Quick Start

Introduction

Blade® is a Windows-based, advanced professional forensic data recovery solution designed and developed by Digital Detective Group. It supports professional module plug-ins which give it advanced data recovery and analysis capabilities. The power and flexibility of the tool can be expanded as new modules become available.   Blade® supports all of the major forensic image/export formats (EnCase® E01/Ex01, FTK, Smart, X-Ways, XRY, VHD, VMDK, DD, Segmented DD, IMA, IMG, RAW as well as memory dumps) and is more than just a data recovery tool. The professional modules (and some of the basic Recovery Profiles) have in-built Intelli-Carve® data validation and interpretation routines to assist with accurate data recovery.

The software has been designed for extremely fast/accurate forensic data recovery. Not only is it highly effective in the pre-analysis stage of a forensic examination, it can be quickly configured to recover/carve bespoke data formats. It has specifically been written for the field of Digital Forensics.

It is ideal for the following situations:

- Carve deleted data from forensic image files without using EnCase
- Can be used without knowledge of programming languages and scripting
- Recover data from Mobile Phone Memory dumps
- Creating recovery profiles for bespoke data recovery and sharing the profile with other agencies or colleagues
- Advanced Recovery of deleted Outlook Express / Microsoft Mail email messages
- Advanced Recovery of live and deleted AOL email messages
- Advanced Recovery of live and deleted Link Files and deconstructing the output
- Conversion of Hyberfil.sys

Professional Recovery Modules

With the addition of professional modules, Blade® can recover data which is not extracted by other forensic tools or traditional simple carvers. Professional Modules add a powerful capability to this product. Blade® is also ideal for practitioners (or technicians with limited forensic training) who want to perform quick and easy data recovery without resorting to using scripting programming languages or tying up their main forensic tool.

Sources of Evidence

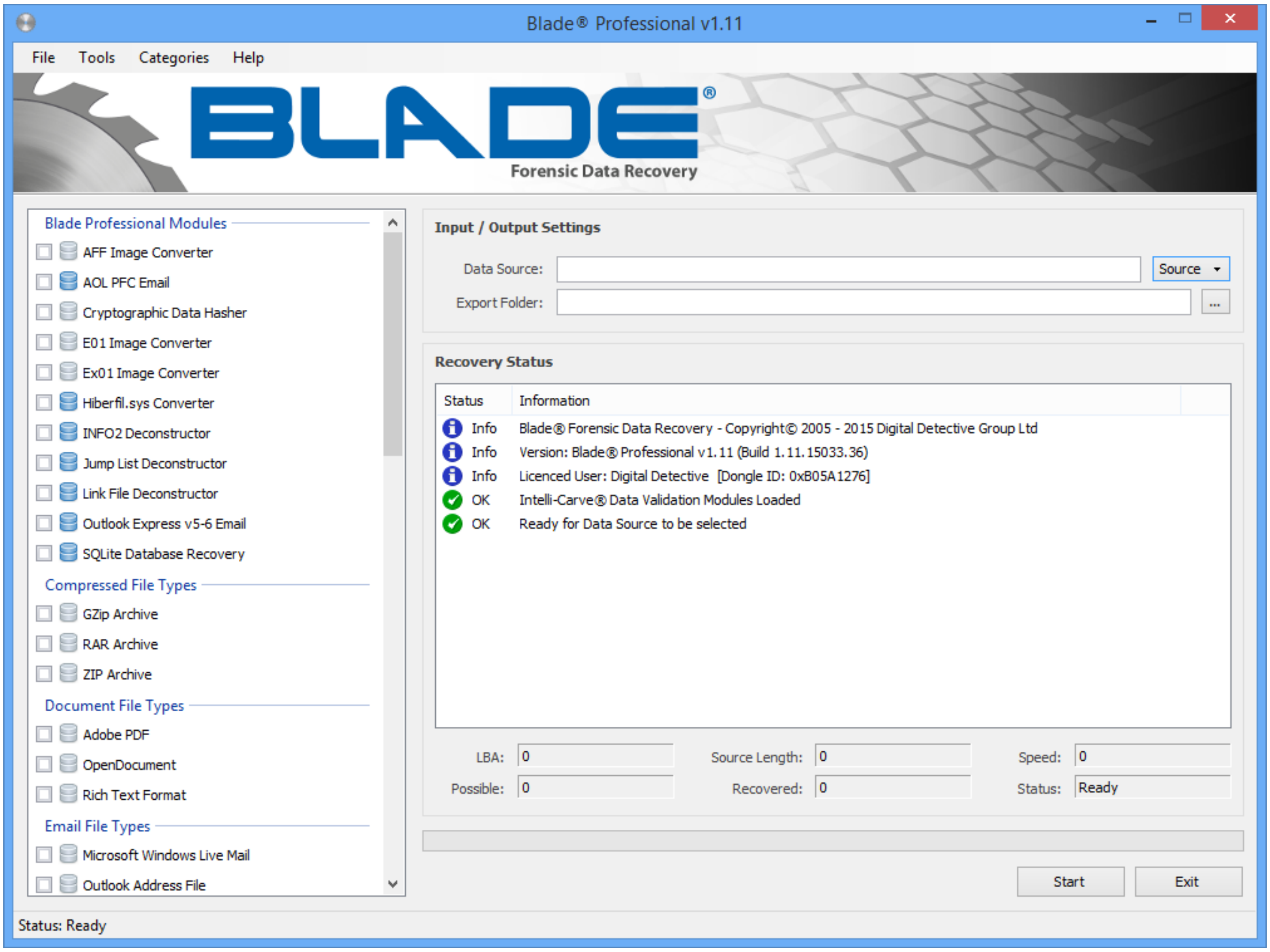
In addition to the live files on the system, evidence can be found in numerous locations such as:

- Unallocated clusters
- Cluster slack
- Live memory, memory dumps and crash dumps
- Page files, system files, hibernation files
- System restore points

Blade® can recover data from a variety of sources. The source of the evidence can be any of the popular forensic image files such as from EnCase® or AccessData FTK, write protected physical and logical devices, flat file monolithic image formats or segmented flat file images.

Getting Started

Blade® is very simple and easy to use. First of all, select the data source. This can be done by selecting the Source drop down button. You can either select a Disk Image/Binary File or Physical/Logical Device.

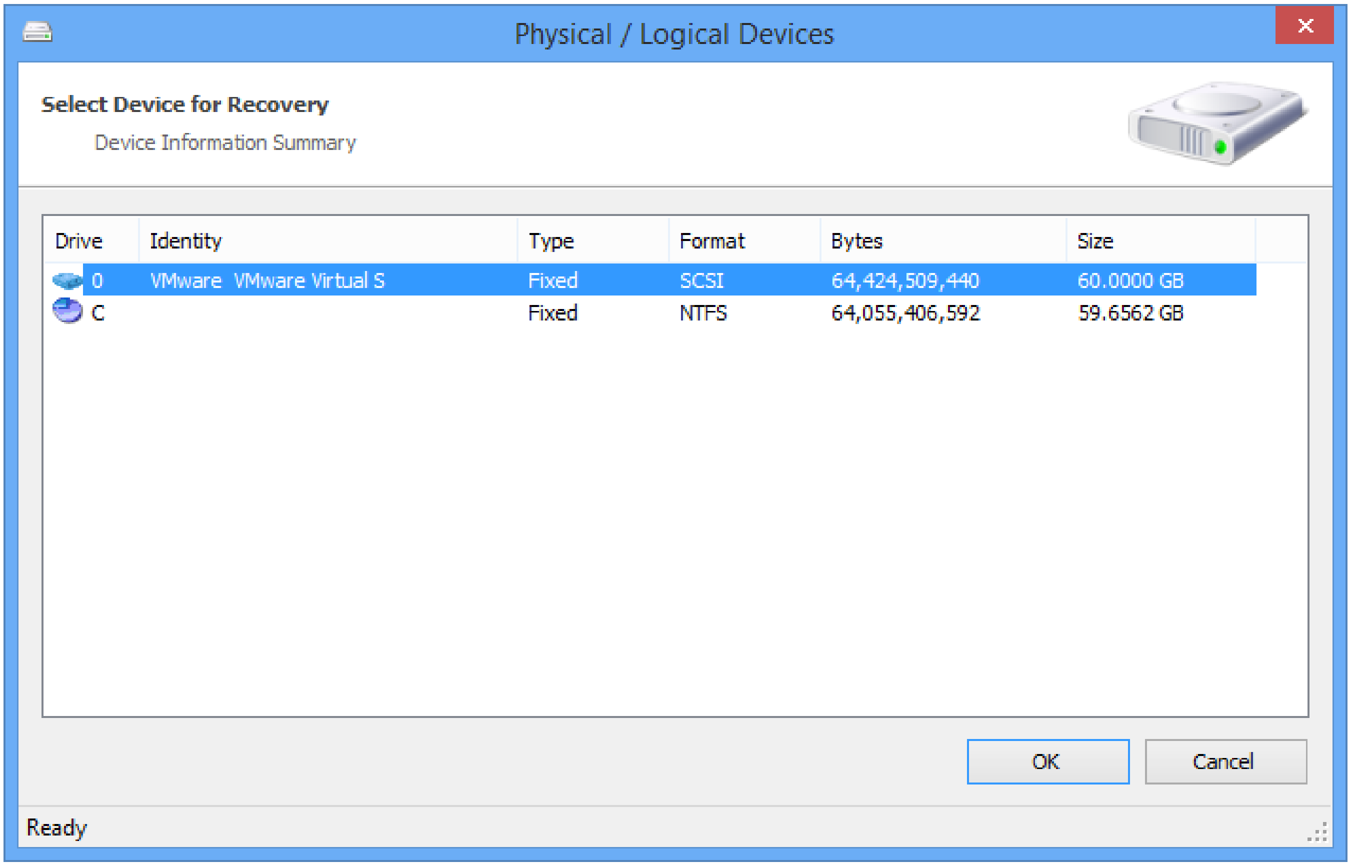


Status	Information
Info	Blade® Forensic Data Recovery - Copyright© 2005 - 2015 Digital Detective Group Ltd
Info	Version: Blade® Professional v1.11 (Build 1.11.15033.36)
Info	Licenced User: Digital Detective [Dongle ID: 0xB05A1276]
OK	Intelli-Carve® Data Validation Modules Loaded
OK	Ready for Data Source to be selected

LBA: 0
Source Length: 0
Speed: 0
Possible: 0
Recovered: 0
Status: Ready

Status: Ready

If you select a Physical/Logical device, Blade® will scan the system for all connected accessible devices. Blade® will not show you mounted network drives as they cannot be opened at low level for data recovery scanning. It is normal practice to have a write blocker protect the source device and prevent any inadvertent writes to your source.



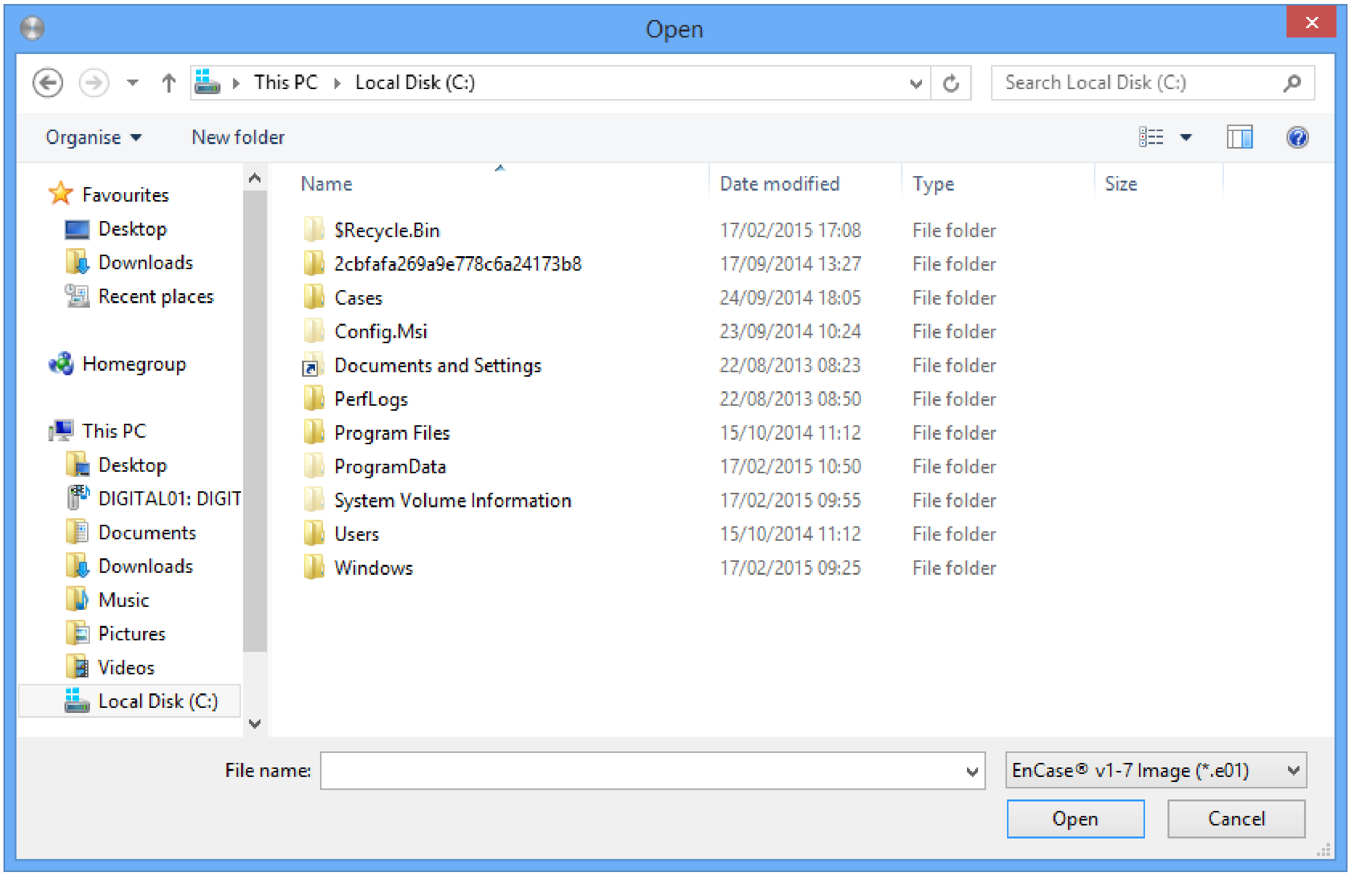
Select Device for Recovery

Device Information Summary

Drive	Identity	Type	Format	Bytes	Size
0	VMware VMware Virtual S	Fixed	SCSI	64,424,509,440	60.0000 GB
C		Fixed	NTFS	64,055,406,592	59.6562 GB

Select the device you wish to scan and press OK.

If you select Disk Image/Binary File, Blade® will open a File Selection window as shown below:



Name	Date modified	Type	Size
$Recycle.Bin	17/02/2015 17:08	File folder	
2cbfafa269a9e778c6a24173b8	17/09/2014 13:27	File folder	
Cases	24/09/2014 18:05	File folder	
Config.Msi	23/09/2014 10:24	File folder	
Documents and Settings	22/08/2013 08:23	File folder	
PerfLogs	22/08/2013 08:50	File folder	
Program Files	15/10/2014 11:12	File folder	
ProgramData	17/02/2015 10:50	File folder	
System Volume Information	17/02/2015 09:55	File folder	
Users	15/10/2014 11:12	File folder	
Windows	17/02/2015 09:25	File folder	

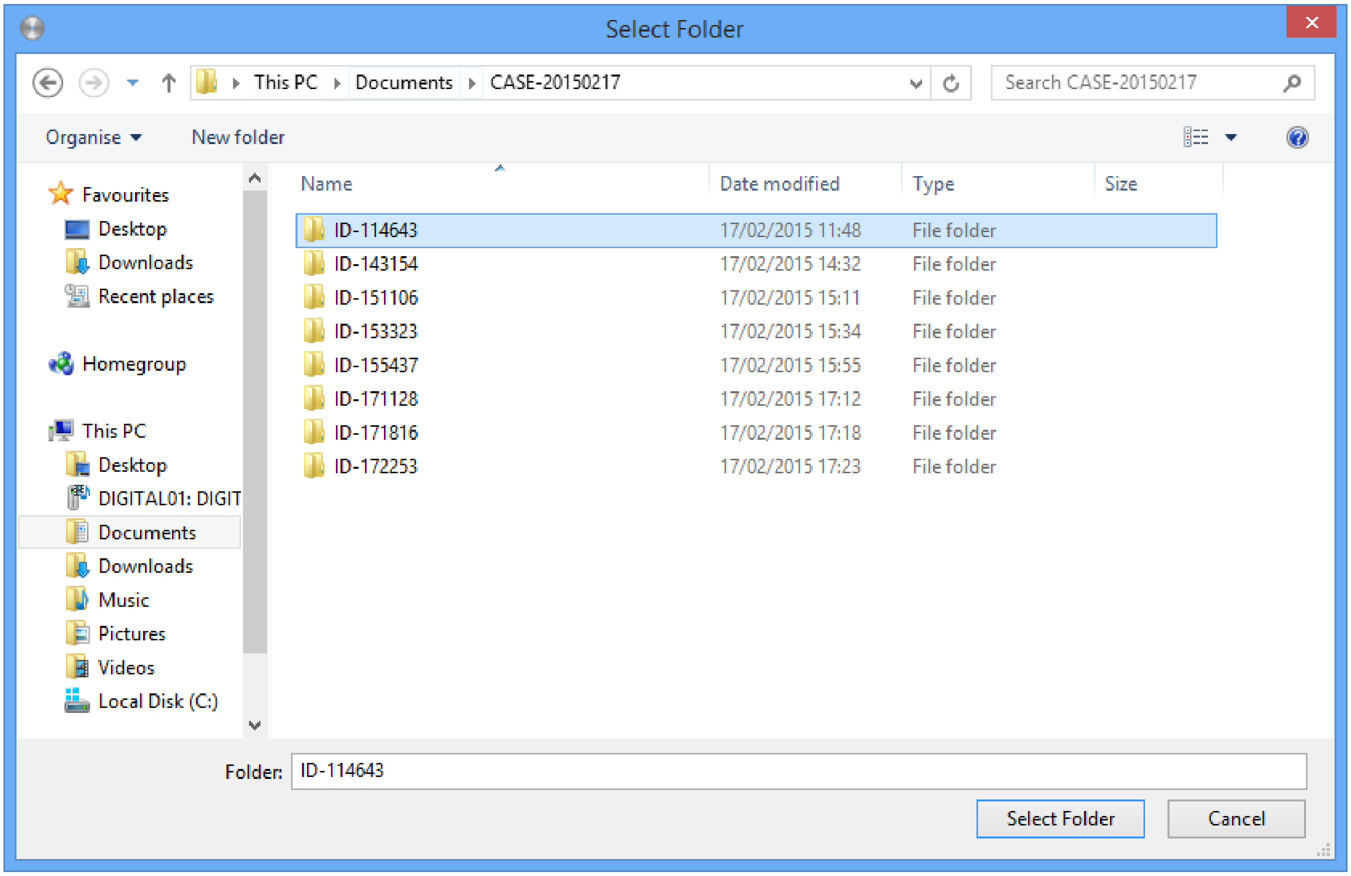
File name:

EnCase® v1-7 Image (*.e01)

The drop down box will list the supported file type filters thereby allowing you to filter a specific file type. Select the file/image you wish to process and select Open. To see the full list of supported source types, please see the following: Forensic Image Formats Supported by Blade.

Selecting the Export Folder

The Export Folder is the location where Blade® will save any recovered data. It will also write its log files to this location. Clicking on the "..." browse button will launch the folder selection window (as shown below). Please ensure you have write permissions for this folder and there is enough space for the recovered data to be saved.



Name	Date modified	Type	Size
ID-114643	17/02/2015 11:48	File folder	
ID-143154	17/02/2015 14:32	File folder	
ID-151106	17/02/2015 15:11	File folder	
ID-153323	17/02/2015 15:34	File folder	
ID-155437	17/02/2015 15:55	File folder	
ID-171128	17/02/2015 17:12	File folder	
ID-171816	17/02/2015 17:18	File folder	
ID-172253	17/02/2015 17:23	File folder	

Folder: ID-114643

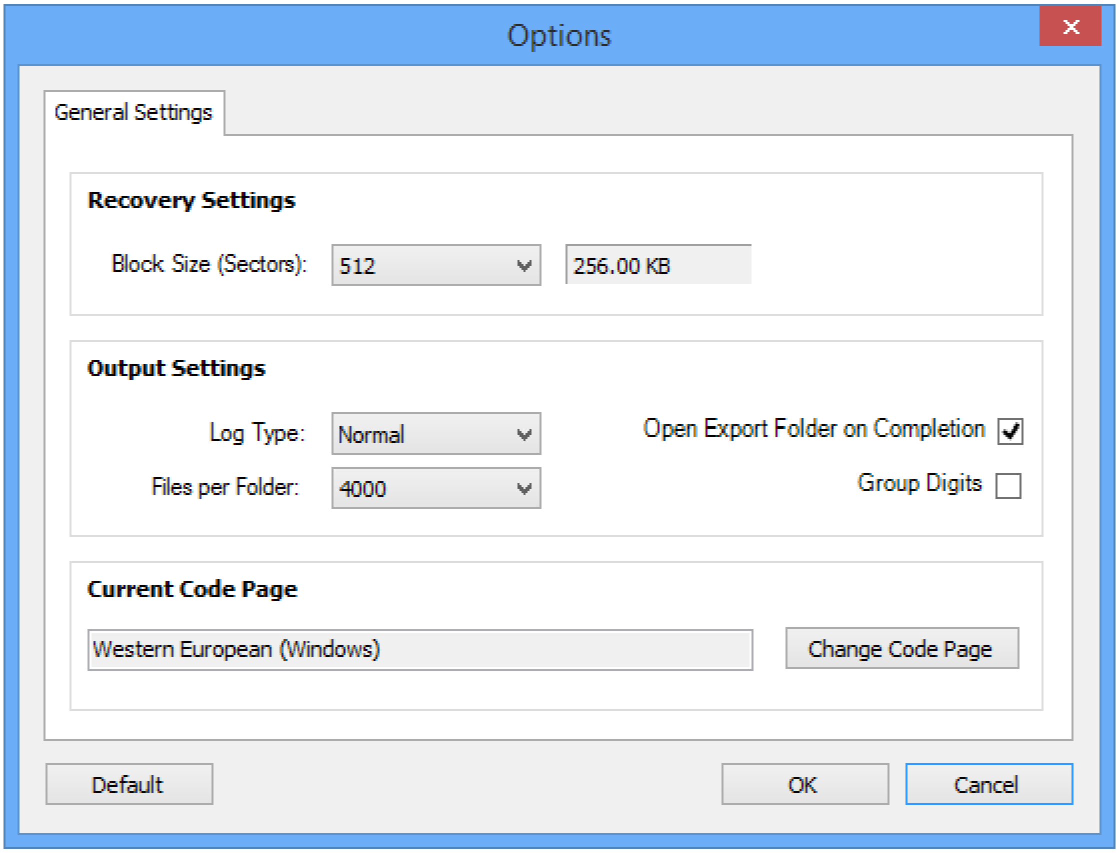
Press the Select Folder to close the window.

Warning

Do not select an export folder on the drive you are trying to process. This will result in data being written to the source drive and will potentially overwrite any data you are trying to recover.

Options

Before you start your recovery, you may wish to review some of the options available. The options window can be viewed by selecting Tools » Options.



Options

General Settings

Recovery Settings

Block Size (Sectors): 512

256.00 KB

Output Settings

Log Type: Normal

Files per Folder: 4000

Open Export Folder on Completion ☑

Group Digits ☐

Current Code Page

Western European (Windows)

Block Size

The block size relates to the size of the buffer used to process the recovery source. The default block size is 512 sectors (256 KiB) for file and disk based recovery. Using larger block sizes can considerably increase the performance of Blade during the search and recovery phases.

Log Type

The options are Normal, Verbose and Debug. It is recommended that you leave the logging at Normal. Setting the logging to Verbose or Debug will slow down the search and extraction as more information is written to the log files. Debug is designed to write additional information to the log files if a problem is encountered. Do not use this setting unless advised by our Technical Support team.

Files per Folder

This option allows you to set how many recovered files will be written to a single folder. The default value is 4,000 files. You have the option to select other values from the drop down list.

Open Export Folder on Completion

This option sets whether the export folder should automatically open at the completion of the recovery session.

Group Digits

This option allows the user to specify whether numbers are grouped using the group delimiter character as specified by the operating system International settings.

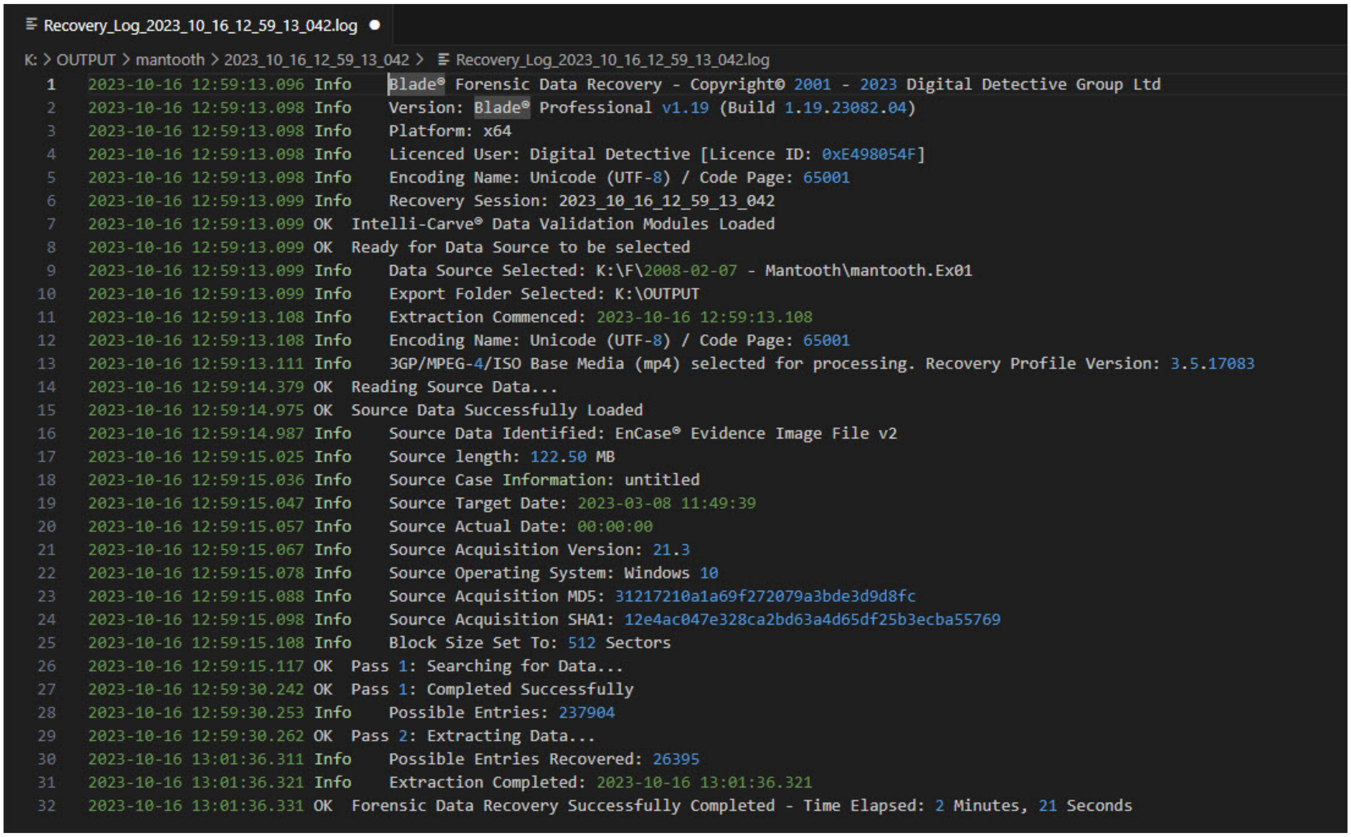
Selecting Recovery Profiles

When you are ready to recover data, select the Recovery Profiles for the data types you wish to recover. You can create your own Recovery Profiles for bespoke data recovery by selecting Personal Profile Database from the Tools menu.

ⓘ Advanced Recovery Profiles can only be run on their own because of the way the searching and recovery process is completed. Multiple Standard Recovery Profiles can be selected for extraction without any problem.

Recovering Data

To start the recovery process, press the Start button. During the recovery, Blade® will write a log to the export folder (and data validation log depending on the type of data recovered) and show important information in the screen log. The recovery log below shows recovery from an EnCase® Ex01 image and also contains the image metadata.


Recovery_Log_2023_10_16_12_59_13_042.log ●
K: > OUTPUT > mantooth > 2023_10_16_12_59_13_042 > Recovery_Log_2023_10_16_12_59_13_042.log

```
2023-10-16 12:59:13.096 Info    Blade® Forensic Data Recovery - Copyright© 2001 - 2023 Digital Detective Group Ltd
2023-10-16 12:59:13.098 Info    Version: Blade® Professional v1.19 (Build 1.19.23082.04)
2023-10-16 12:59:13.098 Info    Platform: x64
2023-10-16 12:59:13.098 Info    Licenced User: Digital Detective [Licence ID: 0xE498054F]
2023-10-16 12:59:13.098 Info    Encoding Name: Unicode (UTF-8) / Code Page: 65001
2023-10-16 12:59:13.099 Info    Recovery Session: 2023_10_16_12_59_13_042
2023-10-16 12:59:13.099 OK  Intelli-Carve® Data Validation Modules Loaded
2023-10-16 12:59:13.099 OK  Ready for Data Source to be selected
2023-10-16 12:59:13.099 Info    Data Source Selected: K:\F\2008-02-07 - Mantooth\mantooth.Ex01
2023-10-16 12:59:13.099 Info    Export Folder Selected: K:\OUTPUT
2023-10-16 12:59:13.108 Info    Extraction Commenced: 2023-10-16 12:59:13.108
2023-10-16 12:59:13.108 Info    Encoding Name: Unicode (UTF-8) / Code Page: 65001
2023-10-16 12:59:13.111 Info    3GP/MPEG-4/ISO Base Media (mp4) selected for processing. Recovery Profile Version: 3.5.17083
2023-10-16 12:59:14.379 OK  Reading Source Data...
2023-10-16 12:59:14.975 OK  Source Data Successfully Loaded
2023-10-16 12:59:14.987 Info    Source Data Identified: EnCase® Evidence Image File v2
2023-10-16 12:59:15.025 Info    Source length: 122.50 MB
2023-10-16 12:59:15.036 Info    Source Case Information: untitled
2023-10-16 12:59:15.047 Info    Source Target Date: 2023-03-08 11:49:39
2023-10-16 12:59:15.057 Info    Source Actual Date: 00:00:00
2023-10-16 12:59:15.067 Info    Source Acquisition Version: 21.3
2023-10-16 12:59:15.078 Info    Source Operating System: Windows 10
2023-10-16 12:59:15.088 Info    Source Acquisition MD5: 31217210a1a69f272079a3bde3d9d8fc
2023-10-16 12:59:15.098 Info    Source Acquisition SHA1: 12e4ac047e328ca2bd63a4d65df25b3ecba55769
2023-10-16 12:59:15.108 Info    Block Size Set To: 512 Sectors
2023-10-16 12:59:15.117 OK  Pass 1: Searching for Data...
2023-10-16 12:59:30.242 OK  Pass 1: Completed Successfully
2023-10-16 12:59:30.253 Info    Possible Entries: 237904
2023-10-16 12:59:30.262 OK  Pass 2: Extracting Data...
2023-10-16 13:01:36.311 Info    Possible Entries Recovered: 26395
2023-10-16 13:01:36.321 Info    Extraction Completed: 2023-10-16 13:01:36.321
2023-10-16 13:01:36.331 OK  Forensic Data Recovery Successfully Completed - Time Elapsed: 2 Minutes, 21 Seconds
```

Blade® searches and recovers data from your source in two different phases:

- During phase 1, the data is identified and logged.
- During phase 2, the data is recovered and validated. It is then written to the Export Folder.

Once the extraction has completed, you can quickly access the Export Folder by selecting CTRL + E or Open Export Folder from the Tools menu.