

18 Sicherung und Archivierung

Digitalfotos sind vielen Gefahren ausgesetzt. Doch gibt es genügend Maßnahmen, um den Umgang mit ihnen sicher zu machen. Das zentrale Konzept für den Erhalt Ihrer Daten ist dabei das Anfertigen von Sicherungskopien von Bilddateien und Katalogen.

Daneben geht es in diesem Kapitel im Besonderen darum, wie Sie dem unbemerkten Verlust von Datenintegrität bei Bilddateien vorbeugen. Dieses Problem tritt für sich genommen zwar sehr selten auf. Wenn Sie allerdings Dateien über Jahrzehnte aufbewahren, steigt das Risiko stark an, davon betroffen zu sein. Weiterhin geht es in diesem Kapitel konkret um die unterschiedlichen Sicherungsstrategien für Arbeits- und Archivfotos sowie darum, wie und warum Sie Fotos archivieren sollten.

Einige der hier vorgestellten Maßnahmen sind weniger aufwändig, andere verlangen mehr Aufwand. Eine für jeden geeignete Lösung kann ich nicht liefern. Sie müssen letztlich selbst entscheiden, welche Risiken Sie vertreten und wie viel Zeit Sie investieren wollen.

18.1 Redundanz schaffen

Den gesamten Bestand an Digitalfotos zu verlieren ist eine Vorstellung, die am Sinn der Digitalfotografie zweifeln lassen kann. In der Analogfotografie war das Risiko, alle Dias oder Negative auf einen Schlag zu verlieren, sehr gering und nur durch wenige Bedrohungen wie beispielsweise Brandkatastrophen möglich. Deutlich einfacher ist es, alle seine Digitalfotos auszulöschen. Ein paar falsche Mausklicks, ein Festplattendefekt oder ein Virus reichen hier unter Umständen aus.

In der Digitalfotografie können Sie jedoch sehr preiswerte exakte Kopien Ihrer Fotos anfertigen. Wenn Sie dies in ausreichender Anzahl und auf die richtige Weise machen, ist das digitale Fotoarchiv sicherer, als es das ana-

loge je sein konnte. Sie können z. B. eine Festplatte mit allen Fotos außer Haus lagern und wären somit sogar vor einem Brand geschützt.

Die Hauptstrategie bei der digitalen Datensicherung besteht daher nicht im bestmöglichen Schutz des Originals wie bei den Dias oder Negativen. Das ist auch wichtig, steht aber nicht an erster Stelle. Stattdessen gehen Sie davon aus, dass immer etwas passieren kann, und sorgen für ausreichende Redundanz, um im Fall des Datenverlusts eine Sicherheitskopie zur Hand zu haben.

Drei Kopien zu jeder Zeit

Wie viel Redundanz ist dabei nötig? Einer Faustregel nach sollte man inklusive des Originals jederzeit mindestens drei Ausfertigungen jeder wichtigen Datei haben. Allerdings ist dies eine Vereinfachung. Es kommt auch darauf an, ob die Redundanz ausreicht, um gegen alle Risiken geschützt zu sein. Es nützt nichts, wenn Sie die drei Ausfertigungen auf derselben Festplatte haben und diese kaputtgeht – oder Ihr Computer gestohlen wird.

Daher geht es auch darum, die Backups (Sicherungskopien) möglichst *offline* (vom Computer getrennt) und teilweise auch *offsite* (in einem anderen Gebäude) aufzubewahren, um Gefahren optimal vorzubeugen. Das Offline-Backup ist nicht ständig an den Computer angeschlossen und befindet sich im Idealfall in einem anderen Raum. Es schützt vor Diebstahl, Viren, Überspannung und menschlichen Fehlern wie versehentlichem Löschen oder Überschreiben. Das Offsite-Backup wird in einem anderen Gebäude gelagert und bietet zusätzlichen Schutz gegen Diebstahl, Feuer und Überschwemmung.

Abb. 18-1

Backups sollten möglichst so angefertigt werden, dass inklusive Original mindestens drei Ausfertigungen einer Datei existieren.

Medienredundanz

Zusätzlich können Sie auf verschiedene Medientypen setzen: Auf Festplatten *und* optischen Medien wie DVD und Blu-ray Disc zu sichern, mit ihren jeweiligen Stärken und Schwächen und ihren unterschiedlichen Dateisystemen, ist sicherer, als sich nur auf Festplatten zu verlassen. Denn beide haben ihre eigenen Vor- und Nachteile. Für kleine Dateien wie beispielsweise Lightrooms Katalogdateien kommt zusätzlich ein Internet-Backup in Frage, das vor Diebstahl und Katastrophen am wirksamsten schützt, da die Daten sofort außer Haus gelagert werden. Mehr zu den Vor- und Nachteilen der verschiedenen Backup-Medien siehe Tab. 18-1.

Ich sichere mittlerweile nur noch auf Festplatten und einige wichtige Daten zusätzlich per Internet-Backup. Der Aufwand für das Brennen optischer Medien ist mir zu hoch. Allerdings ergreife ich zusätzliche Maßnahmen, um einige der Nachteile von Festplatten auszugleichen (siehe unten).

Medium	Vorteile	Nachteile	Sachgerechter Umgang
Festplatten	<ul style="list-style-type: none"> ■ schnell, komfortabel, mehrfach beschreibbar ■ als externe Festplatten einfach offline und offsite lagerbar 	<ul style="list-style-type: none"> ■ kein Schreibschutz, daher anfällig für Viren und Benutzerfehler ■ Diebstahlgefahr (bei externen, versteckten Festplatten Risiko gering) 	<ul style="list-style-type: none"> ■ Magnetquellen können Inhalt zerstören ■ vorsichtiger Transport
Optische Medien	<ul style="list-style-type: none"> ■ lassen sich nur einmal beschreiben, Viren oder Benutzerfehler können keine Dateien löschen! (abgesehen von RW-Varianten oder DVD-RAM) ■ Unempfindlichkeit gegenüber Magnetfeldern ■ einfach offline lagerbar ■ geringer Preis ■ geringe Diebstahlgefahr 	<ul style="list-style-type: none"> ■ umständlich in der Handhabung, langwieriger im Anfertigen und auch im Wiederherstellen des Backups ■ nicht mehrfach beschreibbar 	<ul style="list-style-type: none"> ■ Licht, Hitze und Feuchtigkeit verringern Lebensdauer ■ in Archivhüllen aufbewahren ■ mit CD-/DVD-Filzstift nur auf dem inneren Plastikrand beschreiben
Internet-Backup (Online-Backup)	<ul style="list-style-type: none"> ■ sofort offsite, ohne dass Sie das Backup »aus dem Haus tragen« müssen (was einfach nicht zu jedem Zeitpunkt möglich ist) ■ kann bei entsprechender Einrichtung (ständige Internetverbindung, automatische Ausführung) am komfortabelsten sein 	<ul style="list-style-type: none"> ■ nur für kleine Datenmengen geeignet, da DSL-Upload-Raten sehr gering sind und dadurch auch die z.T. hohen Backup-Kapazitäten von über 50 GB nicht viel nützen ■ Integrität des Backups schlecht nachprüfbar ■ Wer übernimmt die Verantwortung? 	<ul style="list-style-type: none"> ■ nicht für den Fotobestand nutzen, aber z. B. für Lightrooms Katalogdateien ■ nicht als einziges Backup-Medium nutzen

Tab. 18-1

Überblick Backup-Medien

Ausbreiten fehlerhafter Dateien verhindern

Das bloße Anfertigen von Backups hat allerdings eine Schwäche: Was passiert, wenn ein Schaden an einer Originaldatei auftritt und ich diesen nicht sofort bemerke? Vermutlich überträgt sich der Schaden bei den nächsten Sicherungen unbemerkt auf meine beiden Backups. Wenn ich die Datei benötige, muss ich womöglich feststellen, dass alle drei Ausführungen davon beschädigt sind. Hier nützt leider noch so viel Redundanz nichts.

Wenn Sie optische Medien zur Sicherung verwenden, die nur einmal beschreibbar sind, haben Sie dieses Problem nicht. Die Daten, einmal gebrannt, können nicht überschrieben werden. Der Nachteil der optischen Medien wird zu einem Vorteil. Falls Sie Festplatten verwenden, können Sie sich etwas von den optischen Medien abschauen und die Sicherungen über ein »*schreibgeschütztes*« Backup erstellen. Dabei behandeln Sie die Sicherungsfestplatte wie ein optisches Medium: Sie fügen nur Daten zur Festplatte hinzu. Löschen und Ersetzen sind »untersagt«.

Ein solches Backup-Verfahren ist allerdings für Dateien, die sich laufend ändern, hinzukommen oder entfernt werden, ungeeignet. Deshalb unterscheide ich zwischen Arbeitsdateien und archivierten Dateien. Arbeitsdateien, also aktuelle Kataloge und Bilddateien, sichere ich mit

einem sogenannten *Spiegel-Backup*, bei dem regelmäßig und automatisch die Sicherungen an das Original angepasst werden (siehe Abschnitt 18.3). Bei archivierten Dateien, also Dateien in einem Zustand der Abgeschlossenheit, verwende ich ein schreibgeschütztes Backup (siehe Abschnitt 18.5).

Was ist mit Backup-Systemen, die die gespeicherten Dateien nicht überschreiben, sondern eine neue Version speichern, z. B. Apples *Time Machine* auf dem Mac? Die meisten dieser Systeme, auch *Time Machine*, eignen sich für die Sicherung von Katalogen, aber nicht unbedingt für die Sicherung von Bilddateien. Jedes Mal, wenn sich beispielsweise die Metadaten einer DNG-Datei ändern, würde die ganze Bilddatei als neue Version gesichert. Die Sicherungsfestplatte würde also schnell gefüllt und *Time Machine* müsste beginnen, alte Dateien zu löschen, um Platz zu schaffen.

Bilddateien aus Vorschauen wiederherstellen

Möglicherweise kommt es bei Ihnen irgendwann zu einer Katastrophe und Sie verlieren einen Teil Ihrer Bilddateien unwiederbringlich. Falls Sie den Katalog noch haben, in den die Fotos importiert wurden, können Sie diese in geringerer Qualität wiederherstellen. Allerdings nur mit einigen Abstrichen und insgesamt großem Aufwand. Sie machen sich dabei die Vorschauen und evtl. vorhandenen Smart-Vorschauen zunutze.

Laden Sie zunächst das Skript *ExtractPreviews* herunter und installieren Sie es. Anschließend wählen Sie die betreffenden Fotos im Katalog aus und rufen über das Script-Menü das Skript auf. Es speichert die Vorschauen dann als JPEG-Dateien (Vorschauen sind ohnehin nur leicht modifizierte JPEGs) in einen Ordner. Es nimmt immer die größte Vorschau, die für ein Foto vorhanden ist.

Falls Sie Smart-Vorschauen (bei denen es sich lediglich um verkleinerte DNG-Dateien handelt) angelegt haben, können Sie auch diese extrahieren. Stellen Sie dazu die betreffenden Fotos in einer Sammlung zusammen, z. B. über *Bibliothek* ▷ *Nach allen fehlenden Fotos suchen*, und exportieren Sie die Sammlung als Katalog. Beziehen Sie die Smart-Vorschauen dabei ein. Öffnen Sie den Ordner des neuen Katalogs und kopieren oder verschieben Sie den Smart-Vorschau-Ordner (*Katalogname Smart Previews.Irdata*) an einen anderen Ort. Benennen Sie den Ordner um, sodass das *.Irdata* entfernt wird. Importieren Sie den Ordner anschließend in einen neuen Lightroom-Katalog.

Mit Smart-Vorschauen erhalten Sie die Vorzüge von Raw-Dateien und die meisten Metadaten der Fotos. Mit den normalen Vorschauen erhalten Sie die Dateinamen und bei 1:1-Vorschauen außerdem das Foto in Originalgröße. Insofern würde ich im Katastrophenfall immer beide Vorschautypen extrahieren und dann weitersehen. Es wird evtl. einige Zeit dauern, bis Sie alle Fotos identifiziert, umbenannt und mit dem ursprünglichen Katalog verknüpft haben.

18.2 Maßnahmen zur Sicherstellung der Datenintegrität

Eines der unangenehmsten Dinge in der Digitalfotografie ist der Verlust der Integrität der Daten – also »kaputte Dateien«. Wenn ein Negativ in der Analogfotografie einen Kratzer hat, ist das Foto immerhin noch zu gebrauchen. Ändert sich allerdings nur ein einzelnes Bit einer Bilddatei, ist eventuell die ganze Datei nicht mehr lesbar. Kein Problem, ich habe ja zwei Sicherungskopien, werden Sie vielleicht sagen. Das Unangenehme ist aber, dass Sie fehlerhafte Dateien in der Regel nicht sofort bemerken, unter Umständen erst nach langer Zeit oder überhaupt nicht. Wenn Sie beispielsweise eine Festplatte einige Monate liegen lassen, wie können Sie dann sicher sein, dass die Daten darauf noch intakt sind?

Dass man sich als Benutzer um solche Dinge überhaupt kümmern muss, liegt daran, dass es noch keine durchgehende Fehlerüberprüfung in der Dateiverarbeitung gibt. Die heutigen Dateisysteme sind z. B. noch nicht so weit entwickelt, dass sie automatisch einen Datenträger auf durch Alterung verursachte Fehler überprüfen können. Aber fehlerhafte Dateien können beispielsweise auch bei Kopiervorgängen entstehen. Über einige Maßnahmen lässt sich das Risiko jedoch deutlich eindämmen.

Datenintegrität durch Import überprüfen

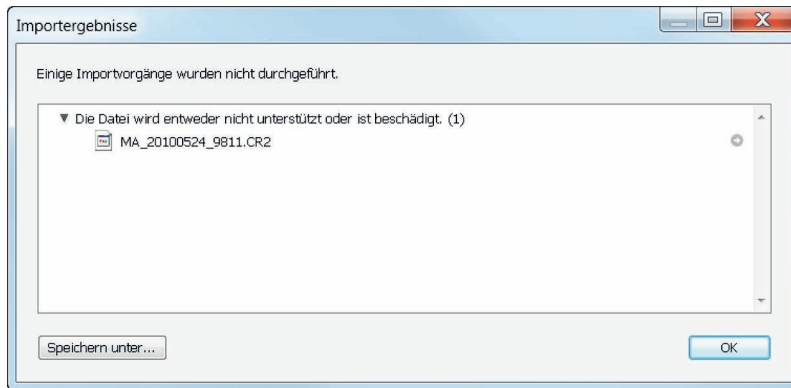
Fehlerhafte Bilddateien erkennen Sie am einfachsten, indem Sie sie in Lightroom importieren. Es gibt zwei Arten von Fehlern: Fehler in der Dateistruktur und Fehler in den Bilddaten. Die erste Art führt dazu, dass Lightroom die Dateien nicht mehr öffnen kann. Lightroom weist dann am Ende des Importvorgangs darauf hin, dass es einige Dateien nicht lesen konnte, und zeigt eine Liste der Dateien an (siehe Abb. 18–3). Sie können solche Dateien aber meist schon im Importieren-Dialog daran erkennen, dass die Miniaturen nicht angezeigt werden.

Die andere Art von Fehlern, bei denen die Bilddaten selbst Fehler enthalten, bemerkt Lightroom überhaupt nicht. Sie müssen also jedes Foto ansehen, um diese Fehler auszuschließen. Im Allgemeinen sehen Sie sie sofort in der Rasteransicht: Große Teile des Fotos fehlen komplett, stattdessen sehen Sie an diesen Stellen ein auffälliges Muster in knalligen Farben (siehe Abb. 18–3 B). Im Importieren-Dialog scheint mit diesen Dateien zunächst alles in Ordnung zu sein, weil Lightroom dort die von der Kamera eingebetteten Vorschauen anzeigt. Erst im Bibliothek-Modul, wo Lightroom seine eigenen Vorschauen erzeugt, werden diese Fehler sichtbar.

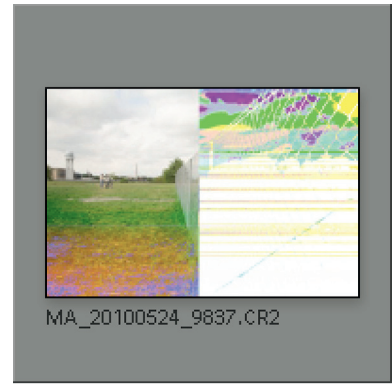


Abb. 18–2

Sind Sie sicher, dass diese Medien (noch) Ihre gesicherten Fotos enthalten? Von den vielen Gefahren, die dem Fotobestand drohen, ist schleichender Verlust der Datenintegrität besonders unangenehm, da man ihn nicht sofort bemerkt.



A



B

Abb. 18-3

Die Integrität von Fotos überprüfen

- A) Einige fehlerhafte Bilddateien identifiziert Lightroom beim Import
 B) und andere nicht – nur Sie können sie erkennen.

Sie können sich zu jeder Zeit mit der Import-Methode behelfen: Wenn Sie beispielsweise ein Backup mit Fotos überprüfen wollen, legen Sie einen temporären Katalog an und importieren die Fotos, um sie anschließend durchzusehen. Nur ist das Ganze sehr aufwändig. Daher lasse ich Backups lieber automatisch anhand von Prüfsummen (siehe unten) kontrollieren.

Hinter fehlerhaften Dateien steht immer eine Ursache. Im Schadensfall sollten Sie so schnell wie möglich versuchen, diese zu ermitteln, um weitere Fehler vermeiden zu können. Meist liegt es an Datenträgern (Speicherkarten, Festplatten, optische Medien), die dann ausgetauscht werden müssen.

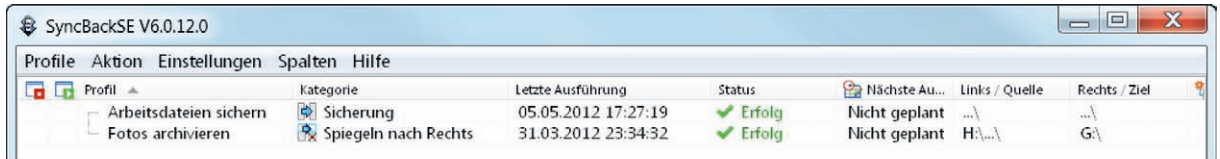
Backup-Software für wichtige Kopiervorgänge benutzen

Eine sinnvolle Maßnahme gegen Datenverlust ist das Nutzen von speziellen Backup- bzw. Synchronisationsprogrammen für alle regelmäßigen Kopiervorgänge. Dies hat gegenüber dem Kopieren von Hand mit dem Explorer/ Finder mehrere Vorteile.

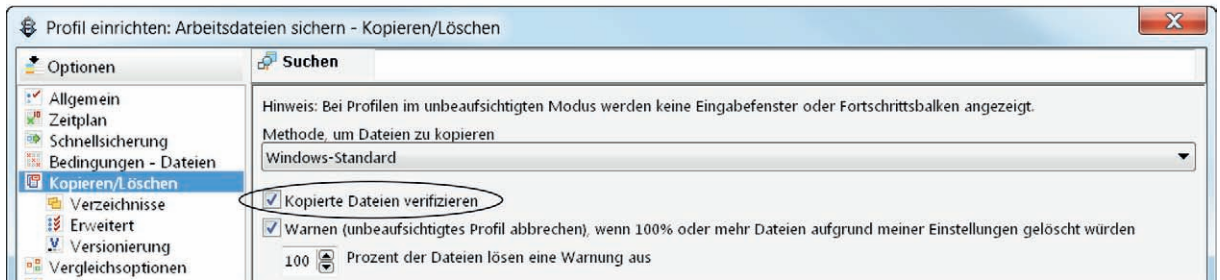
Backup-Programme bieten Schutz vor Benutzerfehlern, indem Einstellungen für regelmäßige Kopiervorgänge gespeichert werden. Hierfür legen Sie ein *Profil* mit den Einstellungen an und rufen es dann für einen Kopiervorgang auf – genau wie bei einer Vorgabe in Lightroom. Diese Profile lassen sich in der Regel automatisch ausführen (*Scheduling*), entweder zu vorher festgelegten Zeiten oder bei definierten Ereignissen, z. B. wenn eine bestimmte Festplatte angeschlossen wird oder beim Start des Computers.

Eine weitere wichtige Funktion ist die Überprüfung auf Übertragungsfehler (*Verifizierung, sichere Übertragung*). Hierdurch wird nach dem Kopieren überprüft, ob die Kopie genau dem Original entspricht. Daten könnten z. B. durch Fehler im Arbeitsspeicher während der Übertragung beschädigt werden. Die Verifizierung ist nicht selbstverständlich und wird weder bei Kopiervorgängen in Lightroom noch im Explorer oder Finder vorgenommen. Man kann sie aber in vielen Backup-Programmen einstellen. Wenn

Sie eine Datei innerhalb derselben Partition *verschieben*, benötigen Sie die Verifizierung übrigens nicht. Hierbei werden keine Daten übertragen, es werden nur die Einträge im Dateisystem für diese Datei angepasst.



A



B

Abb. 18-4

Backup-Programme

A) SyncBack mit mehreren Profilen

B) Die Verifizierung der übertragenen Dateien lässt sich in vielen Backup-Programmen zuschalten.

Gute Backup-Software sollte meiner Meinung nach über alle oben genannten Eigenschaften verfügen. Für Windows gibt es z. B. das Programm *Sync-Back* in einer Shareware- und einer Freeware-Version, für den Mac z. B. *ChronoSync* (Shareware). Backup-Programme können Sie an verschiedenen Stellen einsetzen: beim Spiegel-Backup der Arbeitsdateien, beim Übertragen der Arbeitsdateien ins Archiv und schließlich beim Anfertigen der Archiv-Backups.

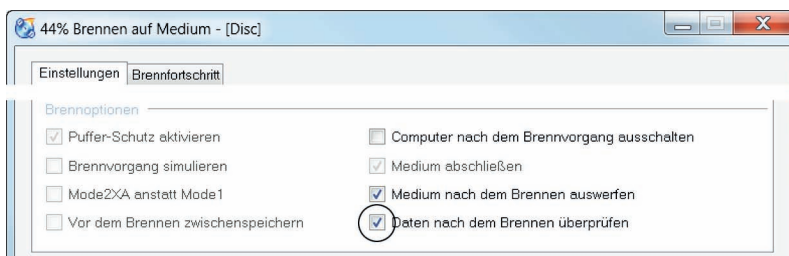


Abb. 18-5

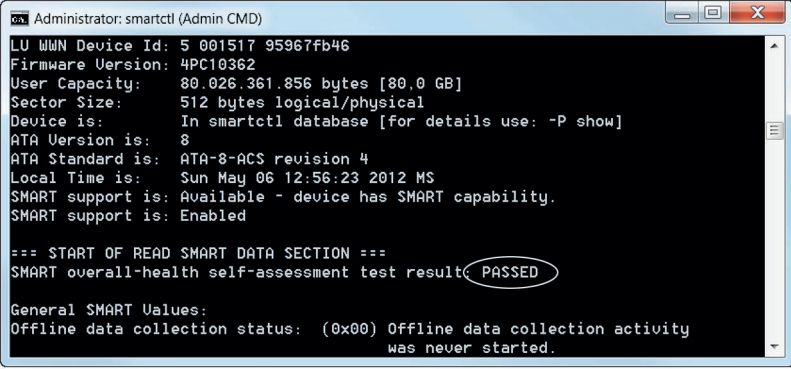
Auch beim Brennen von optischen Medien sollten Sie die gebrannten Daten verifizieren lassen. Viele Brennprogramme beherrschen das. Unter Windows eignet sich dazu das kostenlose Programm *CDBurnerXP* (nebenstehend abgebildet), auf dem Mac können Sie das Standard-Brennprogramm verwenden.

Festplatten vorbeugend überprüfen

Um Datenverlust vorzubeugen, können Sie Festplatten regelmäßig vorbeugend überprüfen.

Die Hardware der Festplatte wird über das SMART-System geprüft, das in jeder Festplatte eingebaut ist. Unter Windows benutze ich die *Smartmon-tools* (kostenlos), um den SMART-Status meiner Festplatten anzuzeigen. Auf dem Mac lässt sich das mitgelieferte Festplattendienstprogramm oder

z. B. *SMARTReporter* (kostenlos) verwenden. Bei externen Festplatten lässt sich der SMART-Status mitunter nicht so einfach auslesen: Der FireWire-Anschluss unterstützt SMART z. B. überhaupt nicht. Bei USB-Laufwerken hängt es vom Modell und von der auslesenden Software ab. Über eSATA funktioniert das Auslesen in der Regel am zuverlässigsten. Allgemein gilt: Festplatten, die den SMART-Test nicht mehr bestehen, haben ein deutlich höheres Risiko, in nächster Zeit auszufallen oder Fehler aufzuweisen, und sollten sofort ausgetauscht werden.



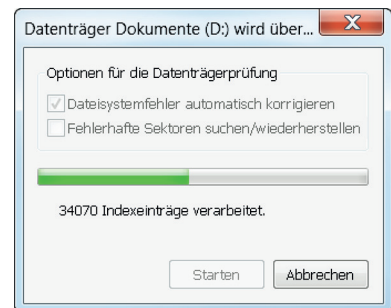
```

Administrator: smartctl (Admin CMD)
LU WWN Device Id: 5 001517 95967fb46
Firmware Version: 4PC10362
User Capacity: 80.026.361.856 bytes [80.0 GB]
Sector Size: 512 bytes logical/physical
Device is: In smartctl database [for details use: -P show]
ATA Version is: 8
ATA Standard is: ATA-8-ACS revision 4
Local Time is: Sun May 06 12:56:23 2012 MS
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED

General SMART Values:
Offline data collection status: (0x00) Offline data collection activity
was never started.
  
```

A



B

Abb. 18-6

Festplatten überprüfen

- A) Programme wie Smartmontools zeigen den SMART-Status einer Festplatte an.
 B) Dateisystemüberprüfung unter Windows

Weiterhin können Sie das Dateisystem einer Festplatte überprüfen (dieses ist für die Dateien, was der Lightroom-Katalog für die Bilddateien ist). Es kann beispielsweise bei einem Stromausfall oder während des regulären Betriebs beschädigt werden. Ist das der Fall, werden Dateien evtl. nicht mehr erkannt oder versehentlich überschrieben. Um Datenverlusten vorzubeugen, können Sie das Dateisystem regelmäßig überprüfen und im Fehlerfall reparieren lassen. Das geschieht für jede Partition einer Festplatte einzeln. Unter Windows heißt die Funktion *Fehlerüberprüfung* (zu finden im Kontextmenü eines Laufwerks unter *Eigenschaften* > *Tools* > *Fehlerüberprüfung*, siehe Abb. 18-6 B). Auf dem Mac können Sie eine Partition mit dem Festplattendienstprogramm (unter *Programme* > *Dienstprogramme*) überprüfen.

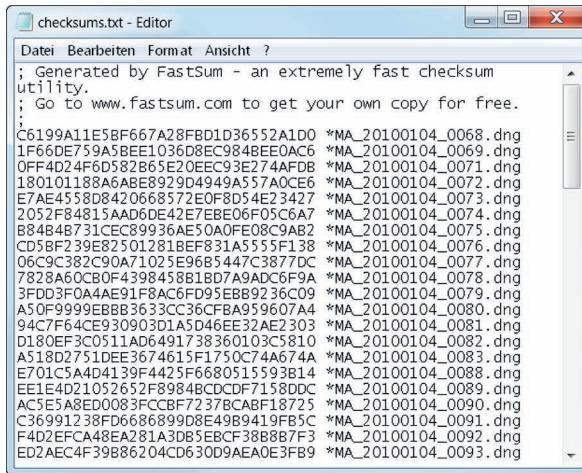
Beides, die Überprüfung des SMART-Status und der Dateisysteme, ist in regelmäßigen Abständen für alle Festplatten sinnvoll. Ein Dateisystem, das nur selten verwendet wird, muss aber nur entsprechend selten überprüft werden.

Prüfsummen verwenden

Eine Prüfsumme ist so etwas wie ein Fingerabdruck einer Datei. Mit ihrer Hilfe lässt sich feststellen, ob sich eine Datei verändert hat. Dazu berechnet man die Prüfsumme zu einem Zeitpunkt, zu dem man weiß, dass die Datei in Ordnung ist. Von Zeit zu Zeit kann man die Prüfsumme neu berech-

nen und mit der alten vergleichen. Stimmen die Prüfsummen nicht mehr überein, hat sich die Datei verändert und ist vermutlich – wenn sie nicht vom Benutzer verändert wurde – defekt (die Wahrscheinlichkeit, dass zwei unterschiedliche Dateien dieselbe Prüfsumme ergeben, ist extrem gering).

Traditionell werden Prüfsummen für alle Dateien eines Ordners als sogenannte Digest-Datei gespeichert (siehe Abb. 18–7 A). Diese Datei wird dann zur Aufbewahrung einfach im selben Ordner abgelegt.

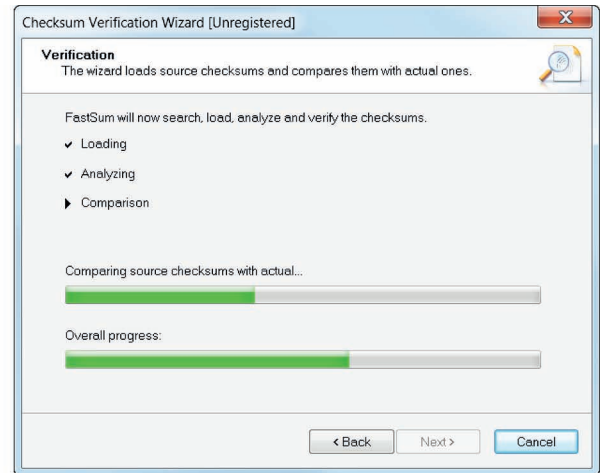


```

Datei Bearbeiten Format Ansicht ?
; Generated by FastSum - an extremely fast checksum
utility.
; Go to www.fastsum.com to get your own copy for free.
;
C6199A11E5BF667A28FBD1D36552A1D0 *MA_20100104_0068.dng
1F66DE759A5BEE1036D8EC984BEE0AC6 *MA_20100104_0069.dng
0FF4D24F6D582B65E20EECC93E274AFDB *MA_20100104_0071.dng
180101188A6ABE8929D4949A557A0CE6 *MA_20100104_0072.dng
E7AE4558D8420668572E0F8D54E23427 *MA_20100104_0073.dng
2052F84815AAD6DE42E7EBE06F05C6A7 *MA_20100104_0074.dng
B84B48731CEC89936AE50A0FE08C9AB2 *MA_20100104_0075.dng
CD5BF239E825012818EF831A5555F138 *MA_20100104_0076.dng
06C9C382C90A71025E9685447C3877DC *MA_20100104_0077.dng
7828A60CB0F4398458B1BD7A9ADC6F9A *MA_20100104_0078.dng
3FDD3F0A4AE91F8AC6FD95EBB9236C09 *MA_20100104_0079.dng
A50F9999EBB83633CC36CFBA959607A4 *MA_20100104_0080.dng
94C7F64CE930903D1A5D46EE32AE2303 *MA_20100104_0081.dng
D180EF3C0511AD6491738360103C5810 *MA_20100104_0082.dng
A518D2751DEE3674615F1750C74A674A *MA_20100104_0083.dng
E701C5A4D4139F4425F668051593814 *MA_20100104_0088.dng
EE1E4D21052652F8984BCDCDF7158DDC *MA_20100104_0089.dng
AC5E5A8ED0083FCCBF7237BCABF18725 *MA_20100104_0090.dng
C36991238FD6686899D8E49B9419FB5C *MA_20100104_0091.dng
F4D2EFC48EA281A3DB5EBCF38B8B7F3 *MA_20100104_0092.dng
ED2AEC4F39B86204CD630D9AEA0E3FB9 *MA_20100104_0093.dng

```

A



B

Abb. 18–7

Prüfsummen

A) Eine Digest-Datei von innen. Die Prüfsummen stehen jeweils links, rechts die Dateinamen.

B) Programme wie FastSum können leicht ganze Ordner überprüfen, wenn sie dort eine Digest-Datei vorfinden.

Leider gibt es im Moment noch wenige Programme, die komfortabel Dateien in mehreren Ordnern an einem Stück überprüfen können. Ich benutze dazu *FastSum* (Shareware), dieses Programm ist aber nur für Windows erhältlich. Auch das Programm *ImageVerifier* kann Prüfsummen erzeugen und verwalten, allerdings speichert es diese in seiner eigenen Datenbank. Das ist zwar komfortabel, aber dadurch ist man auch vom Programm abhängig.

Mit einer Prüfsumme lässt sich zwar kontrollieren, ob sich eine Datei verändert hat. Es ist allerdings nicht erkennbar, ob die Veränderung einen Fehler darstellt oder ob es sich um eine vom Benutzer gewollte Veränderung handelt. Daher eignet sich das Prüfsummen-Verfahren nur für Dateien, die bereits abgeschlossen sind und keinen normalen Veränderungen mehr unterliegen. Ich benutze es nur für die schreibgeschützten Archiv-Backups (siehe Abschnitt 18.5).

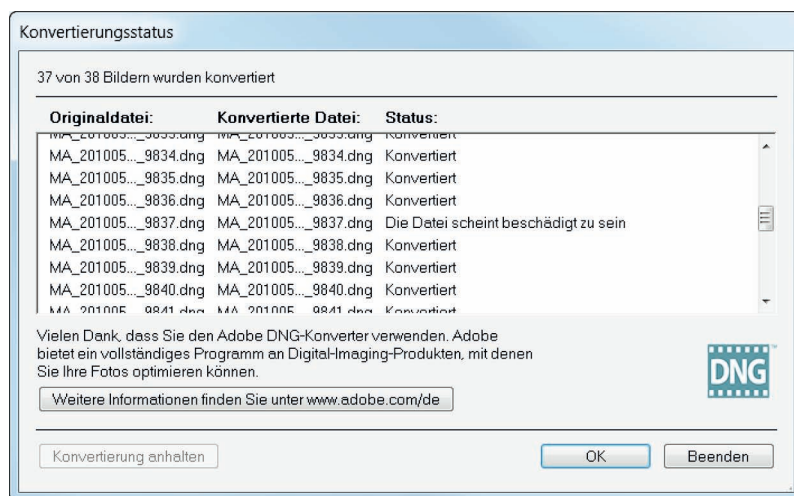
Prüfsummen in DNG-Dateien

Falls Sie das DNG-Format verwenden, können Sie die in den DNG-Dateien enthaltenen Prüfsummen verwenden. Dies ist deutlich eleganter als die

obige Lösung, denn die Prüfsumme wird jeweils automatisch bei Erzeugung der Datei gebildet und in der Datei selbst aufbewahrt. Dabei bezieht sie sich nur auf die Bilddaten. Andere Teile der Datei, z. B. die Metadaten oder die eingebaute Vorschau, können sich noch ändern, ohne dass die Prüfsumme dadurch ungültig würde.

Auf Seite 157 habe ich erläutert, wie Sie DNG-Dateien von Lightroom aus anhand der Prüfsumme verifizieren können. Dies ist aber nur für in Lightroom importierte Dateien möglich. Um auch Dateien außerhalb von Lightroom (also z. B. die Backups) zu überprüfen, können Sie den *Adobe DNG Converter* verwenden (kostenlos). Dazu konvertieren Sie die DNG-Dateien, die Sie überprüfen wollen, erneut nach DNG. Wählen Sie einen Ordner aus (über *Untergeordnet einschließen* können Sie leicht alle DNG-Dateien auf einer Festplatte überprüfen) und stellen einen temporären Ordner mit möglichst viel Platz als Ziel ein. Dann lassen Sie die Konvertierung laufen. Am Ende können Sie die neu erstellten Dateien löschen. Nach der Konvertierung zeigt der DNG Converter im Fenstertitel an, ob alle Dateien konvertiert werden konnten. Falls das nicht der Fall war, können Sie die Liste durchsehen und die betreffenden Dateien identifizieren (siehe Abb. 18–8).

Abb. 18–8
Prüfsummen in DNG-Dateien. Mit dem DNG Converter lassen sich DNG-Dateien auch außerhalb von Lightroom überprüfen.



Falls Sie hauptsächlich DNG-Dateien verwenden, können Sie auf das Anlegen zusätzlicher Prüfsummen für Ihre anderen Bilddateien (wie oben beschrieben) verzichten. Tritt beispielsweise ein Festplattendefekt auf, wird in der Regel auch eine der DNG-Dateien davon betroffen sein, sodass Sie ihn schnell bemerken sollten.