**Lab 16: Using Kernel Debugging Commands with WinDbg**

**Course Name**: Malware Analysis and Reverse Engineering (IAM302)

**Student Name**: Nguyễn Trần Vinh – SE160258

**Instructor Name**: Mai Hoàng Đỉnh

**Lab Due Date**: 15/3/2023

**Purpose**

Practice using simple WinDbg commands.

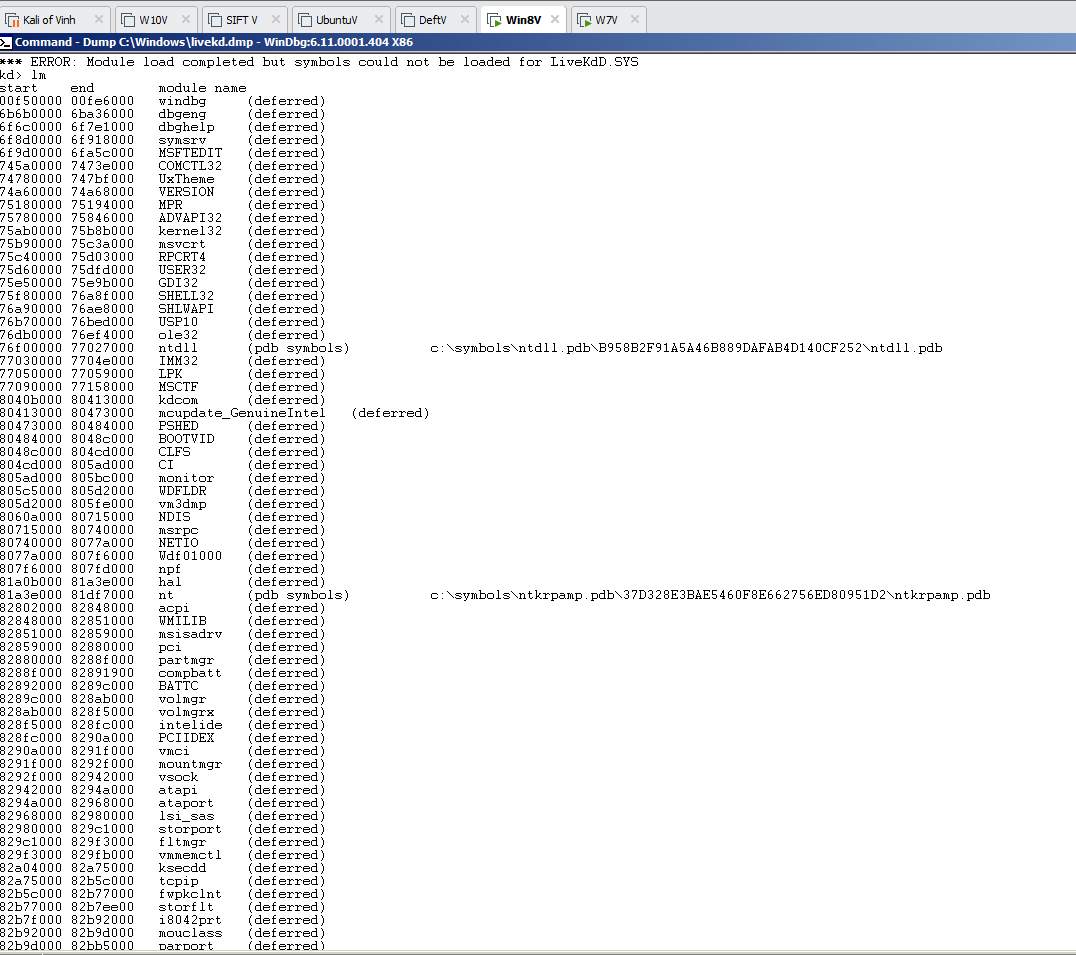
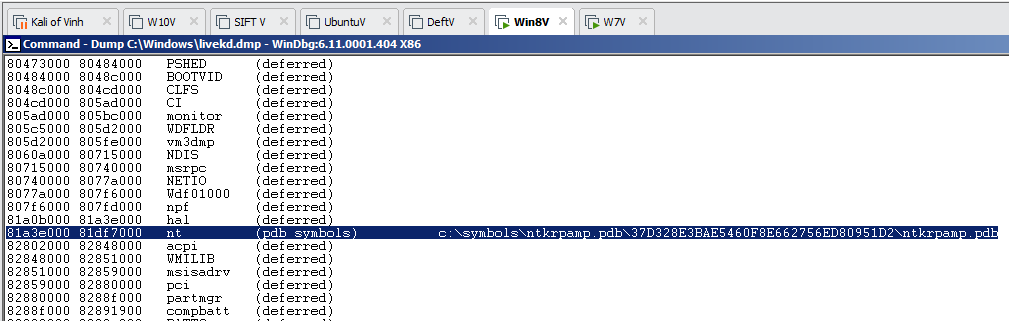
**What You Need**

A Windows 10 machine with Livekd working, as prepared in the previous project. This project should work on Win 7 or any later version, but I only tested it on Windows 10

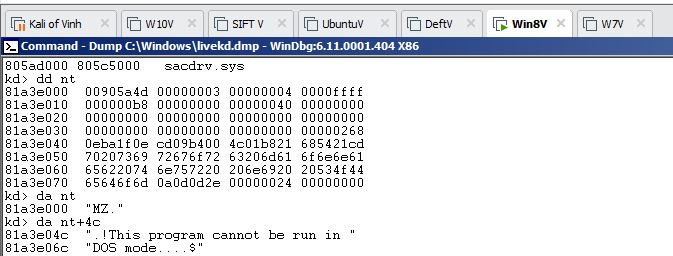
**Starting Configuration**

You should have Livekd running, which launched WinDbg, as you did at the end of the previous project

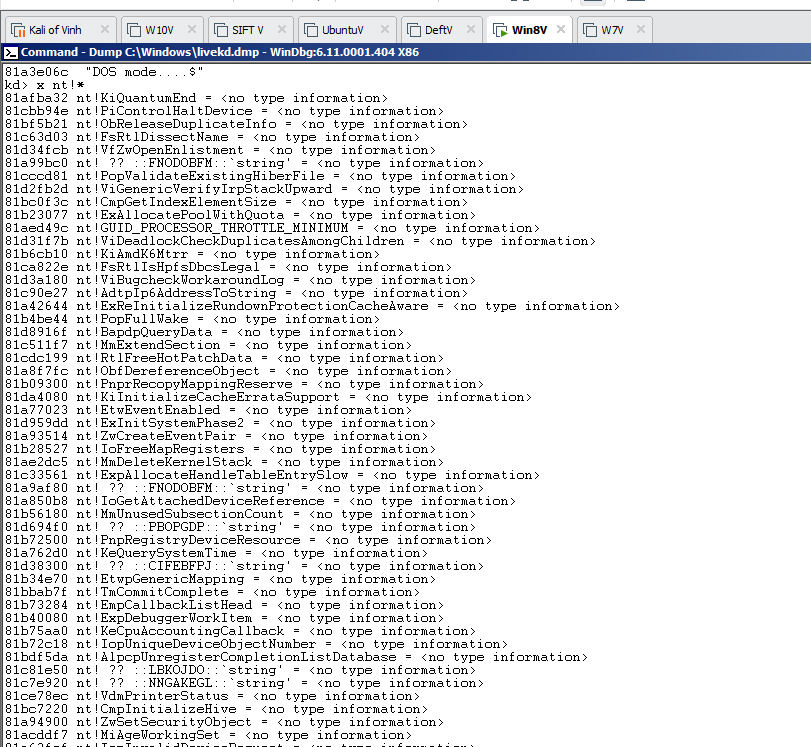
**Listing Modules with lm**

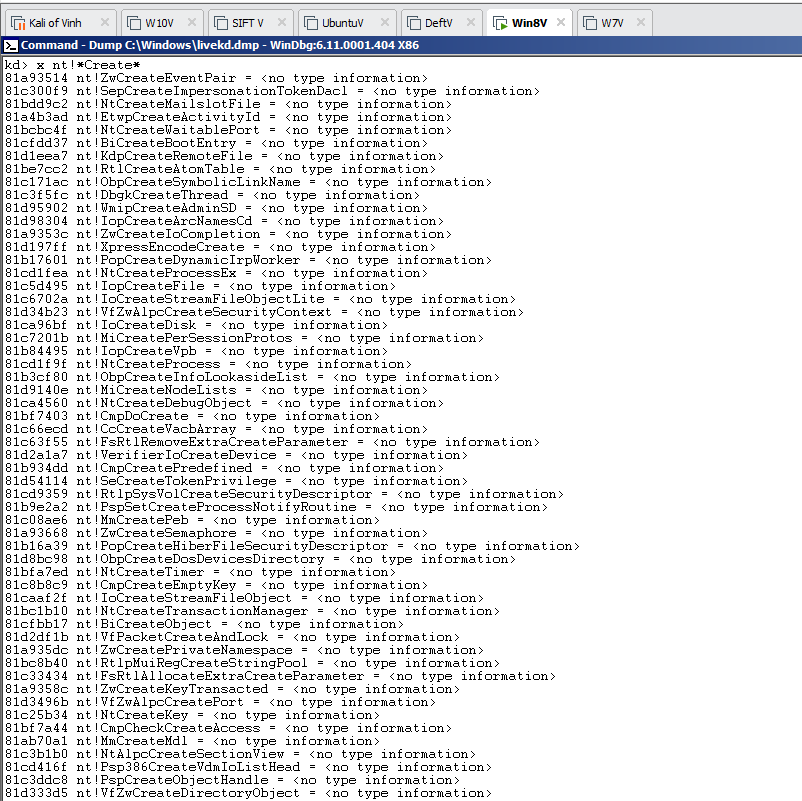
** **

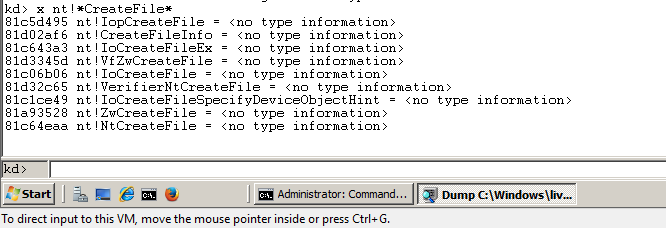
**Viewing Memory**

****

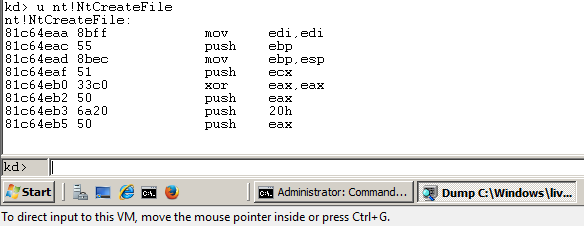
**Searching for Functions**

****

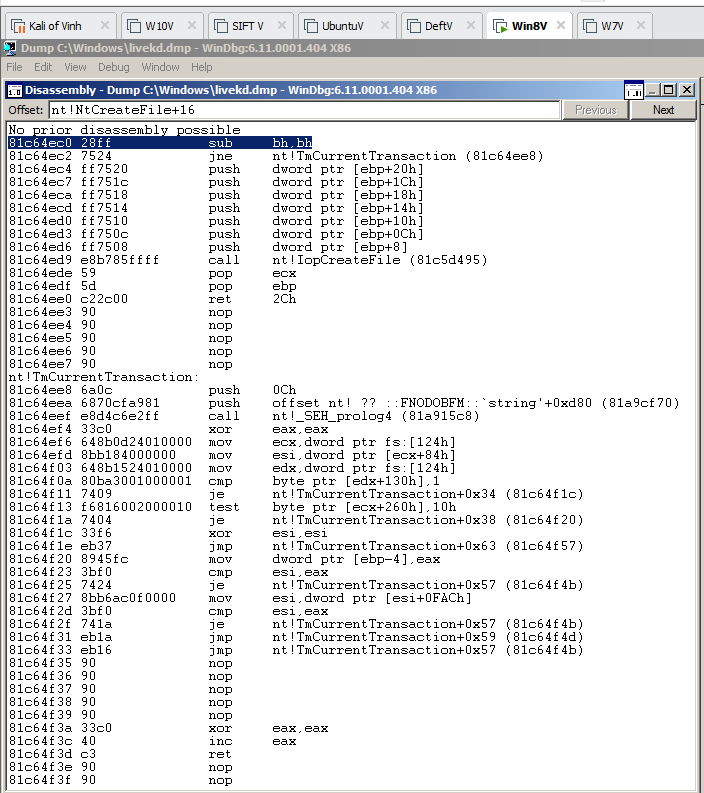
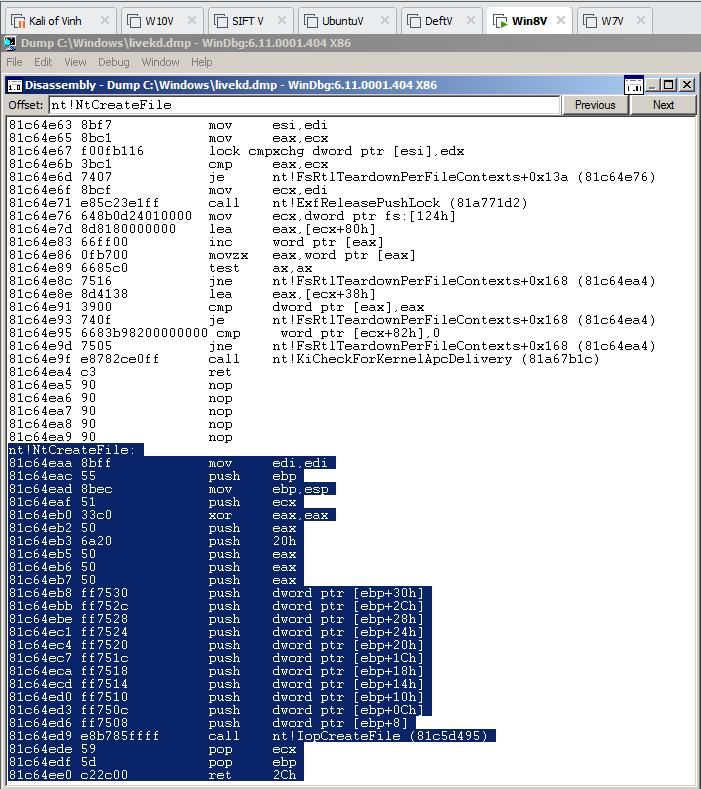
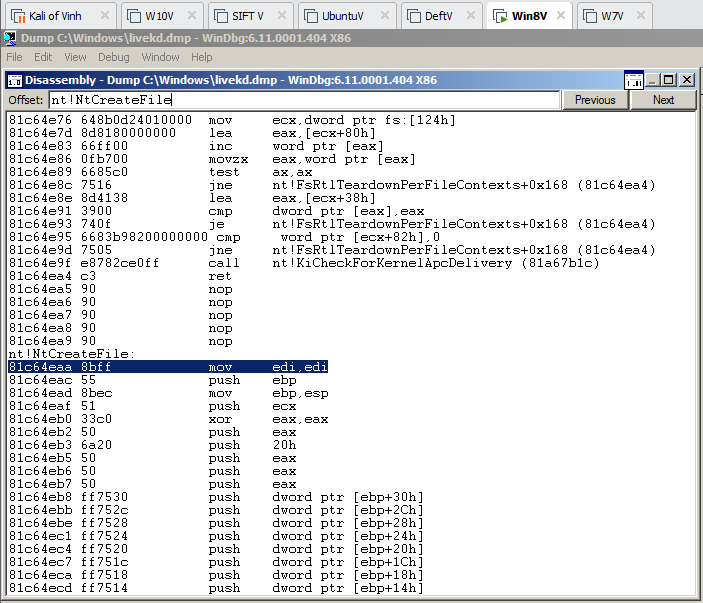
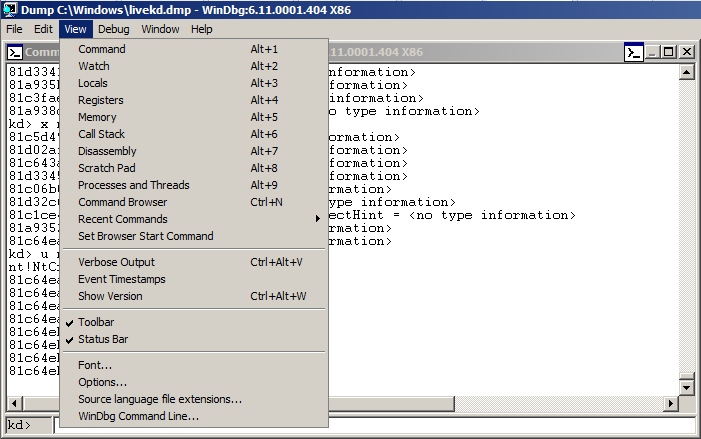
****

****

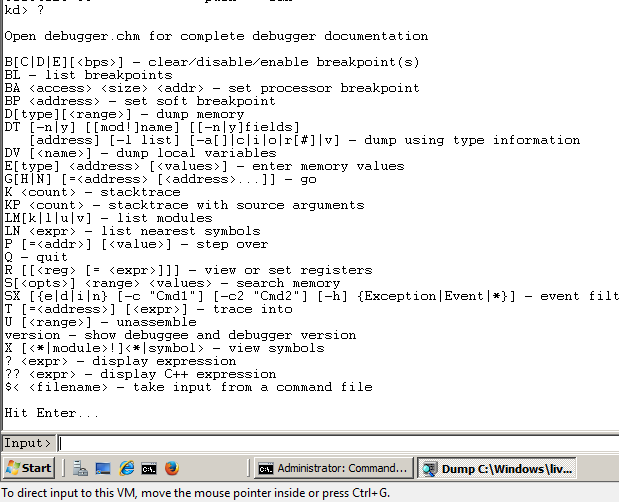
**Unassembling a Function**

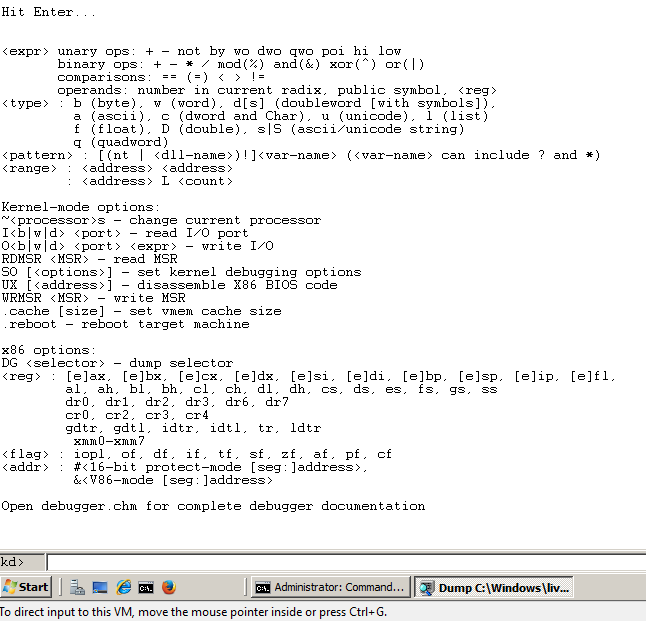
****

**View, Disassembly**

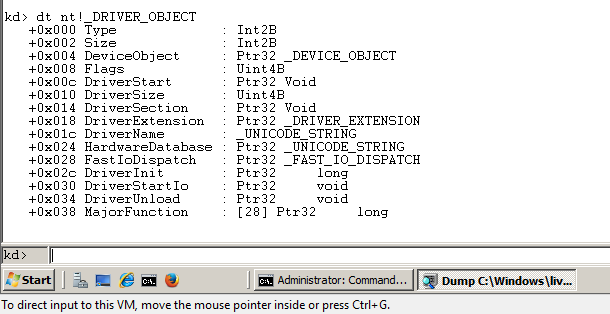
****

**Online Help**

****

****

**Viewing Type Information for a Structure**

****