

Análisis del Registro de Windows

Comenzamos utilizando **FTK Imager** para la adquisición de la evidencia.

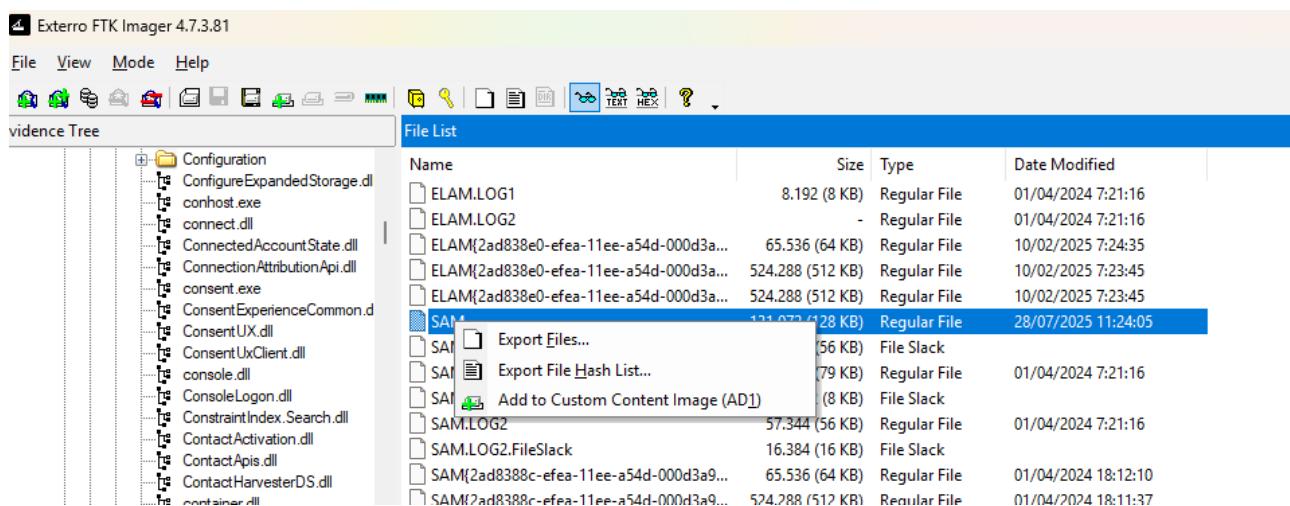
Cargamos nuestro disco con sistema de archivos **NTFS** y navegamos hasta la ruta:

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.

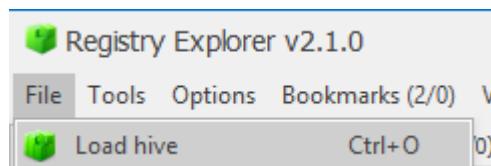
El **SAM** (*Security Account Manager*) es uno de los archivos críticos del registro. Contiene la base de datos de cuentas de usuario locales junto con sus contraseñas cifradas, además de otra información de seguridad como los identificadores de seguridad (**SID**) y la pertenencia a grupos.



The screenshot shows the FTK Imager interface. The Evidence Tree pane on the left displays a folder structure under Configuration, including files like ConfigureExpandedStorage.dll, conhost.exe, connect.dll, ConnectedAccountState.dll, ConnectionAttributionApi.dll, consent.exe, ConsentExperienceCommon.dll, ConsentUX.dll, ConsentUXClient.dll, console.dll, ConsoleLogon.dll, ConstraintIndex.Search.dll, ContactActivation.dll, ContactApis.dll, ContactHarvesterDS.dll, and container.dll. The File List pane on the right shows a table with columns Name, Size, Type, and Date Modified. The SAM file is highlighted in blue and has a context menu open over it. The menu options are Export Files..., Export File Hash List..., and Add to Custom Content Image (AD1). Other files listed include ELAM.LOG1, ELAM.LOG2, and several SAM and ELAM log files with various sizes and dates.

| Name | Size | Type | Date Modified |
|--|------------------|--------------|---------------------|
| ELAM.LOG1 | 8.192 (8 KB) | Regular File | 01/04/2024 7:21:16 |
| ELAM.LOG2 | - | Regular File | 01/04/2024 7:21:16 |
| ELAM{2ad838e0-efea-11ee-a54d-000d3a... | 65.536 (64 KB) | Regular File | 10/02/2025 7:24:35 |
| ELAM{2ad838e0-efea-11ee-a54d-000d3a... | 524.288 (512 KB) | Regular File | 10/02/2025 7:23:45 |
| ELAM{2ad838e0-efea-11ee-a54d-000d3a... | 524.288 (512 KB) | Regular File | 10/02/2025 7:23:45 |
| SAM | 121.072 (128 KB) | Regular File | 28/07/2025 11:24:05 |
| SAM | (56 KB) | File Slack | 01/04/2024 7:21:16 |
| SAM | (79 KB) | Regular File | 01/04/2024 7:21:16 |
| SAM | (8 KB) | File Slack | 01/04/2024 7:21:16 |
| SAM.LOG2 | 57.344 (56 KB) | Regular File | 01/04/2024 7:21:16 |
| SAM.LOG2.FileSlack | 16.384 (16 KB) | File Slack | |
| SAM{2ad8388c-efea-11ee-a54d-000d3a... | 65.536 (64 KB) | Regular File | 01/04/2024 18:12:10 |
| SAM{2ad8388c-efea-11ee-a54d-000d3a... | 524.288 (512 KB) | Regular File | 01/04/2024 18:11:37 |

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.

Registry Explorer V2.1.0

File Tools Options Bookmarks (2/0) View Help

Registry hives (0) Available bookmarks (2/0)

Enter text to search... Find

Values User accounts

Drag a column header here to group by that column

Total rows: 5 Export ?

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.

MiTec Windows Registry Recovery x64 - [SAM]

File Options Explore Windows Help

Free to use for private, educational and non-commercial purposes

NAVIGATOR

- File Information
- Security Records
- SAM**
- Windows Installation
- Hardware
- Startup Applications
- Services and Drivers
- Network Configuration
- Windows Firewall Settings
- Environment
- Shell Folders
- Outlook Express

101 011 Raw Data

Value

| Value | Type | Data |
|------------|-----------|------------|
| 0x00000030 | REG_DWORD | 0x00000030 |

LastSkuUpgrade

Key Properties

Idx: 90
Relative Offset: 00FF90
Number of Subkeys: 0
Number of Values: 1
Security Key offset: 0002D0
Date Modified: 10/02/2025 7:25:11

OK

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.

The screenshot shows the MiTeC Windows Registry Recovery x64 interface. The title bar reads "MiTeC Windows Registry Recovery x64 - [SAM]". The menu bar includes File, Options, Explore, Windows, and Help. A watermark "Free to use!" is visible in the top right. The left sidebar, titled "NAVIGATOR", lists various registry keys: File Information, Security Records, SAM (which is selected and highlighted in orange), Windows Installation, Hardware, Startup Applications, Services and Drivers, Network Configuration, Windows Firewall Settings, Environment, Shell Folders, Outlook Express, and Raw Data. The main pane has tabs "General" and "Groups and Users", with "General" selected. Under "General", there is a tree view under "Users": Administrador, Invitado, DefaultAccount, WDAGUtilityAccount, and Usuario (which is selected and highlighted in blue). To the right of the tree view are columns for "Property" and "Value": Property (SID, Last logon, Account expiration) and Value (S-1-5-21-3559244850-1930152388-1135023662-1001, 09/08/2025 17:46:54, 30/12/1899 2:48:05). Below the tree view are sections for Built-In Users, Groups, and Built-In Groups.

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.

