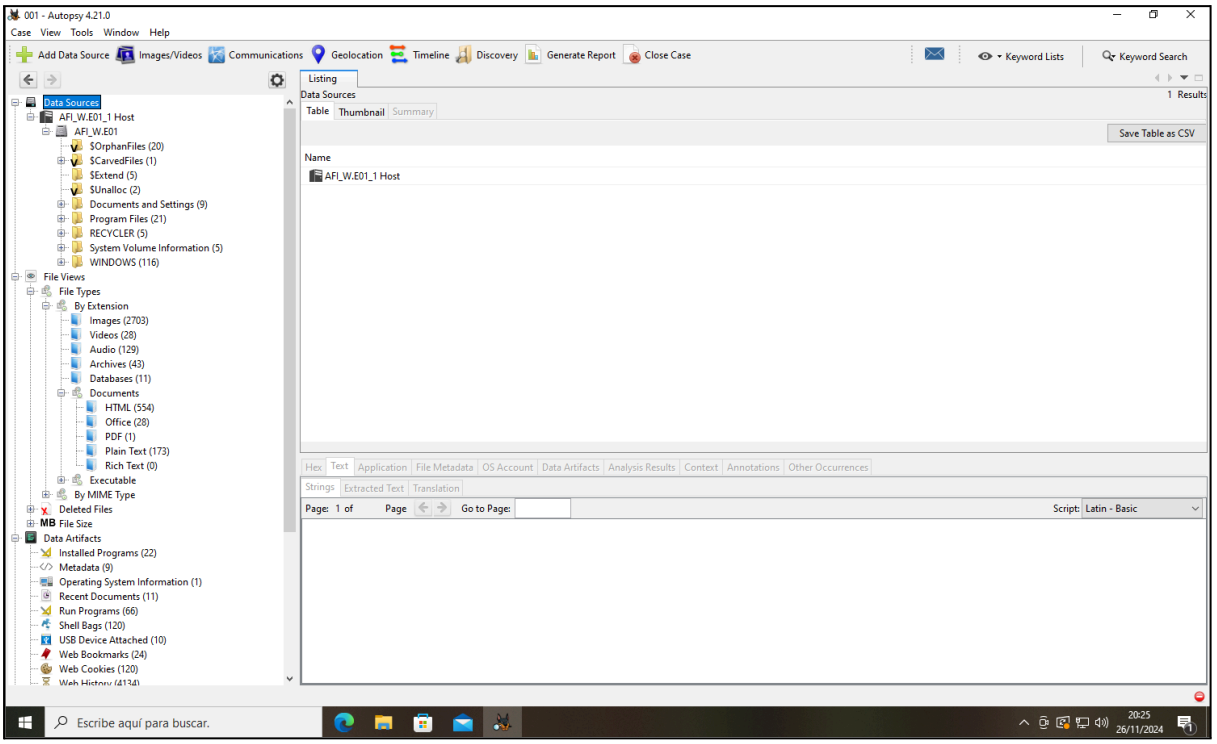
Índice

1. Entorno de trabajo

Para llevar a cabo el análisis forense, se ha configurado un entorno específico que garantiza la precisión y la integridad de los datos. El equipo utilizado para este propósito es un portátil HP Victus, equipado con un procesador Intel i5 12500H, 16 GB de memoria RAM y un SSD de 512 GB, características que aseguran un rendimiento óptimo durante las operaciones de análisis. Adicionalmente, se emplea un disco duro externo para almacenar de manera segura la imagen forense del disco original.

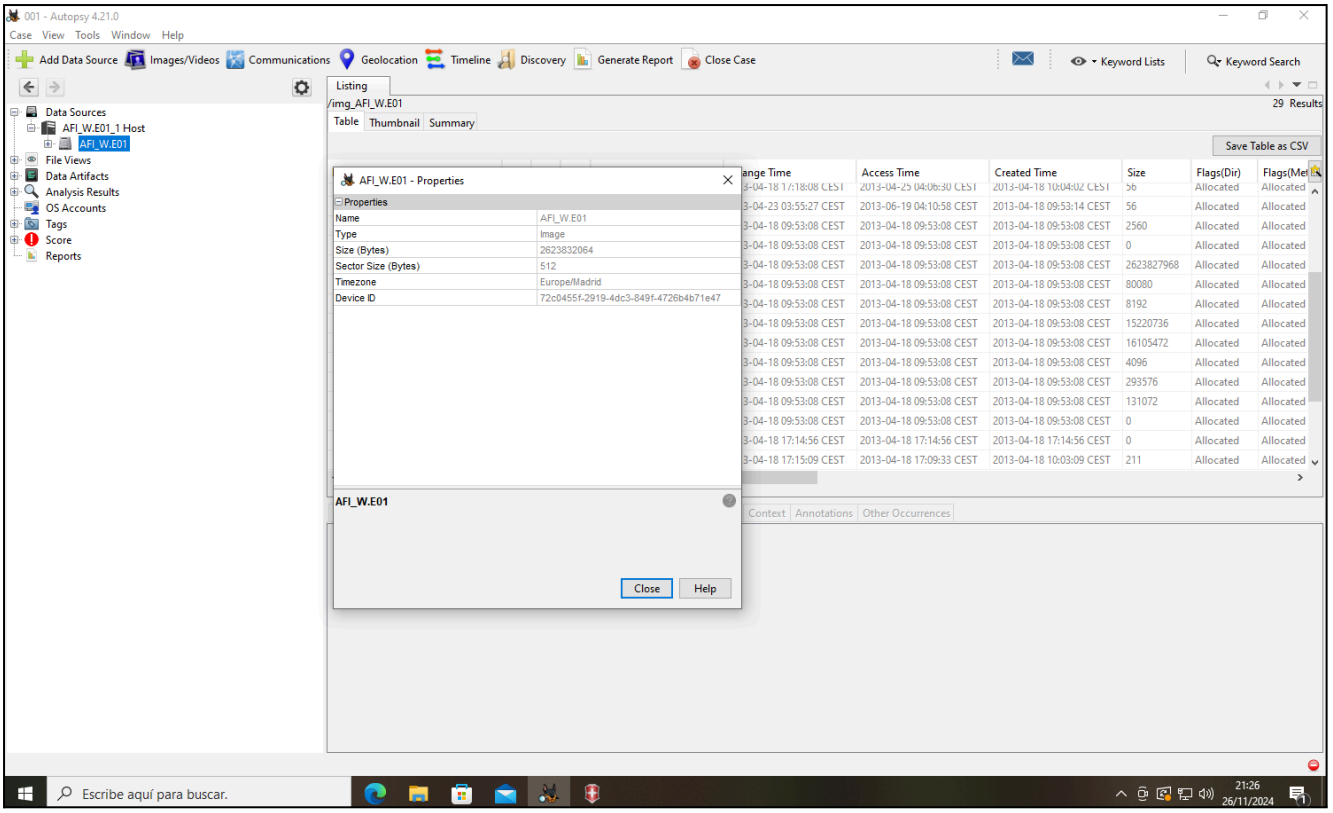
El software seleccionado para el análisis es Autopsy, en su versión 4.21.0, una herramienta de referencia en el campo del análisis forense digital. Este software permite la recuperación, organización y análisis detallado de datos contenidos en discos duros, ofreciendo funcionalidades avanzadas para la investigación. Además, se utiliza MiTeC Windows Registry Recovery, un programa especializado en el análisis de los archivos de registro del sistema operativo, como SYSTEM y SOFTWARE, lo que permite extraer y evaluar información crítica sobre la configuración del sistema y su estado operativo.

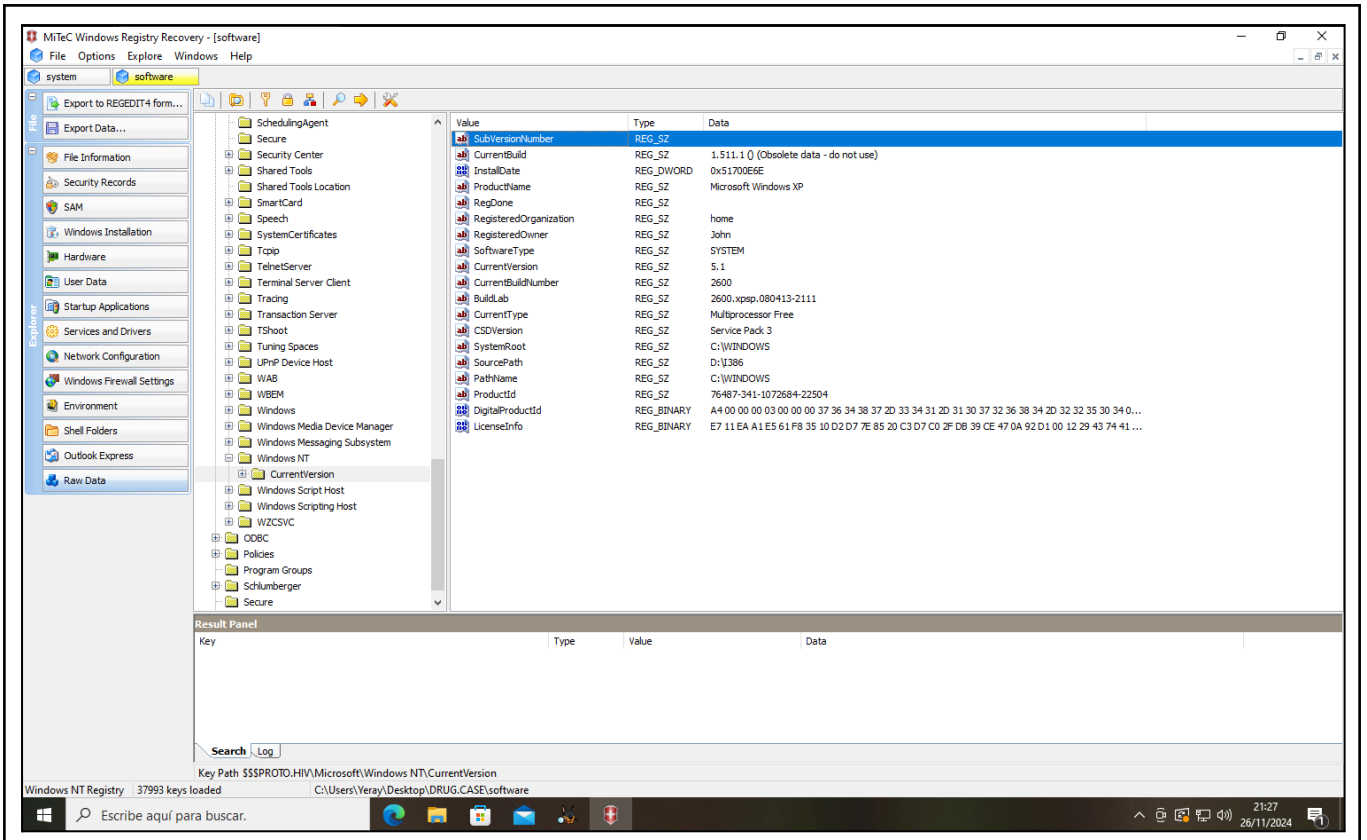
El protocolo de trabajo estipula que todas las operaciones se realizarán exclusivamente sobre una copia forense del disco original, preservando así su integridad. Antes de iniciar el análisis, se verificó la integridad de dicha copia mediante el cálculo de su hash, obteniendo una coincidencia exacta con el del disco original, lo que garantiza la autenticidad y fiabilidad de los datos procesados.

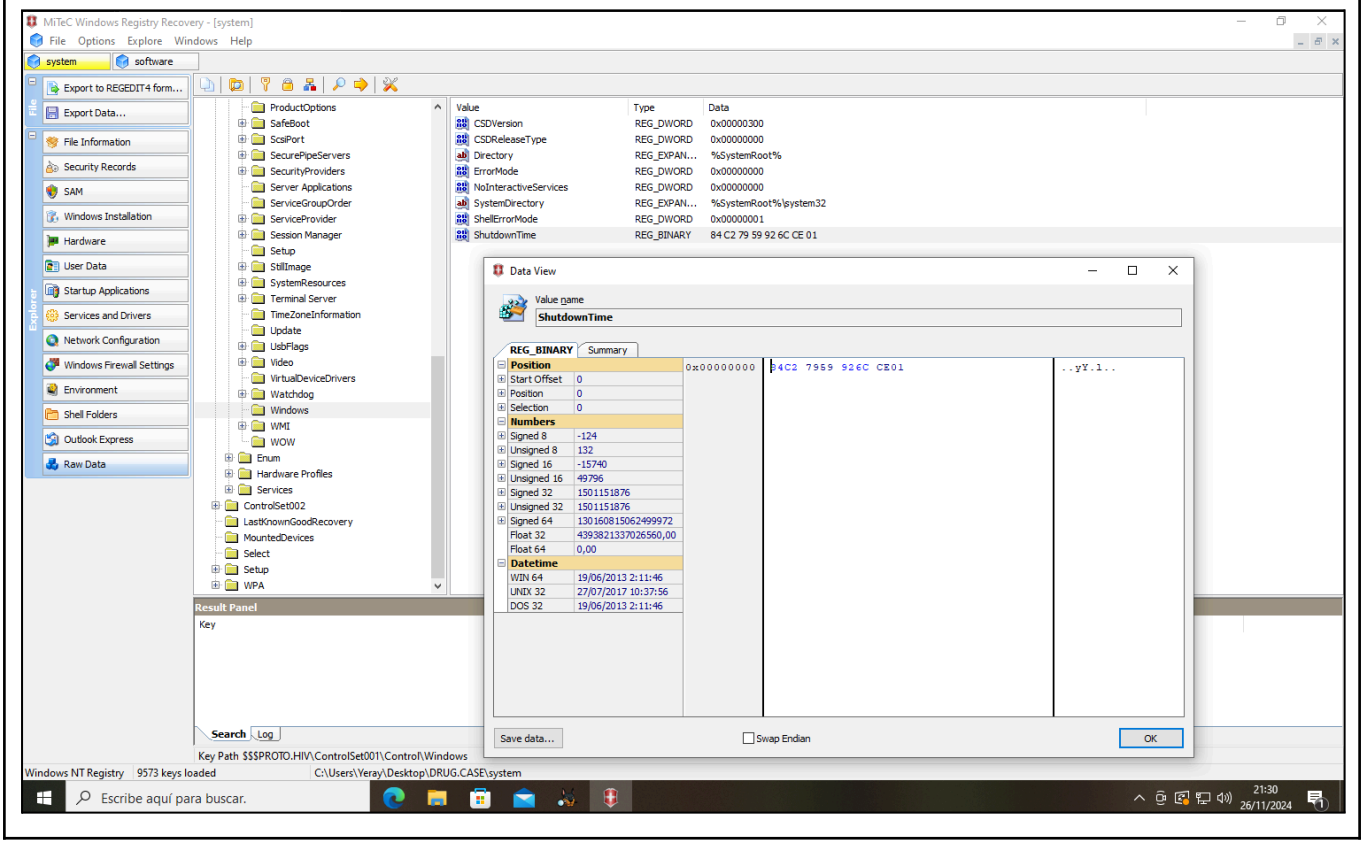


2. Información del sistema operativo

EVIDENCIAS	DATOS
Tamaño de la partición a analizar	2623832064 Bytes (2.44Gb)
Sistema operativo y versión	Microsoft Windows XP
Nombre del usuario	John
Organización registrados	home
Product ID	76487-341-1072684-22504
Service Pack	Service Pack 3
Fecha y hora de instalación del SO	18/04/2013 15:17:02 (UTC)
Fecha y hora del último apagado	WIN 64 - 19/06/2013 2:11:46

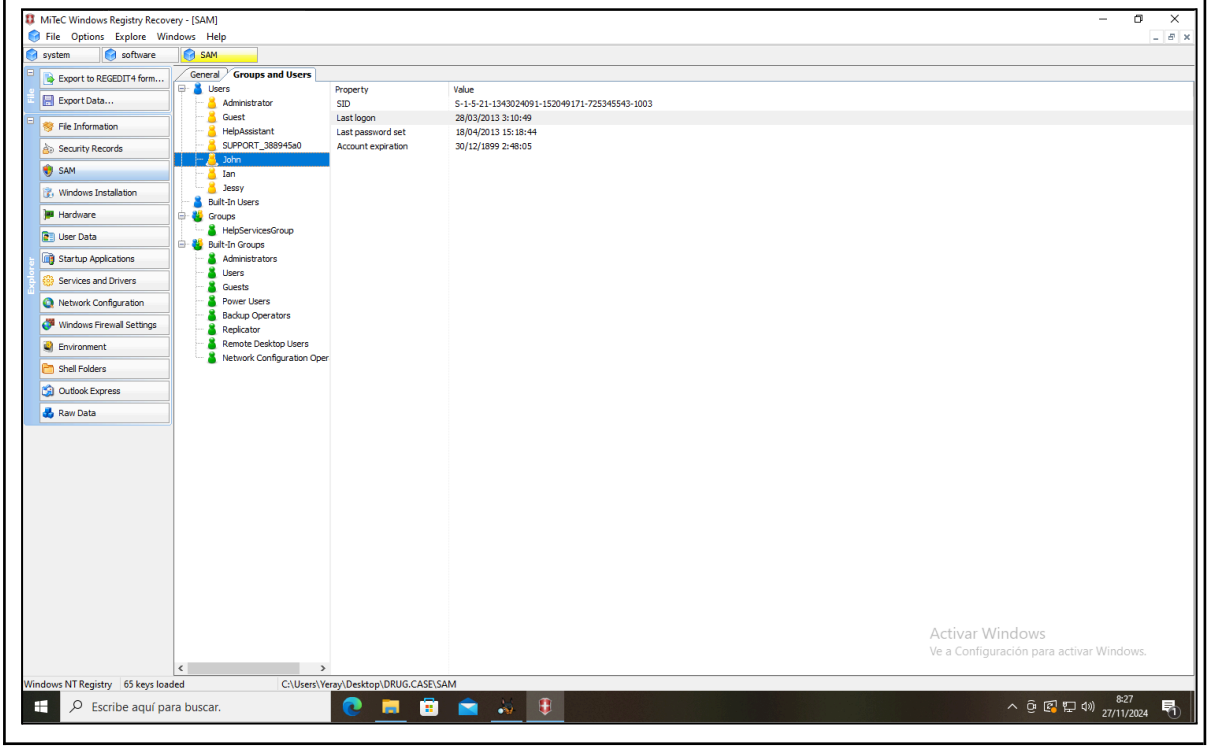



MiTeC Windows Registry Recovery - [software]
File Options Explore Windows Help
system
software
Export to REGEDIT4 form...
Export Data...
File Information
Security Records
SAM
Windows Installation
Hardware
User Data
Startup Applications
Services and Drivers
Network Configuration
Windows Firewall Settings
Environment
Shell Folders
Outlook Express
Raw Data
Explorer
SchedulingAgent
Secure
Security Center
Shared Tools
Shared Tools Location
SmartCard
Speech
SystemCertificates
Tcpip
TelnetServer
Terminal Server Client
Tracing
Transaction Server
TShoot
Tuning Spaces
UPnP Device Host
WAB
WBEM
Windows
Windows Media Device Manager
Windows Messaging Subsystem
Windows NT
CurrentVersion
Windows Script Host
Windows Scripting Host
WZCSVC
ODBC
Policies
Program Groups
Schlumberger
Secure
Value Type Data
SubVersionNumber REG_SZ
CurrentBuild REG_SZ 1.511.1 () (Obsolete data - do not use)
InstallDate REG_DWORD 0x51700E6E
ProductName REG_SZ Microsoft Windows XP
RegDone REG_SZ
RegisteredOrganization REG_SZ home
RegisteredOwner REG_SZ John
SoftwareType REG_SZ SYSTEM
CurrentVersion REG_SZ 5.1
CurrentBuildNumber REG_SZ 2600
BuildLab REG_SZ 2600.xpsp.080413-2111
CurrentType REG_SZ Multiprocessor Free
CSDVersion REG_SZ Service Pack 3
SystemRoot REG_SZ C:\WINDOWS
SourcePath REG_SZ D:\I386
PathName REG_SZ C:\WINDOWS
ProductId REG_SZ 76487-341-1072684-22504
DigitalProductId REG_BINARY A4 00 00 00 03 00 00 00 37 36 34 38 37 2D 33 34 31 2D 31 30 37 32 36 38 34 2D 32 32 35 30 34 0...
LicenseInfo REG_BINARY E7 11 EA A1 E5 61 F8 35 10 D2 D7 7E 85 20 C3 D7 C0 2F DB 39 CE 47 0A 92 D1 00 12 29 43 74 41 ...
Result Panel
Key Type Value Data
Search Log
Key Path $$$PROTO.HIV\Microsoft\Windows NT\CurrentVersion
Windows NT Registry 37993 keys loaded
C:\Users\Yeray\Desktop\DRUG.CASE\software
Escribe aquí para buscar.
21:27
26/11/2024

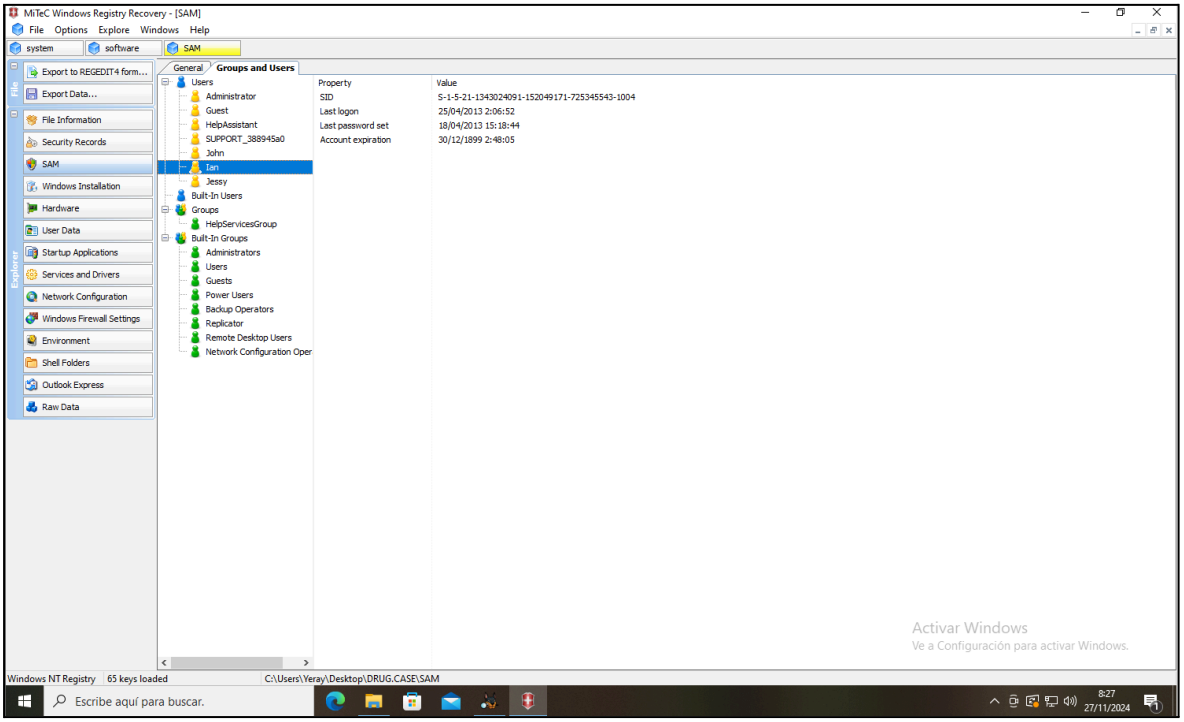

MiTeC Windows Registry Recovery - [system]
File Options Explore Windows Help
system
software
Export to REGEDIT4 form...
Export Data...
File Information
Security Records
SAM
Windows Installation
Hardware
User Data
Startup Applications
Services and Drivers
Network Configuration
Windows Firewall Settings
Environment
Shell Folders
Outlook Express
Raw Data
Explorer
ProductOptions
SafeBoot
ScsiPort
SecurePipeServers
SecurityProviders
Server Applications
ServiceGroupOrder
ServiceProvider
Session Manager
Setup
StillImage
SystemResources
Terminal Server
TimeZoneInformation
Update
UsbFlags
Video
VirtualDeviceDrivers
Watchdog
Windows
WMI
WOW
Enum
Hardware Profiles
Services
ControlSet002
LastKnownGoodRecovery
MountedDevices
Select
Setup
WPA
Value Type Data
CSDVersion REG_DWORD 0x00000300
CSDReleaseType REG_DWORD 0x00000000
Directory REG_EXPAN... %SystemRoot%
ErrorMode REG_DWORD 0x00000000
NoInteractiveServices REG_DWORD 0x00000000
SystemDirectory REG_EXPAN... %SystemRoot%\system32
ShellErrorMode REG_DWORD 0x00000001
ShutdownTime REG_BINARY 84 C2 79 59 92 6C CE 01
Data View
Value name
ShutdownTime
REG_BINARY Summary
Position
Start Offset 0
Position 0
Selection 0
Numbers
Signed 8 -124
Unsigned 8 132
Signed 16 -15740
Unsigned 16 49796
Signed 32 1501151876
Unsigned 32 1501151876
Signed 64 130160815062499972
Float 32 4393821337026560,00
Float 64 0,00
Datetime
WIN 64 19/06/2013 2:11:46
UNIX 32 27/07/2017 10:37:56
DOS 32 19/06/2013 2:11:46
0x00000000 84C2 7959 926C CE01 ..yY.l..
Save data...
Swap Endian
OK
Result Panel
Key
Search Log
Key Path $$$PROTO.HIV\ControlSet001\Control\Windows
Windows NT Registry 9573 keys loaded
C:\Users\Yeray\Desktop\DRUG.CASE\system
Escribe aquí para buscar.
21:30
26/11/2024

3. Usuarios del sistema

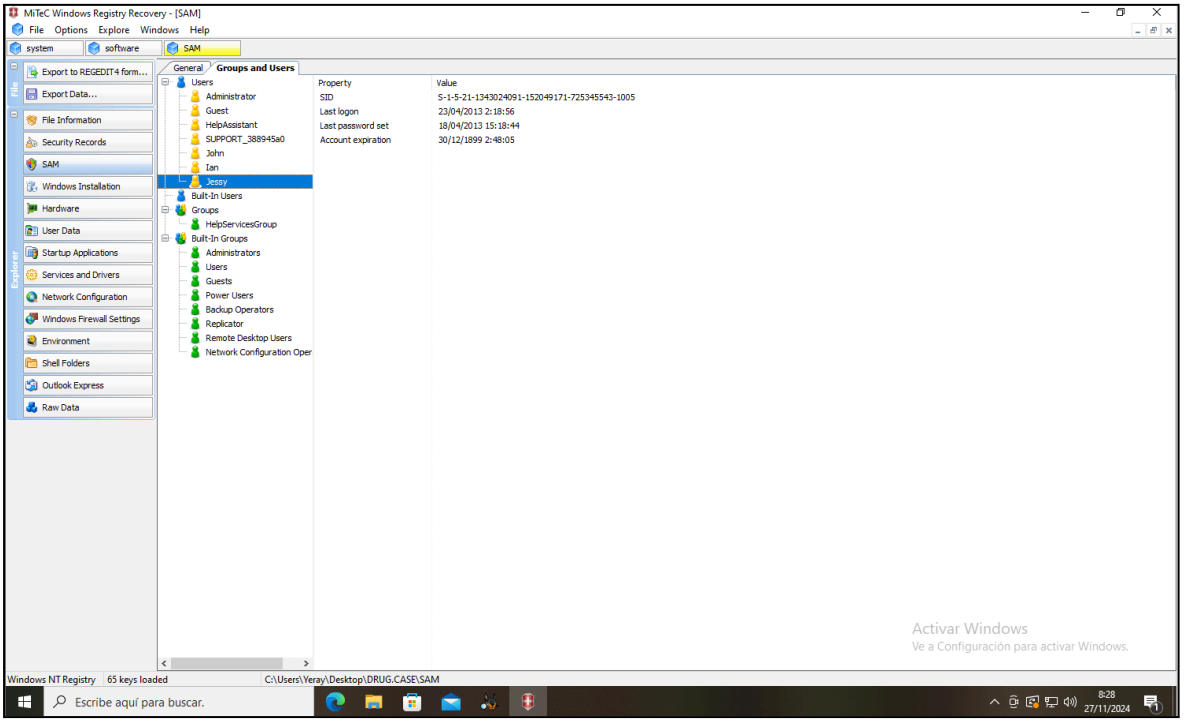
EVIDENCIAS	DATOS
Usuarios	John
Fecha y hora del último logon	28/03/2013 3:10:49
Fecha y hora del último cambio de contraseña	18/04/2013 15:18:44



EVIDENCIAS	DATOS
Usuarios	Ian
Fecha y hora del último logon	25/04/2013 2:06:52
Fecha y hora del último cambio de contraseña	18/04/2013 15:18:44



EVIDENCIAS	DATOS
Usuarios	Jessy
Fecha y hora del último logon	23/04/2013 2:18:56
Fecha y hora del último cambio de contraseña	18/04/2013 15:18:44



¿Existe alguna contradicción entre las fechas halladas en éste apartado y el anterior? En caso afirmativo, ¿a qué crees que puede ser debido?

4. Hallazgos

Se ha elaborado un anexo en formato PDF donde se detallan exhaustivamente todas las evidencias identificadas durante el análisis forense. Este documento está disponible como parte complementaria del informe:

- Enlace al anexo: Anexo.pdf

¿Los ficheros fotográficos contienen algún tipo de metadatos? En caso afirmativo, ¿qué información te permiten obtener?
Se ha realizado la extracción completa de los metadatos asociados a los archivos fotográficos encontrados. La información obtenida incluye los siguientes campos:

- Nombre del archivo
- Tipo de archivo
- Fecha de creación
- Fecha de modificación
- Fecha de acceso
- Tamaño del archivo

Los metadatos extraídos de los archivos fotográficos proporcionan información relevante que puede ser útil para la investigación. En este caso, los datos obtenidos permiten determinar:

1. Identificación del archivo:
    - El nombre y tipo de archivo ayudan a identificar y clasificar el contenido específico dentro del conjunto de evidencias.
2. Cronología de los eventos:
    - Las fechas de creación, modificación y acceso del archivo permiten establecer una línea temporal del uso y manipulación de las imágenes, lo cual puede ser clave para vincularlas con actividades específicas o momentos relevantes en el caso.
3. Tamaño del archivo:
    - Este dato puede ser utilizado para identificar patrones de almacenamiento, determinar si el archivo fue transferido, o detectar posibles modificaciones, como compresiones o ediciones.

¿Has localizado algún fichero con contraseña? ¿Has podido acceder a su contenido?

Durante el análisis, se localizaron un total de dos archivos protegidos con contraseña:

- Uno de ellos fue descifrado con éxito, permitiendo el acceso a su contenido. Los detalles completos pueden consultarse en la página 15 del anexo.
- El segundo archivo no pudo ser descifrado; los intentos realizados y los detalles pertinentes se encuentran documentados en la página 21 del anexo.

5. Otras evidencias

Durante el análisis forense, se identificaron archivos que contienen material de pornografía infantil (pedofilia). Estos archivos han sido extraídos y documentados siguiendo el procedimiento establecido para la preservación de la evidencia. La información detallada sobre estos hallazgos, incluyendo las rutas de localización, el contenido y sus metadatos, se encuentra en el anexo adjunto.

Ubicación en el anexo:

- Archivos relacionados con este hallazgo: página 21.
- Datos adicionales sobre navegación y otras evidencias relacionadas: página 22.