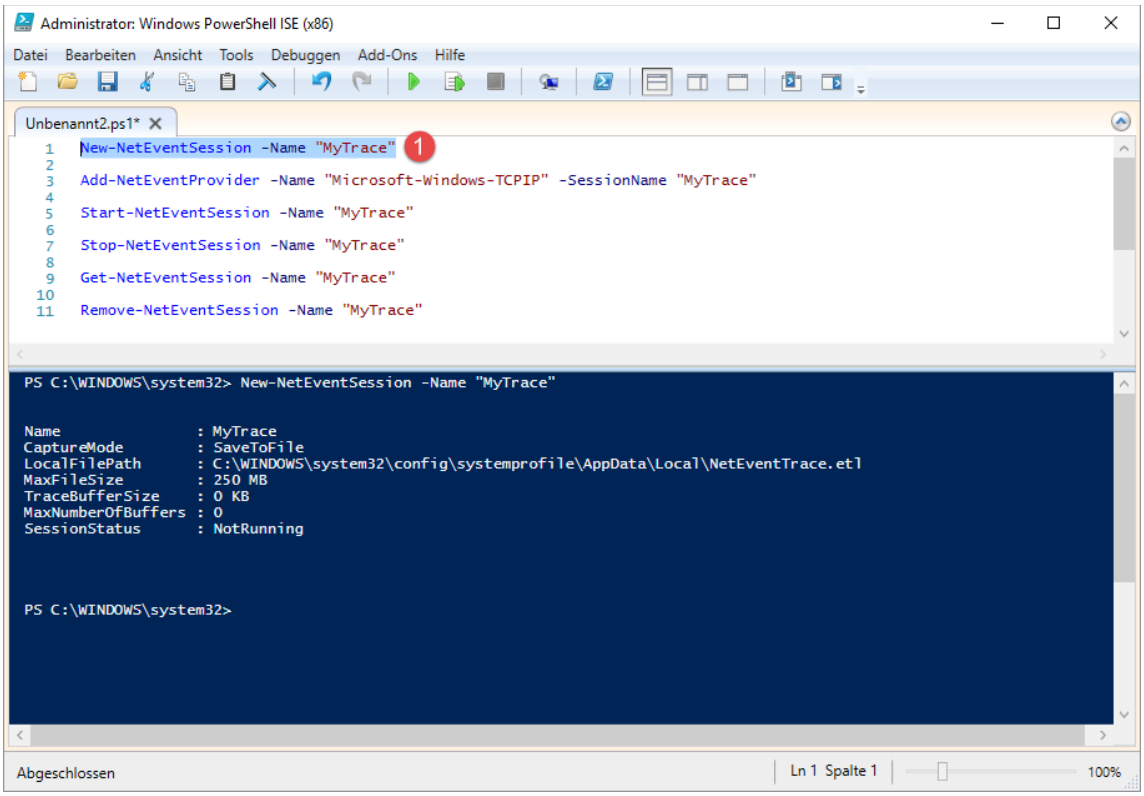
Windows - Netzwerkaufzeichnung Powershell

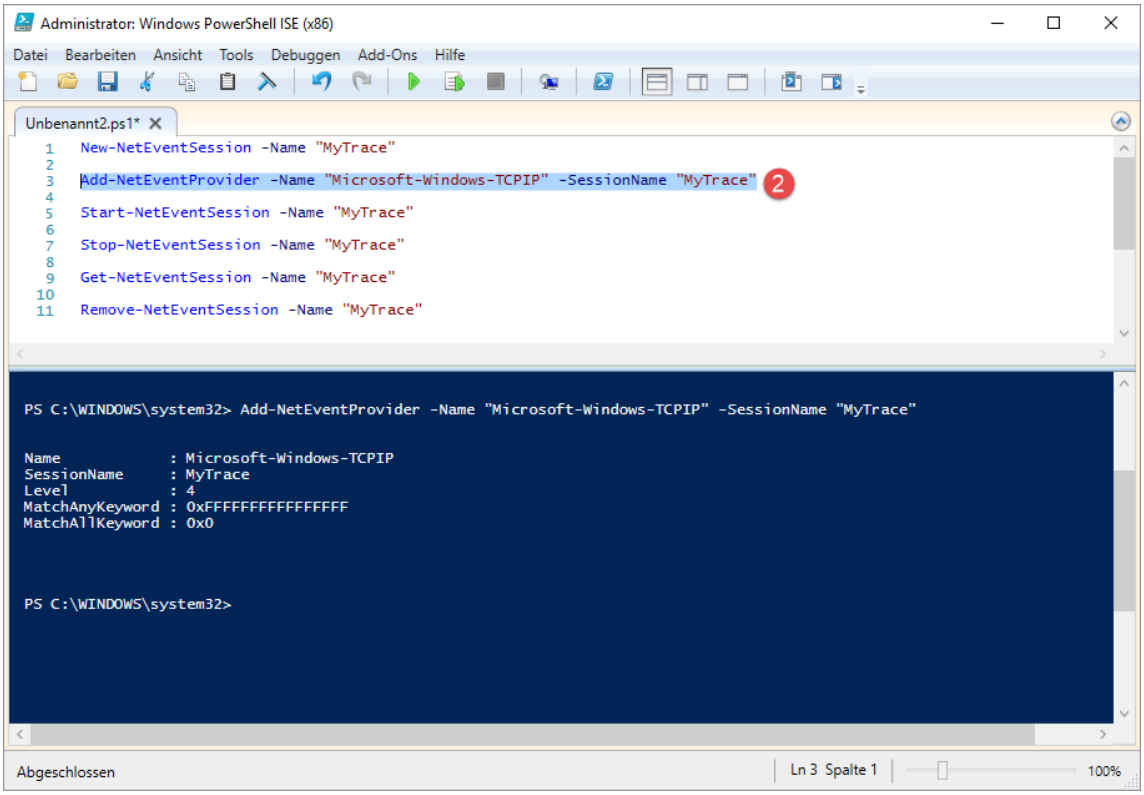
Wer kein Wireshark oder Microsoft Network Analyzer hat kann die Powershell zu Hilfe nehmen um den Netzwerkverkehr aufzuzeichnen und später zu analysieren.

Und so geht's:

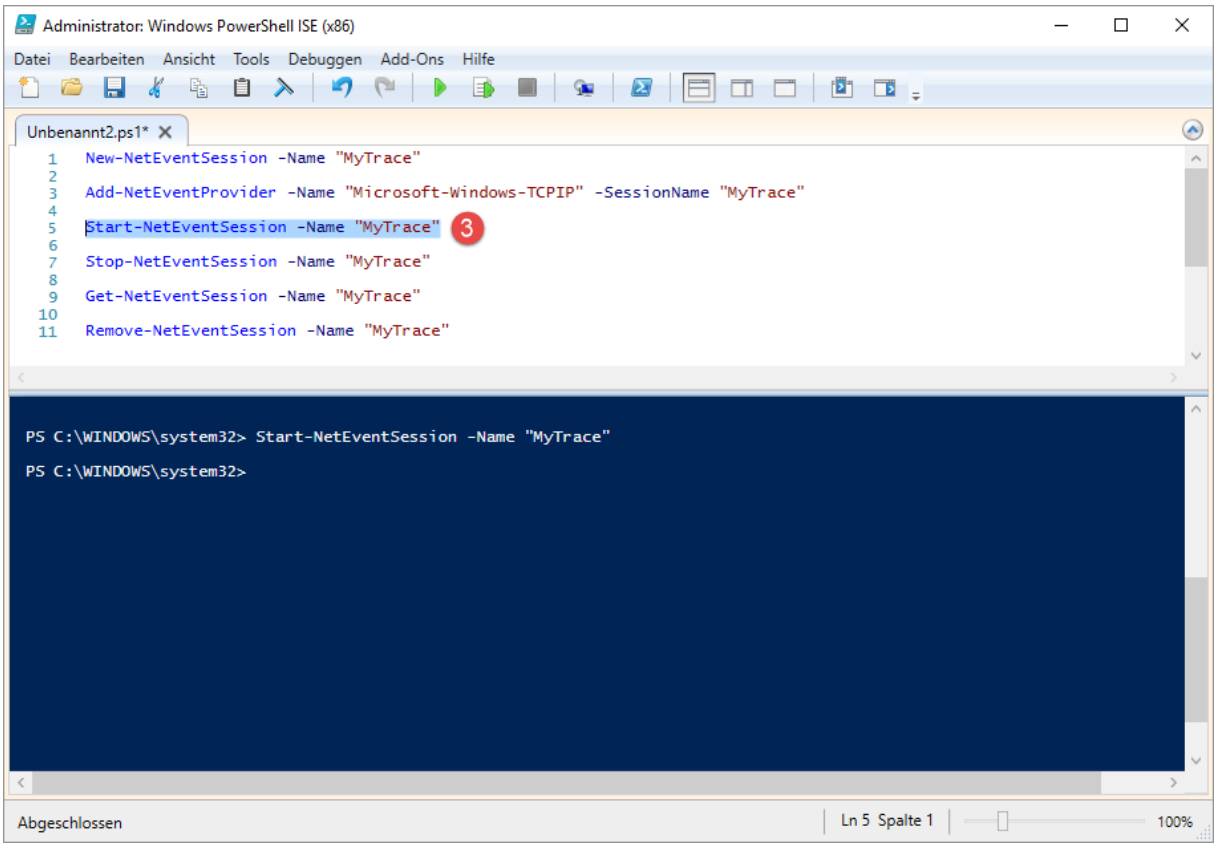
Als erstes erstellen wir ein Event namens „MyTrace"



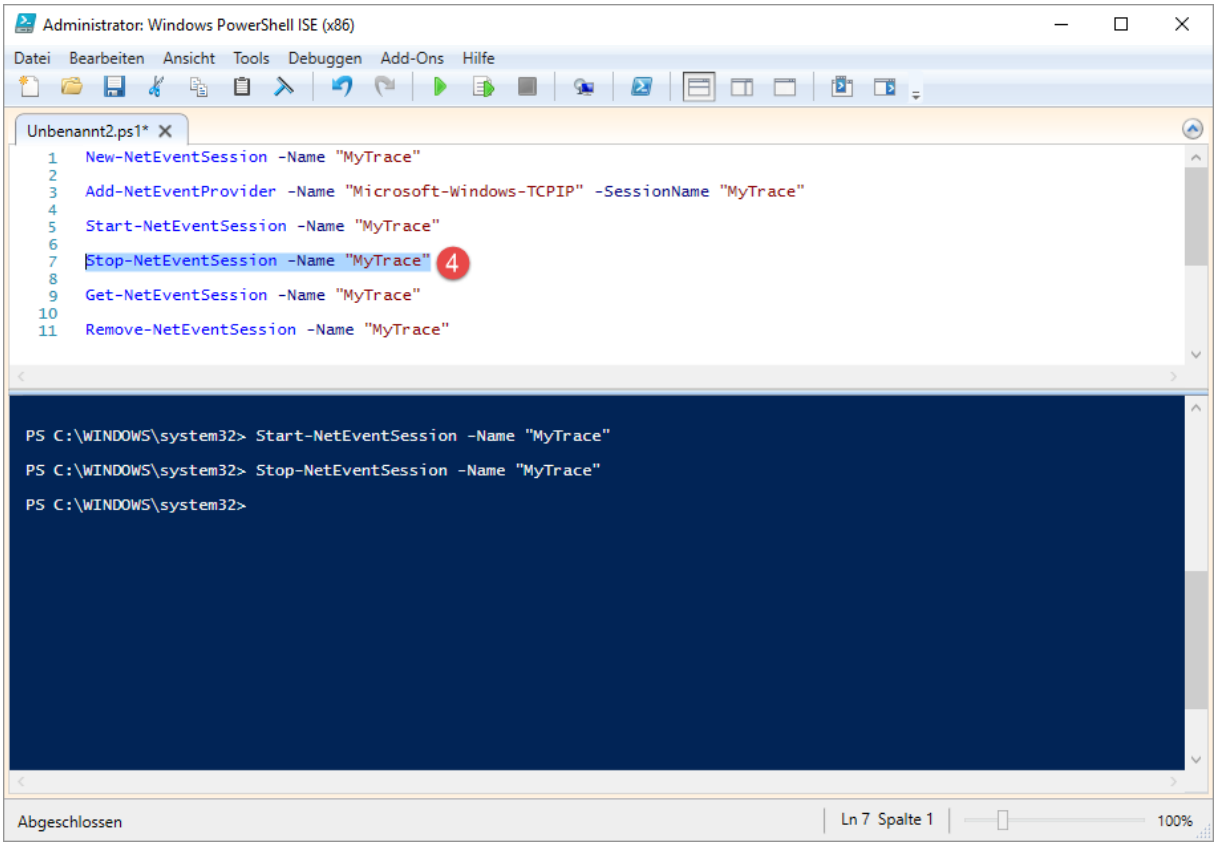
Danach definieren wir den zu überwachenden Provider.



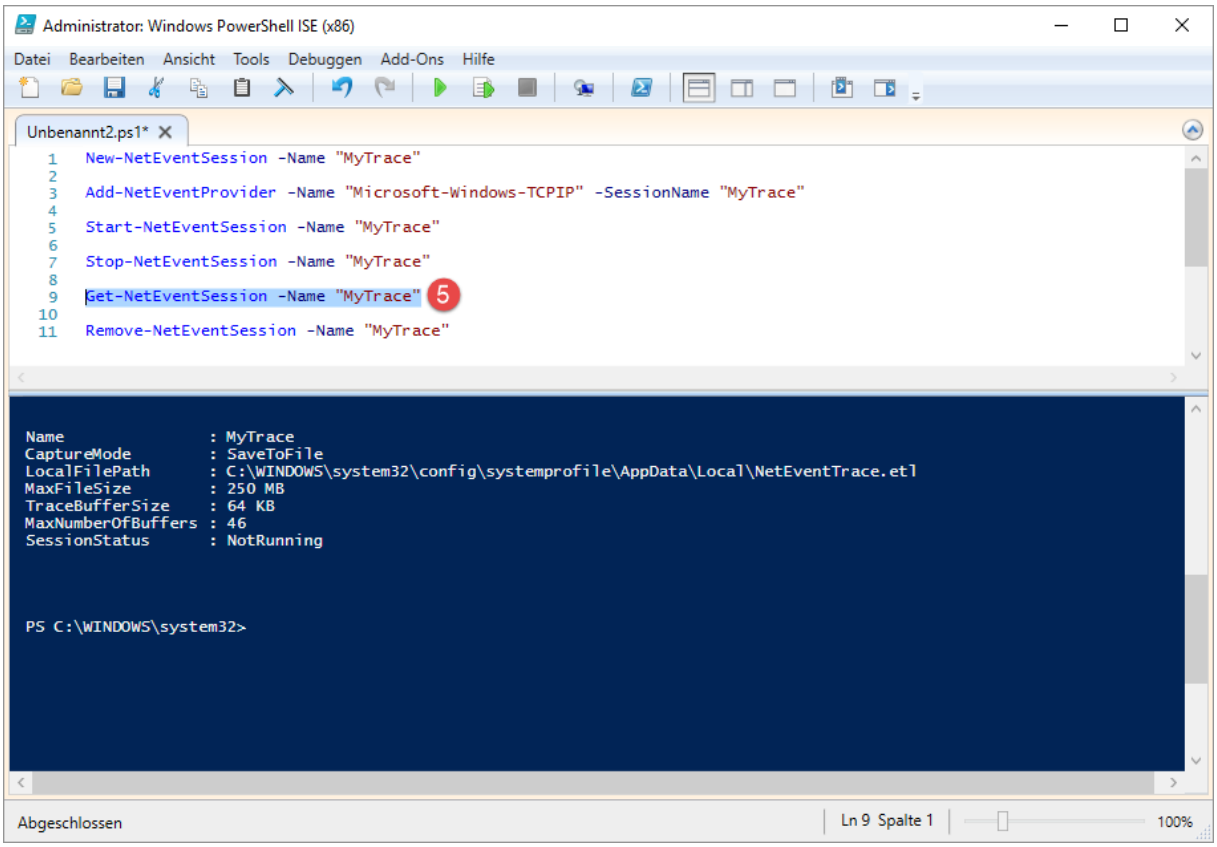
Starten den Trace.



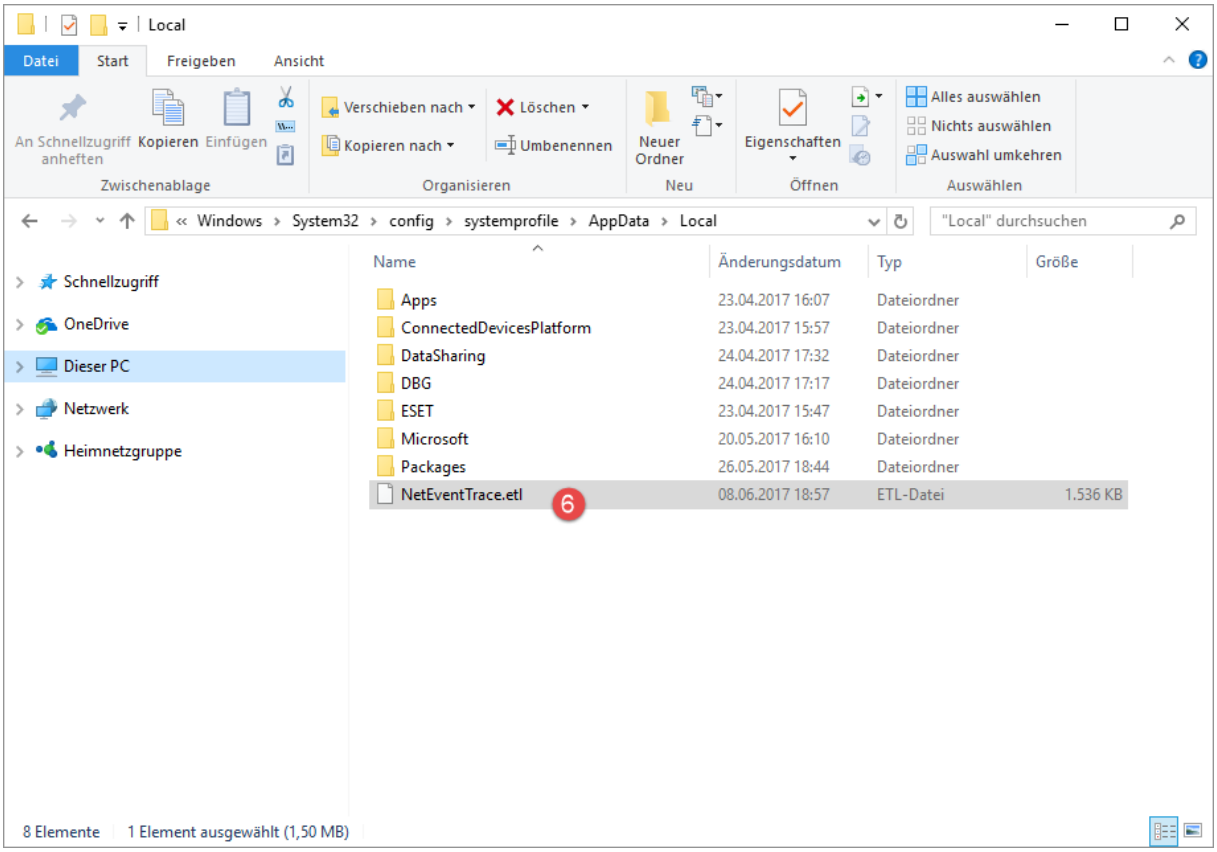
Surfen etwas oder oder oder und stoppen den Trace.



Lassen und die Protokolldatei anzeigen.

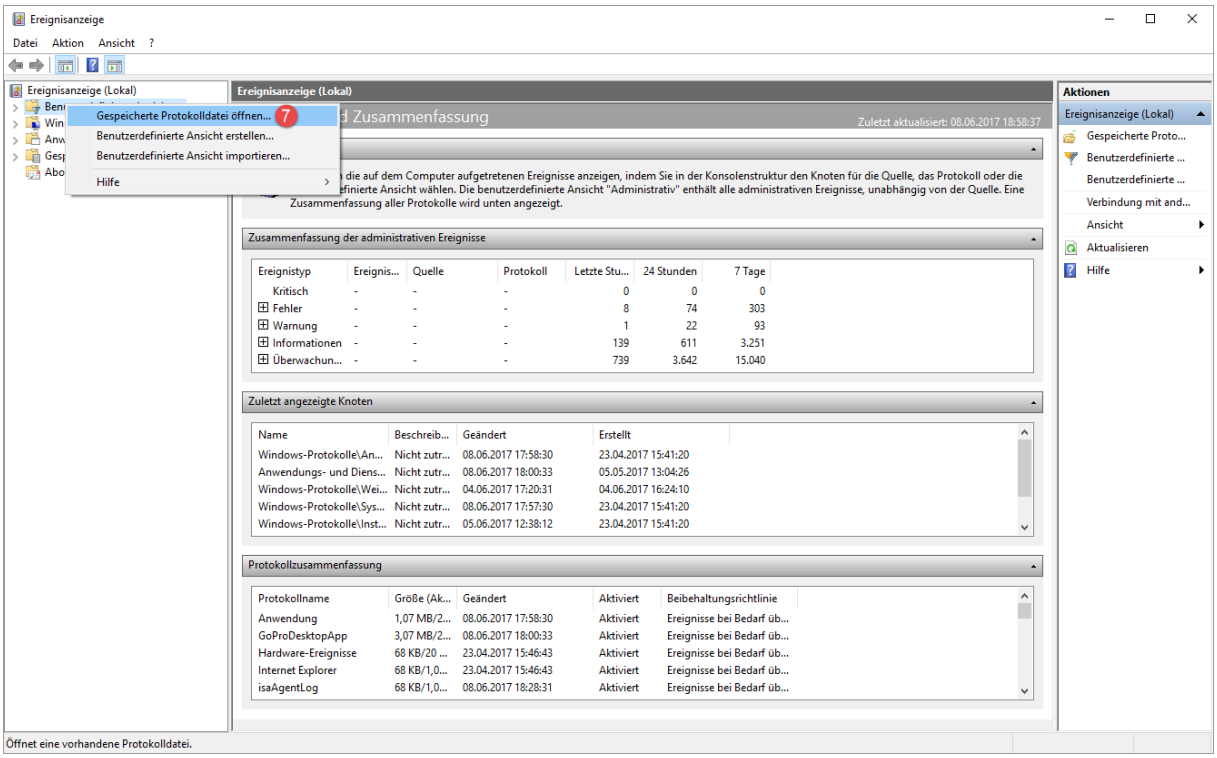


Öffnen den Pfad.

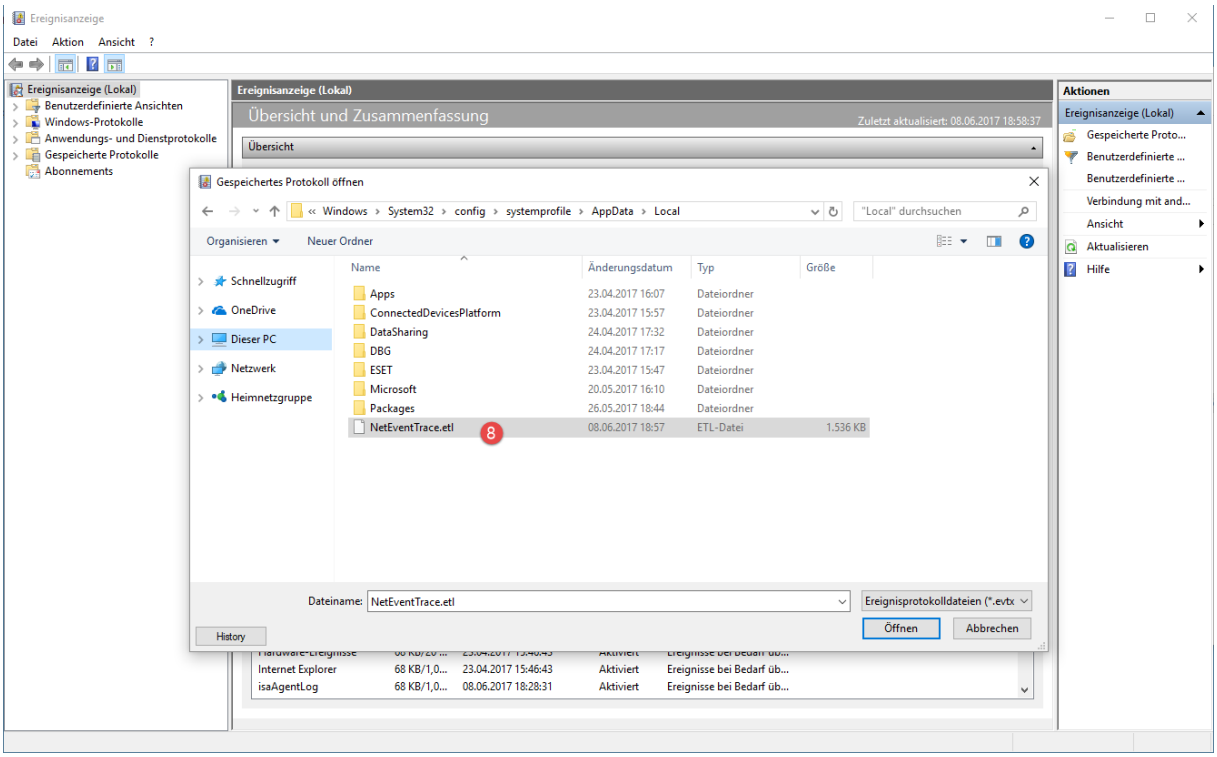


Windows - Netzwerkaufzeichnung Powershell

Starten die Ereignisanzeige und öffnen die Protokolldatei.

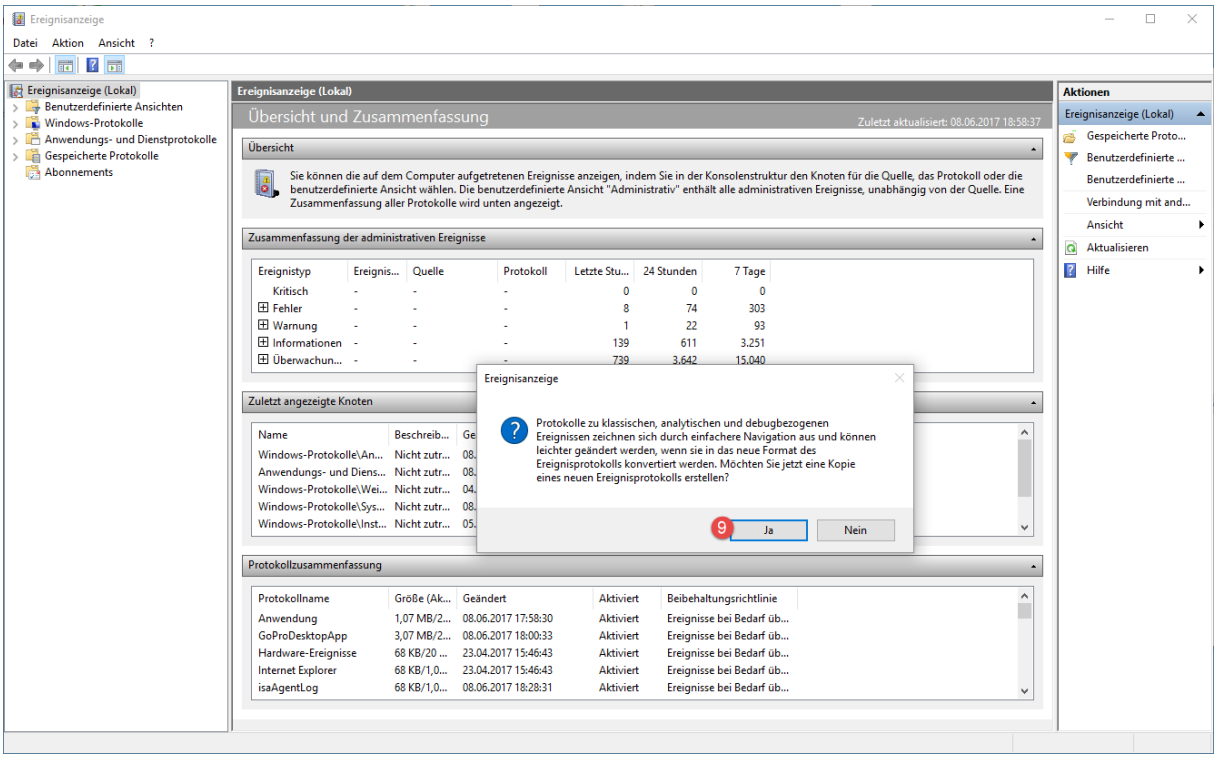


Navigieren zum obigen Pfad und wählen die .etl Datei aus.

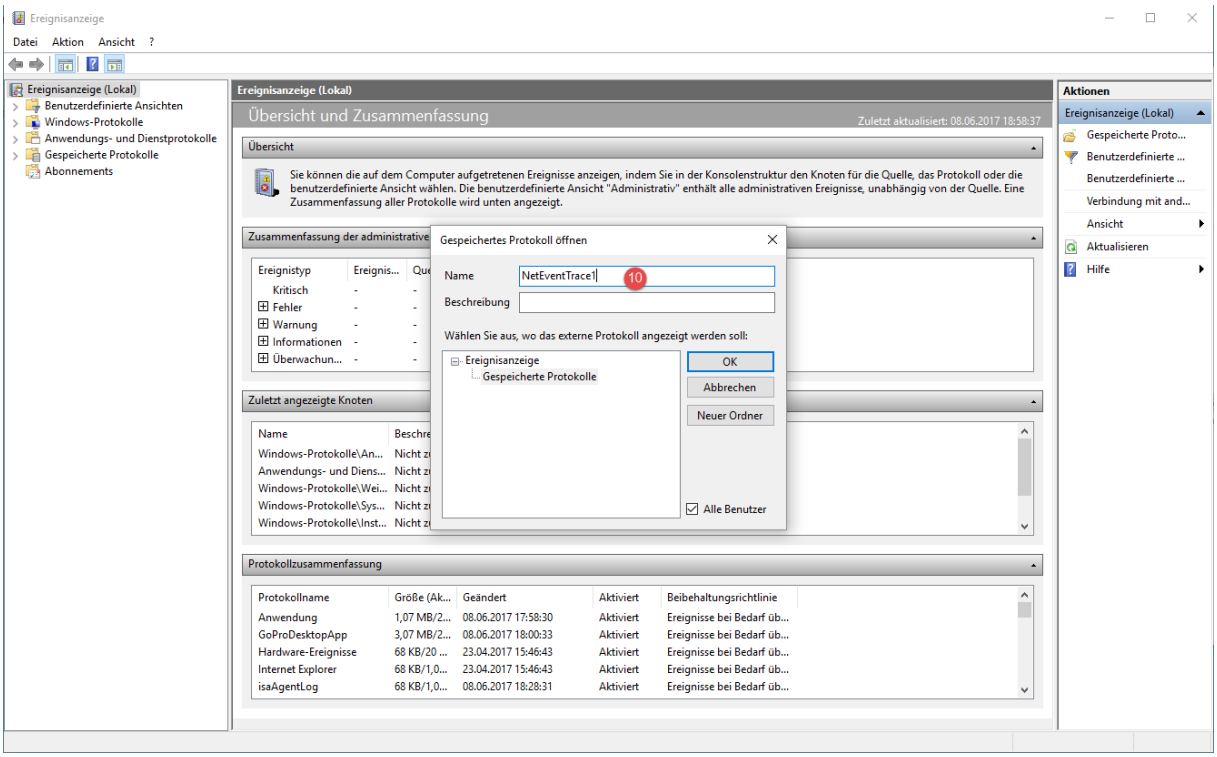


Windows - Netzwerkaufzeichnung Powershell

Konvertieren das Format *.

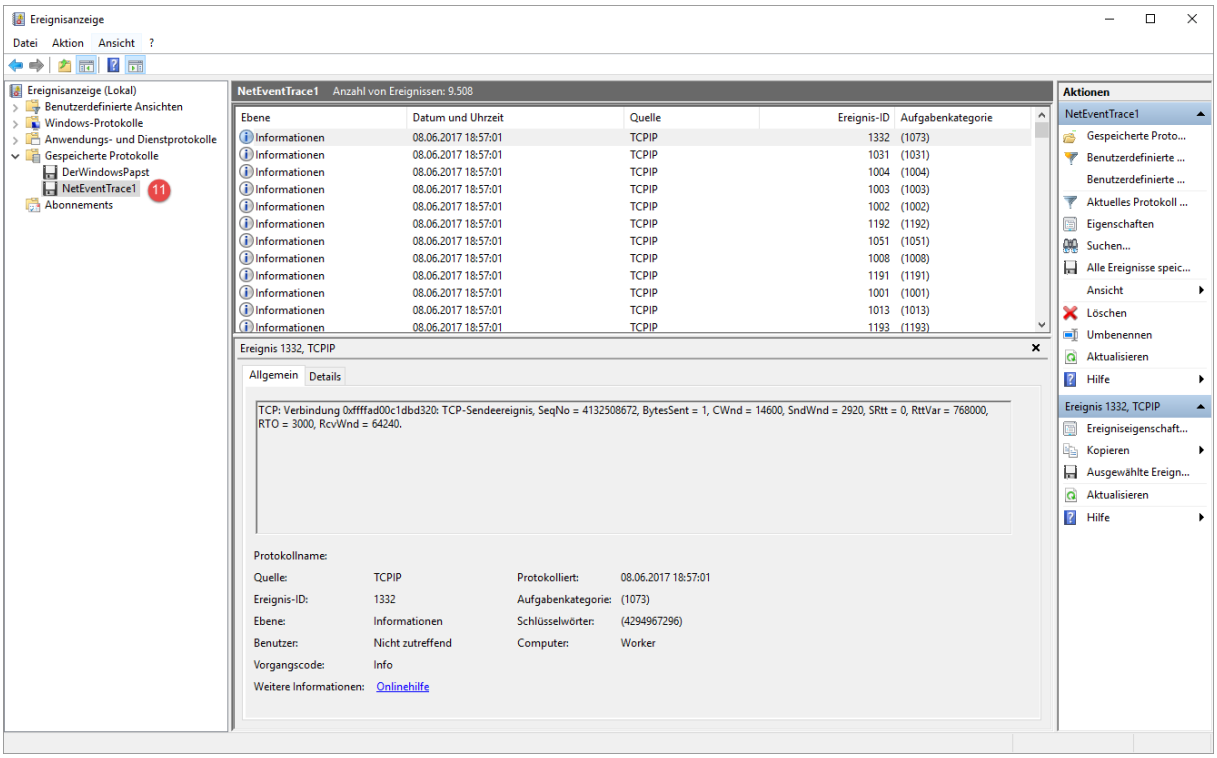


Geben dem zu öffnenden Protokoll einen Namen.

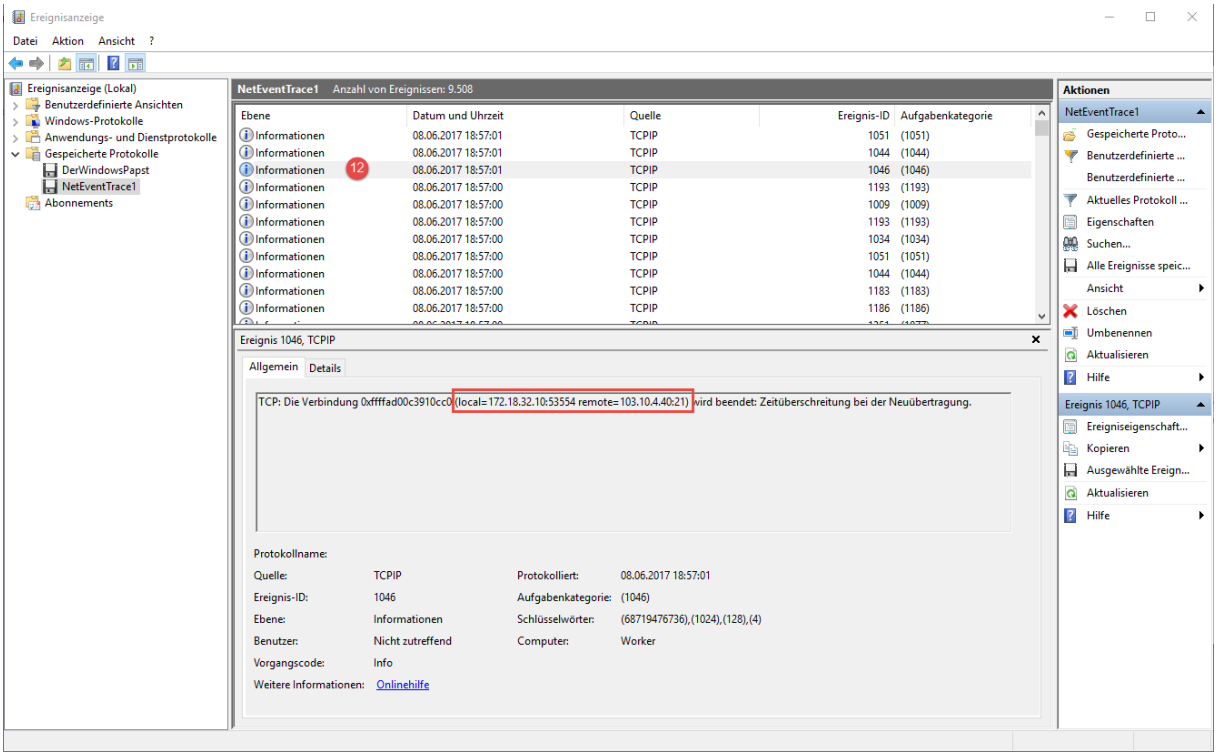


Windows - Netzwerkaufzeichnung Powershell

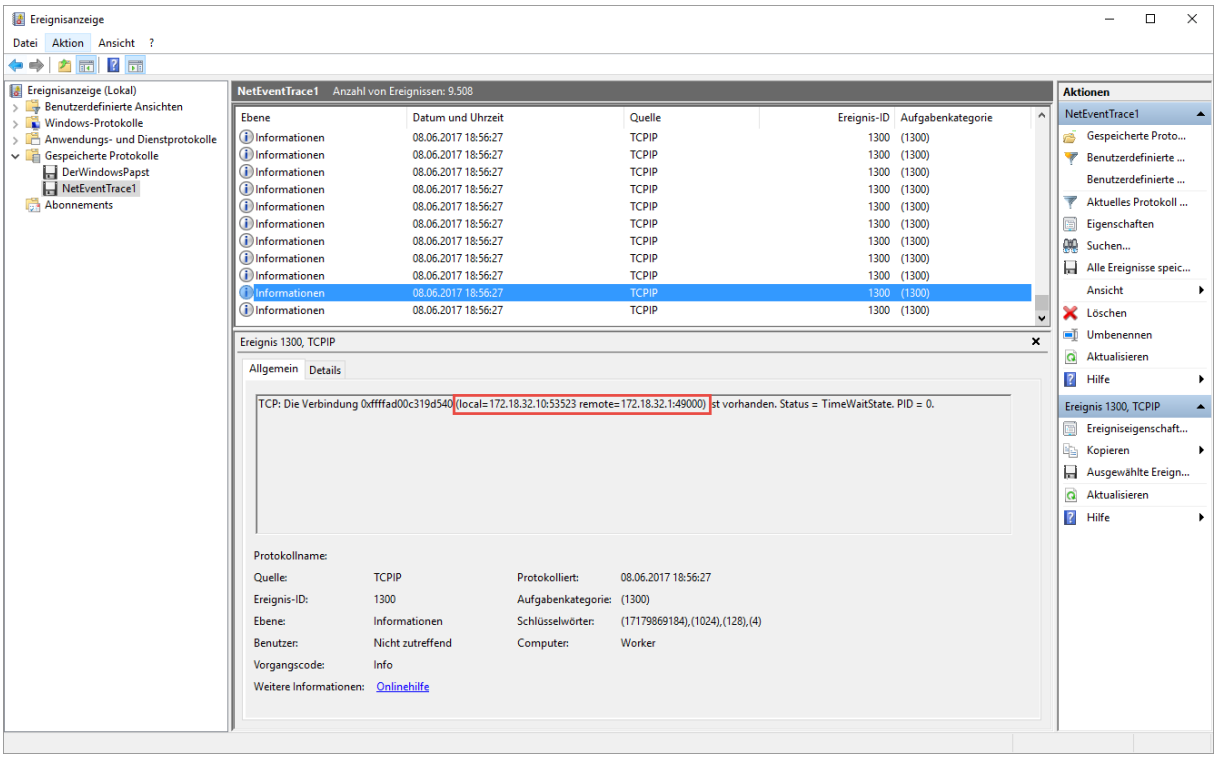
Navigieren nun in den Ereignissen und fangen an zu analysieren.

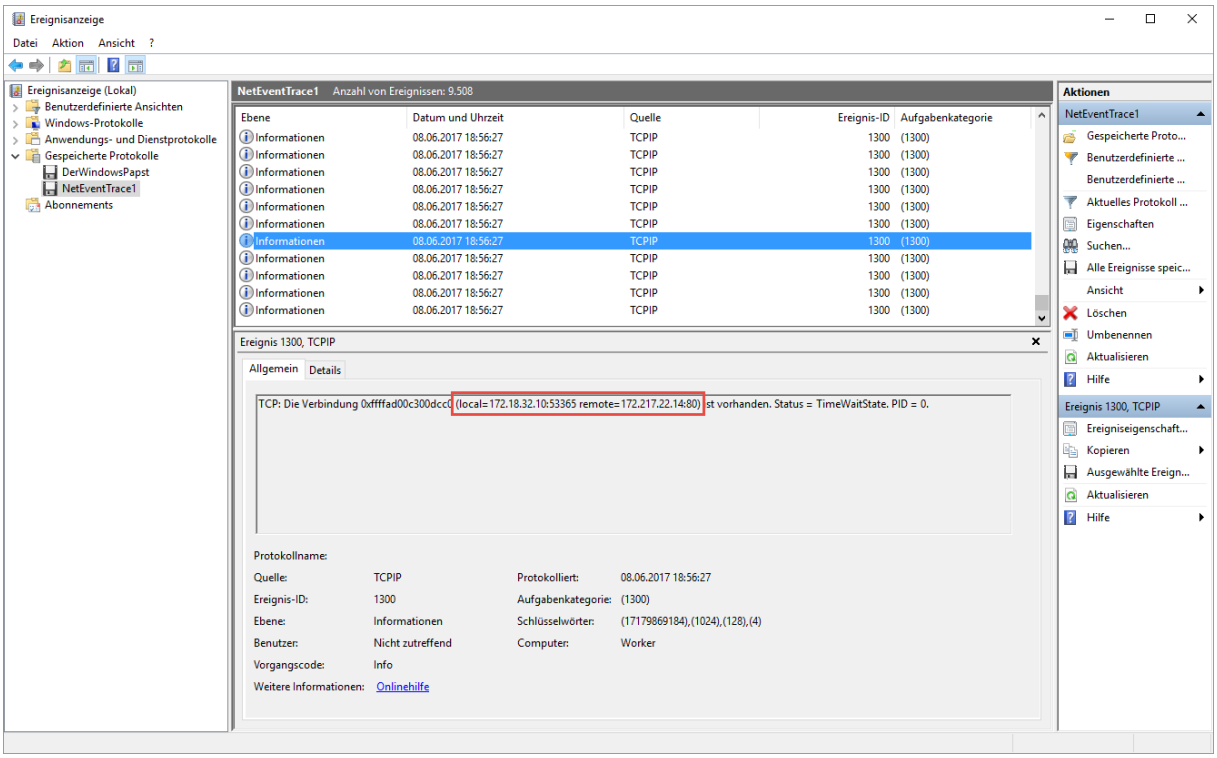


Verlauf:



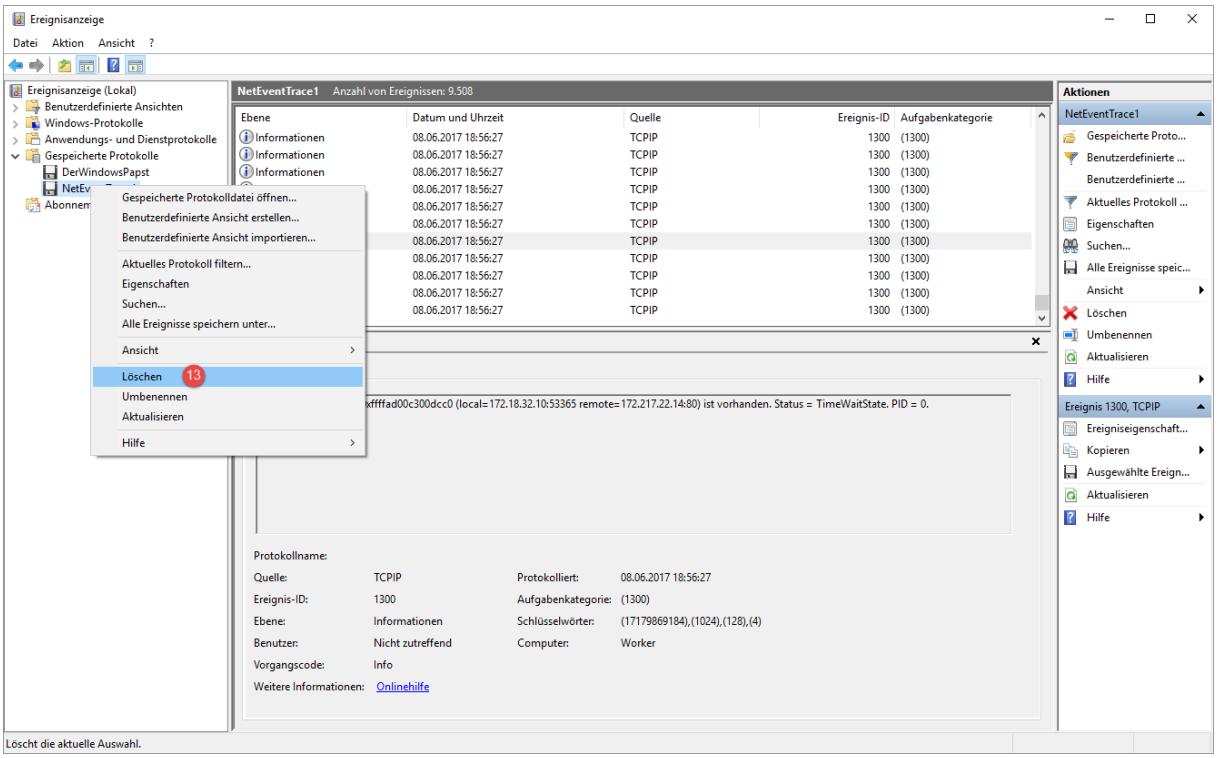
Windows - Netzwerkaufzeichnung Powershell



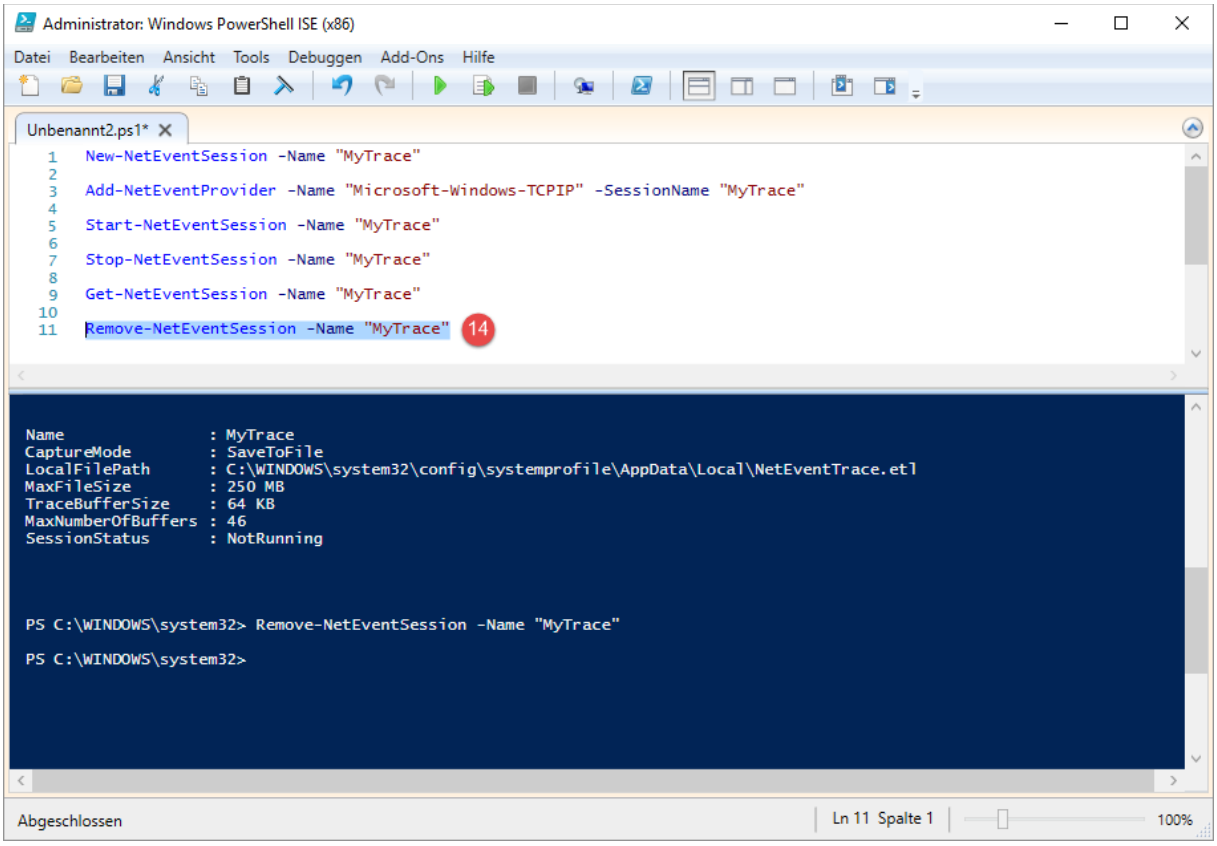


Erstellt von Jörn Walter www.der-windows-papst.de – 08.06.2017

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:**