Prozesse analysieren mit YAPM 2.1.0

auf DVD

Viele Prozesse sind überflüssig, verlangsamen das System oder sind unsicher. Yet Another Process Monitor 2.1.0 analysiert Prozesse und Dienste, untersucht den Netzwerkverkehr und liefert ausführliche Systeminformationen.

Yet Another Process Monitor 2.1.0 (kostenlos, **http://sourceforge.net/projects/yaprocmon** und auf DVD), auch YAPM genannt, beleuchtet, was sich im Hintergrund auf Ihrem PC abspielt. Das Tool liefert dabei wesentlich mehr Informationen als etwa der Task-Manager von Windows.

Yet Another Process Monitor analysiert Prozesse, Dienste und den Netzwerkverkehr. Ein Prozess ist ein ausgeführtes Programm, das Arbeitsspeicher belegt und bei Bedarf die CPU nutzt. Anwendungen wie Word oder der Windows Media Player brauchen normalerweise mehrere Prozesse, um zu laufen.

Im Unterschied dazu ist ein Dienst ein Programm, das im Hintergrund darauf wartet, dass es benötigt wird – sei es vom Anwender oder von einem anderen Programm. Dienste starten in der Regel automatisch. Prozesse, die durch aktive Dienste entstehen, erkennt man in der Prozessliste in der Regel am Besitzer "System". Ausserdem hat ein Dienst keine Schnittstelle zum Benutzer, kann also nicht direkt mit ihm interagieren.

Dazu zeigt YAPM viele Statistiken und Leistungsdaten zu Ihrem System und eignet sich auch als einfacher Dateimanager.

Auf DVD

Sie finden das Tool Yet Another Process Monitor 2.1.0 und den Installer für das .NET-Framework 3.5 auf DVD in der Rubrik *Computer, Prozess-Monitor*.

YAPM installieren

Yet Another Process Monitor benötigt das .NET-Framework 3.5 von Microsoft. Wahrscheinlich ist das auf Ihrem PC bereits vorhanden. Wenn nicht, installieren Sie es, bevor Sie YAPM installieren.

Wenn Sie bereits das .NET-Framework 3.0 auf Ihrem PC installiert haben, dann verwenden Sie den Microsoft-Installer *dotnetfx35setup.exe* (kostenlos, **http://go.microsoft.com/fwlink/?LinkId=124150** und auf), um Version 3.5 SP1 zu installieren.

Ansonsten laden Sie das Paket herunter, das Sie auf derselben Seite weiter unten verlinkt finden. Das *Full Package* ist 231 MByte gross.

Anschliessend starten Sie die Setup-Datei von Yet Another Process Monitor, um das Programm zu installieren.

YAPM nutzen

Es empfiehlt sich, Yet Another Process Monitor mit Administratorrechten zu starten. Das Tool arbeitet zwar auch mit den normalen Benutzerrechten, allerdings haben Sie dann nicht zu allen Funktionen Zugang.

Kompakt

- ***Yet Another Process Monitor analysiert Prozesse, Dienste und den Netzwerkverkehr.***
- ***Zudem zeigt er detaillierte Systeminformationen und Leistungsdaten Ihres PCs.***
- ***Das Tool analysiert über einen Server auch entfernte PCs.***

Zum Start mit Administratorrechten klicken Sie das Programm mit der rechten Maustaste an und wählen den entsprechenden Eintrag aus dem Kontextmenü.

Prozesse analysieren

Gleich nach dem Start zeigt Yet Another Process Monitor eine lange Liste aller Prozesse, die auf Ihrem PC gerade laufen. An den Farben erkennen Sie die Besitzer der Prozesse: Violett kennzeichnet Systemprozesse, die gelb und grün markierten Prozesse gehören zu Ihrem Benutzerkonto. Prozesse mit höherer Priorität sind orange hinterlegt.

Im Prozessfenster sehen Sie Informationen wie die Prozess-ID, die CPU- und Arbeitsspeichernutzung sowie das Programm, das hinter dem Prozess steckt. Mit dem Suchfeld über der Liste suchen Sie gezielt nach Prozessen.

Noch mehr Details erhalten Sie, wenn Sie einen Prozess mit der rechten Maustaste anklicken. Über das Kontextmenü lässt sich der Prozess anhalten oder killen, zudem öffnen Sie darüber das Verzeichnis mit dem entsprechenden Programm oder suchen im Internet nach weiteren Informationen.

Der Menüpunkt *File details* zeigt eine ausführliche Liste mit zusätzlichen Details, darunter die Versionsnummer, den Hersteller und das Datum der letzten Änderung (Bild A).

Inhalt

Das Ganze lässt sich noch weiter steigern: Klicken Sie einen Prozess doppelt an. Es erscheint ein neues Fenster mit 16 Reitern, die jede Einzelheit zu dem entsprechenden Prozess ans Tageslicht holen.

Eine kleine Auswahl der Informationen: Der Reiter *General* zeigt Ihnen allgemeine Informationen zu dem Prozess wie Pfadangaben, die Laufzeit und den Benutzer. Ein Klick auf den Button *Kill* beendet einen möglicherweise hängenden Prozess.

Performances zeigt in Echtzeit Grafiken zur CPU-Nutzung, zum Arbeitsspeicherverbrauch und zu Lese- und Schreibvorgängen.

Network offenbart alle Netzwerkverbindungen, die der Prozess selbst geöffnet hat.

Log ist eine Logbuchfunktion, die alles aufzeichnet, was ein Prozess unternimmt. Sie ist standardmässig deaktiviert. Ein Häkchen bei *Activate log* schaltet das Logbuch an. Bei *Options...* legen Sie fest, welche Prozessdaten YAPM erfassen soll.

Eine systemweite Log-Funktion erhalten Sie, indem Sie im Hauptfenster auf das erste Icon in der oberen Symbolleiste klicken.

Prozesse überwachen

Wenn Ihnen ein Prozess verdächtig erscheint oder Sie einfach nur neugierig sind, wie dieser sich verhält, dann überwachen Sie seine Aktivitäten mit YAPM.

Interessant ist es beispielsweise, den Verlauf des von Firefox benötigten Arbeitsspeichers aufzuzeichnen.

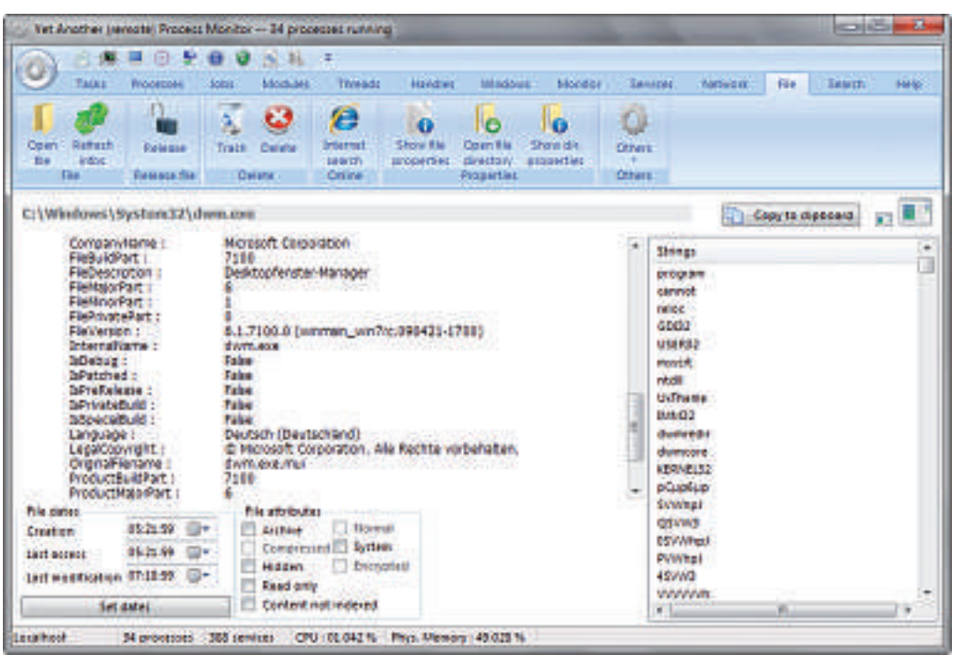
Dazu wechseln Sie zunächst zum Reiter *Monitor*. Dann klicken Sie auf *Add* und stellen bei *Category* den Eintrag *Prozess* ein. *Instance to monitor* ist im Beispiel *firefox*. Dazu muss der Browser natürlich auch laufen.

Bei *Counter type* steht Ihnen nun eine Vielzahl an Parametern zur Auswahl, die sich alle überwachen lassen. Stellen Sie etwa *Arbeitsseiten* ein und klicken Sie anschliessend auf den Button *Add counters from list*. Ein letzter Klick auf *Monitor counters* aktiviert die Funktion, die Sie nun unter *Items* im linken Fenster auswählen. Die Überwachung des Parameters beginnen Sie mit *Start* (Bild B).

Dienste analysieren

Für die Analyse von Diensten stehen weitgehend dieselben Funktionen zur Verfügung wie bei den Prozessen. Dienste haben aber anders als Prozesse keine Schnittstelle zum Benutzer.

Sobald Sie in den Reiter *Services* wechseln, erhalten Sie eine lange Liste mit sämtlichen Diensten, die auf Ihrem PC vorhanden sind. Meist sind dies mehrere Hundert (Bild C). ▶



Detailansicht: Das Fenster zeigt wichtige Informationen zu einem bestimmten Prozess, hier zum Beispiel den Hersteller, den Dateinamen und eine kurze Beschreibung (Bild A).

Um die Dienste zu sehen, die auch tatsächlich laufen, klicken Sie auf die Spalte *State*. Damit sortieren Sie die Liste nach dem Zustand der Dienste, also *Running* oder *Stopped*.

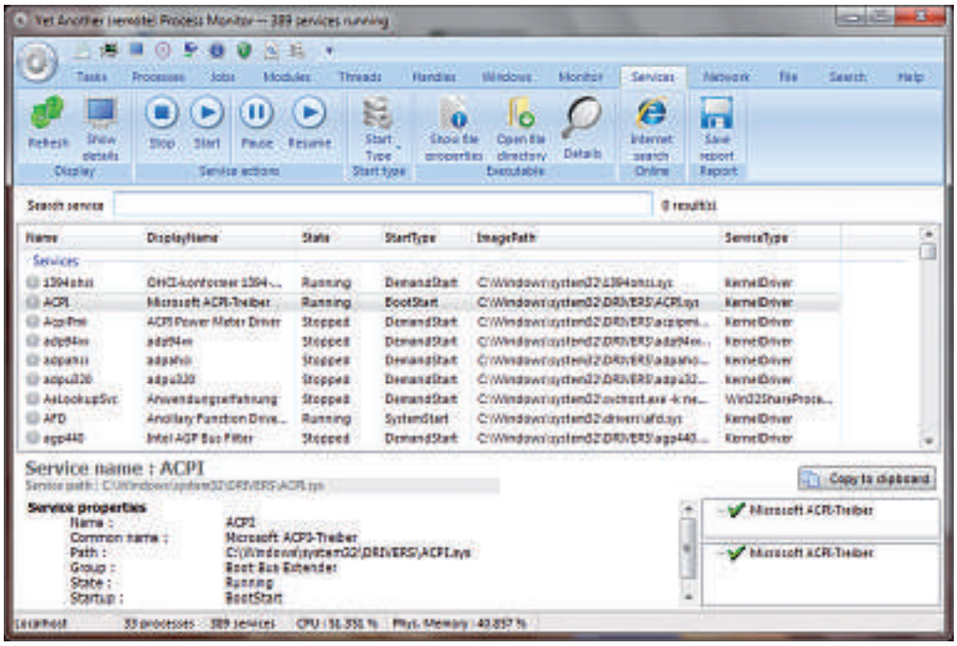
Klicken Sie einen Dienst an, dann sehen Sie im Feld darunter eine kleine Zusammenfassung. Mehr Details erhalten Sie, indem Sie *File details* aus dem Kontextmenü auswählen oder auf die Lupe in der Symbolleiste klicken.

Ein Dienst startet beim Systemstart automatisch, manuell oder nie. Über den Button *Start Type* lässt sich das Startverhalten des ausgewählten Dienstes ändern. Dabei sollten Sie aber Vorsicht walten lassen und sich vorab genau informieren, was der entsprechende Dienst macht. Ausführliche Informationen zu Windows-Prozessen liefert beispielsweise die Webseite **www.processlibrary.com**.

Netzwerkverkehr analysieren

Den Netzwerkverkehr Ihres PCs sehen Sie im Reiter *Network*. Das Fenster zeigt, welche Programme Daten aus dem Internet empfangen oder selbst Daten senden.

Normalerweise finden sich dort Ihr Browser und der E-Mail-Client, aber auch einige Systemdienste. Die Liste entlarvt ebenfalls Programme, die ungefragt mit dem Hersteller Kontakt aufnehmen, etwa um zu fragen, ob ein Update für das Programm vorliegt. Auch Malware verbindet sich mit dem Internet, etwa um ausspionierte Informationen an den Programmierer zu senden.



Services-Übersicht: Das Fenster listet alle 389 auf dem PC vorhandenen Dienste auf (Bild C).

Ein Klick mit der rechten Maustaste auf einen Eintrag in der Liste und auf *Select associated process* führt Sie direkt zum Programm, das den Netzwerkverkehr ausgelöst hat.

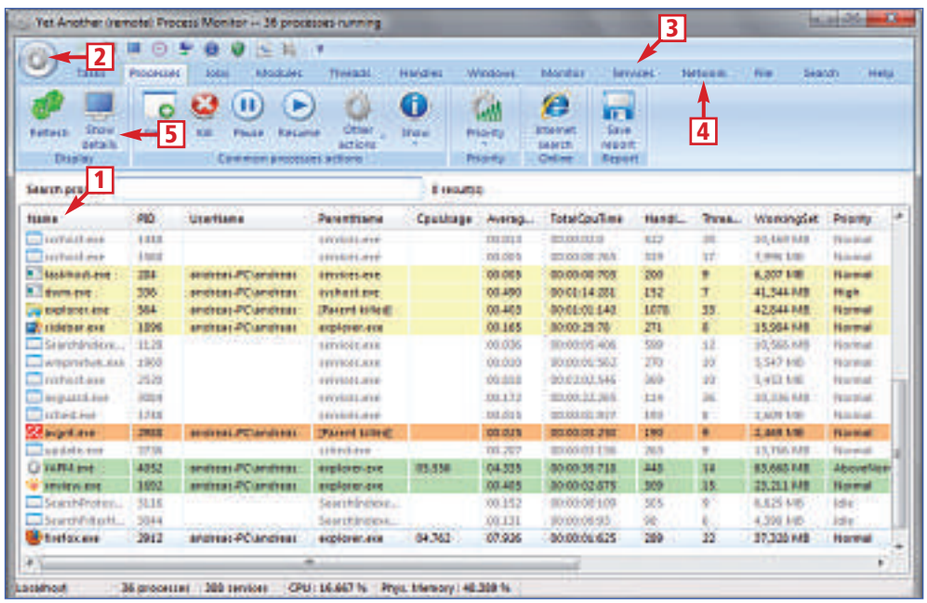
YAPM als Dateimanager

Yet Another Process Monitor ist aber nicht nur ein Prozessmonitor, sondern bietet auch die Funktionen eines einfachen Dateimanagers. Dazu wechseln Sie in den Reiter *File*.

Eine Besonderheit ist die *Release*-Funktion. Diese verwenden Sie, wenn eine Datei hängt, sich nicht beenden lässt oder die gesamte CPU-Last für sich beansprucht. Ein Klick auf *Release* zeigt Ihnen den verantwortlichen Prozess, den Sie dann sogleich beenden können.

Yet Another Process Monitor 2.1.0: So geht's

Yet Another Process Monitor 2.1.0 (kostenlos, http://sourceforge.net/projects/yaprocmon und auf DVD) nimmt Prozesse, Dienste und den Netzwerkverkehr unter die Lupe. So enttarnen Sie überflüssige oder schädliche Programme.



1 Prozesse
Hier finden Sie eine Liste aller laufenden Prozesse. Die Spalten zeigen entsprechende Informationen an.

2 Preferences
Über diesen Button gelangen Sie zu den Einstellungen. Dort lässt sich etwa der Verbindungstyp einstellen.

3 Services
Dieser Reiter führt Sie zur Liste sämtlicher Dienste, die auf Ihrem PC vorhanden sind.

4 Network
Hier sehen Sie den gesamten Netzwerkverkehr Ihres PCs.

5 Show details
Ein Klick auf diesen Button zeigt unzählige Detailinformationen zu dem markierten Prozess.

Die übrigen Funktionen wie Umbenennen, Öffnen, Kopieren oder Einfügen finden sich im Drop-down-Menü unter dem Button *Others*.

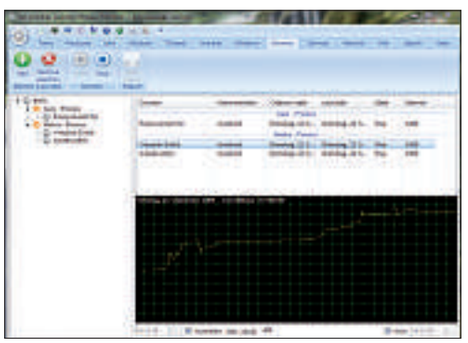
Dort lassen sich Dateien auch mit der Windows-Encryption-Funktion verschlüsseln und wieder entschlüsseln. Diese Verschlüsselung bewirkt, dass andere Benutzer als Sie selbst die entsprechende Datei nicht öffnen oder ausführen können.

Systeminformationen anzeigen

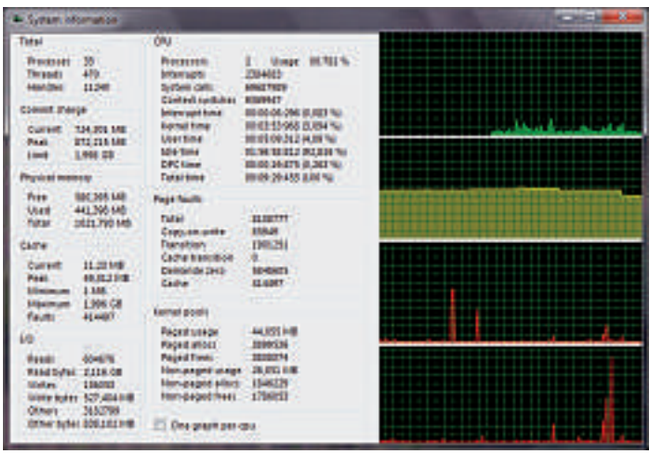
Ähnlich wie der Task-Manager von Windows, nur wesentlich ausführlicher, zeigt auch Yet Another Process Monitor Statistiken und Leistungsdaten zu Ihrem System an (Bild D).

Sie erreichen die entsprechende Funktion mit einem Klick auf das zweite Icon in der oberen Symbolleiste.

Es erscheint ein neues Fenster, das die Systeminformationen in Echtzeit anzeigt.



Prozessmonitor: Hier überwacht der Monitor den Arbeitsspeicherbedarf von Firefox (Bild B).



Systeminformationen: Grafiken und Text zeigen in Echtzeit, was auf Ihrem PC vor sich geht (Bild D).

YAPM remote nutzen

Yet Another Process Monitor lässt sich auch zur Fernwartung einsetzen.

Dazu startet der Anwender auf dem entfernten Rechner YAPM als Server, indem er die mitgelieferte Datei *launch server.bat* aufruft. Auf dem lokalen PC starten Sie dann YAPM und klicken auf das Zahnradsymbol.

Aus dem Menü wählen Sie dort den Punkt *Change connection type*. Im Dialogfenster klicken Sie auf *Disconnect* und aktivieren anschliessend die Option *Remote via YAPM server*. Abschliessend geben Sie die IP-Adresse und den Port ein, welche der Server dem entfernten Anwender mitteilt, und stellen die Verbindung mit *Connect* her.

Sie sehen nun auf Ihrem PC die Prozesse und Dienste des entfernten PCs und haben zum Beispiel die Möglichkeit, Prozesse zu beenden oder Details zu Diensten aufzurufen. ■

Andreas Dumont

Windows®. Leben ohne Grenzen.
Toshiba empfiehlt Windows.

intel CORE 2 Duo inside
Achten Sie auf **Intel Inside®**

TOSHIBA SATELLITE U500 DUCATI EDITION
LEISTUNG TRIFFT AUF TECHNOLOGIE.

Die Rennmaschine unter den Notebooks: der neue Satellite U500-17T in einer Spezialserie von Ducati. Kraftvoll. Sportlich. Schnell, dank dem Intel Core™2 Duo P8700 Prozessor. Eine Fusion von Technologie, Design und Spitzenleistung!

Erfahren Sie mehr unter: www.toshiba.ch/ducati

TOSHIBA CAMILEO S10 DUCATI EDITION
WENN SPASS AUF TOUREN KOMMT.

Auf jeder Tour ein Muss: der neue Camcorder Camileo S10 in einer Spezialserie von Ducati. Kompakt. Leicht. Wendig. Unverzichtbares Zubehör in exklusivem Design. Eine Fusion von Erfahrung und Innovation.

DUCATI Official Licensed Product

TOSHIBA
Leading Innovation

The trademark DUCATI and the relevant logo are registered trademarks owned by DUCATI MOTOR HOLDING S.p.A. and licenced to Toshiba in relation to the products described on this document only. Any and all further use of the same or confusingly similar trademarks will be prosecuted by Ducati Motor Holding S.p.A. under the current Laws and Conventions. Microsoft und Windows sind eingetragene Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern. Intel, das Intel Logo, Intel Inside, Intel Core, und Core Inside sind Marken der Intel Corporation in den USA und anderen Ländern.