

```
Administrator: Eingabeaufforderung
C:\Sysmon>sysmon64 -accepteula -i -h sha256 -n

System Monitor v10.0 - 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.

C:\Sysmon>
```

Sysinternals Sysmon jetzt mit einer DNS Query Protokollierung

Sysinternals - Sysmon mit DNS Protokollierung

Die neue Ereignis-ID für DNS-Abfragen lautet 22. Sobald ein Prozess eine DNS-Abfrage ausführt, wird dieses als Ereignis ins LOG geschrieben, egal ob das Ergebnis positiv oder negativ ist.

Download Sysmon

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

Download aller Tools

<https://live.sysinternals.com/>

```
Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-Sysmon/Operational";id=3;} | Where {$_.message -like "*172.18.32.10*" -and $_.message -like "*DestinationPort: 80*"} | Select-Object -Property message -First
```

<https://www.der-windows-papst.de/2019/06/12/sysinternals-sysmon-jetzt-mit-einer-dns-query-protokollierung/>

1 | Format-List

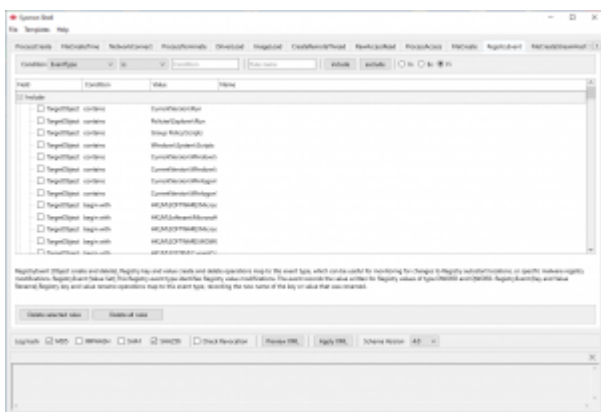
```
Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-Sysmon/Operational";id=3;} | Where {$_.message -like "*172.18.32.10*" -and $_.message -like "*DestinationPort: 443*"} | Select-Object -Property message -First 1 | Format-List
```

```
Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-Sysmon/Operational";id=22;} | Format-List
```

Sysmon Search Event

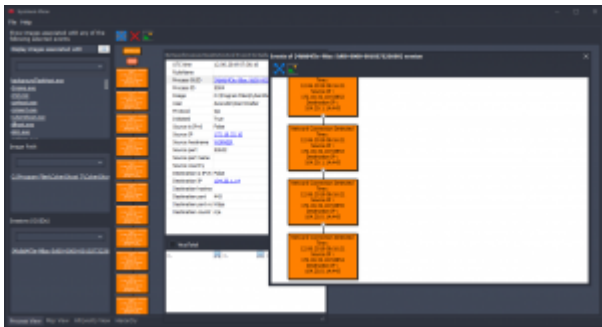
Sysmon Tools

Die Sysmon Shell ein Tool zur Erstellung von Konfigurations-Templates und vieles mehr.



Sysmon View, ein Offline Tool zur grafischen Auswertung der Events. Es unterstützt bei der Verfolgung und Visualisierung von Sysmon-Protokollen, indem verschiedene Sysmon-Ereignisse logisch gruppiert und miteinander in Beziehung gesetzt werden.

<https://www.der-windows-papst.de/2019/06/12/sysinternals-sysmon-jetzt-mit-einer-dns-query-protokollierung/>



[Download Sysmon Tools](#)

<https://www.der-windows-papst.de/2019/06/12/sysinternals-sysmon-jetzt-mit-einer-dns-query-protokollierung/>