WinHex/X-Ways Forensics

Allgemeines

Forensische Features

Arbeiten mit dem Hex-Editor

Menüreferenz

Besonderheiten

WinHex/X-Ways Forensics 12.2

X-Ways Software Technology AG
Carl-Diem-Str. 32 • D-32257 Bünde
E-Mail: mail@x-ways.com
Fax: 0721-151 322 561

Handelsregister Bad Oeynhausen HRB 7475
Vorstand: Dipl.-Wirtsch.inf. Stefan Fleischmann

Programmiert und weiterentwickelt seit 1995, letzte Aktualisierung im Mai 2005.

Unterstützte Betriebssysteme:

- Windows 95/98/Me
- Windows NT 4.0
- Windows 2000
- Windows XP

Die jeweils neueste Version dieses Programms finden Sie immer auf der Web-Site http://www.winhex.com. Besuchen Sie auch das WinHex-Forum unter http://www.winhex.net.

Wertung der ZDNet Software-Library: 5 von 5 Punkten!

Zu den professionellen registrierten Benutzern gehören Universitäts- und nationale Forschungseinrichtungen (z. B. das Institut für Informatik der Technischen Universität München, die Technische Versuchs- und Forschungsanstalt der Technischen Universität Wien, das Institut für Astronomie der Universität Wien, das Oak Ridge National Laboratory in Tennessee, USA), Behörden wie die Bundesstelle für Flugunfalluntersuchung, das Landeskriminalamt Niedersachsen, Zollkriminalamt Köln, Polizei Bremen/LKA, Kriminalpolizeiinspektion Schweinfurt, Landespolizeidirektion Freiburg, Kriminalpolizei Passau, diverse nationale Strafverfolgungsbehörden, Regierungsorganisationen und militärische Einrichtungen insbes. in den USA und Deutschland, das Verteidigungsministerium von Australien sowie Unternehmen aus den verschiedensten Branchen, z. B. Siemens Business Services, Siemens VDO AG, Infineon Technologies Flash GmbH & Co. KG, Toshiba Europe, Hewlett Packard, Microsoft Corp., Ericsson, Commerzbank AG, Visa International, DePfa Deutsche Pfandbriefbank AG, Analytik Jena AG, Ontrack Data International Inc., KPMG Forensic, Ernst & Young, Novell Inc., Lockheed Martin, BAE Systems, TDK Corporation, Seoul Mobile Telecom. Bestellen auch Sie die Vollversion!

Französische Übersetzung: Jérôme Broutin und Henri Pouzoullic, aktualisiert von Bernard Leprêtre
Spanische Übersetzung: José María Tagarro Martí
Italienische Übersetzung: Fabrizio Degni
Portugiesische Übersetzung: Heyder Lino Ferreira
Kryptographische Beratung: Alexandre Pukall

Die Algorithmen Pukall Cipher 1 (PC 1) und Pukall Stream Cipher Hash Function wurden von Alexandre Pukall entwickelt. Quellcode erhältlich unter http://www.freecode.com, http://www.multimania.com/cuisinons/progs/ und unter http://www.multimania.com/pc1/.

Der MD5 Message-Digest wurde entwickelt von RSA Data Security Inc.

Die „zlib"-Datenkompression mit den Algorithmen Deflate und Inflate wurde entwickelt von Jean-loup Gailly und Mark Adler. ftp://ftp.cdrom.com/pub/infozip/zlib/zlib.html

X-Ways Forensics enthält Software von Igor Pavlov, www.7-zip.com.

Werkzeug Hex-Editor

Ein Hexadezimal-Editor ist in der Lage, den Inhalt einer Datei jedes Typs vollständig anzuzeigen. Im Gegensatz zu einem Text-Editor kann er **alle** Bytes einer Datei darstellen, auch Steuerzeichen (für Zeilenumbruch, Tabulator usw.) und Programmcode, und zwar unter Angabe einer zweistelligen Zahl des Hexadezimalsystems (16er-System).

Ein Byte ist eine Kombination aus 8 Bits. Jedes Bit enthält entweder eine 0 oder eine 1, hat also einen von zwei möglichen Zuständen. Ein Byte kann daher einen von 2 hoch 8 (=256) verschiedenen Werten annehmen. Da 256 das Quadrat von 16 ist, kann jedes Byte durch eine zweistellige Zahl aus dem Hexadezimalsystem repräsentiert werden. Jede der beiden Stellen steht für eine Tetrade (auch: ein Nibble) eines Bytes, d. h. 4 Bits. Die möglichen Ziffern dabei sind 0-9 und A-F. Durch Änderung dieser Ziffern kann man einem Byte einem neuen Wert zuweisen.

Genauso ist es möglich, die Zeichen zu editieren, die jedem Byte zugeordnet sind (Textmodus, s. a. »Zeichen eingeben«). Diese Zeichen können z. B. Buchstaben oder Satzzeichen sein. Beispiel: Ein Byte, das den dezimalen Wert 65 hat, wird vom Hex-Editor in der Hexadezimal-Schreibweise mit 41 angeben (**4**•16+**1**=65) und in der Zeichenschreibweise mit dem Buchstaben »A«. Die Zuordnung von Zeichen gibt der sog. Zeichensatz an.

Entscheidend beim Editieren einer Programmdatei (z. B. EXE-Datei) ist, daß nicht die Länge der Datei (die Anzahl der Bytes, die sie enthält) und damit die relativen Positionen von Programmcode und Daten verändert werden. Dies würde die Ausführbarkeit des Programmcodes beeinträchtigen. Es ist generell zu beachten, daß Änderungen an Dateiinhalten zu anormalen Verhaltensweise der zugehörigen Programme führen können. Für viele Zwecke genügt es, sich auf das Editieren des in einer Datei vorkommenden Textes beschränken. Es ist in jedem Fall ratsam, vor dem Bearbeiten eine Sicherung der Datei anzulegen.

Sie werden feststellen, daß WinHex vor der Benutzung aller entscheidenden Funktionen Sicherheitsabfragen durchführt, die Fehlbedienungen vorbeugen.

Bestellung

Sie dürfen WinHex kostenlos ausprobieren. Für den regulären Gebrauch und für den Gebrauch als Vollversion benötigen Sie eine private, professionelle oder Specialist-Basislizenz. Wenn Sie WinHex auf mehr als einem Rechner installieren möchten, benötigen Sie entsprechend Zusatzlizenzen. Mit der Vollversion können Sie Dateien speichern, die größer als 200 KB sind, mit dem Disk-Editor Sektoren schreiben und virtuellen Arbeitsspeicher editieren.

• Private Lizenzen sind zu einem reduzierten Preis verfügbar für den nicht-kommerziellen Einsatz außerhalb von Unternehmen, Institutionen und öffentlicher Verwaltung.
• Professionelle Lizenzen erlauben die Benutzung der Software in *jeder* Umgebung (privat oder gewerblich, zu Hause, in Unternehmen, Organisationen und öffentlicher Verwaltung) und ermöglichen die Benutzung eigener Scripte und der WinHex API.
• Specialist-Lizenzen erlauben zusätzlich den Gebrauch der Specialist-Tools, das Interpretieren der Dateisysteme Ext2, Ext3, CDFS/ISO9660 und UDF, und sie bieten Unterstützung für RAID und dynamische Platten. Insbes. geeignet für IT-Sicherheitsexperten. Außerdem ist X-Ways Replica 1.3 enthalten, ein DOS-basiertes Programm zum forensisch sicheren Klonen von Festplatten und zur Erstellung von Image-Dateien.
• Forensische Lizenzen ermöglichen zusätzlich die mächtige Verwaltung von Fällen, die automatische Erstellung von Berichten, den internen Viewer (für Lizenzen ab v12.05 eine umfangreiche zusätzliche Viewer-Komponente), die Galerie-Ansicht, fortgeschrittene Aspekte der Laufwerksinhaltstabelle sowie ReiserFS-Unterstützung. Ferner erlauben sie die Verwendung von Encase Image-Dateien. Besonders nützlich für Ermittler in der Computerforensik. Die forensische Edition von WinHex heißt X-Ways Forensics. Ebenfalls enthalten ist X-Ways Replica 2.33, mit fortgeschrittenen Features.

Preise

Private Lizenzen:	EUR 36,98 zzgl. Mwst. = EUR 42,90 (Basislizenz) EUR 29,22 zzgl. Mwst. = EUR 33,90 (je Zusatzlizenz)
Professionelle Lizenzen:	EUR 69,90 zzgl. Mwst. (Basislizenz) EUR 44,90 zzgl. Mwst. (je Zusatzlizenz)
Specialist-Lizenzen:	EUR 129,90 zzgl. Mwst. (Basislizenz) EUR 79,90 zzgl. Mwst. (je Zusatzlizenz)
Forensische Lizenzen:	EUR 289,90 zzgl. Mwst. (Basislizenz) EUR 219,90 zzgl. Mwst. (je Zusatzlizenz)

Alle Preise verstehen sich zzgl. 16% Mwst. bei Erwerb innerhalb der Europäischen Union. Wenn Sie in US-Dollar bezahlen möchten, beachten Sie bitte die englische Anleitung.

Zahlung am kostengünstigsten per Überweisung auf u. a. Konto. Falls Sie von außerhalb der Euro-Zone überweisen, addieren Sie bitte EUR 7 hinzu. Sie können auch Bargeld schicken (auf eigenes Risiko). Zur **Online**-Bestellung (etwas teurer als o. a., Kreditkarten werden akzeptiert, schnellster Weg) folgen Sie bitte diesem Link: http://www.x-ways.net/winhex/order-d.html

Bei Ihrer Bestellung (schriftlich oder per E-Mail) nennen Sie bitte die Programmbezeichnung »WinHex 12.2«, Ihre Anschrift und E-Mail-Adresse. Nach Erhalt der Lizenzgebühr erhalten Sie die Freischaltcodes und Instruktionen zu deren Benutzung, damit Sie WinHex als Vollversion verwenden können. Alle späteren Versionen, die innerhalb von 12 Monaten nach Erscheinen *dieser* Version veröffentlicht werden, sind im Preis enthalten! (wahrscheinlich noch mehr)

Im Handelsregister eingetragene Unternehmen sowie Behörden und Institutionen können auf offene Rechnung bestellen. Bitte geben Sie dabei möglichst eine E-Mail-Adresse an.

Anschrift:
X-Ways Software Technology AG
Carl-Diem-Str. 32
D-32257 Bünde

Homepage: http://www.x-ways.net
E-Mail: mail@x-ways.com
Fax: 0721-151 322 561

Bitte besuchen Sie die WinHex-Website, um herauszufinden, ob es bereits eine neuere Version dieses Programms gibt.

Bankverbindung:
Kontoinhaber: X-Ways AG
Kontonr.: 2705390
BLZ: 48070024 (Deutsche Bank PGK)

Für Überweisungen aus dem Ausland:
SWIFT/BIC: DEUT DE 3B 492
IBAN: DE28 4807 0024 0270 5390 00
Adresse der Bank: Deutsche Bank, Filiale Bünde, Bahnhofstr. 7-9, 32257 Bünde, Germany

Vielen Dank für Ihre Bestellung!

Ganzzahlige Datentypen

Format/Typ	Bereich	Beispiel
8 Bit, vorzeichenbehaftet	-128...127	FF = -1
8 Bit, vorzeichenlos	0...255	FF = 255
16 Bit, vorzeichenbehaftet	-32.768...32.767	00 80 = -32.768
16 Bit, vorzeichenlos	0...65.535	00 80 = 32.768
24 Bit, vorzeichenbehaftet	-8.388.608...8.388.607	00 00 80 = -8.388.608
24 Bit, vorzeichenlos	0...16.777.215	00 00 80 = 8.388.608
32 Bit, vorzeichenbehaftet	-2.147.483.648...2.147.483.647	00 00 00 80 = -2.147.483.648
32 Bit, vorzeichenlos	0...4.294.967.295	00 00 00 80 = 2.147.483.648
64 Bit, vorzeichenbehaftet	-2^63...2^63-1	00 00 00 00 00 00 00 80 = -2^63

Sofern nicht anders angegeben, sind ganzzahlige Datentypen im Little-Endian-Format gespeichert. D. h. das erste Byte einer Zahl ist das niederstwertige und das letzte Byte ist das höchstwertige. Dies ist das gebräuchliche Format für Computer, auf denen Windows läuft.

Wenn beispielsweise in einer Datei die Hex-Werte 10 27 stehen, so entspricht dies als numerischer 16-Bit-Wert der Hexadezimal-Zahl 2710 (was ins Dezimalsystem umgerechnet 10000 bedeutet). Ebenso erscheint die Hexadezimal-Zahl 123 als 23 01. Das Byte mit dem Wert 23 ist das niederwertige (es enthält die Einer- und die 16er-Stelle der Zahl) und kommt daher zuerst.

Eine weitere Besonderheit ist beim Interpretieren von Daten-Bytes als numerische Werte zu beachten: Zahlen, die größer als die Hälfte der Maximalzahl verschiedener Werte eines Zahlentyps sind (8 Bit: 2 hoch 8=256, 16 Bit: 2 hoch 16=65536), können als negative Zahlen übersetzt werden. Der Hex-Wert 8235 (der in einer Datei als 35 82 erscheint, s. o.), kann ins Dezimalsystem zu 33333 umgerechnet werden. Ein Programm, das den 16-Bit-Wert aber vorzeichenbehaftet liest, erhält aber die Zahl "-32203". Diese zweite Möglichkeit ergibt sich, wenn von der Übersetzung als vorzeichenloser Wert die Maximalzahl verschiedener numerischer Werte des Zahlentyps subtrahiert wird (Beispiel: 33333-65536=-32203).

Die Darstellung in der Statusleiste, der Daten-Dolmetscher (der Daten in allen obigen Formaten auf einmal übersetzen kann) und die Funktion »Ganze Zahl suchen« im Suchen-Menü berücksichtigen die genannten Besonderheiten automatisch.

Gleitkomma-Datentypen

Typ	Bereich	signifikante Stellen	Bytes
float (single)	± 1,5e-45..3,4e38	7-8	4
real	± 2,9e-39..1,7e38	11-12	6
double (double)	± 5,0e-324..1,7e308	15-16	8
long double (extended)	± 3,4e-4932..1,1e4932	19-20	10

Die Bezeichnungen stammen aus der Programmiersprache C, in Klammern ist die entsprechende Pascal-Bezeichnung angegeben. Der Typ real in nur in Pascal vorhanden.

Die Gleitkommazahlen werden im Computer unter Zuhilfenahme von Zweierpotenzen abgebildet. Gespeichert werden die Mantisse m und der Exponent e aus der Darstellung m × (2 hoch e). Beide Werte enthalten ein Vorzeichen. Die Datentypen unterscheiden sich in ihrem Wertebereich (=der Anzahl der für den Exponenten reservierten Bits) und der Genauigkeit der Werte (=der Anzahl der für die Mantisse reservierten Bits).

Rechenoperationen mit Gleitkommazahlen werden in Intel-Architekturen vom mathematischen Koprozessor ausgeführt während der Hauptprozessor wartet. Der Intel 80x87 rechnet mit einer Genauigkeit von 80 Bit, RISC-Prozessoren häufig mit 64 Bit.

Hexadezimal-Werte in einem Editierfenster können vom Daten-Dolmetscher in alle vier Gleitkomma-Datentypen übersetzt werden.

ANSI-/IBM-ASCII

ANSI-ASCII ist der Zeichensatz, der in Windows-Anwendungen verwendet wird (genormt vom American National Standards Institute). MS-DOS benutzt den IBM-ASCII-Zeichensatz (auch als OEM-Format bezeichnet). Diese Zeichensätze unterscheiden sich in der Zuordnung von Zeichen, deren ASCII-Wert über 127 liegt. Wenn Sie einen Text zum Beispiel mit dem Windows-Notizblock (notepad.exe) schreiben und ihn sich später mit dem Editor von MS-DOS ansehen (edit.com), dann werden Umlaute und Sonderzeichen nicht richtig dargestellt.

Schalten Sie daher die Option »ANSI-Zeichensatz« ab, wenn Sie mit WinHex eine Datei editieren, die zu einem DOS-Programm gehört. Sie sehen dann die in der Datei enthaltenen Texte wie sie auch in diesem Programm erscheinen. Die von ihnen eingegebenen Zeichen werden dann umgekehrt auch richtig in diesem DOS-Programm dargestellt. Wenn Sie hingegen eine typische Windows-Datei bearbeiten (Initialisierungsdateien von Windows-Programmen, Windows-Programmdateien usw.), sollten Sie die Option »ANSI-Zeichensatz« aktivieren.

Mit der Funktion »Konvertieren« im Bearbeiten-Menü können Textdateien von einem Zeichensatz in den anderen konvertiert werden.

Die ersten 32 ASCII-Zeichen sind weder Buchstaben oder Zahlen noch Satzzeichen. Es handelt sich um Steuerzeichen.

Hex	Steuerzeichen
0	Null
1	Start of Header
2	Start of Text
3	End of Text
4	End of Transmission
5	Enquiry
6	Acknowledge
7	Bell
8	Backspace
9	Horizontal Tab
A	Line Feed
B	Vertical Tab
C	Form Feed
D	Carriage Return
E	Shift Out
F	Shift In
10	Data Link Escape
11	Device Control 1 (XON)
12	Device Control 2
13	Device Control 3 (XOFF)
14	Device Control 4
15	Negative Acknowledge
16	Synchronous Idle
17	End of Transmission Block
18	Cancel
19	End of Medium
1A	Substitute
1B	Escape
1C	File Separator
1D	Group Separator

1E Record Separator
1F Unit Separator

Prüfsummen

Eine Prüfsumme ist eine Kennzahl zur möglichst eindeutigen Identifizierung von Daten. Zwei Datensätze mit der gleichen Prüfsumme sind mit hoher Wahrscheinlichkeit exakt (Byte für Byte) gleich. Es kann z. B. sinnvoll sein, die Prüfsumme von Daten *vor* und *nach* einer möglicherweisen fehlerbehaften Übertragung zu berechnen. Ist sie in beiden Fällen gleich, dann sind die Daten mit hoher Wahrscheinlichkeit unverändert geblieben. Allerdings können Daten mit bösartiger Absicht so manipuliert werden, daß ihre Prüfsumme trotz Änderung gleich bleibt. Dadurch wird die Manipulation nicht bemerkt. Diese Möglichkeit schließen Digests aus.

Prüfsummen können in WinHex beim Öffnen einer Datei (s. Sicherheitsoptionen) und mit der Datenanalyse (im Extras-Menü) berechnet werden. Durch Drücken der Tastenkombination Alt+F2 wird die in der Informationspalte angezeigte Prüfsumme neu berechnet, wenn an einer Datei Änderungen vorgenommen wurden.

Die Standard-Prüfsumme ist einfach die Summe aller Bytes einer Datei auf einem 8-Bit-, 16-Bit-, 32-Bit- oder 64-Bit-Akkumulator. Ein CRC (Cyclic Redundancy Code) wird mit einem komplizierteren, auf Polynomdivision beruhenden Algorithmus berechnet, der *sicherer* ist. Das drückt sich in einer niedrigeren Wahrscheinlichkeit dafür aus, für zwei verschiedene Dateien durch Zufall dieselbe Prüfsumme zu erhalten.

Beispiel: Wenn in einer Datei durch fehlerhafte Übertragung zwei Bytes verfälscht werden, sich die Abweichungen aber genau ausgleichen (z. B. erstes Byte +1, zweites Byte -1), dann bleibt die Standard-Prüfsumme im Gegensatz zum CRC unverändert.

Technische Hinweise

Maximalzahl geöffneter Fenster:	1000 (Windows NT/2000), 500 (Windows 9x)
Maximale Datei- u. Datenträgergröße:	ca. 2000 GB
Max. Anz. paralleler Instanzen:	99
Max. umkehrbare Tastatureingaben:	65535
Verschlüsselungstiefe:	128 Bit
Digest in Sicherungsdateien:	128/256 Bit
Zeichensätze der Textdarstellung:	ANSI-/IBM-ASCII, EBCDIC
Offset-Darstellung:	hexadezimal/dezimal

• Die Fortschrittsanzeige bei länger andauernden Operation zeigt in Prozent den Anteil des Vorgangs an, der bereits erledigt ist. Bei allen Suchen- und Ersetzen-Operationen zeigt sie jedoch die relative Position in der aktuellen Datei an. Dies entspricht dem bereits erledigten Anteil des Vorgangs, wenn in der gesamten Datei gesucht wird, also die Option »Nur im Block suchen« nicht verwendet wird.

• Zur optimalen Darstellung aller Schriftzeichen in WinHex sollte Ihr Windows-System *keine* extragroßen Systemschriften benutzen.

• WinHex wurde ausschließlich für Computer im »Little-Endian«-Modus konzipiert.

• Such- und Ersetzen-Funktionen laufen generell schneller ab, wenn kein Jokerzeichen verwendet und (bei Text-Suche) nach Groß- und Kleinschreibung unterschieden wird. Außerdem gilt: Je länger die Such-Zeichenfolge, desto schneller die Such-Funktion.

• Beim Suchen mit aktivierter Option »Vorkommen zählen« und beim Ersetzen ohne Bestätigung bieten sich für einen Suchalgorithmus zwei Alternativen für das Verhalten bei Fundstellen an, die in Sonderfällen zu unterschiedlichen Ergebnissen führen. Dies soll anhand eines Beispiels verdeutlicht werden:

In der Zeichenfolge »ananas« wird nach »ana« gesucht; das Vorkommnis beim ersten Zeichen wurde gefunden.
1. Möglichkeit: Ab dem zweiten Zeichen wird wieder nach »ana« gesucht. Beim dritten Zeichen wird dann ein Vorkommnis registriert.
2. Möglichkeit: Die drei mit der Suchzeichenfolge übereinstimmenden Zeichen werden übersprungen. »ana« wird erst wieder ab dem vierten Zeichen gesucht, in »nas« also nicht mehr gefunden.

In WinHex wird der zweiten Alternative gefolgt, da sie für das Zählen von Vorkommen und das Ersetzen ohne Bestätigung meistens sinnvollere Ergebnisse liefert. (Wenn Sie normale Suchvorgänge mit F3 fortsetzen oder Ersetzen *mit* Bestätigung wählen, wird nach der ersten Methode verfahren.)

• Hier erfahren Sie etwas über den Aufbau des Master-Boot-Sektors einer Festplatte, den Sie mit dem Disk-Editor editieren können.

• Weitere technische Informationen erhalten Sie auf der WinHex-Homepage unter http://www.winhex.com.

Rechtliche Hinweise

Lizenzvereinbarung

Wenn Sie ein Software-Produkt der X-Ways Software Technology AG installieren und/oder benutzen, erklären Sie sich damit einverstanden, durch die Bestimmungen dieser Lizenzvereinbarung gebunden zu sein. Falls Sie nicht zustimmen, installieren und benutzen Sie die Software nicht.

Unlizenzierte Evaluationsversionen dürfen nur zu Testzwecken genutzt werden. Der Erwerb einer Lizenz berechtigt Sie, eine Kopie der Vollversion der Software auf einem Computer zu installieren. Weitere Lizenzen erlauben Ihnen entsprechend weitere Installationen der Vollversion zur selben Zeit. Ein Rückgaberecht besteht auch für Verbraucher im Sinne des § 13 BGB nicht. Auf Grund ihrer Beschaffenheit sind elektronisch übermittelte Software und Lizenzen für eine Rücksendung nicht geeignet (gem. § 312d Nr. 4 BGB).

Die Software und alle sie begleitenden Dateien, Daten und Materialien werden „wie besehen“ (kostenlos verfügbare Evaluationsversion) ohne Garantie auf Fehlerfreiheit übermittelt, unter Ausschluß jeglicher Gewährleistung. Der Benutzer verwendet die Software ausschließlich auf eigenes Risiko, insbesondere wissend, daß sie nicht für den Gebrauch in hochsensiblen Umgebungen entwickelt wurde und vorgesehen ist, die einen fehlerfreien Ablauf erfordern und wo ein Versagen, mißbräuchliche oder unangemessene Anwendung leicht zu Todesfällen, Verletzungen oder großen physischen, ökonomischen oder Umwelt-Schäden führen kann. In keinem Fall ist die X-Ways Software Technology AG oder ihre Vorstände, Mitarbeiter, verbundene Unternehmen oder Zulieferer für Schäden jeglicher Art verantwortlich, die durch den Gebrauch oder die Unmöglichkeit des Gebrauchs entstehen. Die X-Ways AG haftet maximal in Höhe der gezahlten Lizenzgebühr.

Die Software ist urheberrechtlich geschütztes Eigentum. Sie darf nicht verändert, dekompiliert, disassembliert, entschlüsselt, extrahiert oder irgendwie anderweitig verändert werden. Die Software oder Teile davon dürfen nicht als Basis für abgeleitete Werke verwendet oder an Dritte vermietet, verkauft, weiterlizenziert werden, sofern nicht ausdrücklich von der X-Ways Software Technology AG erlaubt. Alle Rechte jeglicher Art an der Software, die nicht ausdrücklich in dieser Lizenzvereinbarung gewährt werden, stehen exklusiv der X-Ways AG zu.

Keine Komponente der Software (außer der WinHex API) darf von anderen Applikationen oder Prozesses aus verwendet werden.

Zur Programmhilfe

Der Hersteller hat alle Sorgfalt walten lassen, um vollständige und korrekte Informationen in diesem Werk zu publizieren. Er übernimmt aber weder Garantie noch die juristische Verantwortung oder irgendeine Haftung für die Nutzung dieser Informationen, für deren Wirtschaftlichkeit oder fehlerfreie Funktion für einen bestimmten Zweck. Ferner kann der Hersteller für Schäden, die auf sachgemäße oder unsachgemäße Handhabung oder Fehlfunktionen des Programms oder ähnliches zurückzuführen sind, nicht haftbar gemacht werden, auch nicht für die Verletzung von Patent- und anderen Rechten Dritter, die daraus resultieren. Der Hersteller übernimmt keine Gewähr dafür, daß die beschriebenen Verfahren, Programme usw. frei von Schutzrechten Dritter sind. Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, daß solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden

dürften.

Allgemeine Optionen

1. Spalte:

• Beim **Programmstart** kann WinHex optional das sog. **Start-Center** anzeigen oder die letzte **Fensterkonstellation wiederherstellen** (alle Fenster mit ihren Größen und Positionen, wie Sie sie am Ende der vorhergehenden WinHex-Sitzung verlassen haben).

• Geben Sie die Zahl der **zuletzt geöffneten Dokumente** an, die WinHex sich **merken** und im Start-Center anzeigen soll (max. 255). Bis zu 9 davon werden gleichzeitig auch am Ende des Datei-Menüs aufgeführt.

• Zusätzlich zu der Information, *welche* **Dokumente** (Dateien oder Datenträger) Sie zuletzt geöffnet hatten, kann WinHex sich optional auch die letzten Editier**positionen** und den Block (falls definiert) **merken**.

• **WinHex** kann sich **im Windows-Kontextmenü** eintragen. Das Kontextmenü sehen Sie, wenn Sie im Windows-Explorer oder auf dem Desktop mit der rechten Maustaste ein Objekt anklicken. Wenn Sie die Option nur halb aktivieren, gibt es keinen Kontextmenü-Eintrag für einzelne Dateien.

• Sie können Winhex auf Wunsch **mehrfach zugleich ausführen**. In der Voreinstellung jedoch wird eine bereits geladene Instanz des Programms aktiviert statt eine neue erzeugt.

• Wenn die Option »**Dateidatum und -zeit beibehalten**« aktiviert ist, werden Datum und Uhrzeit der letzten Änderung einer Datei beim Speichern auf dem Stand belassen, den die Datei zum Zeitpunkt des Öffnens hatte.

• Wenn die Option **Auf Überhangsektoren testen** ausgeschaltet ist, versucht WinHex nicht, beim Öffnen einer physischen Festplatten auf Überhangsektoren zuzugreifen. Falls solche Sektoren gefunden werden, speichert WinHex deren Erkennung für das nächste Mal, wenn Sie eine Festplatte physisch öffnen. Sie können dann aber immer noch einen erneuten Test erzwingen, indem Sie beim Öffnen die Shift-Taste gedrückt halten. Das Testen auf Überhangsektoren kann auf einigen Systemen *in Ausnahmefällen* sehr lange Wartezeiten mit sich bringen, merkwürdiges Verhalten des Windows-Systems oder sogar Schäden an der Betriebssystem-Installationhervorrufen. Nur unter Windows XP werden Überhangsektoren automatisch mit berücksichtigt, was diese Option bedeutungslos macht.

• Wenn die Option **Gelöschte Partitionen erkennen** eingeschaltet ist, versucht WinHex, offensichtliche gelöschte Partitionen ausfindig zu machen, die sich in Lücken zwischen existierenden Partitionen befinden oder direkt am Anschluß an die letzte Partition im unpartitionierten Bereich, und zwar beim Öffnen physischer Festplatten. Solcherlei zusätzlich erkannte Partitionen werden im Zugriffsschaltermenü mit aufgelistet und dort als gelöscht gekennzeichnet. Bitte beachten Sie, daß in Partitionslücken gefundene gelöschte Partitionen die Partitionsnumerierung beeinflussen. Z. B. wird eine Partition Nr. 3 zu Partition Nr. 4, wenn vor ihr eine gelöschte Partition erkannt wird.

• Die **alternative Plattenzugriffsmethode** für physische Festplatten und optische Discs unter Windows NT/2000/XP kann Ihnen u. U. Zugriff ermöglichen auf Festplatten, die mit einer unkonventionellen Sektorgröße formatiert sind, oder andere Datenträger, auf die sonst nicht zugegriffen werden kann, sowie auf einige Sektoren am Ende von CD-ROMs/DVDs, die sonst übersehen werden könnten. Beachten Sie, daß diese Zugriffsmethode langsamer als die reguläre ist.

• Standardmäßig werden **Editierfenster** nicht **maximiert geöffnet**.

• Bei einem Rechtsklick kann **WinHex** ein spezielles **Kontextmenü** anzeigen, das reguläre Bearbeiten-Menü oder das Ende des aktuellen Blocks setzen. Auch wenn diese Option ausgeschaltet ist, können Sie

das Kontextmenu anzeigen lassen, indem Sie die Umschalt-Taste gedrückt halten, wenn Sie einen Rechtsklick ausführen.

• Sofern die Option »**Datei-Icons anzeigen**« aktiviert ist, werden ab einer Bildschirmauflösung von 800×600 die in der aktuellen Datei enthalten Windows-Icons in der Informationsspalte angezeigt. Enthält eine Datei keine Icons, so wird das dem Dateityp zugeordnete Icon dargestellt, wenn die Option »voll« gewählt ist.

• Entscheiden Sie, ob das Betätigen der **»Enter«**-Taste Hex-Werte in die zu editierende Datei schreiben soll. In der Voreinstellung sind dies 0x0D0A (=Zeilenende-Zeichen). Sie können bis zu vier zweistellige Hex-Werte angeben. Das Start-Center könnte dann immer noch mit UMSCHALT+ENTER geöffnet werden.

• Auf Wunsch können Sie mit der Tabulator-Taste auf Ihrer Tastatur das **Tabulator-Zeichen** erzeugen (0x09). Um dann vom Hexadezimal-Modus in den Text-Modus und umgekehrt zu wechseln, müssen Sie die Tabulator-Taste zusammen mit der Umschalt-Taste drücken.

2. Spalte:

• Ändern Sie wenn nötig den **Ordner**, in dem die **temporären Dateien** angelegt werden. Voreingestellt ist der Ordner, den die Umgebungsvariablen »TEMP« Ihres Systems definiert.

• Ebenfalls wählen können Sie den **Ordner**, in dem die **Sicherungsdateien** angelegt werden. Normalerweise ist er identisch mit dem für temporäre Dateien.

• Bestimmen Sie außerdem den **Ordner**, in dem **Projekt-, Script- und Falldateien** angelegt werden. Standardmäßig geschieht dies in dem Verzeichnis, in dem WinHex installiert ist.

• Bestimmen Sie ferner den **Ordner**, in dem die **interne Hash-Datenbank** verwaltet wird.

• If the creation of thumbnails for pictures within large solid RAR archives for gallery view is too slow, you may want to disable it.

• Sie können die von Ihnen bevorzugte Größe der Miniaturansichten in Pixeln angeben. WinHex reduziert die Größe erforderlichenfalls automatisch, so daß zumindest so viele Dateien in der Galerie-Ansicht angezeigt werden können wie im sichtbaren Ausschnitt des Verzeichnis-Browsers.

• Wenn die Galerie-Ansicht aktiv ist, kann WinHex optional das Laden der Miniaturansichten im Hintergrund für Bilder außerhalb des sichtbaren Ausschnitts des Verzeichnis-Browsers fortsetzen, wenn die Anzahl der Dateien nicht zu groß ist.

3. Spalte:

• Bestimmen Sie, ob die **Offsets** (Byte-Adressen) in **dezimaler** oder **hexadezimaler** Schreibweise angegeben und zur Eingabe verlangt werden. Diese Einstellung gilt für den gesamten Umfang des Programms.

• Auf Wunsch können beim Benutzen des RAM-Editors anstelle von Null-basierten Offsets **virtuelle Adressen** angezeigt werden. Dies geschieht grundsätzlich in hexadezimaler Schreibweise. Im Dialogfenster der Funktion »Offset aufsuchen« sind dann auch virtuelle Adressen einzugeben.

• Es können **Seiten**- und Sektor**trennlinien angezeigt** oder ausgeblendet werden. Wenn die Option nur halb gewählt ist, werden nur Sektortrennlinien angezeigt.

• Geben Sie an, wie viele **Bytes** in einem Editierfenster **pro Zeile** dargestellt werden sollen. Standardeinstellungen sind 16 oder 32 Bytes, je nach Bildschirmauflösung.

• Geben Sie an, wie viele **Bytes** als **Gruppe** zusammenhängend angezeigt werden sollen. I. d. R. empfiehlt sich eine Zweier-Potenz.

• Sie können die Anzahl der **Zeilen** bestimmen, die mit Hilfe des **Mausrades** (falls vorhanden) vorwärts und zurück **gerollt** werden können.

• Bestimmen Sie außerdem das Aussehen der **Dialog-** und Meldungs**fenster** und Schalter in WinHex. Sie haben die Wahl zwischen mehreren verschiedenen **Stil**en.

• Bei aktivierter Option »**Windows-Standardfarben benutzen**« wird das Editorfenster in den Farben angezeigt, die in der Windows-Systemsteuerung eingestellt sind. Andernfalls werden die Standardfarben von WinHex verwendet.

• Sie haben die Möglichkeit, die **Hintergrundfarbe** des **Blocks** zu bestimmen, wenn die Option »Windows-Standardfarben benutzen« nicht aktiviert ist.

• Wählen Sie die **Hintergrundfarbe** für jeden zweiten **Datensatz** in der Datensatz-Darstellung.

• Bestimmen Sie die Standard**farbe** für neu aufgenommene **Anmerkungen**/Positionen/Lesezeichen.

• WinHex kann **veränderte Bytes**, also bereits editierte Bereiche einer Datei, eines Datenträgers oder des Arbeitsspeichers, in einer gesonderten Farbe Ihrer Wahl anzeigen, damit Sie Originaldaten von Ihren Änderungen unterscheiden können.

• Wählen Sie eine **Schriftart** für die Darstellung im ANSI-ASCII-Format aus. Das Verwenden der WinHex-Schriftart stellt sicher, daß auch Sonderzeichen in der Textdarstellung angezeigt werden (z. B. die Symbole TM und Euro sowie echte Anführungszeichen).

• Bei aktivierter Option »**Windows-Fortschrittsanzeige**« wird während lang dauernden Vorgängen die Windows-typische anstatt der WinHex-eigenen Fortschrittsanzeige verwendet.

Die Voreinstellungen sämtlicher Optionen können durch Benutzen der Funktion »Initialisieren« im Hilfe-Menü wiederhergestellt werden.

Zeichen eingeben

Mit der Tastatur lassen sich im Hex-Modus nur Hexadezimal-Zeichen eingeben ('0' bis '9' und 'A' bis 'F').

Im Text-Modus lassen sich dagegen alle Zeichen eingeben: Buchstaben, Zahlen, Satzzeichen und auch Sonderzeichen (wie '»', ']' und '^'). Durch Benutzen des Windows-Programms »Zeichentabelle« kann man herausfinden, durch welche Tastenkombinationen evtl. erwünschte Sonderzeichen zu erzeugen sind (z. B. Alt-1-7-5 für '»').

Editier-Modi

Der Modus, in dem eine Datei oder ein Datenträger geöffnet ist, wird in der grauen Informationsspalte angezeigt. Deren Kontextmenü enthält einen Befehl, um den Modus des aktuellen Fensters selektiv zu ändern.

View-Modus: Empfohlener Modus für computerforensische Untersuchungen. Um den strengen forensischen Anforderungen zu genügen, ist dies der einzige Modus, der in X-Ways Forensics verfügbar ist, außer für Dateien im Verzeichnis des aktuellen Falls und im allgemeinen Ordner für temporäre Dateien, damit deren Decodierung, Entschlüsselung oder Konvertierung usw. möglich ist. Dateien und Datenträger, die im View-Modus geöffnet werden, können nicht (absichtlich oder versehentlich) editiert/verändert, sondern nur eingesehen werden. Dies entspricht der Möglichkeit in anderen Programmen, Dateien »schreibgeschützt« zu öffnen..

Standard-Editiermodus: Im Standard-Editiermodus werden Änderungen, die Sie an einer geöffneten Datei oder einem Datenträger vornehmen, in einer temporären Datei gespeichert. Diese wird dynamisch verwaltet. Erst beim Speichern oder Schließen werden die Änderungen dann nach Rückfrage in die Originaldatei bzw. auf den Datenträger übertragen.

In-Place-Modus: Verwenden Sie diesen Modus mit Vorsicht. *Sämtliche* Änderungen (Tastatureingaben, Füllen/Entfernen des Blocks, Schreiben des Zwischenspeichers, Ersetzen-Vorgänge, ...) werden direkt in die Originaldatei bzw. auf den Datenträger (»in-place«) geschrieben. Dies geschieht dynamisch, spätestens aber, wenn das Editierfenster geschlossen wird, ohne weitere Rückfragen. Es ist daher nicht erforderlich, den Menüpunkt »Speichern« im Dateimenü aufzurufen, es sei denn, Sie möchten sicherstellen, daß alle Änderungen zu einem bestimmten Zeitpunkt geschrieben werden, wenn das Editierfenster noch geöffnet ist.

Dieser Modus empfiehlt sich, wenn das im Standard-Editiermodus obligate Übertragen von Daten aus der Originaldatei in die Temporärdatei und umgekehrt zu zeitaufwendig wäre und zuviel Festplattenspeicherplatz verbräuchte. Dies kann z. B. dann der Fall sein, wenn in großen Dateien viele Änderungen vorgenommen werden sollen. Da im In-Place-Modus keine Daten in temporären Dateien gespeichert werden, ist dieser Editiermodus generell schneller als der Standard-Editiermodus. Der In-Place-Modus ist der einzige Modus, in dem der RAM-Editor benutzt werden kann.

Hinweis: Auch im In-Place-Modus muß eine temporäre Datei angelegt werden, wenn die *Größe* der Originaldatei geändert wird.

Statusleiste

Die Statusleiste zeigt beim Einsehen einer Datei folgende Informationen an:

1. Feld: aktuelle Seite und Anzahl der Seiten, auf denen die aktuelle Datei dargestellt wird
2. Feld: Cursorposition (Offset in der Datei)
3. Feld: ins Dezimalsystem übersetzte Hex-Werte an der Cursorposition
4. Feld: Blockanfang und -ende (falls festgelegt)
5. Feld: Größe des Blocks in Byte (dto.)

Durch einen Klick der linken Maustaste läßt sich...
• im 1. Feld eine andere Seite aufschlagen,
• im 2. Feld den Cursor zu einem bestimmten Offset bewegen,
• im 3. Feld das Format festlegen, in dem die Hex-Werte als Zahlen des Dezimalsystems interpretiert werden, und
• im 4. und 5. Feld den Block neu definieren.

Klicken Sie mit der rechten Maustaste, um in einem Feld der Statusleiste angezeigte Informationen in die Zwischenablage zu kopieren.

Durch einen Mausklick rechts im 2. Feld der Statusleiste können Sie von absoluter Offsetdarstellung (Standard) auf relative Datensatz-Offsets umschalten. Dies ist nützlich, wenn die von Ihnen im Hex-Editor untersuchten Daten aus gleichlangen Datensätzen bestehen.

Ein Rechts-Klick auf das 3. Feld der Statusleiste erlaubt es außerdem, die vier Hex-Werte an der aktuellen Cursorposition in umgekehrter Reihenfolge in die Zwischenablage zu kopieren. Dies ist nützlich beim Verfolgen von Zeigern.

Arbeitserleichterungen

- Linke Maustaste — Blockanfang festlegen (Doppelklick)
- Rechte Maustaste — Blockende festlegen
- Rechte Maustaste — Blockmarkierung aufheben (Doppelklick)
- Shift+Pfeiltasten — Block markieren
- Alt+1 — Blockanfang setzen
- Alt+2 — Blockende setzen
- Tabulatortaste — zwischen Text- und Hex-Modus umschalten
- Einfg-Taste — zwischen Überschreib- und Einfüge-Modus umschalten
- Strg+Q — alle Fenster schließen
- Enter — Start-Center aufrufen
- Strg+Enter — Fenster-Manager aufrufen
- ESC — aktuellen Vorgang abbrechen, Blockauswahl aufheben, Dialogfenster oder Schablone verlassen
- PAUSE — aktuellen Vorgang anhalten bzw. fortsetzen
- F11 — »Offset aufsuchen« wiederholen (mit Strg = von aktueller Position in umgekehrter Richtung)
- Alt++ — Variante von »Offset aufsuchen«, um x Sektoren *ab*wärts zu springen
- Alt+- — Variante von »Offset aufsuchen«, um x Sektoren *auf*wärts zu springen
- Shift+F7 — Zeichensatz wechseln
- (Shift+)Alt+F11 — »Block verschieben« wiederholen
- Strg+Shift+M — Anmerkungen eines offenen Asservats aufrufen
- Alt+F2 — Auto-Hash (Prüfsumme oder Digest) neu berechnen
- Strg+F9 — Menü des Zugriffs-Schalters öffnen (bei Datenträgern)

• Alt+Links und Alt+Rechts erlauben das Wechseln zwischen Datensätzen innerhalb einer Schablone (wie die Schalter < und >). Alt+Pos1 und Alt+Ende wechseln zum ersten bzw. letzten Datensatz.

• Alt+G bewegt den Cursor im Editierfenster zur aktuellen Position in einer Schablone und schließt die Schablone.

• WinHex akzeptiert Dateinamen als Startparameter und öffnet Dateien, die per Drag&Drop (mit der Maus) in das Programmfenster gezogen werden.

• Der Einsatz von Scripts kann Ihr Arbeiten mit WinHex effizienter machen.

• Als Befehlszeilenparameter wird auch der Name eines Scripts akzeptiert.

• »Ungültige Eingabe«: Nach dem Schließen einer solchen Fehlermeldung zeigt der blinkende Cursor an, welcher von Ihnen angegebene Parameter ungültig ist und korrigiert werden muß.

• Die Offset-Schreibweise (dezimal oder hexadezimal) läßt sich durch einen Mausklick auf die Offsetdarstellung im Editorfenster umstellen. Die dezimale Schreibweise ist mit oder ohne führende Nullen verfügbar (Mausklick rechts).

• Klicken Sie probehalber auf die Statusleiste (linke und rechte Maustaste).

Disk-Editor

Im Extras-Menü finden Sie die Funktion »Disk-Editor«. Der Disk-Editor ermöglicht es, den Inhalt einer Diskette oder Festplatte ohne Rücksicht auf die Dateistruktur direkt (=sektorweise) einzusehen. Wählen Sie zunächst aus einer Liste mit den auf Ihrem System installierten Laufwerken einen Datenträger aus. Sie können auf einen Datenträger logisch (vom Betriebssystem gesteuert) oder physisch (vom BIOS gesteuert) zugreifen. Auf den meisten Computersystemen können Sie sogar CD-ROMs und DVDs einsehen. Es gibt einen optionalen Roh-Zugriff für optische Laufwerke, der es ermöglicht, von Audio-CDs zu lesen und auch die kompletten 2352-Byte-Sektoren auf Daten-CDs (CD-ROM und Video-CDs), die Fehlerkorrektur-Informationen enthalten.

Logisches Laufwerk meint einen zusammenhängenden, formatierten Teil eines Datenträgers (eine Partition), der unter Windows als Laufwerksbuchstabe zugänglich ist (z. B. »C:«). Zum Öffnen erfordert WinHex, daß Windows auf das Laufwerk zugreifen kann. *Physischer Datenträger* hingegen ist ein Medium als Ganzes, wie es an den Computer angeschlossen ist, z. B. eine Festplatte incl. *aller* Partitionen. Der Datenträger braucht zum Öffnen in WinHex normalerweise nicht formatiert zu sein.

Gewöhnlich ist es vorteilhafter, ein logisches Laufwerk statt eines physischen Datenträgers zu öffnen, weil dann mehr Features zur Verfügung stehen. Beispielsweise sind »Cluster« vom Dateisystem definiert, die Zuordnung von Clustern zu Dateien (und umgekehrt) ist WinHex bekannt, »freier Speicher« und »Schlupfspeicher« haben eine Bedeutung. Nur wenn Sie Sektoren editieren möchten, die außerhalb eines logischen Laufwerks liegen (etwa der Master Boot Record), wenn Sie etwas auf allen Partitionen einer Festplatte auf einmal suchen möchten oder wenn eine Partition beschädigt oder mit einem Windows unbekannten Dateisystem formatiert ist, so daß Windows sie nicht als Laufwerksbuchstaben zugänglich macht, empfiehlt es sich, den physischen Datenträger zu öffnen. Über das Menü, das erscheint, wenn Sie den mit »Zugriff« beschrifteten Schalter anklicken, können Sie auch Partitionen aus einer physischen Festplatte heraus einzeln öffnen. WinHex versteht sowohl konventionelle MBR-Partitionierung als auch die mit Windows 2000 eingeführten, vom LDM (Logical Disk Manager) verwalteten dynamischen Platten (nur Specialist- und forensische Lizenzen). Alle Partitionstypen werden unterstützt: simple, spanned, striped und RAID 5. Das Gedrückthalten der Strg-Taste beim öffnen von Festplatten unterdrückt die Erkennung und spezielle Behandlung von dynamischen Platten und stellt sicher, daß Festplatten so interpretiert werden, als wären sie auf konventionelle Weise partitioniert worden.

Verzeichnis-Browser
Disk Editor Fragen & Antworten

Bitte beachten Sie die folgenden Einschränkungen bzw. Voraussetzungen:

• Um unter Windows NT und seinen Nachfolgern auf Festplatten zugreifen zu können, sind Administrator-Rechte erforderlich.
• Die Ersetzen-Funktionen sind im Disk-Editor nur im In-Place-Modus verfügbar.
• WinHex kann auf CD-R(OM)s und DVDs nicht *schreiben*.
• Der Disk-Editor kann nicht auf Netzlaufwerke zugreifen.

Freien Speicher des Datenträgers editieren (Windows 95/98/Me)

Unter Windows 95/98/Me ist es möglich, den unbenutzten Speicher eines logischen Datenträgers einzusehen und zu editieren. Dabei entfallen die o. g. Einschränkungen. Es wird eine Datei angelegt, die den gesamten freien Speicher auf dem gewählten Datenträger belegt. In dieser Datei können Sie nun im In-Place-Editiermodus Änderungen vornehmen. Dies kann die Integrität der Daten in benutzten Bereich des Datenträgers *nicht* beeinflussen.
Sie können mit Hilfe dieser Funktion versehentlich gelöschte Daten, die noch nicht von neuen Dateien überschrieben worden sind, wiederherstellen, z. B. indem Sie sie erst suchen, dann als Block markieren

und kopieren. Daten aus Dateien, die mit der Funktion »Sicheres Löschen« von WinHex gelöscht wurden, befinden sich natürlich nicht mehr in unbenutzten Bereichen des Datenträgers.

Auf Disk schreiben: Entspricht dem Befehl »Speichern« für Dateien und befindet sich an dessen Stelle im Menü. Schreibt die von Ihnen vorgenommenen Änderungen auf den Datenträger. Bitte beachten Sie, daß Sie damit einen äußerst kritischen Eingriff in die Integrität des Datenträgers vornehmen. Sofern die entsprechende Rückgängig-Option eingeschaltet ist, wird von den betroffenen Sektoren vor dem Überschreiben eine Sicherung angelegt. *Die Funktion nur in der Vollversion verfügbar.*

Hier erfahren Sie etwas über den Aufbau des Master-Boot-Record einer Festplatte, den Sie mit dem Disk-Editor editieren können.

Datei-Menü

Neu: Hier können Sie eine neue Datei anlegen, deren Inhalt mit Null-Bytes initialisiert wird. Es ist die gewünschte Größe der Datei in Bytes anzugeben (>0). Die neue Datei wird prinzipiell im Standard-Editiermodus geöffnet.

Öffnen: In einem Dateiauswahlfenster markieren Sie eine oder mehrere Dateien, die Sie mit dem Hex-Editor einsehen oder bearbeiten möchten. Sofern Sie WinHex nicht schon im Optionen-Menü als Viewer oder In-Place-Editor eingestellt haben, können Sie einen der drei Editier-Modi zum Öffnen der Datei(en) wählen.

Speichern: Hier speichern Sie ein zuvor geöffnete Datei mit allen von Ihnen vorgenommenen Änderungen, nachdem Sie eine Sicherheitsabfrage mit »Ja« beantwortet haben. Im In-Place-Editiermodus ist das Aufrufen dieses Befehls nicht notwendig. Beim Benutzen des Disk-Editors heißt dieser Befehl »Auf Disk schreiben«.

Speichern unter: Speichert eine Datei unter einem neuen Namen oder in einem anderen Ordner. Existiert bereits eine Datei mit diesem Namen, so werden Sie gefragt, ob die vorhandene Datei überschrieben werden soll.

Sicherung anlegen/Datenträger-Sicherung

Sicherung laden: Wählen Sie eine Image- oder Sicherungsdatei (=WHX-Datei) aus, deren Inhalt (eine Datei oder Datenträger-Sektoren) Sie wiederherstellen möchten.

Sicherungs-Manager

Ausführen: Führt die aktuell dargestellte Datei mit allen evtl. vorgenommenen Änderungen aus. Es muß sich entweder um eine unter DOS oder Windows ausführbare EXE- oder COM-Datei handeln oder der Dateityp muß unter Windows mit einer Anwendung verknüpft worden sein. Dann wird dieses Programm gestartet und die aktuelle Datei geladen. Sie können mit dieser Funktion z. B. überprüfen, ob die vorgenommenen Änderungen in einer Programmdatei ihre Ausführbarkeit beeinträchtigt haben.

Drucken

Eigenschaften: Hier können die Größe, Datum und Uhrzeit der Erzeugung, der letzten Änderung und des letzten Zugriffs sowie Attribute (A: zu archivierend, S: System, H: versteckt, R: schreibgeschützt) einer Datei (unter Windows NT auch eines Verzeichnisses) eingesehen und editiert werden. Nach Eingabe neuer Werte in einem der drei Bereiche betätigen Sie die Enter-Taste, damit die Änderungen in kraft treten.

Ordner öffnen: Wählen Sie einen Ordner aus, dessen Dateien Sie öffnen möchten. Wahlweise werden auch die Dateien in untergeordneten Ordnern berücksichtigt. Sie können Dateifilter verwenden (z. B. »w*.exe;x*.dll«) und einen Editiermodus auswählen, wenn Sie WinHex nicht schon im Extra-Menü als Viewer oder In-Place-Editor eingestellt haben. Optional werden nur solche Dateien geöffnet, die einen bestimmten Text oder bestimmte Hex-Werte enthalten. In diesem Fall stehen Ihnen noch weitere Suchoptionen zur Verfügung.

Geänderte speichern: All die von WinHex geöffneten Dateien, an denen Änderungen vorgenommen wurden, werden mit ihrem aktuellen Inhalt gespeichert. Es erfolgen keine weitere Sicherheitsabfragen. Daher ist diese Funktion »mit Vorsicht zu genießen«.

Alle speichern: Sämtliche von WinHex nicht im View-Modus geöffneten Dateien werden mit ihrem aktuellen Inhalt gespeichert. Es erfolgen keine weitere Sicherheitsabfragen.

Beenden: Hier können Sie WinHex schließen. Sie erhalten noch einmal die Möglichkeit, Änderungen an Dateien und Datenträgern zu speichern.

Bearbeiten-Menü

Rückgängig: Erlaubt Ihnen, Tastatureingaben und die Anwendung sonstiger Funktionen ungeschehen zu machen. Dazu müssen die entsprechenden Optionen aktiviert sein.

Ausschneiden: Bewirkt, daß der aktuelle Block aus der Datei entfernt und in die Zwischenablage kopiert wird. Der dahinter liegende Teil der Datei wird entsprechend vorgezogen.

Block/Alles/Sektor kopieren
- normal: Kopiert den markierten Block bzw. den gesamten Dateiinhalt bzw. den aktuellen Sektor in die Zwischenablage, so daß er später wieder eingefügt werden kann.
- in neue Datei: Kopiert die Daten direkt in eine neue Datei (nicht über den Umweg Zwischenablage). Mit dieser Funktion kann man z. B. beliebige Daten von einem Datenträger schnell in Dateien umwandeln.
- Hex-Werte: Kopiert die Daten im Hexadezimal-Format in die Zwischenablage.
- Editoranzeige: Kopiert die Daten als Text so formatiert in die Zwischenablage, wie sie auch im Hex-Editor erscheinen, d. h. mit eine Offset-, einer Hex- und einer ASCII-Text-Spalte.
- C/Pascal-Quellcode: Kopiert die Daten im C-/Pascal-Quelltext-Format in die Zwischenablage.

Zwischenspeicher einfügen: Fügt den Inhalt der Zwischenablage, sofern er in einem kompatiblen Format vorliegt, an der aktuellen Cursorposition ein. Der Teil der Datei, der dahinter liegt, wird hinter die Einfügung versetzt.

Zwischenspeicher schreiben: Überträgt den Inhalt der Zwischenablage an die aktuelle Cursorposition und *überschreibt* dabei die Bytes der Datei, die dahinter folgen. Falls dabei das Dateiende erreicht wird, wird die Datei so weit wie erforderlich verlängert, damit die Daten Platz finden.

Zwischenspeicher in neue Datei schreiben: Legt eine neue Datei mit dem aktuellen Inhalt der Zwischenablage an.

Zwischenspeicher freigeben: Löscht den Inhalt der Zwischenablage gibt den von ihm genutzten Teil des Arbeitsspeichers wieder frei.

Entfernen: Löscht den aktuellen Block aus der Datei. Der hintere Teil der Datei wird dann entsprechend vorgezogen. Der gelöschte Block wird *nicht* in die Zwischenablage kopiert. Wenn in allen geöffneten Dateien der Block gleich definiert ist (also an den gleichen Offsets beginnt und endet), können Sie diese Funktion wahlweise auch auf alle geöffneten Dateien anwenden.

Nullbytes einfügen: Läßt Sie eine bestimmte Anzahl von Bytes mit dem Wert Null an der aktuellen Cursor-Position einfügen.

Block festlegen: In einem Dialogfenster kann man die Offsets einstellen, die den Beginn und das Ende des aktuellen Blocks markieren. Diese Funktion ist auch über die Statusleiste zugänglich. Sie läßt sich wahlweise auch auf alle geöffneten Dateien anwenden.

Alles auswählen: Legt den Dateianfang als Blockanfang und das Dateiende als Blockende fest.

Konvertieren

Daten modifizieren

Block/Datei/Sektoren füllen

Suchen-Menü

Text suchen: Diese Funktion sucht Vorkommen einer max. 50stelligen Zeichenfolge in der aktuellen Datei (s. a. Suchoptionen). Specialist- und forensische Lizenzen: führt direkt zur Parallelen Suche, wenn die Umschalt-Taste nicht gedrückt ist.

Hex-Werte suchen: Sucht Vorkommen einer Kombination von max. 50 jeweils zweistelligen Hex-Werten (s. a. Suchoptionen).

Text ersetzen: Diese Funktion ersetzt Vorkommen einer Zeichenfolge in der Datei durch eine andere (s. a. Ersetzen-Optionen).

Hex-Werte ersetzen: Funktioniert genau wie der Befehl »Text ersetzen«, wird aber auf eine Folge von Hex-Werten angewandt (s. a. Ersetzen-Optionen).

Kombinierte Suche: Mit dieser besonderen Funktion können Sie eine komplexe Suche durchführen: In der aktuell angezeigten und einer auf einem Datenträger bestehenden Datei wird ein gemeinsamer Offset gesucht, an dem die beiden Dateien bestimmte Daten enthalten. Wählen Sie zunächst den Hex-Wert, der in aktuellen Datei an der gesuchten Position stehen soll. Geben Sie dann den Namen der zweiten Datei und den in ihr zu suchenden Hex-Wert an. WinHex sucht nun eine Stelle, an der in jeder Datei der jeweilige Hex-Wert steht.

Ganze Zahl suchen: Geben Sie eine natürliche Zahl (in den Grenzen eines vorzeichenbehafteter 64-Bit-Integer-Wertes) an. Die Funktion sucht dann diejenigen Bytes in der Datei, die als diese Zahl interpretiert werden könnten. Ist sie fündig geworden, gibt sie den Fundort und die entsprechenden Hex-Werte an und nennt das Format, in dem die Hexadezimal-Werte der eingegebenen Zahl entsprechen (s. a. Suchoptionen).

Gleitkommazahl suchen: Geben Sie eine Dezimalzahl (z. B. 12,34 = 0,1234 * (10 hoch 2) = 0,1234E2) und den Fließkomma-Datentyp an. Die Funktion sucht dann diejenigen Bytes in der Datei, die als diese Zahl interpretiert werden könnten. Ist sie fündig geworden, gibt sie den Fundort und die entsprechenden Hex-Werte an.

Textpassagen suchen: Sucht in der Datei einen Bereich mit aufeinanderfolgenden Buchstaben (a-z, A-Z; äöüß im ANSI-ASCII-Zeichensatz), Ziffern (0-9) und/oder Satz- und Leerzeichen. Diese Funktion erfüllt zum Beispiel dann ihren Zweck, wenn Sie in einer Programmdatei den sporadisch zwischen den Steuerzeichen vorkommenden Text finden möchten.
Regeln Sie, wie »sensibel« WinHex nach Vorkommen von Text sucht, indem Sie angeben, wie lang der Text sein muß, damit er als solcher erkannt wird.
Viele Dateitypen neueren Datums, darunter 32-Bit-Programmdateien, reservieren zwei Bytes für ein Zeichen statt eins (Unicode-Zeichensatz). Die Option »Unicode-Zeichen tolerieren« bedeutet, daß auch alphanumerische ASCII-Zeichen, zwischen denen jeweils ein Byte mit dem Wert Null steht, als Text erkannt werden.

Globale Suche fortsetzen: Setzt einen bereits begonnenen globalen, d.h einen mit Option »In allen geöffneten Dateien suchen« durchgeführten Suchvorgang, nach Anzeigen einer Fundstelle in der *nächsten* Datei fort. Soll zunächst in derselben Datei noch weiter gesucht werden, muß die Funktion »Suche fortsetzen« benutzt werden.

Suche fortsetzen: Führt einen bereits begonnenen Suchvorgang, auch nach Vorkommen von Text, aber keinen Ersetzen-Vorgang, von der aktuellen Cursor-Position an fort.

Position-Menü

Offset aufsuchen: Setzt den Cursor auf einen von Ihnen gewünschten Offset, d. h. eine Position in der Datei. Gewöhnlich wird diese relativ zum Anfang der Datei (Offset 0) angegeben. Sie können den Cursor aber auch relativ von der aktuellen Position vorwärts und rückwärts und vom Dateiende aus rückwärts bewegen. Die Maßeinheit ist entweder ein Byte, ein Word (2 Bytes), ein DoubleWord (4 Bytes), ein Datensatz (wenn im Ansicht-Menü aktiv) oder ein Sektor. Verwenden Sie F11, um die gewählte Positionsveränderung zu wiederholen.

Seite/Sektor aufsuchen: Schlägt die von Ihnen angegebene Seite auf bzw. springt im Fall eines Datenträgers zum gewählten Sektor/Cluster. Bitte beachten Sie, daß der Datenbereich auf FAT-Laufwerken mit der Cluster-Nr. 2 beginnt.

FAT-Eintrag/FILE-Record aufsuchen: Erlaubt es, bequem zu einem bestimmten Eintrag in der Dateizuordnungstabelle auf einem FAT-Laufwerk bzw, zu einem bestimmten FILE-Record in der Master File Table auf einem NTFS-Laufwerk zu springen.

Block verschieben: Verschiebt die aktuelle Block-*Markierung* (nicht die *Daten* im Block) nach vorne oder hinten. Geben Sie die Distanz in Byte an. Verwenden Sie Alt+F11, um die gewählte Blockverschiebung zu wiederholen, und Shift+Alt+F11, um in die jeweils umgekehrte Richtung zu verschieben. Diese Funktion kann z. B. beim Editieren einer Datei von Nutzen sein, die aus mehreren gleichartigen Datenfeldern (Records) derselben Länge besteht.

WinHex fertigt Aufzeichnung über die Offset-Sprünge, die Sie in einem Dokument durchführen, an und erlaubt Ihnen, später innerhalb der Kette **vor** und **zurück** zu springen.

Dateianfang: Zeigt die erste Seite der Datei an und setzt den Cursor auf den Anfang der Datei (Offset 0).

Dateiende: Zeigt die letzte Seite der Datei an und setzt den Cursor auf das Ende der Datei (letztes Byte, Offset=Dateigröße-1).

Blockanfang: Setzt den Cursor auf den aktuellen Blockanfang.

Blockende: Setzt den Cursor auf das aktuellen Blockende.

Position markieren: Markiert die aktuelle Position optisch.

Markierung löschen: Löscht eine zuvor gesetzte Markierung vom Bildschirm.

Markierung aufsuchen: Setzt den Cursor auf die zuvor markierte Position.

Positions-Manager

Fenster-Menü

Fenster-Manager: Listet alle Edtierfenster auf und gibt Ihnen die Möglichkeit, schell zwischen verschiedenen Fenstern zu wechseln. Sie können im Fenster-Manager auch einzelne Fenster schließen und geänderte Dateien speichern.

Anordnung als Projekt speichern: Schreibt die gegenwärtige Fensterkonstellation in eine Projektdatei. Vom Start-Center aus können Sie das Projekt dann zu einem späteren Zeitpunkt wieder laden und die Editierpositionen in allen Dokumenten wiederherstellen lassen, um Ihre Arbeit dort fortsetzen zu können, wie Sie sie verlassen haben, oder um die Arbeit im Fall einer wiederkehrenden Aufgabe bequem aufnehmen zu können.

Alle schließen: Schließt alle geöffneten Fenster und damit alle momentan in WinHex dargestellten Dateien und Datenträger.

Ohne Abfragen schließen: Funktioniert wie »Alle schließen«, ohne Ihnen jedoch die Möglichkeit zu geben, eventuelle Änderungen zu speichern.

Übereinander/Horizontal/Vertikal: Ordnet die Editierfenster wie beschrieben an.

Minimieren: Verkleinert alle Editierfenster.

Symbole anordnen: Richtet verkleinert dargestellte Fenster ordentlich am unteren Rand des Rahmenfensters aus.

Extras-Menü

Disk öffnen

Datenträger klonen

Dateien retten nach Name

Dateien retten nach Typ

Freien Speicher initialisieren: Vertrauliche Informationen könnten durch normale Lösch- und Kopiervorgänge in momentan unbenutzten Bereichen des Datenträgers liegen. Mit dieser Funktion kann der unbenutzte Speicher eines Datenträgers aus Sicherheitsgründen initialisiert (überschrieben) werden. Dies verhindert die Wiederherstellung von Daten aus diesem Bereich des Datenträgers. *Nur in WinHex verfügbar, nicht in X-Ways Forensics.*

Schlupfspeicher initialisieren: Überschreibt Schlupfspeicher (englisch »slack space«, die unbenutzten Bytes im jeweils letzten Cluster einer Clusterkette, hinter dem tatsächlichen Ende der Datei) mit Nullbytes. Dies kann in Verbindung mit »Freien Speicher initialisieren« benutzt werden, um vertrauliche Daten auf einem Laufwerk sicher zu löschen oder um den Platzbedarf eines komprimierten Datenträger-Backups zu minimieren (z. B. einer WinHex-Sicherung). Beenden Sie vor Verwendung dieser Funktion alle laufenden oder residenten Programme, die auf den Datenträger schreiben könnten. *Nur in WinHex verfügbar, nicht in X-Ways Forensics.*

MFT-Records säubern: Auf NTFS-Laufwerken kann WinHex alle gegenwärtig unbenutzten File-Records der $Mft (Master File Table) initialisieren, da diese noch Namen und Inhaltsfragmente von Dateien enthalten können, die in ihnen gespeichert waren. *Nur in WinHex verfügbar, nicht in X-Ways Forensics.*

Clusterketten neu scannen: Verfügbar Partitionen mit einem der unterstützen Dateisysteme. WinHex durchläuft alle Clusterketten und kann dadurch für jeden Sektor/Cluster angeben, was in ihm gespeichert ist bzw. ob er unbelegt ist. Auch die vollständige Auflistung gelöschter Dateien auf NTFS-Laufwerken im Verzeichnis-Browser hängt davon ab. Durch Dateioperationen auf dem betreffenden Laufwerk veralten diese Informationen allerdings, und ein erneutes Aufrufen dieser Funktion bietet sich an. Vgl. Sicherheitsoptionen.

Verlorene Partitionen suchen: Ehemals existierende Festplatten-Partitionen, die nicht automatisch gefunden wurden, als die physische Platte (oder eine Image-Datei einer physischen Platte) geöffnet wurde, und die nicht im Zugriffsschalter-Menü aufgelistet werden, können mit diesem Befehl gefunden und entsprechend identifiziert werden. Er sucht nach Signaturen von Master Boot Records und Bootsektoren (0x55AA), optional nur ab dem ersten Sektor, der der letzten (gemäß ihrer physischen Abfolge) Partition folgt, die bereits bekannt ist, und listet die neu gefundenen Partitionen im Zugriffsschalter-Menü auf.

Als Partitionsanfang interpretieren: Wenn Sie den Anfangssektor einer (z. B. gelöschten) Partition auf einer physischen Festplatte finden, können Sie die Partition mit diesem Menübefehl einfach per Zugriffsschaltermenü zugreifbar machen. Wenn kein bekanntes Dateisystem beginnend am aktuell angezeigten Sektor erkannt wird, werden Sie gefragt, wie viele Sektoren in der neu zu definierenden Partition enthalten sein sollen.

Plattenparameter eingeben: Benutzen Sie diese Funktion für einen physischen Datenträger, um die von WinHex erkannte Zahl der Zylinder, Köpfe und Sektoren pro Spur anzupassen. Dies kann nützlich sein, um auf etwaige Überhangsektoren am Ende des Datenträgers zugreifen zu können (sofern diese von WinHex nicht automatisch erkannt werden) oder um das CHS-Koordinatensystem nach Ihren Wünschen zu ändern. Im Fall eines logischen Datenträgers können Sie die Zahl der zu erkennenden Cluster

selbsten bestimmen, was erforderlich werden kann, wenn etwa eine große DVD von Windows 9x nur als 2 GB erkannt wird.

Datei-Tools

RAM öffnen

Einsehen: Verfügbar nur mit einer forensischen Lizenz. Ruft den internen Viewer auf.

Externe Programme: Ruft eins der im Optionen-Menü eingestellten externen Programme auf (wie etwa Quick View Plus) und öffnet darin die aktuelle Datei.

X-Ways Trace aufrufen: Nur verfügbar, wenn X-Ways Trace installiert ist. Diese Software kann die index.dat-History-Datei des Internet Explorer und info2-Dateien des Windows-Papierkorbs entschlüsseln.

Rechner: Startet den Windows-Rechner für sonstige Berechnungen. Dazu muß sich die Datei »calc.exe« im Windows-Ordner befinden.

Umrechnung: Diese Funktion können Sie benutzen, um Zahlen des Hexadezimal-Systems ins Dezimal-System oder umgekehrt zu übersetzen. Nach der Eingabe der Zahl betätigen Sie die ENTER-Taste. Bitte beachten Sie die Hinweise unter »Ganzzahlige Datentypen«.

Block/Datei/Sektoren analysieren: Die Daten im aktuellen Block, in der gesamten Datei bzw. auf dem gesamten Datenträger werden statistisch ausgewertet und das Ergebnis in einem Fenster graphisch veranschaulicht. WinHex ermittelt dazu die Häufigkeiten des Vorkommens aller 256 möglichen Bytewerte und bildet sie proportional in vertikalen Linien entsprechender Länge ab. Dabei wird die Höhe des Fensters optimal genutzt, d. h. die längste Linie (die den häufigsten Bytewert repräsentiert) reicht von unten bis zur Titelleiste des Fensters. Unter der Titelleiste können Sie abhängig von der Mauscursor-Position den relativen Anteil und die absolute Anzahl eines jeden Bytewerts ablesen.
Diese Funktion kann z. B. dazu eingesetzt werden, um Datenmaterial unbekannter Art zu analysieren. Audio-Daten, komprimierte Daten, ausführbarer Code u. a. lassen sich an charakteristische Grafiken erkennen. Außerdem wird die 32-Bit-Standard-Prüfsumme (Summe aller Bytes) und der sicherere CRC32 angegeben. Im Kontextmenü des Fensters läßt sich einstellen, ob Bytes mit dem Wert Null unberücksichtigt bleiben sollen. Dies kann in vielen Fällen die Aussagekraft der Grafik stark erhöhen. Vom Kontextmenü aus können Sie das Analysefenster auch *drucken* und die Analyse in eine Textdatei exportieren.

Hash berechnen: Berechnet für die aktuelle Datei, den aktuellen Datenträger bzw. den gegenwärtig definierten Block eine der folgenden Prüfsummen/Digests: 8-Bit-, 16-Bit-, 32-Bit-, 64-Bit-Prüfsumme, CRC16, CRC32, MD5, SHA-1, SHA-256 oder PSCHF.

Hash-Datenbank

Optionen-Menü

Allgemeine Optionen

Verzeichnis-Browser-Optionen

Externe Programme: Hier geben Sie an, welche externen Programme zum Einsehen von Dateien Sie von WinHex aus (Menü Extras) aufrufen können möchten. Außerdem können Sie hier den Installationspfad der Viewer-Komponente eingeben, die bei forensischen Lizenzen für v12.05 und neuer mitgeliefert wird (standardmäßig im Unterverzeichnis ..\viewer). Die Viewer-Komponente kann gezielt aktiviert oder deaktiviert werden.

Daten-Dolmetscher-Optionen

Rückgängig-Optionen

Sicherheitsoptionen

Editier-Modus: Erlaubt es, den Editier-Modus programmweit zu bestimmen. (Das Kontextmenü der Informationsspalte erlaubt es, den Editier-Modus gezielt nur für das aktive Editierfenster zu ändern.) Editier-Modi

Vereinfachte Benutzeroberfläche: Verfügbar beim Betrieb mit einer forensischen Lizenz. Ersetzt die Standardmenüs Datei und Bearbeiten mit dem Menü, das sonst im Falldatenfenster liegt. Damit sind einige Menübefehle des Standard-Dateimenüs noch über die Symbolleiste verfügbar, das Bearbeiten-Menü als Kontextmenü.

Zeichensatz: An diesem Menüeintrag oder mit der Tastenkombination Shift+F7 kann eingestellt werden, ob für die Textdarstellung der ANSI-ASCII-, der IBM-ASCII- oder der EBCDIC-Zeichensatz verwendet wird. Wie unter Punkt »ANSI-/IBM-ASCII« erläutert, ist der ANSI-Zeichensatz bei der Bearbeitung von Windows-Dateien vorzuziehen. EBCDIC ist auf IBM-Mainframe-Rechnern gebräuchlich. EBCDIC kann in WinHex nicht zum Drucken verwendet werden.

Datei-Tools

Verketten: Diese Funktion läßt Sie eine beliebige Anzahl bestehender Dateien auswählen, die aneinandergehängt eine Zieldatei bilden.

Zerlegen: Wählen Sie eine bestehende Datei, aus der Sie mehrere neue Dateien bilden möchten. Geben Sie für jede Zieldatei den Dateinamen an und den Offset der Quelldatei, an dem die Trennung vorgenommen werden soll. Die Quelldatei bleibt durch diese Funktion unberührt.

Verschmelzen: Geben Sie die Namen zweier Quelldateien und einer Zieldatei an. Die Bytes bzw. Words der Quelldateien werden abwechselnd in die Zieldatei geschrieben (wobei das erste Byte/Word aus der ersten Quelldatei stammt). Auf diese Weise lassen sich die in getrennten Dateien enthaltenen Odd- und Even-Bytes bzw. -Words zu einer Datei zusammenfügen (z. B. in der EPROM-Programmierung).

Aufspalten: Geben Sie die Namen einer Quelldatei und zweier Zieldateien an. Die Bytes bzw. Words der Quelldatei werden abwechselnd in die Zieldateien geschrieben (wobei das erste Byte/Word in die zuerst ausgewählte Zieldatei gelangt). Auf diese Weise lassen sich Odd- und Even-Bytes bzw. -Words in zwei separate Dateien überführen (z. B. in der EPROM-Programmierung).

Vergleichen: Wählen Sie zwei Editierfenster (Dateien oder Datenträger) aus, die Sie Byte für Byte vergleichen möchten. Geben Sie außerdem den Namen der Datei an, in die der Bericht geschrieben werden soll. Bestimmen Sie, ob nach *Unterschieden* oder nach *Übereinstimmungen* gesucht werden soll. Sie geben an, wie viele Bytes verglichen werden sollen. Es ist möglich, eine Anzahl von Unterschieden/Übereinstimmungen anzugeben, bei deren Erreichen der Vergleich abgebrochen werden soll. WinHex erstellt einen Bericht in Form einer Textdatei, den Sie mit dem unter Optionen gewählten Texteditor einsehen können. Bei großen Vergleichsbereichen und vielen Unterschieden/Übereinstimmungen kann diese Textdatei sehr groß werden.
Der Vergleich beginnt an den jeweils angegebenen Offsets. Diese Offsets dürfen unterschiedlich sein, so daß z. B. das Byte an Offset 0 in Datei A mit dem Byte an Offset 32 in Datei B vergleichen wird, und das Byte an Offset 1 mit dem an Offset 33 usw. Wenn Sie Editierfenster für den Vergleich auswählen, wird die aktuelle Cursorposition automatisch hinter "Ab offset" eingetragen.
Es gibt noch eine weitere Vergleichsfunktion in WinHex: Sie können auch Editierfenster mit-ein-ander vergleichen und das Rollen in den Fenstern synchronisieren (s. Ansicht-Menü).

Sicheres Löschen: Löscht eine oder mehrere Dateien definitiv, so daß ihr Inhalt mit Datenrettungs-Programmen nicht rekonstruiert werden kann. Jede gewählte Datei wird in ihrer aktuellen Größe gemäß den Einstellungen überschrieben, auf die Länge Null gekürzt und dann gelöscht. In der Vollversion von WinHex wird zusätzlich ihr Name im Dateisystem unkenntlich gemacht. »Sicheres Löschen« eignet sich daher für Dateien mit vertraulichen Informationen, die vernichtet werden sollen. *Nur in WinHex verfügbar, nicht in X-Ways Forensics.*

Hilfe-Menü

Inhalt: Ruft die Inhaltsübersicht dieser Hilfe-Datei auf.

Setup: Läßt Sie zwischen allen verfügbaren Sprachen umschalten.

Initialisieren: Mit dieser Funktion können Sie die Voreinstellungen sämtlicher Optionen wiederherstellen. Alternativ dazu können Sie die Datei »winhex.cfg« löschen, bevor Sie WinHex starten.

Deinstallieren: Mit dieser Funktion können Sie die WinHex von Ihrer Festplatte entfernen, selbst wenn Sie nicht das Setup-Programm zur Installation verwendet haben.

Online: Lädt die WinHex-Homepage (Internet-Adresse http://www.winhex.com), das Support-Forum (http://www.winhex.net), die Wissensdatenbank (http://www.winhex.com/winhex/kb/), oder die Seite zum Abonnieren des WinHex-Newsletters in Ihrem Browser.

Info: Zeigt Informationen über WinHex an (u. a. die Programmversion und Ihren Lizenzstatus).

Drucken

Mit dieser Funktion des Datei-Menüs können Sie einen Ausschnitt aus einem Editierfenster drucken. Geben Sie den Druckbereich in Form von Offsets an. Sie haben die Möglichkeit, einen Drucker auszuwählen und ihn einzurichten.

Bestimmen Sie den Zeichensatz für den Druck, ändern Sie ggf. die vorgeschlagene Schriftgröße und tragen Sie auf Wunsch einen Kommentar, der am Ende des Ausdruckes erscheinen soll, in das dafür vorgesehene Feld ein. Die empfohlene Schriftgröße berechnet sich als Druckauflösung (z. B. 720 dpi) geteilt durch 6 (z. B. 120).

Wenn Ihnen das Drucken mit WinHex nicht flexibel genug ist, können Sie auch einen Block definieren, ihn mit »Bearbeiten->Kopieren->Editoranzeige« als Hex-Editor-formatierten Text in die Zwischenablage kopieren und in einem Textverarbeitungsprogramm weiterverwenden. Dort eignet sich dann besonders die Schriftart »Courier New«, Größe 10, zum Ausdruck auf DIN A4.

Block

Als »Block« wird ein ausgewählter Bereich bezeichnet, der für jede in WinHex geöffnete Datei festgelegt werden kann. Dieser Bereich ist Gegenstand vieler Funktionen im Bearbeiten-Menü, genau wie Markierungen in anderen Windows-Programmen. Wenn kein Block definiert ist, beziehen sich diese Funktionen gewöhnlich auf den gesamten Dateiinhalt.

Die aktuelle Lage und Größe des Blocks werden in der Statusleiste angezeigt. Durch Drücken der Escape-Taste oder durch einen Doppelklick mit der rechten Maustaste hebt man die Blockmarkierung auf.

Arbeitserleichterungen

Daten modifizieren

Mit dieser Funktion können Sie die Daten im aktuellen Block bzw. in der gesamten Datei (falls kein Block definiert ist) verändern. Entweder Sie *addieren* zu jedem Element der Daten eine Zahl, Sie *invertieren* die Bits, Sie führen eine bitweise XOR-Operation mit einer Konstanten aus (eine einfache Art der Verschlüsselung), eine OR- oder eine AND-Operation, Sie shiften Bits logisch oder Sie *vertauschen* Bytes paarweise. Durch das Shiften (Verschieben) von Bits können Sie das Einfügen oder Entfernen eines einzelnen Bits am Anfang des Blockes simulieren. Daten lassen sich auch um ganze *Bytes* verschieben (derzeit nur nach links, durch Eingabe einer negative Anzahl von Bytes). Dies ist nützlich, wenn Sie im In-Place-Modus Bytes aus einer sehr großen Datei ausschneiden möchten, was sonst die Erstellung einer ebensogroßen temporären Datei erfordern würde.

Bytes vertauschen

Vertauscht benachbarte Bytes paarweise (16-Bit-Vertauschung) oder in 4er-Gruppen (32-Bit-Vertauschung) innerhalb des aktuellen Blocks bzw. innerhalb der gesamten Datei, wenn kein Block definiert ist. Der Bereich muß dazu ein Vielfaches von 2 (16-Bit-Vertauschung) bzw. 4 (32-Bit-Vertauschung) Bytes enthalten. Mit dieser Funktion können Sie »Big-Endian«-Daten in »Little-Endian«-Daten verwandeln.

Addition

Geben Sie einen positiven oder negativen, dezimalen oder hexadezimalen Summanden an, der jedem Datenelement des Blockes hinzuaddiert werden soll. Der numerische Datentyp bestimmt Größe (1, 2 oder 4 Bytes) und Art (vorzeichenbehaftet oder vorzeichenlos) eines Elements.

Es werden zwei Möglichkeiten angeboten, wie WinHex verfahren soll, wenn durch die Addition der Wertebereich des Formats über- oder unterschritten würde. Entweder der Wertebereich wird nicht verlassen, d. h. das Maximum bzw. Minimum des Wertebereichs wird als neuer Wert angenommen (I), oder die Addition wird dennoch durchgeführt und der entstehende Übertrag ignoriert (II).

Beispiel: 8 Bit, vorzeichenlos
I. FF + 1 = FF (255 + 1 = 255)
II. FF + 1 = 00 (255 + 1 = 0)

Beispiel: 8 Bit, vorzeichenbehaftet
I. 80 - 1 = 80 (-128 - 1 = -128)
II. 80 - 1 = 7F (-128 - 1 = +127)

Hinweise:

• Bei Verwendung der ersten Methode erhalten Sie nach Abschluß der Operation eine Meldung, wie oft die Addition nicht durchgeführt werden konnte.
• Wenn Sie die zweite Methode verwenden, ist der Vorgang umkehrbar. Geben Sie einfach die Gegenzahl des zuvor benutzten Summanden bei gleichem Zahlenformat ein. Sie erhalten dann exakt die ursprünglichen Daten.
• Bei Wahl der zweiten Methode ist es egal, ob Sie ein vorzeichenbehaftetes oder vorzeichenloses Format angeben.

Konvertierungen

WinHex erlaubt es, mit dem Befehl »Konvertieren« im Bearbeiten-Menü Daten in andere Formate umzuwandeln, zu verschlüsseln und zu entschlüsseln. Die Konvertierung kann optional in allen in WinHex geöffneten Dateien statt nur in der aktuellen Datei durchgeführt werden. Die mit einem Stern gekennzeichneten Formate können nie blockweise, sondern nur dateiweise konvertiert werden. Die folgenden Formate werden unterstützt:

• ANSI-ASCII, IBM-ASCII (zwei sich teilweise unterscheidende ASCII-Zeichensätze)
• EBCDIC (ein IBM-Mainframe-Zeichensatz)
• Groß-/Kleinbuchstaben (ANSI-ASCII)
• Binär* (Rohdaten)
• Hex-ASCII* (Hexadezimal-Darstellung von Rohdaten als ASCII-Text)
• Intel-Hex* (=Extended Intellec; Hex-ASCII-Daten in einem speziellen Format, incl. Prüfsummen etc.)
• Motorola-S* (=Extended Exorcisor; dto.)
• Base64*
• UUCode*

Bitte beachten Sie:
• Beim Konvertieren von Intel-Hex oder Motorola-S in ein anderes Format werden die in den Daten enthaltenen Prüfsummen nicht auf Korrektheit überprüft.
• In Abhängigkeit von der Dateigröße wird der kleinstmögliche Subtyp in der Ausgabe verwendet: Intel-Hex: 20-Bit oder 32-Bit. Motorola-S: S1, S2 oder S3.
• Beim Konvertieren von Binär nach Intel-Hex oder Motorola-S werden nur Speicherbereiche übersetzt, die nicht mit hexadezimalen FFs gefüllt sind, um die Ergebnisdatei kompakt zu halten.

Der Befehl »Konvertieren« kann auch Rohdaten einer beliebigen Anzahl kompletter 16-Cluster-Einheiten dekomprimieren, die vom NTFS-Dateisystem komprimiert wurden.

Verschlüsselung/Entschlüsselung

Es wird empfohlen, einen Schlüssel zu verwenden, der aus mind. 8 Zeichen besteht. Widerstehen Sie der Versuchung, ein Wort aus einer belieben Sprache zu wählen. Am besten ist eine zufällige Kombination von Buchstaben, Satzzeichen und Ziffern. Beachten Sie, daß Groß- und Kleinbuchstaben unterschieden werden. Es ist unmöglich, ohne den richtigen Schlüssel die verschlüsselten Daten wiederherstellen zu können. Der zur Entschlüsselung eingegebene Schlüssel wird nicht auf Korrektheit überprüft.

Als Verschlüsselungsalgorithmus wird »Pukall Cipher 1« (PC 1) mit einem 128-Bit-Schlüssel benutzt (dem 128-Bit-Digest des von Ihnen angegebenen Schlüssels).

Suchoptionen

Groß-/Kleinschreibung beachten: Wenn diese Option gewählt ist, wird der Text immer in genau der Schreibweise gesucht, in der Sie ihn vorgeben. Z. B. wird »Beispiel« nicht bei der Vorgabe »beispiel« gefunden. Wenn Sie die Option nicht wählen, so wird WinHex selbst bei »bEIsPiEl« fündig. Auch deutsche Umlaute, die im ANSI-ASCII-Format vorliegen, sind dann in der Groß- und Kleinschreibung austauschbar, sonstige sprachspezifischen Buchstaben (çåê...) allerdings nicht.

Im Unicode-Zeichensatz suchen: Der Text wird im Unicode-Zeichensatz gesucht. Dieser Zeichensatz reserviert 16 Bit je Zeichen, wobei die ersten 256 Unicode-Zeichen den ANSI-ASCII-Zeichen entsprechen. Das höherwertige Byte ist dabei Null. In 32-Bit-Programmdateien z. B. sind Texte teilweise im Unicode-Zeichensatz gespeichert. Die parallele Suche erlaubt es, denselben Text gleichzeitig in Unicode und ASCII zu suchen. Dazu muß das Kontrollkästchen »halb« eingeschaltet sein.

Sie können ein frei wählbares **Jokerzeichen** (ein Zeichen bzw. ein zweistelliger Hex-Wert) verwenden, das genau ein Byte abdecken kann. Z. B. kann man mit der Such-Zeichenfolge »Sp?ck« sowohl »Speck« als auch »Spock« finden.

Nur ganze Wörter suchen: Die zu suchende Zeichenfolge wird nur erkannt, wenn sie als einzelnes Wort vorkommt, also von anderen Buchstaben (z. B. durch Leer- oder Steuerzeichen) getrennt ist.

Suchrichtung: Bestimmen Sie, ob von vorne bis hinten oder von der aktuellen Position an ab- oder aufwärts gesucht werden soll.

Bedingung: Offset modulo x = y: Der Suchalgorithmus erfaßt nur Vorkommnisse an Offsets, die die genannte Bedingung erfüllen. Wenn Sie bspw. Daten suchen, von denen Sie wissen, daß sie an Position 10 eines Festplatten-Sektors stehen, geben Sie x=512, y=10 an. Wenn Sie DWORD-ausgerichtete Daten suchen, verwenden Sie x=4, y=0, um irrelevante Treffer auszuschließen.

Nur im Block suchen: Es wird nur derjenige Teil der Datei/des Datenträgers/des virtuellen Speichers durchsucht, der innerhalb des Blockes liegt.

In allen geöffneten Fenstern suchen: Die Suche wird der Reihe nach in allen in WinHex offenen Editierfenstern durchgeführt. Wird WinHex in einem Fenster fündig, kann die Suche danach im selben Fenster normal fortgesetzt werden (durch F3); zum nächsten Fenster geht WinHex mit der Funktion »Globale Suche fortsetzen« (F4) über. Wenn »Nur im Block suchen« aktiviert ist, wird in jedem Fenster nur der dort festgelegte Block durchsucht.

Fundstellen zählen (und speichern): Die Anzahl der Vorkommnisse des gesuchten Texts/der gesuchten Hex-Werte in der Datei/auf dem Datenträger/im virtuellen Speicher wird ermittelt. Die Positionen der Vorkommnisse werden ggf. im Positions-Manager gespeichert, so daß sie zu einem späteren Zeitpunkt wiedergefunden und bearbeitet werden können.

Suche nach »Nicht-Treffern«: Unter »Hex-Werte suchen« können Sie einen Hex-Wert mit einem Ausrufungszeichen als Präfix angeben (z. B. !00), um WinHex das erste Byte mit einem davon *abweichenden* Wert finden zu lassen.

Suchen-Menü
Optionen des Ersetzens
Technische Hinweise

Ersetzen-Optionen

Auf Bestätigung warten: An jeder Fundstelle entscheiden Sie, ob dort ersetzt und ob der Vorgang evtl. abgebrochen werden soll.

Alles ersetzen: Alle Vorkommnisse werden automatisch ersetzt.

Groß-/Kleinschreibung beachten: Bei der Suche nach der zu ersetzenden Zeichenfolge kann nach Groß- und Kleinschreibung unterschieden werden (s. a. Suchoptionen). WinHex verwendet die Ersatz-Zeichenfolge natürlich in jedem Fall in der von Ihnen gewählten Schreibweise.

Unicode-Zeichensatz verwenden: Der Text wird im Unicode-Zeichensatz gesucht. Dieser Zeichensatz reserviert 16 Bit je Zeichen, wobei die ersten 256 Unicode-Zeichen den ANSI-ASCII-Zeichen entsprechen. Das höherwertige Byte ist dabei Null. In 32-Bit-Programmdateien beispielsweise sind Texte teilweise im Unicode-Zeichensatz gespeichert.

Sie können ein beliebiges Zeichen bzw. einen beliebigen zweistelligen Hex-Wert als **Jokerzeichen** verwenden. Z. B. kann man mit der Such-Zeichenfolge »Sp?ck« sowohl »Speck« als auch »Spock« finden.

In der Ersatz-Zeichenfolge kann das Jokerzeichen verwendet werden, um an den betreffenden Stellen das bestehende Zeichen nicht zu ändern. Auf diese Weise kann man bspw. »Huhn« und »Hahn« in einem Schritt durch »Hund« und »Hand« ersetzen (entsprechende Eingabe: »H?hn« ersetzen durch »H?nd«).
Ein Jokerzeichen, das im überstehenden Teil einer Ersatz-Zeichenfolge steht, die länger als die zugehörige Such-Zeichenfolge ist, wird selbst als Ersatz in die Datei geschrieben, da es kein bereits bestehendes Zeichen in der Datei gibt, das sich dem Jokerzeichen zuordnen läßt.

Ganze Wörter: Die zu suchende Zeichenfolge wird nur erkannt, wenn sie als einzelnes Wort vorkommt, also von anderen Buchstaben (z. B. durch Leer- oder Steuerzeichen) getrennt ist. Wenn diese Option gewählt ist, wird z. B. »Tomate« nicht in »Automaten« gefunden.

Suchrichtung: Bestimmen Sie, ob von vorne bis hinten oder von der aktuellen Position an ab- oder aufwärts ersetzt werden soll.

Nur im Block suchen: Es wird nur derjenige Teil der Datei/des virtuellen Speichers durchsucht, der innerhalb des Blockes liegt.

In allen geöffneten Dateien ersetzen: Der Vorgang wird der Reihe nach in allen von WinHex geöffneten Dateien durchgeführt (sofern sie nicht im View-Modus geöffnet wurden). Wenn »Nur im Block suchen« aktiviert ist, wird in jeder Datei nur im dort festgelegten Block ersetzt.

-

Mit WinHex sind Sie in der Lage, eine Zeichenfolge durch eine andere Zeichenfolge unterschiedlicher Länge zu ersetzen. Solche Vorgänge benötigen allerdings mehr Zeit und im Ersetzen-Modus mit Bestätigung sind die Änderungen nicht sofort sichtbar. Immer, wenn Sie diese Möglichkeit nutzen möchten, können Sie bestimmen, auf welche Art dies geschehen soll:

1. Die Dateiinhalte hinter einem Vorkommnis der Suchzeichenfolge werden entsprechend der Längendifferenz von Such- und Ersatzzeichenfolge nach vorne oder hinten verschoben. Die Größe der Datei ändert sich. Viele Arten von Dateien (darunter ausführbare Dateien) werden dadurch unbrauchbar. Es ist sogar möglich, nichts als Ersatz-Zeichenfolge anzugeben. Jedes Vorkommen der Such-Zeichenfolge wird dann aus der Datei entfernt!

2. Die Ersatzzeichenfolge wird ungeachtet ihrer Länge dort in die Datei geschrieben, wo die Suchzeichenfolge gefunden wurde. Wenn die Ersatzzeichenfolge kürzer als Suchzeichenfolge ist, bleibt der hintere Teil des Vorkommnisses der Suchzeichenfolge in der Datei unverändert. Ist die Ersatzzeichenfolge länger, werden auch noch Daten hinter dem Vorkommnis mit dem überstehenden Teil der Ersatzzeichenfolge überschrieben (sofern das Dateiende nicht erreicht ist). Die Größe der Datei bleibt unverändert

Suchen-Menü
Suchoptionen
Technische Hinweise

Rückgängig-Optionen

Für den Befehl »Rückgängig« stehen Ihnen folgende Optionen zur Auswahl:

• Bestimmen Sie, wie viele nacheinander ausgeführte Aktionen ungeschehen gemacht werden können. Wichtig: Dies hat keinen Einfluß auf die Anzahl der umkehrbaren Tastatureingaben, die nur vom Arbeitsspeicher limitiert wird.

• Um Zeit und Speicherplatz auf der Festplatte zu sparen, können Sie ein Dateigrößenlimit angeben, oberhalb dessen keine Sicherungen mehr durchgeführt werden, so daß der »Rückgängig«-Befehl nur noch nach Tastatureingaben zur Verfügung steht.

• Automatisch angelegte Sicherungen für die Benutzung durch den »Rückgängig«-Befehl werden von WinHex selbständig beim Schließen der Datei gelöscht, falls die betreffende Option voll aktiviert ist. Ist sie nur halb aktiviert, werden sie erst bei Programmende gelöscht.

• Geben Sie für alle Arten von Editiervorgängen an, ob sie rückgängig gemacht werden können.

Positions-Manager

In dem »Positions-Manager« genannten Fenster können unbegrenzt viele Datei- und Datenträger-Offsets mit Beschreibungen verwaltet werden, auch *Anmerkungen* genannt, und auch für Suchtreffer verwendet. Es ist leicht, zwischen mehreren Einträgen hin- und herzuspringen, indem Sie Strg+Links und Strg+Rechts drücken. Wenn Sie etwa in einer Datei eine markante Stelle ausfindig gemacht haben, auf die Sie evtl. später noch häufiger zurückkommen möchten, dann lohnt es sich, diese Stelle im Positions-Manager einzutragen. Sie können sie dann später schnell wiederfinden, ohne sie sich merken zu müssen. Klicken Sie auf "Neu", geben Sie den Offset und anschließend eine Beschreibung (z. B. "Hier beginnt der Datenblock!") ein. Beschreibungen dürfen bis zu 8192 Zeichen groß sein. Optional können alle Positionen, die im Positionsmanager verwaltet werden, im Datenfensterin einer von Ihnen festgelegten Farbe *hervorgehoben* werden und ihre Beschreibungen in gelben Tooltips dargestellt werden, wenn der Mauszeiger darüber bewegt wird. Sie können Positionen auch mit dem Kontextmenü des Datenfensters hinzufügen oder editieren, oder auch indem Sie im Datenfenster die mittlere Maustaste betätigen.

Klicken Sie die rechte Maustaste im Positions-Manager, um ein Kontextmenü zu erzeugen. Darin können Sie Positionen löschen, aus einer Datei laden oder in eine Datei speichern (letzteres auch als HTML). Wenn die Daten des allgemeinen Positions-Managers geändert wurden, werden sie nach dem Beenden von WinHex grundsätzlich in der Datei *WinHex.pos* im WinHex-Verzeichnis gespeichert.

Das POS-Dateiformat ist auf der WinHex-Homepage http://www.x-ways.net/winhex/ vollständig dokumentiert.

Sicherungs-Manager

In der wahlweise nach dem Erstellungszeitpunkt, dem Dateinamen oder dem Pfad geordneten Liste können Sie WinHex-Sicherungen auswählen, die Sie wiederherstellen möchten. Ein neues Editierfenster zeigt daraufhin den Datei- bzw. Sektorinhalt vom Zeitpunkt der Sicherung an.

Sie können die Sicherung wiederstellen
• in eine Temporärdatei, so daß sie erst noch gespeichert werden muß,
• sofort direkt auf den Datenträger oder
• in eine neue Datei.

Im Fall von Datenträgersektoren können Sie auch das Ziel der Wiederherstellung (Datenträger und Sektornummer) ändern. Sie können außerdem optional nur einen Teil der Sektoren aus der Sicherung extrahieren (Sektoren am Anfang einer komprimierten Sicherung können allerdings nicht übersprungen werden). Wenn die Sicherung mit einer Prüfsumme und/oder einem Digest versehen war, werden die Daten erst auf Authentizität überprüft, bevor sie direkt auf den Datenträger geschrieben werden.

Mit Hilfe des Sicherungs-Managers können Sie außerdem Sicherungen löschen, die Sie nicht mehr benötigen. Die automatisch erzeugten Sicherungsdateien für die »Rückgängig«-Funktion werden von WinHex standardmäßig selbständig gelöscht (s. u. Rückgängig-Optionen).

Die Sicherungsdateien, die vom Backup-Manager verwaltet werden, heißen »???.whx« und befinden sich in dem unter Allgemeine Optionen gewählten Ordner. An die Stelle von ??? tritt eine aus drei Ziffern bestehende eindeutige Identifikationsnummer, die im Sicherungs-Manager in der letzten Spalte angegeben ist. Eine vollständige Dokumenation des WHX-Dateiformats ist auf der WinHex-Homepage http://www.winhex.com verfügbar.

Daten-Dolmetscher

Der Daten-Dolmetscher ist ein kleines Fenster, das »Übersetzungsmöglichkeiten« für die Daten an der aktuellen Cursorposition anzeigt. In den Optionen können Sie einstellen, welche Datentypen zu berücksichtigen sind. Zur Verfügung stehen diverse ganzzahlige Datentypen (standardmäßig in dezimaler Schreibweise, optional hexadezimal oder oktal), die Bit-Darstellung eines Bytes (Binärformat), vier Gleitkomma-Datentypen, Assembler-Opcodes (Intel) und Datumstypen.

Der Dolmetscher kann alle Datentypen (außer Assembler-Opcodes) auch rückwärts wieder in Hex-Werte übersetzen. Doppelklicken Sie dazu im Daten-Dolmetscher auf die Darstellung eines Datentyps, tragen Sie den gewünschten Wert ein und bestätigen Sie mit ENTER. Daraufhin schreibt der Daten-Dolmetscher die entsprechenden Hex-Werte an der aktuellen Position in das Editierfenster.

Mit einem Klick der rechten Maustaste können Sie ein Kontextmenü im Daten-Dolmetscher aufrufen und darin einstellen, ob die ganzzahligen und Gleitkomma-Datentypen im Little- oder Big-Endian-Format übersetzt werden sollen. Sie können auch zwischen dezimaler, oktaler und hexadecimaler Integer-Darstellung wählen. Dies und eine Option zum Gruppieren von Ziffern finden Sie auch im Dialogfenster Daten-Dolmetscher-Optionen.

Hinweise:

Nicht alle Hex-Werte können in Gleitkomma-Zahlen übersetzt werden. Wenn eine Übersetzung nicht möglich ist, erscheint die Angabe NAN (»**n**ot **a** **n**umber«) im Daten-Dolmetscher.

Ebensowenig können alle Hex-Werte als Datumswerte jeden Typs übersetzt werden. Manche Datumstypen haben stark eingeschränkte gültige Wertebereiche.

Redundanzen im Befehlssatz der Intel-Prozessoren schlagen sich in mehrfach vorkommenden Opcodes und mnemonischen Abkürzungen nieder. Floating-Point-Befehle werden im Daten-Dolmetscher nur als F*** angezeigt.

Beschreibungen der den mnemonischen Abkürzungen entsprechenden Befehle können von Intel über das Internet bezogen werden. Das Dokument heißt »Intel Architecture Software Developer’s Manual Volume 2: Instruction Set Reference« und liegt im PDF-Format vor.

RAM-Editor

Im Extras-Menü finden Sie die Funktion »RAM-Editor«. Der RAM-Editor ermöglicht es, den physischen Arbeitsspeicher/RAM (nur unter Windows 2000/XP, mit Administratorrechten) und den virtuellen Arbeitsspeicher eines in der Ausführung befindlichen Programms (= eines Prozesses) direkt einzusehen. Für letzteres werden alle von dem Prozeß belegten Seiten im Arbeitspeicher als zusammenhängender Speicherbereich abgebildet. Ungenutzte (leere oder nur reservierte) Blöcke im Speicher werden von WinHex standardmäßig ignoriert, optional aber mit erfaßt und mittels »?«-Zeichen angezeigt. Ohne diese Lücken können Sie in Dateien geschriebene Speicherdumps exakt miteinander vergleichen (absolute und virtuelle Adressen sind identisch), um etwa den Stack oder Heap zu beobachten oder Computerviren zu verfolgen.

Wählen Sie zunächst aus einer Liste aller laufenden Prozesse den zu untersuchenden Prozeß aus. Sie können entweder auf den sog. Primärspeicher oder den Gesamtspeicher eines Prozesses oder auf einzelne von diesem Prozeß geladene Module zugreifen. Unter Windows 95/98/Me werden Systemmodule optional augelistet. Als Systemmodule werden diejenigen Module bezeichnet, die stets oberhalb von 2 GB geladen werden (wie z. B. kernel32.dll, gdi32.dll usw.). Als Primärspeicher wird derjenige Bereich bezeichnet, den Programme vorrangig für verschiedenste Zwecke nutzen. Zumindest das Hauptmodul eines Prozesses (die EXE-Datei) ist i. d. R. ebenfalls im Primärspeicher enthalten. Der Gesamtspeicher umfaßt den gesamten virtuellen Speicher eines Prozesses einschließlich dem gemeinsamen Speicherbereich aller Prozesse, bis auf die Systemmodule.

Bitte beachten Sie die folgenden Einschränkungen:

• Vorsicht: Rückgängig gemacht werden können *ausschließlich* Tastatureingaben!
• Der virtuelle Arbeitsspeicher von 16-Bit-Prozessen kann unter Windows 95/98/Me nur unvollständig, unter NT gar nicht erfaßt werden.
• Das Editieren ist nur im In-Place-Editiermodus möglich.
• Systemmodule von Windows 95/98/Me können nur im View-Modus *eingesehen*, nicht editiert werden.
• Die Demo-Version erlaubt generell nur den View-Modus! Bestellen Sie die Vollversion.

Beachten Sie bitte die Optionen »Auf Änderungen im Speicher prüfen« (Sicherheitsoptionen) und »Virtuelle Adressen« (Allgemeine Optionen).

Kontextmenü

Das Kontextmenü sehen Sie, wenn Sie im Windows-Explorer oder auf dem Desktop ein Objekt mit der rechten Maustaste anklicken. WinHex erscheint im Kontextmenü nur, wenn die entsprechenden Optionen eingeschaltet sind.

Editieren mit WinHex: Öffnet die gewählte Datei in WinHex.

Ordner in WinHex öffnen: Läßt Sie alle Dateien des gewählten Ordners in WinHex öffnen (wie „Ordner öffnen" im Datei-Menü)

Datenträger editieren: Öffnet den gewählten Datenträger im Disk-Editor von WinHex. Wenn Sie die Shift-Taste gedrückt halten, wird statt des logischen Laufwerks der zugehörige physische Datenträger geöffnet (letzteres nur unter Windows 95/98).

WinHex stellt in der Statusleiste, im Daten-Dolmetscher und im Positions-Manager eigene Kontextmenüs zur Verfügung.

Schlüssel

Als Schlüssel geben Sie eine Zeichenfolge aus 1-16 Zeichen ein. Je mehr Zeichen Sie eingeben, umso sicherer ist die Verschlüsselung. Der Schlüssel wird nicht direkt für Ver- und Entschlüsselung benutzt, sondern ist nur Datenmaterial für einen Digest. Er wird nicht auf der Festplatte gespeichert. Fall die entsprechende Sicherheitsoption gewählt ist, wird er in verschlüsselter Form im Arbeitsspeicher gehalten, solange WinHex läuft.

Datenträger-Sicherung/Sicherung anlegen

Dieser Befehl im Datei-Menü erlaubt es, eine Sicherung/ein Image des geöffneten Datenträgers bzw. der geöffneten Datei anzufertigen. Drei verschiedene Ausgabeformate mit jeweils besonderen Vorteilen stehen zur Auswahl.

Dateiformat:	WinHex-Backup	Evidence-File	Roh-Image
Dateiendung:	.whx	.e01	z.B. .dd
Interpretierbar:	nein	ja	ja
In Segmente aufteilbar:	ja	ja	ja
Komprimierbar:	ja	ja	nein
Verschlüsselbar:	ja	nein	nein
Optionaler Hash:	integriert	integriert	separate Text-Datei
Optionale Beschreibung:	integriert	integriert	nein
Nur bestimmte Sektoren:	ja	nein	nein
Auf Dateien anwendbar:	ja	nein	nein
Automat. Verwaltung:	Sicherungs-Mngr.	nein	nein
Kompatibilität:	nein	(ja)	ja
Benötigte Lizenzart:	keine	forensisch	privat

Die große Vorteil von Evidence-Files und Roh-Images ist es, daß sie von WinHex wie die Original-Datenträger interpretiert werden können (mit dem entsprechenden Befehl im Specialist-Menü). Daher sind sie auch geeignet für den Gebrauch als Asservate in Ihren Fällen. Evidence-Files sind im besonderen Maße prädestiniert dafür, da sie auch eine optionale Beschreibung einen integrierten Hash für spätere Verifizierung enthalten können. Roh-Images sind weit verbreitet und können leicht zwischen verschiedenen forensischen Tools ausgetauscht werden. Alle Ausgabe-Formate erlauben das Splitten in Segmente einer benutzerdefinierten Größe. Eine Segmentgröße von 650 MB z. B. ist geeignet zum Archivieren auf CD-Rs. Evidence-Files *müssen* bei maximal 2025 MB gesplittet werden.

Hinweise zu Disk-Cloning & -Imaging

Wenn Sie den Namen eines WinHex-Backups automatisch vergeben lassen (Format »???.whx«), wird sie im Verzeichnis für Sicherungsdateien erstellt (s. Allgemeine Optionen), mit dem nächsten freien Namen, der der Konvention des Sicherungsmanagers entspricht (*xxx*.whx). Bei Bedarf kann das Original dann mit dem Sicherungsmanager wiederhergestellt werden. Wenn Sie selbst Dateinamen und Pfad angeben, kann die WHX-Datei immer noch mit dem Menübefehl »Sicherung laden« wiederhergestellt werden, und im Fall von aufgeteilten Sicherungen hängt WinHex automatisch die Teilsicherungsnummerm an die Dateinamen an.

Als Verschlüsselungsalgorithmus wird »Pukall Cipher 1« (PC 1) mit einem 128-Bit-Schlüssel benutzt. Der 128-Bit-Schlüssel ist der Digest aus der 256-Bit-Konkatenation, die aus dem 128-Bit-Digest des von Ihnen angegebenen Schlüssels und einer 128-bittigen Zufallszahl besteht. Die 128-bittige Zufallszahl wird in der WHX-Datei für die Entschlüsselung gespeichert.

Zum Komprimieren wird der verbreitete Deflate-Algorithmus der zlib-Bibliothek verwendet. Er basiert auf LZ77-Kompression und Huffman-Codierung. Die Kompressionsrate ist dieselbe wie bei der ZIP-Komprimierung. Das WHX-Dateiformat ist vollständig dokumentiert (s. WinHex-Homepage http://www.x-ways.net/winhex/).

Es scheint, Sie sind berechtigt, diese Version als kostenloses Update zu erhalten. Allerdings kann diese Version nicht mit der vorhandenen Lizenzdatei "user.txt" freigeschaltet werden. Weitere Informationen erhalten Sie unter http://www.x-ways.net/winhex/upgrade-d.html durch Eingabe Ihrer registrierten E-Mail-Adresse.

Digests

Ein »Digest« (engl.) ist ähnlich einer Prüfsumme eine Kennzahl zur eindeutigen Identifizierung von Daten. Digests sind aber mehr als Prüfsummen. Es handelt sich um »starke« Einweg-Hashcodes, die Datenintegrität mit extrem hoher Sicherheit garantieren. Daten können mit computerunterstütztem Rechenaufwand in bösartiger Absicht so manipuliert werden, daß ihre Prüfsumme trotz Änderung gleich bleibt. Dies kann fälschlicherweise zu der Annahme verleiten, die Daten seien noch im Originalzustand. Diese Möglichkeit schließen Digests aus. Es lassen sich mit vorstellbarem computerunterstütztem Rechenaufwand keine Daten finden, die denselben Digest besitzen wie vorgegebene andere Daten.

Natürlich können durch Verwendung von Digests auch zufällige, etwa durch fehlerhafte Übertragung entstandene Datenveränderungen festgestellt werden, aber dafür reichen Prüfsummen aus, die viel schneller berechnet werden können.

WinHex beherrscht den 128 Bit großen MD5 Message-Digest, SHA-1, SHA-256 und PSCHF (Pukall Stream Cipher Hash Function).

Sicherheitsoptionen

• »**Caching beim Lesen von Sektoren**« beschleunigt den sequentiellen Datenträgerzugriff mit dem Disk-Editor. Diese Option empfiehlt sich insbes. beim Durchsehen von CD-ROM- und Disketten-Sektoren, da sie die Zahl der erforderlichen physischen Zugriffe stark herabsetzt.

• Die Option »**Clusterketten automatisch einlesen**« sorgt dafür, daß WinHex die Cluster eines FAT-, NTFS-, Ext2/3- oder CDFS-Laufwerks selbständig untersucht, wenn ein solches Laufwerk geöffnet wird und die benötigten Informationen noch nicht vorliegen. Dadurch kann WinHex anzeigen, wofür Sektoren/Cluster verwendet werden. Benutzen Sie die Funktion »Cluster inspizieren« im Extras-Menü, um diese Informationen zu aktualisieren.

• Wenn die Option »**Daten über Clusterketten speichern**« eingeschaltet ist, bleiben die Informationen, die WinHex über die Clusterketten von FAT-, NTFS-, Ext2/3- und CDFS-Laufwerken gesammelt hat, beim Beenden von WinHex im Ordner für temporäre Dateien erhalten. WinHex kann sie dann beim nächsten Programmstart wiederverwenden.

• Die Option »**Auf Änderungen im Speicher prüfen**« betrifft den RAM-Editor. Sie sorgt dafür, daß WinHex vor jedem Lesen und Beschreiben des virtuellen Speichers erst prüft, ob sich dessen Größe und Zusammensetzung geändert hat. Ist dies der Fall, wird der Speicher in WinHex neu abgebildet und damit ein möglicher Lesefehler vermieden. Besonders unter Windows NT kann diese Einstellung den RAM-Editor stark verlangsamen. Beim Editieren des *Gesamtspeichers* eines Prozesses wird unabhängig von der gewählten Einstellung nicht auf Änderungen geprüft.

• Auf Wunsch wird beim Öffnen einer Datei **auto**matisch der **Hash berechnet** und in der Informationsspalte rechts angezeigt. Prüfsummen und Digests können auch im Extras-Menü berechnet werden.

• In der Voreinstellung müssen Sie das **Speichern von** Änderungen an existierenden **Dateien bestätigen**. Wenn Sie diese Option ausschalten, entfällt die Sicherheitsabfrage.

• Beim manuellen Wiederherstellen von Sicherungen wird ein Bericht i. d. R. nur dann angezeigt, wenn die Sicherungsdatei einen Digest enthält oder fehlerhaft ist. Sie können sich jedoch auch grundsätzlich einen **Bericht anzeigen** lassen. Wenn diese Option gewählt ist, wird Ihnen auch der Digest angezeigt.

• Den für Verschlüsselung und Entschlüsselung erforderliche **Schlüssel** können Sie entweder in ein normales Editierfeld **eingeben** oder **blind** (es erscheinen nur Sternchen). In letzterem Fall müssen Sie den Schlüssel bestätigen, um Eingabefehler zu vermeiden.

• Standardmäßig wird der **Schlüssel** selbst verschlüsselt **im** Arbeits**speicher** ge**halten**, solange WinHex läuft, damit Sie ihn nicht mehrmals eingeben müssen, wenn Sie ihn mehrmals verwenden möchten. Möglicherweise ziehen Sie es aber vor, daß WinHex sich den Schlüssel **nicht** merkt.

• Entscheiden Sie, ob Sie WinHex **vor dem Ausführen von Scripten fragen** soll, oder auch nur vor dem Ausführen von Scripten per Befehlszeile.

Byte-Reihenfolge (Endian-ness)

Mikroprozessoren unterscheiden sich darin, an welcher Position sie das niederwertigste Bytes innerhalb eines Datentyps, der mehrere Bytes enthält, ablegen. In Systemen mit Prozessoren von Intel®, MIPS®, National Semiconductors und VAX steht das niederwertigsten Byte an erster Stelle. Daten eines aus mehreren Bytes bestehender Datentyps (z. B. 32-Bit-Integertyp, Unicode-Zeichen) stehen im Speicher beginnend mit dem niederwertigsten (»little end«) und endend mit dem höherwertigstem Bytes. Zum Beispiel wird die Hexadezimalzahl 12345678 als 78 56 34 12 gespeichert. Dies wird das **Little-Endian**-Format genannt.

Motorola- und Sparc-Prozessoren dagegen setzen voraus, daß das niederwertigste Byte an hinterster Stelle steht. Mehrfach-Byte-Daten werden beginnend mit dem höchstwertigen Byte (»big end«) und endend mit dem niederstwertigem Byte gespeichert. Zum Beispiel wird die Hexadezimalzahl 12345678 als 12 34 56 78 gespeichert. Dies wird das **Big-Endian**-Format genannt.

Datumstypen

Die folgenden Datumsformate werden vom Daten-Dolmetscher unterstützt.

MS-DOS Datum & Zeit (4 Bytes)

Das niederwertige Word bestimmt die Zeit, das höherwertige das Datum. Wird von zahlreichen DOS-Funktionen und von allen FAT-Dateisystemen benutzt.

Bits	Inhalt
0-4	Sekunden geteilt durch 2
5-10	Minuten (0-59)
11-15	Stunde (0-23)
16-20	Tag (1-31)
21-24	Monat (1=Januar, 2=Februar usw.)
25-31	Jahre seit 1980

Win32 FILETIME (8 Bytes)

Ein ganzzahliger 64-Bit-Wert, der die Anzahl der seit dem 1. Januar 1601 vergangenen 100-Nanosekunden-Intervalle angibt. Wird in der Win32-API benutzt.

OLE 2.0 Datum & Uhrzeit (8 Bytes)

Ein Gleitkommawert (double), dessen ganzzahliger Bestandteil die Zahl der seit dem 30. Dezember 1899 vergangenen Tage angibt (Datum). Der Bruchanteil wird als die Uhrzeit interpretiert (z. B. 1/4 = 6:00 Uhr). Dies ist der OLE-2.0-Standarddatumstyp. Er wird bspw. auch von MS Excel verwendet.

ANSI SQL Datum & Uhrzeit (8 Bytes)

Zwei aufeinanderfolgende ganzzahlige 32-Bit-Werte. Der erste gibt die Anzahl der seit dem 17. November 1858 vergangenen Tage an (Datum). Der zweite bestimmt die Anzahl der seit Mitternacht vergangenen 100-Mikrosekunden-Intervalle (Uhrzeit). Dieser Datumstyp ist ANSI-SQL-Standard und wird in Datenbanken verwendet (u. a. in InterBase 6.0).

UNIX/C/FORTRAN Datum & Uhrzeit (4 Bytes)

Ein ganzzahliger 32-Bit-Wert, der die Anzahl der seit dem 1. Januar 1970 vergangenen Sekunden angibt. Dieser Datumstyp wird bzw. wurde in UNIX, in C und C++ (»time_t«) sowie in FORTRAN-Programmen in den 80er Jahren verwendet. Gelegentlich ist er auch definiert als die Anzahl der seit dem 1. Januar 1970 vergangenen *Minuten*. In den Optionen des Daten-Dolmetschers läßt sich die verwendete Zeiteinheit einstellen.

Java Datum & Uhrzeit (8 Bytes)

Ein ganzzahliger 64-Bit-Wert, der die Anzahl der seit dem 1. Januar 1970 vergangenen Millisekunden angibt. Wird, wie bei Java üblich, generell im Big-Endian-Format gespeichert.

Master-Boot-Record

Der **Master-Boot-Record** befindet sich am physischen Anfang einer Festplatte (editierbar mit dem Disk-Editor). Er besteht aus einem 446 Bytes langen **Master-Bootstrap-Loader-Code** und vier aufeinanderfolgenden, identisch aufgebauten **Partitions-Records**. Abschließend folgt die Hexadezimal-Signatur 55AA, die einen gültigen Master-Boot-Record kennzeichnet.

Das Format eines Partitions-Record sieht wie folgt aus:

Offset	Größe	Beschreibung
0	8 Bit	Der Hexadezimal-Wert 80 kennzeichnet eine aktive Partition.
1	8 Bit	Startkopf der Partition
2	8 Bit	Startsektor der Partition (Bits 0-5)
3	8 Bit	Startspur der Partition (Bits 8, 9 in "Startsektor" als Bits 6, 7)
4	8 Bit	Betriebssystem-Kennung (s. u.)
5	8 Bit	Endkopf der Partition
6	8 Bit	Endsektor der Partition (Bits 0-5)
7	8 Bit	Endspur der Partition (Bits 8, 9 in "Endsektor" als Bits 6, 7)
8	32 Bit	Anzahl der Sektoren vor der Partition
C	32 Bit	Anzahl der Sektoren der Partition

Betriebssystem-Kennungen (Auswahl):
(hexadezimal)

00 Leerer Partitionstabellen-Eintrag
01 DOS FAT12
04 DOS FAT16 (max. 32 MB)
05 DOS 3.3+ erweiterte Partition
06 DOS 3.31+ FAT16 (> 32 MB)
07 OS/2 HPFS, Windows NT NTFS, Advanced Unix
08 OS/2 v1.0-1.3, AIX bootable partition, SplitDrive
09 AIX Datenpartition
0A OS/2 Boot Manager
0B Windows 95+ FAT32
0C Windows 95+ FAT32 (LBA-Modus INT 13 Erweiterungen verwendend)
0E DOS FAT16 (> 32 MB, INT 13 Erweiterungen verwendend)
0F Erweiterte Partition (INT 13 Erweiterungen verwendend)
17 Versteckte NTFS-Partition
1B Versteckte Windows 95 FAT32-Partition
1C Versteckte Windows 95 FAT32-Partition (LBA-Modus INT 13 Erweiterungen verwendend)
1E Versteckte LBA VFAT-Partition
42 Dynamic disk volume
50 OnTrack Disk Manager, schreibgeschützte Partition
51 OnTrack Disk Manager
81 Linux
82 Linux Swap-Partition, Solaris (Unix)
83 Linux natives Dateisystem (ext2fs/xiafs)
85 Linux EXT
86 FAT16 Volume/Stripe-Set (Windows NT)
87 HPFS fehlertolerante, gespiegelte Partition, NTFS Volume/Stripe-Set
BE Solaris Boot-Partition
C0 DR-DOS/Novell DOS gesicherte Partition
C6 FAT16 Volume/Stripe-Set (Windows NT), "corrupted"
C7 NTFS Volume/Stripe-Set, "corrupted"

F2 DOS 3.3+ Sekundärpartition

Löschen und Initialisieren

Zum sicheren Löschen (Schreddern) von Daten, aber auch zum einfachen Füllen von Dateien oder Datenträgersektoren mit bestimmten Byte-Werten, bietet WinHex folgende Optionen an:

Füllen mit Hex-Werten: Geben Sie entweder 1, 2, 3, 4, 5, 6, 12, 15 oder 16 jeweils zweistellige Hex-Werte an, die aneinandergehängt in den aktuellen Block bzw. in die Datei kopiert werden.

Erzeugung zufälliger Bytes: Geben Sie ein Intervall innerhalb von 0-255 (dezimal) an, aus dem zufällig jedem einzelnen Byte des aktuellen Blocks bzw. des gesamten Dateiinhalts ein Wert zugeordnet wird. Jeder Wert aus dem Intervall wird mit gleicher Wahrscheinlichkeit ausgewählt.

Auf Wunsch kann diese Funktion **in allen geöffneten Dateien** ausgeführt werden. Dazu muß in allen Dateien entweder ein Block definiert oder in allen Dateien *kein* Block definiert sein.

Um die Sicherheit zu maximieren, wenn Sie Schlupfspeicher, freien Speicher, unbenutzte NTFS-Records oder ganze Datenträger permanent löschen möchten, können Sie mehr als einen Durchlauf (bis zu drei) zum Überschreiben einstellen.

Gemäß der sogenannten Clearing and Sanitization Matrix, dem im Betriebshandbuch 5220.22-M des U.S.-Verteidigungsministeriums (Department of Defense, DoD) beschriebenen Standard, Methode "c", kann eine Festplatte oder eine Diskette gelöscht werden, indem alle adressierbaren Adressen mit einem einzelnen Zeichen (einmal) überschrieben werden. Üblicherweise ist dies der Hexadezimalwert 0x00, kann aber auch jeder andere Wert sein. Um Festplatten so sicher zu löschen, daß sie bedenkenlos an andere Personen/Abteilungen/Organizationen weitergegeben werden können ("sanitizing"), müssen gemäß Methode "d" alle adressierbaren Bytes mit einem Zeichen, dann seinem Komplement und schließlich einem Zufallswert überschrieben und muß anschließend überprüft werden. (Diese Methode ist vom DoD nicht für das Saniziting von Datenträgern mit *Top*-Secret-Informationen freigegeben worden.)

Der "DoD"-Schalter konfiguriert WinHex für das Sanitizing, so daß erst mit 0x55 (binär 01010101), dann mit dem Komplement (0xAA = 10101010) und schließlich mit einem zufälligen Byte-Wert überschrieben wird.

Der "0x00"-Schalter konfiguriert WinHex für eine einfache Initialisierung, also einmaliges Schreiben von Nullbytes.

Disk-Editor Fragen & Antworten

Wie kann ich auf CD-RW-Sektoren zugreifen?

DirectCD und PacketCD dürfen auf dem Windows-System nicht installiert worden sein.

Wie kann ich auf CD-ROM- und DVD-Sektoren unter Windows 9x zugreifen?

1. Es muß ein Windows-Treiber für das CD-ROM-Laufwerk installiert sein. Ein MS-DOS-Treiber genügt nicht.
2. Es muß eine ASPI-Schnittstelle installiert sein. Ggf. müssen Sie die Datei wnaspi32.dll von Hand in Ihr Windows\System-Verzeichnis kopieren. Die Datei befindet sich auf Ihrer Windows-Installations-CD. Zum Extrahieren aus einem CAB-Archiv empfiehlt sich das Shareware-Programm WinZip (erhältlich von http://www.winzip.com).
3. Das CD-ROM-Laufwerk muß die von WinHex benutzte Zugriffsart unterstützen. Dies ist bei den meisten heutigen ATAPI- und SCSI-Laufwerken der Fall.

Was muß ich tun, damit WinHex eine installierte PC Card ATA Flash Disk bzw. ein PCMCIA-Laufwerk als physischen Datenträger unter Windows 9x anzeigt?

Windows-Systemsteuerung -> System -> Gerätemanager -> Wählen Sie das PCMCIA-Laufwerk -> Klicken Sie auf „Eigenschaften" -> Suchen Sie nach einer Option namens "Interrupt 13 Gerät" o. ä. Je nach Windows-Version kann das Auswahlfeld auch in einem anderen Bereich zu finden sein. Wenn möglich, schalten Sie diese Option *ein* und starten Sie Ihren Computer neu.

Editieren mit Schablonen

Eine Schablone ("Template") ist ein Dialogfenster, das die Mittel zum Editieren maßgeschneiderter Datenstrukturen zur Verfügung stellt. Im Vergleich zum reinen Hex-Editieren ist das Editieren mit Schablonen komfortabler und weniger fehleranfällig. Hier werden Änderungen in getrennten Editierfeldern vorgenommen und mit der ENTER-Taste bestätigt (oder beim Schließen der Schablone). Die zu editierenden Daten können von einer Datei, von Datenträger-Sektoren oder aus dem virtuellen Arbeitsspeicher stammen. Insbesondere beim Editieren von Datenbanken empfiehlt sich das Benutzen von Schablonen aufgrund des leichteren Datenzugriffs. Sie finden den Befehl zum *Drucken* einer Schablone im Systemmenü.

Eine Schablonen-Definition wird als Textdatei gespeichert. Der Schablonen-Editor ermöglicht es Ihnen, solche Definitionen zu verfassen und deren Syntax zu prüfen. Eine Schablonen-Definition enthält hauptsächlich Variablen-Deklarationen, ähnlich wie die in Programmiersprachen. Die Syntax finden Sie hier erläutert. Zu den unterstützten Datentypen gehören alle geläufigen Integer-, Gleitkomma- und Boolean-Varianten, Datumstypen, Hex-Werte, Binärwerte, Zeichen und Strings. Man kann Arrays (Felder) sowohl von einzelnen Variablen als auch von ganzen Blöcken definieren.

Die Möglichkeit, beim Interpretieren von Daten mit einer Schablone die aktuelle Position frei zu bestimmen machen das Editieren mit Schablonen besonders flexibel:
• Dieselbe Variable kann in Form von unterschiedlichen Typen interpretiert und manipuliert werden.
• Irrelevante Datenbereiche können übersprungen werden.

Der Schablonen-Manager listet alle Textdateien im WinHex-Verzeichnis, die Schablonen-Definitionen enthalten, auf. Er zeigt die Bezeichnung der Schablone, eine Beschreibung, den Dateinamen und den Zeitpunkt der letzten Änderung an. Klicken Sie auf den „Anwenden"-Schalter, um unter Verwendung der ausgewählten Schablonen-Definition eine Schablone zum Editieren der Daten im aktuellen Editorfenster an der aktuellen Position anzuzeigen. Sie können im Schablonen-Manager auch neue Definitionen erstellen oder vorhandene Definitionen löschen oder mit dem Schablonen-Editor bearbeiten.

WinHex ist werkseitig mit mehreren Beispiel-Schablonen ausgestattet.

Schablonen-Definition

Eine Schablonen-Definition besteht aus einem Kopf und einem Rumpf.

Syntax des Kopfes
Variablen-Deklarationen im Rumpf
Fortgeschrittene Befehle im Rumpf

Schablonen-Definition: Kopf

Der Kopf einer Schablonen-Definition hat das folgende Format. Die Ausdrücke in Klammern sind optional. Die Reihenfolge der Ausdrücke ist nicht von Bedeutung.

template "*Titel*"
[description "*Beschreibung*"]
[applies_to (file/disk/RAM)]
[fixed_start *Offset*]
[sector-aligned]
[requires *Offset* "*Hex-Werte*"]
[big-endian]
[hexadecimal/octal]
[read-only]
[multiple [*fixe Gesamtgröße*]]
// *Hier ist Platz für allgemeine Kommentare*.
begin
    Variablen-Deklarationen
end

Ausdrücke müssen nur in Hochkommata eingeschlossen werden, wenn sie Leerzeichen enthalten. Kommentare dürfen überall in einer Schablonen-Definition auftauchen; Zeichen, die einem doppelten Schrägstrich folgen, werden vom Parser ignoriert.

Dem Schlüsselwort "applies_to" muß genau eins der Wörter file, disk oder RAM folgen. WinHex gibt eine Warnmeldung aus, wenn Sie eine auf diese Weise gekennzeichnete Schablone auf Daten von einer anderen Quelle anwenden.

Während standardmäßig die Schablone beim Starten die Daten an der aktuellen Cursor-Position interpretiert, sorgt die optionale Anweisung "fixed_start" dafür, daß dies am angegebenen absoluten Offset der Datei bzw. des Datenträgers geschieht.

Wendet man eine Schablone auf einen Datenträger an, so stellt das Schlüsselwort "sector-aligned" sicher, daß sie ungeachtet der exakten Cursor-Position auf den Anfang des aktuellen Sektors bezogen wird.

Ähnlich wie ein "applies_to"-Ausdruck ermöglicht es die "requires"-Anweisung WinHex, eine unabsichtliche Anwendung einer Schablonen-Definition auf nicht auf sie passende Daten zu verhindern. Geben Sie hinter "requires" einen Offset und eine Hex-Wert-Kette beliebiger Länge an. Dies soll die Daten, für die die Schablone konzipiert wurde, identifizieren. Zum Beispiel läßt sich ein gültig Master-Boot-Record an den Hex-Werten 55 AA an Offset 0x1FE erkennen, eine ausführbare Datei an den Hex-Werten 4D 5A ("MZ") an Offset 0x0. Es dürfen mehrere "requires"-Anweisungen im Definitionskopf vorkommen, die alle berücksichtigt werden.

Das Schlüsselwort "big-endian" sorgt dafür, daß alle aus mehreren Bytes bestehende Integer- und Boolean-Variablen in Big-Endian-Reihenfolge gelesen und geschrieben werden (höchst-wertiges Byte vorn).

Das Schlüsselwort "hexadecimal" bewirkt, daß Integer-Variablen innerhalb der Schablonen-Definition in hexadezimaler Schreibweise angezeigt werden.

Das Schlüsselwort "read-only" stellt sicher, daß die Schablone nur benutzt werden kann, um Datenstrukturen einzusehen, nicht um sie zu manipulieren. Die Editierfelder der Schablone erscheinen dann grau.

Wenn das Schlüsselwort "multiple" im Definitionskopf angegeben wird, erlaubt WinHex das Wechseln zu benachbarten Datensätzen derselben Struktur. Das erfordert, daß WinHex die Größe eines Datensatzes kennt. Sofern diese nicht fest als Parameter der "multiple"-Anweisung angegeben wurde, nimmt WinHex an, daß die Gesamtgröße sich berechnet als die aktuelle Position nach der Anwendung der Schablonen-Definition minus Startposition. Wenn dies eine variable Größe ergibt, d. h. Array-Größen oder "move"-Parameter sich dynamisch aus den Werten von Variablen bestimmen, kann WinHex nicht zu vorgelagerten Datensätzen wechseln.

Variablen-Deklarationen

Der Rumpf eine Schablonen-Definition besteht im wesentlichen aus Variablen-Deklarationen, ähnlich wie die in Programmiersprachen. Eine Deklaration hat folgende Gestalt:

type "Bezeichnung"

wobei type einer der folgenden Datentypen sein kann:

• int8, uint8 = byte, int16, uint16, in24, uint24, int32, uint32, int64,
• uint_flex
• binary,
• float = single, real, double, longdouble = extended,
• char, char16, string, string16,
• zstring, zstring16,
• boole8 = boolean, boole16, boole32
• hex,
• DOSDateTime, FileTime, OLEDateTime, SQLDateTime, UNIXDateTime = time_t, JavaDateTime

Die Bezeichnung der Variablen muß nur dann in Hochkammata gesetzt werden, wenn sie Leerzeichen enthält. Sie darf nicht nur aus Ziffern bestehen. WinHex unterscheidet nicht zwischen Groß- und Kleinschreibung. Maximal werden zur Identifikation einer Variablen 41 Zeichen verwendet.

type kann jeweils maximal ein Modifikator der folgenden Modifikatorengruppen vorangestellt werden:

big-endian	little-endian	(s. Endian-ness)
hexadecimal	decimal	octal
read-only	read-write	

Diese Modifikatoren wirken sich nur auf die unmittelbar folgende Variable aus. Sie sind redundant, wenn sie bereits im Definition-Kopf angegeben werden.

Die Nummern am Ende der Typnamen bezeichnet die Größe einer Variablen dieses Typs (Strings: eines Zeichens) in Bits. Mit den Typen "char16" und "string16" unterstützt WinHex Unicode-Zeichen und -Strings. Höhere Unicode-Zeichen als die ersten 256 ANSI-äquivalenten werden allerdings nicht unterstützt. Es können außerdem maximal Strings einer Größe von 8192 Bytes editiert werden.

Die Typen "string", "string16" und "hex" erfordern einen zusätzlichen Parameter, der die Anzahl der Elemente angibt. Dieser Parameter kann eine Konstante oder eine zuvor deklarierte Variable sein. Wenn es sich um eine Konstante handelt, kann sie entweder dezimal oder hexadezimal geschrieben werden, im zweiten Fall muß ihr "0x" vorangestellt werden.

Sie können Arrays (Felder) deklarieren, indem Sie in eckigen Klammern die gewünschte Größe angeben, entweder hinter der Typangabe oder hinter der Variablenbezeichnung. Geben Sie "unlimited" als Array-Größe an, hört die Schablone mit dem Auslesen der Daten erst auf, wenn das Dateiende erreicht wird. Bspw. deklarieren die folgenden zwei Zeilen einen ASCII-String, dessen Länge dynamisch von der vorherigen Variable bestimmt wird:

```
uint8          "Länge"
char[Länge]"Ein String"
```

Dasselbe Ergebnis könnte mit folgenden zwei Deklarationen erzielt werden:

```
byte           "Länge"
```

string Länge "Ein String"

Eine Tilde ("~") kann als Platzhalter eingesetzt werden, um zur Laufzeit mit der tatsächlichen Array-Elementnummer ersetzt werden (s. u. Fortgeschrittene Befehle). Dies trifft nicht auf Arrays des Typs char zu, da diese von WinHex automatisch in einen String übersetzt werden.

Numerische Parameter für string-, string16- und hex-Variablen ebenso wie die Größenangaben von Arrays dürfen in mathematischer Notation angegeben werden. Sie werden vom integrierten Formel-Parser verarbeitet. Solche Ausdrücke müssen in Klammern angegeben werden. Sie dürfen keine Leerzeichen enthalten. Sie dürfen zuvor deklarierte Integer-Variablen verwenden, deren Namen selbst ebenfalls keine Leerzeichen enthalten. Unterstützte Operationen sind die Addition (+), Subtraktion (-), Multiplikation (*), Integer-Division (/), Modulo-Division (%), bitweises AND (&), bitweises OR (|) und bitweises XOR (^). Gültige mathematische Ausdrücke sind zum Beispiel (5*2+1) oder (len1/(len2+4)). Das Resultat ist immer ein Integer und muss ein positiver Wert sein.

zstring und zstring16 sind Null-terminierte Strings, deren Größe dynamisch zur Laufzeit bestimmt wird.

Fortgeschrittene Befehle

Variablendeklarationen können in geschweiften Klammern eingeschlossen werden, so daß sie einen Block bilden, der als ganzes wiederholt eingesetzt werden kann. Beachten Sie aber, daß Blöcke in der aktuellen Implementation nicht verschachtelt werden dürfen. Eine Tilde ("~") kann als Platzhalter für eine spätere Ersetzung mit dem aktuellen Stand des Wiederholungszählers in Variablennamen verwendet werden. Die optionale numbering-Anweisung legt dabei fest, mit welcher Nummer die Zählung begonnen werden soll (standardmäßig mit Null).

```
numbering   1
{
byte          "Länge"
string Länge          "String Nr. ~"
} [10]
```

In diesem Beispiel werden die tatsächlichen Variablennamen in der Schablone "String Nr. 1", "String Nr. 2", ..., "String No. 10" lauten. Anstelle einer fix vorgegebenen Zahl von Wiederholungen (im Beispiel 10) können Sie auch „unlimited" angeben. In diesem Fall wiederholt WinHex den Block bis zum Ende der Datei. "ExitLoop" kann dazu verwendet werden, vorzeitig eine Wiederholungsschleife zu verlassen.

Mit dem Befehl "IfEqual" können zwei Ausdrücke miteinander verglichen werden. Die Vergleichsoperanden können zum einen beide numerisch sein, also jeweils entweder ein konstanter Wert, eine Integer-Variable oder mathematische Ausdrücke. Zum anderen werden Ausdrücke, die entweder als Text oder als hexadezimale Zeichenfolge angegeben werden, byteweise miteinander verglichen. Ausdrücke in Anführungszeichen werden als Zeichenketten interpretiert, Hexadezimalwerte werden durch ein vorangestelltes "0x" identifiziert. Mathematische Ausdrücke müssen von runden Klammern umschlossen sein.

```
{
byte          Wert
IfEqual Wert 1
              ExitLoop
EndIf
} [10]
```

Jedes "IfEqual" muß mit einem "EndIf" abgeschlossen werden. Wenn die Ausdrücke gleich sind, wird der nachfolgende Teil der Schablone abgearbeitet. Ist ein "Else" angegeben, dann wird bei Ungleichheit der Teil nach diesem Schlüsselwort abgearbeitet. "IfEqual"-Anweisungen dürfen nicht verschachtelt sein. Für den Befehl "IfGreater" gelten dieselben Regeln wie für IfEqual, nur dass die Vergleichsbedingung erfüllt ist, wenn der erste Ausdruck größer ist als der zweite. Strings und Hex-Werte werden lexikographisch verglichen.

Um die Übersichtlichkeit einer Schablone zu verbessern, lassen sich Gruppen von Variablen auch visuell bilden, so daß die zugehörigen Editierfelder durch freien Raum im Dialogfenster voneinander getrennt erscheinen.:

```
section "...Bezeichnung des Bereichs..."
...
endsection
```

Die Anweisungen "section", "endsection" und "numbering" haben keinen Einfluß auf die aktuelle Position der Datenauswertung durch die Schablone.

Es gibt noch zwei weitere Befehle, die auch keine Variablen deklarieren, aber explizit benutzt werden, um

die aktuelle Position zu manipulieren. Dies kann z. B. geschehen, um irrelevante Daten zu überspringen (Vorwärtsbewegung) oder um bestimmte Variablen mehrfach in Form von unterschiedlichen Datentypen erfassen zu können (Rückwärtsbewegung). Benutzen Sie die "move n"-Anweisung, um n Bytes von der aktuellen Position aus zu überspringen, wobei n auch negativ sein darf. "goto n" setzt die aktuelle Position auf n, einen absoluten (positiven) Offset auf die Basisposition, auf die die Schablone angewandt wird.

Das folgende Beispiel demonstriert den Zugriff auf 4 Bytes an Daten als 32-Bit-Integer und als eine Kette von 4 Hex-Werten:

```
int32       "Seriennummer des Datenträgers (dezimal)"
move -4
hex 4       "Seriennummer des Datenträgers (hexadezimal)"
```

Datenträger klonen

Läßt Sie eine bestimmte Anzahl von Sektoren von einem Quell- auf einen Zieldatenträger kopieren (oder ersatzweise aus einer Image-Datei bzw. in eine Image-Datei). Dazu müssen beide Datenträger dieselbe Sektorgröße aufweisen. Mit dieser Funktion können Sie exakte Duplikate ganzer Festplatten herstellen, indem Sie einfach *alle* Sektoren kopieren. Aktivieren Sie die entsprechende Option, damit die richtigen Zahlen automatisch für Sie eingetragen werden. Der Zieldatenträger darf nicht kleiner als der Quelldatenträger sein.

Die Funktion »Datenträger klonen« bietet verschiedene Möglichkeiten zu verfahren, wenn defekte Sektoren auf dem Quelldatenträger angetroffen werden:
• Standardmäßig werden Sie benachrichtigt und gefragt, ob der Vorgang abgebrochen oder dennoch fortgesetzt werden soll. Bei eingeschalteter Option „Protokolldatei schreiben" werden Informationen über die gesamte Operation in eine Logdatei in den Ordner für temporäre Dateien geschrieben (Dateiname "Cloning.log.txt"). Darin sind auch die Nummern etwaiger unlesbarer Sektoren enthalten, die nicht kopiert werden können. Diese Option verhindert, daß WinHex jeden defekten Sektor während des Vorgangs einzeln meldet und ist z. B. für forensische Anwendungen nützlich.
• WinHex kann die Zielsektoren, die mit dem Inhalt unlesbarer Quellsektoren beschrieben werden müßten, entweder unverändert lassen oder mit einem ASCII-Muster Ihrer Wahl füllen (z. B. Ihre Initialen oder so etwas wie "BAD "). Lassen Sie das Editierfeld für das Muster leer, um solche Sektoren mit *Nullbytes* zu füllen. Übrigens wird das gewählte Muster auch verwendet, um den Inhalt eines nicht lesbaren Sektors im Disk-Editor anzuzeigen.
• Defekte Sektoren treten häufig in zusammenhängenden Gruppen auf, und jeder Versuch, einen defekten Sektor zu lesen, dauert gewöhnlich sehr lange. WinHex kann solche beschädigten Bereiche versuchen zu meiden: Wenn ein defekter Sektor erkannt wird, kann WinHex versuchen, eine von Ihnen anzugebende Anzahl folgender Sektoren überspringen (in der Voreinstellung 25). Dies ist nützlich, um den Klonvorgang zu beschleunigen, wenn Sie in Kauf nehmen, daß auch einige unbeschädigte Sektoren nicht mit kopiert werden.

Das konventionelle Klonen ist bei austauschbaren Datenträgern (wie Disketten) nicht möglich, wenn nur *ein* entsprechendes Laufwerk installiert ist. Eine geeignete Vorgehensweise für diesen Fall ist *Disk Imaging*, also eine Art »verzögertes« Klonen. Ein Disk-Image kann auf einen anderen Datenträger zurückgespielt werden. Das Ergebnis ist dann dasselbe wie beim Klonen.

Wenn Sie eine Datei namens "dev-null" als Ziel angeben, werden die Daten nur gelesen und nirgendwohin kopiert (und Sie werden diesbezüglich gewarnt). Dies ist nützlich, wenn Sie nur an dem Bericht über defekte Sektoren interessiert sind und den Datenträger nicht wirklich klonen oder in einer Datei sichern möchten.

Sie können "simultane E/A" probieren, wenn das Ziel nicht auf dem gleichen physischen Datenträger liegt wie die Quelle. Bietet die Möglichkeit, den Klonvorgang um bis zu 30% zu beschleunigen.

Es gibt zwei Möglichkeiten, ein Abbild eines Datenträger zu schaffen:
• Der Dialog »Datenträger klonen« erlaubt es, Sektoren von einem Datenträger in eine rohe, originalgetreue Imagedatei zu kopieren (und später zurück). Zusammen mit dem stillen »Protokolldatei-Modus« ist die dem Erstellen einer Sicherung vorzuziehen, wenn es defekte Sektoren auf dem Quelldatenträger gibt.
• Für Optionen wie Komprimierung, Hash-Berechnung und Datei-Segmentierung verwenden Sie bitte die Datenträger-Sicherung. Zur leichten Wiederherstellung enthält eine Backup-Datei Informationen über ihren Inhalt: Sektornummern, Quelldatenträger etc.

Hinweis zu Disk-Cloning & -Imaging

Das Klonen oder Sichern des Laufwerks, auf dem die aktive Windows-Installation enthalten ist, kann eine inkonsistente Kopie zur Folge haben. In jedem Fall stellen Sie bitte sicher, daß das Ursprungslaufwerk während des Klonens/Sicherns/Wiederherstellens nicht von anderen Programmen oder von Windows beschrieben wird. Es wird empfohlen, das von der Umgebungsvariable TEMP angegebene Verzeichnis ggf. auf ein anderes Laufwerk zu verlagern. Die Auslagerungsdatei von Windows sollte ebenfalls auf einem anderen Laufwerk liegen.

Stellen Sie sicher, daß kein anderes Programm oder ein Dienst schreibend auf die zu sichernde oder wiederherzustellende Partition zugreifen kann. Überprüfen Sie z. B. auch im Hintergrund laufende Defragmentiertools und deaktivieren Sie diese für die Dauer des Backups und der Wiederherstellung. Unter Windows NT/2000/XP wird empfohlen, die Partition nicht als logisches Laufwerk/mit einem Laufwerksbuchstaben geladen zu haben.

Ggf. müssen Sie Ihr System neu booten oder "chkdsk /f" auf dem Ziellaufwerk ausführen, damit Windows den neuen Datenträgerinhalt anzeigt (dies löscht intern von Windows verwendete Puffer).

Von WinHex erstellte Datenträger-Clones und -Images sind exakte, sektorweise erstellte, forensisch einwandfreie Kopien, mit allem unbenutzten Speicherplatz und Schlupfspeicher. Sie können nicht dynamisch Partitionsgrößen ändern oder sich an Zieldatenträger anpassen, die eine andere Größe haben als die Quell-datenträger. Dies kann z. B. mit PartitionMagic nachgeholt werden.

Um den Speicherplatz, den ein Backup benötigt, weitestmöglich zu reduzieren, können Sie freien Speicher initialisieren, bevor Sie das Backup erzeugen. Dies liegt daran, daß Sektoren, die nur aus Null-Werten bestehen, die Größe des Backups kaum erhöhen, wenn Kompression eingeschaltet wird.

Datenrettung

In WinHex gibt es vier Möglichkeiten, Daten zu retten. Alle setzen voraus, daß Sie den Datenträger, auf dem die Daten verloren gingen, zunächst mit dem Disk-Editor öffnen.

1) Automatische Datenrettung bei gegebenen Dateinamen (einfachste Methode)

2) Automatische Rettung von Dateien eines bestimmten Typs (setzt kein intaktes Dateisystem voraus)

3) Datenrettung mit dem Verzeichnis-Browser (fortgeschrittener Zugang zum Datenrettungsmechanismus 1)

4) Manuelle Datenrettung

Wichtig: Auf den Datenträger bzw. das Laufwerk, von dem Sie Daten retten möchten, darf auf keinen Fall mehr schreibend zugegriffen werden! Sie überschreiben u. U. sonst unbedachterweise die verlorengegangene Dateien und machen Sie dadurch unwiederherstellbar. D. h. auch, daß Sie Windows nicht mehr auf einem solchen Laufwerk booten dürfen, da dies unzählige Schreiboperationen zur Folge hat.

Diese Version ist ein kostenloses Update für Benutzer, die eine Lizenz für WinHex 11.25 oder neuer erworben haben. Ihre Freischaltcodes sind leider nicht mehr für diese Version gültig. Informationen zu Upgrade-Möglichkeiten erhalten Sie unter http://www.winhex.com/winhex/upgrade-d.html.

Start-Center

Das sog. Start-Center ist ein Dialogfenster, das optional beim Programmstart angezeigt wird und als vereinfachte Schalttafel für den Beginn Ihrer Arbeit mit WinHex gedacht ist. Es erlaubt Ihnen, sowohl Dateien, Datenträger, virtuellen Speicher und Ordner zu öffnen als auch bis zu 255 zuvor geöffnete Dokumente (16 in der Voreinstellung, Liste links). Dies können Dateien, Ordner, logische Laufwerke oder physische Datenträger sein. Wenn diese wieder geöffnet werden, stellt WinHex die letzte Cursor-Position, die Scroll-Position und den Block (falls definiert) wieder her, wenn die entsprechende Option nicht ausgeschaltet ist.

Vom Start-Center aus haben Sie auch Zugriff auf *Projekte* und *Fälle* (Liste rechts oben). Ein Projekt besteht aus einem oder mehreren zu editierenden Dokumenten (Dateien oder Datenträger). Es merkt sich die Cursor-Positionen, die Größe und Positionen der Fenster und einige Anzeige-Optionen. Indem Sie eine Fenster-Anordnung als Projekt speichern, können Sie Ihre Arbeit in mehreren Dokumenten genau dort fortsetzen, wo Sie sie verlassen haben, mit einem einzigen Klick. Dies ist besonders nützlich für wiederkehrende Aufgaben. Wenn Sie ein Projekt laden, werden erst alle zum gegenwärtigen Zeitpunkt geöffneten Fenster automatisch geschlossen.

Außerdem speichert WinHex automatisch die Fensteranordnung am Ende einer WinHex-Sitzung als Projekt und kann sie beim nächsten Mal wiederherstellen. Jedes Projekt wird in einer .prj-Datei gespeichert. Ein Projekt kann gelöscht bzw. umbenannt werden, indem Sie im Start-Center das Kontextmenü benutzen oder das Projekt markieren und die Entfernen- bzw. F2-Taste auf Ihrer Tastatur drücken.

Nicht zuletzt ist das Start-Center auch der Ort, an dem Sie Scripte verwalten können. Mit Hilfe des Kontextmenüs lassen sich Scripte auf die Syntax prüfen, bearbeiten, neu erstellen, umbenennen und löschen. Um ein Script auszuführen, klicken Sie es doppelt an oder nur einfach und betätigen dann den OK-Schalter.

Ansicht-Menü

Nur Text-Anzeige: Blendet die Hexadezimal-Anzeige aus und verwendet die gesamte Breite des Editorfensters für die Text-Anzeige.

Nur Hex-Anzeige: Blendet die Text-Anzeige aus und verwendet die gesamte Breite des Editorfensters für die Hexadezimal-Anzeige.

Datensatz-Darstellung: Beim Editieren aufeinanderfolgender Datensätze, die alle die gleiche Länge aufweisen (z. B. Tabelleneinträge einer Datenbank), können Sie WinHex zur besseren visuellen Unterscheidung jeden zweiten Datensatz mit einer gesonderten Hintergrundfarbe anzeigen lassen. Die Farbe kann im Dialog Allgemeine Optionen bestimmt werden. Außerdem bietet WinHex die Anzeige der aktuellen Datensatz-Nummer und des Offsets innerhalb dieses Datensatzes (also des *relativen* Offsets) in der Statusleiste an. Das alles basiert auf der Datensatzgröße und dem Offset des ersten Datensatzes, wie Sie es im Dialogfenster »Datensatz-Darstellung« angeben.
Wenn Sie eines der beiden Datensatz-Features einschalten, erlaubt es der Befehl »Offset aufsuchen« auch, die aktuelle Cursorposition um ein Vielfaches der aktuellen Datensatzgröße zu verschieben.

Anzeigen: Das Falldaten-Fenster ist Teil der forensischen Benutzeroberfläche von WinHex (X-Ways Forensics). Der **Verzeichnis-Browser** ist für logische Laufwerke/Partitionen verfügbar, die mit dem Disk-Editor geöffnet wurden. **Clusterlisten** können optional für eine jede Datei und einen jeden Ordner angezeigt werden, den Sie im Verzeichnis-Browser doppelt anklicken. Der **Daten-Dolmetscher** ist ein kleines Fenster, das »Übersetzungsmöglichkeiten« für die Daten an der aktuellen Cursorposition anzeigt. Die **Symbolleiste** wird ebenfalls optional angezeigt. Das gleiche gilt für die **Registerleiste**, die es erlaubt, alle Editierfenster mit einem einfachen Mausklick anzuwählen. Die **Informationsspalte,** die Details über das editierte Objekt (Datei, Datenträger, RAM) aufführt, wird auch optional angezeigt.

Schablonen-Manager

Tabellen: Diese Funktion stellt Ihnen Übersichtstabellen zur Verfügung, in denen Sie zu Hexadezimal-Werten von 0 bis FF die Entsprechungen in Dezimalschreibweise, im IBM-ASCII-, ANSI-ASCII- und EBCDIC-Format ablesen können.

Zeilen & Spalten

Rollen synchronisieren: Synchronisiert bis zu vier Fenster auf identische absolute Offsets. Halten Sie die Umschalt-Taste beim Aufrufen dieser Funktion gedrückt, um die Fenster dazu nebeneinander statt übereinander anzuordnen.

Synchronisieren und vergleichen: Synchronisiert bis zu vier Fenster und zeigt unterschiedliche Bytewerte gesondert an. Wenn nicht mehr als zwei Fenster beteiligt sind, hält WinHex beim Rollen immer den anfänglichen Abstand zwischen Offsets der ersten angezeigten Bytes in den beiden Editierfenstern aufrecht. Nicht auf absolute Offsets zu synchronisieren ist nützlich z. B. beim Vergleich zweier Kopien der Dateizuordnungstabelle, die ja an unterschiedlichen Offsets liegen. Sie können zum nächsten bzw. vorherigen verschiedenen Byte springen, indem Sie die zusätzlich in einem der beteiligten Editierfenster bereitgestellten Schalter anklicken.

Anzeige aktualisieren: Erneuert die Anzeige im aktiven Editierfenster. Falls die aktuelle Datei von einem externen Programm geändert wurde, bietet WinHex an, etwaige in WinHex vorgenommenen Änderungen aufzugeben und die Datei nochmal neu zu laden.

Scripte

Ein Großteil der Funktionalität von WinHex kann in automatisierter Weise verwendet werden, z. B. um wiederkehrende Routineaufgaben zu erledigen oder um bestimmte Tätigkeiten an nicht beaufsichtigten Computern im Netz ferngesteuert auszuführen. Die Möglichkeit, andere als die mitgelieferten Beispielscripte auszuführen, ist Besitzern von professionellen und höheren Lizenzen vorbehalten. Scripte können vom Start-Center oder von der Kommandozeile aus gestartet werden. Wenn ein Script ausgeführt wird, können Sie die Esc-Taste drücken, um es abzubrechen. Scripte lösen aufgrund ihrer umfangreicheren Möglichkeiten die von früheren Versionen von WinHex bekannten Routinen ab.

WinHex-Scripte sind Textdateien mit der Namensendung ».whs«. Sie können mit jedem Texteditor bearbeitet werden und bestehen einfach aus einer Folge von Befehlen. Es wird empfohlen, pro Zeile nur einen Befehl einzugeben, um die Übersichtlichkeit zu wahren. Abhängig vom jeweiligen Befehl müssen dahinter ggf. Parameter angegeben werden. Die meisten Befehle wirken sich auf die Datei oder den Datenträger im aktuell aktiven Editierfenster aus.

Groß- und Kleinschreibung spielt bei den Scriptbefehlen *keine* Rolle. Kommentare dürfen überall in einem Script eingefügt werden. Zu ihrer Kenntlichmachung müssen ihnen zwei aufeinanderfolgende Schrägstriche vorangestellt werden. Parameter dürften max. 255 Zeichen lang sein. Sollten Sie im Zweifel sein, weil sowohl Hex-Werte als auch Zeichenketten (oder auch Zahlen) als Parameter akzeptiert werden, können Sie Anführungszeichen benutzen, um die Interpretation eines Parameters als *Text* zu erzwingen. Anführungszeichen sind zwingend erforderlich, wenn eine Zeichenkette oder ein Variablenname eines oder mehrere Leerzeichen enthält, damit alle Zeichen innerhalb der Anführungszeichen als *ein* Parameter erkannt werden.

Wo immer numerische Parameter erwartet werden, ermöglicht der integrierte Formel-Parser die Verwendung mathematischer Notation. Solche Ausdrücke müssen in Klammern angegeben werden. Sie dürfen keine Leerzeichen enthalten. Sie dürfen zuvor deklarierte Variablen verwenden, die als Integer-Werte interpretiert werden können. Unterstützte Operationen sind die Addition (+), Subtraktion (-), Multiplikation (*), Integer-Division (/), Modulo-Division (%), bitweises AND (&), bitweises OR (|) und bitweises XOR (^). Gültige mathematische Ausdrücke sind zum Beispiel (5*2+1), (MyVar1/(MyVar2+4)), oder (-MyVar).

S. auch: WinHex API

Im Folgenden finden Sie Beschreibungen aller gegenwärtig unterstützten Scriptbefehle, incl. Beispiel-Parameter.

Create "D:\My File.txt" 1000
Erzeugt die angegebene Datei mit einer anfänglichen Dateigröße von 1000 Bytes. Wenn die Datei bereits existiert, wird sie überschrieben.

Open "D:\My File.txt"
Open "D:*.txt"
Öffnet die angegebene(n) Datei(en). Geben Sie "?" als Parameter an, um den Nutzer die zu öffnende Datei wählen zu lassen.

Open C:
Open D:
Öffnet das angegebene logische Laufwerk. Opens the specified logical drive. Geben Sie "?" als Parameter an, um den Nutzer das zu öffnende logische Laufwerk oder den physischen Datenträger wählen zu lassen.

Open 80h
Open 81h
Open 9Eh
Öffnet den angegebenen physischen Datenträger. Die Numerierung von Floppy-Laufwerken beginnt mit 00h, die fest eingebauter und Wechseldatenträger mit 80h und die für optische Laufwerke mit 9Eh.

Optional können Sie einen zweiten Parameter mit dem Open-Befehl angeben, der den Editier-Modus angibt, in dem die Datei oder der Datenträger zu öffnen ist ("in-place" oder "read-only").

CreateBackup
Erzeugt ein Backup der aktiven Datei in seinem aktuellen Zustand.

CreateBackupEx 0 100000 650 true "F:\My backup.whx"
Erzeugt ein Backup der aktiven Platte, beginnend mit Sektor 0 bis Sektor 1.000.000. Die Backup-Datei wird automatisch in Stücke von 650 MB segmentiert. Komprimierung ist aktiv ("true"). Die erzeugte Datei ist der letzte Parameter.

Wenn die Backup-Datei nicht segmentiert werden soll, geben Sie 0 als dritten Parameter an. Um Komprimierung abzuschalten, übergeben Sie "false". Um vom Backup-Manager automatisch einen Namen zuweisen zu lassen und die Datei im Verzeichnis für Backup-Dateien ablegen zu lassen, geben Sie "" als letzten Parameter an.

Goto 0x128
Goto MyVariable
Bewegt die aktuelle Cursor-Position zur hexadezimalen Adresse 0x128. Alternativ kann auch eine existierende Variable (bis zu 8 Bytes groß) als numerischer Wert interpretiert werden.

Move -100
Bewegt die aktuelle Cursor-Position um 100 Bytes (dezimal) zurück.

Write "Test"
Write 0x0D0A
Write MyVariable
Schreibt die vier ASCII-Zeichen "Test" oder die zwei Hexadezimal-Werte "0D0A" an die aktuelle Position (im Überschreiben-Modus) und bewegt die aktuelle Cursor-Position entsprechend vorwärts (d.h. um vier bzw. zwei Bytes). Kann auch den Inhalt einer als Parameter angegebenen Variablen schreiben.

Insert "Test"
Arbeitet genau wie der "Write"-Befehl, jedoch im *Einfügen*-Modus. Darf nur mit Dateien benutzt werden.

Read MyVariable 10
Liest 10 Bytes von der aktuellen Position aus in die Variable namens "MyVariable". Wenn diese Variable noch nicht existiert, wird sie erzeugt. Bis zu 32 verschiedene Variablen sind erlaubt. Eine andere Art, eine Variable zu erzeugen, ist der "Assign"-Befehl.

ReadLn MyVariable
Liest von der aktuellen Position in eine Variable namens "MyVariable" bis das nächste Zeilenende-Zeichen gefunden wird. Wenn die Variable bereits existiert, wird ihre Größe entsprechend angepasst.

Close
Schließt das aktive Fenster ohne es zu speichern.

CloseAll
Schließt alle Fenster ohne zu speichern.

Save

Speichert die Änderungen an der Datei oder dem Datenträger im aktiven Fenster.

SaveAs "C:\New Name.txt"
Speichert die Datei im aktiven Fenster unter dem angegebenen Namen und Pfad. Geben Sie "?" als Parameter an, um den Nutzer das Ziel selbst auswählen zu lassen.

SaveAll
Speichert alle Änderungen in allen Fenstern.

Terminate
Bricht die Ausführung des Skripts ab.

Exit
Bricht die Ausführung des Skripts ab und beendet WinHex.

ExitIfNoFilesOpen
Bricht die Ausführung des Skripts ab, wenn aktuell keine Dateien in WinHex geöffnet sind.

Block 100 200
Block "My Variable 1" "My Variable 2"
Legt den aktuellen Block im aktiven Fenster fest beginnend bei Adresse 100 und endend bei Adresse 200 (dezimal). Alternativ können auch existierende Variablen (jede bis zu 8 Bytes groß) als numerische Werte interpretiert werden.

Block1 0x100
Legt den Anfang des Blocks auf die hexadezimale Adresse 0x100. Eine Variable ist ebenfalls als Parameter möglich.

Block2 0x200
Legt das Ende des Blocks auf die hexadezimale Adresse 0x200. Eine Variable ist ebenfalls als Parameter möglich.

Copy
Kopiert den aktuell definierten Block in die Zwischenablage. Wenn kein Block festgelegt ist, bewirkt der Befehl das gleiche wie der "normale" Kopieren-Befehl im Bearbeiten-Menü.

Cut
Schneidet den aktuell markierten Block aus der Datei aus und speichert ihn in der Zwischenablage.

Remove
Entfernt den aktuell markierten Block aus der Datei.

CopyIntoNewFile "D:\New File.dat"
CopyIntoNewFile "D:\File +MyVariable+.dat"
Kopiert den aktuell markierten Block in die angegebene Datei ohne die Zwischenablage zu benutzen. Wenn kein Block festgelegt ist, bewirkt der Befehl das gleiche wie der "normale" Kopieren-Befehl im Bearbeiten-Menü. Kann Datenträger-Sektoren genauso kopieren wie Dateien. Die neue Datei wird automatisch in einem anderen Datenfenster geöffnet. Erlaubt eine unbegrenzte Anzahl von "+" Konkatenationen im Parameter. Eine Variable wird als Integer interpretiert wenn sie nicht größer als 2^24 (~16 Mio.) ist. Nützlich für Schleifen und Datenrettung.

Paste
Schreibt den aktuellen Inhalt der Zwischenablage an die aktuelle Position in einer Datei, ohne die aktuelle Position zu ändern.

WriteClipboard

Schreibt den aktuellen Inhalt der Zwischenablage an die aktuelle Position ein einer Datei oder auf einem Datenträger ohne die aktuelle Position zu verändern und indem es die Daten an der aktuellen Position überschreibt.

Convert *Param1 Param2*
Konvertiert die Daten der aktiven Datei von einem Format in ein anderes. Gültige Parameter sind ANSI, IBM, EBCDIC, Binary, HexASCII, IntelHex, MotorolaS, Base64, UUCode, LowerCase und UpperCase, in den Kombinationen wie sie vom herkömmlichen Konvertieren-Menübefehl bekannt sind.

Encrypt "My Password"
Verschlüsselt die aktive Datei oder den Datenträger oder einen davon ausgewählten Block mit dem angegebenen Schlüssel (bis zu 16 Zeichen lang) unter Verwendung des PC1-Algorithmus (128 bit).

Decrypt "My Password"
Entschlüsselt die aktive Datei oder den Datenträger.

Find "John" [*MatchCase MatchWord Down Up BlockOnly SaveAllPos Unicode Wildcards*]
Find 0x0D0A [*Down Up BlockOnly SaveAllPos Wildcards*]
Sucht im aktiven Fenster nach dem Namen John bzw. dem Hexadezimal-Wert 0x0D0A und hält beim ersten Treffer an. Die anderen Parameter sind optional. Standardmäßig durchsucht WinHex die komplette Datei bzw. Platte. Die optionalen Parameter funktionieren wie von den WinHex-Suchoptionen bekannt.

ReplaceAll "John" "Joan" [*MatchCase MatchWord Down Up BlockOnly Unicode Wildcards*]
ReplaceAll 0x0A 0x0D0A [*Down Up BlockOnly Wildcards*]
Ersetzt alle Suchtreffer einer Zeichenkette oder eines Hexadezimal-Wertes in der aktiven Datei durch etwas anderes. Kann auf Laufwerke nur im In-Place-Modus angewandt werden.

IfFound
Ein boolescher Wert, der davon abhängt, ob die letzte Suchen- oder Ersetzen-Anweisung erfolgreich war. Setzen Sie Anweisungen, die ausgeführt werden sollen, wenn etwas gefunden wird, hinter die IfFound-Anweisung.

IfEqual MyVariable "Hello World"
IfEqual 0x12345678 MyVariable
IfEqual MyVariable 1000
IfEqual MyVariable MyOtherVariable
IfEqual MyVariable (10*MyOtherVariable)
Vergleicht entweder zwei numerische Integer-Werte (von denen jede ein konstanter Wert, eine Integer-Variable oder ein mathematischer Ausdruck sein kann) oder zwei Variablen, ASCII-Zeichenketten oder Hexadezimal-Werte auf binärer Ebene. Der binäre Vergleich zweier Objekte mit unterschiedlichen Längen liefert immer das Ergebnis »falsch«. Wenn die beiden Objekte gleich sind, werden die folgenden Befehle ausgeführt. If-Bedingungen dürfen nicht verschachtelt werden.

IfGreater MyVariable "Hello World"
IfGreater 0x12345678 MyVariable
IfGreater MyVariable 1000
IfGreater MyVariable MyOtherVariable
IfGreater MyVariable (10*MyOtherVariable)
Akzeptiert die gleichen Parameter wie IfEqual. Wenn der erste größer ist als der zweite, werden die folgenden Anweisungen ausgeführt. If-Bedingungen dürfen nicht verschachtelt werden.

Else
Darf nach IfEqual und IfFound auftreten. Setzen Sie Anweisungen, die ausgeführt werden sollen, wenn nichts gefunden wurde oder wenn die verglichenen Objekte nicht gleich sind, hinter die Else-Anweisung.

EndIf

Beendet die bedingte Befehlsausführung (nach IfFound oder IfEqual).

ExitLoop
Beendet eine Schleife. Eine Schleife wird von geschweiften Klammern definiert. Der schließenden Klammer kann direkt ein Integer-Wert in eckigen Klammern folgen, der die Anzahl der Rundendurchläufe angibt. Dies kann auch eine Variable oder das Schlüsselwort "unlimited" (in diesem Fall kann die Schleife nur durch die Anweisung "ExitLoop" verlassen werden) sein. Schleifen dürfen nicht verschachtelt werden.

Beispiel für eine Schleife:
{ Write "Schleife" }[10] schreibt das Wort "Schleife" zehn Mal.

Label ContinueHere
Erzeugt ein Label mit dem Namen "ContinueHere"

JumpTo ContinueHere
Setzt die Ausführung des Skriptes mit der Anweisung, die dem Label folgt, fort.

NextObj
Springt zyklisch zum nächsten geöffneten Fenster und macht es zum "aktiven" Fenster. Wenn beispielsweise drei Fenster offen sind und das Fenster Nr. 3 aktiv ist, macht NextObj Fenster Nr. 1 zum neuen aktiven Fenster.

ForAllObjDo
Der folgende Block von Skriptbefehlen (bis **EndDo** auftritt) wird auf alle offenen Dateien und Laufwerke angewandt.

CopyFile C:\A.dat D:\B.dat
Kopiert den Inhalt von C:\A.dat in die Datei D:\B.dat.

MoveFile C:\A.dat D:\B.dat
Verschiebt die Datei C:\A.dat nach D:\B.dat.

DeleteFile C:\A.dat
Löscht überraschenderweise die Datei C:\A.dat.

InitFreeSpace
InitSlackSpace
Initialisiert den freien bzw. den Schlupfspeicher auf dem aktuellen logischen Laufwerk unter Verwendung der aktuellen Initialisierungs-Einstellungen. InitSlackSpace setzt das Laufwerk vorübergehend in den In-Place-Modus, womit alle noch anstehenden Änderungen gespeichert werden.

InitMFTRecords
Initialisiert alle unbenutzten MFT-FILE-Records auf dem aktuellen logischen Laufwerk, sofern es mit NTFS formatiert ist, unter Verwendung der aktuellen Initialisierungs-Einstellungen. Tut nichts auf anderen Dateisystemen. Die Änderungen werden unmittelbar auf die Platte geschrieben.

Assign MyVariable 12345
Assign MyVariable 0x0D0A
Assign MyVariable "I like WinHex"
Assign MyVariable MyOtherVariable
Speichert die angegebene Integer-Zahl, Binärdaten, ASCII-Text oder den Inhalt einer anderen Variable in eine Variable mit Namen "My Variable". Wenn diese Variable noch nicht existiert, wird sie erzeugt. Bis zu 32 verschiedene Variablen sind erlaubt. Eine andere Methode, eine Variable anzulegen, ist der Read-Befehl.

SetVarSize MyVariable 1

SetVarSize MyVariable 4
Setzt die zugewiesene Speichergröße einer Variablen ausdrücklich auf eine bestimmte Byte-Größe zu diesem Zeitpunkt. Dies kann hilfreich sein, z. B. um Variablen, die Integer-Werte enthalten und die aus einer Berechnung stammen, in eine binäre Datei mit einer fixen Struktur zu schreiben. Ohne Aufruf von SetVarSize dürfen keinerlei Annahmen über die Größe einer Variablen gemacht werden. Zum Beispiel könnte die Zahl 300 in einer beliebigen Zahl von Bytes größer als 1 gespeichert werden. Wenn die neue Größe mit SetVarSize kleiner ist als die bisherige, wird der zugewiesene Speicher abgeschnitten. Wenn die neue Größe größer ist, wird der zugewiesene Speicher ausgeweitet. In jedem Fall wird der Wert der verbleibenden Bytes beibehalten.

GetUserInput MyVariable "Bitte geben Sie Ihren Namen ein:"
Speichert den ASCII-Text oder die binären Daten (0x...), die der Nutzer zur Laufzeit des Skripts eingegeben hat (max. 128 Bytes), in einer Variablen mit Namen "MyVariable". Der Nutzer erhält ein Dialogfenster mit der Nachricht, die Sie als zweiten Parameter angeben. Wenn die Variable nicht existiert, wird sie erzeugt. Andere Möglichkeiten zur Erzeugung einer Variablen: Assign, Read.

GetUserInputI MyIntegerVariable "Bitte geben Sie Ihr Alter in Jahren ein:"
Funktioniert wie GetUserInput, akzeptiert und speichert aber nur Integer-Werte.

Inc MyVariable
Interpretiert eine Variable als Integer (sofern sie nicht größer als 8 Bytes ist) und inkrementiert sie um eins. Praktisch in Schleifen.

Dec MyVariable
Interpretiert eine Variable als Integer (sofern sie nicht größer als 8 Bytes ist) und dekrementiert sie um eins.

IntToStr MyStr MyInt
IntToStr MyStr 12345
Speichert die dezimale ASCII-Text-Repräsentation der Integer-Zahl, die als zweiter Parameter übergeben wird, in die Variable, die als erster Parameter angeben ist.

StrToInt MyInt MyStr
Speichert die Binärcodierung der Integer-Zahl, die als dezimaler ASCII-Text als zweiter Parameter übergeben wird, in die die Variable, die als erster Parameter angegeben ist.

StrCat MyString MyString2
StrCat MyString ".txt"
Hängt eine Zeichenkette an eine andere an. Der zweite Parameter kann eine Konstante oder eine Variable sein. Der erste Parameter muss eine Variable sein. Das Ergebnis wird in der Variablen gespeichert, die als erster Parameter übergeben wurde, und darf nicht länger als 255 Zeichen sein.

GetClusterAlloc MyStr
Kann auf ein logisches Laufwerk angewendet werden, das mit den Dateisystemen FAT oder NTFS formatiert ist. Holt eine textuelle Beschreibung der Zuordnung der aktuellen Position, z.B. welche Datei im aktuellen Cluster gespeichert ist, und speichert diese Beschreibung in der angegebenen Variablen.

InterpretImageAsDisk
Behandelt ein Roh-Image oder ein Evidence-File wie eine echte physische Platte oder Partition. Erfordert eine Specialist- oder forensische Lizenz.

CalcHash HashType MyVariable
CalcHashEx HashType MyVariable
Berechnet einen Hashwert wie es aus dem Extras-Menü bekannt ist und speichert ihn in der angegebenen Variablen (die erzeugt wird, wenn sie nicht existiert). Der HashType-Parameter muss einer der folgenden sein: CS8, CS16, CS32, CS64, CRC16, CRC32, MD5, SHA-1, SHA-256, PSCHF.

CalcHashEx zeigt den Hashwert zusätzlich in einem Dialogfenster an.

MessageBox "Caution"
Zeigt ein Dialogfenster mit dem Text "Caution" an und bietet einen OK und einen Cancel-Knopf. Durch Drücken von Cancel wird der Skriptdurchlauf abgebrochen.

ExecuteScript "ScriptName"
Führt ein anderes Skript aus einem laufenden Skript heraus aus am aktuellen Punkt der Skriptausführung, z.B. abhängig von einer Bedingung. Aufrufe an andere Skripte dürfen verschachtelt sein. Wenn der Aufruf des Skripts beendet ist, wird das ursprüngliche Skript mit dem nächsten Kommando weiter ausgeführt. Diese Funktion ermöglicht eine bessere Strukturierung Ihrer Skripte.

Turbo On
Turbo Off
Im Turbo-Modus werden die meisten Bildschirm-Elemente zur Laufzeit des Skripts nicht aktualisiert und es ist nicht möglich, das Skript abzubrechen (beispielsweise durch Drücken von Esc) oder zu pausieren. Dies beschleunigt das Skript um bis zu 75%, wenn sehr viele einfache Befehle wie Move oder NextObj in einer Schleife ausgeführt werden.

Debug
Alle folgenden Befehle müssen vom Nutzer einzeln bestätigt werden.

UseLogFile
Fehlermeldungen werden in die Log-Datei "Scripting.log" im Verzeichnis für temporäre Dateien geschrieben. Diese Meldungen werden nicht in einem Dialogfenster angezeigt, das Nutzerinteraktion verlangt. Nützlich insbesondere um Skripte unbeaufsichtigt auf einem Rechner laufen zu lassen.

CurrentPos
GetSize
unlimited
sind Schlüsselworte, die als Platzhalter fungieren und die benutzt werden können, wo numerische Parameter erwartet werden. Zur Skriptlaufzeit steht CurrentPos für die aktuelle Adresse im aktiven Datei- oder Laufwerksfenster und GetSize für seine Größe in Bytes. unlimited steht tatsächlich für die Zahl 2.147.483.647.

WinHex API

Ziel

Die WinHex API (Anwendungsprogrammierschnittstelle) erlaubt es Ihnen, die fortgeschrittenen Fähigkeiten des WinHex Hex-Editors von Ihren eigenen C++-, Delphi- oder Visual-Basic-Programmen aus zu verwenden. Insbes. stellt sie eine bequeme und einfache Schnittstelle für den wahlfreien Zugriff auf Dateien und Datenträger zur Verfügung.

Anforderungen

Das Entwickeln von Software, die von der WinHex API Gebrauch macht, erfordert eine gültige *professionelle* oder *Specialist*-WinHex-Lizenz. Außerdem benötigen Sie Import-Deklarationen für Ihre Programmiersprache, die Bibliotheksdatei „whxapi.dll" und die API-Dokumentation. Sie finden alle benötigten Dateien sowie weitere Details unter http://www.winhex.com/winhex/api/.

Sie dürfen jede Software, die die WinHex API benutzt, und WinHex auch *weitervertreiben*. Es gibt zwei Möglichkeiten, WinHex weiterzugeben:

1. Geben Sie die unlizenzierte Evaluationsversion von WinHex weiter. Damit die API funktioniert, muß Ihr Kunde professionelle, Specialist- oder API-Lizenzen in der Zahl der benötigten WinHex-Installationen selbst beschaffen.

-oder-

2. Empfohlen: Bestellen Sie selbst die spezielle API-Version von WinHex und geben Sie sie einfach weiter. Diese Version ist so konfiguriert, daß sie nur die API-Funktionalität bereitstellt (die normale Benutzerschnittstelle ist nicht verfügbar), und sie ist zu einem reduzierten Preis verfügbar. Sie können API-Lizenzen bestellen unter http://www.winhex.com/winhex/api/. Mengenrabatte auf Anfrage. Bitte geben Sie dazu die Anzahl der Lizenzen, an denen Sie interessiert sind, an. Pro Endbenutzer-Computer ist eine WinHex-API-Lizenz erforderlich. WinHex wird auf Ihren Namen lizenziert, *Sie* sind der tatsächliche Inhaber der Lizenzen, aber jeder Ihrer Kunden kann sie verwenden. Der Endbenutzer muß sich im Zusammenhang mit WinHex um nichts selbst kümmern.

Siehe auch: Scripte

Dateien retten nach Typ

Eine Datenrettungsfunktion im Extras-Menü, die nach Dateien an bestimmten Header-Signaturen erkennt, also einer für den jeweiligen Dateityp charakteristischen Bytewert-Folge. Sie wird auch als »file carving« bezeichnet. Aufgrund dieses Ansatzes ist "Dateien retten nach Typ" nicht vom Vorhandensein von funktionierenden Dateisystemstrukturen abhängig. Wenn anhand der Signatur gefunden, werden die Dateien in dem von Benutzer angegebenen Ausgabeordner gespeichert. Optional werden Dateien jedes Typs in ihrem eigenen Unterordner abgelegt (...\JPEG, ...\HTML, usw.). Beachten Sie, daß "Dateien retten nach Typ" physisch zusammenhängende Cluster voraussetzt, also im Fall von fragmentiert gespeicherten Clusterketten inkonsistente Dateien ausgibt. Eine Log-Datei namens "File Recovery by Type.log", die über die gewählten Parameter und die Datenrettungsergebnisse Auskunft gibt, wird zu Prüfzwecken ebenfalls in den Ausgabeordner geschrieben.

Da auf ein ggf. vorhandenes Dateisystem (funktional oder nicht) nicht zurückgegriffen wird, sind dem Algorithmus die Original-Datei*größen nicht bekannt*, und die Original-Datei*namen* auch nicht. Das ist der Grund, warum die resultierenden Dateien nach folgendem Muster benannt werden: Prefix[X]id0000.ext. "Prefix" ist ein von Ihnen angegebenes optionales Prefix. "id" ist eine eindeutige Zeichenkombination, die einen Eintrag in den Dateityp-Definitionen identifiziert (aa = 1. Eintrag, ab = 2. Eintrag, ...). "0000" ist eine laufende Nummer pro Dateityp. "ext" ist die Dateinamenserweiterung, die laut den Dateityp-Definitionen der Datei-Header-Signatur entspricht. Wenn wiederhergestellte JPEG-, GIF- und Dateien einiger anderer Typen beschädigt oder unvollständig sind (z. B. aus Fragmentierung resultierend), kann WinHex das oft feststellen. In einem solchen Fall wird die Datei in der Log-Datei als beschädigt markiert und in ihrem Dateinamen wird ein "X" eingefügt. Wenn erkannt wird, daß das vom Benutzer spezifierte Dateigrößen-Limit für bestimmte Dateien zu klein gewählt ist, wird das ebenfalls in der Log-Datei vermerkt.

Der Algorithmus versucht Dateien vom Typ JPEG, GIF, PNG, BMP, TIFF, CDR, AVI, WAV, ZIP, MS Word, MS Excel, MS PowerPoint, RTF und HTML in ihrer ursprünglichen, korrekten Größe wiederherzustellen, indem es deren Datenstrukturen untersucht. Dies wird begrenzt ungefähr durch die vom Benutzer spezifizierte maximale Dateigröße. Die zugehörigen Einträge in der Dateityp-Definitionsdatei dürfen nicht verändert werden, sonst funktioniert die Größen- und Typerkennung für diese Dateitypen u. U. nicht. Dateien anderen Typs werden in exakt dieser als Maximum in KB angegebenen Größe wiederhergestellt. Seien Sie »großzügig« beim Spezifizieren des Maximums, da "zu groß" wiederhergestellte Dateien durchaus noch von ihren zugehörigen Anwendungsprogrammen geöffnet werden können, abgeschnittene unvollständige Dateien aber nicht.

Technisch können Sie so viele Dateitypen für die simultane Rettung auswählen wie Sie möchten. Wenn Sie allerdings z. B. MS-Office- und AVI-Dateien auf einmal retten möchten, Sie aber für die Office-Dateien Größen von ein paar KB und für die AVI-Dateien Größen von etwas 1 GB erwarten, wäre die Anwendung eines einzigen globalen Dateigrößen-Limits nicht sinnvoll. Daher können Sie optional eine individuelle Standardgröße pro Dateityp in der Dateityp-Definitionsdatei angeben.

Standardmäßig werden Dateiheader nur an *Cluster*-Grenzen gesucht, da der Anfang eines Clusters der einzige Ort ist, an dem eine Datei in einem Cluster-basierten Dateisystem anfangen kann. Sie können allerdings auch nach Dateiheadern an *Sektor*-Grenzen suchen lassen. Das ist nützlich, um Dateien von einer früheren Partition mit einem anderen Cluster-Layout zu finden. Wenn der Algorithmus auf einen physischen Datenträger oder eine einfache Datei angewandt wird, wo keine Cluster definiert sind, sucht WinHex ohnehin an Sektorgrenzen, auch wenn Clustergrenzen auswählt sind. Es gibt noch eine weitere Möglichkeit, die vollständige Suche auf *Byte*-Ebene. Diese ist erforderlich zum Extrahieren von Dateien aus Backups, Bändern o. ä. (oder auch JPEG-Dateien innerhalb von MS-Word-Dokumenten), wo sie nicht an Cluster- oder Sektorgrenzen ausgerichtet sind. Damit kann allerdings eine erhöhte Zahl von fälschlicherweise erkannten Dateiheadern einhergehen, also Bytewertfolgen, die zufällig auf einem Datenträger vorkommen, aber dort nicht den Anfang einer Datei anzeigen.

Sie können den Erfassungsbereich der Datenrettung wenn gewünscht auf einen ggf. ausgewählten Block einschränken und/oder auf belegten oder unbelegten Speicher (bei einem logischen Laufwerk oder einer Partition verfügbar). Um nur Dateien zu retten, die gelöscht worden sind, wählen Sie unbelegten Speicher. Dateien, die z. B. nur aufgrund von Dateisystemfehlern nicht mehr zugreifbar sind, können dagegen durchaus noch in als belegt gekennzeichneten Clustern gespeichert sein.

Die Option "Ext2/Ext3-Block-Logik anwenden" veranlaßt diese Wiederherstellungsmethode, von der Standardannahme nicht-fragmentierter Speicherung abzuweichen: Statt dessen folgt sie dem typischen Ext-Block-Muster, in dem beispielsweise der 13. Block ab dem Header der Datei als indirekter Block betrachtet wird, der selbst auf die folgenden Datenblöcke verweist. Diese Option zeigt keine Wirkung, wenn sie auf Partitionen angewendet wird, von denen WinHex weiß, daß sie ein anderes Dateisystem als Ext2 oder Ext3 haben oder wenn ein Header gefunden wird, der nicht an einer Block-Grenze ausgerichtet ist.

Wenn Sie die Option "Nicht tatsächlich wiederherstellen, bloß auflisten" wählen, werden keine Dateien erzeugt und auch keine Logdatei geschrieben. Die Dateien werden nur im Verzeichnisbrowser aufgelistet, d.h. zur Einsicht mit der Galerie und für die selektive Wiederherstellung direkt aus dem Verzeichnisbrowser.

Specialist-Menü

Nur für Inhaber einer Specialist-Lizenz verfügbar.

Parallele Suche: Diese Funktion läßt Sie nach nach einer beinahe unbegrenzt langen Liste von Zeichenketten (Strings) oder Hex-Werten (mit Präfix 0x anzugeben) gleichzeitig suchen (physische Suche). Je ein Suchbegriff pro Zeile. Die Vorkommnisse können im Positionsmanager archiviert werden. WinHex speichert jeweils Offset, Suchwort, Name der durchsuchten Datei/des durchsuchten Datenträgers und im Fall eines logischen Laufwerks auch die Clusterzuordnung (also den Namen und den Pfad der Datei, die an der Fundstelle gespeichert ist).
Das heißt, forensische Ermittler können nun systematisch mehrere Festplatten und Image-Dateien in einem einzigen Durchlauf nach Wörtern wie z. B. "Droge", "Kokain", umgangssprachlichen Synonymen, Adreßbestandteilen und Personennamen suchen. Bei der Suche auf einem logischen Laufwerk schränkt das die Untersuchung auf eine Liste von Dateien ein, auf die man sich konzentrieren kann. Wenn Sie WinHex die Fundstellen nicht archivieren lassen, können Sie die F3-Taste benutzen, um die Suche fortzusetzen.
Suchoptionen Logische Suche

Laufwerksinhaltstabelle erstellen

Verzeichnisinhaltstabelle erstellen: Funktioniert wie »Laufwerksinhaltstabelle erstellen«, wird aber nur auf ein vom Benutzer ausgewähltes Verzeichnis und dessen Unterverzeichnisse angewandt. Sie finden dieses Kommando nur im Kontextmenü des Verzeichnisbrowsers, wenn Sie ein Verzeichnis rechts anklicken.

Datenträger-Detailbericht: Zeigt Informationen über den aktiven Datenträger bzw. die aktive Datei an und läßt Sie diese kopieren, z. B. in einen Bericht den Sie anfertigen. Besonders ausführlich bei physischen Festplatten, zu denen Details über jede Partition und allen keiner Partition zugeordneten Speicherlücken aufgeführt werden. Unter Windows 2000 und XP berichtet WinHex auch den Paßwortschutz-Status von ATA-Festplatten.
Nur mit forensischer Lizenz: WinHex kann unter Windows 2000 und XP versteckte sog. Host Protected Areas (HPA, auch bekannt als ATA-geschützte Bereiche) auf IDE-Festplatten erkennen. Ein Meldungsfenster mit einer Warnung wird angezeigt, falls ein solcher Bereich gefunden wird. Auf jeden Fall wird die tatsächliche Gesamtzahl der Sektoren laut ATA, wenn erfolgreich ermittelt, im Detailbericht mit aufgelistet.

Image als Datenträger interpretieren: Behandelt eine geöffnete und aktive Image-Datei entweder als logisches Laufwerk oder physischen Datenträger. Das ist nützlich, wenn Sie den Inhalt eines Disk-Image untersuchen möchten, einzelne Dateien aus dem Dateisystem extrahieren möchten usw., ohne das Image zurück auf einem Datenträger zurückzuspielen. Beim Interpretieren als physischen Datenträger kann WinHex die im Image enthaltenen Partitionen öffnen wie von einer »echten« physischen Festplatte. WinHex kann sogar dateiübergreifende Roh-Images interpretieren, also Image-Dateien, die aus einzelnen Segmenten beliebiger Größe bestehen (sog. "spanned image files"). Damit WinHex ein dateiübergreifendes Image erkennt, darf das erste Segment einen beliebigen Namen und eine nicht-numerische Namenserweiterung oder die Namenserweiterung ".001" haben. Das zweite Segment muß denselben Basisdateinamen, aber die Erweiterung ".002" haben, das dritte Segment ".003" usw. Sowohl der Befehl Datenträger-Sicherung als auch das Plattenklon-Programm X-Ways Replica für DOS erzeugen kompatibel benannte Disk-Image-Segmente. Das Segmentieren ist nützlich, da die maximal unterstützte Dateigröße bei FAT-Dateisystemen limitiert ist.
In seltenen Fällen kann WinHex nicht korrekt erkennen, ob der erste Sektor in einem Image ein Sektor ist, der den Master Boot Record enthält, oder bereits ein Bootsektor einer Partition ist, und interpretiert die Struktur der Image-Datei daraufhin falsch. Um Abhilfe zu schaffen, können Sie die Umschalt-Taste beim Aufruf dieses Befehls gedrückt halten, damit WinHex nicht selbst entscheidet, sondern Sie fragt.
Mit einer forensischen Lizenz kann WinHex auch Evidence-Files (.e01-Sicherungen) interpretieren, die

mit dem Befehl Datenträger-Sicherung erstellt werden können.

RAID-System zusammensetzen: WinHex kann RAID-0-Systeme intern zusammenführen ("destripe"), die aus bis zu 5 Komponenten bestehen (physische Festplatten oder Sicherung). Auf diese Weise ist es nicht erforderlich, RAID-Systeme mit Hilfe eines Scripts zusammenzuführen und in eine Image-Datei zu exportieren, was Zeit und Plattenplatz spart. Stellen Sie sicher, daß die Komponenten bereits geöffnet sind, wenn Sie diese Funktion aufrufen. Sie müssen die Komponenten in der richtigen Reihenfolge angeben. WinHex läßt Sie die Blockgröße in Sektoren ("stripe size", oftmals 128) angeben sowie individuelle RAID-Header-Größen pro Komponente (normalerweise einfach 0). Daß entweder Komponentenreihenfolge, Blockgröße oder RAID-Header-Größe nicht korrekt waren, erkennen Sie normalerweise daran, daß keine Partitionen erkannt werden oder Partitionen mit unbekannten Dateisystemen oder mit Dateisystemen, die nicht richtig interpretiert werden.
Wenn Sie zusammengesetztes RAID-System einem Fall hinzufügen (und optional daraus geöffnete Partitionen), werden die gewählten RAID-Parameter zusammen mit dem Asservat gesichert, so daß Sie auf das RAID-System zu einem späteren Zeitpunkt ohne Zeitverlust erneut zugreifen können (nur forensische Lizenzen).

Freien Speicher extrahieren: Durchläuft das gegenwärtig geöffnete logische Laufwerk und sammelt alle unbenutzten Cluster in einer von Ihnen anzugebenen Zieldatei. Nützlich um Datenfragmente von vormals existierenden Dateien, die nicht sicher gelöscht wurden, zu untersuchen. Nimmt keine Änderungen am untersuchten Laufwerk vor. Die Zieldatei muß auf einem anderen Laufwerk abgelegt werden.

Schlupfspeicher extrahieren: Sammelt Schlupfspeicher (englisch »slack space«, die unbenutzten Bytes im jeweils letzten Cluster einer Clusterkette, hinter dem tatsächlichen Ende der Datei) in einer Zieldatei. Jedem Vorkommen von Schlupfspeicher werden Zeilenumbrüche vorangestellt und die Nummer des Clusters, in dem er gefunden wurde, als ASCII-Text. Ansonsten ähnlich wie »Freien Speicher extrahieren«. WinHex kann Schlupfspeicher von Dateien, die auf Dateisystemebene komprimiert oder verschlüsselt sind, nicht erfassen.

Partitionslücken extrahieren: Erfaßt die Speicherbereiche einer physischen Festplatte, die zu keiner Partition gehören, in einer Zieldatei, zur schnellen Untersuchung, um herauszufinden, ob dort etwas versteckt ist oder übrig geblieben von früheren Partitionierungen.

Text extrahieren: Erkennt Text anhand der von Ihnen anzugebenden Parameter, erfaßt alle Vorkommnisse in einer Datei, auf einem Datenträger oder innerhalb eines Speicherbereichs und schreibt diese in eine Datei. Diese Art von Filter ist nützlich, um auszuwertende Datenmengen beträchtlich zu verringern, wenn z. B. bei einer forensischen Computeranalyse Hinweise in Form von Text (wie E-Mails, Dokumente) gesucht werden. Die Zieldatei kann leicht in benutzerdefinierte Größen zerlegt werden. Diese Funktion kann auch auf Dateien mit gesammelten Schlupf- oder freiem Speicher angewandt werden, oder auf beschädigte Dateien in einem proprietären Format, die nicht mehr von der zugehörigen Applikation, wie MS Word, geöffnet werden können, um zumindest unformatierten Text zu retten.

Bates-Numerierung: Versieht alle Dateien innerhalb eines bestimmten Ordners und seiner Unterordner für die forensische Verwendung mit einer Bates-Numerierung. Fügt ein bis zu 13 Zeichen langes konstantes Präfix und eine eindeutige laufende Nummer zwischen Dateinamen und Dateinamenserweiterung ein, ähnlich wie Anwälte Papierdokumente für spätere Bezugnahme kennzeichnen.

Sicherer Dateiexport: Auch: »trusted download« (vertrauenswürdiges Überspielen von Daten). Löst ein Sicherheitsproblem. Wenn als vertraulich oder geheim eingestuftes Material von einem klassifizierten auf einen nicht-klassifizierten Datenträger übertragen wird, muß sichergestellt sein, daß keine überschüssigen Informationen in einem Cluster- oder Sektorüberhang ungewollt mit der eigentlichen Datei mitkopiert werden, da dieser sog. Schlupfspeicher (s. o.) noch vertrauliches oder geheimes Material von einem früheren Zeitpunkt enthalten kann, an dem er noch einer anderen Datei zugeordnet war. Dieser Befehl kopiert die ausgewählte(n) Datei(en) nur in ihrer aktuellen tatsächlichen Größe, und kein weiteres Byte mehr. Er kopiert nicht ganze Sektoren oder Cluster, wie es konventionelle Kopierbefehle

tun. Es können mehrere Dateien eines Ordners auf einmal kopiert werden.

Freien Speicher/Schlupfspeicher hervorheben: Zeigt Offsets und Daten in weicheren Farben an (hellblau bzw. grau). Hilft, diese speziellen Laufwerksbereiche leicht zu erkennen. Funktioniert auf FAT-, NTFS- und Ext2/3-Partitionen.

Manuelle Datenrettung

WinHex bietet nicht nur verschiedene automatische Datenrettungsmechanismen an, es ist auch ein sehr mächtiges Werkzeug, um Daten *manuell* (von Hand) zu retten. Es ist möglich, verlorengegangene oder logisch gelöschte Dateien (oder allgemeiner: Daten), die nur im Dateisystem als »gelöscht« verzeichnet sind, aber nicht tatsächlich *physisch* gelöscht oder überschrieben wurden, wiederherzustellen.

Öffnen Sie das logische Laufwerk, auf dem sich die gelöschte Datei befand, mit dem Disk-Editor. Prinzipiell können Sie eine solche **Datei wiederherstellen**, indem Sie die **Datenträger-Sektoren**, die dieser Datei zugeordnet waren, als aktuellen Block **auswählen** und mit dem Menübefehl »**Bearbeiten | Block kopieren | In neue Datei**« **speichern**. Allerdings kann es sich als schwierig erweisen, die Sektoren, in denen die Datei noch gespeichert ist, zu *finden*. Es gibt zwei verschiedene Möglichkeiten, dies zu bewerkstelligen:

1. Falls Sie einen kurzen Ausschnitt aus der Datei, die Sie suchen, genau kennen (z.B. die charakteristische Signatur im Header einer JPEG-Datei oder die Wörter »Sehr geehrter Herr Meier« in einem MS-Word-Dokument), suchen Sie diesen auf dem Datenträger unter Zuhilfenahme der üblichen Suchbefehle (»Text suchen« oder »Hex-Werte suchen«). Dies ist eine sehr einfache und zuverlässige Möglichkeit, die jedem empfohlen werden kann.

2. Falls Sie nur den Namen der gesuchten Datei kennen, brauchen Sie etwas Hintergrundwissen über das Dateisystem auf dem Datenträger (FAT16, FAT32, NTFS, ...), um Spuren des ehemaligen Verzeichniseintrags der Datei zu finden und dadurch die Nummer des ersten der Datei zugeordneten Clusters zu ermitteln. Detaillierte Informationen über Dateisysteme sind auf der WinHex Web-Site verfügbar. Folgendes gilt für alle FAT-Varianten:

   Wenn das Verzeichnis, das die Datei *enthielt* (nennen wir es »D«) noch existiert, dann können Sie D auf dem Datenträger mit Hilfe des Menübefehls »Extras | Disk-Tools | Verzeichniscluster auflisten« finden. Die WinHex beiliegende Schablone für FAT-Verzeichniseinträge hilft Ihnen dann, die Nummer des ersten der Datei zugeordneten Clusters herauszufinden. Andernfalls, wenn D auch gelöscht wurde, müssen Sie ersten den Inhalt von D (mit Hilfe derselben Schablone) finden, ausgehend von dem Verzeichnis, das D enthielt (möglicherweise das Stammverzeichnis).

   Gelöschte Dateien und Verzeichnisse sind mit dem Zeichen »å« (hexadezimal: E5) als ersten Buchstaben ihres Namens gekennzeichnet.

Möglicherweise stoßen Sie auf das Problem, daß die wiederherzustellende Datei fragmentiert ist, also nicht in aufeinanderfolgenden, zusammenhängenden Clustern gespeichert ist. Auf FAT-Laufwerken kann der nächste Cluster einer Datei in der Dateizuordnungstabelle am Anfang des Datenträgers nachgeschlagen werden, aber diese Information geht beim Löschen einer Datei verloren.

Dateien retten nach Name

Datenrettungsfunktion und Teil des Disk-Tools-Menüs. Läßt sich auf FAT12-, FAT16-, FAT32- und NTFS-Laufwerke anwenden. Öffnen Sie zunächst ein logisches Laufwerk oder eine einzelne Partition eines physischen Datenträgers mit dem Befehl Disk öffnen. Sie können ein oder mehrere Dateinamensmuster angeben, die die wiederherzustellenden Dateien abdecken, z. B.:

Brief an Herrn Schmidt.doc
Rechnung*.pdf
m*.xls
Bild0*.gif
*.tif

Sie können auch bestimmte Dateinamen *ausschließen*, indem Sie dem Muster einen Doppelpunkt voranstellen. Um z. B. alle Dateien außer NTFS-Systemdateien zu erfassen (die immer mit einem Dollar-Zeichen beginnen), geben Sie ein:

*
:$*

Bitte beachten Sie, daß Dateien, die vor der permamenten Löschung in den Papierkorb verschoben wurden, von Windows intern umbenannt wurden, wobei nur die Dateiendung unverändert bleibt, so daß die Verwendung von Jokerzeichen helfen kann (z. B. *.jpg statt abc.jpg). Im Gegensatz zu Dateien retten nach Typ stellt »Dateien retten nach Name« auch Datei-Datum und -Uhrzeit sowie die Datei-Attribute wieder her.

Optional rettet/kopiert diese Funktion nur Dateien, die im Dateisystem aktuell als existierend geführt werden, oder nur nicht-existente (gelöschte oder sonstwie verlorengegangene) Dateien.

Alternativ zum Benutzen der Dateizuordnungstabelle eines FAT-Laufwerks kann WinHex sich optional auch darauf verlassen, daß die Dateien nicht fragmentiert sind, und sie als zusammenhängende Folge von Clustern wiederherstellen.

Schalten Sie »Ungültige Dateinamen abfangen« ein, um das Fehlschlagen der Wiederherstellung wegen eines vom Dateisystem als unzulässig angesehenen Zeichens zu verhindern. Nützlich z. B. wenn Sie mit einer Windows-Version in einer westlichen Sprache Dateien retten möchten, deren Dateinamen aus einer nicht-westlichen Sprache stammen. Diese Option wird solche Dateien erforderlichenfalls umbenennen, um sicherzustellen, daß diese erstellt werden können.

Wenn auf einem NTFS-Laufwerk die Datei, die Sie suchen, nicht gefunden werden kann, hilft es möglicherweise, die Option »intensive Suche« einzuschalten. Sie ist standardmäßig nicht aktiviert, weil sie deutlich mehr Zeit beansprucht.

Sie müssen einen Ausgabeordner angeben, in dem die Originaldatei(en) repliziert werden sollen. Wichtig: Stellen Sie sicher, daß sich dieser Ordner auf einem anderen Laufwerk befindet. Wenn Sie einen Ordner auf demselben Laufwerk angeben, von dem Daten gerettet werden sollen, könnte leicht Speicherplatz überschrieben werden, in dem sich noch die gelöschten Dateien befinden, die Sie retten möchten! Auf diese Weise gingen sie endgültig verloren. Es könnte auch eine Endlosschleife auftreten, wenn WinHex wiederholt die Dateien "rettet", die es gerade erst wiederhergestellt hat.

Überhangsektoren

Dieser Ausdruck wird in WinHex auf folgende Weise verwendet:

Als Überhangsektoren werden auf einem logischen Laufwerk die wenigen Sektoren am Ende bezeichnet, die keinen ganzen Cluster mehr ergeben und daher vom Betriebssystem nicht benutzt werden können (und daher auch von keinem konventionellen Anwendungsprogramm).

Überhangsektoren auf einem physischen Datenträger sind diejenigen Sektoren am Ende, die sich außerhalb der regulären Plattengeometrie befinden (da sie keine volle Zylinder/Kopf/Spur-Einheit mehr ergeben), weshalb sie gewöhnlich von keiner Partition und auch nicht vom Betriebssystem (oder konventionellen Anwendungsprogrammen) benutzt werden.

Überhangsektoren haben nichts mit beschädigten Sektoren zu tun oder Sektoren, die von einer Festplatte intern als unsichbarer Ersatz für beschädigte Sektoren eingesetzt werden.

Flexible Integer-Variablen

Ein besonderer Variablentyp, der von Schablonen unterstützt wird, ist uint_flex. Dieser Typ ermöglicht es, einen vorzeichenlosen Integer-Wert aus verschiedenen individuellen Bits innerhalb eines 32-Bit- (4-Byte-) Bereichs in beliebiger Reihenfolge zusammenzusetzen, und ist sogar flexibler als das sogenannte Bit-Feld der Programmiersprache C.

uint_flex erfordert als zusätzlichen Parameter eine Zeichenkette in Anführungszeichen, die genau festlegt, welche Bits in welcher Reihenfolge verwendet werden, getrennt von Kommas. Das zuerst genannte Bit wird das signifikanteste (höchstwertige) Bit in der resultierenden Zahl und es wird nicht als Vorzeichen interpretiert. Das zuletzt genannte Bit wird das insignifikanteste Bit der resultierenden Zahl.

Die Bits werden gezählt beginnend mit 0. Bit 0 ist das am wenigsten signifikante Bit des ersten Bytes. Bit 31 ist das signifikanteste Bit des vierten Bytes. Die Definition basiert also auf der little-endian Philosophie.

Zum Beispiel ist
uint_flex "15,14,13,12,11,10,9,8,7,6,5,4,3,2,1,0" "Standard 16-Bit-Integer"
genau das gleiche wie uint16, die gewöhnliche vorzeichenlose 16-Bit-Integer Variable.

uint_flex "31,30,29,28,27,26,25,24,23,22,21,20,19,18,17,16,15,14,13,12,11,10,9,8,7,6,5,4,3,2,1,0" "Standard 32-Bit-Integer"
ist genau das gleiche wie uint32, die gewöhnliche vorzeichenlose 32-Bit-Integer Variable.

Der Vorteil von uint_flex ist aber der, dass die Anzahl, die Position und die Interpretationsreihenfolge aller Bits völlig frei gewählt werden kann. Zum Beispiel erzeugt
uint_flex "7,15,23,31" "Ein ungewöhnlicher 4-Bit-Integer"
einen 4-Bit-Integer aus den jeweils signifikantesten Bits von jedem der vier beteiligten Bytes. Wenn diese vier Bytes beispielsweise den Wert F0 A0 0F 0A = **1**1110000 **1**0100000 **0**0001111 **0**0001010 besitzen, dann gilt: Bit 7 ist 1, Bit 15 ist 1, Bit 23 ist 0 und Bit 31 ist 0. Der resultierende uint_flex ist also 1100 = 1*8 + 1*4 + 0*2 + 0*1 = 12.

Verzeichnis-Browser

Auf logischen Laufwerken und Partitionen, die mit FAT12, FAT16, FAT32, NTFS, Ext2, Ext3, CDFS/ISO 9660/Joliet oder UDF formatiert sind, bietet WinHex einen *Verzeichnis-Browser* an, der der Liste auf der rechten Seite des Windows Explorer ähnelt. Dieser kann mit dem Auswahlkästchen rechts neben dem Zugriffsschalter ein- und ausgeschaltet werden. Der Verzeichnis-Browser listet zuerst existierende Dateien und Verzeichnisse auf, dann gelöschte Dateien und Verzeichnisse. Komprimierte Dateien werden in blauer Schrift angezeigt, verschlüsselte in grüner Schrift (nur NTFS). Klicken Sie Dateien oder Verzeichnisse im Verzeichnis-Browser mit der rechten Maustaste an, um ein Kontextmenü zu erhalten. Dieses enthält Befehle, um eine Datei oder ein Verzeichnis zu öffnen, ein Verzeichnis zu erkunden, den Anfang einer Datei oder eines Verzeichnisses auf dem Datenträger zu finden, den zugehörigen Verzeichniseintrag (FAT) bzw. Datei-Datensatz (NTFS) zu finden, die zugehörigen Cluster in einem separaten Fenster aufzulisten und um auf einfachste Weise eine Datei oder ein Verzeichnis, egal ob gelöscht oder nicht, wiederherzustellen. Mit letzterem können Sie ganze Verzeichnisbäume wiederherstellen. Klicken Sie Dateien oder Verzeichnisse doppelt links an, um mehreres auf einmal zu bewirken (Daten finden, Cluster auflisten und im Fall eines Verzeichnisses dieses erkunden). Wenn Sie in dem separaten Listenfenster Cluster-Nummern doppelt anklicken, navigieren Sie im Disk-Editor dorthin.

Verzeichnis-Browser-Optionen

Gelöschte Dateien und Verzeichnisse werden im Verzeichnis-Browser mit blasseren Icons dargestellt. Fragezeichen-Icons zeigen an, daß der Originalinhalt einer Datei oder eines Verzeichnisses noch immer verfügbar sein kann. Gelöschte Objekte, von denen bekannt ist, daß sie nicht mehr zugreifbar sein (weil entweder ihr erster Cluster in der Zwischenzeit anderweitig verwendet wurde oder weil sie eine Größe von 0 Bytes haben), haben Icons mit einem roten Kreuz.

Der Verzeichnis-Browser kann Dateien und Verzeichnisse aufsteigend oder absteigend sortieren und zeigt das vorhergehende Sortierkriterium mit einem helleren Pfeil weiterhin an. Zum Beispiel, wenn Sie zuerst die Dateinamensspalte anklicken und dann die Dateierweiterungsspalte, werden alle Dateien mit der gleichen Erweiterung intern immer noch nach Namen sortiert.

Auf NTFS-Laufwerken listet der Verzeichnis-Browser alle gelöschten Dateien eines Laufwerks, von denen noch Spuren gefunden werden können, komfortablerweise zusätzlich auch in einem einzigen dedizierten virtuellen Ordner namens »Gelöschte Objekte« auf. Dies sind dieselben Dateien, die auch mit Dateien retten nach Name bei ausgeschalteter »intensiver Suche« auffindbar sind.

Spalten

1. Dateiname: Name der aufgelisteten Datei oder des aufgelisteten Verzeichnisses.
2. Erw.: Dateinamenserweiterung/Dateiendung. Der Teil des Dateinamens, der dem letzten Punkt folgt, sofern vorhanden, wenn weniger als 6 Zeichen lang.
3. Kategorie: Dateityp-Kategorie, zu der die Dateiendung gehört, gemäß Definition in "File Type Categories.txt". (nur forensische Lizenz)
4. Pfad: Pfad der Datei oder des Verzeichnisses. Fängt mit einem umgekehrten Schrägstricht an, wenn der Pfad bekannt ist, relativ zum Stammverzeichnis des Dateisystems, oder mit einem Fragezeichen, wenn der exakte Pfad unbekannt ist.
5. Größe: Größe der Datei oder des Verzeichnisses ohne Schlupf. Auf NTFS wird die Größe von Verzeichnissen nur für Inhaltstabellen aufgeführt.
6. Erzeugung: Zeitpunkt (Datum und Uhrzeit), an dem die Datei oder das Verzeichnis in dem Dateisystem erzeugt wurde. Nicht verfügbar in Linux-Dateisystemen.
7. Änderung: Zeitpunkt (Datum und Uhrzeit), an dem die Datei oder das Verzeichnis in dem Dateisystem zuletzt geändert wurde. Auf FAT ist die Uhrzeit nur auf 2 Sekunden genau. Auf CDFS wird der einzige verfügbare Zeitstempel in dieser Spalte angezeigt, auch wenn er nicht notwendigerweise die letzte Änderung angibt.

8. Zugriff: Zeitpunkt (Datum und Uhrzeit), an dem auf die Datei oder das Verzeichnis in dem Dateisystem zuletzt lesen oder anderweitig zugegriffen wurde. Auf FAT wird nur das Datum gespeichert.
9. Record-Änderung: Zeitpunkt (Datum und Uhrzeit), an dem der FILE-Record (NTFS) bzw. die Inode (Linux-Dateisystem) der Datei oder des Verzeichnisses zuletzt geändert wurde. Dies sind Dateisystem-Datenstrukturen, die Meta-Daten über Dateien enthalten.
10. Löschzeitpunkt: Zeitpunkt (Datum und Uhrzeit), an dem die Datei oder das Verzeichnis in dem Dateisystem gelöscht wurden. Nur auf Linux-Dateisystemen verfügbar.
11. Attr.: DOS/Windows-Attribute auf den Dateisystemen FAT und NTFS. Unix/Linux-Permissions auf den Dateisystemen Ext2/Ext3 und Reiser. Kann zusätzlich einige proprietäre Symbole enthalten. S. u.
12. HFA: Hautfarbenanteil. Optional in Inhaltstabellen verfügbar. Gibt den Prozentsatz der Hautfarben in Bildern an. Nach dieser Spalte zu sortieren ist die effizienteste Vorgehensweise, um Spuren z. B. von Kinderpornographie zu suchen.
13. Hash: Der Hash-Wert einer Datei, verfügbar in Inhaltstabellen, sofern berechnet.
14. Hash-Set: Der Name des Hash-Sets in der internen Hash-Datenbank, in der der Hash-Wert enthalten ist, sofern verfügbar.
15. Kategorie: Die Kategorie des Hash-Sets, in dem der Hash-Wert der Datei, sofern verfügbar, enthalten ist. Entweder "irrelevant" oder "beachtenswert" oder nicht angegeben.

Attribute

A = zu archivieren
R = schreibgeschützt
H = versteckt
S = System
P = Junction-/Reparse-Point
C = auf Dateisystemebene komprimiert
c = in einem Archiv (ZIP, RAR, ...) komprimiert
E = auf Dateisystemebene verschlüsselt
e = in einem Archiv (ZIP, RAR, ...) verschlüsselt
e? = möglicherweise verschlüsselt oder komprimiert laut Entropie-Test

Die eingebaute Prioritätsregel beim Sortieren nach den Attributsspalte in absteigender Reihenfolge lautet wie folgt:

1) alternative Datenströme von NTFS, SUID in Linux-Dateisystemen
2) $EFS-Datenströme von NTFS, Symlinks in Linux-Dateisystemen
3) Nicht-Verzeichnis-INDX-Ströme in NTFS, Special Files in Linux-Dateisystemen
4) NTFS-Dateisystem-Verschlüsselung
5) Positivbefund einer Dateinamens-/Dateityp-Unstimmigkeit (z. B. JPEG-Datei mit .dll-Endung)
6) Negativbefund (z. B. Textdatei ohne bekannte Signatur mit .jpg-Endung)
7) Verschlüsselung auf Benutzerebene (z. B. in einem ZIP-Archiv)
8) Verschlüsselung auf Benutzerebene vermutet (bei Entropietest aufgefallen)
9) Kompression auf Benutzerebene (z. B. in einem ZIP-Archiv)
10) NTFS-Dateisystem-Kompression
11) Junction-/Reparse-Point in NTFS
12) normale Windows-Attributes und Linux-Permissions

Kontextmenü

Der Verzeichnis-Browser kann auch von "Laufwerksinhaltstabelle erstellen" gefüllt werden.

Fallbearbeitung

Die integrierte Umgebung für Computerforensik in WinHex kann nur mit einer forensischen Lizenz benutzt werden. Sie bietet eine komplette Fall-Verwaltung an, automatische Protokoll- und Berichtserstellung und verschiedene zusätzliche Features wie Galerie-Ansicht, Kategorie-Ansicht, Erkennung von Dateiname-Dateityp-Unstimmigkeiten, Erkennung von geschützten Festplattenbereichen und Erkennung von Hautfarben in Bildern.

Wenn Sie WinHex zum ersten Mal starten, werden gefragt, ob Sie die Software mit der forensischen Benutzeroberfläche starten möchten. Das heißt, das Falldaten-Fenster wird angezeigt, WinHex im View-Modus ausgeführt und Sie werden gefragt, ob die Ordner für temporäre Dateien und Falldaten korrekt eingestellt sind, um zu verhindern, daß WinHex Dateien auf das falsche Laufwerk schreibt.

Um an einem Fall zu arbeiten, stellen Sie sicher, daß das Falldaten-Fenster (links im Hauptfenster) sichtbar ist. Wenn es das nicht ist, schalten Sie Ansicht | Anzeigen | Falldaten ein.

Vom Datei-Menü aus können Sie einen neuen Fall erstellen (neu beginnen), einen existierenden Fall öffnen, den aktiven Fall schließen, den aktiven Fall speichern, eine Sicherung des Falls in Form eines ZIP-Archivs erstellen (einschließlich aller verknüpfter Dateien wie Inhaltstabellen und Bildschirmfotos, aber ohne Image-Dateien und wiederhergestellte Dateien), und einen automatischen Bericht zum aktiven Fall erzeugen. Ein Fall wird in einer .xfc-Datei gespeichert (xfc steht für X-Ways Forensics Case) und in einem Unterordner desselben Namens, nur ohne die .xfc-Erweiterung. Dieser Unterordner und dessen Unterordner werden automatisch beim Anlegen des Falls erzeugt. Das Basisordner für Ihre Fälle können Sie unter Allgemeine Optionen auswählen. Es ist nicht erforderlich, einen Fall explizit zu speichern, es sei denn, Sie möchten sicher sein, daß er zu einem bestimmten Zeitpunkt gesichert ist. Ein Fall wird spätestens dann automatisch gespeichert, wenn er geschlossen wird oder Sie das Programm verlassen.

Im Fenster »Eigenschaften« eines Falls können Sie einen Fall nach Ihren Konventionen benennen oder ihm eine Nummer zuweisen. Datum und Zeit der Anlage des Falls werden aufgenommen und angezeigt. Der interne Fall-Dateiname ist ebenfalls zu sehen. Sie können eine Beschreibung des Falls (beliebiger Länge) angeben sowie den Namen des Bearbeiters, dessen Organisation und Anschrift usw. Sie können von hier aus auch die automatische Mitprotokollierung für den Fall aus- oder einschalten. Optional werden immer die Unterverzeichnisse der jeweiligen Asservate im Fallordner als Standard-Ausgabeordner beim Wiederherstellen/Herauskopieren von Dateien aus Dateisystemen vorgeschlagen. Diese Eigenheit können ausschalten, wenn Sie z. B. Dateien von verschiedenen Asservaten in einen einzigen Ausgabeordner kopieren möchten.

Asservate

Der mächtigste Konzept in X-Ways Forensics, welches die systematische Auswertung von Dateien auf Computer-Datenträgern erlaubt, ist die sogenannte Laufwerksinhaltstabelle. Es ist möglich, solche Tabellen für alle Asservate in einem Fall in einem Schritt zu erstellen, und sogar Inhaltstabellen von verschiedenen Asservaten zu einer einzigen, globalen, fallweiten Inhaltstabelle zu verschmelzen. Das Resultat ist eine flache, verzeichnisübergreifende Ansicht aller existierenden und gelöschten Dateien von allen Partitionen, Datenträgern und Image-Dateien, die zum Fall gehören, sortierbar nach verschiedenen Kriterien und durchsuchbar mit einem logischen parallelen Suchalgorithmus.

Um einen Fall komplett zu *löschen*, müssen Sie die .xfc-Datei und den zugehörigen Ordner desselben Namens mit all seinen Unterordnern löschen.

Asservate/Beweisobjekte

Sie können jeden an den Computer angeschlossenen Datenträger (wie Festplatte, Speicherkarte, USB-Stick, CD-ROM, DVD, ...), eine Image-Datei oder eine normale Datei dem aktuellen Fall hinzufügen. Dadurch wird das Objekt permanent mit dem Fall verbunden (es sei denn, Sie entfernen es später wieder aus dem Fall), in der baumartigen Fallstruktur angezeigt und fortan als *Asservat* oder *Beweisobjekt* bezeichnet. Im Fallordner wird für jedes Asservat ein Unterordner angelegt, wo Dateien, die Sie von dem Asservat retten, standardmäßig abgelegt werden, so daß immer offenkundig ist, von welchem Asservat genau (und von welchem) wiederhergestellte Dateien stammen.

Im Fenster der Asservat-Eigenschaften könnenn Sie eine Bezeichnung oder eine Nummer für das Asservat nach Ihren Namenskonventionen eingeben. Datum und Zeit des Zuordnens des Asservats zum aktuellen Fall werden aufgenomme und angezeigt. Die programminterne Bezeichnung eines Asservats wird ebenso angezeigt wie seine Originalgröße in Bytes. Sie können Kommentare beliebiger Länge, die sich auf das Asservat beziehen, eingeben. Eine technische Beschreibung wird von WinHex automatisch hinzugefügt (wie aus dem Datenträger-Detailbericht im Specialist-Menü bekannt). Sie können WinHex einen Hash-Wert (Prüfsumme oder Digest) des Asservats berechnen und später überprüfen lassen, so daß Sie sicherstellen können, daß die Datenauthentizität in der Zwischenzeit nicht beeinträchtigt wurde. MD5-Hashes in Evidence Files werden automatisch beim Hinzufügen zum Fall importiert. Ferner können Sie das automatische Mitprotokollieren für ein bestimmtes Asservat ausschalten, wenn es insgesamt für den Fall eingeschaltet ist.

Folgende Möglichkeiten existieren, eine Datei oder einen Datenträger einem Fall hinzuzufügen: Die »Hinzufügen«-Befehle im Datei-Menü des Falldaten-Fensters, der »Hinzufügen«-Befehl im Kontextmenü der Registerkarte eines Editierfensters und der »Hinzufügen«-Befehl im Kontextmenü eines Objekts im Verzeichnis-Browser.

Unter-Elemente

Mit allen Asservaten/Beweisobjekten sind wiederum weitere Elemente assoziiert. Es gibt eine Liste von Lesezeichen, anfänglich leer, in der Sie eine unbegrenzte Anzahl von besonderen Stellen innerhalb von Asservaten besonders markieren und kommentieren können (s. Positions-Manager). Bis zu 32 *Inhaltstabellen* können mit den Befehlen »Laufwerksinhaltstabelle erstellen« und »Verzeichnisinhaltstabelle erstellen« des Specialist-Menüs dem Asservat hinzugefügt werden. Sie zeigen Dateien in einer einzigen Sicht verzeichnisübergreifend an, optional in Dateityp-Kategorien gruppiert. Vom Kontextmenü eines Asservats aus können Sie auch spezielle für Berichtszwecke gedachte Inhaltstabellen anlegen, die anfänglich leer sind und denen Sie fallrelevante Dateien über das Kontextmenü der Verzeichnis-Browsers (Gruppe Position) hinzufügen können. Mit einem Befehl im Kontextmenü der Berichtstabelle können Sie das Hinzufügen zum Fallbericht ein- und ausschalten.

Des weiteren werden auch die resultierenden Dateien der Extraktion von freiem Laufwerksspeicher, Schlupfspeicher und Text von einem Datenträger (unter Verwendung der entsprechenden Befehle im Specialist-Menü) im Fall-Baum unterhalb des Asservats, zu dem sie gehören, aufgeführt.

Log- & Berichterstellung

Nur mit einer forensischen Lizenz von WinHex verfügbar.

Protokoll-Funktion

Wenn im Fall und in den Asservatseigenschaften eingestellt, protokolliert WinHex beharrliche alle Benutzeraktivitäten mit, wenn der Fall offen/aktiv ist. Das erlaubt es, die Schritte, die Sie zu einem bestimmten Ergebnis geführt haben, auf einfachste Weise nachzuvollziehen, zu reproduzieren und zu dokumentieren, zu Ihrer eigenen Informationen oder für ein Gerichtsverfahren.

Folgende Daten werden aufgenommen:
• wenn Sie einen Menübefehl angewählt haben, der Titel des Befehls (oder zumindest seine Identifikationsnummer) und der Name des aktiven Editierfensters, falls kein Asservat, mit vorangestelltem Schlüsselwort »Menu«,
• wenn ein Meldungsfenster angezeigt wird, dessen Text und welchen Schalter Sie gedrückt haben (OK, Ja, Nein oder Abbrechen), mit vorangestelltem Schlüsselwort »MsgBox«,
• wenn ein kleines Fortschrittsfenster angezeigt wird, dessen Titel (wie etwa »Durchsuche Sektoren...«) und ob der Vorgang vollendet oder vorzeitig abgebrochen wurden, mit vorangestelltem Schlüsselwort »Operation«,
• ein Bildschirmfoto eines jeden angezeigten Dialogfensters mit allen gewählten Optionen für einen ggf. folgenden komplexen Vorgang, vorangehend der Titel dieses Fensters,
• Original-Quellpfad einer jeden wiederhergestellten Datei,
• Zielpfad einer jeden wiederhergestellten Datei, die mit dem Verzeichnis-Browser oder dem Zugriffsschaltermenü wiedergestellt wurde,
• das ausführliche Protokoll, das von Datenträger klonen und Dateien retten nach Type erzeugt wird,
• Ihre eigenen Einträge (freier Text), die Sie mit dem Menübefehl »Protokolleintrag« hinzufügen können, entweder zu dem Fall als ganzes oder zu einem speziellen Asservat.

Alle Aktivitäten werden mit Datum und exakter Uhrzeit erfaßt, intern im Datenformat FILETIME mit einer Genauigkeit von 100-Nanosekunden. Aufzeichnungen von Aktivitäten werden standardmäßig mit dem Fall als Ganzes verknüpft. Aktivitäten, die sich auf ein Asservat beziehen, werden jedoch unterhalb des jeweiligen Asservats aufgezeichnet. Dies bestimmt, wo im Bericht die protokollierten Aktivitäten aufgeführt werden. Bildschirmfotos werden als .png-Dateien im Unterordner »log« eines Fallordners abgelegt. Optional können sie in Schwarz-Weiß konvertiert werden, was erlaubt, sie kostengünstig zusammen mit dem Bericht auszudrucken.

Berichte

Sie können einen Bericht mit dem entsprechenden Befehl im Dateimenü des Falldaten-Fensters erzeugen. Der Bericht wird als HTML-Datei gespeichert und kann daher in einer Vielzahl von Applikationen angezeigt und geöffnet werden. Z. B. können Sie ihn mit Ihrem bevorzugten Internet-Browser ansehen oder in MS Word öffnen und weiterverarbeiten.

Der Bericht beginnt mit den allgemeinen Falldaten, gefolgt von einer Liste von Hyperlinks zu den einzelnen Asservat-Sektionen. Zu jedem Asservat gibt der Bericht wiederum Titel, Beschreibung und andere Details, Ihre Kommentare und Anmerkungen und das asservatbezogene Protokoll aus. Der Bericht endet mit dem allgemeinen Teil des Protokolls.

Interner Viewer

Nur mit einer forensischen Lizenz von WinHex verfügbar. Der interne Viewer kann mit dem Befehl "Einsehen" im Menü Extras und im Kontextmenü des Verzeichnis-Browsers auf eine Datei angewandt werden. Er zeigt Bilddateien verschiedener Formate (s. Galerie-Ansicht) und die innere Struktur von Windows-Registrierungsdateien. Wenn Sie versuchen, eine Datei einzusehen, deren Format nicht vom internen Viewer unterstützt wird, wird statt dessen der erste definierte externe Viewer aufgerufen.

Es gibt eine zusätzliche, externe Dateibetrachtungskomponente, die nahtlos in WinHex und X-Ways Forensics integriert werden kann und es ermöglicht, über 200 (!) Dateiformate (wie zum Beispiel MS Word/Excel/PowerPoint/Access/Works/Outlook, HTML, PDF, CorelDraw, StarOffice, OpenOffice, ...) direkt und auf besonders bequeme Art und Weise einzusehen. Dieses Modul wird allen Besitzern einer forensischen Lizenz zur Verfügung gestellt, deren Lizenz auf Version 12.05 oder später ausgestellt wurde. Weitere Informationen online.

Registry-Viewer

MS Windows führt eine interne Datenbank baumförmiger Struktur (die sogenannte System-Registrierung, engl. Registry), in der alle wichtige Einstellungen des Betriebssystems gespeichert sind. Die Daten sind permanent gespeichert in mehreren Dateien (sogenannte Hives), die eine bestimmte Struktur aufweisen. Mit dem RegistryViewer können Hives angezeigt werden, ohne sie in die aktuellen Datenbankeinträge des eigenen Systems zu importieren. Unterstützt wird die Anzeige von Win9x/Me/NT/2k/XP-Hives. Win9x- und WinMe-Hives befinden sich in den Dateien "user.dat", "system.dat" und ihren Sicherungen. WinNT-, Win2k- und WinXP-Hives befinden sich in der Datei "ntuser.dat" im Benutzerprofil und im Verzeichnis \system32\config.

Es können bis zu 16 verschiedene Hives gleichzeitig im Registry-Viewer angezeigt werden. Allerdings können Win9x/Me- und WinNT/2k/XP-Hives aufgrund unterschiedlicher interner Formate nicht zusammen angezeigt werden. Es wird dann nur der zuletzt geöffnete Hive angezeigt.

Durch Klick mit der rechten Maustaste kann an jeder Stelle im Hauptfenster ein Menü aufgerufen werden, über das man die Befehle "Suchen" und "Weitersuchen" ausführen kann. Beim Suchen kann über einen Auswahldialog festgelegt werden, nach welchem Ausdruck gesucht werden soll, und ob der Suchausdruck in den Schlüsselnamen oder in den Namen oder den Werten (oder in allem) gesucht werden soll. Die Suche beginnt am Anfang und erstreckt sich über alle geöffneten Hives. Mit "Weitersuchen" kann der nächste Treffer nach einem bereits gefundenen Treffer gesucht werden. (Das zu der Zeit ausgewählte Element hat keinen Einfluß darauf, von wo aus weitergesucht wird). Im rechten Fenster kann durch Rechtsklick im Menü weiterhin "Kopieren" ausgewählt werden, wodurch sich der Wert des ausgewählten Elements in die Zwischenablage kopieren läßt.

Registry-Berichte automatisch erstellen

Laufwerksinhaltstabelle

Erfordert eine Specialist- oder forensische Lizenz. Mit dem Befehl »Laufwerksinhaltstabelle erstellen« im Specialist-Menü erstellen Sie einen »Katalog« aller existierender und/oder noch spurenweise zu findender gelöschter/verlorener Dateien und Verzeichnisse, mit benutzerkonfigurierten Informationen wie Dateiattributen, allen verfügbaren Datums- und Zeitangaben, Größe, belegte Cluster, Hash (Prüfsumme oder Digest), alternative Datenströme (ADS, welche versteckte Daten enthalten, nur auf NTFS-Laufwerken) usw. Extrem nützlich, um den Inhalt eines Datenträgers systematisch zu untersuchen. Erlaubt es auch, die Suche durch Angabe einer Maske (wie *.jpg;*.gif) auf Dateien eines bestimmten Namens zu beschränken. Bis zu zwei Sternchen sind erlaubt, wenn sie am Anfang und Ende der Maske vorkommen. *Ausschließen* können Sie Dateien mit einer Maske, die mit einem Doppelpunkt (:) beginnt. Um z. B. alle Dateien außer NTFS-Systemdateien zu erfassen, geben Sie folgenden Ausdruck an: *;:$*. Alle Dateien mit Namen, die mit "A" anfangen und nicht das Wort "Garten" enthalten: A*;:*Garten*.

FAT: Die Option »**Dateisystem-Struktur-Suche besonders intensiv**« sucht nach verwaisten Unterverzeichnissen, also Unterverzeichnissen, die von keinem anderen Verzeichnis mehr referenziert werden.
NTFS: Die Option »Dateisystem-Struktur-Suche besonders intensiv« sucht nach FILE-Records in Sektoren, die nicht der MFT in ihrer aktuellen Größe und Lage angehören. Solche FILE-Records können z. B. gefunden werden, wenn eine Partition neu erstellen, neu formatiert, verschoben, vergrößert, verkleinert oder defragmentiert wurde.
Die Option »**Datei-Header-Suche in freien Clustern**« führt dazu, daß solche Dateien mit in die Liste aufgenommen werden, die in freiem Laufwerksspeicher anhand ihrer Datei-Header-Signatur gefunden werden können. Damit dies möglich ist, werden Sie gefragt, welche bestimmten Dateitypen erkannt werden sollen, welche Ausgabenamen den Dateien gegeben werden sollen usw., wie von Dateien retten nach Typ bekannt. Wenn diese Dateien auch anhand von Dateisystem-Datenstrukturen gefunden werden, werden sie tatsächlich zweimal ausgegeben, einmal mit korrektem Namen und korrekter Größe, und einmal mit einem generischen Namen und der Größe wie sie vom Mechanismus »Dateien retten nach Typ« erkannt wird. Wenn sie allerdings nicht mehr von Dateisystem-Datenstrukturen referenziert werden, ist diese Option die einzige Möglichkeit, sie in der Tabelle mit aufzulisten.

Das **Resultat** kann in eine **Textdatei** mit Tab-Trennzeichen geschrieben, was nützlich ist für einen Import und weitere Bearbeitung in einer Datenbank-Software oder MS Excel. Wenn MS Excel auf Ihrem Computer nicht gefunden werden kann oder wenn Sie die Umschalt-Taste Ihrer Tastatur gedrückt halten, können Sie eine anderes Programm auswählen. Das Sortieren nach Datum & Zeit gibt einen guten Überblick darüber, wozu ein Datenträger zu welcher Zeit benutzt wurde. Das NTFS-Attribut "verschlüsselt" könnte z. B. schnell die wichtigsten zu untersuchen-den Dateien bei einer forensischen Analyse enthüllen.

Das **Resultat** kann auch in den **Verzeichnisbrowser** ausgegeben werden. Das heißt, Sie bekommen eine Übersicht über alle Dateien auf einem logischen Laufwerk oder einer Partition direkt in WinHex. Dabei können Sie sortieren nach Datum, Dateinamenserweiterung usw., zu den Clustern, in denen Dateien gespeichert ist, navigieren, Dateien retten/extrahieren, irrelevante Einträge aus der Liste löschen usw. Während der Verzeichnisbrowser zwar ein interaktives Vorgehen erlaubt, zeigt er allerdings keine Hash-Werte. Blaue Einträge im Verzeichnisbrowser zeigen komprimierte Dateien an ("C" in der Attr.-Spalte = auf NTFS-Dateisystemebene komprimierte Dateien, "c" in the Attr.-Spalte = Dateien innerhalb von ZIP- u. ä Archiven), grüne Einträge zeigen verschlüsselte Dateien an ("E" in der Attr.-Spalte = auf NTFS-Dateisystemebene verschlüsselte Dateien, "e" = in Archiven verschlüsselte Dateien). Die Rotfärbung von Einträgen wird ebenfalls in der Attr.-Spalte erklärt: Entweder es handelt sich um Dateinamens-/Dateityp-Unstimmigkeiten, oder alternative Datenströme (ADS) oder benannte Index-Ströme (INDX) in NTFS, die separat aufgelistet werden. Nur mit einer forensischen Lizenz können Dateien in **ZIP-, RAR-**, ARJ-, GZ-, TAR- und BZIP-**Archiven** optional separat aufgelistet und untersucht werden, sofern die Archive nicht verschlüsselt sind. Der Inhalt von Archiven in Archiven kann auch mit ausgegeben werden, aber keine weitere Verschachtelungsebene. Wenn Sie irrelevante Einträge aus

einer Inhaltstabelle löschen, die mit einem Asservat verknüpft ist, kann WinHex diese Änderungen in Inhaltstabellendatei speichern.

Eine forensische Lizenz erlaubt es, **Dateinamens-/**Dateityp-**Unstimmigkeiten** in Dateien aufzudecken. Wenn z. B. jemand ein belastendes JPEG-Bild durch Umbenennen in "Rechnung.xls" (falsche Dateiendung) versteckt hat, wird der erkannte Dateityp "JPEG!" in der Spalte "Mismatch" in der Textdatei-Ausgabe eingetragen und die Datei im Verzeichnis-Browser ein zweites Mal mit der vermuteten korrekte Dateinamenserweiterung und in Rot aufgelistet. Wenn eine Datei mit bekannter Endung (z. B. .jpg) keine bekannte Signatur aufweist, wird das in der Spalte "Mismatch" mit dem Wort "unknown" signalisiert. Die Dateisignaturen und Namensendungen, die für die Erkennung von Unstimmigkeiten verwendet werden, sind in der begleitenden Dateityp-Definitionsdatei definiert. Please note that the link between the current data in unallocated clusters and *deleted* files and their filenames is weak, so false alerts might be displayed if a deleted file's clusters have been re-allocated to another file of a different type in the meantime.

Eine forensische Lizenz erlaubt es auch, alle Dateien in einer **Kategorie-Ansicht** im Verzeichnis-Browser darzustellen (verfügbar nur, wenn der zugehörige Datenträger einem Fall zugeordnet ist). Das bedeutet, daß die Dateien anhand ihrer Dateikategorie gruppiert werden, also in Gruppen wie "Dokumente", "Internet", "Bilder", "Multimedia" usw. eingeteilt werden. Dies ist z. B. nützlich, wenn Sie eine Liste oder Galerieansicht aller Bilder auf einem Laufwerk verzeichnisübergreifend benötigen. Dateien werden einer Kategorie anhand ihrer Dateiendung zugeordnet. Die Zusammenhänge zwischen Dateiendung und Dateikategorie sind in der begleitenden Datei "File Type Categories.txt" definiert, die Sie beliebig gemäß Ihrer Anforderungen anpassen können. Sie wird bei Programmstart geladen. Alle Dateien, die keiner Kategorie zugeordnet sind, landen in der Kategorie "Miscellaneous".

Des weiteren ermöglicht es eine forensische Lizenz, den **Anteil von Hautfarben** in Bildern in Prozent zu berechnen. Dies kann für dieselben Dateitypen geschehen, die auch in der Galerieansicht unterstützt werden. Wenn z. B. ein Ermittler nach Spuren von Kinderpornographie sucht, kann das Sortieren aller Bilder auf einem Laufwerk nach Hautfarbenanteil (HFA) die Arbeit stark beschleunigen, weil es das Prüfen der großen Masse von Bildern mit 0-9% HFA überflüssig macht (etwa tausende kleine Symbole im Browser-Cache). Bitte beachten Sie, daß es falsche Treffer geben kann, also hautartige Farben auf einer Oberfläche, die keine Haut ist. Bilder, die nicht fehlerlos auf Hautfarben überprüft werden können (da z. B. zu groß, defekte Datei oder Schwarz-Weiß-Bild), werden mit einem Fragezeichen statt HFA aufgelistet.

Eine forensische Lizenz erlaubt es, optional einen **Entropietest** an allen Dateien durchzuführen, um zu prüfen, ob sie verschlüsselt oder komprimiert sind. Wenn der Test positiv ist (der Test einen bestimmten Schwellwert überschreitet), wird die betreffende Datei mit dem Hinweis "e?" in der Attributsspalte versehen, um anzuzeigen, daß sie vielleicht besondere Aufmerksamkeit verdient. Der Entropietest wird nicht angewandt auf ZIP-, RAR-, TAR-, GZ-, BZ-, 7Z-, ARJ-, JPG-, PNG-, GIF-, TIF-, MP3- und MPG-Dateien, von denen bekannt ist, daß sie intern komprimiert sind. Dieser Test wird nicht benötigt, um festzustellen, daß Dateien auf NTFS-Dateisystemebene oder innerhalb von Archiven verschlüsselt sind.

Für alle in eine Inhaltstabelle ausgegeben Dateien können **Hash-Werte** berechnet werden. Zusätzlich erlauben es forensische Lizenzen, Hash-Werte mit individuell ausgewählten (oder einfach allen) Hash-Sets in der internen Hash-Datenbank **abzugleichen**. Dabei gibt es drei Möglichkeiten:
1) Die Hash-Werte werden mit der Datenbank abgeglichen, aber es wird nichts herausgefiltert, sondern es werden alle Dateien ausgegeben. Übereinstimmungen mit der Datenbank werden in den Spalten "Hash-Set" und "Kategorie" des Verzeichnis-Browsers kenntlich gemacht. Nach diesen Spalten können Sie sortieren und so bekanntermaßen irrelevante Dateien manuell herausfiltern oder verdächtige Dateien gezielt untersuchen.
2) Nur solche Dateien werden ausgegeben, die entweder unbekannt, also nicht in der Hash-Datenbank verzeichnet, oder als verdächtig bekannt sind. Bekanntermaßen irrelevante Dateien werden nicht ausgegeben, also automatisch herausgefiltert.
3) Nur solche Dateien werden ausgegeben, die der Datenbank als verdächtig bekannt sind. Sowohl bekanntermaßen irrelevante Dateien als auch der Datenbank nicht bekannte Dateien werden herausgefiltert.

Unterschiede zwischen WinHex und X-Ways Forensics

WinHex und X-Ways Forensics sind identisch (und können mit derselben forensischen Lizenz betrieben werden) bis auf die folgenden Unterschiede:

• Die Nutzeroberfläche von WinHex (winhex.exe) identifiziert sich immer als WinHex, die von X-Ways Forensics (xwforensics.exe) als X-Ways Forensics. Die Programmhilfe und das Benutzerhandbuch verwenden allerdings zumeist statisch "WinHex".

• X-Ways Forensics erlaubt das Öffnen von Dateien im Editiermodus nur dann, wenn diese im Fallverzeichnis des aktuellen Falles, einem seiner Unterverzeichnisse oder im allgemeinen Temp-Verzeichnis liegen, z. B. zur Dekodierung, Entschlüsselung oder Umwandlung. Alle übrigen Dateien, Image-Dateien, virtueller Speicher und Datenträger im allgemeinen, werden ausschließlich nur lesend geöffnet, um korrekte forensische Methodik zu unterstützen, die keinerlei Veränderung von Beweisen duldet. Entsprechend gelten nur die Verzeichnisse des aktuellen Falles und das allgemeine Temp-Verzeichnis als legitime Zielverzeichnisse, in denen Dateien gespeichert werden dürfen. Dieser strenge Schreibschutz in X-Ways Forensics stellt sicher, dass die Original-Asservate nicht versehentlich verändert werden können, was vor Gericht von wesentlicher Bedeutung ist.

• Bestimmte Dateien (Details unter http://www.x-ways.net/winhex/setup-d.html) sind nicht Teil des WinHex-Downloads, aber Inhaber einer forensischen Lizenz können diese von X-Ways Forensics kopieren, um den vollen Funktionsumfang von X-Ways Forensics auch in WinHex zur Verfügung zu haben. Die Verwendung von WinHex anstelle von X-Ways Forensics kann wünschenswert sein, wenn keine strengen forensischen Methoden zu beachten sind und Dateien, Datenträger oder Images intensiver bearbeitet werden sollen, z. B. um einen Bootsektor zu reparieren, oder wenn man mit mehreren Kopien arbeitet, von denen eine als Arbeitskopie deklariert und zum Schreiben freigegeben wurde.

Wenn Sie Dateien aus X-Ways Forensics mit WinHex verwenden, stellen Sie bitte sicher, daß die Versionsnummern von X-Ways Forensics und WinHex exakt identisch sind. Wenn Sie das eine Programm herunterladen, laden Sie einfach sofort danach auch das andere herunter, um dies sicherzustellen. Auf die Art ist es auch problemlos möglich, beide Programme in das gleiche Verzeichnis zu installieren.

Automatischer Registry-Bericht

WinHex kann über den Befehl "Bericht erzeugen" im Rechts-Klick-Menü des Registry-Viewer für die geöffneten Hives einen Bericht im HTML-Format erstellen, der potentiell relevante Schlüssel aus der Registry mit ihren Werten auflistet. Die Registry-Dateien müssen ihren Originalnamen haben, sonst kann der Bericht u. U. nicht erstellt werden. Die zu untersuchenden Schlüssel sind in einer Datei "Reg Report Keys.txt" gespeichert, die nach eigenen Bedürfnissen angepaßt oder erweitert werden kann.

Das Format der Einträge in "Reg Report Keys.txt"

(*Betriebssystemkürzel*) (*Tabulator*) (*Schlüsselpfad*) (*Tabulator*) (*Beschreibung*) (*Zeilenvorschub*)

Betriebssystemkürzel:
9x: Windows 9x/Me
NT: Windows NT/2000/XP

Schlüsselpfad:
Kompletter Pfad des Registrierungsschlüssels

HKLM entspricht HKEY_LOCAL_MACHINE
HKCU entspricht HKEY_CURRENT_USER

Wenn ein "*" als Platzhalter im letzten Teilpfad verwendet wird, werden alle Pfade auf dieser Verzweigungsebene und allen tieferen Verzweigungsebenen mit ihren Werten in dem Bericht mitaufgelistet.

Beispiel:
NT HKLM\Software\Microsoft\Windows\CurrentVersion* der gesamte Windows-Unterzweig

Wenn ein bestimmter Wert von Interesse ist, der in allen Unterschlüsseln eines bestimmten Schlüssels vorkommt, dann können die Unterschlüssel abermals durch ein "*" ersetzt werden und der konkrete Wert dahinter angegeben werden.

Beispiel:
9x HKCU\Identities*\UserID UserID-Wert von allen Identitäten

Der erzeugte Bericht enthält jeweils den Schlüsselpfad mit der zugehörigen Zeitangabe der letzten Änderung (nur Windows NT/2000/XP), den Dateinamen des Hives, aus dem dieser Schlüssel ist, die Beschreibung aus "Reg Report Keys.txt" und den Wert.

Modus-Schalter

Beim Untersuchen eines logischen Laufwerks, einer Partition oder einer Image-Datei mit einem Dateisystem, das von WinHex unterstützt wird, gibt es vier Schalter, die die Anzeige in der unteren Hälfte des Fensters (unter dem Verzeichnis-Browser) bestimmen.

Sektoren

Die Standard-Ansicht, die die binären Daten in allen Sektoren als Hexadezimal-Code, ASCII-Text oder als beides anzeigt.

Vorschau

Prüft die Signature der aktuell im Verzeichnis-Browser ausgewählten Datei. Wenn als Bild erkannt (unterstützte Type s. u.), wird es als solches angezeigt, sonst wird ein ASCII-Text-Extrakt vom Anfang der Datei dargestellt. Das Ergebnis der Signaturprüfung (ob die Signatur zur Dateiendung paßt oder nicht) wird in der Statusleiste angezeigt. Durch Doppelklick auf eine Miniaturansicht erhalten Sie eine Ansicht des Bildes in voller Größe, wobei Sie mit den Tasten + und - hinein- und wieder herauszoomen können. Selbst unvollständige Bilder (Datei z. B. wegen Fragmentierung nur partiell korrekt gerettet) können normalerweise teilweise angezeigt werden.

Galerie

Prüft die Signatur aller Dateien im gegenwärtig sichtbaren Ausschnitt des Verzeichnis-Browsers. Wenn als Bild erkannt, wird eine Miniaturansicht angezeigt, sonst ein Kurzinformation (Dateiname, Größe, Signatur). Indem Sie im Verzeichnis-Browser hoch- oder herunterrollen, bewegen Sie auch die Bilderliste im Galerie-Fenster. Sie können das Verzeichnis wechseln auch während die Miniaturansichten noch erzeugt werden. Durch Doppelklick auf eine Miniaturansicht erhalten Sie eine Ansicht des Bildes in voller Größe, wobei Sie mit den Tasten + und - hinein- und wieder herauszoomen können. Selbst unvollständige Bilder (Datei z. B. wegen Fragmentierung nur partiell korrekt gerettet) können normalerweise teilweise angezeigt werden.

Die Galerie-Ansicht zeigt Dateien mit den folgenden Dateiendungen an: BMP, JPG/JPEG, JPEG 2000, PNG, GIF, TIF, TGA, PCX, WMF, EMF, MNG, JBG.

Kalender (Zeitlinien-Ansicht)

Gibt einen komfortablen Überblick darüber, wann die Dateien und Verzeichnisse, die im Verzeichnis-Browser ausgewählt sind, im Dateisystem erzeugt (rot) wurden, zuletzt geändert wurden (blau) und wann auf sie zuletzt zugegriffen wurde (grün). Jeder Tag mit einem Zeitstempel für zumindest eine Datei oder ein Verzeichnis wird im Kalender mit der entsprechenden Farbe gefüllt. Wochenenden (Samstage und Sonntage) werden besonders markiert. Bewegen Sie den Maus-Cursor über einen Tag, um herauszufinden, welche Dateien genau dort repräsentiert sind, und um die jeweiligen Uhrzeiten zu sehen. Wenn die Liste für einen bestimmten Tag zu lang ist, um vollständig angezeigt zu werden, können Sie immer noch den Verzeichnis-Browser geeignet sortieren und dort alles herausfinden.

Beispiel: In welchem Zeitraum wurden JPEG-Dateien auf einem Laufwerk angelegt? Klicken Sie entweder mit der rechten Maustaste das Stammverzeichnis im Verzeichnisbaum (Falldatenfenster) an, um alle existierenden Dateien rekursiv aufzulisten, oder erstellen Sie eine Laufwerksinhaltstabelle. Dann sortieren Sie nach Dateinamenserweiterung, markieren alle JPEG-Dateien, schalten die Kalenderansicht an und halten nach den roten Balken Ausschau.

Dateityp-Definitionen

"File Type Signatures.txt" ist eine durch Tabulatorzeichen in Spalten aufgeteilte Textdatei, die als Datenbank von Dateityp-Definitionen fungiert. Sie wird verwendet bei der Erzeugung von Inhaltstabellen und beim Befehl Dateien retten nach Typ. Sie kann bis zu 255 Einträge enthalten.

WinHex ist werksseitig mit der Kenntnis verschiedenener Dateiheader-Signaturen ausgestattet. Sie können diese Dateityp-Definitionen aber beliebig an Ihren Bedarf anpassen und erweitern. Klicken Sie den Schalter "Typ-Definition" bzw. "Signaturen" an, um die Datei "File Type Signatures.txt" zu editieren. Standardmäßig öffnet WinHex die Datei in MS Excel. Das ist bequem, weil die Datei aus Spalten besteht, die durch Tabulatorzeichen getrennt sind. Wenn Sie die Datei mit einem Text-Editor verändern, stellen Sie sicher, daß die Tabulatorzeichen erhalten bleiben, denn WinHex verläßt sich beim Interpretieren der Datei auf deren Vorhandensein. MS Excel erhält sie automatisch. Nach dem Editieren der Dateityp-Definitionen müssen Sie das Dialogfenster schließen und erneut aufrufen, damit Sie die Änderungen in der Dateityp-Definitionsdatei sehen.

1. Spalte: File Type

Eine menschenlesbare Bezeichnung des Dateityps, z.B. "JPEG". Nur die ersten 19 Zeichen werden berücksichtigt.

2. Spalte: Extensions

Einer oder mehrere Datei-Erweiterungen, die typischerweise für diesen Dateityp benutzt werden, z.B. "jpg;jpeg;jpe". Geben Sie die üblichste Erweiterung zuerst an, denn diese wird für die Benennung wiederhergestellter Dateien verwendet. Nur die ersten 45 Zeichen werden berücksichtigt.

3. Spalte: Header

Eine eindeutige Header-Signatur, anhand derer Dateien dieses Dateityps erkannt werden können. Signaturen können Sie entweder als Folge von ASCII-Zeichen oder in hexadezimaler Notation (z. B. 0xFFD8FF) angeben. Um überhaupt geeignete charakteristische Dateiheader-Signaturen herauszufinden, öffnen Sie ein paar existierende Dateien des gewünschten Typs in WinHex und halten Sie nach übereinstimmenden Bytewerten nah dem Anfang der Dateien an identischen Offsets Ausschau. Nur die ersten 16 Zeichen werden berücksichtigt.

4. Spalte: Offset

Der relative Offset innerhalb einer Datei, an dem die Signatur auftritt. Oft einfach 0.

5. Spalte: Footer

Optional. Eine Signatur (Folge konstanter Byte-Werte), die das Ende einer Datei verläßlich anzeigt. Das kann Ihnen helfen, eine Rettung mit der korrekten Dateigröße zu erzwingen. Der Algorithmus sucht aber hinter dem Header nicht weiter nach Footern als durch die in Bytes angegebene maximale Dateigröße bestimmt. Nur die ersten 16 Zeichen werden berücksichtigt.

6. Spalte: Default in KB

Optional. Eine dateitypspezifische maximale Dateigröße in KB, die die globale Maximalgröße aufheben kann, die im Fenster für die Datenrettung nach Typ angegeben wird. Nützlich, da beispielsweise ein MPEG-Video ca. 1 GB groß sein könnte während eine Windows Symboldatei (.ico) ca. 1 KB groß sein könnte.

Verzeichnis-Browser-Optionen

• Das Gruppieren von Dateien und Verzeichnisse im Verzeichnis-Browser ist optional.

• Das Gruppieren existenter und gelöschter Objekte im Verzeichnis-Browser ist optional.

• Der Verzeichnis-Browser kann optional mit Gitternetzlinien angezeigt werden.

• In neu erstellten Laufwerksinhaltstabellen für NTFS-Partitionen können optional $EFS-Attribute aufgelistet werden und INDX-Ströme, die keine Verzeichnisse sind.

• Standardmäßig werden über den Verzeichnis-Browser wiederhergestellte Dateien im Ausgabeordner incl. Originalpfad neu angelegt.

• Dateien können optional über den Verzeichnisbrowser inklusive ihrem Schlupfspeicher geöffnet und durchsucht werden (verfügbar für FAT, NTFS, Ext2/Ext3 und ReiserFS).

• Das Auflisten gelöschter Dateien und Verzeichnisse im Verzeichnisbrowser ist optional.

• Verzeichnisleichen in den Dateisystemen Ext2 und Ext3 werden optional ausgegeben. Gemeint sind gelöschte Dateien, von denen nur noch der Name bekannt ist, nicht jedoch ursprüngliche Daten, Größe oder Zeitstempel.

• Diverse Spalten im Verzeichnisbrowser sind optional. Sie werden angezeigt, wenn sie eine Spaltenbreite größer 0 haben, oder versteckt, wenn ihre Breite 0 ist.

Logische Suche

Das Kontextmenü des Verzeichnisbrowsers ermöglicht *logische* parallele Suchen in Dateien und Verzeichnissen, die im Verzeichnisbrowser ausgewählt wurden (nur mit Specialist- oder forensischer Lizenz).

Vorteile:

+ Der Suchbereich kann auf bestimmte Dateien und Verzeichnisse eingeschränkt werden, auch auf Dateien, die in einer Inhaltstabelle enthalten sind.

+ Die Suche in Dateien (üblicherweise = in den Clusterketten der jeweiligen Dateien) findet Suchbegriffe auch dann, wenn der Suchbegriff zufällig physisch durch die Dateifragmentierung zerschnitten ist (passiert am Ende und am Anfang nicht zusammenhängender Cluster), und selbst dann, wenn die Datei auf dem NTFS-Dateisystem-Level komprimiert ist und optional sogar dann, wenn sie Teil eines Archivs ist (ZIP, RAR, GZ, TAR, BZ2, 7Z und ARJ, falls nicht verschlüsselt, nur mit forensischer Lizenz).

+ Der Text, der in Dateien der Formate PDF (Adobe), WPD (Corel WordPerfect), CDR (Corel Draw) oder VSD (Visio) enthalten ist, kann automatisch extrahiert und dekodiert werden, bevor er durchsucht wird, so daß deren Klartext ebenfalls durchsucht werden kann. Potentielle Suchtreffer in solchen Dateien würden sonst übersehen, da diese Dateitypen Text üblicherweise auf eine besonders codierte, verschlüsselte oder anderweitig unlesbare Art speichern. Diese Funktion benötigt eine aktivierte externe Viewer-Komponente für die Dekodierung und die Textextraktion.

+ Dateien, die den Suchbegriff enthalten, können automatisch geöffnet oder zu einer gesonderten Inhaltstabelle hinzugefügt werden.

Nicht-allokierte Cluster können in die logische Suche einbezogen werden, indem die fiktive Datei "Freier Speicher" im Stammverzeichnis einbezogen wird, die Dateisystembereiche, indem die fiktive Datei gleichen Namens einbezogen wird. Schlupfspeicher wird in Abhängigkeit von den Verzeichnis-Browser-Optionen berücksichtigt.

- Nur eine physische Suche kann den Übergang von Schlupfspeicher in den direkt darauf folgenden freien Speicher abdecken.

Suchoptionen

Hash-Datenbank

Nur mit forensischer Lizenz verfügbar. Die interne Hash-Datenbank besteht, sofern einmal erstellt, aus 257 binären Dateien mit der Endung .xhd (X-Ways Hash Database). Der Speicherordner dafür kann im Dialogfenster Allgemeine Optionen festgelegt werden. Die Hash-Datenbank ist auf sehr effiziente Weise organisiert, so daß die Performanz beim Abgleich von Hash-Werten maximiert wird. Sie selbst entscheiden, auf welchem Hashtyp die Datenbank aufbauen soll (MD5, SHA-1, SHA-256, ...).

Jeder Hash-Wert in der Datenbank gehört zu einem oder mehreren Hash-Sets. Jedes Hash-Set gehört entweder zur Kategorie “bekanntermaßen gutartig”/“harmlos”/“irrelevant” oder “bekanntermaßen bösartig”/“relevant”/“beachtenswert”.

Hash-Werte von Dateien können berechnet und mit der Hash-Datenbank abgeglichen werden, wenn Sie eine Inhaltstabelle erstellen. Die optionalen Spalten "Hash-Set" und "Kategorie" im Verzeichnis-Browser zeigen dann an, welche Dateien zu welchem Hash-Set und welcher Kategorie gehören, was es Ihnen ermöglicht, nach diesen Aspekten zu sortieren und irrelevante Dateien einfach herauszufiltern.

Das Extras-Menü erlaubt es,
- die aktive Hash-Datenbank zu verwalten: Erstellen Sie eine leere, neue Datenbank, sehen Sie die Liste von Hash-Sets ein, benennen Sie Hash-Sets um oder löschen Sie existierende Hash-Sets.
- einzelne Hash-Sets zu importieren (Textdateien der Formate NSRL RDS 2.x, HashKeeper und ILook werden unterstützt)
- alle Hash-Sets in einem bestimmten Ordner und dessen Unterordnern zu importieren (dito), optional in ein einziges internes Hash-Set, dessen Namen Sie angeben können
- die aktive Hash-Datenbank zu löschen, z. B. um mit einer jungfräulichen Datenbank von Grund auf neu zu beginnen und/oder einen neuen Hashtyp festzulegen.

Der Befehl "Hash-Set erzeugen" im Kontextmenü des Verzeichnis-Browsers erlaubt es Ihnen, Ihre eigenen Hash-Sets in der internen Hash-Datenbank zu erstellen. Die Hash-Datenbank kann bis zu 65.535 Hash-Sets verwalten. Zukünftige Versionen werden das Exportieren von Hash-Sets im Format NSRL RDS unterstützen.

Kontextmenü des Verzeichnis-Browsers

Das Kontextmenü des Verzeichnis-Browsers erlaubt es dem Nutzer, direkt mit den aktuell ausgewählten Dateien zu interagieren. Es gibt eine Reihe von Kommandos, die in Abhängigkeit von den aktuell ausgewählten Objekten verfügbar sind. Ein Doppelklick auf Dateien oder Verzeichnisse löst je nach Kontext entweder "Einsehen", "Erkunden" oder den Aufruf des verknüpften externen Programms aus.

Einsehen

Hiermit können Windows Registry-Dateien und diverse Bilddateiformate mit dem internen Viewer von WinHex eingesehen werden. Für alle anderen Dateien hängt die Funktionsweise dieses Kommandos von den installierten Komponenten ab: Falls X-Ways Trace installiert und die Datei entweder eine "info2"-Datei des Windows-Papierkorbs oder eine "index.dat" des Internet Explorers ist, wird für diese Datei X-Ways Trace aufgerufen. Falls die externe Viewer-Komponente von X-Ways Forensics aktiv ist, werden alle anderen Dateien an diese Komponente übergeben. Falls nicht, wird stattdessen das erste installierte externe Programm aufgerufen.

Ausnahmen zu allem bisher gesagten sind Dateien mit mehr als 2 GB Größe und die NTFS-Systemdateien. Diese werden immer in Datenfenstern geöffnet.

Erkunden

Nur verfügbar für Verzeichnisse und Archive (ZIP, RAR, TAR...): Mit diesem Kommando navigiert man in diese mit dem Verzeichnis-Browser hinein. Ein Doppelklick auf ein Archiv oder Verzeichnis hat dieselbe Wirkung. Ein Kommando, das gleichzeitig alle Inhalte eines Verzeichnisses und aller seiner Unterverzeichnisse auflistet, finden Sie stattdessen im Kontextmenü des Verzeichnisbaums (im Falldatenfenster, "Rekursiv erkunden").

Externe Programme

Gezielt die selektierten Dateien an eines der externen Programme schicken, die aktuell konfiguriert sind, oder an das Programm, das in der aktuellen Windows-Installation mit dem Dateityp verknüpft ist. Diese Verknüpfung wird ausgewertet auf der Basis der Datei-Erweiterung, wie dies in Windows üblich ist.

Position

Die Gruppe der Kommandos im Positionsmenü ermöglicht Interaktionen mit den aktuell ausgewählten Dateien auf einer tendentiell eher technischen Ebene. Es ermöglicht, den ersten Cluster einer Datei bzw. eines Verzeichnisses auf der Platte in der Sektoransicht direkt aufzusuchen, auf die Metainformationen wie MFT-Record in NTFS oder die Inode in Ext2/Ext3 zuzugreifen und auch die Dateien nach ihrer physikalischen Rangfolge auf der Platte zu sortieren: "Nach Eintragsadresse sortieren" (FAT), "Nach Inode-Adresse sortieren" (Ext2/Ext3) bzw. "Nach Record-Adresse sortieren" (NTFS) ermöglichen es, die Dateien und Verzeichnisse in der Reihenfolge zu sehen, in der diese physisch in den Datenstrukturen des Dateisystems (Verzeichniseinträge, die MFT oder die Inode-Tabellen) erscheinen.

Im Positionsmenü kann man außerdem für eine Datei bzw. ein Verzeichnis die Cluster-Liste aufrufen, d.h. das Cluster-Listen-Fenster wird geöffnet und mit der Cluster-Liste des gewählten Objektes befüllt. Ebenfalls im Positionsmenü kann man die gewählten Objekte aus der Liste löschen lassen, was insbesondere im Zusammenhang mit Inhaltstabellen interessant ist. Das Löschen von Objekten aus einer Inhaltstabelle kann dauerhaft gespeichert werden, indem man die Floppy-Diskette anklickt, die nach der Löschung in der Kopfzeile des Verzeichnisbrowsers erscheint. Das Menü ermöglicht es auch, Dateien Inhaltstabellen hinzuzufügen oder dorthin zu verschieben, die speziell zu Berichtszwecken angelegt wurden.

Wiederherstellen/Kopieren

Ermöglicht es, die ausgewählten Dateien von ihrer aktuellen Position, z.B. aus einer interpretierten Image-Datei oder einer lokalen Platte heraus, an einen beliebigen Ort zu kopieren, der für einen Standard-Windows-Dateidialog erreichbar ist. Dies kann sowohl auf existierende als auch auf gelöschte Dateien angewandt werden. Wenn ein Fall mit eingeschaltetem Logging aktiv ist, wird der Kopier-/Wiederherstellungsvorgang im Fallbericht dokumentiert. Sowohl der Quell- als auch der Zielpfad werden festgehalten.

Als wichtig kennzeichnen/Markierung aufheben

Im Verzeichnis-Browser eines Asservats kann man als wichtig markieren. Dadurch werden sie visuell hervorgehoben und einer spezielle Inhaltstabelle hinzugefügt. Die Dateien in dieser Tabelle werden dann auch im Fallbericht aufgelistet und es ist bequem möglich, sie später in einem einzigen Durchgang wiederherzustellen bzw. zu kopieren oder eine Galerie-Übersicht über speziell diese Dateien zu bekommen.

Die visuelle Markierung kann später wieder entfernt per Kontextmenü entfernt werden. Aus der Tabelle wichtiger Dateien können Einträge durch Löschen entfernt werden, über den Kontextmenübefehl "Aus Liste löschen" oder durch Drücken der Entf-Taste auf der Tastatur. Dies hebt auch die Markierung auf. Die geänderte Tabelle kann durch Anklicken des Disketten-Icons gespeichert werden.

Aktivem Fall hinzufügen

Führt dieselbe Operation durch wie Wiederherstellen/Kopieren, jedoch werden die resultierenden Dateien gleichzeitig dem aktiven Fall als Asservate hinzugefügt.

Logische Suche

Hash-Set erzeugen

Erzeugt ein Hash-Set der aktuell ausgewählten Dateien und Verzeichnisse und ihrer Unterverzeichnisse direkt in der internen Hash-Datenbank.

Verzeichnisinhaltstabelle erstellen

Erzeugt eine Inhaltstabelle wie jede andere Laufwerksinhaltstabelle bis auf die Tatsache, dass sich die enthaltenen Dateien auf diejenigen beschränken, die im aktuell ausgewählten Verzeichnis und seinen Unterverzeichnissen enthalten sind.

Öffnen

Öffnet die aktuelle Datei bzw. bei Verzeichnissen die Datenstrukturen des Verzeichnisses in einem eigenen Datenfenster.