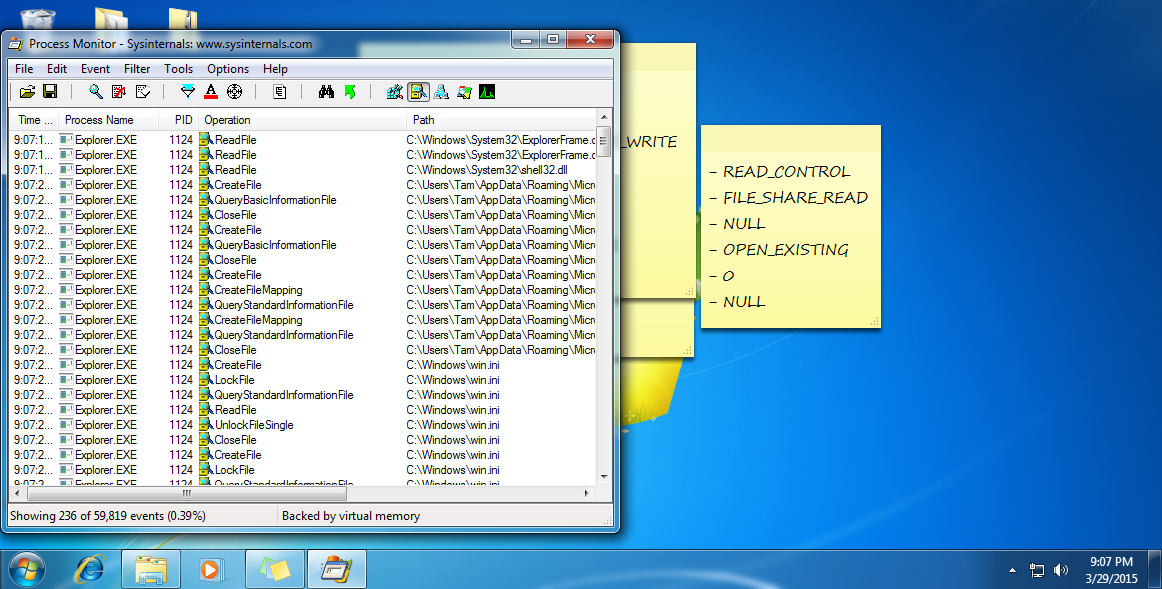
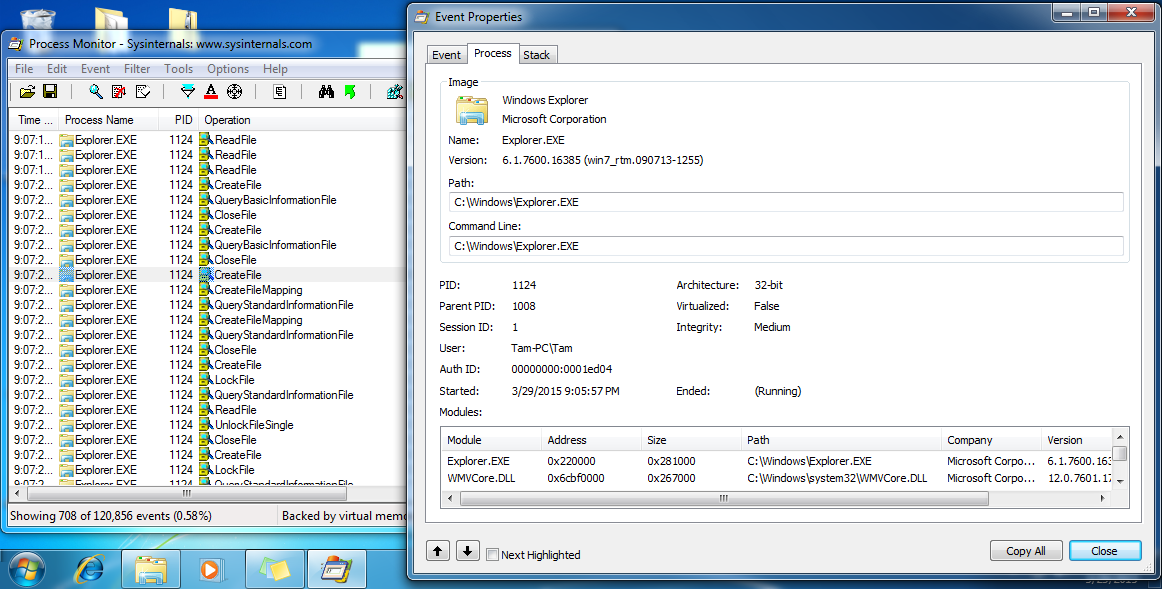
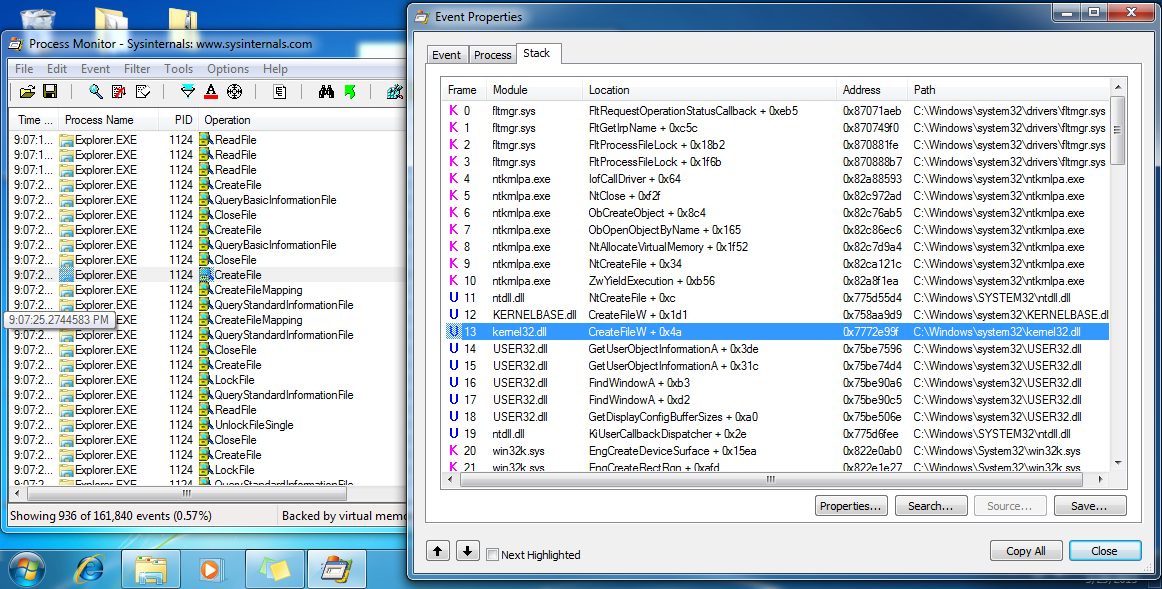
Các tool hiện đang được sử dụng trong luận văn:

1. Process Monitor

* Reference: <https://technet.microsoft.com/en-us/sysinternals/bb896645.aspx>
* Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.
* Sử dụng PM để track các sự kiện mở file, copy & paste file và xem rằng các api nào được gọi.

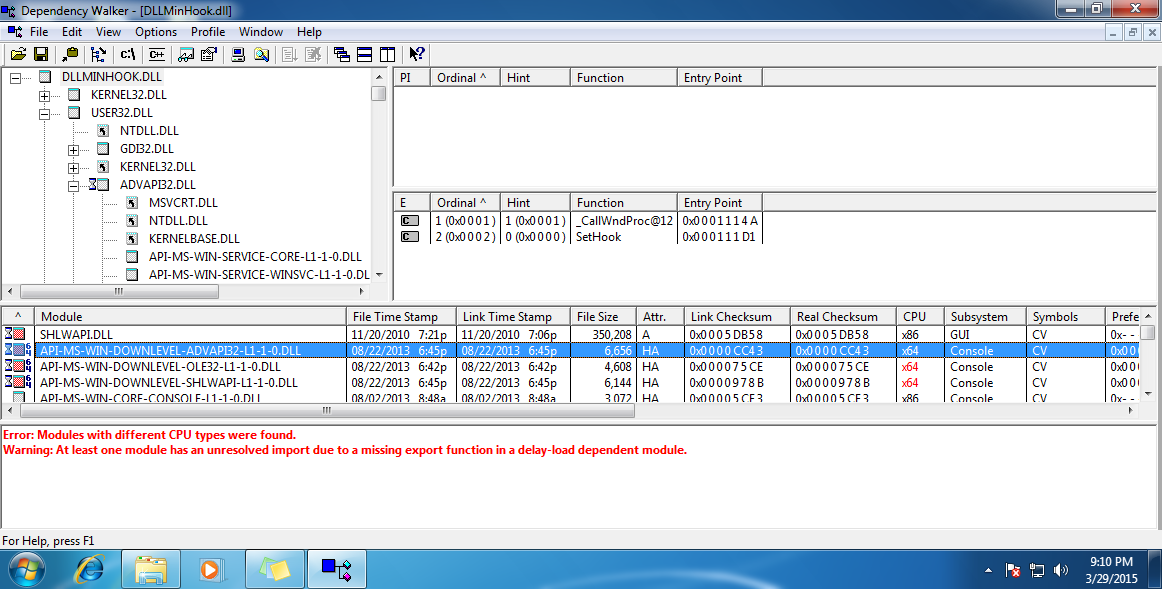






1. Dependency Walker

* Reference: <http://dependencywalker.com/>
* Dependency Walker is a free utility that scans any 32-bit or 64-bit Windows module (exe, dll, ocx, sys, etc.) and builds a hierarchical tree diagram of all dependent modules. For each module found, it lists all the functions that are exported by that module, and which of those functions are actually being called by other modules. Another view displays the minimum set of required files, along with detailed information about each file including a full path to the file, base address, version numbers, machine type, debug information, and more.
* Sử dụng DW để kiểm tra xem các dll cần thiết để chạy một chương trình hay một dll, các dll cần load lên là x32 hay x64, có tương thích hay không ...



1. API Monitor

* Reference: <http://www.rohitab.com/apimonitor>
* API Monitor is a free software that lets you monitor and control API calls made by applications and services. Its a powerful tool for seeing how applications and services work or for tracking down problems that you have in your own applications.
* Sử APIMonitor để đọc các tham số của các API cần được hook để quan sát và theo dõi.

