

Intro to the Windows Registry



# Warning

Please take extreme caution when editing the Windows Registry.

This can be backed up and examined as needed.

Don't launch the Registry Editor and start deleting things etc....

This requires specific knowledge and shouldn't be edited.

We will backup a registry first before our investigative process.



# WHAT IS THE REGISTRY?

Hierarchical database, it contains the value of variables in Windows and in the applications and services that run on Windows.

- Configurations and settings used by components, services, applications etc...
- Registry primarily uses Key / Value pairs.
- Registry Keys are objects that provides logical structure (kind of like folders)
- Values store data and they contain the actual settings.
- *“The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used.”*

- Source: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users>



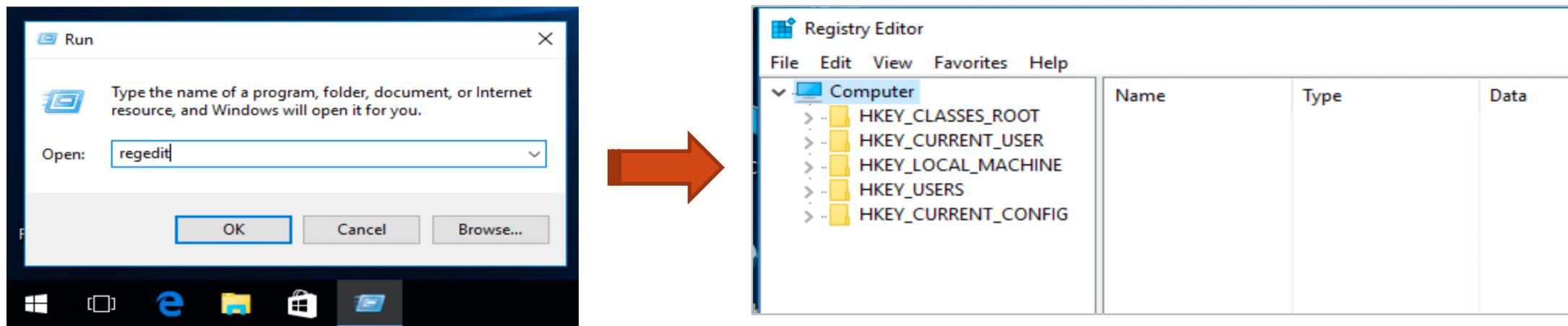
# Notable content in the Registry

- User Profiles
- File extensions and installed applications
- Settings for folders etc
- System Hardware
- Port config for I/O comms
- Install Date
- Time Zone Information
- Users in the system
- Registered owner

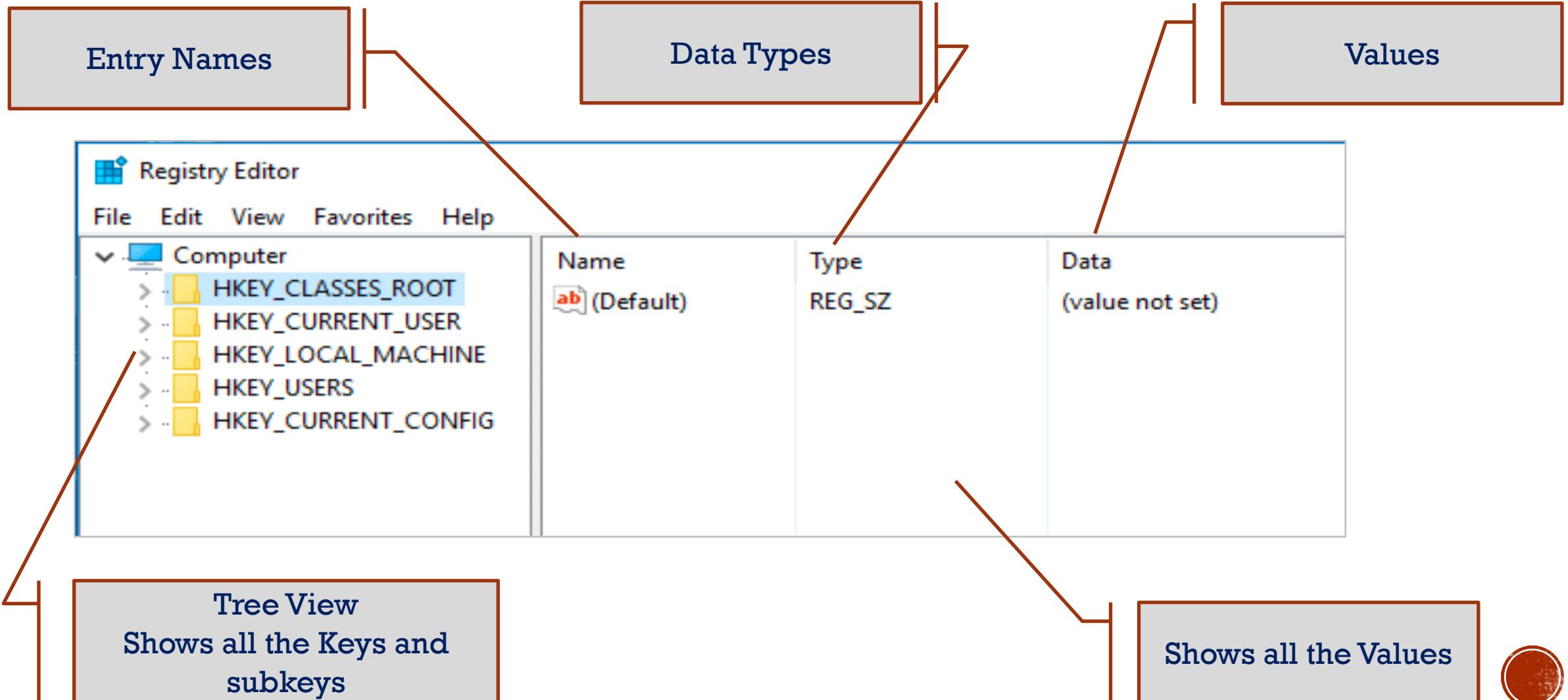


# LAUNCHING THE REGISTRY

- Open a Run Dialog box.
- Type: regedit

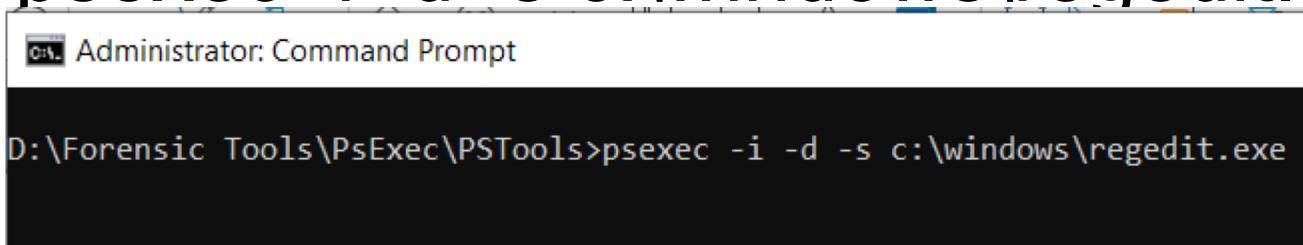


# REGISTRY STRUCTURE



# Run Regedit as System

- Some areas of the registry may be restricted.
- The Registry editor may need to be run with System privilege
- PsExec can be used to launch the registry editor as System
  - <https://docs.microsoft.com/en-gb/sysinternals/downloads/psexec>
- To run:
  - `psexec -i -d -s c:\windows\regedit.exe`



```
D:\Forensic Tools\PsExec\PSTools>psexec -i -d -s c:\windows\regedit.exe
```



# What is a Registry Hive

- A Hive is a major section in the Windows Registry.
- It contains a group of keys, subkeys, and values in the registry that has a set of supporting files that contain backups of its data.
- The Hives are a set of files. Each Hive is a hierarchical structure.
- Paths to hives are set in the Configuration Manager (with exception of user profiles)
- The Configuration Manager creates the root keys and links the hives together in the registry structure.

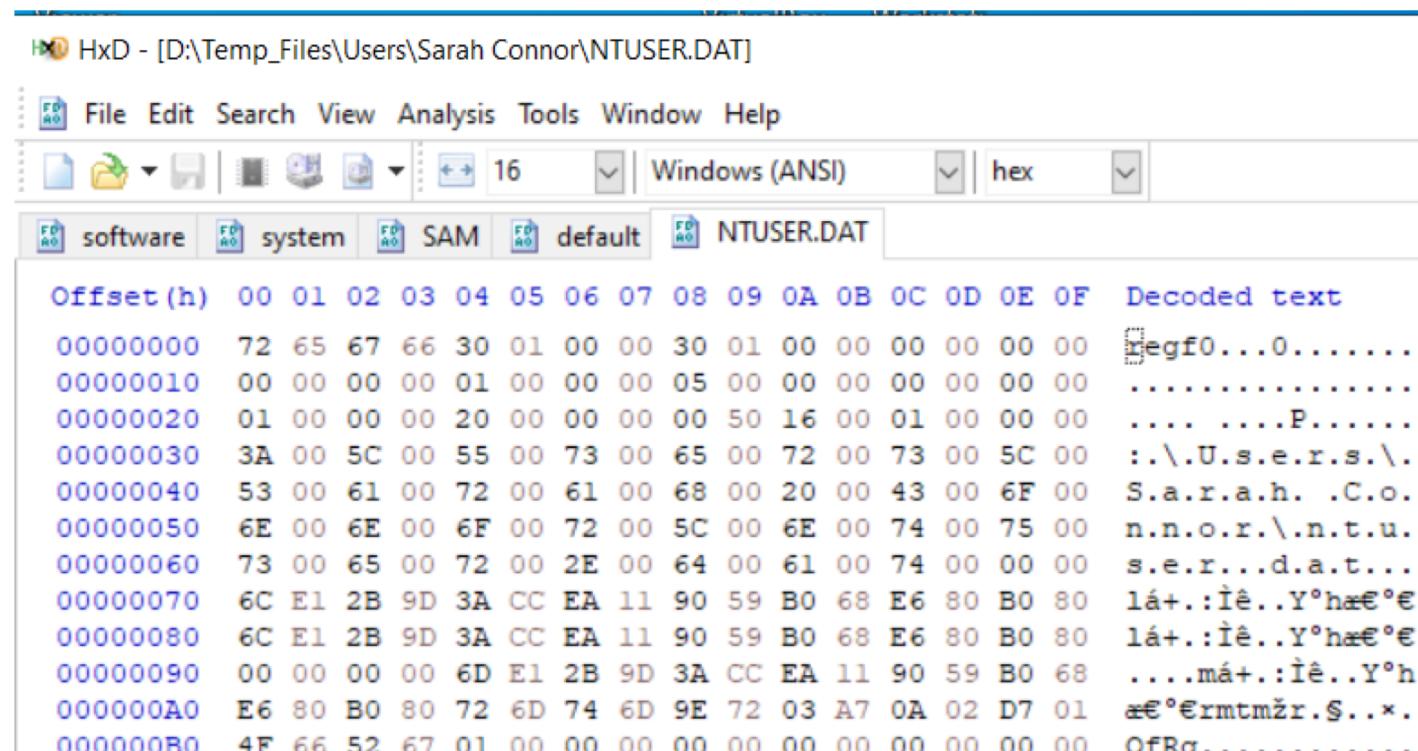


# Registry Hive - Header

- 4096 bytes long
- Stores info on:
  - Signature
  - Primary and secondary sequence numbers
  - Last write timestamp
  - Etc...



# Registry Hive - Header



The screenshot shows the HxD hex editor interface with the file 'NTUSER.DAT' open. The menu bar includes File, Edit, Search, View, Analysis, Tools, Window, and Help. The toolbar has icons for Open, Save, Find, Replace, and various file formats. The status bar shows 'Windows (ANSI)' and 'hex'. The main window displays memory dump data with columns for Offset(h), Decoded text, and a preview pane.

Offset(h)	Decoded text
00000000	\Regf0...0.....
00000010	.....
00000020	.....P.....
00000030	..\U.s.e.r.s.\.
00000040	S.a.r.a.h. .C.o.
00000050	n.n.o.r.\n.t.u.
00000060	s.e.r...d.a.t...
00000070	lá+.:íè..Yºhæ€°€
00000080	lá+.:íè..Yºhæ€°€
00000090	....má+.:íè..Yºh
000000A0	æ€°€rmtmžr.\$...x.
000000B0	OfRg.....

- Signature (offset 0x0)
- Primary and Secondary sequence numbers (offset 0x04 and 0x08)
- Last Write (offset 0xC)
- Major and minor version (offset 0x14 and offset 0x18)
- Root cell offset (offset 0x24)
- Length (offset 0x28)
- Internal file name (offset 0x30)

If sequence numbers don't match the hive is dirty.

If hive is dirty log files will be needed or data may be missing.



# Log Files

- Changes are made to the log files before this is reflected in the registry.



# Hive Locations

- HKEY\_LOCAL\_MACHINE\SYSTEM: %SystemRoot%\system32\config\SYSTEM
- HKEY\_LOCAL\_MACHINE\SAM: %SystemRoot%\system32\config\SAM
- HKEY\_LOCAL\_MACHINE\SECURITY: %SystemRoot%\system32\config\SECURITY
- HKEY\_LOCAL\_MACHINE\SOFTWARE: %SystemRoot%\system32\config\SOFTWARE
- HKEY\_LOCAL\_MACHINE\HARDWARE: Volatile hive
- HKEY\_LOCAL\_MACHINE\SYSTEM\Clone: Volatile hive
- HKEY\_USERS\UserProfile: <profiles folder>\NTUSER.DAT
- HKEY\_USERS.DEFAULT: %SystemRoot%\system32\config\DEFAULT



# Install Date

- The install date will hold information on when the system was installed. This may be relevant to the investigation if a person is saying they only had the machine a few months, but in fact they had it much longer.
- The Software Hive stores the install date.
- The value is a Unix Time Stamp (seconds from 1/1/1970)
- The time stamp is presented with the local time zone and UTC.
- We will talk about time zones later in this session



# CurrentVersion

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

## In-Class Demo...

### Notable content:

InstallDate

InstallTime

PathName

ProductName

RegisteredOwner

SystemRoot



# Time Zones

- The time zones settings for a computer will affect the displayed time and the time that is noted in time stamps.
- For a forensic investigation it is important to verify the time zone we are dealing with.
- The time zone create an offset from UTC (Coordinated Universal Time)
- The time zone settings are kept in the SYSTEM Hive

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation

- The TimeZoneKeyName holds the time zone info
- Daylight saver info is available here too.



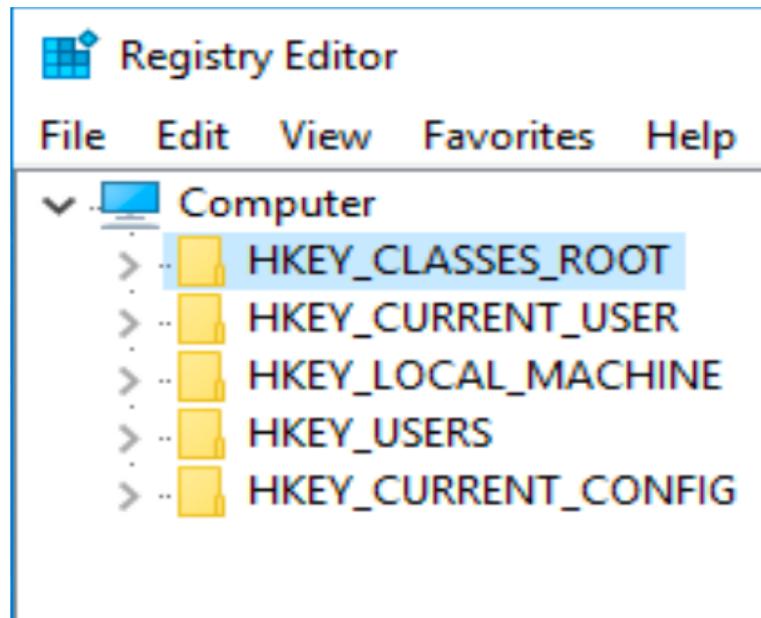
# Users in the System

- As part of an investigation we may need to determine all the users for a given computer. A person accused of a transgression may claim another person/user may have done this.
- Our first source for the list of users would be the file system.
- For windows C:\Users, Mac Users Dir, etc...
- The Registry can be a more reliable source of information, the file system can be easily manipulated
- The user info is located in:
- Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Windows NT\CurrentVersion\ProfileList
- There will be an entry here for each user on the system
- The ProfileImagePath will give the name of the user. The SID is the unique identifier.
- In-Class demo....



# ROOT KEYS

- The root keys offer structure to the different types of information stored in the Registry.



*Interesting Fact: three of the five items on the root level aren't here. These are just linked to items further down in one of the other keys.*



# ROOT KEYS - HKEY\_CLASSES\_ROOT (HKCR)

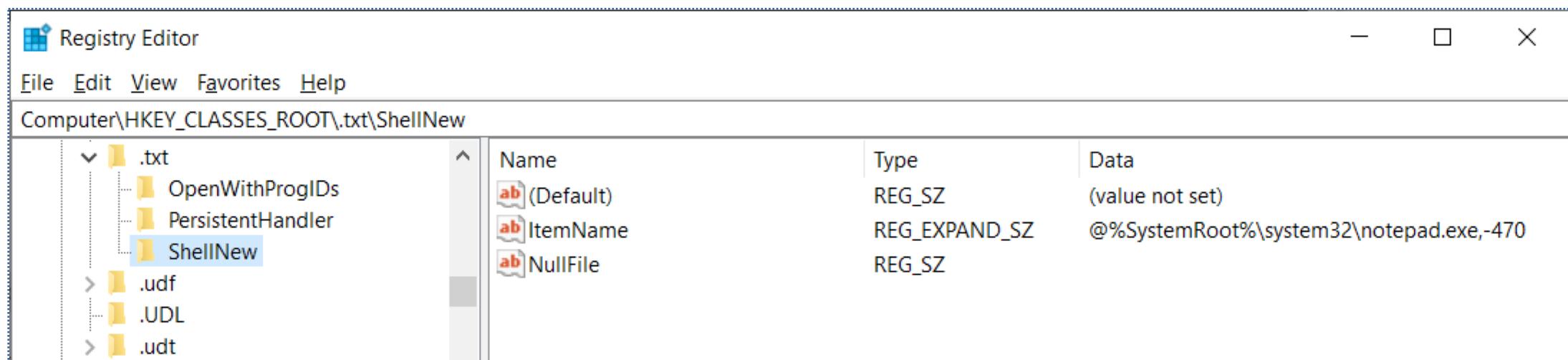
This is used to manage file type associations (mainly file extension associations and COM class registrations)

- This is a link to HKLM\Software\Classes
- content of HKEY\_CLASSES\_ROOT comes from:
  - HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes
  - HKEY\_CURRENT\_USER\SOFTWARE\Classes
- Stores data that associates file types with programs.
- Subkeys in HKCR have the same name as the file name extension for the file type
- The current merged configuration lets the system register program classes independently for each user. This feature is known as per user class registration.
- The **open with** associations are all stored in HKEY\_CLASSES\_ROOT.
- User specific options are in HKEY\_CURRENT\_USER\SOFTWARE\Classes



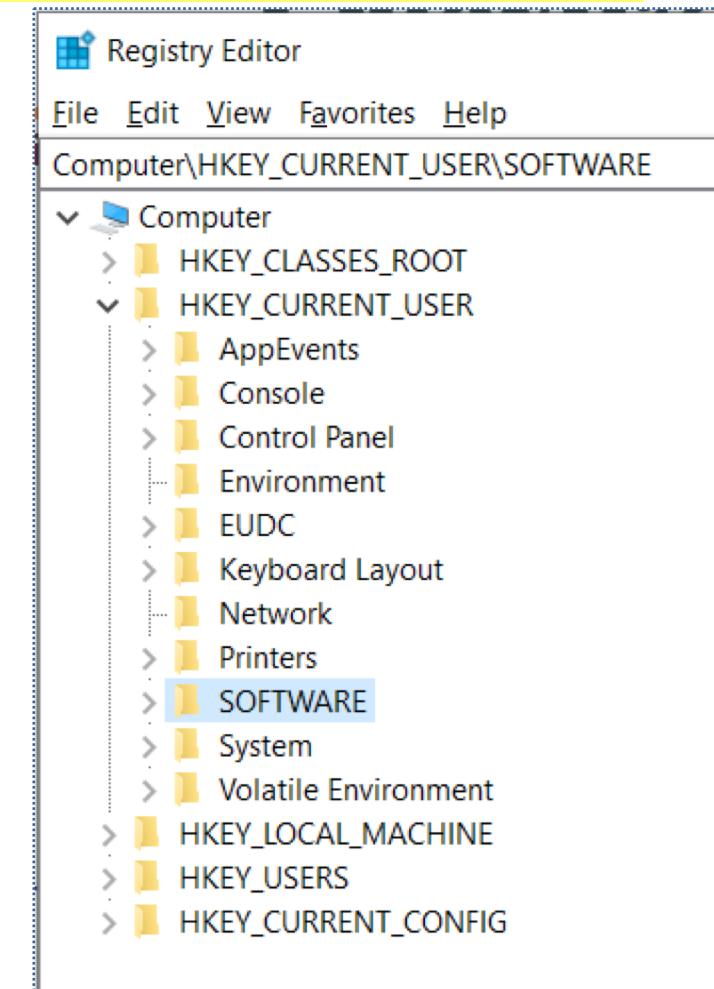
# HKCR - EXAMPLE

- HKEY\_CLASSES\_ROOT



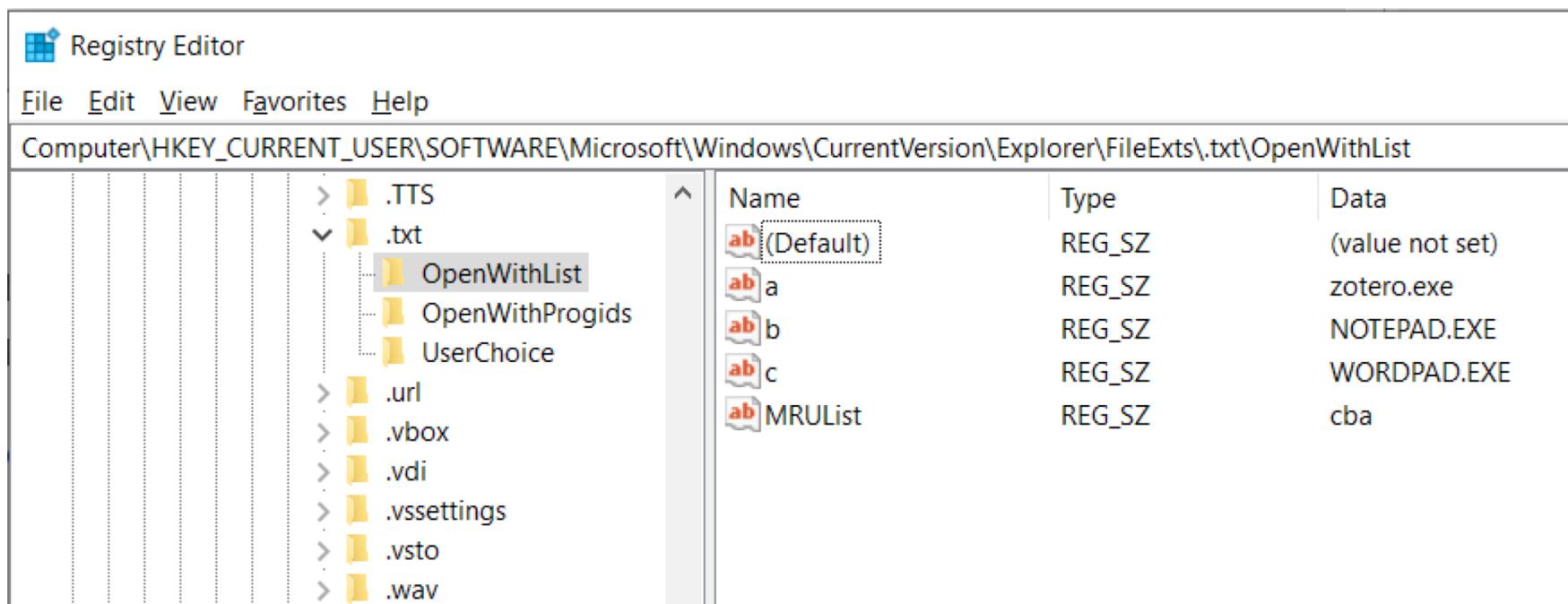
# ROOTKEYS - HKEY\_CURRENT\_USER (HKCU)

- HKCU contains configuration information for Windows and software specific to the currently logged in user.
- The registry keys and values in this hive are used to control user-level settings (wall papers, preferences, shared drives, printers, etc)
- Many of the changes a user makes in Control Panel are stored here.
- HKCU offers default system-wide file extension association for a file.



# HKCU - EXAMPLE

- Change default from notepad to wordpad for .txt (Using Windows Explorer)

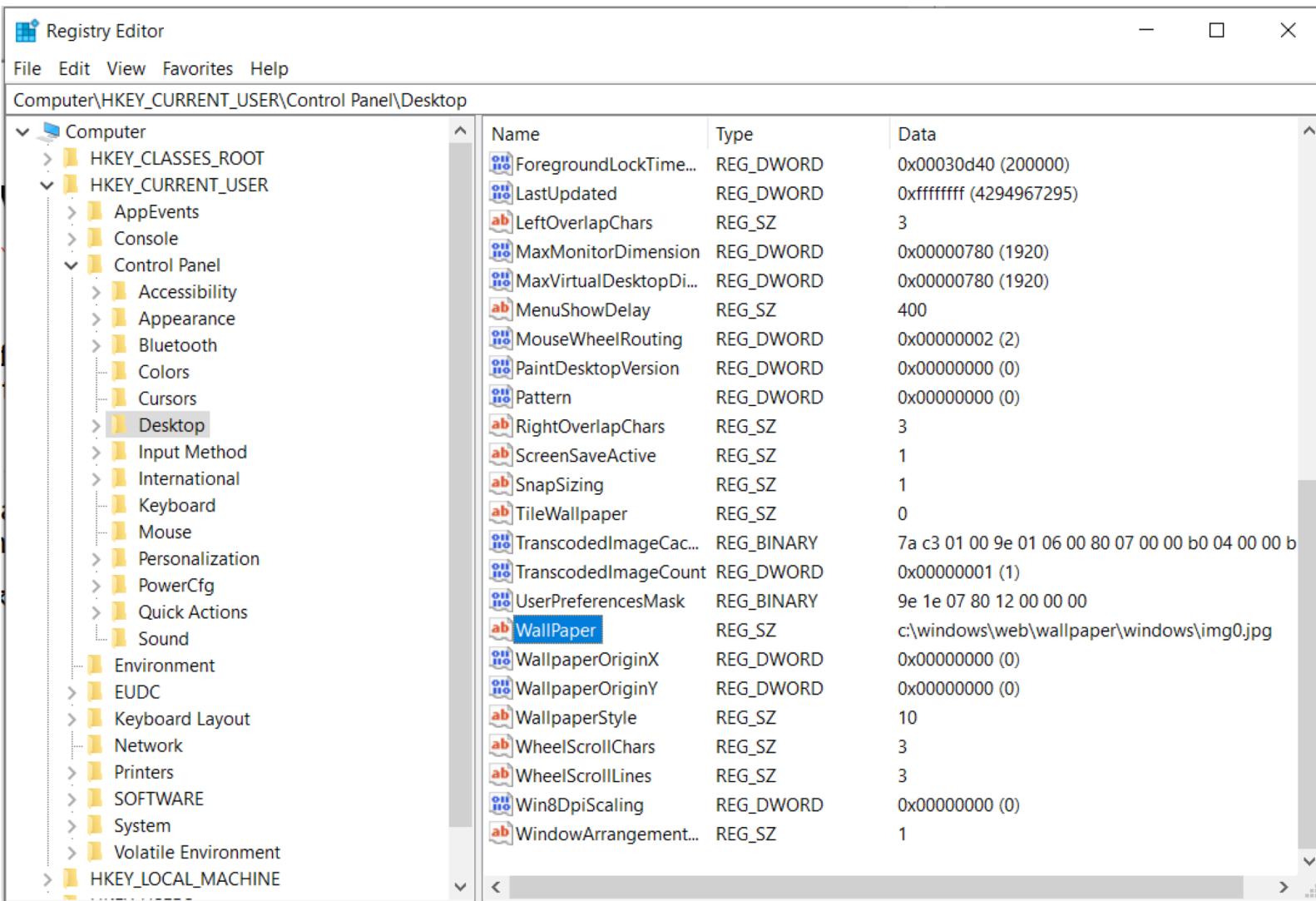


Computer\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt\OpenWithList



# HKCU - EXAMPLE

- Example

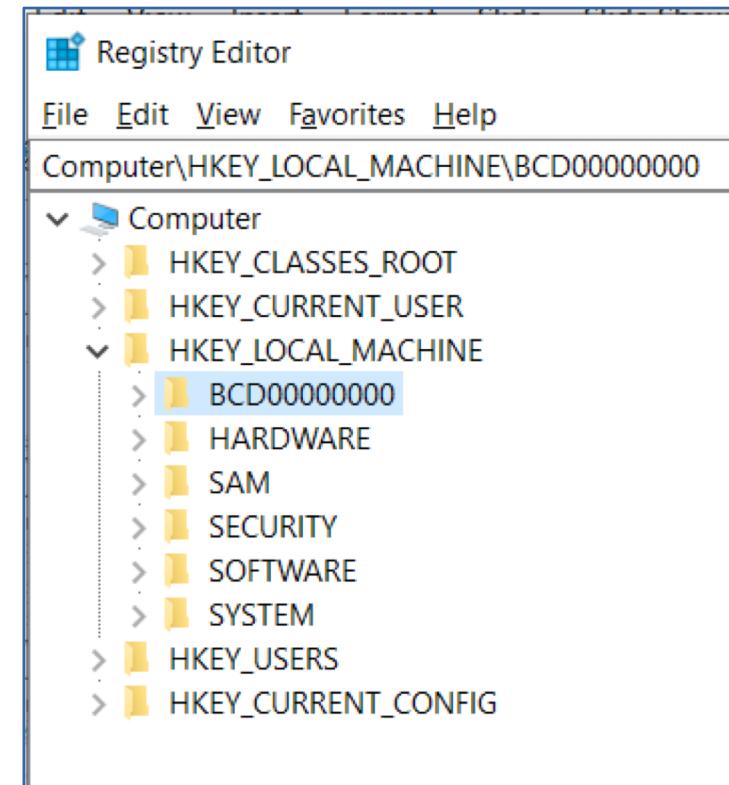


The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'Computer'. The 'Desktop' key under 'Control Panel' is selected. The right pane shows a table of registry values for this key.

Name	Type	Data
ForegroundLockTime...	REG_DWORD	0x00030d40 (200000)
LastUpdated	REG_DWORD	0xffffffff (4294967295)
LeftOverlapChars	REG_SZ	3
MaxMonitorDimension	REG_DWORD	0x00000780 (1920)
MaxVirtualDesktopDi...	REG_DWORD	0x00000780 (1920)
MenuShowDelay	REG_SZ	400
MouseWheelRouting	REG_DWORD	0x00000002 (2)
PaintDesktopVersion	REG_DWORD	0x00000000 (0)
Pattern	REG_DWORD	0x00000000 (0)
RightOverlapChars	REG_SZ	3
ScreenSaveActive	REG_SZ	1
SnapSizing	REG_SZ	1
TileWallpaper	REG_SZ	0
TranscodedImageCac...	REG_BINARY	7a c3 01 00 9e 01 06 00 80 07 00 00 b0 04 00 00 b
TranscodedImageCount	REG_DWORD	0x00000001 (1)
UserPreferencesMask	REG_BINARY	9e 1e 07 80 12 00 00 00
WallPaper	REG_SZ	c:\windows\web\wallpaper\windows\img0.jpg
WallpaperOriginX	REG_DWORD	0x00000000 (0)
WallpaperOriginY	REG_DWORD	0x00000000 (0)
WallpaperStyle	REG_SZ	10
WheelScrollChars	REG_SZ	3
WheelScrollLines	REG_SZ	3
Win8DpiScaling	REG_DWORD	0x00000000 (0)
WindowArrangement...	REG_SZ	1

# ROOTKEYS- HKEY\_LOCAL\_MACHINE (HKLM)

- HKLM stores configuration information for the software you have installed including the Windows operating system.
- This hive also keeps information on currently detected hardware and device drivers.
- Stores information on boot configuration (Win 7/8/10)



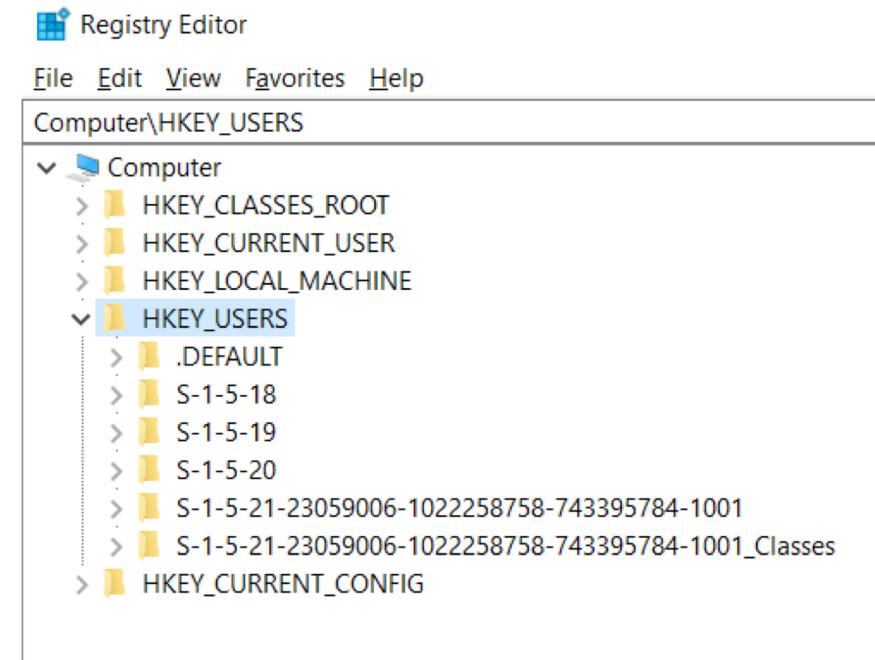
# HKEY\_LOCAL\_MACHINE - BCD00000000

- Stores boot configuration data to boot Windows OS
- For UEFI boot the hive is:  
/EFI/Microsoft/Boot/BCD
- For BIOS boot the hive is:  
/boot/BCD
- Note data should be edited with bcdeedit.exe, not regedit



# ROOT KEYS - HKEY\_USERS (HKU)

- Contains user-specific configuration information for all currently active users on the computer
- Each key under HKU is a user on the system and is linked with a security ID (SID)
- This is loaded when user logs on.
- Stores info on:
  - Mapped drives
  - Printers
  - Env variables
  - Etc...



# ROOT KEYS - HKEY\_USERS (HKU)

C:\> Administrator: Command Prompt

```
D:\Forensic Tools\PsExec\PSTools>whoami  
laptop-tcfk0pi6\jonat
```

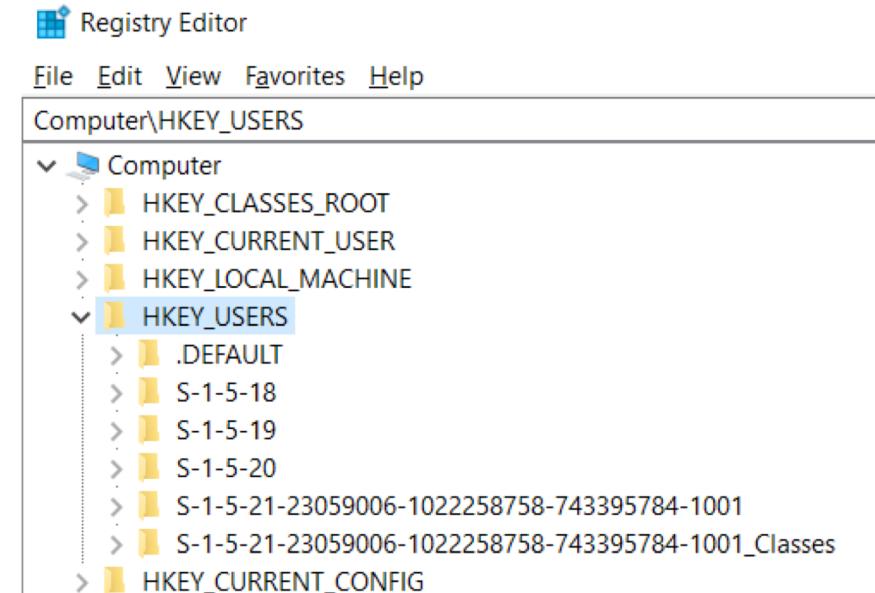
  

```
D:\Forensic Tools\PsExec\PSTools>whoami /user
```

USER INFORMATION

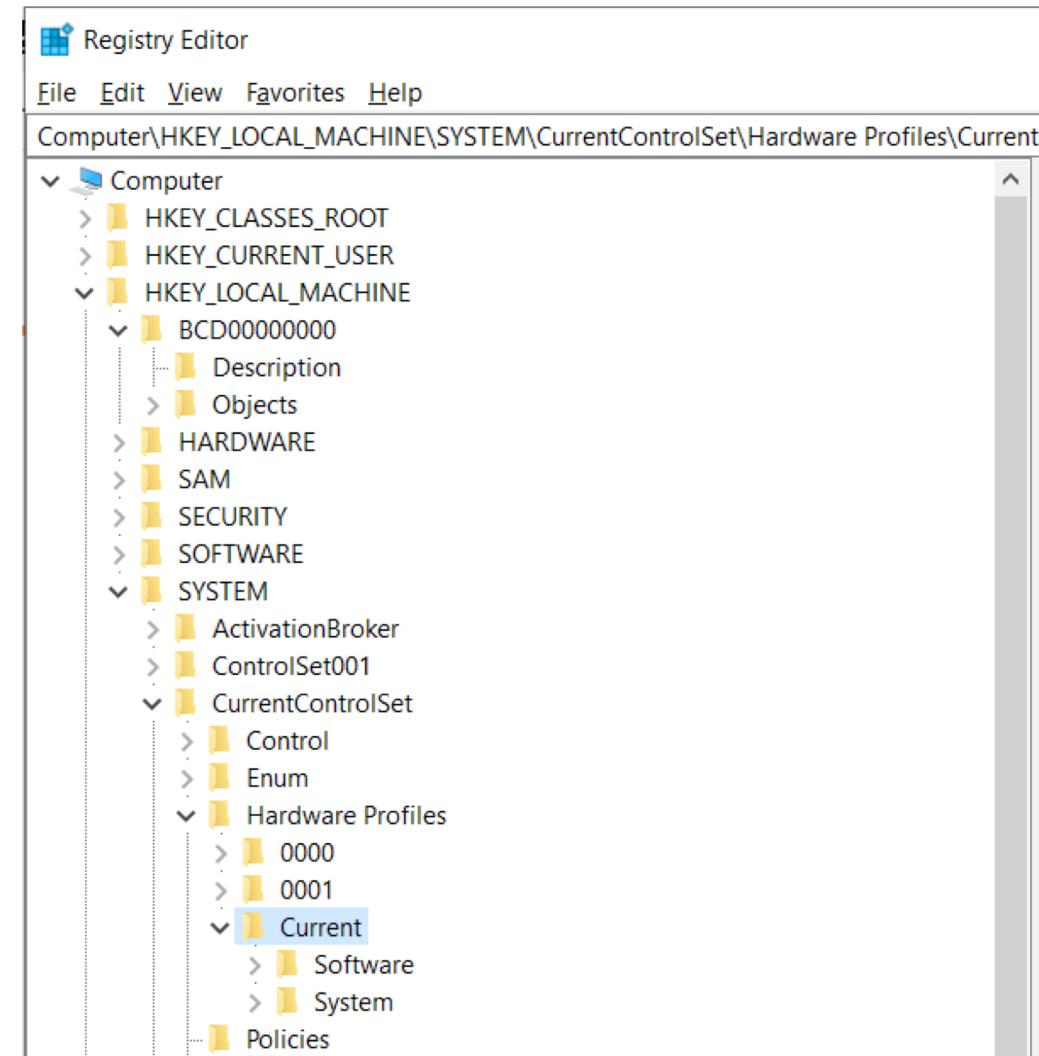
User Name	SID
laptop-tcfk0pi6\jonat	S-1-5-21-23059006-1022258758-743395784-1001

```
D:\Forensic Tools\PsExec\PSTools>
```



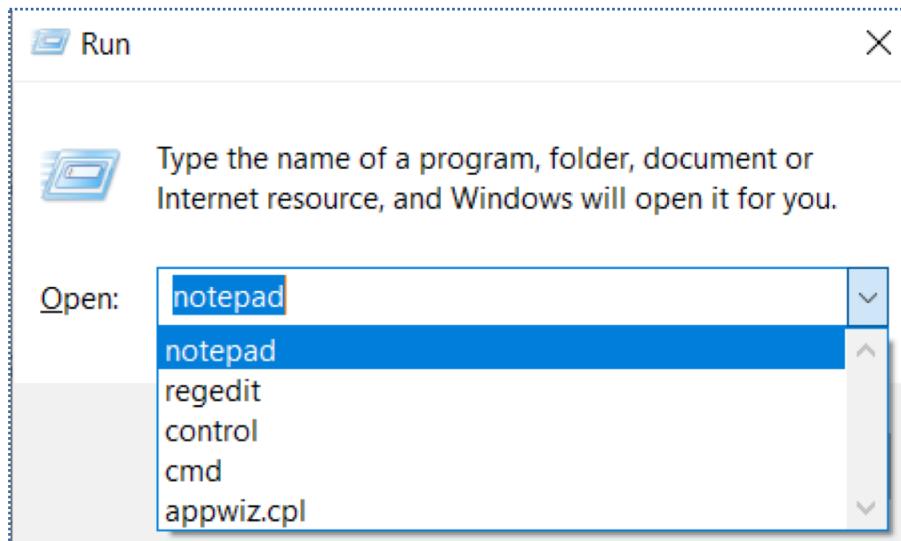
# ROOT KEYS – HKEY\_CURRENT\_CONFIG (HKCC)

- This is a pointer to another location in the Registry
- Info in the Hardware Profile currently being used
- Shortcut to:  
Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentCo  
ntrolSet\Hardware Profiles\Current

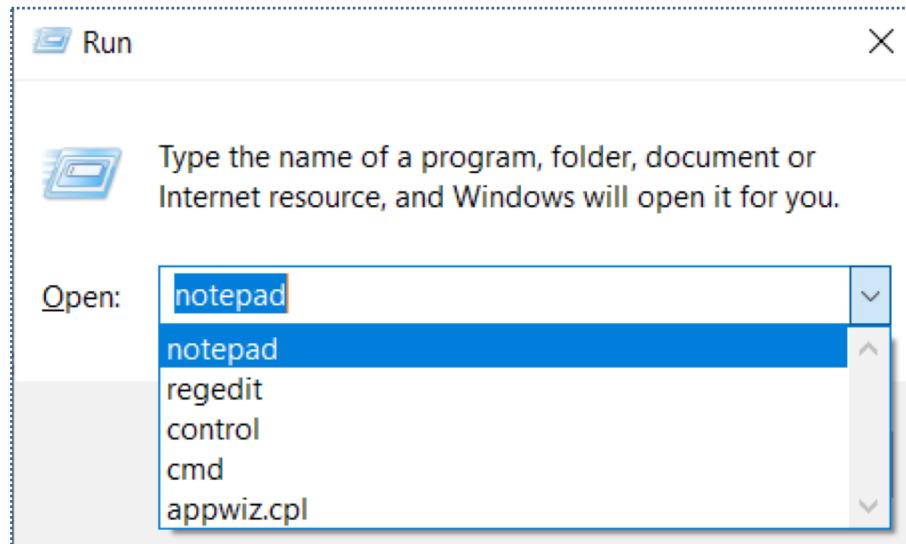


# MOST RECENTLY USED (MRU)

- Windows and some applications store the MRU list in the Registry
- Some programs use local text files.
- This is a list of recently used programs or opened files that the Windows operating system saves in the Windows Registry
- This is linked to the drop down lists for programs opened etc.
- Eg:



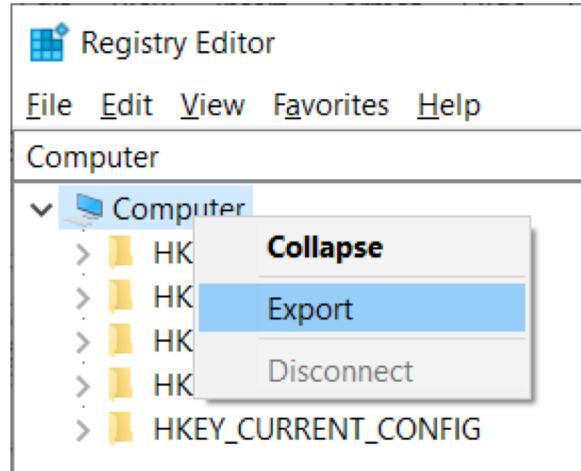
# MOST RECENTLY USED (MRU)



The image shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under "Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU". The right pane shows a table of registry entries with columns for Name, Type, and Data.

Name	Type	Data
ab(Default)	REG_SZ	(value not set)
ab <a href="#">a</a>	REG_SZ	cmd\1
ab <b>b</b>	REG_SZ	notepad\1
abc	REG_SZ	appwiz.cpl\1
abd	REG_SZ	control\1
abe	REG_SZ	regedit\1
abMRUList	REG_SZ	ebdac

# BACKUP THE REGISTRY



- In Registry Explorer, right click a key and export.
- This example is **HKEY\_CLASSES\_ROOT**

WindowsRegBackup	14/04/2021 11:57	Registration Entries	52,998 KB
------------------	------------------	----------------------	-----------



# **BACKUP THE REGISTRY**

- To copy the registry files for examination AccessData FTK Imager created a backup of all registry files.
- In-Class Demo....



# Tracing a USB Device

- **Sequence**
- **Plug and Play** – new usb device is connected, the PnP Manager gets the event notification and gets the device information to try source the appropriate driver for this device.
  - The new driver for the device is recorded in the **setupapi log file**, using this the timestamp the device was connected to the computer can be obtained.
  - An entry is also created in the Registry
    - HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\
    - The registry entry will use the device id as the key.
    - Unique id (usually device serial number or system generated id). If the second character of the id is an & it was system generated.
    - The device descriptor is not located in the memory area of the device and this should be retrieved separately from the image acquisition process



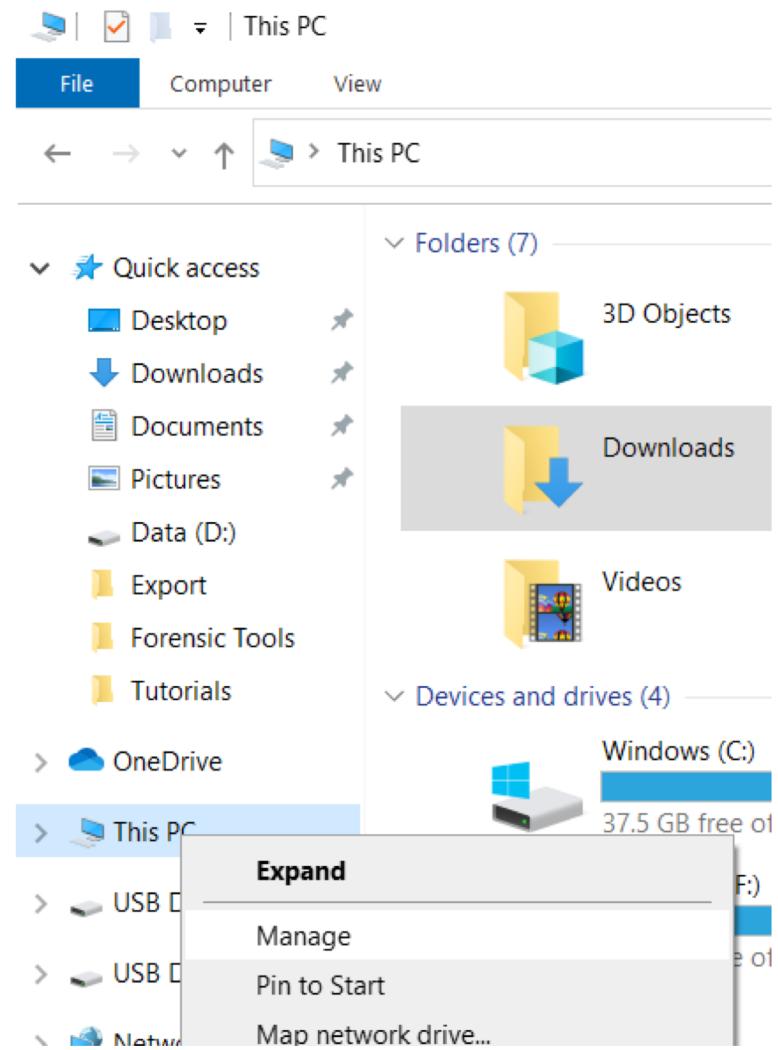
# Tracing a USB Device

- The recommendations from CA1 investigation suggested it would be beneficial to examine the desktop computer of Sarah Connor.
- Lets do this now.... In-Class Example....



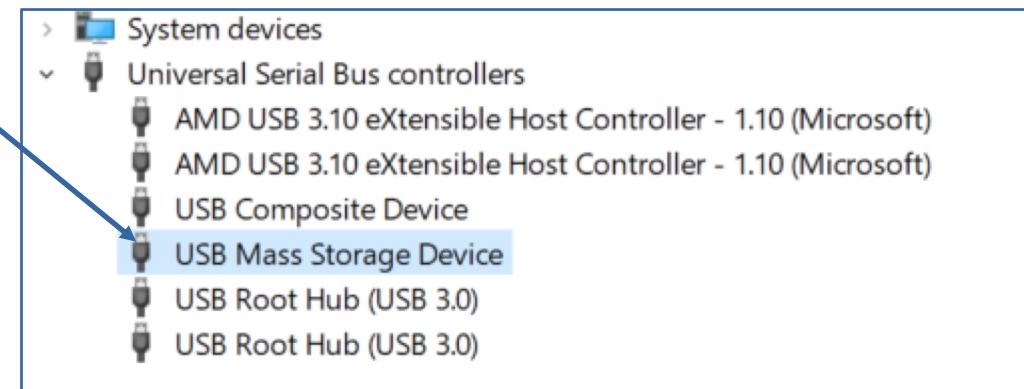
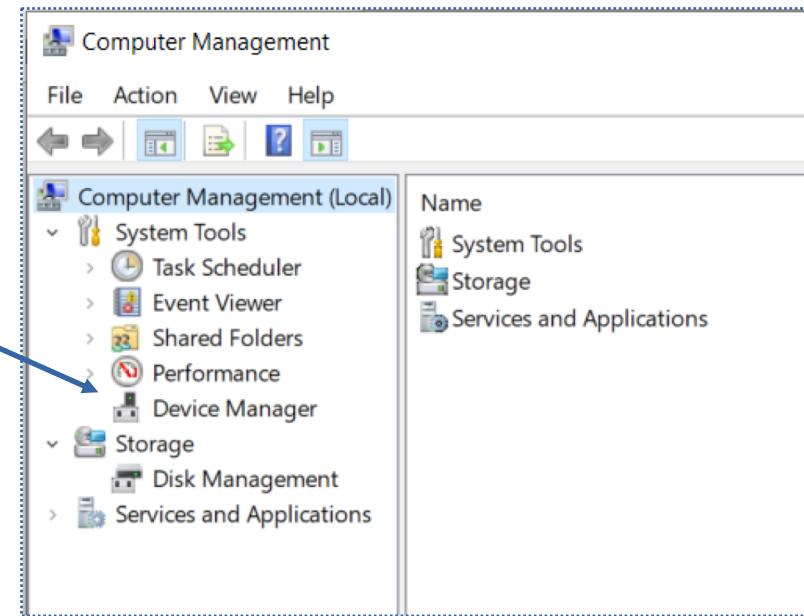
# Get USB Device ID (1/3)

- Open Windows Explorer
- Right Click This PC
- Select Manage



# Get USB Device ID (2/3)

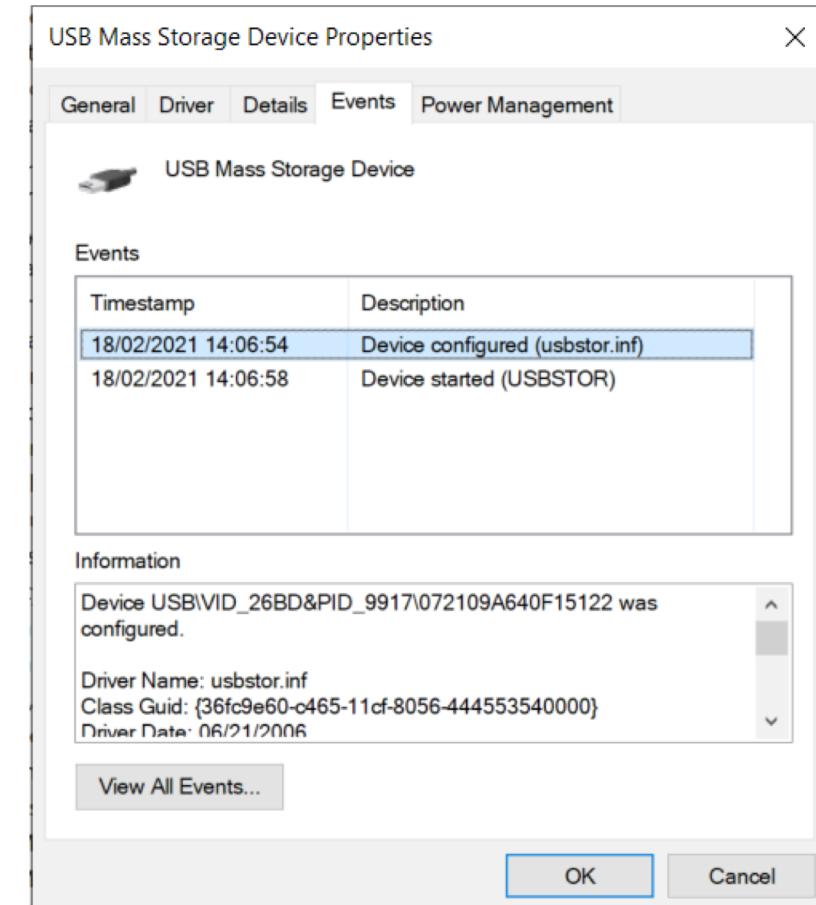
- In Computer Management
- Click Device Manager
- Expand USB Controllers
- Double click the device



# Get USB Device ID (3/3)

- The USB Mass Storage Device Properties will appear
- Click the Event Tab, this Information section contains the Device Info.

Device USB\VID\_26BD&PID\_9917\072109A640F15122 was configured.  
  
Driver Name: usbstor.inf  
Class Guid: {36fc9e60-c465-11cf-8056-444553540000}  
Driver Date: 06/21/2006  
Driver Version: 10.0.19041.1  
Driver Provider: Microsoft  
Driver Section: USBSTOR\_BULK.NT  
Driver Rank: 0xFF2000  
Matching Device Id: USB\Class\_08&SubClass\_06&Prot\_50  
Outranked Drivers:  
Device Updated: false  
Parent Device: USB\ROOT\_HUB30\5&10c37a43&0&0

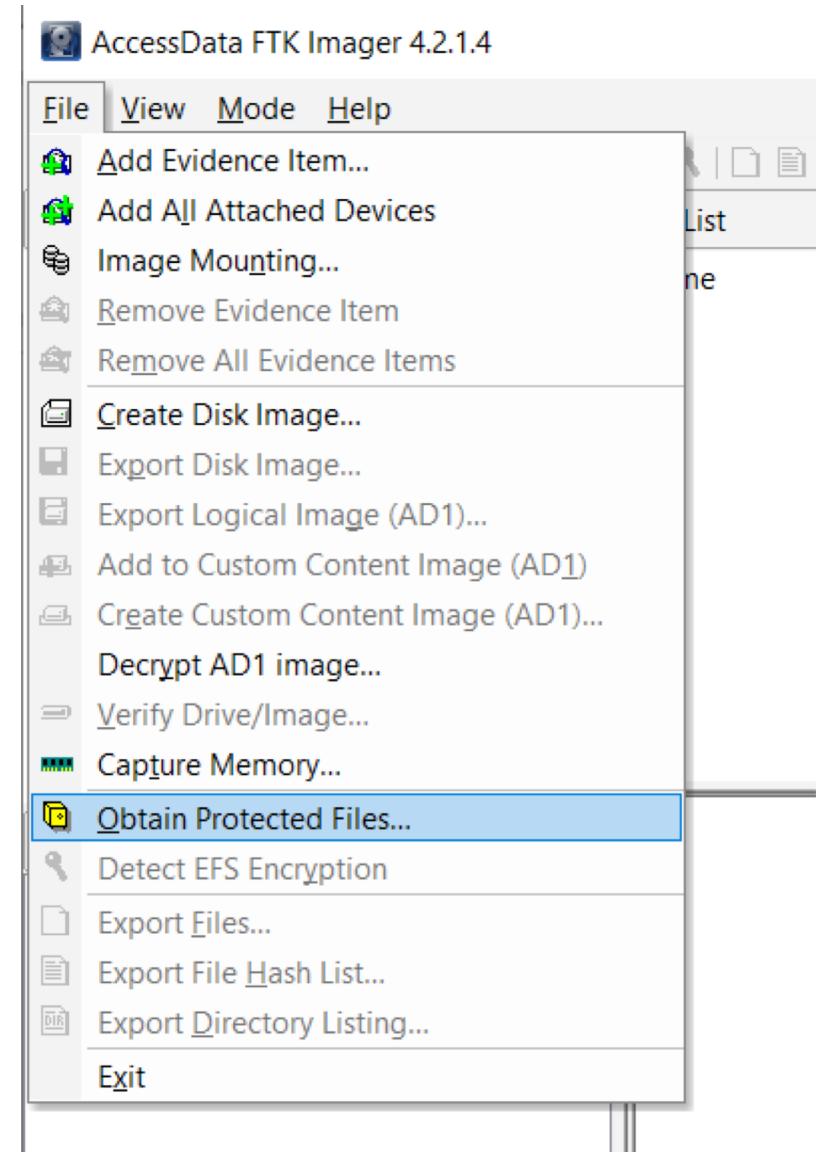


The Device ID is:  
072109A640F15122



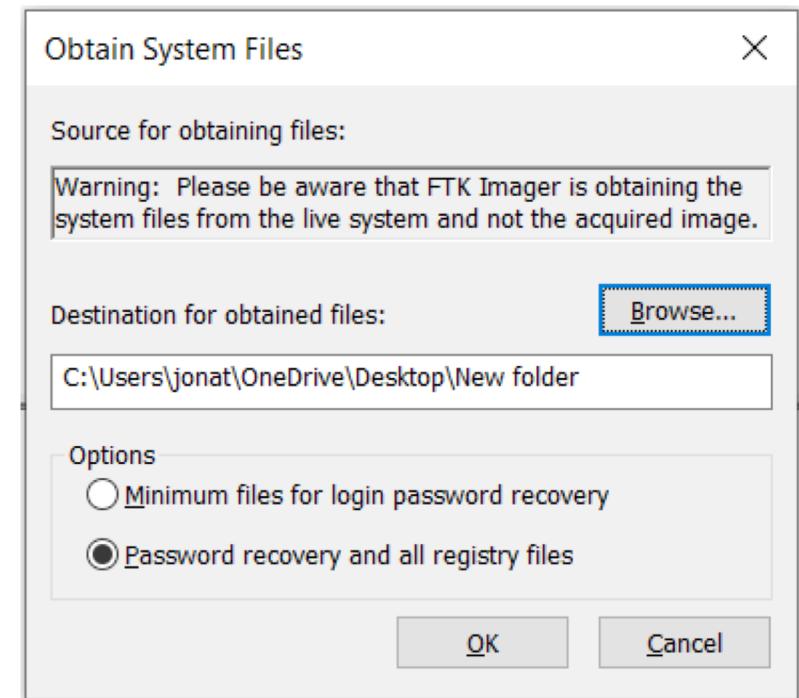
# FTK Imager to get NTUSER.dat (1/3)

- Open FTK Imager
- Select Obtain Protected Files...



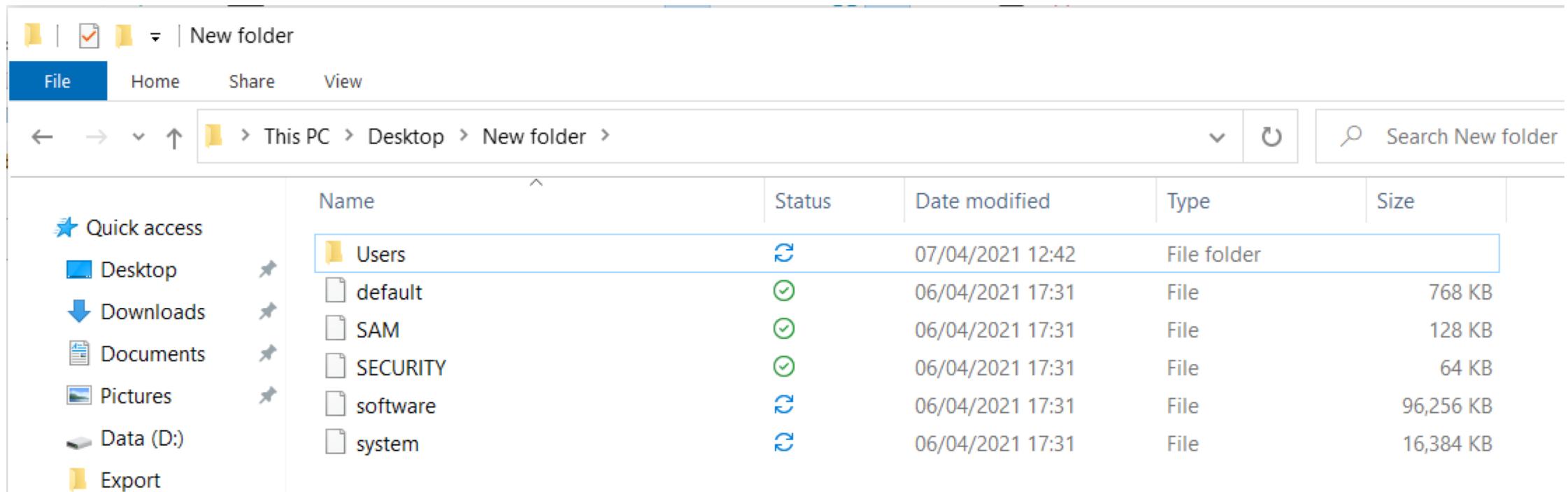
# FTK Imager to get NTUSER.dat (2/3)

- Select Password recovery and all registry files
- Pick a location to store the files
- Click ok



# FTK Imager to get NTUSER.dat (3/3)

- The files will be exported to the folder



# Examine NTUSER.dat

- AccessData Registry Viewer
- <https://accessdata.com/product-download>
- 



# NirSoft - USBDevview

- “USBDevview is a small utility that lists all USB devices that currently connected to your computer, as well as all USB devices that you previously used.”
- Source: [http://www.nirsoft.net/utils/usb\\_devices\\_view.html](http://www.nirsoft.net/utils/usb_devices_view.html)
- Offers data on device name/description, device type, serial number (for mass storage devices), the date/time that device was added, VendorID, ProductID, etc....



# NirSoft - USBDevview



Device Name	Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Serial Number	Registry Time 1	Registry Time 2	VendorID
0003.0000.0003.002.00...	Logitech USB Input Device	HID (Human Interface D...	No	Yes	No	No			05/02/2021 11:59:03	05/02/2021 11:59:03	046d
0003.0000.0003.002.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			05/02/2021 11:59:03	05/02/2021 11:59:03	046d
0003.0000.0003.002.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			05/02/2021 11:59:03	05/02/2021 11:59:03	046d
0003.0000.0003.002.00...	Logitech USB Input Device	HID (Human Interface D...	No	Yes	No	No			05/03/2021 08:56:20	05/03/2021 08:56:20	046d
0003.0000.0003.002.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			05/03/2021 08:56:20	05/03/2021 08:56:20	046d
0003.0000.0003.002.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No			05/03/2021 08:56:20	05/03/2021 08:56:20	046d
0003.0000.0003.004.00...	USB Video Device	Video	Yes	Yes	No	No			06/04/2021 17:31:57	22/07/2020 17:42:49	13d3
Port_#0001.Hub_#0001	Goodix Fingerprint USB Device	Communication	No	No	No	No		000000000001A	17/11/2020 21:02:52	22/07/2020 17:46:40	27c6
Port_#0001.Hub_#0002	Goodix Fingerprint USB Device	Communication	Yes	No	No	No			06/04/2021 17:31:58	17/11/2020 21:02:51	27c6
Port_#0002.Hub_#0001	USB Composite Device	Unknown	No	Yes	No	No			05/02/2021 11:58:24	05/02/2021 11:58:24	046d
Port_#0002.Hub_#0001	Generic USB Hub	Unknown	No	Yes	No	No			05/03/2021 08:56:20	05/03/2021 08:56:19	05e3
Port_#0002.Hub_#0001	TDK LoR TF10 USB Device	Mass Storage	No	Yes	No	No		C70058B48A43E583	03/02/2021 19:59:32	03/02/2021 19:59:30	0718
Port_#0002.Hub_#0001	USB2.0 CardReader SM XD US...	Mass Storage	No	Yes	No	No	G; H:	606569746801	17/02/2021 21:40:37	17/02/2021 21:40:37	0cf2
Port_#0002.Hub_#0001	Ut163 USB2FlashStorage USB ...	Mass Storage	No	Yes	No	No		071117214dc0e3	18/02/2021 11:09:25	18/02/2021 11:09:25	1307
Port_#0002.Hub_#0001	General UDisk USB Device	Mass Storage	No	Yes	No	No		1311301642332816...	21/02/2021 22:05:07	17/02/2021 22:05:15	abcd
Port_#0002.Hub_#0002	Realtek Bluetooth Adapter	Bluetooth Device	Yes	Yes	No	No		00e04c000001	06/04/2021 17:31:57	17/11/2020 21:02:46	1358
Port_#0002.Hub_#0003	USB Composite Device	Unknown	No	Yes	No	No			05/03/2021 08:56:20	05/03/2021 08:56:20	046d
Port_#0003.Hub_#0001	SanDisk Cruzer Blade USB Dev...	Mass Storage	No	Yes	No	No		4C53059994032010...	04/03/2021 17:43:35	04/03/2021 17:43:35	0781
Port_#0003.Hub_#0001	SanDisk Cruzer Blade USB Dev...	Mass Storage	No	Yes	No	No		4C53200001032412...	04/03/2021 16:02:11	22/01/2021 23:43:34	0781
Port_#0003.Hub_#0001	Flash Drive OT_USB20 USB Dev...	Mass Storage	No	Yes	No	No		382F422F350E007A	17/02/2021 22:25:19	03/02/2021 19:25:48	0ea0
ov9734_azurewave_ca...	USB Composite Device	Unknown	Yes	Yes	No	No		0x0001	06/04/2021 17:31:56	22/07/2020 17:42:34	13d3
Port_#0006.Hub_#0001	USB Attached SCSI (UAS) Mas...	Mass Storage	No	No	No	No		MSFT30NA333D28	02/01/2021 21:57:58	30/12/2020 21:58:48	0bc2
Port_#0006.Hub_#0001	VirtualBox USB	Vendor Specific	No	Yes	No	No		MSFT30NA333D28	03/01/2021 16:54:21	03/01/2021 16:54:21	80ee
Port_#0006.Hub_#0002	ASIX AX88179 USB 3.0 to Giga...	Vendor Specific	No	Yes	No	No		00000007600305	17/11/2020 22:37:06	17/11/2020 21:02:52	0b95
Port_#0002.Hub_#0001	USB DISK 2.0 USB Device	Mass Storage	No	Yes	No	No	E:	072109A640F15122	07/04/2021 13:53:53	18/02/2021 13:06:54	26bd

25 item(s)

NirSoft Freeware. <http://www.nirsoft.net>

usb.ids is not loaded

Source: [http://www.nirsoft.net/utils/usb\\_devices\\_view.html](http://www.nirsoft.net/utils/usb_devices_view.html)

# Registry Editor

- <https://ericzimmerman.github.io/#!index.md>
- Registry viewer with searching, multi-hive support, plugins, and more. Handles locked files.
- *“The capabilities of Registry Explorer and RECcmd allows for quickly examining multiple hives at once and they can be leveraged to find new places where currently understood data is located in an easy to use and systematic way. It can be used in educational settings to not only understand the Registry from a functional level, but also from a deeply technical perspective.”*

Source: Registry Explorer User Guide

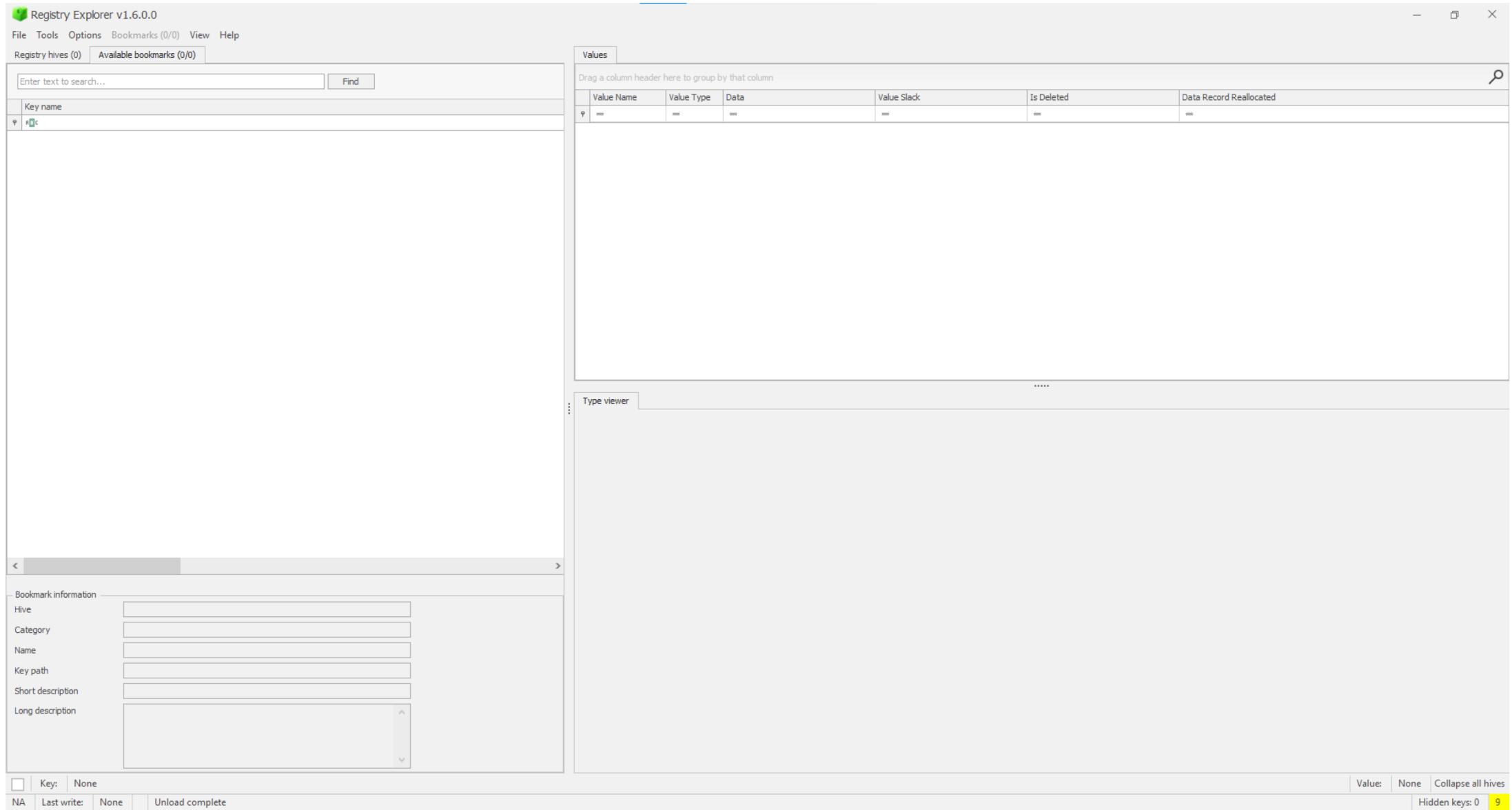


# Registry Editor

- “*Registry Explorer is a GUI based tool used to view the contents of offline Registry Hives. It can load multiple hives at once, search across all loaded hives using strings or regular expressions, exporting of data, and much more.*” Source: *Registry Explorer User Guide*



# Registry Editor



# Registry Editor - Example

- In Class Demo



# Questions

