FORENSICS

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.

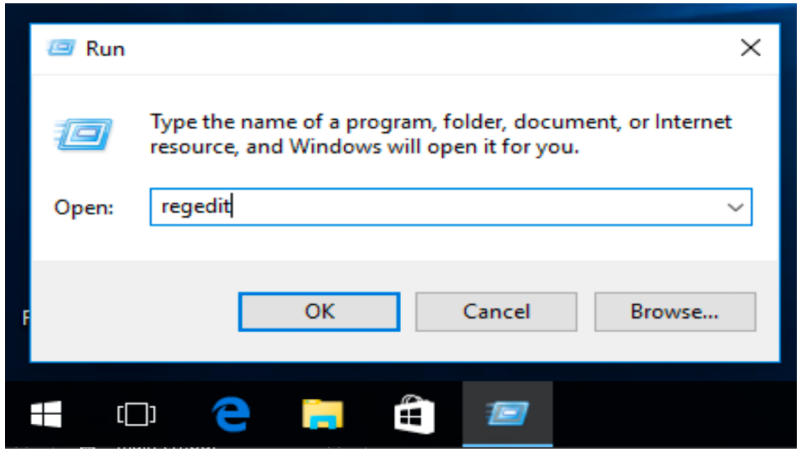
- Configurations and settings used by components, services, applications etc…
- Registry primarily uses Key / Value pairs.
- Registry Keys are objects that provides logical structure (kind of like folders)
- Values store data and they contain the actual settings.
- *"The Registry contains information 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

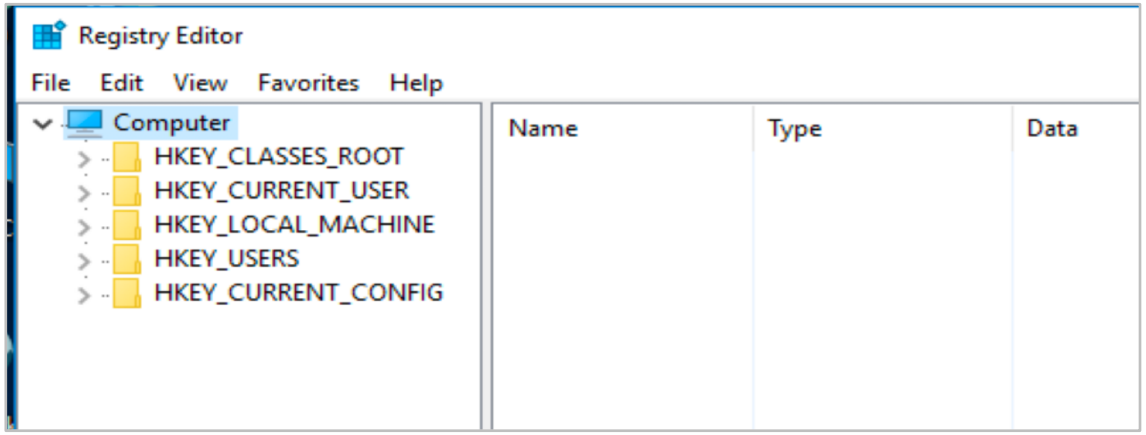
Notable content in the Registry

- 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



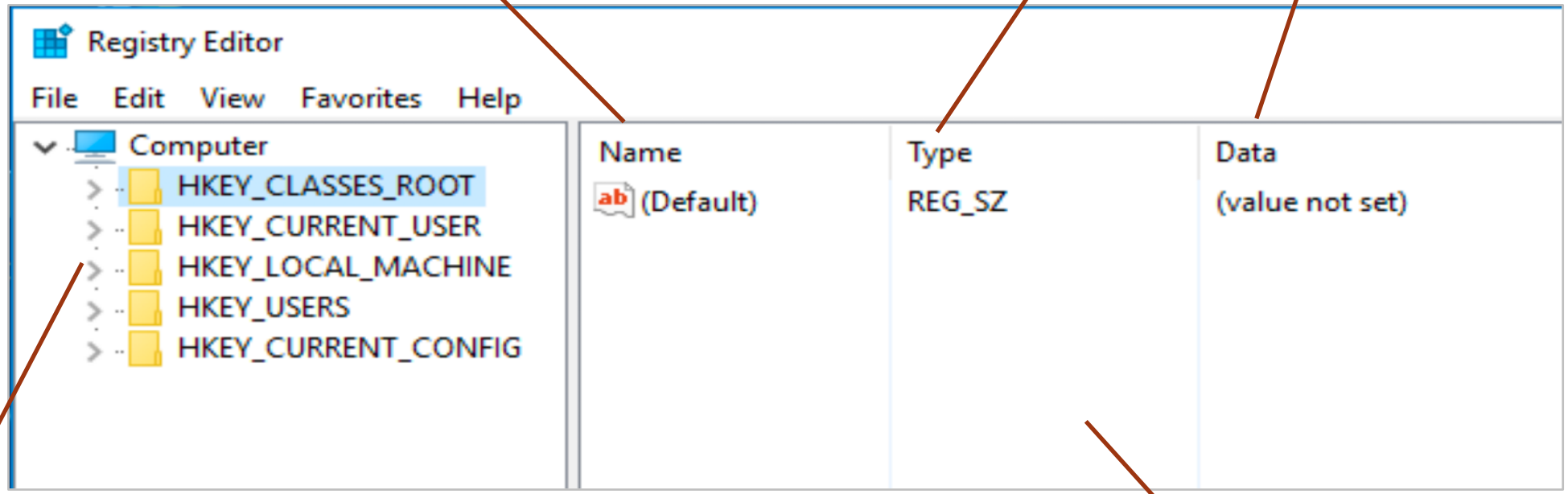


REGISTRY STRUCTURE

Entry Names

Data Types

Values

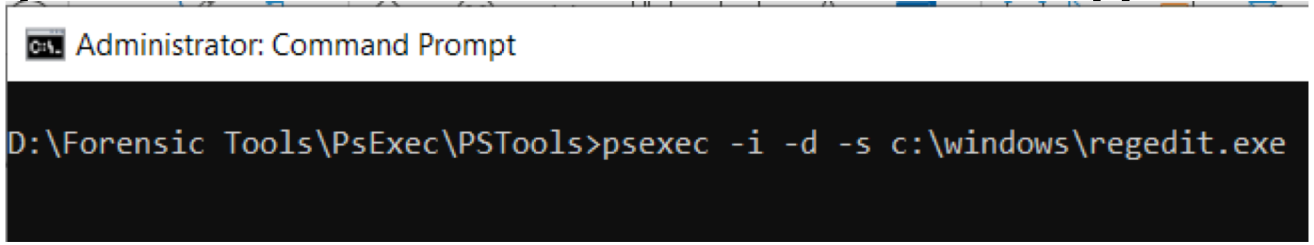


Tree View
Shows all the Keys and subkeys

Shows all the Values

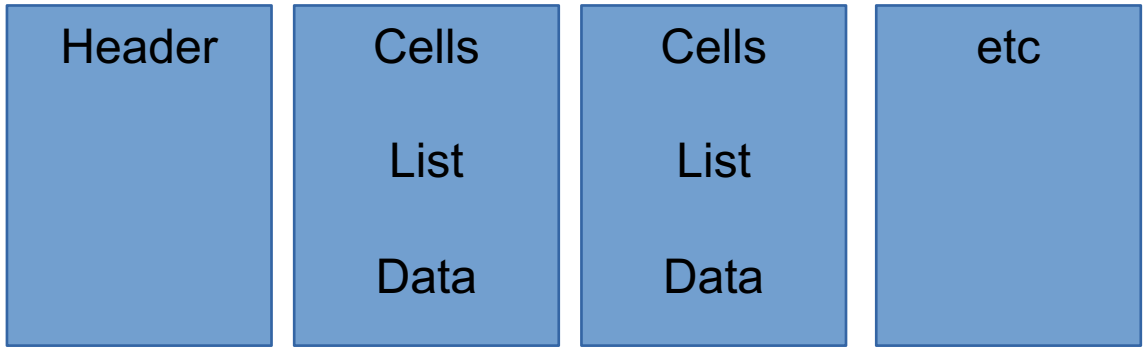
Run Regedit as System

- 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



What is a Registry Hive

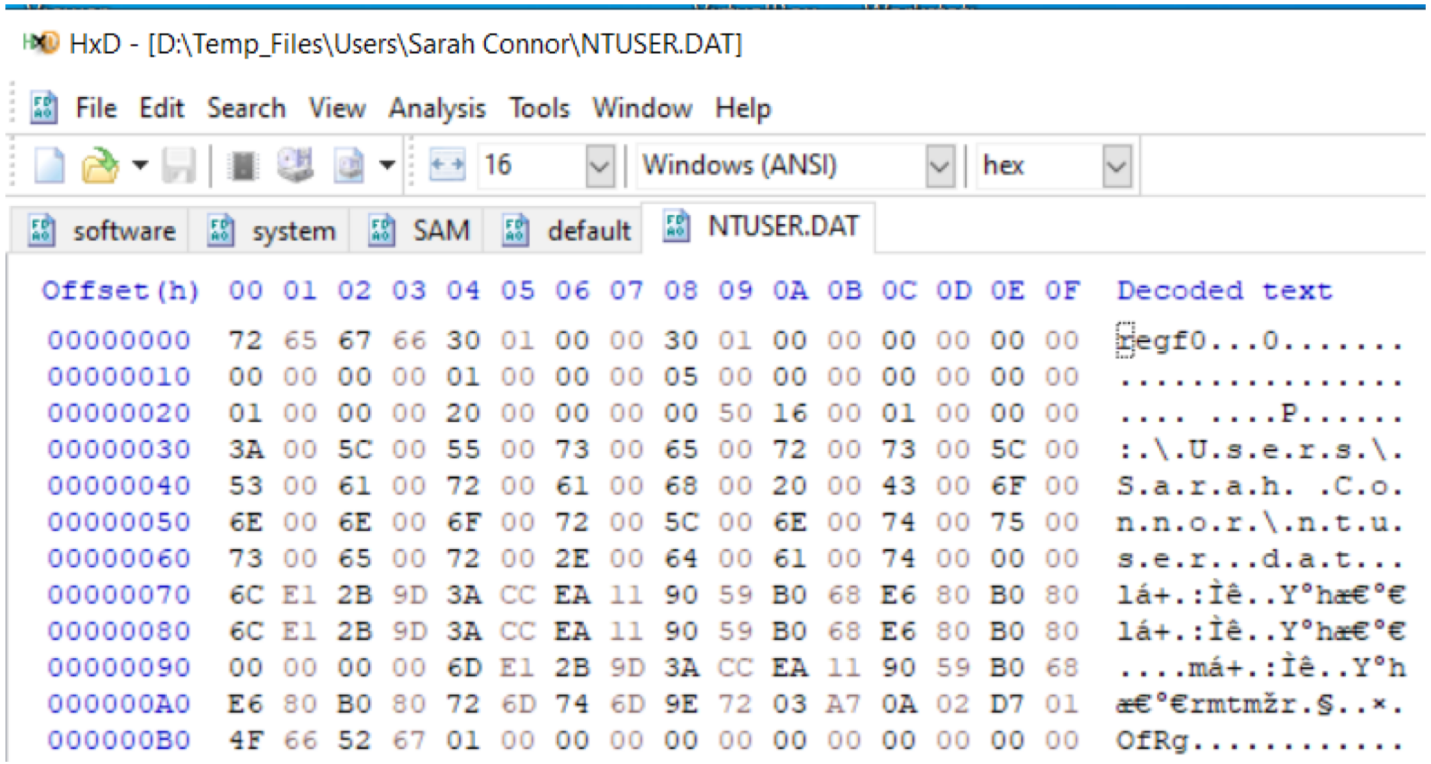
- A Hive is a major section in the Windows Registry.
- It contains a group of keys, subkeys, and values in the registry that has a set of supporting files that contain backups of its data.
- The Hives are a set of files. Each Hive is a hierarchical structure.
- Paths to hives are set in the Configuration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



- 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

Source: https://techcommunity.microsoft.com/t5/ask-the-performance-team/windows-architecture-registry-101/ba-p/372358

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

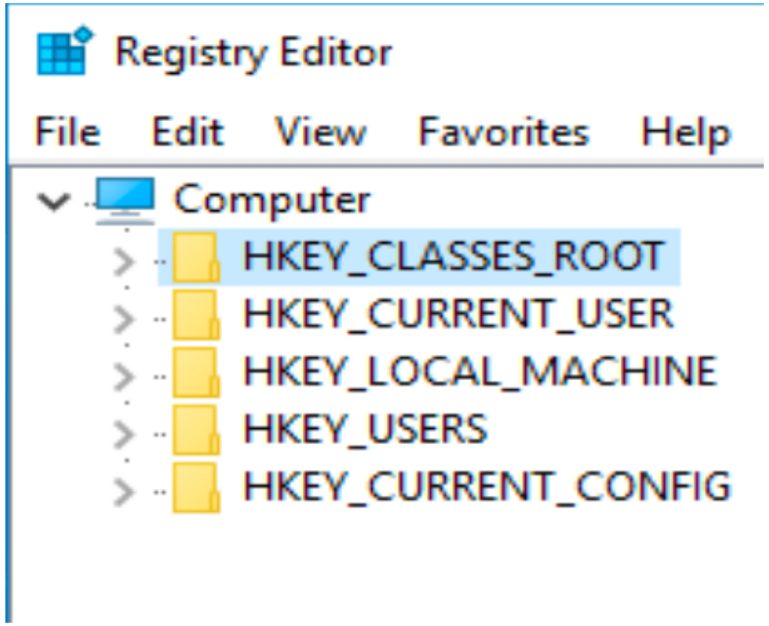
- The TimeZoneKeyName holds the time zone info
- Daylight saver info is available here too.

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.

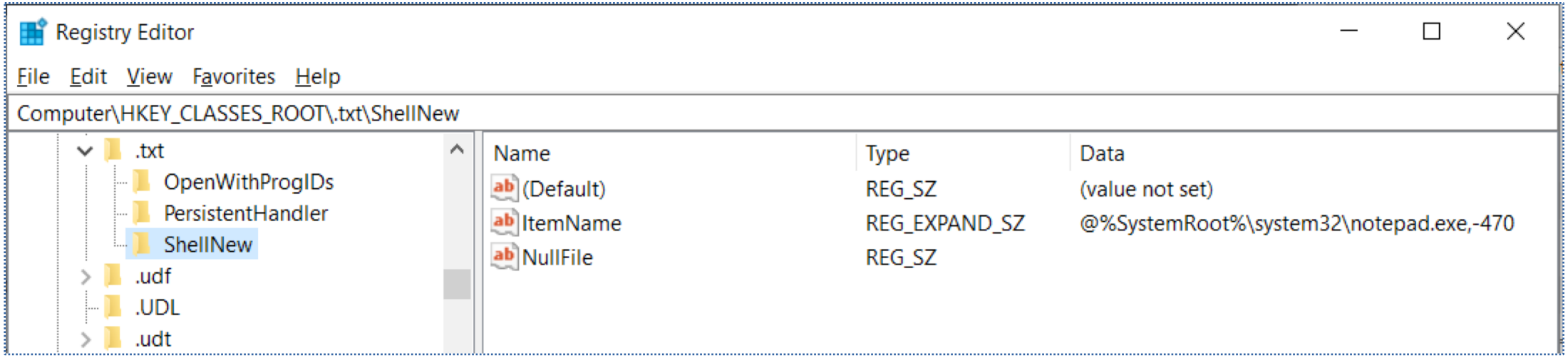
ROOT KEYS - HKEY_CLASSES_ROOT (HKCR)

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

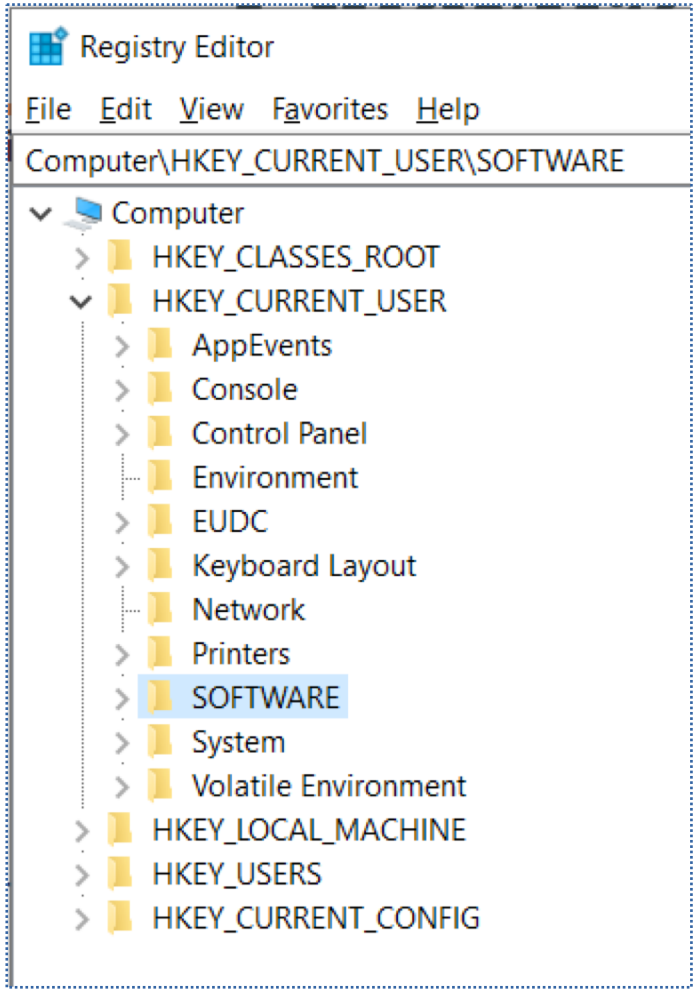
HKCR - EXAMPLE

- HKEY_CLASSES_ROOT



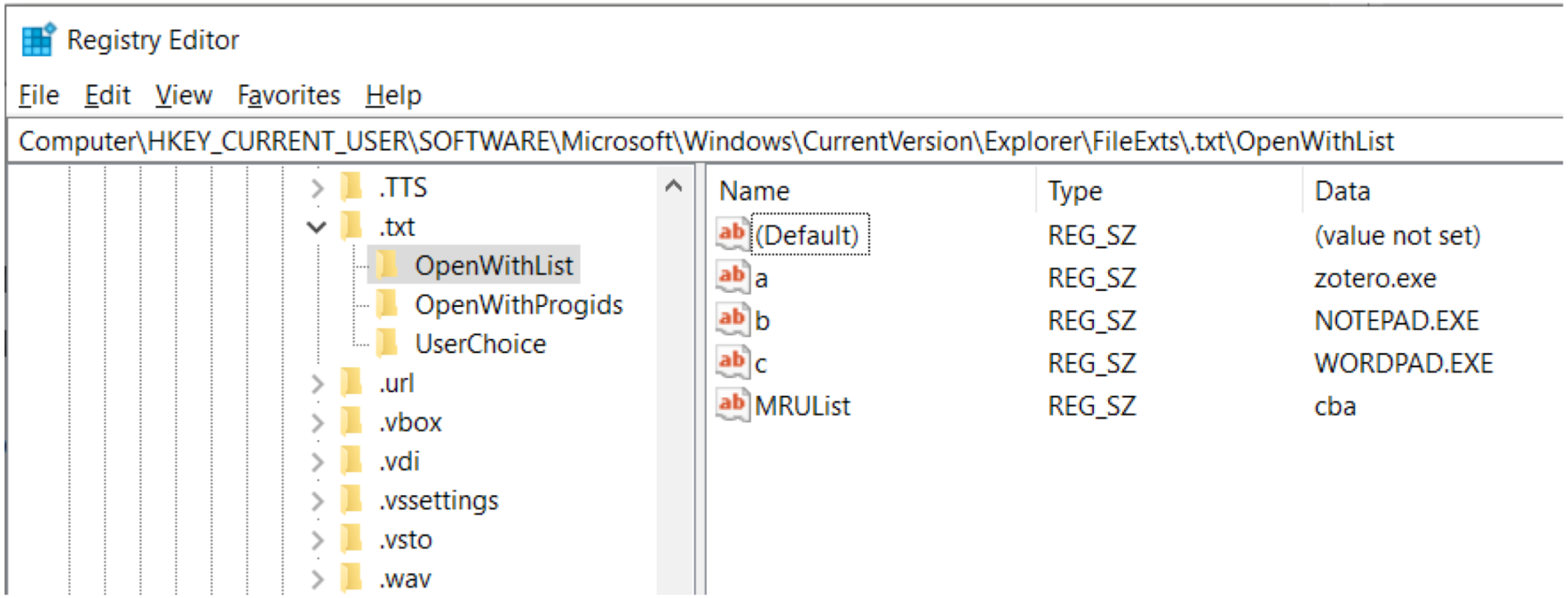
ROOTKEYS - HKEY_CURRENT_USER (HKCU)

- 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

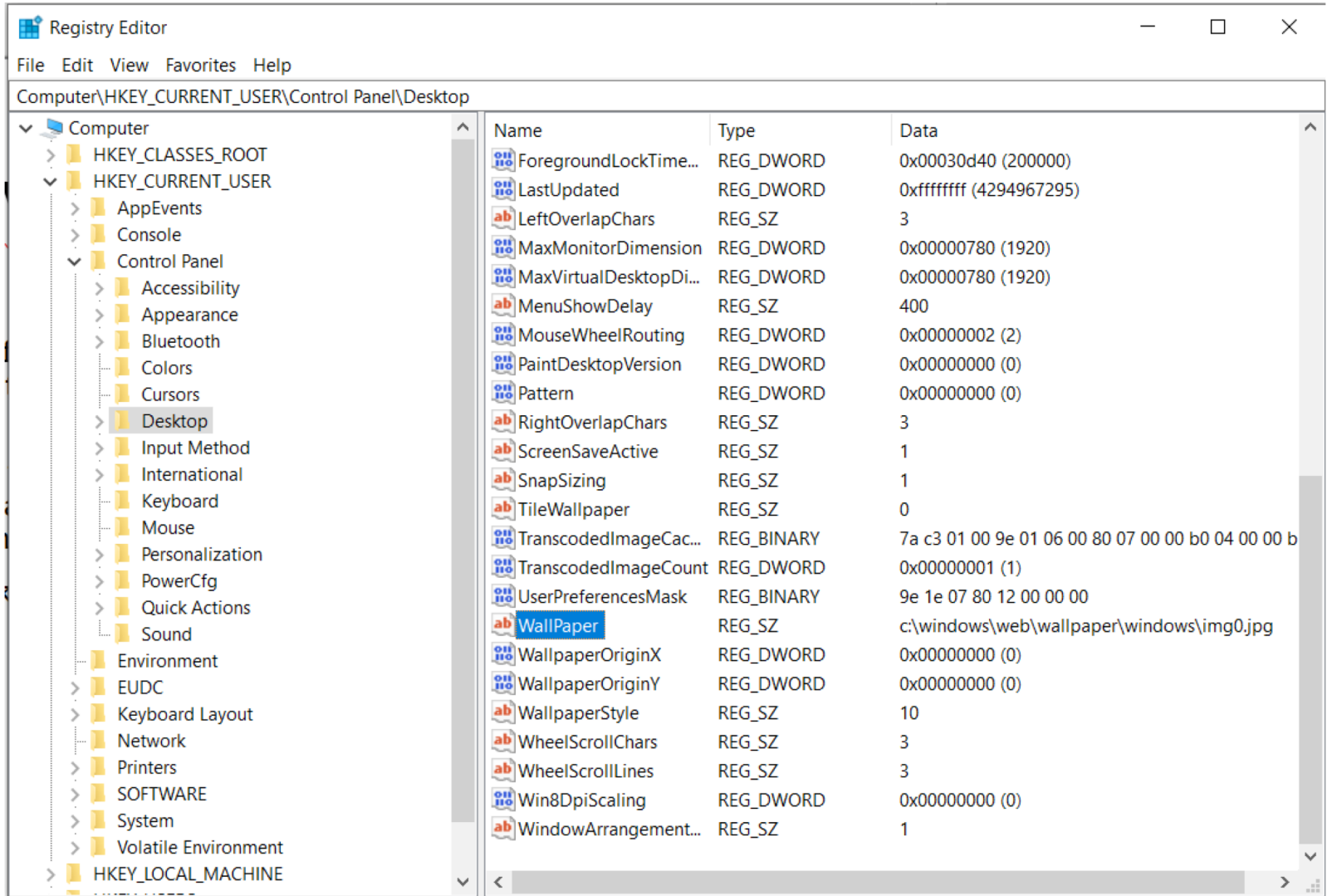
- Change default from notepad to wordpad for .txt (Using Windows Explorer)



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt\OpenWithList

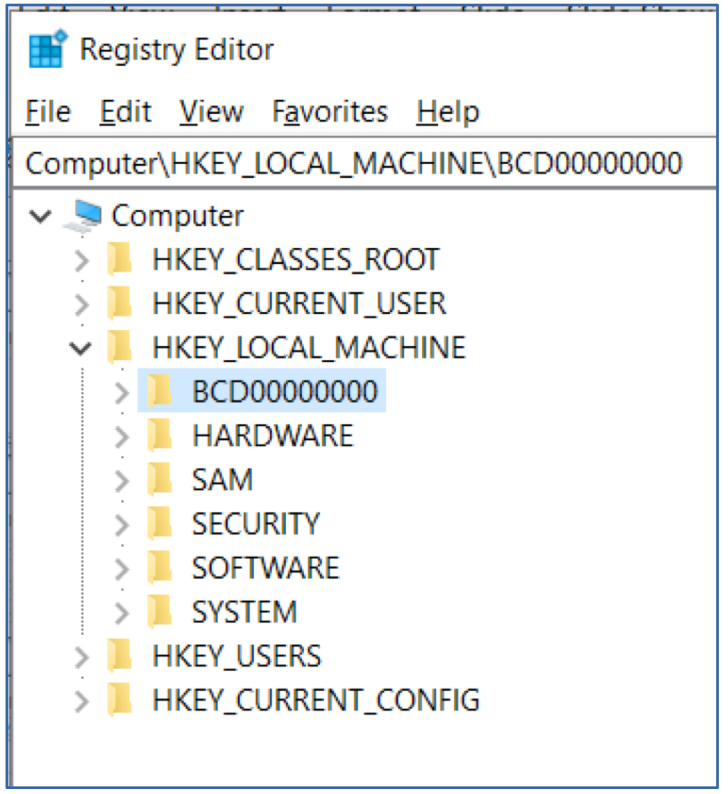
HKCU - EXAMPLE

- Example



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)



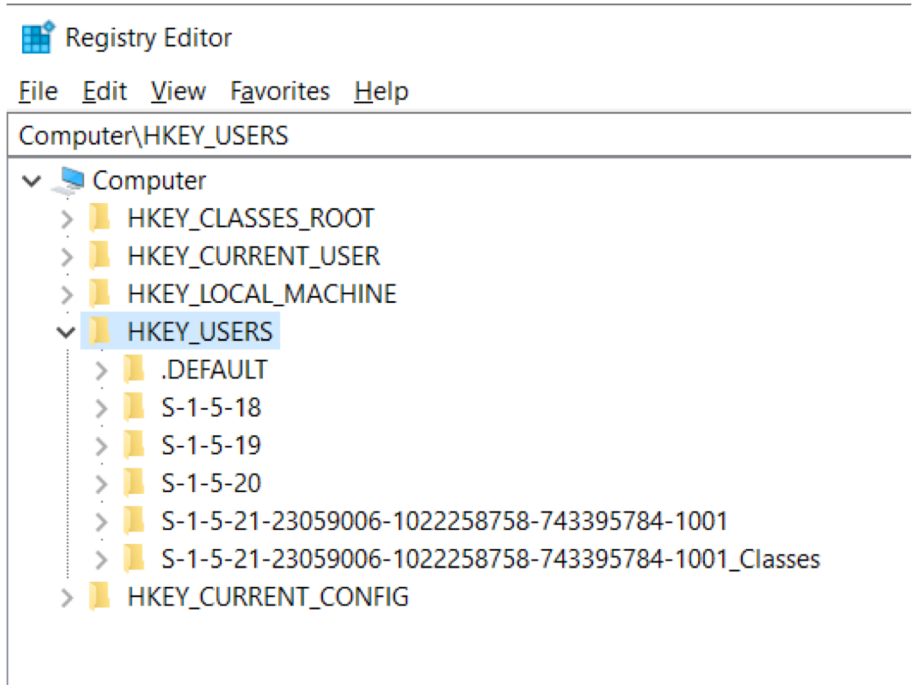
HKEY_LOCAL_MACHINE - BCD00000000

- 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 bcdedit.exe, not regedit

ROOT KEYS - HKEY_USERS (HKU)

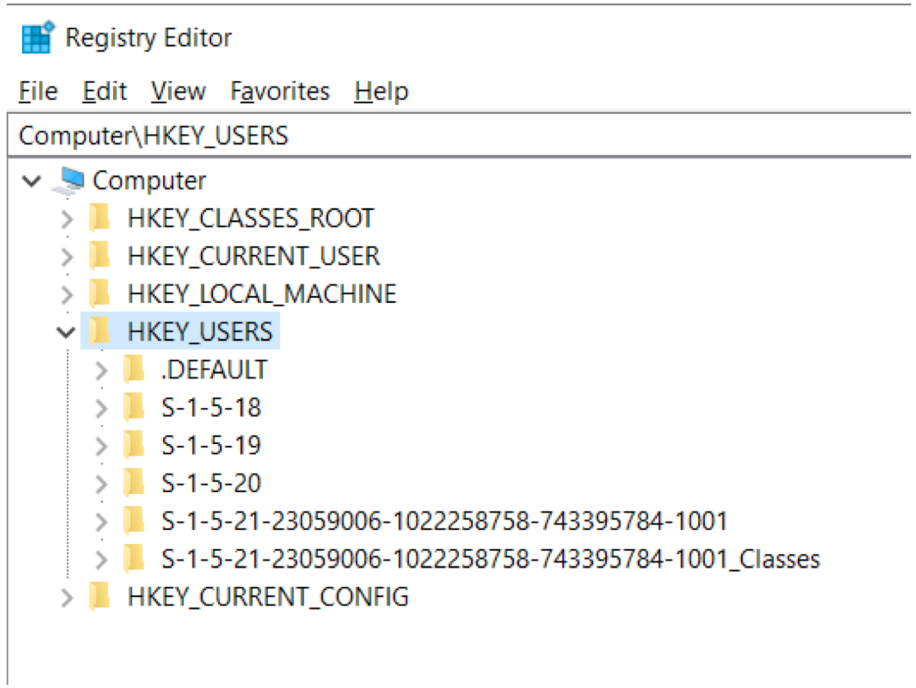
- Contains user-specific configuration information for all currently active users on the computer
- Each key under HKU is a user on the system and is linked with a security ID (SID)
- This is loaded when user logs on.
- Stores info on:
  - Mapped drives
  - Printers
  - Env variables
  - Etc...



ROOT KEYS - HKEY_USERS (HKU)

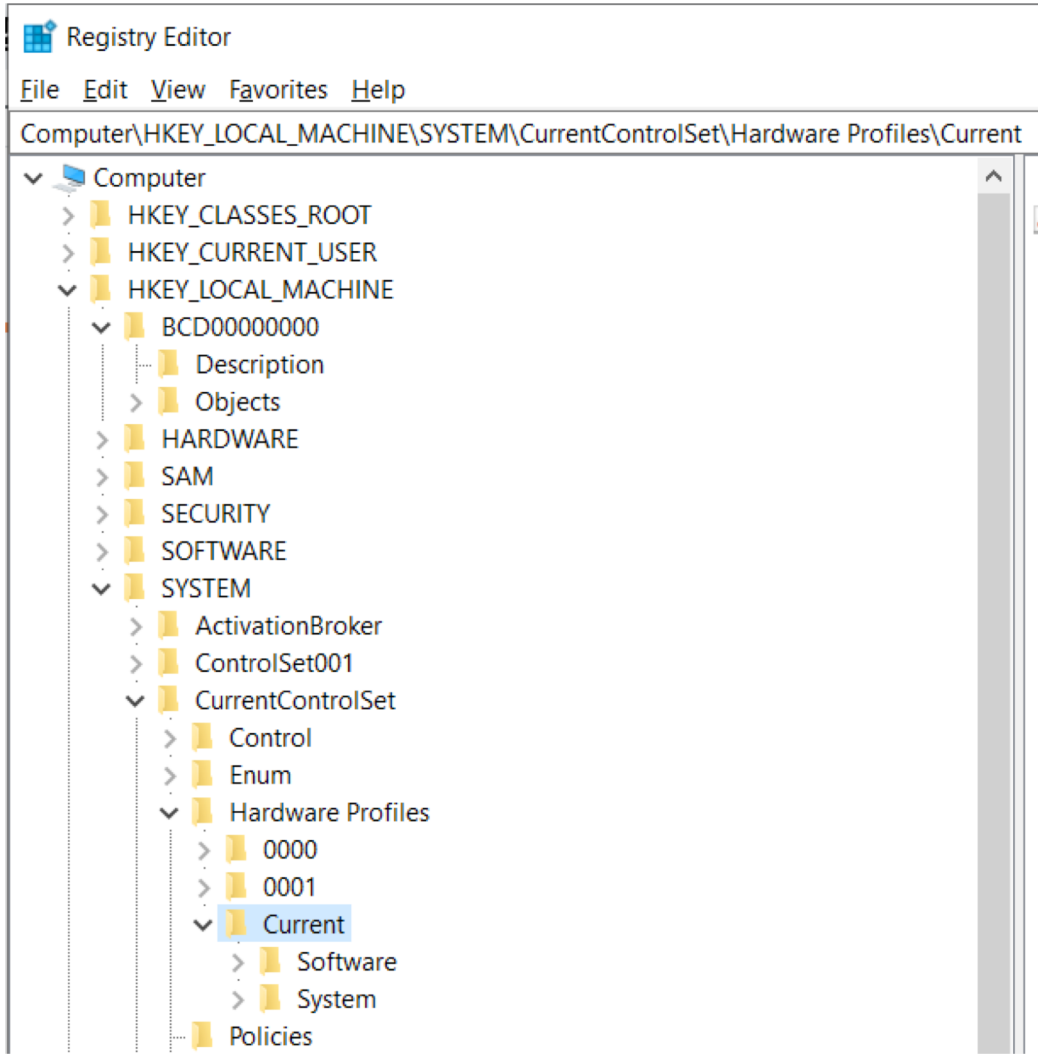
Administrator: Command Prompt

```
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>
```



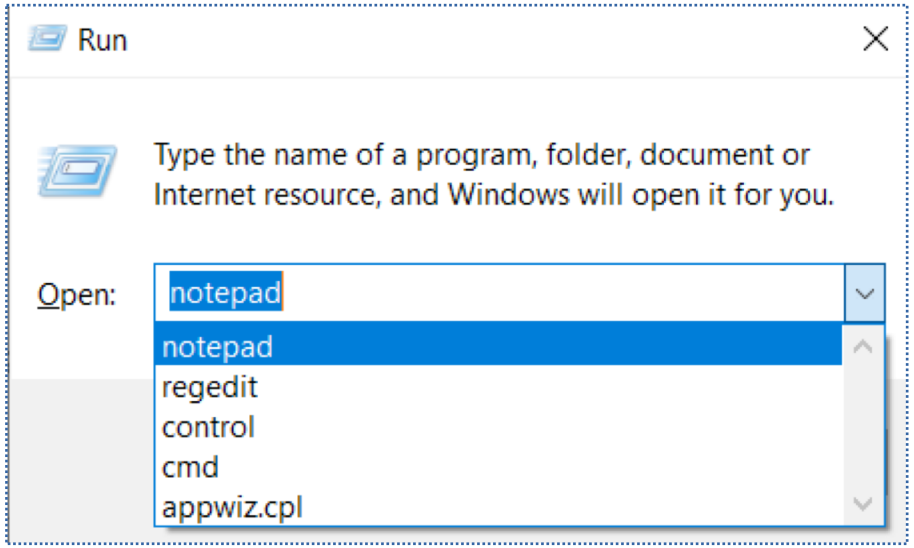
ROOT KEYS – HKEY_CURRENT_CONFIG (HKCC)

- 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\CurrentControlSet\Hardware Profiles\Current

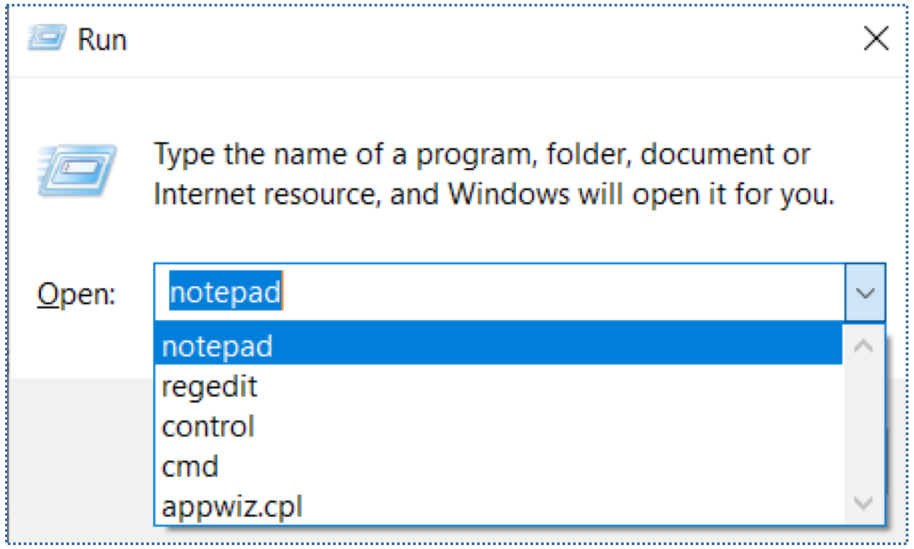


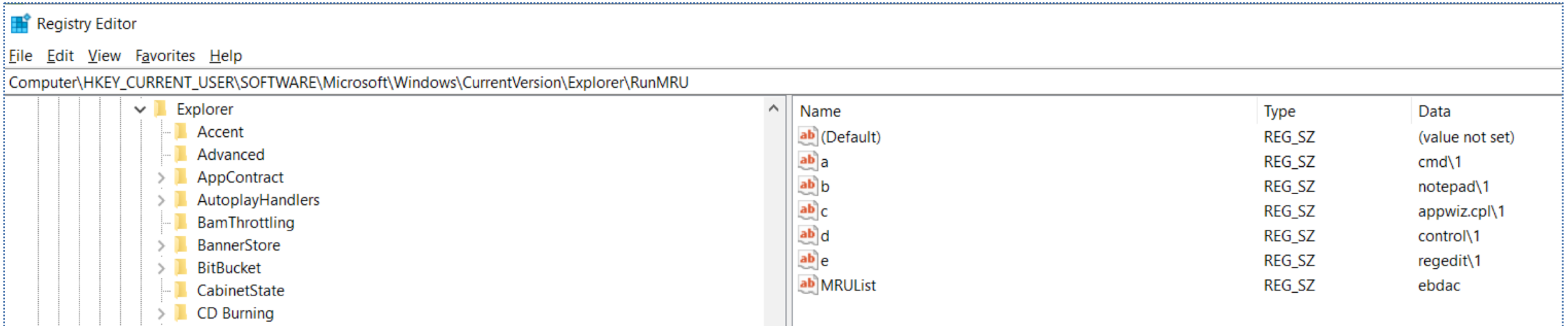
MOST RECENTLY USED (MRU)

- 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:

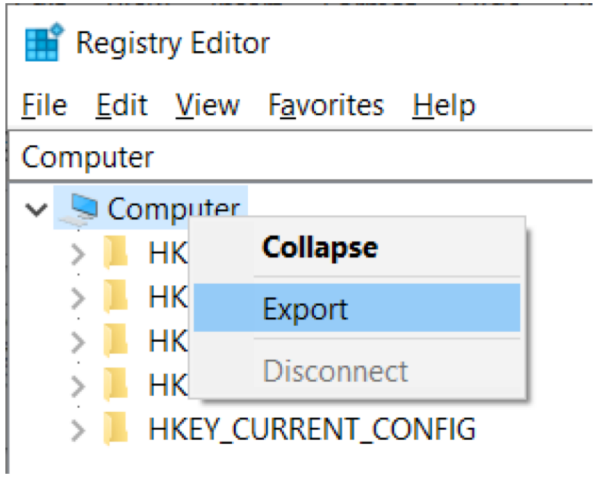


MOST RECENTLY USED (MRU)

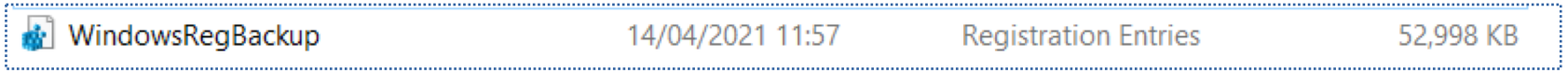




BACKUP THE REGISTRY



- In Registry Explorer, right click a key and export.
- This example is HKEY_CLASSES_ROOT



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

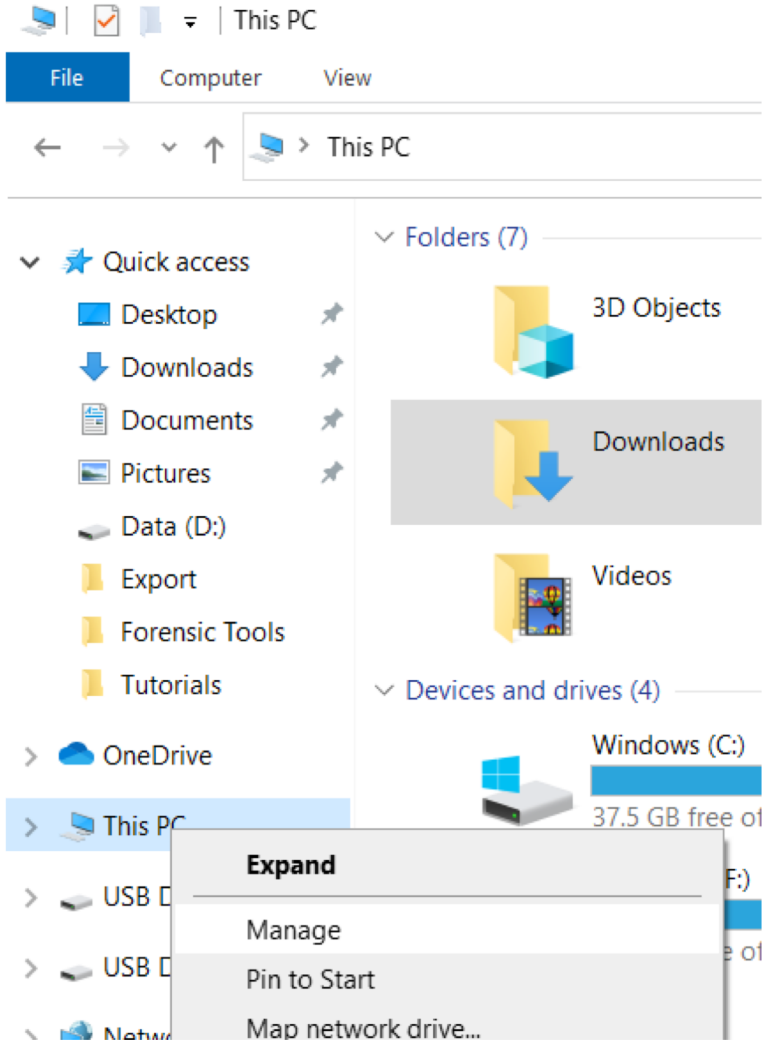
Tracing a USB Device

- 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….

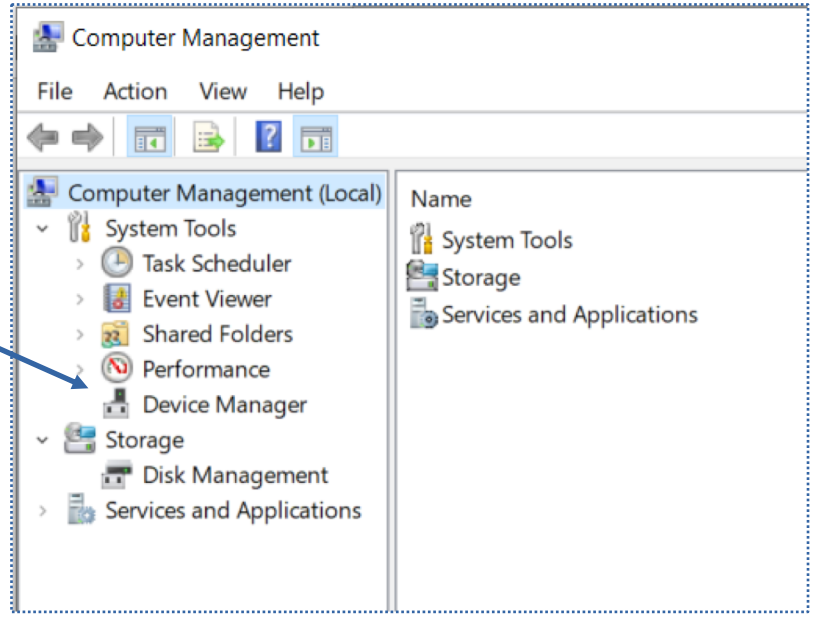
Get USB Device ID (1/3)

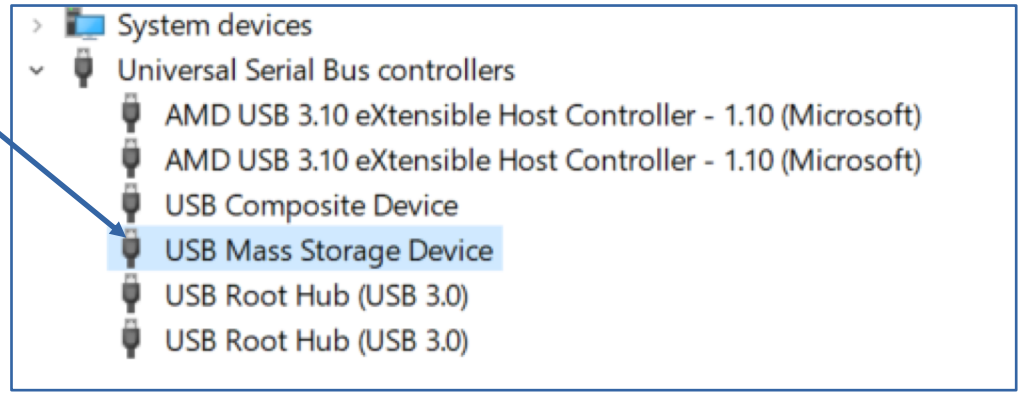
- Open Windows Explorer
- Right Click **This PC**
- Select **Manage**



Get USB Device ID (2/3)

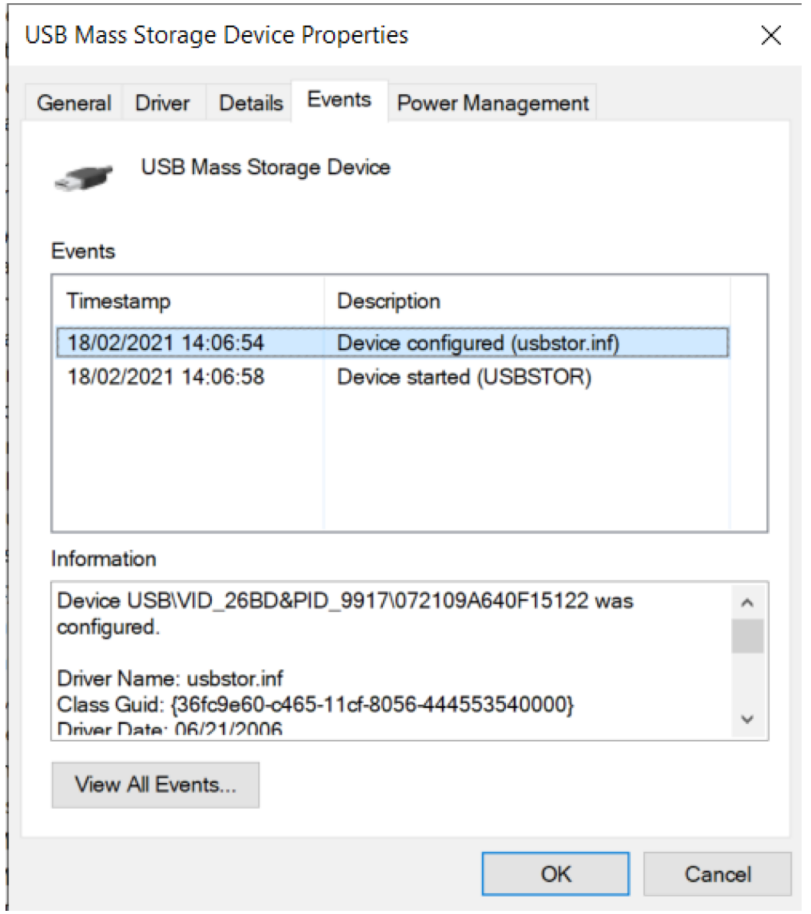
- In Computer Management
- Click Device Manager
- Expand USB Controllers
- Double click the device





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.



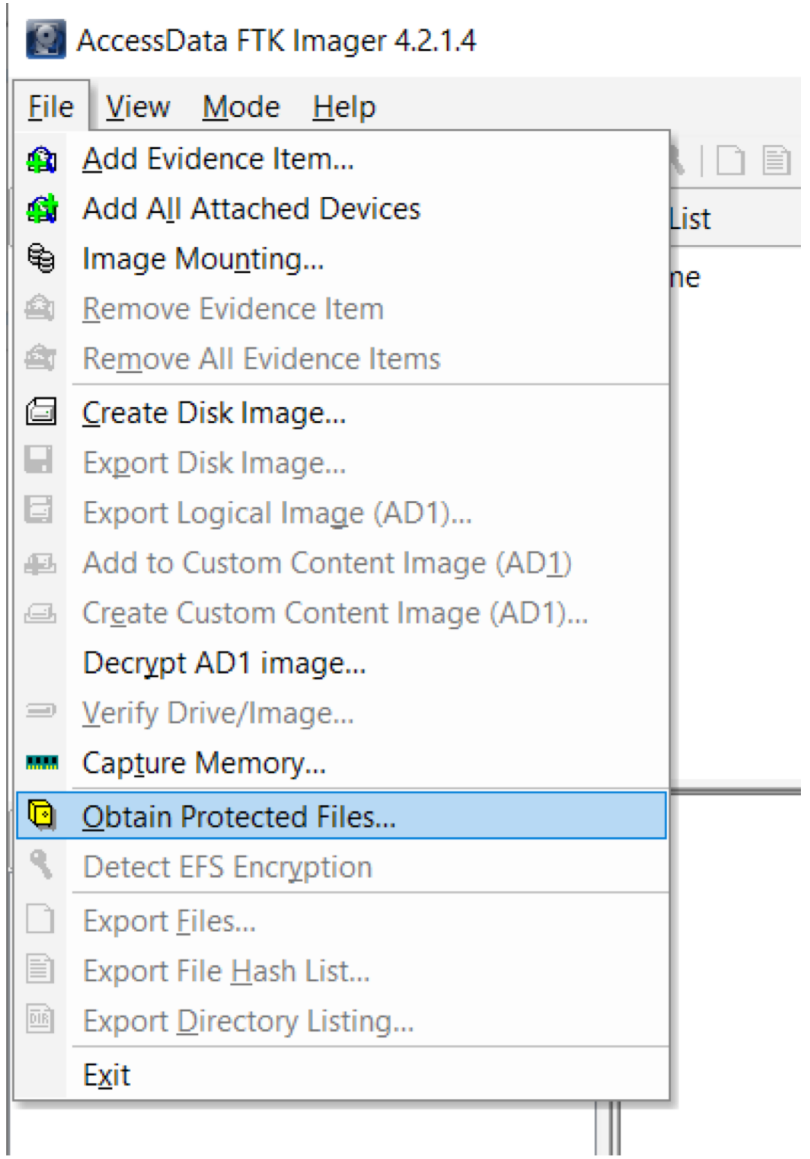
Device USB\VID_26BD&PID_9917\072109A640F15122 was configured.

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

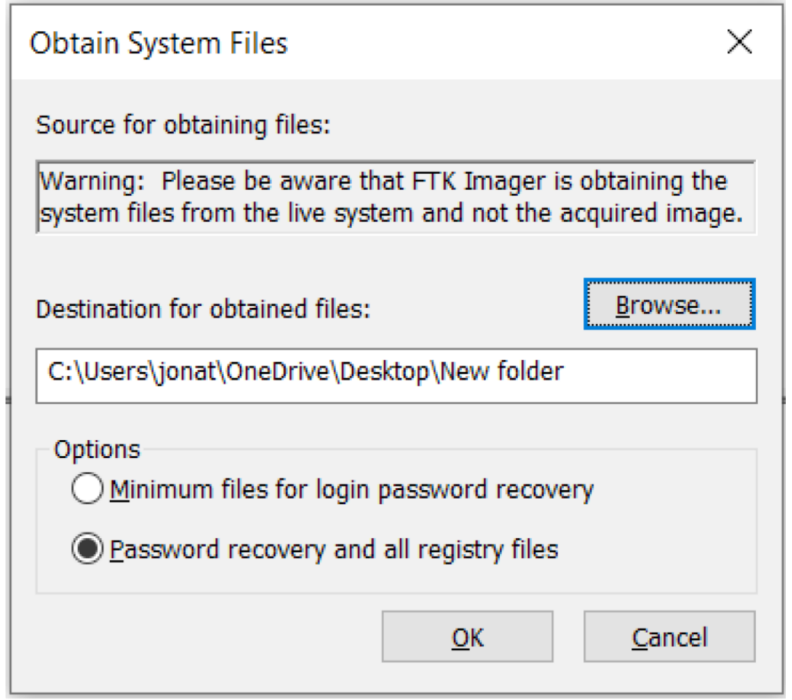
FTK Imager to get NTUSER dat (1/3)

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



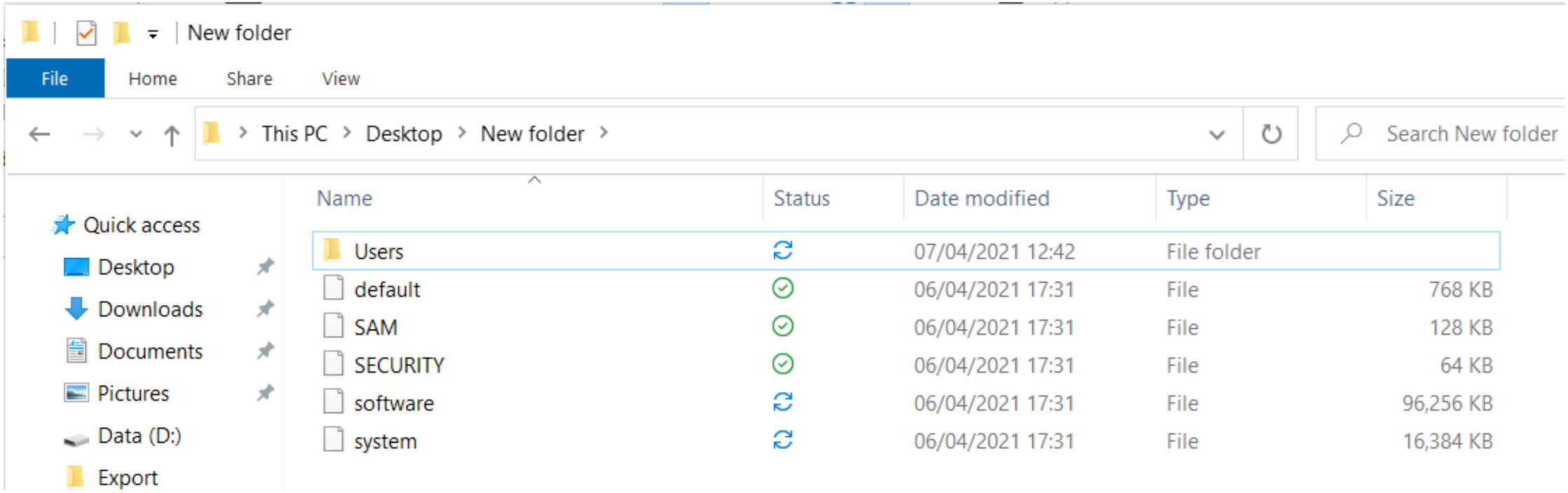
FTK Imager to get NTUSER dat (2/3)

- 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



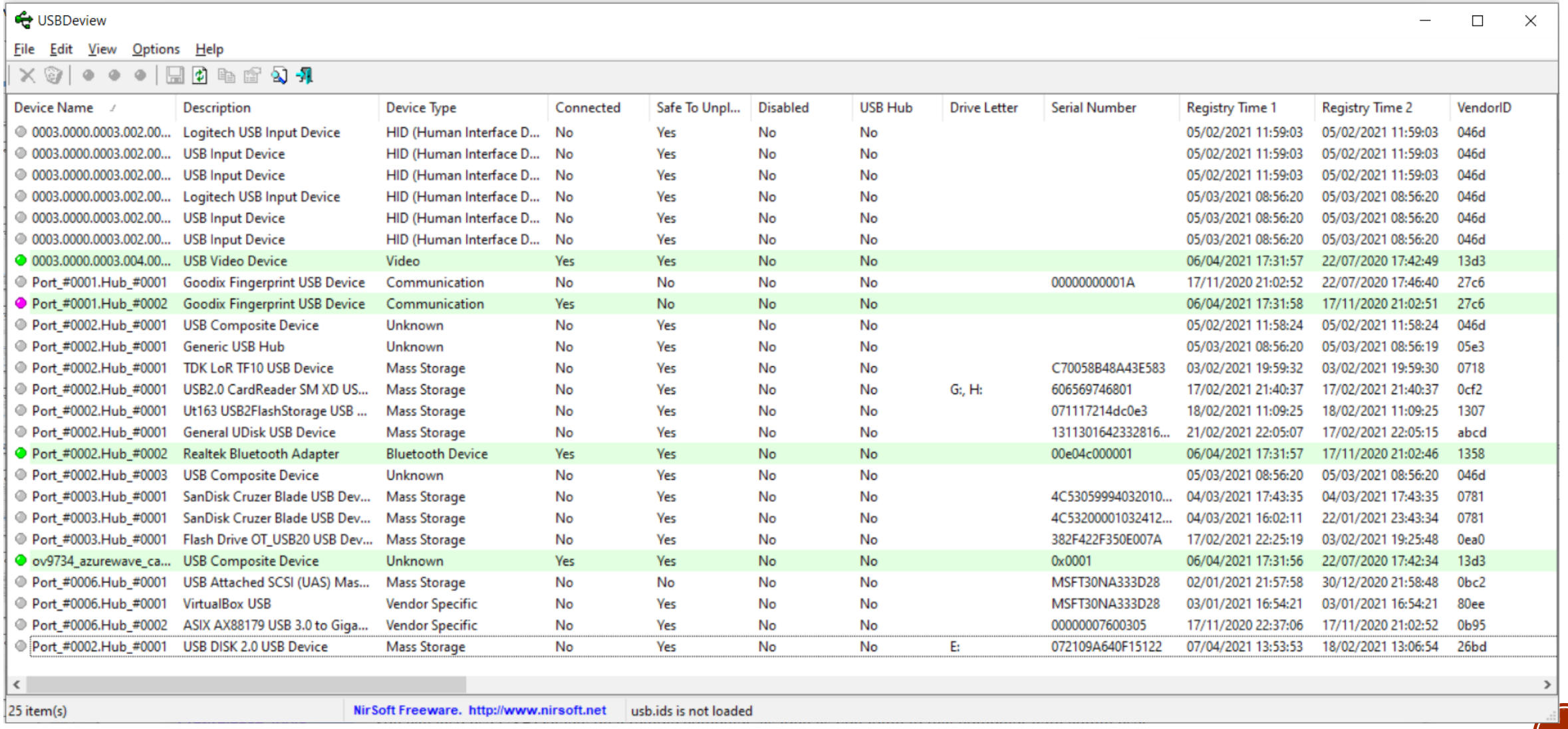
Examine NTUSER.dat

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

NirSoft - USBDeview

- “USBDeview 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
- 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 - USBDeview



Source: http://www.nirsoft.net/utils/usb_devices_view.html

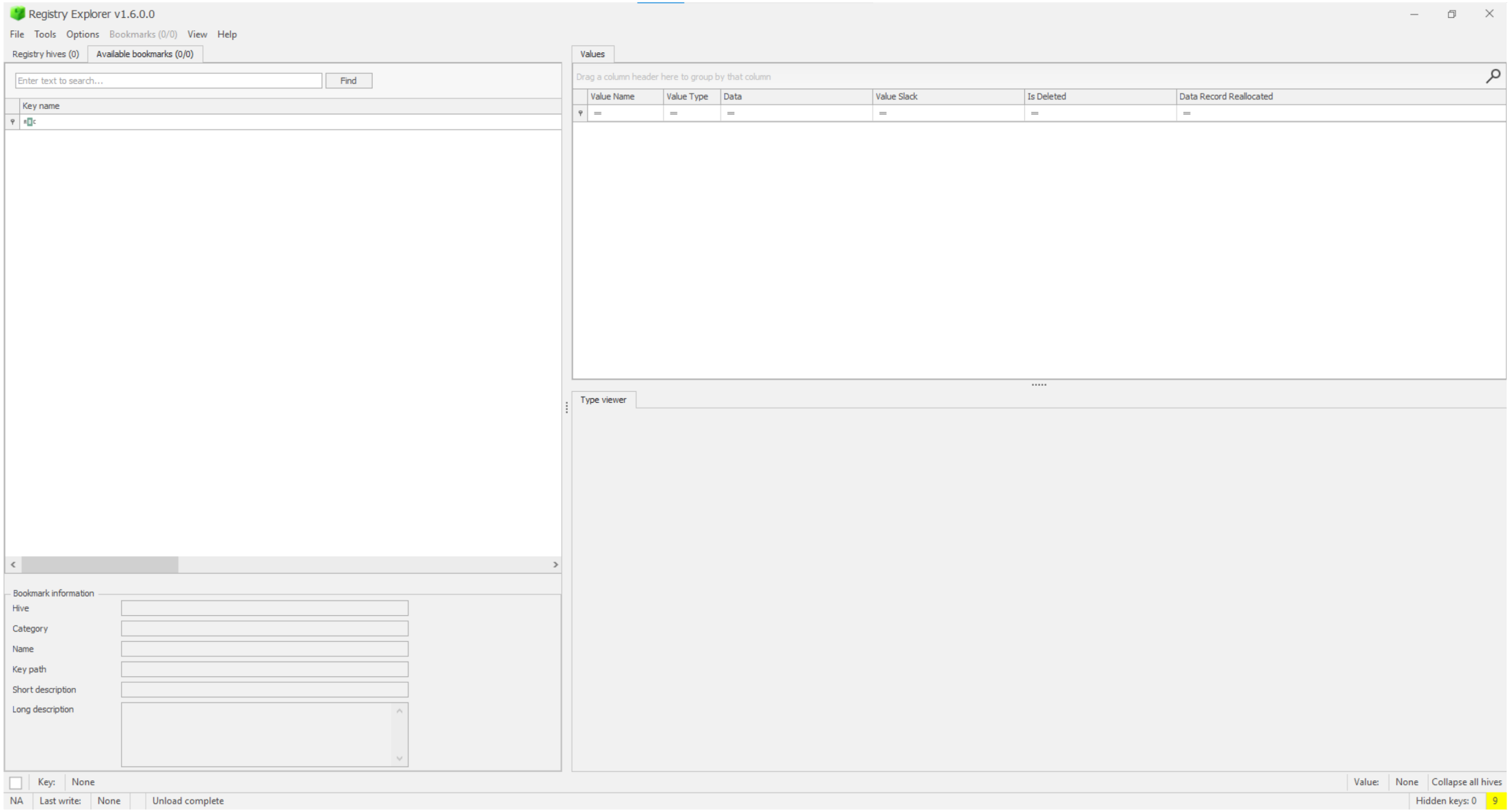
Registry Editor

- 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 RECmd 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