Forensics: A Quick Dive into Windows Registry

Introduction

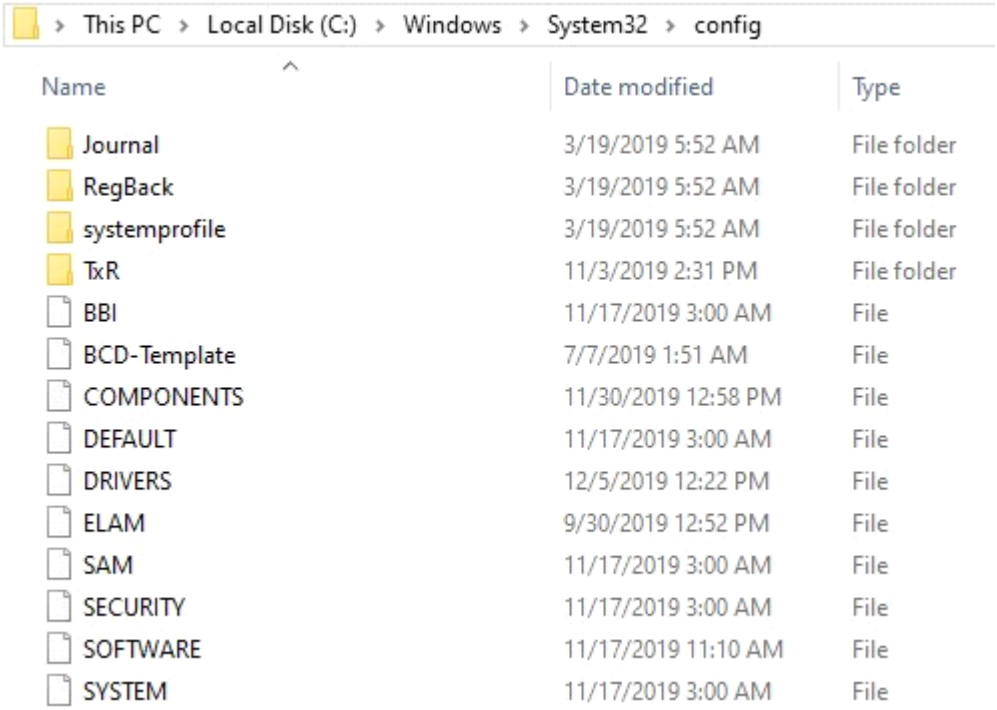
Window registry is more like a database, one that stores all kinds of information that are vital to the proper functioning of the operating system. Information related to:

- 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**:

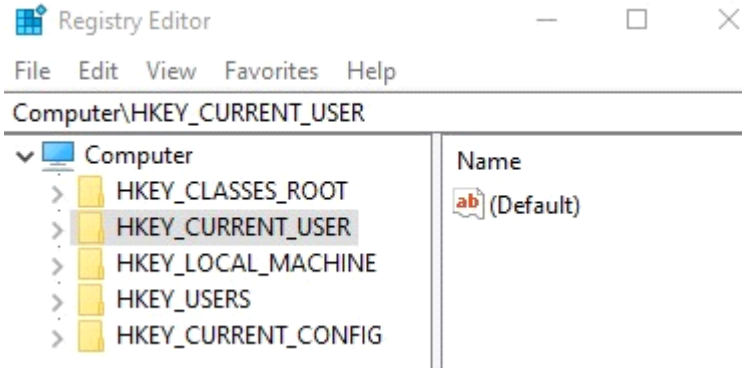
- Values are non-container objects, similar to ' files '.
- Keys are container objects, similar to ' folders ', so keys can contain subkeys and values.

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.



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

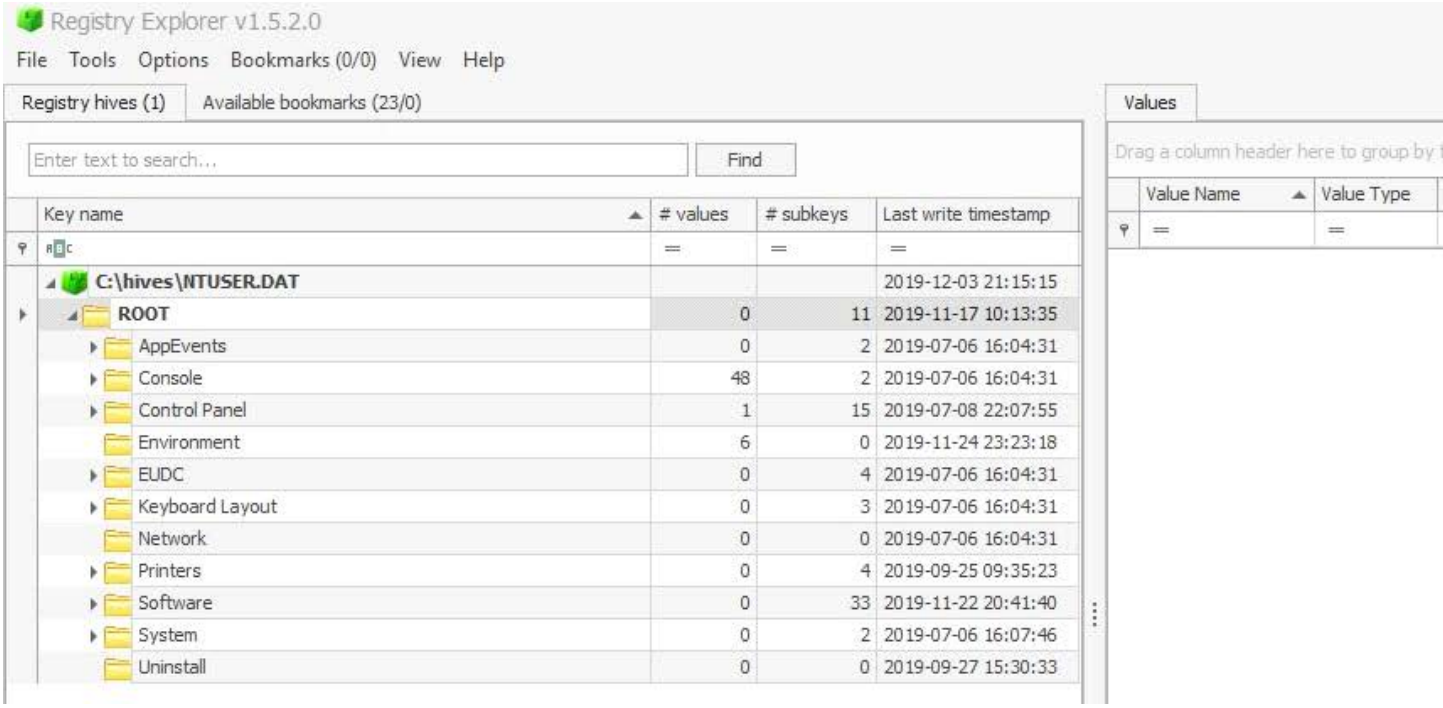
NTUSER.DAT is an important hive that every user has which represents that particular user's registry-related information and it actually plugs in to the registry as HKEY_CURRENT_USER, it's located under **\Users\@username**, . HK_LOCAL_MACHINE on the other hand is formed from the hives mentioned earlier.

```
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}.TMContainer00000000000000000000
```

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.



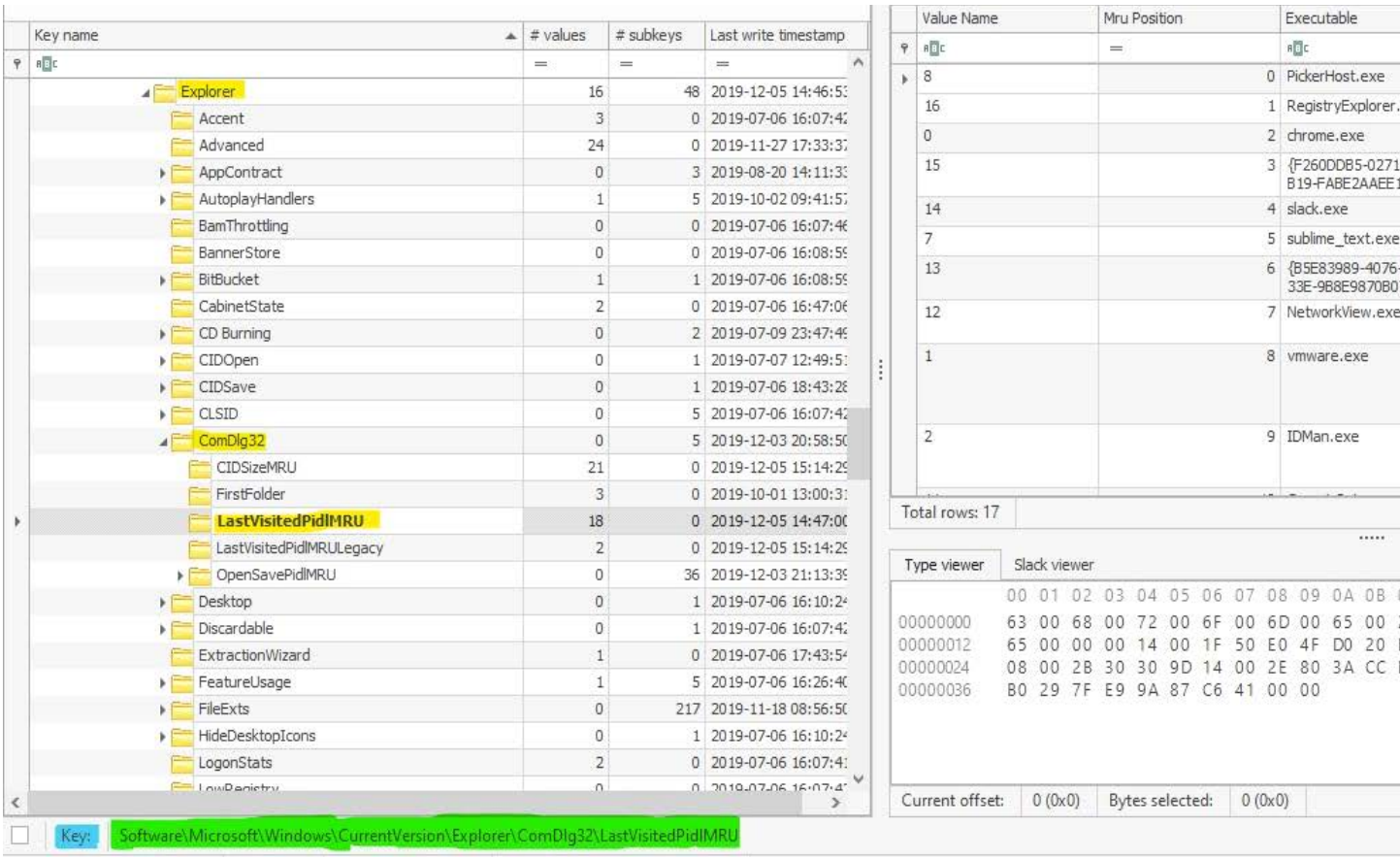
Let's navigate to **\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer:**

\ComDlg32:

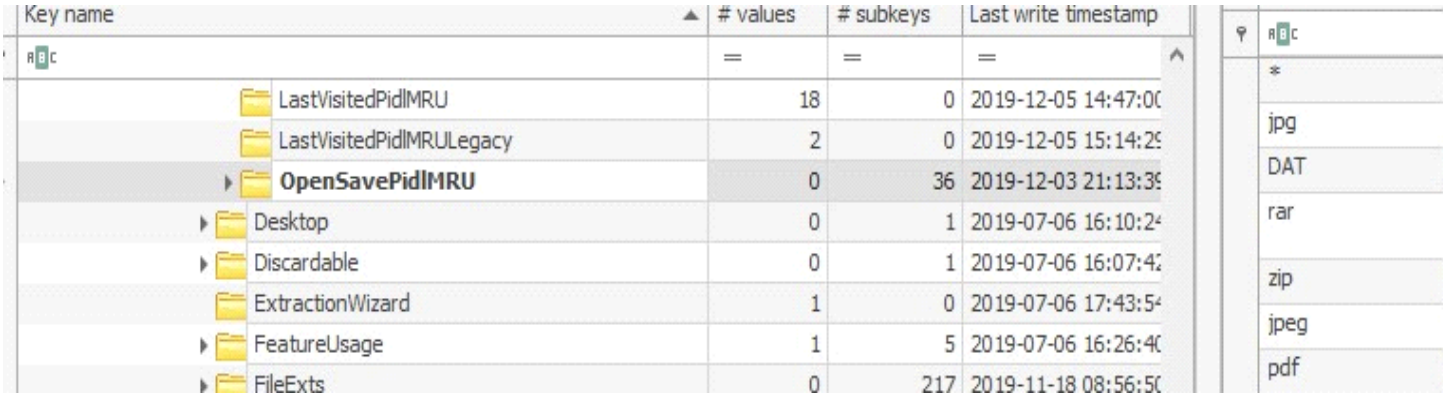
Here we can find information related to files that are opened or saved via windows explorer style dialogue boxes, for example files (pdf, txt, jpg ,..) that are opened/saved from a web browser. The most important subkeys are:

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

*MRU stands for Most Recent Use.



- **\OpenSavedPidlMRU**: contains the files themselves:



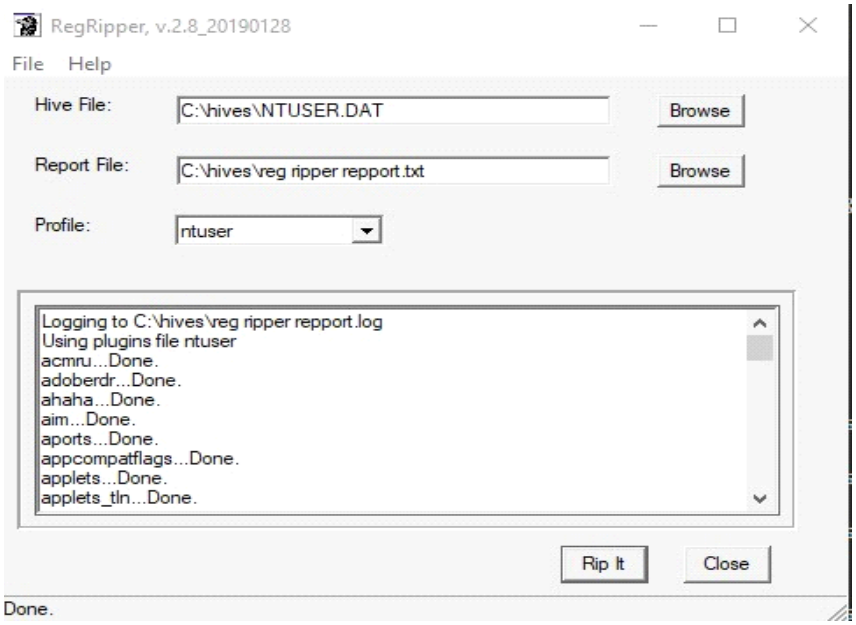
\RecentDocs:

This key shows recent documents that interacted with the system whether opened or saved.

	# values	# subkeys	Last write timestamp
MountPoints2	0	25	2019-11-18 14:09:25
OperationStatusManager	3	0	2019-12-03 20:49:34
Package Installation	1	0	2019-11-17 10:15:05
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 23:54:25

Extension	Value Name	Ta
RecentDocs	133	4.
.jpg	18	4.
Folder	0	Th
.DAT	0	NT
.rtf	10	W fo pa
.txt	16	Ne Do
.rar	4	FO W

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

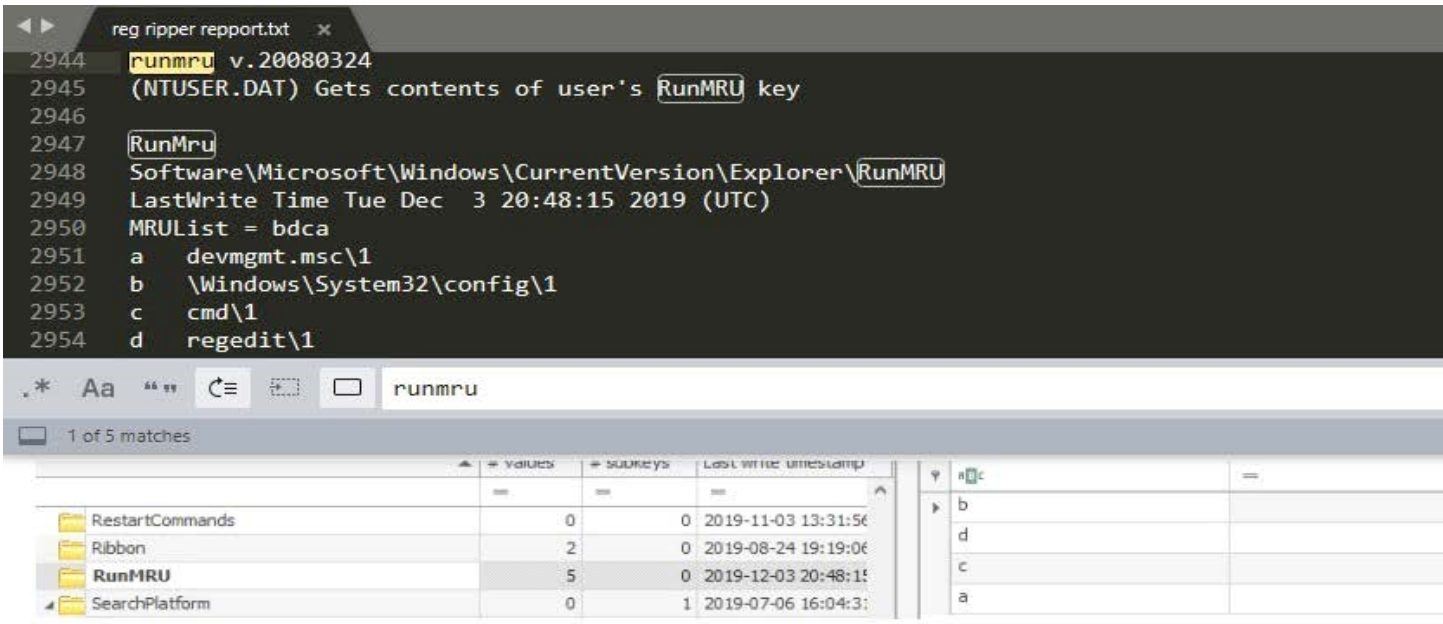


The results are very clear, this tool event sorts the documents by type / extension

```
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=screenclip&sharedAccessToken=0400038F-9401-488C-9903-E0E9FC10441A&secondarySharedAcces
  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
```

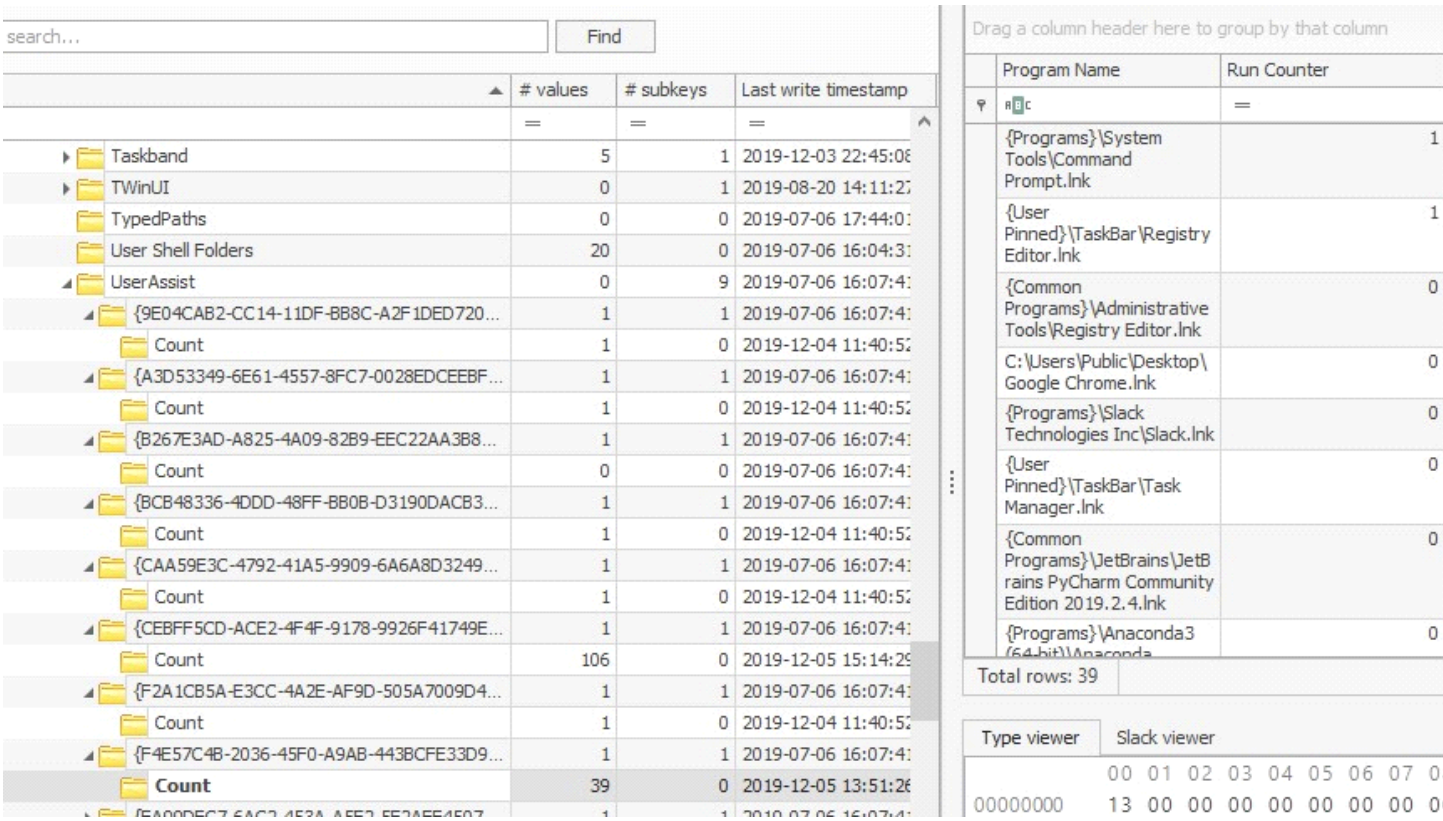
```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ipynb
LastWrite Time Mon Nov 18 08:06:07 2019 (UTC)
MRUListEx = 1,0
  1 = Untitled1 - Copy.ipynb
  0 = Untitled1.ipynb

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



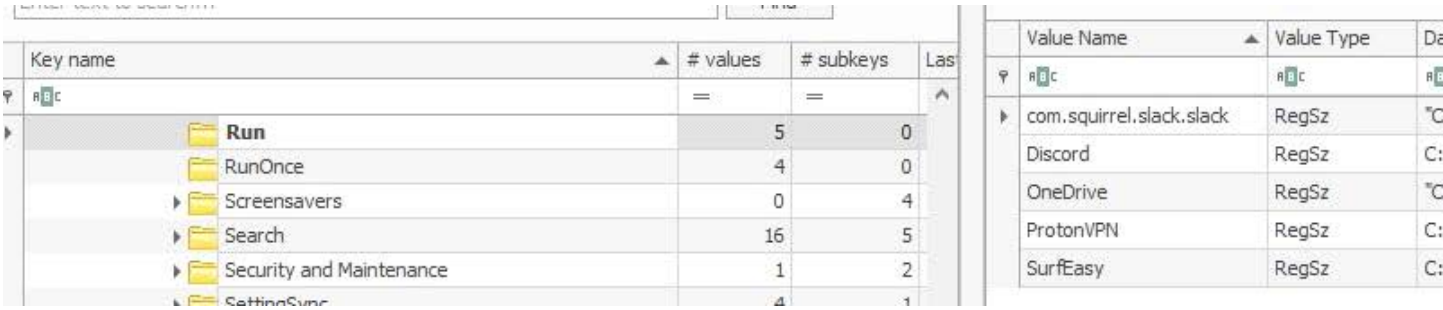
\typedpaths: This key contains information about paths typed-in in windows explorer. an attacker will probably know exactly the location of its target, he'll probably won't stumble around. This is why this key is useful.

\UserAssist: Through this key we can see when GUI applications have been executed, how many times and by whom which is very important in a forensics investigation.



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.

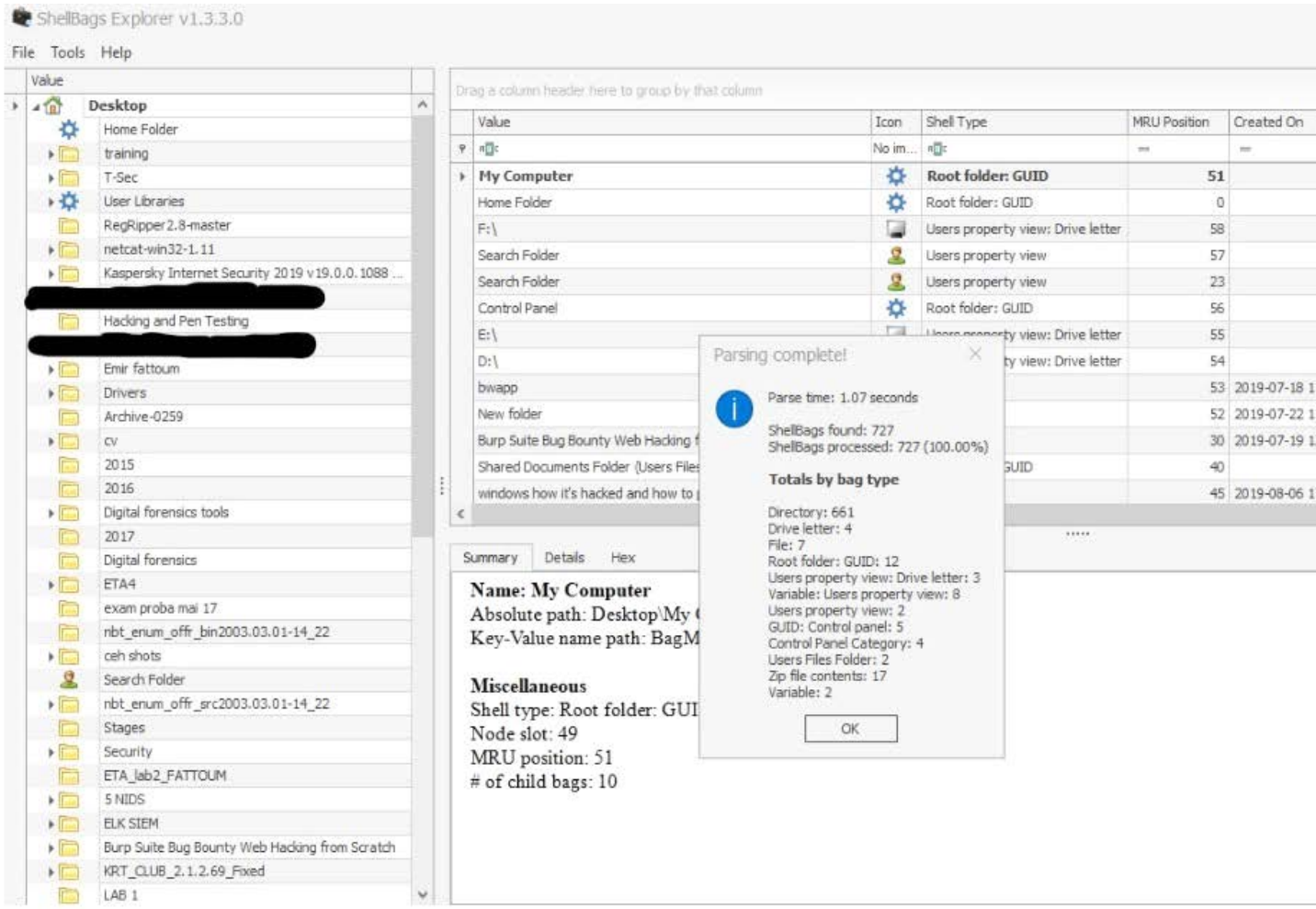


Next, I'm going to briefly introduce **Shellbags:**

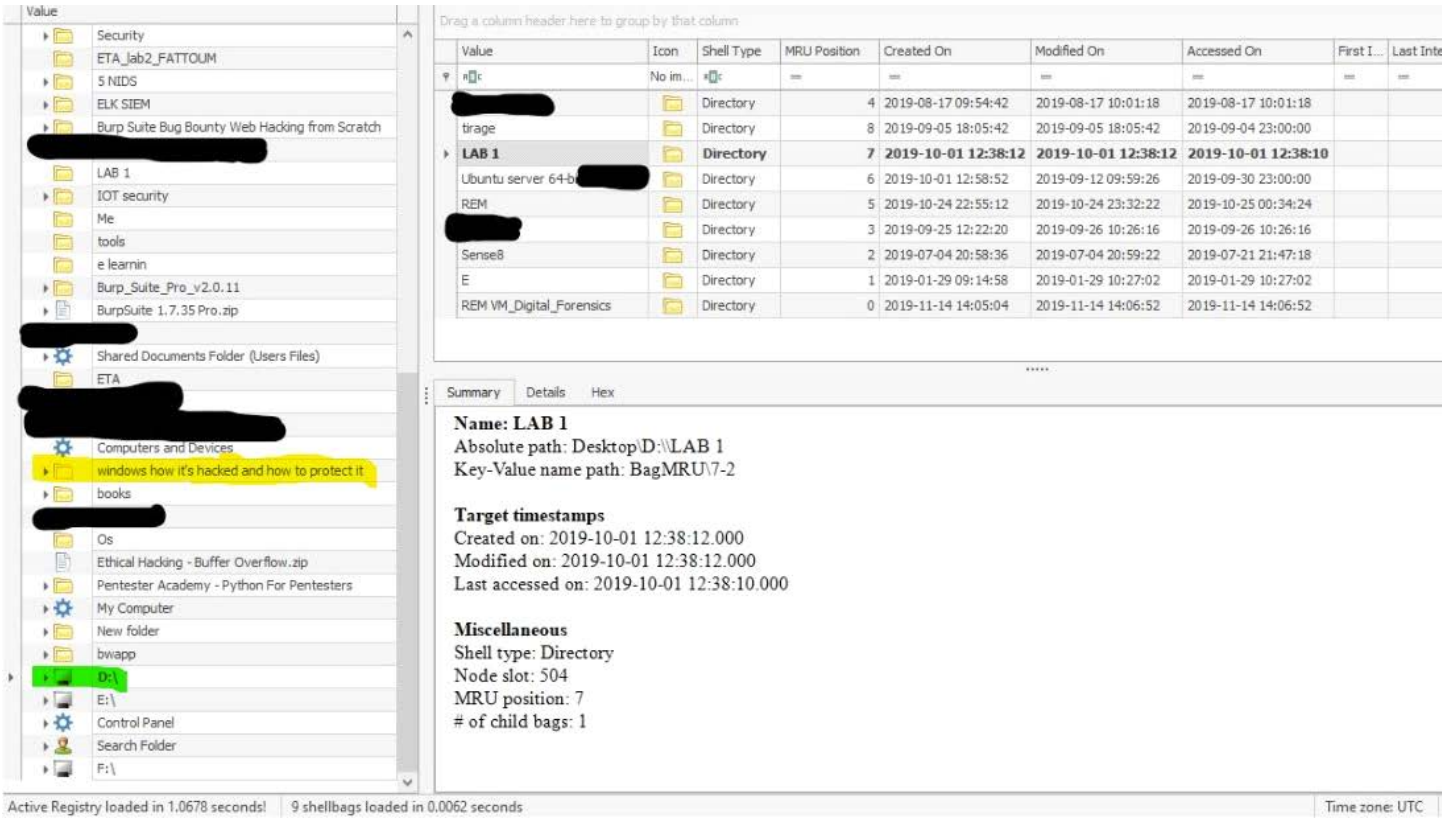
- Shellbags are registry keys that basically store details about a viewed folder when viewed through windows explorer such as the view, the icons, the size, the window position, the sorting method, etc. ... This also include network folders and removable devices.
- Shellbags are important from an investigators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



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.



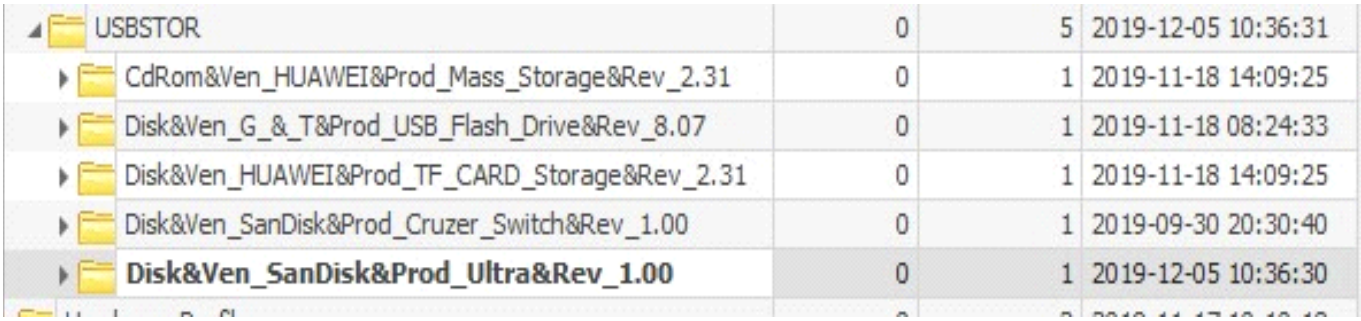
System forensics

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



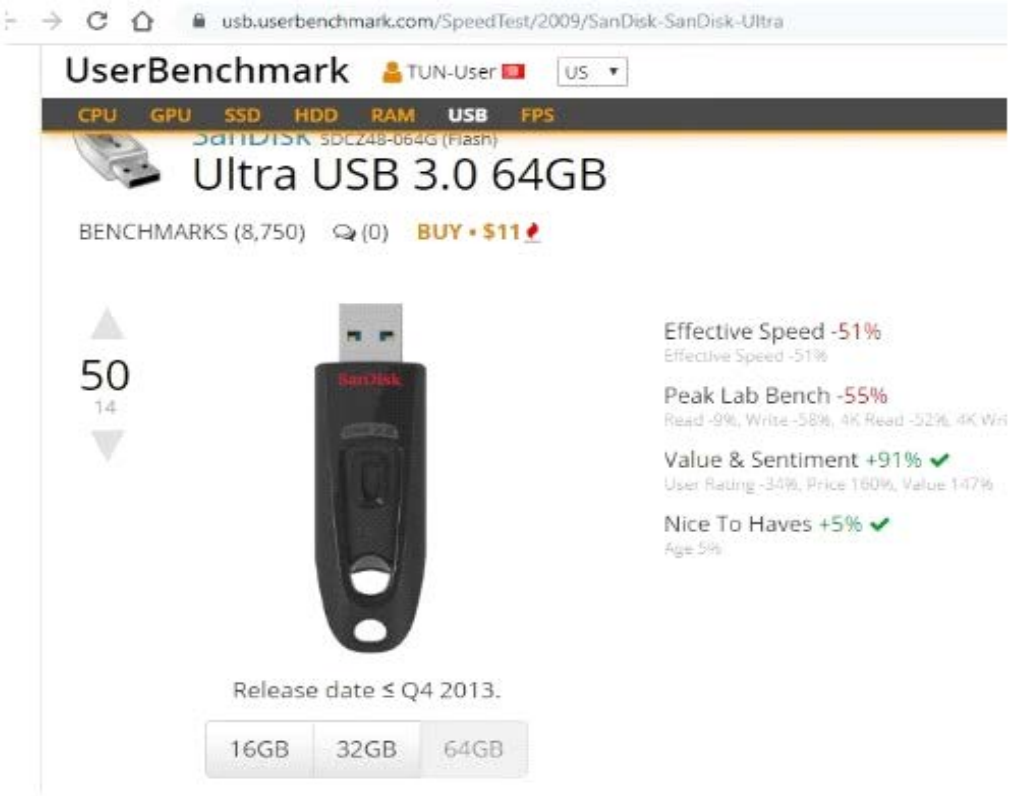
I plugged a flash drive just before I was making this part, if we expand further, as seen below. The number in yellow corresponds to the serial number of the flash drive. Correspondingly we can see a time stamp that is recorded in UTC (windows always use UTC in records),so we need to convert it to local 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
USB	0	17	2019-12-05 10:36:31
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
Hardware Profiles	0	2	2019-11-17 10:10:18
Policies	0	0	2019-03-19 04:53:37
Services	0	752	2019-12-04 02:38:59
Software	0	1	2019-03-19 04:53:37

Value Name	Value Type
Address	RegDword
Capabilities	RegDword
ClassGUID	RegSz
CompatibleIDs	RegMultiSz
ConfigFlags	RegDword
ContainerID	RegSz
DeviceDesc	RegSz
Driver	RegSz
FriendlyName	RegSz
HardwareID	RegMultiSz
Mfg	RegSz
Service	RegSz

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.

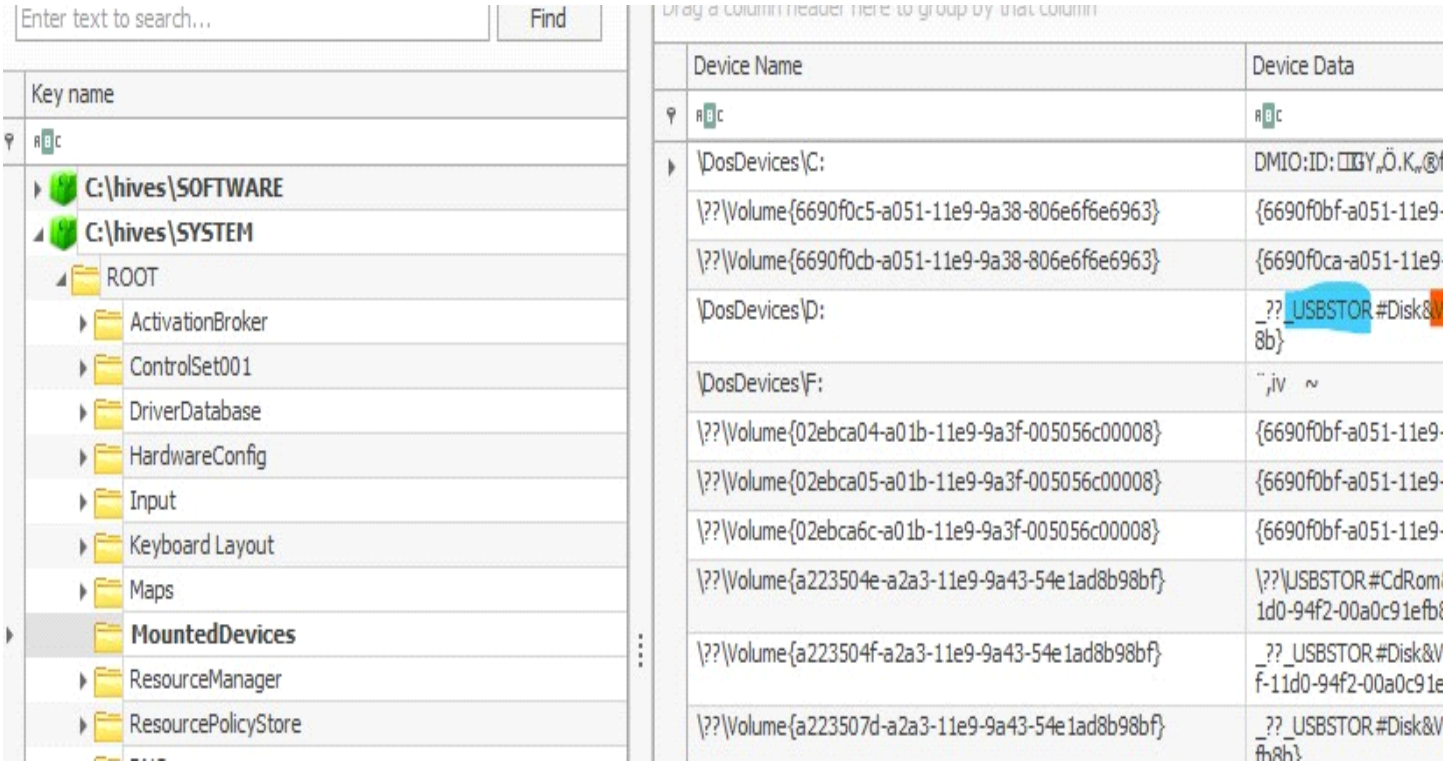
USB	0	17	2019-12-05 10:36:31
ROOT_HUB30	0	1	2019-12-05 10:36:30
VID_04F2&PID_B5AB	0	1	2019-07-06 23:51:50
VID_04F2&PID_B5AB&MI_00	0	1	2019-07-06 23:51:50
VID_058F&PID_6387	0	1	2019-12-05 10:36:29
VID_0781&PID_5572	0	1	2019-09-30 20:30:40
VID_0781&PID_5581	0	1	2019-07-06 23:51:49
4C531001490511103221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



Product Name	Vendor Name	Drive Size	VID	PID	Rea
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



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
\??\Volume{02ebca04-a01b-11e9-9a3f-005056c00008}	RegBinary	7B-00-36-00-36-00-3...	☐	☐
\??\Volume{02ebca05-a01b-11e9-9a3f-005056c00008}	RegBinary	7B-00-36-00-36-00-3...	☐	☐
\??\Volume{02ebca6c-a01b-11e9-9a3f-005056c00008}	RegBinary	7B-00-36-00-36-00-3...	☐	☐
\??\Volume{053b8828-e372-11e9-9a4f-f85971520f02}	RegBinary	5F-00-3F-00-3F-00-5...	☐	☐
\??\Volume{053b88a1-e372-11e9-9a4f-f85971520f02}	RegBinary	5F-00-3F-00-3F-00-5...	☐	☐
\??\Volume{053b8a8c-e372-11e9-9a4f-f85971520f02}	RegBinary	5F-00-3F-00-3F-00-5...	☐	☐
\??\Volume{053b9187-e372-11e9-9a4f-f85971520f02}	RegBinary	5C-00-3F-00-3F-00-5...	☐	☐
\??\Volume{2d9e10cb-a950-11e9-9a44-54e1ad8b98bf}	RegBinary	5C-00-3F-00-3F-00-5...	☐	☐
\??\Volume{2d9e1b19-a950-11e9-9a44-54e1ad8b98bf}	RegBinary	5F-00-3F-00-3F-00-5...	☐	☐
\??\Volume{4da2bffa-099d-11ea-9a54-54e1ad8b98bf}	RegBinary	5F-00-3F-00-3F-00-5...	☐	☐
\??\Volume{4da2c6b9-099d-11ea-9a54-54e1ad8b98bf}	RegBinary	5C-00-3F-00-3F-00-5...	☐	☐
\??\Volume{4da2c6bc-099d-11ea-9a54-54e1ad8b98bf}	RegBinary	5F-00-3F-00-3F-00-5...	☐	☐
\??\Volume{6690f0c5-a051-11e9-9a38-806e6f6e6963}	RegBinary	7B-00-36-00-36-00-3...	☐	☐
\??\Volume{6690f0cb-a051-11e9-9a38-806e6f6e6963}	RegBinary	7B-00-36-00-36-00-3...	☐	☐

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
0000001B  00 73 00 6B 00 26 00 56 00 65 00 6E 00 5F 00 53 00 61 00 6E 00 44 00 69 00 73 00
00000036  6B 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 7B 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

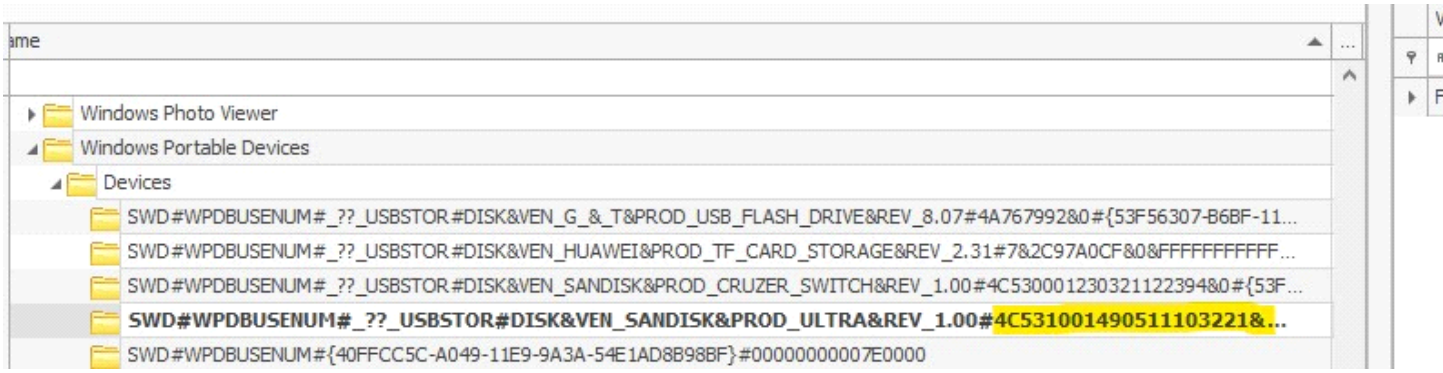
Key name	# values	# subkeys	Last write timestamp
C:\hives\NTUSER.DAT			2019-12-06 15:57:17
ROOT	0	11	2019-11-17 10:13:35
Software	0	33	2019-11-22 20:41:40
Microsoft	0	79	2019-12-06 14:38:48
Windows	0	7	2019-07-06 16:08:11
CurrentVersion	0	62	2019-08-19 10:42:07
Explorer	16	48	2019-12-06 15:25:21
MountPoints2	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.

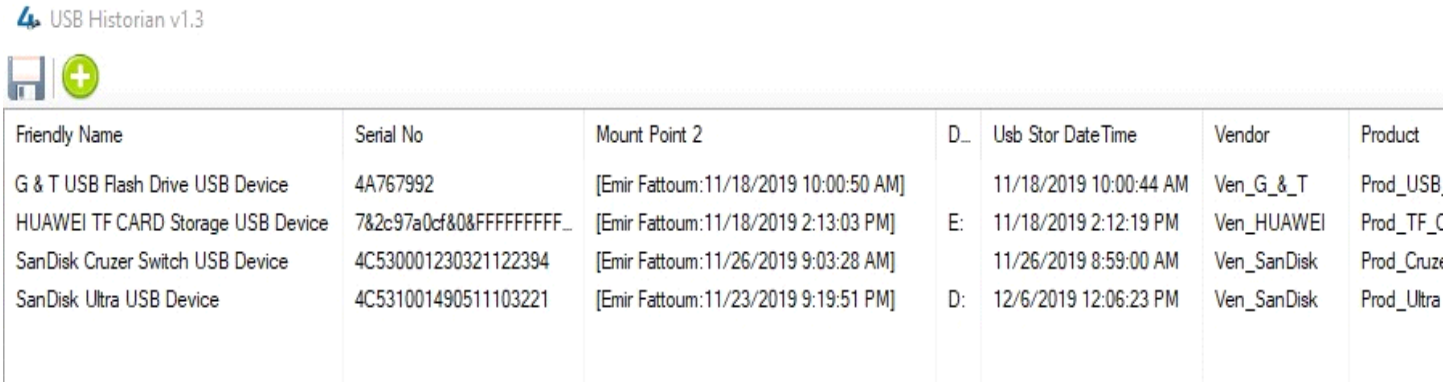
USBSTOR	0	5	2019-12-05 10:36:31
CdRom&Ven_HUAWEI&Prod_Mass_Storage&Rev_2.31	0	1	2019-11-18 14:09:25
Disk&Ven_G_&_T&Prod_USB_Flash_Drive&Rev_8.07	0	1	2019-11-18 08:24:33
Disk&Ven_HUAWEI&Prod_TF_CARD_Storage&Rev_2.31	0	1	2019-11-18 14:09:25
Disk&Ven_SanDisk&Prod_Cruzer_Switch&Rev_1.00	0	1	2019-09-30 20:30:40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

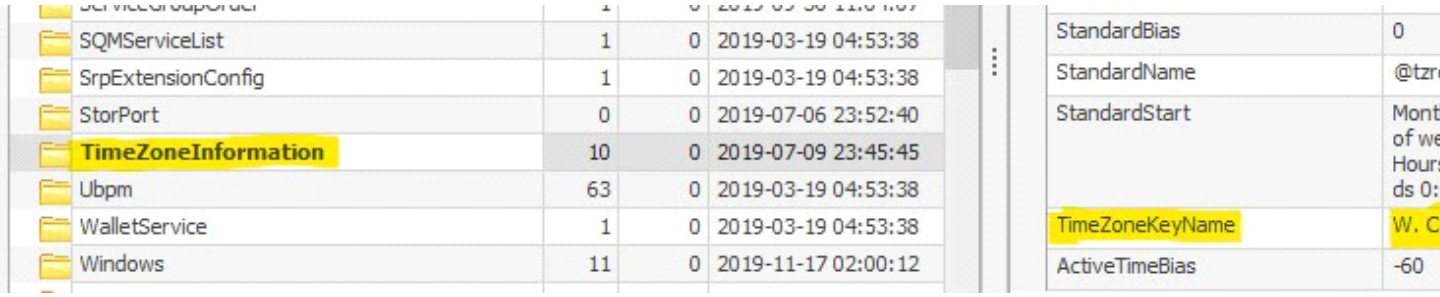


Friendly Name	Serial No	Mount Point 2	D...	Usb Stor DateTime	Vendor	Product
G & T USB Flash Drive USB Device	4A767992	[Emir Fattoum:11/18/2019 10:00:50 AM]		11/18/2019 10:00:44 AM	Ven_G_&_T	Prod_USB
HUAWEI TF CARD Storage USB Device	7&2c97a0cf&0&FFFFFFFFF...	[Emir Fattoum:11/18/2019 2:13:03 PM]	E:	11/18/2019 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**.

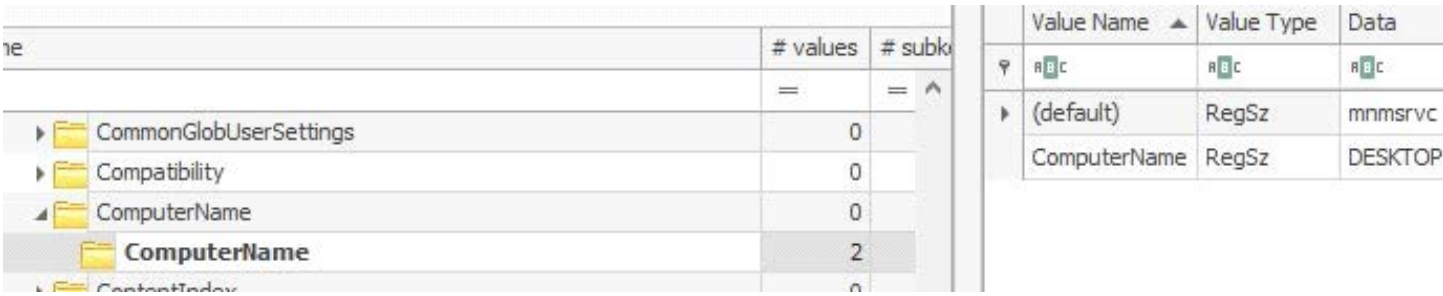


SQMServiceList	1	0	2019-03-19 04:53:38
SrpExtensionConfig	1	0	2019-03-19 04:53:38
StorPort	0	0	2019-07-06 23:52:40
TimeZoneInformation	10	0	2019-07-09 23:45:45
Ubpm	63	0	2019-03-19 04:53:38
WalletService	1	0	2019-03-19 04:53:38
Windows	11	0	2019-11-17 02:00:12

StandardBias	0
StandardName	@tzr
StandardStart	Mont of we Hour ds 0:
TimeZoneKeyName	W. C
ActiveTimeBias	-60

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.**

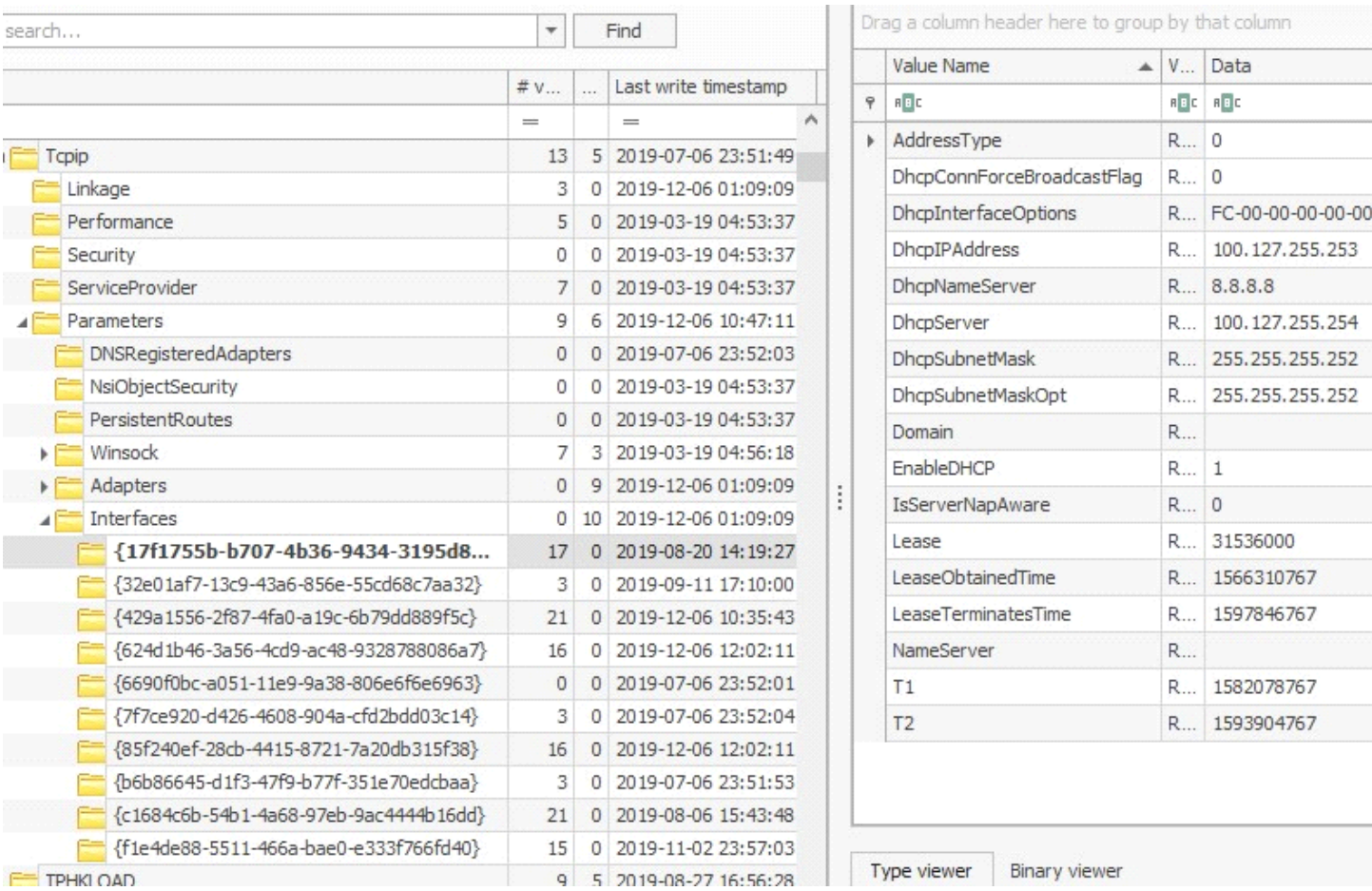


	# values	# subk
CommonGlobUserSettings	0	
Compatibility	0	
ComputerName	0	
ComputerName	2	

Value Name	Value Type	Data
(default)	RegSz	mnmsrvc
ComputerName	RegSz	DESKTOP

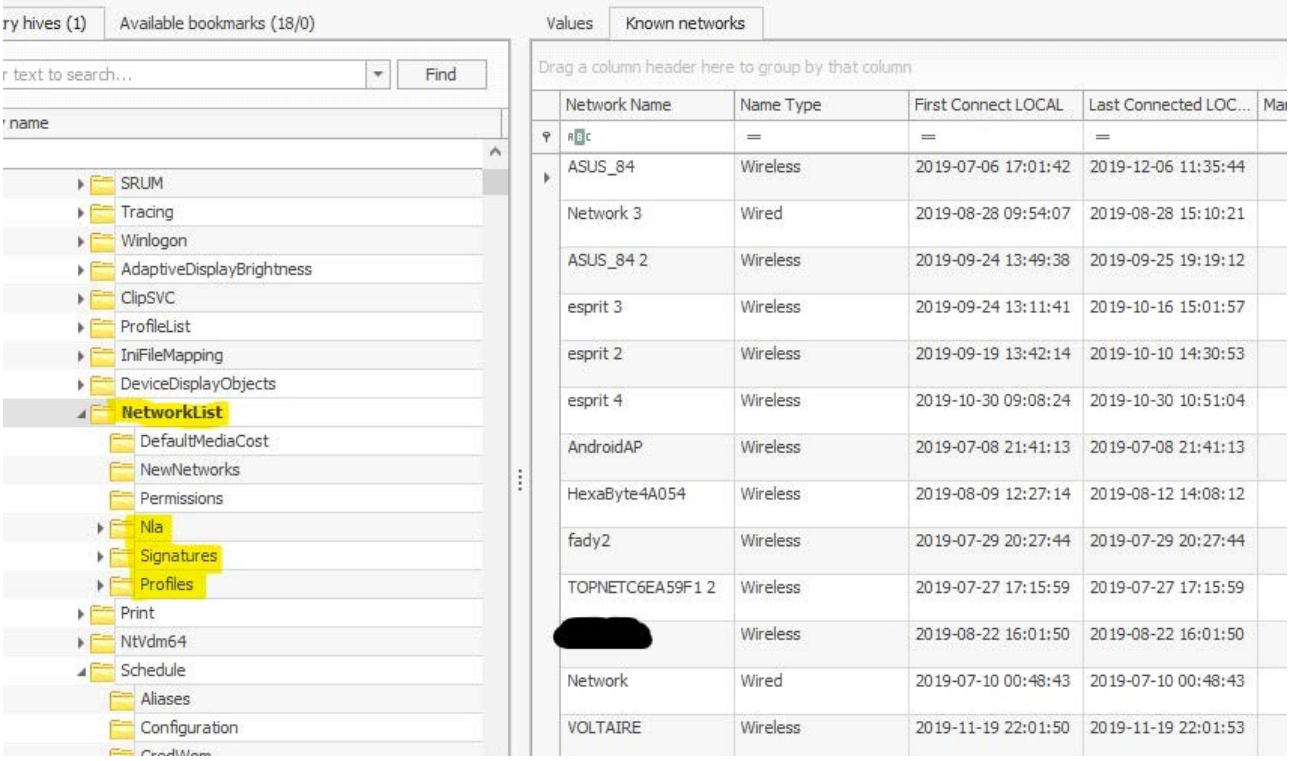
Network Interfaces

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



Wireless Network Listing

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



A lot of information is provided. Furthermore, we can grab the cash, under **\NLA\Cache**, the profiles of each network under **\Profiles** and a lot more such as the domain, DnsSuffix, DefaultGatewayMac under **\Signatures\Unmanaged.**

Prefetcher/SuperFetch

Prefetcher and SuperFetch are part of windows memory manager, they are used to cache data into the RAM so that it can be read fast. Investigators can use this to generate evidence of application execution on the entire machine (not related to users) and that include GUI and command line applications. These files are located under C:\windows\prefetch [main system partition]. We are going to use a tool called **WinPrefetchView** to view all the .pf files, we can see evidence of running "USB Historian" application, when ,where it's located ,etc.

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
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				
SVCHOST.EXE-BE1C404C.pf				
NETCFGNOTIFYOBJECTHOST.EXE-A0C34613.p				BJECTHOST
DLLHOST.EXE-D6E392F8.pf				
SHELLBAGSEXPLORER.EXE-03C94C75.pf				ORER.EXE
DLLHOST.EXE-50DEE1CF.pf				
RR.EXE-DADD85EF.pf				
DLLHOST.EXE-5C94BCB3.pf				
CMD.EXE-CD245F9E.pf				

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		
$MFT	C:\Windows\System		
ACCESSIBILITY.NI.DLL	C:\Windows\assem		
ACCESSIBILITY.NI.DLL...	C:\Windows\assem		
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll	\VOLUME{01d5345dab55086f-e2ab87...	8
AMSI.DLL	C:\Windows\System32\amsi.dll	\VOLUME{01d5345dab55086f-e2ab87...	50
APPHELP.DLL	C:\Windows\System32\apphelp.dll	\VOLUME{01d5345dab55086f-e2ab87...	6
BCRYPT.DLL	C:\Windows\System32\bcrypt.dll	\VOLUME{01d5345dab55086f-e2ab87...	40
BCRYPTPRIMITIVES.DLL	C:\Windows\System32\BCRYPTPRIMI...	\VOLUME{01d5345dab55086f-e2ab87...	16
CFGMGR32.DLL	C:\Windows\System32\cfgmgr32.dll	\VOLUME{01d5345dab55086f-e2ab87...	69