Vorwort

Liebe Leserinnen und Leser,

bei diesem Buch handelt es sich nicht um ein weiteres Windows 7-Buch mit umfangreichen Anleitungen und vielen Informationen, die mancher Leser möglicherweise gar nicht will. In diesem Buch zeigen ich Ihnen haufenweise schnell umsetzbare und hochaktuelle Expertentipps und -tricks zu Windows 7. Ich erkläre wichtige und kostenlose Zusatztools mit denen Sie Windows 7 beschleunigen, absichern und die Bedienung verbessern können. Ein weiteres Thema ist die Erweiterung und Verbesserung des Windows-Explorers. Neben Tipps zur Benutzeroberfläche, zur Installation und zur Reparatur von Windows, zeige ich Ihnen auch, wie Sie effizient mit der PowerShell arbeiten können und den Netzwerkbetrieb verbessern. Last but not least stelle ich Ihnen verschiedene Tools zur Verbesserung der Sicherheit und Leistungsverbesserung vor.

Mit dem Service Pack 1 bietet Microsoft das erste große Aktualisierungspaket für Windows 7 an. Zwar enthält es für Windows 7 keine neuen Funktionen, dafür aber einiges an Verbesserungen. Ich habe die Installation, das Troubleshooting und Eigenschaften des SP1 für Windows 7 in einem eigenen Kapitel zusammengefasst. Dort lesen Sie, wie Sie das SP1 optimal installieren, auch automatisiert, bei Fehlern ein optimales Troubleshooting durchführen und wie Sie Bereinigungsmaßnahmen durchführen. Sie erfahren dort ebenfalls wie Sie eine Installations-DVD für Windows 7 erstellen, die bereits das SP1 enthält.

Für Windows Server 2008 R2 dagegen bietet das Service Pack 1 neue Funktionen wie RemoteFX und Dynamic Memory. Sie spielen auch für Windows 7-Clients in Unternehmen eine Rolle, da es hier um die Virtualisierung von Arbeitsstationen geht. Ich habe beiden Themen jeweils ein eigenes Kapitel gewidmet und zeige Ihnen dort, wie Sie die neuen Funktionen konfigurieren können.

Für Internet Explorer 9 finden Sie in diesem Buch haufenweise Tricks zur Installation, zu den Neuerungen, der automatischen Installation und der optimalen Einrichtung.

Die Verbreitung von SSD-Festplatten nimmt immer mehr zu. Hier bietet Windows 7 eine optimale Anbindung. Ich zeige Ihnen in diesem Buch mit welchen Tricks und Zusatztools Sie Windows 7 noch besser und schneller auf SSD-Platten betreiben können. Die Werkzeuge und Anleitungen in diesem Kapitel sind übrigens nicht nur für Besitzer von SSD-Festplatten interessant.

Ein weiteres wichtiges Thema ist die Optimierung und Verschönerung der Benutzeroberfläche. Lesen Sie wie Sie die Arbeit im Explorer beschleunigen, wie Sie zum Beispiel den Startknopf auswechseln, Befehle zu den verschiedenen Menüs hinzufügen oder auswechseln, den Startvorgang beschleunigen und vieles mehr. Zahlreiche Registryhacks helfen Ihnen Ihre Arbeit mit Windows 7 noch weiter zu verbessern.

Die Zusammenarbeit mit Linux und auch die parallele Installation von Linux und Windows 7 sind ebenfalls Bestandteil des Buches. Ich zeige Ihnen wie Sie die wichtigsten Linux-Distributionen Ubuntu und Suse parallel zu Windows 7 installieren, Daten austauschen und Bootmanager reparieren.

Es würden den Rahmen des Vorworts sprengen alle Bereiche offen zulegen, die ich in diesem Buch beschreibe. Lesen Sie am besten selbst, was Windows 7 bietet und mit welchen Tricks Sie das System verbessern können. Ich hatte großen Spaß beim Schreiben des Buches, da ich mit jedem Trick mein eigenes Windows verbessern konnte und hoffe, Sie erleben beim Lesen die gleiche Freude und finden viele wertvolle Tricks und Anregungen.

Ihr Thomas Joos

Kapitel 7

Windows-Optimierung – Leistung verbessern

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen Tricks zur Optimierung von Windows 7 und wie Sie das Betriebssystem beschleunigen können. Auch Zusatztools zur Analyse finden Sie auf den folgenden Seiten.

Windows beschleunigen und verbessern

Im folgenden Abschnitt gehen wir auf einige Tricks ein, die Ihnen dabei helfen sollen, Windows 7 noch schneller und besser zu machen.

Automatischen Neustart nach Updates deaktivieren

Viele Anwender stören sich daran, dass Windows 7 nach der automatischen Installation von Updates sofort neu starten will. Wollen Sie diese Funktion nicht, können Sie diese deaktivieren. Setzen Sie Windows 7 Ultimate, Professional oder Enterprise ein, können Sie dazu die Richtlinienverwaltung verwenden. Wir zeigen Ihnen im Anschluss die Deaktivierung über die Registry. Diese funktioniert auch in der Windows 7 Home Edition. Die Deaktivierung über Richtlinien nehmen Sie folgendermaßen vor:

1. Geben Sie *gpedit.msc* im Suchfeld des Startmenüs ein.

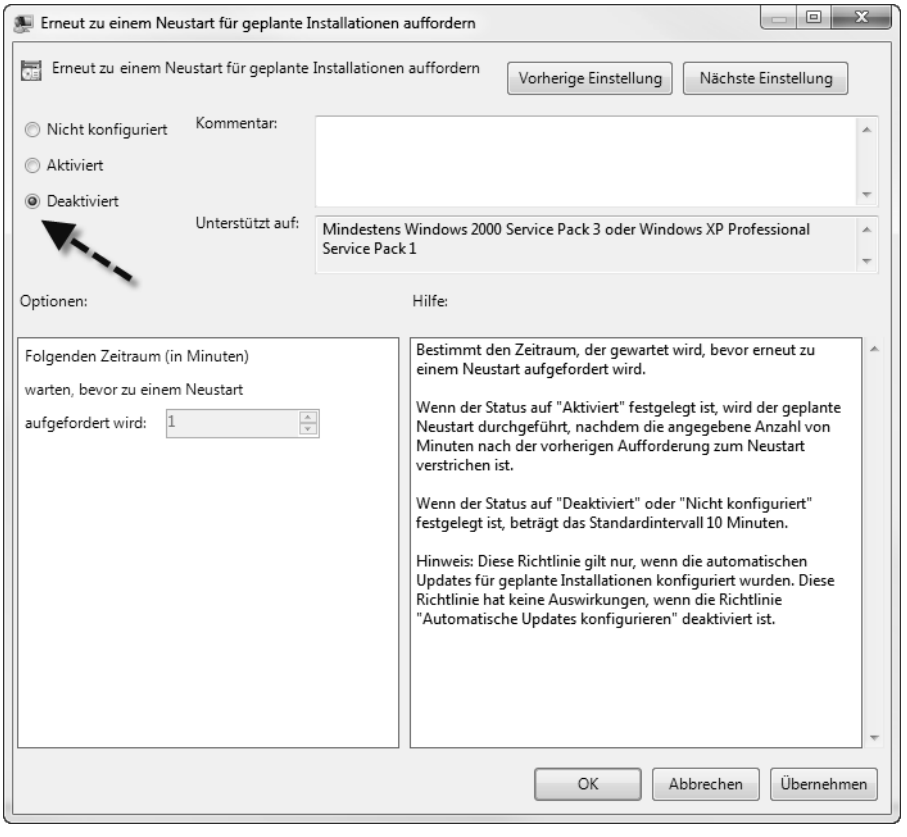


Abbildung 7.1 Deaktivieren der Neustart-Meldung von Windows 7

2. Navigieren Sie zu *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Windows Update.*
3. Im rechten Bereich stehen Ihnen verschiedene Einstellungen für Windows Update zur Verfügung, die in der normalen Verwaltungsoberfläche der Systemsteuerung nicht verfügbar sind.
4. Deaktivieren Sie die Option *Erneut zu einem Neustart für geplante Installation auffordern*. Zusätzlich sollten Sie noch die Option *Keinen automatischen Neustart für geplante Installationen ausführen* aktivieren.

Anwender, die auf die Home-Edition von Windows 7 setzen, können die Einstellung in der Registry vornehmen:

1. Öffnen Sie durch Eingabe von *regedit* im Suchfeld des Startmenüs den Registrierungs-Editor.
2. Navigieren Sie zu *HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU.*
3. Legen Sie einen neuen DWORD-Wert mit der Bezeichnung *NoAutoRebootWithLoggedOnUsers* an und geben Sie diesem den Wert *1*. Dieser Wert verhindert den automatischen Neustart.
4. Erstellen Sie den DWORD-Wert *RebootRelaunchTimeoutEnabled* und geben Sie diesem den Wert *0*, um auch die Meldung zu unterbinden.

Mit Freeware den Systemstart beschleunigen – Soluto

Mit der Freeware Soluto von der Seite *www.soluto.com* können Sie mit wenigen Mausklicks die Leistung Ihres Computers und das Bootverhalten beschleunigen. Sie laden sich die Anwendung herunter und installieren diese auf dem Computer, den Sie beschleunigen wollen.

Während der Installation legt das Tool automatisch einen Wiederherstellungspunkt an. Nach der Installation starten Sie den Computer neu.

Beim ersten Start scannt Soluto automatisch alle Programme und Tools, die mit Windows starten.

Abbildung 7.2 Soluto scannt den Bootvorgang von Windows 7

Nach Abschluss des Bootvorgangs zeigt Soluto ein Konfigurationsfenster an. Hier sehen Sie den Bereich *No-brainer* in Grün. Diese Programme können Sie laut Soluto problemlos vom Autostart ausschließen und damit Windows entlasten. Fahren Sie mit der Maus über diesen Bereich, sehen Sie, welche Anwendungen Soluto vom Autostart entfernen will und wie lange der Start der einzelnen Anwendungen beim Systemstart dauert.

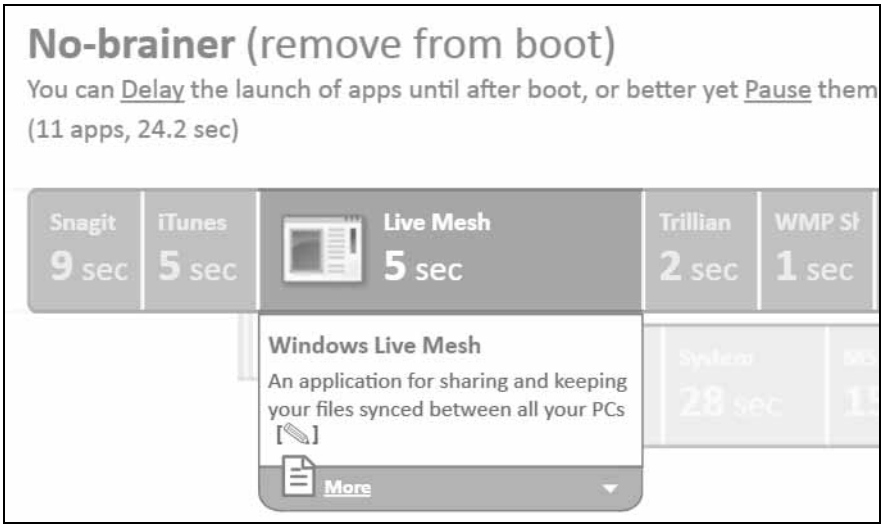


Abbildung 7.3 Programme, die den Systemstart verzögern

Fahren Sie wiederum mit der Maus über die entsprechende Anwendung, zeigt Soluto zusätzliche Informationen an und Sie können diese Anwendung zukünftig mit Pause vom Systemstart entfernen.

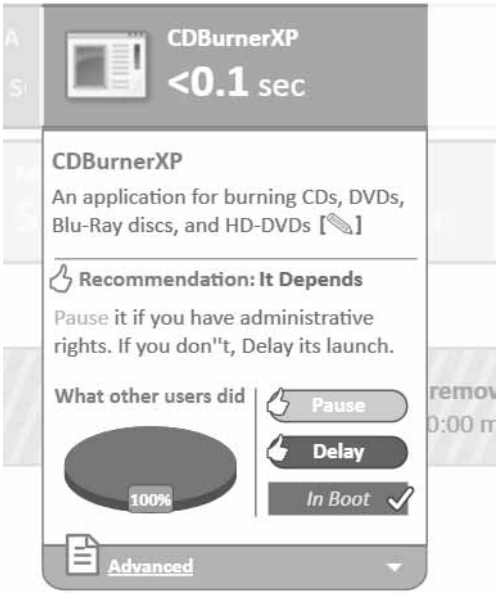


Abbildung 7.4 Pausieren von Anwendungen vom Systemstart

Lassen Sie Anwendungen pausieren, sehen Sie diese im unteren Bereich. Benötigen Sie diese später doch im Autostart, können Sie die entsprechende Anwendung leicht wieder automatisch starten lassen.

Im Bereich *Potentially removable* zeigt das Tool Anwendungen an, die es nicht ordnungsgemäß einordnen kann. Hier können Sie über den gleichen Weg einzelne Anwendungen vom Systemstart ausschließen, diese aber nachträglich manuell starten.

Die Anwendungen bei *Cannot be removed with Soluto* können Sie mit Soluto nicht deaktivieren. Hier müssen Sie selbst Hand anlegen, zum Beispiel mit Tools wie Autoruns von Sysinternals.

Mehr Platz auf USB-Sticks schaffen und Sicherheit erhöhen

Oftmals geht der Speicherplatz auf USB-Sticks aus, egal wie groß die Speicherkapazität ist. Mit Windows 7 haben Sie die Möglichkeit, die Daten auf dem Stick zu komprimieren, ohne dazu eine Zusatzanwendung installieren müssen.

Nutzen Sie das NTFS-Dateisystem, haben Sie die Möglichkeit, einzelne Daten oder ganze Laufwerke standardmäßig zu komprimieren. Dazu müssen Sie bei der Formatierung des USB-Sticks das NTFS-Dateisystem verwenden.

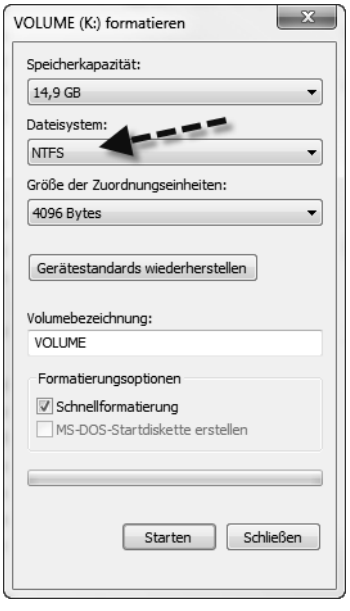


Abbildung 7.5 Formatieren des USB-Sticks mit dem NTFS-Dateisystem

Befinden sich auf dem Stick bereits Dateien, können Sie das Dateisystem auch in der Eingabeaufforderung ändern, ohne dass dabei Daten verloren gehen. Allerdings können Sie nur auf NTFS konvertieren, es gibt keinen Weg zurück. Wollen Sie auf dem Datenträger wieder ein anderes Dateisystem einsetzen, müssen Sie diesen neu formatieren. Verwenden Sie zur Konvertierung den Befehl:

```
convert <Laufwerksbuchstabe> /fs:ntfs
```

Haben Sie auf den Stick Daten kopiert, haben Sie die Möglichkeit, direkt einzelne Verzeichnisse zu komprimieren:

1. Klicken Sie dazu mit der rechten Maustaste auf das Verzeichnis auf dem Stick und rufen Sie die *Eigenschaften* auf.
2. Klicken Sie anschließend auf die Schaltfläche *Erweitert*.
3. Aktivieren Sie anschließend das Kontrollkästchen *Inhalt komprimieren, um Speicherplatz zu sparen*.
4. Klicken Sie auf *OK*, damit Windows den Inhalt komprimieren kann.
5. Rufen Sie anschließend die Eigenschaften des Verzeichnisses auf, sehen Sie die Größe der Dateien und welche Größe die Dateien nach der Komprimierung haben.

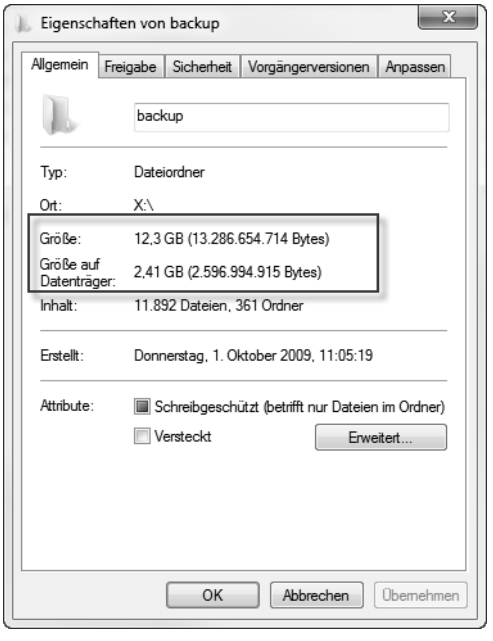


Abbildung 7.6 Anzeigen der Größe von Dateien und dem Platzverbrauch auf dem USB-Stick

Kopieren Sie Dateien in das Verzeichnis, komprimiert Windows diese zukünftig automatisch. Um auf Daten zuzugreifen, müssen Sie diese nur öffnen. Kopieren Sie auf den Stick aber Dateien, die ohnehin schon komprimiert sind, wie zum Beispiel *.jpg* oder *.mp3*, bringt diese Komprimierung nur wenig. Lohnenswert ist die Aktivierung für Dateien, die sich gut komprimieren lassen, wie ältere Office-Dokumente oder *.bmp*-Dateien. Aktuelle Office-Dokumente sind bereits Archive. Das erkennen Sie daran, dass Sie diese Dokumente auch extrahieren können und den Inhalt der Datei sehen.

Windows zeigt das Laufwerk in der Farbe blau an. Wollen Sie das nicht, deaktivieren Sie über *Organisieren/Ordneroptionen* auf der Registerkarte *Ansicht* die Option *Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe anzeigen*.

Neben der Möglichkeit, einzelne Verzeichnisse zu komprimieren, können Sie auch den kompletten USB-Stick automatisch komprimieren lassen. Dazu rufen Sie im Explorer die Eigenschaften des Laufwerks auf und aktivieren das Kontrollkästchen *Laufwerk komprimieren, um Speicherplatz zu sparen*.

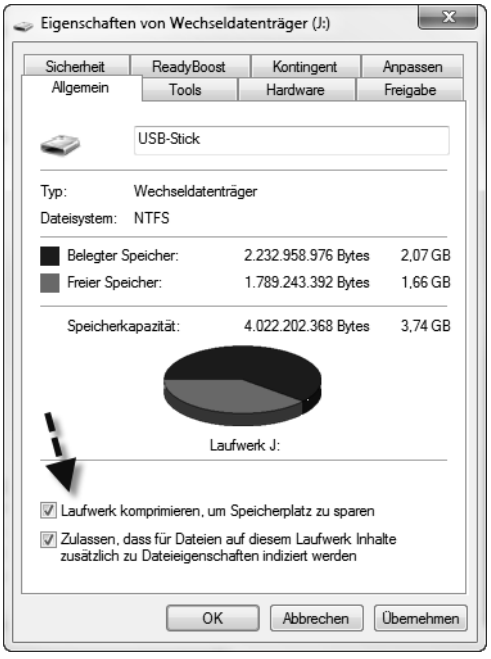


Abbildung 7.7 Komplettes Laufwerk komprimieren

Setzen Sie Windows 7 Ultimate oder Enterprise ein, steht Ihnen über das Kontextmenü von USB-Sticks noch die Option *BitLocker aktivieren* zur Verfügung. Damit können Sie das Laufwerk verschlüsseln. Der Zugriff auf das Laufwerk erfordert die Eingabe des Kennworts, das Sie zur Verschlüsselung angegeben haben.

Windows-Neustart nach Änderungen umgehen

Viele Software-Änderungen, Registry-Tweaks oder Anpassungen an Windows 7 benötigen einen Neustart von Windows oder zumindest eine Neuanmeldung. In vielen Fällen können Sie diese relativ langwierige Prozedur umgehen, indem Sie den Explorer im laufenden Betrieb beenden und wieder starten. Geöffnete Dateien bleiben weiter geöffnet und Daten gehen dabei auch nicht verloren. Natürlich bietet es sich an, wenn Sie wenigstens Dokumente vorher abspeichern:

1. Starten Sie den Task-Manager, zum Beispiel über das Kontextmenü der Taskleiste.
2. Wechseln Sie zur Registerkarte *Prozesse*.
3. Klicken Sie auf *explorer.exe* und beenden Sie den Prozess.
4. Startet der Explorer nicht automatisch neu, wählen Sie im Task-Manager *Datei/Neuer Task*.
5. Geben Sie *explorer* ein und bestätigen Sie.

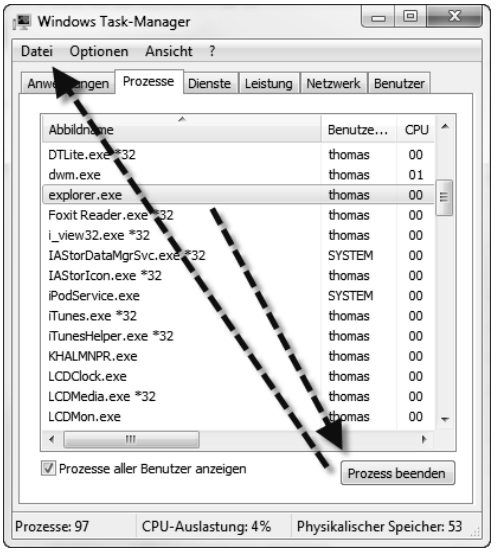


Abbildung 7.8 Beenden und neu starten des Explorers

Leistung verbessern durch Bereinigen der Registry – CCleaner und CCEnhancer

Läuft Windows zu langsam, liegen in vielen Fällen zwei Probleme vor: Zunächst starten mit Windows über die verschiedenen Autostartfunktionen zu viele Programme, die sich aktiv in die Taskleiste legen. Wie Sie diese Programme finden und deaktivieren können, lesen Sie im Trick »Autostartprogramm entdecken und entfernen – Autoruns« ab Seite 250.

Das zweite Problem liegt an zu vielen Einträgen in der Registry, die Windows nicht mehr benötigt. Solche fehlerhaften Einträge kommen vor allem von Anwendungen, die ihre eigenen Einträge nicht mehr entfernen. Mit der Freeware CCleaner, die seit Jahren im Bereich Windows-Pflege bekannt ist, können Sie fehlerhafte Registryeinträge, aber auch temporäre Dateien, die Sie nicht mehr benötigen, schnell und einfach entfernen. Sie finden die aktuellste Version des Tools auf der Seite *http://www.piriform.com/ccleaner*.

CCleaner ist ab Version 3.05.1409 vollständig kompatibel zu Windows 7 SP1, Internet Explorer 9 und auch Mozilla Firefox 4.

ACHTUNG Optimierungstools wie CCleaner führen für die Optimierung tief greifende Änderungen durch und löschen zahlreiche Einträge in der Registry und anderen Bereichen. Aus diesem Grund ist es sehr empfehlenswert, vor der Ausführung eine vollständige Systemsicherung durchzuführen, zum Beispiel eine Systemabbildsicherung. Zwar macht das Tool in den meisten Fällen keine Probleme, allerdings stellt die Verwendung von Systemtools immer eine Gefahr für ein System dar.

Laden Sie das Tool herunter und installieren Sie es auf dem Computer, den Sie optimieren wollen. Während der Installation können Sie auch auswählen, ob Sie das Kontextmenü des Papierkorbs erweitern wollen. Diese Erweiterung benötigen Sie für eine Systempflege nicht und können die entsprechenden Kontrollkästchen deaktivieren.

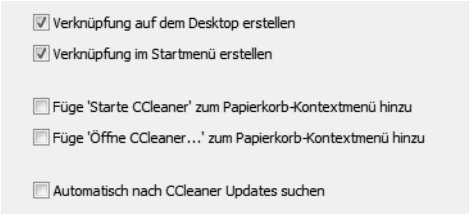


Abbildung 7.9 Installieren von CCleaner und entfernen der Verknüpfungen für das Kontextmenü des Papierkorbs

Nach dem Start können Sie auswählen, ob CCleaner auch Cookies intelligent scannen soll (Cookies also nicht löschen, die Sie benötigen). Solche Cookies sind zum Beispiel Speicherdaten für Webseiten, die Sie lokal gespeichert haben. Anschließend startet das Tool und Sie können auswählen, welche Optionen das Programm durchführen soll. Mit *Analysieren* stellt das Tool zunächst fest, welche Optimierungen möglich sind. Abhängig von den installierten Programmen kann dieser Vorgang über eine Stunde dauern. Sie sollten während der Zeit am besten nicht mit dem Computer arbeiten.

HINWEIS Windows bietet ebenfalls eine Datenträgerbereinigung, die Sie mit *cleanmgr.exe* starten können. Erstellen Sie eine Verknüpfung mit folgendem Befehl, startet die erweiterte Oberfläche der internen Datenträgerbereinigung von Windows 7:

```
C:\Windows\System32\Cmd.exe /c Cleanmgr /sageset:65535 & Cleanmgr /sagerun:65535
```

Mit den zusätzlichen Optionen sageset:65535 & Cleanmgr /sagerun:65535 zeigt das Tool auch versteckte Funktionen an, die Sie durch Aufrufen von cleanmgr.exe nicht erhalten.

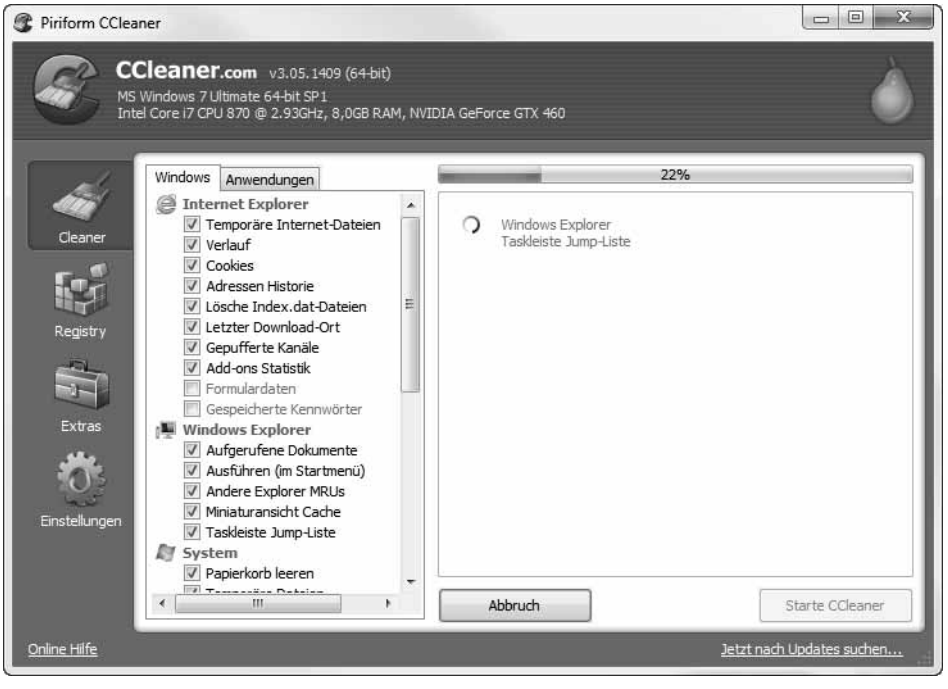


Abbildung 7.10 Optimieren des PCs mit CCleaner

Aktivieren Sie die Option *Registry*, kann das Tool auch die Registrierungsdatenbank nach Optimierungsmöglichkeiten durchsuchen. Dazu klicken Sie auf *Nach Fehler suchen* und anschließend auf *Fehler beheben*. Bevor CCleaner aber Einträge aus der Registry löscht, bietet das Tool eine Sicherung an. Dazu exportiert CCleaner die Bereiche, die es löschen will, in eine *.reg*-Datei. Um die Einträge wiederherzustellen, können Sie anschließend die Änderungen per Doppelklick wieder in die Registry importieren.

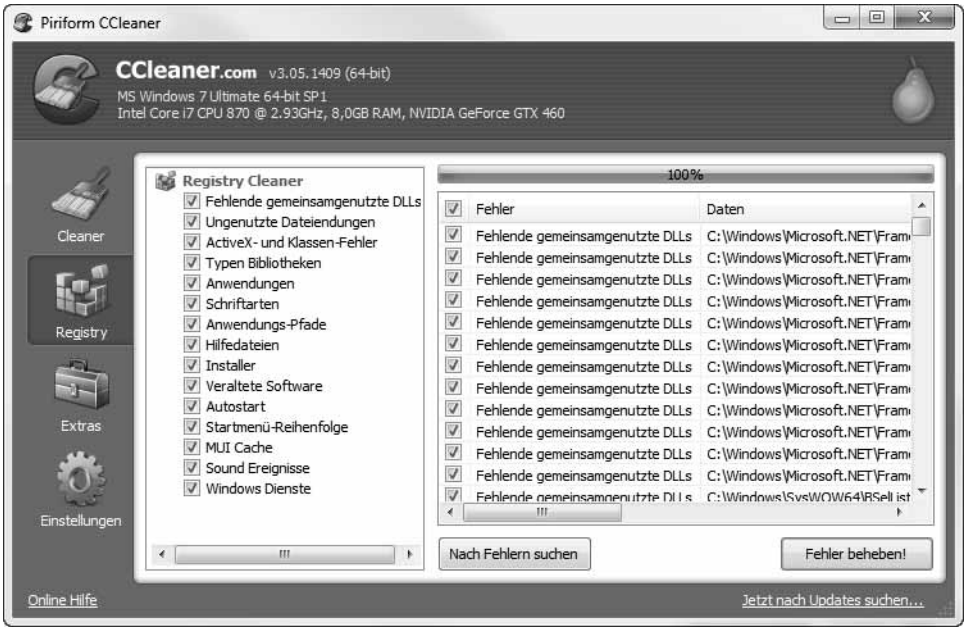


Abbildung 7.11 Bereinigen der Registry mit CCleaner

Neben den Standardprogrammen, die CCleaner untersuchen und bereinigen kann, können Sie das Tool auch mit einer kostenlosen Erweiterung ausbauen. Diese trägt die Bezeichnung *CCEnhancer*. Sie können sich die Installationsdatei der Erweiterung von CCleaner auf der Seite *http://thewebatom.net/software/ccenhancer* herunterladen.

Nach dem Start lassen Sie zunächst das Tool über *Download Latest* aktualisieren. Anschließend können Sie CCleaner starten lassen.

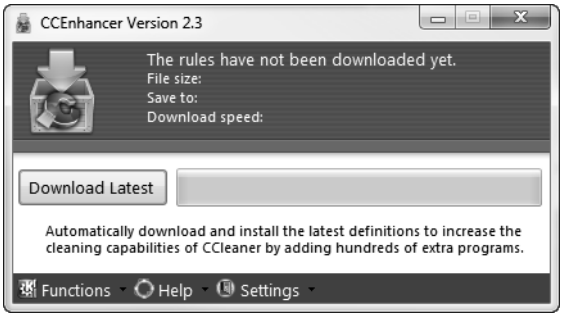


Abbildung 7.12 Erweitern von CCleaner mit CCEnhancer

Auf der Registerkarte *Anwendungen* sehen Sie die neuen Anwendungen, die das Tool jetzt unterstützt und bereinigen kann. Es bietet sich an, zur Optimierung eines Computers einmal den CCleaner durchlaufen zu lassen und einmal die Registrybereinigung.

Setzen Sie keine SSD-Platte ein, bietet sich anschließend eine Defragmentierung an. Die Verwaltungsoberfläche der Defragmentierung starten Sie durch Eingabe von *dfrgui* im Suchfeld des Startmenüs.

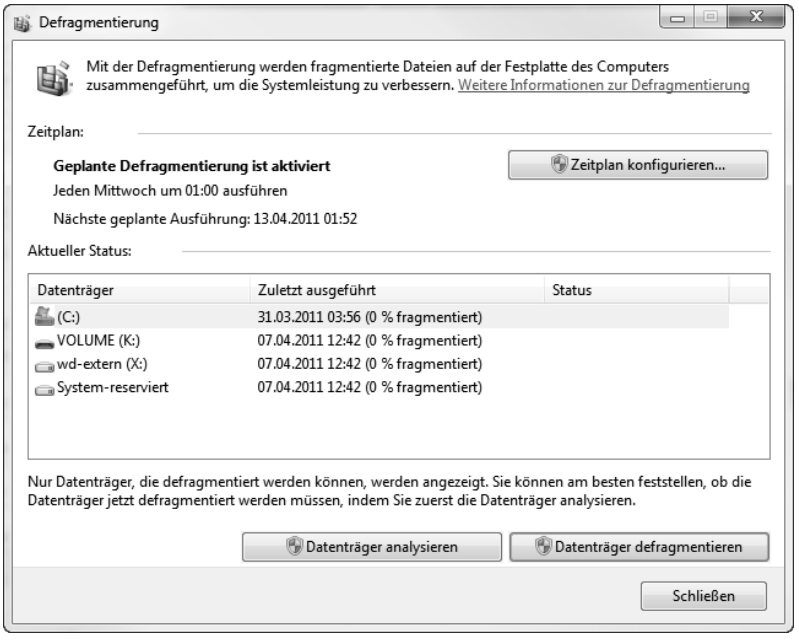


Abbildung 7.13 Defragmentieren eines Computers nach der Bereinigung durch CCleaner

Microsoft-Erweiterung für Touchscreens – Das Microsoft Touch Pack für Windows 7

Microsoft stellt über die Seite *http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=b152fadd-82e4-4ddb-a46a-aebe49944428&displayLang=de* das kostenlose Touch Pack für Windows 7 zur Verfügung.

Hierbei handelt es sich um eine Sammlung von Spielen und Programmen für Touchscreens. Das Pack enthält folgende Programme:

- Microsoft Blackboard Puzzlespiel
- Microsoft Garden Pond Spiel um japanische Gärten
- Microsoft Rebound Spiel zum Bewegen von Bällen mit dem Finger in das gegnerische Tor.
- Microsoft Surface Globe Erde als 3D-Bild
- Microsoft Surface Collage Fotoverwaltung
- Microsoft Surface Lagoon Bildschirmschoner

Häufig genutzte Daten als Ramdisk speichern

Sie haben in Windows 7 die Möglichkeit, einen bestimmten Bereich des Arbeitsspeichers als Festplattenlaufwerk zu verbinden. Der Vorteil dabei ist, dass Dateien, die Sie in diesem Bereich ablegen, zum Beispiel temporäre Dateien von Programmen, wesentlich schneller im Zugriff sind, als über eine normale Festplatte. Ein solches Laufwerk können Sie zum Beispiel für temporäre Dateien oder zum Entpacken von Archiven verwenden. Vor allem auf Computern, die über einen größeren Arbeitsspeicher verfügen, diesen aber im laufenden Betrieb nicht benötigen, profitieren von diesen Möglichkeiten.

Neben Freewareprodukten von Drittherstellern, die wir ebenfalls in diesem Trick zeigen, bietet auch Microsoft ein solches Tool an. Allerdings funktioniert diese Technik nur in den 32-Bit-Versionen von Windows 7. Sie benötigen für das Laufwerk im Arbeitsspeicher einen Treiber von Microsoft. Dieser steht nur als 32-Bit-Version zur Verfügung. Neben Microsoft gibt es aber auch Freewaretreiber, die wesentlich aktueller sind und stabiler funktionieren. Nicht in allen Fällen funktioniert die Ramdisk von Microsoft in Windows 7. Die Software von Drittanbietern funktioniert allerdings in den meisten Fällen problemlos.

Da der Inhalt des Arbeitsspeichers aber beim Herunterfahren oder einem Absturz unwiederbringlich gelöscht wird, sollten Sie in diesem Bereich keine wichtigen Daten ablegen.

Um zu sehen, wie viel Arbeitsspeicher zur Verfügung steht, rufen Sie den Task-Manager auf. In der Zeile *Verfügbar* des Bereichs *Physikalischer Speicher* sehen Sie die MB-Anzahl, die aktuell verfügbar ist.

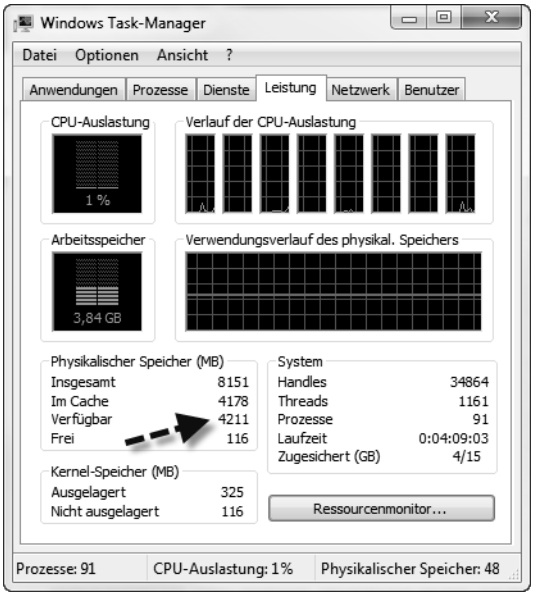


Abbildung 7.14 Anzeigen des freien Arbeitsspeichers eines Computers

Microsoft-Tool nutzen – Ramdisk-Treiber

Um eine Ramdisk anzulegen, gehen Sie folgendermaßen vor. Achten Sie aber darauf, dass nicht auf jedem Computer das Gerät funktioniert. In weiteren Tricks zeigen wir Ihnen zusätzliche Tools, die eine bessere Möglichkeit bieten, aber nicht direkt von Microsoft stammen. Der Microsoft-Treiber funktioniert darüber hinaus nur mit den 32-Bit-Versionen von Windows 7. Den Microsoft RAMdisk-Treiber erkennen Sie folgendermaßen:

1. Laden Sie sich den notwendigen Treiber von der Seite *http://support.microsoft.com/kb/257405* herunter. Der Treiber ist für Windows 2000 entwickelt, funktioniert aber auch noch in Windows 7.
2. Entpacken Sie das Archiv per Klick auf die *.exe*-Datei.
3. Starten Sie durch Eingabe von *devmgmt.msc* den Geräte-Manager.
4. Klicken Sie mit der rechten Maustaste auf den Computernamen und wählen Sie *Legacyhardware hinzufügen*.

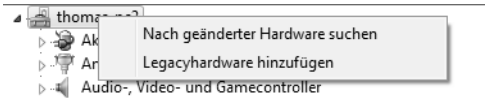


Abbildung 7.15 Hinzufügen von Hardware zu Windows 7

5. Wählen Sie auf der zweiten Seite des Assistenten die Option *Hardware manuell aus einer Liste wählen und installieren*.
6. Klicken Sie auf der nächsten Seite doppelt auf *Alle Geräte anzeigen*.

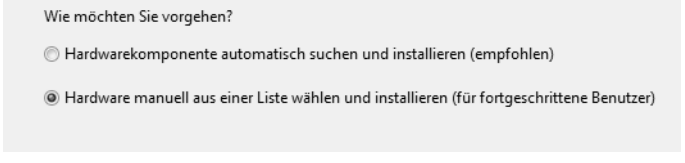


Abbildung 7.16 Manuelle Auswahl des zu installierenden Treibers

7. Klicken Sie auf *Datenträger* und navigieren Sie in das Verzeichnis, in das Sie das Archiv des Ramdisk-Treibers entpackt haben.
8. Wählen Sie die Datei *RAMDISK.INF* aus, klicken Sie auf *Öffnen* und anschließend auf *OK*.
9. Im Fenster erscheint *Ramdisk Driver.*
10. Klicken Sie zwei Mal auf *Weiter.*
11. Klicken Sie bei der Warnung *Der Herausgeber der Treibersoftware konnte nicht überprüft werden* auf *Diese Treibersoftware trotzdem installieren.*
12. Nach der erfolgreichen Installation starten Sie den Computer neu.

Abbildung 7.17 Bestätigen der Treiberwarnung

Nach der erfolgreichen Anbindung müssen Sie den Treiber noch konfigurieren. Die Einstellungen dazu lassen sich nur in der Registry vornehmen:

1. Öffnen Sie durch Eingabe von *regedit* im Suchfeld des Startmenüs den Registrierungs-Editor.
2. Navigieren Sie zu *HKLM\SYSTEM\ControlSet001\services\Ramdisk\Parameters*.
3. In diesem Bereich können Sie den Laufwerkbuchstaben anpassen und über *DiskSize* die Größe. Starten Sie den Rechner nach der Änderung neu.

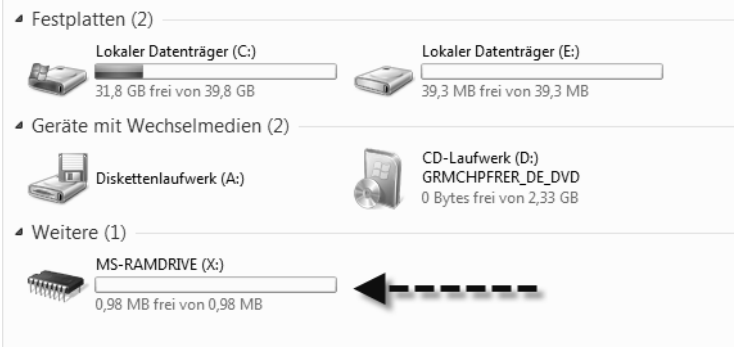


Abbildung 7.18 Verwenden der Ramdisk in Windows 7

Dataram Ramdisk

Über den Link *http://www.dataram.com/products-and-services/ramdisk/download-ramdisk* können Sie sich einen Freewaretreiber für eine Ramdisk herunterladen, die sich leichter konfigurieren lässt und vor allem vollständig kompatibel zu Windows 7 ist. Nach der Installation der *.msi*-Datei starten Sie die Konfiguration über *Ramdisk Configuration Utility*. Im Fenster können Sie festlegen, welche Größe die Ramdisk haben darf und welche Formatierung Sie verwenden möchten.

Haben Sie alle Einstellungen auf der Registerkarte *Settings* vorgenommen, klicken Sie auf *Start RAMDisk*. Anschließend steht der Datenträger über den Explorer zur Verfügung wie jeder andere Datenträger auch. Sie können die Ramdisk in der Festplattenverwaltung genauso konfi-

gurieren wie jeden anderen Datenträger auch. Die Festplattenverwaltung starten Sie am schnellsten durch Eingabe von *diskmgmt.msc* im Suchfeld des Startmenüs.

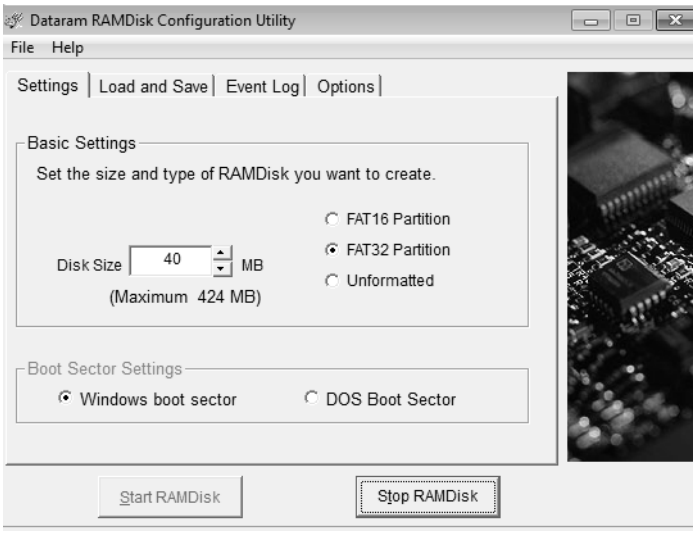


Abbildung 7.19 Konfigurieren und starten der Ramdisk

Vor allem für den schnellen Zugriff auf bestimmte Daten, zum Entpacken von Archiven oder teilweise auch der Bearbeitung von Filmen, kann die Freeware wertvolle Hilfe leisten.

Über die Registerkarte *Load and Save* können Sie das Ramdisk-Laufwerk als virtuelles Image speichern und bei jedem Start neu laden. Dazu aktivieren Sie das Kontrollkästchen *Load Disk Image at Startup*. Zusätzlich haben Sie noch die Möglichkeit, den Inhalt der Ramdisk beim Herunterfahren zu speichern. Dazu aktivieren Sie zusätzlich noch das Kontrollkästchen *Save Disk Image on Shutdown*.

Lassen Sie den Inhalt nicht speichern, löscht Windows diesen automatisch beim Neustart. Die Ramdisk bietet sich aus diesem Grund auch als Speicherort der temporären Dateien an. In vielen Programmen, zum Beispiel auch in Photoshop, können Sie Arbeitsverzeichnisse angeben, in denen das Programm temporäre Daten speichern kann. Da der Zugriff auf eine Ramdisk wesentlich schneller als der Zugriff auf eine normale Festplatte ist, beschleunigen Sie durch die Verwendung auch diese Programme.

Festplattenaktivität mit Diskmon überwachen

Die Freeware Diskmon von Microsoft-Sysinternals (*http://technet.microsoft.com/de-de/sysinternals/bb896646*) zeigt alle Schreib- und Lesevorgänge der Festplatte in einem Fenster an. Sie sehen auf diese Weise den physischen Zugriff und die aktuellen Vorgänger der Festpatte. Sie sehen die Aktion, Sektor, Zeit, Dauer und auf welcher Festplatte der Computer aktuell etwas schreibt. Sie haben die Möglichkeit, die Ausgabe auch in eine Logdatei zu speichern.

Aktivieren Sie die Funktion *Minimize to Tray Disk Light* im Menü *Options*, minimiert sich das Tool direkt in die Taskleiste und zeigt Ihnen die aktuelle Nutzung der Festplatte wie das LED-

Symbol an. Auf diese Weise sehen Sie den Festplattenzugriff. In der minimierten Ansicht sehen Sie Schreibzugriffe als rote Anzeige und Lesezugriffe als grün. Klicken Sie auf das Symbol, öffnet sich wieder die ausführliche Ansicht. Wollen Sie das Tool gleich als Symbol starten, verwenden Sie die Option *diskmon /l* (kleines L).

Damit das Tool Daten auslesen kann, müssen Sie es mit Administratorrechten starten, wenn Sie die Benutzerkontensteuerung aktiviert haben. Windows Server 2008 R2 und Windows 7 blenden das Symbol nach einiger Zeit aus. Um es dauerhaft einzublenden, klicken Sie in der Taskleiste auf die zwei kleinen Pfeile, um auch die ausgeblendeten Symbole anzuzeigen. Wählen Sie *Anpassen* und dann für das Symbol die Option *Symbol und Benachrichtigungen anzeigen*.

Um die Echtzeitanzeige zu deaktivieren, klicken Sie auf die kleine Lupe. Fahren Sie mit der Maus über ein Symbol, erhalten Sie eine kleine Hilfe zur entsprechenden Schaltfläche. Sie können innerhalb des Capture-Fensters auch nach bestimmten Einträgen suchen. Mit *History Depth* legen Sie die maximale Anzahl an Daten fest, die Sie in der grafischen Oberfläche anzeigen lassen wollen. Diskmon ermöglicht auch den Start mehrerer Instanzen. Lassen Sie das Tool zum Beispiel automatisch als LED minimiert starten, lässt es sich dennoch noch einmal parallel starten, sodass die LED aktiv bleibt, auch wenn Sie mit Diskmon arbeiten.

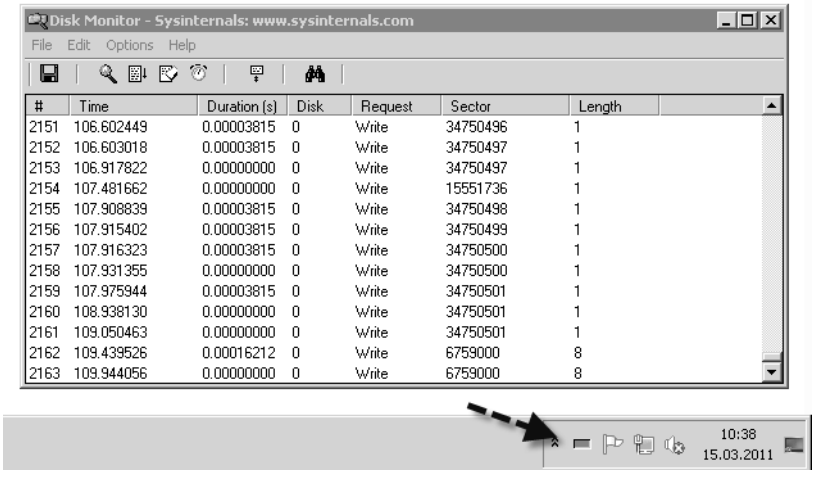


Abbildung 7.20 Festplattenzugriffe überwachen mit Diskmon

Einzelne Dateien und Verzeichnisse defragmentieren mit Contig

Sie haben in den Eigenschaften der Datenträger die Möglichkeit, komplette Datenträger zu defragmentieren. Bei diesem Vorgang fasst Windows alle Datenträgercluster, in deren Bereich die Dateien gespeichert sind, zu einem zusammenhängenden Bereich zusammen. Das beschleunigt deutlich die Leistung von Windows, da die Festplatte nicht ständig die Schreib-Lese-Köpfe neu positionieren muss.

Der Defragmentierungsvorgang des Datenträgers defragmentiert den Datenträger als Ganzes und übergeht dabei eventuell einige Dateien, für die eine Defragmentierung nicht möglich ist.

Sie haben aber auch die Möglichkeit, einzelne Dateien oder ganze Verzeichnisse zu defragmentieren, um sicherzustellen, dass der Zugriff auf diese Datei beschleunigt stattfinden kann. Dazu nutzen Sie die Microsoft-Freeware *contig.exe* von der Seite *http://technet.microsoft.com/de-de/sysinternals/bb897428*.

Das Tool defragmentiert die ausgewählte Datei und sorgt dafür, dass die Cluster der Datei auf dem Datenträger in einem aneinanderhängenden Bereich liegen. Contig verwendet die Windows-Defragmentierungstechnologie und stellt dadurch sicher, dass es nicht zu einer Datenträgerbeschädigung kommt. Das Tool arbeitet über die Eingabeaufforderung. Die Syntax dazu lautet:

```
contig [-v] [-a] [-q] [-s] [Dateiname]
```

- –v Gibt Informationen zum Vorgang aus
- –a Führt nur eine Analyse durch und defragmentiert nicht
- –s Geben Sie einen Dateinamen mit Platzhaltern an, können Sie mehrere Dateien in einem bestimmten Verzeichnis defragmentieren, zum Beispiel *contig –s c:\einkauf*.docx*
- –q Führt das Tool im stillen Modus aus, und gibt keinerlei Informationen zurück

Nach dem Start scannt Contig den Datenträger und findet dabei die Speicherorte der Datei sowie die freien Bereiche der Festplatte. Wollen Sie in einem Verzeichnis alle Dateien defragmentieren, verwenden Sie den Befehl *contig –s **.* Wollen Sie nur bestimmte Dateien defragmentieren, verwenden Sie den Befehl *contig –s *.docx*.

Schneller in der Eingabeaufforderung bewegen und navigieren

Arbeiten Sie mit der Eingabeaufforderung, können Sie schneller die verschiedenen Befehle aufrufen, wenn Sie den Anfangsbuchstaben des Verzeichnisses eingeben, zu dem Sie sich bewegen wollen, und dann die ⇆-Taste drücken. Windows vervollständigt anschließend den Befehl.

Wollen Sie zum Beispiel zum Stammverzeichnis der Partition wechseln, geben Sie den Befehl *cd* ein. Um vom Stammverzeichnis aus das Verzeichnis *Programme* zu öffnen, reicht es auch, wenn Sie *P* eingeben und so lange die ⇆-Taste drücken, bis das richtige Verzeichnis erscheint.

In der Eingabeaufforderung tragen die Verzeichnisse meistens englische Bezeichnungen, außer die Verzeichnisse, die Sie selbst erstellen.

Wollen Sie aus dem Explorer direkt einen Pfad in der Eingabeaufforderung öffnen, klicken Sie auf das Verzeichnis mit ⇧+Rechtsklick und wählen *Eingabeaufforderung hier öffnen*.

Windows Performance Toolkit – Leistungsmessung für Profis

Mit dem kostenlosen Windows Performance Toolkit von Microsoft können Sie die Leistung eines Systems sehr effizient messen. Das Tool bietet umfangreiche Möglichkeiten, Probleme auf einem System zu messen. Wir zeigen Ihnen nachfolgend erste Schritte zur Umsetzung. Ausführliche Informationen erhalten Sie auf der Seite *http://msdn.microsoft.com/en-us/performance*.

Windows Performance Toolkit und .NET Framework 4 installieren

Das Toolkit ist Bestandteil des Windows Software Development Toolkit (SDK), welches Sie kostenlos von der Seite *http://www.microsoft.com/downloads/en/details.aspx?FamilyID=35AEDA01-421D-4BA5-B44B-543DC8C33A20* herunterladen können. Sie benötigen für den Betrieb .NET Framework 4, welches Sie über die Seite *http://go.microsoft.com/fwlink/?LinkID=187668* installieren können.

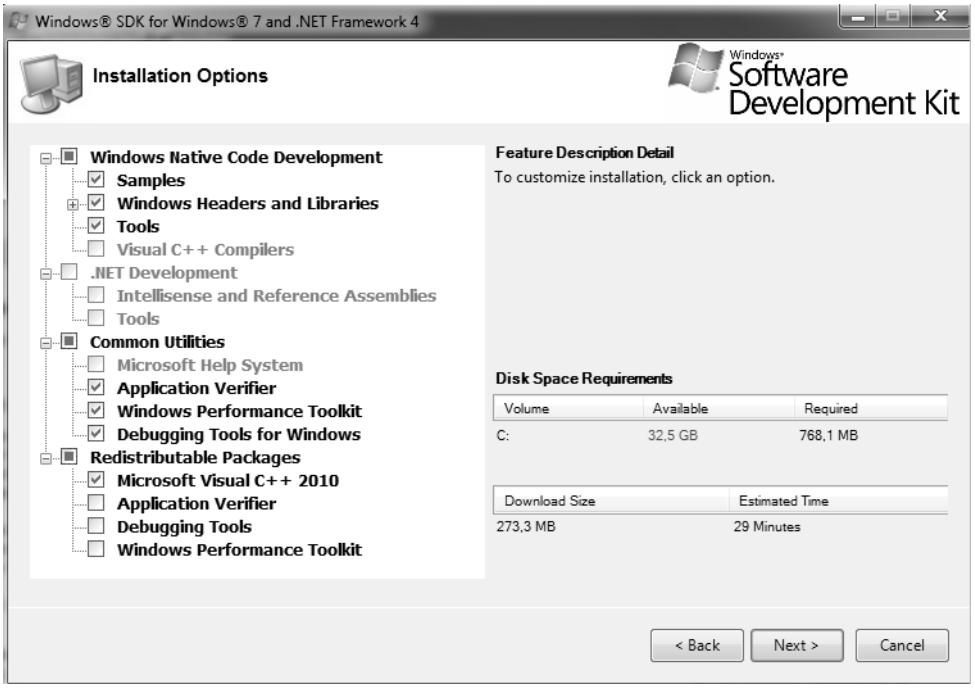


Abbildung 7.21 Installieren des Windows Software Development Kit

Leistung von Windows und dem Bootvorgang messen

Haben Sie das Windows SDK mit dem Windows Performance Toolkit installiert, können Sie einen ersten Bericht zur Systemleistung erstellen:

1. Öffnen Sie dazu eine Eingabeaufforderung mit Administratorrechten.
2. Geben Sie den Befehl *xperf –start –on diageasy* ein.
3. Anschließend läuft das Tool im Hintergrund und misst die Systemleistung.
4. Starten Sie die Programme und Tools, deren Leistung Sie messen wollen. Im Hintergrund misst das Tool die Reaktionszeiten des Computers.
5. Haben Sie alle Aufgaben durchgeführt, geben Sie den Befehl *xperf –stop* ein.

Nach dem Stoppen der Messung erhalten Sie die Meldung, dass das Windows Performance Toolkit eine Messdatei *C:\kernel.etl* erstellt hat. Neben der Messung der Verwendung der Applikationen können Sie mit dem Windows Performance Toolkit auch eine Messung des Bootvorgangs durchführen. Auch dazu benötigen Sie wieder eine Eingabeaufforderung mit Administratorrechten.

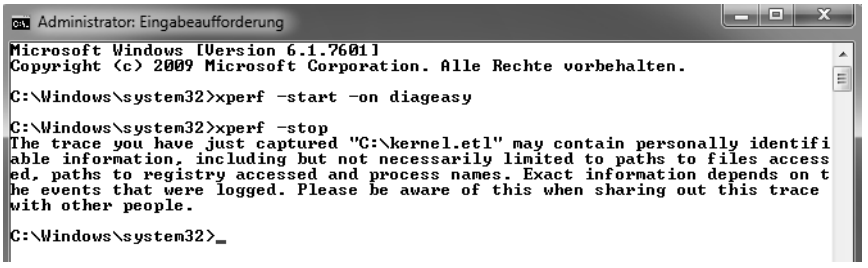


Abbildung 7.22 Erstellen einer Leistungsmessung mit *xperf*

Geben Sie dann den Befehl *xbootmgr –trace boot –resultpath c:* ein. Anschließend startet das Tool den Computer neu und misst den Bootvorgang. Auch hier speichert das Tool eine *.etl*-Datei direkt im Pfad *C:* der Festplatten.

Messdateien auswerten

Die erstellten Dateien können Sie mit dem Windows Performance Analyzer öffnen, den Sie in der Programmgruppe *Windows Performance Toolkit* finden. Um die Messungen anzuzeigen, öffnen Sie die Datei *C:\kernel.etl* oder die *.etl*-Datei des Bootvorgangs über *File/Open*.

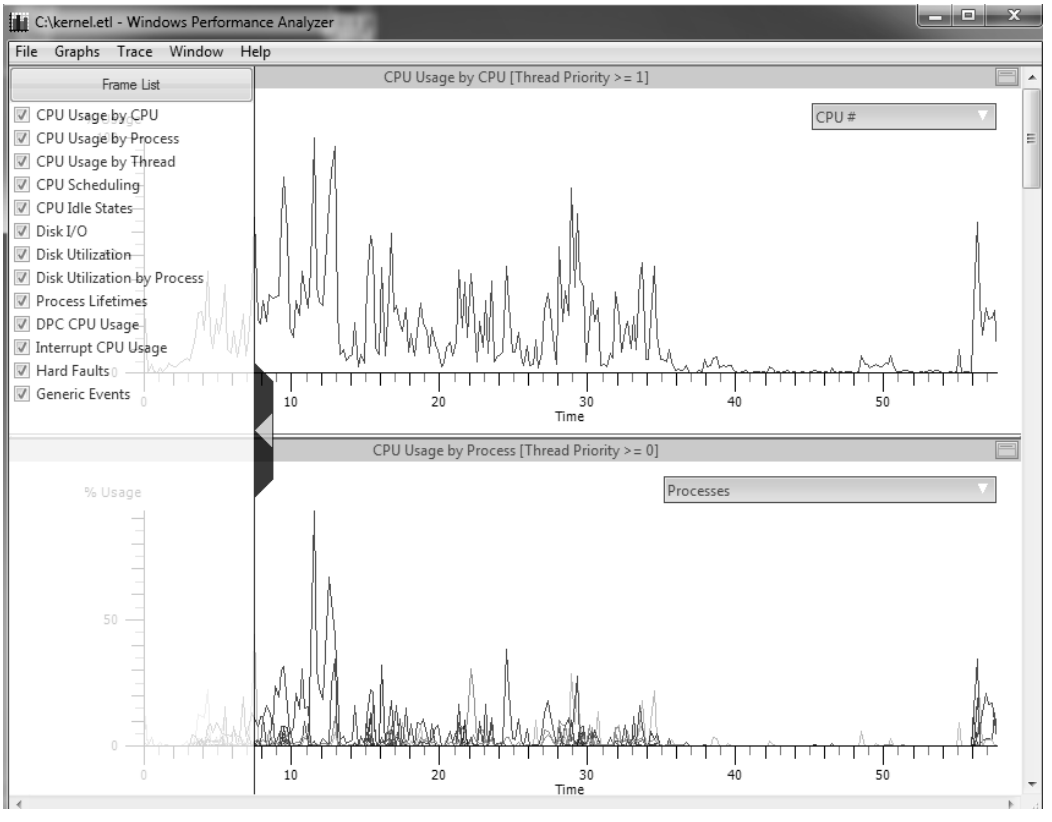


Abbildung 7.23 Anzeigen der Messdatei nach der Messung

Erhalten Sie eine Fehlermeldung beim Öffnen der Bootmessdatei, öffnen Sie diese in einer Eingabeaufforderung über den Befehl *xperfview <Pfad und Name der Datei> –tti*.

Die Anzeige der verschiedenen Bereiche blenden Sie über den Menübereich ein, den Sie durch Anklicken des linken Teils des Fensters einblenden. Klicken Sie auf die Grafik, können Sie zu Teilen der Anzeige heranzoomen, um genauere Ergebnisse zu erhalten. Dazu markieren Sie den Bereich mit der Maus, den Sie zoomen wollen, und klicken diesen mit der rechten Maustaste an. Mit dem Menübefehl *Zoom to Selection* starten Sie den Zoomvorgang.

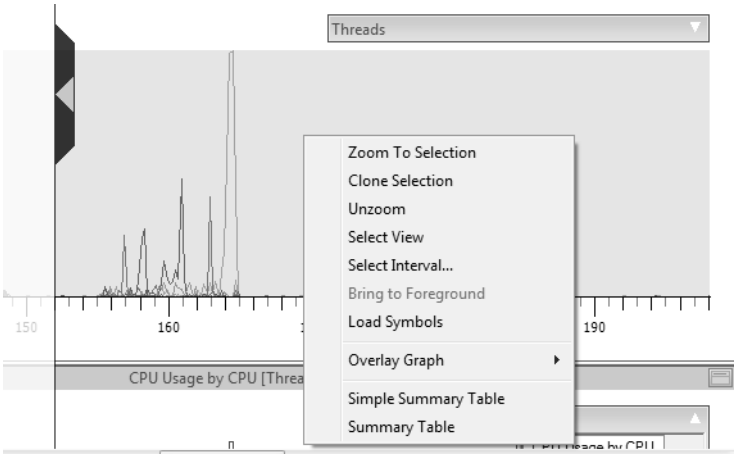
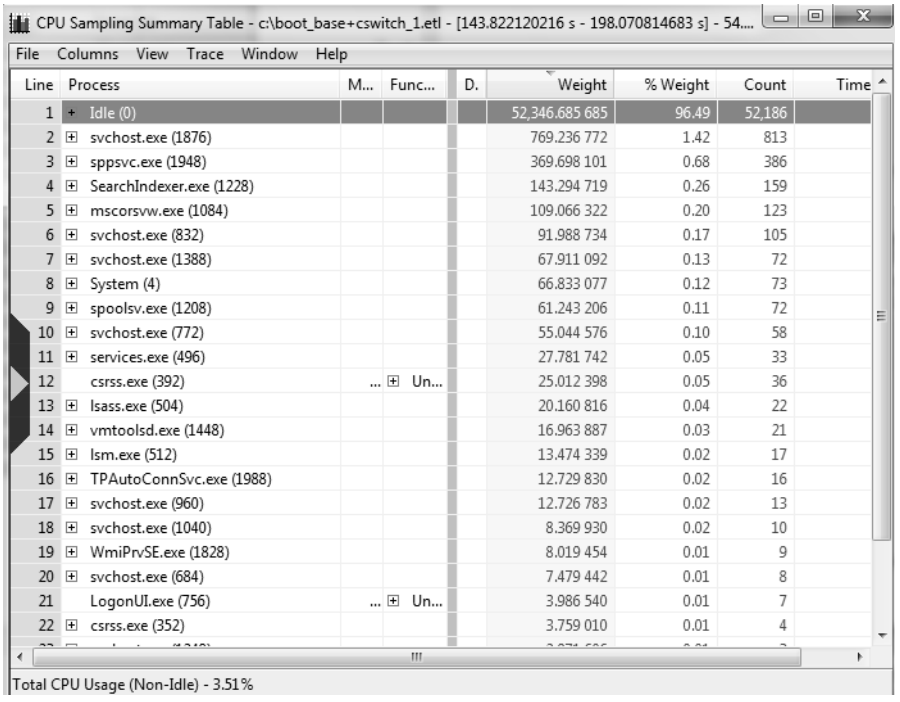


Abbildung 7.24 Zoomen der Anzeige

Neben Grafiken können Sie auch Tabellen anzeigen, indem Sie im Kontextmenü die Option *Summary Table* auswählen. Um eine übersichtliche Anzeige zu erhalten, entfernen Sie das Häkchen bei allen Optionen der linken Seite, die Sie nicht anzeigen wollen.

Lassen Sie sich zum Beispiel beim Messen des Bootvorgangs nur die *CPU Usage by Process* anzeigen, sehen Sie, wie viel CPU-Last die einzelnen Prozesse verursachen. Mit *Disk I/O* sehen Sie die Festplattenzugriffe.



Line	Process	M...	Func...	D.	Weight	% Weight	Count	Time
1	Idle (0)				52,346.685 685	96.49	52,186	
2	svchost.exe (1876)				769.236 772	1.42	813	
3	sppsvc.exe (1948)				369.698 101	0.68	386	
4	SearchIndexer.exe (1228)				143.294 719	0.26	159	
5	mscorsvw.exe (1084)				109.066 322	0.20	123	
6	svchost.exe (832)				91.988 734	0.17	105	
7	svchost.exe (1388)				67.911 092	0.13	72	
8	System (4)				66.833 077	0.12	73	
9	spoolsv.exe (1208)				61.243 206	0.11	72	
10	svchost.exe (772)				55.044 576	0.10	58	
11	services.exe (496)				27.781 742	0.05	33	
12	csrss.exe (392)	...	Un...		25.012 398	0.05	36	
13	lsass.exe (504)				20.160 816	0.04	22	
14	vmtoolsd.exe (1448)				16.963 887	0.03	21	
15	lsm.exe (512)				13.474 339	0.02	17	
16	TPAutoConnSvc.exe (1988)				12.729 830	0.02	16	
17	svchost.exe (960)				12.726 783	0.02	13	
18	svchost.exe (1040)				8.369 930	0.02	10	
19	WmiPrvSE.exe (1828)				8.019 454	0.01	9	
20	svchost.exe (684)				7.479 442	0.01	8	
21	LogonUI.exe (756)	...	Un...		3.986 540	0.01	7	
22	csrss.exe (352)				3.759 010	0.01	4	

Abbildung 7.25 Anzeigen einer Tabelle der Leistungsmessung

Start- und Herunterfahrzeit von Windows 7 messen und Zuverlässigkeit anzeigen

Führen Sie bestimmte Tuningmaßnahmen in Windows 7 durch, ist es sinnvoll zu erfahren, wie sich diese für den Systemstart auswirken. Den Zeitraum, den Windows zum Starten braucht, hält das Betriebssystem in der Ereignisanzeige fest. Auf folgendem Weg zeigen Sie den Zeitraum an:

1. Geben Sie *eventvwr* im Suchfeld des Startmenüs ein.
2. Navigieren Sie zu *Anwendungs- und Dienstprotokolle/Microsoft/Windows/Diagnostics-Performance/Betriebsbereit*.
3. Ereignisse mit der ID 100 zeigen die Startdauer an, Ereignisse mit der ID 200 die Dauer zum Herunterfahren.

Geben Sie den Begriff *zuverlässigkeit* im Suchfeld des Startmenüs ein, erstellt Windows 7 einen Bericht, über den Sie Fehler und Informationen zum Betriebssystem schnell und einfach anzeigen können. Sie sehen einen Index der Systemleistung und erhalten zusätzliche Informationen, wenn Sie eine Meldung anklicken.

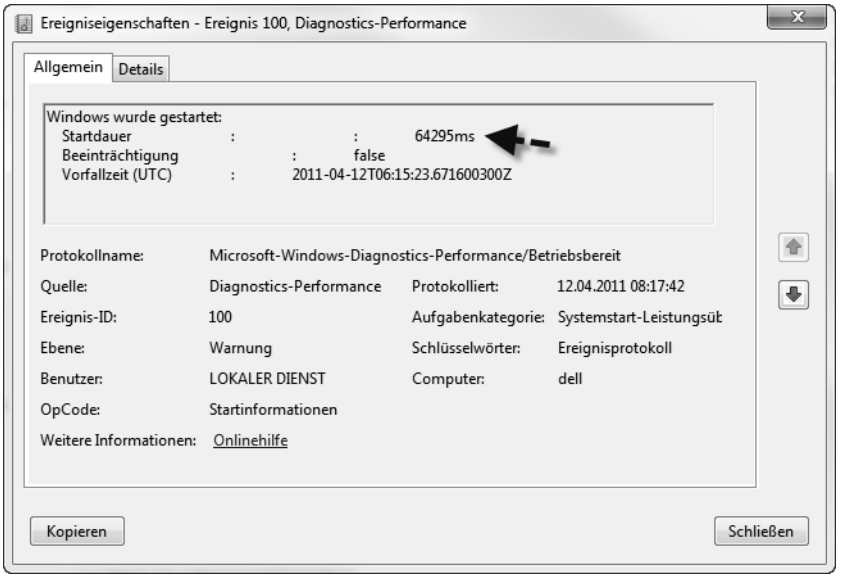


Abbildung 7.26 Windows 7 misst die Start-Zeit des Betriebssystems

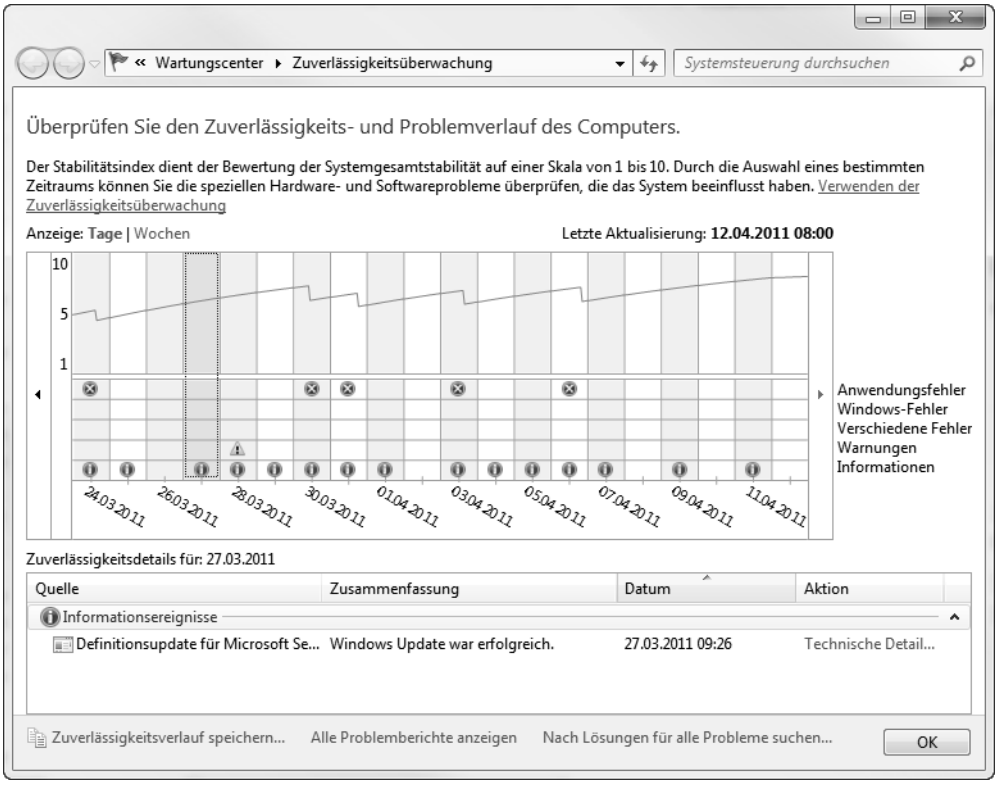


Abbildung 7.27 Anzeigen eines Zuverlässigkeitsberichts in Windows 7

Windows System State Analyzer – Änderungen in Windows nachverfolgen

Installieren Sie eine Anwendung auf einem Computer, führt diese in den meisten Fällen sehr viele Änderungen an Systemdateien, Verzeichnissen und der Registry durch. Microsoft bietet eine kostenlose Zusatztool-Sammlung an, mit der Sie diese Änderungen sehr leicht nachvollziehen können. Sie können sich den Windows System State Analyzer (WSSA) über das Software Certification Toolkit installieren. Dieses steht in einer 32-Bit- und einer 64-Bit-Version zur Verfügung.

WSSA 32-Bit *http://go.microsoft.com/fwlink/?LinkID=140110*

WSSA 64-Bit *http://go.microsoft.com/fwlink/?LinkID=140109*

Der WSSA ist nur ein Bestandteil des Software Certification Toolkit. Sie müssen für die Verwendung nicht das komplette Toolkit installieren.

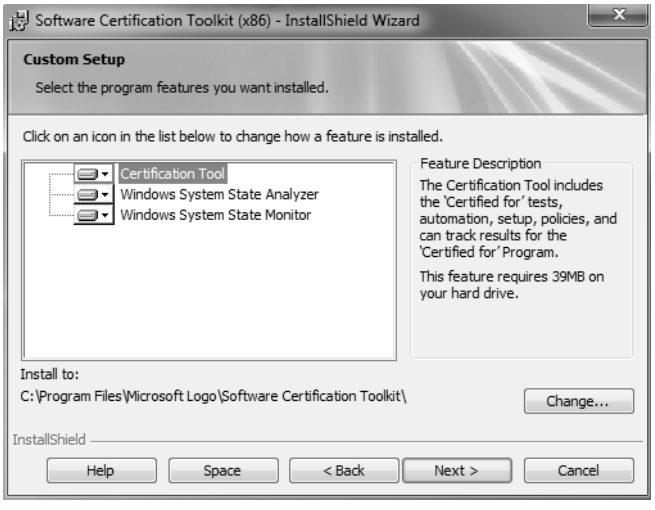


Abbildung 7.28 Installieren des WSSA

Snapshots mit WSSA erstellen

Haben Sie Windows System State Analyzer (WSSA) auf einem Computer installiert, erstellen Sie vor einer Systemänderung zunächst einen Snapshot:

1. Starten Sie Windows System State Analyzer.
2. Aktivieren Sie die Registerkarte *Snapshot*.
3. Belassen Sie die Option *Create New*.
4. Legen Sie den Pfad fest, in dem Windows den Snapshot speichern soll.
5. Klicken Sie auf *Start*.

Windows erstellt jetzt einen Schnappschuss. Anschließend installieren Sie die Anwendung, deren Änderungen Sie überwachen wollen. Lassen Sie den WSSA dabei geöffnet. Haben Sie die

Anwendung installiert, klicken Sie auf der rechten Seite auf die Option *Create New*. Wählen Sie auch hier den Pfad aus. In WSSA liegt jetzt ein Schnappschuss vor und nach der Installation einer Anwendung vor. Der nächste Schritt besteht darin, die Snapshots zu vergleichen.

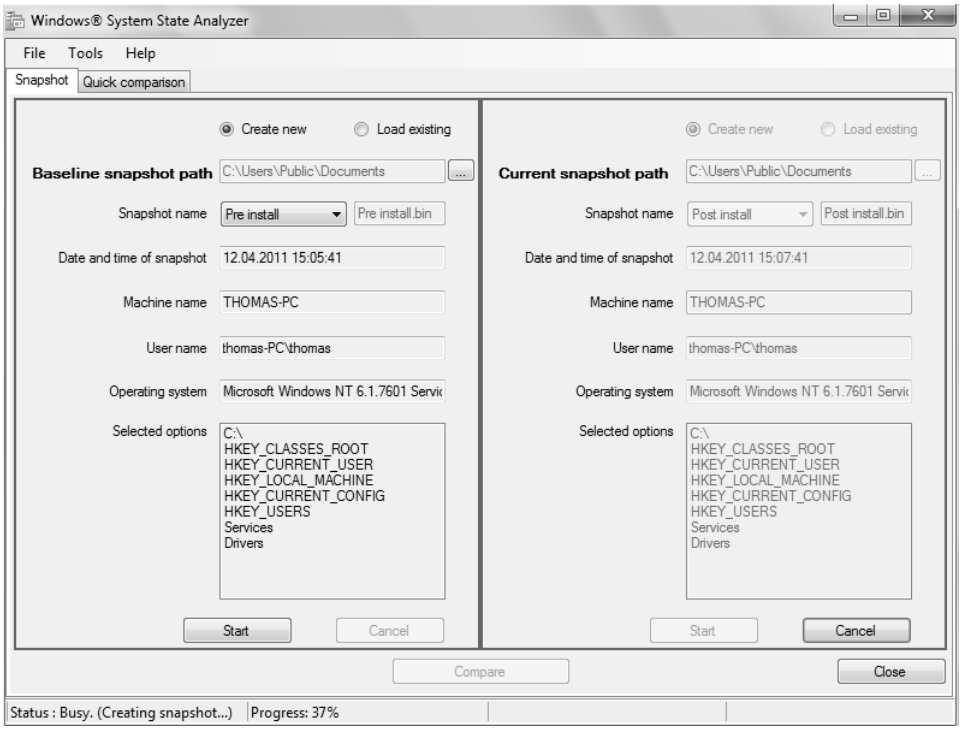


Abbildung 7.29 Erstellen von Snapshots mit WSSA vor und nach einer Softwareinstallation

Systemänderungen mit Windows System State Analyzer anzeigen

Haben Sie vor und nach der Installation einer Anwendung einen Snapshot erstellt, besteht der nächste Schritt darin, dass Sie diese miteinander vergleichen. Dazu wechseln Sie entweder zur Registerkarte *Quick comparison* oder klicken auf die Schaltfläche *Compare*.

Sobald Sie die Schaltfläche *Compare* geklickt haben, beginnt WSSA mit der Analyse der beiden Snapshots und zeigt anschließend sehr detailliert die Änderungen an. Im neuen Fenster zeigt das Tool die Änderungen strukturiert nach Dateisystem, Registry, Dienste und Treiber.

Windows-Prozesse, -Dienste und -Treiber im Griff

Microsoft bietet über *www.sysinternals.com* zahlreiche kostenlose Tools an, welche die Analyse von Computern vereinfachen. Sie können mit den verschiedenen Tools Windows 7-Computer, aber auch Windows Server 2008 R2 effizient analysieren und erhalten einen Überblick über die aktuell gestarteten Prozesse und Anwendungen.

Dateisystem, Registry und Prozesse überwachen – Process Monitor

Die Überwachung laufender Prozesse auf einem Computer oder Server sind vor allem im Bereich der Sicherheit und Systemstabilität ein wichtiger Bestandteil. Mit dem Process Monitor (*http://technet.microsoft.com/de-de/sysinternals/bb896645*) von Sysinternals können Sie in einer grafischen Oberfläche ausführlich und in Echtzeit alle Aktivitäten im Dateisystem, der Registry und der Prozesse/Threads überwachen sowie farblich markieren. Über Schaltflächen aktivieren Sie die einzelnen Überwachungsfunktionen durch einen Klick oder schalten diese wieder aus.

Abbildung 7.30 Aktivieren und deaktivieren verschiedener Überwachungsmöglichkeiten im Process Monitor

Auf diese Weise können Sie die Überwachung der Registry- und der Dateisystemzugriffe sowie die Abfrage der Prozessaktivität steuern und jeweils nur den Bereich überwachen, der Sie interessiert. Lassen Sie alle Optionen überwachen, kann das Fenster schnell übersichtlich werden.

Das Programm ist voll transportfähig (zum Beispiel auf USB-Sticks), das gilt übrigens für alle Tools von Sysinternals. Das Programm läuft auf Windows 2000/XP/2003/2008 und Windows Vista sowie auf allen 64-Bit-Versionen dieser Betriebssysteme. Auch Windows 7 und Windows Server 2008 R2 arbeiten problemlos mit dem Tool, das gilt auch für Small Business Server 2011.

Sie erhalten umfassende Daten zu allen gestarteten und beendeten Prozessen und Threads. Auch der Aufbau von TCP/IP-Verbindungen und der UDP-Verkehr, also der Netzwerkverkehr des Servers, lassen sich überwachen. Allerdings speichert der Process Monitor nicht den Inhalt der TCP-Pakete, sodass sich keine Daten auslesen lassen, sondern nur die reine Funktionalität des Netzwerks. Dazu kommt, dass der Fokus des Tools nicht im Bereich der Netzwerküberwachung liegt. Auf Wunsch kann Process Monitor mehr Informationen zu laufenden Prozessen anzeigen, zum Beispiel die zum Prozess gehörenden *.dll*-Dateien. Sie können durch Filter die Anzeige anpassen und unnötige Informationen ausblenden oder den Fokus auf spezielle Daten legen.

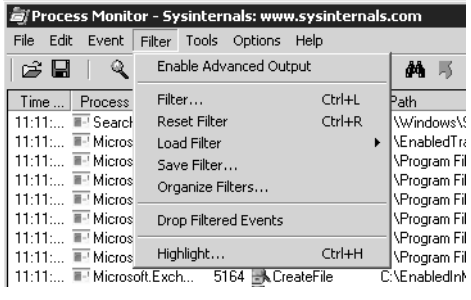


Abbildung 7.31 Verwenden von Filtern für Process Monitor

Im Menü *Tools* stehen verschiedene Ansichten zur Verfügung. Das Tool kann auch den Bootvorgang von Computern überwachen, da es sehr früh startet. Alle Ergebnisse lassen sich dabei in eine Datei umleiten. Kann Windows nicht starten, lässt sich durch Analyse dieser Datei der Fehler schnell finden. Wie alle Sysinternals-Tools ist der Umgang sehr einfach und erfordert keine komplexe Einarbeitung.

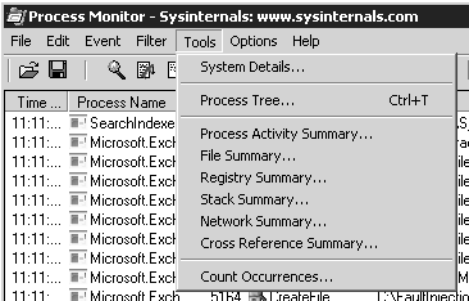


Abbildung 7.32 Anpassen der Ansichten im Process Monitor

Haben Sie die Anzeige angepasst, lassen sich die Daten über das Menü *File* speichern. Auf einem anderen Rechner können Sie die Datei laden und Filter setzen sowie das Ergebnis durchsuchen, genauso wie auf dem Quell-Rechner.

Neben der Möglichkeit, die aktuelle Ausgabe zu speichern, haben Sie auch die Möglichkeit, über *File/Export Configuration* die Einstellungen des Tools zu exportieren. Im Menü steht dazu auch der *Import*-Befehl zur Verfügung. Klicken Sie doppelt auf einen Eintrag, öffnet sich ein Fenster mit weiteren Informationen, die sehr detailliert die Arbeit des Prozesses und die dabei verwendeten Dateien ausgibt. Klicken Sie im Informationsfenster wiederum auf eine der beteiligten Dateien des Prozesses, können Sie von dieser Datei Informationen anzeigen lassen, zum Beispiel Version und Speicherort.

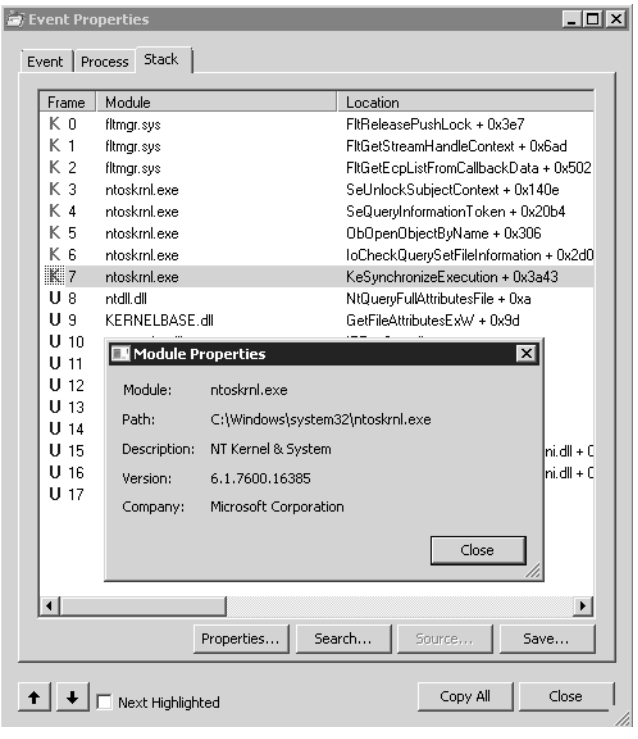


Abbildung 7.33 Anzeigen weiterer Informationen zu Prozessen und beteiligten Dateien

Die Details eines Prozesses können Sie ebenfalls als *.csv*-Datei abspeichern, um diese später weiter zu analysieren. Wie bei Autoruns (siehe Seite 250) haben Sie auch im Process Monitor die Möglichkeit, über das Kontextmenü eine Onlinesuche zum ausgewählten Prozess durchzuführen. Über das Kontextmenü können Sie einen Prozess und dessen Ausgabe auch farblich hervorheben.

Über das Kontextmenü eines Prozesses können Sie alle überwachten Vorgänge, die vor dem Prozess stattgefunden haben, ausblenden lassen, indem Sie die Option *Exclude Events Before* auswählen. Weitere Möglichkeiten im Kontextmenü sind das Einblenden nur eines einzelnen Prozesses und der Vorgänge, die dieser durchführt. Filter erstellen Sie über den Menübefehl *Filter/Filter*. Bestandteil des Downloadpakets ist eine englischsprachige Hilfedatei, die beim Umgang mit dem Tool hilft.

Der bessere Taskmanager – Process Explorer

Ein wichtiges Tool für die Analyse der laufenden Prozesse auf einem Computer ist der Process Explorer (*http://technet.microsoft.com/de-de/sysinternals/bb896653*) von Sysinternals. Process Explorer zeigt Prozesse in einem Fenster und darunter weitere Informationen zum aktuellen Prozess an, zum Beispiel den aktuellen Zugriff auf Verzeichnisse.

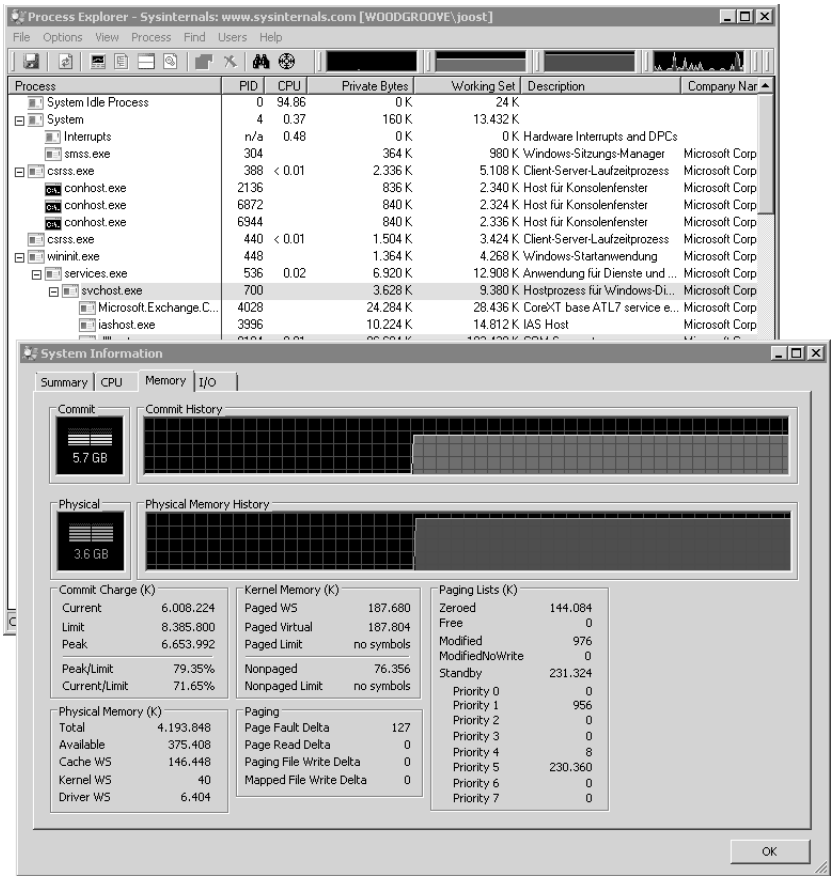


Abbildung 7.34 Systemüberwachung mit dem Process Explorer

Das Tool enthält wesentlich mehr Informationen als der Task-Manager in Windows. Klicken Sie auf die Messfenster im oberen Bereich, blendet der Process Explorer ein Systeminformationsfenster ein, welches ähnliche Informationen enthält, wie der Task-Manager, diese aber viel umfangreicher auf verschiedenen Registerkarten darstellt.

Über *Options/Replace Task Manager* können Sie den Standard-Task-Manager in Windows ersetzen. Rufen Sie diesen zukünftig auf, zum Beispiel über das Kontextmenü der Taskleiste, startet direkt der Process Explorer. Auf dem gleichen Weg können Sie diese Option wieder rückgängig machen. Über *View/Show Lower Pane* blenden Sie den unteren Bereich des Übersichtsfenster ein. Anschließend können Sie über *View/Lower Pane View* konfigurieren, ob Sie im unteren Bereich die DLLs der Prozesse anzeigen wollen oder Handles. Über das Menü *Process* können Sie ausgewählte Prozesse beenden, neu starten oder deren Eigenschaften anzeigen.

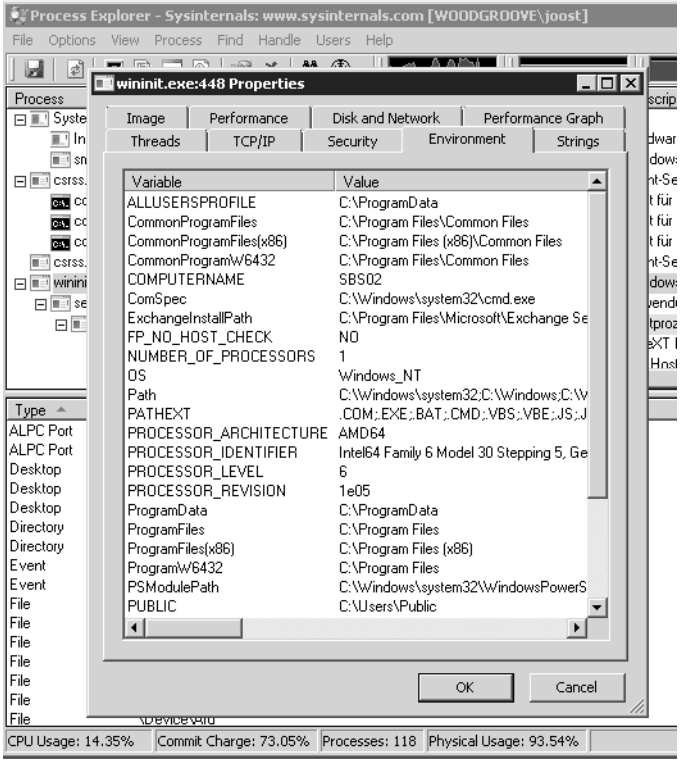


Abbildung 7.35 Anzeigen detaillierter Informationen zu einem Prozess

Daten des Task-Mangers in Excel einlesen – TaskManager.xls

Zur Fehlersuche und Analyse reicht es nicht immer aus, die Daten im Task-Manager oder Zusatztools einzulesen. Hier stellt die Excel-Tabelle *Taskmanager.xls* von der Seite *http://blog.didierstevens.com* eine wertvolle Hilfe dar. Starten Sie die Tabelle in Excel, können Sie einfach die aktuellen Prozesse und deren Daten aus dem Task-Manager in Excel einlesen.

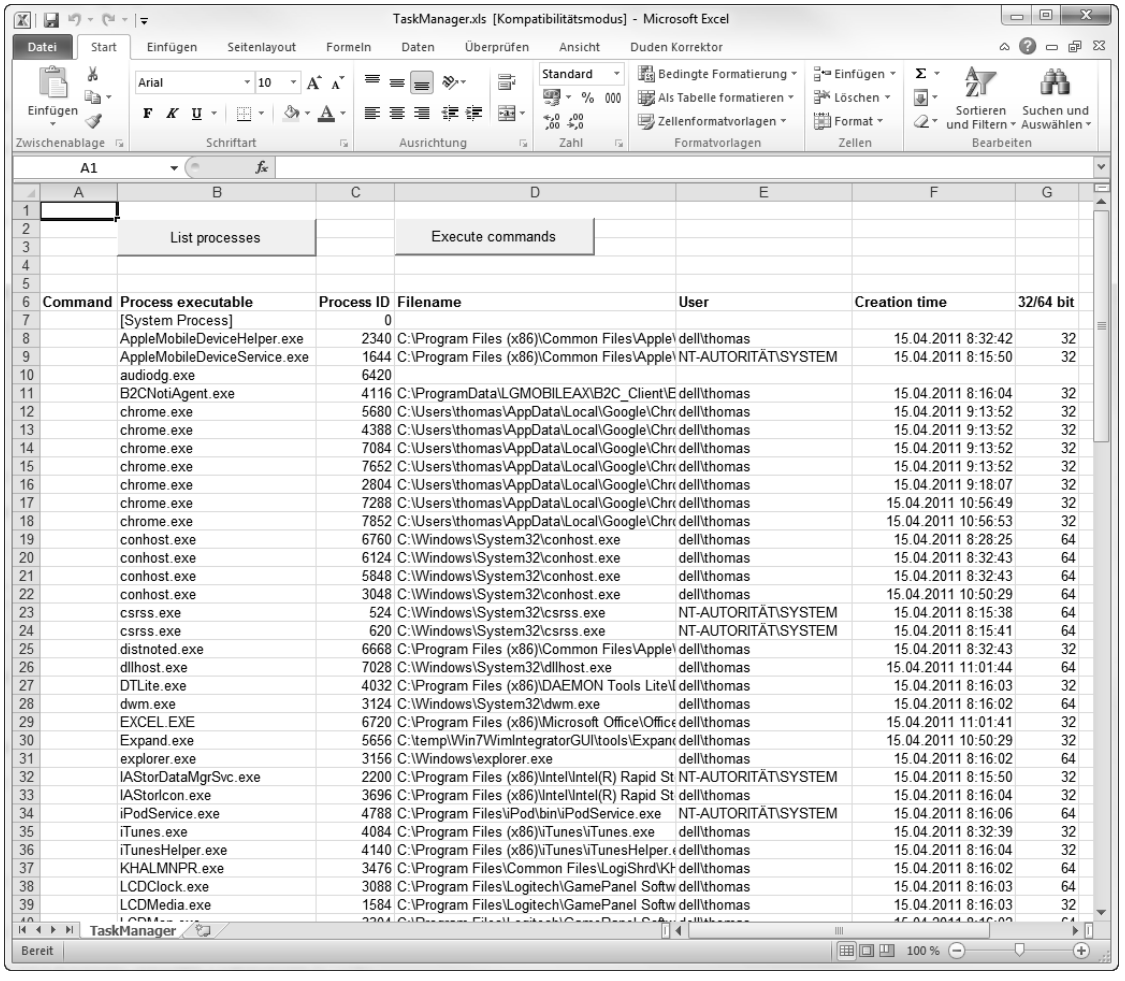


Abbildung 7.36 Einlesen der Datei des Task-Managers in die Excel-Tabelle zur Analyse

Geladene *.dll*-Dateien anzeigen – ListDLLs

Wollen Sie auf einem Computer alle geladenen *.dll*-Dateien (DLL steht für Dynamic Link Library, Dynamische Verbindungsbibliothek) anzeigen, ist ListDLLs (*http://technet.microsoft.com/de-de/sysinternals/bb896656*) von Sysinternals das aktuell beste Werkzeug dazu.

Das Befehlszeilentool zeigt Ihnen in Echtzeit alle *.dll*-Dateien an, die derzeit auf dem Server gestartet sind. Sie sehen den Versionsstand der Datei sowie den genauen Speicherort. Wollen Sie die Ausgabe in eine Textdatei umleiten, verwenden Sie zum Beispiel den Befehl *listdlls >c:\temp\dll.txt*.

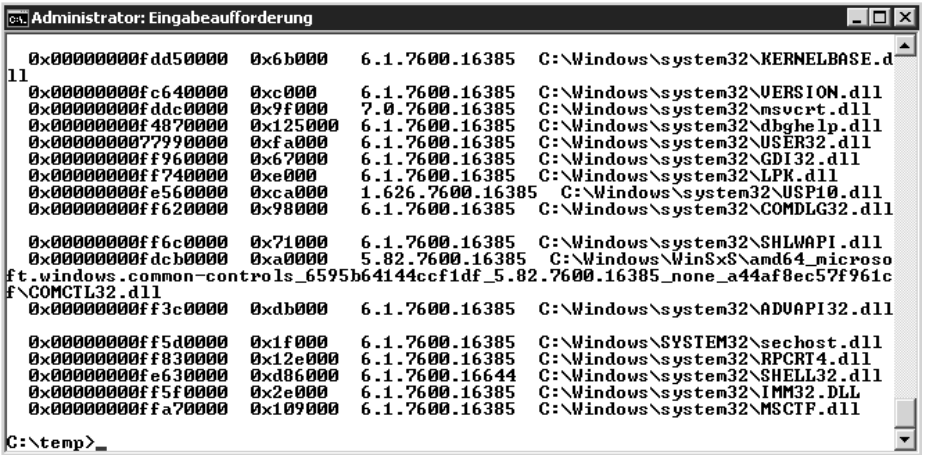


Abbildung 7.37 Anzeigen der geladenen *.dll*-Dateien eines Computers

Das Tool hat keinerlei komplexe Optionen, sondern soll lediglich schnell und einfach *.dll*-Dateien anzeigen. Sie können die Anzeige auch auf Basis geladener Prozesse anzeigen. Dazu verwenden Sie den Befehl:

```
listdlls <Name oder Teil des Namens des Prozesses oder dessen PID>
```

Anschließend zeigt ListDLLs nur die Daten und geladenen *.dll*-Dateien dieses Prozesses an.

Sie haben auch in der PowerShell die Möglichkeit, Prozesse zu verwalten, ohne auf Sysinternals-Tools zu setzen. Über das Cmdlet *Get-Process* können Sie sich alle laufenden Prozesse eines Computers anzeigen lassen. Wollen Sie aber zum Beispiel nur alle Prozesse mit dem Anfangsbuchstaben »S« angezeigt bekommen, geben Sie den Befehl *Get-Process s** ein. Sollen die Prozesse zusätzlich noch sortiert werden, zum Beispiel absteigend nach der CPU-Zeit, geben Sie *Get-Process s** gefolgt von der Pipeoption *|Sort-Object cpu –descending* ein.

Systemtreiber anzeigen – LoadOrder, DriverQuery und Driverview.exe

Mit dem Tool LoadOrder (*http://technet.microsoft.com/de-de/sysinternals/bb897416*) lassen Sie sich die geladenen Systemdateien und die Reihenfolge des Ladens in einer grafischen Oberfläche anzeigen. Starten Sie das Tool, liest es die Startreihenfolge der geladenen Treiber ein. In neuen Windows-Betriebssystemen können natürlich weitere Plug & Play-Treiber im laufenden Betrieb dazukommen, da Windows diese erst bei Bedarf nachlädt. LoadOrder zeigt die Treiber an, die Windows immer bei jedem Systemstart lädt.

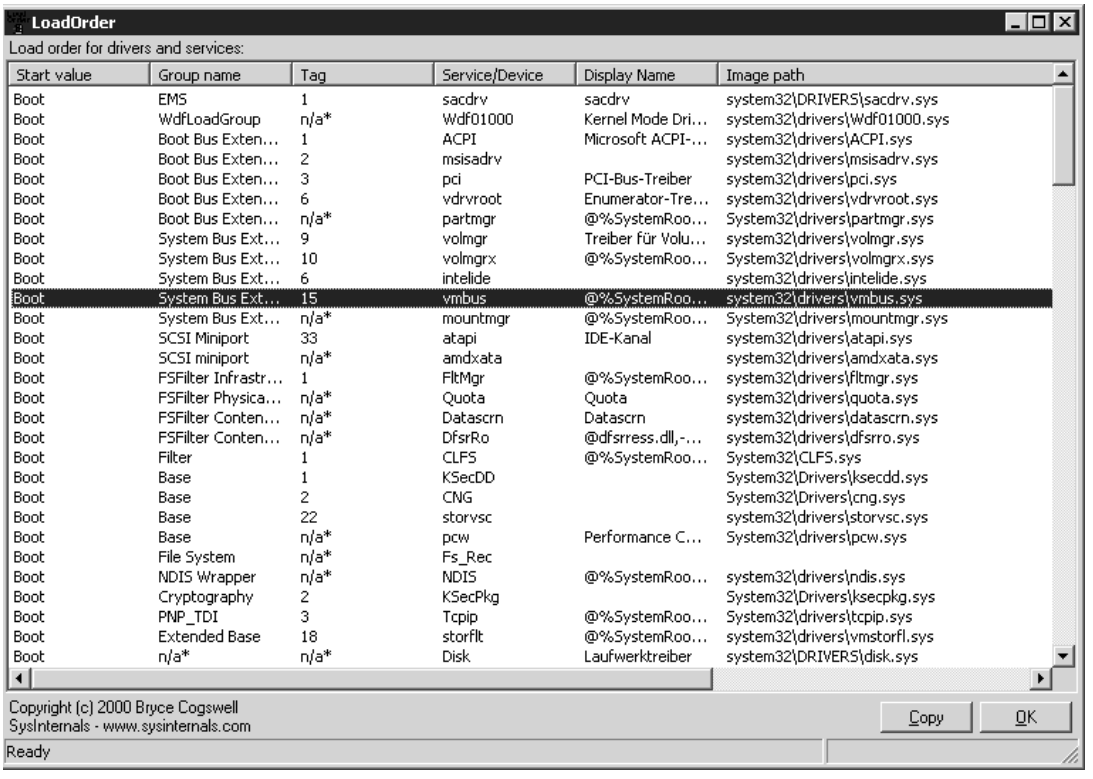


Abbildung 7.38 Anzeigen der Systemtreiber eines Servers und die Reihenfolge des Ladevorgangs

Sie haben die Möglichkeit, diese Liste auch in die Zwischenablage zu kopieren und dadurch zu Analysezwecken zu versenden. Eigentlich ist das Tool nur für Windows NT oder Windows 2000 geeignet. Es lassen sich aber auch Treiber für die aktuellen Microsoft-Betriebssysteme anzeigen. Hier ist die Ansicht aber nicht immer vollständig, zeigt aber zumindest einen Überblick über die Reihenfolge des Treiberstarts.

Nirsoft bietet ebenfalls ein Tool zur Anzeige von geladenen Treibern an. Da dieses etwas aktueller ist und auch Windows 7 unterstützt, bietet sich eine zusätzliche Verwendung des Tools an. Mit DriverView von der Seite *http://www.nirsoft.net/utils/driverview.html* können Sie ohne Installation die Treiber auslesen. Sie müssen das Tool lediglich aufrufen, daher eignet es sich auch für den Start über USB-Sticks.

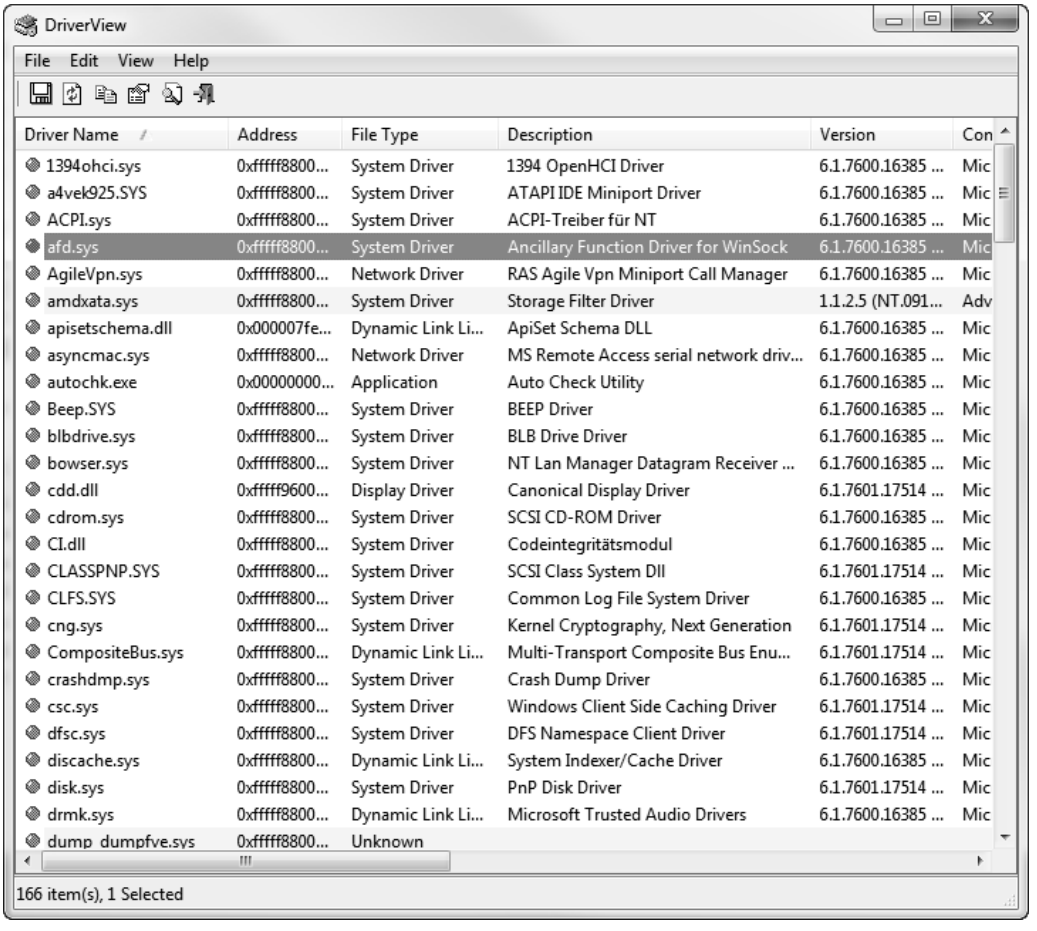


Abbildung 7.39 Anzeigen geladener Treiber mit *DriverView.exe*

Windows 7 verfügt auch über ein internes Tool in der Eingabeaufforderung, mit dem Sie die geladenen Treiber anzeigen können. Dieses starten Sie durch Eingabe von *driverquery*. Mit dem Befehl *driverquery >C:\temp\driver.txt* können Sie die Ausgabe in eine Datei umleiten lassen.

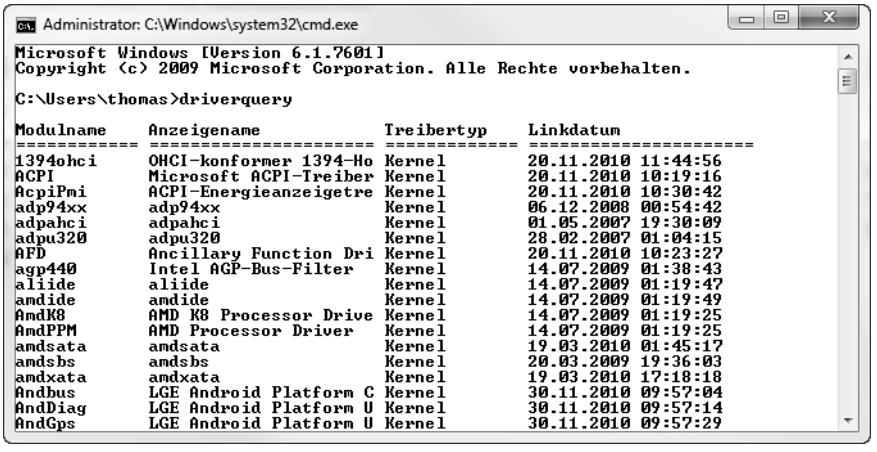


Abbildung 7.40 Anzeigen geladener Treiber in der Eingabeaufforderung

Sysinternals und Co. – Tools für die Sicherheit, Optimierung und Analyse

Neben verschiedenen Analysetools bietet Microsoft mit den kostenlosen Sysinternals-Tools von der Seite *www.sysinternals.com* auch zahlreiche Werkzeuge, mit denen sich die Sicherheit und Geschwindigkeit von Windows 7-Computern verbessern lassen. Die Tools funktionieren auch in anderen Windows-Versionen und auch in Windows Server 2008 R2. Sie können die Tools auch online starten oder direkt herunterladen, wenn Sie die URL *http://live.sysinternals.com/tools* aufrufen.

Automatisch anmelden mit Autologon

Das Anmelden mit einem Benutzerkonto ist nicht immer für die Sicherheit notwendig. Das ist zum Beispiel dann der Fall, wenn Sie am entsprechenden Rechner alleine arbeiten und kein anderer Anwender Zugriff hat. In diesem Fall ist die Anmeldung oft störender als dass sie die Sicherheit erhöht.

Microsoft bietet daher das Sysinternals-Tool Autologon an (*http://technet.microsoft.com/de-de/sysinternals/bb963905*), mit dem Sie schnell und einfach eine automatische Anmeldung an Computern konfigurieren können.

Das Tool verfügt über eine grafische Oberfläche. Nach dem Start wird Ihnen ein Fenster angezeigt, in das Sie den Benutzernamen, das Kennwort und die Domäne oder den Rechnernamen eingeben, mit der zukünftig der Computer automatisch starten soll.

Klicken Sie auf *Enable*, ist die automatische Anmeldung aktiviert. Wollen Sie diese wieder ausschalten, starten Sie das Tool erneut und klicken auf die Schaltfläche *Disable*.

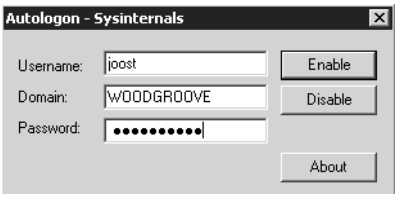


Abbildung 7.41 Konfigurieren der automatischen Anmeldung an einem Computer

Das Tool installiert keine Erweiterungen auf dem Computer, sondern ändert lediglich Einträge in der Registry. Das Kennwort verschlüsselt das Tool, es ist aus der Registry nicht auslesbar.

Autostartprogramme entdecken und entfernen – Autoruns

Automatisch startende Programme sind der maßgebliche Grund für ein langsam startendes Windows, Viren und mangelnder Systemleistung. Autoruns *(http://technet.microsoft.com/de-de/sysinternals/bb963902*) ist ein sehr effizientes Werkzeug, das es ermöglicht, alle automatisch startenden Programme in Windows zu entdecken und bei Bedarf zu deaktivieren oder Einträge zu löschen.

Halten Sie bei der Anmeldung die ⇧-Taste gedrückt, lädt Windows die Autostartprogramme nicht, die über *Alle Programme/Autostart* starten würden. Allerdings sind das die wenigsten. Die meisten Tools binden sich direkt in die Registry ein, um automatisch zu starten. Starten Sie durch Eingabe von *msconfig* im Suchfeld des Startmenüs die Systemkonfiguration, sehen Sie auf der Registerkarte *Systemstart* ebenfalls Autostartprogramme und können diese deaktivieren oder ganz löschen. Sie sehen hier Autostartprogramme der verschiedenen Stellen in der Registry, aber ebenfalls wiederum nicht alle Programme. Autoruns zeigt alle Autostartprogramme an, auch die, welche über die Registry starten.

Sie müssen das Tool nicht installieren, sondern können es direkt starten. Auf der Registerkarte *Everything* sehen Sie verschiedene Bereiche, über die Windows Programme startet. Wichtig ist auch die Registerkarte *Logon*. Hier sehen Sie die Einträge, die bei Benutzeranmeldungen starten. Vor allem Verwaltungswerkzeuge für verschiedene Hardwaregeräte wie Grafikkarten, Soundkarten oder Tastaturen lassen sich meist deaktivieren.

Entfernen Sie zunächst nur das Häkchen, wenn Sie nicht gleich den ganzen Eintrag löschen wollen. Manche Geräte benötigen das Verwaltungsprogramm jeweils für bestimmte Spezialfunktionen. Entfernen Sie alle unnötigen Programme und Zusatztools aus dem Autostart. Weitere Einträge können Sie leicht selbst erkennen, da Autoruns diese auch mit Symbolen anzeigt. Denken Sie daran, dass jedes gestartete Programm CPU-Zeit und Arbeitsspeicher verbraucht.

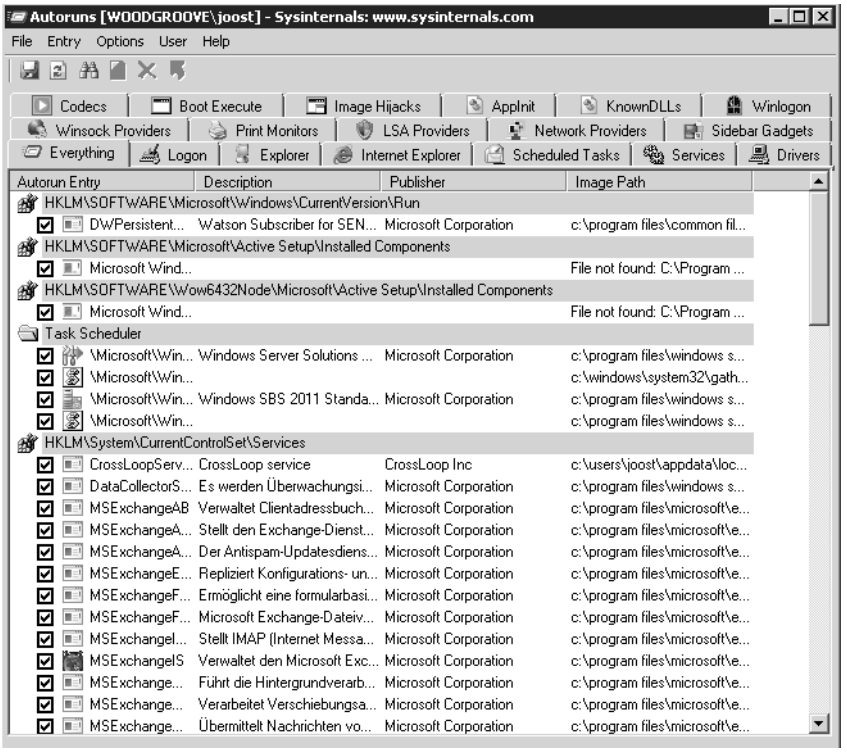


Abbildung 7.42 Entfernen unnötiger Programme mit Autoruns

Mit *Options/Hide Windows Entries* blenden Sie Systemeinträge direkt von Windows aus. Das erhöht deutlich die Übersicht und verhindert, dass Sie versehentlich Windows beeinträchtigen. Zusätzlich enthält der Download auch das Befehlszeilentool Autorunsc, mit dem Sie Einträge in der Eingabeaufforderung überwachen können. Wie für die meisten Sysinternals-Tools gibt es auch für Autoruns ein eigenes Forum (*http://forum.sysinternals.com/forum16.html*).

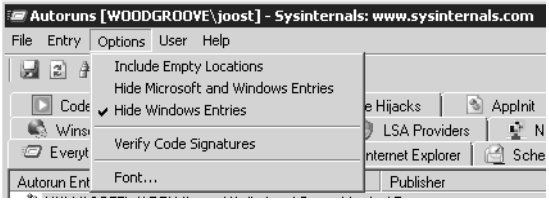


Abbildung 7.43 Windows-Einträge lassen sich in Autoruns ausblenden

Über das Kontextmenü von Einträgen können Sie durch Auswahl von *Search Online* direkt eine Suche im Internet starten, die den jeweiligen Autostarteintrag betrifft. Mit *Jump To* springen Sie direkt in das Windows-Programm, welches den Startvorgang durchführt. Über das Menü *User* lassen Sie sich Autostarteinträge der anderen Benutzerkonten anzeigen, die sich am Computer anmelden.

Wichtige Informationen immer im Blick – BGInfo

Administratoren, die mehrere Server oder Computer von Anwendern im Netzwerk fernwarten, haben oft das Problem, dass nicht alle Informationen über den aktuell verbundenen Computer angezeigt werden, zum Beispiel IP-Adresse, Informationen zu den Laufwerken, Rechnernamen, Bootzeit etc. Es ist sicherlich sinnvoll, die aktuelle IP-Adresse, den genauen Namen des Computers und weitere Einstellungen direkt auf dem Desktop zu sehen, vor allem wenn mehrere Computer gleichzeitig in einer Diagnose auftauchen oder Administratoren parallel mit mehreren Computern arbeiten.

Auch wenn Anwender eine Fernwartung benötigen, ist es hilfreich, wenn diese auf dem Desktop den Namen ihres Computers, die IP-Adresse und weitere Informationen auf einen Blick sehen. In vielen Fällen ist es also für Administratoren extrem hilfreich, wenn auf dem Desktop des ferngewarteten Computers nützliche Informationen angezeigt werden, allerdings ohne dass diese Informationen die Anwender stören. Ein hilfreiches Tool für diese Zwecke ist BGInfo (*http://technet.microsoft.com/de-de/sysinternals/bb897557*) von Sysinternals. Der Entwickler hält in einem eigenen Beitrag (*http://www.windowsitpro.com/article/desktop-management/bginfo.aspx*) weitere Tipps zum Tool bereit. Auch im Sysinternals-Forum (*http://forum.sysinternals.com/forum5.html*) erhalten Sie Informationen zu BGInfo. Allerdings ist eine Einarbeitung nicht unbedingt notwendig, da das Tool sehr leicht bedienbar ist und keine Installation oder Konfiguration erfordert.

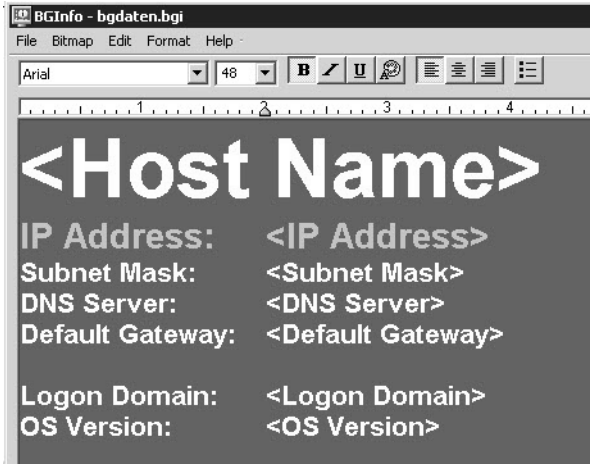


Abbildung 7.44 Informationen bearbeiten mit BGInfo

BGInfo kann Informationen in verschiedenen Schriftgrößen, Farben und anderen Formatierungen auf dem Desktop anzeigen. Neben vorgegebenen Feldern können Sie auch eigene Abfragen erstellen und Informationen einblenden lassen. Diese Anzeige lässt sich vorkonfigurieren, als Konfigurationsdatei abspeichern und per Skript oder Gruppenrichtlinie an Computer im Netzwerk verteilen. Das Tool verbraucht keinerlei Systemressourcen, sondern erstellt beim Start aus den gewünschten Informationen ein neues Hintergrundbild und beendet sich danach wieder. Im laufenden Betrieb ist das Tool daher nicht gestartet.

Der Umgang mit dem Tool ist sehr einfach. Zunächst starten Sie die ausführbare Datei und wählen aus, welche Informationen Sie anzeigen wollen. Die wichtigsten Informationen sind bereits ausgewählt und im Fenster ersichtlich.

Um Änderungen vorzunehmen, klicken Sie zunächst auf *Time remaining* oben rechts oder einen anderen Menübefehl. Ansonsten bindet das Tool bereits automatisch nach 10 Sekunden die ausgewählten Informationen ein und beendet sich wieder. Nach dem Start können Sie konfigurieren, welche Daten Sie zukünftig anzeigen wollen, und diese als Konfigurationsdatei abspeichern. Die Konfiguration ist sehr einfach. Im Feld *Field* sehen Sie, welche Daten Sie in das Hintergrundbild einbinden können. Klicken Sie auf ein Feld und dann auf *<–Add*, um es einzubinden.

Verfügt ein Computer über mehrere Netzwerkkarten, bindet BGInfo diese sowie deren unterschiedliche Konfigurationen wie IP-Adressen, MAC-Adressen und weitere Daten automatisch mit ein. Über die Schaltfläche *Custom* können Sie eigene Felder definieren, indem Sie mit *New* eine neue Abfrage starten. Sie haben im neuen Fenster die Möglichkeit, Umgebungsvariablen, einen Registrywert, eine WMI-Abfrage oder Daten einer Datei abzufragen. In den meisten Fällen ist dies aber nicht notwendig, da die Standardfelder schon viele Informationen umfassen.

Felder und Zeilen, die Sie nicht benötigen, können Sie im mittleren Fenster einfach löschen. Auch Leerzeilen können Sie wie in jeder Textverarbeitung einfügen. Einzelne Zeilen bearbeiten Sie mit den Formatierungswerkzeugen des Tools, die Sie im oberen Bereich finden. Hier können Sie die Schriftgröße und Schriftart einstellen, Farben ändern und die Ausrichtung anpassen.

Haben Sie ausgewählt, welche Felder Sie anzeigen wollen, und diese formatiert, können Sie über die Schaltfläche *Background* festlegen, welches Hintergrundbild Sie mit diesen Informationen anpassen möchten. Standardmäßig verwendet BGInfo das Hintergrundbild des Anwenders, welches aktuell ausgewählt ist. Über die Schaltfläche *Position* bestimmen Sie, an welcher Stelle des Hintergrundbilds BGInfo die Informationen aufnehmen soll. Da das Tool auch mehrere Monitore unterstützt, können Sie bestimmen, auf welchem Monitor die Informationen zu sehen sein sollen. Über die Schaltfläche *Compensate for Taskbar position* (Ausgleich für Taskleistenposition) legen Sie die Position so fest, dass die Taskleiste den Text nicht überdeckt.

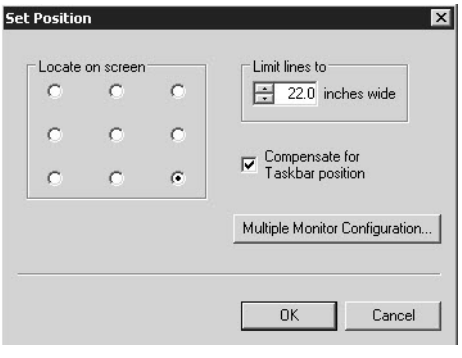


Abbildung 7.45 Festlegen der Position der Informationen auf dem ausgewählten Hintergrundbild

Über die Schaltfläche *Desktops* legen Sie fest, wo BGInfo die Informationen anzeigen soll. Standardmäßig sind die Daten erst ersichtlich, wenn sich ein Anwender anmeldet. Sie können noch für die Option *Logon Desktop for Console Users* den Eintrag *Update this wallpaper* auswählen. In

diesem Fall werden die ausgewählten Informationen bereits am Anmeldebildschirm angezeigt, ohne dass sich Anwender anmelden müssen. Das ist zum Beispiel für Server sinnvoll, wenn an der Konsole kein Administrator angemeldet ist.

Die Option zum Anzeigen des Hintergrunds ist auch für die Anmeldung an Terminalserver-Bildschirmen möglich (in Windows Server 2008 R2 auch Remotedesktop-Sitzungshost genannt) und lässt sich entsprechend aktivieren.

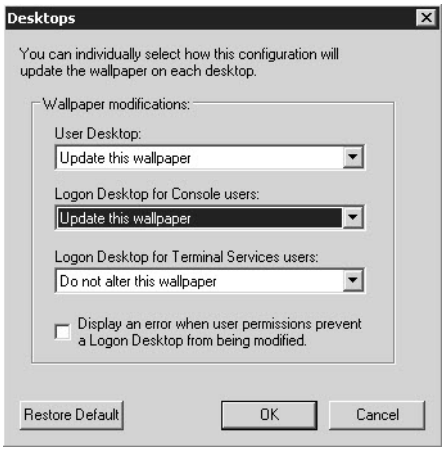


Abbildung 7.46 Auswählen der Konfiguration für die Anzeige der Systeminformationen

Klicken Sie auf *Preview*, zeigt Windows eine Vorschau der Informationen an. Um diese wieder zu deaktivieren, klicken Sie noch einmal auf *Preview*. Um die Anzeige zu übernehmen, klicken Sie auf *Apply*. Mit *OK* übernehmen Sie die Einstellungen und schließen BGInfo.

Abbildung 7.47 Vorschau der Anzeige und anschließende Aktivierung

Natürlich ist es nicht sinnvoll, eine Konfiguration immer wieder neu zu erstellen oder für jeden Computer einzeln anzufertigen. Aus diesem Grund haben Sie in BGInfo auch die Möglichkeit, die von Ihnen angepassten Daten über *File/Save as* als *.bgi*-Datei abzuspeichern. Sie können anschließend BGInfo so starten, dass das Tool diese *.bgi*-Datei als Konfigurationsdatei übernimmt und die ausgewählten Daten anzeigt. Dazu starten Sie BGInfo einfach mit dem Befehl:

```
bginfo <Name der *.bgi-Datei> /timer:0
```

Geben Sie keine Konfigurationsdatei an, verwendet BGInfo die Standardkonfigurationsinformationen, die in der Registrierung im Pfad *HKCU\Software\Winternals\BGInfo* gespeichert sind. Die Option */timer:0* bewirkt, dass das BGInfo-Konfigurationsfenster nicht erscheint, sondern sofort die Informationen übernommen werden. Sie können diesen Befehl in ein Anmeldeskript übernehmen und auf diese Weise auch Daten wie die Anmelde- oder Bootzeit des Computers erfassen. Diese Zeiten sind natürlich immer nur dann aktuell, wenn Sie BGInfo bei jedem Systemstart oder jedem Anmelden starten lassen.

BGInfo aktualisiert sich niemals dynamisch, sondern verwendet immer nur die Daten, die es beim Start vorfindet. Nach der Erstellung des neuen Hintergrundbildes beendet sich BGInfo wieder. Neben Skripts können Sie BGInfo auch mit der Aufgabenplanung in Windows während des Systemstarts und im laufenden Betrieb ständig aktualisieren lassen. Dies ist allerdings nur dann sinnvoll, wenn Sie auch Felder anzeigen lassen, deren Informationen sich im laufenden Betrieb ändern. Neben der Option *timer* stehen in BGInfo weitere Möglichkeiten zur Verfügung:

- /popup Geben Sie diese Option an, öffnet BGInfo ein Popupfenster, welches die Informationen enthält. Dieses können Anwender schließen.
- /taskbar Bei dieser Option blendet BGInfo ein Symbol im Infobereich der Taskleiste ein. Klicken Anwender auf das Symbol, erscheinen die gewünschten Informationen genauso wie bei der Option */popup*.
- /all Ändert die Daten für alle aktuell angemeldeten Benutzer, zum Beispiel auf einem Remotedesktop-Sitzungshost. Auf diese Weise erhalten also alle angemeldeten Anwender das neue Hintergrundbild.
- /log Erstellt eine Logdatei über die Ausführung, in die das Tool auch Fehler schreibt. Diese Option ist sinnvoll, wenn Sie das Tool im laufenden Betrieb über den Aufgabenplaner häufiger starten lassen.
- /rtf Erstellt eine *.rtf*-Datei. Diese Datei enthält auch die Formatierungen und Farben zur Protokollierung.

Über ein Anmeldeskript oder über eine Gruppenrichtlinie können Sie mit diesen Skriptoptionen das Tool auch über eine Freigabe starten lassen. Auch die Konfigurationsdatei kann dazu in einer Freigabe liegen. Sie können natürlich die Datei und das Tool per Gruppenrichtlinie auch direkt auf die einzelnen Computer kopieren lassen.

Über *File/Database* können Sie in der Konfigurationsdatei eine Verbindung zu einer Datenbank vorgeben, um die Daten eines oder mehrerer Computer zu erfassen, zum Beispiel für eine Inventur. In diesem Fall ändert das Tool nicht nur das Hintergrundbild, sondern erfasst die

Daten in der Datenbank oder der ausgewählten Excel-Tabelle. Auf allen Computern, welche diese Konfigurationsdatei nutzen, muss die gleiche Version von MDAC- und JET-Datenbankunterstützung installiert sein.

Microsoft empfiehlt mindestens die Versionen MDAC 2.5 und JET 4.0. Sie können an dieser Stelle als Datenbank auch eine Excel-Tabelle verwenden (*.xlsx*). Die Datei muss verfügbar sein, das Tool kann keine Excel-Dateien erstellen. Wollen Sie mit BGInfo keine Hintergrundbilder ändern, sondern nur die Daten beim Systemstart abfragen und in die Datenbank oder Excel-Tabelle aufnehmen, können Sie in der Konfigurationsdatei festlegen, dass keine Änderungen stattfinden sollen. Dazu klicken Sie im Rahmen der Konfiguration auf Desktops und deaktivieren die Änderung der entsprechenden Desktops.

Systeminformationen in der Eingabeaufforderung – PsInfo

Wollen Sie über einen bestimmten Computer Informationen in der Eingabeaufforderung anzeigen, zum Beispiel zur eingebauten Hardware oder installierten Service Packs und Betriebssystemständen, können Sie das kostenlose Sysinternals-Tool PsInfo aus der PSTool-Sammlung nutzen (*http://technet.microsoft.com/de-de/sysinternals/bb897550*). PsInfo kann nicht nur Daten des lokalen Computers abfragen, dazu können Sie zum Beispiel auch *msinfo32.exe* nutzen oder *systeminfo* in der Eingabeaufforderung, sondern auch Daten von Netzwerkcomputern.

Um Daten des lokalen Systems abzufragen, geben Sie einfach *psinfo* in der Eingabeaufforderung ein. PsInfo benötigt für die Abfrage von Remoteinformationen auch Remotezugriff auf die Registrierung des entsprechenden Computers, um Daten anzuzeigen. Das heißt auf dem Computer muss der Systemdienst *Remoteregistrierung* gestartet sein. Außerdem muss das Benutzerkonto, mit dem Sie PsInfo ausführen, Zugriff auf den Remotecomputer haben.

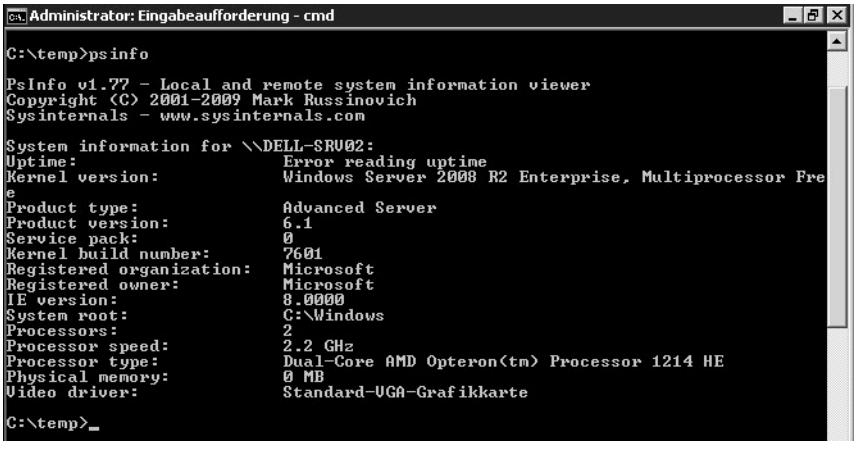


Abbildung 7.48 Anzeigen von Systeminformationen in der Eingabeaufforderung

Die Syntax des Tools lautet:

```
psinfo [[\\Computer[,Computer[,..] | @Datei [-u Benutzer [-p Kennwort]]] [-h] [-s] [-d] [-
c [-t Trennzeichen]] [Filter]
```

- @Datei Führt den Befehl auf allen Computern aus, die in der Textdatei angegeben sind. Schreiben Sie die jeweiligen Computer in eine eigene Zeile.
- –u Benutzernamen für den Remotecomputer
- –p Kennwort für den Benutzer
- –h Liste der installierten Patches
- –s Liste der installierten Anwendungen
- –d Zeigt Informationen zu Datenträgern
- –c Ausgabe im CSV-Format

Mit der Option */filter* können Sie die Ausgabe nach Felder filtern, welche dem angegebenen Text entspricht. *psinfo proc* zeigt zum Beispiel nur Informationen über die Prozessoren an.

Karte des Arbeitsspeichers – RAMMap und VMMap

Für die Fehleranalyse oder Leistungsmessung eines Computers kann es sinnvoll sein, die aktuelle Auslastung des Arbeitsspeichers zu kennen. Das Sysinternals-Tool *RAMMap* (*http://technet.microsoft.com/de-de/sysinternals/ff700229*) zeigt die aktuelle Zuteilung des Arbeitsspeichers in einer grafischen Oberfläche an.

Mit dem Tool erkennen Sie, wie viel Arbeitsspeicher aktuell für den Kernel reserviert ist und welchen Arbeitsspeicher die Treiber des Computers verbrauchen. Auf verschiedenen Registerkarten zeigt das Tool ausführliche Informationen zum Arbeitsspeicher an:

- Use Counts Zusammenfassung
- Processes Prozesse
- Priority Summary Priorisierte Standbylisten
- Physical Pages Seitenübersicht für den kompletten Arbeitsspeicher
- Physical Ranges Adressen zum Arbeitsspeicher
- File Summary Dateien im Arbeitsspeicher
- File Details Individuelle Seiten im Arbeitsspeicher, nach Dateien sortiert

Das Tool hilft vor allem Technikern und Entwicklern dabei, zu verstehen, wie die aktuellen Windows-Versionen den Arbeitsspeicher verwalten und an die verschiedenen Anwendungen, Treiber und Prozesse verteilt. Das Tool funktioniert ab Windows Vista/Windows Server 2008, allerdings nicht in den Vorgängerversionen.

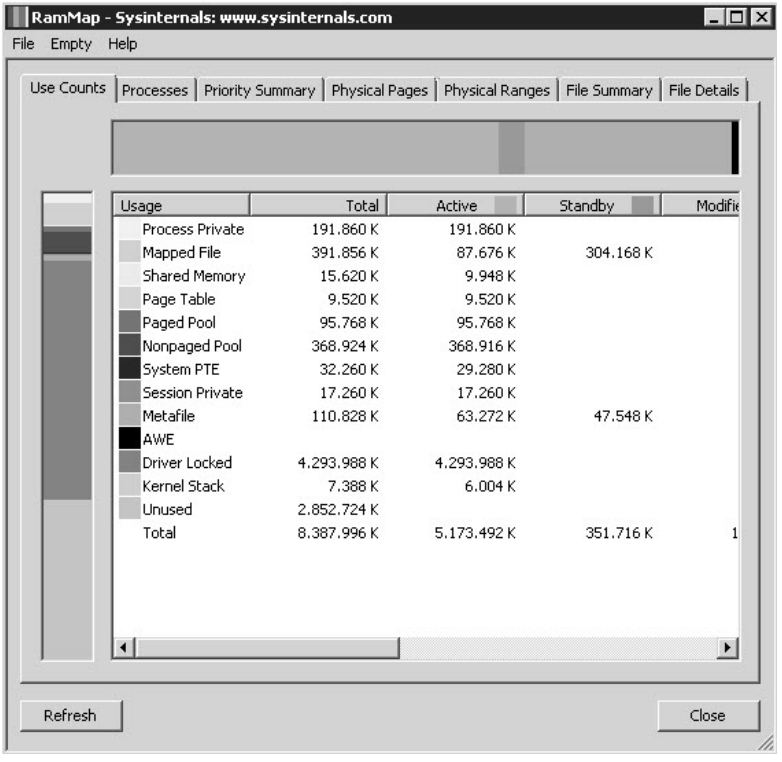


Abbildung 7.49 Anzeige der Arbeitsspeicherverteilung in Windows Server 2008 R2 und Windows 7

Noch ausführlicher bezüglich der Arbeitsspeicheranalyse ist VMMAP (*http://technet.microsoft.com/en-us/sysinternals/dd535533*). Das Tool zeigt sehr detailliert den Arbeitsspeicherverbrauch von Prozessen an. Durch die ausführlichen Filtermöglichkeiten geht *VMMap* bei der Analyse also wesentlich weiter als *RAMMap*.

Beide Tools sind allerdings nicht nur für Administratoren geeignet, sondern auch für Entwickler oder Techniker, die genau das Aufteilen der Ressourcen verstehen wollen. VMMap hat die Möglichkeit, auch anzuzeigen, ob ein Prozess Arbeitsspeicher durch den physischen Arbeitsspeicher erhält, oder durch Windows in die Auslagerungsdatei ausgelagert wird. VMMAP listet extrem detaillierte Daten darüber auf, welche Daten eines Programms oder eines Prozesses in welchen Bereichen des Arbeitsspeichers oder der Auslagerungsdatei liegen. Das Tool ermöglicht auch das Erstellen von Snapshots und unterstützt dadurch Vorher-Nachher-Beobachtungen.

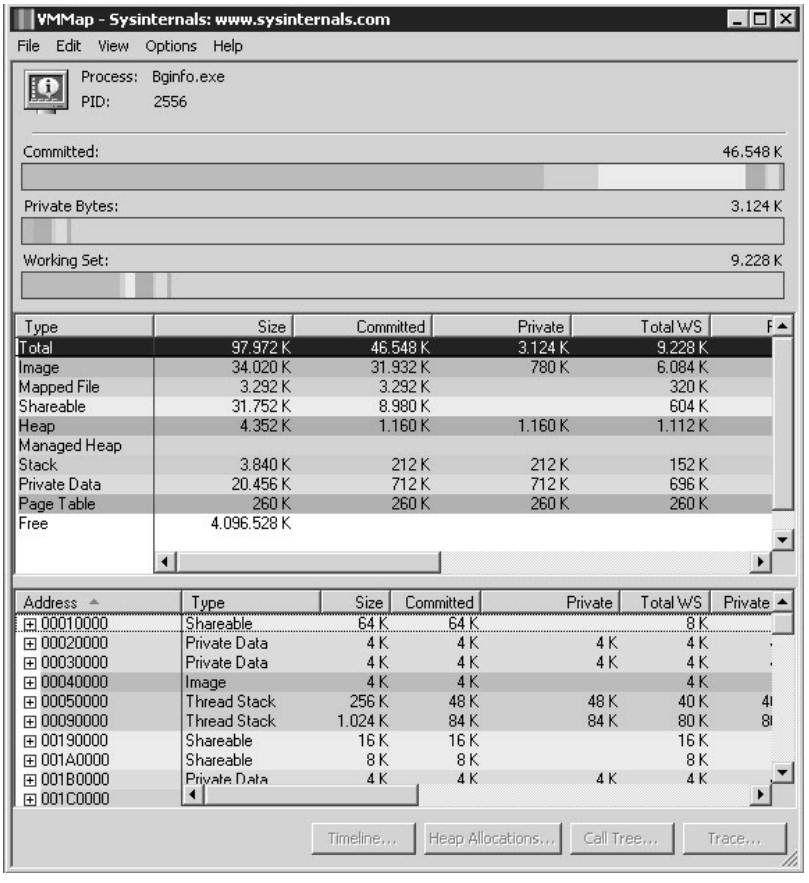


Abbildung 7.50 Analyse des Arbeitsspeicherverbrauchs von Prozessen und Anwendungen

Durch die ausführlichen Analysemöglichkeiten kann das Tool in der grafischen Oberfläche genau anzeigen, wie viel Arbeitsspeicher einzelne Funktionen in einem Prozess benötigen. Über *View/String* lässt sich anzeigen, welche Daten ein einzelner Speicherbereich enthält. Gescannte Ergebnisse lassen sich über *File* abspeichern. Neben dem Format, das VMMap kennt (*.mmp*), lassen sich die Daten auch im *.txt*-Format und als *.csv*-Datei abspeichern. Mit diesen Möglichkeiten lassen sich also auch Analysen mit Excel durchführen.