Lab 1.4 User Account Profiling

Teoría

y

Practica

Windows Registry

El registro (registry) es una colección de archivos de base de datos que almacenan datos de configuración vital para el sistema. Almacena información sobre **software, hardware y componentes del sistema**.

El registro puede detallar el software que se ha instalado, la configuración del sistema, los archivos usados recientemente y los programas de inicio. El registro se puede ver y manipular utilizando "regedit.exe".

El registro tiene **four root keys**:

1. HKEY_CLASSES_ROOT
2. HKEY_CURRENT_USER
3. HKEY_LOCAL_MACHINE
4. HKEY_USERS.

El registro se puede acceder tanto en un sistema en funcionamiento como sin conexión. o. La mayoría de los archivos se almacenan en el directorio **\%WINDIR%\system32\config**. Estos archivos de registro se denominan **DEFAULT, SAM, SECURITY, SOFTWARE y SYSTEM**. Los archivos corresponden a su significado en el registro.

Todos estos archivos del sistema residirían bajo la clave (Hive) **HKEY_LOCAL_MACHINE** en su sub-significado **SAM, SECURITY, SOFTWARE y SYSTEM**. La clave HKEY_LOCAL_MACHINE contiene la configuración del sistema, los archivos de inicio, la configuración de la máquina y otros archivos predeterminados.

- **El archivo(hive) SYSTEM** almacena el **HKEY_LOCAL_MACHINE\SYSTEM**, incluida la configuración de hardware y servicios. También enumerará la mayoría de los nombres de dispositivos en bruto para volúmenes y unidades en el sistema, incluidas las USB Keys.

- **El archivo(hive) SOFTWARE** almacena datos del **HKEY_LOCAL_MACHINE\SOFTWARE**, donde se encuentran todas las configuraciones de las aplicaciones. Los programas/productos de Windows también tienen sus configuraciones almacenadas aquí.

- **El archivo (hive) NTUSER.DAT** contiene la configuración y ajustes del entorno, lo que incluye una gran cantidad de datos identificables relacionados con la actividad del usuario.

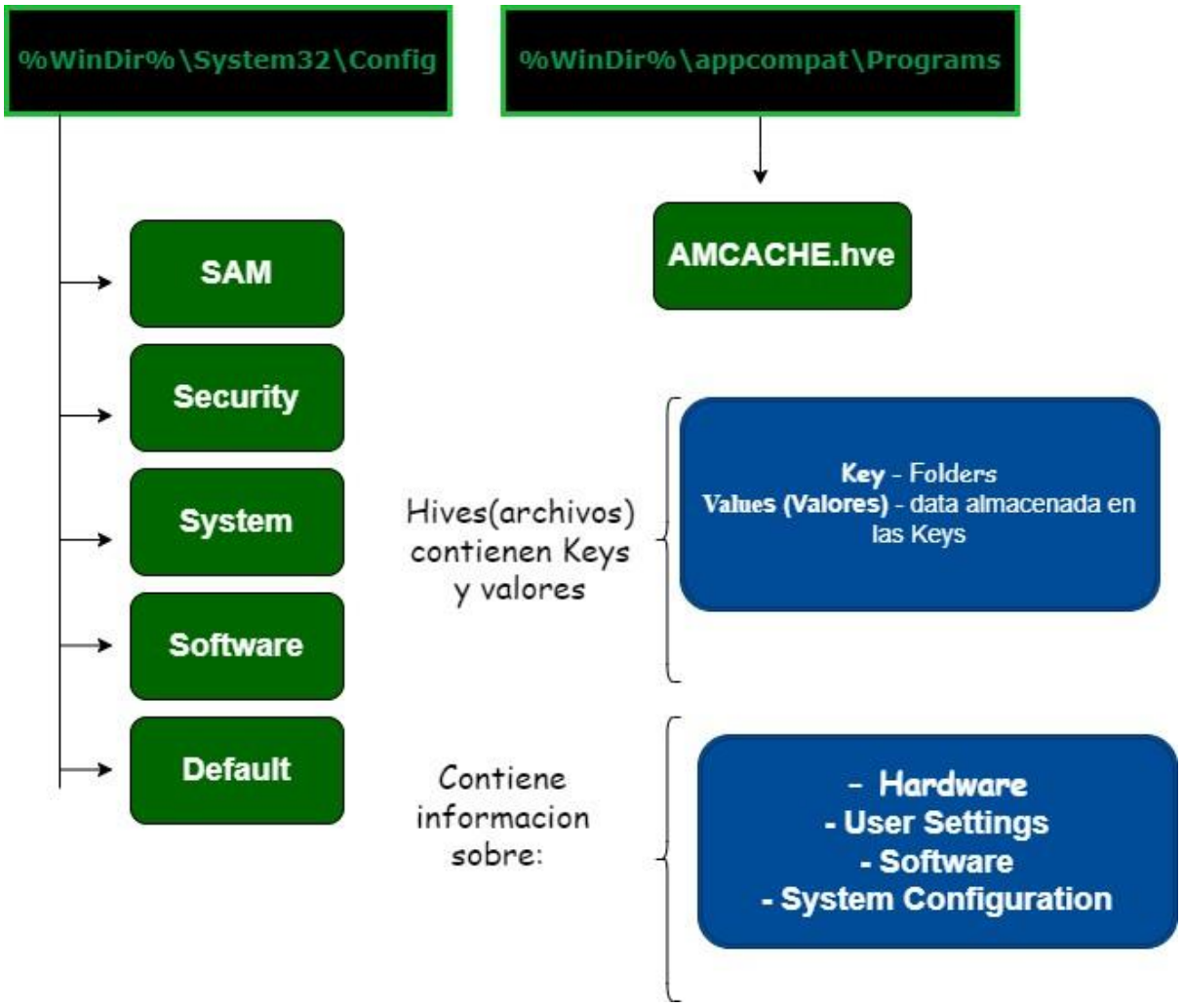
- **El archivo (hive) SAM** contiene todas las cuentas de usuario locales y grupos. Se encuentra en su sistema en **HKEY_LOCAL_MACHINE\SAM.**

- **El archivo (hive) SECURITY** contiene toda la información de seguridad utilizada por el SAM y el sistema operativo, incluidas las políticas de contraseñas, la información de membresía de grupos y más

- **El nuevo archivo AMCACHE.HVE** hizo su debut **en Windows 8** pero ha sido agregado a Windows 7 a través de actualizaciones. **Este archivo se utiliza para la capacidad interna de**

compatibilidad de aplicaciones que permite que Windows ejecute binarios más antiguos encontrados en versiones anteriores de sus sistemas operativos

Podemos resumir lo de arriba en lo siguiente:



User Registry Hives

Cada usuario que ha utilizado la máquina tendrá esta sección: **%UserProfile%.**

El registro se puede usar para enumerar los archivos más recientemente utilizados. También puede mostrar los últimos archivos que se ha buscado en el disco duro o también puede mostrar las últimas URL que se han escrito en las ventanas del navegador.

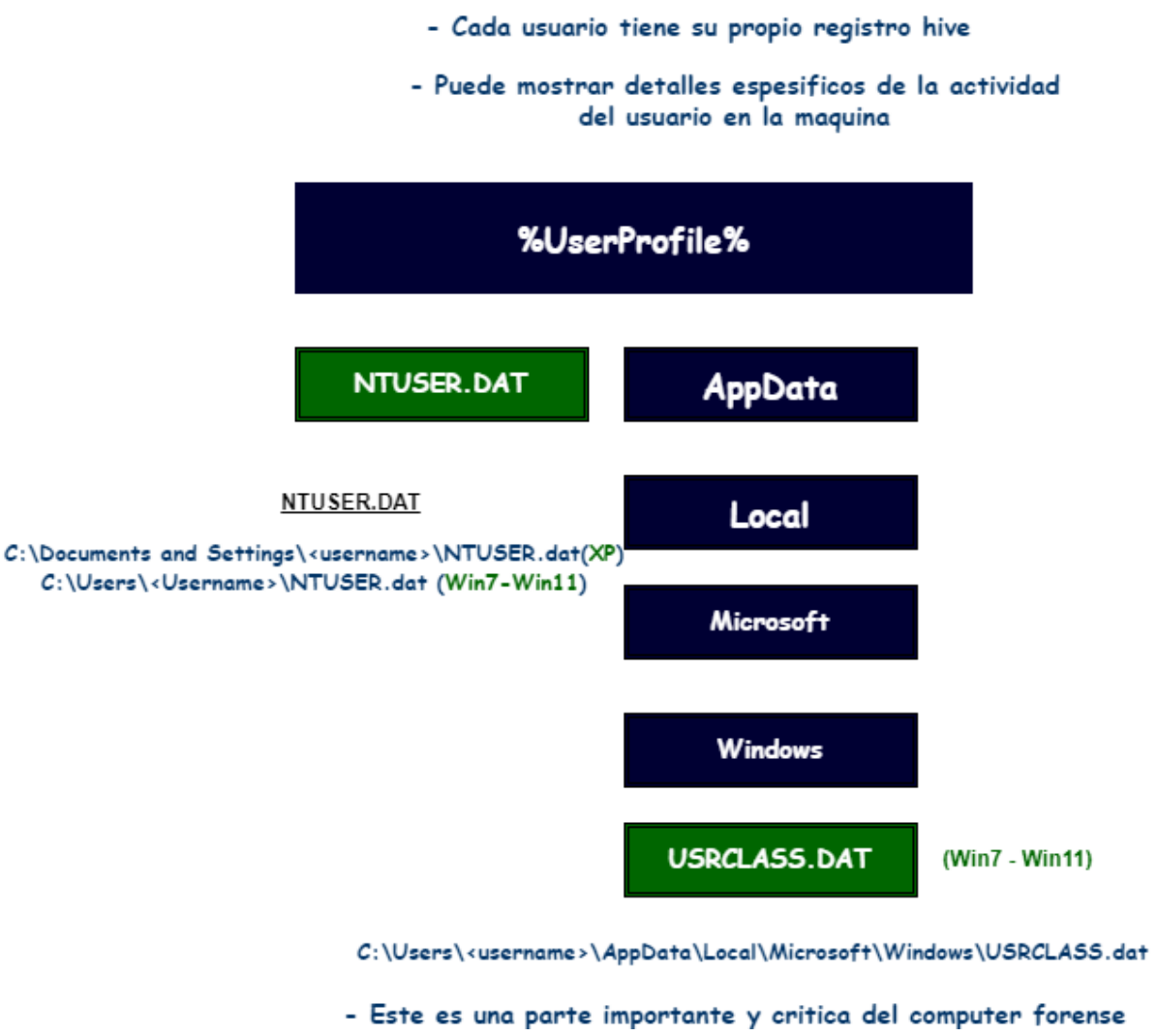
Puede mostrar los últimos comandos ejecutados en el sistema, así como los archivos que se abrieron. También puedes ver qué archivos se guardaron por última vez en el sistema Windows.

El hive NTUSER.dat contiene todas las claves relacionadas con el usuario específico. Se encuentra en el sistema en **HKEY_CURRENT_USER**.

En sistemas Windows 7-10, hay un hive adicional creado en **C:\Users\<username>\AppData\Local\Microsoft\Windows\UsrClass.dat**.

Este hive es muy importante porque contiene información clave sobre la ejecución adicional de programas y nos dará la capacidad de saber qué carpetas ha abierto o cerrado un usuario. El propósito principal de **UsrClass.dat** es ayudar en la raíz de registro virtual para el **User Account Control (UAC).** Existe una clave para cada extensión de nombre de archivo registrado. El registro virtualizado de UAC se encuentra en la **clave VirtualStore.**

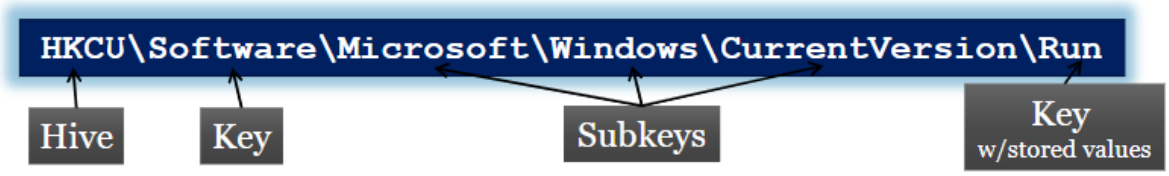
Lo podemos resumir en lo siguiente:



Hasta ahora tenemos lo siguiente sobre registry keys, values y y registry hives

Key: Son similares a los **folders y subfolders**, respectivamente **keys y subkeys**, los mismos producen una jerarquía de **folder/directorio**

Values: Datos almacenados dentro de una key, contiene data en forma de : **string, binary data, integers, lists.**



En cuanto a los registry hives, no son mas que colecciones de archivos llamados hives(archivos, valga la redundancia).

Los hives del registro en una máquina en vivo y encendida lucen muy diferentes de lo que lo harían al analizar una máquina sin conexión. La mayoría de las personas, al leer sobre los hives del registro en línea (maquina encendida) , se encontrarán con su nombre formal.

- **HKEY_LOCAL_MACHINE (HKLM)**
  - SAM
  - Security
  - SYSTEM
  - SOFTWARE
- **HKEY_CURRENT_USER(HKCU)**
  - NTUSER.DAT

Estos se encuentran comúnmente cuando ejecutas **regedit**, y fácilmente puedes abrir la clave **HKEY_LOCAL_MACHINE** y ver las subclaves, que incluyen nuestros cuatro archivos principales de hive (SAM, Security, System y Software) del directorio **C:\Windows\System32\config**. En resumen, sus apodos reducen HKEY_LOCAL_MACHINE a HKLM cuando se escriben.

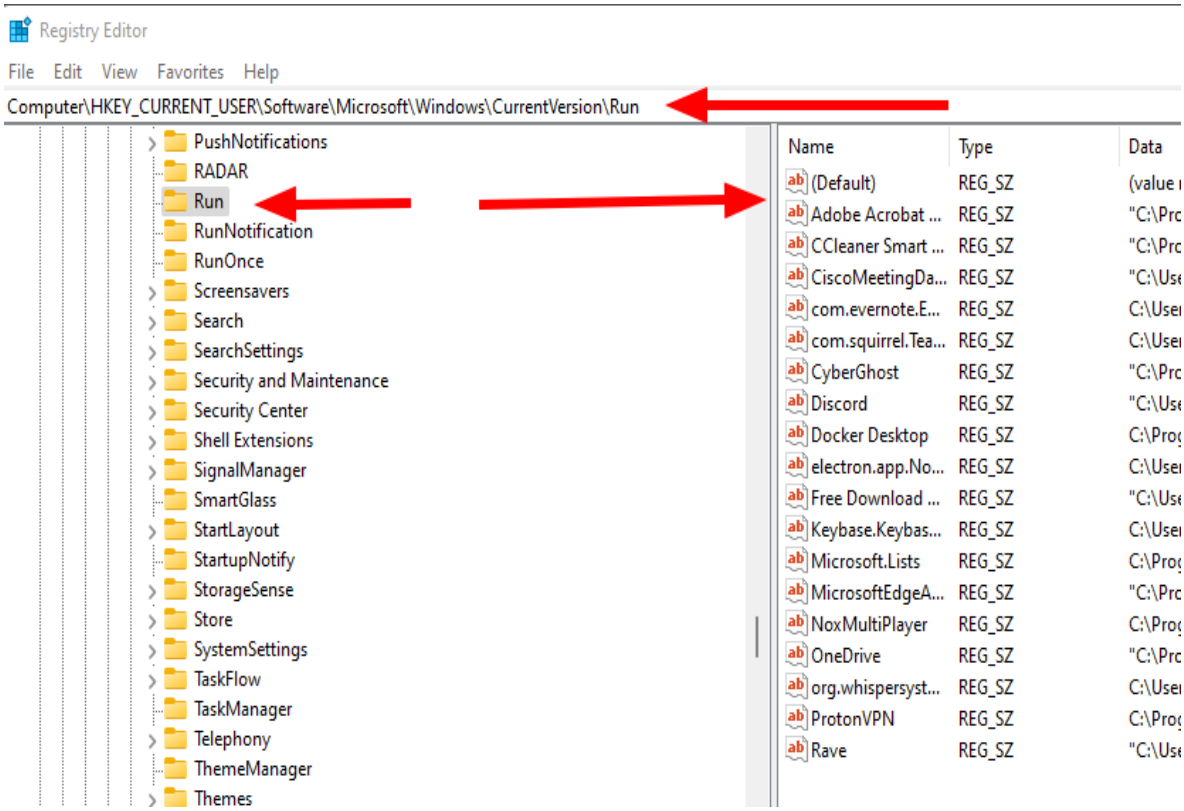
Registry Hive	Nickname	File
HKEY_LOCAL_MACHINE\SAM	HKLM\SAM	SAM
HKEY_LOCAL_MACHINE\Security	HKLM\Security	SECURITY
HKEY_LOCAL_MACHINE\System	HKLM\System	SYSTEM
HKEY_LOCAL_MACHINE\Software	HKLM\Software	SOFTWARE

HKEY_USER o HKEY_CURRENT_USER	HKCU	NTUSER.DAT

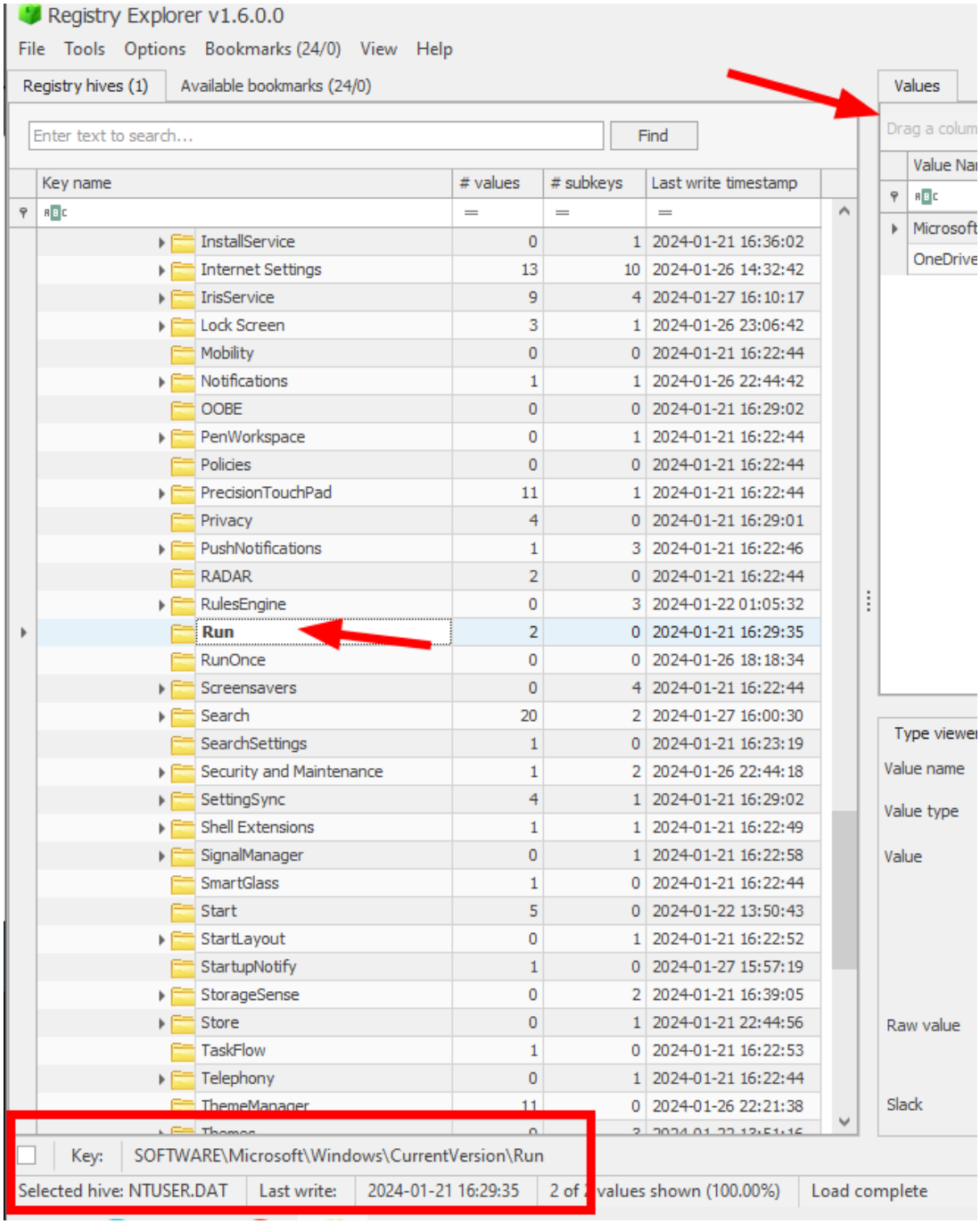
Cuando estás examinando el hive de un usuario, generalmente estás navegando hacia **HKEY_USER (si más de un usuario está conectado)** o HKEY_CURRENT_USER **(el usuario actualmente conectado).**

De esto podemos destacar dos cosas:

1. Online (Maquina encendida): Usamos regedit.exe



2. Offline: Para esto nos apoyamos de una herramienta llamada Registry Explorer, tan fácil como clickear “Open Registry Hive”



Colectando información del usuario: Analizando SAM hive

O

El arte de profiling Users y Groups

Perfilando a un usuario es críticamente importante para un caso. Es útil saber con qué frecuencia un usuario ha iniciado sesión en una máquina específica, la última vez que inició sesión, el último inicio de sesión fallido y la política de contraseñas.

SAM: Profiling Users/ Groups
Username
Relative Indentifier (RID)
User Login Information
• Last Login • Last Failed Login • Logon Count (not incremented if using an MS account to log in) • Password Policy • Account Creation Time
Group Information
• Administrators • Users • Remote Desktop Users

Además, muchos programas, como el Recycle Bin, utilizan el RID (Identificador Relativo – Relative Identifier) del usuario en lugar del nombre de usuario. Es importante examinar cómo buscar este residuo en una máquina durante una investigación.

En un sistema multiusuario, ***¿cómo pueden mapear un RID al usuario original si solo tienen una imagen de disco para examinar?***

Respuesta: Deben examinar el archivo de registro SAM donde se administran las cuentas para ver qué usuario está mapeado con qué RID

Profiling Local Users
Proposito
- **Enumera las cuentas locales del sistema y sus identificadores de seguridad equivalentes.**

Ubicacion
- **SAM\Domains\Account\Users**
¿Porque esto es importante?
- Descubrir el nombre de usuario y el RID asignado a ellos - Capaz de ver una variedad de información relacionada con la actividad del usuario. 1. Last Login 2. Last Failed Login 3. Logon Count 4. Password Policy 5. Account Creation Time

El primer lugar donde buscaremos información es en el **SAM**. El hive SAM nos ayudará a enumerar todos los usuarios que tienen un perfil en la máquina. Si nuestra máquina es parte de un dominio, el archivo **SAM que contiene los perfiles de usuario estará ubicado en el Controlador de Dominio.**

Varias cosas podemos realizar:

1**) Vincular un nombre de usuario a un RID (Identificador Relativo):** Hay muchos artefactos en una máquina con Windows que apuntan al RID de un usuario y **no a su nombre de usuario**. Es importante documentar el nombre de usuario y el RID correspondiente para fines posteriores. Este es un paso muy importante.

2) Perfilando al usuario: Es increíblemente importante perfilar a un usuario de una máquina basado en sus hábitos de inicio de sesión y errores. Puede ver fácilmente el último inicio de sesión de cada usuario y el número total de inicios de sesión que ha realizado este usuario. Ambos son importantes porque podrían indicarle qué tan activo podría ser un usuario específico en una máquina.

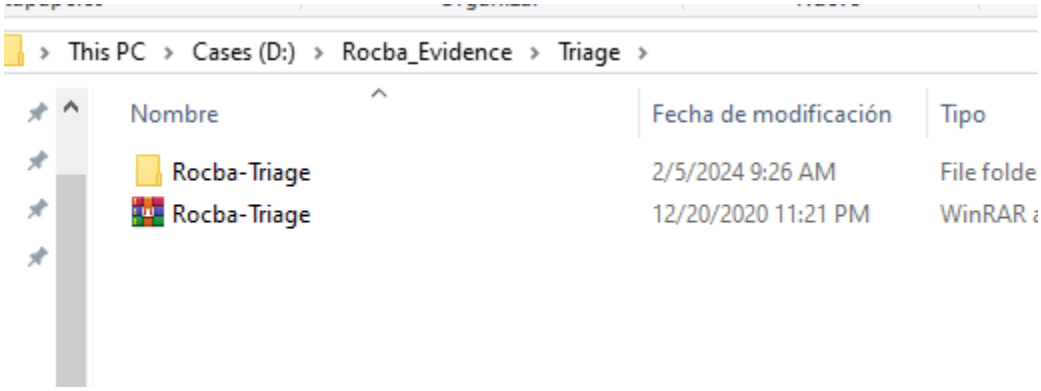
Nota: **El conteo de Último Inicio de Sesión no se incrementará si se utiliza una cuenta de MS. Una cuenta local (no MS) seguirá incrementándose.**

Laboratorio 1.4 : User Account Profiling

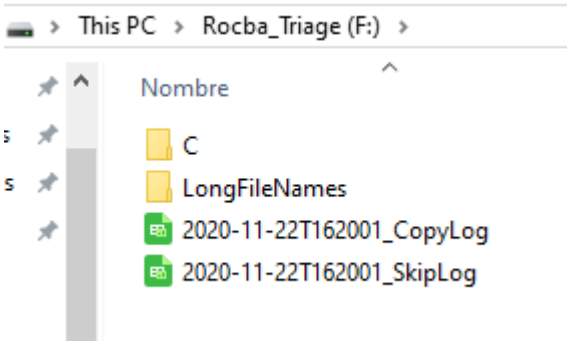
Objetivos:

- El perfilado y la comprensión de las cuentas de usuario son críticos para asegurarse de no cometer errores fáciles mientras se realiza un análisis más complejo posteriormente. Con el análisis del hive del registro SAM, un analista puede documentar las cuentas de usuario locales asociadas con el sistema, buscar elementos que ayuden a responder preguntas investigativas e identificar anomalías. Podrás determinar cuándo se crearon las cuentas, cuándo iniciaron sesión por última vez e incluso si las cuentas son del nuevo tipo de cuenta "Cloud" de Microsoft.

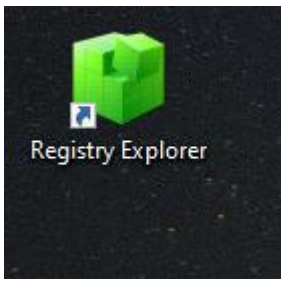
Lo primero que tenemos que realizar es montar nuestra evidencia, para esto en el disco attacheado en la ruta (en mi caso) esta en la siguiente:



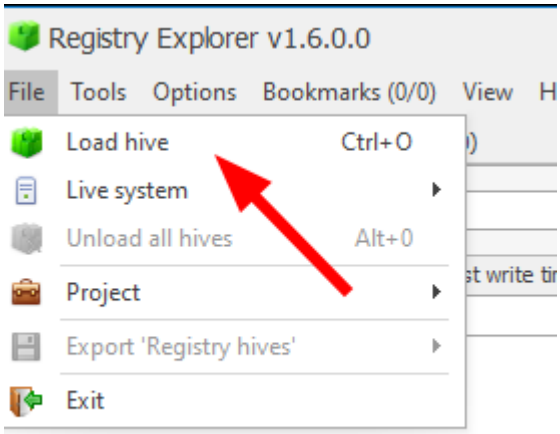
Le damos doble click para montar la evidencia.



Ahora lanzamos desde el escritorio Registry Explorer

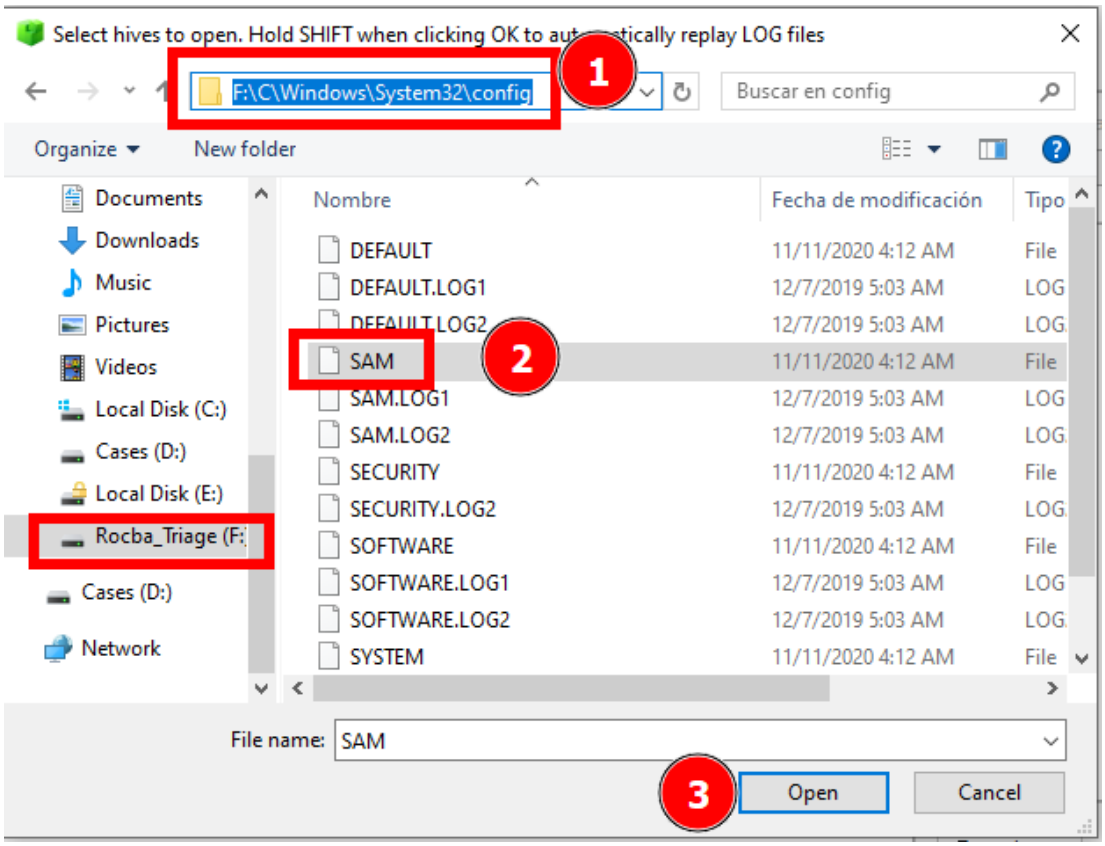


Seleccionamos File – Load hive

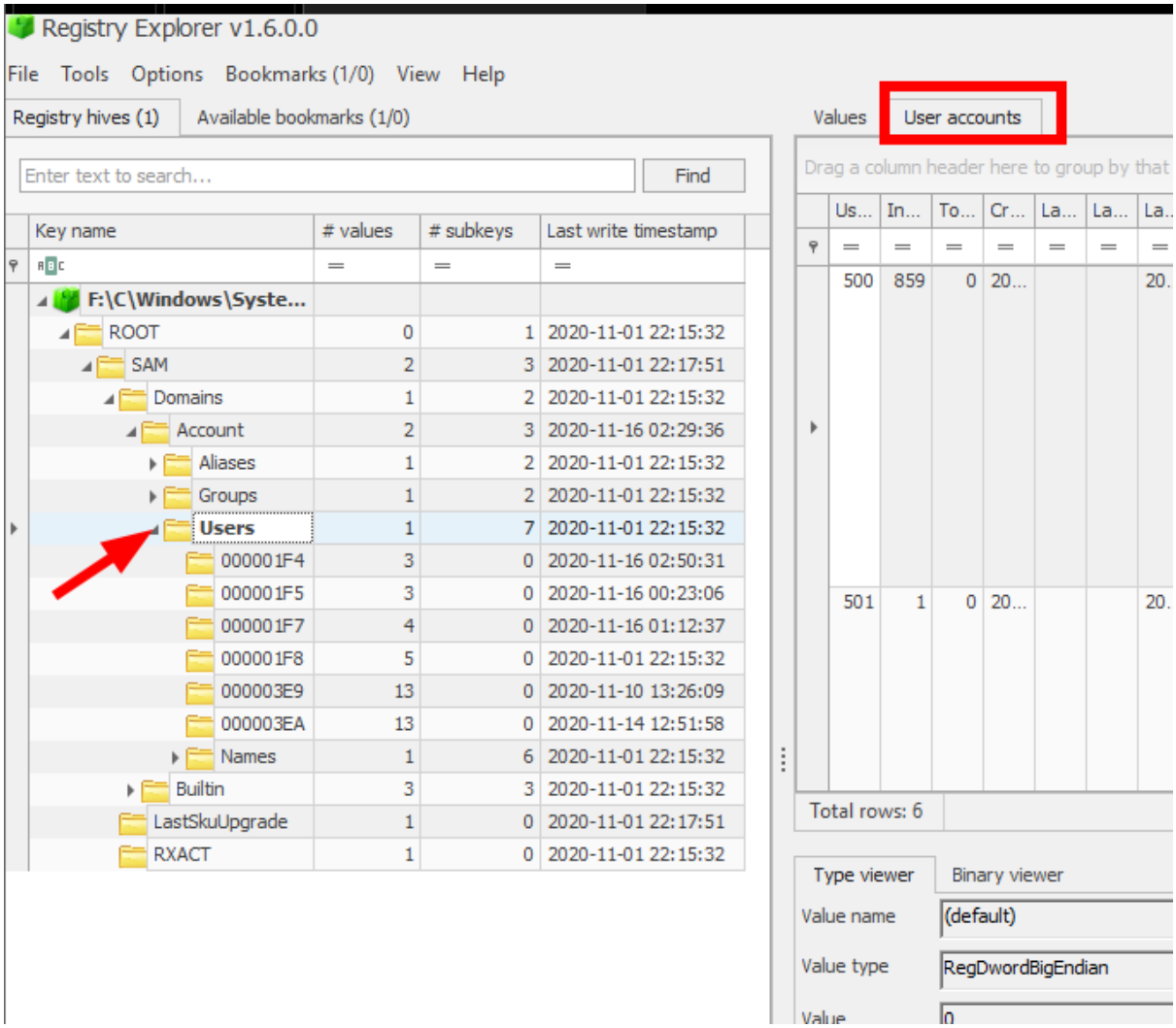


Buscamos el Hive offline en la ruta **F:\C\Windows\System32\Config\SAM**

Nota: La unidad lógica puede variar.



Ahora, dentro del Registry Explorer, vamos a navegar hacia **SAM\Domains\Account\Users** y seleccionamos el Key “Users”

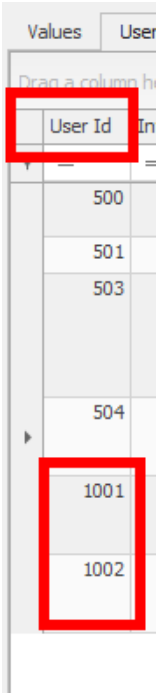


La primera columna en el complemento Registry Explorer User Accounts se llama **User Id** y representa un valor que Microsoft llama "**Identificador relativo** (RID)". Los valores RID de **1000 o más** están reservados para cuentas de usuario y aquellos por debajo de ese valor se utilizan para **cuentas del sistema.**

¿Cuántas cuentas de usuario están presentes en este hive SAM?

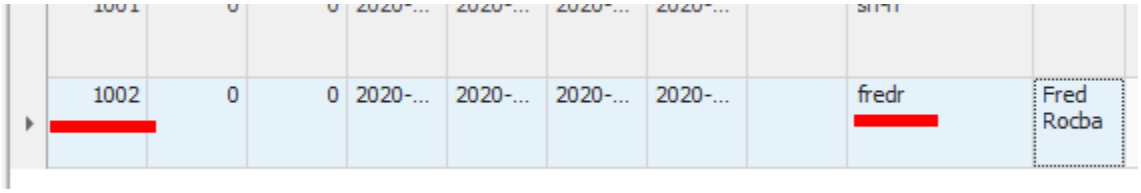
- User Id (RID) = 1001
- User Id (RID) = 1002

Estos valores RID serán importantes más adelante porque algunos artefactos se hacen referencia según el **RID de la cuenta en lugar del nombre de la cuenta** (Papelera de Reciclaje y SRUM son dos ejemplos destacados).



¿Cuál es el nombre de usuario para la cuenta de Fred Rocba y cuál es su valor de Id de usuario?

- **Fredr**
- **User Id (RID) = 1002**



¿De qué grupos era miembro la cuenta de Fred Rocba?

- **Administrators**
- **Users**

User Name	Full N...	Pass...	Groups	U
Administrator			Administrators	
Guest			Guests	
DefaultAccount			System Managed Accounts Group	
WDAGUtilityAccount				
srl-h			Administrators, Users	
fredr	Fred Rocba		Administrators, Users	

¿Cuándo fue la última vez que hizo login la cuenta de fredr?

Last Login Time	Last ...	Last...	Expir...	User Name
		202...		Administrator
		202...		Guest
		202...		DefaultAccount
	2020-...			WDAGUtilityAccount
2020-11 13:26:09	2020-...	202...		srl-h
2020-11-14 12:51:58	2020-...	202...		fredr

¿Cuántas de las built-system accounts (RID < 1000) se han utilizado en el sistema?

Ninguna de las cuentas built-system parece haber tenido un inicio de sesión, como lo evidencia la falta de valores de "Última hora de inicio de sesión" y "Total de conteo de inicio de sesión = 0".

User Id	Invalid...	Total Login Count	Creat...	Last Login Time	L
500	859	0	2020-...		
501	1	0	2020-...		
503	1	0	2020-...		
504	0	0	2020-...		

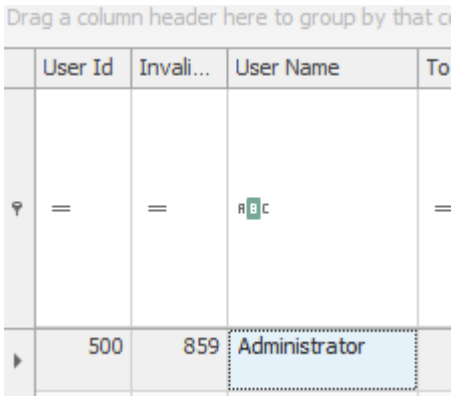
¿Por qué el Conteo total de inicio de sesión es igual a 0 para la cuenta de fredr?

Aunque no sea evidente en esta salida, una explicación discutida en las diapositivas de tu clase es que las nuevas Cuentas de Microsoft ya no actualizan este valor dentro del SAM. Dado que hay una Última hora de inicio de sesión, esperaríamos que el Total de conteo de inicio de sesión fuera mayor que cero.

¿Cuál es el Conteo de Inicios de Sesión Inválidos para la cuenta del Administrador?

Se registraron 859 intentos de inicio de sesión inválidos para la cuenta de Administrador (RID 500)

Esto se parece mucho a un ataque por fuerza bruta. La buena noticia es que no vemos ningún inicio de sesión válido (Total de Inicios de Sesión = 0 para esta cuenta)



¿Por qué la hora del último cambio de contraseña es anterior a la hora de creación de la cuenta de fredr?

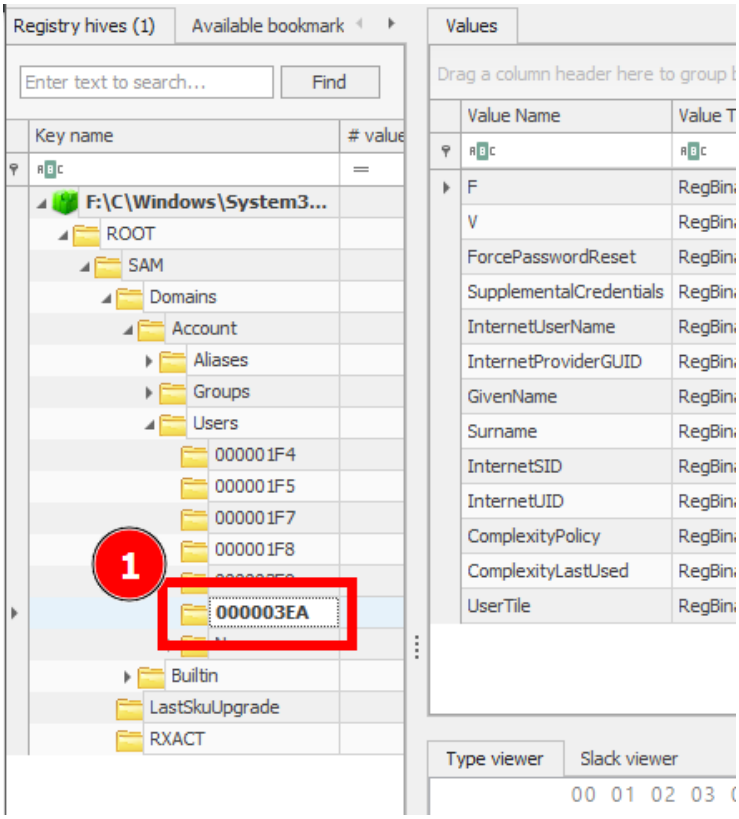
Este es un excelente ejemplo de algo que esperaríamos que identificaras al mantener una "mente investigadora sólida".

Siempre estamos atentos a las anomalías, ¡y Windows proporciona muchas! Crear una hipótesis para esta pregunta realmente requiere algo de experiencia forense. Resulta que las actualizaciones importantes del sistema son conocidas por cambiar muchas marcas de tiempo en el Registro de Windows**. Por lo tanto, una hipótesis podría ser que ocurrió una actualización del sistema el 2020-11-**

01, lo que por alguna razón cambió las horas de creación de las cuentas en el sistema. De hecho, esto es lo que ocurrió y es un fenómeno conocido para las actualizaciones importantes de Windows. Las cuentas existían en el sistema antes del 2020-11-01 y, por lo tanto, tienen marcas de tiempo anteriores a la hora de creación "nueva" asignada. **Para demostrar nuestra teoría, necesitaremos ir al siguiente ejercicio donde documentaremos la última hora de la actualización del sistema.**

Extra- Checking for MS Accounts

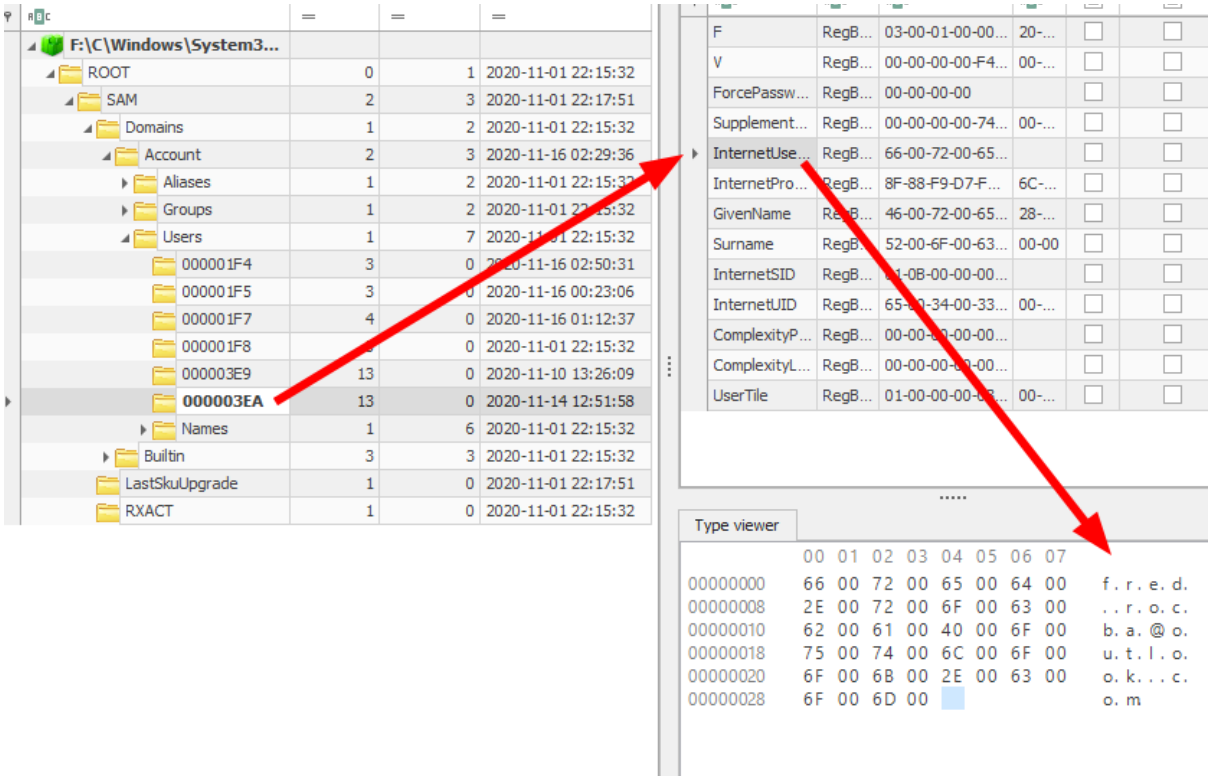
Los datos en bruto de las cuentas de usuario en el registro SAM se almacenan como subclaves(subkeys) bajo la clave(key) **Users.** Cada cuenta tiene una subclave (subkey) nombrada de acuerdo con la representación hexadecimal de su Identificador Relativo (RID). El valor hexadecimal para RID 1002 (fredr) es **3EA**. Haz clic en esta clave para ver los valores en bruto presentes.



Una pista de que esta cuenta en particular es una Cuenta de Microsoft (en la nube) son los valores con "Internet" en sus nombres. Haz clic en el valor InternetUserName y observa los datos en bruto en

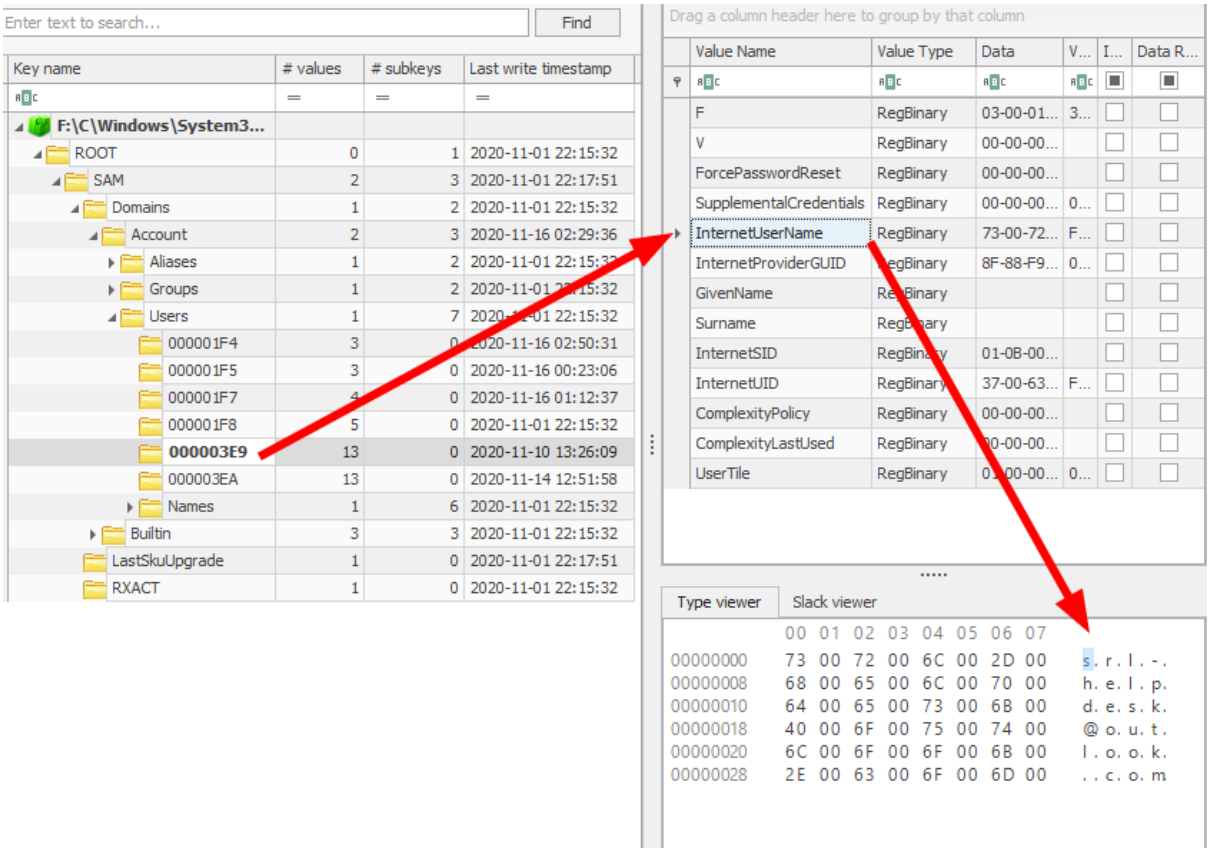
el panel Type Viewer. ¿Qué cuenta de correo electrónico está vinculada a la cuenta fredr?

fred.rocba@outlook.com



¿Es la **cuenta srl-h** una Cuenta de Microsoft? En caso afirmativo, ¿qué correo electrónico está vinculado a esta cuenta?

- Si, srl-h (RID 1001/3E9) es una Microsoft Account igual que la de Fred?
- srl-helpdesk@outlook.com



Datos obtenidos

- El SAM es el más pequeño de los registros, pero es una parada inicial excelente para ver qué cuentas han estado activas en un sistema.

- Determinamos la siguiente información relevante para nuestra investigación:

  - A **Fred Rocba** se le asignó una cuenta llamada fredr:

    - RID 1002

    - Cuenta de Microsoft

    - Vinculada a la dirección de correo electrónico **fred.rocba@outlook.com**

    - Último inicio de sesión el 14 de noviembre de 2020 a las 12:51:58 UTC.

  - La única otra cuenta aparentemente utilizada en el sistema es la cuenta srl-h:

    - RID 1001

- Cuenta de Microsoft

- Vinculada a la dirección de correo electrónico srl-helpdesk@outlook.com

- Último inicio de sesión el 10 de noviembre de 2020 a las 13:26:09 UTC.

- La cuenta de Administrador incorporada en el sistema registró 859 intentos de inicio de sesión fallidos.