

# guymager homepage



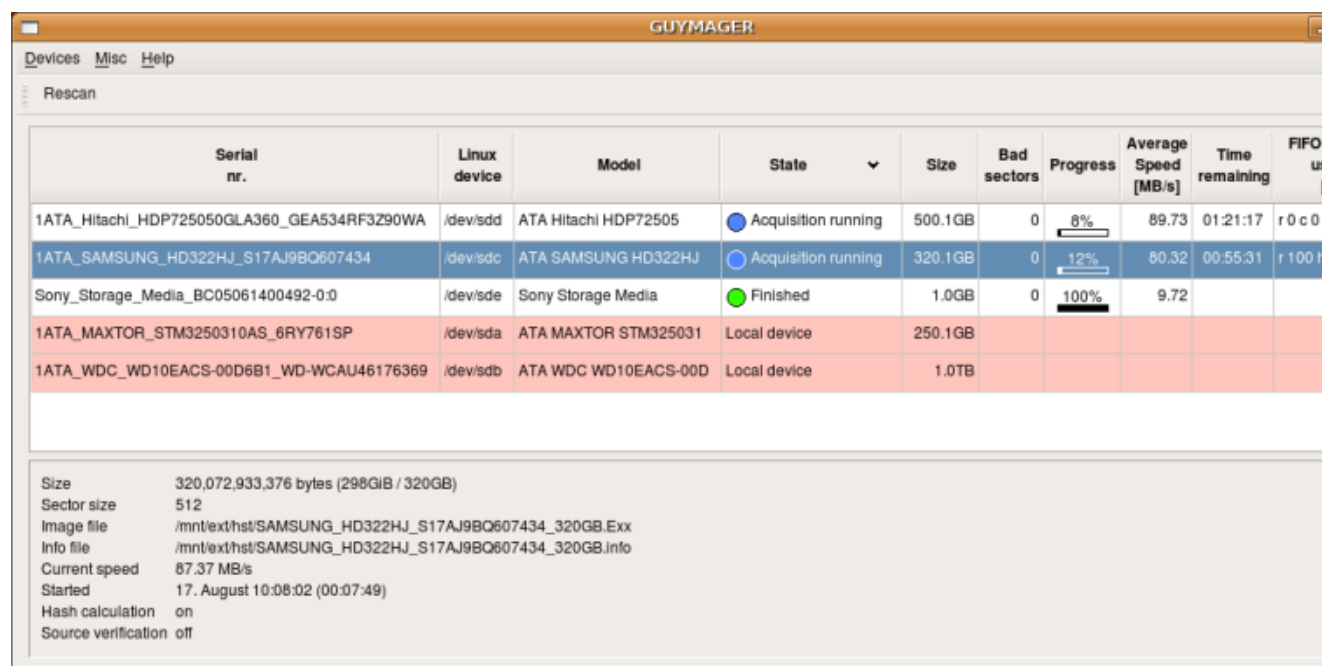
## Introduction

guymager is a free forensic imager for media acquisition. Its main features are:

- Easy user interface in different languages
- Runs under Linux
- Really fast, due to multi-threaded, pipelined design and multi-threaded data compression
- Makes full usage of multi-processor machines
- Generates flat (dd), EWF (E01) and AFF images, supports disk cloning
- Free of charges, completely open source

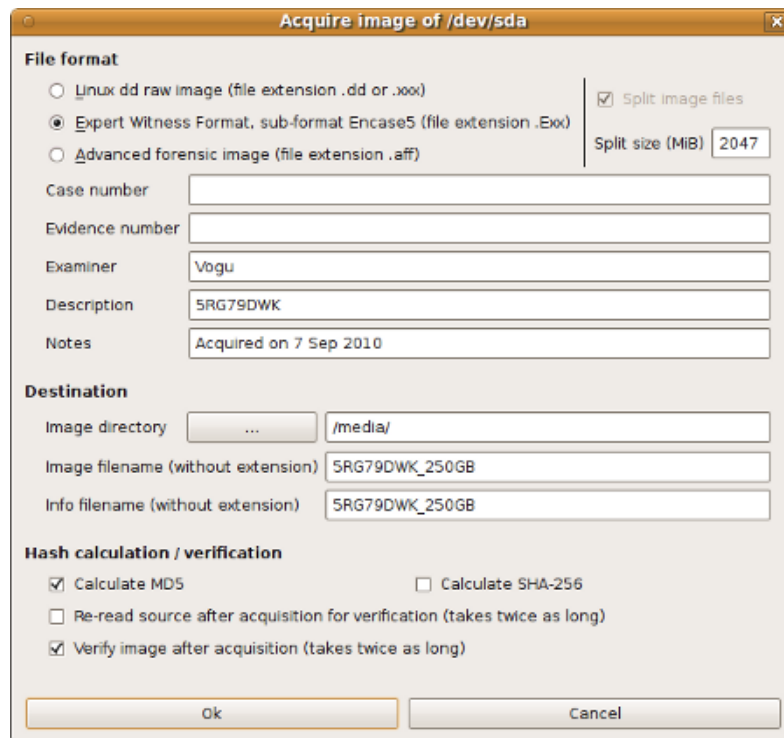
The latest version is 0.6.2

## How it looks



### Explanations:

- The connected storage devices are listed in the upper part. New devices can be connected at any time - press the rescan button for displaying them.
- The devices marked with light red color are local hard disks. They cannot be acquired, thus preventing from acquiring the wrong disks. Local hard disks are recognised by their serial numbers which can be entered in the configuration file.
- The lower part shows more detailed info about the acquisition currently selected by the blue cursor.



The above screenshot shows the default acquisition dialog. Another dialog exists for cloning disks. Both can be easily adapted to fit your requirements. You may add or remove fields. You can set their default values statically (text) and dynamically (current date, size of disk, serial number, ...). Have a look at </etc/guymager/guymager.cfg>.

## Installation

### Debian and Ubuntu

Guymager is contained in the standard repositories of several distributions, for example Debian (Squeeze or later) and Ubuntu (10.04 or later). In Ubuntu, the universe repository must be activated. You may select the Ubuntu menu System / Administration / Software Sources for doing so.

Installation can be done with a graphical tool like Synaptic. The command line is a safe and easy alternative:

```
sudo apt-get update
sudo apt-get install guymager
```

Unfortunately, Guymager doesn't start on new Ubuntu releases due to a change inside Ubuntu. It therefore is recommended to use the penguin APT server, see below.

### Using the penguin APT server

Daniel's penguin server always contains the latest Guymager release. **It is the recommended repository** for installing Guymager and keeping it up to date. Use this repository for your Ubuntu, Debian and Debian-based Linux systems.

Follow these steps:

1. Add the penguin server and its public key by executing the following commands:

```
sudo wget -nH -rP /etc/apt/sources.list.d/ http://deb.penguin.lu/penguin.lu.list
```

```
wget -q http://deb.penguin.lu/debsign_public.key -O- | sudo apt-key add -
```

Currently, i386 and amd64 systems are supported, powerpc packages are available upon request.

**2. Execute the following commands:**

```
sudo apt-get update
sudo apt-get install guymager-beta smartmontools hdparm
```

**3. Start the program with**

```
guymager
```

Eventhough the package is named guymager-beta, it has been intensively tested and is absolutely stable software. It just hasn't found its way into a distribution yet.

## RPM packages

RPM packages are available at the [CERT homepage of the Carnegie Mellon University](#). Many thanks to Larry Rogers for his work!

## Manual download and installation of the Debian packages

If you do not like to add the penguin repository permanently, you can download and install the packages manually:

1. Browse to [apt.penguin.lu](http://apt.penguin.lu), and choose the directory corresponding to your processor architecture (i386 or amd64).  
Remark: amd64 refers to the architecture, not the processor. So, amd64 is ok for both, the AMD and Intel 64 bit processors.
2. Download the guymager-beta package.

Installation from the command line:

1. Open a shell and get root rights
2. Change to the directory with the files you downloaded.
3. Use the following commands for the installation:

```
apt-get update
dpkg -i guymager-beta_xxx_i386.deb
apt-get -f install
```

xxx stands for the version number. In case you have a 64 bit system, replace i386 by amd64.

The 2<sup>nd</sup> command most probably returns some error messages about missing packages. They are installed by executing the 3<sup>rd</sup> command.

4. There are 2 recommended packages you should install as well:

```
apt-get install smartmontools hdparm
```

5. Start the program with

```
guymager
```

## Configuration and log

guymager works with two configuration files:

- /etc/guymager/guymager.cfg

The main configuration file. **You should not change it**, as your changes get lost when installing a new version of guymager.

- `/etc/guymager/local.cfg`  
Use this file for local changes instead. The parameters adjusted here have precedence over those in `guymager.cfg`. `guymager.cfg` includes `local.cfg` at its very end. If a parameter is set several times, guymager retains the last setting.

If you want to try a parameter quickly without editing `local.cfg`, you may put it on the command line. For example:

```
guymager EwfCompression=BEST
```

The command line precedes both configuration files. There are 2 parameters which only can be set on the command line:

- `cfg` - The configuration file to be used. The default is `/etc/guymager/guymager.cfg`.
- `log` - The log file to be used. The default is `/var/log/guymager.log`.

Example:

```
guymager cfg="/tests/g_special.cfg" log="/mylogs/guymager.log"
```

The configuration parameters are well documented inside `/etc/guymager/guymager.cfg`. Just remember not to do any changes there.

If ever there's a problem, have a look at the log file `/var/log/guymager.log`. Please attach the log file when reporting a problem.

## Compiling the source code

For compilation and packaging on Debian based systems refer to the end of this section.

Get the source code:

- guymager's source is stored in a subversion repository on sourceforge. Go to the [developer page of the guymager project](#) and follow the instructions given there (execute the command starting with `"svn co ..."`, you need to have subversion installed).
- The same procedure applies to [libguytools](#).
- The sources for libewf can be downloaded directly from sourceforge. Go to the [libewf project](#) and choose "Browse all files". Choose the latest non-beta release (20100226 at the time of this writing) and download the ".tar.gz" file.

Let's start with libewf:

1. Unpack the archive
2. Compile and install with the standard command trio `configure`, `make`, `make install`. Missing libs and tools have to be installed, refer to the error messages. You probably have to go several times through the "install missing libs / configure" cycle until everything is ok.
3. After successful completion of the 3 commands, you not only have the lib required by guymager, but the libewf tools as well. So, it's easy to check if libewf works fine. Try for instance to run `ewfinfo` on a EWF (E01) image if you have one available. Try `ewfacquire` on a memory stick otherwise (see the man pages for details).

Next comes libguytools:

1. Change to the directory where you did the subversion checkout, go to the subdir `tags` and further down to the latest version.
2. To compile libguytools:  
`./create_version_file.sh`

```
qmake trunk.pro
make
```

Most probably, there will be some tools or libs missing, for instance the Qt developer stuff (libguytools uses qmake). The same procedure as before applies (install/retry /install...). In case where several Qt versions and packages contains the required commands or libs, always choose Qt version 4.

3. Next, a statically linkable version of the lib is built:

```
qmake toolsstatic.pro
make
```

4. There is no installation procedure (except for Debian, see above). After completion of the previous step, the lib is in the subdirectory lib. Copy it to a location that is included in the search path on your system (this could be /usr/local/lib, for instance) or redirect the LD\_LIBRARY\_PATH environment variable.
5. Make the headers from the subdirectory "include" available to other applications (for instance by copying to /usr/local/include).

And finally, guymager:

1. Change to the directory where you did the subversion checkout, go to the subdir tags and further down to the latest version.
2. Create the Makefile:
 

```
qmake
```
3. Compile:
 

```
make
```

If ever you have problems with the include path of libguytools: You can add it in the file guymager.pro (re-execute qmake afterwards).

4. Create the language files:
 

```
lrelease guymager.pro
```
5. Copy the configuration file guymager.cfg to /etc/guymager/

guymager should now be ready. Start it with:

```
./guymager
```

Compilation and packaging on a Debian based system is easier. Get the sources of libewf, libguytools and guymager as described above. Then:

1. Make sure you have the package dpkg-dev installed.
 

```
aptitude install dpkg-dev
```
2. Unpack libewf, change into the directory and execute
 

```
dpkg-buildpackage -B -uc -rfakeroot
```

Follow the instructions given. Most probably, you will be told to install some additional packages before the compilation and packaging can begin. At the end you will get .deb packages in the directory above.
3. Do the same for libguytools.
4. Do the same for guymager. You will be told to install some of the packages you created in the previous steps (libguytools, libguytools1-dev, libewf and libewf-dev). Install these packages by means of dpkg -i (see above for the usage of dpkg).

## Live CDs with guymager

**Guymager is contained on these live CDs:**

- **FCCU**
- **GRML**
- **DEFT**
- **CAINE**
- **PeriBR**
- **Matriux**
- **DFLCD**
- **Forlex**
- **Forens\*nix**

## **Contact**

The author of guymager can be reached by an email to vogu00 at gmail point com. If ever you want to report a problem, be sure to attach the guymager log file.

## **Disclaimer**

The author of guymager and these pages is not responsible, not liable nor anything else for the content of extern web pages that are linked on this website nor for extern web pages linking to this one, nor for anything else. There is no garantuee for any software to work and any software may damage anything.

LPO

Nice photos on [irika.lu](http://irika.lu) - [photographe mariage](#)