Hash-Funktion in P2P-Netzwerken
Genetischer Fingerabdruck oder Etikettenschwindel?!

" *Im Wege eines Testdownloads wurde ein Teil der über Ihren Anschluss angebotenen Datei heruntergeladen. Diesem Teil ist ein bestimmter "Hashwert" zugewiesen, der zweifelsfrei belegt dass es sich bei der über Ihren Anschluss öffentlich zugänglich gemachten Datei um das Musikstück unserer Mandantschaft handelt.*
Der Hashwert ist für eine Datei insofern charakteristisch, als kein anderes Dokument mit demselben Hashwert konstruiert werden kann. Der Hashwert ermöglicht somit, gleich einem Fingerabdruck, die zweifelslose Identifizierung einer Datei. Eine Verwechslung ist bei diesem Verfahren ausgeschlossen. Da unter dem gleichen Hashwert keine unterschiedlichen Dateien angeboten werden können, steht fest, das über Ihren Anschluss das streitgegenständliche Musikstück unter Verletzung der Tonträgerrechte unser Mandantschaft öffentlich zugänglich gemacht worden ist."

Diese oder ähnliche Argumentationen sind regelmäßig zu lesen, wenn man die diversen Schreiben von abmahnenden Kanzleien studiert.
Was ist nun dran an dem eindeutigen und gerichtsbewehrten Beweis der Hash-Funktion?
Zur Beantwortung dieser Frage fanden mehrere Gespräche mit Herrn Dr. Rolf Freitag statt.

Dr. Rolf Freitag

8.12.1968 Geboren in Cuxhaven an der Elbe
1975-1989 Grundschule, Gesamtschule, Hauptschule, Höhere Handelsschule, Fachgymnasium Technik, Teilnahmen bei Jugend Forscht
1990-1996 Physik-Studium an der Uni Bremen,
Diplom-Arbeit: Diffusive dynamische Lichtstreuung von Substanzen am kritischen Punkt
1995 - 2001 Teilzeit-Zusatz-Aufbau-Studium an der Fernuni Hagen:
Praktische Informatik
1997-2001 Promotion an der Uni Ulm: Korrelationsmethoden für hoch dynamische Zeitauflösung in der Foto- und Kathodolumineszenz(siehe erster Weblink unten)
2001 Kryptografics GmbH Nürnberg: Anwendung u. Zertifizierung von echten Zufallszahlengeneratoren
2002-9/2004 Daum Electronic GmbH Fürth: Hard- u. Software-Entwicklung zu Ergometern
Seit 2003 CCC-Mitgliedschaft, Seit 2006 bei Siemens.

Erläuterung des Standpunkts:
Ein Beweis ist, wenn die betreffende Datei vollständig und lokal auf einer Festplatte sich befindet, wobei Byte für Byte verglichen wird

1. Grundlage - Die Fakedatei

Ein "Fake" ist eine Fälschung oder ein Imitat.
Bei Dateien sind "Fakes" häufig, denn der Dateiname ist völlig unabhängig vom Dateiinhalt und die Namensgebung einer Datei hängt neben dem Inhalt unter Anderem auch ab von der Plattform, dem verwendeten Dateisystem, und dem sozikulturellen Kontext des Namengebers. Hierdurch ist es weitgehend Ansichtssache und stark vom Kultur- und Sprachraum abhängig, ob ein Dateiname ein Fake ist oder nicht. Es gibt aber auch gezielte Fakes, beispielsweise um in Tauschbörsen viele gefälschten Dateien zu einem Musiker einzustellen und so den Nutzern die Suche nach solchen Dateien zu Vergrellen. Daneben gibt noch viele andere Motive zum gezielten Faken, beispielsweise um Tauschbörsen als quasi, kostenlosen und privaten Webspace zu missbrauchen.
Ein Beispiel hierfür ist eine Datei, die den Namen:
"***Geiles_neues_Album_von_Marily_Manson.rar***" trägt, in Wirklichkeit aber das Urlaubsvideo der Familie Hempels auf Mallorca als DivX ist. Im Beispiel wollte Familie Hempels vielleicht einfach nicht, dass jemand Fremdes das Video sieht, der aufs Geratewohl nach "Urlaubsvideo" sucht. Darum haben sie Dateinamen und -endung (Präfix u. Suffix) einfach geändert und beispielsweise den eD2K-Link mit dem falschen Namen an Freunde und Verwandte geschickt und zusätzlich den echten Dateinamen per Mail - mit dem Hinweis, dass die Datei erst nach dem Herausnehmen aus dem Share zurück-benannt werden soll.
Hinzu kommt bei einer Datei auf einem Datenträger, das sie an einer bestimmten Stelle eines Dateisystems liegt, d. h. in einem bestimmten Verzeichnis liegt, und das auch über diese Stelle gefakt werden kann, weil Standards wie FHS beschreiben welche Systemdateien an welcher Stelle liegen sollten und welche Dateien wo NICHT liegen sollten.

Zu den Metadaten einer Datei gehören neben dem Namen auch die Dateigröße, Modifikations-Zeit, Prüfsummen wie CRC32 usw. und die allermeisten Metadaten kann man frei wählbar einstellen; dafür gibt es viele Programme wie beispielsweise CRC Faker, das eine Datei mit vorgegebener Prüfsumme (CRC32), vorgegebenem Namen und vorgegebener Größe erzeugt und zudem bei zwei Läufen die Datei mit zwei verschiedenen Inhalten erzeugt.
Hinzu kommt, dass die Metadaten meist mehrdeutig sind. Beispielsweise kann die Dateigröße z. B. durch Sparse Files mehrdeutig sein und durch einen Soft Link können die Daten an einer ganz anderen Stelle unter einem ganz anderen Namen stehen.
Und Dateinamen hängen von der Codierung ab, mit der ein Dateisystem verwendet wird, denn beim Mounten kann man z. B. iocharset=utf8 oder iocharset=iso-8859-1 als Option angeben und entsprechend erhält man unterschiedliche Dateinamen.
Hinzu kommt, das man in Tauschbörsen auch modifizierte Tauschbörsenprogramme verwenden kann, so das man auch die Anzeige/Ausgabe von Daten und Metadaten faken kann, und über Proxies und offene WLANs kann man die IP-Nummer vom betreffenden Rechner verschleiern. Deshalb ist für einen Beweis ist immer noch die Beschlagnahmung und forensische Untersuchung von Festplatten oder anderen Datenträgern erforderlich. Alles andere kann nur schwache Indizien liefern.
Um zu zeigen wie leicht man bekannte Dateien vortäuschen kann, habe ich als simples Beispiel ein Skript geschrieben, das ich logischerweise noscript genannt habe.
Die damit gefakten Dateien haben den originalen Namen, die originale Größe und originale CRC-32-Prüfsumme von Dateien, die in Tauschbörsen weit verbreitet sind und auch bei Abmahnern von Tauschbörsen-Benutzern sehr beliebt sind.
Listen von weiteren bei Abmahnern von Tauschbörsen-Benutzern sehr beliebte Dateien findet man auch auf dieser Abmahnliste: Abmahnwiki: Wer mahnt was ab?.

Den Datei-Inhalt und die CRC32 der Originale, die von dem Skript gefakt werden, habe ich selbst überprüft; die Originale sind keine Fakes! Zudem ist der Titel halbwegs aussagekräftig.
Beispielsweise findet man in Dateien mit "Teenies" im Namen auch Teenies.
Die Herkunft der Originale in den Tauschbörsen ist unbekannt. Es kann sein, das die Dateien von den Rechteinhabern selbst in Tauschbörsen eingestellt wurden, denn es ist nicht ungewöhnlich, das Dateien zur besseren Vermarktung und auch zum späteren Abmahnen (und Abkassieren) in Tauschbörsen von den Rechteinhabern eingestellt werden, so das sie in den Tauschbörsen ganz legal sind und die Rechteinhaber das Gegenteil wieder besseren Wissens behaupten.

Zum Faken auch von Dateien gibt es nicht nur diverse Skripte, sondern auch Programme:
Fake File Generator
Napster Fake Generator
Usenet Fake Generator

Beispiel Script: <noscript>

```
#/bin/sh
#
# noscript: A (Bash) Script for faking some "interesting" files which
# can be found in P2P networks and which are often used for dissuation abuse.
# This Script uses the real file names and fakes a) the file size and c) the
# CRC-32 checksum.
# The working directory is the actual and the faking takes some hours and about 15 GB
disk space.
# At the script end the script cleans up by deleting the crcfaker files and itself.
# This is a simple example that it's easy to generate indications (fakes) and without
# confiscation and forensic analysis there is no court-proof evidence.
# Other sorts of fakes in P2P networks, e. g. faking an IP number via an open WLAN, can
be
# found e. g. in the Heise News.

# "THE BEER-WARE LICENSE" (Revision 43):
# Dr. Rolf Freitag (rolf.freitag@email.de) wrote this file.
# As long as you retain this notice you can do whatever
# the GPL (GNU public License) allows with this stuff.
# If you think this stuff is worth it, you can send me money via
# paypal or if we met some day you can buy me a beer in return.

# Version 0.21, 2008-08-10: Successfully tested, works without a bug,

# Todo: Checks, e. g. for wget, multithreading (CRC Faker is single-threaded), parame-
trisation,
# random timestamp for each file/dir, filetype specific faking of the file
# header, version for Unix/Linux and Cygwin (MS-Windows),
# be verbose set -x

# download CRC Faker, which fakes files with random bytes and a given CRC32 check-
sum
wget http://www.crc2003.250x.com/fakecrc-1.0.zip

# unzip
unzip fakecrc-1.0.zip

# fakes
#   Purzel
# fake_program CRC32   size/bytes file name
Linux/fakecrc 85363198 733657088 "Masturbation 04 (Scenes) [Purzel-Video.com] (So-
lo_Mast_Dildo) (512x384 Super High Quality SHQ) (VG) - 1h32m34s.avi"
Linux/fakecrc 71216f29 733990912 "Purzel Masturbation Nr.6.avi"
Linux/fakecrc 32ca98ae 732518400 "Purzel-Video 125 - Masturbation Nr 3.avi"
Linux/fakecrc 1f4b685c 735899648 "Purzel Video 166 - Dicke Lippen kleine L??cher 4
CD1.avi"
Linux/fakecrc eba26ebb 736216392 "Purzelvideo 89 - Masturbation Nr 2.avi"
Linux/fakecrc 07a07fbc 791248896 "Purzel.Video.Masturbation.11.XXX.DVD-
Rip.XviD.(Ripped.&.Released.by.M.E.G.A).avi"
Linux/fakecrc 16f3a039 730818560 "Purzel Video - Masturbation Nr. 1.avi"

#   Updown Entertainment
Linux/fakecrc 93378129 712396800 "GGG-Geile Girls-fertig zum vollsprit-
zen(divx,xxx,bukkake).avi"
mkdir "GGG.Absolut.Sperma.German.2005.XXX.DVDRiP.XviD-WDE"
Linux/fakecrc 4da1e28d 737757184
"GGG.Absolut.Sperma.German.2005.XXX.DVDRiP.XviD-WDE/wde-as.avi"
```

```
mkdir "GGG.Amili.lernt.schlucken.German.2005.XXX.DVDRiP.XviD-WDE"
Linux/fakecrc ff0716d0 737748992
"GGG.Amili.lernt.schlucken.German.2005.XXX.DVDRiP.XviD-WDE/wde-als.avi"
Linux/fakecrc ca795a1f 737738752
"GGG.Die.Tittenkoenigin.German.2005.XXX.DVDRiP.XviD-www.Bitworld.mpg"

#  Videorama GmbH
Linux/fakecrc 6db8d43c 1523912704 "Videorama Das beste aus Maximum Perversum 5
(Rip by Egofist).avi"
Linux/fakecrc 0020feb4 273002496 "Gina Wild - XXX [DivX].avi"
Linux/fakecrc abbef01a 729861120 "ArschgeileFlittchenXXXDivX.avi"
Linux/fakecrc 63ef76ce 734271488 "Blutjunge.Pfadfinderinnen.im.Sex-
Camp.XXX.MagmaTeeny.Divx502.avi"
Linux/fakecrc 02bd1586 161771520 "Flesh Hunter - Krystal Steal.avi"
Linux/fakecrc ce08d463 273002496 "Gina Wild - 4 - Durchgefickt.avi"
Linux/fakecrc ada737d3 132116992 "Krystal-Steal-Trained-Teens.avi"
Linux/fakecrc 38b664fd 732231680 "Porno_Giganten_XXX_German-DivX.avi"
Linux/fakecrc 4f4c3691 572391424 "Teenies.auf.Ibiza.dvd-rip.by.BadIragS.avi"
Linux/fakecrc c2561fa7 713865216 "Teeny_Exzesse_-
_Sommer_Sonne_freche_Goeren__german_XXX.ShareReactor.avi"
Linux/fakecrc e41288ff 700702720 "Teeny_Exzesse_Peep.ShareReactor.avi"
Linux/fakecrc 00c7c580 87359488 "Gina Wild - After Party.avi"
Linux/fakecrc 660d5114 32163840 "Gina Wild - mannervergewaltigung.avi"


# some trolling: political, war, weapons, crime, sex, music, industy data,
#                trading secrets, patent data, trash,
dd if=/dev/urandom of=Watergate_$((1+$(($RANDOM %10)))).doc
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=National_Defense_Secrets_$((1+$(($RANDOM %10)))).pdf
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=Blackwater_War_Crimes_$((1+$(($RANDOM %10)))).PDF
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=Al-Qaeda_$((1+$(($RANDOM %10)))).doc
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=Anthrax_Powder_$((1+$(($RANDOM %10)))).pdf
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=Bomb_$((1+$(($RANDOM %10)))).doc
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=Child_Porn_$((1+$(($RANDOM %10)))).jpg
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=Gina_Wild_$((1+$(($RANDOM %10)))).avi
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=Bushidos_Greatest_Hits_$((1+$(($RANDOM %10)))).rar
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=SIEMENS_Plans_2009_$((1+$(($RANDOM %10)))).zip
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=TRADING_SECRETS_$((1+$(($RANDOM %10)))).ZIP
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=Patent_data_$((1+$(($RANDOM %10)))).zip
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))
dd if=/dev/urandom of=Secret_$((1+$(($RANDOM %10)))).Encrypted
bs=$((1+$(($RANDOM % 512)))) count=$((42+$(($RANDOM / 42))))

# set an old timestamp
find ./ -exec touch -t 200$((5+$(($RANDOM % 3))))0$(($RANDOM % 10))$(($RANDOM
% 3))$((1+$(($RANDOM % 9))))$(($RANDOM % 2))$((1+$(($RANDOM %
9))))$(($RANDOM % 6))$(($RANDOM % 10)).$(($RANDOM % 6))$(($RANDOM % 10))
{} \;
```

```
# make clean (with self-deletion)
files="$0 fakecrc-1.0.zip index.htm Linux/fake-all.pl Linux/fakecrc Linux/fakecrc-gui \
Linux/README.GUI Linux/fake-one-random.pl Windows/fakecrc.exe Windows/fakecrc-
gui.exe"

for file in $files ; do
  # set size to 0; see also "Unix Power Tools"
  > "$file"
  # flush all buffers via sync
  sync
  unlink "$file"
  # flush all buffers via sync
  sync
done
rm -rf Linux
rm -rf Windows

exit 0
```

2. Grundlage Hash-Funktion:

Können mittels eines Hash-Funktions-Kollisions-Generator, gefakte Dateien mit originaler Prüfsumme versehen und in die P2P-Tauschbörse über einem längeren Zeitraum gestellt werden?
Ziel, es soll anhand dieser Hash-Kollisionen [wenn x≠y, aber h(x)=h(y)] bewiesen werden, dass gefakte Dateien mit originalem Hash, abgemahnte werden können?

Das ist eigentlich nicht nötig: Man kann auch die Tauschbörsen-Software so modifizieren, das sie bestimmte Dateien mit einem Hash-Wert anzeigt, ohne das diese Dateien wirklich existieren müssen!

Deshalb betone ich ja, das nur eine forensische Untersuchung der Datenträger (meist Festplatten), die Dateien wirklich nachweisen kann.
Also den Hash-Wert einer Datei wirklich ermitteln kann man nur mit der kompletten Datei; man benötigt also die komplette Datei und zwar lokal. Aber wenn man die Datei lokal hat, kann man die mit Programmen wie diff oder dupmerge direkt Bit für Bit mit dem Original vergleichen und kann auf Hash-Werte komplett verzichten.
Wenn irgendwo eine Datei mit einem Hash-Wert angezeigt wird, ist der Hash-Wert nur so vertrauenswürdig wie die Stelle, die ihn anzeigt. Das ist wie mit den Spam-Mails die ihnen viel Geld versprechen, bei näherer Überprüfung aber nur Betrug sind.
Solange Sie die Datei nicht direkt auf ihrem Rechner haben und direkt überprüfen können, haben können Sie da nie sicher sein!

Zum Hash-Wert in Tauschbörsen: Ich habe mal zum Testen ein mittelgroßes Share-Verzeichnis mit gut 300 GB eingerichtet und gesehen, das die (unmodifizierte) Tauschbörsen-Software ganz einfach alte Werte verwendet, die sie gespeichert hat denn die Tauschbörsen-Beteiligung lief in wenigen Sekunden an, obwohl ein Überprüfen der Hash-Werte natürlich auch ein komplettes Einlesen der Dateien im ShareVerzeichnis erfordert hätte, was aber gut eine Stunde gedauert hätte und währenddessen einen Core ganz ausgelastet hätte.
Das würde natürlich viel zu lange dauern, würde zu viel CPU-Last erzeugen und wird von Tauschbörsen-Software folglich nicht gemacht. Deshalb stehen die Hash-Werte in irgendwelchen Konfigurations-Dateien gespeichert und nur diese, aber nicht die wirklichen (aktuellen) werden verwendet! Und diese Konfigurations-Dateien kann man leicht verändern und zwar ohne irgendetwas an der Tauschbörsen-Software selbst verändern zu müssen!
Es reicht also völlig aus in Konfigurationsdateien ein paar Hash-Werte einzutragen oder zu modifizieren und dazu passende Dateien zu erzeugen oder die Dateien durch gleichnamige gleicher Größe auszutauschen, denn welche Hash-Werte die Dateien wirklich haben wird dann nicht mehr überprüft; Hash-Werte werden normalerweise nur ermittelt, wenn die Tauschbörsen-Software eine Datei als neu ansieht.
Vielleicht muss man noch die Zeitstempel der Dateien anpassen, damit sie als nicht neu angesehen werden, aber es gibt da kein nennenswertes Problem; dafür gibt es Programme wie Touch oder Stamp.

**Wie ist es mit der Feststellung des genauen Hash-Wertes.
Reicht ein Fragment oder muss die komplette Prüfsumme
(eine andere Bezeichnung für die Hash-Funktion) vorhanden sein?**

Programme wie CRC Faker fälschen auch den Hashwert einer kompletten, lokalen Datei!
Dateien kann man mit Hash-Werten nicht sicher vergleichen!
Deshalb gibt es ja Programme wie - diff- zum Vergleichen von Dateien, wobei Byte für Byte verglichen wird:

Wikipedia: Diff

Und deshalb habe ich z. B. bei meinem Programm - dupmerge - nie in Erwägung gezogen Prüfsummen zu verwenden, denn damit bekommt man eine unnötige Unsicherheit.

Also von einem Fragment auf den gesamten Inhalt zu schließen ist unsicher; bei einem kleinen Fragment wäre das so als ob man aus einer Urinprobe einer Person auch deren Wohnort bestimmen wollte.
Schließlich gibt es in Tauschbörsen Fakes, die zwar originale Stücke enthalten, beispielsweise am Anfang, sozusagen zum Anlocken, danach aber nur Datenmüll enthalten.

"...bei einem kleinen Fragment wäre das so als ob man aus einer Urinprobe einer Person auch deren Wohnort bestimmen wollte."

Dr. Rolf Freitag

**Mir liegt von einer abmahnenden Kanzlei eine Erklärung der Wirkungsweise ihrer Software vor. Darin wird festgestellt mittels Unterschrift des Abmahnanwaltes, dass kein Testdownload durchgeführt wird.
Wie könnte man hier die Beweiskraft einschätzen?**

Also wenn Logg-Firmen behaupten das sie mit ein paar nur aus der Ferne angezeigten Werten
etwas "beweisen" ist das eine Manipulation: Dem Gericht werden wichtige Informationen vorenthalten, die besagen, das es sich nur um schwache Indizien handelt, und die angezeigten Werte richtig sein könnten, aber nicht überprüft wurden.

Das ist so wie z. B. mit der Olympia-Eröffnungsfeier kürzlich, wo die Sängerin und das Feuerwerk im Fernsehen gefälscht waren; allein aus der Ferne kann man das bei den guten Fälschungen nicht erkennen und auch nicht überprüfen.

Erst durch Reporter vor Ort ist der Schwindel aufgeflogen:

Tagesschau.de

Über das Internet ist es nicht anders wie über das Fernsehen: Sofern Sie nicht auf einem anderen Weg kontrollieren, sind die Daten aus der Ferne unsicher und das merken sie ohne unabhängige Überprüfung nicht!

"*Im Wege eines Testdownloads wurde ein Teil der über Ihren Anschluss angebotenen Datei heruntergeladen.*"
Wie am Schluss meines Artikels in dem einen Telepolis-Artikel zu Fakes ausführlich dargelegt wird, gibt es nicht wenige Leute und sogar Firmen, die Fakes in Tauschbörsen einstellen und diese enthalten meistens Teile des Originals.
Es gibt auf diese Verfälschungen von Originalen, die Teile des Originals enthalten, sogar ein einen Patentantrag in den USA; vermutlich ist es inzwischen sogar patentiert.
Und da mehrere Firmen mit diesen Fälschungen sogar Werbung machen und es unübersehbar viele Fälschungen in Tauschbörsen gibt, braucht man über nur teilweise downgeloadete Dateien nicht zu diskutieren. Erst bei komplett downgeloadeten Dateien kann man sicher sein, das es sich um das Original und nicht um eine Fälschung handelt!

Was ist in Tauschbörsen wirklich technisch nachweisbar?

Einleitung

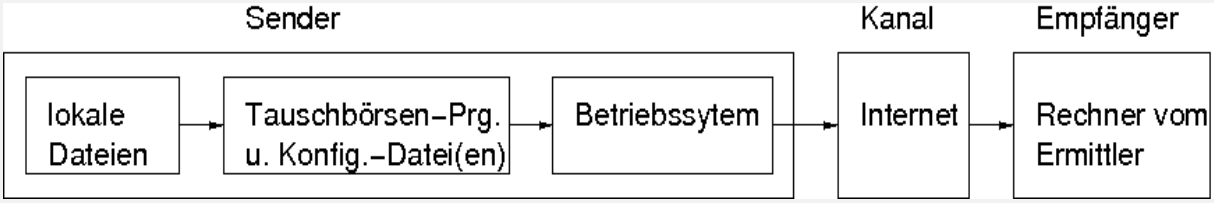
Abmahnungen wegen Urheberrechtsverletzungen in Tauschbörsen sind für viele Anwälte und einige Firmen ein einträgliches Geschäftsmodell, denn die Praxis zeigt das diejenigen, die eine Abmahnung erhalten, oftmals aus Angst vor höheren Forderungen die geltend gemachten Anwaltskosten zahlen, ohne diese juristisch prüfen zu lassen und auch ohne die Anschuldigungen inhaltlich zu überprüfen.

Deshalb ist hier ein kleiner Überblick über das, was rein technisch in Tauschbörsen im bzw. genauer über das Internet nachweisbar ist, mit dem Schwerpunkt des Anbietens von Dateien in Tauschbörsen, aber für das Downloaden gilt im Wesentliche das Gleiche.

Über die Praxis der Rechtspflege (Abmahnungen, Prozesse etc.) sagen die technischen Fakten aber wenig aus, denn Juristen und insbesondere Richter arbeiten nicht mit (Wahrscheinlichkeits-)Rechnungen sondern mit Überzeugungen und entsprechend zeigen unterschiedliche Gerichte unterschiedliche Rechtsauffassungen, die auch von der Tagesform abhängen und auch deshalb schwer vorhersehbar sind. Daher stammt die Römische Juristenweisheit „Vor Gericht und auf hoher See sind wir in Gottes Hand".

Informationstheoretische Betrachtung von Tauschbörsen

Informationstheoretisch hat man in einer Tauschbörse zwischen dem Sender/Anbieter in einer Tauschbörse und dem Empfänger/Ermittler einen klassischen Nachrichtenkanal mit Sender, Kanal und Empfänger:



Bei dem, was für den Empfänger (Ermittler) sichtbar ist, gibt es sehr viele Manipulationsmöglichkeiten schon beim Sender, die im Folgenden aufgelistet sind. Zur Erläuterung sind auch kurze Beispiele für die Shell dabei, mit den Ausgaben, die die Bash unter Linux anzeigt. Unter MS-Windows kann man für die Beispiele beispielsweise Cygwin oder diverse Programme wie 12Ghosts verwenden.

Dateien

Dateiattribute: Name, Größe, Zeit(en)

Von den Dateiattributen werden hier nur die drei wichtigsten erläutert.

Wie jeder weiß, der an Rechnern ein bisschen gearbeitet hat, können Dateinamen frei gewählt werden und Dateien können beliebig umbenannt werden.

Beispiele:

Erzeugen der Datei Beispiel.avi, gefüllt mit Zufallsbytes (Datenmüll):

```
>  dd if=/dev/urandom of=Beispiel.avi bs=512 count=123
123+0 records in
123+0 records out
62976 bytes (63 kB) copied, 0.020581 s, 3.1 MB/s
```

Umbenennen nach bsp.mp3:

```
>  mv -v Beispiel.avi bsp.mp3
`Beispiel.avi' -> `bsp.mp3'
```

Ebenso ist es mit der Dateigröße: Dateien können beliebig verkleinert werden bis auf 0 und vergrößert werden können sie praktisch unbegrenzt; limitiert nur durch das verwendete Dateisystem oder Programm. Zudem ist die Dateigröße durch Sparse-Dateien nicht eindeutig; bei der Größenangabe ist daher wichtig immer genau anzugeben, wie denn die Größe bestimmt wurde.
Beispiele:

Erzeugen einer Datei der Länge Null:

```
 >  dd if=/dev/urandom of=Beispiel.avi bs=512 count=0
0+0 records in
0+0 records out
0 bytes (0 B) copied, 2.5e-05 s, 0 B/s
```

Erzeugen einer Datei, die zehn Millionen Bytes enthält und die auf der Festplatte nur 9728 Bytes belegt:

```
>  dd if=/dev/zero of=sparsefile bs=1 count=0 seek=10000000
0+0 records in
0+0 records out
0 bytes (0 B) copied, 2.7e-05 s, 0.0 kB/s
>  du -B1 --apparent-size sparsefile
10000000        sparsefile
>  du -B1 sparsefile
9728    sparsefile
```

Diese Zweideutigkeit der Größe zeigt sich nicht nur bei besonderen Dateien sondern kommt auch bei ein paar Prozent der MP3-Dateien und Video-Dateien vor, vorausgesetzt die Dateien wurden sparse erstellt oder sparse kopiert. Traditionellerweise ist mit der Größe die apparent-size gemeint.

Weiteres Beispiel: Verlängern auf doppelte Länge(n) durch Anhängen der zweiten Datei an die erste:

```
>  dd if=/dev/urandom of=Beispiel.avi bs=512 count=123
123+0 records in
123+0 records out
62976 bytes (63 kB) copied, 0.017741 s, 3.5 MB/s
>  dd if=/dev/urandom of=Beispiel1.avi bs=512 count=123
123+0 records in
123+0 records out
62976 bytes (63 kB) copied, 0.017741 s, 3.5 MB/s
>  cat Beispiel1.avi >> Beispiel.avi
>  du -B1 --apparent-size Beispiel.avi
125952  Beispiel.avi
```

Die Zeit(en) von Dateien können ebenso leicht modifiziert werden.

Beispiele:

Ändern der Modifikationszeit auf 2004-01-01 12:43, Ändern der (letzten) Zugriffszeit auf einen zufälligen Wert im Zeitraum 2005 bis 2007:

```
> touch -m -t 200401011243.57 bsp.mp3
> touch -t -a 200$((5+$(($RANDOM % 3))))0$(($RANDOM % 10))$(($RANDOM % 3))$((1+$(($RANDOM % 9))))$(($RANDOM % 2))$((1+$(($RANDOM % 9))))$(($RANDOM % 6))$(($RANDOM % 10)).$(($RANDOM % 6))$(($RANDOM % 10)) bsp.mp3
```

Danach sind die Zeiten vom letzten Zugriff, der letzten Modifikation und der Erzeugung:

```
>  ls -lt --time=access bsp.mp3
-rw------- 1 rf0 users 62976 2005-02-21 07:23 bsp.mp3
>  ls -lt bsp.mp3
-rw------- 1 rf0 users 62976 2004-01-01 12:43 bsp.mp3
>  ls -lt --time=ctime bsp.mp3
-rw------- 1 rf0 users 62976 2008-08-16 18:55 bsp.mp3
```

Wird von nur einer Zeit einer Datei gesprochen, ist traditionellerweise nur die Zeit der letzten Modifikation gemeint. Im Beispiel wurde die von 2008-08-16 18:55 auf 2005-02-21 07:23 geändert.

Tauschbörsenprogramm mit Konfigurationsdateien

Das Tauschbörsenprogramm hat mehrere Aufgaben: Die Verwaltung der Dateien und die Kommunikation mit der Tauschbörse, die aus vielen Teilnehmern und Servern besteht. Hierfür legt das Programm (mind.) eine Konfigurationsdatei an.
Das Programm erstellt dort u. A. eine Liste der Dateien, die es in der Tauschbörse anbietet und zwar mit Dateinamen, Dateigröße, File ID (Hash-Wert, Prüfsumme) und evtl. einigem weiteren wie Typ, wobei der Typ aber nur aufgrund vom Dateinamen geraten wird.

Wichtig ist hierbei, das das Einlesen der Dateiattribute, also Dateiname und Dateigröße, schnell geht während der Hash-Wert zeitaufwendig ist, weil hierfür jede Datei komplett eingelesen werden muss. Und dies dauert bei einer 2008 aktuellen und schnellen Festplatte, also bei 100 MByte/s lange: Vorausgesetzt das das Programm mit der vorhandenen CPU-Leistung diese Geschwindigkeit erreichen kann, hat man bei einem

mittelmäßig großen Share-Folder, der mit insgesamt 360 GByte gefüllt ist, einen Zeitaufwand von 360 GByte / 100 MByte/s = 3600 s = eine Stunde!
Folglich gibt es kein Tauschbörsenprogramm, das die Hash-Werte von schon einmal eingelesenen Dateien ein zweites mal berechnet, denn kein Tauschbörsen-Teilnehmer würde akzeptieren wenn das Tauschbörsenprogramm rund eine Stunde allein zum Starten benötigt und zudem durch ständige Festplatten- und CPU-Aktivität den Rechner langsam macht und zusätzlich Strom verbraucht.
Der Hash-Wert wird deshalb nur beim ersten Auftauchen der Datei berechnet, in einer Konfigurationsdatei gespeichert und nur der Hash-Wert aus der Konfigurationsdatei wird in der Tauschbörse angezeigt, selbst wenn die Datei ausgetauscht wurde und längst einen anderen Hash-Wert hat! Und den Hash-Wert in der Konfigurationsdatei kann man auch leicht durch einen beliebigen anderen ersetzen. Notfalls kann man dafür einen Hex-Editor nehmen.

Wichtig ist auch, das man zum Fälschen von Hash-Werten noch mehr Möglichkeiten hat als die Datei auszutauschen oder die Konfigurationsdatei(en) zu verändern: Viele Tauschbörsenprogramme sind Open-Source, so das man deren Quellcode sehr leicht modifizieren kann. Damit kann man alle von den Dateien in Tauschbörsen angezeigte Daten beliebig fälschen, inklusive Hash-Wert! Ausgenutzt wird dies beispielsweise zu gezielten Modifikationen für wissenschaftliche Studien über Tauschbörsen.
Daneben passieren Modifikationen von Dateien (im Share-Folder), Konfigurationsdateien, Programmen und anderen passieren nicht selten durch defekte Festplatten, Dateisystem-Defekte z. B. durch einen Stromausfall, defekte Datenkabel, defektes RAM und viele weitere Ursachen. Zudem ist für jede Rechner-Komponente, beispielsweise Festplatten, eine Fehlerrate für nicht-korrigierbare und nicht-detektierbare Fehler angegeben; Fehler treten deshalb gelegentlich auch bei völlig intakten Rechnern auf, die innerhalb der zulässigen Parameter betrieben werden.
Dies ist mit ein Grund dafür, das man einige Dateien in Tauschbörsen mit gleichem Namen und gleicher Größe aber unterschiedlichem Hash-Wert findet, obwohl der Inhalt, z. B. ein Film, bei allen diesen Dateien gleich aussieht.

Eine weitere Möglichkeit den Hash-Wert zu fälschen ist eine Datei mit dem passenden Hash-Wert zu erzeugen.
Hier ein Beispiel mit dem Programm CRC Faker (http://freshmeat.net/projects/crcfaker/):

> fakecrc 00c7c580 87359488 "Gina Wild - After Party.avi"

Dies erzeugt die Datei "Gina Wild - After Party.avi" mit dem CRC32-Hash-Wert 00c7c580 und der Größe 87359488 Byte.
Das Original, das man in diversen Tauschbörsen findet, enthält einen Porno-Film, während die Nachahmung nur Datenmüll enthält. Zudem liefert ein zweiter Lauf von CRC Faker einen anderen Dateiinhalt bei gleichem CRC32-Hash-Wert.

Ein ausführlicheres Beispiel, das unter Anderem auch andere Gina-Wild-Filme fakt, findet man unter: https://sslsites.de/www.true-random.com/homepage/projects/liberal/fake/noscript

Das Programm CRC Faker fakt nur die relativ kurze Prüfsumme CRC32, aber es gibt seit Jahren auch Open-Source-Programme für die kryptologischen Hash-Funktionen (http://de.wikipedia.org/wiki/Kryptologische_Hash-Funktion) MD5 und MD4:
http://it.slashdot.org/article.pl?sid=05/11/15/2037232
und auch SHA-0 und SHA-1 sind nicht sicher:
http://slashdot.org/article.pl?sid=04/08/17/0030243&tid=93,
http://www.schneier.com/blog/archives/2005/02/sha1_broken.html.

Gleiches gilt für HAVAL, MD2, PANAMA und RIPEMED, wie man z. B. auf Wikipedia nachlesen kann: Auch sie sind kryptologische Hash-Funktionen, aber haben keine so genannte starke Kollisionsresistenz; d. h. auch bei diesen Funktionen ist es leicht Dateien zu finden oder zu erzeugen, die bei verschiedenem Inhalt den gleichen Hash-Wert haben.

Wichtig erscheint mir, das die Aussage, das mit einem Hashwert eine zweifelsfreie Identifizierung möglich ist, definitiv falsch ist; eine fehlerhafte Identifizierung immer und auch mit den besten Hashfunktionen möglich! Das weiß, jeder Informatik-Student, aber Juristen und die meisten Internet-Nutzer wissen es wohl nicht.
Die zweite wichtige Aussage ist, das es sehr wohl möglich ist zu einer Datei eine andere mit gleicher Länge und gleichem Hash-Wert zu erzeugen, und zwar dann, wenn eine Hash-Funktion verwendet wird, die keine stark kollisionsresistente keine kryptologische Hash-Funktion ist.
Deshalb habe ich ja die Beispiele mit CRC Faker gemacht.

Betriebssystem

Beim Betriebssystem gibt es Probleme wie Trojaner und Rootkits, durch die der Rechner ferngesteuert werden kann und so unbemerkt vom Besitzer in Tauschbörsen sein kann. Der Empfänger/Ermittler sieht hiervon nichts, außer er selbst steuert den Rechner fern. Zudem ist aus der Ferne nicht erkennbar, welcher der Benutzer des Rechners denn das Tauschbörsen-Programm verwendet.

Internet

Die Daten werden auf einem Weg übertragen, von dem der Empfänger nur die scheinbare Ausgangsstelle sehen kann, weil schon das IP-Protokoll nicht zwischen End- und Zwischenstellen unterscheidet. Im oberen Bild ist daher der Sender nicht immer derjenige, der zur Verbindung gehörende IP-Nr. offiziell hat; es kann auch ein ganz anderer sein.
Dies zeigt sich schon bei DSL-Routern, die zum Internet hin eine IP-Nr. verwenden und hinter denen mehrere Leute mehrere PCs betreiben. Und es geht weiter über offene WLANs, Proxies, Onion-Router usw.. Woher und wohin genau die Daten gehen ist allein anhand der IP-Nr. schon prinzipiell nicht erkennbar.
Hinzu kommt, das es in manchen Tauschbörsen prinzipiell möglich ist mittels IP-Spoofing Dateien unter einer ganz anderen IP-Nr. anzubieten! Der Grund hierfür ist, dass in den IP-Paketen die Absender-IP-Nr. beliebig gesetzt werden kann und das IP-Protokoll keine Überprüfung der Absender-IP-Nr. enthält.
Beim einfachen IP-Spoofing kann zwar nichts downgeloadet werden, aber es kann zumindest dazu missbraucht werden unter einer anderen IP-Nr. Dateien in Tauchbörsen erscheinen zu lassen.
Eine weitere Möglichkeit eine andere IP-Nr. vorzutäuschen ist die andere IP-Nr. in HTTP-Header wie z. B. dem X-Forwarded-For-Header einzutragen. Über einen Proxy, den man auch sehr leicht selbst installieren kann, erfordert das nur einen Eintrag in der Konfigurations-Datei.

Wichtig bei der IP-Nr. ist auch, das die meisten Tauschbörsen-Teilnehmer eine dynamische IP-Nr. verwenden und es ist z. B. bei instabilen DSL-Anschlüssen nicht selten, das die IP-Nr. nach wenigen Sekunden, häufig nur zwei oder drei, wechselt. Daher ist es für einen Nachweis, von welcher IP-Nr. denn die Daten kamen, die IP-Nummern aller Datenpakete aufzuzeichnen; eine einzige IP-Nr. aus irgendeinem Paket reicht hierfür nicht aus, allein schon weil die Uhren der Provider und Ermittler nicht bis auf die Millisekunde genau sind und ein Datenpaket im Internet nicht selten ein paar Sekunden unterwegs ist.
Zur Aufzeichnung eignen sich Sniffer wie z. B. das kostenlose Wireshark, mit denen die Aufzeichnung und auch die Auswertung der Datenpakete sehr leicht ist.

Rechner vom Ermittler

Hier kann restlos alles gefälscht werden, inklusive angeblich downgeloadeter Dateien. Die ermittelten Daten sind daher bestenfalls nur so vertrauenswürdig wie der oder die Ermittler.
Im Gegensatz zu "handfesten" Beweisen wie einem mit Rauschgift gefüllten Paket mit Fingerabdrücken darauf gibt es zu Tauschbörsen bestenfalls ein paar Dateien, die man sehr leicht Kopieren oder Fälschen kann, beispielsweise mit einem so genannten Beweisscreenshot-Generator: http://www.heise.de/newsticker/Filesharing-Aktivisten-betreiben-Beweisscreenshot-Generator--/meldung/107736
Problematisch hierbei ist, das man an handfesten Beweisen genauere Untersuchungen vornehmen kann, beispielsweise eine Isotopen-Analyse zur Bestimmung der Herkunft, eine C14-Analyse zur Bestimmung des Alters und das man auch eine unabhängige zweite Untersuchung vornehmen lassen kann, aber bei downgelodeten Dateien, Logdateien und Screenshots gibt es diese Möglichkeiten nicht.

Stufen-Nr.	Vorliegende Daten (auf dem Ermittler-Rechner oder beim Gericht)	Beweiskraft
5	Ein glaubhaftes (nicht widerrufenes) Geständnis.	Offenkundiger Beweis
4	Eine zusätzliche Überprüfung, beispielsweise durch forensische Untersuchung verdächtiger PCs und Nachweis der Original-Dateien und Tauschbörsen-Software inklusive Logdateien auf den verdächtigen PCs sowie Ausschluss anderer scheinbaren Datenquellen wie Trojaner, Proxies, Port-Forwarding, offenes WLAN usw..	Durch die Indizienreihe (=Summe der Indizien) hat man hier die Beweiskraft eines Indizienbeweises. Für einen offenkundigen Beweis reicht es nicht, weil noch die Information fehlt, wer von den Leuten, die Zugang zu den betreffenden Rechnern hatten, die Tauschbörsen-Software verwendete.
3	Die Dateien konnten komplett downgeloadet werden und stimmen mit dem Original komplett (nicht nur bezüglich Hash-Werten) überein oder der Vergleich geschieht durch Vergleich von a) Dateilänge und b) eine kryptologische Hash-Funktion mit starker Kollisionsresistenz.	Beweiskraft eines Indizes, denn hier ist nachweisbar, das das Original über die betroffene IP-Adresse erhältlich ist. Als Beweis für die Teilnahme an einer Tauschbörse reicht dies nicht, aber es reicht möglicherweise als Beweis für eine Störung im Sinne der Störerhaftung.
2	Die angezeigten Dateien können teilweise downgeloadet werden; es wird wirklich etwas angeboten. Zudem verwendet der Sender nur eine IP-Nr. bei allen Datenpakten oder die IP-Nummern aller Datenpakete können ihm zugeordnet werden.	Beweiskraft einer Tatsachenbehauptung bezüglich der IP-Nr., denn alles von diesen Daten, bis auf die IP-Nr., kann sehr leicht gefälscht werden und die IP-Nr. zeigt nur wofür die Daten kamen, aber nicht woher. Die IP-Adresse ist aufgrund des IP-Protokolls relativ zuverlässig, weil allein durch IP-Spoofing nicht zu fälschen.
1	In einer Tauschbörse angezeigt werden Dateien mit Namen, Größe, Hash-Wert usw. sowie der IP-Nr. unter der sie angeboten werden.	Beweiskraft einer Meinungsäußerung, denn alles von diesen Daten kann, möglicherweise schon durch Dritte, sehr leicht gefälscht werden und nichts davon kann durch Urkunden, Zeugen oder

		Sachverständige bestätigt oder widerlegt werden. Damit sind die Kriterien für eine negative Feststellungsklage erfüllt und ohne weitere Nachforschungen sind die Daten daher wertlos.

Folgerungen für die Rechtspflege

Für die Rechtspflege zu Tauschbörsen benötigt man neben der Informationstheorie auch eine Interpretation der Daten aus Tauschbörsen.
Deshalb ist im Folgenden eine Checkliste zum Beweismaß in Tauschbörsen, die keine Anonymisierung verwenden, also (scheinbar) direkte Datenverbindungen verwenden und bei denen der Ermittler vollkommen vertrauenswürdig ist.
Hierbei bauen die Stufen jeweils aufeinander auf; d. h. zum Erreichen der Stufe n müssen vorher alle Stufen darunter (Stufe n-1, n-2, ...) erreicht werden.

Zu **1** ist anzumerken, das das Downloden der Dateien schon durch so etwas banales wie unzureichende Zugriffsrechte oder entsprechende Firewall-Einstellungen verhindert sein kann, so das effektiv gar nichts angeboten wird. Dies zeigt sich erst beim Versuch downzuloaden.
Allein ein paar in Tauschbörsen angezeigte Daten sagen deshalb nahezu nichts aus und können bestenfalls die Grundlage weiterer Ermittlungen sein.

Schlussbemerkungen

Was hier weitestgehend ausgeblendet ist, sind Fehler und Fälschungen von Ermittlern, Abmahnern und
Providern. Diese Übersicht ist also nur eine erste Näherung zuungunsten des Beschuldigten,
denn ungefähr ein Prozent der IP-Nummern wird von den Providern falsch
zugeordnet und bei Abmahnern gab es z. B. Zahlendreher in der betreffenden IP-Nr., die zur
Beschuldigung von völlig falschen Leuten führen, wie einige Nachrichten-Meldungen zeigen:
http://www.heise.de/newsticker/meldung/80111
http://www.gulli.com/news/isp-liefert-falsche-ip-50-tage-2007-11-08/
http://www.heise.de/newsticker/meldung/97304
http://www.heise.de/newsticker/IP-Verwechslung-fuehrt-zu-falschem-Kinderporno-Verdacht--/meldung/105094

Was ebenfalls ausgeblendet wurde ist, das Dateien immer eine Herkunft habe und es gibt viele Rechte-Inhaber, die Ihre Dateien in Tauschbörsen einstellen um damit zu werben oder um anschließend abmahnen zu können: http://www.heise.de/newsticker/Torrent-Sites-als-Marketing-Plattform-missbraucht--/meldung/113726
Ob eine urheberrechtlich geschützte Datei in einer Tauschbörse legal oder illegal eingestellt wurde, lässt sich daher nur mit der Klärung der Herkunft in der betreffenden Tauschbörse klären, aber das ist in den meisten Fällen wahrscheinlich nicht möglich.

Daneben gibt es auch einige Leute und sogar ganze Firmen, die nur dafür bezahlt werden gefälschte Dateien in Tauschbörsen einzustellen:
http://www.heise.de/tp/r4/artikel/12/12897/1.html

Die Praxis zeigt, das von Ermittlern in der Regel weder die IP-Adresse noch der tatsächliche Inhalt der angeblichen Daten überprüft wird:
http://www.heise.de/newsticker/Studie-Beweise-fuer-Copyright-Verletzungen-in-P2P-Netzen-oft-unzureichend--/meldung/109252

Deshalb sollte man auch auf Formalien achten wie beispielsweise ob bei der Zeitangabe angegeben ist, welche Zeit genau gemeint ist und ob binäre mit dezimalen Präfixen verwechselt wurden, also ob die Dateigrößen richtig angegeben sind. Ohne eine Angabe wie MESZ ist die Angabe von Datum und Zeit nicht eindeutig und nicht exakt gleich lange Dateien können nicht das Gleiche enthalten.

Bei Abmahnungen stellen sich noch weitere juristische Fragen, die mit aus Tauschbörsen gewonnen Daten nichts zu tun haben:
- Ist der Rechteinhaber überhaupt aktiv legitimiert; ist er der Urheber selbst oder hat er die Rechtekette der Nutzungsrechtseinräumung lückenlos aufgezeigt?
- Mit welcher Software hat der Rechteinhaber die Beweise gesichert. Hält die Software einer gerichtlichen Überprüfung überhaupt stand; liegen beispielsweise Log-Dateien zur Zeitsynchronisation mit einem NTP-Server oder einem DCF-77-Empfänger vor?

"Wichtig erscheint mir, das die Aussage, das mit einem Hashwert eine zweifelsfreie Identifizierung möglich ist, definitiv falsch ist; eine fehlerhafte Identifizierung immer und auch mit den besten Hashfunktionen möglich! Das weiß, jeder Informatik-Student, aber Juristen und die meisten Internet-Nutzer wissen es wohl nicht."

Dr. Rolf Freitag

Ein hundertprozentig sicherer Vergleich mit Hash-Funktionen ist nicht möglich, aber mit stark kollisionsresistenten kryptologischen Hash-Funktionen, beispielsweise SHA-512, hat man eine Sicherheit von über 99,999999 %; ein Irrtum ist da mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen, zumindest nach dem heutigen Stand der Technik und insbesondere Kryptografie. Entscheidend ist, welche Hash-Funktion verwendet wird: SHA-512 und andere stark kollisionsresistente kryptologische Hash-Funktionen sind so zuverlässig, das eine Kollision (gleicher Hash-Wert bei verschiedenen Dateien gleicher Länge) praktisch ausgeschlossen ist!
Bei gleichem SHA-512-Hash-Wert zwei (gleich lange) Dateien direkt zu vergleichen ist daher praktisch sinnlos; die Chance einen Unterschied zu finden ist kleiner als eins zu eine Milliarde.
Sie sollten daher nicht den Eindruck vermitteln, das Hash-Werte immer unsicher sind; so einfach ist es nicht! Andererseits weiß man aber das viele Hash-Funktionen unsicher sind, beispielsweise CRC8, CRC16, CRC32, MD23, MD4, MD5, HAVAL, PANAMA, RIPMED, SHA-0 und SHA-1. D. h. mit ein paar Sekunden bis Stunden Rechenaufwand, kann man eine gleich große Datei mit gleichem Hash-Wert und anderem Inhalt erstellen, von dem zumindest ein Teil, üblicherweise der Anfang, frei wählbar ist. Generell sind Hash-Werte, die nicht länger als 160 Bit sind, unsicher und diese Länge wird in Zukunft noch zunehmen, so dass auch 256 Bit lange Hash-Werte in wohl wenigen Jahren unsicher werden.

Der Verein gegen den Abmahnwahn e.V. bedankt sich recht herzlich bei Herrn Dr. Rolf Freitag
für diese interessanten Ausführungen zum Thema:
Hash-Funktion.