**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

**Môn: Thực Hành Phân Tích Mã Độc**

**---------------------------------------------------------------------**

**Họ Và Tên: Trần Hân Nhi**

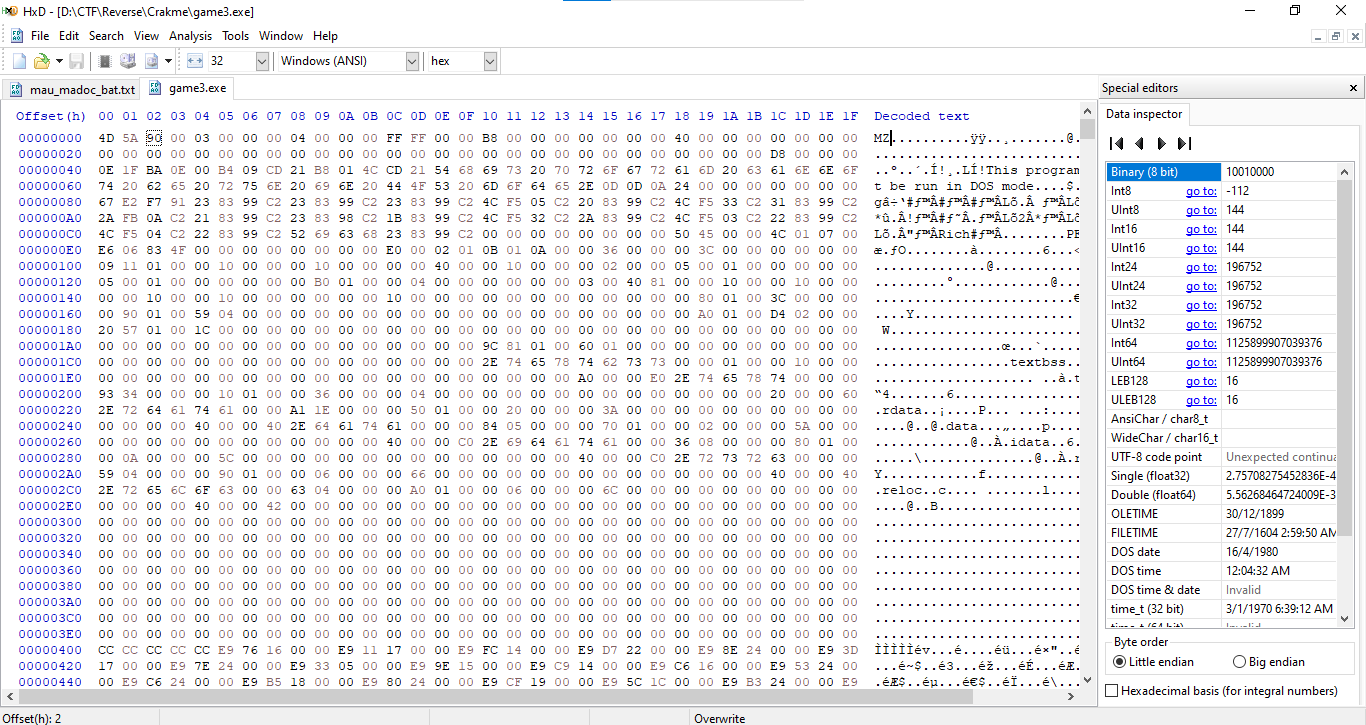
**MSSV: 2011770131**

**Lớp: 20DATA1**

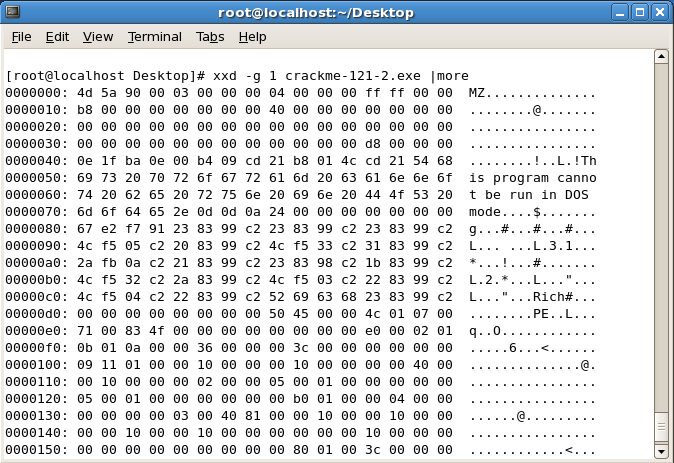
**Báo Cáo Tuần 1**

**Câu 1: Xác định loại tệp**

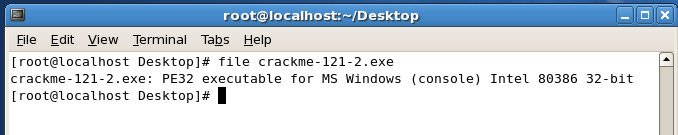
* Sử dụng phương pháp thủ công xem bằng HxD. Kiểm tra từng bye của tệp



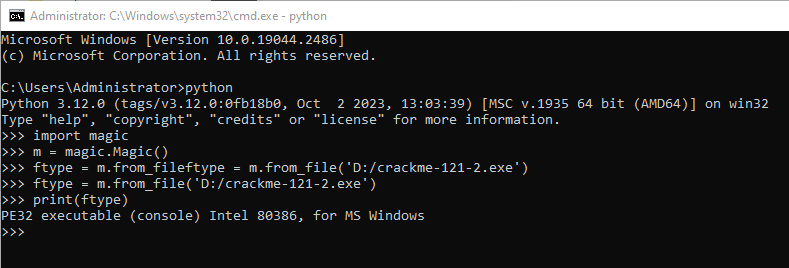
* Sử dụng lệnh xxd trên linux



* Sử dụng công cụ trên Linux, dùng lệnh “file”

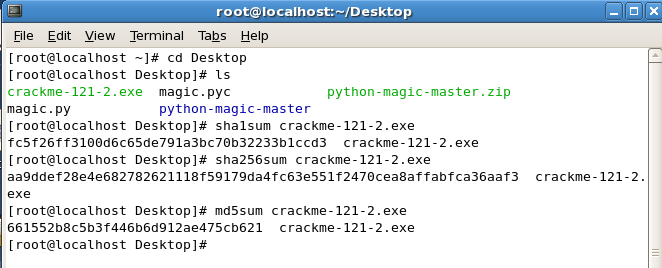
****

* Xác định bằng module python-magic

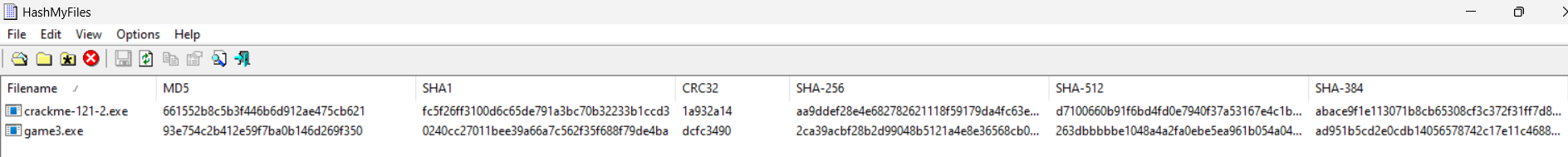
****

**Câu 2: Nhận dạng thông qua hàm băm**

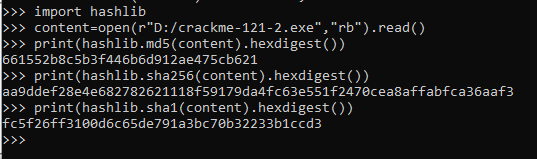
* Dùng lệnh tạo giá trị băm trên linux



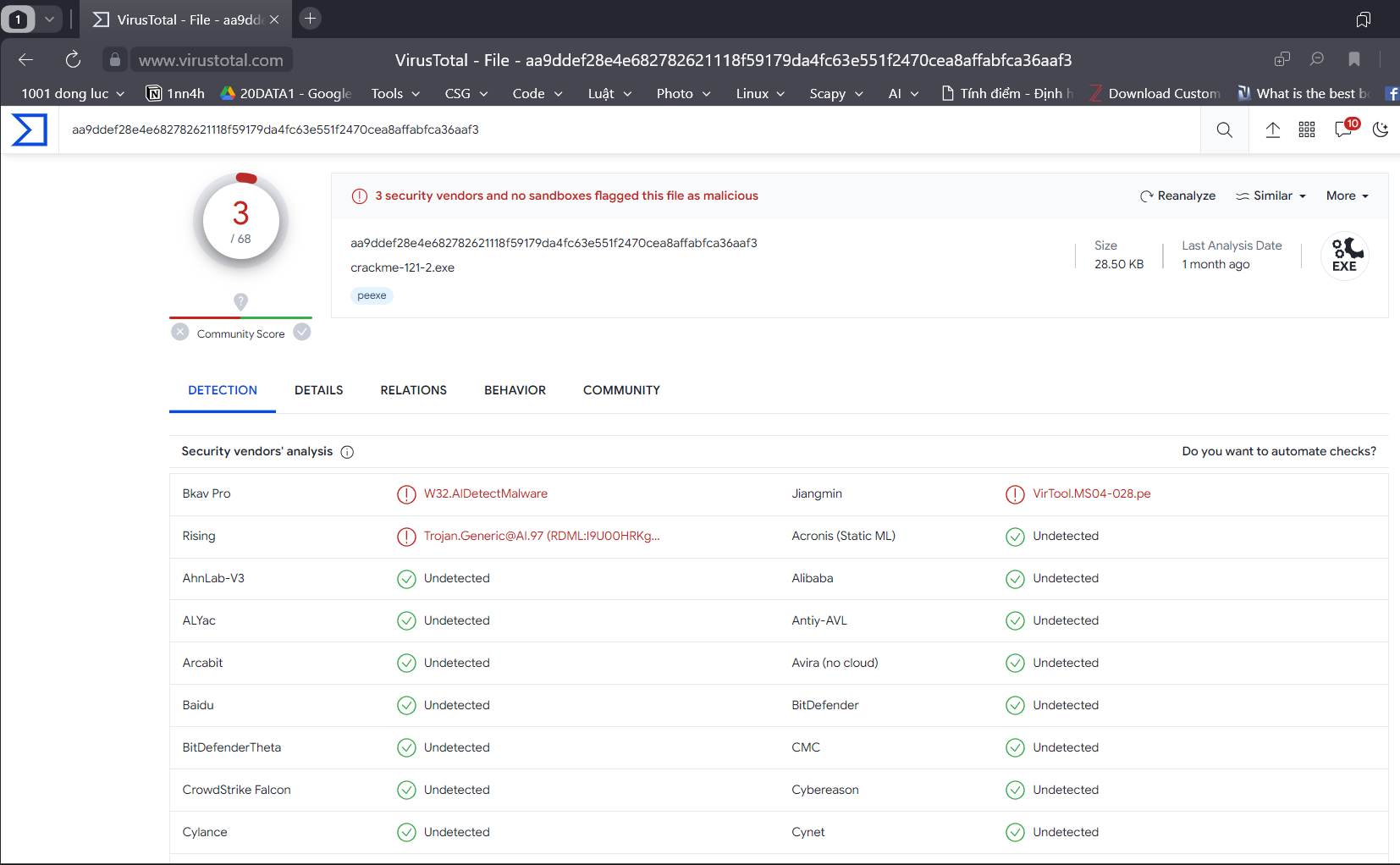
* Dùng HashMyFiles trên Window



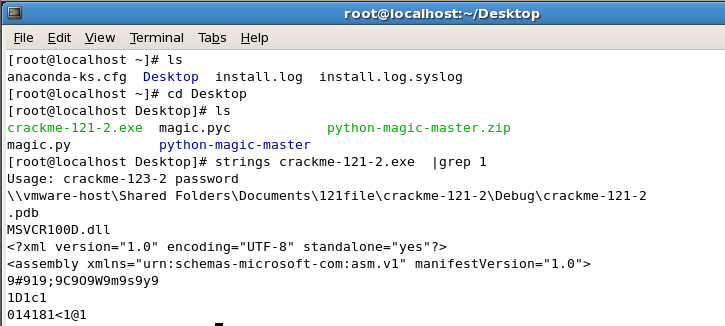
* Xác định giá trị băm bằng python với module hashlib

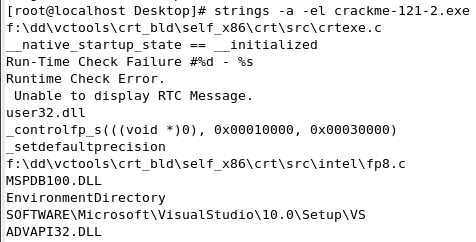
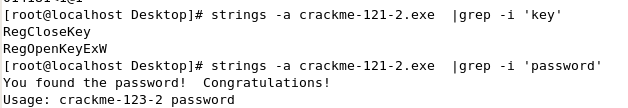


**Câu 3 Phân tích tệp tin chứa Virus**

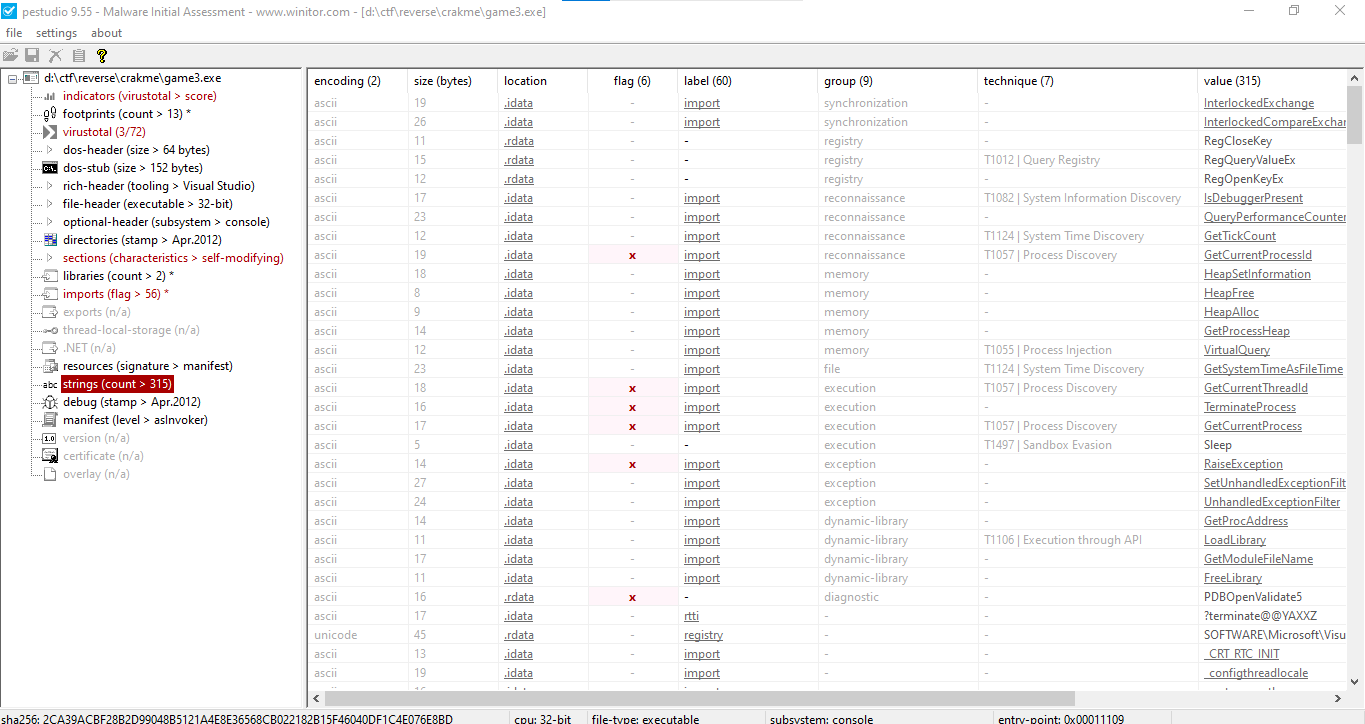


**Câu 4: Trích xuất chuỗi – Strings**

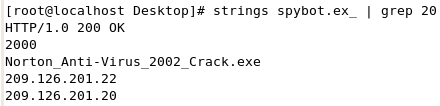




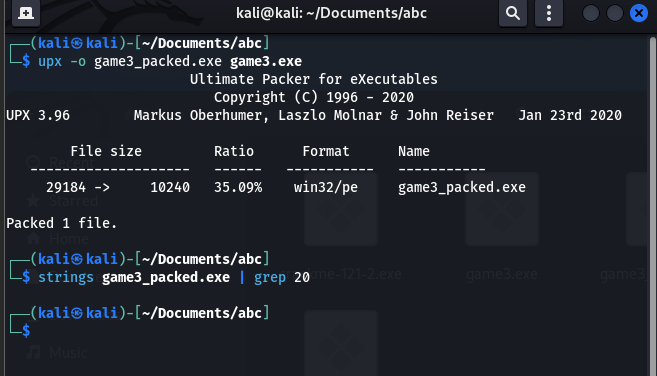
* Dùng Pestudio để phân tích



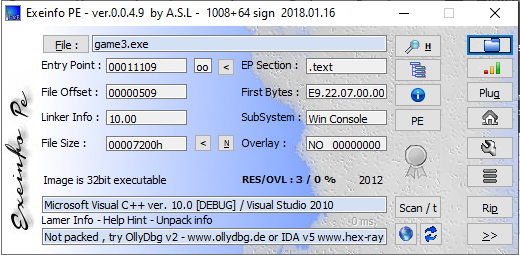
**Câu 5: Xác định tập tin nghi vấn làm rối**



* Dùng upx nén file tăng tính bí mật cho tệp tin

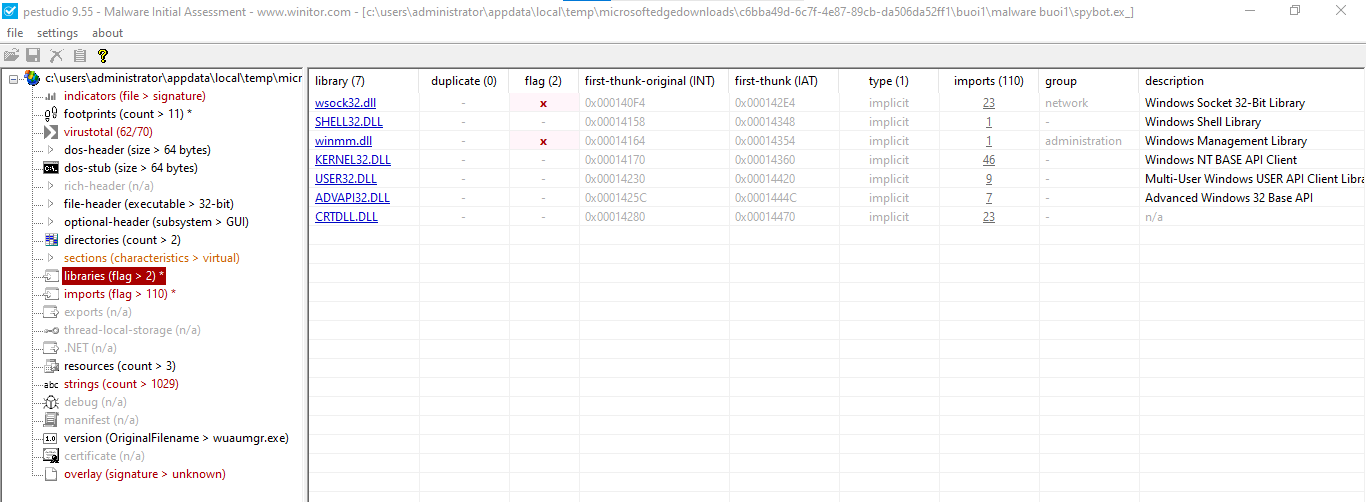
****

* Phát hiện bằng exeinfo PE. Có thể xác định được phần mềm ném vào exeinfo PE nén bằng .text



**Câu 6: Kiếm tra phần đầu PE**

* Dùng pestudio kiểm tra libraries



* Dùng pestudio kiểm tra imports

