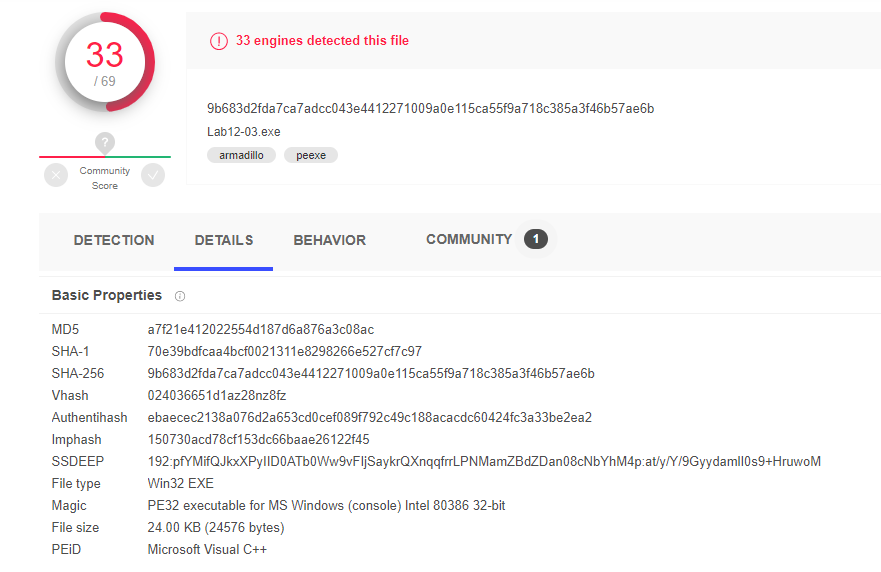
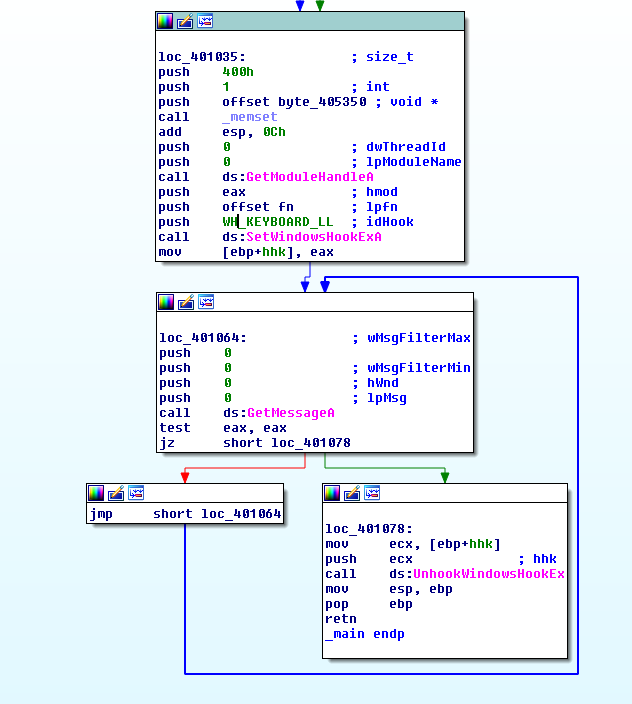
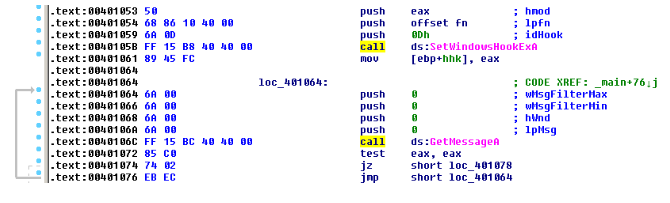
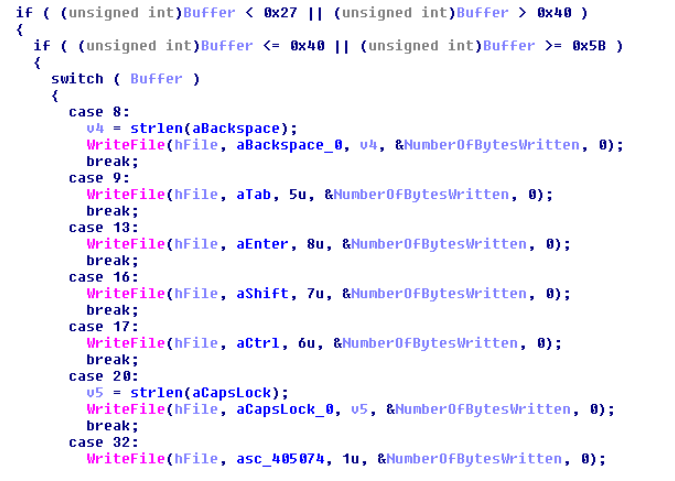
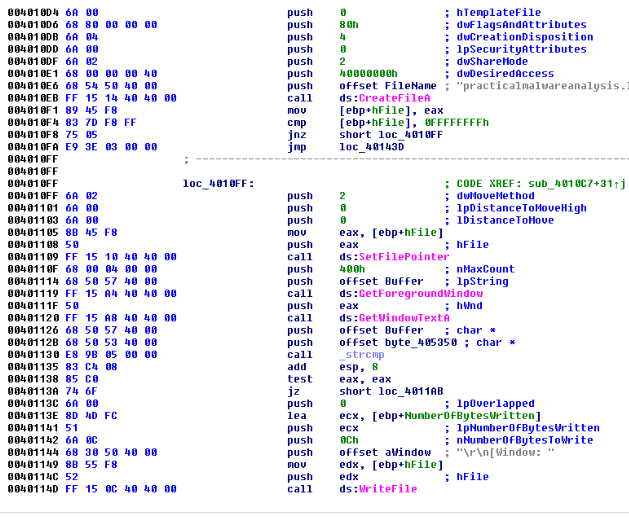
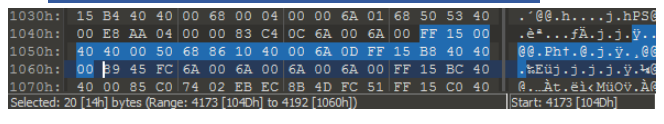
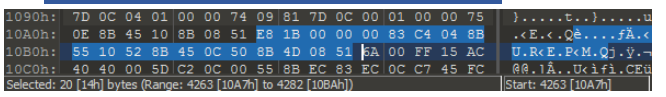
Họ và tên : Nguyễn Thị Kim Huế

Mã số sinh viên: AT13CLC0110

**Đề 4: Phân tích mẫu Lab 12-03.exe**

**-** Phân tích bằng VirusTotal cho kết quả như sau :



* Việc sử dụng **SetWindowsHookExA** với **WH\_KEYBOARD\_LL** làm id cho thấy đây là một keylogger.
* 
* Ban đầu, **Lab12-03.exe** cài đặt một **Hook** bằng **hàm SetWindowsHookEx,** sau đó lặp vô tận thao tác gọi hàm **GetMessage.**
* 
* Đối với mỗi Message, mã độc thực hiện nhảy trong một bảng switch case với **vkCode** tương ứng và ghi vào file **practicalmalwareanalysis.log** trong cùng thư mục với file **Lab12-03.exe.**
* 
* Nội dung keylog được phân loại với đề mục là tên cửa sổ mà người dùng đang thao tác.
* 
* Lab12-03.exe có thể phát hiện bằng **signature:**
* 20 byte từ file offset 4173, là đoạn gọi hàm **SetWindowHookEx** từ hàm **main**
* 
* 20 byte từ file offset 4263, là đoạn xử lý và ghi log đối với mỗi message
* 
* **Cách gỡ bỏ :**
* Kill handle và xóa file thực thi Lab12-03.exe
* Quét trong thư mục của file thực thi và cố gắng xóa file practicalmalwareanalysis.log
* 