Reverse Engineering

T.A. Gonsalves, IIT Mandi
23rd September 2011

This document contains simple step-by-step instructions for reverse engineering a large software application for which you have the source code.

1. Read available documentation. This is usually inadequate
2. Obtain the complete source code
3. Draw the directory structure.

   Examine a few files in each directory & document the purpose of that directory.
4. Figure out filename conventions
5. Find the "main" file and write pseudo-code for it.

   Find the main data structures

   Figure out the conventions: Function naming, variable naming
6. For each "module", list all files

   in each file, list all functions & global variables

   Prepare a data dictionary containing a list of all names; for each name, its type and a short description

   draw the function call tree

   Document each function & global variable with one line each
7. Draw diagrams → block diagrams of modules and data structures
8. For some function of interest, write pseudo-code
9. Build the original source code and execute
10. Modify some function of interest, build, execute and test

If you have done a good job, contribute your documentation and modifications back to the maintainers of the software application.