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

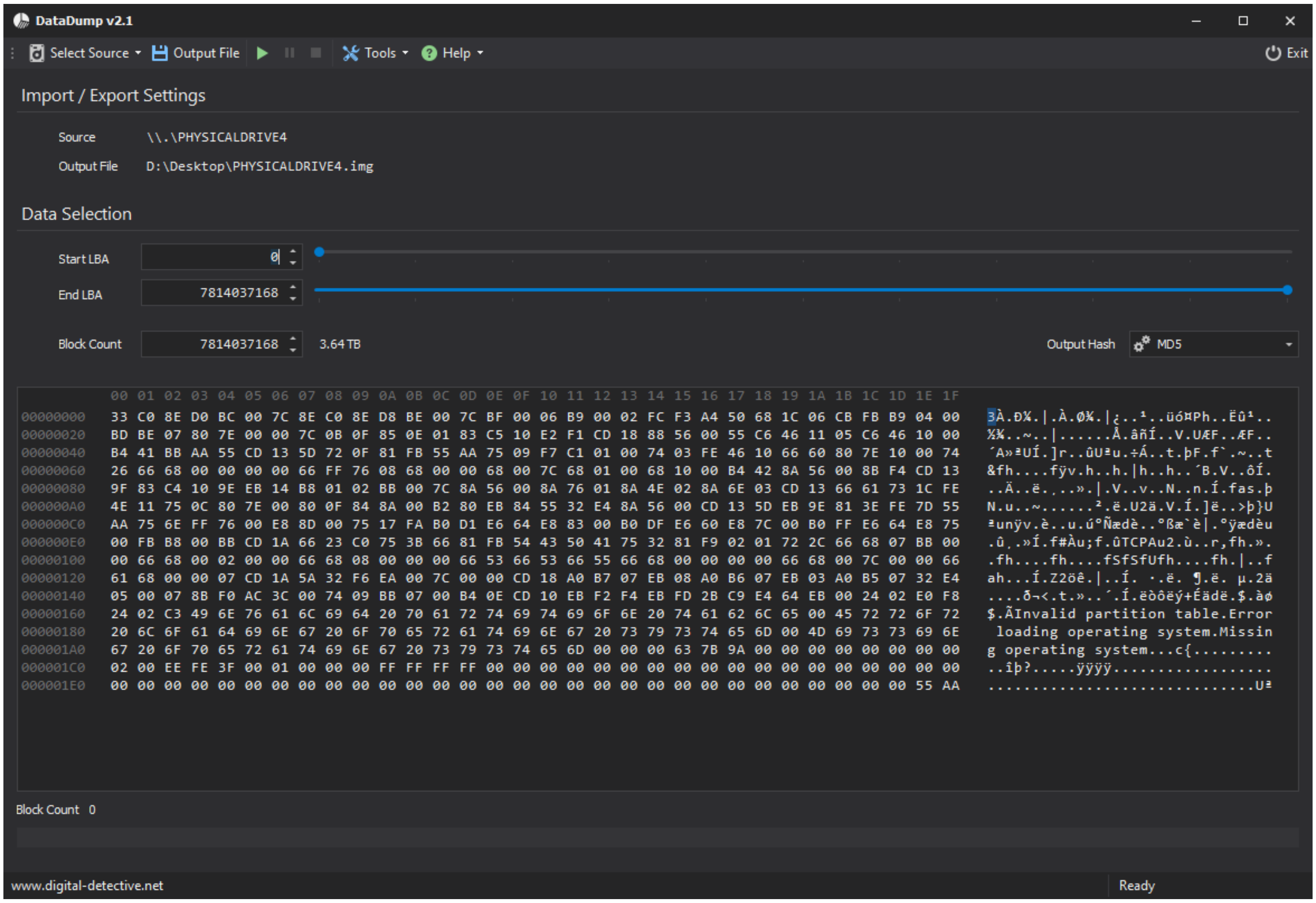
DataDump™ is a free tool which allows you to dump segments of data from an original source image or physical/logical device. It can be used for the following:

- 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



Import / Export Settings

Source \\.\PHYSICALDRIVE4
Output File D:\Desktop\PHYSICALDRIVE4.img

Data Selection

Start LBA 0
End LBA 7814037168
Block Count 7814037168 3.64 TB
Output Hash MD5

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
00000000  33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00 06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00  3À.Ð¼.|.À.Ø¾.|¿..¹..üó¤Ph..Ëû¹..
00000020  BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10 E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00  ½¾..~..|......Å.âñÍ..V.UÆF..ÆF..
00000040  B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09 F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74  ´A»ªUÍ.]r..ûUªu.÷Á..t.þF.f`.~..t
00000060  26 66 68 00 00 00 00 66 FF 76 08 68 00 00 68 00 7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4 CD 13  &fh....fÿv.h..h.|h..h..´B.V..ôÍ.
00000080  9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00 8A 76 01 8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE  ..Ä..ë.¸..».|.V..v..N..n.Í.fas.þ
000000A0  4E 11 75 0C 80 7E 00 80 0F 84 8A 00 B2 80 EB 84 55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E FE 7D 55  N.u..~......².ë.U2ä.V.Í.]ë..>þ}U
000000C0  AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64 E8 83 00 B0 DF E6 60 E8 7C 00 B0 FF E6 64 E8 75  ªunÿv.è..u.ú°Ñædè..°ßæ`è|.°ÿædèu
000000E0  00 FB B8 00 BB CD 1A 66 23 C0 75 3B 66 81 FB 54 43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00  .û¸.»Í.f#Àu;f.ûTCPAu2.ù..r,fh.».
00000100  00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66 53 66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66  .fh....fh....fSfSfUfh....fh.|..f
00000120  61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD 18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E4  ah...Í.Z2öê.|..Í. ·.ë. ¶.ë. µ.2ä
00000140  05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD 10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8  ....ð¬<.t.»..´.Í.ëòôëý+Éädë.$.àø
00000160  24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69 74 69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72  $.ÃInvalid partition table.Error
00000180  20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E   loading operating system.Missin
000001A0  67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 65 6D 00 00 00 63 7B 9A 00 00 00 00 00 00 00 00  g operating system...c{.........
000001C0  02 00 EE FE 3F 00 01 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..îþ?.....ÿÿÿÿ..................
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA  ..............................Uª
```

Block Count 0

www.digital-detective.net Ready

⚠ 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:

Download DataDump™