

COMP 5350 / 6350

Digital Forensics

Windows Registry Analysis

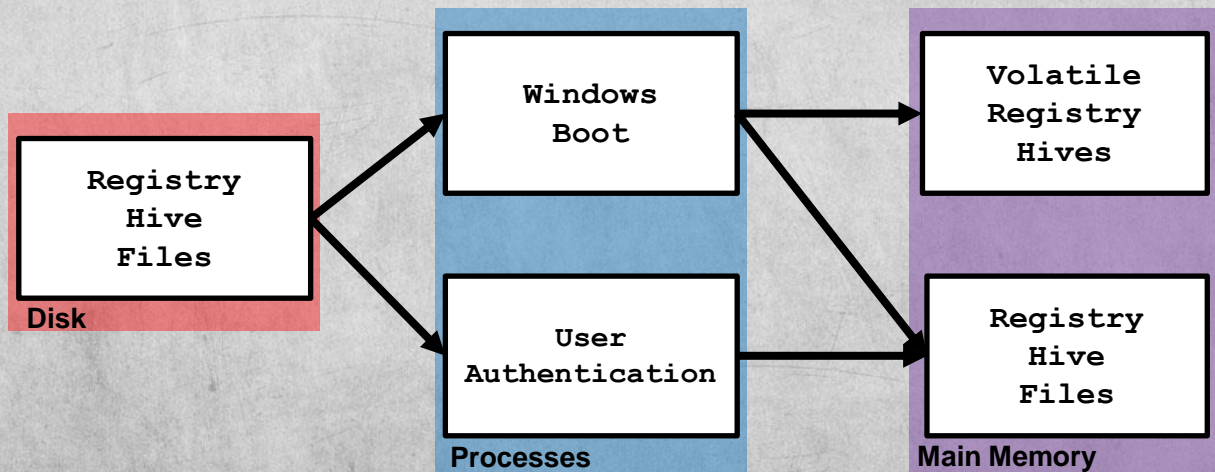


Windows Registry Review

- The Windows registry is a “central hierarchal database used to store information that is necessary to configure the system for one or more users, applications, and hardware devices.”
- Prior to Windows 2000, initialization files were used for system configuration
 - ✓ boot.ini
 - ✓ system.ini
 - ✓ win.ini
- Since Windows 2000, a registry structure was utilized to create a more efficient interaction between kernel and user functions
- Registry entries contain two different structures:
 - Registry Key
 - Similar to a folder in that holds multiple values
 - Registry Value
 - Similar to a file that contains specific values

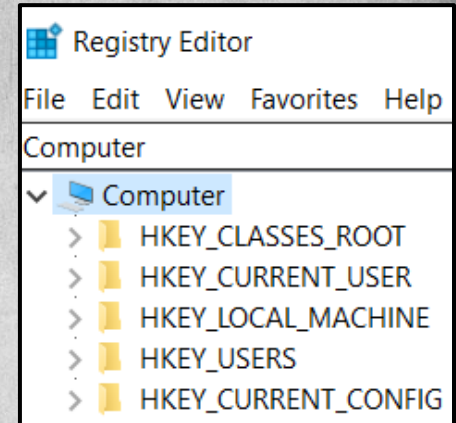
Windows Registry Operation

- A comprehensive copy of the registry can only be found in main memory since it requires both the registry entries along with active processes that create it
- From a forensics standpoint, this is significant because gathering a complete registry requires live memory capture

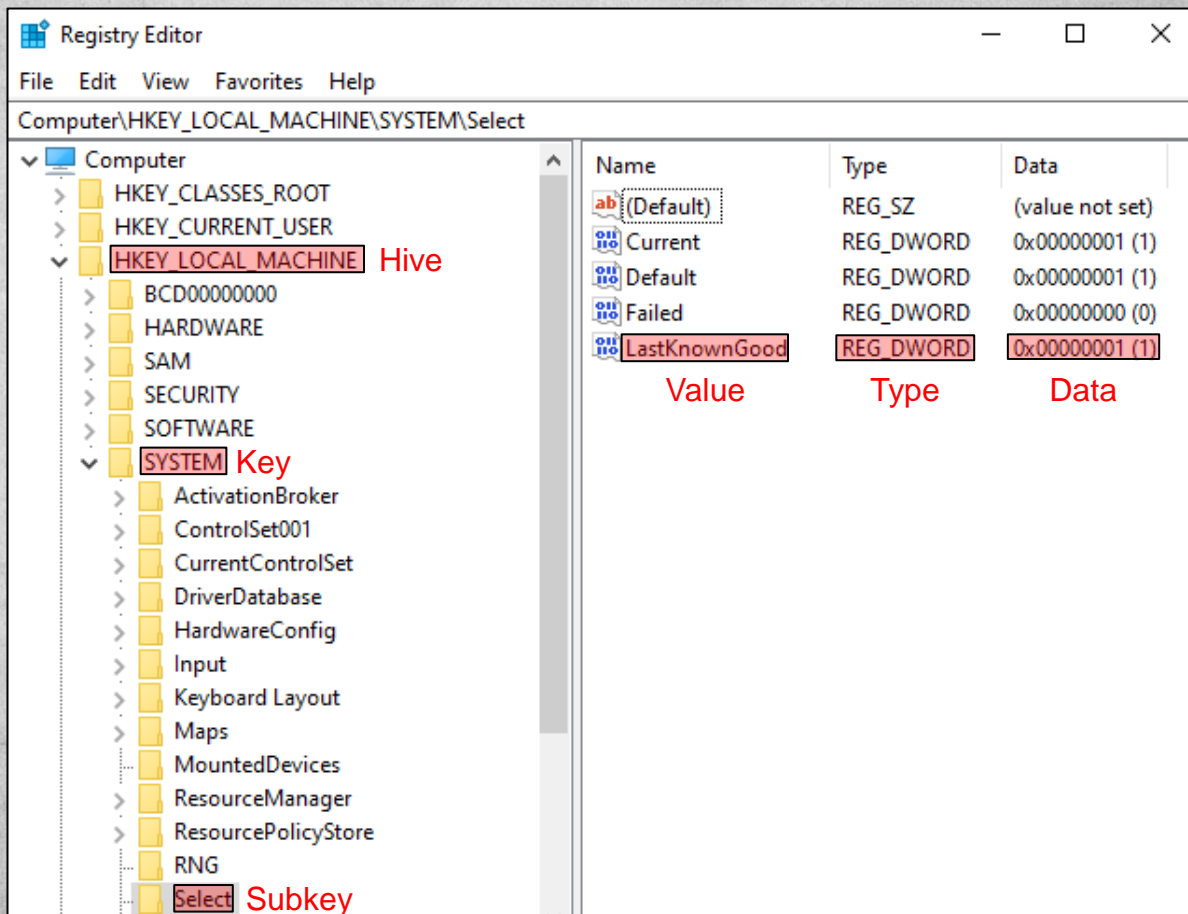


Windows Registry Hives

- The Windows registry contains hierarchical root keys
 - ✓ HKEY_CLASSES_ROOT (HKCR)
 - All information relating to file name extensions and Object Linking and Embedding (OLE)
 - ✓ HKEY_CURRENT_USER (HKCU)
 - Contains settings for the currently logged on user
 - ✓ HKEY_LOCAL_MACHINE (HKLM)
 - Contains information about hardware and software on the system
 - ✓ HKEY_USERS (HKU)
 - Contains information of different user settings and consolidated from HKCU
 - ✓ HKEY_CURRENT_CONFIG (HKCC)
 - Contains information about current hardware configurations
 - Usually empty until loaded during the boot process and loads hardware profiles into HKLM sub keys

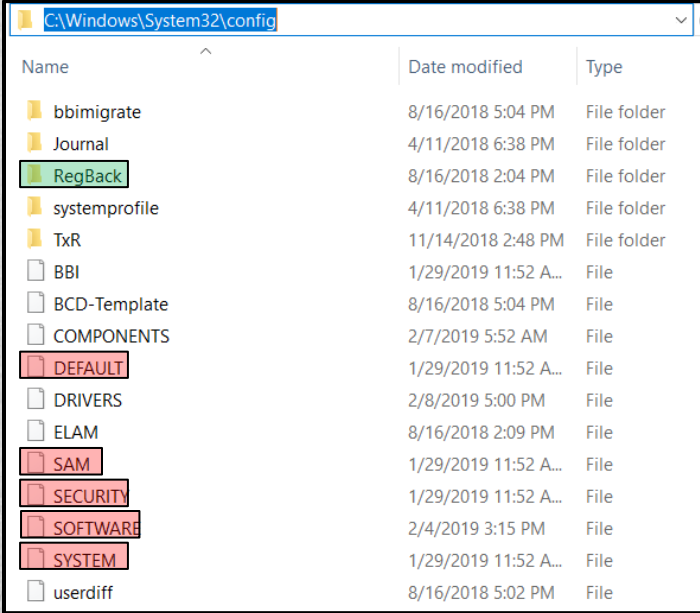


Registry Nomenclature



Windows Registry Storage

- The Windows Registry for each system is stored in:
 - ✓ C:\Windows\System32\config
- The Windows Registry is backed up in:
 - ✓ C:\Windows\System32\config\RegBack
 - DEFAULT
 - SAM
 - SECURITY
 - SOFTWARE
 - SYSTEM



Name	Date modified	Type
bbimigrate	8/16/2018 5:04 PM	File folder
Journal	4/11/2018 6:38 PM	File folder
RegBack	8/16/2018 2:04 PM	File folder
systemprofile	4/11/2018 6:38 PM	File folder
TxR	11/14/2018 2:48 PM	File folder
BBI	1/29/2019 11:52 A...	File
BCD-Template	8/16/2018 5:04 PM	File
COMPONENTS	2/7/2019 5:52 AM	File
DEFAULT	1/29/2019 11:52 A...	File
DRIVERS	2/8/2019 5:00 PM	File
ELAM	8/16/2018 2:09 PM	File
SAM	1/29/2019 11:52 A...	File
SECURITY	1/29/2019 11:52 A...	File
SOFTWARE	2/4/2019 3:15 PM	File
SYSTEM	1/29/2019 11:52 A...	File
userdiff	8/16/2018 5:02 PM	File

Registry Analysis Tools

Windows Registry Analysis Tools

- There are several helpful registry collection and analysis tools including:
 - ✓ RegRipper
 - Perl-based Windows Registry data extraction tool
 - ✓ FTK Imager
 - Disk imaging application from AccessData
 - ✓ ShellBags Explorer
 - Registry shellbag analysis
 - ✓ BulkExtractor
 - High speed disk scanner that analyzes disk images, files, or directories without the need of file system parsing

The screenshot shows the NIST Computer Forensics Tool Catalog search results for 'Windows Registry Analysis'. The interface includes a sidebar with 'Forensic Tool Functionalities' and a main search area with various filters.

Computer Forensics Tool Catalog
NIST National Institute of Standards and Technology U.S. Department of Commerce

Home Tool Search Forensic Tool Taxonomy Vendors Contacts

Home > Tool Search

Search for forensic tools by functionality

☐ find all Windows Registry Analysis tools ☐ refine by search parameters

Forensic Functionality: Windows Registry Analysis

Technical Parameters:

Tool host OS / runtime environment:	Input data type(s):	Automated hive extraction and parsing:	Registry rebuilding:	Deleted key recovery:
any	any	any	any	any
Windows	raw (dd)	active Registry	supports Registry rebuilding	supports deleted key recovery
Mac	EnCase Evidence File Format Version 2 (.e01)	active file system	Registry rebuilding unsupported	
Linux	Expert Witness (.e01)	Windows restore points		

Search

Registry Ripper

- A Perl-based registry parsing tool used for offline forensic analysis of Windows systems
- RegRipper is installed by default within SANS SIFT but requires an update
- RegRipper accounts for run keys which give a specified program permission to run when a user logs on
- Knowledge of registry key structure and values is necessary to conduct effective registry forensics

```
$ rip.pl
Rip v.3.0 - CLI RegRipper tool
Rip [-r Reg hive file] [-f profile] [-p plugin] [options]
Parse Windows Registry files, using either a single module, or a profile.

-r [hive] .....Registry hive file to parse
-d .....Check to see if the hive is dirty
-g .....Guess the hive file type
-a .....Automatically run hive-specific plugins
-aT .....Automatically run hive-specific TLN plugins
-f [profile].....use the profile
-p [plugin].....use the plugin
-l .....list all plugins
-c .....Output plugin list in CSV format (use with -l)
-s systemname.....system name (TLN support)
-u username.....User name (TLN support)
-uP .....Update default profiles
-h.....Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
C:\>rip -r c:\case\ntuser.dat -p userassist
C:\>rip -r c:\case\ntuser.dat -a
C:\>rip -l -c
```

Registry Ripper Plugins

- The current version of RegRipper provides 380+ plugins which are scripts that look for key information within a Windows registry
- RegRipper plugins can parse critical Windows OS information:
 - ✓ System / User GPO History
 - ✓ Deleted Registry Keys and Values
 - ✓ Security Account Manager (SAM) User and Group Membership
 - ✓ Display Autorun Settings
- RegRipper commands generally include:

```
rip.pl -r <RegistryKey> -p <Plugin>
```

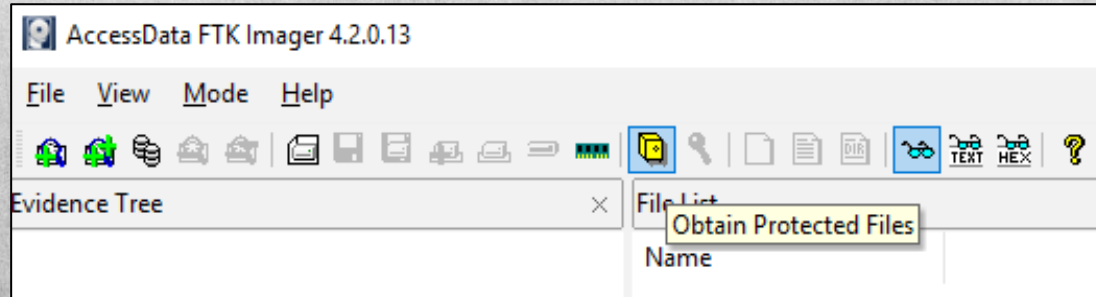
Registry Ripper Plugins

- A consolidated spreadsheet of valuable RegRipper plugins has been provided to align plugins with the required hives

Plugin	Hive	Description
del	All	Parse hive, print deleted keys/values
baseline	All	Scans a hive file, checking sizes of binary value data
regtime_tln	All	Dumps entire hive - all keys sorted by LastWrite time
regtime	All	Dumps entire hive - all keys sorted by LastWrite time
slack	All	Parse hive, print slack space, retrieve keys/values
findexes	All	Scans a hive file looking for binary value data that contains MZ
null	All	Check key/value names in a hive for leading null char
slack_tln	All	Parse hive, print slack space, retrieve keys/values
sizes	All	Scans a hive file looking for binary value data of a min size (5000)
malware	All	Checks for malware-related keys/values
del_tln	All	Parse hive print deleted keys/values
fileless	All	Scans a hive file looking for fileless malware entries
rlo	All	Parse hive check key/value names for RLO character

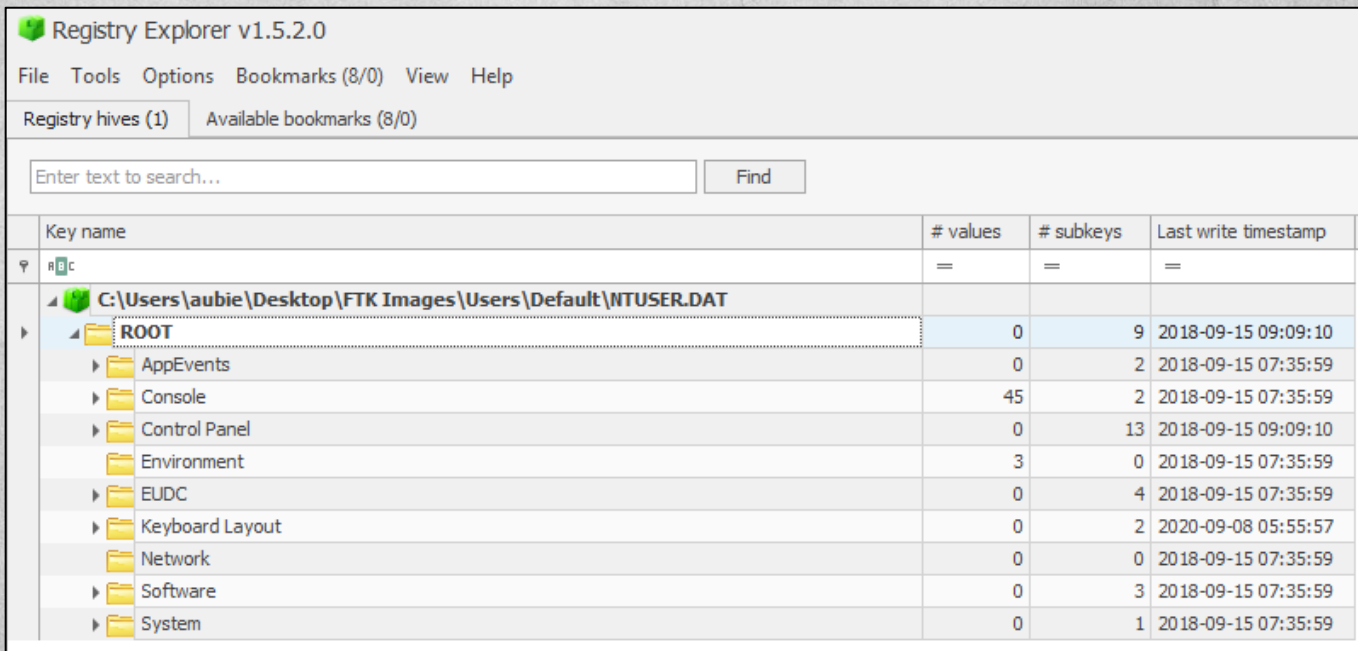
FTK Imager

- A data preview and imaging tool that collects and assess digital evidence
- FTK Imager capabilities include:
 - Creating forensic images of every layer of digital media (HDD, SSD, CD, DVD, USB, or individual files)
 - Recovery of deleted but not overwritten data
 - Parse numerous file systems including FAT, NTFS, XFS, and APFS
 - File and directory export
 - File hashing



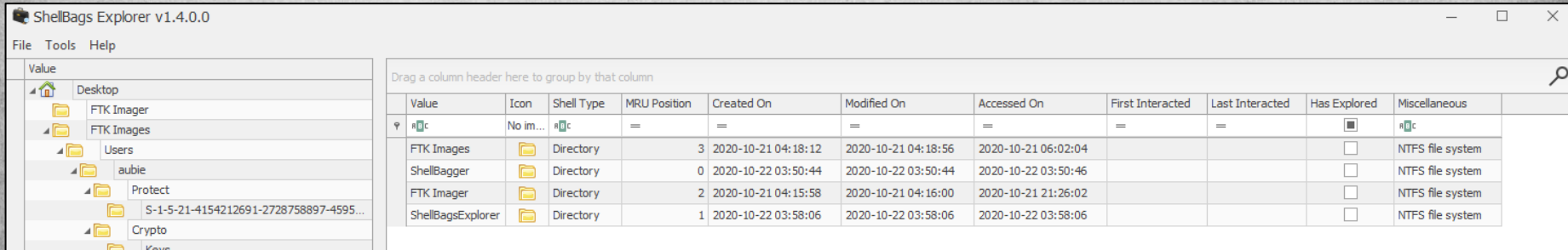
Registry Explorer

- An openly available registry viewer that can quickly iterate through registry entries and provides capabilities not available in registry editor



ShellBags Explorer

- An openly available explorer for the analysis of registry keys containing user preferences



Collection and Analysis Tool Installation

- Windows 10
 - ✓ FTK Imager
 - ✓ Registry Explorer
 - ✓ ShellBags Explorer
- SANS SIFT Workstation
 - ✓ Registry Ripper Installation Script
 - ✓ Perl-Compatible Regular Expressions (PCRE)

Forensic Analysis of Windows Registry Keys

Registry Collection

- Before starting an analysis, we must first collect registry artifacts
- FTK Imager will collect protected files including registry hives and keys
 - ✓ Users
 - ✓ Default
 - ✓ SAM
 - ✓ SECURITY
 - ✓ SOFTWARE
 - ✓ SYSTEM



Forensically Valuable Registry Keys

- Although we have collected high-level registry hives, some of the more valuable files and keys to consider:
 - ✓ NTUSER.DAT
 - ✓ USRCLASS.DAT
 - ✓ HKCU\SOFTWARE
 - ✓ HKLM\SYSTEM
 - ✓ HKLM\SOFTWARE
- From a forensics standpoint we are looking to collect artifacts that can provide information on:
 - ✓ Logon history
 - ✓ OS configuration changes
 - ✓ Application usage
 - ✓ Most recently used items
 - ✓ User settings

NTUSER.DAT

- NTUSER.DAT is a hidden file within each user profile (i.e. C:Users\<User>) that contains settings and preferences that are automatically loaded when a user logs into a Windows system
- Changes tracked by the NTUSER.DAT file include:
 - ✓ User preferences
 - ✓ Installed Programs
 - ✓ Display Settings
- During the boot and user logon process NTUSER.DAT data is loaded into memory and configures previously saved user settings into the HKCU hive

NTUSER.DAT Access

- NTUSER.DAT is stored in a hidden file under each user profile:
C:\Users\<Username>
- Accessibility to hidden files is limited and requires specially configured applications to collect those artifacts

```
C:\Users\aubie>dir /ah
Volume in drive C has no label.
Volume Serial Number is 7CEB-A2F4

Directory of C:\Users\aubie

09/08/2020 12:56 AM <DIR>          AppData
09/08/2020 12:56 AM <JUNCTION>      Application Data [C:\Users\aubie\AppData\Roaming]
09/08/2020 12:56 AM <JUNCTION>      Cookies [C:\Users\aubie\AppData\Local\Microsoft\Windows\INetCookies]
09/08/2020 12:56 AM <JUNCTION>      Local Settings [C:\Users\aubie\AppData\Local]
09/08/2020 12:57 AM <DIR>          MicrosoftEdgeBackups
09/08/2020 12:56 AM <JUNCTION>      My Documents [C:\Users\aubie\Documents]
09/08/2020 12:56 AM <JUNCTION>      NetHood [C:\Users\aubie\AppData\Roaming\Microsoft\Windows\Network Shortcuts]
10/20/2020 11:13 PM          1,310,720 NTUSER.DAT
09/08/2020 12:56 AM          262,144 ntuser.dat.LOG1
09/08/2020 12:56 AM          327,680 ntuser.dat.LOG2
09/08/2020 12:56 AM          65,536 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TM.blf
09/08/2020 12:56 AM          524,288 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer000000000000000001.regtrans-ms
09/08/2020 12:56 AM          524,288 NTUSER.DAT{1c3790b4-b8ad-11e8-aa21-e41d2d101530}.TMContainer000000000000000002.regtrans-ms
09/08/2020 12:56 AM          20 ntuser.ini
09/08/2020 12:56 AM <JUNCTION>      PrintHood [C:\Users\aubie\AppData\Roaming\Microsoft\Windows\Printer Shortcuts]
09/08/2020 12:56 AM <JUNCTION>      Recent [C:\Users\aubie\AppData\Roaming\Microsoft\Windows\Recent]
09/08/2020 12:56 AM <JUNCTION>      SendTo [C:\Users\aubie\AppData\Roaming\Microsoft\Windows\SendTo]
09/08/2020 12:56 AM <JUNCTION>      Start Menu [C:\Users\aubie\AppData\Roaming\Microsoft\Windows\Start Menu]
09/08/2020 12:56 AM <JUNCTION>      Templates [C:\Users\aubie\AppData\Roaming\Microsoft\Windows\Templates]
7 File(s)          3,014,676 bytes
12 Dir(s)          1,849,405,440 bytes free
```


Registry Hive Architecture

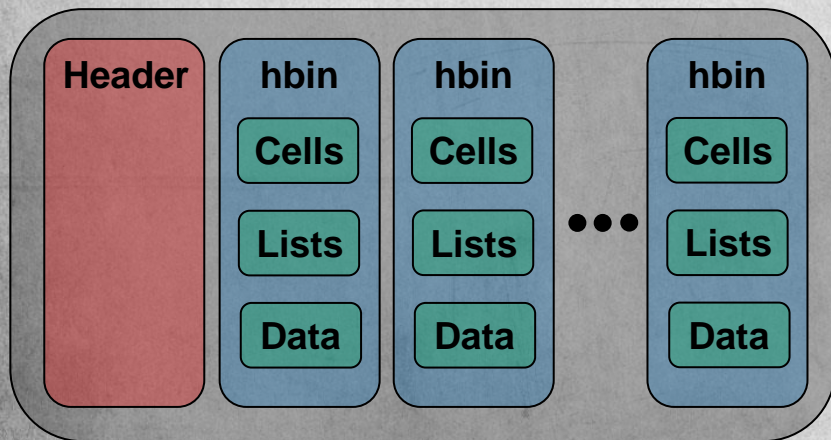
- Registry signatures

✓ nk

- Key Node

✓ vk

- Value Node



\$	hexdump	-C	NTUSER.DAT	-s	0	-n	\$((9*512))										
00000000	72	65	67	66	bd	01	00	00	bc	01	00	00	00	00	00	00	regf.....
00000010	00	00	00	00	01	00	00	00	05	00	00	00	00	00	00	00
00000020	01	00	00	00	20	00	00	00	00	50	12	00	01	00	00	00P.....
00000030	5c	00	3f	00	3f	00	5c	00	43	00	3a	00	5c	00	55	00	\\?.?.\C.:\.U.
00000040	73	00	65	00	72	00	73	00	5c	00	61	00	75	00	62	00	s.e.r.s.\.a.u.b.
00000050	69	00	65	00	5c	00	6e	00	74	00	75	00	73	00	65	00	i.e.\.n.t.u.s.e.
00000060	72	00	2e	00	64	00	61	00	74	00	00	00	00	00	00	00	r...d.a.t.....
00000070	b3	90	37	1c	ad	b8	e8	11	aa	21	e4	1d	2d	10	15	30	..7.....!...0
*																	
00000090	00	00	00	00	b4	90	37	1c	ad	b8	e8	11	aa	21	e4	1d7.....!...
000000a0	2d	10	15	30	72	6d	74	6d	3e	5d	d1	01	9d	a6	d6	01	[-..0rmtm>].....
000000b0	4f	66	52	67	01	00	00	00	00	00	00	00	00	00	00	00	OfRg.....
000000c0	00	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	52	dc	37	4cR.7L
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
*																	
00001000	68	62	69	6e	00	00	00	00	00	10	00	00	00	00	00	00	hbin.....
00001010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00001020	a8	ff	ff	ff	6e	6b	2c	00	80	8f	07	98	cf	a8	d6	01nk,.....
00001030	02	00	00	00	18	07	00	00	0a	00	00	00	01	00	00	00
00001040	c0	06	00	00	e8	03	00	80	00	00	00	00	ff	ff	ff	ff
00001050	c0	53	00	00	ff	ff	ff	ff	2a	00	00	00	00	00	00	00	S.....*.....
00001060	00	00	00	00	00	00	00	00	00	00	00	00	04	00	00	00
00001070	52	4f	4f	54	00	00	00	00	a0	ff	ff	ff	6e	6b	20	00	ROOT.....nk..
00001080	93	9b	a6	c8	a4	85	d6	01	02	00	00	00	20	00	00	00
00001090	02	00	00	00	00	00	00	00	60	71	01	00	ff	ff	ff	ff`q.....
000010a0	00	00	00	00	ff	ff	ff	ff	e0	36	00	00	ff	ff	ff	ff6.....

USRCLASS.DAT

- USRCLASS.DAT is used for registry virtualization since Windows Vista to ensure backwards compatibility with earlier releases of Windows
- Before Windows Vista, applications required administrator rights when accessing and changing registry elements
- After Windows Vista, applications no longer required administrator rights because registry virtualization allowed registry requests to be redirected from system to user context
 - HKEY_LOCAL_MACHINE\Software (Admin)
 - HKEY_USERS_Classes\VirtualStore\Machine\Software (User)
- During boot and user logon process USRCLASS.DAT is loaded into memory and allows for registry virtualization in the HKCU/Software/Classes key

USRCLASS.DAT Access

- USRCLASS.DAT is stored in a hidden file under each user profile
C:\Users\<Username>\AppData\Local\Microsoft\Windows
- As with NTUSER.DAT, USRCLASS.DAT is a hidden file and requires specially configured applications to collect those artifacts

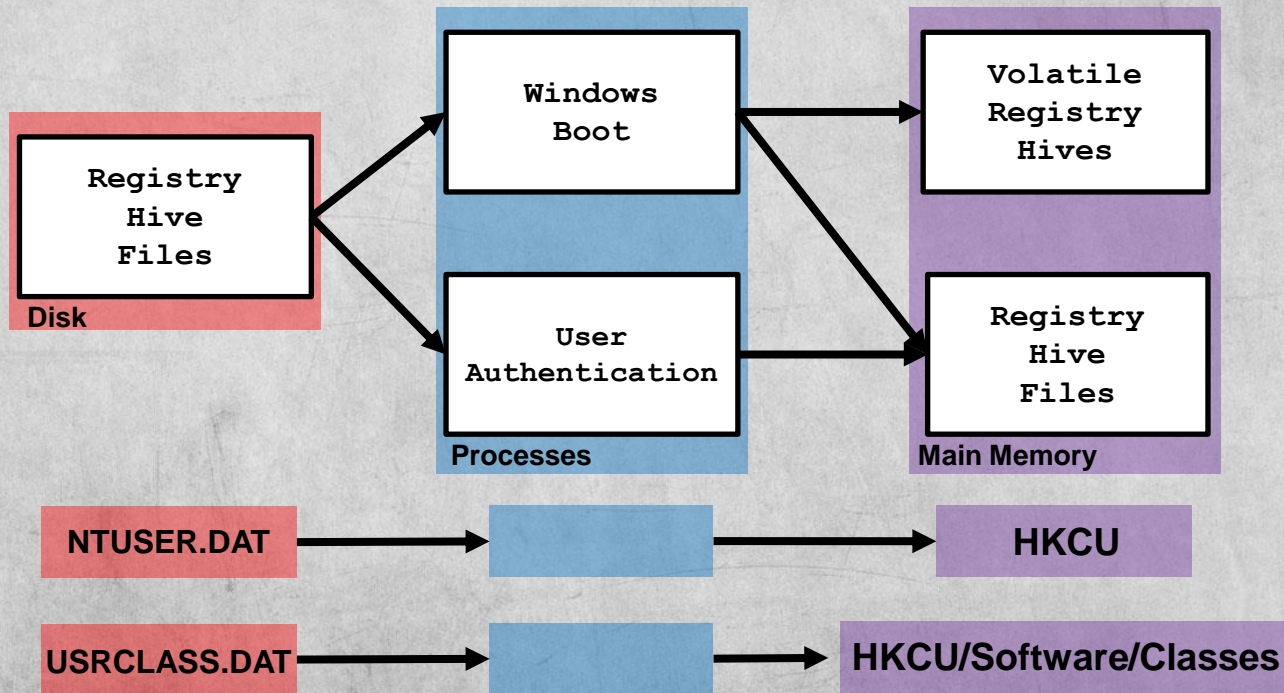
```
C:\Users\aubie\AppData\Local\Microsoft\Windows>dir /ah
Volume in drive C has no label.
Volume Serial Number is 7CEB-A2F4

Directory of C:\Users\aubie\AppData\Local\Microsoft\Windows

09/08/2020 12:57 AM <DIR> AppCache
10/22/2020 01:52 AM 46 desktop.ini
10/21/2020 08:38 AM <DIR> IECompatCache
10/21/2020 08:38 AM <DIR> IECompatUaCache
10/21/2020 08:41 AM <DIR> IEDownloadHistory
10/22/2020 06:30 PM <DIR> INetCache
10/20/2020 12:09 AM <DIR> INetCookies
09/08/2020 12:58 AM <DIR> SettingSync
09/08/2020 12:56 AM <JUNCTION> Temporary Internet Files [C:\Users\aubie\AppData\Local\Microsoft\Windows\INetCache]
10/22/2020 07:00 PM 3,670,016 UsrClass.dat
09/08/2020 12:56 AM 655,360 UsrClass.dat.LOG1
09/08/2020 12:56 AM 899,072 UsrClass.dat.LOG2
09/08/2020 12:56 AM 65,536 UsrClass.dat{6ab0e9f2-f1a8-11ea-b9d0-ac7ba1cda6b2}.TM.blf
09/08/2020 12:56 AM 524,288 UsrClass.dat{6ab0e9f2-f1a8-11ea-b9d0-ac7ba1cda6b2}.TMContainer000000000000000001.regtrans-ms
09/08/2020 12:56 AM 524,288 UsrClass.dat{6ab0e9f2-f1a8-11ea-b9d0-ac7ba1cda6b2}.TMContainer000000000000000002.regtrans-ms
10/22/2020 07:01 PM <DIR> WebCache
09/08/2020 12:56 AM 0 WebCacheLock.dat
      8 File(s)      6,338,606 bytes
      9 Dir(s)      1,309,917,184 bytes free
```


Registry Formation

- Using our graphical view of how the Windows registry is formed during the boot and authentication process we can now see the relationship between NTUSER.DAT, USRCLASS.DAT, and HKCU



Registry Ripper Plugins

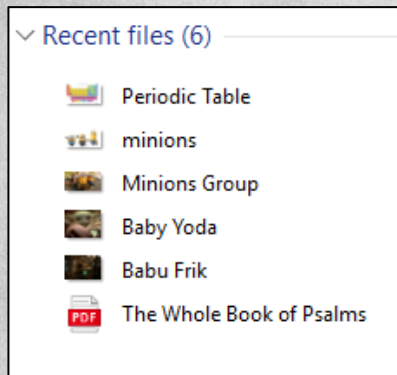
Plugin	Hive	Description
del	All	Parse hive, print deleted keys/values
baseline	All	Scans a hive file, checking sizes of binary value data
regtime_tln	All	Dumps entire hive - all keys sorted by LastWrite time
regtime	All	Dumps entire hive - all keys sorted by LastWrite time
slack	All	Parse hive, print slack space, retrieve keys/values
findexes	All	Scans a hive file looking for binary value data that contains MZ
null	All	Check key/value names in a hive for leading null char
slack_tln	All	Parse hive, print slack space, retrieve keys/values
sizes	All	Scans a hive file looking for binary value data of a min size (5000)
malware	All	Checks for malware-related keys/values
del_tln	All	Parse hive print deleted keys/values
fileless	All	Scans a hive file looking for fileless malware entries
rlo	All	Parse hive check key/value names for RLO character

User Preference Keys

- The first set of registry keys we will analyze are user preferences:
 - ✓ HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
 - \RecentDocs
 - List of files recently opened directly from Windows Explorer
 - \RunMRU
 - List of entries executed using the Windows “Run” application
 - \UserAssist
 - Contains Globally Unique Identifier (GUID) subkeys
 - Each GUID maintains a list of objects such as programs, shortcuts, and control panel applets that a user has accessed

Recent Documents

NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\RecentDocs



User View

```
$ rip.pl -r Users/aubie/NTUSER.DAT -p recentdocs
Launching recentdocs v.20100405
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Wed Oct 21 13:52:26 2020 (UTC)
 8 = Pictures
12 = Periodic Table.png
 7 = minions.png
 9 = Minions Group.jpg
10 = Baby Yoda.jpg
11 = Babu Frik.jpg
13 = The Whole Book of Psalms.pdf
 6 = This PC
 5 = Documents
 4 = New folder
 3 = Default
 2 = NTUSER.DAT
 1 = privacy-location
 0 = The Internet
```

Analyst View – MRU Order

Recent Documents

NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\RecentDocs

```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .DAT
LastWrite Time Wed Oct 21 06:06:12 2020 (UTC)
MRUListEx = 0
    0 = NTUSER.DAT

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .jpg
LastWrite Time Wed Oct 21 13:52:11 2020 (UTC)
MRUListEx = 0,1,2
    0 = Minions Group.jpg
    1 = Baby Yoda.jpg
    2 = Babu Frik.jpg

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .pdf
LastWrite Time Wed Oct 21 13:51:40 2020 (UTC)
MRUListEx = 0
    0 = The Whole Book of Psalms.pdf

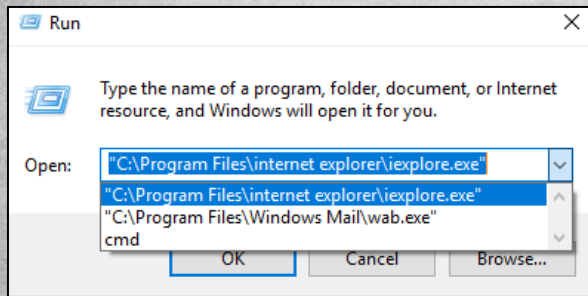
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .png
LastWrite Time Wed Oct 21 13:52:26 2020 (UTC)
MRUListEx = 1,0
    1 = Periodic Table.png
    0 = minions.png

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ Folder
LastWrite Time Wed Oct 21 13:52:26 2020 (UTC)
MRUListEx = 3,2,1,0
    3 = Pictures
    2 = This PC
    1 = Default
    0 = The Internet
```

Analyst View – MRU File Type

Run Application Most Recently Used

NTUSER.DAT\Software\Microsoft\Windows\Current Version\Explorer\RunMRU



User View

```
$ rip.pl -r Users/aubie/NTUSER.DAT -p runmru
Launching runmru v.20080324
runmru v.20080324
(NTUSER.DAT) Gets contents of user's RunMRU key

RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time Wed Oct 21 13:38:13 2020 (UTC)
MRUList = cba
a  cmd\1
b  "C:\Program Files\Windows Mail\wab.exe"\1
c  "C:\Program Files\internet explorer\iexplore.exe"\1
```

Analyst View

User Assist

- Maintains a list of user programs, shortcuts, and control panel apps
- User Assist GUID values provide Windows version information:
 - ✓ Windows XP / Vista
 - {75048700-EF1F-11D0-9888-006097DEACF9}
 - Applications, files, and links accessed
 - {5E6AB780-7743-11CF-A12B-00AA004AE837}
 - IE favorites and toolbar objects
 - ✓ Windows 7 / 8 / 10
 - {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
 - Recently run programs
 - {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
 - Applications, files, and links accessed

User Assist

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\[GUID]\Count

```
$ rip.pl -r Users/aubie/NTUSER.DAT -p userassist
Launching userassist v.20170204
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Tue Sep 8 05:56:28 2020 (UTC)

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

{A3D53349-6E61-4557-8FC7-0028EDCEE6F6}

{B267E3AD-A825-4A09-82B9-EEC22AA3B847}

{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}

{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
```

Windows 10 GUID's

User Assist

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\[GUID]\Count

```
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}  
Wed Oct 21 13:52:22 2020 Z  
    Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint (5)  
Wed Oct 21 13:51:39 2020 Z  
    Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge (5)  
Wed Oct 21 13:38:13 2020 Z  
    Microsoft.InternetExplorer.Default (1)  
Wed Oct 21 13:37:00 2020 Z  
    Microsoft.Windows.Explorer (3)  
    {6D809377-6AF0-444B-8957-A3773F02200E}\Windows Mail\wab.exe (1)  
Wed Oct 21 13:27:57 2020 Z  
    {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (2)  
Wed Oct 21 08:55:39 2020 Z  
    C:\Users\aubie\Desktop\FTK Imager\FTK Imager.exe (5)  
Wed Oct 21 08:55:13 2020 Z  
    SimonTatham.PuTTY (4)  
Wed Oct 21 08:44:59 2020 Z  
    {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\msiexec.exe (1)  
Wed Oct 21 08:43:07 2020 Z  
    C:\Users\aubie\Downloads\TimelineExplorer\TimelineExplorer\TimelineExplorer.exe (1)  
Wed Oct 21 06:03:14 2020 Z  
    C:\Users\aubie\Downloads\RegistryExplorer_RECmd\RegistryExplorer\RegistryExplorer.exe (1)  
Wed Oct 21 06:03:08 2020 Z  
    C:\Users\aubie\Downloads\RegistryExplorer_RECmd\RegistryExplorer\RECmd.exe (1)  
Wed Oct 21 04:12:43 2020 Z  
    {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\AccessData\Registry Viewer\RegistryViewer.exe (3)  
Wed Oct 21 04:08:31 2020 Z  
    {F38BF404-1D43-42F2-9305-67DE0B28FC23}\regedit.exe (2)  
Wed Oct 21 04:07:25 2020 Z  
    C:\Users\aubie\Desktop\AccessData_Registry_Viewer_2.0.0.exe (1)
```

Applications, files, and links accessed

User Assist

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\[GUID]\Count

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}		Last Run Time
Wed Oct 21 08:55:13 2020 Z	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\PuTTY\PuTTY.lnk	(4)
Wed Oct 21 05:33:16 2020 Z	{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Command Prompt.lnk	(1)
Wed Oct 21 04:12:43 2020 Z	C:\Users\Public\Desktop\Registry Viewer.lnk	(3)
Wed Oct 21 04:08:31 2020 Z	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Administrative Tools\Registry Editor.lnk	(2)
Tue Oct 20 04:58:02 2020 Z	{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\File Explorer.lnk	(2)
Tue Sep 8 05:54:48 2020 Z	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk	(9)
	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk	(7)
	{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Notepad.lnk	(6)

Recently run programs

User Logon

- Information relative to when a user lasted logged into a system

NTUSER.DAT\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

```
$ rip.pl -r SOFTWARE -p winlogon
Launching winlogon v.20130425
winlogon v.20130425
(Software) Get values from the WinLogon key

Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Sun Nov 13 01:54:42 2016 (UTC)
DefaultDomainName =
LegalNoticeCaption =
LegalNoticeText =
AutoRestartShell = 1
DisableBackButton = 1
EnableSIHostIntegration = 1
ForceUnlockLogon = 0
PasswordExpiryWarning = 5
PowerdownAfterShutdown = 0
ReportBootOk = 1
ShellCritical = 0
SiHostCritical = 0
SiHostReadyTimeOut = 0
SiHostRestartCountLimit = 0
SiHostRestartTimeGap = 0
WinStationsDisabled = 0
scremoveoption = 0
DisableCAD = 1
AutoAdminLogon = 0
EnableFirstLogonAnimation = 1
CachedLogonsCount = 10
DebugServerCommand = no
ShutdownFlags = 555
Background = 0 0 0
DefaultUserName = IEUser
LastUsedUsername = IEUser
ShutdownStartTime = tēB0P=0
```

```
UserSessionShutdownStopTime = 0rL0P=0
ShellInfrastructure = sihost.exe
Shell = explorer.exe
Userinit = C:\Windows\system32\userinit.exe,
PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}
VMApplet = SystemPropertiesPerformance.exe /pagefile
AutoLogonSID = S-1-5-21-4144202625-3024446806-325092953-1000
```

Notify subkey not found.

```
Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Fri Oct 30 07:25:52 2015 (UTC)
DefaultDomainName =
DefaultUserName =
EnableSIHostIntegration = 1
ShellCritical = 0
SiHostCritical = 0
SiHostReadyTimeOut = 0
SiHostRestartCountLimit = 0
SiHostRestartTimeGap = 0
Shell = explorer.exe
PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}
```

Notify subkey not found.

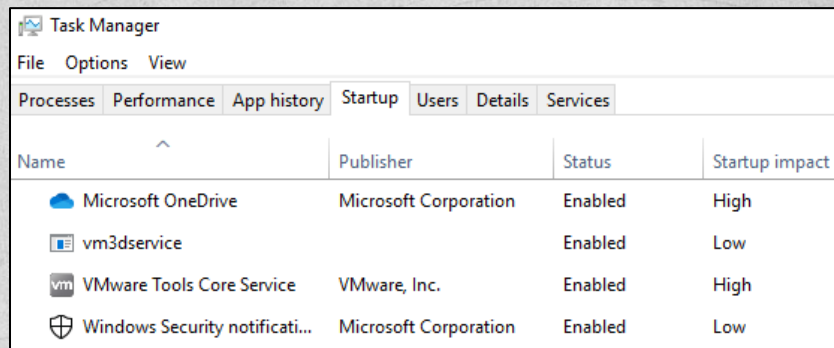
Analysis Tips: The UserInit and Shell values are executed when a user logs on. The UserInit value should contain a reference to userinit.exe; the Shell value should contain just 'explorer.exe'. Check TaskMan & System values, if found.

Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList not found.

Program Start Upon Logon

- There are numerous registry key values that enable programs to start when first logging onto a Windows system
- These registry keys are generated during the installation or application configuration process
- The following keys are valuable because they help identify what programs start for each user
 - ✓ HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - ✓ HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
 - ✓ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - ✓ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Program Start Upon Logon



The screenshot shows the Windows Task Manager application with the 'Startup' tab selected. The table lists four startup items: Microsoft OneDrive, vm3dservice, VMware Tools Core Service, and Windows Security notification area. Each entry includes its name, publisher, status (all are 'Enabled'), and startup impact (High or Low).

Name	Publisher	Status	Startup impact
Microsoft OneDrive	Microsoft Corporation	Enabled	High
vm3dservice		Enabled	Low
VMware Tools Core Service	VMware, Inc.	Enabled	High
Windows Security notificati...	Microsoft Corporation	Enabled	Low

User View

```
$ rip.pl -r software -p soft_run
Launching soft_run v.20130603
soft_run v.20130603
(Software) [Autostart] Get autostart key contents from Software hive

Microsoft\Windows\CurrentVersion\Run
LastWrite Time Wed Oct 21 04:13:54 2020 (UTC)
  VMware VM3DService Process - "C:\Windows\system32\vm3dservice.exe" -u
  VMware User Process - "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
  SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
```

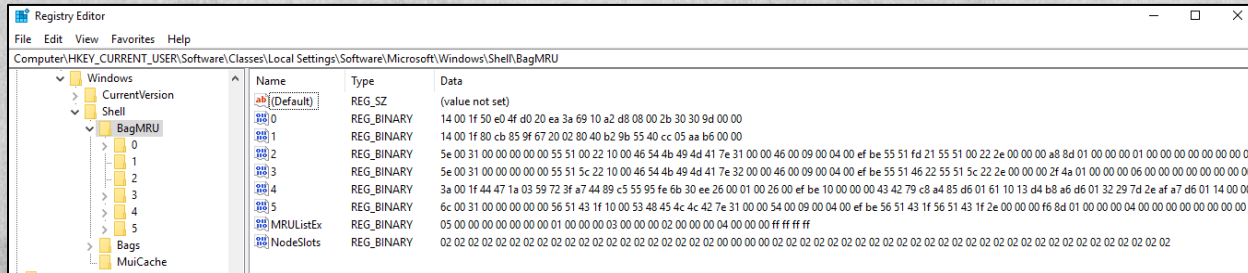
Analyst View

Shellbags

- Microsoft Windows records view preferences of folders and user desktops to ensure preferences are available during next use
- The view preferences stored in the Windows registry are called ShellBags due to the registry key names
 - ✓ HKCU\SOFTWARE\Microsoft\Windows\Shell\Bags
 - ✓ HKCU\SOFTWARE\Microsoft\Windows\Shell\BagMRU
 - ✓ HKCU\SOFTWARE\Microsoft\Windows\ShellNoRoam\Bags
 - ✓ HKCU\SOFTWARE\Microsoft\Windows\ShellNoRoam\BagMRU
 - ✓ HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags
 - ✓ HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- Even after folders and applications are deleted on a Windows system, their data persists within ShellBag related keys

BagMRU vs. Bags

- The ShellBag information is composed of two main registry keys:
 - ✓ BagMRU
 - Stores folder names and records folder paths
 - Represents the user desktop
 - ✓ Bags
 - Stored view preferences including window size, location, and view mode
- Our main objective in the next session is to expand upon the collection and analysis of ShellBag data



References

- Registry Ripper Plugins
 - ✓ <https://hexacorn.com/tools/3r.html#byfile>
- Registry Run Keys
 - ✓ <https://docs.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys?redirectedfrom=MSDN>