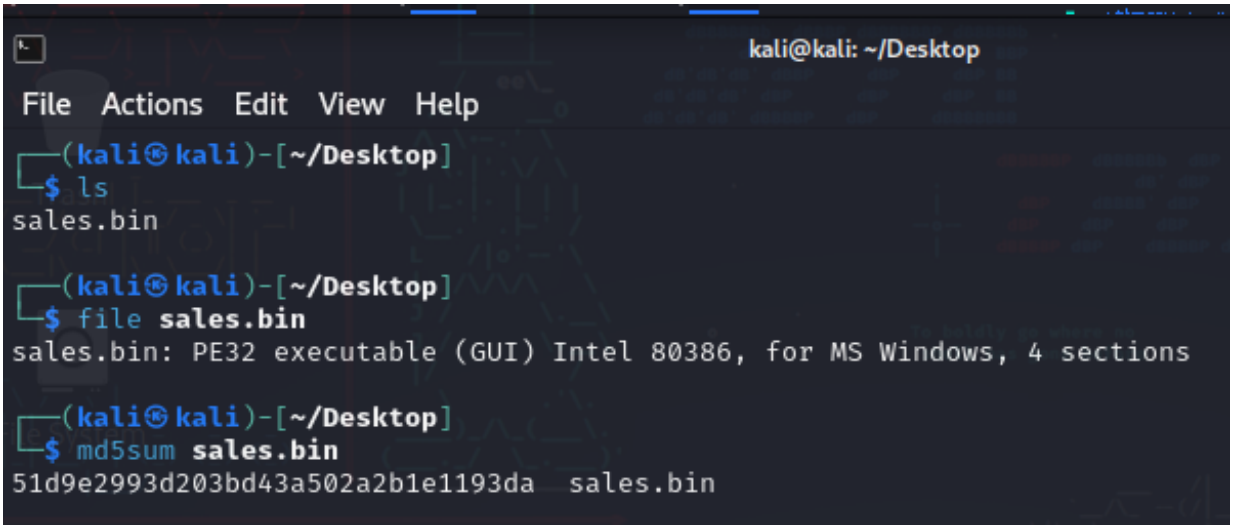
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM
KHOA CÔNG NGHỆ THÔNG TIN
Môn: Thực Hành Phân Tích Mã Độc

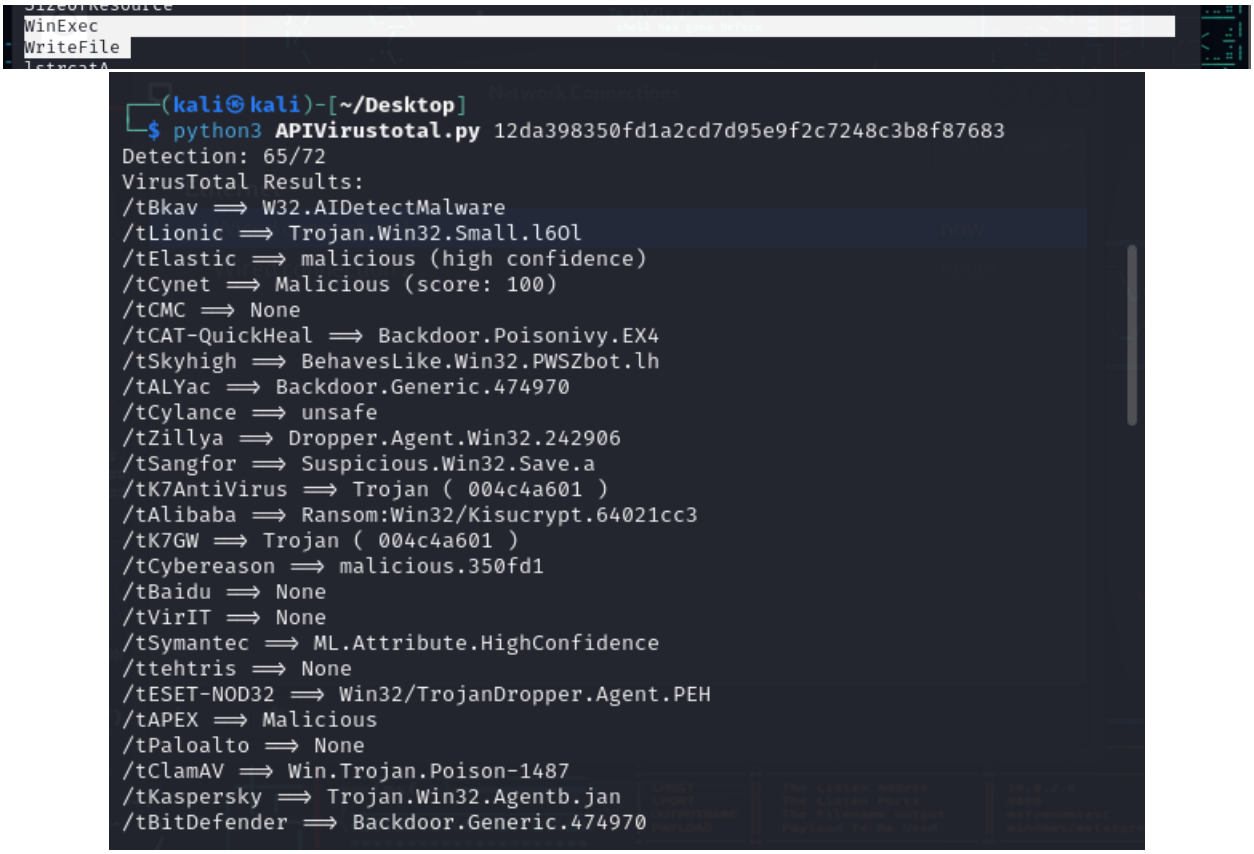
Họ Và Tên: Trần Hân Nhi
MSSV: 2011770131
Lớp: 20DATA1

Báo Cáo Tuần 2

- Thực hiện phân tích tĩnh để kiểm tra mẫu mã độc, dùng md5sum xác định giá trị hàm băm của file sales.bin

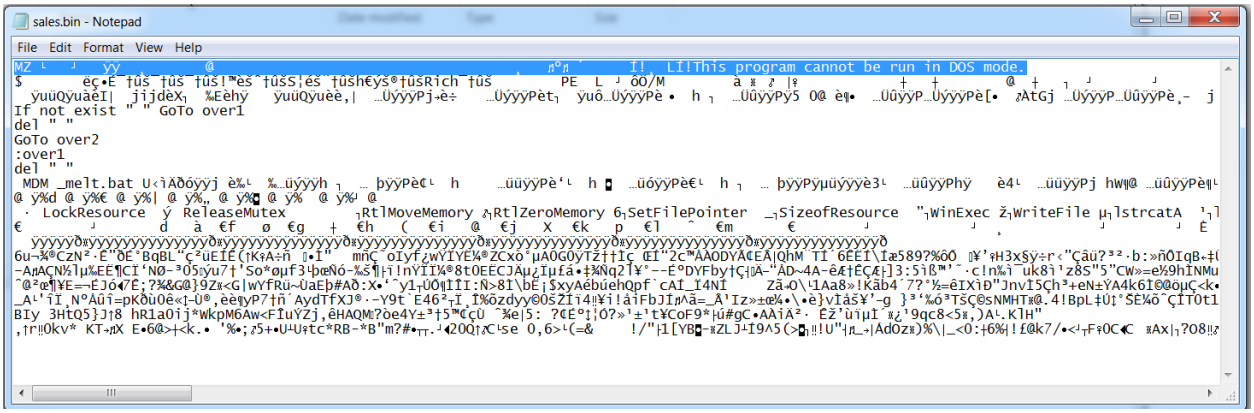


- Dùng strings kiểm tra

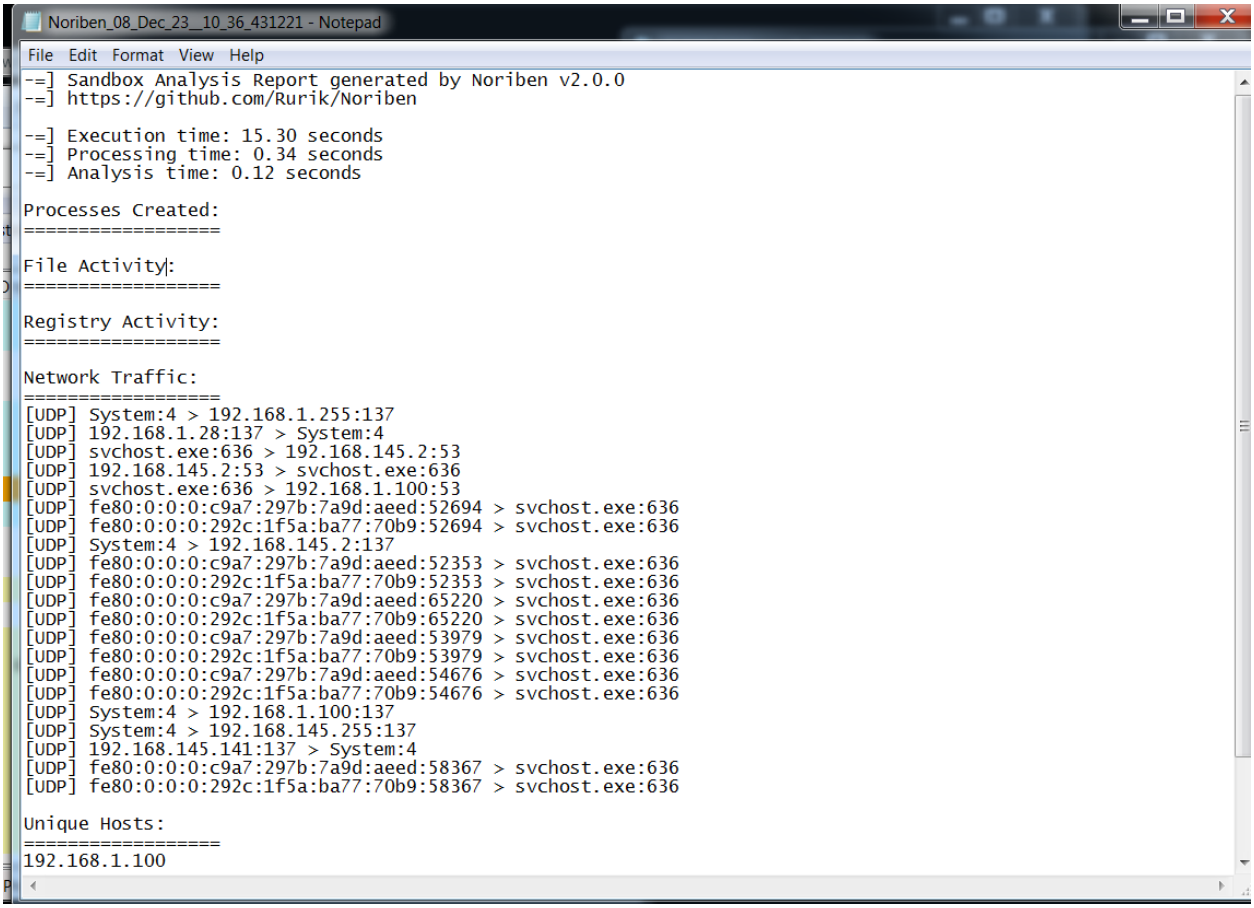


- Dùng inetsim mô phỏng port đánh lạc hướng mã độc.

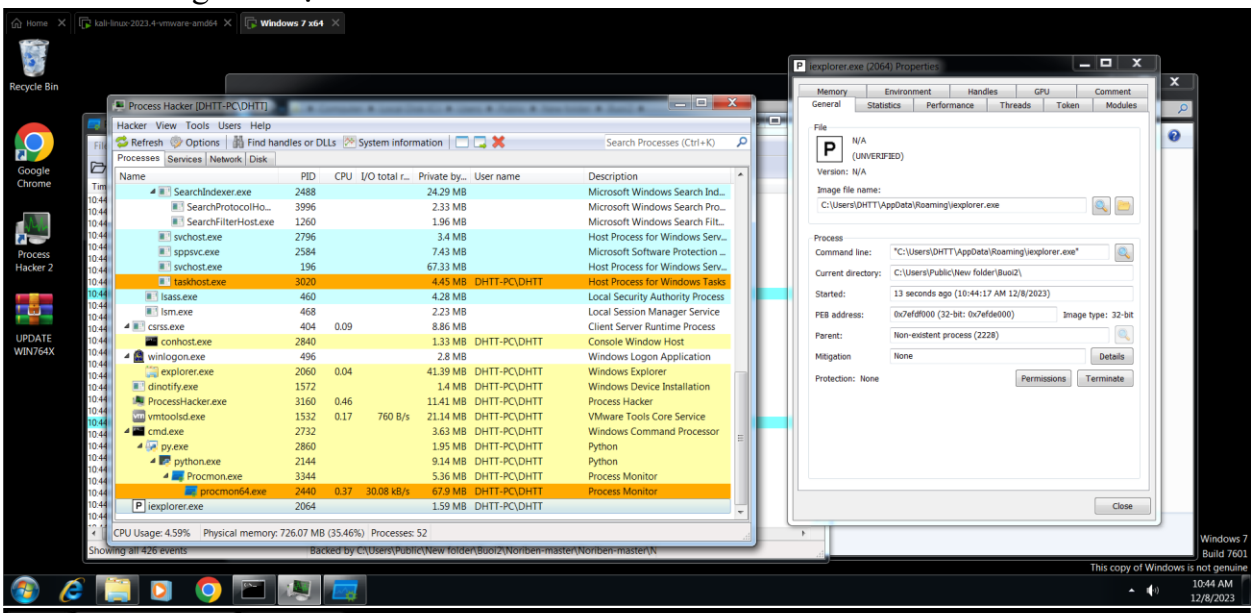
- Xác định tệp thực thi bằng notepad. File hiện dòng MZ, ta xác định được đây là tệp thực thi EXE PE.

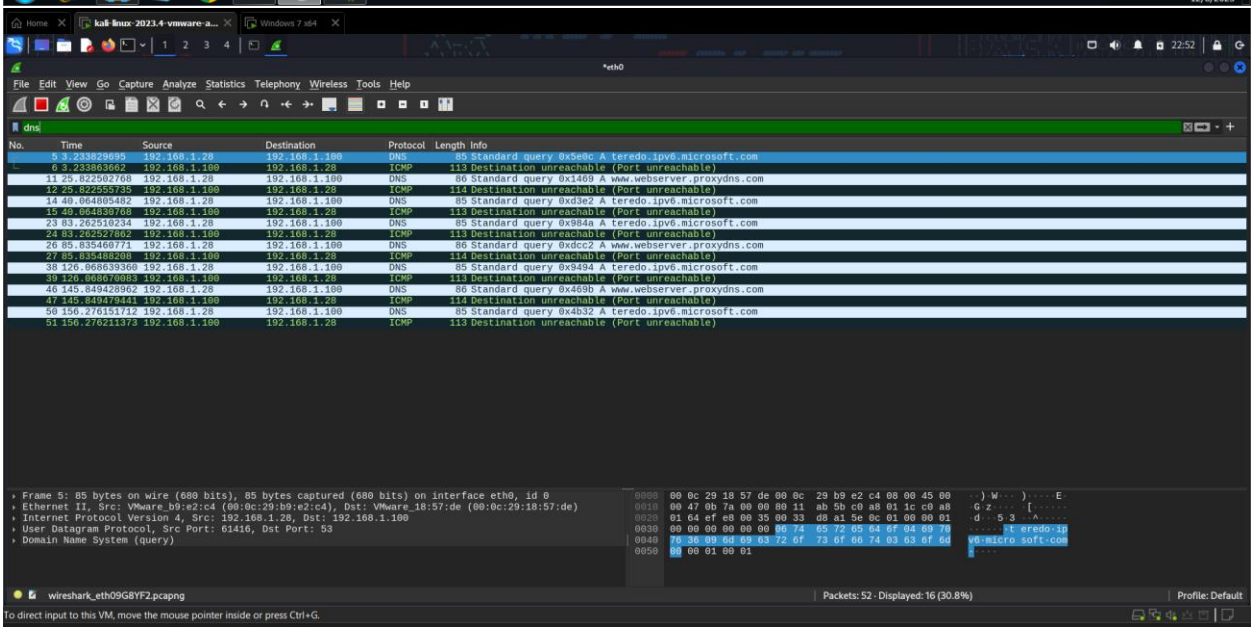


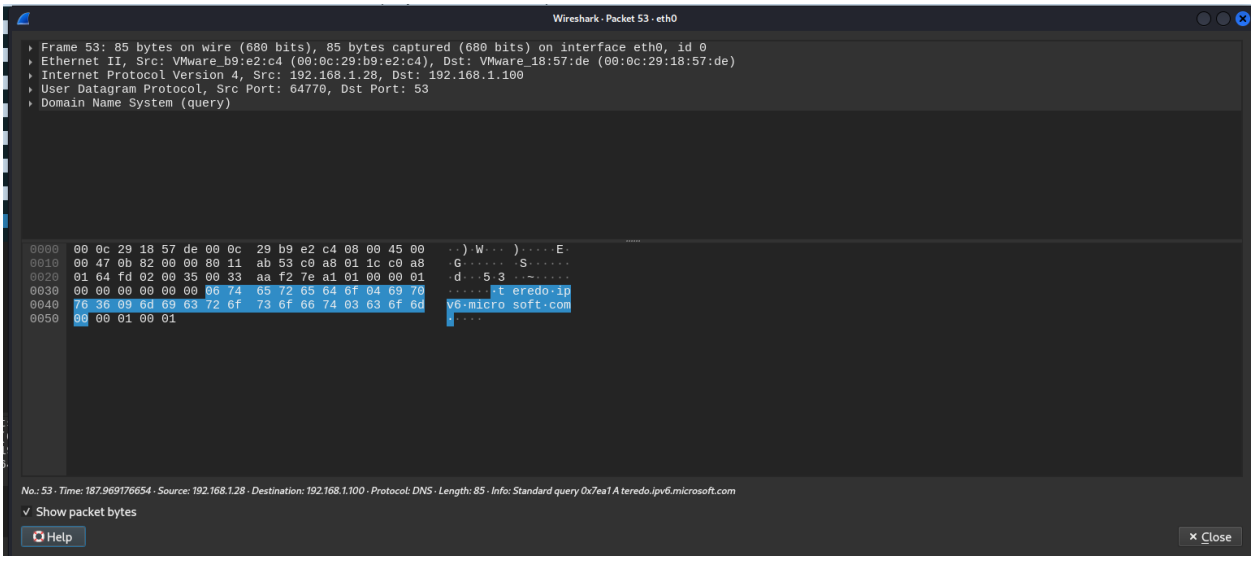
- Chạy Noriben khởi động Process Monitor. Khi hoàn tất giám sát, lưu kết quả vào một tệp văn bản (.txt) và tệp CSV (.csv) trong cùng thư mục.



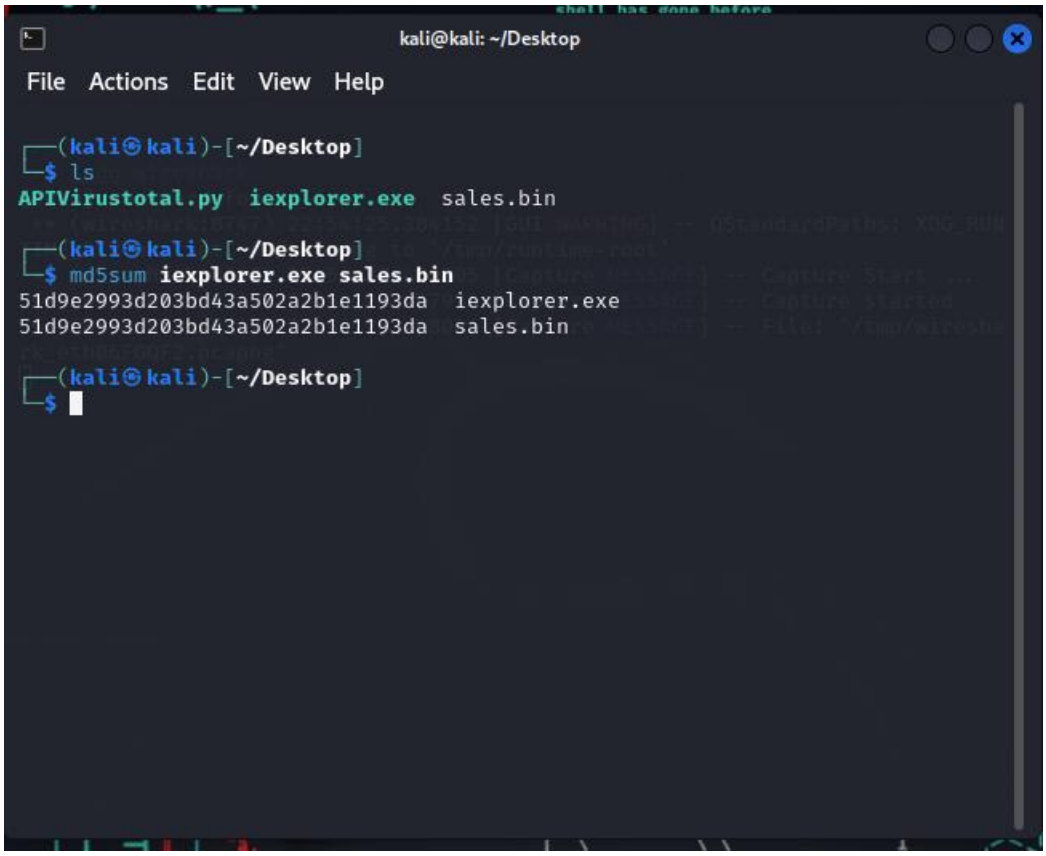
- Khi thực thi file mã độc, Process Hacker hiện 1 tiến trình lạ. Ta tiến hành kiểm tra thông tin của chương trình lạ.



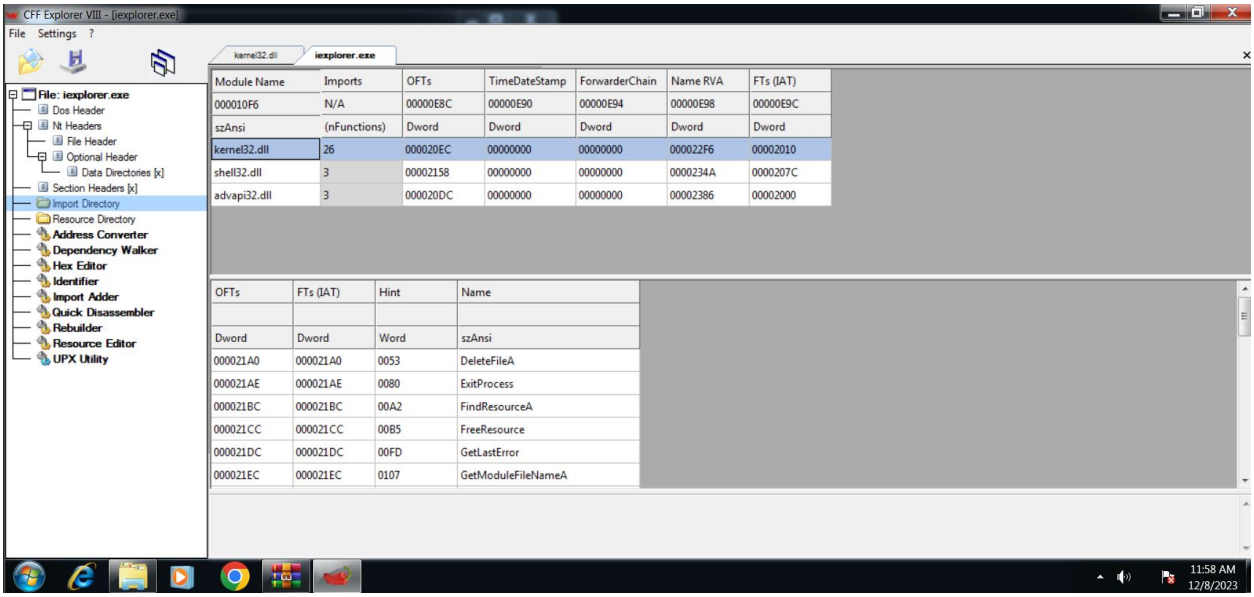




- So sánh giá trị băm md5 của file mã độc và tiến trình lạ.



- File iexplorer.exe không cần triển khai chức năng xoá file trong mã nguồn. Nó chỉ cần nhập và gọi hàm DeleteFile.


CFF Explorer VIII - [iexplorer.exe]
File Settings ?
kernel32.dll
iexplorer.exe
File: iexplorer.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT)
000010F6 | N/A | 00000E8C | 00000E90 | 00000E94 | 00000E98 | 00000E9C
szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword
kernel32.dll | 26 | 000020EC | 00000000 | 00000000 | 000022F6 | 00002010
shell32.dll | 3 | 00002158 | 00000000 | 00000000 | 0000234A | 0000207C
advapi32.dll | 3 | 000020DC | 00000000 | 00000000 | 00002386 | 00002000
OFTs | FTs (IAT) | Hint | Name
Dword | Dword | Word | szAnsi
000021A0 | 000021A0 | 0053 | DeleteFileA
000021AE | 000021AE | 0080 | ExitProcess
000021BC | 000021BC | 00A2 | FindResourceA
000021CC | 000021CC | 00B5 | FreeResource
000021DC | 000021DC | 00FD | GetLastError
000021EC | 000021EC | 0107 | GetModuleFileNameA
11:58 AM
12/8/2023