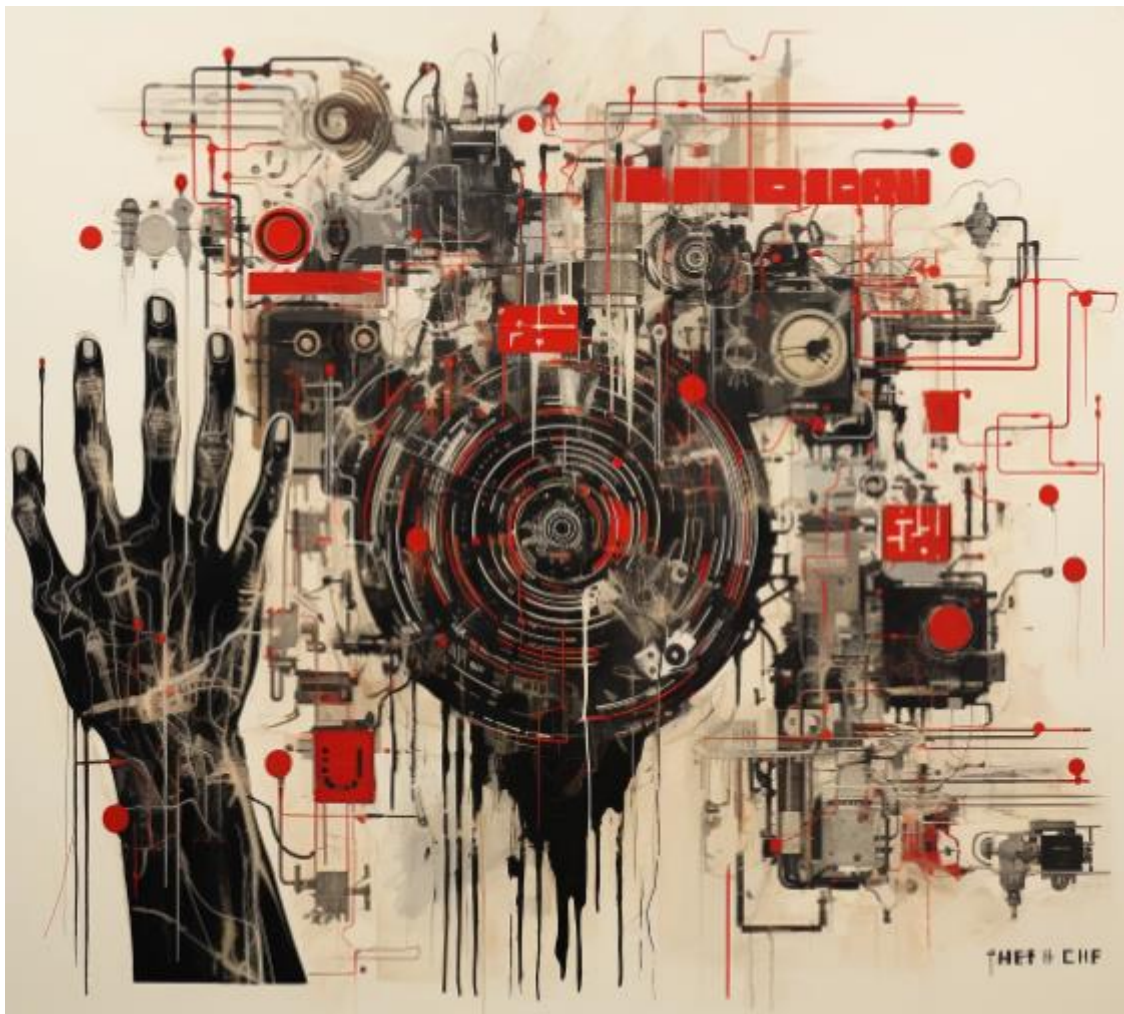


# Lab 1.5 System Profiling

## Teoría

## y

## Práctica



## Examinando la configuración de System



***SYSTEM, SOFTWARE, SECURITY***

### Overview de la configuración de SYSTEM

- Identificar la version del OS de Microsoft
- Current Control Set
- Computer Name
- Time Zone de la maquina
- Network Interfaces
- Historical Networks
- Network Types
- System Autostart Programs
- Last Shutdown Time

## Identificar la versión del OS de Microsoft



Identificar la version de Windows
Proposito
<ul style="list-style-type: none"><li>• Determina la versión de Microsoft Windows, el nivel del service pack y la fecha de instalación de la última versión o actualización principal del sistema operativo utilizando esta clave.<ul style="list-style-type: none"><li>• Identifica la versión del sistema operativo.</li></ul></li></ul>
Localización
<ul style="list-style-type: none"><li>• <b>SOFTWARE\Microsoft\Windows NT\CurrentVersion</b></li></ul>
¿Porque esto es Útil?
<ul style="list-style-type: none"><li>• Es común recibir un disco duro con un sistema operativo Windows desconocido.</li><li>• Esta clave no solo te indicará la versión de Windows y el nivel del service pack instalado, sino que también te mostrará la fecha de instalación del sistema.<ul style="list-style-type: none"><li>• La fecha de instalación también podría significar cuándo se actualizó por última vez el sistema o cuándo ocurrió la última revisión importante. La fecha de instalación no necesariamente significa cuándo se instaló inicialmente el sistema operativo.</li></ul></li></ul>

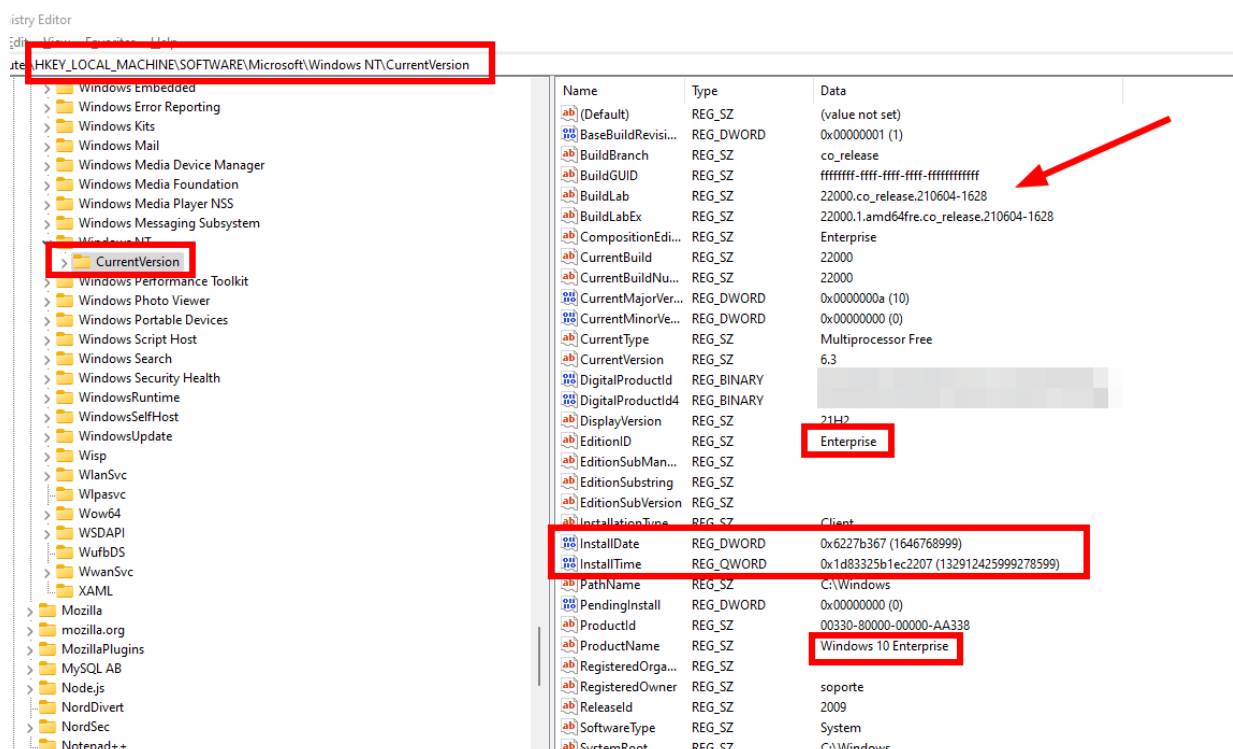


La versión del sistema operativo Windows es crucial para asegurarse de que estás encontrando y utilizando de manera precisa los artefactos correctos durante el proceso análisis. Los directorios, tipos de artefactos e incluso los programas predeterminados cambian según la versión y el service pack del sistema operativo Windows.

No se debe adivinar cuál es la versión del sistema operativo. Esta clave se encuentra en el registro **SOFTWARE**:

**SOFTWARE\Microsoft\Windows NT\CurrentVersion** detallará la versión específica del sistema operativo Windows, el service pack y la fecha de instalación de la máquina que estás investigando.

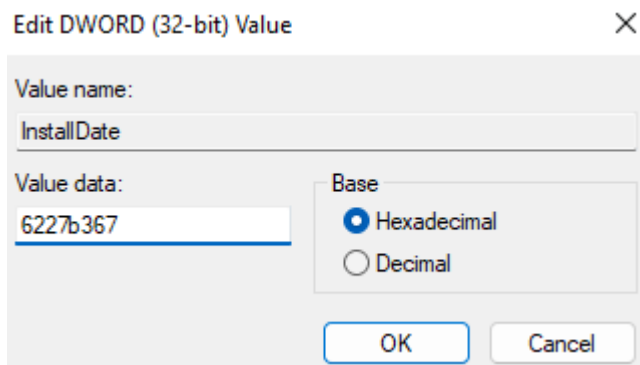
La fecha de instalación es una de las pocas fechas que no sigue el formato de tiempo estándar de Windows de 64 bits. En realidad, es un tiempo EPOCH. La fecha de instalación se basa en el número de segundos desde la 12:00 am del 1/1/1970. A partir de Windows 10, hay un nuevo valor llamado **"InstallTime"** que sigue el tiempo de Windows de 64 bits.



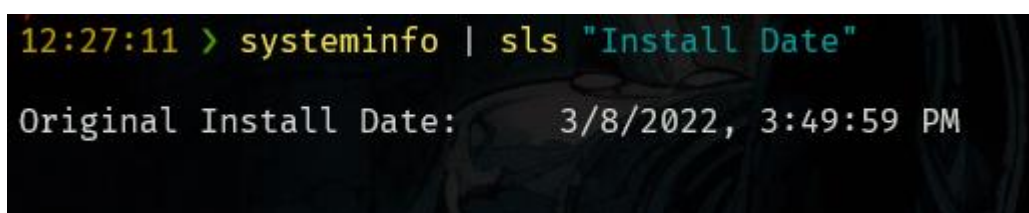
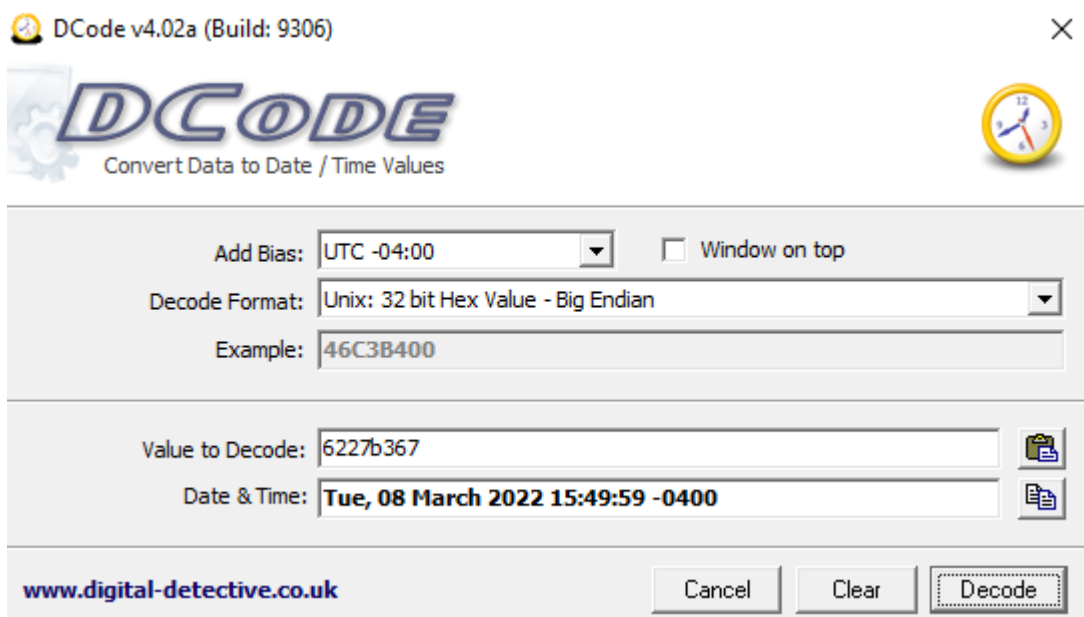
Registry Editor

Path: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Name	Type	Data
(Default)	REG_SZ	(value not set)
BaseBuildRevisi...	REG_DWORD	0x00000001 (1)
BuildBranch	REG_SZ	co_release
BuildGUID	REG_SZ	ffffff-ffff-ffff-ffffff
BuildLab	REG_SZ	22000.co_release.210604-1628
BuildLabEx	REG_SZ	22000.1.amd64fre.co_release.210604-1628
CompositionEdi...	REG_SZ	Enterprise
CurrentBuild	REG_SZ	22000
CurrentBuildNu...	REG_SZ	22000
CurrentMajorVer...	REG_DWORD	0x0000000a (10)
CurrentMinorVe...	REG_DWORD	0x00000000 (0)
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.3
DigitalProductId	REG_BINARY	
DigitalProductId4	REG_BINARY	
DisplayVersion	REG_SZ	21H2
EditionID	REG_SZ	Enterprise
EditionSubMan...	REG_SZ	
EditionSubstring	REG_SZ	
EditionSubVersion	REG_SZ	
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x6227b367 (1646768999)
InstallTime	REG_QWORD	0x1d83325b1ec2207 (132912425999278599)
PathName	REG_SZ	C:\Windows
PendingInstall	REG_DWORD	0x00000000 (0)
ProductId	REG_SZ	00330-80000-00000-AA338
ProductName	REG_SZ	Windows 10 Enterprise
RegisteredOrga...	REG_SZ	
RegisteredOwner	REG_SZ	soporte
ReleaseId	REG_SZ	2009
SoftwareType	REG_SZ	System
SystemRoot	REG_SZ	C:\Windows



Convertimos el valor Hexadecimal usando Data Decode (si estuviéramos usando Registry Explorer nos da la alternativa de Interpretar la fecha, lo veremos mas adelante)



Recuerda que la fecha de instalación puede significar muchas cosas. Podría indicar cuándo se instaló inicialmente el sistema operativo, cuándo tuvo una actualización o revisión importante, o cuándo se actualizó por última vez el sistema. No siempre significa cuándo se instaló inicialmente el sistema. [ [Another Forensics Blog: When Windows Lies](#) ]

## Identificar el CurrentControlSet(I)



Identificar el CurrentControlSet(I)
Propósito
<ul style="list-style-type: none"><li>• Identifica qué conjunto de control (ControlSet00x) se considera el CurrentControlSet.</li><li>• Contiene información sobre la configuración del sistema.</li></ul>
Localización
<ul style="list-style-type: none"><li>• SYSTEM\Select</li></ul>
¿Porque esto es Útil?
<ul style="list-style-type: none"><li>• Determina qué ControlSet00x usar como el "CurrentControlSet".</li><li>• Una vez que identifiques qué ControlSet00x es el "Current Control Set", debemos encentrarnos en este lugar</li></ul>

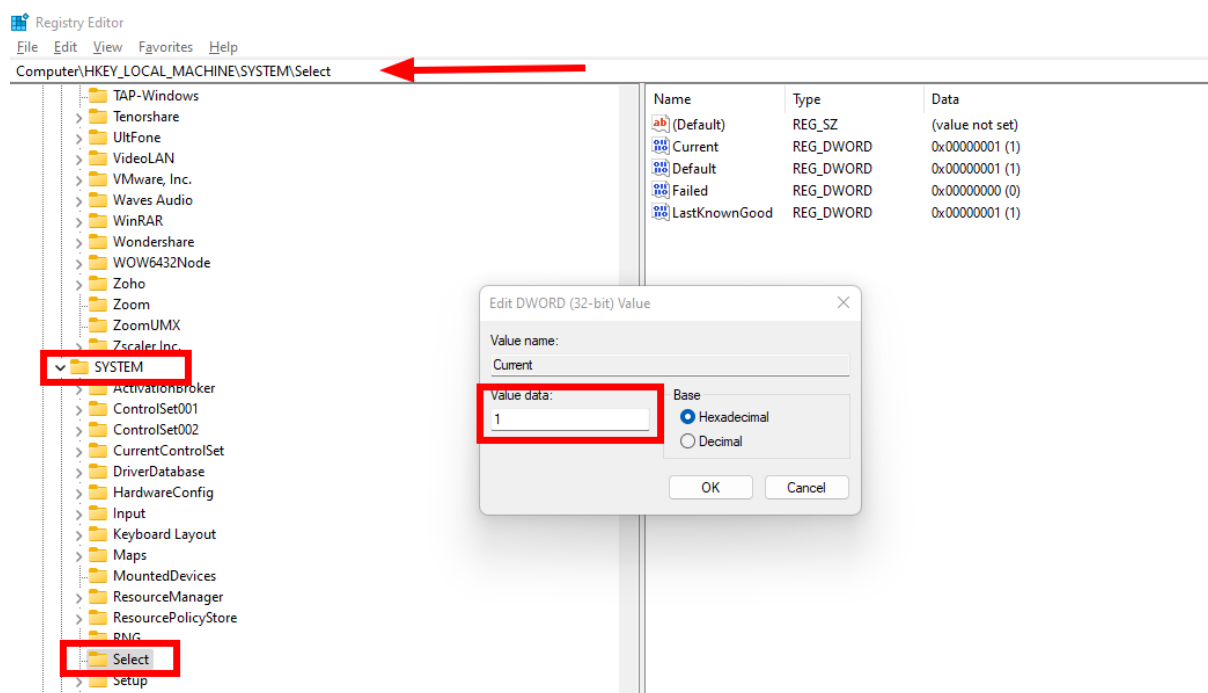
Un conjunto de control (control set) contiene configuraciones del sistema necesarias para controlar el arranque del sistema, como información de controladores y servicios.

¿Por qué generalmente hay dos conjuntos de control (**ControlSet001 y ControlSet002**)?

ControlSet001 es típicamente el conjunto de control en el que acabas de arrancar la computadora. Por lo general, es la versión más actualizada del ControlSet.

**ControlSet002** es la versión de "**Última configuración buena conocida**" ("Last Known Good"). Esta versión se considera buena cuando ocurrió el arranque anterior en caso de que algo drástico haya sucedido durante el ciclo de arranque actual.

Considerando que estamos examinando el **ControlSet** en una máquina no activa, otra forma de ver esto es que **ControlSet001** sería el último arranque exitoso de la máquina y **ControlSet002** sería el "arranque exitoso" anterior a ese.

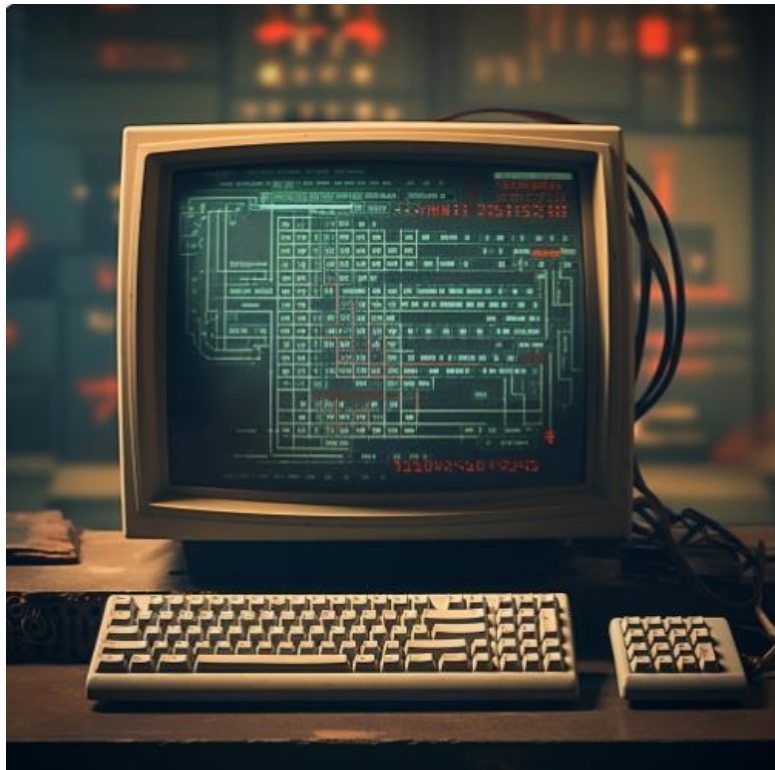


Cuando abrimos una muestra del hive del sistema (SYSTEM) , notamos de inmediato que hay dos rutas de registro para los **ControlSets**: **ControlSet001** y **ControlSet002**. Para examinar la información crítica del sistema para esta máquina, necesitamos saber cuál de esas dos rutas de registro es la representación del Hive Volátil "**CurrentControlSet**". Para lograr esto, examinamos la **clave Select**.

Usando Regedit, vamos a la ruta donde está la key **Select**. El REG\_DWORD, **Current** para la clave **Select** contiene el número del **ControlSet00x que es "actual"**. En este ejemplo, el valor actual está establecido en 0x1 o "**1**". Por lo tanto, el **ControlSet001** es la ruta de registro que está configurada como el "**CurrentControlSet**" y la que debe examinarse en profundidad.

La segunda cosa que podrías notar es que la clave "LastKnownGood" está actualmente configurada en 0x1 o "1", lo que significa que ControlSet001 es la instantánea LastKnownGood de esta ruta de registro durante el último arranque exitoso que ocurrió en esta máquina.

## Computer Name



Computer Name
Proposito
<ul style="list-style-type: none"><li>Identificar el nombre de la computadora en el campo System Properties</li></ul>
Localización
<ul style="list-style-type: none"><li>•SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName</li></ul>
¿Porque esto es Útil?
<ul style="list-style-type: none"><li>El nombre del equipo puede estar vinculado a archivos de registro, conexiones de red y otras actividades.<ul style="list-style-type: none"><li>Se utiliza como una verificación del PC que estás examinando forensemente.</li></ul></li></ul>



El nombre del equipo es útil principalmente para fines de registro y verificación, pero no debe pasar desapercibido. El nombre de la máquina también aparecerá en otras ubicaciones del sistema, pero lo que uso es para estar en la PC correcta que me dijeron, además de tomar nota de la información para su uso y correlación posterior. La ubicación del nombre del equipo está en el hive del sistema:

### **SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName**

The screenshot displays the Windows Registry Editor. The left pane shows the tree structure with the path **SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName** selected. The right pane shows the details for the **ComputerName** value, which is of type **RegSz** and has the data **SRL-FORGE**. A red box highlights the **ComputerName** key in the left pane and the **ComputerName** value in the right pane.

Value Name	Value Type	Data
(default)	RegSz	mnmsrvc
ComputerName	RegSz	SRL-FORGE

## Time Zone Information



Time Zone Information
Propósito
<ul style="list-style-type: none"><li>• Identifica la zona horaria actual del sistema.</li></ul>
Localización
<ul style="list-style-type: none"><li>• SYSTEM\CurrentControlSet\Control\TimeZoneInformation</li></ul>
¿Porque esto es Útil?
<ul style="list-style-type: none"><li>• La actividad temporal es increíblemente útil para la correlación de actividades.</li><li>• Los archivos de registro internos y las fechas/horas estarán basados en la información de la zona horaria del sistema.</li><li>• Es posible que tengas otros dispositivos de red y necesitarás correlacionar la información con la información de la zona horaria recopilada aquí.</li></ul>

Aunque la mayoría de los tiempos de registro y últimos tiempos de escritura se registrarán en UTC, el tiempo general del sistema tendrá sus archivos de registro y otra información basada en el tiempo vinculados a la zona horaria específica. Un buen ejemplo de esto son las marcas de tiempo del sistema de archivos FAT. Las marcas de tiempo del sistema de archivos FAT se actualizarán y asociarán con la zona horaria local establecido en el applet del Panel de Control que controla esa zona horaria.

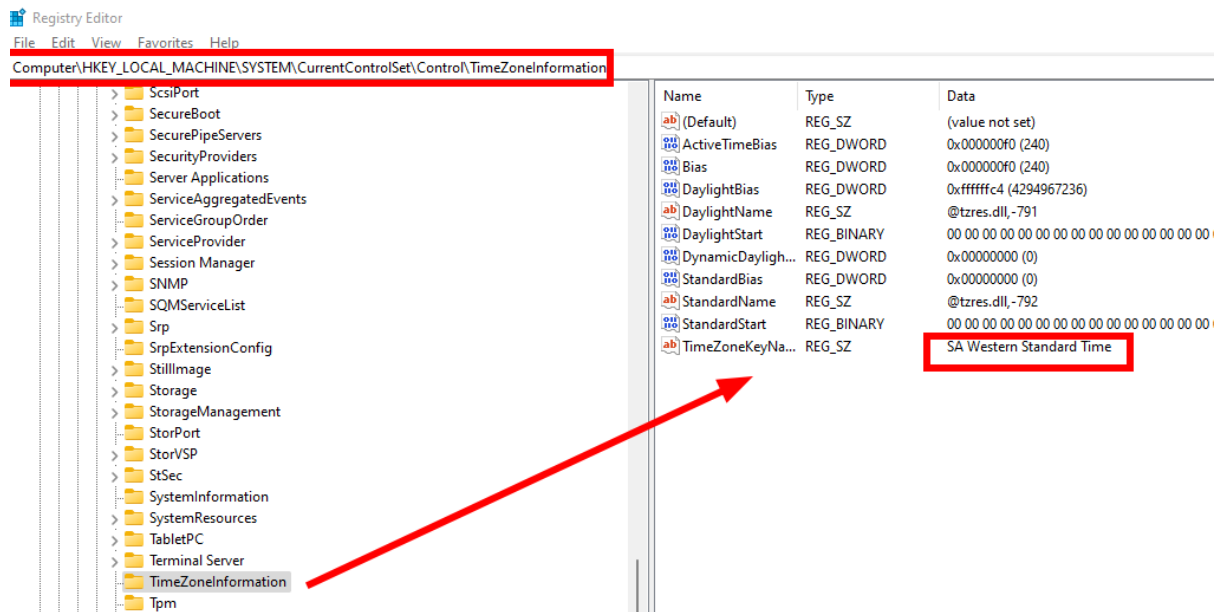
Un usuario podría cambiar fácilmente la zona horaria. El último tiempo de escritura en esta clave mostrará la última vez que se cambió la zona horaria para esta máquina.

Se recomienda **ENCARECIDAMENTE** que ajustes la hora de tu máquina de análisis local a UTC para evitar cualquier sesgo que podría agregarse accidentalmente desde una herramienta forense y potencialmente llevar a la interpretación errónea de datos relacionados con el tiempo en tu caso. Siempre puedes refactorizar la hora local en tu informe más tarde, pero UTC proporciona un formato fácil para realizar análisis y reduce la exposición a errores de conversión o interpretación incorrecta.

Algunas fórmulas útiles incluyen:

- $UTC = \text{Hora local} + \text{Sesgo de hora activa}$
- $\text{Hora local} = UTC - \text{Sesgo de hora activa}$
- $\text{Hora estándar} = \text{Sesgo} + \text{Sesgo estándar}$
- $\text{Hora de verano} = \text{Sesgo} + \text{Sesgo de horario de verano}$

+Info: [TIME\\_ZONE\\_INFORMATION structure](#)



Este es un ejemplo de la ubicación de la información de la zona horaria dentro del hive del sistema (SYSTEM). En este caso, la zona horaria está configurada en Western Standard Time. La información de la zona horaria es importante recordarla para la información basada en el tiempo. Algunos datos del sistema informático se establecen en hora local. Otros datos, incluidas las claves del registro, se establecen en GMT o Tiempo Universal Coordinado (UTC).



## Network Interfaces



Network Interfaces
Propósito
<ul style="list-style-type: none"><li>• Identifica las tarjetas de interfaz de red (NIC) de la PC</li></ul>
Localización
<b>•SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces</b>
¿Porque esto es Útil?
<ul style="list-style-type: none"><li>• Enumera las interfaces de red de la máquina.</li><li>• Puede determinar si la máquina tiene una dirección IP estática o si está configurada por DHCP.</li><li>• Vincula la máquina a la actividad de red que se registró.</li><li>• Obtiene el GUID de la interfaz para un perfil adicional en las conexiones de red.</li></ul>

Poder listar las interfaces de red es muy importante. No solo es la interfaz de red la clave para muchos casos, sino que también puede ahorrarte muchos problemas a largo plazo.

La ubicación clave se encuentra aquí en el hive del sistema (SYSTEM):

## **SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces**

Esta clave contendrá mucha información que es bueno conocer y entender. Específicamente, te permitirá ver la información de **TCP/IP** configurada, la dirección IP, la puerta de enlace y otra información potencialmente útil. Si la máquina estaba configurada para DHCP, contendrá la dirección IP asignada por DHCP, la máscara de subred y la dirección IP del servidor DHCP.

Esta información podría ser increíblemente útil para un caso que tenga información recopilada basada en la red. Una vez más, esto es algo que se considera información esencial y básica que se debe mostrar sobre la máquina al compilar un informe.

El GUID de la interfaz también se podría utilizar para correlacionar datos de perfil de red adicionales obtenidos en claves de registro adicionales. Es útil escribir las interfaces y sus respectivos GUID durante un caso para poder determinar exactamente cómo se accedió a una red (inalámbrica, cableada, 3G y Bluetooth).

## Historical Networks – Network List Keys



Historical Networks – Network List Keys	
Propósito	
<ul style="list-style-type: none"><li>• Identifica las redes a las que se ha conectado el ordenador.<ul style="list-style-type: none"><li>• Las redes pueden ser inalámbricas o cableadas.</li></ul></li><li>• Identifica el nombre de dominio/nombre de intranet.<ul style="list-style-type: none"><li>• Identifica el SSID (Service Set Identifier).</li></ul></li><li>• Identifica la dirección MAC de la puerta de enlace.</li></ul>	
Localización	
<ul style="list-style-type: none"><li>• SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged</li><li>• SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed</li><li>• SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache</li></ul>	
¿Porque esto es Útil?	
<ul style="list-style-type: none"><li>• Identificar las intranets y redes a las que se ha conectado una computadora es increíblemente importante.</li></ul>	

- Se registra la primera y última vez que se estableció una conexión de red.
- Esto también enumerará cualquier red a la que se haya conectado a través de una VPN.
- La dirección MAC del SSID para la puerta de enlace podría ser triangulada físicamente.

Network Location Awareness (NLA, por sus siglas en inglés) ha sido incorporada en Windows 7 y versiones posteriores para ayudar al usuario a identificar dónde podría estar conectada la computadora y ajustar la configuración del firewall. Esto también permite obtener información forense muy única a través de esta estructura.

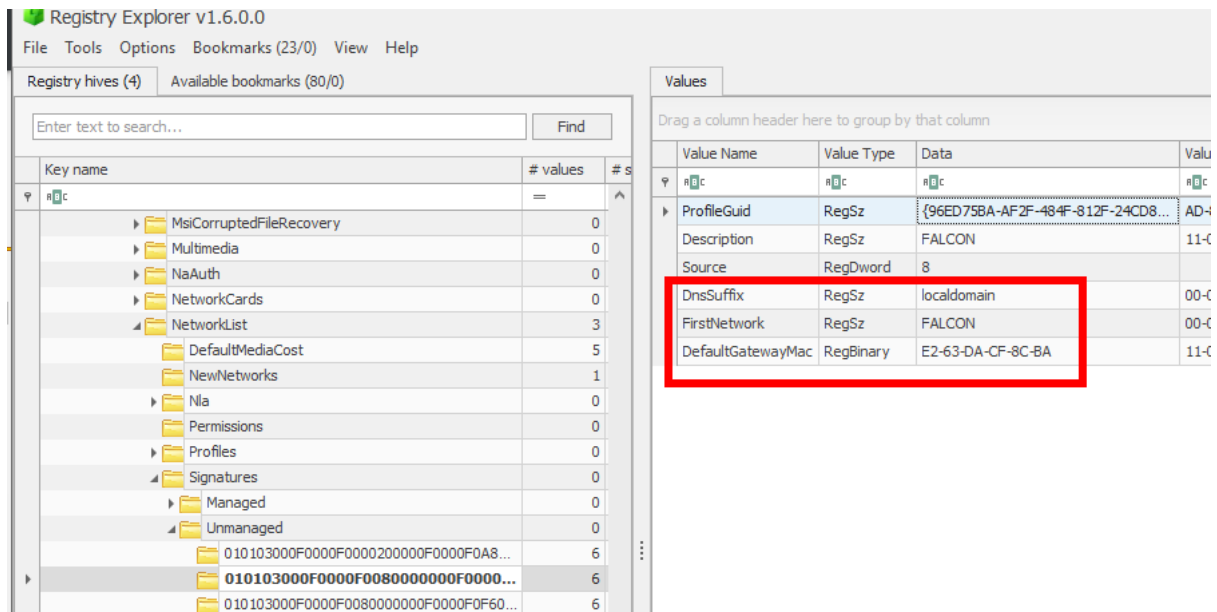
"Primero, comencemos con lo que hace NLA. Para cada interfaz de red a la que está conectada la PC, NLA recopila la información de red disponible para la PC y genera un identificador único a nivel mundial (GUID) para identificar cada red.

En otras palabras, crea un perfil de red para cualquier red a la que se conecta. Luego, el Firewall de Windows utiliza esa información para aplicar reglas del perfil correspondiente del firewall de Windows. Esto te permite aplicar un conjunto diferente de reglas de firewall dependiendo de a qué red estés conectado. Por ejemplo, una red pública podría recibir un conjunto de reglas muy restrictivo, una red doméstica podría recibir un conjunto de reglas menos restrictivo, y una red gestionada podría recibir un conjunto de reglas determinado por un administrador".

Con NLA, se mostrará una lista de todas las redes a las que la máquina ha estado conectada alguna vez a través de su sufijo DNS (por ejemplo, Google.com). Identificar intranets y redes a las que una computadora se ha conectado es increíblemente importante.

Esto es útil esta clave debido al hecho de que, en algunos casos, solo examinando esta clave, podría ser capaz de proporcionar la geolocalización de dónde podría haber estado esta laptop, basado en la identificación de las redes a las que se conectó y cuándo.





## Los detalles del registro:

La mayor parte de la información sobre NLA se almacenará en los siguientes tres lugares:

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\NetworkList
- HKLM\Software\Microsoft\Windows\CurrentVersion\HomeGroup
- C:\Windows\System32\NetworkList

Los datos históricos se pueden encontrar bajo la clave Cache:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

## Network Profiles Key – First and Last Times Connected



Network Profiles Key – First and Last Times Connected
Proposito
<ul style="list-style-type: none"><li>• Identifica el tipo de red a la que se conectó la computadora.</li><li>• Identifica los SSID inalámbricos a los que la computadora se conectó anteriormente.</li><li>• El tiempo se registra en HORA LOCAL, NO UTC.</li></ul>
Localización
<ul style="list-style-type: none"><li>• SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID} (XP)</li><li>• SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles (Win7-10)</li></ul>

<ul style="list-style-type: none"> <li>• Encuentra el GUID de las redes históricas de Win7+ en la lista.</li> </ul>
<p><b>¿Porque esto es Útil?</b></p> <ul style="list-style-type: none"> <li>• Enumera las redes a las que se ha conectado la máquina, incluyendo la primera y última vez de conexión.</li> <li>• Determina el tipo de conexión de red utilizando el valor Nametype. <ul style="list-style-type: none"> <li>- Nametype Value = 6 (0x06) = Cableada [ Wired ]</li> <li>- Nametype Value = 23 (0x17) = VPN</li> <li>- Nametype Value = 71 (0x47) = Inalámbrica [ Wireless ]</li> <li>- Nametype Value = 243 (0xF3) = Banda Ancha Móvil [Mobile Broadband]</li> </ul> </li> </ul>

Para Windows XP, la información final de red que examinaremos son los ajustes de red inalámbrica encontrados en la configuración de "**Windows Wireless Zero Configuration**". Estos ajustes se utilizan para que una máquina recuerde automáticamente los puntos de acceso anteriores a los que se ha conectado y sus respectivos SSID. El SSID es un identificador de seguridad único que la máquina utiliza para saber que ha visto esta red antes y, si está permitido, conectarse nuevamente a ella.

Hay muchos casos en los que saber que una máquina estaba cerca de una ubicación y conectada a esa red específica podría ser decisivo para un caso.

La ubicación clave es

**SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID}.**

Debajo de los identificadores GUID, verás las redes inalámbricas específicas a las que se conectó la máquina. El tiempo de última escritura es la última vez que esta máquina se conectó a esa red en UTC. Nuevamente, esta es información muy útil para un investigador.

Si la máquina es un sistema Windows 7–10, la clave está en una ubicación muy diferente. La clave ahora se encuentra en

**SOFTWARE\Microsoft\Windows**

**NT\CurrentVersion\NetworkList\Profiles.** Cada subclave ubicada en esta clave contendrá un GUID que contendrá el nombre de la red y el tipo de red. Los tipos de red comunes incluyen **0x06 (hex) para**

**cableado, 0x17 (hex) para conexiones VPN/WWAN, 0x47 (hex) para inalámbricas y 0xF3 (hex) para conexiones de banda ancha móvil.**

Poder identificar el tipo de red será útil para determinar cómo un usuario se conectó a un nombre de red definido anteriormente . Usando el ProfileGuid que encontramos anteriormente, puedes mapear la información de red histórica con la dirección MAC y el SSID a la fecha y hora correctas de la última conexión.

Debajo de esta clave, también identificarás la **CreationTime** y la **LastDateConnected**. Ambos tiempos se pueden decodificar usando la herramienta **DCodeDate** ubicada en en la carpeta de HackConRD utilizando el tiempo del sistema de 128 bits de Windows como valor para decodificar. Esto te permitirá ver la primera y última vez que se conectó a la red. El tiempo se almacenará en la Hora del Sistema Local y, por lo tanto, deberá convertirse para que coincida con otros registros de tiempo en formato UTC.

**Nota: Las diferentes categorías**

Public (0) – Sharing Disabled

Private (1) – Home, Sharing Enabled

Domain (2) – Work, Sharing Enabled



## Geolocation de MAC Address/SSID



Una de las estrategias de investigación más interesantes que puedes lograr con la dirección MAC y el SSID de la red inalámbrica que podemos descubrir es intentar determinar la geolocalización del punto de acceso utilizado para la conexión. Ser capaz de descubrir y precisar la ubicación exacta y el momento en que un ordenador o dispositivo específico estuvo podría ser increíblemente importante para un caso. Imagina si estás investigando una computadora portátil que puede ser colocada cerca de la escena del crimen. Si puedes vincular al individuo con la computadora portátil, su coartada no se sostiene, y entonces esta ingeniosa capacidad dará sus frutos.

Usando **<http://wigle.net>** o el `macl.pl` interno encontrado en el directorio `C:\Forensic Program Files\Perl-Scripts` en la maquina virtual proporcionada, puedes identificar fácilmente dónde un dispositivo podría haberse conectado a la red. Correlacionando esto con los primeros tiempos de fecha de última conexión y fecha de creación, puedes verificar el cuándo y dónde de la ubicación de una computadora portátil.



## System Boot autostart Programs



System Boot Autostart Programs
<b>Proposito</b>
<ul style="list-style-type: none"><li>• Enumera programas que muestran persistencia, que se ejecutan al inicio de sesión del usuario o al inicio del sistema.</li></ul>
<b>Localización</b>
<ul style="list-style-type: none"><li>• NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run<ul style="list-style-type: none"><li>• NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnce<ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run<ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Run</li><li>• (SERVICES) SYSTEM\CurrentControlSet\Services</li><li>• Si el valor Start está configurado en 0x02, entonces la aplicación del servicio se iniciará en el arranque (0x00 para controladores).</li></ul></li></ul></li></ul></li></ul>
<b>¿Porque esto es Útil?</b>

- Determinar los programas que se iniciarán automáticamente.
- Útil para encontrar malware en una máquina que se instala en el arranque, como un rootkit.
- Observar cuándo se actualizó por última vez la clave de tiempo; generalmente sería la última vez que se inició el sistema.

Los elementos presentes en las listas anteriores se ejecutan durante un evento de inicio de sesión de usuario. Estas claves existen tanto en el NTUSER.DAT como en las colmenas de SOFTWARE.

Los elementos presentes en la clave de **Servicios [ Services]** pueden configurarse para iniciar en el momento del arranque del sistema.

#### **SYSTEM\CurrentControlSet\Services**

Si el valor de Inicio está configurado en 0x00, entonces el servicio representa un controlador (driver) que se inicia en el momento del arranque.

Si el valor de Inicio está configurado en 0x02, entonces la aplicación del servicio se iniciará en el momento del arranque.



## Shutdown Information



Shutdown Information
Propósito
<ul style="list-style-type: none"><li>• Descubrir cuándo fue la última vez que se apagó el sistema</li><li>• Descubrir cuántas veces se ha apagado exitosamente el sistema</li></ul>
Localización
<ul style="list-style-type: none"><li>•SYSTEM\CurrentControlSet\Control\Windows (Hora de apagado)</li><li>•SYSTEM\CurrentControlSet\Control\Watchdog\Display (Conteo de apagados) - SOLO XP</li></ul>
¿Porque esto es Útil?
<ul style="list-style-type: none"><li>• La última hora de apagado puede ser útil para detectar ciertos tipos de actividad.</li><li>• El conteo de apagados también muestra si el usuario suele apagar correctamente su máquina.</li></ul>

A veces es necesario saber cuándo fue la última vez que se apagó el sistema además de cuántas veces se apagó correctamente. Las siguientes claves serán útiles:

SYSTEM\CurrentControlSet\Control\Windows (Hora de apagado)

## SYSTEM\CurrentControlSet\Control\Watchdog\Display (Conteo de apagados)

La última hora de apagado puede ser útil para detectar ciertos tipos de actividad. El conteo de apagados también muestra si el usuario suele apagar correctamente su máquina. Desde el punto de vista de la investigación, esto puede no ser crítico en todos los casos, pero en ciertos casos, podría ser útil obtener estos datos.

Aquí vemos un ejemplo del valor ShutdownTime presente en

## SYSTEM\CurrentControlSet\Control\Windows

ShutdownTime se almacena como un valor hexadecimal en el formato **FILETIME de 64 bits** de Windows. Registry Explorer incluye una función de intérprete de datos incorporada que intentará convertir los valores en una multitud de formatos diferentes.

The screenshot shows the Registry Explorer interface. On the left, the tree view is expanded to 'SYSTEM\CurrentControlSet\Control\Windows'. A red arrow points from the 'Windows' folder to the 'ShutdownTime' value in the right pane. The 'Data Interpreter' window is open, displaying various conversion options for the 64-bit FILETIME value. The 'Numbers' tab is selected, and the 'Windows FILETIME (64 bit)' option is highlighted in red. The 'Dates and times' tab is also visible, showing the conversion of the FILETIME value to a human-readable date and time.

Value Name	Value Type	Data	Value SI...	Is Delet...	Data f
ComponentizedBuild	RegDword	1			
CSDBuildNumber					
CSDReleaseType					
CSDVersion					
Directory					
ErrorMode					
FullProcessInformationSI					
NoInteractiveServices					
ShellErrorMode					
SystemDirectory					
ShutdownTime					

**Data Interpreter**

**Numbers**

Format	Value
8 bit, signed	94
8 bit, unsigned	94
16 bit, signed	25,950
16 bit, unsigned	25,950
32 bit, signed	1,913,546,078
32 bit, unsigned	1,913,546,078
64 bit, signed	132,495,559,696,999,774
64 bit, unsigned	132,495,559,696,999,774
Float	2.820443E+30
Double	8.48104706336161E-300

**Dates and times**

Format	Value
DOS FAT Time/date (32 bit)	n/a
DOS FAT Date/time (32 bit)	2030-10-30 14:16:28
Unix Posix (32 bit)	2030-08-31 12:34:38
Windows FILETIME (64 bit)	2020-11-11 08:12:49
OLE 32-bit Date/time (64 bit)	1899-12-30 00:00:00
Windows SYSTEM Date/time (128 bit)	n/a

**Other**

Format	Value
GUID	n/a
Maps to	n/a
IP Address	94.101.14.114
Product Key (<= Win7)	n/a
Product Key (>= Win8)	n/a

**Strings**

Format	Value
ASCII	^e 0 _ 0 □
Unicode	微软 810
To Base64	XmUOcGK41gE=
From Base64	n/a

**NOTE: Data is interpreted from the current offset and is not based on t**

## Laboratorio 1.5 – System Profiling



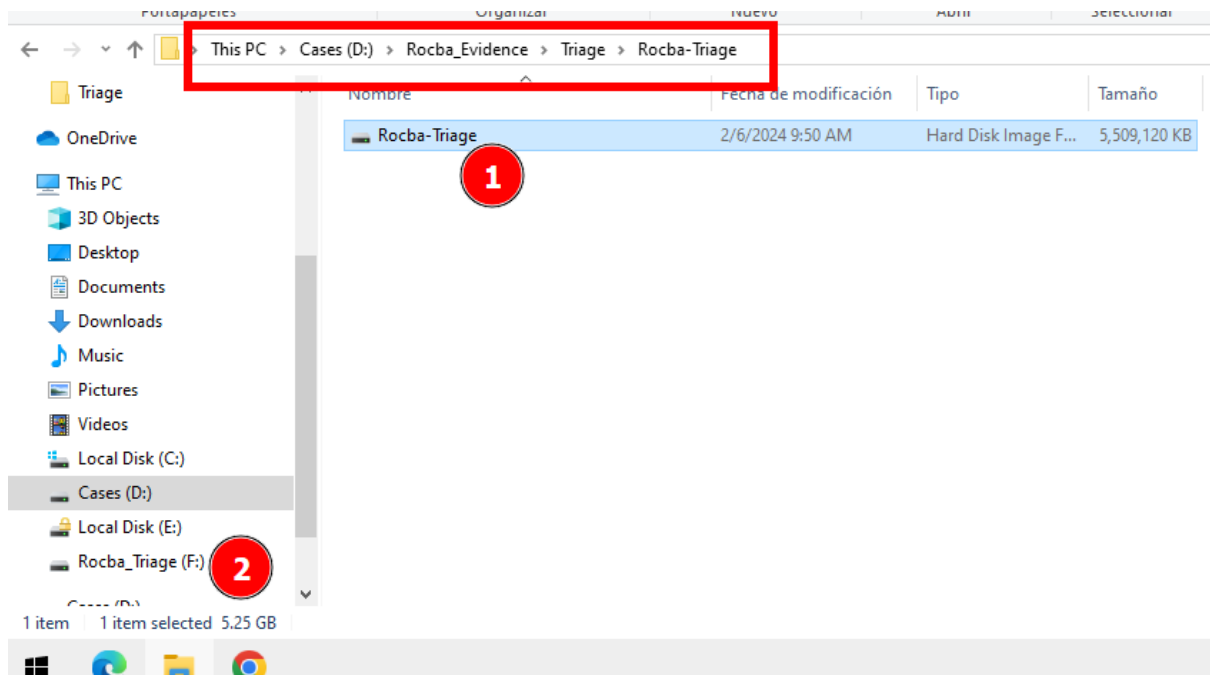
### Objetivos:

Comprender el sistema que estás examinando es crucial para asegurarse de no cometer errores simples mientras realizas análisis más complejos más adelante. Saber algo tan simple como cuántas interfaces de red existen, la configuración de zona horaria e incluso el nombre del sistema son piezas de información crucial necesarias para analizar un sistema correctamente. Dedica un tiempo aquí y explora la información que se puede extraer de estas bases de datos útiles.

- Perfilar el sistema que estaremos analizando. Identifica el nombre del sistema, la última hora de actualización, la zona horaria y otra información importante del sistema.

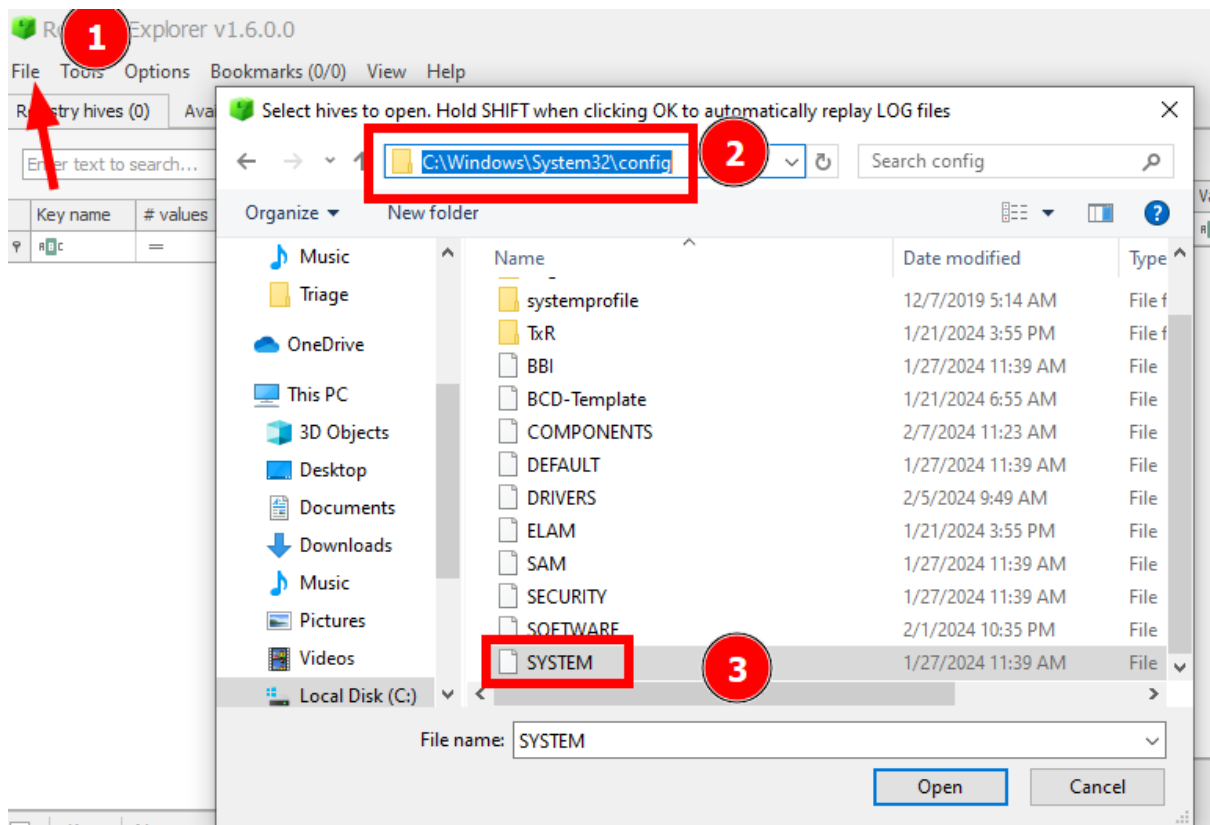
- Perfilar las redes a las que el sistema se ha conectado.  
Identifica las primeras y últimas horas de conexión de las conexiones de red relevantes.

Procedemos a montar el Triage evidence en nuestra ruta

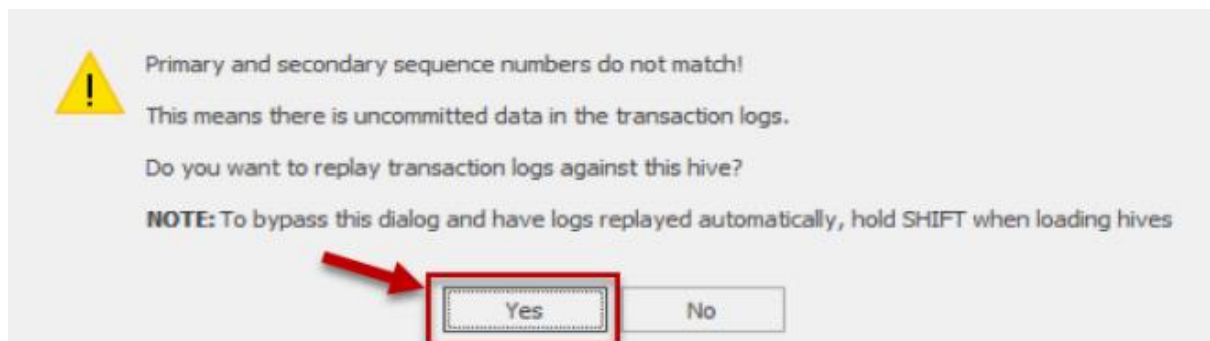


Abrimos Registry Explorer que esta en nuestro Desktop y procedemos a buscar el offline Hive en la siguiente ruta:

**F:\C\Windows\System32\Config\SYSTEM**



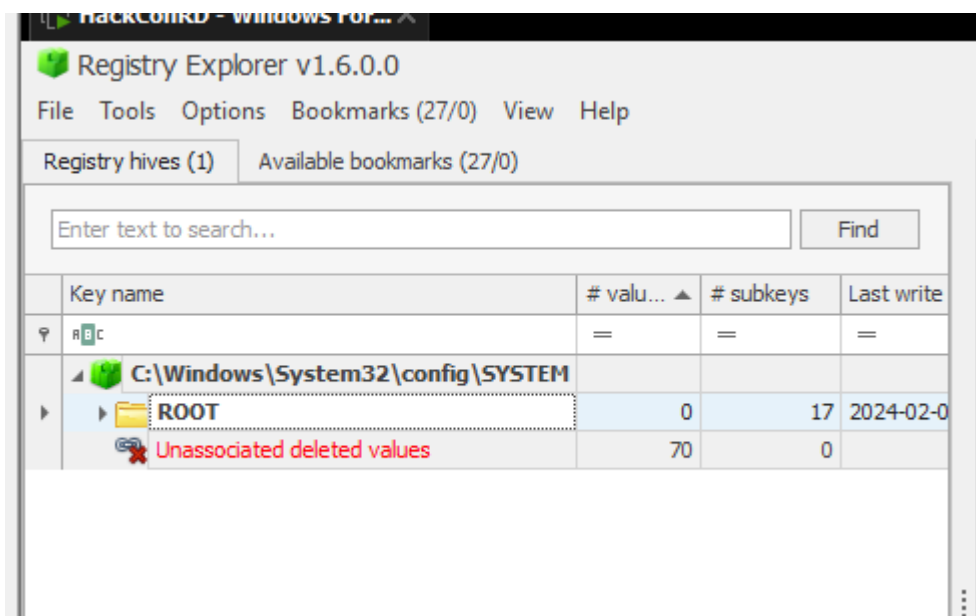
Nota: Si en dado caso un dirty hive es detectado, le damos a “yes”



Click en “OK” para seleccionar transaction logs to replay, y en la misma ruta de SYSTEM, encontraremos SYSTEM.log1 y SYSTEM.log2, seleccionamos ambos y lo abrimos

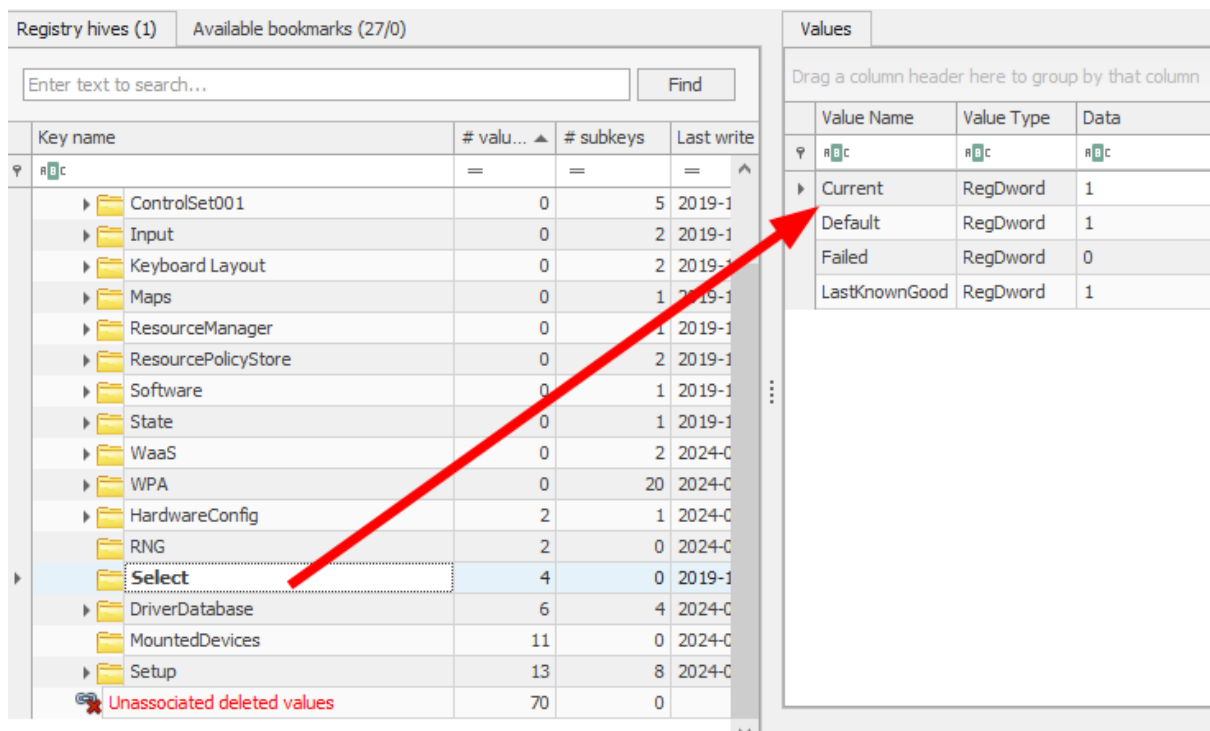
Name	Date modified	Type
DEFAULT.LOG1	12/7/2019 9:03 AM	LOG1 File
DEFAULT.LOG2	12/7/2019 9:03 AM	LOG2 File
SAM.LOG1	12/7/2019 9:03 AM	LOG1 File
SAM.LOG2	12/7/2019 9:03 AM	LOG2 File
SECURITY.LOG2	12/7/2019 9:03 AM	LOG2 File
SOFTWARE.LOG1	12/7/2019 9:03 AM	LOG1 File
SOFTWARE.LOG2	12/7/2019 9:03 AM	LOG2 File
SYSTEM.LOG1	12/7/2019 9:03 AM	LOG1 File
SYSTEM.LOG2	12/7/2019 9:03 AM	LOG2 File

Le damos OK y lo guardamos en el Desktop o en el disco CASES/Exercises/Registry. Registry Explorer nos pedirá si queremos actualizar el nuevo hive y le damos “OK”.



¿Cuál es el CurrentControlSet? Key: **SYSTEM\Select**





- El valor actual es igual a 1, lo que indica que el CurrentControlSet del sistema es ControlSet001.

- Este sistema solo tiene un ControlSet (que parece ser el predeterminado en Windows 10), pero es posible que encuentres sistemas que mantengan múltiples ControlSets "de respaldo" en el futuro. El CurrentControlSet debería contener la configuración más actualizada para el sistema.

Documenta el Nombre de la Computadora del sistema.

Key:

**SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName** [Hint: Recuerda usar el ControlSet que identificamos anteriormente]

**El nombre de la computadora es SRL-FORGE.** Es importante documentarlo, ya que puede servir como una verificación para asegurarse de que estás observando el sistema correcto. También puede ser referenciado en otros artefactos como registros de eventos y elementos de la interfaz de línea de comandos.

Enter text to search...				Find	
Key name	# values	# subkeys	Last		
AppID	0	2	2		
Arbiters	0	3	2		
Audio	0	1	2		
BackupRestore	0	3	2		
Bluetooth	0	1	2		
CI	0	4	2		
Class	0	123	2		
CloudDomainJoin	0	0	2		
CoDeviceInstallers	0	0	2		
CommonGlobUserSettings	0	1	2		
Compatibility	0	1	2		
ComputerName	0	1	2		
<b>ComputerName</b>	2	0	2		
ContentIndex	0	1	2		
Cryptography	0	6	2		
DeviceClasses	0	153	2		
DeviceContainerPropertyUpdateEv...	0	1	2		
DeviceContainers	0	45	2		

Drag a column header here to group by that column		
Value Name	Value Type	Data
(default)	RegSz	mnmsrvc
ComputerName	RegSz	SRL-FORGE

¿A qué zona horaria fue configurado por última vez el sistema? Key: **SYSTEM\CurrentControlSet\Control\TimeZoneInformation**

Enter text to search...				Find	
Key name	# values	# subkeys	Last		
FVEStats	3	0	2		
GraphicsDrivers	3	10	2		
IPMI	4	0	2		
ProductOptions	6	0	2		
Remote Assistance	6	0	2		
CrashControl	10	3	2		
<b>TimeZoneInformation</b>	10	0	2		
Print	11	5	2		
Windows	11	0	2		
HAL	16	0	2		
Power	16	8	2		
Terminal Server	16	13	2		
Lsa	20	19	2		
Session Manager	22	16	2		

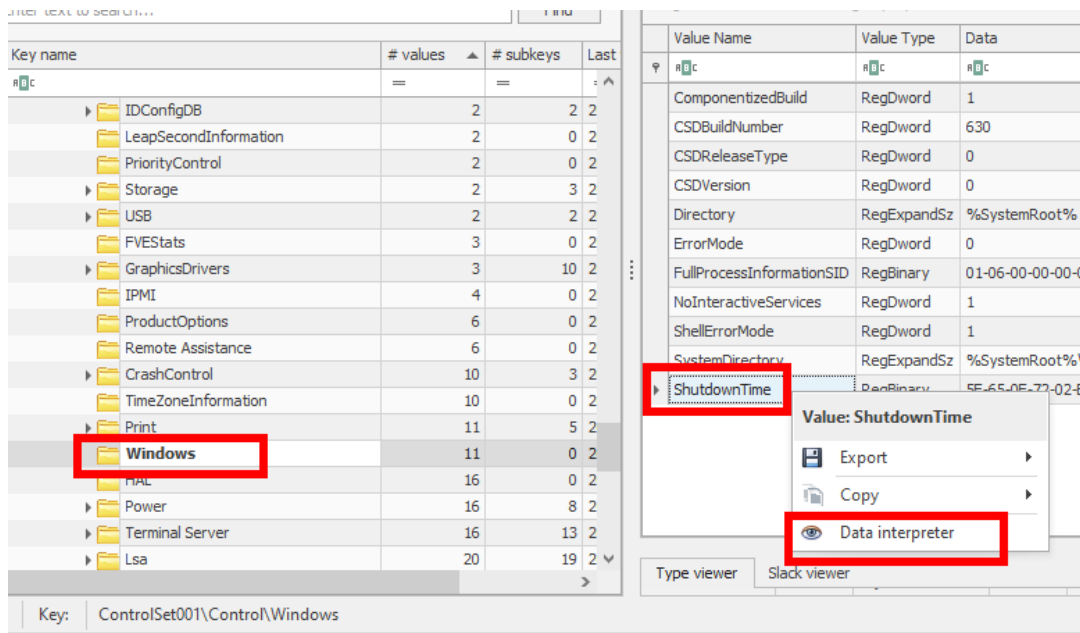
Drag a column header here to group by that column	
Value Name	Value Data
Bias	300
DaylightBias	-60
DaylightName	@tzres.dll,-111
DaylightStart	Month 3, week of month 2, day of week Hours:Minutes:Seconds:Milliseconds 2:0:
StandardBias	0
StandardName	@tzres.dll,-112
StandardStart	Month 11, week of month 1, day of week Hours:Minutes:Seconds:Milliseconds 2:0:
TimeZoneKeyName	Eastern Standard Time
ActiveTimeBias	300

El sistema fue configurado por última vez en la **Zona Horaria Estándar del Este (Eastern Standard Time)**. Mientras que la mayoría de los artefactos en Windows se almacenan en UTC, algunos se almacenan en la hora local, lo que significa que tendrás que convertirlos desde la zona horaria local del sistema a UTC para mantener la consistencia.

**¿Cuándo se apagó o reinició el sistema por última vez? Key: SYSTEM\CurrentControlSet\Control\Windows .**

**Nota:** Haz clic derecho en los valores de datos como raw timestamps para convertirlos en formatos legibles para humanos utilizando la función de Data Interpreter

- El valor ShutdownTime nos indica la última vez que el sistema inició un apagado (incluido un reinicio). La marca de tiempo se almacena en el formato muy común de Windows FILETIME de 64 bits. El Intérprete de Datos intenta analizar los datos de muchas maneras diferentes, pero generalmente es muy evidente qué conversiones son relevantes incluso si no conoces el formato de los datos.
- El último apagado ocurrió el 11 de noviembre de 2020 a las 08:12:49 UTC.

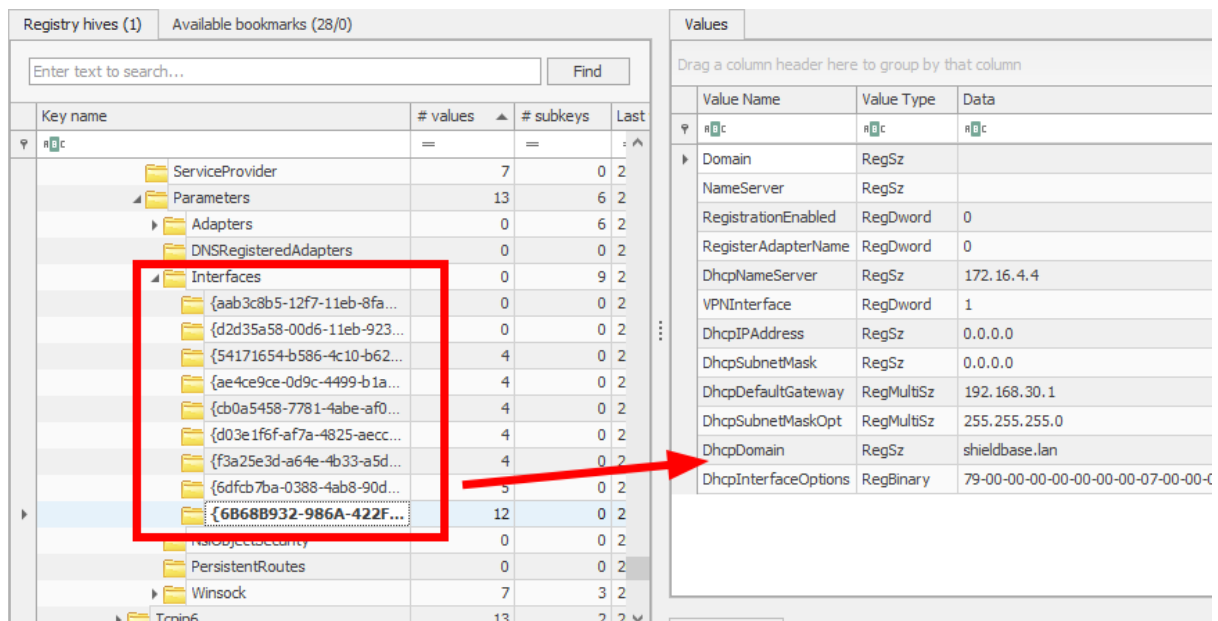


Data Interpreter	
Numbers	
8 bit, signed	94
8 bit, unsigned	94
16 bit, signed	25,950
16 bit, unsigned	25,950
32 bit, signed	1,913,546,078
32 bit, unsigned	1,913,546,078
64 bit, signed	132,495,559,696,999,774
64 bit, unsigned	132,495,559,696,999,774
Float	2.820443E+30
Double	8.48104706336161E-300
Dates and times	
DOS FAT Time/date (32 bit)	n/a
DOS FAT Date/time (32 bit)	2030-10-30 14:16:28
Unix/Posix (32 bit)	2030-08-21 12:34:38
Windows FILETIME (64 bit)	2020-11-11 08:12:49
OLE 2.0 Date/time (64 bit)	1899-12-30 00:00:00
Windows SYSTEM Date/time (128 bit)	n/a

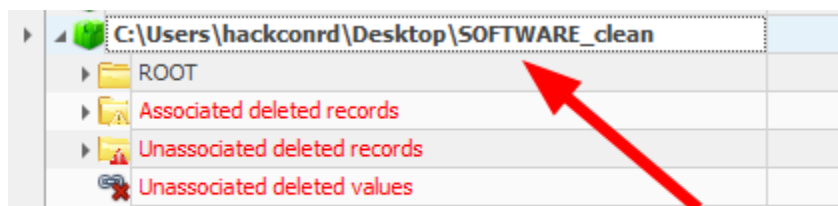
Revisa la clave de Interfaces de red para perfilar las conexiones de red más recientes. Key:

**SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces** . Observaremos que solo hay una interfaz que mantiene información interesante. Documenta el DhcpDomain para esa interfaz de red:

- Este sistema tiene muy poca actividad de red, lo cual se debe a que fue asignado al Sr. Rocba por su empleador solo unas pocas semanas antes de la investigación.
- El valor de DhcpDomain es shieldbase.lan, que es la red interna de Laboratorios de Investigación Stark. Investigaremos esto más a fondo en la siguiente sección.



Ahora examinaremos el offline hive SOFTWARE, lo cargamos al Registry Explorer (Si da problemas con Dirty Hive, realizamos los pasos anteriores)



Comienza nuestra investigación del registro SOFTWARE documentando información adicional del sistema. Ve a **SOFTWARE\Microsoft\Windows NT\CurrentVersion** y responde las siguientes preguntas.

¿Qué versión de Windows se está utilizando?

¿Cuál es el ReleaseID y CurrentBuild del sistema operativo?

¿Cuál es el valor InstallDate en formato de tiempo legible para humanos?

¿Quién es el RegisteredOwner?

name	# values	value name	value type	Data	value...	is D...	Data P
TableTextService		BuildLab	RegSz	19041.vb_release.191206-14...	00-00	<input type="checkbox"/>	
TaskFlowDataEngine		BuildLabEx	RegSz	19041.1.amd64fre.vb_releas...	00-...	<input type="checkbox"/>	
Tcpip		CompositionEditionID	RegSz	Enterprise	00-...	<input type="checkbox"/>	
TelemetryClient		CurrentBuild	RegSz	19042		<input type="checkbox"/>	
Terminal Server Client		CurrentBuildNumber	RegSz	19042		<input type="checkbox"/>	
TermServLicensing		CurrentMajorVersionNumber	RegDword	10		<input type="checkbox"/>	
TPG		CurrentMinorVersionNumber	RegDword	0		<input type="checkbox"/>	
Tpm		CurrentType	RegSz	Multiprocessor Free	65-...	<input type="checkbox"/>	
Transaction Server		CurrentVersion	RegSz	6.3	00-...	<input type="checkbox"/>	
TV System Services		EditionID	RegSz	Professional	00-00	<input type="checkbox"/>	
UEV		EditionSubManufacturer	RegSz			<input type="checkbox"/>	
Unified Store		EditionSubstring	RegSz			<input type="checkbox"/>	
Unistore		EditionSubVersion	RegSz			<input type="checkbox"/>	
UNP		InstallationType	RegSz	Client	00-...	<input type="checkbox"/>	
UPnP Device Host		InstallDate	RegDword	1604269285		<input type="checkbox"/>	
UserData		ProductName	RegSz	Windows 10 Pro	72-...	<input type="checkbox"/>	
UserManager		ReleaseId	RegSz	2009	00-00	<input type="checkbox"/>	
Virtual Machine		SoftwareType	RegSz	System	00-...	<input type="checkbox"/>	
VisualStudio		UBR	RegDword	630		<input type="checkbox"/>	
WAB		PathName	RegSz	C:\Windows	00-...	<input type="checkbox"/>	
Wallet		ProductId	RegSz	00330-62854-36078-AAOEM	60-...	<input type="checkbox"/>	
WIMMount		DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-...		<input type="checkbox"/>	
Windows		DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-...	E8-...	<input type="checkbox"/>	
Windows Defender Security Center		InstallTime	RegQword	132487428857608365	00-...	<input type="checkbox"/>	
Windows Embedded		DisplayVersion	RegSz	20H2	2A-04	<input type="checkbox"/>	
Windows Media Foundation		PendingInstall	RegDword	0		<input type="checkbox"/>	
Windows Media Player NSS		RegisteredOwner	RegSz	srl-helpdesk@outlook.com	00-00	<input type="checkbox"/>	
Windows NT							
CurrentVersion	3						
Windows Performance Toolkit							
Windows Phone							

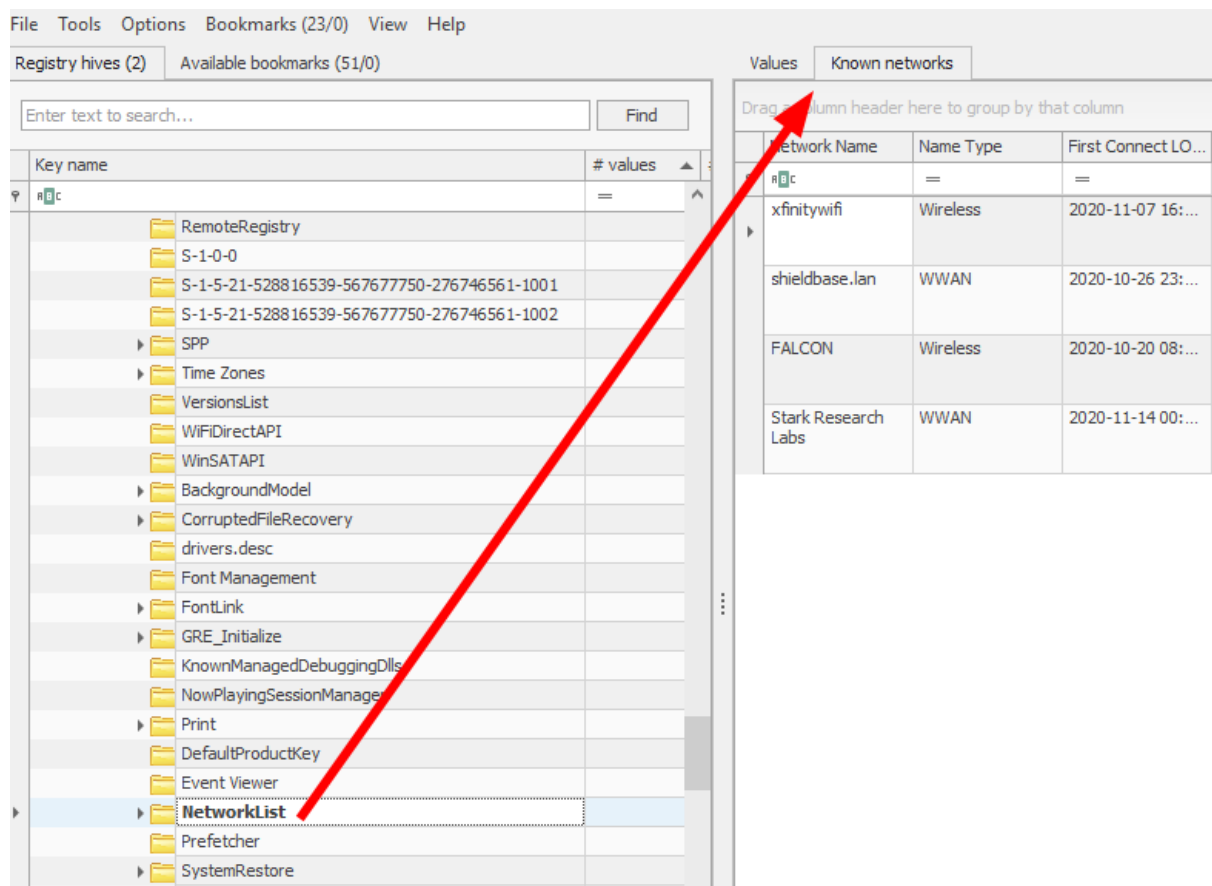
- Windows 10 Pro
- Número de compilación 19042 (**2009**)
- Fecha de instalación: 2020-11-01 22:21:25
- El RegisteredOwner es srl-helpdesk@outlook.com.
- Ten cuidado con tu interpretación de "InstallDate". Este valor podría ser la hora en que se instaló por primera vez el sistema operativo, pero más comúnmente representa la última actualización importante del sistema. A partir de Windows 10, Microsoft comenzó a lanzar actualizaciones importantes de versión con frecuencia, por lo que este tiempo generalmente representa la última actualización. En este caso, el sistema se actualizó a la versión "2009" el 2020-11-01 a las 22:21:25. Esta información será muy útil ya que notarás que muchos de los registros de tiempo están establecidos en torno a esta hora, lo que indica que la actualización, y no la actividad del usuario, fue responsable.



...	EditionSubstring	RegSz			<input type="checkbox"/>
...	EditionSubVersion	RegSz			<input type="checkbox"/>
...	InstallationType	RegSz	Client	00-...	<input type="checkbox"/>
▶	InstallDate	RegDword	1604269285		<input type="checkbox"/>
	ProductName	RegSz	Windows 10 Pro	72-...	<input type="checkbox"/>
	ReleaseId	RegSz		00-00	<input type="checkbox"/>
	SoftwareType	RegSz		00-...	<input type="checkbox"/>
	UBR	RegSz			<input type="checkbox"/>
	PathName	RegSz	Windows	00-...	<input type="checkbox"/>
	ProductId	RegSz	00330-62854-36078-AAOEM	60-...	<input type="checkbox"/>
	DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-...		<input type="checkbox"/>

Data Interpreter	
<b>Numbers</b>	
8 bit, signed	-27
8 bit, unsigned	229
16 bit, signed	13,541
16 bit, unsigned	13,541
32 bit, signed	1,604,269,285
32 bit, unsigned	1,604,269,285
64 bit, signed	n/a
64 bit, unsigned	n/a
Float	2.294409E+19
Double	n/a
<b>Dates and times</b>	
DOS FAT Time/date (32 bit)	2027-12-31 06:39:10
DOS FAT Date/time (32 bit)	n/a
Unix/Posix (32 bit)	2020-11-01 22:21:25
Windows FILETIME (64 bit)	n/a
OLE 2.0 Date/time (64 bit)	n/a
Windows SYSTEM Date/time (128 bit)	n/a
<b>Other</b>	

Vamos a movernos a la clave NetworkList presente dentro del hive SOFTWARE. Esta clave proporciona una vista más histórica de las conexiones de red que la que se puede encontrar en el hive SYSTEM. Registry Explorer contiene un complemento para analizar múltiples subclaves de NetworkList y llevar los datos a una tabla. Ve a la clave **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList** y asegúrate de estar mirando la pestaña del complemento de redes conocidas (**Known networks plugin tab**).



¿Qué redes inalámbricas se han registrado?

- xfinitywifi
- FALCON

Network Name	Name Type	First Connect LOCAL	Last Connected LOCAL
xfinitywifi	Wireless	2020-11-07 16:32:02	2020-11-07 16:32:02
shieldbase.lan	WWAN	2020-10-26 23:28:57	2020-11-14 00:00:17
FALCON	Wireless	2020-10-20 08:01:35	2020-11-12 01:06:10
Stark Research Labs	WWAN	2020-11-14 00:00:17	2020-11-14 00:00:17

¿Cuales WWAN (VPN) fueron registradas?

**shieldbase.lan**

## Stark Research Labs

	Network Name	Name Type	First Connect LOCAL	Last Connected LOCAL
▼	RB	=	=	=
	xfinitywifi	Wireless	2020-11-07 16:32:02	2020-11-07 16:32:02
	shieldbase.lan	WWAN	2020-10-26 23:28:57	2020-11-14 00:00:17
	FALCON	Wireless	2020-10-20 08:01:35	2020-11-12 01:06:10
	Stark Research Labs	WWAN	2020-11-14 00:00:17	2020-11-14 00:00:17

Verifiquemos las marcas de tiempo de las conexiones VPN en nuestros apuntes. Teniendo en cuenta que el Sr. Rocba estaba de vacaciones y físicamente alejado de su computadora portátil desde el 2020-11-10 hasta el 2020-11-15, ¿ves cómo uno de estos momentos podría ser interesante?

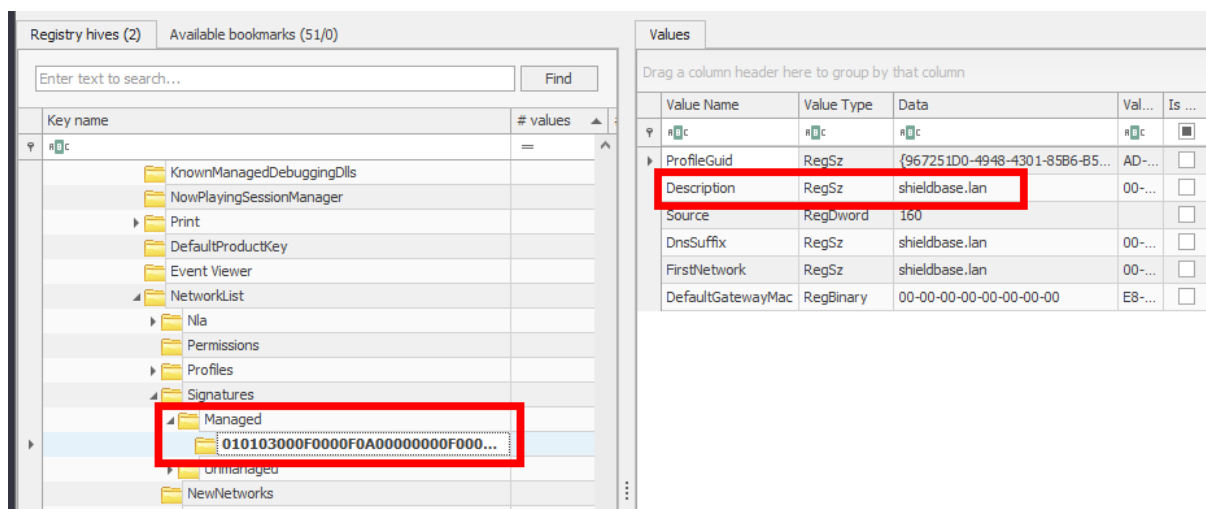
Se registraron conexiones VPN en las siguientes marcas de tiempo:

- **2020-10-26 23:28:57**

- **2020-11-14 00:00:17**

La conexión del 14 de noviembre de 2020 ocurrió durante el período de vacaciones del Sr. Rocba y durante el momento del allanamiento en la residencia de Rocba. Esto podría ser de interés ya que sugiere que alguien podría haber accedido al sistema o a la red desde una ubicación remota durante el incidente del allanamiento.

¿Cuál de las redes identificadas fue almacenada como una red "administrada" (managed)? Las redes administradas suelen ser parte de un dominio de Windows, como una red corporativa. La clave **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures** puede ayudar a hacer esta determinación.



shieldbase.lan es el único perfil de red presente bajo la subclave Managed. Si deseas investigar más a fondo esta red manualmente, debemos registrar el valor ProfileGuid y compararlo con una subclave bajo **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles**, donde puedes encontrar los valores DateCreated, NameType y DateLastConnected. (la salida del complemento de Redes Conocidas que examinaste previamente hace todo este trabajo duro por ti).

### Hasta ahora tenemos:

- Perfil del sistema:
  - **Nombre del sistema:** SRL-FORGE
  - **Sistema operativo:** Windows 10 Pro Build 2009
  - **Hora de instalación/última actualización importante:** 2020-11-01 22:21:25
  - **Zona horaria:** Hora Estándar del Este / : Eastern Standard Time
  - **Último apagado/reinicio:** 2020-11-11 08:12:49 UTC
- La red doméstica probable del usuario se llamaba FALCON.
- Se registró actividad de VPN en el registro. La última conexión de red realizada en el sistema fue a la VPN de Stark Research Labs el 2020-11-14 a las 00:00:17.
- Este es un hallazgo interesante porque el Sr. Rocba estaba de vacaciones y físicamente alejado de su computadora portátil desde el 2020-11-10 hasta el 2020-11-15.