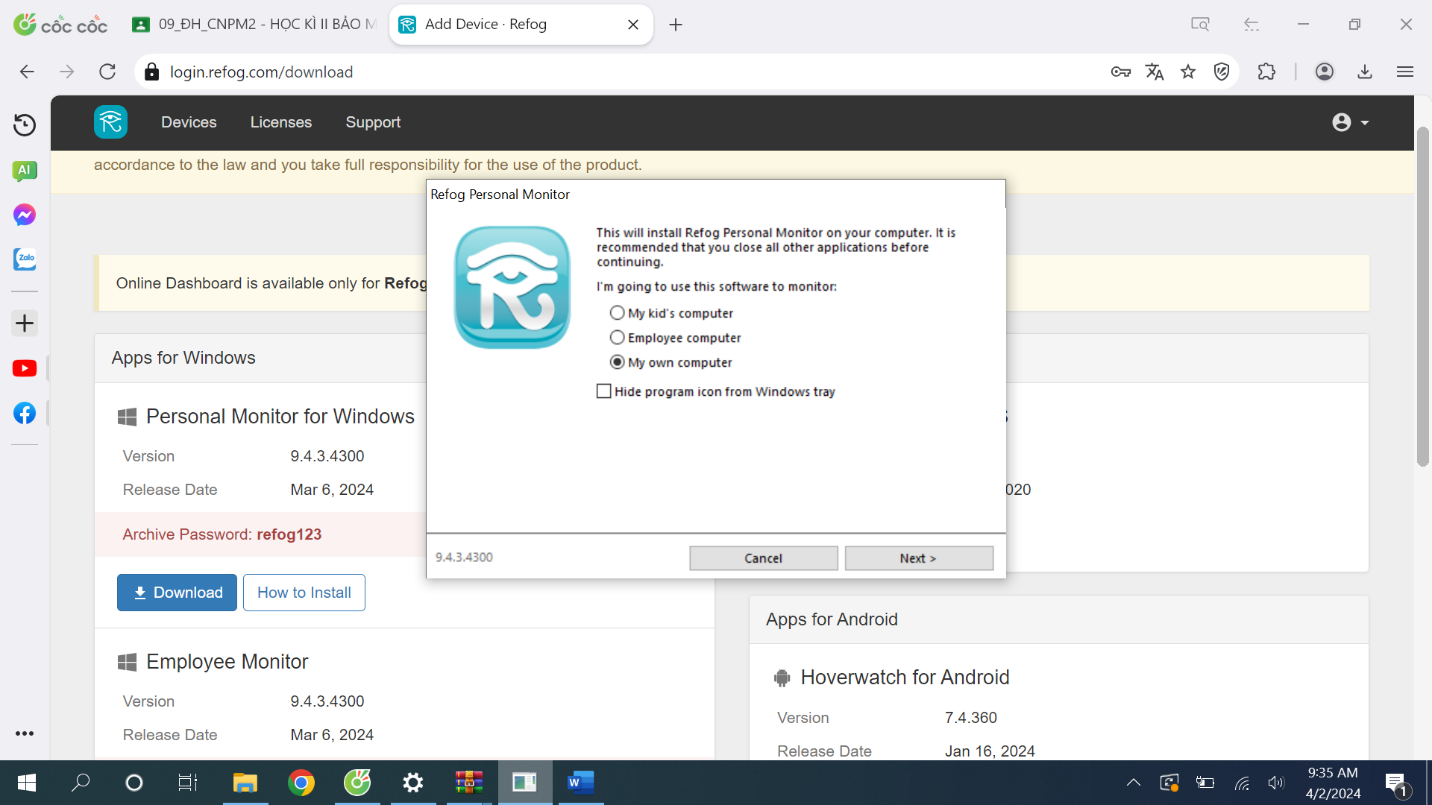
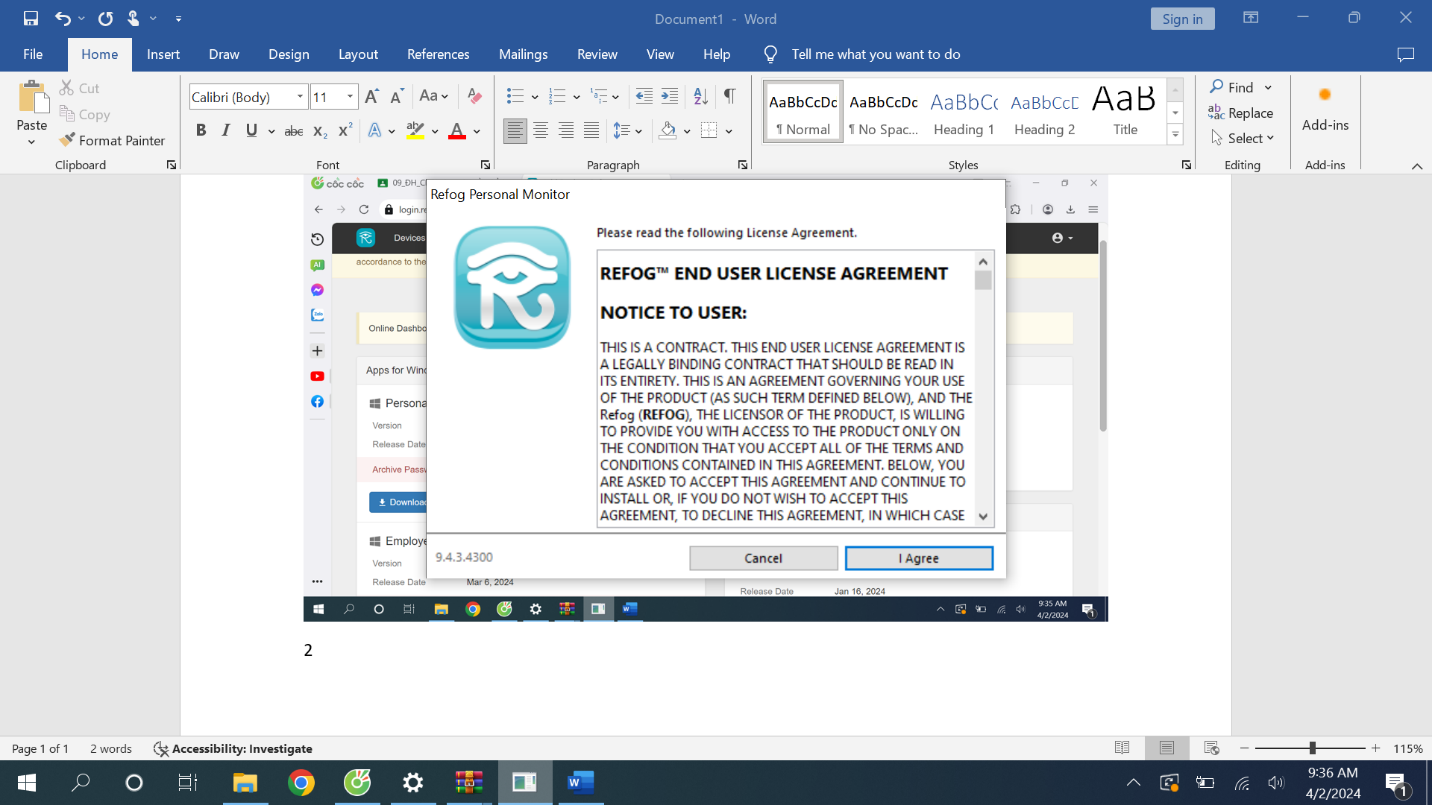
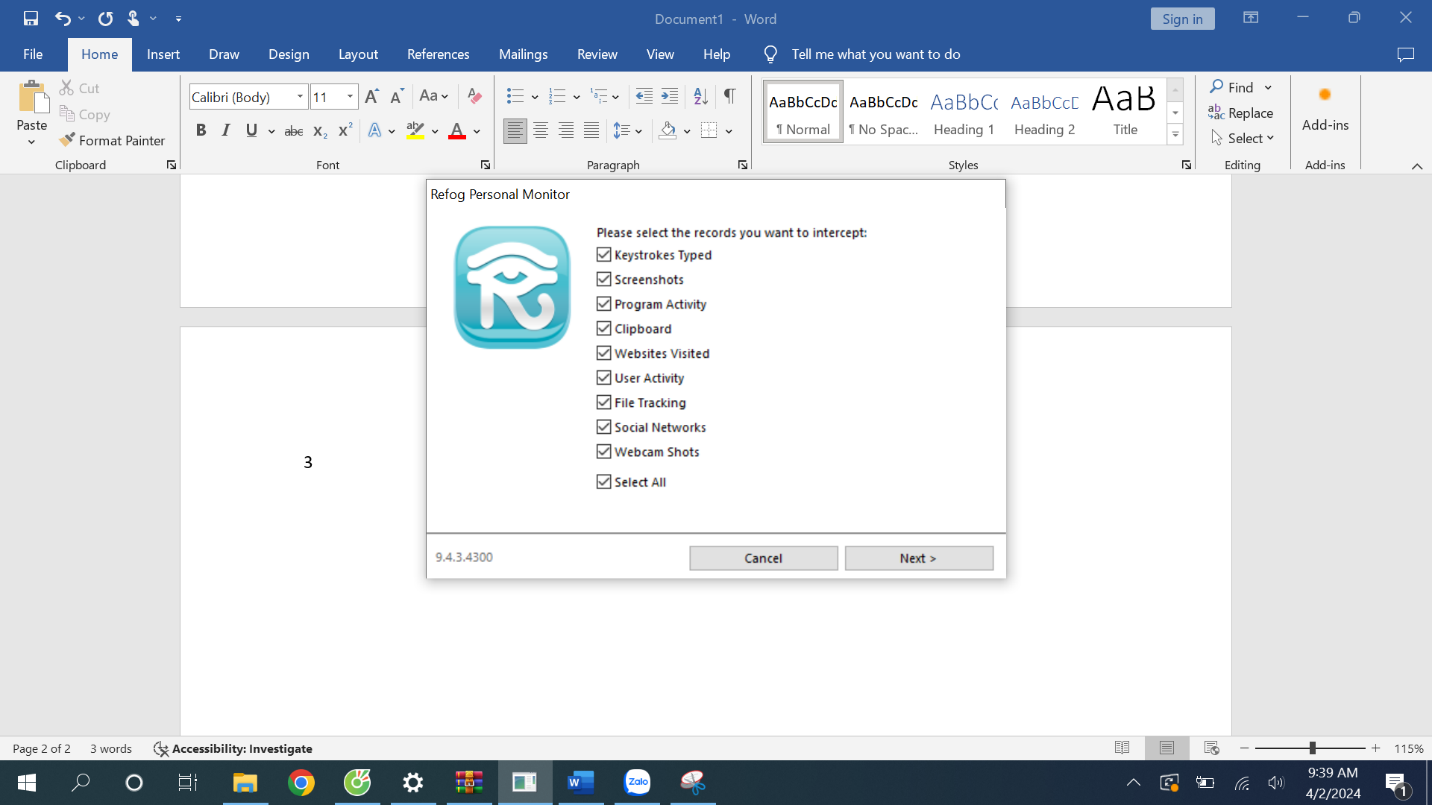
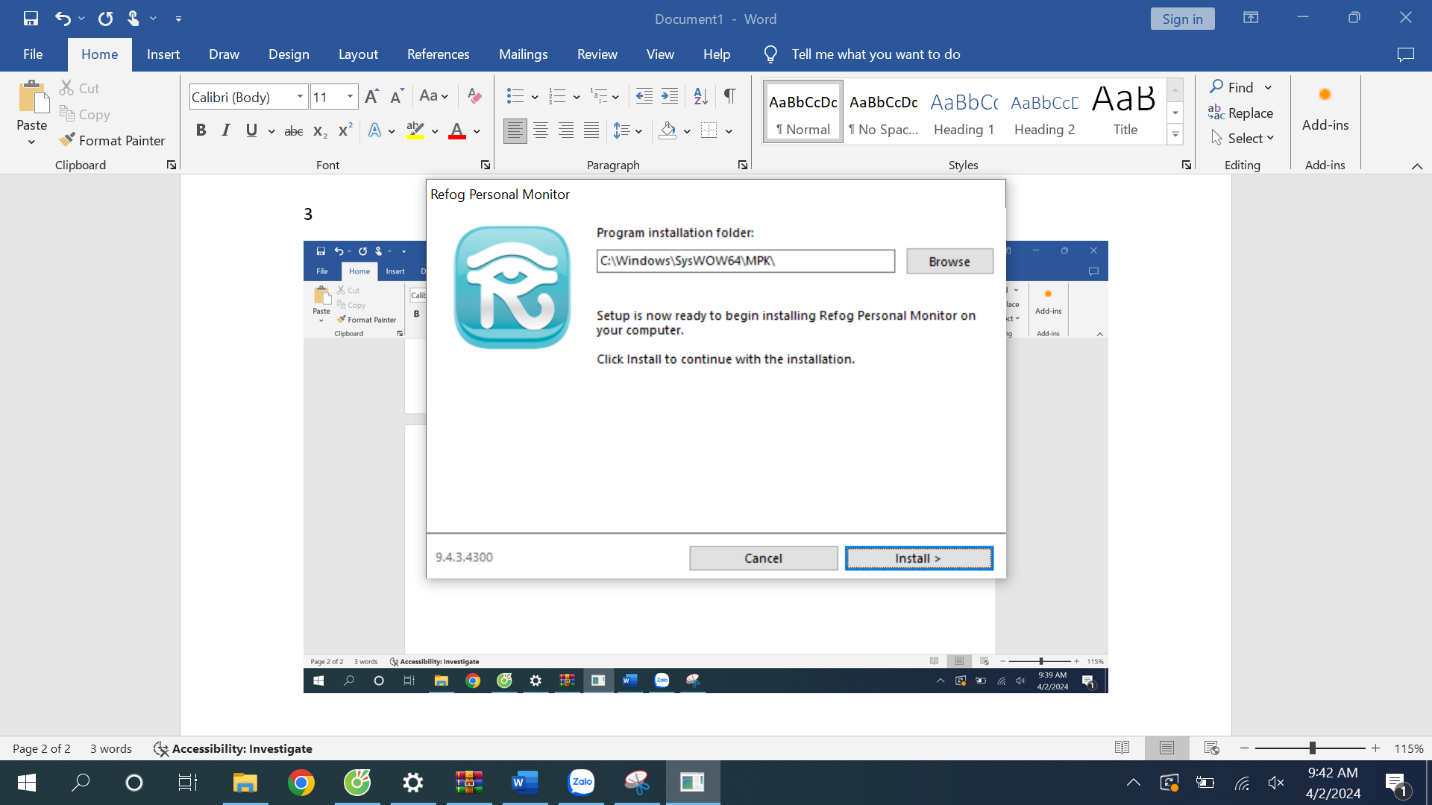
# **LAB 2. Keylogger trên PC và điện thoại**

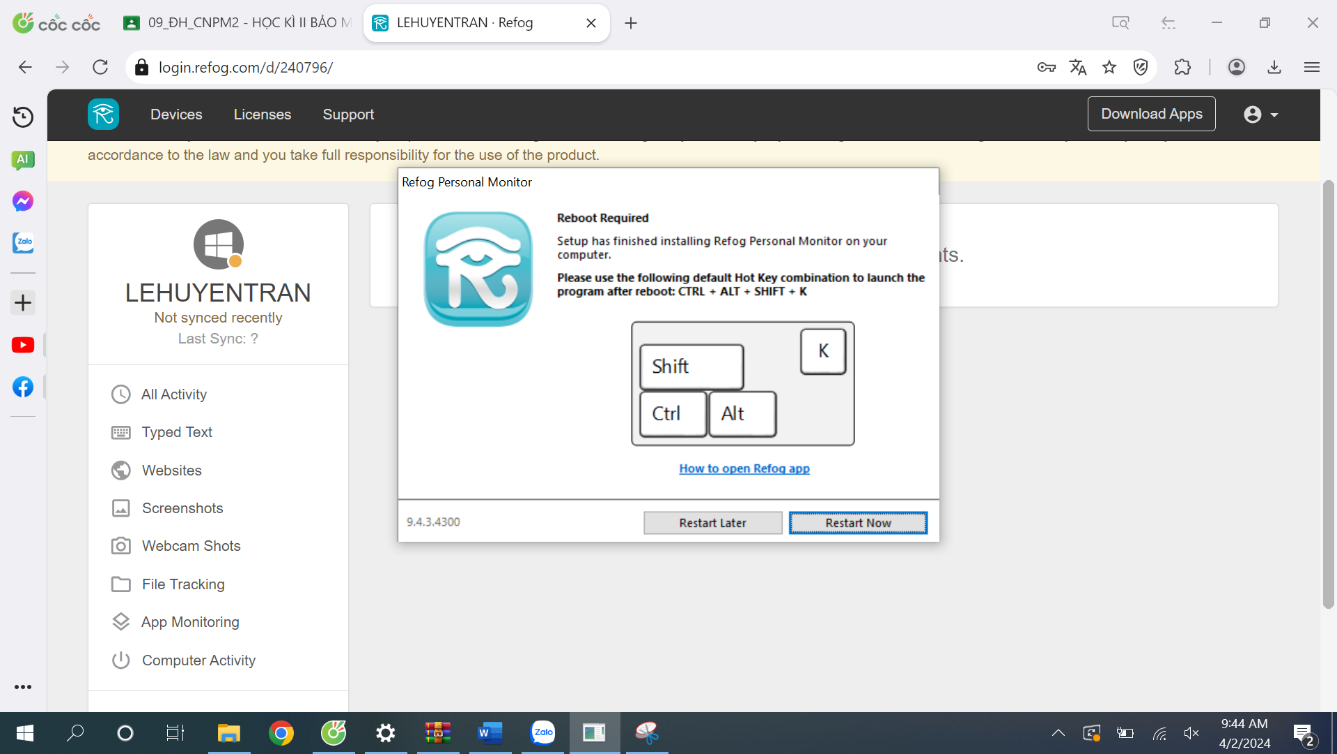
## **1. Thử nghiệm Keylogger đơn giản với REFOG Free Keylogger**

• Bước 1: Tải và cài đặt RFK trên Windows.









• Bước 2: Dùng trình duyệt web, đăng nhập thành công vào một tài khoản Gmail

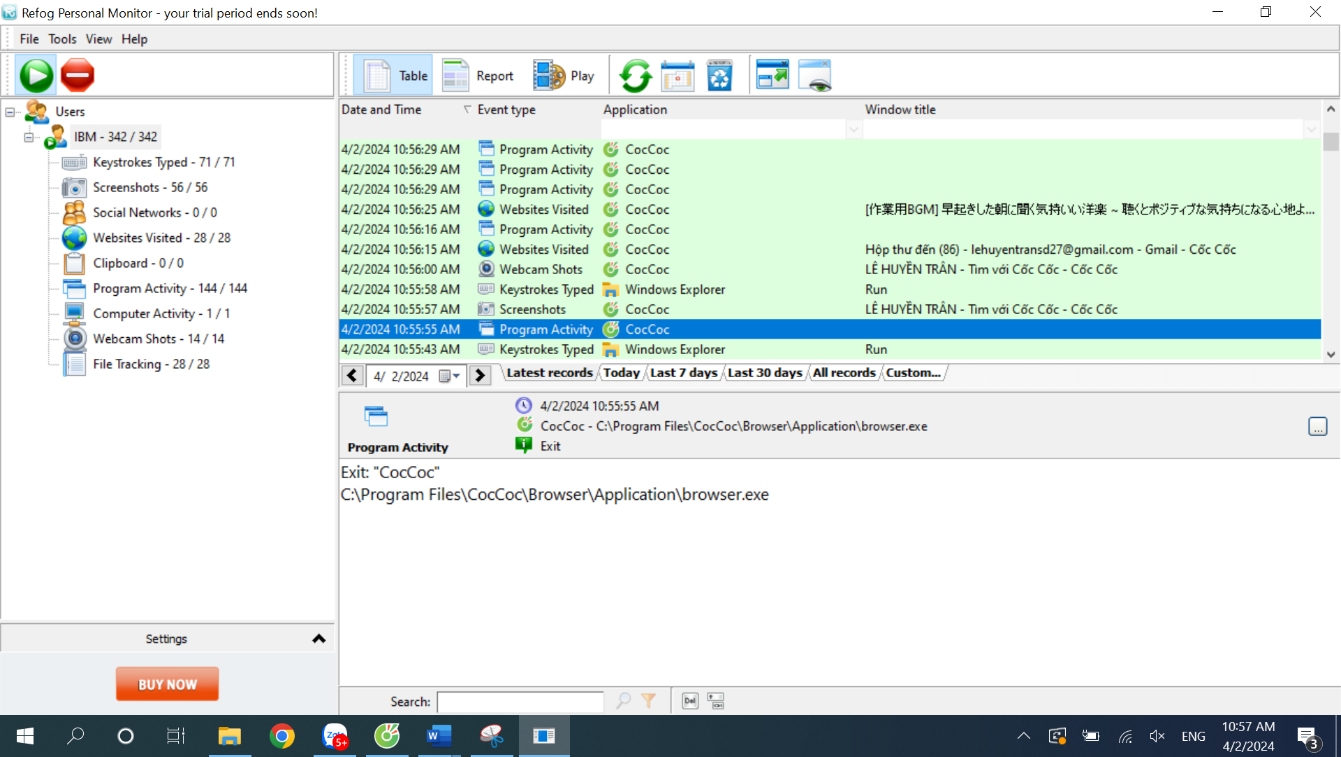
tại https://gmail.com

• Bước 3: Truy cập vào Youtube.com và chọn xem một video bất kỳ.

• Bước 4: Truy cập Google.com và tìm kiếm với từ khóa là tên sinh viên, chọn xem

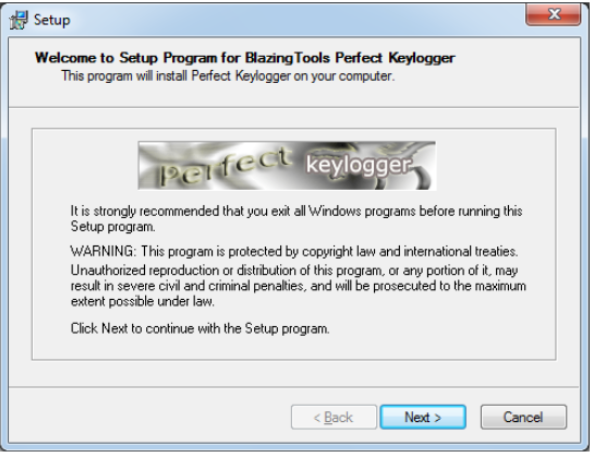
một kết quả bất kỳ.

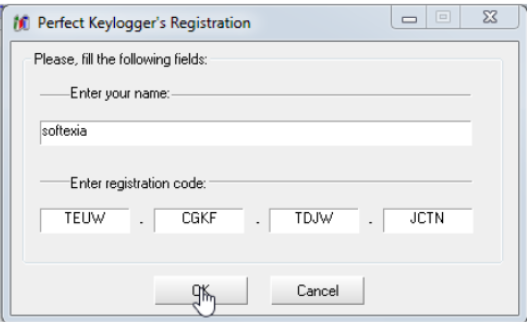
• Bước 5: Mở RFK và xem kết quả thu thập được.



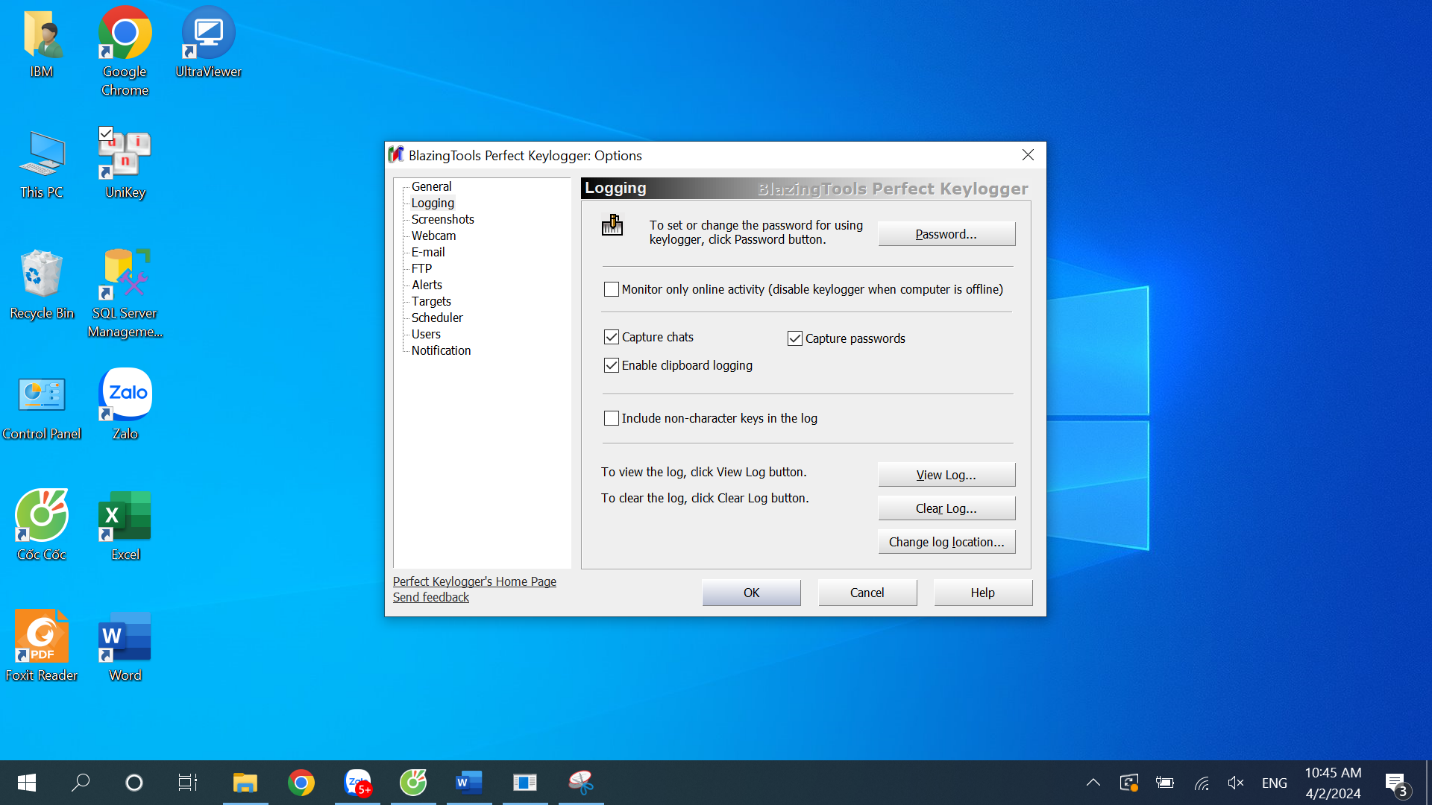
## **2. Thử nghiệm Keylogger gửi kết qué qua email, FTP server**

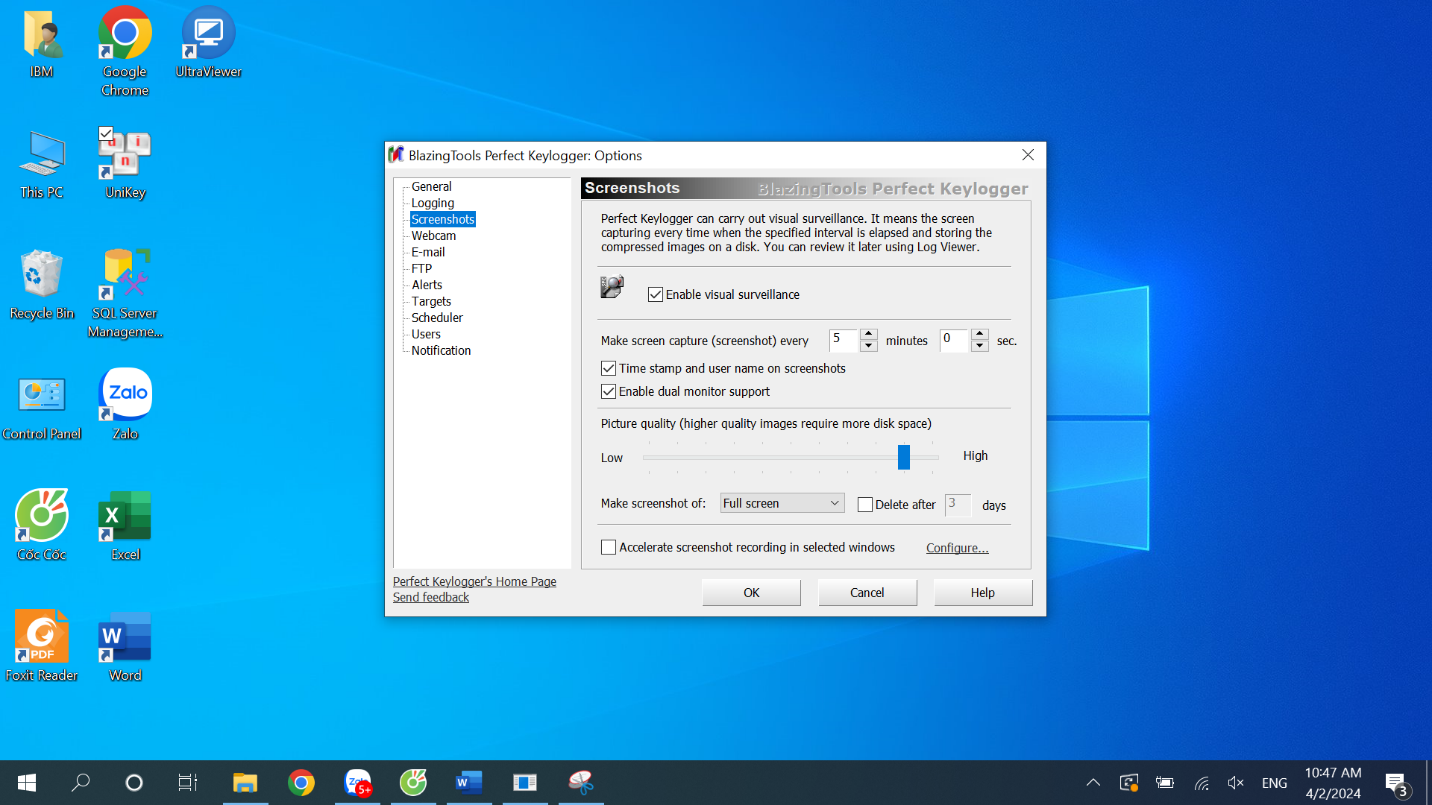
• Bước 1: Cài đặt BPK



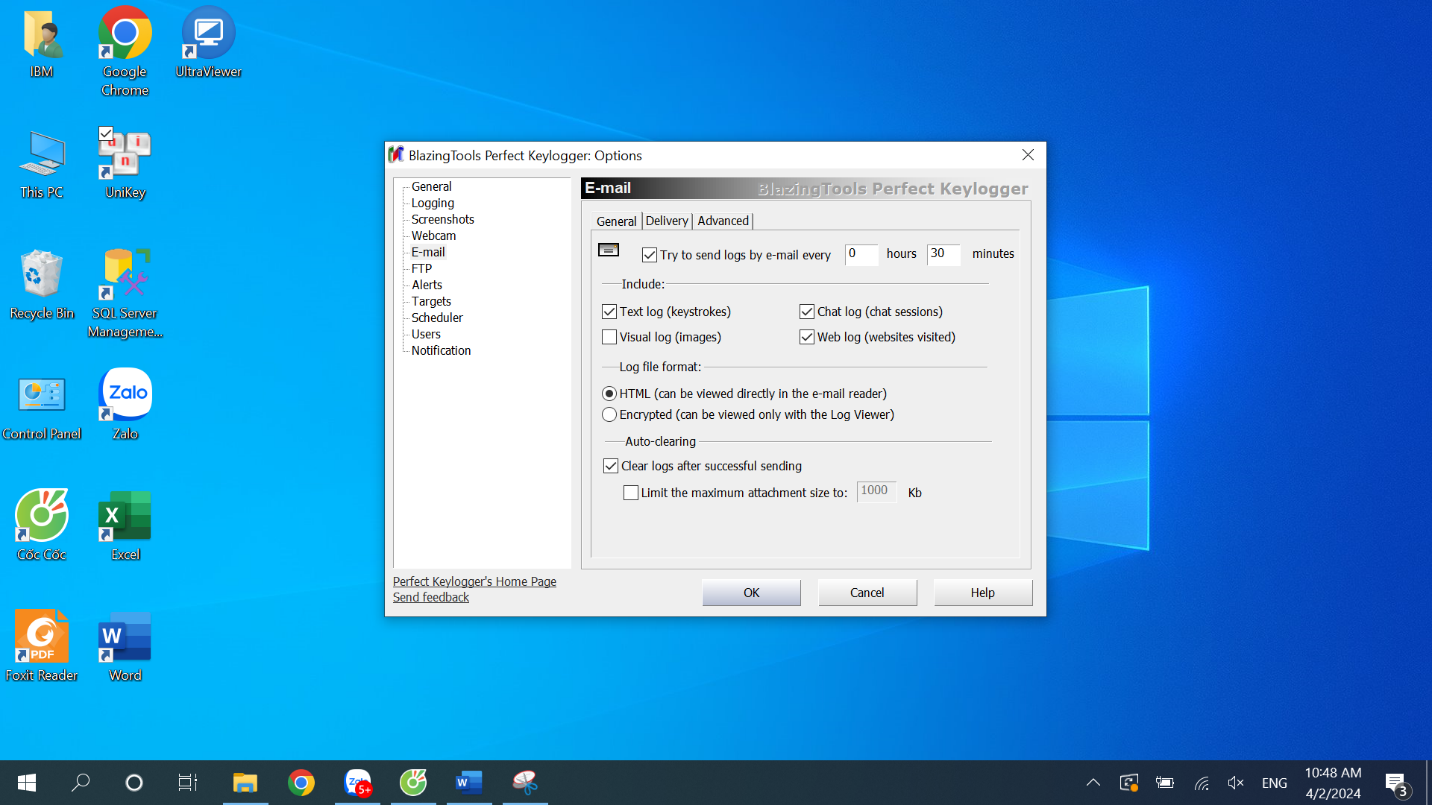


Bước 2: Bật các chức năng chụp ảnh màn hình, theo dõi gõ bàn phím





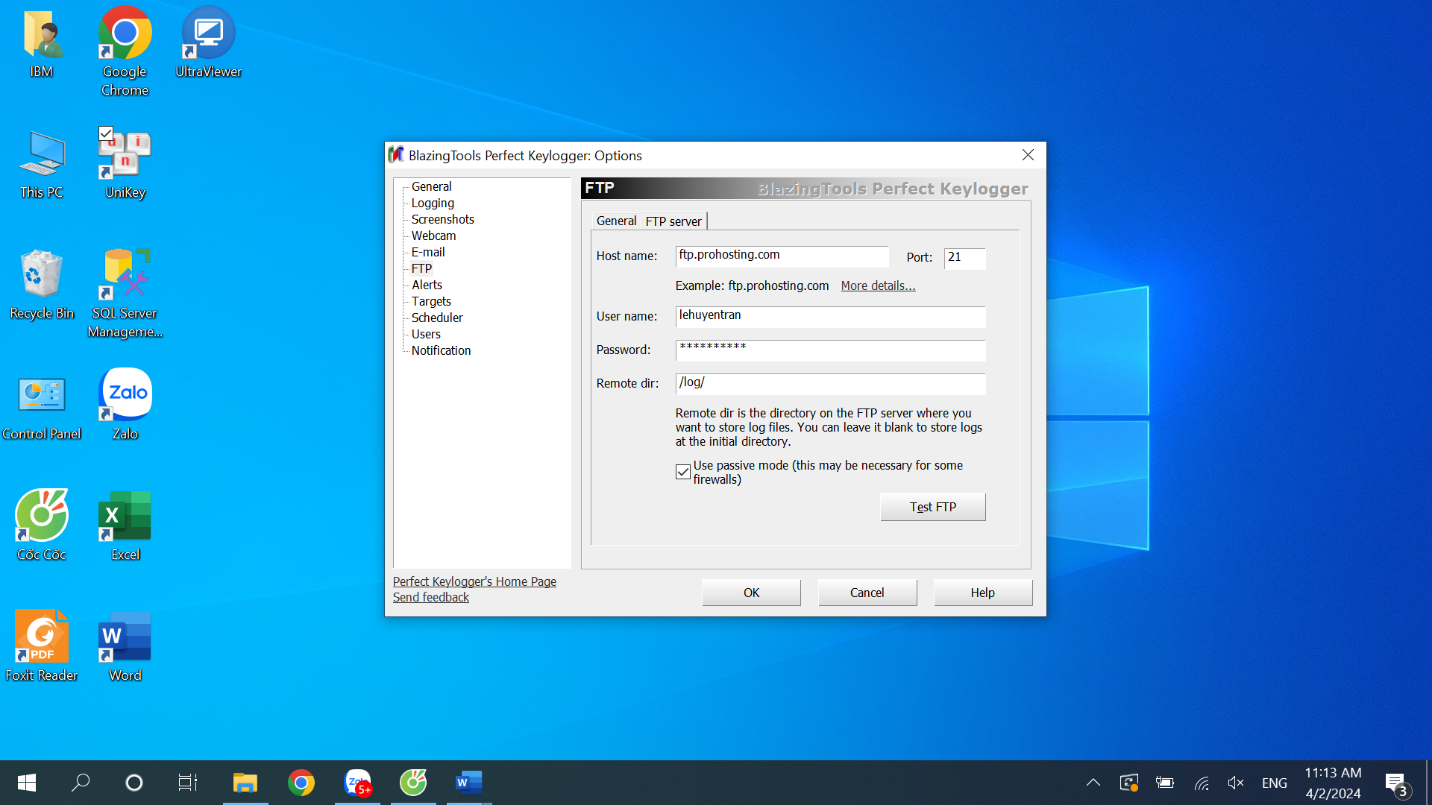
• Bước 3: Cấu hình email để gửi kết quả thu thập được.



• Bước 4: Đăng ký một free hosting có chức năng FTP dùng username/password

để upload file hoặc tự xây dựng 1 FTP server.

• Bước 5: Cấu hình FTP trên BPK để gửi kết quả thu thập được



## **TRẢ LỜI CÂU HỎI**

**1. Nêu biện pháp phòng tránh; các cách phát hiện Keylogger trên máy tính - điện thoại và minh họa nếu có thể.**

Keyloggers là loại phần mềm hoặc thiết bị phần cứng được sử dụng để ghi lại mọi thao tác nhập liệu của người dùng trên máy tính hoặc điện thoại di động, bao gồm cả các phím được nhấn, các chuột được kích hoạt và thậm chí là cả các cú nhấp chuột. Đây là một mối đe dọa đối với sự riêng tư và bảo mật của người dùng, vì thông tin nhạy cảm như tên đăng nhập, mật khẩu và thông tin tài khoản ngân hàng có thể bị đánh cắp.

* **Biện pháp phòng tránh:**

**Cập nhật phần mềm:**

Luôn duy trì phần mềm hệ thống và các ứng dụng lên phiên bản mới nhất để bảo vệ khỏi các lỗ hổng bảo mật có thể được khai thác bởi keyloggers.

**Sử dụng phần mềm chống malware:**

Cài đặt và chạy các phần mềm chống malware chất lượng để phát hiện và loại bỏ keyloggers từ máy tính hoặc điện thoại của bạn.

**Chỉ tải ứng dụng từ nguồn tin cậy:**

Tránh tải ứng dụng từ nguồn không tin cậy, đặc biệt là từ các trang web không rõ nguồn gốc hoặc không được phát triển bởi các nhà phát triển đáng tin cậy.

**Sử dụng mạng riêng ảo (VPN):**

Sử dụng VPN khi kết nối internet để mã hóa dữ liệu và ngăn chặn các loại tấn công gián điệp.

**Kiểm tra các thiết bị ngoại vi:**

Kiểm tra thường xuyên các thiết bị ngoại vi được kết nối với máy tính của bạn, như bàn phím hoặc chuột, để đảm bảo không có keylogger được cài đặt trên chúng.

* **Cách phát hiện Keylogger trên máy tính và điện thoại:**

**Sử dụng phần mềm chống malware:**

Các chương trình chống malware chuyên dụng thường có khả năng phát hiện các keylogger và loại bỏ chúng khỏi hệ thống.

**Kiểm tra quá trình hoạt động của hệ thống:**

Trên máy tính, sử dụng Task Manager hoặc các công cụ quản lý tác vụ khác để kiểm tra các quá trình đang hoạt động. Tìm kiếm các quá trình không quen thuộc có thể là keyloggers.

Trên điện thoại, kiểm tra danh sách ứng dụng đang chạy và tìm kiếm các ứng dụng không quen thuộc hoặc không được cài đặt bởi bạn.

**Kiểm tra ứng dụng và tiến trình:**

Kiểm tra danh sách các ứng dụng và tiến trình được cài đặt trên máy tính hoặc điện thoại của bạn và tìm kiếm các ứng dụng hoặc tiến trình không quen thuộc.

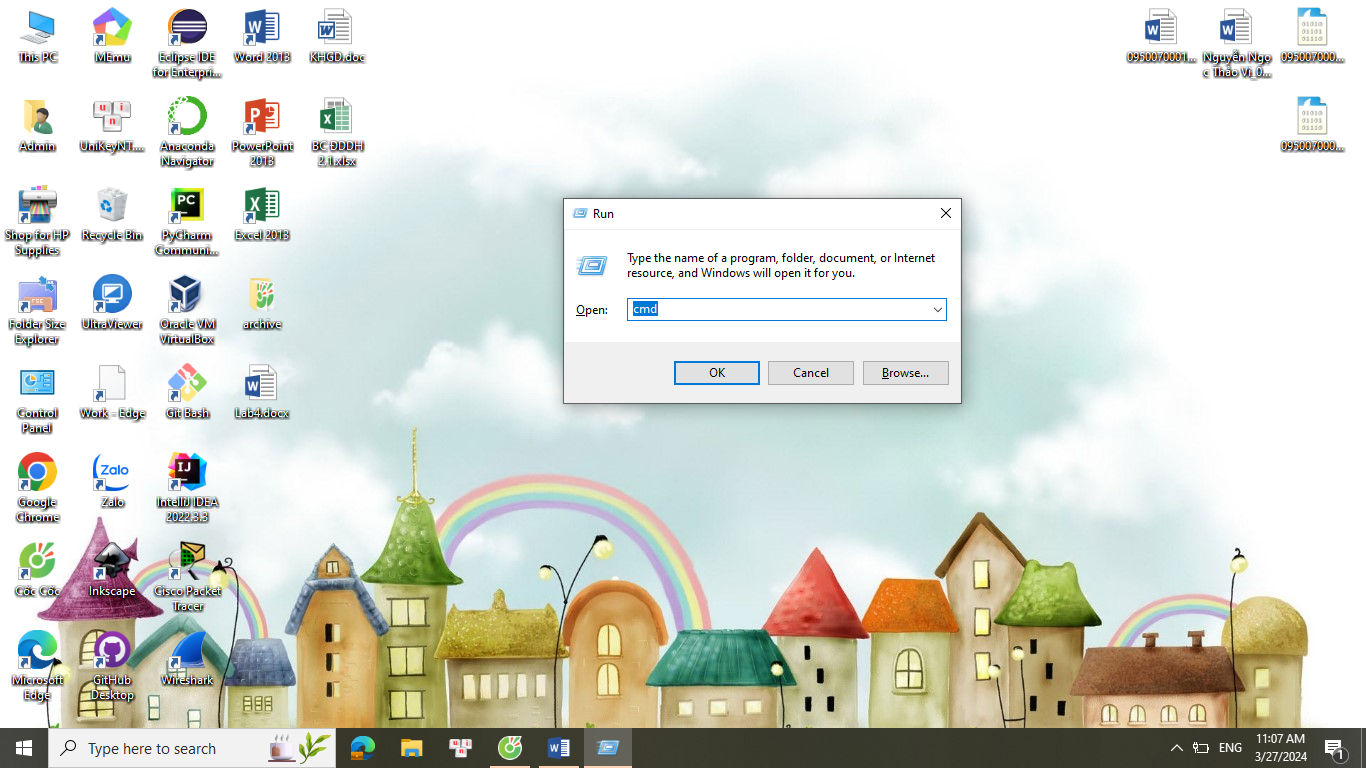
**Sử dụng công cụ phát hiện keylogger:**

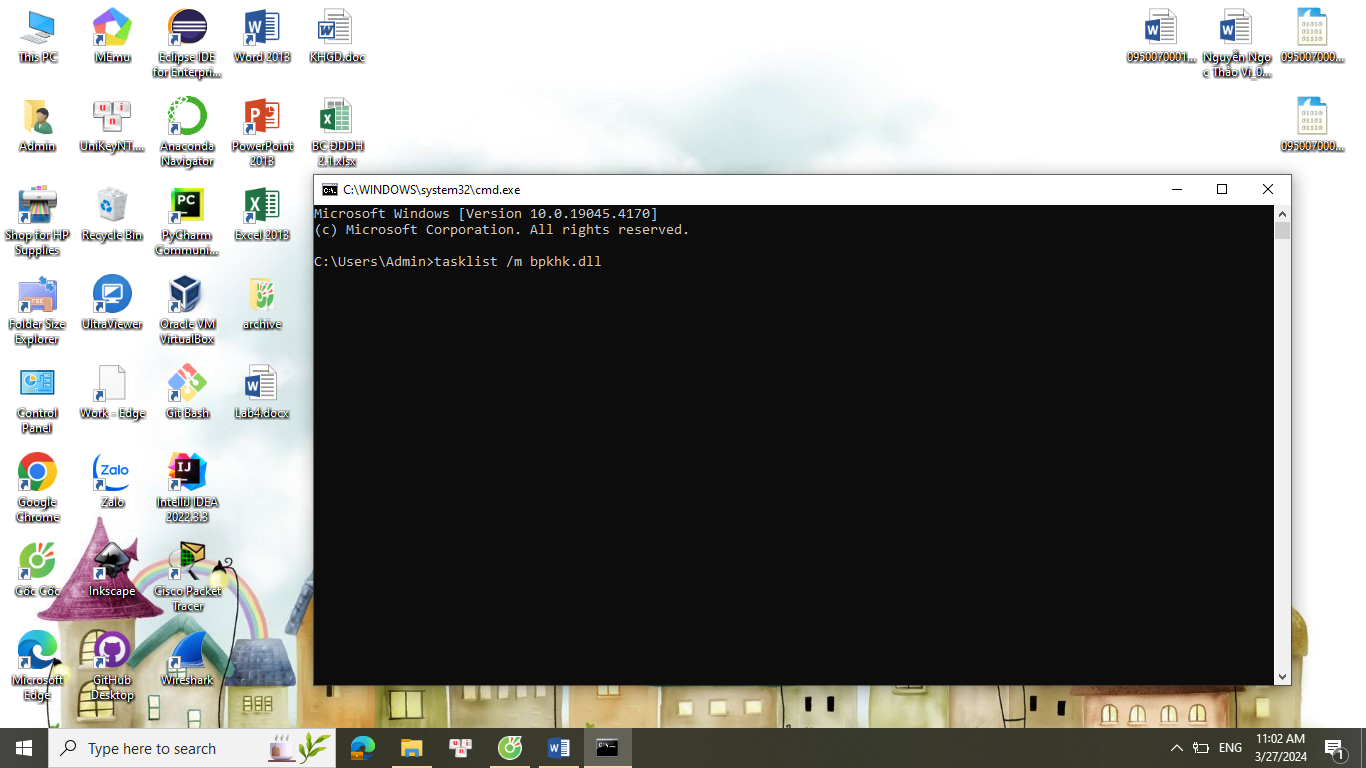
Có một số công cụ phát hiện keylogger có thể được sử dụng để quét hệ thống của bạn và xác định xem có keylogger nào đang hoạt động hay không.

* **Minh họa:**

**Cách kiểm tra Keylogger trên máy tính bằng Perfect keylogger**

**Bước 1**: Tại menu chính của máy, để mở hộp thoại Run thì nhấn tổ hợp phím **Windows + R** > Tại ô **Open**, nhập từ khóa **cmd** > Nhấn **OK** để mở cửa sổ cmd.exe.

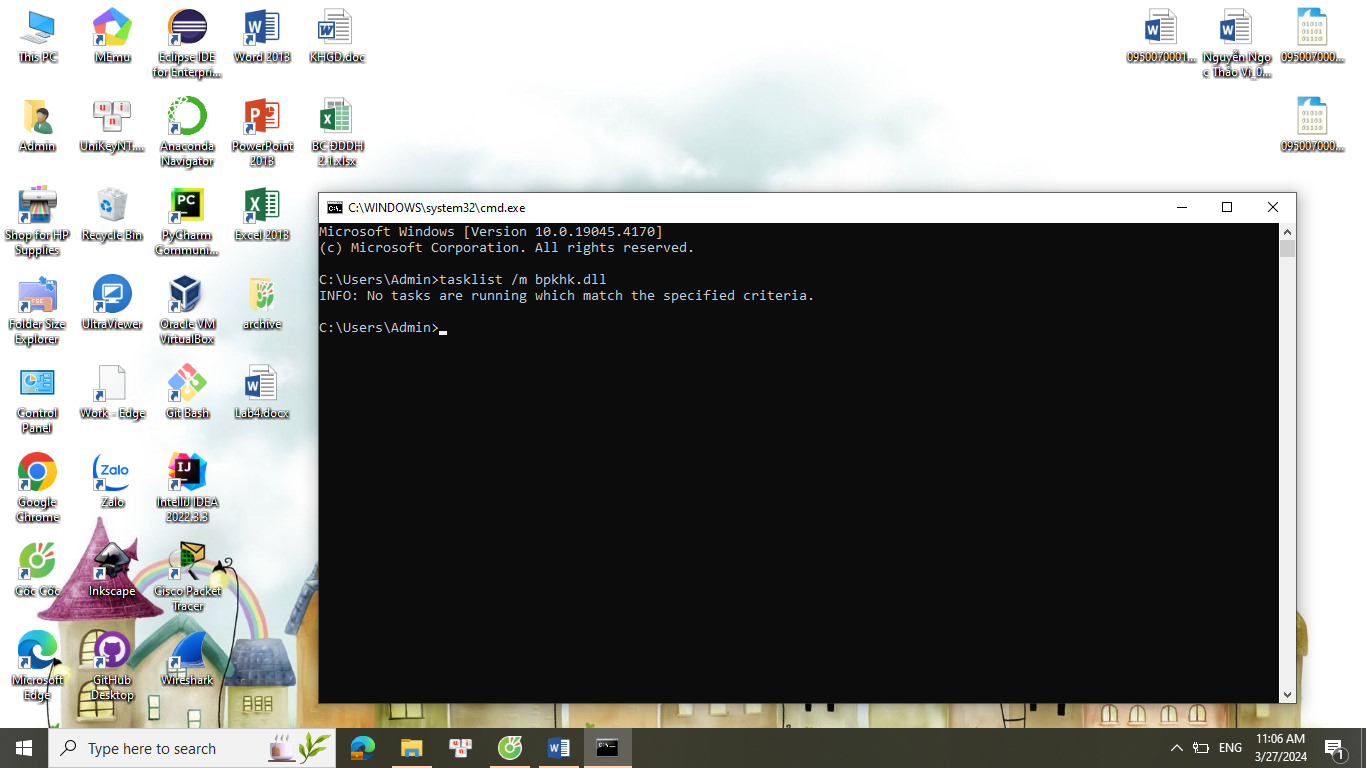


**Bước 2**: Tại đây, nhập lệnh **tasklist /m bpkhk.dll** > Nhấn **Enter**.

**Bước 3**: Nếu màn hình hiển thị thông báo INFO: **No tasks are running which match the specified criteria** thì chứng tỏ máy không bị nhiễm Keylogger. Còn trong trường hợp máy có cài Keylogger thì màn hình sẽ hiển thị Image Name PID Modules cùng một số ký tự khác như:

- explorer\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 468 bpkhk.dll

- DUMeter\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 1444 bpkhk.dll

- ctfmon\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 1548 bpkhk.dll

**2. Tìm thêm và giới thiệu một số loại Keylogger trên máy tính và điện thoại khác.**

* **Keylogger phần mềm:**

**Keylogger Remote Access:**

Loại này ghi lại mọi thao tác đánh máy và gửi dữ liệu đó đến một máy chủ từ xa mà kẻ tấn công có thể truy cập để thu thập thông tin.

**Keylogger cho điện thoại di động:**

Các ứng dụng keylogger được cài đặt trên điện thoại di động ghi lại mọi thao tác nhập liệu trên bàn phím của điện thoại và gửi dữ liệu về máy chủ từ xa.

**Keylogger dựa trên trình duyệt:**

Các keylogger có thể được cài đặt dưới dạng các tiện ích mở rộng hoặc phần mềm trên trình duyệt web. Chúng ghi lại thông tin đăng nhập, mật khẩu và các dữ liệu khác được nhập qua các trang web.

**Keylogger gắn kết với email:**

Keylogger này ghi lại thông tin và gửi chúng đến một địa chỉ email được cấu hình trước, thay vì lưu trữ dữ liệu trên máy chủ từ xa.

* **Keylogger phần cứng:**

**USB Keylogger:**

Thiết bị này kết nối giữa bàn phím và máy tính và ghi lại mọi phím được nhấn trên bàn phím, không cần cài đặt phần mềm trên máy tính.

**Keylogger gắn vào chuột:**

Một số keylogger được tích hợp vào chuột, ghi lại mọi thao tác nhấp chuột và thậm chí cả các cú nhấp và di chuyển chuột.

**Keylogger gắn vào bo mạch chủ (hardware keylogger):**

Các thiết bị này được gắn vào bên trong máy tính, giữa bàn phím và bo mạch chủ, để ghi lại mọi thao tác đánh máy mà không cần cài đặt phần mềm.

**Keylogger trong thiết bị USB:**

Một số keylogger được thiết kế nhỏ gọn và có thể cắm trực tiếp vào cổng USB của máy tính, ghi lại mọi thao tác nhập liệu mà không cần cài đặt phần mềm.