Stephan Bäcker, Christian Hirsch

# c’t-Notfall-Windows 2013

## Live-System auf Basis von Windows PE

**Versehentlich gelöschte Daten retten, umpartitionieren oder nach Schädlingen suchen: Das c’t-Notfall-Windows bringt die notwendigen Programme für solche Aufgaben mit, läuft von DVD oder vom USB-Stick und hilft vor allem auch dann noch, wenn das installierte Windows nicht mehr startet.**


Plötzlich startet Windows nicht mehr oder man arbeitet ganz normal und von einer Sekunde auf die andere verlangt ein nicht wegzubekommendes Fenster nach einer Lösegeldzahlung von 50 Euro. In solchen Fällen hilft in der Regel auch ein Neustart nicht mehr. Hier bekämpft man die Ursache am besten mit einem Live-System von außen. In dieser stressigen Situation ist der an Windows gewöhnte Anwender froh, wenn er auf ein Live-System zurückgreifen kann, das dem normalen Windows möglichst ähnelt. Das c’t-Notfall-Windows bootet direkt von DVD oder USB-Stick und bringt Werkzeuge zur Problemdiagnose und -behandlung mit. Da es auf Windows-PE-4 aufsetzt, hat es gegenüber Linux-Systemen den großen Vorteil, dass es Spezialitäten im Original und nicht in nachgemachter Form enthält, wie etwa die neuen Speicherplätze (Storage Spaces).

Auf die Heft-DVD dürfen wir ein bootfähiges Windows PE leider nicht packen. Deshalb übernimmt die Software Winbuilder das Erstellen des Notfall-Windows. Wir haben den Builder bereits so vorkonfiguriert, dass nur wenige Mausklicks zu einem voll funktionstüchtigen Notfall-Windows führen. Alles, was Sie dazu brauchen, ist die Datei „ctnotfall_2013.zip“ von der Heft-DVD und ein Installationsmedium von Windows 8.

### Vorbereitung

Als Quelle benötigt der Builder das Installationsmedium irgendeiner Version von Windows 8, und zwar unbedingt 8. Mit Windows 8.1 klappt es nicht. Ob Core, Pro, Enterprise oder Enterprise-Testversion spielt dabei genauso wenig eine Rolle wie die Architektur. Sie entscheidet allerdings darüber, ob am Ende ein Notfall-Windows in 32 oder 64 Bit herauskommt. Welche die richtige Wahl ist, hängt davon ab, auf welchen Rechnern man es einsetzen möchte. Zum Testen von mehr als 4 GByte Arbeitsspeicher zum Beispiel kommt nur die 64-Bit-Version in Frage. Soll das Notfall-Windows hingegen auf Computern starten, deren Prozessor nicht 64-Bit-tauglich ist, dann muss es eine 32-Bit-Version sein. Wer auf Nummer sicher gehen möchte, erstellt einfach beides.

## Los gehts

Als erstes kopieren Sie die Installationsdateien von Windows 8 auf die Festplatte. Wer eine Lizenz mit DVD erworben hat, muss lediglich alle Dateien von der DVD in einen Ordner kopieren und kann direkt mit dem Winbuilder weitermachen. Nicht ganz so einfach klappt das bei der Download-Version von Windows 8. Die Dateien kopiert man zwar ebenfalls auf die Festplatte, allerdings kann der Winbuilder damit noch nichts anfangen. Schuld ist die install.esd im Unterordner „Source“. Der Winbuilder erwartet das Windows-Image im herkömmlichen Wim-Format. Unter Windows 8 konvertiert das Bordwerkzeug „dism“ die ESD- in eine WIM-Datei. Starten Sie dazu die Eingabeaufforderung mit Administratorrechten und geben Sie den folgenden Befehl ein:

```
dism /Export-Image /SourceImageFile:↵
        "d:\win8\source\install.esd" /SourceIndex:1 ↵
  /DestinationImageFile:"d:\ win8\source\install.wim" ↵
                                        /Compress:recovery
```

Die Pfadangaben hinter SourceImageFile und DestinationImageFile müssen Sie den Gegebenheiten auf Ihrer Festplatte anpassen. Nach dem Konvertieren können Sie die ESD-Datei einfach löschen.

Wer keine Installationsdateien zur Verfügung hat oder wem das Konvertieren der ESD-Datei zu aufwendig ist, der kann auf die kostenlose Testversion von Windows 8 Enterprise zurückgreifen. Für das spätere Notfall-Windows macht das keinen Unterschied. Den Download-Link für die 64-Bit-Testversion finden Sie über den c’t-Link am Ende des Artikels. Nach dem Download entpacken Sie das Abbild mit einem Programm wie zum Beispiel 7-Zip auf die Festplatte in einen neuen Ordner mit dem Namen „Win8“.

## Bauphase

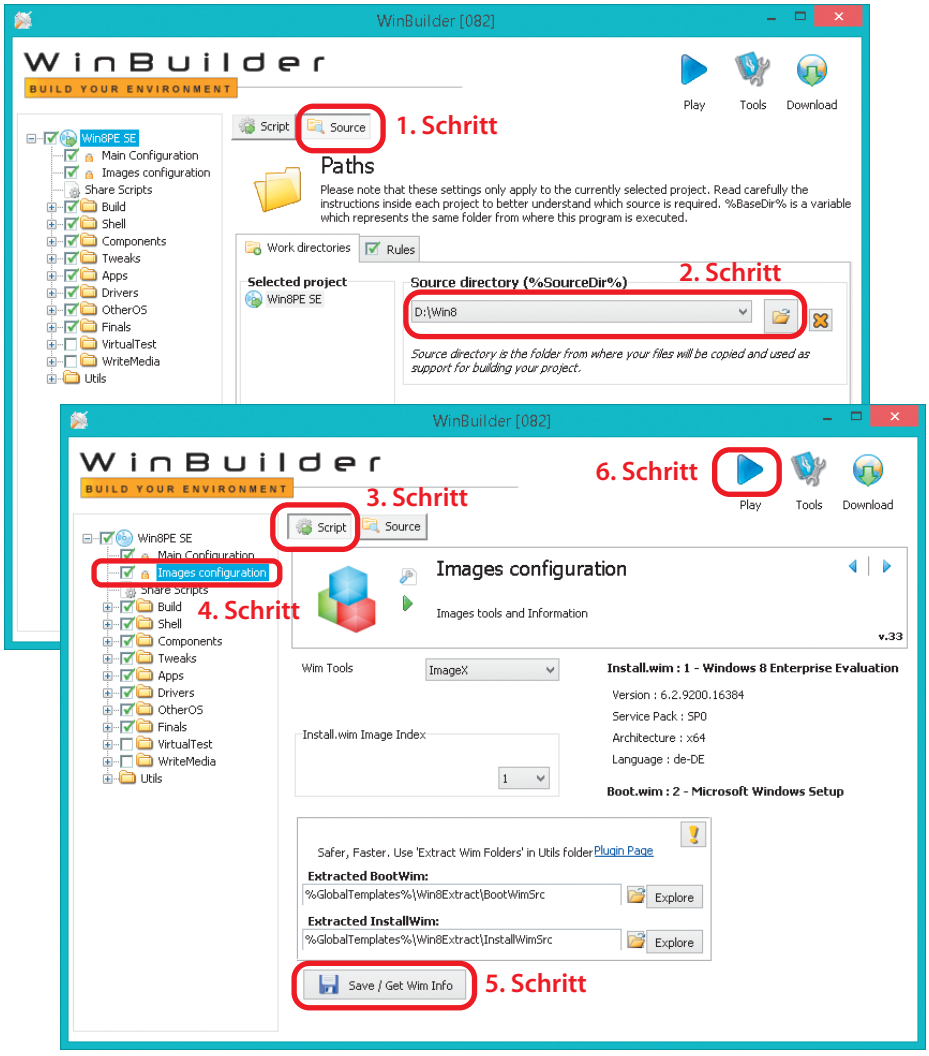
Wenn der Inhalt des Installationsmediums vom Windows 8 auf der Festplatte liegt, geht es im nächsten Schritt mit dem Winbuilder weiter. Beim Winbuilder handelt es sich um eine Umgebung, in der einzelne Skripte alle Schritte zur Erstellung des Notfall-Windows abarbeiten. Das Grundpaket mit dem Namen Win8PE SE stammt von einem Entwickler mit dem Nicknamen ChrisR. Hinzu kommen weitere Skripte von einer kleinen Gemeinschaft, die sich über theoven.org austauscht. Dort und auf der Homepage von Win8PE SE (c’t-Link) stehen auch weitere Skripte zum Download bereit, um etwa zusätzliche Programme in Windows PE einzubauen. Ein Großteil der Programm-Skripte stammt allerdings von uns und steht daher nur auf der Heft-DVD bereit.

Entpacken Sie das Archiv von der Heft-DVD in den Ordner „ctnot“ auf die Festplatte. Das Winbuilder-Verzeichnis wächst im Laufe der Erstellung des Notfall-Windows auf einige GByte an. Stellen Sie also sicher, dass auf dem Laufwerk ungefähr 20 GByte an Speicherplatz frei sind. Der Desktop ist als Speicherort tabu, da der Pfad dann zu lang wird. Benutzen Sie möglichst ein Verzeichnis nah des Root-Verzeichnisses einer Festplatte, so bleibt der Winbuilder-Pfads möglichst kurz. Beim Entpacken schlagen manche Virenscanner bei einigen Dateien im Archiv eventuell Alarm. Die stolpern über ausführbare EXE-Dateien, die in den Skripten mitverpackt sind. Bei einer eingehenden Analyse konnten wir keinen Anhaltspunkt für Schadsoftware finden.

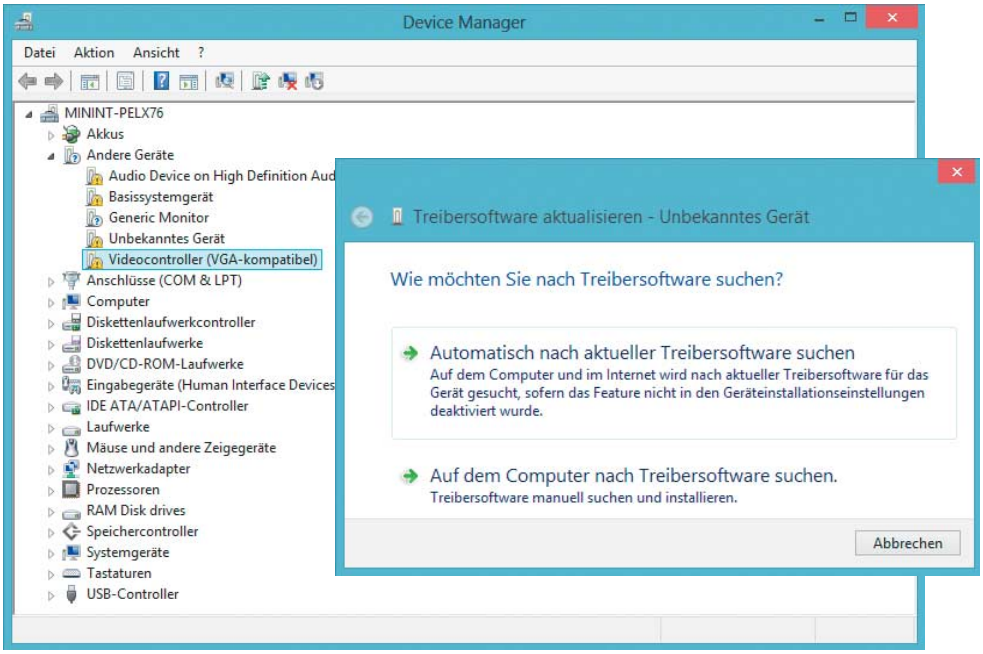
Nach dem Entpacken öffnen Sie den Zielordner, klicken doppelt auf die Datei Win8PESE82_Builder.exe und nicken anschließend die Nachfrage der Benutzerkontensteuerung ab. Der Winbuilder zeigt auf der linken Seite in einer Baumstruktur alle Skripte in verschiedenen Unterordnern. Ein Haken vor einem Skriptnamen oder einem Ordner sorgt dafür, dass das Skript beim Erstellen des Notfall-Windows ausgeführt wird. Bei einem Mausklick auf ein Skript erscheinen im rechten Bereich die zugehörigen Einstellungen.

Als erstes müssen Sie dem Winbuilder mitteilen, wo er die Installationsdateien von Windows 8 findet. Dazu klicken Sie erst auf die Schaltfläche „Source“ und dann auf das Ordnersymbol im Bereich „Source directory“. Im neuen Fenster wählen Sie das Verzeichnis mit den Installationsdateien aus und bestätigen mit „OK“. Wechseln Sie über die Schaltfläche „Script“ zurück zu den Einstellungen, markieren Sie in der Baumstruktur den Eintrag „Images configuration“ und klicken Sie zum Abschluss auf „Save /Get Wim Info“. Es öffnet sich ein neues Fenster und der Winbuilder entnimmt der install.wim-Datei alle benötigten Informationen, beispielsweise Edition und Plattform. Mehr Einstellungen sind nicht notwendig. Nach einem Klick auf die Play-Taste im oberen Bereich arbeitet der Builder alle ausgewählten Skripte ab.

Die meisten von uns für das c’t-Notfall-Windows ausgewählten Werkzeuge sind bereits im Zip-Archiv auf der Heft-DVD enthalten, einige lädt der Winbuilder allerdings erst beim Einbinden herunter. Daher braucht der Computer, an dem man das Notfall-Windows




**Der Winbuilder ist bereits so vorkonfiguriert, dass er nach ein paar Mausklicks ein funktionstüchtiges Notfall-Windows zusammenbaut.**




**Das Notfall-Windows bringt einige Treiber schon mit. Wo der passende Treiber fehlt, lässt er sich schnell über den Gerätemanager nachinstallieren.**

erstellt, einen Zugang zum Internet. Der komplette Erstellprozess kann je nach Hardware zehn bis zwanzig Minuten dauern.

Das fertige Notfall-Windows liegt dann in Form eines ISO-Abbilds im Winbuilder-Verzeichnis im Unterordner „ISO“. Das Abbild können Sie auf eine beschreibbare DVD brennen oder mit 7-Zip auf einen bootfähigen USB-Stick entpacken. Bevor Sie das Notfall-Windows auf dem USB-Stick speichern, müssen Sie ihn bootfähig machen. Dazu dient das Programm „Rufus“, das dabei alle Dateien auf dem Stick löscht. Rufus finden Sie im Winbuilder, wenn Sie in der Baumstruktur den Ordner „WriteMedia“ über das Pluszeichen öffnen. Dort wählen Sie den Eintrag „Rufus“ aus und klicken dann rechts auf „Launch“.

Beim ersten Start fragt Rufus nach, ob es nach Updates suchen darf. Da keine neuere Version notwendig ist, können Sie die Frage verneinen. In Rufus geben Sie zunächst unter „Device“ den USB-Stick vor. Das Partitionsschema können Sie bei der Vorgabe belassen. Als Dateisystem wählen Sie Large FAT32 oder NTFS aus. NTFS müssen Sie auswählen, wenn Sie Dateien größer 4 GByte auf dem Stick speichern wollen. Klicken Sie auf den Knopf am Ende der Zeile „Create a bootable disk using", navigieren Sie im neuen Fenster zur ISO-Datei des Notfall-Windows und bestätigen Sie mit „OK“. Wenn Sie dann auf „Start“ drücken, formatiert Rufus den Stick und kopiert anschließen den Inhalt der ISO-Datei darauf.

Eine bootfähige DVD können Sie mit ImgBurn brennen. Sie finden das Programm wie Rufus unter „WriteMedia“. Zum Brennen klicken Sie allerdings erst auf den Eintrag „ImgBurn ISO“ und dann auf „Launch ImgBurn +ISO“. Sie müssen dann nur noch eine beschreibbare DVD einlegen und auf das große Icon mit dem blauen Pfeil in der Mitte klicken.

## Dateien und Treiber integrieren

Wer will, kann das Notfall-Windows anpassen und zum Beispiel zusätzliche Treiber einbinden, einzelne Programme deaktivieren oder weitere Dateien und Ordner mit in das ISO packen. Das Hinzufügen von zusätzlichen Dateien ist dann praktisch, wenn man das Notfall-Windows später auf eine DVD brennt. Das können zum Beispiel portable Anwendungen, Textdateien oder Batch-Skripte sein. Portable Anwendungen sollte man allerdings vorher ausprobieren, denn nicht alle funktionieren unter Windows PE.

Um zusätzliche Dateien einzubinden, sammeln Sie die in einem eigenen Verzeichnis, öffnen im Winbuilder den Ordner „Build“ und klicken auf „1-Copy Files“. Setzen Sie in den Einstellungen einen Haken bei „Copy Custom Folder“ und klicken Sie mit der Maus auf das Ordnersymbol rechts daneben. Im neuen Fenster wählen Sie erst das Verzeichnis mit den zusätzlichen Dateien und klicken dann auf „OK“. Wer einen USB-Stick für das Notfall-Windows nutzt, kann sich das alles sparen und weitere Dateien einfach auf den Stick kopieren.

Treiberdateien für exotische Hardware oder den WLAN-Adapter lassen sich ebenfalls hinzufügen. Dafür braucht man allerdings die INF-Dateien, mit den Installern kann der Winbuilder die Treiber nicht ins Notfall-Windows einbauen. In einigen Fällen ist es nicht leicht, direkt an die INF-Dateien zu gelangen, da die Hersteller zur Treiberinstallation gleich ein komplettes Setup-Paket liefern. Wenn das so ist, kann 7-Zip die Dateien eventuell entpacken. Oftmals handelt es sich auch nur um ein selbstentpackendes Archiv, das direkt einen Installer startet. Bei Lenovo zum Beispiel kann man das Zielverzeichnis zum Entpacken vorgeben und im Anschluss mit dem Entfernen eines Hakens festlegen, dass die Installation nicht automatisch startet. Falls das alles nicht zum Ziel führt, sollten Sie die Installation trotzdem einmal anstoßen und währenddessen einen Blick in den Ordner“%localappdata%\Temp“ werfen. Viele Setup-Programme entpacken die Dateien zunächst in diesen Ordner. In dem Fall kopieren Sie die benötigten Dateien in einen anderen Ordner und brechen die Installation der Treiber dann ab.

Im Winbuilder gibt es für die Integration von Treibern zwar das Skript „Driver Integration“ im Ordner „Drivers“. In unseren Tests funktionierte es aber nicht immer zuverlässig. Daher sollte man die Treiberdateien lieber wie zuvor beschrieben in den Ordner kopieren, in den auch die zusätzlichen Dateien kommen. Die Treiber installiert man im Notfall-Windows dann über den Geräte-Manager, genauso wie bei einer lokalen Installation von Windows. Wer viele Treiber einbinden möchte, stößt mit der „Driver Integration“ sowieso irgendwann an die Grenzen, da das Notfall-Windows so immer mehr Speicherplatz braucht. Der Grund dafür ist, dass bei der „Driver Integration“ der Builder alle Treiber mit in die boot.wim packt. Die Datei liegt im Unterordner „Source“ der ISO-Datei des Notfall-Windows und ihr Inhalt wandert beim Booten des Notfall-Windows in den Arbeitsspeicher des Rechners. Je größer die boot.wim ist, desto mehr Arbeitsspeicher braucht ein Rechner, damit das Notfall-Windows fehlerfrei läuft. Soll das Notfall-Windows auf möglichst vielen Rechnern laufen, sollte die boot.wim also klein bleiben. Als Anhaltspunkt dafür, wie viel Arbeitsspeicher man braucht, kann man die Größe der boot.wim mit zwei multiplizieren.

## Startmenü anpassen

Wer einige der mitgelieferten Programme nicht im Notfall-Windows haben will, kann diese vor dem Erstellen deaktivieren. Dafür entfernt man einfach den Haken vor dem Programmeintrag. Damit das Notfall-Windows selbst funktionstüchtig bleibt, sollte man von den Skripten in den Ordnern Build, Shell und Components allerdings die Finger lassen.

Die Programme finden Sie im Ordner Apps. Wenn Sie diesen Ordner öffnen, sehen Sie weitere Unterordner, die Programme in verschiedenen Kategorien sortieren. Sie können komplette Ordner deaktivieren oder einzelne Programme. Sobald sie einen Programmeintrag auswählen, sehen Sie auch dort die möglichen Optionen. Der Umfang

der Optionen variiert von Programm zu Programm. Bei den meisten können Sie dort festlegen, wo überall eine Verknüpfung zu dem Programm erscheinen soll.

Wem die Ordnerstruktur des Startmenüs nicht zusagt, der kann es umsortieren. Das geschieht nicht im Winbuilder selbst, sondern im Winbuilder-Verzeichnis auf der Festplatte. Öffnen Sie den Winbuilder-Ordner und wechseln Sie in den Unterordner Projects/Win8PESE/Apps. Hier können Sie die Ordner umbenennen oder einzelne Skripte von einem Ordner in einen anderen verschieben. Möchten Sie zum Beispiel den Eintrag Brennen nicht im Startmenü des Notfall-Windows haben und ImgBurn stattdessen aus Tools starten, dann verschieben Sie die Datei „ImgBurn.Script“ einfach aus dem Ordner „Brennen“ in den Ordner „Tools“ und löschen den Ordner „Brennen“ anschließend. Der Winbuilder erkennt die Änderungen erst beim nächsten Start automatisch.

## Der erste Start

Damit das Notfall-Windows startet, muss der Computer von DVD oder USB booten. Dafür können Sie entweder im BIOS oder UEFI die Bootreihenfolge ändern oder mit einer F-Taste beim Starten das Boot-Menü aufrufen. Welche Funktionstaste die richtige ist, hängt vom PC ab. In der Regel eine zwischen F8 und F12. Nach dem Hochfahren des Notfall-Windows erscheint automatisch der Netzwerk-Manager und aktiviert nach fünf Sekunden die Netzwerkverbindung. Das gelingt auf Anhieb in der Regel nur für kabelgebundene Netzwerkadapter und nicht für WLAN. Wie Sie eine kabellose Verbindung aufbauen, folgt später im Artikel unter „WLAN-Verbindung“. Zum Ändern der Bildschirmauflösung klicken Sie mit der rechten Maustaste unten rechts in der Taskleiste auf das Monitorsymbol und wählen aus der Liste die gewünschte Auflösung. Für einige Grafikkarten bringt das Notfall-Windows Treiber mit. Wenn das nicht der Fall ist, kann man sich mit einer etwas geringeren Auflösung behelfen.

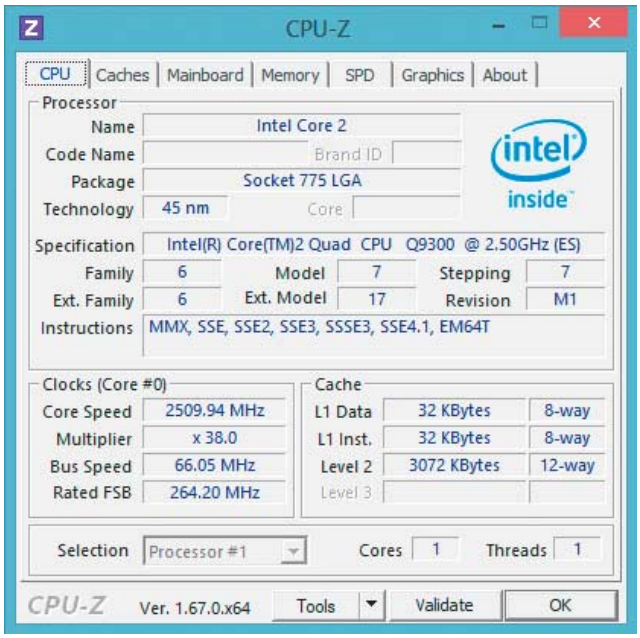
Die Bedienung unterscheidet sich kaum von der eines lokal installierten Windows 8, mit der Ausnahme, dass im Notfall-Windows die Startseite fehlt und man stattdessen den Startknopf mitsamt Startmenü in der Taskleiste findet. Er führt wie gewohnt zu den Programmen und über einen Rechtsklick auf „Computer“ findet man über den Menüeintrag „Verwalten“ zum Geräte-Manager oder zur Datenträgerverwaltung.

## Treiber installieren

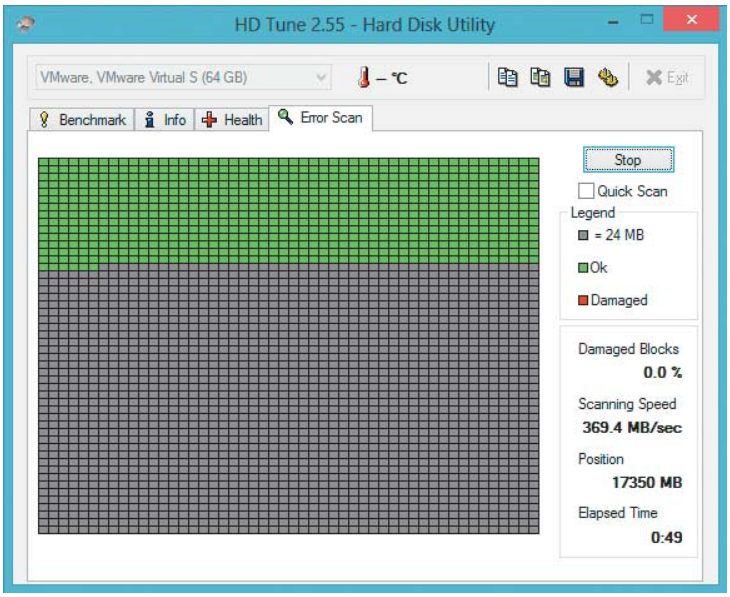
Benötigte Treiber für den WLAN-Adapter oder einen RAID-Controller installieren Sie wie gewohnt über den Geräte-Manager. Am schnellsten klappt die Treiberinstallation, wenn Sie alle Treiber wie zuvor beschrieben auf einem USB-Medium speichern. Im Bereich „Andere Geräte“ listet Windows alle Geräte auf, für die Windows keinen Treiber findet. Klicken Sie mit der rechten Maustaste auf das Gerät, welches Sie installieren möchten, und wählen Sie „Auf dem Computer nach Treibersoftware suchen.“ aus. Dann geben Sie den Laufwerksbuchstaben des USB-Speichers an und klicken auf „Weiter“. Windows findet den passenden Treiber jetzt selbst und Sie müssen für weitere Geräte die Schritte nur wiederholen. Dabei brauchen Sie den Laufwerksbuchstaben aber nicht mehr anzugeben, da Windows sich diesen merkt.

In einigen Fällen erkennt das Notfall-Windows ein USB-Laufwerk nicht direkt. Das kann passieren, wenn man es vom Rechner abzieht und später erneut anstöpselt. Um erneut nach dem Speicher suchen zu lassen,






**Kontrolle ist besser: Mit CPU-Z können Sie nachprüfen, ob der Arbeitsspeicher auch wirklich mit den richtigen Taktfrequenzen und Latenzen läuft.**




**HD Tune kommt defekten Festplatten-sektoren schnell auf die Schliche.**

wählen Sie aus dem Startmenü unter „Computer Management/Drivers“ den Eintrag „force install usb“.

## WLAN-Verbindung

Allein die Installation der passenden Treiber reicht noch nicht, damit sich das Notfall-Windows auch mit einem Access-Point verbindet. Klicken Sie dazu in der Taskleiste mit der rechten Maustaste auf das Symbol mit den zwei Monitoren und wählen Sie aus dem Menü den Punkt „Zeige Hauptfenster“. Im Netzwerk-Manager klicken Sie auf den grünen geschwungenen Pfeil zum Neuladen aller Netzwerkadapter und wählen dann aus dem Drop-Down-Menü daneben den WLAN-Adapter aus. Wechseln Sie auf die Registerkarte „WiFi“, suchen Sie in der Liste das richtige WLAN-Netzwerk aus und klicken Sie dann auf „Verbinden“. Die Eingabe des Netzwerkschlüssels bestätigen Sie mit „OK“.

## Praxis-Einsatz

Wenn das Rettungssystem den eigenen Vorstellungen entspricht und man die Basisschritte mit Internetzugang und Auflösung durch hat, kann die eigentliche Arbeit beginnen. Als Orientierungshilfe haben wir ein paar Problemfälle zusammengestellt und zeigen, welche Werkzeuge im Einzelfall die richtigen sind.

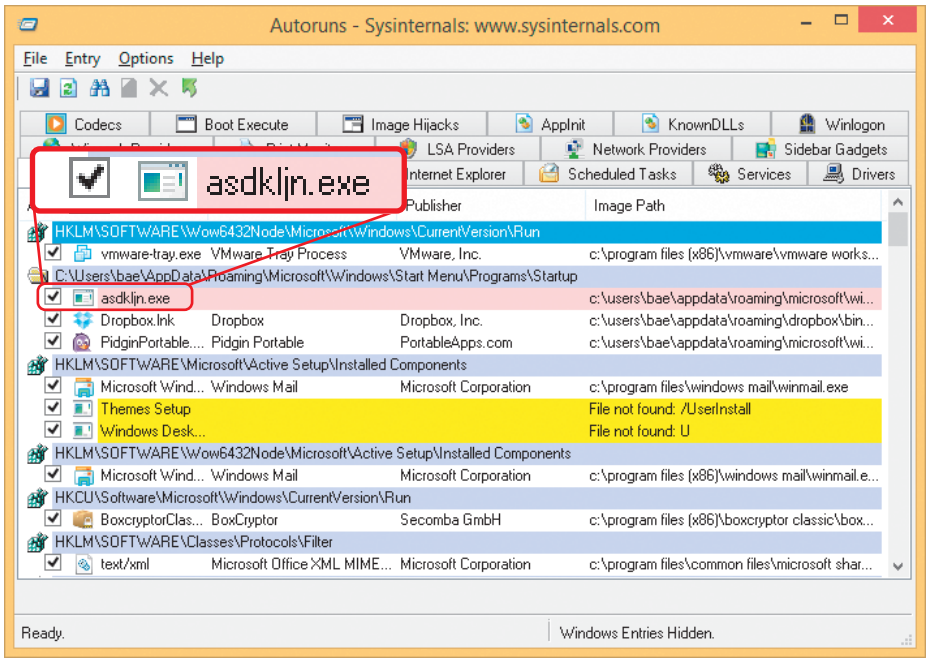
## Abstürzen Herr werden

Wenn im laufenden Betrieb unregelmäßige, nicht reproduzierbare Abstürze von Anwendungen oder dem kompletten Betriebssystem auftreten, liegt womöglich ein Defekt des Arbeitsspeichers vor. Ein kaputter RAM-Baustein muss sich aber nicht gleich als Absturz bemerkbar machen, sondern es könnten stattdessen bei jedem Speichervorgang Dateien beschädigt werden und fehlerhaft auf der Festplatte landen. Der Schaden summiert sich und ist schließlich so groß, dass Dokumente oder Bilder nicht mehr lesbar sind oder das System nicht mehr bootet. Der Test des Arbeitsspeichers empfiehlt sich aber auch bei einem neu zusammengebauten Rechner, da so nicht nur defekte, sondern auch inkompatible RAM-Riegel auffallen.

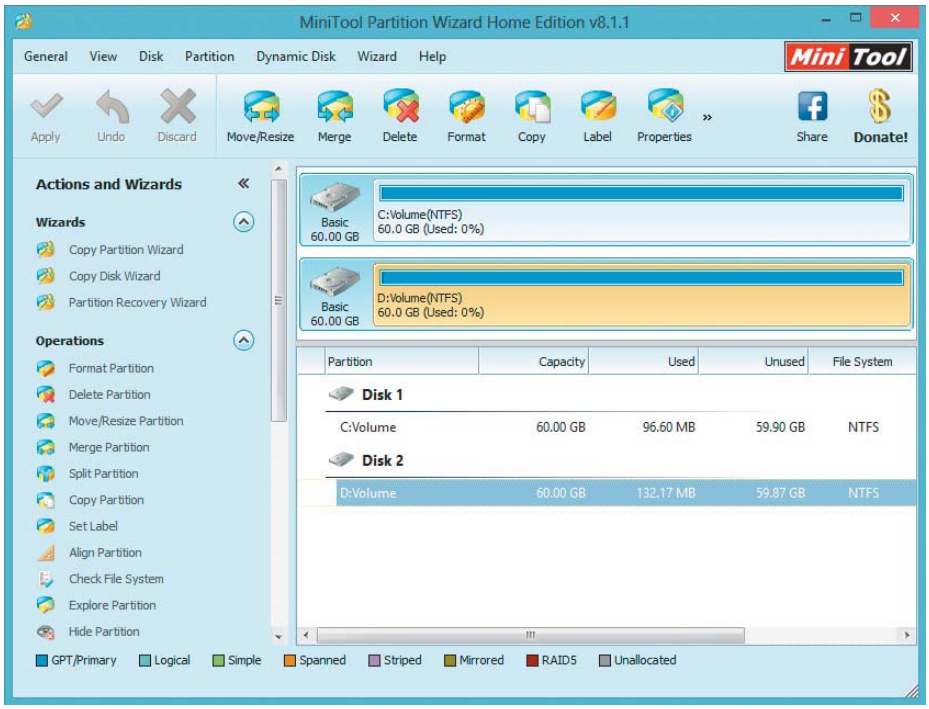
Aus dem Startmenü des Notfall-Windows rufen Sie über „Programme\Analyse\“ **Prime95** auf. Im neuen Fenster wählen Sie „Just Stress Testing“ und anschließen „OK“. Prime95 dient, wie der Name schon sagt, eigentlich zur Berechnung von Primzahlen und belastet jetzt sowohl die CPU als auch den Hauptspeicher.

Treten Fehler auf, ist die CPU zu hoch übertaktet oder mindestens ein defektes oder inkompatibles RAM-Modul steckt auf dem Mainboard. Um den Übeltäter zu überführen, müssen Sie die Module anschließend einzeln prüfen. Speicherfehler können auch von falsch eingestellten Timing-Parametern herrühren. In der Regel erkennt das Mainboard-BIOS automatisch die im sogenannten SPD-EEPROM auf dem RAM-Riegel hinterlegten Werte für die Taktfrequenzen und Latenzzeiten und stellt diese auch ein. Ob das korrekt passiert, können Sie mit **CPU-Z** überprüfen. Es liest sowohl die Sollwerte des Speichermoduls als auch die Istwerte aus, die das Mainboard tatsächlich verwendet. Ist die eingestellte Taktfrequenz höher oder sind die Latenzzyklen niedriger als erlaubt, drohen die beschriebenen Probleme. Darüber hinaus informiert das Programm über die Kenndaten des Prozessors und des Mainboards.

Prime95 kann aber auch eine zu schwache Kühlung entlarven. Bei unzureichend dimensionierter Kühlung oder verschmutzten Lüftern wird es dem Prozessor zu warm. Integrierte Schutzschaltungen verhindern bei modernen CPUs zwar, dass der Chip überhitzt und Schaden nimmt, drosseln dafür aber die Taktfrequenzen und so die Performance. Starten Sie Prime95 und wählen Sie das Profil „In-place large FFTs“. Die Kerntemperaturen und Lüfterdrehzahlen lassen sich mit dem Monitoring-Programm **HWMonitor** überwachen. Darüber hinaus gibt es Auskunft über die aktuelle Leistungsaufnahme des Prozessors sowie die Spannungspegel von Netzteil und Mainboard.




**Autoruns entlarvt Schädlinge, die sich im Startprozess von Windows eingenistet haben.**




**Mit dem Partition Wizard lässt sich die Partitionierung von Festplatten komfortabel ändern und er beherrscht ein paar Tricks, die die Datenträgerverwaltung nicht kennt.**

## Datensalat sortieren

Schäden an Datenspeichern sind doppelt ärgerlich: Zum Ausfall der Hardware an sich gesellt sich der Verlust der darauf gespeicherten Daten. In Festplatten und Solid-State Disks steckt die Selbstdiagnosetechnik SMART (Self-Monitoring, Analysis and Reporting Technology). Neben Laufzeit, Start-Stopp-Zyklen und Temperatur lassen sich über diese Schnittstelle die Zahl verschobener und defekter Sektoren sowie von Übertragungsfehlern auslesen.

In vielen Fällen kündigt sich ein Ausfall bereits vorher durch auffällige SMART-Werte an, die zum Beispiel das Diagnose- und Benchmark-Tool **HD Tune** liefert. Wenn solch ein Programm Warnungen ausgibt, sollten Sie umgehend ein Backup der Daten anlegen und den Datenträger austauschen.

Sofern die Festplatte keinen Hardwareschaden aufweist, liegt der Fehler auf logischer Ebene. Öffnen Sie das Startmenü und klicken Sie auf „Command Prompt“. In der Eingabeaufforderung führen Sie anschließend den folgenden Befehl aus `chkdsk [Laufwerksbuchstabe:] /f /r`. Anstelle der eckigen Klammer setzen die den Laufwerksbuchstaben der Festplatte ein.

Bei USB-Sticks oder Speicherkarten tauchen von Zeit zu Zeit Fälschungen auf, die eine höhere Kapazität vorgaukeln, als die eingebauten Flash-Speicher tatsächlich haben. Überschreitet der Füllstand die physisch vorhandene Speichermenge, werden zuvor gespeicherte Daten überschrieben. Das Programm **H2testw** füllt den kompletten USB-Stick mit Testdaten und meldet zuverlässig die wahre Kapazität des Sticks.

## Schädlinge aufspüren

Wenn ein Virus Windows befallen und den installierten Viren-Scanner vielleicht sogar außer Kraft gesetzt hat, hilft es nur noch, den Schädling von außen zu bekämpfen. Das c’t-Notfall-Windows bemüht dafür den **Eset-Online-Virenscanner** und **ClamAV**.

Schadprogramme sorgen oft dafür, dass Windows sie automatisch beim Hochfahren ausführt. Dafür gibt es einige Ecken in Windows, in denen sie sich einnisten [1]. **Autoruns** schaut in den wichtigsten nach und listet auf, was Windows alles automatisch aufruft.

Autoruns können Sie direkt über die Verknüpfung vom Desktop des Notfall-Windows ausführen. Beim Start zeigt es Informationen zum Notfall-Windows an, die hier aber nicht interessieren. Damit es ein lokal installiertes Windows untersucht, klicken Sie im Menü auf „File“ und dann auf „Analyze Offline System“. Unter „System Root“ geben Sie über den Knopf mit den drei Punkten den Windows-Ordner der zu untersuchenden Installation an und unter „User Profile“ den Pfad zum Benutzerprofil. Das liegt in der Regel auf der gleichen Festplatte wie Windows, allerdings im Ordner „Benutzer“.

Achten Sie vor allem auf die Einträge unter „CurrentVersion\Run“ und „Startup“. Die verschiedenen Formen des Schädlings, der als Bundestrojaner bezeichnet wird, nisten sich zum Beispiel überwiegend im Profileordner

ein und tragen einen Namen aus zufällig gewählten Zahlen wie zum Beispiel „0.78234784.exe“. Solche Einträge können Sie über das Kästchen deaktivieren und die EXE-Datei löschen. Eine Anwendung mit der Beschreibung „Java Update Service“ mag vielleicht seriös erklingen. Wenn das Programm aber im temporären Ordner des Benutzerprofils liegt und eigentlich alökjhsdf.exe heißt, handelt es sich mit Sicherheit um einen Schädling. Wenn Sie sich bei manchen Dateien nicht sicher sind, hilft eine Suche bei Google oder das Hochladen der Datei bei Virus Total. Im Opera-Browser existiert für Virus Total bereits ein Lesezeichen. Wenn Sie immer noch unsicher sind, deaktivieren Sie den Eintrag einfach und benennen Sie die Datei um. Anschließend prüfen Sie, ob es im normalen Windows zu Problemen kommt.

Um die gesamte Festplatte zu überprüfen, sind mit **ClamAV** und dem **Eset Online Scanner** noch zwei Antivirus-Werkzeuge mit an Bord. Beide laden nach dem Öffnen zunächst aktuelle Virendefinitionen herunter. Die Virensuche sollten Sie auf die lokalen Festplatten beschränken. Bei ClamAV wählen Sie einfach die Festplatte aus und starten dann die Suche, bei Eset können Sie in den „Erweiterten Einstellungen“ über „Ändern“ die Laufwerke B und X des Notfall-Windows abwählen.

## Sicher löschen

Windows hat mit **diskpart** einen „Datenshredder“ schon eingebaut, um etwa beim Verkauf des PC alle gespeicherten Daten zu tilgen. Allerdings weigert der sich verständlicherweise, das Systemlaufwerk zu löschen, während Windows noch läuft. Im Notfall-Windows rufen Sie mit der Tastenkombination Windows-Taste+R das Ausführen-Fenster auf, geben `diskpart` ein und bestätigen Sie mit „OK“. Der Befehl `lis dis` zeigt alle Festplatten durchnummeriert an. Identifizieren Sie die richtige anhand der Größe und wählen Sie sie mit dem Befehl `sel dis [Nummer]` aus. Um sicherzugehen, dass Sie die richtige Festplatte erwischt haben, können Sie sich mit `det dis` die Datenträgerbezeichnung zeigen lassen. Um die Festplatte dann komplett zu löschen, geben Sie `clean all` ein. Dabei überschreibt diskpart jeden Sektor einmal.

## Speicherplatz verschieben

Windows braucht Luft zum Atmen. Läuft das Systemlaufwerk voll, ergreift Windows zwar einige Maßnahmen, um Platz zu schaffen. Man kann ihm dabei aber auch helfen [2], in dem man einer anderen Partition auf der gleichen Festplatte etwas freien Speicher abzwackt und der Systempartition zuweist. Die Datenträgerverwaltung erfüllt zwar die meisten Aufgaben der Festplattenverwaltung, das Verschieben von Partitionen ist damit aber nicht so einfach möglich.

Öffnen Sie über Startmenü/Festplatte/Partitionieren den **Partition Wizzard**. Um die Systempartition vergrößern zu können, müssen Sie Platz schaffen. Markieren Sie in der Übersicht die dahinterliegende Partition und klicken Sie am rechten Rand auf „Move/Resize Partition“. Im neuen Fenster können Sie mit den Dreiecken die Partition vom Anfang oder Ende her verkleinern. Klicken Sie auf das rechte Dreieck und schieben Sie es, während Sie die Maustaste gedrückt halten, nach rechts. Wenn genug Platz frei ist, lassen Sie die Maustaste los und bestätigen mit „OK“. Das Gleiche wiederholen Sie für die Systempartition. Dort ziehen Sie jetzt aber das rechte Dreieck so weit wie möglich nach rechts und bestätigen ebenfalls mit „OK“. Die Änderungen merkt sich der Partition Wizzard lediglich. Drücken Sie zum Schluss auf „Apply“, damit er die Partitionierung wirklich ändert.

Möchten Sie den Speicherplatz auf einer weiter hinten liegenden Partition freigeben, dann verkleinern Sie die und schieben zunächst alle Partition zwischen dieser und der Systempartition nach hinten. Zum Verschieben klicken Sie ebenfalls auf „Move/Resize Partition“, greifen mit der Maus nicht nach einem der beiden Dreiecke, sondern dazwischen nach der ganzen Partition und ziehen Sie mit der Maus so weit es geht nach rechts.

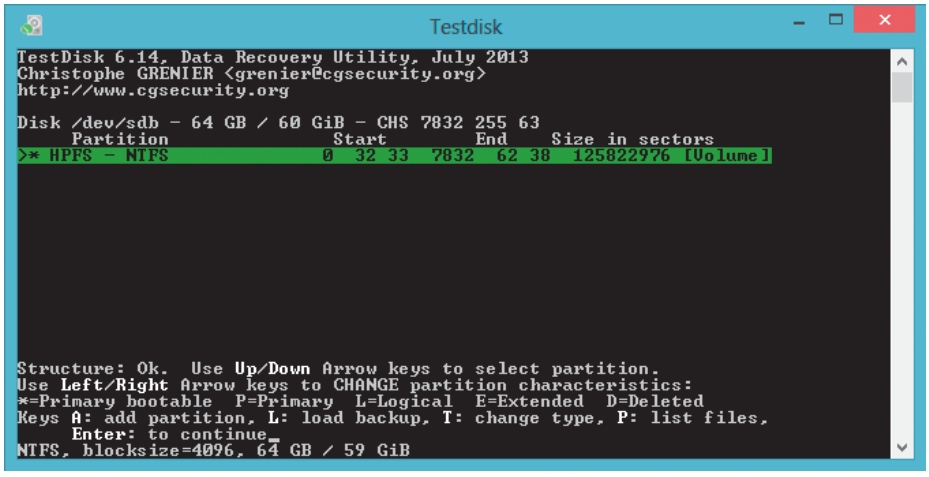
## Daten retten

Die passenden Werkzeuge zur Datenrettung versammeln sich im Startmenü unter Festplatte/Datenrettung. Einzelne Dateien und Ordner stellt **Recuva** wieder her. Starten Sie das Programm und folgen Sie den Anweisungen des Assistenten. Nach der Suche auf der Festplatte sehen Sie in einer Liste alle gefundenen Dateien. Vor dem Dateinamen zeigt Recuva durch einen grünen, orangenen oder roten Punkt an, wie gut die Rettungschance steht. Sollte die gesuchte Datei in der Liste nicht auftauchen, bringt sie vielleicht die Tiefensuche zum Vorschein. Dafür aktivieren Sie diese im Assistenten und lassen Recuva erneut suchen.

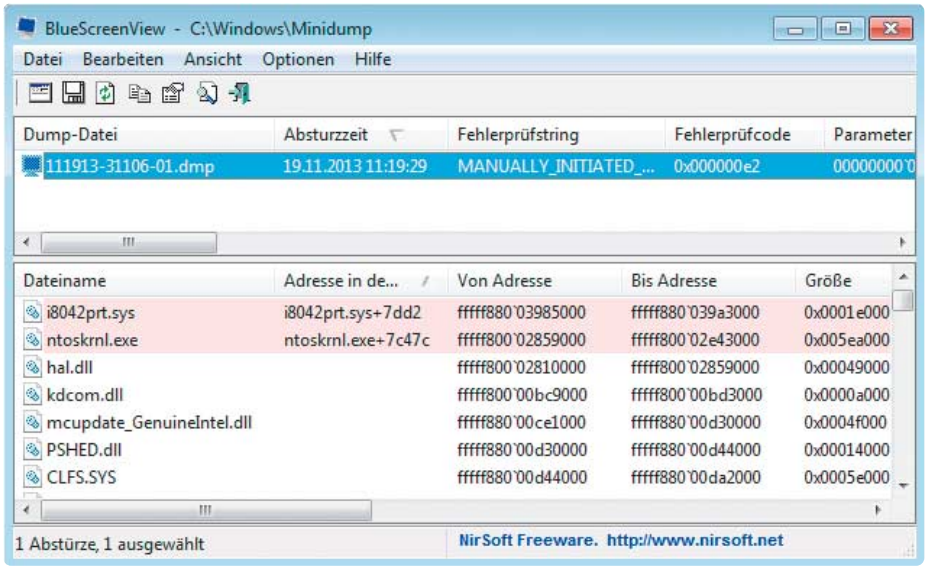
In der Übersicht markieren Sie dann alle Dateien, die Sie retten wollen, und klicken auf „Wiederherstellen“. Recuva fragt nach einem Speicherordner. Die Dateien sollten Sie immer auf einem anderen Speichermedium ablegen, um jegliche Schreibzugriffe auf die Festplatte mit den gelöschten Dateien zu vermeiden.

Gelöschte Partitionen oder Festplatten mit defekter Partitionstabelle behandelt man mit **Testdisk**. In vielen Fällen lassen sich damit beschädigte oder gelöschte Partitionen wiederherstellen. Testdisk kommt ganz ohne grafische Oberfläche daher und wird über die Tastatur mit den Pfeiltasten und der Enter-Taste bedient. Um eine gelöschte Partitionstabelle wiederherzustellen, markieren Sie in Testdisk mit den Pfeiltasten „No Log“ und drücken anschließend die Enter-Taste. Auf die gleiche Weise wählen Sie dann die Festplatte, als Partitionstabelle „Intel“ und zum Schluss „Analyse“ aus. Testdisk zeigt eine Liste mit den gefundenen Partitionen an, die vermutlich noch leer ist. Suchen Sie mit „Quick Search“ nach Partitionen. Testdisk listet gefundene Partitionen auf. Bei nur einer Partition können Sie die direkt mit der Enter-Taste auswählen und anschließen über „Write“ die Partitionstabelle neu schreiben. Auf die Partition zugreifen können Sie allerdings erst nach einem Neustart des Rechners. Vom gleichen Entwickler wie Testdisk stammt auch **PhotoRec**. Es ist in der Bedienung mit Testdisk vergleichbar, aber wie der Name schon sagt, speziell zum Retten von Bilddateien konzipiert.

Von beschädigten Datenträgern kann **Unstoppable Copier** manchmal noch die letzten lesbaren Bytes herunterkratzen. Im Unterschied zum Windows-Explorer bricht es bei Lesefehlern nicht ab, sondern kopiert alle Daten, die es noch zusammenbekommt. Gerade bei zerkratzen CDs und DVDs kann man so häufig noch die ein oder andere Datei retten. Da die Fehlerkorrektur bei DVD-Laufwerken unterschiedlich gut funktioniert, sollten Sie eine zerkratzte CD in möglichst vielen verschiedenen Laufwerken ausprobieren.




**Die Bedienung von Testdisk ist zwar gewöhnungsbedürftig, aber zum Retten verlorener Partitionen ist es erste Wahl.**




**Bluescreenview listet alle Minidumps auf und zeigt außer dem Fehlerprüfcode auch die beteiligten Dateien.**

## Festplatten sichern

Zum Erstellen eines Images von einem Datenträger bringt das Notfall-Windows den **Open Disc Image in a Nutshell** (ODIN) und **HDD Raw Copy** mit. ODIN erstellt komplette Abbilder von Partitionen und erlaubt das Aufteilen der Image-Datei, um sie etwa auf mehrere optische Speichermedien zu verteilen. Auf Wunsch verifiziert es ein Abbild nach dem Erstellen und kann die Daten auch wieder herstellen. HDD Raw Copy arbeitet etwas anders: Es erstellt auf Low-Level-Basis ein Image von einer Festplatte, einer SSD, einem USB-Stick oder einer SD-Karte. Wie dd unter Linux entstehen sektorgenaue Abbilder, auf die man für eine Datenrettung zurückgreifen kann. Daher liegt die Verknüpfung für HDD Raw Copy im Notfall-Windows auch unter Festplatte/Datenrettung und nicht wie ODIN unter „Sicherung“.

## Bluescreen-Diagnose

Standardmäßig führt Windows beim Auftreten eines Fehlers direkt einen Neustart aus. Das geht so schnell, dass man die Fehlerausgabe, den Inhalt des Bluescreen, nicht lesen kann. Für die Fehlersuche ist ein solcher Stop-Fehler aber ein wichtiger Hinweis. **BluescreenView** zeigt alle aufgetretenen Bluescreens an, zumindest dann, wenn Windows noch ein sogenanntes Speicherabbild schreiben konnte. Sie finden Bluescreenview im Startmenü des Notfall-Windows unter „Analyse“. Als erstes müssen Sie dem Programm mitteilen, wo es die Speicherabbilder findet. Öffnen Sie dafür die „Erweiterten Optionen“ über den Menüpunkt „Optionen“. Klicken Sie auf Suchen, wechseln Sie ins Windows-Verzeichnis der lokalen Installation und wählen Sie den Ordner „Minidump“ aus.

Es kann vorkommen, dass der Ordner Minidump gar nicht existiert. Er entsteht erst, wenn Windows ein Speicherabbild auf der Festplatte ablegt. Bei manchem Fehler, gerade bei Problemen mit der Festplatte, klappt das allerdings nicht mehr. Dann ändert man vom Notfall-Windows aus einen Wert in der Registry der lokalen Windows-Installation und verhindert so den automatischen Neustart.

Drücken Sie dazu die Windows-Taste, geben Sie regedit ein und doppelklicken Sie auf „regedit.exe“. Im Registry-Editor markieren Sie „HKEY_LOCAL_MACHINE“ und klicken dann im Menüpunkt „Datei“ auf „Datei/Struktur“. Öffnen Sie von der Festplatte mit der lokalen Windows-Installation die Datei „SYSTEM“ aus dem Ordner Windows/System32/Config. Regedit verlangt einen Schlüsselnamen; geben Sie einfach „Temp“ ein. Anschließend hangeln Sie sich zum Schlüssel „HKEY_LOCAL_MACHINE\Temp\ControlSet001 Control\CrashControl“ durch. Doppelklicken Sie auf „AutoReboot“ und ändern Sie den Wert in 0. Speichern Sie die Änderung, indem Sie zuerst wieder „HKEY_LOCAL_MACHINE“ markieren und dann im Menü auf „Struktur entfernen“ klicken.

Für das Notfall-Windows haben wir eine eigene Projekt-Seite (c’t-Link) auf ct.de eingerichtet. Änderungen oder zusätzliche Skripte werden wir dort veröffentlichen. Sie erreichen über die Projekt-Seite auch das Forum zum c’t-Notfall-Windows 2013. (bae)

### Literatur

[1] Marion Marschalek, Tarnen, täuschen und tot stellen, Die Anti-Virus-Tricks der Trojaner, c’t 20/13, S. 190

[2] Axel Vahldiek, Ballast abwerfen, Platz schaffen auf der Windows-7-Partition, c’t 17/12, S. 74

***www.ct.de/1326174*** c't