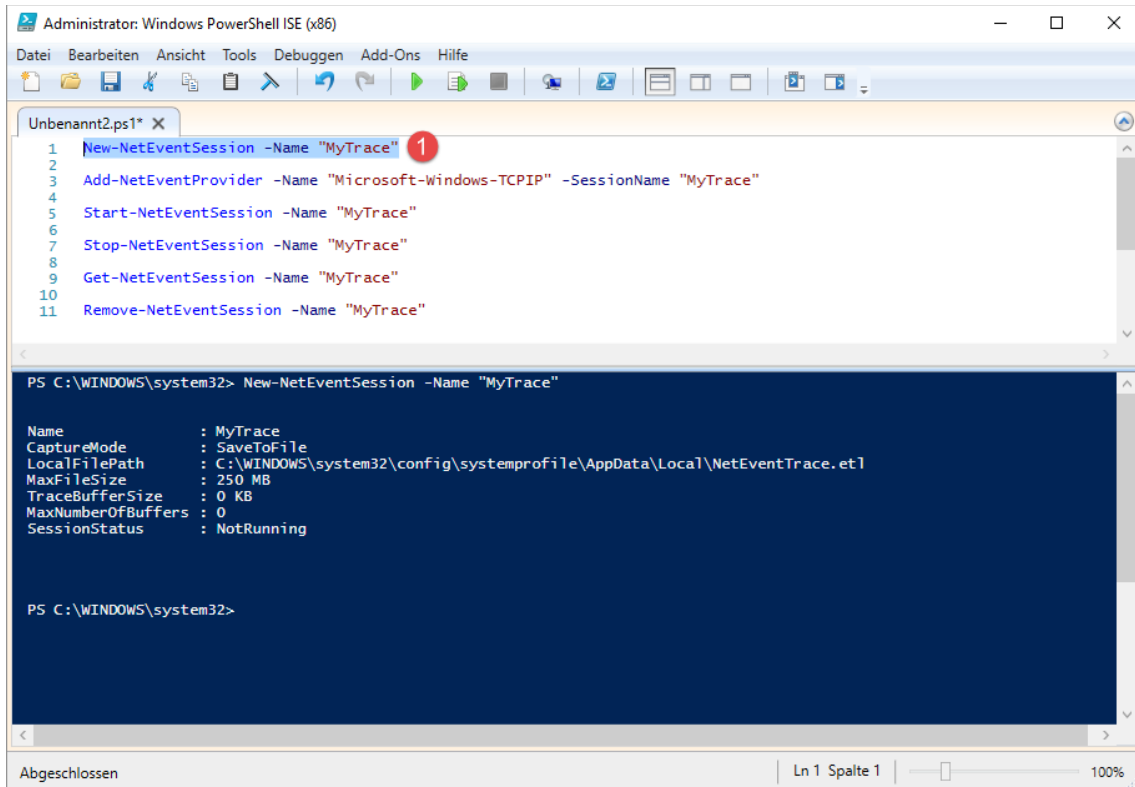


## Windows - Netzwerkaufzeichnung Powershell

Wer kein Wireshark oder Microsoft Network Analyzer hat kann die Powershell zu Hilfe nehmen um den Netzwerkverkehr aufzuzeichnen und später zu analysieren.

Und so geht's:

Als erstes erstellen wir ein Event namens „MyTrace“



```
Administrator: Windows PowerShell ISE (x86)
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

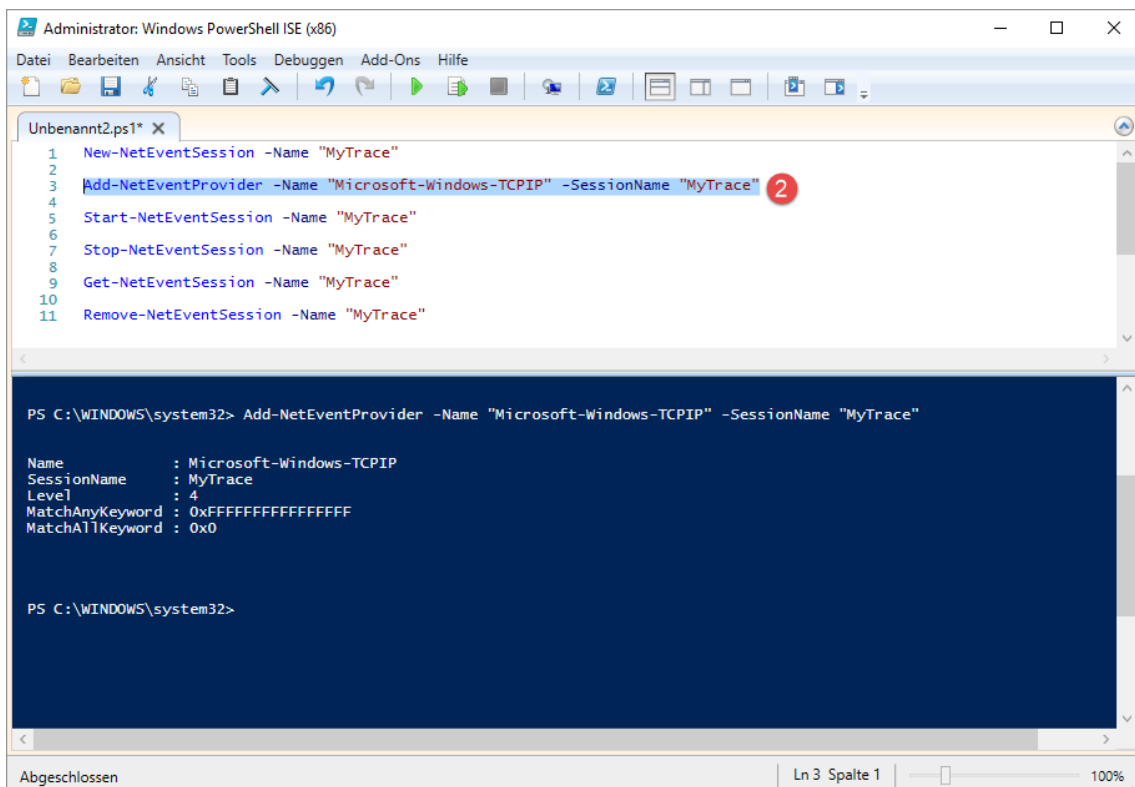
Unbenannt2.ps1 X
1 New-NetEventSession -Name "MyTrace" 1
2
3 Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName "MyTrace"
4
5 Start-NetEventSession -Name "MyTrace"
6
7 Stop-NetEventSession -Name "MyTrace"
8
9 Get-NetEventSession -Name "MyTrace"
10
11 Remove-NetEventSession -Name "MyTrace"

PS C:\WINDOWS\system32> New-NetEventSession -Name "MyTrace"

Name                : MyTrace
CaptureMode          : SaveToFile
LocalFilePath        : C:\WINDOWS\system32\config\systemprofile\AppData\Local\NetEventTrace.etl
MaxFileSize          : 250 MB
TraceBufferSize      : 0 KB
MaxNumberOfBuffers   : 0
SessionStatus        : NotRunning

PS C:\WINDOWS\system32>
```

Danach definieren wir den zu überwachenden Provider.



```
Administrator: Windows PowerShell ISE (x86)
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

Unbenannt2.ps1 X
1 New-NetEventSession -Name "MyTrace"
2
3 Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName "MyTrace" 2
4
5 Start-NetEventSession -Name "MyTrace"
6
7 Stop-NetEventSession -Name "MyTrace"
8
9 Get-NetEventSession -Name "MyTrace"
10
11 Remove-NetEventSession -Name "MyTrace"

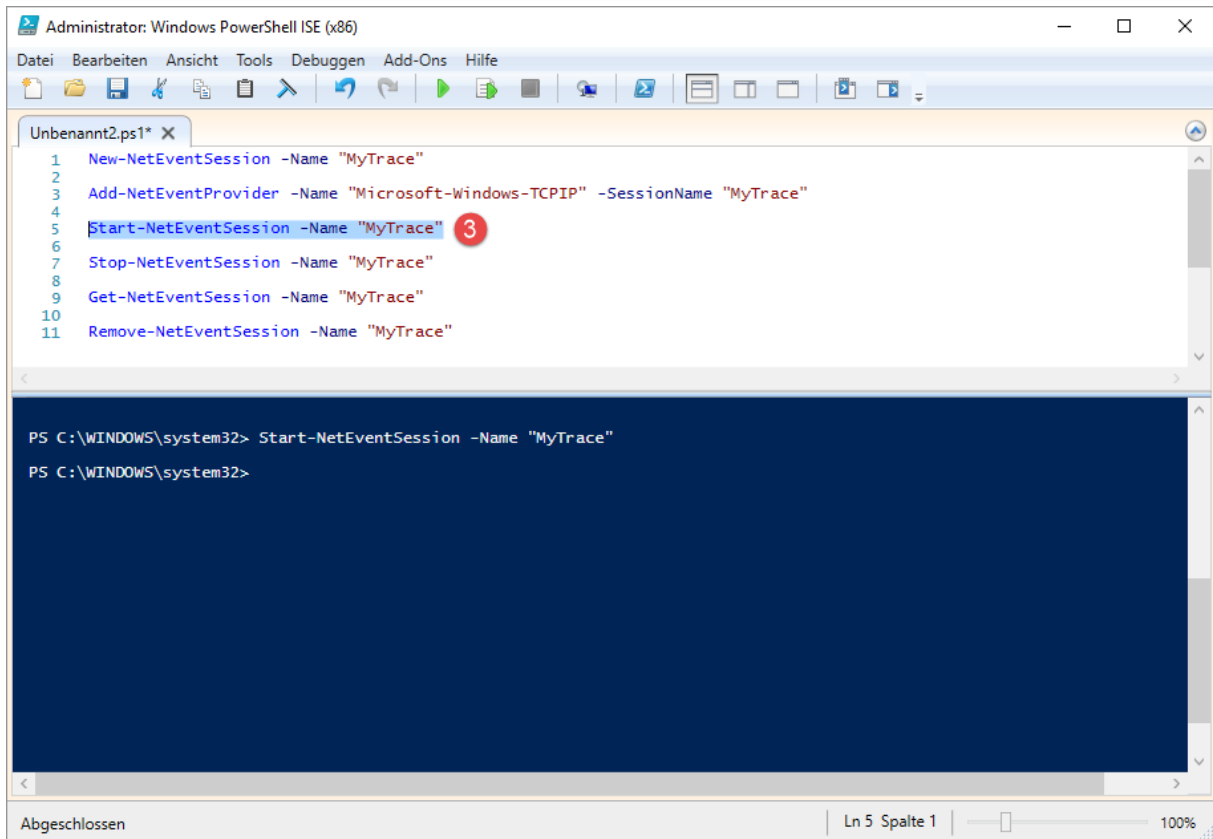
PS C:\WINDOWS\system32> Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName "MyTrace"

Name                : Microsoft-Windows-TCPIP
SessionName          : MyTrace
Level                : 4
MatchAnyKeyword      : 0xFFFFFFFFFFFFFFFF
MatchAllKeyword      : 0x0

PS C:\WINDOWS\system32>
```

## Windows - Netzwerkaufzeichnung Powershell

Starten den Trace.



The screenshot shows the Windows PowerShell ISE interface. The script editor contains the following commands:

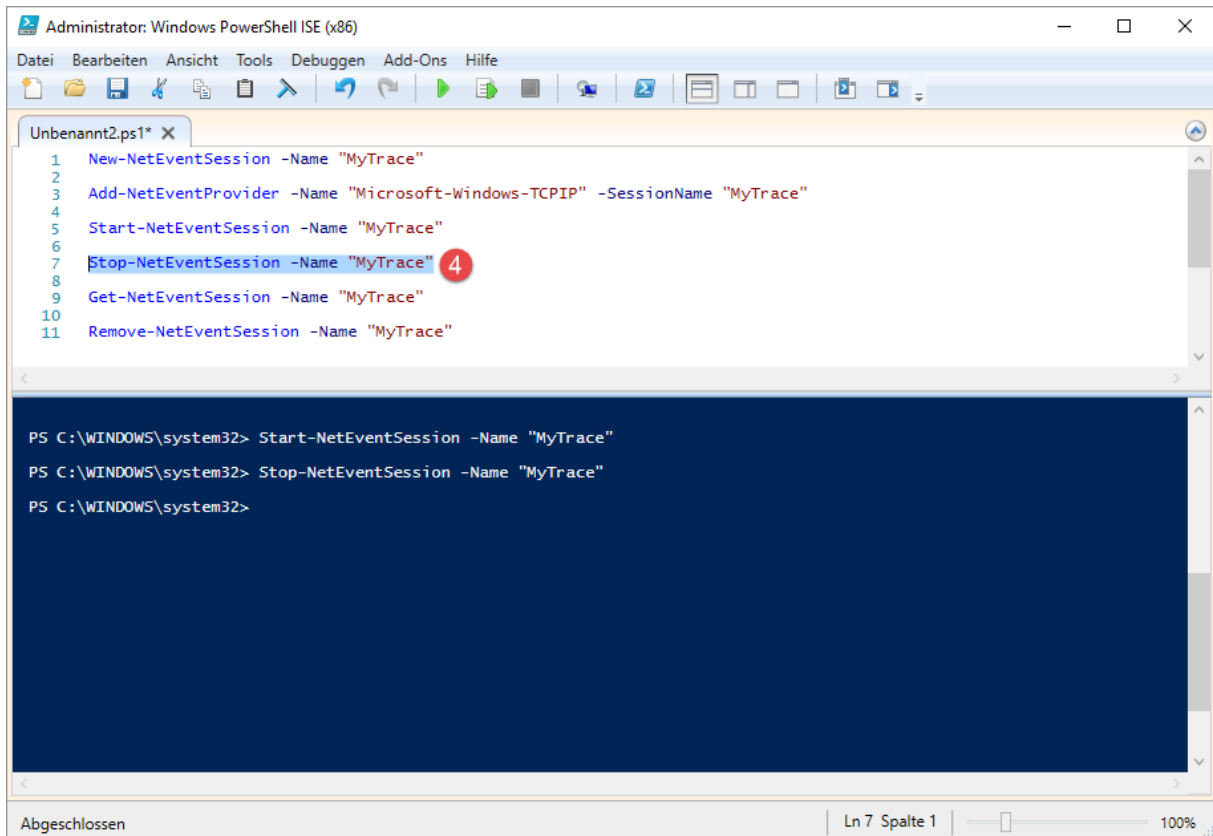
```
1 New-NetEventSession -Name "MyTrace"  
2 Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName "MyTrace"  
3 Start-NetEventSession -Name "MyTrace"  
4  
5 Stop-NetEventSession -Name "MyTrace"  
6  
7 Get-NetEventSession -Name "MyTrace"  
8  
9 Remove-NetEventSession -Name "MyTrace"  
10  
11
```

The command on line 3, `Start-NetEventSession -Name "MyTrace"`, is highlighted in blue. A red circle with the number 3 is next to it. The console window below shows the execution of this command:

```
PS C:\WINDOWS\system32> Start-NetEventSession -Name "MyTrace"  
PS C:\WINDOWS\system32>
```

The status bar at the bottom indicates "Abgeschlossen" (Completed) and "Ln 5 Spalte 1" (Line 5, Column 1).

Surfen etwas oder oder oder und stoppen den Trace.



The screenshot shows the Windows PowerShell ISE interface. The script editor contains the following commands:

```
1 New-NetEventSession -Name "MyTrace"  
2 Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName "MyTrace"  
3 Start-NetEventSession -Name "MyTrace"  
4  
5 Stop-NetEventSession -Name "MyTrace"  
6  
7 Get-NetEventSession -Name "MyTrace"  
8  
9 Remove-NetEventSession -Name "MyTrace"  
10  
11
```

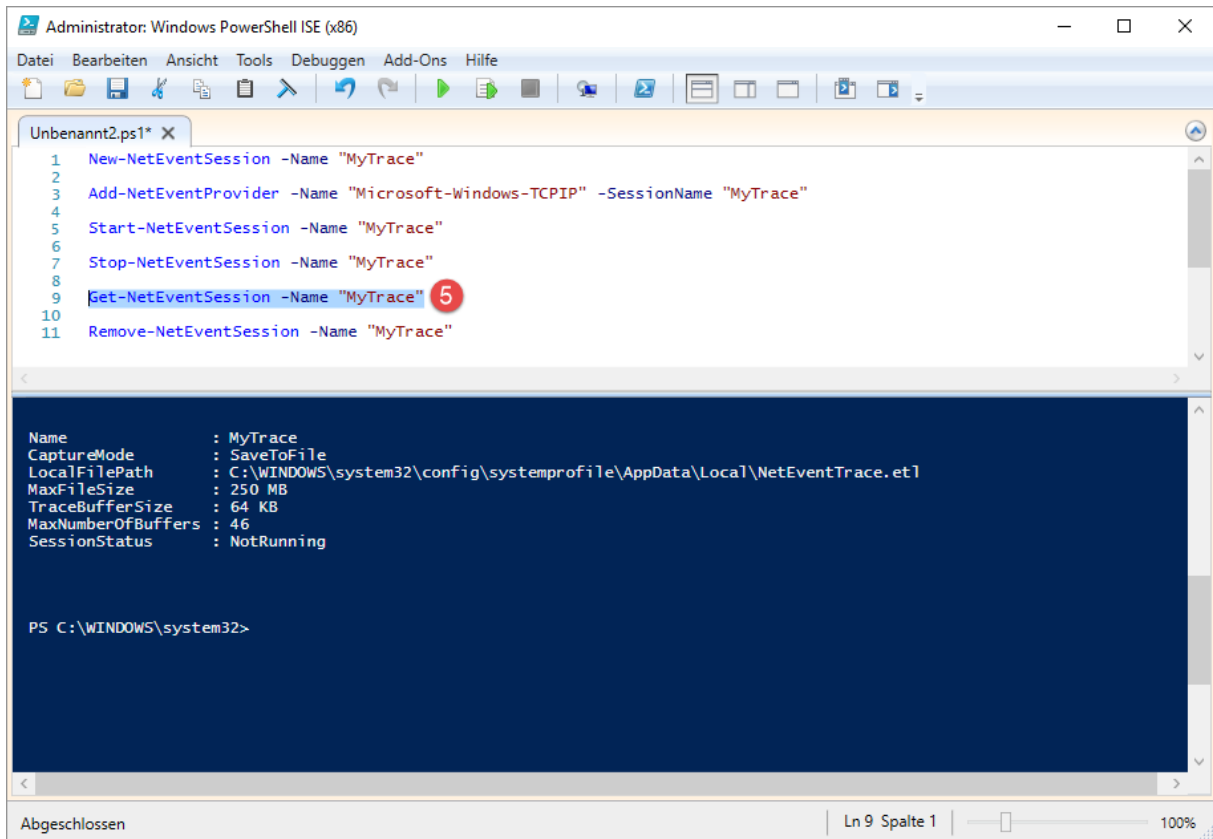
The command on line 5, `Stop-NetEventSession -Name "MyTrace"`, is highlighted in blue. A red circle with the number 4 is next to it. The console window below shows the execution of this command:

```
PS C:\WINDOWS\system32> Start-NetEventSession -Name "MyTrace"  
PS C:\WINDOWS\system32> Stop-NetEventSession -Name "MyTrace"  
PS C:\WINDOWS\system32>
```

The status bar at the bottom indicates "Abgeschlossen" (Completed) and "Ln 7 Spalte 1" (Line 7, Column 1).

# Windows - Netzwerkaufzeichnung Powershell

Lassen und die Protokolldatei anzeigen.



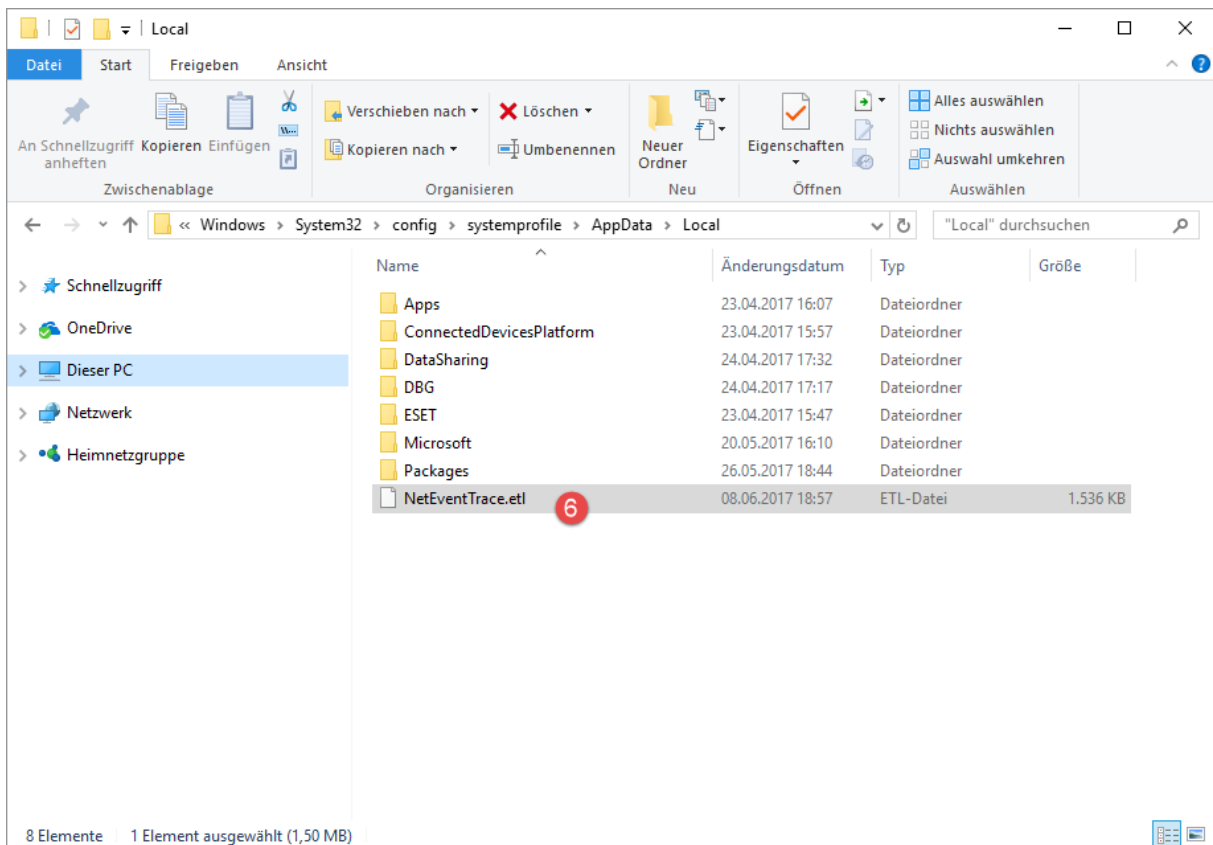
```
Administrator: Windows PowerShell ISE (x86)
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Unbenannt2.ps1* X
1 New-NetEventSession -Name "MyTrace"
2
3 Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName "MyTrace"
4
5 Start-NetEventSession -Name "MyTrace"
6
7 Stop-NetEventSession -Name "MyTrace"
8
9 Get-NetEventSession -Name "MyTrace" 5
10
11 Remove-NetEventSession -Name "MyTrace"

Name           : MyTrace
CaptureMode    : SaveToFile
LocalFilePath  : C:\WINDOWS\system32\config\systemprofile\AppData\Local\NetEventTrace.etl
MaxFileSize    : 250 MB
TraceBufferSize : 64 KB
MaxNumberOfBuffers : 46
SessionStatus  : NotRunning

PS C:\WINDOWS\system32>
```

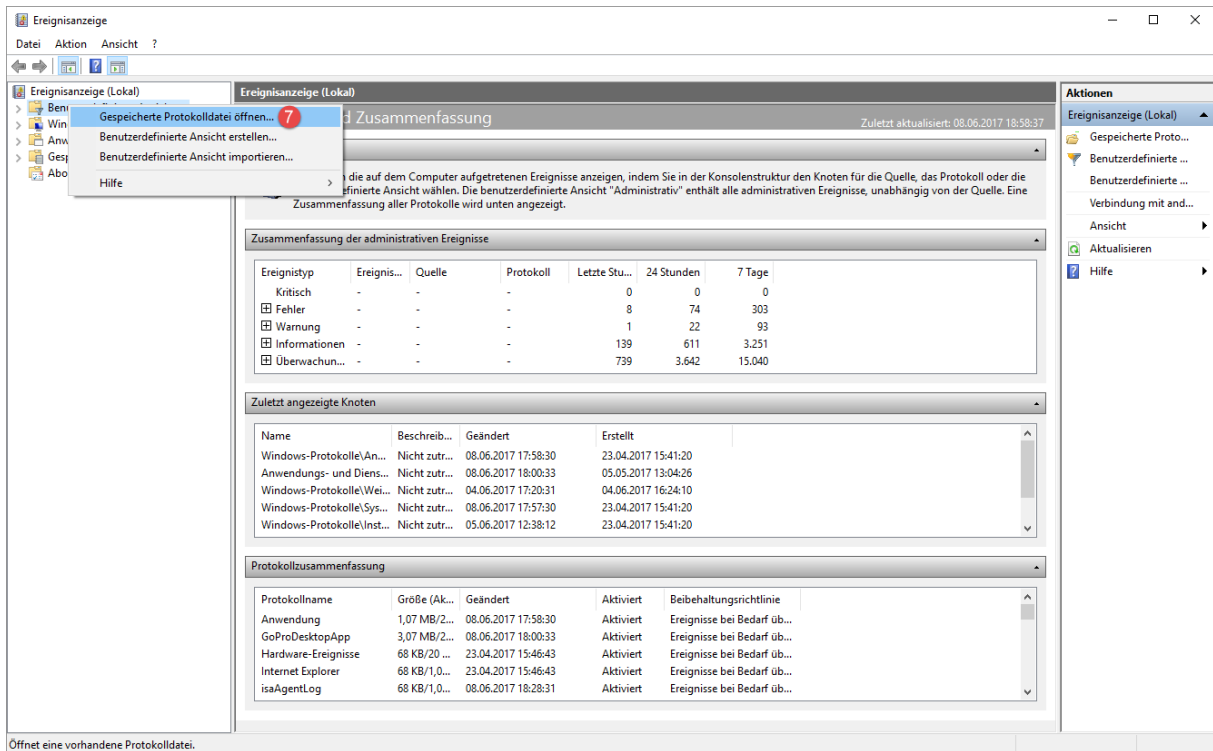
Abgeschlossen | Ln 9 Spalte 1 | 100%

Öffnen den Pfad.

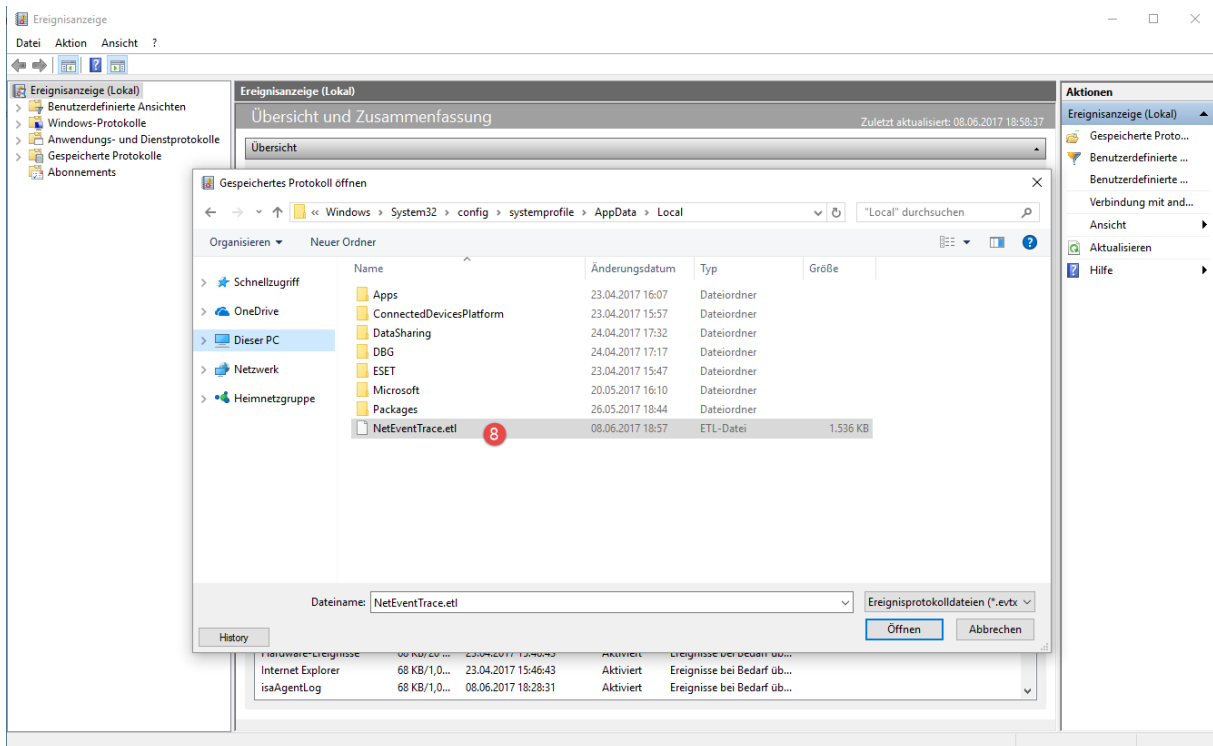


# Windows - Netzwerkaufzeichnung Powershell

Starten die Ereignisanzeige und öffnen die Protokolldatei.

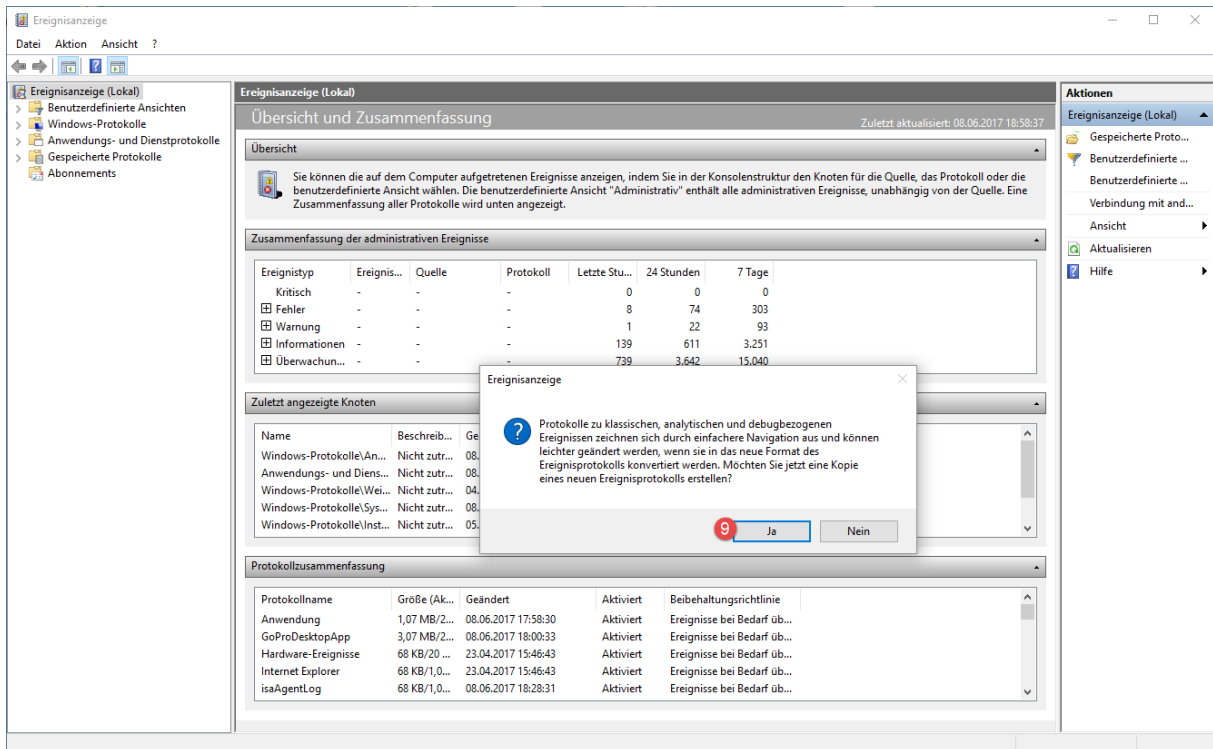


Navigieren zum obigen Pfad und wählen die .etl Datei aus.

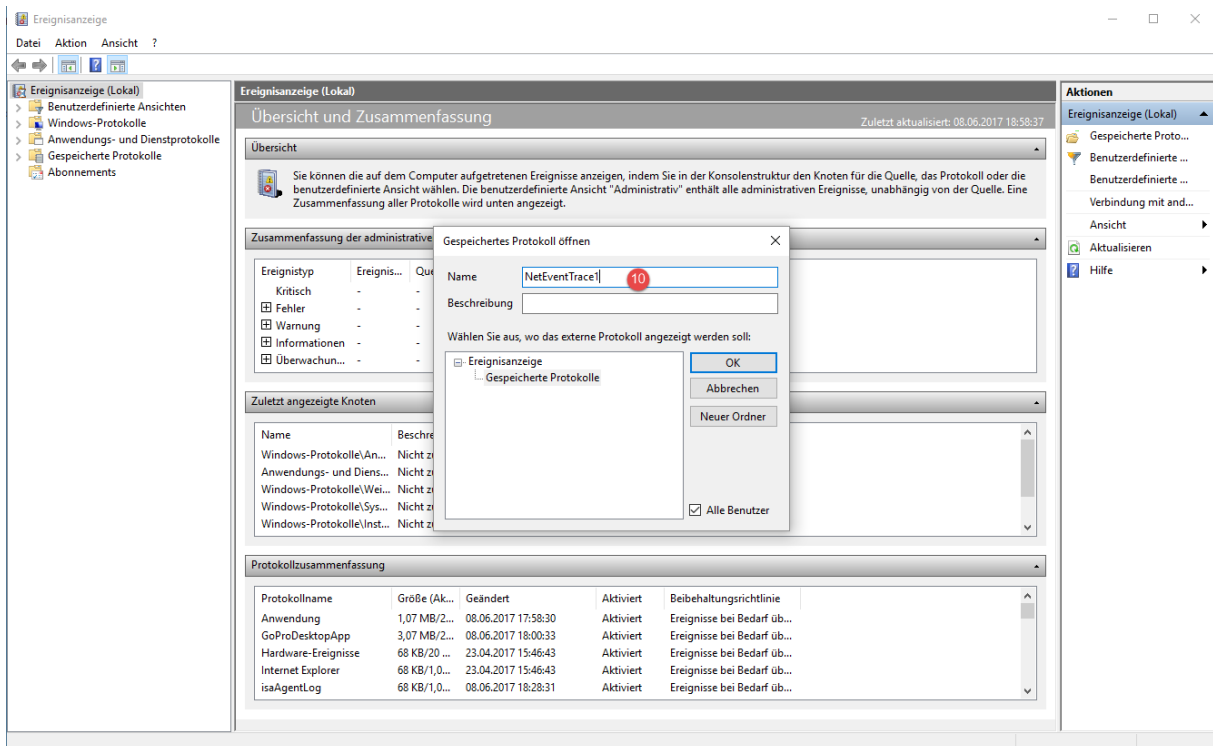


# Windows - Netzwerkaufzeichnung Powershell

Konvertieren das Format \*.



Geben dem zu öffnenden Protokoll einen Namen.



# Windows - Netzwerkaufzeichnung Powershell

Navigieren nun in den Ereignissen und fangen an zu analysieren.

The screenshot shows the Windows Event Viewer interface. The left pane shows the navigation tree with 'NetEventTrace1' selected. The main pane displays a list of events under 'NetEventTrace1' with 9,508 total events. The selected event is ID 1332, categorized as 'Informationen' and 'TCPIP', occurring on 08.06.2017 at 18:57:01. The details pane shows the following information:

TCPIP: Verbindung 0xffffd00c1db320: TCP-Sendeereignis, SeqNo = 4132508672, BytesSent = 1, CWnd = 14600, SndWnd = 2920, Srtt = 0, RttVar = 768000, RTO = 3000, RcvWnd = 64240.

Protokollname:  
Quelle: TCPIP                      Protokolliert: 08.06.2017 18:57:01  
Ereignis-ID: 1332                      Aufgabenkategorie: (1073)  
Ebene: Informationen                      Schlüsselwörter: (4294967296)  
Benutzer: Nicht zutreffend                      Computer: Worker  
Vorgangscod: Info  
Weitere Informationen: [Onlinehilfe](#)

Verlauf:

The screenshot shows the Windows Event Viewer interface. The left pane shows the navigation tree with 'NetEventTrace1' selected. The main pane displays a list of events under 'NetEventTrace1' with 9,508 total events. The selected event is ID 1046, categorized as 'Informationen' and 'TCPIP', occurring on 08.06.2017 at 18:57:01. The details pane shows the following information:

TCPIP: Die Verbindung 0xffffd00c3910cc0 [local=172.18.32.1053554 remote=103.10.4.40:21] wird beendet: Zeitüberschreitung bei der Neuübertragung.

Protokollname:  
Quelle: TCPIP                      Protokolliert: 08.06.2017 18:57:01  
Ereignis-ID: 1046                      Aufgabenkategorie: (1046)  
Ebene: Informationen                      Schlüsselwörter: (68719476736),(1024),(128),(4)  
Benutzer: Nicht zutreffend                      Computer: Worker  
Vorgangscod: Info  
Weitere Informationen: [Onlinehilfe](#)

# Windows - Netzwerkaufzeichnung Powershell

The screenshot shows the Windows Event Viewer interface. The left pane displays the event log hierarchy: Ereignisanzeige (Lokal) > Benutzerdefinierte Ansichten > Windows-Protokolle > Anwendungs- und Dienstprotokolle > Gespeicherte Protokolle > DerWindowsPapst > NetEventTrace1. The main pane shows a table of events for 'NetEventTrace1' with 9,508 events. The selected event is 'Informationen' (ID 1300) from 'TCP/IP' at '08.06.2017 18:56:27'. The details pane shows the event message: 'TCP: Die Verbindung 0xffffad00c319d540 (local=172.18.32.10:53523 remote=172.18.32.1:49000) ist vorhanden. Status = TimeWaitState. PID = 0.' Below the message, the event properties are listed: Protokollname: TCP/IP, Quelle: TCP/IP, Ereignis-ID: 1300, Ebene: Informationen, Benutzer: Nicht zutreffend, Vorgangscodename: Info, and weitere Informationen: [Onlinehilfe](#).

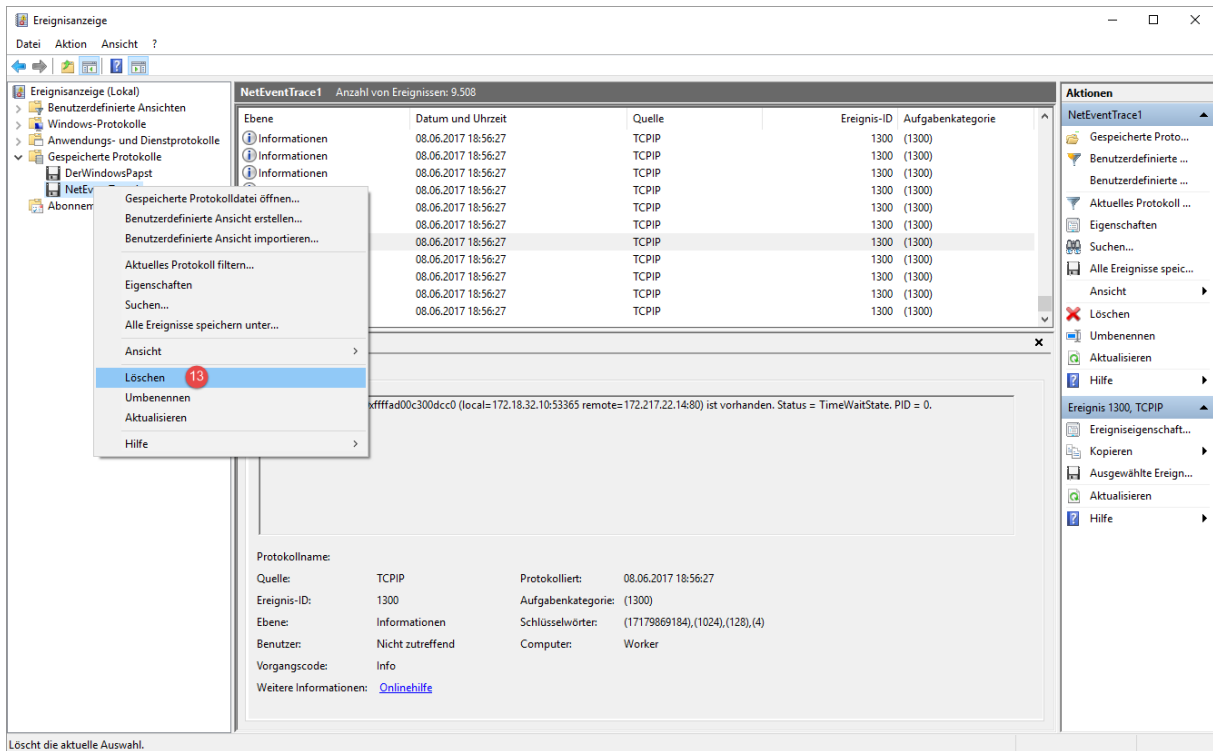
Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	

The screenshot shows the Windows Event Viewer interface. The left pane displays the event log hierarchy: Ereignisanzeige (Lokal) > Benutzerdefinierte Ansichten > Windows-Protokolle > Anwendungs- und Dienstprotokolle > Gespeicherte Protokolle > DerWindowsPapst > NetEventTrace1. The main pane shows a table of events for 'NetEventTrace1' with 9,508 events. The selected event is 'Informationen' (ID 1300) from 'TCP/IP' at '08.06.2017 18:56:27'. The details pane shows the event message: 'TCP: Die Verbindung 0xffffad00c300dccc (local=172.18.32.10:53365 remote=172.217.22.14:80) ist vorhanden. Status = TimeWaitState. PID = 0.' Below the message, the event properties are listed: Protokollname: TCP/IP, Quelle: TCP/IP, Ereignis-ID: 1300, Ebene: Informationen, Benutzer: Nicht zutreffend, Vorgangscodename: Info, and weitere Informationen: [Onlinehilfe](#).

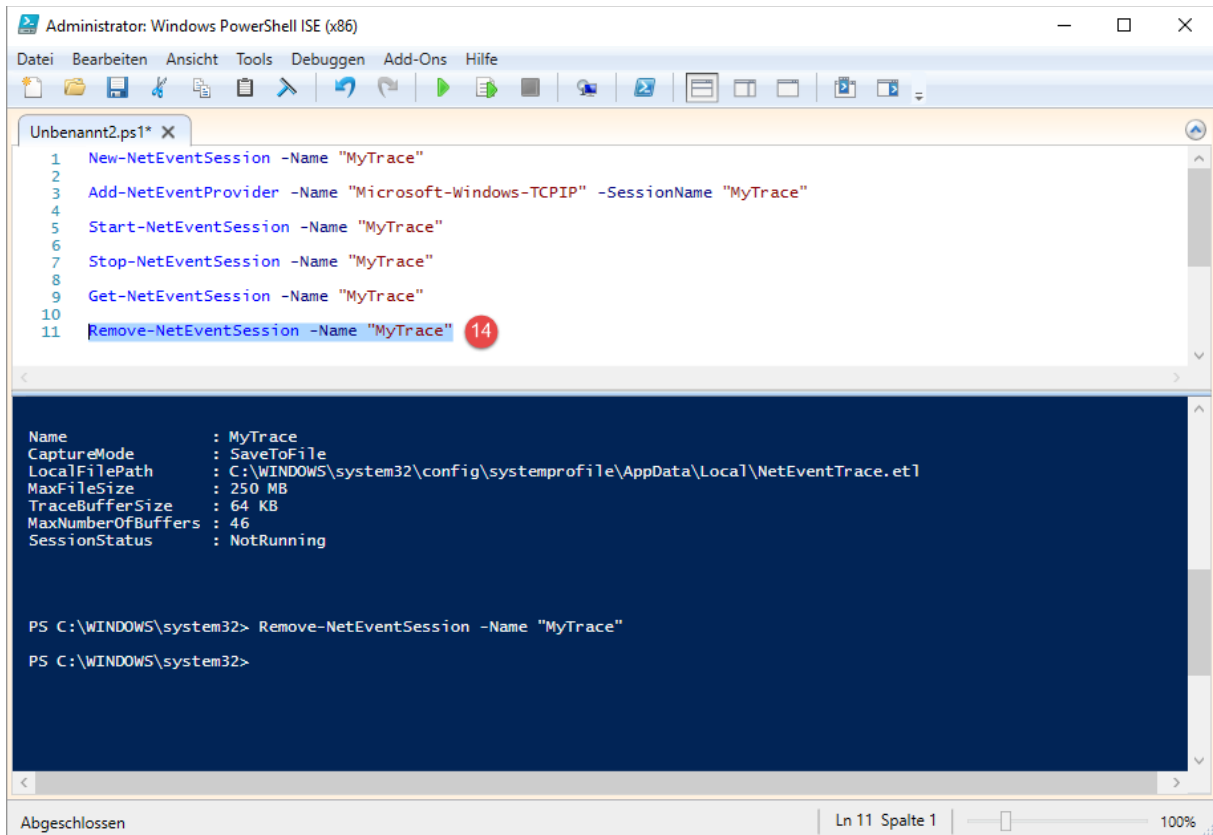
Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	
Informationen	08.06.2017 18:56:27	TCP/IP	1300 (1300)	

# Windows - Netzwerkaufzeichnung Powershell

Zum Schluss löschen wir das Protokoll.



Entfernen die Session.





# Windows - Netzwerkaufzeichnung Powershell

## Powershell:

New-NetEventSession -Name "MyTrace"

Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName "MyTrace"

Start-NetEventSession -Name "MyTrace"

Stop-NetEventSession -Name "MyTrace"

Get-NetEventSession -Name "MyTrace"

Remove-NetEventSession -Name "MyTrace"

## \*Nach der Konvertierung:

