



# 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

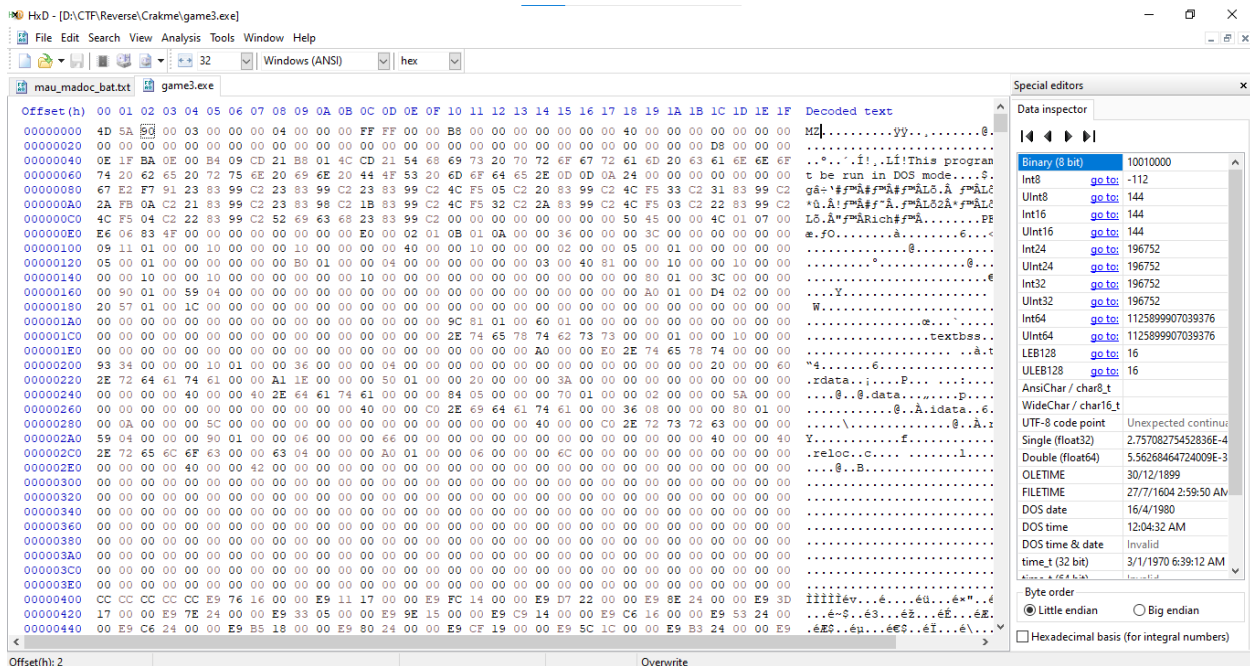
MSSV: 2011770131

Lớp: 20DATA1

## Báo Cáo Tuần 1

### Câu 1: Xác định loại tệp

- Sử dụng phương pháp thủ công xem bằng HxD. Kiểm tra từng byte của tệp



- Sử dụng lệnh xxd trên linux

```
root@localhost:~/Desktop
File Edit View Terminal Tabs Help

[root@localhost Desktop]# xxd -g 1 crackme-121-2.exe |more
00000000: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
00000010: b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00  .....
00000040: 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68  .....!..L.!Th
00000050: 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f  is program canno
00000060: 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20  t be run in DOS
00000070: 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00  mode....$.
00000080: 67 e2 f7 91 23 83 99 c2 23 83 99 c2 23 83 99 c2  g...#...#...#...
00000090: 4c f5 05 c2 20 83 99 c2 4c f5 33 c2 31 83 99 c2  L... ..L.3.1...
000000a0: 2a fb 0a c2 21 83 99 c2 23 83 98 c2 1b 83 99 c2  *...!...#.....
000000b0: 4c f5 32 c2 2a 83 99 c2 4c f5 03 c2 22 83 99 c2  L.2.*...L..."...
000000c0: 4c f5 04 c2 22 83 99 c2 52 69 63 68 23 83 99 c2  L..."...Rich#...
000000d0: 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00  .....PE..L...
000000e0: 71 00 83 4f 00 00 00 00 00 00 00 00 e0 00 02 01  q..0.....
000000f0: 0b 01 0a 00 00 36 00 00 00 3c 00 00 00 00 00 00  ....6...<.....
00000100: 09 11 01 00 00 10 00 00 00 10 00 00 00 00 40 00  .....@.
00000110: 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00  .....
00000120: 05 00 01 00 00 00 00 00 00 b0 01 00 00 04 00 00  .....
00000130: 00 00 00 00 03 00 40 81 00 00 10 00 00 10 00 00  .....@.....
00000140: 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00  .....
00000150: 00 00 00 00 00 00 00 00 80 01 00 3c 00 00 00 00  .....<...
```

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

```
root@localhost:~/Desktop
File Edit View Terminal Tabs Help

[root@localhost Desktop]# file crackme-121-2.exe
crackme-121-2.exe: PE32 executable for MS Windows (console) Intel 80386 32-bit
[root@localhost Desktop]#
```

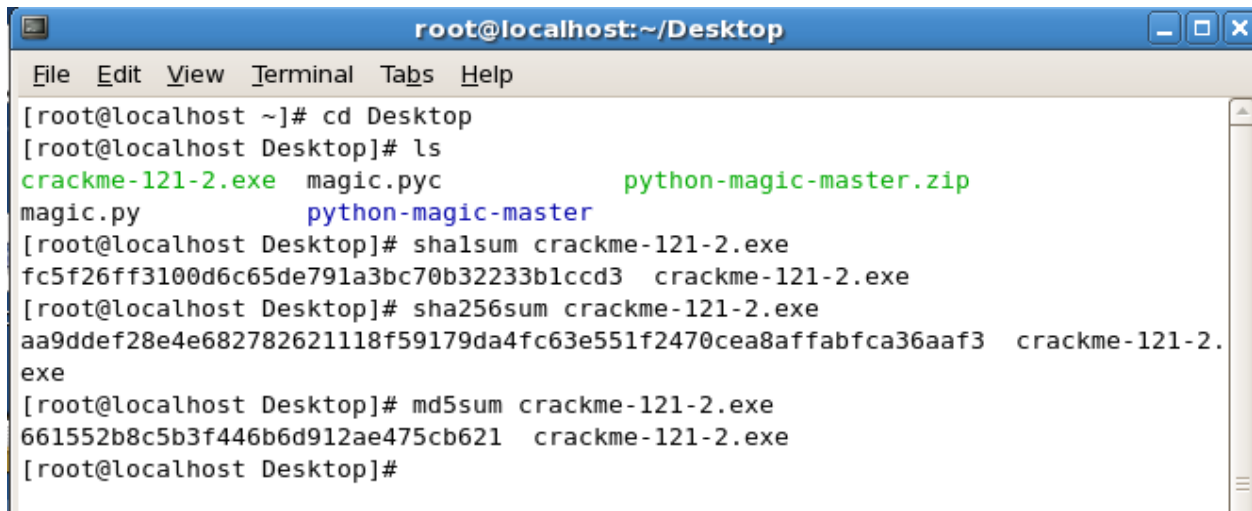
- Xác định bằng module python-magic

```
Administrator: C:\Windows\system32\cmd.exe - python
Microsoft Windows [Version 10.0.19044.2486]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>python
Python 3.12.0 (tags/v3.12.0:0fb18b0, Oct 2 2023, 13:03:39) [MSC v.1935 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import magic
>>> m = magic.Magic()
>>> ftype = m.from_file('D:/crackme-121-2.exe')
>>> print(ftype)
PE32 executable (console) Intel 80386, for MS Windows
>>>
```

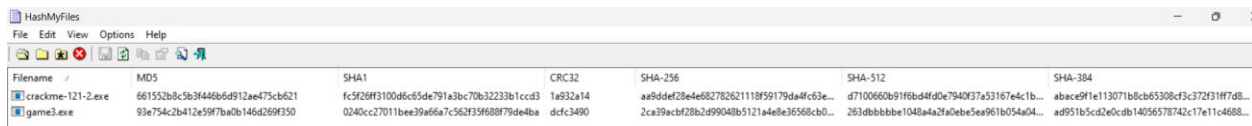
## Câu 2: Nhận dạng thông qua hàm băm

- Dùng lệnh tạo giá trị băm trên linux



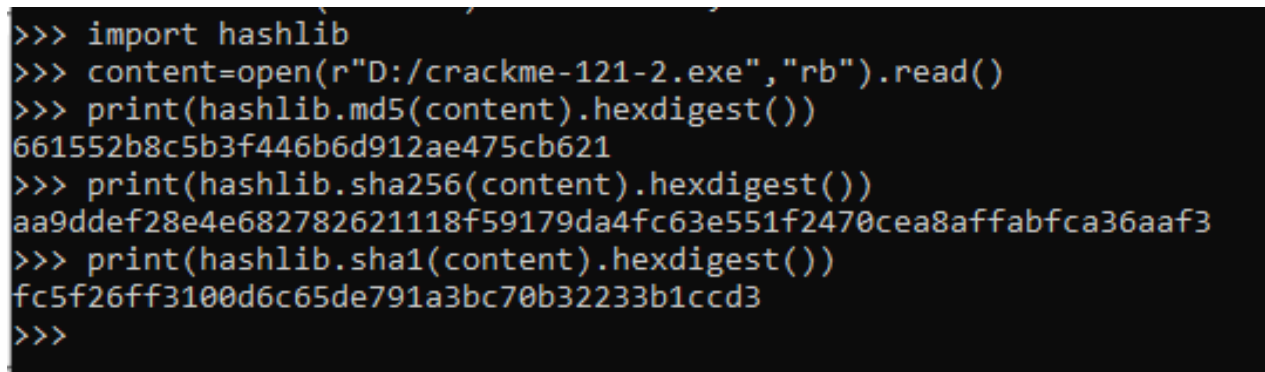
```
root@localhost: ~/Desktop
File Edit View Terminal Tabs Help
[root@localhost ~]# cd Desktop
[root@localhost Desktop]# ls
crackme-121-2.exe  magic.pyc  python-magic-master.zip
magic.py          python-magic-master
[root@localhost Desktop]# shasum crackme-121-2.exe
fc5f26ff3100d6c65de791a3bc70b32233b1ccd3  crackme-121-2.exe
[root@localhost Desktop]# sha256sum crackme-121-2.exe
aa9ddef28e4e682782621118f59179da4fc63e551f2470cea8affabfca36aaf3  crackme-121-2.exe
[root@localhost Desktop]# md5sum crackme-121-2.exe
661552b8c5b3f446b6d912ae475cb621  crackme-121-2.exe
[root@localhost Desktop]#
```

- Dùng HashMyFiles trên Window



Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384
crackme-121-2.exe	661552b8c5b3f446b6d912ae475cb621	fc5f26ff3100d6c65de791a3bc70b32233b1ccd3	1a932a14	aa9ddef28e4e682782621118f59179da4fc63e...	d7100660b91f6bd4fd0e7940f3a53167e4c1b...	abace9f1e113071b8cb65308cf3c372f31f7d8...
game3.exe	93e754c2b412e59f7ba0b146d269f350	0240cc27011bee39a66a7c562f35f68879de4ba	dffc3490	2ca39acf28b2d99048b5121a4e8e36568cb0...	263dbbbbbe1048a4a2fa0be5ea961b054a04...	ad951b5cd2e0db14056578742c17e11c4688...

- Xác định giá trị băm bằng python với module hashlib



```
>>> import hashlib
>>> content=open(r"D:/crackme-121-2.exe","rb").read()
>>> print(hashlib.md5(content).hexdigest())
661552b8c5b3f446b6d912ae475cb621
>>> print(hashlib.sha256(content).hexdigest())
aa9ddef28e4e682782621118f59179da4fc63e551f2470cea8affabfca36aaf3
>>> print(hashlib.sha1(content).hexdigest())
fc5f26ff3100d6c65de791a3bc70b32233b1ccd3
>>>
```

## Câu 3 Phân tích tệp tin chứa Virus

VirusTotal - File - aa9ddf28e4e682782621118f59179da4fc63e551f2470cea8affabfca36aaf3

1001 dòng lục 1m4h 20DATA1 - Google Tools CSG Code Luật Photo Linux Scapy AI Tĩnh điểm - Định Download Custom What is the best

aa9ddf28e4e682782621118f59179da4fc63e551f2470cea8affabfca36aaf3

3 / 68

3 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

aa9ddf28e4e682782621118f59179da4fc63e551f2470cea8affabfca36aaf3

crackme-121-2.exe

Size 28.50 KB Last Analysis Date 1 month ago

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security vendors' analysis

Do you want to automate checks?

Bkav Pro	W32.AI.DetectMalware	Jiangmin	VirTool.MS04-028.pe
Rising	Trojan.Generic@AI.97 (RDM.L:9U00HRKg...	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	CMC	Undetected
CrowdStrike Falcon	Undetected	Cybereason	Undetected
Cylance	Undetected	Cynet	Undetected

## Câu 4: Trích xuất chuỗi – Strings

```

root@localhost:~/Desktop
File Edit View Terminal Tabs Help
[root@localhost ~]# ls
anaconda-ks.cfg Desktop install.log install.log.syslog
[root@localhost ~]# cd Desktop
[root@localhost Desktop]# ls
crackme-121-2.exe magic.pyc python-magic-master.zip
magic.py python-magic-master
[root@localhost Desktop]# strings crackme-121-2.exe |grep 1
Usage: crackme-123-2 password
\\vmware-host\Shared Folders\Documents\121file\crackme-121-2\Debug\crackme-121-2
.pdb
MSVCR100D.dll
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
9#919;9C909W9m9s9y9
1D1c1
014181<1@1

```

```
[root@localhost Desktop]# strings -a crackme-121-2.exe |grep -i 'key'
RegCloseKey
RegOpenKeyExW
[root@localhost Desktop]# strings -a crackme-121-2.exe |grep -i 'password'
You found the password! Congratulations!
Usage: crackme-123-2 password
```

```
[root@localhost Desktop]# strings -a -el crackme-121-2.exe
f:\dd\vctools\crt_bld\self_x86\crt\src\crtexe.c
__native_startup_state == __initialized
Run-Time Check Failure #%d - %s
Runtime Check Error.
Unable to display RTC Message.
user32.dll
_controlfp_s(((void *)0), 0x00010000, 0x00030000)
_setdefaultprecision
f:\dd\vctools\crt_bld\self_x86\crt\src\intel\fp8.c
MSPDB100.DLL
EnvironmentDirectory
SOFTWARE\Microsoft\VisualStudio\10.0\Setup\VS
ADVAPI32.DLL
```

## - Dùng Pestudio để phân tích

pestudio 9.55 - Malware Initial Assessment - www.winitor.com - [d:\ctf\reverse\crackme\game3.exe]

file settings about

	encoding (2)	size (bytes)	location	flag (6)	label (60)	group (9)	technique (7)	value (315)
indicators (virusotal > score)	ascii	19	.idata	-	import	synchronization	-	InterlockedExchange
footprints (count > 13) *	ascii	26	.idata	-	import	synchronization	-	InterlockedCompareExchange
virustotal (3/72)	ascii	11	.idata	-	-	registry	-	RegCloseKey
dos-header (size > 64 bytes)	ascii	15	.idata	-	-	registry	T1012   Query Registry	RegQueryValueEx
rich-header (tooling > Visual Studio)	ascii	12	.idata	-	-	registry	-	RegOpenKeyEx
file-header (executable > 32-bit)	ascii	17	.idata	-	import	reconnaissance	T1082   System Information Discovery	IsDebuggerPresent
optional-header (subsystem > console)	ascii	23	.idata	-	import	reconnaissance	-	QueryPerformanceCounter
directories (stamp > Apr.2012)	ascii	12	.idata	-	import	reconnaissance	T1124   System Time Discovery	GetTickCount
sections (characteristics > self-modifying)	ascii	19	.idata	x	import	reconnaissance	T1057   Process Discovery	GetCurrentProcessId
libraries (count > 2) *	ascii	18	.idata	-	import	memory	-	HeapSetInformation
imports (flag > 56) *	ascii	8	.idata	-	import	memory	-	HeapFree
exports (n/a)	ascii	9	.idata	-	import	memory	-	HeapAlloc
thread-local-storage (n/a)	ascii	14	.idata	-	import	memory	-	GetProcessHeap
.NET (n/a)	ascii	12	.idata	-	import	memory	T1055   Process Injection	VirtualQuery
resources (signature > manifest)	ascii	23	.idata	-	import	file	T1124   System Time Discovery	GetSystemTimeAsFileTime
strings (count > 315)	ascii	18	.idata	x	import	execution	T1057   Process Discovery	GetCurrentThreadId
debug (stamp > Apr.2012)	ascii	16	.idata	x	import	execution	-	TerminateProcess
manifest (level > asInvoker)	ascii	17	.idata	x	import	execution	T1057   Process Discovery	GetCurrentProcess
version (n/a)	ascii	5	.idata	-	-	exception	T1497   Sandbox Evasion	Sleep
certificate (n/a)	ascii	14	.idata	x	import	exception	-	RaiseException
overlay (n/a)	ascii	27	.idata	-	import	exception	-	SetUnhandledExceptionFilter
	ascii	24	.idata	-	import	exception	-	UnhandledExceptionFilter
	ascii	14	.idata	-	import	dynamic-library	-	GetProcAddress
	ascii	11	.idata	-	import	dynamic-library	T1106   Execution through API	LoadLibrary
	ascii	17	.idata	-	import	dynamic-library	-	GetModuleFileName
	ascii	11	.idata	-	import	dynamic-library	-	FreeLibrary
	ascii	16	.idata	x	-	diagnostic	-	PDBOpenValidate5
	ascii	17	.idata	-	rtti	-	-	?terminate@@YAXXZ
	unicode	45	.idata	-	registry	-	-	SOFTWARE\Microsoft\Visu
	ascii	13	.idata	-	import	-	-	_CRT_RTC_INIT
	ascii	19	.idata	-	import	-	-	_configthreadlocale

sha256: 2CA39ACBF282D99048B5121A4E8E3656CB022182B15F4604DF1C4E076E8BD    cou: 32-bit    file-type: executable    subsystem: console    entry-point: 0x0001109

## Câu 5: Xác định tập tin nghi vấn làm rồi

```
[root@localhost Desktop]# strings spybot.ex_ | grep 20
HTTP/1.0 200 OK
2000
Norton_Anti-Virus_2002_Crack.exe
209.126.201.22
209.126.201.20
```

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

```
kali@kali: ~/Documents/abc
(kali@kali)~[~/Documents/abc]
$ upx -o game3_packed.exe game3.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96      Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

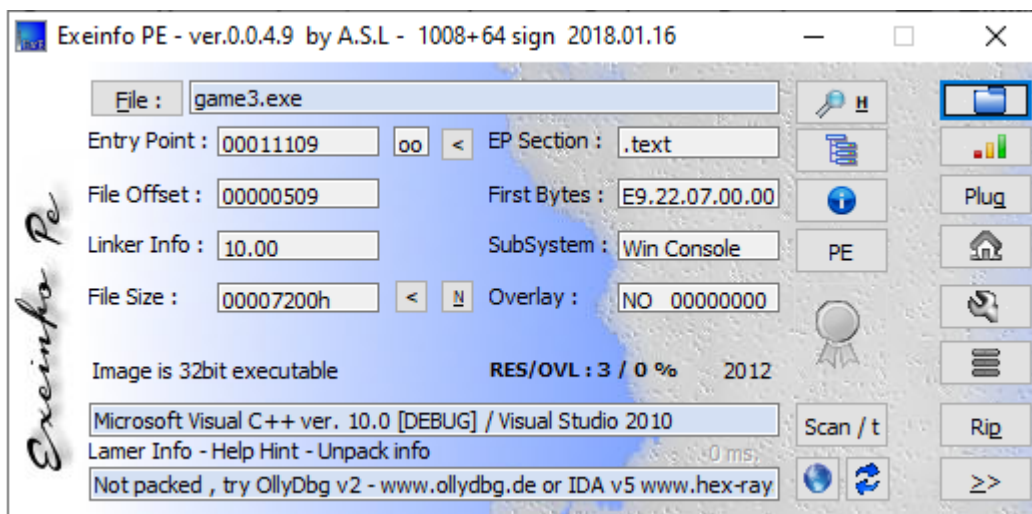
File size      Ratio      Format      Name
-----
29184 -> 10240 35.09% win32/pe  game3_packed.exe

Packed 1 file.

(kali@kali)~[~/Documents/abc]
$ strings game3_packed.exe | grep 20
me-121-2.exe
game3.exe
game3

(kali@kali)~[~/Documents/abc]
$
```

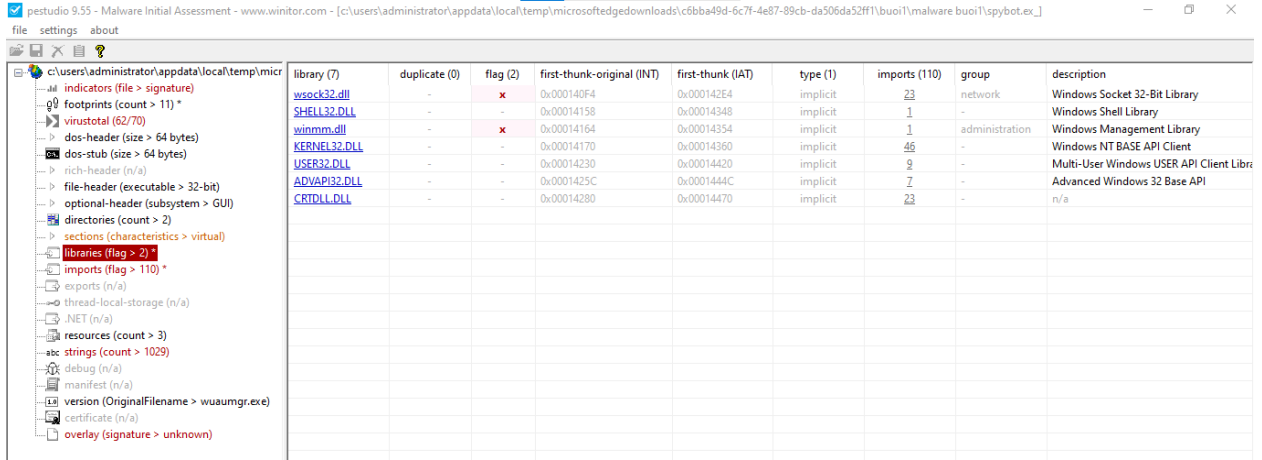
- Phát hiện bằng exeinfo PE. Có thể xác định được phần mềm ném vào exeinfo PE nén bằng .text



## Câu 6: Kiểm tra phần đầu PE



- Dùng pestudio kiểm tra libraries



- Dùng pestudio kiểm tra imports

