Análisis Básico de Computador, Parte V

Colocando al Criminal en el Teclado

SSA Michael S. Morris

Colocando al Criminal en el Teclado

- El Registro
- Usando un archivo SAM para determinar el tiempo de registro
- Usando el archivo SOFTWARE para determinar la configuración de la Versión Actual
- Procesando Información de Volumen del Sistema
- Análisis de Historia

El Registro

- **Qué es el Registro**
- **Registro 9X “Files” y “Hives” *(Archivos – Hives)***
- **Registro XP**
- **Navegación de Registro**
- **Valores de Registro**
- **Asuntos de Perfil Múltiple**

El Registro

- Un depósito central para:
  - Información del Usuario (actualmente registrado)
  - Información del Sistema (actualmente detectado)
- Almacenado en archivos de registro:
  - Información de aplicación
  - Preferencias específicas del usuario
  - Configuración de los componentes del sistema

Archivos de Registro

SYSTEM.DAT (C:\%Windows%\)

Basado en detección, se selecciona un perfil de componentes

- Laptop "Acoplado" ?
- Laptop "Portátil" ?

USER.DAT (C:\%Windows%\Profiles\%User%\)

Basado en el registro, se selecciona un perfil de usuario

- Por Defecto ?
- Registro del Usuario ?

(No olvide copias de seguridad)

“Hives” de Registro

- **Únanse para crear:**

HKEY_CLASSES_ROOT		(HKCR)
HKEY_CURRENT_USER		(HKCU)
HKEY_LOCAL_MACHINE	*	(HKLM)
HKEY_USERS	*	(HKU)
HKEY_CURRENT_CONFIG		(HKCC)
HKEY_DYN_DATA		(HKDD)

(HKEY es el identificador de programación para una *clave*)

“Hives” de Registro

- **Estas claves:**

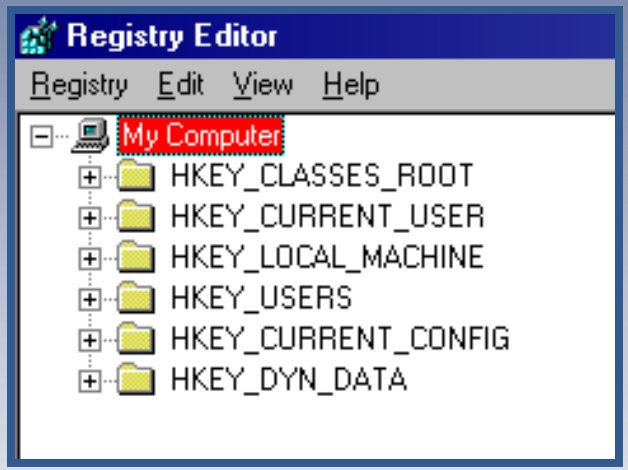
  HKEY_CLASSES_ROOT (HKCR)
  HKEY_CURRENT_USER (HKCU)
  HKEY_CURRENT_CONFIG (HKCC)

- **Se derivan de estas claves:**

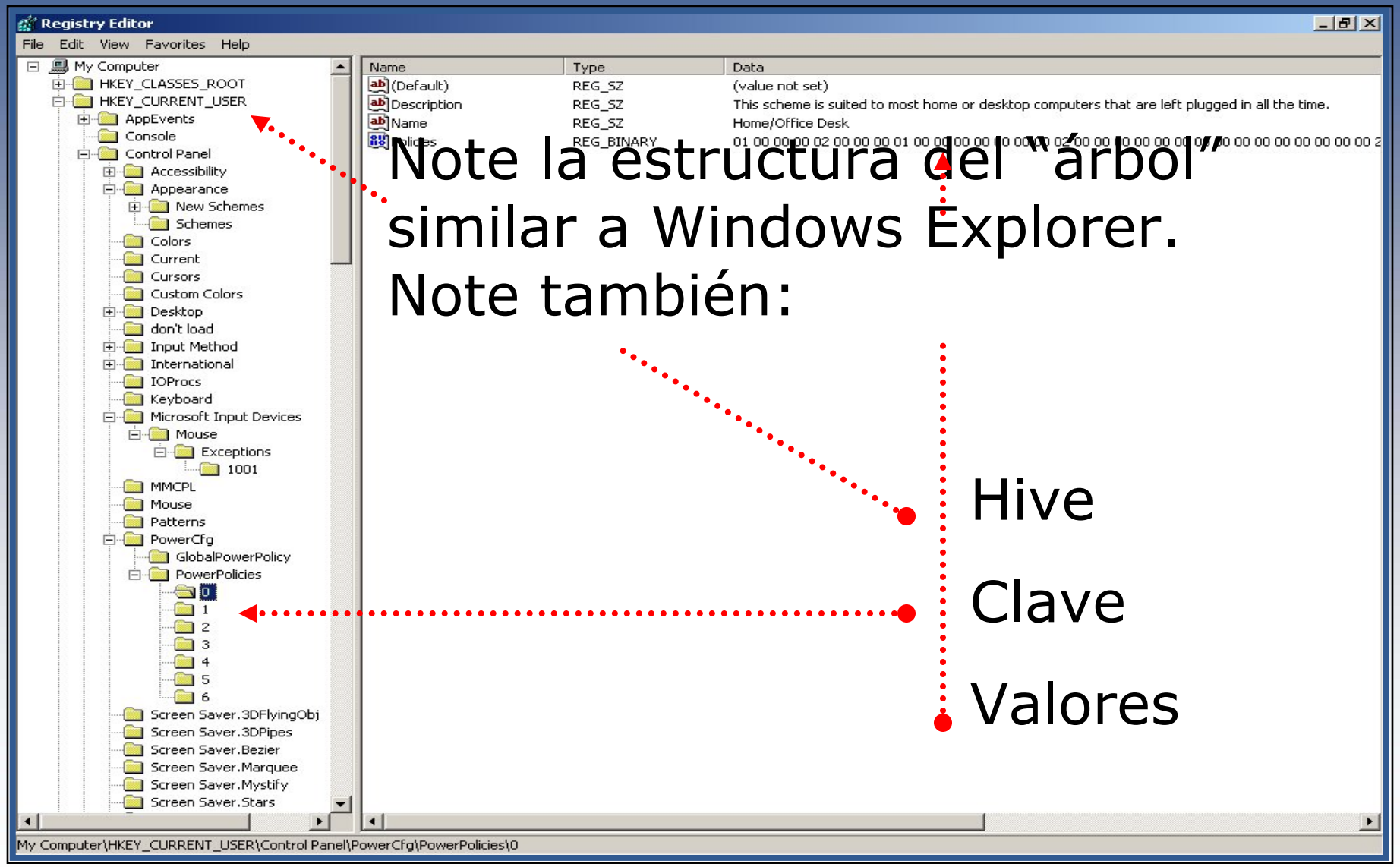
  HKEY_LOCAL_MACHINE (HKLM)
  HKEY_USERS (HKU)

- **Esta clave se deriva de la memoria:**

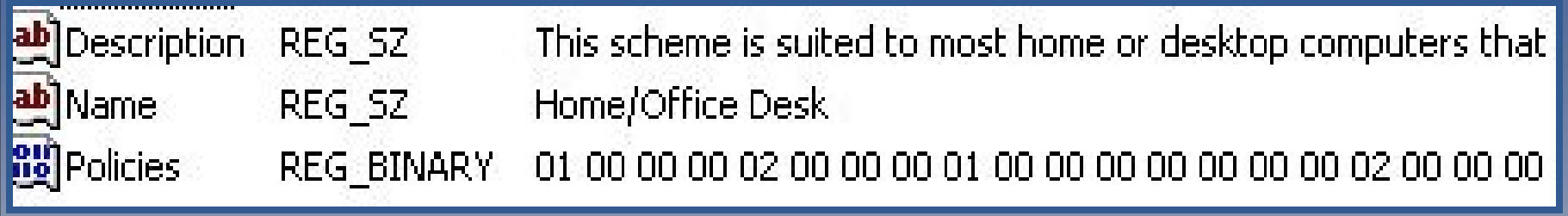
  HKEY_DYN_DATA (HKDD)



Navegación de Registro



Valores de Registro



Description	REG_SZ	This scheme is suited to most home or desktop computers that
Name	REG_SZ	Home/Office Desk
Policies	REG_BINARY	01 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 02 00 00 00

Note los Valores REG_SZ (Secuencia)

Note los Valores REG_BINARY (?)

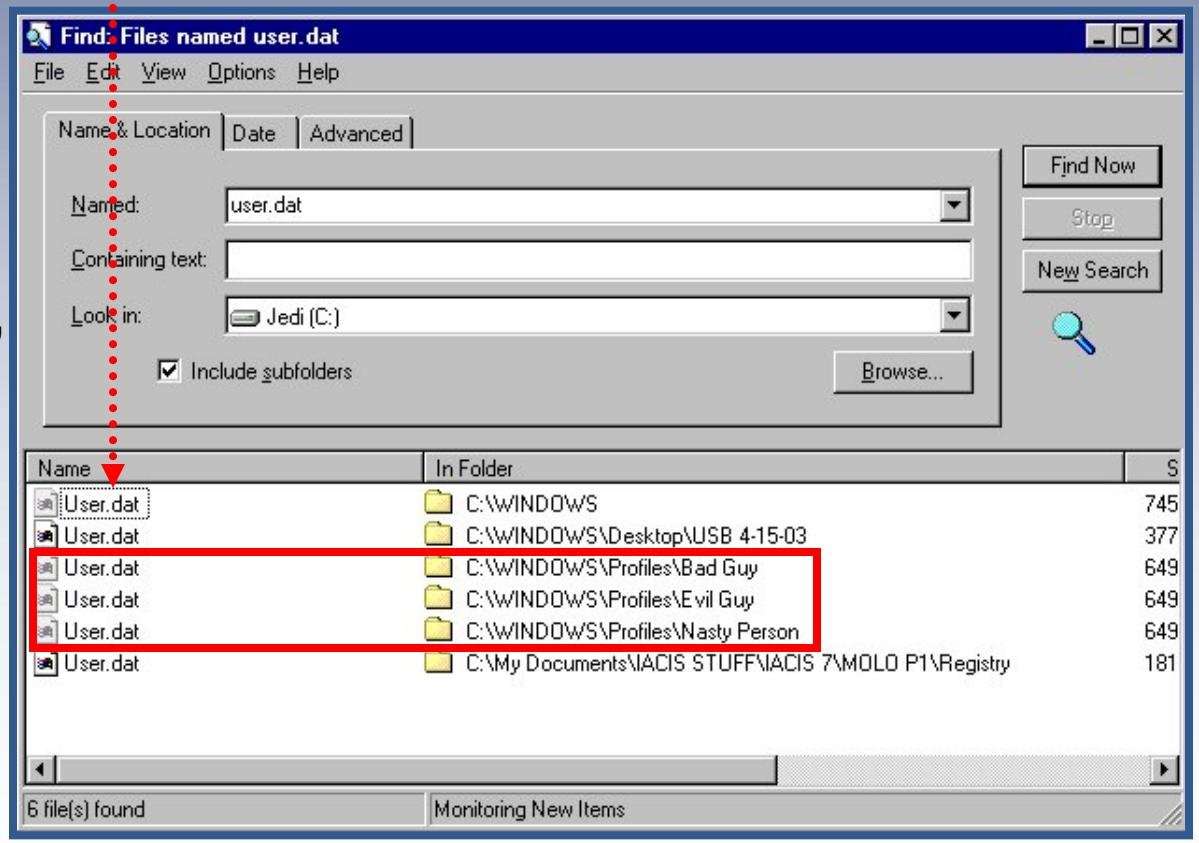
Estos tipos de valores tendrán influencia en nuestros métodos de procesamiento y documentación

Asuntos de Perfil Múltiple

- **Cada usuario creado tendrá un USER.DAT**

  (El USER.DAT in C:\%Windows% *por Defecto* también se incluye)

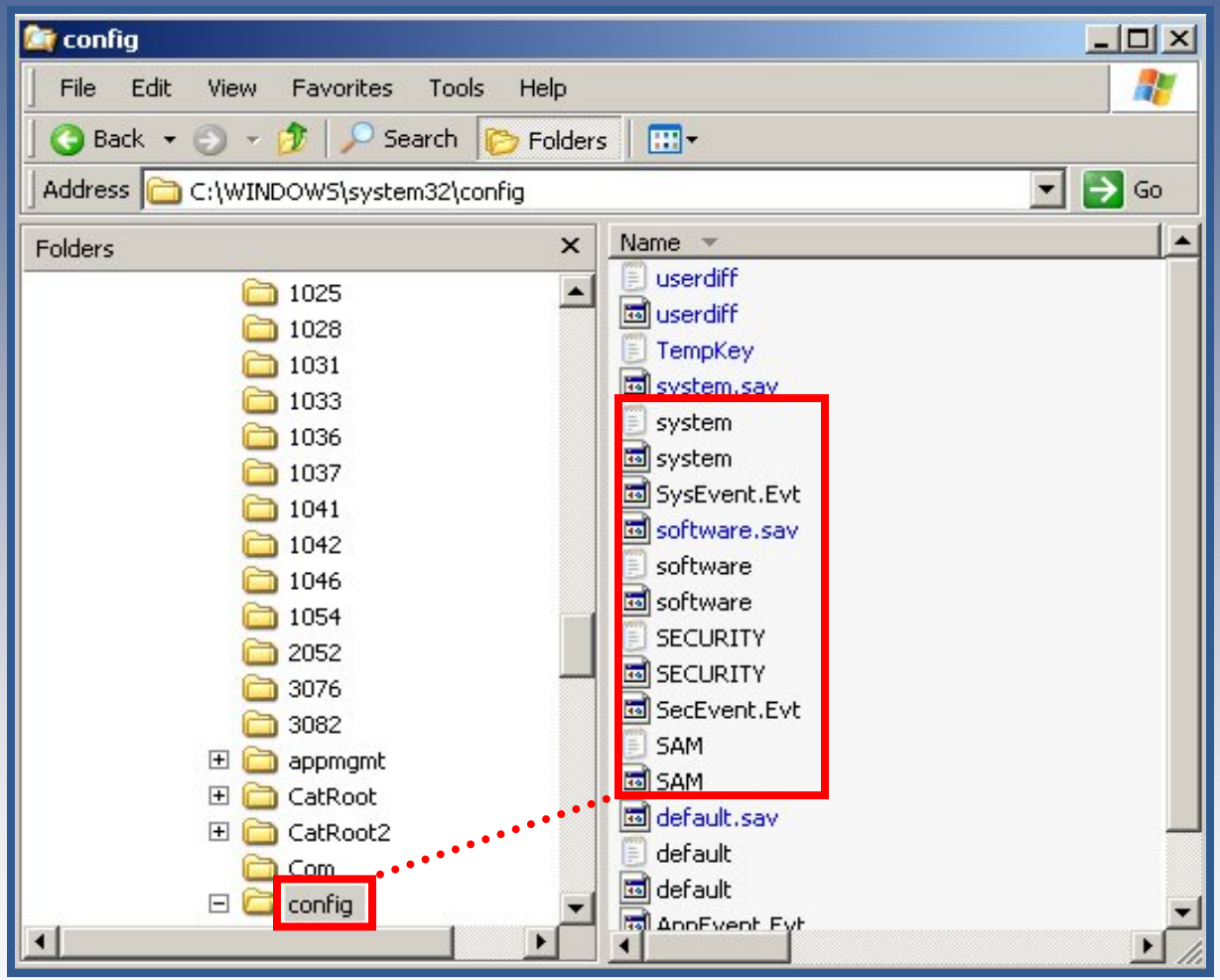
Sea cuidadoso: en el ambiente 9X, cuando se crea un usuario nuevo, el contenido de su USER.DAT reflejará el contenido del archivo USER.DAT *por defecto* actual.



Archivos de Registro 2K + XP

- SAM
- SYSTEM
- SECURITY
- SOFTWARE

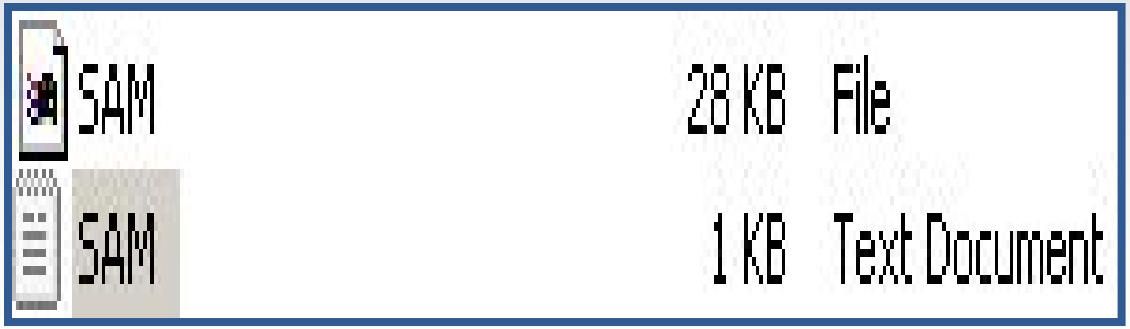
2K vs XP ?



- **Y no olvide para cada usuario → NTUSER.DAT**

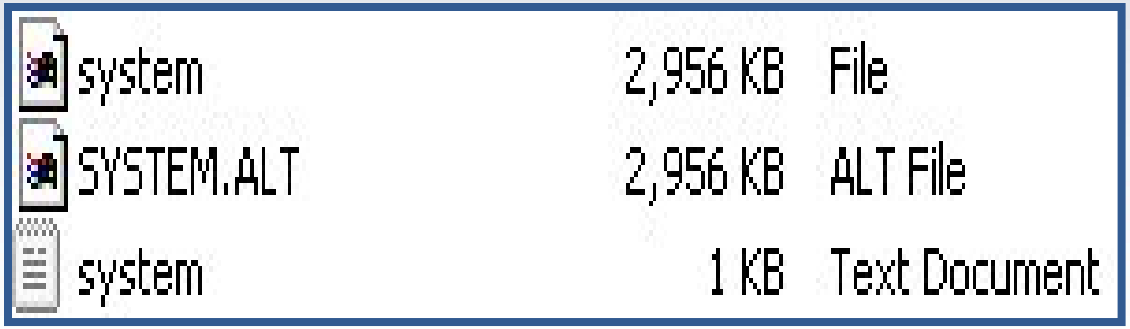
Archivos de Registro 2K + XP

- **SAM *(Base de Datos de las Cuentas de Usuarios)***
  - HKLM \ SAM
  - Información de cuenta para usuarios y grupos en el sistema
  - Contraseñas de Registro!



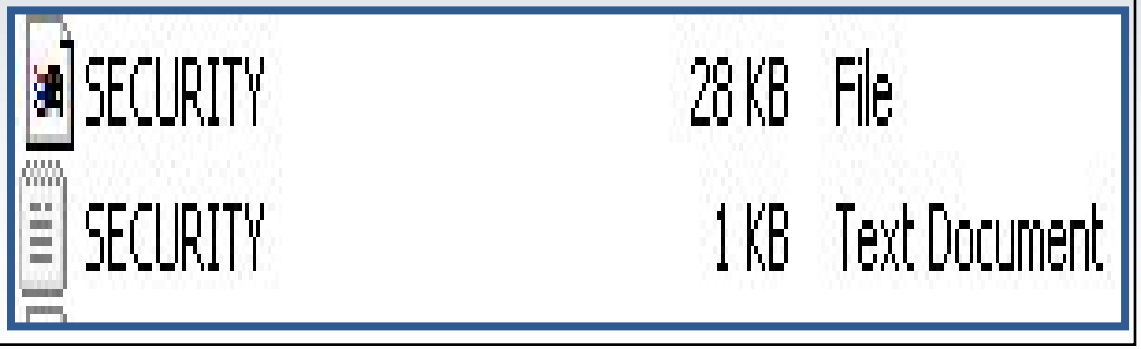
Archivos de Registro 2K + XP

- **SYSTEM *(Sistema)***
  - HKLM \ SYSTEM
  - Controladores de Dispositivo
  - Nombre del Computador
  - Historia Activa



Archivos de Registro 2K + XP

- **SECURITY *(Seguridad)***
  - HKLM \ SECURITY
  - Póliza de seguridad local, derechos del usuario, grupos

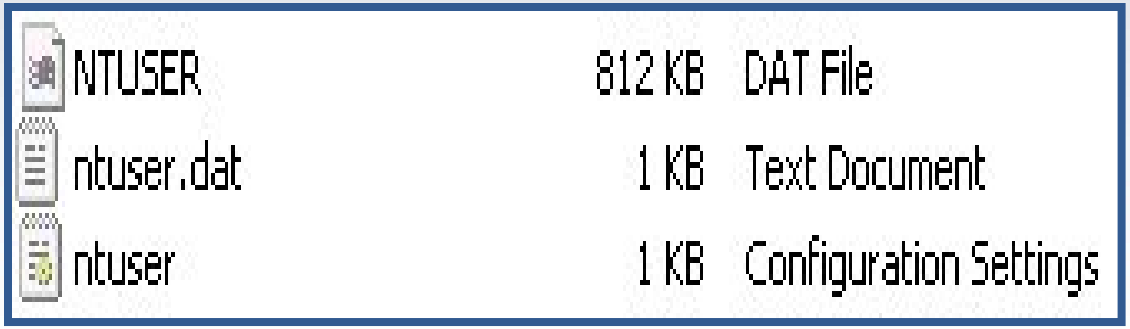


Archivos de Registro 2K + XP

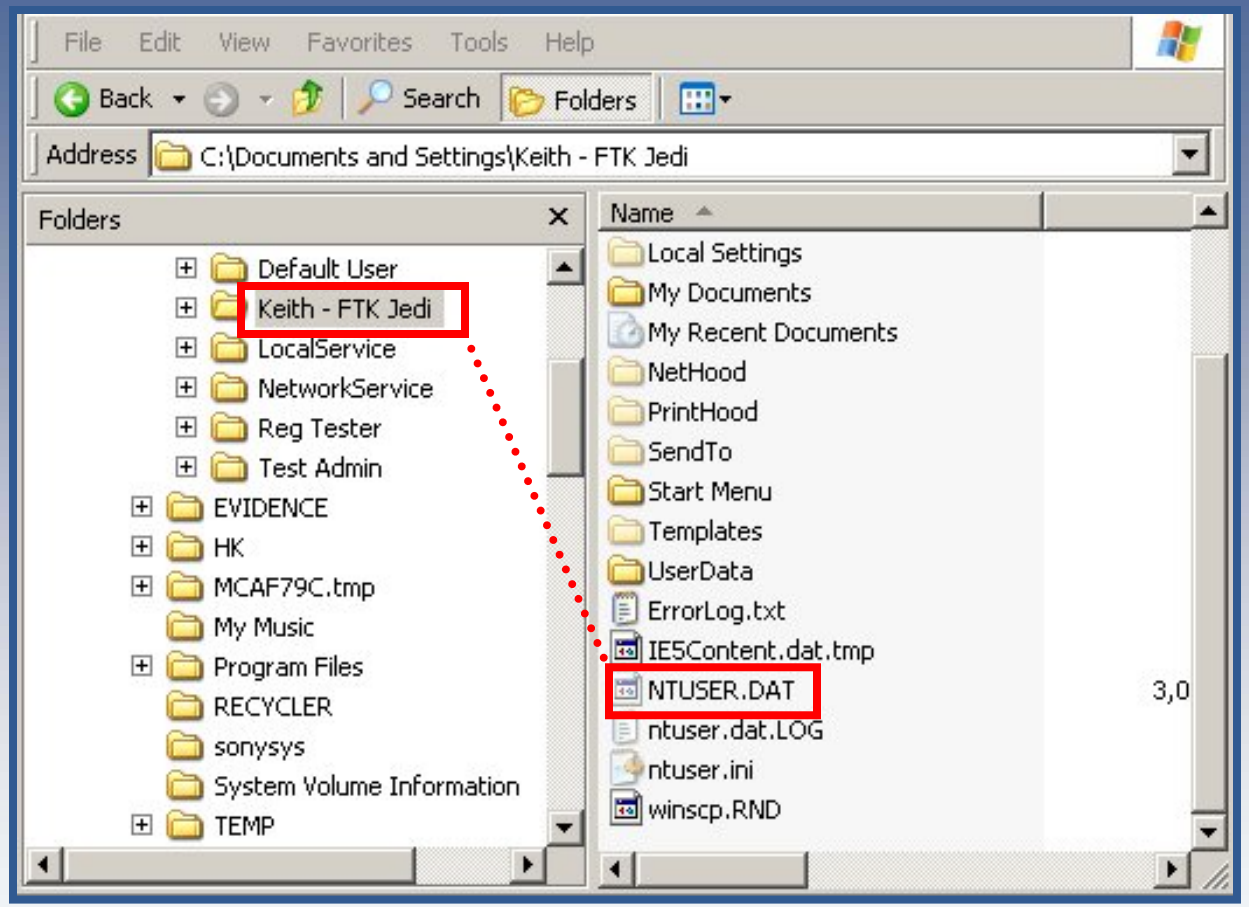
- **SOFTWARE**
  - HKLM \ SOFTWARE
  - Configuración del Programa
  - Configuración de la Versión Actual

Archivos de Registro 2K + XP

- **NTUSER**
  - HKU \ SID
  - Preferencias del Usuario
  - Distribución del Escritorio
  - Fondo de Pantalla \ Protectores de Pantalla
  - etc. …



Asuntos de Perfil Múltiple



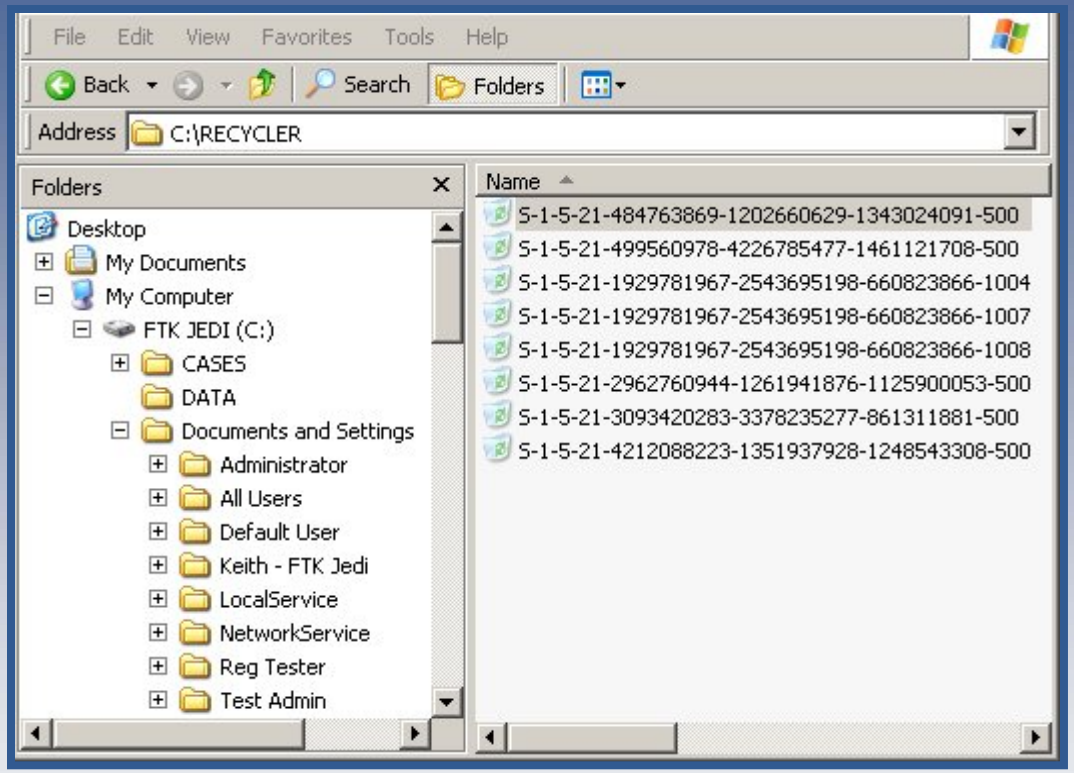
Cada usuario tiene un archivo NTuser.dat

Asuntos de Perfil Múltiple

Cada usuario tiene también algo nuevo en este ambiente:

Un "SID" o

Identificación de Seguridad



S-1-5-21-436374069-842925246-1343024091-1000

Asuntos de Perfil Múltiple

Las preocupaciones pueden ser:

- Resolver Nombres de Usuarios en fólderes SID (Papelera de Reciclaje y Control de Acceso)
- Procesar Información de Usuario SAM (por ejemplo últimos registros)
- Información de Volumen del Sistema

Diferencias Notables de Seguimiento

Información MRU:

- Seguimiento:
  - Abrir / Ejecutar / Guardar Listas
  - Impresoras / Encontrar Archivos / Encontrar Computadores
  - Tipos de Archivos Individuales (números grandes)

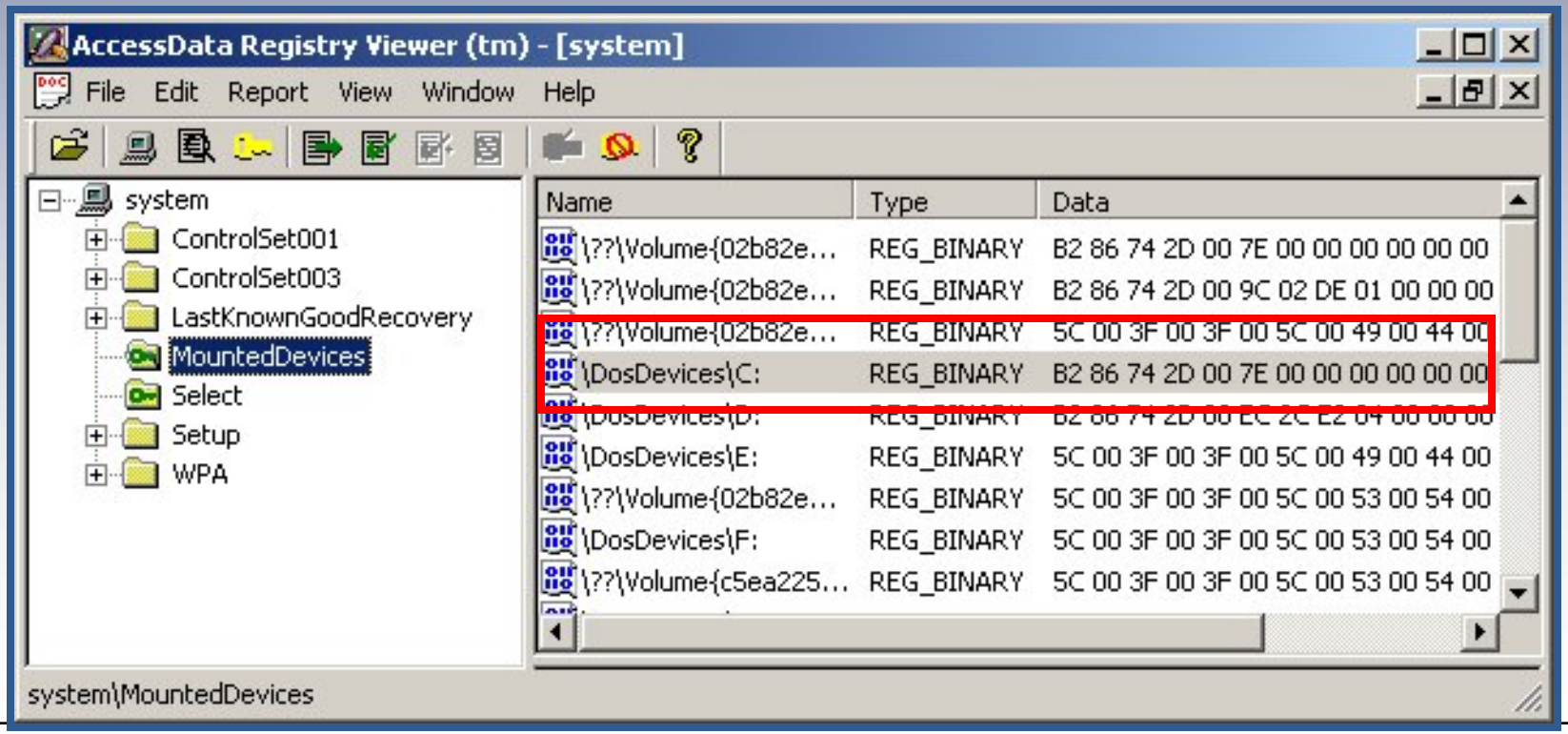
Dispositivos Instalados:

- Indicación de dispositivos recientemente instalados y asignados y letras respectivas a las unidades – (puede ser una clave)

Diferencias Notables de Seguimiento

Revise el archivo del SISTEMA

→ Dispositivos Instalados



Como idea ...

Alguna Información Disponible

Listas Recientes de Documentos
Listas Recientes de Ejecución
de Archivo
Info. Registrada
del Propietario
Direcciones URL Tipo Internet Explorer
Listas de Historia del Reproductor
Multimedia
Dispositivos / Unidades Instaladas
Proveedor del Sistema Protegido
de Almacenamiento

Contactos IM
Info. de Archivos
Compartidos
Info. de Sala de
Charla
Info. de ID Alias
Info. de Historia

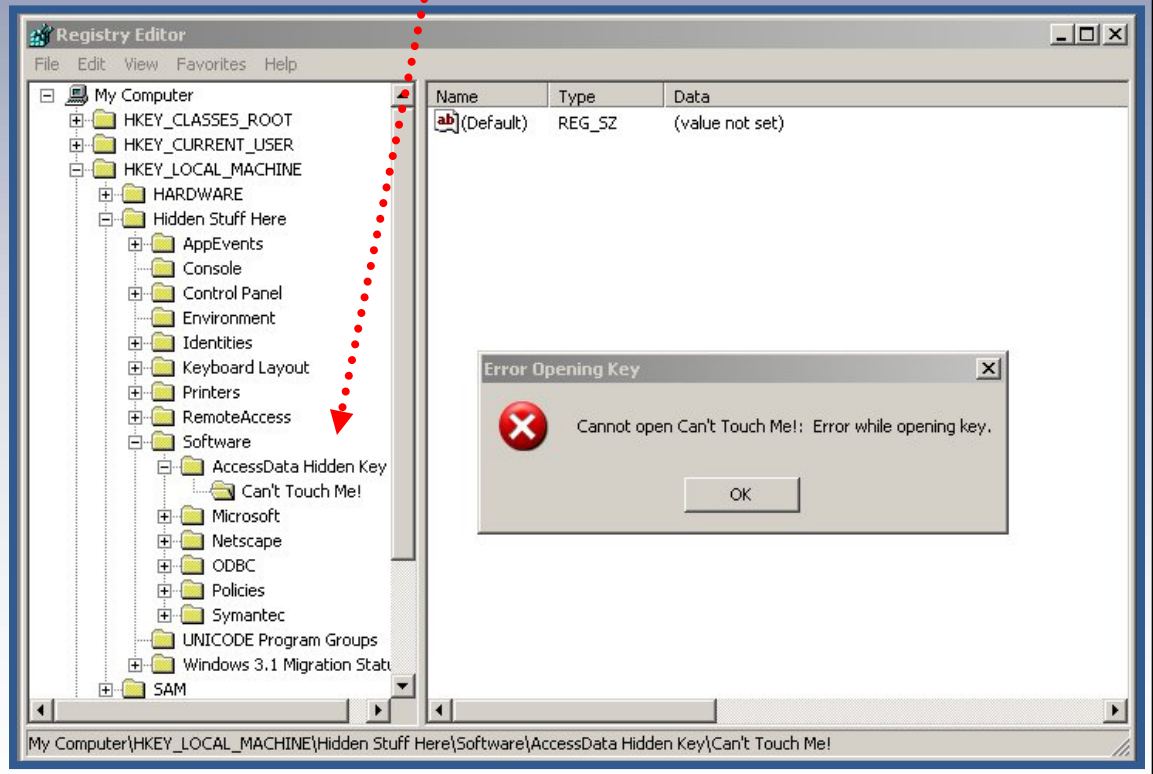
Info. de Perfil
Info. de Versión OS

(eso es apenas tocando la superficie)

Evidencia de Recopilación

Teniendo acceso a un valor clave nulo terminado "hidden" *(escondido)*

Utilice una herramienta que omita Windows API

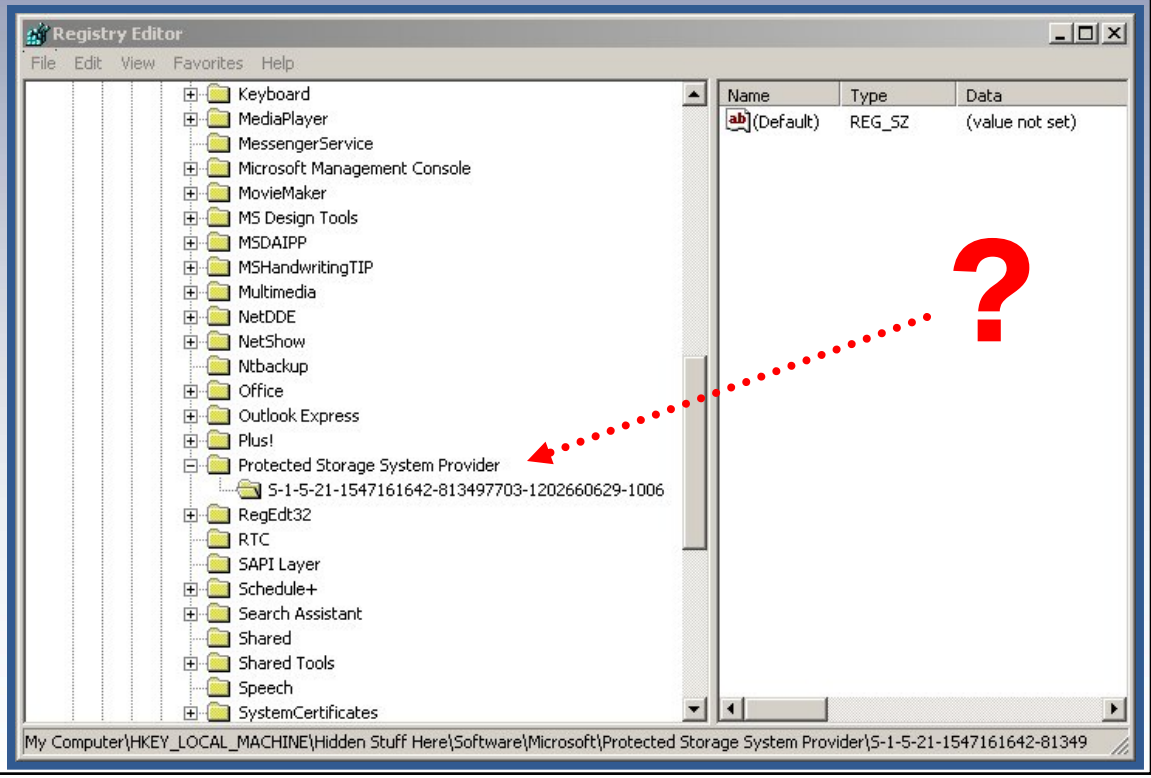


Evidencia de Recopilación

Teniendo acceso al Área Protegida de Almacenamiento

(Clave del Proveedor del Sistema Protegido de Almacenamiento)

Utilice una herramienta que omita Windows API Y descifre los valores !

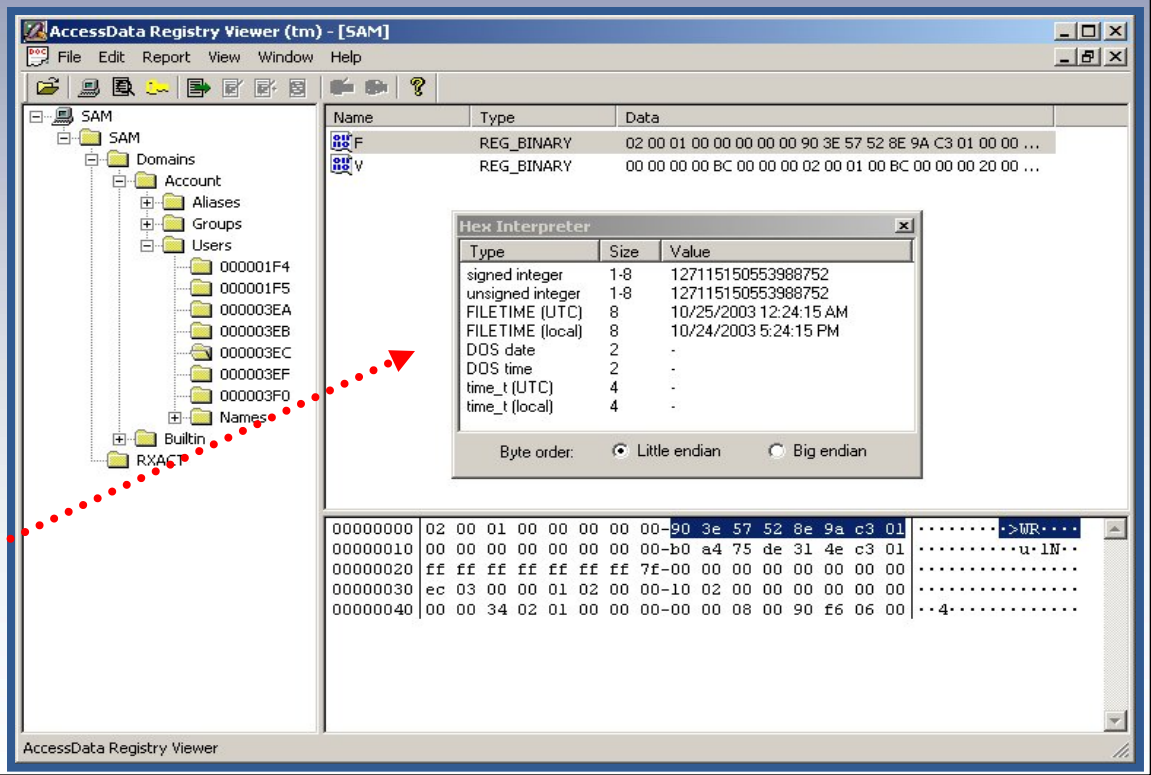


Evidencia de Recopilación

Usando un archivo SAM para determinar los valores del usuario:

- **Ultimo registro**
- **ID SID Único**

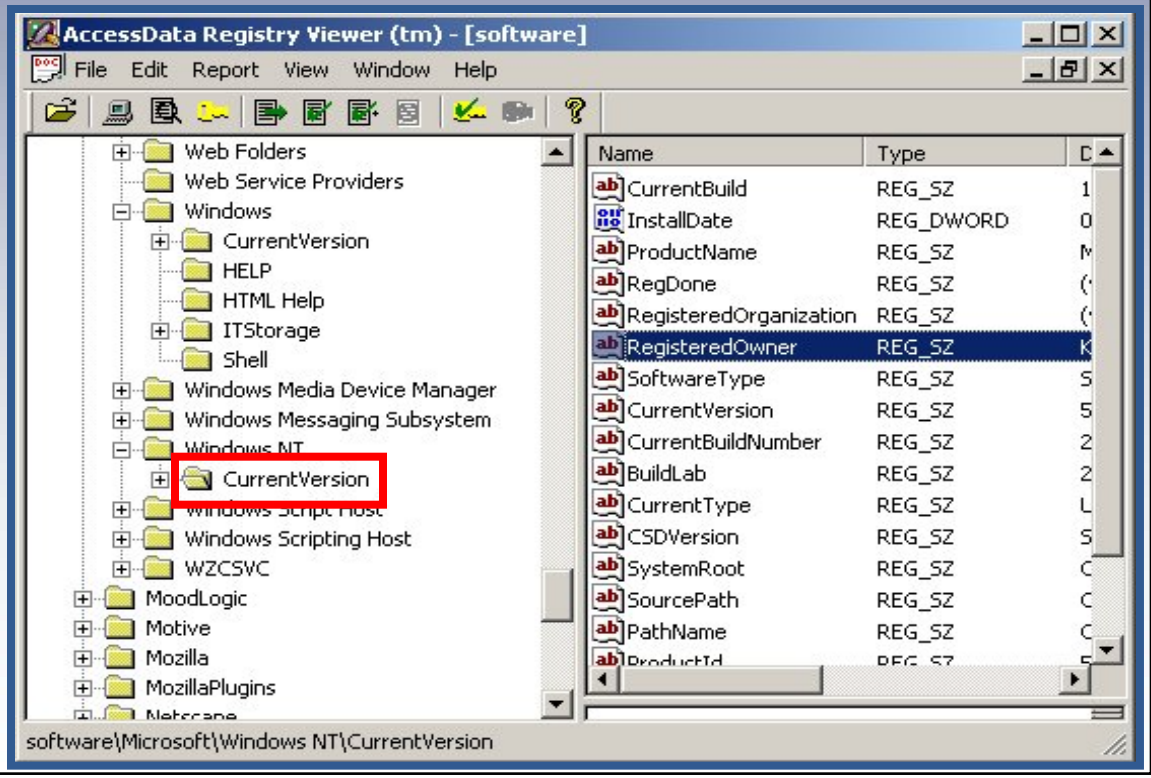
Asegúrese de tener un interprete hex práctico para esto !



Evidencia de Recopilación

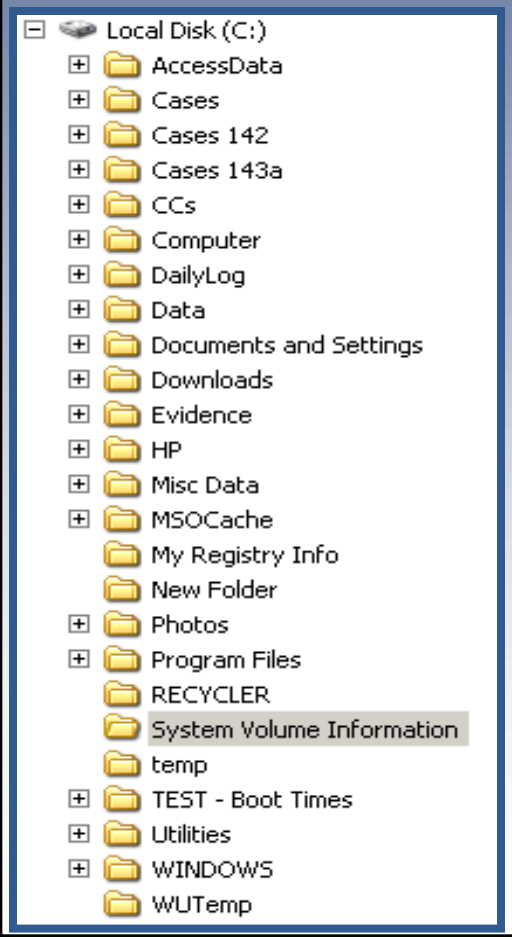
Usando un archivo SOFTWARE para determinar la configuración

Quién
Qué
Cuándo
Dónde ??
Por Qué ????



Información de Volumen del Sistema

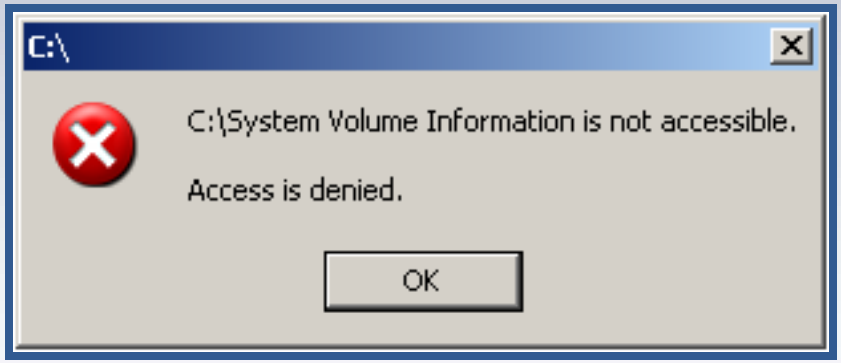
Información de Volumen del Sistema (SVI)



Fólder Protegido del Sistema

%Root%

Información de Punto de Restauración !



SVI – Puntos de Restauración

- ME, XP, (2K)
- “Define Punto de Restauración” cada 24 Horas
- Registro y Otros Archivos del Sistema
- Mínimo 200MB (hasta 12% del Disco)
- Copias de Seguridad permanecen hasta por 90 días

Puntos de Restauración

- Copias de Seguridad del Registro
  (Entre otras cosas)

- Casos
  - Defensa Trojan Visitada de Nuevo
  - Ellos Visitaron o No Ese Lugar?
  - Sospechoso usó software de limpieza

- Reproductor de Imágenes & SVI
  (Hmmmm … ??)

Conclusión

- Entrevista del Sujeto
  - Acceso al Computador
  - Quién tiene contraseña?
  - Computador Público
- Correo Electrónico en la memoria de acceso rápido
- Sitios Web en la memoria de acceso rápido
- Correo Electrónico Internet
- Fuentes Externas
  - Cámaras de vigilancia
  - Registro – Computadores de Biblioteca y Públicos

??

Preguntas?

SSA Michael S. Morris
Michael.morris@ic.fbi.gov