

PRACTICA DE LABORATORIO

ANALIZAR EL REGISTRO DE WINDOWS – PARTE 1

Dentro de los procedimientos a cumplir en una investigación de computo forense sobre equipos que trabajan con sistemas operativos Windows se incluye el análisis de los **Registros de Windows**, los cuales permiten recopilar información complementaria y valiosa para la investigación, dichos registros se encuentran clasificados por secciones y se organizan en forma jerárquica por claves (Hives), subclaves y valores.

Objetivo General.- Obtener y analizar el registro de Windows de nuestro propio equipo con el uso de las herramientas forenses: FTK Imager y Registry Viewer

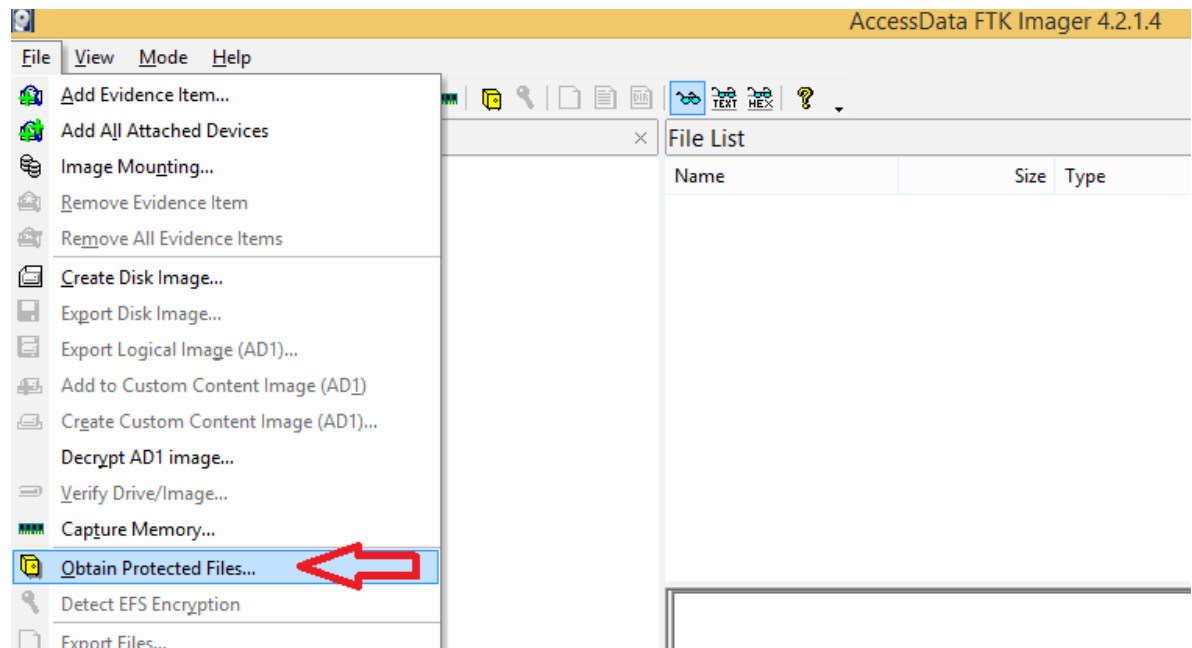
Objetivos Específicos:

- **Averiguar la versión de Windows que tiene el equipo**
- **Averiguar las cuentas de usuario del Sistema**
- **Averiguar la configuración de la Zona Horaria del Sistema**
- **Averiguar el nombre del equipo**
- **Averiguar que dispositivos fueron montados en el Equipo**
- **Averiguar que dispositivos USB de almacenamiento fueron conectados**

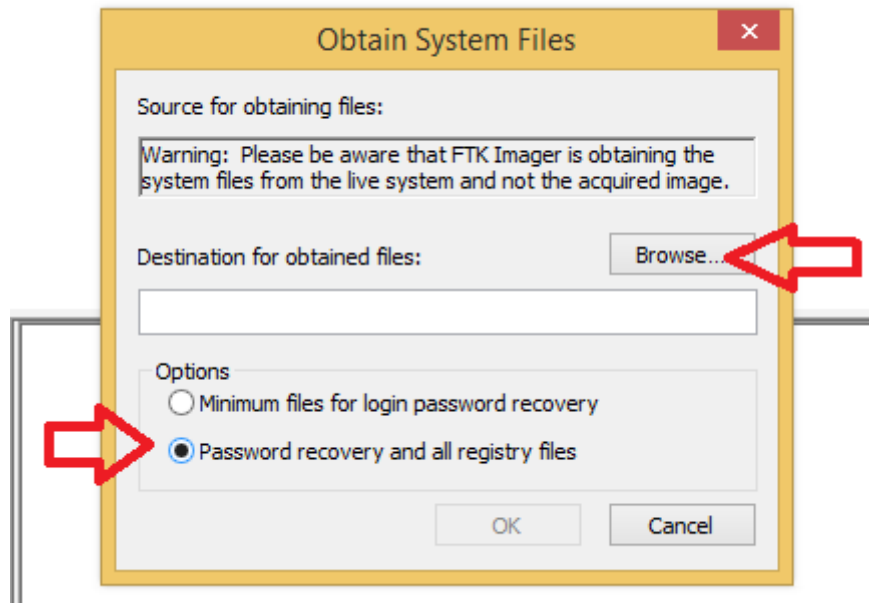
DESARROLLO DE LA PRÁCTICA

1) Extracción de los archivos del Registro de Windows de nuestro equipo

- **Iniciar el programa FTK Imager (la descarga del programa se muestra en prácticas anteriores)**
- **Seleccionar del menú File → Obtain Protected Files**



- En la ventana emergente seleccionar donde serán almacenados los archivos del registro de Windows "Browse", y seleccionar "Password Recovey and all registry files" y presionar OK



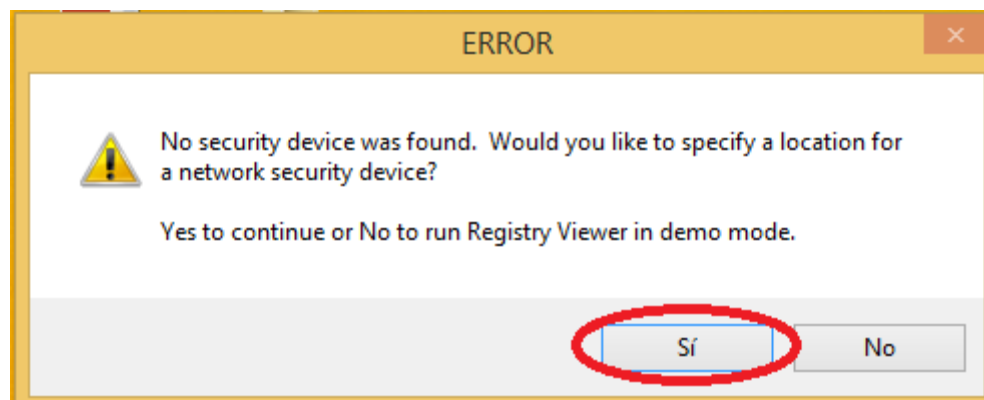
2) Averiguar la versión de Windows que tiene el equipo Investigado

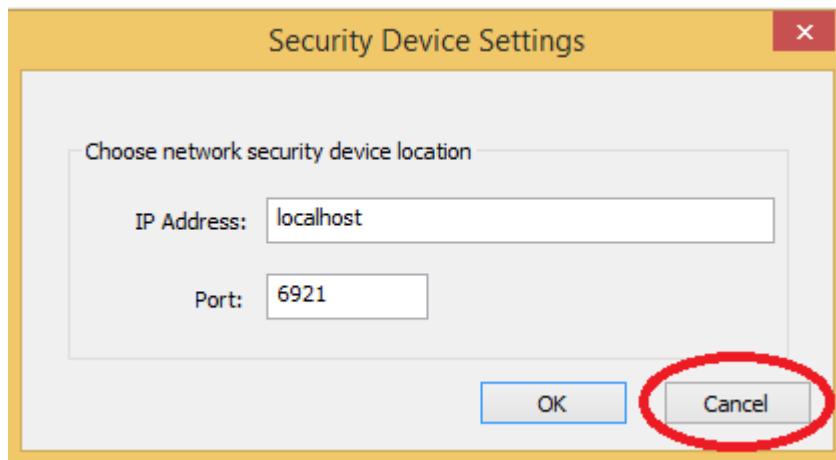
Instalar el programa "Registry Viewer"

- Bajar el programa de → <https://accessdata.com/product-download/registry-viewer-1-8-0-5>
- Iniciar el programa

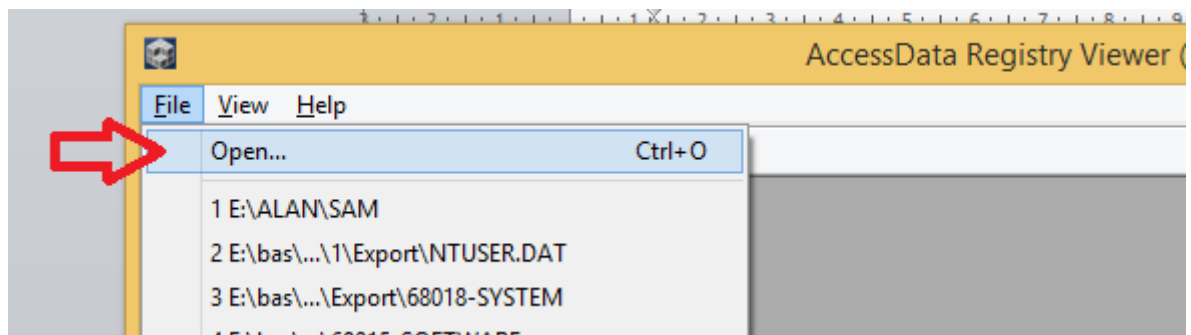


- Como el programa es versión Demo, en la primera ventana emergente presionar "sí"

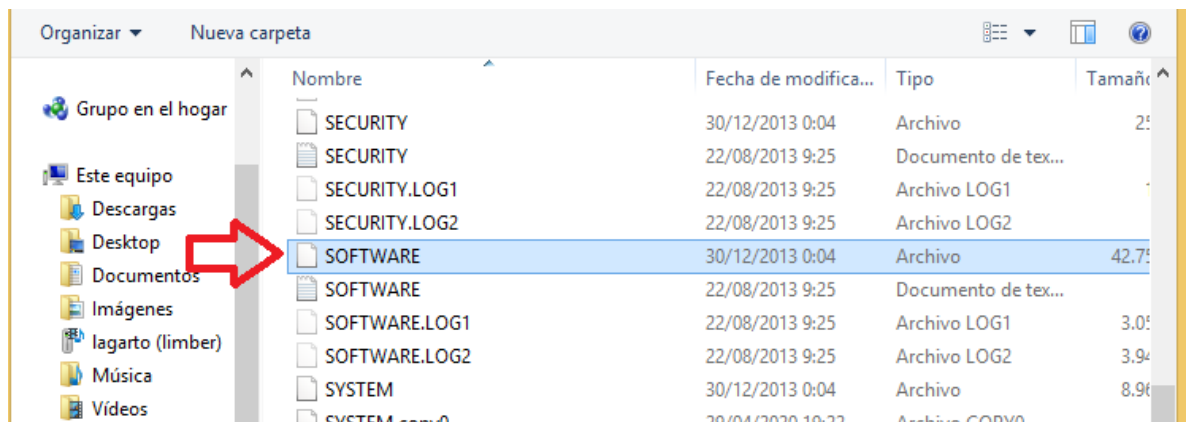




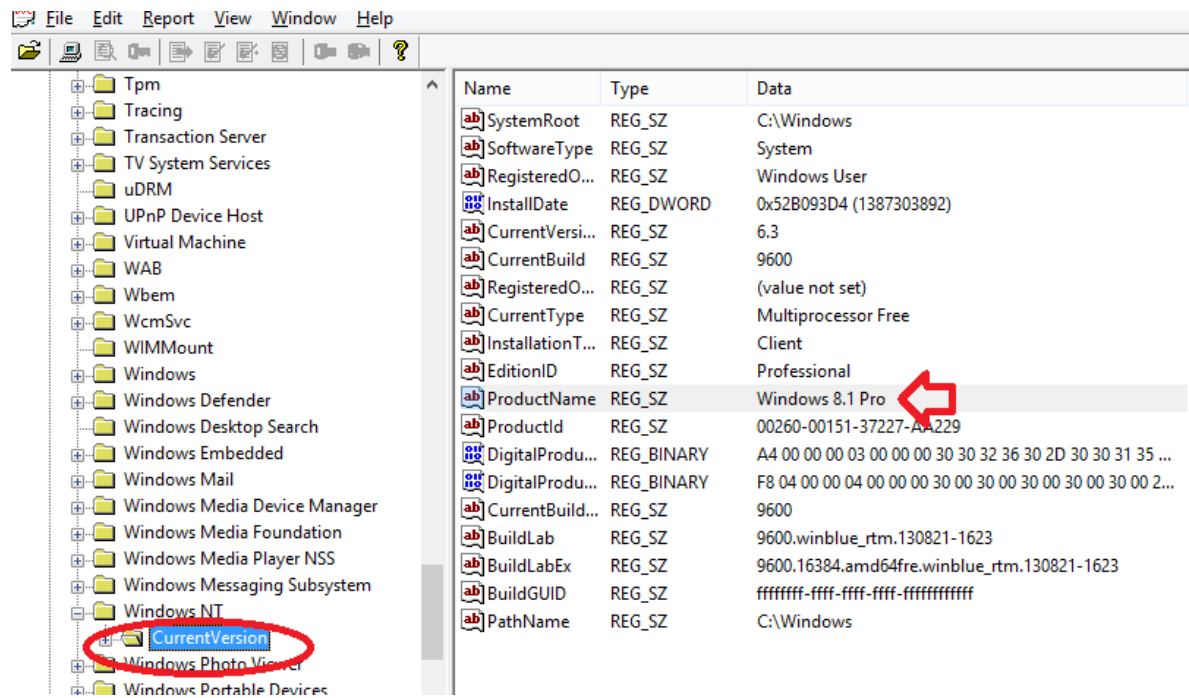
- En el programa seleccionar del menú File → Open



- Abrir el archivo SOFTWARE desde el lugar donde se guardaron los archivos con el programa FTK Imager

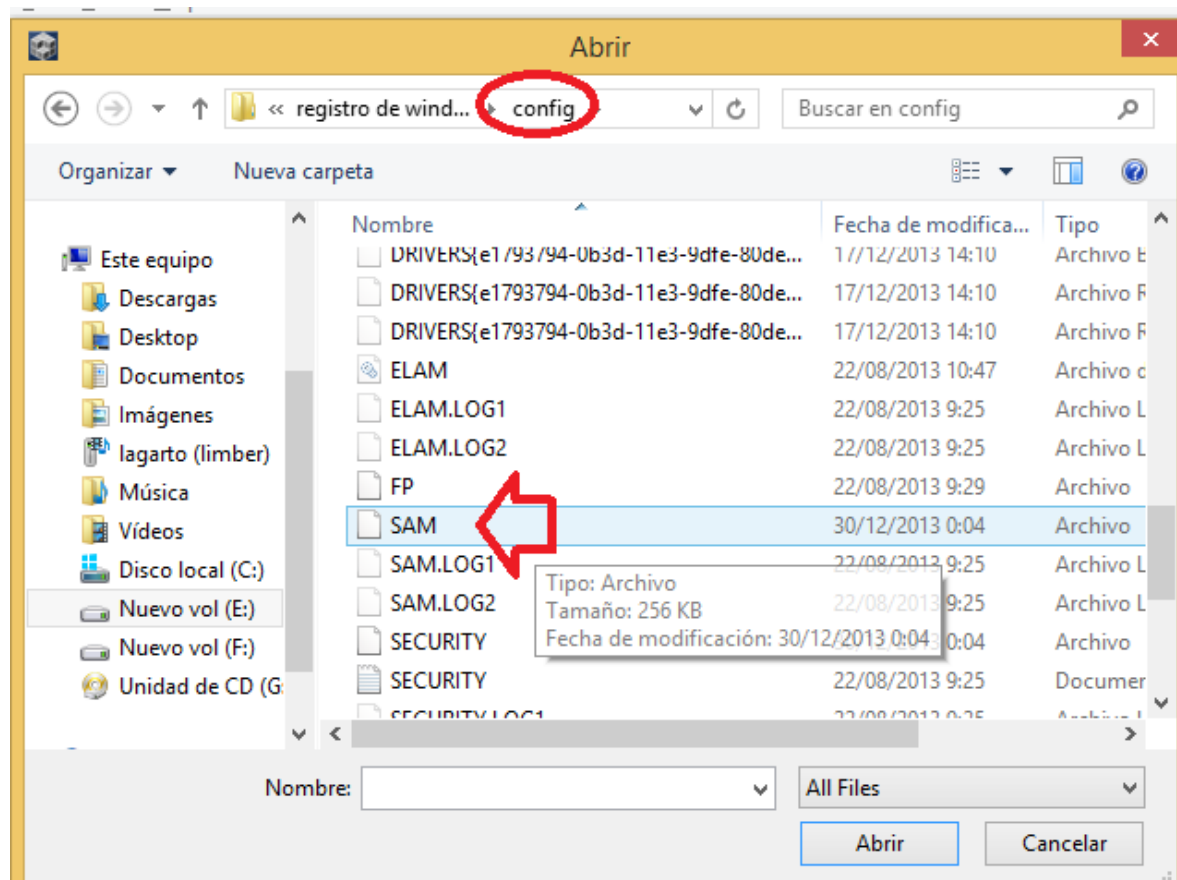


- Seleccionar → SOFTWARE → Microsoft → Windows NT → CurrentVersion
Ahí se puede verificar la versión del Windows instalado en el equipo

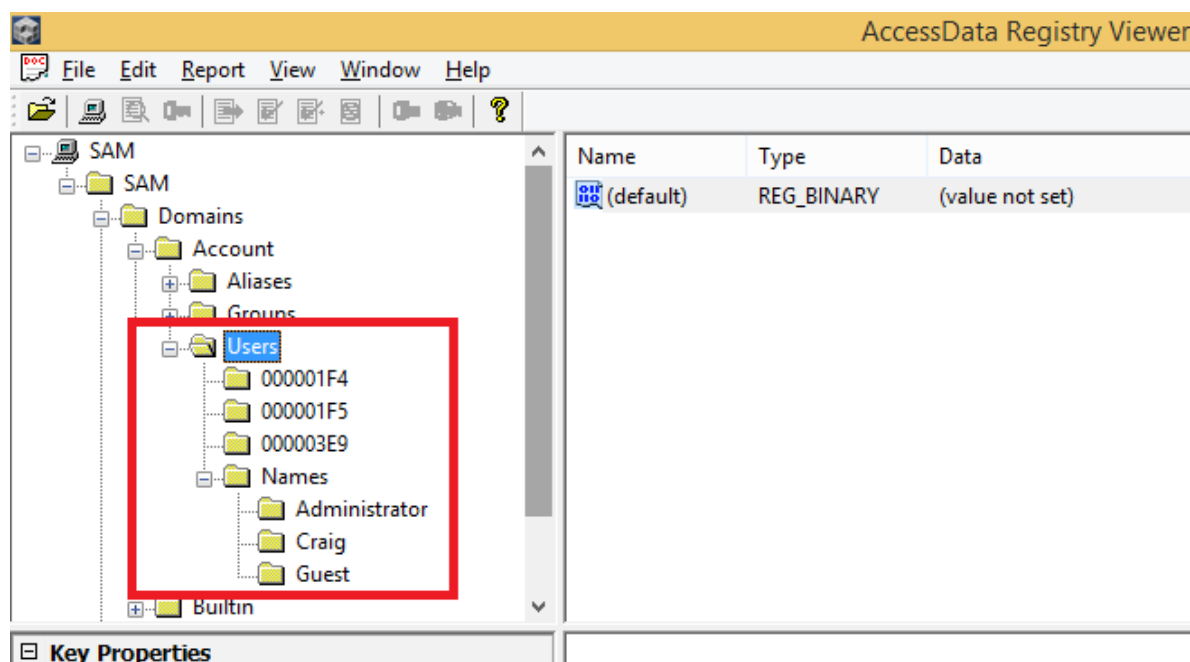


3) Averiguar las cuentas de usuario del Sistema

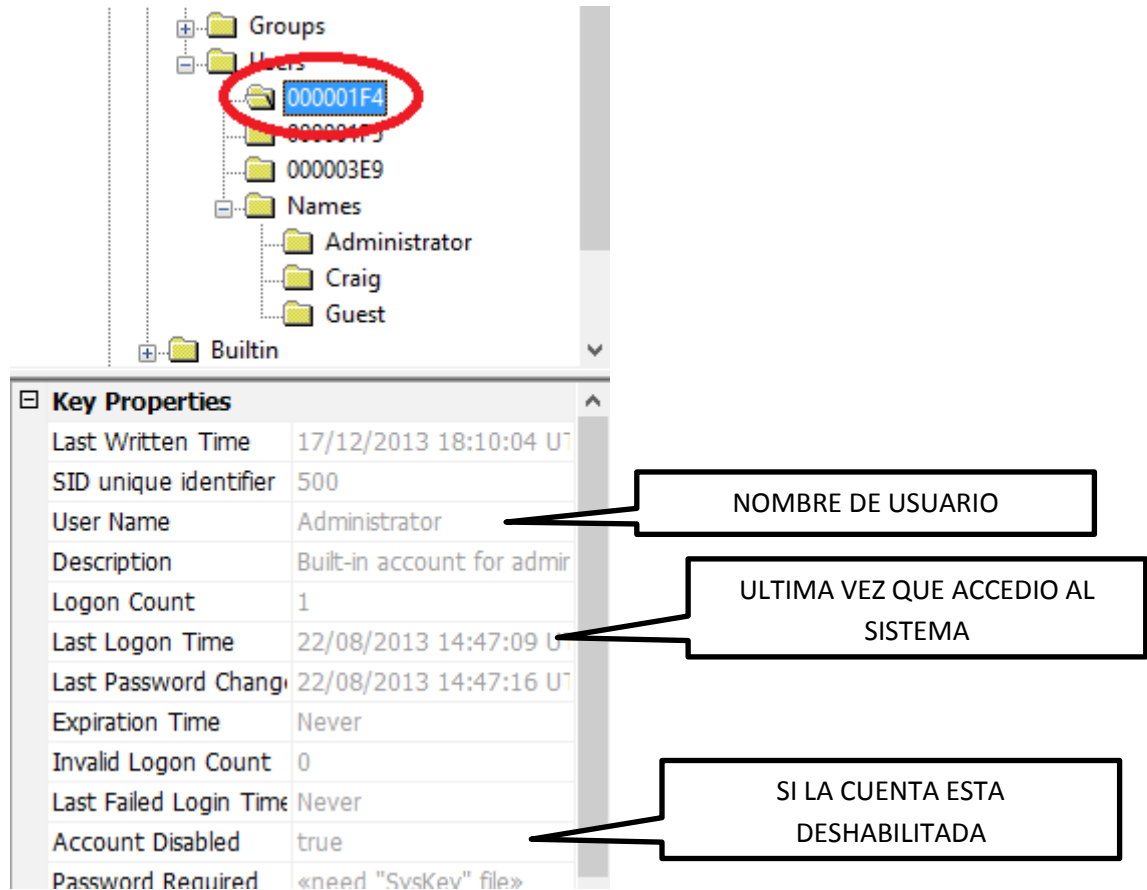
- En el programa Registry Viewer seleccionar del menú File → Open
- Abrir el archivo SAM desde el lugar donde se guardaron los archivos con el programa FTKImager



- Una vez abierto el archivo SAM con el programa Registry Viewer se puede observar tres usuarios y sus nombres



Seleccionando el usuario "000001F4" se puede información al respecto



The screenshot shows the Windows Security console with the 'Users' folder expanded. The user '000001F4' is selected and highlighted with a red circle. Below the folder view, the 'Key Properties' section displays the following information:

Property	Value
Last Written Time	17/12/2013 18:10:04 UT
SID unique identifier	500
User Name	Administrator
Description	Built-in account for admir
Logon Count	1
Last Logon Time	22/08/2013 14:47:09 UT
Last Password Change	22/08/2013 14:47:16 UT
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	true
Password Required	«need "SvsKev" file»

Annotations with callouts point to specific values:

- NOMBRE DE USUARIO** points to the 'User Name' value 'Administrator'.
- ULTIMA VEZ QUE ACCEDIO AL SISTEMA** points to the 'Last Logon Time' value '22/08/2013 14:47:09 UT'.
- SI LA CUENTA ESTA DESHABILITADA** points to the 'Account Disabled' value 'true'.

Seleccionando el usuario "000001F5" se puede información al respecto

The screenshot shows a Windows Security Manager window. In the left pane, a tree view displays folders: '000001F4', '000001F5' (selected), '000003E9', 'Names', 'Administrator', 'Craig', 'Guest', and 'Builtin'. The right pane shows the 'Key Properties' for the selected user '000001F5'.

Key Properties	
Last Written Time	17/12/2013 18:10:04 UT
SID unique identifier	501
User Name	Guest
Description	Built-in account for guest
Logon Count	0
Last Logon Time	Never
Last Password Change	Never
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	true
Password Required	false
Country Code	0 (System Default)
NT Hash	«need "SysKey" file»

Annotations:

- A callout box labeled 'NOMBRE DE USUARIO' points to the 'User Name' field, which contains 'Guest'.
- A callout box labeled 'ULTIMA VEZ QUE ACCEDIO AL SISTEMA' points to the 'Last Logon Time' field, which contains 'Never'.

Seleccionando el usuario "000001F4" se puede información al respecto

The screenshot shows the 'Key Properties' tab for a user named 'Craig'. The following table summarizes the visible information:

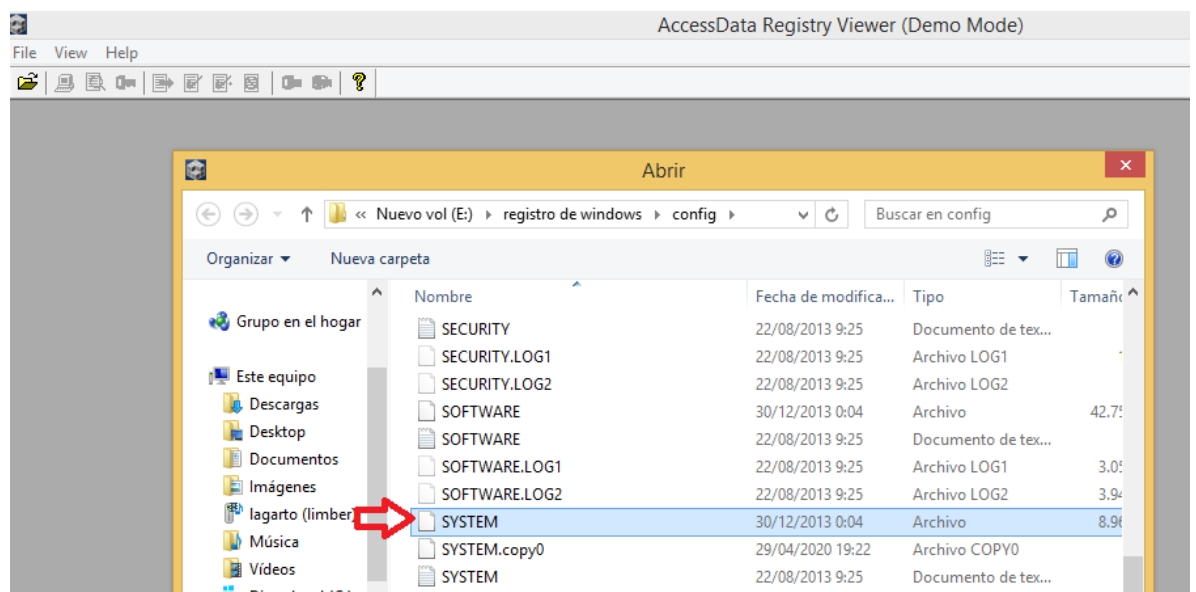
Property	Value
Last Written Time	27/12/2013 8:45:16 UTC
SID unique identifier	1001
User Name	Craig
Full Name	Craig Tucker
Logon Count	4
Last Logon Time	17/12/2013 23:25:49 UTC
Last Password Change	21/12/2013 18:34:37 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	<need "SysKey" file>
Country Code	1 (United States)
Hours Allowed	Anytime

Callouts from the image:

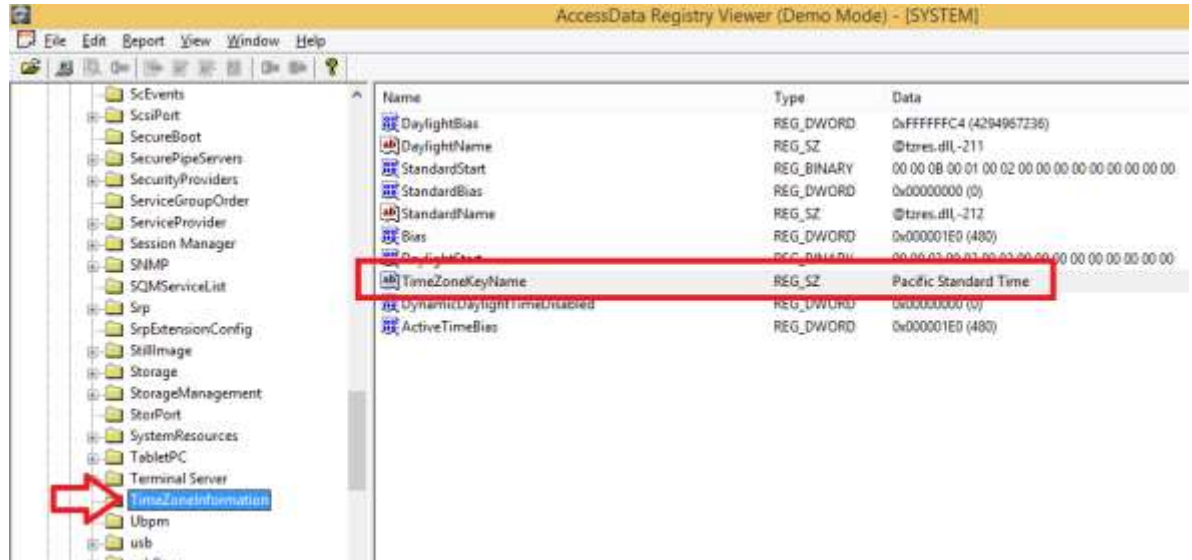
- NOMBRE DE USUARIO**: Points to the 'User Name' field (Craig).
- ULTIMA VEZ QUE ACCEDIO AL SISTEMA**: Points to the 'Last Logon Time' field (17/12/2013 23:25:49 UTC).
- REQUIERE CONTRASEÑA PARA ACCEDER AL SISTEMA**: Points to the 'Password Required' field (<need "SysKey" file>).

4) Averiguar la configuración de la Zona Horaria del Sistema

- En el programa Registry Viewer seleccionar del menú **File→Open** y seleccionar el archivo **SYSTEM**
(De la ubicación donde se extrajeron los archivos con el programa FTK Imager)

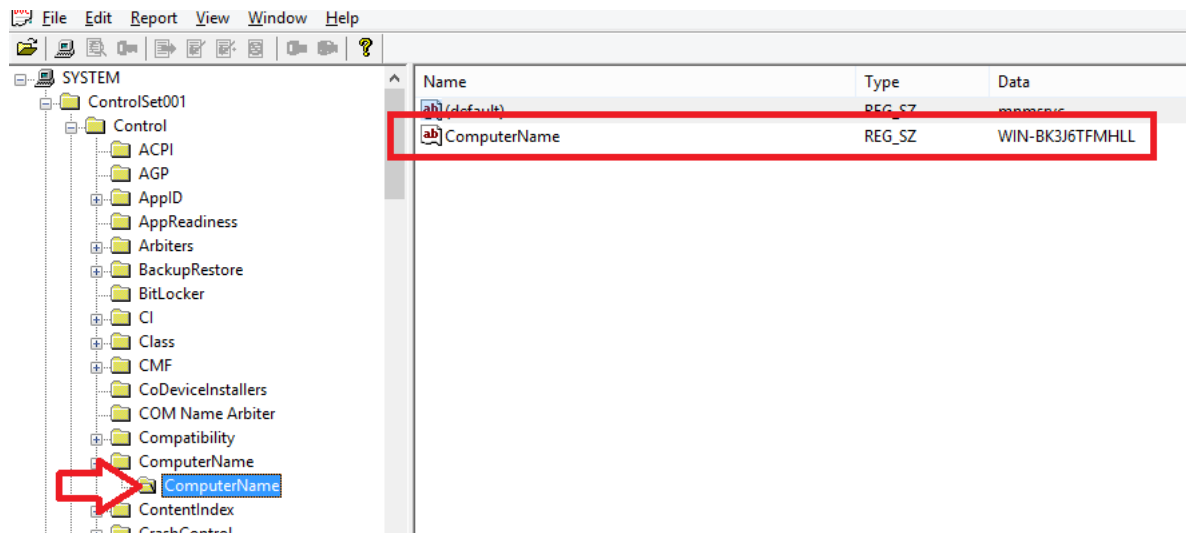


- En el registro acceder a: SYSTEM→ControlSet001 → Control → TimeZoneInformation



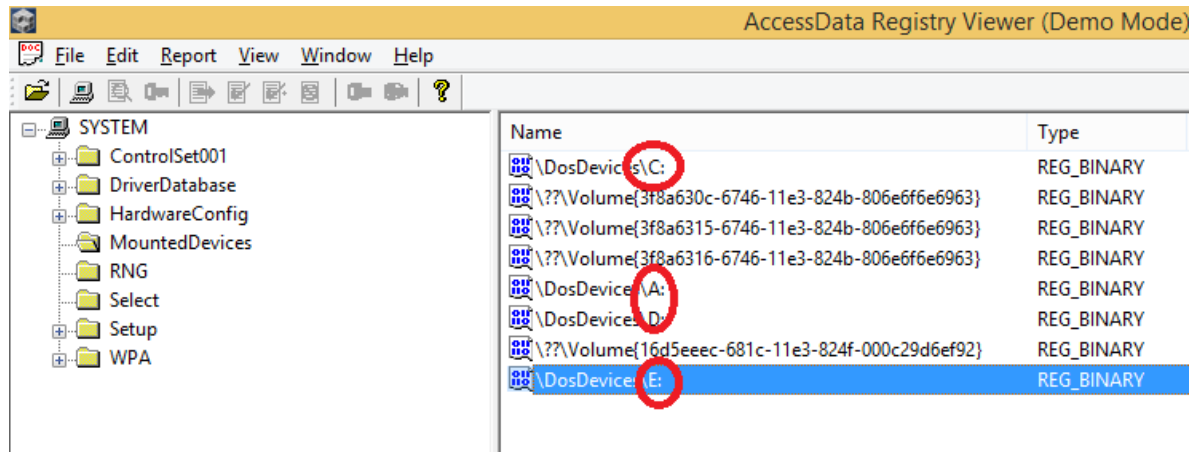
5) Averiguar el Nombre del Equipo

En el registro acceder a: SYSTEM→ControlSet001→Control→ComputerName



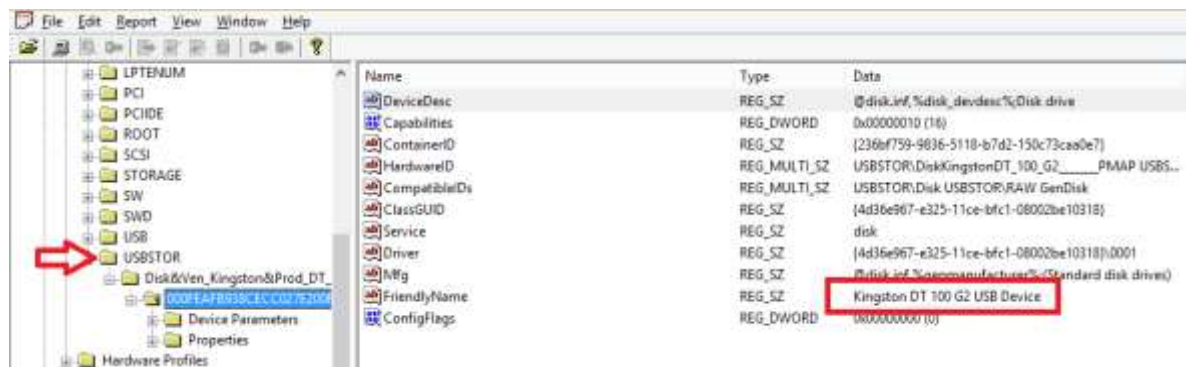
6) Averiguar que dispositivos fueron montados en el Equipo

En el registro acceder a: SYSTEM→MountedDevices



7) Averiguar que dispositivos USB de almacenamiento fueron conectados

En el registro acceder a: SYSTEM→ControlSet001→Enum→USBSTOR



La última vez que conectaron dicho USB

Ir a: Properties → {83da6326 . . . →0066

