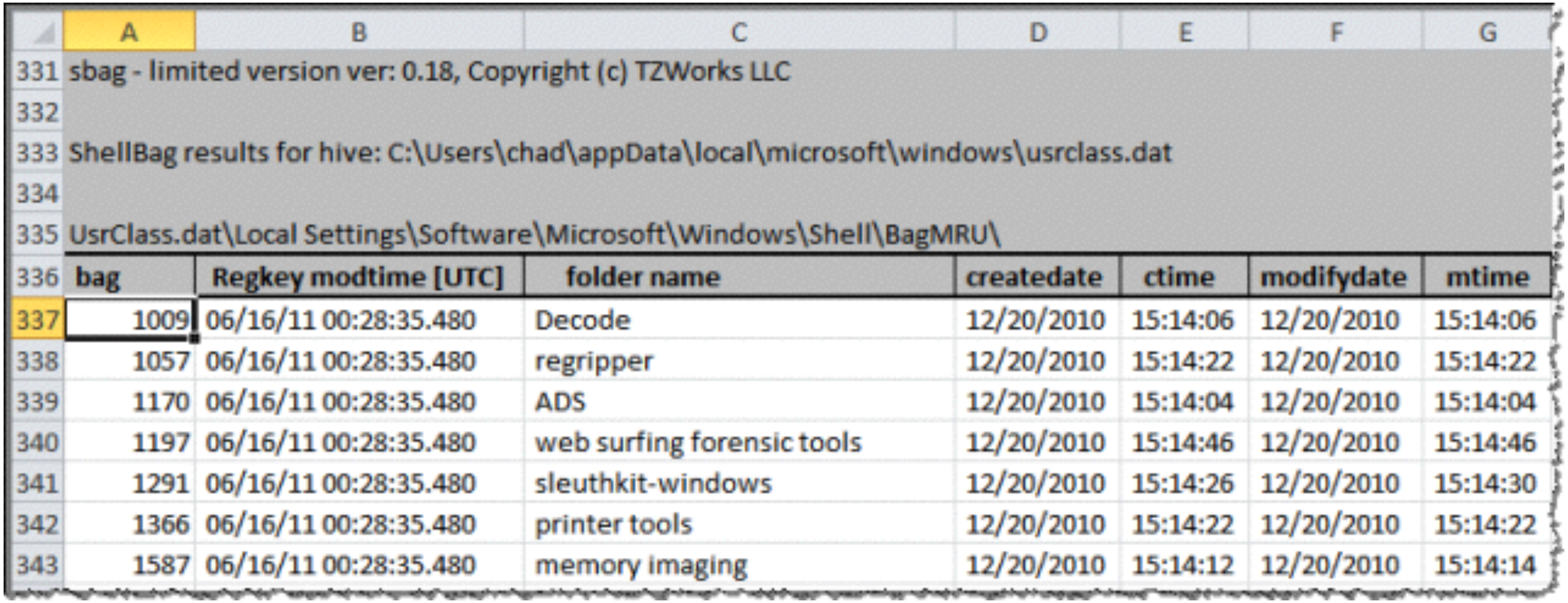
- Windows
  - CurrentVersion
  - DWM
  - Shell
    - Associations
    - BagMRU
    - Bags

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

Analyzing shellbag keys can provide an investigator with the following information:

- Full directory paths accessed via Explorer
- The date and time at which access to each path occurred, obtained by referencing the Last Modified time of the corresponding shellbag key, under certain circumstances (refer to the following note)
- The Modified, Accessed, and Created times of each path tracked in shellbags, recorded *as of the time at which the access occurred*

Example Shellbags

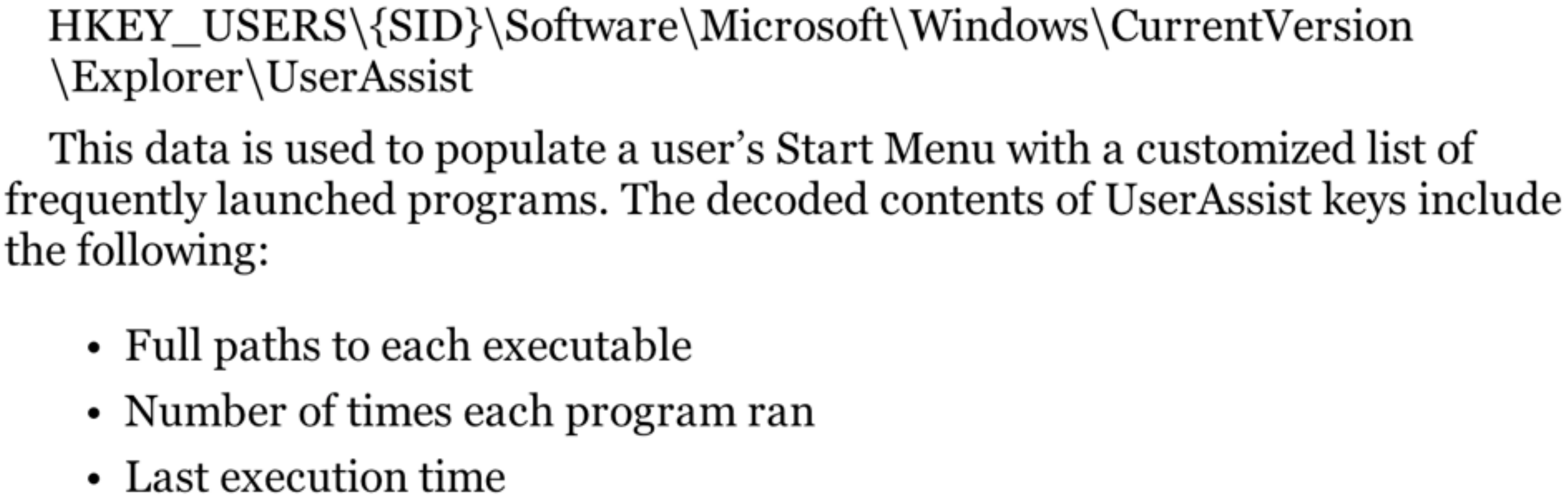


	A	B	C	D	E	F	G
331	sbag - limited version ver: 0.18, Copyright (c) TZWorks LLC						
332							
333	ShellBag results for hive: C:\Users\chad\appData\local\microsoft\windows\usrclass.dat						
334							
335	UsrClass.dat\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\						
336	bag	Regkey modtime [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

- **Link Ch 12q**

UserAssist

- **Tracks applications a user has launched through the Windows Explorer shell**



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

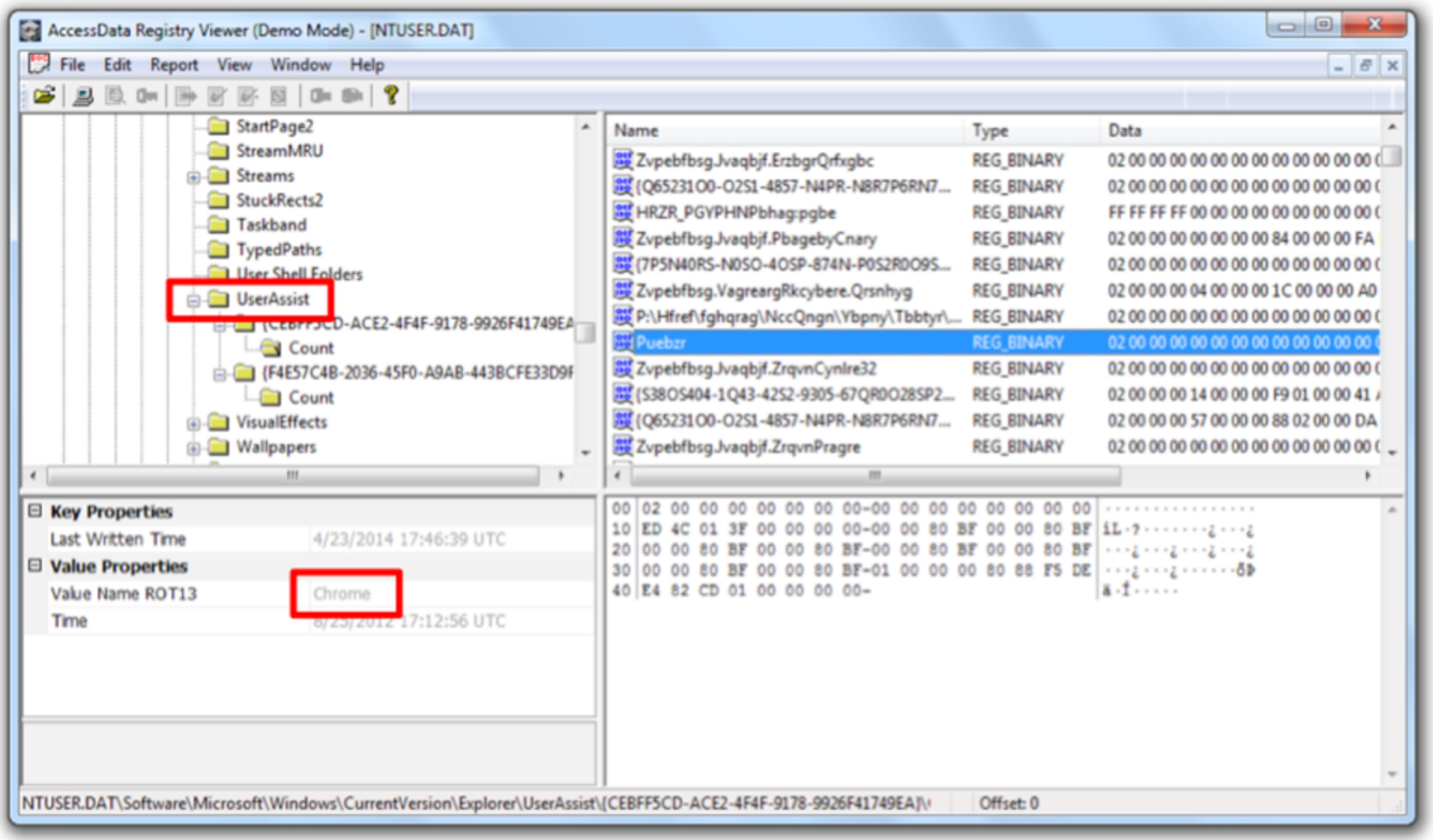
This data is used to populate a user's Start Menu with a customized list of frequently launched programs. The decoded contents of UserAssist keys include the following:

- 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



- StartPage2
- StreamMRU
- Streams
- StuckRects2
- Taskband
- TypedPaths
- User Shell Folders
- UserAssist
  - {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA
    - Count
  - {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F
    - Count
- VisualEffects
- Wallpapers

Name	Type	Data
Zvpebfbsg.Jvaqbjf.ErzbgrQrfxgbc	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00
{Q65231O0-O2S1-4857-N4PR-N8R7P6RN7...	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00
HRZR_PGYPHNPbhag:pgbe	REG_BINARY	FF FF FF FF 00 00 00 00 00 00 00 00
Zvpebfbsg.Jvaqbjf.PbagebyCnary	REG_BINARY	02 00 00 00 00 00 00 00 84 00 00 00 FA
{7P5N40RS-N0SO-4OSP-874N-P0S2R0O9S...	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00
Zvpebfbsg.VagreargRkcybere.Qrsnhyg	REG_BINARY	02 00 00 00 04 00 00 00 1C 00 00 00 A0
P:\Hfref\fghqrag\NccQngn\Ybpny\Tbbtyr\...	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00
Puebzr	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00
Zvpebfbsg.Jvaqbjf.ZrqvnCynlre32	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00
{S38OS404-1Q43-42S2-9305-67QR0O28SP2...	REG_BINARY	02 00 00 00 14 00 00 00 F9 01 00 00 41
{Q65231O0-O2S1-4857-N4PR-N8R7P6RN7...	REG_BINARY	02 00 00 00 57 00 00 00 88 02 00 00 DA
Zvpebfbsg.Jvaqbjf.ZrqvnPragre	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00

Key Properties

Last Written Time	4/23/2014 17:46:39 UTC

Value Properties

Value Name ROT13	Chrome
Time	8/23/2012 17:12:56 UTC

```
00  02 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
10  ED 4C 01 3F 00 00 00 00-00 00 80 BF 00 00 80 BF  íL·?·······¿···¿
20  00 00 80 BF 00 00 80 BF-00 00 80 BF 00 00 80 BF  ···¿···¿···¿···¿
30  00 00 80 BF 00 00 80 BF-01 00 00 00 80 88 F5 DE  ···¿···¿······õÞ
40  E4 82 CD 01 00 00 00 00-                          ä·Í·····
```

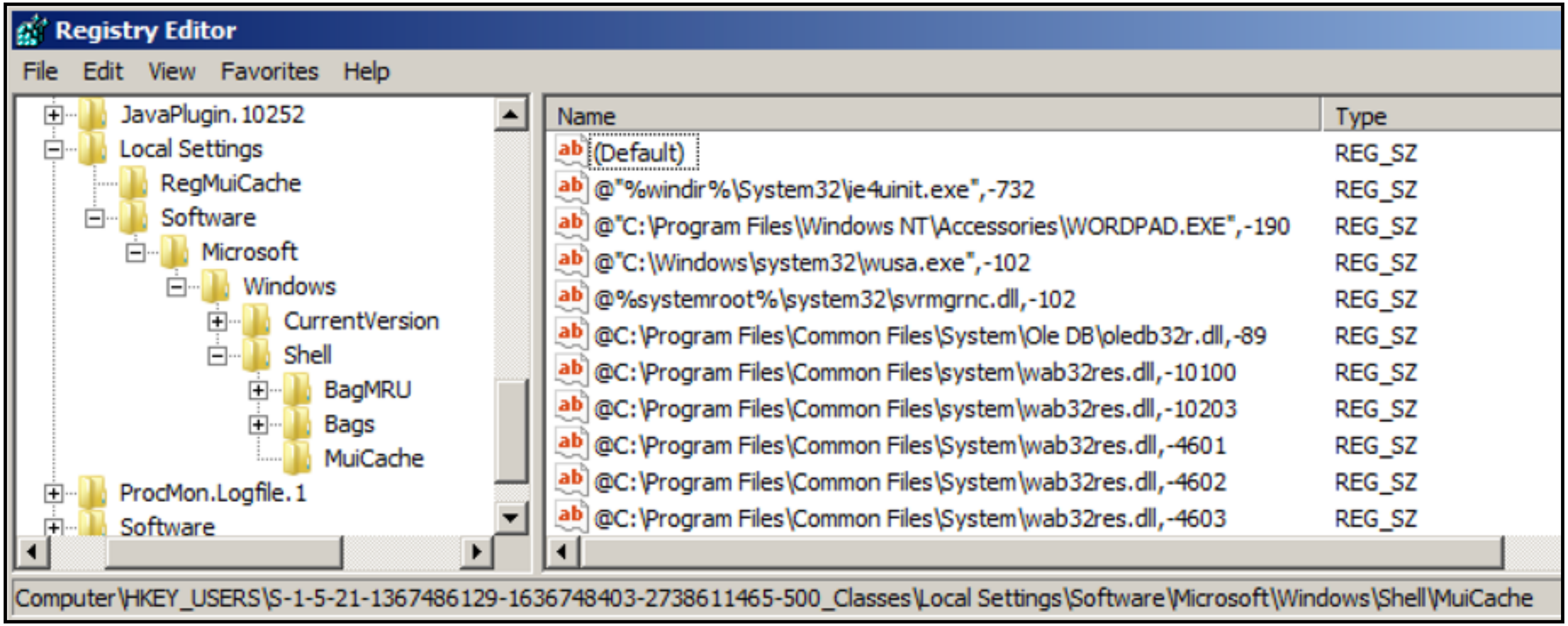
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\

Offset: 0

MUICache

- **Another list of programs executed by a user**

- **Windows Vista, 7, Server 2008** HKEY_USERS\{SID}_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache



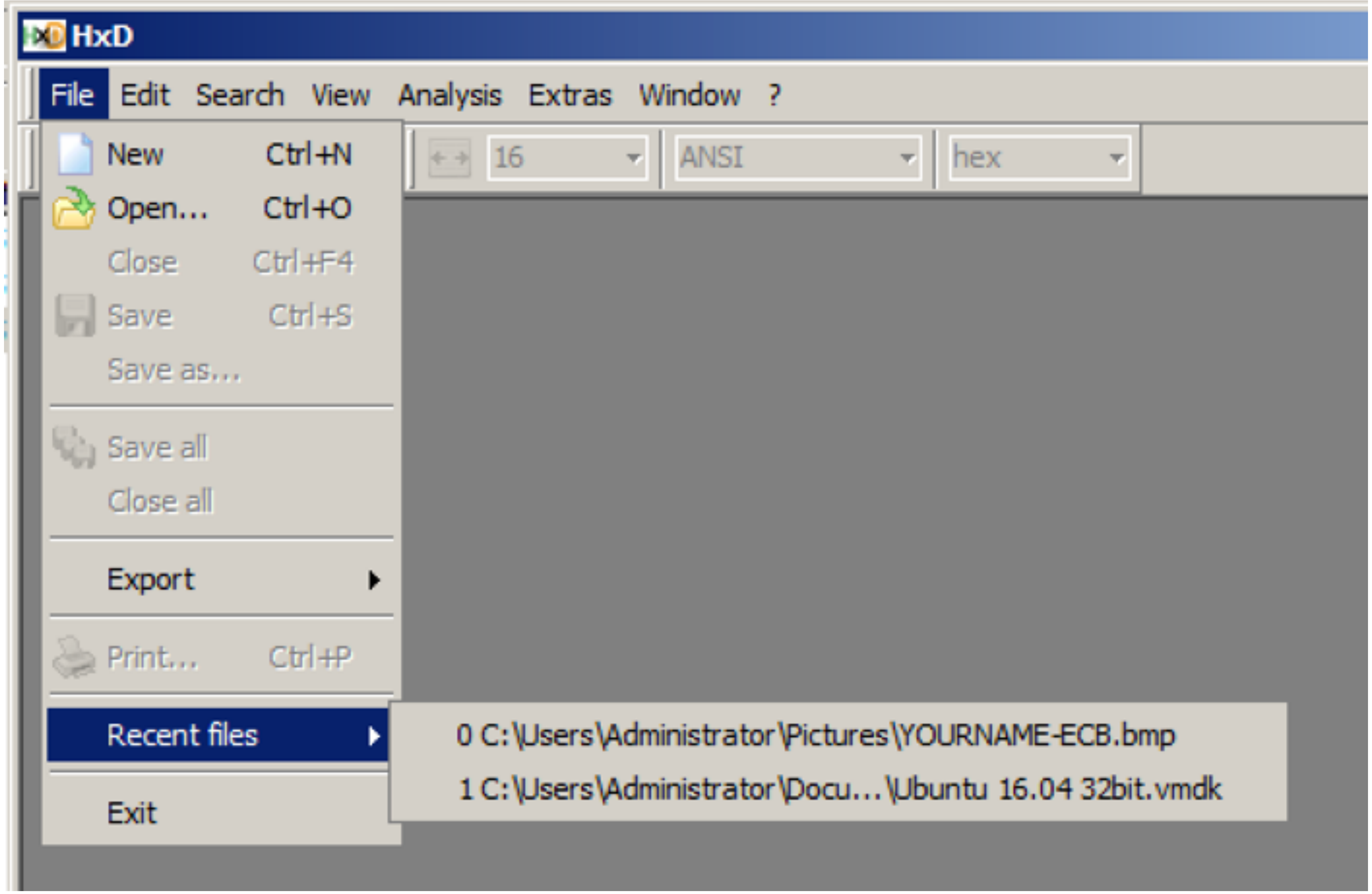
Name	Type
(Default)	REG_SZ
@"%windir%\System32\ie4uinit.exe",-732	REG_SZ
@"C:\Program Files\Windows NT\Accessories\WORDPAD.EXE",-190	REG_SZ
@"C:\Windows\system32\wusa.exe",-102	REG_SZ
@%systemroot%\system32\svrmgrnc.dll,-102	REG_SZ
@C:\Program Files\Common Files\System\Ole DB\oledb32r.dll,-89	REG_SZ
@C:\Program Files\Common Files\system\wab32res.dll,-10100	REG_SZ
@C:\Program Files\Common Files\system\wab32res.dll,-10203	REG_SZ
@C:\Program Files\Common Files\System\wab32res.dll,-4601	REG_SZ
@C:\Program Files\Common Files\System\wab32res.dll,-4602	REG_SZ
@C:\Program Files\Common Files\System\wab32res.dll,-4603	REG_SZ

Computer\HKEY_USERS\S-1-5-21-1367486129-1636748403-2738611465-500_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache

Most Recently Used (MRU) Keys

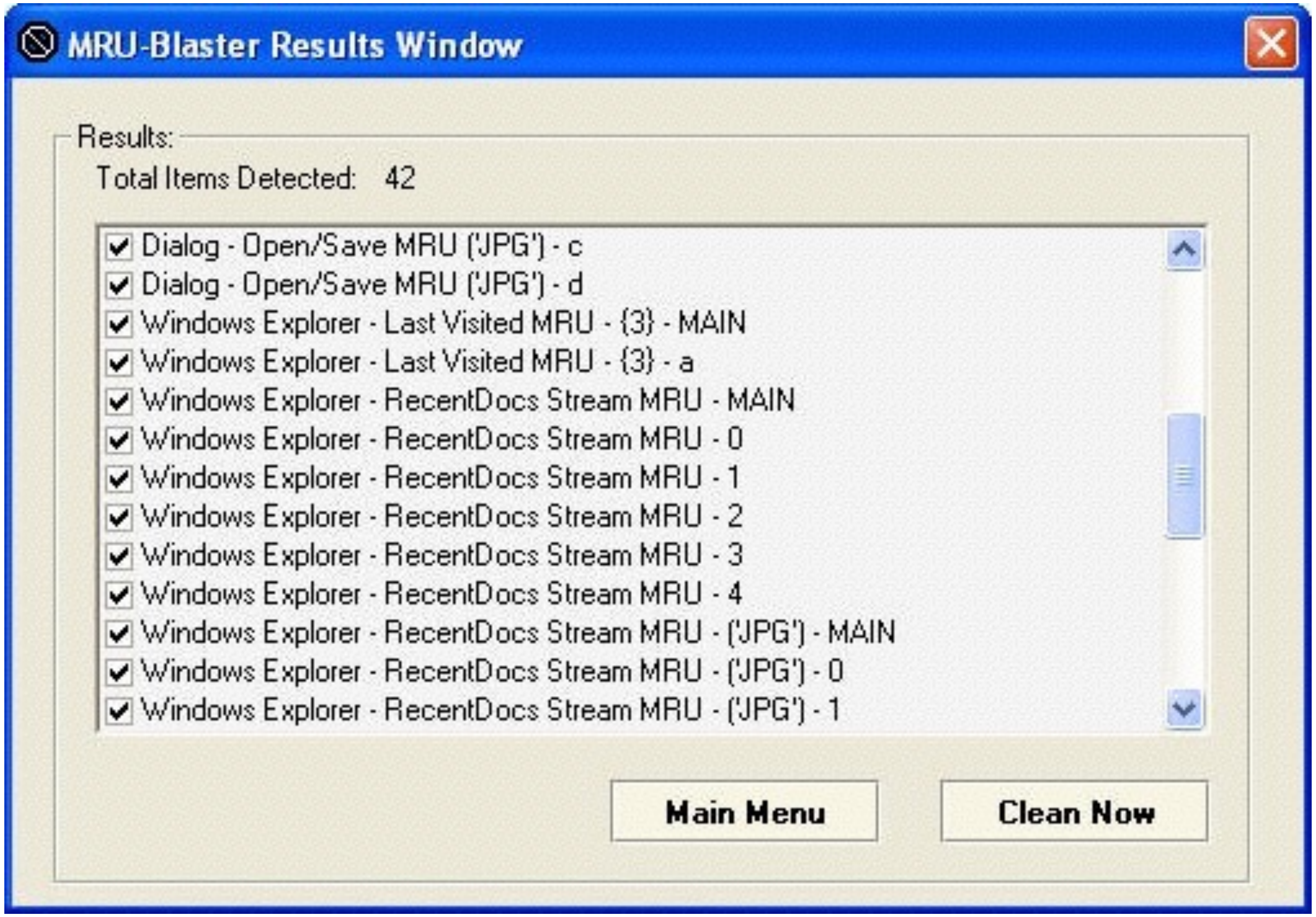
- **Used by many applications**

- **No standard registry path or value naming convention**



MRU-Blaster

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



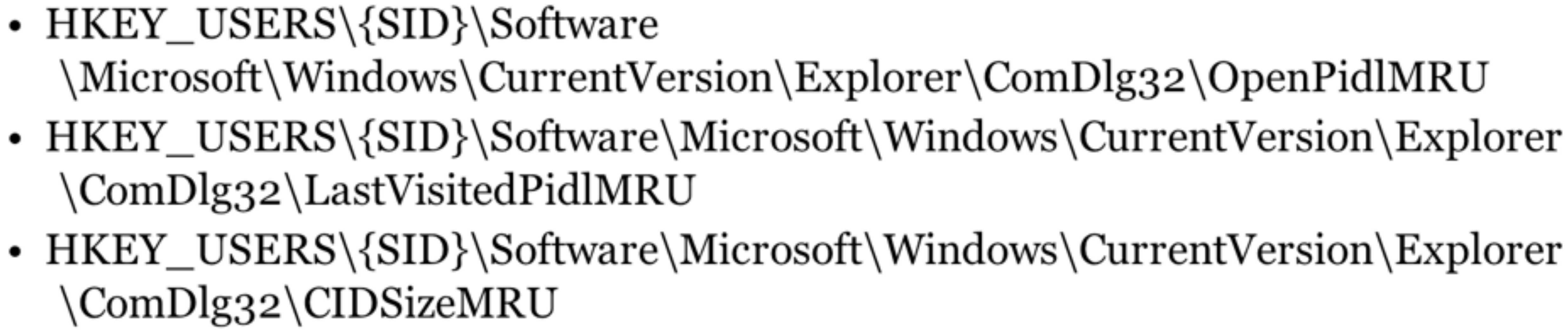
Results:

Total Items Detected: 42

☑ Dialog - Open/Save MRU ('JPG') - c
☑ Dialog - Open/Save MRU ('JPG') - d
☑ Windows Explorer - Last Visited MRU - {3} - MAIN
☑ Windows Explorer - Last Visited MRU - {3} - a
☑ Windows Explorer - RecentDocs Stream MRU - MAIN
☑ Windows Explorer - RecentDocs Stream MRU - 0
☑ Windows Explorer - RecentDocs Stream MRU - 1
☑ Windows Explorer - RecentDocs Stream MRU - 2
☑ Windows Explorer - RecentDocs Stream MRU - 3
☑ Windows Explorer - RecentDocs Stream MRU - 4
☑ Windows Explorer - RecentDocs Stream MRU - ('JPG') - MAIN
☑ Windows Explorer - RecentDocs Stream MRU - ('JPG') - 0
☑ Windows Explorer - RecentDocs Stream MRU - ('JPG') - 1

Explorer Open and Save MRU

- **RegRipper can find the data**

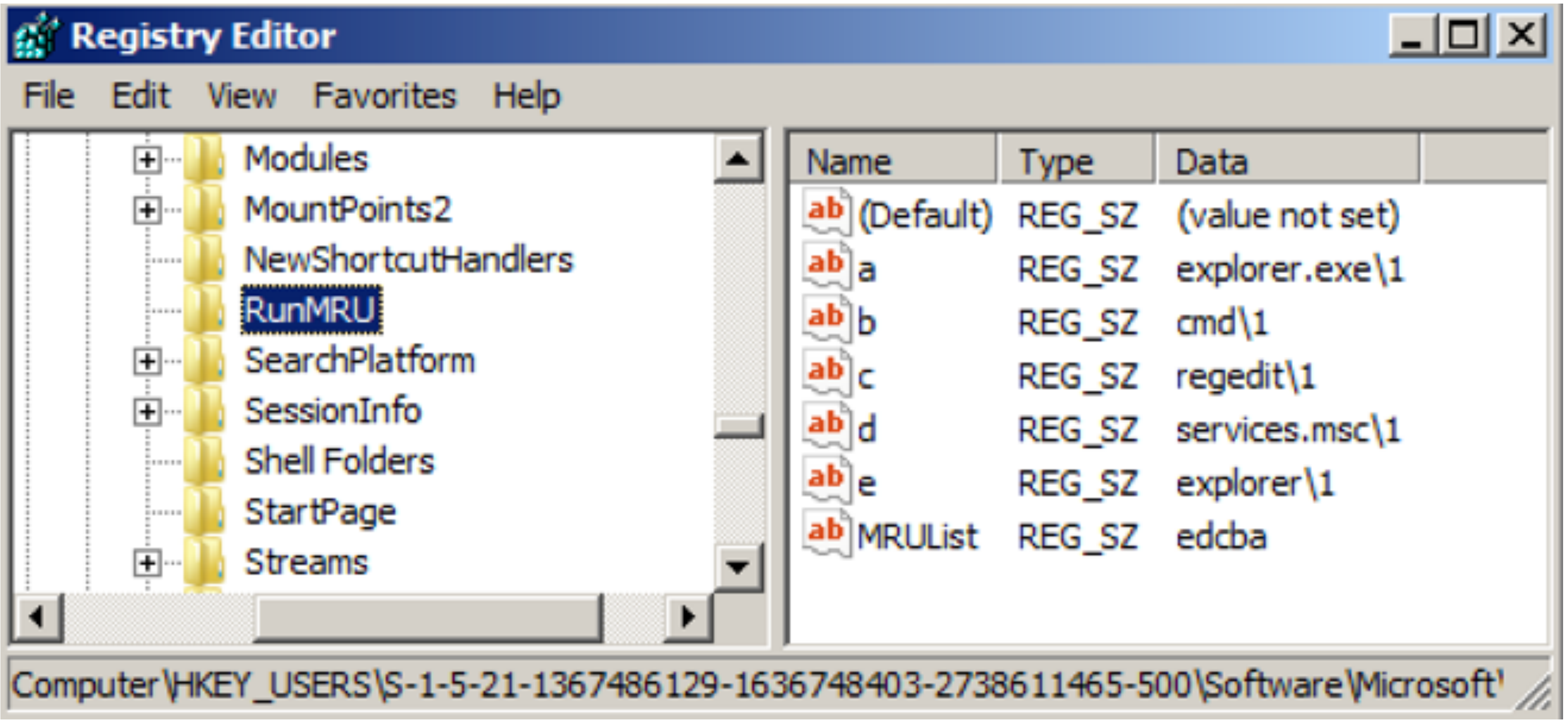


- HKEY_USERS\{SID}\Software \Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenPidlMRU
- HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer \ComDlg32\LastVisitedPidlMRU
- HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer \ComDlg32\CIDSizeMRU

Start Menu Run MRU

- **Programs recently launched from the Run box**
- **Human-readable**

HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

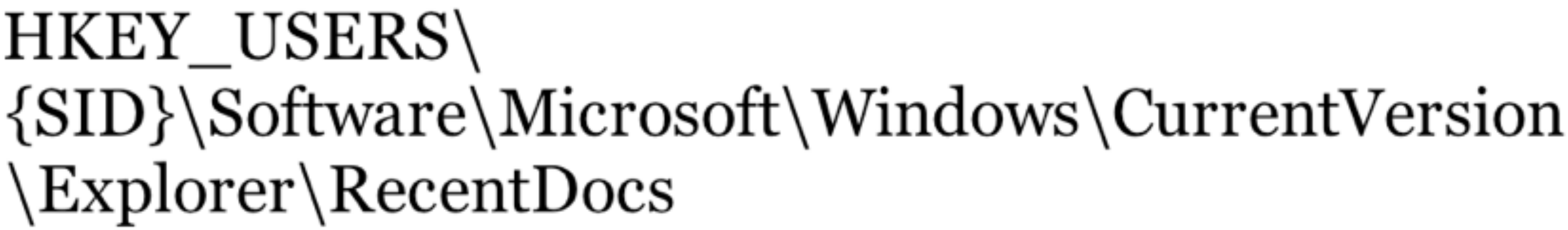


Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	explorer.exe\1
b	REG_SZ	cmd\1
c	REG_SZ	regedit\1
d	REG_SZ	services.msc\1
e	REG_SZ	explorer\1
MRUList	REG_SZ	edcba

Computer\HKEY_USERS\S-1-5-21-1367486129-1636748403-2738611465-500\Software\Microsoft'

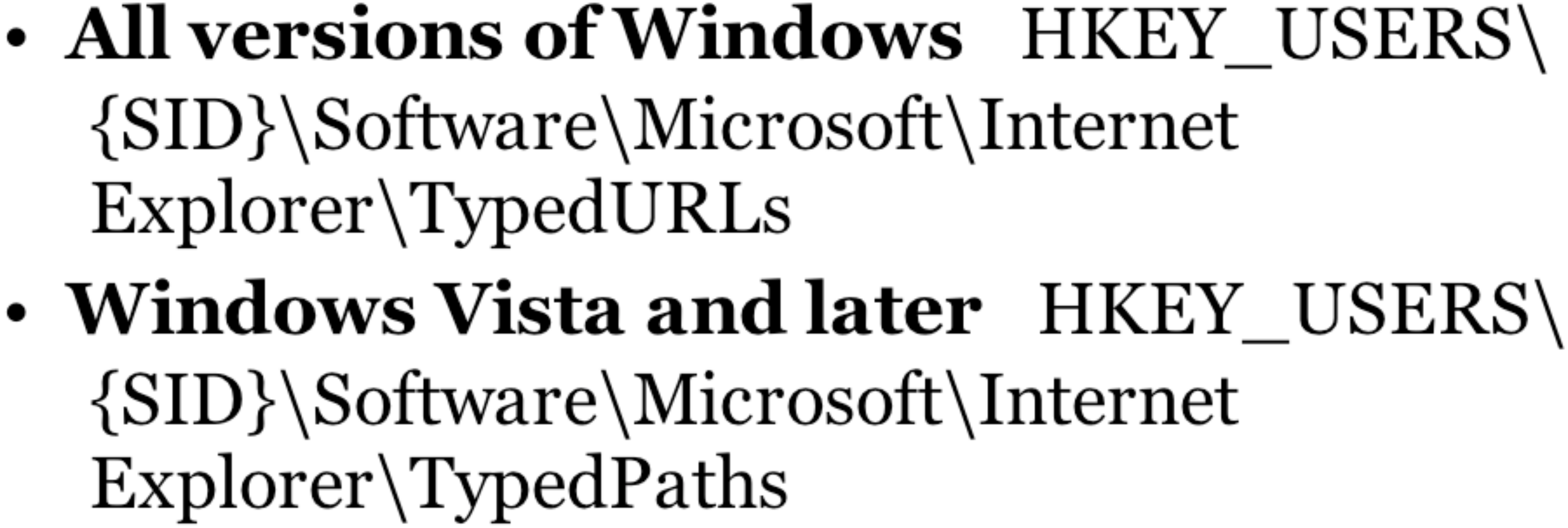
RecentDocs

- **Recently opened documents (any file extension)**
- **Used to populate File menu of various applications**

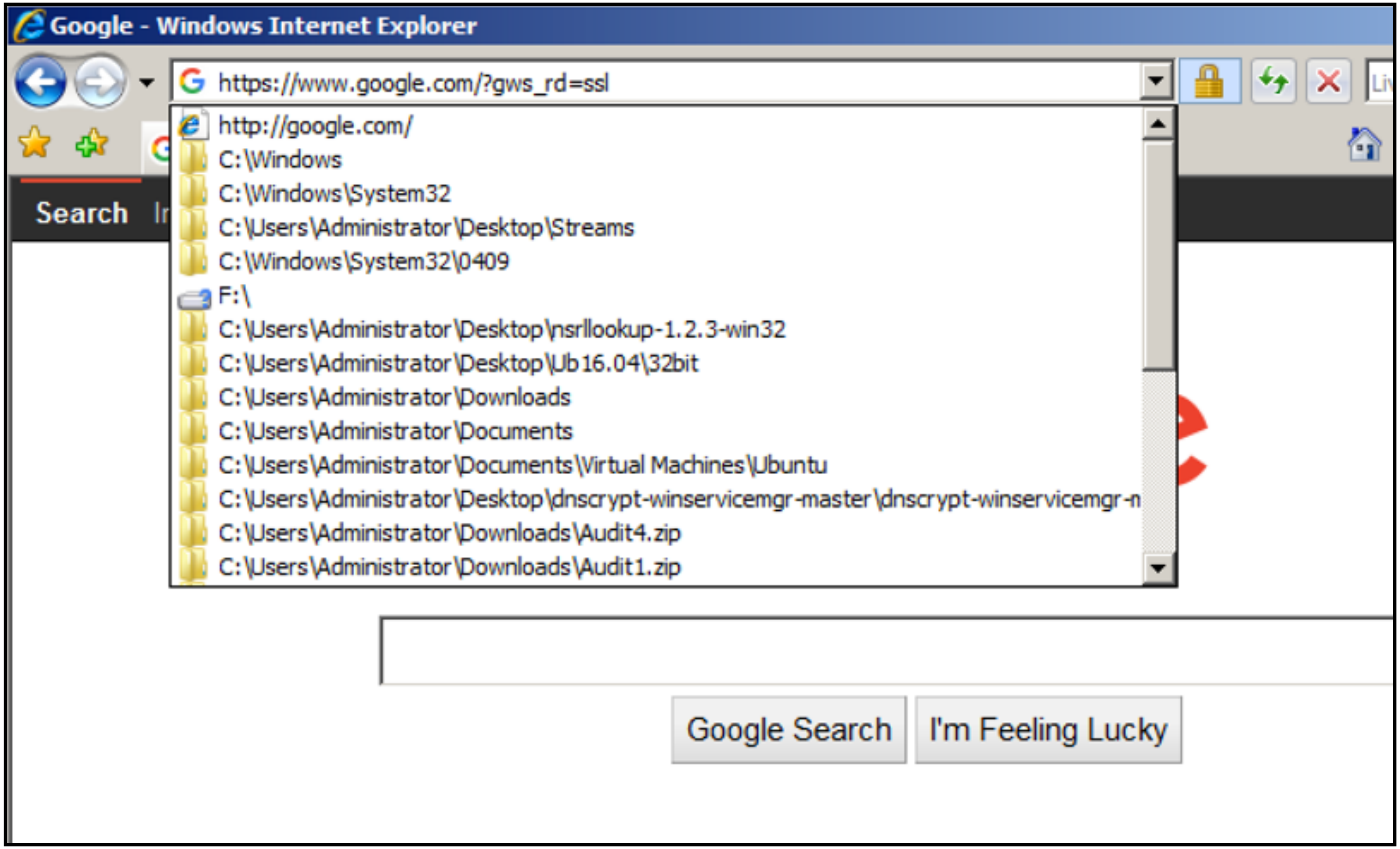


HKEY_USERS\
{SID}\Software\Microsoft\Windows\CurrentVersion
\Explorer\RecentDocs

Internet Explorer TypedURLs & TypedPaths



- **All versions of Windows** HKEY_USERS\{SID}\Software\Microsoft\Internet Explorer\TypedURLs
- **Windows Vista and later** HKEY_USERS\{SID}\Software\Microsoft\Internet Explorer\TypedPaths



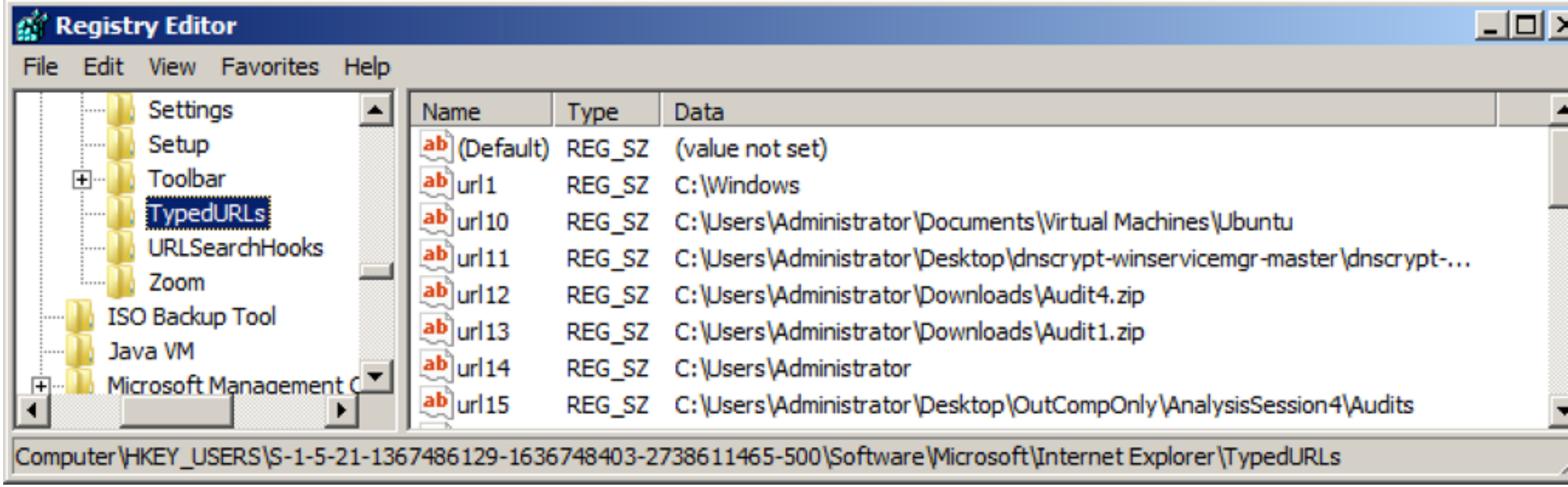
Google - Windows Internet Explorer

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

Proves Intent

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

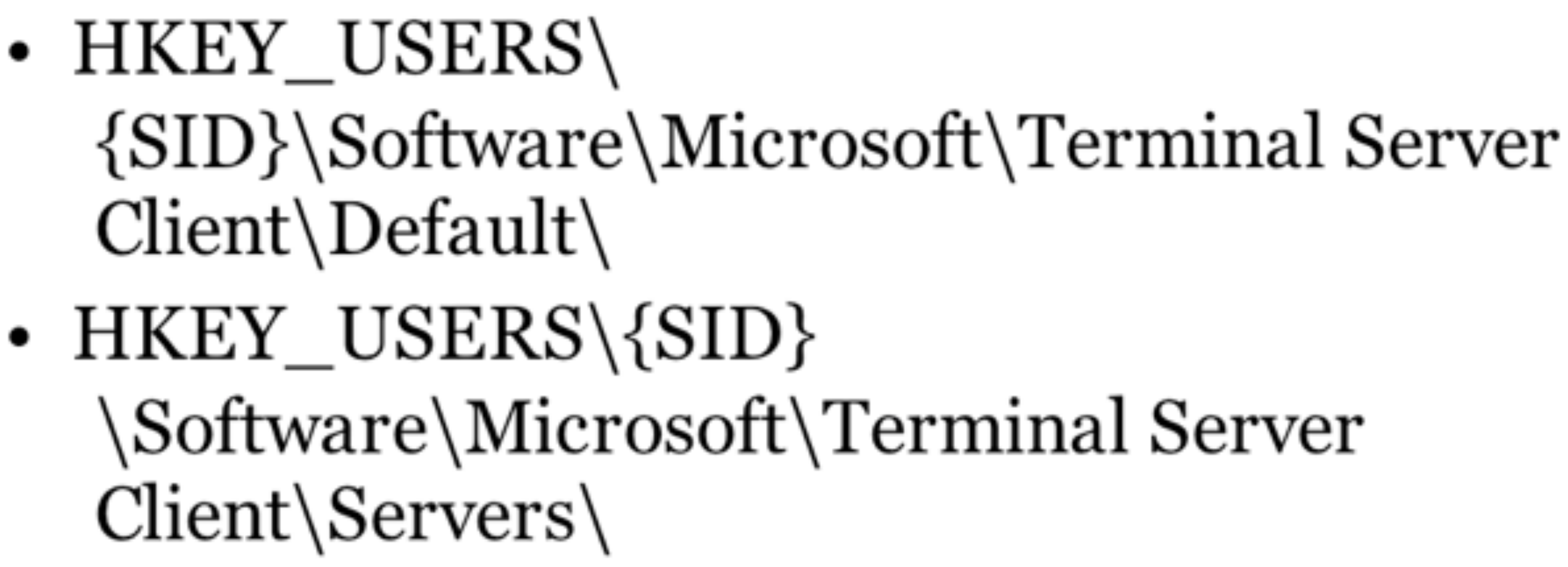


Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	C:\Windows
url10	REG_SZ	C:\Users\Administrator\Documents\Virtual Machines\Ubuntu
url11	REG_SZ	C:\Users\Administrator\Desktop\dnscrypt-winservicemgr-master\dnscrypt-...
url12	REG_SZ	C:\Users\Administrator\Downloads\Audit4.zip
url13	REG_SZ	C:\Users\Administrator\Downloads\Audit1.zip
url14	REG_SZ	C:\Users\Administrator
url15	REG_SZ	C:\Users\Administrator\Desktop\OutCompOnly\AnalysisSession4\Audits

Computer\HKEY_USERS\S-1-5-21-1367486129-1636748403-2738611465-500\Software\Microsoft\Internet Explorer\TypedURLs

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**
- **Redline**

Single-Purpose Utilities

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