

# C.4 MATERIALE ȘI METODE ÎN INGINERIA ÎNVERSĂ (I)

PAUL A. GAGNIUC



Academia Tehnică Militară „Ferdinand I”

# **PRINCIPALELE PĂRȚI ALE PREZENTĂRII**

---

## **C.4 Materiale și metode în ingineria inversă:**

- **C.4.1 MEDIUL DE DETONARE**
- **C.4.2 INSTRUMENTELE DE INGINERIE INVERSĂ (I)**

# PACHETUL DE FIŞIERE PENTRU INSTRUMENTE

- kit\Gazda\VirtualBox.exe
- kit\Gazda\win7.iso
- kit\Gazda\IDA.zip
  
- kit\Gazda\PEstudioX86.zip
- kit\Gazda\Cutter.zip
- kit\Gazda\x64dbg.zip
- kit\Masina Virtuala\sysinternals.zip
- kit\Masina Virtuala\wireshark.zip
- kit\Masina Virtuala\procdot.zip
- kit\Masina Virtuala\pestudio.zip
- kit\Masina Virtuala\BCompare.exe

(Gazdă)

(Masina Virtuală)

C.4.1

# MEDIUL DE DETONARE

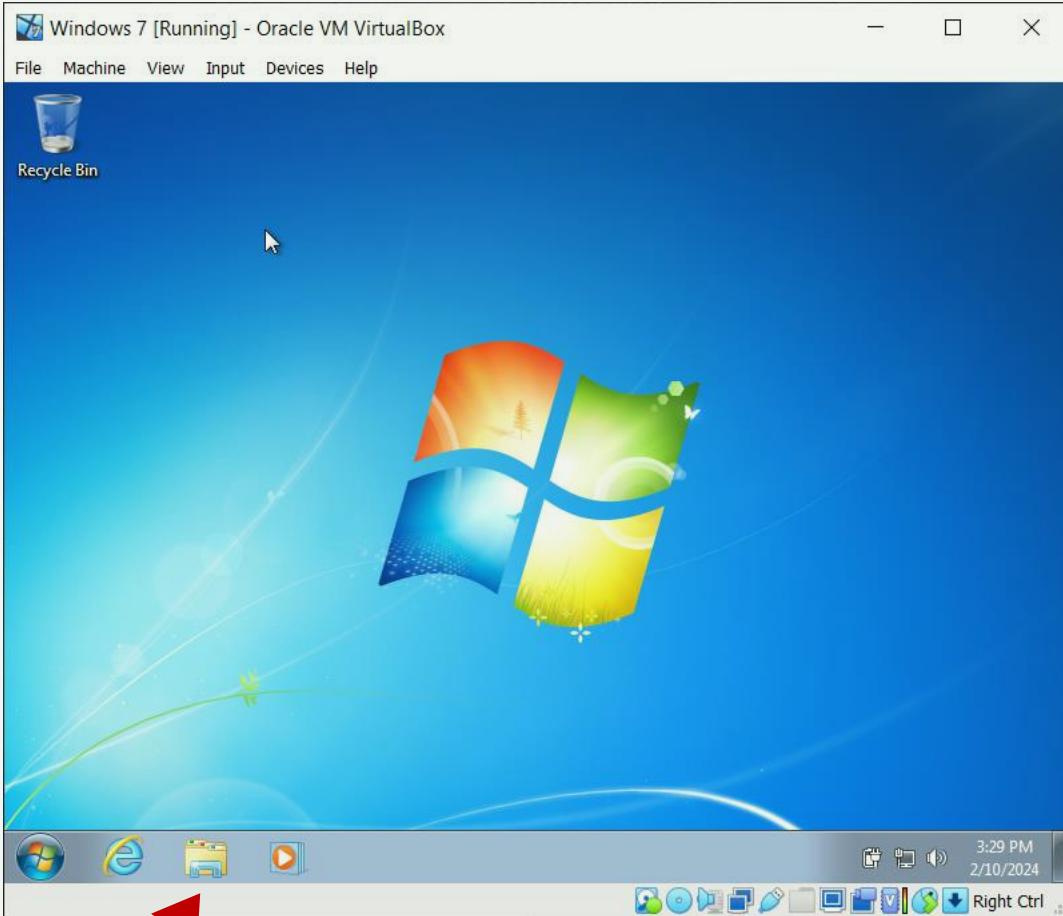


# Afișarea extensiilor și a fișierelor ascunse !

De ce Windows 7 pe mașina virtuală?

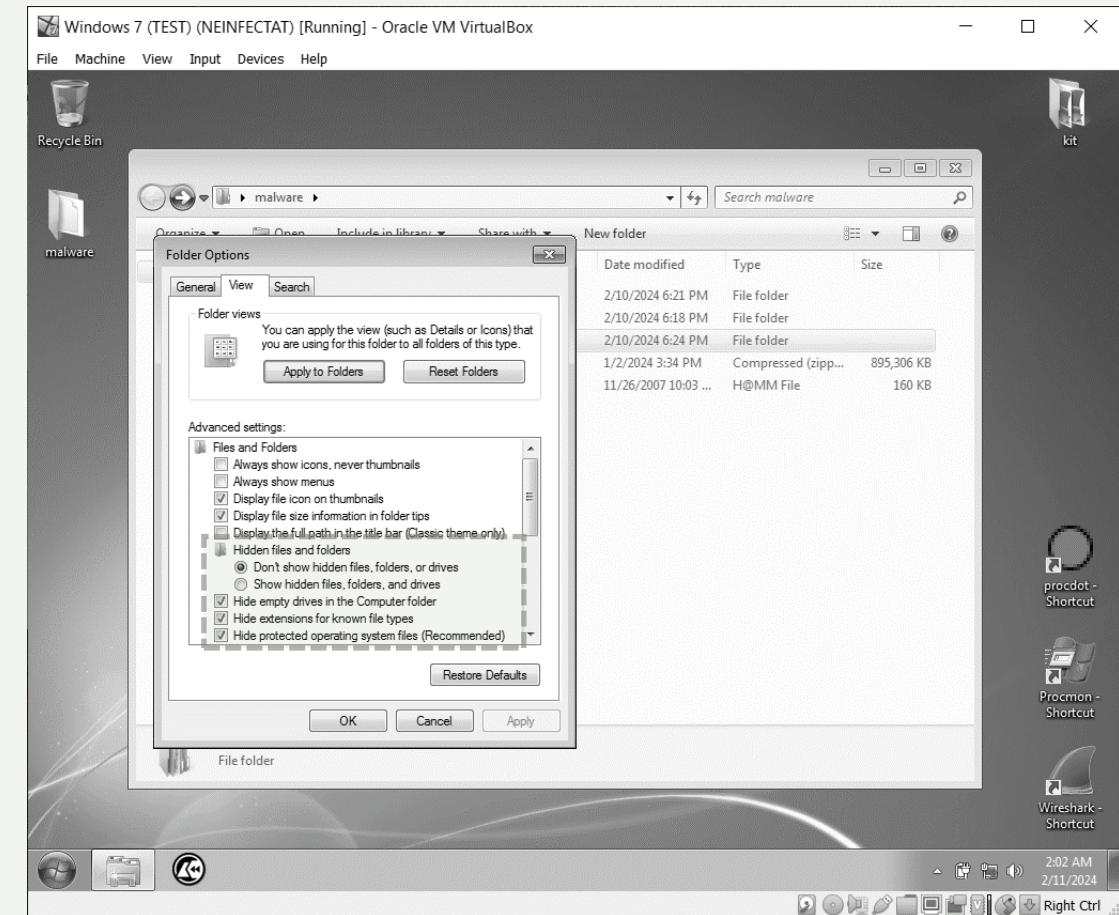
Windows 7 reprezintă echilibrul perfect între dimensiunea kit-ului de instalare și structura modernă a sistemului de operare (ex. Windows 11):

File explorer/Organize/Folder and search options:



1

Deselectare: *Hide OS files; Hide extensions*  
Selectare: *Show hidden files, folder, and drives*



# *Eliminarea zgomotului de fundal: Oprirea serviciilor*

Pentru a reduce activitatea în background („zgomotul”) pe o mașină virtuală cu Windows 7 (valabil și pentru versiunile moderne de Windows), astfel încât în monitorul de procese să fie vizibil doar programul pe care îl execuți, puteți dezactiva sau configura următoarele servicii și funcționalități:

- **Indexing Service (Indexare).** Dacă nu aveți nevoie de căutare rapidă prin fișiere, dezactivați acest serviciu pentru a reduce activitatea pe disc și procesor.
- **System Restore (Restaurare Sistem).** Deactivați restaurarea sistemului pentru a preveni crearea punctelor de restaurare în fundal.
- **Windows Update (Actualizări Windows).** Dezactivați actualizările automate Windows pentru a opri verificarea și instalarea actualizărilor în fundal.
- **Windows Defender (sau alte soluții antivirus).** Antivirusul poate efectua scanări periodice care pot interfera cu monitorizarea. Deactivați-l dacă mediu este controlat și sigur.
- **Windows Search (Căutare Windows).** Similar cu serviciul de indexare, acesta poate fi oprit pentru a reduce activitatea discului.
- **Remote Registry (Registrul la Distanță).** Oprește modificările la distanță ale registrului, care de obicei nu sunt necesare.
- **Print Spooler (Listă de așteptare pentru tipărire).** Dacă nu tipăriți de pe mașina virtuală, acest serviciu poate fi oprit.
- **Background Intelligent Transfer Service (BITS).** Oprește transferurile în fundal de date folosind lățimea de bandă neutilizată.
- **Superfetch.** Deși este proiectat să îmbunătățească performanța sistemului, poate fi dezactivat pentru a reduce utilizarea discului și a memoriei.
- **Diagnostic Tracking Service (Serviciul de Urmărire Diagnostic).** Dezactivați acest serviciu pentru a preveni colectarea datelor despre performanța sistemului.
- **Secondary Logon (Autentificare Secundară).** Permite rularea proceselor sub un alt utilizator și poate fi dezactivat dacă nu este necesar.
- **Event Log (Jurnal de Evenimente).** Dacă nu aveți nevoie de jurnale detaliate, puteți să opriți acest serviciu, deși este recomandat să fie lăsat activ pentru depanare și monitorizare de securitate.

# OPRIREA SERVICIILOR

PENTRU A DEZACTIVA ACESTE SERVICII, URMAȚI ACEȘTI PAȘI

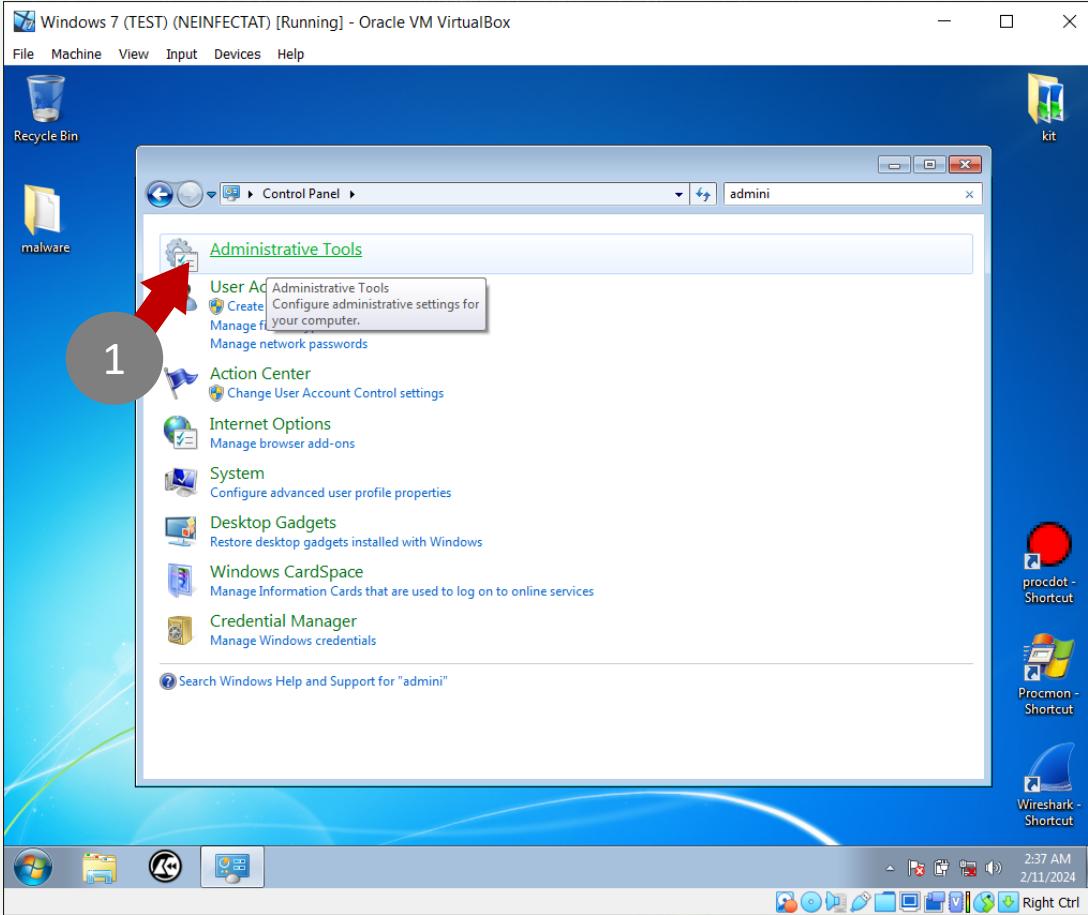
- Deschideți services.msc prin Start > Run/Căutare și introducând **services.msc**.
- Căutați serviciul pe care doriți să-l dezactivați.
- Faceți clic dreapta pe serviciu și selectați **Properties** (Proprietăți).
- În tabul **General**, schimbați **Startup type** (Tipul de pornire) în **Disabled** (Dezactivat).
- Faceți clic pe **Stop** (Oprire) pentru a opri serviciul imediat.
- Aplicați schimbările și închideți fereastra.

Rețineți că dezactivarea unor servicii esențiale poate afecta stabilitatea și funcționalitatea sistemului. Este întotdeauna o practică bună să creați un punct de restaurare înainte de a face astfel de schimbări, astfel încât să puteți reveni la o configurație anterioară dacă apare o problemă.

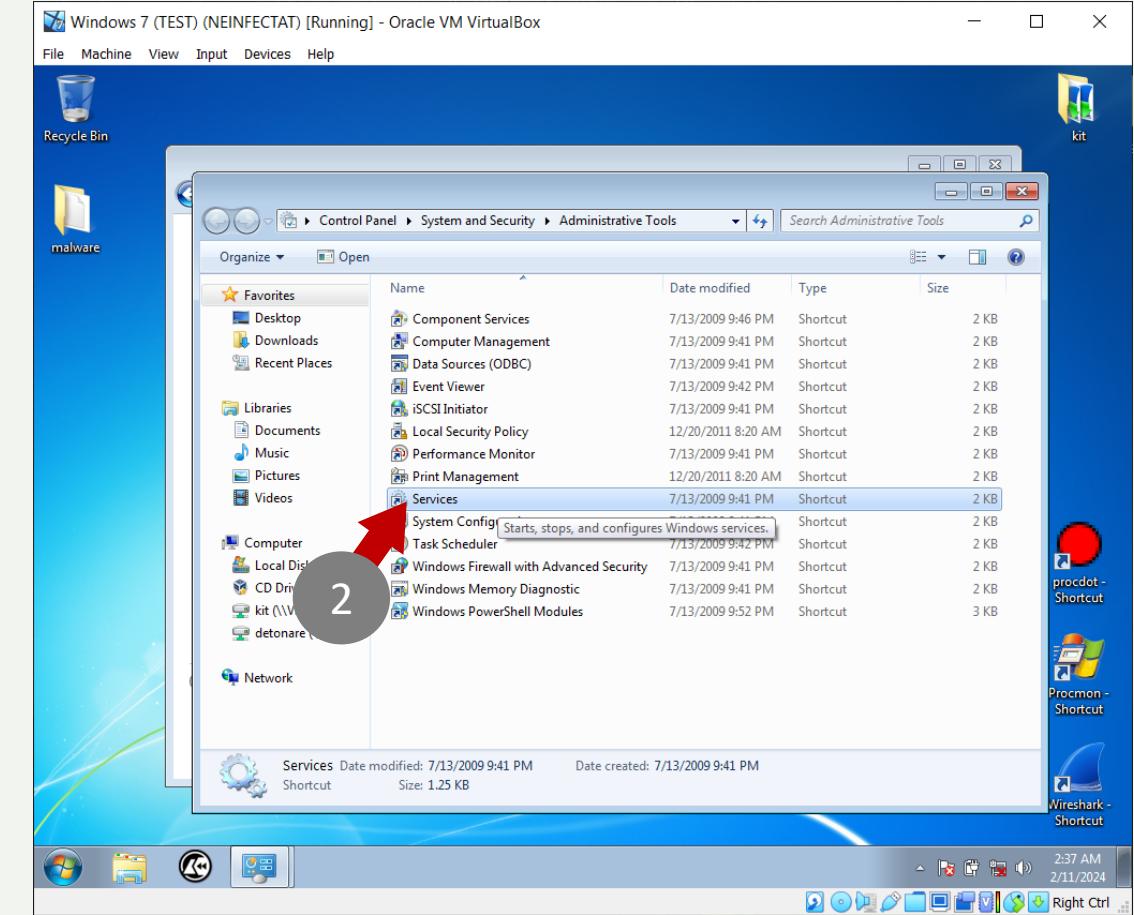
# Dezactivarea serviciilor (I)

- Utilizare: Administrative tools
- Selectați opțiunea: Services

## Administrative tools



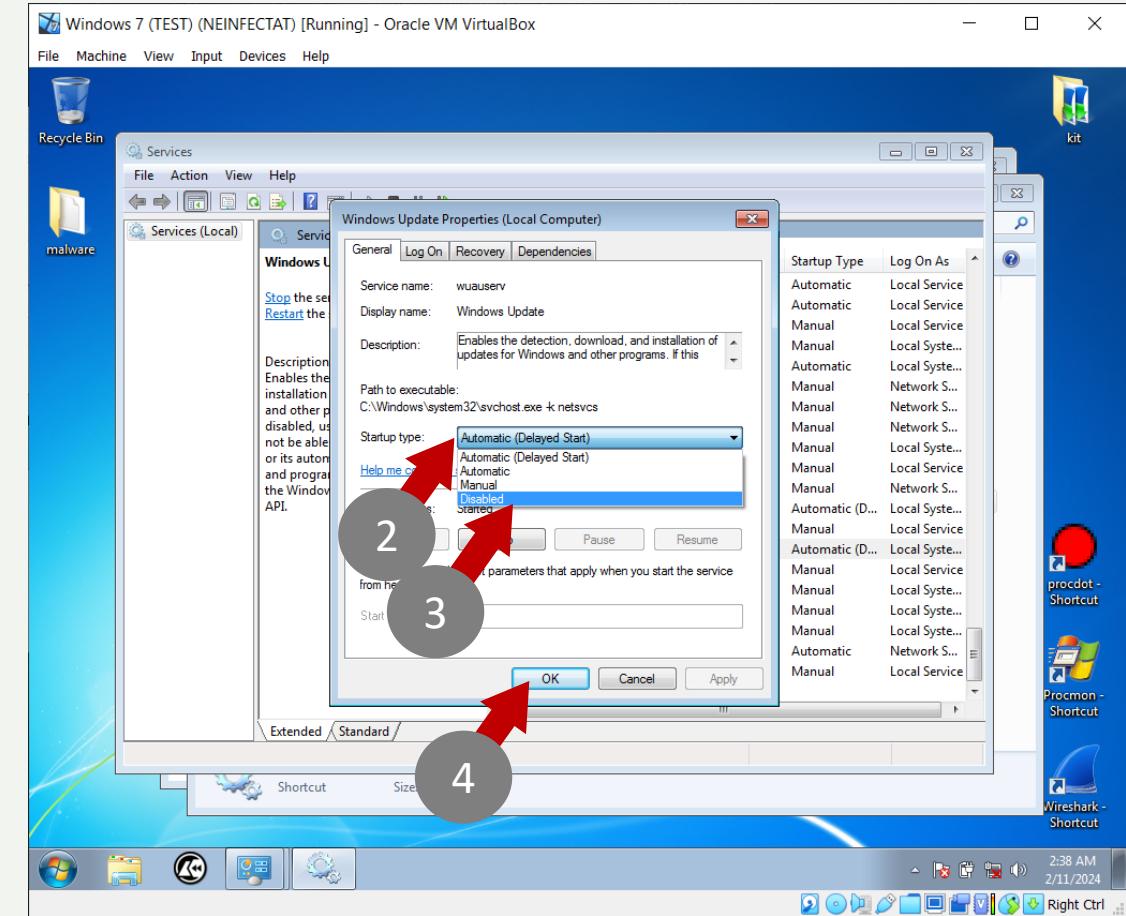
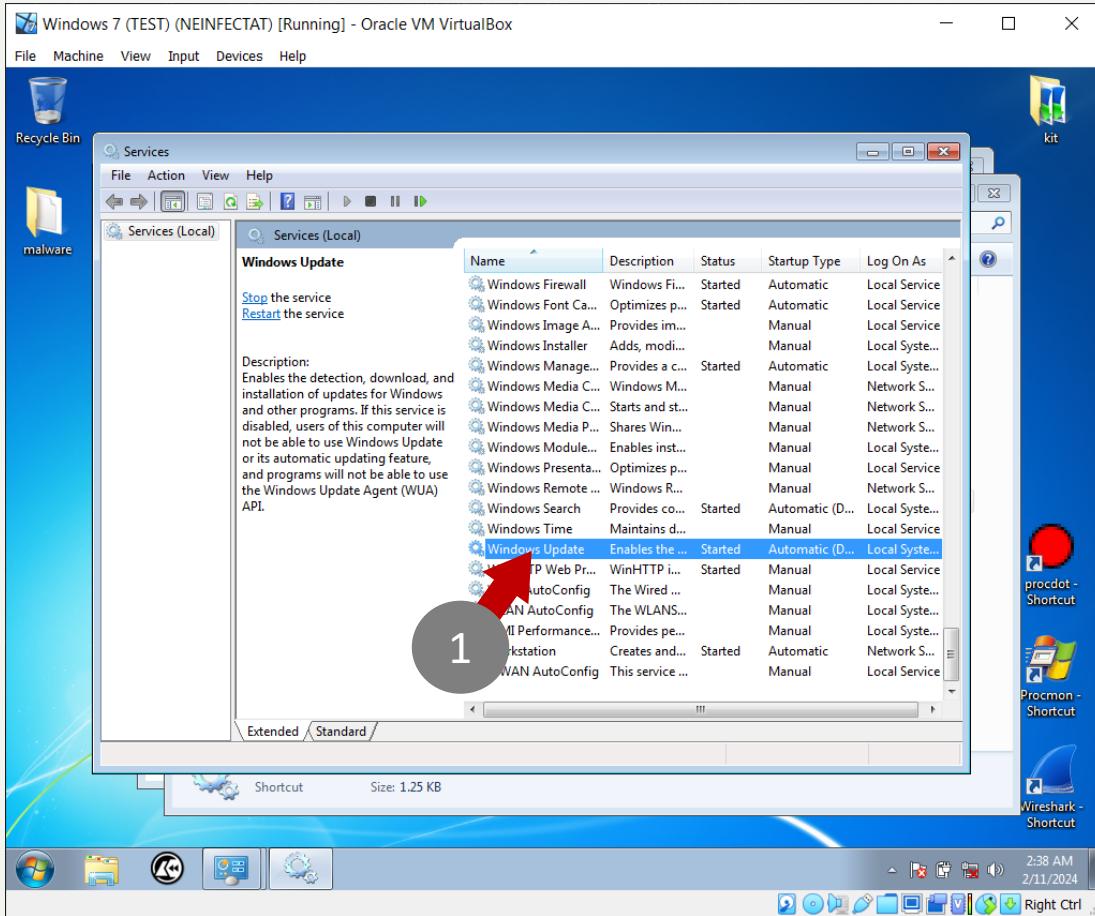
## Services



# Dezactivarea serviciilor (II)

- Selectare serviciu: Windows Update
- Oprire serviciu (Startup type: Disabled)

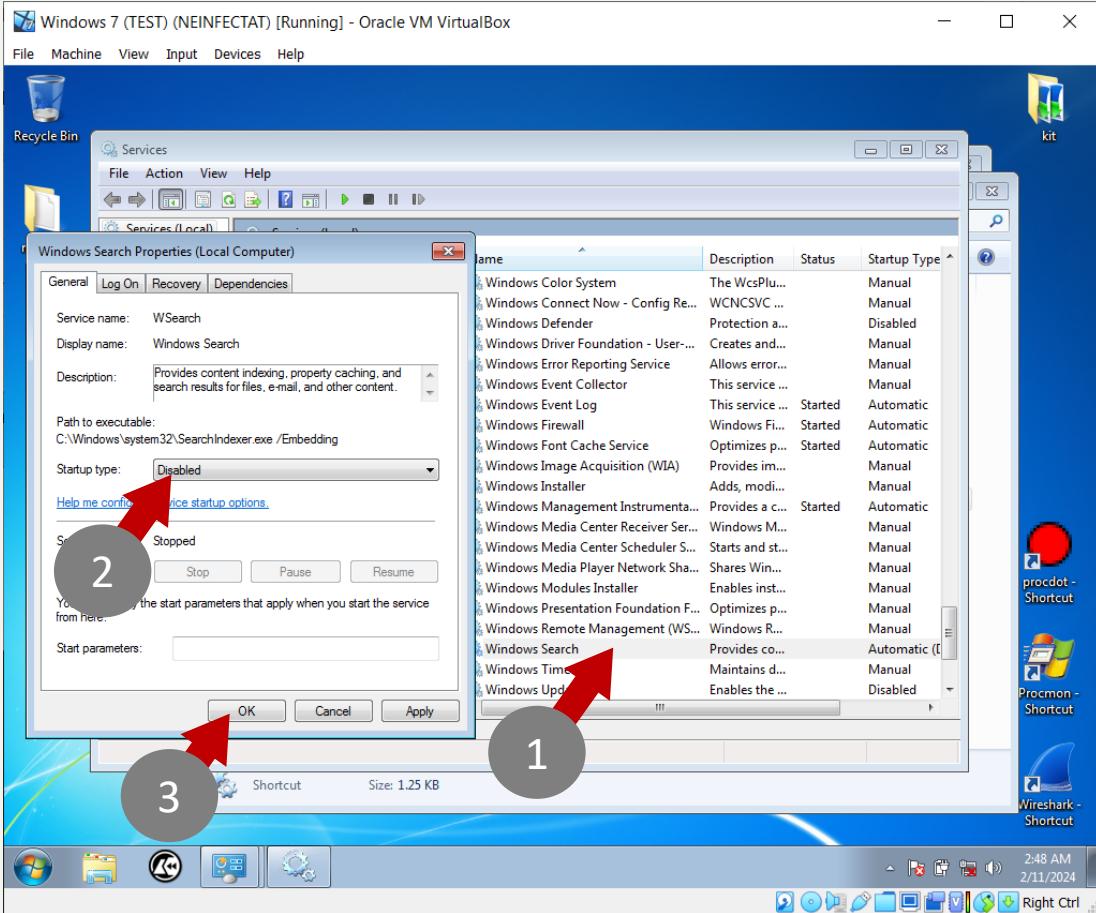
## Dezactivare: Windows Update



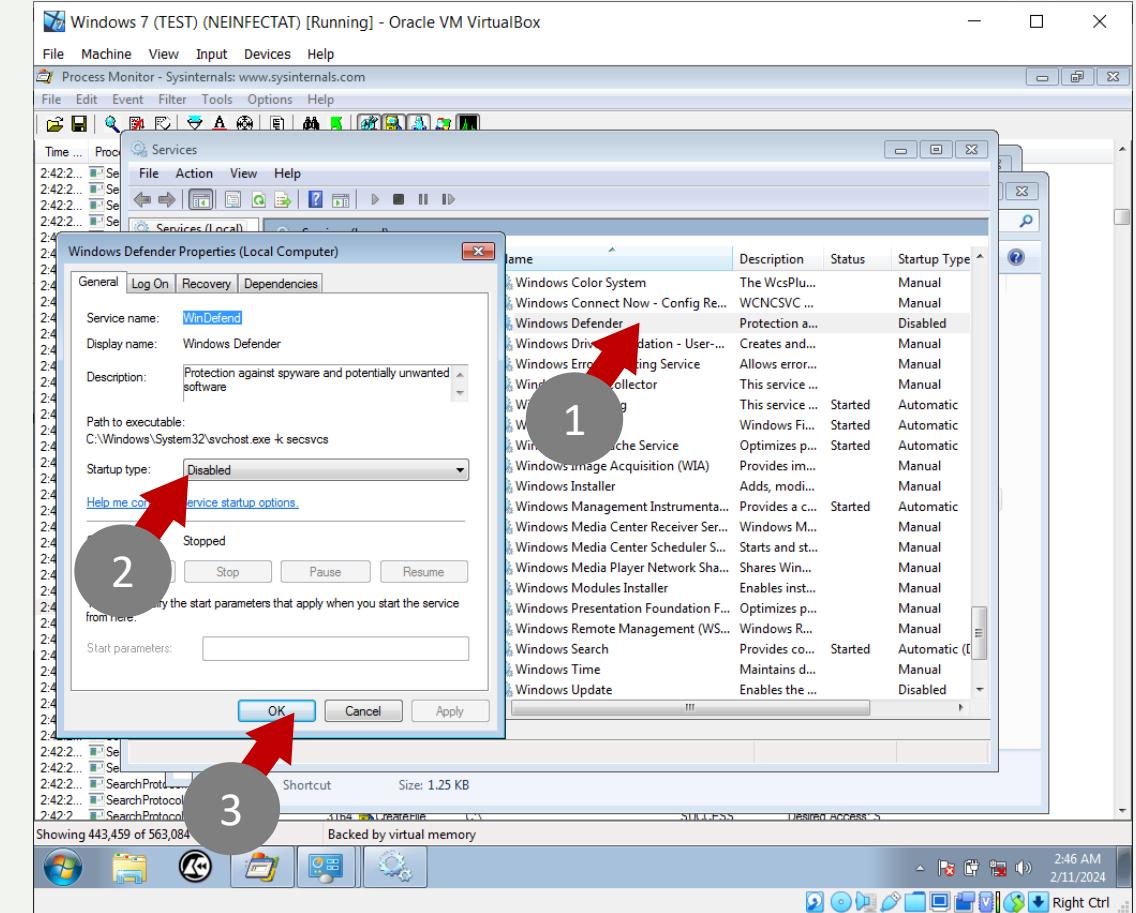
# Dezactivarea serviciilor (III)

- Selectare serviciu: Windows Defender
- Opreire serviciu (Startup type: Disabled)

## Dezactivare: Windows Search



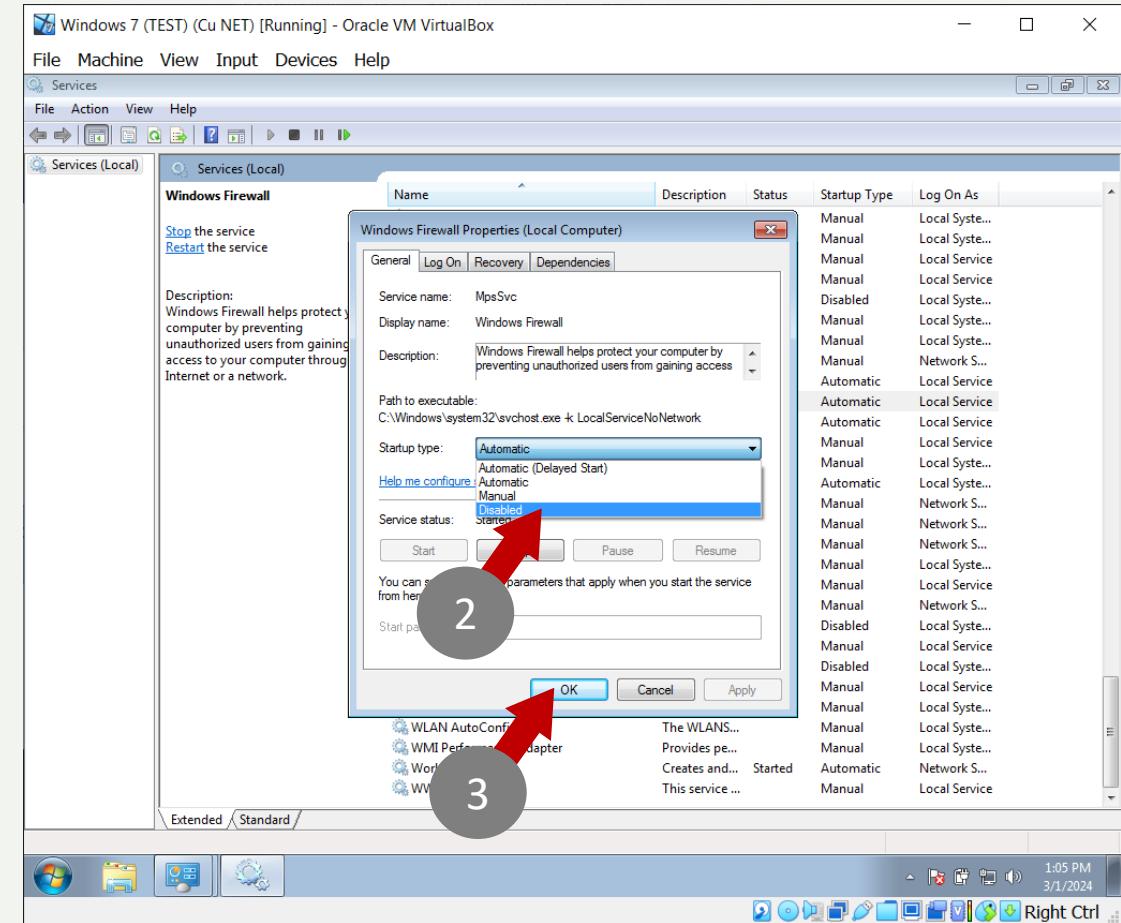
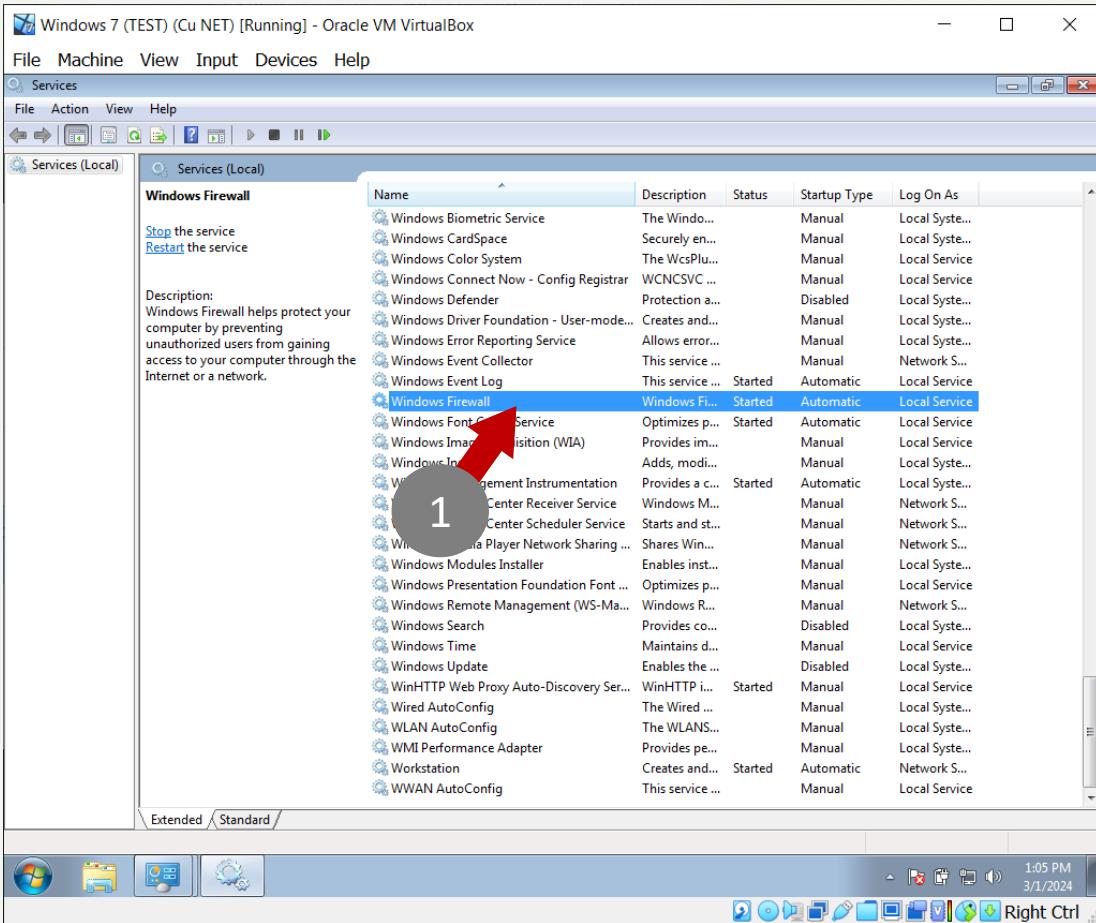
## Dezactivare: Windows Defender



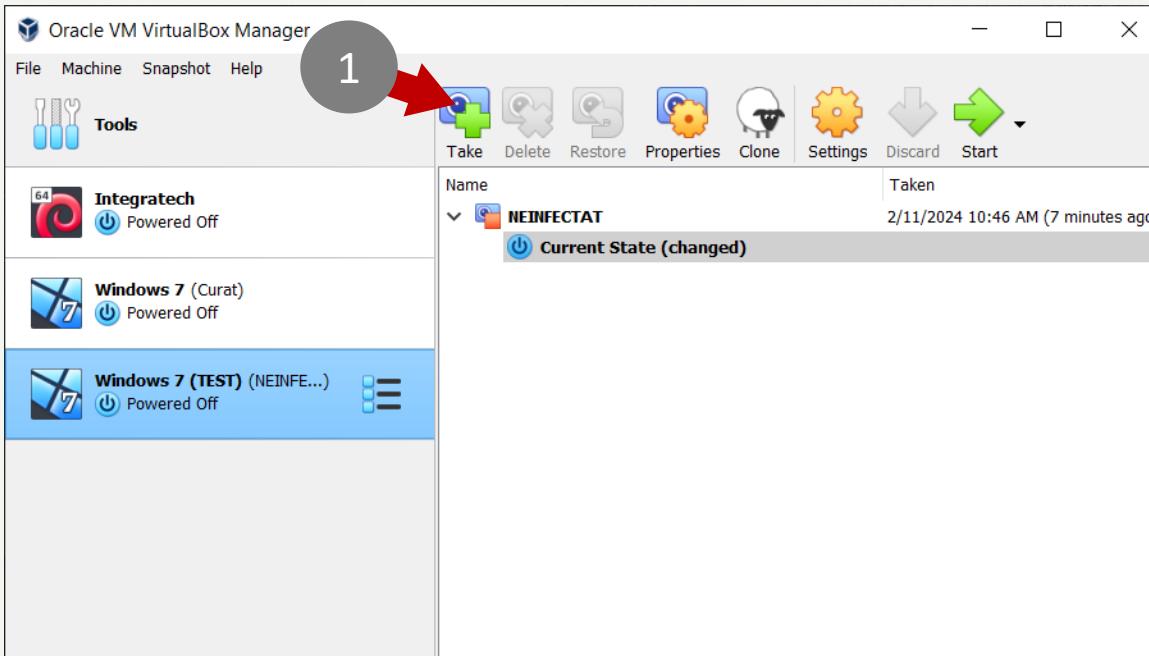
# Dezactivarea serviciilor (IV)

- Selectare serviciu: Windows Firewall
- Opreire serviciu (Startup type: Disabled)

## Dezactivare: Windows Firewall



# MAŞINA VIRTUALĂ SALVARE STARE:



- Salvare stare: permite păstrarea tuturor setărilor efectuate până în acest moment.
- Până în acest moment avem o mașină virtuală care rulează Windows 7, cu toate setările necesare pentru a detona mostrele malware.

---

# INSTALAREA MAȘINII VIRTUALE PE LINUX

---

## VIRTUALBOX GUEST ADDITIONS

OFERĂ FUNCȚIONALITĂȚI ÎMBUNĂTĂȚITE PENTRU MAȘINILE VIRTUALE PE LINUX



C.4.2

# INSTRUMENTELE DE INGINERIE INVERSĂ



Metodologie:



## Analiza Statică

Măsoară potențialul



## Analiza Dinamică

Observați comportamentul



## Analiza Cloud

La distanță:  
potențial și comportament

# ANALIZA STATICĂ:



Inventariere/Inginerie inversă

# COD MALIȚIOS: INSTRUMENTE DE ANALIZĂ



## ■ PEStudio

■ Bcompare

■ Cutter & IDA & x64dbg

■ Sysinternals

■ Wireshark

■ procDOT

■ Analiza malware in Cloud

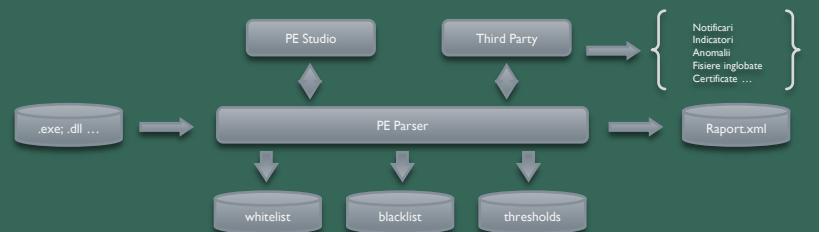
Analiză Statică

Analiză Dinamică

Analiză Cloud

# PE STUDIO

## INDICATORI & CLOUD (TEST BANCA MALWARE)



## Înțelegerea indicatorilor și verificarea în cloud:

File Details		Level
File Path:	c:\users\elliebook\desktop\detonare\virusi analiză	
File Type:	Indicator (27)	
File Size:	58/66	+++++
File MD5:	virustotal > score	
File SHA-256:	groups > API	+++++
File SHA-1:	mitre > technique	+++++
File SHA-3:	overlay > file-type	+++++
File SHA-512:	overlay > size	++
File SSDeep:	75.87%	++
File Hash:	222208 bytes	++
File Extension:	7.179	++
File Signature:	Dev-C++ v4	++
File Embedded:	signature: unknown, location: overlay, offset: 0x00011400, size: 222208 b...	++
File Shared:	signature: registry, location: .rsrc, offset: 0x000090D0, size: 897 bytes	++
File Virtualized:	signature: registry, location: .rsrc, offset: 0x000090D0, size: 897 bytes	++
File Section:	.bss	++
File Shared Section:	.rsrc	++
File Flag:	12	++
File Entropy:	6.909	+
File Type:	executable	+
File CPU:	32-bit	+
File SHA-256:	491FFE981A1A7F9E68CA995709283D37A7D85309000C3C100E621D2EF13...	+
File Size:	292864 bytes	+
File URL:	https://www.virustotal.com/gui/file/491ffe981a1a7f9e68ca995709283d3...	+
File Scan Date:	2019-04-15 13:37:15	+
File Compiler Stamp:	Fri Aug 24 15:00:00 2001	+
File Name Version:	AgentServer	+
File Checksum:	0x00000000	+
File Subsystem:	GUI	+
Entry Point:	0x000011F0	+
Certificate Info:	n/a	+
IMPHASH:	D7401947D3623A2199A2114D62923CD5	+

# Fișier PE infectat luat din banca de malware !

# PE STUDIO

## SECTIUNI EXECUTABIL & ENTROPIE

### ■ Capul de fisier

pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)

[file](#) [settings](#) [about](#)

c:\users\elitebook\Desktop\detonare\virusi analizat

- indicators (virustotal > score)
  - footprints (count > 9)
  - virustotal (58/66)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 64 bytes)
  - rich-header (n/a)
  - file-header (executable > 32-bit)
  - optional-header (subsystem > GUI)
  - directories (count > 2)
  - sections (files > 4)
  - libraries (count > 3)
  - imports (flag > 74)
  - exports (n/a)
  - thread-local-storage (n/a)
  - .NET (n/a)
  - resources (count > 12)
  - strings (count > 5253)
  - debug (n/a)
  - manifest (n/a)
- version (FileDescription > Microsoft Agent Se
  - certificate (n/a)
  - overlay (signature > unknown)

property value

footprint > sha256	BFD5E72651B4EC588BD5FC6A9F17E9E0972248146BBA
size	0x40 (64 bytes)
entropy	3.669
file-ratio	0.00 %
file-header-offset	0x00000080

sha256: 491FFE981A1A7F9E68CA995709283D37A7D85309000C3C100E621D2EF13BA924

cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x000011F

pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)

[file](#) [settings](#) [about](#)

c:\users\elitebook\Desktop\detonare\virusi analizat

property value value value value

section	section[0]	section[1]	section[2]	section[3]
name	.text	.data	.bss	.idata
footprint > sha256	2B365E0B0A75D1CA75C61E...	298D4C27C8E1347B5AC0947...	n/a	E9911860489605C
entropy	6.202	1.358	n/a	4.335
file-ratio	23.78%	0.35 %	n/a	0.87 %
raw-address (begin)	0x00000400	0x00007C00	0x00000000	0x00008000
raw-address (end)	0x00007C00	0x00008000	0x00000000	0x00008A00
raw-size (69632 bytes)	0x00007800 (30720 bytes)	0x00000400 (1024 bytes)	0x00000000 (0 bytes)	0x00000A00 (2560)
virtual-address	0x00001000	0x00009000	0x0000A000	0x0000B000
virtual-size (68844 bytes)	0x00007670 (30320 bytes)	0x0000022C (556 bytes)	0x00000224 (548 bytes)	0x000008E4 (2276)
characteristics	0x60000020	0xC0000040	0xC0000080	0xC0000040
write	-	x	x	x
execute	x	-	-	-
share	-	-	-	-
self-modifying	-	-	-	-
virtual	-	-	x	-
items				
directory > import	-	-	-	0x0000B000
directory > resource	-	-	-	-
version	-	-	-	-
base-of-code	0x00001000	-	-	-
base-of-data	-	0x00009000	-	-
entry-point	0x000011F0	-	-	-
file (signature: registry, size 897 bytes)	-	-	-	-
file (signature: typelib, size 20844 bytes)	-	-	-	-
file (signature: htmfile, size 2002 bytes)	-	-	-	-

sha256: 491FFE981A1A7F9E68CA995709283D37A7D85309000C3C100E621D2EF13BA924

cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x000011F

■ Secțiuni în fișierele PE

# PE STUDIO LIBRARII & API

## ■ Librării folosite

pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)

file settings about

c:\users\elitebook\desktop\detonare\virusi analiză

- library (3) duplicate (0) flag (0) first-thunk-original (INT) first-thunk (IAT)
- ADVAPI32.DLL - - 0x0000B054 0x0000B53C 429 (0x01AD) synchronization
- KERNEL32.dll - - 0x0000B08C 0x0000B580 535 (0x0217) synchronization
- msvcr7.dll - - 0x0000B12C 0x0000B5DC 63 (0x03F) synchronization

indicators (virustotal > score)  
footprints (count > 9)  
virustotal (58/66)  
dos-header (size > 64 bytes)  
dos-stub (size > 64 bytes)  
rich-header (n/a)  
file-header (executable > 32-bit)  
optional-header (subsystem > GUI)  
directories (count > 2)  
sections (files > 4)  
libraries (count > 3)  
imports (flag > 74)  
exports (n/a)  
thread-local-storage (n/a)  
.NET (n/a)  
resources (count > 12)  
strings (count > 5253)  
debug (n/a)  
manifest (n/a)  
version (FileDescription > Microsoft Agent Se...  
certificate (n/a)  
overlay (signature > unknown)

sha256: 491FFE981A1A7F9E68CA995709283D37A7D085309000C3C100E621D2EF13BA924

cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x000011F

pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)

file settings about

c:\users\elitebook\desktop\detonare\virusi analiză

imports (74)	flag (12)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (11)	tech ^
InterlockedIncrement	-	0x0000B53C	0x0000B53C	429 (0x01AD)	synchronization	-
ReleaseMutex	-	0x0000B580	0x0000B580	535 (0x0217)	synchronization	-
CreateMutexA	-	0x0000B5DC	0x0000B5DC	63 (0x03F)	synchronization	-
WaitForSingleObject	-	0x0000B654	0x0000B654	696 (0x02B8)	synchronization	-
CloseServiceHandle	-	0x0000B2D0	0x0000B2D0	58 (0x03A)	services	T15E
CreateServiceA	x	0x0000B2E8	0x0000B2E8	90 (0x005A)	services	T15A
DeleteService	x	0x0000B2FC	0x0000B2FC	135 (0x0087)	services	T14B
OpenSCManagerA	-	0x0000B30C	0x0000B30C	356 (0x0164)	services	T15E
OpenServiceA	-	0x0000B320	0x0000B320	358 (0x0166)	services	T15A
RegisterServiceCtrlHandlerA	-	0x0000B368	0x0000B368	437 (0x01B5)	services	T11C
SetServiceStatus	-	0x0000B388	0x0000B388	475 (0x01DB)	services	T15A
StartServiceA	-	0x0000B39C	0x0000B39C	480 (0x01E0)	services	T15E
StartServiceCtrlDispatcherA	x	0x0000B3AC	0x0000B3AC	481 (0x01E1)	services	-
RegCloseKey	-	0x0000B330	0x0000B330	384 (0x0180)	registry	-
RegCreateKeyExA	x	0x0000B340	0x0000B340	388 (0x0184)	registry	T11I
RegGetValueExA	x	0x0000B354	0x0000B354	430 (0x01AE)	registry	T11I
GetDriveTypeA	-	0x0000B44C	0x0000B44C	255 (0x00FF)	reconnaissance	-
GetStartupInfoA	-	0x0000B4E4	0x0000B4E4	333 (0x014D)	reconnaissance	-
GetVersionExA	-	0x0000B508	0x0000B508	370 (0x0172)	reconnaissance	-
GetWindowsDirectoryA	-	0x0000B518	0x0000B518	378 (0x017A)	reconnaissance	T10E
malloc	-	0x0000B710	0x0000B710	603 (0x025B)	memory	-
memcpy	-	0x0000B71C	0x0000B71C	609 (0x0261)	memory	-
memset	-	0x0000B728	0x0000B728	611 (0x0263)	memory	-
FindClose	-	0x0000B3DC	0x0000B3DC	142 (0x008E)	file	-
FindFirstFileA	x	0x0000B3E8	0x0000B3E8	146 (0x0092)	file	T10E
FindNextFileA	x	0x0000B3FC	0x0000B3FC	155 (0x009B)	file	T10E
FlushFileBuffers	-	0x0000B40C	0x0000B40C	168 (0x00A8)	file	-
GetFileAttributesA	-	0x0000B45C	0x0000B45C	765 (0x01DD)	file	-

sha256: 491FFE981A1A7F9E68CA995709283D37A7D085309000C3C100E621D2EF13BA924

cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x000011F

## ■ API folosit

# PE STUDIO

## RESURSE & STRINGURI

- Resurse
- Strings

#### ■ Resursele executabilului

pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)

**file settings about**

**c:\users\elitebook\Desktop\detonator\virusi analisi**

- > indicator (virustotal > score)
- > 99 footprints (count > 9)
- > virustotal (58/66)
- > dos-header (size > 64 bytes)
- > dos-stub (size > 64 bytes)
- > rich-header (n/a)
- > file-header (executable > 32-bit)
- > optional-header (subsystem > GUI)
- > directories (count > 2)
- > sections (files > 4)
- > libraries (count > 3)
- > imports (flag > 74)
- > exports (n/a)
- > thread-local-storage (n/a)
- > .NET (n/a)
- > resources (count > 12)
  - > strings (count > 5253)
  - > debug (n/a)
  - > manifest (n/a)
- > version (FileDescription > Microsoft Agent Se
  - > certificate (n/a)
  - > overlay (signature > unknown)

---

name	instance (12)	signature	location
icon	1	icon	.jsrc:0x00009458
version	1	version	.jsrc:0x00008D20
REGISTRY	109	registry	.jsrc:0x000090D0
REGISTRY	109	registry	.jsrc:0x000090D0
icon-group	113	icon-group	.jsrc:0x0000B520
icon	2	icon	.jsrc:0x0000A300
icon-group	215	icon-group	.jsrc:0x0000B980
icon	3	icon	.jsrc:0x0000ABA8
icon	4	icon	.jsrc:0x0000B110
icon	5	icon	.jsrc:0x0000B3F8
icon	6	icon	.jsrc:0x0000B570
icon	7	icon	.jsrc:0x0000B858

pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)

file settings about

c:\users\elitebook\Desktop\detonare\virusi analiză

- indicators (virustotal > score)
- footprints (count > 9)
- virustotal (58/66)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 64 bytes)
  - rich-header (n/a)
  - file-header (executable > 32-bit)
  - optional-header (subsystem > GUI)
- directories (count > 2)
- sections (files > 4)
- libraries (count > 3)
  - imports (flag > 74)
  - exports (n/a)
  - thread-local-storage (n/a)
  - .NET (n/a)
  - resources (count > 12)
  - strings (count > 5253)
  - debug (n/a)
  - manifest (n/a)
  - version (FileDescription > Microsoft Agent Se)
    - certificate (n/a)
    - overlay (signature > unknown)

enco...	si...	location	fl...	label (1...	group (16)	technique (18)	value
ascii	13	overlay	-	-	windowing	-	DestroyWindow
ascii	8	overlay	-	-	windowing	-	IsWindow
ascii	15	overlay	-	-	windowing	-	IsWindowVisible
ascii	12	overlay	-	-	windowing	-	UpdateWindow
ascii	12	overlay	-	-	windowing	-	SetWindowPos
ascii	15	overlay	-	-	windowing	-	IsWindowEnabled
ascii	10	overlay	-	-	windowing	-	ShowWindow
ascii	13	overlay	-	-	windowing	-	DefWindowProc
ascii	13	overlay	-	-	windowing	T1055   Process Injection	SetWindowLong
ascii	13	overlay	-	-	windowing	T1055   Process Injection	GetWindowLong
ascii	14	overlay	-	-	windowing	-	CreateWindowEx
ascii	13	overlay	-	-	windowing	-	RegisterClass
ascii	11	overlay	-	-	windowing	T1055   Process Injection	SendMessage
ascii	24	overlay	x	-	windowing	-	AllowSetForegroundWindow
ascii	10	overlay	-	-	windowing	-	GetCapture
ascii	11	overlay	-	-	windowing	-	PeekMessage
ascii	12	overlay	-	-	windowing	-	EnableWindow
ascii	15	overlay	-	-	windowing	-	RegisterClassEx
ascii	18	overlay	-	-	windowing	T1055   Process Injection	SendMessageTimeout
ascii	15	overlay	-	-	windowing	-	DispatchMessage
ascii	16	overlay	-	-	windowing	-	TranslateMessage
ascii	10	overlay	-	-	windowing	-	GetMessage
ascii	21	overlay	-	-	windowing	-	RegisterWindowMessage
ascii	17	overlay	-	-	windowing	T1055   Process Injection	SendNotifyMessage
ascii	19	overlay	-	-	windowing	-	SetForegroundWindow
ascii	19	overlay	x	-	windowing	T1010   Window Discovery	GetForegroundWindow
ascii	10	overlay	-	-	windowing	-	MoveWindow
ascii	14	overlay	-	-	windowing	-	CallWindowProc

sha256: 491FFE981A1A7F9E68CA995709283D37A7D85309000C3C100E621D2EF13BA924

cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x000011F

subsystem: GUI entry-point: 0x000011F

## Şiruri găsite în executabil

#### ■ Siruri găsite în executabil

# COD MALIȚIOS: INSTRUMENTE DE ANALIZĂ

- PEStudio
- **Bcompare**

Analiză Statică

- Cutter & IDA & x64dbg
- Sysinternals & Process Hacker

- Wireshark
- procDOT

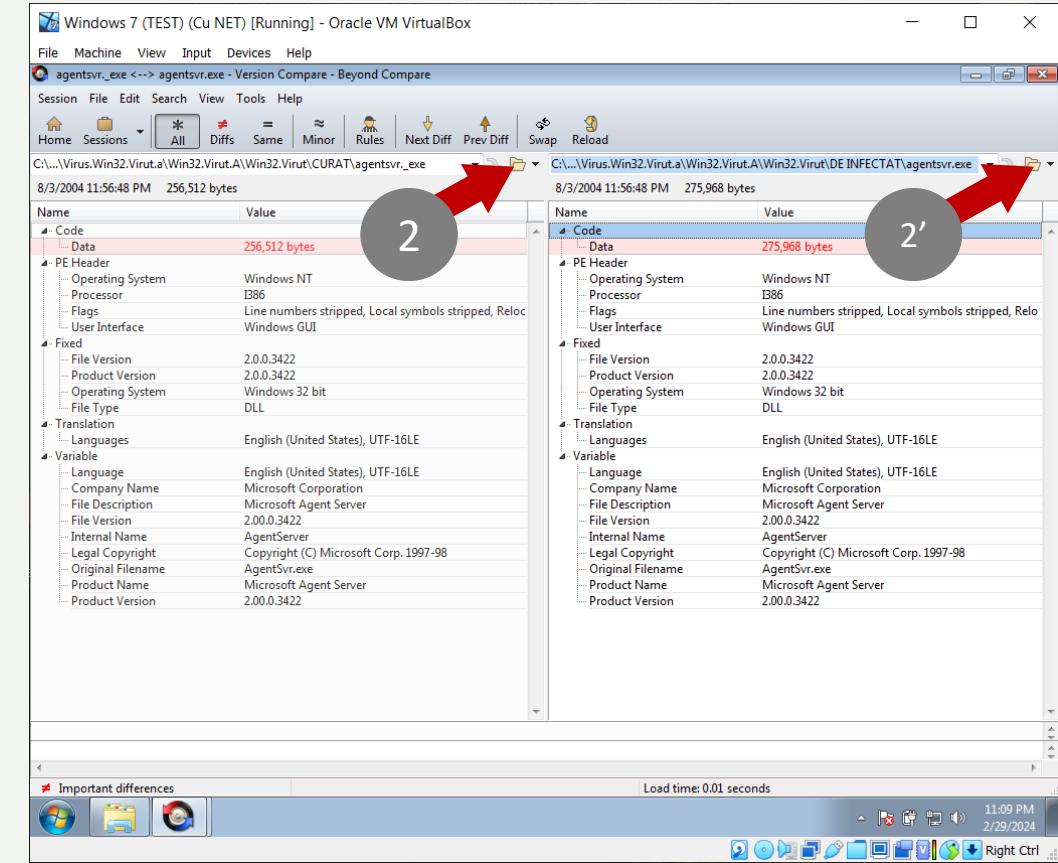
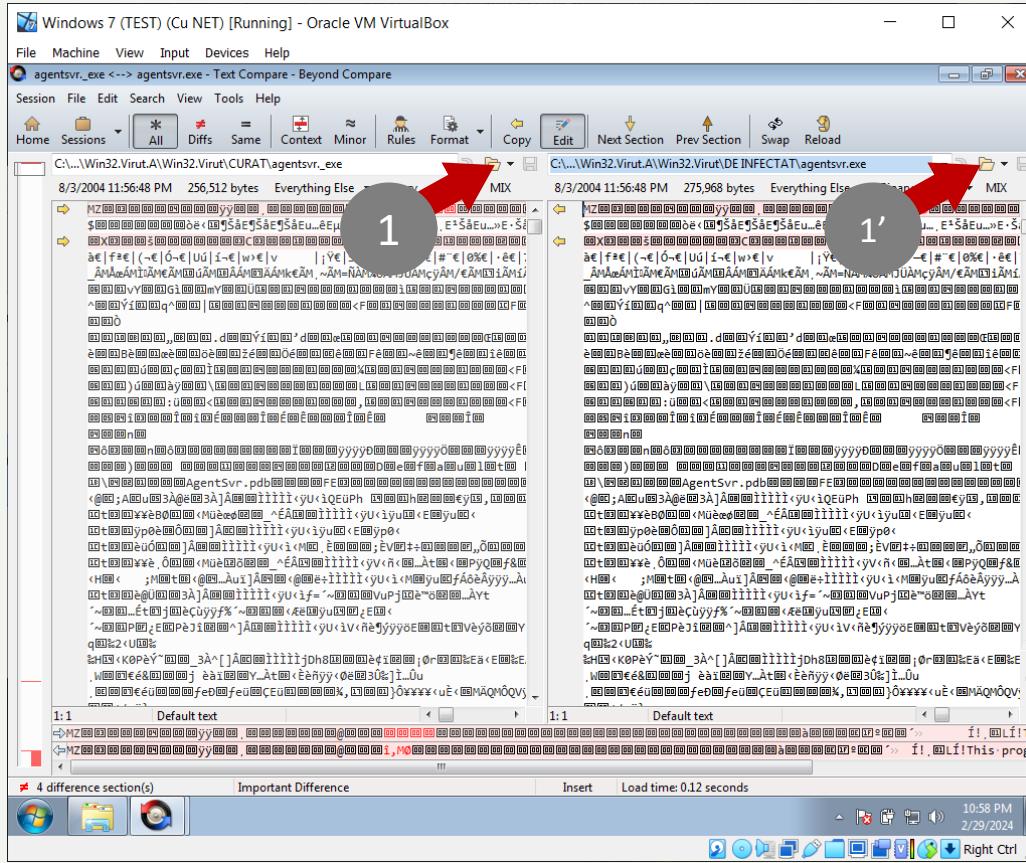
Analiză Dinamică

- Analiza malware in Cloud

Analiză Cloud

# BCOMPARE

## COMPARAREA TEXTULUI ȘI COMPARAREA VERSIUNILOR



# BCOMPARE

## COMPARAREA CONȚINUTULUI A DOUĂ FIȘIERE

Windows 7 (TEST) (Cu NET) [Running] - Oracle VM VirtualBox

VX <-> Bazar - Folder Compare - Beyond Compare

Session Actions Edit Search View Tools Help

Home Sessions \* All Diffs Same Structure Minor Rules Copy Expand Collapse Select Files Refresh Swap Stop

Filters: \*.\* Filters Peek

C:\Users\Paul\Desktop\malware\VX C:\Users\Paul\Desktop\malware\Bazar

Name	Size	Modif.	Name	Size	Modif.
Backdoor		2/10/2024 6:23:06 PM	criptominer password infected.zip	154,312	2/10/2024 6:08:25 PM
Email-Worm		2/10/2024 6:23:16 PM	lumma.zip	403,523	2/10/2024 6:12:40 PM
Net-Worm		2/10/2024 6:23:18 PM	NyMaim.zip	210,908	2/10/2024 6:11:28 PM
Trojan		2/10/2024 6:24:01 PM	vbs.zip	1,083	2/10/2024 6:09:33 PM
vir		2/10/2024 6:24:01 PM	cls.zip	344,377	2/10/2024 6:11:05 PM
Virus.MSEcel		2/10/2024 6:24:03 PM	zbet.zip	2,327,058	2/10/2024 6:15:43 PM
Virus.VBS		2/10/2024 6:24:04 PM			
Virus.WinREG		2/10/2024 6:24:04 PM			
VIRUS ANALIZATI		2/10/2024 6:24:04 PM			

2/29/2024 10:52:38 PM Username: Paul-PC\Paul  
2/29/2024 10:52:38 PM Load comparison: <->  
2/29/2024 10:52:56 PM Load comparison: C:\Users\Paul\Desktop\malware\VX <->  
2/29/2024 10:53:05 PM Load comparison: C:\Users\Paul\Desktop\malware\VX <-> C:\Users\Paul\Desktop\malware\Bazar

17.6 GB free on C:\ 6 file(s), 3.28 MB 17.6 GB free on C:\ 10:53 PM 2/29/2024

Right Ctrl

Windows 7 (TEST) (Cu NET) [Running] - Oracle VM VirtualBox

HKEY\_CURRENT\_USER - Registry Compare - Beyond Compare

Session File Edit Search View Tools Help

Home Sessions \* All Diffs Same Copy Next Diff Prev Diff Swap Reload Expand Collapse

reg\PAUL-PC\HKEY\_CURRENT\_USER reg\PAUL-PC\HKEY\_CURRENT\_USER

Name	Type	Name	Type
AppEvents		AppEvents	
Console		Console	
Control Panel		Control Panel	
Environment		Environment	
EUDC		EUDC	
Identities		Identities	
Keyboard Layout		Keyboard Layout	
Network		Network	
Printers		Printers	
Software		Software	
System		System	
Volatile Environment		Volatile Environment	

Binary same Load time: 0.09 seconds 10:52 PM 2/29/2024

Right Ctrl

# BCOMPARE

## COMPARAREA CONȚINUTULUI A DOUĂ FIȘIERE

Observați diferența în cantitatea de informație dintre coada fișierului infectat și cel neinfectat.

Windows 7 (TEST) [Cu NET] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

agentsrv.exe <-> agentsrv.exe - Hex Compare - Beyond Compare

Session File Edit Search View Tools Help

Home Sessions All Diffs Same Rules Format Copy Next Diff Swap Reload

C:\...\Win32.Virut.A\Win32.Virut\DE INFECTAT\agentsrv.exe 8/3/2004 11:56:48 PM 275,968 bytes Everything Else

C:\...\Win32.Virut.A\Win32.Virut\CURAT\agentsrv.exe 8/3/2004 11:56:48 PM 256,512 bytes Everything Else

00000000 4D 5A 00 00 03 00 00 00 MZ.....

00000008 04 00 00 00 FF FF 00 00 ..yy.....

00000010 B8 00 00 00 00 00 00 00 ..

00000018 40 00 00 00 EE 2C 4D D8 @...i,MO

00000020 00 00 00 00 00 00 00 00 ..

00000028 00 00 00 00 00 00 00 00 ..

00000030 00 00 00 00 00 00 00 00 ..

00000038 00 00 00 E0 00 00 00 ....â...

00000040 0E 1F BA 0E 0B 84 09 CD ..%...í

00000048 21 B8 01 4C CD 21 54 68 !..ÍÍT!

00000050 69 73 20 70 72 6F 67 72 is progr

00000058 61 6D 20 63 61 6E 6F am canno

00000060 74 20 62 65 20 72 75 6E t be run

00000068 20 69 6E 20 44 4F 53 20 in DOS

00000070 6D 6F 64 65 2E 0D 00 0A mode....

00000078 24 00 00 00 00 00 \$.....

00000080 F2 EB 8B 16 B6 8A E5 45 öé...ßé

00000088 B6 8A E5 45 B6 8A E5 45 ßé...ßé

00000090 75 85 EA 45 B5 8A E5 45 ..é...ßé

00000098 B6 8A E4 45 1C 88 E5 45 ßé...ßé

000000A0 75 85 BB 45 B9 8A E5 45 ..E...ßé

000000A8 75 85 BB 45 B7 8A E5 45 ..w...ßé

000000B0 75 85 85 45 84 8A E5 45 ..w...ßé

000000B8 75 85 BA 45 A0 8A E5 45 ..w...ßé

000000C0 75 85 BF 45 B7 8A E5 45 ..z...ßé

000000C8 52 69 63 68 B6 8A E5 45 Richßé

000000D0 00 00 00 00 00 00 00 ..

000000E0 50 45 00 00 4C 01 03 00 PE.L...

000000E8 3F 78 10 41 00 00 00 ?!.A...

000000F0 00 00 00 E0 00 0F 01 ....à...

0000004F

Binary differences Insert Load time: 0.02 seconds

3 1 1' 4

Windows 7 (TEST) [Cu NET] [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

agentsrv.exe <-> agentsrv.exe - Hex Compare - Beyond Compare

Session File Edit Search View Tools Help

Home Sessions All Diffs Same Rules Format Copy Next Diff Swap Reload

C:\...\Win32.Virut.A\Win32.Virut\DE INFECTAT\agentsrv.exe 8/2/2004 11:56:48 PM 275,968 bytes Everything Else

C:\...\Win32.Virut.A\Win32.Virut\CURAT\agentsrv.exe 8/3/2004 11:56:48 PM 256,512 bytes Everything Else

0003E9A4 00 00 00 00 00 00 00 00 ..

0003E9A0 00 00 00 00 00 00 00 00 ..

0003E9B0 00 00 00 00 00 00 00 00 ..

0003E9C4 00 00 00 00 00 00 00 00 ..

0003E9C0 00 00 00 00 00 00 00 00 ..

0003E9D4 00 00 00 00 00 00 00 00 ..

0003E9D0 00 00 00 00 00 00 00 00 ..

0003E9E4 00 00 00 00 00 00 00 00 ..

0003E9EC 00 00 00 00 00 00 00 00 ..

0003E9F4 00 00 00 00 00 00 00 00 ..

0003E9FC 00 00 00 00 00 00 00 00 ..

0003EA00 74 20 62 65 20 72 75 6E t be run

0003EA08 20 69 6E 20 44 4F 53 20 in DOS

0003EA00 6D 6F 64 65 2E 0D 00 0A mode....

0003EA08 24 00 00 00 00 00 00 \$.....

0003EA00 F2 EB 8B 16 B6 8A E5 45 öé...ßé

0003EA08 B6 8A E5 45 B6 8A E5 45 ßé...ßé

0003EA00 75 85 EA 45 B5 8A E5 45 ..é...ßé

0003EA08 B6 8A E4 45 1C 88 E5 45 ßé...ßé

0003EA00 75 85 BB 45 B9 8A E5 45 ..E...ßé

0003EA08 75 85 BB 45 B7 8A E5 45 ..w...ßé

0003EA08 75 85 85 45 84 8A E5 45 ..w...ßé

0003EA08 75 85 BA 45 A0 8A E5 45 ..w...ßé

0003EA08 75 85 BF 45 B7 8A E5 45 ..z...ßé

0003EA08 52 69 63 68 B6 8A E5 45 Richßé

0003EA00 00 00 00 00 00 00 00 ..

0003EA00 50 45 00 00 4C 01 03 00 PE.L...

0003EA08 3F 78 10 41 00 00 00 ?!.A...

0003EA00 00 00 00 E0 00 0F 01 ....à...

0003EA0F

Binary differences Insert Load time: 0.02 seconds

2 2'

Coadă fisier neinfectat

Coadă fisier infectat

# COD MALIȚIOS: INSTRUMENTE DE ANALIZĂ

- PEStudio
- Bcompare
- **Cutter & IDA & x64dbg**

Analiză Statică

- Sysinternals
- Wireshark
- procDOT

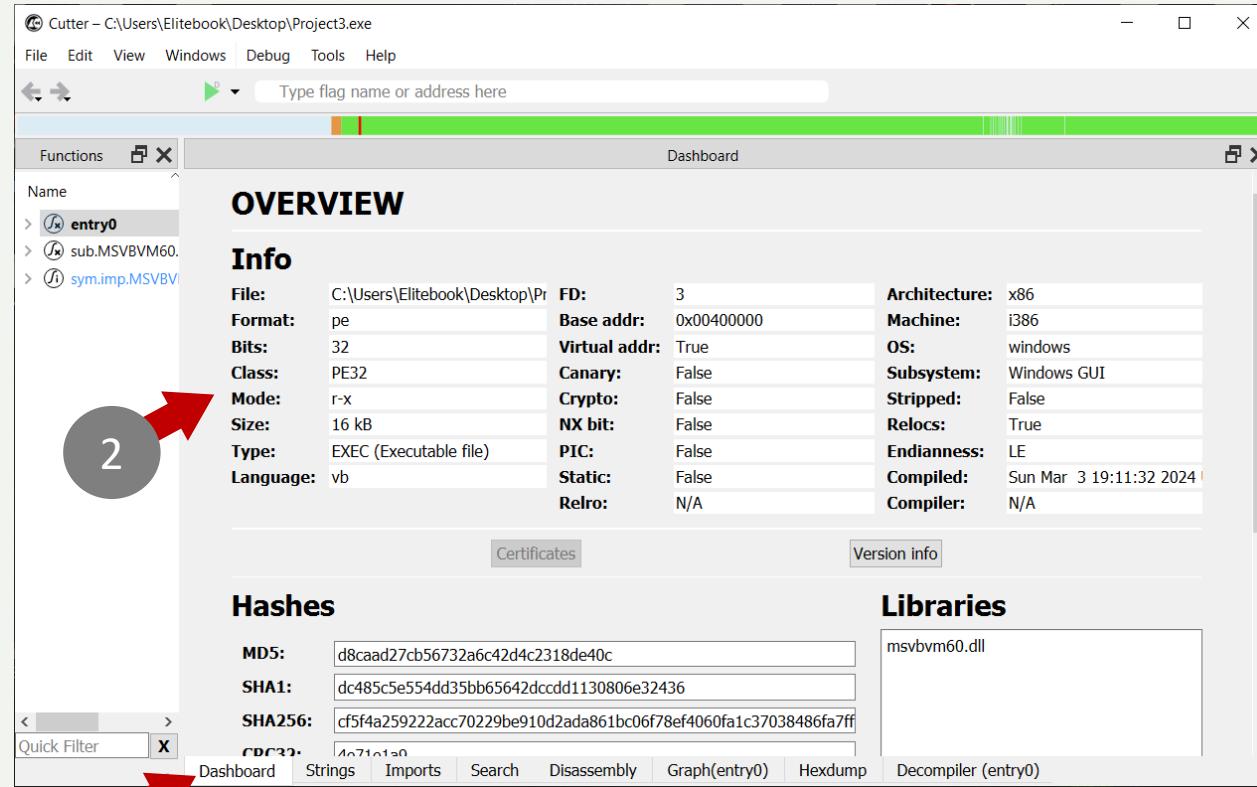
Analiză Dinamică

- Analiza malware in Cloud

Analiză Cloud

# CUTTER DASHBOARD

MD5: O valoare hash de 128 de biți, utilizată pentru a verifica integritatea fișierului.  
SHA1: O valoare hash de 160 de biți, mai sigură decât MD5.  
SHA256: O valoare hash de 256 de biți, parte din familia SHA-2, oferă o securitate și mai puternică.



- **File.** Calea către fișierul executabil analizat.
- **Format.** Indică formatul fișierului; în acest caz, "pe" pentru Portable Executable.
- **Bits.** Arată lățimea arhitecturii procesorului în biți; aici este "32", indicând un executabil pe 32 de biți.
- **Class.** Se referă la clasa specifică a formatului fișierului; "PE32" indică un Portable Executable pe 32 de biți.
- **Mode.** Permișunile cu care fișierul este mappat; "r-x" înseamnă citire și executare.
- **Size.** Dimensiunea fișierului în kiloocteți.
- **Type.** Tipul fișierului, în acest caz "EXEC" (Executable file).
- **Language.** Limbajul de programare folosit, aici este "vb" pentru Visual Basic.

# CUTTER DASHBOARD

MD5: O valoare hash de 128 de biți, utilizată pentru a verifica integritatea fișierului.  
SHA1: O valoare hash de 160 de biți, mai sigură decât MD5.  
SHA256: O valoare hash de 256 de biți, parte din familia SHA-2, oferă o securitate și mai puternică.

The screenshot shows the CUTTER Dashboard interface for the file C:\Users\Elitebook\Desktop\Project3.exe. The 'OVERVIEW' section displays various file properties:

File:	C:\Users\Elitebook\Desktop\Pr	FD:	3
Format:	pe	Base addr:	0x00400000
Bits:	32	Virtual addr:	True
Class:	PE32	Canary:	False
Mode:	r-x	Crypto:	False
Size:	16 kB	NX bit:	False
Type:	EXEC (Executable file)	PIC:	False
Language:	vb	Static:	False
		Relro:	N/A

The 'Hashes' section shows the following hash values:

- MD5: d8caad27cb56732a6c42d4c2318de40c
- SHA1: dc485c5e554dd35bb65642dccdd1130806e32436
- SHA256: cf5f4a25922acc70229be910d2ada861bc06f78ef4060fa1c37038486fa7ff

The 'Libraries' section lists msvbvm60.dll.

A red arrow points to the number '1' in a circle, which is overlaid on the 'Version info' button.

- **FD.** Numărul descriptorului de fișier.
- **Base addr.** Adresa de bază unde executabilul este mapat în memorie.
- **Virtual addr.** Indică dacă fișierul are o adresă virtuală; aici este "True".
- **Canary.** O caracteristică de securitate pentru a preveni atacurile de tip buffer overflow; "False" indică faptul că nu este prezent.
- **Crypto.** Indică dacă sunt detectate funcții criptografice; "False" sugerează că nu sunt.
- **NX bit.** No-Execute bit, care dacă este "False" permite executarea codului în toate regiunile de memorie.
- **PIC.** Position Independent Code, care dacă este "False" înseamnă că codul nu este independent de poziție.
- **Static.** Indică dacă binarul este legat static; "False" înseamnă că nu este.
- **Relro.** Relocation Read-Only, o caracteristică de securitate care face anumite secțiuni ale binarului să fie doar de citire după ce relocațiile au fost procesate; "N/A" indică că nu este aplicabil sau nu este prezent.

# CUTTER DASHBOARD

MD5: O valoare hash de 128 de biți, utilizată pentru a verifica integritatea fișierului.  
SHA1: O valoare hash de 160 de biți, mai sigură decât MD5.  
SHA256: O valoare hash de 256 de biți, parte din familia SHA-2, oferă o securitate și mai puternică.

The screenshot shows the CUTTER Dashboard interface with the following details:

**File:** C:\Users\Elitebook\Desktop\Project3.exe

**Format:** pe

**Bits:** 32

**Class:** PE32

**Mode:** r-x

**Size:** 16 kB

**Type:** EXEC (Executable file)

**Language:** vb

**Architecture:** x86

**Machine:** i386

**OS:** windows

**Subsystem:** Windows GUI

**Stripped:** False

**Relocs:** True

**Endianness:** LE

**Compiled:** Sun Mar 3 19:11:32 2024

**Compiler:** N/A

**Hashes**

- MD5:** d8caad27cb56732a6c42d4c2318de40c
- SHA1:** dc485c5e554dd35bb65642dccdd1130806e32436
- SHA256:** cf5f4a25922acc70229be910d2ada861bc06f78ef4060fa1c37038486fa7ff

**Libraries**

- msvbvm60.dll

**Decompiler (entry0)**

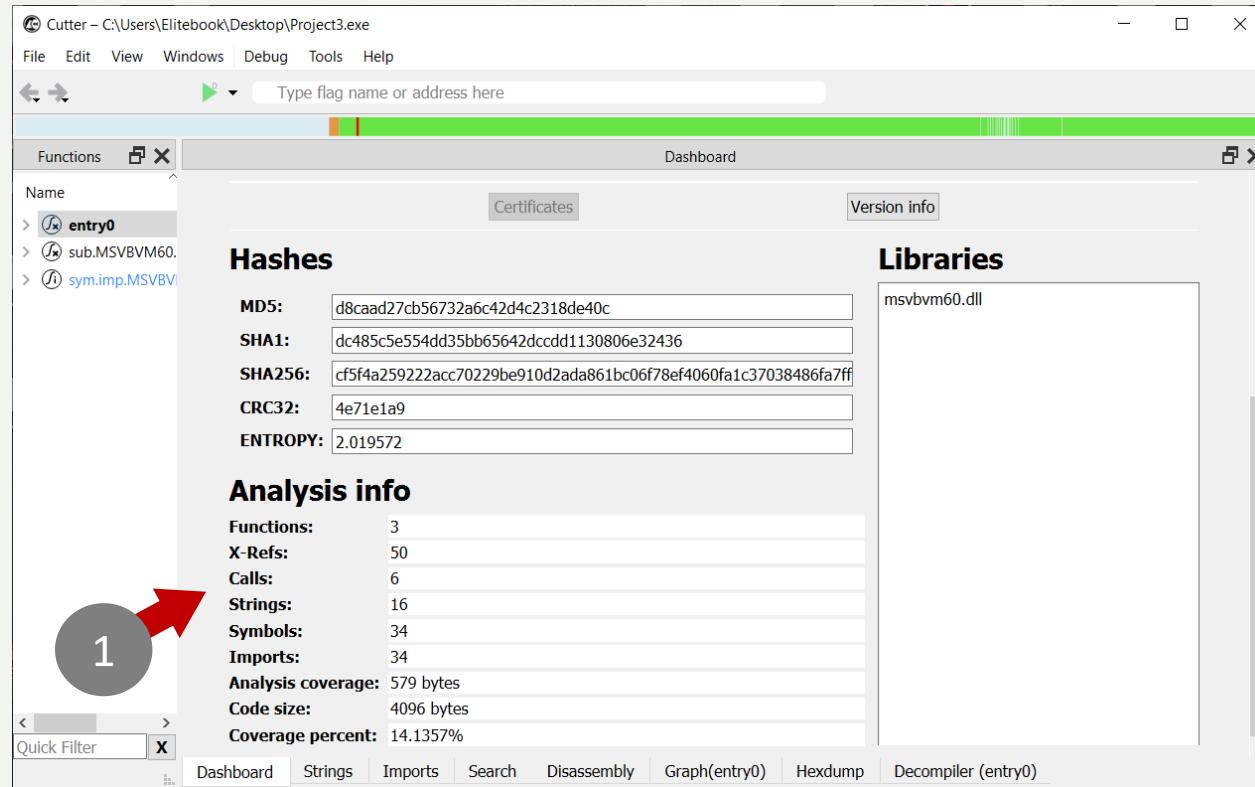
A red arrow points from a circled '1' in the middle-left area towards the architecture information.

- Architecture.** Indică arhitectura CPU, care este x86.
- Machine.** Tipul specific de mașină sau procesor, i386, compatibil cu arhitectura x86 de 32 de biți.
- OS.** Sistemul de operare, care este Windows.
- Subsystem.** Subsistemul sub care executabilul funcționează, aici este "Windows GUI".
- Stripped.** Indică dacă informațiile despre simboluri sunt eliminate din executabil; "False" înseamnă că nu sunt.
- Relocs.** Relocații, indică dacă binarul poate fi relocat; "True" înseamnă că poate fi.
- Endianness.** Ordinea octetilor utilizată de sistem; "LE" înseamnă Little Endian.
- Compiled.** Data și ora când executabilul a fost compilat.
- Compiler.** Compilatorul folosit pentru a construi executabilul, în acest caz, "N/A" indică că nu este disponibil.

# CUTTER

## DASHBOARD - ANALYSIS INFO

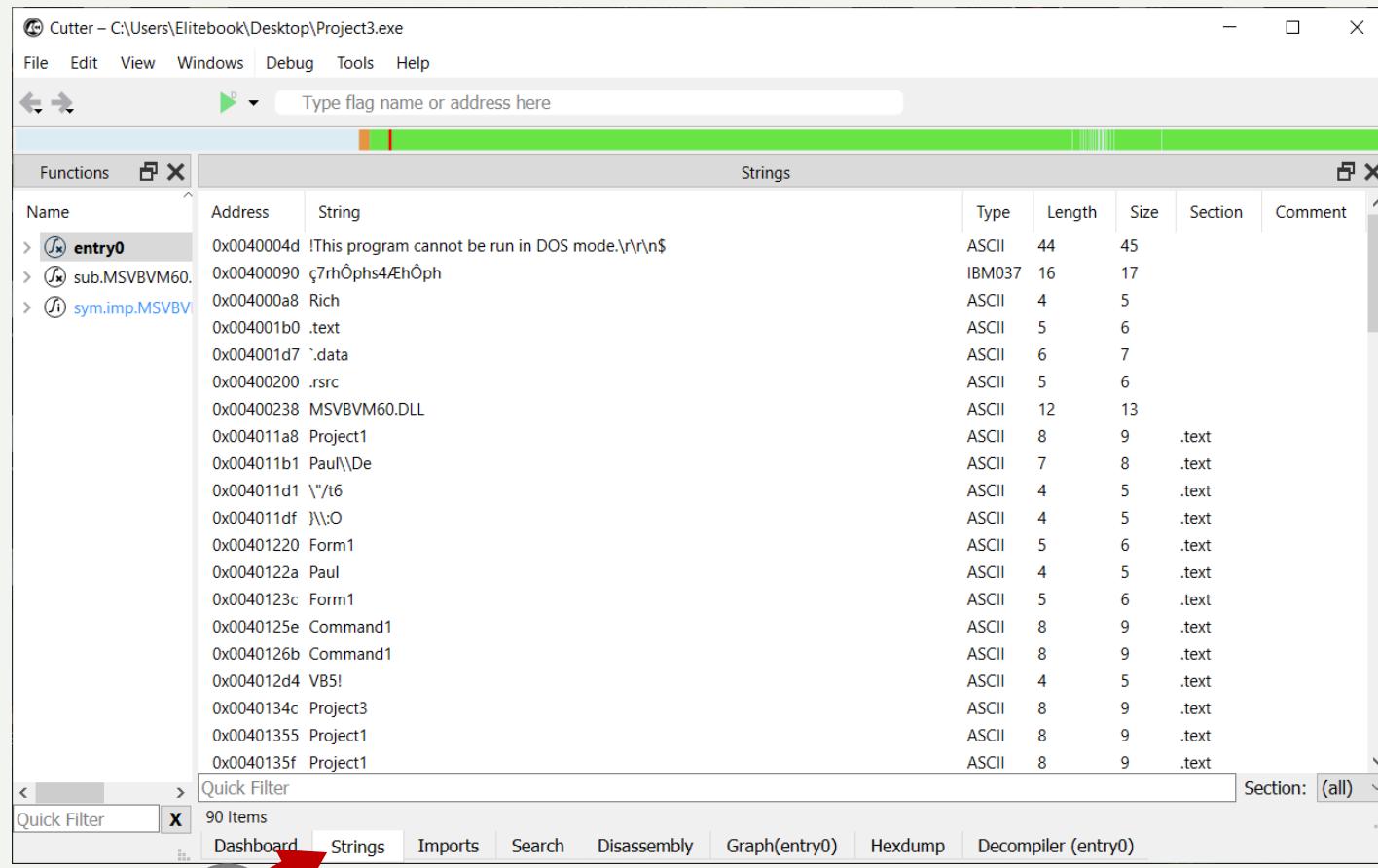
MD5: O valoare hash de 128 de biți, utilizată pentru a verifica integritatea fișierului.  
SHA1: O valoare hash de 160 de biți, mai sigură decât MD5.  
SHA256: O valoare hash de 256 de biți, parte din familia SHA-2, oferă o securitate și mai puternică.



- **Functions.** Numărul de funcții identificate în fișierul executabil.
- **X-Refs.** Numărul de referințe încrucișate care arată cum sunt legate între ele diversele secțiuni de cod sau date.
- **Calls.** Numărul de apeluri de funcții din cadrul codului.
- **Strings.** Numărul de siruri de caractere detectate în fișierul executabil.
- **Symbols.** Numărul de simboluri detectate, care pot include funcții și variabile.
- **Imports.** Numărul de funcții importate, care sunt de obicei funcții din biblioteci externe folosite în cod.
- **Analysis coverage.** Cantitatea de cod analizată în octeți.
- **Code size.** Dimensiunea totală a secțiunii de cod din fișierul executabil în octeți.
- **Coverage percent.** Procentul de cod care a fost analizat în raport cu dimensiunea totală a codului.

# CUTTER STRINGS

Această funcție este utilă pentru a identifica mesaje, căi de fișiere, URL-uri și alte date posibil interesante pentru cei care fac inginerie inversă sau analize de securitate.

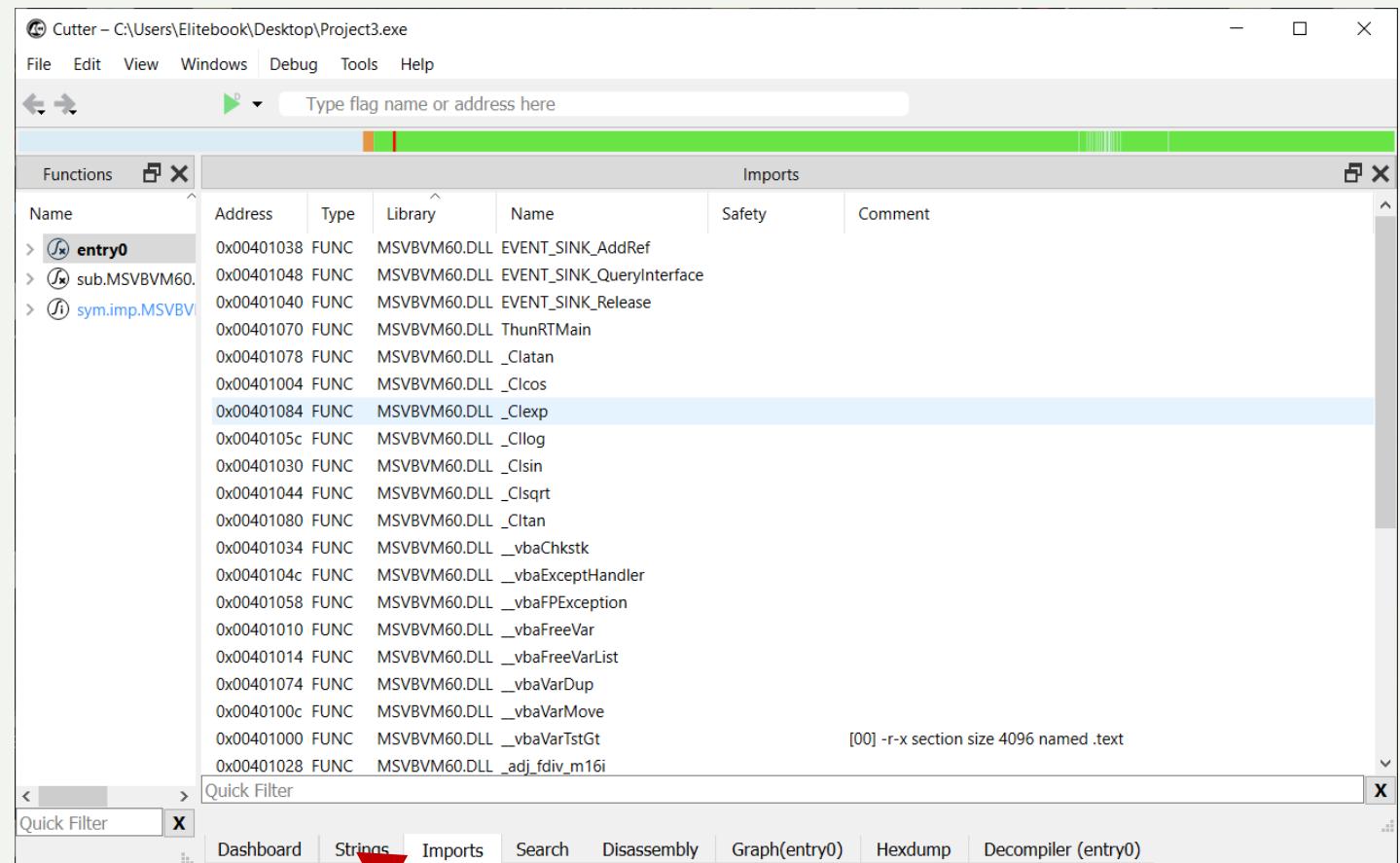


- **Name.** Numele sau eticheta asociată cu șirul în cadrul fișierului binar.
- **Address.** Adresa de memorie unde este localizat șirul.
- **String.** Textul efectiv al șirului.
- **Type.** Tipul de codificare a șirului, de exemplu ASCII sau un alt tip de codificare.
- **Length.** Lungimea șirului, fără a include caracterul terminator null.
- **Size.** Mărimea șirului în octeți, care poate include terminatorul null.
- **Section.** Secțiunea fișierului binar unde se află șirul. De exemplu, secțiunea ".text" conține cod executabil, în timp ce ".data" și ".rsrc" conțin de obicei date.

# CUTTER

## IMPORTURI (EXECUTABILE IMPURE & DEPENDENTE DE MV SAU PSEUDO-MV)

- Executabilele create cu Visual Basic 6 (VB6) nu rulează pe o mașină virtuală în modul în care înțelegem astăzi termenul de "mașină virtuală" pentru limbaje de programare cum ar fi Java (care utilizează Java Virtual Machine) sau C# (care rulează pe Common Language Runtime - CLR, parte a .NET Framework).
- În schimb, VB6 compilează codul sursă în cod de mașină nativ pentru procesorul sistemului de operare pe care rulează, de obicei Windows. Cu toate acestea, VB6 se bazează pe un set mare de componente runtime, cunoscute sub numele de VB6 Runtime, pentru a funcționa corect.
- Aceste biblioteci runtime trebuie să fie prezente pe sistemul pe care rulează executabilul pentru a furniza funcționalitățile necesare, cum ar fi gestionarea ferestrelor, controlul interfețelor utilizator și alte funcții de nivel înalt.
- Aceste componente runtime acționează ca un strat intermediar între aplicația VB6 și sistemul de operare.



# CUTTER DEZASAMBLARE

- Cum arată un punct de intrare (entry point) al unui executabil impur care își cere „mașina virtuală”?
- „adresele virtuale” sunt adresele la care codul și datele ar fi încărcate în memoria virtuală a unui proces dacă executabilul ar rula efectiv.

The screenshot shows the Cutter debugger interface with the title bar "Cutter – C:\Users\Elitebook\Desktop\Desktop\Project3.exe". The main window has tabs for "Functions", "Disassembly", "Search", "Imports", "Graph(entry0)", "Hexdump", and "Decompiler (entry0)". A red arrow points to the "Search" tab. The "Functions" pane lists three entries: "entry0" (selected), "sub.MSVBVM60.", and "sym.imp.MSVBV". The "Disassembly" pane displays assembly code for the "entry0" function, starting with:

```
entry0();
0x0040116c push    data.004012d4 ; 0x4012d4
0x00401171 call    sub.MSVBVM60._ThunRTMain ; sub.MSVBVM60._ThunRTMain
0x00401176 add     byte [eax], al
0x00401178 add     byte [eax], al
0x0040117a add     byte [eax], al
0x0040117c xor    byte [eax], al
0x0040117e add     byte [eax], al
0x00401180 inc    eax
0x00401181 add     byte [eax], al
0x00401183 add     byte [eax], al
0x00401185 add     byte [eax], al
0x00401187 add     byte [eax], cl
0x00401189 sahf
0x0040118a xor    dword [edx + 0x4667dcda], esp
0x00401190 movsb  byte es:[edi], byte ptr [esi]
0x00401191 jge    0x40114f
0x00401193 int1
0x00401194 lahf
0x00401195 push    0x678f
0x0040119a add     byte [eax], al
0x0040119c add     byte [eax], al
0x0040119e add     dword [eax], eax
0x004011a0 add     byte [eax], al
0x004011a2 add     byte [eax], al
0x004011a4 add     byte [eax], al
0x004011a6 add     byte [eax], al
0x004011a8 push    eax
```

# INFECTIE

## VIZIBIL CU UN CUTTER - ANALIZA A TREI FIŞIERE INFECTATE !

The image shows three separate windows of the Cutter debugger, each displaying the assembly code of a different file. The windows are arranged vertically.

- Jeffo.A:** The first window shows the assembly code for the file 'Virus.Win32.Jeffo'. It includes the entry point, various function definitions, and data sections. The assembly code is heavily obfuscated, typical of malware.
- Delf.ad:** The second window shows the assembly code for the file 'Virus.Win32.Delf.ad'. It also displays the entry point and several functions. The assembly is similar to Jeffo.A, with many direct jumps and calls.
- Bube.a:** The third window shows the assembly code for the file 'Virus.Win32.Bube.a'. This file appears to be a loader or a component of the infection, as it interacts with kernel32.dll functions like VirtualProtect and LoadLibrary.

Each window has a title bar, a menu bar (File, Edit, View, Windows, Debug, Tools, Help), and a toolbar with various icons. The main area of each window is a text-based disassembly view with syntax highlighting for assembly instructions and comments. The bottom of each window contains a navigation bar with tabs for Dashboard, Strings, Imports, Search, Disassembly, Graph(entry0), Hexdump, and Decomplier (entry0).

# CUTTER

## DESCRIDERE ȘI DEZASAMBLARE

Exemple de fișiere executabile infectate. Observați poziția relativă a punctului de intrare în execuție:

The image displays two screenshots of the Cutter debugger interface, comparing the assembly code of two executable files. Both windows show the 'Disassembly' tab.

**Left Window (Infectated File):**

- Entry Point:** entry0 (Address: 0x0040d495)
- Registers:** eax, al, esi, edi, ebp, esp
- Stack Frame:** StackFrame: 44
- Call Type:** cdecl
- Code:** Shows assembly instructions starting with add byte [eax], al and pushal, followed by various jumps and calls to other functions like fcn.00401000, fcn.00401030, etc.

**Right Window (Non-infectated File):**

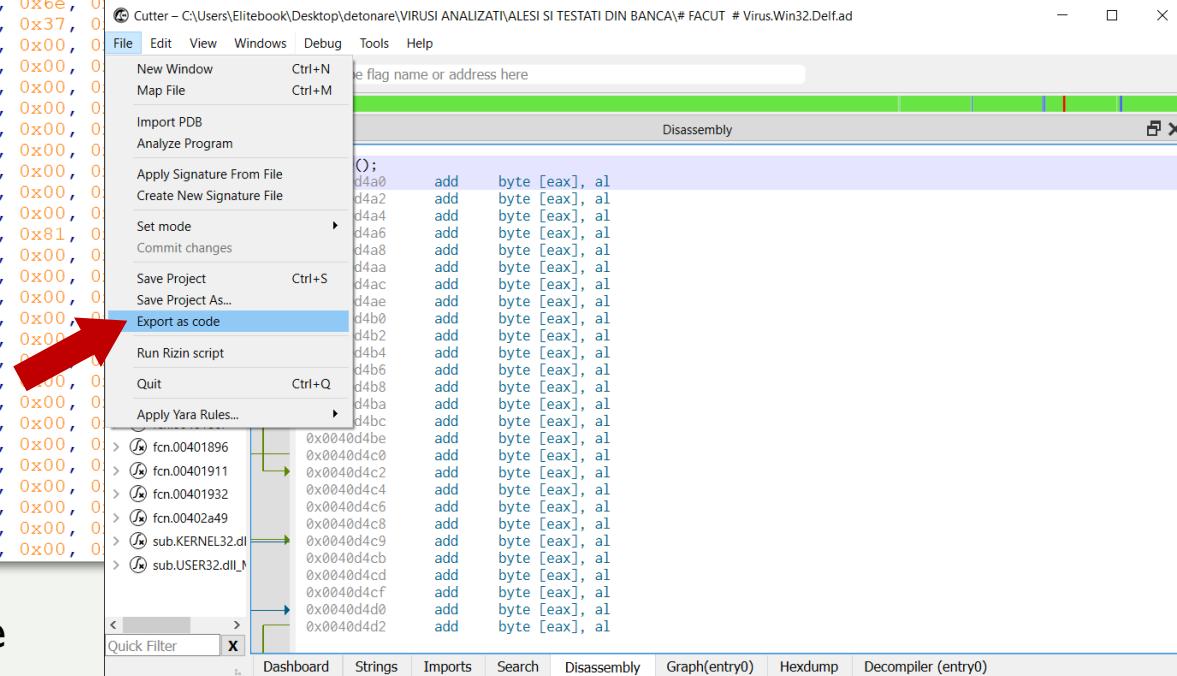
- Entry Point:** entry0 (Address: 0x004011f0)
- Registers:** eax, al, esi, edi, ebp, esp
- Stack Frame:** StackFrame: 44
- Call Type:** cdecl
- Code:** Shows assembly instructions starting with push ebp, mov esp, sub esp, add esp, and various jumps and calls to other functions like fcn.00401000, fcn.00401030, etc.

Dezasamblare (fisier infectat & ne-infectat)

# CUTTER

## MENIURI UTILE – EXPORTAȚI FIȘIERUL ANALIZAT CA SHELLCODE

## Shellcode in C++



# Shellcode in Python

# CUTTER GRAPH (VISUALIZARE)

Cutter - C:\Users\Elitebook\Desktop\Project3.exe

File Edit View Windows Debug Tools Help

Type flag name or address here

Graph(entry0)

Name void entry0();

entry0()

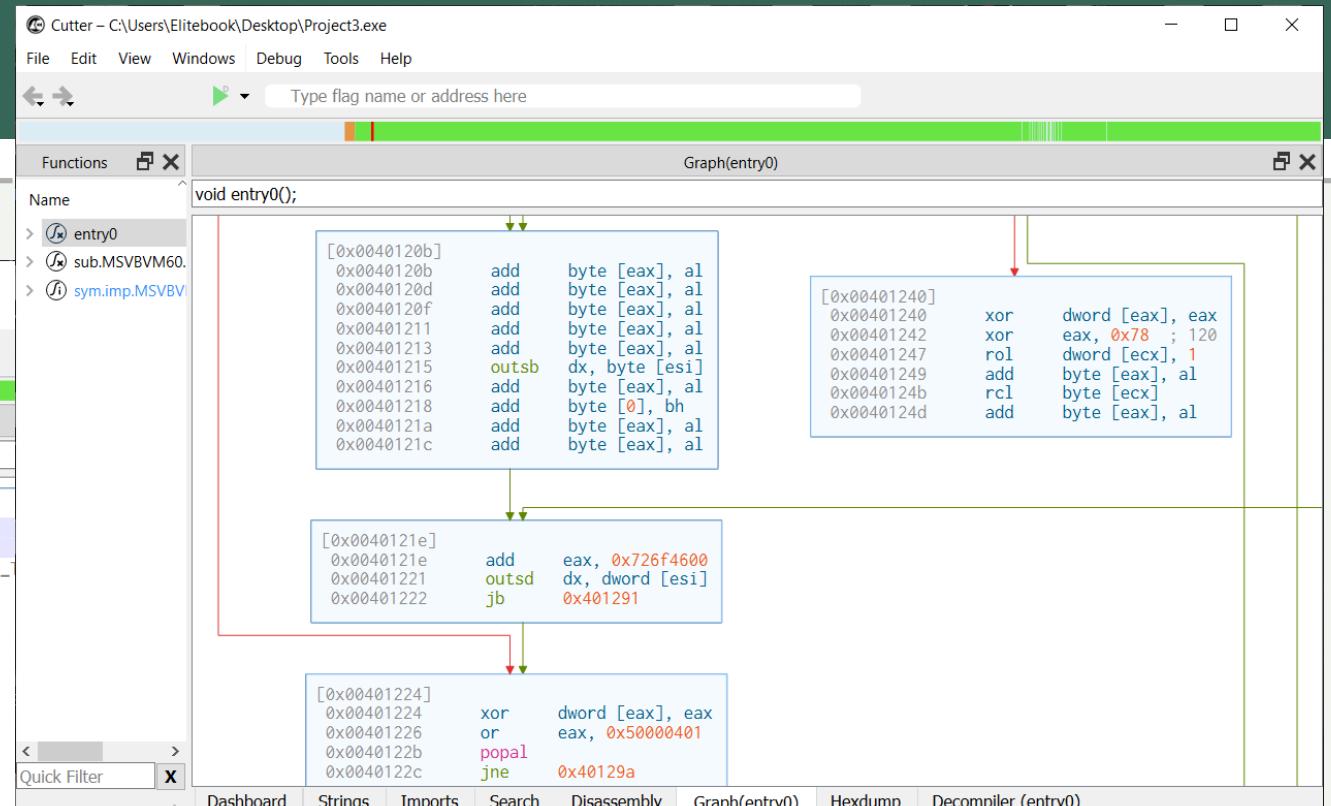
```
[0x0040116c]    entry0();
[0x0040116c]    push    data.004012d4 ; 0x4012d4
[0x00401171]    call    sub.MSVBVM60.DLL_ThunRTMain ; sub.MSVBVM60.DLL_
[0x00401176]    add     byte [eax], al
[0x00401178]    add     byte [eax], al
[0x0040117a]    add     byte [eax], al
[0x0040117c]    xor    byte [eax], al
[0x0040117e]    add     byte [eax], al
[0x00401180]    inc    eax
[0x00401181]    add     byte [eax], al
[0x00401183]    add     byte [eax], al
[0x00401185]    add     byte [eax], al
[0x00401187]    add     byte [eax], cl
[0x00401189]    sahf
[0x0040118a]    xor    dword [edx + 0x4667dcda], esp
[0x00401190]    movsb  byte es:[edi], byte ptr [esi]
[0x00401191]    jge    0x40114f

[0x00401193]    int1
[0x00401193]    lahf
[0x00401194]    push   0x678f
[0x00401195]    add    byte [eax], al
[0x0040119a]    add    byte [eax], al
[0x0040119c]    add    byte [eax], al
[0x0040119d]    add    byte [eax], al

[0x0040114f]    and   eax, __vbaVarMove ; 0x40100c
[0x0040114f]    jmp    dword [EVENT_SINK_QueryInterface] ; 0x40100c
```

Quick Filter X

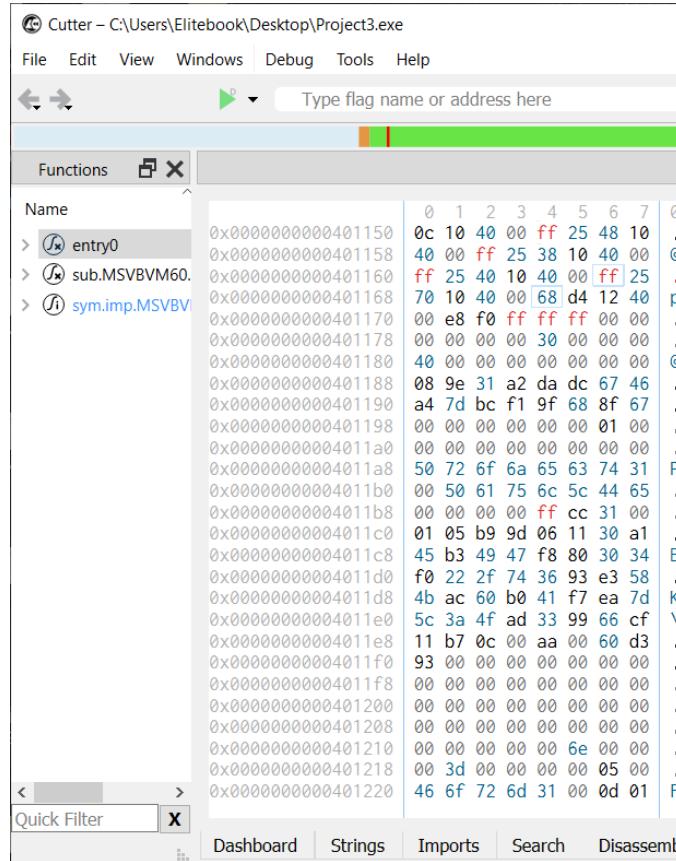
Dashboard Strings Imports Search Disassembly Graph(entry0) Hexdump Decompiler (entry0)



- Fiecare panou poate fi văzut ca un mic modul.

# CUTTER HEXDUMP

## ■ Vizualizare hex



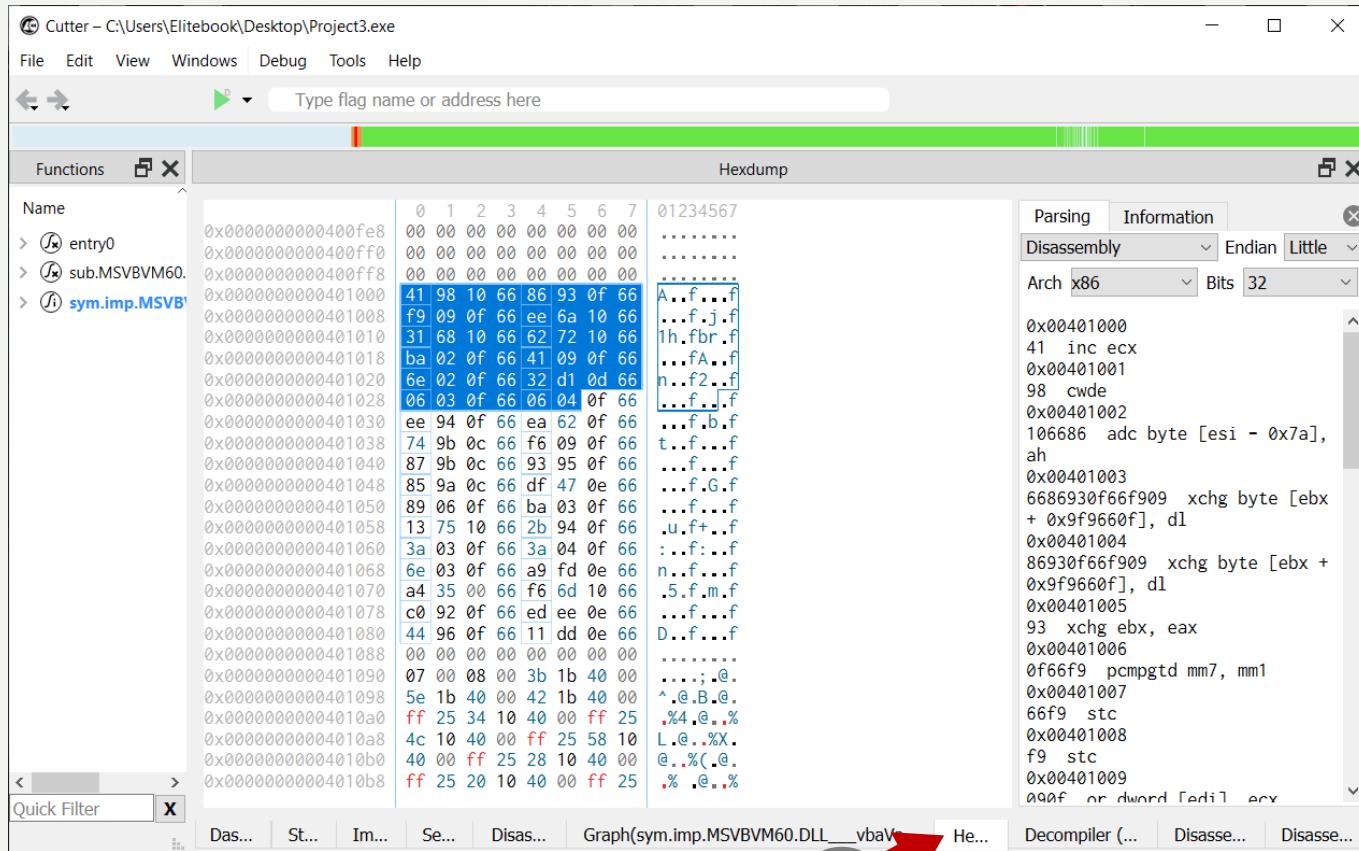
2

1

■ În timpul selecției se calculează o serie de indicatori (semnaturi hash)!

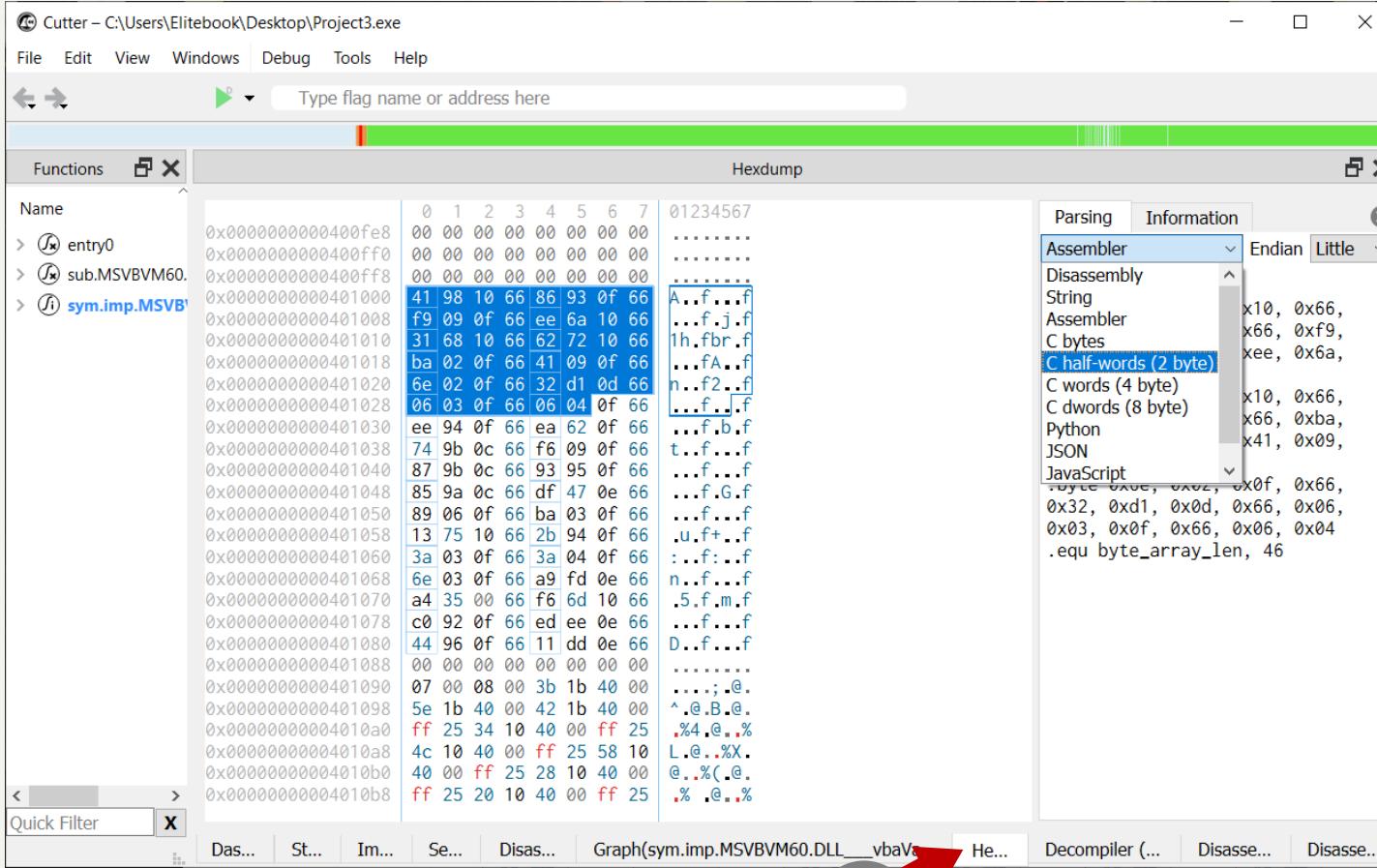
# CUTTER

## HEXDUMP – DEZASAMBLARE LA SELECTIE



- Oferă posibilitatea de demontare la selectarea sirului hexazecimal cu mouse-ul.

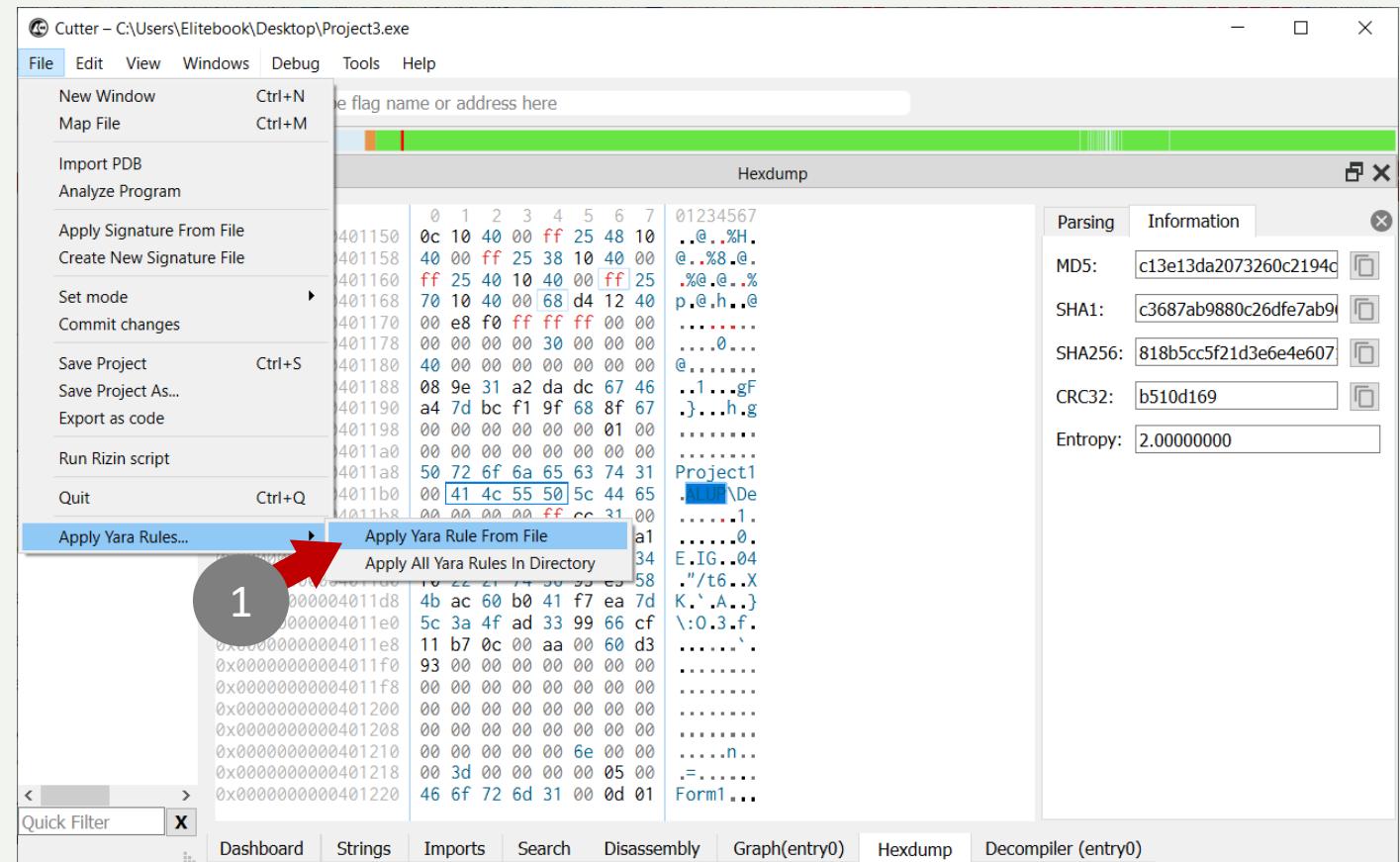
# CUTTER HEXDUMP – EXPORTARE IN COD SURSA



- Poate exporta selecția în codul sursă pentru diferite limbi de programare.

# CUTTER EXPORT YARA

- YARA este un instrument de securitate a sistemelor informatiche, folosit pentru identificarea și clasificarea malware-ului.
- Este bazat pe reguli care utilizează pattern-uri de șiruri de caractere și un set de expresii logice pentru a detecta anumite caracteristici sau comportamente ale fișierelor suspecte.
- YARA este folosit adesea de cercetătorii în securitatea cibernetică pentru a crea semnături care ajută la identificarea rapidă a amenințărilor specifice, a variantelor de malware sau a documentelor malicioase. Este extrem de versatil și poate fi integrat în diverse fluxuri de lucru de securitate și sisteme de analiză automată.



# CUTTER DECOMPILARE

```
/* jsdec pseudo code output */
/* C:\Users\Elitebook\Desktop\Project3.exe @ 0x401198 */
#include <stdint.h>

uint32_t rotate_left32 (uint32_t value, uint32_t count) {
    const uint32_t mask = (CHAR_BIT * sizeof (value)) - 1;
    count &= mask;
    return (value << count) | (value >> (-count & mask));
}

uint8_t rotate_left8 (uint8_t value, uint32_t count) {
    const uint8_t mask = (CHAR_BIT * sizeof (value)) - 1;
    count &= mask;
    return (value << count) | (value >> (-count & mask));
}

int32_t entry0 (void) {
    do {
        eax &= __vbaVarMove;
        al = MSVBVM60__DLL_ThunRTMain (data.004012d4);
        *(eax) += al;
        *(eax) += al;
        *(eax) += al;
        *(eax) ^= al;
        *(eax) += al;
        eax++;
        *(eax) += al;
        *(eax) += al;
        *(eax) += al;
    } while (1);
}
```

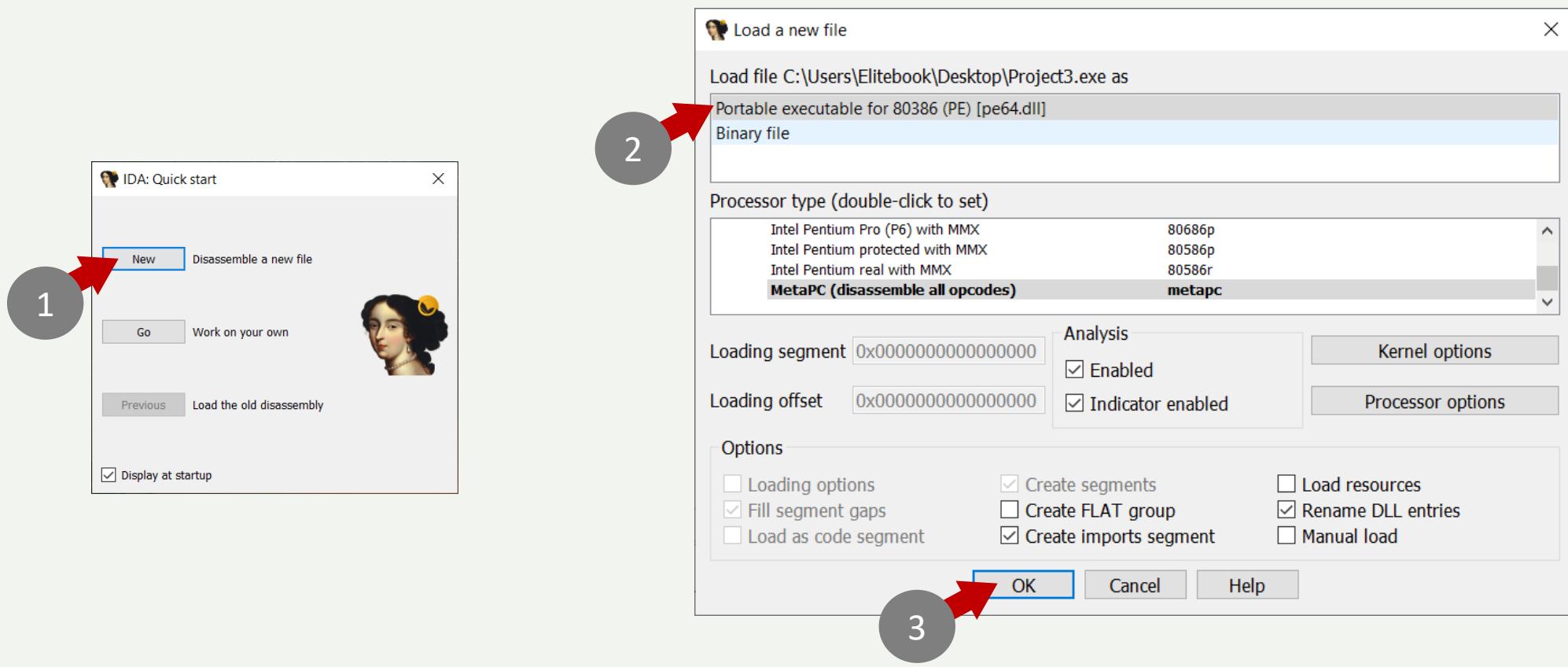
```
void entry0(void)
{
    uint32_t *puVar1;
    uint32_t uVar2;
    code *pcVar3;
    uint8_t uVar4;
    char cVar5;
    uint8_t *puVar6;
    char extraout_CL;
    undefined *unaff_ESI;
    undefined *unaff_EDI;
    undefined8 uVar7;
    code *pcStack_4;

    pcStack_4 = data.004012d4;
    uVar7 = sub.MSVBVM60.DLL_ThunRTMain();
    puVar6 = (uint8_t *)uVar7;
    uVar4 = (uint8_t)uVar7;
    *puVar6 = *puVar6 + uVar4;
    *puVar6 = *puVar6 + uVar4;
    *puVar6 = *puVar6 + uVar4;
    *puVar6 = *puVar6 ^ uVar4;
    *puVar6 = *puVar6 + uVar4;
    puVar6 = puVar6 + 1;
    cVar5 = (char)puVar6;
    *puVar6 = *puVar6 + cVar5;
    *puVar6 = *puVar6 + cVar5;
```

- Ghidra
- Jsdec

# IDA FREE

## DESCRIDERE SI DEZASAMBLARE



# IDA FREE INSPECTIE – FISIER VIRUSAT

IDA - calc.exe C:\Users\Elitebook\Desktop\detonare\VIRUSI ANALIZATI\VIRUSI FACUTI\Virus.Win32.Jeffo.A\Backup\Win32.Jeffo.A\CURAT\calc.exe

File Edit Jump Search View Debugger Options Windows Help

Local Windows debugger

Library function Regular function Instruction Data Unexplored External symbol Lumina function

Functions

Function name	Segment	Start	Length	Locals	Arguments	R	F	L	M	O	S	B	T	=
sub_1011990	.text	01011990	00000008	0000000C	00000000	R	.	.	.	.	.	B	.	.
sub_1011A18	.text	01011A18	00000002	00000000	00000004	R	.	.	.	.	.	.	.	.
sub_1011A3C	.text	01011A3C	00000004	00000008	0000000C	R	.	.	.	.	.	.	.	.
sub_1011A40	.text	01011A40	00000004	0000000C	0000000C	R	.	.	.	.	.	B	.	.
sub_1011B00	.text	01011B00	00000005	00000001	0000000C	R	.	.	.	.	.	B	.	.
sub_1011C90	.text	01011C90	00000027	00000024	0000000C	R	.	.	.	.	.	B	.	.
sub_1011E67	.text	01011E67	00000026	00000000	0000000C	R	.	.	.	.	.	B	.	.
sub_1011F1D	.text	01011F1D	00000021	00000044	00000000	R	.	.	.	.	.	B	.	.
sub_101208E	.text	0101208E	00000028	0000002C	00000008	R	.	.	.	.	.	B	.	.
sub_1012314	.text	01012314	0000008A	0000000C	00000008	R	.	.	.	.	.	B	.	.
sub_101239E	.text	0101239E	0000004D	00000010	00000008	R	.	.	.	.	.	B	.	.
sub_10123E8	.text	010123E8	0000008A	0000000C	00000008	R	.	.	.	.	.	B	.	.
start	.text	01012000	00000000	00000090	00000000	R	.	.	.	.	.	B	.	.
CxxFrameHandler	.text	01012659	00000006	00000000	00000000	R	.	.	.	.	.	B	.	.
CxxException	.text	01012670	00000006	00000000	00000000	R	.	.	.	.	.	T	.	.
sub_1012676	.text	01012676	00000048	00000008	00000004	R	.	.	.	.	.	T	.	.
sub_1012600	.text	01012600	00000095	00000004	00000010	R	.	.	.	.	.	T	.	.
sub_1012770	.text	01012770	00000034	00000000	00000010	R	.	.	.	.	.	T	.	.
_XcptFilter	.text	010127A4	00000000	00000000	00000000	R	.	.	.	.	.	T	.	.
_initterm	.text	010127AA	00000006	00000000	00000008	R	.	.	.	.	.	T	.	.
sub_1012700	.text	01012700	00000000	00000000	00000000	R	.	.	.	.	.	T	.	.
UserDefinedErrorFunction	.text	010127C2	00000003	00000000	00000000	R	.	.	.	.	.	T	.	.
SEH_prolog	.text	010127C8	00000039	00000010	00000008	R	.	L	.	.	.	B	.	.
SEH_epilog	.text	01012801	00000011	00000000	00000000	R	.	L	.	.	.	T	.	.
operator delete(void *)	.text	01012812	00000006	00000000	00000000	R	.	.	.	.	.	T	.	.
sub_1012818	.text	01012818	0000005E	00000034	00000010	R	.	.	.	.	.	B	.	.
sub_1012876	.text	01012876	00000060	0000002C	00000010	R	.	.	.	.	.	B	.	.
type_info::type_info(void)	.text	01012806	00000006	00000000	00000000	R	.	.	.	.	.	T	.	.
_controlP	.text	010128DC	00000006	00000000	00000008	R	.	.	.	.	.	T	.	.
_except_handler3	.text	010128E2	00000006	00000000	00000000	R	.	.	.	.	.	T	.	.
terminated(void)	.text	010128E8	00000006	00000000	00000000	R	.	.	.	.	.	T	.	.

Line 158 of 177, /start

Output

100.00% (398,364) (50,624) 00011875.01012475: (synchronous)

Please check the Edit/Plugins menu for more information.

Using FLIRT signature: SEH for vc7-14

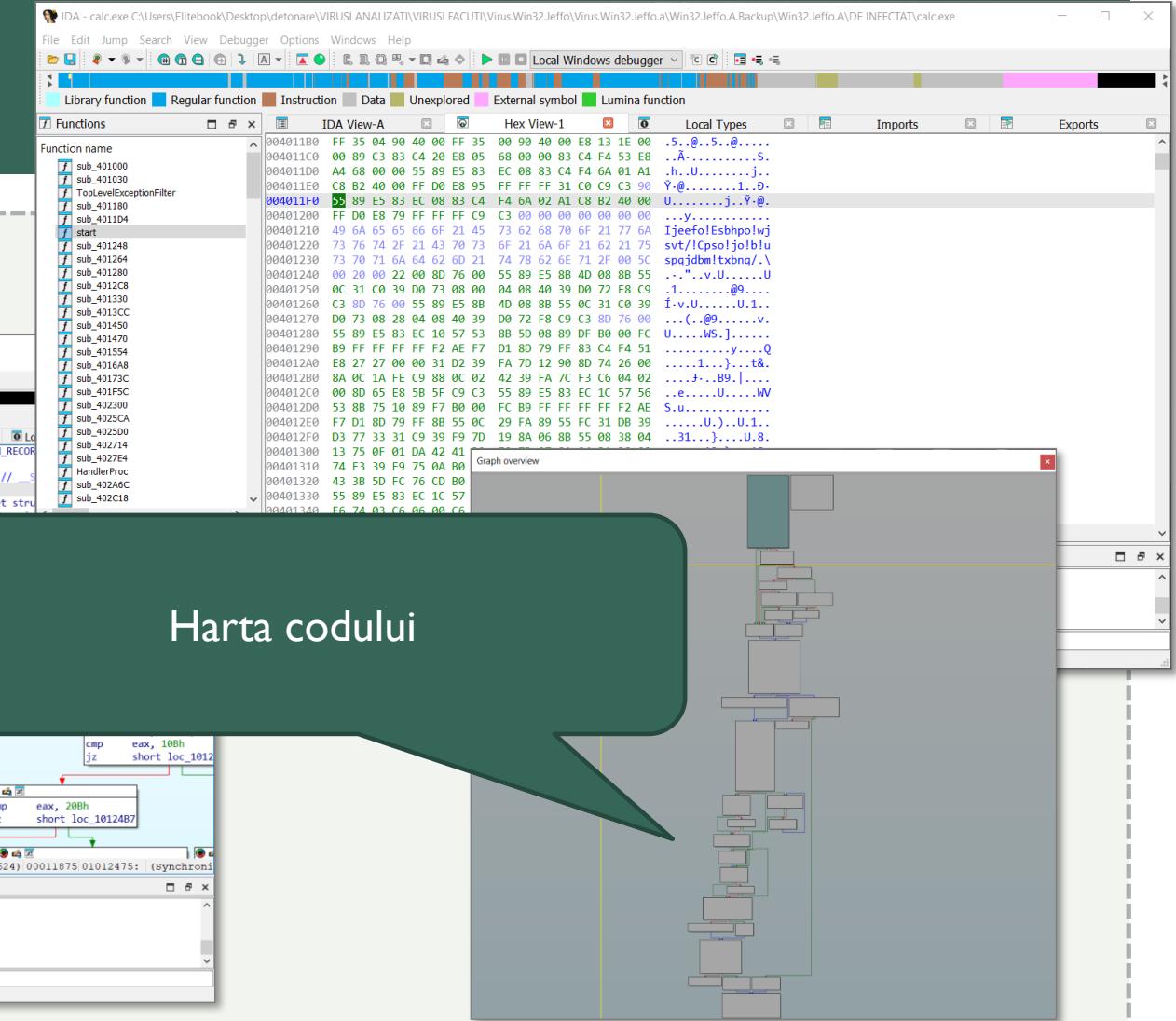
Propagating type information...

Function argument information has been propagated

The initial autoanalysis has been finished.

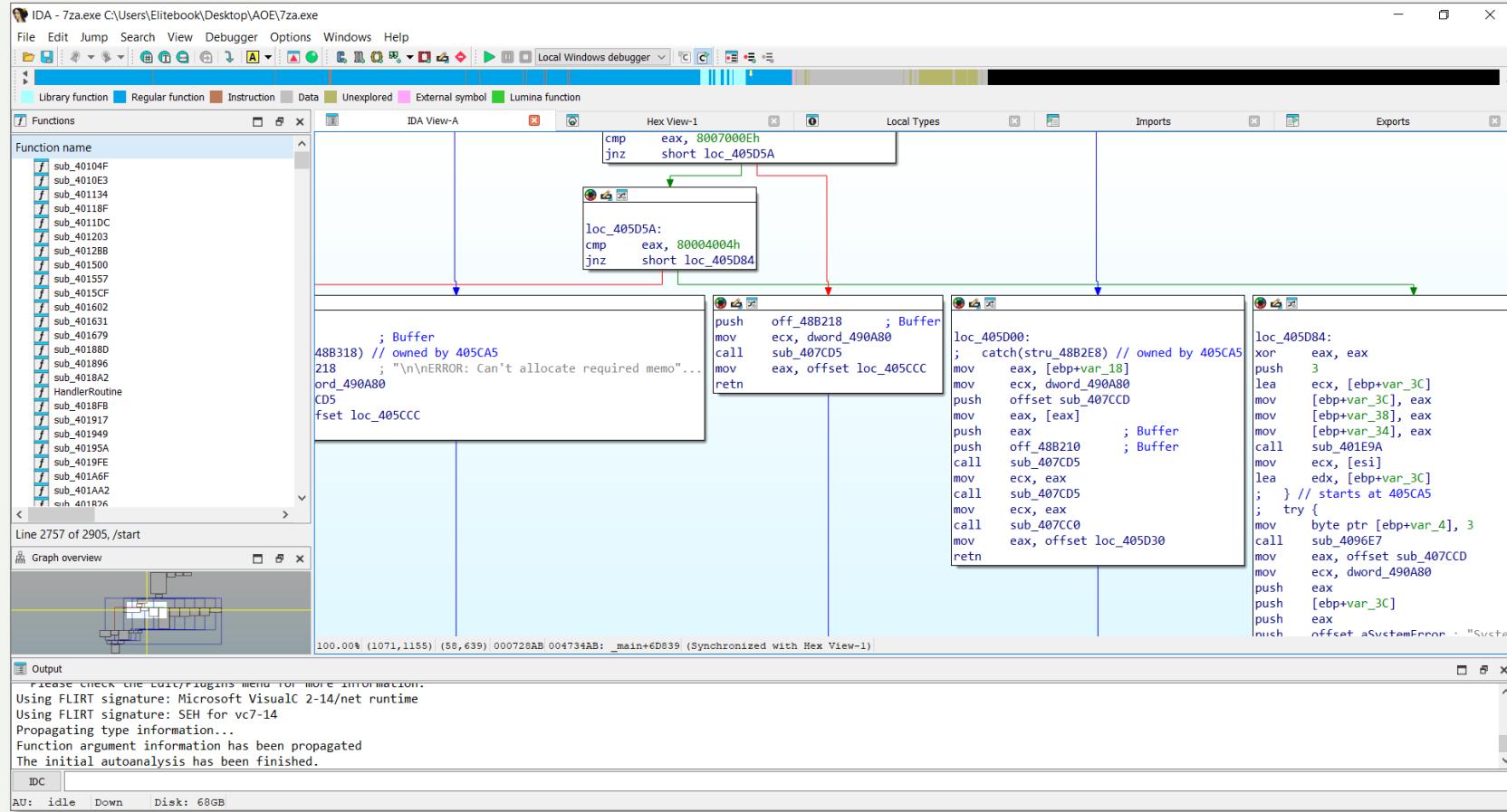
IDC

AU: idle Down Disk: 62GB



# IDA FREE

## DEZASAMBLARE – EXECUTABILE PURE

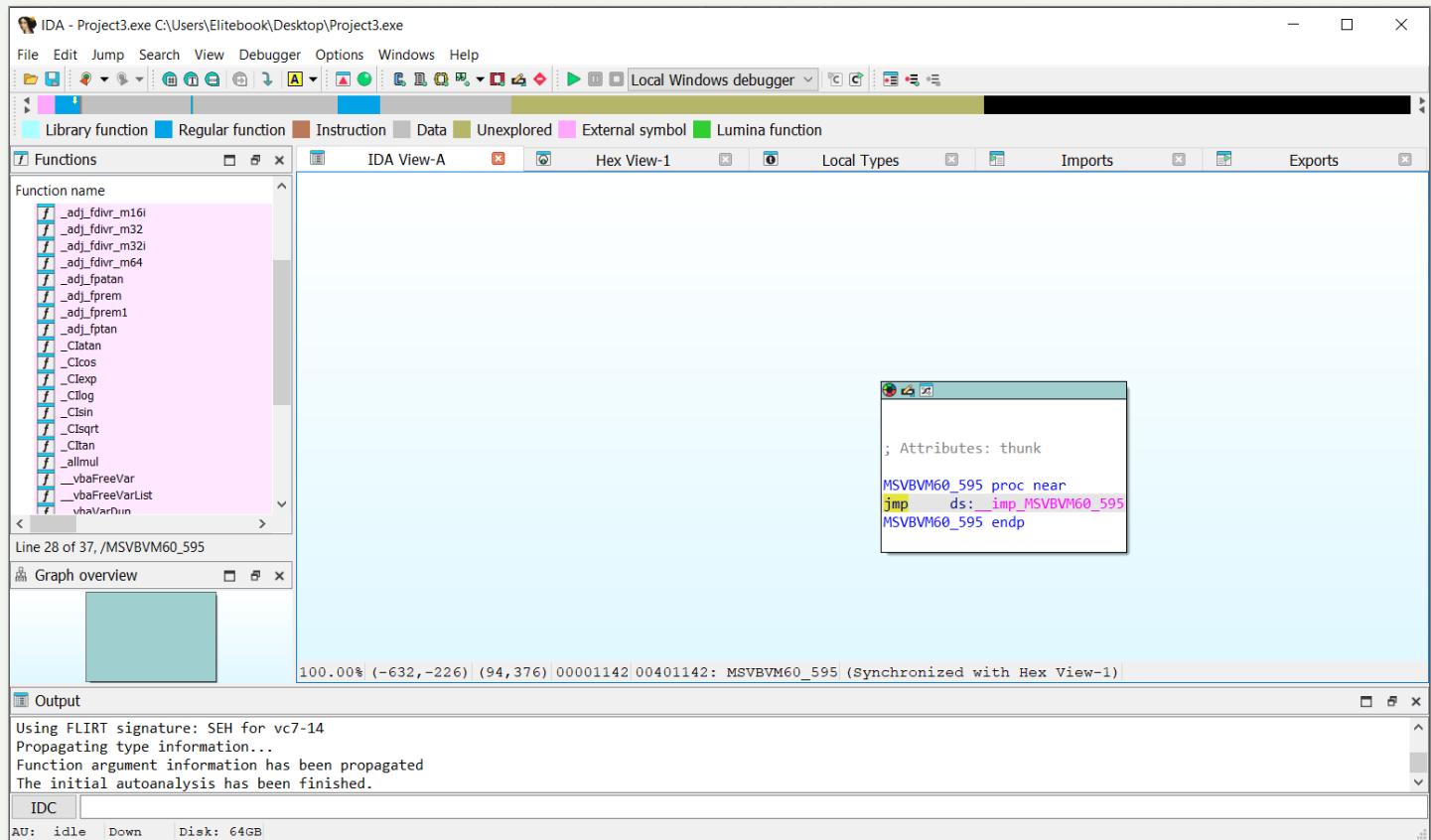


- Relativ independent cu utilizarea importurilor.
- Permite IDA să mapeze codul.

# IDA FREE

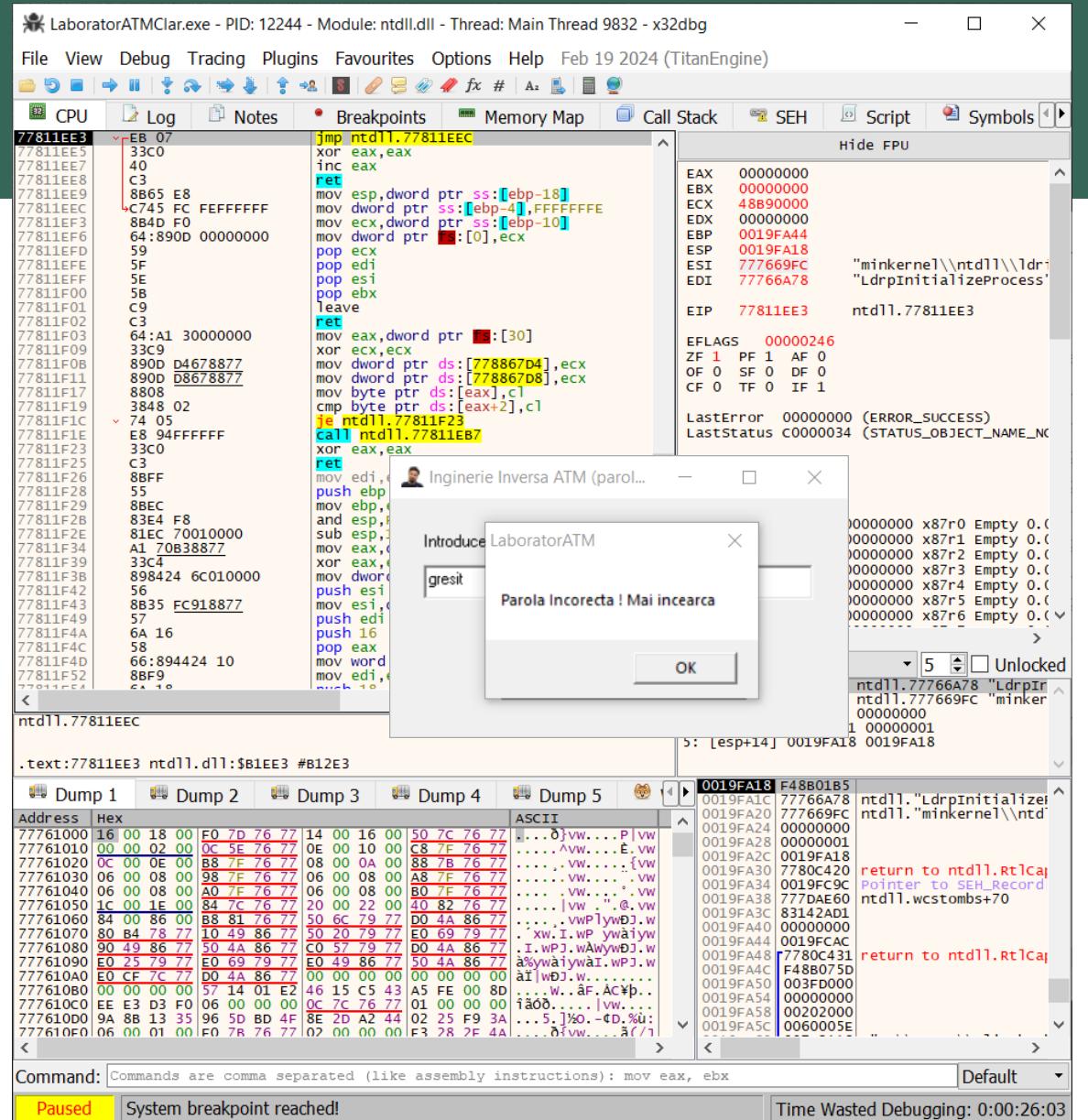
## DEZASAMBLARE – EXECUTABILE INPURE (MSVBVM60.DLL)

- Executabile dependente de mașini virtuale sau de un sistem intermediar între OS și executabil.
- IDA nu știe să mapeze codul fără suportul intermediar.



# PETICIRI DE EXECUTABILE IDA & CUTTER & X32DBG

- CPU - Panoul CPU este probabil cel mai important și afișează instrucțiunile mașină ale programului (codul assembly), permitând utilizatorului să navegeze prin ele, să pună puncte de oprire (breakpoints) și să urmărească execuția pas cu pas. Acest panou include de obicei și vizualizarea regisrelor procesorului, arătând starea curentă a acestora.
- Registre - Afisează starea curentă a regisrelor CPU. Acestea includ regisre generale (cum ar fi EAX, EBX pentru arhitectura x86), regisre de index și de bază, regisre de segment, pointerul de instrucțiuni (EIP), și flags-urile. Modificările în regisre sunt adesea evidențiate pentru a facilita urmărirea modificărilor de stare.
- Dump - Panoul de dump arată conținutul memoriei la o anumită adresă. Este util pentru examinarea și modificarea datelor în memorie. Utilizatorii pot căuta anumite valori sau stringuri în acest panou.
- Stack - Afisează conținutul stack-ului curent al programului, oferind o vedere asupra apelurilor de funcții și a datelor locale. Acest panou este esențial pentru a urmări cum sunt gestionate apelurile de funcții și pentru a identifica posibile probleme legate de stack.



# BIBLIOGRAFIE / RESURSE

- Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.
- Paul A. Gagniuc. *An Introduction to Programming Languages: Simultaneous Learning in Multiple Coding Environments*. Synthesis Lectures on Computer Science. Springer International Publishing, 2023, pp. 1-280.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in MATLAB*, Springer, 2024, pp. 1-255.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Python*, Springer, 2024, pp. 1-245.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Javascript*, Springer, 2024, pp. 1-240.
- Paul A. Gagniuc. *Markov chains: from theory to implementation and experimentation*. Hoboken, NJ, John Wiley & Sons, USA, 2017, ISBN: 978-1-119-38755-8.

<https://github.com/gagniuc>

