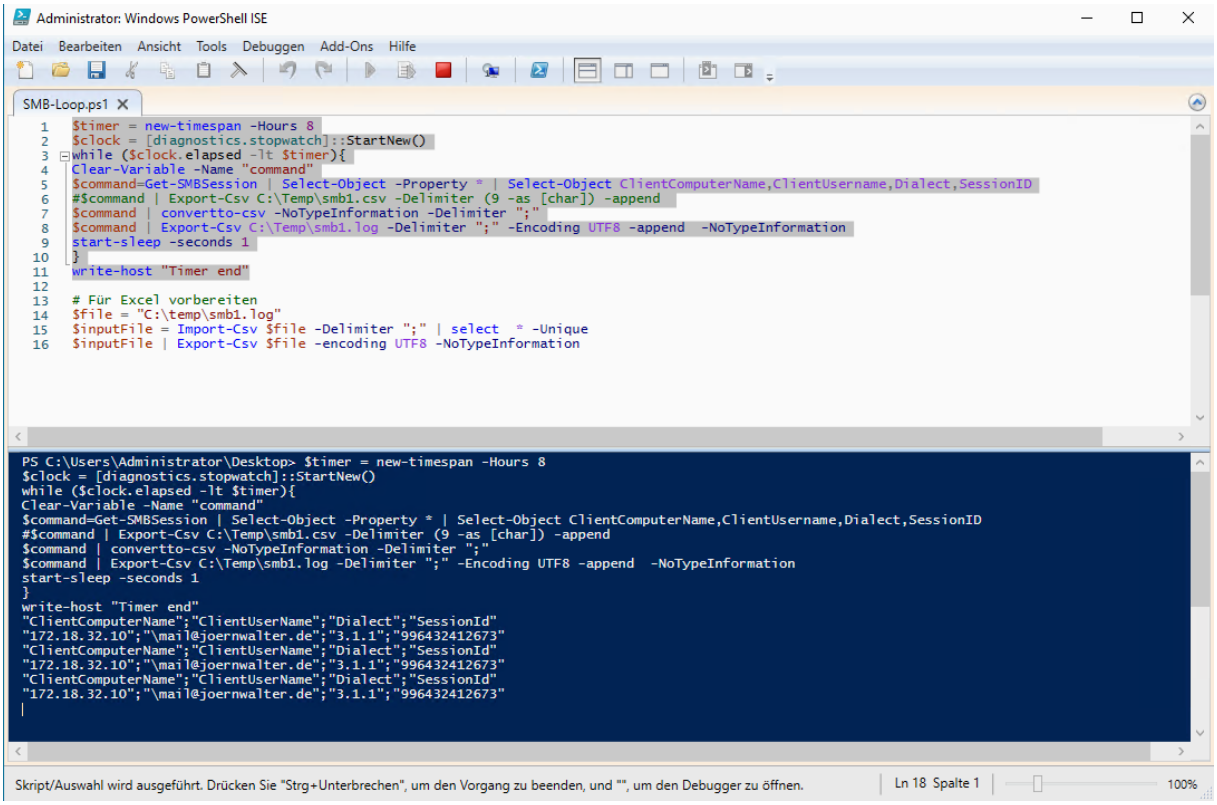
SMBv1 - Monitoring

Mit diesem Skript loggen wir für eine definierte Zeit den Zugriff via SMB-Protokoll.

Nachdem das Skript gestartet wurde, sperrt man einfach den Bildschirm.

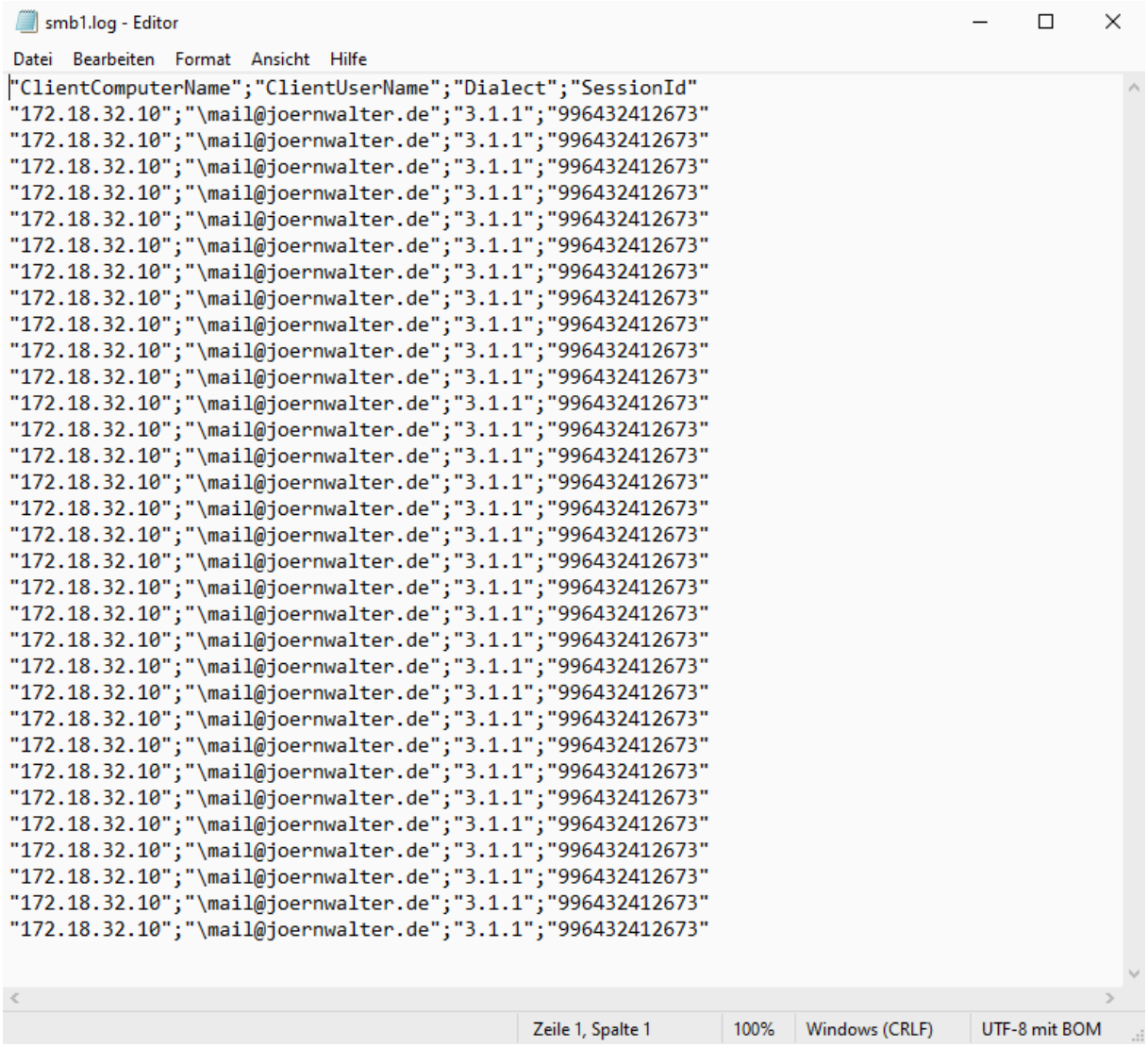



```
$timer = new-timespan -Hours 8
$clock = [diagnostics.stopwatch]::StartNew()
while ($clock.elapsed -lt $timer){
Clear-Variable -Name "command"
$command=Get-SMBSession | Select-Object -Property * | Select-Object
ClientComputerName,ClientUsername,Dialect,SessionID
#$command | Export-Csv C:\Temp\smb1.csv -Delimiter (9 -as [char]) -append
$command | convertto-csv -NoTypeInformation -Delimiter ";"
$command | Export-Csv C:\Temp\smb1.log -Delimiter ";" -Encoding UTF8 -append  -
NoTypeInformation
start-sleep -seconds 1
}
write-host "Timer end"
```

Erstellt von Jörn Walter **17.05.2021**

Das Ergebnis mit welcher Protokollversion der Zugriff stattfand ist ausschlaggebend für die Deaktivierung bzw. der weiteren Prüfung.

Das Log sagt aus, das der Zugriff nur mit der SMB-Protokollversion 3.11 stattfand.

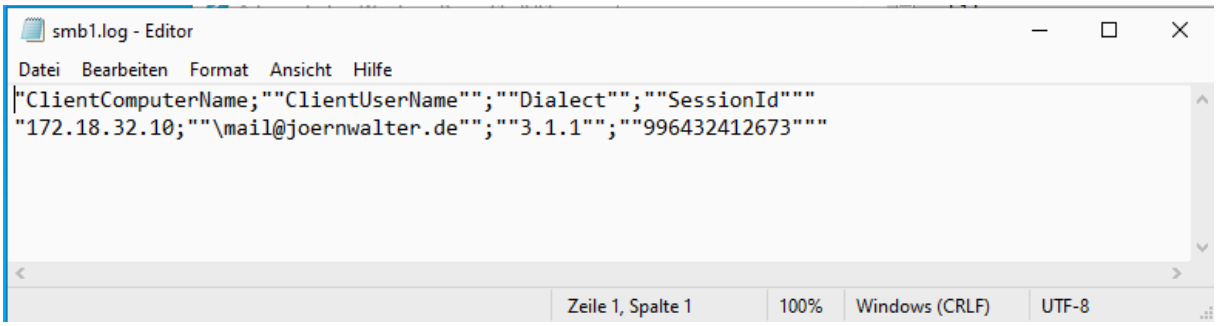


Somit kann SMBv1 ohne Sorge deaktiviert bzw. deinstalliert werden.

SMBv1 - Monitoring

Die Ausgabe für Excel etwas verschönern. Doppelte Einträge werden entfernt und alles schön mit Semikolon getrennt.

```
# Für Excel vorbereiten
$file = "C:\temp\smb1.log"
$inputFile = Import-Csv $file -Delimiter ";" | select  * -Unique
$inputFile | Export-Csv $file -encoding UTF8 -NoTypeInformation
```



https://www.der-windows-papst.de/2021/05/27/smb-dialect-revision-konfigurieren/