# **Dumping Data from an Image or Disk**

- Introduction
- DataDump
- Running DataDump
- Download

#### Introduction

When debugging or testing a digital forensic tool, or performing a data recovery procedure, you may have a requirement to extract some binary data from a forensic image or physical/logical disk. This is where DataDump can be of value.

## DataDump

DataDump™ is a free tool which allows you to dump segments of data from an original source image or physical/logical device. It can be used for the following:

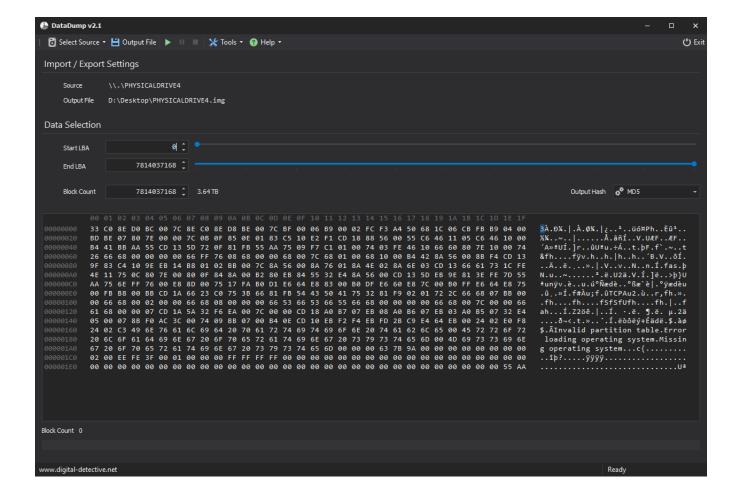
- · Extract a stream of binary data from a source image or logical device
- Convert an entire image or a segment of an image to a single flat file
- · Extract binary chunks of data from files, images or physical/logical devices
- Extract a partition from a source device as a single binary file
- Hash the output data using MD5, SHA-1, SHA-256 or SHA-512

## Running DataDump

Once you have downloaded and installed the application, dumping a selection of binary data from your source is relatively straight forward.

- 1. Select the source by clicking on the Select Source drop down button menu, then select either Disk Image File or Physical / Logical Device
- 2. Select the file you want the data to write to by clicking on the Output File button
- 3. Select the Logical Block Address (LBA) of the start of the data you wish to extract
- 4. Select the Block Count or End Logical Block Address (LBA) to set the length of the data to be extracted
- 5. If you wish the dumped data to be hashed, select MD5, SHA-1, SHA-256 or SHA-512 from the drop down list
- 6. Click the Start (F5) button to start dumping data







The smallest block of data that can be dumped is 1 block (512 bytes).

#### Download

The software can be downloaded by clicking the button below:

