

# *X-Ways Forensics*

*Integrierte Computerforensik-Umgebung  
Fortschrittliche Datenrettungs- und IT-Sicherheitssoftware  
auf Englisch, Deutsch, Französisch, Spanisch, Italienisch und Portugiesisch*

- **Umfassende Fallverwaltung**

X-Ways Forensics verwaltet Ihre Fälle getrennt voneinander und ermöglicht Ihnen die genaue Identifizierung aller Asservate und gefundener Beweise, die zu einem bestimmten Fall gehören. Es erzeugt eine baumähnliche Struktur für jeden Ihrer Fälle wo Sie beliebig Laufwerke, Images und andere Dateien hinzufügen können. Für jedes Asservat werden die zugehörigen Notizen und gefundenen Beweise getrennt gespeichert.

- **Automatisierte Protokollierung**

Die Protokollierung aller Aktivitäten ist standardmäßig aktiviert. Dies kann hilfreich sein, wenn Sie Ihre bereits unternommenen Schritte zurück verfolgen wollen, weil Sie die Arbeit unterbrechen und zu einem späteren Zeitpunkt fortsetzen müssen. Da jede Operation aufgezeichnet wird, können Sie dies dazu verwenden, die Integrität Ihrer Beweissicherungsmethodik aufzuzeigen.

- **Automatisierte Berichte im HTML-Format**

Die automatisierte Protokollierung ermöglicht auch die Generierung eines Untersuchungsberichtes unter Verwendung der eingegebenen Beschreibungen und der unternommenen Schritte. Alle Aktivitäten werden sortiert nach Asservat und inklusive des jeweiligen Resultats. Diese Berichtsfunktion befreit Sie von der Aufgabe, Ihre Berichte ausschließlich auf der Basis Ihrer eigenen Notizen selbst schreiben zu müssen. Sie können den generierten Report jederzeit weiter verbessern, indem Sie den HTML-Text in eine beliebige Anwendung importieren, die HTML-Importe unterstützt, beispielsweise Microsoft Word oder OpenOffice.org.

- **Schutz vor versehentlichen Änderungen an den Asservaten**

X-Ways Forensics erlaubt keinerlei Änderungen an Asservaten. Nur Dateien, die in den Ausgabe- oder Temp-Verzeichnissen erzeugt wurden, können von X-Ways Forensics modifiziert werden, um die übliche forensische Methodik zu unterstützen. WinHex, verwendet mit forensischer Lizenz, kann in Editiermodi wechseln, allerdings wird auch hier vorher vom Nutzer eine ausdrückliche Bestätigung gefordert, um versehentliche Wechsel auszuschließen.

- **Darstellung aller existierenden und gelöschten Dateien nach Dateitypkategorie**

X-Ways Forensics unterstützt den Ansatz, nach bestimmten Dateitypen zu suchen, ohne sich auf jeweils eine bestimmte Dateierweiterung pro Suche einzuschränken. In vielen Fällen sucht ein Ermittler nach Office Dokumenten, aber nicht ausschließlich Word-Dokumente, oder nach

Bildern unabhängig von deren Format. X-Ways Forensics kann Laufwerksinhaltsstabellen erstellen, die die eigentliche Verzeichnisstruktur eines Dateisystems komplett ignorieren und stattdessen nach vordefinierten Kategorien wie „Bilder“, „Office“ oder „Internet“ suchen. Diese Kategorien sind vom Nutzer vollständig anpassbar.

- **Galerieansicht für Bilder**

X-Ways Forensics bietet eine Galerieansicht für alle Bilddateien in einem Verzeichnis oder in der „Bilder“-Kategorie der Laufwerksinhaltsabelle. Durch die Übersicht über die Thumbnails kann die Suche nach relevanten Grafiken erheblich beschleunigt werden. Unterstützte Dateitypen für die Galerieansicht sind JPEG, JPEG 2000, GIF, TIFF, Bitmap, PNG, TGA, PCX, WMF, EMF, MNG und JBG.

- **Dateien einsehen**

Wählen Sie beliebig viele Dateien im Verzeichnisbrowser zum Einsehen aus. Zur Darstellung im integrierten Betrachter muss eine Datei nicht einmal zunächst aus einer Festplattenpartition oder einer Imagedatei extrahiert werden. Wenn der integrierte Betrachter die Datei nicht öffnen kann, wird ein externer Betrachter aufgerufen. Bis zu drei verschiedene externe Programme können festgelegt und direkt aufgerufen werden. Der interne Betrachter unterstützt diverses Bilddateiformate und auch Windows Registry-Dateien.

- **Hautfarbenanteil**

In Fällen von Kinderpornographie erscheint es offensichtlich, dass vermutlich relevante Bilder sehr wahrscheinlich einen hohen Anteil an Hautfarben haben. Um die Suche des Ermittlers nach Bildern mit potentiell relevantem Inhalt zu beschleunigen, besitzt X-Ways Forensics die Möglichkeit, Bilder nach ihrem Hautfarbenanteil zu sortieren.

- **Entdeckung von Dateierweiterungs-/Dateityp-Unstimmigkeiten**

X-Ways Forensics erkennt Versuche, relevante Dateien zu verstecken, indem sie in unscheinbar aussehende Dateien mit falschen Dateierweiterungen umbenannt werden. Zum Beispiel könnte eine JPEG-Bilddatei unter dem Namen sys782.dll im Windows-Verzeichnis gespeichert sein, was es dem menschlichen Ermittler praktisch unmöglich macht, den illegitimen Inhalt der Datei zu erraten. Um die Aufmerksamkeit auf solche offensichtlichen Fälle der Dateiverschleierung zu lenken, ermöglicht X-Ways Forensics die Erzeugung von Laufwerksinhaltsstabellen, in denen Dateien ausdrücklich hervorgehoben werden, deren Header nicht zu ihrer Dateierweiterung passt.

- **Dateisystem-Untersuchung**

Eingebaute Unterstützung von FAT12, FAT16, FAT32 und NTFS, in kürze zusätzlich Ext2, Ext3, ReiserFS und CDFS.

- **Unterstützung von EnCase-Images**

Forensikexperten haben möglicherweise EnCase von Guidance Software verwendet, um ein Image für ihre Untersuchungen zu erzeugen. X-Ways Forensics kann so ein EnCase-Image zu einem Fall hinzufügen und untersuchen wie jedes andere Asservat.

- **Entdeckung ATA-geschützter Bereiche (Host-Protected Areas, HPA)**

Eine der ausgefeilteren Methoden zum Verstecken von Daten auf einer Festplatte ist es, die Größe zu verändern, die eine Festplatte an das Betriebssystem meldet. Auf die Art kann

beispielsweise eine 100 GB Festplatte, die zu 80 GB verändert wurde, 20 GB versteckten Speicherplatz enthalten. Diese sogenannten ATA-geschützten Bereiche werden von X-Ways Forensics entdeckt und dem Ermittler direkt gemeldet.

- **Disk-Editor, Datei-Editor, RAM-Editor**

WinHex, der technische Kern von X-Ways Forensics, ist ein fortschrittlicher binärer Editor, der Ihnen Zugriff auf alle Dateien, Cluster, Sektoren, Bytes, Nibbles und Bits auf einem Datenträger verschafft. Er unterstützt praktisch unbegrenzt große Dateien und Datenträger bis in die Terabyte-Region (Tausende von Gigabytes!). Dabei ist der Bedarf an Arbeitsspeicher minimal und die Zugriffsgeschwindigkeit hervorragend.

- **Verzeichnis-Browser für FAT & NTFS**

Der Verzeichnis-Browser ist genauso leicht zu benutzen wie der Windows Explorer (rechtsseitige Liste). Es werden sowohl existierende als auch gelöschte Dateien und Verzeichnisse mit allen Details aufgelistet. Er ermöglicht es, Clusterketten anzuzeigen, mit dem Disk-Editor zu Dateien und Verzeichnissen zu navigieren und Dateien von einem Datenträger herunterzukopieren. Dank der nativen Dateisystem-Unterstützung funktioniert er auch mit Image-Dateien und Partitionen, die nicht in Windows als Laufwerk geladen sind.

- **Klonen von Datenträgern / Disk-Imaging unter DOS und Windows**

X-Ways Forensics erstellt sektorweise Kopien von den meisten Datenträgertypen, entweder auf andere Datenträger (Klone, Duplikate) oder in Form von Image-Dateien. Die Kopien sind „forensisch einwandfrei“, d. h. sie enthalten allen Schlupfspeicher (Slack Space) sowie den freien Laufwerksspeicher. Dies ist für forensische Zwecke von großer Bedeutung, da auf einer Kopie des Originaldatenträgers gearbeitet werden kann. Image-Dateien können optional komprimiert oder in kleine, unabhängige Segmente aufgeteilt werden. WinHex kann Protokolldateien erstellen, die jeden beim Klonen entdeckten beschädigten Sektor verzeichnen, ohne dass Sie ständig Fehlermeldungen wegklicken müssen. Alle lesbaren Daten werden in die Kopie übertragen. WinHex lässt Sie die Integrität und Authentizität von Image-Dateien vor deren Rücküberspielung auf einen Datenträger überprüfen.

Außerdem ist ein DOS-basiertes Programm, X-Ways Replica, zum Klonen von Festplatten enthalten. Die meisten Windows-Umgebungen greifen ungefragt auf ein neu angeschlossenes Laufwerk zu, wobei z. B. das Datum des letzten Zugriffs einiger Dateien verfälscht wird. Dies kann beim Klonen des Originals unter DOS vermieden werden. [X-Ways Replica](#)

- **Forensisch sicheres Löschen von Festplatten**

WinHex kann jeden einzelnen Sektor eines Datenträgers mit Nullbytes auffüllen (wobei die Bytefolge beliebig bestimmt oder sogar zufällig gewählt werden kann). Die Überschreibung der Festplatte mit Nullbytes kann beliebig oft wiederholt werden. Dies gewährleistet maximale Sicherheit. Durch diese Methode werden sämtliche Spuren von Dateien, Verzeichnissen, Viren, proprietären und Diagnosepartitionen der Festplatte gelöscht und eine „klinisch“ saubere Festplatte hinterlassen. Dabei wird der durch das US-Verteidigungsministerium erlassene Standard DoD 5220.22-M für das sichere Löschen von Daten eingehalten.

Zusätzlich ist es möglich, mit WinHex einzelne Dateien oder lediglich den freien ungenutzten Speicherplatz einer Festplatte sicher zu löschen. Darüber hinaus können vor dem Klonen

Sektoren auf dem Zieldatenträger mit spezifischen Byte-Mustern gefüllt werden, die beispielsweise für den ASCII String „BADSECTOR“ stehen. So können die Teile einer Festplatte leicht identifiziert werden, die während des Klonens nicht überschrieben wurden, weil die Originalsektoren nicht gelesen werden konnten (wegen physischer Beschädigung) oder weil die Ursprungsfestplatte kleiner war. Alternativ können die nichtlesbaren Sektoren mit einem Muster Ihrer Wahl auf die Zielplatte geschrieben werden.

- **Schlupfspeicher extrahieren**

Sammelt den Schlupfspeicher (englisch "slack space"), die unbenutzten Bytes im jeweils letzten Cluster einer Clusterkette, hinter dem tatsächlichen Ende der Datei von FAT12-, FAT16-, FAT32- und NTFS-Dateisystemen in einer Zielformat um die Untersuchung zu erleichtern. Jedem Vorkommen von Schlupfspeicher werden Zeilenumbrüche vorangestellt sowie die Nummer des Clusters, in dem er aufgefunden wurde. Diese Informationen werden dann als ASCII-Text gespeichert. Specialist | Schlupfspeicher extrahieren

- **Freien Speicher extrahieren**

Durchläuft das gegenwärtig geöffnete logische Laufwerk und sammelt alle unbenutzten Cluster in einer von Ihnen anzugebenden Zielformat. Dies ist nützlich um Datenfragmente von vormals existierenden Dateien, die nicht sicher gelöscht wurden, zu untersuchen. Es werden keine Änderungen am untersuchten Laufwerk vorgenommen. Die Zielformat muss auf einem anderen Laufwerk abgelegt werden. Spezialist | Freien Speicher extrahieren.

- **Partitionsrüfen extrahieren**

Erfasst die Speicherbereiche einer physischen Festplatte, die zu keiner Partition gehören, in einer Zielformat. So kann schnell untersucht werden, ob dort etwas versteckt ist oder ob der Speicher von früheren Partitionen übrig geblieben ist. Specialist | Partitionsrüfen extrahieren.

- **Text extrahieren**

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

- **Laufwerksinhaltslisten erstellen**

Erstellt einen „Katalog“ aller existierenden und/oder noch spurenweise zu findenden gelöschten Dateien und Verzeichnisse. Dabei werden benutzerkonfigurierte Informationen wie Dateiattribute, alle verfügbaren Datums- und Zeitangaben, Größe, belegte Cluster, Hash-Werte (Prüfsumme oder Digest), alternative Datenströme (ADS, welche versteckte Daten enthalten, nur auf NTFS-Laufwerken) usw. gesammelt. Dies ist extrem nützlich, um den Inhalt eines Datenträgers systematisch zu untersuchen. Die Suche kann auch durch die Angaben in einer Maske (wie \*.jpg;\*.gif) auf Dateien eines bestimmten Typs eingeschränkt werden. Die daraus resultierende Tabelle kann von Datenbanken oder MS Excel importiert und weiterverwendet

werden. Das Sortieren nach Datum & Zeit gibt einen guten Überblick darüber, wozu ein Datenträger zu welcher Zeit benutzt wurde. Das NTFS-Attribut „verschlüsselt“ kann z.B. schnell die wichtigsten Anhaltspunkte liefern, welche Dateien interessant für eine forensische Analyse sind.

Die Laufwerksinhaltsstabelle kann auch gegen eine Hash-Datenbank mit wahlweise bekannten harmlosen oder schädlichen Dateien erzeugt werden, um solche Dateien ausdrücklich aus- bzw. einzuschließen. Unterstützte Hash-Datenbank-Formate sind NSRL RDS 2.x, ILook und HashKeeper. Während der Erzeugung einer Laufwerksinhaltsstabelle kann auch eine solche Datenbank im Format NSRL RDS 2.x erzeugt werden.

- **CD Raw-Modus**

Ermöglicht den vollen Zugriff auf CD-Daten, um Audio-CDs auszulesen und die vollen 2352-Byte Sektoren von Daten-CDs (CD-ROM und Video-CDs) einschließlich Fehlerkorrektur-Codes zu lesen.

- **Unterstützung für NTFS-Kompression**

Sie können auf Dateien, die auf der NTFS-Dateisystemebene komprimiert wurden, zugreifen, sie öffnen, wiederherstellen und untersuchen. Ihre Dekomprimierung erfolgt bei Bedarf und für den Nutzer unbemerkt.

- **Datenträger-Detailbericht**

Zeigt Informationen über den aktiven Datenträger bzw. die aktive Datei an. Diese Informationen können kopiert werden, z.B. in einen Bericht. Besonders detaillierte Informationen werden bei physischen Festplatten gefunden, zu denen Details über jede Partition und alle keiner Partition zugeordneten Speicherlücken aufgeführt werden.

- **Image als Datenträger interpretieren**

Behandelt eine geöffnete und aktive Image-Datei entweder als logisches Laufwerk oder als physischen Datenträger. Das ist nützlich, wenn Sie beispielsweise den Inhalt eines Disk-Image untersuchen möchten, einzelne Dateien aus dem Dateisystem extrahieren möchten usw., ohne das Image auf einen Datenträger zurückzuspielen. Beim Interpretieren als physischen Datenträger kann X-Ways Forensics die im Image enthaltenen Partitionen öffnen wie von einer „echten“ physischen Festplatte.

X-Ways Forensics kann sogar dateiübergreifende Images interpretieren, also Image-Dateien, die aus einzelnen Segmenten beliebiger Größe bestehen (sog. „spanned image files“). Damit X-Ways Forensics ein dateiübergreifendes Image erkennt, sollte das erste Segment einen beliebigen Namen und eine nicht-numerische Namenserverweiterung oder die Namenserverweiterung ".000" haben. Das zweite Segment muss denselben Basisdateinamen, aber die Erweiterung ".001" haben, das dritte Segment ".002" usw. Das Plattenklon-Programm X-Ways Replica für DOS ist imstande, Disk-Images in einer solchen Segmentierung zu erzeugen. Das ist nützlich, da die maximal unterstützte Dateigröße bei FAT16 und FAT32 bei 2 GB bzw. 4 GB liegt.

- **Bates-Numerierung**

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

Bezugnahme kennzeichnen.

- **Daten-Dolmetscher**

Mit diesem Werkzeug lassen sich alle Integer- und Gleitkomma-Datentypen, Datenformate, Assembler-Opcodes und andere Datentypen in beide Richtungen konvertieren. ([Details](#))

- **Datenanalyse**

Diese Funktion kann z. B. dazu eingesetzt werden, um Datenmaterial unbekannter Art zu analysieren. ([Details](#))

- **Binäre / Volltextsuche**

Mit X-Ways Forensics können Sie nach allen vorstellbaren Daten suchen, die in hexadezimaler, ASCII- oder EBCDIC-Schreibweise oder in allgemeinen Textpassagen versteckt sind. Dabei kann gewählt werden, ob X-Ways Forensics entweder bei jedem Auftreten der gesuchten Daten anhalten oder sämtliche gefundene Daten in einen Bericht schreiben soll. Dies ermöglicht eine automatisierte Suche durch große Datenbestände. Nützlich ist dies z. B. bei der Suche nach bestimmten Schlüsselwörtern bei kriminalistischen Untersuchungen. Auf Wunsch können Lesefehler ignoriert werden, dies ist gerade bei beschädigten Datenträgern sehr hilfreich. Die Suchfunktion von X-Ways Forensics durchsucht den gesamten Speicherbereich, den Schlupfspeicher sowie den nach dem Löschen wieder freigegeben Speicher.

- **Parallele Suche**

Specialist | Parallele Suche. Eine parallele Suchfunktion, die es Ihnen ermöglicht, eine praktisch unbegrenzte Anzahl an Suchbegriffen festzulegen, einen pro Zeile. Nach diesen Begriffen wird simultan gesucht und jede Fundstelle kann wahlweise im Positions-Manager oder in einer Tabulator-getrennten Textdatei ähnlich der Laufwerksinhaltstabelle gespeichert werden, die dann in MS Excel oder einer Datenbank weiter verarbeitet werden kann. X-Ways Forensics speichert den Offset jeder Fundstelle, den Suchbegriff, den Namen der Datei oder des Laufwerks, das durchsucht wurde und im Fall eines logischen Laufwerks auch die Clusterbelegung, d.h. den Namen und Pfad der Datei, die an dem betreffenden Offset gespeichert ist, falls vorhanden.

Das bedeutet, dass Sie in der Lage sind, systematisch mehrere Laufwerke und Image-Dateien in einem Durchlauf simultan nach Begriffen wie Insiderbezeichnungen für Drogen, alternative Schreibweisen, Namen bekannter Dealer, etc. zu durchsuchen. Dies wird Ihnen helfen, die Untersuchung auf eine Liste von Dateien zu beschränken.

- **Scripte**

Mit dem in X-Ways Forensics integrierten Scripttool haben Sie die Möglichkeit, Scripts individuell für Ihre Bedürfnisse zu entwickeln. So können Routineschritte, beispielsweise, wenn nach bestimmten Kennwörtern immer wieder gesucht werden muss, wenn bestimmte Cluster regelmäßig auf ein anderes Laufwerke kopiert werden sollen oder verschiedene langwierige Suchvorgänge nacheinander über Nacht durchgeführt werden sollen, automatisiert werden.

- **Positions-Manager**

Mit dem Positions-Manager können die Fundstellen von Zeichenketten oder anderen wichtigen Adressen in den untersuchten Dateien oder Festplatten als Lesezeichen gespeichert werden. Die gesammelten Lesezeichen können als HTML-Tabellen exportiert werden (z.B. um sie in MS Excel weiterzunutzen) und sind im automatisch erzeugten Fallbericht enthalten.

- **Prüfsummen, CRC16, CRC32, MD5, SHA-1, SHA-256, PSCHF**

X-Ways Forensics kann verschiedene Prüfsummen von jeder Datei, Festplatte, Partition oder beliebigen Teilen eines Datenträgers berechnen und unterstützt sogar 256-Bit-Digests. X-Ways Forensics verwendet auch den [MD5](#)-Algorithmus (128-bit), mit dem starke individuelle Einwegprüfsummen berechnet werden können (sogenannte Hash-Werte). Die Hash-Werte von bekannten Dateien (z. B. Windows-Systemdateien) können mit denen auf beschlagnahmten Computersystemen verglichen werden. Stimmen diese Hash-Werte überein, ist dies ein statistisch eindeutiges Zeichen, dass sich die Dateien auf dem beschlagnahmten System noch im Originalzustand befinden und somit auch nicht weiter untersucht werden müssen.

- **Datenrettung**

Mit seinem hochentwickelten Disk-Editor ermöglicht X-Ways Forensics nicht nur die gezielte manuelle Wiederherstellung von Dateien. X-Ways Forensics kann Dateien und sogar ganze verschachtelte Verzeichnisstrukturen auch automatisch retten. Dazu sind verschiedene Datenrettungs-Methoden integriert:

„Dateien retten nach Name“: Geben Sie einfach einen oder mehrere Dateifilter an (wie \*.gif, Meier\*.doc, etc.) und lassen Sie X-Ways Forensics den Rest erledigen. Funktioniert auf FAT12, FAT16, FAT32 und NTFS. Es können die gefundenen Dateien auch lediglich im Verzeichnisbrowser dargestellt werden, ohne tatsächlich bereits etwas wiederherzustellen.

„Dateien retten nach Typ“: X-Ways Forensics rettet alle Dateien, die an einer bestimmten Dateiheader-Signatur erkannt werden können. Unterstützte Dateitypen: jpg, png, gif, tif, bmp, dwg, psd, rtf, xml, html, eml, dbx, xls/doc, mdb, wpd, eps/ps, pdf, qdf, pwl, zip, rar, wav, avi, ram, rm, mpg, mov, asf, mid. Dies funktioniert auf praktisch allen Dateisystemen, selbst auf rohen Platten ohne funktionsfähiges Dateisystem. Die Rettung kann auf einen bestimmten Bereich eingeschränkt werden, indem man den gewünschten Block vorher auswählt. ([Details](#))

Mit dem zuvor erwähnten Verzeichnis-Browser lassen sich die aufgelisteten Dateien und Verzeichnisse bequem und selektiv wiederherstellen. ([Details](#))

- **Wiederherstellung von Partitionen / Boot Records**

Mit X-Ways Forensics können sowohl FAT12-, FAT16-, FAT32- und NTFS-Bootsektoren als auch Partitionstabellen mit maßgeschneiderten Schablonen editiert werden.

### **Preisliste:**

Basislizenz (1 benötigt): EUR 249,90

Zusatzlizenzen (jede weitere): EUR 159,90

*(Änderungen vorbehalten)*

# Die X-Ways Software Technology AG

X-Ways Software Technology AG  
Agrippastr. 37-39  
50676 Köln  
Tel.: +49-(0)221-420 486 5  
Fax: +49-(0)721-151 322 561

Web: <http://www.x-ways.net>  
Produkt-Homepage: <http://www.x-ways.net/forensics/>  
Bestellung: <http://www.x-ways.net/winhex/order-d.html>  
Support-Forum: <http://www.winhex.net>  
E-Mail: [mail@x-ways.com](mailto:mail@x-ways.com)

Die X-Ways Software Technology Aktiengesellschaft ist ein junges Unternehmen mit Sitz in Bünde in Westfalen (Amtsgericht Bad Oeynhausen HRB 7475). Operatives Zentrum ist die Zweigniederlassung in Köln. WinHex wurde erstmalig 1995 veröffentlicht. X-Ways Forensics 11.7 ist im September 2004 erschienen. X-Ways Forensics läuft auf Windows 95, 98, Me; Windows NT 4.0, Windows 2000, and Windows XP. Weitere Informationen finden sie im WinHex-Benutzerhandbuch: (<http://www.x-ways.net/winhex/winhex-d.pdf>)

Als Referenzkunden dürfen wir namentlich nennen: Siemens AG, Siemens Business Services, Siemens VDO AG, Infineon Technologies Flash GmbH & Co. KG, Toshiba Europe, Microsoft Corp., Hewlett Packard, Ericsson, National Semiconductor, Novell Inc., Commerzbank AG, DePfa Deutsche Pfandbriefbank AG, Deutsches Zentrum für Luft- und Raumfahrt, Analytik Jena AG, Ontrack Data International Inc., KPMG Forensic, Lockheed Martin, BAE Systems, TDK Corporation, Seoul Mobile Telecom, Visa International, Institut für Informatik der Technischen Universität München, Technische Versuchs- und Forschungsanstalt der Technischen Universität Wien, Oak Ridge National Laboratory in Tennessee, USA, Bundesstelle für Flugunfalluntersuchung, Zollkriminalamt Köln, Landeskriminalamt Niedersachsen, Polizei Bremen/LKA, Kriminalpolizeiinspektion Schweinfurt, Landespolizeidirektion Freiburg, Kriminalpolizei Passau, Verteidigungsministerium von Australien sowie viele weitere Regierungsbehörden, Unternehmen und Institute.

## Weitere Produkte der X-Ways AG:

WinHex – Der Kern von X-Ways Forensics	Davory – Datenrettung ganz einfach
Evidor – der elektronische Ermittler	X-Ways Replica – Datenträger klonen mit DOS
X-Ways Trace – Browser-Logdatei entschlüsseln	X-Ways Security – 100% sicheres Löschen