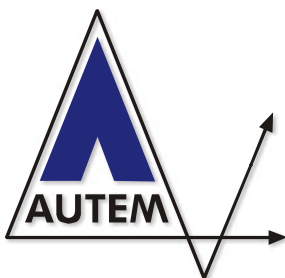


PERKEO[®]++

Benutzerhandbuch

*Der Datenscanner
zum Aufspüren von
Kinderpornographie*



Benutzerhandbuch - PERKEO® ++

© Copyright 1995 - 2009 AUTEM GmbH. Alle Rechte vorbehalten. Kein Teil dieses Handbuchs darf - auch nicht auszugsweise - reproduziert, fotokopiert oder elektronisch gespeichert werden ohne ausdrückliche schriftliche Genehmigung von AUTEM.

Die in diesem Buch beschriebene Software unterliegt einem Software-Lizenzvertrag und darf nur gemäß den Bestimmungen dieses Vertrages genutzt werden.

AUTEM GmbH
Dithmarscher Straße 29
D-26723 Emden
Deutschland

Telefon +49 (0) 49 21-96100
Telefax +49 (0) 49 21-961096
E-Mail perkeo@perkeo.com
Web www.perkeo.com

AUTEM gibt keine Garantie für dieses Handbuch sowie keine ausdrücklichen oder stillschweigenden Garantien auf handelsübliche Qualität und Eignung für einen bestimmten Einsatzzweck. AUTEM übernimmt keine Haftung für darin enthaltene Fehler oder auftretende Folgeschäden, die durch Ausstattung, Leistung und den Gebrauch dieses Materials entstehen.

Die in diesem Buch erwähnten Soft- und Hardwarebezeichnungen sind in den meisten Fällen auch eingetragene Warenzeichen und unterliegen als solche den gesetzlichen Bestimmungen. PERKEO ist eingetragenes Warenzeichen der AUTEM GmbH, Deutschland.

Für Hinweise, Anregungen und Verbesserungsvorschläge sind wir stets dankbar. Bitte richten Sie diese schriftlich an AUTEM.

1. Auflage 2009

Inhaltsverzeichnis

1	EINFÜHRUNG	1
1.1	Übersicht	1
1.2	Wer setzt PERKEO ein?	1
1.3	Leistungsmerkmale	2
1.4	Wie funktioniert PERKEO?	2
1.5	Technischer Support	3
2	INSTALLATION	4
2.1	Betriebssysteme	4
2.2	Installation	4
2.3	Update der PERKEO-Suchlibrary (perkeo.lib)	4
3	PERKEO IM EINSATZ	5
3.1	PERKEO Parameter	5
3.2	Konfigurationsdatei (perkeo.cfg)	12
3.3	Scannen von DNEWS	13
3.4	Mehrteilige Dateien in Mail oder News Archiven	14
3.5	Anwendungsbeispiele	14
4	ANHANG	16
4.1	Häufig gestellte Fragen (FAQ)	16
4.2	Fehlermeldungen	17
4.3	Definition Kinderpornographie	18
4.4	Was tun bei Treffern ?	19

1 Einführung

PERKEO++ ist ein sehr schneller und leistungsfähiger Datenscanner, der Sie beim Auffinden von illegaler Kinderpornographie bzw. Tierpornographie unterstützt. PERKEO++ versetzt Sie in die Lage, Datenbestände in Ihrem Unternehmen gezielt nach derartigen Objekten zu durchsuchen und damit größeren Schaden abzuwenden.

Der Besitz und die Verbreitung von kinderpornographischen Darstellungen ist in Deutschland (§184 StGB) und in den meisten anderen Ländern der Welt strafbar.

Das folgende Handbuch gibt Ihnen alle Informationen zum Einsatz von PERKEO++.

1.1 Übersicht

PERKEO++ ist der Datenscanner zum Aufspüren von Kinderpornographie und Tierpornographie in Datenbeständen jeglicher Art.

Dabei ist es vollkommen gleichgültig, ob es sich bei den zu durchsuchenden Datenträgern um lokale Laufwerke, Netzwerklaufwerke, Proxy-Server, News-Server oder Webspaces handelt. PERKEO++ findet illegale Pornographie schnell und zuverlässig.

PERKEO++ wurde in Zusammenarbeit mit dem deutschen Bundeskriminalamt (BKA) entwickelt. Auf Basis digitaler Fingerabdrücke werden kinder- oder tierpornographische Dateien sicher erkannt.

PERKEO++ wird von deutschen und internationalen Polizeibehörden seit 1998 erfolgreich eingesetzt. Das Programm wurde konzipiert für Geschwindigkeit, Zuverlässigkeit und Treffsicherheit.

Die Suchlibrary für PERKEO++ wird ständig in Zusammenarbeit mit dem Deutschen Bundeskriminalamt (BKA) aktualisiert, so dass PERKEO++ immer auf dem aktuellen Stand ist.

1.2 Wer setzt PERKEO ein?

- Internet-Provider (ISP)
- Unternehmen
- Behörden
- Schulen / Hochschulen / Universitäten
- EDV-Sachverständige
- Strafverfolgungsbehörden

1.3 Leistungsmerkmale

- Extrem hohe Performance. Suchgeschwindigkeiten von mehr als 100 MB/s
- Anwendung auf beliebige Datenträger
- Suche in komprimierten Archiven (ZIP, ARJ)
- Suche in News, Webspaces, E-Mail, Proxy-Cache
- Treffergenauigkeit 100%
- Minimaler Administrationsaufwand
- Einbindung als Modul
- Flexible Steuerung durch Skripte und Batchjobs möglich
- Auf Wunsch automatische Meldung an Strafverfolgungsbehörde möglich

1.4 Wie funktioniert PERKEO?

PERKEO++ arbeitet prinzipiell wie ein Virens Scanner, d. h. PERKEO++ untersucht Datei für Datei, ob es sich bei ihr um ein bereits bekanntes Datenobjekt handelt. Um derartige Dateien eindeutig zu identifizieren, wird das Prinzip des digitalen Fingerabdrucks verwendet. Der Fingerabdruck einer jeden Datei wird mit den Fingerabdrücken in der PERKEO++ Suchlibrary verglichen.

Das für die Suche verwendete zertifizierte Verfahren hat eine Fehlerwahrscheinlichkeit von weniger als $1 : 10^{34}$ und ist damit praktisch zu 100% sicher. Fehlalarme sind daher so gut wie ausgeschlossen.

Während eines Suchlaufs erstellt PERKEO++ eine Protokolldatei `report.txt`, in der das Suchergebnis dokumentiert wird. Existiert diese Datei bereits, so wird die neue Protokolldatei an die Bestehende angehängt. In der Protokolldatei wird das Suchergebnis mit Zeit- und Pfadangaben sowie weiteren Informationen festgehalten.

Für jeden Treffer kann eine beliebige Aktion automatisch ausgeführt werden. Sie können beispielsweise eine E-Mail zur Benachrichtigung versenden, das strafbare Datenobjekt sofort löschen oder es in eine „Quarantänezone“ verschieben.



HINWEIS

Bedenken Sie immer: Schon *ein* Treffer reicht, um verdächtigen Aktivitäten aufzuspüren!

1.5 Technischer Support

Wenn Sie Schwierigkeiten bei der Verwendung von PERKEO++ haben, dann lesen Sie zunächst sorgfältig im Handbuch nach. Schauen Sie außerdem in die Hilfeseiten von PERKEO++. Einen Überblick über die Hilfeseiten bekommen Sie mit PERKEO -h.

Wenn Sie das Problem nicht lösen können, senden Sie eine E-Mail mit einer genauen Fehlerbeschreibung sowie detaillierten Informationen zur Systemumgebung an **perkeo@perkeo.com**.



HINWEIS

Trotz größter Sorgfalt bei der Entwicklung ist niemals gänzlich auszuschließen, dass eine Software wie PERKEO++ den auszuwertenden Datenträger bei der Analyse verändern könnte.

Aus Sicherheitsgründen raten wir daher an, Auswertungen mittels PERKEO++ nur auf Kopien des Originaldatenträgers durchzuführen.

2 Installation

2.1 Betriebssysteme

PERKEO++ ist lieferbar für folgende Betriebssysteme:

Windows 9x/NT/2000/XP/Vista 32/64Bit, Linux (i386), FreeBSD (i386), Mac OS X (PPC), AIX (PowerPC), Sun Solaris (Sparc).

2.2 Installation

PERKEO++ ist klein und leistungsfähig. Es besteht im wesentlichen aus zwei Dateien: PERKEO bzw. PERKEO.EXE ist das ausführbare Programm. PERKEO.LIB ist die zugehörige Suchlibrary.

Kopieren Sie die die Dateien vom PERKEO++ Datenträger in ein beliebiges Unterverzeichnis auf Ihrer Festplatte.

Für das Durchsuchen von Archiven benötigt PERKEO++ ein Unterverzeichnis für temporäre Dateien. Dies wird normalerweise vom Betriebssystem automatisch angelegt und verwaltet (Umgebungsvariable TEMP oder TMP).

2.3 Update der PERKEO-Suchlibrary (perkeo.lib)

AUTEM stellt im Rahmen der Servicevereinbarung Updates der Suchlibrary perkeo.lib bereit. Registrierte Benutzer erhalten aktualisierte Libraries automatisch per E-Mail.

Achten Sie darauf, die Update-Service Subscription rechtzeitig zu verlängern, damit Ihr System immer ausreichend geschützt ist.

3 PERKEO im Einsatz

Die Bedienung von PERKEO++ ist sehr einfach. Häufig wiederkehrende komplexere Aufrufe können Sie mittels Script (Batchdatei) automatisieren.

3.1 PERKEO Parameter

In der folgenden Auflistung finden Sie die Eingabeparameter von PERKEO++. Parameter werden einfach hinter `perkeo` angegeben. Vor jedem Parameter muss ein "-" gesetzt werden.

Beispiel

```
perkeo c:\ -archives
```

Bei der Angabe von Parametern wird zwischen Groß- und Kleinschreibung nicht unterschieden.

```
-archives  
-arc
```

Aktiviert die Durchsuchung von ARJ- und ZIP-Archiven.



HINWEIS

Eine Kombination von `-archives` und `-exec` (s. u.) ist möglich. In diesem Fall kopiert PERKEO++ jede in einem Archiv gefundene Datei in ein temporäres Verzeichnis. Danach wird der angegebene Befehl mit dieser Datei ausgeführt. Als Pfad zum Auspacken muss die Umgebungsvariable `TEMP` oder `TMP` gesetzt sein (siehe 2.2).

```
-dnp path
```

Parameter zur Überprüfung von DNEWS-Artikeln auf einem lokalen Laufwerk oder einem News-Server. Nach dem Parameter `-dnp` muss eine Laufwerks-/Pfadangabe folgen (siehe auch `-np`).

Beispiel

```
perkeo -dnp /var/dnews/spool
```

```
-dnews:include_del
```

Sorgt dafür, dass als gelöscht markierte DNEWS-Artikel (db_*.del) trotzdem durchsucht werden.

```
-dx:
```

Bei DOS/Windows Systemen können sämtliche Laufwerke durch den Parameter ?:\ angegeben werden (z.B. „perkeo ?:\“). Durch den Parameter „-dx:“ können ein oder mehrere Laufwerke hiervon ausgeschlossen werden. Soll beispielsweise eine Liste dynamisch angebundener Netzwerklaufwerke durchsucht werden sollen, jedoch ohne die Bootpartition jedes Mal zu durchsuchen so wäre dies üblicherweise durch den Befehl „perkeo -dx:c ?:\“ erreicht.

Die dem Parameter folgenden Laufwerksbuchstaben werden direkt hintereinander angegeben. Um beispielsweise die Laufwerke C:, E: sowie H: auszuschließen wäre der Aufruf „perkeo -dx:ceh ?:\“

Beispiel

```
perkeo -dx:c ?:\
perkeo -dx:ce ?:\
```

```
-exclude path
-x path
```

Gibt Pfade an, die nicht durchsucht werden sollen. Als Sonderzeichen kann an erster Stelle ein „*“ angegeben werden, um alle Pfade auszuschließen, die mit dem angegebenen Text enden. Die ignorierten Pfade werden in der Protokolldatei (report.txt) und auf dem Bildschirm ausgegeben. Pfade dürfen keine Laufwerksbezeichnungen enthalten, also \windows ist korrekt, c:\windows hingegen falsch.

Beispiel

```
perkeo -x \windows
perkeo -x \perkeo\hits
perkeo -x \*hits
```

```
-execute command
-exec command
```

Führt für jede gefundene Datei den Befehl `command` aus. Bei der angegebenen Kommandozeile werden bestimmte Variablen von PERKEO++ ersetzt. Die Schreibweise der Variablen ist `${varname}` ähnlich der UNIX Korn-Shell (ksh). Alle folgenden Argumente werden als Teil der Kommandozeile interpretiert, wobei ein einzelner „\“ das Ende des Parameters kennzeichnet.



HINWEIS

Wenn Sie die gefundenen Dateien in ein anderes Verzeichnis verschieben oder kopieren und dieses Verzeichnis sich in dem durchsuchten Verzeichnisbaum befindet, dann sollten Sie sicherheitshalber dieses Verzeichnis von der Suche ausschließen (siehe Parameter `-x`).



HINWEIS

Windows: Shell eigene Befehle, wie z. B. `move`, werden nach `-exec` nur korrekt interpretiert, wenn Sie vorher den Kommandozeileninterpreter (`cmd /c`) explizit aufrufen:

falsch: `-exec move ${containername} ...`

richtig: `-exec cmd /c move ${containername} ...`



HINWEIS

Unix: Achten Sie darauf, dass einige Shells versuchen, Parameter der Schreibweise `${containername}` selber aufzulösen. In einem solchen Fall kommt bei PERKEO nur ein leerer Parameter an. Um die Expansion der Shell zu verhindern, sollten Sie üblicherweise die Parameter für `-exec` mit Anführungsstrichen „casten“.

falsch: `-exec rm ${containername}`

richtig: `-sshell -exec rm ` ${containername} ``



HINWEIS

Unix: Achten Sie darauf, dass einige Parameter einen fast beliebigen Inhalt haben können. Benutzen Sie z.B. `${containername}`, so kann es auftreten, dass die gefundene Datei einen Namen besitzt, der von der Shell bei der weiteren Verarbeitung expandiert wird. Ein Beispiel wäre eine Datei mit dem Namen „ `${test}` “. Variablen, die diese Inhalte liefern können, sind z.B. `containername` oder `originalname`. Nutzen Sie den Parameter „`-sshell`“, um die Dateinamen sicher zu übergeben.

falsch: `-exec rm ` ${containername} ``

richtig: `-sshell -exec rm ` ${containername} ``

Gültige Variablen:

`Containername`

Name der Datei, die strafrechtlich relevante Daten enthält. Bei einem gepackten Archive (.ZIP oder .ARJ) ist dies der Name des gepackten Archives.

`Datalength`

Länge der von PERKEO++ identifizierten Datei.

Dataname

Name einer von PERKEO++ erzeugten und zur Weiterverarbeitung erstellten temporären Datei. Der Dateiname der temporären Datei wird von PERKEO++ frei gewählt und stimmt nicht unbedingt mit dem Dateinamen der gefundenen Datei überein.

Datatype

Liefert den Datentyp des Treffers. Falls der Datentyp nicht erkannt werden kann, wird „bin“ zurückgeliefert. Ein gefundenes GIF-Bild würde beispielsweise als Datatype den Text „gif“ liefern.

Date

Aktuelles Datum im Format mm.dd.yyyy

Hitnum

1-basierte¹ Nummer des aktuellen Treffers während dieses Suchlaufes. Beachten Sie bitte, dass bei Treffern die aus mehreren Teildateien bestehen (mehrteiligen Treffern), über Hitnum für alle Teile die gleiche Nummer geliefert wird. Bei mehrteiligen Treffern sollte daher nicht Hitnum sondern Hitstring verwandt werden.

Hitstring

Bei einteiligen Treffern erzeugt Hitstring ebenso wie Hitnum eine 1-basierte Nummer des aktuellen Treffers. Im Fall eines mehrteiligen Treffers liefert Hitstring zusätzlich eine angehängte, durch Unterstrich getrennte 1-basierte Nummerierung für jeden einzelnen Teil des Treffers (z.B. „1_1“ und „1_2“ für die beiden Teile des ersten mehrteiligen Treffers).

Mailfilename

Name der exportierten temporären Datei, welche die Nachricht mit dem Treffer enthält. Diese Variable ist nur beim Scannen von DNEWS-Verzeichnissen gültig.

Message-ID

Die zum gefundenen Mail- oder Newsartikel gehörige Message ID. Wenn keine Message ID identifiziert wurde, so ist der Parameter „<>“.

Originalname

Der Originalname der gefundenen Datei. Achtung, dieser kann Sonderzeichen enthalten die nicht in einem Dateinamen enthalten sein dürfen.

Partnum

Liefert die 1-basierte Nummer eines mehrteiligen Treffers. Bei einem einteiligen Treffer wird die Zahl „0“ geliefert. Partnum eignet sich daher zur einfachen Erkennung ob ein mehrteiliger Treffer vorliegt. Zur Erzeugung von Dateinamen, sollte anstatt einer Kombination von Hitnum und Partnum, allerdings die Variable Hitstring vorgezogen werden.

Signature

Die Signatur ist die Kategorie der gefundenen Datei. Über diese Variable kann daher unterschieden werden welche Art von Datei gefunden wurde.

Time

Die aktuelle Uhrzeit im Format hh:mm:ss. Beachten Sie bitte, dass hier unter Windows die Uhrzeit aufgrund der „:“ nicht einfach als Dateiname genommen werden kann!

¹ „1-basiert“ bezeichnet eine Nummerierung beginnend mit der Zahl 1.

Beispiel

```
perkeo c:\ -arc -sshell -exec echo `${containername}`
```

In der ZIP Datei hallo.zip im Pfad c:\data befindet sich ein relevantes Bild mit dem Namen test1.gif. Der containername ist c:\data\hallo.zip. Der dataname gibt den Namen der temporär ausgepackten Datei wieder, z. B.: c:\temp_18.aaa. Der origname der Datei ist in diesem Fall test1.gif.

Beispiel

```
perkeo -np d:\news -sshell -exec echo `${containername}` found
```

Die Datei 290590 im Verzeichnis d:\news\de\test ist eine MIME kodierte Nachricht. Als Anhang befindet sich ein Bild test1.gif an der Nachricht. In diesem Fall beinhaltet die Variable containername den Pfad: d:\news\de\test\290590. Die Variable dataname beinhaltet den Pfad der temporär ausgepackten Datei z. B.: c:\tmp_18.aaa und die Variable origname beinhaltet test1.gif.

```
-ignoresignature sig
-ignsig sig
```

Ignoriert bei der Suche die angegebene PERKEO++ Signatur (Kategorie) sig.

Beispiel

```
perkeo c:\ -ignsig ANIMALP
```

Bei der Überprüfung von Laufwerk c:\ werden tierpornographische Datenobjekte ignoriert.

```
-newspath path
-np path
```

Parameter zur Überprüfung von News/Mails auf einem lokalen Laufwerk oder einem News-Server. Nach dem Parameter -np muss eine Laufwerks-/Pfadangabe folgen.

Beispiel

```
perkeo -np f:\usr\spool\news
```

**HINWEIS**

Da bei der Durchsuchung von Newsdateien die gesamte Datei jeweils dekodiert und durchsucht werden muss, ist die Überprüfung hierbei langsamer als bei normalen Dateien.

**HINWEIS**

Bei erneuter Prüfung der News-Dateien werden nur noch die zuvor noch nicht geprüften Dateien überprüft, was erheblichen Geschwindigkeitsvorteil bringt.

```
path [path....]
```

Es können beliebig viele Suchpfade angegeben werden.

Beispiel

```
perkeo c:\
perkeo c:\windows d:\tools
perkeo \windows\grafiken
```

Als Sonderzeichen kann hier "?" an Stelle eines Laufwerkes gesetzt werden, um alle Laufwerke zu wählen. Diskettenlaufwerke werden dabei jedoch nicht berücksichtigt.

```
-rename <report-filename>
```

Angabe des alternativen Pfades (Name) für die Reportdatei (default: report.txt).

```
-scanmultipart
```

Dieser Parameter wirkt sich nur auf das Scannen von News bzw. Mail aus. Hierdurch werden sämtliche in Artikeln vorkommende Einzelteile von Dateien indexiert. Sobald alle Teile einer mehrteiligen Datei vollständig sind, wird die Datei dekodiert und überprüft.

```
-sshell
```

Schaltet „safe shell casting“ für Variablennamen bei der Nutzung des `-exec` Parameters ein. Unter **Unix** ist das casting kompatibel zu gängigen Shells wie der „bash“ und „csh“.

```
-squid path
```

Parameter zur Überprüfung eines SQUID Proxy Caches. Nach dem Parameter `-squid` muss die Laufwerks-/Pfadangabe folgen. Es wird das Format von Squid 2.x unterstützt.

Beispiel

```
perkeo -squid /var/squid
```

```
-test
```

Sucht für Testzwecke zusätzlich nach einigen bekannten Medienobjekten. Die Testdateien können u. a. unter <http://www.perkeo.com/test/> heruntergeladen werden.

Beispiel

```
perkeo -test /home
```

-tstamp

Beschleunigt die wiederholte Suche mit PERKEO++ durch Nutzung der Zeitstempel von Dateien. Dieser Parameter sollte nur verwendet werden sofern sichergestellt ist, dass weder die Zeitstempel eines Dateisystems noch die Uhrzeit des Rechners manipuliert werden können.

Beispiel

```
perkeo -tstamp /home
```

-waitfortimeframe

In der Konfigurationsdatei können über den Parameter "dontrun" Zeitfenster definiert werden in denen PERKEO++ nicht ablaufen darf. Wird PERKEO++ innerhalb eines solchen Zeitfensters gestartet, terminiert es sofort. Mit dem Parameter "-waitfortimeframe" würde PERKEO++ sich nicht sofort beenden, sondern auf das nächste Zeitfenster warten in dem es laufen darf. Dabei wird der Prozeß in einen Zustand versetzt, der so gut wie keine CPU Zeit verbraucht.

Es kann also z. B. auf einem Server eine einfache Scriptdatei PERKEO++ immer wieder mit dem Parameter "-waitfortimeframe" starten. PERKEO++ wird - falls nötig - im Hintergrund warten, bis ein erlaubtes Zeitfenster erreicht wird und dann den nächsten Suchvorgang vornehmen. Sinnvollerweise sollte man dennoch in einer solchen Scriptdatei eine kurze Pause zwischen mehreren Aufrufen von PERKEO++ einbauen.

Beispiel

```
perkeo -waitfortimeframe -dnp /var/dnews/spool
```

3.2 Konfigurationsdatei (perkeo.cfg)

Beim Start versucht PERKEO++ die Datei `perkeo.cfg` zu lesen. Dabei wird wie folgt vorgegangen:

Windows:

- PERKEO versucht, die Datei `perkeo.cfg` im Startverzeichnis zu lesen.

Unix:

- PERKEO versucht, die Datei `perkeo.cfg` anhand der Umgebungsvariable `HOME` zuerst im Heimverzeichnis des Benutzers zu lesen. Sollte dort die Datei nicht existieren, wird im Startverzeichnis nach der Datei `perkeo.cfg` gesucht. Wurde in einem der Verzeichnisse `perkeo.cfg` gefunden, so wird die UID/GID der Datei mit derjenigen des aufrufenden Benutzers verglichen. Sind UID und/oder GID unterschiedlich, so wird PERKEO++ mit einer Fehlermeldung beendet.



HINWEIS

Achten Sie unter Unix immer auf die Lese- und Schreibrechte Ihres Benutzerzeichnisses sowie der Verzeichnisse, in denen PERKEO++ installiert und aufgerufen wird.

Die Konfigurationsdatei wird vor der Auswertung von Kommandozeilen-Parametern gelesen. Widersprechen die Kommandozeilen-Parameter den Angaben in der Konfigurationsdatei, so werden die Angaben der Kommandozeile benutzt.

Die Konfigurationsdatei ist unterteilt in Sektionen, in denen sich wiederum verschiedene Parameter befinden. Zeilen mit führendem `#` werden ignoriert (Kommentare).

Sektion „[general]“ – generelle Einstellungen.

```
dontrun time
```

Hiermit können Zeitenfenster festgelegt werden, in denen PERKEO++ nicht aktiv sein darf. Bei Newsservern lässt sich damit beispielsweise verhindern, dass PERKEO++ während des täglichen Purgings der Spool läuft. Bei Proxies kann damit ein Lauf während besonderer Lastzeiten verhindert werden. Wird ein Zeitenfenster angegeben, so prüft PERKEO++ beim Start und bei jedem Verzeichnis- oder Dateiwchsel, ob die lokale Zeit in eines der Zeitenfenster fällt. Ist dies der Fall, so wird der Suchlauf sofort beendet.

`time` ist eine Angabe im 24-Stunden Format „hh:mm-hh:mm“ (hh: Stunde, mm: Minute). Es kann nur ein Zeitenfenster pro Parameter angegeben werden, jedoch können beliebig Zeitenfenster in aufeinanderfolgenden Zeilen angegeben werden. Siehe auch Parameter „-waitfortimeframe“.

Beispiel

```
dontrun 03:00-05:30
```

Hiermit wird ein Lauf von PERKEO++ zwischen 3.⁰⁰ - 5.³⁰ Uhr morgens verhindert.

Beispiel für perkeo.cfg

```
[general]
# Mittagspause ;-)
dontrun 12:30-13:30
# Newspurge
dontrun 03:00-05:30
```

3.3 Scannen von DNEWS

DNEWS ist ein kommerzielles News-Server System der Firma NetWin Ltd. (siehe <http://netwinsite.com>). PERKEO++ unterstützt das Scannen von DNEWS 4.x Dateien und wurde erfolgreich getestet mit DNEWS 4.6 und DNEWS 4.7.

PERKEO++ durchsucht die `db_*.itm` Dateien im DNEWS Spoolverzeichnis und beachtet dabei die `db_*.del` Dateien, damit gelöschte Artikel nicht gescannt werden.

Wenn `/var/dnews/spool` das Spoolverzeichnis Ihrer DNEWS-Installation ist, dann wäre der Befehl zum Durchsuchen der Dateien:

```
perkeo -dnp /var/dnews/spool
```

Bei einem Treffer kann automatisch eine weitere Aktion mit dem Parameter `-exec` veranlasst werden.

DNEWS speichert viele News-Artikel in einer einzelnen .ITM-Datei. Somit würde das Löschen der ganzen Datei viele andere Artikel ebenfalls löschen. Deshalb erlaubt PERKEO++ beim Scannen von DNEWS die Verwendung der Variablen `${mailfilename}` innerhalb des `-exec` Befehls. Dies ist eine temporäre Datei, die den gefundenen Artikel enthält.

Um den Artikel zu eliminieren, brauchen Sie nur den Artikel innerhalb der DNEWS zu suchen und einen Cancel-Befehl - wie er oft auch gegen Spam zum Einsatz kommt - auszuführen (z.B. „`tellnews killitem \"${message-id}\"`“).

Hier ein Beispiel, um alle trefferbehafteten DNEWS-Newsartikel in das Verzeichnis `hits` unter dem Homeverzeichnis des Anwenders zu kopieren:

```
perkeo -dnp /var/dnews/spool -sshell -exec `cp ${mailfilename} ~/hits`
```

PERKEO++ beachtet normalerweise, dass die in `db_*.del` als gelöscht markierten DNEWS-Artikel nicht durchsucht werden. Der Parameter `-dnews:include_del` sorgt dafür, dass gelöschte Artikel trotzdem durchsucht werden. Wenn die schon gelöscht markierten Artikel noch einmal durchsucht werden, kann es dabei zum erneuten aufspüren schon gelöschter Artikel kommen.

3.4 Mehrteilige Dateien in Mail oder News Archiven

Durch den Parameter „-scanmultipart“ kann bei der Durchsuchung von Mail und Newsarchiven die Überprüfung von Dateien eingeschaltet werden, die über mehrere Artikel verteilt sind. PERKEO++ kann dabei Dateien zusammensetzen die über mehrere Tage/Suchläufe, über mehrere Newsgruppen verteilt sowie in beliebiger Reihenfolge gepostet wurden. Dazu wird im Startverzeichnis eine Indexdatei angelegt die je nach Umfang und Art der mehrteiligen Dateien zusätzlichen Speicherplatz benötigt. Der Platzbedarf kann dabei auch nach mehreren Wochen sich im Rahmen von 1-2 Megabyte bewegen, kann andererseits aber auch bei sehr grossen Archiven die sämtliche Binären Gruppen führen um den Faktor 10 oder 20 steigen.

Mehrteilige Treffer erfordern unter Umständen leicht veränderte Verarbeitung in Scripten. Wurde bisher die Variable „hitnum“ verwandt um Dateien zu speichern, so sollte jetzt der Parameter „hitstring“ zur Namensbildung verwandt werden. Weitere nützliche Variablen zur Behandlung von mehrteiligen Treffern sind „partnum“ oder „datatype“.

Ein mehrteiliger Treffer erzeugt einen einzelnen Eintrag in der Report Datei, jedoch mehrere Aufrufe für die -exec Funktion. Die Variable „containername“ kann bei DNEWS dementsprechend auf mehrere unterschiedliche ITM Dateien verweisen.

3.5 Anwendungsbeispiele

Die folgenden Beispiele verdeutlichen die Benutzung von PERKEO++:

Beispiel (Windows): Durchsuchen von Laufwerk c:

```
perkeo c:\
```

Beispiel (Windows): Durchsuchen aller Laufwerke

```
perkeo ?:\
```

Beispiel (Windows): Durchsuchen aller Laufwerke mit Scannen von ARJ- und ZIP-Archiven

```
perkeo ?:\ -arc
```

Beispiel (Windows): Durchsuchen von Laufwerk c:, d: und z:. Das Verzeichnis \system wird von der Durchsuchung ausgeschlossen

```
perkeo c:\ d:\ z:\ -x \system
```

Beispiel (Windows): Durchsuchen Laufwerk c: mit zusätzlicher Suche nach PERKEO-Testbildern

```
perkeo -test c:\
```

Beispiel (UNIX): Durchsuchen des Heimverzeichnisses aller User

```
perkeo /home
```

Beispiel (Windows): Verschieben strafbarer Dateien in Zielverzeichnis

```
perkeo c:\ -sshell -x \hit -exec cmd /c move ${containername} c:\hit
```

Beispiel (Unix): Kopieren strafbarer Dateien in Zielverzeichnis

```
perkeo /home -sshell -x \hit -exec cp `>${containername}` /hit
```

**HINWEIS**

Das Verzeichnis \hit wird mittels -x \hit von der Suche ausgeschlossen. So wird sichergestellt, dass bereits gefundene Dateien nicht ein zweites Mal von PERKEO++ aufgespürt werden.

Beispiel (Windows): Löschen strafbarer Dateien

```
perkeo c:\ -sshell -exec del ${containername}
```

Beispiel (Unix): Löschen strafbarer Dateien

```
perkeo / -sshell -exec rm -f `>${containername}`
```

Beispiel (Unix): Scannen von News

```
perkeo -sshell -dnp /var/dnews/spool -exec `cp ${mailfilename} ~/hits`
```

Kopiert alle trefferbehafteten DNEWS-Newsartikel in das Verzeichnis hits unter dem Homeverzeichnis des Anwenders.

Beispiel (Unix): Squid-Proxy scannen

```
perkeo -sshell -squid /var/squid -exec rm -f `>${containername}`
```

Durchsucht einen Squid-Proxy Cache und löscht strafbare Dateien.

4 Anhang

4.1 Häufig gestellte Fragen (FAQ)

In diesem Abschnitt werden die am häufigsten gestellten Fragen zu PERKEO++ beantwortet. Wenn bei der Verwendung von PERKEO++ ein Problem auftritt, sollten Sie zunächst hier nachsehen.

Kann PERKEO direkt von einer Diskette gestartet werden?

Aufgrund der Größe der Suchlibrary ist es nicht möglich, PERKEO++ direkt von der Diskette zu starten.

Können Pfade von der Durchsuchung ausgeschlossen werden?

Durch den Parameter `-exclude` oder `-x` können Pfade von der Durchsuchung ausgeschlossen werden. Pfadangaben beziehen sich grundsätzlich auf alle angegebenen Ziellaufwerke und dürfen daher keine Laufwerkskennung enthalten (falsch: `c:\windows` - korrekt: `\windows`).

Welche bekannten Archive werden gescannt?

In der Programmversion 1.x werden ARJ- und ZIP-Archive bearbeitet.

Dateien werden doppelt gefunden.

Wenn Sie mittels `-exec` gefundene Dateien an einen anderen Ort kopieren oder verschieben, wird PERKEO++ diese evtl. nochmals finden. Das Zielverzeichnis für gefundene Objekte sollte immer durch `-x` von der Suche ausgeschlossen werden.

Können Suchlibraries/Kategorien von der Suche ausgeschlossen werden?

Durch die Verwendung des Parameters `-ignsig` können einzelne Kategorien von der Suche ausgeschlossen werden. Ganze Suchlibraries werden ignoriert, wenn Sie diese aus dem PERKEO-Verzeichnis entfernen. Besser jedoch ist es, alle in dieser Suchlibrary vorhandenen Signaturen, durch die mehrfache Verwendung des Parameters `-ignsig`, einzeln auszuschließen.

Wird der Datenträger bei der Auswertung verändert?

PERKEO++ nimmt von sich aus niemals Schreibzugriffe auf das zu untersuchende Medium vor.

Trotz größter Sorgfalt bei der Entwicklung ist allerdings niemals gänzlich auszuschließen, dass eine Software wie PERKEO++ den auszuwertenden Datenträger bei der Analyse verändern könnte. Außerdem ist zu berücksichtigen, dass es durch die Komplexität des Zusammenspiels von BIOS, Betriebssystem und PERKEO++ theoretisch zu ungewollten Schreibzugriffen kommen kann.

Natürlich greift PERKEO++ selbst schreibend auf die Datei REPORT.TXT zu. Bei der Verwendung des Parameters „-arc“ wird das eingestellte temporäre Verzeichnis (meist C:\TMP unter Windows) genutzt. Der Parameter „-exec“ wird oft zum Aufruf von Befehlen verwendet, die schreibend auf Medien zugreifen.

4.2 Fehlermeldungen

Fehlermeldung	Bedeutung
Couldn't open library 'PERKEO.LIB'	PERKEO++ benötigt die Datei PERKEO.LIB im selben Verzeichnis wie PERKEO.EXE. Bei der Verwendung auf UNIX-Systemen stellen Sie bitte sicher, dass die Dateirechte korrekt gesetzt sind.
Couldn't read from library 'PERKEO.LIB'	Die Datei PERKEO.LIB konnte nicht korrekt gelesen werden. Sie ist ggf. beschädigt.
This library has an incompatible signature	Die Datei PERKEO.LIB ist nicht kompatibel zu ihrem Programm. Achtung: Demo- und Vollversion dürfen nicht vermischt werden!
Error 0010 - failed to approve 'PERKEO.LIB' as a valid library	Die Datei PERKEO.LIB ist verändert worden. Ein Virus oder Übertragungsfehler beim Download können die Ursache dafür sein.
PERKEO.EXE has been modified - check for possible virus infection	Die Datei PERKEO.EXE ist verändert worden. Ein Virus oder Übertragungsfehler beim Download können die Ursache dafür sein.
You need to supply a temporary directory. This can be done for example by 'set temp=c:\temp'.	Sie haben vergessen, die Umgebungsvariable TEMP oder TMP zu setzen. PERKEO für UNIX verwendet das Verzeichnis /tmp für temporäre Daten.
The path '\' is not a valid TMP path. You need to supply a drive letter like 'c:\'.	Fügen Sie einen Laufwerksbuchstaben in der Angabe bei SET TEMP=... hinzu.
Aborted because '\${xxx}' could not be parsed	Der angegebene Variablenname wird von PERKEO++ nicht unterstützt.
Could not open directory 'g:\'	Dieser Fehler kann diverse Ursachen haben. Unter Windows kann beispielsweise ein CD-ROM Laufwerk ohne eingelegte CD die Ursache sein. Unter UNIX können z. B. fehlende Rechte zu diesem Fehler führen.
Could not scan 'c:\swapfile'	Diverse Dateien, die vom Betriebssystem benutzt werden, können die Ursache für diese Fehlermeldung sein. Ferner können falsche Dateirechte

Fehlermeldung	Bedeutung
	oder defekte Archive diese Fehlermeldung auslösen.
Could not read from file 'test'	Der Inhalt der Datei "test" konnte nicht vollständig gelesen werden.
'test.arj' contains an invalid local fileheader	Das ARJ-Archiv ist beschädigt.
Can not deal with extended headers in archive 'test.arj'	Sog. "extended headers" in ARJ-Archiven werden nicht interpretiert.
Can't check encrypted file 'test.arj@password.txt'	Verschlüsselte Dateien innerhalb von ARJ-Archiven können nicht überprüft werden.
Not enough memory to scan 'test.arj@big.avi'	Es steht nicht genügend Speicher zur Verfügung, um die angegebene Datei zu untersuchen.
Could not write to temporary file 'big.avi'	Entweder kann die Datei "big.avi" nicht überschrieben werden oder es ist nicht genug Speicherplatz vorhanden.
ZIP: test.zip@big.avi (unsupported compression type 1)	PERKEO++ kennt nur die wichtigsten Kompressionstypen innerhalb von ZIP-Archiven. Einige Typen sind durch Patente geschützt sind und werden deshalb nicht interpretiert.
Couldn't call -EXEC for 'big.avi'	Dieser Fehler deutet auf Speichermangel hin.
Unknown structure in ZIP 'test.zip' (0x90909090)	Das ZIP-Archiv beinhaltet ungültige Datenstrukturen. Normalerweise deutet dies auf einen Übertragungsfehler hin.
CRC error, skipping test.zip@big.avi	PERKEO++ überspringt diese Datei, da die interne CRC-Prüfsumme fehlerhaft ist, was auf einen Übertragungsfehler hindeutet.
Aborted scanning 'test.zip' (error 8)	PERKEO++ bricht den Suchvorgang für dieses Archiv wegen schwerwiegender Fehler ab.

4.3 Definition Kinderpornographie

Hinweise auf kinderpornographische Inhalte, die lediglich zu Bildern von spärlich bekleideten, jungen Frauen führen, beschäftigen die Beamten unnötig und behindern andere Ermittlungen. Bitte vergleichen Sie daher die folgende Definition mit dem von Ihnen gefundenen Material, ehe Sie den Behörden einen Hinweis übermitteln.

Kinderpornographie ist die Darstellung des sexuellen Missbrauchs von Kindern. Bei der Darstellung kann es sich um tatsächlich stattgefundenes oder um wirklichkeitsnahes Geschehen

handeln, so dass auch mit Bildbearbeitungssoftware konstruiertes Material unter das Verbot fällt. Als Altersgrenze für Kinder gilt die Vollendung des 14. Lebensjahres.

Sexueller Missbrauch bedeutet, dass an dem Kind sexuelle Handlungen durch einen Erwachsenen oder ein anderes Kind vorgenommen werden, oder dass das Kind diese Handlungen an einem Erwachsenen vornimmt. Darunter fallen auch Handlungen, die das Kind an sich selbst vornimmt.

Nacktbilder von Kindern (FKK-Fotos) sind keine Kinderpornographie, sofern dabei nicht die Darstellung von Geschlechtsteilen in den Vordergrund rückt. Dies ist gegeben, wenn das Kind auf Regieanweisung unnatürliche Posen einnimmt (weit gespreizte Beine etc.).

4.4 Was tun bei Treffern ?

Nach derzeitiger Rechtslage ist eine Anzeige in diesem Fall nicht zwingend erforderlich. Es liegt also an Ihnen, ob Sie die Informationen über die gefundenen Daten weiterleiten. Bitte senden Sie **niemals** strafrechtlich relevante Daten an AUTEM GmbH. Meldungen können Sie an eine der nachfolgend aufgeführten Adressen senden. Sammeln Sie alle Informationen, die den Behörden helfen können, den Urheber der Veröffentlichung zu ermitteln. Diese können je nach Internet-Dienst variieren. Weisen Sie bei Ihrer Meldung darauf hin, dass PERKEO++ die Objekte aufgespürt hat.

Baden-Württemberg:	flz@lka.bwl.de
Bayern:	blka@polizei.bayern.de
Berlin:	lka@polizei.berlin.de
Brandenburg:	dauerdienst.lka@polizei.brandenburg.de
Bremen:	office@polizei.bremen.de
Hamburg:	www.polizei.hamburg.de (rechte Spalte unter "Hinweise auf Kinderpornografie")
Hessen:	hlka@polizei.hessen.de
Mecklenburg-Vorpommern:	www.isinet-mv.de/pages/index.htm?/pages/inhalt_meldestelle.htm
Niedersachsen:	www.polizei.niedersachsen.de/dst/lka/aktuelles/archiv/2002/kinderpornografie.htm
Nordrhein-Westfalen:	https://service.polizei.nrw.de/egovernment/service/internet.php
Rheinland-Pfalz:	landeskriminalamt.fahndung@polizei.rlp.de
Saarland:	kpik6kdd@land.slpol.de
Sachsen:	lka@polizei.sachsen.de
Sachsen-Anhalt:	Anzeigen.Hinweise@lka.pol.lsa-net.de
Schleswig-Holstein:	www.polizei.schleswig-holstein.de/wir/wir_missbrauch.html
Thüringen:	cybercop-tlka@t-online.de

In Österreich betreibt die Kriminalpolizei eine Meldestelle für Kinderpornographie: www.bmi.gv.at/meldestellen/. In der Schweiz nimmt die nationale Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBİK) Meldungen über verdächtige Internet-Inhalte ent-

gegen und leitet sie nach einer ersten Prüfung und Datensicherung an die zuständigen Strafverfolgungsbehörden im In- und Ausland weiter: www.cybercrime.admin.ch