Windows Registry

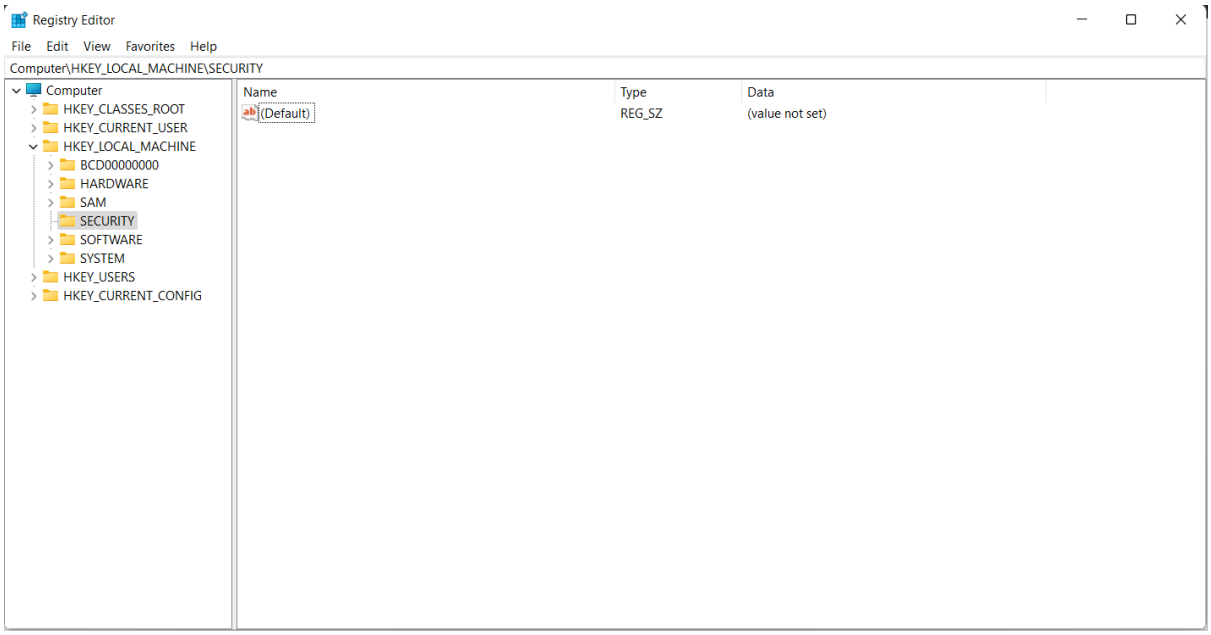
Windows Registry

- a collection of databases that contains the system's configuration data
- This configuration data can be about the hardware, the software, or the user's information.
- It also includes data about the recently used files, programs used, or devices connected to the system.
- The registry on any Windows system contains the following **five root keys**:

Folder/predefined key	Description
HKEY_CURRENT_USER	- Contains the **root of the configuration** information for the **user** who is **currently logged** on. - The user's folders, screen colors, and Control Panel settings are stored here. - This information is associated with the user's profile. - This key is sometimes abbreviated as **HKCU**.
HKEY_USERS	- Contains all the actively **loaded user profiles** on the computer. - HKEY_CURRENT_USER is a **subkey** of HKEY_USERS. - HKEY_USERS is sometimes abbreviated as **HKU**.
HKEY_LOCAL_MACHINE	- Contains configuration information **particular to the computer** (for any user). - This key is sometimes abbreviated as **HKLM**.
HKEY_CLASSES_ROOT	- Is a subkey of `HKEY_LOCAL_MACHINE\Software`. - The information that is stored here **makes sure that the correct program opens** when you open a file by using Windows Explorer. - This key is sometimes abbreviated as **HKCR**. - Starting with Windows 2000, this information is stored under both the **HKEY_LOCAL_MACHINE** and **HKEY_CURRENT_USER** keys. 1. The `HKEY_LOCAL_MACHINE\Software\Classes` key contains default settings that can apply to **all users** on the local computer. 2. The `HKEY_CURRENT_USER\Software\Classes` key has settings that override the default settings and apply **only to the interactive user**. - **`HKEY_CLASSES_ROOT` key provides a view of the registry that merges the information from these two sources.** - `HKEY_CLASSES_ROOT` also provides this merged view for programs that are designed for earlier versions of Windows. - To change

	the settings for the interactive user, changes must be made under `HKEY_CURRENT_USER\Software\Classes` instead of under `HKEY_CLASSES_ROOT`. - To change the default settings, changes must be made under `HKEY_LOCAL_MACHINE\Software\Classes` . - If you write keys to a key under `HKEY_CLASSES_ROOT`, the system stores the information under `HKEY_LOCAL_MACHINE\Software\Classes`. - If you write values to a key under `HKEY_CLASSES_ROOT`, and the key already exists under `HKEY_CURRENT_USER\Software\Classes`, the system will store the information there instead of under `HKEY_LOCAL_MACHINE\Software\Classes`.
HKEY_CURRENT_CONFIG	Contains information about the **hardware profile** that is used by the local computer at system startup.

Accessing registry hives offline (`regedit.exe`)



Accessing registry hives online

- if you only have access to a **disk image**, you must know where the registry hives are located on the disk.
- The majority of these hives are located in the `C:\Windows\System32\Config` directory and are:

1. **DEFAULT** (mounted on `HKEY_USERS\DEFAULT`)
2. **SAM** (mounted on `HKEY_LOCAL_MACHINE\SAM`)

3. **SECURITY** (mounted on `HKEY_LOCAL_MACHINE\Security`)
4. **SOFTWARE** (mounted on `HKEY_LOCAL_MACHINE\Software`)
5. **SYSTEM** (mounted on `HKEY_LOCAL_MACHINE\System`)

Hives containing user information:

- For Windows 7 and above, a user's profile directory is located in `C:\Users\<username>\` where the hives are:

1. **NTUSER.DAT** (mounted on `HKEY_CURRENT_USER` when a user logs in)
    - located in the directory `C:\Users\<username>\`
2. **USRCLASS.DAT** (mounted on `HKEY_CURRENT_USER\Software\CLASSES`)
    - located in the directory `C:\Users\<username>\AppData\Local\Microsoft\Windows`

- Remember that **NTUSER.DAT** and **USRCLASS.DAT** are **hidden files**.

The Amcache Hive:

- Windows creates this hive **to save information on programs that were recently run on the system.**
- This hive is located in `C:\Windows\AppCompat\Programs\Amcache.hve`.

Transaction Logs and Backups:

Transaction Logs (Yet to be done**)**

- The transaction logs can be considered as **the journal of the changelog of the registry hive**.
- Windows often uses transaction logs when writing data to registry hives.
- This means that the transaction logs can often have the latest changes in the registry that haven't made their way to the registry hives themselves.
- The transaction log for each hive is stored as a **.LOG** file in the same directory as the hive itself. It has the same name as the registry hive, but the extension is .LOG.
- For example, the transaction log for the SAM hive will be located in `C:\Windows\System32\Config` in the filename **SAM.LOG**.
- Sometimes there can be multiple transaction logs as well. In that case, they will have .LOG1, .LOG2 etc., as their extension.

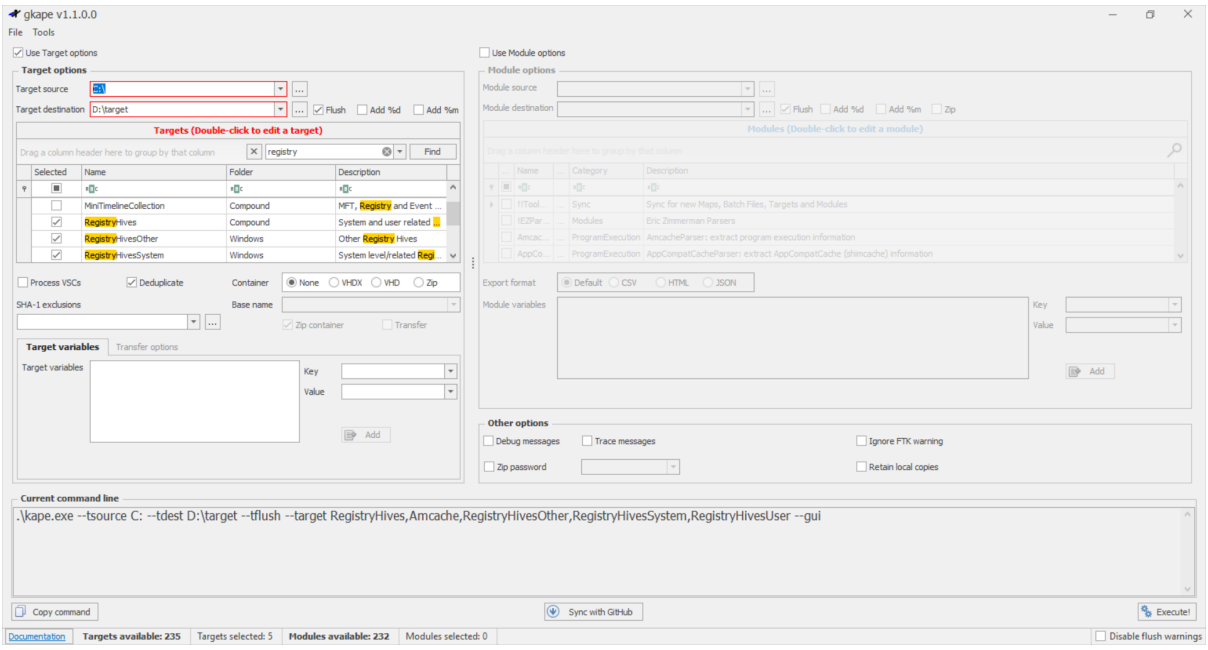
Backups

- Registry backups are the **opposite** of Transaction logs.
- These are the backups of the registry hives located in the `C:\Windows\System32\Config` directory.
- These hives are copied to the `C:\Windows\System32\Config\RegBack` directory **every ten days**.
- It might be an excellent place to look if you suspect that some registry keys might have been deleted/modified recently.

Data Acquisition Tools

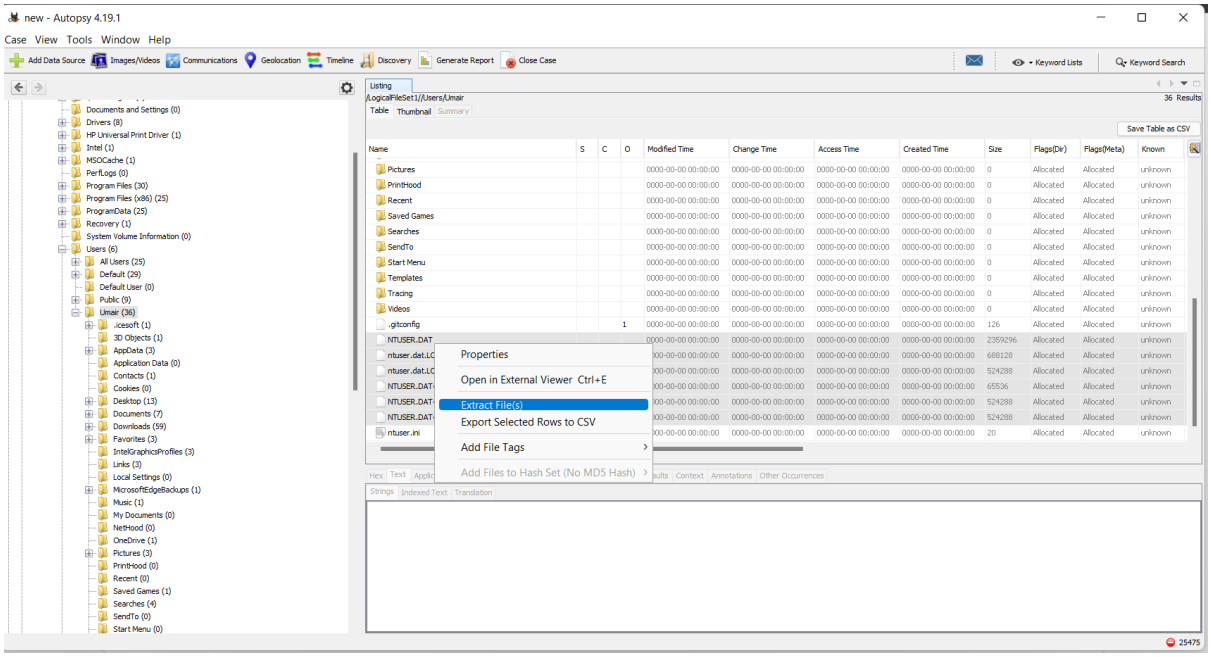
KAPE

KAPE is a live data acquisition and analysis tool which can be used to acquire registry data. It is primarily a command-line tool but also comes with a GUI.



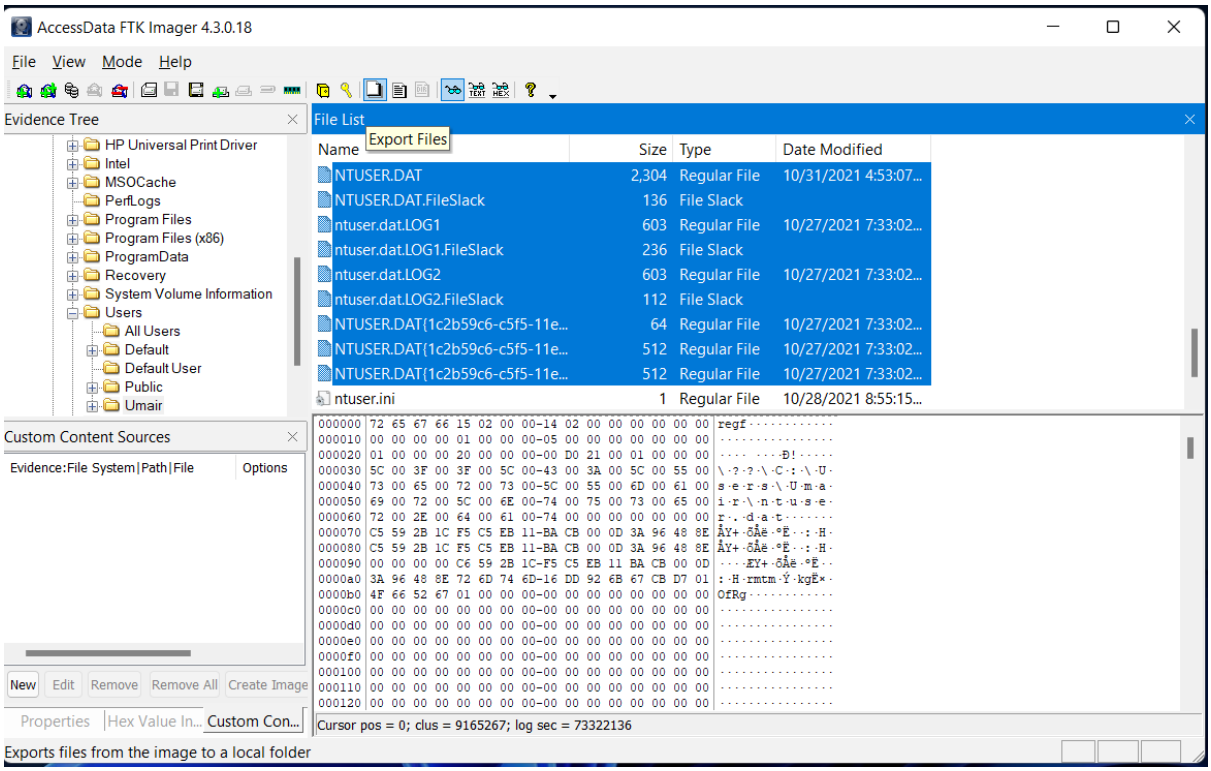
Autopsy

Autopsy gives you the option to acquire data from both live systems or from a disk image. After adding your data source, navigate to the location of the files you want to extract, then right-click and select the Extract File(s) option.



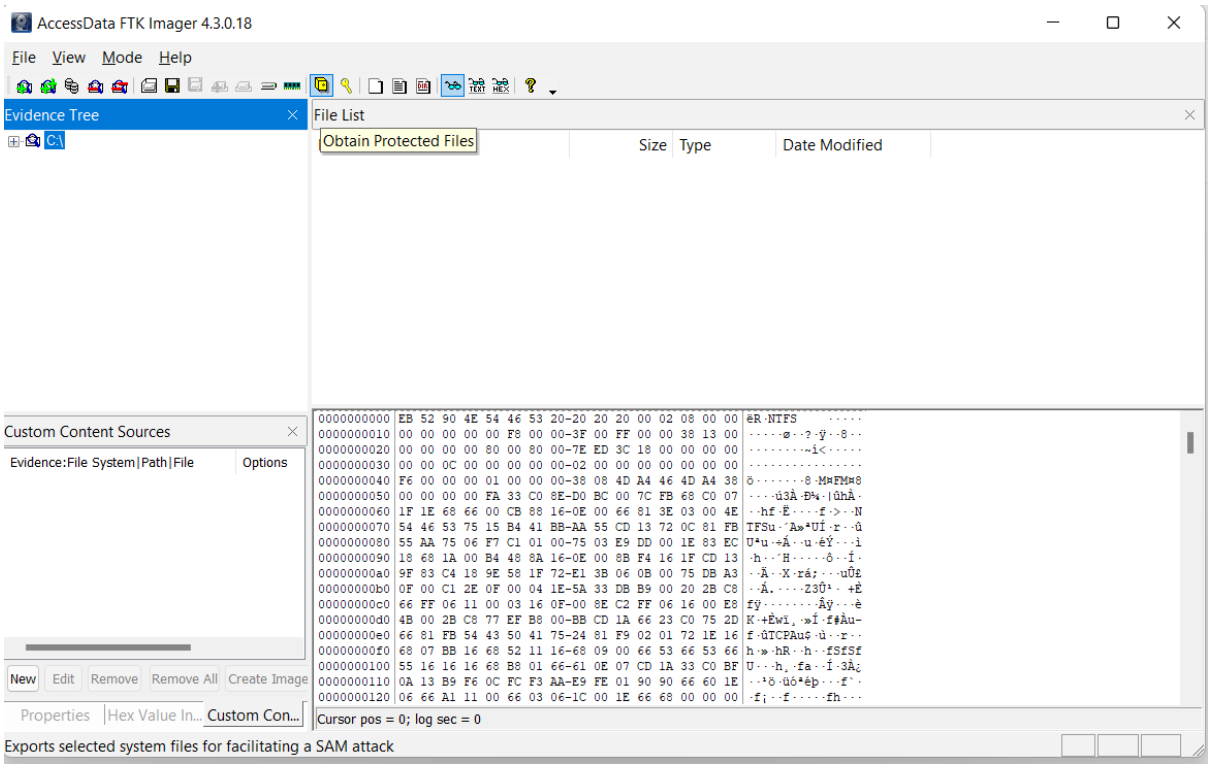
FTK Imager

FTK Imager is similar to Autopsy and allows you to extract files from a disk image or a live system by mounting the said disk image or drive in FTK Imager.



- Another way you can extract Registry files from FTK Imager is through the **Obtain Protected Files option.**

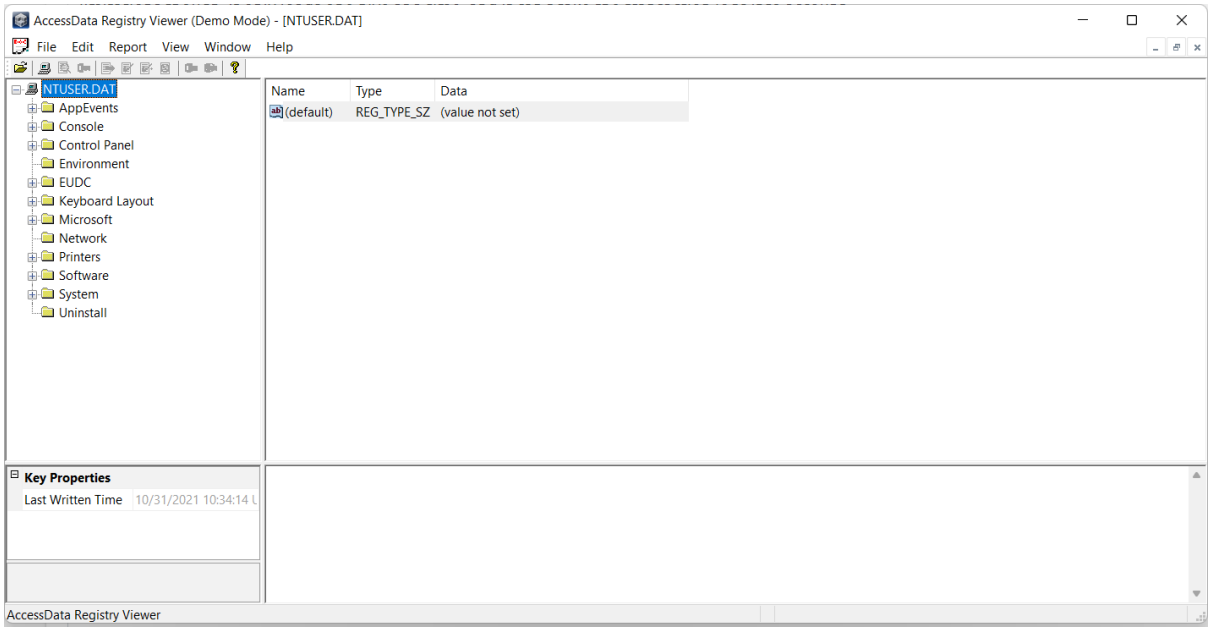
- This option is only available for live systems and is highlighted in the screenshot below. This option allows you to extract all the registry hives to a location of your choosing. However, it will not copy the `Amcache.hve` file



Tools to read/Parse registry

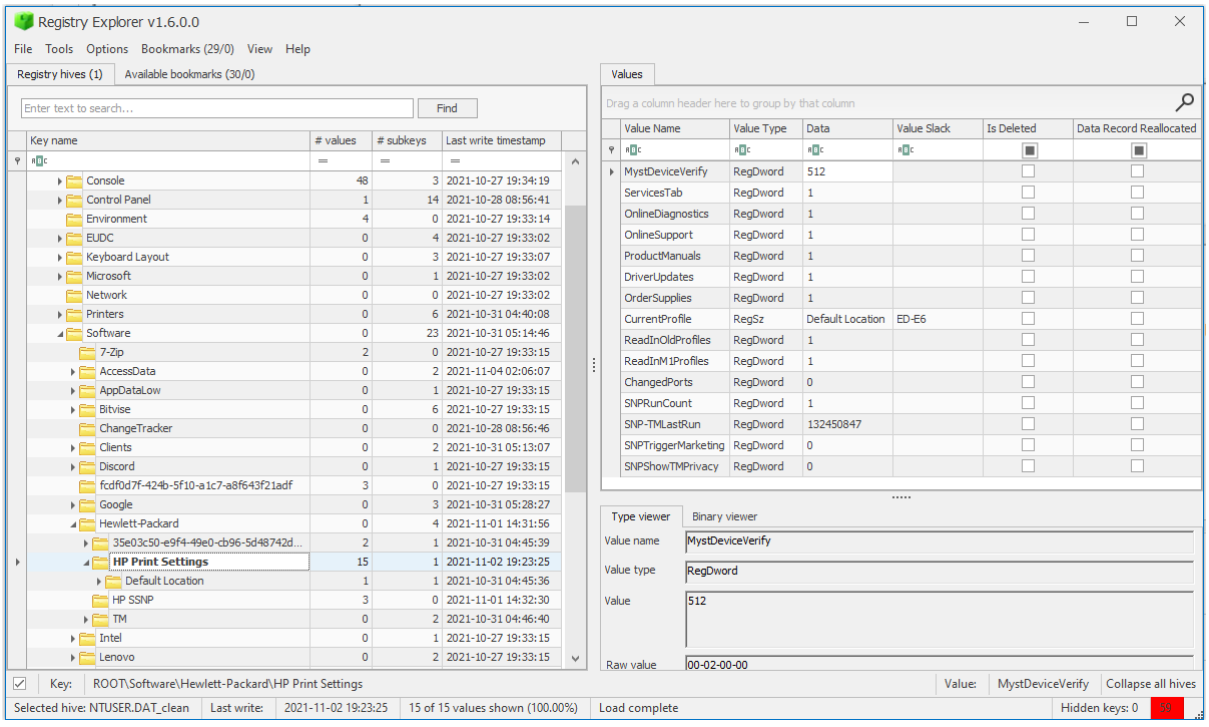
Registry Viewer

- It only loads one hive at a time, and it can't take the transaction logs into account.



Zimmerman's Registry Explorer

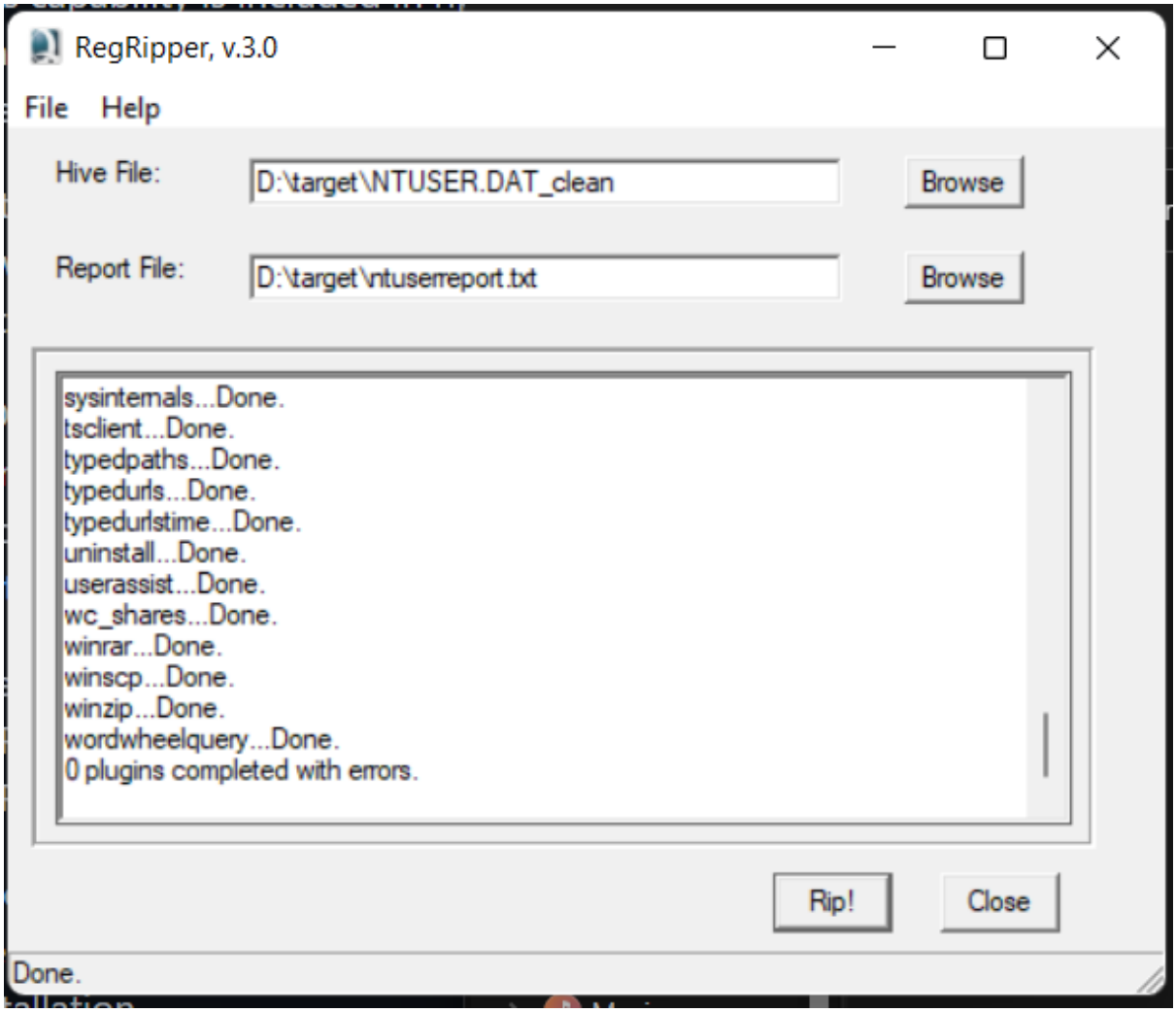
- It **can load multiple hives simultaneously** and **add data from transaction logs into the hive** to make a more 'cleaner' hive with more up-to-date data.



RegRipper

- takes a registry hive as input and outputs a report that extracts data from some of the forensically important keys and values in that hive. The output report is in a text file and shows all the results in sequential order.

- One shortcoming of RegRipper is that it does not take the transaction logs into account.

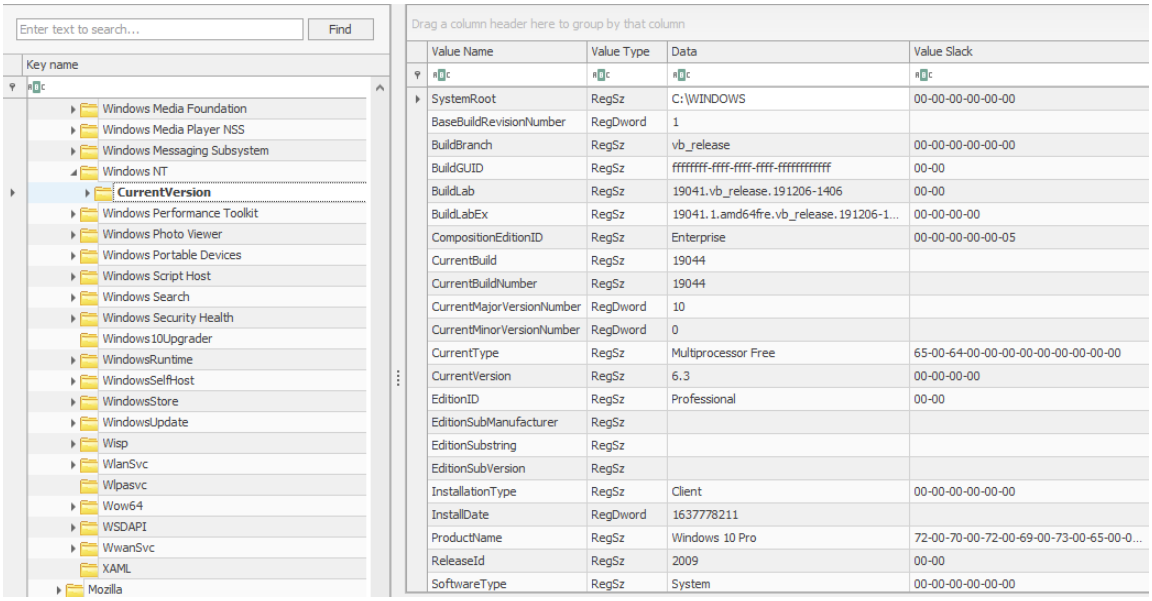


Investigating

System Information and System Accounts

OS Version

- SOFTWARE\Microsoft\Windows NT\CurrentVersion



Autostart Programs (Autoruns)

The following registry keys include information about programs or commands that run when a user logs on.

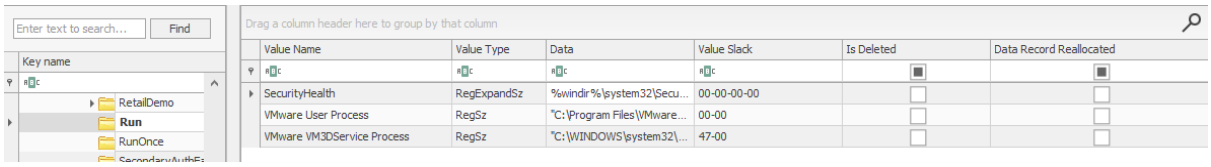
`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run`

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce`

`SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`

`SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run`

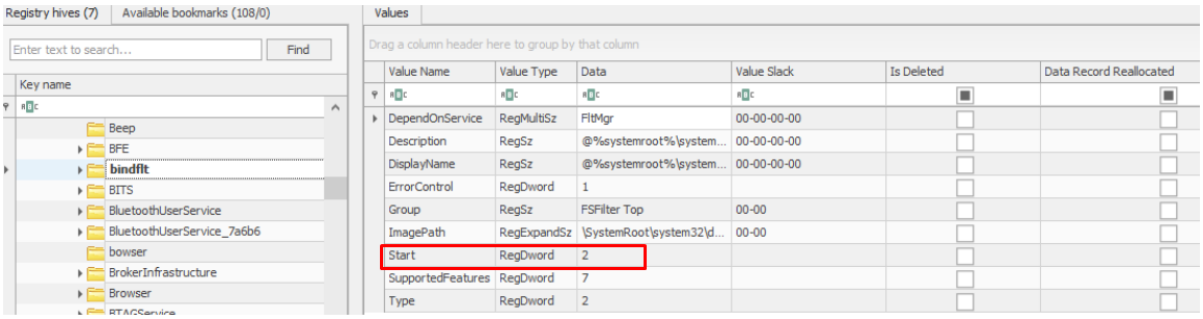
`SOFTWARE\Microsoft\Windows\CurrentVersion\Run`



Services info

`SYSTEM\CurrentControlSet\Services`

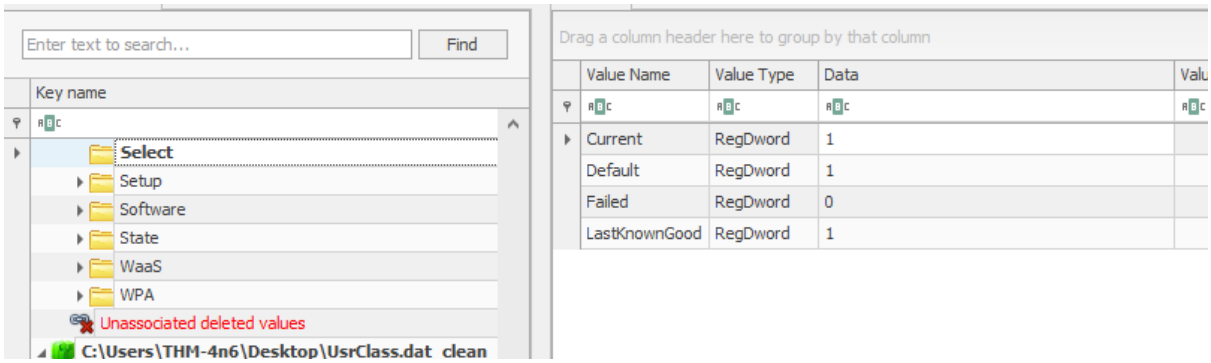
- Notice the Value of the Start key in the screenshot below.



In this registry key, if the `start` key is set to 0x02, this means that this service will start at **boot**.

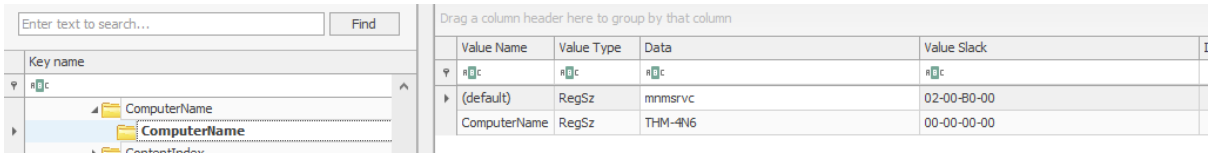
Current control set

- The hives containing the machine's configuration data used for **controlling system startup.**
- Commonly, we will see two Control Sets, **ControlSet001** and **ControlSet002**, in the SYSTEM hive on a machine.
  - In most cases, **ControlSet001** will point to the Control Set that the machine **booted with**
    - `SYSTEM\ControlSet001`
  - ControlSet002 will be the `last known good` configuration.
    - `SYSTEM\ControlSet002`
- Windows creates a volatile Control Set when the machine is **live**, called the CurrentControlSet (`HKLM\SYSTEM\CurrentControlSet`). For getting the most accurate system information, this is the hive that we will refer to.
- We can find out which Control Set is being used as the CurrentControlSet by looking at the following registry value: `SYSTEM\Select\Current`
- Similarly, the `last known good` configuration can be found using the following registry value: `SYSTEM\Select\LastKnownGood`



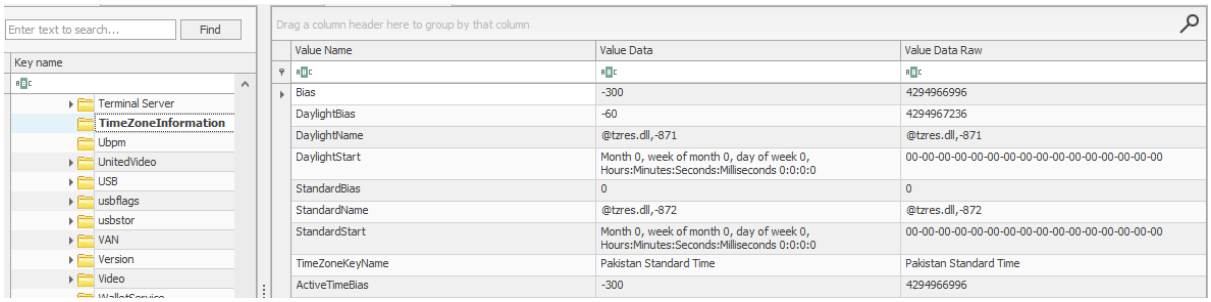
Computer Name

`SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName`



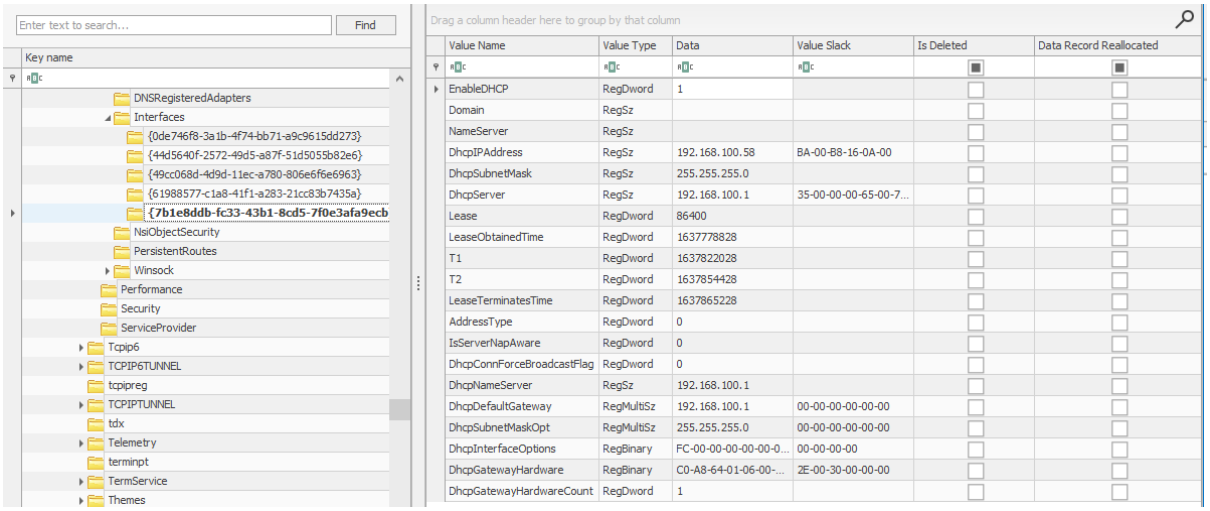
Time Zone Information

`SYSTEM\CurrentControlSet\Control\TimeZoneInformation`



Network Interfaces and Past Networks

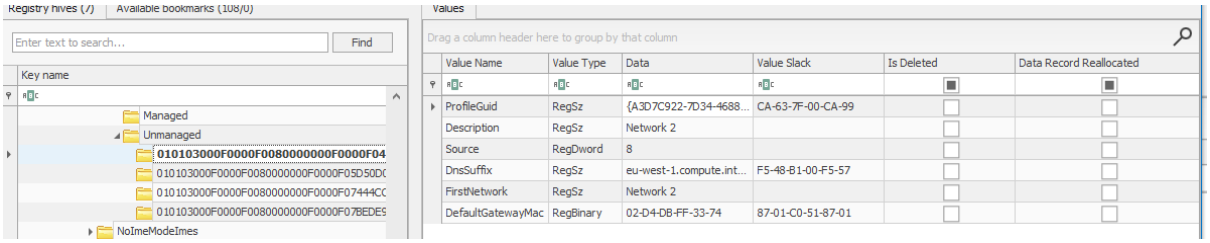
`SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces`



The past networks a given machine was connected to can be found in the following locations

`SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged`

`SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed`

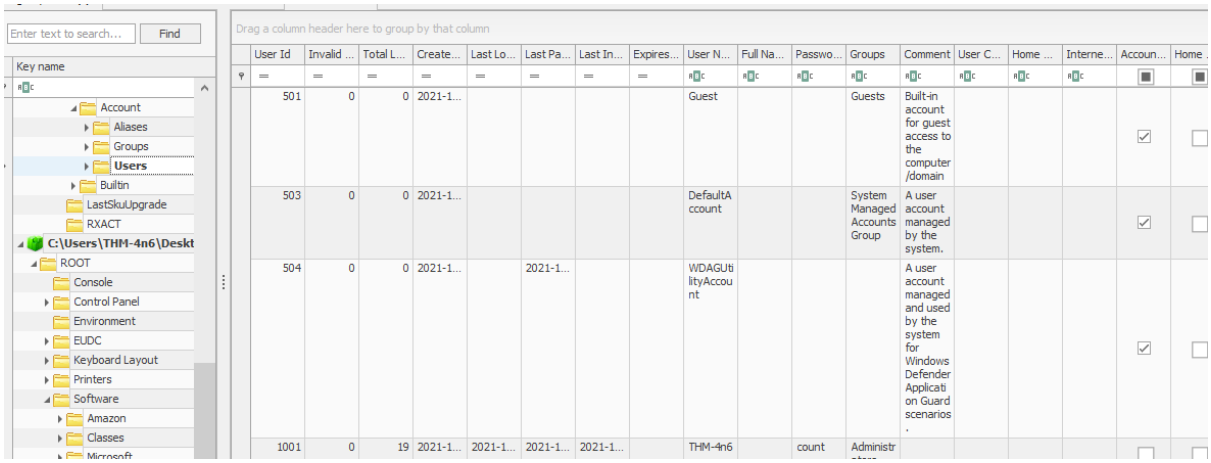


- These registry keys contain past networks as well as the last time they were connected.

SAM hive and user information

- The SAM hive contains user account information, login information, and group information.

`SAM\Domains\Account\Users`



- The information contained here includes the relative identifier (RID) of the user, number of times the user logged in, last login time, last failed login, last password change, password expiry, password policy and password hint, and any groups that the user is a part of.

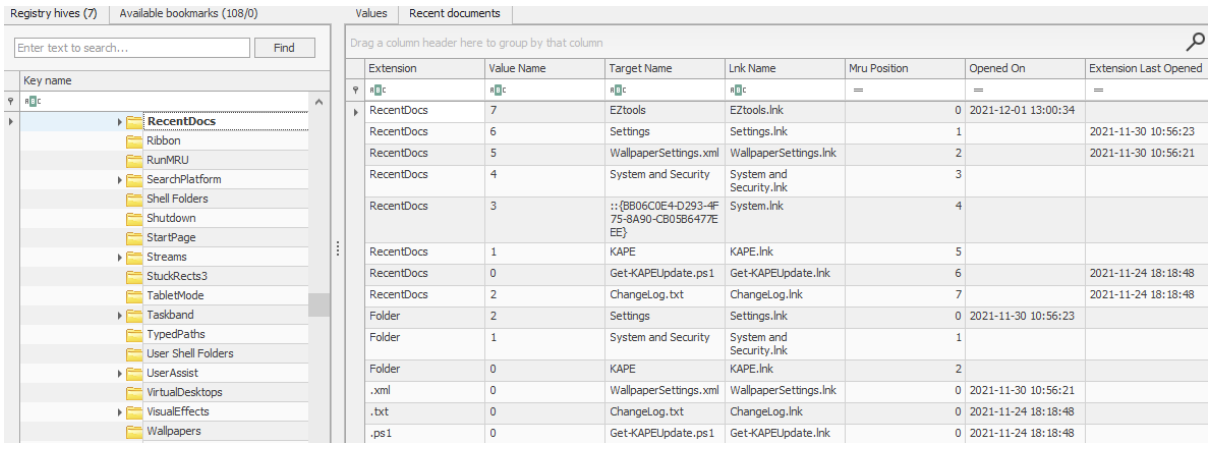
Usage or knowledge of files/folders

Recent Files

- **a list of recently opened files for each user**

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`

- located in the directory `C:\Users\<username>\`



- if we are looking specifically for the last used **PDF(or any extention)** files, we can look at the following registry key:

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ .pdf`

- located in the directory `C:\Users\<username>\AppData\Local\Microsoft\Windows`

Office Recent Files

- Microsoft Office also maintains a list of recently opened documents.

`NTUSER.DAT\Software\Microsoft\Office\<VERSION_Number>`

- An example registry key will look like this:

`NTUSER.DAT\Software\Microsoft\Office\15.0\Word`

- Starting from **Office 365**, Microsoft now ties the location to the user's live ID. In such a scenario, the recent files can be found at the following location.

`NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU`

ShellBags

- When any user opens a folder, it opens in a specific layout.
- Users can change this layout according to their preferences.
- These layouts can be different for different folders.
- **This information about the Windows *'shell'* is stored and can identify the Most Recently Used files and folders.**
- Since this setting is different for each user, it is located in the user hives. We can find this information on the following locations:

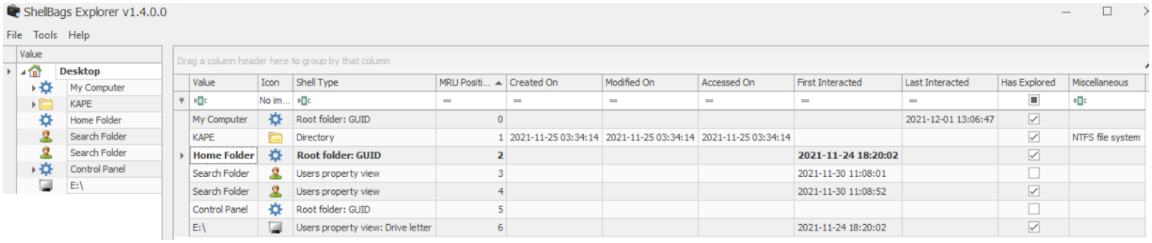
`USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags`

`USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU`

`NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU`

`NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags`

- Registry Explorer doesn't give us much information about ShellBags.
- However, another tool from Eric Zimmerman's tools called the **ShellBag Explorer** shows us the information in an easy-to-use format. We just have to point to the hive file we have extracted, and it parses the data and shows us the results

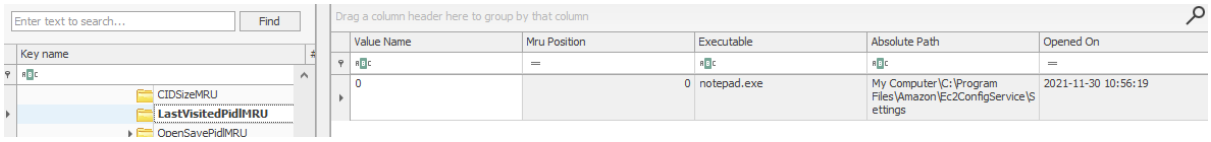


Open/Save and LastVisited Dialog MRUs:

- When **we open or save a file**, a dialog box appears asking us where to save or open that file from.
- It might be noticed that once we open/save a file at a specific location, Windows remembers that location.
- This implies that we can find out recently used files if we get our hands on this information. We can do so by examining the following registry keys

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU`

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU`

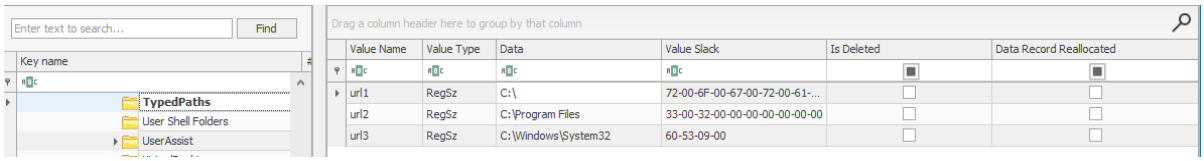


Windows Explorer Address/Search Bars:

- the paths typed in the Windows Explorer address bar or searches performed

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths`

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery`

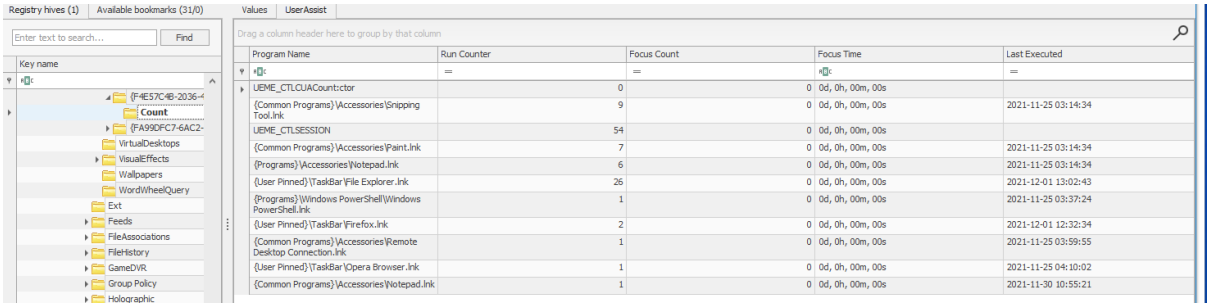


Evidence of Execution

UserAssist

- These keys contain information about the **programs launched**, the **time of their launch**, and the **number of times they were executed**.
- However, **programs that were run using the command line can't be found** in the User Assist keys.
- The User Assist key is present in the NTUSER hive, mapped to each user's **GUID**.

`NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count`

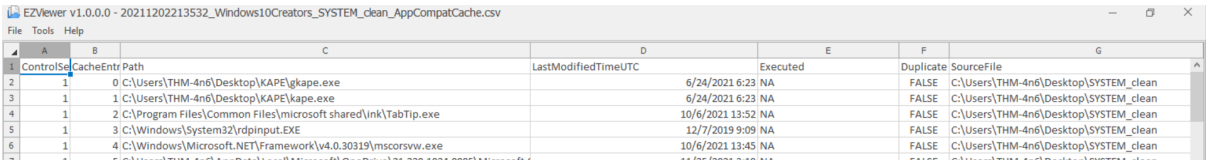


ShimCache

- ShimCache is a mechanism used **to keep track of application compatibility with the OS** and **tracks all applications launched on the machine.**
- Its main purpose in Windows is to ensure **backward compatibility** of applications.
- It is also called **Application Compatibility Cache** (**AppCompatCache**).
- It is located in the following location in the SYSTEM hive:

```
SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache
```

- ShimCache stores **file name**, **file size**, and **last modified time of the executables**.
- Our goto tool, the Registry Explorer, doesn't parse ShimCache data in a human-readable format, so we go to another tool called **AppCompatCache Parser, also a part of Eric Zimmerman's tools.** It takes the **SYSTEM** hive as input, parses the data, and outputs a CSV file that looks like this:



- We can use the following command to run the AppCompatCache Parser Utility:

```
AppCompatCacheParser.exe --csv <path to save output> -f <path to SYSTEM hive for data parsing> -c <control set to parse>
```

AmCache

- This performs a **similar function to ShimCache**, and **stores additional data related to program executions.**

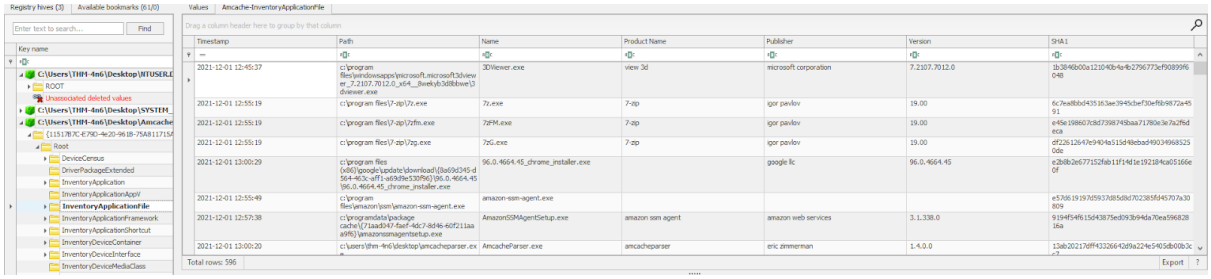
- This data includes **execution path**, **installation**, **execution** and **deletion times**, and **SHA1** hashes of the executed programs.
- This hive is located in the file system at:

```
C:\Windows\appcompat\Programs\Amcache.hve
```

- Information about the last executed programs can be found at the following location in the hive:

```
Amcache.hve\Root\File\{Volume GUID}\
```

This is how Registry Explorer parses the AmCache hive:



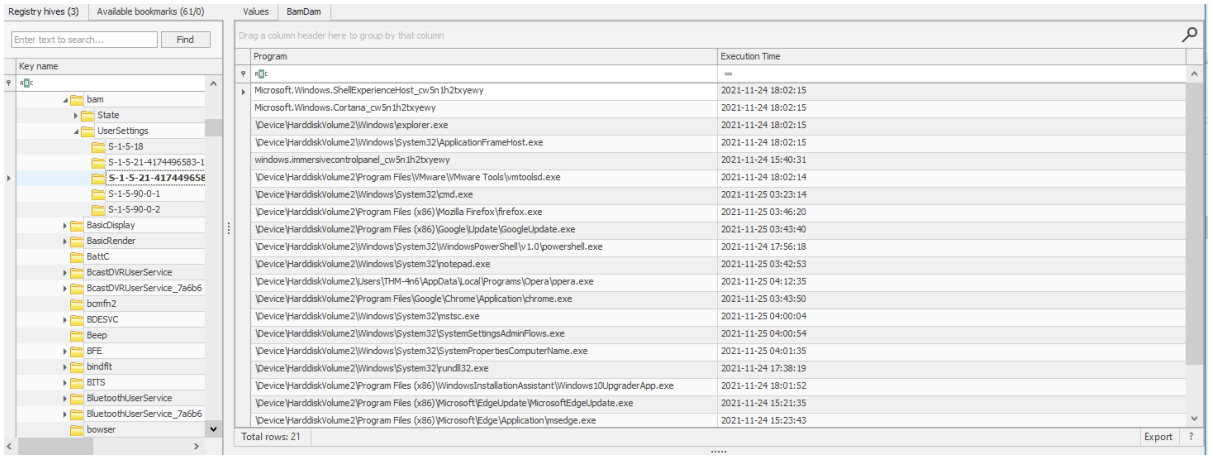
BAM/DAM

- **Background Activity Monitor** or **BAM** keeps a tab on the activity of background applications.
- **Desktop Activity Moderator** or **DAM** is a part of Microsoft Windows that optimizes the **power consumption of the device**.
- Both of these are a part of the Modern Standby system in Microsoft Windows.
- In the Windows registry, the following locations contain information related to BAM and DAM.
- This location contains information about **last run programs**, **their full paths**, and **last execution time.**

```
SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
```

```
SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}
```

Below you can see how **Registry Explorer** parses data from BAM:



External Devices/USB device forensics

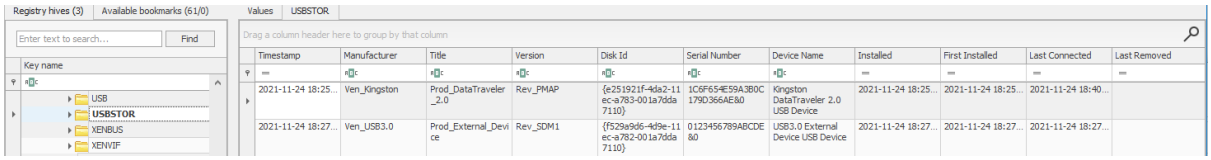
Device identification:

- The following locations keep track of **USB keys** plugged into a system.
- These locations store the vendor id, product id, and version of the USB device plugged in, the time the devices were plugged into the system and can be used to identify unique devices.

`SYSTEM\CurrentControlSet\Enum\USBSTOR`

`SYSTEM\CurrentControlSet\Enum\USB`

Registry Explorer shows this information in a nice and easy-to-understand way.



First/Last Times:

Similarly, the following registry key tracks the first time the device was connected, the last time it was connected and the last time the device was removed from the system.

`SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####`

In this key, the #### sign can be replaced by the following digits to get the required information:

Value	Information

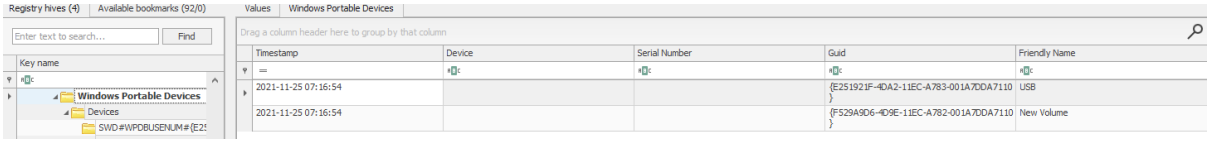
0064	First Connection time
0066	Last Connection time
0067	Last removal time

Although we can check this value manually, as we have seen above, Registry Explorer already parses this data and shows us if we select the USBSTOR key.

USB device Volume Name:

The device name of the connected drive can be found at the following location:

`SOFTWARE\Microsoft\Windows Portable Devices\Devices`



We can compare the GUID we see here in this registry key and compare it with the Disk ID we see on keys mentioned in device identification to correlate the names with unique devices. Take a look at these two screenshots and answer Question # 3.

Combining all of this information, we can create a fair picture of any USB devices that were connected to the machine we're investigating.

- **reg query HKLM /s /f "C:\TMP\mim.exe sekurlsa::LogonPasswords > C:\TMP\o.txt”**
    - to search for a specific value in the registry