

# Working With UCF's ProcDump32

The Best Unpacker On Earth

By = hades = [PNC/KAC]

Hey everybody! In this tut i'll show you how to work with ProcDump...  
Maximize notepad for the best result

## Some Basic Info

### About Procdump32

ProcDump is a tool to dump the contents of packed executables on your hard drive and has even some other great stuff too. It is mainly written by three people: G-RoM, Lorian and Stone of UCF2000.

### Procdump's Main Screen

If you start ProcDump you'll see 2 lists and a row of buttons. The first list contains all running processes under Windoze. The second list contains all modules attached to a certain process.

On the left you'll see 7 buttons:

- Unpack: Unpack a executable or dumpfile from your hard drive
- Rebuild PE: Rebuilds the PE header of a executable or dump file from your hard drive
- PE Editor: let's you edit a PE header
- Bhrama Server: Starts the Bhrama Server
- Options: let's you change options in the program (READ THE PROCDUMP.TXT FILE SUPPLIED WITH IT CAREFULLY)
- About: Shows information about ProcDump
- Quit: Exit from ProcDump

### The Task List

When you click on a task on the task list you'll notice two things:

- The module list will fill itself with modules (DLL's) which are  
<http://66.98.132.48/krobar/beginner/104.txt> (1 of 4)1/2/2004 3:27:23 PM  
<http://66.98.132.48/krobar/beginner/104.txt>  
attached to the task

You have the ability to access a popup menu. The options in the popup menu are:

- Dump (FULL): let's you fully dump an active process to your hard drive
- Dump (PARTIAL): let's you partially dump an active process to your hard drive
- Kill Task: Shuts down a task
- Process Infos: Pops up the PE Editor with info about the active task
- Refresh List: Freshes up the Task List

### The Module List

If you rightclick on a module in the module list a popup menu will show up. There are 2 options available in the popup menu:

- Dump (FULL): Fully dumps a module to your hard drive

# WORKING WITH UCF's ProcDump32

The Best Unpacker On Earth

By = hades = [PNC/KAC]

- Dump (PARTIAL): Partially dumps a module to your hard drive

## Unpacking An Application

First you'll have to click the Unpack button. After that you'll have to choose the packer which protects the program (like Shrinker, VBox or SoftSentry) (BTW: We will see how to add protections later)

Now an Open Dialog will pop up. Choose the executable you want to unpack and hit open.

Now ProcDump will load the executable in memory. If it is done hit OK and the program will unpack itself nicely.

## Adding Protections

I'll use WinAmp v2.0 as an example.

First open script.ini with Notepad or another ASCII editor. Find the section INDEX and add an entry for WinAmp v2.0 eg.

```
[INDEX]
http://66.98.132.48/krobar/beginner/104.txt (2 of 4)1/2/2004 3:27:23 PM
http://66.98.132.48/krobar/beginner/104.txt
P1=Hasiuk/NeoLite
P2=PESHIELD
P3=Standard
P4=Shrinker 3.X
P5=WinAmp v2.0 example (<- THIS IS THE ADDED ENTRY)
```

Now create a section with the same name as your entry eg.

```
[WinAmp v2.0 example]
```

and add the following lines:

L1=LOOK E9,46,53,F5,FF (seek 497970, the location where the decompressed code starts)

L2=BP (put a breakpoint there)

L3=STEP (do a step by step analysis and write the decrypted data on disk) and your done.

Save the file to disk start ProcDump and you easily can unpack WinAmp v2.0.

## The Brahma Server

The Brahma server is used to write your own custom plugins for ProcDump. You'll have to find out how this thingy works on yer own cause I didn't had time to properly check this out.

## Final Words

Well this is the FIRST release of this tut... If you have any contributions, comments or additions contact me ASAP (ofcourse your name will be mentioned in the credits of the revision).

I really hoped you liked it... if not FUCK YOU hehehe.