

DISASSEMBLE FOR WINDOWS PORTABLE EXECUTABLE (PE) FILES

Prepared by: Nyeo Heng Seng

ABSTRACT

The Win32 Portable Executables Format (PE) was designed to be a standard executable format for use on all version of Win32 platform on all supported processor. The PE file types are; EXE, DLL, SYS, DRV, MSSTYLE, CPL, OCX, BPL, DPL, SCR and more. This project addresses issues on good understanding of the Portable Executable file format leads to a good understanding of the operating system. It focuses on the development or design of the data structure for all PE files. The project sought solutions on reading out the internal arrangements of PE files. It researches new methods, techniques on memory address reading when the PE files have loaded into the memory by windows loader. Ultimately, this project aims to solve problems that encountered by serious development projects, for restoring lost information, to reverse engineer projects with missing source code.