

# Troubleshooting and FAQ

- [Troubleshooting](#)
  - I'm having trouble reading a specific legacy floppy disk.
  - I've added the BitCurator VM using VirtualBox, but the virtual machine won't start (or crashes when it tries to boot)
  - I've downloaded the BitCurator virtual machine. What do I do with this .tar.gz file?
  - I mounted a USB drive and lost control of my mouse cursor
  - Why isn't Bulk Extractor finding SSNs that I know are there?
  - Using an FC5025 with the BitCurator VM
- [FAQ](#)
  - Is BitCurator intended to be a data preservation environment?
  - I work at a small institution with limited resources. Am I going to need an expensive new dedicated workstation just to do digital forensics work?
  - The BitCurator virtual machine is built for VirtualBox. Can I use VMWare instead?
  - What's a hardware write-blocker? Do I really need one?
  - What's the advantage of saving my disk images as AFF or E01 rather than raw?
  - What file systems does BitCurator support?
  - Will BitCurator help me crack passwords on encrypted files in my collection?

## Troubleshooting

### I'm having trouble reading a specific legacy floppy disk.

#### Problem

Determining how to extract data from a specific floppy disk within my collection.

#### Solution

BitCurator does not provide specific solutions for working with magnetic media. There are a number of projects that handle floppy drive interfaces. In particular, these include the [KryoFlux](#) ( a low-level data recovery device widely-used within the archives community), the [SuperCard Pro](#) (similar to the KryoFlux but with more limited support), the [FC5025](#) (a USB interface for 5.25" drives) and the [DiscFerret](#). Given the appropriate floppy interface, software used by BitCurator can read raw data on any required media.

### I've added the BitCurator VM using VirtualBox, but the virtual machine won't start (or crashes when it tries to boot)

#### Problem

The Virtual Machine won't boot, or crashes on startup.

#### Solution

There are a number of reasons this could be happening. If you're attempting to run BitCurator on a machine with less than 4GB of RAM, the default settings could be causing the host to lock up. Check the Oracle VM VirtualBox Manager to see if any of the tabs under "Settings" are indicating "non-optimal settings detected".

**Many PC laptops with Intel processors ship with hardware-assisted virtualization extensions disabled in the BIOS**, which may affect your ability to run 64-bit guest OSs in VirtualBox in Windows.

If this is the case, you will need to reboot the machine and **change the BIOS settings to enable Intel VT-x extensions**. The process for doing this varies from machine to machine. You may need to Google the manufacturer and model of your machine along with "VT-x enable" to determine how to do this.

**If you're attempting to run BitCurator on a machine running a 32-bit (uncommon) operating system, please note that we do not test or support this configuration.**

### I've downloaded the BitCurator virtual machine. What do I do with this .tar.gz file?

#### Problem

I'm not familiar with the .tar.gz format, or how to unpack it.

#### Solution

On most modern Windows 10 and Mac OS operating systems, you can simply double-click on the file to decompress the contained folder.

If you're using an earlier version of Windows (not recommended or supported), you can download 7-zip [here](#) to provide support for this compressed format.

Once you've installed 7-zip, you'll need to right click on the .tar.gz file and click "Extract here". Once the .tar file has been extracted, you'll need to right click on that file and again click "Extract here". This will produce a folder containing the latest BitCurator virtual machine image.

Once you've extracted the contents, you can add the machine in VirtualBox by choosing Machine->Add in the VirtualBox menu, and navigating to the location where you've extracted the .vdi and .vbox files. On a Mac, you can simply double-click the .tar.gz file, and the built-in extractor should take care of extracting the contents. Then you can add the VM in VirtualBox using the same method.

## I mounted a USB drive and lost control of my mouse cursor

### Problem

Mouse control lost when plugging in another USB device.

### Solution

This is a known issue with VirtualBox on some Windows hosts when both a USB mouse and USB drive are plugged into the computer.

**On some Windows systems you may need to right-click on the Oracle VirtualBox icon and choose "Run as Administrator" when starting up VirtualBox.**

Alternatively, shut down BitCurator and unplug the USB drive; restart BitCurator. Once BitCurator has fully started up, plug the USB drive in again; both the drive and your mouse should now work.

## Why isn't Bulk Extractor finding SSNs that I know are there?

### Problem

Bulk Extractor does not find Social Security numbers that you as a user know are present in the disk or directory being scanned.

### Solution

#### Command line

In Bulk Extractor 1.5+, the program offers three modes for identifying social security numbers.

These are:

- `ssn_mode=0` SSN's must be labeled "SSN:". Dashes or no dashes are okay.
- `ssn_mode=1` No "SSN" required, but dashes are required.
- `ssn_mode=2` No dashes required. Allow any 9-digit number that matches SSN allocation range.

By default, Bulk Extractor uses `ssn_mode 0`, meaning that only social security numbers prefaced with the exact string "SSN:" will be located.

When running Bulk Extractor from the command line, you can specify which `ssn_mode` to use with the `-S` flag. For example, to use `ssn_mode` pattern matching mode 1, the appropriate command is:

```
bulk_extractor -S ssn_mode=1 -o <output directory> -i <source to scan>
```

Using higher `ssn_modes` will likely result in more matches (including, potentially, more false positives).

### Bulk Extractor Viewer (GUI)

BEViewer (Bulk Extractor Viewer) does not currently allow users to select which `ssn_mode` to use for pattern matching of Social Security numbers.

However, BEViewer does allow users to specify particular [regular expressions](#) to search for, the results of which are written into the "find.txt" feature file.

In the "Run bulk\_extractor" menu, the user can enter a regular expression directly into the GUI using the "Use Find Regex Text" option or provide a regular expressions file to Bulk Extractor with the "Use Find Regex Text File" option.

To find all valid SSNs matching the patterns `#####`, `### ## #####`, or `###-##-####`, you can use the following regex:

```
^(?!219-09-9999|078-05-1120)(?!666|000|9\d{2})\d{3}-(?!00)\d{2}-(?!0{4})\d{4}|((?!219 09 9999|078 05 1120)
(?!666|000|9\d{2})\d{3} (?!00)\d{2} (?!0{4})\d{4})|((?!219099999|078051120)(?!666|000|9\d{2})\d{3}(?!00)\d{2}
(?!0{4})\d{4}))$
```

## Using an FC5025 with the BitCurator VM

See this post: <http://www.wcsarchivesblog.org/getting-data-out-of-its-floppy-cage/> for additional guidance.

## FAQ

### Is BitCurator intended to be a data preservation environment?

#### Problem

I'm trying to determine if BitCurator can be used as a discrete data preservation environment.

#### Solution

BitCurator is **not a data preservation environment**. BitCurator is intended to support existing long-term data preservation environments, both as a data triage system and as a provider of software that may be integrated as microservices into existing toolchains. BitCurator depends on and produces only open source and public domain software, in order that the technologies may be fully integrated into existing Free data management and preservation environments such as [Archivematica](#).

### I work at a small institution with limited resources. Am I going to need an expensive new dedicated workstation just to do digital forensics work?

#### Problem

Determining if the hardware requirements for digital forensics tools are within my budget.

#### Solution

Modern digital forensics workstations incorporate features such as built-in write-blockers, hard-disk cooling trays, and dedicated storage media for local artifacts and databases in order to support a high level of performance and low level of failure in risk-reduced environments. The higher initial cost (relative to a standard workstation) is often offset by the simplicity of having an integrated, manufacturer-supported solution.

However, most of the functionality can be replicated on standard desktop hardware using add-on write blockers. If you have a clear plan for the types of media you will be working with, purchasing standalone write-blockers, external drives, and cooling solutions to work with existing hardware can lower the overall cost.

### The BitCurator virtual machine is built for VirtualBox. Can I use VMWare instead?

#### Problem

Trying to run the virtual machine in VMWare.

#### Solution

The BitCurator VM is shipped as a .vdi, which is VirtualBox-specific. You can convert a .vdi to .vmdk (the VMWare native format) by following the instructions on [this page](#).

This process can be somewhat involved. A **more reliable alternative** is simply to create a new VMWare-specific VM and install BitCurator on that using the BitCurator ISO.

### What's a hardware write-blocker? Do I really need one?

#### Problem

Determining whether a hardware write-blocker is appropriate for my use case.

## Solution

A hardware write-blocker is a device that connects to your host machine and prevents inadvertent changes to writeable media. Changes can be caused by modern operating systems at the time of connection even if you do not issue an explicit command or action within the operating system. Detailed information is available at [the forensics wiki](#). We recommend that you use a hardware write blocker with all writable media, in order to prevent hidden, accidental, and malicious changes. We do not make specific hardware recommendations; the BitCurator project has successfully tested Tableau USB writeblockers, Tableau Ultrabays, and Digital Intelligence read-only switchable 3.5" floppy drives with a variety of media.

NIST has prepared a series of technical reports on tests of software write blockers. The reports can be found at [software write block tools page](#).

## What's the advantage of saving my disk images as AFF or E01 rather than raw?

### Problem

Determining whether or not a forensic disk image format is appropriate for my use case.

### Solution

Both the **Advanced Forensic Format** (AFF) and **Expert Witness Format** (E01) file formats supported by BitCurator store bitstreams compressed, and incorporate metadata about the capture process and device configuration. There are some known issues with AFFv3 when working with heavily fragmented NTFS volumes. The original developer recommends the use of E01, which has a [fully open](#) library for read and write access.

Forensic formats can provide an additional degree of resilience against bitrot in the long term, as file damage can be isolated to checksummed segments within the image.

## What file systems does BitCurator support?

### Problem

Determining which file systems are supported by BitCurator.

### Solution

BitCurator natively supports FAT16, FAT32, NTFS, HFS, HFS+ and ext2, 3, and 4. The various forensic tools included may support only a subset of these (for example, The Sleuthkit does not provide support for legacy HFS).

The BitCurator virtual environment can recognize and provide browsable access to additional file systems, but many of the tools that we rely on (including fiwalk for producing file system hierarchical metadata) are currently limited to these file systems.

Note that stream-based tools, such as bulk\_extractor, will attempt to extract relevant features irrespective of the underlying file system, although the effectiveness of the feature extractors will be limited in cases where the underlying file formats are not recognized.

## Will BitCurator help me crack passwords on encrypted files in my collection?

### Problem

I'm trying to decrypt or crack a specific item within my collection.

### Solution

BitCurator does not currently include password or encryption cracking tools. There are many good [commercial](#) and [open source](#) tools to help you do this, some of which can be installed in BitCurator.

If you would like to provide feedback for this page, please follow this [link to the BitCurator Wiki Google Form](#) for the Troubleshooting and FAQ section.