sedian

Seguridad Digital
de Andalucía

Charla virtual de sensibilización

Monitorización de eventos en Windows (Sysmon)

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

Contenidos

Qué vamos a tratar

Contenidos

1. ¿Qué es Sysmon? Funcionalidades
2. Instalación de System Monitor
3. Configuración
    a. Tipos de eventos
    b. Ficheros de configuración
4. Analizando la información
    a. Filtrando las entradas
    b. Extrayendo logs con powershell
5. Ejemplos de uso
    a. Obtener conexiones de procesos
    b. Obtener modificaciones claves del registro
    c. Obtener procesos que se han creado

Objetivos

- Aprender a monitorizar procesos en el sistema.
- Detectar posibles amenazas.
- Investigar posibles fallos en el sistema debido a un ataque o un mal funcionamiento del sistema.

¿Qué es y para qué sirve?

System Monitor (Sysmon) es un servicio que una vez instalado permanece activo siempre para supervisar y registrar la actividad del sistema en el registro de sucesos de Windows. Proporciona información detallada sobre creaciones de procesos, conexiones de red y cambios en el tiempo de creación de archivos...

Para monitorizar el equipo de cara a una investigación posterior:

- Procesos de que se crean
- Conexiones de red
- Cambios en el registro
- Comandos que se ejecutan

Instalación

- Junto a la suite de sysinternals
- Por separado en la web de Microsoft
- Con el gestor de paquetes Chocolate

Instalación
¿Dónde lo podemos obtener?

Se puede descargar la suite de Sysinternals desde:

- https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

También se puede descargar por separado desde:

- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

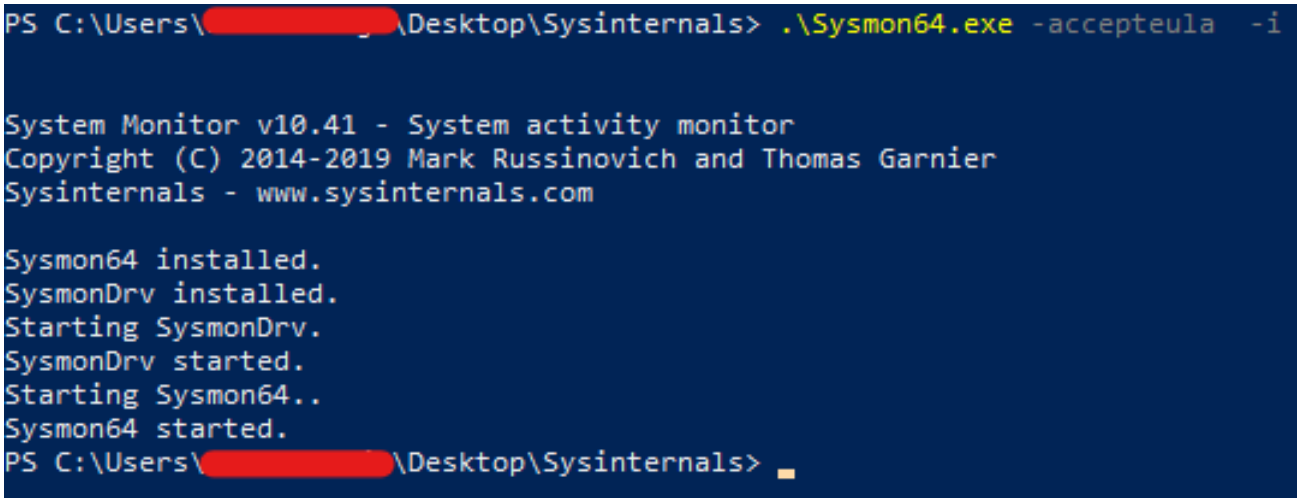
Además, se puede instalar mediante chocolatey:

- https://chocolatey.org/packages/sysmon

Para instalarlo ejecutar el fichero Sysmon.exe o Sysmon64.exe según la arquitectura de nuestro Windows.

Importante **ejecutarlo en modo Administrador.**

symon.exe -accepteula -i



Para instalarlo desde chocolatey tenemos que tener este gestor de paquetes previamente instalado.

Importante **ejecutarlo en como Administrador.**

choco install sysmon

```
PS C:\Users\[redacted]\Desktop\Sysinternals> choco install sysmon -y --reinstall --ignore-checksums
Chocolatey v0.10.15
Installing the following packages:
sysmon
By installing you accept licenses for the packages.
Progress: Downloading sysmon 10.10... 100%

sysmon v10.10 [Approved] - Likely broken for FOSS users (due to download location changes)
sysmon package files install completed. Performing other installation steps.
File appears to be downloaded already. Verifying with package checksum to determine if it needs to be redownloaded.
WARNING: Ignoring checksums due to feature checksumFiles turned off or option --ignore-checksums set.
WARNING: Ignoring checksums due to feature checksumFiles turned off or option --ignore-checksums set.
Extracting C:\Users\Rafael Sojo\AppData\Local\Temp\chocolatey\sysmon\10.10\Sysmon.zip to C:\ProgramData\chocolatey\lib\sysmon\tools...
C:\ProgramData\chocolatey\lib\sysmon\tools
 ShimGen has successfully created a shim for Sysmon.exe
 ShimGen has successfully created a shim for Sysmon64.exe
 The install of sysmon was successful.
  Software installed to 'C:\ProgramData\chocolatey\lib\sysmon\tools'

Chocolatey installed 1/1 packages.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
PS C:\Users\[redacted]\Desktop\Sysinternals>
```

https://chocolatey.org/packages/sysmon

Configuración

Instalar con las opciones por defecto (imágenes de procesos hasheadas con sha1 y sin monitorización de la red)

- sysmon -accepteula -i

Para desinstalar

- sysmon –u

Para cambiar la configuración para utilizar todos los hashes, sin monitorizar la red y monitorizando las DLLs en Lsass

- sysmon -c -h * -l lsass.exe

Para cambiar la configuración de sysmon utilizando un fichero de configuración

- sysmon -c c:\windows\config.xml

Para cambiar la configuración de sysmon a las opciones por defecto

- sysmon -c –

Mostrar esquema de configuración actual (XML)

- sysmon –s

Para mostrar la configuración actual

- sysmon –c

Configuración sysmon
Ejemplos operadores

```
PS C:\Users\[redacted]Desktop\Sysinternals> .\Sysmon64.exe -h


System Monitor v10.41 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Usage:
Install:    C:\Users\[redacted]\Desktop\Sysinternals\Sysmon64.exe -i [<configfile>]
              [-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]
              [-l [<process,...>]
Configure:  C:\Users\[redacted]\Desktop\Sysinternals\Sysmon64.exe -c [<configfile>]
              [--|[-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]
              [-l [<process,...>]]]
Uninstall:  C:\Users\[redacted]Desktop\Sysinternals\Sysmon64.exe -u [force]
  -c   Update configuration of an installed Sysmon driver or dump the
       current configuration if no other argument is provided. Optionally
       take a configuration file.
  -d   Specify the name of the installed device driver image.
       Configuration entry: DriverName.
       The service image and service name will be the same
       name of the Sysmon.exe executable image.
  -h   Specify the hash algorithms used for image identification (default
       is SHA1). It supports multiple algorithms at the same time.
       Configuration entry: HashAlgorithms.
  -i   Install service and driver. Optionally take a configuration file.
  -l   Log loading of modules. Optionally take a list of processes to track.
  -m   Install the event manifest (done on service install as well).
  -n   Log network connections. Optionally take a list of processes to track.
  -r   Check for signature certificate revocation.
       Configuration entry: CheckRevocation.
  -s   Print configuration schema definition of the specified version.
       Specify 'all' to dump all schema versions (default is latest).
  -u   Uninstall service and driver. Adding force causes uninstall to proceed
       even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational". On older systems, events are written to the System event log.

If you need more information on configuration files, use the '-? config' command. More examples are available on the Sysinternals website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to accept it.

Neither install nor uninstall requires a reboot.

PS C:\Users\[redacted]Desktop\Sysinternals>
```

Para actualizar la configuración:

sysmon –c .\config.xml

....

```
<EventFiltering>
    <EventType onmatch="include/exclude">
        <Field condition="begin with">Foo</Field>
    </EventType>
</EventFiltering>
```

....

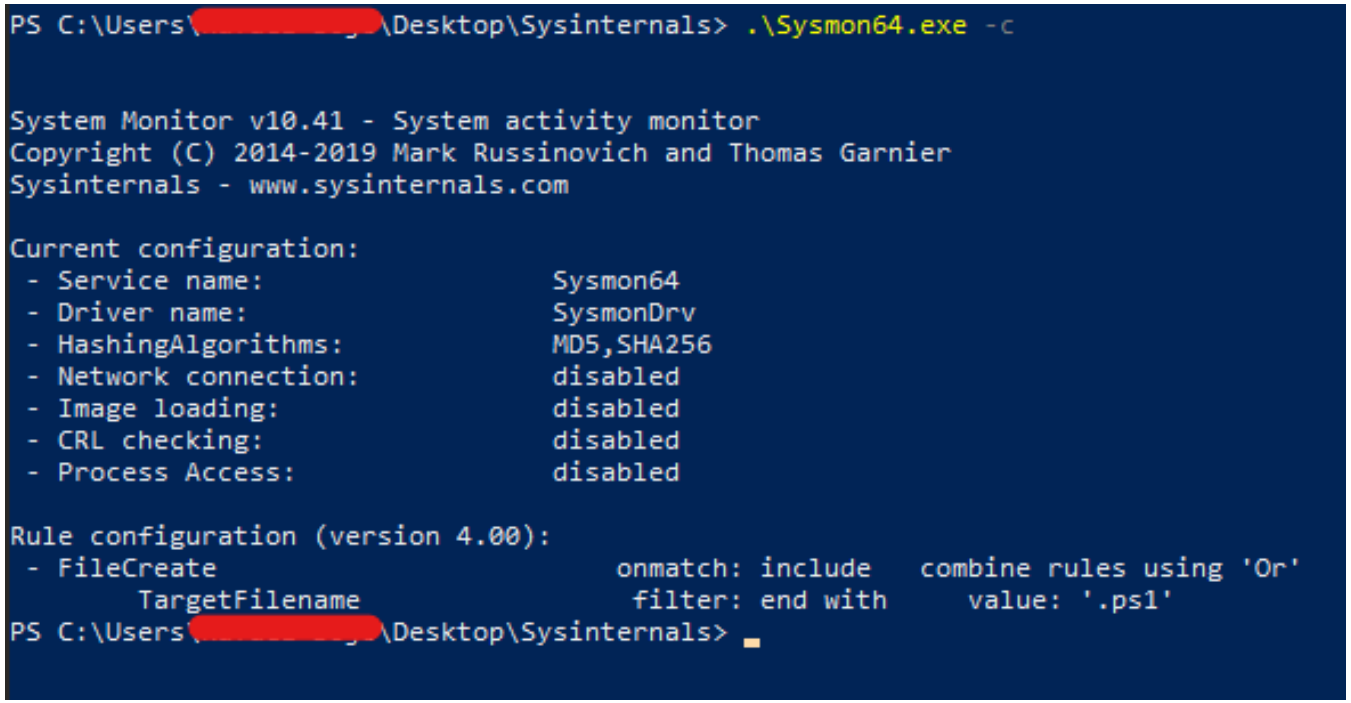
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon#configuration-files

Ejemplo de un fichero de configuración para monitorizar todos los ficheros creados que acaben por .ps1 (Ficheros de powershell)

```
<Sysmon schemaversion="4.00">
        <HashAlgorithms>md5,sha256</HashAlgorithms>
        <EventFiltering>
                <FileCreate onmatch="include">
                        <TargetFilename condition="end with">.ps1</TargetFilename>
                </FileCreate>
        </EventFiltering>
</Sysmon>
```

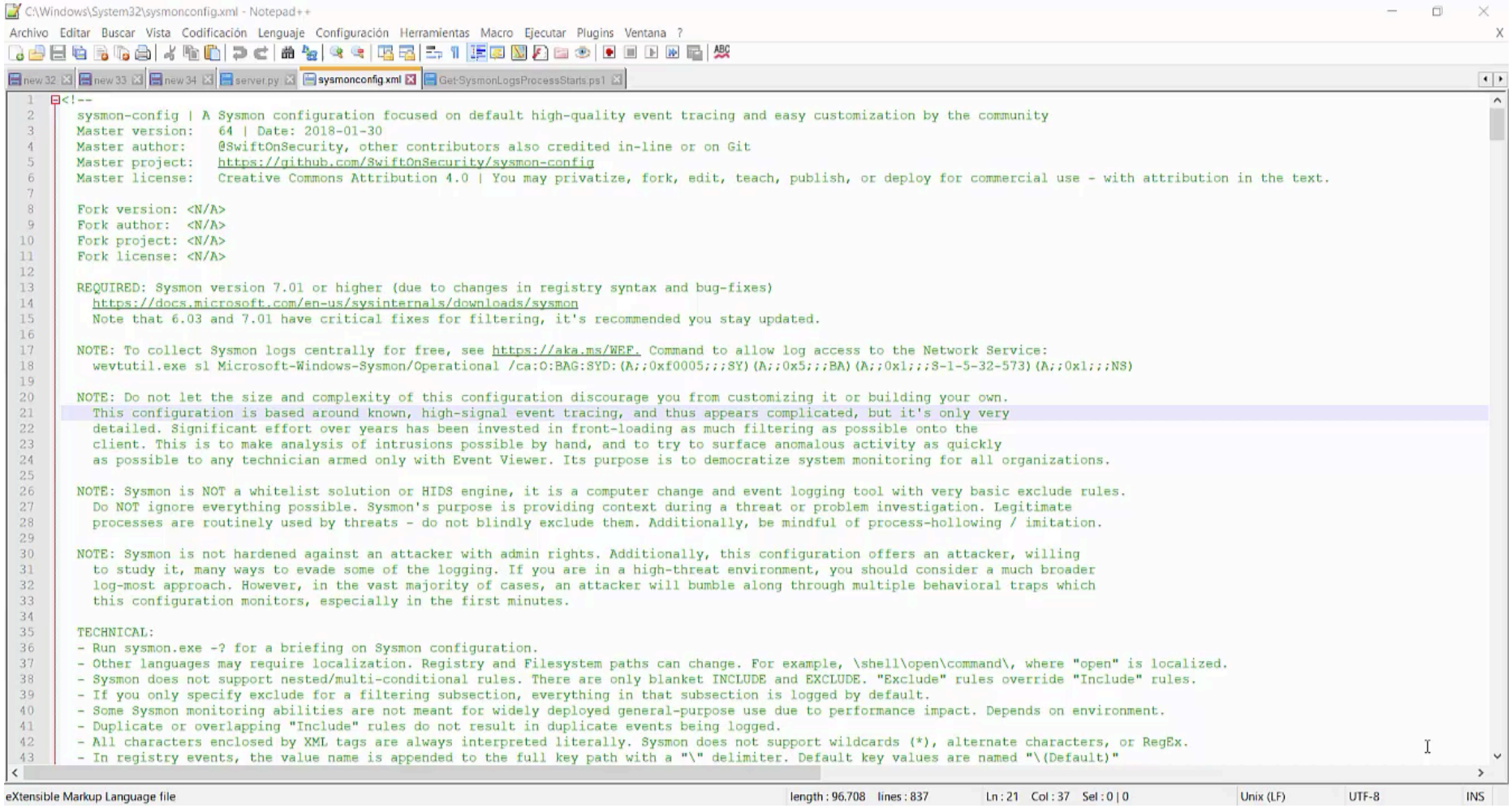
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon#configuration-files

Tras aplicar la configuración anterior debería aparecer algo como la siguiente imagen:



Fichero de configuración creado por la comunidad que usaremos de ejemplo:

https://github.com/SwiftOnSecurity/sysmon-config

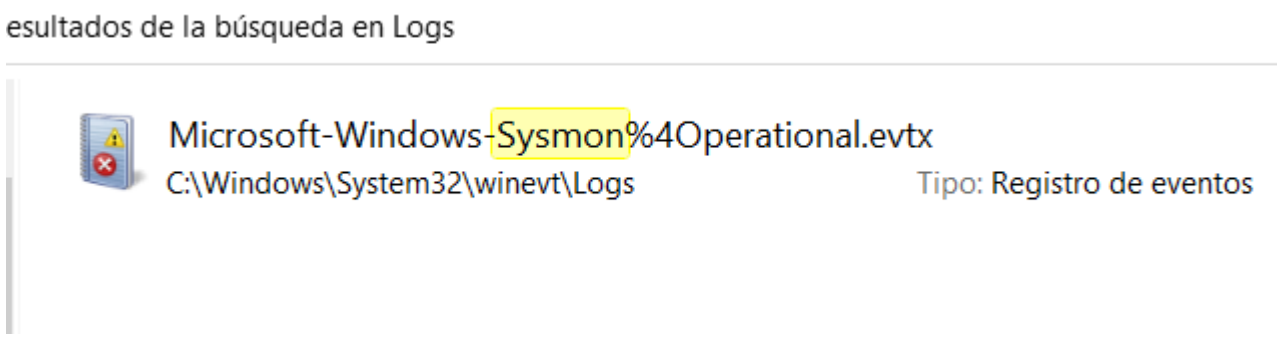


Configuración-Ejemplo

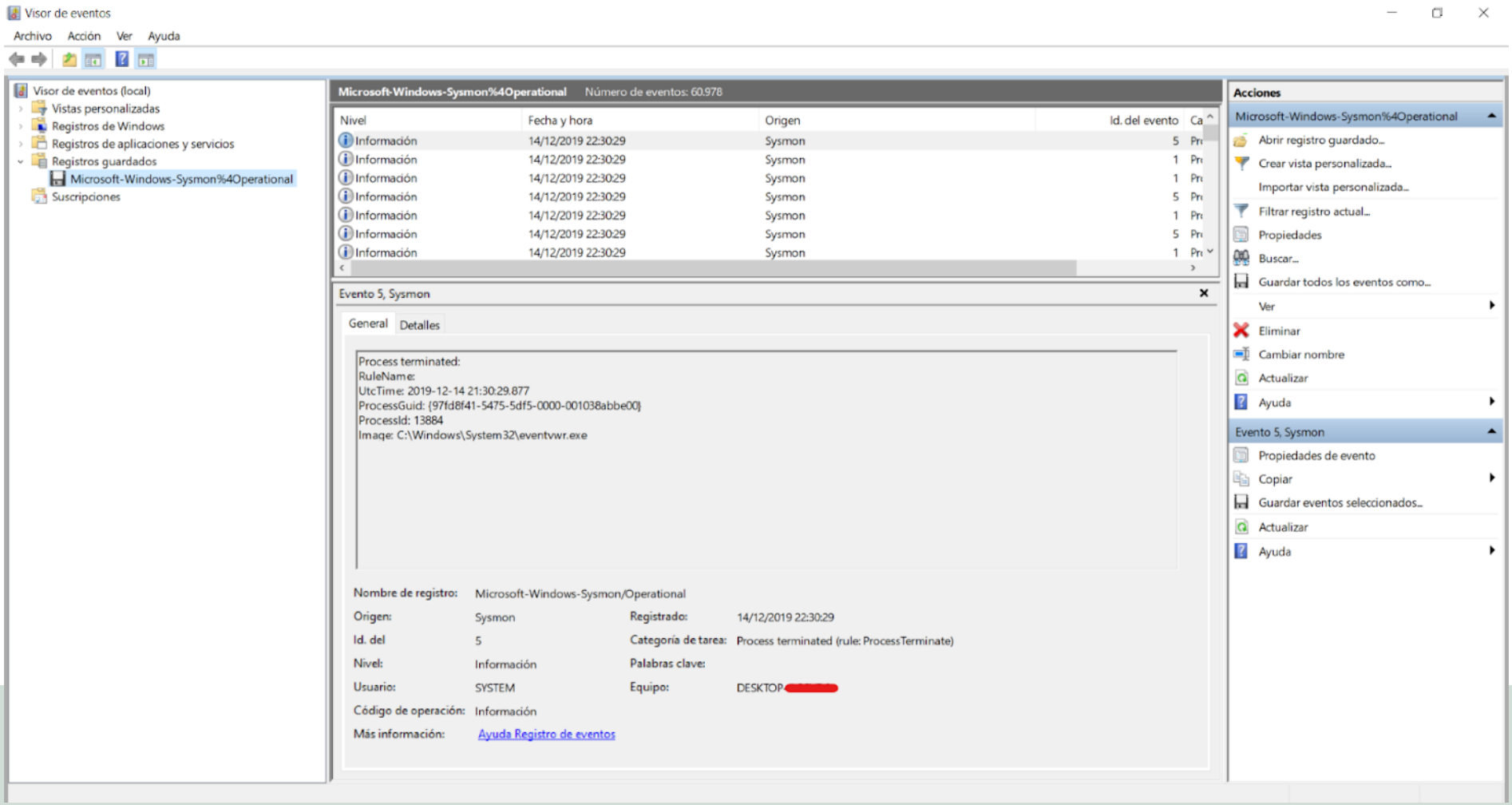
Análisis de la información

Por defecto los logs se guardan en la siguiente ruta:

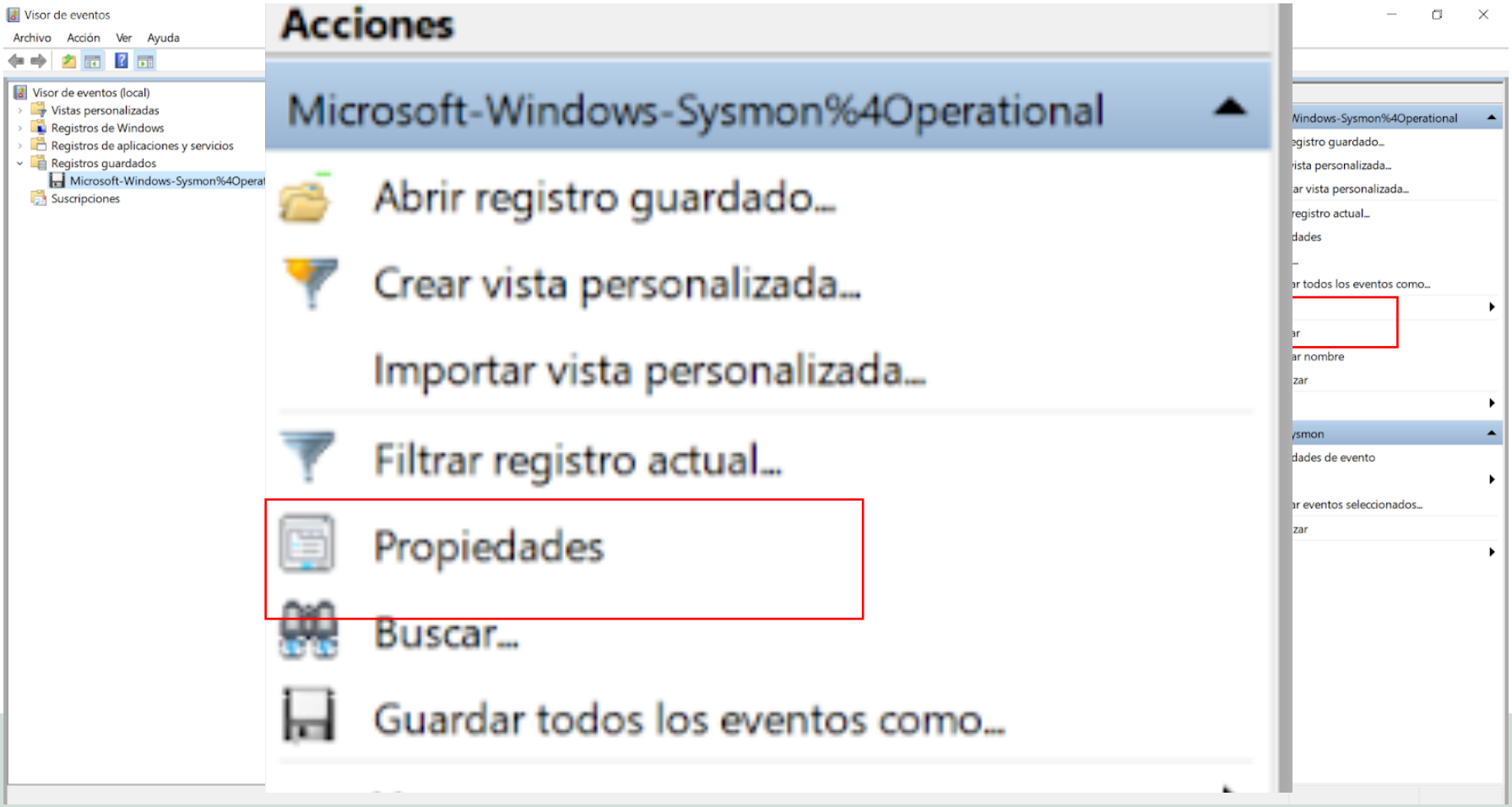
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx



Este es el aspecto del visor de eventos de Windows

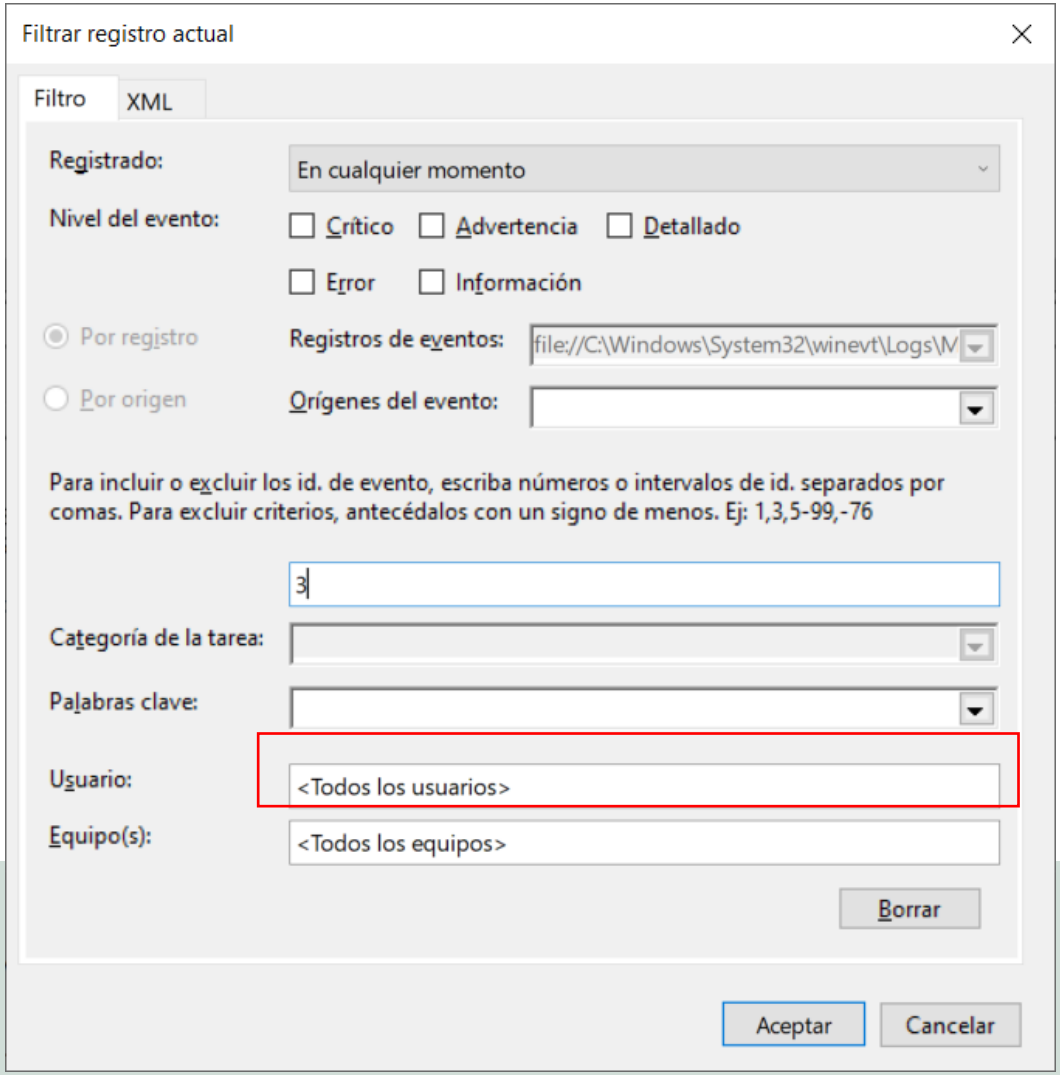


Para filtrar eventos tenemos que hacer clic en “Filtrar registro actual”

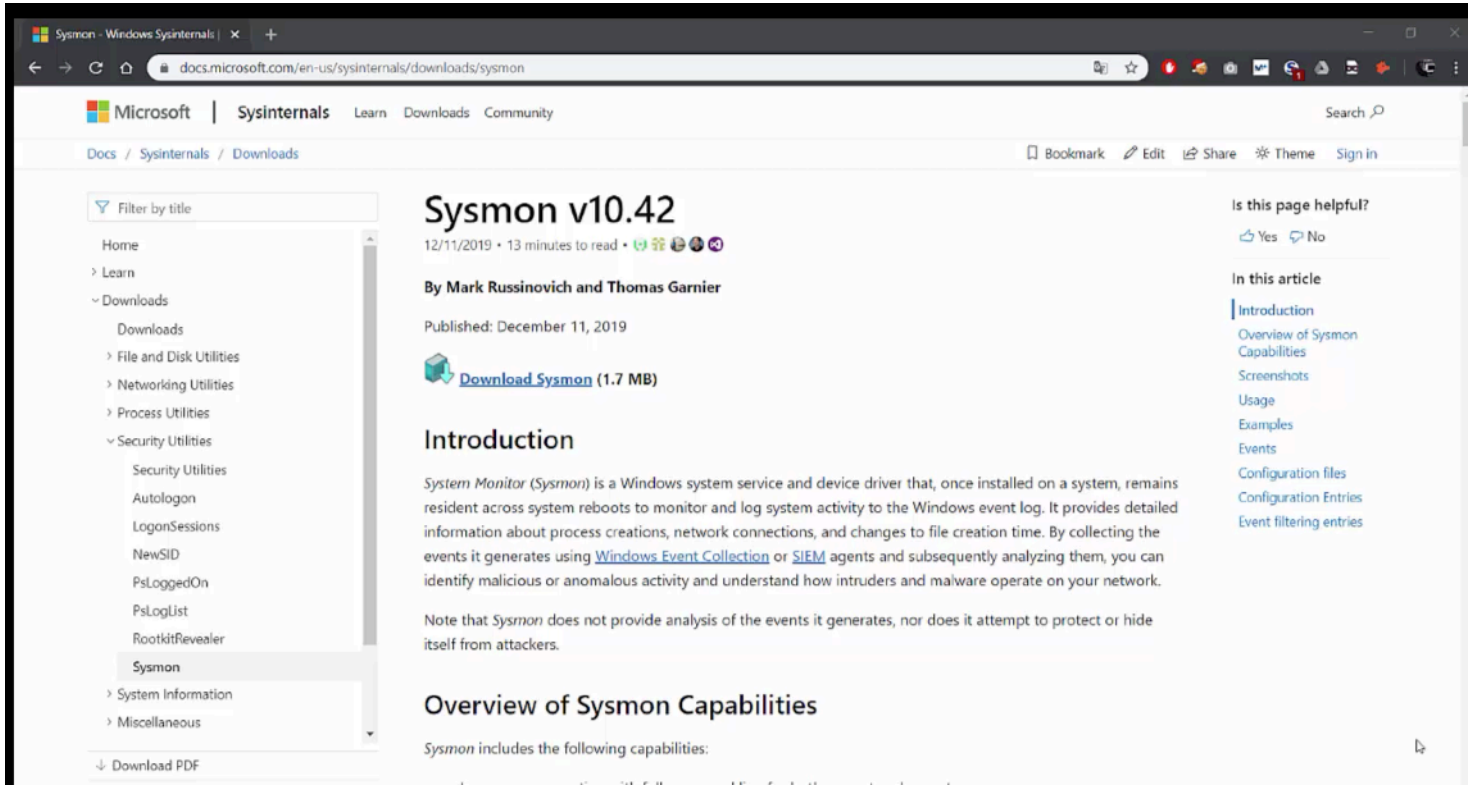


Filtrando eventos
Conexiones de red

En esta ventana, para filtrar por tipo de evento, pondremos los IDs de los eventos separados por comas



En la documentación oficial están todos los IDs de procesos. El proceso para filtrar para ver sólo los eventos de red sería el siguiente:



https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Para obtener todos los registros del log en powershell tenemos que ejecutar el siguiente comando:

Get-WinEvent -FilterHashtable @{ logname = "Microsoft-Windows-Sysmon/Operational"; }

Importante: **ejecutar como administrador**

Para obtener los registros del log, podemos usar el comando Get-WinEvent.

```
PS C:\WINDOWS\system32> $events = Get-WinEvent  -FilterHashtable @{ logname = "Microsoft-Windows-Sysmon/Operational"; }
```

```
PS C:\Users\[redacted]Desktop> $events


   ProviderName: Microsoft-Windows-Sysmon

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
15/12/2019 16:56:47              2 Información      File creation time changed:...
15/12/2019 16:56:39              2 Información      File creation time changed:...
15/12/2019 16:56:33              2 Información      File creation time changed:...
15/12/2019 16:56:29              2 Información      File creation time changed:...
15/12/2019 16:56:23              1 Información      Process Create:...
15/12/2019 16:56:16              5 Información      Process terminated:...
15/12/2019 16:56:16              5 Información      Process terminated:...
15/12/2019 16:56:12              2 Información      File creation time changed:...
15/12/2019 16:56:05              2 Información      File creation time changed:...
15/12/2019 16:55:00              2 Información      File creation time changed:...
15/12/2019 16:54:29              2 Información      File creation time changed:...
```


Obteniendo registro en powershell

Para mostrarlos de una forma más legible, podemos hacerlo con el siguiente comando:

Write-Host ($events[0] | Format-List | Out-String)

```
PS C:\Users[redacted]\Desktop> Write-Host ($events[0] | Format-List | Out-String)


TimeCreated  : 15/12/2019 16:56:47
ProviderName : Microsoft-Windows-Sysmon
Id           : 2
Message      : File creation time changed:
               RuleName:
               UtcTime: 2019-12-15 15:56:47.237
               ProcessGuid: {97fd8f41-0953-5df6-0000-00100b5c2200}
               ProcessId: 15372
               Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
               TargetFilename: C:\Users[redacted]\AppData\Local\Google\Chrome\User Data\448a0a2b-0cb7-45d9-984b-645235450aaf.tmp
               CreationUtcTime: 2019-01-29 13:41:53.024
               PreviousCreationUtcTime: 2019-12-15 15:56:47.222
```

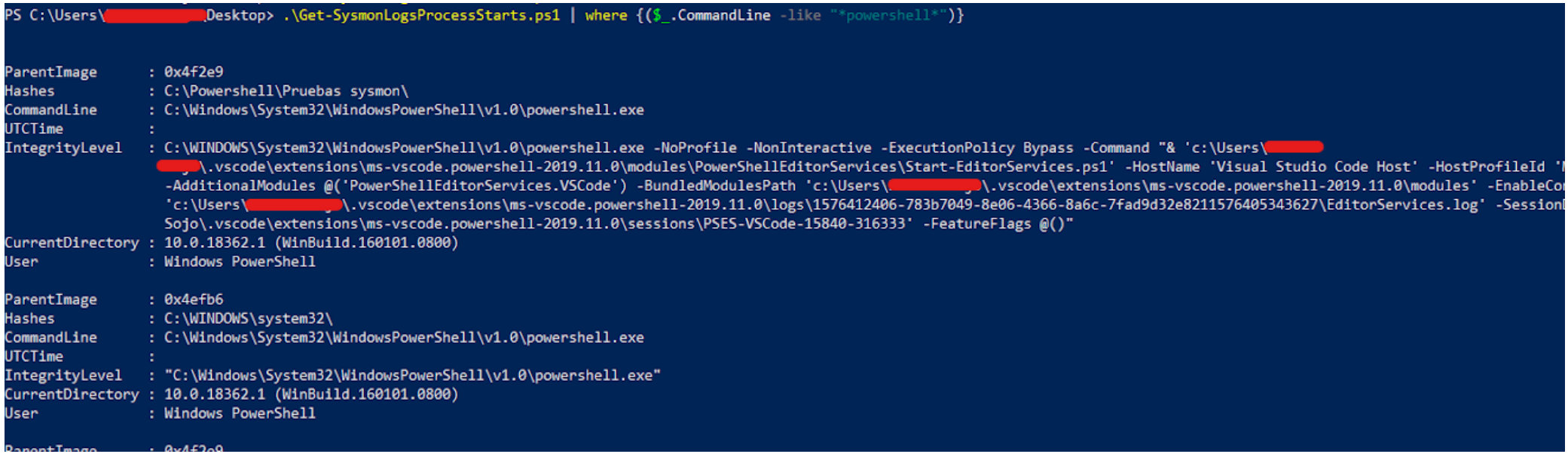
Función en powershell para poder buscar y filtrar más fácilmente:

https://github.com/mattiasborg82/PowerShell_Scripts/blob/master/Get-SysmonLogsProcessStarts.ps1

Esta función lo que hace es coger la salida del comando Get-WinEvent, la parsea y transforma en un objeto de powershell para poder aplicar filtros más fácilmente.

En este ejemplo se muestran todos los comandos en los que se ha ejecutado powershell.

.\Get-SysmonLogsProcessStarts.ps1 | where {($_.CommandLine -like "*powershell*")}



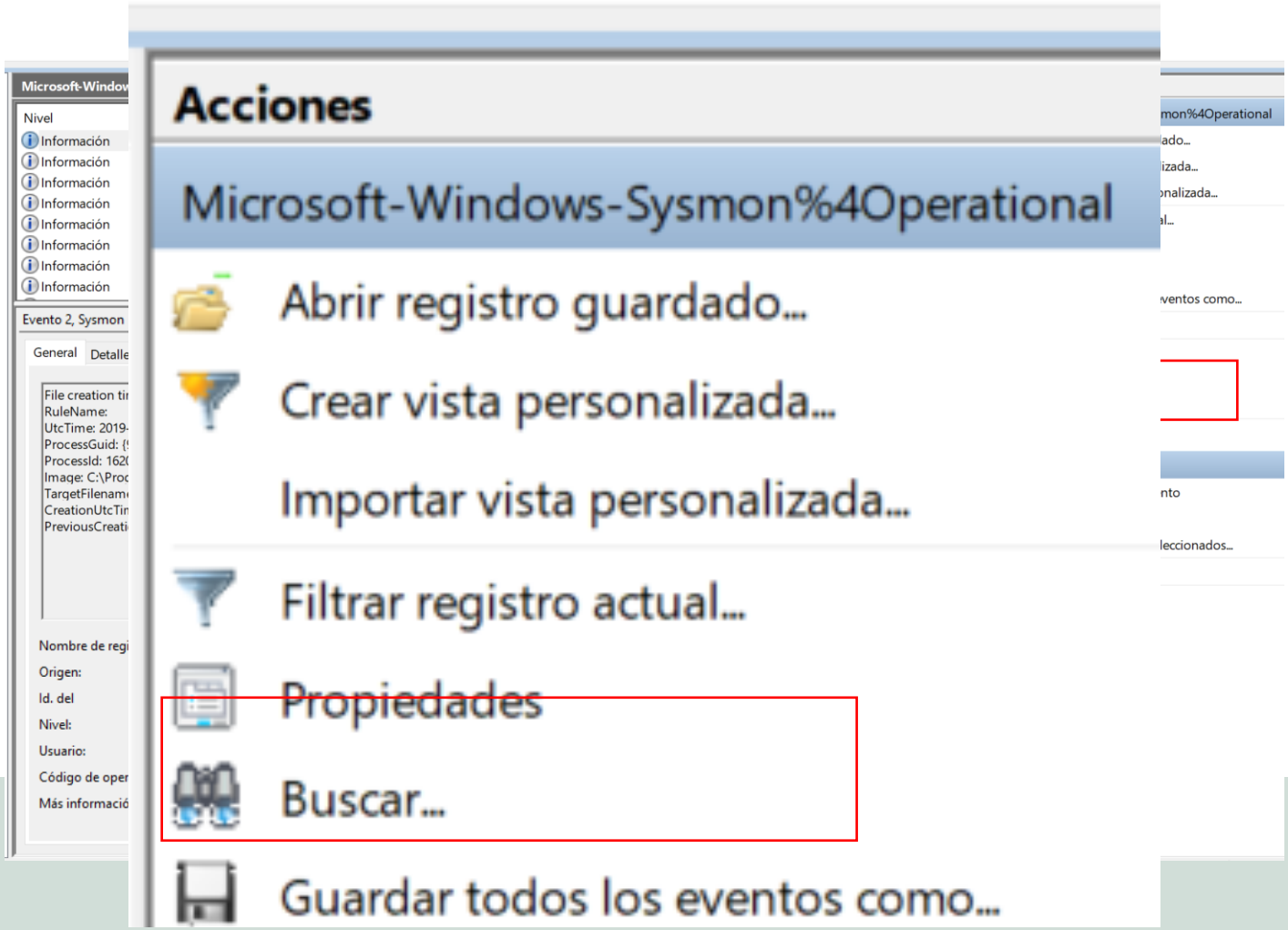
Ejemplos de uso

Para ver las modificaciones del registro las obtenemos si filtramos por eventos con ID 12, 13 y 14.

- El ID de evento 12 corresponde a cuando se añade o elimina un objeto del registro.
- El ID de evento 13 corresponde a cuando se modifica un valor del registro.
- El ID de evento 14 corresponde a cuando se renombra un objeto de registro.

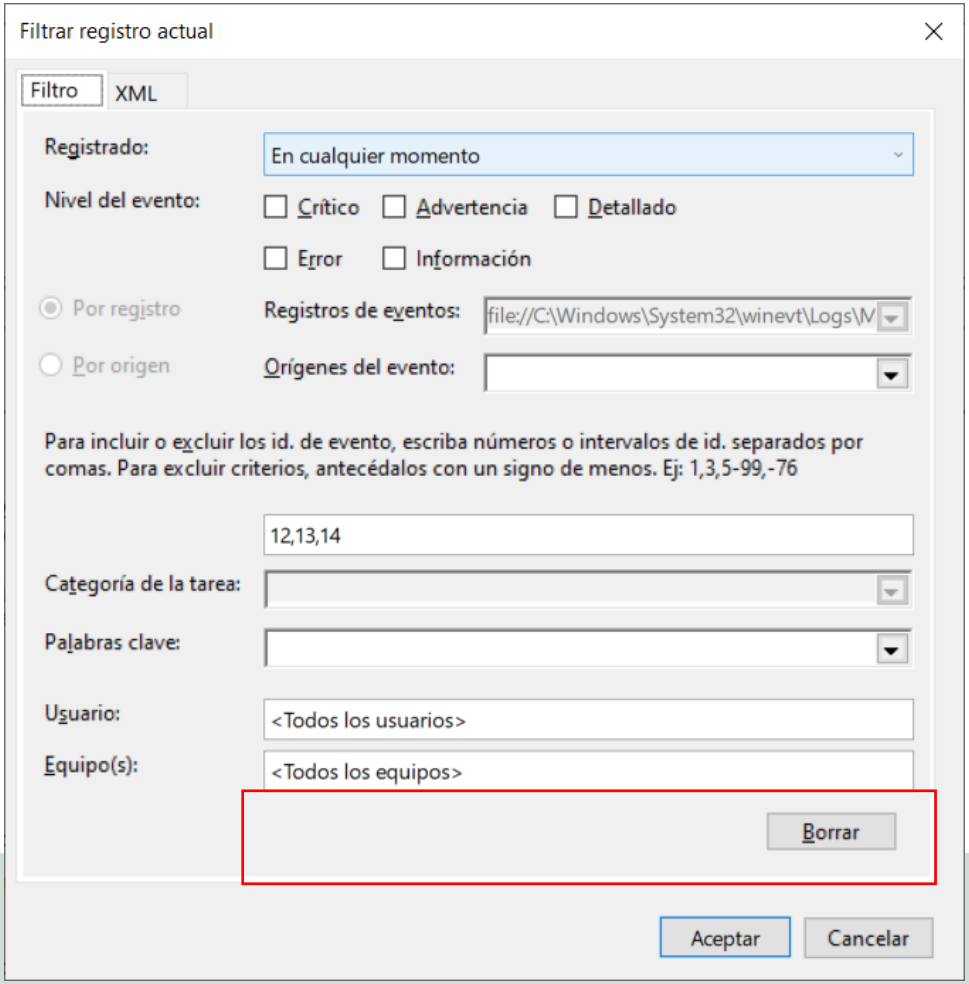
Ejemplo 1
Obteniendo modificaciones del registro

Para filtrar hay que hacer clic en “Filtrar registro actual…”



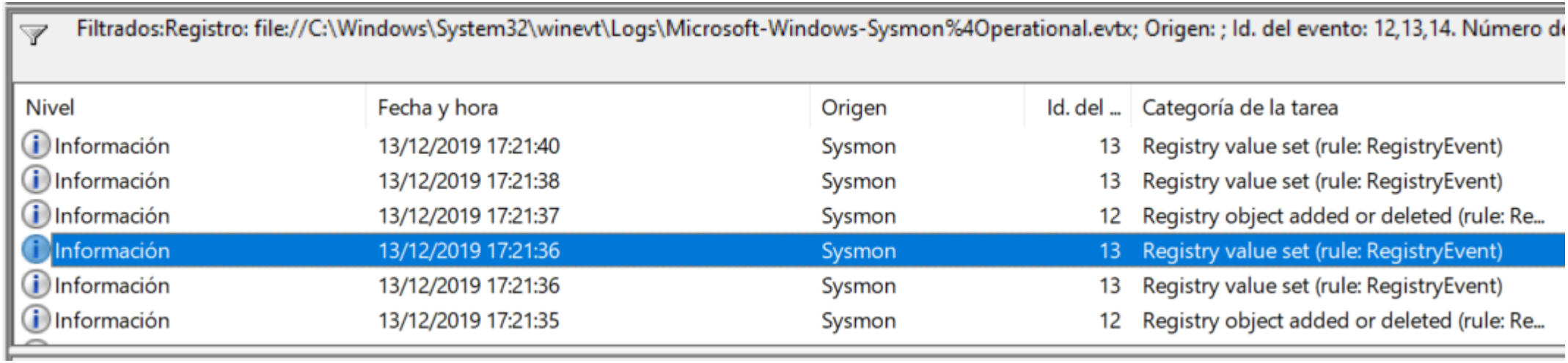
Ejemplo 1
Obteniendo modificaciones del registro

Para obtener las modificaciones del registro tenemos que filtrar por los eventos con **ID 12, 13 y 14**



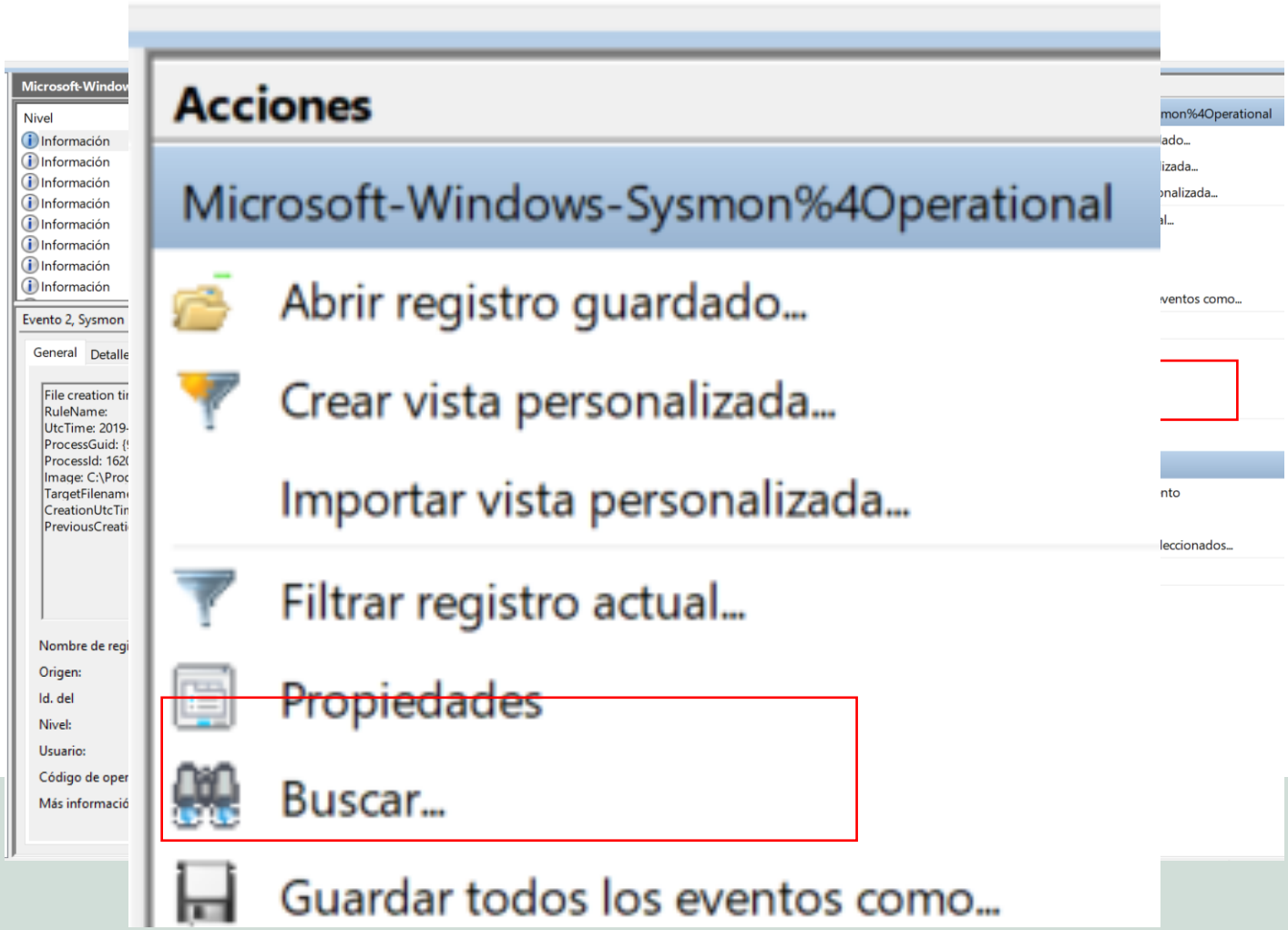
Ejemplo 1
Obteniendo modificaciones del registro

Ahora ya veríamos todos los cambios que ha ido sufriendo el registro de Windows.



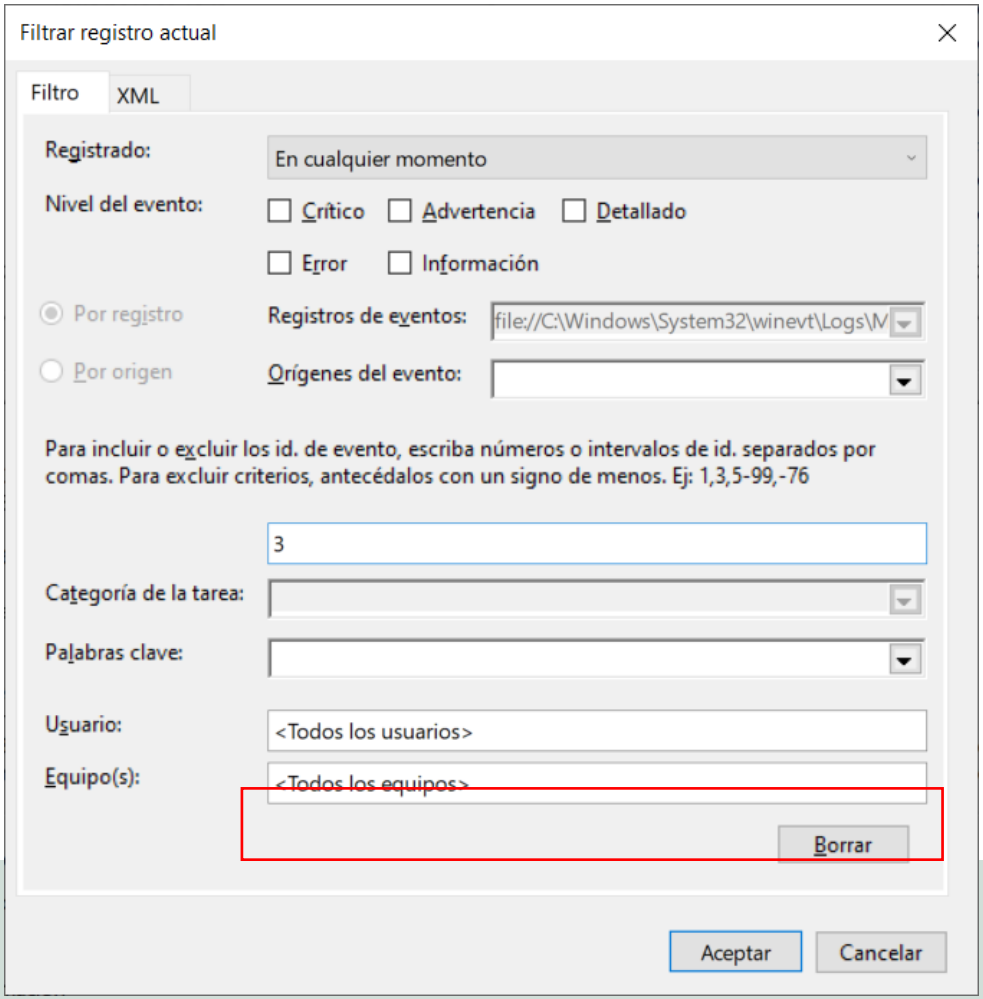
Ejemplo 1
Obteniendo modificaciones del registro

Para filtrar hay que hacer clic en “Filtrar registro actual…”



Ejemplo 2
Obteniendo las conexiones de los procesos

Para obtener las conexiones de red, tenemos que filtrar por el **ID de evento 3**



Ejemplo 2
Obteniendo las conexiones de los procesos

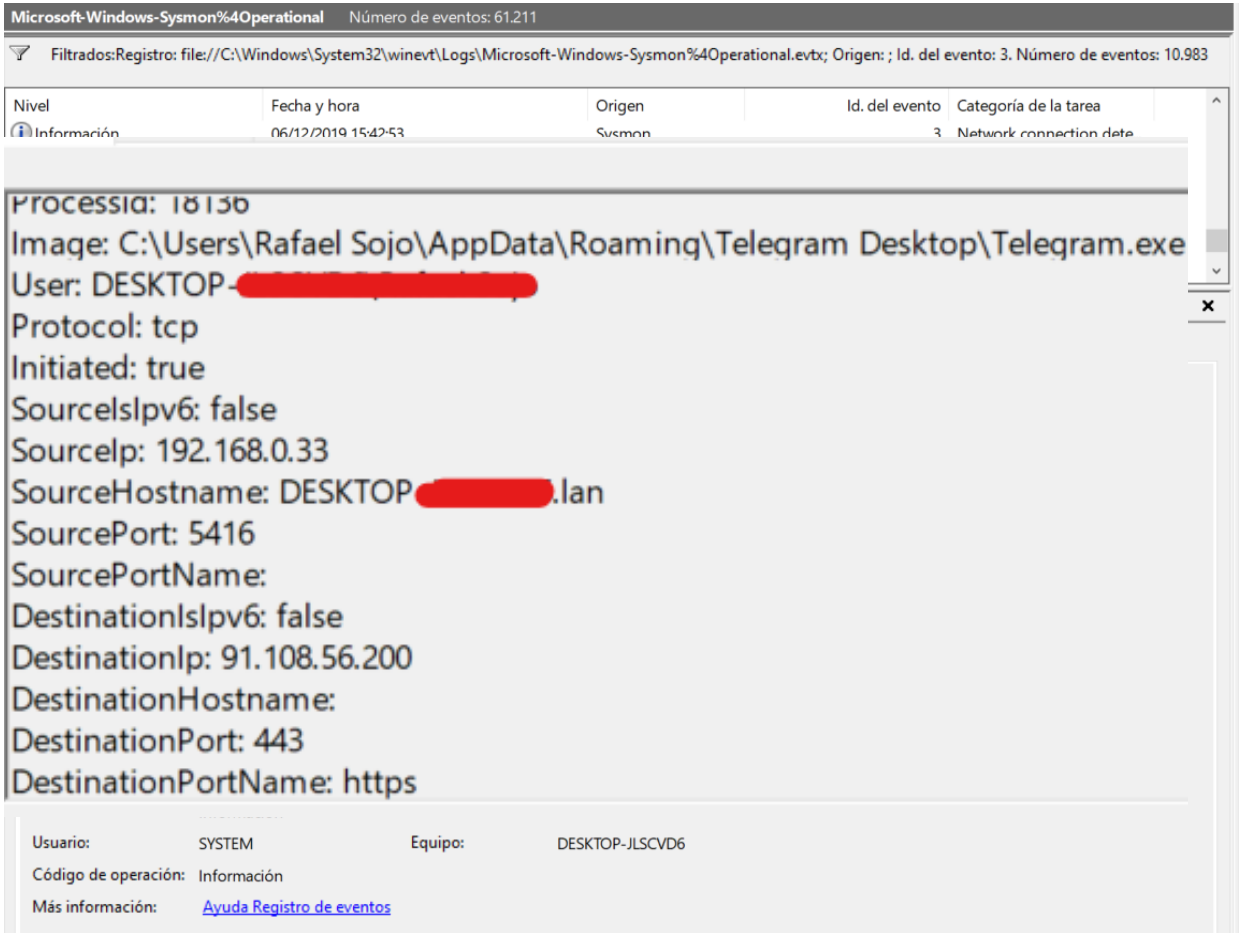
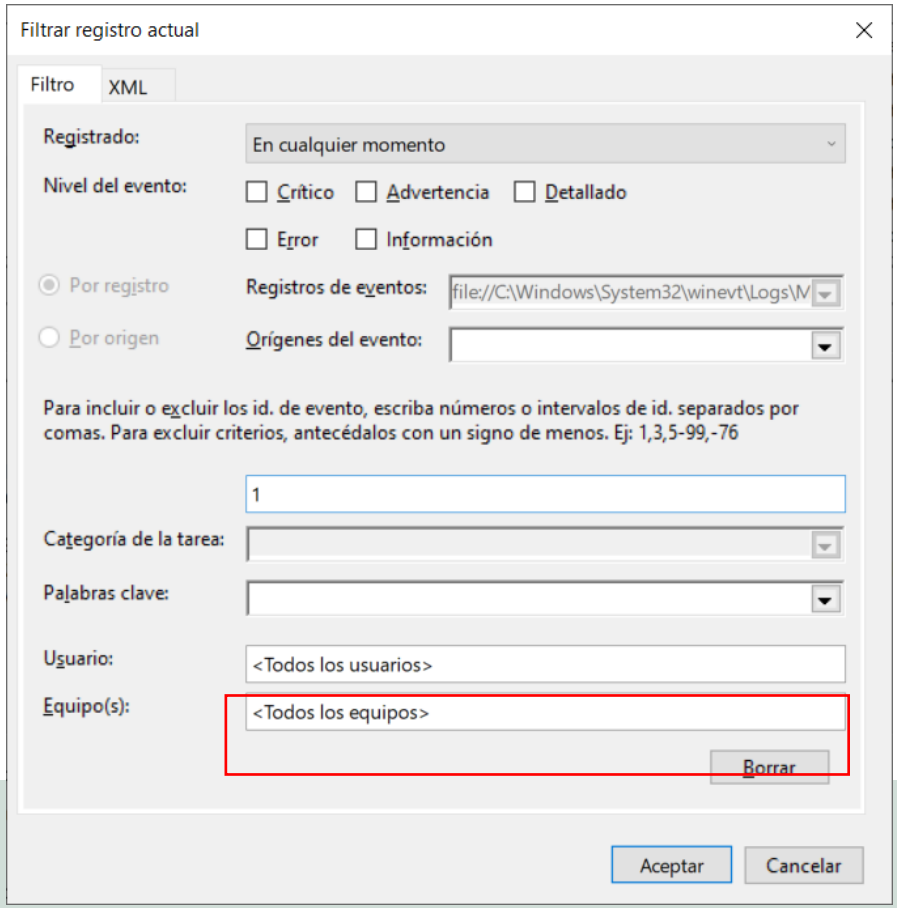


Image es el binario que ha realizado la conexión. En este caso ha sido **Telegram.exe**.

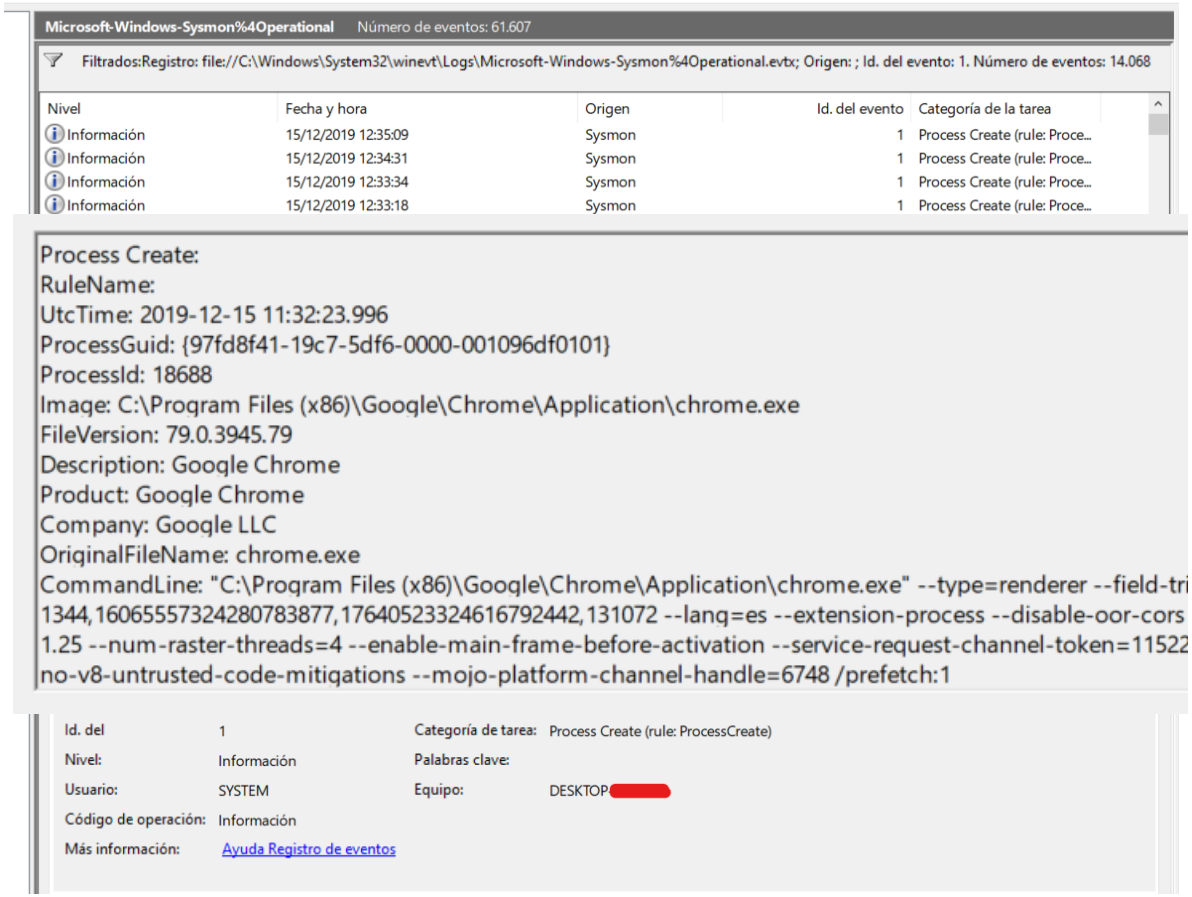
- Conexión desde la IP **192.168.0.33**
- Puerto de origen **5416**
- IP de destino **91.108.56.200**
- Puerto de destino **443**

Ejemplo 2
Obteniendo las conexiones de los procesos

Para obtener la lista de los procesos creados tenemos que filtrar (como hemos hecho en los ejemplos anteriores) por el **ID de evento 1**.



Ejemplo 3
Obteniendo los procesos creados



Podemos obtener la siguiente información:

- Fecha de creación del proceso
- ID de proceso
- Imagen (Ejecutable)
- Versión del ejecutable
- Descripción del ejecutable
- Producto y compañía
- Nombre original del ejecutable
- Comando para la ejecución del ejecutable

Ejemplo 3
Obteniendo los procesos creados

- https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5d5588b51fd81f0001471db4/1565886646582/Windows+Sysmon+Logging+Cheat+Sheet_Aug_2019.pdf
- https://cqureacademy.com/blog/server-monitoring/sysmon
- https://fwhibbit.es/sysmon-el-gran-hermano-de-windows-y-el-super-sysmonview
- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

sedian Seguridad Digital de Andalucía