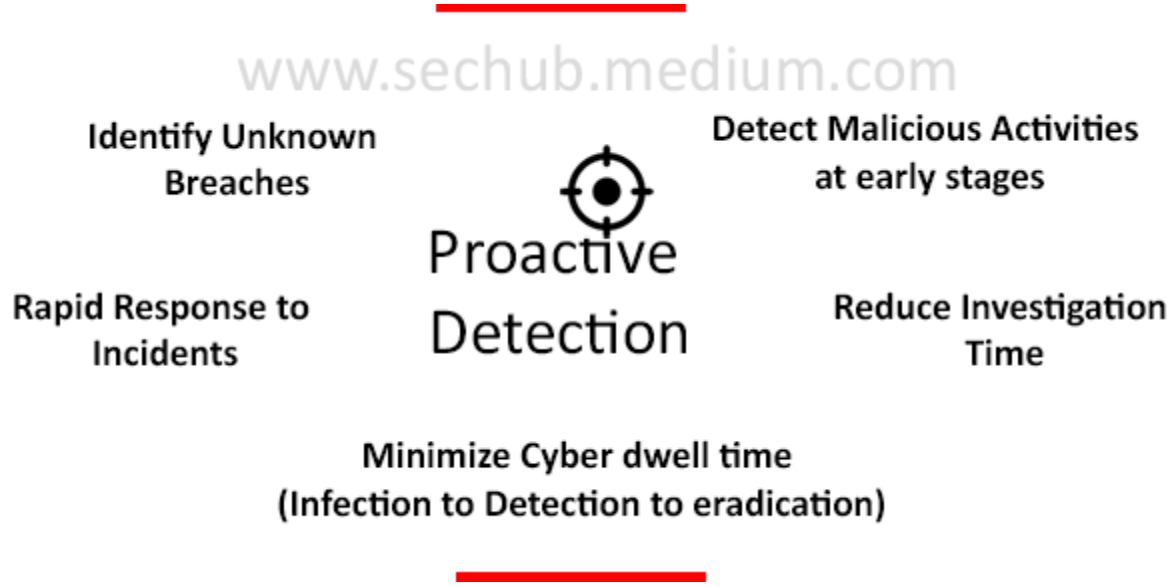
System Live Analysis [Part 1]

If you have not hit by cyberattacks yet, It does not mean it will never happen to you! It's just a matter of time!

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; — *Sun Tzu*

As well quoted by Sun Tzu, it's all about our readiness, what would you do? Just deploy a tool and wait for alerts? No way! It's not a task of a tool only, Yes even an AI one, but an expert with the help of tools and rules [tactic | technique].

We should proactively and iteratively look for evidence of suspicious or malicious activities in a digital environment. It significantly helps to reduce risks as a proactive approach has many advantages as follows:



Proactive Incident Detection Benefits

1- Shall we keep up the tradition?!

Ideally [and traditionally!], when it comes to incident response and digital forensics, we think of having forensics data acquisition, etc. It is a common practice for in-depth analysis. But… it's a non-interactive approach with no chance to investigate the entire running system.

Some sophisticated attacks may not leave any trace on harddisk! or it would be a challenge to catch them on forensics images [e.g. Encrypted or file-less attacks].

Besides, we may deal with servers with a massive volume of harddisk in which making forensics images requires a long time and a few packs of popcorn! Sometimes it may not be even practical [e.g. NAS, SANs, large RAID arrays].

On the other hand, the live system analysis provides a better understanding of ongoing events. However, the considerable risk of unintentional changes in system or environment is there, especially during a manual analysis; moreover, the investigation process may not be repeatable as the system state keep changing!

what to do…? it's not about choosing either one of the techniques we need both!

2- Live Analysis: An offer we can't refuse

System live analysis is a good practice to conduct a **light investigation** and to have **first look** at potential incident to determine if any serious issue is there which needs detailed traditional forensics analysis.

Just keep in mind that we should be well trained to conduct the live analysis as unlike working on forensics images we may have only one chance to do it right. Therefore:

- Maintain forensic integrity and Minimize system changes.
- Avoid installing any tools on the target system.
- Avoid copying anything on the target system.
- Validate the publisher of third-party tools.
- Use light tools which require minimum user interaction.
- When its possible record the results for further analysis.

Please Note this write-up series aims to discuss manual system analysis without using automated tools such as EDR.

3- Alice in wonderland!

One of the main factors in a successful investigation is to know what to look for! Otherwise, we get confused as much as Alice was in the wonderland.

Digital Forensics Wonderland: A considerable amount of forensics images [hardsik, RAM, memory cards…], Logs, data, records, etc. that make investigators' life miserable if they don't have a proper strategy [sop, cheatsheet, playbooks, and indeed enough expreince] to formulate initial hypothesises.

How to become a master in blue teaming, simple steps that need commitment and effort. Read and practice, keep ourselves updated with the latest techniques, communicate with experts and join professional communities, read and practice [Yes its is essential that's why I mentioned it twice :)]

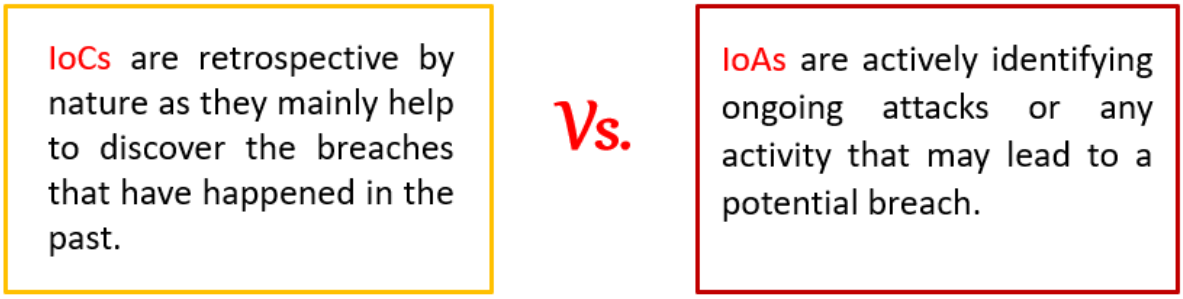
We should actively sharpen our skills by understanding the different Techniques, Tactics, and Procedures (TTP) used by cybercriminals, and learn how to look for their traces.

Let's start with two essential concepts that help us to investigate a potential case, Indicators of Compromise and Indicators of Attack.

4- IoC and IoA: Game of Indicators!

Indicators of compromise (IoC) is a forensics artifact left by intruders in systems or network logs that proves some form of malicious/suspicious activity or infection has occurred.

In contrast, Indicators of attack (IoA) is any sign of the beginning of a malicious or suspicious activity that helps us to detect them at early stages or even before they become a successful attack.



IoC vs IoA

IoCs and IoAs can be applied to most of the stages of an attack life cycle, so we should use both!... Ha, wait you said this post is about the proactive hunt! Is looking for IoC-based detection considered active detection!

Let's think a little bit out of the box, IoC-based detection may not look proactive as IoA-based. But when it comes to the full lifecycle of cyberattacks, finding IoCs related to the successful early stages [e.g. initial access and excution] may help to look for the indicators of next potential steps such as privilege escalation, lateral movement, secondary infection, etc. And yes that is considered a proactive hunt to me.

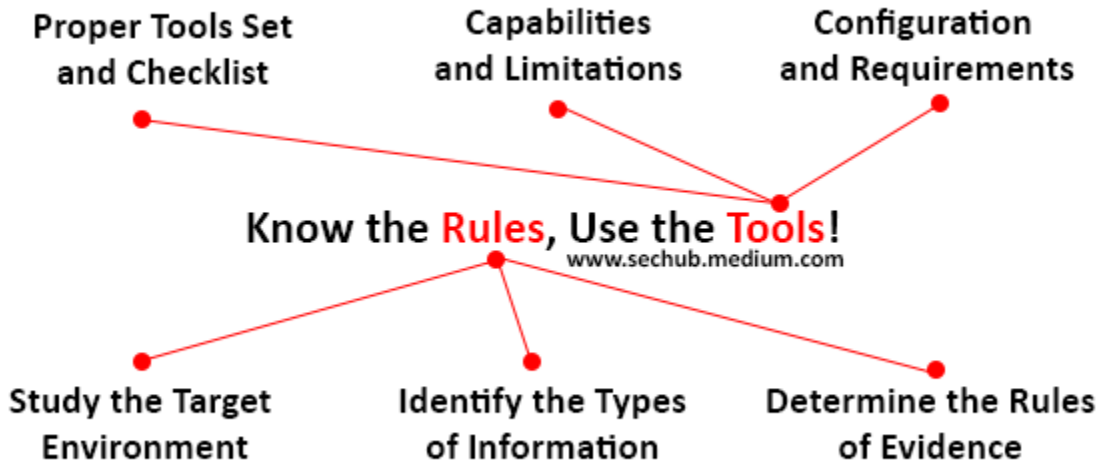
System Live Analysis [Part 2]- Windows: Rules and Tools

Part two will cover some rules and tools that can be employed to conduct live forensics analysis on the Windows platform. So which one comes first rules or tools?

1- Know the rules before using tools

I keep telling myself this every time before starting any investigation, be prepared! Well prepared. It does not matter how good is your tools and how effective is your techniques.

Digital environments are fragile and keep changing every second.



Blue Team: Rules and Tools

Before every investigation, the status of the target systems must be studied in detail to identify the potential challenges to tailor and fine-tune our tools, techniques, and procedures.

2. Rules are Rules

Rules are rules, and they are made to be broken! I like the quote but it's not applicable for blue teamers :). NOT AT ALL!

- Try to do not to install or copy anything on the systems under investigation.
- Copy all things that you need on a forensically clean external storage and connect it to the victim system using write blockers.
- Prepare chain of custody and document everything!
- Record the results for further investigations [in external storage!]
- Generate hash value forever collected data and record them.
- Document All the steps!

Things may happen unintentionally! Do not worry; any mistake should be documented and reported to the higher management and authorities in charge.

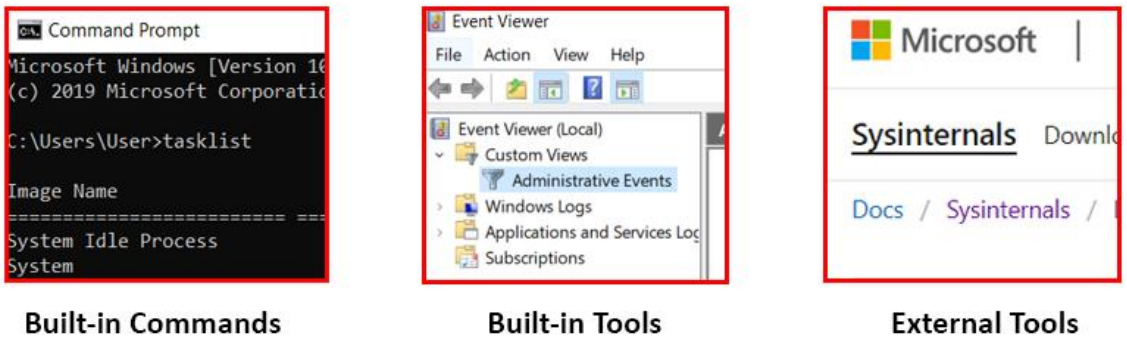
3. The right Tools for the Right Job

There are many tools out there to help us carry out our investigation. In this post, I cover a few for windows live analysis.

Validate the publisher of third-party tools.

Use light tools which require minimum user interaction.

In general, we have three categories, as follows:



Built-in Commands **Built-in Tools** **External Tools**

Windows Live Analysis Commands and Tools

- Windows Built-in commands [CMD commands, WMIC, and Powershell] are always my first choice! Why? Because they are from the vendor itself and light!
- There are plenty of useful built-in tools in windows that can be used to look for potential security issues. Event viewer is one of them.
- External tools may be developed by the vendors or their trusted parties that's cool. For any third-party tool, they need to be evaluated and well tested before using them.

4. What to collect!

This is an essential question every examiner has in mind! What to collect and what to look for?

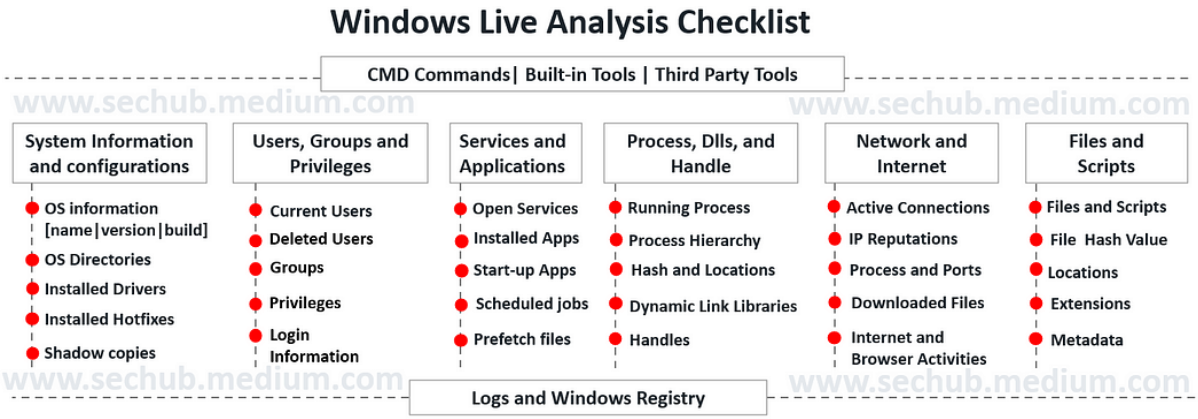
The proactive system analysis is a little bit challenging as we are looking for any potential malicious activities rather than following a specific indicators.

We should collect and examine different evidences to look at first and make the decision on further investigation accordingly. In general, I have my checklist on the six following categories:

- System Information and configurations
- Users, Groups and Privileges
- Services and Applications
- Process, Dlls, and Handle
- Network and Internet
- Files and Scripts

System Live Analysis [Part 3]- Windows: Technical Checklist

In part three, I will focus on the type of data to be collected in addition to the tools, commands, and technical requirements. Let's review the six categories again:



Windows Live Analysis Checklist

Note 1: *The above checklist is for high-level live analysis. We may need more details for in-depth forensics investigation and root cause analysis.*

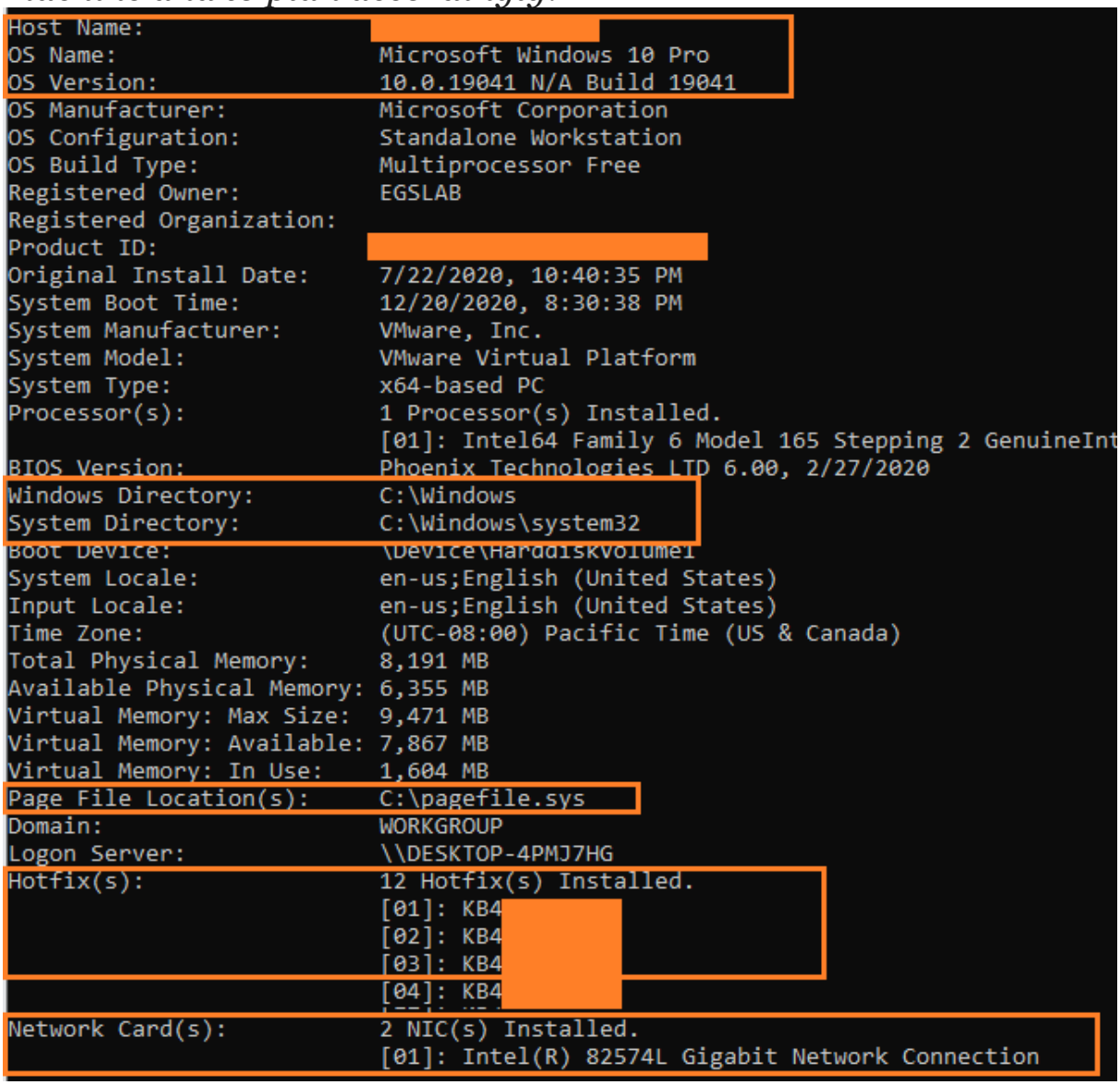
Note 2: *Windows logs and registry are valuable sources of data for investigators, but in this series, we just use them at a very high level to justify findings.*

1. System Information and Configurations

One of the first actions we should do as an investigator is to study the current state of the windows machine. It gives us an overall idea of how to plan the rest of the analysis.

Data Types: Current System settings and configurations [e.g. OS installation date, essential folders, hotfixes, drives, Environment Variable, shadow copies, top-level network information, etc.]

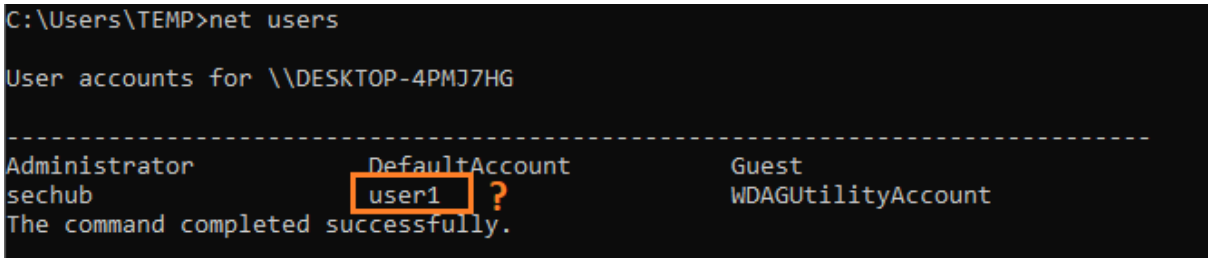
Investigation Value: To understand the current state of the machine and to plan accordingly.



System Information Sample

2. Users, Groups and Privileges

Abusing valid users' credentials, manipulating existing accounts, or creating new accounts upon initial access are common techniques used by attackers. These techniques are not only for gaining initial access and can be used for persistence, privilege escalation, or even defence evasion.



User Accounts

Data Types: User account information, login timestamps, account activities, account groups, and privileges.

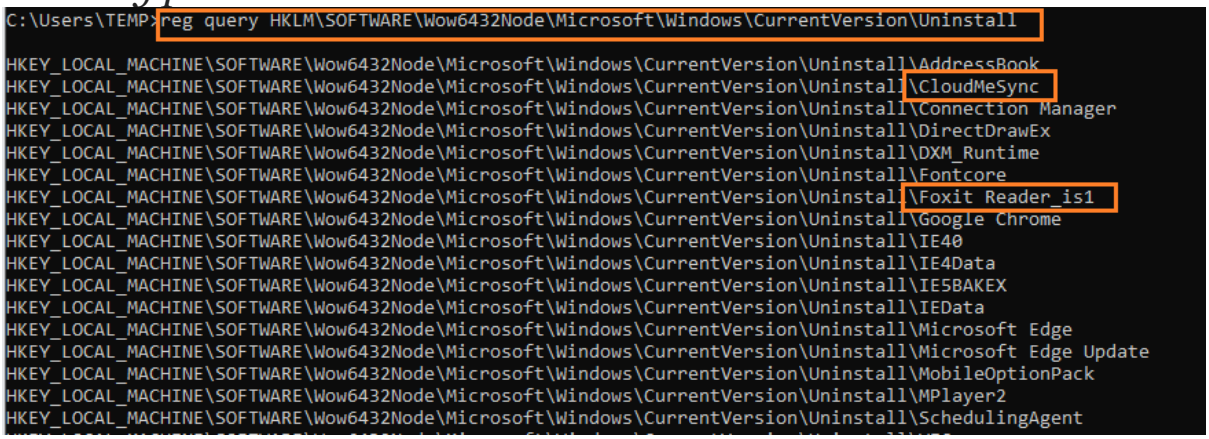
Investigation Value: To look for any questionable activities related to user accounts such as suspicious and unexpected login hours, locations, and privileges.

3. Services and Applications

Cybercriminals target different layers of any organization from technology, to people and processes. Vulnerable services and applications can open the door for them, so as an investigator, we should proactively examine any available services and installed application to look for any security issues.

Data Types: List of enabled services and installed applications along with their versions and configurations.

Investigation Value: To look for any possible vulnerability, weakness, and misconfiguration that may be used by attackers as an entry point.



Retrieving Installed Application using Reg Query

4. Process, Dlls, and Handle

Identifying mysterious running processes is very curial for every investigation as it may help to detect ongoing attacks. It’s not all about running malware or suspicious processes, it could be a standard windows process that is misusing by an attacker.

```
C:\Users\TEMP\Desktop>pslist64.exe

PsList v1.4 - Process information lister
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for [redacted]

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   2    0     60   0:30:36.171     0:16:40.349
System                4   8 115 2774    196   0:00:08.640     0:16:40.349
Registry             92   8   4    0   4692   0:00:00.296     0:16:45.198
smss                320  11   2   53   1032   0:00:00.046     0:16:40.342
csrss               432  13  10  560   1636   0:00:00.203     0:16:39.661
wininit             508  13   1  165   1356   0:00:00.109     0:16:39.545
csrss               516  13  12  425   1756   0:00:00.578     0:16:39.542
winlogon            612  13   5  275   2552   0:00:00.140     0:16:39.491
services            660   9   7  701   4960   0:00:01.015     0:16:39.405
lsass               668   9  11 1272   7124   0:00:01.203     0:16:39.375
svchost             780   8  22 1173  10552   0:00:02.140     0:16:39.178
fontdrvhost         796   8   5   39   1284   0:00:00.000     0:16:39.173
```

Retrieving Installed Application using pslist

Data Types: All running process [name, location, hash, parent ID], all the loaded DLLs, and open handles [Files, Folders, Registry Keys].

Investigation Value: To look for any malicious [Known Bad] or suspicious [Potential Unknown Bad] processes, and attacks such as DLL injection!

5. Network and Internet

Many factors tag this network information as one the most crucial point of investigation such as remote access attacks, Botnets and C&C, remote trojans, and any type of network-based attacks.

```
C:\Users\TEMP\Desktop>netstat -ano |find /i "ESTABLISHED"
  TCP    192.168.177.151:49752  [redacted]:443      ESTABLISHED     3244
  TCP    192.168.177.151:49838  [redacted]:443      ESTABLISHED     1728
  TCP    192.168.177.151:49839  [redacted]:443      ESTABLISHED     1728
  TCP    192.168.177.151:49840  [redacted]:443      ESTABLISHED     1728
```

List of Established TCP Connections

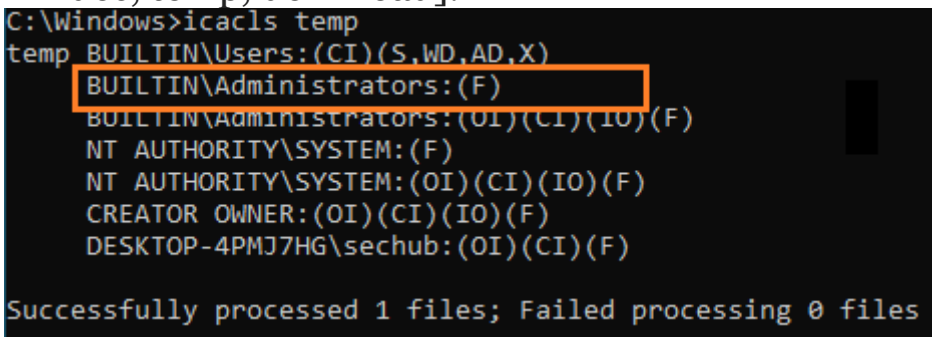
Besides, a careless end-user with Internet access has become a preferred attack vector for cybercriminals to walk into our digital environment. Thus, all web browsing and Internet surfing activities must be investigated carefully as well.

Data Types: Active connections, the process to port mapping, enabled protocols, visited URLs, installed extensions, downloaded files, and browsing history.

Investigation Value: To look for any suspicious remote accesses, visited URLs and IPs, malicious network connections, etc.

6. Files and Folders

Finally files and writable folders [common ones in particular suchas windos, temp, download].



Access Aontrol List for Temp Directory

Data Types: Executable files, Scripts, password protected or hidden files, compressed files, all downloaded files, etc.

Investigation Value: To look for any suspicious file or scripts.

system Live Analysis [Part 4]- Windows: System Information and Configurations

Data Types: Current System settings and configurations [e.g. OS installation date, essential folders, hotfixes, drives, shadow copies, top-level network information, etc.]

Investigation Value: To understand the current state of the machine and to plan accordingly.

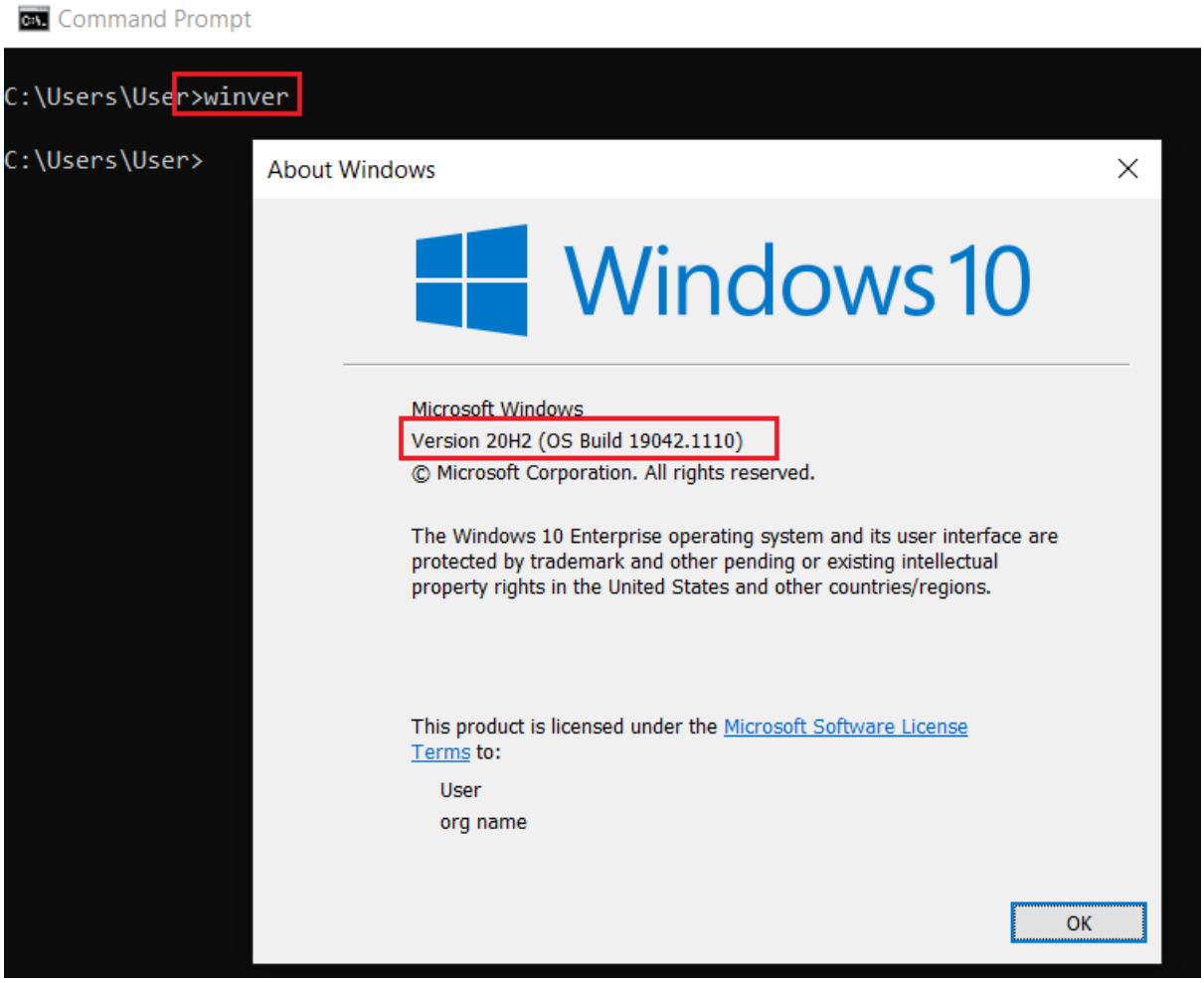
1- General System Information

There are many ways to retrieve general system information and current settings. I prefer the winver and Systeminfo command to

look for general information, followed by WMIC or PowerShell, to get specific details.

Winver

It's a straightforward yet useful command to quickly check the version and build the number of running Windows.

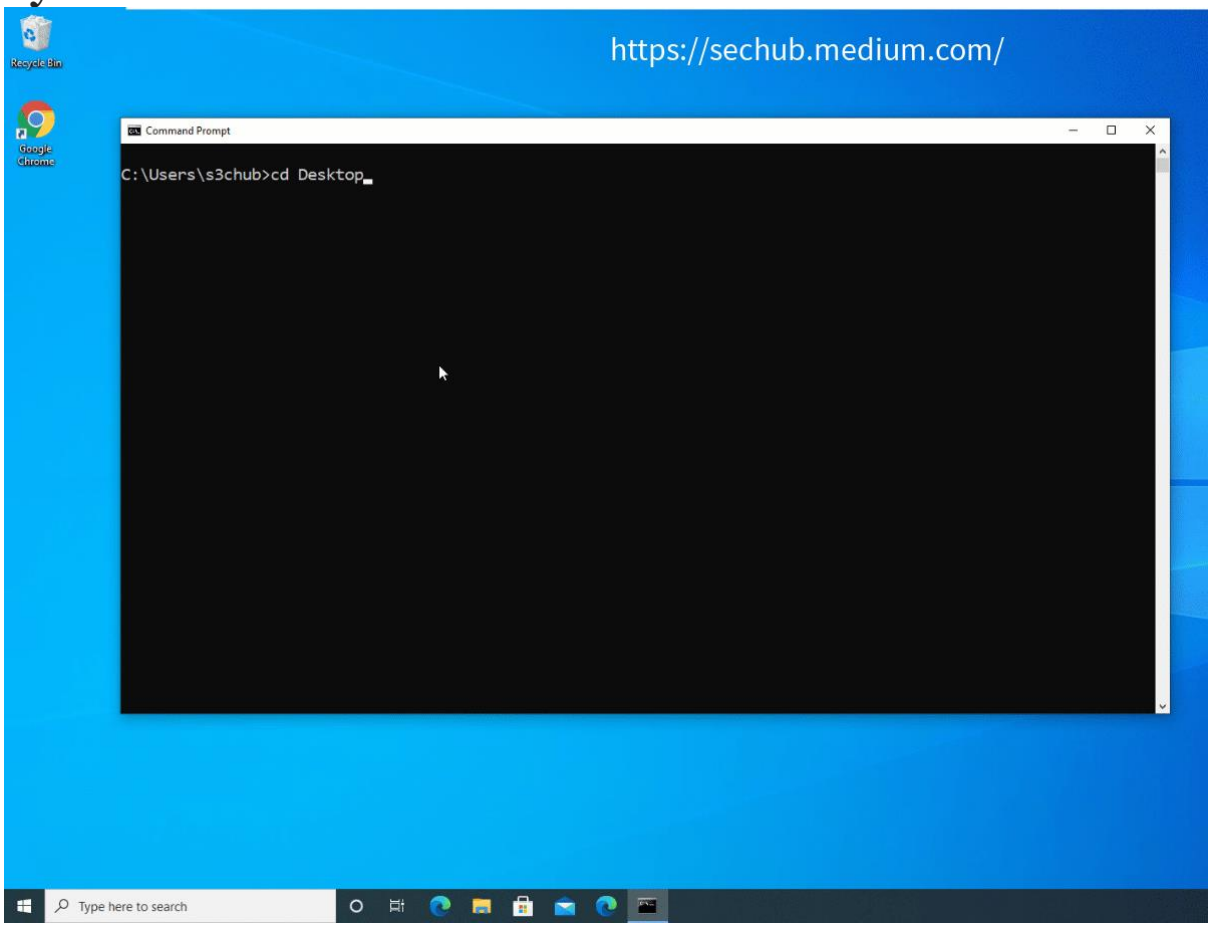


Winver Command

The version number can help investigators to obtain more information about issues and potential security risks. For instance, the issues related to the example above [version 20H2] can be found here.

Moreover, The compatibility of our tools with the version of OS being investigated is crucial. For example, not all Windows 10 versions are fully supported by the volatility framework for memory analysis. Thus, the OS exact version and build number [e.g. 10.0.18363 N/A Build 18363] helps us select the proper toolset for further investigation.

Systeminfo

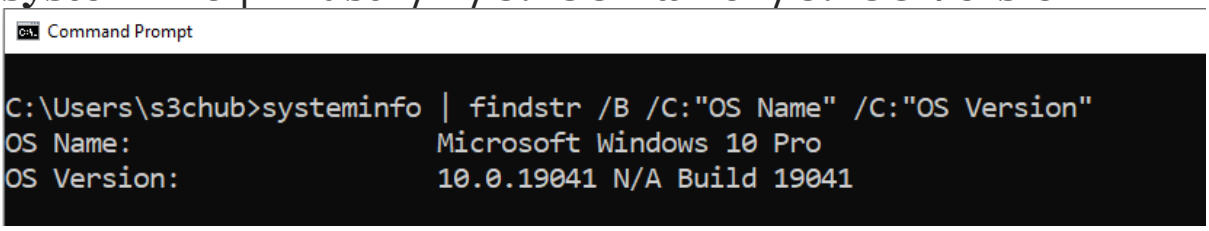


Systeminfo Command

The animation above shows the use of the systeminfo command. There is several useful information that helps the analyst to plan the rest of the investigation.

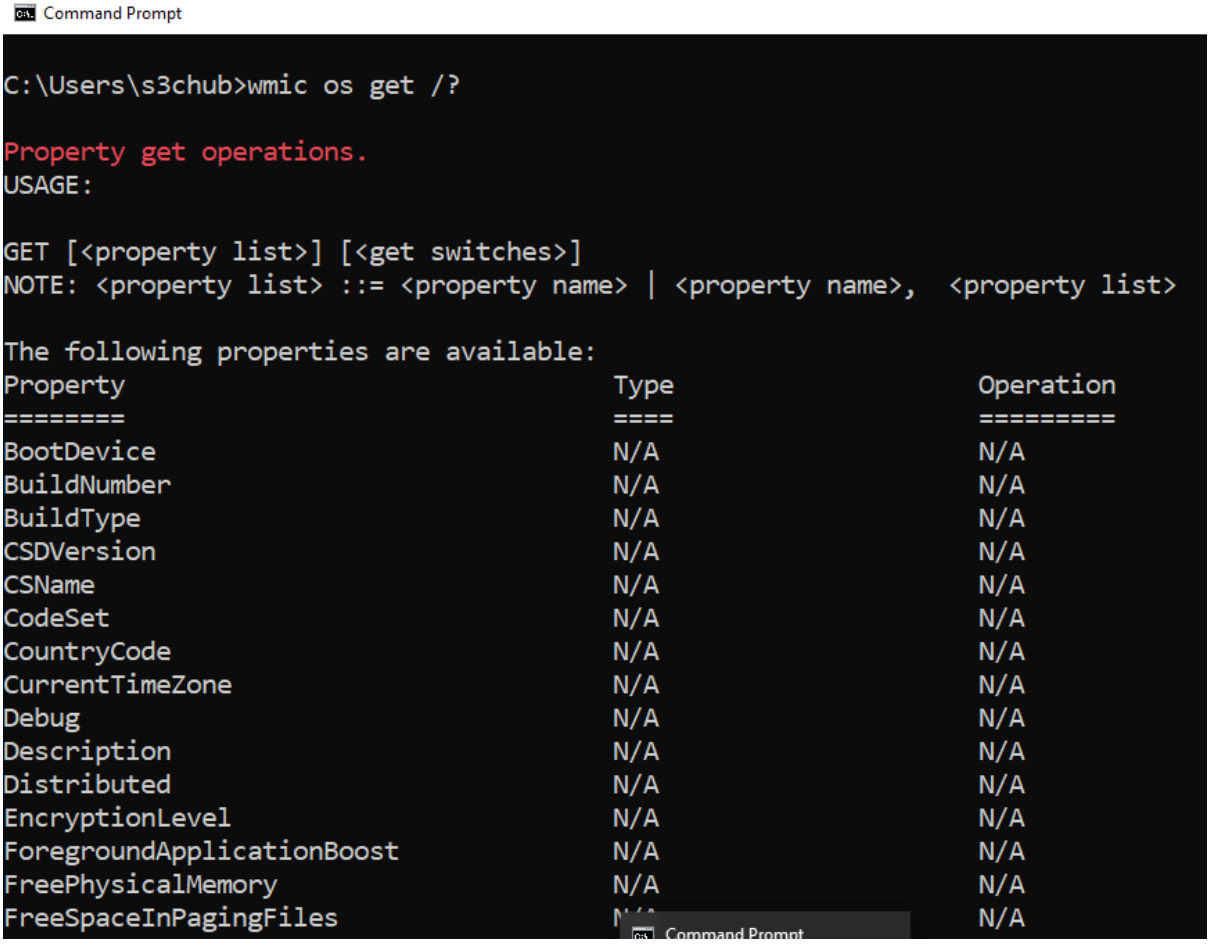
We can filter out specific information by using the findstr command. For instance, if we look for OS name and version, we can use the command below:

systeminfo | findstr /B /C:"OS Name" /C:"OS Version"



Filter Results with Findstr

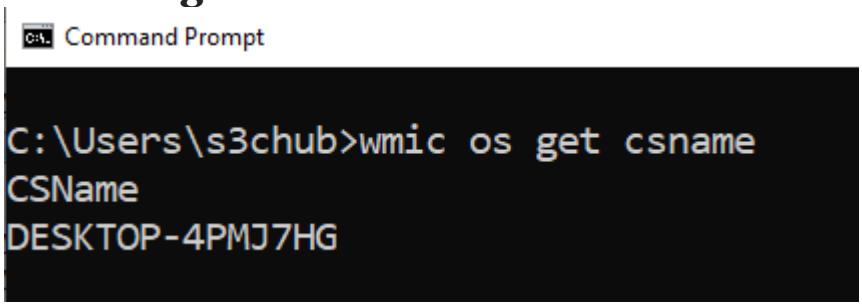
WMIC makes it easy to look for specific information. Type "wmic os get/?" to retrieve the list of available options as follows:



WMIC Available Options to Obtain System Information

In case we want to check the hostname, we can use the command below:

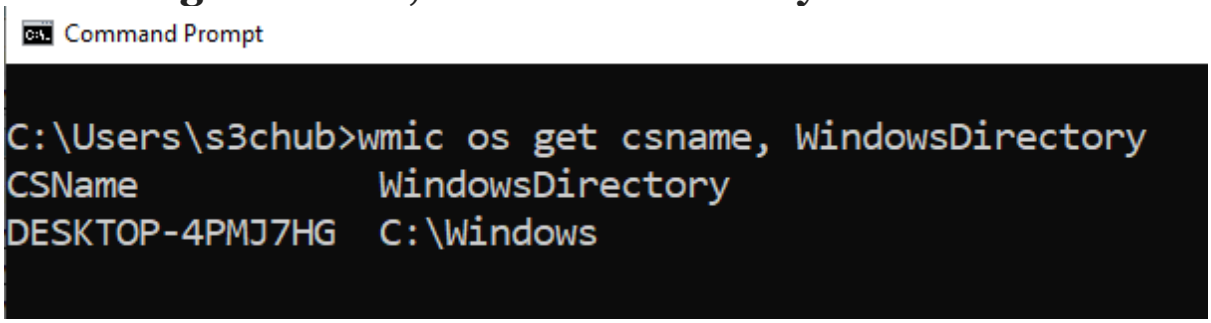
wmic os get csname



OS name obtained by WMIC

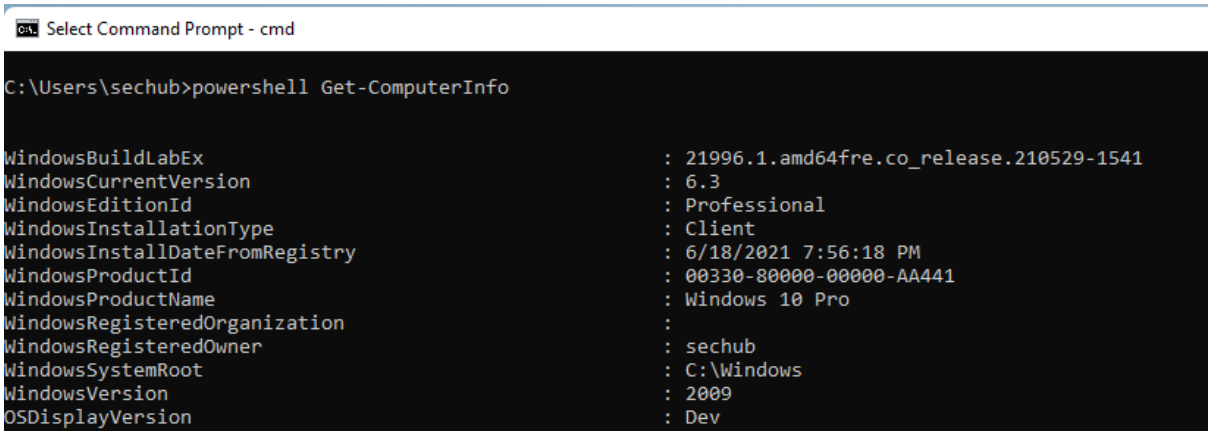
We can combine several values with comma as a separator as follows:

wmic os get csname, WindowsDirectory



OS name and directory obtained by WMIC

powershell Get-ComputerInfo



Obtain System Information Using powershell Get-ComputerInfo

Get-ComputerInfo -Property OsWindowsDirectory

Windows Installed directory obtained by powershell Get-ComputerInfo

2- Environment variables

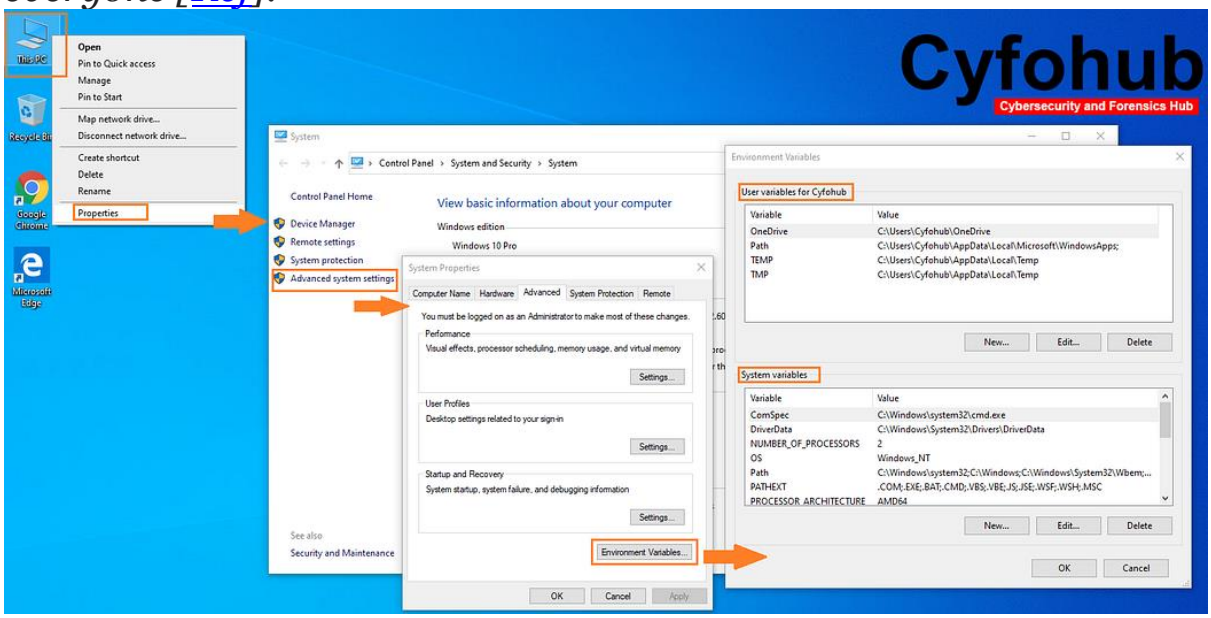
Environment variables are stored information such as search paths for files, directories for temporary files, application-specific options, etc. That tells us about the environment used by system users and processes.

They provide a wide variety of information that could be useful during the investigation. You can check the list of Standard (built-in)

windows environment variables here. The environment variables are divided into three scopes as follows:

- Machine (or System) scope: Belong to running instance of the system.
- User scope: Belong to a particular user under a system.
- Process scope: Combination of variables in the *Machine* and *User scopes*.

Note 1: *User environment variables are set for each user individually, while Machine environment variables are set for everyone [Ref].*

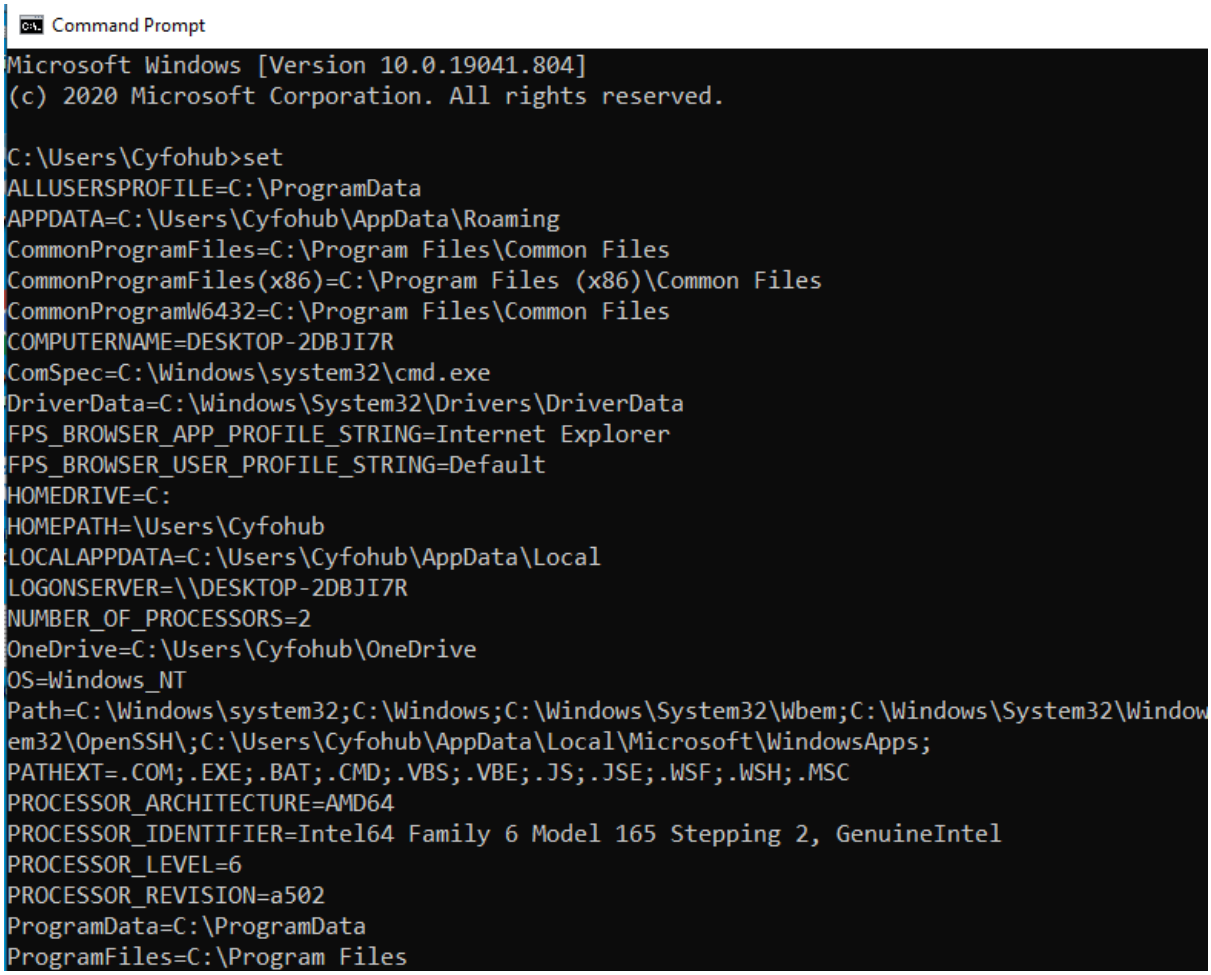


System and User Environment Variables

As shown in the figure above, we can see system and user environment variables from advanced system settings.

SET Command

The above information can be easily retrieved by using the SET command as well.

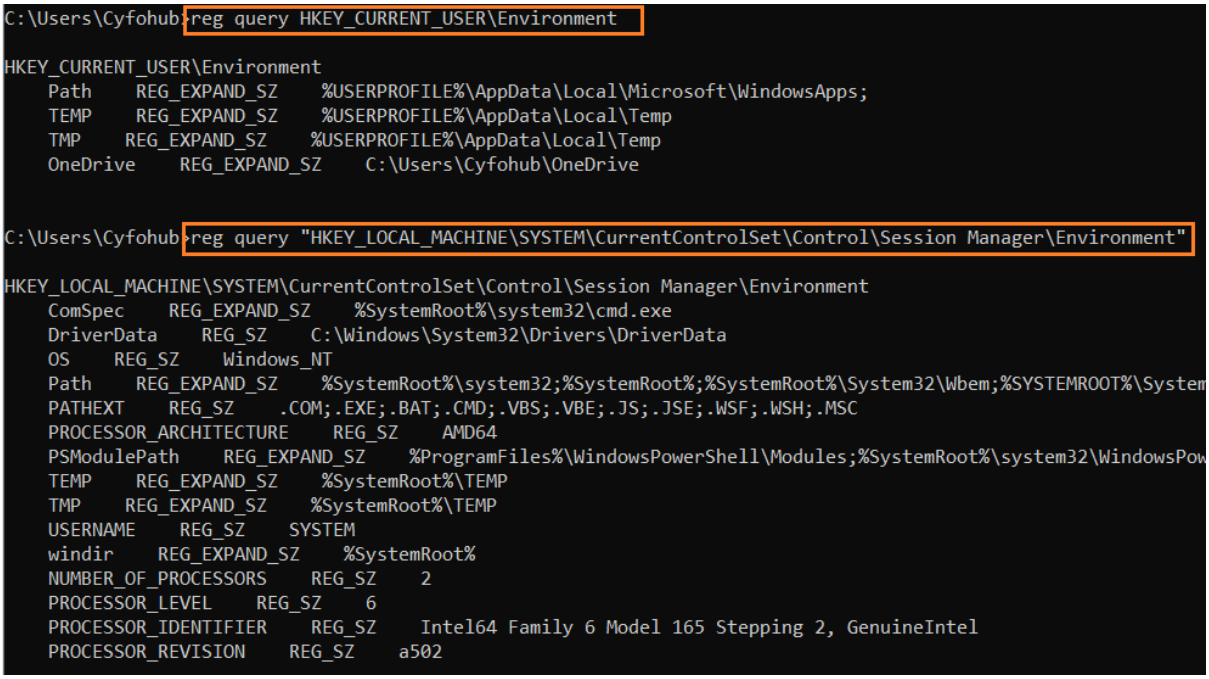


SET Command to Display System and User Environment Variables

Windows Registry

The locations of system and user environment variables in the registry are as follows and can display by reg query.

```
System:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\EnvironmentUser:
HKEY_CURRENT_USER\Environment
```



Reg Query Command to Display System and User Environment Variables from Windows Registry

Note 2: *the user variables in this post are associated with the currently logged-in user. The coming posts about the user accounts will discuss how to display the variables for other user accounts.*

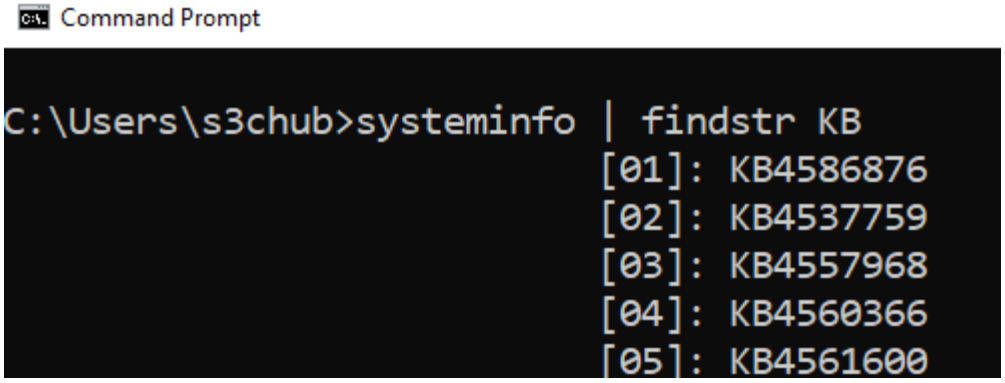
3- Hotfixes

Without a doubt, the list of installed hotfixes is one of the most important information to be collected as they determine if any patches or updates are missing and if the system is vulnerable.

There are many ways to obtain the installed hotfixes as follows:

Systeminfo: As you may notice, the systeminfo command shows the list of installed hotfixes as well; let's use systeminfo and findstr to get the hotfixes lists.

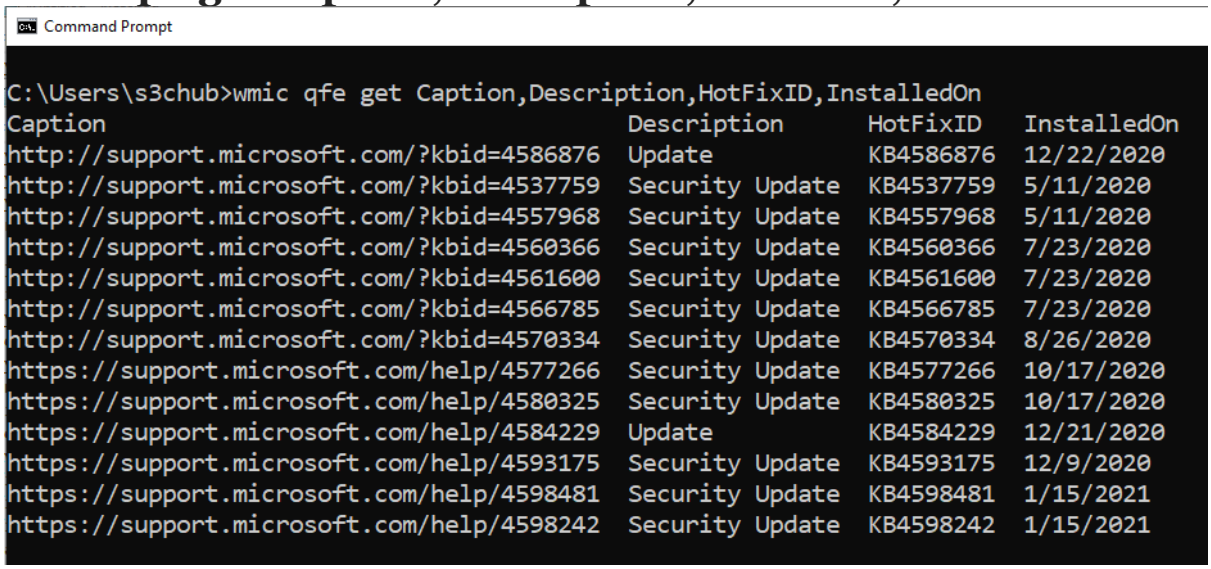
systeminfo | findstr KB



List of Installed Hotfixes from Systeminfo.

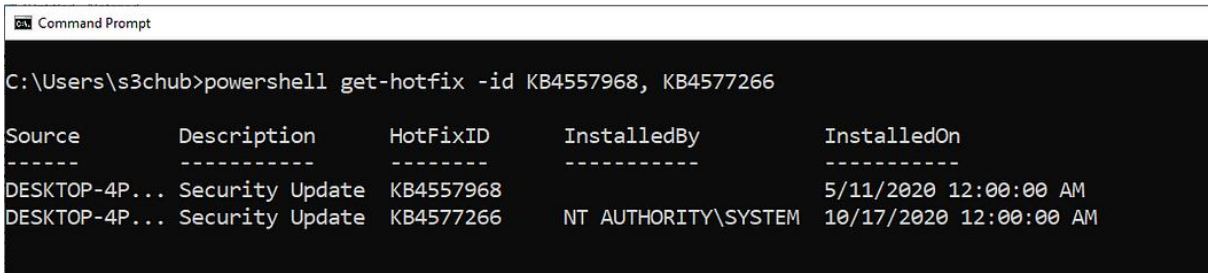
WMIC: We can obtain the same list by using *"wmic qfe get hotfixid"*, but let's get more details.

wmic qfe get Caption,Description,HotFixID,InstalledOn



Installed Hotfixes obtained by WMIC

Powershell: PowerShell provides investigators with a powerful command interface and scripting capabilities to collect numbers of artifacts. The *"powershell get-hotfix"* command helps us to get the list of installed hotfixes. However, we can look for specific hotfixes by their number.



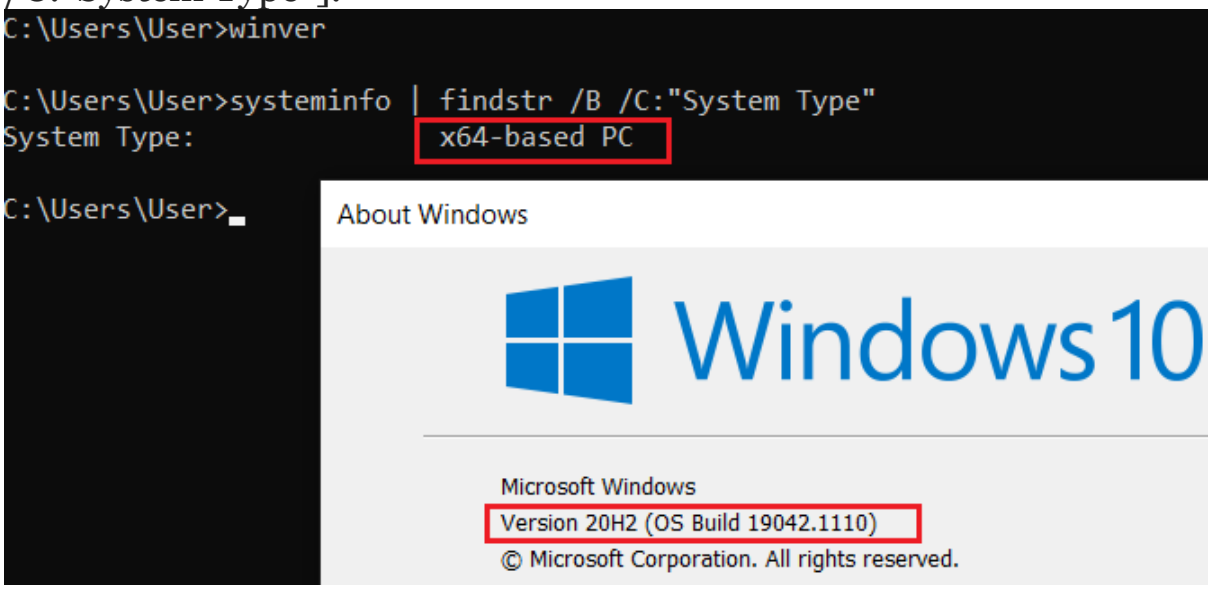
Installed Hotfixes obtained by Powershell

Note1: *findstr can be combined with systeminfo or WMIC to look for specific hotfixes as well.*

Note 2: *This post is not comparing the capabilities of windows commands, WMIC, and Powershell. The main aim is to demonstrate different data collection techniques.*

4- Missing Updates

The list of installed hotfixes must be validated to ensure all the latest patches have been installed. We just need to obtain the window version [Winver command] and System type [systeminfo | findstr /B /C:"System Type"].

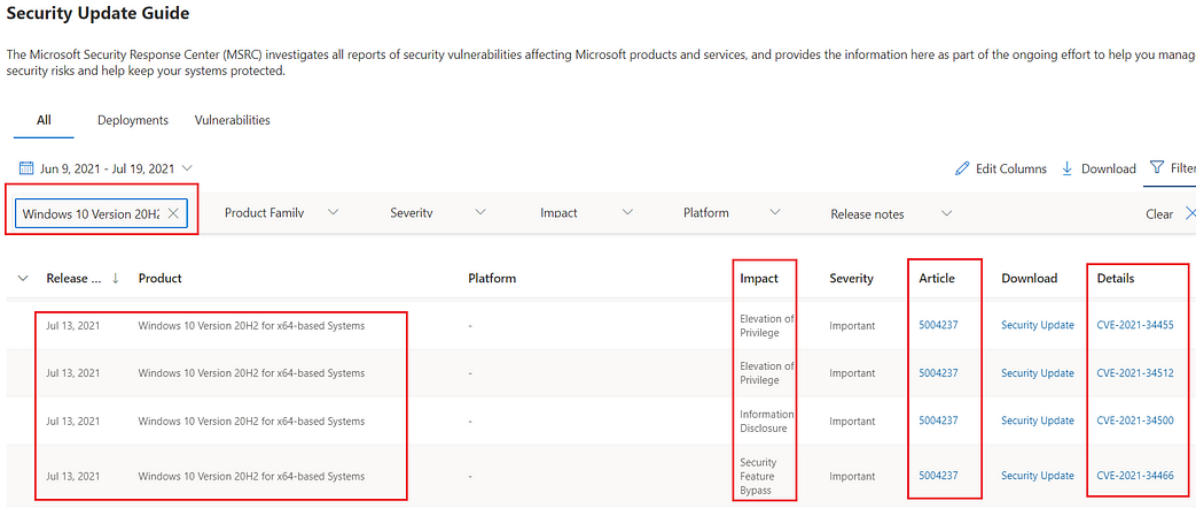


Windows Version and Type

For example, the above system OS is a 64 bit Windows with the version number 20H2 and built the number 19042. Now it's time to check the official Microsoft security update portal.

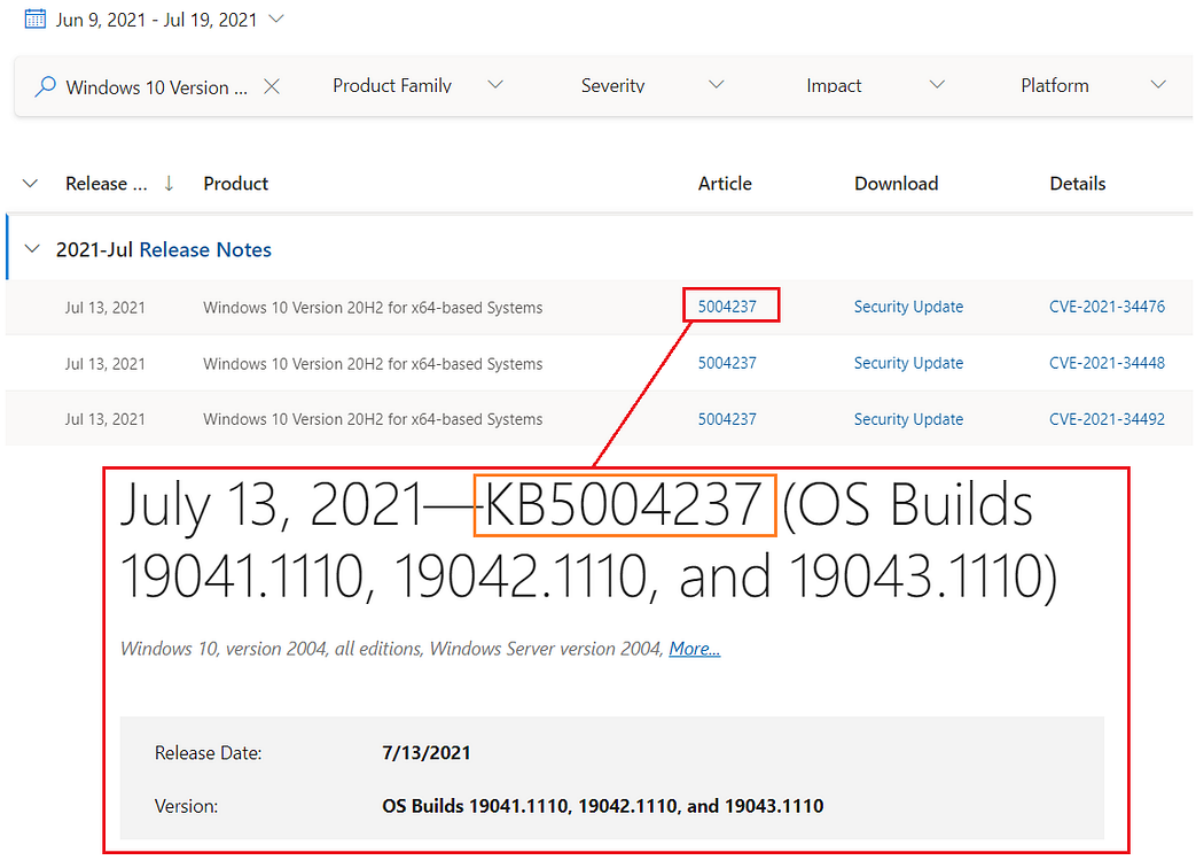
Security Update Guide - Microsoft Security Response Center
Edit description
msrc.microsoft.com

In the Security Update Guide section, we can use a keyword search to look for any update that matches our OS version and type.



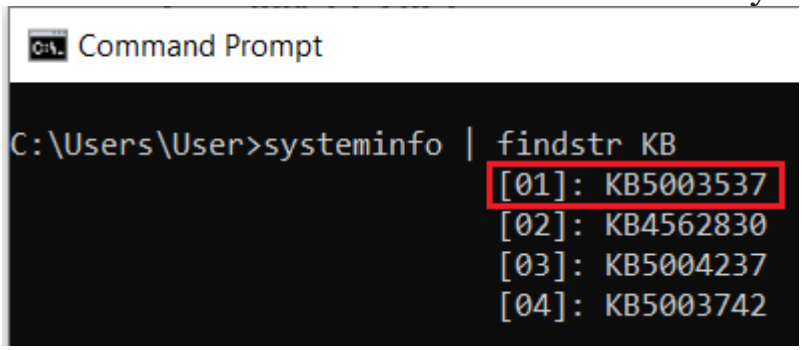
Security Update Guide for Windows 10 Version 20H2 for x64-based Systems

As depicts in the figure above, we can check the security issues impact, severity and related CVE details. The Article section gives us details information about updates s including released hotfixes, if any.



More Information about KB5004237

Let's check if the hotfix is installed on the system or not:



Installed Hotfixes

Yes, it's already there! But wait, what if it was missing:

- Look at the patch policies, rewrite, edit and roll out new ones.

- Formulate a vulnerability oriented hypothesis to examine the system.

Suppose a missing hotfix connects to a specific vulnerability. In that case, we can look for any indicator of compromise (IoC), an indicator of attack (IoA), or any unwanted activities related to that particular vulnerability.

5- Drivers!

A simple conversation with uncle google gives us several stories on how a security flaw in installed drivers opened the doors for attackers! The news below, for instance!

Living off another land: Ransomware borrows vulnerable driver to remove security software
Sophos has been investigating two different ransomware attacks where the adversaries deployed a legitimate, digitallyé
news.sophos.com

```
C:\Users\s3chub>driverquery

Module Name  Display Name           Driver Type   Link Date
============ ====================== ============ ======================
1394ohci     1394 OHCI Compliant Ho Kernel
3ware        3ware                  Kernel        5/18/2015 3:28:03 PM
ACPI         Microsoft ACPI Driver  Kernel
AcpiDev      ACPI Devices driver    Kernel
acpiex       Microsoft ACPIEx Drive Kernel
acpipagr     ACPI Processor Aggrega Kernel
AcpiPmi      ACPI Power Meter Drive Kernel
acpitime     ACPI Wake Alarm Driver Kernel
Acx01000     Acx01000               Kernel
ADP80XX      ADP80XX                Kernel        4/9/2015 1:49:48 PM
AFD          Ancillary Function Dri Kernel
```

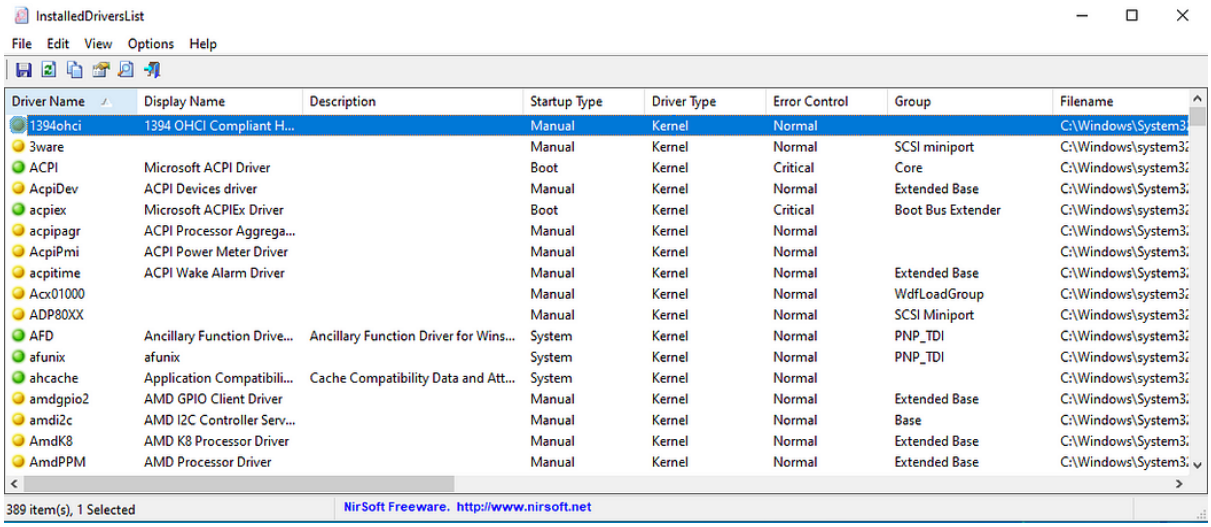
Built-in Command

```
PS C:\Users\s3chub> Get-WmiObject Win32_PnPSignedDriver| select devicename, driverversion

devicename                                   driverversion
----------                                   -------------
Local Print Queue                            10.0.19041.1
Local Print Queue                            10.0.19041.1
Local Print Queue                            10.0.19041.1
Local Print Queue                            10.0.19041.1
Local Print Queue                            10.0.19041.1
Local Print Queue                            10.0.19041.1
WAN Miniport (Network Monitor)               10.0.19041.1
WAN Miniport (IPv6)                          10.0.19041.1
WAN Miniport (IP)                            10.0.19041.1
WAN Miniport (PPPOE)                         10.0.19041.1
WAN Miniport (PPTP)                          10.0.19041.1
```

Powershell

Installed Drivers List obtained.

The image above depicts the use of windows built-in command and Powershell to retrieve the list of drivers. Nirsoft provides a GUI-based tool called installed_drivers_list to retrieve the list of available drivers as well.



InstalledDriverList by Nirsoft

- Green Icon — The driver is running on the Windows kernel.
- Yellow Icon — The driver is not running on the Windows kernel.
- Red Icon — The driver is not running on the Windows kernel, but it should be loaded automatically when Windows starts.

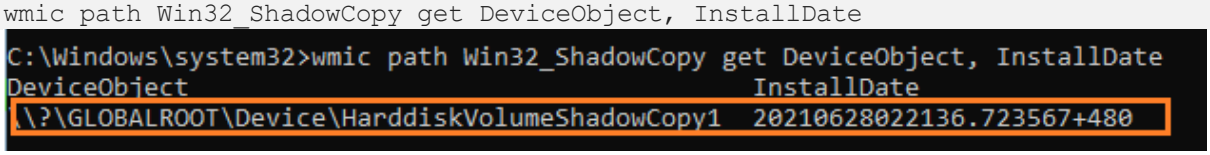
6- Shadow Copies

Shadow copies are the snapshots — backup — of Windows files and can be used to restore data when required. The shadow copies kept the previous state, data, and files of a machine and may help us during an investigation. However, they are not as good as forensics images of a hard disk as they contain a snapshot of a file at a particular point in time.

Besides, not all machines being investigated may have the shadow copies or restore point enabled. Thus, we should check if there is any shadow copy that exists on the target machine.

The image below shows WMIC and vssadmin to obtain the list of available shadow copies in a system.

```
wmic path Win32_ShadowCopy get DeviceObject, InstallDate
```



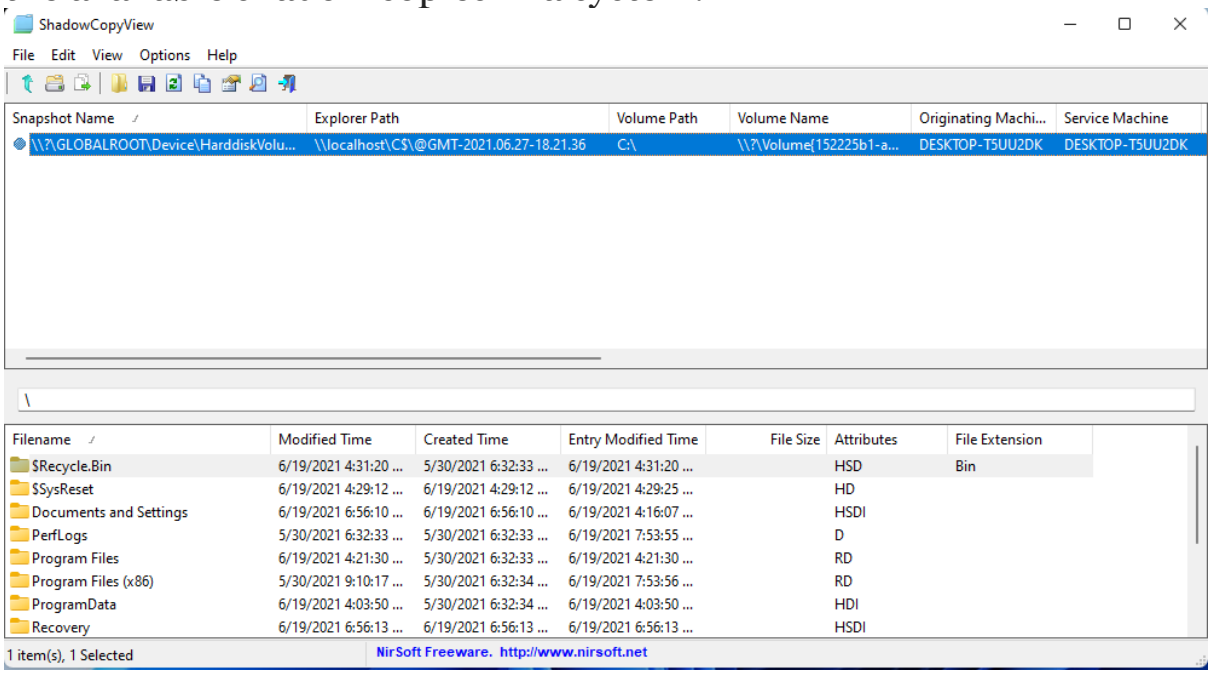
The List of Available Shadow Copies in a system obtained by WMIC

```
vssadmin list shadows
```

```
C:\Windows\system32>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {f67e851c-b538-402d-962c-81a0234708b1}
   Contained 1 shadow copies at creation time: 6/28/2021 2:21:36 AM
      Shadow Copy ID: {6392fc08-ca4a-4b60-b1a6-77deff6616f8}
         Original Volume: (C:)\\?\Volume{152225b1-ab20-4d33-a18d-b6d365b6ef43}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
         Originating Machine: DESKTOP-T5UU2DK
         Service Machine: DESKTOP-T5UU2DK
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessible
         Attributes: Persistent, Client-accessible, No auto release, No writers, Differential
```

The List of Available Shadow Copies in a system obtained by VSSADMIN

Nirsoft provides a GUI-based tool called ShadowCopyView to view the available shadow copies in a system.



The List of Available Shadow Copies in a system obtained by Nirsoft Tool

Note1: *having the shadow copies does not guarantee any successful or complete data recovery. It highly depends on the type of shadow copies, creation time, and the last overwritten point by OS.*

Note 2: *Based on the golden rule of digital forensics, we collect data as much as possible and available; may the force be with us later in in-depth analysis.*

System Live Analysis [Part 5]- Windows: Users, Groups, and Privileges

Data Types: User account information, login timestamps, account activities, account groups, and privileges.

Investigation Value: To look for any questionable activities related to user accounts such as suspicious and unexpected login hours, locations, and privileges.

1- How User Accounts Abused by Hackers!

Finding user account exists on systems being analyzed is an integral part of every forensics investigation. Why? Because there might be a mystery behind every user account [Local | Domain]!

- **Existing/Default Accounts:** Users and system default accounts are one of the hackers' top favorite targets as they may able to abuse them to carry out malicious activities.

Local Accounts (Windows 10) - Microsoft 365 Security
Windows 10 Windows Server 2019 Windows Server 2016 This reference topic for IT professionals describes the defaulté
docs.microsoft.com

- **Newly Created Accounts:** As mentioned in part 3, creating new accounts upon initial access are a common technique used by attackers. Therefore, the user account list in a system must be verified and validated by the user or

company IT team to look for any user without their knowledge. The Stolen Pencil malware utilized a tool to create an admin account on an infected Windows machine.

STOLEN PENCIL Campaign Targets Academia | NETSCOUT
ASERT has learned of an APT campaign, possibly originating from DPRK, we are calling STOLEN PENCIL that is targetingé
www.netscout.com

- **Deleted/Modified Accounts:** Yes! It's not all about the existing users only! An attacker may delete a user account, disable it or change its password or privilege to interrupt system or resource availability. For instance, LockerGoga ransomware changed user passwords right after the initial infection and their log them off from the system.

What You Need to Know About the LockerGoga Ransomware
The systems of Norwegian aluminum manufacturing company Norsk Hydro were reportedly struck last Tuesday, March 19, byé
www.trendmicro.com

2- The hackers' mindset: Use of user name in a cyber attack lifecycle

Hackers use user accounts for initial access and several ways in different stages of a cyber attack. I just try to briefly explain the key points from MITRE ATT&CK knowledge base of adversaries.

- **Lateral Movement:** Having access to legitimate user account credentials may allow attackers to establish a remote connection, interact with target machines, or log in to them via services such as telnet, SSH, RDP, SMB, WinRM, and VNC.
- **Persistence:** Creating a new account [local |domain] or manipulating the existing ones is a common technique used by adversaries to maintain access to compromised systems across conditions that may remove or limit the initial access.
- **Privilege Escalation:** Obtaining the default and valid accounts' credentials may help an attacker evaluate the initial access to the higher levels with more permissions such as system and root.
- **Defense Evasion:** Attackers may abuse the valid account in the system to establish legitimate access to the victim machine, which is more challenging to be traced and detected.
- **Impact:** We are mostly thinking of how hackers may use the user accounts. However, they may delete, disable or limit the account to interrupt legitimate accesses.

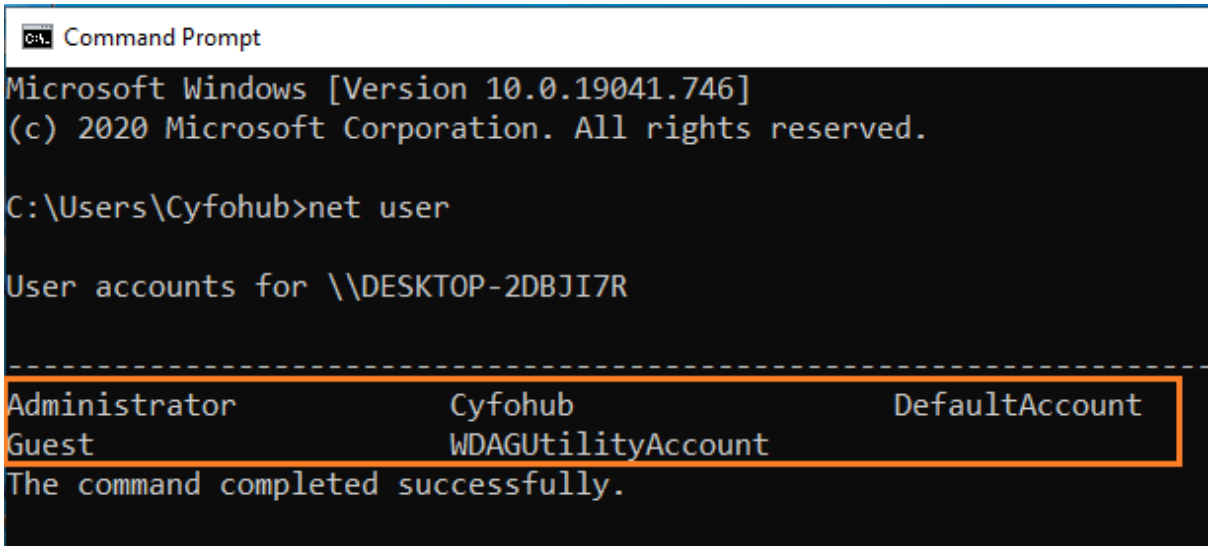
3- List of User Accounts in Windows

There are many ways to retrieve the user accounts during live windows analysis. As a common practice of my write-ups, I will

cover several methods without a detailed comparison of their efficiency.

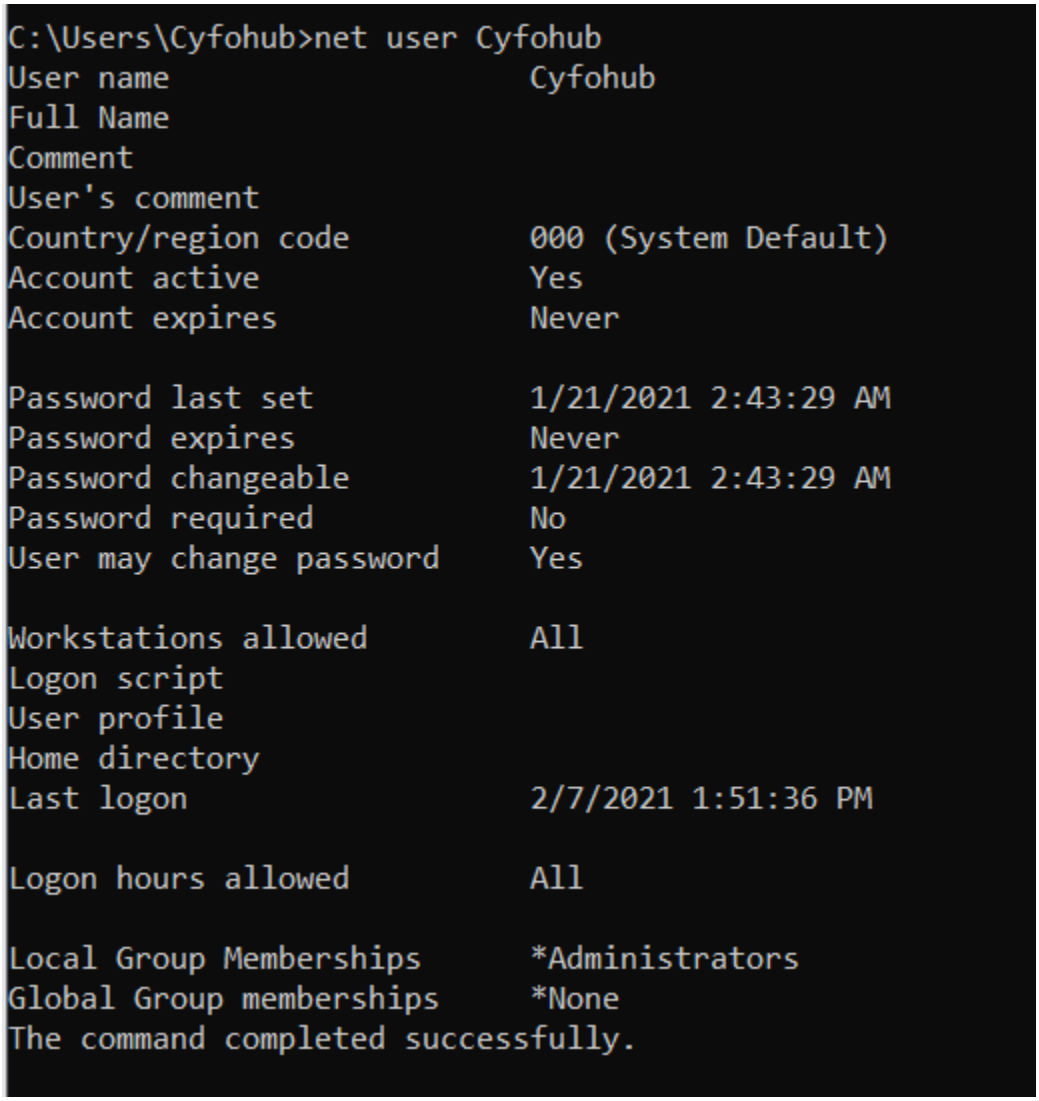
net user:

net user is a built-in windows commands to displays a list of all user accounts. The figure below shows the use of the net user to find the local accounts:



Net User Command and Local Users List

can use the net user command to get more information on a particular user account. Example: net user Cyfohub



Specific User Account Information

As shown in the figure above, we can determine the last login time and local group membership of the Cyfohub user account. As discussed in previous parts, we can always combine the commands with findstr if we only aim to retrieve specif information. For instance, to only obtain the last logon time of the Cyfohub user account, we can use the command below:

```
net user  username | findstr /B /C:"Last logon"
```

wmic useraccount:

The wmic useraccount is my favorite command as we can obtain more information in an organized way. We have LIST and GET options. Let's try both of them:

```
wmic useraccount list full
```

```
C:\Users\User>wmic useraccount list full


AccountType=512
Description=Built-in account for administering the computer/domain
Disabled=TRUE
Domain=DESKTOP-H5G6KM6
FullName=
InstallDate=
LocalAccount=TRUE
Lockout=FALSE
Name=Administrator
PasswordChangeable=TRUE
PasswordExpires=FALSE
PasswordRequired=TRUE
SID=S-1-5-21-[redacted]-500
SIDType=1
Status=Degraded
```

WMIC User Account List Option

The “/?” help us to display the list of available options. For instance, the command below shows the list of “get” options.

```
wmic useraccount get /?
```

```
C:\Users\Cyfohub\Desktop>wmic useraccount get /?

Property get operations.
USAGE:

GET [<property list>] [<get switches>]
NOTE: <property list> ::= <property name> | <property name>,  <property list>

The following properties are available:
Property                                Type                    Operation
========                                ====                    =========
AccountType                             N/A                     N/A
Description                             N/A                     N/A
Disabled                                N/A                     N/A
Domain                                  N/A                     N/A
FullName                                N/A                     N/A
InstallDate                             N/A                     N/A
LocalAccount                            N/A                     N/A
Lockout                                 N/A                     N/A
Name                                    N/A                     N/A
PasswordChangeable                      N/A                     N/A
PasswordExpires                         N/A                     N/A
PasswordRequired                        N/A                     N/A
SID                                     N/A                     N/A
SIDType                                 N/A                     N/A
Status                                  N/A                     N/A
```

wmic useraccount GET properties

I'm going to retrieve the name, account type, sid, and status for user accounts:

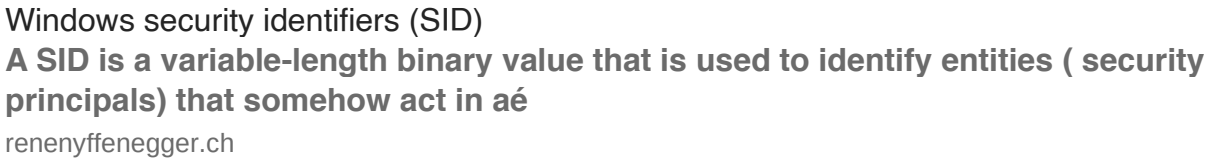
```
wmic useraccount get name, accounttype, sid, status
```

```
C:\Users\Cyfohub\Desktop>wmic useraccount get name, accounttype, sid, status
AccountType  Name               SID                                            Status
512          Administrator      S-1-5-21-[redacted]-500   Degraded
512          Cyfohub            S-1-5-21-[redacted]-1001  OK
512          DefaultAccount     S-1-5-21-[redacted]-503   Degraded
512          Guest              S-1-5-21-[redacted]-501   Degraded
512          WDAGUtilityAccount S-1-5-21-[redacted]-504   Degraded
```

[i] Account Type: Indicates the type of users such as Normal account (512), Temporary duplicate account (256), Interdomain trust account (2048), and Server trust account (8192).Workstation trust account (4096).

Code 512 represents default or normal accounts; thus, we only see this account type when a system is not part of a domain and only contains local accounts.

[ii] SID: Security Identifier is a unique value assigned to an object such as a user, a group, or a service within a system. SID is issued by an authority, such as a Microsoft AD Domain Controller or the Windows OS, and used to set special privileges or restrictions for objects (e.g., user).

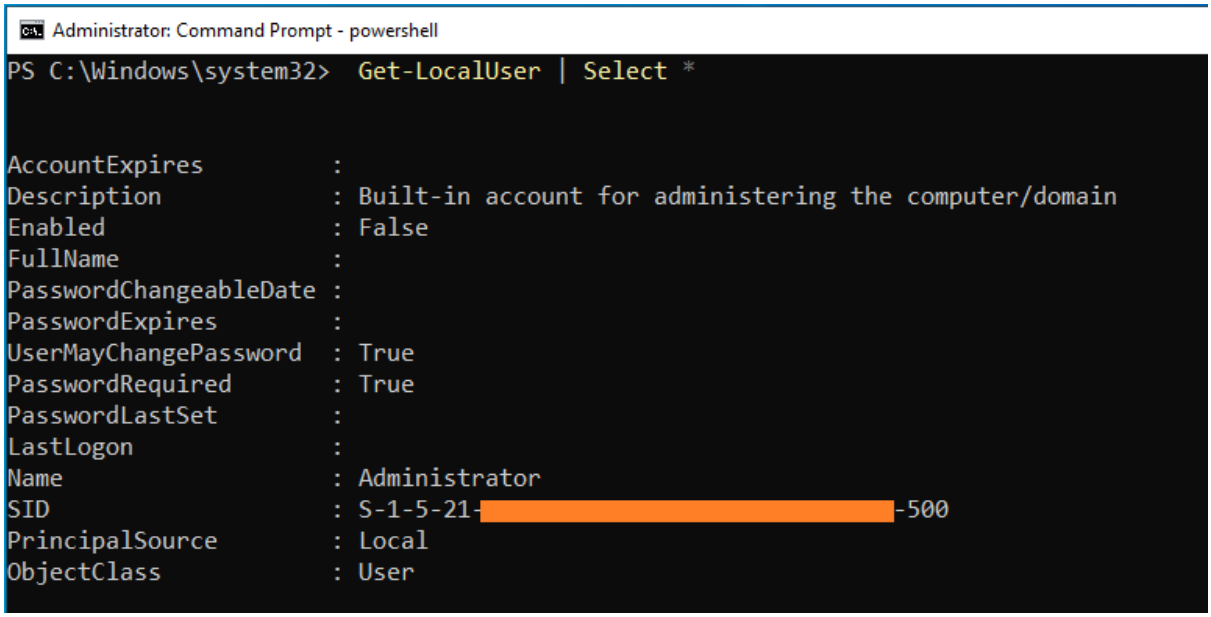


[iii]Status: This is the current status of the user account. The value for the enabled account is “Ok” and for disabled accounts is “Degraded”.

Powershell Get-LocalUser

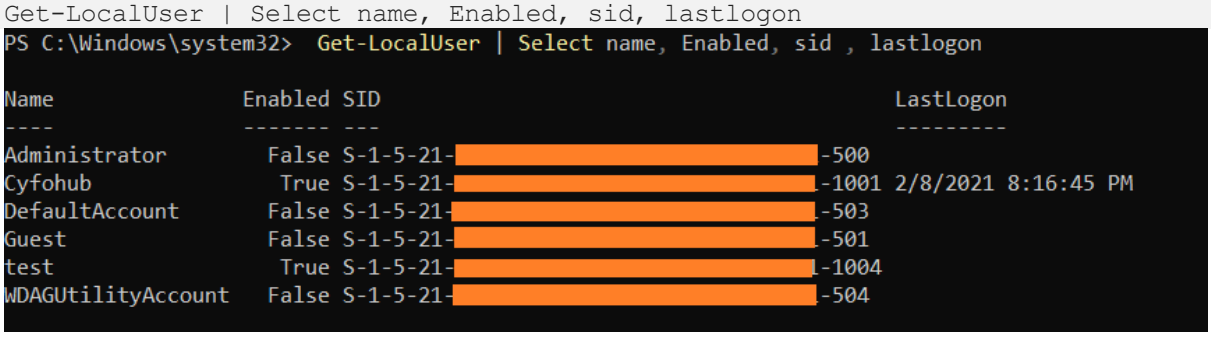
The Get-LocalUser, along with “select *” displays the list of all existing users in addition to the associated fields.

```
Get-LocalUser | Select *
```



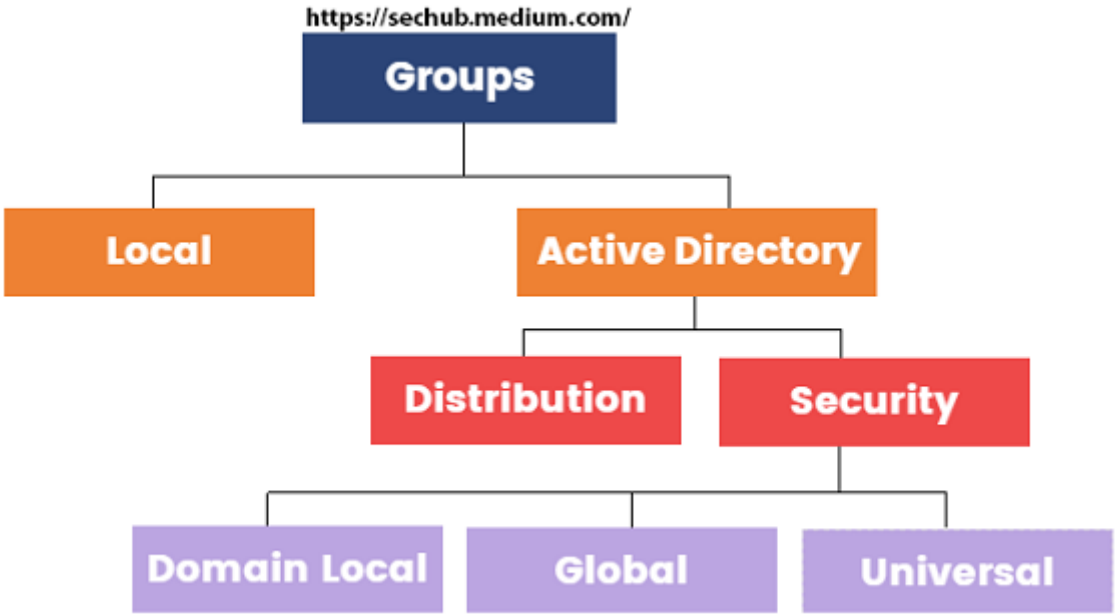
We can use the select option only to retrieve specific information about each user.

```
Get-LocalUser | Select name, Enabled, sid, lastlogon
```



4- Groups and Privileges

A group is a set of user accounts with the same security rights and have the same privileges [access rights] to deal with the system or network resources. A group can be defined at the host level only as a local group or can be part of the Domain level as a Distribution or security group.

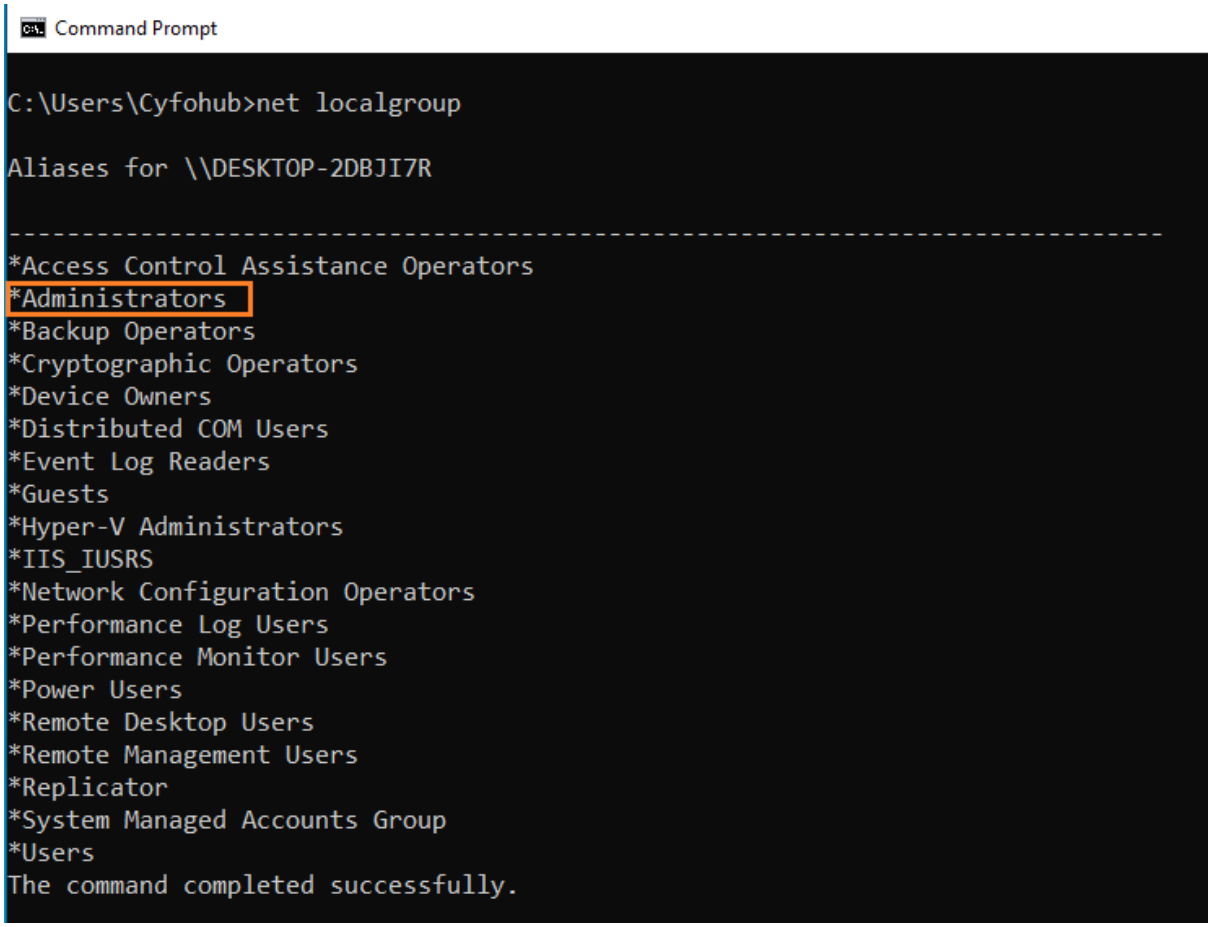


Windows Local and Active Directory Groups

Note: These write-up series focuses on local groups only.

net localgroup

A built-in Windows command helps to display the local groups that exist on the target being analyzed.



Local Groups in Windows

Windows create most of the groups above as a default group during OS installation. Let's check the user members of the administrator and user groups.

net localgroup [Group name]

```
net localgroup Administrators
net localgroup Users
```

```
C:\Windows\system32>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
Cyfohub
The command completed successfully.


C:\Windows\system32>net localgroup Users
Alias name     Users
Comment        Users are prevented from making accidental or intentional system-wide change
ns

Members

-------------------------------------------------------------------------------
NT AUTHORITY\Authenticated Users
NT AUTHORITY\INTERACTIVE
Sechub
The command completed successfully.
```

Users in Administrators and Users Groups

As shown in the figure above, we have two accounts for the Administrators group [Administrator, and Cyfohub] and one under the User group [Sechub].

Powershell

```
Get-LocalGroupMember -Group “Administrators” | select name,PrincipalSource,
sid
```

```
Command Prompt - powershell
PS C:\Users\Cyfohub> Get-LocalGroupMember -Group "Administrators" | select name,PrincipalSource, sid

Name                          PrincipalSource SID
----                          --------------- ---
DESKTOP-2DBJI7R\Administrator          Local S-1-5-21-[redacted]-500
DESKTOP-2DBJI7R\Cyfohub                Local S-1-5-21-[redacted]-1001
```

5. What would be Next

If you read this post, you may ask… mmm… ok! now I know:

- How hackers may use user accounts

- How would be the use of a username in a cyberattack life cycle
- How to obtain the list of user accounts in the system
- how to determine the groups that user account belongs to and what they can do in that group.

But….. what would be next! How to look for suspicious or malicious acts!

System Live Analysis [Part 6]- Windows: User Account Forensics-Road Map

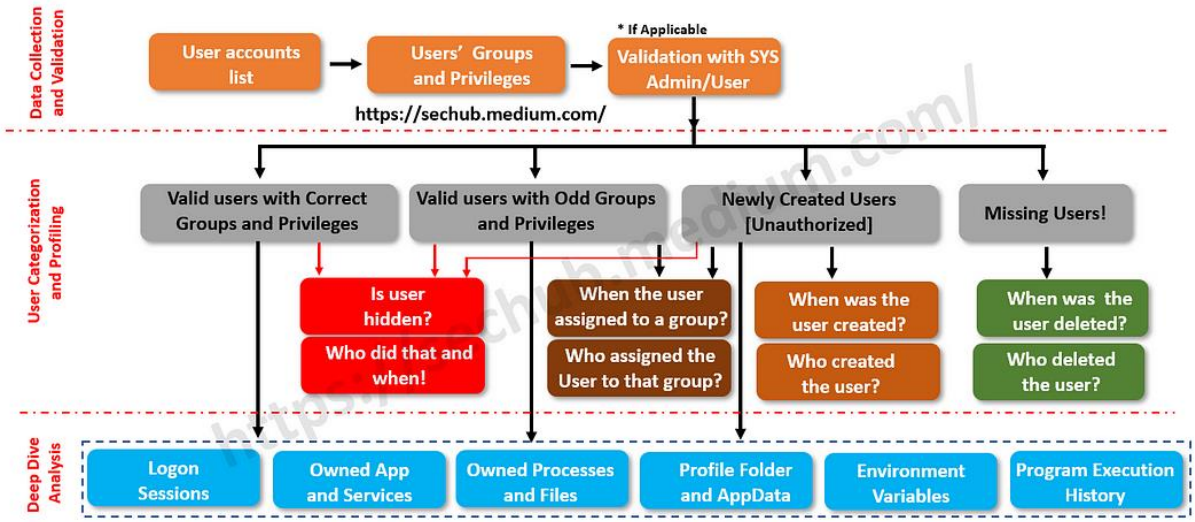
Digital forensics and incident response are not about obtaining the data only. Profiling the activities, analyzing them, and looking for any evidence of suspicious/malicious activities is a challenging part of the journey.

Collecting data could be much more comfortable in comparison to data analysis and evidence interception. This part presents a road map for user accounts forensics to identify the good, the bad, and the unknown!!

1. **User Account Forensics — The Road Map**

The proposed Road Map is designed based on my experience and best practices that I have employed to carry out the number of projects and yet to learn more.

If you can help me make it better, you are most welcome! together we care, together we share, together we win :)



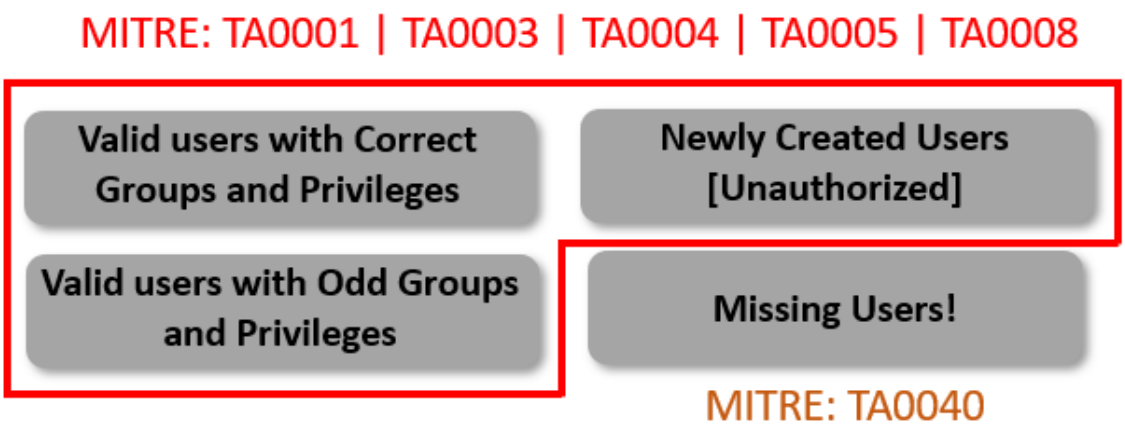
User Account Forensics Roadmap

The road map is divided into three main phases as follows:

- **Data collection and validation:** Once the data on user account are collected, we should validate them with network admins or system users where it is applicable. It significantly helps us to identify unknown user account or odd characteristics. The last post discussed the different methods of user account data collection.

Blue Team-System Live Analysis [Part 5]- Windows: Users, Groups, and Privileges
Let's Connect | LinkedIn
sechub.medium.com

- **User categorization and profiling:** In this phase, we will categorize the user accounts as they could be used in different stages of a cyber attack.



User Account Attacks mapped with MITRE

- **Deep-dive analysis:** Finally, we should conduct an in-depth analysis of each user account to look for Good, Bad, and Unknowns!

Note: *It is essential to understand the operational needs, business logic, and standard configuration [baseline] of the targeted system and form a standard system profile to look for any deviation accordingly.*

2. User Account Categories

The user accounts on a system can be categorized as follows:

- **Valid Users with Valid Groups and permissions:** These are legitimate user account created by network admin or system users. We can't simply assume these accounts are safe as cybercriminals might misuse them.

- **Valid Users with odd groups and permissions:** However, this group of accounts is still legitimate, but the group that they are assigned to or the privileges they have may not be what supposed to be. For instance, a cybercriminal may abuse a valid user's credentials to gain access or modify the privileges to carry out malicious activities.
- **Newly Created Users [Unknowns]:** As the name suggests, these users are unknown and can't be verified and validated by the system user or IT team. Creating new accounts upon initial access is a common technique used by attackers. Thus, they are tagged as a high risk.
- **Missing Users!:** We are mostly thinking of how hackers may misuse valid user accounts; however, they may also delete, disable or limit the account to interrupt legitimate accesses.

3. User accounts at a glance

Let's use the wmic command explained in the last part to obtain the list of user accounts in a test system and intercept the findings.

```
wmic useraccount get name, accounttype, sid, status
```

```
C:\Users\Cyfohub>wmic useraccount get name, accounttype, sid, status
AccountType  Name               SID                                                Status
512          Administrator      S-1-5-21-[redacted]-500    Degraded
512          Cyfohub            S-1-5-21-[redacted]-1001   OK
512          DefaultAccount     S-1-5-21-[redacted]-503    Degraded
512          Guest              S-1-5-21-[redacted]-501    Degraded
512          sechub             S-1-5-21-[redacted]-1005   OK
512          WDAGUtilityAccount S-1-5-21-[redacted]-504    Degraded
```

Account Type:

As shown in the figure above, we have 6 local user accounts, all with type 512 representing a typical user account. It indicates only local user accounts exist in this system; thus, if the system used to be part of a domain, we have to tag it as abnormal and do further investigations.

SID and RID:

The first step in user account analysis is to know the well-known security identifiers (SID) in Windows operating systems, especially the RIDs. RID or Relative Identifier is the last segment of a SID and is unique for each user account.

There are two types of RIDs on the target systems, such as 5XX and 1XXX. Windows reserves RIDs less than 1000 for special accounts. Based on the well-known SID list, users with RIDs of 500, 501, and 503 are expected in our test machine.

```
S-1-5-21-<machine>-500 : Administrator
S-1-5-21-<machine>-501 : Guest
S-1-5-21-<machine>-503 : DefaultAccount
S-1-5-21-<machine>-504 : WDAGUtilityAccount
```

The user account with RID 504 is not on the well-known list; however, a simple search shows that this user account used by the system for Windows Defender Application Guard.

Tip: *why the RID of 502 is missing? Because it's for Kerberos tickets in the active directory! As the target machine is not part of any domain, so it's normal!*

Let's focus on the RIDs in the range of 1XXX; windows allocate the RID to entities starting at 1000. well, we have only two user accounts with RIDs 1001 and 1002 as following:

```
S-1-5-21-<machine>-1001 : Cyfohub
S-1-5-21-<machine>-1005 : sechub
```

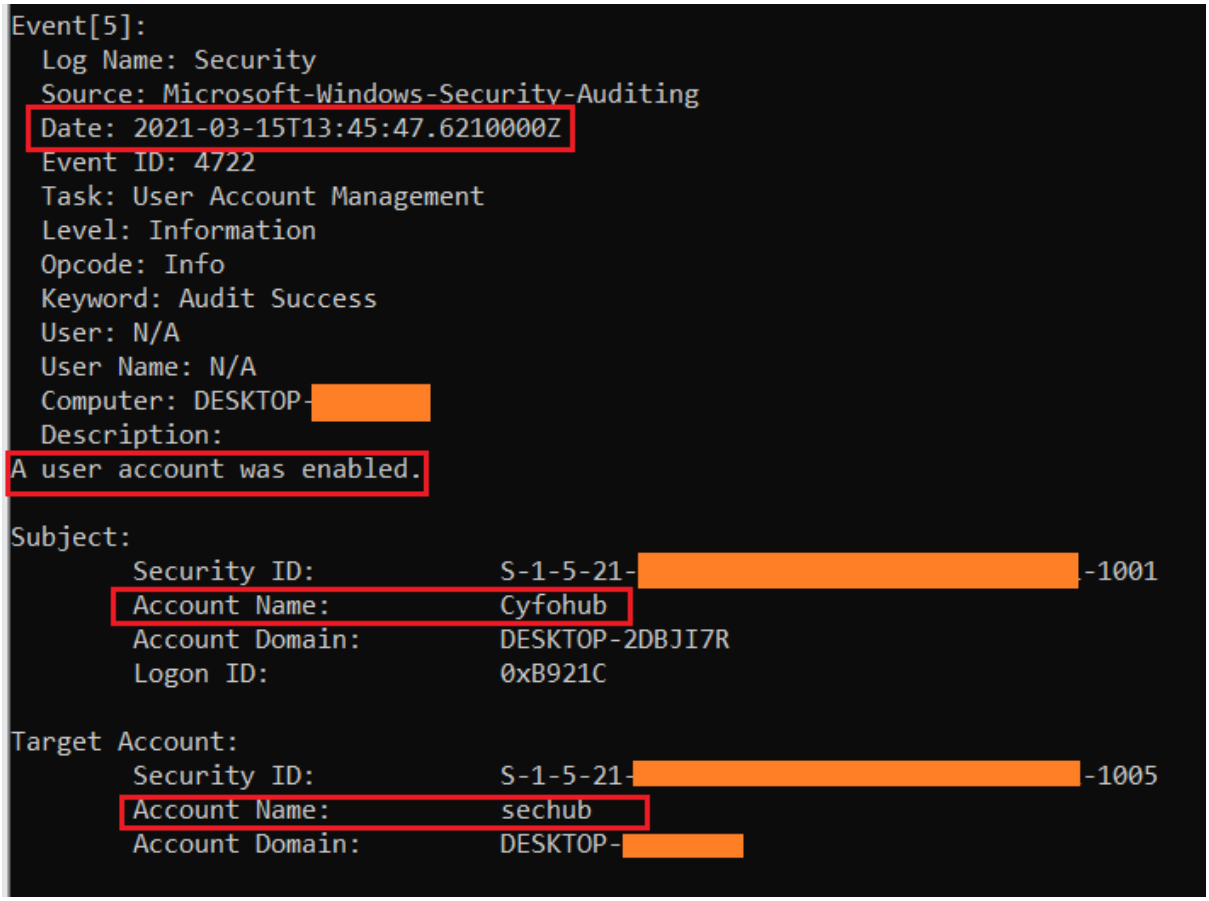
Why are the RIDs 1001 and 1005? What happened to 1000? How about 1002, 1003, and 1004? it's an excellent question! We will dive deep into it in the next post.

Status:

This is the current status of the user accounts. The value for the accounts with RIDs 5XX is Degraded [disabled]. In a normal situation, all of these accounts are disabled for better security. So nothing is wrong with our test system.

During the investigation, if we noticed any of these accounts are enabled, specially build-in administrator and Guest, we must put them in suspicious status to do further analysis. We can use the event ID 4722 to check when a user is enabled and by who!

```
wevtutil qe security /f:text "/q:*[System[(EventID=4722)]]"
```



The above result shows that the user sechub [Target Account]was enabled by Cyfohub [Subject] on 15 of March 2021.

Note: Logs are logs, and there will be nothing if they are not enabled! To use the windows events and logs as a precious source of data for investigation, we should ensure they are enabled. For instance, we need to enable “Audit account management” for all the information related to user accounts.

```
Computer Configuration > Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Account Management: Audit User Account Management → Define → Success and Failures
```

4. What’s Next!

So far, we have listed the existing local user accounts in the test system, we have analyzed the Type, RIDs, and Statuses. The next post will explain more on user account profiling to understand:

· When were users created?

· Who created the users!

· When users assigned to a specific group and by who?

. Is there any hidden user account? who hides them and when?

· In case of any deleted user account, who deleted them and when!

System Live Analysis [Part 7]- Windows: User Account Forensics- Categorization and Profiling

Here we are with the second phase of windows user accounts live forensics to categorize the local user accounts in a windows test system and profile them into four categories as follows:

- Valid Users with Valid Groups and permissions
- Valid Users with odd groups and permissions
- Newly Created Users [Unknowns]
- Missing Users!

Note: It is essential to understand the operational needs, business logic, and standard configuration [baseline] of the targeted system and form a standard system profile to look for any deviation accordingly.

Read more on previous parts: Users, Groups, and Privileges | User Account Forensics-Road Map

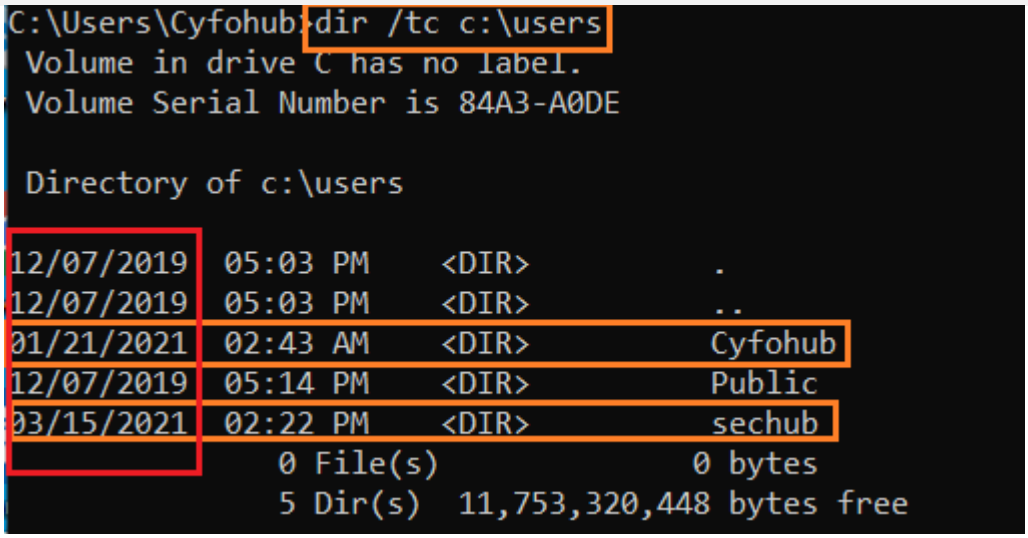
1. When users created?

One of the main steps in user account forensics is to check when the user is created and who created it! Especially for the newly created accounts where the system/network admins are not aware of them.

Check the user folders: Not really!

I came across many resources that checked the user folder creation time and considered it a fast way to determine when that user was created.

```
dir /tc c:\users
```



User Folder Creation Time

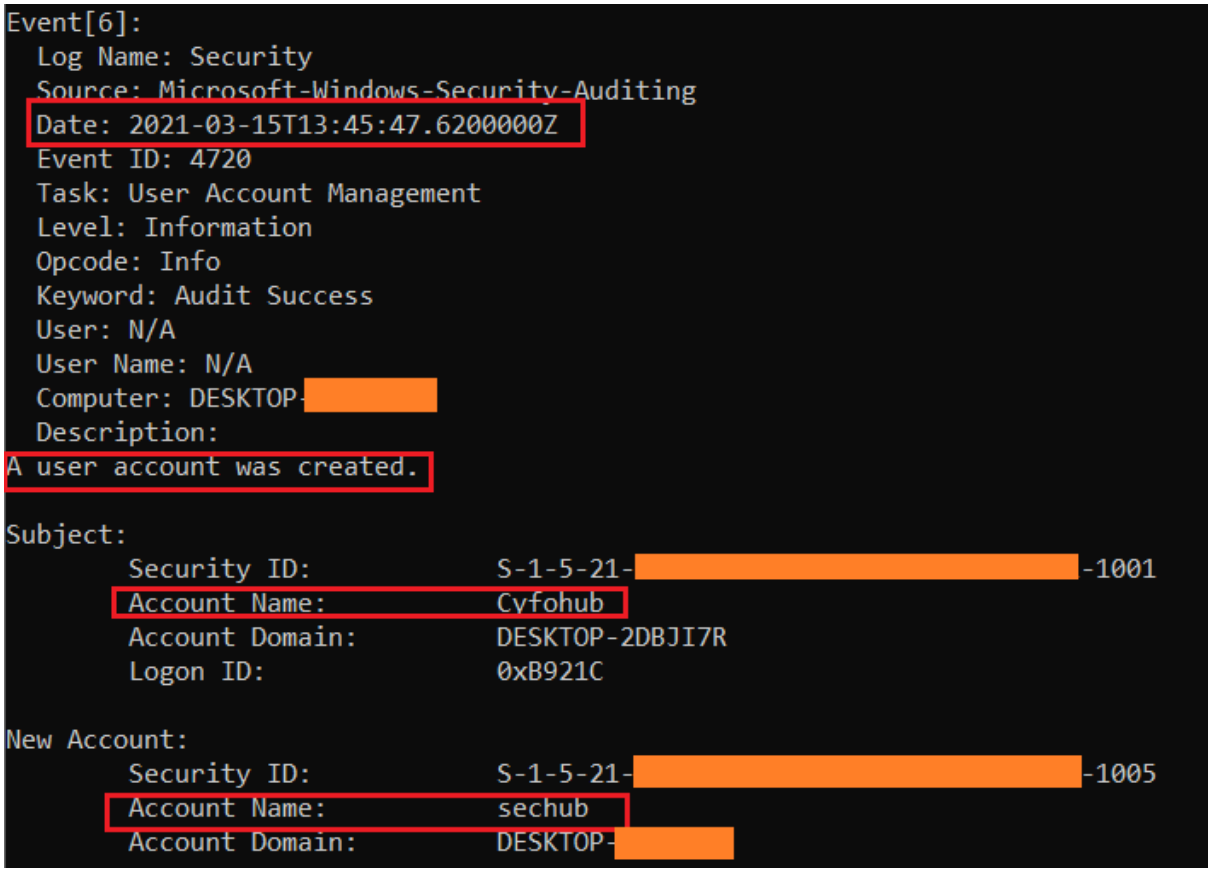
This is the user profile folder's creation time and may not represent the user's actual birthday! There is a chance that the user was created earlier than its profile folder!

Tip: *We still need the folder creation time as it gives us an idea about the time gap between user creation and the First-time Login!!*

Windows Event ID 4720

As we discussed earlier, if logs were enabled, we can use the event ID of 4720 to check when a user created and by who.

```
wevtutil qe security /f:text "/q:*[System[(EventID=4720)]]"
```

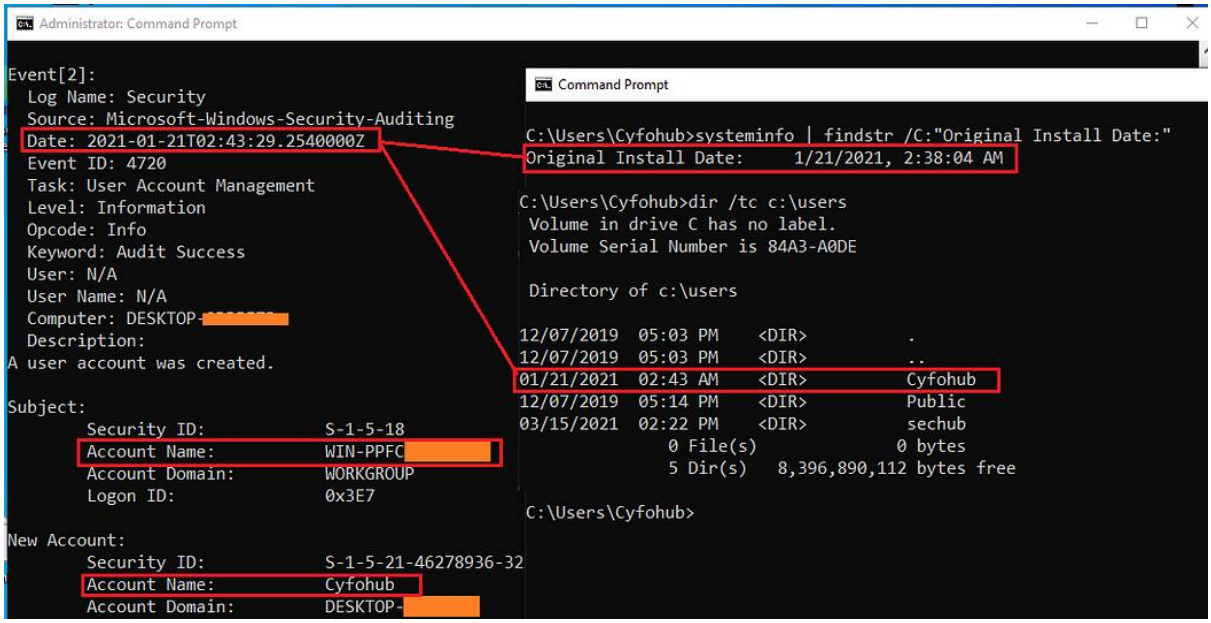


Windows Event Log for Created Users

The above result shows that the user sechub [Target Account]was created by Cyfohub [Subject] on 15 of March 2021.

Note: *As shown in the different results above, the user "sechub" was created at 13:45 while the user profile folder was created at 14:22. This is the gap between user creation and the First-time Login.*

There are other users and all created by Cyfohub, so what is the story behind this creator?!



Correlation: User and User folder Creation Time and Windows Install Date

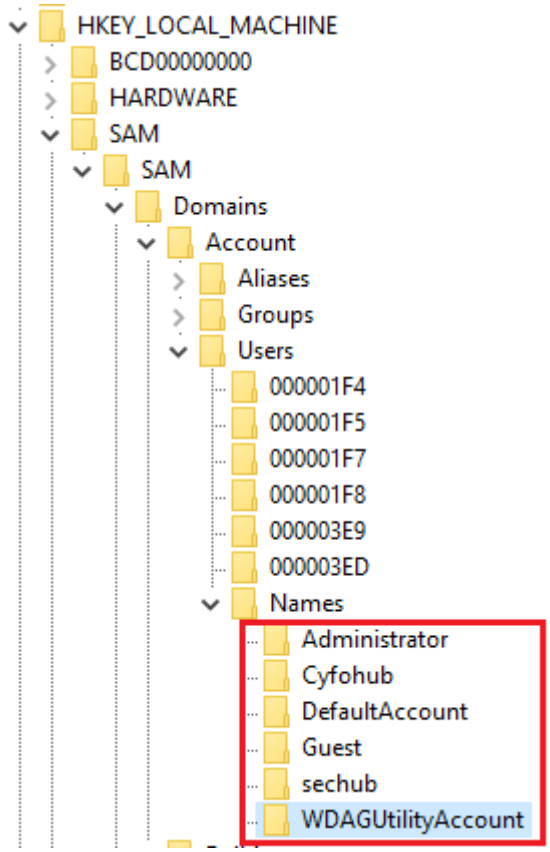
The figure above shows the correlation between the user and user profile creation time and the windows installation time. You should have guessed correctly by now! The account was created during the first installation of Windows.

Windows registry and SAM hive

The SAM hive of windows registry is another great source of data to look for user account information in case the event logs are not available. The SAM hive located at HKEY_LOCAL_MACHINE\SAM, however, it is protected by the system account and can't be viewed if the registry editor opens with the current account even if the account has admin rights.

To view the SAM hive the windows registry editor [regedit] must be opened with the system account by using tools such as PsExec.

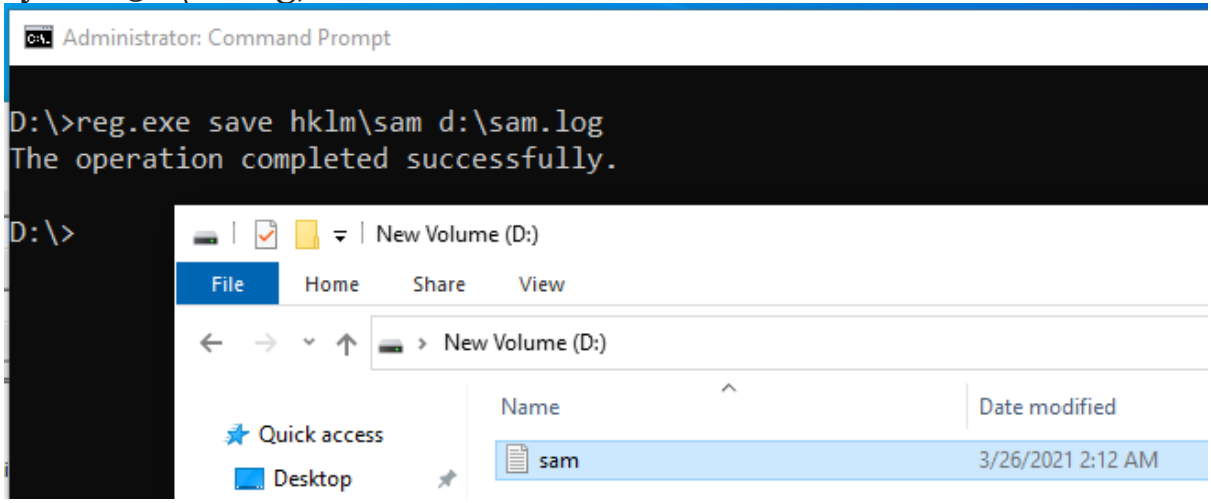
```
PsExec64.exe -s -i regedit
```



SAM Hive in Windows Registry

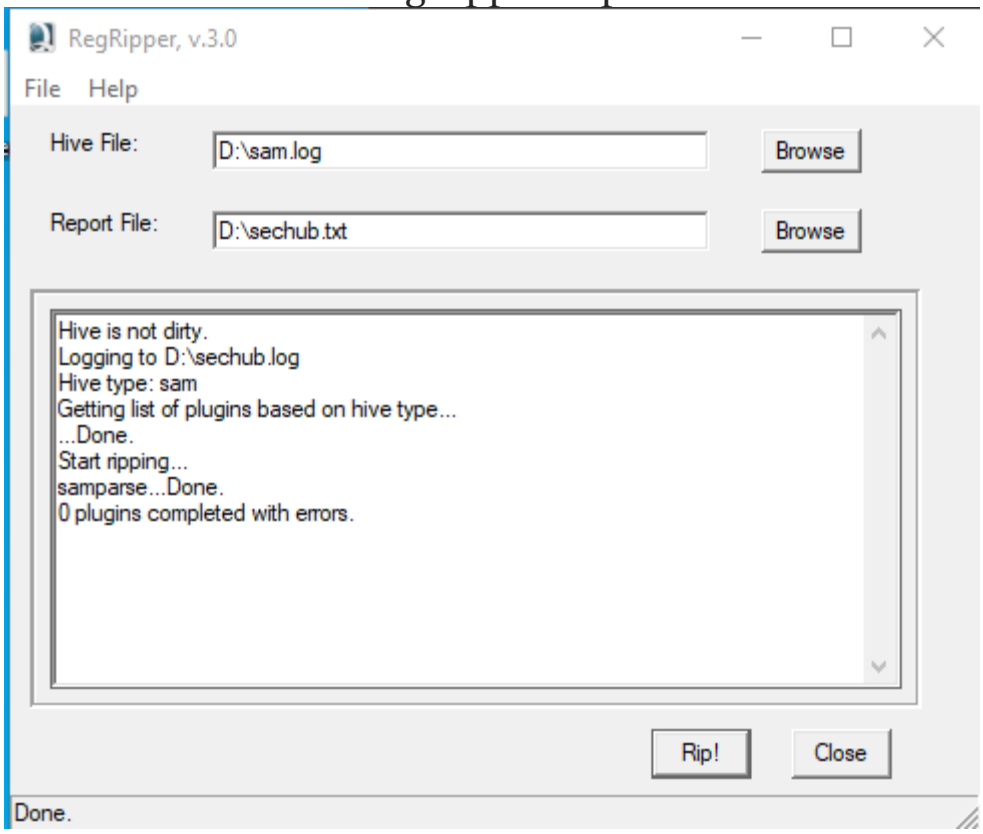
Even though we can view the list of user accounts, we need the SAM hive parser tools such as [RegRipper] to get all related information.

Note: RegRipper cant access the SAM file located in system32\config, thus we need to save the hive into a file as follows:



Exporting SAM Hive

Now we can use the RegRipper to parse the SAM hive.



The RegRipper

The result will be saved into the text file we defined as a Report File:

```
Username        : sechub [1005]
Full Name       :
User Comment    :
Account Type    :
Account Created : 2021-03-15 05:45:47Z
Name            :
Last Login Date : 2021-03-15 06:22:54Z
Pwd Reset Date  : 2021-03-15 05:45:47Z
Pwd Fail Date   : Never
Login Count     : 1
Embedded RID    : 1005
  --> Normal user account

--------------------------
Group Membership Information
--------------------------
Group Name    : Event Log Readers [0]
LastWrite     : 2021-01-21 10:35:30Z
Group Comment : Members of this group can read event logs from local machine
Users         : None
```

User Creation Time from SAM Hive

2. When a user assigned to a group?

A simple net user command shows the sechub is part of the local admin group.

```
C:\Windows\system32>net user sechub | findstr "Group"
Local Group Memberships      *Administrators
Global Group memberships     *None
```

A User Account Group

Event ID 4732: A member was added to a security-enabled local group

```
CMD:
wevtutil qe security /f:text "/q:*[System[(EventID=4732)]]"
```

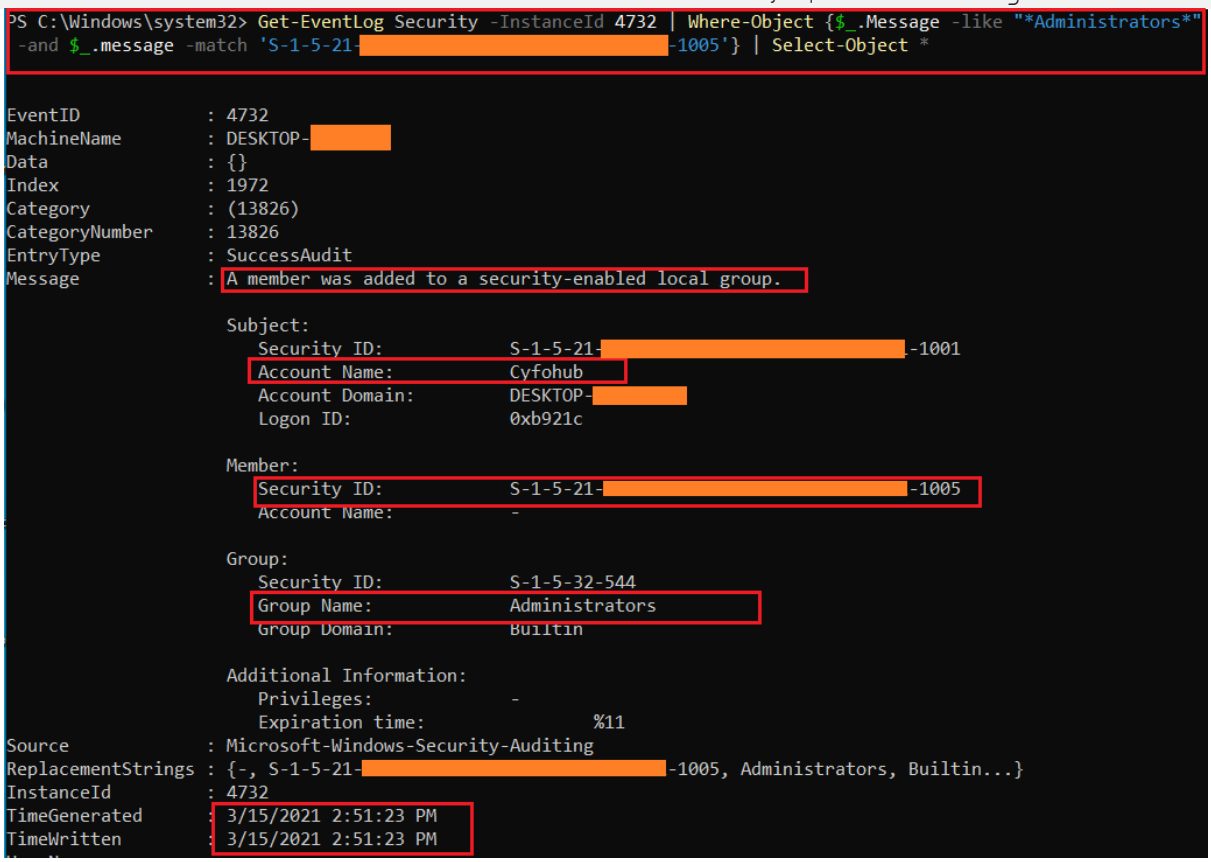
```
Event[11]:
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2021-03-15T14:51:23.2750000Z
  Event ID: 4732
  Task: Security Group Management
  Level: Information
  Opcode: Info
  Keyword: Audit Success
  User: N/A
  User Name: N/A
  Computer: DESKTOP-[redacted]
  Description:
A member was added to a security-enabled local group.

Subject:
        Security ID:            S-1-5-21-[redacted]-1001
        Account Domain:         DESKTOP-[redacted]
        Logon ID:               0xB921C

Member:
        Security ID:            S-1-5-21-[redacted]-1005
        Account Name:           -

Group:
        Security ID:            S-1-5-32-544
        Group Name:             Administrators
        Group Domain:           Builtin

Additional Information:
        Privileges:             -
```

Windows Event for User Account that has been added to a Group

The wevtutil command displays all the events with the ID of 4732 regardless of the group name.

Powershell helps us to display results for a particular group or user account. For instance, the command below shows the events with the ID of 4732 associated with the local administrator and sechub user accounts only[based on SID].

```
Powershell:
Get-EventLog Security -InstanceId 4732 | Where-Object
{$_.Message -like "*Administrators*" -and $_.message -match 'S-
1-5-21-xxxxxxxx-xxxxxxxxx-xxxxxxxxx-1005'} | Select-Object *
```



Powershell Command to obtain information for a specific user.

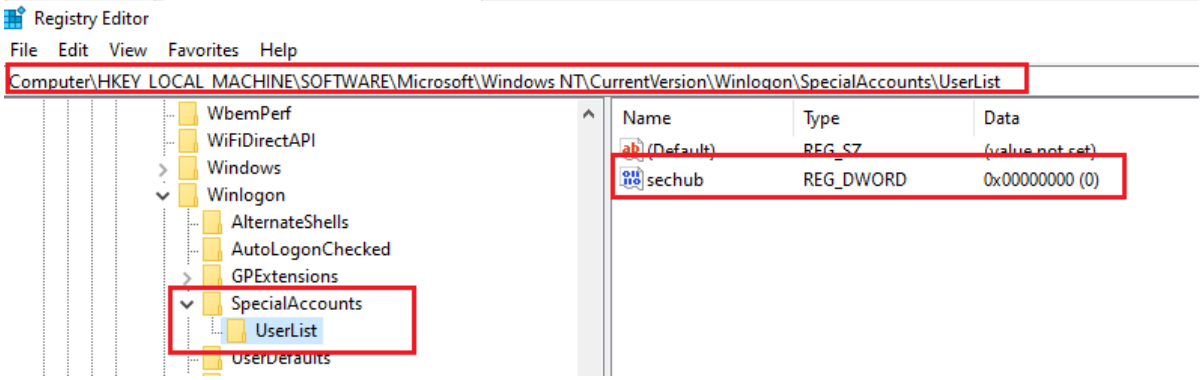
The sechub account was added to the admin group by Cyfohub on 15 MARCH 2021. The above commands can be used to obtain

information about event ID 4733 to check if a user account was removed from a security-enabled local group.

3. Is there any hidden user?

A hacker who gained initial access to our system may create a user account to maintain access and hide it from the Windows login screen! There are many ways to hide a user account, and one is via the Windows registry.

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /t REG_DWORD /f /d 0 /v sechub
```



Hiding Users via Registry

Reg Query

Reg query assists to obtain the list of users from the above location if there is any :

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList"
```

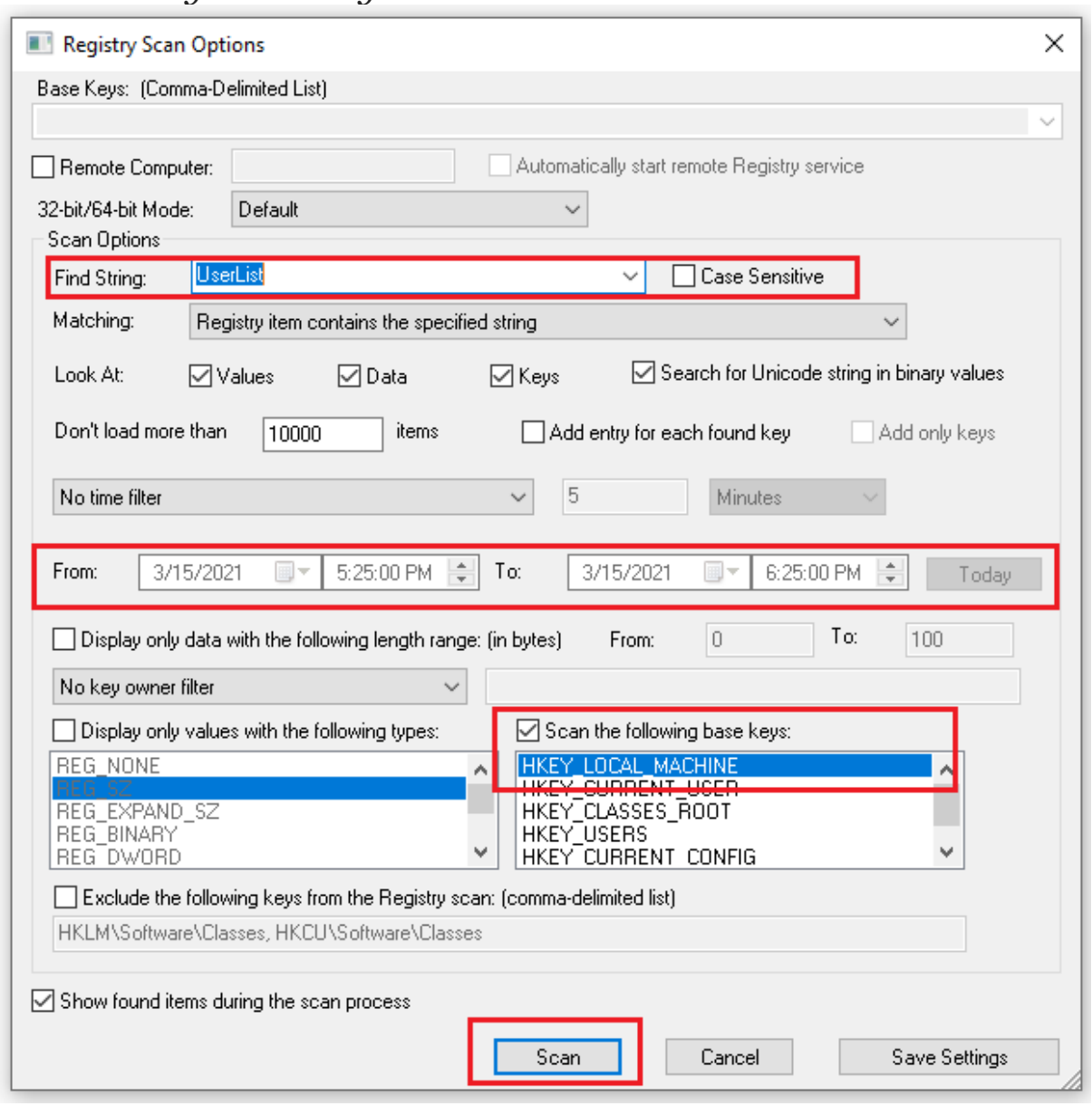
```
C:\Windows\system32>reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList
    sechub    REG_DWORD    0x0
```

A hidden User in Registry

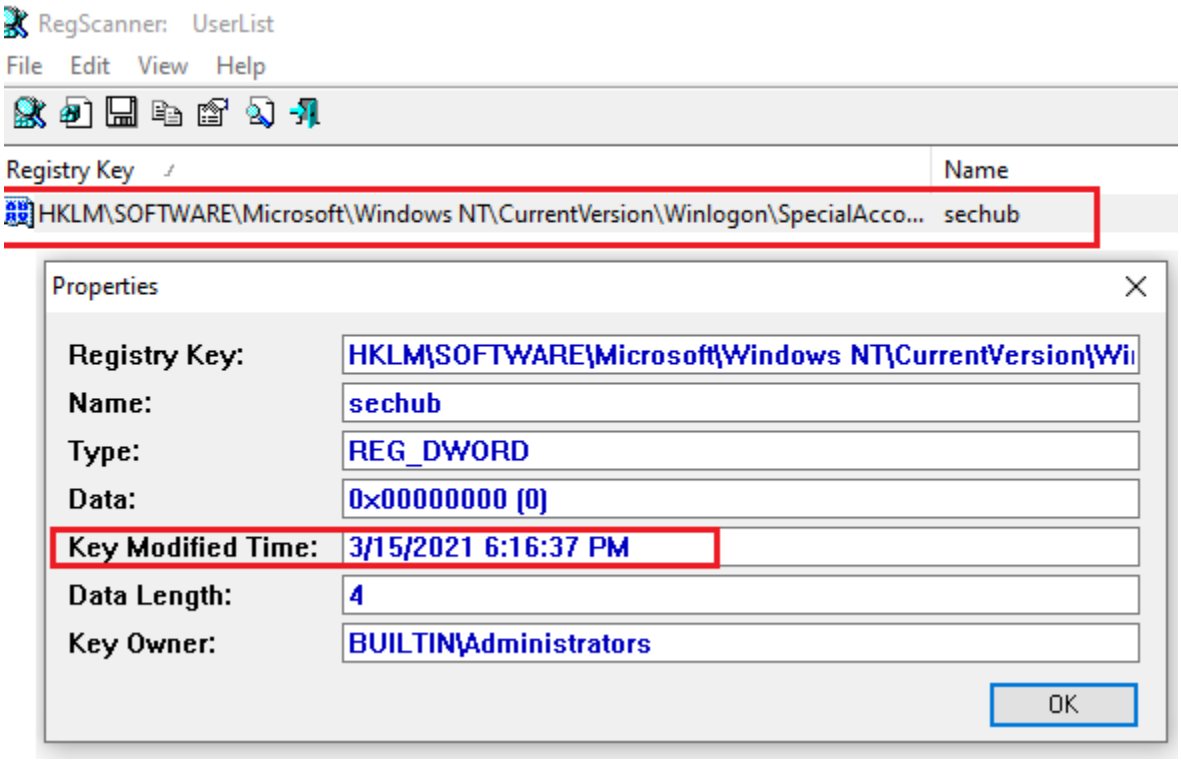
RegScanner

The RegScanner developed by Nirsoft is a GUI-based to receive information for Windows Registry.

Note: *Do not copy any tool to the target systems; save all things you need on a forensically clean external storage and connect it to the victim system using write blockers.*



RegScanner Scan Settings



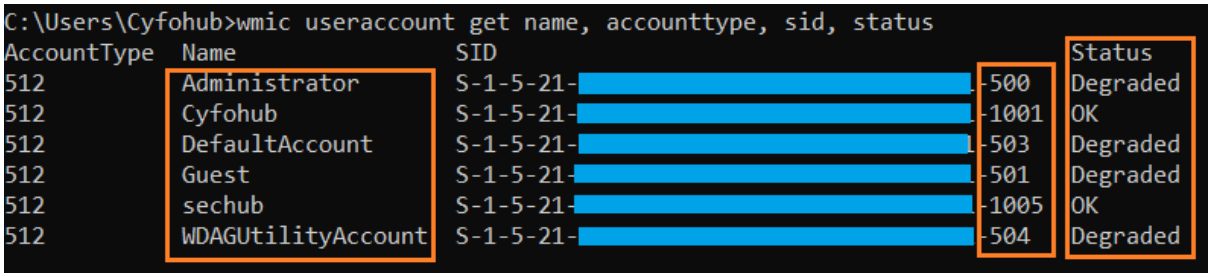
RegScanner Scan Results

Note 1: *The time shown by the above command and tool is the last time that registry key was updated [last-modified timestamp] or modified as the registry doesn't keep a record of creation time.*

Note 2: *We cannot determine which user account made changes or modifications unless we use object access auditing to audit registry changes.*

4. When a user Deleted?

We are mainly thinking of how hackers may misuse valid user accounts; however, they may also delete, disable or limit the account to interrupt legitimate accesses. Let's look at the user accounts list again and focus on RIDs range 1XXX.



User Account on Test System

Why are the RIDs 1001 and 1005? What happened to 1000? How about 1002, 1003, and 1004? it's an excellent question!

Fact 1: RID is given to user accounts at creation.

Fact 2: Any time a user is created, the RID increased by one.

Considering the facts above, we can say there were few user accounts deleted from that system. What are those deleted users? Event ID 4726 indicates a user accounts deletion.

```
wevtutil qe security /f:text "/q:*[System[(EventID=4726)]]"
```

```
Event[1]:
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2021-03-15T13:45:56.6000000Z
  Event ID: 4726
  Task: User Account Management
  Level: Information
  Opcode: Info
  Keyword: Audit Success
  User: N/A
  User Name: N/A
  Computer: DESKTOP-[redacted]
  Description:
A user account was deleted.

Subject:
        Security ID:            S-1-5-21-[redacted]-1001
        Account Name:           Cyfohub
        Account Domain:         DESKTOP-[redacted]
        Logon ID:               0xB921C

Target Account:
        Security ID:            S-1-5-21-[redacted]-1002
        Account Name:           meisam
        Account Domain:         DESKTOP-[redacted]

Additional Information:
        Privileges      -
```

Windows Event for Deleted Users

The above result shows that the user Meisam [Target Account]was deleted by Cyfohub [Subject] on 15 of March 2021. There are other deleted accounts as follows:

```
Powershell:
wevtutil qe security /f:text "/q:*[System[(EventID=4726)]]" |
Select-String -Pattern 'Target Account' -Context 0,2
```

```
PS C:\Windows\system32> wevtutil qe security /f:text "/q:*[System[(EventID=4726)]]" | Select-String -Pattern 'Target Account' -Context 0,2

> Target Account:
        Security ID:            S-1-5-21-[redacted]-1000
        Account Name:           defaultuser0
> Target Account:
        Security ID:            S-1-5-21-[redacted]-1002
        Account Name:           meisam
> Target Account:
        Security ID:            S-1-5-21-[redacted]-1003
        Account Name:           admin
> Target Account:
        Security ID:            S-1-5-21-[redacted]-1004
        Account Name:           user
```

All Deleted Users on Test System

Four user accounts were deleted from our test system, as shown in the results above; however, we may only need to focus on 3 of them! Why!

Tip: Defaultuser0 is a default account used by windows during installation and up before any other user accounts have been created on the system. It will be deleted right after the first reboot during the installation.

5. Summary of Fininindg

The table below summarises all findings regarding the existing and deleted accounts [It's just a template as a sample, and you can make it based on your style].

User Accounts	*Type*	*RID*	*Status*	*Description*
Administrator	512	500	Degraded	As a common practice, all of these accounts are disabled for better security.
DefaultAccount		503	Degraded	
Guest		501	Degraded	
WDAGUtilityAccount		504	Degraded	
Cyfohub		1001	Active	The account was created during the first installation.
sechub		1005	Active / Hidden	- The account created by Cyfohub on [Date and Time] - The account added to local admin groups by Cyfohub on [Date and Time] - The account hides from the Windows login screen on [Date and Time] ***Note: It's not possible to tell who hides the account as registry audit was not enabled.***
Defaultuser0		1000	Deleted	Default account used by windows during installation
meisam		1002	Deleted	- The account created by XXXX on [Date and Time] - The account deleted by XXXX on [Date and Time]
admin		1003	Deleted	- The account created by XXXX on [Date and Time] - The account deleted by XXXX on [Date and Time]
user		1004	Deleted	- The account created by XXXX on [Date and Time] - The account deleted by XXXX on [Date and Time]

User Account Profiling Sample

For the above example, we need more verification and further investigation on red categories as they are tagged as suspicious. However, it's not the end of the story? Why!

Cybercriminals may misuse valid accounts like Cyfohub to carry out malicious activities; even though creation and privileges are normal, we need to look for other related information to look for potential attacks!

6. What's Next!

- Users' Logon Sessions
- Owned App and Services
- Owned Processes and Files
- Profiles and Searches
- Environment Variables
- Program Execution History

System Live Analysis [Part 8]- Windows: User Account Forensics- Profile Folder, AppData, and Environment Variables

The deep-dive analysis phase focuses on detailed analysis of user settings and behaviours to obtain information about:

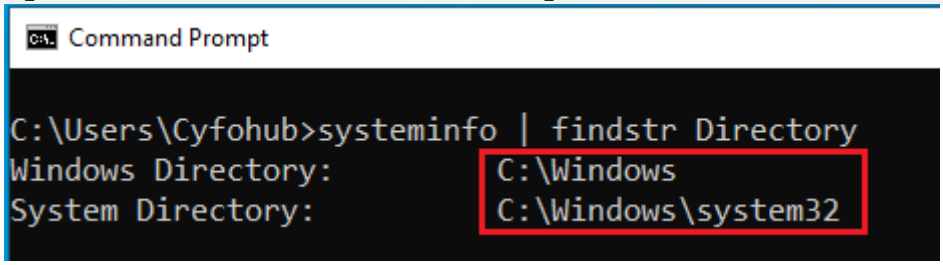
User Account Forensics — Deep-Dive Analysis

This part discusses the Profile Folder, AppData, and Environment Variables for each user account.

1. Users Profile Location

As discussed earlier, windows create a user profile folder for each user account upon the First-time Login. The folders are located in C:\users. The “C:\” here refers to the OS installation drive [%SystemDrive%].

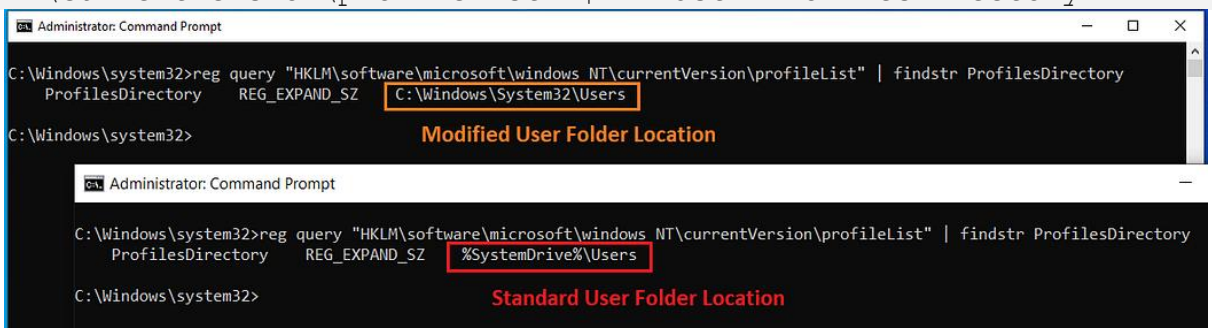
```
systeminfo | findstr Directory
```



Windows Installation Directories

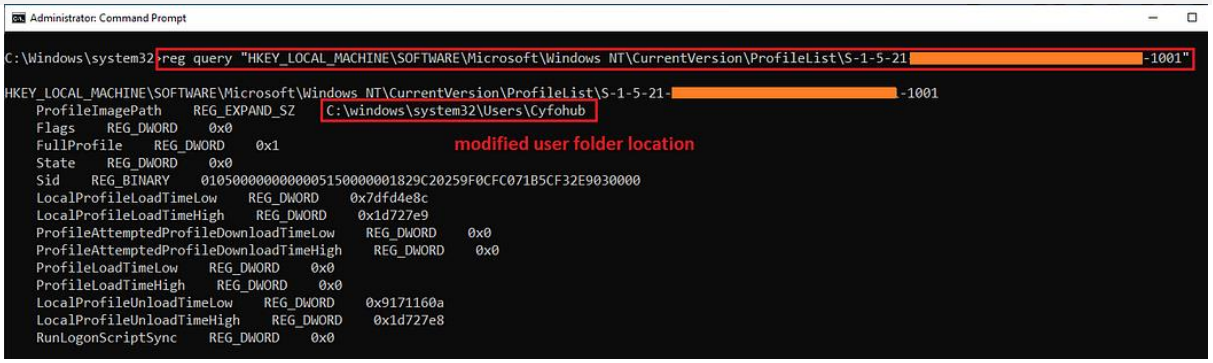
We can’t rely on the above technique alone as there may be a chance that users folder location changed to another drive or folder. Thus, we should always validate the correct location.

```
reg query “HKLM\software\microsoft\windows NT\currentVersion\profileList” | findstr ProfilesDirectory
```



Users Folder Location — Standard and Modified Examples

```
reg query "HKLM\software\microsoft\windows NT\currentVersion\profileList\S-1-5-21-xxxxxxxxx-xxxxxxxxxx-xxxxxxxxx-1001"
```

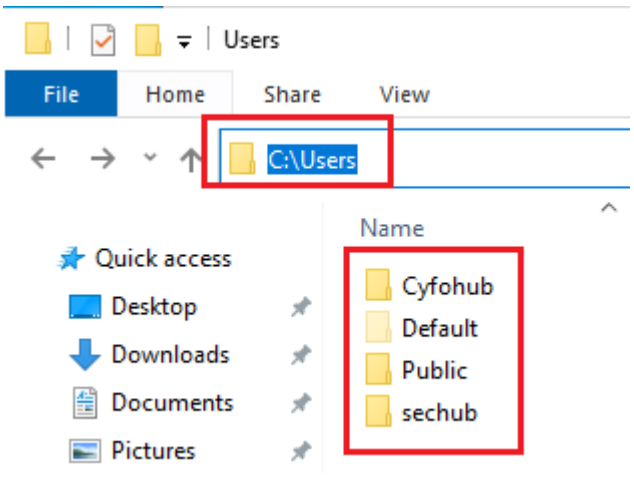


Cyfohub User Folder in Odd Location

The example above shows a User Folder with an odd location [i.e. System32 folder] instead of the default location, which is %SystemDrive%\Users.

2. Users Profile Subfolders

There are different types of subfolders in the User Folder regardless of its location as follows:

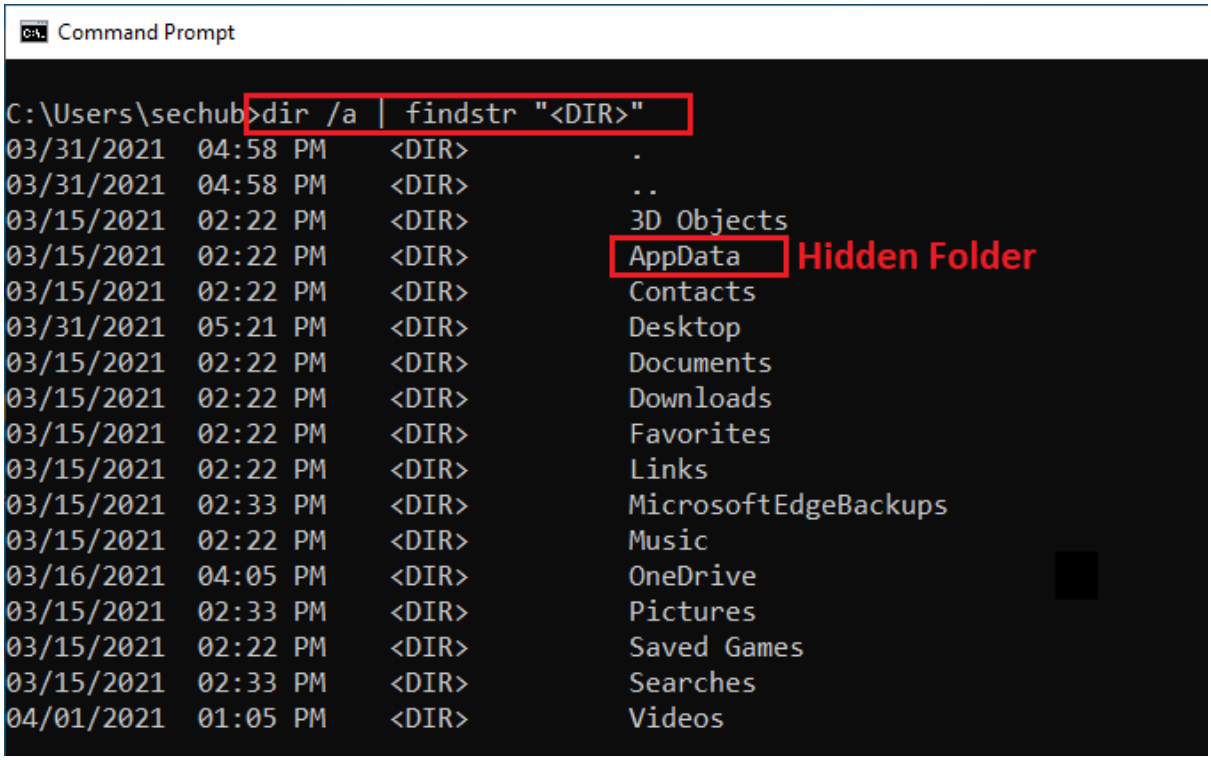


Users Folder

- **Default:** This is a hidden folder used by Windows as a generic template for the user accounts folder. When a new user account is created, Windows build the associated subfolder based on this default template.
- **Public:** As the name suggests, all user accounts can access this folder to share files on the same machine.
- **User Account Folders [e.g. Cyfohub, and Sechub]:** These are the user-specific folders that Windows create for each user account upon the first-time login.

Each user profile folder [e.g. sechub] contains numbers of subfolders as follows:

```
dir /a | findstr "<DIR>"
```



Sechub User Subfolders

The folder names suggest their forensics values, such as Desktop, Downloads, Favorites, Music, etc. The content of each folder may help forensics analysts to understand each user's behaviour.

Note: *We may also found application-related folders created by an application installed on the system under specific user accounts.*

For instance, the Nmap is installed on the target system under the Cyfhub user. Once the Zenmap runs for the first time, it creates a folder in the Cyfohub user folder.

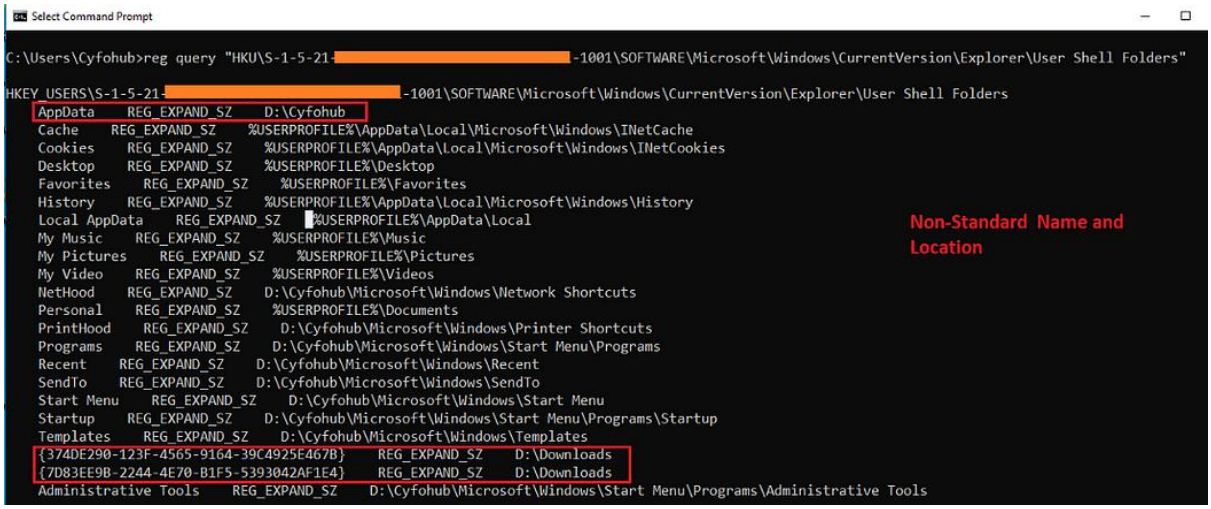
```
Command Prompt

C:\Users\Cyfohub>dir  /tc /a | findstr "<DIR>"
01/21/2021  02:43 AM    <DIR>          .
01/21/2021  02:43 AM    <DIR>          ..
04/03/2021  01:26 PM    <DIR>          .zenmap
01/21/2021  02:44 AM    <DIR>          3D Objects
01/21/2021  02:43 AM    <DIR>          AppData
01/21/2021  02:44 AM    <DIR>          Contacts
01/21/2021  02:43 AM    <DIR>          Desktop
01/21/2021  02:43 AM    <DIR>          Documents
01/21/2021  02:43 AM    <DIR>          Downloads
01/21/2021  02:43 AM    <DIR>          Favorites
01/21/2021  02:43 AM    <DIR>          Links
01/21/2021  02:46 AM    <DIR>          MicrosoftEdgeBackups
01/21/2021  02:43 AM    <DIR>          Music
01/21/2021  02:46 AM    <DIR>          OneDrive
01/21/2021  02:43 AM    <DIR>          Pictures
01/21/2021  02:43 AM    <DIR>          Saved Games
01/21/2021  02:44 AM    <DIR>          Searches
01/21/2021  02:43 AM    <DIR>          Videos
```

The above folder names and their location [%USERPROFILE%] are standards modified by users. Thus, we should validate them.

```
reg query "HKU\S-1-5-21-xxxxxxxx-xxxxxxxxxx-xxxxxxxxx-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"
```

```
Command Prompt

C:\Users\Cyfohub>reg query "HKU\S-1-5-21-[redacted]-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"

HKEY_USERS\S-1-5-21-[redacted]-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
    AppData    REG_EXPAND_SZ    %USERPROFILE%\AppData\Roaming
    Cache      REG_EXPAND_SZ    %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache
    Cookies    REG_EXPAND_SZ    %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies
    Desktop    REG_EXPAND_SZ    %USERPROFILE%\Desktop
    Favorites  REG_EXPAND_SZ    %USERPROFILE%\Favorites
    History    REG_EXPAND_SZ    %USERPROFILE%\AppData\Local\Microsoft\Windows\History
    Local AppData    REG_EXPAND_SZ    %USERPROFILE%\AppData\Local
    My Music   REG_EXPAND_SZ    %USERPROFILE%\Music
    My Pictures    REG_EXPAND_SZ    %USERPROFILE%\Pictures
    My Video   REG_EXPAND_SZ    %USERPROFILE%\Videos
    NetHood    REG_EXPAND_SZ    %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Network Shortcuts
    Personal   REG_EXPAND_SZ    %USERPROFILE%\Documents
    PrintHood  REG_EXPAND_SZ    %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
    Programs   REG_EXPAND_SZ    %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
    Recent     REG_EXPAND_SZ    %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent
    SendTo     REG_EXPAND_SZ    %USERPROFILE%\AppData\Roaming\Microsoft\Windows\SendTo
    Start Menu     REG_EXPAND_SZ    %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu
    Startup    REG_EXPAND_SZ    %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
    Templates  REG_EXPAND_SZ    %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Templates
    {374DE290-123F-4565-9164-39C4925E467B}    REG_EXPAND_SZ    %USERPROFILE%\Downloads

Standard Folder Name and Location
```

Standard Folder Name and Location for a User Account

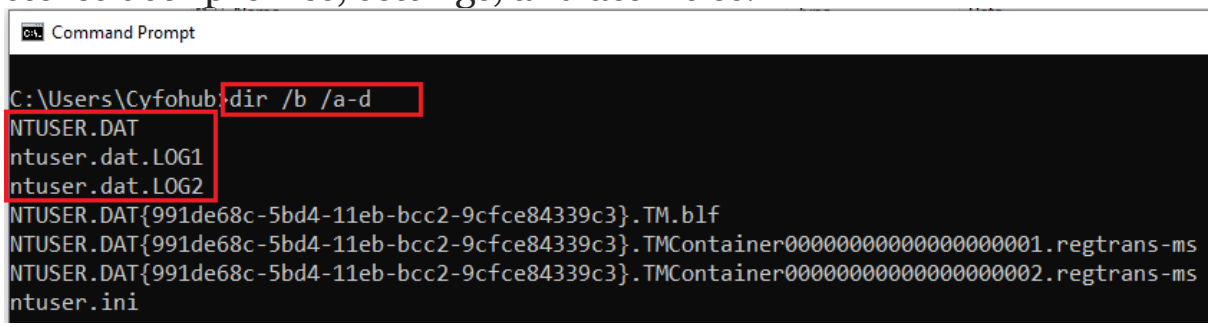


Non-Standard Name and Location for a User Account

As shown in the figure above, the Downloads folder for the Cyfohub user account moved to drive D. The AppData Roaming folder moved to drive D, and its name changed to Cyfohub.

3. NTUSER.DAT

The **NTUSER.DAT** is the main registry hive for the users residing in the user account profile folder and contains the most valuable forensics data. Each user accounts has its NTUSER.DAT file that stores user profiles, settings, and activities.



NTUSER.DAT Location

Windows keep a backup of all the activities and changes such as accessing folders, opening files, network shares, etc., in

the transaction logs called netuser.dat.LOG1 and netuser.dat.LOG2 during the live session and saves them into NTUSER.DAT during Log off.

Note: To have the most updated version of NTUSER.DAT, we should also have the transaction logs 1 and 2.

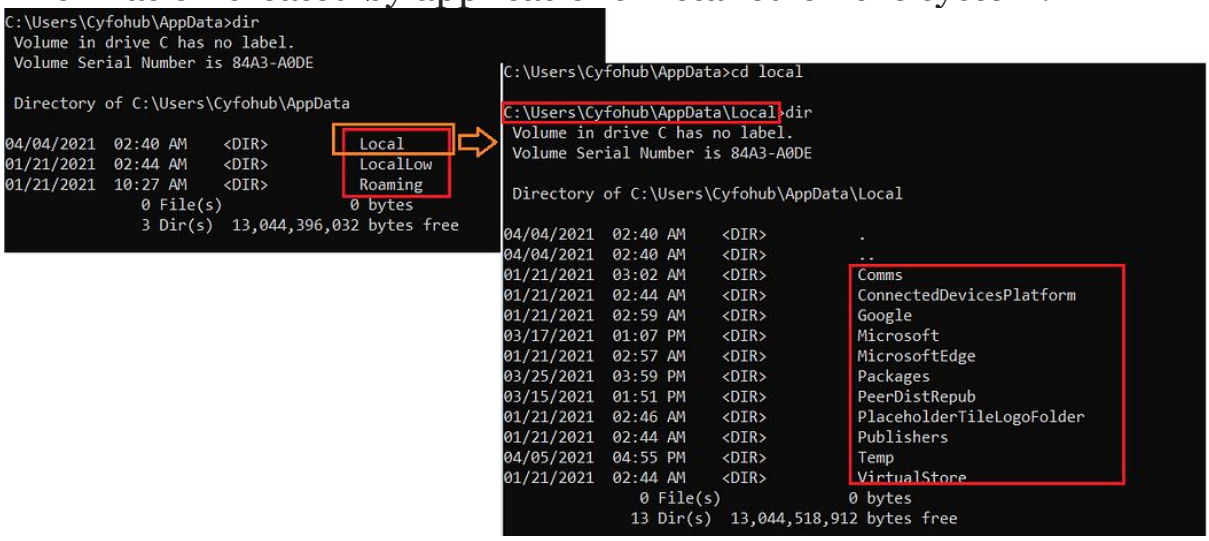
The file and associated logs provide us with fantastic information with high forensics values as follows:

- Executed programs and applications
- Recently opened directories, files, applications, and documents
- Files executed with Run command and startup programs
- Typed paths in Windows Explorer and User search history in the search bar
- Internet Settings and typed URLs in Internet Explorer
- File extensions, Desktop contents, ShellBags, and Connected printers

Note: *We cannot use standard copy and paste methods to copy the NTUSER.DAT, LOG1, and LOG2 for the logged-in user during the live investigation as the files are in active use and protected. The forensics tools such as FTK Imager will help to make a copy. We will discuss this in the following posts.*

4. AppData Folder

One of the most exciting data sources for windows forensics is AppData [Hidden] Folder containing custom settings files and other information created by applications installed on the system.



AppData Local Subfolder

The data in Local and LocalLow subfolders are under Windows user profile only and cannot be synced to move them to another computer in a domain environment.

On the other hand, the Roaming subfolder data can be synced to a server and move with our user profile from a computer to another.

- **UsrClass.dat:** · Just Like NTUSER.DAT, the UsrClass is another registry hive to obtained user-related information. This file is located at AppData Local Microsoft Windows, and we need the FTK Imager to copy it during live analysis.

5. Environment Variables

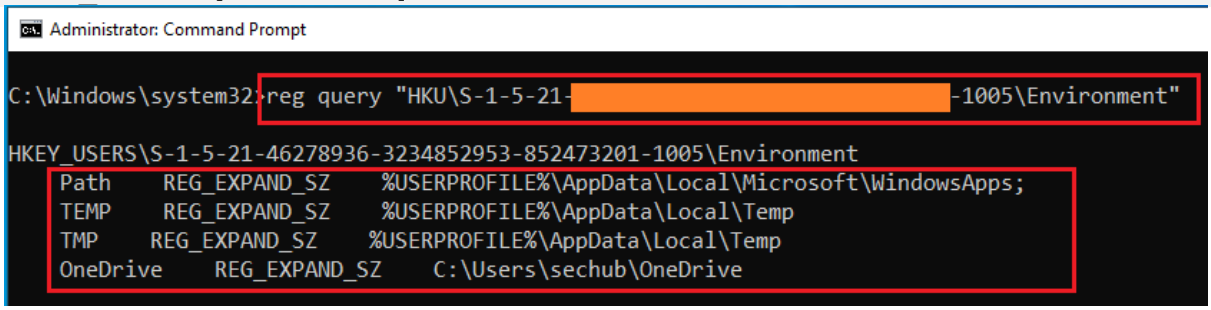
Environment variables are stored information such as search paths for files, directories for temporary files, application-specific options, etc., that tells us about the environment used by each user.

Part 4 of the system live analysis series explained how to retrieve environment variables for the system and current user by SET command and Regquery as follows:

```
System:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
User:
HKEY_CURRENT_USER\Environment
```

To check the environment variables for other user accounts, we can use reg query too; however, we need to obtain the information from another location as follows:

```
HKEY_USERS\[USER SID ]\Environment
```



Environment Variables for Sechub

Using the above technique, I obtained the sechub user account's environment variables while logged in with the Cyfohub user account.

System Live Analysis [Part 9]- Windows: User Account Forensics- Ownership: Process, Applications, Folders, and Files

So far, we have discussed user account creation, deletion, privileges, and associated folders and settings such as users profile and AppData folders, and user-specific environment variables.

The above information is essential for an investigator to identify the existing and deleted user accounts. However, these data may not be sufficient to tag a user account as malicious or benign.

For instance, a legitimate user account with valid groups and permissions may look normal by analyzing the above information. However, there are many WHAT IFs that can change the story! What if the user…

- Runs an odd process
- Owns malicious files
- Has access to a restricted folder
- Installed unsolicited or malicious application

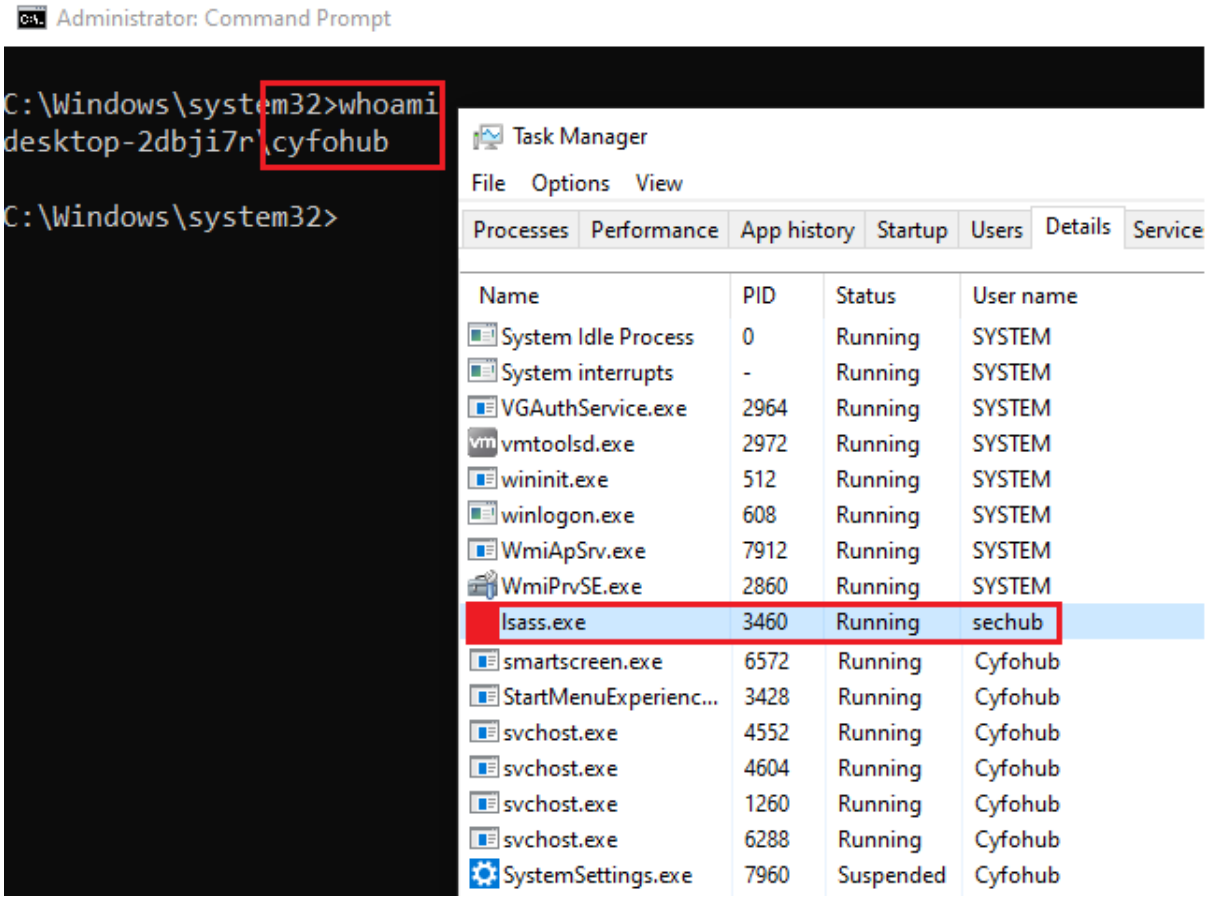
This post discusses the ownership of running processes, installed applications, folders, and files to address the above issues.

1- Running Processes

Windows programs [executables] run as one or more processes and tasks. The complete analysis of running processes will be explained in upcoming posts. This section covers the techniques to obtain the name of user accounts running a process on the Windows operating system.

Task Manager

The details Tab in task manager shows the name of running processes in addition to the user accounts name that running that processes, as shown in the figure below:



Users that Run a Process — Task Manager

- The currently logged-in user is Cyfohub; however, a process named lsass.exe is running by the sechub user account!
- According to the Windows standard baseline for processes, the lsass.exe user name is supposed to be NT AUTHORITY\SYSTEM, not any other local user account.

Note: *We will have a dedicated post for Windows process investigation.*

Tasklist:

The tasklist is a built-in Windows command to display the running processes.

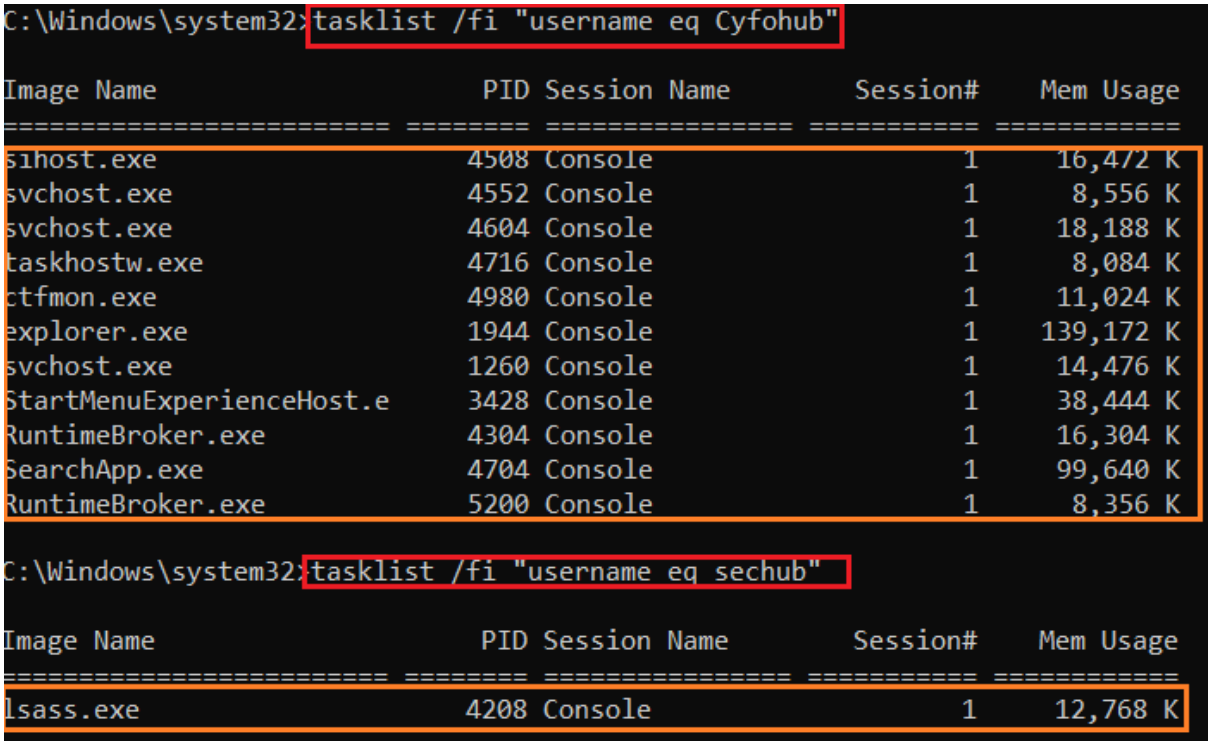
```
Tasklist /v
```

```
C:\Windows\system32>Tasklist /v

Image Name                     PID Session Name        Session#    Mem Usage Status          User Name
========================= ======== ================ =========== ============ =============== ==============================================
System Idle Process              0 Services                   0          8 K Unknown         NT AUTHORITY\SYSTEM
System                           4 Services                   0         24 K Unknown         N/A
Registry                        92 Services                   0     22,476 K Unknown         NT AUTHORITY\SYSTEM
smss.exe                       316 Services                   0        300 K Unknown         NT AUTHORITY\SYSTEM
csrss.exe                      436 Services                   0      1,416 K Unknown         NT AUTHORITY\SYSTEM
wininit.exe                    512 Services                   0        980 K Unknown         NT AUTHORITY\SYSTEM
csrss.exe                      524 Console                    1      1,904 K Running         NT AUTHORITY\SYSTEM
conhost.exe                   8124 Console                    1     17,904 K Running         DESKTOP-2DBJI7R\Cyfohub
Taskmgr.exe                   3920 Console                    1     32,216 K Running         DESKTOP-2DBJI7R\Cyfohub
ShellExperienceHost.exe       2368 Console                    1     11,724 K Running         DESKTOP-2DBJI7R\Cyfohub
RuntimeBroker.exe             4576 Console                    1      2,648 K Running         DESKTOP-2DBJI7R\Cyfohub
svchost.exe                   4572 Services                   0      5,076 K Unknown         NT AUTHORITY\LOCAL SERVICE
svchost.exe                   6648 Services                   0     10,076 K Unknown         NT AUTHORITY\SYSTEM
svchost.exe                   5400 Services                   0      2,940 K Unknown         NT AUTHORITY\SYSTEM
svchost.exe                   1200 Services                   0      7,060 K Unknown         NT AUTHORITY\SYSTEM
RuntimeBroker.exe             4792 Console                    1     22,812 K Unknown         DESKTOP-2DBJI7R\Cyfohub
```

Users that Run a Process — Tasklist

The Tasklist command allows us to list all the processes runs by a specific user account.

```
tasklist /fi "username eq Cyfohub"
```

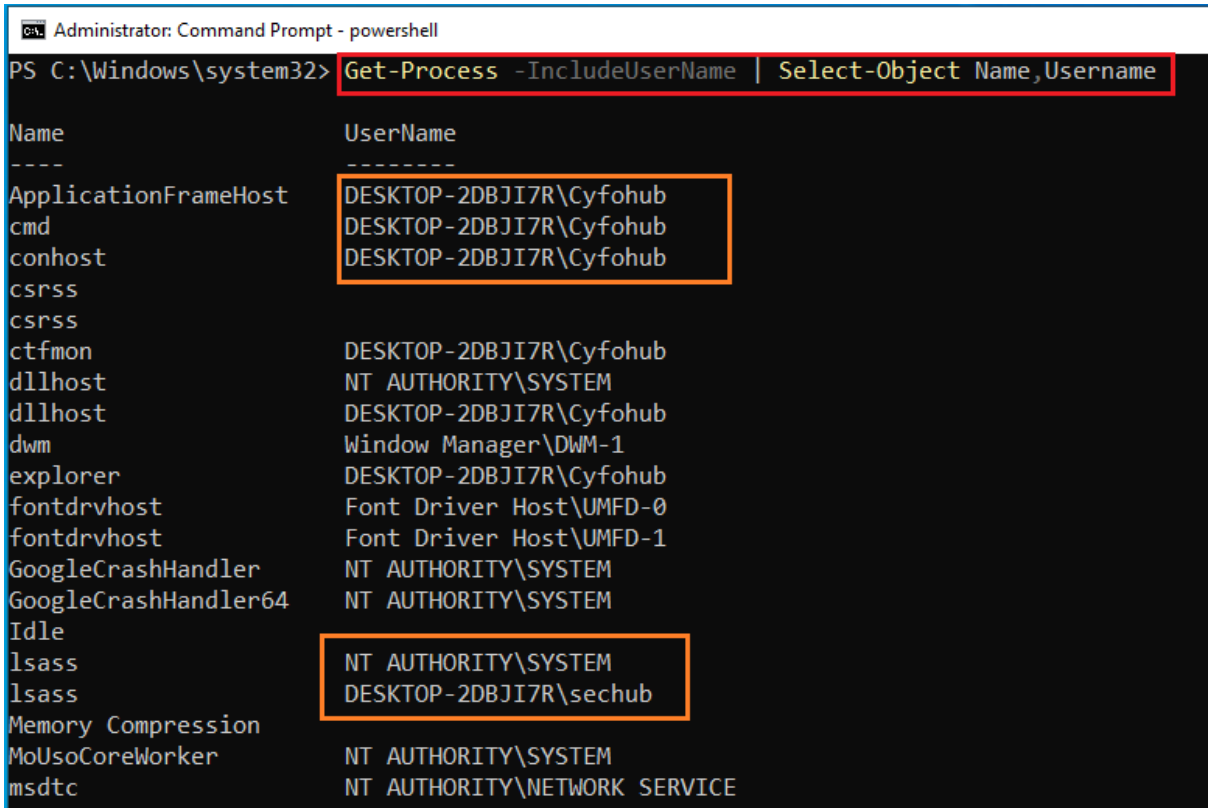


List of Processes Running by Specific User Accounts — Tasklist

Powershell:

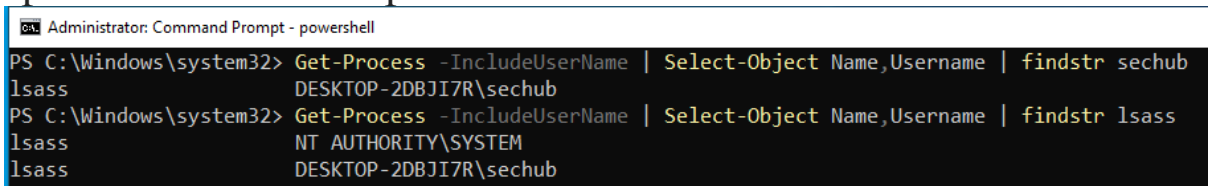
Using powershell, we can obtain the list of running processes' name, domain, and user name as follows:

```
Get-Process -IncludeUserName | Select-Object Name,Username
```



Users that Run a Process — Powershell

The above PowerShell command can be combined with findstr to list specific user name or processes as follows:



List of Processes Running by Specific User Accounts — Powershell

When it comes to installed applications and user accounts, the system investigators must look at it from two perspectives as follows:

- Who installed it? — Which user account installed that application.

- Installed for Who? — To check whether the application is installed for a specific user or all.

Let's answer the first question first. Who installed the application?

2- Installed Applications — Who Installed them?

To install any application in a Windows environment, we use two common installers such as Windows Installer (MSI) and EXE [e.g., setup.exe]. It's highly recommended to learn the differences between these installers.

MSI Installer:

In general, Windows logs few events [event ID 11707 and 1033] related to install/uninstall of applications if they use Windows Installer (MSI).

Event Logging (Windows Installer) - Win32 apps
Windows Events provides a standard, centralized way for applications (and the operating system) to record importanté
docs.microsoft.com

Limitation: The above events only log the applications installed by Windows Installer (MSI) and do not record any information related to any other type of installers such as .exe files.

Let's check the event ID of 11707 from Application Event Log to check the successful installation of an application.

```
wevtutil qe application /f:text "/q:*[System[(EventID=11707)]]"
```

```
Event[7]:
  Log Name: Application
  Source: MsiInstaller
  Date: 2021-04-20T17:18:31.8510000Z
  Event ID: 11707
  Task: N/A
  Level: Information
  Opcode: Info
  Keyword: Classic
  User: S-1-5-21-[redacted]-1005
  User Name: DESKTOP-2DBJI7R\sechub
  Computer: DESKTOP-2DBJI7R
  Description:
Product: Autopsy -- Installation completed successfully.
```

Successful Installation of Autopsy Application — Event ID 11707

The event ID of 1033 provides us with more details on installed product descriptions.

```
wevtutil qe application /f:text "/q:*[System[(EventID=1033)]]"
```

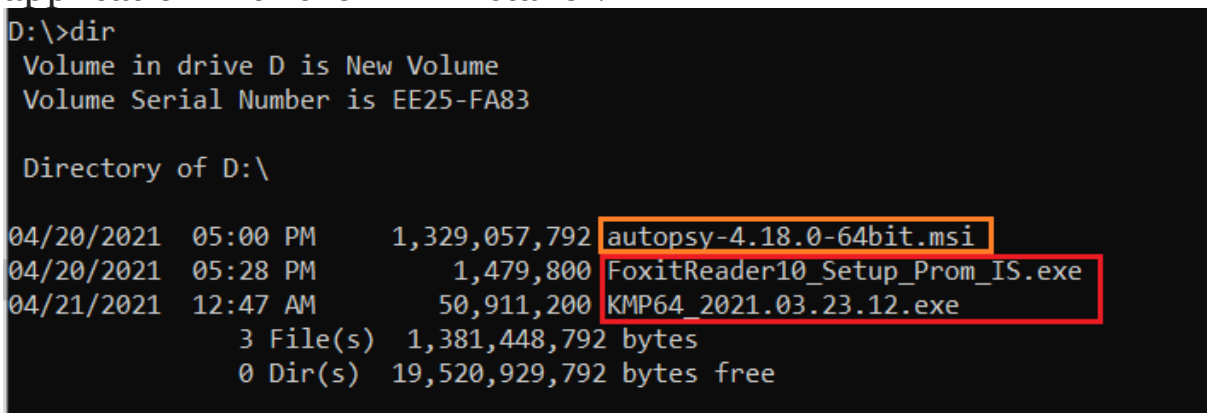
```
Event[18]:
  Log Name: Application
  Source: MsiInstaller
  Date: 2021-04-20T17:18:31.8520000Z
  Event ID: 1033
  Task: N/A
  Level: Information
  Opcode: Info
  Keyword: Classic
  User: S-1-5-21-[redacted]-1005
  User Name: DESKTOP-2DBJI7R\sechub
  Computer: DESKTOP-2DBJI7R
  Description:
Windows Installer installed the product. Product Name: Autopsy. Product Version: 4.18.0. Product Language: 1033.
 Manufacturer: The Sleuth Kit. Installation success or error status: 0.
```

Successful Installation of Autopsy Application — Event ID 1033

The results above show that Atpuosy software was installed by the sechub user on 20 April 2021 on the target system.

EXE Installer:

As discussed above, the event ID such as 11707 does not log any application with the EXE installer.



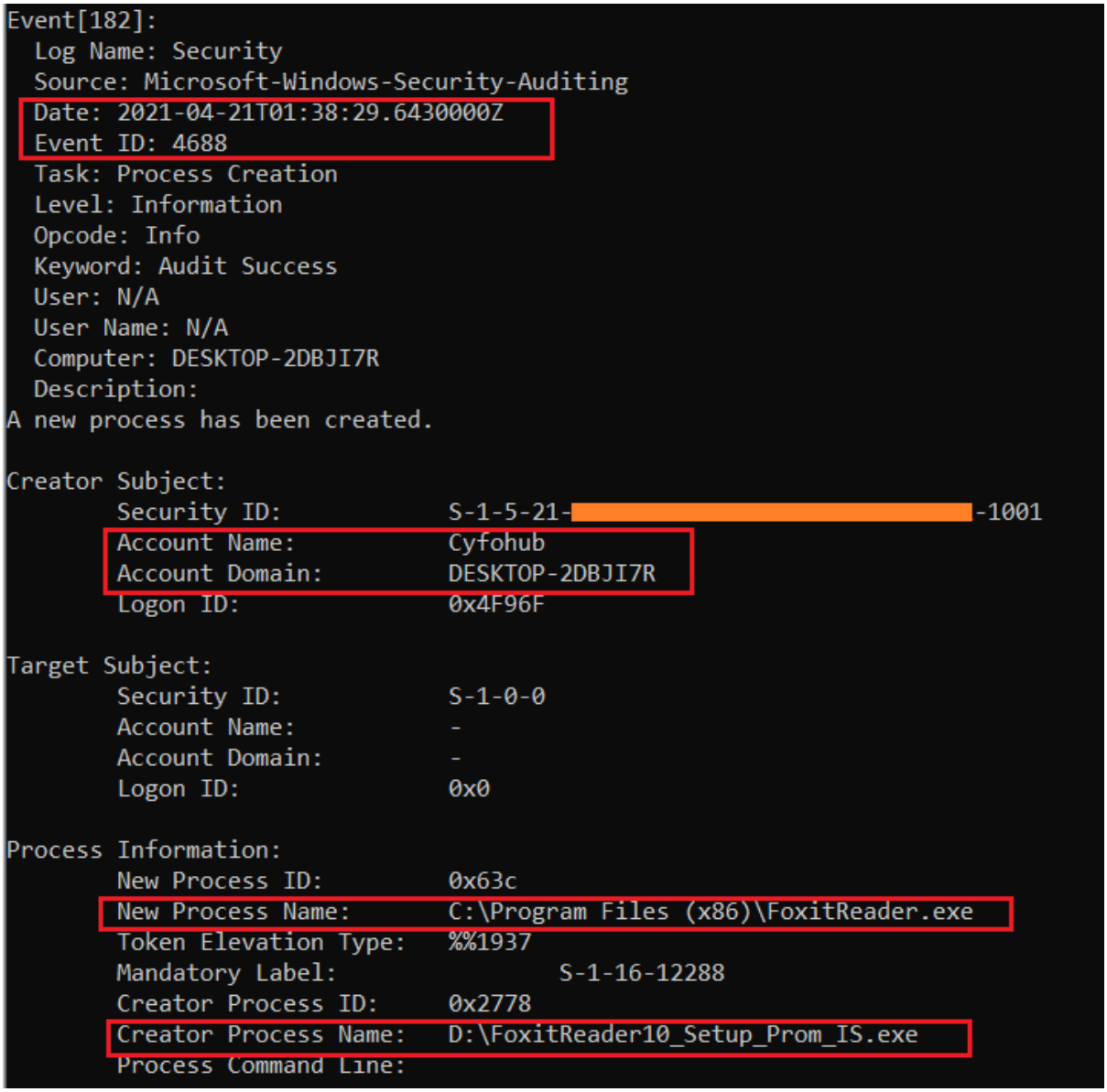
MSI vs. EXE Installers

For instance, the above applications were installed in a test system using MSI and EXE installers. The Autopsy.exe installation information was easily obtained by event IDs 11707 and 1033.

In contrast, it was quite challenging to get the same info for another two applications as not all the EXE installers key in installation information to the application log!

TIP: *There is another event with an ID of 4688 from security that logs the creation of a process. If an application creates an executable file [exe] upon successful installation, this event can be used to understand when the application is installed and by who.*

```
wevtutil qe security /f:text "/q:*[System[(EventID=4688)]]"
```



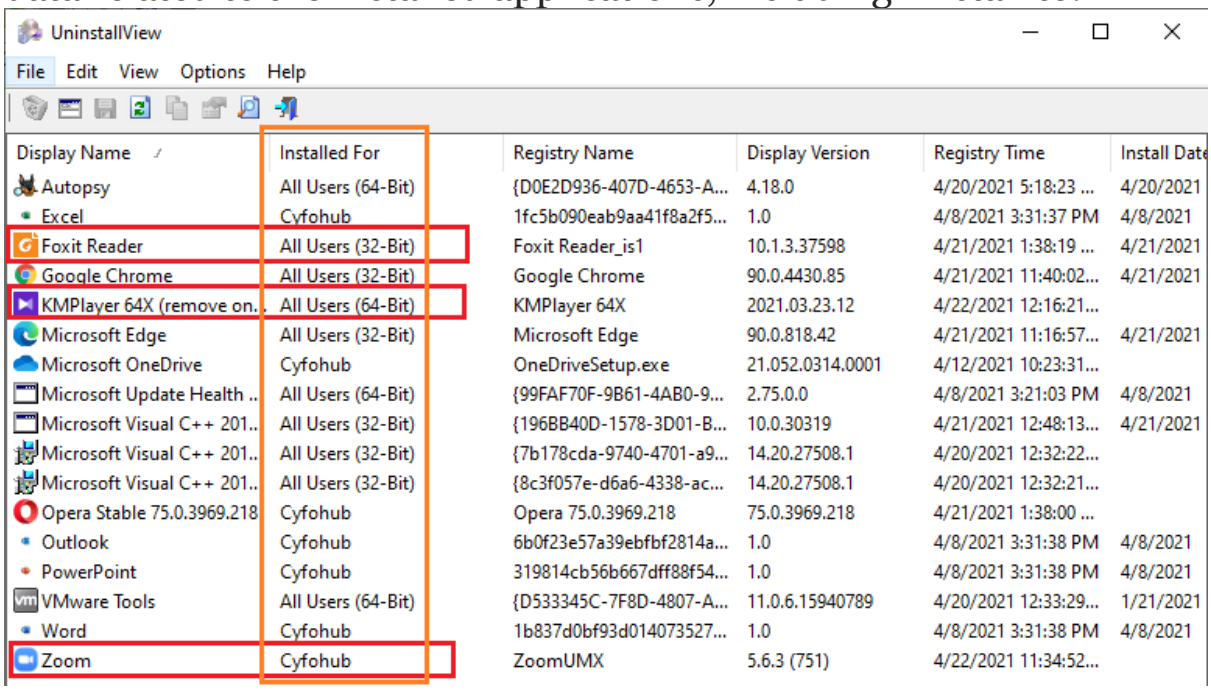
Obtain a Process Creator

3- Installed Applications — Installed for Who?

The second question for installed applications is whether they were installed for a specific user or all. Let's start with a tool before we discuss the rules.

UninstallView by Nirsoft:

Nirsoft developed an amazing tool called UninstallView to display data related to the installed applications, including “install to.”



Display Name	Installed For	Registry Name	Display Version	Registry Time	Install Date
Autopsy	All Users (64-Bit)	{D0E2D936-407D-4653-A...	4.18.0	4/20/2021 5:18:23 ...	4/20/2021
Excel	Cyfohub	1fc5b090eab9aa41f8a2f5...	1.0	4/8/2021 3:31:37 PM	4/8/2021
Foxit Reader	All Users (32-Bit)	Foxit Reader_is1	10.1.3.37598	4/21/2021 1:38:19 ...	4/21/2021
Google Chrome	All Users (32-Bit)	Google Chrome	90.0.4430.85	4/21/2021 11:40:02...	4/21/2021
KMPlayer 64X (remove on...	All Users (64-Bit)	KMPlayer 64X	2021.03.23.12	4/22/2021 12:16:21...	
Microsoft Edge	All Users (32-Bit)	Microsoft Edge	90.0.818.42	4/21/2021 11:16:57...	4/21/2021
Microsoft OneDrive	Cyfohub	OneDriveSetup.exe	21.052.0314.0001	4/12/2021 10:23:31...	
Microsoft Update Health ...	All Users (64-Bit)	{99FAF70F-9B61-4AB0-9...	2.75.0.0	4/8/2021 3:21:03 PM	4/8/2021
Microsoft Visual C++ 201...	All Users (32-Bit)	{196BB40D-1578-3D01-B...	10.0.30319	4/21/2021 12:48:13...	4/21/2021
Microsoft Visual C++ 201...	All Users (32-Bit)	{7b178cda-9740-4701-a9...	14.20.27508.1	4/20/2021 12:32:22...	
Microsoft Visual C++ 201...	All Users (32-Bit)	{8c3f057e-d6a6-4338-ac...	14.20.27508.1	4/20/2021 12:32:21...	
Opera Stable 75.0.3969.218	Cyfohub	Opera 75.0.3969.218	75.0.3969.218	4/21/2021 1:38:00 ...	
Outlook	Cyfohub	6b0f23e57a39ebfbf2814a...	1.0	4/8/2021 3:31:38 PM	4/8/2021
PowerPoint	Cyfohub	319814cb56b667dff88f54...	1.0	4/8/2021 3:31:38 PM	4/8/2021
VMware Tools	All Users (64-Bit)	{D533345C-7F8D-4807-A...	11.0.6.15940789	4/20/2021 12:33:29...	1/21/2021
Word	Cyfohub	1b837d0bf93d014073527...	1.0	4/8/2021 3:31:38 PM	4/8/2021
Zoom	Cyfohub	ZoomUMX	5.6.3 (751)	4/22/2021 11:34:52...	

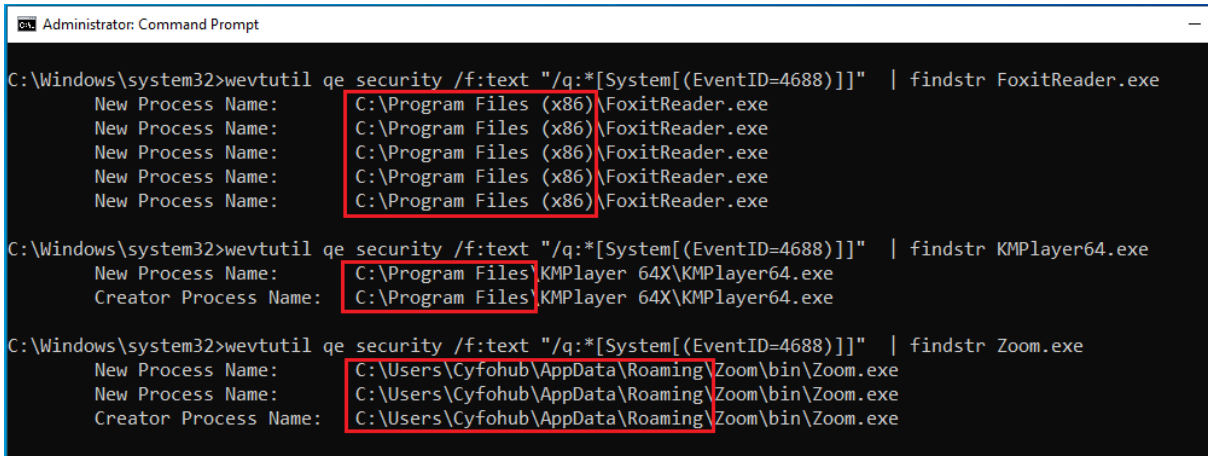
UninstallView by Nirsoft

As shown in the figure above, the Foxit Reader and KMPlayer are both installed for all users, where the Zoom is only installed for a specific user account called Cyfohub.

Event ID 4688:

As explained earlier, this event ID provides us information about process creation, such as “New Process Name,” which includes the full path of a process. The last part explains the User Profile and AppData Folders, and we can use the same concept here.

```
wevtutil qe security /f:text "/q:*[System[(EventID=4688)]]" |
findstr [process name].exe
```



Installed Application Executable File Locations

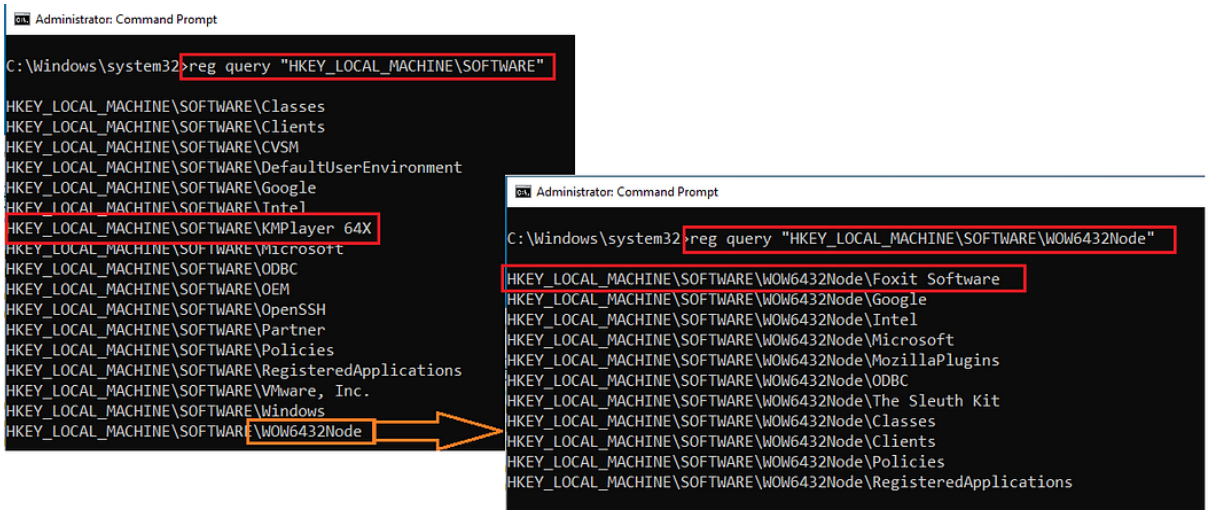
The applications such as Foxit Reader and KMPlayer, installed for all users, are located at C:\Program Files and C:\Program Files (x86). On the other hand, Zoom, installed for a specific user account, is located in the user AppData folder.

Windows Registry: HKEY_LOCAL_MACHINE

The HKEY_LOCAL_MACHINE, or in short HKLM, is a registry hive that keeps specific settings and information of the system. If an application is installed for all users, it should appear in HKEY_LOCAL_MACHINE\SOFTWARE or HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node.

Note: *The WOW6432Node registry records the 32-bit applications installed on 64-bit Windows.*

```
reg query “HKEY_LOCAL_MACHINE”
and
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node"
```

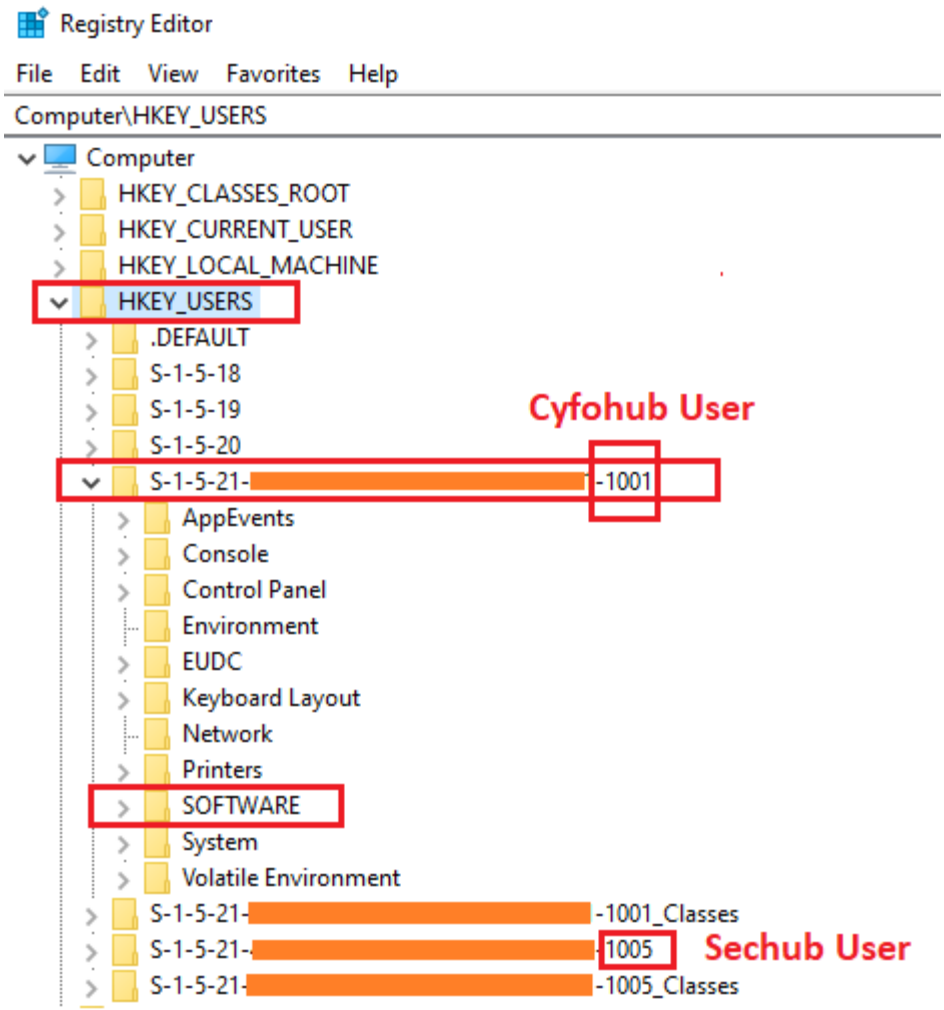


List of Applications that are installed for All Users

The Foxit Reader and KMPlayer are listed under HKEY_LOCAL_MACHINE software indicated these applications are installed for all users.

Windows Registry: HKEY_USERS

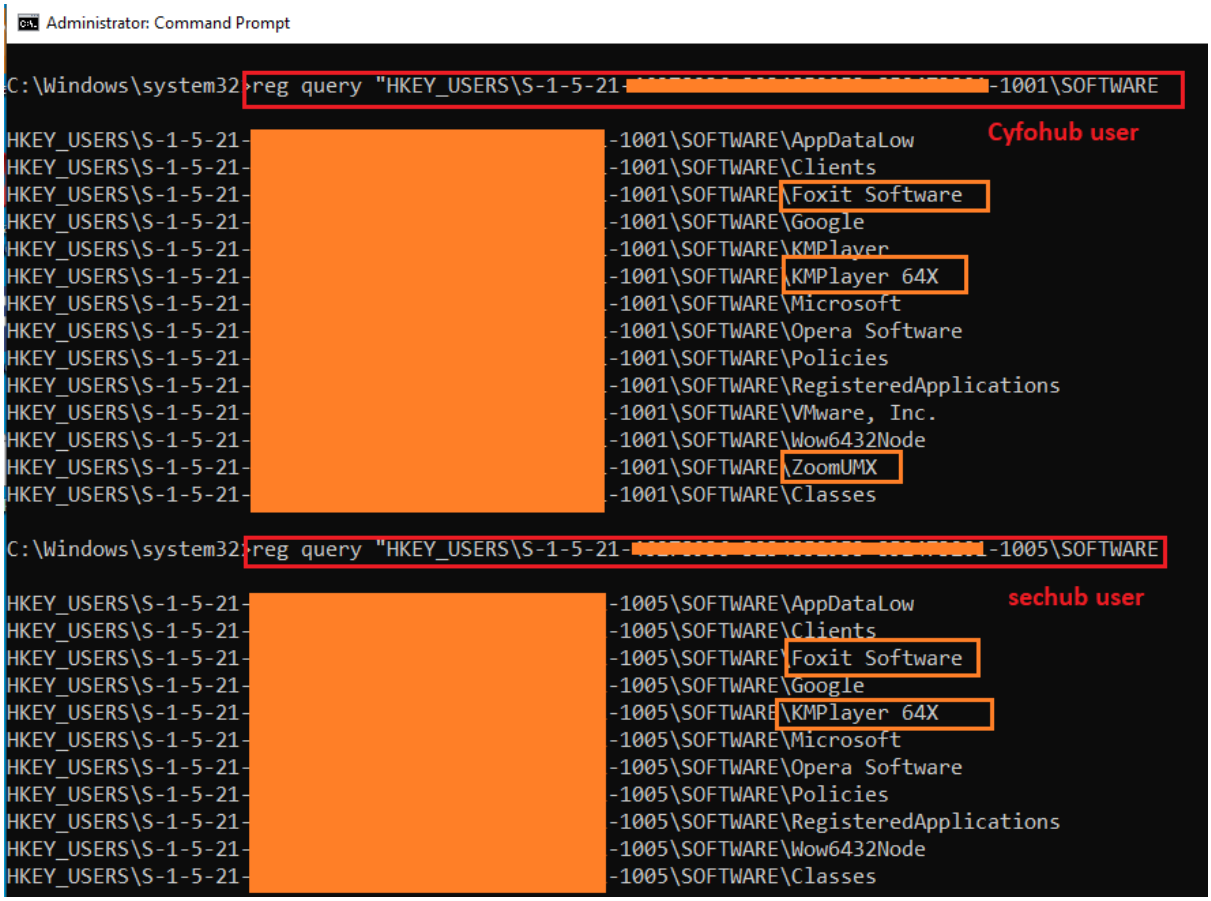
The HKEY_USERS, aka HKU, is one of the Windows registry hives that stores user-specific information for all active user account, including the installed software.



List of Softwares Installed for Specific User

Let's retrieve the software key data for the above user accounts.

```
reg query "HKEY_USERS\[User SID]\SOFTWARE
```



List of Softwares Installed for Specific User [Cyfohub and sechub user accounts]

As expected, the Foxit Reader and KMPlayer can be found for both user accounts; in contrast, the Zoom application only exists under Cyfohub.

4- Folder and Files

Without a doubt, analyzing folders and files is an integral part of every digital forensics investigation; in the following post, we will explain it in detail. This section only focuses on the folder and files' ownerships.

DIR Command:

The DIR is a built-in windows command to display the list of directories, subdirectories, and files. There are many switches to customize the output of the DIR command, and we are using two of them:

- **/q:** Displays file ownership information.
- **/s:** Lists all of the file names within the directory along with all subdirectories.

```
DIR /s/q
```

```
 Directory of D:\Checklists

04/26/2021  08:53 AM    <DIR>          DESKTOP-2DBJI7R\sechub .
04/26/2021  08:53 AM    <DIR>          NT AUTHORITY\SYSTEM    ..
04/26/2021  08:53 AM                 0 DESKTOP-2DBJI7R\sechub IR and DF.txt
04/26/2021  08:53 AM                 0 DESKTOP-2DBJI7R\sechub RED Team.txt
04/26/2021  08:53 AM                 0 DESKTOP-2DBJI7R\sechub VAPT.txt
               3 File(s)              0 bytes

 Directory of D:\Tools

04/26/2021  08:52 AM    <DIR>          DESKTOP-2DBJI7R\Cyfohub.
04/26/2021  08:52 AM    <DIR>          NT AUTHORITY\SYSTEM    ..
04/21/2021  12:47 AM        50,911,200 DESKTOP-2DBJI7R\CyfohubKMP64 2021.03.23.12.exe
04/26/2021  08:49 AM                 0 DESKTOP-2DBJI7R\CyfohubList of tools.txt
01/21/2021  03:28 AM             3,566 DESKTOP-2DBJI7R\Cyfohubpowerinfo.txt
04/26/2021  08:52 AM            37,668 DESKTOP-2DBJI7R\sechub screen.png
01/21/2021  03:26 AM             2,639 DESKTOP-2DBJI7R\Cyfohubsysteminfo.txt
03/13/2021  09:59 PM           192,376 DESKTOP-2DBJI7R\CyfohubUninstallView.exe
04/22/2021  11:34 AM        15,577,792 DESKTOP-2DBJI7R\CyfohubZoomInstaller.exe
               7 File(s)     66,725,241 bytes

    Total Files Listed:
              20 File(s)  1,448,174,957 bytes
               6 Dir(s)  19,454,181,376 bytes free
```

Folder and File Owners with DIR Command

We can combine the above command with the findstr to list specific users:

```
DIR /s/q | findstr sechub
```

```
D:\>DIR /s/q | findstr sechub
04/26/2021  08:53 AM    <DIR>          DESKTOP-2DBJI7R\sechub Checklists
04/26/2021  08:53 AM    <DIR>          DESKTOP-2DBJI7R\sechub .
04/26/2021  08:53 AM                 0 DESKTOP-2DBJI7R\sechub IR and DF.txt
04/26/2021  08:53 AM                 0 DESKTOP-2DBJI7R\sechub RED Team.txt
04/26/2021  08:53 AM                 0 DESKTOP-2DBJI7R\sechub VAPT.txt
04/26/2021  08:52 AM            37,668 DESKTOP-2DBJI7R\sechub screen.png
```

Folder and File for Specific Owner

Powershell:

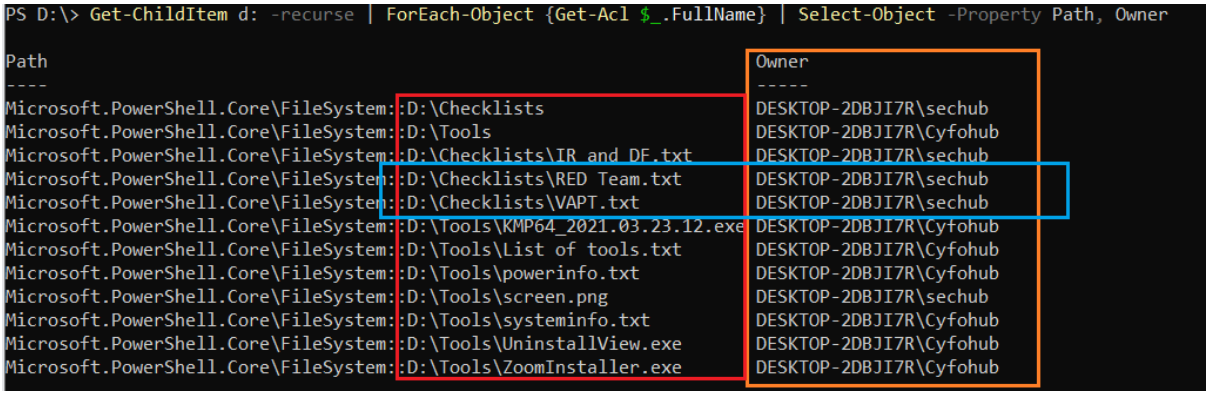
The Powershell Get-Acl displays the security descriptor for resources, including files and folders.

```
D:\>dir
 Volume in drive D is New Volume
 Volume Serial Number is EE25-FA83

 Directory of D:\

04/26/2021  08:53 AM    <DIR>          Checklists
04/26/2021  08:52 AM    <DIR>          Tools
               0 File(s)              0 bytes
               2 Dir(s)  19,454,181,376 bytes free

D:\>powershell Get-Acl d:\tools

    Directory: D:\


Path  Owner                  Access
----  -----                  ------
tools DESKTOP-2DBJI7R\Cyfohub BUILTIN\Administrators Allow  FullControl...
```

Folder Owners with Powershell

Let's use it along with Get-ChildItem to displays owners for all folders, subfolders, and files.

```
Get-ChildItem d: -recurse | ForEach-Object {Get-Acl $_.FullName}
| Select-Object -Property Path, Owner
```



Folder, Subfolder, and File Owners with Powershell

5. What would be Next

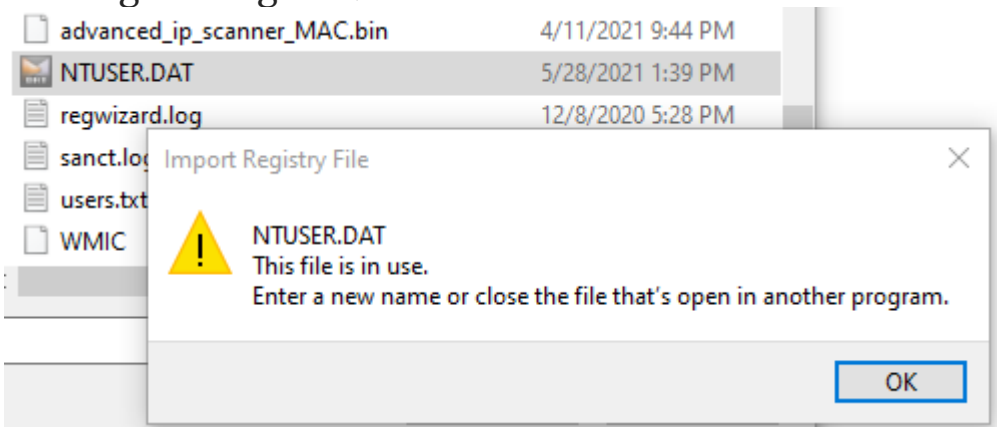
This post explained the ownerships of Process, Applications, Folders, and Files. Yet we have no idea about applications that executed, recently opened directories and files.

Do you remember where to look for this information? Yes, you are correct … NTUSER.DAT! Stay Tune…

System Live Analysis [Part 10]- Windows: User Account Forensics- In-use and Locked Files Acquisition

One of the main challenges in live forensics is to deal with in-use or locked files and resources. Unlike the traditional forensics investigation, we are not making a full forensics image of the hard disk during system live analysis.

In fact, we are interacting with running and operational systems where numbers of files and resources may be in use by running process and cant be open with any tools. Thus, we would face the nursing message as below:



Opening an in-use file failed!

Are you wondering how this could be related to user account forensics? Let's review two important files [explained in part 8] that contain user activities and settings:

- **NTUSER.DAT:** This is the main registry hive for the users residing in the user account profile folder and contains the most valuable forensics data.

- **UsrClass.dat:** Just Like NTUSER.DAT, the UsrClass is another registry hive to obtained user-related information.

We cannot use standard copy and paste methods to copy the above files for the logged-in user during the live investigation as the files are in active use and protected.

What if we kill all the processes using a particular file to make it free and accessible?

Note: *Rule number one in live analysis and digital forensics is to minimize the modifications in systems that are being investigated. Thus, we can't easily kill the process as we may affect the system's integrity and change forensics evidence.*

Blue Team: System Live Analysis [Part 2]- Windows: Rules and Tools
Let's Connect | LinkedIn
sechub.medium.com

How about retrieving the files from shadow copies? They are backups of Windows files and can be used to restore data when required!

Note: *As explained earlier, shadow copies are amazing, but they are snapshots of a system at a particular point in time and may not fully represent the current state of files and resources. Besides, not*

all machines being investigated may have the shadow copies or restore point enabled.

Mmm... then what to do? There is a way, a forensics method, to acquire these types of files using FTK Imager. Let's do it...

1- Some Forensics Considerations

We can install the FTK imager on the victim machine and make a copy of the files. Still, forensically we are not supposed to install and copy anything on the system under investigation.

It's highly suggested [as a best practice] to use external storage, which contains a copy of FTK imager, connects it to the system, makes a copy of files, and saves them into external storage.

The external storage must be forensically clean and completely free of any actual and residual data. This to avoid any data conflict between collected evidence and whatever data exist on the medium.

Moreover, it will help to ensure the external storage is malware-free to avoid any possible cross-contamination.

2- USB Storage Wipe

Delete, shift delete, fast format, format..? No, none of them sterilizes the storage forensically. In fact, the storage may appear empty, but the files will still be there and could be recovered. Why?

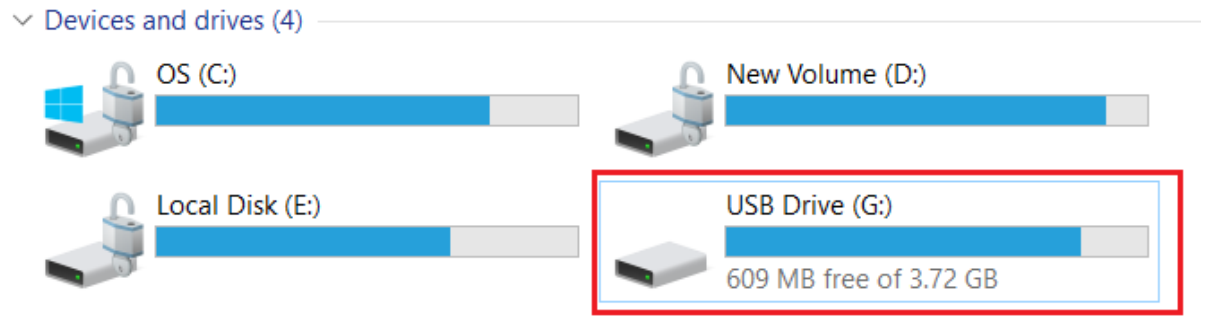
Because these techniques delete the file system only and make the files invisible rather than completely remove them from the storage. In contrast, the storage wipe operation overwrites the existing data with zeros or random data, ideally in several rounds.

- **Manual Storage Wipe**

A standard windows format comment combined with the parameter /p: can be used to wipe storage as follows:

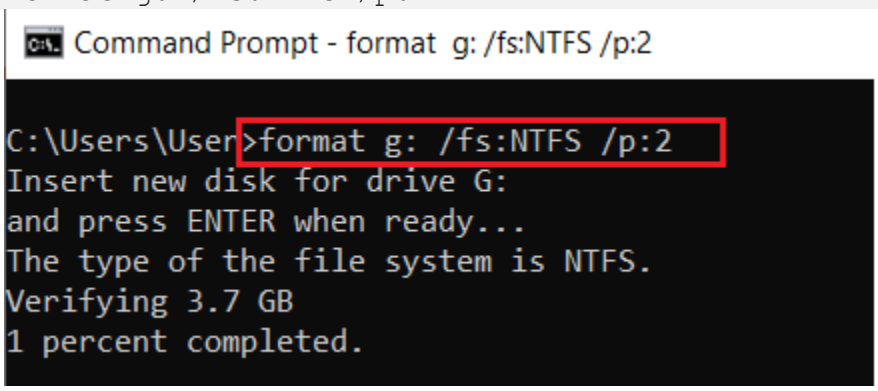
```
format [Strorage Drive] /fs:[type of file system] /p:[Number of Rounds]
```

For instance, I would like to forensically wipe my USB drive with a drive letter of G with NTF format and overwrite every data sector with Zero for two rounds.



USB Drive with Drive Letter of G

```
format g: /fs:NTFS /p:2
```

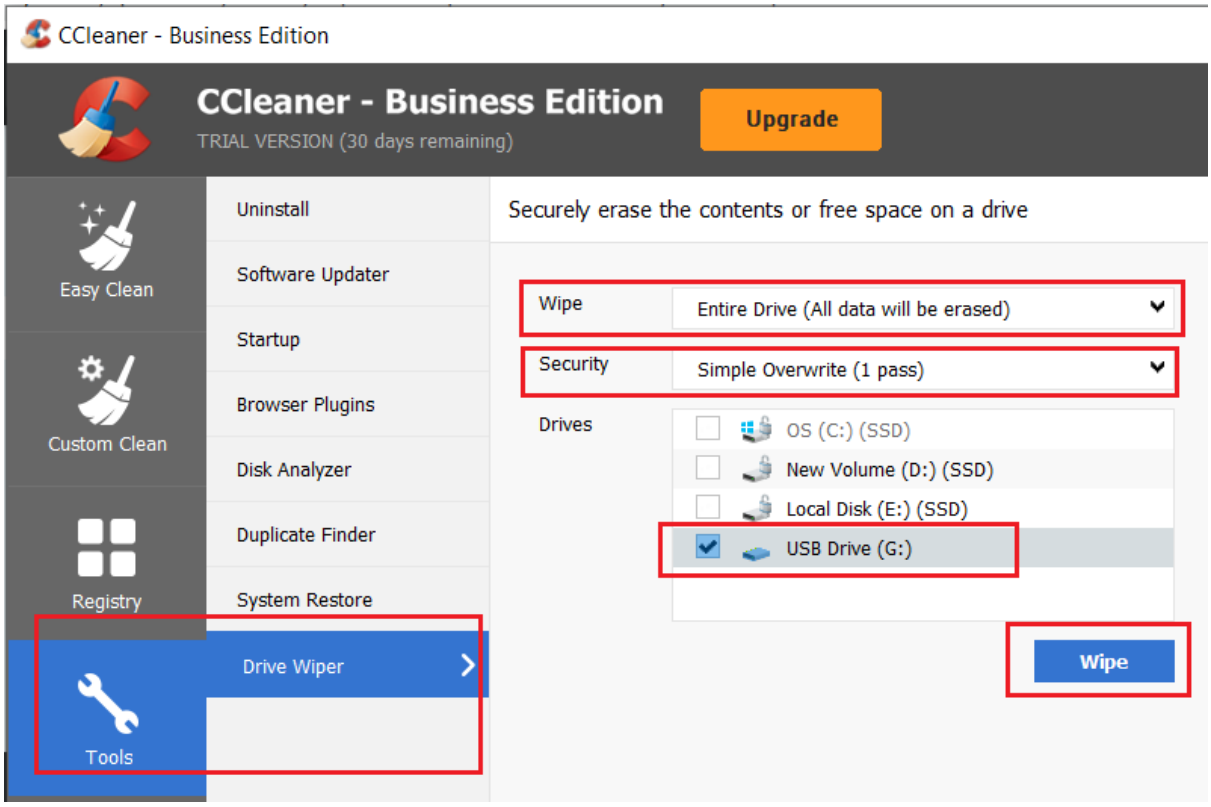


Wipe USB Drive with Format Command

The above command does not support quick format; thus, we will need few packs of popcorn while we are waiting for the process to be completed[the more the round, the longer the process]

- **CCleaner**

We know the rules now; let's use some tools. There are numbers of tools out there that provide us with storage wipe function, and CCleaner is one of them, which provides us with 30 days free trial.

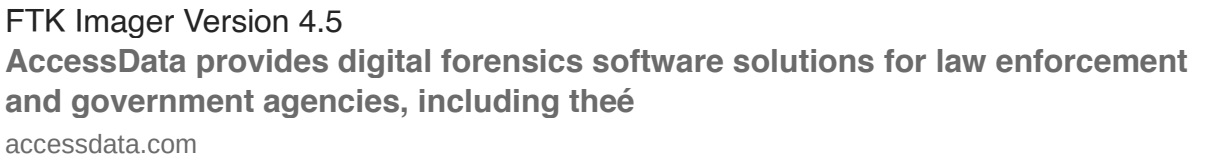


Wipe USB Drive with CCleaner

Note: Several other tools are available to wipe the storage mediums; we just need to validate their publisher to make sure they are reputable software.

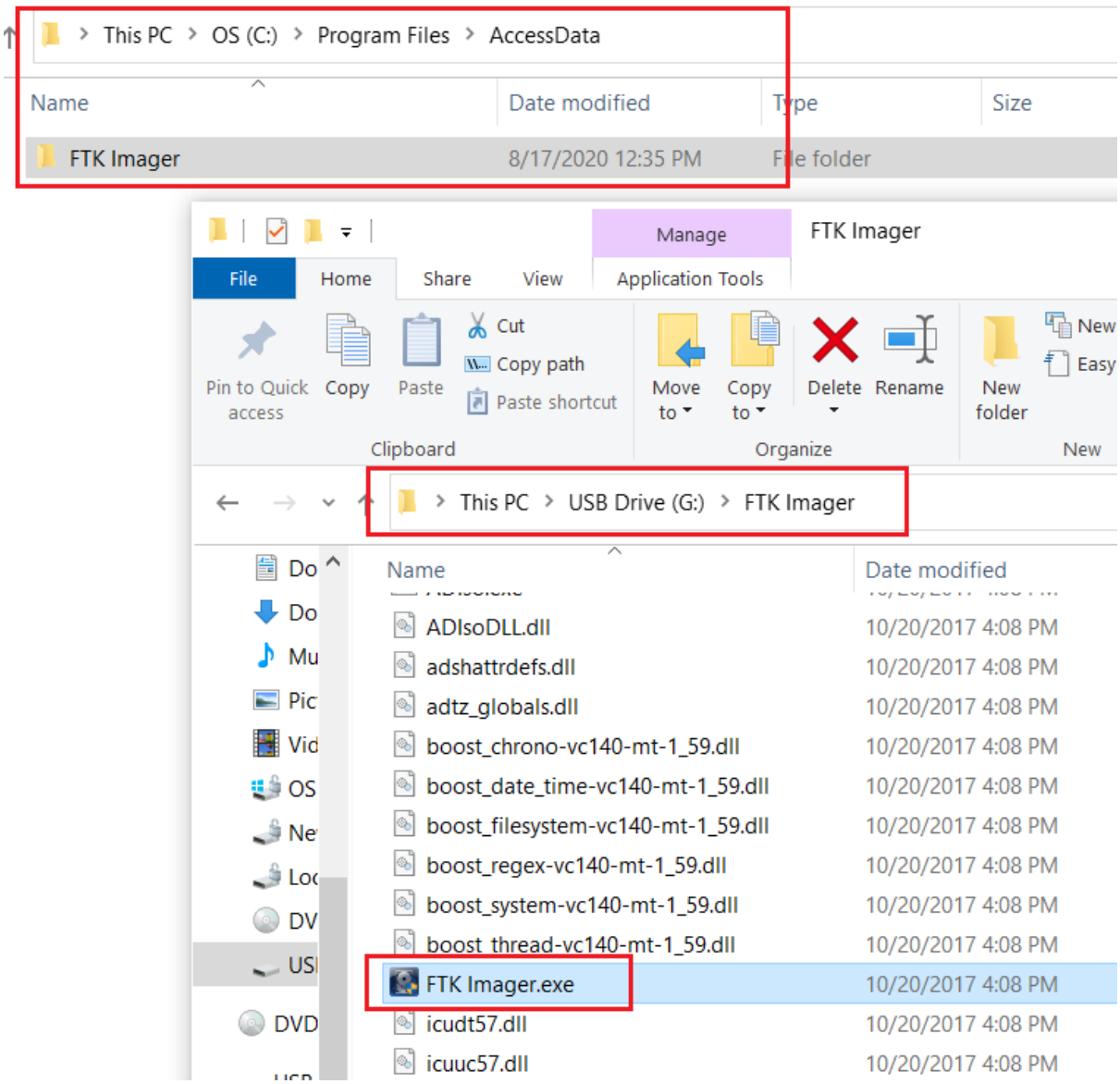
3- FTK Imager Preparation

As our USB drive is ready, now it's time to install FTK Imager. Kindly note, there may be many other tools to use, but FTK image is one of the leaders in the forensics industry with a high reputation, and it's free.



FTK imager installation is pretty simple, and we just need to execute the binary and click a bunch of Next. However, as mentioned several times, we are not supposed to install the systems under investigation. Here is the trick...

Install the tool in your own system or any system dedicated to the investigation, and then copy and paste the installed folder to the forensically wiped USB.



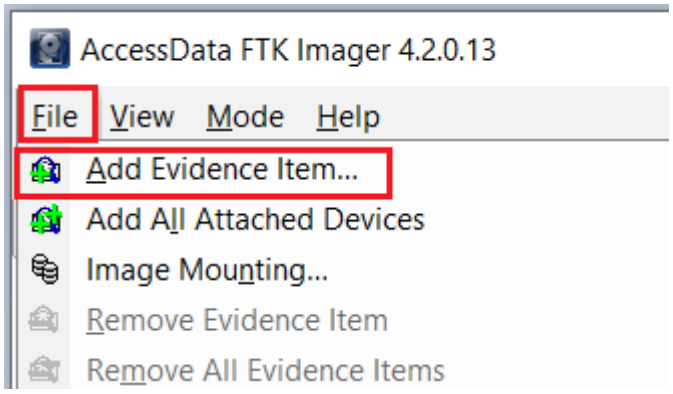
Copy Installed FTK Imager Folder to USB Drive

Ready? 1…2…3… action…

4- Copy in-use / locked files

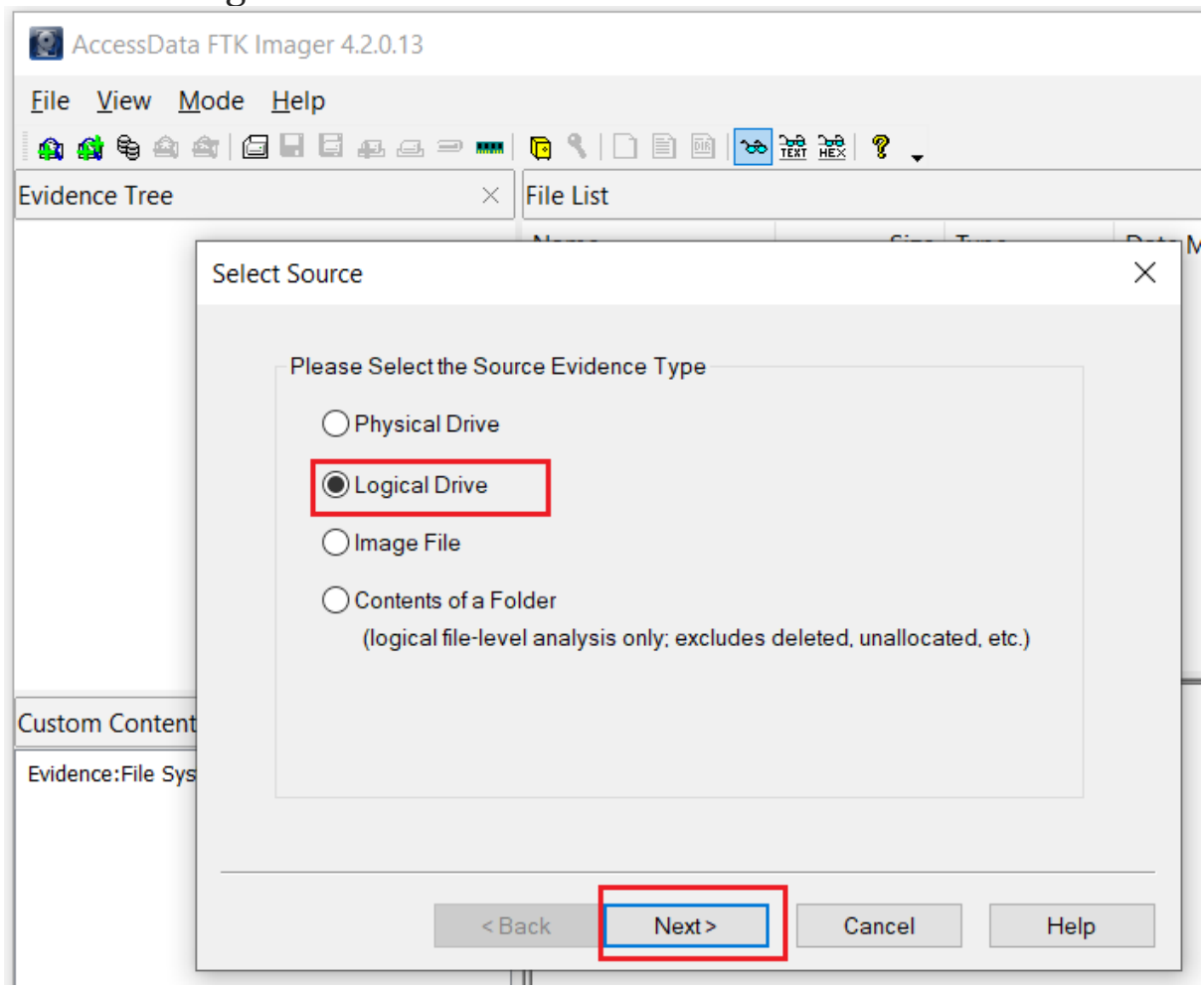
Now we can connect the USB drive to the target machine and run the FTK Imager.

- Select “Add Evidence Item” from the file menu



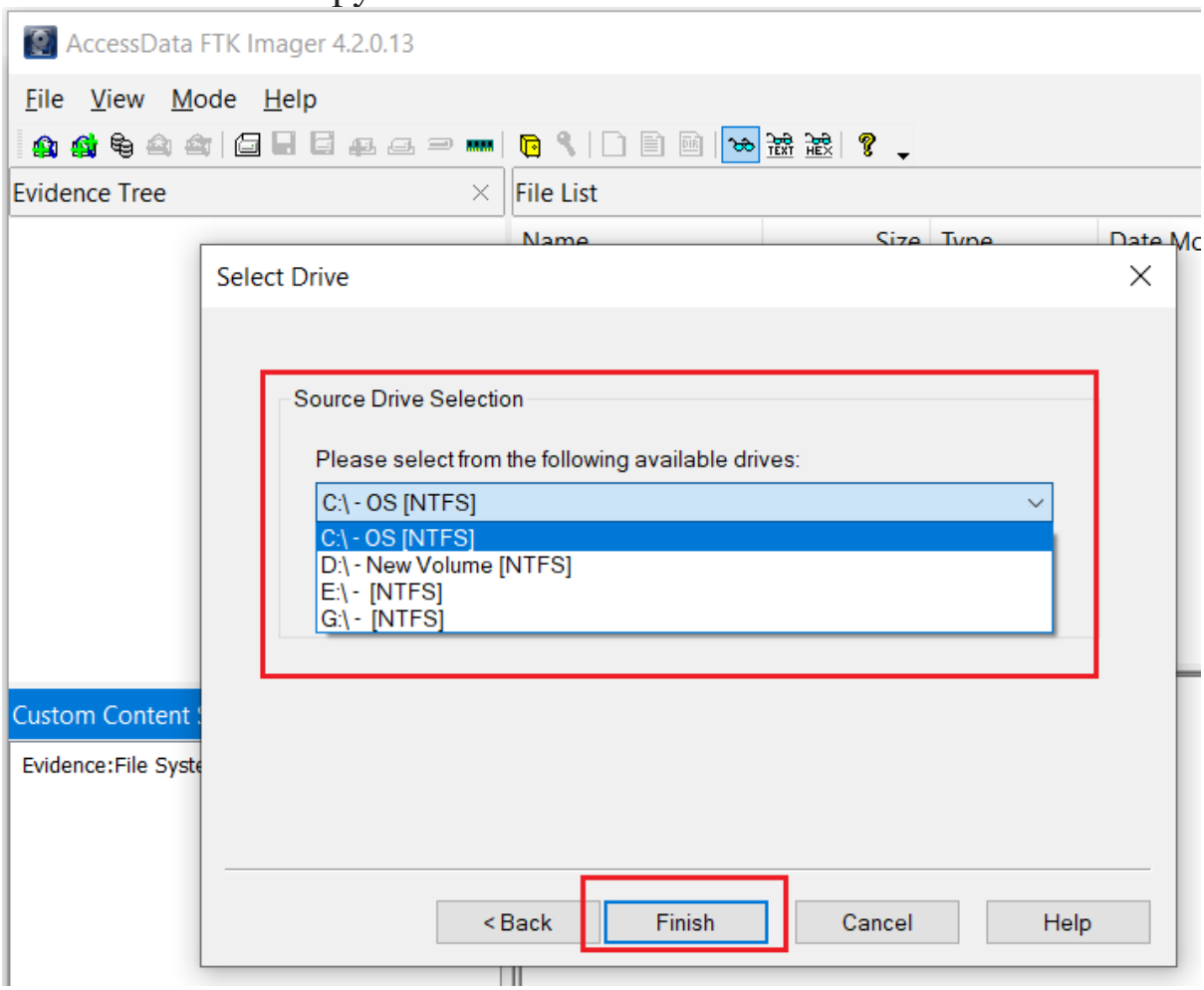
FTK Imager File Menu

- Select the “Logical Drive” option as we are not going to image the entire hard disk



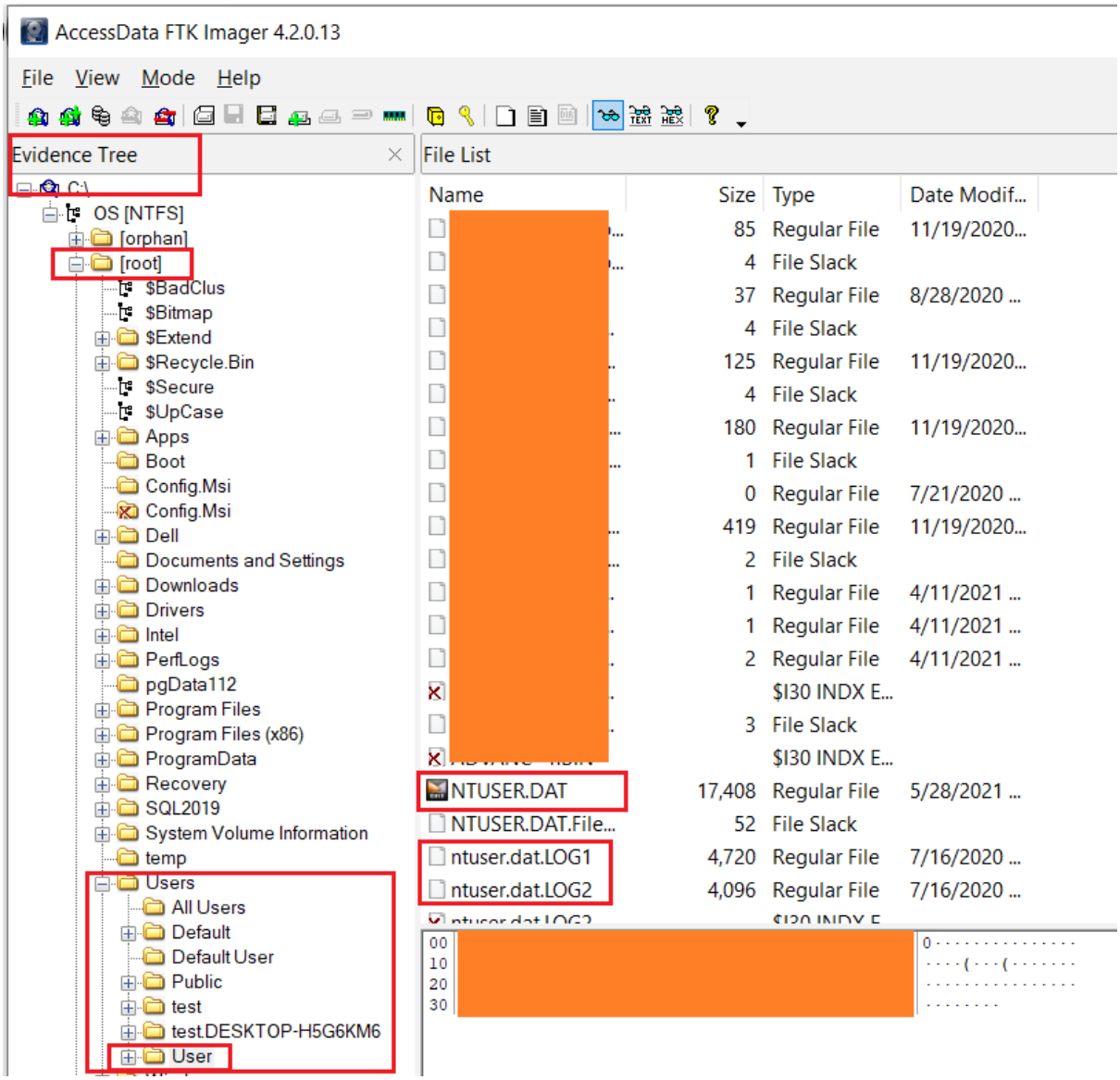
FTK Imager Source — Logical Drive Option

- Please select the desired drive where our targeted locked file is located. I selected drive C in this post. I'm going to make a copy of **NTUSER.DAT.**



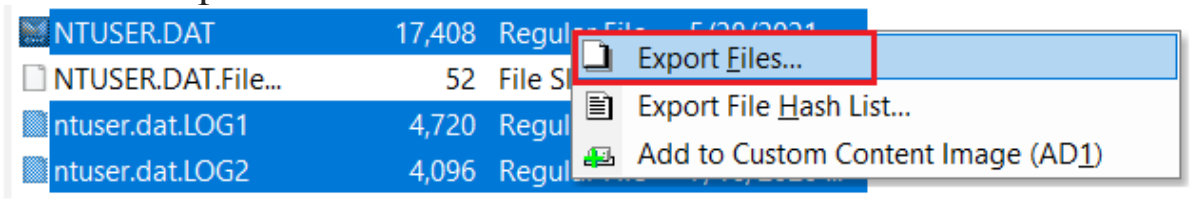
Select the Target Drive

- In the left side pane called Evidence Tree, we can navigate to the target folder. In this case, it's the user folder. We can view the **NTUSER.DAT, NTUSER.DAT.LOG1, and NTUSER.DAT.LOG2.**



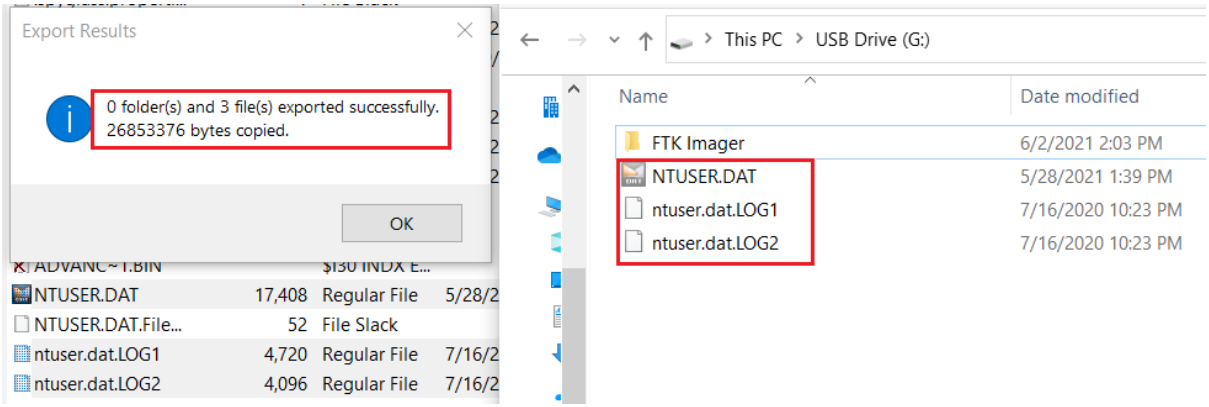
FTK Imager — Evidence Tree

- Select all the required locked files, right-click and choose export



FTK Imager — Export Locked Files

- Done!



Copy Locked Files

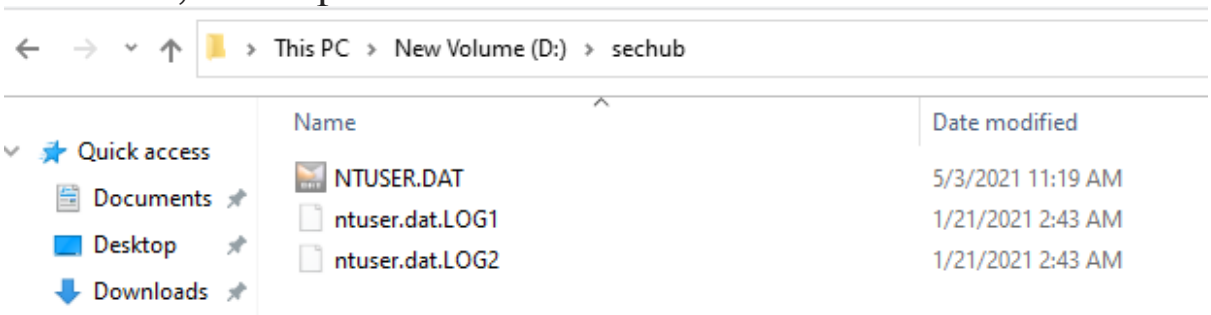
Stayed tuned … we gonna dive deep into user account activities investigation as we have a copy of the in-use **NTUSER.DAT** file in hand. We can use the same technique to acquire other registry files such as System, Sam, Security, Software, and Default.

System Live Analysis [Part 11]- Windows: User Account Forensics- NTUSER.DAT Rules, Tools, Structure, and Dirty Hives!

Without a doubt, the Windows registry is one of the most valuable forensics data sources that investigators can use. I should think of a dedicated series on Windows Registry Forensics, but, for now, we only focus on NTUSER.DAT and its role in user account forensics.

Note: This post only focuses on the NTUSER.DAT, however, the rules and tools can be used for other registry files such as System, Sam, Security, Software, and Default.

Part 10 explained how we could forensically extract one of the most important files to analyse user profiles, settings, and activities. Yes, the NTUSER.DAT. The data stored in NTUSER.DAT and the logs give us fantastic information about each user. As we have them in hand now, let's explore.



NTUSER.DAT, netuser.dat.LOG1 and netuser.dat.LOG2 extracted from a test system using FTK Imager

1- Rules First, Tools Next!

You may know the main principle of my writeups: ***Know the Rules, Before Using Tools.*** We can be masters of tools, quickly refer to them, and start analyzing our files, nothing wrong with that!

But, in my opinion, dive into how things are working (e.g. file structures, operations, interactions, logic, formats, etc.) makes us an expert and even helps us understand tools capabilities better.

Example: We may have heard that how amazing is Registry Explorer to deal with windows registry forensics. I do agree with this statement too! Why? Well, let's learn few rules then.

2- Unreconciled data (Dirty Hive!)

The NTUSER.DAT is the primary file for the HKEY_CURRENT_USER hive and keeps user-related information; however, Windows is not updating this file in real-time.

In fact, when a system is running, the data being stored in transaction logs first and will be synced with the primary file when the system is logging off, all the users are inactive, or an hour has elapsed since the last sync.

Part 8 Recap: Windows keep a backup of all the activities and changes such as accessing folders, opening files, network shares, etc., in netuser.dat.LOG1 and netuser.dat.LOG2 during the live session and saves them into NTUSER.DAT during Log off.

- **The Challange**

The NTUSER.DAT collected from a victim system may not contain the most updated data as we are conducting the live analysis, and the transaction logs data may have not yet been transferred to the primary file.

- **The Solution**

To address this issue, we need to obtain the netuser.dat.LOG1 and netuser.dat.LOG2 (we did it in part 10) and aggregate them with NTUSER.DAT to have all the data in hand.

Wait? How do we know whether the NTUSER.DAT is updated or not!

3- How to Detect dirty hives

Some tools make life easy, but if you ask me, the manual analysis gives us a greater understanding of what we are doing, which is crucial for every investigator.

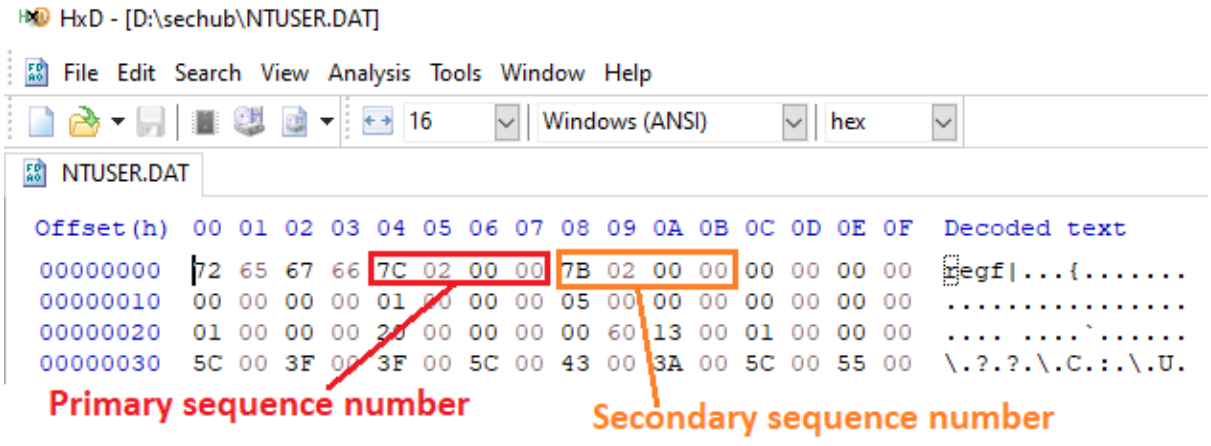
Don't get me wrong, what I just suggested must be employed during training and capability development. We are not supposed to avoid tools and waste our time and energy on the battlefield. There are many tools available to have fun, and we will use them right away in a real investigation.

It's highly recommended to understand the structure of the primary hive. However, to make it simple, we need to check two fields of the NTUSER.DAT header as follows:

- **Primary sequence number**: This number incremented by 1 when the write operation on NTUSER.DAT begins.
- **Secondary sequence number**: This number incremented by 1 when the write operation on NTUSER.DAT ends.

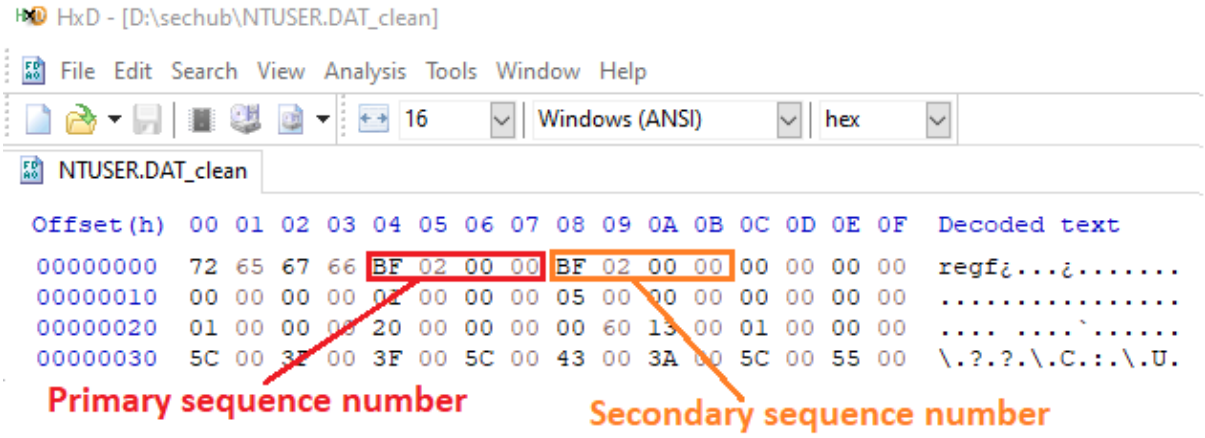
The above numbers should be equal in the event of a successful write operation. Thus:

- If the Primary sequence number !=Secondary sequence number: the NTUSER.DAT is not updated (Dirty Hive) and must be aggregated with netuser.dat.LOG1 and netuser.dat.LOG2.



Dirty NTUSER.DAT opened with Hex Editor.

- If the Primary sequence number ==Secondary sequence number: the NTUSER.DAT is updated (Clean Hive) and contains the complete actual data.



Clean NTUSER.DAT opened with Hex Editor.

Now we have a good idea of why it is important to obtain the netuser.dat.LOG1 and netuser.dat.LOG2 in addition to the primary file. We need them to update the NTUSER.DAT. How? Well, it's time to justify why Registry Explorer is one of the bests!

The main strength of the Registry Explorer tool is the ability to identify the dirty NTUSER.DAT and replay the netuser.dat.LOG1 and netuser.dat.LOG2 to fix the issue.

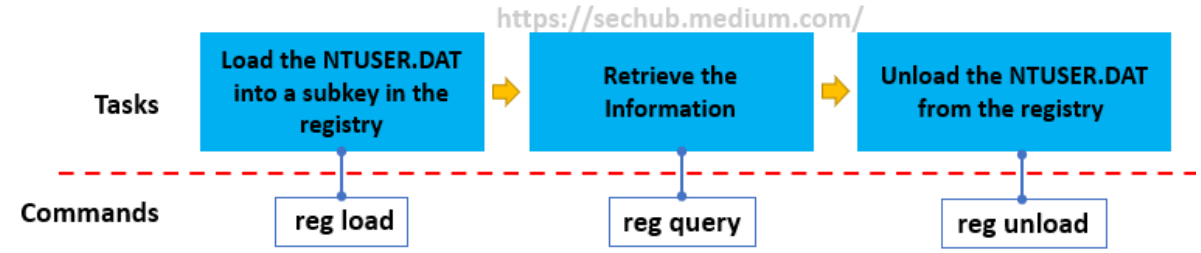
4- How to Read NTUSER.DAT

There are few paid tools such as OSForesnics and FTK Registry Viewer to work with NTUSER.DAT and registry files in general. We can use demo versions to get familiar with them.

However, Windows built-in commands and free tools such as RegRipper and Registry Explorer are good enough to conduct our investigation.

4.1 Windows built-in command

The reg commands enable us to perform various operations on windows registry subkeys. We need the reg load, reg query, and reg unload commands to work with NTUSER.DAT collected from the test system.



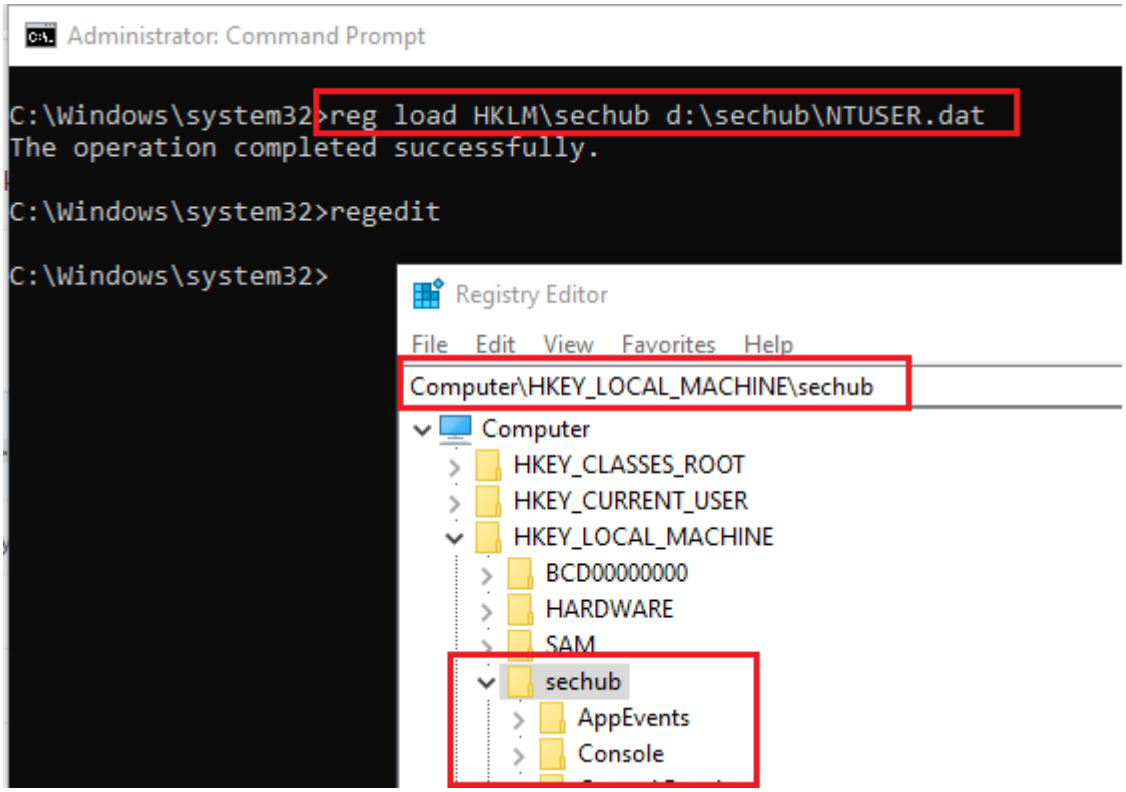
Reg Commands for NTUSER.dat Analysis

- **Load the NTUSER.DAT**

We can use the reg load command to load the NTUSER.DAT into a temporary subkey in the Windows registry to view and read it.

```
reg load HKLM\sechub d:\sechub\NTUSER.dat
```

The above command loads the NTUSER.dat into the sechub subkey under the HKEY_LOCAL_MACHINE that can be viewed in Regedit.

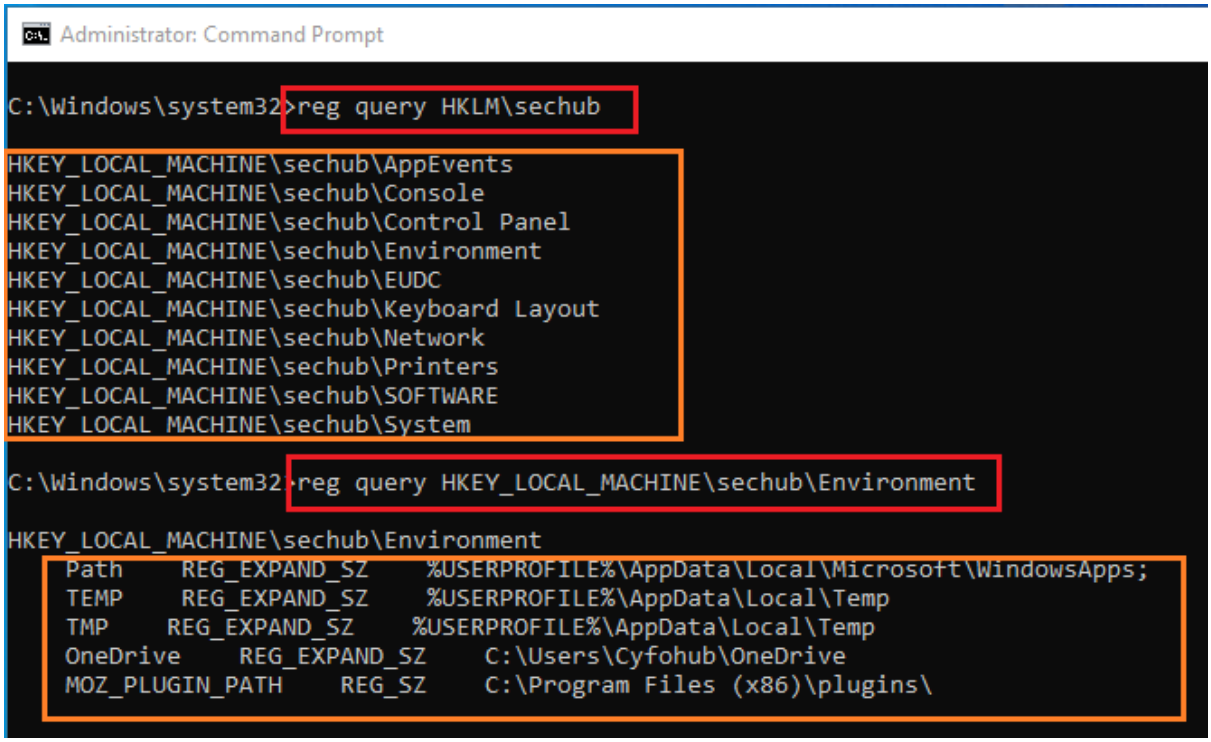


NTUSER.dat Loaded into HKLM\sechub

- **Retrieve Information**

Now we can use the reg query to retrieve desired information from the loaded NTUSER.dat. The figure below depicts the two queries as an example.

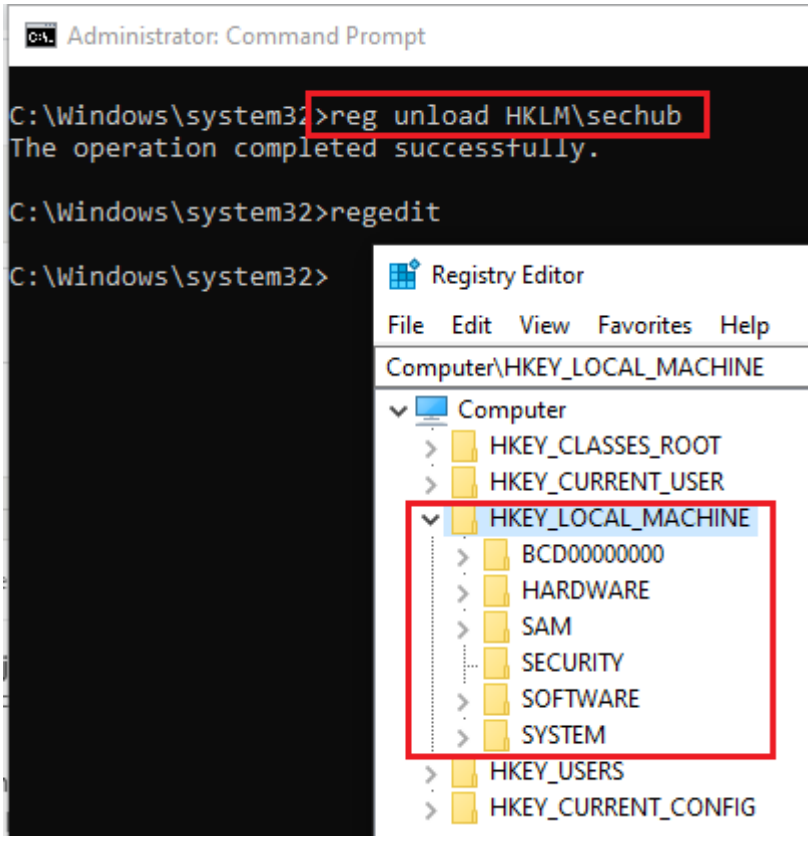
```
reg query HKLM\sechub
and
reg query HKEY_LOCAL_MACHINE\sechub\Environment
```



Retrieve the Information from Loaded NTUSER.DAT using Reg Query Command

- **Unload the NTUSER.DAT**

Once we get all the information we look for, we should unload the NTUSER.DAT from the registry and remove the temporary subkey.

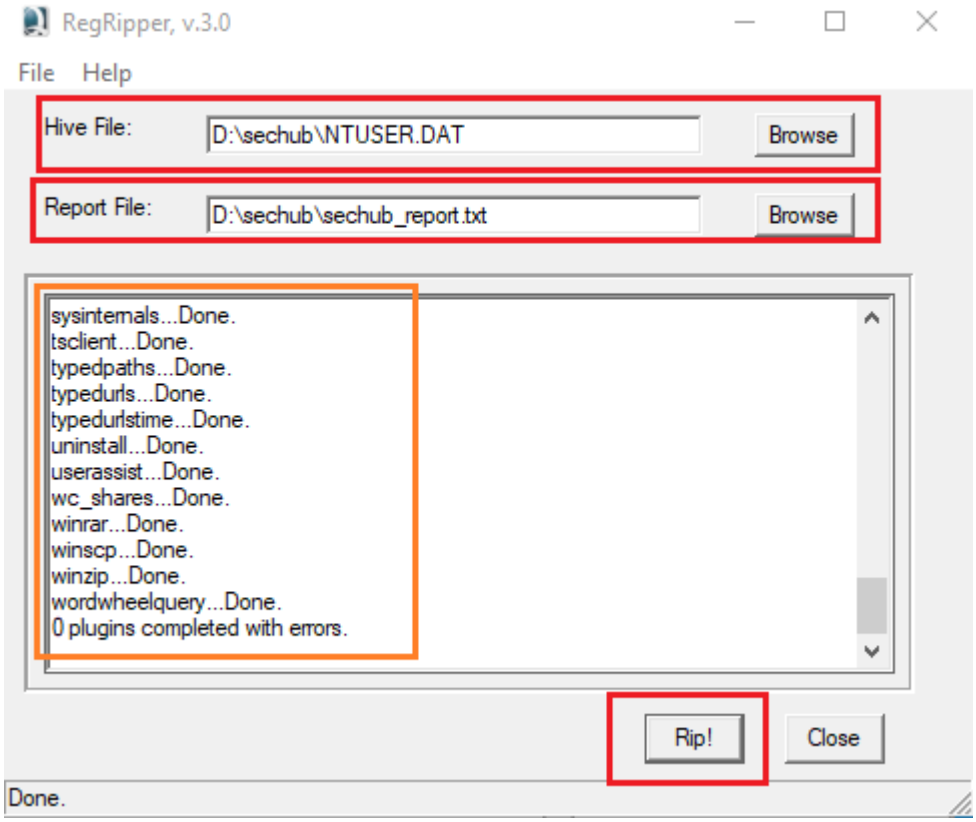


Unload NTUSER.dat from Registry

Note: The windows registry must be closed during the load and unload process.

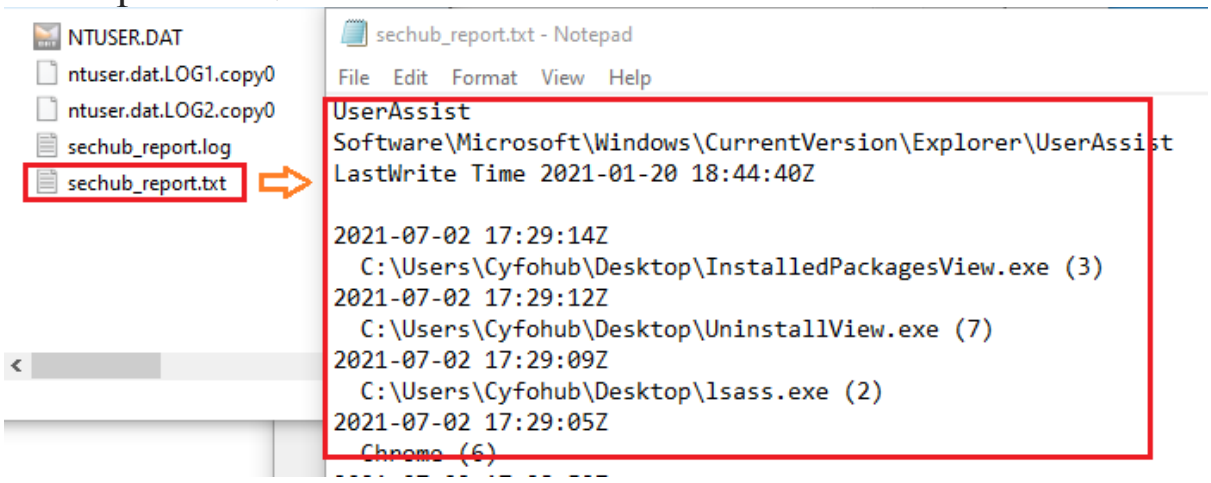
4.2 RegRipper

Working with the RegRipper is quite straightforward; load the NTUSER.DAT as Hive File, set the file name and directory for the report, and we are good to go!



Retrieve the Information from Loaded NTUSER.DAT using RegRipper

The report will be in txt format as follows:



The RegRipper Report Sample

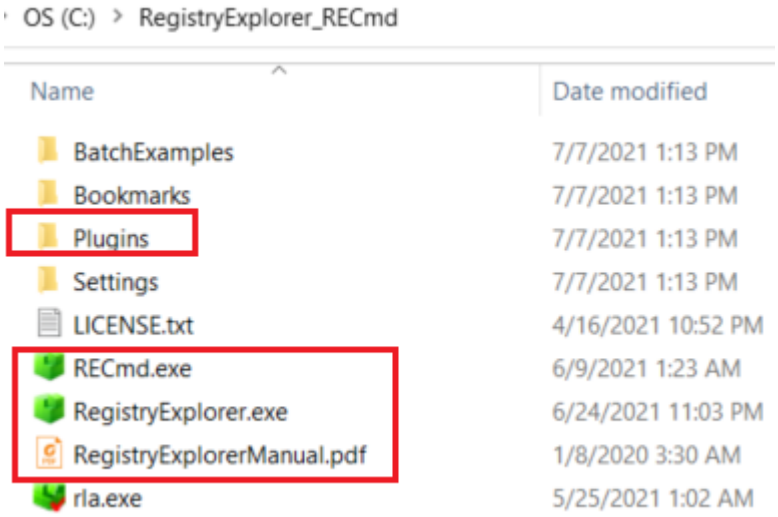
Even though the RegRipper is easy to use, the result will be in plain text that makes data navigation difficult, not a big deal! But, the is a bigger issue.

The RegRipper will not handle the unreconciled data restored in transaction logs (netuser.dat.LOG1 and netuser.dat.LOG2), and as a result, we may not have the most updated data by just analyzing the main file (NTUSER.DAT).

Note: We may have the same issue using the Built-in Command!

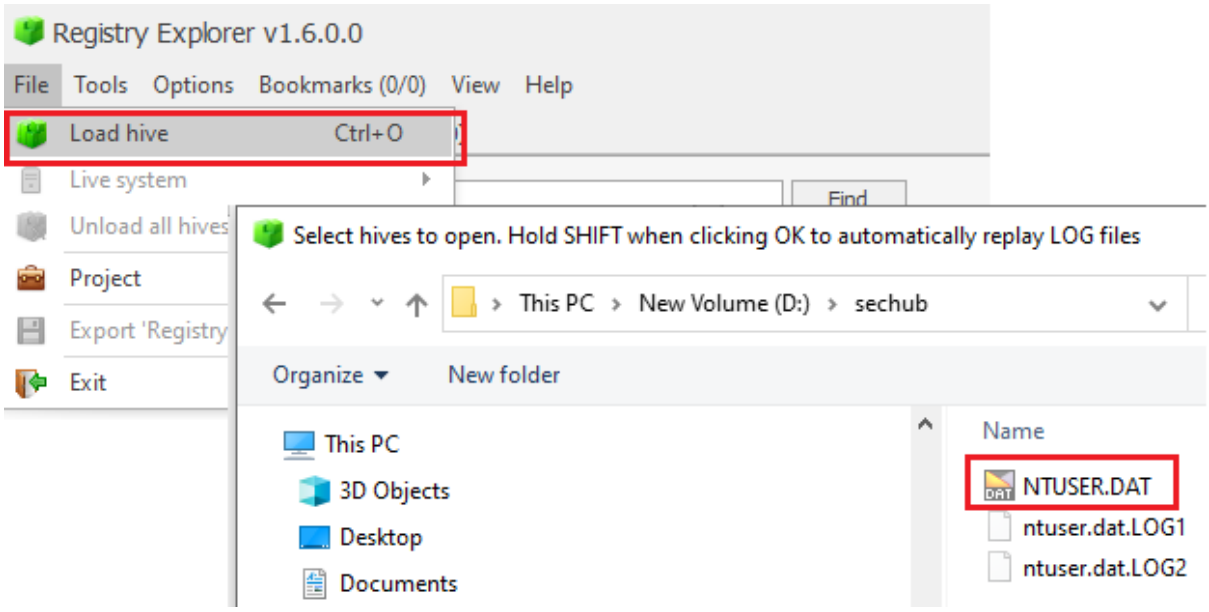
4.3 Registry Explorer

It's free and powerful; what else do we want! It is highly recommended to download the tool and give it a try. It has an amazing user manual covering both the GUI based Registry Explorer and RECmd command-line tool.



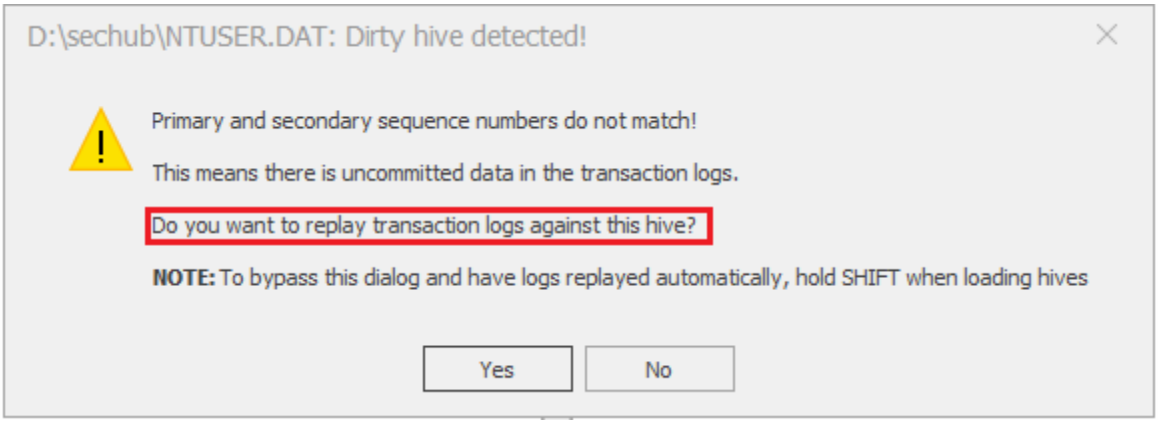
Registry Explorer and RECmd

Load the NTUSER.DAT hive from the file menu:



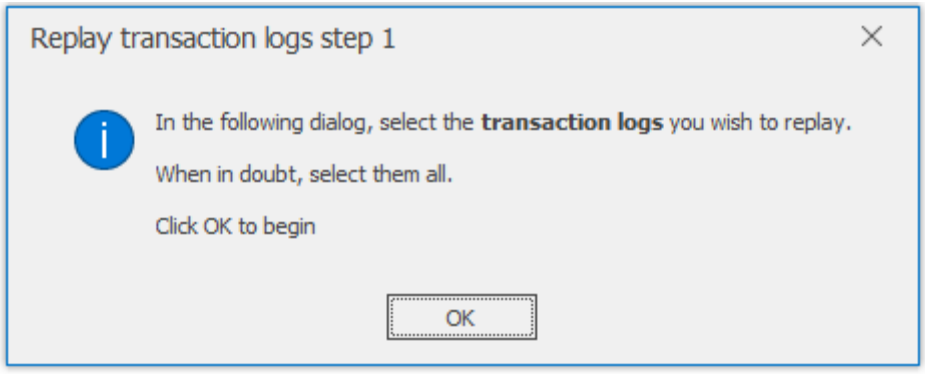
Load NTUSER.DAT Hive

As expected, we will face a warning message that shows that the “primary and secondary sequence numbers do not match. “ Oh.. we know what does it mean!



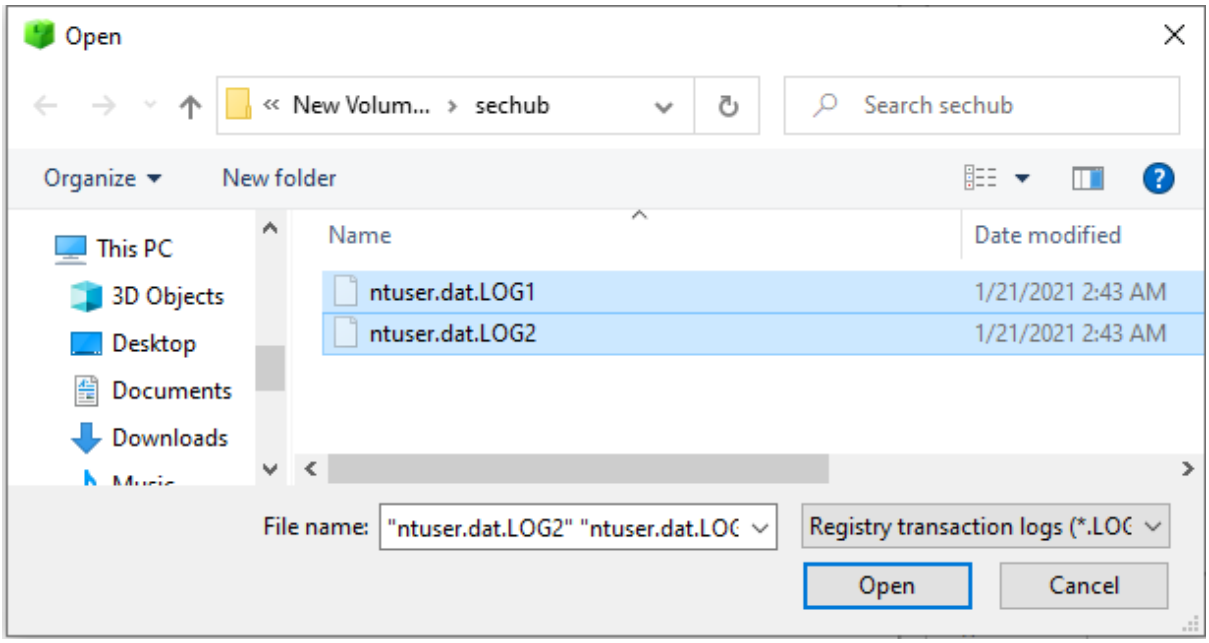
Dirty Hive Warning

We can also press No and open the NTUSER.DAT as it is, but why would we do that! Let's press yes and replay the transaction logs to update our primary file.



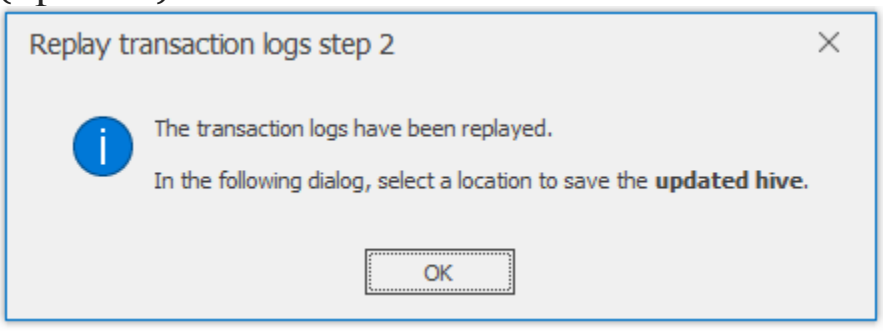
Replay Transaction Logs

Just click on the ok and select the ntuser.dat.LOG1 and ntuser.dat.LOG2.



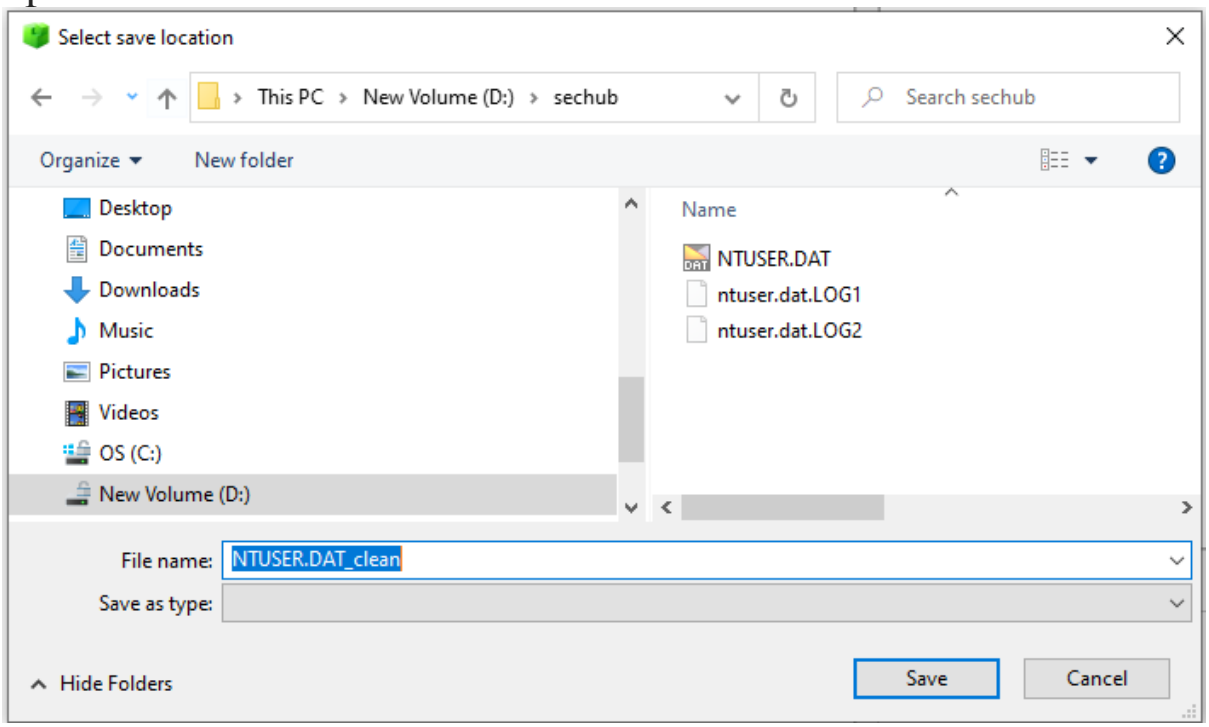
Select ntuser.dat.LOG1 and ntuser.dat.LOG2

It will be quick, and we need to click the OK button to save the clean (updated) version of the NTUSER.DAT in the desired location.



Save the Updated Hive

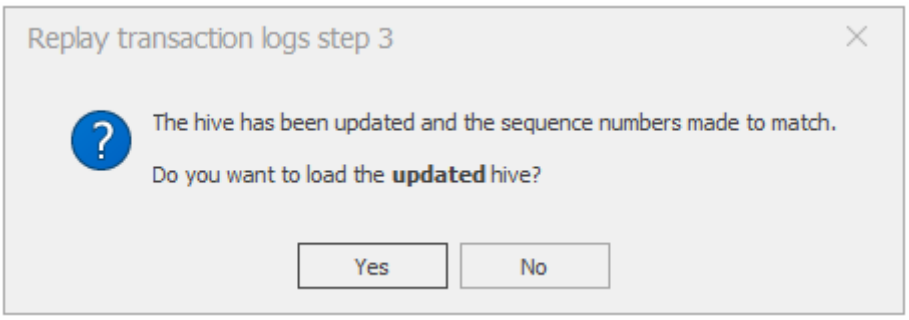
The NTUSER.DAT_clean name is automatically given to the updated version.



Save the Updated Hive File

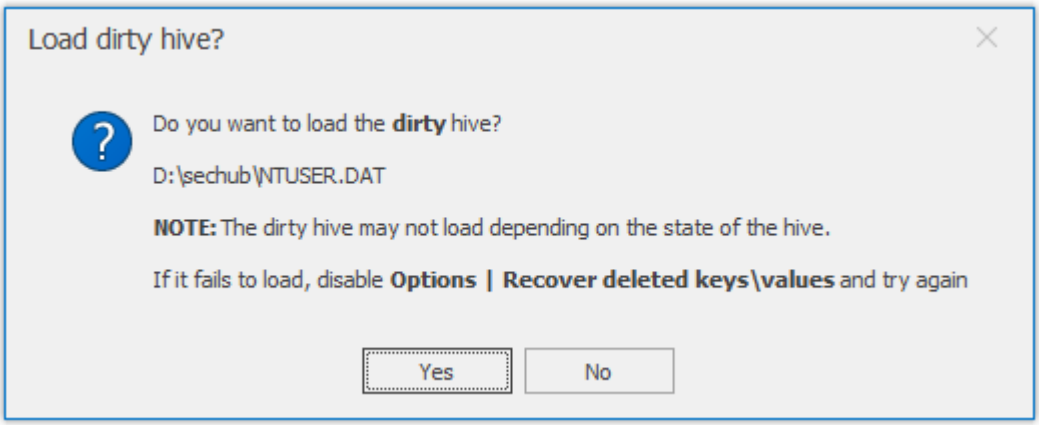
Note: *By holding shift while loading the NTUSER.DAT file at the beginning we can shorten the above process and let the logs replayed automatically. However, the updated primary file will reside on memory only and we will not have a copy of clean NTUSER.DAT on the hard disk.*

The saved file has exact similar sequence numbers as it's updated now. We can load it later or click on the yes and load it now.



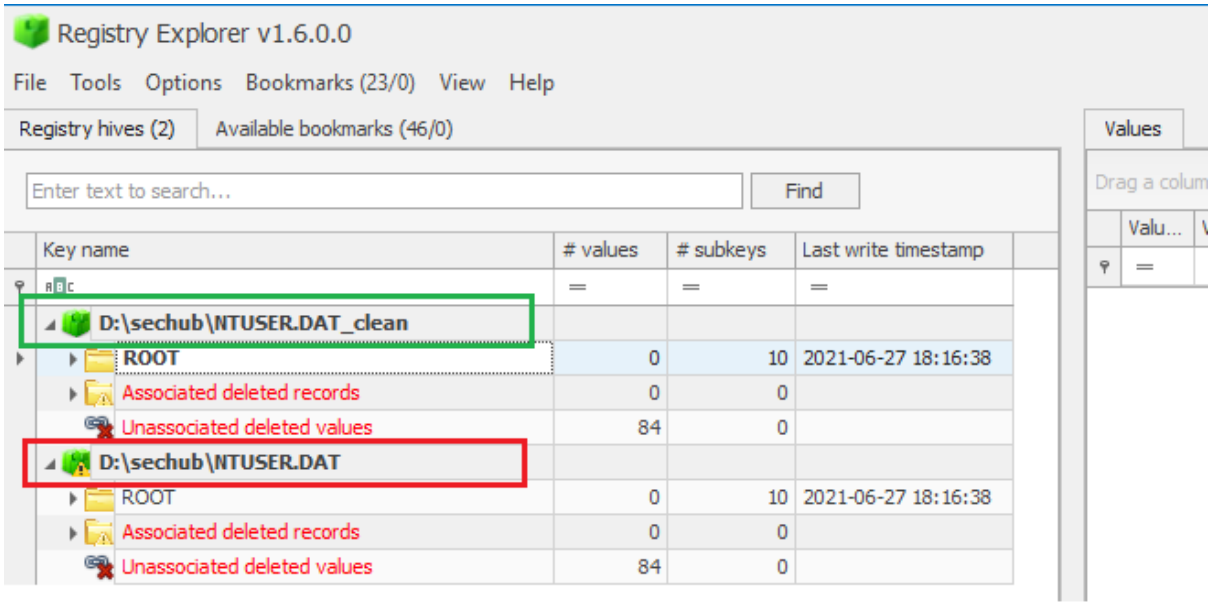
Load the Updated Hive

We have an option to open the old file at the same e time to have a comparison.



Load the Old (Dirty) hive

We can work with both the clean and the dirty hives at the same time:



The Dirty and Clean NTUSER.DAT Loaded in Registry Explorer

Done! we can now enjoy the investigation. Are you wondering what we should look for and what we can have by analysing the NTUSER.DAT?

Stay tuned; the next post will discuss the forensics values of the NTUSER.DAT and their locations in the hive.