**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

\*\*\*



**BÁO CÁO BÀI TẬP LỚN**

**MÔN: HỆ ĐIỀU HÀNH**

Đề tài: Phần mềm Keylogger

Họ tên sinh viên: Đoàn Xuân Tùng

Mã lớp: 103113

MSSV: 20164505

Lớp: CNTT 1.02

Email: [tung.dx164505@sis.hust.edu.vn](mailto:tung.dx164505@sis.hust.edu.vn)

*Hà Nội 2018*

Mục Lục

[NỘI DUNG 3](#_Toc511675519)

[**I.** **Giới thiệu đề tài:** 3](#_Toc511675520)

[**II.** **Phân tích:** 3](#_Toc511675521)

[1. Chạy ngầm trên nền tảng Windows: 3](#_Toc511675522)

[2. HotKey ẩn hiện chương trình: 3](#_Toc511675523)

[3. Khởi động cùng hệ thống: 3](#_Toc511675524)

[4. Theo dõi bàn phím: 3](#_Toc511675525)

[5. Chụp ảnh màn hình: 4](#_Toc511675526)

[6. Gửi mail: 4](#_Toc511675527)

[**III.** **Tham khảo:** 4](#_Toc511675528)

[**IV.** **Thiết kế:** 5](#_Toc511675537)

[1. Sử dụng kĩ thuật Hook của Windows API. 5](#_Toc511675538)

[2. Để sử dụng các hàm API Hook, ta phải khai báo các thư viện .dll: 6](#_Toc511675539)

[3. Để ẩn/hiện màn hình console thì ta cần sử dụng API: 7](#_Toc511675540)

[4. Danh sách hàm chính và tác dụng: 7](#_Toc511675541)

[5. Mô phỏng cách chương trình hoạt động: 9](#_Toc511675542)

[**V.** **Công việc cần thực hiện:** 10](#_Toc511675543)

[**VI.** **Phương pháp:** 10](#_Toc511675544)

[**VII.** **Thành quả:** 10](#_Toc511675545)

[ Các hình ảnh khi chương trình được hoàn thành: 11](#_Toc511675546)

[**VIII.** **Hướng phát triển chương trình** 16](#_Toc511675547)

[KẾT LUẬN 17](#_Toc511675552)

# **NỘI DUNG**

## **Giới thiệu đề tài:**

Với nhu cầu theo dõi hoạt động của bản thân hoặc người khác để quản lý và thống kê từ đó đặt ra vấn đề về phát triển phần mềm theo dõi máy tính.

Đối tượng sử dụng phần mềm có thể là dùng cho cá nhân tự ghi lại hành động của mình, bố mẹ theo dõi con cái, …

## **Phân tích:**

Chương trình lấy tên Keylogger hoạt động trên nền tảng Windows và sử dụng các API của Windows cung cấp. Sau khi khởi chạy, chương trình sẽ cung cấp các chức năng sau:

1. Chạy ngầm trên nền tảng Windows:

Chương trình là hiện lên là 1 cửa sổ console nhưng sau đó sẽ tự động ẩn cửa sổ đó đi. Chương trình vẫn tồn tại trong Task Manager chứ không được ẩn đi hoàn toàn.

1. HotKey ẩn hiện chương trình:

Khi chương trình được ẩn trên màn hình, có thể sử dụng tổ hợp phím LCtrl + Home để ẩn/hiện màn hình console của chương trình. Sử dụng để theo dõi tiến độ, mức độ hoàn thành công việc của chương trình, ngoài ra khi hiện chương trình thì chúng ta có thể tắt chương trình bằng việc tắt cửa sổ console.

1. Khởi động cùng hệ thống:

Khi chương trình được khởi chạy lần đầu tiên thì nó sẽ tự động thêm value tại regedit qua đó làm cho chương trình có thể chạy cùng hệ thống mỗi lần máy tính khởi động.

1. Theo dõi bàn phím:

Chương trình sẽ theo dõi các phím mà người dùng ấn trong quá trình sử dụng máy tính và ghi lại các phím đó ra 1 file text được tạo khi có phím được ghi lại.

1. Chụp ảnh màn hình:

Chương trình sẽ tự động chụp ảnh màn hình theo 1 chu kì thời gian nhất định cho người thiết kế đặt ra, các ảnh sẽ được lưu vào 1 folder và sau đó được đính kèm vào mail để gửi đi.

1. Gửi mail:

Chương trình sẽ tự động gửi mail theo 1 chu kì thời gian nhất định cho người thiết kế chương trình đặt ra, nội dung mail bao gồm nội dung file text ghi lại các phím người dùng và toàn bộ ảnh có mặt trong folder lưu ảnh đã chụp màn hình.

Sau khi gửi mail thì chương trình sẽ xóa file text chứa nội dung các phím mà người dùng đã ấn và toàn bộ ảnh trong folder ảnh đã lưu.

## **Tham khảo:**

* Lập trình C với Windows

<http://voer.edu.vn/c/lap-trinh-c-tren-windows/d02b9bcd>

* Win32 - kĩ thuật Hook

<https://yinyangit.wordpress.com/2011/08/07/win32-introduction-to-hook-and-some-basic-concepts/>

* Lập trình Win32 API – vncoding

<http://vncoding.net/lap-trinh-win32-api/>

* Keylogger Application C#

<http://www.howkteam.vn/course/lap-trinh-keylogger-voi-c-application-25>

* MSDN Microsoft

<https://msdn.microsoft.com/vi-vn/>

* Lập trình C# - vietjack

<http://vietjack.com/csharp/hoc_c_sharp_co_ban_nang_cao.jsp>

* Lập trình C# - howkteam

<http://www.howkteam.vn/course/khoa-hoc-lap-trinh-c-can-ban-1>

<http://www.howkteam.vn/course/khoa-hoc-lap-trinh-c-nang-cao-39>

<http://www.howkteam.vn/course/lap-trinh-oop-voi-c-32>

* Google

<https://www.google.com.vn/>

## **Thiết kế:**

### Sử dụng kĩ thuật Hook của Windows API.

#### Hook là gì?

Hook là một cơ chế mà một ứng dụng có thể chặn các sự kiện, như các thông điệp, thao tác chuột, bàn phím. Hàm dùng để chặn một loại sự kiện riêng biệt được gọi là hook procedure/ Hook function. Mỗi khi nhận được sự kiện, hook procedure có thể thay đổi và thậm chí hủy bỏ các sự kiện đó.

#### Cơ chế của Hook?

Như đã nói ở trên, có nhiều loại hook (như chuột, bàn phím) và hệ điều hành luôn duy trì một danh sách các hook procedure cho mỗi loại đó. Mỗi danh sách các Hook procedure này được gọi là **hook chain**. Bản chất của hook chain là một dãy các con trỏ hàm trỏ đến các Hook procedure.

Khi hệ thống thực một sự kiện nào đó, nó sẽ tìm kiếm trong hook chain tương ứng với sự kiện đó. Nếu một hook procedure phù hợp được tìm thấy, hệ thống sẽ thực hiện nó và chỉ lấy lại quyền điều khiển sau khi hook chain kết thúc. Vì thế khi một hook procedure thực hiện xong, nó phải thực hiện việc chuyển quyền điều khiển cho hook procedure kế tiếp trong hook chain.

Tuy nhiên cơ chế này còn tùy thuộc vào loại hook. Như một số loại hook chỉ có thể theo dõi các thông điệp, vì vậy cho dù hook procedure có chuyển quyền điều khiển cho hook procedure kế tiếp hay không, hệ thống vẫn sẽ tự động làm việc này.

#### Hook Procedure

Hook procedure là một loại [callback function](http://en.wikipedia.org/wiki/Callback_%28computer_programming%29) (hàm hồi quy). Hệ thống sẽ gọi các hàm này khi các sự kiện, thông điệp tương ứng với loại hook. Mỗi loại hook có một hook procedure khác nhau nhưng đều có cùng tham số như cú pháp bên dưới. Với mỗi hook procedure khác nhau thì việc xét các giá trị tham số cũng khác nhau.

Danh sách hook procedure tương ứng với từng loại hook được liệt kê trong phần giới thiệu về hàm SetWindowsHookEx.

Cú pháp: LRESULT CALLBACK HookProc(int nCode, WPARAM wParam, LPARAM lParam)

#### Các hàm Win32 API cần thiết

Để sử dụng hook, ta cần sử dụng ba hàm API của Windows là:

* SetWindowsHookEx: cài đặt một hook procedure vào một hook chain.
* CallNextHookEx: chuyển quyền điều khiển cùng các thông tin hook cho hook procedure kế tiếp trong hook chain. Bạn có thể không sử dụng hàm này tuy nhiên chỉ khi nào bạn muốn chặn các hook procedure còn lại trong hook chain.
* UnhookWindowsHookEx: gỡ hook procedure ra khỏi hook chain được cài đặt bởi SetWindowsHookEx.

### Để sử dụng các hàm API Hook, ta phải khai báo các thư viện .dll:

[DllImport("user32.dll", CharSet = CharSet.Auto, SetLastError = true)]

private static extern IntPtr SetWindowsHookEx(int idHook, LowLevelKeyboardProc lpfn, IntPtr hMod, uint dwThreadId);

[DllImport("user32.dll", CharSet = CharSet.Auto, SetLastError = true)]

[return: MarshalAs(UnmanagedType.Bool)]

private static extern bool UnhookWindowsHookEx(IntPtr hhk);

[DllImport("user32.dll", CharSet = CharSet.Auto, SetLastError = true)]

private static extern IntPtr CallNextHookEx(IntPtr hhk, int nCode,

IntPtr wParam, IntPtr lParam);

[DllImport("kernel32.dll", CharSet = CharSet.Auto, SetLastError = true)]

private static extern IntPtr GetModuleHandle(string lpModuleName);

### Để ẩn/hiện màn hình console thì ta cần sử dụng API:

[DllImport("kernel32.dll")]

static extern IntPtr GetConsoleWindow();

[DllImport("user32.dll")]

static extern bool ShowWindow(IntPtr hWnd, int nCmdShow);

### Danh sách hàm chính và tác dụng:

* WriteLog(vkCode): Viết kí tự vừa hook được vào file text, nếu file chưa tồn tại thì tạo file mới.
* CheckHotKey(vkCode): Check xem có phải là tổ hợp phím ẩn/hiện màn hình console.
* HideWindow(): Ẩn màn hình console
* DisplayWindow(): Hiện màn hình console
* CaptureScreen(): Chụp ảnh màn hình, lưu ảnh vào folder được định sẵn.
* StartWithOS(): Đăng kí key mới để khởi động cùng hệ thống
* SendMail(): Gửi mail với nội dung của file text và các ảnh màn hình đã chụp được.
* StartTimmer(): Tạo thread mới chạy song song với Hook và đếm thời gian, nếu sau khoảng thời gian đặt trước thì chụp ảnh màn hình và gửi mail.
* Ngoài ra còn có các hàm liên quan đến việc kĩ thuật Hook và kĩ thuật ẩn/hiện màn hình console
* Các hàm của các lớp có sẵn trong Windows, với các lớp, thư viện:

using Microsoft.Win32;

using System;

using System.Collections.Generic;

using System.Diagnostics;

using System.Drawing;

using System.Drawing.Imaging;

using System.IO;

using System.Linq;

using System.Net.Mail;

using System.Runtime.InteropServices;

using System.Text;

using System.Threading;

using System.Threading.Tasks;

using System.Windows.Forms;

### Mô phỏng cách chương trình hoạt động:

SendMail()  
Gửi mail theo địa chỉ mail đã cài đặt, nội dung lấy từ file New Text Document và folder New Folder

Sau khi gửi mail xong thì xóa file New Text Document và nội dung New Folder

WriteLog()  
Viết kí tự vkCode vào file New Text Document

CheckHotKey()  
Nếu người dùng bấm phím thỏa mãn thì ẩn/hiện console

New Folder

New Text Document

CaptureScreen()  
Chụp ảnh màn hình và lưu vào folder New Folder

Keylogger

StartTimmer()  
Thiết lập để:

30s chạy CaptureScreen()

300s chạy SendMail()

HOOK  
Sử dụng kĩ thuật Hook và lấy được mã phím vkCode mỗi khi mà người dùng ấn phím trên bàn phím

## **Công việc cần thực hiện:**

* Học lập trình C# cơ bản và nâng cao
* Học lập trình C# hướng đối tượng OOP
* Đọc qua tài liệu lập trình C trên Windows để hiểu về cơ chế của Win32
* Tìm hiểu về kĩ thuật Hook
* Tìm hiểu về Bitmap
* Tìm hiểu về Thread
* Tìm hiểu về cách gửi mail trong C#
* Tìm hiểu về cách thao tác với tệp và thư mục trong C#
* Tìm hiểu về thao tác với màn hình console
* Và cuối cùng là bắt tay vào code và sửa lỗi, kiểm thử chương trình.

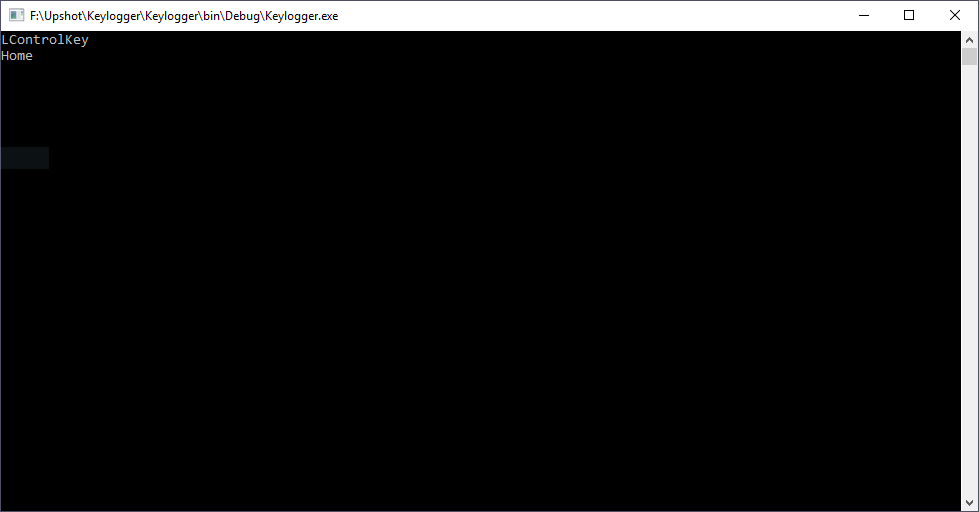
## **Phương pháp:**

Thực hiện xây dựng chương trình dựa trên ngôn ngữ C# và phần mềm Visual Studio 2017

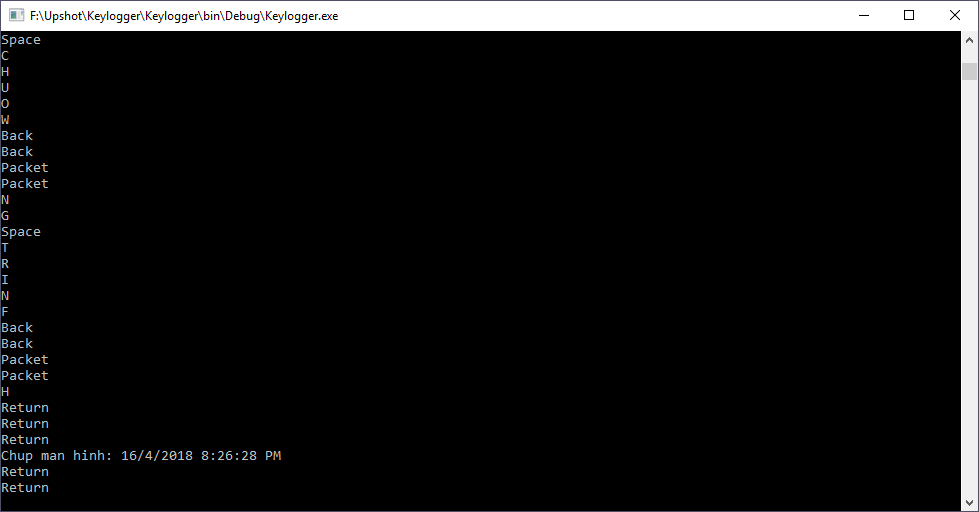
## **Thành quả:**

* Nâng cao khả năng tư duy và sử dụng ngôn ngữ lập trình C#
* Nâng cao hiểu biết và sử dụng thành thạo phần mềm Visual Studio 2017
* Có kinh nghiệm thực hiện các đề tài khác liên quan đến C#, API Window, các phần mềm trên Windows.
* Hoàn thành tốt chương trình, chương trình sử dụng module hóa theo cấu trúc và sử dụng các class hướng đối tượng được Windows hỗ trợ.

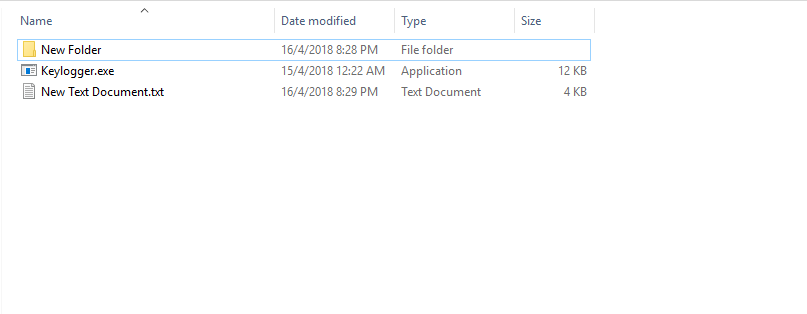
### Các hình ảnh khi chương trình được hoàn thành:



*Chương trình được khởi động và tự động ẩn cửa sổ chương trình, ấn LCtrl + Home để ẩn/hiện chương trình*



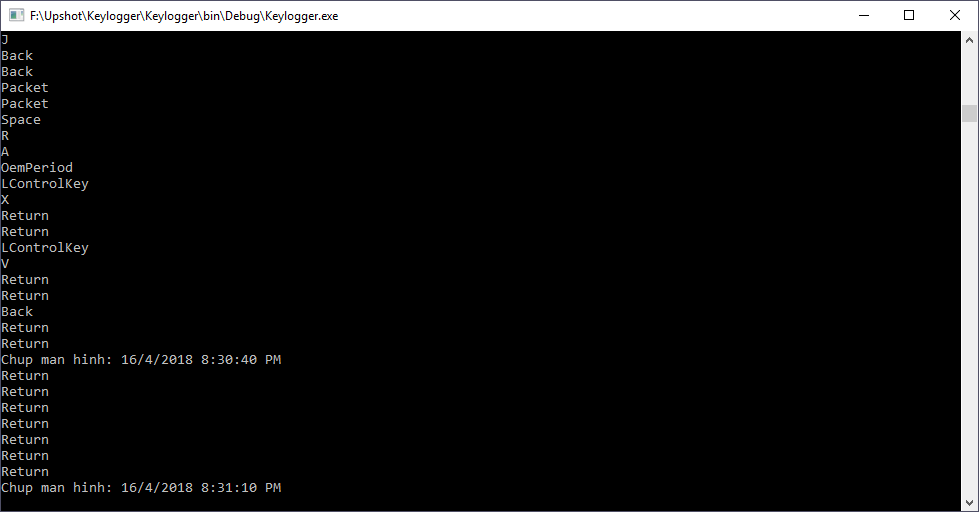
*Chương trình tự động ghi lại các phím mà người dùng đã bấm sau đó ghi vào file log và in ra màn hình console*



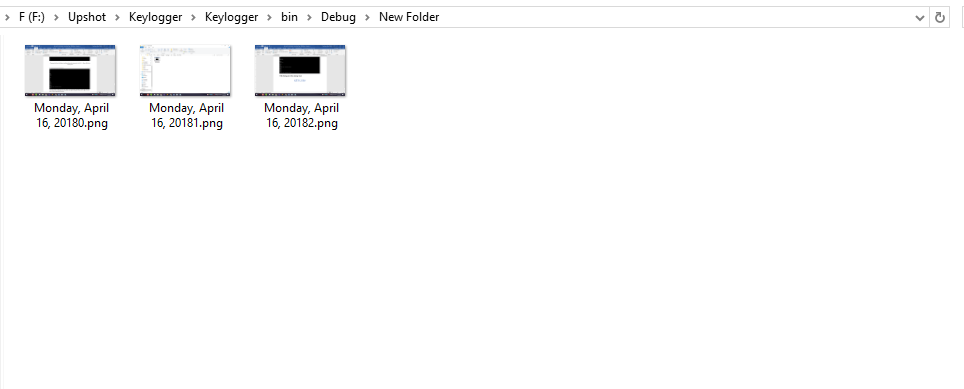
*Hình ảnh thư mục chứa chương trình, có folder New Folder và file New Text Document đã được tạo ra.*



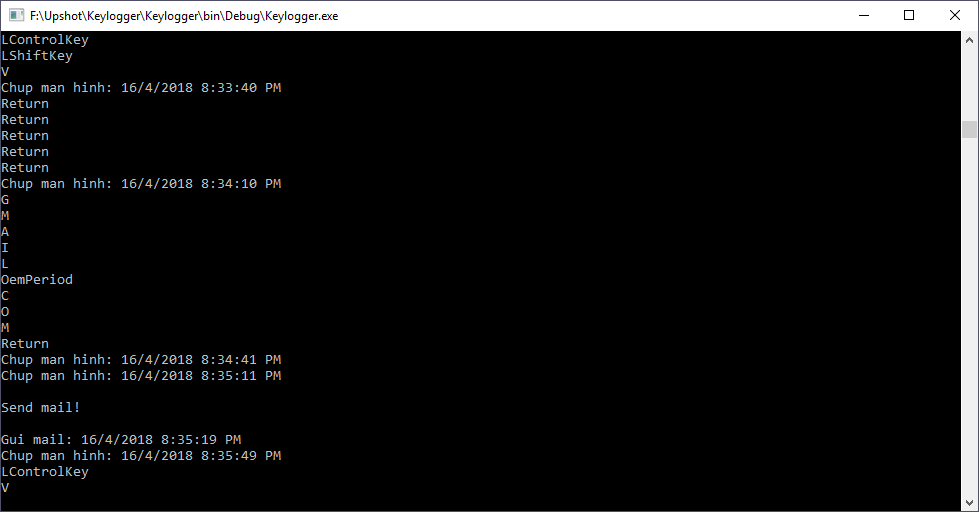
*Hình ảnh file .txt New Text Document được tạo ra và chứa các phím mà người dùng đã bấm trên bàn phím*



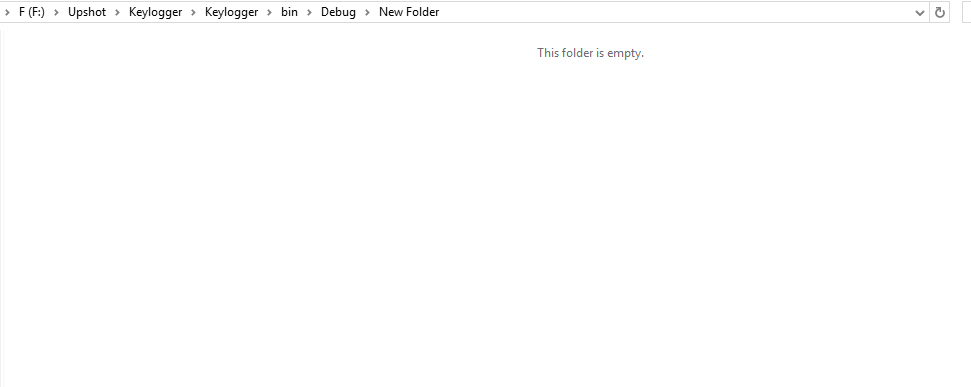
*Hình ảnh thông báo rằng đã chụp màn hình kèm ngày giờ chụp*



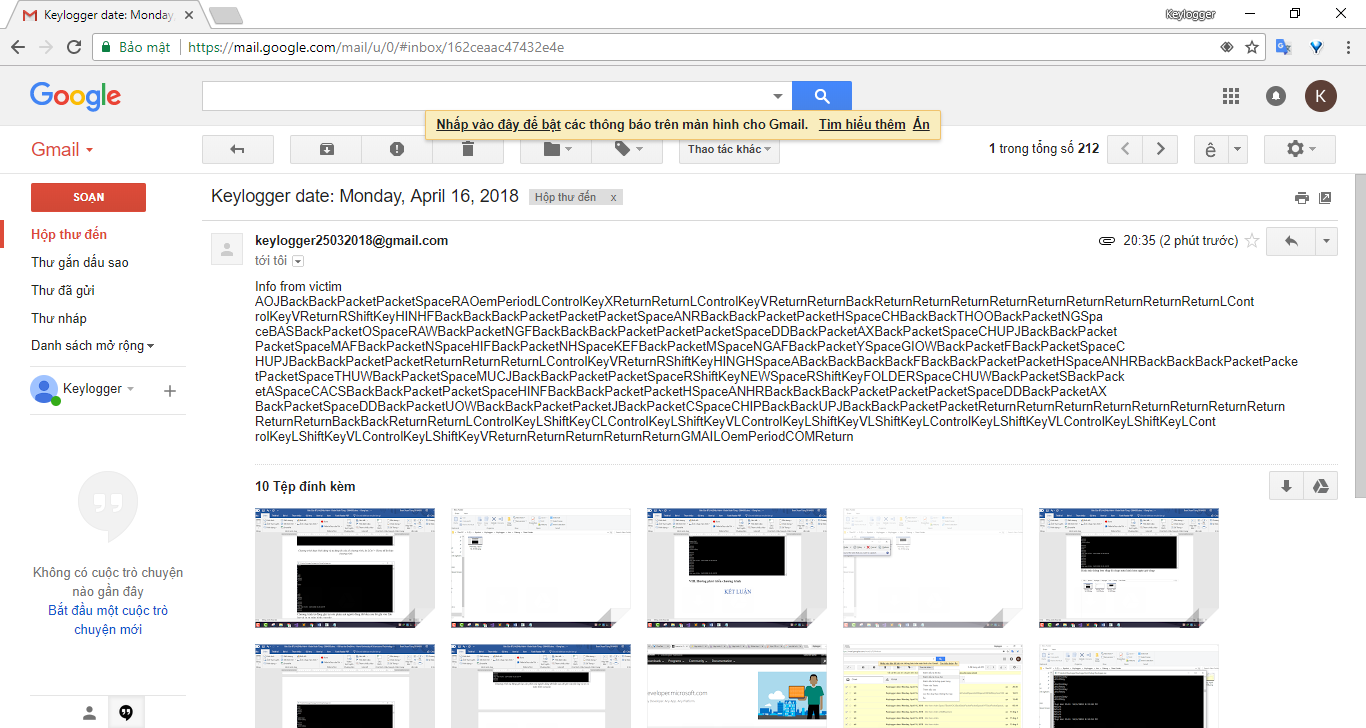
*Hình ảnh thư mục New Folder chứa các hình ảnh đã được chụp*



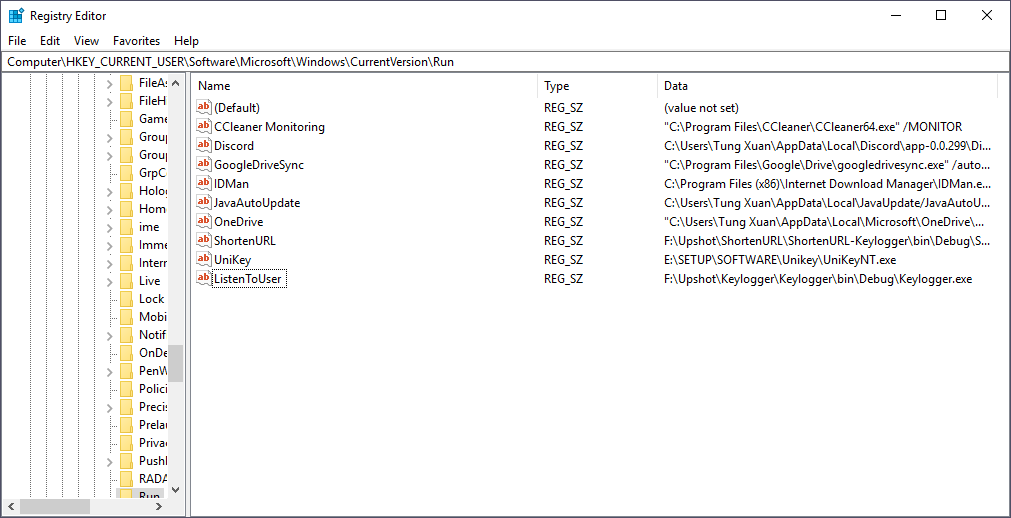
*Hình ảnh thông báo chương trình đã gửi mail thành công.*



*Hình ảnh trong thư mục New Folder đã bị xóa hết khi chương trình gửi mail*



*Hình ảnh mail nhận được với nội dung là file text và các ảnh chụp màn hình*



*Hình ảnh cho thấy đã tạo thành công 1 key trên regedit dưới cái tên ListenToUser để giúp chương trình khởi động cùng Windows*

## **Hướng phát triển chương trình**

### Viết 1 chương trình cho phép người dùng nhập vào mail và password sau đó build ra chương trình Keylogger với mail nhận thông tin và mail mà người dùng đã nhập.

### Mã hóa code để vượt qua được các chương trình antivirus và Windows Defender.

### Cho phép nhập vào khoảng thời gian chụp ảnh màn hình và thời gian gửi mail, tên chương trình xuất hiện trong Task Manager và tên chương trình lưu trong máy sau đó build ra chương trình Keylogger.

### Phát triển 1 phần mềm giải mã, dùng để chuyển hóa nội dung các phím mà victim sử dụng qua đó đoán được nội dung các từ mà victim đã sử dụng.

# KẾT LUẬN

Phần mềm đạt được những mục tiêu nhất định tuy nhiên còn nhiều khuyết điểm cũng như tính năng còn hạn chế.

Tuy nhiên những gì mà em thu được sau bài tập lớn lần này giúp em có thể tự tin hơn để tiếp tục đam mê của mình trong con đường lập trình viên.

Em rất mong có thể nhận được những sự góp ý từ thầy để có thể phát triển bản thân hơn nữa.

Em chân thành cảm ơn thầy!

*Hà Nội, ngày 16 tháng 4 năm 2018*