

X-Ways 軟件技術股份公司

X-Ways 取證/ WinHex

集成計算機取證環境。

數據恢復和 IT 安全工具。

文件、磁盤和 RAM 的十六進制編輯器。

手動的

內容

1 前言	1
性 關於 WinHex 和 X-Ways Forensics	2.1.3 同等可證類合法
型 和 X-Ways Forensics 之間的更多差異	5 X-Ways 取證入 4.1.4 WinHex
門 6 1.5	
2 技術背景	7 使用十六進制編輯
2.1 器	7 字節
2.2 序-	8
2.3 整數數據類型	8.2.4 浮點數據類
型 型	9.2.5 日期類
ASCII/IBM 機器SCII	9.2.6 ANSI
例 例	10.2.7 校驗和、散列、摘要
示 示	12.2.9 技術提示
	13
3 用戶界面	14
心 概述	14.3.1 3.2 啟動序目錄
瀏覽器 述	16.3.3.26 請對概
象 濾	18.3.3.3 過
	19
3.3.4 色譜柱和過濾器	20
3.3.5 有關時間戳列的更多信息	32.3.3.6 靈活過濾
器 按鈕	33.3.4 模式按
	34.3.5 狀態
欄 欄經	41.3.6 數據解釋
	42.3.7 職位經
理 提	43.3.8 有用的提示
示 數	46.3.10 用於各項快捷
鍵	49
4 菜單參考	52
4.1 目錄瀏覽上下文菜單	52 案例數據窗口上下文菜
4.2 單 61 數據窗口上下文菜	61 數據窗口上下文菜
4.3 單 63 文件菜	63 文件菜
4.4 單 63 編輯菜	63 編輯菜
4.5 單 65 搜索菜	65 搜索菜
導航菜單 68.4.8.查看菜單	68.4.8.查看菜單 67.4.6.4.7
..... 單 69 工具菜	69 工具菜 70 4.9 4.10 文件工
工具 單 75.4.12 選項菜 專家菜	75.4.12 選項菜 專家菜
單 單 78.4.13 窗口菜 幫助菜	78.4.13 窗口菜 幫助菜
單 79.4.15 視窗上下文菜	79.4.15 視窗上下文菜
單	80

5.1	取證特徵	80
5.2	將圖像文件解釋為磁盤	80 個案管
5.3	理	82 大型案例的多用戶協
5.4	調	84 證據對
5.5	象	88 案例日誌（活動日
	誌）	90 5.6 病例報
	告	91 5.7 報告
	表	94 5.8 查看器功
	能	100 5.9 同時搜
	索	102 5.11 遷輯搜
	表	104 5.12 搜索
	數	111 5.14 搜尋詞彙查詢統計
	表	113 5.15 事件列
	符	116 5.17 文件類型分
	類.txt	113 5.16 掛載為驅動器盤
	庫	117 5.18 哈希數據
DNA		118 5.19 光
字識別)		120 5.20 光學字符識別（圖片中的文
念		124 5.21 時區概
器		125 5.22 證據文件容
目		126 5.23 相關項
名		129 5.24 生成器簽
口		130 5.25 外部分析接
		132
6 卷快照及其細化		133
6.1	介紹	133 在卷/部門級別進行細
Tensions.化		134 6.2.6.2.1 運行
件系統數據結構搜索		134 6.2.2 特別徹底文
找		134 6.2.3 文件頭簽名查
配		136 6.2.4 逐塊散列和匹
化		136 6.3 文件級別的細
配	證	137 6.3.1 哈希值計算與匹
取		138 6.3.2 文件類型驗
索		139 6.3.3 內部元數據的提
取		139 6.3.4 檔案探
據		143 6.3.5 郵件提
像		144 6.3.6 發現嵌入式數
理		146 6.3.7 從視頻中捕捉靜止圖
檔		148 6.3.8 圖片分析與處
測		150 6.3.9 模糊文
引		152 6.3.10 加密檢
Snapshot Refinement		153 6.3.11 索
項		154 6.4 更多信息關於 Volume
		156 6.4.1 相互依賴
		157 6.4.2 注意事
		157
7 一些基本概念		159
7.1	編輯模式	159 腳
7.2	本	160 X-
7.3	Tensions API	161 磁盤編輯
7.4	器	162

7.5 內存編輯器/分析.....	163	7.6 模板編輯.....	165
8 數據恢復.....	165	使用目錄瀏覽	
8.1 器恢復文件	165	按類型/文件頭簽名搜索的	
8.2 文件恢復.....	166	文件類型定	
8.3 義.....			168 手動數據恢
8.4 復.....			172
9 選項.....	173	一般選	
9.1 項	173	目錄瀏覽	
9.2 器		181 卷快照選	
項.....	191	9.5 撤消選	186
項.....	9.6	9.4 查看器程序與畫廊選	195
項.....	9.7	安全選	195
上.....	9.8	搜索優化	198
項	203	替換選	
10 其他.....	204		
10.1 塊.....	204	10.2 修改數	
據.....		204	10.3 轉
換		205	10.4 扇區疊
加.....		206	10.5 擦除和初始
化.....	207	10.6 磁盤克	
隆.....		208	10.7 圖像和備
份		210	10.8 虛擬圖像片
段.....		215	10.9 磁盤克隆、鏡像、鏡像修復
提示.....	216	10.10 骨架圖	
像.....	217	10.11 備份管理	
器.....	12	恢復/複製命	
令.....	222	10.12 代理模	
測.....	10.13	重複文件檢	
式.....	228	14 代理模	
統.....	227	20.15 重建 RAID 系	
附錄 A :	模板定義.....	231	
明.....	232	3 正文 :高級命	231
頁眉.....	3	1 2 正文 :變量聲	
令.....	233	正文 :靈活的整數變	
量.....	235	4	
附錄 B :	腳本命令.....	236	
附錄 C :	主引導記錄.....	243	

1 前言

1.1 關於 WinHex 和 X-Ways Forensics

版權所有 © 1995-2022 Stefan Fleischmann ,X-Ways Software Technology AG 版權所有。

X-Ways Software Technology AG Carl-Diem-Str。 32 32257 Bünde 德國

網址：www.x-ways.net
訂購地址：www.x-ways.net/order.html
用戶論壇：www.winhex.net

郵箱地址：mail@x-ways.com

在巴特恩豪森 (HRB 7475) 註冊。首席執行官 :Stefan Fleischmann。董事會（主席） :M. 霍斯特邁爾。

X-Ways Software Technology AG 是一家根據德意志聯邦共和國法律成立的股份公司。WinHex 於 1995 年首次發布。本手冊由 WinHex/X-Ways Forensics 20.6 的在線幫助編譯而成，最後更新於 2022 年 7 月。

軟件可運行於 Windows 7、Windows 8/8.1/Server 2012、Windows 10/Server 2016/Server 2019、Windows 11；32 位和 64 位；標準、PE 和 FE；範圍不同。它也可能仍然可以在 Windows XP、Windows 2003 Server、Windows Vista/Server 2008 上運行，但有限制。在 Linux+Wine 下運行時也可以使用一些功能。

然而，不幸的是，一些複製保護方法（其中包括加密狗）在 Linux+Wine 下根本不起作用。

用戶界面翻譯：Sprite Guo 中文。Takao Horiuchi 和 Ichiro Sugiyama 的日語（未普遍提供）。Jérôme Broutin 的法語，由 Bernard Leprêtre 修訂。

何塞·瑪麗亞·塔加羅·馬蒂 (Jose Maria Tagarro Marti) 的西班牙語。安德里亞·吉拉爾迪尼 (Andrea Ghirardini) 的意大利語。Heyder Lino Ferreira 的巴西葡萄牙語。ProCertiv Sp. z oo (有限責任公司)。

我們要感謝萊茵蘭-普法爾茨州執法機構就 X-Ways Forensics 和 X-Ways Investigator 的開發提供了大量重要的建議。

感謝 A. Kuiper 博士提供了使用 MPlayer 處理視頻的方法。

世界各地的專業用戶包括...（此列表來自 ~18 年前）

美德聯邦執法機構、澳大利亞國防部等部委、美國國家研究所（如田納西州橡樹嶺國家實驗室）、維也納科技大學、慕尼黑科技大學（計算機科學研究所）、德國航空航天中心、德國聯邦航空事故調查局、Microsoft Corp.、Hewlett Packard、Toshiba Europe、Siemens AG、Siemens Business Services、Siemens VDO AG、Infineon Technologies Flash GmbH & Co. KG、Ontrack Data International Inc.、Deloitte & Touche、KPMG Forensic、Ernst & Young、Ericsson、National Semiconductor、Lockheed Martin、

BAE Systems、TDK Corporation、首爾移動電信、Visa International、Analytik Jena AG 以及許多其他公司和科研機構。

1.2 合法性

版權所有 © 1995-2022 Stefan Fleischmann、X-Ways Software Technology AG。未經作者事先許可，不得複製本出版物的任何部分，或將其存儲在數據庫或檢索系統中。程序或本手冊中提及的任何品牌名稱和商標均為其各自所有者的財產，通常受法律保護。

FuzZyDoc™ 是 X-Ways Software Technology AG 的商標。

本出版物旨在提供有關所涵蓋主題的準確和權威信息。但是，作者既不提供任何保證或陳述，也不對程序或手冊承擔任何責任。

許可協議

致謝

MD5 消息摘要的版權歸 RSA Data Security Inc 所有。

X-Ways Forensics 包含 Igor Pavlov 的軟件，www.7-zip.com 和 Arnaud Bouchez 的 Adler32 實現。

Outside In® Technology 版權所有 © 1991, 2019, Oracle Corp. 和/或其附屬公司。版權所有。

NEXT3® 是 CTERA Networks 的註冊商標。

FuzZyDoc™ 是 X-Ways Software Technology AG 的商標。

X-Ways Forensics 使用 ResIL，它是 DevilL 的一個分支。ResIL 受 LGPL (<http://www.gnu.org/copyleft/lesser.html>) 2.1 版管轄。源代碼可以從<http://sourceforge.net/projects/resil> 下載。

X-Ways Forensics 包含 libPFF 的非官方版本。libPFF 受 LGPL (<http://www.gnu.org/copyleft/lesser.html>) 3.0 版管轄。原始源代碼可以從<http://libpff.sourceforge.net/> 下載。

X-Ways Forensics 使用 Dokan。Dokan 受 LGPL (<http://www.gnu.org/copyleft/lesser.html>) 3.0 版管轄。源代碼可以在<https://dokan-dev.github.io/> 找到。

Windows 事件日誌 (.evtx) 查看功能基於 Andreas Schuster 的作品。

MiniZ :麻省理工學院許可證。特此免費授予任何獲得

本軟件和相關文檔文件（“軟件”）的副本，不受限制地處理本軟件，包括但不限於使用、複製、修改、合併、發布、分發、再許可和/或出售本軟件副本的權利軟件，並允許獲得軟件的人這樣做，但須滿足以下條件：上述版權聲明和本許可聲明應包含在軟件的所有副本或主要部分中。

本軟件“按原樣”提供，不提供任何明示或暗示的保證，包括但不限於對適銷性、特定用途的適用性和非侵權的保證。在任何情況下，作者或版權持有人均不對任何索賠、損害或其他責任負責，無論是在合同訴訟、侵權行為還是其他方面，由軟件或軟件的使用或其他交易引起、由軟件引起或與之相關軟件。

TinyXML：版權所有 (C) 1995-1998 Eric Young (eay@cryptsoft.com) 保留所有權利。這個包是由 Eric Young (eay@cryptsoft.com) 編寫的 SSL 實現。編寫實現是為了符合 Netscapes SSL。只要滿足以下條件，該庫可免費用於商業和非商業用途。以下條件適用於此發行版中的所有代碼，無論是 RC4、RSA、lhash、DES 等代碼；不僅僅是 SSL 代碼。此發行版中包含的 SSL 文檔受相同版權條款的約束，但所有者是 Tim Hudson (tjh@cryptsoft.com)。

版權歸 Eric Young 所有，因此代碼中的任何版權聲明都不會被刪除。如果在產品中使用此包，則應將 Eric Young 列為所用庫部分的作者。這可以在程序啟動時以文本消息的形式出現，也可以以隨包提供的文檔（在線或文本）的形式出現。如果滿足以下條件，則允許以源代碼和二進制形式重新分發和使用，無論是否進行修改：1. 源代碼的重新分發必須保留版權聲明、此條件列表和以下免責聲明。2. 二進制形式的重新分發必須在隨分發提供的文檔和/或其他材料中複制上述版權聲明、此條件列表和以下免責聲明。3. 所有提及此軟件的功能或使用的廣告材料必須顯示以下聲明：

“此產品包括由 Eric Young (eay@cryptsoft.com) 編寫的加密軟件”如果例程來自正在使用的庫與密碼無關:-)。4. 如果您從應用程序目錄（應用程序代碼）中包含任何 Windows 特定代碼（或其衍生代碼），您必須包含一個確認信息：“本產品包含由 Tim Hudson (tjh@cryptsoft.com) 編寫的軟件”。本軟件由 ERIC YOUNG 按“原樣”提供，不提供任何明示或暗示的保證，包括但不限於對適銷性和特定用途適用性的暗示保證。在任何情況下，作者或貢獻者均不對任何直接、間接、偶然、特殊、懲戒性或後果性損害（包括但不限於替代商品或服務的採購；使用、數據或利潤損失；或業務中斷）

無論如何導致和基於任何責任理論，無論是合同、嚴格責任或侵權行為（包括疏忽或其他）以任何方式因使用本軟件而引起，即使已被告知此類損害的可能性。此代碼的任何公開可用版本或衍生版本的許可和分發條款不得更改。即這段代碼

不能簡單地複制並置於另一個分發許可證下 [包括 GNU 公共許可證]。

Unicode 版權所有 2001-2004 Unicode, Inc. 免責聲明 此源代碼由 Unicode, Inc. 按原樣提供。未針對任何特定用途的適用性提出任何聲明。沒有任何明示或暗示的保證。接收方同意確定所提供的信息的適用性。如果此文件是從 Unicode, Inc. 購買的磁性或光學介質，則任何索賠的唯一補救措施是在收到後 90 天內更換有缺陷的介質。

重新分發此代碼的權利限制 Unicode, Inc. 特此授予以下權利：在創建支持 Unicode 標準的產品時自由使用此文件中提供的信息，並以任何形式複制此文件以供內部或外部分發只要此通知仍然存在。

來自 <http://zlib.net/> 的 ZLib：該軟件“按原樣”提供，沒有任何明示或暗示的保證。在任何情況下，作者均不對因使用本軟件而造成的任何損害承擔責任。任何人都可以出於任何目的（包括商業應用程序）使用本軟件，並可以自由更改和重新分發本軟件，但須遵守以下限制：1. 不得歪曲本軟件的來源；您不得聲稱您編寫了原始軟件。如果您在產品中使用此軟件，我們將不勝感激，但不是必需的。2. 更改後的源版本必須清楚地標明，不得被誤認為是原始軟件。3. 不得從任何源分發中刪除或更改此通知。

FFmpeg <https://www.ffmpeg.org/>：(http://
www.gnu.org/copyleft/lesser.html)，版本 3.0。

治理 經過 這 LGPL

1.3 許可證類型

您可以免費評估 WinHex，最多 45 天。對於常規使用和作為完整版本使用，您至少需要一個許可證。對於多個用戶同時或一個用戶同時在多台機器上使用，您將需要多個許可證。[許可協議](#)。

與評估版不同，WinHex 的完整版將保存大於 200 KB 的文件、寫入磁盤扇區、編輯虛擬內存並且不顯示評估版提醒。它將在啟動時和“關於”框中顯示其許可狀態（單擊右上角的版本號時出現的窗口）。

- 在非商業、非機構和非政府環境中，個人許可僅可用於非商業目的以優惠價格獲得。
- 專業許可證允許在任何環境（家庭、公司、組織或公共管理）中使用該軟件。專業許可證提供執行腳本的能力。
- 除了允許使用專家菜單命令、讀取文件系統 exFAT、Ext2、Ext3、Ext4、Next3®、CDFS/ISO9660、UDF 之外的專家許可證，可以突出顯示可用驅動器空間和空閒空間，啟用對 RAID 重建的支持，Windows 動態磁盤，

Linux LVM2 ,目錄瀏覽器中的更多列 ,以及反向磁盤克隆/映像 。
對 IT 安全專家特別有用 。

- WinHex Lab Edition 除了了解文件系統 HFS 、HFS+/HFSJ/HFSX 、ReiserFS 、Reiser4 、XFS 、Btrfs (支持通過 LVM2 或 RAID 設置的多個磁盤 , 但不支持 Btrfs 多設備設置) 、UFS1 、UFS2 、APFS (未加密) 和 QNX , 允許創建證據文件容器 , 並允許運行常規 X-Tensions 。
- 除上述許可外 ,X-Ways Forensics 許可證 (“取證許可證”) 允許使用強大的案例管理和報告生成功能 、內部查看器和單獨的查看器組件 、畫廊視圖 、更多卷快照優化操作 , 目錄瀏覽器中的更多列和過濾器 (並且可以更改列的順序) 、評論和報告表 。此外 , 它們還允許讀取和寫入證據文件 (.e01) , 並且可以做很多很多事情 ! 對計算機取證檢查員特別有用 。

X-Ways Investigator 是 X-Ways Forensics 的簡化版本 。它不具備 X-Ways Forensics 的所有功能 , 甚至不具備 WinHex 的所有功能 。 X-Ways Forensics 的用戶可以暫時將 X-Ways Forensics 的用戶界面縮減為 X-Ways Investigator 的用戶界面 , 以查看 X-Ways Investigator 的額外許可證是否有利於他們的組織將調查工作量分配給多個用戶 , 一些用戶他們是非技術人員 。 X-Ways Investigator 並不是真正意義上的獨立產品 。

文本顯示中同時顯示的最大字符集數也取決於許可類型 (參見查看菜單) 。可以在 <http://www.x-ways.net/winhex/comparison.html> 在線找到更完整的許可證類型比較 。請參閱 <http://www.x-ways.net/order.html> 了解如何訂購您的許可證 。謝謝你 。

1.4 WinHex 和 X-Ways Forensics 之間的更多區別

WinHex (主要可執行文件為 winhex.exe 或 winhex64.exe) 在用戶界面中始終將自己標識為 WinHex , X-Ways Forensics (主要可執行文件為 xwforensics.exe 或 xwforensics64.exe) 始終標識為 X-Ways Forensics 。然而 , 共享程序幫助和共享手冊在大多數情況下靜態引用名稱 “WinHex” , 有時引用 “X-Ways Forensics” 。

WinHex 和 X-Ways Forensics 共享相同的代碼庫 。 X-Ways Forensics 在具有專業許可證的 WinHex 上提供了許多額外的取證功能 , 但不允許編輯磁盤扇區或解釋的圖像 , 並且缺乏擦除 WinHex 已知數據的各種功能 。在 X-Ways Forensics 中 , 磁盤 、解釋圖像文件 、虛擬內存和物理 RAM 嚴格以僅查看模式 (只讀) 打開 , 以執行取證程序 , 其中任何證據都不得有絲毫改變 。 X-Ways Forensics 的這種嚴格的寫保護確保不會意外更改原始證據 , 這在法庭訴訟中可能是一個至關重要的方面 。

僅當不受嚴格的取證程序約束和 / 或需要更積極地處理磁盤或圖像時 (例如 , 您必須修復引導扇區或擦除機密或

不相關的數據)。那麼 X-Ways Forensics 的用戶將改為運行 WinHex。使用 WinHex，您可以編輯磁盤扇區並擦除整個硬盤、可用空間、空閒空間、選定文件、選定磁盤區域等。

X-Ways Forensics 的用戶可以簡單地複制他們的 xwforensics.exe 可執行文件並將副本命名為 winhex.exe（或者對於 64 位版本，複製他們的 xwforensics64.exe 可執行文件並將副本命名為 winhex64.exe）以獲取 WinHex。安裝程序會自動創建此類副本。或者您可以創建硬鏈接而不是副本（更高的酷度係數）。如果程序作為 *winhex*.exe 執行，它將在任何地方（在用戶界面、案例報告、案例日誌、圖像描述和所有屏幕截圖中）將自己標識為 WinHex，並像 WinHex 一樣行動/表現。該版本是兩全其美，具有 X-Ways Forensics 的完整取證功能集以及 WinHex 的扇區編輯和數據擦除功能。

1.5 X-Ways 取證入門

對於最新的下載說明，如果您的更新維護是最新的，您可以[在此處檢查您的許可證狀態](#)。有關安裝 WinHex 和 X-Ways Forensics 的更多信息，請參閱[此網頁](#)。

將 X-Ways Forensics 下載中的文件解壓縮到您選擇的目錄中。不需要使用安裝程序進行安裝。該程序是可移植的，也可以直接從其他計算機上的 U 盤啟動，例如您想要檢查的實時系統。同時下載查看器組件（它不包含在標準下載中，因為它很少更新）。將 64 位版本的查看器組件用於 64 位版本的 X Ways Forensics。默認情況下，查看器組件應位於子目錄 \viewer (32 位)或 \x64\viewer (64 位)中。請注意，查看器組件會在當前登錄用戶的配置文件中創建文件，這與 X-Ways Forensics 不同，因此如果您希望避免在您檢查的實時系統上創建文件，請不要讓 X-取證使用查看器組件的方式。如果您打算讓 X-Ways Forensics 從視頻中生成靜止圖像以在畫廊中查看它們，您可能還希望下載 MPlayer。較新的版本始終可以提取到較早版本的現有目錄中。您可以在以後的版本中繼續使用早期版本中的 WinHex.cfg 配置文件（但絕不能反過來）。

以下是一些幫助您入門並找到一些重要功能的說明：創建一個案例，添加一個證據對象（例如您自己的 C: 驅動器或硬盤 0，或者一個圖像文件）。在目錄樹中，您可以使用右鍵單擊在目錄瀏覽器中列出目錄的內容，包括其所有子目錄。例如，如果您右鍵單擊一個卷的根目錄，您將獲得整個卷中所有文件的列表。同時，您可以使用動態過濾器來關注基於特定文件名、特定文件類型、大小或特定時間戳等的文件，通過 Options |目錄瀏覽器。

可以在搜索 | 中找到強大的邏輯搜索功能。同時搜索。X-Ways Forensics 中更多有趣的功能可以在目錄瀏覽器的上下文菜單中找到（例如，從圖像中複製文件的能力）和專家菜單中，特別是“優化卷快照”。後者允許您自動進一步處理文件，例如探索 zip 檔案、提取電子郵件和附件、檢查圖片的數量。

膚色、檢查文檔是否加密等。

X-Ways Forensics 可以用於一千種不同的目的，因此我們認為分步說明（先單擊此處，然後單擊此處，然後查看此處）並不是解釋該軟件的正確方法。本程序幫助/用戶手冊旨在準確描述所有可用功能，並讓您創造性地組合不同的命令以實現特定目標。仍然是用戶必須進行思考，知道他/她在做什麼以及如何解釋發現的結果。

建議使用 64 位版本，尤其是在 32 位內存地址空間可能不足的情況下，處理包含數百萬文件的磁盤或圖像時，或者處理數百萬的搜索結果時，前提是您有足夠的安裝的物理內存。某些計算密集型操作（例如散列或加密）在 64 位版本中也可能更快。

2 技術背景

2.1 使用十六進制編輯器

十六進制編輯器能夠完整顯示每種文件類型的內容。與文本編輯器不同，十六進制編輯器甚至可以顯示控制代碼（例如換行符和回車符）和可執行代碼，使用基於十六進制系統的兩位數字。

將一個字節視為一個 8 位序列。每個位要么是 0 要么是 1，它假定兩種可能狀態之一。因此一個字節可以有 $2 \cdot 2 = 2^8 = 256$ 個不同值之一。

由於 256 是 16 的平方，一個字節值可以定義為一個基於十六進制的兩位數字，其中每個數字代表一個字節的四分之一或半字節，即 4 位。十六進制使用的十六位數字是 0-9，AF。

您可以通過在十六進制模式下更改這些數字來更改字節的值。也可以輸入由字符集分配給特定字節值的字符（cf.

輸入字符）。允許使用各種字符（例如字母和標點符號）。

示例：一個十進制值為 65 的字節，在十六進制 ($4 \cdot 16 + 1 = 65$) 中顯示為 41，在文本模式中顯示為字母 A。ASCII 字符集定義大寫字母 A 的十進制值為 65。

在編輯某種類型的文件（例如可執行文件）時，重要的是不要更改文件大小。移動可執行代碼的地址和包含的數據會導致嚴重損壞此類文件。請注意，更改文件內容通常可能是相應應用程序行為異常的原因。編輯文件中的文本段落是非常安全的。無論如何，建議在編輯之前創建備份文件。

“組合搜索”命令是專門為編輯電腦遊戲創建的文件以保存遊戲狀態而設計的。如果您知道其中兩個文件中某個變量的值，您可以

找出偏移量，即保存此數據的位置。示例：如果兩個文件包含您有 5 個 resp 的信息。7 點/生命/...，同時搜索第一個文件中的十六進制值 05 和第二個文件中的 07。

2.2 字節順序

微處理器在最低有效字節的位置上有所不同。Intel®、MIPS®、National Semiconductor 和 VAX 處理器的最低有效字節在前。多字節值存儲在內存中，從最低字節（“小端”）到最高字節。例如，十六進制數 12345678 存儲為 78 56 34 12。這稱為小端格式。

Motorola 和 Sparc 處理器將最低有效字節放在最後。多字節值從最高字節（“大端”）到最低字節存儲在內存中。例如，十六進制數 12345678 存儲為 12 34 56 78。這稱為大端格式。

2.3 整數數據類型

格式/類型	範圍	例子
有符號 8 位	-128...127	FF = -1
無符號 8 位 有符號 16 位 無符號	0...255	ff = 255 00 80 =
16 位 有符號 24 位 無符號 24 位	-32,768...32,767	-32,768 00 80 = 32,768 00 00
有符號 32 位 無符號 32 位 有符號	0...65,535	00 80 = -8,388,608 00 00 00 80
64 位	-8,388,608...8,388,607	= 8,388,608 00 00 00 00 00 80 =
	0...16,777,215	-2,147,483,648 00 00 00 00 00 00 00
	-2,147,483,648...2,147,483,647	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0...4,294,967,295 -263 (\approx -9 · 1018)	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	...263-1 (\approx 9 · 1018)	000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 乘

除非另有說明，否則多字節數字以小端格式存儲，這意味著數字的第一個字節最不重要，最後一個字節最重要。這是運行 Microsoft Windows 的計算機的通用格式。按照小端模式，十六進制值 10 27 可以解釋為十六進制數 2710（十進制：10,000）。

數據解釋器能夠將數據解釋為上述所有整數類型，以及無符號 48 位整數。

2.4 浮點數據類型

類型	範圍	精度 [位數]	字節
3.438 浮動 (單)	$\pm 3.4 \times 10^{-38} \text{ 到 } \pm 3.4 \times 10^{38}$	7-8	4
雙 (雙)	$5.0 \times 10^{-324} \text{ 到 } 1.7 \times 10^{308}$	11-12	6
		15-16	8
長雙 (擴展)	$\pm 3.4 \times 10^{-4932} \text{ 到 } \pm 1.1 \times 10^{14932}$	19-20	10

類型名稱源自 C 編程語言。相應的 Pascal 名稱在括號中指定。 Real 類型僅存在於 Pascal 中。數據解釋器能夠將編輯器窗口中的十六進制值轉換為所有四種類型的浮點數，反之亦然。

反之亦然。

在計算機中，浮點數 F 由尾數 M 和指數 E 表示，其中 $M \times 2^E = F$ 。M 和 E 本身都是有符號整數值。四種數據類型的取值範圍（即為指數保留的位數）和精度（即為尾數保留的位數）不同。

在基於 Intel® 的系統上，浮點數的計算由數學協處理器執行，而主處理器則處於等待狀態。 Intel® 80x87 使用 80 位精度進行計算，而 RISC 處理器通常使用 64 位精度。

2.5 日期類型

Data Interpreter 支持以下日期格式：

- MS-DOS 日期和時間（4 字節）

下字確定時間，上字確定日期。由多個 DOS 函數調用、FAT 文件系統和許多系統實用程序（例如文件歸檔器）使用。

位	內容
0-4	秒除以 25-10 分鐘 (0-59)
5-8	
9-10	11-15 小時 (24 小時制為 0-23)
11-12	16-20 月中的第幾天 (1-31)
13-14	21-24 月 (1 = 一月，2 = 二月，依此類推)
15-16	25-31 年從 1980 年偏移

- Win32 文件時間（8 字節）

FILETIME 結構是一個 64 位整數值，表示自 1601 年 1 月 1 日以來的 100 納秒間隔數。由 Win32 API 使用。

- OLE 2.0 日期和時間 (8 字節)

一個浮點值 (更準確地說 :雙精度值) ,其整數部分確定自 1899 年 12 月 30 日以來經過的天數 。小數部分被解釋為白天時間 (例如 1/4 = 6:00 am) 。這是 OLE 2.0 標準日期類型 ,例如 ,它被 MS Excel 使用。 ICQ 7.0 在聊天消息中使用大端 OLE 2.0 時間戳

- ANSI SQL 日期和時間 (8 字節)

兩個連續的 32 位整數值 。第一個確定自 1858 年 11 月 17 日以來的天數 。第二個是自午夜以來 100 微秒間隔的數量 。

這是 ANSI SQL 標準 ,用於許多數據庫 (例如 InterBase 6.0) 。

- UNIX、C、FORTRAN 日期和時間 (4 個字節)

一個 32 位整數值 ,它確定自 1970 年 1 月 1 日以來的秒數 。自 80 年代以來 ,此數據類型被用於 UNIX、C 和 C++ (“time_t”) 以及 FORTRAN 程序 。

偶爾定義為自 1970 年 1 月 1 日以來的分鐘數 。數據解釋器選項允許您在兩種子類型之間切換 。

- Macintosh HFS+ 日期和時間 (4 字節)

一個 32 位整數值 ,用於確定自格林威治標準時間 1904 年 1 月 1 日 (HFS :當地時間) 以來的秒數 。可表示的最大日期是格林威治標準時間 2040 年 2 月 6 日 06:28:15 。日期值不考慮閏秒 。他們確實在每一年都包含了一個可以被 4 整除的閏日 。

- Java 日期和時間 (8 字節)

一個 64 位整數值 ,指定自 1970 年 1 月 1 日以來的毫秒數 。通常以 big endian 存儲 ,這是 Java 中的典型字節順序 ,但在 BlackBerry 內存中以 little endian 存儲 。

- Mac 絶對時間 ,又名 Mac 紀元時間 (4 字節)

一個 32 位整數值 ,用於確定自 2001 年 1 月 1 日以來的秒數 。

2.6 ANSI ASCII/IBM ASCII

ANSI ASCII 是 WinHex 中使用的名稱 ,用於擴展非 Unicode Windows 應用程序中使用的 ASCII 字符集 。它被微軟以美國國家標準協會的名字命名為 ANSI ,但該協會並未對其進行定義 。存在幾種不同的區域變體 ,其中一種在 Windows 中處於活動狀態 ,通常在使用西歐語言的國家/地區使用代碼頁 1252 。 MS-DOS 和 Windows 命令提示窗口使用 WinHex 中所謂的 IBM ASCII 字符集 (在別處也稱為 OEM 或 DOS 字符集) 。所有這些 7 位 ASCII 字符集的 8 位擴展在字符上都不同

值大於 127。例如，如果您使用 Windows 記事本以 ANSI 編碼存儲純文本文件，然後在命令提示符窗口中使用 type 命令查看它，則德國變音符號等特殊字符將無法正確顯示。一些區域性 ANSI 代碼頁是雙字節代碼頁，即對某些字符甚至使用 2 個字節，而不是每個字符僅使用 1 個字節。

在“查看”菜單中為文本列選擇字符集，或單擊文本列的頂部，其中顯示活動代碼頁/字符集的名稱以更改設置。使用“編輯”菜單的“轉換”命令將文本文件從一種字符集轉換為另一種字符集。

前 32 個 ASCII 值不定義可打印字符，而是控制代碼：

十六進制控制代碼	十六進制控制代碼
00 空	10 數據鏈轉義
01 標題開始	11 設備控制 1
02 文本開始	12 設備控制 2
03 正文結束	13 設備控制 3
04 傳輸結束	14 設備控制 4
05 詢/債	15 否定確認
06 確認	16 同步空閒
07 貝爾	17 傳輸塊結束
08 退格鍵	18 取消
09 水平製表符	19 媒體結束
0A 換行	1A 替補
0B 垂直製表符	1B 逃牛
0C 換頁	1C 文件分隔符
0D 回車	—維組分隔符
0E 移出	1E 記錄分隔符
0F 移入	1F 單元分離器

2.7 校驗和、散列、摘要

校驗和是用於驗證數據真實性的特徵數。兩個校驗和相等的文件很可能本身相等（逐字節）。在可能不準確的傳輸之前和之後計算和比較文件的校驗和可能會發現傳輸錯誤。未受影響的校驗和表示文件（很可能）仍然相同。但是，可以故意以其校驗和不受影響的方式對文件進行操作。在這種情況下，使用摘要代替校驗和，要檢測對原始數據的惡意（即不僅僅是隨機）修改。

在 WinHex 中，可以使用工具菜單中的命令計算校驗和。

標準校驗和通過將數據解釋為整數序列來計算為總和，在 8 位、16 位、32 位或 64 位累加器上計算。確切的操作模式取決於選項 | 中的設置。安全。CRC（循環冗餘碼）基於更複雜的算法，更安全。

示例：如果傳輸以這樣的方式更改文件的兩個字節，即修改是

反補貼（例如字節一+1，字節二-1），標準校驗和不受影響，而 CRC 變更。

所謂摘要，類似於校驗和，是用來驗證數據真實性的特徵碼。但摘要不止於此：摘要是一種強大的單向哈希碼。

以其校驗和不受影響的方式操作任何數據在計算上是可行的。在這種情況下驗證校驗和會導致假設數據沒有被更改，儘管它已經更改。因此，如果要檢測對原始數據的惡意（即不僅僅是隨機）修改，則使用摘要而不是校驗和。找到對應於給定摘要的任何數據在計算上是不可行的。找到對應於同一個摘要的兩條數據在計算上甚至是不可行的。

當然，使用摘要時也可以檢測到隨機修改，例如由不準確的傳輸引起的修改，但是校驗和就足夠了並且可以更好地用於此目的，因為它們可以更快地計算出來。

WinHex 可以計算以下摘要：MD4、MD5、SHA-1、SHA-256、RipeMD-128、RipeMD-160、Tiger128、Tiger160、Tiger192 以及 TTH（Tiger Tree Hash）和 ed2k（僅限專家和取證許可）。

2.8 屬性圖例

A :待存檔 R :只讀

H :隱藏 S :系統 X :
未編入索引 P :NTFS

重新分析點 O :離線
T :臨時 I :具有對象

ID C :在文件系統級別壓縮
c :在存檔中壓縮 E :加密在
文件系統級別 e: 在存檔中
加密 e!: 文件類型特定加
密/DRM e?: 高熵，可能完全加密 (Res):
HFS+ 資源 (\$EFS): NTFS 加密元數據
(INDX): NTFS 非目錄索引屬性(ADS)：
NTFS 備用數據流 (SC) :在卷影副本中
找到 (SUID) :設置用戶 ID (SGID) :設置組 ID

文件模式 :=

符號鏈接 c=字符

設備 b=塊設備 s=套

接字 p=管道

權限 :所有者讀/

寫/執行組讀/寫/執行其他讀/寫/

執行

2.9 技術提示

- 技術規格

支持的磁盤和文件大小 :	至	
少 120 TB 卷快照中支持的文件大小 :	120
TB-1 一般最大扇區數 :	
240-1 一般最大簇數 :	
232-1 每個散列的最大散列值數數據庫 :	
231-1 PhotoDNA 數據庫中值的最大數量 (64 位) :	~ 5880 萬個文	
件系統支持的捲 > 232 個扇區 :	NTFS 、Ext* 、XFS 、Reiser* 文件系統	
支持的捲 > 232 個簇 :	NTFS , Ext4, XFS Windows 中編號	
的可尋址物理存儲設備 :	0-127 同時打開解釋磁	
盤映像的最大數量	100 同時打開的分區和解釋的捲	
圖像的最大數量	256 在一個案例中的最大搜索詞		
數	8191 最大數據窗口	
數 :	1000 同時程序實例的	
最大數量 :	99 可逆鍵盤輸入的最	
大數量 :	65535 加密深	
度 :	128-256	
位偏移介紹 :	十六進制 / 十進制	

- 在大多數情況下，進度顯示顯示操作的完成百分比。但是，在搜索和替換操作期間，它指示當前文件或磁盤中的相對位置。
- 您指定用於加密/解密的密鑰不會保存在硬盤上。如果啟用了相應的安全選項，只要 WinHex 正在運行，密鑰就會以加密狀態存儲在 RAM 中。
- 搜索和替換操作通常在打開區分大小寫和沒有啟用通配符。
- 當使用激活的“計數出現次數”選項進行搜索時，或者在沒有提示的情況下進行替換時，對於搜索算法，通常有兩種行為方式

已經發現，在某些情況下可能會有不同的結果。以下示例對此進行了解釋：

在單詞“banana”中搜索字母ana。已在第二個字符處找到第一次出現。第一種選擇：算法在第三個字符處繼續搜索。所以在第四個字符處再次找到ana。第二種選擇：跳過單詞“banana”中的三個字母ana。剩餘的

字母na不再包含ana。

WinHex以第二種方式編程，因為這在計算或替換出現次數時會提供更合理的結果。但是，如果您使用F3鍵繼續搜索或選擇替換選項“找到時提示”，算法將遵循第一個範例。

特殊性能增強

在處理某些壓縮和稀疏的.e01證據文件時，文件頭簽名搜索、逐塊哈希匹配、FILE記錄搜索、丟失分區搜索和物理同步搜索都是稀疏感知操作。這意味著原始硬盤上從未寫入的區域因此仍然被清零，或者原始硬盤上已被擦除的區域或清理圖像中有意省略的區域被跳過並且幾乎不需要時間，因為它們的數據既不必被讀取、解壓縮或進一步處理（針對塊哈希數據庫進行搜索/哈希/匹配）。

對於由X-Ways Forensics和X Ways Imager創建的塊大小為32 KB、128 KB或512 KB的.e01證據文件，稀疏感知處於活動狀態。也可能適用於由第3方軟件創建的圖像，具體取決於設置和內部佈局。Windows動態磁盤映像、LVM2磁盤映像以及基於.e01證據文件重建的RAID上的操作不是稀疏感知的。

存儲在NTFS文件系統中的文件中的邏輯搜索和索引在.e01證據文件級別也是稀疏感知的，並且通常是虛擬“可用空間”文件中的邏輯搜索。

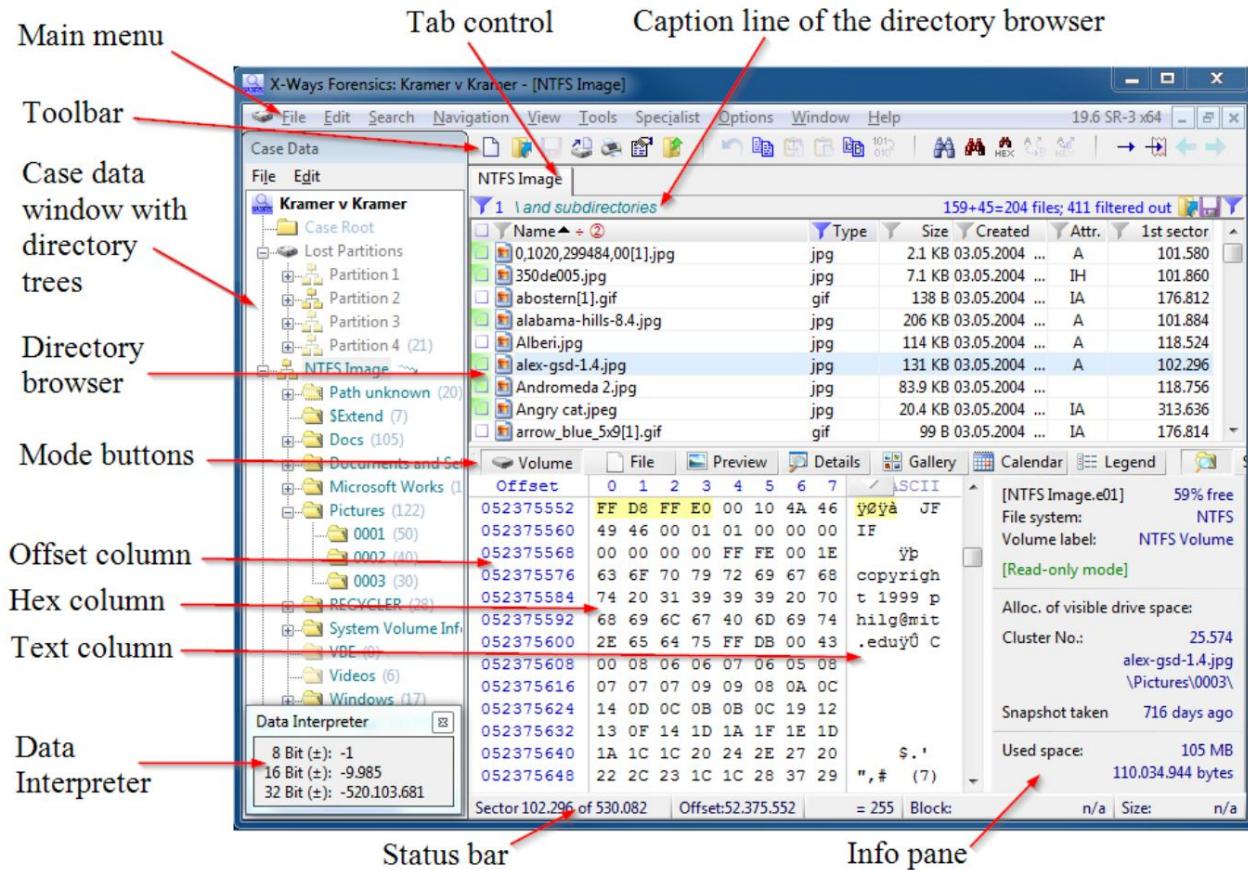
NTFS、Ext*、XFS和UFS文件系統中的邏輯搜索和索引在文件系統級別是稀疏感知的。這意味著不會在稀疏文件中的大面積稀疏區域上浪費時間。這些區域將被忽略，無論證據對像是.e01證據文件、原始圖像、RAID還是實際磁盤。

3 用戶界面

3.1 概述

要熟悉用戶界面各種元素的名稱，請參閱

到這個截圖：



3.2 啟動中心

所謂的 Start Center 是一個對話窗口，它可以在啟動時選擇性地顯示，並作為一個簡化的控制面板來開始您的工作。它允許快速打開文件、磁盤、內存模塊和文件夾以及多達 255 個最近編輯的文檔（默認情況下為 16 個，左側列表）。這些可能是文件、文件夾、邏輯驅動器或物理磁盤。再次打開時，WinHex 恢復每個文檔的最後一個光標位置、滾動位置和塊（如果已定義），除非相應的選項被禁用。

從啟動中心，您還可以訪問項目和案例（右側頂部列表）。一個項目由一個或多個要編輯的文檔（文件或磁盤）組成。它會記住編輯位置、窗口大小和位置以及一些顯示選項。通過將窗口排列保存為項目，您只需單擊一下，就可以繼續在您離開它們的地方處理多個文檔。這對於重複性任務特別有用。加載項目時，所有當前打開的窗口都會首先自動關閉。

此外，WinHex 會自動將 WinHex 會話結束時的窗口排列保存為一個項目，並可以在下次啟動時重新創建它。每個項目都存儲在一個 .prj 文件中。它可以直接在啟動中心（上下文菜單或 DELETE/F2 鍵）中刪除或重命名。

最後一點，啟動中心是管理腳本的地方。您可以使用上下文菜單檢查、編輯、創建、重命名和刪除腳本。要執行腳本，請雙擊它或單擊它並單擊確定按鈕。

3.3 目錄瀏覽器

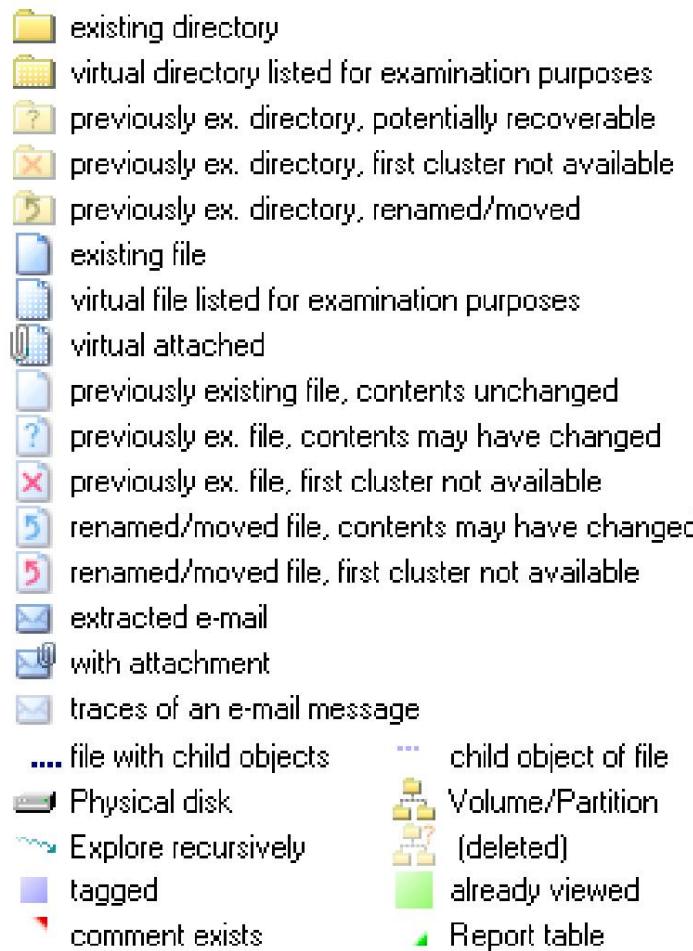
3.3.1 一般說明

WinHex 和 X-Ways Forensics 中最重要的用戶界面元素可能是所謂的目錄瀏覽器，它類似於 Windows 資源管理器的右側列表。它的主要任務是顯示（並與之交互）卷快照。完整的功能只有在獲得取證許可後才能使用。默認情況下，目錄瀏覽器首先列出目錄，然後是文件。

壓縮文件以藍色顯示，加密文件以綠色顯示。右鍵單擊目錄瀏覽器中的任何項目會彈出一個上下文菜單，其中包含用於打開文件或目錄、瀏覽目錄、定位磁盤上文件或目錄的開頭、定位相應的目錄條目 (FAT) 或文件記錄的命令(NTFS)，在單獨的窗口中列出分配的簇，等等。

從一個目錄導航到另一個目錄、瀏覽包含子對象的文件（例如帶有附件的電子郵件消息）、導航到子對象的父對象、激活或停用過濾器、嘗試不同的排序標準等時，請注意您可以使用“位置”菜單中的“後退”命令或工具欄中的“後退”按鈕輕鬆返回到上一個視圖。

這些圖標直接在程序中的圖例中進行了解釋（僅限取證許可）。已刪除的文件和目錄在目錄瀏覽器中以較淺的圖標表示。帶有藍色問號的圖標表示原始文件或目錄內容可能仍然可用。WinHex 知道的已刪除對像不再可訪問（因為它們的第一個簇已被重新分配，因為它是未知的，或者因為它們的大小為 0 字節）用紅色劃掉的圖標。FAT 卷（僅具有專家或取證許可）和（在優化卷快照後）NTFS 卷上帶有箭頭的圖標顯示重命名和移動的文件及其原始名稱/在其先前目錄中。在 Reiser4 上，這些文件是在它們原來的目錄中以當前名稱移動的文件。藍色箭頭表示文件的內容可用（儘管這些內容並不是文件重命名或移動之前的具體內容）。紅色箭頭表示沒有內容可用。



在目錄瀏覽器的標題行中，您會在左側看到探索路徑（在遞歸探索的情況下，斜體和綠松石色）。單擊當前路徑的任何組件時，現在將直接導航到您單擊其名稱的目錄（或具有子對象的文件）。在右側，您可以看到列出的文件和目錄的數量（通常是現有對象的單獨數字 + 以前存在的對象 + 虛擬對象）。此外，如果有標記的文件，則會指示列出的標記文件的數量。活動過濾器的數量也會顯示在左側藍色過濾器符號的旁邊。基於列和與列無關的活動過濾器分別計算。這很有用，因為對於當前在目錄瀏覽器中不可見的列，可能有基於列的過濾器處於活動狀態，並且與列無關的過濾器處於活動狀態可能只有在目錄瀏覽器選項對話框中檢查時才會顯示出來。

目錄瀏覽器可以按升序或降序對文件和目錄進行排序，並且仍然以較淺的箭頭顯示前兩個排序標準。例如，如果您先單擊文件名列，然後單擊文件擴展名列，則具有相同擴展名的文件在內部仍會按名稱排序。要取消定義二級和三級排序標準，請在單擊列標題時按住 Shift 鍵以確定一級排序標準。

在內部，這會選擇內部 ID 作為次要排序標準。這是為了確保在同時按其他排序標準排序後，對於主要排序標準具有相同數據的項目的順序仍然定義明確且可重現。無論您如何排序，卷或磁盤級別的虛擬文件（涵蓋可用空間、卷鬆弛、未分區空間等的文件）始終列在底部，因為它們更好地處理

與普通文件分開。

作為主要排序標準的列也是“鍵入時跳轉”的目標。

也就是說，當目錄瀏覽器具有焦點時，您可以鍵入要查找的條目的第一個字符或前幾個字符，以自動導航並選擇列表中的第一個或下一個匹配項，從當前位置開始。例如，如果目錄瀏覽器按類型列排序，如果您希望在列表中查找第一個 zip 文件，請鍵入“z”。但是，如果列出了另一個文件，其類型以“z”開頭，按字母順序在“zip”之前，例如

“zac”，則鍵入下一個字符（在功能超時之前忘記您擁有的“z”已經輸入），在本例中為“i”，直到找到您要查找的內容或不再發生任何事情（如果沒有匹配項）。匹配發生在一個循環中。這意味著即使當前位置顯示的是 zip 文件，您也可以鍵入任何前面的字母以再次跳轉到從頂部開始的第一個匹配項目，例如“d”表示.docx。如果您要查找.docx 文件，但找到一大群.doc 文件，那麼您需要鍵入所有四個字符的docx，因為只有“x”將docx 與doc 區分開來。

3.3.2 虛擬對象

當發現孤立的對象時，例如已被刪除且其原始路徑無法由程序確定的文件，或者通常當原始路徑對程序未知時，此類對象將列在特殊的虛擬目錄“路徑未知”中。

使用專家或取證許可，根目錄中有虛擬文件，可讓您方便地尋址卷中的特殊區域。這些總是分組在列表的底部：

文件系統區域：文件系統本身為內部目的而聲明的保留扇區和/或簇。

可用空間：文件系統標記為未使用的集群。取決於卷快照選項。

空閒空間：卷中 WinHex 不知道其用途的區域，包括文件系統標記為正在使用的簇，但無法確定其確切分配。如果文件系統丟失了對它們的跟蹤，即忘記了這些簇實際上可用於重新分配，則可能是這種情況。通常沒有閒置空間。空閒空間的大小和第一個空閒簇的數量僅在需要時確定（例如，當您第一次單擊“空閒空間”文件時），因為取決於簇的數量，這是一個潛在的耗時操作。

Volume slack：文件系統未使用的分區末尾的扇區，因為它們不會添加到另一個集群。

間接塊（Ext2、Ext3、UFS）：包含塊號的特殊塊。不是“文件系統區域”的一部分。

未註釋的屬性簇 (NTFS) :包含 X-Ways Forensics 未單獨處理的非常駐屬性的簇。不是“文件系統區域”的一部分。

.journal (ReiserFS) :形成固定日誌區域的塊。在 Ext3 和 HFS+ 上，這不被視為虛擬文件，因為它是由文件系統本身在專用記錄中定義的。

3.3.3 過濾

您可以根據標準（列）激活過濾器，例如文件名、描述、文件類型類別、屬性或哈希集。每當活動過濾器實際過濾掉目錄瀏覽器中的文件或目錄時，目錄瀏覽器的標題行中都會用藍色過濾器圖標標記，您將被告知列表中究竟遺漏了多少項目。您還可以選擇通過單擊目錄瀏覽器標題行右側的“打開文件” / “保存文件”圖標，將過濾器和排序設置存儲在單獨的文件中，然後再次加載它們任何時候。此類文件的擴展名為“.settings”。請注意，不保證不同版本的軟件可以加載彼此的設置。

您可以選擇同時加載多個.settings 文件，每個文件都可以使用不同的過濾器（在內部與 AND 或 OR 組合）針對不同的文件，並且所有結果文件都將添加到單個報告表中。這允許複雜的嵌套過濾條件，例如：僅當包含在路徑 X 中的類型 A 文件加上類型 B 文件（如果未刪除）加上名稱包含單詞 Y 或 Z 且具有系統屬性等的文件等。過濾器對於生成的報告表是自動激活的。

每當一個或多個過濾器處於活動狀態且實際過濾掉當前顯示的目錄瀏覽器中的項目時，目錄瀏覽器的標題行中就會出現兩個藍色過濾器符號。他們指出，由於活動文件，您當前的視圖不完整，並且他們還允許您通過單擊鼠標來停用所有過濾器，以確保您在不再需要過濾器時不會丟失任何文件。您可以通過在按住 Shift 鍵的同時單擊列標題的過濾器符號來單獨激活或停用基於列的過濾器。在這種情況下，相應過濾器的選項保持不變。

當從父文件導航到子文件或從父文件導航到子文件時，過濾器被賦予了一些“智能”，以便過濾器“知道”何時是關閉的好時機。

例如： - 如果您

使用過濾器以遞歸方式關注所有提取的電子郵件，然後雙擊單個電子郵件以在目錄瀏覽器中查看其附件，過濾器將自動停用，這樣您就可以真正看到這些附件。只需單擊“後退”按鈕即可返回到之前的探索點並恢復之前的過濾器設置和上次選擇，這樣您就可以輕鬆地繼續查看下一封電子郵件！

- 如果您正在使用過濾器來關注視頻或文檔，然後雙擊視頻或文檔以分別查看為該視頻導出的視頻靜止圖像或該文檔中的嵌入圖片，則過濾器會自動停用，也。

- 當您僅在圖庫中查看視頻靜止圖像時，您使用退格鍵或“查找父對象”菜單命令導航至該靜止圖像所屬的視頻（例如，為了

播放該視頻），然後將關閉任何活動過濾器，以便實際列出視頻。

只需單擊“後退”按鈕即可返回到之前的靜止圖像概覽，再次啟用之前的過濾器，並恢復上次選擇的項目，以便您可以輕鬆地繼續下一個靜止圖像！

- 這在系統地查看電子郵件附件時類似地工作。如果偶爾對於相關附件，您希望查看包含的電子郵件消息（例如打印它或將其包含在報告中），然後返回到附件列表。

3.3.4 列和過濾器

大多數過濾器和許多列僅適用於更高級別的許可證類型，標有例如 [為了]。

姓名 列出的文件或目錄的名稱以及（僅具有取證許可證，僅適用於目錄和具有子對象的文件）在不同顏色的括號中（可選）卷快照中包含的文件總數。允許基於一個或多個文件名掩碼進行過濾，每行一個。如果您有相關文件名或關鍵字的列表並且想快速找出是否存在具有此類名稱的文件，則此過濾器很有用。

有兩種不同的方法可以使用名稱過濾器。第一種方法是將某些表達式與全名進行匹配。表達式可能包含星號（通配符），例如 * .jpg。如果它們位於掩碼的開頭和結尾，則每個掩碼最多允許使用兩個星號。您可以使用以冒號（:）開頭的文件掩碼來排除文件。示例：名稱以字母“A”開頭但不包含“花園”一詞的所有文件：一行為 A*，另一行為：*garden*。當使用多個正文件掩碼表達式時，它們與邏輯 OR 組合，負表達式（:）與邏輯 AND 組合。

如果“文件名中的子字符串搜索”選項處於活動狀態，則上述所有規則均不適用。取而代之的是，在文件名中運行搜索以查找指定的字符或可選的正則表達式。例如，只需鍵入“invoice”即可查找其文件名包含單詞 invoice 而非“*invoice*”的文件。有關正則表達式的解釋，請參閱搜索選項。錨 \$ 在這種情況下不起作用。

可以粘貼到名稱過濾器中的文本數量已擴展到 200 萬個字符。這並不意味著 X-Ways Forensics 可以有效地使用具有數萬個或更多字符的過濾器。如有疑問，請使用“匹配全名”選項，而不是子字符串搜索，以獲得更好的性能。

如果在元數據提取期間在 Windows 回收站或 iPhone 備份或某些其他文件中找到文件的原始名稱，則該名稱將顯示在名稱列中，當前唯一名稱位於方括號中。當前的唯一名稱現在也顯示在案例報告中的方括號中。這兩個名稱都是名稱過濾器的目標。

如果您在名稱列單元格的右下角發現一些小三角形，

這些提醒您存在相應文件的報告表關聯。灰色是指自動生成的報表，綠色是指手動創建（用戶創建）的報表。

名稱列的標題允許通過單擊鼠標快速標記或取消標記所有列出的項目。它還指示在列出的項目中是否有任何標記或未標記的項目。

存在的

顯示文件是否是現有文件或現有文件的子對象（根據其參考點存在，例如文件系統），帶有復選標記或數學符號或自然語言，具體取決於表示法選項。第三種狀態是“虛擬”。要過濾存在狀態，請使用描述過濾器。請記住，您可以使用目錄瀏覽器選項按存在狀態對文件進行分組，或者您可以按此列排序。

描述

項目的文本描述。顯示與名稱欄中的圖標類似的屬性，例如項目是文件還是目錄或提取的電子郵件或視頻靜止等，存在/刪除/虛擬/雕刻狀態，以及卷快照中的狀態（例如已標記、已查看）。列中包含的文本可以在符號選項中自定義（通過常規選項）。Description 列的設置是 Notation Options 的一部分，這意味著您可以有兩種不同的設置，一種通常用於目錄瀏覽器，另一種專門用於 Export List 命令。這可能很有用，因為在導出的列表中，沒有圖標可以幫助您區分某些對像類型及其刪除狀態，這與目錄瀏覽器不同。

此列還允許按所涵蓋的屬性進行篩選或排序，這使得描述篩選器成為最重要的篩選器之一。例如，您可以過濾掉：

- 現有文件（如果您只對以前存在的文件感興趣，則很有用
[可以駐留在現有目錄中]）
- 以前存在的文件和目錄。 · 標記的文件和目錄。 ·
半標記文件和目錄（包含至少 1 個標記和至少 1 個
未標記的文件）。
- 未標記的文件和目錄。 · 標記為已查看
的文件。 · 未標記為已查看的文件。 · 排除的文件和
目錄（在卷快照中標記為排除）。 · 未排除的文件和目錄。

通過右鍵單擊目錄瀏覽器的標題行，可以通過快捷方式快速進入過濾器對話框。即使 Description 列不可見，這仍然有效。（如果您依靠圖標來區分不同種類的項目，您可能不需要目錄瀏覽器中的描述列。）代表描述列過濾器的漏斗符號有四種可能的顏色：1) 不活動時為灰色，如通常。2) 灰色有非常非常淺的藍色傾向，幾乎與灰色沒有區別，當過濾器在理論上打開時，但只有排除的文件會被過濾掉，但實際上沒有排除的文件被過濾掉。

目前。3) 藍灰色，當過濾器只過濾掉被排除的文件，而這些文件實際上已經被過濾掉了。4) 普通藍色，如果 Description 過濾器處於活動狀態並且不僅關注排除的文件，還會根據其他屬性過濾掉文件，以引起注意。引入這種柔和的配色方案是因為許多用戶認為排除的文件被過濾掉是相當“正常的”，因為他們排除它們的目的是不再看到它們，因此他們可能不希望被刺眼的藍色提醒顏色。

視頻中靜止圖像的過濾器有一個特殊選項，允許還列出相應的視頻，直接在其靜止圖像之前。這樣很容易看出哪些靜止圖像屬於哪個視頻，您可以對視頻發表評論或將視頻添加到報告表中，而無需來回導航，也無需使用稍微不太直觀的方式將報告表關聯應用到您看不到的項目（使用“父文件”選項）。如果您在圖庫選項中禁用輔助縮略圖，則表示視頻的圖塊可能會充當圖庫中的視覺分隔符，以便您可以輕鬆查看下一個視頻的靜止圖像的開始位置。

過濾器還允許關注一般的雕刻文件，特別是在扇區邊界對齊或不對齊的雕刻文件，例如在字節級別運行文件頭簽名搜索後，刪除垃圾文件，這些文件更在未對齊的文件中頻繁出現。您還可以專注於從中提取文本以進行邏輯搜索（通過 OCR 或解碼）的文件，具有一定的最小字符數（例如 5 或 10，最多 255），例如避免圖片中有幾個字符只是錯誤地被識別，即實際上不包含文本的圖片。

一個特殊的過濾器設置可用，使您可以專注於創建日期晚於修改日期的文件，即顯然被複製並以這種方式獲得新創建日期的文件。Notation 選項允許用“已複制”一詞標記所有此類文件。該詞的存在可用於條件單元格著色，以便您快速查看哪些文件可能是原始文件以及哪些文件是複制的。請注意，搜索“複製”一詞是特定於語言的（以防您與其他國家/地區的用戶共享您的條件單元格著色設置）。

分機。

文件擴展名。最後一個點之後的文件名部分（如果有的話），除非最後一個點是第一個字符（在 Unix/Linux 世界中並不少見）。

類型
[輸入，
為了]

文件類型。如果沒有特別檢查文件的標頭簽名（請參閱 Refine Volume Snapshot），這只是文件擴展名的重複，並以灰色顯示。否則，如果文件簽名驗證揭示了文件的真實性質，則將輸出該類型的典型擴展名。如果該擴展名仍與文件的實際擴展名相同，則該擴展名將顯示為黑色，如果實際擴展名與文件類型不匹配，則將顯示為藍色。可以基於此列激活一個方便的過濾器。在過濾器對話框中，您可以選擇單個文件類型或整個類別。您可以加載和保存您的選擇。有些按鈕允許一次展開或折疊所有類別。如果您想通過以下方式快速查找特定文件類型，則展開所有類別會很有用。

在樹視圖窗口具有輸入焦點時鍵入其字母。

請注意，當文件類型過濾器的選擇是從 .settings 文件或案例中加載時，文件類型名稱之間的衝突會變得很明顯。例如，如果您最初選擇了 “mmf”= “MailMessage 文件”（電子郵件類別），那麼您會發現 “mmf”也被選為 “Yamaha SMAF”（聲音/音樂類別）。這是正常的，不會改變類型過濾器的作用。如有疑問，類型過濾器還包括具有相同名稱的其他類型，以避免忽略任何內容。

類型狀態 [輸入， 為了]	類型列的狀態。最初“未驗證”。根據簽名驗證文件類型後（作為優化卷快照或在預覽或畫廊模式下查看文件的一部分），如果文件非常小（小於 8 字節），則狀態為“不相關”。如果文件類型簽名數據庫或內部算法都不知道給定文件的擴展名和簽名，則狀態為“不在列表中”。如果根據數據庫簽名與擴展名匹配，或者如果內部算法同意擴展名適合文件類型，則狀態為“已確認”。如果從數據庫中知道文件擴展名，但簽名定義和內部算法都無法識別文件類型，則狀態為“未確認”。如果文件類型已識別且文件名沒有擴展名或無意義的擴展名（如 .dat 或 .tmp），或者如果設置了更標準化的類型名稱，則狀態為“新識別”。如果簽名與數據庫中的某種文件類型匹配，或者內部算法識別出某種文件類型，但擴展名是不同文件類型的擴展名，則狀態為“檢測到不匹配”。 過濾器 可用。
---------------------	---

此外，此列可能包含有關各種支持類型的文件格式一致性的提示，如“正常”、“不規則”或“損壞”，對於雕刻文件可能立即，對於其他文件可能在文件類型驗證或元數據之後提取已經發生。“不規則”可能意味著不完整、不一致、出乎意料、不可見……任何不尋常的事情。例如，在 JPEG 的情況下，不規則可能意味著在文件末尾找不到頁腳簽名。

有關文件類型等級和組的說明，請參閱文件類型 Categories.txt 的說明。

類型 說明 [輸入， 為了]	顯示文件類型所屬的應用程序名稱、文件擴展名代表什麼等，如文件類型 Categories.txt 中所指定。如果同一擴展名在定義文件中多次出現，則列出其所有含義。例如，.pm 可以是 Perl 模塊、PageMaker 文檔、Pegasus 文件或 X11 Pixmap 文件。
-------------------------	--

類別 [輸入， 為了]	文件類型對應的文件類型類別，根據“文件類型類別.txt”中的定義（見下）。 過濾器 可用。您可以選擇多個文件類型類別進行過濾，而不是只選擇一個，在對話框窗口中而不是（使用起來更快）彈出菜單中。如果同一文件類型/擴展名被定義多次，屬於不同的類別，則該文件類型只會顯示一個類別。儘管如此，類別過濾器仍然有效。可以使用彈出菜單激活類別過濾器。在該彈出菜單中，您還可以看到有關的統計信息。
-------------------	--

當前在目錄瀏覽器中列出了每個類別的多少個文件（或者如果類別過濾器被關閉，將會列出）。

物證對象 [輸入, 為了]	文件或目錄所屬的證據對象的名稱。在遞歸案例根列表中很有用，即當目錄瀏覽器顯示所有證據對象的所有文件時。按此列排序會按證據對象編號進行排序，您可以在證據對象屬性中看到該編號。該數字通常取決於證據對像在案例樹中的位置。
小路	文件或目錄的路徑，以反斜杠開頭，基於卷的根。 過濾器可用 。過濾器表達式被解釋為可以匹配路徑任何部分的子字符串，因此不需要或不支持通配符。
完整路徑 [固相萃取、實驗室、 為了]	路徑包括文件名或目錄本身。按完整路徑排序可以產生一個方便的順序，因為子對象直接跟在它們各自的父對象之後，即使某些父文件或目錄或電子郵件消息具有完全相同的名稱。 過濾器可用 。
家長 姓名， 子對象 [輸入, 為了]	兩列都帶有 過濾器 。例如，子對象過濾器允許您快速查找所有帶有特定名稱附件的電子郵件。例如，父名稱過濾器允許您快速找到所有附加到主題包含特定單詞的電子郵件的附件。請注意，Name、Parent name 和 Child 對象列的過濾器共享相同的設置並且相互排斥（不能同時激活，一個將停用另一個）。
尺寸	文件的邏輯大小（即沒有鬆弛的大小）或目錄的物理大小。 物理文件大小和有效數據長度（對於存儲在 NTFS 文件系統中的文件）可以在文件模式下的信息窗格中看到。如果啟用了遞歸選擇統計，則對於取證許可證，目錄的大小是直接或間接包含在該目錄中的所有文件的總大小，否則是目錄數據結構的大小。 過濾器可用 。要特別關注大小未知的文件，請使用 ≤ -1 的過濾條件。在查找原始磁盤映像或 TrueCrypt/VeraCrypt 容器文件等時，您可以使用取模選項過濾掉不是扇區大小倍數的文件。
已創建	在其所在的捲上創建文件或目錄的日期和時間。在大多數 Linux 文件系統中不可用。
修改的	上次修改文件或目錄的日期和時間。在 FAT 上，時間精度僅為 2 秒間隔。在 CDFS 上，此列中列出了唯一可用的日期和時間戳，儘管它不一定表示最後修改。 過濾器可用 。
已訪問	上次讀取或以其他方式訪問文件或目錄的日期和時間。如果 NTFS 上次訪問時間戳與創建時間戳相同，則顯示為灰色，因為在大多數系統上，出於性能原因，這可能意味著這些時間戳根本沒有維護，因此不是很重要。在 FAT 上，只記錄日期。 過濾器可用 。
記錄已更 改	上次修改文件或目錄的 FILE 記錄（在 NTFS 上）或索引節點（Linux 文件系統）的日期和時間。這些是包含文件元數據的文件系統數據結構。 過濾器可用 。

已刪除 刪除文件或目錄的日期和時間。通常在 Linux 文件系統和可能在 NTFS 上可用（在特定的徹底文件系統數據結構搜索和查看/預覽卷上的 \$UsnJrnl:\$J 文件後，如果有的話）。不要與其他取證工具可能會在 NTFS 卷上向您顯示的所謂刪除時間戳相混淆，這些時間戳甚至還沒有從文件系統中刪除。[過濾器](#)可用。

內容創建 可以從各種文件類型的內部存儲元數據中提取的創建時間戳（請參閱上下文菜單命令），由創建文件的程序放置在那裡。與文件系統級別的時間戳相比，內部時間戳通常更不易變，並且更難操作。例如，它們對於確證很有用。如果在內部元數據中找到官方創建時間戳，則該時間戳將顯示在此列中。如果不是，可以使用各種其他可能的時間戳作為替代，如果需要，甚至可以使用從文件名派生的時間戳。這樣一來，大約 60% 的 JPEG 文件都可以用內容創建的值來呈現。[過濾器](#)可用。

有關時間戳列的更多信息，請參閱下一章。

屬性。 FAT/NTFS 文件系統上的 DOS/Windows 屬性、Unix/Linux/Mac 文件系統上的 Unix/Linux 權限和文件模式，以及圖例（僅限取證許可）和主題 2.9 中解釋的一些專有符號。

“部分初始化”是指根據文件系統（NTFS或exFAT）所謂的有效數據長度小於邏輯文件大小，即文件末尾的數據未定義，類似於file slack沒有任何意義處理文件，並且之前存儲在該位置的磁盤上。您可以在 Info Pane 的 File 模式下看到文件的有效數據長度，未定義的區域以不同的顏色突出顯示。

一些 GUID 分區表分區屬性顯示在 Attr 中。列：系統（=操作系統需要），隱藏（=未安裝為驅動器號），只讀，卷影副本。

按屬性排序時，列中，具有“更有趣”屬性的文件列在最前面，例如表示加密的屬性，而沒有設置任何屬性或屬性未知的文件列在最後。

[過濾器](#)可用。

**第一扇區
[非 INV]** 包含文件或目錄數據的起始文件的扇區數。按第一個扇區排序意味著按磁盤上的物理位置排序，並將顯示彼此相鄰的文件，這些文件在物理上彼此靠近。此列專門為 Zip 存檔中的文件填充，扇區包含此類文件的本地 zip 記錄。在卷/分區模式下單擊 zip 存檔中的文件會自動直接跳轉到其本地 zip 記錄，其後是（通常）壓縮文件數據。這不適用於嵌套 zip 存檔中的文件。[過濾器](#)可用，它允許關注內容從特定扇區範圍開始的文件，例如識別明確受已知壞扇區影響的文件或識別其內容存儲在已知不完整圖像末尾的文件。請記住，如果需要，您可以選擇在此處查看物理扇區號（基於磁盤）而不是邏輯扇區號（基於分區），請參閱目錄瀏覽器選項。用模數

選項，您可以定位是否與群集對齊的文件。

在帶有目錄瀏覽器選項的對話窗口中，此列可以變成“偏移量”列，顯示文件數據的十進製或十六進制起始偏移量而不是起始扇區號。這是更精確的信息，適用於大多數文件。列的標題將在用戶界面的大部分位置相應更改。可以選擇將偏移量設為物理偏移量（如果顯示在分區中，則從物理磁盤/映像的角度來看），就像扇區號可以設為物理扇區號一樣。該列的過濾器需要與目錄瀏覽器中顯示的含義相同的數字（即偏移量或扇區，邏輯或物理），並採用相同的表示法（扇區號為十進制，偏移量為十進製或十六進制）。如果“第一個扇區”列中填充了偏移量，則目錄瀏覽器上下文菜單命令“在列表中查找重複項”可以根據完全相同的起始偏移量而不是僅相同的起始扇區來識別重複項。

FS偏移量

[固相萃取、實驗室、
為了]

顯示文件系統中文件或目錄的定義數據結構的偏移量，即作為將文件包含在卷快照中的基礎的結構。如果對 X-Ways Forensics 從何處獲取文件系統級元數據有任何疑問，您可以在該偏移量處手動檢查詳細信息。這也是您可以應用合適的模板以獲得替代解釋的地方，並且您可以將其他工具的弱勢用戶指向那裡，因為他們可能無法找到如此重要的位置，否則甚至不會列出某些已刪除的文件。由於顯而易見的原因嵌入到其他文件中的雕刻文件和文件在文件系統中沒有這樣的偏移量（或者至少在雕刻文件的情況下 X-Ways Forensics 不知道它）。當您使用專用上下文菜單命令定位文件的 FILE 記錄/inode/文件條目/目錄鍵等時，文件系統偏移量也是您導航到的位置，如所有版本所知。在磁盤/分區/卷模式下，單擊文件或目錄的 FS 偏移單元會自動導航到該偏移量而不是第一個數據扇區。

ID

由文件系統或 WinHex 分配給文件或目錄的標識符。不一定是獨一無二的。[過濾器](#)可用，這使得查找給定文件的其他硬鏈接更加方便。

你。ID

卷快照中文件或目錄的唯一內部標識符。最後添加到卷快照的項目具有最高的標識符。[過濾器](#)可用。例如，如果您想關注最後添加到卷快照的x 個文件（在優化它之後），或者如果您想恢復內部 ID 為y 的邏輯搜索（過濾掉文件），這很有用並且非常易於使用之前可能已經搜索過）。

對於包含大量文件的證據對象，取模選項允許您關注或多或少代表所有文件的文件子集（儘管比按哈希值排序時首先列出的文件隨機性要小）。對內部 ID 應用取模操作將從任何目錄中選擇文件，具有任何名稱、創建日期等。要僅查看 100,000 個文件中的 1,000 個，即每第 100 個文件，請使用操作“內部 ID 取模 100 = 0”。也可用於測試目的：如果您想比較不同硬盤、RAID 系統的性能，

處理器 ,卷快照優化的配置 ,您不必處理證據對像中的所有文件 。如果您只處理每 10 個文件 (由內部 ID 偶隨機選擇) ,您可以獲得更快但可能具有代表性的結果 ,例如 ,只需 1/10 的時間 。

即使是正常工作 ,他們的老闆/他們的檢察官可能不會要求審查員進行 100% 的完整審查 ,例如 ,如果在審查了一個合理大小和代表性的子集之後 ,您可以推斷出幾萬張照片中大約有 10% 是非法材料.

詮釋。父母 [不是INV] 卷快照中文件或目錄的父目錄的唯一內部標識符 。很有用 ,例如 ,當導出文件和目錄時 ,同一路徑中有多個同名目錄 (例如 ,一個存在 ,一個已刪除) ,這樣通過內部父 ID ,即使路徑是曖昧 。

唯一身份 [輸入, 為了] 文件或目錄的內部標識符 ,它在整個案例中是唯一的 ,而不僅僅是在一個證據對象的捲快照中 ,並且在案例的整個生命週期內都是唯一的 。唯一 ID 易於閱讀 。它包含一個分隔符 ,分隔證據對象 ID 和 int 。 ID 。

作為 GUID 的唯一 ID 格式化並擴展為 GUID 的唯一 ID 。

[輸入,
為了]

所有者 [為了] 根據文件系統顯示文件所有者的 ID ,有時還根據操作系統顯示名稱 。

團體 [為了] 顯示 Linux 文件系統中指定文件組的 ID 。

**作者 [輸入,
為了]** 在元數據提取後顯示各種類型文檔 (MS Office 、OpenOffice/LibreOffice 、RTF 、PDF 等) 的作者姓名 。[過濾器](#)可用 。

**發件人 , 接受者 [輸入,
為了]** 這些列是為 X Ways Forensics 從電子郵件存檔中提取的電子郵件消息和附件填充的 ,如果元數據已從中提取 ,則還為原始 .eml 文件填充 。它們帶有[過濾器](#) 。允許您輸入電子郵件地址或姓名的任何部分來搜索某些電子郵件 。過濾器表達式被解釋為子字符串 ,因此不需要或不支持通配符 。

您可以選擇您希望使用過濾器定位的收件人類型 :To: 、Cc: 或 Bcc: 或它們的組合 。如果願意 ,您還可以在各自的列中分別查看收件人 : 、抄送 和密送 :收件人 。

鏈接數 [為了] 文件或目錄的硬鏈接計數 ,即它被目錄引用的頻率 。

僅提供短文件名 (SFN) 以滿足舊 Microsoft DOS/Windows 版本的遺留 8.3 要求的硬鏈接不算作硬鏈接 。

相反 ,此類文件的硬鏈接計數會在目錄瀏覽器的 “鏈接”列中以 ° 標記 。這樣 ,硬鏈接計數更準確地反映了

硬鏈接實際上存在於 X-Ways Forensics 的捲快照中，普通文件的計數始終為 1，而 2 或更多意味著更特殊的東西。如果硬鏈接數 1 標有星號 (*)，這意味著文件或目錄在 HFS+ 的目錄結構中存儲為硬鏈接，儘管根據硬鏈接數它不是必需的。如果硬鏈接計數變灰，則表示在邏輯搜索期間可選擇忽略的文件，以避免不必要的重複搜索工作和重複搜索命中。

**文件數
[輸入,
為了]** 在捲快照中，遞歸地包含在目錄中或包含子對象的文件中的文件總數，即包括更多子目錄。這個數字也可以在括號中的名稱列中找到（取決於設置）。

**命中數
[輸入,
為了]** 在文件中找到的搜索命中數。

**詞數
[輸入,
為了]** 在文件中找到的搜索詞（不是搜索命中）的數量。這會考慮在一個案例中同時搜索中曾經使用過的所有搜索詞，而不僅僅是可能已在搜索詞列表中選擇的搜索詞，除非您刪除了搜索命中。您可以按此列排序以首先列出可能更相關的文件（因為它們包含更多您要查找的搜索詞）。此列僅為案例的證據對象填充。

**搜索詞
[輸入,
為了]** 列出最多 25 個在文件中找到的搜索詞，這些搜索詞計入前一列。即使在普通目錄瀏覽器中，也有助於了解文件中的搜索結果，而無需切換到搜索結果列表。（僅限取證許可）[過濾器](#)可用，不限於此列中顯示的 25 個搜索詞。

**頁數
[輸入,
為了]** 頁數作為元數據提取的一部分從 PDF 和某些 Office 文件類型中提取並顯示在此列中。

**像素
[輸入,
為了]** 以千像素 (KP) 或百萬像素 (MP，百萬像素) 為單位的圖片的大致圓形尺寸，作為寬度乘以高度的結果，出於效率原因存儲為精度非常低的值。尺寸與膚色百分比同時計算，加上查看圖片（全屏模式、預覽模式或在畫廊中）時。允許輕鬆區分例如小型瀏覽器緩存垃圾圖片和高質量數碼照片，以及相關的[過濾器](#)，它允許您專注於小於或等於您指定的像素數或大於或等於或兩者的圖片同時。（由於像素數的低精度存儲，只能近似使用。）從視頻文件中導出至少 1 個視頻後，也可以在此列中看到視頻的近似分辨率。（僅限法醫執照）

**分析
[輸入,
為了]** 組合列顯示文本文檔的 FuzzyDoc 匹配以及 PhotoDNA 匹配和光柵圖像中膚色的計算量（或者圖片是黑白或灰度圖片或太小而無法包含任何相關圖形內容的事實）。如果底層技術可用，則在優化捲快照後可用。按此列排序或[過濾](#)最多。

發現痕跡的有效方法，例如兒童色情或搜索掃描文檔（灰度或黑白圖片）。按“分析”列降序排列首先列出具有 FuzzyDoc 匹配項的文件（那些與靠近頂部的任何哈希集最有信心匹配的文件，隨後是較低的百分比），然後是 PhotoDNA 匹配項（顯示內部 PhotoDNA 哈希中的類別名稱）數據庫，然後是沒有 PhotoDNA 匹配的圖片，按膚色百分比降序排列。之後是不相關的圖片（尺寸很小的圖片），然後是不是圖片的文件，最下面是黑白灰度圖片。該列中的文本顏色編碼可以更輕鬆地區分不同類型的分類。FuzzyDoc 匹配、PhotoDNA 匹配和顏色分析結果相互排斥。這意味著如果對圖片進行顏色分析並發現與 PhotoDNA 哈希值的相似性，則分析列中只會記住 PhotoDNA 類別匹配，而不是膚色百分比，因為 PhotoDNA 匹配被認為更有幫助。對於在卷快照中存儲了至少一個 PhotoDNA 哈希值的圖片，其分析列中會顯示一個程式化的 P。如果是這樣，則可以在詳細信息模式下查看哈希值。

散列

[固相萃取、實驗室、
為了]

最多可以為一個文件計算兩個散列值（例如 MD5 和 SHA-1），然後顯示在兩個散列列中。[過濾器可用](#)。過濾器允許關注具有哈希值、沒有哈希值、其哈希值以特定十六進制值開頭（如果您僅指定哈希值的開頭）或具有特定值（如果您指定完整的哈希值）。此過濾器可以將文件的哈希值與用戶提供的最多 4 個哈希值（以十六進制 ASCII 形式提供）進行比較。

如果您只想快速找到幾個文件，例如可以從目錄瀏覽器的哈希列中複制具有已知哈希值的文件副本，則可以在哈希數據庫中創建一個小哈希集。在查找文件副本時使用此過濾器的最簡單方法（甚至不需要複制和粘貼散列值）是在目錄瀏覽器中以十六進制 ASCII 表示法（不是 Base32）右鍵單擊給定文件的散列值並調用上下文菜單中的“篩選依據”命令。

第一個哈希列以淺灰色顯示偽哈希值，直到計算出真正的哈希值 [FOR]。偽哈希值基於文件元數據，而不是文件內容。這就是為什麼即使對於非常大的文件，它們也可以立即使用。它們允許您以隨機順序列出文件，就像按實際哈希值排序時一樣，但無需先花時間計算實際哈希值。例如對於分類很有用，如果您的時間有限並且只是希望首先快速查看大型證據對像中的一些隨機選擇的文件（例如圖庫中的圖片）以確定證據對象的相關性。

以隨機順序查看文件可能會讓您對證據對像中存儲的內容有更完整和準確的印象，因為列出的前 x% 的文件更加多樣化，並且更能代表整個證據對象，如果它們是以真正隨機的順序。另一方面，如果您按名稱、路徑、大小或時間戳排序，您看到的許多文件可能會有些相似（由相同的應用程序或操作系統、相同的用戶、相同的用戶創建）

相似的目的，大約在同一時間創建或複製或接收，相同的文件格式，.....），所以如果運氣不好，即使有同樣多的相關文件，你也只會看到不相關的文件。請記住，如果您根本不在目錄瀏覽器中排序，視圖也會傾斜，因為您將按照卷快照引用文件的順序看到文件，這或多或少是它們由文件系統引用，因此不是隨機的。

按哈希值排序可以與任何過濾器結合使用，例如以隨機順序僅查看大於 1 MB 的圖片或僅查看特定用戶的文件。偽散列不保證是唯一的，甚至在您關閉並重新打開證據對象時保持不變。

可以在“目錄瀏覽器選項”對話框中更改“哈希”列中顯示存儲在卷快照中的可能兩個哈希值中的哪個哈希值。主要哈希值或次要哈希值或兩者同時存在（如果該框被選中一半）。哈希列過濾器應用於當前顯示的哈希類型。可以在列標題中看到哈希列中顯示的哈希類型。

哈希集
[輸入，為了]
在其中找到文件哈希值的內部哈希數據庫中哈希集的名稱。最多返回 64 個匹配項。[過濾器](#)可用。哈希集列同時顯示兩個內部哈希數據庫的已知匹配項。過濾器可用於一次過濾其中一個數據庫的選定哈希集。

可以在過濾器對話框中選擇要從中選擇哈希集的數據庫。

分類
[輸入，為了]
可以使用目錄瀏覽器上下文菜單手動設置，或使用 X-Tensions、證據文件容器中的元數據、與哈希數據庫匹配或使用其他方式自動設置。使用哈希數據庫時，它取決於在其中找到文件哈希值的哈希集的類別。最初所有文件都被認為是未知的。如果知道，它們要么是“無關緊要”、“值得注意”，要么是“未分類”。[過濾器](#)可用。使用兩個內部哈希數據庫的用戶請注意：Categorization 列僅顯示一個類別。如果您將一個哈希數據庫中的某個文件的哈希值分配給一個類別，而將另一個哈希數據庫中的同一文件的哈希值分配給另一類別，您將在匹配過程中被警告一次，並給出關於哪個哈希值的確切信息其中哈希數據庫中的哈希集有衝突。如有疑問，將以“著名”分類為準。

報告表
[輸入，為了]
文件或目錄已分配給的報告表的名稱。
[過濾器](#)可用。如果文件的父文件已被用戶分配給一個或多個報告表，則在子對象的“報告表”列中也會以淺灰色和箭頭指出這一點，除非子對象本身有報告表關聯。提醒用戶父級已被審查並標記為相關，這可以使他或她免於再次導航到父級的額外步驟。

評論
[輸入，為了]
審查員可能已分配給文件或目錄的自由文本註釋。[過濾器](#)可用。

**元數據
[輸入,
為了]** 通過優化卷快照，可以從各種類型的文件中提取內部文件元數據，並顯示在該列中。這是以詳細信息模式顯示的更廣泛元數據的子集，可用於過濾、導出和報告目的。可以使用目錄瀏覽器上下文菜單中的命令對其進行編輯。

請注意，可以在元數據列中看到的頻繁出現的單詞“生成器簽名”並未按字面意義存儲在內部，因此無法通過目錄瀏覽器單元格中的邏輯搜索或過濾器找到。

生成器簽名 從元數據列中獲知的生成器簽名另外顯示在其自己的單獨列中，用於排序目的，這可能允許識別文件之間的邏輯連接。

[為了]

**設備類型
[輸入,
為了]** 對於 JPEG、PDF、視頻或 PNG 文件，此列可能會顯示該文件是由哪類設備生成的。設備類型可以是掃描儀、DSLR（單鏡頭反光）、無反光鏡相機、數碼後背、攝像機（攝像機）、傻瓜（緊湊型）相機、智能手機、智能手機前置（副）相機、移動電話、網絡攝像頭/ IPCam、運動相機、監控相機或平板電腦。JPEG 文件的“打印機”表示要打印的圖片。屏幕可以表示從屏幕上截取的屏幕截圖，或本應顯示在屏幕上的牆紙。設備類型源自生成器簽名。過濾設備類型可能很有用，例如，如果您正在尋找相當私密的照片（使用智能手機前置攝像頭拍攝的自拍照）或專業照片（例如

DSLR 或數碼相機後背）。

**結構
類型** 此列可以作為元數據提取的一部分進行填充。過濾器可用。

[輸入,
為了]

**關聯
[輸入,
為了]** 文件的一般相關性。可以在提取元數據時計算。這種相關性基於多種因素，例如文件類型、其生成器（如果已知）（對於 JPEG 和 PDF 文件）、當前性（最後修改日期）、是否從任何哈希數據庫中獲知、豐富的它包含的內部元數據、它的大小、圖片的視覺內容，PNG 文件是否是智能手機屏幕截圖、HTML 文件是否已被用戶手動保存在本地、文件是否有異常等。相關性不僅基於內容，而且是基本特徵的結果。特別是生成器簽名是基於來源的標準。主要思想是，如果您的檢查時間有限，您可以從具有最高通用相關性的文件開始，以最大限度地增加找到您要查找的內容（如果存在）的機會，並儘早找到它。要按相關性降序對列出的文件進行排序，即優先查看它們，您還可以使用 Navigation | 從目錄瀏覽器上下文菜單中按相關性排序。

元數據、評論和事件描述過濾器最多支持使用 4 個表達式，可以靈活地與 AND 和 OR 組合。最後一個組合始終具有優先權。例如“A and B or C”被解釋為“A and (B or C)”。 “A or B and C”解釋為“A or (B and C)”。表達式可能以冒號開頭，以表示在表達式級別不是。

搜索命中列表的附加列 [INV, FOR] :物理/絕對偏移量，邏輯/相對

偏移量，關於搜索命中性質的描述（代碼頁/Unicode，是否在解碼文本中，是否在文件鬆弛中），搜索命中與上下文預覽。如果邏輯相對偏移量以灰色打印，則意味著在解碼文本中找到了搜索命中，並且偏移量不是文件中的偏移量，而是解碼文本中的偏移量。

事件列表的附加列 [INV, FOR]：時間戳、事件類型、事件類型類別、描述。

更多提示：右鍵單擊目錄瀏覽器中的列標題可快速激活或停用該列的過濾器，而不會顯示設置對話框窗口。通過右鍵單擊目錄瀏覽器標題行左側或右側的藍色漏斗符號，您可以獲得所有當前活動過濾器及其設置的文本摘要。

3.3.5 有關時間戳列的更多信息

用上標²指定的時間戳列包含替代時間戳 [SPE、LAB、INV、FOR]。在 NTFS 的情況下，這些值取自 0x30 屬性並表示從文件上次重命名或移動時或可能在某些回溯操作發生之前的先前有效時間戳。回溯操作通常由安裝程序和 Windows 本身應用（臭名昭著的創建時間戳隧道效應，參見<http://support.microsoft.com/kb/172190>），當然也可能由普通應用程序和用戶應用出於各種合法或不太崇高的目的。請注意，僅當這些先前有效的時間戳實際上與當前對應的時間戳不同時，才會填充這些列，並且僅當與 Created² 不同時，Modified² 和 Record changed² 才會被填充，以避免因冗餘信息不必要地使屏幕混亂。這意味著您在那裡看到的²時間戳實際上包含其他信息並且不是多餘的。任何

Created² 也為 HFS+ 文件系統填充，具有來自 Mac OS X Lion 和更高版本以及 iOS 的相對較新的“添加日期”時間戳，如果可用並且與常規創建日期不同。該時間戳指定文件何時添加到包含它的特定目錄，即使最初創建的時間更早。

對於電子郵件：從電子郵件存檔中提取的電子郵件消息標題中“日期：”行中的時間戳（如果帶有時區指示符，如 -0700 或 +0200）顯示為創建電子郵件及其所有附件的日期和時間。“Delivery-Date:”行中的時間戳（或者，如果不可用，第一個“Received:”行中的時間戳）被列為最後修改日期和時間。電子郵件附件在“創建”和“修改”列中顯示與其所屬的電子郵件相同的時間戳，因此您可以直接查看這些附件的發送和傳遞時間，而無需導航至父電子郵件。記錄更改時間戳告訴您 OST 文件中有關電子郵件消息的數據結構中的數據何時發生更改，例如，當用戶單擊“發送”按鈕時發送的電子郵件消息或當用戶單擊“發送”按鈕時收到的電子郵件消息已傳送到電子郵件客戶端，或者通常是在將消息複製到另一個 PST/OST 存檔時。

所有時間戳列的組合過濾器允許過濾特定日期範圍（典型應用程序）或僅時間，匹配任何可能的日期。例如，如果您有興趣

在合法的辦公室計算機用戶不工作的半夜發生異常活動，您可以過濾 22:00:00 和 05:59:59（24 小時制）之間的時間。顯然，為時間戳過濾器選擇正確的本地時區對此至關重要。

請注意，對於 FAT 卷，所有時間戳均顯示為本地時間（未調整）。對於所有其他文件系統，時區概念適用。

普通目錄瀏覽器中符合時間戳過濾條件的時間戳會高亮顯示。事件列表中與事件時間戳相同的時間戳也會突出顯示。

時間戳列中的下溢和溢出（支持範圍之外的時間戳）用文本“越界”標記，可以將它們彼此區分開來並進行適當的排序和過濾。支持的範圍是 1829 年 5 月 5 日到 2514 年 5 月 14 日。

在許多時間戳列之一中對時間戳進行排序時，可能會發生基於 UTC 的時間戳必須與具有未定義時區參考的本地時間戳或具有用戶定義時區參考的本地時間戳進行比較（用戶定義的含義定義由考官），看哪個在前，哪個在後。例如，如果一個證據對象具有 NTFS 文件系統而另一個具有 FAT 文件系統，則案例根窗口中基於文件系統的時間戳會發生這種情況。它也發生在同一個證據對像中，例如當對從文件內容中檢索到的內部創建時間戳進行排序時，例如 JPEG 中的普通 Exif 時間戳（本地）和 JPEG 中的 GPS 時間戳（存儲在 UTC 中）。

對所有此類時間戳進行排序會考慮這些時間戳的顯示方式（以原始本地時間或用戶定義的顯示時區），以便順序與顯示的值一致，而不是與時間戳的內部存儲方式一致。這意味著例如本地 Exif 時間戳 2017-01-01 14:01 LT 在 UTC GPS 時間戳 2017-01-01 14:00 +2 之後排序。如果未定義的本地時區等於顯示，則這是正確的時區，在本例中為 UTC +2。該順序當然可能是錯誤的，因為本地內容創建的時間戳的未知時區可能位於 UTC +2 以東的某個地方。如果來自 FAT 文件系統的時間戳的用戶定義時區參考錯誤，則順序也可能是錯誤的。

3.3.6 彈性過濾器

WinHex Lab Edition、X-Ways Investigator 和 X Ways Forensics 中提供了兩個所謂的 FlexFilters。它們可以針對用戶希望關注的普通目錄瀏覽器中的任何列（即不是搜索命中列表或事件列表特定列），具有任意數量的子字符串，並且它們可以與邏輯 OR 或邏輯 AND 組合。因此，這使它們成為唯一可以通過邏輯 OR 相互組合的過濾器。

例如，如果您希望定位不是在特定的連續時間段內創建或修改的文件，而是通常在某些工作日或週末創建或修改的文件，即這些列中的任何一個包含單詞“星期六”或長日期表示法格式的“星期日”。當特定於列的列過濾器沒有為您提供所需的選項時也很有用（例如，對於作者、發件人、收件人，目前您只能輸入一個

name 或 address 或 substring ,並且使用 Description 過濾器 ,您目前無法專門針對某些操作中可選擇省略的其他硬鏈接）。

指示 FlexFilter 處於活動狀態的顏色是紫色而不是藍色 ,因此可以更好地將其與常規列過濾器區分開來 。兩個 FlexFilters 都帶有一個 NOT 選項 ,並且它們也可能針對同一列 ,這樣您就可以實現類似 “在發件人字段中顯示所有以姓名 John Doe 發送的電子郵件消息 ,其中發件人字段不包含域命名為 company.com” 。

3.4 模式按鈕

使用 WinHex 支持的文件系統檢查邏輯驅動器、分區或圖像文件時 ,有幾個按鈕可以確定窗口下半部分 (目錄瀏覽器下方) 的顯示 。僅限法醫執照。

磁盤/分區/卷/容器

以前標記為 “扇區” ,此默認視圖將活動數據窗口表示的磁盤/分區/卷/容器的所有扇區中的二進制數據顯示為十六進制代碼、文本或兩者 。偏移量和扇區號是相對於相應磁盤/分區/卷/容器的開始的 。

文件

看起來類似於磁盤/分區/卷/容器模式 ,但僅顯示分配給當前在目錄瀏覽器中選擇的文件或目錄的簇 ,按照文件使用的順序 ,如果碎片則進行碎片整理 ,如果壓縮則解壓縮 ,與相對於文件開頭的偏移量 。當從文件模式切換到分區/卷模式時 ,X-Ways Forensics 會自動將您指向從分區/卷的角度來看的偏移量 ,該偏移量等於光標最後定位的文件內的偏移量 ,即使文件是碎片化的 ,如果有相同的位置 (如果文件是壓縮或虛擬附件 ,提取的電子郵件或導出的視頻靜止等) 。

原始子模式可用於文件模式下的 NTFS 壓縮和 WofCompressed 文件 ,以查看完整的壓縮數據 。 (List Clusters 命令列出了此類文件的所有簇 ,也包括鬆弛部分 。WofCompressed 數據的鬆弛區域也在分區/卷模式下突出顯示 。)

預習

檢查當前在目錄瀏覽器中選擇的文件的類型 ,並在單獨的查看器組件的幫助下顯示文件 ,除非查看器組件未處於活動狀態或者它是圖片 (支持的文件類型請參見下面的圖庫) 和查看器組件不應該用於圖片 。即使是不完整的圖片 (例如 ,由於碎片而未完全恢復的文件) 通常也可以部分顯示 。如果查看器組件未激活且文件不是支持格式之一的圖片 ,則從文件開頭提取基本的 ASCII 文本是

顯示。

如果預覽模式下的圖片由內部圖形查看庫顯示，而不是單獨的查看器組件，現在可以通過單擊鼠標左鍵（向左旋轉）和鼠標右鍵（向左旋轉）以 90° 的步長旋轉它們向右。某些大廠的手機和數碼相機拍攝的人像模式照片以橫向存儲，並標記為向左或向右旋轉。帶有內部圖形查看庫的預覽模式會自動將這些照片調整到正確的方向。

當內部圖形查看庫顯示圖片時，在預覽模式下單擊鼠標中鍵將鏡像圖片（水平翻轉），或者如果按下 Shift 鍵，則垂直翻轉圖片。請注意，除了任何主動旋轉之外，還會應用此操作。當前激活的旋轉和翻轉模式由右上角的一些符號描述。如果沒有發生翻轉，而是發生了旋轉，則字母“BR”表示原始圖形數據中的右下角。

在預覽模式下單擊“詳細信息”按鈕上的“+”後，您可以選擇同時並排查看同一文件的預覽和詳細信息模式的演示文稿。

再次單擊“詳細信息”或“預覽”按鈕將使該模式成為唯一的活動模式。

細節

包含來自所有目錄瀏覽器列的單個選定文件的所有信息，包括那些當前不可見的文件。非常有用，例如，如果路徑很長並且不適合路徑列中的屏幕，甚至可能不適合路徑工具提示顯示。在目錄瀏覽器中選擇不同的文件或關閉並重新打開數據窗口或應用程序時，恢復詳細信息模式下的大致滾動位置。單擊狀態欄中的軟盤圖標可以將詳細信息模式的內容保存到 HTML 文件中。

詳細信息模式還顯示 NTFS 文件權限（存儲在訪問控制列表，ACL 中）。每個元素通常具有屬性“Grant”或“Deny”以及權限適用的 SID。如果可能，SID 將被翻譯成一個友好的名稱。權限本身是 R = 讀取權限、C = 更改權限、完全控制或特殊訪問權限。對於特殊訪問權限，列出了所有個人權限。對於每個權限，可以有兩個繼承標誌：容器繼承 (CI)、對象繼承 (OI) 或兩個傳播標誌：僅繼承 (IO)、不傳播繼承 (NP)。通常最後的列表元素是組成員屬性。

詳細信息模式還從 OLE2 複合文件（例如 2007 年之前的 MS Office 文檔）、MS Office 2007 XML、OpenOffice XML、StarOffice XML、HTML、MS Access、MDI、PDF、RTF、WRI、AOL PFC、ASF、WMV、WMA、MOV、MP4、3GP、M4V、M4A、JPEG、BMP、EXE/DLL、JIDX（Java 小程序緩存）、THM、TIFF、GIF、PNG、GZ、ZIP、PF、IE cookies、DMP 內存轉儲、hiberfil.sys、PNF、SHD & SPL 打印機假脫機、RecentFilecache.bcf、WIM Vista 圖像文件、PhotoShop PSD、INDD (Adobe InDesign)、DocumentSummary 備用數據流、tracking.log、.mdb MS Access 數據庫、manifest.mbdx /mbdb iPhone 備份、IconCache.db 等等。對於 MS Office 文檔，您通常會看到更多時間戳（例如上次打印）、主題、作者、組織、關鍵字、總編輯時間等等。在可以通過按“IM”按鈕激活的“IM”子模式下，您將只能看到文件的內部元數據。這使得它更有效率。

無需滾動即可檢查多個文件的此類元數據。特別是這對於照片的法醫審查很有用，可以檢查 Exif 數據。根據某些因素，您可以在查看內部 JPEG 元數據時在單列和雙列 IM 模式之間切換。給定足夠的屏幕分辨率和窗口寬度，無需滾動即可以雙列模式快速查看整個內部元數據，因為匯總表位於右側。

對於 JPEG 文件，此模式會在底部顯示一個附加表格。此表包含生成器簽名以及文件的“條件”，可能是“不完整”（如果文件被截斷）、“尾隨數據”（如果多餘數據附加到 JPEG 數據）、“旋轉”。條件“嵌入”標識不是作為獨立文件生成的圖片，而是嵌入在較大文件中的圖片，如縮略圖或分辨率降低的替代品。如果使用工具追溯刪除 JPEG 元數據，也可能會出現這種情況。如果存在此類鬆弛，則 EXIF 段末尾的鬆弛量（零值字節）將以詳細信息模式顯示。例如，iPhone 4 和 iPhone 5 通常會產生這種長度可變的區域，但 iPhone 7 不會。如果旋轉後鬆弛仍然存在，則意味著旋轉是微創的，沒有再壓縮（沒有質量損失）。但是，如果照片編輯程序重寫 JPEG 文件，鬆弛部分就會消失。

報告的 JPEG 圖片“大小”有 1 個或 2 個值。根據 Wordpress 建立的術語，非具有通用名稱（例如“XGA”）的標準尺寸的尺寸被描述為“縮略圖”、“中號”、“中號大號”、“大號”或“大號”。如果識別出生成設備，則該字段被命名為“傳感器尺寸”，或者在掃描儀的情況下被命名為“紙張尺寸”。

“處理狀態”取決於檢測到的生成器，其中每個生成器現在都分配給三個生成器類 D（設備）、E（編輯器）或 C（內容管理系統）之一。生成器類 D 生成的 JPEG 文件是絕對原始的。它們的處理狀態始終是“原始的”。E 類生成器生成的 JPEG 文件為相對原件。他們的處理狀態總是“正常編輯”。例如路透社等新聞機構發布的照片。

第三個生成器類（CMS，如 WordPress、Drupal、TYPO3、Joomla 等）的檢測處理狀態可以採用不同的值。它們通常是不定期編輯的，即它們的編輯狀態未被正式指明。可以根據文件名、生成器簽名、像素尺寸間接推導出狀態。“亂編”狀態也可能是圖片處理造成的。狀態“EXIF 剝離”指的是 JPEG 圖片，儘管不存在 EXIF 元數據，但其設備來源已被檢測到。該設備可能會根據生成器簽名、文件名或特徵像素尺寸被檢測到。國家“社交媒體”被單獨指出，因為這樣的圖片往往具有較高的情報價值。與新聞機構的圖片不同，它們本質上是半公開的。狀態“縮放”是新的，指的是經典內容管理系統。可以說，這樣的照片已經大概率公開了。它們自動且單獨地適應各自的輸出顯示，以優化網頁的加載時間。“最小化”狀態也是新狀態，表示 JPEG 質量降低或文件大小通過優化的重新壓縮（jpeg-recompress、JPEGMini）減小。狀態“未定義”是所有剩餘內容的類別。此類圖片通常也是內容管理系統的輸出，這些系統不標識自己且其格式尚未確定（在未來版本中可能會更改）。

“EXIF 合規性”是另一個聚合的單一值，一個可以查看是否低的分數

質量照片編輯器用於編輯照片。尼康或佳能相機製作的 JPEG 圖片通常具有良好的評級，只有高質量的照片編輯程序才能保留。此類圖片的差評表示由低質量程序編輯。EXIF 數據中不規則編碼的字段標有星號。不規則可能意味著使用了錯誤的數據類型或違反了允許的值範圍或有重複的標籤或字符串不是空終止或包含鬆弛。有些標籤不能同時出現，有些標籤必須存放在指定的目錄下。通常，EXIF 表示不是所有 EXIF 值的簡單非結構化輸出，而是旨在提供背景信息並突出顯示其上下文中的某些參數，以使審查員意識到不規則之處。數碼相機的原始文件中已經產生了典型的 EXIF 元數據錯誤。通過編輯照片，可能會產生其他錯誤，或者可能會修復其他錯誤。

如果 Exif 元數據中的 IFD GPS 字段可用，但為空，或者包含無效坐標，則屬於異常情況，不同於 IFD GPS 根本不存在，通常意味著 GPS 數據已被追溯刪除。它反映為“GPS 格式 :NaN”，其中 NaN 表示“不是數字”。

評估 JPEG 文件中的 DHT 標記。如果標記具有 JPEG 標準定義的值，它將被標記為“標準”，否則將輸出表條目數。

實際上，所有數碼相機都使用標準表格，但社交網絡編碼的 JPEG 却不使用。

他們使用優化的表格並將文件大小減少了大約 5%。

JPEG 文件的內部元數據中的值不是相應相機/設備型號的默認值，而是由用戶分配或由照片編輯程序更改，或者根本不被視為該特定設備型號的原始/正常值生成文件的文件以藍色突出顯示。如果 JPEG 文件中的 GPS 坐標存在異常，這些 GPS 坐標也會以藍色突出顯示。例如，如果 GPS 坐標存在而 GPS 時間戳不存在，對於已知總是同時包含兩者的移動設備類型（有時取決於使用的是前置還是後置攝像頭），或者對於攝像頭類型已知沒有 GPS，這可能意味著坐標已追溯嵌入。與照片拍攝時間不同的 GPS 時間戳也以藍色突出顯示。GPS 處理模式（如果可用）列在詳細信息模式中。此模式允許估計坐標的可靠性/精度。它由各種製造商使用，可以是以下值之一：unknown、GPS、Network、Hybrid、Fused 或 CELLID。“地理定位”以谷歌地圖、OpenStreetMap 或 Bing 地圖接受的符號顯示 GPS 坐標。Exif GPS 數據的三個附加字段在可用的詳細信息模式下輸出：高度、圖像方向和 GPS 誤差。海拔高度可能有助於判斷地理坐標的可靠性。圖像方向是高端智能手機的一個功能。對於許多三星手機創建的 JPEG 文件，詳細信息模式還顯示固件日期和地區，這有助於驗證其他元數據。

JPEG 文件內部元數據的摘要部分有一個名為“Light value”的字段。該值源自著名的攝影公式 $Ev = \log_2(N^{**2}/t) + \log_2(100/ISO)$ 。

值範圍在 16 左右結束，這意味著充滿陽光。一些審查員可能會對這個聚合值感興趣，因為它可以區分室內和室外照片，並且可以檢查照片的當地時間是否合理。

PNG 文件的處理狀態和其他值（大小、每像素位數、文件名分析）也會輸出。使用與 JPEG 相同的處理狀態，除了“不規則編輯”和

“EXIF 剝離”是不可能的。如果屏幕截圖已通過特殊測試，則“原始”值僅用於屏幕截圖。與 PNG 類似，還為 WEBP 文件提供了處理狀態。

安裝目錄中名為“Phone Alias Table.txt”的文件包含從內部設備名稱到人類可讀營銷名稱的翻譯。特別是三星、摩托羅拉、LG 和華為使用的設備名稱相當隱晦，如果翻譯的話更好理解。該表還可以包含設備的發布日期和地區。它的格式在標題中有解釋，以便用戶可以幫助完成它。該表必須按字母順序排序，因為這樣可以提高性能。請注意，這只是一個輔助表。“Generator Signatures.txt”中的相應條目對於檢測和設備類別分類至關重要。

如果適用，QuickTime 格式系列視頻的處理狀態“原始”會在詳細信息模式下引起您的注意。然而，這種說法並不像 JPEG 圖片那麼強烈。這樣的視頻的內容可能已經以一些不規則的方式改變了，而無法檢測到它（例如，交換個別幀）。該語句是指格式結構。傳統的編輯工具實際上總是改變這個結構，所以“正常”的編輯將被檢測到。

畫廊

檢查目錄瀏覽器當前可見部分中所有文件的文件簽名（如果之前未對卷快照中的這些文件執行此操作）。如果文件被識別為受支持的圖片文件類型，則會顯示縮略圖，否則您會看到帶有文件名的白色圖塊，或者甚至可以為此類非圖片文件生成可選的縮略圖（請參閱選項 | 查看器程序）。通過在目錄瀏覽器中滾動，畫廊視圖也會滾動。圖庫反映目錄瀏覽器中的選擇。即使縮略圖仍在加載，您也可以切換目錄。通過雙擊縮略圖，您可以獲得圖片的全尺寸視圖，您可以在其中使用 + 和 - 鍵放大和縮小。即使是不完整的圖片（例如，由於碎片而未完全恢復的文件）通常也可以部分顯示。

支持的圖片文件類型：JPEG、PNG、GIF、TIFF、BMP、WEBP、HEIC、一些 DICOM 變體、PSD、HDR、PSP、SGI、PCX、CUT、PNM/PBM/PGM/PPM、ICO。圖庫與搜索命中列表不能很好地結合在一起。

圖庫可以在另一種模式下運行，使用同步按鈕左側的按鈕激活。

在該模式下，圖庫不顯示當前在目錄瀏覽器中列出的項目，而是顯示單個選定項目的所有子對象（如果有任何此類子對象）。這些要么只是直接的子對象，要么是（在² 模式下）遞歸的子對象。這是一種通過單擊鼠標即可快速瀏覽整個目錄或文件存檔的獨特方式。對於從中提取靜止圖像的視頻也非常有用。在該模式下，畫廊可以有自己的選擇，與目錄瀏覽器分開。您可以右鍵單擊庫中列出的任何子對象，然後對該特定對象執行各種操作。目錄瀏覽器上下文菜單中已知的大多數命令都可用。特別是，您可以通過這種方式將子對象與報告表相關聯、排除、標記或導航以在目錄瀏覽器的本機父目錄中查看它以及所有元數據（然後您可以單擊“後退”按鈕返回到以前的觀點）。子對象按內部 ID 的升序列在庫中。圖庫中的選擇通常完全複製目錄瀏覽器中的選擇。但是，當代表在目錄瀏覽器中選擇的文件的子對象時，畫廊現在

允許在子對像中對其本身進行單獨選擇。

當視圖窗口顯示一張圖片時，如果僅限於一個這樣的窗口，則當您在圖庫中按下光標鍵時，該窗口將更新為下一張圖片。如果畫廊位於第一台顯示器上，在跨桌面上，當視圖窗口位於第二台顯示器的中心時尤其有用。避免必須按 Enter 鍵才能查看圖片，然後再按另一個鍵才能關閉“視圖”窗口以將輸入焦點返回到圖庫。

日曆

從目錄瀏覽器的所有 6 個時間戳列中以日曆的形式提供所有列出的文件/目錄的時間戳的方便的視覺概覽，或者在事件列表模式下提供所有列出的事件時間戳的類似概覽。至少有一個時間戳的每一天在日曆中用灰色標記。一天的活動越多，顏色越深。

週末（週六和周日）特別標有 x。將鼠標懸停在一天上可以找出有多少個時間戳恰好屬於那一天。左鍵單擊某一天以選擇該天作為時間戳過濾器的左邊界，或右擊它以將其定義為右邊界。中間單擊一天以僅過濾該特定日期的時間戳。如果同一個文件被多次列出（如果它包含超過 1 個搜索命中，則可能會在搜索命中列表中發生），那麼它的時間戳也會在日曆中出現不止一次。

當不顯示事件時，您現在可以決定日曆中應包含哪一列的時間戳。排除隱藏的列（寬度為 0 像素），包括所有其他列。狀態欄會提醒您包含哪些列，即使由於水平滾動而當前不可見也是如此。

日曆中沒有時間戳的年份顯示為灰色。年份數字顯示為較深的灰色陰影，為此列出的時間戳越多。所有灰色陰影都試圖讓檢查者更好、更快地了解峰值或無活動。

由於日曆模式中表示的年數有限，如果您不設置過濾器或不刪除具有垃圾時間戳的事件，那麼過去的垃圾時間戳會使您看不到您感興趣的以後年份。您可以指定將由日曆表示的最小年份。即使沒有過濾器處於活動狀態，日曆也會忽略早年的任何時間戳。默認情況下，最小年份是 2000 年。要更改它，請在日曆模式中單擊左側第一年的數字。

示例：在哪個時間段內處理卷上的 JPEG 文件最多？右鍵單擊目錄樹（案例數據窗口）中的根目錄以遞歸地列出所有子目錄中的所有文件，然後使用文件類型過濾器將視圖限制為 JPEG 文件，啟用日曆視圖。

生的

在 Preview 模式下，結合查看器組件，在查看非圖片文件時，Raw 模式將文件呈現為純文本。這對於 HTML 文件查看 HTML 源代碼、.eml 文件查看完整的電子郵件標題以及通常在搜索命中列表模式下查看器組件無法在預覽模式下突出顯示搜索命中很有用。

(因為它可能包含在元數據或控制代碼中，這些元數據或控制代碼將以原始預覽模式而非普通預覽模式表示)。您可以通過在激活 Raw 模式時按住 Shift 鍵來使 Raw 預覽模式持久化。

文件模式現在為 NTFS 壓縮文件提供“原始”子模式。在原始模式下，您實際上可以看到壓縮數據和稀疏簇，而不是文件的解壓縮狀態。這對於研究或教育目的很有用，因為理論上少量數據可以手動隱藏在每個壓縮單元的未明確定義但隱含存在的鬆弛區域中，該鬆弛區域跟隨壓縮的有效負載數據。

風險投資公司

當查看內部圖形查看庫支持的類型的圖片時，VC 按鈕僅在預覽模式下可見。默認情況下，內部圖形查看庫用於預覽或查看圖片。但是，如果按下“VC”按鈕，則會使用查看器組件，它還負責在圖庫中顯示縮略圖。

同步

同步目錄瀏覽器和目錄樹，當您遞歸視圖中選擇目錄瀏覽器中的文件時，其父目錄將突出顯示。非遞歸探索模式中的同步模式與 Windows 資源管理器中的“自動擴展到當前文件夾”選項具有類似的效果。這意味著當同步模式關閉時使用目錄瀏覽器從一個目錄導航到另一個目錄時，左側的目錄樹將不再反映當前目錄，必要時既不會展開其父目錄，也不會選擇當前目錄。對於遞歸和非遞歸探索以及每個數據窗口，分別記住同步模式是否處於活動狀態。

Case Root 窗口中的 Sync 按鈕具有特殊功能。這是可能的，因為目錄導航在該窗口中不可用。該按鈕控制是否將焦點從一個數據窗口切換到另一個數據窗口（例如使用選項卡控件）是否應在案例數據窗口中突出顯示相應的證據對像或其當前瀏覽的目錄。

探索模式

帶有捲曲綠松石箭頭的按鈕。在目錄的正常探索和遞歸探索之間切換。遞歸探索時，您不僅會看到當前目錄的內容，還會看到其所有子目錄及其子目錄的內容，等等。要遞歸地瀏覽目錄，您也可以在目錄樹中右鍵單擊它。

多顯示器支持

可以從數據窗口中分離數據窗口的下半部分（磁盤/分區/卷模式、文件模式、預覽、圖庫等），方法是單擊模式按鈕左側的三個點，兩次。之後，您可以在屏幕上自由移動和調整它的大小。在多顯示器上，這允許您將用戶界面的那部分顯示在單獨的屏幕上，甚至可以在那裡最大化它。通過再次單擊相同的三個點或單擊最小化按鈕將其重新集成到主窗口中。

第一次單擊三個點將在目錄瀏覽器的右側而不是下方顯示數據窗口的這一部分。這在當今垂直屏幕空間稀缺的寬屏顯示器上非常有用，因此您可以看到一長串垂直文件列表，同時還可以充分利用可用的垂直屏幕空間，例如預覽基於頁面的文檔應該以縱向模式而不是橫向模式查看。對畫廊也很有用，對於肖像模式照片、細節模式和磁盤/分區/捲和文件模式下的十六進制編輯器顯示非常有效，傳統上每行只有 16 個字節。

右鍵單擊模式按鈕欄中所有按鈕外的任意位置，將顯示或隱藏目錄瀏覽器和數據窗口下半部分之間的分隔線，位於模式按鈕欄上方。將鼠標懸停在分隔線上時，鼠標光標形狀會發生變化，表示您可以將其向上或向下移動。如果分隔線不可見，您可以通過在所有按鈕外的模式按鈕欄中單擊鼠標左鍵並在按住鼠標按鈕的同時上下移動鼠標光標來調整窗口高度。如果沒有分隔線，更直觀的是，模式按鈕欄的右側與目錄瀏覽器相關，並且還充當其狀態欄。

3.5 狀態欄

狀態欄顯示有關文件的以下信息：

1. 當前頁數和總頁數（磁盤編輯器 :sectors）
2. 當前位置（偏移量）
3. 當前位置十六進制值的十進制轉換
4. 當前塊的開始和結束（如果當前已定義）
5. 當前塊的大小（以字節為單位）（同上）

單擊狀態欄單元格以...

1. 移動到另一個頁面/扇區， 2. 移動到另一個偏移量， 3. 定義十進制轉換的整數類型和 4. 定義塊。

右鍵單擊狀態欄以將狀態欄中的信息片段複製到剪貼板中。

右鍵單擊第二個狀態欄單元格允許在絕對（默認）和相對偏移顯示之間切換。這在檢查包含固定長度記錄的數據時很有用。

以字節為單位指定記錄長度後，狀態欄顯示當前記錄號和其中的相對偏移量。

右鍵單擊狀態欄第三個單元格可以將當前位置的四個十六進制值以相反的順序複製到剪貼板中。這對於跟蹤指針很有用。

3.6 數據解釋器

數據解釋器是一個小窗口，可為當前光標位置的數據提供可能的翻譯。是否顯示可以通過視圖菜單控制，而不是數據解釋器的選項。與某些用戶普遍認為的相反，如果選擇了任何塊，它會完全忽略任何塊，並且始終從光標所在的字節開始解釋。選項對話框允許您指定要解釋的數據類型。這些是各種整數數據類型（默認為十進製表示法，可選十六進製或八進制）、二進制格式（一個字節的 8、16 或 32 位）、四種浮點數據類型、彙編程序操作碼（Intel®）和日期類型。

數據解釋器可以解釋 UNIX/C、Java/BlackBerry/Android 和 Mac 絕對時間戳存儲為十進制 ASCII 文本而不是二進制中的整數。您會在選項對話框中找到一個上下文菜單項以及一個複選框。數據解釋器可選擇將除 MS-DOS 日期和時間之外的所有格式的時間戳轉換為本地時間（在常規選項中定義的時區）。您將找到一個上下文菜單項以及選項對話框中的一個複選框。

數據解釋器還能夠將大多數數據類型轉換回十六進制值。確保文件以編輯模式而不是只讀模式打開，在數據解釋器中輸入新值，然後按ENTER。然後數據解釋器將相應的十六進制值輸入到當前光標位置的編輯窗口中。

右鍵單擊數據解釋器以顯示上下文菜單。這將允許您在整數和浮點數據的大端和小端轉換之間切換。您還可以選擇十進制、八進制或十六進制整數表示形式。有關更多設置，請參閱數據解釋器選項。

在數據解釋器和模板中將 V1 GUID 分解為時間戳、序列號和 MAC 地址是可選的。在 Data Interpreter 選項中，您現在可以選擇強制分解（完全選中）或阻止它（始終獲得帶大括號的標準 GUID 符號）或僅在時間戳不是太難以置信時才查看分解（選中一半）。後一種設置很有用，例如，Apple GPT 值聲稱是 V1 GUID，但包含扭曲的 ASCII 文本而不是有效時間戳。

提示：

- 某些十六進制值無法轉換為浮點數。對於這些十六進制值，數據解釋器顯示 NAN（不是數字）。
- 某些十六進制值無法轉換為有效日期。不同日期類型的取值範圍

或多或少是狹窄的。

- 英特爾® 指令集中存在冗餘，這些冗餘在數據解釋器中顯示為十六進制操作碼和助記符的重複。浮點指令一般顯示為F***。更詳細的參考資料可以在英特爾® 架構軟件開發人員手冊第 2 卷：指令集參考資料中找到，該資料以 PDF 格式在互聯網上提供。

3.7 崗位經理

位置管理器維護一個文件或磁盤偏移量列表以及相應的描述，稱為位置，可以用作註釋/書籤。當不處理案例時，它也可用於搜索命中，但遠不如搜索命中列表強大。如果按 Ctrl+Left 和 Ctrl+Right，從一個條目導航到下一個條目很容易。您可以輸入新職位並編輯或刪除現有條目。如果文件中的特殊偏移量對您很重要，您可以將其添加到位置管理器。這使得以後再次找到它變得容易得多，而且您不必記住它。描述最多可包含 8192 個字符。例如，適當的描述可以是“數據塊從這裡開始！”。

可選地，位置管理器維護的所有位置都可以在編輯器窗口中以您指定的唯一顏色突出顯示，並且當鼠標光標移動到它們上方時，它們的描述顯示在黃色工具提示窗口中。

您還可以使用編輯窗口的上下文菜單或通過在編輯窗口中單擊鼠標中鍵來添加或編輯位置。

單擊鼠標右鍵以查看位置管理器中的上下文菜單。上下文菜單提供了額外的命令。您可以刪除、加載或保存位置，甚至可以將列表導出為 HTML。如果通用位置管理器中的位置列表發生更改，則在退出 WinHex 時將其保存在文件 WinHex.pos 中，以便它們在下一個會話中仍然可用。只有搜索結果不會永久保存，除非它們已通過上下文菜單進行編輯。

有一個通用位置管理器，它存儲應用於所有數據窗口的位置，還有一個用於案例中每個證據對象的位置管理器，它存儲為該特定證據對象定義的位置並且僅應用於該證據對象的數據窗口。前者通過主菜單（導航 | 位置管理器）調用，後者通過在證據對像打開時單擊屏幕中間最右邊的按鈕調用，上面有十字準線。如果您找不到您之前定義的位置，這可以解釋它。如果職位經理處於活動狀態，它會在數據窗口頂部附近顯示您當前正在查看的職位經理。

通用位置管理器中的搜索命中默認情況下會在通用位置管理器關閉後立即刪除，以避免混淆，因為通用位置管理器中的位置沒有引用特定文件或磁盤，而是有意應用於任何活動的數據源調用時。如果您希望保留搜索命中，請在通用職位管理器的上下文菜單中更改相應的選項。

POS 文件格式的完整文檔可從 WinHex 主頁 <http://www.x-ways.net/winhex/> 獲得。

3.8 有用的提示

- 影響目錄瀏覽器或搜索結果或書籤列表中單個選定項目的菜單命令可以在右鍵單擊此類項目時打開的上下文菜單中找到。您不會在主菜單中找到此類命令。
- 按如下方式使用鼠標按鈕定義塊（如果上下文菜單已關閉）：

· 向左雙擊設置塊開始。 · 單擊右鍵設置塊結束。 · 雙擊
右鍵清除塊。

- 您可能希望使用鍵盤 (SHIFT+箭頭鍵或ALT+1和Alt+2)。
- 使用TAB鍵在十六進制和文本模式之間切換。 · 使用INS鍵在插入和覆蓋模式之間切換。 · ENTER顯示啟動中心。 · ESC中止當前操作 (如果有) ,否則清除塊 ,關閉活動對話框或模板窗口。 · PAUSE停止或繼續當前操作。 · 如果案例處於活動狀態且未打開為寫保護 ,則CTRL+S可保存當前案例。 · F11重複上次轉到偏移命令。 CTRL+F11作用於相反的方向 (從當前位置開始) 。 · ALT++是 Go To Offset 命令的變體 ,專門用於跳轉一定數量的

板塊下跌。

- ALT+-是另一種變體 ,專門用於向上跳轉一定數量的扇區。 · SHIFT+F7在三個字符集之間切換。
- (SHIFT+)ALT+F11重複最後一個移動塊命令。 · CTRL+SHIFT+M調用打開的證據對象的註釋。 · ALT+F2在文件被修改後重新計算自動散列 (校驗和或摘要) 。 · ALT+LEFT和ALT+RIGHT允許在模板內的記錄之間切換 (就像“<”和“>”按鈕) 。 ALT+HOME 和ALT+END分別訪問第一條和最後一條記錄。
- ALT+G將編輯窗口中的光標移動到當前模板位置並關閉模板窗口。
- CTRL+F9打開訪問按鈕菜單 (僅限磁盤編輯窗口) 。 · 在目錄瀏覽器中按CTRL+C將所選項目的文本數據複製到剪貼板 ,使用與目錄瀏覽器本身相同的符號 ,否則使用導出列表命令的功能。
- 使用腳本使您使用WinHex 的工作更有效率。 · WinHex 具有拖放功能 ,但是 ,如果接收到 Windows 會阻止拖放應用程序以管理員身份運行 ,而發送應用程序不是。
- “Invalid input” :在對話框中點擊OK ,出現 “Invalid input”錯誤時 ,注意對話框中哪個控制項在閃爍 ,因為該項中的值是不被接受的。 · 通過單擊偏移數字從十六進制切換到十進制偏移表示。 · 嘗試單擊狀態欄單元格 (鼠標左鍵和右鍵) 。

整個程序中的所有編輯框 (密碼編輯框和列寬框除外)都會記住最多 10 個最後輸入的歷史記錄。單擊出現在具有歷史記錄的編輯框中的小按鈕時 ,可以看到歷史記錄。或者 ,您可以像在普通下拉框 (組合框)中一樣按 F4 鍵。如果您從彈出菜單中選擇了上一個條目 ,它將自動插入到編輯框中。希望刪除這些歷史記錄或將它們傳遞給其他人的用戶 ,請注意 ,當程序結束時 ,它們存儲在文件 History.dat 中。可以簡單地複製或刪除該文件。如果您不想保留

會話之間的歷史記錄，您可以自己創建一個名為 History.dat 的空文件並將其呈現為只讀。要刪除特定編輯框的特定歷史條目，請按住 Shift 鍵從彈出菜單中選擇該條目。

自 Windows 95（甚至可能是 Windows 3.1？）時代以來，用戶可以按 Ctrl+C 在剪貼板中生成標準 Windows 消息框的純文本表示形式。對於 WinHex 和 X-Ways Forensics 中的消息框，它的工作原理是一樣的。儘管這是 20 多年來 Windows 中的一項基本功能，任何有經驗的 Windows 用戶都應該知道，儘管 WinHex 和 X-Ways Forensics 讓用戶意識到這一點（“你知道嗎？……”），但偉大的大多數用戶出於某種原因仍然截取消息框的圖形屏幕截圖並將它們粘貼到 HTML 電子郵件中，例如當他們報告錯誤消息時，儘管這比簡單地按 Ctrl+C 和 Ctrl+V 更有效，儘管它會膨脹電子郵件的大小是不必要的，因為一些 ASCII 字符需要更少的空間，而它們有數千個像素值。這也意味著如果電子郵件在回復時被轉換為純文本，屏幕截圖將丟失，當然錯誤消息文本將無法在圖形屏幕截圖中搜索到，也無法方便地選擇並作為文本複製到剪貼板由收件人發送，並且收件人無法確定存在多個變體的某些字符的確切 Unicode 值。

在 WinHex 和 X-Ways Forensics 中，甚至可以復制對話框及其幾乎所有控件項（靜態文本、按鈕、複選框、單選按鈕、列錶框、組合框和樹視圖控件）的基本 ASCII 表示形式包括它們的狀態（未選中、選中、半選中），方法是在屏幕上出現活動對話框時按 Ctrl+C（如果帶有選擇的編輯框具有輸入焦點，則不會）。在對話框的窗口菜單中也有專門的命令。該菜單又稱為系統菜單或控制菜單，在右鍵單擊對話框標題時彈出。這個複制命令是一種非常有效的方式，可以在特定對話框中向其他用戶顯示您的設置，並讓他們複製字符串以在他們自己的編輯框中使用，這樣他們就不必鍵入它們，避免拼寫錯誤。文本表示比屏幕截圖更強大，因為它完整地顯示了編輯框和列錶框的內容，即使這些控件具有滾動條並且內容超出了屏幕上控件的物理邊界。支持 Unicode 字符。我們建議用戶僅在絕對必要時截取消息框和對話框的屏幕截圖，例如，如果他們希望在 Photoshop 或類似程序中以圖形方式突出顯示某些控制項以獲取消息

穿過。

幾乎所有對話框中的設置也可以根據需要方便地保存到文件或從文件中加載，例如通過系統菜單與其他用戶共享或供將來使用。這個函數可以記住最重要的控件類型的選擇狀態：複選框、單選按鈕、列錶框、組合框和樹視圖控件。即使控件當前不可見，這也有效。這些設置存儲在擴展名為 .dlg（“對話框”）的文件中，與模板和腳本位於同一目錄中。編輯框的內容也會被記住。

但是，此功能不會記住複選框、列錶框、組合框和樹視圖控件的內容/文本標籤，例如，複選框在“同步搜索”對話框中代表哪個代碼頁，“報告表”過濾器中存在哪些報告表列錶框，查看器程序對話框窗口中列出了哪些外部程序，樹視圖控件中列出了哪些文件類型等。它也不記得控件或列表項的順序。它也不會記住相關對話框窗口中的設置（例如，當單擊“...”按鈕時打開）。該功能不適用於“目錄瀏覽器選項”對話框窗口。為了

目錄瀏覽器選項 請通過單擊目錄瀏覽器標題行中的圖標來保存和加載 .settings 文件。在文件中存儲對話框窗口選擇的功能非常有用，例如對於導出列表命令，一些用戶為了不同的目的反復需要不同的設置，並且列錶框中的項目總是相同的（只是可用的列），除了更改用戶界面的語言之後。

3.9 命令行參數

- 1) 您可以簡單地指定您希望自動打開的文件的名稱作為命令行參數，必要時包括路徑。也可以打開物理磁盤，例如指定:0 表示硬盤 0。
- 2) 命令行可用於運行文件編輯腳本。只需將 .whs 腳本文件名指定為參數即可。它將被執行而不是被打開。
- 3) 您可以使用名為“XT”的命令運行 X-Tension，後跟一個冒號以及 X-Tension 的路徑和文件名。
- 4) 命令行可用於打開現有案例。只需將 .xfc 案例文件名指定為第一個參數即可。您可以使用 AddImage: 命令將圖像添加到這種情況（見下文）。如果命令行中的參數是 .xfc 文件的路徑或名稱，並且如果在處理該參數時案件已經打開，則該 .xfc 文件的證據對象將被導入到已經激活的案子。
- 5) 命令行可用於 X-Ways Forensics（不是 X-Ways Investigator）自動
 - a) 創建案例
 - b) 添加圖像、存儲設備、目錄和文件
 - c) 優化所有添加證據的捲快照對象，以及
 - d) 運行關鍵字搜索。示例 :xwforensics64.exe NewCase:D:\Cases\My AddImage:Z:\Images\My image.dd RVS:~ auto
 案子” AddImage:Z:\Images*.e01

如果沒有為案例指定路徑，它將在案例的默認目錄中創建。只有包含空格的參數才需要引號。如果“NewCase”後跟一個分號而不是冒號，那麼如果指定的 .xfc 文件已經存在，則生成一個唯一的文件名。使用冒號，現有案例將被刪除並覆蓋（沒有提示或憐憫）。 “NewCase”命令支持相對大小寫路徑以及對環境變量的引用。

要細化案例中所有證據對象的捲快照（“RVS:~”命令）或僅新添加的證據對象（“RVS:~+”），X-Ways Forensics 將運行相同的操作並使用相同的設置根據 WinHex.cfg 文件，上次已應用於“原始”（即完全未優化的）捲快照。具有活動細化設置的對話窗口的屏幕截圖會自動包含在案例活動日誌中。根據您的案例活動日誌設置，它本質上是文本的還是圖形的。在處理命令行參數 AddImage 和 RVS 時，通常需要用戶單擊的消息框中的文本被重定向到消息窗口。對話框（如果有的話）仍會正常彈出（請參閱下面的補救措施）。

命令“LST”允許加載搜索詞列表。如果後跟一個冒號和文本文件的名稱或完整路徑，每行有 1 個搜索詞，並且如果這先於 RVS 以隱式觸發的同步搜索運行，則這些詞將用於該搜索。

6) AddImage 命令支持星號。它還支持可選的子參數，以強制將圖像解釋為物理的分區介質 (P) 或卷 (V)，並強制使用特定扇區大小進行解釋，其中扇區大小是可選的，例如

添加圖像 :#P#Z:\Images*.dd 添
加圖像 :#P,4096#Z:\Images*.dd

如果您不指定這些子參數，可能會彈出一個對話窗口，要求用戶輸入此信息，但只有在極少數情況下才會出現，前提是前幾個扇區的數據對 X-Ways Forensics 而言不明顯它是什麼類型的圖像，圖像是不是由 X-Ways Forensics 或 X-Ways Imager 創建的，以及圖像是否是 .e01 證據文件格式（例如原始圖像）。

只有同時滿足所有三個條件並且您不指定子參數，才會彈出對話窗口。

7) “AddDir”命令後跟一個冒號，然後指定要添加到案例中的目錄，例如AddDir:X:\。如果冒號後面的字符是星號，所有可用盤符的根目錄將被添加到大小寫 :AddDir:*.但是，網絡驅動器是可選的，因為它們可能過大並且探索起來很慢。添加網絡驅動器取決於選項 | 中的新選項卷快照。如果您從具有驅動器號的捲運行 X-Ways Forensics，則該驅動器號將被忽略，假設您這樣做是為了對實時系統進行分類並從您自己的可移動設備運行 X-Ways Forensics。此命令也可用於將單個文件添加到案例中。

8) “AddDrive”命令後跟一個冒號，然後指定要添加的驅動器盤符，以大寫字母表示，例如AddDrive:C。與通過操作系統訪問和探索的目錄不同，驅動器盤符需要扇區級訪問權限（因此需要管理員權限），如果支持，任何現有的文件系統都將由 X-Ways Forensics 本身進行解析。如果冒號後面的字符是星號，則系統中所有可用的驅動器號都將被添加到大小寫中 :AddDrive:*.網絡驅動器再次是可選的，並且將跳過帶有 X-Ways Forensics 的驅動器號。如果您在沒有管理員權限的情況下運行該軟件，但您指定了 AddDrive:* 命令，那麼將運行 AddDir:* 命令。如果網絡驅動器作為 AddDrive:* 的一部分遇到，它們將在內部使用 AddDir 命令添加，因為它們必須由操作系統在沒有扇區級別的情況下進行探索

使用權。

9) 如果您希望對不同類型的案例應用不同的設置，您需要將這些設置存儲在單獨的 WinHex.cfg 文件中（在不同的目錄中或使用不同的名稱）並在執行 X-Ways Forensics 之前恢復所需的設置。或者您可以使用命令行參數“Cfg:”，它確定 X-Ways Forensics 將在啟動期間讀取的配置文件的名稱（而非路徑）以及在終止時將寫入的配置文件的名稱，在以下情況下需要使用替代配置（不是存儲在主 WinHex.cfg 文件中的配置）。例如，如果對於自動處理您需要與手動執行不同的設置，選擇特定的捲快照優化操作或避免提示

是否應該啟動第二個實例。這樣的參數看起來像“Cfg:My other settings.cfg”。與往常一樣，僅當名稱包含空格時才需要引號。名稱的最大長度為31個字符。當前僅支持ANSI/ASCII字符。命令行參數通常按照您指定的順序進行處理，除了Cfg：參數總是在所有其他參數之前處理，所以它去哪裡並不重要。另外，請注意一些設置存儲在其他文件中，例如“X-Tensions.txt”和“Unwanted Metadata.txt”。

10) 您可以加載對話框窗口選擇。這通常會在處理命令行參數時覆蓋最初從WinHex.cfg文件讀取的配置的特定部分（而不是當配置的這些部分可能影響應用程序的操作時）。命令為“Dlg.”，後面直接跟.dlg文件的路徑。支持相對路徑，您可以使用文件掩碼同時加載同一目錄中的多個.dlg文件。在您保存對話框窗口選擇以供將來使用命令行後，請在保存後單擊確定來驗證它們是否可以被接受。只能使用在v20.2及更高版本中創建的.dlg文件。

11) 名為“Override”的命令行參數覆蓋消息框和對話框，直到處理完最後一個命令行參數。這些框的文本將輸出到消息窗口（因此也間接輸出到msglog.txt，除非禁用），並且將模擬自動點擊OK（如果參數為“Override:1”）或點擊取消時（在“Override:2”的情況下）。如果消息框只有一個按鈕，則指定哪個參數值都沒有關係。所有這些都有助於避免程序在等待用戶輸入時自動處理的中斷和延遲。

默認設置和推薦行為（如果未指定Override參數）類似於“Override:0”，其中消息框和對話框正常顯示，並可能警告用戶嚴重錯誤情況和異常情況，例如不完整的圖像、無法檢測的圖像格式等。該參數在啟動時立即生效，在其他參數的常規處理開始之前，即使在命令行最後指定了Override參數。

Override參數還將整個命令行輸出到“消息”窗口（即使值為“0”），這取決於參數在命令行中的位置。這允許稍後研究日誌的用戶知道對被抑制的消息框和對話框的模擬響應是什麼。

12) 也可以通過命令行自動鏡像物理設備（例如本地硬盤或遠程硬盤或通過F-Response打開的RAM）。第一個參數應以冒號開頭，然後在Windows中指定設備號（例如“:1”表示1號硬盤，即第二個硬盤）。這將導致該設備在啟動時自動打開。第二個參數應以管道開頭，後跟“e01”或“raw”以指示首選圖像文件格式，然後是另一個管道和圖像的路徑和文件名，然後可選地後跟描述和檢查者姓名（例如“|e01|G:\Output filename.e01|我的描述|我的名字”）。如果願意，您可以創建圖像文件的兩個副本：第二個副本的路徑可以附加在第一個副本的路徑之後，由正斜杠分隔。示例：“|e01|Z:\First Copy.e01\V:\Second Copy.e01”。

13) 最後一個參數可以是“auto”，如果你希望在以下情況下自動退出X-Ways Forensics

完成的。

3.10 用戶自定義快捷鍵

選項中有一個按鈕 |您可以單擊通用對話框窗口，為目錄瀏覽器上下文菜單和其他地方的命令定義最多 20 個自定義鍵盤快捷鍵。

目前僅在 X-Ways Forensics 中可用。快捷方式旨在提高您執行最常用活動時的工作效率。僅支持涉及鍵 Ctrl、Ctrl+Alt、Alt Gr、Shift 和 Space 的組合鍵。請注意，如果您將空格鍵用於任何鍵盤快捷方式，則不能再使用它來標記或取消標記項目。第二個鍵可以相對自由地選擇，當灰色的編輯框有輸入焦點時按下它即可。如果沒有提供所選鍵的人類可讀描述並且您後來忘記了您定義的鍵，您可以查看此十六進制鍵代碼列表：[https://msdn.microsoft.com/en-us/library/windows/Desktop/dd375731\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/Desktop/dd375731(v=vs.85).aspx)

理論上可以使用以下 ~80 目錄瀏覽器菜單命令代碼（未全部測試）並且必須輸入為數字：

9800 :使用外部查看器程序 #1 查看

9801 :使用外部查看器程序 #2 查看

9802 :使用外部查看器程序#3 查看

...

9831 :使用外部查看器程序 #32 查看

9919 :定義文件類型

9920 :轉到相關文件

9921 :優化選定文件的捲快照

9927 :對所選文件運行 X-Tension

9928 :附加外部文件

9931 :編輯元數據

9932 :在其目錄中查看此文件

9933 :從卷根目錄中查看此文件

9934 :尋找父對象

9935 :在選定文件中進行邏輯搜索

9937 :附加外部目錄

9938 :安全擦除

9939 :保留特定目錄的搜索命中列表

9940 :刪除列表中重複的搜索結果

9941 :選擇排除項目

9942 :編輯評論

9944 :包含

9945 :選擇標記的項目

9946 :排除除標記項以外的所有項

9947 :排除標記的項目

9948 :如果在後台處於活動狀態，則添加到證據文件容器或骨架圖像

9949 :調整搜索大小

9950 :將搜索命中轉換為雕刻文件 9951 :調整雕刻文件和虛擬文件的大小 9952 :將搜索命中分配給其他搜索詞 9953 :提取連續的視頻幀
9954 :在報告中包含搜索命中 9955 :安裝為驅動器號（僅當一個目錄時才有意義被選中，並且只有一個）
9956 :使用首選視頻播放器觀看 9957 :使用首選 HTML 查看器查看 9958 :使用首選文本編輯器查看 9959 :在關聯的外部程序中執行/打開
9960 :選擇查看的項目 9961 :使用要選擇的外部程序查看
9962 :刪除重複項基於散列 9963 :基於 int 查找項目。ID
9964 :按相關性排序 9965 :打印 9966 :根據列表項目編號查找項目 9967 :不進行排序 9968 :全選 9969 :按所選文件的哈希值過濾（以查找重複項）

9971 :探索
9972 :將搜索命中標記為值得注意
9973 :打開 9974 :導航到定義數據結構
9975 :導出列表 9976 :列出集群 9977 :恢復/
複製 9978 :探索/查看 9979 :反轉選擇 9980 :
包含在哈希數據庫中

您會注意到遞增的數字之間存在一些可疑的差距。缺少的數字要么未分配，要么不鼓勵調用，或者根本沒有為鍵盤快捷鍵定義的意義。作為後者的示例，9929 將刪除選定的搜索命中或事件，這當然可以通過按 Del 鍵來完成。此信息將減少您隨機嘗試此處未列出的號碼的衝動，儘管誰知道一個未記錄的號碼是否可能觸發秘密的“查找所有證據”命令。

請注意，即使沒有定義任何此類鍵盤快捷方式，您也可以通過按上下文菜單鍵僅使用鍵盤訪問所有目錄瀏覽器上下文菜單命令。

（通常位於右側 Windows 鍵和右側 Ctrl 鍵之間。）一些菜單命令已經具有預定義的鍵盤快捷鍵。例如，Enter 鍵與雙擊相同（查看或瀏覽，具體取決於您的設置）。數字鍵盤的乘法鍵觸發探索命令。Del 表示排除。Ctrl+Del 將文件重置為“仍有待卷快照優化處理”狀態並撤消一些優化操作。Ctrl+Shift+Del 刪除散列集匹配項、散列類別和 PhotoDNA 分類。Ctrl+Caps Lock+Del 從文件中刪除“文件內容未知”標誌。

（例如，如果由於臨時 I/O 問題 X-Ways Forensics 將文件標記為

雖然通常文件可以很好地讀取。)Ctrl+C 使用 “導出列表” 對話框窗口的特殊設置將所選項目複製到剪貼板。

主菜單

用戶定義的鍵盤快捷鍵也應該能夠調用主菜單中的幾乎所有命令，即使目錄瀏覽器以外的用戶界面部分具有輸入焦點。如果菜單命令的命令代碼在未來的版本中發生變化，X-Ways Forensics 將確保任何針對該代碼的鍵盤快捷方式將自動變為非活動狀態，以防止意外誤用。要找出主菜單中命令的命令代碼（也稱為菜單項的 ID），您可以在所謂的資源編輯器中打開主要的可執行文件，然後查看您喜歡的語言的菜單資源。此類工具的一個極力推薦的輕量級示例是“Pelles C for Windows”，它恰好也是一個優秀的 C 編譯器和適合創建 X-Tensions 的完整開發工具包。

主菜單命令的鍵盤快捷鍵應該不如目錄瀏覽器上下文菜單命令重要，因為主菜單已經預定義了許多專用的鍵盤快捷鍵，或者即使沒有，也可以在不將手從鍵盤上移開並從 Alt 鍵開始的情況下使用。為了給您一些關於有用應用程序的想法，僅供參考，在遞歸探索和非遞歸探索之間切換的命令代碼是 122，拍攝新卷快照的命令代碼是 109。

為過濾器定義的命令代碼（順序是引入過濾器的歷史順序。）

9700 :名稱
 9701 :類型
 9702 :類型狀態
 9703 :類別 9704 :
 大小 9705 :路徑
 9706 :發件人
 9707 :收件人
 9708 :時間戳
 9709 :屬性 9710 :
 哈希 1 9711 :哈
 希集 9712 :哈希
 類別 9713 :報告
 表 9714 :註釋 9715 :
 元數據 9716 :分析
 9717 :像素 9718 :
 Int。ID 9719 :唯一
 ID 9720 :搜索詞
 9721 :所有者 9722 :
 父名稱 9723 :子對象

9724 :身份證
9725 :作者
9726 :搜索命中說明
9727 :事件時間戳
9728 :事件類型
9729 :事件描述
9730 :搜索命中
9731 :第一扇區
9732 :說明
9733 :哈希 2
9734 :完整路徑
9735 :柔性過濾器 1
9736 :柔性過濾器2

模式按鈕和相關按鈕的命令代碼

122 :遞歸探索
138 :訪問按鈕彈出菜單
172 :切換目錄瀏覽器
186 :切換位置管理器
223 :切換搜索命中列表
224 :切換事件命中列表
225 :磁盤/分區/卷/容器模式
226 :文件模式
227 :預覽模式
228 :細節模式
229 :圖庫模式
230 :日曆模式
231 :圖例模式
232 :同步模式
249 :原始預覽模式
250 :Viewer X-Tension 預覽模式

4 菜單參考

注意 :主菜單中的命令 (文件、編輯、搜索...)始終作為一個整體應用於活動數據窗口 (例如代表一個打開的文件或一個打開的磁盤) ,或應用於仍處於打開狀態的文件/磁盤由用戶指定。它們從不應用於當前在目錄瀏覽器中選擇的文件。這就是目錄瀏覽器上下文菜單的用途。

4.1 目錄瀏覽器上下文菜單

目錄瀏覽器上下文菜單允許用戶直接與當前選擇的文件/目錄交互 ,特別是不是標記的項目。有許多菜單命令

根據所選項目可用。雙擊文件和目錄將根據情況調用“查看”、“瀏覽”或相關的外部程序。

看法

此命令允許使用 Windows 註冊表文件和各種圖形文件格式的內部查看器查看所選文件。如果 X Ways Forensics 附帶的單獨查看器組件處於活動狀態，則所有其他文件都將發送到該查看器。如果不是，將調用第一個安裝的外部程序。NTFS 系統文件始終作為數據窗口打開。

在單獨的窗口中查看文件時，您可以按 (Ctrl+)*Page Dn/Up* 關閉窗口並在新窗口中查看目錄瀏覽器中的下一個文件。如果“查看”窗口顯示圖片並且一次只能查看一張圖片，則當您按光標鍵時，該窗口將更新。如果視圖窗口位於第二台顯示器的中心並且圖庫位於第一台顯示器上，則在跨桌面上尤其有用。

避免必須按 *Enter* 鍵才能查看圖片，然後再按另一個鍵才能關閉“視圖”窗口以將輸入焦點返回到圖庫。

使用內部圖形顯示庫查看圖片時，您可以選擇將此類視圖窗口置於屏幕中央，或者在將它們移動到屏幕上的其他位置後記住它們的左上角位置或中心位置。要做出選擇，請打開視圖窗口的系統菜單（即單擊窗口左上角的圖標）。您還可以決定此類視圖窗口是否應始終位於前台，甚至位於其他應用程序窗口的前面。最後同樣重要的是，您可以選擇大致記住窗口大小。與記住視圖窗口左上角位置一樣只有一個視圖窗口以及只需單擊一個文件即可自動更新視圖窗口的選項結合使用特別有用，以便在您的位置在您自己選擇的屏幕上，您基本上擁有固定的圖片預覽，而數據窗口的下半部分可以顯示預覽模式以外的內容，例如詳細信息模式。

探索

僅適用於目錄和檔案 (ZIP、RAR、TAR...)，此命令允許在目錄瀏覽器中導航到它們。雙擊檔案或目錄也有同樣的效果。允許同時列出目錄及其子目錄內容的命令可以在目錄樹的上下文菜單中找到（在案例數據窗口中，“遞歸探索”）。

觀眾節目

允許將所選文件發送到當前配置的外部程序之一或當前 Windows 安裝中文件的關聯程序。此關聯是根據文件擴展名確定的，這在 Windows 中很常見。

您還可以選擇在臨時選擇的外部程序中打開文件。如果您還沒有為外部查看器程序使用所有插槽，您選擇的程序將被保存為標準的自定義查看器程序，然後在您下次調用相同的菜單命令時也會記住。

打開

在單獨的數據窗口中打開當前選定的文件或目錄。不同於文件 |打開，在操作系統的幫助下，可以像在任何其他應用程序中一樣打開文件。這是一個可靠的取證操作，因為它不會更新任何時間戳等，因為操作系統和讀取文件的邏輯被繞過了來自正確磁盤扇區的內容在 WinHex 本身中為各種文件系統實現。但是，不能對以這種方式打開的文件進行任何更改。在目錄的情況下，目錄的數據結構將被打開。

打印

如果單獨的查看器組件處於活動狀態，您可以選擇文件（甚至目錄）進行打印。

您可以不間斷地打印多個選定的文檔/無需單擊每個文檔後的某處，可以選擇與子對像一起打印（例如，電子郵件附件及其各自的電子郵件消息）。可選的封面包含打印作業開始的日期和時間以及選定的元數據，例如文件名、路徑、證據對象標題、文件大小、描述、時間戳、註釋……

可以在封面底部打印文件預覽。此預覽的格式取決於預覽模式下查看器組件的設置，例如“最適合”或“實際像素”或“適合窗口寬度”等。這是一個三態復選框。如果只選中一半，則預覽會以更淺的顏色打印，以節省墨水/碳粉或提高元數據字段的可讀性（如果您輸出許多元數據字段並且它們溢出到預覽中）。封面由 X-Ways Forensics 本身打印，包含實際文檔的後續頁面由查看器組件打印。您可以只打印封面或所選文件或兩者。封面頁的標題行是可選的，它指定哪個用戶以及哪個程序和版本創建了打印作業。如果您希望向證人或不應該知道檢查者用戶名的嫌疑人出示打印輸出，這很有用。

另一種選擇是讓 X-Ways Forensics 在第一頁上打印文件名和路徑。此選項不受與查看器組件可選打印的標題（“打印標題”，作業名稱 = %p）相同的路徑長度限制的約束。為避免路徑在第一頁上打印兩次，讓 X-Ways Forensics 或查看器組件打印它，而不是同時打印。

恢復/複製：參見單獨的主題

出口清單

需要專業執照。將有關目錄瀏覽器中所選項目的數據導出到製表符分隔的文本文件或 HTML 文件，這些文件可以在任何 Web 瀏覽器中輕鬆查看，也可以導入並進一步處理，例如在 MS Excel 和 MS Word 中。第三個選項（搜索命中列表除外）是 XML 文件。該列表可以選擇的格式複製到剪貼板，例如將其直接粘貼到外部編輯的報告中。可以自由選擇要導出的列。甚至搜索命中列也可以導出，每個實際命中都有文本上下文，搜索詞本身可以用黃色背景顏色在視覺上突出顯示（不推薦輸出到 MS Excel）。例如，您可以選擇將結果拆分為多個文件，以避免 Internet 瀏覽器會阻塞的巨大 HTML 文件

上。

有一個選項可以從磁盤/圖像中複製文件並從 HTML 輸出中鏈接它們。可以在“名稱”列中找到這些鏈接。確切的行為取決於兩個案例報告選項：“在之後命名輸出文件”和“在父.eml 文件中嵌入附件”。此選項是報告表常規輸出的有趣佈局替代方案，也是恢復/複製命令的替代方案。

在名稱列中，您可以輸出原始名稱，如果存在替代名稱（如果該框已完全選中）或兩者（如果復選框處於中間狀態），則可以輸出替代名稱。

當導出文件或目錄列表及其按完整路徑排序的子對象時，子對象直接跟隨其各自的父對象，以 TSV 或 HTML 格式，稱為“縮進”的選項允許縮進子對象的名稱，以便在輸出中很容易看出哪些對像是哪些其他對象的子對象，即使不查看或者甚至不包括可能很長的完整路徑作為附加列也是如此。縮進可以很強烈（完全檢查）或不那麼強烈（一半檢查）。

導出列表命令會記住其自己的符號設置，這與常規選項中的符號設置不同。這很有用，因為您選擇的要導入數據的數據庫或電子表格程序可能不喜歡您希望在目錄瀏覽器中看到的格式（例如時間戳中的秒分數、時區偏差、日期中的工作日、日期和時間之間的分隔符，整數數字分組，...）。當導出列表對話框窗口在屏幕上時，後台的目錄瀏覽器反映導出列表命令的符號設置，作為一種預覽。

複製 :提取的文本

允許將已解碼或 OCRed 的文本從選定文件複製到其他位置。如果您只需要這些文件，則範圍可以限於特別需要 OCR 的文件（即圖片和某些 PDF）。提取的文本可以在卷快照中進行內部緩衝，用於將來的邏輯搜索或索引以及搜索命中的上下文預覽。它可以複製到相應文件的評論中（特別適用於從圖片中進行 OCR 的少量文本），例如將文本包含在案例報告或導出的列表中，可以選擇帶有解釋性前綴，如 [OCR] 或 [Extracted文本]。提取的文本也可以作為子對象（文本文件）輸出。或者可以將其收集在您自己的存儲設備上的單個文本文件中，或複製到剪貼板中，以上的任意組合也是可能的。

提取連續幀

專門從所選視頻的定義部分中提取所有幀。如果視頻的某個部分很受關注並且您需要仔細檢查某些幀中的視覺細節或將它們包含在報告中，則此功能很有用。您可以指定要提取多少個連續幀以及從哪一秒開始。您需要覆蓋特定時間段的幀數可以從元數據單元格中顯示的幀速率中扣除（fps = 每秒幀數）。請注意，根據視頻中關鍵幀（又名 MPEG 中的 I 幀）的頻率，開始秒數的解釋可能非常粗略。MPlayer 只能根據關鍵幀搜索視頻文件。例如，如果某個視頻文件僅每 4 秒包含一次關鍵幀，則提取的開始秒數最多可能會偏移 4 秒。當您輸入所需的幀數或開始秒數時，請記住這一點。也就是說，要安全

一邊，提取比您實際需要更多的幀，也許從更早的開始開始。

這些幀以 JPEG 文件的形式保存在您自己驅動器上您選擇的目錄中，您可以在 X-Ways Forensics 之外查看它們。如果願意，您當然可以將最相關的幀作為子對象附加到卷快照中的原始視頻文件。默認情況下，幀不會存儲在卷快照中，因此卷快照的大小不會因可能幾乎不相關和冗餘的圖片而不合理地膨脹。如果輸出目錄已經包含提取的幀，則具有相同相對幀編號的文件將被覆蓋。每次提取的相對幀編號始終以 00000001 開頭，並隨每一幀遞增。如果需要更強的壓縮或更好的質量，您可以調整 JPEG 壓縮。（當然，您通常不能期望質量非常好，因為視頻通常已經高度壓縮。）

Report Table Association :對於Report Tables，見上

編輯評論

需要法醫執照。使用此命令向目錄瀏覽器中的項目添加評論，或者編輯或刪除現有評論。輸入評論後，您可以方便地設置過濾器，以便僅顯示評論的項目或僅顯示具有特定評論的項目，例如具有特定相關性的項目。

編輯元數據

需要法醫執照。允許在提取元數據後編輯文件的元數據字段。如果您希望在報告中包含選定的元數據（不是所有提取的元數據），這很有用。

在目錄瀏覽器中選擇的項目中優化卷快照和同步搜索

標記/取消標記項目

需要法醫執照。標記文件意味著在視覺上突出顯示它們（在目錄瀏覽器項目的開頭放置一個藍色方塊），出於各種原因，例如將它們標記為相關，或記住排序列表中的位置，或將卷快照細化限制為標記文件。不要將標記與選擇混淆。

排除/包括

您可以排除選定的項目（按 Del）或所有標記或所有未標記的項目。如果確實被過濾掉，目錄瀏覽器、圖庫視圖以及可以從目錄瀏覽器上下文菜單運行的所有命令都會忽略排除的文件。如果您只被允許檢查某些目錄的內容，您可以首先排除所有其他目錄中的所有文件以確保這一點。優化卷快照可以限制為未排除的文件。只有在目錄瀏覽器選項中啟用了相應的過濾器，才會實際過濾掉排除的項目。如果未過濾掉，它們將以灰色列出，並且可以通過目錄瀏覽器上下文菜單或按 Shift+Del 再次包含。

在列表中查找重複項： cf 。主題重複文件檢測

過濾重複項

僅當哈希值可用於所選文件和其他文件時，才能夠過濾目錄瀏覽器中當前也列出的單個選定文件的副本。實際上當時過濾那個哈希值，因此不依賴於先前使用上述命令“查找列表中的重複項”對重複文件的大量識別。在 X-Ways Investigator 中，不會顯示也無法計算實際哈希值，但它們是從帶有文件哈希值的證據文件容器中導入的，可用於識別重複文件。

過濾相似文件

使用“結構類型”過濾器查找相同類型的文件，這些文件可能由相同的應用程序或設備以相同的設置或出於相同的目的等大致在同一時間創建。此功能僅在“結構類型”列已填充，用於支持的文件類型。

在搜索命中列表中，您可以

1) 永久刪除選定的搜索命中，
2) 永久刪除重複的搜索命中。如果

搜索命中具有相同的物理偏移量，或者如果它們沒有物理偏移量，但它們的邏輯偏移量和相應的內部文件 ID 相同，則搜索命中被視為重複。如有疑問，X-Ways Forensics 將保留較長的搜索命中（例如，“Smithsonian”比“Smith”更具體）並支持現有文件中的搜索命中。

3) 調整大小：允許調整大小或重新定位選定的搜索結果。例如，如果您正在搜索標識某種數據庫中的記錄的簽名，並且您獲得了這些簽名的許多搜索結果，但您真正感興趣的是簽名後面的記錄數據，並且您希望將其導出數據，然後您可以以合適的方式調整搜索命中的偏移量和長度。此外，您可以在導出搜索結果之前擴大搜索結果本身，而不是使用“導出列表”命令圍繞搜索結果導出更多上下文。效果在搜索命中列表的搜索命中預覽中立即可見（但不一定立即在數據窗口下半部分的突出顯示中）。

4) 搜索命中列表中的另一個上下文菜單命令允許將搜索命中轉換為雕刻文件。

如果您希望將搜索結果作為文件包含在報告中，將它們添加到報告表、對其進行評論、打印內容、恢復/複製它們等，這將很有用。請注意，具有物理和邏輯偏移量的搜索結果將在扇區級別進行雕刻，並將出現在雕刻文件的虛擬目錄中。僅具有邏輯偏移量的搜索命中將被刻在找到它們的文件中，並將顯示為子對象。文件的解碼文本中的搜索命中以及目錄瀏覽器列中的搜索命中不能被雕刻並且將被省略。

5) 分配給其他搜索詞：能夠通過將選定的搜索結果移至其他搜索詞（現有的或新的搜索詞）來對其進行分類。例如，如果您在運行搜索詞“invoice”的搜索時獲得多個相關匹配，並且一些匹配與其他匹配的相關方式不同，那麼您可以將它們分配給其他搜索詞，例如“Invoice ABC Ltd.”、“發票 XYZ 公司。”等等。那些新創建的搜索詞將出現在搜索詞列表中，但它們的功能

更像是類別，因為它們本身並沒有被逐字搜索。

導航

此子菜單中的命令允許根據估計的相關性（參見元數據提取）對文件進行排序，或者避免在排序上浪費時間。

導航命令組還允許在通常更技術的級別上與當前選定的文件進行交互。它允許直接定位定義文件的文件系統中的數據結構（例如 NTFS 中的 FILE 記錄，Ext2/Ext3/Ext4 中的 inode，FAT 中的目錄條目）。

導航菜單還允許生成分配給所選文件或目錄的所有簇的列表。從該列表窗口的上下文菜單中，可以將集群列表導出到文本文件。上下文菜單還提供了縮短列表並通過省略片段中間的集群來加速其創建的選項。省略號表示遺漏。此選項僅在您下次生成集群列表時生效。如果您只對每個連續系列的集群（=每個片段）從何處運行到何處感興趣，則簡潔表示很有用。

查找父對象：導航到並選擇所選對象的父對象。相當於按退格鍵。子對象可以是目錄中的普通文件、電子郵件存檔中的電子郵件消息、電子郵件消息中的文件附件、文檔中的圖片或壓縮存檔中的文件等。

查找相關對象：如果所選文件或目錄存在相關對象，此命令可讓您方便地導航到所謂的相關對象。或者，您可以按 Shift+Backspace。

查看其目錄中的選定項目：將向您顯示其兄弟姐妹中的選定文件或目錄。

有助於快速檢查同一目錄中是否有更多值得注意的文件，或者當您 在上下文中看到文件時更好地理解文件的功能。

從卷根目錄中查看所選項目：將向您顯示同一卷中所有其他文件中的所選文件，從該文件系統的根目錄遞歸探索。例如，查看同一文件系統中是否有任何具有相同名稱、相同 ID（例如卷影副本的先前版本）、相同所有者、相同發件人或類似時間戳等的文件（只需相應排序）。

這兩個命令也可以在案例根窗口和搜索命中列表中使用（因此之前的“轉到目錄瀏覽器中的文件”命令已過時）。請記住，您可以單擊工具欄中的“後退”按鈕以方便地返回到上一個視圖。

Seek Path 有助於在目錄瀏覽器中找到您指定其完整路徑的文件或目錄。

“**Seek Int. ID**”可以方便地查找具有給定內部 ID 的項目，無論是文件還是目錄。如果過濾器阻止列出該項目，所有過濾器將自動停用。

“**Seek Item #**”將跳轉到當前列表中具有指定位置的項目。當您將鼠標光標懸停在文件或目錄的圖標上時，將顯示列表中任何項目的位置。

分類

卷快照中的文件默認被認為是未知的。根據哈希數據庫匹配、基於 X-Tensions、採用證據文件容器中的數據、使用此子菜單以及其他方式，此狀態可能會更改為不相關、值得注意或未分類。可以在“分類”列中查看狀態。

優化卷快照、同步搜索、運行 X-Tensions

這些命令可從主菜單中獲知。從目錄瀏覽器上下文菜單中，它們可以應用於選定的文件。

包含在哈希數據庫中

使用普通文件哈希值或塊哈希值或 PhotoDNA 哈希值，直接在內部哈希數據庫中創建當前選定文件和目錄及其子目錄的哈希集。對於普通散列值，可以選擇一步創建多個散列集，其中所選文件的散列值被放入以每個文件的報告表關聯命名的散列集中。如果您在一種情況下使用報告表（例如，基於不同類型的 CP）對重要文件進行分類，並希望稍後在其他情況下再次快速識別相同文件，並自動查看您最初分配的類別，這將很有用，因為哈希集名稱。

該複選框標記為“在報告表關聯之後命名，如果有的話”。如果所選文件沒有任何報告表關聯，則其哈希值將分配給您指定的哈希集，就像您沒有選中該複選框一樣。

此命令還可用於使用所選文件的 PhotoDNA 哈希值創建單獨的文件，或者僅使用存儲在卷快照中的註釋更新 PhotoDNA 哈希數據庫中文件的文件描述。

附加外部文件/目錄

需要法醫執照。能夠將一個或多個外部文件或包含子目錄的目錄附加到卷快照，並讓 X-Ways Forensics 像卷快照中的常規文件一樣處理它們。如果您需要翻譯、轉換或解密原始文件，並希望將結果重新集成回原始卷快照、原始路徑中，以進行進一步檢查、報告、過濾、搜索等，這很有用。此類文件將完全由 X-Ways Forensics 附加後，將其內容複製到案例的內部證據對象子目錄，以便可以刪除源文件。

您將被要求將您附加的文件按實際情況分類，例如，在 X-Ways Forensics 之外製作的視頻靜止圖像、從 X-Ways Forensics 之外的電子郵件存檔中提取的電子郵件、OLE2 對象、附件各種（特別是 PDF 文檔）等。如果正確分類為視頻靜止圖像，則附加的圖片將用作相應父視頻文件的預覽。分類可以在描述欄中看到。

當附加單個外部文件並按住 Shift 鍵時，X-Ways Forensics 會提出一個

該文件的新名稱基於所選文件的名稱，附件將添加到同一目錄中。否則將使用文件的外部文件名，它們將成為所選對象的子對象。稍後仍然可以隨時重命名卷快照中的虛擬文件。

將外部目錄附加到卷快照時，系統會提示您是否也應附加所選目錄本身或僅附加其內容。通常 X-Ways Forensics 在卷快照的新虛擬目錄的子目錄中創建虛擬文件。但是，可以選擇將現有目錄中的文件容納在目錄樹中相同位置的同名卷快照中。如果您從圖像中復制整個目錄結構以轉換/解密/翻譯/... X-Ways Forensics 之外的文件，然後想要將結果帶回捲快照並在原始文件旁邊查看編輯後的文件，則很有用相應子目錄中的對應項。例如，如果您希望使用 Adobe Acrobat 對 X-Ways Forensics 認為不可搜索的 PDF 文檔進行 OCR 和轉換，這會有所幫助。

X-Ways Forensics 可以選擇在卷快照（創建、修改和/或訪問）中採用附加文件的時間戳。如果您確定時間戳是原始的而不是您自己的任何文件複製/解碼/解密活動等的結果，則可以使用它。

改名

允許您重命名卷快照中的虛擬目錄和虛擬附加文件，或者如果按下 Shift 鍵甚至是普通文件。雖然後者在處理原始證據時在法醫上並不完全可靠，但在特殊情況下證明這很有用，例如，如果文件名或目錄名太長而無法從圖像中複製文件等。原始文件名將保留為替代文件名。請注意，這不會重命名文件系統中的文件（磁盤或映像中沒有任何更改！），只會在卷快照中重命名，即 X-Ways Forensics 中關於文件系統的內部數據庫。

指定類型

能夠自己指定所選文件的類型。如果您希望以 X-Ways Forensics 未知的單獨方式識別類型或子類型，例如以後能夠按這些類型進行過濾，則很有用。例如，將以數字方式存儲的傳真的 TIFF 圖片歸類為“傳真”類型怎麼樣？請記住，您可以在 File Type Categories.txt 中定義自己的文件類型。

調整大小

通過文件頭簽名搜索找到的文件和刻在其他文件中的文件可以由用戶手動重新定義。您可以使用相對偏移更改 (+/-) 重新定位此類文件，和/或調整它們的大小，使用絕對新大小或正負相對大小調整（單擊箭頭按鈕進行切換）。您可以使用相同的設置同時調整多個文件的大小。

安全擦拭

在目錄瀏覽器中選擇的文件和目錄可以在 WinHex (不是 X-Ways Forensics) 中安全地擦除。文件邏輯部分 (即不包括文件鬆弛部分) 和目錄簇 (例如，包含 NTFS 中的 INDX 緩衝區和 FAT 中的目錄條目) 中的數據將被擦除/覆蓋為您選擇的十六進制值模式。文件在其文件系統中的存在狀態不會改變，即不會被標記為已刪除，集群不會被釋放等。沒有文件系統級別的元數據，如時間戳或屬性將被更新，因為沒有操作系統文件級別使用寫命令。不會更改文件系統數據結構，也不會刪除文件名，只會覆蓋文件內容。唯一的例外是，在 NTFS 的情況下，可以選擇額外刪除 MFT 中所選文件的文件記錄。無法刪除存檔中壓縮的文件或其他文件中的一般文件（例如電子郵件和電子郵件存檔中的附件）。不會刪除已知其簇已被重複使用的先前存在的文件。請注意，通過擦除已刪除的文件，您可能會擦除屬於其他文件的簇中的數據，因此如果您想避免這種情況，請僅選擇現有文件（假設文件系統一致）。另請注意，通過擦除雕刻的文件，您可能會擦除過多或不足的數據，具體取決於檢測到的文件大小以及文件最初是否碎片化。請注意，擦除目錄，即擦除分配給目錄的簇中的數據，將導致該目錄中的現有文件成為孤立文件。更典型的情況是，如果用戶仍希望使用文件系統，則他們僅使用此功能擦除文件的內容，而不擦除目錄的內容（數據）。

例如，如果將圖像副本轉發給不允許查看某些文件內容的案件中的調查員/檢查員/其他方，則很有用。如果您在清除這些文件後必須將發現兒童色情內容的計算機媒體歸還給所有者，這也很有用。如果您正在準備要發布的用於培訓目的的圖像，以及如果您想追溯刪除受版權保護的文件（例如操作系統或應用程序文件）的內容，這也很有用。

成功擦除的文件和無法成功擦除的文件都將添加到單獨的報告表（處理案件時，僅限法醫許可證），您可以通過該表進行過濾以驗證結果。

將命中標記為顯著

在搜索命中列表中，用黃色標記標記選定的命中，並將其包含在重要搜索命中列表中。您也可以按空格鍵將命中標記為值得注意或刪除該標記。在調用菜單命令時按住 Shift 鍵會從所有選定的搜索結果中刪除“顯著”標誌。

包含在報告中

在搜索命中列表中，用綠色網格圖標標記要包含在案例報告中的選定搜索命中。

4.2 案例數據窗口上下文菜單

一些命令：

導出子樹 :案例數據窗口中的此上下文菜單命令允許您在 Unicode 文本文件中導出所選子樹的偽圖形表示 ,最好使用固定寬度的字體查看 。導出的樹反映了子目錄的當前狀態 (展開或折疊) 。如果在案例樹中右鍵單擊目錄時按住 Ctrl 鍵 ,則菜單命令可用於證據對象和目錄 。請記住完全遞歸地展開要導出的樹的一部分 ,您可以單擊該部分的根並按數字鍵盤上的星號 (乘法)鍵 。

附加外部文件 :此命令允許同時自動將外部文件作為子對象附加到多個證據對像中的原始副本 (在解密、翻譯、轉換、OCRing 等之後) ,如果它們以唯一 ID 命名的話原始文件 。

(忽略文件擴展名。)當您使用恢復/複製命令從圖像中複製文件時 ,您可以使用唯一 ID 命名文件 ,並且您不需要保留路徑 ,因為唯一 ID 已經完全識別文件。如果您希望將外部工具應用於具有超長路徑問題的複製文件 ,如果您希望將結果返回到卷快照中 ,則很有用 。

附加外部文件時 (例如在解密、轉換、翻譯等之後) ,您有四種選擇 :1) 附加文件可以成為原始文件的子對象

或者

2) 附加文件可以成為原始文件的兄弟文件 (顯示在它旁邊 ,在同一目錄中)

或者

3) 附件可以替換原文件 (原文件不存在)

或者

4) 附加文件可以替換原文件 ,如果還需要 ,原文件可以成為新文件的子對象 。

您可以為普通文件和電子郵件附件分別選擇附件方式。後三種方法對電子郵件附件特別有用 ,因為在恢復/複製那些 .eml 文件時 ,只有 .eml 文件的直接子對象嵌入到父 .eml 文件中。因此 ,如果您希望將附件的解密/轉換/翻譯版本嵌入到 .eml 文件中 ,該版本不應成為孫對象。如果您希望同時嵌入原始版本和新版本 ,請將它們設為兄弟姐妹。如果您不需要嵌入原始版本 ,請將其完全替換或僅將其保留為新版本的子對象 (即 .eml 文件的孫對象) 。

附加文件採用原始文件的分類 ,例如作為提取的電子郵件消息或 OLE2 對象。如果原始文件沒有特殊分類 ,附件將被簡單地標記為附件 。

導出文件以供分析 :案例數據窗口中的此菜單命令可應用於整個案例 ,並從那裡應用於選定的證據對象 ,或僅應用於活動證據對象。它使用文件外部分析接口調用外部自動化分析工具 ,如DoublePics 。

目錄也有一個上下文菜單 。右鍵單擊目錄時顯示

取決於常規選項以及您是否同時按住 Shift 鍵。否則右鍵單擊目錄意味著遞歸地瀏覽它。

4.3 數據窗口上下文菜單

當您右鍵單擊文件或磁盤的十六進制編輯器顯示（由偏移列、十六進制列、文本列組成）時，您將獲得一個上下文菜單，允許您定義塊的邊界（開始和結束）和調用更多適用於該塊的命令：

添加到用戶搜索命中：僅限取證許可。允許您手動定義搜索命中。

每當您遇到一些相關文本時，例如在磁盤/分區/卷模式下漂浮在可用空間中或在文件模式下在某個文件中，您可以將其選擇為塊並右鍵單擊該塊將其添加為 so -稱為用戶搜索命中（即程序未找到的某種搜索命中）。您可以將搜索命中分配給任意命名的搜索詞/類別。例如，如果您發現的內容與嫌疑人 A 相關，則將其作為搜索命中分配給以嫌疑人 A 命名的搜索詞。如果還與嫌疑人 B 相關，您還可以將其分配給另一個搜索詞。

您還可以將其分配給您用於自動搜索的真實搜索詞。

用戶搜索命中可以方便地列在搜索命中列表中並很好地從搜索命中列表中導出，就像普通（自動生成的）搜索命中一樣。為了與普通搜索命中區分開來，在搜索命中描述欄中，用戶搜索命中用星號 (*) 標記。您可以在定義用戶搜索時自行指定正確的代碼頁，這對於正確顯示文本可能是必不可少的。如果您在文件模式下定義用戶搜索命中，則它們與卷快照中的對象相關。用戶搜索命中是向前兼容的，即舊版本（v16.2 及更高版本）也可以看到由 v16.6 創建的用戶搜索命中。

添加塊作為虛擬文件：僅限取證許可證。請參見編輯菜單。

添加位置：允許您記住當前定義的塊指示的位置，在一般位置管理器或證據對象的位置管理器中（處理案例時，如果您右鍵單擊在證據對象，僅限法醫許可證）。使以後更容易再次找到相同的位置，並且可用於很好地突出顯示和解釋（使用工具提示）您正在分析/嘗試進行逆向工程等的特定格式的文件或記錄的結構。

如果搜索命中在文件模式中突出顯示（請參閱常規選項），您也可以通過上下文菜單。

您還可以從這裡獲得完整的編輯菜單。

4.4 文件菜單

新建：此命令用於創建文件。該文件主要以默認編輯模式打開。

您必須指定所需的文件大小。在 X-Ways Forensics 中，您還可以使用此命令為 .e01-Images 創建虛擬段。

打開 :讓您打開一個或多個文件。如果“選項”菜單中未預先確定，您可以選擇一種編輯模式。

還允許通過單擊文件選擇對話框中標有“設備...”的按鈕將物理磁盤、分區和卷作為文件打開。您可以輸入設備路徑，例如 \\.\PhysicalDrive1（對於硬盤 1）

\\?\Volume{12345678-9abc-11a1-abcd-0123456789ab}（對於具有該 GUID 的卷）

\\.\C:（對於安裝為盤符 C: 的卷）

此功能允許打開未安裝為驅動器號的卷。要獲得 Windows 已知卷的概覽，請在命令提示符窗口中鍵入“mountvol”。您還可以嘗試打開 Windows 支持的特殊設備，例如磁帶和轉換器（未測試）。這也是您可以打開路徑和名稱已知的備用數據流的方法，這些數據流無法通過普通文件 | 打開 | 打開對話框，而不打開它們所在的卷。

將硬盤作為文件打開可能很有用，例如，如果您希望克隆該磁盤並且源磁盤和目標磁盤具有不同的扇區大小（儘管扇區不匹配，首先克隆硬盤是否有意義取決於數據）。當被視為文件時，沒有定義的扇區大小，因此扇區大小不匹配的可能性不大。設備文件也可以像圖像一樣被解釋為磁盤。

保存 :將當前顯示的文件保存到磁盤。在就地編輯模式下，不需要使用此命令。使用磁盤編輯器時，此命令名為“Save Sectors”。

另存為 :以不同的名稱保存當前顯示的文件。

創建磁盤映像/製作備份副本 : cf。“圖像和備份”

創建/驗證骨架圖像 : cf。“骨架圖像”

Restore Image :選擇一個你想恢復的圖像，即你想複製回原始介質或其他介質的扇區，或者選擇一個或 WinHex 備份 (.whx) 文件，你想恢復其內容（可以是文件或磁盤扇區）。在圖像的情況下，圖像將被預設為克隆磁盤窗口中的源（具有專業許可證或更高版本，已解釋）。只有擁有專業許可證或更高跨度的原始圖像才能恢復。可以使用任何類型的許可證恢復跨區 WinHex 備份。

備份管理器 : cf。“備份”

執行 :如果可執行則執行當前文件，否則執行相關程序。

打印 :使用此命令打印文件、磁盤扇區或 RAM 內容。通過偏移定義打印範圍。您可以選擇並設置打印機。選擇用於打印的字符集並接受或更改建議的字體大小。推薦的字體大小計算如下：打印分辨率（例如 720 dpi）/ 6（例如 = 120）。如果需要，您可以輸入將在最後打印的註釋。

如果您需要更靈活的打印，您可以定義一個塊並使用“編輯”複製它

>Copy->Editor Display”作為十六進制編輯器格式的文本到剪貼板。您可以將其粘貼到您最喜歡的文字處理器中。它應該在“Courier New”中看起來很完美，10 pt。

屬性：允許您在自己的 Windows 系統中編輯文件或目錄的大小、時間戳和屬性。可變屬性有 :A（待歸檔）、S（系統）、H（隱藏）、R（只讀）、X（不可索引）、T（臨時）和 ~（稀疏）。在任何區域（大小、時間戳或屬性）中輸入新值後，只需按ENTER按鈕即可應用它們。單擊帶省略號的按鈕選擇一個新文件，或直接在該按鈕旁邊的編輯框中輸入路徑和名稱，然後按ENTER鍵。後者也適用於目錄。

請注意，設置或刪除稀疏屬性不一定會改變已分配簇的分配狀態，但當您通過在同一對話框窗口中設置更大的文件大小來擴展文件時，肯定會對新分配的簇產生影響。

打開目錄：打開一個代表您自己計算機上的目錄的窗口，並允許您查看其所有文件和子目錄。

打開文件：該命令用於一次打開多個滿足特殊要求的文件。

選擇要在其中打開文件的文件夾。可選擇瀏覽器文件夾。您可以指定一系列文件掩碼（如“w*.exe;x*.dll”）。還有一個開關允許只打開那些包含特定文本或特定十六進制值的文件。為此，應要求顯示標準搜索對話框。如果 WinHex 未設置為在只讀或就地編輯模式下工作（這可以在選項菜單中完成），您可以選擇一種編輯模式。

Save Modified Files：將所有已更改的文件寫入磁盤。

保存所有文件：將所有未在查看模式下打開的文件寫入磁盤。

退出：使用該命令結束 WinHex。系統將提示您保存對文件和磁盤的任何修改。

4.5 編輯菜單

撤消：如果激活了相應的撤消選項，則撤消上次修改。

剪切：從文件中刪除當前塊並將其放入剪貼板。塊之後的數據被拉到前一個塊的開頭。

複製塊/全部/扇區：·正常：將

當前塊/整個文件/當前扇區複製到剪貼板。這

剪貼板的內容可以稍後粘貼或寫入。

·作為Unicode/ANSI：專門從文本列複製文本為UTF-16 Unicode，即使文本列未以Unicode顯示，或者專門複製為ANSI編碼文本，即使文本列未顯示為ANSI ASCII。

·進入新文件：將數據直接複製到新文件中（不通過剪貼板）。例如，

此命令可用於從磁盤扇區恢復丟失的文件。

·十六進制值：將數據複製為串聯的十六進制值。

編輯器顯示 :將數據複製為文本 ,格式如同在十六進制編輯器中顯示一樣 ,即
帶有偏移量、十六進制和文本列。 · GREP

Hex :將數據複製為 GREP 語法中的十六進制值。 · C/Pascal 源代
碼 :將數據作為C/Pascal 格式的源代碼複製到剪貼板中。

粘貼剪貼板 :在文件的當前位置插入剪貼板內容。該位置之後的文件數據向前移動。

寫入剪貼板 :將剪貼板內容複製到當前位置的當前文件。該位置的數據被覆蓋。如果遇到文件末尾 ,文件大小會增加 ,以便剪
貼板內容找到位置。

將剪貼板粘貼到新文件中 :創建剪貼板內容的新文件。

清空剪貼板 :此命令用於釋放剪貼板使用的內存。

刪除 :從文件中刪除當前塊。塊之後的數據被拉到前一個塊的開頭。剪貼板不受此命令的影響。如果塊在所有打開的文件中定
義相同 (即它以相同的偏移量開始和結束) ,則此命令甚至可以同時應用於所有打開的文件。

粘貼零字節 :使用此命令在文件的當前位置插入零字節。

添加塊作為虛擬文件 : (僅限取證許可證)如果您在卷/分區/磁盤/文件模式下手動定義塊 ,此命令允許您將其作為雕刻文件添
加到卷快照 ,或者 (在文件模式下) 作為原始文件的子對象。如果您希望將特定區域中的數據 (例如 HTML 代碼或在自由
空間中發現的電子郵件消息) 視為一個文件 ,例如查看它、專門搜索它、評論它、將它添加到報告中 ,這很有用 ,等。如果您在文
件模式下手動在另一個文件中雕刻一個文件 ,生成的文件將在屬性中標記。列作為摘錄 ,可以這樣過濾。主機文件中已經雕刻
的區域在文件模式下突出顯示。在繼續查看該主機文件時 ,提醒用戶他或她是否已經從文件中創建了摘錄以及在何處 (例如 ,
從一個大的可用空間虛擬文件中) 很有用。

定義塊 :可從菜單和狀態欄訪問此功能。對話框允許您指定所需的塊邊界或大小。此命令也可以應用於所有打開的文件。

全選 :將當前文件的開頭和結尾定義為其塊限制。

疊加扇區 :見下文

轉換 : cf轉換

修改數據 :見下文

填充塊/文件/磁盤扇區 :見下文 (擦除和初始化)

4.6 搜索菜單

同時搜索 :見上文

索引 ,在索引中搜索 :見上文

優化指數 :見上文

導出單詞列表 :創建索引後可用。允許將索引中所有單詞的列表保存到文本文件中。在該列表中，索引文件中出現的每個單詞都將出現，並且只包含一次。對自定義字典攻擊很有用。

查找文本 :此命令用於在當前文件、磁盤或 RAM 部分中搜索最多 100 個 ASCII 字符的指定字符串（參見搜索選項）。僅支持 0x00...0xFF 範圍內的 Unicode 字符。如需更強大的搜索變體，請嘗試同時搜索。

查找十六進制值 :此命令用於搜索最多 100 個雙字符十六進制值的序列（參見搜索選項）。

替換文本 :使用此命令將出現的指定字符串替換為另一個字符串（每個字符串最多 100 個 ASCII 字符），參見。替換選項。僅支持 0x00...0xFF 範圍內的 Unicode 字符。

替換十六進制值 :功能與替換文本命令完全相同，但應用於十六進制值序列（最多 100），參見。替換選項。

組合搜索 :提供複雜的搜索機制。在當前文件和第二個文件中搜索公共偏移量，其中每個文件包含指定的相應十六進制值。

整數值 :輸入一個整數（在有符號 64 位整數數據類型的限制內）。該函數在當前文件中搜索數據，可以解釋為這個整數。

浮點值 :輸入一個浮點數（例如 $12.34 = 0.1234 * 10^2 = 0.1234E2$ ）並選擇一個浮點數據類型。該函數在當前文件中搜索數據，可以解釋為這個浮點值。

文本段落 :使用此命令查找一系列字母（az、AZ）、數字 (0-9) 和/或標點符號。例如，如果您打算翻譯隱藏在具有可執行代碼的文件中某處的文本段落，這將很有用。

通過指定識別字符序列的長度來設置搜索的靈敏度。單擊“容忍 Unicode 字符”以強制算法接受兩個字符之間的零字節。

繼續全局搜索 :該命令用於在下一個文件中繼續全局搜索操作（即對所有打開的文件應用搜索操作）。

繼續搜索 :讓您在當前文件的當前位置繼續搜索操作。

4.7 導航菜單

Go To Offset :將當前位置移動到指定的偏移量。通常這是相對於文件的開頭（偏移量 0）完成的。您還可以相對於當前位置（向前或向後）或從文件末尾（向後）移動光標。可以按字節（默認）、字（2 個字節）、雙字（4 個字節）、記錄（如果已定義）或扇區指定偏移量。按 F11 重複上次位置移動。

轉到頁面/扇區 :瀏覽到指定的頁面、扇區或簇。請注意，FAT 驅動器上的數據區從簇 #2 開始。Go To Sector 對話框，當應用於物理磁盤時，可選擇跳轉到相應分區窗口內的指定扇區，以便您可以立即看到相應簇的分配狀態。僅適用於普通分區，不適用於 Windows 動態卷或 LVM2 卷。

Go To FAT Entry/FILE Record :分別跳轉到 FAT 驅動器上文件分配表中的某條記錄或 NTFS 驅動器上主文件表中的某條 FILE 記錄。

移動塊 :向前或向後移動當前塊選擇（不是塊內的數據）。以字節為單位指定距離。按 ALT+F11 重複上一個塊移動，按 SHIFT+ALT+F11 反向移動。此命令可能有助於編輯由固定長度的同類記錄組成的文件。

WinHex 和 X-Ways Forensics 在文件或磁盤中保留偏移量跳躍的歷史記錄，並允許稍後在鏈中來回移動。僅限取證許可證：使用後退和前進，您還可以方便地返回到某個目錄瀏覽器設置。這考慮了：探索路徑、遞歸或非遞歸、排序標準、所有過濾器的開/關狀態、一些過濾器的設置、一些目錄瀏覽器選項。後退和前進命令還允許在窗口之間切換時再次激活先前活動的數據窗口。

去...

Beginning Of File :顯示當前文件的第一頁，並將當前位置移動到偏移量 0。

End Of File :顯示當前文件的最後一頁並將當前位置移動到最後一個字節（偏移量 = 文件大小 - 1）。

Beginning Of Block :將當前位置移動到當前塊的開頭。

End Of Block :將當前位置移動到當前塊的末尾。

標記位置 :標記當前位置，以便您以後可以再次找到它。

刪除標記 :從屏幕上刪除標記。

Go To Marker :將當前位置移動到由 Mark Position 設置的標記。

職位經理 :見下文

4.8 查看菜單

僅文本顯示 :隱藏十六進制列並使用編輯器窗口的整個寬度進行文本顯示。

僅十六進制顯示 :隱藏文本列並使用編輯器窗口的整個寬度來顯示十六進制數據。

字符集 :選擇文本顯示的字符集或代碼頁。您還可以使用SHIFT+F7切換活動字符集/代碼頁。默認設置為 ANSI ASCII。它使用最有效和最簡單的顯示方法，僅調用最簡單的 Windows API 函數，並且它似乎總是根據代碼頁 1252 顯示字符解釋，即使 Windows 中的區域設置不同，如果在字體選擇對話框（可訪問通過常規選項）選擇“西方”腳本。

為了更好地利用寬屏顯示器並協助審查員，尤其是亞洲的審查員，他們可能會在同一案例中遇到以許多不同字符集和代碼頁編碼的文本，可以在十六進制編輯器的文本顯示中看到二進制數據的多種文本解釋：同時取決於許可證類型。這對於遍歷使用密碼編碼的 Outlook PST 文件的原始數據、能夠同時讀取編碼的 ANSI 文本、編碼的 Unicode 文本和完全未編碼的文本也很有用。

WinHex 的個人許可證：一次不超過 1 個字符集

WinHex 的專業許可證：一次最多 2 個字符集

WinHex、X-Ways Investigator 的專業許可證：一次最多 3 個字符集

WinHex 實驗室版：一次最多 4 個字符集

X-Ways Forensics：一次最多 5 個字符集

您可以選擇將數據解釋為 UTF-16 LE 中未對齊的文本以及未對齊的 UTF-16 BE。未對齊意味著從奇數偏移量開始。這在非西歐語言中有所不同，並使以這種方式存儲的文本真正可讀。存儲以偶數偏移量對齊的 UTF-16 文本更為常見，但您不能指望它。某些應用程序的文件格式和內存分配不介意對齊，甚至可能同時使用對齊和未對齊的 UTF-16 文本。

請注意，從鍵盤輸入的任何文本（當不處於只讀模式時）都被解釋為基於 Windows 中活動的 ANSI 代碼頁，除非主文本列設置為 IBM/OEM/DOS 代碼第 850 頁（拉丁語 I），在這種情況下，輸入基於該代碼頁。

記錄呈現：編輯後續相同大小的數據記錄時（例如，表格

數據庫的條目)您現在可以讓 WinHex 以不同的背景顏色顯示每隔一條記錄 ,作為一種視覺輔助 。可以在 “常規選項”對話框中選擇顏色 。此外 ,WinHex 根據指定的記錄大小和第一條記錄的偏移量 ,在狀態欄中顯示當前記錄號和該記錄內的偏移量 (相對偏移量) 。

如果啟用了兩個記錄功能中的任何一個 ,Go To Offset 命令允許以當前記錄大小為單位移動當前位置 。如果啟用相對偏移 ,則 Page Dn/Up 鍵以記錄大小為單位移動光標 ,除非您按住 Ctrl 鍵 。

顯示 :案例數據窗口是 WinHex/X-Ways Forensics 取證用戶界面的一部分 ,是處理案例所必需的 (隱藏窗口時 ,案例關閉) 。目錄瀏覽器可用於使用磁盤編輯器打開的邏輯驅動器/分區 。Data Interpreter是一個小窗口 ,為當前光標所在位置的數據提供 “翻譯服務” 。工具欄也可選擇顯示 。選項卡控件使每個編輯窗口只需單擊鼠標即可訪問 。信息窗格提供有關任何打開對象 (文件、磁盤、RAM)的深入信息 。

模板管理器

表 :提供四個轉換錶 (參見 ANSI ASCII/IBM ASCII) 。

行和列

同步滾動 :在相同的絕對偏移量上同步最多四個平鋪窗口 。

啟用此功能時按住 Shift 鍵可水平而非垂直平鋪窗口 。

Synchronize & Compare :同步最多四個窗口並直觀地顯示字節值差異 。如果涉及的窗口不超過兩個 ,則 WinHex 在滾動時會保持這些窗口中第一個顯示字節的偏移量之間的初始距離 。不在絕對偏移量上同步是有用的 ,例如在比較文件分配表的兩個副本時 ,這兩個副本顯然處於不同的偏移量 。您可以通過單擊兩個編輯窗口之一中提供的額外箭頭按鈕跳轉到下一個或上一個字節值差異 。

刷新視圖 :重繪當前編輯窗口的內容 。如果當前文件已被外部程序更新 ,WinHex 會拒絕在 WinHex 中所做的任何更改並從頭重新加載文件 。

如果目錄瀏覽器具有輸入焦點 ,也會重新填充目錄瀏覽器 。例如 ,當標記項目的過濾器處於活動狀態並且您刪除了一些列出的文件的標記時 ,如果您希望更新目錄瀏覽器中的列表並刪除那些不再標記的文件 ,這很有用 。

4.9 工具菜單

打開磁盤 :參見 “磁盤編輯器”一章 。

克隆磁盤 :請參閱 “磁盤克隆”一章。

遞歸探索 :更改為目錄瀏覽器中當前列出的目錄的遞歸視圖或返回普通視圖。遞歸視圖意味著不僅會列出直接包含在當前目錄中的文件，還會列出該目錄及其子目錄等所有子目錄中的所有文件。例如，這允許從不同路徑複製/恢復所選文件一步。

按類型恢復文件 :見下文。

Take New Volume Snapshot :可用於具有受支持文件系統之一的分區。
WinHex 遍歷所有簇鏈，從而生成驅動器映射。這使 WinHex 能夠填充目錄瀏覽器並為每個扇區顯示它分配給的文件或目錄。建議在驅動器上的文件操作後再次調用此命令，以保持 WinHex 顯示的信息是最新的。比照。安全選項。

初始化可用空間 :由於正常的刪除、複製和保存操作，機密信息可能存儲在驅動器當前未使用的部分中。出於安全原因，可以初始化驅動器上的可用空間。這有效地覆蓋了磁盤未使用部分中的所有數據，並且無法恢復這些數據。可用於作為驅動器號打開的分區。僅適用於 WinHex，不適用於 X-Ways Forensics。

初始化鬆弛空間 :用零字節覆蓋鬆弛空間（所有簇鏈的各個最後簇中未使用的字節，超出文件的實際末尾）。這可以與“初始化可用空間”一起使用，以安全地擦除驅動器上的機密數據或最小化壓縮磁盤備份（如 WinHex 備份）所需的空間。在使用此命令之前關閉任何可能寫入磁盤的正在運行或駐留的程序。僅適用於 WinHex，不適用於 X-Ways Forensics。

初始化 MFT 記錄 :在 NTFS 卷上，WinHex 可以清除所有當前未使用的 \$MFT (主文件表)FILE 記錄，其中可能包含元數據（例如名稱）甚至以前存在的文件的內容。僅適用於 WinHex，不適用於 X-Ways Forensics。

初始化目錄條目 :在 FAT 卷上，WinHex 可以清除所有當前未使用的目錄條目，以從文件系統中徹底刪除以前存在的文件或現有文件的早期名稱/位置的痕跡。與初始化所有空閒空間的函數結合使用時尤其有用。僅適用於 WinHex，不適用於 X-Ways Forensics。

掃描丢失的分區 :打開物理硬盤（或物理硬盤的映像）時未自動找到的以前存在的硬盤分區可以使用此命令找到並正確識別。此命令通過 0x55 0xAA 簽名以及 Ext2/Ext3/Ext4 超級塊搜索主引導記錄、分區表扇區、FAT 和 NTFS 引導扇區的簽名，可選擇僅從最後一個（位置明智的）分區之後的第一個扇區已找到，並在目錄瀏覽器中列出新發現的分區。

僅適用於 512 字節的扇區大小。

解釋為分區開始 :當您找到卷的開始扇區（例如丟失的分區）時

物理磁盤 :此菜單命令允許您通過訪問按鈕菜單輕鬆訪問此類分區。如果從當前顯示的扇區開始沒有檢測到已知文件系統，系統將詢問您希望包含在新定義的分區中的扇區數。

設置磁盤參數 :在物理磁盤上使用此命令，您可以覆蓋扇區總數或可選（可以留空）每個磁道的柱面數、磁頭數和扇區數（如今這些都幾乎沒有意義）。這可能有助於訪問磁盤末尾的多餘扇區（以防未正確檢測到可訪問扇區的總數），或根據您的需要調整 CHS 坐標系。或者，您可以選擇更改檢測到的物理硬盤或圖像的扇區大小，如程序內部用於各種導航和計算工作。如果您應該調整扇區大小，扇區數也會相應調整。例如，如果將檢測到的扇區大小從 512 字節更改為 4 KB（即乘以 8），則扇區總數會自動除以 8 以保持相同的總檢測磁盤容量（假設檢測到的容量正確）。

打開內存 :參見“內存編輯器”一章。

捕獲進程 :允許連續獲取實時系統上正在運行的進程的內存中的所有數據（即按進程分配的順序排列的頁面）。進程的創建時間可以看作是內存轉儲的創建時間戳。標記為包含可執行代碼（PAGE_EXECUTE* 樣式）的頁面是可選的，如果您僅對關鍵字搜索或雕刻而不是惡意軟件分析感興趣，則如果省略將適當減少數據量。內存轉儲（顯示為“mem”類型的文件）中的雕刻可以通過揭示嵌入數據來執行，這是卷快照優化的功能之一。“捕獲過程”的輸出文件夾默認是案例的子目錄，或者 - 如果沒有案例處於活動狀態 - 圖像目錄的子目錄。一旦輸出完成和/或作為目錄添加到活動案例，就可以在 Windows 文件資源管理器中自動探索它。如果您在其中鍵入文本的應用程序（例如電子郵件客戶端）突然凍結並且您想恢復您所寫的內容，則“捕獲進程”轉儲的內存在您自己的系統上也很有用。

此命令還可以生成所有頂級窗口的製表符分隔列表及其標題和相應的進程加上（逗號分隔）它們的子窗口的標題。一些頂層窗口的屏幕截圖被自動截取並輸出。如果在沒有管理員權限的情況下使用此功能，則僅覆蓋當前用戶的進程，否則覆蓋所有進程。過濾器可用於進程轉儲。您可以像 X-Ways Forensics 中的其他文件掩碼過濾器一樣使用它。例如，“explorer.exe”只會轉儲 Windows 文件資源管理器進程的內存和窗口。“:C*”將轉儲所有進程，但名稱以字母“C”開頭的進程除外，例如不是“Chrome.exe”。文件掩碼不區分大小寫。

多個文件掩碼可以用分號連接。（但是，總長度是有限的。）

查看 :僅在法醫許可下可用。調用內部查看器。

外部查看器 :調用外部文件查看程序，如在選項菜單中選擇的 Quick View Plus 等，並打開當前文件。

調用 X-Ways Trace :僅當安裝了 X-Ways Trace 時可用。該軟件可以分析各種互聯網瀏覽器的歷史/緩存文件。

計算器 :運行 Windows 計算器 “calc.exe”。強烈建議切換到科學模式。

十六進制轉換器 :使您能夠將十六進制數轉換為十進制數，反之亦然。只需輸入號碼並按ENTER。

表 :提供四個轉換錶（參見 ANSI-/IBM-ASCII）。

比較 :該命令用於逐字節比較兩個數據窗口（文件或磁盤）。

決定是否應報告不同或相同的字節。您可以指定要比較的字節數。如果需要，操作可以在發現一定數量的差異或相同字節後自動中止。該報告可以存儲為文本文件，否則其大小可能會急劇增加。比較從每個編輯窗口指定的相應偏移量開始。這些偏移量可能不同，例如文件 A 中偏移量 0 處的字節與文件 B 中偏移量 32 處的字節進行比較，偏移量 1 處的字節與偏移量 33 處的字節進行比較，等等。當您選擇一個編輯窗口進行比較時，當前位置將自動輸入到“起始偏移量”框中。

在 X-Ways Forensics 中，還有一個選項可以將已識別的不同或相同數據區域輸出為搜索命中（每個匹配區域 1 個條目）而不是文本文件（每個匹配字節 1 行），以便在程序內方便地查看和導航在搜索命中列表中，類似於塊哈希匹配。僅當至少第二個數據源是證據對象時，此選項才可用。

結果可以在該證據對象的搜索命中列表中看到。例如，對於希望比較具有微小更改的克隆磁盤的用戶很有用，如果它們具有不同的哈希值或其中一個已被使用得更多一些，則可以真正找到差異並更好地了解導致它們的原因。也可用於比較硬件 RAID 級別 0 系統或鏡像卷的組件磁盤，以檢查它們是否真的完全相同。如果不能輕鬆找到不同的區域，請查看它們有多大，這些區域的數據類型包含並評估第二個副本本身是否需要全面處理，包括雕刻、關鍵字搜索等。

還有另一個比較功能：您可以直觀地比較編輯窗口並在這些窗口中同步滾動，使用同步和比較命令（查看菜單）。

分析塊/文件 :掃描當前塊/整個文件中的數據併計算每個字節值 (0...255) 的出現次數。結果通過成比例的垂直線以圖形方式顯示。將鼠標移到相應的垂直線上時，會顯示每個字節值的出現次數和百分比。

例如使用此命令來識別未知類型的數據。音頻數據、壓縮數據、可執行代碼等產生特徵圖形。使用窗口的上下文菜單打開或關閉零字節考慮、打印分析窗口或將分析導出到文本文件。

當分析少量數據 (<50,000 字節)時，zlib 為該數據實現的壓縮率顯示在分析窗口標題中，這也允許得出有關數據性質的結論。

計算哈希 :計算整個當前文件、磁盤或當前選定塊的以下校驗和/摘要之一：8 位、16 位、32 位、64 位校驗和、CRC16、CRC32、MD5、SHA-1、SHA-256 或 PSCHF。

4.10 文件工具

串聯 :選擇要復製到一個目標文件中的多個源文件。源文件不受影響。

拆分 :此命令使用單個源文件的內容創建多個目標文件。
為每個目標文件指定一個拆分偏移量。源文件不受此功能的影響。

統一 :選擇兩個源文件和一個目標文件。源文件中的字節/字將交替寫入目標文件。第一個字節/字來自首先指定的源文件。使用此功能創建一個文件，其中奇數和偶數字節/字來自單獨的文件（例如，在 EEPROM 編程中）。

解剖 :選擇一個源文件和兩個目標文件。源文件中的字節/字將交替寫入目標文件。第一個字節/字將被傳輸到首先指定的目標文件。使用此函數創建兩個單獨的文件，每個文件包含原始文件的奇數或偶數字節/字（例如，在 EEPROM 編程中）。

創建硬鏈接 :在 NTFS 卷中創建文件硬鏈接的功能。例如，在參加 NTFS 文件系統培訓時使用硬鏈接很有用，或者如果您想再次將相同的圖像添加到相同的案例中，這只能在不同的名稱下進行，或者如果您想創建一個硬鏈接鏈接到名為 WinHex.exe 的 xwforensics.exe，以便將 X Ways Forensics 作為 WinHex 運行。首先選擇現有文件，然後選擇附加硬鏈接的路徑和名稱。

複製稀疏 :可以複制選定的文件，如果它是 NTFS 稀疏文件，則在目標文件中保留稀疏性質。這意味著，例如，當複制僅分配了 100 MB 數據的 1 TB 骨架磁盤映像時，複製過程幾乎會立即完成，因為 1 TB 數據中只需複制 100 MB。傳統的複制功能不會保留文件的稀疏特性，也不會複制由標稱文件大小指示的數據量，即使大部分數據在內部未分配並且實際上讀取為二進制零。

複製目錄 :遞歸地複制一個目錄及其所有文件和子目錄，並在目標文件系統和其間的任何層支持的情況下，在相應的輸出文件夾中單獨重新創建 NTFS 壓縮源文件作為 NTFS 壓縮文件。該命令不會在創建此類文件後追溯壓縮這些文件，而是立即將它們作為壓縮文件寫入，這樣效率更高。但是，它仍然必須複製/發送源文件的解壓縮數據量。支持超長路徑。首先選擇源目錄，然後指定/創建目標目錄。此功能非常有用，例如，如果您希望複製或移動一個案例目錄，其中包括一些 NTFS 壓縮文件，這些文件對於

存儲為未壓縮。請注意，您也可以打開一個案例並使用“案例數據”窗口中的“另存為”命令來獲得相同的效果。

Wipe Securely：該命令用於不可撤銷地擦除磁盤上一個或多個文件的內容，使它們無法被 WinHex 或其他專用數據恢復軟件恢復。每個選定的文件都被用戶選擇的數據覆蓋，縮短為零長度，然後刪除。文件的名稱條目也被刪除。即使是專業人士嘗試恢復文件也將是徒勞的。因此，該命令適用於需要銷毀的具有機密內容的文件。僅適用於 WinHex，不適用於 X-Ways Forensics。

遞歸刪除：此命令可用於遞歸刪除目錄及其所有子目錄。如果由於目錄名稱中的非法字符或缺少權限（例如，如果“受信任”安裝程序是所有者）如果您可以獲得這些權限（如果您以管理員權限運行 WinHex）。請注意，您不能將此命令應用於此類有問題的目錄本身，而只能應用於父目錄。

4.11 專家菜單

僅限專家和法醫執照。

優化卷快照：請參閱單獨的章節

技術細節報告：顯示有關當前活動磁盤或文件的信息，並允許您將其複製到例如您正在編寫的報告中。在物理硬盤上最廣泛，其中指出了每個分區的詳細信息，甚至指出了現有分區之間未分配的間隙。在 Windows XP 下，WinHex 還會報告 ATA 磁盤的密碼保護狀態。

僅限取證許可：X-Ways Forensics 試圖檢測隱藏的主機保護區（HPA，又名 ATA 保護區）和 ATA/SATA 硬盤上的設備配置覆蓋（DCO 區域）。

如果磁盤大小被人為減小，將顯示一個帶有警告的消息框。根據 ATA 的實際扇區總數，如果可以確定，將在詳細報告中列出。對於通過支持 SMART 的 [S]ATA 連接的硬盤，還會顯示一些重要的 SMART 狀態信息。用於檢查自己的硬盤以及嫌疑人的硬盤。例如，您可以了解硬盤的使用頻率和使用時長，以及它是否有任何壞扇區（在某種意義上，不可靠的扇區在內部被替換為備用扇區）。如果將硬盤退還給嫌疑人，他或她因此抱怨壞扇區並指責您損壞了磁盤，那麼在最初捕獲硬盤時創建的詳細報告現在可以顯示它是否已經處於不良狀態那時。

此外，看到備用扇區正在使用意味著知道有額外的數據可以從硬盤中獲取（通過適當的技術手段）。

輸出有關 BitLocker 和 BitLocker To Go 卷的以下元數據：卷創建時間戳、文本卷描述、加密方法、保護類型和卷主密鑰上次修改時間戳。與 BitLocker 相關的時間戳也會輸出到事件列表。

技術細節報告還檢查在數據區域中從未寫入/使用過的數據未定義的閃存介質（例如某些品牌/型號的 USB 記憶棒，但不是其他品牌/型號）可能發生的某些讀取不一致。在此類區域中讀取的數據（例如在對介質成像時）可能取決於使用單個內部讀取命令一次讀取的數據量。報告中提到了結果。如果檢測到不一致（報告中的“讀取結果不一致！”），您將看到一個消息框，它會提供從該設備讀取較小塊的扇區，只要它是打開的，這可能會產生預期的零值字節在讀取這些區域時，一些看起來隨機的非零模式數據。使用此選項不會為您提供更準確或更原始的數據（未定義是未定義的，並不意味著歸零）或包含或多或少的證據，它只會對實現的壓縮率和哈希值的可重複性產生重大影響與其他工具一起使用，這些工具可能使用不同的塊大小進行讀取，從而產生不同的數據和哈希值。請注意，可能會發生 X Ways Forensics 未檢測到的讀取不一致，因為完整檢查會非常慢。同樣，這些不一致不是致命的，也不是軟件的錯誤，它們是可以解釋的。請注意，當您使用 File | 啟動磁盤映像時，技術詳細信息報告已按常規創建。創建磁盤映像命令，因此您無需在映像前自行調用報告。

當有疑問時，除了通過操作系統報告的序列號之外，還有一個選項可以顯示硬盤序列號的字節交換版本。某些干擾硬件寫阻止程序的一些用戶可能會發現這很有用。

將圖像文件解釋為磁盤：請參閱單獨的章節

掛載為驅動器號：參見單獨的章節

OS-Wide Write Protection：允許寫保護本地連接的物理存儲設備（包括可移動媒體，光學媒體除外）及其所有捲在操作系統中的任何位置，在所有應用程序中，甚至在 WinHex 本身的扇區級別，無論哪個編輯模式處於活動狀態。這可用於保護需要獲取或分析的原始磁盤（但僅在 Windows 檢測並訪問它們之後）和您自己的包含圖像的磁盤，以防止意外更改、刪除或數據損壞。該效果將持續到您再次取消寫保護或拔下設備或重新啟動計算機。為了防止 Windows 在您可以對它們進行寫保護之前接觸新連接的物理存儲設備（即首先將它們保持在“離線”模式），您需要禁用 Windows 中的自動安裝（並驗證它是否有效）。為脫機磁盤打開寫保護將自動使磁盤聯機，同時將其呈現為只讀。小心，不要寫保護您的 Windows 系統需要寫入才能正常運行的磁盤！

此命令還允許有選擇地僅對 GPT 分區磁盤上的特定卷（如果安裝為驅動器盤符）進行寫保護，而不是對整個物理存儲設備進行寫保護。請注意，如果整個底層物理存儲設備都是只讀的，則無法選擇性地解除卷的只讀狀態。警告：對 MBR 分區磁盤上的單個捲進行寫保護也會對同一磁盤上的其他卷產生影響。

重建 RAID 系統：參見單獨的章節

Gather Free Space :遍歷當前打開的邏輯驅動器並將所有未使用的簇收集到您指定的目標文件中。有助於檢查以前存在的文件中未安全刪除的數據片段。不以任何方式改變源驅動器。目標文件必須位於另一個驅動器上。

收集鬆弛空間 :在目標文件中收集鬆弛空間（所有簇鏈的各個最後簇中未使用的字節，超出文件的實際末尾）。否則類似於收集可用空間。WinHex 無法訪問在文件系統級別壓縮或加密的文件的鬆弛空間。

收集分區間空間 :捕獲物理硬盤上不屬於目標文件中任何分區的所有空間，以便快速檢查以查明是否隱藏了某些內容或先前分區留下的內容。

收集文本 :根據您指定的參數識別文本，並從文件、磁盤或文件的內存範圍中捕獲所有出現的地方。這種過濾器可用於顯著減少要處理的數據量，例如，如果計算機取證專家正在尋找文本形式的線索，例如電子郵件消息、文檔等。目標文件可以很容易地拆分為用戶定義的大小。此功能還可應用於具有已收集的閒置空間或可用空間的文件，或專有格式的損壞文件，這些文件無法再被其本機應用程序（如 MS Word）打開，以至少恢復未格式化的文本。

證據文件容器 :見上文

外部病毒檢查：(僅限取證許可證。)將證據對象卷快照中的所有文件或所有標記文件發送到外部病毒掃描程序，可選擇僅發送大小低於特定閾值的文件。在輸出目錄中被病毒掃描器鎖定、刪除或重命名的文件將被添加到名為“Virus suspected”的報告表中。用戶有責任驗證病毒掃描程序是否處於活動狀態，它會監視文件夾中的臨時文件，並且確實會鎖定、刪除或重命名受感染的文件。在驗證文件是否已被鎖定、刪除或從外部重命名後，X-Ways Forensics 會自行刪除它（如果它仍然存在）。

貝茨編號文件 :貝茨編號給定文件夾及其子文件夾中的所有文件以供發現或證據使用。在文件名和擴展名之間插入一個不變的前綴（最多 13 個字符）和一個唯一的序列號，這是律師傳統上標記紙質文件以供日後準確識別和參考的方式。

受信任的下載 :解決了潛在的安全問題。將非機密材料從機密硬盤驅動器傳輸到非機密媒體時，您需要確定在與實際文件一起虛假複製的任何簇或扇區“懸垂”中沒有無關信息，因為此空閒空間可能仍包含機密信息分配給不同文件時的材料。此命令以當前大小複製文件，不再多字節。它不像傳統的複制命令那樣複製整個扇區或簇。可以同時複制同一文件夾中的多個文件。

4.12 選項菜單

一般選項 :見下文

查看器程序 :見下文

撤消選項 :見下文

安全選項 :見下文

數據解釋器選項 : cf 。數據解釋器

編輯模式 :允許您全局選擇在 Winhex 中使用的編輯模式。（信息窗格的上下文菜單僅允許選擇專門用於活動編輯窗口的編輯模式。）

4.13 窗口菜單

窗口管理器 :顯示所有數據窗口並提供“即時窗口切換”功能。您也可以關閉數據窗口並保存更改。

Save Arrangement As Project :將當前窗口配置（打開的案例、打開的數據窗口、屏幕上數據窗口的位置、數據窗口中的光標位置、塊選擇……）寫入項目文件。從開始中心，您將能夠隨時加載項目並恢復每個文檔中的編輯位置，以便在您離開的地方方便地繼續您的工作，或者在重複任務的情況下開始您的工作。

全部關閉 :關閉所有數據窗口，從而關閉所有打開的文件、磁盤和 RAM 部分。如果您編輯了任何數據，如果其中的數據有未保存的更改，系統會在每個數據窗口提示您，因此您可以決定是保存還是放棄這些更改。

Close All Without Prompting :關閉所有數據窗口，從而關閉所有打開的文件和磁盤，而不讓您有機會在所有這些窗口中保存對數據的任何更改，而不提示您每個有更改的數據窗口。由於這是一個潛在的危險命令（如果您在多個數據窗口中編輯數據，您可能會丟失很多工作），因此會有警告，您仍然可以中止。您知道，由於命令名稱末尾的省略號，將首先顯示一個需要額外確認的窗口，這是慣例。

Cascade/Tile :以上述方式排列數據窗口。

全部最小化 :最小化所有數據窗口。

排列圖標 :此命令將所有最小化的數據窗口整齊地排列在主窗口中。

4.14 幫助菜單

內容 :顯示程序幫助的內容。

設置 :允許您切換用戶界面的語言。使用Initialize ,您可以恢復程序的默認設置。卸載 :使用此命令從系統中刪除WinHex 。即使您沒有使用安裝程序安裝 WinHex ,它也能正常工作。

UI 文本調整 :您可以根據自己的喜好重命名任何目錄瀏覽器列 ,例如為了保持早期版本和未來版本之間用戶界面的連續性 ,或者為了數據傳輸的兼容性 (例如導出列表命令) ,或者因為某個列標題尚未翻譯成您首選的基於拉丁語的用戶界面語言 ,您希望看到自己對英文標題的翻譯 ,或者因為您更喜歡看到 “Attributes”而不是縮寫 “Attr.”等 。在帶有目錄瀏覽器選項的對話框窗口 ,您可以簡單地右鍵單擊該列的標題 ,然後將有機會用您自己的措辭替換標題。

通過 “幫助”菜單中的此菜單命令 ,可以自定義用戶界面中的更多文本片段 (字符串) 。您需要確定要替換的確切標準文本片段並提供您自己的版本 。如果沒有找到您正在尋找的文本 ,並且您不確切知道它在內部是如何存儲的 ,您可以在文件 “language.dat”中搜索它。

您的自定義設置存儲在文件 “UI Text Adjustments.txt”中 ,可以與其他用戶共享 。該文件大概也可以在未來的版本中使用 ,只要原始文本片段保持不變即可 。它只包含每行一次調整 ,首先是原始文本 ,然後是替換文本 ,由製表符分隔 (這意味著無法調整那些已經包含製表符的少數原始文本) 。您也可以手動編輯該文件。

請注意 ,非拉丁語言的翻譯以簡單文本文件的形式提供 ,因此可以更直接地在這些文件中進行更改。

在線 :在您的瀏覽器中打開 ,如果您有 Internet 連接、X-Ways 網站、支持論壇、時事通訊訂閱頁面 ,以及您可以在其中檢查您的許可證狀態、檢索最新下載鏈接和獲得升級優惠的頁面。還有一個選項可以在軟件啟動時偶爾或在您喜歡的任何時候在線檢查更新 。這可以報告當前使用的版本 (不是預發布版本)的更新版本或新服務版本的可用性 ,並允許開始下載 。不從程序內部向互聯網發送任何數據 ,例如沒有系統或用戶信息或加密狗 ID ,既不直接也不加密也不匿名 ,當然沒有案例數據 ,甚至沒有當前使用的版本號 ,什麼都沒有 。只有當程序確定它在用戶自己的系統上運行時 (如果它是從 C: 驅動器執行的或如果它是使用安裝程序安裝的) ,此選項默認情況下才處於活動狀態 。第一次運行程序時不會進行檢查 ,因此您肯定有機會在發生任何事情之前關閉此選項 。鑑於運行 X-Ways Investigator 和 X-Ways Forensics 的大多數系統都沒有 Internet 連接 ,該選項的作用有限。

點擊菜單欄最右側的版本號 :顯示軟件信息 ,如程序版本、解鎖狀態、驅動器上有多少可用空間用於臨時文件和圖像文件、程序是否可用正在以管理員身份運行

權利，是否安裝了 MS Visual C++ 2013 Redistributable Package（用於最新版本的查看器組件和 Dokan），如果沒有安裝，是否至少安裝了 MS Visual C++ 2005 Package（用於查看器組件的 v8.5.2 及更早版本）。當在實時系統上運行 X-Ways Forensics 時，其中一些信息可能很重要，例如，您希望檢查的系統不是您自己的系統。

4.15 Windows 上下文菜單

當用戶用鼠標右鍵單擊對象時，Windows shell 會顯示上下文菜單。WinHex 僅在您啟用相應選項時才會出現在上下文菜單中（請參閱“常規選項”）。

使用 WinHex 編輯：在 WinHex 中打開選定的文件。

在 WinHex 中打開：讓您在 WinHex 中打開所選文件夾的所有文件，就像文件菜單中的打開文件夾命令一樣。

編輯磁盤：在 WinHex 的磁盤編輯器中打開選定的磁盤。如果按住 SHIFT 鍵，則打開相應的物理磁盤（如果有）而不是選定的邏輯驅動器。

WinHex 在狀態欄、數據解釋器和位置管理器中提供了自己的上下文菜單。

5 取證特徵

5.1 將圖像文件解釋為磁盤

專家菜單中的此命令將當前打開和活動的磁盤映像文件視為邏輯卷（可能具有受支持的文件系統）或物理（可能已分區）磁盤。如果您希望在沒有任何操作系統幫助的情況下仔細檢查磁盤映像的文件系統結構、提取文件等，這將很有用。如果解釋為物理磁盤，WinHex 可以單獨訪問和打開圖像中包含的分區，就像從“真實”物理硬盤中知道的那樣。將圖像添加到 X-Ways Forensics 中的案例並稍後重新打開它們時，或者使用文件 | 時，內部也會使用相同的功能。打開命令，你已經提前告訴應用程序你要打開的文件是一個圖像文件。

也可以解釋跨越的原始圖像文件，即由任意大小的單獨片段組成的圖像文件。對於 WinHex 檢測跨越的圖像文件，命名支持的幾種可能性：1) 第一段可以具有任意非數字文件擴展名（例如.dd 或.img），然後第二段必須命名為。002，第三段。003，依此類推。

2) 第一段可能具有以下數字文件擴展名之一：.001、.0001、.00001、

.000、.0000 或 .00000。接下來的段必須直接以遞增的數字和完全相同的數字繼續，即三、四或五。3) abc.bin, abc_1.bin, abc_2.bin, ...

對於 1) 和 2)，所有段必須具有相同的基本文件名（擴展名之前的名稱部分）。創建磁盤映像命令可以映像磁盤並生成規範命名的文件段。圖像分割很有用，因為 FAT32 文件系統或 DVD 等媒體支持的最大文件大小非常有限。它還可能有助於降低風險（段越小，如果文件由於文件系統錯誤而丟失，丟失數據量的災難性就越小）並且可能具有性能優勢（如果操作系統更有效地緩衝頻繁需要的圖像數據如果存儲在較小的段中）。

在極少數情況下，WinHex 可能無法正確確定圖像的性質，即它是物理磁盤的圖像還是卷的圖像，因此以錯誤的方式解釋圖像中的數據。如果是這樣，請在調用此命令時按住 Shift 鍵。這樣 WinHex 就會詢問您而不是自己決定。這也會讓 WinHex 提示您輸入正確的扇區大小，如果是原始圖像，還會提示您輸入更多圖像文件段的額外存儲位置（以防您不得不將它們分佈在兩個不同的驅動器上）。如果在檢測卷中的文件系統時出現任何問題，您可以在打開卷時按住 Shift 鍵以指示卷中您認為的文件系統類型。

還支持模式 1 和模式 2 Form 1 ISO CD 映像，每個扇區有 2,352 字節，如果它們沒有跨接的話，並且（有取證許可證）也支持主內存轉儲。VMware 的虛擬機磁盤映像 (VMDK) 也可以解釋為默認子類型“稀疏”和子類型“固定大小”和“差異”（快照）的動態 Virtual PC 映像（VHD、VHDX）和 Virtual Box 磁盤映像（VDI）。快照圖像只能在父級可用且事先打開並自行解釋的情況下才能解釋。不支持 ESXi 服務器使用的具有 ESXi 主機稀疏範圍（也稱為“寫入時復制磁盤”或 COWD）的 VMDK 映像，例如用於虛擬機快照。只能編輯虛擬機映像中的分配區域。X-Ways Forensics 和 X-Ways Investigator 還可以解釋.e01 證據文件（可以使用 Create Disk Image 命令創建）以及未加密的 Ex01 證據文件。

還可以解釋各種圖像（原始圖像和大多數 VHD/VHDX/VMDK/VDI 以及 Apple Time Machine 通過文件“com.apple.TimeMachine.MachineID.plist”創建的備份包）和自然（磁盤/卷），即使它們存儲在其他映像（您自己創建的取證磁盤映像）中，也無需先將它們從外部映像中復制出來，只要它們不包含多個段即可。這可以節省大量時間，特別是如果在解釋包含的圖像後您可以快速發現它並不是真正相關的，當然也可以節省空間。首先右鍵單擊目錄瀏覽器中的圖像，然後在單獨的數據窗口中使用上下文菜單的打開命令打開它。

之後，使用主菜單中的命令解釋圖像。然後，一旦拍攝了卷快照，如果您認為圖像是相關的，您可以像往常一樣使用數據窗口選項卡的上下文菜單中的“添加到活動案例”命令或使用在案例數據窗口的文件菜單中添加命令。TAR 存檔中的圖像文件也應該可以工作，這對於 OVA 文件（打開 TAR 格式的虛擬化存檔）中的 VMDK 虛擬機磁盤很方便。

鬆散的 \$MFT 文件可以直接方便地解釋為 NTFS 映像

卷，以至少獲得所有文件和目錄的完整列表，包括它們的路徑、時間戳和屬性。可以打開駐留文件（內容小到足以放入 FILE 記錄的文件），但不能打開其他文件。如果在特殊情況下您只有 \$MFT 而不是整個卷，這很有用。

5.2 個案管理

WinHex 中集成的計算機取證環境只能使用 WinHex 的取證許可證。它提供完整的案例管理、自動日誌和報告文件生成，以及各種附加功能，例如畫廊視圖、文件簽名檢查、HPA 檢測和圖片中的膚色檢測。

首次啟動 WinHex 時，系統會詢問您是否使用取證界面運行它。這意味著顯示“案例數據”窗口，WinHex 以只讀模式運行，並要求您確保臨時文件和案例數據的文件夾設置正確，以防止 WinHex 將文件寫入錯誤的驅動器。

為了處理案例，請確保“案例數據”窗口在主窗口的左側可見。如果沒有，啟用查看 | 顯示 | 案例數據。

從文件菜單中，您可以創建一個新案例（從頭開始）、打開一個現有案例、關閉活動案例、保存活動案例、在 ZIP 存檔中備份案例文件和整個案例文件夾（僅適用於文件< 4 GB），或自动生成案例報告。您可以將媒體作為證據對象添加到案件中，或圖像（將被解釋為媒體的文件，請參閱專家菜單），或內存轉儲，或您自己計算機上的目錄。如果感興趣的目錄或文件駐留在具有許多不相關文件的驅動器上，則添加目錄而不是整個分區或磁盤會很有用，如果您只想查看、散列或搜索其中的一些文件，請檢查它們的元數據或將它們複製到證據文件容器等。

案例存儲在 .xfc 文件（xfc 代表 X-Ways Forensics Case）和同名的子文件夾中，只是沒有 .xfc 擴展名。創建案例時會自動創建此子文件夾及其子文件夾。您可以在常規選項中為您的案例選擇基礎文件夾。沒有必要顯式保存案例，除非您需要確保它在給定時間保存。案例最晚會在您關閉或退出程序時自動保存。唯一的例外是使用“關閉案例（不保存）”命令關閉案例時。例如，如果您不小心丟失了精心設置的標記（通過取消所有標記，在列標題中誤擊）或者如果您不小心丟失了報告表關聯（通過對所有選定文件按 Ctrl+0），重要的是在下次自動保存間隔結束之前盡快調用該特殊菜單命令，以避免保存卷快照。之後您可以再次打開案例，並找到上次保存案例時的所有內容，這意味著您平均只會丟失在自動保存間隔內完成的工作量的一半，而不是所有內容。

在案例屬性窗口中，您可以根據自己的約定（例如標題或編號）命名案例。記錄並顯示您創建案例的日期和時間。內部案例文件名也會顯示。您可以輸入案例的描述（任意長度）和

審查員的姓名、審查員所在組織的名稱和地址。您可以為整個案例啟用或禁用自動日誌功能。或者，始終建議將案例文件夾中的證據對象子文件夾作為從文件系統恢復/複製的文件的默認輸出文件夾。如果您喜歡將文件從各種證據對象複製到同一個輸出文件夾中，您可能希望禁用該功能。

您最多可以選擇兩個與案例相關的代碼頁（更準確地說：與使用與案例相關的原始媒體的區域設置相關）。在根據主題命名 .eml 文件（從電子郵件存檔中提取的 .eml 文件）時使用這些代碼頁。如果兩個代碼頁相同，那沒有壞處。如果與 Windows 中當前活動的代碼頁相同，則它們沒有任何作用。這些代碼頁還用於將 zip 存檔中的文件名轉換為 Unicode。在未來的版本中可能會有更多的用途。

有一個選項可以在將圖像添加到案例時自動驗證哈希值，如果存在這樣的哈希值，或者（如果復選框被完全選中）如果圖像沒有哈希值則從頭開始計算哈希值。新創建的案例從上一個已定義設置的案例繼承此選項的狀態。這也意味著您可以使用 AddImage 命令從命令行驗證圖像。結果將輸出 1) 在消息窗口中，2) 如果需要，在 msglog.txt 中，以及 3) 在證據對象的屬性中，即案例中的圖像表示。

案例文件可以用密碼保護。這不涉及加密，只是一種鎖。

如果密碼被用戶丟失，X-Ways Investigator 保存的案例文件可以使用超級用戶密碼解鎖，前提是在保存案例文件時使用的安裝中已經輸入了這樣的密碼（未記錄在要求）。

創建新案例時，您可以選擇讓 X-Ways Forensics 通過證據對象自身的固有屬性而不是 Windows 磁盤編號來識別作為物理媒體（而非圖像）的證據對象。使用此選項將阻止早期版本的 X-Ways Forensics 打開案例。優點是您可以在不同時間添加多個硬盤或外部 USB 磁盤或棒到連接到計算機的外殼，並獲得 Windows 分配的相同磁盤編號。另一個優點是，如果 Windows 分配的同一磁盤的編號發生變化，X-Ways Forensics 仍會識別該磁盤。在不處理圖像時尤其適用於分類。請注意，如果下次通過不同的硬件寫入阻止程序附加外部媒體，X-Ways Forensics 可能無法識別案件已知的外部媒體。在這種情況下，您仍然可以使用證據對象上下文菜單中的“替換為新磁盤”命令將 X-Ways Forensics 指向正確的磁盤。

請注意，當重新打開已添加到磁盤的 RAID 時，Windows 磁盤編號仍會記住內部重建 RAID 的組件磁盤（讀取磁盤，而不是圖像）

案子。

單擊“密碼...”按鈕時，用於加密通用文件存檔的案例密碼列表將在您首選的文本編輯器中打開以進行編輯。

當單擊“IDs...”按鈕時，您可以看到在該案例中遇到的所有 SID/用戶名組合的集合（從添加到該案例的圖像/媒體上的所有 Windows 安裝中的 SAM 註冊表配置單元中收集）。在處理該案例時，X-Ways Forensics 使用它們將 SID 解析為用戶名。

X-Ways Forensics 中最強大的概念，允許系統和完整地審查計算機媒體上的文件，是所謂的精煉卷快照。可以一步提煉一個案件的所有證據對象的標準卷快照，並藉助虛擬全局案件根窗口邏輯搜索所有捲快照的證據對象。請注意，通過遞歸探索根目錄，可以從分區上的所有子目錄或分區的圖像文件中生成所有現有文件和已刪除文件的平面概覽。為了以遞歸方式探索目錄（即列出其內容及其所有子目錄的內容及其子目錄），請在案例數據窗口的目錄樹中右鍵單擊該目錄。為了標記目錄，您可以在目錄樹中用鼠標中鍵單擊它。

備份

案例數據上下文菜單中的“備份/恢復”命令使您可以方便地備份所選證據對象的捲快照。可以在以後的任何時間使用相同的命令恢復備份，也可以使用相同的命令刪除它們（右鍵單擊備份列表中的項目以獲取刪除命令）。這樣的備份就像卷快照的快照。如果您認為您可能希望稍後恢復到某個處理階段（即撤消對卷快照的更改），例如在仔細標記您不想丟失的數千個文件之後，在運行文件頭簽名搜索之前，這很有用可能會產生大量垃圾文件的實驗性設置，在使用您以前從未嘗試過的選項附加外部文件之前，在運行第三方製作的 X-Tension 之前，在從卷快照中完全刪除刪除的項目之前等。報告表關聯、事件和搜索命中也包含在備份中。僅當案例的搜索詞列表在此期間沒有更改時，才能從備份中恢復搜索命中。索引不包含在備份中，但當然可以手動備份。

在案例級別應用相同的命令（右鍵單擊粗體案例標題）允許備份整個案例，涵蓋所有證據對象的捲快照、所有報告表、事件、搜索詞、搜索命中、索引、圖像文件路徑等。此類備份可以從同一對話窗口中恢復。如有必要，也可以使用打開案例命令直接打開此類備份，因為它們是案例的完整副本。（不過，備份 .xfc 文件是使用“隱藏”屬性創建的，因為它們只能在 X-Ways Forensics 中處理。）

要想完全刪除一個案例或者手動刪除一個案例的備份，需要刪除它的 .xfc 文件和對應的同名目錄及其所有子目錄。

5.3 大型案例的多用戶協調

X-Ways Forensics 和 X-Ways Investigator 可以區分在不同時間或同時處理同一案件的不同審查員，並將他們的結果分開。

多用戶支持對於大型案例特別有用。每個案例最多支持 255 個用戶（審查員）。考官通過其 Windows 用戶帳戶在內部得到認可。

多個用戶可以同時打開同一個案件中的同一個證據對象進行審查。相同案例是指存儲在共享網絡位置或終端服務器上的相同案例文件，而不是副本。X-Ways Forensics 負責將報告表關聯、評論和添加文件同步到卷快照，並讓用戶在訪問衝突發生之前就知道它們並在大多數情況下阻止它們。

通過單擊案例屬性對話框窗口中標有“多用戶支持選項”的按鈕，可以找到所有相關選項。特別是，在創建案例時（並且僅在此時），您可以選擇讓 X-Ways Forensics 不區分不同的用戶。如果您知道只有您會處理該案例，並且如果您希望在擁有不同 SID 的 Windows 帳戶的不同計算機上處理它，那麼您將始終被視為同一用戶，這將很有用。如果多名審查員將在不同時間處理同一案件並希望直接共享他們的所有結果，這也很有用。

另一個多用戶支持選項更仔細地協調對卷快照的某些類型的訪問（與向快照添加項目以及編輯註釋和元數據相關）。如果禁用它可能會有一些性能優勢。僅對於絕對一次僅由 1 個用戶處理的情況，才建議禁用此同步。

不同審查員的報告表關聯和評論可以選擇通過顯示創建審查員的首字母（默認）或他們姓名的其他縮寫或（如果未指定縮寫）他們的完整用戶名來在視覺上區分。

審查員可以選擇是否查看其他用戶的報告表關聯或僅查看他們自己的關聯（或者，如果選中一半，則僅查看他們自己的關聯以及未知用戶的關聯）。同一個文件只能由 1 個審查員關聯到同一個報告表。當重新打開證據對像或案例自動保存間隔結束或手動調用保存案例命令時，X-Ways Forensics 會在共享分析模式下導入並顯示新創建的同時其他用戶的報告表關聯。顯示報告表關聯首字母的選項表示為一個三態復選框。如果選中一半，它只對目錄瀏覽器有影響，對導出列表或恢復/複製命令沒有影響，例如對案例報告也沒有影響。共享分析模式下無法移除其他考官的報表關聯，只能在普通模式下移除。

X-Ways Forensics 會分別為每位審查員記住文件的“已標記”、“已查看”和“已排除”狀態。您可以選擇在打開證據對象時採用所有其他審查員卷快照中文件的“已查看”狀態。如果目標是避免重複工作，如果您不希望審閱您的任何同事已經審閱過的文件，這將很有用。請注意，如果一位審查員從卷快照中刪除項目，則單個文件狀態（“已標記”、“已查看”和“已排除”）以及其他用戶的搜索命中將丢失。

搜索命中和搜索詞也按用戶存儲。第一個審查員打開 v17.5 或更高版本的舊案例將吸收 v17.4 或更早版本存儲在案例中的搜索命中和搜索詞。“多用戶支持選項”對話框窗口包含一個按鈕，允許您導入其他用戶的搜索命中和搜索詞。有一個選項可用於將另一個用戶的搜索命中的導入限制為標記為顯著的搜索命中或該用戶手動定義的搜索命中（所謂的用戶搜索命中）。另一個選項允許在導入時從其他用戶那裡刪除搜索結果。如果其他用戶要

稍後恢復他的工作，並希望在他或她再次接管時導入您的搜索結果，以避免重複搜索結果，因為您的搜索結果在您導入之後已經包括他或她的結果。

要查看同事的所有結果（報表關聯、搜索命中、標記標記、文件已查看狀態、文件排除狀態），您可以以只讀模式以他或她的身份打開案例。為此，請在打開案例時嘗試“選項...”複選框。您可以阻止您的同事像您一樣以只讀模式打開案例。

“選項...”複選框允許您以以下三種模式中的任何一種打開案例：

- 1) 整個案例只讀（案例文件和卷快照）
- 2) 共享分析模式（能夠協同生成報告表關聯、評論、搜索命中和虛擬文件；標記文件；記住已經查看的文件、排除文件）
- 3) 完全訪問

如果同一用戶希望同時在程序的多個實例中打開同一案例（同一副本），則該用戶有兩個選擇。要么 1) 在第二種情況下，整個案例（包括證據對象）以只讀方式打開，

或者

- 2) 用戶作為一個單獨的、虛構的用戶（稱為他或她的“另一個自我”）打開案例，具有單獨的文件狀態、搜索命中、報告表關聯等（案例和證據對象的共享使用由 X 協調）-Ways Forensics 就好像另一個自我是一個真實的、不同的審查員，即使用戶名是相同的）。

前面提到的“選項...”複選框允許您隨時打開案例作為您的另一個自我，而不僅僅是在程序的第二個實例中打開相同的案例。它還允許您在共享分析模式下打開一個案例，如果它目前沒有在其他任何地方打開的話。

多個用戶同時運行搜索、創建報告表關聯、輸入或編輯評論、編輯提取的元數據、標記文件、排除文件、將文件標記為已查看都支持所有這些操作。但是，當證據對像在其他地方打開時從卷快照中刪除項目是被禁止的，並且會被程序拒絕。v17.5及之後的多用戶協同的目標是支持多個考官同時進行分析/審稿工作。從卷快照中刪除文件不被視為普通的審查/分析工作。卷快照優化應該提前系統地完成。

在v17.5及以後的文件名旁邊的方括號中可以看到在卷快照上附加文件或手工刻文件的審查員的姓名首字母，這樣就很容易判斷是誰將這些文件引入到案例中的。

保留對如何同時協調多個用戶的方式進行技術更改。

為了安全起見，請確保同時運行的用戶運行相同版本的軟件。

最後同樣重要的是 v17.5 允許您在其屬性中查看案例的處理歷史記錄。這揭示了它使用了哪些版本（僅由 v17.3 SR-10 及更高版本、v17.4 SR-4 和

更高版本和 v17.5 及更高版本)以及由哪些用戶 (僅由 v17.5 及更高版本記錄)。

如果一次只有一個案例的用戶，您可以關閉“更仔細地協調同時用戶的處理”以獲得一些性能優勢。

有一個選項可以在打開案例時始終建議共享分析模式。該模式甚至對於打開同一案例的許多並髮用戶中的第一個也是有用的，因為只有在該模式下，新創建的報告表關聯才會定期共享給其他並髮用戶（取決於案例自動保存選項）。

共享分析工作的替代方法

選項 #1：多個計算機法醫檢查員可以同時處理他們自己的同一案例副本（始終複製 .xfc 文件和相應的子目錄）並相互交換結果或核對案例主副本中的所有結果，通過導出和導入報告表關聯（即所有相關文件、電子郵件等的分類）。

選項 #2：將潛在相關文件從原始證據對象複製到多個證據文件容器。在新創建的案例中（在 X-Ways Forensics 或 X-Ways Investigator 中），不同的調查員同時檢查容器。他們還可以導出他們的報告表關聯，然後可以將其導入回原始案例。

報告表關聯的導出和導入這兩個命令都可以在案例樹的上下文菜單中找到。案例和證據對象級別支持導出，案例級別支持導入。如果在原始情況下誰創建了哪些關聯應該很明顯，那麼檢查員/調查員的姓名可以包含在報告表的名稱中。請注意，如果您拍攝了新的捲快照或同時從卷快照中刪除了對象，則無法再導入原始情況下的報告表關聯，因為在這種情況下無法保證內部 ID 該文件保持不變，並且可以建立可靠的關聯。僅當您導入到您從中導出的同一證據對象（同一案例中的同一證據對像或同一案例的副本）時，導入才有效。如果它在不同的情況下是相同的圖像或磁盤，則無濟於事。即使是同一案件，磁盤或圖像從案件中取出後又重新添加，也不再視為同一證據對象。但是，您（例如，作為 X-Ways Investigator 的用戶）可以從新案例中的證據文件容器導出，並讓 X-Ways Forensics 的用戶將報告表關聯導入原始案例中的原始證據對象，從容器中的文件源自哪個。這是可能的，因為證據文件容器具有允許識別原始證據對象的信息。

分佈式捲快照細化

X-Ways Forensics 允許使用同一網絡上的多台機器同時優化同一案件的不同證據對象的捲快照，以通過並行化節省時間。

每個用戶/計算機打開相同的 .xfc 案例文件（同一台計算機上的相同副本）。所有參與的用戶/計算機或除一個（主會話）以外的所有用戶/計算機都必須打開案例。

部分只讀，即只允許共享分析工作/分佈式捲快照細化。這可以通過選中“打開案例”對話框窗口中的“選項...”框來完成，或者如果案例已經在另一個會話中以非只讀方式打開（即在主會話中），則在打開案例時會自動提示您。其他會話最晚會在精化完成以及重新打開相應的證據對象時看到精化結果。案例不必關閉和重新打開。

您可以選擇專門打開單個證據對象（而不是整個案例），並將捲快照視為只讀，使用案例數據窗口中證據對像上下文菜單中的專用命令。請注意，這與證據對象本身（磁盤或圖像）的處理方式無關。X-Ways Forensics 在打開磁盤扇區或解釋圖像文件作為證據對象時絕不會更改它們中的數據。只有捲快照，即包含找到的所有文件和目錄的信息的數據庫，是只讀的，或者是可更改的，這是正常狀態。

5.4 證據對象

您可以將任何當前連接的計算機介質（如硬盤、SSD、存儲卡、U 盤、CD-ROM、DVD...）、任何圖像文件、目錄或普通單個文件添加到活動案例中。然後它將永久地與該案例相關聯（除非您稍後將其從案例中刪除），顯示在樹狀案例結構中，並指定為證據對象或證據來源。在案例文件夾中為每個證據對象創建一個子文件夾，默認情況下將保存您從該證據對象複製/恢復的文件，因此從哪個對象（以及哪個案例）恢復的文件起源總是顯而易見的。如果您希望從同一目錄中添加超過 1 個文件到案例中，請添加整個目錄，只需排除或刪除那些不相關的文件即可。

在證據對象屬性窗口中，您可以根據自己的習慣為該證據對象輸入標題或編號。您可以使用左上角的小箭頭按鈕更改案例樹中證據對象的順序，“相關”證據對象（屬於物理磁盤的分區）除外。記錄並顯示與活動案例關聯的日期和時間。顯示證據對象的內部名稱及其原始大小（以字節為單位）。您可以輸入適用於證據對象的任意長度的註釋，並且 X-Ways Forensics 會自動添加它的技術描述（從“專家”菜單中的“技術詳細信息報告”命令中得知，以及有關 Windows 安裝的一些基本信息，如果在分區中找到）。您可以讓程序計算證據對象上的一個或兩個哈希值（校驗和或摘要）並在以後驗證它們，以便您可以確保數據真實性在這兩者之間沒有受到損害。存儲在證據文件中的散列在添加到案例時會自動導入。帶有文件夾和放大鏡的按鈕允許快速打開證據對象的默認輸出目錄。按住 Ctrl 鍵的同時單擊以導航到內部使用的目錄，卷快照存儲在該目錄中。

要將圖像或媒體添加到案例，您可以使用案例數據窗口的文件菜單中的“添加”命令。添加圖片時，也可以選擇對新添加的證據對象的捲快照進行立即細化。另一種添加打開的圖像或磁盤的方法

案例是數據窗口選項卡的上下文菜單中的“添加”命令。如果案例的圖像存儲在案例目錄中（不要與案例目錄混淆），那麼即使案例路徑發生變化，它們也會被自動找到。可以在案例的屬性中定義圖像的專用案例特定默認路徑，然後覆蓋圖像的通用默認路徑。特定於案例的路徑可能是相對路徑，其中 .指案例目錄，.. 指案例目錄的父目錄。請注意，出於性能原因，建議將案例和圖像存儲在不同的物理存儲設備上。

證據對像上下文菜單中的命令“用新圖像替換”允許您用圖像替換在您的案例中用作證據對象的磁盤（如果您在獲取磁盤之前首先預覽磁盤很有用，即創建它的圖像），而不會丟失您的卷快照、搜索命中、評論等。還可以用來簡單地告訴 X-Ways Forensics 圖像的新路徑，以防圖像被移動或驅動器號發生變化，或者如果更改了圖像文件名，或者更改了圖像類型（例如，要用壓縮和加密的.e01 證據文件替換原始圖像）。如果是物理的、分區的證據對象，建議將此命令應用於該父對象（即物理磁盤）。然後，更改也將自動應用於子證據對象（即分區）。如果新映像是不同磁盤或不同證據文件容器的映像或已被進一步填充的證據文件容器，即如果卷快照無法匹配，您可能會收到警告，因為新映像的大小是與之前圖像的尺寸不同。一次又一次，X-Ways Forensics 的用戶嘗試使用此命令將案件中的證據對象替換為不同的證據對象，儘管這沒有任何意義，因為這樣技術描述、卷快照、任何搜索點擊、評論和報告表關聯與其他證據對像不匹配。然後，這些用戶通常會抱怨他們收到一條錯誤消息。顯示該消息是因為 X-Ways Forensics 通常會根據新圖像的大小注意到它是完全不同的圖像。如果您的案例中不再需要證據對象 A，而需要添加證據對象 B，那麼您可以簡單地刪除 A 並添加 B。除此之外別無選擇，替代方案既不合理也不需要。

即使磁盤或映像當前不可用，也可以通過證據對象的上下文菜單中的特殊命令打開證據對象，以至少查看卷快照。這意味著您可以看到卷快照中存儲的所有文件元數據（文件名、路徑、文件大小、時間戳、屬性等），可以使用大多數過濾器等，但看不到扇區中的任何數據，也無法打開/查看任何文件。

在 Case Root 窗口中，可以通過上下文菜單或點擊空格鍵將證據對象標記為帶有黃色標記的重要對象。您將在案例數據窗口中以及選擇證據對象時看到黃色標誌，例如從案例根進行遞歸探索或生成報告時。

在具有 FAT 文件系統的證據對象的屬性中，如果您對此有想法/意見，您可以選擇定義該文件系統中的本地時間戳所基於的時區。該時區取決於寫入文件系統的計算機或設備的設置。（請記住，這些設置可能會隨時間發生變化，因此單個時區可能不足以讓所有時間戳都正確。）如果您定義時區參考，文件系統級別的時間戳將根據選定的顯示時區顯示而不是在他們的

不再是原來的當地時間。在顯示時間戳的那一刻，它們在內部從本地時間轉換為 UTC（基於您的時區參考），然後從 UTC 轉換為顯示時區。效果不是永久性的，參考時區設置可以隨時更改。如果您在早於 v19.3 的版本中打開案例，時區參考的定義將丟失。

當從 FAT 文件系統複製文件到證據文件容器時，這些文件的文件系統級時間戳通常在容器中標記為基於未知的本地時區，以便將來查看容器時不會調整時區。但是，如果您確定原始時區並為源證據對象定義時區參考，則時間戳將根據參考時區在容器內轉換為 UTC，並在容器中永久標記為 UTC 時間戳。在該狀態下，稍後將根據所選顯示時區調整時間戳，即使您改變主意並更改源證據對象中的參考時區也是如此。一旦文件被複製，證據文件容器是獨立的並且與源證據對象分開。

案例上下文菜單中的命令允許將證據對像從另一個案例導入到當前案例中，例如，當您希望將不同的案例（可能已經由不同的用戶處理以拆分工作量）合併到一個案例中時。默認情況下，案例中的所有證據對像都會被導入。如果您在導入開始時按住 Shift 鍵，則只會導入標記為重要的證據對象（在其原始案例中標有燈泡）。

這還將導入（實際上：複製）證據對象的卷快照，其中包含報告表關聯、評論、書籤、搜索命中、索引、事件、RAID 重建參數、時區選擇等等，但不包括卷快照備份，也不是其他案例的用戶（審查員）和他們自己的報告表關聯和搜索命中之間的區別。執行導入的當前用戶將吸收這些結果。所選導入案例中與目標案例中現有報表同名的報表將與後者合併。將證據對象添加到原始案例時記錄的時間戳將被接管到新案例中。在新案例中，文件的唯一 ID 將有所不同。但是，可以在源和目標案例之間交換（導出和導入）該證據對象的報告表關聯，因為保留了卷快照 ID 和內部 ID。從另一個案例中導入證據對象的命令也可以用來簡單地複制同一個案例中的證據對象。只需選擇當前活動案例的 .xfc 文件即可為標記的證據對象執行此操作。這對於同時維護、查看和比較兩個卷快照、使用未測試的簽名定義進行文件頭簽名搜索等進行實驗可能很有用。

5.5 案例日誌（活動日誌）

在案例屬性中啟用時，X-Ways Forensics 會記錄案例打開時執行的所有活動。這使您可以輕鬆地跟蹤、複製和記錄您為達到特定結果所遵循的步驟，以供您自己記憶、展示給您的同事、法庭等。

記錄如下：

· 當您選擇一個菜單項時 ,命令標題 (或至少一個 ID)和活動編輯窗口的名稱 (如果不是證據對象 ,前面有關鍵字 “Menu”) , · 當顯示消息框時、消息文本和您按下的按鈕 (確定、是、否或取消) ,前面是關鍵字 “MsgBox” , · 當顯示一個小的進度指示器窗口時 ,它的標題 (如 “正在恢復文件...”)以及操作是完成還是中止 ,前面是關鍵字 “Operation” ,

- 每個顯示的對話框窗口的屏幕截圖以及所有選定的選項 ,例如對於一個複雜的隨後的操作 ,前面是窗口的標題 ,* · 克隆磁盤和文件恢復按類型生成的大量日誌 , · 您使用添加日誌條目命令添加的您自己的條目 (自由文本) ,或者到案件整體或某一證據對象 。

使用目錄瀏覽器上下文菜單複制/恢復的每個文件的目標路徑 ,以及該文件的選定元數據 (例如原始名稱、原始路徑、大小、時間戳...) ,記錄在單獨的文件 “copylog.html” 中或 “_log” 子目錄中的 “copylog.txt” 。

所有活動都記錄有準確的日期和時間 ,內部採用 FILETIME 格式 ,間隔精度為 100 納秒。默認情況下 ,日誌與整個案例相關聯 。但是 ,適用於特定證據對象的活動日誌與該證據對象直接關聯 。這決定了它們在報告中的顯示位置 。要輸出活動日誌 ,請生成案例報告 。屏幕截圖作為 PNG 文件單獨保存在案例文件夾的 “_log” 子文件夾中 。

*如果案例屬性中案例日誌截圖的複選框被選中一半 ,這意味著不會截取對話窗口的實際圖形截圖 ,日誌中只會存儲一個簡單的文本表示 (與通過 Ctrl+C)。這些詳細信息以特殊方式包含在 HTML 輸出中 ,因此它們不會對主要日誌條目造成太大影響 。

它們要么以較小的字體和灰色輸出 (如果報告選項中的 “帶屏幕截圖” 被完全選中) ,或者當鼠標光標懸停在節省空間的佔位符矩形上時僅作為彈出窗口 (如果選中一半) 或根本沒有 (如果未選中) 。佔位符矩形和彈出窗口在 Google Chrome 中查看時效果最佳 ,因為該瀏覽器不會截斷冗長的文本 ,甚至會在佔位符矩形中顯示第一行的預覽 。如果您讓 X Ways Forensics 對日誌中的對話框進行常規 (圖形) 截圖 ,則可以將具有灰色背景顏色的像素更改為純白色 ,以節省碳粉/墨水 ,以防您在某個時間打印日誌 (無論如何 ,請三思並節省紙張) 。

5.6 痘例報告

您可以從案例數據窗口的文件菜單創建報告 。報告保存為 HTML 文件 ,因此可以在各種應用程序中顯示和打開 。例如 ,您可以在您最喜歡的 Internet 瀏覽器中查看它 ,然後在 MS Word 中打開並進一步處理它 。可以在 Options | 中指定打開報告的應用程序 。查看器程序 。如果沒有定義此類程序 ,報告文件將在與您計算機上的文件擴展名關聯的應用程序中打開 。使用 “打開報告” 命令 ,您可以選擇任何現有文件並在定義的或關聯的應用程序中打開它 。

報告可以包含以下元素：

·**基本報告**：以可選的標題行、可選的徽標、可選的前言（您可以在其中使用 HTML 代碼）、案例標題和詳細信息開始，然後是指向各個證據對象部分的超鏈接列表。對於每個證據對象，報告都指定了它的標題、詳細信息和技術描述、您的意見和註釋。如果只勾選一半，案情報告中不包含證據對象的技術細節，只是列舉證據對象。如果報告是為組織外部人員生成的，則可以選擇不在案例報告中顯示檢查員姓名、案例路徑和圖像路徑等內部信息。還有一個選項可以不顯示證據對象的技術描述。這可能有助於避免在法庭或其他地方與計算機外行就什麼是“扇區大小”等進行不必要的討論。

·**報告表**：選定報告表中的所有文件都可以輸出到報告中，並帶有選定的元數據，例如文件名、路徑、時間戳、註釋。可以選擇將文件從證據對象複製到保存報告的子目錄中。然後他們也將從報告中鏈接。要么可以復制所有文件，要么只能複製圖片。如果只有圖片，對於視頻，至少會復制第一張靜止圖像（如果可用）並用於在報告中表示視頻。默認情況下，圖片將直接顯示在 HTML 報告文件中，而不僅僅是鏈接。它們的大小會調整為您指定的最大尺寸，同時保持其縱橫比。如果指定最大尺寸為 0×0 ，則圖片將只被鏈接，就像其他文件一樣。如果您選擇在同一行中引用多個文件（以在打印時使報告更緊湊），您會發現長文件名和路徑可以在用戶定義的像素數後人為地分成多行，以確保寬度不超過紙張尺寸。

有一個選項可以只製作標記文件的副本以包含在案例報告中，而不是全部或不包含。如果您希望在報告中引用所有值得注意的文件及其元數據，但僅顯示其中的一部分，則很有用。某些受支持類型的文件可以轉換為 PDF 格式，以供報告的收件人使用，否則他們將無法使用合適的應用程序來查看文件。您可以定義不需要轉換的文件類型，例如可以通過網絡瀏覽器或 Windows 工具輕鬆顯示的文件類型。如果無法轉換，將復制原始文件而不進行轉換。

文件可以按證據對象分組並按內部 ID 排序或按當前在案例根窗口中列出的順序輸出，您可以根據最多 3 個排序標準自由更改順序。如果案例根中當前沒有文件列出（因為它還沒有被遞歸探索），那麼第二個選項是灰色的。

首先以遞歸方式探索案例根以使其可用（右鍵單擊它）。請注意，如果您選擇第二個選項，則不會輸出未在案例根窗口中列出的文件，即使它們是報表的一部分。這意味著當前的過濾器設置也會影響報告的生成。如果文件由於生成報告時未在案例根窗口中列出而被省略，您將在報告和消息框中收到通知。

如果輸出報表的框只被選中一半，則只報告每個報表中的項目數。

許多不同的設置允許根據您的喜好調整報告。例如，您可以根據其唯一 ID 命名輸出文件，以確保文件名簡潔、唯一、可跟蹤和可重現，這也將確保如果相同的文件與多個報告表相關聯，它只會被複製到報告子目錄一次。這樣可以節省時間和驅動器空間。您還可以根據文件的哈希值或其他各種或多或少的獨特屬性來命名文件。如果這些恰好為空白，則將使用原始名稱。

“只列出每個文件一次”是一個三態復選框。如果完全勾選，則沒有一個文件會在一個報告中被多個報告表引用。請注意，如果您輸出“報告表”字段，則當文件在報告中的第一個報告表中列出時，您仍然可以看到該文件的所有報告表關聯。如果該復選框被半選中，這意味著如果一個文件具有多個關聯，它仍將被報告中的其他報告表引用（列出），但僅複製一次並僅從第一個報告錶鍊接。

一個特殊的選項允許以 HTML 格式從案例報告中的文件中輸出完整的內部元數據，而不是以純文本格式在元數據列中提取的子集。如果您希望在您的案例報告中輸出文件的哈希值，並且您之前沒有通過優化卷快照計算哈希值，則可以選擇在生成報告時即時計算哈希值。

可以選擇專門為報告生成較小版本的圖片，以大大減少加載 HTML 報告時 Internet 瀏覽器或文字處理應用程序的內存需求，並加快加載速度。對於包含許多高分辨率照片的報告，這可能會產生很大的不同。JPEG 壓縮因子是用戶可定義的。分辨率取決於指定的“圖片的最大尺寸”。表示此選項的復選框是一個三態復選框。如果選中一半，則圖片的較小版本僅用於直接在 HTML 報告中進行預覽。如果完全勾選，即使點擊報告中的圖片也只會看到較小的版本，而原來較大的文件根本不會包含在報告中。如果您主要關心的是帶有鏈接文件的報告的驅動器空間要求，而不是圖片的輸出質量，那麼這可能是有益的。

報告還可以選擇性地顯示非圖片文件的預覽/縮略圖，例如Office文檔、電子郵件、網頁、程序源代碼等，類似於圖庫。

您可以稍微或大量或根本不縮小預覽表示，以便能夠在不打開文檔的情況下直接閱讀報告中的某些文本，或者更好地了解文本的整體格式並僅查看徽標等等。

·可以選擇輸出標記為包含在報告中的搜索結果，並在左側和右側顯示上下文。如果文件是報告表的一部分並且該報告表實際上在報告中輸出，則文件相關搜索命中會輸出到有關相應文件的報告表部分，以及所有選定的文件元數據。如果沒有，這樣的搜索

可以在有關它們所屬的證據對象的部分中找到命中。純物理用戶搜索命中（在磁盤/分區模式下定義，而不是文件模式）始終在關於證據對象的部分中輸出。

·案例日誌

默認情況下，報告是為整個案例創建的。可選地，它僅為選定的證據對象創建。使用CSS（級聯樣式表）進行病例報告格式定義相對容易。除了為標準HTML元素定義參數外，還為報告的關鍵元素分配了“類”參數，以簡化用於格式化目的的定位。

示例樣式表可用作進一步修改的基礎。報告選項允許選擇或編輯CSS文件作為報告過程的一部分。默認為“案例報告.txt”。v18.0及更早版本的默認外觀仍可作為“Case Report Classic.txt”使用。

您可以選擇將HTML案例報告轉換為PDF格式。這不能與在一定數量的文件之後拆分報告文件的選項一起使用。如果完全選中帶有PDF選項的框，則意味著您將*僅*收到報告的PDF版本。如果選中一半，則意味著您將收到報告的HTML和PDF版本。請注意，如果您在Windows資源管理器/文件資源管理器中刪除其中一個，這將自動刪除包含複製文件的相應子目錄（如果有的話），即使相應的其他版本的報告仍然需要它。

5.7 報告表

在證據對象的目錄瀏覽器中，您可以將重要文件與報告表相關聯。

報告表是用戶定義的（虛擬的）文件列表，尤其是值得注意的文件。然後，與報告表關聯的文件可以很容易地包含在案例報告中，包括它們的所有元數據甚至鏈接（可以直接包含圖片），您可以在遞歸視圖中按它們的報告表關聯進行過濾，以便以後輕鬆定位這些文件（如書籤文件）。該過濾器可以同時引用多個報告表（使用OR、AND和NOT運算符），甚至還有一個選項允許額外包含某個報告表文件的兄弟文件，即同一目錄中的文件。這很有用，尤其是在遞歸探索和按路徑排序時，以檢查附近是否還有其他值得注意的文件。

例如，您可以創建報告表，如“與X公司有關”、“針對嫌疑人A的證據”、“定罪圖片”、“不正當支出”、“轉發給調查員B”、“稍後打印”、“獲得翻譯”、“顯示見證C”等，稍後當您完成查看文件時，您可以通過使用報告表篩選器獲得所有相關文件的大圖（例如“顯示與公司X相關的所有文件，這些文件也被認為是針對嫌疑人的證據乙”）。您實際上是將文件分配給您自己定義的某些自定義類別。還允許您稍後重新訪問仍在仔細檢查的文件。

將文件放在專用報告表中還允許在以後的某個時間點方便地通過一個步驟複製/恢復它們，或者專門獲取這些文件的畫廊概覽。同一個文件可以關聯多個報表。這可以在目錄瀏覽器上下文菜單中調用報告表關聯命令時出現的對話窗口中完成，

一次為一個文件或幾個選定的文件。此對話框窗口不顯示所選文件的現有關聯（對於多個所選文件來說實現起來會相當複雜，而是簡單地查看“報告表”列），而是以方便的方式創建新的報告表關聯和用戶可配置的方式和/或刪除現有的關聯。該程序會記住最後選擇的用於創建關聯的報表。在同一對話窗口中，您還可以創建新的報告表、重命名或刪除現有報告表，以及刪除/覆蓋以前的關聯。對於每個報告表，您可以指定您通常是否希望僅將所選文件或目錄關聯到該報告表和/或同時關聯所選文件的父文件（如果有）和/或文件或目錄的子對象和/或任何當前打開的證據對像中所選文件的任何已識別副本（已根據哈希值識別並在 Attr. 列中相應標記的重複項，請參閱上下文菜單，以及除 HFS+ 之外的硬鏈接）。

另一個選項允許自動將選定文件的兄弟文件與報告表相關聯。

例如，在查看搜索命中時很有用，如果您在電子郵件的附件中找到相關的搜索命中，並且希望確保在進一步處理中包含同一電子郵件的其他附件，即使它們不包含搜索命中。

如果您需要藉助報告表對大量文件進行分類，您還可以使用鍵盤快捷鍵。X-Ways Forensics 自動將快捷方式 Ctrl+1、Ctrl+2、...、Ctrl+9 分配給您的報告表。在報告表關聯的對話框窗口中，您也可以自己將這些快捷方式分配，只需在選擇報告表時按下按鍵即可。

或者，如果 Num Lock 處於活動狀態，您可以直接按下鍵盤上數字鍵盤中的鍵，而無需使用 Ctrl。儘管未按下 Ctrl 鍵，但在目錄瀏覽器中這不會被視為正常輸入。數字小鍵盤鍵可能不適用於所有計算機。Ctrl+0 從所選文件中刪除所有報告表關聯。Alt+1, Alt+2, ..., Alt+9 從所選文件中刪除與相關報表的關聯。

可選地，在將一個項目與報表相關聯後，可以自動選擇目錄瀏覽器中的下一個項目。三態復選框允許您從不或僅對使用鍵盤快捷鍵創建的關聯或對所有關聯方法執行此操作。

您可以通過單擊報告表關聯對話框中帶有“屬性”圖標的按鈕，為任何報告表輸入自由文本描述。如果輸出報告表，則描述將包含在案例報告中。對於報告表的內容的一些解釋很有用。有助於使出現在用戶界面中許多地方的報表表名稱本身更加簡潔。

報告表可以在對話框窗口中按字母順序排序以進行過濾和報告表管理。默認情況下，它們按照創建順序列出，和以前一樣。

由應用程序創建的作為用戶提示的報告表是可選的，並且它們以縮進顯示。

有一個選項可以根據文件根據“搜索詞”列包含的搜索詞為文件創建報告表關聯。如果您希望在刪除搜索命中後仍保留有關哪個文件包含哪些搜索詞的信息，或者將其保存在證據文件容器中，則很有用。表示包含的搜索詞的報告表是第三種報告表，前兩種是 X-Ways Forensics 創建的報告表，使用戶

了解某些文件特性和用戶創建的通用報告表。

另一個選項允許將匹配的哈希集轉換為報告表關聯。這可能很有用，例如，如果您希望從頭開始重新創建哈希數據庫或刪除哈希數據庫，並且不僅希望保留卷快照中已知文件的哈希類別，還希望保留精確匹配的哈希集名稱。如果您希望將文件添加到證據文件容器並希望讓收件人知道原始哈希集匹配，而不僅僅是哈希類別，這也很有用。這些輔助報告表以不同的顏色突出顯示，以區別於其他類型的報告表。在將文件複製到證據文件容器時，也可以即時創建與基於散列集的報告表的關聯。

總共有 5 種不同類型的報告表：1) 用戶創建的報告表，可能用於報告目的，也可能不用於報告目的，2) X-Ways Forensics 創建的報告表，讓用戶了解文件的特殊屬性，3) 代表文件中包含的搜索詞的報告表，4) 代表在其中找到文件的哈希集的報告表，5) 代表重複文件組的報告表。為了避免在報告創建期間可供選擇的報告表列表過大，現在僅當報告表確實用於報告目的時才會在該對話框窗口中提供報告表。默認情況下，所有用戶創建的報告表都採用這種方式。您可以通過分配或刪除“星號”符號，在報告表關聯對話框窗口中切換每個報告表的報告用途。

可以在報告表關聯對話框窗口中保存和加載報告表名稱及其描述的列表。這對於立即開始使用特定類型案例通常需要的一組預定義報告表很有用。保存的文件是人類可編輯的。格式可以是：a) 每行一個報告表名稱（如果不需要說明）。不允許有空行。b) 報表名稱，前面是 Unicode 字符 U+25B8（黑色右指小三角形），後面是換行符和任何描述。根據需要重複。

在這兩種情況下，文件都必須採用帶有初始字節順序標記的 UTF-16 格式。一個案例中報表的最大個數為 1000 個。

可以導出和導入報告表關聯。請參閱共享分析工作的替代方法。可以使用更易於使用和簡化的對話窗口版本來創建報告表關聯，減少可能會使新用戶感到困惑的設置，這是 X-Ways Investigator 中的默認設置，並且可以選擇在 X-Ways Forensics 和 X-Ways 調查員。例如，在簡化版本中，應用程序創建的讓用戶知道某些內容的報告表將不會列出，並且可以在不使用鍵盤快捷鍵的情況下專門從所選文件中刪除報告表關聯。

為了將報告表輸出到報告（報告表的最初用途，因此得名），請使用案例數據窗口中的創建報告命令。

報告表關聯也在內部使用並由 X-Ways Forensics 自動創建，以使用戶了解某些文件的各種潛在特性。是否要跟進並仔細查看這些文件取決於您。內部創建的報告表的名稱以縮進顯示並以不同的顏色顯示，以避免與您自己的報告表混淆。自動生成的報告表包括：

沒有可檢測的文本內容 無法解碼文
本 有關錯誤消息 ,請參閱元數據 無
法探索空存檔 ?

跨區存檔 未找到電
子郵件 路徑太長 。

大型非駐留 \$EA 動畫 GIF
動畫 PNG 多頁 TIFF 多頁
JPEG 標記 手機截圖 ?

拉鍊炸彈 ?未完全處理 意外的尾巴
(SFX ?) /包含未知片段 (SFX ?)
FSG Packer / PECompact / UPX / Unknown segment / Binder?
包含嵌入文檔
包含嵌入對象
包含嵌入文件 包含隱藏文
件 混合 MS Office 文檔 !

RAR hybrid
包含嵌入的非 JPEG/非 PNG 圖片 包含不可見的舊修訂
Concatenated-PDF 包含私有塊 未提取圖片 崩潰原因 ?

不支持的文件類型變體 省略 未復
制 懷疑有病毒 無法讀取 未解壓

5.8 查看器功能

可以使用 “工具”菜單和目錄瀏覽器的上下文菜單中的“查看”命令以及預覽模式調用內部查看器。它顯示各種文件
格式的圖片文件 (JPEG、PNG、GIF、TIFF、BMP、WEBP、HEIC、一些 DICOM 變體、PSD、HDR、PSP、PCX、
CUT、ICO，使用內部圖形查看庫)加上結構Windows 註冊表文件、Windows 事件日誌 (.evt 和 .evtx) 、
Windows 快捷方式文件 (.lnk)、Windows 預取文件、\$LogFiles、\$UsnJrnl:\$J、Ext3/Ext4.journal、.ds_store、
Windows 任務計劃程序 (.job)、\$EFS LUS、INFO2、Restore Point change.log.1、wtmp 和 utmp 登錄記錄、
MacOS X kpassword、MacOS X finder 書籤 (flnk)、AOL PFC、Outlook NK2 自動完成文件、

Outlook WAB 地址簿、Internet Explorer 旅行日誌文件（又名 RecoveryStore）、Skype 聊天同步、MS Outlook Express DBX 和許多其他內部文件。如果您嘗試查看內部查看器不支持的文件，則會調用單獨的查看器組件。

還有一個額外的獨立查看器組件，可以無縫集成並允許方便地查看超過 270 (!) 種文件格式（例如 MS Word、Excel、PowerPoint、Access、Works、Outlook；HTML、PDF、StarOffice、OpenOffice、...）直接在 WinHex 和 X-Ways Forensics 中。此組件提供給為 v12.05 及更高版本頒發的取證許可證的所有所有者。它可以在選項 | 中啟用。查看器程序，也可選擇用於可以由內部圖形查看器庫顯示的圖片。[更多信息在線](#)。單獨查看器組件使用的臨時文件文件夾由 WinHex/X-Ways Forensics 控制，即設置為用戶在常規選項中指定的文件夾。但是，與 X-Ways Forensics 不同的是，查看器組件不會默默地接受只讀媒體上不合適的路徑。

請注意，自版本 8.2 起，查看器組件會在當前登錄用戶的 Windows 配置文件中創建文件，並在其中存儲其配置和設置。在早期版本中，如果實際使用，而不僅僅是加載時，它會在系統註冊表中留下條目。

如果密碼可用，查看器組件允許查看或預覽某些受密碼保護的文檔。僅支持 Microsoft Office 和 PDF 文檔、Microsoft Outlook PST 97-2013 和 Zip 文件的某些加密變體。預覽此類文件時，密碼將從該文件的元數據單元格中獲取（如果在以“密碼：”開頭的行中可用），否則將自動嘗試當前活動案例密碼集合中的所有密碼。如果密碼集合中的其中一個密碼匹配，它將被記住在文件的元數據單元格中以供將來重新使用和用戶信息。查看此類文件時，如果沒有找到匹配的密碼，則會額外提示用戶輸入密碼，直到他或她提供正確的密碼或放棄（單擊取消）。

註冊表查看器

MS Windows 維護一個稱為註冊表的內部數據庫，它包含本地系統的所有重要設置和樹狀結構中安裝的軟件。數據永久存儲在稱為註冊表配置單元的文件中。您可以通過在目錄瀏覽器中雙擊或使用上下文菜單來打開和查看配置單元。這將在集成註冊表查看器中打開它們。支持的格式是 NT/2K/XP/Va/7 配置單元。Win9x 和 WinMe 配置單元只能由 X-Ways Forensics 15.9 及更早版本的註冊表查看器加載。NT/2K/XP/Va/7 配置單元位於用戶配置文件中的文件“ntuser.dat”和目錄 \system32\config 中。

在註冊表查看器中最多可以同時打開 32 個配置單元。註冊表查看器能夠在包含未使用空間的配置單元中查找已刪除的鍵和值，並在損壞/不完整的配置單元中查找丟失的鍵/值。如果不知道密鑰的完整路徑，它們將被列為名為“路徑未知”的虛擬密鑰的子項。

通過右鍵單擊，可以在窗口的任何位置打開一個彈出菜單，它可以讓您調用命令“搜索”和“繼續搜索”。單擊“搜索”會調用一個對話框，您可以在其中指定搜索表達式和要搜索的位置。您可以瀏覽鍵或名稱或值或所有這些。搜索總是從第一個加載的配置單元的最頂層根開始，並跨越所有打開的配置單元。“繼續搜索”在至少匹配了一個匹配項後找到下一個匹配項。

成立。當前選擇的元素與繼續搜索的位置無關。“僅搜索整個單詞”選項不保證對值有效。

在右側窗口中，彈出菜單還包含命令“複製”，可讓您將所選元素的值複製到剪貼板。

當在註冊表查看器中點擊一個已加載的配置單元的值時，如果加載配置單元的驅動器/圖像的數據窗口處於文件模式，則光標將自動跳轉到註冊表文件中的所選值，並且該值將自動被選為該文件中的一個塊。有用的是，它允許以十六進制和文本形式查看值，並且允許以二進制或文本形式輕鬆複製二進制值，而不僅僅是十六進制 ASCII。

註冊表查看器上下文菜單中的導出列表命令允許將所選配置單元中的所有值導出到製表符分隔的文本文件。

選擇一個值時，右下角的編輯窗口會告訴您該值的邏輯大小及其鬆弛度的大小。它還解釋以下類型的註冊表值，從註冊表報告中得知：MRUListEx、BagMRU、ItemPos、ItemOrder、Order（菜單）、ViewView2、SlowInfoCache、IconStreams（托盤通知）、UserAssist、Timestamps（FILETIME、Epoch、Epoch8）、MountedDevices、OpenSavePidlMRU 和 LastVisitedPidlMRU。

如果選擇了（默認），編輯窗口還會顯示註冊表項的訪問權限/權限。

\$日誌文件查看器

基本概念：每條語句

都屬於以下三類之一：1) 日誌操作 在重做/撤消操作的情況下，磁盤上的數據 (LCN，字節偏移量) 將被替換為日誌中指定的數據手術。

2) PAGE 語句指示新日誌頁的開始 (4 KB 的倍數)。LSN 指定此頁面的最後一個結束 LSN。* 標記過時的頁面。

3) CheckPoint 語句指定了一個用於重新啟動的 LSN。

每個語句之前都有一個指向 \$LogFile 的字節偏移量。

縮寫：

LSN=邏輯序號

LCN=邏輯簇號

VCN=虛擬集群號

FID=文件ID

限制：僅顯示影

響磁盤結構的日誌操作。FILE 記錄和 INDX 緩衝區未完全轉儲。對於完整的數據，請遵循為感興趣的操作顯示的字節偏移量。只有當此類文件的路徑包含字符串 \$LogFile 時，才會處理 NTFS 日誌。

5.9 註冊報告

在註冊表查看器中，當您在右鍵單擊彈出菜單中調用“創建註冊表報告”命令時，WinHex 可以創建一個 HTML 報告，列出可能相關的註冊表項的值。要在所有打開的配置單元中報告的註冊表項在文本文件中定義，例如預先提供的“Reg Report *.txt”，可以根據您的需要進行定制。您查看的註冊表文件必須有其原始名稱，否則報告可能會失敗。您可以編輯此文件中的註冊表項列表以根據您自己的需要定制報告。

標準表有 4 列：描述、提取的值、註冊表路徑（作為工具提示提供）和相應鍵的最後修改日期。對於不是其各自鍵中唯一值的值，日期以灰色顯示，作為視覺輔助提醒讀者它們不是值本身的修改日期。

可以使用報告定義文件“Reg Report Free Space.txt”分析註冊表配置單元中的可用空間。可用空間可能大到幾 MB，尤其是在使用病毒掃描程序和註冊表清理程序的情況下。已刪除的註冊表值現在在報告中以紅色突出顯示。

註冊表值 slack 在 NTUSER.DAT 配置單元中也有相關的大小。這個事實被利用了 2

措施：

- 1) 如果 slack 包含文本字符串，它將在註冊表報告中輸出（綠色）。可以選擇關閉此新功能的註冊表查看器上下文菜單。
- 2) 對於包含項目列表（即二進制）的值，您可以使用“Reg Report Free Space.txt”定義來輸出註冊表報告將輸出帶有綠色時間戳的文件名列表。第一個時間戳是訪問日期，第二個是創建日期。如果無法輸出時間戳，則這些是來自“RecentDocs”的工作。

“Reg Report *.txt”中的條目格式

(類型) (製表符) (註冊表路徑) (製表符) (描述) (換行)

類

型：??任何 Windows 版本的定義 NT for
Windows NT through XP VT for Windows Vista
and 7 new function (without absolute paths)
**

hive空閒空間FR查詢

註冊表路徑：

註冊表項的完整路徑

HKLM :HKEY_LOCAL_MACHINE
香港中文大學 :HKEY_CURRENT_USER

如果提供星號（ * ）作為最後一個鍵，則同一級別和更深級別的所有鍵及其值都將包含在報告中。

例子：

NT HKLM\Software\Microsoft\Windows\CurrentVersion* 報告整個 Windows 分支

如果您希望報告存在於某個鍵的所有子鍵中的特定值，您也可以為所有子鍵寫一個“*”，然後包含該值。

生成的報告包含註冊表路徑及其時間戳，在其中找到密鑰的註冊表配置單元的文件名、“Reg Report *.txt”文件中提供的描述以及值。

描述字段末尾可能包含一個以 % 字符開頭的附加語句。如果 % 後跟數字字符 n，則註冊表路徑的第 n 個元素將附加到報告中的描述中。如果路徑而不是值（或不僅是值）包含相關信息，這將非常有用。如果 % 後跟一個字母，則該值最好被解釋為該字母代表的數據類型。目前定義了以下字母和數據類型：%f Windows FILETIME 時間戳 %e Epoch (Unix) 時間戳 %E Epoch8 (Unix) 時間戳作為 QWORD %D 十進制數 %T Windows 系統時間時間戳 %s ANSI-ASCII null-終止 %S UTF-16 字符串空終止 %b 二進制數據不被解釋為字符 (REG_BINARY)

%P Windows PIDL 數據結構 %I ItemPos
數據結構（涵蓋 Shell Bag、桌面快捷方式等）
%B 條件：如果值為 TRUE %F 條件：如果
值為 FALSE %- 無空模式 %+ 子樹的遞歸
%i 值不區分大小寫 %d 僅刪除值 也可以
組合數字字符和字母（例如 %10f）。在這種
情況下，數字字符必須在字母之前。

// 在一行的開頭註釋掉該行（將導致它被忽略）。## 在一行的開頭將解釋性文本輸出
到報告中。

附加輸出

在創建註冊表報告的第二階段，將分析附加數據並將其輸出為 HTML 文件末尾的表格。屬於該第二階段的定義文件中的規範標有“Dummy”。這導致第一階段阻止任何正常輸出。如果您想獲得第一階段的輸出，只需將定義中的描述更改為“Dummy”以外的任何內容。

“Attached devices by serial number”表是根據 Harlan 的算法創建的

Carvey 在他的書的第 4 章中描述了這一點。此外，您還可以找到“按磁盤簽名劃分的分區”、“Windows 便攜式設備”、“已安裝的驅動程序”、“已安裝的文件系統”、“已安裝的服務”、“網絡”和“網卡”表格。

另一個表稱為“瀏覽器助手對象”，使用來自配置單元 NTUSER.DAT 和 SOFTWARE 的關於瀏覽器使用情況的數據編譯而成。“外部存儲設備”是一個可以從 Windows Vista 和更高版本的軟件配置單元中檢索到的表格，其中列出了具有訪問時間戳、硬件序列號、卷標、卷序列號和卷大小（大小通常僅在 Vista 下）的外部媒體。選擇定義文件“Reg Report Devices.txt”獲取表格。

5.10 同時搜索

搜索菜單中的此搜索命令適用於專家和取證許可證的所有者，並且僅為取證許可證的所有者提供所有選項。這種搜索是同時進行的，因為它允許用戶指定幾乎無限的搜索詞列表，每行一個。這些搜索詞的出現被保存並列在證據對象的搜索命中列表中（法醫許可，在處理案件時，為了獲得完整的功能，強烈推薦），或者在一般位置管理器中。

默認情況下，相同搜索詞的搜索命中會合併，並可通過搜索詞列表中的相同項目進行訪問。例如，當在不同的證據對像中以增量方式（多次運行）運行對相同關鍵字/正則表達式的搜索時，這很有用。

但是，您可以取消選中一個複選框，以便始終在搜索詞列表中生成新項目，即使您要查找的關鍵字與以前使用的關鍵字或同一運行中的關鍵字相同。如果您使用不同的設置運行搜索（例如，相同的關鍵字同時作為一個完整的詞而不是一個完整的詞），這將很有用，以便以後能夠區分結果搜索結果。

您可以使用同時搜索系統地在多個硬盤或磁盤映像中搜索“藥物”、“可卡因”、（可卡因的街道同義詞 #1）、（可卡因的街道同義詞 #2）、（街道可卡因的同義詞#3），（可卡因的街頭同義詞#3，替代拼寫），（經銷商#1 的名稱），（經銷商#2 的名稱），（經銷商#3 的名稱）等。搜索結果可以將檢查範圍縮小到要關注的文件列表。

同步搜索可用於在扇區中進行物理搜索，或在文件或先前創建的索引中進行邏輯搜索。實際上，它按 LBA 順序搜索介質上的扇區（除非您向上搜索，然後按相反的順序搜索）。如果您沒有 WinHex 列出物理搜索的命中，您可以使用 F3 鍵搜索下一個命中。從邏輯上講，搜索是逐個文件進行的，這是更可取的，而且功能更強大、更徹底。有關邏輯搜索的更多信息。

您可以同時在最多 6 個代碼頁中搜索相同的搜索詞。在您的 Windows 系統中處於活動狀態的默認代碼頁標有星號並且最初是預選的。

例如，在美國和西歐的計算機上，通常的默認代碼頁是 1252 ANSI Latin I。Microsoft Windows 中使用名為“ANSI”的代碼頁。“MAC”表示

Apple Macintosh 代碼頁。“OEM”表示在 MS-DOS 和 Windows 命令提示符中使用的代碼頁。如果由於代碼頁中的未知字符而無法將搜索詞轉換為指定的代碼頁，則會發出警告。在稱為“正則表達式的直接逐字節轉換”的“非”代碼頁中搜索時，可以使用與代碼頁無關的 RegEx 搜索精確的字節值，該代碼頁可以轉換字節值，而無需對某些代碼頁進行任何映射或大小寫匹配。X-Ways Forensics 還允許在小端和大端 UTF-16 以及任何區域 Windows 代碼頁和應用了 MS Outlook 密碼（可壓縮加密）的 UTF16 中進行搜索。

在 X-Ways Forensics 和 X-Ways Investigator 中，您可以應用字符調整列表。（這裡的內部工作原理與相應的索引選項略有不同。）該列表應在名為“Character Adjustment.txt”的 UTF-16 文本文件中。它以小端字節順序標記開始，每行跟一個指令，中間有一個箭頭（大於符號），它將一個字符映射到另一個字符。您可以按照您認為適合的方式對其進行編輯，以便以您自己的語言進行搜索。法語搜索示例 :É>E 表示應用同步搜索的原始數據中的字母 É（當在合適的代碼頁中搜索時）將被接受為搜索詞中 E 的變體。

您只需搜索 Edith Piaf，即可找到 Edith Piaf 和 Édith Piaf。兩種變體都將在內部進行搜索。 $\text{ç}>\text{c}$ 表示搜索 Francois（如果您的鍵盤無法輕鬆生成 ç 字符，您可能會發現更可取）您可以找到 Francois（簡化拼寫）和 François（原始法語拼寫）。反之亦然： $\text{:c}>\text{ç}$ 表示搜索 François（如果對您來說更正確，您可能更喜歡這種方式），您可以同時找到 François 和 Francois。但是，不建議將後一種替換用於索引。即使您對匹配多個拼寫變體不感興趣，如果您不能輕易地用鍵盤生成特殊字母，您也可以一次性定義此類替換（例如使用複制和粘貼）。

不區分大小寫在字符調整之上不起作用。因此，例如當調整 $\text{é}>\text{e}$ 處於活動狀態時，對 e 的不區分大小寫的搜索將找到 e 和 é 以及 E，但不會找到 É。為此，您需要添加調整 $\text{É}>\text{E}$ 。請注意，理論上您可以僅使用字符調整來定義自己的不區分大小寫規則。同一個目標字符最多可以有 16 個映射。字符調整也可以與正則表達式結合使用（僅適用於在正則表達式中沒有特殊含義且不包含在 [] 集中的目標字符）。

您可以定義哪些字符應被視為單詞的一部分。這有助於避免錯誤命中二進制垃圾數據或 Base64 代碼中的短真實語言單詞，並且通常適用於將數字視為單詞一部分的用戶（例如“GIF89”）。示例：如果您僅在將字母表重新定義為包含數字 0-9（即，將它們視為單詞字符）時將其作為整個單詞進行搜索，則可以避免對“7HZsIF9BAND4TpksBSBS”中的“band”的意外命中。

可以在正在進行的同步搜索中查看（不完整的）搜索命中列表。您可以隨時點擊搜索命中列表按鈕，查看初步搜索命中列表。

當您像往常一樣通過單擊搜索詞列表中的 Enter 按鈕刷新搜索結果列表時，將列出隨著搜索繼續收集的其他搜索結果。這種查看初步搜索結果的方法很有用，例如，在現場預覽實時系統以確定媒體是否可能包含相關文件並應被捕獲時。如果之後

搜索 5% 的數據並查看到目前為止收集的搜索結果，答案是肯定的，搜索已經可以停止並且節省了大量時間。

5.11 邏輯搜索

同時搜索的強大子變體。允許搜索所有文件、所有標記文件或（如果從目錄瀏覽器上下文菜單調用）所有選定文件。與物理搜索相比，邏輯搜索有幾個優點：

- 可以專門針對文件鬆弛（針對所有文件，或者如果只檢查一半，則針對未省略的文件）或忽略。在 X-Ways Investigator 中，鬆弛空間將被覆蓋；為簡單起見，只是複選框不可見。
- 通過標記或選擇文件，可以將搜索範圍限制在某些文件和文件夾內。請注意，對話窗口中可能顯示的要搜索的數據量只是估計值。搜索的實際範圍可能因空間不足而有所不同。
- 在文件中搜索（通常 = 在分配給文件的集群鏈中）將找到搜索命中，即使搜索詞恰好在碎片文件中物理拆分（出現在不連續集群的結尾和開頭）。
- 即使在 NTFS 文件系統級別壓縮的文件中，邏輯搜索也可以成功，因為這些文件被解壓縮以進行搜索。這甚至適用於通過文件頭簽名搜索找到的文件，如果它專門適用於 NTFS 壓縮。
- 有一個專用複選框來控制是否針對 NTFS 壓縮的某些鬆弛區域。它沒有標籤，但有一個工具提示。如果完全選中，普通 NTFS 壓縮文件的每個壓縮單元末尾的未定義鬆弛區域將被原始搜索（按原樣，不解壓）。如果該複選框至少被選中一半，則 WofCompressed 文件的定義明確的鬆弛部分是目標（搜索原始文件，沒有解壓縮）。
- 如果檔案的內容（ZIP、RAR、GZ、TAR、BZ2、7Z 和 ARJ 中的文件，如果未加密，僅取證許可證）和個人電子郵件消息和附件已包含在卷快照中，它們可以也被搜查。
- 查看器組件支持其格式的文件中包含的文本，例如 PDF (Adobe)、WPD (Corel WordPerfect)、VSD (Visio)、SWF (Shockwave Flash)，可以在搜索之前自動提取/解碼/解壓縮，從而生成無格式的 ASCII 或 UTF-16 明文，可以在除了原始數據本身。否則可能會錯過搜索命中，因為各種文件類型通常或至少有時以編碼、加密、壓縮、碎片化或其他亂碼方式存儲文本。重要提示：特別是對於 HTML、XML 和 RTF 文檔以及 .eml 文件中的 HTML 格式的電子郵件消息，它們可能使用

編碼（例如 UTF-8）非 7 位 ASCII 字符（例如德語變音符號）的各種方法，解碼可能會有用，具體取決於您的搜索詞的語言/搜索詞中包含的字符。當您指定用於解碼的文件掩碼時，該掩碼不僅會應用於搜索到的文件的名稱，而且如果經過簽名驗證，還會應用於它們的真實類型（請參閱精簡卷快照）。此功能要求單獨的查看器組件在解碼和文本提取部分處於活動狀態。解碼後的文本以 Latin 1 或 Unicode 格式輸出，並且可以選擇進行緩衝（參見選項 | 查看器程序），以便為解碼文本中的搜索命中提供方便的上下文預覽，並加速未來的搜索。此選項的默認文件掩碼是 *.pdf;*.docx;*.pptx;*.xlsx;*.odt;*.odp;*.ods;*.pages;*.key;*.numbers;*.eml;*.wpd;*.vsd。

建議根據搜索的字符添加;*.html;*.xml;*.rtf，更多取決於你的要求。例如，如果您想要非常詳盡，*.doc 可能是個好主意，因為在 MS Word 文檔的中間，文本可能會支離破碎或從一種字符集突然更改為另一種字符集。請記住，額外的解碼和搜索需要更多時間，並且會導致重複的搜索命中（在原始格式和文本提取結果中找到的搜索命中）。當僅搜索 7 位 ASCII 字符時，電子郵件通常不會被 X-Ways Forensics 解碼。文件掩碼應用於文件名和檢測到的真實文件類型。要查看此功能從文檔中提取了哪些文本，您可以在預覽模式下的目錄瀏覽器中選擇文檔，並在切換到原始模式時按住 Shift 鍵。

- 能夠查找數字和日期，不僅可以按字面存儲為文本，而且可以查找以二進制形式存儲在某些電子表格文件（例如 OLE2 複合文件格式）或其他編碼形式（例如編碼為 XML 中的文本整數的日期）中的數字和日期，如果“解碼文本”選項打開並且如果在 Options | Viewer Programs 複選框“將電子表格中的數字/日期的二進制存儲轉換為文本”被選中。但是，這比常規文本解碼慢。這對於 Excel 和 LibreOffice Calc 電子表格中的數字非常有效，但如果原始 Excel 用戶選擇了自定義日期格式而不是標準日期格式之一，並且由於某些特殊性，有時日期格式可能會很棘手無法 100% 預測日期將以預期格式提取的計算文件。這種搜索可能也適用於某些其他文件類型，例如較舊的電子表格類型，如 MS Works 或 Lotus 123。您可以嘗試在選項 | 中定義文件類型 | 查看器程序（如果需要）。要快速查看並仔細檢查從感興趣的特定文件中提取的數字和日期，您可以在目錄瀏覽器中選擇該文件，然後按住 Shift 鍵從普通預覽模式切換到原始預覽模式。如果您不需要在電子表格中搜索數字和日期，請完全刪除那裡的文件掩碼以加快文本解碼速度。

有關數字搜索的更多詳細信息：考慮 MS Excel 電子表格中的一個單元格，其中包含數字 1234567。您現在可以通過同時搜索簡單地搜索“1234567”（不帶引號）來找到該數字。即使您只知道部分數字序列並蒐索“34567”，您也會獲得搜索命中（除非“僅全字”選項打開）。如果單元格具有“數字”格式（不是“一般”），並且啟用了數字分組，您可以選擇在第一次在該卷快照中搜索/索引/解碼文件時獲取帶有數字分組的數字。

時間，使用在 Options | X-Ways Forensics 中定義的數字分組符號表示法，但通常不建議這樣做，因為如果您不知道原始電子表格單元格的格式是帶或不帶數字分組的“數字”還是“一般的”。無論如何，再舉一個例子，如果您在選項 | 中的數字單元格中啟用該選項以進行數字分組。查看器程序和您住在英語國家，使用逗號作為數字分組符號，因此您將搜索“1,234,567”以在數字單元格中找到該數字。您也可以僅搜索“,567”以在該表示法中任何更長數字的末尾或中間找到數字組“567”。

如果您要查找的數字是浮點數，則適用相同的規則，並且您可以選擇輸入您希望在原始應用程序的單元格中看到的小數位數（或更少）的數字，使用與您在 X-Ways Forensics 中的符號設置中相同的十進制符號（點或逗號）。例如，如果浮點數存儲為 9.876 並格式化為顯示 2 位小數，則它將在原始應用程序中四捨五入顯示為 9.88，並且也可以像在 X-Ways Forensics 中那樣進行搜索。相同的規則適用於貨幣金額。如果您確定貨幣符號以原始格式顯示以及如何顯示（例如，貨幣符號和數字之間有或沒有空格），則可以附加或預先添加貨幣符號，或者您只是省略符號。

您可以使用 X-Ways Forensics 中活躍的符號作為所謂的簡單日期格式在純日期單元格中搜索日期。如果您的簡單日期格式是 MM/dd/YY，您將搜索 12/31/19 以查找日期 2019 年 12 月 31 日。部分日期搜索也是可能的，並且在您不使用美國日期樣式時尤其有意義。例如，在 ISO 符號“yyyy-MM-dd”中，您可以搜索“2019-07-”。或者在德語符號“dd.MM.yy”中，您可以搜索“.07.19”以查找 2019 年 7 月的任何日期。也可以進行純時間單元格搜索（使用部分或全部時間表達式）。只需確保使用 X-Ways Forensics 中的活動分隔符來顯示時間。支持搜索合併的日期和時間值，但是，您可以預期的日期和時間之間的分隔符不是選項 | 中定義的分隔符。符號，但通常是單個空格，或由電子表格用戶定義的單獨分隔符。

如果 Excel 工作表嵌入在 .docx、.pptx 或 .odt 文件中，並且卷快照已經過充分優化，則工作表將按照與單獨文件相同的方式進行處理和搜索。如果嵌入到 .doc 文件中，您會收到報告表關聯形式的通知“包含嵌入的文檔”，這對於手動檢查通常很有用。數字搜索功能應該證明非常有用，尤其是在法務會計、稅務欺詐調查等方面。請注意，普通（“漂亮”）預覽模式下查看器組件（Ctrl+F）的簡單搜索功能或 View 命令無法找到數字或電子表格中的日期，無論您如何鍵入它們。

您可以在選項 | 中啟用另一種方法，將電子表格中的數據提取為文本。查看器程序。該選項有點實驗性，需要 X-Ways Forensics 保留在前台。它提高了提取文本在單元格順序和排列方面的保真度，標準化了解碼文本中日期單元格的格式。

到 X-Ways Forensics 中活躍的符號以獲得更可靠的搜索結果，並且它可靠地包含隱藏的單元格。工作表的邊界和序號用分隔線標記。如果您需要保留您的活動 Windows 代碼頁不支持的字符（例如美國或歐洲的典型計算機上的中文字符），因為您要搜索它們，您需要選中一個額外的框（“必須支持 Unicode”），如果使用該選項，此方法將需要使用 Windows 剪貼板。

- OCR 功能。
- 如果您對每一個搜索結果都不感興趣，而只是對包含至少一個指定搜索詞的文件感興趣，則可以通過告訴 X-Ways Forensics 每個文件只需要一次命中來大大加快邏輯搜索，因此它可以在記錄命中後跳過文件的其餘部分並繼續下一個文件。生成的搜索命中列表在本質上和系統上都是不完整的，並且不必假設以某種方式收集每個文件中“最有用”的搜索命中，或者，如果使用多個搜索詞，搜索詞的搜索命中您認為更重要的將被收集。但是，可以保證它包含至少有一次命中（對於使用的搜索詞之一）的所有文件，並且每個這樣的文件只包含一次。這樣的列表足以（並且有效！）手動查看受影響的文件、對其進行評論、從圖像中複製文件或將它們傳遞給證據文件容器中的其他調查人員等。請注意，當然不可能如果每個文件僅記錄 1 次匹配，則將搜索詞與邏輯 AND 組合。毫無戒心的人通常會忘記這種後果

用戶。

- 從哈希數據庫中已知的文件（或者只知道不相關和未分類的文件，或者，如果完全檢查，甚至已知值得注意的文件）已被用戶排除或被活動過濾器過濾掉的文件可以從邏輯搜索以節省時間並減少不相關搜索命中的數量。如果“Open and search files incl. slack”選項被完全選中，這些文件的 slack 仍然被覆蓋，因此該選項具有更高的優先級。如果只檢查一半，這些文件的鬆弛部分也會被忽略。
- 推薦的數據縮減專門從搜索中省略了某些文件，以避免浪費時間或產生不必要的重複匹配。

如果支持類型（ZIP、RAR 等）的文件存檔中包含的文件已包含在卷快照中，則不會搜索它們以節省時間。在這種情況下，只會搜索那些處於自然（未壓縮）狀態的提取文件。

這對於關鍵字搜索可能是合理的，特別是對於索引（它很難處理，例如 Base64 代碼），但對於簽名等技術搜索則不一定。使用此選項構成折衷。如果啟用了 file slack 選項，歸檔文件的 slack 仍然包括在內，因為該選項具有更高的優先級。

如果啟用數據縮減並且主要搜索卷中的所有文件（而不是僅標記或選定的文件），則不會搜索標記為重命名/移動的文件，因為已搜索相同的文件在其下

當前名稱/當前位置。

如果 *.docx; *.pptx; *.xlsx; *.odt; *.odp; *.ods; *.pages; *.key; *.numbers 被解碼用於搜索，包含的 .xml 文件與主要內容 (document.xml \content.xml \index.xml ...) 以及在 .pages 的情況下，任何現有的 Preview.pdf 也被省略，以避免冗餘搜索命中。

帶有紅色 X 圖標的文件將不會被搜索，除非它們是通過選擇或標籤標記專門定位的。

- 在 NTFS 中，除了一個以外的所有“真實”硬鏈接（即 SFN 以外的硬鏈接）都可以從邏輯搜索和索引中選擇性地省略。如今在 Windows 安裝上通常存在 10,000 到 100,000 個系統文件硬鏈接，例如 27 個鏈接到目錄中的“Ph3xIB64MV.dll”文件，例如 \Windows\System32\DriverStore\FileRepository\ph3xibc9.inf_amd64_neutral_ff3a566…

\Windows\System32\DriverStore\FileRepository\ph3xibc2.inf_amd64_neutral_7621f5…
 \Windows\System32\DriverStore\FileRepository\ph3xibc5.inf_amd64_neutral_22703…
 \Windows\winsxs\amd64_ph3xibc9.inf_31bf3856ad364e35_6.1.7600.16385_none_a…
 \Windows\winsxs\amd64_ph3xibc5.inf_31bf3856ad364e35_6.1.7600.16385_none_9…
 \Windows\winsxs\amd64_ph3xibc12.inf_31bf3856ad364e35_6.1.7600.16385_none_6… 等

通過只搜索文件的一個硬鏈接，您通常可以排除幾 GB 的重複數據，而且如果搜索所有其他文件也不會遺漏任何內容。那些被省略的附加硬鏈接是那些硬鏈接計數顯示為灰色的鏈接。唯一被搜索到的硬鏈接中的搜索命中在描述中標有提示“→鏈接”。列提醒您同一文件的其他硬鏈接，以防這些搜索結果相關。

- 除了文件內容之外，還有一個選項可以將邏輯同步搜索應用於文件的各種元數據。更準確地說，它們可以應用於任何選定的目錄瀏覽器列的單元格，例如名稱、作者、發件人、收件人或元數據。這可以避免您將關鍵字粘貼到各種目錄瀏覽器列的過濾器對話框中。該方法也更徹底，因為此功能處理的所有文本都可以在 UTF-16 中搜索，而在其他地方，相同的數據可能是碎片化的（例如文件名，特別是 FAT 中的文件名），經過特殊編碼（例如，在 e 中引用的可打印的發件人和收件人-mails），壓縮或存儲在意外的代碼頁中。這也很方便，因為任何命中都將以與文件內容中普通搜索命中相同的方式呈現和列出，只需在搜索命中描述欄中特別標記包含搜索命中的文本實際所屬的列的名稱並以不同的顏色突出顯示。您還可以過濾元數據中的搜索結果。

選擇元數據中的搜索命中時，它會在詳細信息模式下自動搜索並突出顯示，就像在預覽模式下自動搜索文件內容中的普通搜索命中並突出顯示一樣。

請注意，同時搜索元數據不會搜索其他單元格文本

以不同的顏色顯示，例如“名稱”列中的替代文件名和文件數。

- X-Ways Forensics 不存在其他計算機取證軟件產品中存在的邏輯搜索盲點。卷中的特殊區域甚至可以通過邏輯搜索來尋址，即從文件鬆弛到緊隨其後的可用空間的任何過渡，在 NTFS 和 exFAT 中也從已知未初始化（但物理分配）的文件尾部到緊隨其後的可用空間，加上 RAM 鬆弛 NTFS 壓縮單元。

如果此操作在某個文件上凍結，請記住內部 ID 和當前處理文件的名稱顯示在小進度指示器窗口中。如果此操作應用於證據對象並崩潰，X-Ways Forensics 將在您重新啟動程序時告訴您哪個文件並將其與報告表相關聯（取決於安全選項）。所有這些都是為了讓您在再次嘗試時可以排除和忽略該文件。

並行化選項（目前仍被認為是實驗性的）允許您通過使用多個線程更好地利用多個處理器內核。它僅在搜索圖像或目錄而不是磁盤的證據對象時有效。您的大容量存儲解決方案執行得越快（在尋道時間和數據傳輸速度方面），您節省的時間百分比就越多。在完美的條件下，這可以使邏輯搜索的速度提高一倍以上。如果您只選擇沒有額外的線程進行邏輯搜索，它將像在 18.9 之前的 X-Ways Forensics 版本中一樣工作。如果您選擇 1 個或多個額外線程，搜索將在額外的工作線程中完成，進程的主線程將空閒，這意味著 GUI 將保持高度響應。在 X-Ways Investigator 中最多可使用 3 個工作線程，在 X-Ways Forensics 中最多可使用 16 個，具體取決於檢測到的處理器內核數量。

5.12 搜索命中列表

僅適用於取證許可證，在處理案例時，用於具有捲快照的證據對象。（否則職位經理將列出搜索結果。）

目錄瀏覽器可以顯示搜索結果。要進入此顯示模式（搜索命中列表而不是普通目錄瀏覽器），請在模式按鈕所在的同一欄中單擊帶有雙箭頭遠鏡和四條水平線的按鈕。它僅適用於證據對象。在該操作模式下，還有四個附加列：搜索命中的物理/絕對偏移量、邏輯/相對偏移量、包括發現搜索命中的代碼頁的描述和在文件 slack 中找到的提示，以及搜索命中本身（通常帶有上下文預覽，可按搜索詞排序，上下文預覽對於阿拉伯語和希伯來語文本或 UTF 8 中的命中不準確）。當搜索命中按這三列之一排序時，目錄瀏覽器的分組選項無效。搜索命中描述列帶有一個過濾器，允許關注顯著的命中、案例報告中包含的命中、用戶搜索命中、特定代碼頁中的命中、文檔文本提取中的命中以及鬆弛空間中的命中或未初始化的文件尾部區域。在描述中標記了未在偶數偏移處對齊的所有 UTF-16 變體中的搜索命中。列為“未對齊”，作為一個小提示和解釋為什麼您只能在搜索命中列的對齊感知上下文預覽中閱讀文本，而不是在文本列中。

目錄瀏覽器上下文菜單中的幾乎所有命令也可用於搜索命中列表，特別是複制、查看、標記和評論文件的能力。基於常用目錄瀏覽器列的動態過濾器可以與搜索命中列表結合使用，例如，專注於某些類型和具有特定最後修改日期的文件中的命中。

搜索命中列表是根據你點擊的目錄樹中的位置和層級，這樣你就可以看到例如\Documents and Settings及其子目錄下文件的所有搜索命中，甚至是所有證據對象的搜索命中整個案例同時使用案例根窗口。還可以在案例數據窗口的搜索詞列表中方便地選擇一個或多個搜索詞來查看搜索結果。同樣，找出案例樹中任何級別的任何給定搜索詞有多少搜索命中也是一項簡單的任務，因為該數字基於當前搜索命中列表顯示在目錄瀏覽器的標題中。

搜索命中列表是“動態的”，因為它們是“動態”組成的，具體取決於所選搜索詞、探索路徑、當前過濾器設置，並基於搜索詞列表的設置（邏輯 AND 組合和“每項 1 次命中”“選項”）。

您可以通過“搜索命中”列過濾器過濾搜索命中，例如根據上下文或您是否已將它們標記為值得注意。所有過濾器選項都可以與邏輯 OR 或邏輯 AND 組合，您可以專注於滿足定義條件或不滿足定義條件的搜索命中。

可以使用目錄瀏覽器上下文菜單或按空格鍵將搜索結果標記為顯著（例如左側顯示黃色燈泡）。使用 Space 鍵，您也可以刪除該標記。您可以通過在調用“標記為值得注意”上下文菜單命令時按住 Shift 鍵來取消將多個選定的搜索結果標記為值得注意。另一個上下文菜單命令允許取消將當前數據窗口表示的證據對像中的所有搜索命中標記為顯著。這允許增量過濾。示例：您過濾上下文包含單詞“Hello”的搜索結果。然後將這些命中標記為顯著（Ctrl+A 加上上下文菜單命令）。然後過濾出值得注意且包含“嘿”一詞的搜索結果。然後取消標記所有搜索命中（即使是那些當前未列出的！），這對顯示的列表沒有立即影響，並再次將那些列出的標記為值得注意的。結果是所有在上下文中同時包含“Hello”和“Hey”的搜索結果現在都被標記為值得注意。

如果您不再需要某些搜索結果，您可以選擇並刪除它們。例如，因為可能存在重複項，或者因為您想使用略有不同的設置再次在相同文件中搜索相同的搜索詞。如果您不再需要某些搜索詞的任何搜索命中，您可以在搜索詞列表中選擇這些搜索詞並刪除它們及其所有搜索命中。

如果出現極度緩慢或不穩定等問題，可以在上下文菜單中打開和關閉直接在搜索命中列表中圍繞搜索命中的上下文預覽。

另一個上下文菜單命令允許重新定位搜索命中，相對偏移變化 (+/-)，並調整搜索命中的大小，使用絕對新大小或正或負相對大小調整（單擊箭頭按鈕切換）。您可以使用相同的設置同時調整多個搜索結果的大小。

5.13 搜索詞列表

在搜索命中查看模式下顯示在案例數據窗口中（在使用雙筒望遠鏡和四條水平線單擊按鈕後）。搜索詞列表包含案例中曾經搜索過的所有搜索詞，除非被用戶刪除。通過搜索詞列表的上下文菜單，搜索詞可以選擇按字母順序升序排序或按列出的搜索命中計數降序排序，以便更容易在冗長的列表中找到某個搜索詞。

在搜索詞列表中選擇搜索詞，然後單擊 Enter 按鈕，您可以在搜索命中列表中列出當前所選路徑中這些搜索詞的所有搜索命中，受過濾器限制。您可以通過在單擊時按住 Shift 或 Ctrl 鍵來選擇多個搜索詞。您可以按 Del 鍵永久刪除選定的搜索詞及其所有搜索匹配項。

要將搜索命中列表縮減為包含至少一個搜索命中的唯一文件列表，請選中“List 1 hit per item only”，然後單擊 Enter。如果您要手動查看所有此類文件，確保每個此類文件僅列出一次，這將非常有用。不必假設每個文件中“最有用”的搜索命中以某種方式進入列表，或者如果選擇了多個搜索詞，則列出的搜索命中是您認為更重要的搜索詞。減少是非破壞性的。恢復原始的、完整的搜索命中列表只需要您取消選中此特殊框並再次單擊 Enter 按鈕。

僅列出每個項目 1 個搜索命中的選項不會過濾掉鬆弛空間或文件未初始化部分（超過所謂的有效數據長度的部分）中的搜索命中。這很有用，因為文件的鬆弛部分通常與該文件的內容無關，因此這些特殊區域中的任何搜索命中可能與文件邏輯部分中的搜索命中具有完全不同的上下文（尤其是文件未初始化部分的搜索命中可能駐留在來自各種不同來源的數據中），因此需要對其進行額外審查。請注意，仍然需要取消選擇“每項 1 次命中”選項，以單獨檢查聯合體中的搜索命中，例如 pagefile.sys 和虛擬“可用空間”文件，它們包含來自完全不同來源的數據。“每項 1 次點擊”選項對文檔最有用，在預覽模式下快速瀏覽一下後，您通常可以判斷該特定文件是否相關。

可以查看（並通過上下文菜單副本中的導出列表命令）搜索詞列表中選定搜索詞的命中計數。這些命中數基於屏幕上搜索命中列表的當前設置，考慮了所有過濾器、探索的路徑、任何活動的 AND 組合等。實際列出的是命中數，而不是數字已記錄/保存的命中數。要查看總命中數，請停用任何過濾器並選擇所有搜索詞。請注意，“List 1 hit per item only”選項的功能也類似於搜索命中的過濾器。

您可以使用搜索詞列表的上下文菜單中的命令重命名搜索詞，例如，將冗長的正則表達式替換為更簡潔、更易於理解的友好名稱，例如“IP 地址”、“信用卡號”，“電子郵件地址”等。

程序可以記住這些名稱，以便將來搜索相同的表達式時，會立即在搜索詞列表中添加更容易識別的條目。

友好的名字。友好的名稱和相應的正則表達式存儲在文本文件“Regular Expressions.txt”中，您可以與同事共享該文件，並在需要時從中輕鬆複製和粘貼正則表達式。通過單擊帶有黃色燈泡的按鈕（燈泡表示要搜索的表達式的“想法”），可以從同步搜索對話框窗口中打開該文件。您可以使用任何文本編輯器直接編輯該文件。只需保持結構完整：始終是 1 個友好名稱，後跟 1 個正則表達式，每個這樣的對 2 行，採用 UTF-16 格式。

有兩種方法可以將多個搜索詞與布爾運算符進行邏輯組合：

1) 默認情況下，多個選定的搜索詞用邏輯或組合。要強制搜索詞，請選擇它並按“+”鍵。要排除搜索詞，請選擇它並按“-”鍵。要將搜索詞返回到正常的 OR 組合，請按 Esc 鍵。您也可以使用搜索詞列表的上下文菜單來完成所有這些。以下示例描述了根據“+”或“-”狀態選擇搜索詞 A 和 B 的效果。

一個

B

= 在任何文件中出現的 A 搜索命中和 B 搜索命中（正常 OR 組合）

+A

B

= A 的搜索命中和包含 A 的文件中出現的 B 的搜索命中

+A

+B

= 在同時包含 A 和 B 的文件中出現的 A 搜索命中和 B 搜索命中 (AND)

一個

-B

= 在不包含 B 的文件中出現的 A 搜索命中

2) 對於邏輯 AND 組合，如果搜索詞沒有標有“+”或“-”，也可以使用選擇多個搜索詞時出現的小滾動條。允許您僅查看同時包含所有選定搜索詞的文件中的搜索結果。您最多可以組合 7 個搜索詞。如果您選擇超過 2 個搜索詞，您還可以選擇不那麼嚴格，只在同一文件中指定最少數量的不同搜索詞，例如，要求搜索詞 A、B、C 和 D 是兩者的任意組合它們在同一個文件中就足夠了，例如 A 和 B，或 A 和 C，或 B 和 D，等等（模糊/靈活的 AND 組合）。

除了“最小 x”選項之外，搜索詞列表還提供了一個“最大 1”選項，當選擇了多個搜索詞時，這些搜索詞沒有被 + 強製或被 - 排除。“最多 1 個”僅當搜索結果包含在不包含任何其他選定搜索詞的文件中時才會列出搜索結果。例如，對於 3 個搜索詞，要獲得相同的結果，您必須列出搜索詞 A 的搜索命中同時排除 B 和 C，然後列出 B 的搜索命中同時排除 A 和 C，然後列出搜索命中 C 而排除 A 和 B，這當然不那麼優雅，並且不會同時向您顯示所有此類單一搜索結果。

當在搜索詞列表中選擇 2 個搜索詞並與邏輯 AND 組合（使用兩種可用方法中的任何一種）時，您現在還可以要求搜索命中必須彼此“接近”才能列出，以查找更多同一文件中兩個搜索詞的可能相關組合，與鄰近搜索完全一樣。構成“NEAR”的搜索命中之間的最大距離可以由用戶以字節為單位定義。NEAR 組合也可以應用於 2 個以上的選定搜索詞。結果是，只有在附近出現*任何*其他選定的搜索詞時，才會列出搜索命中。

這段引自 wikipedia.org：基本的語言假設是文檔中單詞的接近度意味著單詞之間的關係。鑑於文檔的作者試圖構建包含單個想法的句子，或者將相關想法聚集在相鄰的句子中或組織成段落，因此在文檔結構中存在一種內在的、相對較高的概率，即一起使用的詞是相關的。而當兩個詞位於一本書的兩端時，這些詞之間存在關係的概率相對較弱。通過將搜索結果限制為僅包括單詞在指定的最大接近度或距離內的匹配項，搜索結果被假定為比單詞分散的匹配項具有更高的相關性。

更重要的是，搜索詞列表除了“NEAR”之外還提供了“NOT NEAR”選項（縮寫為NTNR）。使用 2 個選定的搜索詞，NTNR 將確保僅列出不位於相應其他搜索詞的任何搜索命中附近的搜索命中。如果選擇了 2 個以上的搜索詞，則結果當前未定義。

5.14 搜索詞列表中的命中計數

問題：為什麼當所有搜索詞都選擇“List 1 hit per item only”時，返回的計數與我使用相同設置單獨單擊每個搜索詞時返回的計數不同？

答：因為選項是“僅列出每個項目的 1 個匹配項”，而不是“每個項目的每個搜索詞僅列出 1 個匹配項”。許多用戶不明白這一點。想像一下，如果在同一個文件中，搜索詞 A 有 1 次命中，搜索詞 B 有 1 次命中，並且您在啟用該選項的情況下同時選擇 A 和 B，則只會列出 1 次命中，要么是 A 的命中，要么是 B（由 X-Ways Forensics 決定）。因此，一個搜索詞顯示的命中數為 1，另一個搜索詞為 0。如果然後您僅選擇其他搜索詞並單擊“輸入”，則該搜索詞的計數將從 0 變為 1，因為這是現在可以列出命中的唯一可能的搜索詞，最多 1 個搜索命中是每個文件列出，以便列出 1 個命中。

5.15 事件列表

僅適用於取證許可證，在處理案例時，用於具有捲快照的證據對象。

提取元數據（卷快照優化的一部分）時，X-Ways Forensics 可以根據時間戳編譯事件列表，這些時間戳可以在文件系統級別以及內部

文件和主存。可以想像的來源是瀏覽器歷史記錄、Windows 事件日誌、Windows 註冊表配置單元、電子郵件等。事件列表的工作方式與搜索命中列表完全相同，可以通過單擊位於搜索命中列表按鈕旁邊的按鈕來顯示，上面有一個時鐘圖標。就像搜索命中列表一樣，事件列錶帶有附加列：事件時間戳、事件類型、事件類別，並且某些事件具有單獨的描述/附加文本，例如 Windows 註冊表和 Internet Explorer 索引中記錄的事件。數據文件。

如果事件列表按時間順序按時間戳排序，它就像時間線一樣工作，它可以讓您找出存儲在不同位置的不同類型的事件序列（例如收到的電子郵件、保存的附件、啟動的應用程序、打印的文檔、文件已刪除），否則無法在上下文中一起看到。您可以從案例根窗口同時查看來自不同證據對象的事件，遞歸或按路徑探索，按事件類型或事件類別排序，查看所有常用文件屬性，查看文件，導航到事件的定義一個文件（如果相對偏移量可用）並過濾某些日期範圍。

您可以將事件標記為值得注意的，就像搜索命中一樣，並通過時間戳列過濾值得注意的事件。

基於事件的分析而不是基於文件的分析是一種漸進的新方法，具有完全不同的視角，可以導致有關記錄在計算機上的活動的知識，否則很難獲得這些知識。您可能會看到在其他情況下可能會被忽略的聯繫（相關活動），並且可能能夠更好地解釋所發生事情背後的邏輯。

本版本元數據提取所利用的事件源包括所有支持的文件系統（即目錄瀏覽器時間戳列中列出的所有時間戳；如果與相應的創建相同，則省略修改、記錄更新和上次訪問）時間戳）、支持的內存轉儲中的進程、提取或處理的電子郵件，以及這些類型的文件：`index.dat` Internet 瀏覽器 SQLite 數據庫 `.firefox (~55)` 片段 `_CACHE_001_` 和 `_CACHE_002_.lnk` 快捷方式 `.automaticDestination-ms` `.chrome Chromium 緩存` `data_1`data_2.usnjrn` 片段 註冊表配置單元* Windows `.evt` 事件日誌 Windows `.evtx` 事件日誌（大多數提取的事件都帶有描述，包括事件源、事件 ID 和記錄號。記錄號使您可以快速如果您需要有關該特定事件的更多詳細信息，請在 HTML 預覽中搜索記錄。）

DataStore.edb (MS Windows 操作系統更新事件) .hbin 註冊表配置
單元片段 .doc (最後打印) .msg rp.log XP 還原點 INFO2 XP 回收
站 .recycler Vista 回收站

.snapprop Vista volume shadow copy
properties .cookie .gthr;.gthr2 Gatherer and
Gatherer fragments .pf prefetch attach timestamps
from EDB signing date from EXE/DLL/SYS/... 從 ETL
(事件跟蹤日誌)文件啟動時間 OLE2 最後修改最後保存
在 Office 文檔和 RTF Skype main.db 中 (聊天、通話、
文件傳輸、帳戶創建..... - 如果按時間順序排序，您可以閱
讀整個聊天記錄)

Skype Chat Sync

內部創建來自各種文件類型，包括來自照片的 Exif 時間戳 JPEG GPS Unix/Linux/Macintosh 系統日
誌（這些事件實際上很重要，尤其是對於 USB 設備歷史檢查。）

* 根據所使用的報告定義，當您創建註冊表報告時，可以選擇輸出比標準註冊表時間戳更多的特殊事件！

如果時間戳是以前有效的時間戳，例如在 NTFS 中的 0x30 屬性或 INDX 緩衝區鬆弛的索引記錄中找到的事件類型，
則事件類型顯示為灰色

\$日誌文件。

來自 NTFS 文件系統中 0x30 屬性的時間戳僅在實際不同於它們的 0x10 對應物並且與 0x30 創建時間戳不相同時
才作為事件輸出。它們在“事件類型”列中標記為“0x30”。惡意軟件可能會在部署後為自己提供看起來無害的時間
戳，因此它似乎與入侵/感染的時間無關。然而，0x30 屬性時間戳保持不變（除非文件被重命名或稍後移動），這就
是一些審查員對它們感興趣的原因。如果知道入侵/感染的時間範圍，由於原始的 0x30 屬性時間戳，相關文件將在事
件列表中找到。

如果 0x30 時間戳晚於相應的 0x10 時間戳，則它們在事件列表中用星號標記，這似乎不自然，並且在極少數情況下可
能是計算機本身的合法用戶回溯的結果。在某些情況下，追溯文件被視為欺詐和非法的。然而，更常見的是早於 0x30
時間戳的 0x10 時間戳只是安裝程序的工作或複製文件或將文件從一個卷移動到另一個卷或從 zip 存檔中提取文件
的結果，其中 Windows 或其他程序人為地應用了複製成功後源文件到目標的原始創建時間（內部編程回溯）。

從一個會話到下一個會話，程序不會記住事件類型過濾器中的選擇。

請參閱時間戳列的說明以獲取更多信息。

5.16 掛載為盤符

在 X-Ways Forensics 和 WinHex Lab Edition 中可用。 (對於具有 WinHex 任何許可證類型的不超過 1,000 個對象的證據文件容器 ,即使是評估版 ,也是免費的。)

允許將活動數據窗口表示的捲掛載為 Windows 驅動器盤符 ,可以完全掛載 (如果在專家菜單或整個卷的案例樹上下文菜單中調用該命令)或部分掛載 (如果應用於使用目錄瀏覽器上下文菜單或案例樹上下文菜單的子對象的目錄或文件) 。這允許在必要時使用外部程序方便快捷地訪問所有文件 (無需先將文件複製到您自己的本地驅動器盤符) 。如果您希望使用病毒掃描程序檢查整個卷或目錄或某些文件 ,則效率尤其高 。掛載適用於所有受支持的文件系統、所有受支持的分區方法和所有受支持的圖像類型 (在 X Ways Forensics 中 :原始圖像、.e01、.VDI、.VMDK、.VHD ,當然還有證據文件容器) ,甚至適用於圖像在圖像中 ,也適用於使用 Windows 未知的文件系統格式化的物理連接磁盤的分區 。對所有文件的訪問都是完全只讀的 ,在圖像或磁盤分區中安裝卷不會改變圖像/磁盤上的任何內容 。要卸載驅動器盤符 ,只需再次調用任何菜單中的安裝命令 ,然後單擊 “取消”按鈕 。

您可以選擇查看驅動器盤符中卷中的所有現有文件和可選的所有已知已刪除文件 ,這些文件與 X-Ways Forensics 本身非常徹底的捲快照中已知的文件完全相同 ,這取決於您是否已經對其進行了優化或不是 。可選擇過濾掉的文件可以從目錄列表中省略 。文件的子對象 (文件中的文件)也可以選擇公開 ,在與父文件同名的人工目錄中顯示為文件 ,僅附加一個字符以使名稱唯一 ,您可能從恢復/複製命令 。默認情況下 ,該後綴字符是不可見的 ,即沒有寬度的 Unicode 字符 ,以使子對象的路徑看起來盡可能原始 。您可能希望用其他內容替換該字符 ,例如下劃線 ,例如因為您正在使用不支持 Unicode 的外部程序 。為此 ,您需要先從編輯框中刪除不可見字符 ,例如按退格鍵 ,即使它沒有任何可見效果也能正常工作 。之後 ,您可以插入任何其他字符 。

以前存在的項目可以選擇列出 ,如果列出 ,它們將以 “隱藏”屬性顯示 ,這樣即使在 Windows 資源管理器 (也稱為文件資源管理器)中也可以在視覺上將它們與現有項目區分開來 。現有文件也可以選擇列出 (但現有目錄是強制性的 ,因為它們可能需要導航到某些以前存在的文件) 。

虛擬目錄以相同的方式呈現 。(當然 ,隱藏文件只有在您選擇查看它們時才會顯示在 Windows 中 ,請參閱工具 | 文件夾選項 | 查看 。)捲快照中的虛擬文件以及文件系統的內部文件 (例如 NTFS 和目錄中的 \$MFT 在 HFS+ 中)是可選的 ,被重命名/移動的文件的原始名稱和位置也是如此 。備用數據流、提取的電子郵件、視頻靜止圖像、嵌入的縮略圖、手冊文件摘錄等特殊對像在安裝的驅動器中作為普通文件顯示 。文件鬆弛不暴露 。同一目錄中具有相同名稱的文件 (例如 1 個現有文件、1 個以前存在的文件 ,最多 16 個)掛載時沒有問題 。這樣的文件可以

可以通過驅動器號從已安裝的捲中打開，就好像它們具有唯一的名稱一樣。

名為“遞歸應用”的選項可用於在平面列表中顯示當前活動證據對像或選定目錄的所有子目錄中的文件。如果您希望使用外部程序來查看許多文件並且不想為目錄導航而煩惱，這將很有用。使用此選項時，int 文件的 ID 被插入到文件名中，以使 X-Ways Forensics 能夠更好地識別文件。

此功能需要Windows 7及更高版本並安裝驅動程序（首次使用任何掛載命令時都會啟動）和Microsoft Visual C++ 2013 Redistributable Package（默認情況下不包含在Windows中，可能需要下載）。這意味著 X-Ways Forensics 的這個特定部分不可移植，但它無論如何也不是實時系統預覽的典型功能。

交互性：在Windows中刪除X-Ways Forensics掛載的捲中的文件當然不會刪除鏡像中或磁盤上的文件，但在 Windows 7下可以選擇性地觸發捲快照中的以下操作之一：1)在卷快照中排除文件 2) 將文件標記為已查看，或 3) 將文件與您選擇的報告表相關聯。

如果您掛載卷以便使用外部病毒掃描程序檢查文件中是否存在惡意軟件，則後者非常有用。如果病毒掃描程序刪除或隔離任何文件，X-Ways Forensics 將注意到並將該文件添加到指定的報告表中。請注意，如果您手動將文件從卷移到其他驅動器盤符，這將觸發相同的操作，因為這種移動與復制後刪除相同。不允許在同一卷內移動文件。

在 Windows 中重命名已安裝卷中的文件也會重命名卷快照中的文件。
(原始名稱被保留並另外顯示在目錄瀏覽器中。)

5.17 文件類型Categories.txt

這個可自定義的文件定義了包含哪些文件類型類別。類別的名稱前面有三個星號和一個空格（***）。以下是屬於該類別的文件類型列表，每行一個。這些行必須以“+”或“-”開頭，其中“+”僅表示在文件類型過濾器中檢查了該類型。之後是該文件類型的典型擴展名，外加一個空格字符，然後是文件類型的描述。擴展中只能使用小寫字母。相同的文件擴展名/類型可能出現在多個類別中（有關限制，請參閱類別別列說明）。

除了擴展名之外，還支持整個文件名。這對於某些具有明確定義的名稱的文件很有用，這些文件的擴展名不夠具體或沒有任何擴展名。完整的文件名必須用分號括起來。示例：-;index.dat; Internet Explorer 歷史記錄/緩存
-;history.dat; Mozilla/Firefox 瀏覽器歷史記錄 -;passwd;現有用戶

有一個虛擬的“其他/未知類型”類別，它沒有在文件中具體定義，只是涵蓋不屬於任何其他定義類別的所有文件。

文件類型按重要性/相關性排名，您可以按此排名過濾。例如，過濾掉排名 #0 的文件類型將排除字體文件、光標、圖標、主題、皮膚、剪貼畫等。排名較低的文件僅在非常具體的調查中才重要，例如源代碼，其中例如，您在查找辦公文檔或圖片時不會感興趣，但在尋找病毒程序員時肯定會感興趣。在更多情況下，排名較高的文件類型相關。一般來說，排名在簡單的情況下很有用，在這種情況下，您可以期望在眾所周知的文件類型中找到您要查找的內容。作為另一個想法，您可以養成只索引排名較高的文件的習慣。

您還可以選擇將文件類型分配給所謂的組，這是一個與文件類型類別不同的概念。例如，如果您的標準程序是讓考官 A 檢查圖片和視頻、考官 B 文檔、電子郵件和其他 Internet 活動，以及考官 C 的各種操作系統文件，因為它們的專業性。您可以為這些組賦予有意義的名稱並對其進行過濾，也可以使用“類型狀態”對話框窗口。這些組顯示在類型過濾器中。

所有關於文件類型等級和文件類型組的定義都在“文件類型類別.txt”文件中進行。已經預定義了排名建議和可能值得特別注意的一組文件的示例。等級（從 0 到 9，其中缺失表示 0）和組（從 A 到 Z 的字母）都可以在行尾的製表符之後以任何順序選擇性地指定，例如“2P”或“DI3”。所以最多 10 個等級是可以的，但是沒有必要完全利用這個範圍。最多可以有 26 個組。您不必按字母順序開始。

忽略字母的大小寫。您還可以在類別行中的選項卡之後為整個類別定義等級和組。沒有等級和組的文件類型都從它們所屬的類別繼承。

要給組一個比單個字母更具描述性的名稱，請在文本文件的末尾插入以等號開頭的組定義行，例如
 =P=圖像組的照片和視頻 =D=文檔、電子郵件
 和 Internet =I=要索引的文件類型

您可以將文件類型和類別的其他自定義定義存儲在名為“File Type Categories User.txt”的單獨文件中。除了“File Type Categories.txt”中的標準定義外，該文件將被讀取和維護，並且具有相同的結構如果包含在安裝目錄中，則不會被軟件更新覆蓋，因此即使用新版本覆蓋安裝，您也可以輕鬆繼續使用它。

5.18 哈希數據庫

只有法醫許可才能使用的功能。內部哈希數據庫一旦創建，就包含 257 個二進製文件，擴展名為 .xhd（X-Ways 哈希數據庫）。在“常規選項”對話框中選擇存儲文件夾。這樣的哈希數據庫以非常有效的方式組織

方式，在匹配哈希值時最大化性能。由用戶決定數據庫將基於什麼哈希類型（MD5、SHA-1、SHA-256，...），並由用戶用哈希集和哈希填充哈希數據庫值，通過自己在 X-Ways Forensics 中創建哈希集或從其他來源導入哈希集。如果選擇同一個存儲文件夾，同一個哈希數據庫可以被多個用戶/實例同時共享和使用。

但是，當其他用戶/實例正在使用它時，它無法更新。

可以同時維護兩個獨立的哈希數據庫，基於相同哈希類型或不同哈希類型的數據庫。例如，如果您從具有不同散列類型的不同源接收散列集（例如，一些具有 MD5 值，一些具有 SHA-1 值）並希望同時使用它們，則很有用。第二哈希數據庫可以存儲在不同的驅動器上。例如，如果用於一般用途的主哈希數據庫與網絡驅動器上的同事共享並且用戶希望創建或導入新的哈希集（僅供臨時使用或當主哈希數據庫被其他用戶鎖定時）到本地存儲的第二個數據庫。

哈希數據庫中的每個哈希值都屬於一個或多個哈希集。每個哈希集屬於“不相關” / “已知良好” / “無害”或“值得注意” / “已知不良” / “惡意” / “相關”類別，或者可以保持未分類（意思是“尚未決定”或“不確定”）。

在優化卷快照時，可以計算文件的哈希值並將其與哈希數據庫進行匹配。目錄瀏覽器的可選列“哈希集”和“類別”將顯示每個文件屬於哪個哈希集和類別（如果有）（這允許您按這些方面進行排序/過濾並輕鬆忽略不相關的文件或專注於文件你正在尋找）。

如果一個文件的哈希值包含在多個選定的哈希集中，程序將報告所有匹配的哈希集，並指出其中一個哈希集的類別。它還會檢查匹配的哈希集是否都屬於同一類別，如果不屬於，則會顯示警告。

一個可選的第二個單獨的塊哈希值（而不是普通文件哈希值）的哈希數據庫存儲在一個單獨的目錄中，允許您在其他媒體上逐塊搜索已知高度相關文件的不完整殘餘。

通過“工具”菜單，您可以調用對話窗口來管理活動的哈希數據庫，它允許您：啟動一個全新的空白哈希數據庫（並丟棄現有的當前數據庫）使用

“初始化”命令，您可以在其中選擇新的哈希類型）， · 查看包含在數據庫中的哈希集列表，
· 重命名哈希集， · 合併哈希集（注意重複的哈希值在生成的哈希集不會立即刪除，但下次添加哈希集時，請注意，如果您合併不同類別的哈希集，則不會收到警告），

- 切換哈希集的類別， · 驗證哈希數據庫的完整性， · 導入選定的哈希集文本文件*， · 導入特定文件夾及其所有子文件夾（同上）中的所有哈希集文本文件，可選
進入一個必須指定其名稱的內部哈希集，
· 導出選定的散列集（例如，如果您希望與其他審查員交換單個散列集，而不是整個數據庫），

- 並在普通文件哈希數據庫和塊哈希數據庫之間切換。

* 支持 NSRL RDS 2.x、HashKeeper 和 ILook 文本文件，以及 Project Vic（版本 1.0、1.1、1.2 或 2）使用的 JSON/ODATA 格式佈局中的哈希集，可在 Hubstream 收件箱中找到。另一種導入和唯一的導出格式是一個非常簡單和通用的散列集文本文件，其中第一行只是散列類型（例如“MD5”），接下來的所有行只是散列值作為 ASCII 十六進製或（對於 SHA-1）採用 Base32 表示法，每行一個換行符是 0x0D 0x0A。

從 NSRL RDS 導入哈希值時，如果您將哈希集歸類為不相關，則標記為特殊或惡意的哈希值將被忽略（不導入）。如果您將哈希集歸類為值得注意的，則只會導入標記為惡意的哈希值。如果將散列集設置為未分類狀態，則只會導入標記為特殊或具有未知標誌的散列值。如果你想導入所有的哈希值，你可以導入同一個 NSRL 哈希集文件三次，不同的分類，所有的哈希值最終都會在適當分類的內部哈希集中。

目錄瀏覽器上下文菜單中的“包含在哈希數據庫中”命令允許您在任何內部哈希數據庫中創建自己的哈希集。每當導入/創建哈希集時，將消除同一哈希集中的重複哈希值。導入 NSRL RDS 哈希數據庫時，X-Ways Forensics 檢查帶有標誌“s”（特殊）和“m”（惡意）的記錄，以便這些哈希值不會錯誤地包含在應分類的同一內部哈希集中無關緊要。哈希數據庫最多支持 65,535 個哈希集。

哈希數據庫中已經包含的重複哈希值可以選擇從新創建或新導入的哈希集中或從所有現有哈希集中刪除，以在需要時保持哈希數據庫更緊湊/冗餘更少。

有一種方法可以通過導入哈希集文件（簡單的 1 列格式，每行 1 個哈希值）有效地從現有哈希集中刪除單個哈希值，其中必須首先列出要刪除的哈希值，並且必須在前面加上帶有減號（“-”）。該文件必須與您要更新的數據庫中的現有哈希集同名（允許附加文件擴展名）。

如果在所有數據窗口關閉時（最後一個打開的數據窗口關閉時）加載哈希數據庫，則可以選擇卸載哈希數據庫，以節省主內存或專門允許其他並髮用戶或實例更改哈希數據庫。

5.19 照片DNA

出於許可原因，PhotoDNA 功能作為單獨的下載提供，並且由 X-Ways 本身僅提供給執法機構，執法機構可能使用它來防止兒童性虐待內容的傳播以及旨在停止其分發和擁有的調查。有關 PhotoDNA 的詳細信息，請參閱此[高級技術說明](#)和此[新聞信息](#)。

X-Ways Forensics 可以將 PhotoDNA 哈希算法應用於照片。由於哈希算法的穩健性和它在照片中的專業性，它通常允許自動識別已知照片，即使它們已經反復經歷有損壓縮（例如 JPEG），如果它們以不同的文件格式存儲，調整大小，部分模糊/像素化、顏色調整或對比度調整等。與傳統通用算法計算的散列值不同，PhotoDNA 散列可以抵抗各種此類圖像更改或僅發生輕微變化。可選地，已知照片即使被鏡像（水平翻轉）也可以被識別。為避免在無關緊要的小圖片上浪費時間，PhotoDNA 不適用於寬度或高度小於 50 像素的圖片。

如果存在 PhotoDNA 功能，則可以在 X-Ways Forensics 中創建和維護具有照片 PhotoDNA 哈希值的數據庫，並且可以將照片與 X-Ways Forensics 和 X-Ways Investigator 中的哈希數據庫進行匹配，以自動識別已知的罪犯內容。

執法機構可能希望根據以前案例中的圖片創建和共享他們自己的此類哈希值集合，或者從[Project Vic](#)（JSON/ODATA 格式佈局版本 1.0，來自 X-Ways v18.1）導入大量現有集合Forensics 也是 1.1 版，X-Ways Forensics 的 v18.2 也是 1.2 版。您還可以導入其他 X-Ways 用戶的 PhotoDNA 哈希數據庫（選擇“RHDB”文件！），您可以刪除不再需要的哈希類別，還可以合併或重命名數據庫中的類別。當導入別人的哈希數據庫時，他們的同名類別將與您的合併。如果 PhotoDNA 散列值存儲在文本文件中，則也可以導入它們，第一行中有“PhotoDNA”，然後每行 1 個十六進制 ASCII 或 Base64 散列值。

可以使用目錄瀏覽器上下文中的“包含在哈希數據庫”命令，將證據對象卷快照中圖片的哈希值添加到 PhotoDNA 哈希數據庫，方法與將傳統哈希集添加到傳統哈希數據庫的方式相同菜單。該數據庫是可以使用工具 | 管理的幾個數據庫之一。哈希數據庫命令。PhotoDNA 哈希數據庫存儲在哈希數據庫 #1 旁邊的目錄中。

在 X-Ways Forensics 中導入 PhotoDNA 散列集合或將所選文件的 PhotoDNA 散列值直接包含到數據庫中時，會檢查其他條目是否存在相互之間以及數據庫中現有條目的冗餘和分類衝突，以保留數據庫盡可能小、快和有用。這是推薦的，但可選的，如果您跳過此步驟並且如果數據集非常大，您可能會節省數小時的時間，代價是在體積快照優化期間將圖片與數據庫進行匹配將花費更多時間，並且對於同一張圖片的變體可能會返回不同的分類。您可以單獨定義導入嚴格性，以定義相似的散列值必須如何才能保證對現有值進行重新分類（以保持數據庫一致），並定義相似的散列值必須如何覆蓋（替換）現有值具有新值（以保持數據庫緊湊和減少冗餘）。後者的嚴格程度不得低於前者。散列值可以是數據庫中現有的舊值、當前導入操作在數據庫中添加的新散列值，也可以是尚未添加到數據庫中的掛起散列值。

1) 如果待處理的哈希 Y 與舊的或新的哈希 X 完全相同，則 Y 將被忽略並且不會添加到數據庫中。如果 Y 和 X 剛好相似，則添加 Y。如果 Y 和 X 幾乎

相同，X 直接替換（覆蓋）為 Y。

2)如果Y和X相同或相似且，但屬於不同的類別，且X是新的，則說明導入文件質量低。你會看到一個警告。如果導入的是一個ProjectVic哈希集合，並且這兩個類別是比較相似的類別“虐待兒童”和“剝削兒童”，則不採取任何特殊行動。如果所涉及的兩個類別不是那兩個：如果 X 或 Y 屬於“不相關”類別並且圖片基本上是單色圖片，則 X 將被分配到“不相關”類別。否則，分類衝突將通過將 X 分配給類別“未分類”來解決。

3)如果Y和X相同或相似，但屬於不同的類別，並且X是舊的，則X將被分配到與Y相同的類別，假設之前的分類錯誤或過時並且導入文件包含correct/new信息。這對於原始分類來自外國來源（例如 Project Vic）並且由於您所在國家/地區的不同立法或司法管轄區或僅僅因為分類錯誤或不同解釋而需要調整的條目是有益的。在一個國家/地區被視為兒童色情製品的內容在另一個國家/地區不一定屬於此類（例如：計算機生成的圖像、動畫）。重新分類要求您在您的收藏中擁有相同圖片的副本（不一定是完全相同的文件），或者知道哪些哈希值恰好屬於哪張圖片。

美國的標準 Project Vic 類別在用戶可編輯的文本文件 PVicCat.txt 中預定義。來自英國和加拿大的執法用戶可以從我們網絡服務器上的 PhotoDNA 下載部分下載他們的定義，並替換他們安裝中的默認 PVicCat.txt 文件。不同類別的其他國家/地區的用戶可以很高興地與他們分享

我們。

當使用“包含在哈希數據庫中”命令將 PhotoDNA 哈希值添加到內部 PhotoDNA 哈希數據庫時，您可以選擇將您對所選文件的評論作為描述存儲在該哈希數據庫中。下次在另一個案例中發現相同的圖片時，這些描述可以自動再次被採納為評論。在另一種情況下，它們可以替換現有評論，或者（如果相應的複選框被半選中）附加到現有評論。這對於法院要求提供每張兒童色情圖片的文字描述的警察調查員來說非常有用，至少可以免除他們多次輸入相同已知圖片的描述的工作。也可用於存儲信息，例如照片中人員的已知身份、以前的案例編號等，以供日後在其他地方找到相同照片時參考。只需通過“包含在哈希數據庫中”命令將相同文件的 PhotoDNA 哈希值再次添加到內部數據庫，即可使用您的評論更新哈希數據庫中的描述。當您導入同事的內部哈希數據庫（通過選擇他們的 RHDB 文件）時，請確保不僅在同一目錄中存在相應的 RHCN 文件（帶有類別名稱），而且還包含包含描述的新子目錄（如果有的話），如果您希望導入這些描述。

要刪除所有內部描述，您只需刪除 PhotoDNA 哈希數據庫目錄的 D* 子目錄即可。或者，如果您希望在沒有描述的情況下與其他用戶共享您的數據庫，只需不包含 D* 子目錄即可。您也可以隨時手動刪除或更新 D* 子目錄中文本文件中的任何個別描述。

如果您再次從其他來源導入相同圖片的散列值，您數據庫中已有的描述不會丟失，除非如果其他來源被覆蓋，它們將被覆蓋。

X-Ways Forensics 的 PhotoDNA 哈希數據庫，其中包含對相同圖片的描述。

在創建所選圖片的 PhotoDNA 哈希集時，您可以選擇不將哈希集添加到內部數據庫中，而是創建一個單獨的純文本文件，其中包含 PhotoDNA 哈希值。為此，請選中“另存為...”框。如果其他用戶希望將指定的哈希值添加到他們的數據庫或刪除它們（見上文），則可以將此類文件傳遞給其他用戶。

可以從不需要的哈希值中清除 PhotoDNA 哈希數據庫。要刪除的散列值以純文本文件的形式提供，每行有一個十六進制 ASCII 符號的散列值，第一行是“PhotoDNA”。指定的散列值與散列數據庫中包含的精確等效值匹配，也匹配小的變化（允許與匹配集相同的偏差）。如果您從外國來源導入的哈希集的內容部分不符合您的要求，則可能有必要清理 PhotoDNA 哈希數據庫。如果您不希望刪除整個哈希集，則當您獲得錯誤命中時，這會變得很明顯，或者如果您自己不小心在哈希數據庫中包含了錯誤的圖片。

有一個按鈕允許將選定的哈希集合導出到文本文件中以與其他用戶共享它們或檢查包含哪些哈希值/哪些哈希值被重複刪除等。

另一個功能（帶放大鏡的按鈕）將幫助您檢查數據庫中是否存在以十六進制 ASCII 或 Base64 表示法指定的特定哈希值。如果命中，您將看到包含哈希值的哈希集合的名稱。如果數據庫中匹配的條目有文本描述，那麼該描述也會顯示出來。最多返回 19 個匹配項。對於每個匹配項，您將看到匹配項的精確度（越高，越精確；與用戶指定的匹配嚴格度相同的基本尺度，即級別 1 表示非常粗略的匹配項）。您可以選擇通過強制執行更高的最低嚴格級別來將結果列表縮小到更精確的匹配項，如果匹配項多於可以列出的項，這將很有用。

有一個功能可以將選定的 PhotoDNA 類別標記為“首選”，並帶有黑色星號。這樣，如果卷快照中的圖片與不同類別的散列值匹配，它們將獲得優先權。即使與非首選類別的替代匹配更接近，此類首選類別也將被報告為匹配項。這很有用，例如，如果您的數據庫中有您認為準確和合適的類別，而您不太信任其他類別，例如因為已知它們包含錯誤（例如，同一圖片被分類為 CP，但在同一時間）和/或因為它們來自外國並且基於不同的法律和司法管轄區。

匹配是 Specialist | 中“圖片分析處理”操作的一部分。優化卷快照。如果同一張圖片在 PhotoDNA 哈希數據庫的不同類別中存在匹配項，您可以在目錄瀏覽器中看到：顯示最接近匹配項的類別名稱，後跟一個逗號和一個省略號。在發生這種情況的極少數情況下，手動查看圖片並就其與案例的相關性做出最終決定可能很重要。您還可以過濾在多個類別中找到的圖片。此類圖片可能與傳統哈希數據庫中同時屬於“不相關”類別和“值得注意”類別的副本一樣值得關注，並且通常是填充數據庫不一致的結果，例如用戶意外錯誤分類或正確分類在不同的司法管轄區等。如果您認為返回的圖片最佳匹配類別是錯誤的，您可以通過將該圖片的 PhotoDNA 哈希值添加到

PhotoDNA 數據庫，指定正確的類別。

5.20 OCR (圖片文字識別)

軟件包 Tesseract 的 OCR 功能可以在 X-Ways Forensics 和 X-Ways Investigator 中使用。該軟件包可以從我們的網絡服務器上下載。

更新的下載說明一如既往地從同一個地方提供。如果在首次運行 X-Ways Forensics 時在安裝目錄的\Tesseract 子目錄中找到 Tesseract，Tesseract 將自動激活。否則請轉到選項 | 查看器程序來指示路徑。

OCR 可作為邏輯搜索或索引的一部分應用於合適的文件，例如文檔掃描或 TIFF 格式的數字存儲傳真或僅包含圖形內容的 PDF 文檔。文件掩碼與文件名和類型列匹配（在文件類型驗證後非常可靠和標準化）。默認情況下，它甚至包括 *.jpg，但是，將 OCR 應用於案例中的每個 JPEG 文件是否有點過度或有必要由您決定，並且您可以通過各種方式完全控制搜索範圍。請注意，高分辨率照片會花費大量時間來檢查文本。JPEG 和 HEIC 格式的數碼照片將根據 Exif 元數據中的說明進行旋轉，以恢復正確的方向，從而有望對最初大致水平拍攝的文本進行 OCR。如果對於包含在兩個文件掩碼 (*.pdf) 中的類型的給定文件，普通文本解碼已經成功，則不會額外應用 OCR。“為上下文預覽和未來搜索存儲解碼文本”選項還將保留從 OCR 派生的文本存儲在卷快照中。

在 OCR 派生文本中邏輯搜索返回的所有命中都在描述中標識為這樣。列並以不同的顏色突出顯示。描述過濾器允許您僅列出此類 OCR 搜索匹配項或不列出 OCR 匹配項。舊版本的 X-Ways Forensics 在打開同一個案例時可以看到 OCR 搜索結果，但不知道它們是 OCR 搜索結果。

您最多可以同時選擇兩種語言進行文本識別，在選項 | 中單擊 ... 按鈕後。查看器程序。但是，如果您同時選擇中文/日語和西方語言，則需要權衡取捨。這會降低對亞洲字符的識別。您可能希望選擇*僅*中文/日語，以便更好地識別該語言。在這種情況下仍然可以識別英語（實際上是拉丁語）字母，即使沒有明確選擇英語，但質量會降低。僅當正確識別西方語言對您更重要時，才同時選擇中文/日語和西方語言。

除了 Raw 子模式之外，預覽模式現在還有一個單獨的子模式，稱為文本模式，其中從非圖片文件中提取純文本，就像使用解碼選項的邏輯搜索一樣。該子模式也有助於更好地理解如何從各種文檔類型中提取文本，尤其是從電子表格中提取文本。對於這些文檔類型，存在不同的提取選項，這些選項的輸出可能不同，尤其是格式方面。

如果 Text 子模式下的普通文本提取/解碼沒有返回任何結果，或者如果

預覽文件是圖片文件，如果 Tesseract 可用且處於活動狀態，則會應用 OCR。這使您可以更好地了解 OCR 在搜索您正在處理的文件類型時的效果。您還可以嘗試選擇不同的語言並比較結果的質量。默認情況下，子模式按鈕名為“文本”，但會將其標籤更改為“OCR”，讓您知道 OCR 正在或曾經用於檢索文本。對於多頁 TIFF 和 PDF 文件，OCR 可能非常耗時，但如有必要，用戶可以將其中斷。如果邏輯搜索或索引之前已將 OCR 應用於文件並且結果存儲在卷快照中，則基於 OCR 的預覽將立即可用，並且不會從頭開始重新應用 OCR。

在您離開預覽模式或選擇不同類型的文件之前，預覽模式中的原始和文本子模式都保持活動狀態。如果您希望使這些子模式中的任何一個更持久，以便即使在預覽不同類型的文件時它也保持活動狀態，您可以在單擊相應子模式按鈕的同時按住 Shift 鍵。

可從我們的網絡服務器下載的 Tesseract 軟件包已經集成了對以下語言的支持，按字母順序排列：ara :阿拉伯語
chi_sim :簡體中文（僅限橫寫） chi_tra :繁體中文（僅限橫寫） deu :德語 eng :英語 fra :法語 heb :希伯來語
ita :意大利語 jpn :日語（僅限橫寫） kor :韓語（僅限橫寫） nld :荷蘭語 pol :波蘭語 rus :俄語 spa :西班牙語
swe :瑞典語 tur :土耳其語 如果您需要，可以添加其他語言可以在 https://github.com/tesseract-ocr/tessdata_fast 找到它們的 .traineddata 文件。這些文件只需要放入 Tesseract 的 \tessdata 子目錄中。或者您可以訪問 https://github.com/tesseract-ocr/tessdata_best 為任何支持的語言下載更高質量的 OCR 引擎。（請注意，OCR 需要花費更多時間。）

支持的文件類型通常如下：PDF、PostScript (PS)、TIFF、JPEG、HEIC、PNG、GIF、BMP、WEBP、AutoCAD DXF、Photoshop PSP 等等。

5.21 時區概念

以下內容適用於使用專家或取證許可證操作時的 WinHex 和 X-Ways Forensics。

X-Ways Forensics 使用自己的而非 Windows 的邏輯將 UTC 時間戳轉換為自由選擇的時區，以便在目錄瀏覽器、報告表和導出列表中顯示。它顯示獨立於考官系統控制面板中所選時區的時間戳。X-Ways Forensics 中時間戳的顯示可能與 Windows 不同，因為在 Windows 中，如果在查看該時間戳時夏令時未激活，則不會根據夏令時顯示夏令時時間戳。

使用案例時，為該案例選擇的時區將全局應用於整個程序（可在案例屬性中選擇），否則將應用在常規選項對話框中選擇的時區。在處理案例時，可以選擇為每個證據對象指定不同的時區，以便您始終可以看到本地文件時間，即使是在不同時區使用的媒體（如果需要）。請注意，時間戳只是為了顯示而轉換的。這意味著，在涵蓋多個媒體的案例根中的遞歸視圖中，排序基於絕對 UTC 時間戳。或者，也可以顯示實際使用的轉換偏差（請參閱目錄瀏覽器選項）。

FAT 卷上的時間戳永遠不會轉換，因為它們在 UTC 中不可用，而是基於一個或多個未知的本地時區。顯式存儲時區的文件系統中的時間戳在內部轉換為 UTC，然後出於顯示目的從 UTC 轉換為本地時區。

如有必要，可以調整時區定義。請注意，在任何對話窗口中更改這些定義會影響整個程序中時區的定義。

標準的 Windows 轉換技術取決於在用戶系統的控制面板中選擇的時區，仍在使用……。在文件 | 中屬性，其中可以訪問/更改用戶自己系統上文件的時間戳，用於案例記錄功能，通常在沒有專家或取證許可的情況下操作，以及在沒有文件“timezone.dat”的情況下操作。

如果“常規選項”對話框中的“顯示時區”按鈕變灰或不可見，您可以判斷後兩者之一為真。

5.22 證據文件容器

僅適用於取證許可證。專家菜單允許創建一個新的文件容器，打開一個現有的文件容器，並關閉活動的文件容器。目錄瀏覽器上下文菜單允許用選定的文件填充它。

當您需要將與案件特別相關的選定文件（甚至來自不同的證據對象）的集合傳遞給該案件中涉及的其他人，例如不需要或不得看到不相關文件的專業調查人員，證據文件容器可能會派上用場。大多數文件系統級元數據（名稱、路徑、大小、屬性/文件模式、

時間戳、刪除狀態、備用數據流或虛擬文件或電子郵件消息或附件的分類，……），尤其是文件的內容完全保留在證據文件容器中。此外，當傳統的（物理的、按扇區的）圖像因為您只需要獲取選定的文件而不是整個媒體而變得過大時，建議使用容器。證據文件容器使用特殊文件系統（XWFS），可以容納來自 Windows、Linux 和 Apple 世界的傳統文件系統的大多數元數據。

證據文件容器可以像其他圖像文件一樣被解釋、添加到案例中並方便地檢查，特別是在 X-Ways Investigator [CTR] 中，X Ways Forensics 的簡化版本適用於不是計算機取證檢查員，但專門在其他領域，如腐敗、會計、兒童色情、建築法……容器的接收者可以將容器添加到他或她自己的案例中，查看其中包含的文件，就像在磁盤分區或常規圖像中一樣，可以運行關鍵字搜索、評論文件、將文件添加到報告表、創建報告等。報告表關聯甚至可以通過案例樹上下文菜單命令導出和導入回原始案例。這允許將大型案件中的工作量分配給同時工作的多個調查人員，並協調他們的結果。

X-Ways 以外的某些計算機取證工具可以理解當前格式的證據文件容器。舊版本的 WinHex（具有專家許可證或更高版本）、X Ways Forensics 和 X-Ways Investigator 也可以理解它們。他們都可以讀取所有文件的內容並顯示最重要的元數據（例如文件名、路徑、許多屬性、大多數時間戳、現有或已刪除）。但是，要查看最大數量的元數據，請使用 WinHex/XWF/XWI 16.3 及更高版本。[更多信息](#)。原始（非 .e01）證據文件容器可以被解釋為 WinHex 中具有任何許可證類型的驅動器號。如果其他工具本身不理解容器格式，則可以在其他工具中呈現這些文件。（如果這樣的容器包含不超過 1,000 個對象，那麼即使是 WinHex 的評估版也可以做到這一點。）

容器理論上可以容納大約 10 億個文件。X-Ways Forensics 自動防止同一文件被複製到容器中兩次。如果您想在填充證據文件容器時檢查其內容，那沒問題。開放填寫時，您可以嘗試將其作為證據對象添加到同一個案例中。您無需將其從案件中移除或關閉證據對像以進一步填充容器。在每個填充步驟之後，您可以拍攝容器的新卷快照以查看完整的最新內容。裝滿容器後，您可以將其從箱子中取出，因為裡面可能不再需要它了。

為了識別/保存源自不同證據對象的文件的來源，這些證據對象的名稱可以作為頂級目錄級別包含在容器中。如果插入人工頂級目錄級別的選項僅被選中一半，則意味著僅包括具有物理證據對像作為父項的分區證據對象的名稱。

如果父證據對象名稱非常長且包含冗餘，則很有用，因為您將僅使用來自該物理證據對象的文件填充整個容器，並且已經在容器名稱中引用該對象的名稱。

創建容器時，您可以在直接方法和間接方法之間進行選擇來填充它。
間接方式是通過自己的硬盤，即文件內容不直接複製到

容器，但首先到您的臨時文件文件夾（參見常規選項），然後才從那裡進入容器。這可能是有益的，因為它允許常駐防病毒軟件攔截這些文件（檢查它們是否有病毒、清除/解除它們、重命名它們、移動/刪除/鎖定它們等），從而防止病毒將其變成容器。生成的容器沒有已知病毒（取決於所使用的防病毒軟件），可以合理地傳遞到具有更高敏感性、更高安全要求和/或不太複雜的病毒防護的環境中並在其中使用。重要提示：請首先通過使用已知惡意軟件進行測試來驗證您的防病毒軟件在這種情況下是否按預期工作。

可以指定一個可選的內部名稱（最多 31 個字符），它將成為 XWFS 文件系統的捲標。還可以指定可選描述（最多 60,000 個字符），一旦將容器添加到 X-Ways Forensics 中的案例，該描述將作為證據對象註釋導入。存儲在容器中的描述仍然可以在以後添加或編輯。

可以使用目錄瀏覽器的上下文菜單將在目錄瀏覽器中選擇的文件添加到在後台打開的容器中。您可以分別複製文件的邏輯內容、邏輯內容和文件 slack，僅複製 slack，僅複製在文件模式中選擇的塊，或者僅複製文件的文件系統級元數據。您還可以指定所選文件的子對像是否也應複製到容器中，即使它們本身未被選中，任何類型的子對象的子對象（如果完全選中）或僅電子郵件附件（如果選中一半）。

可選地，容器可以包含目錄本身的數據/內容，即取決於文件系統、目錄條目、INDX 緩衝區等。如果容器的接收者精通技術並且可能對這些數據結構中的時間戳或其他元數據感興趣，則很有用。如果您選擇在創建容器時將目錄數據包含在容器中，則這只會對自己選擇的目錄產生直接影響。僅當您啟用附加選項（“包括直接父項的數據結構/內容”）時，它才會對所選項目的相應父目錄產生影響。這個額外的決定是必要的，因為否則目錄數據可能會無意中洩露容器中有意省略的文件的名稱和其他元數據，例如出於保密原因。

您可以在容器中包含帶有或不帶有原始路徑的對象。如果僅選擇了此選項，則意味著僅包含部分路徑，從您正在復制的目錄/您探索過的目錄向下，這種行為直觀上可以理解，因為 Windows 文件資源管理器就是這樣複製選定文件和目錄的。如果在容器中您有 X-Ways Forensics 重新創建作為其他文件的子對象的文件的原始路徑，那麼這些父文件將至少像名義上一樣包含在容器中，沒有數據，以便子對象顯示正確的路徑，只需查看容器即可清楚它的來源。此類父文件的示例是所選附件所屬的電子郵件消息、包含所選文件的 zip 存檔以及嵌入所選圖片的文檔。選項“包括直接父級的數據結構/內容”項，此類文件的數據也包含在容器中，即使這些文件未被選擇用於復制自身。可以選擇在容器中創建人工目錄以容納文件的子對象，以便與不接受文件作為其他文件的子對象的工具兼容。WinHex/XWF/XWI 不需要這樣的人工目錄。

任何作為卷快照一部分的文件（例如，即使提取的單個電子郵件消息）也可以添加到容器中。添加後，無法再物理刪除文件，但是，可以將其排除在容器中。您可以選擇為已添加到證據文件容器的文件自動創建報告表關聯。

可選地，可以為複製到容器中的文件存儲散列值。這允許稍後在將容器添加到案例後通過優化卷快照來驗證文件的完整性。直接為從原始源介質讀取的數據（除非您僅將元數據複製到容器）或從卷快照（如果可用）中獲取的數據計算哈希值。

可選地，證據文件容器的準備者可以傳遞報告表關聯（所有或不是由 X-Ways Forensics 內部創建的關聯）或關於包含在容器中的文件的評論。不僅可以將一系列文件轉發給其他調查人員，還可以轉發案件的具體信息和初步調查結果。例如，評論可以解釋為什麼首先選擇一個文件包含在容器中的原因。在證據文件容器中傳遞內部文件元數據是一個三態復選框。如果選中一半，將僅傳遞提取的電子郵件發件人和收件人，而不傳遞元數據列中已知的一般元數據。請注意，如果收件人想要使用事件列表，則不建議將提取的元數據傳輸到容器，因為事件不會傳輸到容器，如果文件是，從文件內容中派生的事件將不會添加到事件列表標記為已處理元數據。

讀取錯誤時中止操作：此選項允許在讀取錯誤時中止將文件複製到證據文件容器中，並且不部分包含受影響的文件。從網絡位置獲取文件並且連接可能會中斷時很有用，如果您假設如果發生這種情況您將恢復連接並且在您重試時會更成功，以避免容器中有不完整的文件，這是不可能的追溯替換為完整副本。僅在不間接填充容器時可用。

當關閉在後台打開的容器時，系統會向用戶提供壓縮、加密和/或拆分它的功能。如果容器完整且相對較大，則拆分很有用，例如應該通過 CD 或 DVD 發送給其他人。您可能還會發現為容器中的所有數據提供一個可驗證的整體哈希值很有用，該哈希值可以在那個時候計算並嵌入到目標容器中。您還可以凍結以 .e01 證據文件格式創建的目標容器中的文件系統，這樣即使稍後再次轉換回其普通狀態（原始圖像）也無法進一步填充它。

5.23 相關項目

僅適用於取證許可證。

在卷快照中具有相應“相關”文件或目錄的文件/目錄在目錄瀏覽器中用圖標左側向下的藍色小箭頭標記。將鼠標光標懸停在圖標上時，帶有“相關”文件的文件會出現輔助工具提示，它可以方便地告訴您該相關文件的路徑和名稱，

例如符號鏈接的目標。有四種不同類型的相關對象：

- 1) 對基於 Unix 的文件系統進行卷快照時，符號鏈接作為所謂的相關文件連接到它們在卷快照中的目標，以便您可以通過按 Shift+Backspace 方便地導航到目標。此外，指向特定目標的潛在多個符號鏈接之一將成為目標的相關文件，以便您可以方便地導航到符號鏈接或快速查看存在一個或多個指向特定目標的符號鏈接，因為任何文件具有卷快照中的“相關”文件在其圖標旁邊標有一個藍色小箭頭。同樣的箭頭也會告訴你符號鏈接的目標是否真的可以在文件系統中找到。如果符號鏈接鏈接到其他符號鏈接，則這些符號鏈接不會遞歸鏈接。如果由於卷中有許多符號鏈接而解析符號鏈接需要很長時間，您可以隨時安全地中止該步驟。
- 2) 使用 Windows 安裝拍攝卷快照時，某些重新分析點（也稱為連接點）連接到卷快照中的目標，就像基於 Unix 的文件系統中的符號鏈接一樣，因此您可以方便地導航到目標按 Shift+Backspace。此外，還會有一個對一個重分析點的反向引用，以便您可以方便地導航到該重分析點或快速查看是否存在一個或多個重分析點並鏈接到某個目錄，因為任何目錄都具有“相關”目錄在卷快照中，其圖標旁邊標有一個藍色小箭頭。僅限法醫執照。未與其目標目錄連接的重分析點仍會顯示一條註釋，建議您使用 X-Ways Forensics 的早期版本中的目標路徑。
- 3) HFS+中的硬鏈接指向對應的iNode*（間接節點）文件。iNode*文件指向其對應的硬鏈接之一，因此可以非常方便地找到至少一個硬鏈接並查看文件的實際用途和位置。要查找同一 iNode* 文件的其他硬鏈接，您可以按“第一扇區”列排序。
- 4) 在 NTFS 的捲影副本中找到的文件指向它們的捲影副本主機文件。VSC 主機文件指向其對應的快照屬性文件。

5.24 生成器簽名

生成器簽名是一個概念，用於識別 JPEG、視頻和 PDF 等常見文件類型的子類型。這些子類型可以與設備（掃描儀、相機）或應用程序（例如 Photoshop）相關聯。對於 JPEG，簽名基於量化表和所有 JPEG 文件共享的一些其他不變特徵。生成器簽名以 32 位原始十六進制數的形式隨元數據一起提供，並附有從文件“Generator Signatures.txt”派生的文本描述。

607AE169 (IJG 庫 94 / 油漆)

此示例顯示了由 Microsoft Paint 生成的 JPEG 文件產生的簽名。該數字是 1...100 範圍內的圖像質量。94 是特定於 Microsoft Paint 的固定圖像質量設置。

JPEG 簽名可以細分為三組。第一組名為標準（與 IJG 庫相同）。該組中的文件使用 JPEG 標準定義的量化表。正好有99個質量等級。第二組名為擴展。

這裡通過插入標準量化表將特定等級細分為大約 100 個附加等級。這些簽名通常屬於根據大小優先壓縮方法運行的入門級相機型號。

D3D8AD02 (擴展 95.10 / 10 MP 攝像頭)

圖像質量在元數據列中以兩個小數顯示，在詳細信息窗格中以 DQT 標記顯示。可以通過Exif 字段 CompressedBitsPerPixel 來判斷相機是否使用尺寸優先方案。

第三組稱為自定義。該組中的文件使用特定於某些設備或應用程序的專有量化表。此處圖像質量也顯示在 0…100 範圍內，帶有兩個小數位。例外情況是具有 0…12 範圍內 13 個等級的 Photoshop、具有 1…1024 範圍內等級的 Apple Quicktime 以及具有 2…255 範圍內等級的 LEAD Technologies。

53631B67 (領先技術 2 / 掃描)

描述的第二部分，掃描，也可以有值 Facebook、WhatsApp 或 MsPhoto。MsPhoto 表示此文件已被 Microsoft Photo Gallery 編輯過。

生成器簽名構成了通用相關性計算的基礎。此外，如果沒有“更好”的元數據可用（例如來自 Exif 數據的相機型號和時間戳），在文件頭簽名搜索期間 X-Ways Forensics 會使用生成器簽名來命名雕刻的 JPEG 文件。如果元數據提取無法找到任何“更好”的元數據，生成器簽名仍然可以輸出，並且該簽名至少可以讓您識別可能具有相同來源的文件組。驗證生成器簽名和可用的 Exif 元數據是否相互一致可能會告訴您圖片是否被再次編輯和保存。

特別是生成器簽名允許識別由掃描儀生成的文件，因為只有少數幾種生成器常用於掃描儀。這允許可靠地識別掃描的圖像，即使它們不是黑白的或不是 100% 僅使用灰度顏色。掃描儀生成的 PDF 文件也可以通過生成器簽名來識別。這些文件與報告表“掃描”相關聯。

即使沒有元數據或無法提取元數據，PDF 生成器簽名也可用。擁有 4,700 個簽名（自 v19.0 起），覆蓋了所有 PDF 文件的 99% 以上。“Generator Signatures.txt”文件中一個特別值得注意的 PDF 生成器簽名類別是“Reporting Records”，它標識銀行賬戶報表和發票等文件。

這種識別也提高了自動相關性判斷。

文件“Generator Signatures.txt”類似於 X-Ways Forensics 附帶的其他文本文件，並且可以對其進行編輯以調整作為元數據提取一部分的相關性估計。例如，如果知道 JPEG 文件是由掃描儀生成的對於

你（因為你是稅務欺詐或其他對掃描文件感興趣的白領犯罪調查員），你會確保“JPEG/Scan”組具有高權重（例如 9）。這是帶有 *** 組定義的行中選項卡後面的數字。如果這樣的文件對您來說不太重要（例如，因為您要查找的圖片是 CP 照片），那麼您可以降低該組的權重（例如將其設置為 1）簽名的權重必須編輯組中每個生成器的單獨相對性。對於組的權重沒有這樣的範圍限制。

已知掃描設備的型號名稱可以在“Generator Signatures.txt”的“KnownScanner”部分手動擴展。如果掃描圖像包含 Exif 數據或經過編輯，則通過型號名稱進行識別有助於識別掃描圖像。通常，作為掃描圖像的檢測基於 1) 生成器簽名，2) Exif 元數據的通用屬性（文件源、密度等）和 3) KnownScanner 清單。

生成器簽名定義中的前綴“Reporting::”允許更輕鬆地過濾類別報告/記錄。

單獨文件“Video Signatures.txt”的結構與“Generator Signatures.txt”的結構相同，但它只處理 QuickTime 格式系列視頻文件的簽名。它目前由兩個子類別組成：原始類別和通用類別。如果您確定視頻未被編輯，您可以在原始部分插入新發現的簽名（如詳細信息模式所示），否則在通用部分。

5.25 外部分析接口

通過 CaseData 窗口中的菜單命令“導出文件進行分析”，您可以將文件（例如案例中屬於特定類別的所有文件）發送到外部程序以進行進一步分析。這個外部程序必須符合下面描述的接口。需要具有取證許可證的 X-Ways Forensics 或 X-Ways Investigator 或 WinHex。

可以使用案例數據窗口中的報告表導入菜單命令將分析結果導回 X-Ways Forensics。（例如，右鍵單擊粗體打印的案例標題。）這會將外部軟件分類的文件與某些報告表相關聯（並可能創建新的報告表），從而允許您過濾此類文件或創建關於他們的報導。

例如，軟件 DoublePics 可以識別已知圖片（即使以不同格式存儲或更改過）並返回“CP”、“相關”或“不相關”等分類。

接口技術說明

某個類別中的所有文件或文件或所有標記文件或所有未排除的文件都將複製到您指定的輸出文件夾中。子文件夾以十六進制字符的 CRC 命名，對於活動案例是唯一的。這些文件以唯一 ID（64 位整數）命名。創建一個名為“Checksum”的附加文件，其中包含 4 個具有相同 CRC 的字節，4 個字節具有 X-Ways Forensics（或 X

Ways Investigator ,就此而言) ,8 個保留字節和 128 個字節 ,帶有 UTF-16 格式的案例標題。
複製文件後 ,X-Ways Forensics 執行外部分析程序 ,並在引號中指定子文件夾的完整路徑作為參數。

外部程序現在可以執行分析 。它可以通過為每個分類創建一個 .rtd 文件來對文件進行分類 。

完成後 ,程序可以選擇檢查 X-Ways Forensics 主窗口是否仍然存在 ,如果存在 ,則通過向文本開始的主窗口發送 WM_SETTEXT 消息讓 X-Ways Forensics 知道結果的可用性帶有 “導入 :” ,後跟查找 .rtd 文件的目錄路徑 ,不帶引號 。這將自動觸發導入 。或者 ,用戶可以如上所述導入結果 。

.rtd 文件 (報告表定義文件)的名稱將用作報告表名稱 。.rtd 文件以 4 字節簽名 (0x52、0x54、0xDE、0xF0) 、4 字節校驗和 (見上文)開頭 ,後跟指示應關聯文件的 64 位文件 ID (整數)與那個報告表 。

6 卷快照及其改進

6.1 簡介

卷快照是給定時間點卷或物理介質 (文件、目錄等)內容的數據庫 。目錄樹和目錄瀏覽器顯示了該數據庫的視圖 。基於底層文件系統的數據結構 ,它由每個文件或目錄的一條記錄組成 ,並記住幾乎所有元數據 (名稱、路徑、大小、時間戳、屬性...) ,但不包括文件內容或目錄數據 。

卷快照通常引用現有的和以前存在的 (例如已刪除的)文件 ,如果它們對計算機取證檢查有用 (例如 ,甚至可以覆蓋磁盤或卷的未使用部分) ,也可以引用虛擬 (人工定義的)文件 。目錄瀏覽器上下文菜單中的邏輯搜索、索引和所有命令等操作將應用於卷快照中引用的文件和目錄 。由於壓縮文件以及刪除的文件和虛擬 “可用空間”文件可能多次與卷的同一簇關聯 ,卷快照中所有文件和目錄的總和很容易超過卷的總物理大小 。

卷快照作為臨時文件文件夾中名為 Volume*.dir 的一組文件存儲在磁盤上 ,或者 (如果與案例關聯)作為名為 “Main 1” 、“Main 2” 、“Main 3”的文件存儲 , “Names” , … , 在證據對象的元數據目錄中 。

6.2 體量/行業層面的細化

Specialist 菜單允許以各種方式擴展/優化標準卷快照，以便它們包含比常規文件系統引用更多的內容。需要專家或法醫執照。只有法醫許可證才能提供全部功能。

6.2.1 運行 X-Tension

X-Tensions 是 DLL，您可以自己編程，以擴展 X-Ways Forensics 的功能或自動將其用於您自己的目的。[更多信息](#)。

6.2.2 特別徹底的文件系統數據結構搜索

運行特別徹底的文件系統數據結構搜索可能是一項冗長的操作，具體取決於卷的大小，因此在拍攝卷快照時不會自動完成。

FAT12/FAT16/FAT32 :搜索孤立的子目錄（不再被任何其他目錄引用的子目錄）。

Ext3/Ext4 :類似於 FAT 的過程。檢查整個卷中以前存在的目錄結構，其內容不再從相應的 inode 中獲知（這些已經被視為常規卷快照的一部分）。這些目錄以通用名稱列出，通常在“未知路徑”中，但可能在根目錄中，如果它們以前存在於根目錄中（根目錄在這種情況下是特殊的，因為它具有不可更改的 ID）。可選地，某些以前存在的文件，否則將僅與文件系統元數據一起呈現，沒有內容可以使用 Ext3/Ext4 日誌與數據關聯。

ReiserFS、Reiser4 :搜索已刪除的文件（這些文件根本不包含在標準卷快照中）。

UDF :雖然會自動列出多區段 UDF CD/DVD 的第一個和最後一個區段，但只能使用此選項找到中間的其他區段。

CDFS :通常會自動檢測多區段 CD/DVD 上的所有區段。在它們不是的情況下（例如，當 CDFS 與 UDF 共存時，或者如果會話之間的間隔異常大），這將檢測第一個會話之後的會話。

RAM（主內存）：可能會發現已終止的進程和 Rootkit。

NTFS :可以使用取證許可證選擇性地解析卷影副本。檢查現有和以前存在的捲影副本主機文件以獲取有價值的信息，否則這些信息將不可用，例如在當前 \$MFT any 中找不到的文件。

內容已更改的更多或以前版本的文件。根據卷影副本，這些文件將被重建到 1 GB 的長度。卷影副本的處理（如果有）發生在所有其他操作之前，這些操作是特別徹底的文件系統數據結構搜索的一部分（解析 \$LogFile，可選地在 \$MFT 和 VSC 之外搜索 FILE 記錄，搜索索引記錄在 INDX 緩衝區的鬆弛）。如果有捲影副本，小進度指示器窗口的標題會告訴您它們何時被解析。在處理之前排除的捲影副本主機文件將被忽略。

在卷影副本中找到的文件在 Attr 中特別標有“SC #”列，或“SC #, prev. version”，如果它們是在徹底的文件系統數據結構搜索之前卷快照已知的文件的先前版本，那麼很容易將它們過濾進或過濾掉。# 代表在其中找到這些文件的快照的序號。請記住，您可以按 ID 排序以查看它們旁邊的先前版本的文件。

您還可以使用命令 Navigation | 輕鬆導航到 VSC 主機。例如，在目錄瀏覽器上下文菜單中查找相關文件，以便在詳細信息模式下了解有關該特定快照的更多信息。然後您可以再次調用相同的命令以導航到相應的快照屬性文件，在詳細信息模式下您可以了解更多信息，例如描述和正式創建日期。

如果卷影副本中的文件是完全重複的（相同的文件內容），則可以選擇避免將其以前版本的文件添加到卷快照中，這樣可以更容易地關注實際上以前的數據仍然可用的文件。即使修改日期不同，操作系統安裝的文件的文件內容通常也是相同的。如果完全選擇，X Ways Forensics 將比較最大 128 MB 的文件，如果選擇一半，則最多只比較 16 MB，以免在此功能上浪費太多時間。

NTFS：可以選擇在任何地方搜索 FILE 記錄，在既不屬於當前 MFT 也不屬於由上述選項處理的捲影副本 (VSC) 的扇區中。

這樣的 FILE 記錄可以在例如分區被重新創建、重新格式化、移動、調整大小或碎片整理後的空閒空間中找到。在非常大的分區上耗時。跳過屬於某些虛擬機磁盤映像類型的集群，以避免在主機捲的捲快照中包含虛擬機文件系統中的文件。

NTFS：使用取證許可證，可以利用當前的 \$LogFile 以及在已處理的捲影副本中找到的舊版本 \$LogFile。由於 \$LogFile，刪除文件的內容通常可以重建。\$LogFile 中的索引記錄殘餘以及 INDX 緩衝區的剩餘部分可以被利用，這些記錄可以顯示卷快照之前已知的重命名/移動文件/目錄的先前名稱或路徑，或者卷快照不知道的已刪除文件之前的（雖然沒有文件內容）。您可以指出您是否對重命名/移動的文件和目錄的早期名稱和路徑感興趣。如果早期名稱/路徑的複選框被選中一半，您可能會在元數據列中找到更早名稱/重命名/移動文件的路徑，並且不會在每個早期名稱/路徑的捲快照中獲得其他文件。您還可以表明您是否感興趣，包括卷快照中的文件跟蹤，這些文件的集群未知並且只有名稱、大小、時間戳和屬性可用。

在 NTFS 的所有子操作期間，盡可能避免在卷快照中包含冗餘（相同）文件。如果僅從舊版本的

FILE 記錄或索引記錄是先前有效的時間戳，沒有文件的較早名稱/路徑/內容，或者如果您已表明您對較早的名稱/路徑不感興趣，則這些時間戳僅作為事件輸出，具體取決於卷快照細化選項“提供來自各種來源的副漁獲物時間戳作為事件”。

NTFS：您可以表明您是否有興趣將文件包含在卷快照中，這些文件的集群（以及數據）完全未知，只有元數據（例如文件名、路徑、大小、屬性和時間戳），如可以在INDEX 緩衝區或 \$LogFile 中的索引記錄。如果選中，所有僅知道其元數據的先前存在的文件將包含在卷快照中。如果未選中，這些文件將被忽略。

其他文件系統：未採取任何措施

6.2.3 文件頭簽名查找

“文件頭簽名搜索”操作有助於將文件包含在卷快照中，這些文件仍然可以根據文件頭簽名在可用或已用驅動器空間中找到，並且不再被文件系統數據結構引用。系統會要求您選擇某些文件類型進行檢測、指定默認文件大小、可選文件名前綴等。請參閱“按類型恢復文件”和文件類型定義以了解詳細信息。只有當卷快照中沒有其他具有相同起始扇區號的文件時（被覆蓋的文件不算），使用此方法找到的文件才會包含在卷快照中，以避免重複。但是，出於性能原因，將始終包含未在扇區邊界對齊的文件。使用此方法找到的文件列出了“按類型恢復文件”機制檢測到的通用文件名和大小。如果應用於物理的、分區的證據對象，將只在未分區的空間和分區間隙中搜索文件頭，因為分區被視為單獨的、額外的證據對象。

文件頭簽名查找的結果通常輸出到雕刻文件專用的虛擬目錄中，該目錄為“未知路徑”的子目錄。但是，如果在這些其他文件中找到雕刻文件，則可以選擇將生成的文件顯示為現有文件的子對象。

6.2.4 塊級哈希和匹配

具有取證許可證。逐塊散列可以識別已知重要文件的完整或不完整殘餘，這些文件仍然漂浮在可用驅動器空間中，即使它們是碎片化的並且碎片的位置未知，以一定或非常確定地顯示這些文件曾經存在於該媒體上。哈希值是在從證據對象按扇區讀取時計算的，並且在運行文件頭簽名搜索（如果選擇）時同時發生，以避免不必要的重複 I/O，具有相同的扇區範圍。匹配作為一種特殊的搜索命中返回。連續塊的多個匹配比孤立的單個匹配更有意義，因為它們更不可能是某種巧合的結果，並且它們通常組合在一次命中中。列出搜索結果時會顯示所有此類結果的大小。尺寸越大，證據價值越高。

匹配。請注意，X-Ways Forensics 不會自行驗證連續匹配塊的順序是否與原始文件中的順序相同，但可以手動驗證，並且對於與壓縮數據一樣獨特的數據，最有可能是案子。

最適合選定的大於幾個扇區的顯著文件，這些文件被理想地壓縮或至少不僅稀疏地填充了非零數據，而且不包含經常出現的字節值的其他瑣碎組合。zip 樣式的 Office 文檔、圖片和視頻文件就是很好的例子。文件中主要由 1 個字節值組成的非常瑣碎的塊將被忽略並且不會被散列（創建散列集時已經相同）。為了更快地匹配，最好使用小型哈希數據庫，並且不要選擇強於 MD5 的哈希類型。塊哈希匹配的長度顯示在“大小”列中。這很有用，因此您可以按長度對它們進行排序並首先查看更重要（更大的）匹配項。

塊哈希的哈希集可以用與普通哈希集相同的方式創建或導入，即使用目錄瀏覽器上下文菜單選擇文件，但它們由單獨的哈希數據庫處理塊哈希（與文件哈希相反）。該單獨的數據庫在內部存儲在主哈希數據庫目錄的子目錄中。您可以一次創建由 1 個文件的塊哈希組成的哈希集，或多個選定文件的組合哈希集。塊大小當前始終為 512 字節，並且可能在未來版本中由用戶定義。

6.3 文件級別的細化

以下操作在上述操作之後應用於卷快照中已包含的文件，並且它們全部一起應用並按文件方式應用（即首先對一個文件進行所有操作，然後對下一個文件進行所有操作，依此類推），按照內部 ID 升序處理文件。其中一些操作可能會產生額外的文件，這些文件將獲得下一個更高的可用內部 ID。已知其第一個簇已被覆蓋或其第一個簇未知的先前存在的文件不會被處理，除非您通過標記或選擇專門針對它們。

基於哈希匹配被認為不相關的文件可以從所有進一步的操作中自動省略，以節省時間並避免可能以其他方式從中提取更多不相關的文件。還可以從進一步處理中不僅省略已知的不相關文件，而且省略已知的相關文件。例如，如果在大情況下您擁有或期望確實有很多這樣的文件並且證明它們的存在對您來說就足夠了並且您不需要提取它們的內部元數據，不需要計算它們的膚色百分比或 PhotoDNA 哈希值，這很有用，並且不需要檢查它們的嵌入數據等。還有一個選項可以忽略被過濾掉的文件。所有這些選項都特別強大，因為它們甚至可以在細化開始時提前定位尚未成為卷快照一部分的文件。例如，當通過文件頭簽名搜索將其他文件添加到快照時，如果類型過濾器在卷快照細化的後期處於活動狀態，則根據文件類型可以進一步處理（例如散列）或不處理這些文件。

有一個選項可以從卷快照優化中省略 NTFS/HFS+ 中同一文件的額外硬鏈接，就像從邏輯搜索中一樣，以節省時間並減少冗餘相同子對象的數量等。這可以在分區上產生很大的不同視窗。

具有大量硬鏈接和 HFS+ 分區的 Mac OS X Time Machine 安裝。

哪些硬鏈接在內部被認為是“附加”硬鏈接可以在“鏈接計數”欄中看到（灰色數字表示被省略），也可以在描述欄中看到，它標識了所有硬鏈接（即具有硬鏈接計數的文件大於 2）和額外的特別是文本。在 Description 列中未標記為“可選省略”的硬鏈接在內部被視為“主要”硬鏈接。

6.3.1 哈希值計算與匹配

可以為卷快照中的文件計算哈希值。如果您將此操作再次應用於相同的文件，則不會重新計算它們。除了單純的哈希計算之外，取證許可還允許將哈希值與內部哈希數據庫中單獨選擇的（或簡單的所有）哈希集進行匹配。該過濾器稍後可用於隱藏已知的不相關文件。在哈希數據庫的幫助下被識別為不相關的文件可以有選擇地從進一步的捲快照優化操作中排除，這在其他好處中節省了時間。散列值一旦計算出來就不會在卷快照中更新。但是，匹配過程（在卷快照中查找文件的哈希值）可以隨時針對相同的文件重複進行。這將首先丟棄卷快照中所有文件的先前哈希集匹配項，除非您僅將匹配應用於標記文件（在這種情況下，只有那些文件會丟失其先前的哈希集匹配項）。哈希類別字段只會更新，不會清空。

在優化卷快照時，可以同時計算兩種不同哈希類型的哈希值，用於一般目的或將它們與具有不同哈希類型的兩個哈希數據庫進行匹配。如果選擇匹配，則所有哈希值將與哈希類型匹配的兩個哈希數據庫中的任何一個進行匹配。這意味著即使卷快照中的主要散列類型是 MD5，次要散列類型是 SHA-1，並且散列數據庫 #1 基於 SHA-1 而散列數據庫 #2 基於 MD5，X-Ways Forensics 也會相應地匹配散列值。卷快照和哈希數據庫中的哈希類型不必按相同順序排列。

取證許可證允許驗證在較早時間點計算的或從證據文件容器導入的哈希值。結果將輸出到消息窗口。任何當前哈希值與原始記錄不匹配的文件都將與一個特殊的報告表相關聯，以便於查看。第二次運行散列卷快照優化步驟永遠不會更新已經為卷快照中的文件計算的散列值。

文件的子對像從其父對象繼承散列類別“無關”。這是可能的，因為如果整個文件是不相關的，那麼可以從該文件中提取的所有內容也一定是不相關的。然而，從“顯著”文件中提取的內容不一定也是顯著的，因為可能只有父文件的某些部分或方面是顯著的。當然，僅當用戶選擇不首先從進一步處理中忽略不相關文件時，才會輸出不相關父對象的子對象。

當將哈希值與哈希數據庫（普通哈希如 MD5、SHA-1、SHA 256 等）進行匹配時，可以選擇製作數據庫的本地副本並使用該副本。這個

如果您與同事共享數據庫並且您的同事想要在數據庫用於匹配時更新數據庫（例如添加額外的哈希集），這可能會很有幫助，否則這將無法在卷快照優化的整個過程中進行。如果數據庫很大並且不適合主內存並且存儲在遠程網絡驅動器上，它還可以提高性能。如果本地副本尚不存在，則在臨時文件目錄中創建本地副本，並且僅在散列數據庫的主副本發生更改時更新（所有用戶都應具有 v19.8 或更新版本，以避免不必要的複制未更改的數據庫）。

6.3.2 文件類型校驗

取證許可證允許您根據簽名和各種算法驗證文件類型，即檢測卷快照中所有文件的文件名/文件類型不匹配，但已知其原始第一個簇不再可用的文件除外。例如，如果有人通過將其命名為“invoice.xls”（錯誤的文件擴展名）來隱藏一張有罪的 JPEG 圖片，則識別的文件類型“jpg”會顯示在目錄瀏覽器的類型列中。有關詳細信息，請參閱類型和狀態列的說明。用於不匹配檢測的文件簽名和擴展名在隨附的文件類型定義文件中定義，您可以完全自定義這些文件。它也是用於文件頭簽名搜索的同一個數據庫。請注意，空閒簇中的當前數據與先前存儲在該簇中的已刪除文件及其文件名之間的鏈接很弱，因此文件擴展名和檢測到的類型之間的差異可能只是重新分配的自然結果在此期間將此群集到一個完全不同的文件。如果您希望重複文件類型驗證，例如在編輯文件類型簽名數據庫之後，請務必選中再次選項。目錄瀏覽器類型欄的狀態見“類型狀態”欄。

大多數自解壓.exe 存檔也由文件簽名檢查在內部檢測到。它們被歸類為“sfx”文件類型並分配給“檔案”類別，以便可以專門針對它們。這可以防止此類存檔中的壓縮文件在調查中完全被忽視。Zip 壓縮的.exe 檔案可以在預覽模式下查看，其他自解壓檔案需要從圖像中復制並使用適當的工具（如 WinRAR 或 7-Zip）打開。

文件簽名檢查還揭示了混合 MS Office 文件，即合併的 MS Word 和 MS Excel 文檔，可以在兩個應用程序中打開，顯示不同的內容。將在消息窗口中顯示一條通知，並且任何檢測到的文件都將與一個特殊的報告表相關聯。混合 MS Office 文件是一種隱藏其中一個合併文檔內容的巧妙嘗試。

6.3.3 內部元數據提取

需要法醫執照。

- 可以檢查EXE、ZIP、RAR、JPEG、GIF、PNG、RIFF、BMP、PDF文件的文件格式一致性。Type Status 列將顯示結果，“OK”或“corrupt”。

b) 允許從 OLE2 複合文件（例如 2007 年之前的 MS Office 文檔） .EDB、PDF、MS Office HTML、EML、MDI、ASF、WMV、WMA、MOV、JPEG、THM、TIFF、PNG 中提取內部存儲的創建時間、GZ、GHO、PGP pubring.pkr 密鑰環、ETL、SQM、IE Cookies、CAT、CER、CTL、SHD 打印機假脫機、PF 預取、LNK 快捷方式和 DocumentSummary 備用數據流。這個時間戳將顯示在 Int. 目錄瀏覽器的創建列。在某些情況下，將提取最早的時間戳，這最接近真實的原始創建日期。

c) 允許將某些文件元數據複製到元數據列，這將允許您按此元數據進行過濾，使用導出列表命令導出元數據，並在案例報告中將其與報告表一起輸出。可以從詳細信息模式特別支持的所有文件類型以及 Windows 快捷方式文件 (.lnk) 和預取文件 (.pf) 中提取元數據。僅提取您在“詳細信息”模式下看到的元數據的子集。您可以選擇從提取的元數據中去除某些行，以便在元數據列中看不到它們，例如使案例報告或導出列表命令的輸出更緊湊以便在屏幕上打印或查看，或者只是因為某些元數據字段與您無關。您可以通過子字符串識別不需要的元數據字段。該子字符串可以匹配字段名稱（例如

“焦距”）或字段的值（例如，如果您事先知道如果文檔作者的姓名是“Joe Huber”，您對“作者”字段不感興趣）。每行輸入 1 個子字符串。子字符串可以包含空格。您可以通過共享文件“Unwanted Metadata.txt”來共享您的定義。

基於名為“Jump List Names.txt”的新用戶可編輯文本文件，跳轉列表哈希值被轉換為 customDestinations-ms 和 automaticDestinations-ms 跳轉列表文件的呈現元數據中的應用程序名稱。翻譯表目前包含大約 500 個條目。如果您添加條目，請確保將它們插入正確的位置，以便所有條目按 CRC 升序排序。CRC 中的前導零顯然必須保留。CRC 和應用程序名稱之間有一個製表符。

d) 允許在 \$!* 回收站文件和 iPhone 移動同步備份索引 (Manifest.mbdx) 等某些文件類型中找到時恢復原始文件系統元數據（例如文件名、時間戳）。原始文件名通常比隨機名稱更有意義，隨機名稱只是為了保證備份目的在單個目錄中的唯一性。

此類隨機名稱的示例是 3a1c41282f45f5f1d1f27a1d14328c0ac49ad5ae (iPhone 備份中的文件) 或 \$RAE2PBF.jpg (Windows 回收站)。根據文件系統的當前文件名仍然可以在名稱列中的方括號中看到，以及在詳細信息模式下，名稱過濾器將找到原始名稱和當前名稱，因此當前文件名不會完全丟失。

替代名稱和時間戳也從 Linux PNG 縮略圖中提取，如 Ubuntu 和 Kubuntu 發行版、桌面管理器 MATE 和 GNOME ThumbnailFactory。

原始文件的名稱顯示在名稱列中的方括號中，原始文件的記錄時間戳顯示為“內容創建”時間戳。原始文件的完整路徑可以在元數據列中看到。

e) 填充原始單個電子郵件文件 (.eml、.emlx、.olk14msgsource) 的發件人和收件人列。提取此類電子郵件的主題並將其顯示在名稱列中（如果與文件名稱不同），除非該文件是雕刻文件（即帶有

人工生成的文件名），原始文件名將被保留並在同一列中顯示為替代名稱。

f) 創建 Internet 瀏覽器 SQLite 數據庫的預覽，這可能需要檢查文件的真實文件類型。支持 Firefox 歷史、Firefox 下載、Firefox 表單歷史、Firefox 登錄、Chrome cookie、Chrome 存檔歷史、Chrome 歷史、Chrome 登錄數據、Chrome 網絡數據、Chrome 同步、Safari 緩存、Safari 提要和 Skype 的 main.db 關於聯繫人和文件傳輸的數據庫。谷歌 Chrome 瀏覽器歷史記錄還顯示每個訪問過的網站的轉換，從而更容易確定訪問是由用戶觸發的還是由重定向等其他操作觸發的。還列出了每次訪問的持續時間。從 Chrome 地址欄運行的互聯網搜索列在單獨的表格中，並且也添加到事件列表中。

解析 Google Chrome SNSS 會話文件（當前/上一個會話和當前/上一個標籤）。生成的會話概覽列出了所有打開的選項卡及其瀏覽歷史記錄。還創建 Internet Explorer index.dat 文件（包括在文件頭簽名搜索期間從不同位置的單個記錄編譯的人工 index.dat 文件）、Internet Explorer 10 的 WebCacheV*.dat 文件、Edge 瀏覽器的 spartan.edb 文件（所有收藏夾和閱讀列表條目將添加到事件列表）和 \$UsnJrnl:\$J、Windows 事件日誌 (.evt 和 .evtx)、Apple FSEvent 日誌。從 iOS 的 sms.db 中，所有通過短信記錄的對話都被提取到單獨的聊天文件中，所有消息都被添加到事件列表中，可以根據電話號碼或電子郵件地址對其進行過濾。還從 Safari 的圖標數據庫中提取瀏覽歷史信息。

這個替代源非常有趣，因為即使 Safari 處於隱私瀏覽模式，它也會記錄瀏覽歷史。

X-Ways Forensics 可以從 .evtx 事件日誌中的事件負載中提取特定數據，並將它們直接列在事件列表中。這使得事件日誌的使用更加強大，因為它允許快速過濾用戶名、登錄或 RDP 事件的 IP 地址、任務或服務名稱、PowerShell 命令等。有一個製表符分隔的定義文件“事件日誌安裝目錄中的“Events.txt”，其中包含事件 ID 列表、(可選)日誌提供程序、要提取的各個數據字段列表（以逗號分隔）和 (可選) 將添加到事件描述中的文本註釋場地。定義文件可以根據您自己的要求進行調整，包括通過在第一列中放置一個分號來註釋掉各個行。.evtx 文件中的事件在 TSV 表中輸出。該表包含每個事件的完整負載。它最好在 MS Excel 或類似應用程序中查看。

index.dat 的 HTML 預覽和視圖 Internet Explorer 瀏覽器緩存/歷史文件包含一個列，其中包含文件中記錄的偏移量，其中每一行的數據都已找到。

此偏移量顯示為鏈接。如果單擊它，您將自動導航到文件模式下相應 index.dat 文件中的該偏移量，以便於驗證 X-Ways Forensics 從該位置的記錄中提取的信息。（請注意，只有當鏈接沒有分成兩行時，這才能正常工作，這可能發生在查看器組件的 v8.4 中，但不會發生在 v8.3.7 中。無論如何，您仍然可以手動導航到該偏移量。）

元數據和事件是從 SRUDB.dat 中提取的，即系統資源使用監視器 (SRUM) 捕獲的活動。您可以看到隨著時間的推移啟動的進程，列出它們的所有者以及大量統計信息。每個進程的網絡使用活動也被提取出來。提取的信息可用於查明可能的入侵時刻或導致入侵的過程。該信息在詳細的 HTML 子對象文件中顯示，並作為事件列表中的事件顯示。還包括對 iOS netusage.sqlite 文件的支持，該文件記錄了

應用程序的數據使用。除了流入和流出的數據量外，它們還提供應用程序首次和最後一次使用的大致時間戳。提取適當的事件並創建包含所有相關信息的 HTML 預覽。

將生成的 HTML 子對像不僅可以由 X-Ways Forensics 在內部用於父文件的預覽。您還可以通過將這些子對象發送到您選擇的程序（目錄瀏覽器上下文菜單），在您首選的瀏覽器或 MS Excel 等外部程序中查看所有這些表格。您可以讓 X-Ways Forensics 在任意行數之後拆分 HTML 表格。如果您確實使用首選 Internet 瀏覽器而不是使用無法處理非常大的表格的查看器組件在外部查看 HTML 預覽，則可以將此數字設置得更高。具有瀏覽器數據、事件日誌和更多數據源的可搜索文本的 HTML 子對象的存在也提高了搜索和索引的效率。

g) 從各種其他 SQLite 數據庫中以 TSV 格式提取表格，並將第一個表格用作 SQLite 數據庫文件本身的預覽。

h) 提取已編輯的 PDF 文檔的原始修訂版（如果可用）作為子對象。

i) 提供來自文件系統的時間戳作為事件以在事件列表中進行分析。

j) 提供文件中的內部時間戳作為事件。

k) 可以估計文件的一般相關性，您可以通過按相關性列排序來按相關性順序檢出文件。文件的當前性和大小影響其計算的通用相關性的權重是用戶可定義的。100% 表示默認權重。50% 意味著其中的一半。0% 表示該因素根本沒有影響。最大值為 255%。用於通用相關性判斷的設備類型的權重可以在文件 Generator Signatures.txt 中定義。權重因子可以在 *** 行的末尾找到。取值範圍為 0~50。對於 JPEG、PNG、GIF、WEBP 等格式的圖片，算法更注重情報價值而非新聞價值，證據價值的權重高於信息價值。相關值 3.0 是在文件類型 Categories.txt 中為 JPEG 文件定義的基本值。這個價值也是你可以從只是廣告的圖片中得到的。3.2 = 典型的瀏覽器緩存圖片。3.5 = 系統分區圖片的典型值。3.9 = 社交媒體。4.1 = 網絡攝像頭。4.2 = 備份。4.7 = 最初由數碼相機拍攝的照片。按相關性對圖片進行排序可在畫廊中實現分組效果，因為來自相似上下文的圖片會彼此相鄰排序。

l) 可以填充“結構類型”列。結構類型是對生成器簽名概念的改進，具有可擴展類型學的思想，填補了文件類型和哈希值之間的空白。結構類型以十六進製表示法表示為 32 位整數。相同的數字通常標識屬於同一序列的圖片/視頻/文檔/文件（例如，可能是在同一張照片拍攝期間拍攝的照片）。JPEG、PNG、GIF、WEBP、BMP、DOC、XLS、WEBP、WAV、EML、MSG、GZIP、普通 ZIP、TAR、MP3、HTML、PDF、Quicktime 視頻（MP4、MOV、3GP、...），以及 DOCX、PPTX、XLSX。請使用時間戳和其他元數據驗證通過此專欄獲得的任何見解。您可以復制感興趣文件的結構類型。

並使用該列的過濾器來搜索具有相同結構類型的文件（或為此使用“類似文件的過濾器”上下文菜單命令）。結構類型也可用作“在列表中查找重複項”命令中的標準。

m) 當 X-Ways Forensics 確定某些受支持文件類型的文件的生成設備類型時，如果此發現的置信度超過您指定的最小百分比，它將在“設備類型”列中輸出結果。

6.3.4 檔案探索

取證許可證允許在卷快照中包含 ZIP、RAR、ARJ、GZ、TAR、7Z 和 BZIP 存檔的內容，以便這些存檔中的文件可以在其解壓縮時單獨列出、檢查、搜索等狀態，只要檔案未加密。

理論上，可以處理的嵌套級別數沒有限制（即檔案中的檔案中的檔案……）。如果文件在存檔中被加密，則它們在屬性列中標記為“e”，存檔本身標記為“e！”。這允許使用屬性過濾器輕鬆關注此類文件。

MS Office 2007/2010/2013、LibreOffice、OpenOffice 和 iWork 的文檔文件在技術上通常也是 Zip 存檔，如果是的話，默認情況下以相同的方式處理。如果您或您準備的證據文件容器的接收者只希望看到整個文件，而不希望單獨看到嵌入的圖片或 XML 文件，並且不需要從這些 XML 文件中提取元數據，則可以選擇不處理這些文件並且可以在必要時自己識別嵌套文檔（嵌入在其他文檔中的文檔）。還有許多其他文件類型在技術上是 Zip 的子類型，可以選擇性地進行處理。內容通常不相關的 Zip 子類型例如 .jar、.apk 和 .ipa，儘管惡意軟件調查員等特殊利益集團可能不這麼認為，所以選擇權在您手中。

X-Ways Forensics 嘗試檢測並保護自己免受 zip 炸彈以及遞歸 zip 和 gz 存檔以及可能的其他遞歸存檔類型的攻擊。保護意味著一旦檢測到存檔的惡意性質，處理將在一定級別停止。以這種方式識別的檔案將被標記為已處理並添加到特殊的內部報告表中。

請注意，如果之後您希望手動挖掘比遞歸自動探索停止的級別更深，您可以通過將到達的最內部存檔標記為仍有待處理（通過按 Ctrl+Del）然後應用手動探索上下文菜單中的命令。

請注意，要正確處理文件名中包含非 ASCII 字符的 Zip 存檔，您需要先在大小寫屬性中選擇正確的代碼頁。例如，對於在 Linux 下創建的 Zip 檔案，這可能是 UTF-8。對於在 Windows 下使用 WinZip 創建的 Zip 存檔，這可能是區域代碼頁。支持 PKZIP/WinZip 和 7-Zip 樣式的跨區 Zip 存檔，以及跨區 7z 存檔，但不支持其他拆分/跨區/分段存檔類型。

根據 Apple 規範，提取 zip 記錄中額外字段的擴展時間戳並顯示在時間戳列中，這並不總是這些時間戳的含義。在詳細信息模式下，可以看到每個 zip 記錄的替代解釋。

選擇 zip 存檔。後一種解釋顯示了這些帶有“UT”前綴的時間戳，並試圖識別實際的格式變體，例如在 GrayKey 集合中使用的格式變體，並且從 GrayKey 集合中還提取了另一種類型的時間戳（記錄更改時間戳）。擴展時間戳的替代解釋也可以在目錄瀏覽器中提供。這是 Options | 中的一個選項卷快照。這種處理需要更多的時間。

也可以處理加密的 ZIP、RAR 和 7Z 文件存檔，前提是知道或可以猜到密碼。X-Ways Forensics 將嘗試當前案例的密碼集合中列出的任何密碼。可以從案例屬性中編輯案例特定的密碼集合，它存儲在案例目錄中的 UTF-16 編碼文本中，名為“Passwords.txt”。支持幾乎所有的 Unicode 字符，包括空格字符和漢字等。密碼通常區分大小寫。如果集合包含特定文件存檔的正確密碼，則該密碼將被記住在該文件的提取元數據中，並直接從那裡獲取，而不是密碼集合。如果以後需要再次讀取存檔中的文件。或者，您可以通過編輯該文件的元數據手動和直接為特定文件存檔提供特定密碼，您只需要知道密碼必須以“密碼：”為前綴。（法語用戶請注意：冒號前沒有空格。）如果在將文件添加到卷快照時正確的密碼可用，則加密文件存檔中的文件不會被視為和顯示為加密（“e”屬性）。檔案本身仍然以“e！”顯示。屬性。當前不支持不僅文件內容而且名稱都被加密的 RAR 壓縮文件和 7Z 壓縮文件。

6.3.5 郵件提取

取證許可證允許分別列出和檢查以下列電子郵件存檔文件格式存儲的電子郵件消息和電子郵件附件：Outlook 個人存儲 (.pst)、離線存儲 (.ost)、Exchange (.edb)、Exchange 支持 2010 及更早版本（2010 仍處於測試階段）、Outlook 消息 (.msg)、Outlook 模板 (.oft)、Outlook Express (.dbx)、Outlook for Mac、Kerio Connect（store.fdb 文件可以像普通 PST/OST 文件）、AOL PFC 文件、Mozilla 郵箱（包括 Netscape 和 Thunderbird）、通用郵箱（mbox、Unix 郵件格式）、MHT Web Archive (.mht)、winmail.dat = TNEF 文件。默認情況下，X 這些方式類型：pst,ost,edb,dbx,pfc,mbox,eml,emlx,mht,mim,msg,olk14msgsource,olk14message,olk14msgattach,olk15msgattach,olk15msgsource,olk15message

取證 嘗試 至 提煉 從 文件

電子郵件消息通常輸出為.eml 文件。為了方便地關注從所有電子郵件存檔中提取的所有電子郵件消息（甚至處理過的原始.eml 文件），建議遞歸探索並使用屬性過濾器（而不是類型或類別過濾器）。出於技術原因，從 MBOX 存檔中提取的深度嵌套電子郵件（已作為附件轉發且其父級再次作為附件轉發）顯示為主要父級電子郵件消息的直接子對象。有一個未標記但帶有工具提示的複選框，當從中提取電子郵件消息和附件時，X-Ways Forensics 會在電子郵件主題之後命名 MSG 文件。這在處理一般命名的 MSG 文件時可能很有用。

對於提取的電子郵件及其附件，發件人和收件人將顯示在目錄瀏覽器的相應欄中。您可以按創建和修改日期以及發件人和收件人進行過濾。

如果電子郵件消息除了發件人 : 行之外還有發件人 : 行，那麼根據發件人 : 行的發件人現在會另外顯示在目錄瀏覽器的發件人列中，在發件人 : 發件人之後，如果實際上不同的話。它們由空格和豎線 (|) 分隔。例如，英文版 MS Outlook 將此類電子郵件顯示為“代表”其他人發送（發件人 : 發件人代表發件人 : 發件人）。您可以通過輸入豎線作為發件人列的子字符串來過濾此類電子郵件。類似地，不同類型的收件人（To:、Cc: 和 Bcc:）在 Recipient 列中由豎線分隔。

如果在電子郵件存檔中找到附件和嵌入文件，也會提取附件和嵌入文件（例如 AOL PFC）並且通常成為卷快照中它們各自包含的電子郵件消息的子對象。所有提取的電子郵件和附件實際上都位於證據對象的元數據子目錄中，並且可能會佔用大量驅動器空間。

從 PST 中提取電子郵件可以在沒有密碼的情況下處理受密碼保護的 PST 檔案！

它支持以下編碼 PST 文件的代碼頁：ISO8859-1、ISO8859-2、ISO8859-3、ISO8859-4、ISO8859-5、ISO8859-6、ISO8859-7、ISO8859-8、ISO8859-9、ISO8859-10、ISO8859-11、ISO8859-13、ISO8859-14、ISO8859-15、ISO8859-16，koi8-r、koi8-u、1250、1251、1252、1253、1254、1255、1256、1257、1258、874、UTF16、UTF32、UTF8

在某些舊的 AOL PFC 文件中，圖片可能以特殊方式嵌入到電子郵件中。在那種情況下，此類電子郵件消息將標有回形針圖標，但不會單獨提取圖片。但是，當從 *.pfc 中提取 JPEG 和 PNG 文件時，可以找到圖片（如果是 JPEG 或 PNG）。

.eml 輸出格式的一些優點：輸出為 .eml 文件的電子郵件消息表現得盡可能簡單、真實和通用。它們易於理解，標題和正文結構清晰，並且非常容易在各種簡單程序（例如文本編輯器、文字處理、Internet 瀏覽器、免費電子郵件客戶端，如 Thunderbird 和 Windows Mail）中完整查看。查看 .eml 文件不需要像 MS Outlook 這樣的商業軟件。.eml 是電子郵件的“自然”格式，就像原始圖像是磁盤圖像的自然格式一樣，如果你甚至想稱它為“格式”（實際上它沒有額外的格式規範，它只是一個它應該表示的數據的簡單表示）。.eml 文件包含電子郵件消息的完整原始元數據，完好無損，與發送和交付時完全相同。如果您將文件複製給其他人，您就可以完全控制該文件，可以查看所有數據，可以驗證沒有意外數據進入文件。您可以使用簡單的文本編輯器輕鬆地手動編輯正文中的任何文本，編輯標題中的任何元數據，如果需要，可以使用簡單的文本編輯器輕鬆地追溯刪除任何附件，所有這些都是複雜的專有二進製文件格式無法做到的比如味精。.eml 文件的一般格式是任何人都可以理解的，它只是一個文本文件。MSG 文件的格式只有具有計算機科學或編程背景才能理解，學習它需要花費大量時間。編輯隱藏在 MSG 文件中的電子郵件數據很困難。

電子郵件處理的一個附帶任務是從電子郵件相關的 MIM 檔案中提取文件並製作

它們以純二進制形式作為卷快照中的子對象訪問。

6.3.6 發現嵌入式數據

僅限法醫執照。允許通過某些文件中的字節級文件頭簽名搜索來雕刻嵌入在其他各種類型文件中的各種類型的文件。如果外部文件（宿主文件）完好無損且嵌入文件未以碎片方式存儲在宿主文件中，則此操作成功。否則嵌入的文件可能顯示為已損壞。值得注意的是，此功能可搜索 JPEG 和 PNG 圖片，甚至是其他 JPEG 文件（包含自身縮略圖的文件）中的 JPEG 圖片。通過這種方式找到的文件將被統稱為“Embedded 1....jpg”、“Embedded 2....png”等。HEIC 文件中的縮略圖以 JPEG 格式輸出。

此功能還提取嵌入在多頁打印輸出中的.emf 文件 (.spl 假脫機程序文件)。僅包含單個.emf 文件的.spl 文件可以直接使用查看器組件查看。同樣以這種方式提取的還有來自.customdestinations-ms 跳轉列表的.lnk 快捷方式文件。

存在特殊的內部算法，通過遵循相應文件格式的數據結構，即使碎片化，也可以從.automaticdestinations-ms 跳轉列表中正確提取.lnk 快捷方式文件，從 OLE2 複合文件（例如 MS Word .doc，MS PowerPoint .ppt）、Firefox 瀏覽器緩存（基於“_CACHE_MAP_”文件）、Safari 瀏覽器緩存、諾頓備份文件（N360 備份、.nb20）和 Windows Vista/7 Windows.edb 數據庫（來自後者甚至電子郵件信息），以及在 VCF 文件（電子名片）中嵌入為 Base64 的圖片。

Chrome 瀏覽器緩存基於“索引”文件進行處理，支持同一緩存條目的多個流：輸出 HTTP 韻應（名為.chrome1）以及編譯的 JavaScript 條目(.js1)（如果存在）。如果 web 服務器發送了 no-cache 指令，至少 HTTP 韵應仍然被緩存。在預覽模式下，您可以看到 HTTP 韵應的特殊表示。如果 Chrome 緩存的索引不可用，現在也可以處理 Chrome 緩存，例如，如果緩存碎片已被分割或緩存被部分刪除或損壞。在某些情況下，即使存在索引，也可能在沒有索引的情況下獲得更好的提取結果。要嘗試這樣做，如果之前未處理過索引，則可以讓 uncover 函數處理“data_4”文件並省略索引。data_4 是可選的“特殊興趣”組的一部分。

還提取了來自 thumb*.db 文件的縮略圖，來自 Google 的 Picasa 3 圖像管理器和查看器軟件（thumbindex.db 和相關文件）、Photoshop 縮略圖緩存（Adobe Bridge Cache.bc）、Canon ZoomBrowser 縮略圖集合（.info），以及 Paint Shop Pro 緩存（.jbf）。

某些非常舊的“thumbs.db”文件中的縮略圖無法正確顯示。此類 thumbs.db 文件將分配給報告表“Unsupported thumbs.db”，並且可以通過 GreenSpot Technologies Ltd. 免費提供的程序“DM Thumbs”等查看。Windows Vista 及更高版本的 Thumbcache*.db 文件是間接目標thumbcache_idx.db 是否在掩碼中並且該文件是否在同一目錄中可用。這樣可以加快提取速度並避免輸出大量重複縮略圖（僅輸出最高分辨率）。如果 thumbcache_idx.db 在掩碼中，那也意味著 thumbcache*.db 文件是專門

除非也選擇/標記了 thumbcache_idx.db 文件，否則不會處理選擇或標記的處理。

此外，它從 PDF 文檔中提取任何類型的標記為嵌入的文件以及 JPEG 和 JPEG 2000 以及 XML 格式的 Acrobat 表單文件和 JavaScript 對象（後者可以更容易地確定 PDF 文件是否應被視為惡意軟件）。從 Firefox 和 Chrome SQLite 數據庫中提取單個 cookie 文件，還提取作為 Base64 嵌入 XML 格式的 PList (.plist) 中的數據塊和嵌入二進制 PList (.bplist) 中的原始數據塊。

建議同時驗證文件類型，以便 X-Ways Forensics 可以區分傳統（XML 格式）PList 和二進制 PList (BPList)。許多 PList 沒有 .plist 擴展名，需要先識別為 PList。由於嵌入數據的類型不由 PList 本身識別，因此輸出也受益於同步文件類型驗證。Nested PLists (PLists embedded in PLists) 也會被遞歸識別和處理。為 PList 創建的另一個子對像以人類可讀的方式表示已解析的文本，並用作 PList 本身的預覽。

還重建電子郵件消息並從 Windows Mail 客戶端（Windows 7 和更新版本）使用的 Livecomm.edb 數據庫中提取聯繫人和帳戶信息，從 Windows Live Mail contacts.edb 數據庫中提取聯繫人，也從 Windows Live 中提取聯繫人 Messenger 的 contacts.edb 數據庫..

您還可以在 32 位和 64 位 Windows PE 可執行文件（程序和庫）中發現各種可能相關的資源作為子對象，特別是 RCDATA、命名對象、位圖、圖標和清單。例如對惡意軟件分析很有用。這不會自動發生，只有當您通過一系列合適的文件掩碼專門針對可執行文件時才會發生。

卷快照中的完全 Base64 編碼文件，前提是它們在 Type 列中具有“b64”可以自動解碼，並且結果以二進制形式輸出為（令人驚訝的）子對象。

最後同樣重要的是，此功能可以從 Windows XP、Vista 和 7（32 位和 64 位）解壓縮 hiberfil.sys 文件，並自動將結果作為原始內存轉儲添加到案例中。 hiberfil.sys slack（來自以前使用 hiberfil.sys 文件的壓縮數據，如果最後一次使用比以前的使用實現更強的壓縮，則在末尾找到）作為解壓縮形式的子對象提供。

通常，此函數生成的所有文件都作為它們所在主機文件的子對象添加到卷快照中。出於性能原因，不會觸及小於 65 字節的文件。

維護兩個單獨的文件掩碼以發現各種文件類型中的嵌入數據。第二個面具是可選的，標記為“特殊興趣”。例如，惡意軟件調查人員可能會選擇在需要時也以這種方式處理可執行文件。您可以在掩碼的任何元素前面加上冒號以暫時將其排除，但將其保留在列表中以供將來參考。例如：*.jpg 表示不是以 jpg 作為擴展名或類型的文件。

在沒有內置內部提取算法的文件類型中，X-Ways Forensics 嘗試使用“文件頭”中標記的那些文件頭簽名來雕刻嵌入數據

帶有“e”標誌的簽名 Search.txt”。這意味著如果您願意，您可以讓 X-Ways Forensics 發現比默認情況下更多的文件類型中的嵌入數據！

採取了額外的預防措施，以免產生文件頭簽名搜索已經雕刻的文件副本。更準確地說，此函數的輸出將替換卷快照中相應的雕刻文件。雕刻文件的內部 ID 將保持不變，但可能會提供其他元數據（例如作為父文件的子對象的路徑/表示、假定的原始文件名、更正確的文件大小等）。使用通常的設置，這會影響相當多的扇區對齊文件。

在上面未處理的所有文件中搜索文件頭簽名

一個單獨的可選子操作允許您在第一個子操作未處理的任何文件中自由雕刻任何類型的文件。默認情況下，為此選擇帶有“e”標誌的文件類型。請格外小心，以避免延遲和大量垃圾文件（誤報）和重複。請非常謹慎地應用此新功能，並且僅在有充分理由的情況下才應用於專門針對特定目標的文件，例如交換文件或存儲文件，備份應用程序在其中連接其他文件而不壓縮，而不是盲目地針對所有文件或隨機文件。請記住，能力越大，責任越大。

標有“E”標誌（大寫）的簽名永遠不會刻在其他文件中，以防止最壞的影響，例如 MPEG 視頻中刻有 MPEG 幀，zip 存檔中刻有 zip 記錄，.eml、.html 和 .mbox 文件雕刻在電子郵件檔案中，.hbin 註冊表片段雕刻在註冊表配置單元中。如果您知道自己在做什麼，當然可以刪除 E 標誌。

有一個選項可以遞歸地應用雕刻過程，也就是雕刻已經在其他文件中雕刻的文件。如果第 1 層的外部文件刻得太大，以至於可以在其中刻下同樣在第 0 層（原始文件）刻下的文件，這可能會導致許多重複項。

如果您想在原始文件中雕刻未在 512 字節邊界對齊的嵌入文件，則可以使用擴展字節級選項。文件永遠不會刻在 \$MFT 中。

默認設置將使 X-Ways Forensics 在 pagefile.sys 文件中的字節級別進行文件頭簽名搜索，以查找電子郵件片段、.lnk 快捷方式文件、圖片等。

6.3.7 從視頻中捕捉靜止圖像

取證許可證允許偶爾從JPEG 格式的視頻文件中捕獲靜止圖像。

這可以在用戶定義的時間間隔（例如每 20 秒）中發生，該時間間隔可以根據視頻的播放長度動態變化，或者您可以為每個視頻選擇固定數量的視頻靜止圖像（1-255），無論播放長度。雖然固定長度的間隔會導致靜止圖像的數量隨播放長度成比例增長，但如果要查看畫廊中的所有靜止圖像，固定的絕對數量會限制您的工作量，並且還會減少處理長視頻的時間，但是

當然，如果任何嫌疑人將相關內容隱藏在無傷大雅的視頻中的某處，代價是不那麼徹底和遺漏某些東西的風險增加。X-Ways Forensics 試圖從整個視頻中均勻地提取固定數量的靜止圖像，以給出具有代表性的印象。

此功能適用於類型與指定文件掩碼系列匹配的文件。需要一個外部程序([MPlayer](#))並要求該卷與活動案例相關聯。

可以從 MPlayer 支持的所有視頻格式和編解碼器中提取圖片。如果您必須系統地檢查許多視頻是否存在不當、非法或其他相關內容（例如兒童色情或恐怖分子訓練營說明），這將很有用。使用間隔可確保您不會錯過隱藏在無害假期或生日聚會視頻中間的視頻的重要部分。

提取圖片大大減少了數據量，而且在畫廊中查看靜態照片比一個接一個地觀看所有視頻要快得多、高效且舒適得多。

可能耗時的提取過程可以在無人值守的情況下運行，例如提前整夜運行。

如果您需要在打印的報告中包含提取的圖片，這也很有用。同時提取的第一張圖片可以選擇作為預覽和畫廊模式下視頻文件的預覽圖片。無法處理受 DRM 保護的 ASF/WMV 視頻，因此會被標記為 e! 在屬性中。柱子。請注意，您可能偶爾會聽到視頻中的聲音。如果您想避免這種情況，請關閉計算機上的聲音。另請注意，如果您選擇較小的間隔，則不一定會獲得額外的圖片。這取決於視頻的編碼/壓縮方式。例如，如果某個特定視頻的編碼方式使其每 8 秒僅包含一個 I 帀（完整圖像），並且其間的所有幀僅描述減少數據的變化，那麼您可以期望靜止間隔不小於 8 秒。那是因為此函數旨在快速工作並且不會在準確的時間索引處重建準確的幀。如果您需要更多詳細信息，可以使用目錄瀏覽器上下文菜單導出所有幀。使用 MPlayer 提取圖片時會省略重複的靜止圖像。

從視頻中導出 JPEG 圖片後，可以選擇在畫廊中動態表示視頻，包括所有提取的靜止圖像，循環顯示靜止圖像，無需進一步的用戶交互即可對視頻內容給出更完整的印象（沒有必須探索它們）。因此，查看大量視頻的另一種有效方法是：遞歸探索、過濾視頻、按子對像數量降序排序（以便將具有相似數量靜止圖像的視頻顯示在一起），並激活圖庫模式。觀看每個視頻的各種視頻劇照。當您確定當前頁面上沒有顯示有罪的視頻時，例如，當所有靜止圖像都已顯示時，請進入下一個畫廊頁面，您會知道畫廊已為每個視頻旋轉回第一個靜止圖像時的情況。

導出靜止圖像時會從視頻中提取少量元數據，通常是視頻數據的編碼/壓縮格式、分辨率、每像素位數、每秒幀數、每秒數據速率。這是對常規元數據提取所提供的元數據的補充。

6.3.8 圖片分析與處理

取證許可證還允許計算照片中膚色的百分比並檢測黑白照片。這可以用於文件類型 JPEG、PNG、GIF、TIFF、BMP、PSD、HDR、PSP、SGI、PCX、CUT、PNM/PBM/PGM/PPM、ICO。在查找掃描的文檔和以電子方式存儲的傳真時，檢測黑白或灰度圖片非常有用。必須尋找兒童色情痕跡的法醫檢查員可以按膚色百分比降序對圖片進行排序，以極大地加快工作速度。

檢查大量 0%...9% 膚色百分比的圖片（例如，數千個瀏覽器緩存垃圾文件）可能不再需要，因為最有可能犯罪的文件將排在列表頂部附近。請注意，可能存在誤報，即非皮膚表面的類似皮膚的顏色。無法正確掃描其顏色內容的圖片，例如因為它們太大或損壞，將以問號而不是膚色百分比列出。

尺寸非常小的圖片（寬度或高度不超過 8 像素，或寬度乘以高度不超過您指定的尺寸）將被標記為無關，假設它們不包含有罪的色情內容或文件。

對於大型 JPEG、PNG、GIF 和 TIFF 文件，在體積快照優化期間分析圖片中的顏色的同時，X-Ways Forensics 還可以選擇提前創建縮略圖，以便稍後在圖庫模式下更快地顯示更新。只有在文件中沒有嵌入原始縮略圖並同時提取時，才會創建內部縮略圖，並且只有在啟用輔助縮略圖時才會將它們實際用於圖庫（請參閱選項 | 一般）。可以指定縮略圖的首選分辨率（以像素為單位的最大寬度或高度）和質量（JPEG 壓縮係數）。但是，縮略圖卷快照中可存儲的最大數據量有限，為 64 KB，因此如果生成的縮略圖大於此值，X-Ways Forensics 將相應地自動降低用戶定義的分辨率。要丟棄所有內部縮略圖，但保留計算出的膚色百分比，您可以在 X-Ways Forensics 背後的證據對象的“_”子目錄中刪除文件“Secondary 1”，即當證據對象當前未打開時。

如果您擁有[Excire PhotoAI](#)的許可證並安裝可下載的軟件包，在此步驟中，您可以擁有人工智能 a) 識別照片中的對象（如人物、建築物、動物、標誌、文本、裸體……）和圖片的屬性（如主要顏色），b) 在照片中找到已知的面孔，並且 c) 找到與您已有的相關照片相似的照片。使用報告表，您可以專注於具有特定內容的照片。您可以定義哪些內容應自動歸類為不相關或值得注意的內容。

右側有一個小按鈕，顯示一個手指。單擊該按鈕將顯示用於使用 Excire PhotoAI 和 PhotoDNA 的用戶界面控件，即使該功能不可用，也可以讓您了解如何使用這些模塊。Excire PhotoAI 可在市場上買到並在此處進行描述：<https://www.x-ways.net/excire.html>。

PhotoDNA 免費提供給執法機構的用戶。

如果您有一個內部 PhotoDNA 哈希數據庫，即使在視覺上有所改變，也可以自動識別已知照片。如果您選擇更嚴格的匹配（允許圖片中的變化更少），則在大型數據庫中該過程會明顯更快。可以看到任何結果匹配

在合併的分析列中過濾。請注意，已通過 PhotoDNA 識別的照片不會額外檢查膚色量。僅當圖片包含的像素總數大於用戶定義的最小值（寬度乘以高度）時，才會計算和匹配 PhotoDNA 哈希值。這避免了在非常大的 PhotoDNA 哈希數據庫中可能非常耗時的數據庫查找，並且通常對小的垃圾圖片沒有任何好處。作為條件允許的最小尺寸為 50x50 像素。PhotoDNA 算法本質上需要一定的最小像素數才能提供有意義的結果。如果您選擇盡可能低的匹配嚴格級別（級別 1），系統會詢問您是否真的確定，因為已知該級別偶爾會出現錯誤匹配。X-Ways Forensics 中提供該級別只是因為它是由 PhotoDNA 的原始開發人員臨時建議的。X-Ways Forensics 中的推薦和默認級別是級別 3。

可以更方便地再次將圖片與 PhotoDNA 哈希數據庫進行匹配，例如，在將一些哈希值添加到數據庫之後，或者在將哈希值分配給不同類別之後，這要歸功於簡單標記為“再次”的複選框。您仍然可以取消選中“已經完成？”整個圖片分析和處理操作的複選框也丟棄膚色計算和預計算縮略圖的結果並重新生成兩者以及從頭開始的 PhotoDNA 匹配。請注意，在重新使用之前計算的 PhotoDNA 哈希值時使用“再次”選項，更改複選框“即使鏡像也能識別圖片”的狀態無效。這意味著如果在第一次計算散列值並將其存儲在卷快照中時之前未進行檢查，則稍後在重新使用存儲的散列值時進行檢查不會有任何好處。

如果在上一次運行期間您讓 X-Ways Forensics 將計算出的 PhotoDNA 哈希值存儲在卷快照中，那麼再次將圖片與 PhotoDNA 哈希數據庫進行匹配會快得多。節省再次從磁盤/圖像讀取文件和再次解碼/解壓縮 JPEG 數據或其他格式（高分辨率照片耗時）和重新計算哈希值的時間。請注意，PhotoDNA 散列比普通散列需要更多的驅動器空間。此外，一張圖片可能需要多個 PhotoDNA 散列。建議僅當您希望 PhotoDNA 哈希數據庫在案例處理過程中發生變化時，才將哈希值存儲在卷快照中以供將來快速重新匹配，例如，如果您或您的同事可能會在該案例中發現更多相關圖片情況下，迫使您搜索這些圖片的其他副本。

在計算 PhotoDNA 哈希值並存儲哈希值以進行重複數據刪除和快速重新匹配時，X-Ways Forensics 現在還會自動將嵌入的縮略圖與其父文件進行比較。如果差異很明顯，將通過兩個報告表“縮略圖差異”和“縮略圖值得注意（數據損壞/不完整）”提請用戶注意，其中後者意味著差異很可能只是因為父級文件損壞或不完整。（縮略圖需要很少的存儲空間並且位於文件開頭附近，可能不受影響因此很有用。）前者可能表明有人追溯性地更改/編輯了全分辨率圖片並保留了嵌入的縮略圖。

曾是。

要丟棄存儲的哈希值，您可以拍攝新的捲快照，或者您可以刪除證據對象的“_”子目錄中的文件“PDNA”，捲快照在內部存儲在該目錄中。

如果匹配從常規哈希數據庫以及 PhotoDNA 哈希數據庫同時返回，但分類衝突，則“更嚴重”類別佔上風：未知 < 已知良好 < 已知，但未分類 < 已知不良。當文件被歸類為不相關時，將文件標記為已查看的選項現在應用於普通哈希數據庫和 PhotoDNA 哈希數據庫匹配的組合結果。

6.3.9 模糊文檔

所謂的FuzZyDoc™技術可以幫助您識別已知文檔（文字處理文檔、演示文稿、電子表格、電子郵件、純文本文件……），其方法比傳統的哈希值更可靠。即使文檔以不同的文件格式存儲（例如，首先是 PPT，然後是 PPTX，然後是 PDF），它仍然可以被識別。內部元數據更改，例如在“另存為”之後或打印之後（可能會更新“最後打印的”時間戳），也不會阻止識別。很多時候，即使插入/刪除/重新排序/修改了文本，文檔仍然可以被識別。這是通過使用模糊哈希來實現的。

FuzZyDoc 哈希值存儲在 X-Ways Forensics 中的另一個哈希數據庫中。基於所選文檔的哈希集可以添加到 FuzZyDoc 數據庫中，就像可以在普通哈希數據庫中創建哈希集一樣，並且 FuzZyDoc 哈希數據庫也可以在與其他哈希數據庫相同的對話窗口中進行管理。對於每個選定的文檔，您可以創建 1 個單獨的哈希集，或者您可以為所有選定的文檔創建 1 個哈希集。FuzZyDoc 哈希數據庫最多支持 65,535 個哈希集。您可以選擇導出、導入和合併 FuzZyDoc 哈希集。導出的結果可以與導入功能一起使用，或者也可以作為獨立的數據庫使用。

FuzZyDoc 可供 X-Ways Forensics 和 X-Ways Investigator 的所有用戶使用（即不僅像 PhotoDNA 這樣的執法部門）。FuzZyDoc 應該可以很好地處理幾乎所有西歐和東歐語言的文檔，許多亞洲語言（例如中文、日語、韓語、印度尼西亞語、馬來語、泰米爾語、他加祿語……但不是泰語、迪維希語、藏語、旁遮普語……）和中東語言（例如阿拉伯語、希伯來語……但不是普什圖語……）。請注意，~~算法不會檢測電子帳單或新舊期的數字的文檔和腐敗文本~~。請 FuzZyDoc 哈希數據庫匹配。因此，當請求 FuzZyDoc 匹配時，會自動應用文件類型驗證。

根據相同文本的數量，即使重要細節發生變化（帳單地址、價格、產品描述），算法也會將內容基本相同的文檔（例如，由同一家公司創建的具有相同抬頭的發票）視為相似文檔。這意味著如果您有一份公司發票的副本，與未知文件進行匹配將很容易識別出同一家公司的其他發票。對於與數據庫匹配的每個文檔，最多返回 4 個匹配的哈希集。如果匹配超過 4 個，則選擇 4 個最匹配的哈希集。對於每個匹配的散列集，X-Ways Forensics 還提供一個百分比，粗略地指示文檔內容與散列集匹配的程度。有兩種不同的百分比類型可用。基於已處理文檔中總文本的百分比讓您了解文檔中有多少文本是已知的/曾經是

識別，而基於哈希集表示的文本的百分比讓您了解文檔與哈希集所基於的原始文檔的相似程度（僅當您為每個文檔生成1個哈希集時才有意義，即不將多個文檔合併到1個哈希集中）。匹配百分比不會一個一個地計算字符，它只適用於真正有意義的文檔，而不適用於只包含幾個單詞的小測試文件。

在將文件與 FuzZyDoc 哈希數據庫（Specialist | Refine Volume Snapshot 的新操作）進行匹配之前，您可以指定要分析的文件類型，並且可以取消選擇暫時不感興趣的數據庫中的哈希集。請注意，處理較少的文件（例如，通過在掩碼中指定較少的文件類型）當然需要較少的時間，但按比例選擇較少的哈希集進行匹配並不會節省時間。您可以指定匹配所需的某個最小百分比（默認為 15%）以忽略無關緊要的次要相似性。該選項也不是為了節省時間。

為了將捲快照中的所有文檔與 FuzZyDoc 哈希數據庫重新匹配，請先取消“已完成”框中的複選標記。否則，出於性能原因，相同的文件將不會再次匹配。不僅在向 FuzZyDoc 數據庫添加額外的哈希集時，而且在刪除哈希集時，都可能需要重新匹配相同的文件，因為這會使某些內部鏈接無效（如果發生這種情況，它將顯示在結果列）。

與 FuzZyDoc 數據庫的匹配顯示在與 PhotoDNA 匹配和膚色百分比相同的列中，稱為“分析”。FuzZyDoc 匹配過濾器可用。

FuzZyDoc 應該對多種白領犯罪案件非常有用，最明顯（但不限於）那些涉及被盜知識產權（例如軟件源代碼）或機密文件洩漏的案件。

6.3.10 加密檢測

取證許可證允許有選擇地執行文件格式特定和統計加密測試。通過熵測試，檢查每個大於 255 字節的現有文件是否已完全加密，即從第一個字節到最後一個字節。如果測試是肯定的（熵超過某個閾值），則文件被標記為“e？”在屬性列中，以表明它可能值得特別注意。典型示例：加密的容器文件，可以通過 TrueCrypt、PGP Desktop、BestCrypt 或 DriveCrypt 等加密程序掛載為盤符。

熵測試不適用於 ZIP、RAR、TAR、GZ、BZ、7Z、ARJ、CAB、JPG、PNG、GIF、TIF、MPG 和 SWF 文件，這些文件眾所周知是內部壓縮的，因此幾乎無法區分來自隨機或加密數據。不需要此測試來檢測文件是否在 NTFS 文件系統級別或內部存檔中加密。

其次，擴展名/類型為 .doc (MS Word 4...2003)、.xls (MS Excel 2...2003)、.ppt、.pps (MS PowerPoint 97-2003)、.mpp (MS Project 98-2003)、.pst (MS Outlook)、.docx (MS Word 2007...2010)、.xlsx (MS Excel 2007...2010)、.pptx、.ppsx (MS PowerPointer 2007-2010)，檢查 odt (OpenOffice2 Writer)、.ods (OpenOffice2 Calc) 和 .pdf (Adobe Acrobat) 文件格式的特定加密；MS Office 文檔還用於數字版權管理 (DRM) 保護。如果是肯定的，這些文件會被標記為“e！”在屬性中。

柱子。此檢查要求單獨的查看器組件處於活動狀態。X-Ways Forensics 還會使用此類文件自動嘗試當前案例的密碼集合中的密碼，並在文件的元數據單元格中記住匹配的密碼（如果有），以供將來查看/預覽文件和用戶信息時使用。

此外，加密測試可以檢測 eCryptfs 加密的文件（由 Linux 企業加密文件系統存儲的文件），測試基於 Ubuntu 8.10、9.04、9.10 和 10.04 的 eCryptfs 實現。此類文件將在“屬性”列中標記為“E”，就像 NTFS 中的 EFS 加密文件一樣。

6.3.11 索引

僅在法醫許可下可用。使用與邏輯搜索相同的邏輯讀取數據，具有相同的優點（請參閱該主題）。

根據您提供的字符、Unicode 字符集和/或您選擇的最多兩個代碼頁，為卷快照中所有或某些文件中的所有單詞創建索引。每個證據對象最多可以有三個這樣的索引（例如，在 Unicode 中索引的西里爾字符和兩個西里爾代碼頁）。X-Ways Forensics 允許您方便地從超過 22 種語言中選擇字符進行索引。目前，大多數歐洲語言和許多亞洲語言都是預定義的，例如德語、西班牙語、法語、葡萄牙語、意大利語、斯堪的納維亞語言、俄語、南斯拉夫語言、東歐語言、希臘語、土耳其語、希伯來語、阿拉伯語、泰語、越南語。您可以明確指定每個字符，或者指定字符範圍，如果字符池的編輯框以“範圍：”開頭，則可以選擇後跟其他單個字符（例如 a-zA-Zäöü）。要索引破折號本身（不推薦），請將其指定為編輯框中的最後一個字符。

編制索引可能是一個耗時的過程，可能需要大量的驅動器空間（默認設置和平均數據的經驗法則：原始數據量的 5-25%）。

然而，該索引將允許您非常快速和自發地進行進一步的搜索。

索引文件保存在相應證據對象的元數據文件夾的子目錄中。索引的範圍，即要索引哪些文件，可以微調。

請注意，分區介質（如物理硬盤）的索引僅覆蓋未分區的區域。那是因為每個分區都可以有自己的索引。

短於您指定的下限的單詞將被忽略。字符的最小長度越長，索引越小，索引過程越快。默認下限為 4 個字符。可以使用減號前綴從例外列表中的索引中排除頻繁不相關的詞（例如 -and，如果 3 個字母的詞已經被接受），這會減少索引的大小和創建它所需的時間。可接受的字長範圍越大，索引就越大，索引所需的時間也就越多。重要的 3 個字母的單詞可以添加到帶有加號前綴（例如 +xtc）的排除列表中，這會覆蓋 4 個字符的默認下限。例外列表不必按字母順序排序。例外列表中超過您指定的上限的單詞在索引中被截斷。例外列表中的單詞受字符池限制，不能包含不同的字符。

X-Ways Forensics 可以選擇性地區分大小寫字母，即創建區分大小寫的索引。這可能很有用，例如，如果您創建索引是為了稍後導出單詞列表以進行自定義字典攻擊。

如果 X-Ways Forensics 在索引中包含子字符串，這將進一步減慢索引創建速度（3 到 5 倍）並使索引膨脹，但是，您稍後將能夠在“家庭主婦”中找到例如“wife”和“解決”中的“解決”。如果索引中不包含子串，後面仍然可以在索引中搜索子串，但結果會不完整，搜索速度會慢很多。請注意，如果要索引的語言中的單詞沒有用空格分隔（例如中文、日語或泰語），則用戶有責任啟用子字符串索引。

如果要編制索引的數據與創建索引的案例文件和目錄位於同一磁盤上，則編制索引會不必要地變慢。如果您的 Windows 系統配置為下載更新並在安裝時自動重啟，請盡量避免使用活動的 Internet 連接進行索引。

可選地，某些文件類型中的文本可以被解碼以用於索引（參見邏輯搜索），並且可以在一個步驟中為與案例關聯的多個選定的計算機媒體/圖像創建索引。您最多可以同時在六個不同的代碼頁中建立索引。

可以在 Unicode 中定義一個字符替換列表，使某些字母被索引為其他字母（例如，“é”只是“e”）。這將允許您通過單個索引搜索找到某些拼寫變體，例如名稱“René”末尾帶有重音符號 e 和“Rene”不帶任何拼寫。此列表必須具有結構 é>e è>e à>a

...

（即每行 1 個替換）並且需要作為名為“Character Adjustment.txt”的 Unicode 文本文件存在，該文件以 LE Unicode 指示符 0xFF 0xFE 開頭。“Character Adjustment.txt”是一個可選文件，應位於 X-Ways Forensics 安裝目錄中。

如果您將空格字符定義為單詞的一部分，您將收到警告。那是因為空格字符是用來分隔單詞的，它們不是單詞本身的一部分。如果一個空格字符被定義為單詞的一部分，那就意味著像“Mike Smith lost his credit card yesterday”這樣的整個句子被認為只是一個詞。

您可以通過刪除“優化卷快照”對話框中的“已完成”複選標記來刪除證據對象的所有索引。這還將清除卷快照中所有索引文件的“i”標誌。

在索引中搜索：在索引文件後，您可以使用同步搜索功能快速搜索索引中的關鍵字。從底部的下拉框中選擇“在索引中搜索”。任何超過用於索引的最大單詞長度的內容都將被忽略（因此即使在索引中根據 7 個字母的最大單詞長度將單詞截斷為“ridicul”，也會在索引中找到“ridiculous”）。X-Ways Forensics 不區分大小寫字母，除非創建了區分大小寫的索引。在搜索命中列表中

由索引搜索填充，物理偏移量不可用。

您可以方便地運行非 RegEx 索引搜索來搜索包含空格字符的搜索詞，就像在常規搜索中一樣。這對於名稱（例如“John Doe”或“XYZ Technology Ltd”）和帶空格的複合詞（例如“銀行帳戶”或“信用卡限額”）非常重要。即使化合物的各個組成部分已經超過索引的最大字長（默認為 7 個字符），這仍然有效，因此您可以毫不費力地找到“籃球位置”（10+9 個字母）或“摩天大樓建築”（10+12 個字母）。

與往常一樣，組件只匹配索引的長度，這不是什麼大問題，因為除了“basketball”和“skyscraper”之外，沒有多少詞分別以“basketb”或“skyscra”開頭。事實上，搜索詞中的空格也匹配空格以外的未索引的單詞分隔符，例如連字符，因此在搜索“蜘蛛俠”和“凍乾”時，您還會找到“蜘蛛俠”和“凍乾”，或“bank_account”中的下劃線（想想“bank_account.html”這樣的文件名），或“credit+card”中的加號（例如，在搜索超過 1 個單詞時在 Google 搜索 URL 中很常見），或句點在“interview.pdf”中。所以在這方面索引搜索甚至比傳統搜索更強大。將空格定義為單詞的一部分是一個很大的禁忌。

6.4 有關卷快照細化的更多信息

如果某個文件的處理凍結，請注意，內部 ID 和當前處理文件的名稱顯示在小進度指示器窗口中。如果卷快照細化應用於證據對象並且細化在一次處理單個文件時崩潰，X-Ways Forensics 將在您重新啟動程序時告訴您哪個文件並將其與名為“崩潰原因”的報告表相關聯？（取決於安全選項）。所有這些都是為了讓您在再次嘗試時可以排除和忽略該文件。如果您從頭開始為該卷重新啟動快照優化，這不會造成任何傷害（不會創建重複並且不會再次花費太多時間），因為已經處理過的文件將很快被跳過，直到上次保存優化進度的點，這取決於案例的自動保存間隔。卷快照分別為每個文件記住卷快照優化的哪些操作已經應用於它，因此通常不會將相同的操作再次應用於同一文件。

如果計算了有問題（崩潰）文件的哈希值，那麼如果您（繼續）優化卷快照和計算哈希值（至少如果針對相同崩潰文件的保護在案例的屬性）。要使案例忘記以前的 crasher 文件，請單擊案例屬性中的刪除按鈕。跳過的文件也會自動添加到上述報告表中。

卷快照優化的文件處理部分支持多線程（僅當未應用於選擇時）。根據所選的子操作和卷中文件的類型，以及 I/O 速度，這可以使性能翻倍、翻三倍甚至翻四倍。就尋道時間和數據傳輸速度而言，您的大容量存儲解決方案（HDD、SSD、RAID）越快，您節省的時間百分比就越多。此並行化功能仍被認為是實驗性的，尚未完成，但在程序最重要和最耗時的功能之一中節省的時間是巨大的。選擇

多個額外線程僅在搜索圖像或目錄而非磁盤的證據對象時有效。如果您選擇 0 個額外線程，它將像 19.0 之前的 X-Ways Forensics 版本一樣工作。如果您選擇 1 個或多個額外線程，處理將在額外的工作線程中完成（與您選擇的一樣多），並且進程的主線程將空閒，這意味著 GUI 將保持高度響應。在 X-Ways Investigator 中最多可以使用 3 個工作線程，在 X-Ways Forensics 中最多可以使用 16 個，如果您的 CPU 支持的話。如果多線程處理崩潰，下次當你重新啟動程序時，它可能無法告訴你究竟是哪個文件導致了崩潰。如果 X-Tensions 將自己標識為線程安全的，則由 X-Tensions 進行的文件方式處理（通過調用 XT_ProcessItem 或 XT_ProcessItemEx）也會並行化。文件存檔中文件的處理目前在內部被排除在並行化之外。

您可以在卷快照優化後的時間提前安排同時搜索。

6.4.1 相互依賴

所有這些操作之間存在各種相互依賴關係。例如，如果檔案的內容包含在卷快照中，則這些文件中可能有要檢查膚色的圖片，或者要檢查加密的文檔。您可以在以下前提下工作：如果將其他文件添加到卷快照，或者如果檢測到文件的真實類型作為優化卷快照的一部分，則所有適當的其他操作都將應用於該文件（如果它們都被選中）。在適當的情況下，一個操作的輸出會自動成為所有其他操作（甚至再次相同的操作）的輸入。

想像一下，有人試圖通過將一張 JPEG 圖片嵌入到 MS Word 文檔中來隱藏有罪的 JPEG 圖片，將該 .doc 文件誤命名為 .dll，將該文件壓縮到 Zip 存檔中，將 .zip 文件誤命名為 .dll，再將該 .dll 壓縮到另一個文件中 Zip 存檔，再次將該 .zip 文件誤命名為 .dll，然後使用 MS Outlook 通過電子郵件將此 .dll 文件作為附件發送。如果選擇了所有相應的選項，Refine Volume Snapshot 將執行以下操作：從 PST 電子郵件存檔中提取電子郵件附件。它檢測到 .dll 附件實際上是一個 Zip 存檔。然後它將其內容包含在卷快照中，即擴展名為 .dll 的文件。發現該文件實際上是另一個 Zip 存檔。因此，將探索該存檔，並將其中的 .dll 文件檢測為 .doc 文件。通過搜索嵌入的圖片，X-Ways Forensics 在 .doc 文件中找到了 JPEG 文件，如果需要，可以立即檢查它的膚色。所有這一切都發生在一個步驟中。

6.4.2 注意事項

X-Ways Forensics 可以方便地記住卷快照中的每個文件已經應用了哪些優化操作，這樣文件就不會不必要地再次處理，這會導致子對象的不希望的重複、浪費時間等。

X-Ways Forensics 不會記住每個操作的各個子選項（例如，是否為元數據提取選擇了“創建瀏覽器數據庫的預覽”），並且無法逐個跟蹤這些子選項。將始終應用的唯一操作

重複索引和哈希值與傳統哈希數據庫的匹配。如果出於任何原因您希望對同一文件再次應用某些其他操作（例如，然後使用不同的子選項或在更新簽名數據庫以進行文件類型驗證之後），您可能會發現“再次”複選框或將文件完全重置為通過選擇它並按 **Ctrl+Del** 鍵，卷快照細化“仍待處理”的狀態。這還將清除所有計算出的膚色百分比、提取的元數據、散列值、散列匹配等。但是，此函數不會從卷快照中刪除任何子對象。如果需要，這必須由用戶單獨完成，方法是排除和刪除它們。此函數也不會刪除在先前優化操作期間創建的任何事件。另一個鍵盤快捷鍵 **Ctrl+Shift+Del** 允許從卷快照中的選定文件中刪除與普通哈希集、FuzzYDoc 哈希集和 PhotoDNA 類別的匹配項，即使哈希集從哈希數據庫中刪除也不會被丟棄，否則，加上刪除描述列中的“找到重複項”標記。

文件是否應該由卷快照細化處理僅在輪到該文件時決定，而不是在您開始操作時決定。這意味著如果您在卷快照優化正在進行時繼續在程序中工作，並且更改或激活或停用過濾器或標記或取消標記文件或排除或包含文件，這可能仍會影響操作的範圍，具體取決於所選的選項並取決於您標記/取消標記/排除/包含/...的文件是否仍然需要處理。因此，例如，如果您發現該操作花費了太多時間，您仍然可以使過濾器更嚴格或取消標記某些非常大的文件等，而不會中斷該過程。

當卷快照細化處於處理單個文件階段時，則進度百分比只是當前處理文件的內部 ID 除以卷快照中的項目總數。X-Ways Forensics 事先並不知道哪些文件需要大量時間來處理，只有在實際讀取文件時才會決定應該對文件做什麼並發現嵌入了多少數據等。文件類型驗證和潛在的哈希數據庫匹配可能會改變關於如何處理文件的決定，如果有的話。如果整個證據對象僅由 1 個文件組成，例如，如果您將單個文件添加到案例中，則進度百分比不會增加。進度最初為 0%，完成後幾分之一秒為 100%。顯示的百分比不反映給定大文件中的子進度。

卷快照優化對話框窗口中未標記（但有工具提示）的複選框現在可以使 X-Ways Forensics 顯示當前應用於當前處理的文件的子操作。將顯示一個 3 位數的縮寫，含義如下：
Sig :文件類型驗證
Hsh :哈希
Vid :從視頻中捕獲零星的靜止圖像
Idx :預處理原始文件內容以供索引
Dec :文本解碼以供索引
IdX :預處理解碼文本以供索引
Emb :搜索嵌入數據
PDN :PhotoDNA 數據庫匹配
Pic :其他圖片分析步驟
Eml :郵件提取
Fuz :FuzzYDoc 數據庫匹配

Met :元數據提取 Enc :特定

於文件格式的加密測試 Ent :熵檢查 Arc :將檔案中的文件包含到卷快照中如果不是絕對必要，可以通過不選擇它們來節省時間。它也可能對調試有用。此選項是否會減慢某些計算機上的處理速度尚未經過測試。

在 NTFS 上特別徹底的文件系統數據結構搜索的各種子操作期間，某些先前有效的文件時間戳作為事件輸出，具體取決於細化選項“提供來自各種來源的副捕獲時間戳作為事件”，這也可能影響其他操作主要目的不是檢索時間戳/事件。

7 一些基本概念

7.1 編輯模式

信息窗格顯示每個文件/磁盤，它是在程序中打開的模式。信息窗格的上下文菜單允許有選擇地更改活動窗口的編輯模式。

只讀/查看模式：推薦用於計算機取證檢查。為了執行嚴格的取證程序，X-Ways Forensics 中唯一可用的模式，除了當前案例目錄中的文件和臨時文件的通用文件夾中的文件，允許對其進行解碼、解密和轉換等。文件或在查看模式下打開的磁盤不能（有意或無意地）在 WinHex 中編輯/更改，只能查看。換句話說，它們被 WinHex 打開為 write protected = read-only。

默認編輯模式：在默認編輯模式下打開的文件或磁盤的修改存儲在臨時文件中。這些臨時文件是在需要時動態創建和維護的。

只有當您關閉編輯窗口或使用文件菜單的保存菜單命令時，修改才會刷新，並在提示用戶後更新原始文件或磁盤。

就地編輯模式：在就地編輯模式下打開文件或磁盤時請小心。所有類型的修改（鍵盤輸入、填充/刪除塊、寫入剪貼板數據、替換……）都會在沒有提示的情況下寫入原始文件或磁盤（“就地”）。修改後無需手動保存文件。相反，最遲在關閉編輯窗口時，會延遲並自動保存修改。但是，您可以使用 Save 命令來確保在給定時間刷新緩衝區。

如果數據從原始文件傳輸到臨時文件，反之亦然，這在某些操作的默認編輯模式下是強制性的，消耗了太多時間或磁盤空間，則最好使用就地編輯模式。打開非常大的文件或修改大量數據時可能會出現這種情況。由於在就地編輯模式下通常不需要臨時文件，因此此編輯

模式通常比默認編輯模式更快。就地編輯模式是使用內存編輯器時唯一可用的模式。提示：即使在就地編輯模式下，更改文件大小時也不可避免地會創建臨時文件。

如果您使用操作系統打開文件（例如，通過文件 | 打開，從 Windows 當前可用的任何驅動器盤符），然後將使用操作系統文件寫入命令來更改磁盤上的文件。然而，在 WinHex 中，甚至可以在不使用操作系統文件寫入命令的情況下編輯文件，直接在磁盤上/在任何支持的文件系統的原始磁盤映像中，即使 Windows 不知道該文件系統，即使文件不可見 Windows（例如刪除的文件），即使在 Windows 看不到的分區中（例如損壞或刪除），也不會更改任何時間戳或屬性，僅在就地模式下。對於此編輯功能，必須從包含它的已打開卷中打開文件，方法是通過目錄瀏覽器上下文菜單中的打開命令或文件模式（僅限取證許可證）。壓縮文件或其他文件中的一般文件（例如電子郵件和電子郵件存檔中的附件）無法編輯，除非是在證據文件容器中，如果它們是從原始磁盤/圖像複製到那裡的。請注意，不能以這種方式縮短或擴展文件，只能修改已分配區域中的數據。如上所述，僅在 WinHex 中可以編輯直接從磁盤/原始圖像中打開的文件，而不是在 X-Ways Forensics 或 X-Ways Investigator 中，其中扇區級寫訪問（文件編輯在內部轉換）被禁用並且只有磁盤和解釋的圖像以及從卷內打開的文件可用的模式是只讀模式。如果願意，X-Ways Forensics 可以為 WinHex 輕鬆運行（只需重命名 .exe 文件）。

在法醫計算、電子發現和 IT 安全中，這種編輯功能有助於手動編輯（例如改寫）不應檢查/披露/查看的特定數據，或安全地擦除文件中的特定區域（例如定義為塊並填充塊）。請注意，如果證據文件容器尚未轉換為 .e01 證據文件格式，則它們是原始圖像，因此允許追溯文件編輯，但是這將使任何隨附的哈希值無效。甚至可以編輯目錄，即具有目錄數據的簇，例如 NTFS 中的 INDX 緩衝區，例如，如果您需要編輯某些文件的名稱。

7.2 腳本

WinHex 的一些功能可以以自動化的方式使用，例如加速重複的例行任務或在無人值守的遠程計算機上執行某些任務。執行提供的示例腳本以外的腳本的能力僅限於專業許可證或更高許可證的所有者。腳本可以從啟動中心或命令行運行。執行腳本時，您可以按 Esc 鍵中止。

WinHex 腳本是文件擴展名為 “.whs”的文本文件。它們可以使用任何文本編輯器進行編輯，並且只包含一系列命令。出於視覺清晰的原因，建議每行僅輸入一個命令。根據命令的不同，您可能需要在命令旁邊指定參數。大多數命令會影響當前活動窗口中顯示的文件或磁盤。

有關當前支持的腳本命令的說明，請參閱附錄 B。

7.3 X-Tensions API

使用X-Tensions自動執行調查任務並擴展 X-Ways Forensics 的功能：X-Ways Forensics X-Tension API（應用程序編程接口）允許您以編程方式使用 X-Ways Forensics 計算機軟件的許多高級功能，並且用你自己的功能擴展它們。例如，您可以為某些文件類型實施一些專門的文件雕刻、自動分類功能、替代報告生成，或者根據您的要求自動過濾掉不需要的搜索結果等。

除其他外，X-Tensions 允許您：
- 從磁盤/分區/卷/映像中讀取 - 在卷快照中檢索有關每個文件和目錄的大量信息 - 從任何文件中讀取 - 在卷快照中創建新對象 - 分配將文件添加到報告表 - 向文件添加註釋 - 處理、驗證和刪除搜索結果 - 幾乎可以使用 Windows 程序執行所有其他操作！（非常感謝

窗口應用程序接口）

您可以使用您選擇的編程語言，例如 C++、Delphi 或 Visual Basic，而不必學習任何新的編程語言。您可以使用您選擇的編譯器，例如 Visual Studio Express（免費軟件）。

由於擴展不是解釋腳本，而是在應用程序本身的地址空間中運行的常規編譯可執行代碼，因此您可以獲得最高性能，與內部實現的功能相同。X-Tensions 使您可以輕鬆直接地訪問 X-Ways Forensics 內部的重要而強大的功能。

何時可以調用 X-Tensions 函數：
- 優化卷快照時
- 運行同步搜索時 - 通過目錄瀏覽器上下文菜單 -
通過搜索命中列表上下文菜單

X-Tension API 還允許開發和使用所謂的磁盤 I/O X-Tensions。

這些管理單元一方面位於所有分析功能和 X-Ways Forensics 的用戶界面之間，另一方面位於從中讀取扇區的磁盤/映像/RAID/分區/卷之間。例如，他們可以處理全盤加密，並在需要時對 X-Ways Forensics 即時讀取的所有扇區中的數據進行解密，以便所有相關功能只能看到解密後的數據，並且可以像處理數據一樣處理它。普通磁盤/卷。

用戶可以使用案例數據窗口的上下文菜單中的命令通過這樣的磁盤 I/O X-Tension 打開選定的證據對象。選擇預期的 X-Tension DLL 後，如果 DLL 發出信號表明它可以成功處理該證據對像中的數據，則案例將記住選擇的是哪個 DLL，並在下次打開同一證據對象時自動應用它。請注意，與往常一樣，分區算作證據對象。

他們自己。這樣可以解決全盤加密以及卷級加密。

完全運行後，系統會提示用戶是否應在執行後完全卸載頑固的 C# X-Tension DLL。程序員在調試自己的 X-Tensions 時可能更喜歡這樣做，但顯然這可以防止在 X-Ways Forensics 的同一個會話中再次使用同一個 DLL，因此普通用戶最好選擇否。

您可以根據您認為合適的任何許可條款免費或什至收費分發您編譯的 X-Tension DLL 和/或您的源代碼。

有關詳細信息，請參閱<http://www.x-ways.net/forensics/x-tensions/api.html>。

7.4 磁盤編輯器

“工具”菜單中的“打開磁盤”命令允許您打開本地連接的物理存儲設備以及由具有扇區級訪問權限的驅動器號表示的捲。請注意，如果您打開物理分區磁盤，之後您可以通過雙擊該分區打開該磁盤上的分區。分區的表示包括卷鬆弛（不添加到另一個完整集群的多餘扇區），如果存在，邏輯驅動器號不存在。

邏輯卷列表可以選擇包括在 Windows 中處於活動狀態但當前未與任何驅動器號關聯的捲。不是普通卷的活動卷顯示有特殊圖標和特殊描述，例如“TrueCryptVolumeX”。有用的是，在您希望預覽、檢查或獲取的實時系統上，您可以快速查看哪些卷可能需要單獨處理（除了物理存儲設備之外），因為以後很難根據物理存儲設備上的數據。如果列出沒有連接驅動器號的捲，則還包括已作為另一個卷中的連接點安裝在 Windows 中的捲。此類卷以特殊鏈接圖標列出，連接點顯示在卷標和卷大小之間。沒有驅動器盤符的捲列表現在可能還包括以前在 Windows 中處於活動狀態的捲。那些標有劃掉的紅色圓圈圖標。例如，以前安裝的 TrueCrypt 卷可能會以這種方式顯示。

這樣的捲不能再打開，它們只是為了提供信息而列出，這在需要檢查的實時系統上工作時很有用。

通常最好使用捲而不是整個物理存儲設備，因為在這種情況下會提供更多功能。例如，“簇”由文件系統定義，簇到文件的分配（反之亦然）是 WinHex 已知的，“可用空間”和“空閒空間”具有含義。如果您需要編輯邏輯驅動器之外的扇區（例如主引導記錄），如果您希望同時在硬盤的多個分區上搜索某些內容，或者如果分區已損壞或格式化為未知的文件系統 Windows，因此 Windows 無法將其作為驅動器號訪問，您可以改為打開物理磁盤。從代表物理介質的窗口中，您通常也可以打開單個分區，方法是在該窗口的目錄瀏覽器中雙擊它們。WinHex 了解常規 MBR 分區、GPT（GUID 分區類型）、Apple 分區、

superfloppy 格式、由 LDM (邏輯磁盤管理器、MBR 和 GPT 樣式)、LVM2 (MBR 和 GPT 樣式)和 PC 兼容的 BSD 磁盤標籤組織的 Windows 動態磁盤。支持所有動態卷類型：簡單、跨區、條帶和 RAID 5。在打開硬盤時按住 Ctrl 鍵可禁用對動態卷的檢測和特殊處理，並確保將硬盤視為以傳統方式進行分區。上述某些分區類型僅受專業和取證許可支持。

光盤有一個可選的原始模式，允許從音頻 CD 以及數據 CD (CD-ROM 和視頻 CD) 上包含糾錯碼的完整 2352 字節扇區讀取。如果物理存儲設備在 Windows 磁盤管理中被視為脫機或只讀，則該信息將顯示在所有磁盤選擇對話框窗口中。可以打開離線磁盤進行讀取/成像/分析，但它們是寫保護的。

請注意以下限制：

· 需要管理員權限才能訪問任何類型媒體上的扇區。在 Windows Vista 及更高版本下，您需要專門以管理員身份運行該程序，僅以管理員身份登錄是不夠的。

- 無法按扇區訪問遠程 (網絡)驅動器。 · X-Ways Forensics 根本無法編輯磁盤扇區或解釋圖像中的扇區，只能編輯 WinHex 能夠。
- WinHex 不能寫入 CD-ROM 或 DVD。
- 在 Windows Vista 及更高版本下，WinHex 無法寫入活動分區上的扇區 Windows 安裝和運行 WinHex 的分區。

本手冊的附錄 C 提供了主引導記錄的規格，可以使用磁盤編輯器進行編輯。

保存扇區：類似於文件的保存命令。文件菜單的一部分。

將所有修改寫入磁盤。請注意，根據您的更改，這可能會嚴重損壞磁盤數據的完整性。如果啟用了相應的撤消選項，則會在覆蓋之前創建相關扇區的備份。此命令僅在完整版中可用。

7.5 內存編輯器/分析

內存編輯器允許檢查實時系統中進程（即正在執行的程序）的物理 RAM/主內存和邏輯內存。進程提交的所有內存頁面都顯示在一個連續的塊中。默認情況下忽略未使用的（免費或保留）頁面，但可選擇包含並顯示為“？”人物。沒有這樣的差距，您可以將內存轉儲與文件完全相互比較（絕對地址和虛擬地址相同），例如檢查堆棧和堆狀態或觀察病毒。

如果您展開列表中列出的進程之一，您可以打開所謂的主內存或該進程的整個內存或加載的模塊 (DLL) 之一。主內存是地址範圍的較低部分，低於加載系統 DLL 的區域。

通常它還包含進程的主要模塊 (EXE 文件)、堆棧和堆。這

“整個內存”包含進程整個邏輯內存地址空間中所有分配的頁面。

使用 64 位版本的 WinHex/X-Ways Forensics，您可以在列出的 64 位進程中獲取超過 4 GB 障礙的加載模塊，並讀取和編輯此類地址範圍內的內存。內存編輯器中的進程和模塊名稱和路徑支持 Unicode。頁面邊界由水平線表示。表示相鄰分配區域之間間隙的邊界由較暗的水平線表示。Info Pane 顯示了諸如所表示的最大地址和分配間隙數（=連續分配的頁面範圍數 -1）以及當前顯示頁面的保護狀態和類型等信息。

請注意以下限制：

- 只能在 Windows XP (32 位) 下訪問物理 RAM，不超過 4 GB，並且只有管理員權限
- 注意：只能撤銷鍵盤輸入！ · 只能在就地模式下進行編輯。 · 評估版僅支持查看模式。

與內存編輯器相關的選項是“檢查虛擬內存更改”（選項|安全）和“內存編輯器中的邏輯地址”（選項|常規）。

主內存分析

需要法醫執照。當您打開本地物理 RAM（通過工具 | 打開 RAM，僅在 Windows XP 下）或將主內存轉儲作為文件打開（並完全像解釋磁盤映像一樣解釋該文件）或將內存轉儲添加到案例中時，進程將在目錄瀏覽器中列出，即使是隱藏的進程，它們的時間戳和進程 ID，以及它們各自的內存地址空間都可以在“進程”模式下單獨查看，頁面以每個進程看到的正確邏輯順序連接。“特別徹底的數據結構搜索”是基於簽名的，比拍攝標準卷快照花費的時間稍長，並且可能會發現包括 rootkit 在內的其他進程的痕跡。可以在 F-Response（工具 | 打開磁盤）的幫助下遠程獲取內存。Windows 2000、Windows XP、Windows 2003 Server、Windows Vista、Windows 2008 Server 和 Windows 7（32 位和（不太完整）64 位）的大多數（但不是全部）變體（服務包）都支持該分析。

僅支持完整的內存轉儲，其中包括 RAM 中由 BIOS 和 PCI 設備使用的區域。

Windows 內核數據結構和命名對像在“對象”下的捲快照中的樹中方便地列出。加載的模塊列在“模塊”下。這使得 X-Ways Forensics 能夠以 RAM 模式分配它們佔用的內存頁面，並為它們計算哈希值，以便可以通過特殊的哈希集來識別它們。出於散列目的，建議僅列出加載模塊的不變標頭（請參閱卷快照選項）。

技術細節報告通知您重要的系統範圍參數以及重要內核數據結構和加載的內核模塊的當前地址。在 Details 模式下可以找到每個進程的進程相關數據結構的地址和進程的 ID。

父進程。在 RAM 模式下，信息窗格會為每個內存頁顯示一個分配給它的進程（如果有的話）及其內存管理狀態。

通過適當的背景知識，可以使用此功能了解有關機器及其進程、套接字、打開的文件、加載的驅動程序和附加媒體的當前狀態的更多信息，以識別惡意軟件、查找加密數據的解密版本、分析事件響應中的網絡痕跡，並在內存取證領域做進一步的研究。

7.6 模板編輯

模板是一個對話框，它提供了以比原始十六進制編輯更舒適和更能防止錯誤的方式編輯自定義數據結構的方法。編輯是在單獨的編輯框中完成的。按下ENTER鍵或在收到提示後退出模板時更改生效。數據可能來自文件、磁盤扇區或虛擬內存。

特別是在編輯數據庫時，您可能更願意定義自定義模板以便於訪問記錄。您將在系統菜單中找到打印模板的命令。

模板定義存儲在擴展名為.tpl 的文本文件中。模板編輯器使您能夠編寫模板定義並提供語法檢查。模板定義主要包含變量聲明，類似於編程語言源代碼中的變量聲明。

語法在附錄 A 中有詳細解釋。支持的數據類型包括所有常見的整數、浮點和布爾變體、日期類型、十六進制值、二進制、字符和字符串類型。可以使用單個變量和變量組的數組。

在數據中自由向前和向後移動的能力使得使用模板特別靈活：· 可以用多種方式解釋和操作相同的變量。· 可以跳過不相關的數據部分。

模板管理器列出了 WinHex 目錄中包含模板定義的所有文本文件。顯示模板的標題以及描述、文件名以及上次修改的日期和時間。單擊“應用”按鈕可在當前編輯器窗口的當前位置顯示使用為數據選擇的模板定義的模板。您還可以創建新的模板定義、刪除或編輯現有模板定義。

WinHex 附帶了幾個示例模板。

8 數據恢復

8.1 使用目錄瀏覽器恢復文件

最明顯的是，目錄瀏覽器中列出的已刪除文件和目錄可以

使用目錄瀏覽器的上下文菜單輕鬆且有選擇地恢復。您導航到一個目錄（或遞歸地瀏覽根目錄），選擇要恢復的文件，然後使用上下文菜單中的恢復/複製命令。請參閱“目錄瀏覽器”一章。理想情況下，您首先優化卷快照，以便在目錄瀏覽器中找到並列出更多以前存在的文件。

8.2 按類型/文件頭簽名搜索恢復文件

磁盤工具菜單中的數據恢復功能，以及作為優化卷快照命令的一部分查找以前存在的文件的策略。這種恢復方法也稱為“文件雕刻”。它搜索可以通過特徵文件頭簽名（特定字節值序列）識別的文件。由於這種方法，文件雕刻不依賴於功能文件系統結構的存在。

按類型恢復文件：根據文件頭簽名找到的文件被雕刻並存儲在您在自己的驅動器之一上指定的輸出文件夾中。可以選擇將每種類型的恢復文件放入它們自己的子文件夾中（...\\JPEG、...\\HTML 等）。文件的假定內容實際上被複製了。

文件頭簽名搜索：根據文件頭簽名找到的文件不會存儲在任何地方，而只是列在卷快照的專用虛擬目錄中。僅存儲對文件的引用，具有人工生成的名稱（基於遞增數字或起始扇區編號）、假定大小、起始偏移量。當需要查看/複製文件時，文件內容從原始磁盤/圖像中即時讀取。或者，您可以將文件從單獨的文件頭簽名搜索操作輸出到單獨的子目錄中，以便在需要時更容易區分它們。

請注意，文件雕刻通常假定連續的文件簇，因此它會產生損壞的文件，以防文件最初以碎片化的方式存儲。存在以下例外情況：如果在具有 Ext2/Ext3 以外的受支持文件系統的卷中進行文件頭簽名搜索，在集群邊界的可用空間中找到文件的開頭，則默認情況下假定數據在可能跟隨的集群周圍流動被文件系統標記為正在使用。這將正確地重建在其他文件之後創建並存儲在其他文件周圍然後刪除的文件，只要釋放的集群之後沒有被重新使用和覆蓋。為了防止以這種方式純粹在空閒空間中雕刻文件，即假定連續的集群，您可以取消選擇“在已用集群周圍的空閒集群中雕刻文件”選項。例如，考慮分區中的 9 個連續簇：f1 f2 f3 u1 u2 u3 f4 f5 f6。這些是 3 個空閒簇，然後是 3 個已用簇，然後是 3 個空閒簇。在使用過的簇“周圍”的純自由空間中雕刻可以為您提供一個由 f1 f2 f3 f4 f5 f6 組成的文件。如果沒有“around”選項，您可以獲得包含 f1 f2 f3 u1 u2 u3 的雕刻文件。

“Ext2/Ext3 塊邏輯”選項導致此恢復方法也偏離了沒有碎片的標準假設，因為它將遵循典型的 Ext 塊模式，例如文件頭的第 13 個塊被認為是一個引用以下數據塊的間接塊。當應用於 WinHex 知道具有 Ext2 和 Ext3 以外的文件系統的分區時，或者當發現標頭不是塊對齊時，此選項無效。

有關所選參數和恢復結果的日誌文件“按 Type.log 恢復文件”將寫入輸出文件夾以進行驗證。

您可以通過單擊適當的按鈕來展開或折疊此對話窗口中的整個文件類型樹。這很有用，因為展開時您只需鍵入文件類型描述的前幾個字符即可自動跳轉到樹中的第一個匹配項目。

由於不使用可能存在的（一致或損壞的）文件系統，因此原始文件大小對於此恢復方法來說基本上是未知的，原始文件名也是如此。這就是為什麼生成的文件大多根據以下模式一般命名：Prefix#####.ext。“前綴”是您提供的可選前綴。#####是每個證據對象的遞增數字。“ext”是根據文件類型定義對應於文件頭簽名的文件擴展名。輸出文件名前綴可以選擇包含佔位符“%d”，它將被驅動器名稱替換。如果您一次將文件恢復按類型應用於多個驅動器並希望能夠輕鬆區分來自不同驅動器的文件，這將很有用。

使用專業許可證或更高版本，“智能命名”選項將使 Exif JPEG 文件以創建它們的數碼相機型號及其內部時間戳（如果可用）命名。許多 Windows 註冊表配置單元文件都有其原始名稱，還有一些 JPEG 文件，其元數據中 Photoshop 嵌入了一個名稱。沒有已知名稱和 Exif 元數據但由已知庫創建的 JPEG 文件在括號中的人工名稱中接收一些附加信息（請參閱生成器簽名）。Thumbs.db 文件始終命名為 thumbs.db，index.dat 始終命名為 index.dat。上述前綴不與原始文件名一起使用。

各種算法在內部工作，試圖確定許多不同類型文件的原始大小（其中包括 JPEG、GIF、PNG、BMP、TIFF、Nikon NEF、Canon CR2 raw、PSD、CDR、AVI、WAV、MOV、MPEG、MP3、MP4、3GP、M4V、M4A、ASF、WMV、WMA、ZIP、GZIP、RAR、7Z、TAR、MS Word、MS Excel、MS PowerPoint、RTF、PDF、HTML、XML、XSD、DTD、PST、DBX、AOL PFC、Windows Registry、index.dat、Prefetch、SPL、EVTX、EML）通過檢查它們的數據結構。這適用於在頁腳列中具有“~”的文件類型定義數據庫中的條目。不應更改這些條目以使大小和類型檢測適用於這些文件類型。或者，頁腳簽名也可以幫助找到文件的結尾。對於既不存在內部算法也不存在頁腳簽名定義的文件，或者可用內部算法不知道其原始大小且實際上未找到頁腳簽名的文件，將以文件類型定義數據庫中指定的默認大小恢復字節。指定這樣的大小時要大方一些，因為恢復的“太大”的文件仍然可以通過其關聯的應用程序打開，而過早截斷的文件通常不能打開，因為它們不完整。通過搜索頁腳來檢測某些類型文件的原始大小的嘗試受到大小檢測限制的限制，該限制也可以在數據庫中指定，在默認大小和正斜杠之後。這樣的限制是必要的，以避免在整個卷中搜索給定文件的頁腳，如果卷很大，這將非常耗時。此外，如果不在頁眉附近，則越來越不可能找到正確的頁腳，即使發現相距很遠，這樣的文件也可能是碎片化或部分覆蓋等。標準默認大小（如果未指定）是 1MB。標準最大大小（如果未指定）是默認文件大小的 64 倍。

文件頭通常位於簇邊界處，因為這是文件系統通常放置文件開頭的地方。但是，搜索扇區對齊的文件頭會更徹底（而且不會更慢），因為這樣還可以從具有不同簇佈局的先前存在的分區中查找文件，因此在扇區邊界處搜索是默認行為。如果在沒有定義簇佈局的物理介質或原始文件上執行，WinHex 無論如何都必須在扇區邊界進行搜索。還有另一種可能性，即徹底的字節級搜索。當您嘗試查找在任何扇區邊界處不可靠對齊的文件（例如備份文件或磁帶圖像中的文件或嵌入其他文件中的文件）或嘗試查找條目/記錄/微格式/內存工作等時，這是必需的，即不完整的普通文件。然而，這是以可能增加誤報數量為代價的，錯誤識別的文件簽名隨機出現在媒體上，並不表示文件的開頭。文件類型定義數據庫中的各個標誌可以幫助在每個文件類型的基礎上決定要搜索哪些文件的簇、扇區或字節邊界。

卷快照已知的文件的起始扇區總是從文件雕刻中排除是可選的。當然，X-Ways Forensics 通常仍會嘗試防止重複，但如果文件頭簽名定義或內部文件大小檢測足夠強大，表明已知已刪除的文件已被新文件覆蓋，則該新文件將被刪除儘管它與已知文件共享相同的起始扇區，但仍被雕刻。另一個例外是完全未初始化文件的第一個扇區（有效數據長度 = 0）不會從文件頭簽名搜索中省略。

如果您故意中止文件頭簽名搜索或者如果文件頭簽名搜索導致 X-Ways Forensics 崩潰，下次當您在同一證據對像中開始文件頭簽名搜索時，您會發現一個選項可以在正確的位置恢復它被中斷，或者在崩潰發生之前最後一次保存卷快照時的位置（取決於案例的自動保存間隔）。

如有必要，您可以將恢復範圍限制為當前選定的塊和/或分配或未分配的空間（邏輯驅動器或卷上可用的選項）。例如，為了恢復已刪除的文件，您選擇僅從未分配的空間中恢復。由於文件系統錯誤而無法再訪問的文件可能仍存儲在被視為正在使用的簇中。

在許多情況下，NTFS 壓縮對文件數據的影響可以選擇在文件頭簽名搜索（僅限取證許可）中進行補償。如果找到 NTFS 壓縮文件的簽名，該文件將被標記為已壓縮，並在需要時嘗試使用複雜的算法“即時”解壓縮文件，該算法甚至可以解壓縮包含多個壓縮文件的文件單位。

8.3 文件類型定義

“文件類型簽名 *.txt”是製表符分隔的文本文件，用作文件類型定義數據庫，用於優化卷快照和文件恢復類型命令。

WinHex 自帶各種預設文件類型簽名。您可以完全自定義文件類型定義並添加您自己的定義，無論是在“File Type Signatures Search.txt”還是在名為“File Type Signatures *.txt”的任何其他此類文件中，這些文件也將被加載並且可能有一個好處，即如果它們與其中一個默認文件的名稱不同，則在您安裝下一個更新時它們不會被覆蓋。只有當文件名包含“搜索”一詞時，文件類型才可用於文件頭簽名搜索。否則，它們僅用於驗證已經是卷快照一部分的文件的文件類型（僅限取證許可證）。總共支持最多 4096 個條目（1024 個用於搜索）。

當您單擊自定義按鈕編輯文件“File Type Signatures Search.txt”時，默認情況下 WinHex 在 MS Excel 中打開該文件。這很方便，因為文件由製表符分隔的列組成。如果您使用文本編輯器編輯文件，請務必保留這些選項卡，因為 WinHex 依靠它們的存在來正確解釋文件類型定義。MS Excel 會自動保留它們。編輯文件類型定義後，您需要退出對話窗口並再次調用“按類型恢復文件”或“優化卷快照”菜單命令以查看文件類型列表中的更改。

第一列：文件類型

文件類型的人類可讀名稱，例如“JPEG”。忽略前 19 個字符以外的所有內容。

第二列：擴展

通常用於此文件類型的一個或多個文件類型擴展名。例如“jpg ;jpeg ;jpe”。首先指定最常見的擴展名，因為默認情況下將使用該擴展名來命名恢復的文件。

如果第一個擴展名以大寫字符指定，文件類型驗證將使用它來填充文件的類型列，即使該文件具有可選的合理文件擴展名之一。支持超過 255 個字符。

第三列：標題

可以識別此文件類型的文件的唯一標頭簽名。它被指定為正則表達式（有關解釋，請參閱搜索選項），因此可以匹配可變字節值（例如`\xE1\xE2`表示“字節值可以是 0xE1 或 0xE2”）或未定義的區域（.）表示簽名的最大長度為 48 字節。要首先找出特徵文件頭簽名，請在 WinHex 中打開幾個特定類型的現有文件，並在文件開頭附近以相同的偏移量查找常見的字節值。

第四列：偏移量

文件中發生簽名的相對偏移量。通常只是 0。簽名必須包含在前 512 個字節中。

第五列：頁腳

可選的。可靠地指示文件結尾的簽名（字節序列）。指定為正則表達式。表示可變大小數據的正則表達式可能無法像

預期的。頁腳簽名可能有助於以正確的文件大小實現恢復。恢復算法不會搜索頁腳超過指定為最大文件大小的字節數，從標題開始。

比頁腳更好的是 X Ways Forensics 內部實現的算法的潛在可用性，該算法非常了解文件格式，並且如果文件沒有碎片、不完整或損壞，通常可以找出正確的文件大小。這種算法在頁腳列中用波浪號 (~) 和算法 ID 號表示。

第 6 列 :默認大小

可選的。1 或 2 個值。如果有 2 個值，則第二個是文件類型特定的大小檢測限制，並用正斜杠與默認大小分隔。

第七列 :標誌

可選的。可以為某些文件類型進一步定製文件雕刻，並且是 X-Ways Forensics 中文件雕刻的複雜性和強大程度的另一個指標。

A :意味著一個定義在很大程度上取決於相關算法（用 ~ 字符定義的算法）並且如果沒有它就太通用而無法識別。

b（小寫）：如果給出選擇，將在字節級別搜索簽名。對於通常不在任何扇區或簇邊界對齊的條目/記錄/微格式/內存工件（即不完整的普通文件）尤其有用。

B（大寫）：為了性能，防止對該特定簽名進行字節級搜索
原因。

c（小寫）：如果考慮在內（取決於用戶界面設置），則忽略未在簇邊界對齊的標頭簽名。對某些文件類型很有用，可以避免許多誤報。

C（大寫）：表示文件類型簽名。如果啟用了 NTFS 壓縮補償，則不應將其用於搜索 NTFS 壓縮文件，因為它們太弱，會產生太多誤報，或者無論如何都不會實際存儲為壓縮文件。

d（小寫，表示“直接”）：簽名將按字面解釋，而不是正則表達式，逐個字符，根據 Windows 系統中的活動代碼頁使用字節值。例如，如果您不是很熟悉正則表達式或不需要它們並且只想根據 Windows 系統中活動的代碼頁按字面解釋所有字符，而不考慮這些字符是否被認為是特殊字符，則很有用正則表達式中的字符。例如，<?xml version= 1是某些 XML 文件的有效簽名，但它僅適用於直接標誌，因為問號具有特殊含義。如果整個表達式被解釋為正則表達式，如果正則表達式解釋處於活動狀態，則不會產生任何匹配項。

e :代表“嵌入式”。如果文件類型在頁腳列中具有波浪號 (~) 算法並標有此標誌，則在卷快照細化期間，將預先選擇它以搜索某些其他文件中的嵌入數據，在“所有文件頭簽名搜索”中上面未處理的文件”部分。“e”標誌僅有助於初始化此選項的刻度線。

最後，用戶可以在用戶界面中更改為該操作選擇的文件類型。

此外，標有“e”標誌的類型將被搜索嵌入在不存在內部提取算法的類型文件中。

E :切勿在其他文件中雕刻為嵌入文件。

f (小寫) :表示指定的頁腳簽名用於查找不再屬於文件且應排除的數據。普通頁腳包含在雕刻文件中。對於沒有明確定義的頁腳的文件格式很有用，在這種情況下，可以通過不再屬於文件的數據的出現來檢測文件的結尾。這可能是與標頭相同的簽名（如果該類型的文件通常成組出現，背靠背）或只是 \x00（對於文件格式，例如不包含零值字節的文本文件，但是 \x00 可以預計在 RAM 鬆弛中很有可能）。這樣的頁腳簽名應該被標記為獨占的，因為它匹配的數據不是文件本身的一部分。

F (大寫) :如果在定義中指定了頁腳簽名，則如果找不到相應的頁腳，則使 X-Ways Forensics 放棄文件頭簽名搜索的命中。

可用於減少或完全避免誤報的數量。

G :代表“貪婪”。貪婪地排他性地分配所有扇區。文件類型簽名搜索僅在此類文件的假定結尾之後繼續搜索其他文件頭。如果可以使用內部實現的算法確保雕刻文件包含所有有效數據，則可能很有用，這樣就不必在先前雕刻文件的邊界內搜索其他文件。僅當在扇區邊界處找到文件頭簽名時，該標誌才有效。如果空閒空間中的文件圍繞分配的簇進行分割，則在搜索進一步的文件頭簽名時，只會跳過文件的第一個片段。

g (小寫) :同一標誌的較弱版本。僅當文件類型存在內部文件大小檢測算法並且具有相同起始扇區號的文件已存在且檢測到的文件大小相同時，“g”標誌將導致 X-Ways Forensics 跳過受影響的扇區。這有助於防止 zip 文件重疊，從而避免可能包含許多重複文件。

h :表示指定的頭簽名用於查找不屬於文件本身的數據。

這意味著標頭簽名將從雕刻文件中排除。雕刻的文件將在標題簽名之後開始。此外，此標誌可防止在為此類文件分配的簇周圍的可用空間中進行文件雕刻。

H :該定義僅用於簽名高亮功能，不適用於常規文件頭簽名搜索或文件類型驗證。這樣的定義只需要三個信息：關鍵字或正則表達式、相對偏移量（通常為 0）和標誌“H”。

行首的描述是可選的，但建議使用，因為顏色取決於描述，對於不同的描述，您可能會看到不同的顏色。您甚至可以創建一個專用的文本文件，例如名為“File Type Signatures Search Highlighting.txt”的文件，

它定義了您一直感興趣的各種關鍵字或正則表達式，並且希望在每種情況下立即突出顯示，甚至在運行適當的搜索之前。如果您分析或逆向工程文件格式也很有用，例如記錄沒有固定長度（因此 WinHex 中的記錄顯示選項不適用），但可以通過簽名識別。

L :標識僅鏈接到其他定義的鏈接。例如，有一個 OpenOffice 文件的條目很有用，一些用戶錯過了這個條目，如果沒有這個條目，可能會導致誤認為無法雕刻 OpenOffice 文件。如果選擇 OpenOffice 的條目進行雕刻，這會在內部自動選擇 zip 存檔進行雕刻，這是合理的，因為 OpenOffice 文件在技術上是 zip 文件並且可以這樣雕刻。缺點只是其他非 OpenOffice 文件的 zip 壓縮包也被壓縮。

但是，由於內部文件類型檢測，例如基於自動分配的文件擴展名，這些文件將是可區分的。

S :標記足以用於文件頭簽名搜索的簽名（可能與雕刻算法結合使用），但由於偶爾的錯誤識別而不適用於文件類型驗證。這個標誌應該很少需要。

t :防止 X-Ways Forensics 立即顯示已確認的雕刻文件類型。

例如，對於 XML 等文件格式系列很有用，可以在稍後的文件類型驗證期間確定確切的子類型。

u（小寫）：代表“未使用”。允許僅在根據文件系統空閒的集群中雕刻文件。

U（大寫）：允許僅在根據文件系統空閒且卷快照中包含的先前存在的文件未使用的集群中雕刻文件。

W（大寫）：標識太弱而不能新檢測文件類型的標頭簽名，僅用於確認文件擴展名所建議的類型。

x :標識實際文件擴展名不是該文件類型標準擴展名的比較正常的文件類型，這樣這些類型的文件在文件類型驗證後不會被高亮為“檢測到不匹配”，而只是呈現為“新識別”，以免引起對這些文件應有的更多關注。

y :標識已在內部使用加密的文件類型，這允許在 Attr 中標記這些類型的雕刻文件。立即列為“e！”。

8.4 手動數據恢復

可以恢復丟失或邏輯刪除的文件（或更一般的‘數據’），這些文件僅在文件系統中標記為已刪除，但尚未被物理擦除（或覆蓋）。

使用磁盤編輯器打開被刪除文件所在的邏輯驅動器。原則上你可以

通過選擇分配給文件的磁盤扇區作為當前塊並使用菜單命令編輯|保存它們來重新創建這樣的文件。複製塊|進入新文件。但是可能很難找到仍然存儲文件的扇區。有兩種通用方法可以實現此目的：

1. 如果您知道要查找的文件的片段（例如 JPEG 文件標題中的特徵簽名或 MS Word 文檔中的“親愛的史密斯先生”一詞），請使用以下方法之一在磁盤上搜索它。搜索命令（例如“查找文本”或“查找十六進制值”）。這是一種非常簡單可靠的方法。
2. 如果您只知道文件名，則需要了解磁盤上的文件系統（FAT16、FAT32、NTFS 等），以查找以前的目錄條目或定義文件的其他數據結構的痕跡，從而確定編號分配給文件的第一個簇。

您可能會遇到要恢復的文件是碎片化的問題，即沒有存儲在後續的連續簇中。在 FAT 文件系統中，可以在驅動器開頭的文件分配表中查找文件的下一個簇，但是當文件被刪除時，這些信息將被刪除。

9個選項

9.1 一般選項

第一欄：

- 在 Windows Vista 及更高版本下，如果您需要對媒體進行扇區級訪問，建議始終以管理員身份運行 WinHex/X-Ways Forensics。這可以被 Windows 在 \Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers 下的配置單元 HKEY_CURRENT_USER ^這中記住，值 ~~關~~ 應移動媒體上的安裝沒有影響。
- 允許多個程序實例選項允許您一次多次執行 WinHex。如果未選中，WinHex 會將前一個實例的主窗口設為前台窗口，而不是創建新的程序實例。默認情況下，此選項處於半選中狀態。屆時，如果陷入無限循環，您還可以嘗試恢復以前的實例。例如，如果 X-Ways Forensics 在卷快照優化期間處理某個文件時進入無限循環，這可能會幫助已經運行的實例跳出該循環並繼續處理下一個文件。第二個實例還顯示了一些關於已經運行的實例目前正在做什麼的技術信息，並且即使沒有恢復假定掛起的先前實例也可以這樣做。終止先前的實例是另一種選擇，但當然應該避免，因為可能會發生數據丟失。
- 在啟動時，WinHex 可以選擇顯示啟動中心或恢復上一個窗口

安排（所有窗口及其大小和您在先前的 WinHex 會話中離開它們時的位置）。

- 默認情況下，編輯窗口不會以最大化狀態打開。
- 指定要記住並在啟動中心列出的最近打開的文檔數
(最多 255 個)。在“文件”菜單的末尾還列出了其中最多 9 個。
- 不更新文件時間意味著 WinHex 將保留最後修改時間
修改後的文件用 File | 保存保存或另存為。
- 更多上下文菜單：如果完全選中或在案例數據窗口中右鍵單擊目錄時按下 Shift 鍵，則會出現一個上下文菜單，允許遞歸瀏覽右鍵單擊的目錄（就像沒有顯示上下文菜單時一樣），允許遞歸地標記目錄（就像按下空格鍵時一樣），遞歸地展開目錄（就像按下數字鍵盤的乘法鍵時一樣），折疊所有目錄，將子樹導出到 ASCII 文本文件中，或將該目錄的整個路徑複製到剪貼板中。如果至少選中一半，或者在右鍵單擊十六進制編輯器顯示時按下 Shift 鍵，也會在那裡出現一個合適的上下文菜單。
- 您可能讓 WinHex 出現在 Windows 上下文菜單中。當用戶用鼠標右鍵單擊對象時，shell 會顯示上下文菜單。
WinHex 為文件、文件夾和磁盤提供菜單項。如果此選項未完全選中，則沒有文件菜單項。
- 一個三態復選框可以選擇性地阻止 Windows 屏幕保護程序啟動並可能要求重新輸入當前用戶的密碼，要么僅在顯示進度指示器窗口的操作期間（如果選中一半），要么通常在程序運行時（如果完全檢查）。無論主窗口是否可見或程序是否在後台運行，此選項都會產生影響。例如，在獲取您不想在成像過程中失去控制的實時系統時很有用，或者如果您希望從辦公室的另一個角落關注您自己機器上的進度指示器。
- 用戶可以在對話框窗口中為四種類型的控件項定義自己的工具提示：複選框、單選按鈕、下拉框/組合框和普通按鈕（“確定”、“取消”和“幫助”除外）。這是通過在按住 Shift 鍵的同時單擊這些項目來完成的，這對於個人筆記和想法很有用，這樣您就可以描述並更好地記住您在不同情況下的首選設置及其含義。工具提示文本將存儲在名為 Tooltips.txt 的文件中，並且可以與其他用戶共享，例如在組織內提醒您的同事根據您定義的標準應使用哪些設置。工具提示文本以 Unicode 格式存儲，最長可達 510 個字符，並且可能包含出於格式化目的的換行符。如果控件項左側有一個灰色星號，則可以判斷該控件項有一個用戶定義的工具提示。包含一個英文 Tooltips.txt 文件。如果您希望從該文件加載工具提示，請確保選中“ToolTips.txt”框。
- Save program settings in .cfg file：如果勾選一半，設置會在任何時候被保存。

程序終止（乾淨地）。如果完全選中，則每次在任何對話框窗口中單擊“確定”時（如果程序未完全終止，這可能很有用，以避免丟失最新設置）。如果完全取消選中，則程序設置根本不會保存，除非您在退出程序時按住 Shift 鍵，如果您想在 .cfg 文件中保存從那時起設置應該不再得救。

- 默認情況下，WinHex 按照物理位置的順序對磁盤分區進行編號。
- 如果啟用了自動檢測已刪除的分區，WinHex 會在打開物理硬盤時嘗試在現有分區之間的空隙中以及在最後一個分區之後的未分區空間中自動識別明顯已刪除的分區。此類額外檢測到的分區將列在“訪問”按鈕菜單中並標記為已刪除。請注意，在現有分區之間的間隙中檢測到的已刪除分區會導致分區編號發生更改。例如，如果在其之前的磁盤上檢測到已刪除的分區，則現有分區 #3 可能會變成分區 #4。
- 您可以控制開放捲是否應包括卷鬆弛，即分區中未添加到另一個集群的剩餘扇區。除了潛在的 NTFS 備份引導扇區外，該區域中的數據在邏輯上不屬於該卷，並且在創建卷之前就存儲在那裡。不需要解析文件系統或掛載卷（儘管如果不包含某些工具可能會輸出錯誤消息）。如果在使用前僅清理（擦除）卷的常規可訪問部分，而不是整個分區或物理存儲設備，則在卷映像中包含此類數據可能會造成 IT 安全漏洞。
- 如果禁用檢查剩餘扇區，WinHex 將不會在打開物理硬盤時嘗試訪問剩餘扇區。當檢測到其他扇區時，WinHex 會在您下次打開磁盤時記住它們。您可以在打開磁盤時按住 Shift 鍵來強制進行新的檢查。檢查多餘的扇區可能會導致很長的延遲、奇怪的行為，甚至會損壞某些極少數系統上的 Windows 安裝。
- 物理硬盤的替代訪問方法 1 可能允許訪問格式化為非常規扇區大小的硬盤或其他無法訪問的媒體。請注意，它可能比常規訪問方法慢。如果相當慢，WinHex 會通知您並建議恢復到標準訪問方法。

訪問方法 2 也只影響物理硬盤。這兩種替代方法都允許您指定以毫秒為單位的超時時間，超過此時間讀取嘗試將被中止。這在有壞扇區的磁盤上很有用，否則嘗試對單個扇區進行讀取訪問可能會導致數秒或數分鐘的延遲。

- 扇區讀取緩存加速磁盤編輯器的順序磁盤訪問。特別推薦在滾動 CD-ROM 和軟盤扇區時使用此選項，因為必要的物理訪問次數會顯著減少。
- 另一種選擇是始終請求用戶輸入原始圖像以確認圖像的類型（卷或磁盤）、假設的扇區大小和可能存在的路徑

額外的圖像文件段。如果在調用圖像解釋或將圖像添加到案例時按住 Shift 鍵，會發生什麼情況。如果圖像是由 X-Ways Forensics 自己創建的，通常不需要，但仍然可能使用了一些可移動媒體（USB 記憶棒和存儲卡），並在不同時間將其格式化為捲和分區媒體。在這種情況下，將其解釋為捲和分區介質可能會揭示相互重疊的不同文件系統。

專門的章節描述了不可讀扇區的替代模式。

第二欄：

- 指定要在其中創建臨時文件的文件夾。默認情況下，這是 Windows 系統中 TEMP 變量指示的目錄。您還可以指定一個點(.) 作為執行 WinHex/X-Ways Forensics 的目錄的佔位符，而不是絕對路徑。或者 .. 該目錄的父目錄。或相對於 . 或 .. 目錄（例如 .\temp 或 ..\temp）。這個概念也適用於下一個文件夾。
- 指定要在其中創建和期望圖像和備份文件(.whx)的文件夾。
- 指定在其中創建和預期案例和項目的文件夾。
- 指定存儲模板和腳本的文件夾。
- 指定用於維護內部散列數據庫和PhotoDNA 散列數據庫的文件夾。塊哈希值的哈希數據庫（如果完全使用）存儲在與第一個內部哈希數據庫相同級別的目錄中，具有相同的基本名稱加上附加的 “[塊哈希值]”。

在所有這些標準路徑中，您可以使用系統和用戶環境變量，其中變量名稱必須用百分號括起來，例如 %TEMP%。

- X-Ways Investigator [CTR]/X-Ways Imager GUI：在使用法醫許可證操作時可用。允許激活顯著減少的 X-Ways Investigator [CTR] 用戶界面，這適用於調查人員 - 專門從事某一領域，例如白領犯罪 - 他們不需要深入的計算機取證知識 - 他們不需要需要眾所周知的 WinHex 和 XWF 提供的技術見解 - 他們從精通計算機取證審查員那裡收到例如易於處理的 X-Ways 證據文件容器，其中僅包含來自各種來源的選定文件（例如“所有包含關鍵字 x 和 y”），已經過濾掉明顯不相關的內容

出去

- 需要審閱數百份電子文檔、識別相關文檔、向其添加評論、借助評論識別邏輯結構和它們之間的聯繫並打印文檔的人，只需在同一環境中單擊幾下鼠標即可完成所有這些操作，從而節省在相關應用程序中提取和加載每個文檔的時間。無論如何，他們可能需要也可能不需要在系統管理員嚴格限制的環境中工作

X-Ways Investigator 界面缺少許多高級技術選項，以方便非技術人員訪問。僅允許使用此 GUI 的 X-Ways Investigator 許可證可按要求以正常費率的 50% 提供。可選文件“investigator.ini”控制額外的簡化和管理安全預防措施，例如允許用戶只打開證據文件容器，並且只允許被歸類為

安全的。

- 自v20.0起，WinHex/X-Ways Forensics 採用了窗口文本和背景顏色的Windows 設置。在 Windows XP 的控制面板中單擊幾下鼠標即可訪問這些設置，在 Windows 7 中仍可通過個性化 | 找到它們。窗口顏色 | 高級外觀設置，在 Windows 10 中，它們仍然可以使用註冊表編輯器在這個鍵中編輯為原始 RGB 值 :HKEY_CURRENT_USER | 控制面板 | 顏色（隨後登錄和註銷）。特別是支持幾乎所有用戶界面部分（主窗口、數據窗口、案例數據窗口...）的黑色背景，這在環境光很少的環境中工作時很有用，這通常有利於思考的用戶他們可以在不太亮的屏幕上工作更長時間，這通常會減少褪黑激素產生的中斷，以及面對屏幕發出不自然光線的人的晝夜節律。查看器組件尊重大多數文檔類型的這些設置（但它不會或不能尊重它們，例如 PDF 文件）。要獲得最完整的黑屏體驗，您可以將整個 Windows 系統更改為深色主題。不僅對於“應用程序”，而且對於真正的桌面應用程序，實現這一點的最簡單方法是激活黑色高對比度主題。在 Windows 10 中，您將轉到 PC 設置 | 個性化 | 高對比度設置 | 激活高對比度 | 對比黑色。還有一個內部黑暗模式，即使沒有上述任何程序或設置也可以隨時使用，您可以在夜間或一般情況下出於健康原因或在黑暗敵對環境中進行秘密工作時吸引較少注意力時激活該模式。它不是 100% 完整的，例如它不會影響用戶界面元素，例如窗口標題、彈出菜單、滾動條、標準文件選擇窗口或日期選擇框。對於那些需要來自 Windows 的暗模式支持（見上文）。

圖形用戶界面中的各種有意義的顏色必須在 X-Ways Forensics 自己的深色模式中進行調整，或者當檢測到並採用 Windows 設置中的黑色背景顏色時，例如文件類型的顏色取決於類型狀態。在日曆中，如果背景顏色為黑色，則將活動較多的日子的灰度編碼反轉。

塊選擇、標籤標記、“已查看”、修改的字節和位置/搜索命中突出顯示的顏色首選項分別記住正常模式和暗模式。

- 與深色模式結合使用的一個單獨選項是能夠將帶有內部圖形查看庫的圖片以及畫廊中的所有縮略圖渲染得更暗。如果可以在暗模式複選框旁邊找到該複選框，選中一半，則意味著像素會變暗一點。
- 如果您選擇顯示文件圖標，存儲在文件中的圖標將顯示在信息窗格中。如果文件不包含圖標，則在“完全”選擇此選項時顯示文件類型的圖標。僅適用於使用 File | 打開的文件打開菜單命令。

- 最後同樣重要的是，您可以選擇幾種不同的對話框窗口和按鈕樣式中的一種。
- 在“Sleep(0) Frequency”子對話框窗口中，您可以通過按Shift+Ctrl+F5 指定在與其他進程競爭CPU 時間時，X-Ways Forensics 在長時間操作（例如散列、搜索）期間的行為方式。0是默認設置（不是特別配合）。您可以嘗試 10、25、50 或 100（共享 CPU 時間的最大意願）等值，例如，如果 X-Ways Forensics 由同一服務器上的不同用戶同時執行，則可以更公平地分配 CPU 時間。
- 使用取證許可證，您可以從同一網絡中的其他計算機監控冗長的操作，即查看它們是否仍在進行或已完成。您可以在用戶定義的時間間隔內通過文本文檔（可以在網絡驅動器的目錄中創建）和電子郵件啟用進度通知。如果用逗號分隔，也可以指定多個收件人電子郵件地址。正確的 SMTP 端口通常是 25，有時是 587。正確的設置由您的管理員或 Internet 提供商提供。

第三列：

- ENTER鍵可用於輸入最多四個兩位十六進制值。一個有用的例子是0x0D 0x0A，它在 Windows 世界中被解釋為行尾標記（Unix :0xD）。然後仍然可以使用SHIFT+ENTER 打開啟動中心。
- 確定是要使用TAB鍵從文本模式切換到十六進制模式，反之亦然，還是輸入TAB字符 (0x09)。在任何情況下，都可以按下 TAB+SHIFT來切換當前模式。
- 字符集值小於0x20的不可打印字符可由用戶定義的其他字符（如空格或句點）表示。該替代字符也可用於高 Unicode 值。如果不是您自己的語言的字符實際上沒有顯示，那麼在眼睛上會更容易看，而且如果您不是在尋找外語文本（例如中文、日語、韓語），您可能可以承受看不到它們的代價。要在 ANSI ASCII 和所有 UTF-16 變體中僅查看純 7 位 ASCII 字符（足以滿足英語），您可以將替換字符應用於 0x0080 以上。要查看至少來自其他西歐語言（如西班牙語、法語、德語）的字母，您可以將其應用於 > 0x00FF。要查看東歐語言，請僅將其應用於 > 0x04FF。

顯示中的字節可以一一表示為文本列中的字符，或者 WinHex 可以嘗試將它們組合起來。如果 Windows 中的活動代碼頁是雙字節字符集，則可能需要正確獲取字符（如果 2 個字節 = 1 個字符），或者由於行長度可變而不需要。這只有在 View | 時才有效字符集 | * 選擇 ASCII，因為只有這樣 Windows 中活動的代碼頁才能對顯示產生影響。

偏移量可以以十進製或十六進製表示法顯示和提示。此設置對整個程序有效。

- 使用內存編輯器時，讓 WinHex 顯示邏輯內存可能很有用

進程的地址，而不是基於零的、線性的、連續計數的偏移量。這始終以十六進製表示法完成。Goto Offset 命令的對話窗口也會提示輸入邏輯地址。

- 可能會顯示頁面和扇區分隔符。如果此選項部分啟用，則僅扇區顯示分隔符。

- 在編輯窗口中指定每行的字節數。常用值為 16 或 32
(取決於屏幕分辨率)。

- 選擇組中應顯示的字節數。2 的幕最適合大多數人目的。

- 有一個選項可以定義十六進制編輯器顯示中行之間額外間隙的大小（以像素為單位），它與所選字體的官方高度一起定義了行之間的距離。默認值在 v17.2 之前一直是 3，現在可以調低，同時顯示更多的行，看到更多的數據。例如，對於 Courier 字體，顯示看起來仍然很好，額外的間隙為 1，但是您看到的數據多了 15%（基於字體大小 10）。甚至負值也是可能的。使用 -1，您可能會看到比以前多 35% 的數據。

- 文件模式下的搜索命中突出顯示：選項可以同時在文件模式下突出顯示文件中的所有搜索命中，或者僅在顯示搜索命中列表時（如果選中一半），或者一旦加載搜索命中後永久顯示證據對象，即即使在使用普通目錄瀏覽器時（如果完全選中）。打開證據對像後，一旦列出搜索結果，就會加載搜索結果。此功能也適用於用戶搜索命中。需要法醫執照。

- 自動著色：1) 當光標位於 NTFS 文件系統的 FILE 記錄中時，突出顯示該記錄中的各種元素，以方便導航和理解。需要專家或法醫執照。如果選中一半，則只會在 NTFS 格式的捲上突出顯示，而不會在其他文件系統和物理分區磁盤上突出顯示。

- 2) 在磁盤/分區/捲和文件模式下突出顯示 FILETIME 值。在手動檢查各種 Microsoft 格式的文件時很有用，這些文件可能包含比自動提取更多的時間戳（例如嘗試使用 index.dat、註冊表配置單元、.lnk 快捷方式文件等）。如果數據窗口的下半部分有焦點並且 FILETIME 值突出顯示，您還可以將鼠標光標懸停在這樣的值上以獲得時間戳的人類可讀解釋。或者，當然，如果您單擊該值的第一個字節，您可以從數據解釋器中獲取它。如果選中一半，則僅突出顯示以 4 字節偏移量對齊的 FILETIME 值。

- 3) X-Ways Forensics 和 WinHex Lab Edition：在十六進制顯示中突出顯示文件頭簽名（X-Ways Forensics：磁盤/分區/捲和文件模式）。識別是通過將“文件頭簽名搜索 *.txt”中的簽名定義與當前可見頁面中的每個偏移量進行匹配來完成的。“~”算符的增強效果，

通常可以在文件頭簽名搜索期間識別誤報或進一步區分不同的子類型，但不適用。這種突出顯示將幫助您立即發現眾所周知的數據/文件類型的起始位置，即使它們相互嵌入，例如 JPEG 文件中的縮略圖、zip 存檔中的單個記錄、Exif 元數據中的 TIFF 簽名、Windows 註冊表中的證書 hives 等。更多信息請參考簽名定義文件的 H 標誌的文檔。如果選中一半，則僅突出顯示對齊到 512 字節邊界的簽名。

· 突出顯示可用空間/空閒空間：以較柔和的顏色（分別為淺藍色和灰色）顯示偏移量和數據。有助於輕鬆識別這些特殊驅動器區域。至少需要專業執照。

- 選擇一種顏色用作當前塊的背景。您只能在以下情況下更改顏色
“使用 Windows 默認顏色”選項已關閉。

· 如果啟用了記錄顯示，請選擇一種顏色用作每個其他固定長度記錄的背景（請參閱“位置”菜單）。

· 為新創建的註釋/位置/書籤選擇默認顏色。

- 您可能希望 WinHex 突出顯示修改的字節，即以不同的顏色顯示文件、磁盤或內存的更改部分，以便您可以區分原始數據和到目前為止所做的更改。您可以選擇 hilite 顏色。

· 選擇空閒空間和未初始化空間的顏色。

- 您可以為十六進制編輯器顯示選擇一種字體，並決定標準 Windows GUI 字體是否應用於 WinHex/X-Ways Forensics GUI 的其他部分（通過附加複選框）。

符號選項

- 選擇您喜歡的日期、時間和數字符號設置。如果您在非您自己的計算機上使用 X-Ways Forensics，這對於獨立於您要預覽的實時系統的 Windows 區域設置尤其重要。您也可以選擇僅用 2 位數字顯示年份。

· 有一個選項可以在目錄瀏覽器和用戶界面的其他部分以更好、更長和更特定於區域設置的表示法輸出日期，其中可以包括工作日和基於您的語言的月份名稱或英語。此外，該格式支持 Unicode，例如可以使用原始的中文日期表示法。請參閱 <http://msdn.microsoft.com/en-us/library/dd317787%28v=vs.85%29.aspx> 以獲得可能的表示法的完整說明。如何表示月份的示例（英文）：MMMM = April，MMM = Apr，MM = 04，M = 4。完整格式示例：d/MMM/yyyy (ddd) = 2/Apr/2014 (Wed)。

- 可以選擇以毫秒或更高的精度顯示時間戳。你可以

輸入所需的小數位數。效果取決於原始時間戳格式的可用精度以及時間戳的存儲位置。（卷快照中的時間戳最多顯示 4 位小數，其中第 4 位四捨五入。）可用的更高精度用於排序目的，即使不顯示也是如此。所有這些都非常有用，例如對於像 NTFS 這樣的文件系統，它在所有或某些時間戳中提供非常高的精度。

- 可選地，實際使用的時區轉換偏差（包括適當的夏令時）可以直接顯示在目錄瀏覽器的時間戳列中。
- 文件大小可以選擇始終以字節顯示而不是四捨五入。如果該複選框被選中一半，則僅適用於卷中的項目，否則也適用於物理分區媒體上的項目。
- SHA-1 和 TTH192 散列可以選擇以 Base32 表示法顯示在目錄中
瀏覽器，在 P2P 程序中很常見。
- 如果您願意，可以在描述列中顯示一些“內部”標誌。那些旗幟在卷快照優化中識別文件的狀態。
 [Emb] :檢查嵌入數據以發現 [Arc] :檢查文件存檔的內容 [Enc] :已執行加密測試 [Ext] :檢查電子郵件或電子郵件存檔的可提取內容 [Met] :檢查內部元數據 [Xtn] :由 X-Tension 創建

使用幫助菜單的初始化命令可以恢復所有選項的出廠設置。

9.2 目錄瀏覽器

在目錄瀏覽器中對文件和目錄進行分組是可選的。X-Ways Forensics 分別記住排序標準和此選項：1) 卷的普通目錄瀏覽器，2) 分區磁盤的普通目錄瀏覽器，3) 搜索命中列表和 4) 事件列表。默認情況下，此框是半選中的，這意味著分組僅在不遞歸探索時發生，即僅當目錄需要導航並因此在列表頂部有幫助/預期時才發生。

在目錄瀏覽器中對現有和刪除的項目進行分組是可選的。如何使用此功能有兩種可能性。可能可恢復（問號圖標）和已知不可恢復（紅色 X 圖標）的先前存在的文件也在內部分組（因此總共將有三組）或不分組（只有 2 組）。帶有一個或兩個水平分隔符的小符號表示列表是否分為兩組或三組，也在作為主要排序標準的列的標題中，作為一個小提示，當在目錄瀏覽器中滾動並觀看時例如，對於某個基於其名稱的文件，您需要簽入每個組，因為排序發生在每個組內，而不是跨組。

·雙擊一個目錄將瀏覽它。雙擊普通文件將查看它。此選項控制是否通常通過雙擊查看或瀏覽具有子對象的文件。如果復選框被選中一半，系統將提示您。

·可以選擇打開和搜索文件，包括它們的空閒時間。此復選框的中間狀態僅對邏輯搜索有影響（參見該主題）。

·當在卷內從一個目錄導航到另一個目錄時，可以選擇在目錄瀏覽器的頂部列出“..”項目。如果顯示，它會凍結在頂部並且不會與所有其他項目一起滾動。它顯示了它所代表的目錄（如果雙擊它就會導航到的目錄）的所有信息，就像目錄瀏覽器中的所有其他項目一樣。一個“..” item 也可以選擇顯示，代表當前探索的目錄。例如，如果您希望在查看其子對象的元數據的同時查看父對象的某些元數據（例如時間戳），則很有用。如果 .. item 是一個文件，您選擇它，然後您可以在文件、預覽或詳細信息模式下看到該特定文件。

它以畫廊模式表示。

·在目錄瀏覽器中列出卷的根目錄，在根目錄本身中，實際上有點不合邏輯，但可以非常有助於查看該目錄的時間戳（如果有的話，取決於文件系統）或快速導航到它的集群（如果有的話，也取決於文件系統）或作為另一個地方快速標記或取消標記卷中的所有項目。

·在普通目錄瀏覽器中列出文件系統的內部文件是可選的。例如，這會影響 NTFS 中的各種 \$* 文件。特別是在 X-Ways Investigator 中，這些文件不再列出，因為它們與非技術審查員（X-Ways Investigator 的目標群體）無關，並且可能會使他們感到困惑，因為他們不熟悉使用普通高級計算機軟件。

·如果多個過濾器處於活動狀態，它們通常是 ANDed，這意味著每個文件必須通過第一個活動過濾器以及目錄瀏覽器中列出的所有其他活動過濾器。但是，您也可以使用邏輯 OR 過濾文件，這意味著將列出通過第一個活動過濾器或任何其他活動過濾器的任何文件。如果活動過濾器與邏輯 OR 組合，則會顯示在活動過濾器計數旁邊的目錄瀏覽器標題行中。單擊過濾器計數或單詞 OR 可在 AND 和 OR 組合之間切換。如果多個過濾器與 OR 組合，則描述過濾器仍然可以選擇進行 AND 運算，並且默認情況下為 AND 運算，正如您可以從描述過濾器對話框窗口中標記為 AND 的附加複選框中看出的那樣，在這種情況下可見，然後該過濾器分別計算和處理。請注意，使用多個 .settings 文件可以實現帶有 OR 和 AND 的複雜嵌套過濾器設置。

·過濾器也應用於目錄，這是可選的。如果激活，則只涉及合適的過濾器。不適用對目錄沒有意義的過濾器（類型、類型狀態、哈希、哈希集、作者……）。

·在遞歸探索時列出子目錄是可選的。如果已經列出了所有子目錄中的所有文件，則導航不需要它們，並且當您僅對查看文件感興趣時可能會分散您的注意力。默認情況下，此選項處於半選中狀態。這意味著

導航不需要目錄，並且僅當它們與實際適用於目錄的任何活動過濾器（名稱、時間戳過濾器、所有者、Int.ID、屬性...）匹配時才會列出。例如，如果 Name 過濾器和 Type 過濾器同時處於活動狀態，則不會列出目錄，因為即使它們滿足 Name 過濾器，它們也不可能滿足 Type 過濾器（目錄沒有文件類型）。但是，如果啟用了名稱過濾器和時間戳過濾器，則如果目錄與兩個過濾器條件都匹配，則會列出這些目錄。

選擇統計顯示在目錄瀏覽器下方（僅限取證許可證）。如果以遞歸方式計算，當您在目錄瀏覽器中選擇一個目錄（或包含子對象的文件）時，它們會顯示有多少子目錄、文件和多少數據，除非您已經遞歸探索，採取任何主動過濾器考慮在內。如果未啟用此選項，則統計信息只會告訴您目錄瀏覽器中的直接選擇，而不是可能間接選擇的子對象。如果此選項被選中一半，統計將考慮目錄的子對象，但不考慮文件的子對象。

可以遞歸或非遞歸地在目錄瀏覽器中標記或排除項目。非遞歸意味著在目錄瀏覽器中標記/取消標記/排除/包含文件或目錄對父對像或子對像或父目錄或子目錄沒有影響。例如，如果文件的所有子對像都應在卷快照優化中處理或搜索，而不是父對象，則很有用。如果它遞歸地工作，那麼不可能有一個未標記的父對象，其子對像都被標記了。如果遞歸標記選項處於其中間狀態，這意味著子對像在新添加到卷快照時仍然從其父對象繼承標記狀態，例如，當您從標記的 e 中提取電子郵件和附件時 - 郵件存檔。是否遞歸地進行標記和排除也可以通過按住 Shift 鍵來控制。

在大容量快照中，遞歸地標記或取消標記可能非常慢。

高級排序：比高度優化的標準 Unicode 排序花費 4 到 6 倍的時間（在排序數百萬個文件時很明顯），但有幾個有用的設置和特徵：

- 語言特定的字符等價規則（對待 ß 像 ss，對待 é 類似於 e，ü 類似於 u 等）

- 語言上改進的大小寫不敏感 - 對連字符和撇號的

特殊處理（它們與其他非字母數字字符的處理方式不同，以確保諸如 “coop” 和 “co-op” 之類的詞在排序列表中保持在一起）。

- 將十進制數字視為數字，例如在 “10” 之前排序 “2”（對十六進製表示法無用，僅在 Windows 7 及更高版本下可用）

- 對待半角和全角字符相同（東亞人有時在寫英文字母時使用全角字符）

- 忽略假名類型（將相應的日語平假名和片假名字符視為相同）

高級排序取決於當前登錄用戶的區域設置。例如，如果北歐國家/地區的區域設置處於活動狀態，則 Å 位於 Z 之後，如該區域字母表中所定義，否則接近 A，這可能是非本地人所期望的。當按搜索命中列對搜索命中進行排序時，也會應用高級排序規則。

有一個選項可以按數據和上下文對搜索結果進行排序，而不僅僅是按它們所屬的搜索詞進行排序。有助於關鍵字搜索（非技術搜索，例如十六進制值搜索）。確實較慢，因為必須讀取要排序的所有搜索命中的數據和上下文並將其轉換為可比較的代碼頁。按搜索命中的數據排序有助於 RegEx 搜索。它只對匹配可變數據的正則表達式有影響，因為對於常量搜索詞，搜索詞和它們對應的搜索命中的數據是相同的。例如，在搜索帶有表達式 [a-zA-Z0-9_\.]{1,20}@{a-zA-Z0-9_\.}{2} 的電子郵件地址後，[a-zA-Z]{2,7}，按數據排序可讓您快速識別並直觀地跳過相同電子郵件地址組或查看相似電子郵件地址（以相同字符開頭）彼此相鄰。如果搜索命中數據相同，則繼續按實際搜索命中後的文本排序，會將相同或相似的文本段落並排顯示，使您可以更快地查看搜索命中列表。您可以指定要考慮排序的數據和上下文的字符數。字符越多，排序所需的內存就越多，這在列出大量搜索結果時會有所不同。

- 可選地，在啟動後，出於性能原因，目錄瀏覽器可以完全不排序。這意味著該程序將忘記上次使用的最後一個排序標準。如果選中，單擊鼠標關閉所有過濾器時現在也不會進行排序，以避免突然遞歸再次列出所有文件時出現更長的延遲。

- 目錄瀏覽器設置（特別是列寬、過濾器設置和排序順序）可以選擇存儲在案例中並在加載案例時重新激活（如果兼容版本存儲）。

- 動態電子郵件和時間戳列讓 X-Ways Forensics 決定是否在目錄瀏覽器中包含發件人和收件人列。如果目錄瀏覽器的可見部分中至少有一封提取的電子郵件消息，則它們將被包括在內，否則不會。

有用，因為當不需要專門為提取的電子郵件消息填充的列時，這會為其他列留出更多空間。具有替代時間戳的列也可以動態顯示，即僅當卷快照中具有此類時間戳的項目顯示在目錄瀏覽器的可見部分中時。

- 如果分區是從物理磁盤/磁盤映像中打開的，則第一個扇區列可以選擇顯示分區中文件的物理起始扇區號（從物理磁盤或磁盤映像開始計算）而不是邏輯起始扇區號。在這種情況下，列標籤在圓圈中包含一個 P（P 代表物理）。僅適用於普通分區，不適用於 Windows 動態卷或 LVM2 卷。

- 存在一個選項以在類型狀態列中顯示文件類型等級，這也會導致按該列排序以按這些等級排序。排名在文件類型 Categories.txt 文件中定義。

- 文件計數可以選擇顯示在目錄瀏覽器中帶有子對象的目錄和文件名稱的末尾。如果完全選中，這也會在案例數據窗口的目錄樹中發生。

- 默認情況下，路徑列在遞歸探索時顯示當前探索基地的部分路徑。這與僅複製部分路徑時使用恢復/複製命令獲得的路徑相同。例如，如果您希望與某人共享目錄列表（包括子目錄）（導出列表命令），區分不同子目錄中的文件而不透露文件的完整路徑（例如在您自己的存儲驅動器上），這很有用。如果完全選中，則部分路徑以目錄名稱開頭。

如果選中一半，則以...\\開頭，以指出遺漏。

- 帶箭頭的按鈕允許右對齊路徑列，以防您對路徑的結尾更感興趣並希望保持列寬緊湊。箭頭指向路徑將對齊的位置。
 - 一個特殊的圖片文件圖標可用，當您主要關注此類文件時非常有用。
- 根據複選框是完全選中還是半選中，進一步顯示文件狀態的問號、箭頭、剪刀、錘子等符號會額外疊加或不疊加。如果沒有，那對眼睛來說更容易。從Description一欄還是可以看出具體的刪除狀態，從圖標的對比來看，粗略的刪除/存在狀態還是很明顯的。

條件單元格背景著色有助於將您的注意力吸引到感興趣的項目上，而不必過濾掉所有不匹配的項目。通過在選定列的單元格內容中進行子字符串搜索來找到匹配項。子字符串表達式最長可達 15 個字符。您可以使用星號來匹配除空白單元格以外的任何內容。如果在單元格中檢測到匹配項，則可以僅對該特定單元格的背景著色（稱為“單元格目標著色”）或整行。要為整個列著色，而不考慮單元格內容，請為該列激活單元格目標著色並指定一個空條件字符串，即根本沒有條件。如果一個單元格滿足多個單元格目標條件或多個行目標條件，則只會應用每個組的第一個條件。如果不同的條件適用於同一單元格（一種單元格目標顏色和一種線目標顏色），則該單元格將以兩種顏色的混合顯示。對於以行為目標的著色，只能保證搜索相應單元格中的前 255 個字符。

不能為搜索命中特定列定義條件，但為事件特定列定義條件。

這在嘗試識別事件模式時很有用。例如，您可以將“程序已啟動”類型的所有事件標記為紅色，將登錄事件標記為黃色，這樣可以更輕鬆地查看它們之間的距離。如果選擇“在案例中存儲目錄瀏覽器設置”，則條件單元格背景著色是特定於案例的。顏色設置也存儲在名為“Conditional Coloring.cfg”的文件中，它們與其他目錄瀏覽器設置一起存儲在.settings 文件中並從中加載。最多可以定義 255 個條件。

“包括所有”按鈕允許撤消活動數據窗口中證據對象的捲快照中所有文件和目錄的排除。要有選擇地包含文件，請確保它們未被過濾掉。然後您可以在選擇它們後將它們包含在上下文菜單命令中。

如果不相關/不需要，還有另一個按鈕允許從卷快照中完全刪除排除的項目，特別是通過文件頭簽名找到的無意義的垃圾文件。

搜索。這將使卷快照更小，即更有效地處理，並節省主內存。如果您希望 X-Ways Forensics 通過文件頭簽名搜索再次找到某些文件，也很有用，但是例如，如果最初指定的默認文件大小不合適，則使用不同的默認文件大小列出它們。如果您在執行之前刪除搜索命中，則刪除操作會更快。作為刪除的一部分，內部 ID 被打亂，因此它們不再指示將項目添加到卷快照的順序。具有未排除子對象的已排除項不會被刪除。強烈建議在使用此功能時使用您案例的副本，例如使用“另存為”命令生成的副本。

列

目錄瀏覽器中提供了各種列。它們都是可選的。如果它們的列寬（以像素為單位）為非零，則顯示它們，如果它們的寬度為零，則隱藏它們。如果願意，您可以通過單擊對話框窗口中的列標籤來完全用鼠標切換列可見性。

可以重新定義目錄瀏覽器中列的順序。這也將更改案例報告（即報告表）、打印封面、導出文件列表和導出/複製日誌中字段的順序。您可以通過單擊其單選按鈕來選擇要重定位的列。然後使用出現在頂部的垂直滾動條。您可以通過右鍵單擊該滾動條將列順序重置為默認順序。

9.3 卷快照選項

可以通過目錄瀏覽器選項訪問這些選項。它們中的大多數在拍攝新的捲快照時生效。

- NTFS 中的擴展屬性可選擇包含在卷快照中作為它們所屬的目錄或文件的子對象，名稱為 “\$EA”並在 Attr 中標記。帶有 “(\$EA)” 的列。所有這些屬性（如果該框被完全選中）或只有非駐留屬性（如果半選中，默認）。如果完全沒有，則屬於現有對象的非常駐擴展屬性的簇將像以前一樣被虛擬文件 “misc 非常駐屬性”覆蓋。

背景信息 :Microsoft 使用系統二進製文件的擴展屬性作為安全啟動組件的一部分。在一些引人注目的案例中，攻擊者一直在使用大型擴展屬性來隱藏惡意軟件。大型擴展屬性由報告表關聯自動標記。

· 在新創建的捲快照中包括NTFS中記錄的實用程序流(LUS)是可選的。

可以包含所有LUS（如果完全選中）或僅包含非 \$EFS LUS（如果選中一半）或根本不包含 LUS。如果您對 \$TxF_DATA LUS 不感興趣，則對 Windows Vista 寫入的 NTFS 卷很有用。

- 如果它們的替代數據流 “Zone.Identifier”表示為報告表關聯而不是卷快照中的子對象，則可以方便地識別 NTFS 格式的下載文件。這意味著您不需要導航到子對象來找出

子對象可能是。“ZoneId=3”作為報告表的名稱標識從 Internet 下載的文件。

- 您可以選擇要使用的FAT12/FAT16/FAT32 文件分配表副本。這可以是用戶指定的副本，也可以是在引導扇區中定義為活動的副本（對於 FAT32）。如果用戶既沒有選擇副本，也沒有引導扇區將單個副本定義為活動副本，則將使用第一個副本，標記為“FAT 1”。在拍攝卷快照時選擇的副本將用於該卷快照的整個生命週期，即使設置已更改。它顯示在信息窗格中。技術細節報告通知哪些副本或哪些副本在文件系統中被認為是活動的。

- 默認情況下，在讀取已刪除文件的數據時會跳過FAT12、FAT16、FAT32 和exFAT 文件系統中分配的簇。這意味著刪除文件的數據不一定假定為連續的，而是假定從起始簇號開始佔用盡可能多的空閒簇以容納已知文件大小，同時跳過標記為已被現有文件使用的簇。如果以這種方式到達卷的末尾，則下一個空閒簇將從卷的開頭獲取，複製典型FAT32 文件系統驅動程序的內置邏輯，以在搜索可分配簇時在卷中循環。此選項追溯更改卷快照中已包含的文件存儲位置的假設，因此更改此選項也會導致哈希值在重新計算時發生更改。

- X-Ways Forensics 為在卷快照中正確包含 FAT32 文件系統中已刪除的對象而付出的額外努力是可選的。如果只選中一半，則僅對子目錄而不是文件進行額外的工作。

- 如果您在拍攝卷快照時在 CD/DVD 上遇到讀取錯誤（例如，由於表面划痕），您知道並非所有具有文件系統數據結構的扇區都是可讀的。除了可能存在的Joliet文件系統之外，在 CD 上列出 ISO9660 文件系統的目錄樹可能很有用，因為如果相同目錄的相應數據結構位於可讀扇區中，這意味著有第二次機會列出所有目錄和文件在ISO9660領域。

- 在 Ext 文件系統中，在初始創建卷快照期間對已刪除的目錄條目進行更深入的解析是一個選項，甚至涵蓋與現有目錄條目相關的未對齊條目。這可能會在 Ext 中找到其他以前存在的文件，同時發現一些垃圾條目的風險可能是可控的。

- 默認情況下不檢查HFS+/APFS 中EA（擴展屬性）的完整輸出。X-Ways Forensics 認為相關的所有擴展屬性仍然在元數據列中處理和輸出，如果它們本質上是文本的，或者作為駐留文件或壓縮文件的文件內容，或者作為相關目錄的鏈接，或者作為標記在屬性。帶有 (EA) 的列。如果選擇一半，“firstlink”屬性和“quarantine”屬性會額外輸出到Metadata欄中。如果完全選中新選項，即使是空的二進制 PList 和普通的“安全”屬性也會作為子對象輸出。

- Apple 文件系統中的簡單擴展屬性作為元數據列中的特殊行而不是子對象的輸出是可選的。如果包含在元數據列中，元數據字段也將以詳細信息模式顯示。
- 為了在將散列值與特殊散列集進行匹配時獲得更好的結果，在主內存分析中只能列出加載模塊的不變標頭。
- 在獲取目錄（或沒有扇區級訪問權限的整個驅動器盤符）的捲快照時，不是 X-Ways Forensics 本身解析文件系統，而是 Windows（內部稱為文件系統“OS dir list”= operating 系統支持的目錄列表），也可以包括備用數據流。如果您對 ADS 不感興趣和/或希望節省時間，可以將其關閉。
- 在將操作系統目錄列表作為證據對象處理時（當您將目錄添加到案例中時），有一個增量快照完成選項。如果選中，捲快照最初僅包含頂級目錄的內容，並且僅在需要時進一步完成，當您手動瀏覽子目錄時逐步完成。這正是 Windows 中的 Windows 資源管理器/文件資源管理器的工作方式，並且在處理需要很長時間才能完全掃描的緩慢且龐大的網絡驅動器時非常有用。但這與 X-Ways Forensics 中的常用方法有很大不同，並且顯然會阻止您在遞歸探索時獲得所有文件的完整列表，因為在您之前無法保證所有文件都已包含在捲快照中探索了所有子目錄。如果您在任何時候決定要在捲快照中遞歸地包含某個目錄的內容，您可以使用案例數據窗口上下文菜單中的“全部展開”命令（右鍵單擊該目錄）或取消選擇按需完成捲快照然後瀏覽該目錄的選項。請記住，展開整個子樹最方便的方法是單擊其根並按數字鍵盤上的乘法鍵（Windows 中的標準功能）。
- 計算在操作系統目錄列表中找到的文件中的數據總量是可選的。原始數據量與重新打開證據對象時計算出的新數據量之間的任何差異都會引起用戶的注意，並觸發拍攝新捲快照的提議。
- v18.8 及更高版本的證據文件容器特別記住它們包含的文件的捲快照優化 (RVS) 狀態，例如是否已經從視頻中捕獲了靜止圖像，或者是否已經從文件中發現了嵌入數據。

如果您選擇接受並信任此狀態，那麼如果您決定細化容器的捲快照，將不會再次處理這些文件。如果您懷疑原始審查員沒有像您那樣應用徹底的設置，或者他們可能使用了較舊、功能較差的 X 版本，您可能偶爾不想接受容器中文件的 RVS 狀態，以避免遺漏某些內容。X-Ways Forensics 處理文件。採用 RVS 狀態也是在畫廊中表示的容器中獲取視頻的必要條件，其中包含旋轉捕獲的靜止圖像。

· 繼承刪除狀態：使已刪除的分區將其刪除狀態傳遞給它們包含的所有內容（文件和目錄），並使已刪除的電子郵件存檔將其刪除狀態傳遞給所有

它們包含的電子郵件、目錄和附件。這可能看起來合乎邏輯，但會導致信息丟失，因為根據引用，所有內容都可能被列為已刪除，甚至文件系統/電子郵件存檔點的文件/電子郵件在分區時仍然存在/文件已被刪除。默認情況下，此選項未選中，因此 X-Ways Forensics 會區分現有和已刪除的文件和電子郵件等，即使是在已刪除的分區/已刪除的電子郵件存檔中，以便保留更多信息。

- 新發現的名稱（例如原始.eml 文件的電子郵件主題行或 iPhone 備份中的文件名稱）可以成為卷快照中的主要文件名（因此如果它們有子對象，也可能成為路徑的一部分），因此根據文件系統的原始名稱成為替代名稱，或者它們本身可以成為替代名稱，以較淺的顏色顯示在方括號中的主要名稱之後作為附加信息。

淨可用空間計算：允許您使用經過調整的虛擬可用空間文件，該文件不包含被識別為屬於先前存在的文件的簇，以最大限度地減少文件系統中為邏輯搜索和索引讀取兩次的空間量。更改此選項後或發現更多以前存在的文件後，虛擬可用空間文件會在下次打開時更新，例如在文件模式下選擇或在邏輯搜索期間輪到該文件時。這個虛擬文件中搜索命中的相對偏移量在它發生變化時可能會變得錯誤（例如，當更多的簇被分配給更多已識別的先前存在的文件時，因此淨可用空間文件變得更小），因此它們不能用於導航到搜索在文件模式下命中。只有在分區/卷模式下可用的搜索命中的物理偏移量才能保證保持有效。虛擬可用空間將被凍結，一旦被索引或獲得子對像後將不再更改，即通常在文件模式下手動刻入其中的文件，因為它們依賴於虛擬可用空間內不變的相對偏移量空間文件。

- 可選地，邏輯驅動器字母 A: 到 Z: 上的文件可以在操作系統的幫助下從目錄瀏覽器中打開，而不是使用扇區級別的內置邏輯。請注意，這僅適用於寫保護媒體。在可寫媒體上，Microsoft Windows 可能會更新（即更改、偽造）您打開的文件的最後訪問時間戳。然而，好處是在許多情況下，訪問此類文件的速度會明顯加快，尤其是在 CD 和 DVD 等慢速媒體上，例如，當您計算卷快照中文件的哈希值或膚色百分比時，因為 Microsoft Windows 使用讀取超前機制和娛樂文件緩存系統。另一個好處是在操作系統的幫助下打開的文件可以在 WinHex 中編輯。限制：無法以這種方式讀取多區段 CD 和 DVD 上的文件。

- 某些文件系統中文件末尾的已知未初始化部分會記住此類條件（有效數據長度 < 邏輯文件大小），由 Windows 提供給通過操作系統打開文件（並且不直接讀取文件內容）的普通應用程序來自卷的扇區）作為二進制零。這意味著實際存儲在分配的簇中並且比相應文件更早且通常與相應文件無關的數據將被忽略。

可以選擇重現 Windows 的這種行為。“將未初始化區域讀為零”是一個三態復選框。如果完全選中，它會影響除邏輯搜索、索引和搜索命中上下文預覽之外的所有讀取操作。如果選中一半，它會影響除這三個之外的所有讀取操作以及文件內容在文件模式和預覽模式下以及在

單獨的數據窗口。如果選中（完全或一半），這是一個有用的設置，可以實現與普通（用戶級）Windows 應用程序的文件哈希兼容性。如果根本不檢查，這是與普通取證工具的散列兼容性所需的設置，它會導致所有特定於文件的讀取操作返回存儲在分配的（但未初始化的）集群中的數據，這些數據來自以前的使用，例如也用於恢復/複製命令。對於下一個內部讀取操作，更改此設置即使對已經打開的文件也會立即生效。儘管 NTFS 文件系統另有說明，但卷影副本主機文件被視為其數據已初始化/有效，以避免不必要的複雜化。

- 有一個選項可以顯示新拍攝的捲快照中的碎片文件和目錄。

在證據對像中，此類項目與特殊報告表相關聯。當不使用案例時，這些項目會被部分標記。該標識可用於教育目的（查找文件系統需要記住具有特殊數據結構的非連續簇鏈的文件，並更好地理解文件系統驅動程序選擇使用哪些邏輯自由簇進行分配）或得出一些關於體積使用的粗略結論。（如果文件是在文件系統生命週期的後期創建的，那麼文件更有可能是碎片化的，此時許多其他文件已經被刪除，但許多其他文件仍然存在，從而留下分配漏洞。）

· 您可以表明您是否有興趣將文件包含在卷快照中，這些文件的集群（以及數據）完全未知，只有元數據（例如，只有文件名和路徑和/或時間戳），在 Ext*、XFS、Reiser* 中和 NTFS。如果完全選中，則所有以前存在的僅元數據已知的文件都將包含在卷快照中。如果根本不檢查，這些文件將被忽略。如果選中一半，將只包括已知名稱或時間戳以外的文件，但不包括 Ext* 或 Reiser 文件系統中的目錄條目殘餘。

· 沒有集群分配的快速快照可以加快卷快照的拍攝速度（特別是對於文件系統 Ext2、Ext3 和 ReiserFS，尤其是當卷快照文件是通過慢速 USB 1.1 接口或網絡創建時），但是，會導致 WinHex 失去分辨每個扇區和簇的分配（它用於哪個文件）的能力。您可以使用工具菜單的命令“Take New Volume Snapshot”來更新卷的視圖，例如在取消選中此選項之後。

· 啟用“保留會話之間的捲快照”選項後，WinHex（磁盤工具菜單和/或專家菜單）收集的打開卷中文件系統的所有信息都保留在臨時文件文件夾中，即使 WinHex 終止也是如此。然後 WinHex 可以在以後的會話中重用快照。無論此設置如何，案例中證據對象的捲快照始終保存在該證據對象的元數據子目錄中。

- 在內存中保留卷快照的更多數據，例如，以便按時間戳更快地排序。

· 為了加速各種操作，例如卷快照優化、邏輯搜索，尤其是搜索命中列表中圍繞搜索命中的可選動態上下文預覽呈現，X-Ways Forensics 可以在卷快照緩存中保留更多文件存檔的解壓縮內容。這通常會加速第一次打開檔案中的文件，尤其是嵌套檔案。這樣捲快照緩存可能會變得非常大。它可以

如果您願意，可以在關閉數據窗口時選擇性地丟棄（如果您暫時處理完該證據對像或完成整個案例，這很有用），這是案例屬性中的案例特定設置。丟棄後，如果/當再次打開文件時，如果該選項處於活動狀態，則可以隨時再次緩存文件。如果緩存框被選中一半，這意味著只有嵌套的檔案被緩存。

- 將某些 RTF 格式的電子郵件正文從 Outlook 電子郵件存檔轉換為純 UTF-8（提取電子郵件時）的選項，以便能夠更好地查看外部電子郵件客戶端中生成的.eml 文件，並允許替代.eml 預覽。
- 當在卷快照中包含文件存檔的內容時，擴展時間戳的替代解釋選項會產生影響。比照。“檔案探索”一章。

9.4 查看器程序和圖庫選項

您可以在此處激活單獨的查看器組件並指定其所在的路徑。

默認情況下，為了簡單起見，查看器組件的文件應從 zip 存檔中提取到運行主程序（X-Ways Forensics 或 X-Ways Investigator）的同一目錄中。如果這樣做，您只需輸入一個句點作為路徑。句點是執行主程序的目錄的佔位符。也可以是更複雜的相對路徑，例如“..\viewer”指的是安裝目錄的父目錄中名為“viewer”的目錄。當然也可以使用絕對路徑，例如“X:\Viewer854”。

查看器組件需要單獨下載，因為它不像 X-Ways Forensics 那樣頻繁更新，而且查看器組件的相同版本和副本可以由 X-Ways Forensics 的多個安裝/版本共享。絕對建議在您自己的考試機上激活查看器組件，因為特別需要它的功能來查看各種文件類型以及解碼文本以進行搜索和索引。查看器組件將其設置存儲在當前用戶的 Windows 配置文件目錄中的文件中。出於這個原因，您可能不想在不是您自己的計算機並且您希望檢查的實時系統上運行主程序時激活查看器組件，以防止對該系統進行可避免的更改。

跟蹤查看過的文件：有了取證許可，程序可以選擇跟蹤哪些文件已經被查看過，並在標籤周圍用綠色背景色直觀地標記它們。這在長時間查看數百或數千個文檔或圖片時特別有用，以避免意外多次查看相同的文檔。在全窗口或預覽模式下查看文件時，在圖庫中查看圖片時，或根據哈希數據庫將文件識別為已知良好時，文件可以自動標記為已查看。

當基於哈希值識別重複文件時，其中一個文件已被標記為已查看，則重複項也可以選擇性地標記為已查看。類似地（僅當相應的複選框被完全選中時），如果文件已被標記為具有重複項並且它們的哈希值可用，則在查看它們時，任何打開的捲中的已知重複項將同時標記為已查看，但這有可能

與畫廊一起使用時速度較慢。當查看帶有更多硬鏈接（也是重複的）的文件時，這些文件也將自動標記為已查看，但在 HFS+ 中除外。

要手動將文件標記為已查看，您可以同時按 Alt 和光標鍵。

Alt+Left 刪除標記。您還可以在目錄瀏覽器中右鍵單擊文件的標籤區域，將其標記為已查看或刪除該標記。

如果一個目錄包含的所有文件和子目錄都被標記為已查看，則該目錄被視為已查看。

如果使用內部圖形查看庫查看圖片，而不是查看器組件，則可以選擇在查看新圖片時自動關閉圖片查看器窗口（如果未選擇“同時查看多張圖片”）。在這種情況下，自動更新選項可用，允許在選擇新圖片後立即自動將下一張圖片加載到單個圖片查看器窗口中，例如通過單擊鼠標或定義報告時預覽圖片的表關聯或按其中一個箭頭鍵時。這應該主要在使用多個監視器時有用，其中圖片查看器窗口保留在第二個監視器上。如果使用內部圖形查看庫查看圖片，這將在必要時根據其 Exif 數據自動調整 JPEG 照片的方向。

在預覽模式下可以使用替代電子郵件表示（也在案例報告中）。

在預覽模式下，附件還沒有直接從這種電子郵件表示形式鏈接。

可以選擇排除電子郵件標頭（不是原始模式）。如果您想在不滾動的情況下查看更多電子郵件正文，則對標準電子郵件表示很有用。您可以在目錄瀏覽器中看到主題、發件人、收件人和日期，並且在瀏覽父.eml 文件時會列出附件。

“Clean up after GDI font object leaks”主要功能是允許對可能永久消耗GDI句柄的查看器組件進行大量操作。例如，為案例報告生成數千個 PDF 文件的縮略圖時，為了避免崩潰，該選項應該處於活動狀態。默認情況下，該複選框處於半選中狀態。全面檢查意味著更頻繁地執行手柄洩漏的必要檢查。

在預覽模式、視圖命令、圖庫中、OCR 和 Excire PhotoAI 中應用 Exif 方向元數據是可選的，由三態復選框控制。如果完全選中，則嚴格應用 Exif 方向。如果選中一半（默認），如果 X-Ways Forensics 認為不（進一步）旋轉或翻轉圖片很可能是正確的，則不會應用它。JPEG 文件中嵌入的縮略圖和低分辨率備選方案從其父文件繼承 Exif 方向。

圖庫選項

圖庫的屏幕空間得到了非常有效的利用，因為縮略圖沒有被強制為正方形。

您可以分別指定您喜歡的縮略圖寬度和高度，以像素為單位。指定的尺寸將動態調整（增加）以最好地填充可用的屏幕空間，而不會顯示部分縮略圖。由於大多數照片和幾乎所有視頻都是以橫向格式拍攝的，因此您在查看圖片時可能需要相應地選擇寬度和高度（寬度大於高度）。文檔縮略圖通常可以自由調整為任何矩形形狀，

例如那些代表文字處理文檔或電子表格，但不代表演示文稿的。對於除演示文稿以外的大多數文檔，縱向格式感覺像是一種更自然的表示方式。您指定的寬度和高度的縱橫比顯示在選項對話框中，讓您快速了解這些措施與普通照片、視頻或文檔的兼容性如何。

- 如果在用於圖庫視圖的大型（例如固態 RAR）檔案中為圖片創建縮略圖的速度太慢，您可能需要禁用它。這還將禁用存檔文件中搜索命中上下文預覽。
- 如果大型 JPEG 已經包含嵌入的縮略圖並且這些縮略圖已經包含在卷快照中，或者如果已經為大型圖片計算了內部縮略圖，則可以選擇將它們用作圖庫中的輔助縮略圖以表示主圖片。

好處是它們當然比主要的大圖片加載快得多。此外，從視頻導出的視頻靜止圖像可以用作輔助縮略圖來表示視頻，如果完全選中，甚至所有這些都可以動態旋轉。

- 畫廊有自己的“Dbl-click=View instead of Explore”三態選項，類似於目錄瀏覽器。默認情況下，雙擊表示在圖庫中查看。
- 有一個選項可以通過在圖庫中單擊而不是雙擊來查看文件。
例如，如果您希望在單獨的監視器上查看某些圖片時很有用，您不必關閉視圖窗口即可再次查看畫廊，而不是一個接一個地查看所有圖片（對於這些圖片，Page Up 或 Dn 鍵是更高效）。
- 另一個選項允許通過單擊縮略圖中的任意位置來標記文件，而不僅僅是在標記方塊中。這樣可以更方便地標記大量文件，並且比按住 Ctrl 鍵選擇多個文件更舒服。
- 圖庫可以選擇顯示查看器組件支持的任何文件類型的縮略圖，包括 Office 文檔、PDF、HTML、電子郵件和內部圖形查看庫無法顯示的圖片（例如.emf、.wmf、.jp2、...）。您可以在正常、略微縮小和強烈縮小的文檔縮略圖之間進行選擇。縮小的縮略圖顯示了原始文檔和原始佈局的更多細節，但以可讀性為代價。原始文檔中較大的字體（特別是標題）如果沒有縮小，通常在縮略圖中是可讀的，並且即使不查看它也可以讓您了解它是哪種文檔，因此您可以更快地找到您正在尋找的文件。

另外，您將能夠看到哪些文件可以用查看器組件很好地查看。當使用帶有非圖片選項的圖庫時，強烈建議在 Windows 中啟用 Aero 的情況下運行 X-Ways Forensics。

如果此框僅選中一半，則非圖片文件只有在確認其類型狀態或新識別或檢測到不匹配時才會顯示為縮略圖。這意味著包含難以理解的數據的文件更有可能被忽略，並且更有可能顯示格式正確的受支持文檔類型。出於性能原因，大於 16 MB 的文件不會用縮略圖表示。如果縮略圖的生成時間超過幾秒鐘，X-Ways Forensics 會嘗試中止縮略圖的生成。如果真實縮略圖的生成是

不成功，您可能會在縮略圖中看到一條查看器組件錯誤消息，例如以紅色小字顯示的“操作已取消”。如果 X-Ways Forensics 甚至沒有嘗試生成縮略圖，您只會看到文件名和一個圖標。

- 可以選擇在圖庫中對真彩色圖片的縮略圖進行顏色調整。此選項適用於負責審查兒童色情照片的執法用戶，以減少精神影響和壓力水平。如果完全選中此選項的複選框，則縮略圖將以灰度顯示。如果選中一半，顏色交換將以這樣一種方式進行，即人體皮膚會顯得非常不自然。
- 當使用圖庫的內部圖形顯示庫加載圖片被中止（例如，損壞或不受支持或非常大的圖片文件）時，超時（以毫秒為單位）是用戶可定義的。為圖片分析和處理以及 XWF_GetRasterImage() API 函數和報告加載圖片的超時時間是為圖庫定義的超時時間的兩倍。

用於邏輯搜索、索引和預覽模式的文本子模式的文本解碼

崩潰安全文本解碼：如果啟用，用於邏輯搜索和索引的某些文件類型的文本提取將由查看器組件在單獨的進程中完成，這樣如果查看器組件崩潰或變得不穩定，它不會呈現主進程(X-Ways Forensics) 不穩定或導致崩潰。

有一個選項可以過濾掉解碼文本中常見漢字周圍的空格。此類空格可能會意外出現，例如在處理某些 PDF 文檔時可能會阻礙中文關鍵字搜索。

用於上下文預覽的緩衝區解碼文本：如果啟用，從某些文件類型中提取用於邏輯搜索和索引的文本結果將由 X-Ways Forensics 存儲在卷快照中，以便在再次搜索/索引時重複使用，以節省時間。

外部程序、自定義查看器程序

您可以選擇您喜歡的文本編輯器和 HTML 查看程序。HTML 查看器程序可以是 MS Word 或 NVU，即可用於進一步編輯 X-Ways Forensics 可自動創建的 HTML 案例報告的程序。如果只是查看和打印，我們推薦使用 Internet Explorer。

也可以指定MPlayer的.exe文件路徑，允許 X-Ways Forensics 從視頻中提取圖片的程序。如果在X-Ways Forensics 安裝目錄的\MP3Player子目錄下找到mp3player.exe，它會自動定義為視頻提取程序和外部查看器程序。支持以.\或..\開頭的相對路徑，其中.代表執行 X-Ways Forensics 的目錄及其父目錄。請注意，我們無法為外部程序提供支持。

您還可以指定最多 32 個自定義查看器程序，這些程序可以通過目錄瀏覽器上下文菜單從 X-Ways Forensics 內部方便地調用。另外，您可以指定哪個

您希望在與其系統中的擴展名關聯的程序中查看的文件類型，通常是單獨的查看器組件不支持的文件類型。有一個標記為“如果新識別則將類型附加為擴展名”複選框的複選框。允許更輕鬆地讓 Windows 為錯誤命名的文件、沒有擴展名的文件等運行正確的程序。這些外部查看器程序的路徑定義在一個名為 Programs.txt 的單獨文件中，以便共享外部查看器的集合很容易程序，或者在從其他人那裡接管所有其他程序設置時保留它們。在該文本文件中，您還可以將絕對路徑更改為相對路徑（使用 . 和 ..），用於與 X-Ways Forensics 本身一樣便攜的程序，並且您希望隨身攜帶 U 盤來分析實時系統。

Tesseract :OCR

如果 OCR 派生文本不包含至少 x 個連續的有用字符，則該文本將被忽略。這樣的 OCR 結果將不會被存儲/輸出/複製/索引/搜索。如果您將 OCR 應用於未知/隨機/普通圖片（即未知文本數據），以減少稍後將（誤導性地）響應具有 OCR 派生文本的文件的描述過濾器或針對哪個子項的文件數量，這將很有用對象（不必要地）由“複製 : 提取的文本”功能等創建。“有用”字符此處定義為 ASCII/Unicode 值為 0x30 或更高的字符。這意味著 $\leq 0x20$ 的空格不計算在內，可打印字符 !#\$%& ()*+,-.& (0x21-0x2F 範圍)也不計算在內，因為它們中的一些偶爾會在隨機像素中被誤檢測。任何語言中的所有真實字母都算在內，數字（“0”到“9”）也是如此。

9.5 撤消選項

“撤消”命令的可用性取決於以下選項：

- 指定撤消命令要撤消的順序操作的數量。此選項不影響可逆鍵盤輸入的數量，這僅受可用 RAM 的限制。
- 為了節省時間和硬盤空間，您可以指定文件大小限制。如果文件大於此限制，則不會創建備份，並且除鍵盤輸入外，撤消命令不可用。
- 如果完全選擇了相應的選項，則在關閉文件時，WinHex 會刪除自動創建的內部使用撤消命令的備份。如果它被部分選中，它們將在 WinHex 終止時被刪除。
- 對於所有類型的編輯操作，您可以選擇它們是否應該是可逆的。如果是這樣，則會在操作發生之前創建內部備份。

9.6 安全選項

- 在保存對現有文件的修改之前（即在更新文件之前），您通過

默認提示確認，但可以更改此行為。

- 如果在處理文件時優化卷快照、邏輯搜索或索引中的任何操作崩潰，X-Ways Forensics 在下次啟動時會告訴您哪個文件可能導致崩潰。如果您讓它收集崩潰信息報告。如果全面檢查，如果卷快照優化使程序崩潰，重新啟動程序也會指出程序崩潰時對有問題的文件應用了哪個子操作。尚未測試這種增強的日誌記錄粒度是否會導致任何明顯的減速。如果在崩潰時有多個工作線程處於活動狀態，則可能有多個候選文件觸發了不穩定。
- X-Ways Forensics 能夠在崩潰（非自願程序終止）後自動恢復某些操作，無需任何用戶干預。當前支持的操作是從主菜單或命令行調用或通過將證據對象添加到案例時卷快照細化的“文件頭簽名搜索”和“單個文件處理”階段。崩潰後，這些操作將在取決於上次保存卷快照的時間點恢復。（這又取決於案例屬性中的自動保存間隔，因為每當保存案例時，所有打開的證據對象的捲快照也會被保存。您也可以在優化卷快照時手動保存案例。）如果不清楚哪個特定文件觸發了崩潰，因為您正在使用其他線程運行該操作，那麼該操作將首先在沒有其他線程的情況下恢復。運氣好的話，不會再次觸發崩潰。如果是，則再次恢復操作。一旦確定了確切的文件，它將被自動跳過。如果在文件頭簽名搜索期間發生崩潰，將跳過觸發創建有問題文件的扇區。
- 只有在預覽版和 Beta 版中，如果您希望觀察、測試或演示此自動解決方法，您可以模擬崩潰，例如因為您希望在使用命令行或多或少地自動運行 X-Ways Forensics 時從中受益參數，並且需要對 X-Ways Forensics 的一個實例消失並立即被另一個不是您自己啟動的實例的情況做出反應。對於模擬，您提供要在支持的操作中觸發崩潰的文件的名稱。文件名應該是唯一的，並且理想情況下只針對您知道在初始卷快照中的一個文件，或者您希望將其添加到優化後的捲快照中的文件。它區分大小寫。請注意，如果您讓 X-Ways Forensics 根據遞增數字為已雕刻文件分配名稱，並使其模擬崩潰並使用名稱預計為 012345.jpg 的已雕刻文件，那麼即使 X-Ways Forensics 成功學會了避免在文件頭簽名搜索中找到該文件的扇區，之後的下一個雕刻文件也可能被命名為 012345.jpg（取決於文件類型），從而引發另一次崩潰。

雕刻文件的唯一名稱來自智能命名選項（如“Canon DIGITAL IXUS 950 IS 2007-07-01 12:01:46.jpg”或來自基於起始扇區命名文件的選項。模擬隨機，不可重複的崩潰，您可以使用 Windows 任務管理器簡單地終止 X-Ways Forensics。

- 關於異常的輸出消息：確定程序在異常錯誤情況下的冗長程度。如果完全不檢查，只有具有潛在嚴重影響的異常錯誤（如相當不完整的分析結果）才會引起您的注意

消息窗口。如果完全選中，所有這些都將被輸出，即使是那些通常只出現在損壞文件中並且對其他分析結果沒有負面影響的那些。中間狀態是一個合理的妥協。無論此選項如何，異常錯誤都將記錄在 error.log 文件中。

- 所有輸出到消息窗口的通知和警告都可以選擇性地自動保存在安裝目錄中的文本文件“msglog.txt”中。如果當時案例處於活動狀態，通知/警告將寫入該案例的日誌子目錄中的 msglog.txt 文件。默認行為是該框被選中一半。完全選中意味著即使是進度指示器窗口中的消息（操作描述以及已處理文件的名稱）也會被輸出。
- 使用選項Check for virtual memory changes確保內存編輯器每次在讀取或寫入之前檢查虛擬內存的結構。如果結構已更改，則可以防止可能的讀取錯誤。特別是在 Windows NT 下，檢查可能會導致速度下降。在編輯進程的“整個內存”時，WinHex 通常不會在讀取之前檢查更改，即使啟用了此選項也是如此。

· 嚴格的驅動器盤符保護：僅適用於取證許可證。默認情況下在 X Ways Forensics 中處於活動狀態。確保只能在某些驅動器盤符上保存和編輯文件，即 X-Ways Forensics 即使在檢查實時系統時也可以假定位於檢查者自己的媒體上的文件。它們是：1) 承載活動案例的驅動器盤符（如果有活動案例），2) 帶有臨時文件目錄的驅動器盤符，3) 運行 X-Ways Forensics 的驅動器盤符，以及 4) 驅動器盤符包含圖像文件的目錄。

· 可以在普通編輯框中輸入加密和解密所需的密鑰。

或者，您可以盲目輸入（顯示星號而不是實際字符）。在這種情況下，您必須在第二個編輯框中確認密鑰以檢測拼寫錯誤。

- 默認情況下，只要 WinHex 正在運行，密鑰就會保存在主內存中（處於加密狀態），因此如果您多次使用它，就不必一次又一次地鍵入它。可能您更喜歡 WinHex 在使用後擦除密鑰。
- 決定 WinHex 是在執行腳本之前提示，還是僅在執行腳本之前提示
通過命令行執行腳本。
- 可選地，多字節累加器（16 位、32 位和 64 位校驗和）的校驗和按字節計算，而不是添加與累加器本身大小相等的單元，例如 4 字節用於 32 位校驗和。這兩種變體都存在於現實生活中的應用程序中。
- .e01 塊中的CRC 可以在讀取塊時自動即時檢查，任何差異都將在消息窗口中報告。這需要一點計算能力。
- 使用256 位AES 加密創建的.e01 證據文件的密碼驗證散列是否包含在.e01 證據文件中由您決定。哈希允許

X-Ways Forensics 檢查您在打開此類圖像時輸入的密碼是否正確。

- 如果發現 .e01 證據文件的佈局非常低效（每個表部分少於 32 個塊或壓縮率低於 0.1% 的壓縮塊），請引起用戶注意，以便他們可以避免任何軟件或硬件創建了該圖像。
- 如果有關大型 .e01 證據文件的某些元數據保存在單獨的文件中（擴展名為 .xmet），則 X-Ways Forensics 下次可以更快地重新打開圖像。如果圖像存儲在訪問速度較慢的媒體上，尤其是遠程網絡驅動器上，這可能會產生很大的不同。如果完全選中此框，則單獨的文件將存儲在與圖像本身相同的目錄中，這樣即使其他情況/打開同一圖像的相同副本的其他用戶也可以從創建單獨文件時提高的性能中受益。如果選中一半，則單獨的文件存儲在當前案例的證據對象的內部元數據目錄中。偏執狂的用戶不僅寫入塊可疑存儲設備，而且還寫入他們自己的帶有圖像的存儲設備，如果他們希望從提高的速度中受益，出於顯而易見的原因，建議半選中此框。

可以通過單擊安全選項對話框窗口中的按鈕來維護一般密碼集合。它存儲在文件“Password.txt”中。新創建案例的密碼集合使用該通用密碼集合進行初始化。每當加載案例時，案例的密碼集都會與加密檔案和加密文檔一起使用。

此對話框中的按鈕之一允許耗盡系統內存，例如，為了獲得與性能測試可比的結果，如果 Windows 在其文件緩衝區中仍有圖像文件的一部分，這些結果可能會失真。

另一個按鈕允許在一定的分鐘數後安排機器的關機或休眠。只有在沒有任何東西阻止機器斷電的情況下才能保證工作，例如其他應用程序具有未保存的工作等。如果你半檢查以“粗暴地”繼續，即使應用程序掛起也應該關閉機器。如果完全選中，那甚至不會等待其他應用程序提示用戶如何處理任何未保存的工作超過幾秒鐘。如果退出已安排關閉的 WinHex/X-Ways Forensics 實例，則不會發生關閉。可以在不重新啟動程序的情況下取消先前計劃的關閉。

9.7 搜尋選項

匹配大小寫：如果搜尋區分大小寫，則意味著區分大小寫字符，例如在單詞“optionally”中找不到帶有大寫字母“O”的“Option”。通過取消選中該複選框，您可以搜尋搜尋詞的所有大寫/小寫變體。

只有同時搜尋時搜尋完全不區分大小寫，而查找文本命令僅適用於拉丁/英語字母表和德語變音符號中的字母。在同步搜尋中，如果“匹配大小寫”選項被選中一半，您可以同時使用區分大小寫和不區分大小寫的搜尋詞。在這種情況下，您可以在搜尋詞前加上

“case:”將它們標記為區分大小寫。

Unicode :指定文本在 UTF-16 Little Endian 中搜索。同時搜索允許同時在 Unicode 和其他代碼頁中搜索相同的文本。

您可以指定一個通配符（一個字符或兩位十六進制值），它代表一個字節。

例如，當使用問號作為通配符搜索“Sp?ck”時，此選項可用於查找“Speck”和“Spock”。

僅全詞：僅當搜索詞作為一個完整詞出現時才會被找到，即如果用除 a...z、A..Z 以及德文和法文字母以外的任何字符（例如標點符號、空格、二進制控制代碼、數字）。如果啟用此選項，例如在“automaton”中找不到“tomato”。在同時搜索中，所有搜索詞都作為整個單詞搜索，或者僅搜索縮進的搜索詞（以製表符開頭）或不搜索，具體取決於相應複選框的狀態。如果您希望將整個單詞的搜索縮進與區分大小寫的“case:”前綴組合，請先輸入“case:”前綴，然後插入縮進的製表符。

對於同步搜索功能，“全詞”是一個三態選項。中間狀態只允許匹配單詞的開頭（在搜索命中的開頭需要單詞邊界）。這意味著例如使用“box”你可以同時找到“boxes”（但不是“checkbox”）並且使用“tend”你可以同時找到“tends”和“tended”（但不是“attended”或“擴展”）。

否則這只能通過正則表達式來實現，如果您希望同時搜索某些搜索詞作為整個單詞和其他搜索詞的開頭，您仍然需要使用正則表達式。

您可以為使用 Latin 1 代碼頁的語言自定義詞邊界檢測，即通過定義被視為字母的字符字母表（即屬於單詞的字符）而不是非單詞字符。一個單詞字符後跟一個非單詞字符或相反的方式被認為是一個單詞邊界。共有三個易於使用的預定義設置。最徹底的搜索結果設置是默認設置。對非文本數據（如 Base64 或二進制垃圾）中的短關鍵字的垃圾命中不知所措的用戶可能想嘗試其他兩個選項。這另外兩個選項可能會導致在某些星座中丟失有效的搜索命中（取決於文件格式），但仍然可以作為文本文檔中搜索的大量時間節省是合理的，例如在電子發現中，而不是在計算機取證中。

有關整個單詞選項如何工作的更多解釋和示例，請繼續閱讀：單詞邊界是兩個連續字符之間的邊界，其中一個字符是單詞字符，另一個字符不是單詞字符。如果兩個連續的字符都是單詞字符（例如“ns”），那麼顯然“s”不是一個新的整個單詞的開始，而“n”不可能是一個完整單詞的結尾。它可以在整個單詞中間的某個地方（例如

“mansion”），但是在這兩個字符“ns”之間絕對沒有單詞邊界。如果兩個字符都是非單詞字符（如“!”，感嘆號後跟一個空格），那麼顯然兩者之間的位置也不是單詞邊界。感嘆號不能作為單詞的結尾（不能出現在單詞的任何地方），空格不能作為單詞的開頭（也不能出現在單詞的任何地方，複合詞除外）。如果您在“我們的豪宅”中搜索“man”作為一個完整的詞，那麼 XWF 將

臨時/內部找到“man”，然後首先檢查“m”之前的字符是否為單詞字符。那個字符是一個空格。空格字符不是單詞字符。然後它還根據字母表檢查“m”是否是單詞字符。這是。這意味著在“m”之前有一個單詞邊界。接下來XWF需要檢查“n”和“s”是否是單詞字符。兩者都是。這意味著在“n”之後沒有單詞邊界。因此，“mansion”中的三個字母“man”不被視為“man”的整個單詞出現。

根據用戶選擇的字母定義（僅檢查搜索命中中的第一個和最後一個字符），同時搜索的僅全詞限制不適用於不是單詞的搜索命中。例如，如果您正在搜索“LOL!!”，那麼這不可能是一個完整的單詞，因為感嘆號不是字母，因此不包含在定義的字母表中（好吧，除非您手動將感嘆號添加到它）。

然而，RegEx 單詞邊界指示符 \b 仍然適用於這種情況，例如能夠在單詞之間搜索某些數據，這些數據本身不被視為單詞。

除了拉丁 1 代碼頁（所有西歐語言）的字符字母表之外，還可以為另一種語言的字母定義一個可選的附加字母表。如果激活，它用於在 UTF-16、UTF-8 和區域 ANSI/OEM/IBM/ISO/Mac 代碼頁中搜索只有 1 個字節的字符，例如西里爾文、希臘文、土耳其文、阿拉伯文、希伯來文、越南文和各種中/東/東南歐語言。西里爾字母是預定義的。

搜索方向：決定 WinHex 是從頭到尾搜索，還是從當前位置向下或向上搜索。

條件：偏移模 $x = y$ ：搜索算法僅接受在滿足給定要求的偏移處出現的搜索字符串。例如，如果您搜索通常出現在硬盤扇區第 10 個字節的數據，您可以指定 $x=512, y=10$ 。如果您正在尋找 DWORD 對齊的數據，您可以使用 $x=4, y=0$ 來縮小命中數。

Search in block only：搜索操作僅限於當前塊。

在所有打開的窗口中搜索：搜索操作應用於所有打開的編輯窗口。按 F4 在下一個窗口中繼續搜索。如果同時啟用“Search in block only”，則搜索操作僅限於每個窗口中的當前塊。

計算出現次數/保存出現位置：強制 WinHex 不顯示每一次出現，而是對它們進行計數。如果完全啟用此選項，WinHex 會將所有事件輸入到位置管理器中。

搜索“不匹配”：在“查找十六進制值”中，您可以指定一個帶有感嘆號作為前綴的單個十六進制值（例如 !00），以使 WinHex 在遇到第一個不同的字節值時停止。

正則表達式：搜索選項僅適用於同步搜索。正則表達式是一種強大的搜索工具。一個正則表達式可以匹配許多不同的詞。要么所有搜索詞都被視為正則表達式，要么僅被視為前綴為

“grep :”或無，取決於相應複選框的狀態。您可以在搜索詞前加上“case:”（見上文）和“grep:”的順序。以下字符在正則表達式中具有特殊含義，如下所述：()[]{}|\。#+?。如果要按字面意思理解這些特殊字符，則需要在它們前面加上反斜杠字符(\)。

運算符用於表示替代匹配項。您可以使用正則表達式car (wheel|tire)來搜索單詞“car wheel”和“car tire”。任何匹配項必須等於任何|之前、之後或之間的部分運營商在場。的影響僅受括號限制。

.和#是通配符：.匹配任何字符，#匹配任何數字字符。您可以在方括號的幫助下定義字符集:[xyz]將匹配任何字符x、y、z。[^xyz]將匹配除x、y或z之外的任何字符。您可以使用破折號定義字符範圍:[az]匹配任何小寫字母。[^az]匹配除小寫字母以外的所有字符。

該列表可以同時包含單獨列出的字符和範圍:[aceg-loq]匹配a、c、e、g、h、i、j、k、l、o和q。除了[、]、-和\之外的所有字符都按字面意思放在方括號之間，甚至是通配符。和#。

\b代表單詞的開始或結束，即單詞字符和非單詞字符之間的邊界。哪些字符/字母被同時搜索視為單詞字符是用戶定義的。文件的開頭和結尾也算作字邊界。\\b僅在搜索詞的開頭和/或結尾受支持，不能與|一起使用。\\b、^和\$僅在搜索案例的證據對象時有效，不適用於索引搜索。

對應於鍵盤無法輕易產生的ASCII字符的字節值可以用十進製或十六進製表示法指定：例如，\032和\x20都相當於ASCII字符集中的空格字符。即使在方括號之間也支持這種表示法。例如[\000-\x1f]匹配不可打印的ASCII字符。

乘數字符(*、+和?)表示前面的字符可能或必須出現多次（見下文）。複雜示例:a(b|cd|e[fh]i)*j匹配aj、abj、acdij、aefij、aegij、aehij、abcdj和abefij。

在[]括號內，字符.*+?{}|不被視為特殊字符，而是字面意思。

支持的語法特性的簡要概述（其他一切按字面解釋）

- 句點匹配任何單個字符。
- # 井號匹配任何數字字符[0-9]。\\nnn用三個十進制數字(0...255)指定的字節值\\xnn用兩個十六進制數字(0...FF)指定的字節值。

例如，\\xD\\xA是Windows換行符。\\unnnn用四個十六進制數字指定的Unicode值。

- 根據所選的代碼頁，對應於不同的字節值。
- ? 匹配一個或零個前面的字符或集合。
- * 匹配前面字符出現的任意次數，包括零次。
- + 字符後的加號匹配它出現的任意次數，但零除外。
- [XYZ]括號中的字符匹配出現在括號中的任何一個字符。

[^XYZ] 括號中字符串開頭的抑揚符表示 NOT。
 [AZ] 括號內的破折號表示一個字符範圍。 \{X,Y} 重複前面的字符或字符組 XY 次。
 (ab) 函數類似於斷句標記，但將括號面意思處理。

將 ab 組合在一起表示 +、?、*、| 和 {}。一個 |
 b 管道充當邏輯或。所以它會讀作 “a or b”。\b
 ^ 匹配單詞邊界。
 \$ 匹配文件的開頭。
 \$ 根據搜索選項匹配文件的邏輯或物理結尾。

正則表達式示例

電子郵件地址 [a-zA-Z0-9_\-\+\.\.]{1,20}@[a-zA-Z0-9_\-\.\.]{2,20}\.[a-zA-Z]{2,7} (Gmail 地址支持 @ 前的 +)
 Z0-9_\-\+\.\.]{1,20}@[a-zA-Z0-9_\-\.\.]{2,20}\.[a-zA-Z]{2,7} (Gmail 地址支持 @ 前的 +)

以 http://、https://、ftp:// [a-zA-Z]+://[a-zA-Z0-9/_?\$_&=\-\.\.]+ 開頭的互聯網地址

Visa 和 Mastercard 信用卡號碼 [^\#az]
 [45]######[^\#az] [45]###-####-#### [45]###-####-#### (理想情況下通過 X-Tension 和 Luhn 算法檢查結果，以減少錯誤命中的數量並在沒有 [^\#az 的情況下進行搜索])

允許重疊命中。如果您使用常規語法搜索可變長度的搜索命中，則可能會在同一位置出現多個有效命中。例如，如果您搜索電子郵件地址，並且搜索算法輸入字符序列 “mail@x-ways.com”，那麼它將確定 “mail” 中 “m” 中的字符匹配常規表達，它會記錄一個命中。之後，它繼續處理 “郵件” 中的 “a” 並意識到 ail@x-ways.com 也符合要求，il@x-ways.com 和 l@x-ways.com 也是如此。所有這些都可能是有效的電子郵件地址。所以搜索算法是完全正確的，但通常用戶不希望看到這些額外的命中。因此，如果您不允許重疊點擊，則新點擊僅記錄在 “.com” 中的 “m” 之後。不允許重疊命中意味著將命中所涵蓋的字符專門分配給該命中，而不再分配給潛在的其他命中。

搜索窗口，鄰近搜索

搜索窗口寬度默認為 128 字節。這意味著不能保證使用可變長度的正則表達式（即使用 {}*+ 語法）您可以找到超過 128 字節的數據。如果您需要覆蓋更多內容，您可以增加搜索窗口的寬度。

例如，這對於鄰近搜索是必需的。如果您要求一個文檔同時包含兩個搜索詞，並且搜索詞應該彼此靠近，您可以使用兩個正則表達式搜索這些搜索詞，並指定它們之間允許的最大距離作為第二個參數在大括號中：

keyword1.{0,maxdistance}keyword2
keyword2.{0,maxdistance}keyword1使

用 8 位字符集搜索時所需的搜索窗口寬度（以字節為單位）是 maxdistance、length(keyword1)和length(keyword2)的總和。

請注意，當兩個搜索詞在單獨搜索後已經用邏輯 AND 組合在一起時，找到彼此靠近的兩個搜索詞的首選方法是搜索詞列表中的 NEAR 組合。

9.8 替換選項

發現時提示：WinHex 在發現事件時等待您的決定。您可以替換它、繼續或中止搜索。

替換所有事件：自動替換所有事件。

區分大小寫：使用此選項搜索要替換的字符（參見搜索選項）。

Unicode 字符集：以 Unicode 格式搜索和替換指定的字符（參見搜索選項）。

您可以指定一個字符或兩位十六進制值作為通配符。這通常在搜索字符串中完成。如果替換包含通配符，則不會更改出現在相應位置的字符。因此，“black”和“block”可以同時替換為“crack”和“crock”（輸入“bl?ck”和“cr?ck”）。

只有完整的單詞：搜索的字符串只有在與其他單詞分開時才能被識別，例如通過標點符號或空格。如果啟用此選項，則不會在“自動機”中替換“番茄”。

搜索方向：決定WinHex是從頭到尾，還是從當前位置向下或向上進行替換。

Replace in block only：替換操作僅限於當前塊。

在所有打開的文件中替換：替換操作應用於所有未在查看模式下打開的文件。如果同時啟用“僅替換塊”，則替換操作僅限於每個文件的當前塊。

暗示：

WinHex 能夠將一個字符串或十六進制值序列替換為另一個具有不同長度的字符串或十六進制值序列。系統將提示您應用以下哪種方法：

第一種方法：由於長度不同移動了出現後面的數據。所以文件大小是

變了。此方法不得應用於某些文件類型，例如可執行文件。甚至可以不指定任何內容作為替代，這意味著所有出現的內容都將從文件中刪除！

第二種方法：將替換項寫入文件中出現的位置。如果替換比搜索的字符序列短，超出的字符將保留在文件中。否則，即使發生後的字節也會被覆蓋（只要未到達文件末尾）。文件大小不受影響。

10 雜項

10.1 塊

您可以將打開的文件或磁盤的一系列字節或扇區標記為“塊”。這部分可以通過編輯菜單中的幾個功能來操作，就像在其他 Windows 程序中的選擇一樣。

如果沒有定義塊，這些函數通常應用於整個文件或磁盤。

塊的當前位置和大小顯示在狀態欄中。雙擊鼠標右鍵或按 ESC 鍵清除塊。

10.2 修改數據

如果沒有定義塊，則使用此命令修改塊內或整個文件內的數據。在這個版本的 WinHex 中，有四種類型的數據修改可用。要么將固定整數添加到數據的每個元素，反轉位，將常量與數據進行異或（一種簡單的加密），或或與，以循環模式向左旋轉的位（第一個字節旋轉 1 位，第二個字節 2 位，依此類推），邏輯移位或字節交換。通過移位，您可以模擬在塊的開頭插入或刪除單個位。您也可以移動整個字節（目前僅通過輸入負數字節向左移動）。如果您希望以就地模式從一個非常大的文件中剪切字節，這將很有用，否則需要創建一個巨大的臨時文件。

添加

指定要添加到當前塊的每個元素的正數或負數、十進制數或十六進制數。整數格式定義元素的大小（1、2 或 4 字節）和類型（有符號或無符號）。

如果加法的結果超出了所選整數格式的範圍，有兩種處理方法。假定範圍限制為新值 (I) 或忽略進位 (II)。

示例 :無符號 8 位格式 I。

$$\begin{aligned} \text{FF} + 1 &\rightarrow \text{FF} (255 + 1 \rightarrow 255) \\ \text{二。} \quad \text{FF} + 1 &\rightarrow \text{00} (255 + 1 \rightarrow 0) \end{aligned}$$

示例 :帶符號的 8 位格式 $80 - 1 \rightarrow 80$

$$\begin{aligned} (-128 - 1 \rightarrow -128) \\ \text{二。} \quad 80 - 1 \rightarrow 7F (-128 - 1 \rightarrow +127) \end{aligned}$$

- 如果您決定使用第一種方法 ,WinHex 會告訴您 ,範圍限制的頻率是多少超過了。
- 第二種方法確保操作是可逆的 。只需添加 $-x$ 而不是基於 x 在相同的整數格式上重新創建原始數據。
- 當使用第二種方法時 ,無論您選擇有符號的還是有符號的都沒有區別。無符號格式。

反轉字節順序

此命令假定所有數據均由 16 位元素 (分別為 32 位元素) 組成 ,並交換高位字節和低位字節 (以及高位字和低位字) 。使用它來將大端數據轉換為小端數據 ,反之亦然。

10.3 轉換

WinHex 提供了Edit 菜單的Convert 命令 ,方便不同數據格式的轉換和加解密 。可以選擇將轉換應用於所有打開的文件 ,而不僅僅是當前顯示的文件 。標有星號 (*) 的格式只能作為一個整體文件進行轉換 ,而不能作為一個塊進行轉換 。支持以下格式 :

- ANSI ASCII 、IBM ASCII (兩種不同的 ASCII 字符集) · EBCDIC (IBM 大型機字符集)
- 小寫/大寫字符 (ANSI ASCII) · Binary* (原始數據) · Hex ASCII*
- (原始數據的十六進製表示形式為 ASCII 文本) · Intel Hex* (=Extended Intel Hex ;特殊格式的十六進制 ASCII 數據 ,包括校驗和等) · Motorola S*
- (=Extended Exorcisor ;同上) · Base64*
- UUCode* ·
- 百分比 URL 編碼 · 引用可打印

請注意 : · 在
轉換 Intel Hex 或 Motorola S 數據時 ,這些格式的內部校驗和是未檢查。

- 根據文件大小，自動選擇可能的最小輸出子格式。
Intel Hex :20 位或 32 位。摩托羅拉 S :S1、S2 或 S3。
- 從二進制轉換為 Intel Hex 或 Motorola S 時，只有未填充的內存區域
轉換十六進制 FF，以保持生成的文件緊湊。

Convert 命令還可以解壓縮由 NTFS 文件系統壓縮的任意數量的完整 16 簇壓縮單元*和（具有取證許可）從圖像複製的整個 hiberfil.sys 文件以及來自此類文件的單個 xpress 塊。此外，它還允許將 Android 設備的 NAND 閃存的所謂 Nandroid 備份文件轉換為常規原始圖像。

此外，它還可以將壓縮的 7 位 ASCII 擴展為可讀的 8 位 ASCII*，這對於手機短信等非常有用。

加密/解密

指定由 1-16 個字符組成的字符串作為加密/解密密鑰。密鑰區分大小寫。輸入的字符越多，加密越安全。密鑰本身不
用於加密和解密，而是消化為實際密鑰。密鑰未保存在您的硬盤上。如果啟用了相應的安全選項，只要 WinHex 正在
運行，密鑰就會以加密狀態存儲在 RAM 中。

建議指定至少 8 個字符的組合作為加密密鑰。不要使用任何語言的單詞，最好選擇字母、標點符號和數字的任意組合。請注意，加密密鑰區分大小寫。請記住，如果沒有適當的密鑰，您將無法檢索加密數據。您輸入的解密密鑰在解密前未經驗證。

加密算法：256 位 AES/Rijndael，計數器 (CTR) 模式。此加密算法使用一個 256 位密鑰，該密鑰使用 SHA-256 從您
指定的密鑰的 SHA-256 的 512 位串聯和 256 位加密可靠的隨機輸入（“鹽”）中提取。該文件擴展了 48 個字節以
容納 256 位鹽和一個隨機化的 128 位初始計數器。

WinHex 不僅可以加密整個文件，還可以只加密一塊數據。然而，在這種情況下，您會被警告，沒有使用鹽，也沒有使用隨機初始計數器，因此您不能重複使用您的密鑰來使用相同的加密方法加密其他數據。塊的大小保持不變。

10.4 扇區疊加

使用此功能，您可以將其他數據疊加在以只讀方式打開的磁盤或解釋圖像之上。當您需要對程序範圍內的扇區中的數
據進行微小的臨時虛擬調整以使其在內部正確解釋時很有用，但不希望或不允許更改磁盤或映像本身的扇區（或不
能，因為它不是原始圖像，而是 .e01 證據文件）並且也不想製作另一個完整的圖像工作副本，例如，如果只需要更改 1
個字節，則大小為 2 TB。這樣的

例如在分區或文件系統元數據損壞的情況下，可能需要進行調整，其中缺少一個幻數會使 WinHex 無法檢測文件系統，或者只有一個翻轉位會使 WinHex 無法在 NTFS 中找到 \$MFT 或分區中只有一個錯誤的半字節table 使 WinHex 無法將分區識別為 LVM2 容器分區等。在這些情況下，您可以手動提供並疊加更正後的數據，然後希望可以毫無問題地使用磁盤或映像，立即將所有分區和文件列為如果沒有錯的話。此功能適用於高級用戶，他們在第一次看到“什麼都沒有”時不會輕易放棄，並且對低級數據結構有一定的了解並知道如何修復它們。

您可以使用編輯 | 在活動數據窗口中啟用和禁用磁盤或分區的疊加。疊加扇區菜單命令。此命令允許您選擇具有磁盤扇區原始內容的任何文件。例如，您可以通過選擇一個或多個扇區作為一個塊來創建這樣的文件，將塊複製到一個新文件中，進行必要的調整（甚至在 X-Ways Forensics 中也是可能的，因為不同於磁盤或解釋圖像的普通文件可以被編輯）並保存該文件。應用時，此文件的內容將疊加到以光標所在扇區開頭的扇區，或者如果文件名為“n.sector”，其中n是一個數字，它將應用於以光標所在扇區開頭的扇區扇區n，以及同一目錄中匹配相同掩碼的所有其他文件也將應用於文件名中指示的扇區號。導航到受影響的扇區時，您將立即看到疊加的數據，如果您在單獨的窗口中將其打開，則可以繼續對疊加的原始數據文件進行調整。一旦您在該窗口中保存了更改，它們將在代表您嘗試修復其數據的磁盤或分區的數據窗口中生效，當您刷新視圖、拍攝新的捲快照、定義分區的開始時，再次嘗試打開文件記錄損壞的文件等。

請注意，只能疊加完整的扇區，不能疊加部分扇區。疊加一次只能對一個打開的磁盤或磁盤分區或圖像有效。如果對物理分區磁盤或物理分區磁盤的映像處於活動狀態，則從物理磁盤內打開的分區也將顯示疊加數據。如果需要，您可以在疊加生效時使用常用命令製作虛擬修復的磁盤或映像的副本（映像或克隆磁盤），這樣副本將直接嵌入疊加的扇區。活動扇區疊加記憶在證據對像中，下次打開證據對象時自動重新激活，並提醒您。

10.5 擦除和初始化

要安全地擦除（切碎）磁盤扇區、未使用的磁盤區域（磁盤工具菜單）或使用“安全擦除”命令選擇的文件中的數據，以及簡單地用特定字節值填充文件，

WinHex 提供以下選項：

With constant byte values specified in hexadecimal notation:指定最多 16 個兩位數的十六進制值，這些值將分別被重複複製到當前塊、整個文件或所有磁盤扇區。非常快。

使用簡單的偽隨機字節值：指定小數間隔（最大為 0 到 255）

隨機數，分別重複複製到當前塊、整個文件或所有磁盤扇區。隨機字節是拉普拉斯分佈的。快速地。

使用模擬加密的偽隨機數據：應該與加密數據無法區分的隨機數據。蠻快。

使用加密可靠的偽隨機數據：名為 ISAAC 的加密安全偽隨機數生成器 (CSPRNG)，非常慢。

如果在所有打開的文件中定義了一個塊或沒有定義塊，則可以選擇同時將此命令應用於所有這些文件。

為了最大限度地提高安全性，如果您希望完全擦除（清理）閒置空間、可用空間、未使用的 NTFS 記錄或整個媒體，您可能需要應用不止一次覆蓋磁盤空間（最多三個）。

根據清除和消毒矩陣，美國國防部 (DoD) 5220.22-M 操作手冊中概述的標準，方法“c”，可以通過覆蓋（一次）所有可尋址位置來清除硬盤或軟盤單個字符。這通常是十六進制值 0x00，但也可以是任何其他值。根據方法“d”清理硬盤，用一個字符覆蓋所有可尋址位置，其補碼，然後是一個隨機字符，並驗證。（國防部未批准此方法用於淨化包含絕密信息的媒體。）

“DoD”按鈕配置 WinHex 進行清理，這樣它將首先用 0x55（二進制 01010101）覆蓋，然後用它的補碼（0xAA = 10101010）覆蓋，最後用隨機字節值覆蓋。

“0x00”按鈕將 WinHex 配置為簡單初始化，用零字節擦除一次。

10.6 磁盤克隆

工具 | 磁盤工具 | 克隆磁盤。此函數將定義數量的扇區從源複製到目標。源和目標都可以是磁盤（單擊帶有磁盤圖標的按鈕）或文件（單擊帶有文件圖標的按鈕）。

如果源和目標都是磁盤，則兩個磁盤的扇區大小必須相同。

為了有效地複制介質（即復制所有扇區），只需複制所有扇區。選擇適當的選項，以便自動輸入正確的扇區數。目標磁盤不得小於源磁盤。作為磁盤，您還可以選擇在後台從物理磁盤中打開的解釋圖像或分區。作為目標，您不能選擇已解釋的 .e01 證據文件，因為此類圖像無法重寫，只能重寫原始圖像。作為文件，您只能指定未分段的原始圖像，例如 .dd、.001、.img 等，不能指定其他圖像類型，例如 .e01、.vhd、.vmdk 等。

磁盤克隆提供了一些選項來控制磁盤上遇到壞扇區時的行為

源磁盤： ·

默認情況下，系統會通知您錯誤並提示您繼續或中止操作。“Log procedure silently”在臨時文件（文件名“Cloning Log.txt”）文件夾中創建整個操作的完整日誌文件，包括關於不可讀扇區（無法複製）的報告，並防止 WinHex 報告每個不可讀扇區部門分開。

- WinHex 可以保留與損壞的源扇區相對應的目標扇區不變，或者用您指定的 ASCII 模式填充它（例如您的首字母，或類似“BAD”的東西）◦將模式編輯框留空以用零字節填充此類扇區◦順便說一句，所選模式還用於在磁盤編輯器中顯示壞扇區的內容。
- 壞扇區經常出現在連續的組中，每次嘗試讀取壞扇區通常需要很長時間。您可以讓 WinHex 避開此類損壞的磁盤區域。當遇到壞扇區時，WinHex 可以跳過您指定的多個後續扇區。如果您希望加速克隆過程並且您不關心某些實際可讀的扇區沒有進入克隆，這將很有用。

如果您想要在只有一個可移動驅動器的情況下複製可移動驅動器（例如軟盤）中的磁盤，則不能選擇常規磁盤克隆。此應用程序的正確概念是磁盤映像，其中數據首先存儲在映像文件中。然後可以將映像複製到不同的磁盤。結果與磁盤克隆相同。

當您指定一個名為“dev-null”的文件作為目標時，數據將只被讀取而不會複製到任何地方（並且您會收到警告）。如果您對有關壞扇區的報告感興趣，但不希望實際克隆或鏡像磁盤，這將很有用。

如果目標與源不是同一物理介質，您可以嘗試“同步 I/O”。

提供將克隆過程加速高達 30% 的機會。

專家許可證或更高：與同步 I/O 結合，您還可以讓 WinHex 從源磁盤的末尾向後反向複製磁盤的扇區。如果源磁盤存在嚴重的物理缺陷，例如導致磁盤映像程序或整個計算機在到達某個扇區時凍結或崩潰，則很有用。在這種情況下，您還可以通過從磁盤向後一個扇區一個扇區讀取扇區來額外創建一個圖像獲得盡可能完整的圖像，從兩端填充，理想情況下中間只有一個小的零間隙，代表源硬盤上無法讀取的損壞點。為此，您只需選擇一個您已有的不完整原始圖像文件作為目標文件，系統將詢問您是否希望完成它而不是覆蓋。WinHex 將完成剩下的工作，例如分配映像文件中缺失的扇區（歸零），使其具有源磁盤的完整大小，然後儘可能向後填充文件。請務必在 NTFS 卷而非 FAT32 上創建反向映像。為反向成像指定的源起始扇區與傳統正向成像相同，即在成像整個硬盤時通常為 0。

對於一般的磁盤映像，建議使用 File | Create Disk Image 功能代替，出於各種原因（具有取證許可證：支持.e01 證據文件、壓縮、拆分、散列、加密、元數據、技術詳細信息報告，更方便）。只有在

特定情況下，例如處理多個物理磁盤缺陷或目標是僅複製特定範圍的扇區時，高級用戶可以使用工具 |磁盤工具|克隆磁盤可以更詳細地控制哪些扇區以何種順序從何處複製到何處。

10.7 圖像和備份

文件菜單中的“創建磁盤映像” / “製作備份副本”命令允許創建當前打開的邏輯驅動器、物理磁盤或單個文件的備份或映像。共有三種可能的輸出文件格式，每種格式都有其獨特的優勢。

文件格式：WinHex Backup	文件擴展名：.whx 可解釋為磁盤：否	可拆分：是	可壓縮：是	可加密：是	證據文件.e01	原始圖像例如.dd 是 是
可選散列：集成	可選描述：集成	僅扇區範圍：是	適用於文件：是	自動標識：備份管理器兼容性：必需		
					是是是	
					是是集	
					成集成	不
					(是)	不
						分開分開（是）
					不	不
					不	不
					(是)法醫	是的個人
					沒有任何	

證據文件和原始圖像的主要優點是它們可以像原始磁盤一樣被 WinHex 解釋（使用專家菜單中的命令）。這也使它們適合在您的案件中用作證據對象。這尤其適用於證據文件，因為它們可以存儲可選的描述和集成的哈希值，以供以後自動驗證。原始圖像的好處是它們可以在更多取證工具之間輕鬆交換。所有輸出文件格式都支持拆分成用戶定義大小的段。例如，650 或 700 MB 的段大小適合在 CD-R 上存檔。證據文件必須最大拆分為 2047 MB，以使其與 v14.9 之前的 X-Ways Forensics 版本和 v6 之前的 EnCase 版本以及某些其他工具兼容。有了取證許可，原始圖像文件和證據文件可以在創建後立即自動驗證，方法是重新計算最初從媒體計算的哈希值，而不是圖像。

證據文件和 WinHex 備份壓縮基於“Deflate”壓縮算法，該算法是流行的通用庫 zlib 的一部分。該算法由 LZ77 壓縮和霍夫曼編碼組成。使用“正常”壓縮級別，平均數據的壓縮率可以達到 40-50%。然而，這是以顯著降低成像速度為代價的。“快速/自適應”壓縮是速度和良好壓縮之間非常好的智能折衷，不像其他程序中的普通快速壓縮選項。使用“高”壓縮，您只能獲得幾個百分點的壓縮率，但成本卻高得不成比例。對於 WinHex 備份，“自適應”與“正常”相同。

如果原始圖像文件是在 NTFS 卷上創建的，則可以在 NTFS 文件系統級別壓縮它們。要么使用正常的 NTFS 壓縮，要么可以使圖像文件“稀疏”，這樣大量的零值字節就不需要驅動器空間了。

清理過的圖像：有了取證許可，對於那些需要或想要從取證圖像中排除某些文件的用戶來說，有一個獲取選項，稱為“省略排除的文件”。存儲在與您在開始成像過程之前排除的文件相關聯的簇中的數據將在圖像中自動歸零。這不會對內容未存儲在其自己的集群中的文件產生任何影響。在開始分區磁盤的映像過程之前，打開要排除的文件所在的分區。

如果之前沒有拍過卷快照，請等到卷快照拍完。然後排除文件。

您不需要打開並拍攝要完全包含其數據的分區的捲快照。所有其他數據都會正常複製到圖像中。有一個選項可以使用 ASCII 或 Unicode 文本字符串為圖像中的擦除扇區添加“水印”，這樣在處理圖像時，當您查看受影響的區域時，系統會提醒您遺漏的部分。

清理過的圖像對於需要編輯文件系統中某些文件的任何人都很有用，但除此之外還想創建一個普通的取證可靠的扇區圖像，與其他工具兼容。在其立法特別保護個人最私密的個人數據和從職業機密保管人（例如律師和醫生，其職業發誓保密/保密）獲得的某些數據的國家/地區，這是必須的。限制：不適用於分區為 Windows 動態磁盤或使用 Linux LVM* 的磁盤。只能省略支持的文件系統中的文件。請注意，您還可以通過目錄瀏覽器上下文菜單安全擦除選定文件，在 WinHex 中追溯清理（編輯）已經創建的傳統原始圖像。這種操作的粒度不限於整個集群。例如，這意味著它還可以使用所謂的駐留/內聯存儲擦除 NTFS 文件系統中的文件，並且不會同時刪除文件。有關證據文件容器、骨架圖像和清理圖像的比較，請訪問[我們的網站](#)。所有這些都是僅傳輸原始數據子集的圖像。

另一種清理圖像是這樣一種圖像，其中文件系統標記為空閒的所有集群都被清零（僅限專家或取證許可）。如果您創建圖像是為了備份目的而不是為了取證目的，或者如果為了取證目的您不需要可用空間中的數據或不應該獲取它（僅檢查現有文件），這將非常有用。結合壓縮，此選項有可能節省大量驅動器空間，具體取決於有多少可用空間，如果卷/分區中有大的連續可用驅動器空間區域，則可以大大加快成像速度。請注意，在文件系統不一致的情況下，集群可能會被錯誤地視為空閒。如果您希望忽略某些（排除的）文件和可用簇，還可以排除虛擬文件“可用空間”並在卷快照選項中關閉“淨可用空間計算”。

您必須特別確認清理圖像的創建，因為在傳統意義上它們在法醫上是不可靠的（儘管在更現代的意義上它們可以是，這取決於您在個人隱私權和個人隱私權更嚴格的國家/地區工作的司法管轄區）。

X-Ways Forensics 在創建分區物理磁盤的清理映像時檢查重疊分區並發出警告。受影響的磁盤區域中的簇不會被忽略。在這種情況下，建議將相關分區單獨鏡像。

取證許可：創建圖像時，會創建技術細節報告並將其寫入圖像文件隨附的文本文件中。對於.e01 證據文件，它也直接合併。

進入 .e01 文件作為描述。鏡像完成後再次查詢SMART信息寫入文本文件，可以查看鏡像時壞盤狀態是否進一步惡化。其次，您可以看到“開機時間”是如何變化的，這有助於推斷其計量單位（通常是小時，但在某些硬盤型號上可能有所不同）。該文本文件還指示創建圖像所花費的時間、所達到的壓縮率、基於哈希值（如果已選擇）對圖像進行即時驗證的結果以及任何扇區讀取錯誤。

取證許可證：能夠在對磁盤進行映像時立即創建圖像的第二個副本，這比稍後複製圖像文件要快得多，並且如果第二個副本是在不同的驅動器上創建的，則有意義。文件跨越（即何時開始另一個圖像文件段）在兩個副本之間保持同步，即使僅在兩個目標驅動器之一上的空間不足時也是如此。

取證許可：您可以提前指定一個溢出位置，如果主輸出驅動器上的空間用完，將在該位置存儲更多圖像文件段。如果將該字段留空，或者即使溢出位置也沒有剩餘空間，系統將在需要時像以前一樣提示您輸入新路徑。如果預先指定了溢出位置，同時您選擇創建圖像的兩個副本，那麼請注意，溢出位置僅用於空間不足的第一個圖像副本（如果有）。對於其他圖像副本，如果空間不足，系統會提示您。

取證許可證：能夠同時計算兩個哈希值。如果您使用此選項，則兩個哈希值都將存儲在描述性文本文件中。第一個哈希值是成像完成時可以自動驗證的哈希值。您可以有意為此選擇更快的算法，因為此時的主要目的是檢測 I/O 錯誤和文件錯誤。

在將圖像添加到時，將第二個哈希值導入到證據對象屬性中
一件事。

一個特殊的選項允許在哈希驗證之前耗盡系統內存，以使 Windows 使用的任何文件緩衝區無效並阻止它，以便直接從磁盤讀取圖像數據以進行驗證，而不是從內存緩衝區中獲取。此選項適用於小圖像和有點偏執或超級勤奮的用戶。對於比安裝在計算機中的 RAM 的物理量大得多的圖像，不需要它，因為當圖像的最後部分被寫入時，初始部分不再在緩衝區中，並且一旦final parts are about to be verified 它們不在緩衝區中，因為那時初始部分在緩衝區中，因為它們剛剛被驗證過。使用此選項時，您的系統可能會在一段時間內表現得有點遲鈍，並且驗證速度可能會比平時稍慢。

取證許可證：能夠在其他實例中提前安排後續磁盤映像操作，這些操作將等到先前實例中已經進行的映像操作完成，以避免在同一輸出磁盤上同時創建多個映像的效率低下（這不必要地緩慢並且產生高度碎片化的圖像文件）。其他實例僅等待先前也選中等待複選框的實例，但不會等待其他實例。

取證許可：如果您在過程中取消磁盤映像，X-Ways Forensics 會快速確定 .e01 證據文件格式（更準確地說，當前段）以保證

一致的圖像，即使它不是完整的圖像。例如在緊急情況下在現場對媒體進行成像時很有用，因為可以毫無錯誤地使用的不完整圖像比無法使用的損壞圖像要好。如果啟用散列，不完整的.e01 圖像甚至會有一個散列值，以後可以驗證。

取證許可：對於.e01 證據文件格式，您可以選擇內部塊大小。

可能被某些人認為是有用的，可以為普通數據實現略微更好的壓縮比，但代價是在創建圖像時和以後隨機訪問圖像中的數據時需要更多時間，但對於極度可壓縮的數據（例如擦除或未使用的硬盤區域）。與 32 KB 塊大小相比，512 KB 塊大小在其他條件不變的情況下將具有理想數據（例如，僅 0x00 字節）的圖像大小減少了 40%。針對 32、128 和 512 KB 的塊大小在內部應用了特殊優化。

取證許可證：為圖像生成的描述性文本文件指出原始圖像文件所有段的確切字節大小以及.e01 證據文件所有段中的確切塊數。如果出於某種原因一個或多個段丟失或損壞，這允許創建具有正確容量的人工佔位符段來填充任何空白（使用 File | New 命令），這樣後續段中的所有數據都將具有正確的與前面段中的數據的邏輯距離，以保持數據中指針的有效性（分區表中的分區起始扇區，文件系統數據結構中的簇號），只要包含源和目標的原始圖像文件段可用。

取證許可證：您可以在創建.e01 證據文件時調整壓縮選項。如果您的優先級（更高的壓縮率或更高的速度）發生變化，這很有用，例如，當您發現驅動器空間突然變得稀缺或您必須比以前想像的更快地完成該過程時。當不確定哪個壓縮選項最適合特定系統配置時（例如，在現場對實時系統進行映像並且必須通過 USB 將映像寫入外部硬盤時，I/O 速度很慢並且壓縮比沒有壓縮的整個過程可能更快）。

取證許可：當使用.e01 格式的主動壓縮進行成像時，X-Ways Forensics 會提供有關在磁盤上發現的實際數據量的即時視覺反饋。這是可能的，因為從未寫入的磁盤區域以及已擦除的磁盤區域實現了極高的壓縮率。滾動壓縮比在成像過程中由單獨窗口中的垂直條表示。條越高，該區域的“數據密度”越低。壓縮統計數據也存儲在.e01 證據文件中，因此當您單擊“壓縮”按鈕時，以後任何时候都可以從證據對象屬性對話框中獲得相同的圖表。

取證許可證：能夠指定在創建.e01 證據文件時用於壓縮的額外線程數。默認情況下，X-Ways Forensics 將使用不超過 4 或 8 個，這取決於您的系統有多少處理器內核，但您可以嘗試在具有更多內核的非常強大的系統上增加數量，通常沒有問題，有機會進一步提高速度，或者你可以降低它遇到穩定性問題。

取證許可證：您可以選擇在創建圖像時更改圖像（磁盤或卷）的性質及其扇區大小。這不僅適用於.e01 證據文件，其中

在內部元數據中明確定義（與其他工具兼容），但也適用於原始圖像（通過外部元數據，僅與 X-Ways Forensics/Image v18.4 及更高版本兼容。如果圖像離開 NTFS 文件系統領域，則會丟失）。當數據源不是理想的解釋時很有用。例如，如果重建的 RAID 實際上代表一個卷，而不是物理磁盤，那麼您已經可以在創建它時相應地調整映像的性質。或者，如果重建的 RAID 或盤櫃中的磁盤的扇區大小與分區中的文件系統的扇區大小不匹配，您可以相應地調整鏡像的扇區大小。所有這些都將允許以後更順暢和更成功地使用圖像，特別是那些不太注意圖像類型和扇區大小等細節的用戶。

由於原始圖像存在額外的元數據，X-Ways Forensics 不需要提示用戶圖像的性質及其扇區大小，即使在正常情況下它會提示用戶（例如，因為圖像不是以易於識別的開頭）分區方法或卷引導扇區）。

具有技術頭腦的用戶可能希望為新創建的圖像文件設置所需的屬性，例如“只讀”或“加密”，以及在異常環境（例如“寫入”）中調整性能的緩衝標誌。屬性在<https://docs.microsoft.com/en-us/windows/win32/fileio/file-attribute-constants>, <https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-createfilea>。不應使用“無緩衝”標誌。屬性和標誌通過或運算（或相加）組合在一起，並且必須以十六進製表示法指定。旗幟 在

在成像過程結束時，可以選擇關閉計算機或（如果您的系統支持）休眠以節省電量。如果您選擇休眠並且 Windows 發出休眠失敗的信號，X-Ways Forensics 將改為嘗試關閉系統。

有一個選項可以將新創建的圖像添加到案例中，並在沒有進一步用戶交互的情況下自動開始優化它們的捲快照，如果源磁盤尚未添加到案例中，並且如果案例在您開始時打開成像。

使用此命令是創建磁盤映像的推薦方法。為了對任意範圍的扇區進行成像，您可以選擇一個扇區範圍作為一個塊，然後通過編輯 | 將其複製到一個文件中 | 複製塊 | 進入新文件，或使用工具 | 磁盤工具 | 克隆磁盤。後者對於具有嚴重物理缺陷（不僅僅是普通壞道）的硬盤進行部分映像特別有用，甚至可以倒序複製扇區。

對於成像自動化，請參閱有關命令行參數的章節。

.e01 證據文件中可選擇使用的加密算法是 128 位或 256 位 AES/Rijndael，採用計數器 (CTR) 模式。這允許在證據文件中進行隨機讀取訪問。

128 位實現更新更快，僅受 X-Ways Forensics v16.4 及更高版本支持。加密將使 .e01 證據文件與其他工具不兼容。加密算法使用 256 位密鑰，該密鑰使用 SHA-256 從您指定密碼的 SHA-256 的 512 位串聯和存儲在證據文件的標題。對於 128 位 AES，256 位密鑰通過前半部分和後半部分的異或運算減少為 128 位。128 位計數器是隨機的，每個加密塊遞增，作為 256 位 AES 中的小端整數，作為 128 位 AES 中的大端整數。AES 的加密塊大小為 128 位。額外的

SHA-256 也存儲在標頭中（對於 256 位 AES 是可選的，請參閱安全選項），稍後用於確定用戶指定的用於解密的密碼是否正確。

SHA-256 算法應用於鹽、散列 x 和散列 y 的串聯以計算此密碼驗證散列，其中散列 x 是用戶提供的密碼的 SHA-256，散列 y 是用戶提供的密碼的 SHA-256。對於 128 位 AES， y 變為 x 並一遍又一遍地連接和散列 100,000 次，實際上使彩虹表攻擊在計算上不可行。請注意，當您同時使用壓縮和加密時，.e01 證據文件中的每個塊都會先壓縮，然後再加密。因此，即使壓縮數據已加密，也可能僅根據塊的壓縮大小（即其壓縮率）來判斷給定塊中數據的性質。

如果您讓 WinHex 自動為 WinHex 備份分配文件名，該文件將在備份文件夾中創建（參見常規選項），根據備份管理器的命名約定（“xxx.whx”），並將在備份管理器中可用。如果您明確指定路徑和文件名，您可以稍後使用 Restore Backup 命令恢復備份或映像，並且在拆分備份的情況下，WinHex 會自動將段號附加到文件名。

10.8 虛擬圖像片段

與文件 | 新命令，在 X-Ways Forensics 中，您可以選擇方便地為 .e01 證據文件創建虛擬/臨時片段，以替換丟失/丟失/損壞的原始片段。用戶必須指定所需的塊大小和塊數以及所需段的文件名（必須具有正確的擴展名，標識段號，而不是數字 1）。寫入塊中的數據可以是重複出現的文本模式/水印（“缺少圖像文件段！”），當運行英文版 X-Ways Forensics 時，這樣您就知道在瀏覽解釋後的文件時您正在查看可用數據之間的差距合併後的圖像。但是，出於性能原因，這是可選的。清零塊的生成速度更快。

這種人工虛擬段的想法是，如果正確創建，它可以用作佔位符，確保後續段中的數據與前面段中的數據具有正確的邏輯距離。當然，如果原始數據不存在，則無法再成功驗證整個圖像的哈希值，當然，如果沒有丟失的段文件的備份並且數據不足，則此功能只能作為最後的手段使用恢復失敗等，並且應正確記錄此類虛擬圖像文件段的創建和使用。

在解釋包含虛擬片段的 .e01 證據文件時，您會收到通知，並且在將圖像添加到案例時，佔位符塊的總數會記錄在證據對象屬性中。

如果您需要一個佔位符來表示您不知道塊大小和塊數的單個缺失片段，因為圖像是在沒有包含此信息的描述性文本文件的情況下創建的，我們至少可以想到兩種方法來找出：

1) 將倒數第二個段的文件擴展名更改為缺失段的文件擴展名，以便沒有間隙。然後將最後一段重命名為現在丟失的倒數第二段。（如果丟失的部分實際上是倒數第二個，最後一步就足夠了；如果丟失的是最後一個，則根本不需要重命名。）然後像往常一樣將圖像（第一個部分）添加到 X Ways Forensics 中的案例中。X-Ways Forensics 會在消息窗口中提醒您注意命名錯誤的片段，您可以忽略該片段。檢查塊大小的證據對象屬性以及預期的塊數和實際引用的塊數。從預期的塊數中減去實際引用的塊數。現在你知道有多少塊丟失了。將文件擴展名改回原來的樣子，然後用正確的塊大小、正確的塊數和正確的擴展名創建丟失的虛擬段。

通過變體，如果多個連續段丟失，此方法也適用，只需在第一步中重命名更多可用段以填補空白，然後根據需要創建盡可能多的虛擬段來填補空白。哪個虛擬段準確包含多少代理塊並不重要，只要代理塊的總數必須準確地佔丟失塊的總數即可。

或（不太複雜）

2) 在將缺少片段的圖像添加到案例中時，您已經記下了塊大小。然後，您根據該塊大小快速創建一個非常小的臨時虛擬片段，其中包含任意少量的塊，例如 1000。然後您再次將圖像添加到案例中。

應用程序會通知您缺少多少塊（假設為x），然後您創建包含 $1000+x$ 個塊的最終虛擬段。

如果多個不連續的段丟失，這些方法都不起作用；只能使用 X Ways Forensics 和 X-Ways Imager 生成的描述性文本文件中的詳細信息來創建合適的虛擬片段。

10.9 磁盤克隆、映像、映像恢復提示

使用 WinHex/X-Ways Forensics 進行克隆或成像可製作精確的扇區、法醫聲音副本，包括所有未使用的空間和空閒空間。圖像通常比克隆更可取，因為圖像文件中的所有數據（和元數據，如時間戳）都受到操作系統的保護。

如果您出於備份目的克隆/映像磁盤，請盡量避免在此過程中操作系統或其他程序正在寫入磁盤，例如通過在開始前卸載作為驅動器號安裝的分區。當然，如果您從執行 WinHex/X-Ways Forensics 的位置克隆/映像包含活動 Windows 安裝的磁盤，則此類寫入操作是不可避免的。如果在此過程中正在寫入源磁盤，則從操作系統的角度來看，克隆/映像可能具有不一致的狀態（例如，它可能無法再啟動 Windows 安裝）。然而，從取證的角度來看，在克隆/映像實時系統時，儘管非常希望不發生任何寫入。

更重要的是，這應該不是一個主要問題，因為您仍然可以獲得每個部門的準確快照。

如果克隆或映像恢復的目標是作為驅動器盤符安裝的分區，WinHex 將嘗試清除該目標分區的所有 Windows 內部緩衝區。如果在操作完成後您仍然沒有在目標的 Windows 資源管理器中看到新內容，您可能只需要重新啟動系統。

請注意，WinHex 不會動態更改分區大小並使分區適應比源磁盤更大或更小的目標磁盤。

10.10 骨架圖像

僅限法醫執照。一個典型的 X-Ways 功能鞏固了 X-Ways Forensics 作為工具的地位，在任何可以想像的級別上選擇/定位/過濾數據時給予用戶最大程度的控制：創建取證物理骨架磁盤圖像的能力僅包含某些目的所需的那些扇區，同時保持與其他工具的兼容性。這些可以是具有分區表的扇區、文件系統數據結構、它們的相鄰扇區以及具有文件內容的扇區或未分區的無人區中的任何扇區。骨架圖像通常由稀疏的數據填充，中間有大量區域未定義，因此對其使用 NTFS 稀疏文件技術是有意義的。

稀疏骨架圖像中未寫入的區域在稍後閱讀時就像被清零一樣。如果不是稀疏的，這些區域實際上被清零了。

您可以通過調用 File | 開始骨架成像。創建骨架圖像菜單命令。從那時起哪些扇區將被複製到圖像中是間接定義的，方法是讓 X-Ways Forensics 從源磁盤讀取特定目的所需的那些扇區。當目標圖像在後台打開時，接下來您通常會打開磁盤或分區，或者打開並解釋您希望部分獲取的圖像。這樣它將被自動定義為源，這樣即使在重要的打開或解釋步驟中的讀取操作也已經被觸發，當必須解析分區表和引導扇區時，這些定義分區和標識的基本數據結構文件系統包含在骨架映像中。

所以打開一個分區的物理磁盤後，你的目標鏡像中就有了一個“基本骨架”：分區表指向分區引導扇區或嵌套分區表，其作用是支撐其間的所有其他數據（文件系統數據和用戶數據）。如果您還希望確保可以從骨架映像中獲取某個分區的捲快照，即獲取該分區中文件系統引用的所有文件和目錄的列表，那麼您可以從源中打開該分區硬盤，以便實際拍攝卷快照。同樣，在此過程中從源硬盤讀取的所有扇區都同時複製到映像中，即文件系統數據結構，例如 NTFS 中的 \$MFT，FAT 中的所有目錄簇，以及 HFS+ 中的目錄文件。這會為您的骨架圖像添加相當多的管理數據和元數據，但仍然沒有或幾乎沒有用戶內容。不被文件系統使用的無關扇區不會被讀取，因此不會被複製。這也意味著在骨架圖像中查找以前存在的文件的能力將受到限制。

如果您希望在圖像中包含任意範圍的扇區，您只需要找到一種方法讓 X-Ways Forensics 讀取這些扇區。例如，要包括從數字 1,000,000 到 1,000,999 的扇區，將這 1,000 個扇區定義為一個塊並使用工具 | 散列該塊（在磁盤模式下）計算哈希命令，或僅在該塊中運行物理搜索。或者，要獲得分區 1 和分區 2 之間異常大的分區間隙，您可以散列表示該間隙的虛擬文件。您還可以手動導航到您想要包含的任何單個感興趣的扇區（例如導航 | 轉到扇區）或使用任何文件系統導航菜單命令。所有這一切都有效，因為閱讀部門觸發了他們的收購。

但是，如果您希望專門獲取選定的文件，那會更容易，並且最好關閉間接獲取沿途出於任何目的讀取的任何扇區，這樣對於您預覽的示例文件結果證明是無關緊要的不是預覽操作已經獲得的。為此，您可以使用“文件”菜單中的“狀態”命令將在後台打開的骨架圖像的狀態更改為“空閒”。在“空閒”模式下，只有目錄瀏覽器上下文菜單中的“添加到[骨架圖像的名稱]”命令允許獲取選定的文件（通過臨時激活圖像並觸發讀取操作）。

如果您希望包括一些操作系統文件，例如 Windows 註冊表配置單元，請從根目錄遞歸地探索分區，過濾這些文件並在目錄瀏覽器上下文菜單中調用“添加到”命令。（僅當當時後台沒有打開證據文件容器進行填充時才可用。）只有生成的骨架圖像的檢查員因此能夠查看蜂巢並創建關於它們的註冊報告，假設您已經復制了找出哪些扇區包含文件數據所需的文件系統數據結構。

更改目標圖像狀態的對話窗口也允許您將其關閉，即暫時停止採集或完成圖像。通過使用“創建骨架圖像”命令再次選擇它，可以在以後的任何時間進一步完成相同的骨架圖像，但是您選擇不覆蓋，而是更新它。

如您所見，您可以完全控制將哪些數據放入圖像中。該方法只是假設您對您想要/需要的數據有一定的了解，如果這些數據不存儲在普通的易於選擇的文件中，在哪裡可以找到它/如何物理地獲取它。這些扇區可以按任何順序作為目標。多次讀取相同扇區不會改變骨架圖像中的任何內容，也不會產生負面影響，除非它們可能會導致 X-Ways Forensics 可以生成的可選日誌文件中出現不必要的重複行。這樣的日誌文件創建在與骨架圖像相同的目錄中，並將列出所有被複製的扇區範圍，可選地以及每個扇區範圍的哈希值，這允許在有疑問的情況下手動驗證某些區域中的數據關於它。如果使用“Add to”命令將文件複製到一個骨架鏡像中，每個這樣的文件的名稱也會在日誌中輸出，後面是它對應的扇區範圍（如果文件是碎片的話會多一個）或者如果 X-Ways Forensics 只是選擇以多個塊的形式複制扇區）。

您可能希望將生成的原始骨架圖像轉換為壓縮和/或加密的.e01 證據文件，並在將其傳遞給其他用戶之前使用 WinRAR 或 7-Zip 等對其進行哈希處理或壓縮。如果骨架圖像只是稀疏的，壓縮率會異常高。

填充，並且讀取速度非常快，因為不必從磁盤讀取未定義/未分配的區域。對於您自己的使用，您可以保持原樣，因為由於 NTFS 稀疏存儲，它不會使用標稱文件大小建議的那麼多驅動器空間。如果您希望復制原始骨架圖像，請務必將其複制為稀疏文件（可以在 X-Ways Forensics 中使用工具 | 文件工具 | 複製稀疏命令完成），這樣副本也將是一個稀疏文件，並且只佔用與原始文件一樣多的驅動器空間。傳統的複制命令甚至會將稀疏文件中大量未使用和未分配的區域複製為二進制零。

為了驗證傳輸到骨架圖像的數據沒有改變，可以像普通圖像一樣對這樣的圖像進行整體哈希處理。或者，您可以更快地使用命令“驗證骨架圖像”，根據.log 文件（從骨架圖像讀取）再次僅散列那些實際傳輸的扇區範圍，並將散列值與.log 文件。然後，為了驗證.log 文件沒有改變，它本身將被散列，並將生成的非常有價值的所有包含主散列值與存儲在可選.log.log 文件中的散列值進行比較。如果該文件是創建的，可能需要額外驗證骨架圖像中所有未使用的區域是否仍未分配或至少填充了二進制零。這不是由這個函數完成的。

選項： ·

骨架圖像應創建為 NTFS 稀疏文件，除非您打算複製

可能超過一半的行業（只是一個非常粗略的經驗法則）。

- 如果您沒有讓 X-Ways Forensics 將標稱（邏輯）圖像文件大小設置為源磁盤的完整大小，那麼在解釋骨架圖像並從中讀取時，將報告較小的“容量”，您可能會出現扇區讀取錯誤。仍然值得考慮一下，例如，如果您只想捕獲 1 TB 硬盤的前 1 MB。如果您希望將骨架圖像轉換為.e01 證據文件或希望對其進行整體哈希處理，可以節省大量時間。

- 跳過已經清零的源扇區（源磁盤的僅包含二進制零的扇區）將把這些扇區與未獲取的扇區完全一樣。這會使生成的骨架圖像更小（“更稀疏”），但它會阻止您僅使用骨架圖像顯示這些扇區在源磁盤上僅包含零。它們與未被收購的部門沒有區別。· 當您將目錄瀏覽器上下文菜單的“添加到”命令應用於所選目錄時，“包括文件系統的目錄數據結構”會產生影響。如果選擇此選項，您還將復制這些目錄的文件系統的數據結構，如果有的話，例如 NTFS 中的 INDX 緩衝區，FAT 中的子目錄簇等（HFS+ 中沒有），否則僅複製內容這些目錄中的文件。·

- “報告表關聯”將為您專門添加到源卷快照中骨架映像的每個文件創建一個報告表關聯，以便在有任何疑問時很容易看到哪些文件已經被複製。· 如果“創建日誌文件”至少被選中一半，將創建一個引用所有復制的扇區範圍的.log 文件。X-Ways Forensics 努力防止獲取重複扇區，例如，在第二次復製完全相同的扇區範圍或複制重疊扇區範圍時，這可以解釋為什麼在複制再次相同的部門。如果完全選中該複選框，將創建一個關於.log 文件的.log.log 文件，其中包含.log 文件的哈希值。

- 所有復制的扇區範圍都可以選擇散列，散列值可以寫入

.log 文件，可以在關閉骨架圖像後進行驗證。

- 骨架圖像的好處：
- 部分圖像，
 - 節省驅動器空間。 · 快速創建，尤其是在通過慢速網絡獲取遠程硬盤時
 - 使用 F-Response 連接。
 - 僅傳輸/顯示特定目標數據，排除不相關的數據，因為可能法律、常識、時間壓力或客戶要求的。
 - 非常適合技術數據結構（分區表、文件系統）和文件系統中的文件。 · 無需了解文件系統及其數據結構存儲在哪些扇區，即可獲取所有基本文件系統數據。 · 如果準備充分，結果與磁盤的所有預期目的的傳統原始圖像完全一樣，並保留原始偏移量和數據結構之間的相對距離（與證據文件容器不同）。 · 文件格式是通用的，所有支持原始圖像的取證工具都有機會理解數據，除非他們需要比包含的更多的數據或者已經不理解原始完整磁盤的分區方法或文件系統等/圖片。

注意事項

項： · 請注意，屏幕上帶有搜索命中上下文預覽的搜索命中列表會導致大量讀取活動，因此當骨骼圖像在某些情況下的背景。 · 為避免在分區/卷模式下僅在目錄瀏覽器中單擊的文件或目錄的起始扇區被複製到骨骼圖像（因為這樣的單擊會自動跳轉到相應的第一個扇區），您可以導航目錄瀏覽器相反，在圖例模式下，或者必須將圖像的狀態更改為“空閒”。 · 從大多數提取的文件（如電子郵件消息、附件、視頻靜止圖像、嵌入 MS Excel 電子表格的圖片等）中讀取數據不會觸發磁盤級別的相應讀取操作，因此無法複製它們。骨骼映像僅適用於文件系統級別的文件，不適用於卷快照中看到的任何其他級別的文件。為此目的，請改用證據文件容器。

· 請注意，對於毫無戒心的檢查者來說，骨骼圖像可能看起來非常像普通的完整圖像。必須讓這樣的檢查者意識到圖像的不完整、稀疏的性質。與邏輯證據文件容器不同，其內容不包含在圖像中的文件不會在為不完整物理圖像拍攝的捲快照中被特別標記為此類。如果 X-Ways Forensics v17.1 及更高版本檢測到骨骼圖像，則在將圖像添加到案例時，它會通知檢查員圖像的性質。

可以在[網站上找到證據文件容器和骨架圖像的比較。](#)

片段成像

骨架成像的一種變體稱為“片段成像”。在文件 | 的文件選擇對話框中單擊標有“片段成像”的按鈕Create Skeleton Image 菜單命令啟動

片段成像。當片段成像處於活動狀態時，X-Ways Forensics 從任何磁盤或圖像讀取的任何扇區都被寫入以扇區編號命名的單獨文件中，擴展名為 .sector，位於以扇區命名的圖像默認目錄的子目錄中磁盤或卷。連續的扇區讀取被複製到一個文件中。

片段成像模式可以通過調用文件 | 來停用。片段成像菜單命令。片段成像僅在特定情況下有用，例如用於調試目的，當只需要軟件自動最佳定位的非常特定的扇區時（例如打開特定文件時所需的數據結構）。與骨架成像相比，片段成像可能是有益的，因為不會創建與源磁盤大小相同的圖像文件。（即使它只是標稱大小並且圖像是稀疏的，如果文件需要通過 Internet 發送或複製到不保留文件稀疏性質的文件系統，稀疏也無濟於事。）

由於名稱兼容，片段圖像文件可以直接用於扇區疊加。它們還可以方便地並且由於它們通常很小，可以非常非常快速地恢復到其他磁盤，所有此類文件同時位於同一目錄中，當然要考慮文件名中的扇區號，方法是單擊按鈕文件中的“片段成像” | 恢復圖像對話窗口。

10.11 備份管理器

顯示以前創建的 WinHex 備份列表。這些項目可以按時間順序或字母順序列出。選擇您要還原的備份。該功能完成後，將顯示原始文件或扇區內容。

您可以先將備份恢復到一個臨時文件中，這樣您仍然需要將其保存，直接並立即恢復到磁盤，或者到一個新文件中。

對於磁盤扇區，您可能還希望指定不同的目標磁盤或不同的目標扇區號。也可以只從備份中提取部分扇區。（但是，在恢復過程中不能遺漏壓縮備份開頭的扇區。）如果備份是用校驗和和/或摘要保存的，則在將扇區直接寫入磁盤之前會驗證數據的真實性。

備份管理器還允許刪除您不再需要的備份。WinHex 可以自動刪除由 Undo 命令創建供內部使用的備份（參見 Undo Options）。

備份管理器維護的備份文件位於“常規選項”對話框中指定的文件夾中。它們的文件名為“xxx.whx”，其中xxx是唯一的三位數標識號。該編號顯示在備份管理器列表的最後一列中。

10.12 恢復/複製命令

允許將所選文件從其當前位置複製到標準 Windows 文件對話框可用的位置，例如從解釋的圖像文件或從本地磁盤。這可以應用於現有和已刪除的文件和目錄。非法文件名字符被過濾掉。

如有必要，您可以通過單擊顯示路徑的同一行中的“...”按鈕手動輸入輸出路徑。如果您希望指定 Windows 不會在默認情況下在路徑選擇對話框窗口中列出的網絡位置，則此選項很有用。如果您輸入一個不存在的輸出路徑，您將收到通知並可以繼續，在這種情況下，如果可能，將自動創建該路徑。“...”按鈕旁邊未標記的複選框可用於表示您希望在複製完成後為輸出路徑打開一個 Windows 資源管理器窗口以檢查結果。

取證許可證可提供許多額外功能：

- 可以選擇在輸出目錄中重新創建完整的原始路徑，或者選擇（如果選中一半）僅部分路徑。如果您從案例根目錄中複制，或者如果您沒有 X-Ways Forensics 默認將證據對象文件夾作為輸出目錄（請參閱案例屬性），則證據對象名稱也會成為重新創建路徑的一部分。部分路徑是從當前探索的目錄開始的路徑，或者當從遞歸探索的案例根窗口複制時僅複製證據對象名稱，而不是證據對象內的路徑。
- 支持超長路徑（超過260 個，最多510 個字符，用於輸出路徑+ 可選原始路徑+ 原始文件名）。如果您無法訪問（例如查看、複製或刪除）此類文件，您仍然可以將路徑限制為 260 個字符或更少的普通長度（因為 Windows 7 中的 Windows 資源管理器等普通工具不允許這樣做）。如果所選文件的輸出路徑超出限制，則文件名將被縮短，直到適合為止。如果縮短名稱不利於保持在指定的路徑長度限制內，則不複制該文件，而是將其添加到報表中，以便您以後可以方便地選擇所有省略的文件並根據需要單獨複製它們而無需原始路徑。· 可以在單獨的目錄中創建所有選定文件的第二個副本。如果您需要向兩方提供相關文件的副本並希望節省時間，這很有用。不過，日誌記錄選項僅適用於第一個副本。
- 輸出文件可以在目錄瀏覽器中的任何其他列之後隨意命名，例如唯一 ID、哈希值、ID、註釋、文件系統中的偏移量等。此類元數據信息也可以添加到名稱前或附加到名稱中，例如，它可以與替代名稱、存在狀態、報告表、時間戳、作者、發件人、描述、屬性、分析結果、哈希集等結合使用。

如果單元格文本由多行組成（例如註釋或元數據列），則僅使用第一行。路徑列中的反斜杠會自動替換為下劃線。這允許在其完整的原始路徑之後命名文件。· 無法複製的文件（例如，如果路徑太長）被添加到報告表中。· 如果新識別文件的假定正確文件類型與原始文件名中的擴展名不同，或者文件名沒有任何擴展名，則可以選擇性地附加到輸出文件名。此選項在複製文件以查看它們時也有影響。

相關的程序。

- 除非您選擇覆蓋或跳過輸出目錄中存在的同名文件，否則通過在擴展名前插入遞增數字，重複的文件名將更改為唯一的文件名。因此，如果您將所有文件複製到同一目錄，即使是來自不同證據對象的文件，所有輸出文件名都將是唯一的（並且複制日誌文件允許您稍後找出哪個文件最初是如何命名的，起源於何處以及它具有哪些元數據）。

- 如果“Apply original timestamps to copies”被選中一半，文件系統級別的創建、修改和上次訪問時間戳（如果可用）將重新應用於恢復/複製的文件，加上內部內容創建時間戳（如果可用）可以替代缺少文件系統級創建時間戳。如果完全選中該框，則意味著 X-Ways Forensics 將額外努力設置對某些原始時間戳的創建、修改和最後訪問，以避免這三個標準時間戳中的任何一個都反映使用恢復/複製命令的時間。例如，提取的電子郵件或附件或檔案中的文件或雕刻文件可能沒有全部或任何時間戳。X-Ways Forensics 可能會使用記錄更改時間戳、替代創建時間戳、內容創建時間戳和修改時間戳來替代創建、修改和上次訪問。如果您選中一個額外的框，輸出文件甚至可以繼承父文件和目錄的創建時間戳。如果選中一半，則僅繼承父文件的時間戳（想想包含電子郵件附件的電子郵件或包含縮略圖的圖片）。如果完全選中，時間戳也可以從父目錄（或祖父目錄或曾祖父目錄等）繼承。一個極端的例子是一個完全沒有時間戳的雕刻文件。它的父目錄是虛擬目錄，也沒有原始時間戳。因此，如果可用（不在 FAT 文件系統中），將採用根目錄的創建時間戳。父目錄創建時間戳可以被視為文件的未知創建時間戳的時間順序下限。如果父文件是文件存檔或電子郵件消息，則父文件創建時間戳可被視為文件的未知創建時間戳的上限。如果文件是嵌入在 JPEG 文件中的縮略圖，則父對象的創建時間戳應該完全適合子對象。

- 在處理活動案例時，如果啟用了此命令的特殊日誌記錄，複製/恢復過程將記錄在文件“copylog.html”或“copylog.txt”中。可以記錄所有可用的元數據和輸出文件名（可選地包括目標路徑）。

該文件可以在案例的 _log 子目錄或恢復/複製目標文件夾中創建。比照。也案例屬性。

- 可以選擇將鬆弛空間包含在輸出中，作為文件的一部分或單獨包含，或者可以單獨複製鬆弛空間。

· 您可以選擇是否也複製所選文件的子對象。 · 您還可以選擇是否複製過濾掉的文件。 ·

如果您讓 X-Ways Forensics 為複制的文件重新創建原始路徑，則作為其他文件的子對象的文件的層次結構位置也必須適當地反映出來。這必須在目錄的幫助下發生，因為普通文件系統不支持文件可以包含更多文件的概念，而 X Ways Forensics 中的捲快照是正常的。但是，如果創建一個與父文件同名的人工目錄，則會出現名稱衝突，因為該父文件也可能被選擇進行複制，並且當然會在與上述人工目錄相同的目錄中創建需要反映子對象的路徑。因此，人工目錄的名稱必須略有不同。它可以在用戶定義的數量之後被截斷。

字符，這對於以主題行命名的電子郵件消息尤其有用，當然可以包含作為子對象的附件，以避免路徑過長。此外，您還可以附加一個您選擇的後綴字符（默認情況下，這是一個特殊的 Unicode 字符，在完整的 Unicode 字體中是不可見的，這樣該目錄似乎與相應的父文件具有完全相同的名稱），或者其他一些像“子對象”這樣的描述性詞被附加到名稱中（但不幸的是，這增加了總路徑長度，這往往超過了常見的限制）。如果後綴字符的編輯框看起來是空白的，那很可能是因為前面提到的不可見的 Unicode 字符在那裡。它的寬度為 0。要用任何其他字符替換它，請先刪除不可見字符，方法是單擊編輯框並按鍵盤上的退格鍵。

- 文件可以根據最多兩個選定的目錄瀏覽器列在單獨的輸出目錄中進行分組/分類，例如存在狀態（以便輕鬆區分最初存在的文件和已刪除的文件）、描述、證據對象、文件類型、文件類型描述、文件類型類別、發件人、所有者、哈希集、哈希類別、報告表關聯、搜索詞。也可以將分組目錄名稱限制為一定數量的字符。這可能非常有用，例如為了按年份分組文件（創建或修改時間戳中的前四個字符，給定適當的符號設置）或簡單地將大量輸出文件拆分為大致相等的子目錄（使用哈希值的第一個或兩個字符，對於 16 或 256 個這樣的子目錄），基於大數定律，或者只是為了減少超長路徑的風險。
- 某些受支持類型的文件可以轉換為 PDF 格式，以便與沒有合適的應用程序來查看文件的計算機用戶共享。您可以定義不需要轉換的文件類型，例如可以通過網絡瀏覽器或 Windows 工具輕鬆顯示的文件類型。如果無法進行轉換，則復制原始文件而不進行轉換。還有一個將所有選定文件轉換為單個 PDF 文檔的選項。

這甚至包括通常不會單獨轉換為 PDF 的文件類型。 · · · 可以從某些支持類型的文件中提取純文本並輸出為純文本文件。

這與您從普通預覽模式切換到文本預覽模式時得到的表示相同，並且當您讓 X-Ways Forensics “解碼”文件時，邏輯搜索會看到該文件的相同文本。不適合文本提取的文件（例如圖片文件）或由於任何其他原因無法從中提取文本的文件，如果相應的複選框僅選中一半，則正常複製（及其原始內容），或者如果完全選中則省略（這意味著輸出是 100% 純文本）。

- 如果附件和相應的電子郵件消息（其父項）都被選中進行複制並且未被過濾器排除，則可以選擇將附件作為 Base64 代碼嵌入到生成的輸出.eml 文件中，而不是單獨複製。這有助於查看包括附件在內的完整電子郵件。要查看.eml 文件，您可以使用 Outlook Express、Windows Mail、Windows Live Mail 或 Thunderbird（全部免費）。如果無法嵌入某些附件，您將通過“消息”窗口收到通知，在這種情況下，它們將被單獨複製，就好像沒有選擇嵌入選項一樣。 · NTFS 替代數據流 (ADS) 可以選擇作為 ADS 輸出。默認情況下，它們是

重新創建為普通文件，使它們更容易訪問。

- X-Ways Forensics 可以嘗試在寫入數據時將文件中的歸零區域編碼為稀疏區域。只有當歸零區域稍微對齊且足夠大時，這才會有效果，當然只有在寫入 NTFS 或 ReFS 卷時才會有效果，而不是 FAT。無論如何都有效

源文件是否定義為稀疏文件。此選項會降低數據傳輸速率，僅當您知道您正在複制的數據可能合適時才推薦使用。

- 如果可用，您可以使用文件的替代名稱作為輸出。備用名稱（如果存在）可以在方括號中的目錄瀏覽器中看到。例如，在解析 iPhone 備份時，X-Ways Forensics 會自動將人工通用文件名更改回原來的名稱。或者，當從 Windows 回收站解析 \$I 文件時，相應的 \$R 文件被賦予其原始名稱。如果出於某種原因您在將此類文件從圖像複製到您自己的硬盤時更喜歡未翻譯的文件名，例如因為您希望使用一些需要人工文件名的外部工具來處理這些文件，那麼您現在可以使用此選項。

在搜索命中列表中使用恢復/複製命令時，包含命中的目錄將在輸出文件夾中重新創建為文件，因為用戶可能希望保留包含實際搜索命中的原始數據。從搜索命中列表中，子對象永遠不會與其父對像一起復制。

10月13日 **重複文件檢測**

如果您希望只查看一次重複文件並且文件系統級別的元數據（如時間戳和刪除狀態）是次要的，那麼您可以使用目錄瀏覽器上下文菜單中的“在列表中查找重複項”命令來識別重複文件。所有當前列出的文件都被選中（列出，而不是選擇！）。如果需要，可以在卷快照中自動排除重複項。每組相同文件中只有一個文件不會被排除。可以選擇將每組相同的文件分配給一個唯一的報告表，這使得使用過濾器查看給定組的所有成員變得容易，即使它們包含在不同的證據對像中。

當不確定要排除哪些重複項時，此功能會選擇保留現有（未刪除）文件，而在已刪除文件中，寧願丟棄雕刻文件並保留通過文件系統數據結構找到的文件。當有疑問時，它更願意保留所有者已知的文件的副本。

可選的特殊規則：具有不同附件（子對象）的相同電子郵件將被標記為重複，但不排除。相同的附件（子對象）將被標記為重複，但如果它們是相同電子郵件的一部分並且也被排除，它們將被間接排除。這方便了檢查，也避免了排除一個電子郵件+附件家族的父對象（電子郵件消息）和另一個家族的子對象（附件）的情況。

如果稍後您發現有重複的相關文件並且您也對重複的文件感興趣（希望查看它們的文件名、路徑或時間戳等），您可以例如創建該文件的哈希集以方便且通過將所有文件的散列值與該特定散列集進行匹配並使用散列集過濾器，自動識別所有重複項，或者您可以直接使用散列集過濾器。

同一卷快照中的成對重複項可以選擇性地鏈接為所謂的相關項目，這樣就可以輕鬆地從一個這樣的文件導航到至少一個重複項。然而，這樣做

不能跨證據對象邊界工作。在描述列中將文件標記為重複是可選的。

將文件識別為重複文件的最常見和最可靠的標準是常規哈希值。

然而，在大型數據集中計算哈希值會花費大量時間，因此任何不需要哈希值的合理重複數據刪除選項都有望得到一些用戶的讚賞。

備選標準可用。您可以簡單地根據相同的名稱來比較文件。這是一個不區分大小寫的比較，當然只有當您知道自己在做什麼時才應該使用，因為它根本不比較文件內容。例如，如果您希望刪除備份中發現的相同文件的多個副本，並且不需要保留這些文件的不同版本，這可能很有用。例如，如果在比較之前您按最後修改日期降序排序，這將確保保留文件的最新版本並排除所有舊版本。具有相同名稱的文件不會在 Attr 中標記為重複項。柱子。文件名中要比較的字符數是用戶可定義的。

另一個有用的標準是修改時間戳。時間戳作為字符串進行比較，檢查的字符越多，您要求時間戳相同的精度就越高。

考慮到您的符號設置，您可以通過定義字符數來選擇僅比較日期或日期 + 時間，精度為分鐘、秒、毫秒或介於兩者之間的任何值。立即顯示基於要比較的字符數和當前符號設置的截斷時間戳的外觀示例。請注意，要比較的字符數會限制精度（有意或無意）以及您的符號設置允許的小數位數。例如，即使由於 FAT 時間戳四捨五入，NTFS 和 FAT 文件副本的修改時間相差 1 秒，也可能需要有限的精度來將文件識別為相同。可以直接從重複數據刪除選項對話框中訪問符號設置。

您還可以添加一個或兩個額外的標準來識別重複項：全精度修改時間戳和大小，有用且非常可靠，例如與文件名一起使用。主要標準的另一個選項是結構類型，它實際上識別相似或相關文件的組。結合修改時間和大小，這對於識別重複項也相對可靠，但僅適用於某些文件類型。

如果您可以在 X-Ways Forensics 中訪問 PhotoDNA，您還可以使用 PhotoDNA 識別和排除重複的圖片。所有重複項都可以在“描述”列中標記為“找到重複項”，並且除一個外的所有重複項都將被排除。如有疑問，將排除已刪除的文件或分辨率較差的圖片，並保留現有的分辨率較高的文件和圖片。請注意，如果目錄瀏覽器中列出了許多圖片，哈希值比較可能是一項耗時的操作，比傳統的哈希值要多得多。但是，您可以隨時中止比較。此操作要求事先使用 Specialist | 計算 PhotoDNA 哈希值。優化卷快照 | 圖片處理 | 計算 PhotoDNA 哈希值。例如，對於希望僅創建獨特圖片的 PhotoDNA 哈希集並為此目的維護合法的犯罪圖片集而沒有重複的執法機構來說，它很有用。圖片對比的嚴格程度和 Specialist | 裝置的一樣。優化卷快照 | 用於與 PhotoDNA 哈希數據庫匹配的圖片處理對話窗口。

10.14代理模式

如果程序在讀取磁盤/分區/卷或文件/預覽模式或搜索、散列、成像等數據時遇到問題，問題是它應該向請求者提供數據。對於不同級別的讀取錯誤，它使用不同的代理項/替換字符串（預設文本）。順便說一下，其中許多都依賴於語言。這些字符串被重複複製到讀取緩衝區中，直到它已滿，形成一個重複出現的模式。如果顯示在屏幕上，這種模式很容易在視覺上發現，並且應該很容易引起用戶的注意並讓他或她立即意識到問題所在。

- 1) 例如，“無法讀取文件”意味著至少文件的某些部分/段/範圍無法讀取，因為文件系統沒有定義在哪裡可以找到它們，或者因為它定義了但是該定義無效或者因為它定義了但X-Ways Forensics不理解它。

示例：文件系統定義一個文件由卷中從簇 1000 開始的 6 個簇和卷中從簇 55,555 開始的 4 個簇組成。

此示例中出現“UNABLE TO READ FILE”的一個可能原因是該卷僅包含 40,000 個簇。可以讀取文件的前 6 個簇，但無法讀取文件的後 4 個簇，原因很簡單，因為沒有可以讀取的簇 55,555。如果這涉及現有文件，則說明是某種文件系統損壞或卷不一致。

如果縮小卷時出現問題，或者它是覆蓋多個磁盤的跨卷，其中只有第一個段可用，則可能會被視為整個卷。“無法讀取文件”的另一個可能原因是 X-Ways Forensics 只能部分重建先前存在的文件。大小可以從 \$LogFile 或卷影副本中獲知，文件的前幾個簇可以從源中獲知，但其餘簇的下落可能是未知的。如果它是文件存檔中的壓縮文件，則“無法讀取文件”的另一個可能原因是文件存檔已損壞，因此無法完全讀取包含的壓縮文件。

[更多的](#)

如果是文件系統問題，那麼您可以通過查看定義卷的文件系統數據結構來更準確地找到發生了什麼。用戶通常可以通過右鍵單擊文件、導航 | 輕鬆在 2 秒內找到它們。尋找[數據結構的名稱]。

- 2) “BADEVIDENCEFILE！”指的是.e01 證據文件格式的圖像中的問題。看到這種模式的一個可能原因是請求的扇區包含在壓縮塊（也稱為塊）的第二半中，其中一些位翻轉，因此只有大約前半部分可以成功解壓。

- 3) UNREADABLESECTOR 是在 Options | 中定義的模式。一般，如果無法讀取這些扇區，則始終使用它代替存儲在磁盤扇區中的原始數據，用於所有目的（在屏幕上顯示、成像、克隆、散列、搜索……）。如果您要對具有壞扇區的磁盤進行散列處理，並希望與其他工具比較/重現結果，那麼您可以在此處指定其他工具使用的相同模式。請注意，此類哈希值很難重現，因為在多次嘗試過程中壞扇區可能會成倍增加。如果在嘗試讀取壞扇區時您希望返回零值字節，請完全刪除。

模式（確保編輯框完全空白）。如果保留該模式，將更容易分辨哪些扇區可以讀取，哪些扇區不能讀取，直接在原始硬盤上，當您查看圖像中的相同扇區時也是如此。該硬盤，前提是該模式在使用 X-Ways Forensics 創建圖像時處於活動狀態。例如，硬盤上的壞扇區的內部 CRC 不再與該扇區中的有效負載數據匹配。

4) 其他替代模式是“缺少圖像文件段！”、“IMG 結束”和“無法讀取的頁面”，所有這些基本上都應該是不言自明的。（“頁面”指的是內存頁面。）

10.15 重建 RAID 系統

WinHex 和 X-Ways Forensics 可以在內部對 RAID 級別 0、5、5EE 和 6 系統以及由多達 16 個組件組成的 JBOD 進行條帶化處理。對於硬件 RAID，這些組件可能是物理硬盤或物理磁盤映像，對於 Linux 軟件 RAID，這些組件可能是分區。

在使用此功能之前，需要打開和解釋以圖像形式提供的組件。需要先打開作為分區的組件，然後才能進行 RAID 重建。

您需要以正確的順序選擇組件。WinHex 允許您指定扇區中的條帶大小（通常為 128 或至少 2 的幕，如 32、64、256）和每個組件的不同 RAID 標頭大小（通常僅為 0）。條帶大小乘以 RAID 組件磁盤的數量得出所謂的條帶大小，即整行。

標頭是組件磁盤開始處的保留區域，某些 RAID 控制器為它們的私有數據預留了該區域，因此必須從重建中排除。如果在組件磁盤的末尾有一些保留扇區，這對於 JBOD 來說並不罕見，那麼在重建之前，您可以通過工具 | 為每個組件指定實際使用的扇區數和標頭大小。磁盤工具 | 將磁盤參數設置為“扇區數”。

當未檢測到分區或分區包含未知文件系統或文件系統無法正確解釋時，您通常可以判斷組件順序、條帶大小、條帶模式或 RAID 標頭大小選擇不正確。

當您將重建的 RAID 系統添加到案例（以及從此類 RAID 系統打開的可選分區）時，選定的 RAID 配置參數將與證據對像一起保存，這允許在以後的會話中立即訪問 RAID 系統（僅限取證許可）。

在 RAID 級別 5 和 6 中，數據不僅以旋轉模式跨所有組件磁盤條帶化，而且還散佈有奇偶校驗塊以實現冗餘。RAID 級別 5 和 6 由不同的 RAID 控制器製造商以不同的方式實現，因為它們採用不同的條帶/奇偶校驗模式。支持的模式如下：

級別 5：向後奇偶校驗又名左異步 (Adaptec)

組件 1 :1 3 P
組件 2 :2 P 5
第 3 部分 :P 4 6

級別 5 :後向動態奇偶校驗又名左同步 (AMI 和 Linux 標準)

組件 1 :1 5 9 P
組件 2 :2 6 P 10
第 3 部分 :3 P 7 11
組件 4 :P 4 8 12

第 5 級 :向後延遲奇偶校驗 (HP/Compaq)

組件 1 :1 3 5 7	9 11 13 15
分量 2:2 4 6 8	P 購買力平價
第 3 部分 :PPPP	10 12 14 16

級別 5 :前向奇偶校驗 (又名右異步)

組件 1 :P 3 5
組件 2 :1 P 6
組件 3 :2 4 P

級別 5 :前向動態奇偶校驗 (又名右同步)

組件 1 :P 6 8 10
組件 2 :1 P 9 11
第 3 部分 :2 4 P 12
組件 4 :3 5 7 P

級別 5 :前向延遲奇偶校驗

級別 5 :前向動態延遲奇偶校驗 (CRU/數據端口)

5EE 級 :向後平價 (Adaptec)
組件 1 :1 3 SP
組件 2 :2 SP 7
組件 3 :SP 5 8
組件 4 :P 4 6 S (S = 備用)

5EE 級 :正向平價
組件 1 :1 個 PS 7
組件 2 :2 3 PS
組件 3 :S 4 5 P
組件 4 :PS 6 8

級別 6 :向後奇偶校驗 (Adaptec/JetStor)

組件 1 :1 3 PQ
組件 2 :2 PQ 7
組件 3 :PQ 5 8
組件 4 :Q 4 6 P

級別 6 :後向動態平價
組件 1 :1 4 PQ
組件 2 :2 PQ 7
組件 3 :PQ 5 8

組件 4 :Q 3 6 P

級別 6 :前向延遲奇偶校驗

級別 6 :正向平價

對於許多 RAID 變體 ,如果需要 ,可以不同地定義奇偶校驗起始組件 。要堅持選擇標準模式 ,將該值保留為 0 。為了定義非標準奇偶校驗起始組件 ,請指定奇偶校驗首先位於的組件編號 (基於 1) 。

HP/Compaq 控制器上奇偶校驗移動的延遲通常為 4 或 16 ,但可自由配置 。

如果其中一個 RAID 組件磁盤不可用 ,您仍然可以重建 RAID 5 系統 ,因為一個組件是冗餘的 。只需選擇一個虛擬替代品 (同一 RAID 系統的其他可用組件之一) 作為丢失的組件 ,並聲明該組件 “丢失” ! RAID 5EE 和 RAID 6 也可以在缺少一個組件的情況下進行內部重建 。

支持軟件 RAID

Linux MD RAID 容器分區會被自動識別 。它們表示為兩個不同的項目 :一個靜態標頭區域 ,其中包含有關 RAID 的一般元數據和特定的以下組件 ,通常位於相對偏移量 4096 處 ,以及一個用作 RAID 組件的可探索分區 。在 RAID 級別 1 的情況下 ,可探索分區包含一個完全獨立的捲 ,如果支持 ,其文件系統可以正常解析 (無需任何重建工作) 。在其他 RAID 級別的情況下 ,可以使用 Specialist | 完成重建 。Reconstruct RAID 命令 ,一些關於正確重建參數的提示顯示為附加到標題區域項的註釋 。請注意 ,您需要先打開所有相關分區 ,以便將它們提供給選擇作為 RAID 的組件 。重建的結果將是單個卷 ,表示為包含在虛擬物理磁盤中 。由於內部原因 ,RAID 組件必須保留在案例中作為證據對象 ,以便稍後通過單擊鼠標重新打開重建的 RAID 。

Windows 存儲池容器分區也被自動識別 ,並且可以正確打開其扇區大小是底層物理磁盤扇區大小的倍數的分區 。這對於 Windows 存儲空間池磁盤中的 Windows 存儲空間分區很重要 。這些分區和磁盤的模擬扇區大小為 4 KB ,即使它們駐留在扇區大小為 512 字節的物理磁盤上也是如此 。搜索丢失分區可以在存儲空間容器分區中找到 NTFS 存儲空間分區 ,儘管扇區大小存在差異 ,這對於簡單的單磁盤存儲空間來說是一種有用的解決方法 。

附錄 A :模板定義

1 個標題

模板定義的標頭具有以下格式：

模板 “標題” [描述 “描述”] [applies_to (文件/磁盤/RAM)]
[fixed_start偏移量] [扇區對齊] [需要偏移量 “十六進制值”] [big-endian] [十六進制/八進制]
[read-僅] [多個[固定整體尺寸]]

//將任何一般性評論放在此處的模板中。開始變量聲明

結尾

括號中的標籤是可選的。標籤的順序無關緊要。如果表達式包含空格字符，則只能用引號括起來。註釋可以出現在模板定義中的任何地方。雙斜杠後面的字符將被解析器忽略。

關鍵字apply_to必須後跟一個且僅一個單詞文件、磁盤或RAM。如果您要對來自不同來源的數據使用模板，WinHex會發出警告。

雖然默認情況下模板在應用時開始解釋當前光標位置的數據，但可選的fixed_start語句確保解釋始終從文件或磁盤內指定的絕對偏移量開始。

如果模板適用於磁盤，則關鍵字扇區對齊可確保模板解釋從當前扇區的開頭開始，而不管光標的確切位置如何。

與apply_to語句類似，requires語句使WinHex能夠防止將模板定義錯誤地應用於不匹配的數據。指定一個偏移量和一個任意長度的十六進制值鏈，用於標識模板定義所針對的數據。例如，有效的主引導記錄可以通過偏移量0x1FE處的十六進制值55 AA識別，可執行文件通過偏移量0x0處的十六進制值4D 5A（“MZ”）識別。一個模板定義頭中可能有多個requires語句，這些都考慮在內。

關鍵字big-endian導致模板定義中的所有多字節整數和布爾變量以big-endian順序讀取和寫入（高位字節在前）。

關鍵字hexadecimal導致模板定義中的所有整數變量是

以十六進製表示法顯示。

關鍵字read-only確保模板只能用於檢查，而不能操作數據結構。模板中的編輯控件將變灰。

如果在標題中指定了關鍵字multiple，則WinHex允許在顯示模板時瀏覽到相鄰的數據記錄。這要求WinHex知道記錄的大小。如果未將其指定為multiple語句的參數，則WinHex假定模板結構(record)的總體大小是模板解釋末尾的當前位置減去基本編輯位置。如果這是可變大小，即數組大小或移動參數由變量值動態確定，則WinHex無法瀏覽到先例數據記錄。

2 正文：變量聲明

模板定義的主體主要由變量聲明組成，類似於編程語言中的變量聲明。聲明具有基本形式

輸入“標題”

其中type可以是以下之一：

- int8, uint8 = byte, int16, uint16, int24, uint24, int32,
 uint32, uint48, 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,
· GUID

如果標題包含空格字符，則只能用引號括起來。標題不能只包含數字。WinHex不區分標題中的大小寫字符。最多使用41個字符來標識一個變量。

type前面最多可以有以下每個修飾符組的一個成員：

big-endian 十六進制 只讀本地	little-endian 十進制讀寫	八進制
-------------------------	---------------------	-----

這些修飾符只影響緊隨其後的變量。如果他們

已經出現在標題中。“本地”將除 DOSDateTime 之外的時間戳從 UTC 轉換為在常規選項中指定的時區。

類型名稱末尾的數字表示每個變量（字符串：每個字符）的大小（以位為單位）。使用 char16 和 string16，WinHex 支持 Unicode 字符和字符串。但是，不支持前 256 個 ANSI 等效字符以外的 Unicode 字符。可以使用模板編輯的最大字符串大小為 8192 字節。

string、string16 和 hex 類型需要一個額外的參數來指定元素的數量。該參數可以是常量或先前聲明的變量。如果是常量，可以用十六進制格式指定，如果數字前面有 0x 就可以識別。

您可以通過將數組大小放在類型或標題旁邊的方括號中來聲明變量數組。指定“unlimited”作為數組大小，使模板僅在遇到文件末尾時停止。以下兩行聲明了一個動態大小的 ASCII 字符串，其長度取決於前面的變量：

```
uint8 len char[len] —  
個字符串
```

同樣可以通過以下兩個聲明來實現：

```
byte len string len —  
個字符串
```

字符“~”可以用作佔位符，以便稍後用實際的數組元素編號替換（見下文）。這不適用於 char 變量數組，因為它們會自動轉換為字符串。

字符串、字符串16和十六進制變量的數字參數以及數組大小表達式可以用數學符號指定。它們將由集成的公式解析器處理。此類表達式需要括在括號中。它們不得包含空格字符。

它們可以使用先前聲明的整數變量，其名稱也不包含空格字符。支持的運算有加法 (+)、減法 (-)、乘法 (*)、整數除法 (/)、模除法 (%)、按位與 (&)、按位或 (|) 和按位異或 (^)。有效的數學表達式例如 $(5*2+1)$ 或 $(len1/(len2+4))$ 。結果總是一個整數，而且必須是正數。

zstring 和 zstring16 是以 null 結尾的字符串，其大小在運行時動態確定。

3 正文 : 高級命令

當用大括號括起來時，幾個變量聲明組成一個塊，可以作為一個整體重複使用。但是請注意，塊不能嵌套在當前

執行。字符~可以在變量名稱中用作佔位符，以便稍後用實際重複計數替換。可選的編號語句定義從哪裡開始計數（默認為0）。

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

在此示例中，模板中的實際變量名稱將是“String No. 1”、“String No. 2”、...、“String No. 10”。除了固定的重複次數（本例中為10次），您還可以指定“無限制”。在這種情況下，WinHex 將重複該塊，直到遇到文件末尾。“ExitLoop”可用於隨時跳出循環。“退出”完全終止模板的執行。

“IfEqual”對於比較兩個表達式很有用。操作數既可以是數值，也可以是十進製表示法中的常量值、整數變量或公式，也可以是作為文本或十六進制值給出的字節序列，逐字節進行比較。ASCII 字符串表達式必須用引號引起來，十六進制序列必須以“0x”標識符開頭。

公式需要用括號括起來。

{ 字節	價值
如果等於值 1	
退出循環	
結束如	
果 } [10]	

“IfEqual”命令塊以“EndIf”語句終止。如果比較的表達式相等，則模板解釋在“IfEqual”之後繼續。可選地，“IfEqual”後面可以跟一個“Else”語句。如果表達式不相等，模板處理器分支到“Else”塊。“IfEqual”命令不得嵌套。“IfGreater”類似於“IfEqual”。如果第一個表達式大於第二個，則條件為真。字符串和十六進制值按字典順序進行比較。

為了便於閱讀和瀏覽模板，您可以在對話框中定義由空格分隔的變量組：

部分	“.....章節標題.....”
...	
結束部分	

section、endsection和numbering語句不會推進要解釋的數據中的當前位置。

有兩個命令也沒有聲明變量，但明確用於改變當前位置。這樣做可以跳過不相關的數據（向前移動）或能夠多次訪問某些變量作為不同類型（向後移動）。使用move n語句從當前位置跳過n個字節，其中n可能為負數。goto n導航

從模板解釋開始到指定的絕對位置（必須為正）。`gotoex n`跳轉到基於數據窗口開始的指定絕對位置（例如文件或磁盤）。

以下示例演示瞭如何以 32 位整數和由四部分組成的十六進制值鏈的形式訪問變量：

int32 移動 -4 十六進制 4	“磁盤序列號（十進制）”
	“磁盤序列號（十六進制）”

4 主體：靈活的整型變量

模板支持的一種特殊變量類型是 `uint_flex`。這種類型允許以任意順序從 32 位（4 字節）範圍內的各個位組成無符號整數值，甚至比 C 編程語言中所謂的位字段更靈活。

`uint_flex` 需要一個用逗號分隔的附加參數字符串，該字符串準確指定以何種順序使用哪些位，以逗號分隔。首先列出的位成為結果整數中的最高有效位（高值位），並且它不被解釋為 + 或 - 指示符。最後列出的位成為結果整數中的最低有效位。

這些位從 0 開始計數。位 0 是第一個字節的最低有效位。

第 31 位是第四個字節的最高有效位。因此，該定義是基於小端哲學。

例如 `uint_flex`

`15,14,13,12,11,10,9,8,7,6,5,4,3,2,1,0` 標準 16 位整數 與 `uint16` 完全一樣，常見的無符號 16 位整數變量。

`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` 與 `uint32` 完全一樣，都是普通的無符號 32 位整型變量。

不過，`uint_flex` 的好處是可以任意選擇所有位的數量、位置和使用順序。例如，`uint_flex “7,15,23,31”` “一個不尋常的 4 位整數” 從所涉及的四個字節中的每一個的相應最高有效位組成一個 4 位整數。如果這四個字節恰好是 F0 A0 0F 0A = 11110000 10100000 00001111 00001010，則第 7 位為 1，第 15 位為 1，第 23 位為 0，第 31 位為 0。

所以得到的 `uint_flex` 是 $1 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 0 \cdot 1 = 12$ 。

附錄 B :腳本命令

腳本命令不區分大小寫。註釋可以出現在腳本文件的任何位置，並且必須以兩個斜線開頭。參數最長可達 255 個字符。如果因為十六進制值、文本字符串（甚至整數）被接受為參數而有疑問，您可以使用引號來強制將參數解釋為文本。如果文本字符串或變量名稱包含一個或多個空格字符，則需要使用引號，以便將其間的所有字符識別為構成一個參數。如果引號內的文本是已定義變量的名稱，則該變量將用作參數。

無論在何處需要數字參數（整數），集成的公式解析器都允許您使用數學表達式。此類表達式需要括在括號中。

它們不得包含空格字符。他們可能會使用可以解釋為整數的變量。支持的運算有加法 (+)、減法 (-)、乘法 (*)、整數除法 (/)、模除法 (%)、按位與 (&)、按位或 (|) 和按位異或 (^)。有效的數學表達式例如 (5*2+1)、(MyVar1/(MyVar2+4)) 或 (- MyVar)。

以下是當前支持的腳本命令的說明，包括示例參數。

Create D:\My File.txt 1000創建

初始文件大小為 1000 字節的指定文件。如果該文件已經存在，它將被覆蓋。

打開 “D:\My File.txt”

打開 “D:*.txt”

打開指定的文件。指定”？”作為參數讓用戶選擇要打開的文件。

Open C:

Open D:打

開指定的邏輯驅動器。指定”：？”作為參數讓用戶選擇要打開的邏輯驅動器或物理磁盤。

Open 80h

Open 81h

Open 9Eh打

開指定的物理媒體。軟盤編號以 00h 開頭，固定和可移動驅動器編號以 80h 開頭，光介質編號以 9Eh 開頭。

或者，您可以使用 Open 命令傳遞第二個參數，該參數定義打開文件或媒體的編輯模式（“就地”或“只讀”）。

CreateBackup創

建活動文件當前狀態的 WHX 備份。

CreateBackupEx 0 100000 650 true F:\My backup.whx

創建活動磁盤的 WHX 備份，從扇區 0 到扇區 1,000,000。備份文件將自動拆分為 650 MB 大小。啟用壓縮（“真”）。輸出文件指定為最後一個參數。

如果不應拆分備份文件，請將第三個參數指定為 0。要禁用壓縮，請指定 “false”。要讓備份管理器自動分配文件名並將文件放在備份文件的文件夾中，請將 “” 指定為最後一個參數。

Goto 0x128

Goto MyVariable 將當

前光標位置移動到十六進制偏移量 0x128。或者，現有變量（最大 8 個字節）也可以解釋為數值。

Move -100 將

當前光標位置向後移動 100 個字節（十進制）。

寫 “測試”

Write 0xD0A

Write MyVariable 在當前

位置寫入四個 ASCII 字符 “Test” 或兩個十六進制值 “0D0A”（在覆蓋模式下）。也可以寫入指定為參數的變量的內容。

將當前位置向前移動寫入的字節數。當到達文件末尾時，為完成此操作，將附加一個空字節。有用的是，進一步的寫入命令不會覆蓋前一個寫入命令寫入的最後一個字節。

Write2 與

Write 相同，但如果已到達文件末尾則不附加空字節。因此假設 Write2 總是將當前位置向前移動寫入的字節數是不安全的。

插入 “測試”

功能與 “寫入” 命令相同，但處於插入模式。只能與文件一起使用。

Read MyVariable 10 從當前

位置讀取 10 個字節到名為 “MyVariable”的變量中。如果此變量尚不存在，則會創建它。最多允許 48 個不同的變量。另一種創建變量的方法是 Assign 命令。

ReadLn MyVariable 從當前

位置讀入名為 “MyVariable”的變量，直到遇到下一個換行符。如果變量已經存在，它的大小將相應地調整。

關閉關

閉活動窗口而不保存。

CloseAll 關

閉所有窗口而不保存。

保存

在活動窗口中保存對文件或磁盤的更改。

另存為 “C:\新名稱.txt”

將文件保存在指定路徑下的活動窗口中。指定”？”作為讓用戶選擇目的地的參數。

SaveAll

保存所有窗口中的更改。

終止中止腳

本執行。

Exit

終止腳本執行並結束 WinHex。

ExitIfNoFilesOpen如

果沒有文件已經在 WinHex 中打開，則中止腳本執行。

塊 100 200 塊 “我

的變量 1” “我的變量 2”

定義活動窗口中從偏移量 100 到偏移量 200 (十進制)的塊。

或者，現有變量 (每個最多 8 個字節)可以解釋為數值。

Block1 0x100定

義從十六進制偏移量 0x100 開始的塊。變量也可以作為參數。

Block2 0x200

將塊結束定義為十六進制偏移量 0x200。變量也可以作為參數。

Copy

將當前定義的塊複製到剪貼板。如果沒有定義塊，它的工作方式與“編輯”菜單中的“複製”命令相同。

Cut

從文件中剪切當前定義的塊並將其放入剪貼板。

Remove

從文件中移除當前定義的塊。

CopyIntoNewFile D:\New File.dat

CopyIntoNewFile D:\File +MyVariable+.dat

將當前定義的塊複製到指定的新文件中，而不使用剪貼板。如果沒有定義塊，它的工作方式與“編輯”菜單中的“複製”命令相同。可以復制磁盤

扇區和文件。允許在參數中使用無限數量的“+”連接。如果變量名稱不大於 2^{24} (~16 Mio.)，則將被解釋為整數。用於循環和文件恢復。

粘貼將

當前剪貼板內容粘貼到文件中的當前位置，而不更改當前位置。

WriteClipboard 通

過覆蓋當前位置的數據，將當前剪貼板內容寫入文件或磁盤扇區中的當前位置，而不更改當前位置。

Convert Param1 Param2 將

活動文件中的數據從一種格式轉換為另一種格式。有效參數是 ANSI、IBM、Binary、HexASCII、IntelHex、MotorolaS、Base64、UUCode、LowerCase、UpperCase 和 hiberfil，以及從 Convert 菜單命令中得知的組合。

AESEncrypt “我的密碼”

使用 AES 使用指定的密鑰（最多 32 個字符）加密活動文件或磁盤，或其中的選定塊。

AESDecrypt “我的密碼”

解密活動文件或磁盤。

查找“John” [MatchCase MatchWord Down Up BlockOnly SaveAllPos Unicode 通配符]

查找 0x1234 [Down Up BlockOnly SaveAllPos Wildcards]

在活動窗口中分別搜索名稱 John 或十六進制值 0x1234，並在第一次出現時停止。其他參數是可選的。默認情況下，WinHex 搜索整個文件/磁盤。可選參數的工作方式與通常的 WinHex 搜索選項相同。

ReplaceAll Jon Don [MatchCase MatchWord Down Up BlockOnly Unicode 通配符]

ReplaceAll 0x0A 0x0D0A [向下向上 BlockOnly 通配符]

用其他內容替換活動文件中所有出現的字符串或十六進制值。如果處於就地模式，則只能應用於磁盤。

IfFound

一個布爾值，取決於最後一個 Find 或 ReplaceAll 命令是否成功。放置在 IfFound 命令之後發現某些內容時應執行的命令。

IfEqual MyVariable “你好世界”

IfEqual 0x12345678 我的變量

如果等於我的變量 1000

IfEqual MyVariable MyOtherVariable

IfEqual MyVariable (10*MyOtherVariable)

比較兩個數字整數值（每個都是常量值、整數變量或數學表達式）或兩個變量、ASCII 字符串或十六進制值

二進制級別。比較具有不同長度的二進製文件中的兩個對象總是返回 False 作為結果。如果相等，將執行以下命令。If 條件不得嵌套。

```
IfGreater MyVariable "你好世界"
IfGreater 0x12345678 MyVariable IfGreater
MyVariable 1000 IfGreater MyVariable
MyOtherVariable IfGreater MyVariable (10*MyOtherVariable)
```

接受與 IfEqual 相同的參數。如果第一個大於第二個，將執行以下命令。If 條件不得嵌套。

Else可

能發生在 IfFound 或 IfEqual 之後。在 Else 命令之後放置如果未找到任何內容或比較的對像不相等時應執行的命令。

EndIf結

束條件命令執行（在 IfFound \IfEqual \IfGreater 之後）。

```
{...
退出循環...}
```

退出循環。循環由大括號定義。右大括號後面可以跟方括號中的整數，它確定要執行的循環數。這也可以是變量或關鍵字“unlimited”（因此只能使用 ExitLoop 命令終止循環）。循環不得嵌套。

循環示例：Write

Loop }[10] 會將單詞“Loop”寫十次。

標籤 ContinueHere

創建一個名為“ContinueHere”的標籤

JumpTo ContinueHere 使用該標

籤後面的命令繼續執行腳本。

NextObj循

環切換到下一個打開的窗口並使其成為“活動”窗口。例如，如果打開了 3 個窗口，並且窗口 #3 處於活動狀態，則 NextObj 將使 #1 成為活動窗口。

ForAllObjDo以下腳

本命令塊（直到發生 EndDo）將應用於所有打開的文件和磁盤。

CopyFile C:\A.dat D:\B.dat 將 C:\A.dat

的內容複製到文件 D:\B.dat 中。

移動文件 C:\A.dat D:\B.dat

將文件 C:\A.dat 移動到 D:\B.dat。

DeleteFile C:\A.dat 令

人驚訝的是，刪除了 C:\A.dat。

InitFreeSpace

InitSlackSpace 使用

當前設置的初始化設置分別清除當前邏輯驅動器上的可用空間或空閒空間。 InitSlackSpace 暫時將驅動器切換到就地模式，從而保存所有未決的更改。

InitMFTRecords 使用當

前設置的初始化設置清除當前邏輯驅動器上未使用的 MFT 文件記錄（如果它使用 NTFS 格式化）。在其他文件系統上什麼都不做。更改會立即寫入磁盤。

分配 MyVariable 12345 分配

MyVariable 0x0D0A 分配 MyVariable

“我喜歡 WinHex”

Assign MyVariable MyOtherVariable 將指定的整數、二

進制數據、ASCII 文本或其他變量的內容存儲在名為 “MyVariable”的變量中。如果此變量尚不存在，則會創建它。其他創建變量的方法：例如 Read、GetUserInput、IntToStr。最多允許同時存在 48 個不同的變量。

Release MyVariable 專門處理

一個現有的變量。僅在腳本執行過程中使用超過 48 個不同名稱的變量時才強制調用，以便銷毀更早不再需要的變量。

SetVarSize MyVariable 1 SetVarSize

MyVariable 4 確定設置變量在給定時

間分配的內存大小，以字節為單位。這對於保存整數值和計算結果的變量很有用，如果要將此值寫入具有固定長度結構的二進製文件。如果沒有 SetVarSize，則不必對變量的大小做出任何假設。例如，數字 300 可以存儲在大於 1 的任意字節數中。如果 SetVarSize 設置的新大小小於舊大小，則分配的內存將被截斷。如果新大小更大，則分配的內存會擴大。無論如何，持久字節的值被保留。

GetUserInput MyVariable 請輸入您的姓名：

將用戶在腳本執行時指定的 ASCII 文本或二進制數據 (0x...)（最多 128 字節）存儲在名為 “MyVariable”的變量中。您作為第二個參數提供的消息會提示用戶。如果該變量尚不存在，則會創建它。其他創建變量的方法：Assign、Read。

GetUserInputI MyIntegerVariable 請輸入您的年齡：

與 GetUserInput 類似 ,但只接受和存儲整數。

Inc MyVariable將

變量解釋為整數 (如果不大於 8 個字節)並將其遞增 1 。對循環很有用。

Dec MyVariable將

變量解釋為整數 (如果不大於 8 個字節)並將其遞減 1 。

IntToStr MyStr MyInt

IntToStr MyStr 12345將指

定為第二個參數的整數的十進制 ASCII 文本表示形式存儲在指定為第一個參數的變量中。

StrToInt MyInt MyStr將第

二個參數中指定為十進制 ASCII 字符串的整數的二進製表示形式存儲在指定為第一個參數的變量中。

StrCat MyString MyString2

StrCat MyString “.txt”

將一個字符串附加到另一個字符串。第二個參數可以是變量或常量字符串。第一個參數必須是一個變量。結果將保存在第一個參數指定的變量中 ,並且不得超過 255 個字符。

GetClusterAlloc MyStr可應

用於邏輯卷 。檢索當前位置分配的文本描述 ,例如哪個文件存儲在當前簇中 ,並將該描述保存在指定變量中。

GetClusterAllocEx IntVar可應

用於邏輯卷 。檢索一個整數值 ,該值指示當前位置的簇是否已分配 (1) 或未分配 (0) ,並將該描述保存在指定變量中。

GetClusterSize IntVar可應

用於邏輯卷 。檢索簇大小並將該值保存在指定的整數變量中。

InterpretImageAsDisk將

原始圖像或證據文件視為原始物理磁盤或分區。需要專家或法醫執照。

CalcHash HashType MyVariable

CalcHashEx HashType MyVariable計算從

“工具”菜單中的命令已知的散列 ,並將其存儲在指定的變量中 (如果尚不存在 ,將創建該變量) 。 HashType 參數必須是以下之一 :CS8 、CS16 、CS32 、CS64 、CRC16 、CRC32 、MD5 、SHA-1 、SHA-256 、PSCHF 。

CalcHashEx 還在對話窗口中顯示散列。

消息框 “警告”

顯示一個帶有文本 “警告”的消息框，並為用戶提供一個確定和一個取消按鈕。

按取消按鈕將中止腳本執行。

執行腳本 “腳本名稱”

在當前執行點從正在運行的腳本中執行另一個腳本，例如，取決於條件語句。可以嵌套調用其他腳本。調用的腳本完成後，將使用下一個命令恢復原始腳本的執行。此功能可以幫助您更清晰地構建腳本。

Turbo On

Turbo Off 在

turbo 模式下，大多數屏幕元素在腳本執行期間不會更新，您無法中止（例如，通過按 Esc）或暫停。如果在循環中執行大量簡單命令（如 Move 和 NextObj），這可能會加速腳本執行。

調試以

下所有命令必須由用戶單獨確認。

UseLogFile錯

誤消息被寫入臨時文件文件夾中的日誌文件“Scripting.log”。這些消息不會顯示在需要用戶交互的消息框中。在無人值守的遠程計算機上運行腳本時尤其有用。

CurrentPos

GetSize

unlimited 是

用作佔位符的關鍵字，可用於需要數字參數的地方。

在腳本執行時，CurrentPos 代表活動文件或磁盤窗口中的當前偏移量，GetSize 代表其大小（以字節為單位）。unlimited 實際上代表數字 2,147,483,647。

附錄 C :主引導記錄

主引導記錄位於硬盤的物理開頭，可使用磁盤編輯器進行編輯。它由一個主引導加載程序代碼（446 字節）和四個後續的、結構相同的分區記錄組成。最後，十六進制簽名 55AA 完成了一個有效的 Master Boot Record。

分區記錄的格式如下：

偏移大小	說明8 位	值 80 指定活動
0	分區。	8 位分區起始頭
...		

2個	8 位分區起始扇區 (位 0-5) 8 位分區起始磁道 (“起始扇區”中的位 8,9 作為位 6,7) 8 位操作系統指示器 , 見下文 8 位分區
3 4	結束頭
5個	
6個	8 bit Partition end sector (bits 0-5) 8 bit
前的扇區	Partition end track (bits 8,9 in end sector as bits 6,7) 7 8 32 bit 分區
C 32 位扇區分區長度	

操作系統指標 : (十六進制 , 不完全列
表)

00 空分區表條目	01 DOS 12 位 FAT 04
DOS	16 位 FAT (最大 32M)
05 DOS 3.3+擴展分區	06 DOS 3.31+大文件系統 (16位FAT , 超過32M)
07 Windows NT NTFS, OS/2 HPFS, Advanced Unix	08 OS/2 v1.0-1.3, AIX 可啟動分區, SplitDrive
管理器	09 AIX 數據分區
0B Windows 95 with 32-bit FAT	
0C 帶有 32 位 FAT 的 Windows 95 (使用 LBA 模式 INT 13 擴展)	
0E 邏輯塊可尋址 VFAT (與 06 相同 , 但使用 LBA 模式 INT 13)	
0F 邏輯塊可尋址 VFAT (與 05 相同 , 但使用 LBA 模式 INT 13)	
17 隱藏的 NTFS 分區	
1B 隱藏 Windows 95 FAT32 分區	
1C 隱藏 Windows 95 FAT32 分區 (使用 LBA 模式 INT 13 擴展)	
1E 隱藏的 LBA VFAT 分區	
42 動態磁盤捲	
50 OnTrack 磁盤管理器 , 只讀分區	
51 OnTrack 磁盤管理器 , 讀/寫分區	
81 Linux	
82 Linux 交換分區 , Solaris (Unix)	
83 Linux 原生文件系統 (ext2fs/xiafs)	
84 休眠分區	
85 Linux 擴展	
86 FAT 16 卷/條帶集 (Windows NT)	
87 HPFS容錯鏡像分區 , NTFS卷/條帶集	
A0 筆記本電腦休眠分區	
BE Solaris 引導分區	
C0 DR-DOS/Novell DOS 安全分區	
C6 損壞的 FAT 16 卷/條帶集 (Windows NT)	
C7 損壞的 NTFS 卷/條帶集	
戴爾OEM分區	

F2 DOS 3.3+ 二級分區 FE IBM
OEM 分區