

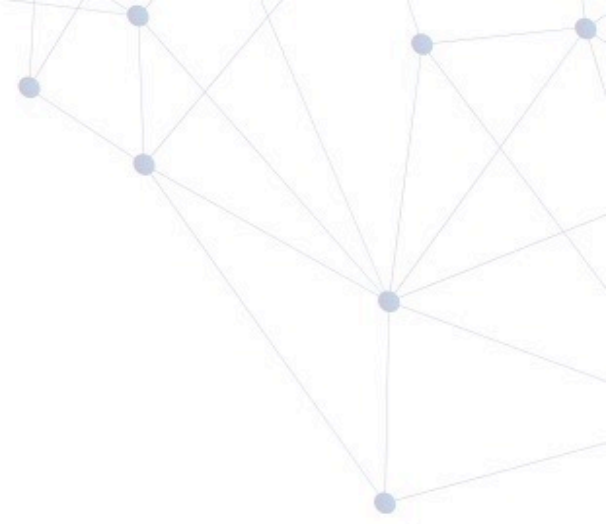
sedian

Seguridad Digital
de Andalucía

Charla virtual de sensibilización

Monitorización de eventos en Windows (Sysmon)





Contenidos

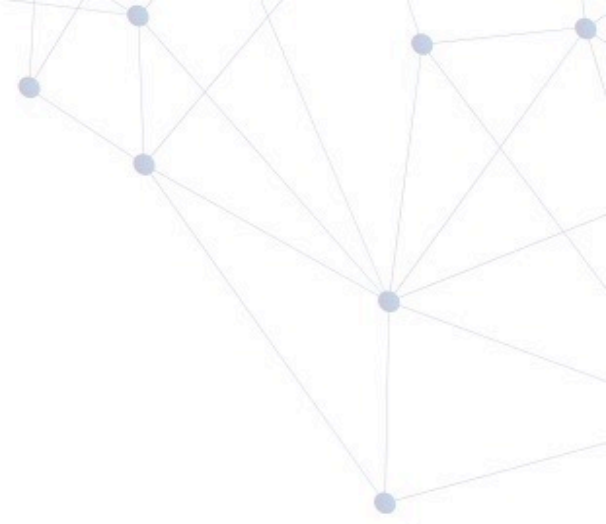
Qué vamos a tratar

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.

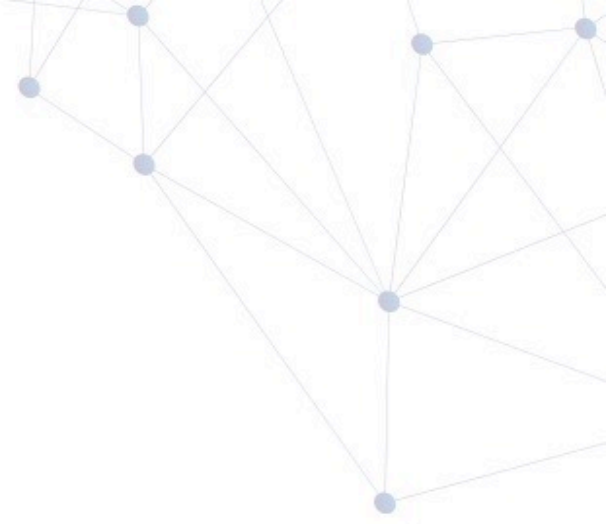


¿Qué es y para qué sirve?

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

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

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

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

Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\[redacted]\Desktop\Sysinternals> _
```

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

Importante **ejecutarlo en como Administrador**.

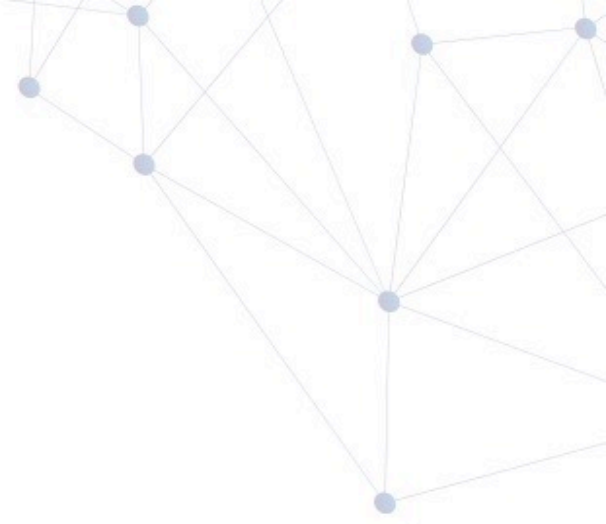
choco install sysmon

```
PS C:\Users\Rafael Sojo\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\Rafael Sojo\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`

```
PS C:\Users\██████████\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\██████████\Desktop\Sysinternals\Sysmon64.exe -i [<configfile>]  
        [-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]  
        [-l [<process,...>]]
```

```
Configure: C:\Users\██████████\Desktop\Sysinternals\Sysmon64.exe -c [<configfile>]  
           [--|[-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]  
           [-l [<process,...>]]]
```

```
Uninstall: C:\Users\██████████\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\██████████\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:

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

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

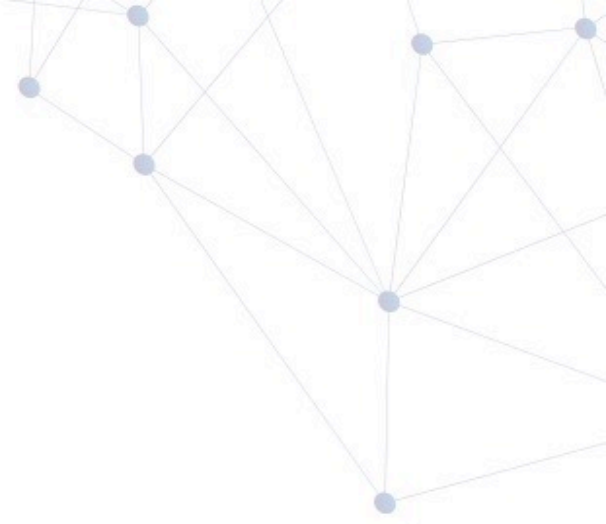
Current configuration:
- Service name:           Sysmon64
- Driver name:            SysmonDrv
- HashingAlgorithms:      MD5,SHA256
- Network connection:     disabled
- Image loading:          disabled
- CRL checking:           disabled
- Process Access:         disabled

Rule configuration (version 4.00):
- FileCreate               onmatch: include   combine rules using 'Or'
  TargetFilename           filter: end with   value: '.ps1'
PS C:\Users\ [redacted] \Desktop\Sysinternals> █
```

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

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

```
C:\Windows\System32\sysmonconfig.xml - Notepad++
Archivo  Editar  Buscar  Vista  Codificación  Idioma  Configuración  Herramientas  Macro  Ejecutar  Plugins  Ventana  ?
new 32  new 33  new 34  server.py  sysmonconfig.xml  Get-SysmonLogsProcessStarts.ps1
1  <!--
2  sysmon-config | A Sysmon configuration focused on default high-quality event tracing and easy customization by the community
3  Master version: 64 | Date: 2018-01-30
4  Master author: @SwiftOnSecurity, other contributors also credited in-line or on Git
5  Master project: https://github.com/SwiftOnSecurity/sysmon-config
6  Master license: Creative Commons Attribution 4.0 | You may privatize, fork, edit, teach, publish, or deploy for commercial use - with attribution in the text.
7
8  Fork version: <N/A>
9  Fork author: <N/A>
10 Fork project: <N/A>
11 Fork license: <N/A>
12
13 REQUIRED: Sysmon version 7.01 or higher (due to changes in registry syntax and bug-fixes)
14 https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
15 Note that 6.03 and 7.01 have critical fixes for filtering, it's recommended you stay updated.
16
17 NOTE: To collect Sysmon logs centrally for free, see https://aka.ms/WEP. Command to allow log access to the Network Service:
18 wevtutil.exe sl Microsoft-Windows-Sysmon/Operational /ca:0:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)
19
20 NOTE: Do not let the size and complexity of this configuration discourage you from customizing it or building your own.
21 This configuration is based around known, high-signal event tracing, and thus appears complicated, but it's only very
22 detailed. Significant effort over years has been invested in front-loading as much filtering as possible onto the
23 client. This is to make analysis of intrusions possible by hand, and to try to surface anomalous activity as quickly
24 as possible to any technician armed only with Event Viewer. Its purpose is to democratize system monitoring for all organizations.
25
26 NOTE: Sysmon is NOT a whitelist solution or HIDS engine, it is a computer change and event logging tool with very basic exclude rules.
27 Do NOT ignore everything possible. Sysmon's purpose is providing context during a threat or problem investigation. Legitimate
28 processes are routinely used by threats - do not blindly exclude them. Additionally, be mindful of process-hollowing / imitation.
29
30 NOTE: Sysmon is not hardened against an attacker with admin rights. Additionally, this configuration offers an attacker, willing
31 to study it, many ways to evade some of the logging. If you are in a high-threat environment, you should consider a much broader
32 log-most approach. However, in the vast majority of cases, an attacker will bumble along through multiple behavioral traps which
33 this configuration monitors, especially in the first minutes.
34
35 TECHNICAL:
36 - Run sysmon.exe -? for a briefing on Sysmon configuration.
37 - Other languages may require localization. Registry and Filesystem paths can change. For example, \shell\open\command\, where "open" is localized.
38 - Sysmon does not support nested/multi-conditional rules. There are only blanket INCLUDE and EXCLUDE. "Exclude" rules override "Include" rules.
39 - If you only specify exclude for a filtering subsection, everything in that subsection is logged by default.
40 - Some Sysmon monitoring abilities are not meant for widely deployed general-purpose use due to performance impact. Depends on environment.
41 - Duplicate or overlapping "Include" rules do not result in duplicate events being logged.
42 - All characters enclosed by XML tags are always interpreted literally. Sysmon does not support wildcards (*), alternate characters, or RegEx.
43 - In registry events, the value name is appended to the full key path with a "\" delimiter. Default key values are named "(Default)"
44
45
eXtensible Markup Language file      length: 96,708  lines: 837  Ln: 21  Col: 37  Sel: 0 | 0  Unix (LF)  UTF-8  INS
```



Análisis de la información

Por defecto los logs se guardan en la siguiente ruta:

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

esultados de la búsqueda en Logs

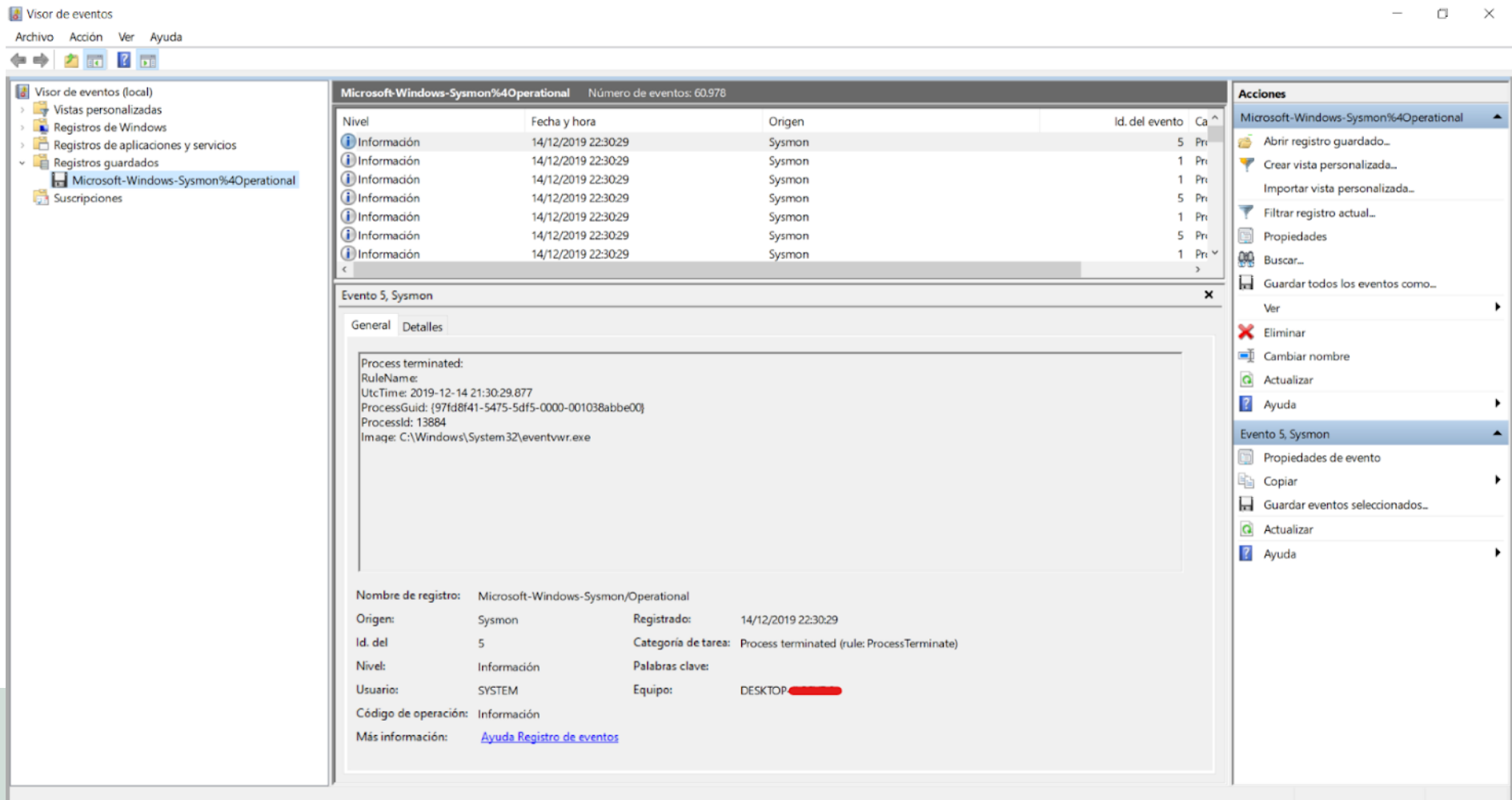


Microsoft-Windows-Sysmon%4Operational.evtx

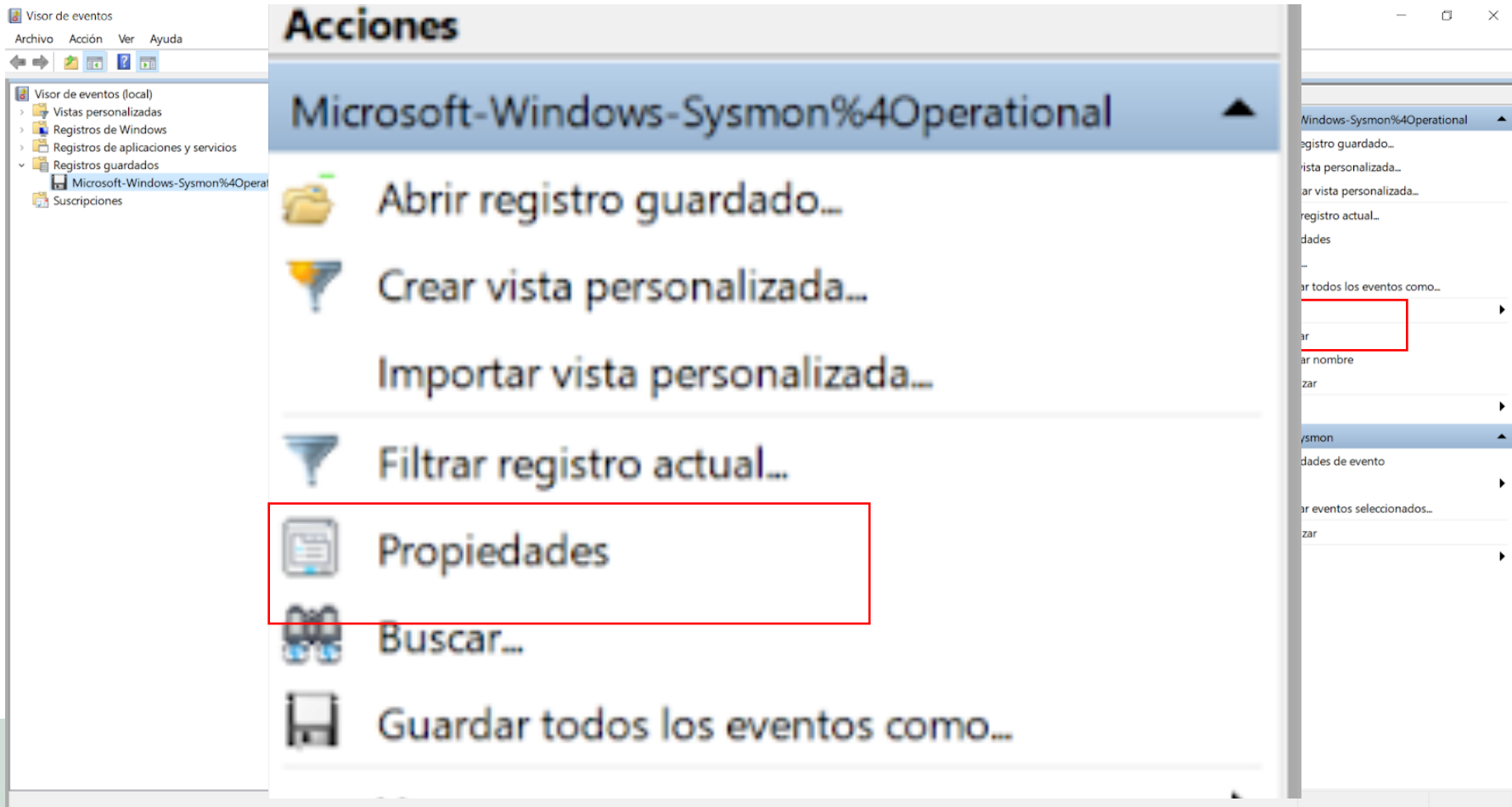
C:\Windows\System32\winevt\Logs

Tipo: Registro de eventos

Este es el aspecto del visor de eventos de Windows



Para filtrar eventos tenemos que hacer clic en "Filtrar registro actual"



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

Filtrar registro actual

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado
☐ Error ☐ Información

☒ Por registro ☐ Por origen

Registros de eventos: file:///C:/Windows/System32/winevt/Logs/W

Orígenes del evento:

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

3

Categoría de la tarea:

Palabras clave:

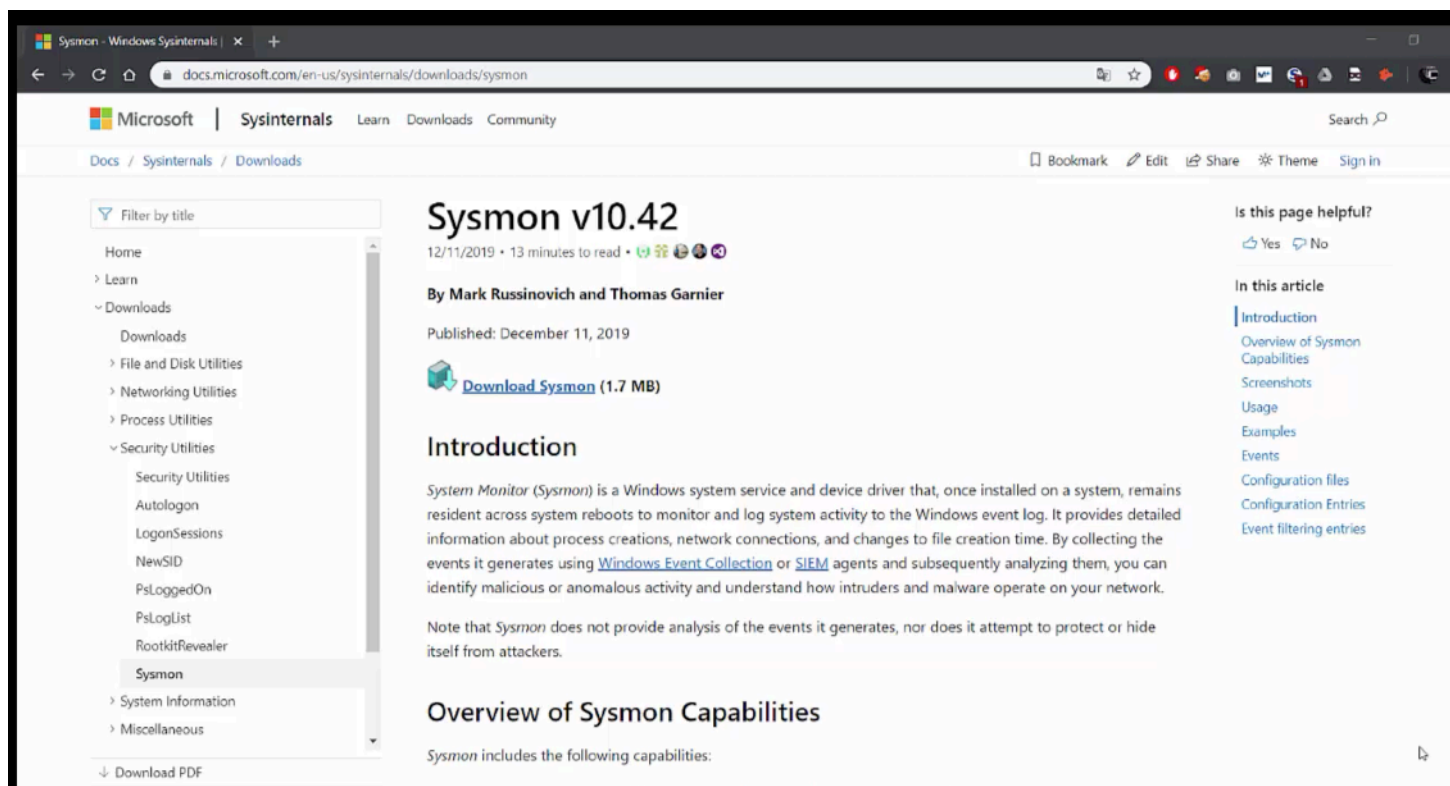
Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>

Borrar

Aceptar Cancelar

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\█████████\Desktop> $events
```

ProviderName: Microsoft-Windows-Sysmon

TimeCreated	Id	Level	DisplayName	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:...

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

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

```
PS C:\Users\██████████\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\██████████\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*)}`

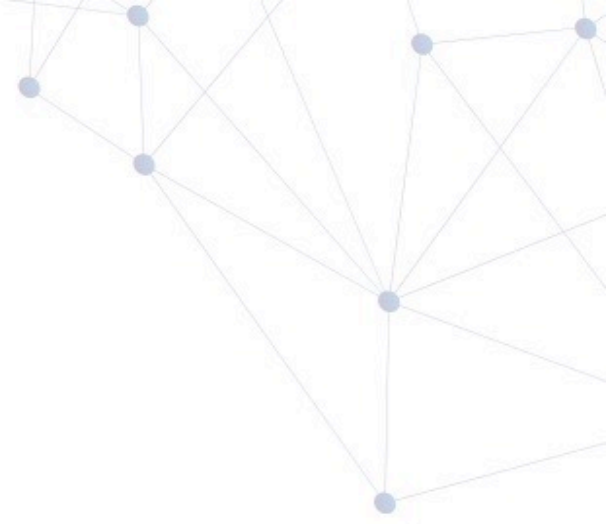
```
PS C:\Users\█████████\Desktop> .\Get-SysmonLogsProcessStarts.ps1 | where {($_.CommandLine -like "*powershell*")}

ParentImage      : 0x4f2e9
Hashes            : C:\Powershell\Pruebas sysmon\
CommandLine      : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
UTCTime          :
IntegrityLevel    : C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe -NoProfile -NonInteractive -ExecutionPolicy Bypass -Command "& 'c:\Users\█████████\
                    .\vscode\extensions\ms-vscode.powershell-2019.11.0\modules\PowerShellEditorServices\Start-EditorServices.ps1' -HostName 'Visual Studio Code Host' -HostProfileId 'M
                    -AdditionalModules @( 'PowerShellEditorServices.VSCode' ) -BundledModulesPath 'c:\Users\█████████\vscode\extensions\ms-vscode.powershell-2019.11.0\modules' -EnableCo
                    'c:\Users\█████████\vscode\extensions\ms-vscode.powershell-2019.11.0\logs\1576412406-783b7049-8e06-4366-8a6c-7fad9d32e8211576405343627\EditorServices.log' -SessionI
                    Sojo\vscode\extensions\ms-vscode.powershell-2019.11.0\sessions\PSES-VSCode-15840-316333' -FeatureFlags @()"
CurrentDirectory : 10.0.18362.1 (WinBuild.160101.0800)
User             : Windows PowerShell

ParentImage      : 0x4efb6
Hashes            : C:\WINDOWS\system32\
CommandLine      : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
UTCTime          :
IntegrityLevel    : "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
CurrentDirectory : 10.0.18362.1 (WinBuild.160101.0800)
User             : Windows PowerShell

ParentImage      : 0x4f2e9
```

Obteniendo registros en powershell
y filtrando



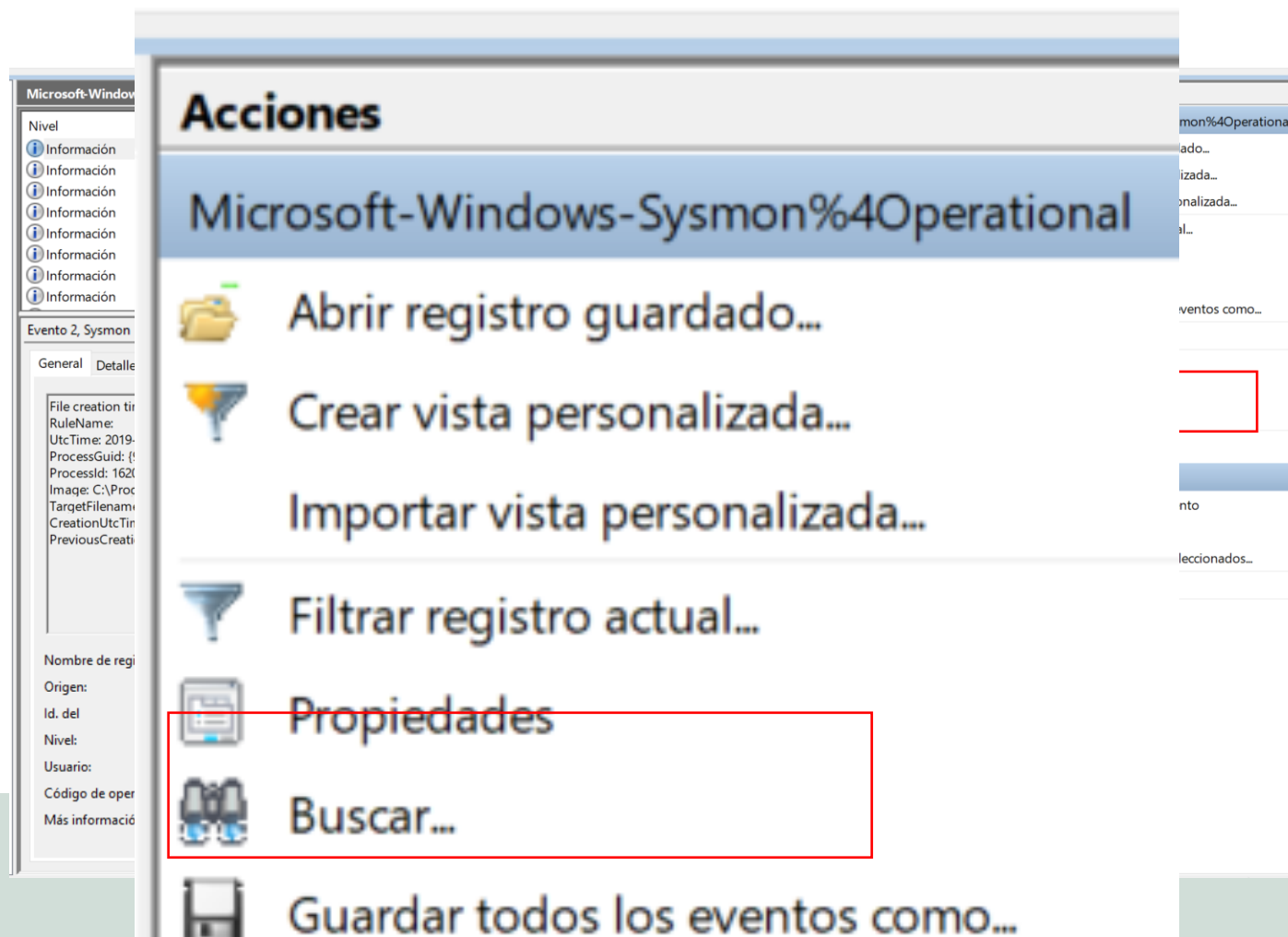
Ejemplos de uso

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**

Filtrar registro actual

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado
☐ Error ☐ Información

☒ Por registro ☐ Por origen

Registros de eventos: file:///C:/Windows/System32/winevt/Logs/W

Orígenes del evento:

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

12,13,14

Categoría de la tarea:

Palabras clave:

Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>

Borrar

Aceptar Cancelar

Ejemplo 1
Obteniendo modificaciones del
registro

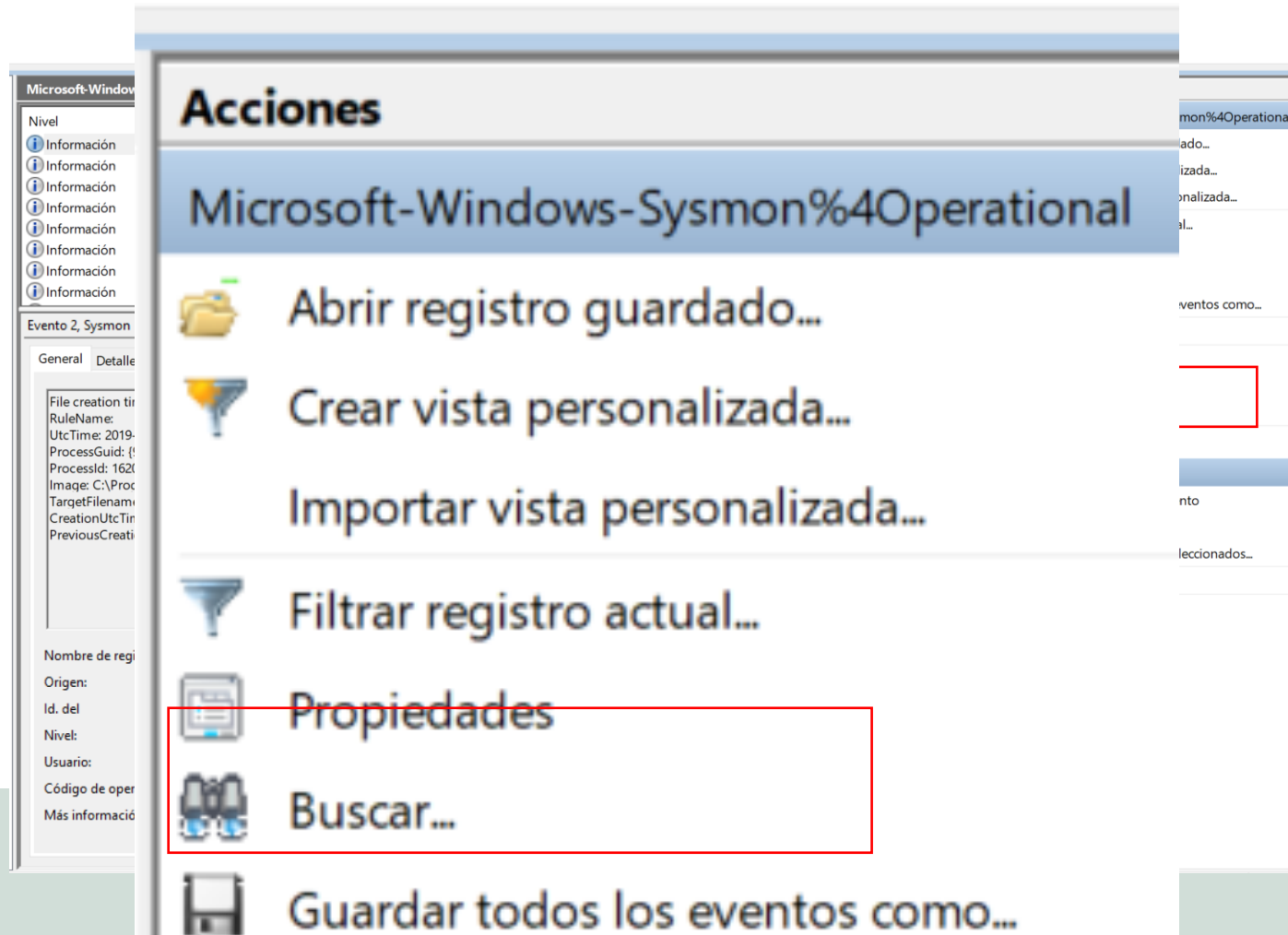
Ahora ya veríamos todos los cambios que ha ido sufriendo el registro de Windows.

Filtrados:Registro: file://C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx; Origen: ; Id. del evento: 12,13,14. Número de

Nivel	Fecha y hora	Origen	Id. del ...	Categoría de la tarea
Información	13/12/2019 17:21:40	Sysmon	13	Registry value set (rule: RegistryEvent)
Información	13/12/2019 17:21:38	Sysmon	13	Registry value set (rule: RegistryEvent)
Información	13/12/2019 17:21:37	Sysmon	12	Registry object added or deleted (rule: Re...
Información	13/12/2019 17:21:36	Sysmon	13	Registry value set (rule: RegistryEvent)
Información	13/12/2019 17:21:36	Sysmon	13	Registry value set (rule: RegistryEvent)
Información	13/12/2019 17:21:35	Sysmon	12	Registry object added or deleted (rule: Re...

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**

Filtrar registro actual

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado
☐ Error ☐ Información

☒ Por registro Registros de eventos: file:///C:/Windows/System32/winevt/Logs/V...
☐ Por origen Orígenes del evento: ...

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

3

Categoría de la tarea: ...

Palabras clave: ...

Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>

Borrar

Aceptar Cancelar

Ejemplo 2
Obteniendo las conexiones de
los procesos

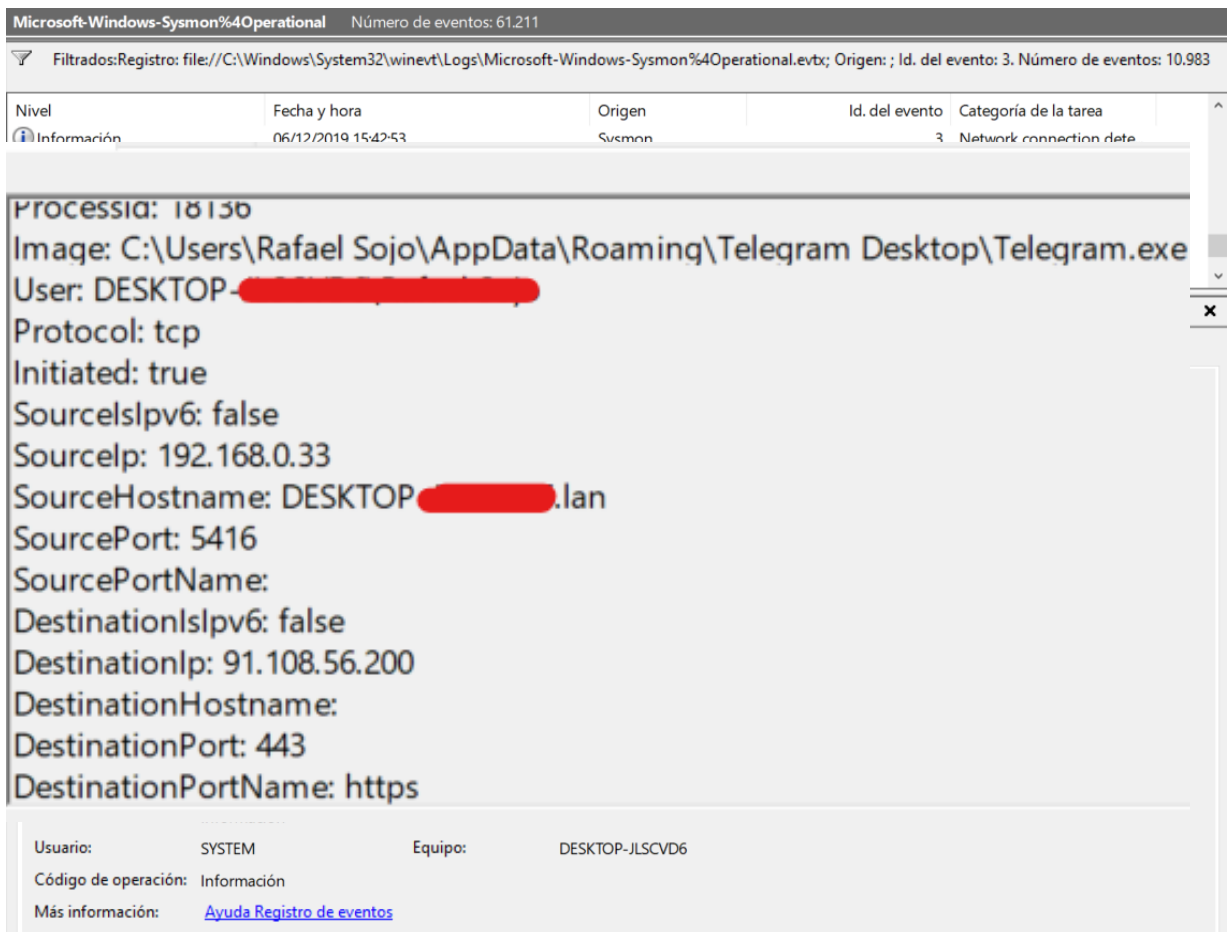


Image es el binario que ha realizado la conexión. En este caso ha sido **Telegram.exe**.

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

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

Filtrar registro actual

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado
☐ Error ☐ Información

☒ Por registro Registros de eventos: file://C:\Windows\System32\winevt\Logs\W
☐ Por origen Orígenes del evento:

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

1

Categoría de la tarea:

Palabras clave:

Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>

Borrar

Aceptar Cancelar

Ejemplo 3
Obteniendo los procesos creados

Microsoft-Windows-Sysmon%4Operational Número de eventos: 61.607

Filtrados: Registro: file://C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx; Origen: ; Id. del evento: 1. Número de eventos: 14.068

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	15/12/2019 12:35:09	Sysmon	1	Process Create (rule: Proce...
Información	15/12/2019 12:34:31	Sysmon	1	Process Create (rule: Proce...
Información	15/12/2019 12:33:34	Sysmon	1	Process Create (rule: Proce...
Información	15/12/2019 12:33:18	Sysmon	1	Process Create (rule: Proce...

Process Create:
RuleName:
UtcTime: 2019-12-15 11:32:23.996
ProcessGuid: {97fd8f41-19c7-5df6-0000-001096df0101}
ProcessId: 18688
Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
FileVersion: 79.0.3945.79
Description: Google Chrome
Product: Google Chrome
Company: Google LLC
OriginalFileName: chrome.exe
CommandLine: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-tri
1344,16065557324280783877,17640523324616792442,131072 --lang=es --extension-process --disable-oor-cors
1.25 --num-raster-threads=4 --enable-main-frame-before-activation --service-request-channel-token=11522
no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=6748 /prefetch:1

Id. del	1	Categoría de tarea:	Process Create (rule: ProcessCreate)
Nivel:	Información	Palabras clave:	
Usuario:	SYSTEM	Equipo:	DESKTOP- XXXXXXXXXX
Código de operación:	Información		
Más información:	Ayuda Registro de eventos		

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

- https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5d5588b51fd81f0001471db4/1565886646582/Windows+Sysmon+Logging+Cheat+Sheet_Aug_2019.pdf
- <https://cquireacademy.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