

Forensics: A Quick Dive into Windows Registry

Introduction

Window registry is more like a database, one that stores all kinds of information that are vital to the proper functioning of the operating system. Information related to:

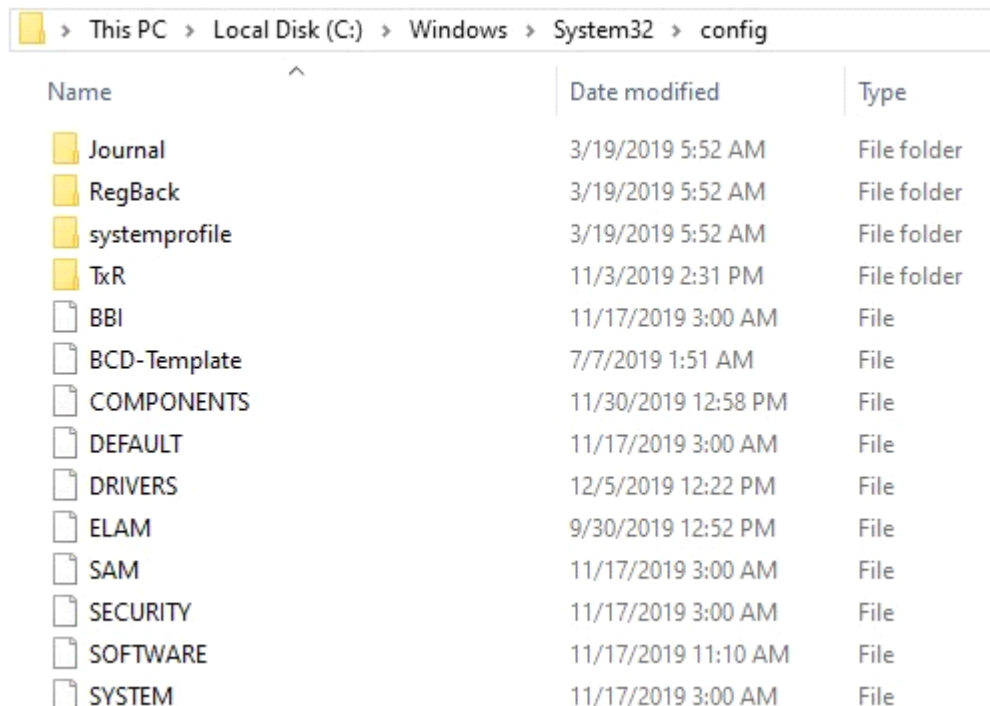
- Applications: info [timestamps, version, ...], settings, options, etc..
- Users: profiles, configs, etc..
- Hardware: serials, state, drivers, etc.

The registry has a hierarchical nature and works with two basic elements which are **Keys** and **Values**:

- Values are non-container objects, similar to ' files '.
- Keys are container objects, similar to ' folders ', so keys can contain subkeys and values.

The most important registry hives are **DEFAULT**, **SAM**, **SECURITY**, **SOFTWARE**, **SYSTEM** they are located under **\Windows\System32\config** and also automatically backed up in

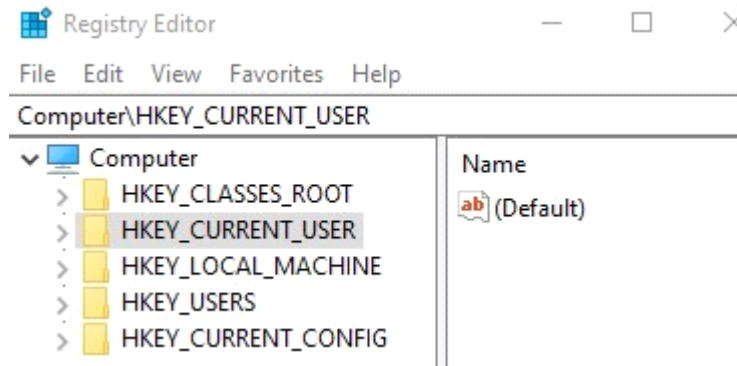
\Windows\System32\config\RegBack. Regback folder is important because most often, attackers who try to cover their tracks and perform anti-forensics techniques like deleting certain keys or purging the registry forget to delete or purge the back up.



This PC > Local Disk (C:) > Windows > System32 > config			
Name		Date modified	Type
Journal		3/19/2019 5:52 AM	File folder
RegBack		3/19/2019 5:52 AM	File folder
systemprofile		3/19/2019 5:52 AM	File folder
TxR		11/3/2019 2:31 PM	File folder
BBI		11/17/2019 3:00 AM	File
BCD-Template		7/7/2019 1:51 AM	File
COMPONENTS		11/30/2019 12:58 PM	File
DEFAULT		11/17/2019 3:00 AM	File
DRIVERS		12/5/2019 12:22 PM	File
ELAM		9/30/2019 12:52 PM	File
SAM		11/17/2019 3:00 AM	File
SECURITY		11/17/2019 3:00 AM	File
SOFTWARE		11/17/2019 11:10 AM	File
SYSTEM		11/17/2019 3:00 AM	File

There are five root keys visible in the registry editor, but today we are going to work with tow:

HKEY_CURRENT_USER and HKEY_LOCAL_MACHINE.



User related forensics

NTUSER.DAT is an important hive that every user has which represents that particular user's registry-related information and it actually plugs in to the registry as HKEY_CURRENT_USER, it's located under **\Users\@username**, . HK_LOCAL_MACHINE on the other hand is formed from the hives mentioned earlier.

```
C:\Users\Emir Fattoum>dir /ah
Volume in drive C has no label.
Volume Serial Number is E2AB-8747

Directory of C:\Users\Emir Fattoum

07/06/2019  05:04 PM  <DIR>          AppData
07/06/2019  05:04 PM  <JUNCTION>     Application Data [C:\Users\Emir Fattoum\AppData\Roaming]
07/06/2019  05:04 PM  <JUNCTION>     Cookies [C:\Users\Emir Fattoum\AppData\Local\Microsoft\Windows\INetCookies]
11/17/2019  11:13 AM  <DIR>          IntelGraphicsProfiles
07/06/2019  05:04 PM  <JUNCTION>     Local Settings [C:\Users\Emir Fattoum\AppData\Local]
07/06/2019  05:08 PM  <DIR>          MicrosoftEdgeBackups
07/06/2019  05:04 PM  <JUNCTION>     My Documents [C:\Users\Emir Fattoum\Documents]
07/06/2019  05:04 PM  <JUNCTION>     NetHood [C:\Users\Emir Fattoum\AppData\Roaming\Microsoft\Windows\Network Short
s]
11/17/2019  11:13 AM           2,883,584  NTUSER.DAT
07/06/2019  05:04 PM           1,224,704  ntuser.dat.LOG1
07/06/2019  05:04 PM           978,944   ntuser.dat.LOG2
07/06/2019  05:07 PM           65,536   NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TM.blf
07/06/2019  05:04 PM           524,288   NTUSER.DAT{fd9a35db-49fe-11e9-aa2c-248a07783950}.TM.Container000000000000000000
```

Usually, if we talk about HKeys we're referring to live system forensics, on the other hand if we talk about hives such as NTUSER.DAT we're referring to forensics of a dead/offline system.

Now Let's grab those hives and dive straight through some very common and basic artifacts. To do that I'm going to use **Registry explorer** to explore through the hives. you can find the tools here <https://ericzimmerman.github.io/#!index.md> .

First, let's start by loading NTUSER.DAT and discuss some artifacts from there.

Registry Explorer v1.5.2.0

File Tools Options Bookmarks (0/0) View Help

Registry hives (1) Available bookmarks (23/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
C:\hives\NTUSER.DAT			2019-12-03 21:15:15
ROOT	0	11	2019-11-17 10:13:35
AppEvents	0	2	2019-07-06 16:04:31
Console	48	2	2019-07-06 16:04:31
Control Panel	1	15	2019-07-08 22:07:55
Environment	6	0	2019-11-24 23:23:18
EUDC	0	4	2019-07-06 16:04:31
Keyboard Layout	0	3	2019-07-06 16:04:31
Network	0	0	2019-07-06 16:04:31
Printers	0	4	2019-09-25 09:35:23
Software	0	33	2019-11-22 20:41:40
System	0	2	2019-07-06 16:07:46
Uninstall	0	0	2019-09-27 15:30:33

Values

Drag a column header here to group by

Value Name	Value Type

Let's navigate to **\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer:**

\ComDlg32:

Here we can find information related to files that are opened or saved via windows explorer style dialogue boxes, for example files (pdf, txt, jpg ...) that are opened/saved from a web browser. The most important subkeys are:

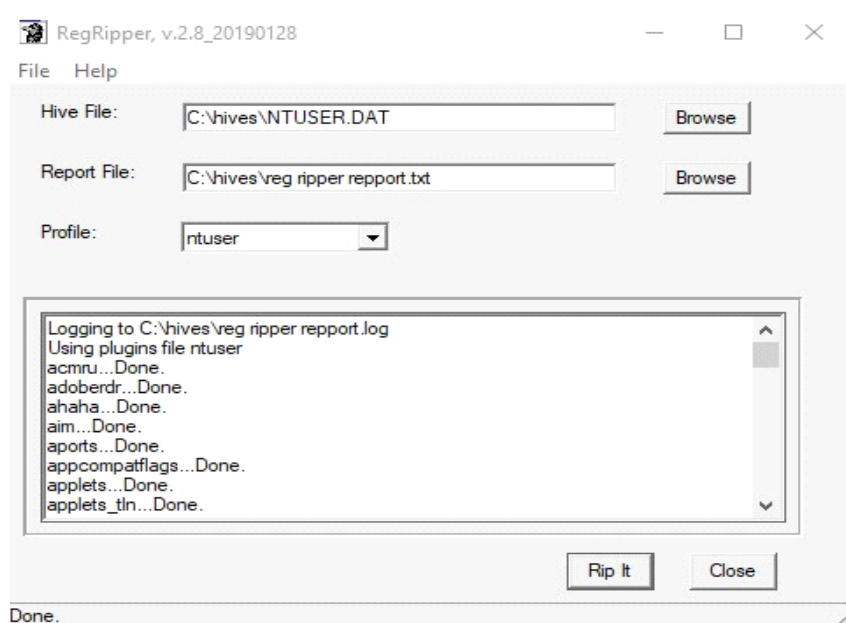
- **\LastVisitedPidlMRU:** which contains the binaries that are used to open or store these files.

*MRU stands for Most Recent Use.

	# values	# subkeys	Last write timestamp
	=	=	=
MountPoints2	0	25	2019-11-18 14:09:29
OperationStatusManager	3	0	2019-12-03 20:49:34
Package Installation	1	0	2019-11-17 10:15:09
RecentDocs	150	45	2019-12-05 14:47:00
.7z	3	0	2019-07-18 13:34:50
.apk	4	0	2019-08-19 12:11:56
.bmp	2	0	2019-11-14 12:28:43
.com/	2	0	2019-07-20 10:23:58
.com/search?q=excel&filters=ufn%3a%22...	1	0	2019-08-21 11:58:09
.csv	3	0	2019-11-17 23:54:29

Extension	Value Name	Value
RecentDocs	RecentDocs	133
.jpg	.jpg	18
Folder	Folder	0
.DAT	.DAT	0
.rtf	.rtf	10
.txt	.txt	16
.rar	.rar	4

There are tools that can parse these types of keys automatically. For example **RegRipper** [<https://github.com/keydet89/RegRipper2.8>]



The results are very clear, this tool event sorts the documents by type / extension


```

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 Thu Dec 5 14:47:00 2019 (UTC)
133 = 4.jpg
2 = The Internet
113 = edit?isTemporary=true&source=screenshot&sharedAccessToken=0400038F-9401-488C-9903-E0E9FC10441A&secondarySharedAccess
05CA-478D-9309-B9C5E17C30AC&viewId=-2034847
31 = hives
29 = NTUSER.DAT
111 = This PC
57 = C:\
110 = Local Disk (C:)
102 = Annotation 2019-12-05 144654.jpg

```

```

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ipynb
LastWrite Time Mon Nov 18 08:06:07 2019 (UTC)
MRUListEx = 1,0
1 = Untitled1 - Copy.ipynb
0 = Untitled1.ipynb

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.iso
LastWrite Time Sun Oct 20 21:23:49 2019 (UTC)
MRUListEx = 3,2,1,0
3 = ubuntu-19.04-live-server-amd64.iso
2 = en_windows_10_multiple_editions_x64_dvd_6846432.iso
1 = Windows10.iso
0 = kali-linux-2019.2-amd64.iso

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jar
LastWrite Time Wed Sep 25 10:33:12 2019 (UTC)
MRUListEx = 2,1,0
2 = jython-installer-2.7.1.jar
1 = burpsuite_community_v2.1.01.jar
0 = jython-installer-2.7.0.jar

```

\RunMRU: This one contains the most recent programs executed and their order

search...	Find	Drag a column header here to group by that column	
	# values	# subkeys	Last write timestamp
Taskband	5	1	2019-12-03 22:45:08
TWinUI	0	1	2019-08-20 14:11:27
TypedPaths	0	0	2019-07-06 17:44:01
User Shell Folders	20	0	2019-07-06 16:04:31
UserAssist	0	9	2019-07-06 16:07:41
{9E04CAB2-CC14-11DF-BB8C-A2F1DED720...}	1	1	2019-07-06 16:07:41
Count	1	0	2019-12-04 11:40:52
{A3D53349-6E61-4557-8FC7-0028EDCEE...}	1	1	2019-07-06 16:07:41
Count	1	0	2019-12-04 11:40:52
{B267E3AD-A825-4A09-82B9-EEC22AA3B8...}	1	1	2019-07-06 16:07:41
Count	0	0	2019-07-06 16:07:41
{BCB48336-4DDD-48FF-BB0B-D3190DACB3...}	1	1	2019-07-06 16:07:41
Count	1	0	2019-12-04 11:40:52
{CAA59E3C-4792-41A5-9909-6A6A8D3249...}	1	1	2019-07-06 16:07:41
Count	1	0	2019-12-04 11:40:52
{CEBFF5CD-ACE2-4F4F-9178-9926F41749E...}	1	1	2019-07-06 16:07:41
Count	106	0	2019-12-05 15:14:29
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D4...}	1	1	2019-07-06 16:07:41
Count	1	0	2019-12-04 11:40:52
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9...}	1	1	2019-07-06 16:07:41
Count	39	0	2019-12-05 13:51:26
{F400DE07-6A02-4E2A-A5E3-EE3A5E4507...}	1	1	2019-07-06 16:07:41

Program Name	Run Counter
{Programs}\System Tools\Command Prompt.Ink	1
{User Pinned}\TaskBar\Registry Editor.Ink	1
{Common Programs}\Administrative Tools\Registry Editor.Ink	0
C:\Users\Public\Desktop\Google Chrome.Ink	0
{Programs}\Slack Technologies Inc\Slack.Ink	0
{User Pinned}\TaskBar\Task Manager.Ink	0
{Common Programs}\JetBrains\JetBrains PyCharm Community Edition 2019.2.4.Ink	0
{Programs}\Anaconda3 (64-bit)\Anaconda	0
Total rows: 39	
Type viewer	Slack viewer
00000000	00 01 02 03 04 05 06 07 0
	13 00 00 00 00 00 00 00 0

Next let's check **\SOFTWARE\Microsoft\Windows\CurrentVersion\Run & ~\RunOnce:**

These keys provide us with information regarding applications that starts automatically with system, even in the background.

Key name	# values	# subkeys	Last write timestamp
Run	5	0	
RunOnce	4	0	
Screensavers	0	4	
Search	16	5	
Security and Maintenance	1	2	
SettingsSync	4	1	

Value Name	Value Type	Data
com.squirrel.slack.slack	RegSz	"C:\Program Files\Slack\slack.exe"
Discord	RegSz	"C:\Program Files\Discord\Discord.exe"
OneDrive	RegSz	"C:\Program Files\OneDrive\OneDrive.exe"
ProtonVPN	RegSz	"C:\Program Files\ProtonVPN\ProtonVPN.exe"
SurfEasy	RegSz	"C:\Program Files\SurfEasy\SurfEasy.exe"

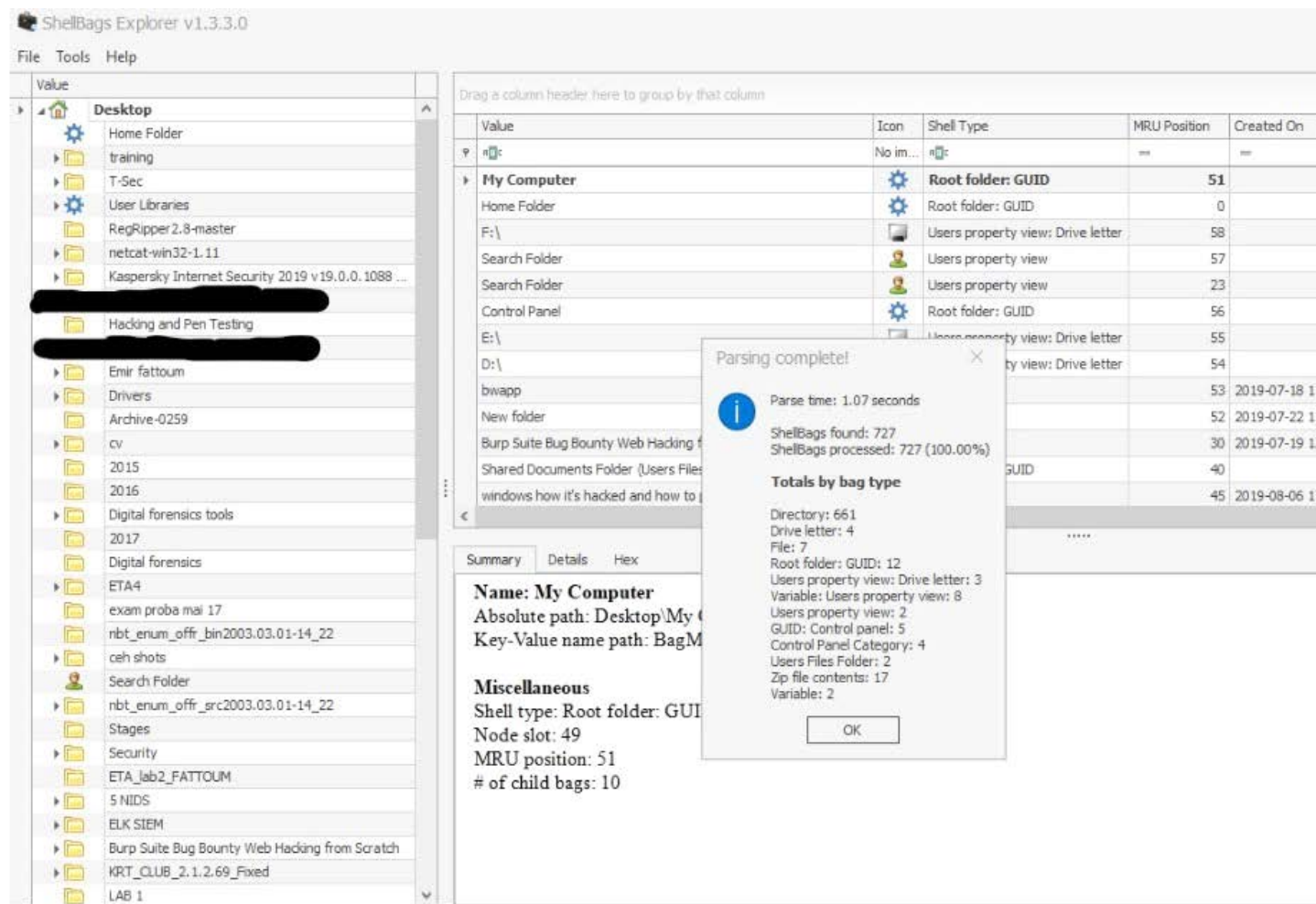
Next, I'm going to briefly introduce **Shellbags:**

- Shellbags are registry keys that basically store details about a viewed folder when viewed through windows explorer such as the view, the icons, the size, the window position, the sorting method, etc. ... This also include network folders and removable devices.

- Shellbags are important from an investigators perspective because they persist even after the folder is deleted from the system, which gives great insight about the browsing history and content of folders

that are no longer accessible (located in removable device or even deleted).

For shellbags we're going to use **ShellBags Explorer** [from the same source as Registry explorer]
This is the initial window that shows information regarding the parsed shellbags.



As we can see below, the left side panel shows the contents of the shellbags. For example, the drive in green is actually a USB flash drive that I used on my machine recently and the folder in yellow is one that was deleted ages ago.

Value

Security
ETA_Jab2_FATTOUM
5 NIDS
ELK SIEM
Burp Suite Bug Bounty Web Hacking from Scratch
LAB 1
IOT security
Me
tools
e learnin
Burp_Suite_Pro_v2.0.11
BurpSuite 1.7.35 Pro.zip
Shared Documents Folder (Users Files)
ETA
Computers and Devices
windows how it's hacked and how to protect it
books
Os
Ethical Hacking - Buffer Overflow.zip
Pentester Academy - Python For Pentesters
My Computer
New folder
bwapp
D:
E:\
Control Panel
Search Folder
F:\

Drag a column header here to group by that column

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First I...	Last Inte
trage		Directory	4	2019-08-17 09:54:42	2019-08-17 10:01:18	2019-08-17 10:01:18		
LAB 1		Directory	7	2019-10-01 12:38:12	2019-10-01 12:38:12	2019-10-01 12:38:10		
Ubuntu server 64-b		Directory	6	2019-10-01 12:58:52	2019-09-12 09:59:26	2019-09-30 23:00:00		
REM		Directory	5	2019-10-24 22:55:12	2019-10-24 23:32:22	2019-10-25 00:34:24		
Sense8		Directory	3	2019-09-25 12:22:20	2019-09-26 10:26:16	2019-09-26 10:26:16		
E		Directory	2	2019-07-04 20:58:36	2019-07-04 20:59:22	2019-07-21 21:47:18		
REM VM_Digital_Forensics		Directory	1	2019-01-29 09:14:58	2019-01-29 10:27:02	2019-01-29 10:27:02		
		Directory	0	2019-11-14 14:05:04	2019-11-14 14:06:52	2019-11-14 14:06:52		

Summary

Details

Hex

Name: LAB 1
Absolute path: Desktop\D:\LAB 1
Key-Value name path: BagMRU\7-2

Target timestamps
Created on: 2019-10-01 12:38:12.000
Modified on: 2019-10-01 12:38:12.000
Last accessed on: 2019-10-01 12:38:10.000

Miscellaneous
Shell type: Directory
Node slot: 504
MRU position: 7
of child bags: 1

Active Registry loaded in 1.0678 seconds! 9 shellbags loaded in 0.0062 seconds Time zone: UTC

System forensics

USB forensics

USB forensics is very important, they can be used to steal sensitive data from companies by a recently fired employee for example, inject malware, break into a system once physical access is gained and many more possible scenarios.

After loading the SYSTEM hive, let's take a look under **\USBSTOR** and **\USB** keys located under **\SYSTEM\ControlSet001\Enum**.

Under **\USBSTOR** we can see a list of thumb drives that were used in this machine

USBSTOR			
CdRom&Ven_HUAWEI&Prod_Mass_Storage&Rev_2.31	0	5	2019-12-05 10:36:31
Disk&Ven_G_&T&Prod_USB_Flash_Drive&Rev_8.07	0	1	2019-11-18 14:09:25
Disk&Ven_HUAWEI&Prod_TF_CARD_Storage&Rev_2.31	0	1	2019-11-18 08:24:33
Disk&Ven_SanDisk&Prod_Cruzer_Switch&Rev_1.00	0	1	2019-11-18 14:09:25
Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00	0	1	2019-09-30 20:30:40
	0	1	2019-12-05 10:36:30

I plugged a flash drive just before I was making this part, if we expand further, as seen below. The number in yellow corresponds to the serial number of the flash drive. Correspondingly we can see a time stamp that is recorded in UTC (windows always use UTC in records),so we need to convert it to local time so that we can build an event line or a chain of events . In red is the name of the flash drive. As you can see, a lot of readable and useful information.

	# values	# subkeys	Last write timestamp	Value Name	Value Type
USB	0	17	2019-12-05 10:36:31	Address	RegDword
USBSTOR	0	5	2019-12-05 10:36:31	Capabilities	RegDword
CdRom&Ven_HUAWEI&Prod_Mass_Storage&Rev_2.31	0	1	2019-11-18 14:09:25	ClassGUID	RegSz
Disk&Ven_G_&_T&Prod_USB_Flash_Drive&Rev_8.07	0	1	2019-11-18 08:24:33	CompatibleIDs	RegMultiSz
Disk&Ven_HUAWEI&Prod_TF_CARD_Storage&Rev_2.31	0	1	2019-11-18 14:09:25	ConfigFlags	RegDword
Disk&Ven_SanDisk&Prod_Cruzer_Switch&Rev_1.00	0	1	2019-09-30 20:30:40	ContainerID	RegSz
Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00	0	1	2019-12-05 10:36:30	DeviceDesc	RegSz
4C531001490511103221&0	12	2	2019-12-06 12:06:23	Driver	RegSz
Device Parameters	0	2	2019-07-06 23:51:49	FriendlyName	RegSz
Properties	0	5	2019-07-06 16:02:45	HardwareID	RegMultiSz
Hardware Profiles	0	2	2019-11-17 10:10:18	Mfg	RegSz
Policies	0	0	2019-03-19 04:53:37	Service	RegSz
Services	0	752	2019-12-04 02:38:59		
Software	0	1	2019-03-19 04:53:37		

Under \USB we can see the VID and PID that corresponds to the serial number, google can find more information about the make, model and even pictures. This will help us pinpoint the physical USB device that can be used later as evidence.

USB	0	17	2019-12-05 10:36:31
ROOT_HUB30	0	1	2019-12-05 10:36:30
VID_04F2&PID_B5AB	0	1	2019-07-06 23:51:50
VID_04F2&PID_B5AB&MI_00	0	1	2019-07-06 23:51:50
VID_058F&PID_6387	0	1	2019-12-05 10:36:29
VID_0781&PID_5572	0	1	2019-09-30 20:30:40
VID_0781&PID_5581	0	1	2019-07-06 23:51:49
4C531001490511103221	12	2	2019-12-06 12:06:23
VID_0BDA&PID_0316	0	1	2019-07-06 23:51:49

usb.userbenchmark.com/SpeedTest/2009/SanDisk-SanDisk-Ultra

UserBenchmark TUN-User US


CPU GPU SSD HDD RAM **USB** FPS

SANDISK SDCZ48-064G (Flash)

Ultra USB 3.0 64GB

BENCHMARKS (8,750) (0) BUY • \$11

50
14



Effective Speed -51%
Effective Speed -51%

Peak Lab Bench -55%
Read -9%, Write -58%, 4K Read -52%, 4K Write -51%

Value & Sentiment +91% ✓
User Rating -34%, Price 160%, Value 147%

Nice To Haves +5% ✓
Age 5%

Release date ≤ Q4 2013.

16GB 32GB 64GB

← → ↻ 🏠 ⓘ Not secure | usbspeed.nirsoft.net/?o=78&vname=&&vid=19218&pid=21889

Product Name	Vendor Name	Drive Size	VID	PID	Real Size
SanDisk Ultra USB Device	SanDisk Corp.	14.53 GB	781	5581	37.20
SanDisk Ultra USB Device	SanDisk Corp.	116.25 GB	781	5581	36.25
SanDisk Ultra USB Device	SanDisk Corp.	232.29 GB	781	5581	39.33
SanDisk Ultra USB Device	SanDisk Corp.	7.43 GB	781	5581	21.08

Under **\SYSTEM\MountedDevices**

There is details about the flash drive and the drive letter associated with it

Device Name	Device Data
\DosDevices\C:	DMIO:ID: 00000000, 00000000, 00000000, 00000000
\\?\Volume{6690f0c5-a051-11e9-9a38-806e6f6e6963}	{6690f0bf-a051-11e9-9a38-806e6f6e6963}
\\?\Volume{6690f0cb-a051-11e9-9a38-806e6f6e6963}	{6690f0ca-a051-11e9-9a38-806e6f6e6963}
\DosDevices\D:	\\?_USBSTOR#Disk&8b}
\DosDevices\F:	\\.\iv ~
\\?\Volume{02ebca04-a01b-11e9-9a3f-005056c00008}	{6690f0bf-a051-11e9-9a38-806e6f6e6963}
\\?\Volume{02ebca05-a01b-11e9-9a3f-005056c00008}	{6690f0bf-a051-11e9-9a38-806e6f6e6963}
\\?\Volume{02ebca6c-a01b-11e9-9a3f-005056c00008}	{6690f0bf-a051-11e9-9a38-806e6f6e6963}
\\?\Volume{a223504e-a2a3-11e9-9a43-54e1ad8b98bf}	\\?_USBSTOR#CdRom&1d0-94f2-00a0c91efb}
\\?\Volume{a223504f-a2a3-11e9-9a43-54e1ad8b98bf}	\\?_USBSTOR#Disk&Vf-11d0-94f2-00a0c91efb}
\\?\Volume{a223507d-a2a3-11e9-9a43-54e1ad8b98bf}	\\?_USBSTOR#Disk&Vf-11d0-94f2-00a0c91efb}

But the most important thing here is we get the Volume GUID related to the flash drive as we can see below in red. The **Volume GUID** is a unique identifier assigned by windows the first time it encounters a new volume and it does not change even if the drive letter is changed. This is useful to track the activities of the USB in the system.

Values	MountedDevices														
Drag a column header here to group by that column															
	Value Name	Value Type	Data	Data Record Realloc...	Is Deleted										
▼	RegBinary	RegBinary	RegBinary	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{02ebca04-a01b-11e9-9a3f-005056c00008}	RegBinary	7B-00-36-00-36-00-3...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{02ebca05-a01b-11e9-9a3f-005056c00008}	RegBinary	7B-00-36-00-36-00-3...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{02ebca6c-a01b-11e9-9a3f-005056c00008}	RegBinary	7B-00-36-00-36-00-3...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{053b8828-e372-11e9-9a4f-f85971520f02}	RegBinary	5F-00-3F-00-3F-00-5...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{053b88a1-e372-11e9-9a4f-f85971520f02}	RegBinary	5F-00-3F-00-3F-00-5...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{053b8a8c-e372-11e9-9a4f-f85971520f02}	RegBinary	5F-00-3F-00-3F-00-5...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{053b9187-e372-11e9-9a4f-f85971520f02}	RegBinary	5C-00-3F-00-3F-00-5...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{2d9e10cb-a950-11e9-9a44-54e1ad8b98bf}	RegBinary	5C-00-3F-00-3F-00-5...	<input type="checkbox"/>	<input type="checkbox"/>										
▶	\\??\Volume{2d9e1b19-a950-11e9-9a44-54e1ad8b98bf}	RegBinary	5F-00-3F-00-3F-00-5...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{4da2bffa-099d-11ea-9a54-54e1ad8b98bf}	RegBinary	5F-00-3F-00-3F-00-5...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{4da2c6b9-099d-11ea-9a54-54e1ad8b98bf}	RegBinary	5C-00-3F-00-3F-00-5...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{4da2c6bc-099d-11ea-9a54-54e1ad8b98bf}	RegBinary	5F-00-3F-00-3F-00-5...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{6690f0c5-a051-11e9-9a38-806e6f6e6963}	RegBinary	7B-00-36-00-36-00-3...	<input type="checkbox"/>	<input type="checkbox"/>										
	\\??\Volume{6690f0cb-a051-11e9-9a38-806e6f6e6963}	RegBinary	7B-00-36-00-36-00-3...	<input type="checkbox"/>	<input type="checkbox"/>										

.....

Type viewer	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A
00000000	5F	00	3F	00	3F	00	5F	00	55	00	53	00	42	00	53	00	54	00	4F	00	52	00	23	00	44	00	69
00000018	00	73	00	68	00	26	00	56	00	65	00	6E	00	5F	00	53	00	61	00	6E	00	44	00	69	00	73	00
00000036	68	00	26	00	50	00	72	00	6F	00	64	00	5F	00	55	00	6C	00	74	00	72	00	61	00	26	00	52
00000051	00	65	00	76	00	5F	00	31	00	2E	00	30	00	30	00	23	00	34	00	43	00	35	00	33	00	31	00
0000006C	30	00	30	00	31	00	34	00	39	00	30	00	35	00	31	00	31	00	31	00	30	00	33	00	32	00	32
00000087	00	31	00	26	00	30	00	23	00	78	00	35	00	33	00	66	00	35	00	36	00	33	00	30	00	37	00
000000A2	2D	00	62	00	36	00	62	00	66	00	2D	00	31	00	31	00	64	00	30	00	2D	00	39	00	34	00	66
000000BD	00	32	00	2D	00	30	00	30	00	61	00	30	00	63	00	39	00	31	00	65	00	66	00	62	00	38	00
000000D8	62	00	7D	00																							

Searching for matches for the Volume GUID in NTUSER.DAT hives, of all existing users, under **\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Mountpoints2**, can give us the exact user that mounted the USB drive and the last time he did that. We can also use the search box of Registry Explorer to do the job:

Registry hives (3)		Available bookmarks (68/0)		
{2d9e1b19-a950-11e9-9a44-54e1ad8b98bf}		Find		
Key name	# values	# subkeys	Last write timestamp	
C:\hives\NTUSER.DAT	=	=	2019-12-06 15:57:17	
ROOT	0	11	2019-11-17 10:13:35	
Software	0	33	2019-11-22 20:41:40	
Microsoft	0	79	2019-12-06 14:38:48	
Windows	0	7	2019-07-06 16:08:11	
CurrentVersion	0	62	2019-08-19 10:42:07	
Explorer	16	48	2019-12-06 15:25:21	
MountPoints2	0	25	2019-11-18 14:09:25	
{2d9e1b19-a950-11e9-9a44-54e1ad8b98bf}	0	1	2019-12-06 12:06:23	

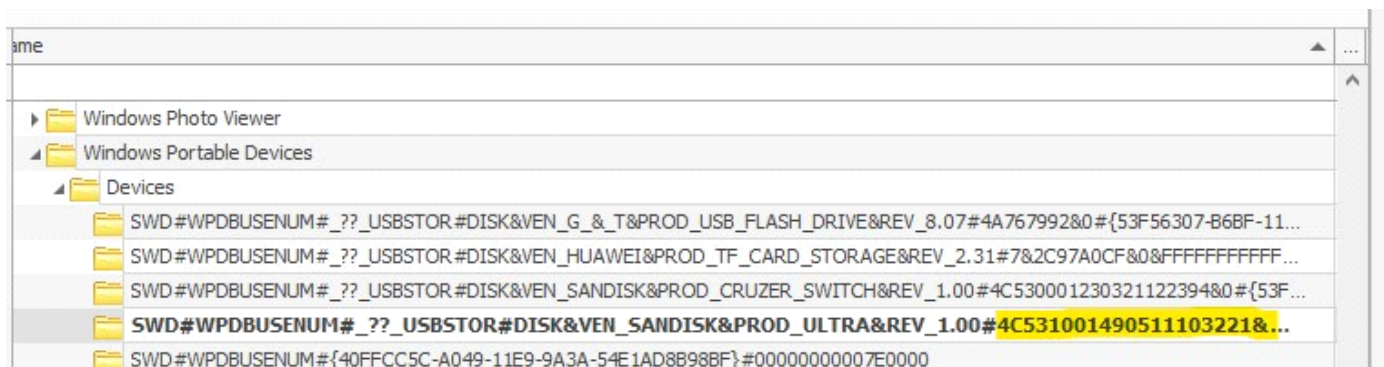
Another Bonus, in SYSTEM hive, under
`\SYSTEM\CurrentSet00X\Enum\USBSTOR\Ven_Prod_Version\"@targetUSBSerial"\Properties\"@Target_Volume_GUID\"`

we can find important timestamps:

- 0064 => The first time the USB was plugged in.
- 0066 => The Last time the USB was plugged in.
- 0067 => The Last time the USB was removed/disconnected.

USBSTOR	0	5	2019-12-05 10:36:31
CdRom&Ven_HUAWEI&Prod_Mass_Storage&Rev_2.31	0	1	2019-11-18 14:09:25
Disk&Ven_G_&T&Prod_USB_Flash_Drive&Rev_8.07	0	1	2019-11-18 08:24:33
Disk&Ven_HUAWEI&Prod_TF_CARD_Storage&Rev_2.31	0	1	2019-11-18 14:09:25
Disk&Ven_SanDisk&Prod_Cruzer_Switch&Rev_1.00	0	1	2019-09-30 20:30:40
Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00	0	1	2019-12-05 10:36:30
4C531001490511103221&0	12	2	2019-12-06 12:06:23
Device Parameters	0	2	2019-07-06 23:51:49
Properties	0	5	2019-07-06 16:02:45
{3464f7a4-2444-40b1-980a-e0903cb6d912}	0	1	2019-07-06 16:02:45
{80497100-8c73-48b9-aad9-ce387e19c56e}	0	1	2019-07-06 23:51:49
{540b947e-8b40-45bc-a8a2-6a0b894cbda2}	0	2	2019-07-06 23:51:49
{83da6326-97a6-4088-9453-a1923f573b29}	0	6	2019-07-06 16:47:02
0003	1	0	2019-07-06 23:51:49
000A	1	0	2019-07-06 23:51:49
0064	1	0	2019-07-06 23:51:49
0065	1	0	2019-07-06 23:51:49
0066	1	0	2019-12-06 12:06:23
0067	1	0	2019-12-06 12:06:51

Under **Software\Microsoft\Windows Portable Devices\Devices**: We can see the serial number & the volume name of the USB device



Again, such information can be retrieved automatically by other tools but it's important to know where it is in the registry and retrieve it manually.

For example, **USB Historian** can retrieve useful information on the fly.

 USB Historian v1.3



Friendly Name	Serial No	Mount Point 2	D...	Usb Stor DateTime	Vendor	Product
G & T USB Flash Drive USB Device	4A767992	[Emir Fattoum:11/18/2019 10:00:50 AM]		11/18/2019 10:00:44 AM	Ven_G_&_T	Prod_USB...
HUAWEI TF CARD Storage USB Device	7&2c97a0cf&0&FFFFFFFFF...	[Emir Fattoum:11/18/2019 2:13:03 PM]	E:	11/18/2019 2:12:19 PM	Ven_HUAWEI	Prod_TF_C...
SanDisk Cruzer Switch USB Device	4C530001230321122394	[Emir Fattoum:11/26/2019 9:03:28 AM]		11/26/2019 8:59:00 AM	Ven_SanDisk	Prod_Cruze...
SanDisk Ultra USB Device	4C531001490511103221	[Emir Fattoum:11/23/2019 9:19:51 PM]	D:	12/6/2019 12:06:23 PM	Ven_SanDisk	Prod_Ultra...

Miscellaneous info

Time zone information

First of all, it's recommended to record the system time zone at the very beginning of the analysis so that any time related information or events extracted during the investigation are accurate. We can find this information under **\SYSTEM\ControlSet001\Control\TimeZoneInformation**.

ServiceGroupList	1	0	2019-03-19 04:53:38	StandardBias	0
SQMServiceList	1	0	2019-03-19 04:53:38	StandardName	@tzr
SrpExtensionConfig	1	0	2019-03-19 04:53:38	StandardStart	Mont of we Hour ds 0:
StorPort	0	0	2019-07-06 23:52:40	TimeZoneKeyName	W. C
TimeZoneInformation	10	0	2019-07-09 23:45:45	ActiveTimeBias	-60
Ubp	63	0	2019-03-19 04:53:38		
WalletService	1	0	2019-03-19 04:53:38		
Windows	11	0	2019-11-17 02:00:12		

Computer Name

It's also logical to grab the computer name of the machine being analyzed. we can find that under **\SYSTEM\ControlSet001\Control\ComputerName\ComputerName**.

	# values	# subk	Value Name	Value Type	Data
ne	=	=	Reg	Reg	Reg
CommonGlobUserSettings	0		(default)	RegSz	mnmsrvc
Compatibility	0		ComputerName	RegSz	DESKTOP
ComputerName	0				
ComputerName	2				
ContentIndex	0				

Network Interfaces

Interfaces, Configuration can be found under **\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces**

search...		▼	Find
	# v...	...	Last write timestamp
	=		=
Tcpip	13	5	2019-07-06 23:51:49
Linkage	3	0	2019-12-06 01:09:09
Performance	5	0	2019-03-19 04:53:37
Security	0	0	2019-03-19 04:53:37
ServiceProvider	7	0	2019-03-19 04:53:37
Parameters	9	6	2019-12-06 10:47:11
DNSRegisteredAdapters	0	0	2019-07-06 23:52:03
NsiObjectSecurity	0	0	2019-03-19 04:53:37
PersistentRoutes	0	0	2019-03-19 04:53:37
Winsock	7	3	2019-03-19 04:56:18
Adapters	0	9	2019-12-06 01:09:09
Interfaces	0	10	2019-12-06 01:09:09
{17f1755b-b707-4b36-9434-3195d8...	17	0	2019-08-20 14:19:27
{32e01af7-13c9-43a6-856e-55cd68c7aa32}	3	0	2019-09-11 17:10:00
{429a1556-2f87-4fa0-a19c-6b79dd889f5c}	21	0	2019-12-06 10:35:43
{624d1b46-3a56-4cd9-ac48-9328788086a7}	16	0	2019-12-06 12:02:11
{6690f0bc-a051-11e9-9a38-806e6f6e6963}	0	0	2019-07-06 23:52:01
{7f7ce920-d426-4608-904a-cfd2bdd03c14}	3	0	2019-07-06 23:52:04
{85f240ef-28cb-4415-8721-7a20db315f38}	16	0	2019-12-06 12:02:11
{b6b86645-d1f3-47f9-b77f-351e70edcbaa}	3	0	2019-07-06 23:51:53
{c1684c6b-54b1-4a68-97eb-9ac4444b16dd}	21	0	2019-08-06 15:43:48
{f1e4de88-5511-466a-bae0-e333f766fd40}	15	0	2019-11-02 23:57:03
TPHKI QAD	9	5	2019-08-27 16:56:28

Drag a column header here to group by that column			
Value Name	V...	Data	
AddressType	R...	0	
DhcpConnForceBroadcastFlag	R...	0	
DhcpInterfaceOptions	R...	FC-00-00-00-00-00	
DhcpIPAddress	R...	100.127.255.253	
DhcpNameServer	R...	8.8.8.8	
DhcpServer	R...	100.127.255.254	
DhcpSubnetMask	R...	255.255.255.252	
DhcpSubnetMaskOpt	R...	255.255.255.252	
Domain	R...		
EnableDHCP	R...	1	
IsServerNapAware	R...	0	
Lease	R...	31536000	
LeaseObtainedTime	R...	1566310767	
LeaseTerminatesTime	R...	1597846767	
NameServer	R...		
T1	R...	1582078767	
T2	R...	1593904767	

Wireless Network Listing

Under **\Software\Microsoft\Windows NT\Currentversion\Networklist**, we can find all the Networks that this machine has ever connected to:

WinPrefetchView

File Edit View Options Help

Filename	Created Time	Modified Time	File Size	Process EXE
AM_DELTA_PATCH_1.305.3464.0.E-553C0FAF.pf	12/6/2019 6:44:14 PM	12/6/2019 6:44:14 PM	2,171	AM_DELTA_PATCH_1.305.3464.0.E-553C0FAF.EXE
AM_DELTA.EXE-3A6EE7FD.pf	12/6/2019 4:30:47 PM	12/6/2019 4:30:47 PM	2,169	AM_DELTA.EXE
RUNTIMEBROKER.EXE-F1DFDEE1.pf	12/6/2019 3:35:47 PM	12/6/2019 3:35:47 PM	4,940	RUNTIMEBROKER.EXE
USB HISTORIAN.EXE-73303047.pf	12/6/2019 2:26:05 PM	12/6/2019 2:26:05 PM	27,938	USB HISTORIAN.EXE
NGENTASK.EXE-CD4E002C.pf	12/6/2019 2:15:45 PM	12/6/2019 2:15:45 PM	19,179	NGENTASK.EXE
NGENTASK.EXE-4DB88ADA.pf	12/6/2019 2:15:44 PM	12/6/2019 2:15:44 PM	16,390	NGENTASK.EXE
WUDFHOST.EXE-0D78D366.pf				WUDFHOST.EXE
SVCHOST.EXE-BE1C404C.pf				SVCHOST.EXE
NETCFGNOTIFYOBJECTHOST.EXE-A0C34613.pf				NETCFGNOTIFYOBJECTHOST.EXE
DLLHOST.EXE-D6E392F8.pf				DLLHOST.EXE
SHELLBAGSEXPLORER.EXE-03C94C75.pf				SHELLBAGSEXPLORER.EXE
DLLHOST.EXE-50DEE1CF.pf				DLLHOST.EXE
RR.EXE-DADD85EF.pf				RR.EXE
DLLHOST.EXE-5C94BCB3.pf				DLLHOST.EXE
CMD.EXE-CD245F9E.pf				CMD.EXE

Properties

Filename: USB HISTORIAN.EXE-73303047.pf

Created Time: 12/6/2019 2:26:05 PM

Modified Time: 12/6/2019 2:26:05 PM

File Size: 27,938

Process EXE: USB HISTORIAN.EXE

Process Path: C:\USERS\EMIR FATTOUM\DESKTOP\USB_HISTORI...

Run Counter: 3

Last Run Time: 12/6/2019 2:25:55 PM

Missing Process: Yes

OK

Filename	Full Path
SMFT	C:\Windows\System32\smft.dll
ACCESSIBILITY.NI.DLL	C:\Windows\assembly\X-MSDN\SHELL32\65958641-88E0-4362-B317-82E6B3D1243D\ACCESSIBILITY.NI.DLL
ACCESSIBILITY.NI.DLL...	C:\Windows\assembly\X-MSDN\SHELL32\65958641-88E0-4362-B317-82E6B3D1243D\ACCESSIBILITY.NI.DLL
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll
AMSI.DLL	C:\Windows\System32\amsi.dll
APPHELP.DLL	C:\Windows\System32\apphelp.dll
BCRYPT.DLL	C:\Windows\System32\bcrypt.dll
BCRYPTPRIMITIVES.DLL	C:\Windows\System32\BCRYPTPRIMI...
CFGMR32.DLL	C:\Windows\System32\cfgmgr32.dll