

Họ và tên: Trần Trí Dũng

MSSV: HE190680

Lớp: IA1901

Lab 6:

Upload VirusTotal:

The screenshot shows the VirusTotal web interface within a Windows 10 VM. The file being analyzed is 'wildfire-test-pe-file.exe' (54.00 KB, last analyzed 1 minute ago). It has a Community Score of 40/71 and is flagged as malicious by 40/71 security vendors. The file is categorized as a 'trojan' and 'pua' (potentially unwanted application). The 'Security vendors' analysis' section shows a table of detections from various vendors.

Vendor	Detection
AliCloud	Trojan:Win/Agent.gyf
Antiy-AVL	Trojan:Script.Phonyzy
Arctic Wolf	Unsafe
Avira (no cloud)	SPR/PanCar.A
Bkav Pro	W32.AIDetect/Malware
ClamAV	Win.Dropper.Bebloh.9554185-0
Cynet	Malicious (score: 99)
DeepInSight	MALICIOUS
DrWeb	BackDoor.Bebloh.375
Elastic	Malicious (high confidence)
Fortinet	Riskware.WildFireTestFile
GData	Win32.Riskware.PanCar.A
Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Gen.vb1s1
Ikarus	Trojan.Win32.Agent
Jiangmin	Exploit.Multi.ar
K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)

Upload hybrid-analysis:

The screenshot shows the Hybrid Analysis website interface. The browser address bar displays the URL: <https://www.hybrid-analysis.com/sample/9662967f562592a6e2e1d0859c6b0d66885fd503233f34a6591cf85e8a93e775e>. The page title is "Free Automated Malware Analysis". The navigation bar includes links for "Sandbox", "Quick Scans", "File Collections", "Resources", and "Request Info".

Analysis Overview

Submission name: wildfire-test-pe-file.exe
Size: 54KiB
Type: [exe](#) [executable](#)
Mime: application/vnd.microsoft.portable-executable
SHA256: 9662967f562592a6e2e1d0859c6b0d66885fd503233f34a6591cf85e8a93e775e
Submitted At: 2025-06-03 02:02:15 (UTC)
Last Anti-Virus Scan: 2025-06-03 02:02:15 (UTC)
Last Sandbox Report: 2025-06-03 02:02:14 (UTC)

malicious
AV Detection: 26%
Labeled As: Backdoor.Bebloh
Community Score: 0

Anti-Virus Results

CrowdStrike Falcon
Static Analysis and ML
Clean
No Additional Data

MetaDefender
Multi Scan Analysis
Malicious (19/25)
More Details

Falcon Sandbox Reports (1)

Windows 10 64 bit

CrackMe #5:

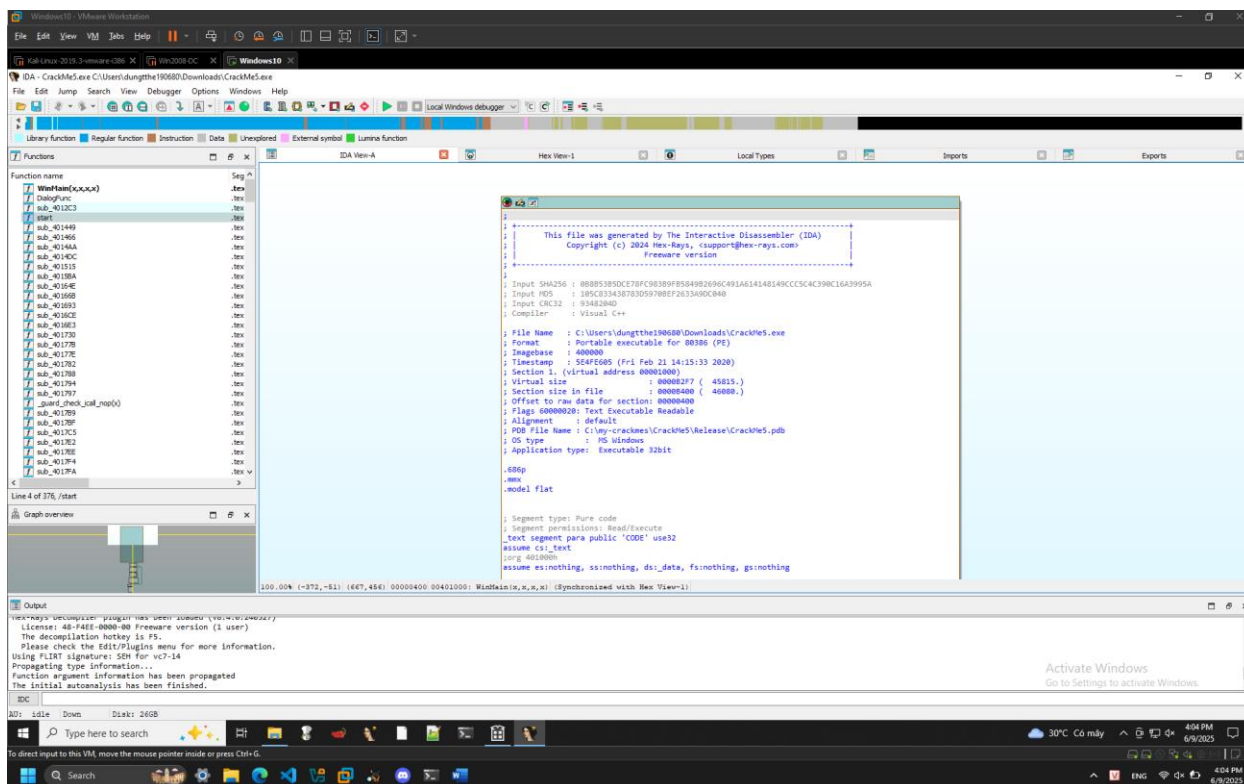
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “Wrong”:

The screenshot shows a Windows 10 desktop environment. The desktop background is a blue gradient with a stylized robot character. The taskbar at the bottom shows the Start button, search bar, and several application icons. The system tray on the right shows the date and time as 4:26 PM on 6/9/2025.

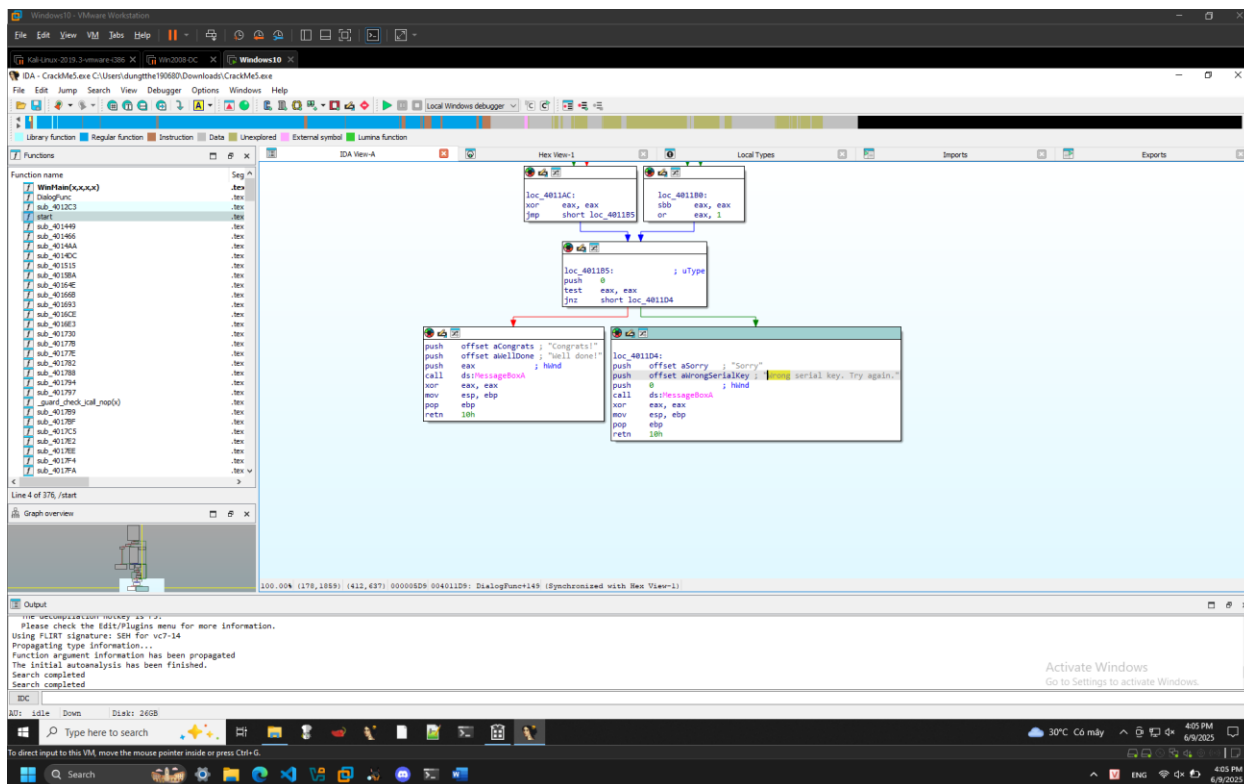
A window titled "CrackMe #3 by crackinglessons.com" is open in the center. It contains two input fields: "Enter filename:" with the text "dungh" and "Enter Serial Key:" with the text "abcd1234". Below these fields is a "Sorry" dialog box with the message "Wrong serial key. Try again." and an "OK" button.

The desktop also shows several icons: Recycle Bin, Microsoft Edge, PS_Trench..., ProDiscover Basic, Visual Studio Code, EBBB8888..., Boxstarter Shell, desktop.ini, config.xml, install.ps1, Tools, desktop.ini, and fakenet_logs.

Sau đó em mở phần mềm IDA và tiến hành dịch ngược file:

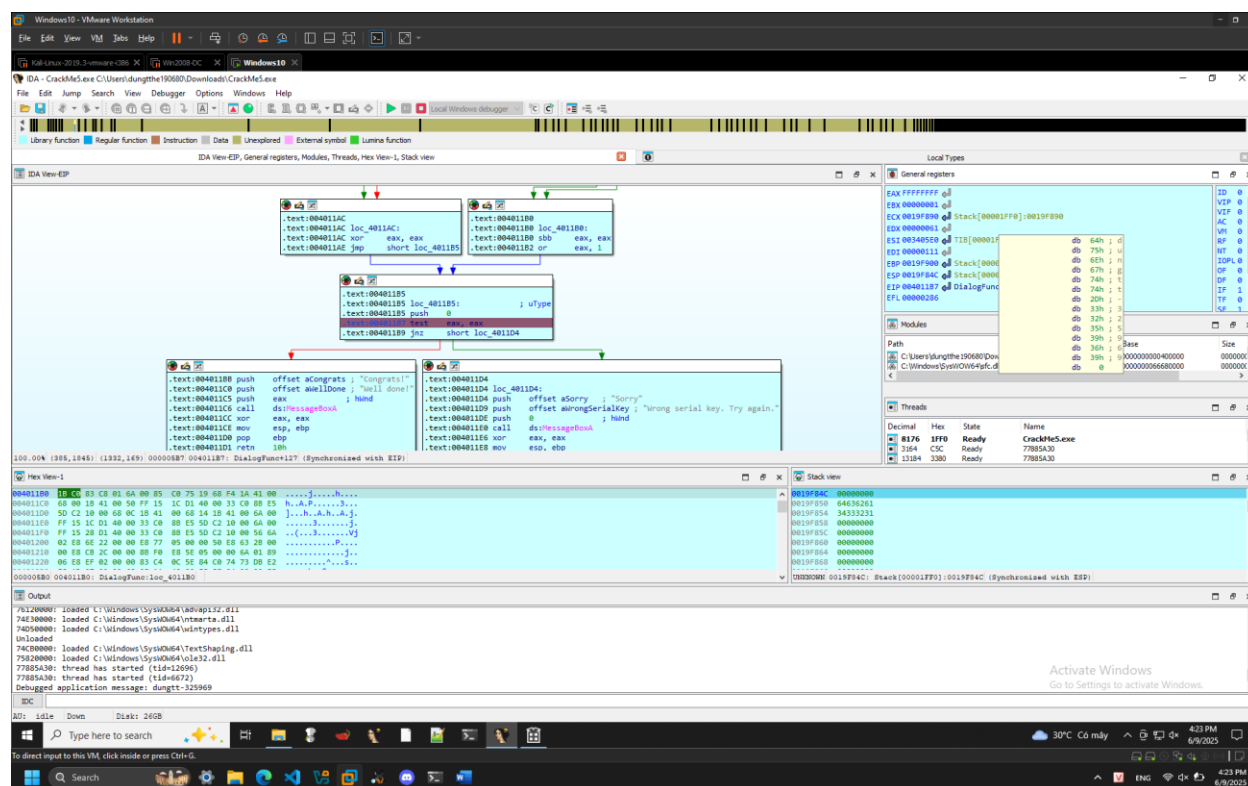


Em search từ khóa “Wrong” và được điều hướng đến đoạn code này:



[illegible]

Kiểm tra giá trị trong thanh ghi thì em tìm được mật khẩu chính xác của người dùng “dungtt”:



Em chạy lại chương trình, nhập mật khẩu vừa tìm được và nhận được thông báo báo chính xác:

