

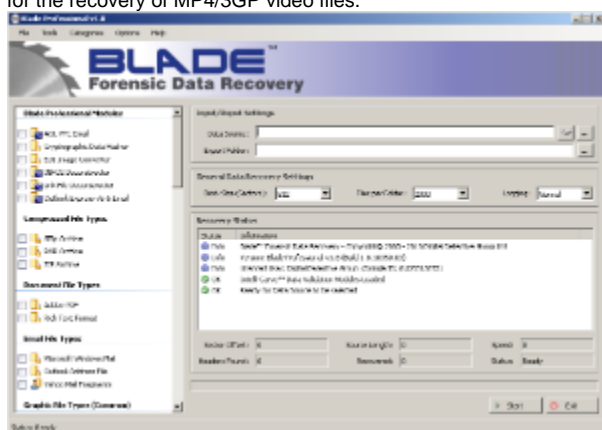
Blade v1.8

? Unknown Attachment

- [Overview](#)
- [User Interface](#)
- [Select Profile Categories](#)
- [Unique Output Session Folders](#)
- [Cancel / Partial Recovery Option](#)
- [Recovery Profiles](#)
- [3GP/MPEG-4/ISO Base Media Format](#)
- [INFO2 Record Extraction and Deconstruction](#)
- [Cryptographic Hashing](#)

Overview

This release of Blade has a number of new features and improvements. We have added 8 new Recovery Profiles to the Global Recovery Database, as well as releasing some new Professional Modules. We have also released a new 3GP/MPEG-4/ISO Base Media Format Intelli-Carve™ Recovery Profile for the recovery of MP4/3GP video files.



User Interface

We have made some minor updates to the user interface of Blade to make it easier to identify Global, Personal and Intelli-Carve™ Recovery Profiles. As you can see from Figure 1, different types of recovery profiles are represented by different icons.

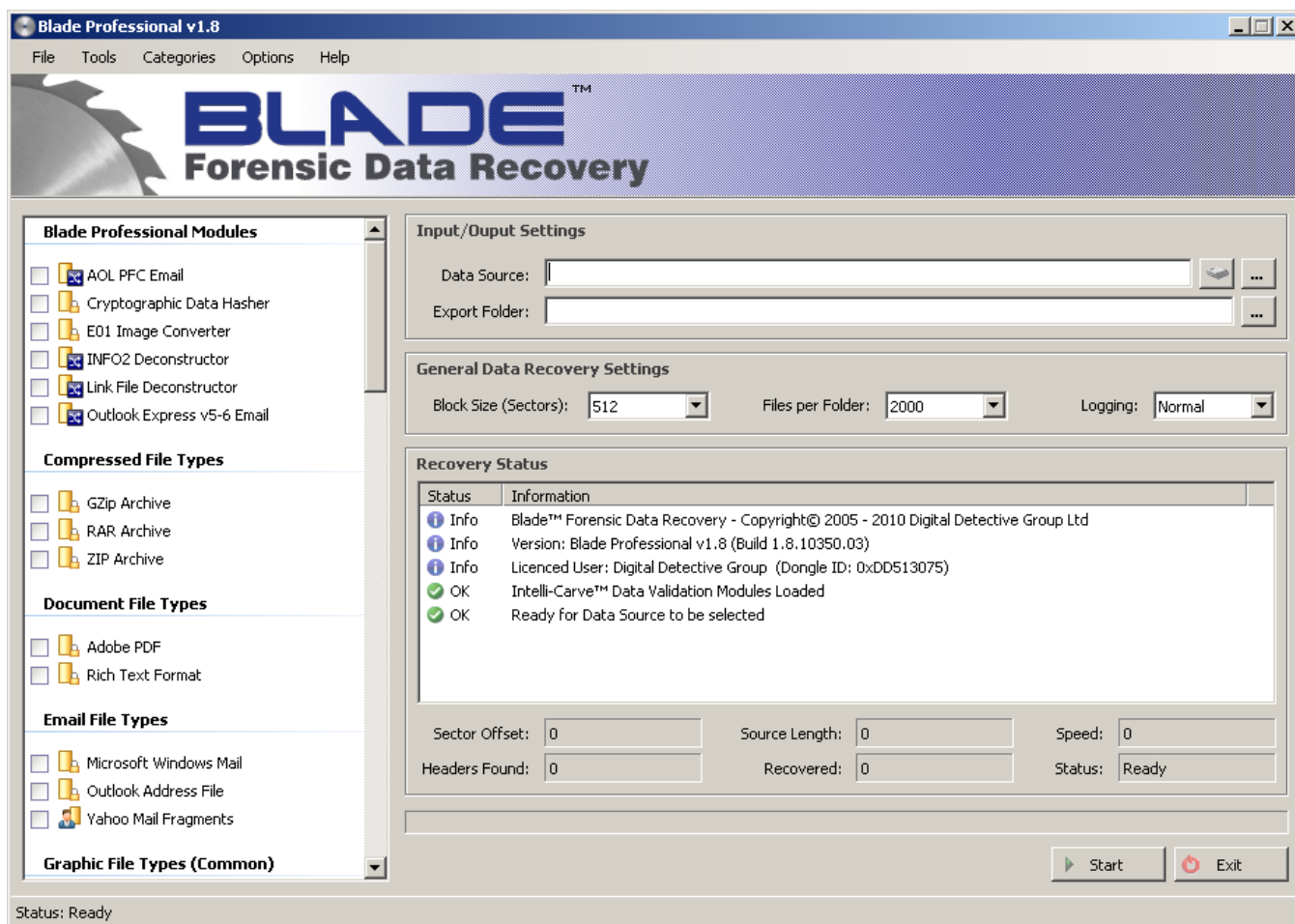


Figure 1

Select Profile Categories

We have added the option to select recovery categories as well as individual recovery profiles. Available from the Tools menu, select the category you wish to recover (e.g. common graphic types). This will auto-select the profiles from that category. To clear all of the selected profiles, simply select from the Tools menu or press F5. We have not added an option to select all profiles as this would not be practical to attempt to recover every supported file type (and would also not make sense from a forensic perspective).

Unique Output Session Folders

In previous versions of Blade, if you attempted to extract data into a folder that had already been used, Blade would report that the folder was not empty and not permit the folder to be used; this can be a torment for examiners if they wish to keep all of the extracted data together. To solve the issue, Blade now creates a session folder for every extraction. This means that multiple passes across the same data source can be kept neatly within a single folder.

Cancel / Partial Recovery Option

We have added this feature at the request of a number of users. Sometimes it is difficult to get your personal recovery profiles working correctly. Having to wait until the whole disk or image is processed to find out if they have worked correctly is extremely time consuming. We have now added an option to perform a partial recovery on pressing cancel during the search phase (pass one). If data headers have been identified during the search phase, Blade will prompt to recover that data. In addition, we have added an option to automatically open the export folder once the extraction has completed. This allows you to quickly open the export folder and start examining the recovered data.

Recovery Profiles

We have made a number of changes to the Recovery Profiles to add additional functionality. Figure 2 shows the new Personal Profile screen. In the File Header section, we have added a new field for the number of bytes to the Start of the File (Bytes to SOF). This value can be positive or negative and represents where the start of the file is in relation to the File Header Signature. This takes into account data where there is a recognisable pattern or structure x bytes into the file, but no static header exists.

Personal Profile Database

- LG KP501 3GP
- Data with Default
- Data with Default & Floating Landmark
- Data with Default & Static Landmark
- Data with Footer
- Data with Footer & Floating Landmark
- Data with Footer & Static Landmark
- Data with Length Marker
- Data with Length Marker & Floating L...
- Data with Length Marker & Static Lan...
- Facebook Chat Carver
- Facebook Chat Carver (Craig)
- MMS
- RegEx Test
- SAMSUNG GT-S5230 MP4
- SAMSUNG SGH-E250 MP4
- SMIL
- SMS Foreign
- SMS Message
- TestReader
- Yahoo Mail Fragments

Forensic Data Recovery Profile

Description:

Category:

Author:

File Extension:

Date:

Version:

File Header

Signature:

* Bytes to SOF: * +/- Number of Bytes from Start of Header to Start of File

File Landmark

Signature:

Location:

File Landmark Relative Offset:

File Landmark (Secondary)

Signature:

Location:

File Landmark Relative Offset:

File Footer

Signature:

* Bytes to EOF: * +/- Number of Bytes from Start of Footer to End of File

Data Length

Length Marker Size:

Length Marker Relative Offset:

+/- Length Marker Adjustment:

Data Boundary

Minimum Length:

Maximum Length:

Personal Data Recovery Signatures

Figure 2

We have added a secondary File Landmark section for additional data validation. We have put this to good use for the recovery of Microsoft Office 2007 documents.

And finally, we have added a new field to take into account length adjustments for data types which contain length markers. In the Data Length section, you can see the Length Marker Adjustment field. This value can also be positive or negative. We have put this into good use with AVI files where is a UInt32 length marker at offset 0x04. This marker provides the length of the data following the header but does not take into account the four bytes containing the length marker or the header itself. This meant that the AVI files recovered were 8 bytes too short. Now you can add a length marker adjustment to add the missing 8 bytes back on to the file.

3GP/MPEG-4/ISO Base Media Format

ISO base media file format defines a general structure for time-based multimedia files such as video and audio. It is used as the basis for other media file formats (e.g. container formats MP4 and 3GP). ISO base media file format was specified as ISO/IEC 14496-12 (MPEG-4 Part 12). Blade now contains an Intelli-Carve profile™ which reads and validates the recovered data prior to writing it out. In addition, Blade also recovers the metadata from each file and can write it out to a CSV log. This is particularly useful for recovering date/time information from video data where the video has been recovered from unallocated clusters. To set the metadata extraction options, right click on the recovery profile.

Blade also identifies the type of file and appends the correct file extension. Below is a list of file extensions which are supported:

3GP/MPEG-4/ISO Base Media Format Supported Extensions

3gp, 3g2, dvb, f4v, f4p, f4a, f4b, jp2, jpm, jpx, m4v, m4p, m4a, m4b, mj2, mp4, mgv and mov

INFO2 Record Extraction and Deconstruction

We have added a new Professional Recovery Module for the recovery and deconstruction of INFO2 records. This recovery module has a number of output options. The profile recovers INFO2 records relating to deleted files and writes the various fields out to a number of different formats. Figure 3 shows the options which are available for this module.

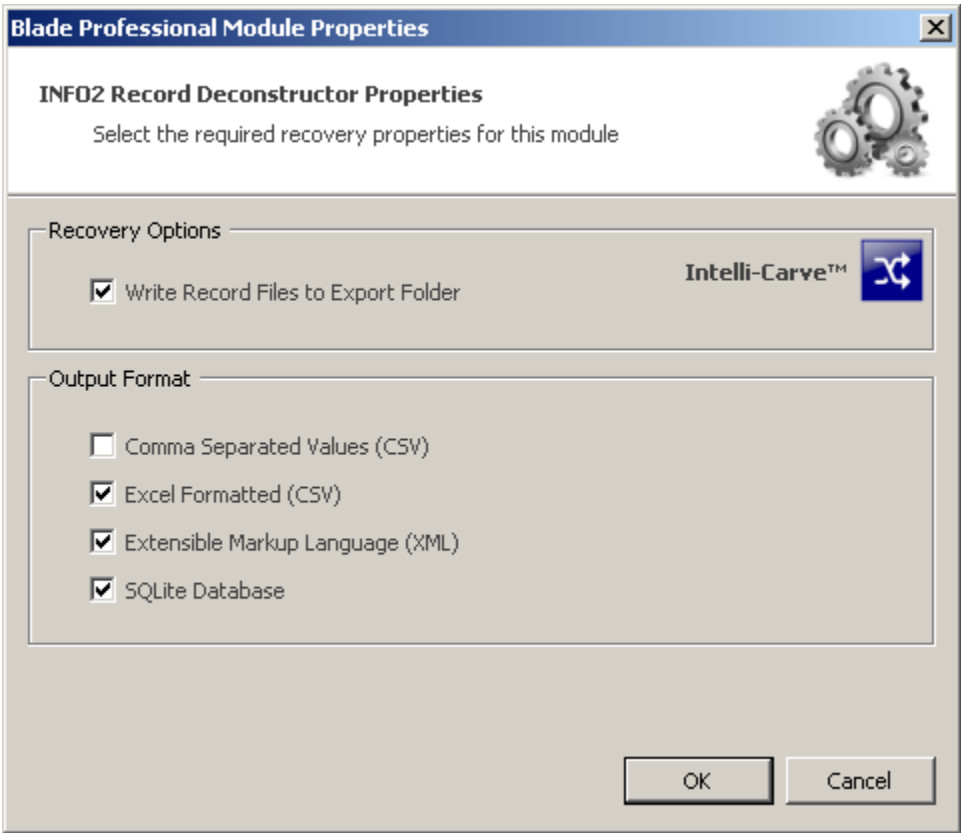




Figure 3

The INFO2 extractor is bundled as part of the Link File Recovery module and is available to all Blade Professional users.

 This module fully supports Unicode data.

Cryptographic Hashing

We have also added a hashing module which will work with a number of sources including forensic images

 If you wish to MD5/SHA1 hash the content of EnCase e01 files, please use the e01 conversion module which has an option to hash the internal data and check it against the embedded hash without converting the image

Supported Cryptographic Hashing Algorithms
MD5, SHA1, SHA256, SHA384, SHA512 and RIPEMD160

To select the required hashing algorithms, right click on the module, select module properties and select/tick the required values. Select the required source file or image (e.g. segmented image file *.001) and then an export folder which will contain the hashing report.