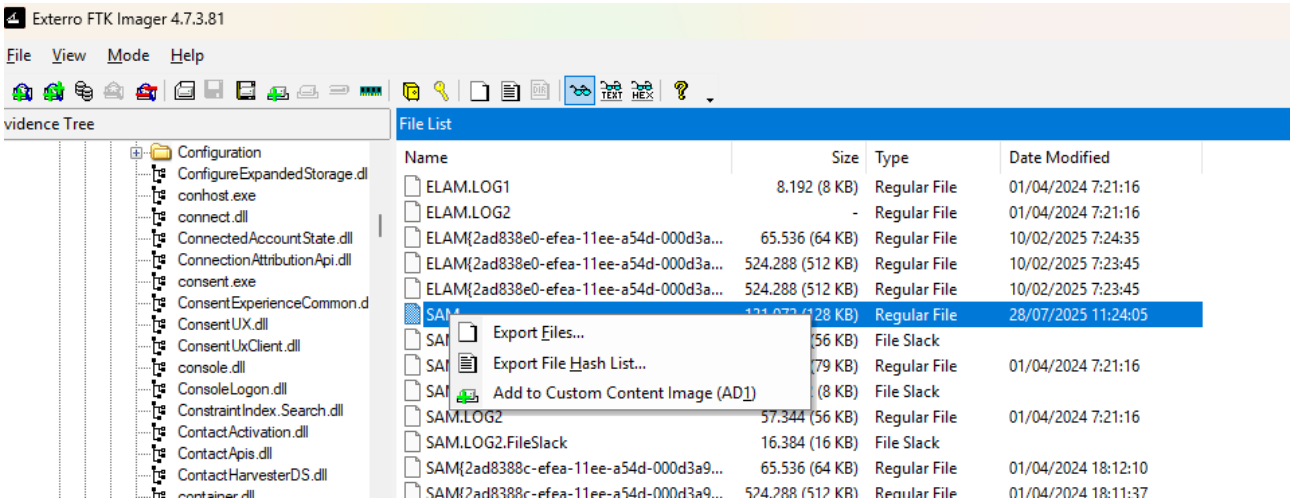
Análisis del Registro de Windows

Comenzamos utilizando **FTK Imager** para la adquisición de la evidencia.
Cargamos nuestro disco con sistema de archivos **NTFS** y navegamos hasta la ruta:

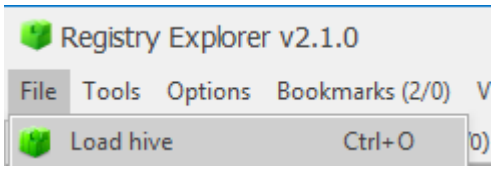
```
Windows\System32\config
```

En esta ubicación se encuentran los principales **hives** del registro de Windows.
En este caso, extraemos el archivo **SAM**, que es el que nos interesa analizar.

El **SAM** (*Security Account Manager*) es uno de los archivos críticos del registro. Contiene la base de datos de cuentas de usuario locales junto con sus contraseñas cifradas, además de otra información de seguridad como los identificadores de seguridad (**SID**) y la pertenencia a grupos.



Ahora usaremos la herramienta RegistryExplorer de Eric Zimmerman para cargar el Hive que hemos descargado anteriormente:



Si vamos al apartado de User podemos ver:

Identificación de la cuenta

- **RID** (*Relative Identifier*) → Identificador único de la cuenta dentro del sistema.
- **Nombre de usuario** (*User Name*).
- **Nombre completo** (*Full Name*) si está configurado.
- **Comentario / Descripción** (*Comment*).

Información de grupos

- **Grupos a los que pertenece** (Administradores, Usuarios, Invitados, etc.).

Fechas y horas importantes

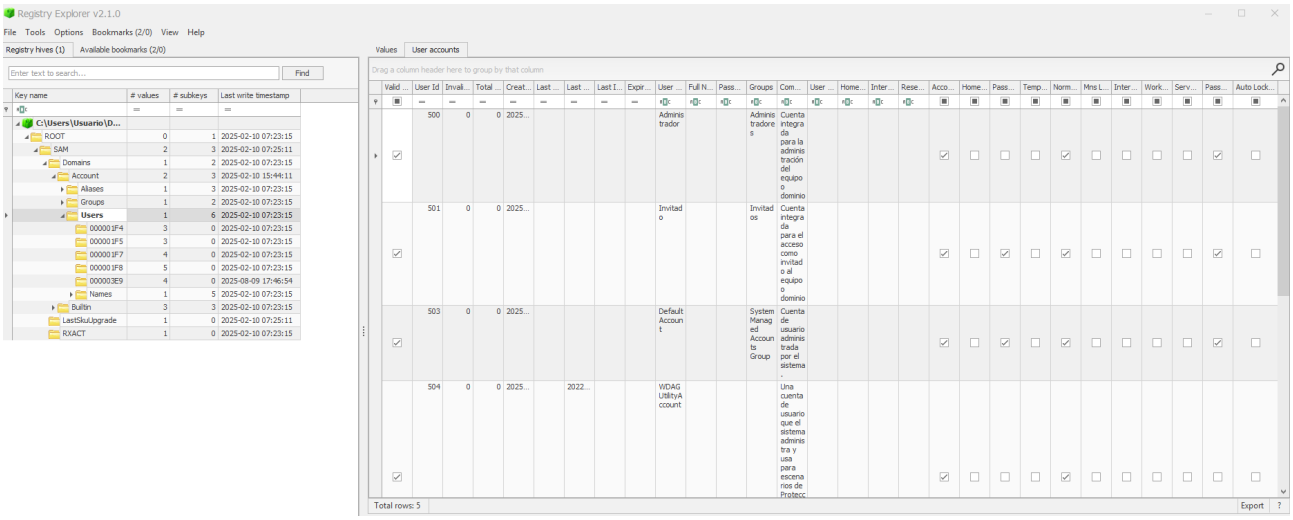
- **Fecha/hora de creación de la cuenta**.
- **Último inicio de sesión** (*Last Login*).
- **Última vez que se cambió la contraseña**.
- **Fecha de expiración de la cuenta** (si está configurada).

Estado y configuraciones

- **Cuenta habilitada o deshabilitada**.
- **Requiere contraseña para iniciar sesión**.
- **La contraseña nunca expira**.
- **Bloqueo de cuenta** (si está bloqueada tras intentos fallidos).
- **Cuenta interna del sistema** (ej. DefaultAccount, WDAGUtilityAccount).

Estos datos son muy valiosos en análisis forense porque permiten:

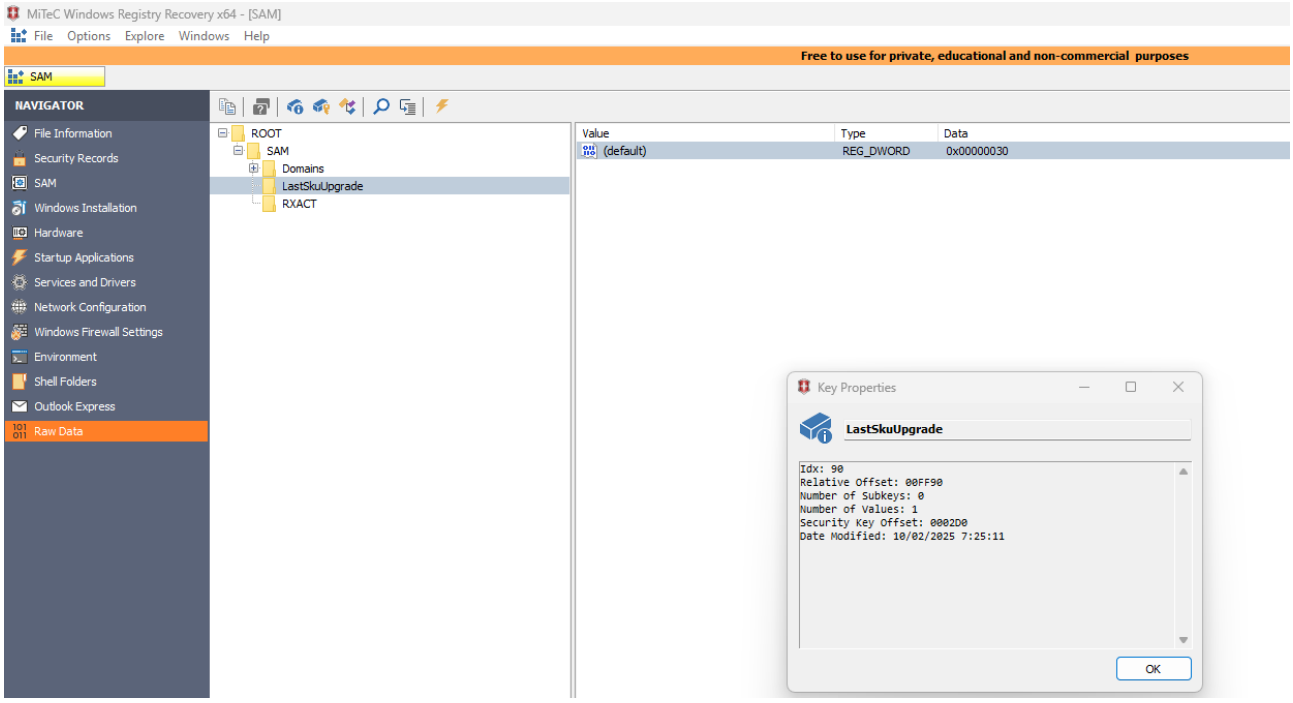
- Identificar cuentas sospechosas o recién creadas.
- Determinar si una cuenta fue usada recientemente.
- Saber si se modificaron contraseñas o se intentó ocultar actividad.



Ahora vamos a visualizar el *hive* con otro software llamado **Windows Registry Recovery**.
A primera vista, la interfaz es muy similar al editor de registro habitual de Windows: cada clave aparece junto a su valor correspondiente.

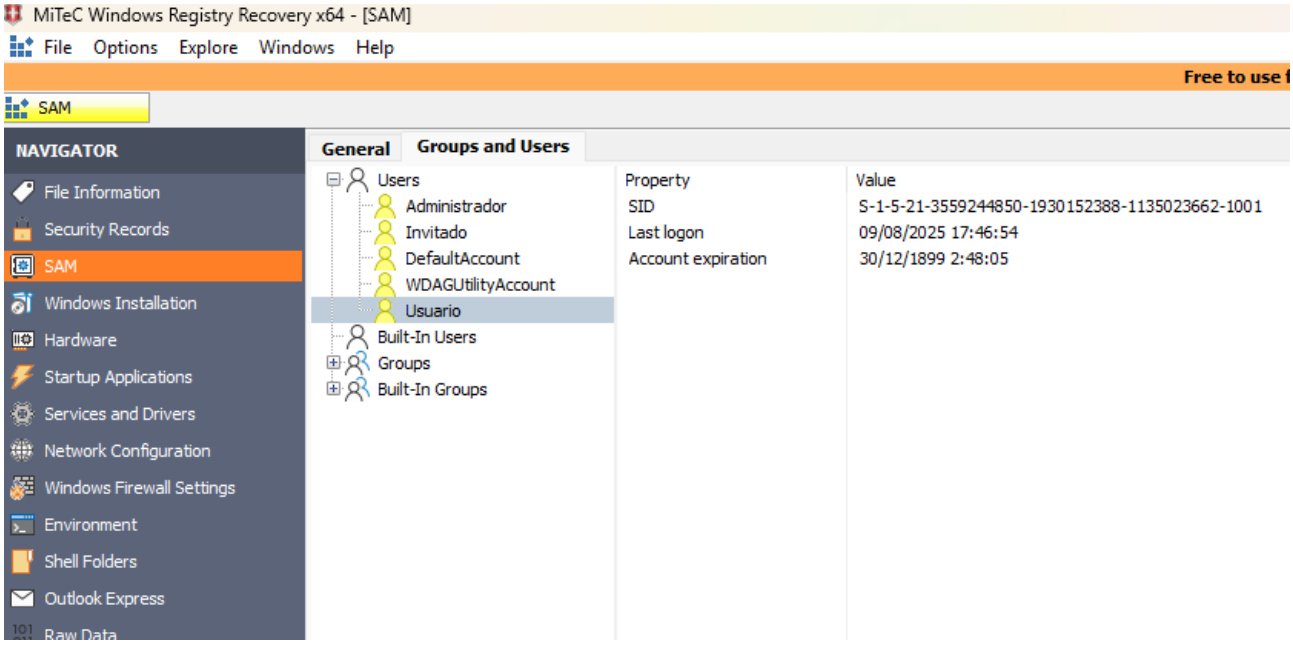
Sin embargo, al tratarse de una herramienta forense, ofrece funciones adicionales, como la posibilidad de acceder a las **propiedades** de cada clave.

En esta vista de propiedades, además de datos técnicos internos, podemos encontrar información muy útil como el **TimeStamp** (*Date Modified*), que indica la fecha y hora exactas en que esa clave fue modificada por última vez, algo relevante para el análisis temporal de eventos en el sistema.



En este caso, al visualizar los usuarios, se aprecia que la interfaz es más intuitiva que la de **Registry Explorer** de Eric Zimmerman, lo que facilita identificar rápidamente las cuentas locales y su información básica.

Sin embargo, algunos datos específicos —como la fecha exacta de creación de la cuenta— no se muestran en esta vista, por lo que para obtener esa información será necesario recurrir a otros hives del registro o herramientas complementarias que permitan correlacionar la información.



Comparativa práctica

- **Registry Explorer**: más potente para obtener datos detallados (creación, último inicio de sesión, grupos, estados).

- **Windows Registry Recovery**: interfaz más intuitiva, ideal para una revisión rápida de cuentas y valores; muestra claramente la marca temporal (*TimeStamp*) de cada clave, pero no siempre ofrece la misma profundidad de datos.

En la práctica, la combinación de ambas herramientas permite:

1. **Windows Registry Recovery** → revisión rápida y extracción de marcas temporales.

2. **Registry Explorer** → análisis detallado y correlación de datos para reconstruir la actividad de usuarios.