Windows OpenFiles

Mit dem CMD Tool openfiles ermitteln wir die zurzeit geöffneten (in Benutzung) Ordner und Dateien und trennen diese auch bei Bedarf wieder. Das Tool kann auch zur Analyse eingesetzt werden, um herauszufinden, welcher Prozess eine Datei gerade sperrt.

Damit wir die geöffneten Ordner und Dateien angezeigt bekommen, müssen wir zuerst das maintain objects list Systemflag aktivieren.

openfiles /local on

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.17763.195]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>openfiles /local on

ERFOLG: Das globale Systemkennzeichen "maintain objects list" ist aktiviert.
        Diese Änderung wird nach einem Neustart wirksam.

C:\WINDOWS\system32>
```

Gefolgt von einem Neustart des Systems.

Mit diesem Befehl exportieren wir alle geöffneten Dateien in eine .txt Datei und legen diese auf den Desktop ab.

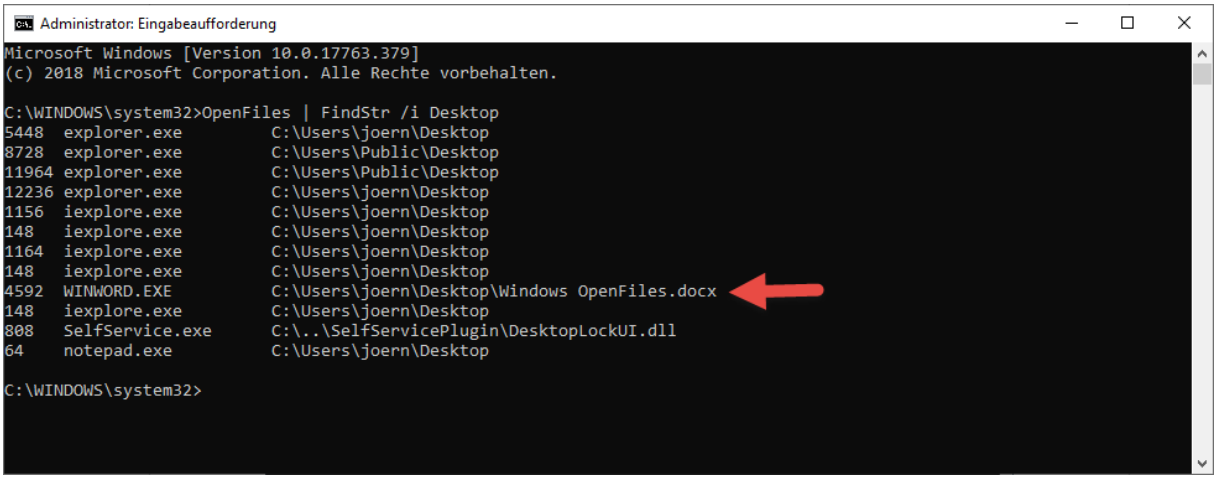
openfiles > %userprofile%\desktop\files.txt

```
files.txt - Editor
Datei  Bearbeiten  Format  Ansicht  Hilfe

Lokal ge"ffnete Dateien:
---------------------

Kennu Prozessname          Open File (Pfad\ausfhrbare Datei)
===== ==================== ================================================
64    schedhlp.exe         C:\Windows
136   schedhlp.exe         C:\Windows\SysWOW64
712   schedhlp.exe         C:\..-4F28-AB89-52829BDDDEC1-S-1-5-5-0-277461.log
720   schedhlp.exe         C:\..\Common Files\Acronis\Schedule2\schedhlp.exe
756   schedhlp.exe         C:\..\Windows\System32\de-DE\user32.dll.mui
64    sihost.exe           C:\Windows\System32
1808  sihost.exe           C:\..\Windows\System32\de-DE\KernelBase.dll.mui
72    svchost.exe          C:\Windows\System32
312   svchost.exe          C:\..\Windows\System32\de-DE\svchost.exe.mui
1012  svchost.exe          C:\..\31b4e2385bc4734b\ActivitiesCache.db
1016  svchost.exe          C:\..\31b4e2385bc4734b\ActivitiesCache.db-wal
1020  svchost.exe          C:\..\31b4e2385bc4734b\ActivitiesCache.db-shm
1064  svchost.exe          C:\..\Windows\System32\de-DE\crypt32.dll.mui
1272  svchost.exe          C:\..\Windows\System32\de-DE\winnlsres.dll.mui
1356  svchost.exe          C:\..\Windows\System32\de-DE\mswsock.dll.mui
72    svchost.exe          C:\Windows\System32
300   svchost.exe          C:\..\Windows\System32\de-DE\svchost.exe.mui
816   svchost.exe          C:\..\Windows\Notifications\wpndatabase.db
820   svchost.exe          C:\..\Windows\Notifications\wpndatabase.db-wal
824   svchost.exe          C:\..\Windows\Notifications\wpndatabase.db-shm
Windows (CRLF)   Zeile 1, Spalte 1   100%
```

Windows OpenFiles

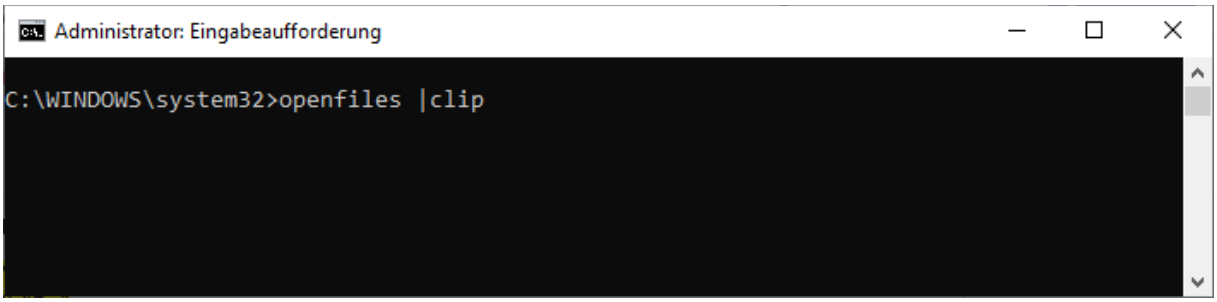
Dieser Befehl zeigt uns die geöffneten Ordner und Dateien an die das Wort „Desktop“ inne haben:

OpenFiles | FindStr /i Desktop
OpenFiles | FindStr /i "D:"



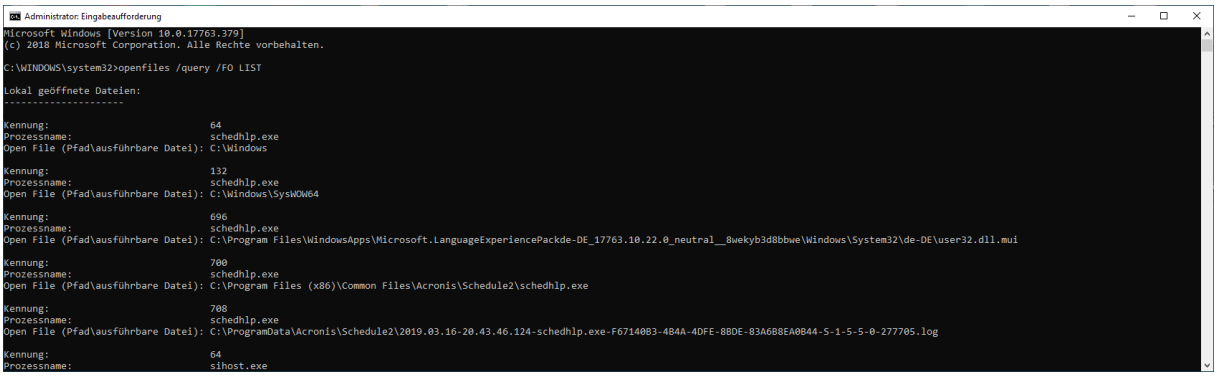
Dieser Befehl speichert die Ergebnisse in die Zwischenablage ab:

openfiles |clip



Dieser Befehl zeigt die Ergebnisse in Listenansicht an:

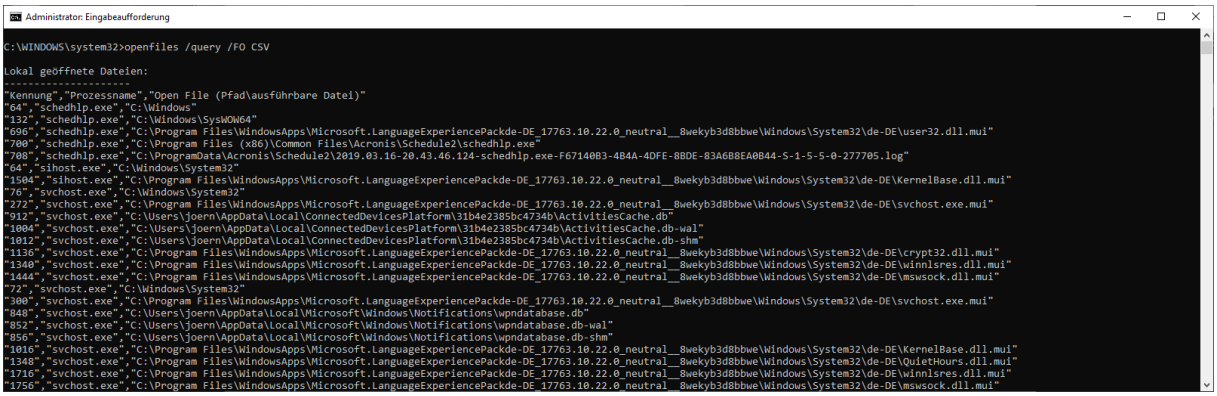
openfiles /query /FO LIST



Windows OpenFiles

Dieser Befehl zeigt die Ergebnisse in einer Tabellenansicht an:

openfiles /query /FO CSV



Dieser Befehl kopiert die Ergebnisse als Tabellenansicht in die Zwischenablage. Danach einfach kommagetrennt in Excel importieren:

openfiles /query /FO CSV|CLIP

Mit diesem Befehl trennen wir eine Datei, entweder mithilfe der ID oder der Angabe des Benutzers:

- openfiles /disconnect /id 4592
- openfiles /disconnect /a Joern
- openfiles /disconnect /S Worker /U Joern /ID 5

ID = File-ID
A = in Benutzung durch
S = Remote System

Mit diesem Befehl setzen wir das maintain objects list Systemflag wieder zurück und schließen die CMD:

openfiles /local off