

Compiling Barnyard2 for Cygwin/Win32

Contents

Cygwin Setup:	2
Install PostgreSQL:	4
Install MySQL:	5
Extract Pcap Libraries:.....	5
Compile Barnyard2:	6
Standalone or Portable Install:	6
Full MySQL Error:	7

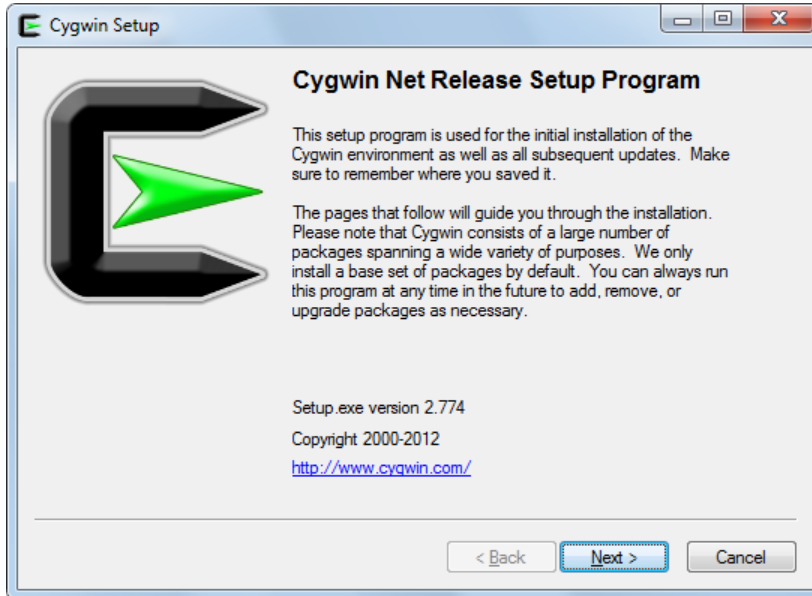
This guide assumes you do not have any version of Cygwin currently installed or in use on your system. It also assumes you do not have any experience setting up said environment, and this guide documents the bare minimum configurations for building Barnyard2 for Win32. If this does not apply to you, skip to [page 4](#) and beyond.

Compiling Barnyard2 for Cygwin/Win32

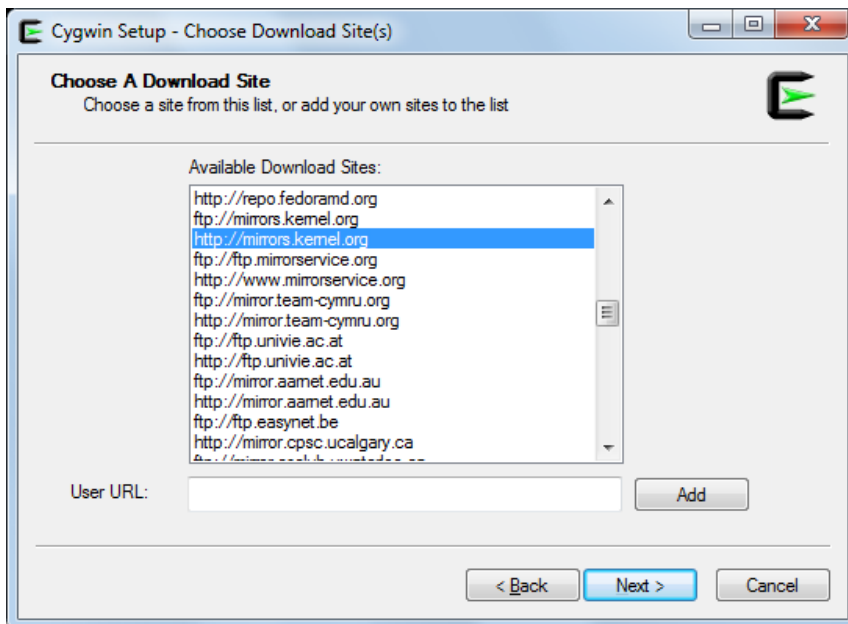
This guide only applies to Barnyard 2 from the “pre-stable” branch found here: <https://github.com/binf/barnyard2/tree/pre-stable> Your mileage may vary, you have been warned.

Cygwin Setup:

Download and run/install cygwin: <http://cygwin.com/setup.exe>

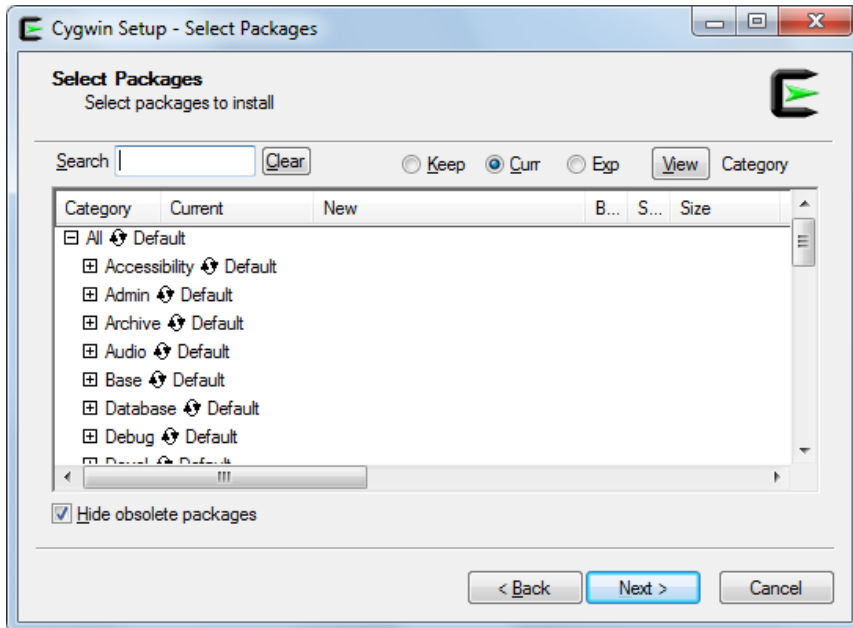


Next, then “Install from Internet” (default) click Next. Use the default “All Users”- Next, Set the path you want Cygwin to download packages to, click next. Choose direct connection (default), Select a mirror from the list, typical mirrors that are fast are <http://mirrors.kernel.org> and <ftp://mirrors.kernel.org>.

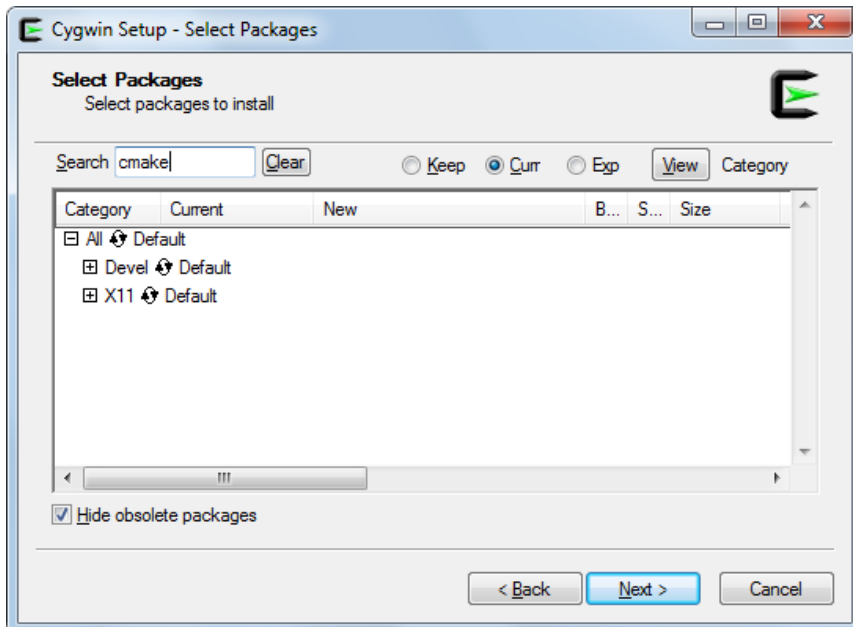


Compiling Barnyard2 for Cygwin/Win32

Highlight the mirror you chose then click “Next”. After the package lists are downloaded you can start choosing what to install by using the Search field:

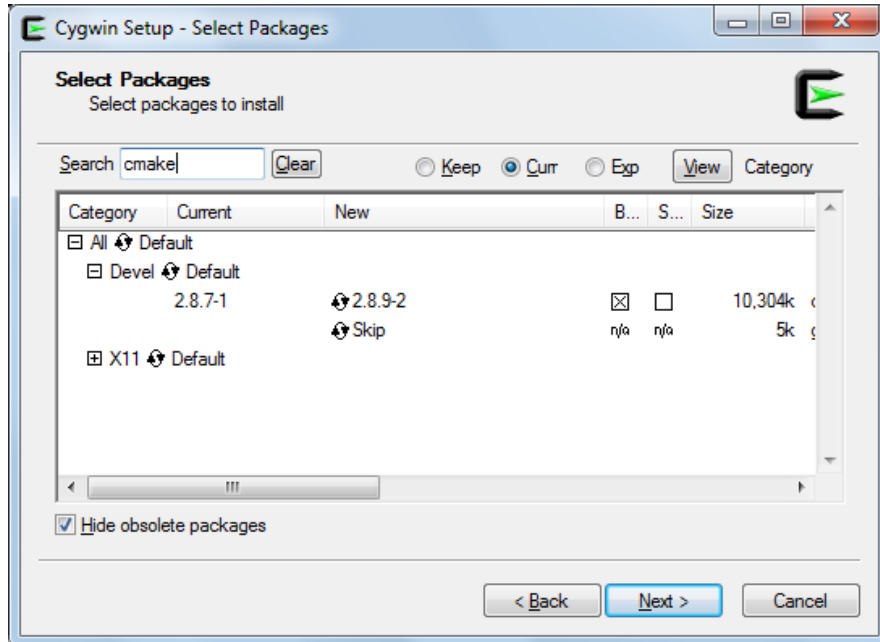


For instance, typing “cmake” will narrow down the results a great deal:



Clicking the PLUS next to the “Devel” category will expand and show you the current state of the package

Compiling Barnyard2 for Cygwin/Win32



Make sure “SKIP” is not selected, if it is, click the word “skip” and change it to a file version, in the example above that version is 2.8.7-1. Do the same to all the packages list below.

You will need the following packages, the Cygwin setup will figure out additional packages and dependencies to install as well.

autoconf **automake** **binutils** **bison** **cmake** **gcc** **gcc-core**
libtool **make** **openssl-devel** **readline** **zlib-devel** **perl**

Once you’ve chosen all of those packages (all located in the Devel category), you can click next and next again and all the dependencies will be added in for you. Click Finish and your Cygwin environment should be ready for the next steps after everything is installed and the Cygwin Terminal icon is on your desktop and or in the start menu.

Install PostgreSQL:

The version tested and used in this build is beta:

<http://ftp.postgresql.org/pub/source/v9.2beta4/postgresql-9.2beta4.tar.gz>

Extract to C:\cygwin\postgresql (7zip is used in this guide)

In the Cygwin terminal window run:

```
cd /cygdrive/c/cygwin/postgresql
./configure
make
make install
```

Compiling Barnyard2 for Cygwin/Win32

Install MySQL:

This is the only step that requires any effort. One file needs to be edited (dtoa.c), or you can try the find replace script I cobbled together, but it's probably best to do it manually ☺

Change directory (cd) to the mysql directory in the cygwin terminal
cd /cygdrive/c/cygwin/mysql

Run the configure perl script (located in the cmake directory)
perl cmake/configure.pl

Now you need to find and replace the instances of "dtoa" and "DTOA" in the dtoa.c file to avoid getting this error "dtoa.c:55: error: conflicting types for 'dtoa'"

(See the full error at the end of this guide)

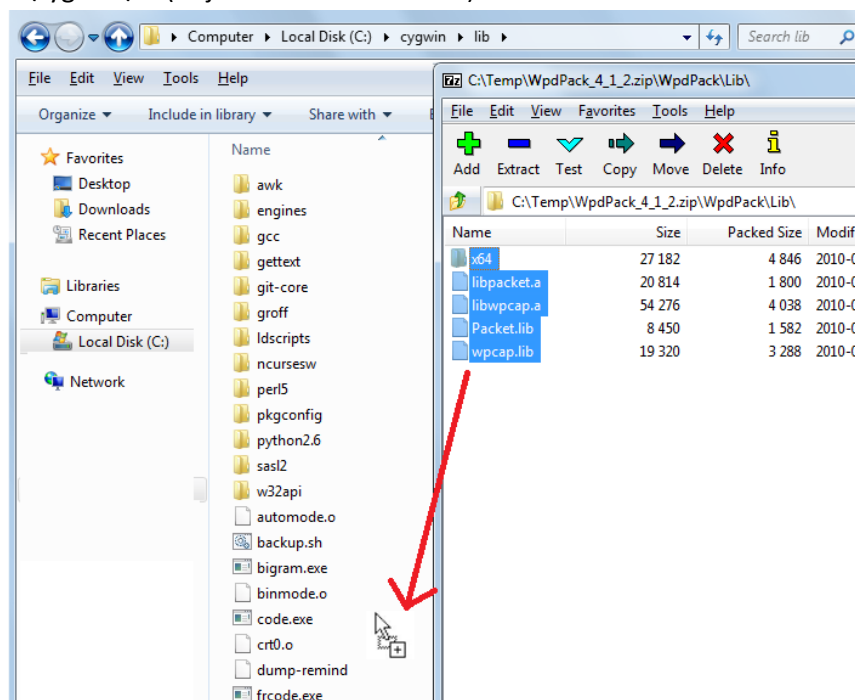
Replace "dtoa" with underscore dtoa (_dtoa) and do the same for the uppercase version, you can use the script below to do it for you:

```
perl -pi -e 's/dtoa/_dtoa/g;s/DTOA/_DTOA/g;' strings/dtoa.c
```

Once you have changed those "dtoa's" you can then make the mysqlclient
make mysqlclient
make install

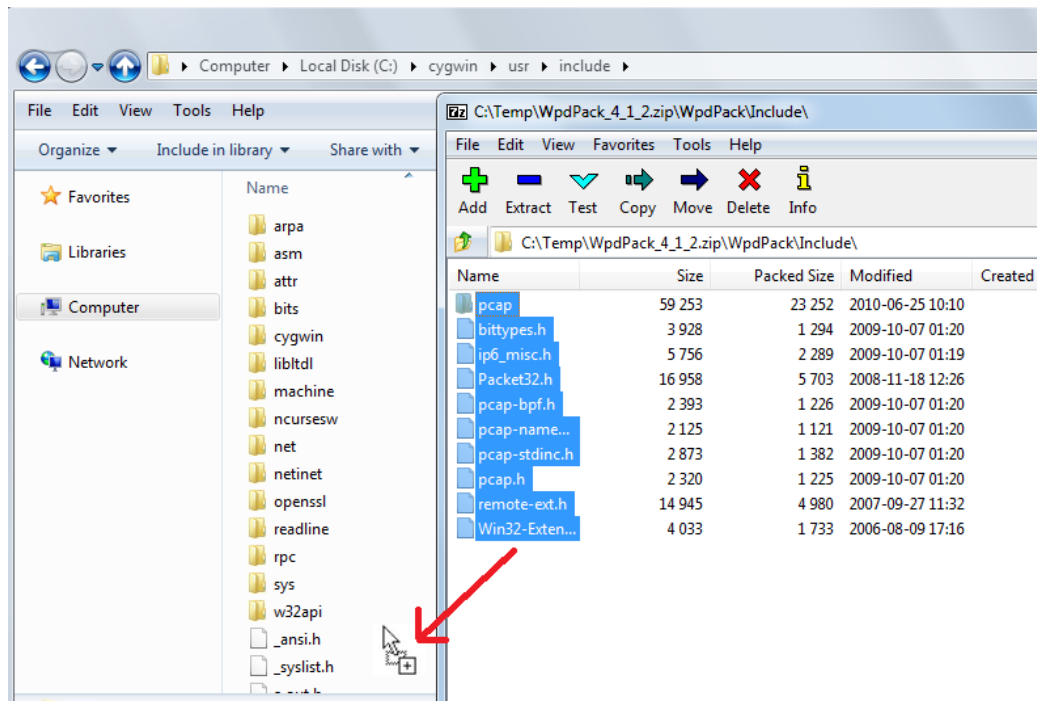
Extract Pcap Libraries:

Download the winpcap developer's pack: <http://www.winpcap.org/devel.htm> I use 7zip, with the winpcap (WpdPack_4_1_2.zip\WpdPack\Lib) package open, select all (ctrl+a) and drag it to c:\cygwin\lib (or just extract it to there)



Compiling Barnyard2 for Cygwin/Win32

Do the same to the Include directory of the winpcap package, this time copy or extract to c:\cygwin\usr\include



Compile Barnyard2:

Download and extract By2 to C:\cygwin\barnyard2. *NOTE* As of this writing the "Pre-Stable" branch is the latest version that is working properly for win32 builds of barnyard2. You can download the version used in this guide here: <https://nodeload.github.com/binf/barnyard2/zipball/pre-stable>

```
cd /cygdrive/c/cygwin/barnyard2
./autogen.sh
./configure --with-mysql --with-postgresql
make
make install
```

Once that is done By2 is made and ready to be used on this client. To make a standalone or portable version please read the next section.

Standalone or Portable Install:

You must copy the following files into the same directory to use By2 on any machine it was not compiled or "installed" on. Create a folder/directory called "by2" (for example)

```
mkdir /cygdrive/c/cygwin/by2
cp /cygdrive/c/barnyard/src/.libs/barnyard2.exe /cygdrive/c/cygwin/by2/
cp /cygdrive/c/cygwin/bin/cygwin1.dll /cygdrive/c/cygwin/by2/
cp /cygdrive/c/cygwin/usr/local/mysql/lib/cygmssqlclient-18.dll /cygdrive/c/cygwin/by2/
cp /cygdrive/c/cygwin/bin/cygz.dll /cygdrive/c/cygwin/by2/
cp /cygdrive/c/cygwin/bin/cyggcc_s-1.dll /cygdrive/c/cygwin/by2/
cp /cygdrive/c/cygwin/usr/local/pgsql/lib/cygpq.dll /cygdrive/c/cygwin/by2/
```

Compiling Barnyard2 for Cygwin/Win32

After that you should have a working Barnyard2.exe. You can also use the barnyard2.conf file found in the "etc" directory of the barnyard2 source code, or if you want a minimalist version you can edit accordingly and use the following:

#Example By2 Config file by Rich Rumble

config classification_file: C:\Snort\etc\classification.config

config gen_file: C:\Snort\etc\gen-msg.map

config reference_file: C:\Snort\etc\reference.config

config sid_file: C:\Snort\etc\sid-msg.map

input unified2

output database: log, mysql, user=snort-user password=SXhPnC3wa7bhnaSq dbname=snort host=127.0.0.1

#NOTE# Use 127.0.0.1 instead of "localhost" on windows!

NOTE: Remember the username and password for your environment need to be changed ☺

FULL MYSQL ERROR:

```
/cygdrive/c/cygwin/mysql/strings/dtoa.c:55: error: conflicting types for 'dtoa'
/usr/include/stdlib.h:162: error: previous declaration of 'dtoa' was here
/cygdrive/c/cygwin/mysql/strings/dtoa.c:55: error: conflicting types for 'dtoa'
/usr/include/stdlib.h:162: error: previous declaration of 'dtoa' was here
strings/CMakeFiles/strings.dir/build.make:583: recipe for target
`strings/CMakeFiles/strings.dir/dtoa.c.o' failed
make[3]: *** [strings/CMakeFiles/strings.dir/dtoa.c.o] Error 1
CMakeFiles/Makefile2:1711: recipe for target `strings/CMakeFiles/strings.dir/all'
failed
make[2]: *** [strings/CMakeFiles/strings.dir/all] Error 2
CMakeFiles/Makefile2:2048: recipe for target
`libmysql/CMakeFiles/mysqlclient.dir/rule' failed
make[1]: *** [libmysql/CMakeFiles/mysqlclient.dir/rule] Error 2
Makefile:749: recipe for target `mysqlclient' failed
make: *** [mysqlclient] Error 2
```

The error above is from a conflict in the dtoa.c file, while the fix I use may not be the best or most correct way of dealing with the error, it is the only one I know or that I am capable of doing ☺