**Lab 4. keylogger**

Sinh viên : Lâm Quốc Khánh – 18110304

# \* Chuẩn bị

* Trong bài lab này, em build một chương trình Key Logger bằng cách chỉnh sửa lại source code từ HowKtem.vn.
* Link khóa học: [Lập trình Keylogger với C# Application | How Kteam](https://www.howkteam.vn/course/lap-trinh-keylogger-voi-c-application-25) (<https://www.howkteam.vn/course/lap-trinh-keylogger-voi-c-application-25>)
* Có đính kèm source code (đã chỉnh sửa, C# .NET Framework Console App) và file build.

# 1. Tính năng của Key Logger

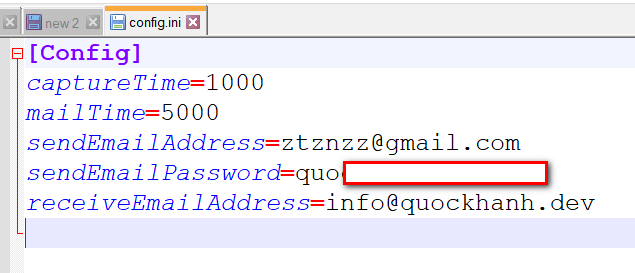
* Tự động chụp ảnh màn hình sau một khoảng thời gian nhất định.
* Ghi lại các phím mà người dùng ấn vào file log.
* Tự độn gửi mail đến một địa chỉ mail chỉ định, nội dung bao gồm ảnh chụp màn hình và các phím mà người dùng đã nhấn.
* Có thể khởi động cùng hệ thống.
* Chạy ngầm, không lấy bàn phím của người dùng (người dùng vẫn dùng bàn phím bình thường và các phím đã nhấn vẫn được lưu vào file log).

# 2. Hạn chế của Key Logger

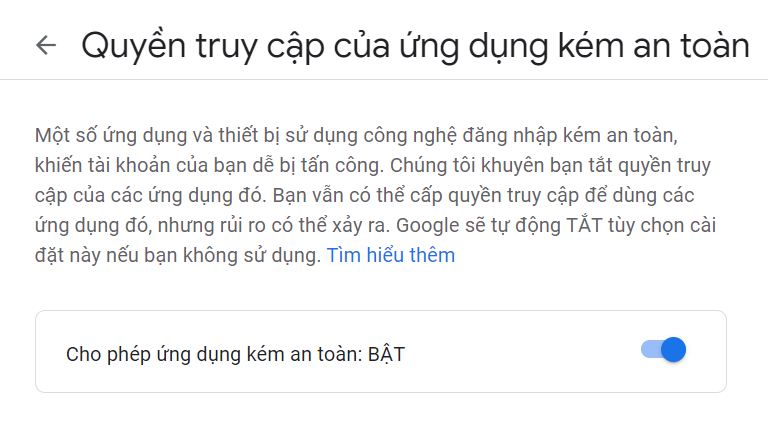
* Vẫn còn hiển thị trong TaskManager (có thể ẩn nhưng tìm hiểu thêm).
* Bị phần mềm diệt virus phát hiện (như McAfee).

# 3. Config Key Logger

Để thuận tiện cho việc thử nghiệm phầm mềm với các giá trị khác tạo, ta tạo ra file có tên **config.ini** đặt cùng với thư mục chứa phần mềm, nội dung như sau:



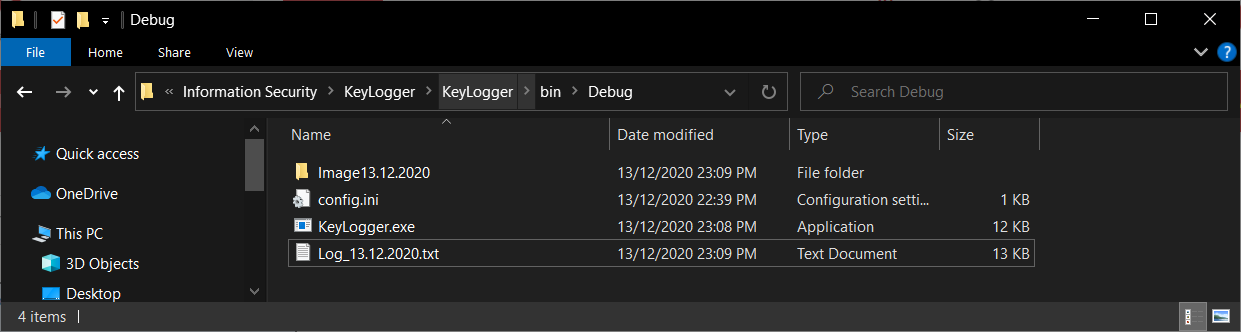
* **captureTime** là khoảng thời gian giữa 2 lần chụp ảnh màn hình, tính bằng mili second. Ví dụ: với giá trị là 1000 thì sau 1s, phần mềm sẽ tự chụp màn hình lại 1 lần
* **mailTime** là khoảng thời gian giữa 2 lần gửi mail, tính bằng mili second. Ví dụ: với giá trị là 5000 thì sau 5s, phần mềm sẽ gửi đi 1 email
* **sendEmailAddress** và **sendEmailPassword** là email và password của tài khoản Gmail dùng để gửi. Chú ý
  + Phần mềm dùng giao thức STMP(host = smtp.gmail.com, port = 587) để gửi mail.
  + Tài khoản Gmail phải bật quyền truy cập kém an toàn tại <https://www.google.com/settings/u/1/security/lesssecureapps> để có thể gửi mail bằng giao thức STMP



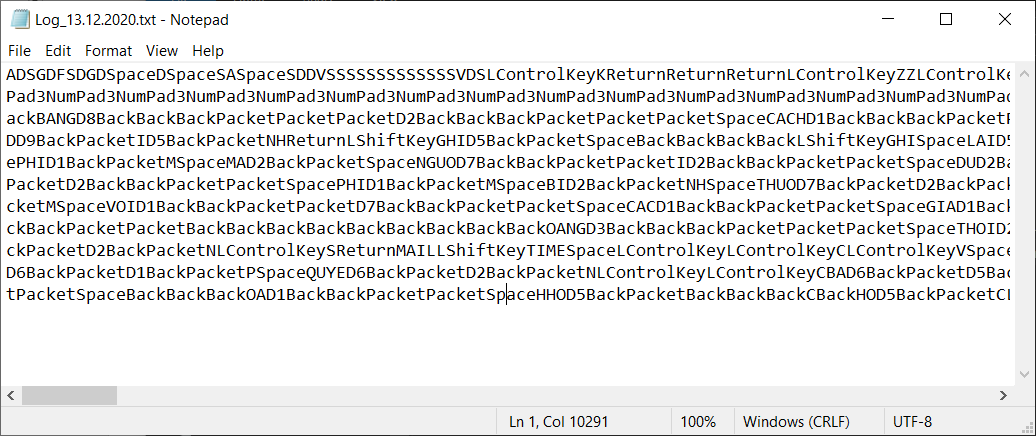
* **receiveEmailAddress** là địa chỉ nhận mail
* Các giá trị này có thể set cứng trong code.

# 4. Demo

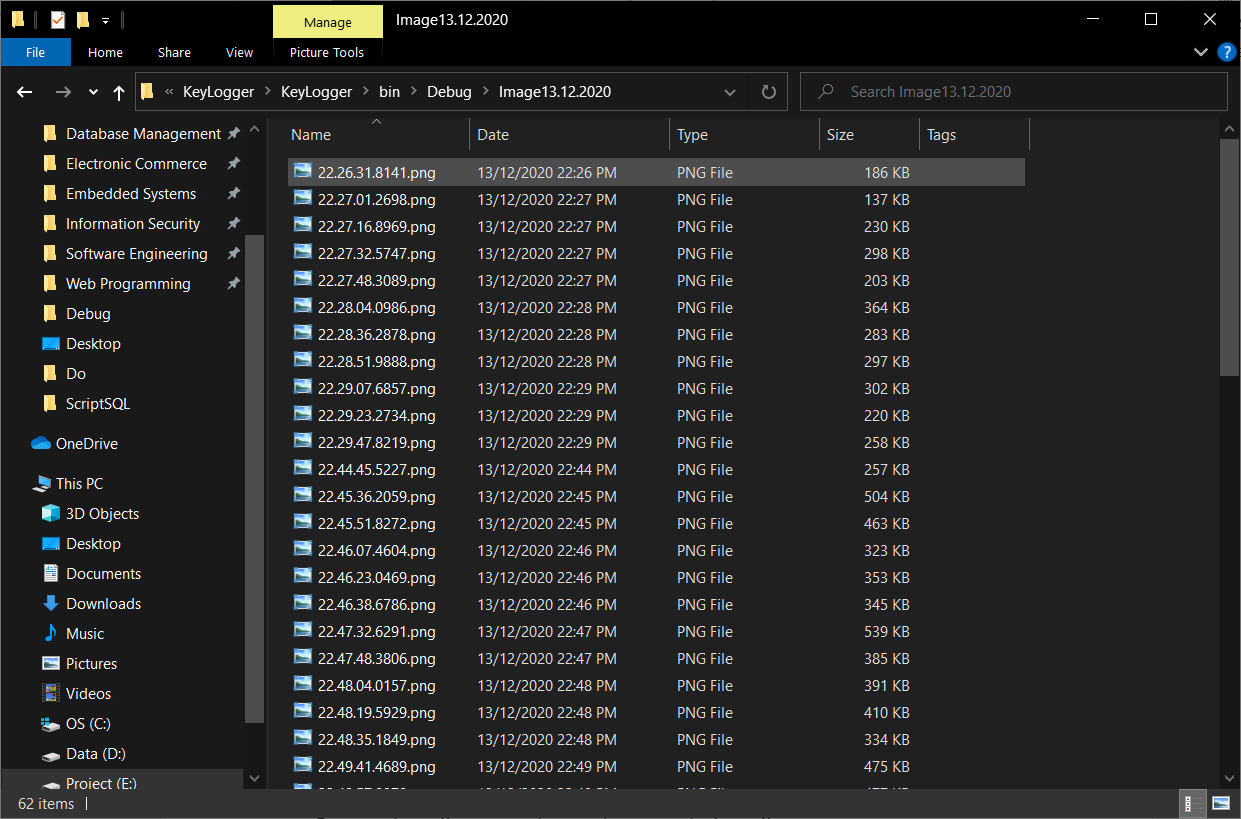
Mỗi khi chạy, phầm mềm sẽ tạo ra 1 file có định dạng là “Log\_dd.MM.yyyy.txt” để ghi lại các phím bấm của người dùng và 1 thư mục có tên là “Imagedd.MM.yyyy” chứa các ảnh chụp màn hình.



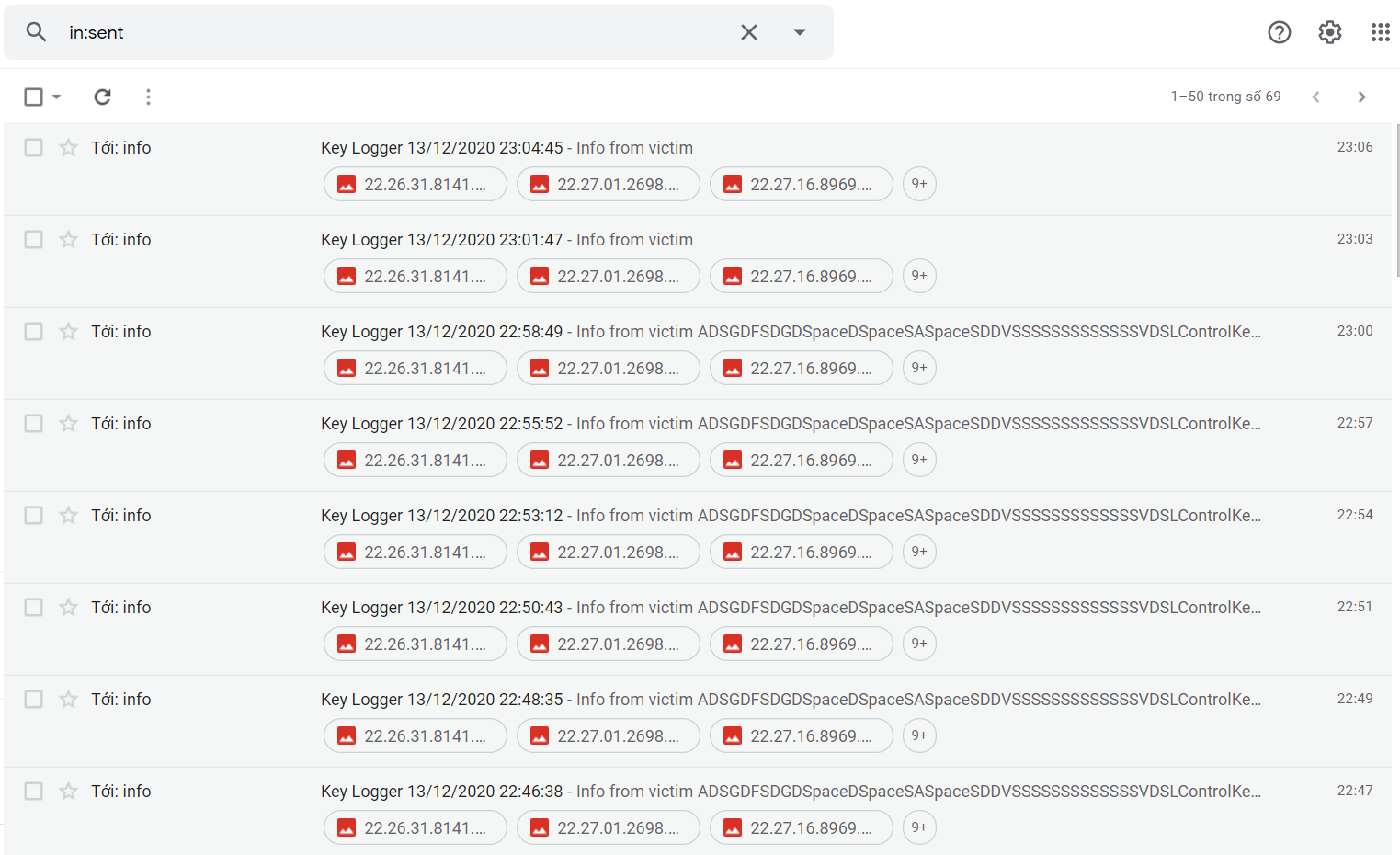
File log do không có thời gian để optimize code, các key được chuyển từ kiểu int sang enum Keys (trong C#) rồi lại convert sang chuỗi nên hiển thị chưa được đẹp. Vấn để này hoàn toàn có thể nâng cấp, chỉnh sửa sau nếu có thời gian.



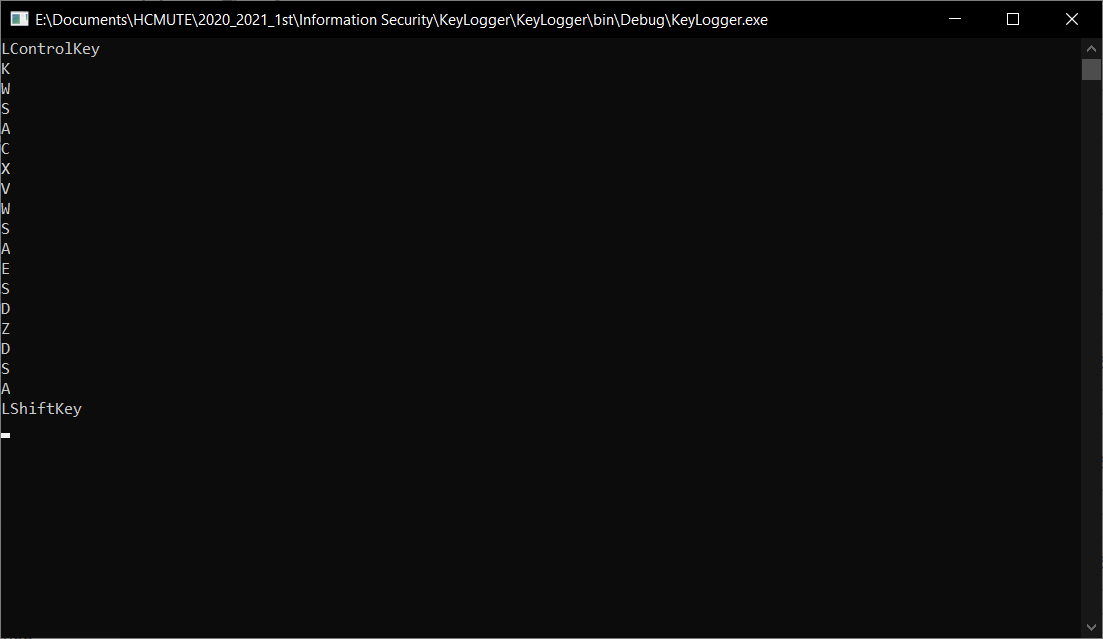
Ảnh chụp màn hình



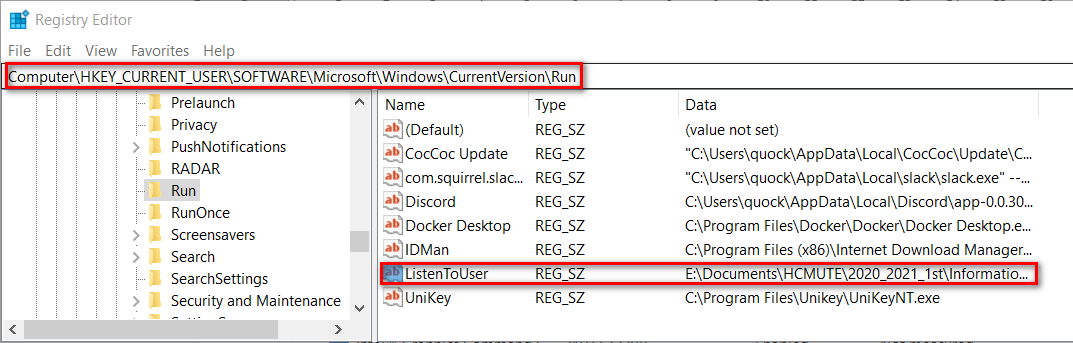
Các email được gửi đi



Khi nhấn phím tắt Ctrl + K thì phần mềm sẽ hiện lên để chúng ta có thể xem và tắt nó



Khi phầm mềm chạy một giá trị được thêm vào trong Registry tại **Computer\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** để phần mềm có thể khởi động cùng hệ thống



Có thể Name và Publisher để đánh lừa người dùng bằng các config khi build source code

