

Werkzeuge für Windows NT, die betriebssystemspezifische Schwächen ausbügeln oder einen Einblick in die internen Abläufe gewähren, sind zwar inzwischen recht zahlreich vorhanden, doch lassen sich die Hersteller ihre Entwicklungen in der Regel recht teuer bezahlen.

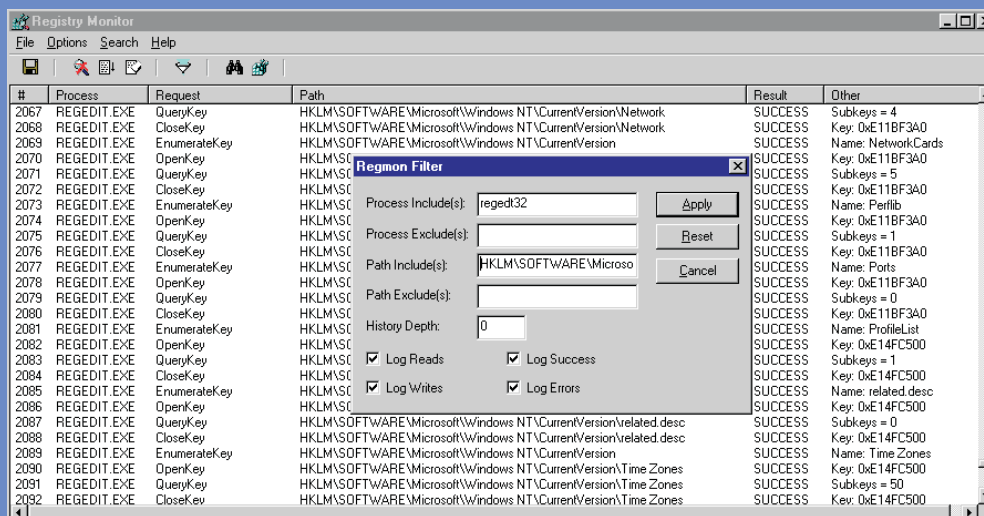
**DIRK PELZER**

Die gute Nachricht ist, daß es im Internet eine Web-Site gibt, die nicht nur zahlreiche Tools bereithält, um hinter die Kulissen von Windows-NT blicken zu können, sondern die meisten dieser Tools entweder kostenlos oder gegen eine vergleichsweise niedrige Lizenzgebühr zur Verfügung stellt. Als besonderes Schmankerl sind viele der nützlichen Helfer samt Quellcode erhältlich, so daß der versierte C-Programmierer in der Lage ist, die Tools nach seinen eigenen Bedürfnissen anzupassen. Im folgenden werden einige der interessantesten Tools kurz vorgestellt. Die Web-Seite unter der sich der Hilfesuchende die Tools herunterladen kann, lautet [www.sysinternals.com](http://www.sysinternals.com).

**Datei- und Registryzugriffe analysieren**

Ein Problemstellung, die insbesondere bei der Installation von Softwarepaketen immer wieder auftaucht ist die Frage, auf welche Dateien die Setup-Prozedur zugreift und an welchen Stellen in der NT-Registry Modifikationen stattfinden oder Informationen ausgelesen werden. Zur Lösung hält

die Web-Seite von Sysinternals die beiden Tool namens Ntregmon und Ntfilemon bereit. Während ersteres dem Administrator zeigt, welcher Prozeß auf welche Registryeinträge zugreift, listet Ntfilemon alle Dateizugriffe sämtlicher Prozesse auf. Standardmäßig zeigen beide Tools sämtliche Zugriffsoperationen, also zum Beispiel READ, WRITE, QUERY, etc. aller Prozesse auf und geben auch drüber Aufschluß, ob die Operation erfolgreich abgeschlossen werden konnte. Durch die Definition geeigneter Filterkriterien ist der Administrator darüber hinaus in der Lage, nur Informationen darstellen zu lassen, die für die zu untersuchende Fragestellung relevant sind. Mögliche Kriterien sind beispielsweise Prozesse, die vom Monitoring eingeschlossen sind, sowie Pfade von Dateien oder Registrypfaden, die relevant sind. Als sehr praktisch erweist sich auch die Suchfunktion, die in beide Tools integriert ist, mit deren Hilfe der Administrator gezielt nach bestimmten Einträgen suchen kann und so nicht Zeile für Zeile des unter Umständen sehr umfangreichen Reports durchforsten muß. Ein weiteres nützliches Feature von Ntregmon ist die Möglichkeit, durch Doppelklick auf einen Reporteintrag den Registry-editor starten zu können, der dann sogleich an der gewünschten Stelle steht.



Mit dem Registrymonitor kann der Administrator verfolgen, welche Prozesse auf die Registry zugreifen

### Monitor für die Schnittstellen

Wenn es darum geht, zu beobachten, welche Aktivitäten sich im Bereich der parallelen und seriellen Schnittstellen abspielen, so hält die Sysinternals-Homepage einen Portmonitor namens Portmon bereit, der akribisch jeden Systemaufruf protokolliert. Mit ihm ist der Administrator in der Lage mitzuverfolgen, wie eine Anwendung oder ein Treiber auf die COM- beziehungsweise LPT-Ports zugreift und so eventuell auftretende Probleme zu erkennen. Der Portmon ist nach Aussage seines Entwicklers in der Lage, alle I/O-Control-Kommandos (IOCTLs) der parallelen und seriellen Schnittstellen zu erkennen und darzustellen. Aber nicht nur die Kommandos selbst, sondern auch die für eine Fehleranalyse häufig noch interessanteren Parameter der Aufrufe werden erkannt und protokolliert. Bei Lese- und Schreibkommandos stellt der Portmon darüber hinaus die ersten 48 Byte des Schreib-/Lesebuffers dar, so daß der Administrator gegebenenfalls auch erkennen kann, welche Daten gesendet oder empfangen werden. Da auch bei der Beobachtung der Kommunikationsschnittstellen sehr schnell sehr viele Daten anfallen können, bietet der Portmon ebenso wie zum Beispiel der Registrymonitor eine Filter- und eine Suchfunktion an.

### DLLs beobachten

Häufig werden Softwareprodukte mit DLLs ausgeliefert, die bestehende System- oder Anwendungs-DLLs ersetzen. Dabei kommt es nicht selten zu Überraschungen, wenn auf einem NT-System eine Applikation, die bislang ohne Probleme lief plötzlich meldet, daß sie diesen oder jenen Einsprungpunkt in einer DLL nicht mehr finden kann. Um Problemen dieser Art vorzubeugen und bereits im Vorfeld einer Softwareinstallation herauszufinden, welche Anwendungen möglicherweise von einer Softwareinstallation betroffen sein könnten, bietet die Sysinternals-Web-Seite das Programm Listdlls. Hierbei handelt es sich auch wieder um ein Kommandozeilenutility, das ohne Parameter aufgerufen wird. Listdlls erstellt eine Liste sämtlicher im Speicher befindlicher Anwendungen und Dienste und zeigt an, auf welche DLLs die jeweiligen Pro-

gramme zugreifen. Da Listdlls auch den Pfad angibt, von dem eine DLL geladen wurde, kann der Administrator außerdem auch feststellen, ob eine Anwendung auf die richtige DLL zugreift oder ungewollt auf eine andere gleichen Namens, die sich aber in einem anderen Verzeichnis befindet, was unter Umständen ebenfalls zu Problemen führen kann.

### Defragmentierung für einzelne Dateien

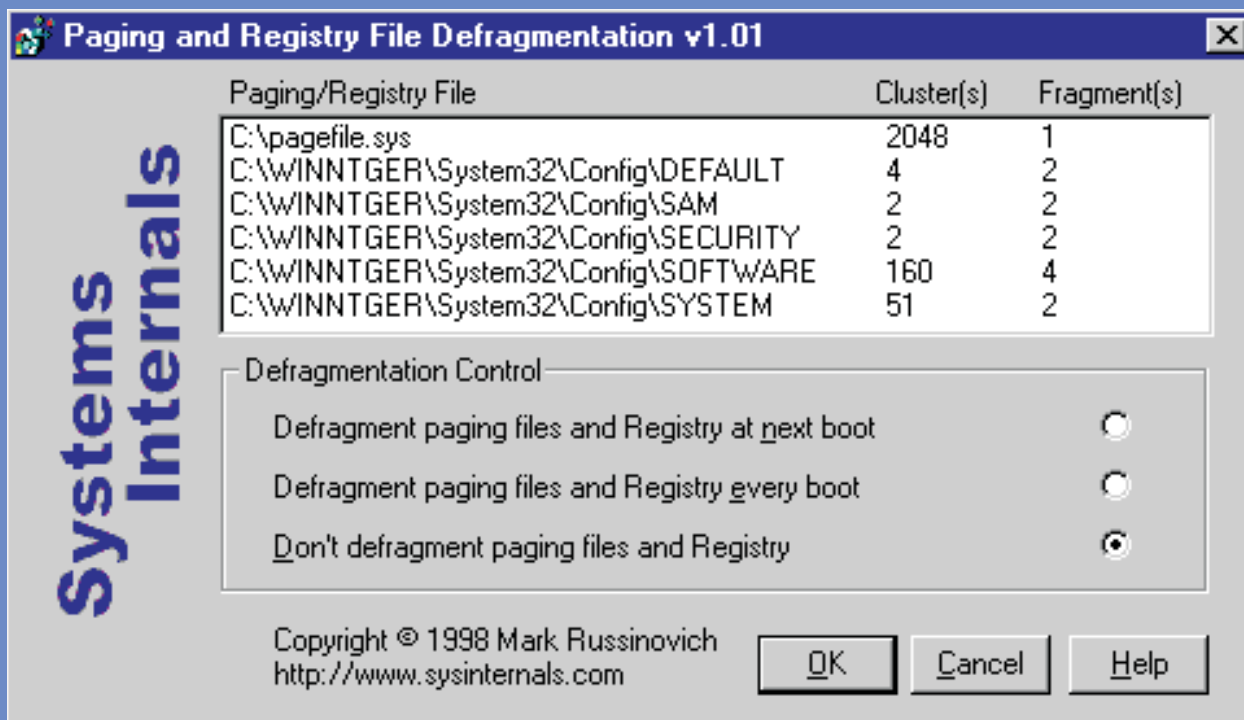
Zahlreiche kommerzielle Hersteller bieten Festplattendefragmentierungstools für Windows-NT an. Jedoch arbeiten die meisten dieser Tools so, daß sie eine komplette Partition defragmentieren, aber nicht in der Lage sind, einzelne Verzeichnisse oder gar nur einzelne Dateien zu defragmentieren. Sysinternals hat auch für diese Fälle ein Tool namens Contig (für Contiguous File = durchgehende Datei) parat, das genau auf den geschilderten Einsatzzweck zugeschnitten ist. Selbstverständlich ist Contig auch in der Lage, eine komplette Partition zu defragmentieren, wenn es erforderlich sein sollte. Damit eröffnet es dem Administrator die größtmögliche Flexibilität. Contig ist ein reines Kommandozeilen-tool, das sich sowohl für den interaktiven als auch den automatisierten Einsatz beispielsweise über den NT-Scheduler eignet. Die Syntax ist sehr einfach und mit folgendem Kommando kann der Administrator zum Beispiel die komplette *C:\-Partition* eines Rechners defragmentieren: `contig -s c:\*.*`. Möchte er hingegen nur die Datei *C:\USER\TESDOC.DOC* defragmentieren, so gibt er folgendes ein: `contig c:\user\testdoc.doc`. Contig gestattet es aber auch, eine Datei anzulegen, die von vornherein nicht defragmentiert ist.

Ein ähnlich interessantes Tool wie Contig ist Pagedefrag. Dieses gestattet es dem Administrator nämlich auch NT-Systemdateien zu defragmentieren, die sich normalerweise permanent im Zugriff des Betriebssystems befinden. Hierzu zählen die Auslagerungsdatei oder die Dateien, in denen die NT-Registry abgelegt wird, also zum Beispiel SAM, SYSTEM, SECURITY und so weiter. Im Gegensatz zu den meisten kommerziell verfügbaren Defragmentierungstools für Windows-NT ist Pagedefrag sogar in der Lage, im laufenden NT-Betrieb anzuzeigen, ob die diese Dateien fragmentiert sind,

## Kostenlose Tools für NT

so daß der Administrator sehen kann, ob eine Defragmentierung erforderlich ist. Das einzige was Pagedefrag nicht kann, ist die im Zugriff befindlichen Dateien im laufenden Betrieb zu defragmentieren. Dazu ist ein Systemneustart erforderlich. Ob eine

automatische Defragmentierung stattfinden soll, oder nicht, kann der Administrator über eine GUI-Oberfläche einstellen, die auch anzeigt, ob und wenn ja in wie viele Fragmente das Pagefile und die Registrydateien aufgeteilt sind.



Mit Pagedefrag lassen sich lokale Auslagerungsdateien, sowie die NT-Registry-Dateien defragmentieren.

### NTFS-Dateien unter DOS lesen

Einer der Klassiker der Sysinternals-Web-Seite ist sicherlich das Tool Ntfsdos. Dieses Utility gestattet dem Administrator ein NT-System mit einer DOS-Diskette zu booten und anschließend auf Partitionen zuzugreifen, die mit dem NT-Filesystem NTFS formatiert sind. Ntfsdos kann beispielsweise dann zum Einsatz kommen, wenn die Maschine eines Anwenders nicht gebootet werden kann und nicht mehr genügend Platz für eine zweite NT-Installation vorhanden ist. Um wichtige Daten retten zu können, die sich noch auf dem Rechner befinden, startet der Administrator den PC mit einer MS-DOS Bootdiskette und ruft anschließend einfach NTFSDOS auf. Das Tool erkennt automatisch vorhandene NTFS-Partitionen und macht diese für DOS

zugreifbar. Eventuell vorhandene NTFS-Sicherheitseinstellungen werden dabei umgangen. Allerdings ist die kostenlos verfügbare Version von NTFSDOS nur in der Lage, lesend auf NTFS-Laufwerke zuzugreifen. Damit lassen sich aber immerhin Dateien einer nicht mehr funktionsfähigen NT-Installation retten und auf einen anderen Rechner übertragen. Eine Version die sowohl lesend als auch schreibend auf NTFS zugreifen kann, wird es laut Angabe der Programmautoren nicht geben. Jedoch bieten sie zwei kostenpflichtige Zusatztools für NTFSDOS an, mit deren Hilfe der Administrator Dateien auf die NTFS-Partition kopieren oder bestehende NTFS-Dateien umbenennen kann. Somit könnte zum Beispiel ein System, das aufgrund eines defekten oder falsch installierten Systemtreibers nicht mehr starten kann, repariert werden.

## Kostenlose Tools für NT

### FAT-32 für Windows NT

Ein weiteres Highlight der Sysinternals-Webpage ist ein Treiber, mit dem das FAT-32-Dateisystem von Windows-9x auch unter Windows-NT unterstützt wird. Damit kann der Anwender nun endlich beide Betriebssysteme auf einem Rechner betreiben und muß sich nicht mit FAT-16 als kleinstem gemeinsamen Nenner begnügen. Eine Version des Treibers, die nur lesend auf FAT-32-Partitionen zugreifen kann, ist kostenlos verfügbar. Wer auch Schreibzugriff benötigt, kann für ein paar Dollar einen entsprechenden Treiber erwerben. Einen Wehmutstropfen gibt es allerdings, denn die NT-Systempartition kann sich nicht auf einem FAT-32-Laufwerk befinden. Da NT keine generische Unterstützung für FAT-32 mitbringt, ist es erforderlich, für einen Parallelbetrieb von NT und Windows-9x eine Primäre Partition auf dem ersten logischen Laufwerk mit FAT-16 einzurichten und dort die beiden Betriebssysteme zu installieren. Die übrigen Partitionen können dann mit FAT-32 formatiert werden. Ebenfalls enthalten ist ein Prüfprogramm für FAT-32-Partitionen unter NT namens Chkfat32. Dieses ist allerdings nicht in der Lage erkannte Probleme zu beseitigen, sondern weist nur darauf hin, daß eine Partition fehlerhaft ist. Um eine Reparatur durchzuführen ist, der Anwender auf die Hilfsmittel von Windows-9x in Form von Scandisk angewiesen.

### Fazit

Die Sysinternals-Web-Seite bietet eine Menge Tools für NT aber auch Windows-9x, von denen die meisten kostenlos oder sehr preisgünstig zu haben sind. Auf der Web-Seite sind noch zahlreiche weitere Tools enthalten, die an dieser Stelle nicht angesprochen werden konnten und es kommen ständig neue hinzu, so daß es sich durchaus lohnt, einen Bookmark auf [www.sysinternals.com](http://www.sysinternals.com) zu setzen.

## Shortcut

### Executive Summary

Gute und preiswerte Tools für Windows-NT zu finden, ist nicht immer einfach. Im Internet gibt es jedoch eine Quelle, von der sich Administratoren zahlreiche nützliche Werkzeuge und Entwickler gleich den dazugehörigen Quellcode kostenlos herunterladen können. Vom einfachen Monitor, die mitprotokliert, welche Prozesse auf welche Einträge in der NT-Registry zugreifen, bis zum DOS-Programm, das NTFS-Partitionen lesen kann, ist alles dabei.

### Zur Person

DIPL. ING. DIRK PELZER arbeitet als freier Consultant und Journalist in München. Er betreibt ein Storage Labor für verschiedene namhafte Fachzeitschriften. Zudem beschäftigt er sich mit Speichernetzen und Hochverfügbarkeit.