HstEx v3.1

Overview

HstEx v3 is an advanced, Windows-based, multi-threaded, forensic data recovery solution which has been designed to recover deleted Browser History and Cache data from a variety of source forensic evidence files as well as physical and logical devices. Designed to work in conjunction with NetAnalysis, this powerful software can recover deleted data from a variety of Internet browsers, whether they have been installed on Windows, Linux or Apple Mac systems.

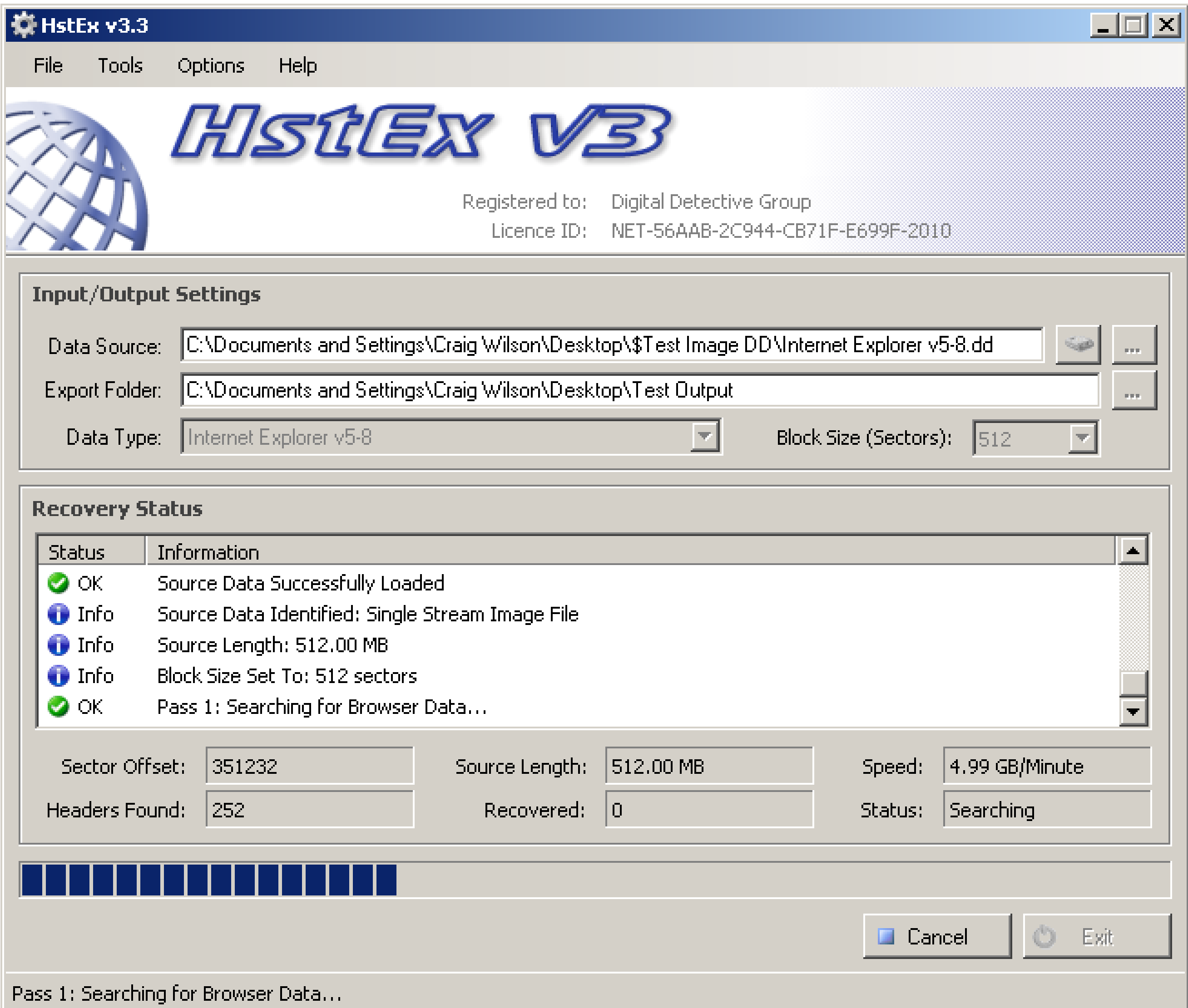

Figure 1

Supported Forensic Sources

This version is a complete re-write of HstEx v2 and supports direct extraction from forensic evidence files produced by EnCase and AccessData FTK Imager. It supports extraction from the following sources as shown in the table below. It also supports direct disk access to write protected hard drives, volumes and removable media.

Supported Forensic Image Formats	
EnCase® v1-6 Image File (EVF / Expert Witness Format)	*.e01
AccessData® FTK Image Files	*.e01, *.001, *.s01
SMART/Expert Witness Image File	*.s01
X-Ways Forensics Image File	*.e01
VMWare Virtual Disk File	*.vhd
Segmented Image Unix / Linux DD / Raw Image Files	*.000, *.001
Single Image Unix / Linux DD/Raw Image Files	*.dd; *.img; *.ima; *.raw
Virtual Hard Disk File	*.vhd
Binary / Memory Dumps	*.bin; *.dat; *.dmp; *.mem; *.dump; *.crash

HstEx v3 has been designed to be extremely fast and is considerably faster than HstEx v1 or 2. The HstEx output file format has also been changed and enhanced.

Please note, the output from HstEx v3 is not compatible with NetAnalysis versions prior to v1.50.

During the extraction process, HstEx identifies the extract Physical Sector and Sector Offset of the data on the original disk. This information is embedded within the file and read by NetAnalysis when the data is imported. This means that you can pin-point the exact physical location of a piece of evidence on the original hard disk. HstEx also logs the source evidence metadata which is also read and logged by NetAnalysis. This means that you will always be able to identify the source forensic evidence files from an output file and there is a clear link between produced evidence and the original forensic source. HstEx v3 also maintains a recovery log for each extraction.

Supported Browsers

All of the extraction engines have been re-written and optimised. HstEx v3 now supports extraction of the following file types. We are currently working on support for the extraction from other browsers.

HstEx v3 Supported Browsers	
Microsoft Internet Explorer v4	Full Support
Microsoft Internet Explorer v5-9	Full Support
Mozilla Firefox v1-2 File	Firefox v1-2 History / Cache Entries (All Mozilla based including Netscape)
Mozilla Firefox v1-3 Cache Entries	Firefox v1-3 Cache Entries for all Mozilla based browsers
Safari (XML) Plist History Entries	Safari XML based PLIST (Early Windows and Apple Mac Versions)
Safari (Binary) Plist History Entries	Safari Binary based PLIST History
Mozilla / Netscape / Firefox Bookmarks Entries	Mozilla based browser Bookmark File
Yahoo! BT Browser History Entries	Yahoo! Browser from British Telecom

Firefox v1-3 Cache

Research and development has allowed us to identify a method for recovering Firefox v1-3 cache index entries. HstEx v3 is the only forensic software product that can recover this deleted data directly from a disk or forensic evidence file.

Links

See the following for further information on getting started with HstEx.

- Quick Start Guide - HstEx