X-Ways Software Technology AG

WinHex/ X-Ways Forensics

Outil pour les expertises juridiques et la récupération de données

Editeur hexadécimal de fichier, disque et RAM

Manuel

Sommaire

1 Préface

1.1 A propos de WinHex et X-Ways Forensics

X-Ways Software Technology AG
Carl-Diem-Str. 32
32257 Bünde
Allemagne
Fax: +49 721-151 322 561

Web: http://www.x-ways.net
Homepage de WinHex: http://www.x-ways.net/winhex/
Commandes: http://www.x-ways.net/winhex/order-f.html
Forum d'aide: http://www.winhex.net
Adress e-mail: mail@x-ways.com

X-Ways Software Technology AG est une société anonyme constituée sous forme de directoire et conseil de surveillance et enregistrée en Allemagne à Bad Oeynhausen sous HRB 7475.

WinHex gère les systèmes d'exploitation suivants: Windows 2000, Windows XP, Windows 2003 Server

La première version à été éditée en 1995. Ce manuel a été rédigé à partir de l'aide en ligne de WinHex v13.0, diffusée juin 2006.

Traduction française de Jérôme Broutin (interface utilisateur) et Henri Pouzoullic (fichier d'aide et manuel), janvier 2000. Mises à jour: Bernard Leprêtre et Gilbert Morin. Consultant en cryptologie: Alexandre Pukall

Des instituts nationaux U.S. (ex. Oak Ridge National Laboratory, Tennessee), l'Université de Technologie de Vienne (Autriche), l'Université de Technologie de Munich (Institut d'Informatique), German Aerospace Center, Toshiba Europe, Microsoft Corp., Hewlett Packard, National Semiconductor, Ericsson, Siemens AG, Siemens Business Services, Siemens VDO AG, Infineon Technologies Flash GmbH & Co. KG, Novell Inc., Ontrack Data International Inc., KPMG Forensic, Ernst & Young, Lockheed Martin, BAE Systems, TDK Corporation, Seoul Mobile Telecom, Visa International, German Aerospace Center, Commerzbank AG, et de nombreuses autres compagnies, instituts scientifiques, unités militaires, et agences gouvernementales (particulièrement les agences fédérales américaines et allemandes chargées de l'application des lois) et ministères (comme le département ministériel australien de la défense).

Veuillez visiter site web de WinHex pour savoir comment commander la version complète.

1.2 Mentions légales

Le présent document vise à fournir une information la plus exacte et fiable pour autant que faire se peut sur l'utilisation du programme. Toutefois l'auteur n'offre aucune garantie d'aucune sorte et ne saurait être inquiété en responsabilité quant à l'utilisation du logiciel WinHex, des codes numériques édités ou modifiés, avec ou sans corrélation avec le présent manuel.

License Agreement

Your use, distribution, or installation of a software product published by X-Ways Software Technology AG indicates your acceptance of this license agreement. If you do not agree to any of the terms, then do not install, distribute or use the product.

A trial version may be only used for evaluation purposes. Purchasing one license authorizes you to install one copy of the full version of the software on a single machine. Additional licenses authorize you to install and use the full version on additional machines at the same time. Exception: For computers in the same location, *forensic* licenses for WinHex/X-Ways Forensics do not impose an upper limit on the number of computers with *installations* of the software, only on the number of concurrent uses on different computers.

This software, and all accompanying files, data, and materials, are distributed “as is” and with no warranties of any kind, whether express or implied, to the maximum extent permitted by applicable law. The user must assume the entire risk of using the program, knowing in particular that this software is not designed or intended for use in hazardous environments requiring fail-safe performance, where its failure to perform, misuse or inability to use adequately can reasonably be expected to lead to death, personal injury, or severe physical or environmental damage. In no event shall X-Ways Software Technology AG, or its officers, directors, employees, affiliates, contractors, or subsidiaries be liable for any direct, indirect, incidental, consequential, or punitive damages whatsoever arising out of the use or inability to use the software, to the maximum extent permitted by applicable law. Any liability will be limited exclusively to refund of purchase price by X-Ways Software Technology AG.

You may not rent, lease, modify, translate, reverse-engineer, decompile or disassemble the software or create derivative works based on it without prior explicit permission. All rights of any kind in the software product which are not expressly granted in this license agreement are entirely and exclusively reserved to and by X-Ways Software Technology AG.

No component of the software (except the WinHex API) must be accessed by other applications or processes.

Should any part of this agreement be or become invalid, such invalidity shall not affect the validity of the remaining provisions of the agreement.

Acknowledgements

Les algorithmes "Pukall Cipher 1" (PC 1) et "Pukall Stream Cipher Hash Function" sont sous copyright d'Alexandre Pukall. Code source disponible à `http://www.multimania.com/pc1`, `http://www.multimania.com/cuisinons/progs/` et `http://www.freecode.com`.

Le MD5 est sous copyright de RSA Data Security Inc.

La bibliothèque de compression "zlib" est sous copyright de Jean-loup Gailly et Mark Adler. Page d'accueil: `ftp://ftp.cdrom.com/pub/infozip/zlib/zlib.html`

X-Ways Forensics contains software by Igor Pavlov, www.7-zip.com.

1.3 Types de licences

Pour utiliser WinHex en version complète il faut obtenir une licence de *base* pour un usage privé, professionnel ou spécialiste. Si vous envisagez d'utiliser WinHex sur plusieurs machines informatiques, vous devrez également souscrire des licences additionnelles. La version complète vous permet d'enregistrer des fichiers de taille de plus de 200 Ko, d'écrire sur des secteurs disques et de modifier la mémoire vive et n'affiche pas de rappel d'utilisation de version d'évaluation. Elle affiche le statut de l'utilisateur ayant souscrit une license, à l'écran, au démarrage et dans la boîte "A propos".

- Les licences privées peuvent être souscrites à prix réduit pour un usage à but non lucratif uniquement. Hors toutes entreprises commerciales, institutions administrations, ou associations régies par la Loi de 1901.

- Les licences professionnelles permettent l'utilisation sous tout environnement (à domicile,

dans une entreprise, une organisation ou une administration publique), l'exécution de scripts et l'usage de l'API WinHex.

- Les licences spécialistes permettent en outre d'utiliser le menu "Outils Spécialiste", d'examiner les lecteurs Ext2, Ext3, CDFS/ISO9660 et UDF, et elles supportent les disques RAID et les disques dynamiques. Util particulièrement pour les spécialistes en sécurité de la technologie de l'information. Plus X-Ways Replica 1.3, a DOS-based forensically sound disk cloning and imaging software is included.

- Les licences forensiques* permettent en outre d'utiliser the powerful case managing and report generating capabilities of WinHex, the internal viewer and additionally a powerful viewer component, the gallery view and advanced features of the drive contents table, comments in the directory browser, plus ReiserFS, Reiser4, HFS, HFS+, and UFS support. Furthermore, they allow to read and write evidence files (.e01). Util particulièrement pour les expertises juridiques/informatiques. The forensic edition of WinHex is called X-Ways Forensics. Also includes X-Ways Replica 2.35, with advanced disk cloning and imaging capabilities.

Pour obtenir la license choisie, merci de visiter notre page d'acceuil internet. Pointez votre navigateur à l'adresse web http://www.x-ways.net/winhex/.

**Forensique : Adjectif. Qui appartient à la cour de justice, qui relève du domaine de la justice. Ce qui est à la fois légal, et scientifique et technique. Forensique est un néologisme de "forensics" en anglais, le mot existe dans la plupart des langues européennes comme allemand et l'italien mais son usage en français est récent. Les sciences forensiques se définissent comme l'ensemble des principes scientifiques et des méthodes techniques appliqués à l'investigation criminelle, pour prouver l'existence d'un crime et aider la justice à déterminer l'identité de l'auteur et son mode opératoire. L'adjectif "forensique" s'utilise également en médecine et en théologie. Il vient du latin "forum" : place publique, lieu du jugement dans l'Antiquité. (d'après Hervé Schauer Consultants)*

1.4 Differences between WinHex and X-Ways Forensics

A forensic license offers numerous additional features over a specialist license. WinHex and X-Ways Forensics can be operated with the same forensic license. If so, they are identical, except for the following:

- WinHex (winhex.exe) always identifies itself as WinHex in the user interface, X-Ways Forensics (xwforensics.exe) as X-Ways Forensics. The program help and the manual, however, statically refer to "WinHex" in most cases.

- X-Ways Forensics only allows to open those files in an editable mode that are located on the drives that contain the current case, the general folder for temporary files, or the installation folder, for decoding/decryption/conversion purposes, etc. All other files, image files, virtual memory, and disks in general, are strictly opened in view mode (read-only), to enforce forensic procedures, where no evidence must be altered in the slightest. Similarly, only the above-mentioned drives are considered legitimate output folders where files can be saved. This strict

write protection of X-Ways Forensics ensures that no original evidence can possibly be altered accidentally, which is a crucial aspect in court proceedings.

- Certain files (see http://www.x-ways.net/winhex/setup.html for details) are not part of the WinHex download, but owners of forensic licenses can copy them from X-Ways Forensics to enable the full feature set known from X-Ways Forensics in WinHex as well. Using WinHex instead of X-Ways Forensics can be desirable when not bound by strict forensic procedures and when in need to work more aggressively on files, disks, or images, e.g. repairing boot sectors etc., or when working with multiple clones where one clone is declared a working copy and cleared for write access.

2 Informations générales

2.1 Utilisation d'un éditeur hexadécimal

Un éditeur hexadécimal permet afficher le contenu complet de tout types de fichiers. Contrairement à un éditeur de texte, un éditeur hexadécimal affiche même les codes de contrôle invisible (par exemple les caractères d'avance et de retour chariot) et les codes exécutables utilisant un nombre à deux chiffres du système hexadécimal.

Considérons qu'un octet est une séquence de 8 bits. Chaque bit est soit 0 ou 1, et n'assume qu'un des deux états possibles. Par conséquent un octet peut avoir une des $2*2*2*2*2*2*2*2 = 2^8 =$ 256 différentes valeurs. Comme 256 est le carré de 16, une valeur d'octet peut être décrite par un nombre à deux chiffres basé sur un système hexadécimal, ou chaque chiffre représente un quartet (c'est à dire quatre bits). Les seize chiffres utilisés dans le système hexadécimal sont 0-9, A-F.

Vous pouvez changer la valeur d'un octet en changeant ces chiffres dans le mode hexadécimal. Il est aussi possible d'entrer le caractère, qui est attribué à une certaine valeur d'octet par un jeu de caractère (voir: Entrée de caractères). Toutes sortes de caractères sont autorisés (par exemple les lettres et caractères de ponctuation). Exemple: Un octet dont la valeur décimale est 65 est affiché comme 41 dans la notation hexadécimale (4*16+1=65) et comme la lettre A en mode texte. Le jeu de caractères ASCII définit la lettre majuscule A comme ayant la valeur décimale 65. Par conventions d'usages, en valeur hexadécimale, les caractères h, H, $ ou 0x, 0X, sont notées en suffixe ou en préfixe: 41h, 41H, $41, 0x41, 0X41.

Lors de l'édition de certains types de fichiers (fichiers exécutables par exemple) il est primordial que leur taille de ne soit pas modifiée. Changer les adresses de code exécutable et de données cruciales entraîne des dommages sévères pour de tels fichiers. Notez que le changement le contenu d'un fichier peut entraîner un fonctionnement anormal, voire une absence de fonctionnement, de l'application correspondante. De plus, cela peut entraîner un blocage de la machine. Il peut être dommageable d'éditer des passages texte dans un fichier. Il est préférable d'éditer des sections de texte dans un fichier. Dans tous les cas il est recommandé de créer des

fichiers de sauvegarde avant d'éditer.

La commande "Recherche combinée" a été spécialement conçue pour l'édition des fichiers créés pour les jeux et ce, dans le but de sauvegarder leur état. Si vous connaissez la valeur d'une variable dans deux fichiers de ce type il est possible de trouver la valeur de l'offset, c'est à dire l'endroit où cette donnée est sauvegardée. Exemple: Si deux fichiers comportent l'information stipulant que vous avez respectivement 5 et 7 points de vie, cherchez simultanément la valeur hexadécimale 05 dans le premier fichier et 07 dans le second fichier.

2.2 Terminaison hexadécimale

Les microprocesseurs diffèrent de par la position de l'octet le moins significatif: les processeurs Intel®, MIPS®, National Semiconductor et VAX ont l'octet le moins significatif en premier. Une valeur multi-octets est stockée en mémoire en partant de l'octet de poids faible (le moins significatif) vers l'octet de poids fort (le plus significatif). Par exemple, la valeur hexadécimale 12345678 est stockée 78 56 34 12. Ceci est appelé format "poids faible en tête" (little endian).

Les processeurs Motorola et Sparc ont l'octet le moins significatif à la fin. Une valeur multi-octet est stockée en mémoire de l'octet de poids fort (le plus significatif) vers l'octet de poids le plus faible (le moins significatif). Par exemple la valeur hexadécimale 12345678 est stockée comme 12 34 56 78. Ceci peut être appelé format "poids fort en tête" (big endian).

2.3 Données à nombre entier

Format, Type	Etendue	Exemple
Signé, 8 Bits	-128...127	FF = -1
Non Signé, 8 Bits	0...255	FF = 255
Signé, 16 Bits	-32 768 ... 32 767	00 80 =-32 768
Non Signé, 16 Bits	0...65 535	00 80 = 32 768
Signé, 24 Bits	-8 388 608...8 388 607	00 00 80 = -8 388 608
Non Signé, 24 Bits	0...16 777 215	00 00 80 = 8 388 608
Signe, 32 Bits	-2 147 483 648... 2 147 483 647	00 00 00 80 = 2 147 483 648
Non Signé, 32 Bits	0...4 294 967 295	00 00 00 80 = 2 147 483 648
Signé, 64 Bits	-2^{63} ($\approx -9\cdot10^{18}$)...$2^{63}-1$ ($\approx 9\cdot10^{18}$)	00 00 00 00 00 00 00 80 = -2^{63}

Si le format n'est pas autrement spécifié, les nombres multi-octets sont stockés au format "poids faible en tête" (little-endian), signifiant que le premier octet du nombre est le moins significatif et que le dernier octet est le plus significatif. C'est le format commun aux micro-ordinateurs fonctionnant sous Windows. En suivant le modèle "poids faible en tête" (little-endian), la valeur hexadécimale 10 27 peut être interprétée comme le nombre hexadécimal 2710 (en décimal: 10 000).

L'interpréteur de donnée est capable d'interpréter les données de tous les types entiers mentionnés ci-dessus.

2.4 Données du type flottant

Type	Gamme	Précision [Digits]	Octets
Float (Single)	$\pm 1.5^{-45}...3.4^{38}$	7-8	4
Real	$\pm 2.9^{-39}...1.7^{38}$	11-12	6
Double (Double)	$\pm 5.0^{-324}...1.7^{308}$	15-16	8
Long Double (Extended)	$\pm 3.4^{-4932}...1.1^{4932}$	19-20	10

La terminologie des noms de type vient du langage de programmation C. Ceux correspondants en Pascal sont entre parenthèses. Le type réel n'existe qu'en Pascal. L'interpréteur de données peut traduire les valeurs hexadécimales d'une fenêtre d'édition en nombres flottants de chacun des quatre types.

Dans l'ordinateur, un nombre flottant F est représenté par une mantisse M et un exposant E où $M \times 2^E = F$. M et E sont chacun une valeur entière signée. Les quatre types de données diffèrent dans la gamme de leurs valeurs (c'est à dire le nombre de bits réservés pour l'exposant) et par leur précision (c'est à dire le nombre de bits réservés pour la mantisse).

Sur les systèmes à base de processeurs Intel®, les calculs sur les nombres à virgule flottante sont exécutés par un coprocesseur mathématique pendant que le processeur principal attent. Le 80x87 d'Intel® travaille en précision de 80 bits de précision pour les calculs, tandis que les processeurs de type RISC (Motorola™ par exemple) utilisent le plus souvent une précision de 64 bits.

2.5 Types dates

Les formats date suivants sont gérés par l'Interpréteur de données:

- **MS-DOS Date & Heure (4 Octets)**

Le mot le plus bas détermine l'heure et le mot le plus haut la date. Utilisé par plusieurs appels à des fonctions DOS, par la FAT (Table d'allocation de fichiers) et par beaucoup d'utilitaires système tels que les utilitaires d'archivage de fichiers.

Bits	Signification
0-4	Secondes divisées par 2
5-10	Minutes (0-59)
11-15	Heures (0-23 sur une horloge 24 heures)
16-20	Jour du mois (1-31)
21-24	Mois (1 = Janvier, 2 = Février, etc.)
25-31	Décalage d'années depuis 1980

- **Win32 FILETIME (8 octets)**

La structure FILETIME est une valeur entière de 64 bits représentant le nombre d'intervalles de 100 nanosecondes depuis le 01 janvier 1601. Est utilisé par Win32 API.

- **OLE 2.0 Date & Heure (8 octets)**

Une valeur flottante (plus exactement: un double), qui détermine pour la partie entière le nombre de jours passés depuis le 30 Décembre 1899. La partie fractionnaire est interprétée comme l'heure du jour (Par exemple: 1/4 = 6:00 du matin). C'est le type standard de date OLE 2.0, il est utilisé par exemple par MS Excel.

- **ANSI SQL Date & Heure (8 octets)**

Deux valeurs entières consécutives de 32 bits. La première détermine le nombre de jours depuis le 17 Novembre 1858. La seconde est le nombre d'intervalles de 100 microsecondes depuis minuit. C'est le type SQL ANSI, utilisé par de nombreuses bases de données (ex. InterBase 6.0).

- **UNIX, C, FORTRAN Date & Heure (4 octets)**

Une valeur entière de 32 bits détermine le nombre de secondes depuis le 01 janvier 1970. Ce type de données était utilisé par UNIX, par C et C++ ("time_t"), et par les programmes FORTRAN dès les années 80. Sporadiquement utilisé comme définissant le nombre de *minutes* écoulés depuis le 01 Janvier 1970. Les options de l'interpréteur de données vous permettent de commuter entre ces différents sous-types.

- **Macintosh HFS+ Date & Time (4 bytes)**

A 32-bit integer value that determines the number of seconds since January 1, 1904 GMT (HFS: local time). The maximum representable date is February 6, 2040 at 06:28:15 GMT. The date values do not account for leap seconds. They do include a leap day in every year that is evenly divisible by 4.

- **Java Date & Heure (8 octets)**

Une valeur entière de 64 bits représentant les millisecondes depuis le 1er janvier 1970. Principalement stockée au format "poids fort en tête", qui est l'ordre des octets caractéristique de Java.

2.6 ASCII ANSI/IBM

ASCII ANSI est le jeu de caractères utilisé dans les applications Windows. Il est standardisé par l'American National Standards Institute. MS DOS utilise le jeu de caractères ASCII IBM (appelé aussi ASCII OEM). Ces jeux de caractères diffèrent par leur seconde partie, celle qui contient les caractères ayant des valeurs ASCII plus grandes que 127.

Il est conseillé de commuter l'option menu "Utiliser ASCII ANSI" sur OFF lors d'affichage ou d'édition de fichiers d'origine DOS.

Utilisez la commande "Convertir" du menu Edition pour convertir des fichiers textes d'un jeu de caractères dans un autre.

Les 32 premières valeurs ASCII ne sont pas des caractères imprimables, mais des codes de contrôle:

Hex	Control Code	Hex	Control Code
00	Null	10	Data Link Escape
01	Start of Header	11	Device Control 1
02	Start of Text	12	Device Control 2
03	End of Text	13	Device Control 3
04	End of Transmission	14	Device Control 4
05	Enquiry	15	Negative Acknowledge
06	Acknowledge	16	Synchronous Idle
07	Bell	17	End of Transmission Block
08	Backspace	18	Cancel
09	Horizontal Tab	19	End of Medium
0A	Line Feed	1A	Substitute
0B	Vertical Tab	1B	Escape
0C	Form Feed	1C	File Separator
0D	Carriage Return	1D	Group Separator
0E	Shift Out	1E	Record Separator
0F	Shift In	1F	Unit Separator

2.7 Sommes de contrôle

Une somme de contrôle (checksum) est un nombre caractéristique utilisé pour vérifier l'authenticité de données. Deux fichiers ayant une somme de contrôle identique présentent une très forte probabilité d'égalité l'un par rapport à l'autre (c'est à dire octet par octet). Calculer et comparer les sommes de contrôle d'un fichier avant et après une transmission éventuellement imprécise peut révéler des erreurs survenues lors de la transmission. Une somme de contrôle valide indique que les fichiers sont (selon toute vraisemblance) encore identiques. Toutefois, un fichier peut être manipulé de telle sorte que sa somme de contrôle reste non affectée. Le "hash-

code" (condensé, digest) est utilisé dans de tels cas à la place d'une somme de contrôle, et dés lors, des modifications malveillantes (c'est à dire nullement aléatoires) apportées aux données originales pourront être détectées.

Dans WinHex, des sommes de contrôles sont calculées lors de l'ouverture (optionnel, cf. Options de Sécurité) ou lors de l'analyse (cf. menu Outils) d'un fichier. Après des modifications de fichiers, des sommes de contrôle peuvent être recalculées en tapant ALT+F2.

La somme de contrôle standard est simplement la somme de tous les octets d'un fichier, calculée dans un accumulateur 8 bits, 16 bits, 32 bits ou 64 bits. Le CRC (un code de redondance cyclique) est basé sur des algorithmes plus sophistiqués, qui sonst certes plus sûrs. Un CRC est le résultat de la division des données par un générateur polynômique.

Exemple: Si une transmission altère deux octets dans un fichier de manière telle que les modifications se contrent (par exemple octet un + 1, octet deux - 1), la somme de contrôle standard ne sera pas affectée, alors que le CRC changera.

2.8 Hachage à sens unique

Un *hash-code monodirectionnel* (=condensé, digest), similaire à une somme de contrôle, est un nombre caractéristique utilisé pour la vérification de l'authenticité de données. Mais le hash-code est beaucoup plus que cela: contrairement aux systèmes avec CRC le hash-code ne laisse passer aucune erreur d'intégrité.

A partir d'un ordinateur il est faisable de manipuler n'importe quelles données de telle sorte que sa somme de contrôle reste non affectée. Vérifier la somme de contrôle dans de tels cas pourrait laisser penser que les données n'ont pas été changées, alors qu'elles l'ont été. C'est pourquoi le hash-code est utilisé au lieu de la somme de contrôle dans le cas où des modifications malveillantes (c'est à dire nullement aléatoires) de données originales doivent être détectées. Même en utilisant des ordinateurs il est *impossible* de trouver des données qui correspondent à un hash spécifique. Il est même infaisable de trouver deux ensembles de données qui correspondent à un même hash.

Bien sûr, des modifications aléatoires, telles que celles causées par une transmission imprécise, peuvent aussi être détectées en utilisant des hashes, mais dans ce cas les sommes de contrôle rendent un meilleur service, car elles peuvent être calculées plus rapidement.

WinHex gère les fonctions 128-bit MD5, SHA-1, SHA-256 et PSCHF (Pukall Stream Cipher Hash Function).

2.9 Caractéristiques techniques

Nombre maximum de fenêtres:	1000 (WinNT/2000), 500 (Win9x/Me)
Taille maximum du disque et des fichiers:	≈2000 Go
Nombre maximum d 'instances de programmes simultanées:	99
Nombre maximum de signets:	limité seulement par la RAM
Nombre maximum de saisies claviers réversibles:	65535
Niveau de cryptage:	128 bit
Longueur des condensés pour les sauvegardes:	128/256 bit
Jeux de caractères supportées:	ASCII ANSI/IBM, EBCDIC, Unicode (limité)
Présentation du décalage (Offset):	hexadécimal/décimal

- Dans la plupart des cas, l'affichage de progression montre le pourcentage complet d'une opération. Cependant, lors d'opération de recherche ou de remplacement il indiquera la position relative dans le fichier courant.

- Il est recommandé de ne pas utiliser de très grande police de caractères dans votre système Windows.

- WinHex s'attend à ce que votre ordinateur fonctionne dans le mode "*poids faible en tête*".

- Les clés que vous spécifiez pour le cryptage et le décryptage ne sont pas sauvegardées sur votre disque dur. Prévoyez que l'option de sécurité soit prise afin que la clé soit stockée en mémoire dans un état chiffré tant que WinHex est en service.

- Les opérations de recherche et de remplacement sont plus rapides si vous n'utilisez ni "joker" ni l'option "Sensible majuscule/ minuscule".

- Lors d'une recherche avec l'option "Compte d'occurrences" activée ou lors de remplacement sans demande de confirmation, pour un algorithme de recherche il y a généralement deux façons de se comporter lorsque l'on trouve une occurrence, ce qui peut amener dans certains cas des résultats différents. Ceci est expliqué dans l'exemple suivant:

  Les lettres *ana* sont recherchées dans le mot "banana". La première occurrence est d'emblée trouvée au second caractère.

  1ère alternative: L'algorithme continue la recherche à partir du troisième caractère. Ainsi *ana* est à nouveau trouvé à partir du quatrième caractère.

  2ème alternative: Les trois lettres trouvées dans le mot "banana" sont sautées. Les lettres restantes *na* ne contiennent plus *ana*.

  WinHex est conçu sur le concept de la deuxième alternative parce que celle-ci fournit des résultats plus plausibles lors de comptages ou de remplacements d'occurrences. Si vous continuez une recherche en utilisant la touche F3 ou que vous choisissiez l'option "Confirmer chaque remplacement", l'algorithme se conformera à la première alternative.

3 Fonctions forensiques

3.1 Case Management

The integrated computer forensics environment in WinHex can be used with a forensic license of WinHex only. It offers complete case management, automated log and report file generation, and various additional features such as gallery view, file signature check, HPA detection, and skin color detection in pictures.

When starting up WinHex for the first time, you are asked whether to run it with the forensic interface. This means the “Case Data” window is displayed, WinHex is run in read-only mode, and you are asked to make sure the folders for temporary files and for case data are set correctly, in order to prevent WinHex from writing files to the wrong drive.

In order to work with a case, make sure the "Case Data" window is visible on the left of the main window. If not, enable View | Show | Case Data.

From the File menu, you may create a new case (start from scratch), open an existing case, close the active case, save the active case, back up the case file and the entire case folder in a ZIP archive, or automatically generate a case report. A case is stored in a .xfc file (xfc stands for X-Ways Forensics Case) and in a subfolder of the same name, just without the .xfc extension. This subfolder and its child folders are created automatically when the case is created. You may select the base folder for your cases in General Options. It is not necessary to explicitly save a case, unless you need to be sure it is saved at a given time. A case is saved automatically at latest when you close it or exit the program.

In the case properties window, you may name a case according to your own conventions (e.g. title or number). The date and time you create a case is recorded and displayed. The internal case filename is displayed as well. You may enter a description of the case (of arbitrary length) and the examiner's name, the examiner's organization's name and address. You may enable or disable the automated log feature for the whole case. Optionally, the evidence object subfolders in the case folder are always suggested as default output folders for files recovered/copied off a file system. You may wish to disable that feature if your preference is to copy files from various evidence objects into the same output folder.

The most powerful concept in X-Ways Forensics, that allows to systematically and completely review files on computer media, is the so-called *refined volume snapshot*. It is possible to refine the standard volume snapshot for all evidence objects of a case in one step, and to search all evidence objects with volume snapshots logically with the help of the virtual global case root window. Note that it is possible to generate a flat overview of all existing and deleted files from all subdirectories on an partition or image file of a partition by recursively exploring the root directory. In order to explore a directory recursively (i.e. list its contents plus the contents of all its subdirectories plus their subdirectories), *right*-click the directory in the directory tree in the Case Data window. In order to *tag* a directory, you can click it with the middle mouse button in

the directory tree.

In order to completely *delete* a case, you need to delete its .xfc file and the corresponding directory with the same name and all its subdirectories.

3.2 Evidence Objects

You may add any currently attached computer medium (such as hard disk, memory card, USB stick, CD-ROM, DVD, ...), any image file, or ordinary file to the active case. It will then be permanently associated with this case (unless you remove it from the case later), displayed in the tree-like case structure, and designated as an *evidence object*. A subfolder is created in the case folder for each evidence object, where by default files will be saved that you recover from that evidence object, so it will always be obvious from which object exactly (and from which case) recovered files originate.

In the evidence object properties window, you may enter a title or number for that evidence object according to your own conventions. The date and time it was associated with the active case is recorded and displayed. The internal designation of the evidence object is displayed as well as its original size in bytes. You may enter comments of arbitrary length that apply to the evidence objects, and a technical description of it is added by WinHex automatically (as known from the Medial Details Report command in the Specialist menu). You may have WinHex calculate a hash (checksum or digest) on the evidence object and verify it later, so that you can be sure that data authenticity has not been compromised in between. Hashes stored in evidence files are imported automatically when added to a case. You may disable the automated log feature for a specific evidence object if the log feature is enabled for the case as a whole.

Ways how to add files or media to a case: The "Add" commands in the case data window's File menu. The "Add" command in the edit window's tab's context menu. The "Add" command of a directory browser's item's context menu.

Sub-elements

All evidence objects in turn have further elements associated with them. There is a list of annotations/bookmarks, initially blank, where you may specially mark and comment an unlimited number of positions of interest, specifically for the evidence object. See Position Manager. Up to 32 contents tables can be associated with an evidence object. They are created by the Specialist menu commands Create Drive Contents Table and Create Directory Contents Table. They show the files of a volume including those in subdirectories in a single flat view, optionally grouped by file categories. From an evidence object's context menu you can also create special report contents tables, which are initially blank and to which you can add notable files via the directory browser's context menu (Position section). There is an item in the report table's context menu that allows you to toggle inclusion in the report.

Finally, if you extract free space, slack space, or text from a volume (using Specialist menu commands), the resulting files will show up in the case tree below the corresponding evidence

object as well.

3.3 Log & Report Feature

Logs

When enabled in the case and the evidence properties window, WinHex obstinately logs all activities performed when the case is open. That allows you to easily track, reproduce, and document the steps you have followed to reach a certain result, for your own information and for the court room.

The following is recorded:

- when you a select a menu item, the command title (or at least an ID), and the name of the active edit window, if not an evidence object, preceded by the keyword "Menu",
- when a message box is displayed, the message text and what button you pressed (OK, Yes, No, or Cancel), preceded by the keyword "MsgBox",
- when a small progress indicator window is displayed, its title (like "Recovering files...") and whether the operation was completed or aborted, preceded by the keyword "Operation",
- a screenshot of each displayed dialog window with all selected options, e.g. for a complex operation that follows, preceded by the window's title,
- original source path of each recovered file,
- destination path of each recovered file when recovered with the directory browser or the Access button menu,
- the extensive log produced by Clone Disk and File Recovery by Type,
- your own entries (free text) that you add with the Add Log Entry command, either to the case as a whole or to a certain evidence object.

All actitivities are logged with their exact date and time, internally in FILETIME format with 100-nanosecond interval precision. Logs are by default associated with the case as a whole. However, logs of activities that apply to a certain evidence object are directly associated with that evidence object. This determines where they appear in a report. Screenshots are saved as .png files in the "log" subfolder of a case folder. They can optionally be converted to black & white images, which allows to print them in a cost-effective way along with the report.

Reports

You may create a report from the File menu of the Case Data window. The report is saved as an HTML file and can thus be displayed and opened in a variety of applications. For example, you may view it in your favorite Internet browser and open and further process it in MS Word.

The report starts with the general case title and details, followed by a list of hyperlinks to the individual evidence object sections. For each evidence object, the report specifies its title, details, and description, your comments, your annotations, and the evidence object related log. The report ends with the general log.

3.4 Navigateur de répertoire

On logical drives and partitions formatted with FAT12, FAT16, FAT32, NTFS, Ext2, Ext3, ReiserFS, Reiser4, HFS, HFS+, UFS, CDFS/ISO 9660/Joliet, or UDF, WinHex offers a *directory browser*, which resembles the Windows Explorer's right-hand list. It can be disabled or enabled by clicking the checkbox next to the Access button. The directory browser lists existing files and directories first, then deleted files and directories. Compressed files are displayed in blue, encrypted files in green (NTFS only). Right-clicking any item in the directory browser brings up a context menu with commands for opening a file or directory, exploring a directory, locating the beginning of a file or directory on the disk, locating the corresponding directory entry (FAT) or file record (NTFS), listing the allocated clusters in a separate window, and for easily recovering a lost or existing file or directory. The latter can recreate entire directory structures. Double-clicking executes the default action (locating the data in the Sectors view, listing clusters, and exploring in the case of a directory).

Deleted files and directories are represented in the directory browser with lighter icons. Question mark icons indicate that the original file or directory contents may be still available. Deleted objects that WinHex knows are no longer accessible (either because their first cluster has been reallocated or because they have a size of 0 bytes) have icons crossed out in red.

The directory browser can sort files and directories in ascending or descending order, and still reveals the previous sort criterion with a lighter arrow. For example, if you first click the filename column and then the filename extension column, files with the same extension will internally still be sorted by name.

Fictitious Items

When orphaned objects are found, e.g. files that have been deleted and whose original path is unknown, they are listed in a special fictitious directory “Path unknown”. With a specialist or forensic license, there are fictitious files in the root directory that allow you to conveniently address special areas in a volume:

File system areas: Reserved sectors and/or clusters that are claimed by the file system itself for internal purposes.

Free space: Clusters marked by the file system as not in use.

Idle space: Clusters marked as in use, whose exact allocation however could not be determined by X-Ways Forensics. This can be the case if the file system lost track of them, i.e. forgot that these cluster are actually available for re-allocation. Usually there is no idle space. The size of idle space and the number of the first idle cluster are only determined when needed (e.g. when you click the "Idle space" file for the first time), as depending on the number of cluster this is a potentially time-consuming operation.

Volume slack: Sectors at the end of the partition that are unused by the file system because they do not add to another cluster.

Indirect blocks (Ext2, Ext3, UFS): Special blocks that contain block numbers. Not part of "File system areas".

Unnoted attribute clusters (NTFS): Clusters that contain non-resident attributes that have not been individually processed by X-Ways Forensics. Not part of "File system areas".

.journal (ReiserFS): Blocks that form the fixed journalling area. On Ext3 and HFS+, this is not considered a fictitious file because it is defined by the file system itself in dedicated records.

Columns

Filename	Name of the listed file or directory. Allows to filter based on file masks. The filter expression may consist of several file masks, delimited by semicolons, like *.jpg;*.gif. Up to two asterisks allowed per mask if they are located at the beginning and the end of a filename mask. You may exclude files using file masks that start with a colon (:). For example, you may include all files except NTFS system files by providing the following masks: *;:$* (or simply :$*). Another example: All files with names that start with the letter "A", but do not contain the word "garden": A*;:*garden*.
Ext.	Filename extension. The part of the filename that follows the last dot, if any.
Type	If the header signature of a file was not specifically checked (see Refine Volume Snaphot), this is merely a repetition of the filename extension and displayed in gray. Otherwise, if the file signature verification revealed the true nature of the file, a typical extension of that type will be output. That extension will be displayed in black if it is still the same as the actual extension of the file, or in blue if the actual extension does not match the type of the file. (forensic license only)
Status	The status of the preceding Type column. Initially “not verified”. After verifying file types based on signatures or after previewing files: If a file is very small, the status is “don't care”. If neither the extension nor the signature is known to the file type signature database, the status is “not in list”. If the signature matches the extension according to the database, the status is “confirmed”. If the extension is referenced in the database, yet the signature is unknown, the status is “not confirmed”. If the signature matches a certain file type in the database, however the extension matches a different file type or there is no extension at all, the status is “newly identified”. (forensic license only)
Category	File type category corresponding to the file type, according to the definition in “File Type Categories.txt”. (see below, forensic license only)
Path	Path of the file or directory, starting with a backward slash if the path is known, based on a volume's root, or starting with a question mark if the exact path is unknown.
Size	Size of the file or directory, without slack.
Created*	The date and time the file or directory was created on the volume it resides on. Not

	available on Linux filesystems.
Modified*	The date and time the file or directory was last modified on the volume it resides on. On FAT, time precision is 2-second intervals only. On CDFS, the only available date and time stamp is listed in this column altough it does not necessarily indicate last modification.
Accessed*	The date and time the file or directory was last read or otherwise accessed on the volume it resides on. On FAT, only the date is recorded.
Record update*	The date and time the file's or directory's FILE record (on NTFS) or inode (Linux filesystems) was last modified. These are filesystem data structures that contain the file's meta data.
Deletion*	The date and time the file or directory was deleted. Available on Linux filesystems only.
Attr.	DOS/Windows attributes on FAT/NTFS filesystems, Unix/Linux permissions on Ext2/Ext3/Reiser/HFS+ filesystems, plus some proprietary symbols. See below.
1st cluster	The number of the cluster that contains the beginning file the file's or directory's data. Sorting by 1st cluster means to sort by physical location on the disk.
ID	The identifier assigned to the file or directory by the file system or by WinHex. Not necessarily unique.
Int. ID	The internal identifier of a file or directory in the volume snapshot. Items added to a volume snapshot last have the highest identifiers.
SC%	Skin color percentage. Optionally available for contents tables. Indicates the degree pictures are composed of skin tones. Sorting by this column is the most efficient way to discover traces of e.g. child pornography.
Hash	The file's hash value, if computed.
Hash set	In the internal hash database, the name of the hash set that the file's hash value, if available, belongs to.
Category	The category of the hash set that the file's hash value, if available, belongs to. Either "irrelevant", "notable", or blank.

*Please note that for FAT volumes, all timestamps are displayed unmodified, for all other volumes the time zone concept applies.

Attributes

A = to be archived
R = read-only
H = hidden
S = system
P = junction point
C = compressed at file system level
c = compressed in an archive (ZIP, RAR, ...)

E = encrypted at file system level
e = encrypted in an archive (ZIP, RAR)
e? = possibly encrypted or compressed, according to the entropy test

The built-in priority when sorting by the Attr. column in descending order is as follows:

1) Document-level encryption
2) User-level encryption (e.g. in a ZIP archive)
3) NTFS filesystem encryption
4) User-level encryption supposed (flagged by the entropy test)
5) Unix/Linux SUID
6) Unix/Linux SGID
7) NTFS reparse/junction points
8) NTFS alternate data streams
9) File slack (listed separately only in evidence file containers)
10) User-level compression (e.g. in a ZIP archive)
11) NTFS filesystem compression
12) NTFS $EFS attributes
13) NTFS INDX/BTM attributes
14) HFS/HFS+ resource forks
15) Unix/Linux symlink
16) Unix/Linux other special file
17) ordinary DOS/Windows attributes and Linux permissions

File Type Categories.txt

This customizable file defines what filename extensions belong to which category, in that each category is followed by its extensions. A category name is preceded by :x: where x is the incrementing unique number of the category. No more than 32 categories supported. Lines with filename extensions must start with either a “+” or a “-”, where “+” means that extension is checked in the file type filter. Only lower-case letters are to be used in extensions. 1 extension per line. An extension may be followed by arbitrary comments after a space. Correct filtering is not guaranteed if same extension occurs more than once.

In addition to extensions, full filenames are supported as well. This is useful for certain files with a well-defined name whose extension alone is not specific enough:
-;index.dat; Internet Explorer history/cache
-;history.dat; Mozilla/Firefox browser history

Note that the virtual “Other” category, which is not specifically defined in the file, covers all unknown extensions, that means even files whose full name has been included as described above.

3.5 Internal Viewer

The internal viewer can be invoked with the “View” command in the Tools menu and in the directory browser's context menu. It shows picture files of various file formats (see Gallery View) and the internal structure of Windows registry files. If you try to view a file that is not supported by the internal viewer, the first defined external viewer is invoked instead.

There is an additional viewer component that integrates seamlessly and allows to conveniently view more than 200 (!) file formats (such as MS Word/Excel/PowerPoint/Access/Works/Outlook, HTML, PDF, CorelDraw, StarOffice, OpenOffice, ...) directly in WinHex and X-Ways Forensics. This component is provided to all owners of forensic licenses issued for v12.05 and later. It can be enabled in Options | External Programs. More information online. The folder for temporary files used by the separate viewer component is controlled by WinHex/X-Ways Forensics, i.e. set to the one the user specifies in General Options. However, unlike X-Ways Forensics, the viewer component does not silently accept unsuitable paths on read-only media. Please note that the viewer component, if actually used, also leaves entries in the system registry.

Registry Viewer

MS Windows maintains an internal database called registry which contains all important settings for the local system and installed software in a tree-like structure. The data is persistently stored in files called registry hives. You can open and view hives without importing them into your own active registry. Supported formats are Win9x/Me/NT/2k/XP hives. Win9x and WinMe hives are located in the files "user.dat", "system.dat", and their backups. WinNT, Win2k, and WinXP hives are located in the file "ntuser.dat" in a user profile and in the directory \system32\config.

Up to 16 hives can be opened in the registry viewer at the same time. Since Win9x/Me and WinNT/2k/XP registries have different internal structures, their hives cannot be opened and viewed at the same time. If a different format is encountered, only the hive that was opened last will be displayed in the window.

With a right-click a popup menu can be opened anywhere in the window, which lets you invoke the commands "Search" and "Continue Search". Clicking "Search" pops up a dialog that lets you specify a search expression and where you want to search. You can browse either keys or names or values or all of them. The search starts at the topmost root and spans all opened hives. "Continue Search" finds the next match after at least one match has been found. (The currently selected element is not relevant for where the search continues). In the right-hand window the popup menu also contains the command "Copy" which lets you copy the value of the selected element to the clipboard.

3.6 Registry Report

From within the registry viewer, WinHex can create a HTML-based report, listing values of possibly relevant registry keys, when you invoke the command "Create Registry Report" in the pop-up menu. The registry keys that are to be reported in all open hives are specified in a text file called "Reg Report Keys.txt". The registry files you view must have their original names, or else the report may fail. You may edit the list of registry keys in this files to tailor the report to your

own needs.

Format of entries in "Reg Report Keys.txt"

(*operating system shortcut*) (*tabstop*) (*registry path*) (*tabstop*) (*description*) (*linefeed*)

operating system shortcuts:
9x: Windows 9x/Me
NT: Windows NT/2000/XP

registry path:
Full path of registry keys

HKLM: HKEY_LOCAL_MACHINE
HKCU: HKEY_CURRENT_USER

If an asterisk ("*") is provided as the last key, all keys on the same level and deeper and their values will be included in the report.

example:
NT HKLM\Software\Microsoft\Windows\CurrentVersion* report whole Windows branch

If you wish to report a particular value that exists in all subkeys of a certain key, you can as well write an "*" for all subkeys and include the value after that.

example:
9x HKCU\Identities*\UserID UserID value of every identity

The generated report contains the registry path with its timestamp (Windows NT/2000/XP only), the filename of the registry hive that the key was found in, the description that was provided in the "Reg Report Keys" file, and the value.

3.7 Refined Volume Snapshots

The Specialist menu allows to expand the standard volume snapshot (=the overview of files presented in the directory tree and in the directory browser) in various ways. Requires a specialist or forensic license. Refining volume snapshots serves as the same purpose and offers similar features as creating a drive contents table. Volume snapshots are superior to contents tables, though, since they can be examined both as a flat list (when exploring recursively) or directory-wise.

Particularly thorough file system search

- FAT12/FAT16/FAT32: This option searches for orphaned subdirectories (subdirectories that are no longer referenced by any other directory).

- NTFS: This option searches for file records in sectors that do not belong to the current MFT. Such file records can be found e.g. after a partition has been recreated, reformatted, moved, resized, or defragmented.
- ReiserFS, Reiser4: Searches for deleted files (which are not included in the standard volume snapshot at all).
- Other: no difference

Taking a thorough volume snapshot is possibly a lengthy operation, depending on the size of the volume, and for that reason this is not the standard procedure when opening volumes.

The "**File header search**" option causes files to be included in the list that can still be found in free or used drive space based on their file header signature and are no longer referenced by file system data structures. You are asked to select certain file types for detection, specify output filenames etc. as known from File Recovery by Type. Files found with this method will be included in the volume snapshot only if there is no other file in the volume snapshot with the same start cluster number or if they are not aligned at cluster boundaries, to avoid duplicates. Files found with this method are listed with a generic filename and size as detected by the File Recovery by Type mechanism.

Hash values can be computed for all files listed in a contents table. In addition to this, a forensic license allows to **match** the hash values against individually selected (or simply all) hash sets in the internal hash database. The filter can then later be used to hide known irrelevant files. Irrelevant files can optionally be hidden right away and excluded from further processing as part of volume snapshot refinement.

Only a forensic license allows to separately list and examine files in **ZIP, RAR**, ARJ, GZ, TAR, and BZIP **archives**, as long as the archives are not encrypted. The contents of archives in archives can be included as well, but no further level.

A forensic license allows you to **verify file types based on signatures**, i.e. detect filename/file type mismatches in files. For example, if someone has concealed an incriminating JPEG picture by naming it "invoice.xls" (wrong filename extension), the recognized file type "jpg" is stated in the Type column of the directory browser. For more information see the description of the columns Type and Status. The file signatures and extensions used for mismatch detection are defined in the accompanying file type definition database, which you may fully customize. 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.

A forensic license additionally allows to calculate the **percentage of skin colors** in pictures. This can be done for the same file types also supported by the gallery view, both for output to the directory browser and to a file. For example, if a forensic examiner is looking for traces of child pornography, sorting images by skin color percentage in descending order may accelerate your work immensely because it renders checking the mass of 0%..9% skin color percentage pictures obsolete (e.g. thousands of browser cache garbage files). Please note that there may be false positives, i.e. skin-like colors of a non-skin surface. Pictures that cannot be correctly scanned for skin colors (e.g. too large, corrupt file or black-and-white) will be listed with a question mark

instead of the skin color percentage.

A forensic license allows to optionally search for **JPEG and PNG pictures embedded in documents** such as MS Word, PDF, MS PowerPoint, MS Excel as well as in thumbs.db thumbnail buffers. Such pictures can be found by their file header signature and will be listed with generic names as "Embedded 1....jpg", "Embedded 2....png", etc. When including files in archives or pictures embedded in documents, the host files will be displayed as fictitious directories for convenient browsing. Also if *.jpg is in the series of file masks you can find JPEG thumbnails incorporated in JPEG pictures. Those will be listed as a fictitious file with the original filename and "Thumbnail" appended.

A forensic license allows to optionally perform **file format specific and statistical encryption tests**. With an entropy test, each existing file larger than 255 bytes is checked whether it is fully encrypted. If the test is positive (the entropy exceeds a certain threshold), the file is flagged with “e?” in the attribute column, to indicate that it might deserve special attention. Typical example: Encrypted container files, which can be mounted by encryption programs like PGP Desktop, BestCrypt, or DriveCrypt as drive letters. The entropy test is not applied to ZIP, RAR, TAR, GZ, BZ, 7Z, ARJ, JPG, PNG, GIF, TIF, MP3, MPG, and .??_ files, which are well-known to be compressed internally and therefore almost indistinguishable from random or encrypted data. This test is not needed to detect that files are encrypted at the NTFS file system level or inside archives. Secondly, documents with the extensions .doc (MS Word 4...2003), .xls (MS Excel 2...2003), .ppt, .pps (MS PowerPoint 97-2003), .mpp (MS Project 98-2003), and .pdf (Adobe Acrobat) are checked for file format specific encryption. If positive, these files are flagged with “e!” in the attribute column. This check requires that the separate viewer component is active.

3.8 Mode Buttons

When examining a logical drive, partition, or image file with a file system supported by WinHex, there are four buttons that determine the display in the lower half of the window, below the directory browser.

Sectors

The default view that shows the binary data in all sectors as hexadecimal code, ASCII text, or both, along with an offset column.

Preview

Checks the file signature of the file currently selected in the directory browser. If found to be a picture (supported file types see below), the picture is displayed, otherwise an ASCII text extract from the beginning of the file. The result of the signature check (whether it matches the filename extension or not) is displayed in the status bar. By double-clicking the preview, you get a full-size view of a picture, where you may zoom in and out using the keys + and -. Even incomplete pictures (e.g. files incompletely recovered because of fragmention) can usually be displayed partially.

Gallery

Checks the file signature of all the files in the currently visible portion of the directory browser. If found to be a picture, a thumbnail is displayed, otherwise a brief summary (filename, size, signature). By scrolling in the directory browser, the gallery view scrolls as well. You may switch the directory even while the thumbnails are still loading. By double-clicking a thumbnail, you get a full-size view of a picture, where you may zoom in and out using the keys + and -. Even incomplete pictures (e.g. file incompletely recovered because of fragmention) can usually be displayed partially.

Supported picture file types: BMP, JPG/JPEG, JPEG 2000, PNG, GIF, TIF, TGA, PCX, WMF, EMF, MNG, JBG

Calendar (timeline view)

Gives a convenient overview of when the files/directories selected in the directory browser were created in a file system (red), last modified (blue), and last accessed (green), in the form of a calendar. Each day with a time stamp for at least one file or directory is filled in the calendar with the corresponding color. Weekends (Saturdays and Sundays) are specially marked. Hover the mouse over a day to find out which files exactly are represented and to see the corresponding times. If the list for a certain day is too lengthy to be displayed completely, you can still sort the directory browser in a suitable way and find out there.

Example: During which period of time were JPEG files created on a volume? Either right-click the root directory in the directory tree (case data window) to recursively list all existing files or create a contents table, then sort by filename extension, select all JPEG files, then enable the calendar view, and watch out for red bars.

3.9 Logical Search

The directory browser's context menu allows logical simultaneous search operations in files and folders that are selected in the directory browser (specialist or forensic license only).
Advantages:

+ The search scope can be limited to certain files and folders, also certain files and folders that are part of a contents table.

+ Searching in files (usually = in the cluster chains allocated to files) will find search term occurrences even if the search term happens to be physically split in a fragmented file (occurs at the end and the beginning of discontiguous clusters).

+ Searching will be successful even for files that are compressed at the NTFS file system level.

+ If the contents of archives (files in ZIP, RAR, GZ, TAR, BZ2, 7Z, and ARJ, if not encrypted,

forensic license only) have been included in the volume snapshot and they are selected in the directory browser or if the containing archives are selected and treated like directories, they will be searched as well.

+ The text contained in PDF (Adobe), WPD (Corel WordPerfect), CDR (Corel Draw), and VSD (Visio) files can automatically be extracted and decoded prior to search, to unformatted ASCII plaintext, which can be successfully searched in addition to the actual file contents themselves. Potential search hits in such files would otherwise be missed because these file types typically store text in an encoded, encrypted or otherwise garbled way. This feature requires the separate viewer component to be active for the decoding and text extraction part.

+ Files in which the searm term occurs can be automatically opened or added to a dedicated contents table.

Unallocated space can be included in a logical search by including the fictitious file "Free Space" in the root directory, file system areas by including the fictitious file of the same name. Slack space is included depending on the directory browser options.

- Only a physical search can cover the transition from slack space to directly following free space.

3.10 Search Hit Lists

Available only with a forensic license, when working with a case (otherwise the Position Manager will list search hits). The directory browser can show search hits. In that mode of operation is consists of three additional columns: physical/absolute offset of the search hit, logical/relative offset, and search term (usually with a context preview). The directory browser's grouping options have no effect when search hits are sorted by one of these three columns. To get into that display mode, click the button with the binoculars and the 4 horizontal lines. It is only available for evidence objects.

Almost all commands in the directory browser context menu are available for search hit lists as well, notably the ability to copy, view, tag and comment files. The dynamic filter based on the usual directory browser columns can be used in conjunction with search hit lists e.g. to view hits in all .doc and .xls files with certain last modification dates only.

The search hit list is based on the position and level in the directory tree where you click, so that you can e.g. see all search hits in files in \Documents and Settings and subdirectories of the same, and even search hits from all evidence objects of the entire case at the same time, using the case root window. Also it's possible to conveniently select one or several search terms for search hit viewing, in the search term list in the Case Data window. The search term list contains all the search terms ever used for conventional (non-index) searches in that case. Like that it's also an easy task to find out how many search hits there are for any given search term for any level in the case tree, as that number is displayed in the directory browser's caption based on the current search hit list.

Search hit lists are "dynamic" in that they are composed "on the fly" depending on selected search terms, current filter settings etc. and in that they can be non-destructively "thinned out" with the directory browser's context menu, leaving only one hit per file in the list. This allows you to conveniently copy files to your own hard disk or to an evidence file container without duplicates even from a search hit list.

Search hits can be marked as notable with the directory browser context menu or by pressing the Space key. With the Space key you may also remove that mark. The search term list allows to create a quick overview of all hits marked as notable. Alternatively, you may use the directory browser option "Group tagged items" to group marked search hits at the beginning of the list.

When you no longer need certain search hits, select them and press the Del key. When you no longer need any search hit of certain search terms, select the search terms in the search term list and press the Del key.

3.11 Hash Database

Only available with a forensic license. The internal hash database, once created, consists of 257 binary files with the extension .xhd (X-Ways Hash Database). The storage folder is selected in the General Options dialog. The hash database is organized in a very efficient way, which maximizes performance when matching hash values. It is up to you to decide, around what hash type the database is built (MD5, SHA-1, SHA-256, ...).

Each hash value in the hash database belongs to one or more hash sets. Each hash set belongs to either the category “known good”/“harmless”/“irrelevant” or “known bad”/“malicious”/“relevant”/“notable”.

Hash values of files can be calculated and matched against the hash database when creating a contents table. The directory browser's optional columns “Hash Set” and "Category” will then reveal for each file to which hash set and category it belongs, if any (which allows you to sort by these aspects and filter out irrelevant files easily). Please note that if a hash value is contained in multiple hash sets, only the first matching hash set will be displayed in the hash set column.

The Tools menu allows you to

- manage the active hash database: create a new (empty) one, view the list of hash sets, rename and delete hash sets, toggle the hash set category, and verify the integrity of the hash database (F8)
- import a single hash set text file (NSRL RDS 2.x, HashKeeper, and ILook text files are supported)
- import all the hash set text files in a certain folder and all its subfolders (ditto), optionally into a single internal hash set whose name you have to specify
- delete the active hash database, e.g. to start a fresh one with new hash sets and/or a new hash type.

The Create Hash Set command in the directory browser's context menu allows you to create your

own hash sets in the internal hash database. The hash database supports up to 65,535 hash sets. Future versions will allow you to export hash sets in the hash database to the NSRL RDS format.

3.12 Time Zone Concept

The following applies to WinHex and X-Ways Forensics when operated with a specialist or forensic license.

Since v12.8, X-Ways Forensics no longer employs Windows' logic for converting UTC to local filetimes and displays timestamps independently of the time zone selected in the examiner's system's Control Panel. When working with a case, the time zone selected for that case applies globally to the entire program (selectable in the Case Properties), otherwise the one selected in the General Options dialog. When working with a case, optionally it is possible to specify different time zones per evidence object, so that you can always see local filetimes even for media that were used in different time zones, if preferable. Note that the timestamps are converted for display only. That means, in a recursive view in the case root that covers multiple media, sorting is based on absolute UTC timestamps. Optionally, the actually used conversion bias can be displayed as well (see directory browser options).

Timestamps on FAT volumes are never converted as they are not available in UTC, but in one or several unknown local time zones.

Report tables and export lists are output in local time, for your convenience, and internally converted back to UTC when read. They remember based on which time zone they were output, so importing them yields correct timestamps even if you had changed the time zone for that evidence object or the entire case in the meantime. Report tables created by earlier versions of X-Ways Forensics, on the other hand, are imported assuming they were created in the time zone selected in the examiner's system's Control Panel, which is consistent behavior.

The time zone definitions can be adjusted, if necessary. Please note that changing these definitions in any dialog window affects the definition of time zones throughout the program.

WinHex and X-Ways Forensics still employs the standard Windows conversion technique, which depends on the time zone selected in the user's system's Control Panel:

- in File | Properties, where the timestamps of files on the user's own system can be accessed/changed,
- for its case logging features,
- generally when operated without a specialist or forensic license, and
- when operated without the file “timezone.dat”.

You can tell that either of the two latter is true if the time zone button in the General Options dialog is not available or visible.

4 Travailler avec l'éditeur hexadécimal

4.1 Démarrage rapide centralisé

Le Démarrage Rapide Centralisé est une fenêtre de dialogue affichée en option au démarrage est conçue comme un panneau de contrôle simplifié pour la mise en route de votre travail. Il permet d'ouvrir rapidement des fichiers, disques, modules de mémoire et dossiers, et jusqu'aux 255 derniers documents édités (16 par défaut, liste de gauche). Il peut s'agir de fichiers, dossiers, lecteurs logiques ou disques physiques. A l'ouverture WinHex restaure la dernière position du curseur, la position de défilement, et le bloc (s'il a été défini) de chaque document, sauf si l'option correspondante a été désactivée.

Depuis le démarrage rapide centralisé vous pouvez aussi accéder à des *projets* et *cas* (liste à droite dessus). Un projet est constitué d'un ou plusieurs documents à éditer (fichiers ou disques). Il mémorise les positions d'édition, de la taille et de la position des fenêtres et de quelques options d'affichage. En sauvegardant un groupement de fenêtres comme projet vous pouvez continuer à travailler sur plusieurs documents à l'endroit exact où vous les y aviez laissés précédemment, par un simple clic. Ceci est particulièrement utile pour les tâches récurrentes. Quand vous chargez un projet, toutes les fenêtres déjà ouvertes sont d'abord automatiquement fermées.

De plus, WinHex sauvegarde automatiquement comme projet le groupement des fenêtres à la fin d'une session de travail de WinHex, et peut le recréer au démarrage suivant. Chaque projet est sauvegardé comme fichier .prj. Il peut être supprimé et renommé depuis le démarrage rapide centralisé avec le menu contextuel ou en le sélectionnant et en appuyant sur la touche SUPPR/F2 du clavier.

Enfin, le démarrage rapide centralisé est l'interface d'où vous pourrez gérer les *scripts*. Vous pouvez vérifier, éditer, créer, renommer et supprimer des scripts par le menu contextuel. Pour exécuter un script, faites un double clic sur son nom ou un simple clic puis OK.

4.2 Saisie de caractères

En mode hexadécimal seuls des caractères hexadécimaux peuvent être entrés ('0'...'9', 'A'...'F'). En mode texte vous pouvez entrer toutes sortes de caractères: lettres, chiffres, signes de ponctuation et caractères spéciaux (par exemple '»', ']' et '^'). Utilisez le programme Grille de caractères de Windows pour trouver les combinaisons de touches correspondants à de tels caractères (par exemple , ALT+175 pour '»'). La police "WinHex" gère le symbole Euro (€).

4.3 Les modes d'édition

The details panel displays for each file/disk, in which mode it was opened. The details panel's context menu allows to selectively change the edit mode of the active window.

Mode vue seule: Recommended for computer forensic examinations. In order to enforce strict forensic procedures, the only mode available in X-Ways Forensics, except for files in the current case's directory and in the general folder for temporary files, to allow to decode, decrypt, and convert them, etc. Les fichiers/disques qui sont ouverts en mode vue seule ne peuvent pas être édités/modifiés (intentionally or accidentally), seulement affichés. En d'autres termes ces fichiers/disques sont ouverts en écriture protégée.

Mode edition par défaut: Les modifications de fichiers/disques ouverts dans le mode d'édition par défaut sont mémorisées dans des fichiers temporaires. Ces derniers sont créés dynamiquement. Only when you close the edit window or utilisez la commande "enregistrer" du menu Fichier, le fichier/disque original est mis à jour, after prompting the user.

Mode édition directe: Soyez précautionneux quand vous ouvrez des fichiers en mode d'édition directe. Toutes les modifications (saisies clavier, remplissage/déplacement de blocs, écriture de données du presse-papiers, remplacements,...) sont écrites *dans le fichier original* (en substitution) sans demande d'acquiescement préalable! Il n'est pas nécessaire d'enregistrer manuellement le fichier après l'avoir modifié. En fait, les modifications sont enregistrées automatiquement, en fin de tâche quand vous quittez la fenêtre d'édition. Cependant, vous pouvez utiliser la commande "Enregistrer" pour vous assurer que les modifications soient prises en compte à un moment donné. Le mode d'édition directe est recommandé dans les cas où le transfert de données du fichier original vers le fichier temporaire et vice versa, obligatoire en mode d'édition par défaut, prend trop de temps ou trop d'espace disque. Ceci peut être le cas lors de l'ouverture de très grands fichiers et l'édition de nombreuses données à l'intérieur de ceux-ci. Comme habituellement aucun fichier temporaire n'est nécessaire dans le cas du mode d'édition directe, ce mode d'édition est généralement plus rapide que le mode d'édition par défaut. Le mode d'édition directe est le seul mode disponible quand vous utilisez l'Editeur de RAM.

Même en mode d'édition directe la création d'un fichier temporaire est inévitable lorsque la taille du fichier est altérée.

4.4 Barre d'états

La barre d'états affiche les informations suivantes concernant un fichier:

1. Numéro de la page courante et nombre total de pages
2. Position courante (offset du fichier)
3. Traduction décimale des valeurs hexadécimales de la position courante
4. Début et fin du bloc courant (s'il y en a un)
5. Taille du bloc courant (ditto)

Cliquez sur le bouton gauche de la souris afin de...

1. Vous déplacer vers une autre page,
2. Vous déplacer vers un autre offset,
3. Définir le type de la traduction décimale
4. Définir le bloc.

Cliquez sur le bouton droit de la souris pour copier des parties d'information de la barre d'état vers le presse-papiers.

Un clic droit sur le 2ème champ de la barre d'état permet de basculer entre une présentation absolue de l'offset (par défaut) et relative. Ceci est utile si vous examinez des données organisées en enregistrements de longueur fixe. Une fois spécifiée la longueur en octets de l'enregistrement, la barre d'états affiche le numéro de l'enregistrement courant et l'offset relatif à l'intérieur de celui-ci.

Un clic droit sur le 3ème champ de la barre d'état permet de copier dans le presse-papiers les quatre valeurs hexa à la position courante en ordre inversé. Ceci est utile pour suivre les pointeurs.

4.5 Scripts

La plupart des fonctions de WinHex peuvent être automatisées, par exemple pour accélérer des tâches répétitives ou exécuter certaines tâches sur des ordinateurs distants et sans supervision. La possibilité d'exécuter des scripts autres que les exemples fournis est limitée aux seuls possesseurs d’une licence professionnelle ou supérieure. Les scripts peuvent être lancés depuis le démarrage rapide centralisé ou la ligne de commande. Vous pouvez interrompre un script en cours d'exécution en appuyant sur la touche Echap. Par leurs possibilités supérieures, les scripts remplacent les routines, seules méthodes d'automatisation dans les versions antérieures de WinHex.

Les scripts WinHex sont des fichiers texte avec l'extension ".whs". Ils peuvent être édités par n'importe quel éditeur de texte et consistent en une simple suite de commandes. Il est recommandé d'entrer une commande par ligne, simplement par clarté visuelle. Selon la commande, il peut être nécessaire de lui ajouter des paramètres. La plupart des commandes agissent sur le fichier ou le disque affiché dans la fenêtre active courante.

Voir Appendice B pour une description des commandes de scripts actuellement reconnues.

4.6 API WinHex

L'API (application programming interface) WinHex permet d'utiliser les capacités avancées de l'éditeur hexadécimal de WinHex par programmation depuis vos propres programmes C++,

Delphi ou Visual Basic. Il offre en particulier un moyen simple et commode d'accès aléatoire aux fichiers et disques.

Developing software that uses the WinHex API requires a valid *professional* or *specialist* WinHex license. De plus, vous devez importer, pour votre language de programmation choisi, le fichier DLL "whxapi.dll", et la documentation. Please find those files and more detailed information online at http://www.x-ways.net/winhex/api/.

Vous pouvez aussi *distribuer*, à la fois n'importe quel logiciel faisant usage des fonctions de l'API de WinHex et de WinHex lui-même (version sans license). There are two ways how to distribute WinHex:

1. Distribute the unlicensed WinHex version. For the API to work, l'utilisateur final devant obtenir les licenses profesionnelles en fonction du nombre d'installations de WinHex nécessaire.
-ou-
2. Recommended: distribute a special API version of WinHex that is configured to only provide the API functionality and that is available at a reduced price. You may place your order online at http://www.x-ways.net/winhex/api/. Volume discount available on request (please specify the number of licenses you are interested in). One WinHex API license needed per end user computer. The product will be licensed to you, you will be the actual owner of the licenses, but any of your customers may use them. The end user does not have to take care of anything related to WinHex.

4.7 Editeur de disque

L'éditeur de disque (menu "outils") vous permet d'accéder à une disquette ou à un disque dur à un niveau inférieur à celui du système de fichiers. Vous pouvez accéder au disque soit logiquement (c'est à dire sous contrôle du système d'exploitation) soit physiquement (sous contrôle du BIOS). Sur la plupart des systèmes d'ordinateur vous pourrez même accéder aux CD-ROM et DVD-ROM. There is an optional raw mode for optical drives that allows to read from audio CDs and also the complete 2352-byte sectors on data CDs (CD-ROM and Video CDs) that contain error correction codes.

Opening a *logical drive* means opening a contiguous formatted part of a disk (a partition) that is accessible under Windows as a drive letter. It's also called a “volume”. WinHex relies on Windows being able to access the drive. Opening a *physical disk* means opening the entire medium, as it is attached to the computer, e.g. a hard disk including *all* partitions. It could also called the “raw device”. The disk normally does not need to be properly formatted in order to open it that way.

Usually it is preferable to open a logical drive instead of a physical disk, because more features are provided in this case. For example, “clusters” are defined by the file system, the allocation of clusters to files (and vice versa) is known to WinHex, “free space” and “slack space” have a meaning. Only if you need to edit sectors outside a logical drive (e.g. the master boot record), if

you wish to search something on several partitions of a hard disk at the same time, or if a partition is damaged or formatted with a file system unknown to Windows, so Windows is unable to make it accessible as a drive letter, you would open the physical disk instead. Via the menu that appears when clicking the “Access” button, you may also open individual partitions from within a physical disk. WinHex understands both conventional MBR partitioning and Windows 2000's dynamic disks as organized by the LDM (Logical Disk Manager, specialist and forensic licenses only). All dynamic volume types are supported: simple, spanned, striped, and RAID 5. Holding the Ctrl key when opening hard disks disables detection and special handling of dynamic volumes and ensures the hard disk is treated like it has been partitioned in the conventional way.

Notez cependant les limitations suivantes:

- Sous Windows NT/2000/XP, des autorisations de l'administrateur sont nécessaires pour accéder aux disques durs.
- Sous Windows 9x, certaines obligations doivent être remplies pour accéder aux CD-ROM et DVD (consultez Appendice C).
- Les fonctions de remplacement ne sont pas disponibles.
- WinHex ne peut pas *écrire* sur CD-ROM et DVD.
- L'éditeur de disque ne gère pas les lecteurs en réseau.

L'appendice E de ce manuel vous fournit les spécifications du secteur "master boot", qui peut être édité en utilisant l'éditeur de disque.

Editer l'espace libre sur disque (Windows 95/98/Me)

Sous Windows 95/98/Me, il est possible d'éditer les espaces couramment inutilisés d'un disque logique. Pour ce type d'utilisation, les limitations mentionnées ci-dessus ne s'appliquent pas. Winhex créé un fichier qui utilise la totalité de l'espace libre sur le disque sélectionné. Vous pouvez éditer ce fichier en mode d'édition directe. L'intégrité des données dans les parties utilisées du disque ne risquent pas être affectées.

Vous pouvez utiliser cette fonction pour récupérer des données effacées (non intentionnellement) mais qui n'ont cependant pas encore été écrasées par de nouveaux fichiers. Recherchez les données, marquez les comme bloc courant et copiez-les. Bien sûr, les données qui ont été effacées en utilisant la commande "Effacement irréversible" ne peuvent en aucun cas être trouvées dans les parties inutilisées du disque.

Enregistrer les secteurs: Peut être utilisé d'une manière analogue à la commande "Enregistrer" des fichiers. Toutes les modifications sont écrites sur le disque. Notez que ceci peut entraîner de sérieux dommages quant à l'intégrité des données du disque. Si l'option correspondante "revenir" (undo) est validée, une sauvegarde des secteurs concernés est créée, avant que les nouvelles données ne soient écrasées.
La commande ne peut pas être utilisée tant que vous ne vous êtes pas un utilisateur enregistré.

4.8 Editeur de RAM

L'éditeur de RAM vous permet d'examiner the physical RAM/main memory (under Windows 2000/XP, with administrator rights only) et la mémoire virtuelle d'un processus (c'est à dire un programme en cours d'exécution). Toutes les pages de mémoire utilisée par ce processus sont présentées en un bloc contigu. Les pages inutilisées (libres ou réservées) sont ignorées by default, but optionally included and displayed with “?” characters. With no gaps, you may compare memory dumps to files exactly with one another (absolute and virtual addresses are identical), e.g. to examine stack and heap states or observe virusses.

Sélectionnez un des processus listés. Vous pouvez accéder soit à la mémoire primaire soit à la totalité de la mémoire du processus ou à l'un des modules chargés par le processus. La mémoire primaire est utilisée pour pratiquement tous les usages. D'habitude elle contient aussi le module principal du processus (le fichier EXE). La "mémoire entière" contient la totalité de la mémoire virtuelle d'un processus exceptés les modules système. Sous Windows 95/98/Me, les modules systèmes sont listés d'une manière optionnelle. Tous les modules qui sont chargés au-dessus de la barrière des 2 GO (tel que kernel32.dll, gdi32.dll) sont définis comme des modules système. Ils sont partagés entre tous les processus d'exécution.

Notez les limitations suivantes:

- Attention: Seules les saisies clavier peuvent être annulées!
- La mémoire virtuelle des processus 16 bits n'est que partiellement accessible sous Windows 95/98/Me.
- L'édition est seulement possible en mode d'édition directe.
- Les modules système de Windows 95/98/Me peuvent seulement être examinés en mode vue, mais non modifiés.

Les options relevant de l'éditeur de RAM sont "Intégrité de la mémoire virtuelle" et "Adresses virtuelles".

4.9 Editer avec des formulaires

Un formulaire ("template") est une boîte de dialogue qui fournit les moyens d'éditer des structures de données définies par l'utilisateur d'une manière plus sûre et plus confortable que l'édition de données hexadécimales brutes. L'édition est faite dans des boîtes d'édition distinctes. Les modifications prennent effet quand vous appuyez sur la touche **ENTREE** ou quand vous quittez le formulaire après confirmation. Les données peuvent provenir d'un fichier, de secteurs de disque, ou de la mémoire virtuelle. Quand vous éditez des bases de données en particulier, il peut être préférable de définir un formulaire sur-mesure pour un accès plus facile aux enregistrements. Vous trouverez la commande d'impression de formulaires dans le menu système.

Les *définitions de formulaires* sont stockées sous format texte. L'*Editeur de formulaires* vous permet d'écrire des définitions de formulaires et en vérifie la syntaxe. Une définition de formulaire contient principalement des déclarations de variables, semblables à celles du code source des langages de programmation. La syntaxe est détaillée dans l'Appendice A. Les types de

données supportés comprennent toutes les variables habituelles: entières, en virgule flottante et booléenne, les types de dates, et les types hexadécimal, binaire, caractère et chaîne. On peut utiliser des tableaux de variables uniques ou de groupes de variables.

La possibilité de se déplacer librement dans les données vers l'avant ou l'arrière rend l'emploi des formulaires particulièrement flexible:

- Une même variable peut être interprétée et manipulée de différentes façons.
- Les blocs de données non concernés peuvent être ignorés.

Le *gestionnaire de formulaires* liste tous les fichiers texte du répertoire de WinHex contenant des définitions de formulaires. Le titre du formulaire, sa description, le nom du fichier et la date et l'heure de sa dernière modification sont affichés. Cliquez sur le bouton Appliquer pour afficher un formulaire en utilisant la définition de formulaire choisie pour les données de la fenêtre d'édition en cours à la position courante. Vous pouvez également créer une nouvelle définition de formulaire, et supprimer ou éditer un formulaire existant.

WinHex est livré avec plusieurs exemples de formulaires.

4.10 Conseils utiles

- Utilisez les boutons de la souris pou définir le bloc. Un double clic sur le bouton droit libère le bloc.
- Vous pouvez définir le bloc en utilisant le clavier (**MAJ**+Touche Flèches ou **ALT+1** et **ALT+2**)
- Utilisez la touche **TAB** pour commuter d'hexadécimal en mode texte.
- Utilisez la touche **INS** pour commuter d'overwrite en mode d'insertion.
- **CTRL**+**Q** ferme toutes les fenêtres.
- **ENTRÉE** affiche le Démarrage Rapide Centralisé.
- **ESC** annule l'opération courante s'il y en a une, sinon libère le bloc, ferme la fenêtre de dialogue ou la fenêtre de formulaire.
- **PAUSE** arrête ou continue l'opération courante.
- **F11** répète la dernière commande "Aller à la Position". **CTRL**+**F11** works in the opposite direction (from the current position).
- **ALT**+**+** is a variant of the Go To Offset command specifically to jump a certain number of sectors *down*.
- **ALT**+**-** is another variant specifically to jump a certain number of sectors *up*.
- **MAJ**+**F7** choisit un jeu de caractères.
- (**MAJ**+**ALT**+**F11)** répète la dernière commande Déplacement Bloc
- **CTRL**+**MAJ**+**M** invokes an open evidence object's annotations
- **ALT**+**F2** recalcule le auto-hash (checksum ou digest) après qu'un fichier a été modifié.
- **ALT**+**GAUCHE** et **ALT**+**DROITE** permet d'alterner entre les enregistrements dans un formulaire (comme les boutons "<" et ">"). **ALT**+↖ et **ALT**+**FIN** accèdent respectivement au début et à la fin de l'enregistrement.

- **ALT+G** déplace le curseur de la fenêtre d'édition vers la position courante du formulaire et ferme la fenêtre de formulaire.
- **ALT+G** moves the cursor in the edit window to the current template position and closes the template window.
- **CTRL+F9** ouvre le menu du bouton Accès (fenêtres d'édition de disque seulement).
- WinHex accepte les noms de fichiers spécifiés dans la ligne de commande et réalise les opérations glisser-lâcher.
- Utilisez des scripts pour rendre votre travail avec WinHex plus efficace.
- You can specify the name of a script as a command line parameter.
- «Invalid input»: After dismissing this error message box, the blinking cursor indicates what parameter provided by you is invalid and needs to be corrected.
- Commutez la présentation du décalage d'hexadécimal en décimal en cliquant sur le nombre affichant le décalage.
- Faites des essais en cliquant la barre d'état (boutons droit et gauche de la souris).

5 Récupération de Données

5.1 Récupération de fichier avec le navigateur de disque

Most obviously, deleted files and directories that are listed in the directory browser can be recovered easily and selectively with the directory browser's context menu. See chapter "directory browser".

5.2 Récupération de fichier par *nom*

This is a very easy to use mass file recovery function, part of the the Disk Tools menu. Requires that you have opened a logical drive or a single partition of a physical disk with the disk editor. Works on FAT12, FAT16, FAT32, and NTFS drives. You may specify one or more filename patterns that cover all the files you wish to retrieve, e.g.:

```
Letter to Mr. Smith.doc
Invoice*.pdf
m*.xls
Image*.gif
*.tif
```

You may exclude files using filename patterns that begin with a colon (:). For example, you may include all files except NTFS system (which always start with a dollar sign) files by providing the following patterns:

```
*
:$*
```

Please note that files that were moved to the recycle bin prior to permanent deletion are internally

renamed by Windows, where only the filename extension remains the same, so using wildcards will often come handy (e.g. *.jpg instead of abc.jpg). Unlike File Recovery by Type, this function will also restore the file date & time and its attributes.

Optionally this function recovers/copies only those files that currently exist in the file system (from a user's pointer of view) or that are considered non-existent (deleted or otherwise lost).

Alternatively to using the file allocation table of a FAT drive, WinHex can optionally also rely on files not being fragmented, recovering them as a continuous stream of consecutive clusters.

Check "Intercept invalid filenames" to prevent a failure of the recovery because of filenames with characters considered as invalid by the file system. Useful for example if you wish to recover files that had filenames in a non-western language with a western-language Windows version. This option will rename such a file if necessary to ensure that it can be recreated.

On an NTFS drive, if the file you are looking for cannot be found, it may help to enable the "thorough" search. It is not enabled by default because it takes significantly more time.

You must also specify an output folder where to recreate the original file(s). Important: make sure this folder is on a different drive. Specifying a folder on the same drive where you are recovering from could easily overwrite disk space where deleted files reside that you still wish to recover! That way they would be lost forever. It might also lead to a loop, if WinHex repeatedly "recovers" files that it has just recreated.

5.3 Récupération de fichier par *type*

La deuxième fonction automatique pour la récupération de données du menu Outils de Disque. Elle sert à la restauration de fichiers d'un certain type. This recovery method is also referred to as "file carving". Elle recherche les fichiers qui peuvent être reconnus à un en-tête particulier (signature, a certain sequence of byte values). Because of this approach, File Recovery by Type does not depend on the existence of functional file system structures. When found based on the signature, the files are saved to the output folder that is specified by the user. Optionally, recovered files of each type are put into their own subfolder (...\JPEG, ...\HTML, etc.). Note that File Recovery by Type assumes contiguous file clusters, so produces corrupt files in case the files were originally stored in a fragmented way. A log file "File Recovery by Type.log" about the selected parameters and the recovery results is written to the output folder for verification purposes.

Since no use is made of a possible presence of a (functional or non-functional) file system, the original *file sizes* are principally *unknown* to this algorithm, and so are the original *filenames*. That is why the resulting files are named according to the following pattern: Prefix[X]id0000.ext. "Prefix" is an optional prefix you provide. "id" is a unique character combination that identifies an entry in the file type definition database (aa = 1st entry, ab = 2nd entry, ...). "0000" is an incrementing number per file type. "ext" is the filename extension that corresponds to the file header signature according to the file definition database. WinHex can often detect if recovered

JPEG, GIF, and files of some other types, are corrupt or incomplete (caused e.g. by file fragmentation). If this is the case, it will mark these files as corrupt in the log file and insert a capital X in the output filename. If the user-supplied file size limit is found to be too small for certain files, this will be noted in the log file as well. The output filename prefix may optionally contain a placeholder *%d*, which will be replaced by the drive name. This is useful if you apply File Recovery by Type to multiple drives at a time and wish to be able to easily distinguish files from different drives even without checking the log file.

The algorithm tries to determine the original size of JPEG, GIF, PNG, BMP, TIFF, CDR, AVI, WAV, ZIP, MS Word, MS Excel, MS PowerPoint, RTF, PDF, and HTML files by examining their data structure, roughly limited by the user-supplied maximum size. The corresponding entries in the file type definition database must not be altered in order for the size and type detection to work for these file types. For other types, the files are recovered at the exact size specified by the user as the maximum (in KB). Be generous when specifying this size because whereas files recovered "too large" can still be opened by their associated application, truncated files often can't be and are obviously incomplete.

Technically it is possible to select as many file types for simultaneous recovery as you like. However, if you e.g. recover MS Office and AVI files at the same time and the MS Office files you expect are around a few KB and the AVI files around a 1 GB in size, using a single global maximum file size would not be a good idea. That's why optionally you can define an individual default size for each file type in the file type definition database.

By default, file headers are only searched at *cluster* boundaries because the beginning of a cluster is the only place where a file can start in a cluster-based file system. However, you may also select to search for sector-aligned file headers. This is useful to find files from a previously existing volume with a different cluster layout. If performed on a physical medium or raw file with no cluster layout defined, WinHex searches at sector boundaries anyway if cluster boundaries are selected. There is yet another possibility, a thorough byte-level search. This is necessary when recovering files from backup files or tapes, or JPEG files from within MS Word documents, where they are not aligned at cluster or sector boundaries. This comes at the cost of a possibly increased number of false positives, though, misidentified file signatures occurring randomly on a media, not indicating the beginning of a file.

You may limit the scope of the recovery to a currently selected block if necessary and/or to allocated or unallocated space (option available on a logical drive or volume). E.g. in order to recover files that were deleted, you select to recover from unallocated space only. Files that are not accessible any more because of file system errors may still be stored in clusters that are considered as in use.

The option "Ext2/Ext3 block logic" causes this recovery method to deviate from the standard assumption of no fragmention in that it will follow the typical Ext block pattern, where e.g. the 13th block from the header of the file is considered an indirect block that references the following data blocks. This option has no effect when applied to partitions that WinHex knows have a file system other than Ext2 and Ext3 or when a header is found that is not block-aligned.

5.4 File Type Definitions

"File Type Signatures.txt" is a tab-delimited text file that serves as a file type definition database for contents tables and for the File Recovery by Type command.

WinHex comes with various preset file type signatures. You may fully customize the file type definitions and add your own ones, either in "File Type Signatures.txt" itself or you create additional such files of the same format named "File Type Signatures *.txt", which will be loaded as well and have the benefit that they will not be overwritten when you install the next update. Up to 255 entries are supported altogether.

When you click the Customize button to edit the file "File Type Signatures.txt", by default WinHex opens the file in MS Excel. This is convenient because the file consists of columns separated by tabs. If you edit the file with a text editor, be sure to retain these tabs, as WinHex relies on their presence to properly interpret the file type definitions. MS Excel retains them automatically. After editing the file type definitions, you need to exit the dialog window and invoke the File Recovery by Type or Create Drive Contents Table menu command again to see the changes in the file type list.

1st column: File Type

A human-readable designation of the file type, e.g. "JPEG". Everything beyond the first 19 characters is ignored.

2nd column: Extensions

One or more file type extensions typically used for this file type. E.g. "jpg;jpeg;jpe". Specify the most common extension first because that one will be used by default for naming recovered files. Everything beyond the first 45 characters is ignored.

3rd column: Header

A unique header signature by which files of this file type can be recognized. May be specified in either ASCII or hex (e.g. 0xFFD8FF means the bytes 0xFF 0xD8 0xFF). Header signatures up to 16 bytes in size are supported. To find out characteristic file header signatures in the first place, open several existing files of a certain type in WinHex and look for common byte values near the beginning of the file at identical offsets.

4th column: Offset

The relative offset within a file at which the signature occurs. Often simply 0.

5th column: Footer

Optional. A signature (constant byte sequence) that reliably indicates the end of a file. May be specified in either ASCII or hex. A footer signature may help to force a recovery with the correct

file size. Still, the recovery algorithm does not search for the footer further than the number of bytes specified as the maximum file size, starting from the header. Footer signatures up to 8 bytes in size are supported.

6th column: Default in KB

Optional. A file type specific default maximum file size in KB that can override the global maximum file size specified in the File Recovery by Type dialog window. Useful because e.g. an MPEG video could be more around 1 GB in size, where a Windows icon file (.ico) could be around 1 KB in size.

5.5 Récupération de données manuelle

Aside from offering various automatic data recovery mechanisms, WinHex is a powerful tool to manually recovery data. Il est possible de restaurer des fichiers perdus ou logiquement supprimés (ou plus généralement: des données) qui sont simplement marqués comme supprimés dans le système de fichiers mais n'ont pas été *physiquement* effacés (ou écrasés).

Ouvrez le lecteur logique sur lequel le fichier supprimé était enregistré dans l'éditeur de disque. Pour l'essentiel, vous pouvez recréer un tel fichier en sélectionnant les secteurs disque qui étaient alloués au fichier comme bloc courant et en les sauvegardant par le menu Edition | Copier le Bloc | Dans un Nouveau Fichier. Mais il peut être difficile de *trouver* les secteurs où le fichier est encore stocké. Il y a deux manières de le faire:

1. Si vous pouvez identifier un fragment du fichier recherché (ex: la signature caractéristique de l'en-tête d'un fichier JPEG ou les mots "Cher M. Legrand" dans un document MS Word), cherchez-le sur le disque avec les fonctions de recherche habituelles ("Chercher Texte" ou "Chercher Chaîne Hexa"). Cette méthode est simple et sûre, et peut être recommandée pour tous les utilisateurs.

2. Si vous ne connaissez que le nom du fichier, vous devrez avoir une idée du système de fichiers sur le disque (FAT16, FAT32, NTFS, ...) pour localiser des traces d'anciennes informations de dossiers du fichier et ainsi déterminer le numéro du premier cluster qui était alloué au fichier. Des renseignements détaillés sur les systèmes de fichiers sont disponibles sur le site de WinHex. Ce qui suit s'applique à tous les types de FAT:

   Si le dossier qui *contenait* le fichier (appelons ce dossier "D") existe encore, vous trouverez D sur le disque en utilisant Outils | Outils de Disque | Lister les Clusters d'un Dossier. Le formulaire standard pour les entrées de dossiers FAT livré avec WinHex vous aidera alors à trouver le numéro du premier cluster qui était alloué au fichier supprimé dans ce dossier. Sinon, si D a été également effacé, vous devrez trouver le contenu de D (en utilisant le formulaire d'entrées de dossiers) en commençant par le dossier qui contenait D.

   Les fichiers et dossiers supprimés sont marqués du caractère "å" (hexadécimal: E5) comme première lettre du nom.

Vous rencontrerez peut-être le problème d'un fichier à récupérer fragmenté, c'est-à-dire sauvegardé dans des clusters non contigus. Sur les lecteurs FAT, le cluster suivant d'un fichier peut être localisé dans la table d'allocation des fichiers au début du, mais cette information est effacée quand le fichier est effacé.

6 Référence Menu

6.1 Menu Fichier

Nouveau: Cette commande est utilisée pour créer un fichier. Le fichier est principalement ouvert en mode d'édition par défaut. Vous devez spécifier la taille du fichier.

Ouvrir: Vous permet d'ouvrir un ou plusieurs fichiers. Vous pouvez choisir un mode d'édition dans le cas où il ne serait pas prédéterminé dans le menu Options.

Enregistrer: Enregistre le fichier couramment affiché sur le disque. En mode d'édition directe, utiliser cette commande n'est pas nécessaire. Lors de l'utilisation de l'Editeur de Disque, cette commande se nomme "Enregistrer des secteurs".

Enregistrer sous: Enregistre le fichier couramment affiché sous un nom différent.

Créer une Sauvegarde: voir „Sauvegarde“

Charger une Sauvegarde: Sélectionne un fichier d’image ou de sauvegarde (fichier WHX) dont vous voulez restaurer le contenu (soit un fichier, soit un ou des secteurs de disque).

Gestion de Sauvegardes: voir ci-dessous

Exécuter: Exécute soit le fichier courant soit le programme y associé, si le fichier courant n'est pas un programme exécutable (.exe, .com).

Imprimer: Utilisez cette commande pour imprimer un fichier ou des secteurs. Indiquez les marges à imprimer. Vous pouvez sélectionner et configurer une imprimante. Choisissez le jeu de caractères et acceptez ou changez la taille suggérée. La taille de police est calculée comme suit: la résolution d'impression (par exemple 720 dpi) / 6 (par exemple = 120). Si désiré, vous pouvez ajouter un commentaire qui sera imprimé à la fin.
Au cas ou vous auriez besoin d'imprimer d'une façon plus flexible, vous pouvez définir un bloc et le copier en utilisant "Edition/Copier/Affichage de l'éditeur" comme texte "formaté éditeur hexadécimal" dans le presse-papiers. Vous pourrez alors le coller dans votre traitement de texte favori. Il aura une excellente allure en "Courier New", 10pt.

Propriétés: Vous permet d'éditer la taille, les marques de temps et les attributs d'un fichier et d'un dossier. Les attributs valides sont A (archive), H (caché), R (lecture seule). Après entrée de nouvelles valeurs dans certaines zones (taille, temps ou attributs) appuyez simplement sur la touche Entrée, pour que les modifications prennent effet.

Ouvrir Dossier: Cette commande est utilisée pour ouvrir, en même temps, plusieurs fichiers présentant des exigences spéciales. Sélectionnez un dossier dans lequel vous voulez ouvrir un fichier. Eventuellement ouvrez même un sous-dossier. Vous pouvez spécifier des masques de fichier (par exemple "w*.exe;x*.dll"). Il y a aussi la possibilité d'ouvrir seulement les fichiers qui contiennent un certain texte ou une certaine valeur hexadécimale. Les dialogues standards de recherche sont affichés sur demande à ce propos. Si WinHex n'est pas configuré pour travailler comme afficheur ou en éditeur de remplacement (ceci peut être fait dans le menu Outils), vous pourrez choisir un mode d'édition.

Enregistrer les Fichiers Modifiés: Tous les fichiers qui ont été modifiés par vous de quelque manière que ce soit sont écrits sur disque.

Enregistrer Tous les Fichiers: Tous les fichiers non ouverts en mode vue seule seront écrits sur disque.

Quitter: Utilisez cette commande pour quitter WinHex. Vous aurez l'opportunité d'enregistrer les modifications de fichiers et de disques.

6.2 Menu Edition

Annuler: Annule la dernière modification, au cas où l'option correspondante a été activée.

Couper: Enlève le bloc courant du fichier et le met dans le presse-papiers. Les données derrière le bloc sont extraites et remises à la place du premier bloc.

Copier un bloc/tous/un Secteur:

- **Normal:** Copie le bloc courant / le fichier entier / le secteur courant dans le presse-papiers. Le contenu du presse-papiers peut être collé ou écrit plus tard.
- **Dans un nouveau fichier:** Copie les données directement dans un nouveau fichier (pas en utilisant le presse-papiers). Par exemple, cette commande peut être utilisée pour récupérer, à partir d'un disque, un fichier perdu.
- **Valeurs Hexa:** Copie les données comme des valeurs hexadécimales concaténées.
- **Affichage de l'Editeur:** Copie les données comme texte, formatées comme si elles étaient affichées par l'Editeur Hexadécimal, c'est à dire avec un décalage, une partie hexadécimale et une colonne texte.
- **Code Source en C/Pascal:** Copie les données formatées comme code source en C/Pascal.

Coller le Presse-papiers: Insère le contenu du presse-papiers à la position courante du fichier en cours. Les données du fichier après cette position sont déplacées.

Ecrire le Presse-papiers: Copie le contenu du presse-papiers à la position courante du fichier en cours. Les données après cette position sont écrasées. Si la fin du fichier est atteinte, la taille du fichier est augmentée du contenu du presse-papiers.

Coller le Presse-papiers dans un Nouveau Fichier: Créé un nouveau fichier utilisant le contenu du presse-papiers.

Vider le Presse-papiers: Cette commande est utilisée pour libérer la mémoire occupée par le presse-papiers.

Supprimer: Efface le contenu du bloc du fichier. Les données après le bloc sont déplacées vers le début de l'ancien bloc. Le presse-papiers n'est pas affecté par cette commande. Si le bloc est également défini dans tous les fichiers ouverts (c'est à dire qu'il commence et finit avec les mêmes offsets), cette commande peut même être appliquée à tous les fichiers en cours ouverts.

Coller des Octets Zéro: Utilisez cette commande pour insérer des octets à zéro à la position courante d'un fichier.

Définir Bloc: Cette fonction est accessible à partir du menu et de la barre d'état. Une boîte de dialogue vous permet de spécifier les limites du bloc. Cette commande peut aussi être appliquée à tous les fichiers ouverts.

Tout Sélectionner: Définit le début et la fin du fichier courant comme limites du bloc courant.

Convertir: cf. Conversions

Modifier les Données: ci-dessous

Remplir un Bloc/un Fichier/des Secteurs Disque: ci-dessous (Effacer et initialiser)

6.3 Menu Recherche

Chercher Texte: Cette commande est utilisée pour trouver une chaîne spécifique allant jusqu'à 50 caractères dans le fichier courant (cf. Options de Recherche). Specialist and forensic licenses only: identical to Simultaneous Search, unless Shift key is pressed.

Chercher Chaîne Hexa: Cette commande est utilisée pour chercher une séquence pouvant comporter jusqu'à 50 valeurs hexadécimales à deux caractères.

Remplacer Texte: Cette commande est utilisée pour remplacer les occurrences d'une chaîne spécifique par une autre chaîne (chacune d'elles pouvant comporter jusqu'à 50 caractères), cf. Options de Remplacement.

Remplacer Chaîne Hexa: Cette commande fonctionne exactement comme Remplacer un Texte, sauf qu'elle s'applique à une séquence de valeurs hexadécimales (50 au maximum), cf. Options de Remplacement.

Recherche Simultanée: see Specialist menu

Indexing: Available only with a forensic license, for evidence objects. Creates an index of all words in all or certain files in the volume snapshot, based on ASCII characters you provide. This is a time-consuming process and principally will require large amount of drive space (rule of thumb for default settings and average data: 15-60% of the original amount of data). However, the index will allow you to conduct further searches very quickly and spontaneously. The index files are saved in the metadata output folder of the corresponding evidence object. The scope of the index, i.e. which files are to be indexed, can be fine-tuned. The default setting is that all existing files (including their slack, unless disabled in the directory browser options) plus the fictitious files (which includes all free space) will be index. This avoids that certain parts of free space are indexed multiple times if they are referenced by several deleted files at the same time.

Words shorter than a lower limit you specify are ignored. The longer the minimum length in characters, the small the index and the faster the indexing procedure. The default lower limit are 3 characters. Frequent irrelevant words can be excluded from the index in the exception list with a minus prefix (e.g. -and), which reduces the size of the index and the time needed to create it. A noticably smaller index and an acceleration can be achieved by specifying 4 as the minimum length in characters. You could then still add important 3-letter words to the exclusion list with a plus prefix (e.g. +xtc), which overrides the lower limit. The exception list does not have to be sorted alphabetically. Words *longer* than the *upper* limit you specify are truncated in the index.

X-Ways Forensics does not distinguish between uppercase and lowercase letters. If you have X-Ways Forensics include substrings in the index, this will further slow down index creation (by a factor of 3 to 5) and inflate the index, however, you will later be able to find e.g. "paper" in "newspaper" and "solve" in "resolve". If you do not include substrings in the index, it will still be possible to search the index for substrings later, but the result will be incomplete, and the search speed is much slower. The more main memory you allow X-Ways Forensics to use for indexing, the faster the indexing procedure. Just note that if the specified amount of main memory is not available, indexing may fail and you may need to start over. Indexing will be unnecessarily slow if you index data that resides on the same disk with the case data, where the index is created. Try to avoid indexing with an active Internet connection if your Windows system is configured to download updates and reboot automatically upon installation.

Search in Index: After indexing files, you may search the index for keywords very quickly. Type in a single keyword and press Enter. Anything in excess of 8 characters is ignored. X-Ways Forensics does not distinguish between uppercase and lowercase letters. If listing search hits takes too long, e.g. because you entered a single character only or a very frequent short word, you may press Esc or close the progress indicator window to abort. In the search hit list, physical offsets are not available, and sorting by the search term has no effect.

Export Word List: Available once an index has been created. Allows to save a list of all the

word in the index to a text file. In that list, each word that occured in the files that were indexed will be present, and only contained once. Useful for a customized dictionary attack.

Recherche Combinée: Offre un mécanisme de recherche complexe. Dans un fichier courant et dans un second fichier un offset commun est recherché, où chaque fichier doit contenir les mêmes valeurs hexadécimales que celles spécifiées.

Valeur Entière: Saisissez un entier (dans les limites des données entières signées de 64 bits). Cette fonction recherche dans le fichier courant la donnée qui peut être interprétée comme cet entier.

Valeur Réelle: Entrez un nombre en flottant (tel que 12,34 = 0,1234 * 10^2 = 0,1234E2) et sélectionnez une donnée du type flottant. Cette fonction recherche recherche dans le fichier courant la donnée qui peut être interprétée comme cette valeur flottante.

Extraits de Texte: Utilisez cette commande pour rechercher une séquence de lettres (a-z, A-Z), de chiffres (0-9) et/ou des signes de ponctuation. Cette fonction est utile par exemple si vous avez l'intention d'éditer des passages de texte cachés quelque part à l'intérieur d'un fichier au milieu d'un code exécutable.
Fixez le degré de sensibilité de la recherche en spécifiant la longueur que doit avoir la séquence de caractères pour être reconnue. Cliquez sur "Tolère les Caractères Unicode" de façon à forcer l'algorithme à accepter des octets à zéro entre deux caractères.

Continuer Recherche Globale: Cette commande est utilisée pour poursuivre une opération de recherche globale (c'est à dire une recherche appliquée à tous les fichiers ouverts) dans le fichier suivant.

Continuer Recherche: Vous permet de poursuivre une opération de recherche dans un fichier courant à la position courante.

6.4 Menu Position

Aller à la Position: Déplace la position courante à l'offset spécifié. Normalement ceci est fait d'une manière relative à partir du début de fichier (offset nul). Vous pouvez déplacer le curseur relativement à la position courante (en avant ou en arrière) ou à partir de la fin du fichier (en arrière). Un offset peut être spécifié en octets (par défaut), en mots (2 octets), en double mots (4 octets), en enregistrements (si cette option est active), ou en secteurs. Appuyer sur F1 pour répéter le dernier déplacement de position.

Aller à la Page/au Secteur: Déplace à la page ou au secteur de disque spécifié. Sector and cluster numbers may optionally be entered in hexadecimal notation (with the 0x prefix). Please note that the data area on FAT drives starts with cluster #2.

Go To FAT Entry/FILE Record: Jump to a certain entry in the file allocation table on a FAT

drive or to a certain FILE record in the master file table on an NTFS drive, respectively.

Déplacer Bloc: Déplace le bloc courant sélectionné en avant ou en arrière, mais non les données du bloc. Spécifiez la distance en octets. Appuyez sur ALT+F11 pour répéter le dernier mouvement de bloc, appuyez sur MAJ+ALT+F11 pour inverser le mouvement. Cette commande peut faciliter l'édition d'un fichier qui consiste en enregistrements homogènes de longueur fixe.

WinHex conserve un historique de vos sauts d'offset dans un document et permet de reculer et d'avancer dans la séquence de chaîne ultérieurement.

Atteindre...

Début de Fichier: Affiche la première page du fichier courant et déplace la position courante au décalage 0...15.

Fin de Fichier: Affiche la dernière page du fichier courant et déplace la position courante sur le dernier octet (offset = taille du fichier - 1).

Début de Bloc: Déplace la position courante au début du bloc courant.

Fin de Bloc: Déplace la position courante à la fin du bloc courant.

Placer Marqueur: Marque la position courante et vous rend ainsi capable de la retrouver ultérieurement.

Effacer Marqueur: Efface le marqueur de l'écran.

Atteindre Marqueur: Déplace la position courante vers celle établie par le Marqueur de Position.

Gestion de Signets: ci-dessous

6.5 Menu Affichage

Affichage Texte Seul: Cache l'affichage hexadécimal et utilise la fenêtre éditeur entière pour l'affichage de texte.

Affichage Hexa Seul: Cache l'affichage de texte et utilise la fenêtre éditeur entière pour l'affichage hexadécimal.

Affichage d'Enregistrement: A l'édition d'enregistrements consécutifs de données de même taille (par exemple matrice d'entrées d'une base de données) vous pouvez laisser WinHex afficher chaque autre enregistrement avec une couleur de fond différente, comme une sorte d'aide visuelle. La couleur peut être choisie dans la boite de dialogue "Options Générales". Une fois spécifiée la

longueur en octets de l'enregistrement et le décalage du premier enregistrement, la barre d'états peut afficher le numéro de l'enregistrement courant et le décalage relatif à l'intérieur de celui-ci.
Si n'importe quelle des deux options d'enregistrements est activée, la commande Aller à la Position permet le déplacement de la position courantes dans des unités de la taille de l'enregistrement courant.

Afficher: The Case Data window is part of the forensic user interface of WinHex (X-Ways Forensics). Le **navigateur de disque** est disponible pour les lecteurs logiques/les partitions ouverts avec l'éditeur de disque. L'**Interpréteur de données** est une petite fenêtre qui fournit des "services de traduction" pour les données de la positon courante du curseur. La **barre d'icônes** est affichée en option également. Le **contrôle tab** rend chaque fenêtre d'édition accessible par un simple clic. La **section de détails** fournit une information détaillée sur tout objet ouvert (fichier, disque, RAM).

Gestion de Formulaires

Tables: Fournit quatre tables de conversion (cf. ASCII ANSI/IBM).

Lignes & Colonnes

Synchroniser le Défilement: Synchronise jusqu'à quatre fenêtres en mosaïque en offsets absolus identiques. Hold the Shift key when enabling this feature to tile the windows horizontally instead of vertically.

Synchroniser et Comparer: Synchronise jusqu'à quatre fenêtres et affiche visuellement les différences de valeur pour chaque octet. If no more than two windows are involved, WinHex conserve l'écart initial entre les offsets du premier octet affiché dans les deux fenêtres d'édition lors du scroll. Ne pas synchroniser les offsets absolus est utile par exemple pour comparer deux copies de la table d'allocation de fichiers, qui ont évidemment des différences d'offset**.** Vous pouvez aller à la difference de la valeur de l'octet suivant ou précédant en cliquant sur les boutons supplémentaires rajoutés sur l'une des deux fenêtres d'édition.

Rafraîchir l'Affichage: Repeint la fenêtre d'édition courante. In case the current file was updated by an external program, WinHex offers to dismiss any changes made in WinHex and reload the file from scratch.

6.6 Menu Outils

Ouvrir Disque: Consultez chapitre "Editeur de Disque".

Cloner Disque: Consultez chapitre "Clonage de Disque".

Recupération des Fichiers: Voir Appendice D.

Nouveau Instantané du Disque: Disponible pour les partitions with one of the supported file systems. WinHex parcourt les chaînes de clusters et en tire une carte du lecteur. Ensuite, WinHex est capable de remplir le navigateur de répertoire et de spécifier l'allocation de chaque secteur et chaque cluster (fichier, dossier, FAT, libre, ...). Il faut lancer cette fonction à nouveau après des opérations sur le lecteur pour actualiser l'affichage de WinHex. Consultez Options de Sécurité.

Initialiser d'Espace Libre: Il est possible que des informations confidentielles soient enregistrées dans des parties couramment inutilisées du disque suite à un effacement normal, une copie ou une opération d'enregistrement. L'espace libre sur disque peut être initialisé. Effectivement, pour des raisons de sécurité, ceci efface (écrase) toutes les données des parties inutilisées du disque et rend impossible la récupération de ces données. *Available in WinHex only, not in X-Ways Forensics.*

Initialiser l'Espace Chutes: Remplit l'espace chutes (les résidus, les octets inutilisés dans les derniers clusters respectifs de chaque chaîne de clusters, après la fin réelle d'un fichier) d'octets zéro. On peut utiliser cette fonction en même temps que "Initialiser l'espace libre" pour effacer de façon sûre des données sur un lecteur ou pour minimiser l'espace requis par un backup de disque compressé (tel qu'une sauvegarde WinHex). Fermer tout programme en cours d'exécution ou résident susceptible d'écrire sur le disque avant d'invoquer cette fonction. *Available in WinHex only, not in X-Ways Forensics.*

Nettoyer la MFT: On NTFS drives, WinHex can clear all currently unused $Mft (Master File Table) file records, as they may still contain names and fragments of files previously stored in them. *Available in WinHex only, not in X-Ways Forensics.*

Scan For Lost Partitions: Formerly existing hard disk partitions that were not automatically found when opening a physical hard disk and are not listed in the Access button menu may be found and properly identified with this command. This command searches for a master boot record and boot sector signature (0x55AA), optionally only from the first sector that follows the last (location-wise) partition that was already found, and lists newly found partitions in the Access button menu.

Interpret as Partition Start: When you find the start sector of a volume (e.g. lost partition) on a physical disk, this menu command allows you to make such a partition easily accessible via the Access button menu. If no known file system is detected starting at the currently displayed sector, you will be asked for the number of sectors that you wish to include in the newly defined partition.

Entrer Paramètres du Disque: En utilisant cette commande sur un disque physique, vous pouvez redéfinir le nombre de cylindres, de têtes et de secteurs par piste reconnus par WinHex. Ceci peut être utile pour accéder à des secteurs en surplus à la fin du disque (au cas où WinHex ne les reconnaîtrait pas automatiquement), ou pour ajuster le système de coordonnées CHS à vos besoins. Utilisez cette commande sur un lecteur logique pour redéfinir le nombre total de clusters détecté par WinHex sur le lecteur. Ceci peut s'avérer utile lors de l'examen de très gros DVD, qui sont détectés comme médias de 2 Go sous Windows 9x.

Ouvrir RAM: Consultez chapitre "Editeur de RAM".

View: Available only with a forensic license. Invokes the internal viewer.

External Viewer: Exécute un viewer externe comme p.e. Quick View Plus, as selected in the Options menu, and opens the current file.

Lancer X-Ways Trace: Available only if X-Ways Trace is installed. This software can analyze the Internet Explorer's index.dat history file and the Windows recycle bin's info2 files.

Calculatrice: Démarre le calculateur Windows "calc.exe". La commutation en mode scientifique est hautement recommandée.

Convertisseur Hexa: Cette commande fournit une boite de dialogue, qui vous permet de convertir des nombres hexadécimaux en nombres décimaux et vice versa. Tapez simplement le nombre et appuyez sur Entrée**.**

Tables: Fournit quatre tables de conversion (cf. ASCII ANSI/IBM).

Analyser Bloc/Fichier/Secteurs: Scrute les données dans le bloc courant/le fichier entier et compte les occurrences de chaque valeur d'octet (0...255). Le résultat est affiché graphiquement par des lignes verticales proportionnelles. Le nombre d'occurrences et le pourcentage sont affichés pour chaque valeur d'octet lors du déplacement de la souris sur la ligne verticale correspondante.
Utilisez cette commande par exemple pour identifier des données d'un type inconnu. Les données audio, les données compressées, les codes exécutables etc... produisent des graphiques caractéristiques. Please note that this feature is not intended for use with gigabytes of data. La somme de contrôle standard de 32 bit (la simple somme de tous les octets) et le CRC32 des données sont aussi affichés.
Utilisez le menu contexte de la fenêtre pour commuter la considération d'octet à zéro sur on ou sur off, to print the analysis window, or to export the analysis to a text file.

Calculer Hash: Calculates one of the following checksums/digest of the entire current file, disks, or the currently selected block: 8-bit, 16-bit, 32-bit, 64-bit checksum, CRC16, CRC32, MD5, SHA-1, SHA-256, or PSCHF.

6.7 Outils de fichier

Concaténer: Sélectionnez plusieurs fichiers-source, qui seront copiés dans un fichier-cible unique. Les fichiers-source ne seront pas affectés par cette fonction.

Découper: Cette commande crée plusieurs fichiers-cible utilisant le contenu d'un fichier-source unique. Spécifiez un décalage de séparation pour chaque fichier-cible. Le fichier-source n'est pas affecté par cette fonction.

Unifier: Sélectionnez deux fichiers-source et un fichier-cible. Les octets/mots des fichiers-source seront alternativement écrits dans le fichier-cible. Le premier octet/mot en tête sera celui spécifié en premier dans le fichier-source. Utilisez cette fonction pour créer un fichier avec des octets/mots impairs et pairs originaires de fichiers séparés. (par exemple, pour la programmation d'EPROM)

Disséquer: Sélectionnez un fichier-source et deux fichiers-cible. Les octets/mots en provenance du fichier-source seront écrits alternativement dans les fichiers-cible. Le premier octet/mot sera transféré dans le fichier-cible qui aura été spécifié en premier. Utilisez cette fonction pour créer deux fichiers séparés contenant l'un les octets/mots impairs et l'autre les octets pairs d'un fichier original. (par exemple, pour la programmation d'EPROM)

Comparer: Cette commande est utilisée pour comparer deux fenêtres d'edition (fichiers ou disques) octet par octet. Décidez lesquels des octets différents ou identiques feront l'objet du rapport. You may indicate how many bytes to compare. Si désiré l'opération se termine d'elle-même quand un certain nombre de différences ou de coïncidences a été rencontré. Le rapport est stocké dans un fichier texte, dont la taille peut s'accroître de façon spectaculaire.
The comparison starts at the respective offsets specified for each edit window. These offsets may differ, such that e.g. the byte at offset 0 in file A is compared to the byte at offset 32 in file B, the byte at offset 1 with the one at offset 33, etc. When you select an edit window for comparison, the current position will automatically be entered in the "From offset" box.
Il existe une autre fonction de comparaison dans WinHex: vous pouvez également comparer les fenêtres d'édition visuellement et synchroniser le défilement de ces fenêtres (voir menu Affichage).

Effacement irrévocable: Cette commande est utilisée pour effacer définitivement le contenu d'un fichier, de telle façon qu'il ne pourra pas être restauré par des programmes spéciaux de restauration. Chaque fichier sélectionné est rempli selon la configuration courante, réduit à une taille nulle et ensuite effacé. De même le *nom* du fichier est écrasé sur le disque. Même des tentatives professionnelles de restauration du fichier seront vaines. Par conséquent cette commande ne devrait être appliquée qu'à des fichiers aux contenus confidentiels, devant être détruits. *Available in WinHex only, not in X-Ways Forensics.*

6.8 Menu Spécialiste

Licences spécialiste et forensiques seulement.

Refine Volume Snapshot: voir si-dessus

Créer Table Contenu de Lecteur: voir si-dessus

Simultaneous Search: A parallel search facility, that lets you specify a virtually unlimited list of search terms, one per line (physical search). The search terms are either text strings or hex values (specified with a 0x prefix). They are searched simultaneously, and their occurrences can be archived in the Position Manager. WinHex will save the offset of each occurrence, the search

term, the name of the file or disk searched, and in the case of a logical drive the cluster allocation as well (i.e. the name and path of the file that is stored at that particular offset, if any).
That means e.g. a forensic examiner is now able to systematically search through multiple hard drives and disk images in a single pass for words like

- drug
- cocaine
- (street synonym #1 for cocaine)
- (street synonym #2 for cocaine)
- (street synonym #3 for cocaine)
- (street synonym #3 for cocaine, alternative spelling)
- (name of dealer #1)
- (name of dealer #2)
- (name of dealer #3)

at the same time. When searching a logical drive, this will narrow down the examination to a list of files upon which to focus. If you do not have WinHex archive the occurrences, you may use the F3 key to continue the search.

Créer Table pour un Répertoire: Fonctionne comme Créer Table Contenu de Lecteur, mais seulement pour un répertoire selectionné par l'utilisateur et les sous-répertoires. You will find this command only in the directory browser's context menu, when right-clicking a directory.

Media Details Report: Shows information about the currently active disk or file and lets you copy it e.g. into a report you are writing. Most extensive on physical hard disks, where details for each partition and even unallocated gaps between existing partitions are pointed out. Under Windows 2000 and XP, WinHex also reports the password protection status of ATA disks.
Forensic license only: WinHex is able to detect hidden host-protected areas (HPAs, a.k.a. ATA-protected areas) and device configuration overlays (DCO areas) on IDE hard disks up under Windows 2000 and XP. A message box with a warning will be displayed in case the disk size has been artificially reduced. At any rate, the real total number of sectors according to ATA, if it can be determined, is listed in the details report.

Interpreter Fichier Comme Disque: Traite un currently open and active disk image file as either a logical drive or physical disk. This is useful if you wish to closely examine the file system structure of a disk image, extract files, etc. without copying it back to a disk. If interpreted as a physical disk, WinHex can access and open the partitions contained in the image individually as known from “real” physical hard disks.
WinHex is even able to interpret *spanned* raw image files, that is, image files that consist of separate segments of any size. For WinHex to detect a spanned image file, the first segment may have an arbitrary name and a non-numeric extension or the extension “.001”. The second segment must have the same base name, but the extension “.002”, the third segment “.003”, and so on. Both the Create Disk Image command and the DOS cloning tool X-Ways Replica are able to image disks and produce canonically named file segments. Image segmentation is useful because the maximum file size supported FAT file systems is limited.
In some rare cases WinHex may be unable to correctly determine whether the first sector in an image is the sector that contains a master boot record or already a boot sector, and consequently interprets the image structure in a wrong way. If so, hold the Shift key when invoking this

command. That way WinHex will ask you and not decide on its own. When the segments of a raw image are spread across two different drives, you may hold the Control key to be able to specify the other storage location.
With a *forensic* license, WinHex can also interpret evidence files (.e01 images), which can be created with the Create Disk Image command.

Assemble RAID System: WinHex can internally destripe RAID level 0 and level 5 systems consisting of up to 5 components (physical hard disks or images). That way it is not necessary to use scripts that unstripe and export RAID systems to a new image, saving you time and drive space. Components that are available as images need to be opened and interpreted before you use this function. You need to select the components in the correct order. WinHex lets you specify the strip size in sectors (often 128) and different RAID header sizes per component (often simply 0). You can usually tell that either the component order, the stripe size, the stripe pattern, or the RAID header size is incorrect when no partitions are detected or partitions with unknown file systems or with file systems that cannot be interpreted properly.

When you add an assembled RAID system to a case (and optionally partitions opened from such a RAID system), the selected RAID configuration parameters are saved with the evidence objects, which allows to access the RAID system instantly in later sessions (forensic licenses only).

In RAID level 5, data is not only striped across all component disks in a rotating pattern, but also interspersed with parity blocks for redundancy. RAID level 5 is implemented in different ways by different RAID controller manufacturers in that they employ different stripe/parity patterns. The supported patterns are the following:

Backward Parity (Adaptec)
Component 0: 0 2 P
Component 1: 1 P 4
Component 2: P 3 5

Backward Dynamic Parity (AMI)
Component 0: 0 3 P
Component 1: 1 P 4
Component 2: P 2 5

Backward Delayed Parity (HP/Compaq)
Component 0: 0 2 4 6 8 10 12 14
Component 1: 1 3 5 7 P P P P
Component 2: P P P P 9 11 13 15

Forward Parity
Component 0: P 2 4
Component 1: 0 P 5
Component 2: 1 3 P

If one of the RAID component disks is not available, you can assemble a RAID 5 system

nonetheless because one component is redundant. Simply select a dummy substitute (one of the *other, available* components of the same RAID system) as the *missing* component and declare that component “missing”.

Collecter l'Espace Libre: Parcourt le lecteur logique ouvert et collecte tous les clusters non utilisés dans un fichier de destination que vous spécifiez. Utile pour examiner des fragments de données provenant d'anciens fichiers qui n'ont pas été effacés de façon sûre. Ne modifie aucunement le lecteur source. Le fichier-destination doit se trouver sur un autre lecteur.

Collecter l'Espace Chutes: Rassemble les "chutes" (les résidus, les octets inutilisés dans les derniers clusters respectifs de chaque chaîne de clusters, après la fin réelle d'un fichier) vers un fichier-destination. Sinon cette fonction est semblable à Collecter l'Espace Libre. WinHex ne peut pas collecter les chutes de fichiers compressés ou chiffrés au niveau du système de fichiers.

Gather Inter-Partition Space: Captures all space on a physical hard disk that does not belong to any partition in a destination file, for quick inspection to find out if something is hidden there or left from a prior partitioning.

Collecter Texte: Reconnaît le texte selon les paramètres spécifiés et capture toutes les occurrences trouvées dans un fichier, un disque, ou une zone de mémoire dans un fichier. Ce type de filtre est utile dans la mesure où il réduit considérablement la quantité de données à traiter, par exemple pour un spécialiste d'expertise légale en informatique qui cherche des indices sous forme de texte tel que messages emails ou documents, etc. Le fichier cible peut facilement être découpé à la taille définie par l'utilisateur. Cette fonction peut aussi être appliquée à un fichier rassemblant des espaces chutes ou de l'espace libre, ou à des fichiers endommagés de format propriétaire qui ne peuvent plus être ouverts par leur application d'origine, comme MS Word, pour récupérer au moins le texte non formaté.

Evidence File Container: Only available with a forensic license: Allows to create a new file container, open an existing one, and close the active file container. An evidence file container is a raw image file formatted with the XWFS file system by X-Ways AG. Files selected in the directory browser can be added to the active file container with the directory browser's context menu. Certain technical metadata (e.g. the original cluster allocation) are lost, however, name, path, size, attributes, timestamps, deletion state, and especially the contents of the file are fully retained in a file container. So when you need to pass on selected files (even from different evidence objects) that are of particular relevance to a case, in a single handy archive, to other persons involved in that case, who do not need to or must not see irrelevant files, this feature comes highly recommended. Evicence file containers can be interpreted and conveniently examined like other image files with X-Ways Forensics 12.6 and later. Please note that only files that are part of the volume snapshot can be added to a container. Once added, a file cannot be removed any more in this version. Hold the Shift key when invoking this command in order to specifically add file slack to the container as well. Hold the Ctrl key to add only a file's slack, not the file itself. Depending on the Security Options, your virus scanner might be able to prevent that viruses will be added to an evidence file container.

Bates-Number Files: Bates-numbers all the files within a given folder and its subfolders for discovery or evidentiary use. A constant prefix (up to 13 characters long) and a unique serial number are inserted between the filename and the extension in a way attorneys traditionally label paper documents for later accurate identification and reference.

Export Sécurisé: Résout un problème de sécurité. Lors d'un transfert de matériel non classé depuis un disque dur classé vers un support non classé, il faut être sûr qu'aucune information externe dans un cluster ou secteur "supplémentaire" ne sera accidentellement copiée avec le fichier lui-même, puisque cet espace mort peut encore contenir des informations classées datant d'une époque où elles étaient attribuées à un autre fichier. Cette commande copie les fichiers selon leurs taille courante, sans aucun octet supplémentaire. Elle ne copie pas de secteurs ou de clusters entiers comme le font les commandes de copie ordinaires. Multiple files in the same folder can be copied at the same time.

Highlight Free Space/Slack Space: Displays offsets and data in softer colors (light blue and gray, respectively). Helps to easily identify these special drive areas. Works on FAT, NTFS, and Ext2/Ext3 partitions.

6.9 Menu Options

Options Générales: ci-dessus

Programmes Externes: Here you can specify what external file viewing programs you would like to invoke from inside WinHex using the Tools menu. Also the installation path of the viewer component that is included in forensic licenses for v12.05 and later can be specified here (by default: subdirectory ..\viewer). The viewer component can also be specifically enabled or disabled.

Options de Sécurité: ci-dessus

Options d'Annulation: ci-dessus

Options de l'Interpréteur de données: cf. Interpréteur de données

Mode d'Edition: Allows you to select the edit mode globally. (The details panel's context menu allows to select the edit mode specifically for an active edit window.)

Jeu de Caracères: Vous laisse décider si le jeu de caractères ASCII ANSI, ASCII IBM, EBCDIC ou Unicode sera utilisé pour l'affichage (Unicode: keyboard input not supported). You may also use MAJ+F7. ANSI ASCII is the default character set. EBCDIC (originating from IBM mainframes) n'est pas supporté par la fonction impression. Unicode characters (little-endian) are always expected at even offsets.

6.10 Menu Fenêtre

Gestion de Fenêtres: Affiche toutes les fenêtres et fournit une fonctionnalité "Commutation instantanée de fenêtre". Vous pouvez aussi fermer des fenêtres et enregistrer des fichiers.

Sauvegarder Groupement Comme Projet: Sauvegarde la configuration de fenêtres courante comme fichier projet. A partir du Démarrage Rapide Centralisé vous pourrez alors recharger le projet et restaurer les positions d'édition de chaque document à tout moment, afin de continuer votre travail confortablement là où vous l'aviez laissé ou de commencer le travail dans le cas d'une tâche récurrente.

Fermer Tout: Ferme toutes les fenêtres ainsi que tous les fichiers et disques ouverts.

Ferme Tout sans Confirmation: Ferme toutes les fenêtres ainsi que tous les fichiers et disques ouverts sans vous donner l'opportunité d'enregistrer vos modifications.

Cascade/Mosaïque: Ces commandes rangent les fenêtres comme spécifié.

Minimiser: Minimise toutes les fenêtres.

Réorganiser les Icônes: Cette commande range les fenêtres minimisées.

6.11 Menu Aide

Sommaire: Affiche le contenu du fichier d'aide.

Configuration: Commute entre les interfaces utilisateur en Anglais, en Français, en Allemand, ...

Initialiser: Utilisez cette commande pour restaurer les caractéristiques par défaut de ce programme.

Désinstaller: Utilisez cette commande pour enlever WinHex de votre système. Celle-ci fonctionne correctement même si vous n'avez pas installé WinHex avec son programme d'installation.

En Ligne: Ouvre la page d'accueil web de WinHex dans votre navigateur, le forum d'aide, la base de connaissance, ou l'abonnement aux lettres de diffusion.

A Propos de WinHex: Affiche les informations relatives à WinHex : numéro de version, statut de license, etc..

6.12 Menu contextuel

Le système de commande de Windows affiche un menu contextuel quand l'utilisateur clique sur un objet avec le bouton droit de la souris. WinHex est présent dans le menu contextuel seulement si vous validez l'option correspondante (ci-dessous "Options Générales").

Editer avec WinHex: Ouvre le fichier sélectionné dans WinHex.

Ouvrir le dossier dans WinHex: Ouvre tous les fichiers du dossier sélectionné dans WinHex (consultez la commande "Ouvrir dossier" de menu Fichier).

Editer le disque avec WinHex: Ouvre le disque sélectionné dans l'éditeur de disque de WinHex. Si vous maintenez la touche MAJ appuyée, au lieu du lecteur logique sélectionné, c'est le disque physique correspondant qui est ouvert, s'il y en a un.

WinHex fournit ses propres menus contextuels sur la barre d'état, sur l'interpréteur de données et dans le gestionnaire de signets.

6.13 Directory Browser Context Menu

The directory browser context menu allows the user to directly interact with the currently *selected* files/directories, notably *not* the *tagged* items. There are a number of menu commands which are available depending on the selected items. Double clicking files and directories will, depending on the circumstances, either call "View", "Explore" or the associated external program.

View

This command allows viewing the selected file with WinHex' internal viewers for Windows Registry files and various graphical file formats. For other files, the mode of operation depends on the installed components: If X-Ways Trace is installed, and the file is either an “info2” file used by the Windows Recycle Bin or Internet Explorer's “index.dat” or Mozilla's/Firefox's “history.dat” or Opera's “dcache4.url”, X-Ways Trace is invoked for these files. If the X-Ways Forensics external viewer component is active, all other files are sent to that viewer. If it is not, the first installed external program will be called instead.

Exceptions to all of the above are files beyond 2 GB in size and NTFS system files. These are always opened as data windows.

Explore

Only available for directories and archives (ZIP, RAR, TAR...), this command allows navigating into them within the directory browser. Double-clicking archives or directories does the same. A command that allows listing the contents of directories as well as their subdirectories at the same time can be found in the directory tree's context menu instead (in the Case Data window,

"Explore recursively").

External Programs

Allows sending the selected file(s) to one of the external programs currently configured or the file's associated program in the current Windows installation. This association is determined based on file extension as is usual within Windows.

Recover/Copy

Allows copying the selected files from their current location to a location available for a standard Windows file dialog, e.g. out of an interpreted image file or from a local disk. This can be applied to both existing and deleted files and directories. When working with an active case and if logging is enabled, the copy/recovery process is documented in the case log. Both the source and the target paths are recorded. Optionally, files can be recreated in the output folder including their original path.

Edit Comment

Use this command to add a comment to an item in the directory browser or to edit or remove an existing comment. After entering comments, you can conveniently set the filter such that only commented items are shown or only items with specific comments, e.g. those with a certain relevance. Requires a forensic license.

Add to Noteworthy Table/Tag/Untag Item

In the directory browser of an evidence object, you include files in a report table of noteworthy items. These files will then also be listed in the case report. Having them in a dedicated contents table allows to conveniently copy/recover them in a single step at a later point of time or get a gallery overview of these files specifically. In order to remove files from the dedicated contents table of noteworthy files, use the "Delete from list" command in the directory browser context menu when that contents table is loaded or press the Del key on your keyboard. The click the floppy disk icon to save.

Tagging files means highlighting them visually. The visual highlighting can be undone with the context menu command "Untag item". Refining the volume snapshot can be limited to tagged files.

Add to Active Case

Performs the same operation as Recover/Copy but at the same time, the resulting file(s) will be added to the current case as evidence objects.

Export List

Outputs the current contents of the directory browser to a tab-delimited text file, which can be

easily imported and further processed e.g. in MS Excel. The output format is the same as for a so-called report table. However, this command is also available when not working with a case. Requires a specialist license.

Hide

You may hide selected items or hide all but the tagged items. If actually filtered out, hidden files are excluded from the directory browser, the gallery view, logical searches, copying actions, additions to an evidence file container, etc. If you are only allowed to examine the contents of certain directories, you could initially hide all files in all other directories to ensure that. Refining the volume snapshot can be limited to files that are not hidden. Hidden items are actually filtered out only if the corresponding filter is enabled in the directory browser options.

Position

The Position group of commands allows interactions with the currently selected file on a generally more technical level. It allows accessing the file's (or directory's) first cluster on the disk in the sectors view, accessing its related information like MFT record in NTFS or Inode in Ext2/Ext3 and also sorting the files by their physical order on disk: "Sort by directory entry location" (FAT), "Sort by Inode Offset" (Ext2/Ext3) or "Sort by MFT ID" (NTFS), respectively, allow to see files and folders in the order in which they physically appear in file system data structures (directory entries, the MFT, or Inode tables).

The Position menu also allows calling for a file's or directory's cluster list, i.e. the cluster list window will be opened and filled with the selected item's cluster list, and it allows deleting the selection from contents tables. The deletion of items from a contents table can be made permanent by clicking the floppy disk icon that will appear in the directory browser's caption line. You may also mark items as to be hidden in the volume snapshot (see directory browser Filter options). The menu also allows to add or move files to special report contents tables.

When you are examining files based on their contents only, where filenames, timestamps, deletion status and other meta-data are of no relevance, then you can use the "Remove duplicates" command to remove duplicated files from a contents table or to hide duplicated files from the currently listed part of a volume snapshot, based on hash values (if hash values were calculated). This command will first sort by hash values.

Logical Search

See chapter of that name.

Create Hash Set

Creates a hash set of the currently selected files and directories and their subdirectories directly within the internal hash database.

Create Directory Contents Table

Creates a contents table just like a drive contents table except that it exclusively focuses on files located within the directory currently selected and its subdirectories.

Print

If the separate viewer component is active, you may select files for printing. You will be prompted for each file.

Open

Opens currently selected files or directories in separate data windows. Unlike File | Open, this is a forensically sound operation in that it does not update any timestamps etc. In the case of a directory, the directory's data structures will be opened.

7 Options

7.1 Options générales

1ère colonne:

- Au démarrage, WinHex peut en option **afficher** le **démarrage rapide centralisé** ou **restaurer** le **dernier groupement de fenêtres** (toutes les fenêtres avec leur taille et position comme vous les avez laissées dans votre session WinHex précédente).

- Spécifiez le nombre de **documents récemment ouverts** à rappeler et **afficher** dans le Démarrage Rapide Centralisé (255 max.). 9 au plus sont aussi listés à la fin du menu Fichier.

- Vous pouvez faire apparaître WinHex dans le **menu contextuel** de Windows. Le système affiche le menu contextuel quand l'utilisateur clique sur un objet avec le bouton droit de la souris. WinHex fournit des éléments de menu pour les fichiers, dossiers et disques. Si cette option n'est pas complètement sélectionnée, il n'y pas d'éléments de menu pour les fichiers.

- Les options **Permettre plusieurs instances** vous permettent d'exécuter WinHex plus d'une fois en même temps. Si cette option n'est pas activée, WinHex met la fenêtre principale de l'instance courante en second plan au lieu de créer une instance de nouveau programme. De cette façon vous pouvez être assuré qu'il n'est pas nécessaire d'avoir de multiples licences du programme quand vous exécutez de multiples instances sur un simple ordinateur....

- **Ne pas changer la date des fichiers** signifie que WinHex n'actualisera pas le marqueur date-heure quand un fichier a été modifié, et est enregistré avec le menu Fichier.

- Si **Rechercher secteurs en surplus** est désactivé, WinHex ne tentera pas d'accéder aux secteurs en surplus à l'ouverture d'un disque dur physique. Lorsque ces secteurs sont trouvés, WinHex les mémorise pour la prochaine ouverture du disque. Vous pouvez obliger une nouvelle vérification an appuyant sur la touche MAJ à l'ouverture du disque. Vérifier l'occurrence de secteurs en surplus, peut (très rarement) générer un délai de réponse assez long, voire un comportement inhabituel, ou même causer des dommages sur certaines machines. Only under Windows XP surplus sectors are included automatically, which makes this option obsolete.

- Since v12.7 SR-8, WinHex by default **sorts** and enumerates disk **partitions** by their physical **location**.

- If **Auto-detect deleted partitions is enabled**, WinHex tries to identify obvious deleted partitions automatically in gaps between existing partitions and in unpartitioned space directly following the last partition, when opening physical hard disks. Such additionally detected partitions will be listed in the Access button menu and marked as deleted. Please note that deleted partitions detected in gaps between existing partitions cause the partition numbering to be changed. E.g. an existing partition #3 might become partition #4 if a deleted partition is detected on the disk before it.

- The **alternative access method 1** for physical hard disks under Windows 2000/XP may allow to access hard disks formatted with an unconventional sector size or other media that cannot be accessed otherwise. Note that it may be slower than the regular access method. If considerably slower, WinHex will notify you of this and recommend to revert to the standard access method. **Access method 2** affects physical hard disks only as well, under Windows 2000/XP. Both alternative methods allow you to specify a timeout in milliseconds after which read attempts will be aborted. This can be useful on disks with bad sectors, where an attempted read access to a single sector could otherwise cause a delay of many seconds or minutes.

- Par défaut, les **fenêtres d'édition** ne sont pas **ouvertes** à l'état **maximisé**.

- Par un clic droit **WinHex** peut ouvrir un **menu contextuel** spécial, le menu d'édition standard, ou définir la fin du bloc courant. If this option is disabled, you can still bring up the context menu if you hold the Shift key while right-clicking.

- Si vous sélectionnez **Montrer les icônes des fichiers**, les icônes stockés dans les fichiers sont affichés dans la section de détails. Si un fichier ne contient pas d'icône, l'icône *type* du fichier est affiché, sauf si cette option n'est pas "pleinement" sélectionnée.

- La touche **ENTREE** peut être utilisée pour saisir jusqu'à quatre valeurs hexadécimales à deux chiffres. Il est utile de spécifier **0x0D0A**, qui est interprété comme un marqueur-de-fin-de-ligne dans le monde Windows (Unix . 0x0D). The Start Center could then still be opened using **SHIFT**+**ENTER**.

- Choisissez si vous voulez utiliser la touche **TABULATION** pour commuter de mode texte en mode hexadécimal et vice versa ou pour entrer le caractère tabulation (0x09). Dans tous les cas on peut appuyer sur TAB+MAJ pour commuter le mode courant.

2ème colonne:

- Spécifie le **dossier** dans lequel sont créés les **fichiers temporaires**.

- Spécifie le **dossier** dans lequel sont créés les fichiers de **sauvegardes** (.whx).

- Spécifie le **dossier** dans lequel sont créés les fichiers de **projets, scripts et cas**.

- Specify the **folder** in which to maintain the **internal hash database**.

- **Reduced user interface**: Available when operated with a forensic license. Slightly reduces and simplifies the menu structure. The checkbox has a third state ("forensic lite interface"), which is meant for investigators in law enforcement
  - who are specialized in areas such as white-collar crime, tax fraud, etc.
  - who do not need profound knowledge of computer forensics
  - who do not need technical insights that WinHex and XWF are well-known to offer
  - who receive e.g. convenient-to-handle X-Ways evidence file containers from well-versed computer forensics examiners with only selected files from various sources (e.g. "all documents that contain the keywords x and y"), with obviously irrelevant stuff already filtered out
  - who need to review hundreds of electronic documents, identify relevant ones, add comments to them, identify logical structures and connections between them with the help of their comments, and print documents, all within the same environment with a few mouse clicks, which saves the time to extract and load each document in its associated application
  - who may or may not need to work in an environment severely restricted by the system administrator anyway

  The "forensic lite" interface lacks many advanced technical options, to allow for easier access to non-technical personnel. Forensic licenses that only allow to use the "forensic lite" interface are available at 50% the regular rate on request.

- You may specify your **preferred thumbnail size** in pixels. WinHex will decrease the size automatically if needed to ensure that at least as many files are displayed in the gallery view as are displayed in the currently visible section of the directory browser.

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

- When gallery view is enabled, WinHex can optionally continue **loading thumbnails in the background** when the current view is full, if the number of files in the current directory is not too big.

3ème colonne:

- Non-printable **characters** with a character set value smaller than **0x20** can be represented by a user-defined other character.

- Les **offsets** peuvent être présentés et modifiés en notation décimale ou **hexadécimale**. Ce réglage est valide pour la totalité du programme.

- Lors de l'utilisation de l'Editeur de RAM il peut être raisonnable de faire afficher par WinHex des **adresses virtuelles** plutôt que des offsets par rapport à zéro. Ceci est toujours fait en notation hexadécimale. La boite de dialogue de la commande Aller à la Position vous demandera aussi des adresses virtuelles.

- Les **séparateurs de page** et de secteur peuvent être **affichés**. Si cette option est validée partiellement seuls les séparateurs de secteurs sont affichés.

- Choisissez le numéro d'**octets par ligne** (typiquement 16 ou 32).

- Décidez comment **grouper** les **octets**. Des puissances de deux sont recommandées pour former un groupe.

- Spécifiez combien de **lignes doivent être déroulées** avec le **bouton déroulant** de la souris (si disponible).

- **NTFS: MFT auto coloring:** Highlights the various elements in FILE records of the NTFS file system, when the blinking cursor is located within such a record, to facilitate navigation and understanding. Requires a specialist or forensic license.

- Sélectionnez une **couleur** utilisée comme arrière-plan du **bloc** courant. Vous pouvez seulement changer la couleur si l'option "Utiliser les couleurs Windows par défaut" est désactivée.

- Sélectionnez une **couleur** utilisée pour le **fond** d'un **enregistrement** de longueur fixe sur deux, si la présentation d'enregistrement est activée (voir menu Position).

- Select the default **color** for newly created **annotations**/positions/bookmarks.

- WinHex peut en option **mettre en valeur les octets modifiés**, c'est-à-dire afficher les parties modifiées d'un fichier, d'un disque ou de la mémoire dans une couleur différente de votre choix.

- Vous pouvez choisir une **police** de caractères pour le mode ASCII ANSI. La police WinHex comprend le jeu complet des caractères Windows (même les caractères tels que les symboles ™, € et les différents guillemets).

- Afficher la **barre de progression Windows** remplace la barre de progression WinHex par la barre typique de progression commune à la plupart des programmes Windows.

- Enfin, vous pouvez sélectionner l'un des différents **styles** de **fenêtre de dialogue** et de **bouton**.

Le positionnement d'origine de toutes ces options peut être restauré en utilisant la commande Initialiser du menu aide.

7.2 Directory Browser Options

- **Grouping files and directories** in the directory browser is optional.

- **Grouping existing and deleted items** in the directory browser is optional. There are two possibilities how to enable this feature, either potentially recoverable deleted files (marked with a question mark) and known unrecoverable files (marked with an X) are internally grouped as well or not.

- **Group tagged and untagged items** to see all tagged items listed first, which can be convenient to review those items as a whole, followed by all untagged items. Both groups are internally sorted depending on the current sort criteria. Cannot be combined with the aforementioned grouping option for reasons of clarity.

- Optionally, X-Ways Forensics can **append** the presumed **correct ext**ension when copying files (to a hard disk or to a container) after the signature check, also when copying files to execute them with the associated program.

- Files can optionally be **opened**, **searched**, and **copied**/recovered including their **slack**.

- By default, **Ctrl+A** (select all) in the directory browser **includes** non-existent **files** whose first cluster has been reallocated. However, that behavior can be disabled so that e.g. less clusters are covered twice when you search logically in selected files.

- **Recursive selection statistics** reveal how many subdirectories, files and how much data are in a directory when you select it in the directory browser.

- Listing sub**dir**ectorie**s** when **exploring recursively** is optional.

- The **directory browser** can optionally be displayed with a **grid**.

- There is an option to display timestamps with **tenths of seconds**. Useful for the file systems NTFS and FAT that provide for this precision in all or some timestamps. Note that fractions of seconds are not retained when you export file lists or report tables.

- Optionally, the actually used **time zone conversion bias**, including daylight saving where

appropriate, can be displayed right in the timestamp columns in the directory browser.

- **List**ing the **ISO9660** file system's directory tree on CDs *in addition* to a possibly also existing **Joliet** file system can be useful if the Joliet file system is damaged e.g. if scratches on the surface of the CD led to unreadable (bad) sectors. Takes effect when taking a new volume snapshot.

Various columns in the directory browser are optional. They are displayed if they have a non-zero column width or hidden if their width is zero.

Filters

The following can be dynamically filtered out:

- Deleted files and directories. Useful if you are merely interested in data in existing files.
- Existing files. Useful if you are merely interested in recovering lost files.
- Files and directories that have been marked as to be hidden in the volume snapshot. (All such marks can be removed.)
- $EFS attributes, non-directory INDX streams and BMP attributes on NTFS volumes.

You may also define filters based on criteria such as filenames, file type categories, and matching hash set categories. Whenever an active filter actually filters out files or directories in the directory browser, this is flagged with a filter icon in the directory browser's header line. Please note that report tables are not automatically reloaded to reflect new filter settings.

7.3 Options d'annulation

La disponibilité de la commande "Annuler" dépend des options suivantes.

- Spécifiez combien d'actions séquentielles doivent pouvoir être réversibles par la commande Annuler. Cette option n'affecte pas le nombre de saisies clavier réversibles, qui est seulement limité par la taille de la RAM.

- De manière à gagner du temps et de la place sur votre disque dur, vous pouvez spécifier une limite de taille de fichier. Si un fichier est plus grand que cette limite, des sauvegardes ne seront pas créées et la commande Annuler ne sera valable que pour une entrée clavier.

- Si l'option correspondante est pleinement activée, les sauvegardes créées automatiquement pour l'usage interne avec la commande Annuler sont effacées par WinHex lors de la fermeture du fichier. Si l'option est partiellement activée, les sauvegardes sont effacées lors de l'arrêt de WinHex.

- Choisissez quelles sortes d'actions d'édition devront être réversibles ou pas. Au cas où elles doivent l'être, une sauvegarde interne est créée avant que l'action ne s'effectue.

7.4 Options de sécurité

L'option **Lecture de secteurs accélérée** se réfère à l'éditeur de disque. Elle réduit considérablement le nombre d'accès physiques nécessaires. Particulièrement recommandée pour scroller les secteurs CD-ROM ou disquette.

With the option **Keep volume snapshots between sessions** enabled, all information on file systems in opened volumes collected by WinHex (Disk Tools menu and/or Specialist menu) remains in the folder for temporary files even when WinHex terminates. WinHex can then reuse drive maps during later sessions. Volume snapshots of evidence objects are always kept, regardless of this setting.

Quick snapshots without cluster allocation speeds up taking a volume snapshot (in particular for the file systems Ext2, Ext3 and ReiserFS, and in particular also when the volume snapshot files are created across a slow USB 1.1 interface or network), however, causes WinHex to lose its ability to tell each sector’s and cluster’s allocation (for which file it is used). This will also disable the functionality of the Sync button and the preview mode when reviewing search hits. You may use the command “Take New Volume Snapshot” of the Tools menu to update the view of a volume, e.g. after unchecking this option.

Utilisez l'option **Intégrité de la mémoire virtuelle** pour être sûr que l'éditeur de RAM inspecte la structure de la mémoire virtuelle avant de la *lire* ou *écrire*. Si la structure a changé, une erreur possible de lecture est prévenue. Spécialement sous Windows NT la vérification peut entraîner une perte de vitesse. Lors de l'édition de la "mémoire entière" d'un processus, WinHex en règle générale ne vérifie jamais les altérations avant lecture, même si cette option est validée.

Avant que les modifications apportées à un fichier existant ne soient enregistrées (c'est à dire avant que le fichier ne soit actualisé), vous êtes avisé pour **confirmation**. Pour inhiber ce mode de fonctionnement de WinHex, commutez l'option correspondante.

Optionally, files can be **indirectly** added to evidence file **containers**, via your own hard disk. That means they are not copied directly into the container, but to your folder for temporary files first (cf. General Options), and only then from there into the container. This can be beneficial because it allows a resident antivirus software to intercept these files (check them for viruses, disinfect/disarm them, rename them, move/delete/lock them, etc.), so that it prevents viruses from making it into a container. The resulting container is free of known viruses (depending on the antivirus software in use) and can reasonably be passed on to and used in an environment with higher sensitivity, higher security requirements, and/or less sophisticated virus protection.

Creating containers based on **Unicode** filenames is optional to allow for compatibility with earlier version of X-Ways Forensics (pre-12.85) that did not support Unicode. For full

functionality, have X-Ways Forensics create containers with the new format.

La **clé** qui est requise pour le **cryptage** et le décryptage peut être saisie dans une boîte normale d'édition. Facultativement vous l'entrez d'une manière aveugle (des astérisques étant affichés à la place des caractères). Dans ce cas vous devez confirmer la clé dans une seconde boite d'édition pour détecter d'éventuelles erreurs de frappe.

Par défaut, la **clé** est **gardée en RAM** (en état chiffré) aussi longtemps que WinHex fonctionne, ainsi vous n'avez pas à la retaper à chaque fois que vous l'utilisez. Il est possible aussi que vous préfériez que WinHex efface la clé après chaque usage.

Choisissez si vous souhaitez que WinHex vous **prévienne avant l'exécution d'un script**, ou seulement avant son exécution via la ligne de commande.

Optionally, **files** on the logical drive letters A: through Z: can be **opened** with the help of the **operating system** instead of with the built-in logic at the sector level. Please note that this is forensically sound only for write-protected media. On writeable media, Microsoft Windows will at least update (i.e. alter, falsify) the last access timestamp of files you open. The benefit, however, is that access to such files will be noticeably faster in many situations, especially on slow media such as CDs and DVDs, e.g. when you compute hashes or skin color percentages for files in a volume snapshot, because Microsoft Windows employs read-ahead mechanisms and entertains a file caching system.

7.5 Options de recherche

Respecter la casse: Si cette option est validée, WinHex fait une distinction entre les majuscules et minuscules, dans ce cas "Option" n'est pas trouvé dans le mot "optionnel".

Jeu de caractères Unicode: Le texte spécifié est recherché en utilisant les 256 caractères Unicode équivalents ASCII ANSI, même ceux où l'octet d'ordre haut est 0. The simultaneous search allows to search for the same text at the same time in Unicode and ASCII. For this to work, the checkbox needs to be “half” checked.

Vous pouvez spécifier un **joker** (un caractère ou une valeur hexadécimale à deux chiffres), qui représente un octet. Par exemple cette option peut être utilisée pour trouver "Speck" aussi bien que "Spock" lors de la recherche de "Sp?ck" avec le point d'interrogation comme joker.

Mots entiers seulement: La chaîne recherchée est reconnue seulement si elle est séparée d'autres mots, c'est à dire par des caractères de ponctuations ou d'espaces. Si cette option est validée, "tomato" n'est pas trouvé dans "automaton".

Direction de la recherche: WinHex peut rechercher du début à la fin, ou chercher vers le bas ou vers le haut, depuis la position courante du curseur.

Condition: Offset modulo x = y: L'algorithme de recherche ignore les occurrences qui ne correspondent pas aux exigences. Par exemple, si vous cherchez des données qui typiquement apparaissent à un offset relatif au début d'un secteur du disque dur, spécifiez x=512. Si vous cherchez des données alignées DWORD, utilisez x=4, y=0.

Rechercher seulement dans le bloc: L'opération de recherche est limitée au bloc courant.

Examiner tous les fenêtres ouverts: L'opération de recherche est appliquée à tous les fenêtres ouvertes. Appuyez sur F4 pour continuer la recherche dans la fenêtre suivante. Si "rechercher dans le bloc seulement" est validé, la recherche est limitée au bloc courant dans chaque fenêtre.

Compter les occurrences/enregistrer les positions d'occurrence: Force WinHex non pas à afficher chaque simple occurrence, mais à les compter. Si cette option est pleinement validée, WinHex entrera toutes les occurrences dans le gestionnaire de signets.

Search for “non-matches”: In "Find Hex Values" you may specify a single hex value with an exclamation mark as a prefix (e.g. !00) to make WinHex stop when it encounters the first byte value that *differs*.

GREP syntax: Available with the Simultaneous Search and Logical Search only. Regular expressions are a powerful search tool. A single regular expression may match many different words. The following characters have a special meaning in regular expressions, as explained below: ( ) [ ] { } | \ . # + ?. Where these special characters are to be taken literally, you need to prefix them with a backslash character (\).

The | operator is used to denote alternative matches. You can use the regular expression *car (wheel|tire)* to search for the words "car wheel" and "car tire". Any match must equal the parts before, after, or between any | operators present. The effect of | is only limited by parentheses.

. and # are wildcards: . matches any character, # matches any numeric character. You can define sets of characters with the help of square brackets: [xyz] will match any of the characters x, y, z. [^xyz] will match any character except x, y, or z. You can define ranges of characters using a hyphen: [a-z] matches any lower-case letter. [^a-z] matches all characters except lower-case letters. The listing may comprise individually listed characters and ranges at the same time: [aceg-loq] matches a, c, e, g, h, i, j, k, l, o, and q. All characters except [,], -, and \ are taken literally between square brackets, even the wildcard characters . and #.

Byte values that correspond to ASCII characters that cannot be easily produced with a keyboard can be specified in decimal or hexadecimal notation: For example, \032 and \x20 are both equivalent to the space character in the ASCII character set. This kind of notation is supported even in between square brackets. E.g. [\000-\x1f] matches non-printable ASCII characters.

Multiplier characters (*, +, and ?) indicate that the preceding character(s) may or must occur more than once (see below). Complex example: a(b|cd|e[f-h]i)*j matches aj, abj, acdj, aefij, aegij, aehij, abcdj, and abefij.

. A period matches any single character.
A pound sign matches any numeric character [0-9].
\nnn A byte value specified with three decimal digits (0...255)
\xnn A byte value specified with two hexadecimal digits (0…FF).
E.g. \x0D\x0A is the Windows line break.
? Matches one or zero occurrences of the preceding character or set.
* Matches any number of occurrences of the preceding character, including zero time.
+ A plus sign after a character matches any number of occurrences of it except zero.
[XYZ] Characters in brackets match any one character that appears in the brackets.
[^XYZ] A circumflex at the start of the string in brackets means NOT.
[A-Z] A dash within the brackets signifies a range of characters.
\ Indicates that the following special GREP character is to be treated literally.
{X,Y} Repeats the preceding character or group of characters X-Y times.
(ab) Functions like a parenthesis in a mathematical expression. Groups ab together for + and *.
a | b The pipe acts as a logical OR. So it would read "a or b".

7.6 Options remplacement

Confirmer chaque remplacement: WinHex attend votre décision quand il trouve une occurrence. Vous devez soit la remplacer, continuer ou abandonner la recherche.

Tout remplacer: Toutes les occurrences son automatiquement remplacées.

Respecter la casse: Les caractères qui doivent être remplacés sont recherchés en utilisant cette option. (cf. Options de Recherche)

Jeu de caractères Unicode: Les caractères spécifiés sont recherchés dans le format Unicode (cf. Options de Recherche).

Vous pouvez spécifier un caractère ou une valeur hexadécimale à deux chiffres comme **joker**. Ceci est généralement fait en recherche de chaîne. Si le substitut contient un joker, le caractère à la position correspondante en occurrence ne sera pas changé. Ainsi, "black" et "block" peuvent être remplacés simultanément par "crack" et "crock" (en entrant "bl?ck" et "cl?ck").

Mots entiers seulement: La chaîne recherchée est reconnue seulement si elle est séparée des autres mots c'est à dire par des caractères de ponctuation ou des espaces. Si cette option est validée, "tomato" n'est pas remplacé dans "automaton".

Direction du remplacement: WinHex peut rechercher du début à la fin, ou chercher vers le bas ou vers le haut, depuis la position courante du curseur.

Seulement dans le bloc: L'opération de remplacement est limitée au bloc courant.

Dans tous les fichiers ouverts: L'opération de remplacement est appliquée à tous les fichiers non ouverts en mode vue seule. Si "Remplacer dans le bloc seulement" est validé, l'opération de remplacement est limitée au bloc courant de chaque fichier.

Conseils:

WinHex est capable de remplacer une chaîne de même qu'une séquence de valeurs hexadécimales par une autre qui a une longueur différente. Vous serez averti d'une des méthodes suivantes qui sera appliquée.

1ère méthode: La donnée derrière l'occurrence est déplacée à cause de la différence de longueur. Cette méthode ne doit pas être appliquée à certains types de fichiers, tels que les fichiers exécutables. Il est même possible de ne rien spécifier comme substitut, de telle manière que toutes les occurrences seront déplacées dans le fichier!

2ème méthode: Le substitut est écrit dans le fichier à la position de l'occurrence. Si le substitut est plus court que la séquence de caractères recherchés, les caractères excédentaires resteront dans le fichier. Autrement même les octets derrière l'occurrence seront écrasés (tant que la fin du fichier n'est pas atteinte). La taille du fichier n'est pas affectée.

8 Divers

8.1 Bloc

Vous pouvez marquer une partie d'un fichier ouvert comme un "bloc". Cette partie peut être manipulée par plusieurs fonctions dans le menu Edition exactement comme des sélections dans d'autres programmes Windows. Si aucun bloc n'est défini, ces fonctions sont normalement appliquées au fichier entier.

La position courante et la taille sont affichées dans la barre d'état. Un double clic sur le bouton droit de la souris ou un appui sur la touche **ESC** efface le bloc.

8.2 Modifier des données

Utilisez cette commande pour modifier les données à l'intérieur d'un bloc ou dans le fichier entier, au cas où aucun bloc ne serait défini. Dans cette version de WinHex, quatre types de modifications de données sont disponibles. Un nombre fixe est ajouté ou traité en mode booléen en XOR, OR ou AND, ou bien les bits sont inversés ou décalés logiquement, ou bien les octets sont permutés. On peut employer l'opération XOR comme une manière d'encryptage simple. En décalant (shifting) les bits, on peut simuler l'insertion ou la suppression des bits au début du bloc.

You may also shift entire *bytes* (currently to the left only, by entering a negative number of bytes). This is useful if you wish to cut bytes from a very huge file in in-place mode, which would otherwise require the creation of a huge temporary file.

Inversion d'octets

Cette commande affecte toutes les données qui consistent en éléments de 16 bits (de même que de 32 bits) et échange les octets de haut et de bas rangs (de même que des mots de hauts et de bas rangs). Utilisez cette commande pour convertir des données de "poids fort en tête" en "poids faible en tête" et vice versa.

Additionner

Spécifiez un nombre décimal ou hexadécimal, positif ou négatif, qui sera ajouté à chaque élément du bloc courant. Un format entier définit la taille (1,2 ou 4 octets) et le type (signé ou non signé) d'un élément.
Il y a deux manières de procéder si le résultat est hors de la gamme du format entier sélectionné. Soit la gamme est limitée en se conformant à la nouvelle valeur (I) ou soit que la retenue est ignorée (II).

Exemple: format non signé 8 bits
I. FF + 1 → FF (255 + 1 → 255)
II. FF + 1 → 00 (255 + 1 → 0)

Exemple: format signé 8 bits
I. 80 - 1 → 80 (-128 - 1 → -128)
II. 80 - 1 → 7F (-128 - 1 → +127)

- Si vous décidez d'utiliser la première méthode, WinHex vous dira combien de fois la l'étendue limite a été dépassée.

- La seconde méthode assure une opération réversible. Il faut simplement ajouter *-x* au lieu de *x* basé sur le même format entier pour recréer la donnée originale.

- Lors de l'utilisation de la seconde méthode il n'est pas fait de différence que vous choisissiez un format signé ou non signé.

8.3 Conversions

WinHex fournit la commande Convertir du menu Edition pour des conversions aisées des différents formats de données et le cryptage et le décryptage. La conversion peur être appliquée facultativement à tous les fichiers ouverts au lieu de celui couramment affiché. Les formats marqués avec un astérisque (*) peuvent seulement être convertis comme fichier entier, et non comme bloc. Les formats suivants sont supportés:

- ASCII ANSI, ASCII IBM (deux jeux de caractères ASCII différents)
- EBCDIC (un jeu de caractères de IBM mainframe)
- Caractères majuscules/minuscules (ASCII ANSI)
- Binaire* (données brutes)
- Hexadécimal ASCII* (représentation hexadécimale de données brutes sous forme de texte ASCII)
- Intel Hex* (= Intellec étendu; données ASCII hexadécimales dans un format spécial, comprenant des sommes de contrôle etc..)
- Motorola S* (=Exorcisor étendu; données comme ci-dessus)
- Base64*
- UUCode*

Notez:
- Lors de conversions de données Intel Hex ou Motorola S, les sommes de contrôle internes de ces formats ne sont pas vérifiées.
- Selon la taille du fichier, le format de sortie le plus petit possible est choisi automatiquement. Intel Hex: 20-bit ou 32-bit. Motorola S: S1, S2, ou S3.
- When converting from binary to Intel Hex or Motorola S, only memory regions not filled with hexadecimal FFs are translated, to keep the resulting file compact.

The Convert command can also decompress raw data from any number of complete 16-cluster units compressed by the NTFS file system* and can stretch packed 7-bit ASCII to readable 8-bit ASCII*.

Cryptage/Décryptage

La clé utilisée pour l'encryptage et le decryptage doit contenir entre 1 et 16 caractères. Plus il y a de caractères, plus l'encryption est sécure. Pour une sécurité maximale la clé est hachée pour produire la clé finale. La clé n'est pas enregistrée sur le disque dur. Elle est gardée en RAM en état chiffré (voir Options de Sécurité).

Il est recommandé de spécifier une combinaison d'au-moins 8 caractères comme clé de cryptage. The key is case-sensitive. N'utilisez pas de mots d'une quelconque langue, il est préférable de choisir une combinaison aléatoire de lettres, de signes de ponctuation et de chiffres. Notez que les clés de cryptage sont sensibles à la casse. Rappelez qu'il vous sera impossible de retrouver vos données cryptées sans la clé appropriée. La clé de décryptage que vous saisissez n'est pas vérifiée avant le décryptage.

Encryption algorithms available in WinHex:

• State-of-the-art 256-bit AES/Rijndael, in counter (CTR) mode. This encryption algorithm uses a 256-bit key that is digested with SHA-256 from the 512-bit concatenation of the SHA-256 of the key you specify and 256 bits of cryptographically sound random input (“salt”). The file is expanded by 48 bytes to accommodate the 256 bits of salt, and a randomized 128-bit initial counter.

WinHex allows you to encrypt not only an entire file, but also a block of data only. In that case you are warned, however, that no salt is used and no random initial counter is used, so you must not reuse your key to encrypt other data with the same encryption method. The size of the block is left unchanged.

• Pukall cipher 1 (PC 1), utilisant une clé de 128 bits (=le hash à 128 bits de la clé que vous spécifiez).

8.4 Effacer et initialiser

For securely erasing (shredding) data, and also simply for filling files or disk sectors with certain byte values, WinHex offers the following options:

Remplir avec des valeurs hexadécimales: Spécifiez 1, 2, 3, 4, 5, 6, 12, 15 ou 16 valeurs hexadécimales à deux caractères, qui seront respectivement copiées les unes à la suite des autres dans le bloc courant, le fichier entier ou dans tous les secteurs du disque.

Remplir avec des octets aléatoires: Spécifiez un intervalle décimal (0 à 255 max.) pour des nombres aléatoires, qui seront respectivement copiés les uns à la suite des autres dans le block courant, le fichier entier ou dans tous les secteurs du disque.

Au cas où dans tous les fichiers ouverts soit un bloc soit aucun bloc n'est défini, cette commande peut facultativement être appliquée à tous ces fichiers en même temps.

To maximize security, if you wish to totally wipe (sanitize) slack space, free space, unused NTFS records, or an entire media, you may want to apply more than one pass for overwriting disk space (up to three).

According to the Clearing and Sanitization Matrix, the standard outlined in the U.S. Department of Defense (DoD) 5220.22-M operating manual, method "c", a hard disk or floppy disk can be cleared by overwriting (once) all addressable locations with a single character. This is usually the hexadecimal value 0x00, but can be any other value. To sanitize hard disks according to method "d", overwrite all addressable locations with a character, its complement, then a random character, and verify. (This method is not approved by the DoD for sanitizing media that contain top secret information.)

The "DoD" button configures WinHex for sanitization, such that it will first overwrite with 0x55 (binary 01010101), then with its complement (0xAA = 10101010), and finally with random byte values.

The "0x00" button configures WinHex for simple initialization, wiping once with zero bytes.

8.5 Clonage de disque

La commande "Cloner Disque" fait partie du menu Outils. Cette fonction copie un nombre déterminé de secteurs d'un disque-source vers un disque-cible (or alternatively from a disk image file or to a disk image file). Les deux disques doivent avoir la même taille de secteur. Pour effectuer une véritable *duplication* d'un lecteur (c'est-à-dire pour copier tous les secteurs), activez l'option correspondante, pour que le nombre correct de secteurs soit déterminé automatiquement. Le disque-cible ne doit pas être plus petit que le disque-source.

Cloner Disque offre des options qui contrôlent son comportement lorsque des secteurs défectueux sont trouvés sur le disque-source:

- par défaut, vous serez averti de l'erreur et pourrez choisir de poursuivre l'opération ou d'y mettre fin. "Rapport silencieux" crée un journal complet de toute l'opération dans le dossier pour les fichiers temporaires (fichier "Cloning Log.txt"), y compris un rapport sur les secteurs illisibles (ce qui ne peuvent pas être copiés), empêchant WinHex de faire un rapport séparé pour chaque secteur défectueux. Ceci peut s'avérer utile, par exemple pour les expertises légales.
- WinHex peut soit laisser intact le secteur-destination correspondant à un secteur source endommagé, soit le remplir with an ASCII pattern you specify (e.g. your initials, or something like «BAD »). Leave the pattern edit box blank to fill such sectors with *zero* bytes. BTW, the chosen pattern is also used to display a bad sector's contents in the disk editor.
- Bad sectors often occur in contiguous groups. You may have WinHex avoid such damaged disk areas. When a bad sector is encountered, WinHex can skip a number of subsequent sectors you specify (25 by default). This is useful when you do not care about some actually readable sectors not making it to the clone, but want to accelerate the cloning process, since each attempt to read a bad sector usually takes a long time.

Le clonage de disque standard n'est pas possible si vous voulez cloner un disque de lecteur amovible (par exemple une disquette) avec seulement un lecteur amovible présent. Le concept qui convient pour cet usage est celui d'*image* disque (on pourrait aussi l'appeler "clonage de disque différé"). L'image peut être recréée sur un autre disque, avec le même résultat que celui du clonage.

When you specify a file named “dev-null” as the destination, the data will only be read and not copied anywhere (and you will be warned of this). This is useful if you are interested in the report about bad sectors, but do not wish to actually clone or image a disk.

You may try “simultaneous I/O” if the destination is not the same physical medium as the source. Offers a chance to accelerate the cloning process by up to 30%.

Il existe deux façons de créer une image d'un disque:

- Le dialogue Clonage de disque permet de copier des secteurs depuis un disque sous forme brute, comme *fichier image sans en-tête*, et plus tard en sens inverse. Combinée au mode "rapport silencieux", cette méthode est préférable à la création d'une copie de sécurité en cas de secteurs endommagés sur le disque-source.

- For options like compression, hashing, and file splitting, please use the image and backup functionality. For easy recovery, a backup file includes information on its contents: sector numbers, source disk etc.

Cloner ou créer une image du lecteur qui contient l'installation active de Windows peut donner des résultats incohérents. Dans tous les cas assurez-vous qu'aucun autre programme, ni Windows, n'écrit sur le lecteur pendant la procédure de clonage/sauvegarde/restauration. Il est recommandé de déplacer le dossier TEMP vers un autre lecteur. Le fichier d'échange (swap) doit également être créé sur un autre lecteur.

Assurez-vous qu'aucun autre programme ou service ne peut écrire dans la partition que vous allez cloner. Par exemple vérifiez si des outils de défragmentation tournent en tâche de fond et désactivez-les pendant la durée du clonage/de la sauvegarde/de la restauration. Sous Windows NT/2000/XP il est recommandé de démonter la partition comme lecteur logique/lettre de lecteur.

Vous devrez redémarrer votre machine ou exécuter «chkdsk /f » sur les volumes restauré au format NTFS pour obtenir une mise à jour de la structure de répertoire (this definitely clears all of Windows' internal buffers). When cloning over a logical drive letter, WinHex itself will attempt to refresh Windows' view of it.

Cloning or imaging with WinHex makes exact sector-wise, forensically sound copies, including all unused space and slack space. WinHex cannot dynamically change partition sizes or adapt to destination disks larger or smaller than the source disks. This can be done by tools like PartitionMagic.

In order to reduce the space a backup occupies as much as possible, you can initialize unused drive space before making the backup. This is because sectors that consist but of zero values barely increase the backup size when compression is enabled.

8.6 Images et Sauvegardes

La commande Créer une Sauvegarde dans le menu Fichier allows to create a backup or image of the currently open logical drive, physical disk, or individual file. There are three possible output file formats, each with unique advantages.

File format:	**WinHex Backup**	**Evidence File**	**Raw Image**
Filename extension:	.whx	.e01	e.g. .dd
Interpretable as disk:	no	yes	yes
Splittable:	yes	yes	yes
Compressible:	yes	yes	no
Encryptable:	yes	yes	no
Optional hash:	integrated	integrated	separate
Optional description:	integrated	integrated	no
Range of sectors only:	yes	no	no
Applicable to files:	yes	no	no
Automated maintenance:	Backup Manager	no	no

Compatibility:	no	(yes)	yes
Required license:	none	forensic	personal

The major advantage of evidence files and raw images is that they can be interpreted by WinHex like the original disks (with the command in the Specialist menu). This also makes them suitable for usage as evidence objects in your cases. This holds true for evidence files in particular because they can store an optional description and an integrated hash for later automated verification. Raw images have the benefit that they can be easily exchanged between various forensic tools. All output file formats support splitting into segments of a user-defined size. A segment size of 650 MB e.g. is suitable for archiving on CD-R. Evidence files are *required* to be split at 2025 MB at max.

The encryption algorithm optionally used in evidence files is exceptionally strong: 256-bit AES/Rijndael, in counter (CTR) mode. This allows for random read access within evidence files. This encryption algorithm uses a 256-bit key that is digested with SHA-256 from the 512-bit concatenation of the SHA-256 of the key you specify and 256 bits of cryptographically sound random input (“salt”), which is stored in the header of the evidence file. The 128-bit counter is randomized and incremented per encryption block. The block size of AES is 128 bits. An additional SHA-256 is stored in the header as well and used later to determine whether a password, specified by the user for decryption, is correct or not. The SHA-256 algorithm is applied to a concatenation of the salt, hash x, and hash y to compute this password verification hash, where hash x is the SHA-256 of the user-supplied password and hash y is the SHA-256 of the concatenation of the user-supplied password and hash x.

L'algorithme de cryptage dans les fichiers WHX est le "Pukall Cipher 1" (PC 1), utilisant une clé à 128 bits qui est hachée à partir d'une concaténation à 256 bits d'un hash-code à 128 bits de la clé que vous avez entrée et d'une entrée aléatoire de 128 bits. L'entrée aléatoire est enregistrée dans le fichier WHX pour un futur décryptage.

Si vous devez assigner à WinHex un nom de fichier pour le fichier WHX automatique, le fichier sera créé dans le dossier pour les sauvegardes (cf. Options Générales), named with the next free “slot” according to the Backup Manager's naming conventions (“*xxx*.whx”) et sera disponible dans le gestionnaire de sauvegarde. Si vous spécifiez explicitement un chemin et un nom de fichier, vous pouvez restaurer la sauvegarde en utilisant la commande "Charger une Sauvegarde", and in case of split backups WinHex will automatically append the volume number to the filenames.

WinHex utilise l'algorithme de compression "Deflate" de la librairie commune zlib. Cette algorithme consiste en compression LZ77 et codage Huffman. Le degré de compression est le même que celui de ZIP. La documentation complète du format du fichier WHX est disponible à partir de la page d'accueil de WinHex à http://www.x-ways.net/winhex/api/.

8.7 Hints on Disk Cloning, Imaging, Image Restoration

Cloning or imaging with WinHex/X-Ways Forensics makes exact sector-wise, forensically sound copies, including all unused space and slack space. An image is usually preferable to a clone, as

all data (and metadata such as timestamps) in an image file is protected from the operating system.

If you clone/image a disk for backup purposes, try to avoid that the disk is being written to by the operating system or other programs during the process, e.g. by unmounting partitions that are mounted as drive letters before starting. Such write operations are unavoidable, of course, if you clone/image the disk that contains the active Windows installation from where you execute WinHex/X-Ways Forensics. If the source disk is being written to during the process, the clone/image may have an inconsistent state from the point of view of the operating system (e.g. it may not be able to boot a Windows installation any more). From a forensic standpoint, however, when cloning/imaging a live system, although it is highly desirable that no writing occurs any more, that should not be a major problem, as you still get an accurate snapshot of each and every sector.

If the destination of cloning or image restoration is a partition that is mounted as a drive letter, WinHex will try to clear all of Windows' internal buffers of that destination partition. If nonetheless you don't see the new contents in Windows Explorer on the destination after the operation has complete, you may simply need to reboot your system.

If your goal is not to create a forensic image, but merely a backup of a disk, to save drive space for the image, you could initialize unused drive space (free space and slack space) before creating the backup. This is because sectors that consist but of zero values barely increase the image size when compression is on.

Note that WinHex does not dynamically change partition sizes and adapt partitions to destination disks larger or smaller than the source.

8.8 Gestion de sauvegardes

Affiche une liste des sauvegardes WinHex préalablement créées. Les éléments sont listés en ordre chronologique ou alphabétique. Sélectionnez suivant le cas le fichier ou le secteur que vous aimeriez restaurer. Lorsque la fonction est terminée les contenus originaux du fichier ou du secteur sont affichés.

Vous pouvez restaurer la sauvegarde
• d'abord dans un fichier temporaire, mais que vous devrez ensuite sauvegarder,
• directement et immédiatement sur disque, ou bien
• dans un nouveau fichier.

Dans le cas "directement et immédiatement sur disque" vous pouvez spécifier un nouveau lecteur-destination ou un nouveau numéro de secteur-destination. Il est aussi possible d'extraire seulement un sous-ensemble de secteurs de la sauvegarde. (Toutefois, les secteurs situés au début d'une sauvegarde *compressée* ne peuvent pas être laissés de côté lors d'une restauration.) Si la sauvegarde a été enregistrée avec une somme de contrôle et/ou un hash-code, l'authenticité est vérifiée avant que le secteur ne soit directement écrit sur le disque.

Le gestionnaire de sauvegardes vous permet aussi d'effacer des sauvegardes dont vous n'avez plus besoin. Les sauvegardes créées pour un usage interne par la commande Annuler peuvent être effacées par WinHex automatiquement (cf. Options d'Annulation).

Les fichiers de sauvegarde qui sont gérés par le gestionnaire de sauvegardes sont situés dans le dossier spécifié dans le dialogue des Options Générales. Leurs noms de fichier sont "???.whx" où ??? est un unique nombre d'identification à trois chiffres. Ce nombre est affiché dans la dernière colonne de la liste du gestionnaire de sauvegardes.

8.9 Gestion de signets

Le gestionnaire de signets gère une liste des offsets de fichiers et de disques et les descriptions correspondantes, also called *annotations*, also used for search hits. Navigating from one entry to the next is easy if you press Ctrl+Left and Ctrl+Right. Vous pouvez créer de nouveaux signets et éditer ou effacer ceux déjà existants. Si un offset particulier d'un fichier est important parce que vous devez l'éditer plusieurs fois, vous pouvez le saisir dans le gestionnaire de signets. Ceci fait qu'il est beaucoup plus facile à retrouver plus tard, et que vous n'aurez pas à vous en souvenir. Descriptions may be up to 8192 characters in size. Une description appropriée pourrait être "Le tronçon de données commence ici". Optionally all positions maintained by the Position Manager can be *highlighted* in the editor window in a unique color you specify, and their descriptions displayed in yellow tooltip windows when the mouse cursor is moved over them. You may also add or edit positions with the context menu of an edit window or by clicking the middle mouse button in an edit window.

Cliquez le bouton droit de la souris de façon à afficher le menu contextuel in the Position Manager. Le menu contextuel fournit des commandes additionnelles. Vous pouvez effacer, charger ou enregistrer des signets (enregistrer aussi en HTML). Si la liste dans la gestion *générale* de signets a été changée, elle est enregistrée dans le fichier WinHex.pos lors de l'édition de WinHex.

La documentation complète du format du fichier POS est disponible à partir de la page d'accueil de WinHex à http://www.x-ways.net/winhex/.

8.10 Interpréteur de données

L'Interpréteur de données est une petite fenêtre qui fournit des "services de traduction" pour les données à la positon courante du curseur. Les options du dialogue vous permettent de spécifier les types de données qui doivent être prises en compte. Celles-ci sont couramment de 9 types de données entières (par défaut en notation décimale, optionnellement en héxadécimale ou octale), le format binaire (les 8 bits d'un octet), quatre types de données flottantes, les codes opération en assembleur (Intel®), et les types date.

L'Interpréteur de données est aussi capable de traduire tous les types de données (exceptés les codes opération en assembleur) en valeurs hexadécimales. Exécutez un double clic sur un nombre dans la fenêtre de l'Interpréteur de données, entrez une nouvelle valeur et appuyez sur **ENTREE**. L'interpréteur de données entrera les valeurs hexadécimales correspondantes dans la fenêtre d'édition à la position courante.

Quand vous cliquez sur l'interpréteur de données avec le bouton droit de la souris, WinHex affiche un menu contextuel, qui vous laisse commuter entre traduction *big-endian* ou *little-endian* (consultez "Terminaison Hexadécimale"). You may also choose between decimal, octal, or hexadecimal integer representation. This plus the digit grouping can also be selected in the Data Interpreter Options dialog.

Conseils:

- Quelques valeurs hexadécimales ne peuvent pas être traduites en nombres flottants. Pour ces valeurs l'Interpréteur de données affiche NAN (Not A Number: pas un nombre).
- Quelques valeurs hexadécimales ne peuvent pas être traduites en dates valides. Les gammes de valeur de différents types de dates sont plus ou moins étroites.
- Il y a des redondances dans le jeu d'instructions Intel®, qui sont affichées dans l'Interpréteur de données comme une duplication soit en code opération hexadécimal soit en mnémoniques. Les instructions en nombres flottants sont généralement affichées comme F***.
- Des références plus détaillées peuvent être trouvées dans le livre "Intel® Architecture Software Developer’s Manual Volume 2: Instruction Set Reference", disponible au format PDF sur Internet.

Appendice A: Définition d'un formulaire

1 En-tête

L'en-tête d'une définition de formulaire a le format suivant:

```
template "titre"
[description "description"]
[applies_to (file/disk/RAM)]
[fixed_start offset]
[sector-aligned]
[requires offset "valeurs hexa"]
[big-endian]
[hexadecimal/octal]
[read-only]
[multiple [taille globale fixe]]
// Ajouter ici les commentaires généraux sur le formulaire.
```

```
begin
      déclarations des variables
end
```

Les marqueurs ("tags") entre crochets sont optionnels. L'ordre des marqueurs est indifférent. Les expressions ne doivent être mises entre guillemets que si elles contiennent des espaces. Les commentaires peuvent figurer n'importe où dans la définition du formulaire. Les caractères suivant une double barre oblique sont ignorés par l'interpréteur.

Le mot-clé `applies_to` doit être suivi de l'un des mots (et un seul) : `file`, `disk`, ou `RAM`. WinHex lance un avertissement si vous tentez d'utiliser un formulaire sur des données provenant d'une source différente.

Alors que par défaut les formulaires commencent l'interprétation des données à la position courante du curseur quand on les applique, une déclaration optionnelle `fixed_start` fait en sorte que l'interprétation commence toujours au décalage absolu spécifié du fichier ou du disque.

Si le formulaire s'applique à un disque, le mot-clé `sector-aligned` fait en sorte que l'interprétation du formulaire commence au début du secteur courant, quelle que soit la position du curseur.

Comme le mot-clé `applies_to`, le mot-clé `requires` permet à WinHex d'empêcher l'application erronée d'une définition de formulaire à des données qui ne lui correspondent pas. Spécifiez un offset et une chaîne de valeurs hexadécimales de longueur arbitraire identifiant les données auxquelles doit s'appliquer la définition de formulaire. Par exemple, un enregistrement valide de boot maître se reconnaît aux valeurs 55 AA à l'offset 0x1FE, un exécutable aux valeurs 4D 5A ("MZ") à l'offset 0x0. Des mots-clé `applies_to` multiples peuvent coexister dans un en-tête de définition et seront tous pris en compte.

Le mot-clé `big-endian` a pour effet de faire lire et écrire toutes les variables entières multi-octets et booléennes de la définition en ordre big-endian (octet de poids fort en tête).

Le mot-clé `hexadecimal` affiche toutes les variables entières de la définition en notation hexadécimale.

Le mot-clé `read-only` fait que la définition ne peut être utilisée que pour examiner, mais non manipuler, les structures de données. Les contrôles d'édition du formulaire seront affichés en grisé.

Si le mot-clé `multiple` est spécifié dans l'en-tête, WinHex permet d'aller dans les enregistrements voisins tout en affichant le formulaire. Ceci nécessite que WinHex connaisse la taille de l'enregistrement. Si elle n'est pas spécifiée comme paramètre du mot-clé `multiple`, WinHex suppose que la taille totale d'une structure de formulaire (= enregistrement) est la position courante à la fin de l'interprétation du formulaire moins la position d'édition de base. Si celle-ci est d'une taille variable, c'est-à-dire que la taille de tableaux ou de paramètres `move` est déterminée dynamiquement par la valeur des variables, WinHex ne peut pas se déplacer vers les enregistrements de données précédents.

2 Corps: déclarations de variables

Le corps d'une définition de formulaire consiste principalement en déclarations de variables, similaires à celles des langages de programmation. Une déclaration a la forme de base:

```
type "titre"
```

où `type` peut être:

- `int8, uint8 = byte, int16, uint16, int24, 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`

`titre` ne doit être placé entre guillemets que s'il contient des caractères espace. `titre` ne peut pas ne comprendre que des chiffres. WinHex ne fait pas la distinction entre majuscules et minuscules dans les titres. 41 caractères au plus peuvent être utilisés pour identifier une variable.

`type` peut être précédé d'au plus un libellé de chacune des groupes de modificateurs suivantes:

```
big-endian      little-endian
hexadecimal     decimal         octal
read-only       read-write
```

Ces modificateurs n'affectent que la variable qui les suit immédiatement. Ils sont redondants s'ils apparaîssent déjà dans l'en-tête.

Le nombre qui suit un nom de type indique la taille de chaque variable (chaînes: de chaque caractère) en bits. Avec `char16` et `string16`, WinHex reconnaît les caractères et chaînes Unicode. Cependant les caractères Unicode autres que les 256 premiers caractères équivalents-ANSI ne sont pas reconnus. La taille maximum d'une chaîne qui peut être éditée par formulaire est de 8192 octets.

Les types `string`, `string16`, et `hex` exigent un paramètre supplémentaire spécifiant le nombre d'éléments. Ce paramètre peut être une constante ou une variable déjà déclarée. Une constante peut être spécifiée en notation hexadécimale: celle-ci est reconnue si le nombre est précédé de `0x`.

On peut déclarer des tableaux de variables en plaçant la taille du tableau entre crochets près du

type ou du titre. Précisez "unilimited" pour la taille du champ pour que le formulaire s'arrête seulement lorsque la fin du fichier est atteinte. Les deux lignes qui suivent déclarent une chaîne ASCII de taille dynamique, dont la longueur dépend de la variable précédente:

```
uint8      "len"
char[len]  "Ma chaine"
```

On obtiendrait le même résultat avec:

```
byte       "len"
string len "Ma chaine"
```

Le caractère "~" peut être employé comme substitut pour remplacement ultérieur par le nombre véritable d'éléments du tableau (cf. ci-dessous). Ceci ne s'applique pas aux tableaux de `char`, ceux-ci étant automatiquement traduits en chaînes.

Numerical parameters of `string`, `string16`, and hex variables as well as array size expressions may be specified in mathematical notation. They will be processed by the integrated formula parser. Such expressions need to be enclosed in brackets. They must not contain space characters. They may make use of previously declared integer variables whose names do not contain space characters either. Supported operations are addition (+), subtraction (-), multiplication (*), integer division (/), modular division (%), bitwise AND (&), bitwise OR (|), and bitwise XOR (^). Valid mathematical expressions are for example (5*2+1) or (len1/(len2+4)). The result is always an integer and must be a positive number.

`zstring` et `zstring16` are null-terminated strings whose size is determined dynamically at run-time.

3 Corps: commandes avancées

Plusieurs déclarations de variables mises entre accolades forment un bloc qu'on peut réutiliser comme un tout. Notez cependant que les blocs ne peuvent pas être imbriqués dans cette version. On peut utiliser le caractère ~ dans un nom de variable comme substitut pour remplacement ultérieur par le compteur réel. Le mot optionnel `numbering` spécifie la valeur d'où part le compte (0 par défaut).

```
numbering  1
{
byte       "len"
string len "Chaine No. ~"
}[10]
```

Dans cet exemple les noms de variables réels du formulaire seront "Chaine No. 1", "Chaine No. 2", ..., "Chaine No. 10". Au lieu d'un nombre constant de repetitions (10 dans cet exemple), vous pouvez aussi préciser "unlimited". Dans ce cas WinHex répètera le bloc jusqu'à ce qu'il rencontre la fin du fichier. "ExitLoop" can be used to break out of a loop at any time.

"IfEqual" is useful for the comparison of two expressions. Operands can be either both numerical values, be it constant values in decimal notation, integer variables or a formulas, or byte sequences given as text or hex values which are compared byte by byte. ASCII string expressions must be enclosed in quotation marks, hex sequences must be preceded by a "0x" identifier. Formulas need to be enclosed in brackets.

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

An "IfEqual" command block is terminated with an "EndIf" statement. If the compared expressions are equal, template interpretation continues after "IfEqual". Optionally, "IfEqual" can be followed by an "Else" statement. The template processor branches into the "Else" block if the expressions are not equal. "IfEqual" commands must not be nested. "IfGreater" is similar to "IfEqual". The condition is true if the first expression is greater than the second. Strings and hex values are compared lexicographically.

Pour faciliter la lecture et les déplacements dans le formulaire, vous pouvez définir des groupes de variables séparés par des espaces dans la boîte de dialogue:

```
section    "...Titre de section..."
...
endsection
```

Les mots `section`, `endsection`, et `numbering` ne font pas avancer la position courante du curseur dans les données à interpréter.

Il existe deux commandes qui elles non plus ne déclarent pas de variables, mais sont explicitement utilisées pour modifier la position courante du curseur. Ceci peut servir à passer au-dessus de données non concernées (en avant) ou à pouvoir accéder à certaines variables plus d'une fois comme types différents (en arrière). Utilisez le mot `move n` pour sauter `n` octets depuis la position courante, `n` pouvant être négatif. `goto n` se rend à la position absolue (depuis le début du formulaire interprété) spécifiée (`n` doit être positif).

L'exemple suivant montre comment accéder à une variable à la fois comme entier 32-bit et chaîne à 4 éléments de valeur hexadécimale:

```
int32      "Numéro de série disque (décimal)"
move -4
hex 4      "Numéro de série disque (hex)"
```

4 Corps: Variables flexibles

A special variable type supported by templates is `uint_flex`. This type allows to compose an unsigned integer value from various individual bits within a 32-bit (4-byte) range in an arbitrary order and is even more flexible than a so-called bit field in the C programming language.

uint_flex requires an additional parameter string in inverted commas that specifies exactly which bits are used in which order, separated by commas. The bit listed first becomes the most significant bit (high value bit) in the resulting integer, and it is not interpreted as a + or - indicator. The bit listed last becomes the least significant bit in the resulting integer.

The bits are counted starting with 0. Bit 0 is the bit that is the least significant bit of the 1st byte. Bit 31 is the most significant bit of the fourth byte. Thus, the definition is based on little-endian philosophy.

For example,
`uint_flex "15,14,13,12,11,10,9,8,7,6,5,4,3,2,1,0" "Standard 16-bit integer"`
is exactly the same as `uint16`, the common unsigned 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"`
is exactly the same as `uint32`, the common unsigned 32-bit integer variable.

The benefit of `uint_flex`, though, is that the number, the position, and the usage order of all bits can be chosen arbitrarily. For example,
`uint_flex "7,15,23,31" "An unusual 4-bit integer"`
composes a 4-bit integer out of the respective most significant bits of each of the four bytes involved. If these four bytes happen to be
F0 A0 0F 0A =
11110000 **1**0100000 **0**0001111 **0**0001010,
bit 7 is **1**, bit 15 is **1**, bit 23 is **0**, and bit 31 is **0**.
So the resulting uint_flex is **11**0**0** = **1***8 + **1***4 + **0***2 + **0***1 = 12.

Appendice B: Commandes de scripts

Les commandes de scripts sont *in*sensibles à la casse. Les commentaires peuvent apparaître n'importe où dans le script et doivent être précédés de deux barres obliques. Les paramètres ont une longueur maximum de 255 caractères. Where in doubt because hex values, text strings (or even integer numbers) are accepted as parameters, you may use inverted commas (quotation marks) to enforce the interpretation of a parameter as text. Inverted commas are *required* if a text string or variable name contains one or more space characters, so that all characters between the inverted commas are recognized as constituting *one* parameter.

Whereever numerical parameters are expected (integer numbers), the integrated formula parser allows you to use mathematical expressions. Such expressions need to be enclosed in brackets. They must not contain space characters. They may make use of variables that can be interpreted

as integer numbers. Supported operations are addition (+), subtraction (-), multiplication (*), integer division (/), modular division (%), bitwise AND (&), bitwise OR (|), and bitwise XOR (^). Valid mathematical expressions are for example (5*2+1), (MyVar1/(MyVar2+4)), or (-MyVar).

Voici une description des commandes de script actuellement reconnues, avec des exemples de paramètres.

Create "D:\My File.txt" 1000
Créé le fichier avec une taille initiale de 1000 octets. Si le fichier existe déjà, il est écrasé.

Open "D:\My File.txt"
Open "D:*.txt"
Ouvre le ou les fichiers specifies. Specify "?" as the parameter to let the user select the file to open.

Open C:
Open D:
Ouvre le lecteur logique spécifié. Specify ":?" as the parameter to let the user select a logical drive or physical disk to open.

Open 80h
Open 81h
Open 9Eh
Ouvre le média physique spécifié. Floppy disk numbering starts with 00h, fixed and removable drive numbering with 80h, optical media numbering with 9Eh.

Optionally, you may pass a second parameter with the Open command that defines the edit mode in which to open the file or media ("in-place" or "read-only").

CreateBackup
Créé une sauvegarde du fichier actif dans son état courant.

CreateBackupEx 0 100000 650 true "F:\My backup.whx"
Creates a backup of the active disk, from sector 0 through sector 1,000,000. The backup file will be split automatically at a size of 650 MB. Compression is enabled (“true”). The output file is specified as the last parameter.
If the backup file should not be split, specify 0 as the third parameter. To disable compression, specify “false”. To have the Backup Manager automatically assign a filename and place the file in the folder for backup files, specify "" as the last parameter.

Goto 0x128
Goto MyVariable
Déplace la position hexadécimale du curseur au décalage 0x128. Une variable existante (jusqu’à 8 octets) peut aussi être interprétée comme une valeur numérique.

Move -100

Déplace en arrière la position courante du curseur de 100 octets (en decimal).

Write "Test"
Write 0x0D0A
Write MyVariable
Ecrit les quatre caractères ascii “Test” ou les valeurs hexa “0D0A” depuis la position courante (en mode écrasement) et déplace la position courante vers l’avant en conséquence (dans cet exemple: de 4 octets). Permet aussi d’écrire le contenu d’une variable précisée comme paramètre.

Insert "Test"
Functions just as the "Write" command, but in *insert* mode. Must only be used with *files*.

Read MyVariable 10
Lit les 10 octets depuis la position courante dans une variable nommée «MyVariable». Si la variable n’existe pas, elle est créée. Up to 32 different variables allowed. Un autre moyen de créeer une variable est la commande «Assign».

ReadLn MyVariable
Reads from the current position into a variable named "MyVariable" until the next line break is encountered. If the variable already exists, its size will be adjusted accordingly.

Close
Ferme la fenêtre active sans enregistrer.

CloseAll
Ferme toutes les fenêtres sans enregistrer.

Save
Enregistre les modifications du fichier ou du disque dans la fenêtre active.

SaveAs "C:\New Name.txt"
Enregistre le fichier de la fenêtre active dans le chemin d’accès spécifié. Specify "?" as the parameter to let the user select the destination.

SaveAll
Enregistre les modifications de toutes les fenêtres.

Terminate
Aborts script execution.

Exit
Termine l’exécution d’un script et ferme WinHex.

ExitIfNoFilesOpen
Arrête l’exécution d’un script si aucun fichier n’est déjà ouvert dans WinHex.

Block 100 200
Block "My Variable 1" "My Variable 2"
Définit un bloc dans la fenêtre active pour exécuter de l'offset 100 à l'offset 200 (en décimal). Alternatively, existing variables (each up to 8 bytes large) can be interpreted as numeric values.

Block1 0x100
Définit le bloc debutant à l'offset hexadecimal 0x100. Une variable est aussi autorisée comme paramètre.

Block2 0x200
Définit la fin du bloc à l'offset hexadecimal 0x200. Une variable est aussi autorisée comme paramètre.

Copy
Copie le bloc courant dans le presse-papiers. Si aucun bloc n'est spécifié, la commande agit depuis la commande «Copier» dans le menu d'édition.

Cut
Coupe le bloc courant pré-défini du fichier et le met dans le presse-papiers.

Remove
Enlève le bloc pré-défini depuis le fichier

CopyIntoNewFile "D:\New File.dat"
CopyIntoNewFile "D:\File +MyVariable+.dat"
Copie le bloc courant pré-défini dans le nouveau fichier spécifié, sans utiliser le presse-papiers. Si aucun bloc n'est défini, la commande agit comme depuis la commande «Copy» du menu d'édition. Peut aussi copier des secteurs disques. Le nouveau fichier ne sera pas automatiquement ouvert dans une nouvelle fenêtre. Autorise un nombre illimité de «+» concaténés dans le paramètre. Un nom de variable sera interprété come un entier s'il n'est pas supérieur à 2^24 (env. 16Mo). Ceci est utile pour les boucles et la récupération de fichiers.

Paste
Colle le contenu courant du presse-papiers à la position courante d'un fichier, sans en changer sa position courante.

WriteClipboard
Ecrit le contenu courant du presse-papiers à la position courante d'un fichier ou de secteurs disques, sans changer sa position courante, en écrasant les données de la position courante.

Convert *Param1 Param2*
Converti les données du fichier actif d'un format à un autre. Les paramètres valides sont ANSI, IBM, EBCDIC, Binaire, HexASCII, IntelHex, MotorolaS, Base64, UUCode, LowerCase et UpperCase, en combinaisons depuis la commande «Convert» du menu Edition.

AESEncrypt "My Password"

Encrypte le fichier ou le disque actif, ou le bloc sélectionné, avec la clé spécifiée (jusqu'à une longueur de 32 caractères) en utilisant l'algorithme AES.

AESDecrypt "My Password"
Décode le fichier ou disque actif.

Find "John" [*MatchCase MatchWord Down Up BlockOnly SaveAllPos Unicode Wildcards*]
Find 0x1234 [*Down Up BlockOnly SaveAllPos Wildcards*]
Recherche dans la fenêtre active le nom John ou les valeurs hexadécimales 0x1234, et s'arrête à la première occurrence. D'autres paramètres sont optionnels. By default, WinHex searches the entire file/disk. Les paramètres optionnels fonctionnent comme dans les options «recherche» de WinHex.

ReplaceAll "Jon" "Don" [*MatchCase MatchWord Down Up BlockOnly Unicode Wildcards*]
ReplaceAll 0x0A 0x0D0A [*Down Up BlockOnly Wildcards*]
Remplace toutes occurrences of either a string or hexadecimal values in the active file with something else. Can only be applied to a disk if in in-place mode.

IfFound
Une valeur booléenne dépend ou non de la dernière commande «Find» ou «ReplaceAll», réussie. Place les commandes devant être exécutées si quelque chose a été trouvé après la commande «IfFound»

IfEqual MyVariable "Hello World"
IfEqual 0x12345678 MyVariable
IfEqual MyVariable 1000
IfEqual MyVariable MyOtherVariable
IfEqual MyVariable (10*MyOtherVariable)
Compares either two numerical integer values (each of them being a constant value, an integer variable or a mathematical expression) or two variables, ASCII strings, or hexadecimal values at the binary level. Comparing two objects at the binary with a different length always returns False as the result. If equal, the following commands will be executed. If conditions must not be nested.

IfGreater MyVariable "Hello World"
IfGreater 0x12345678 MyVariable
IfGreater MyVariable 1000
IfGreater MyVariable MyOtherVariable
IfGreater MyVariable (10*MyOtherVariable)
Accepts the same parameters as IfEqual. If the first one is greater than the second one, the following commands will be executed. If conditions must not be nested.

Else
Peut se produire après "IfFound" ou "IfEqual". Les commandes après la commande «Else» seront exécutées si rien n'a été trouvé ou si les objets comparées sont inégales.

EndIf

Arrête l’exécution conditionnelle de commandes (après IfFound ou IfEqual).

ExitLoop
Sort d'une boucle. Une boucle est definie entre accollades: {}. La fermeture peut être suivi d'un entier entre crochets [], ce qui détermine le nombre de boucles à exécuter. L'expression entre crochets peut aussi être une variable ou le mot "unlimited" (dans ce cas la boucle ne peut être interrompue que par la commande «ExitLoop»). Les boucles ne doivent être imbriquées.

Exemple de boucle:
{ Write "Loop" }[10] écrira le mot “Loop” 10 fois.

Label ContinueHere
Creates a label named "ContinueHere"

JumpTo ContinueHere
Continues script execution with the command following that label.

NextObj
Bascule cyclique à la fenêtre ouverte suivante et l’active. Ex: Si 3 fenêtres sont ouvertes, et la fenêtre 3 active, «NextObj» rendra la fenêtre 1 active.

ForAllObjDo
Les commandes de script du bloc suivant (jusqu’à la commande «EndDo» soit rencontrée) sera appliquée à tous les fichiers et disques ouverts.

CopyFile C:\A.dat D:\B.dat
Copie le contenu de c:\A.dat dans le fichier D:\B.dat.

MoveFile C:\A.dat D:\B.dat
Déplace le fichier C:\A.dat vers D:\B.dat.

DeleteFile C:\A.dat
Surprisingly, deletes C:\A.dat.

InitFreeSpace
InitSlackSpace
Clears free space or slack on the current logical drive, respectively, using the currently set initialization settings. InitSlackSpace switches the drive temporarily to in-place mode, thus saving all pending changes.

InitMFTRecords
Clears unused MFT FILE records on the current logical drive if it is formatted with NTFS, using the currently set initialization settings. Simply does nothing on other file systems. The changes are written immediately to the disk.

Assign MyVariable 12345

Assign MyVariable 0x0D0A
Assign MyVariable "J'aime WinHex"
Assign MyVariable MyOtherVariable
Assigne l'entier spécifié ou le contenu d'une variable (ou des données binaire ou de texte ASCII) dans une variable nommée «MyVariable». Si cette variable n'existe pas, elle est créée. Jusqu'à 32 différentes variables sont autorisées. Une variable peut aussi être créée par la commande «Read».

SetVarSize MyVariable 1
SetVarSize MyVariable 4
Explicitly sets the allocated memory size of a variable at a given time, in bytes. This can be useful e.g. for variables that hold integer values and that are the result of a calculation, if this value is to be written to a binary file with a fixed-length structure. Without SetVarSize, no assumption must be made about the size of the variable. For instance, the number 300 could be stored in any number of bytes larger than 1. If the new size set by SetVarSize is smaller than the old size, the allocated memory is truncated. If the new size is larger, the allocated memory is expanded. At any rate, the value of the persisting bytes is retained.

GetUserInput MyVariable "Please enter your name:"
Stores the ASCII text or binary data (0x...) specified by the user at script execution time (128 bytes at max.) in a variable named "MyVariable". The user is prompted by the message you provide as the second parameter. If this variable does not yet exist, it will be created. Other ways to create variables: Assign, Read.

GetUserInputI MyIntegerVariable "Please enter your age:"
Works like GetUserInput, but accepts and stores only integer numbers.

Inc MyVariable
Gère la variable comme un entier (si sa taille ne dépasse pas 8 octets) et l'incrémente de 1. Utile pour les boucles.

Dec MyVariable
Gère la variable comme un entier (si sa taille ne dépasse pas 8 octets) et la décrémente de 1.

IntToStr MyStr MyInt
IntToStr MyStr 12345
Stores the decimal ASCII text representation of the integer number specified as the second parameter in a variable specified as the first parameter.

StrToInt MyInt MyStr
Stores the binary representation of the integer number specified as a decimal ASCII string in the second parameter in a variable specified as the first parameter.

StrCat MyString MyString2
StrCat MyString ".txt"
Appends one string to another. The second parameter may be a variable or a constant string. The first parameter must be a variable. The result will be saved in the variable specified by the first

parameter and must not be longer than 255 characters.

GetClusterAlloc MyStr
May be applied to a logical volume. Retrieves a textual description of the current position's allocation, e.g. which file is stored in the current cluster, and saves that description in the specified variable.

GetClusterAllocEx IntVar
May be applied to a logical volume. Retrieves an integer value that indicated whether the cluster at the current position is allocated (1) or not (0), and saves that description in the specified variable.

GetClusterSize IntVar
May be applied to a logical volume. Retrieves the cluster size and saves that value in the specified integer variable.

InterpretImageAsDisk
Treats a raw image, Encase image or evidence file like the original physical disk or partition. Requires a specialist or forensic license.

CalcHash HashType MyVariable
CalcHashEx HashType MyVariable
Calculates a hash as known from the command in the Tools menu and stores it in the specified variable (which will be created if it does not yet exist). The HashType parameter must be one of the following: CS8, CS16, CS32, CS64, CRC16, CRC32, MD5, SHA-1, SHA-256, PSCHF. CalcHashEx in addition displays the hash in a dialog window.

MessageBox "Caution"
Affiche un message «Caution» et offer à l'utilisateur le choix OK ou annuler. Pressing the Cancel button will abort script execution.

ExecuteScript "ScriptName"
Exécute un script depuis un autre script, depuis la position courante, p. e. dependant de l'état conditionnel. Calls to other scripts may be nested. When the called script is finished, execution of the original script will be resumed with the next command. This feature can help you structure your scripts more clearly.

Turbo On
Turbo Off
In turbo mode, most screen elements are not updated during script execution and you are not able to abort (e.g. by pressing Esc) or pause. This accelerates the script by up to 75% if a lot of simple commands such as Move and NextObj are executed in a loop.

Debug
Chacune de toutes les commandes suivantes doivent être confirmées par l'utilisateur.

UseLogFile
Les messages d'erreurs sont écrites dans le fichier log "Scripting.log" dans le dossier destine aux fichiers temporaries. These messages are not shown in a message box that requires user interaction. Useful especially when running scripts on unattended remote computers.

CurrentPos
GetSize
unlimited
Sont des mots-clés qui agissent comme subsitut pour remplacement ultérieur et peuvent être utilisés où des paramètres numériques sont requis. Un script en cours d'exécution «CurrentPos» correspond pour l'offset dans le fichier actif ou la fenêtre disque, «GetSize» pour la taille en octets. «unlimited » actually stands for the number 2,147,483,647.

Appendice C: Q&R éditeur disque

Comment accéder aux secteurs CD-RW?

DirectCD and PacketCD must not be installed on the Windows system.

Comment accéder aux secteurs CD-ROM et DVD sous Windows 9x?

Assurez-vous que les conditions suivantes sont réunies:

1. Un pilote Windows doit être installé pour le lecteur CD-ROM/DVD. Un pilote MS-DOS ne suffit pas.
2. L'interface ASPI doit être installée. Vous devrez peut-être copier le fichier wnaspi32.dll manuellement dans votre dossier Windows\System. Ce fichier se trouve sur le CD d'installation de Windows. Le programme shareware WinZip (disponible à http://www.winzip.com) est recommandé pour l'extraction d'archives CAB.
3. Le lecteur CD-ROM/DVD doit accepter la manière dont WinHex tente de lire les secteurs. La plupart des lecteurs ATAPI et SCSI modernes conviennent.

Comment faire détecter par WinHex un Disque Flash ATA Carte PC / Lecteur PCMCIA installé en tant que disque physique sous Windows 9x?

Panneau de configuration Windows → Système → Gestionnaire de périphériques → Sélectionner le périphérique PCMCIA → Cliquer sur "Propriétés" → Chercher une option semblable à "Int 13h device". La manière de trouver cette case à cocher varie selon les versions de Windows. Si possible, *activez* cette option and redémarrez votre ordinateur.

Appendice D: Secteur du boot maître

Le secteur du boot maître est situé au début physique du disque dur, éditable en utilisant l'éditeur de disque. Il consiste en un maître boostrap chargeur de code (446 octets) et de quatre enregistrements consécutifs de partition identiquement structurés. Finalement, la signature hexadécimale 55AA termine un Secteur Boot Maître valide.

Le format d'une partition enregistrée est comme suit:

Offset	Size	Description
0	8 bit	A value of 80 designates an active partition.
1	8 bit	Partition start head
2	8 bit	Partition start sector (bits 0-5)
3	8 bit	Partition start track (bits 8,9 in “start sector” as bits 6,7)
4	8 bit	Operating system indicator
5	8 bit	Partition end head
6	8 bit	Partition end sector (bits 0-5)
7	8 bit	Partition end track (bits 8,9 in “end sector” as bits 6,7)
8	32 bit	Sectors preceding partition
C	32 bit	Length of partition in sectors

Operating system indicators:
(hexadecimal)

00	Empty partition-table entry
01	DOS FAT12
04	DOS FAT16 (up to 32M)
05	DOS 3.3+ extended partition
06	DOS 3.31+ FAT16 (over 32M)
07	Windows NT NTFS, OS/2 HPFS, Advanced Unix
08	OS/2 v1.0-1.3, AIX bootable partition, SplitDrive
09	AIX data partition
0A	OS/2 Boot Manager
0B	Windows 95+ FAT32
0C	Windows 95+ FAT32 (using LBA-mode INT 13 extensions)
0E	DOS FAT16 (over 32 MB, using INT 13 extensions)
0F	Extended partition (using INT 13 extensions)
17	Hidden NTFS partition
1B	Hidden Windows 95 FAT32 partition
1C	Hidden Windows 95 FAT32 partition (using LBA-mode INT 13 extensions)
1E	Hidden LBA VFAT partition
50	OnTrack Disk Manager, read-only partition
51	OnTrack Disk Manager, read/write partition
81	Linux
82	Linux Swap partition, Solaris (Unix)
83	Linux native file system (ext2fs/xiafs)

85	Linux EXT
86	FAT16 volume/stripe set (Windows NT)
87	HPFS fault-tolerant mirrored partition, NTFS volume/stripe set
BE	Solaris boot partition
C0	DR-DOS/Novell DOS secured partition
C6	Corrupted FAT16 volume/stripe set (Windows NT)
C7	Corrupted NTFS volume/stripe set
F2	DOS 3.3+ secondary partition

Appendice E: Secteurs en surplus

This term is used in WinHex in the following way:

Surplus sectors on a logical drive are those few sectors at the end that do not add to a full cluster and thus cannot be used by the OS (and thus by no conventional application program either).

Surplus sectors on a physical disk are those sectors situés en fin de disque, en dehors du schéma normal de géométrie du disque (because they do not add to a full cylinder/header/track entity), ce qui explique qu'ils ne sont pas utilisés par aucune partition ou par le système d'exploitation (or any conventional application program).

Surplus sectors have nothing to do with "bad" or damaged sectors or sectors a hard disk internally uses as a replacement for sectors found to be faulty.