Spoor in 10 stappen de problemen op in Windows

Door: Redactie Computer!Totaal

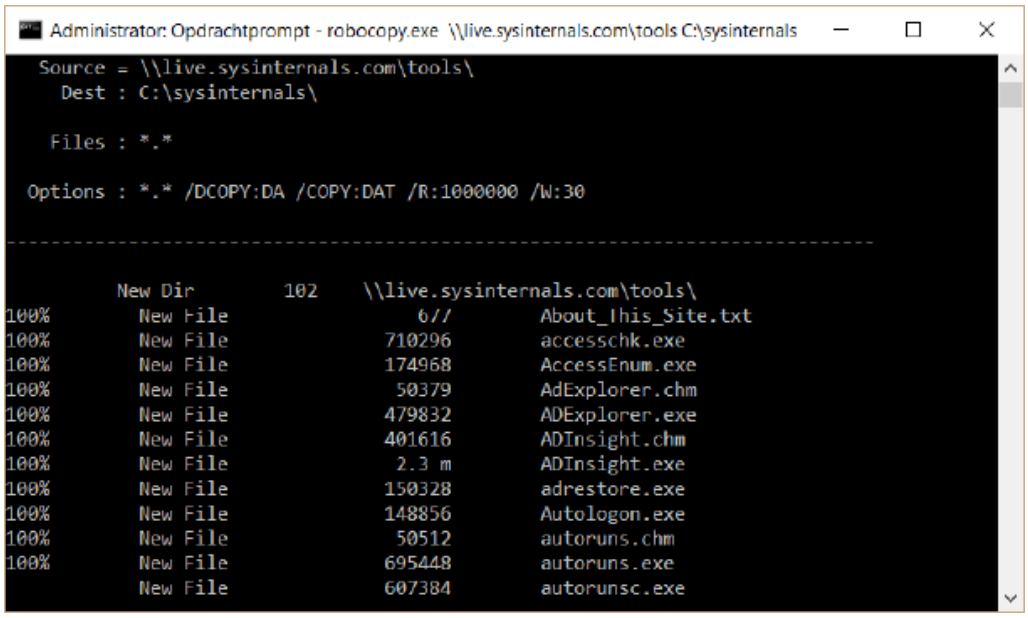
Vroeg of laat kom je op zijn minst wel een keer problemen tegen in Windows. Een registersleutel die verkeerd staat, een proces dat niet wil stoppen, malware die maar mee blijft opstarten of je hebt even wat systeeminformatie nodig. De Sysinternals-tools bieden uitkomst.

In dit artikel gaan we enkele handige programma's bespreken van de Sysinternals-suite van Microsoft (zie ook www.sysinternals.com). Deze suite bevat tools die net even verder gaan dan de ingebouwde tools in Windows, waarmee het mogelijk wordt om veelvoorkomende problemen in Windows het hoofd te bieden, om malware te voorkomen en om inzicht te krijgen in je systeem. **Lees ook: Windows 10 terugzetten naar oude Windows-versie.**

01 Aan de slag met Sysinternals

Alle programma's in de suite van Sysinternals zijn portable, dat wil zeggen dat je ze dus niet hoeft te installeren. De tools in de suite die wij zullen gaan bespreken zijn Process Explorer, een veel krachtigere versie van Taakbeheer, Process Monitor dat de pc in de gaten kan houden, Autoruns, dat opstartitems kan beheren en BgInfo om systeeminformatie op hetbureaublad weer te geven.

De makers van Sysinternals willen de software zo eenvoudig mogelijk beschikbaar maken: daarom kun je via deze url de volledige collectie aan tooltjes in één keer downloaden als zipje van slechts 14,5 MB. Natuurlijk kun je ook de losse tools downloaden, als je dat liever wilt. Sysinternals heeft ook nog een alternatieve distributiemethode: een netwerkschijf die voor iedereen beschikbaar is met daarop alle Sysinternals-tools. Je opent deze netwerkschijf met een aantal commando's via de Opdrachtprompt. Open de Opdrachtprompt door met de rechtermuisknop op het startmenu te klikken (in Windows 8 en 10) en te kiezen voor**Opdrachtprompt (administrator)**. Voer het volgende commando in: **net start webclient** en druk op Enter, gevolgd door **robocopy.exe \\live.sysinternals.com\tools C:\sysinternals**. De bestanden worden nu gekopieerd en automatisch in betreffende map geplaatst. Typ ten slotte **net stop webclient** gevolgd door Enter om de verbinding weer te verbreken. Als je nu naar de map C:\sysinternals gaat, zie je daar alle Sysinternals-tools.

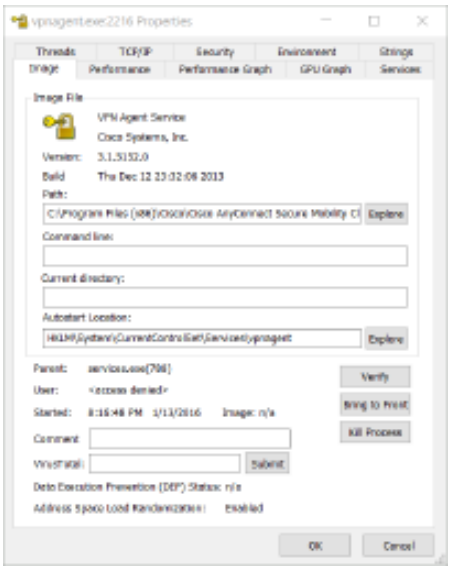


01 Alle tools in de Sysinternals-suite worden binnengehaald en in de map C:\sysinternals geplaatst.

02 Process Explorer openen

We beginnen met Process Explorer, een geavanceerder soort Taakbeheer dan die in Windows. Je opent Process Explorer door in de map C:\sysinternals het bestand procexp.exe te openen. Doe dat wel even met administratorrechten, door er met de rechtermuisknop op te klikken en te kiezen voor **Als administrator uitvoeren**. Klik na het openen op **Agree** om akkoord te gaan met de licentievoorwaarden.

Op het hoofdscherm zie je direct al behoorlijk wat informatie. Links staan alle processen in een 'boomweergave'. In deze weergave is het eenvoudig in te zien welke processen bij elkaar horen. Van elk proces zijn de volgende gegevens zichtbaar: **CPU**, **Private Bytes**,**Working Set**, **PID**, **Description** en **Company Name**. De kolom **CPU** duidt de hoeveelheid processorkracht aan die een proces verbruikt. **Private Bytes** geeft de hoeveelheid werkgeheugen aan die toegekend is aan een proces, en **Working Set** de hoeveelheid geheugen dat daadwerkelijk verbruikt wordt. De kolom **PID** tot slot toont de zogenoemde process identifier, een uniek nummer om een specifiek proces mee te identificeren. Het is mogelijk om Taakbeheer te vervangen met Process Explorer. Hiervoor klik je op **Options / Replace Task Manager**. Mocht je het originele Windows Taakbeheer weer terug willen hebben, dan selecteer je simpelweg dezelfde optie.



03 Op het Image-tabblad van een proces vind je veel extra informatie, zoals wanneer het gestart is, de mogelijkheid om het te verifiëren en de locatie waar gedefinieerd is om automatisch te starten (bij Autostart Location).

03 Process Explorer-interface

Als je met de rechtermuisknop op een proces klikt, verschijnt een aantal opties.
Met **Window** kun je indien van toepassing het venster dat bij het proces hoort naar voren brengen, door op **Bring to Front** te klikken. Met **Restart** kun je een proces opnieuw starten, en met **Search Online** wordt de browser geopend met een zoekopdracht naar de naam van het proces. Met de optie **Check VirusTotal** wordt het proces geüpload naar de VirusTotal-service. Als je deze optie kiest (en op **Yes** klikt om akkoord te gaan met de voorwaarden van die dienst), dan zie je na een tijdje in de kolom **VirusTotal** bijvoorbeeld **0/54**. In dat geval hebben nul van de 54 virusscanners die de webdienst VirusTotal gebruikt malware in het proces aangetroffen.
Kies je voor optie **Properties** in het rechtermuisknopmenu dan verschijnt veel andere informatie van een proces, verdeeld over tien tabbladen. We noemen een paar voorbeelden: op het tabblad **Image** zie je onder meer wanneer een proces gestart is (achter het kopje **Started**). Op het tabblad **Performance Graph** zie je wat voor systeembronnen recentelijk verbruikt zijn en op het tabblad **Threads** zie je het aantal threads dat het proces heeft.
Een andere handigheid is om het proces te vinden bij een bepaald open venster. Hiervoor klik je op de reddingsboei naast de verrekijker (laatste pictogram in de rij). Houd de knop ingedrukt, waarna Process Explorer verdwijnt en beweeg de muis naar het venster waarvan je het achterliggende proces wilt weten. Laat de muis los en het proces wordt automatisch in Process Explorer geselecteerd.

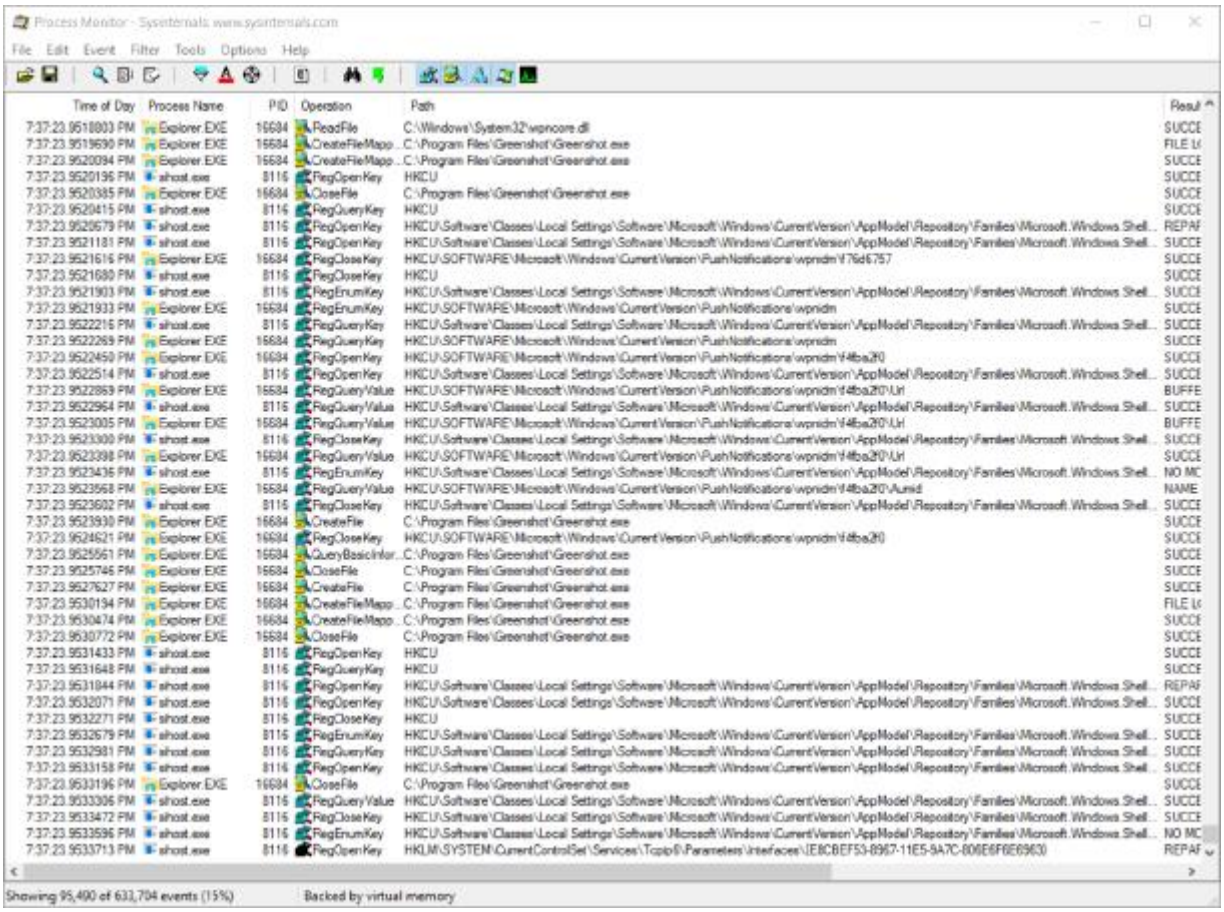
Wat is een 'handle'?

Regelmatig zie je in Windows Taakbeheer en ook in Process Explorer de term 'handle' voorbijkomen. Windows gebruikt een uniek getal om daarmee unieke objecten in het geheugen mee aan te duiden, zoals een venster, een bestand dat open is of een proces, dat is de handle. Zo'n handle dient als referentie naar het object. Zo kun je bijvoorbeeld zien welke bestanden een proces in gebruik heeft. In Process Explorer kun je de handles van een proces zien door op Ctrl+H te drukken en desgewenst specifieke handles sluiten.

Overigens zijn DLL's (de zogenoemde dynamic link libraries) gedeelde code die bepaalde functionaliteiten leveren. Deze DLL's zijn aparte bestanden, zodat ze eenvoudig door meerdere programma's gebruikt kunnen worden. Deze zie je met Ctrl+D.

04 Process Monitor

Process Monitor is, in tegenstelling tot Process Explorer, meer een passieve tool om te zien wat er allemaal aan de gang is binnen je systeem. Je opent het door in de map C:\sysinternals te kiezen voor het bestand Procmon.exe. Voer ook dit programma uit als administrator voor alle mogelijkheden en klik na het openen op **Agree** om akkoord te gaan met de licentievoorwaarden.
Er komen continu nieuwe gebeurtenissen binnen die Process Monitor vastlegt, dus de lijst wordt alsmaar langer. Standaard zie je de volgende kolommen in Process Monitor: **Time**,**Process Name**, **PID**, **Operation**, **Path**, **Result** en **Detail**. **Time** is de tijd waarop het event plaatsvond; **Process Name** is het verantwoordelijke proces; **Operation** is wat voor actie er plaatsvond, **Path** is het bestandspad waarop het event betrekking had. De kolom **Result**geeft aan of een actie is gelukt, en kan onder andere de aanduiding **SUCCESS**, **NAME NOT FOUND** of **ACCESS DENIED** bevatten.
In **Detail** staat verder gedetailleerdere informatie. Wat handig is bij een event, is om er met de rechtermuisknop op te klikken en te kiezen voor**Jump To**. Het **Path** wordt dan geopend, dat kan registersleutel zijn of een map of bestand.

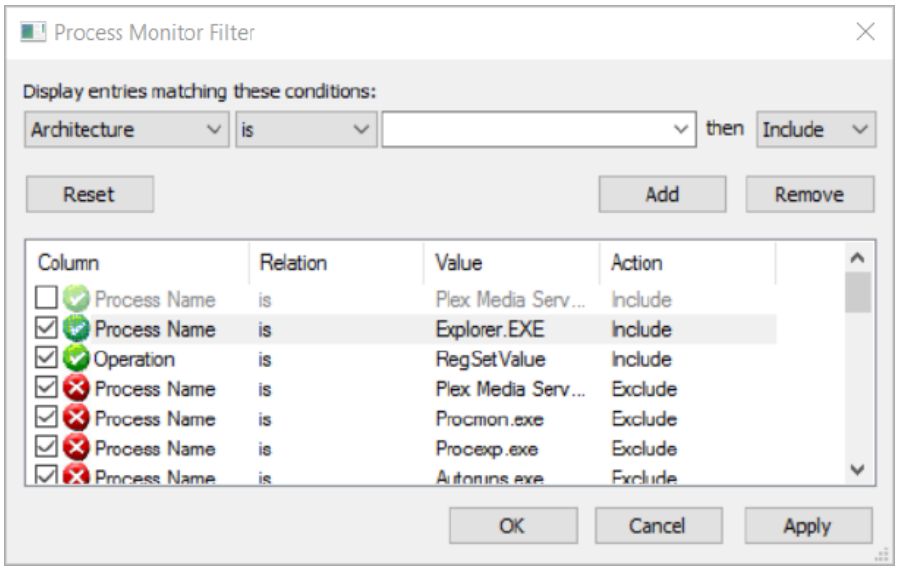


04 Hier zie je een heleboel events bij Process Monitor binnenkomen, dat gebeurt al als je maar een paar programma's open hebt staan.

05 Dieper in Process Monitor

Het aantal problemen dat je kunt oplossen met Process Monitor is zeer groot, al bestaat daar niet zo maar een eenvoudig stappenplan voor. Wat kan helpen als je een probleem hebt, is om Process Monitor open te houden en zodra het probleem optreedt het loggen stop te zetten, door op **File** en **Capture Events** te klikken. Vervolgens kun je filteren door met de rechtermuisknop op de procesnaam of **Operation** te klikken en te kiezen voor**Include** om alleen events van dat proces weer te geven of met die operation. Klik op**Exclude** om events van dat proces weg te halen.

Voorbeeld: je wilt weten waar een bepaalde registersleutel is voor een Windows-instelling. Dan filter je op **Explorer.EXE** door die te 'includen', vervolgens voer je de Windows-instelling uit door deze aan te passen en op te slaan en daarna stop je het vastleggen van events door op **File / Capture Events** te klikken. Nu filter je bijvoorbeeld op **RegSet Value**, omdat een Windows-instelling altijd een registerinstelling wijzigt. Na even zoeken zie je daar de betreffende wijziging. Dit kun je ook bijvoorbeeld doen met een foutmelding: filter op het proces dat de foutmelding veroorzaakt en kijk wat er gebeurt net voor de foutmelding. Dat kan hints bieden over wat er misgaat.



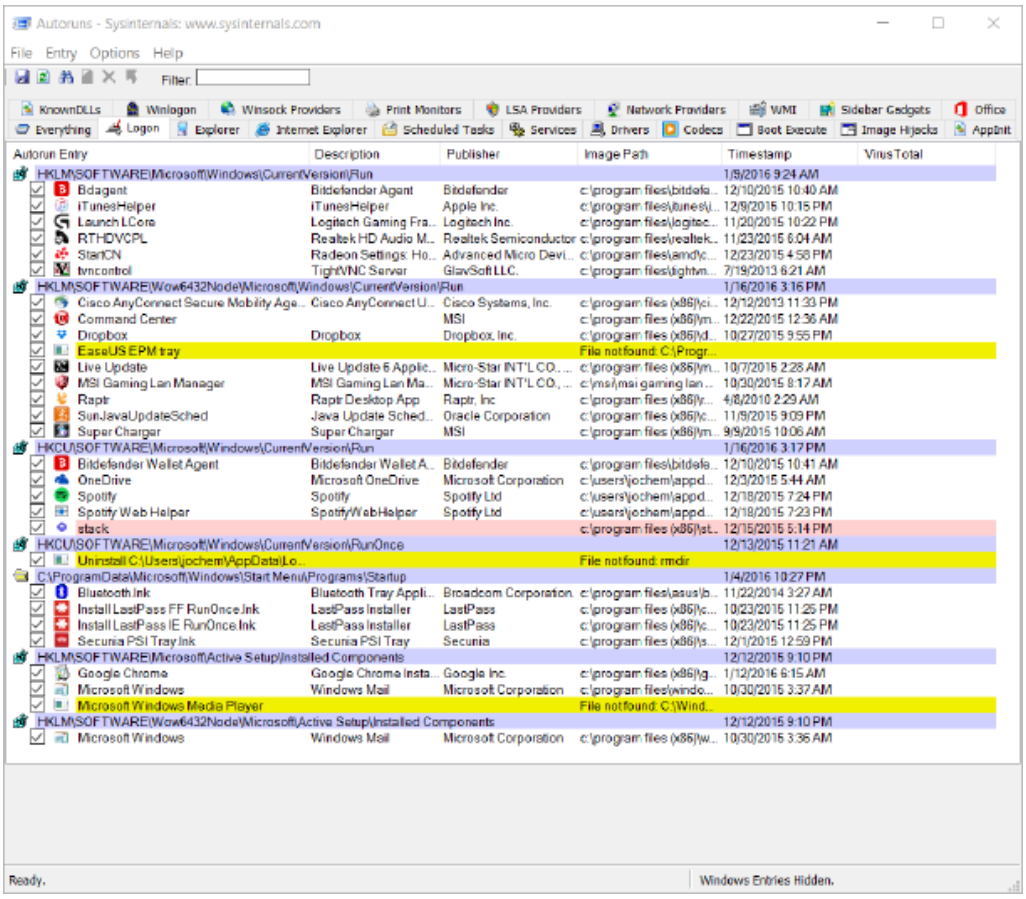
05 In dit geval hebben we een filter ingesteld voor Explorer.EXE met RegSet-events.

06 Autoruns

Autoruns is een zeer krachtige tool bedoeld voor elke Windows-poweruser. Met Autoruns kun je inzien wat er allemaal mee opstart met de computer. Dat is meer dan alleen de processen die je ziet in de Taakbeheer van Windows 8.1 en Windows 10. Je opent Autoruns door het bestand autoruns.exe te openen in de map C:\sysinternals. Voer ook dit programma uit als administrator om optimaal van alle functies gebruik te kunnen maken en ga daarna akkoord met de voorwaarden. Je ziet hier een aantal kleuren per opstartitem. Standaard analyseert Autoruns alle opstartitems of deze ondertekend zijn. Vaak zijn ondertekende processen veiliger.
Roze houdt in dat er geen handtekening is gevonden. Geel houdt in dat er een opstartitem bestaat, maar dat het bestand of de taak niet langer bestaat. Net als bij Process Explorer en Process Monitor kun je met de rechtermuisknop op een item klikken en kiezen voor **Jump to** om direct naar het item te springen om rond te kijken. Om een opstartitem uit te schakelen, vink je het uit. Om het permanent te verwijderen, klik je er met de rechtermuisknop op en klik je op **Delete**.

07 Malware herkennen met Autoruns

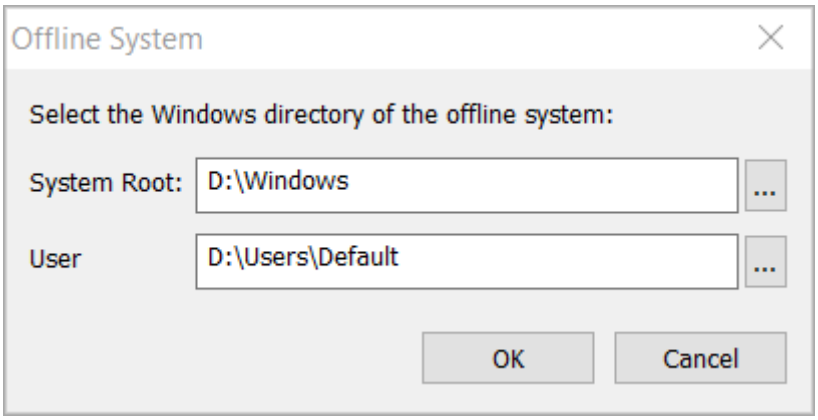
Bovenin Autoruns kun je overigens filteren per item, bijvoorbeeld op loginitems (**Logon**), geplande taken (**Scheduled Tasks**). Op het tabblad **Internet Explorer** zie je alle IE-invoegtoepassingen. Met een vinkje schakel je het een en ander uit. Het beste vink je alles uit, voor een optimale browserervaring. Eventuele malware herken je aan een mogelijke combinatie van dingen: dat de invoegtoepassing niet digitaal ondertekend is, er geen**Publisher** is, dat de invoegtoepassing zich vaak bevindt bij het **Logon**-tabblad. Verder bevindt malware bevindt zich vaak in C:\Windows of C:\Windows\System32 en heeft het een naam die nergens op slaat met een willekeurig pictogram. Zie je zo'n proces, scan het dan even met VirusTotal (op dezelfde manier als bij Process Explorer) en schakel het uit. Een andere handigheid is om wijzigingen bij te houden van opstartitems.
Je kunt de huidige scan opslaan in Autoruns door op **File** en dan **Save** te klikken. Als je dan op een later tijdstip opnieuw Autoruns opent, kun je de wijzigingen sindsdien eenvoudig zien door op **File** en **Compare** te klikken. Kies in het venster dat nu verschijnt voor het bestand dat je toen op hebt geslagen. Vervolgens zie je gewijzigde configuraties in Autoruns in het groen weergegeven. Zo wordt het makkelijker om de malware te herkennen: je hoeft alleen de wijzigingen door te nemen.



07 In dit geval is het enige verdachte proces stack.exe: het is niet ondertekend (roze kleur), heeft geen Publisher, het staat op het Logon-tabblad. Echter, het staat wel in de Program Files-map, dus alles lijkt toch veilig.

08 Andere Windows-installatie analyseren met Autoruns

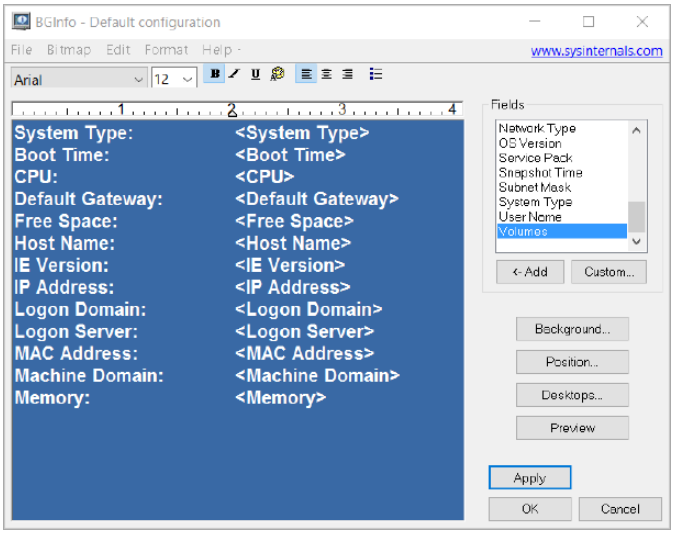
Autoruns heeft een heel handige functie waarmee je een harde schijf kunt analyseren van een andere computer. Stel je zit met een pc die niet meer op wil starten of die helemaal vol zit met malware, dan heeft Autoruns de mogelijkheid om deze harde schijf te analyseren en de opstartitems in te zien en aan te passen. Hiervoor is het nodig de harde schijf aan met je computer te verbinden, bijvoorbeeld met een usb-dockingstation met SATA-aansluiting erin. Heb je dat eenmaal gedaan, dan klik je in Autoruns op **File** en daarna op **Analyze Offline System**. Vul nu het pad in naar de Windows-map op de harde schijf bij **System Root**en ook het pad **User Profile** met het pad naar een gebruikersprofiel dat aanwezig is op de computer. Heb je dat eenmaal gedaan, klik dan op **OK** om Autoruns de Windows-installatie te laten analyseren. Je kunt nu rustig alle opstartitems bekijken, de verdachte processen er tussen uit vissen en deze uitschakelen.



08 Om een offline systeem te analyseren, vul je even de locatie van de Windows-map in en het User Profile.

09 Systeeminfo op je bureaublad met BgInfo

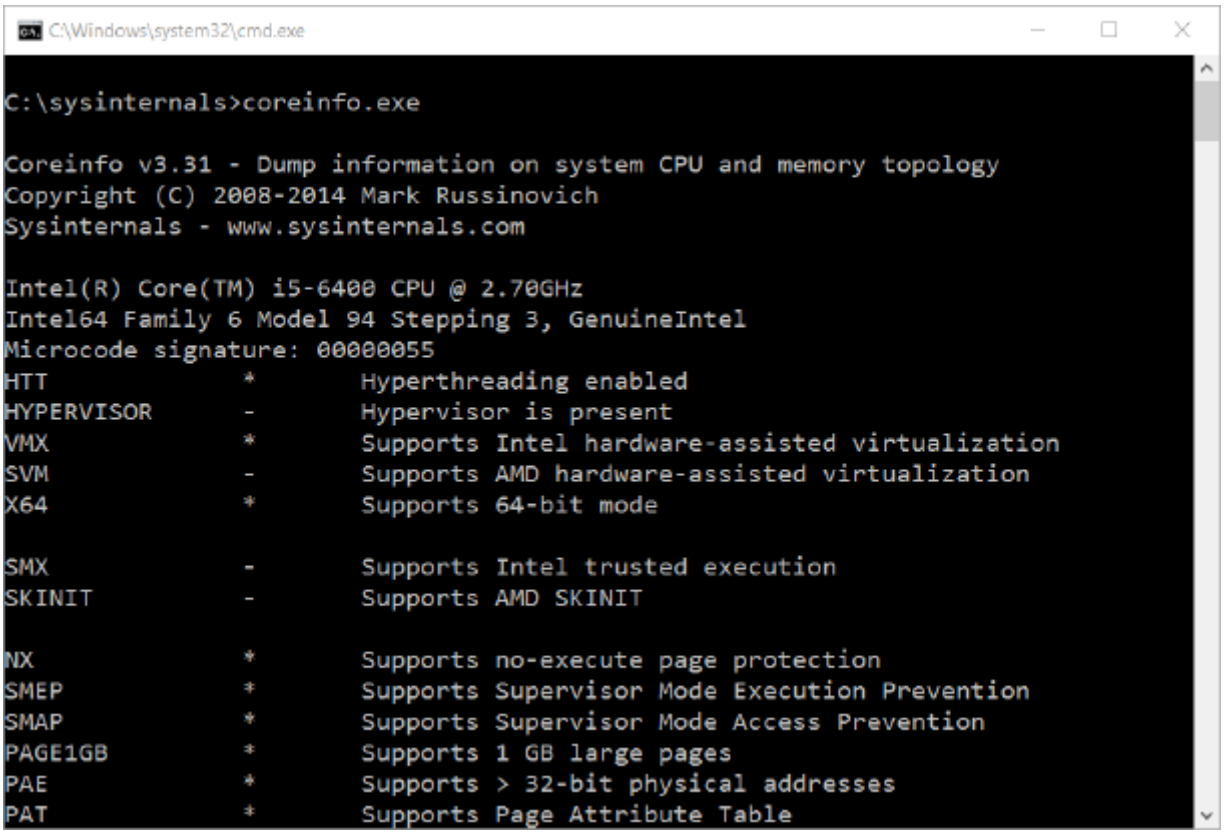
Om de belangrijkste systeembronnen in de gaten te houden, kan BgInfo van pas komen. Daarmee wordt belangrijke systeeminformatie op de bureaubladachtergrond weergegeven. Let op, als je beeldscherm een hoog aantal dpi heeft, is het nodig even met de rechtermuisknop op **Bginfo.exe** te klikken en te kiezen voor **Eigenschappen**. Ga naar het tabblad **Compatibiliteit** en kies voor **Beeldscherm aanpassen uitschakelen bij hoge DPI-instellingen**. Klik op **OK** om het venster te sluiten en de wijzigingen actief te maken. Je opent BgInfo door op het bestand **Bginfo.exe** te klikken in je Sysinternals-map.
Als je nu op **Apply** klikt in **BGInfo** verschijnt direct veel pc-informatie op de achtergrond, zoals de hoeveelheid vrije ruimte, de opstarttijd, de cpu, het geïnstalleerd geheugen, het IP-adres en meer. Je kunt het geheel configureren door in het grote tekstvak te typen en de tekst aan te passen. Variabelen zijn aangegeven met de haakjes: . Je kunt informatie weghalen door het gewoon in het tekstvak weg te halen. Als je weer iets wilt toevoegen, selecteer je die bij **Fields** en klik je op **Add**. Bij **Position** kun je instellen waar BgInfo wordt weergeven en bij **Background** kun je kiezen wat er moet gebeuren met je bureaubladachtergrond. Standaard wordt die gewoon behouden en wordt de systeeminformatie er transparant overheen gelegd. Je kunt op **Use these settings** klikken om deze aan te passen.



09 Rechts kun je extra informatie toevoegen en in het blauwe vak kun je gewoon typen en schuiven met alle informatie.

10 Overige tools

Er bevinden zich nog een heleboel andere tools in Sysinternals. Als je bezig bent een probleem te analyseren, kunnen deze tools in Sysinternals je eveneens helpen, bovenop de eerdere. Een handige tool is bijvoorbeeld TCPView, dat je kunt starten met Tcpview.exe. Je ziet vervolgens een lijst met actieve internetverbindingen, met de procesnaam, het protocol (TCP of UDP), het lokale adres, de poort, het externe adres en de externe poort en de staat. Door met de rechtermuisknop op een verbinding te klikken, kun je deze bijvoorbeeld stoppen door voor **Close Connection** te kiezen. Je kunt ook een 'Whois' doen om informatie over de domeinnaam, indien beschikbaar, te verkrijgen. Rode verbindingen zijn overigens net verwijderd, groene verbinding zijn nieuw.
Om snel informatie te verkrijgen over de pc, is Coreinfo handig. Je opent Coreinfo door met de rechtermuisknop in de map C:\sysinternals te klikken met shift ingedrukt. Kies dan voor**Opdrachtpromptvenster hier openen**. Typ vervolgens Coreinfo.exe en druk op Enter. Je ziet nu bijvoorbeeld of er een hypervisor is of de processor 64 bit is en je ziet de overige instructies die je cpu ondersteunt.



Coreinfo geeft veel informatie weer over de processor van het systeem, zoals welke functies die allemaal heeft.