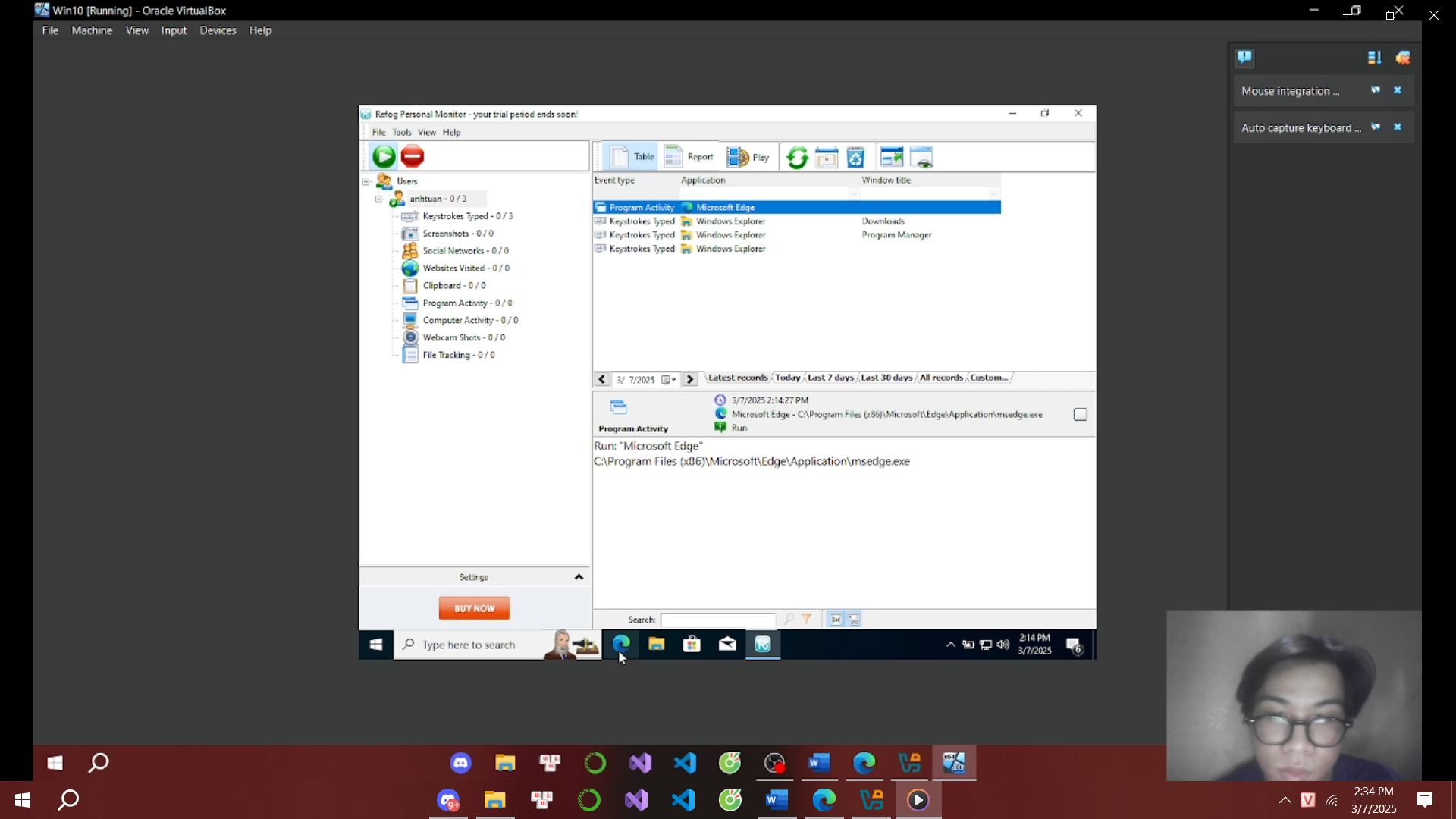
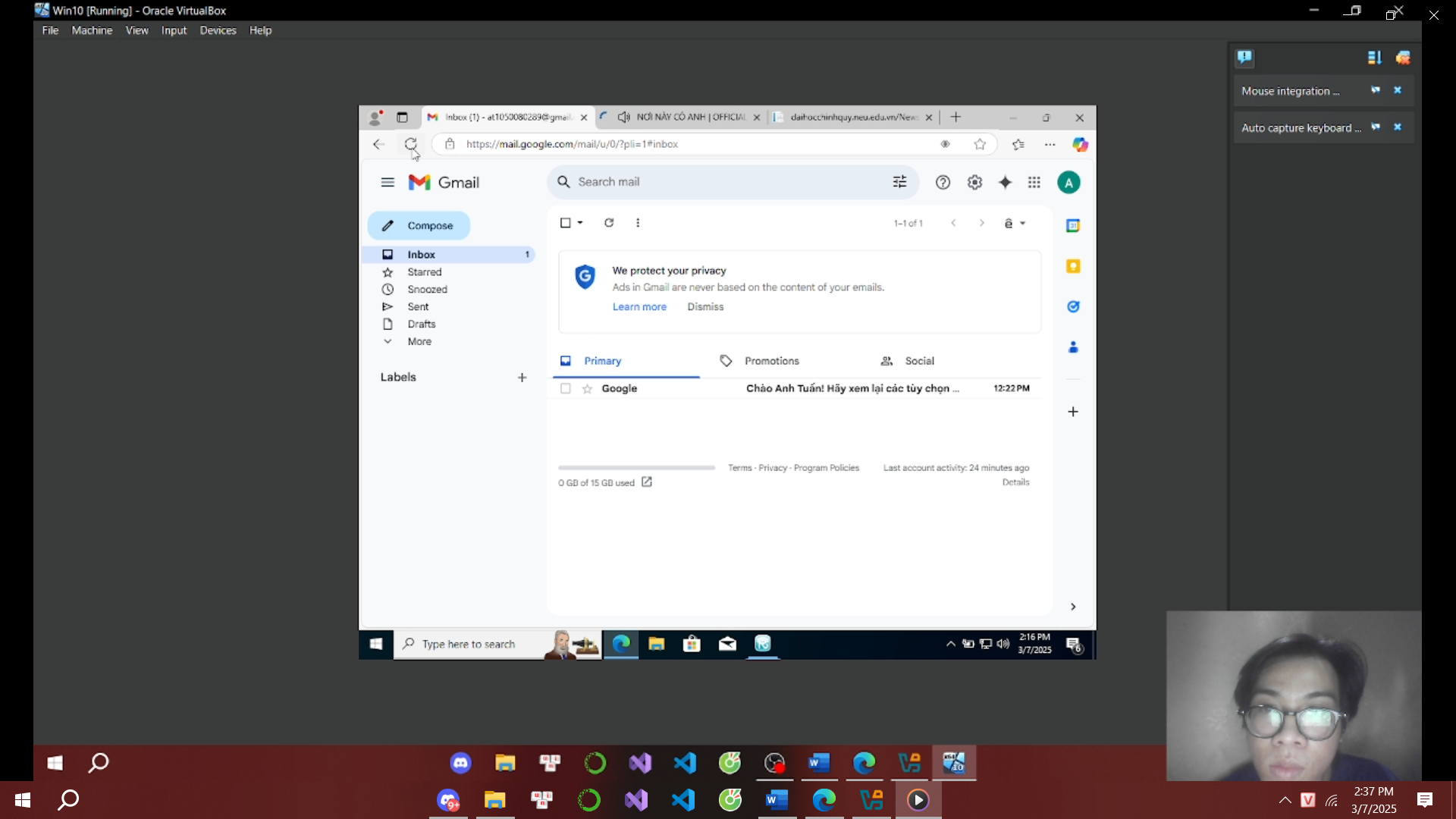
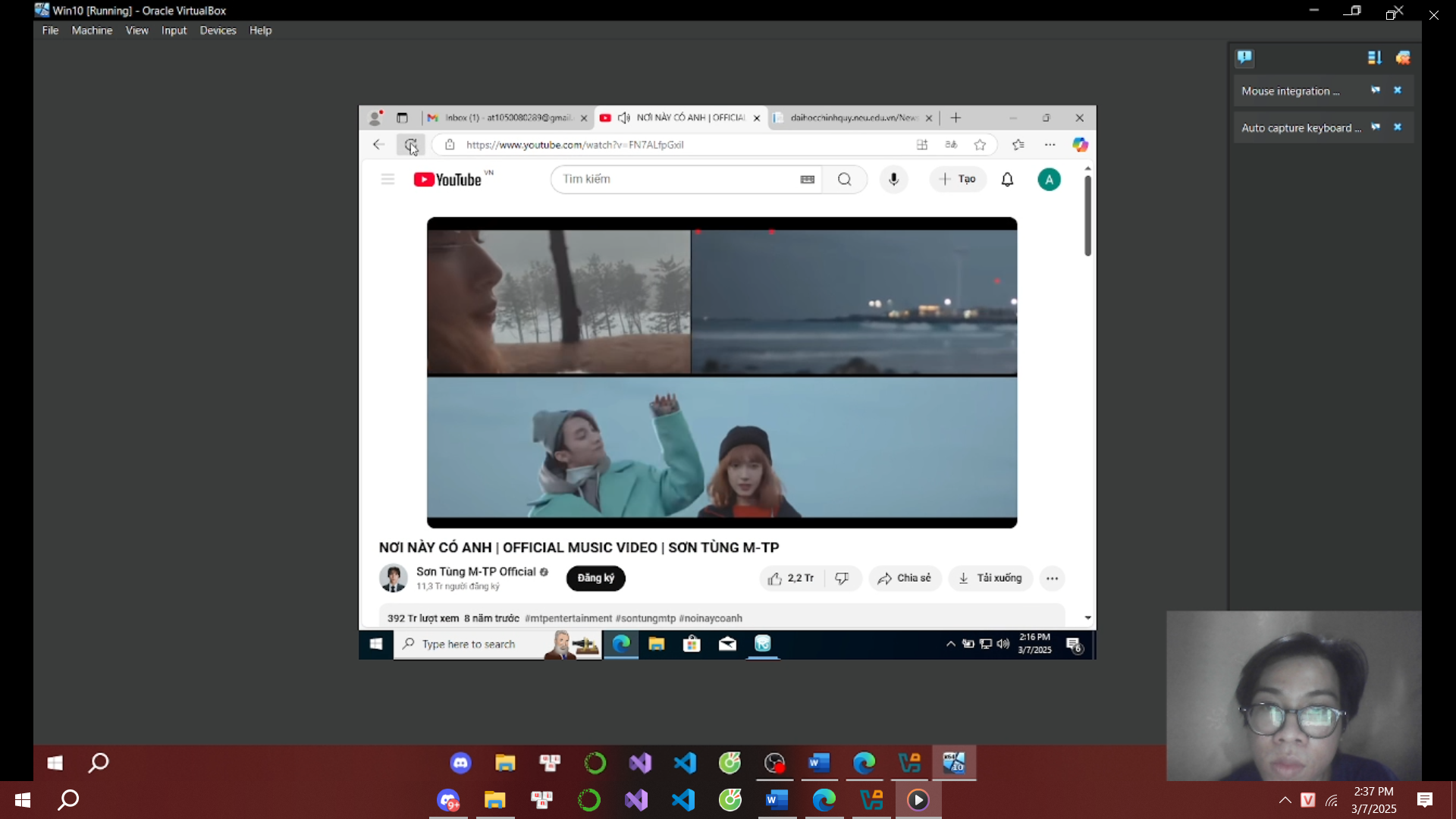
**LAB 2 KEYLOGGER**

**Khởi động RFK.**

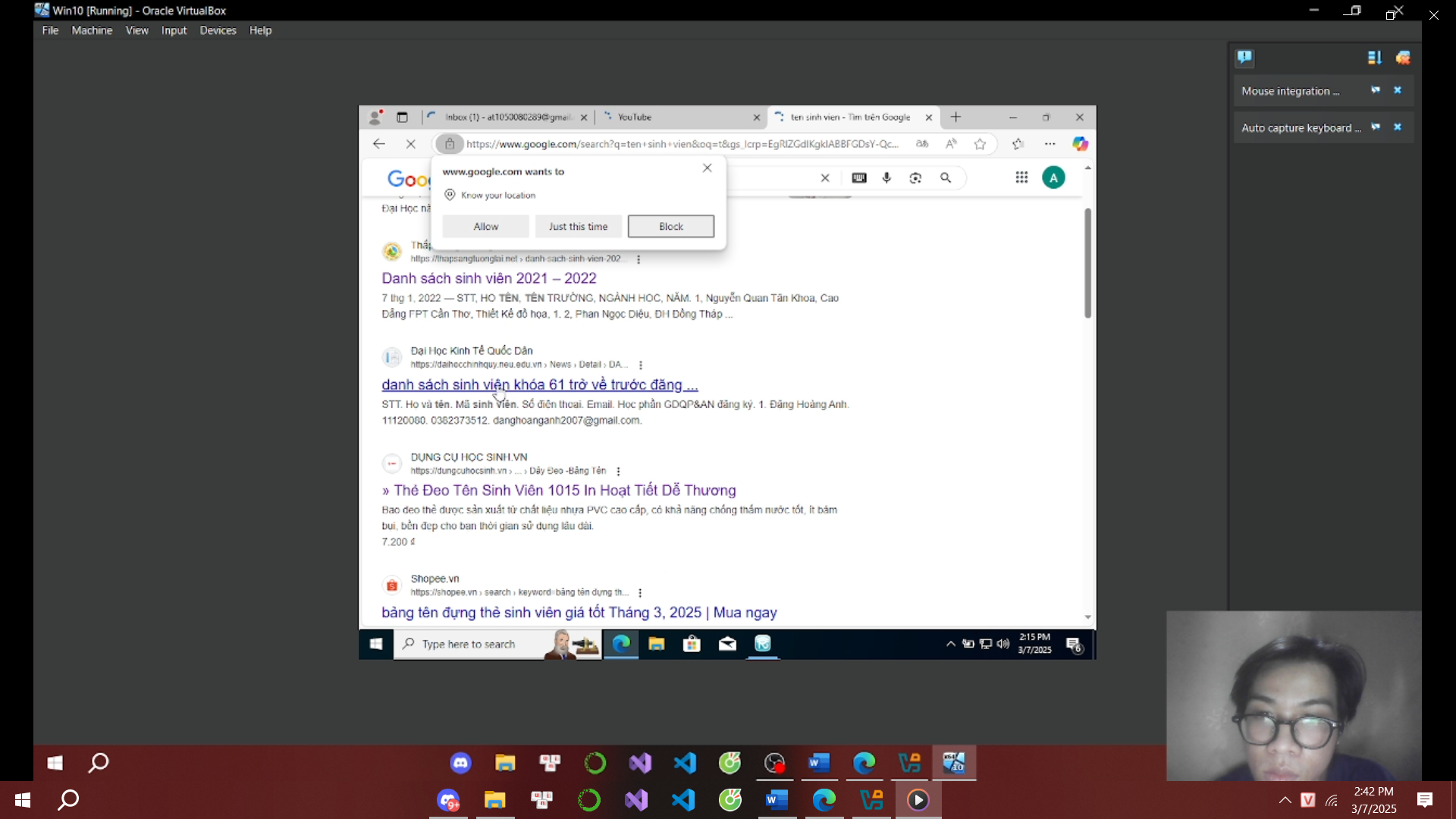


**Dùng trình duyệt web, đăng nhập thành công vào một tài khoản Gmail tại** [**https://gmail.com**](https://gmail.com)

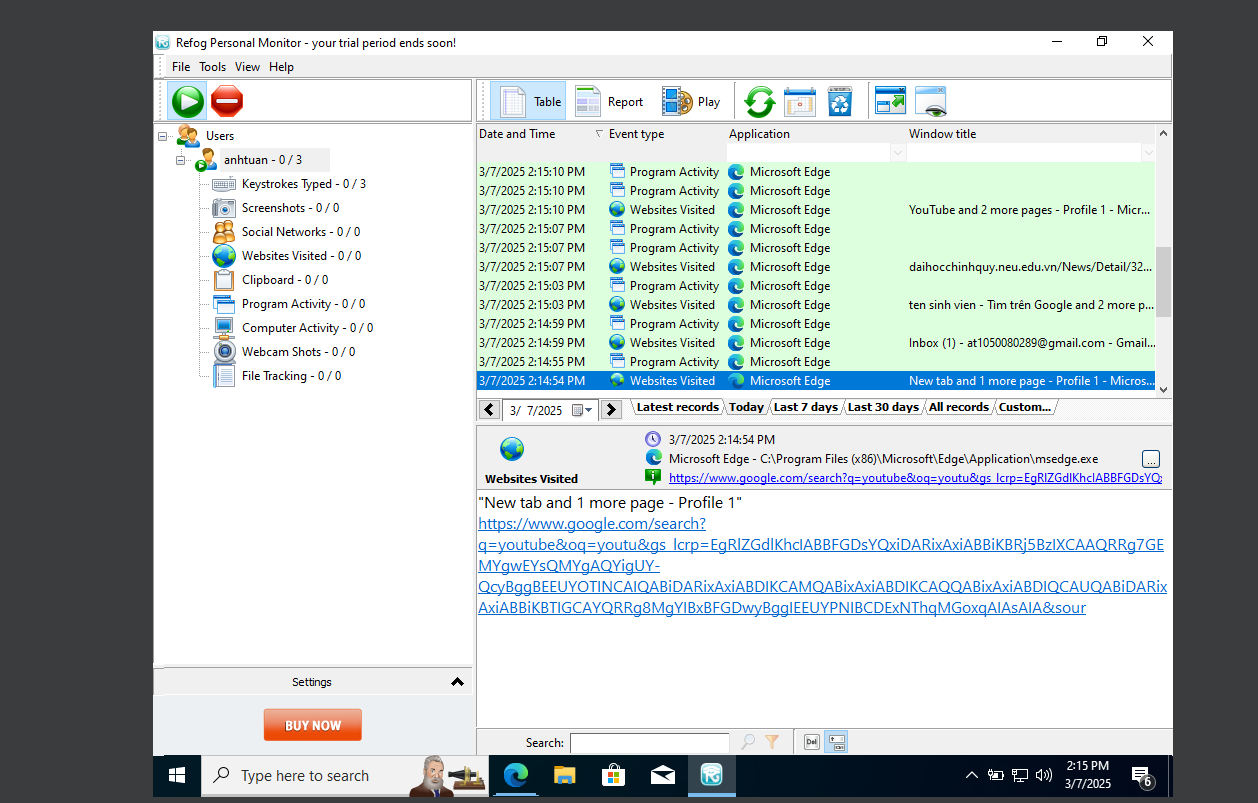


**Truy cập vào Youtube.com và chọn xem một video bất kỳ.**

**Truy cập Google.com và tìm kiếm với từ khóa là tên sinh viên, chọn xem một kết quả bất kỳ.**



**Xem các kết quả thu thập được từ RFK**



**CÂU HỎI**

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

**Biện pháp phòng tránh Keylogger:**

* **Trên máy tính:** 
  1. Cài đặt và cập nhật phần mềm diệt virus (Antivirus): Sử dụng các phần mềm uy tín như Kaspersky, Bitdefender, hoặc Malwarebytes để quét và loại bỏ keylogger. Đảm bảo phần mềm luôn được cập nhật để nhận diện các mối đe dọa mới nhất.
  2. Sử dụng bàn phím ảo (On-screen keyboard): Khi nhập thông tin nhạy cảm như mật khẩu, sử dụng bàn phím ảo tích hợp trong Windows (truy cập qua "Ease of Access") để tránh bị ghi lại thao tác gõ phím.
  3. Kiểm tra phần cứng: Thường xuyên kiểm tra các cổng USB hoặc bàn phím để phát hiện thiết bị keylogger phần cứng (hardware keylogger) được gắn vào máy tính.
  4. Tránh tải phần mềm từ nguồn không tin cậy: Chỉ tải phần mềm từ các trang web chính thức hoặc kho ứng dụng đáng tin cậy để giảm nguy cơ cài đặt phần mềm chứa keylogger.
  5. Sử dụng tường lửa (Firewall): Kích hoạt tường lửa để chặn các kết nối đáng ngờ mà keylogger có thể sử dụng để gửi dữ liệu ra ngoài.
* **Trên điện thoại:** 
  1. Cài đặt ứng dụng từ nguồn chính thức: Chỉ tải ứng dụng từ Google Play Store (Android) hoặc App Store (iOS) để tránh cài đặt ứng dụng chứa mã độc.
  2. Kiểm tra quyền ứng dụng: Định kỳ kiểm tra các quyền mà ứng dụng yêu cầu (ví dụ: quyền truy cập bàn phím, tin nhắn) và gỡ bỏ ứng dụng đáng ngờ.
  3. Cập nhật hệ điều hành: Luôn cập nhật phiên bản mới nhất của Android hoặc iOS để vá các lỗ hổng bảo mật mà keylogger có thể khai thác.
  4. Mã hóa dữ liệu: Sử dụng tính năng mã hóa của điện thoại và tránh kết nối với Wi-Fi công cộng không an toàn.

**Cách phát hiện Keylogger:**

* **Trên máy tính:** 
  1. Kiểm tra tiến trình (Task Manager): Mở Task Manager (Ctrl + Shift + Esc trên Windows) để tìm các tiến trình lạ đang chạy. Ví dụ, nếu thấy một tiến trình tiêu tốn CPU bất thường hoặc không rõ nguồn gốc, đó có thể là dấu hiệu của keylogger.
     + Minh họa: Chạy REFOG Free Keylogger (như trong bài Lab), sau đó kiểm tra Task Manager, bạn có thể thấy tiến trình "rfk.exe" xuất hiện.
  2. Quét bằng phần mềm chống mã độc: Sử dụng Malwarebytes hoặc ESET Online Scanner để phát hiện và loại bỏ keylogger phần mềm.
  3. Theo dõi lưu lượng mạng: Dùng công cụ như Wireshark để kiểm tra xem có dữ liệu nào (như email, FTP) được gửi đi từ máy tính mà bạn không khởi tạo hay không.
  4. Kiểm tra phần cứng: Tháo rời bàn phím hoặc kiểm tra cổng USB để tìm thiết bị keylogger vật lý.
* **Trên điện thoại:** 
  1. Kiểm tra mức sử dụng pin: Nếu pin hao nhanh bất thường, có thể một ứng dụng keylogger đang chạy ngầm. Vào "Settings > Battery" để kiểm tra ứng dụng tiêu tốn pin.
     + Minh họa: Cài thử một ứng dụng như Hoverwatch, sau đó quan sát mức tiêu thụ pin tăng đột biến.
  2. Kiểm tra dữ liệu mạng: Vào "Settings > Data Usage" để xem ứng dụng nào đang gửi dữ liệu ra ngoài mà bạn không sử dụng.
  3. Sử dụng ứng dụng chống mã độc: Tải các ứng dụng như Avast Mobile Security hoặc Kaspersky Mobile Antivirus để quét và phát hiện keylogger.

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

**Dưới đây là một số loại keylogger khác ngoài REFOG Free Keylogger và BlazingTools Perfect Keylogger (đã đề cập trong tài liệu):**

* **Trên máy tính:** 
  1. Spyrix Personal Monitor:
     + Mô tả: Là một phần mềm giám sát toàn diện, ghi lại thao tác bàn phím, chụp ảnh màn hình, theo dõi webcam và gửi báo cáo qua email hoặc FTP.
     + Tính năng nổi bật: Hỗ trợ ẩn mình khỏi Task Manager, phù hợp để giám sát từ xa.
     + Nguồn: <https://www.spyrix.com/>
  2. All In One Keylogger:
     + Mô tả: Ghi lại toàn bộ phím bấm, chụp ảnh màn hình, theo dõi clipboard và gửi dữ liệu qua email hoặc FTP.
     + Tính năng nổi bật: Có chế độ mã hóa dữ liệu thu thập được để tăng tính bảo mật cho người dùng keylogger.
     + Nguồn: <https://www.relytec.com/>
  3. Elite Keylogger:
     + Mô tả: Một keylogger nhẹ, dễ cài đặt, có khả năng ghi lại mật khẩu, tin nhắn và hoạt động web.
     + Tính năng nổi bật: Chạy ở chế độ ẩn (stealth mode) và khó bị phát hiện bởi phần mềm diệt virus.
     + Nguồn: <https://www.widestep.com/>
* **Trên điện thoại:** 
  1. mSpy:
     + Mô tả: Một ứng dụng giám sát phổ biến cho Android và iOS, ghi lại tin nhắn, cuộc gọi, thao tác bàn phím và vị trí GPS.
     + Tính năng nổi bật: Hỗ trợ xem dữ liệu từ xa qua giao diện web, không yêu cầu root/jailbreak trong một số trường hợp.
     + Nguồn: <https://www.mspy.com/>
  2. FlexiSPY:
     + Mô tả: Keylogger mạnh mẽ cho Android và iOS, ghi lại mọi thao tác bàn phím, cuộc gọi, và cả âm thanh xung quanh qua micro.
     + Tính năng nổi bật: Có thể ghi âm cuộc gọi và theo dõi ứng dụng nhắn tin như WhatsApp, Telegram.
     + Nguồn: <https://www.flexispy.com/>
  3. Hoverwatch:
     + Mô tả: Ứng dụng giám sát cho Android, ghi lại phím bấm, chụp ảnh màn hình, theo dõi cuộc gọi và tin nhắn.
     + Tính năng nổi bật: Hoạt động ẩn, gửi báo cáo qua email hoặc tài khoản trực tuyến.
     + Nguồn: <https://www.hoverwatch.com/>