

C.11 ANALIZA DINAMICĂ SI INGINERIA INVERSĂ A COMPORTAMENTULUI

PAUL A. GAGNIUC



Academia Tehnică Militară „Ferdinand I”

PRINCIPALELE PĂRȚI ALE PREZENTĂRII

C.11 Detonarea malware și ingineria inversă a comportamentului:

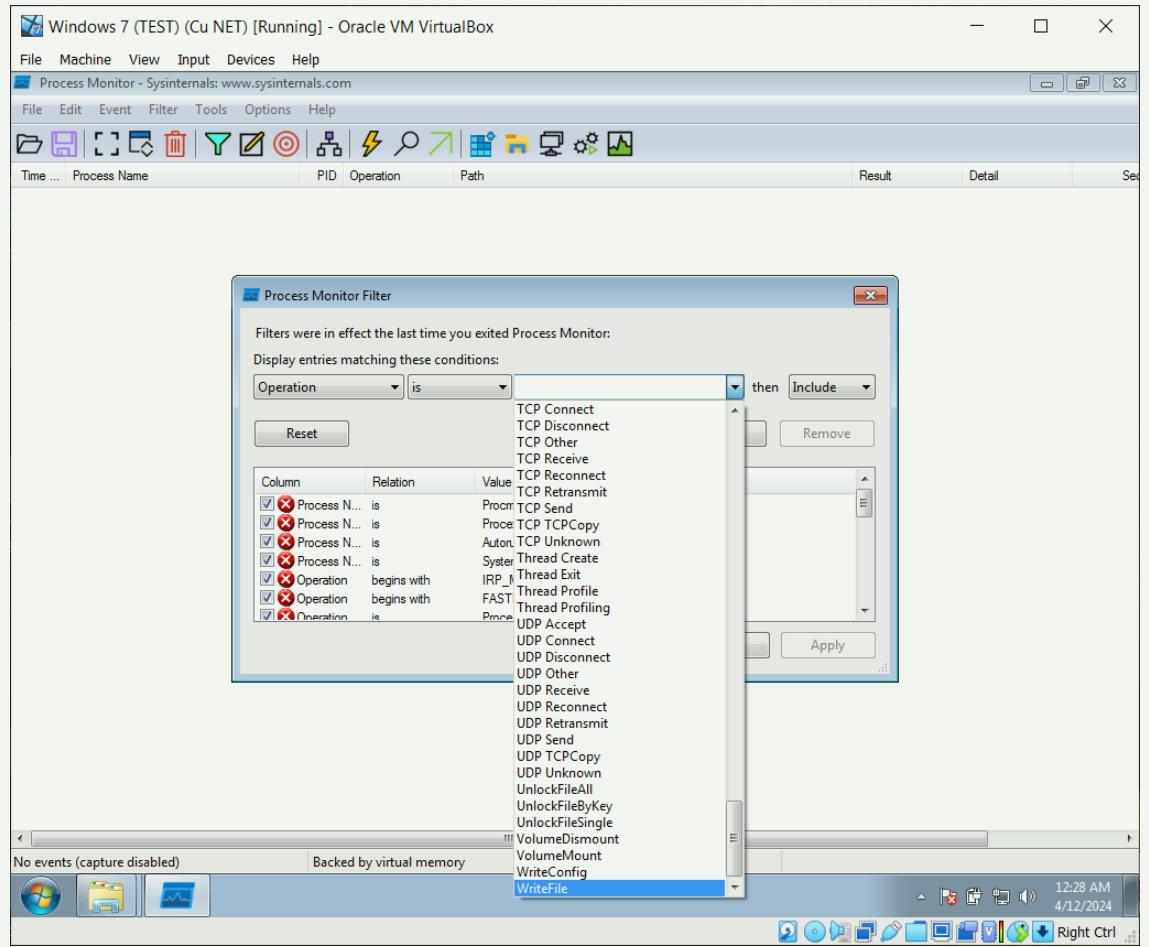
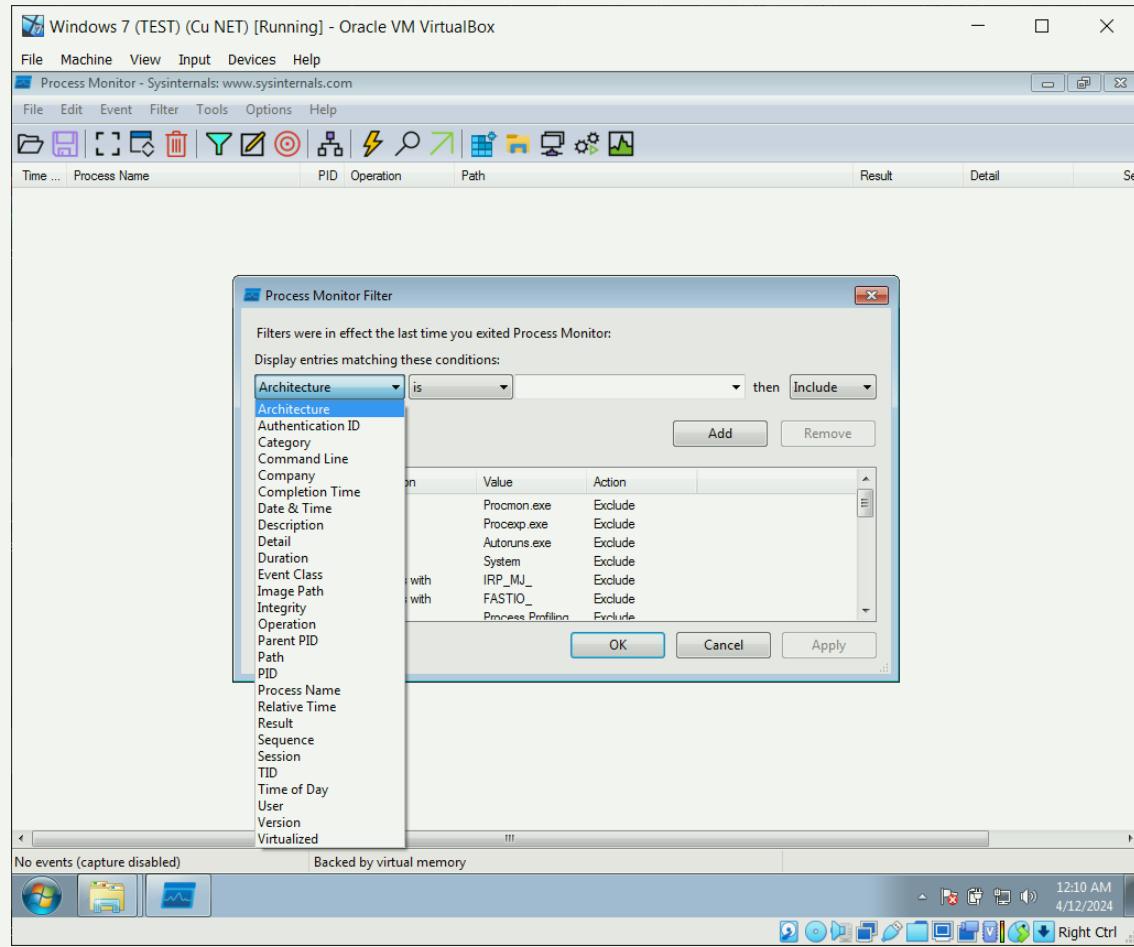
- **C.11.1 FILTRE PE EVENIMENTELE SISTEMULUI DE OPERARE CU PROCESS MONITOR**
- **C.11.2 DETONAREA ȘI INSPECȚIA COMPORTAMENTALĂ A APLICAȚIILOR MALWARE**
- **C.11.3 CAPTAREA EVENIMENTELOR EFEMERE ȘI ELIMINAREA ZGOMOTULUI**
- **C.11.4 DETONAREA ȘI ANALIZA VIRUȘILOR PRIN UTILIZAREA UNUI HONEYPOT**

C.10.1

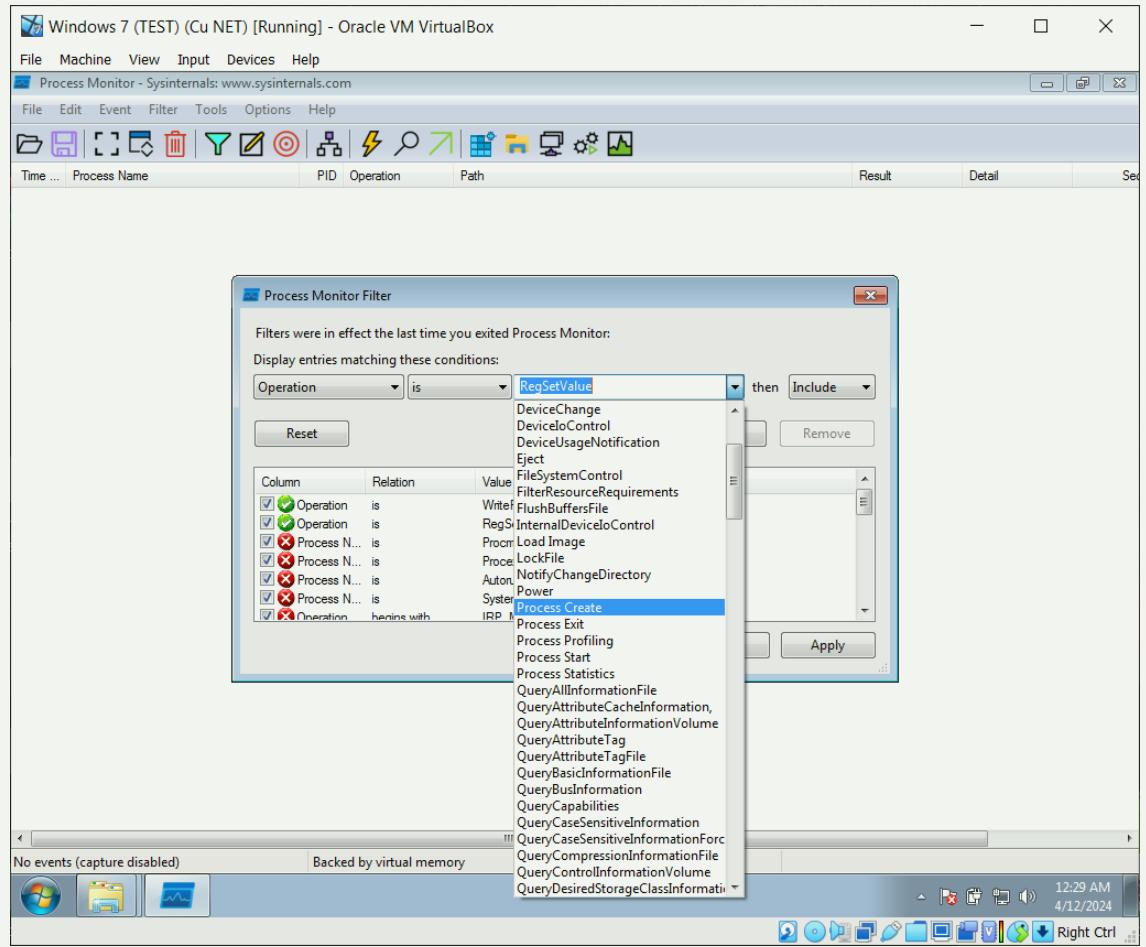
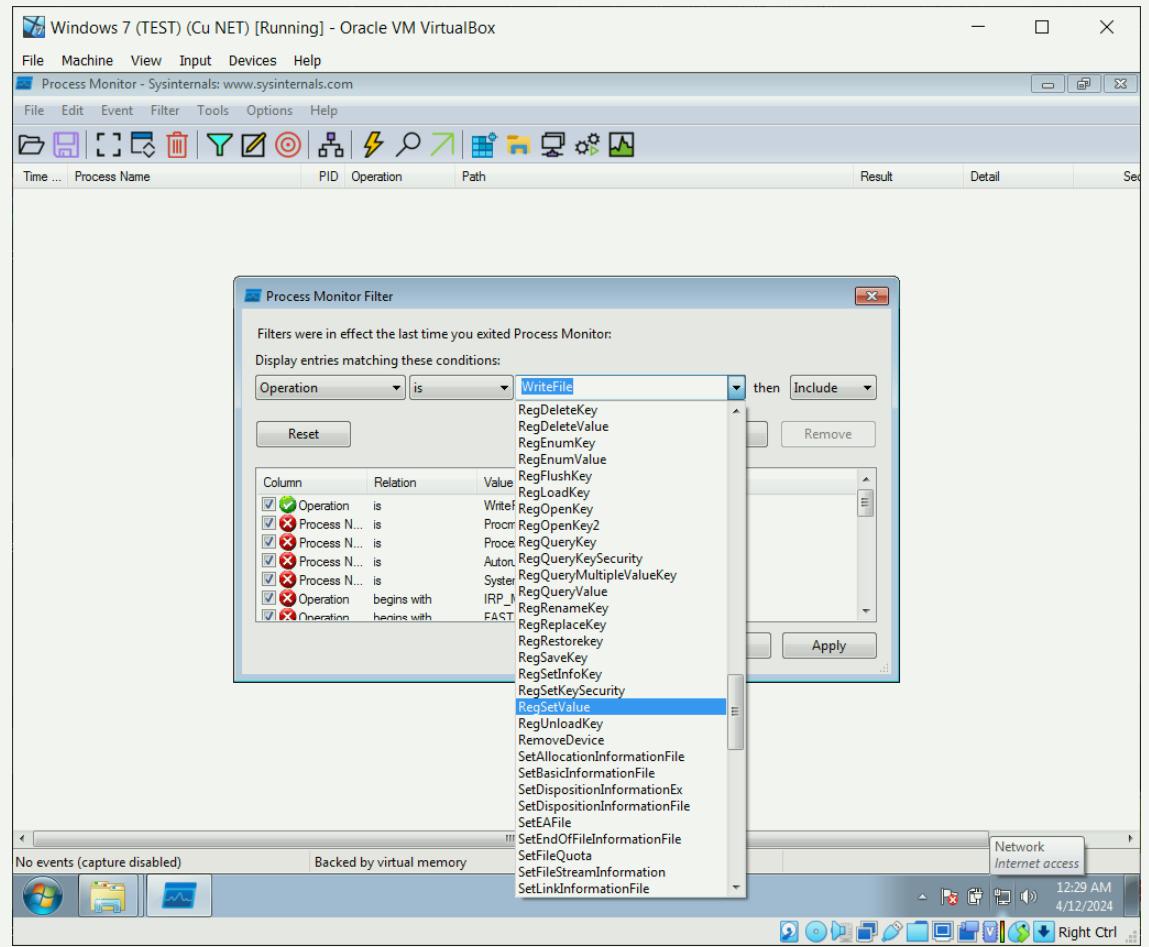
FILTRE PE EVENIMENTELE SISTEMULUI DE OPERARE CU PROCESS MONITOR



PROCESS MONITOR FILTRE



PROCESS MONITOR OPERATION





Ingineria Inversă în Analiza Malware folosind Filtrele ProMon

Filtrarea după Numele Procesului (Process Name Filtering)

- Analizează activitățile specifice ale proceselor suspecte
- Izolează comportamentul malware-ului

Accesul la Registrul (Registry Activity)

- Monitorizează modificările în registru
- Vizează locațiile frecvent accesate de malware

Activitatea de Rețea (Network Activity)

- Filtrează și supraveghează conexiunile de rețea
- Detectează comunicațiile neobișnuite sau către adrese IP suspecte

Modificările Fișierelor Sistem (File System Changes)

- Detectează crearea, modificarea sau ștergerea de fișiere
- Se concentrează pe locații critice care semnalează acțiuni de malware

Operațiuni de Injecție de Cod (Code Injection Operations)

- Identifică încercările de injectare a codului în alte procese
- O metodă comună utilizată de malware pentru a se ascunde și a executa cod malicioz

Activități Suspicioase de Thread (Suspicious Thread Activity)

- Monitorizează crearea de noi thread-uri în procese
- Indică posibile activități malicioase desfășurate în secret

Filtrarea după Căi și Tipuri de Fișiere Specifice (Path and File Type Filtering)

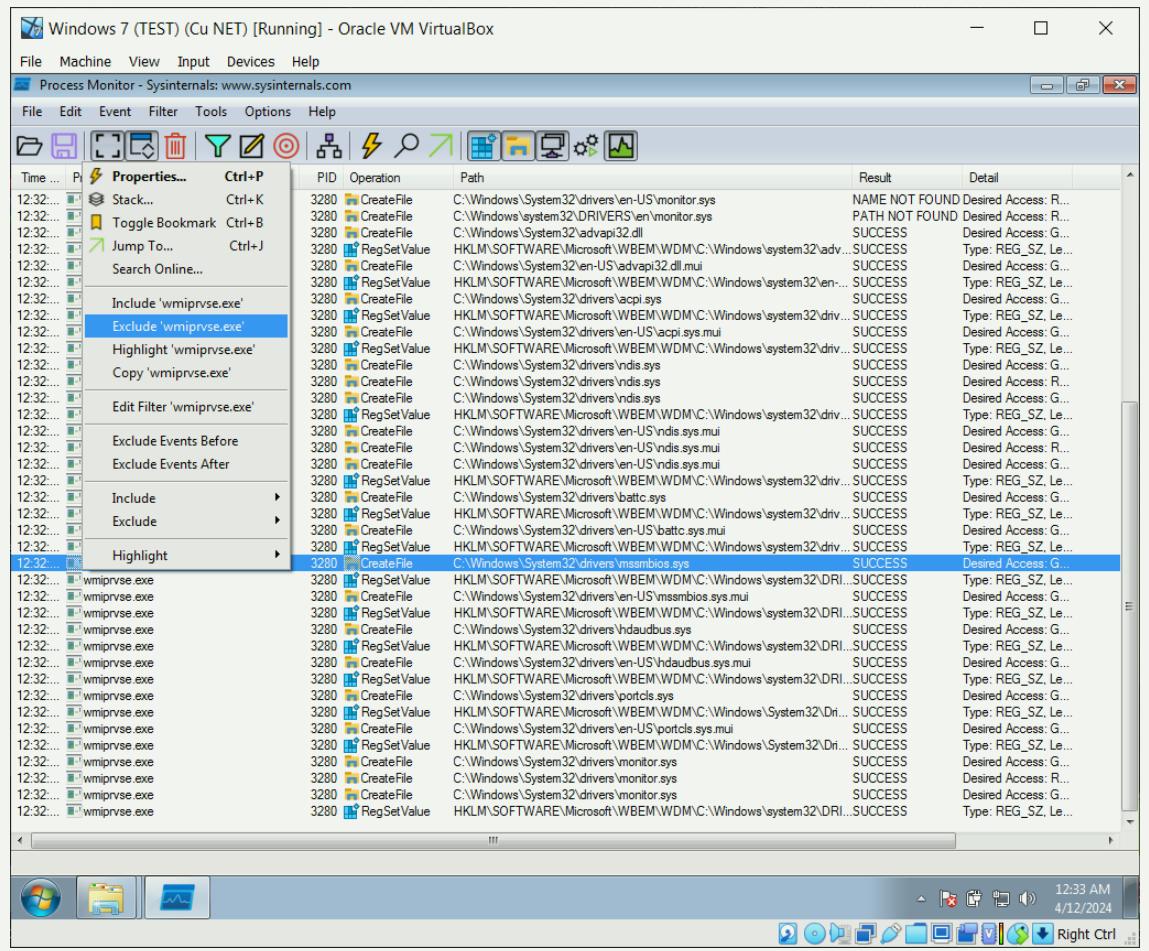
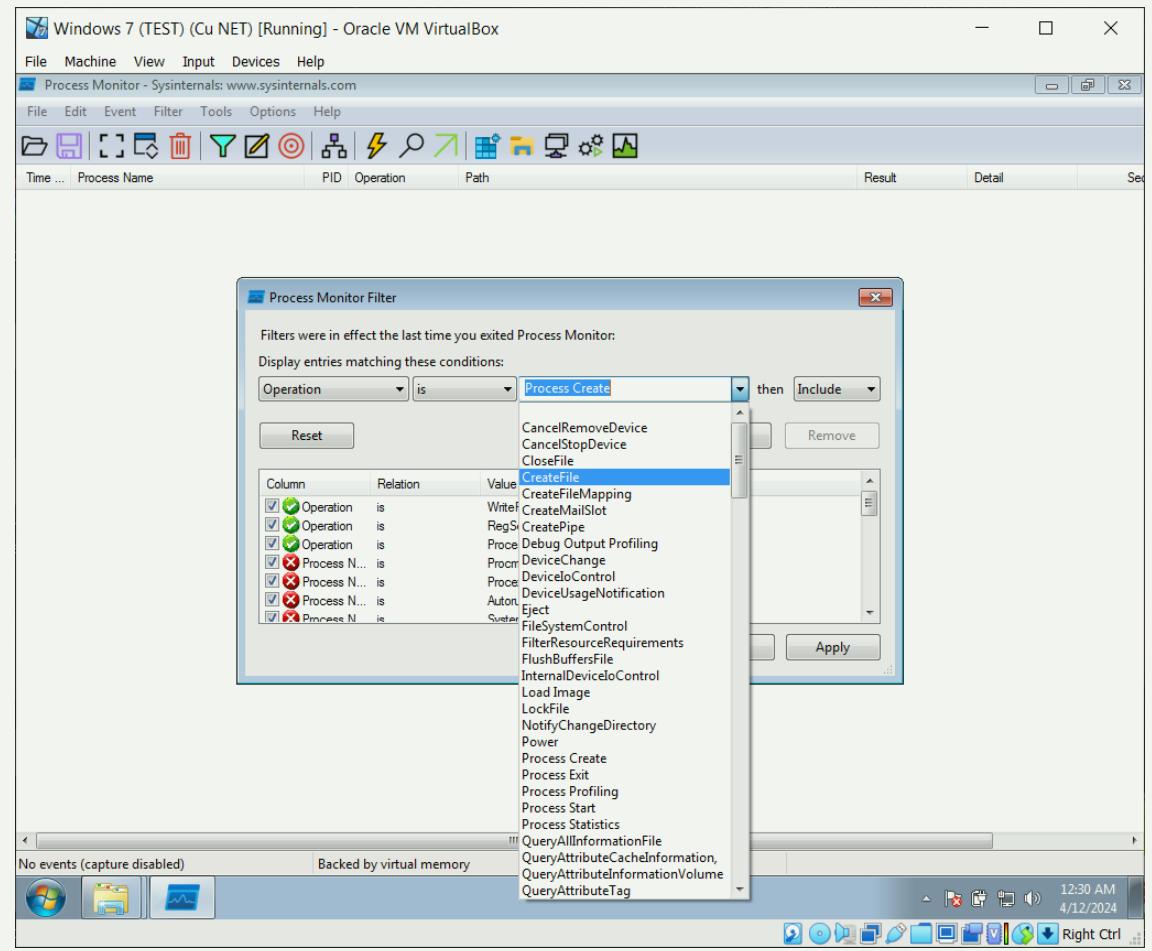
- Se concentrează pe accesul la fișiere executabile (.exe, .dll) sau scripturi (.js, .vbs) în locații neașteptate sau temporare
- Semnalează activitate malicioasă

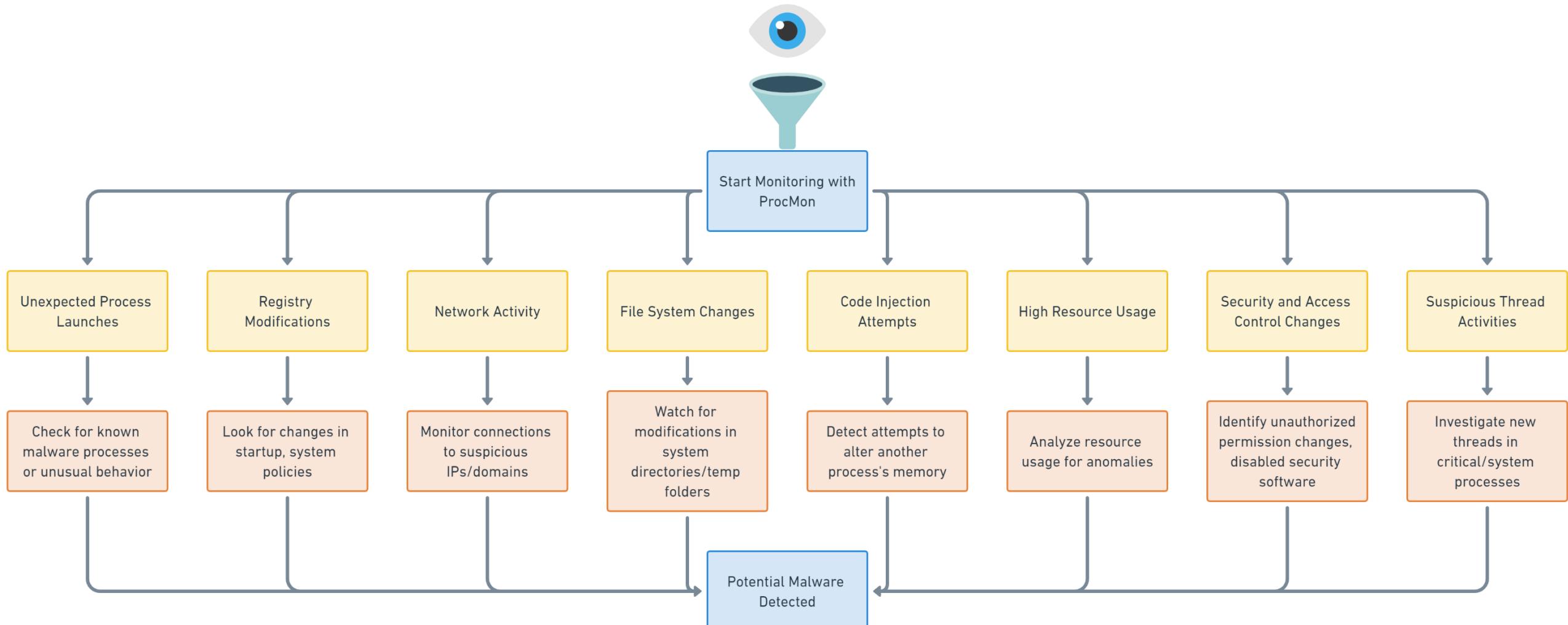
Modificările de Securitate (Security Changes)

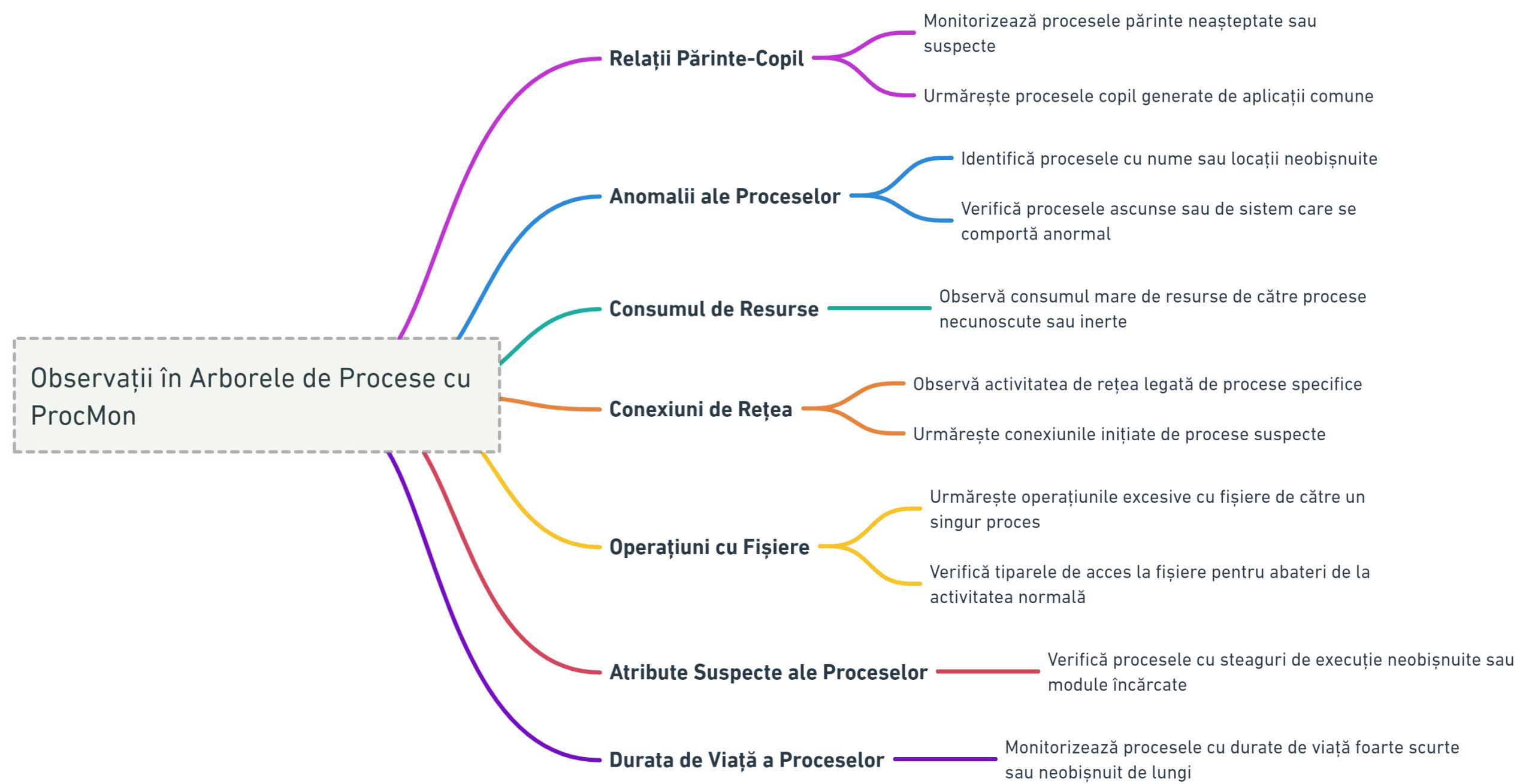
- Supraveghează schimbările în permisiunile fișierelor sau directoarelor
- Sugeraază încercări de evitare a măsurilor de securitate

PROCESS MONITOR

OPERATIONS / INCLUDE / EXCLUDE

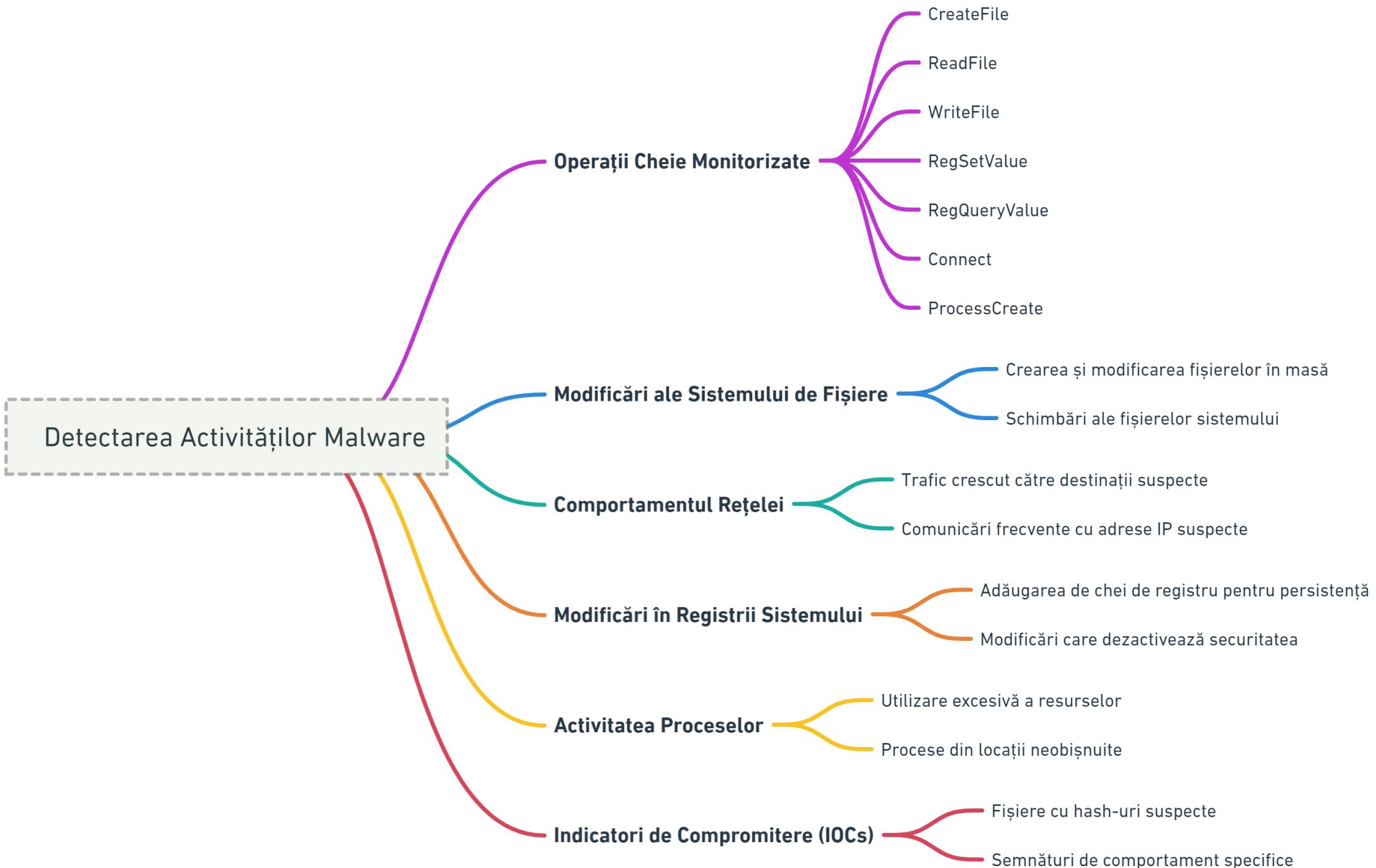






Opțiuni Importante ale Filtrului Monitorului de Procese

- Arhitectură:** Filtrează după arhitectura procesorului Operării: Include sau exclude evenimente bazate pe tipul de procesor
- Linia de Comandă:** Filtrează procesele după argumentele liniei de comandă Operării: Include sau exclude procese bazate pe argumentele specificate
- Companie:** Filtrează după compania care a semnat procesul Operării: Include sau exclude procese bazate pe semnatura companiei
- Dată & Timp:** Filtrează evenimentele după data și ora apariției Operării: Include sau exclude evenimente bazate pe marcatul temporal
- Descriere:** Filtrează după câmpul descrierii în proprietățile procesului Operării: Include sau exclude procese bazate pe descriere
- Durată:** Filtrează după durata de timp în care un eveniment are loc Operării: Include sau exclude evenimente bazate pe durată
- Cale:** Filtrează după calea fișierului asociat cu evenimentul Operării: Include sau exclude evenimente bazate pe calea specificată
- Numele Procesului:** Filtrează după numele procesului Operării: Include sau exclude procese bazate pe nume



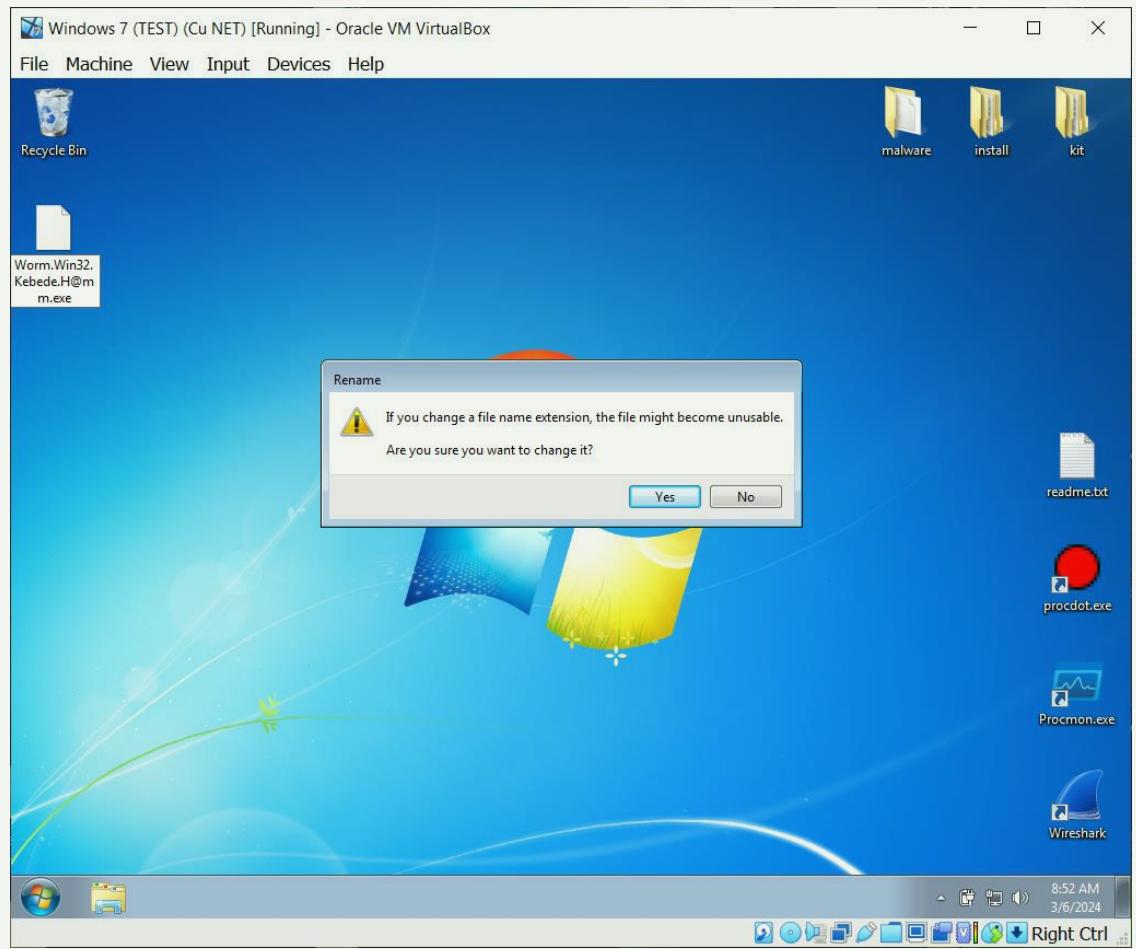
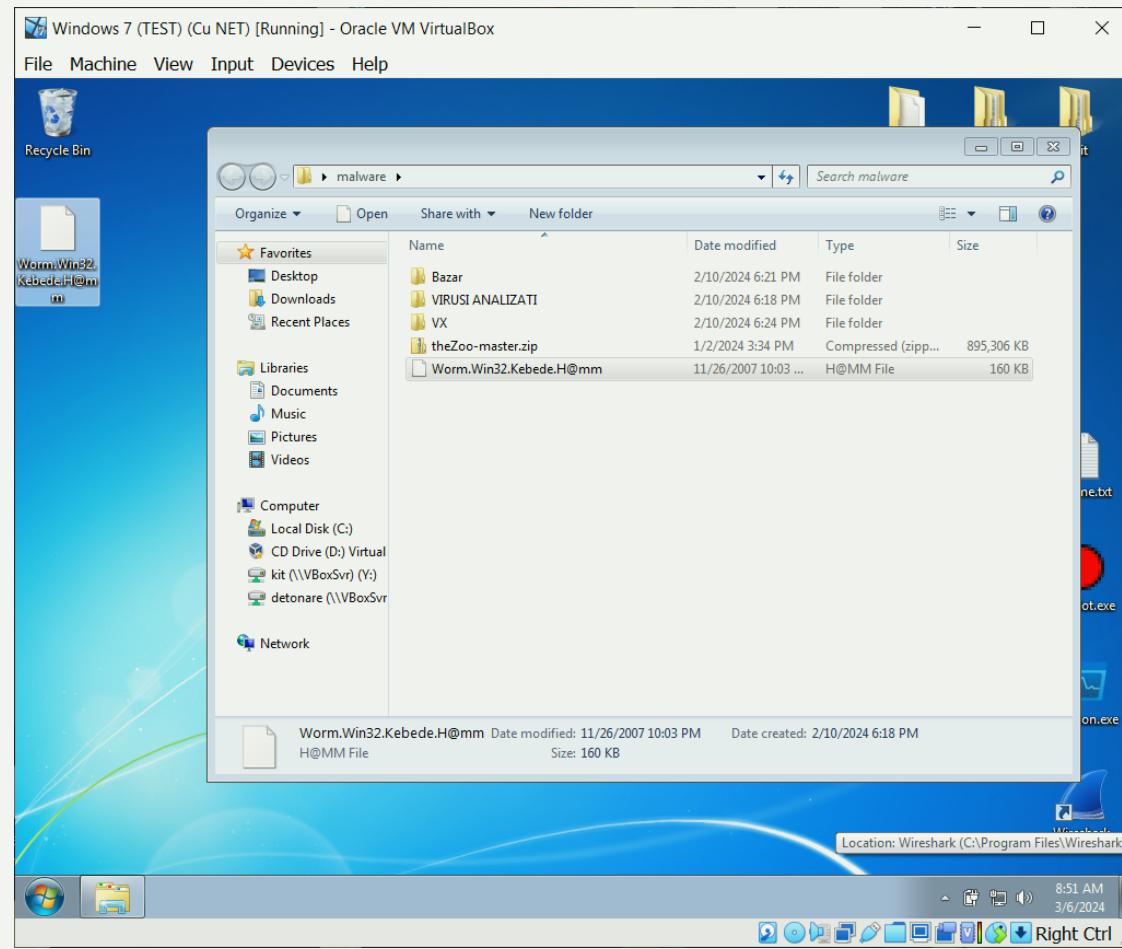
c.11.2

DETONAREA SI INSPECTIA COMPORTAMENTALĂ A APLICAȚIILOR MALWARE



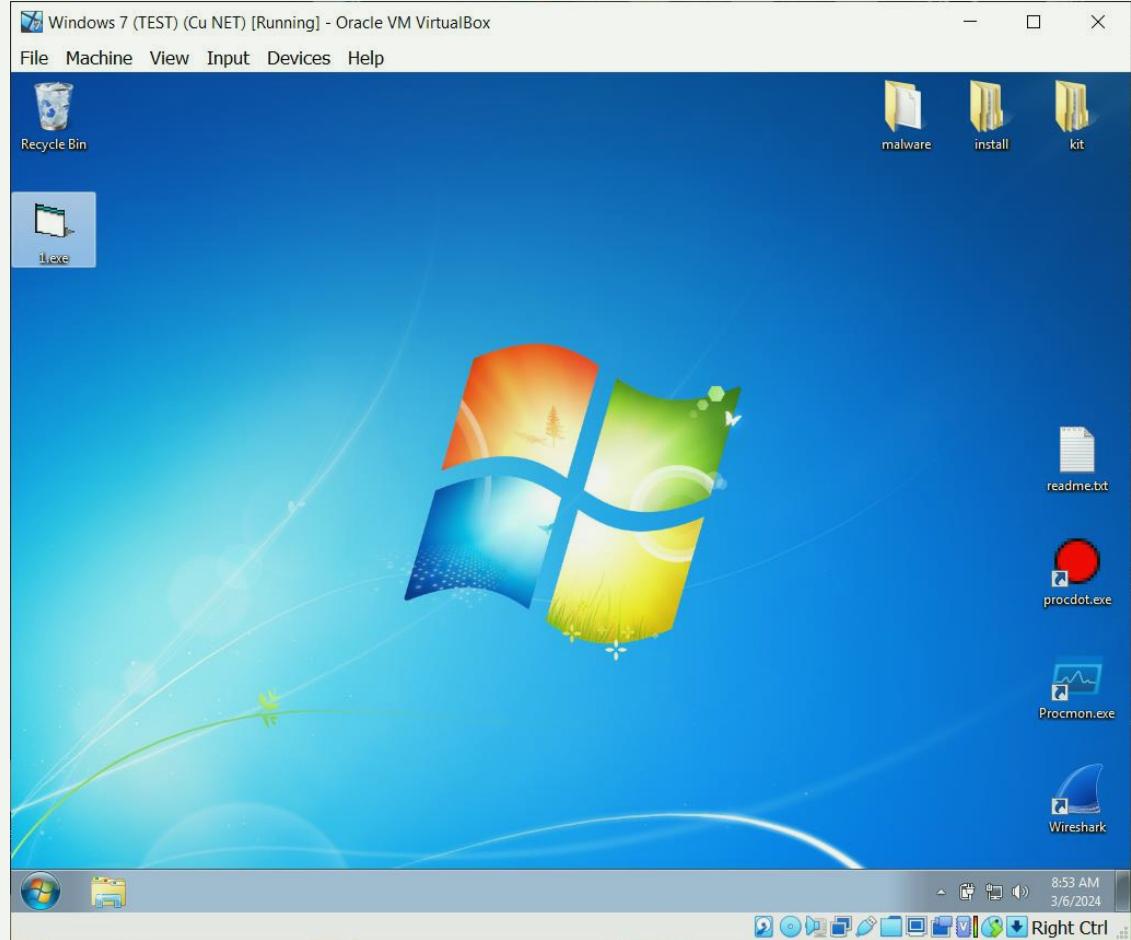
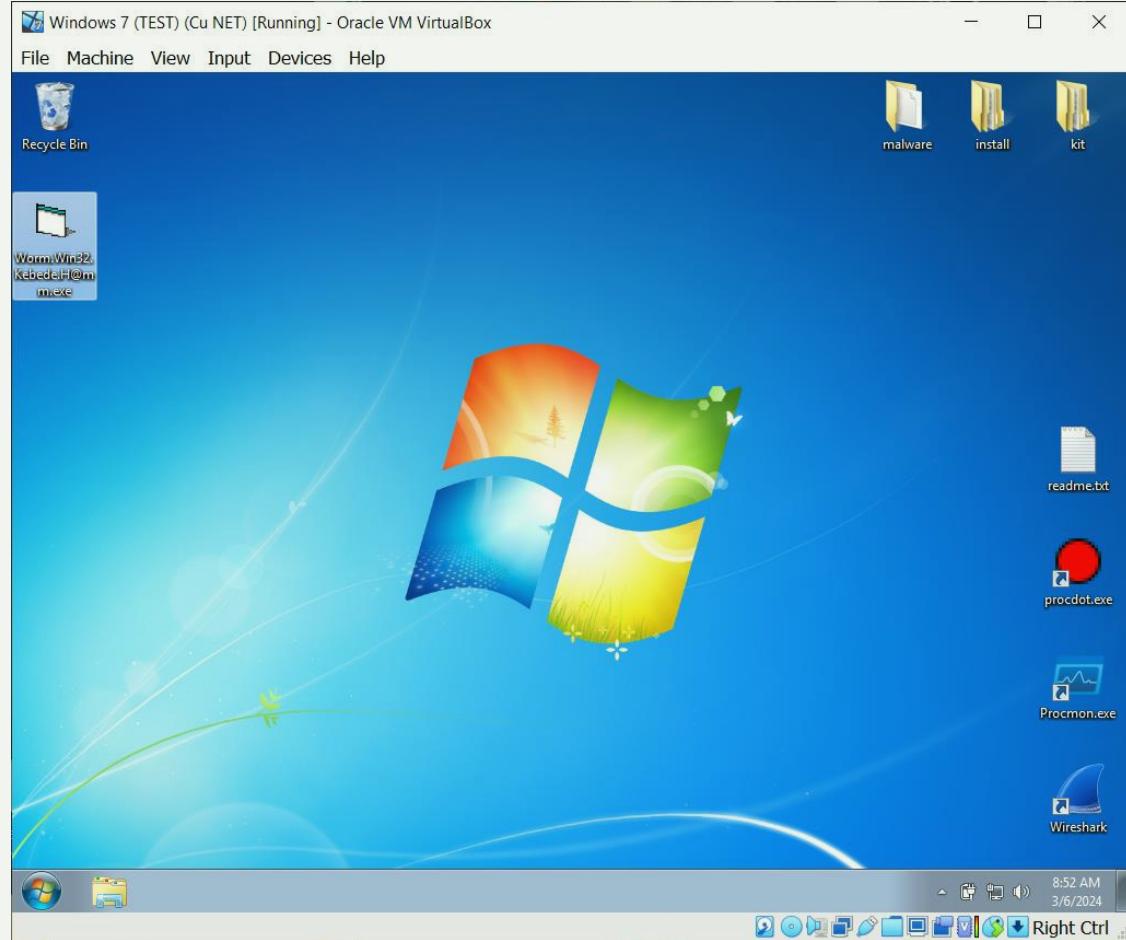
PROCESS MONITOR & WIRESHARK

DETTONAREA UNUI TROIAN



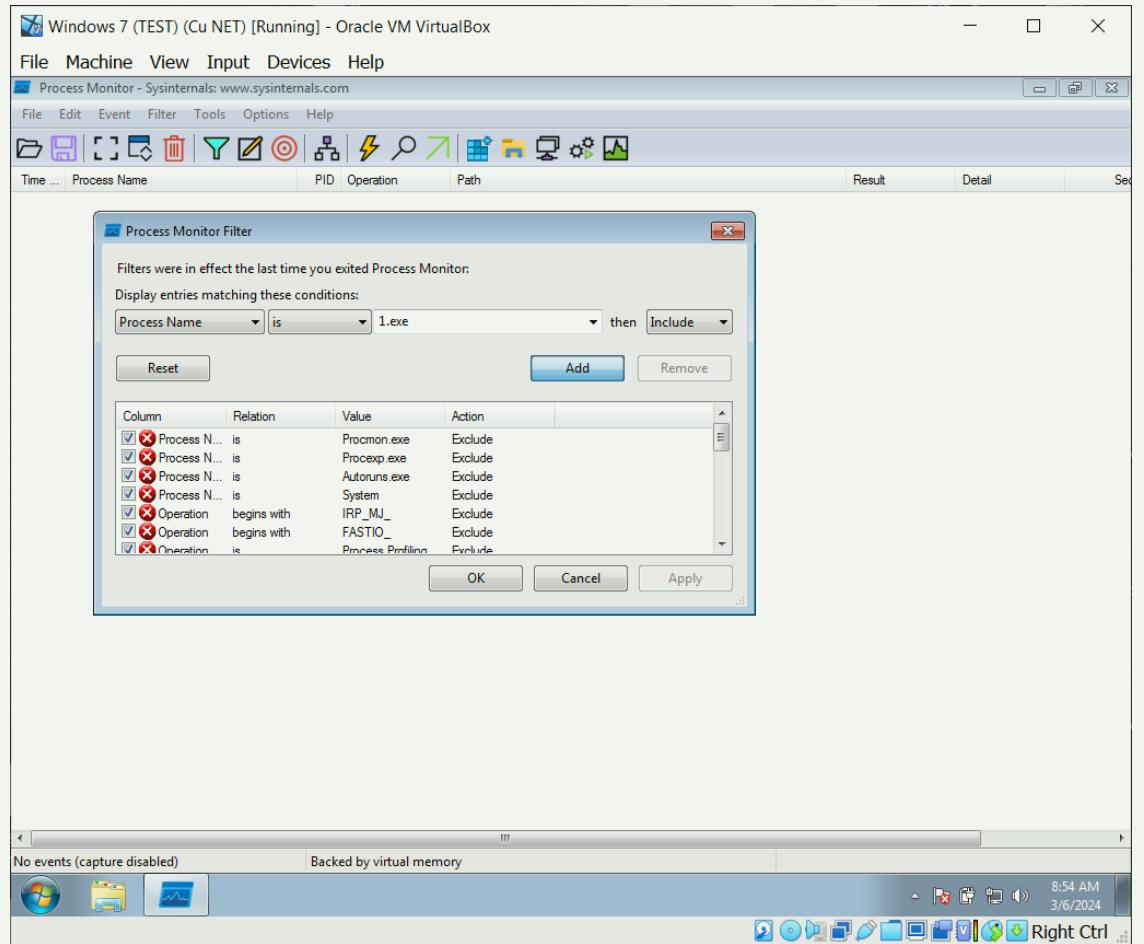
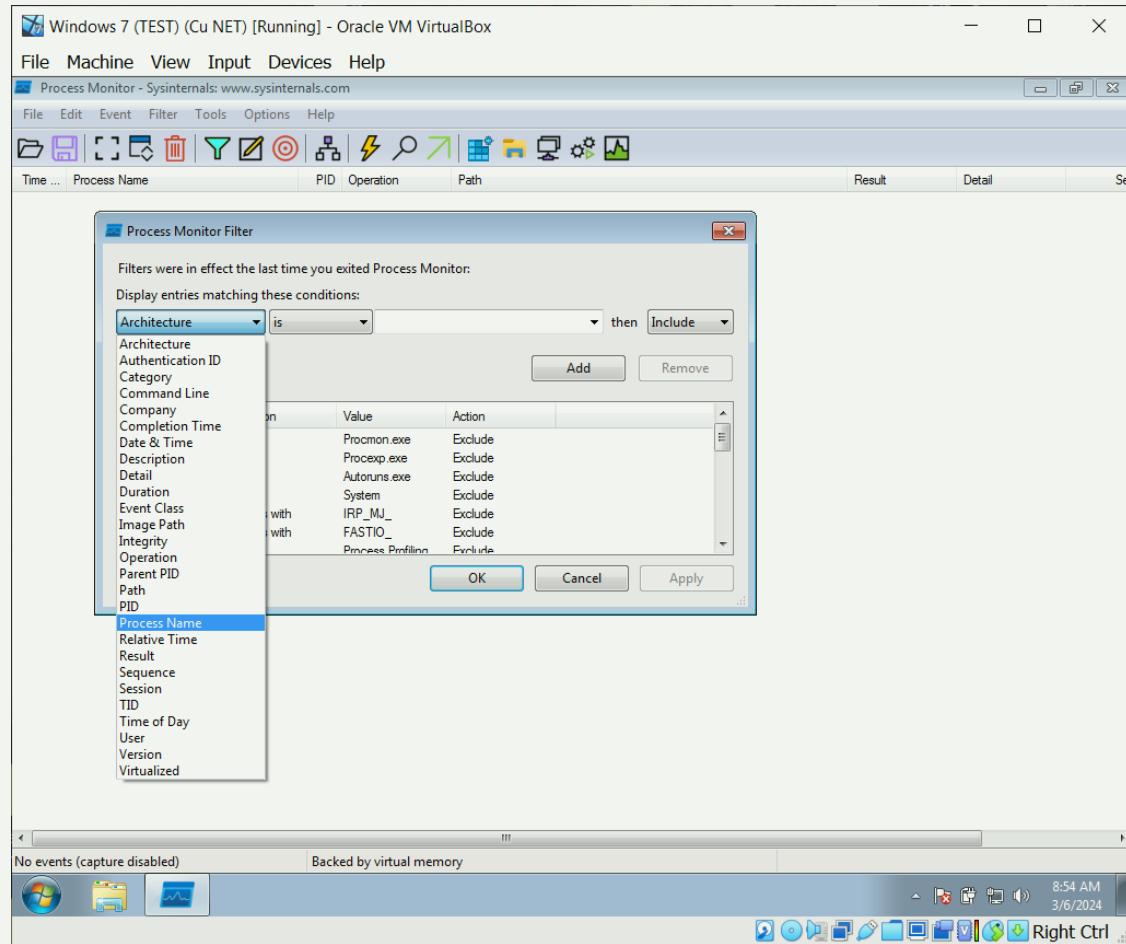
PROCESS MONITOR & WIRESHARK

DETTONAREA UNUI TROIAN / PREGATIRE SCENA



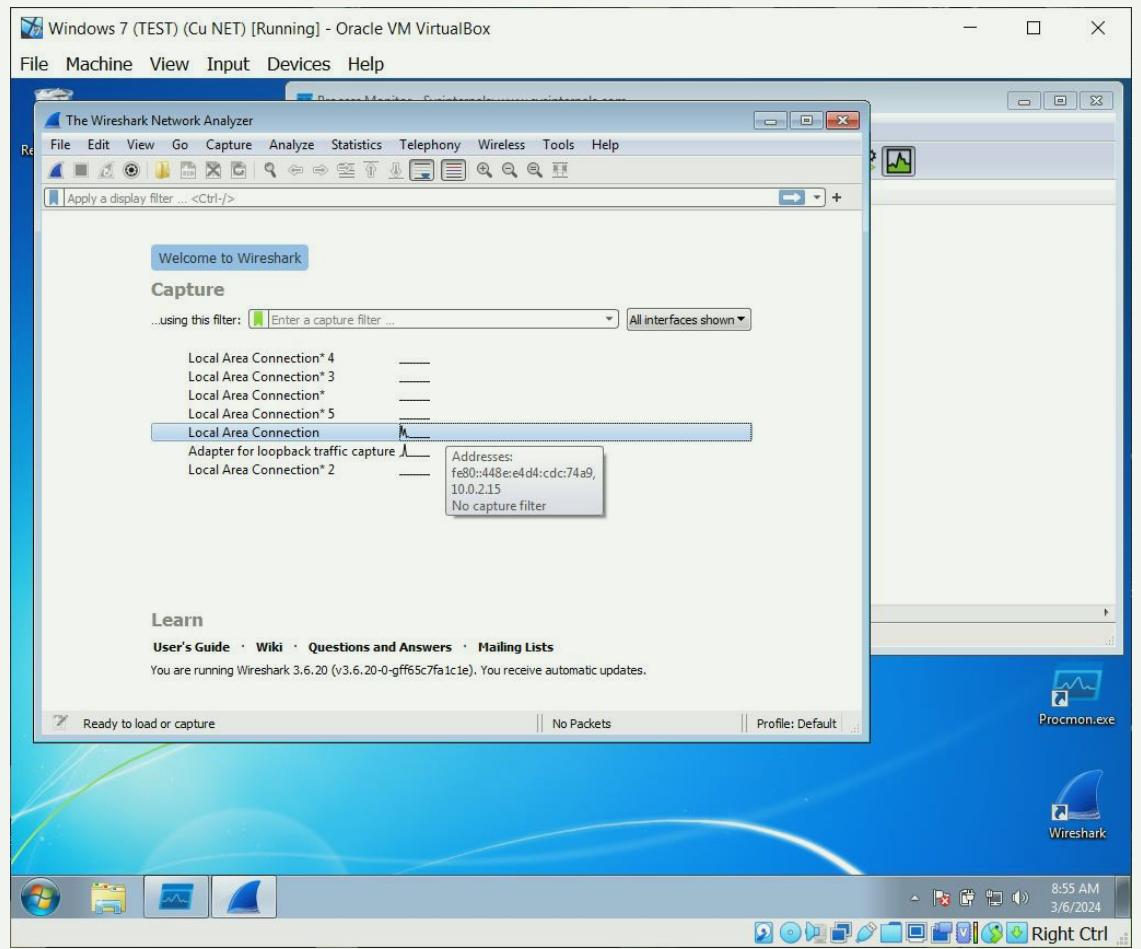
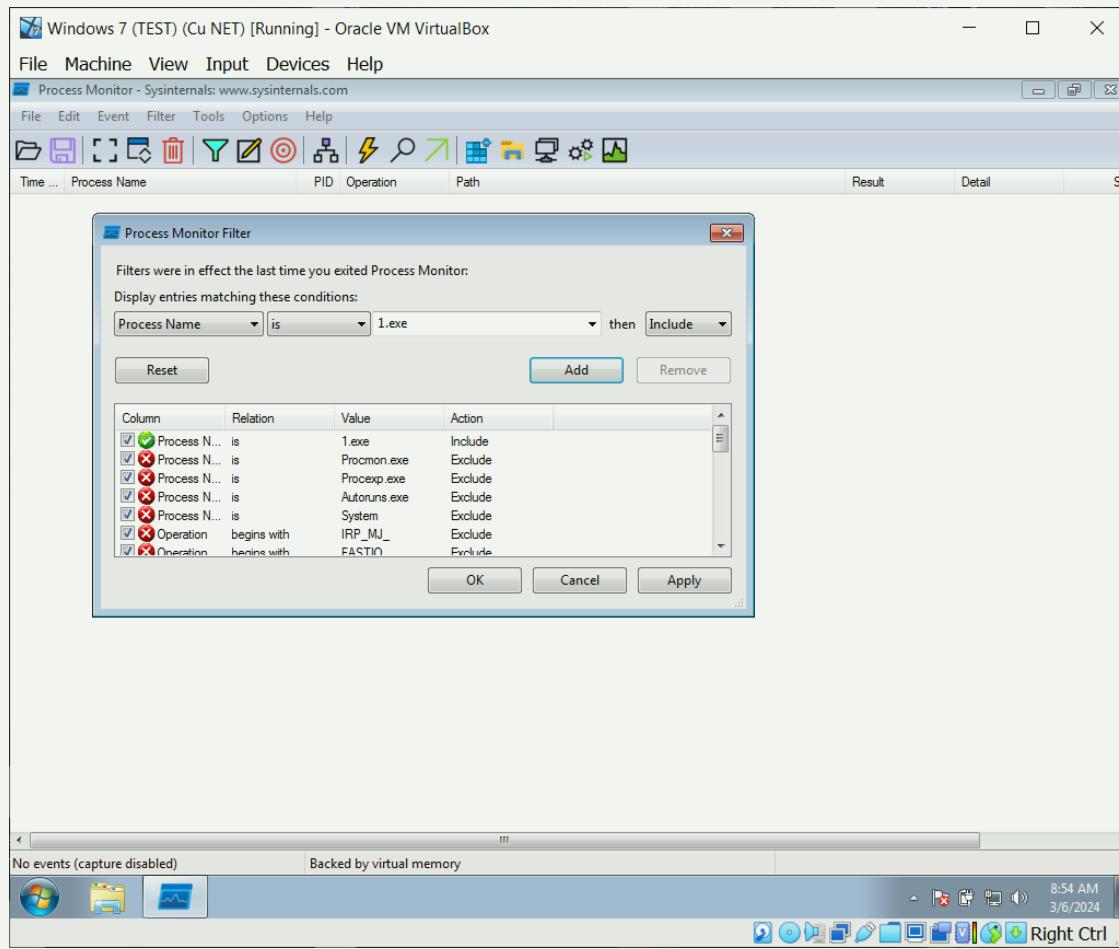
PROCESS MONITOR & WIRESHARK

DETTONAREA UNUI TROIAN / FILTRU PE NUMELE PROCESULUI



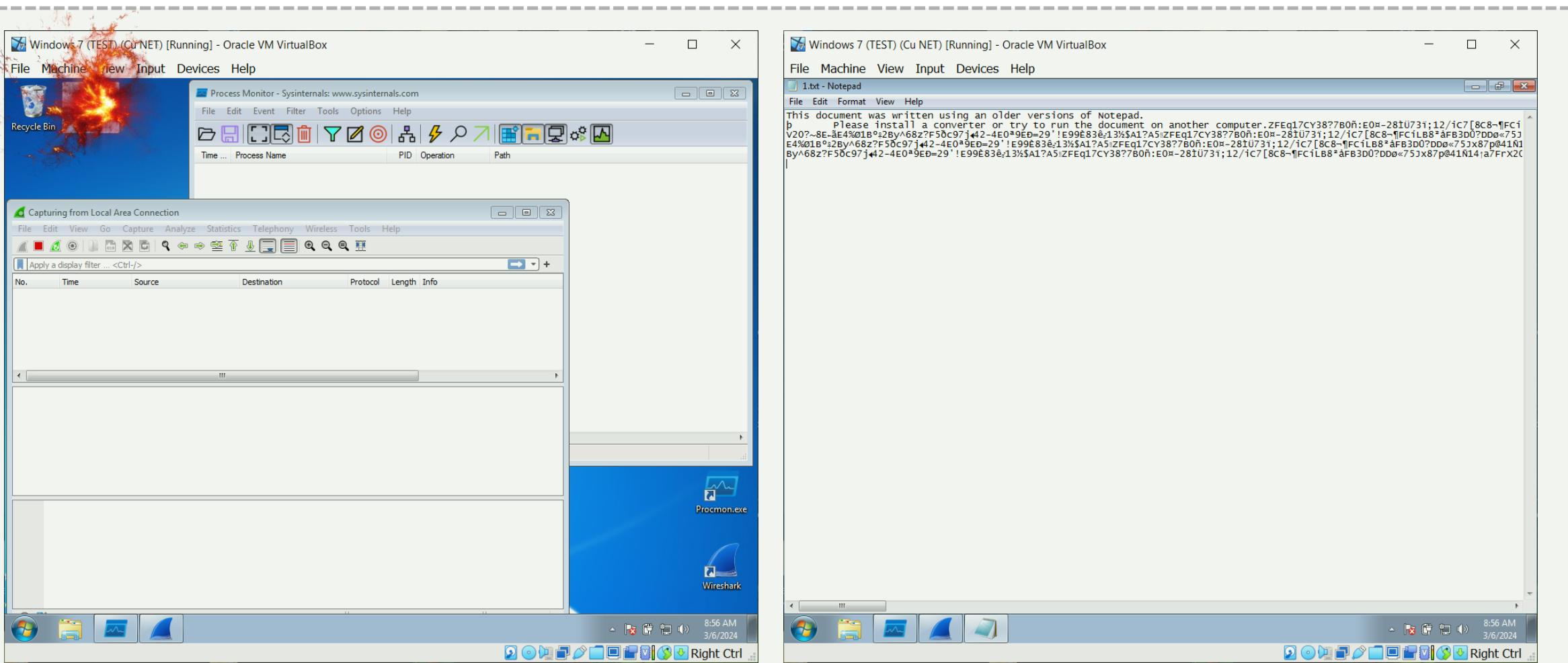
PROCESS MONITOR & WIRESHARK

DETTONAREA UNUI TROIAN / ADAUGAREA FILTRULUI SI PORNIREA WIRESHARK



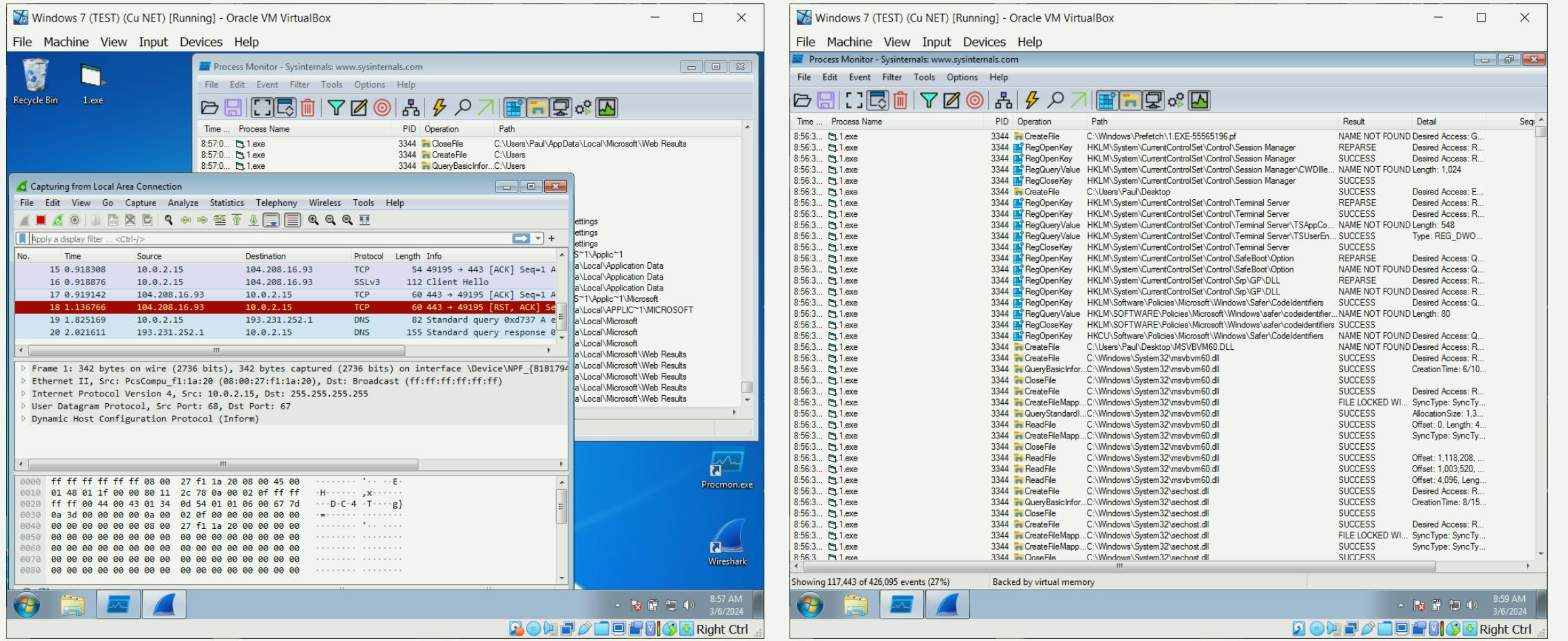
PROCESS MONITOR & WIRESHARK

SCENA PREGATITA - DETONAREA APLICATIEI MALWARE

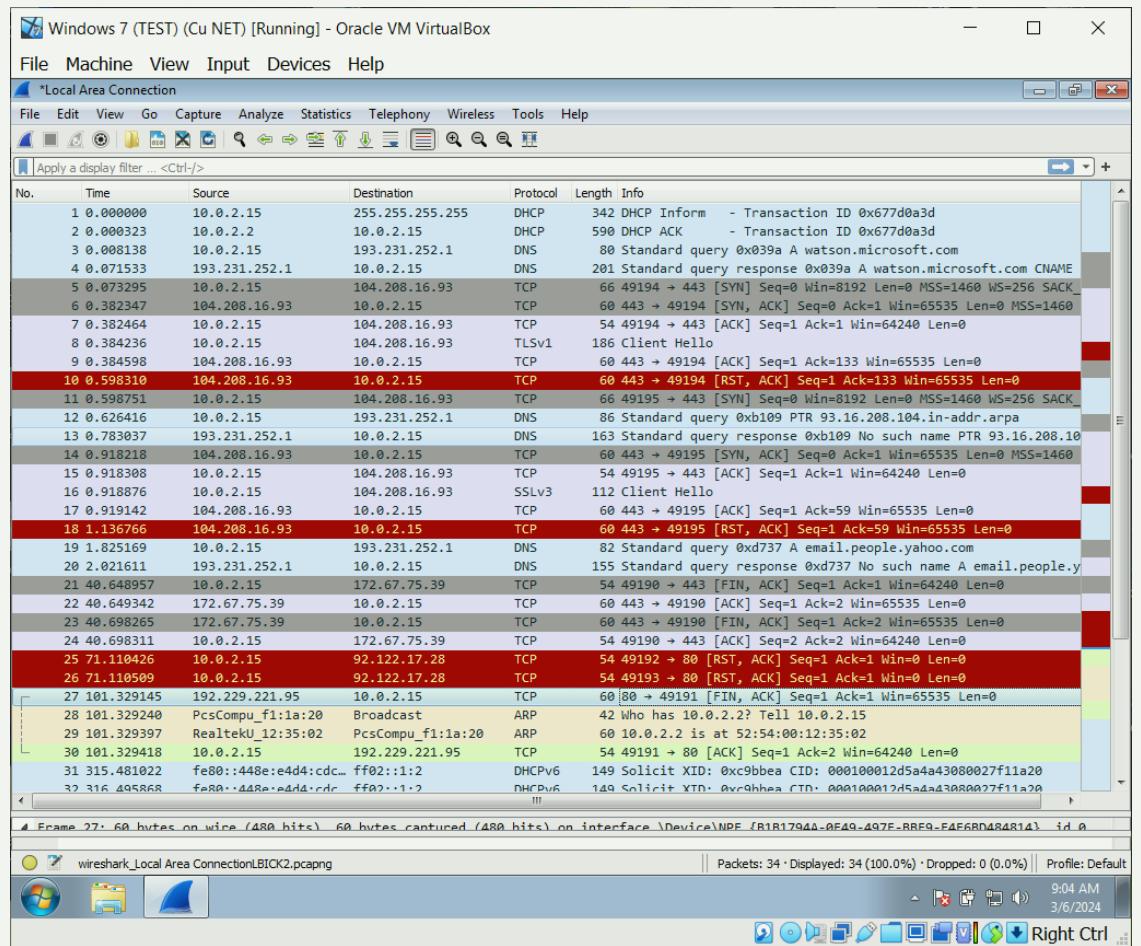
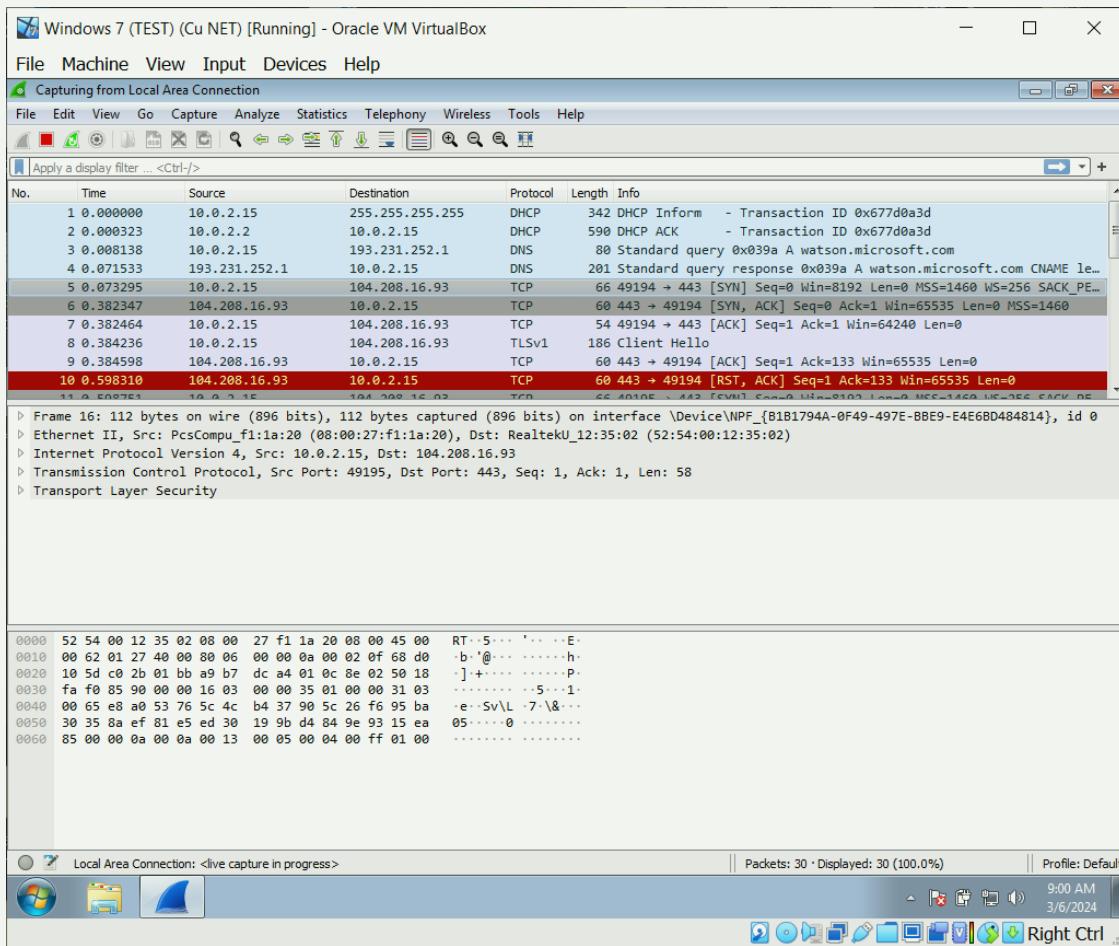


PROCESS MONITOR & WIRESHARK

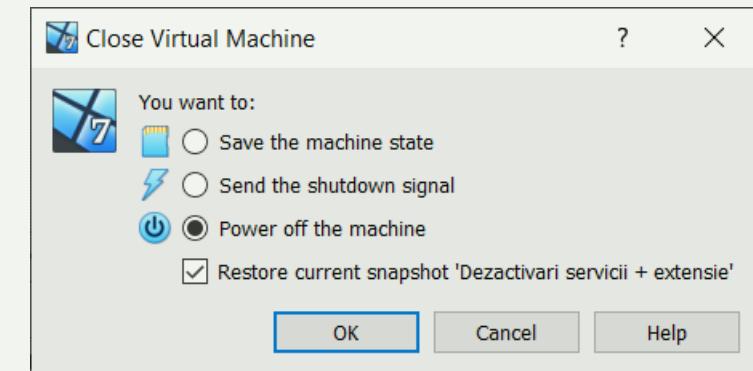
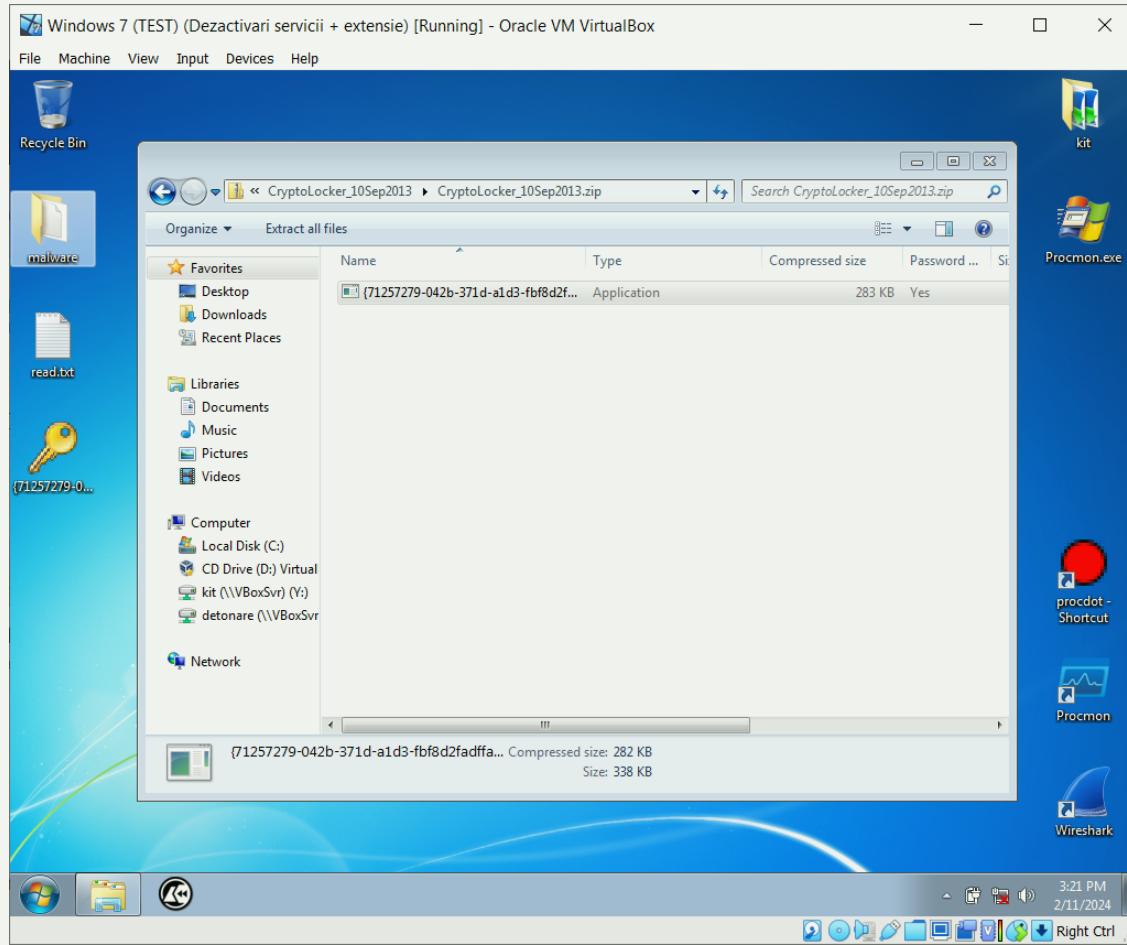
MONITORIZARE POST-DETONARE



PROCESS MONITOR & WIRESHARK CE URMARIM IN WIRESHARK?



POST-ANALIZA RESETAREA MASINII VIRTUALE



Dupa un experiment Masina Virtuala trebuie
Resetata prin selectarea : Restore current
snapshot ...

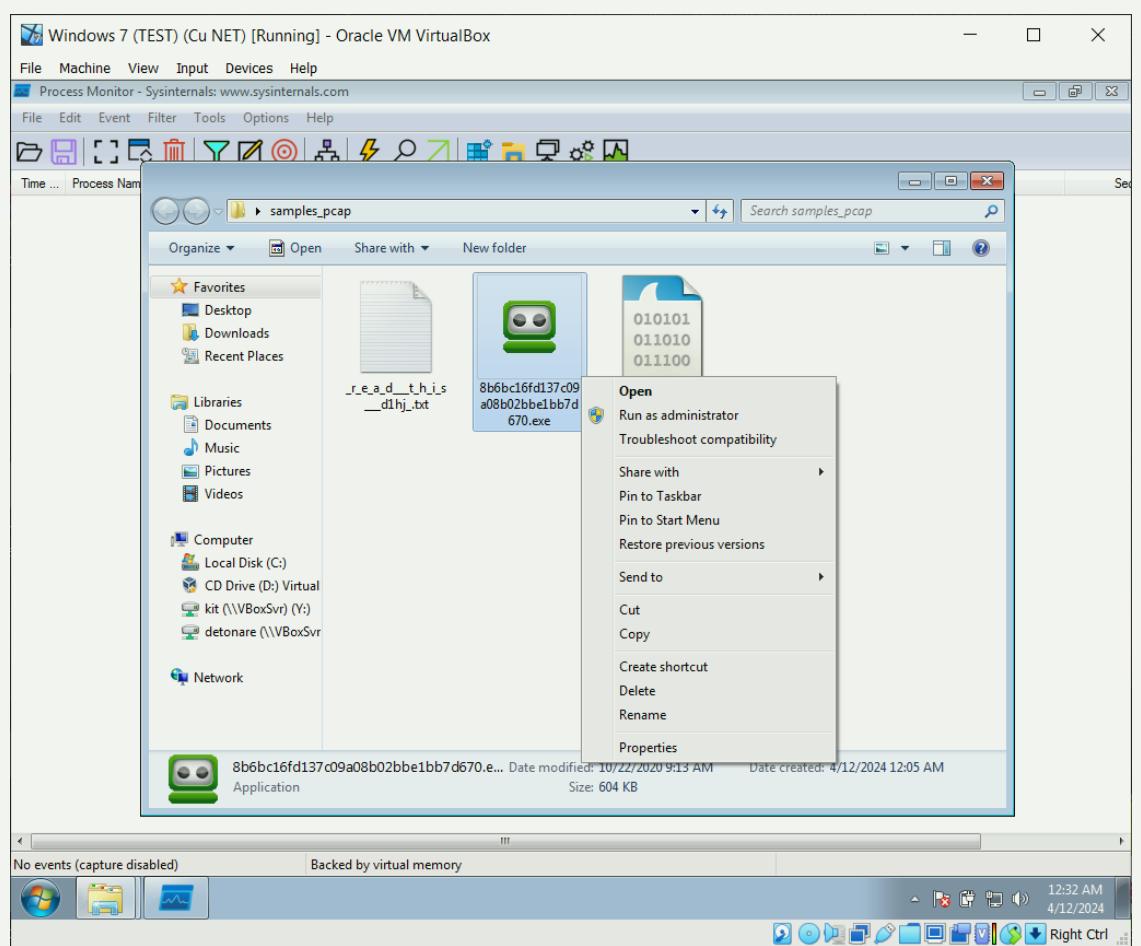
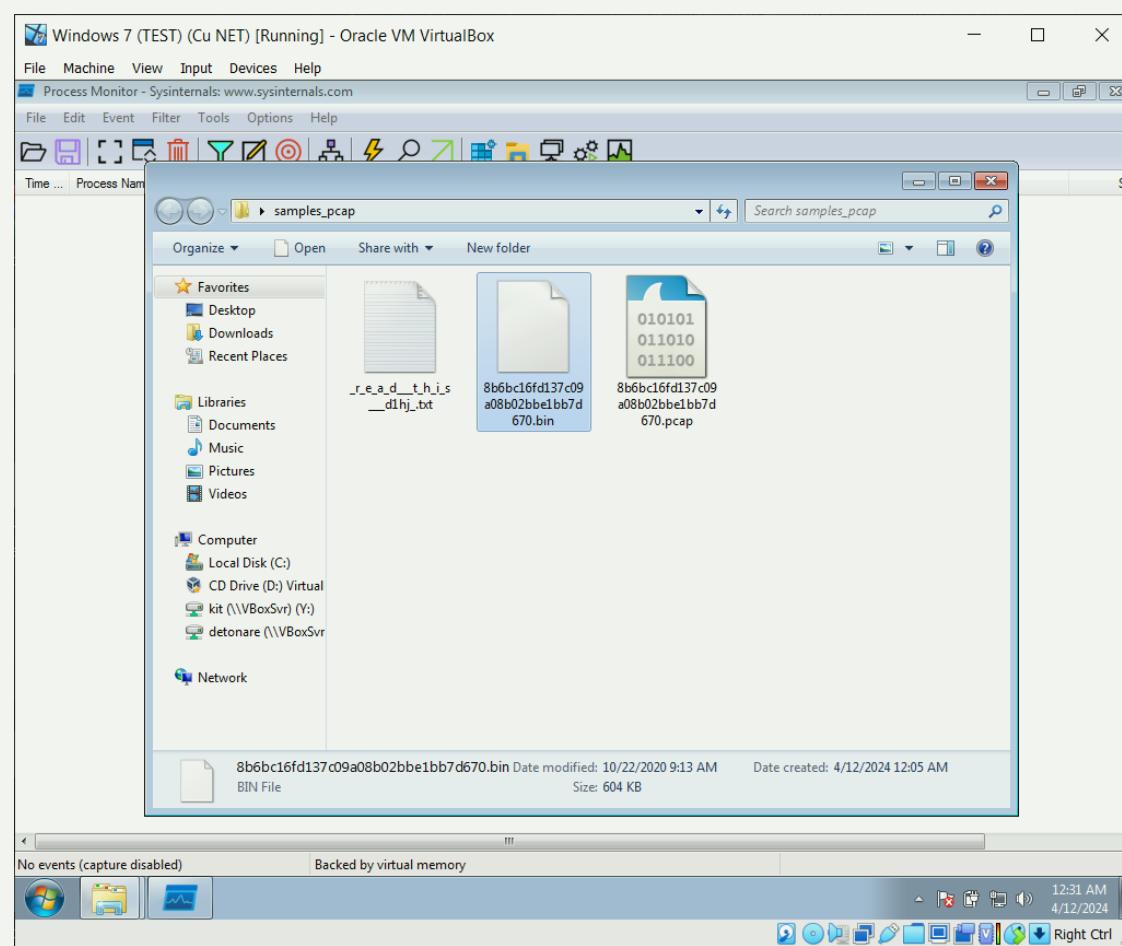
C.11.3

CAPTAREA EVENIMENTELOR EFEMERE ȘI ELIMINAREA ZGOMOTULUI



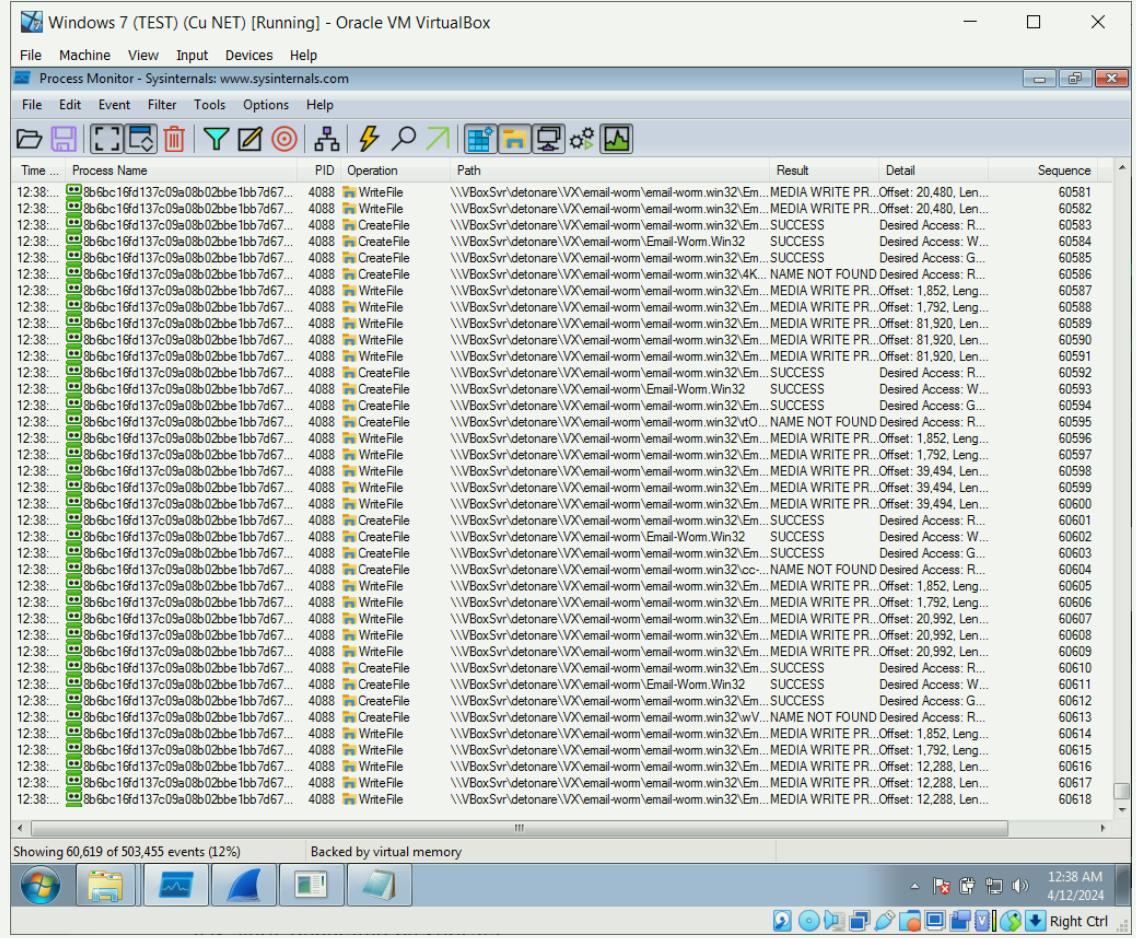
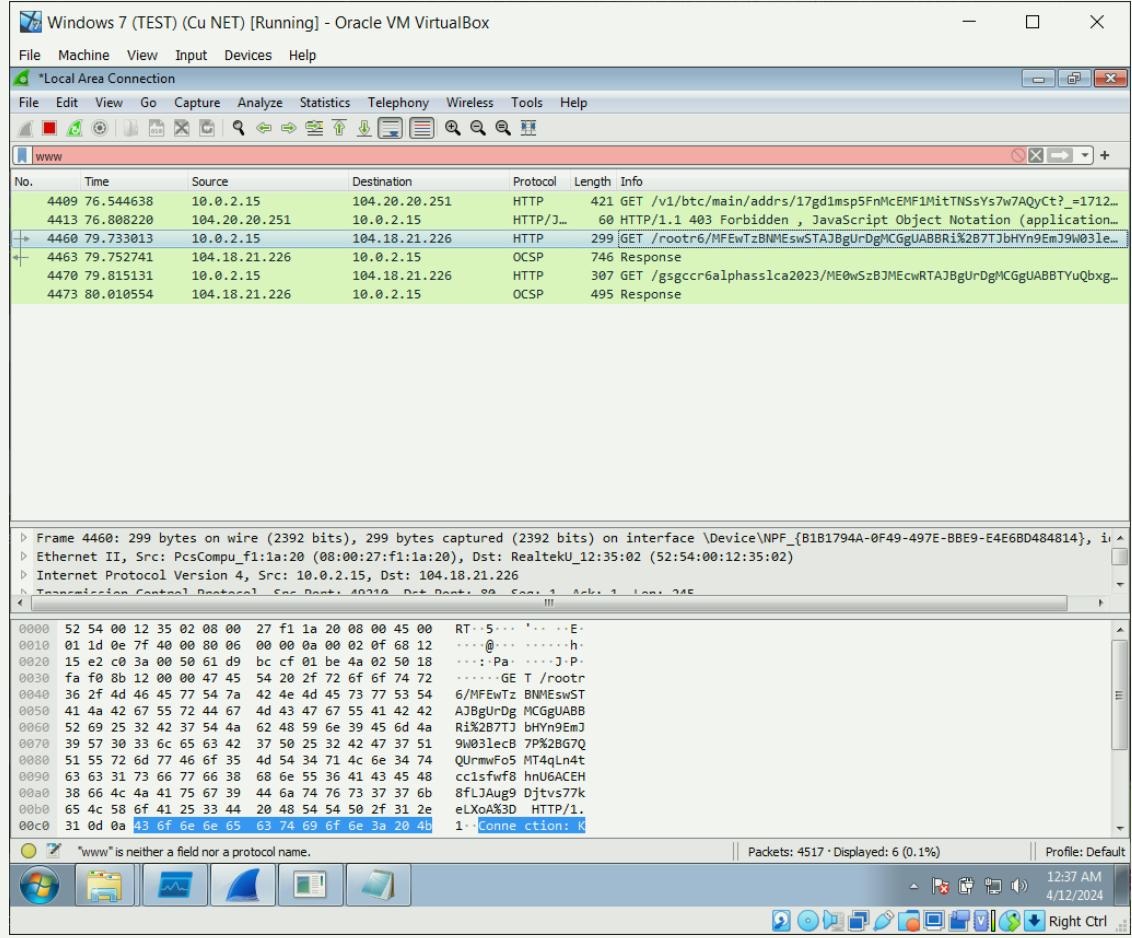
PROCESS MONITOR & WIRESHARK

DETAREA UNUI FISIER SUSPECT



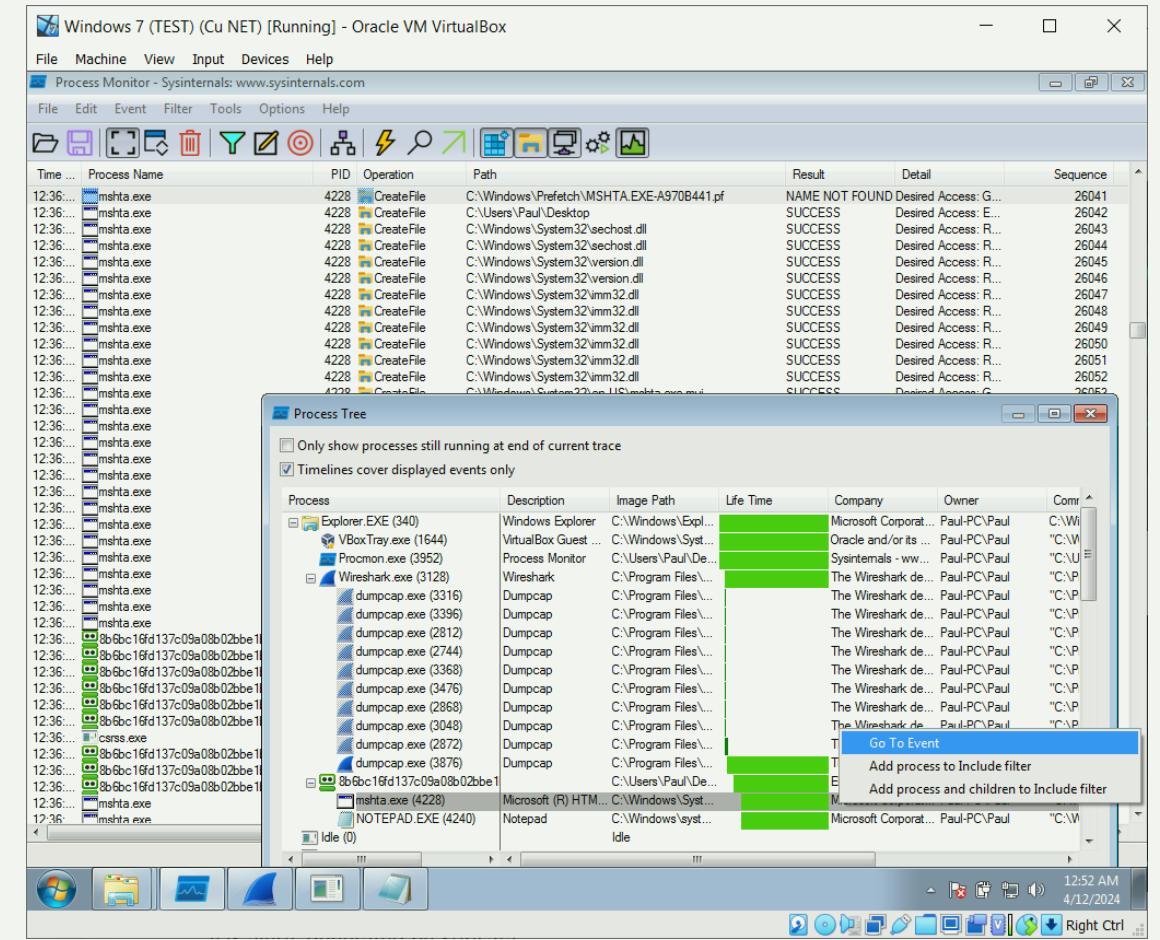
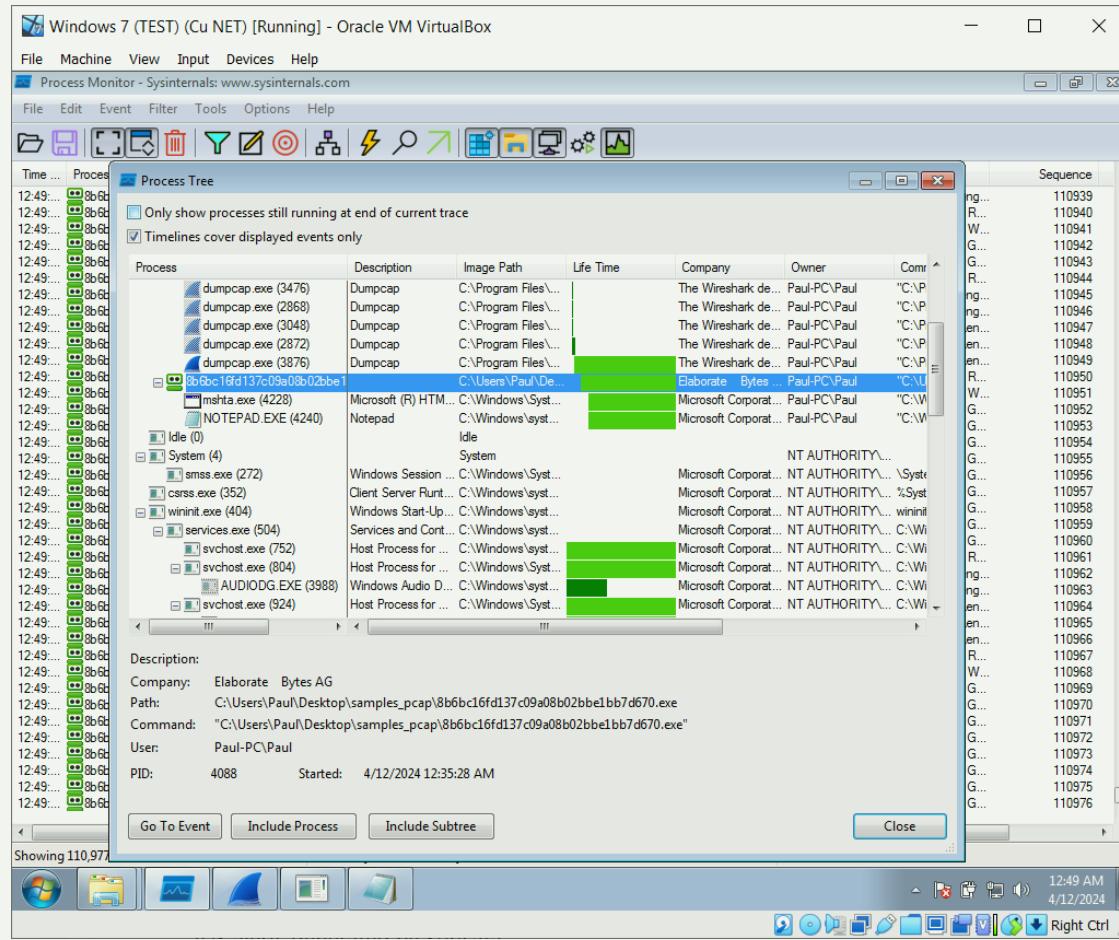
PROCESS MONITOR & WIRESHARK

OPERATIUNI DE SCRIERE & FILTRELE WIRESHARK !



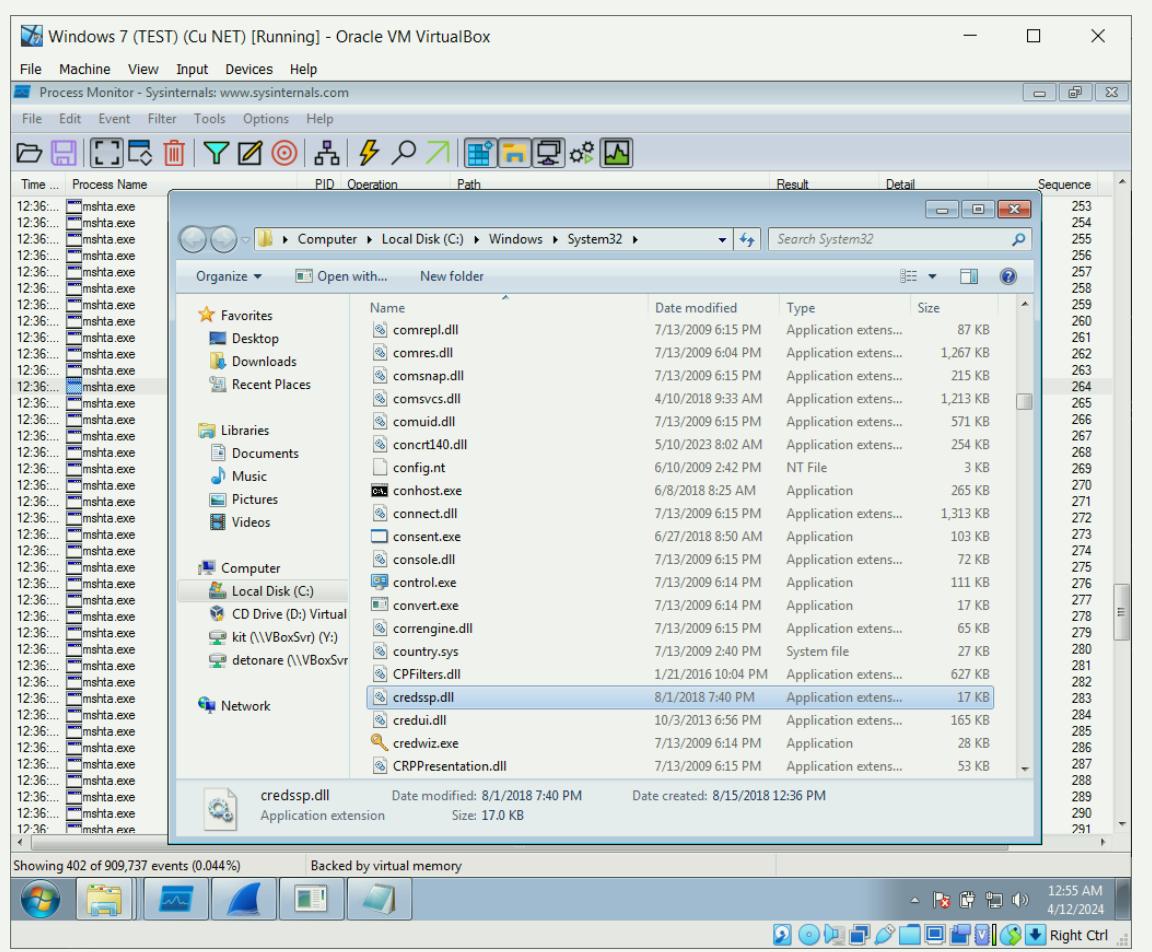
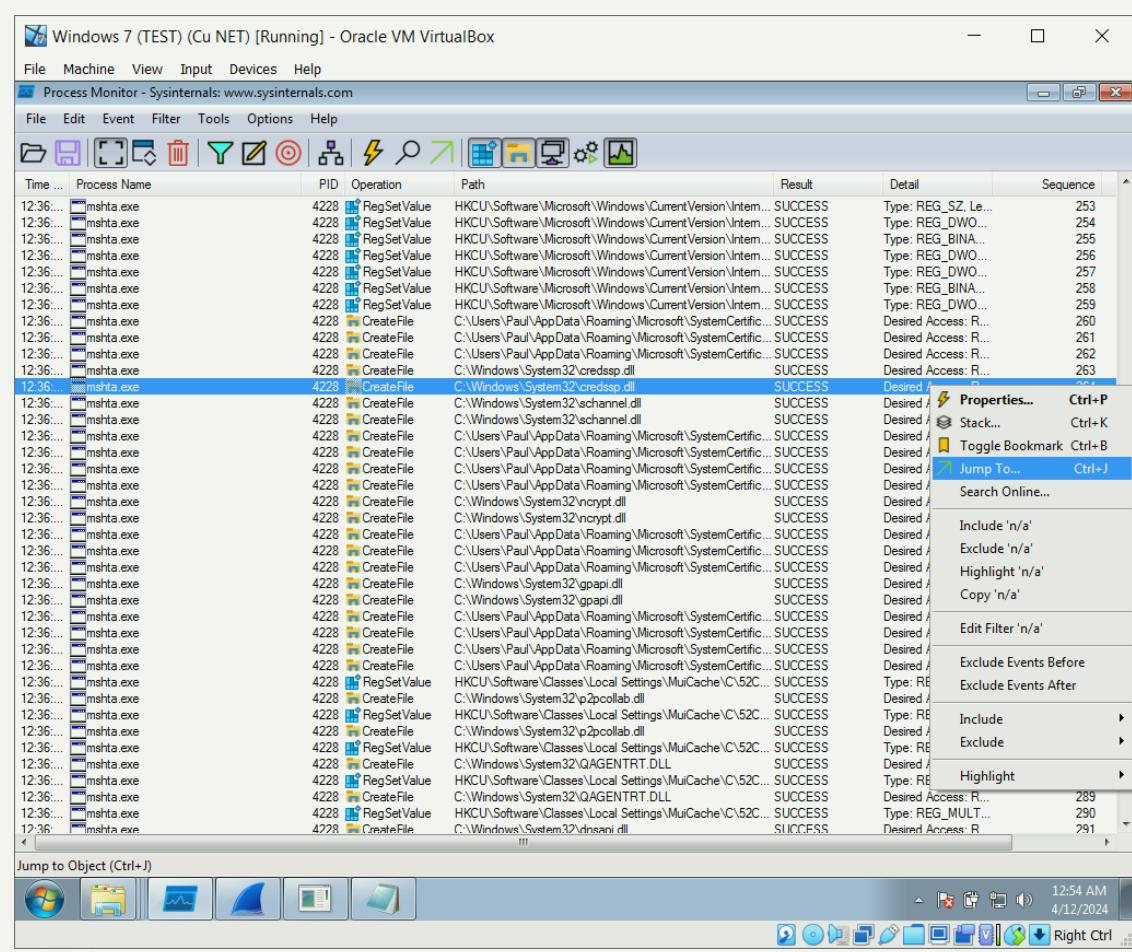
PROCESS MONITOR

EVALUAREA EVENIMENTELOR EFEMERE POST-DETONEARE



PROCESS MONITOR & WIRESHARK

ACCESAREA FISIERELOR SCRISE DE MALWARE

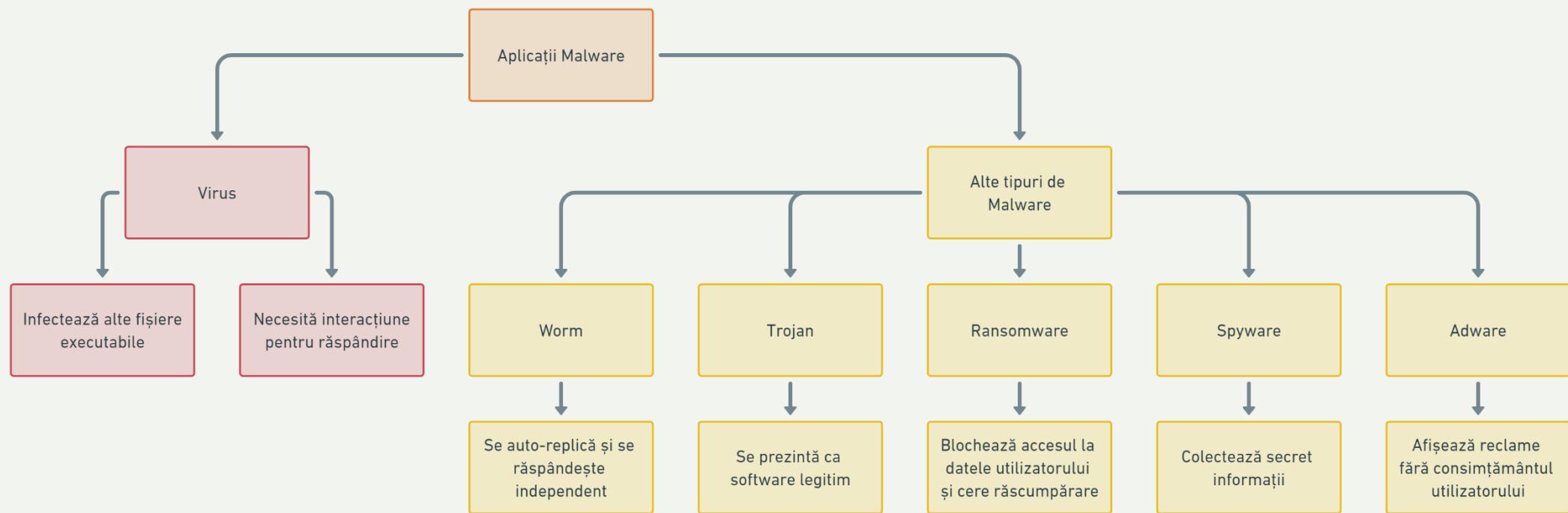


C.11.4

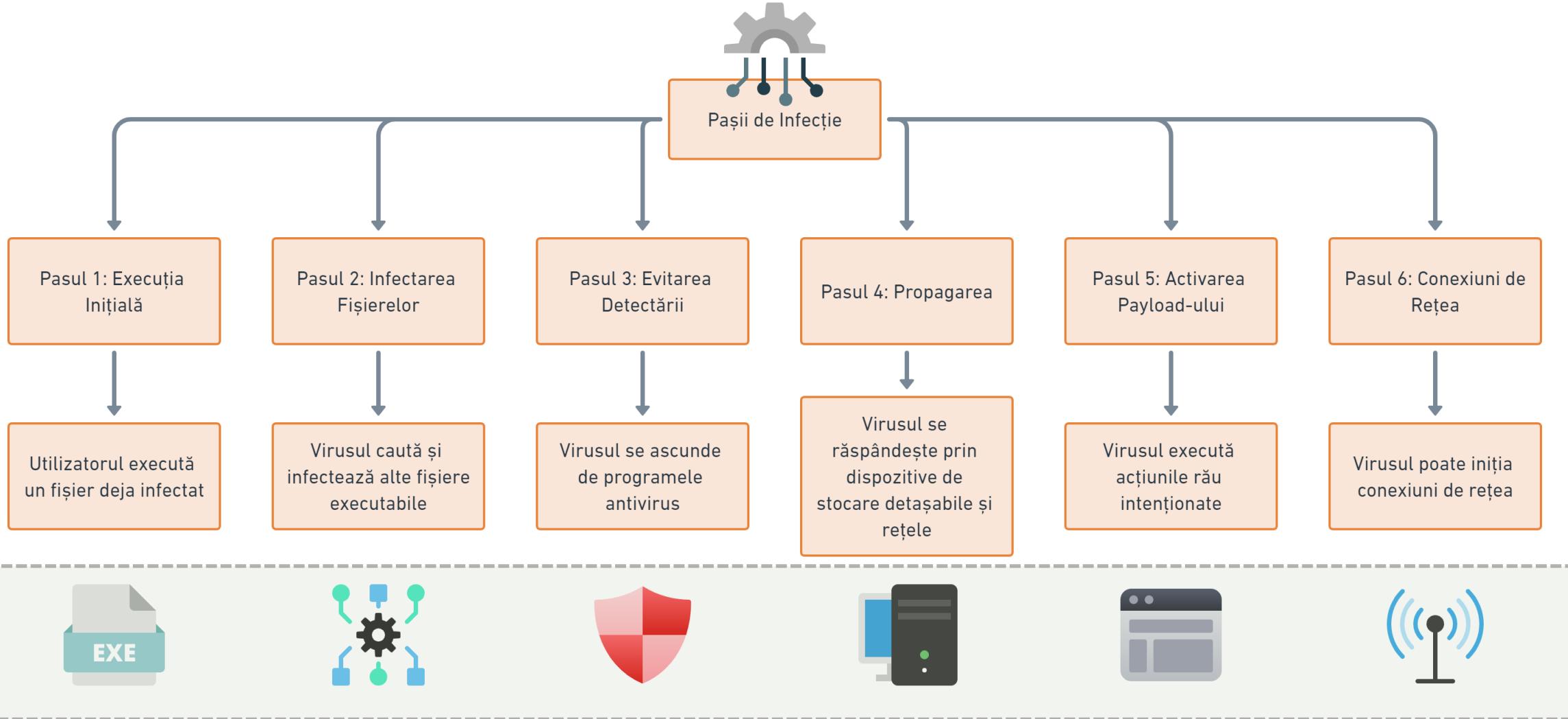
DETONAREA ȘI ANALIZA VIRUȘILOR PRIN UTILIZAREA HONEYPO



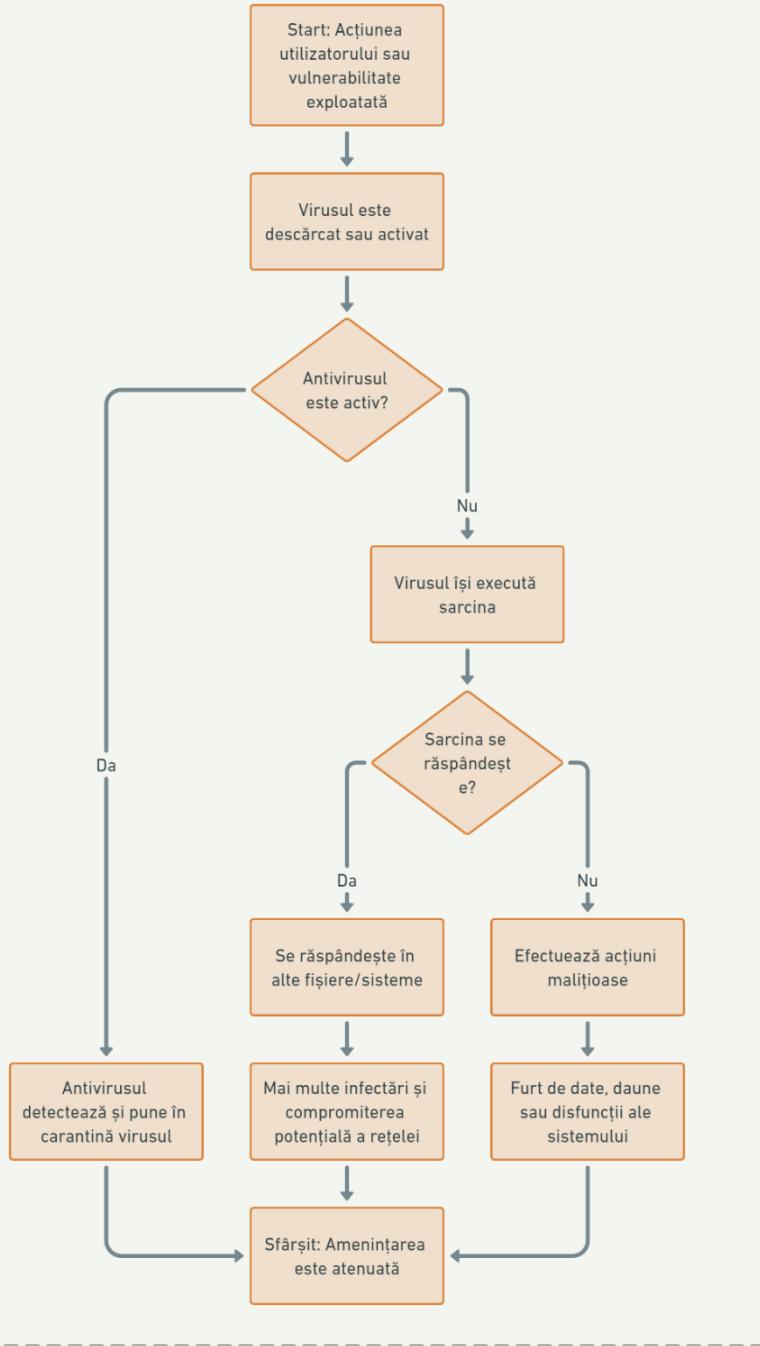
Două puncte principale:







La ce ne asteptam post-infectie?

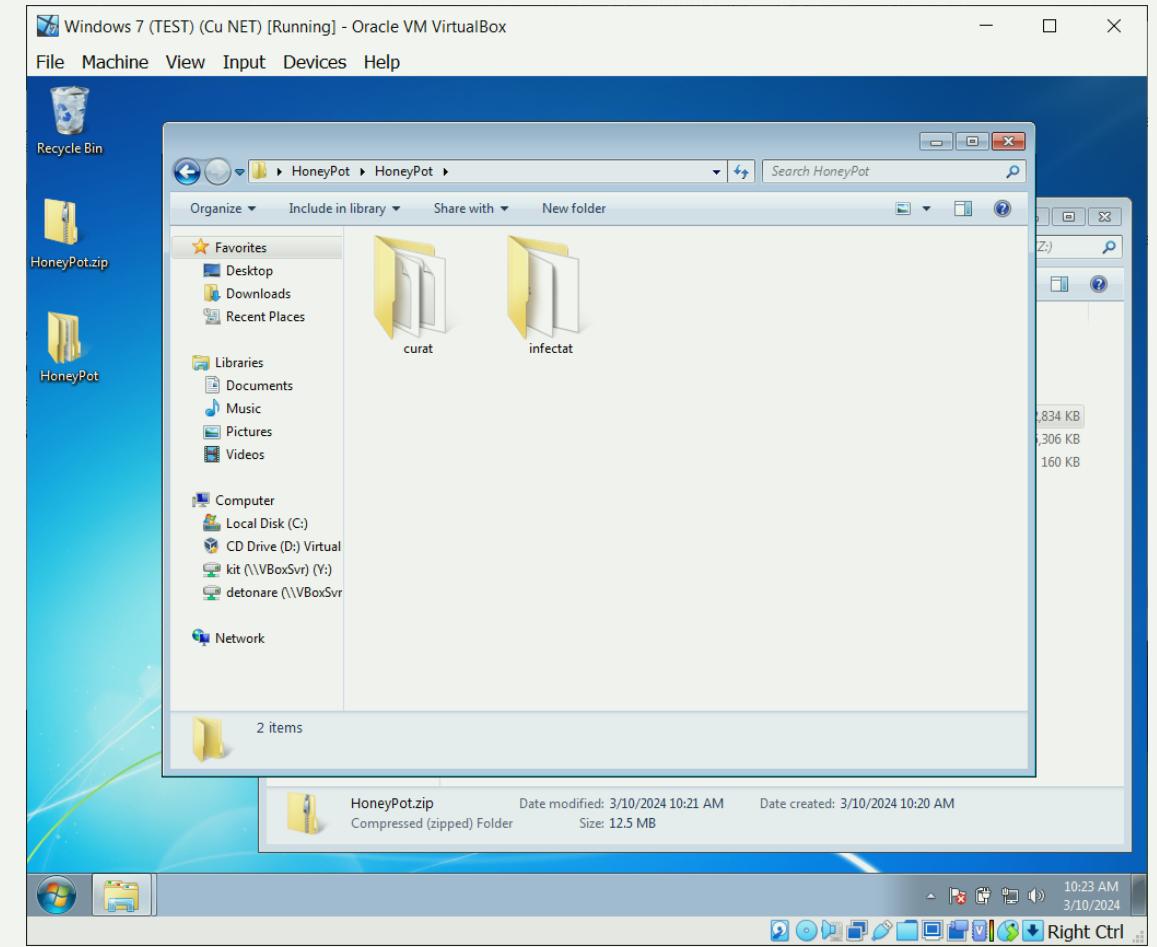
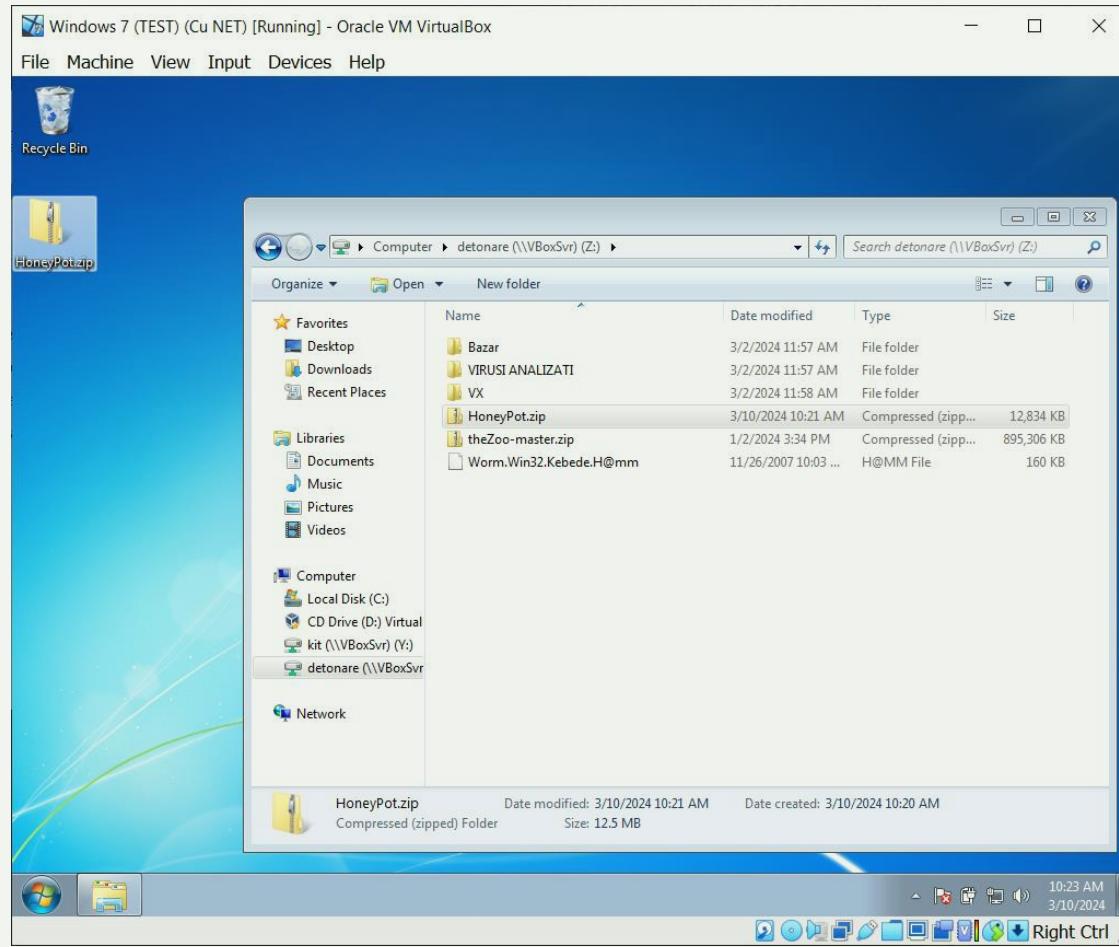


ȚINTE TENTANTE

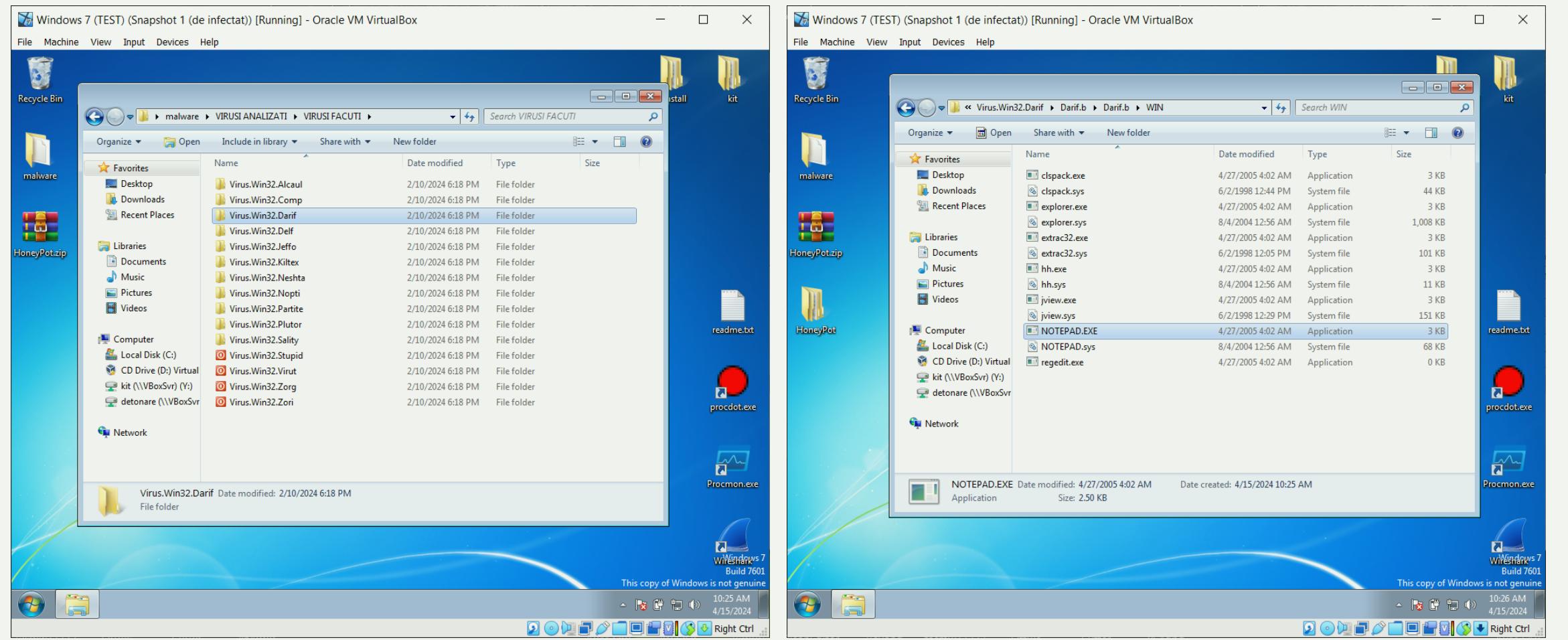
HONEYPOT (BORCANUL CU MIERE)



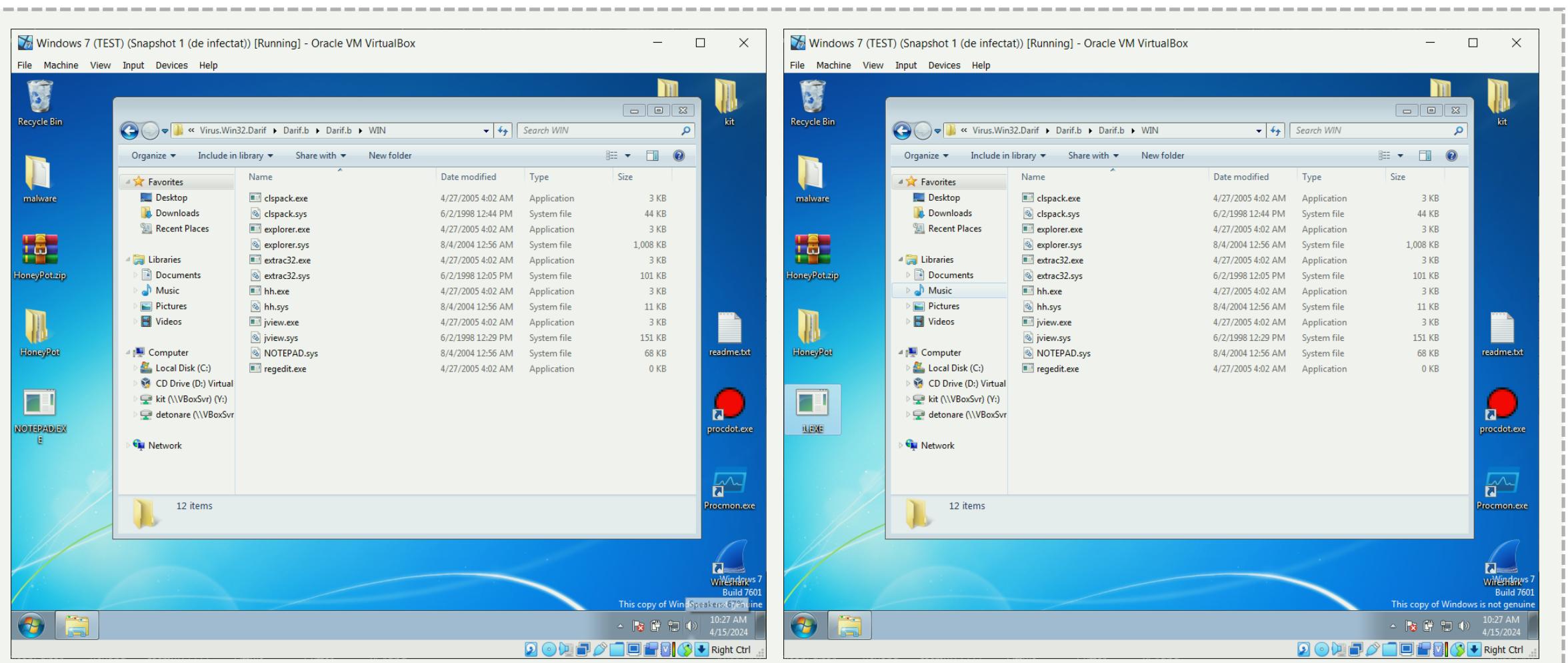
INSTALARE HONEYBOT DE PE MOODLE CE ESTE UN HONEYBOT PENTRU INFECTIE?



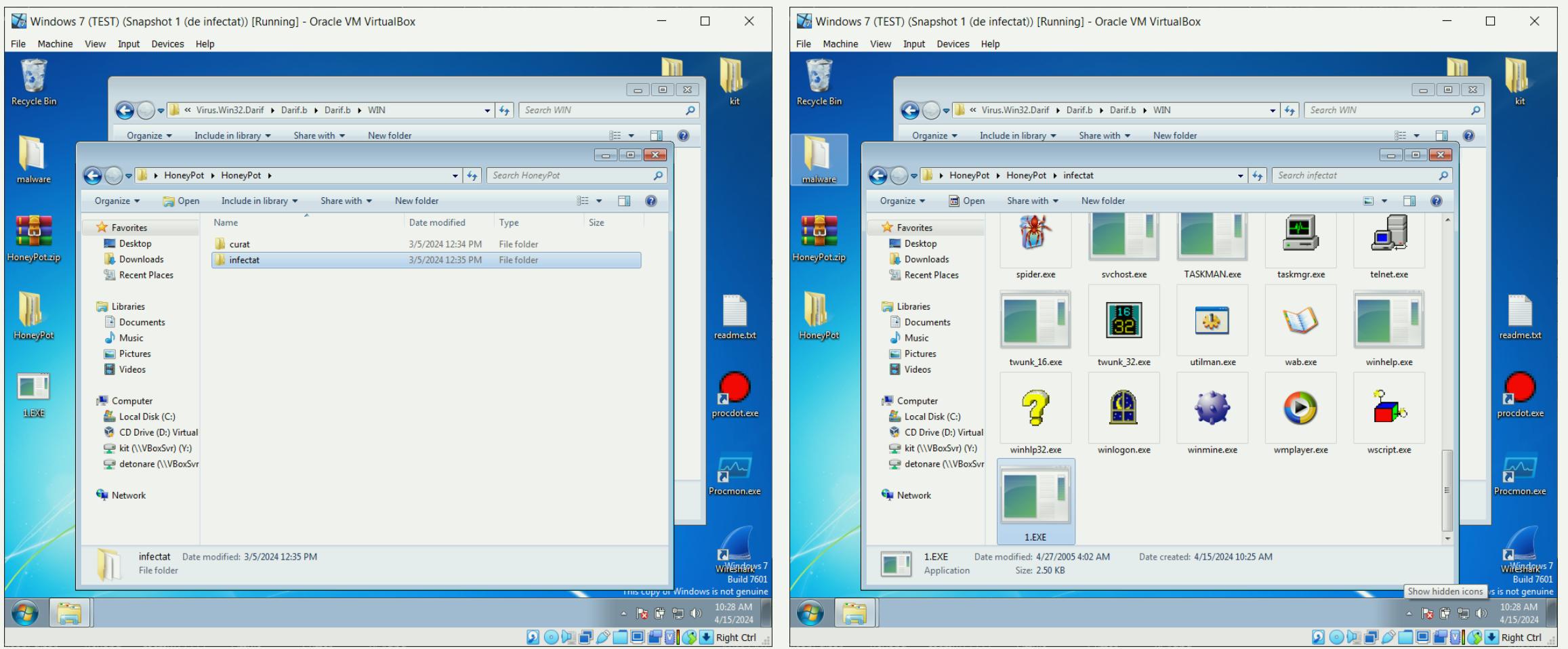
VERIFICAREA TIPULUI DE INFECTIE ALEGEREA UNEI MOSTRE DE VIRUS (FISIER INFECTAT)



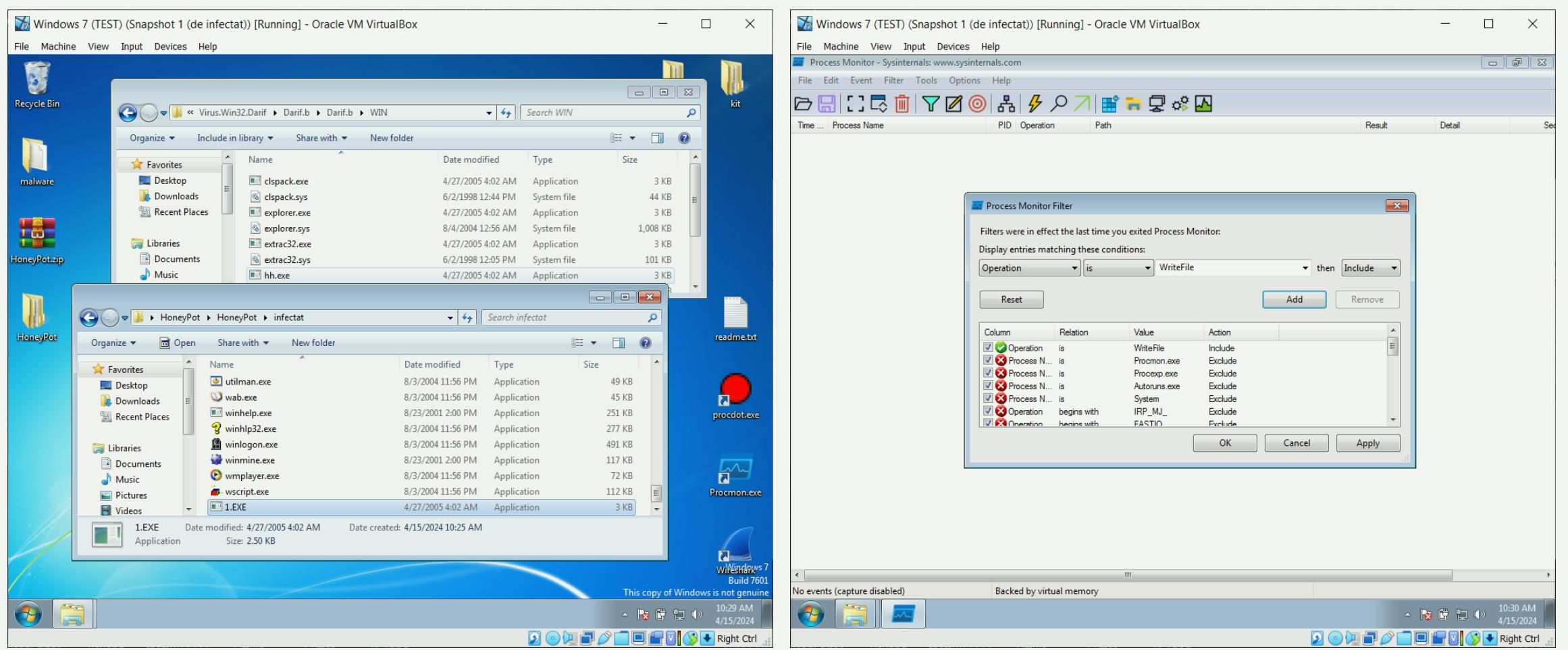
MODIFICAREA NUMELUI FISIEREULUI INFECTAT COPIEREA TEMPORARA PE DESKTOP



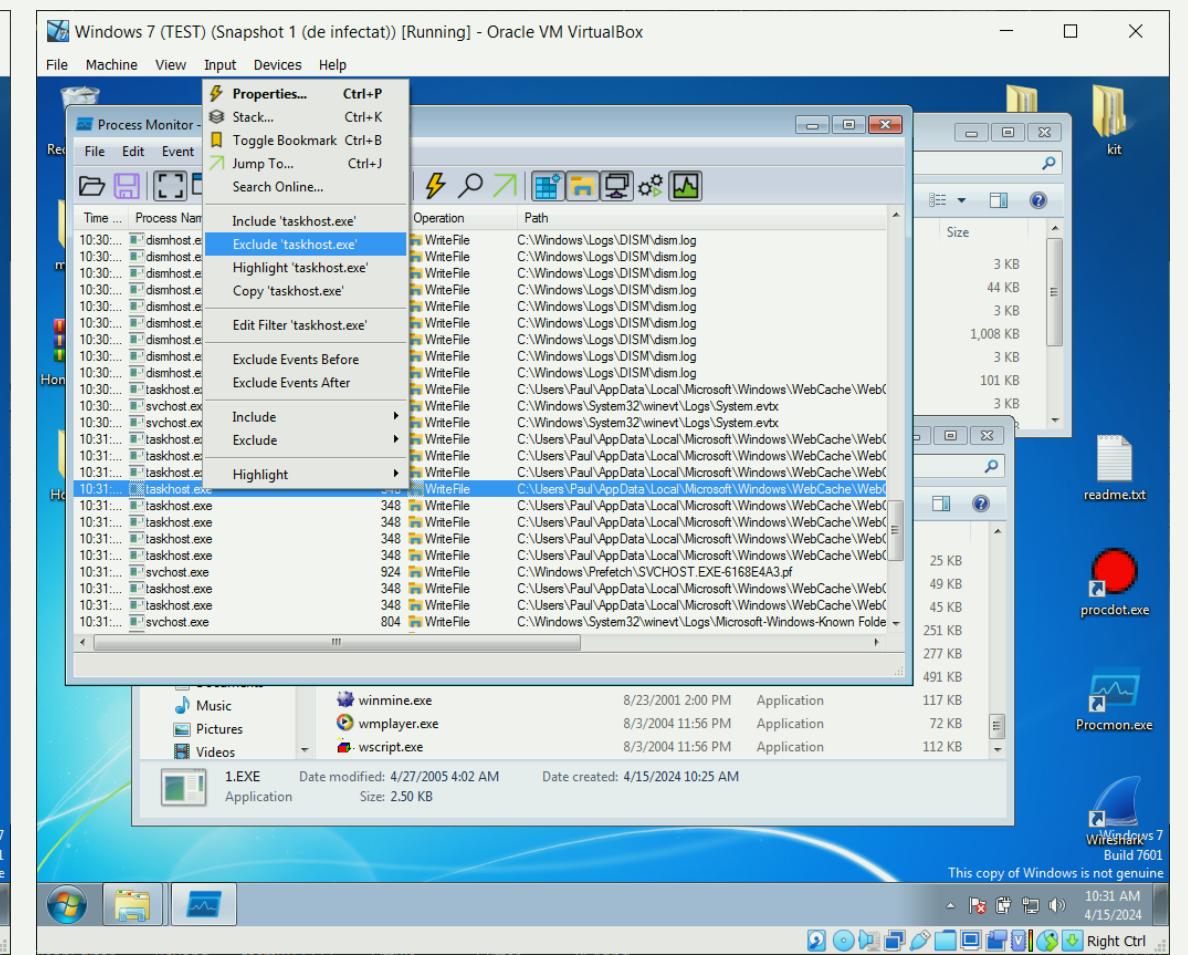
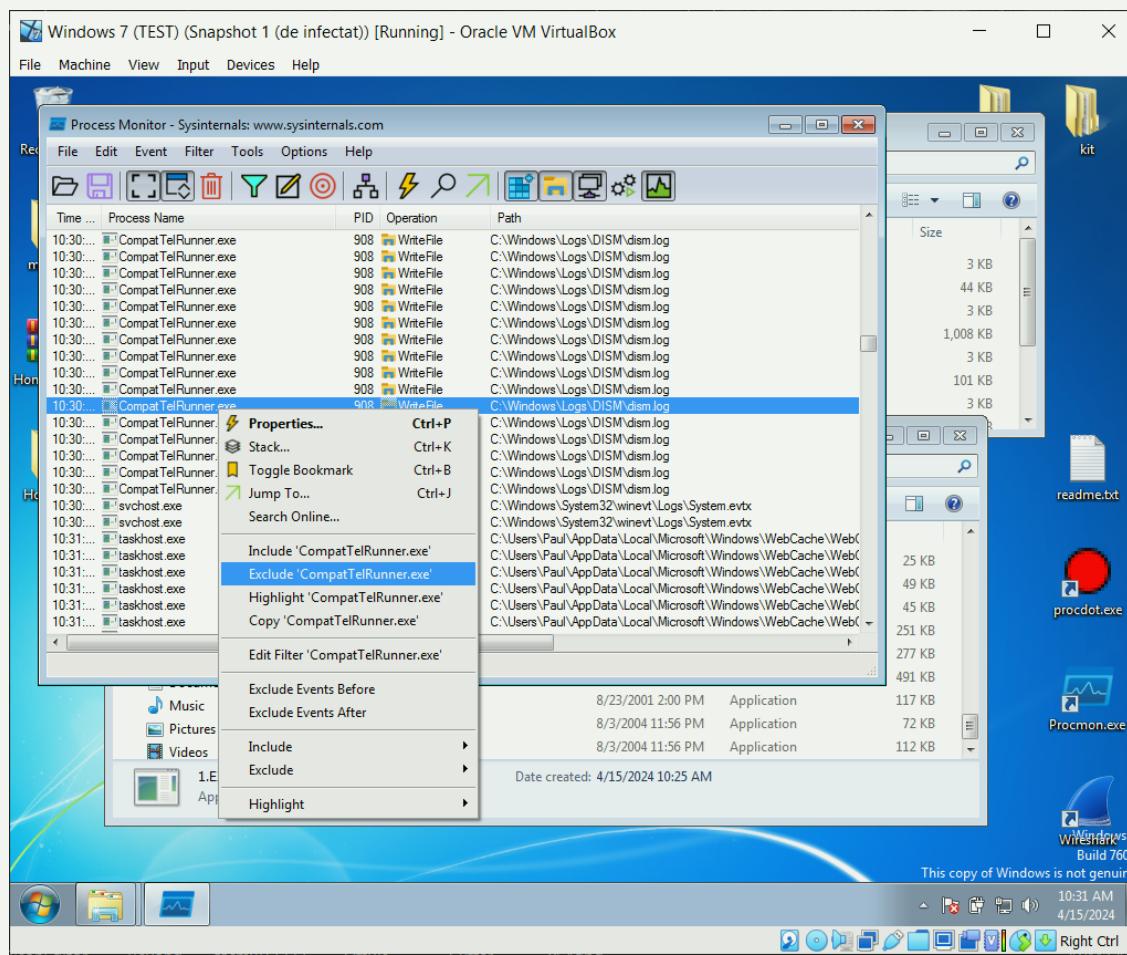
MUTAREA VIRUSULUI DE PE DESKTOP IN DIRECTORUL DESKTOP AL HONEYPOT



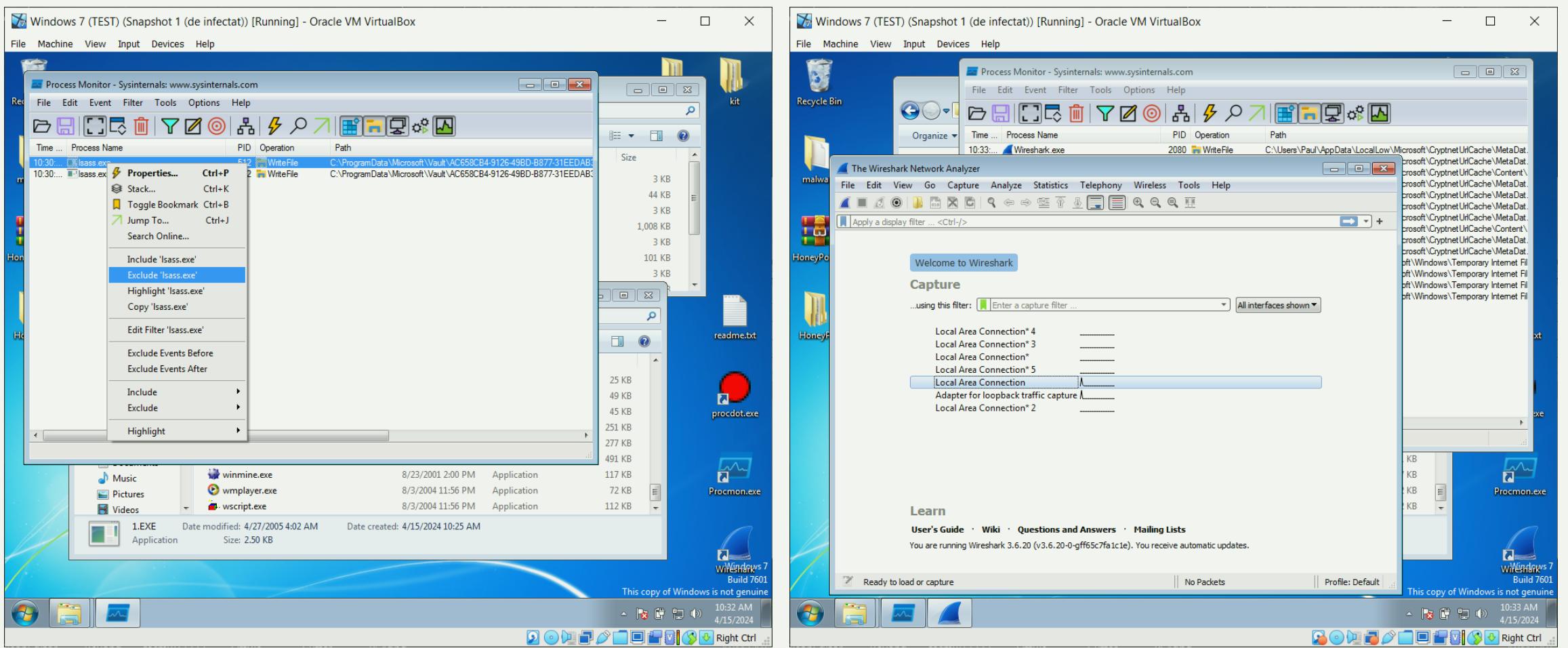
PREGATIREA FILTRELOR PENTRU PROCESS MONITOR



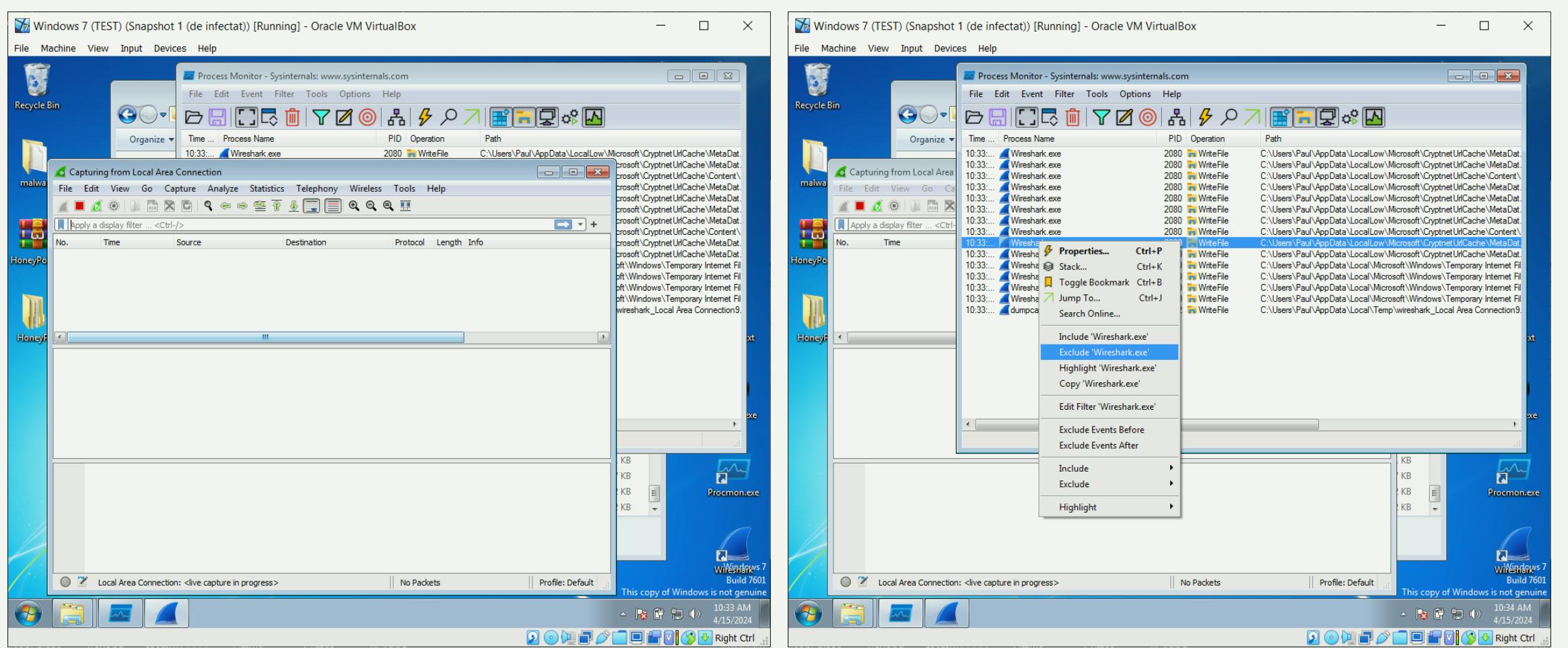
ELIMINAREA MANUALĂ A ZGOMOTUUI DIN PROCESS MONITOR



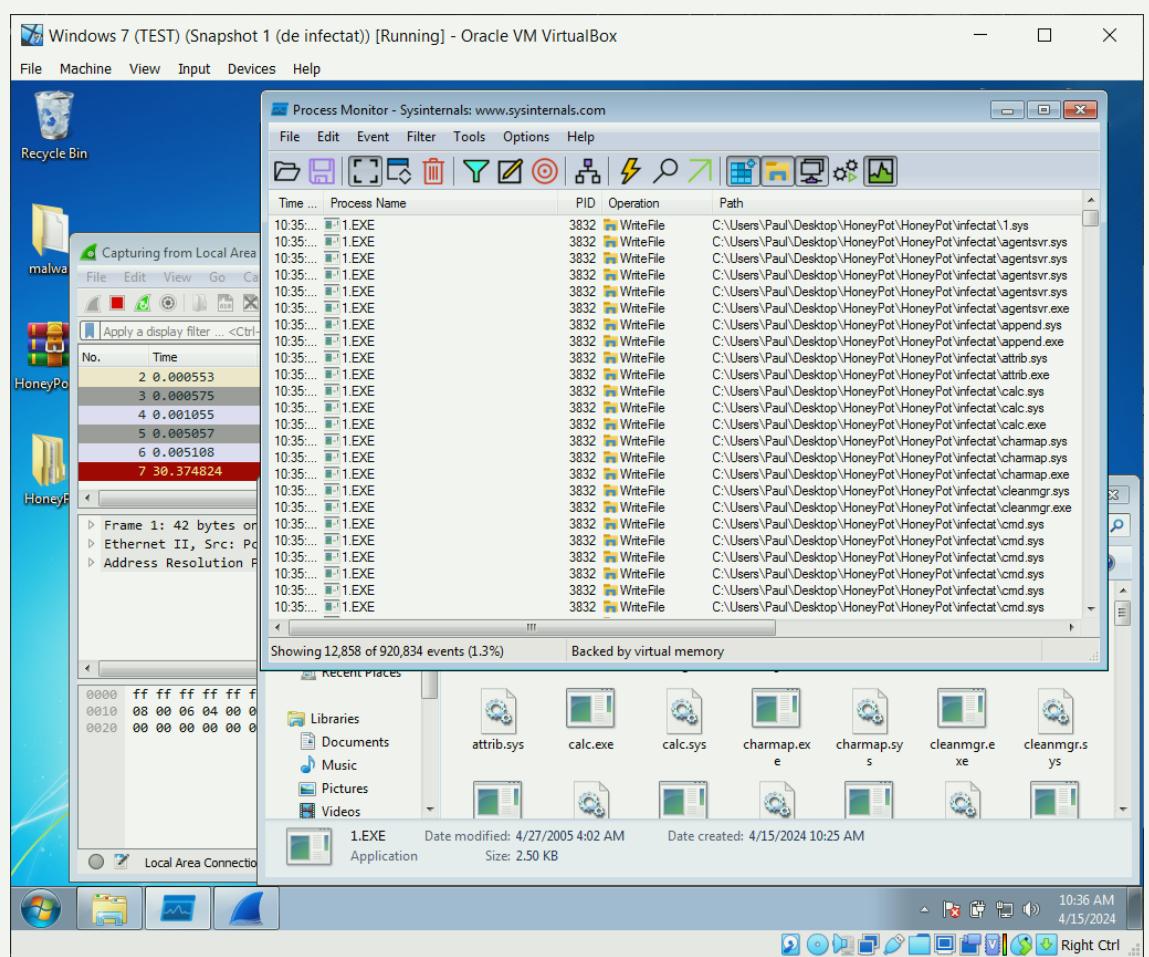
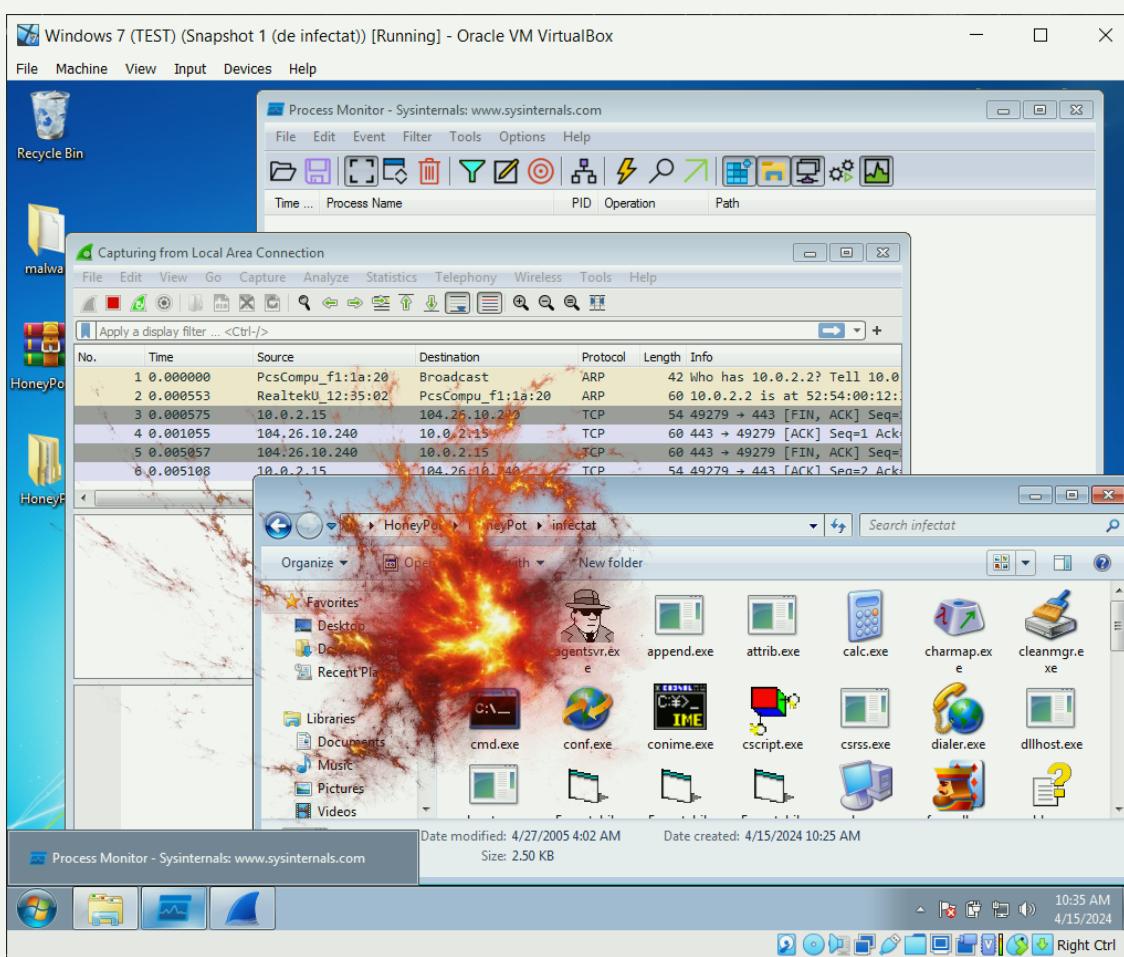
PORNIREA WIRESHARK IN PARALEL CU PROCESS MONITOR



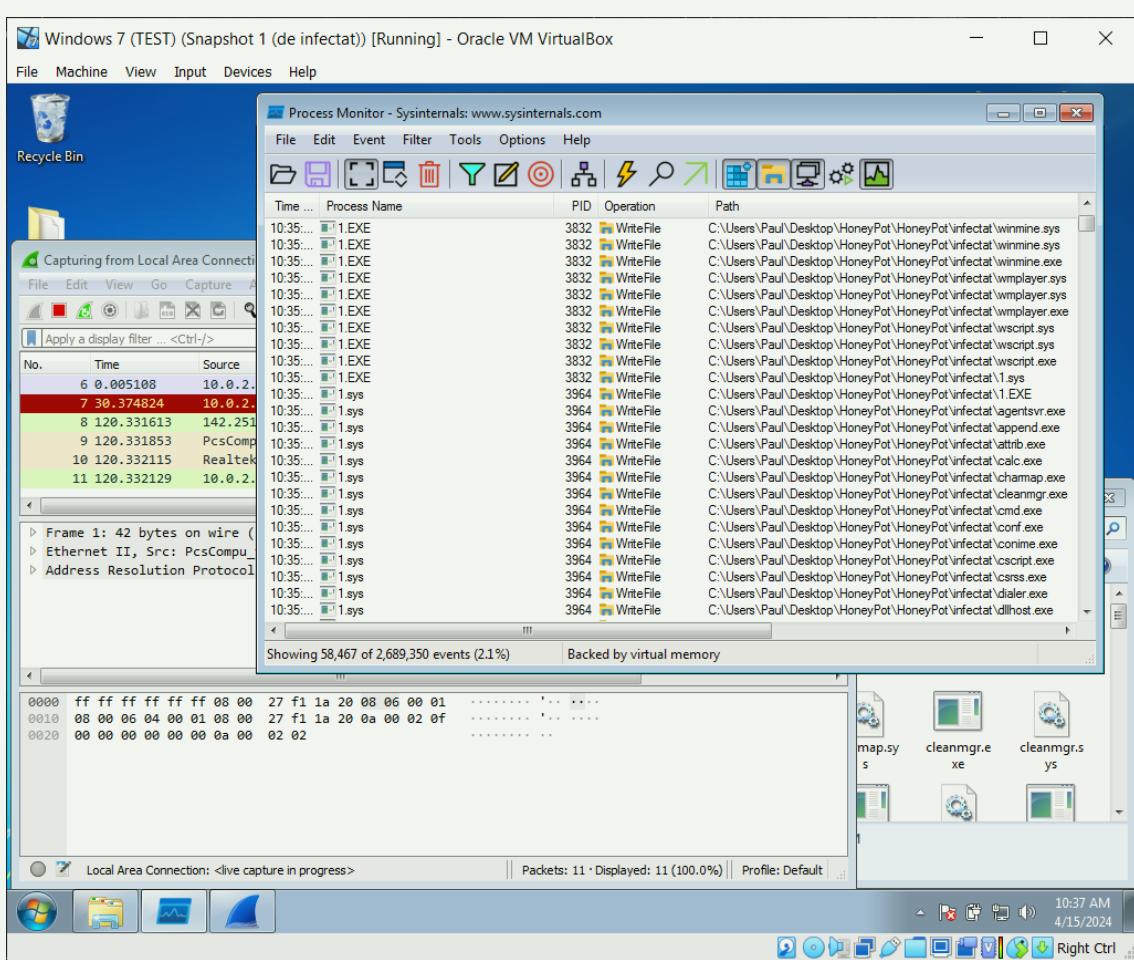
ELIMINAREA ZGOMOTULUI PRODUS DE WIRESHARK



DETONEARE VIRUS & OBSERVATII

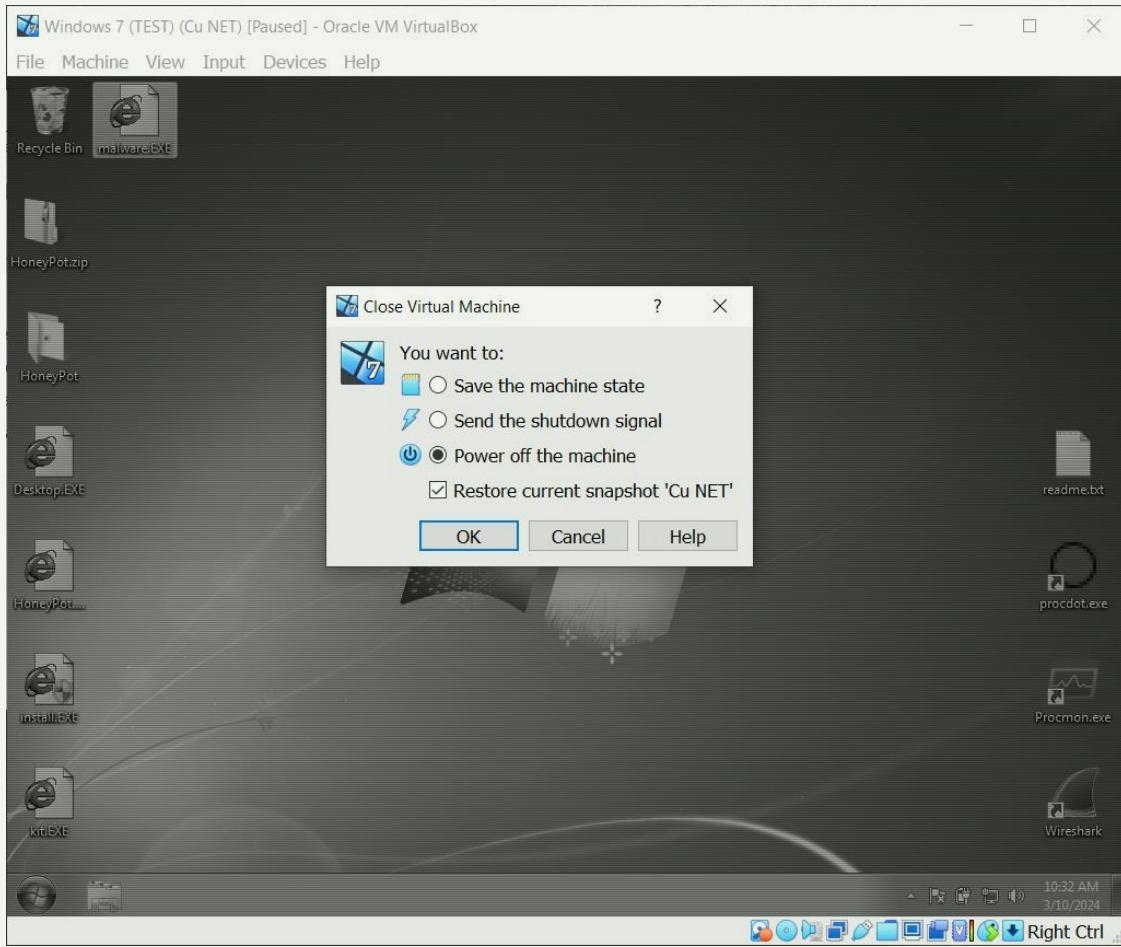


INFECȚIE ÎN DESFĂȘURARE ...



Time	Process Name	PID	Operation	Path	Result	Detail	Sequence
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 0, Length: 65,536, Priority: N...	312
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 65,536, Length: 65,536	313
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 131,072, Length: 65,536	314
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 196,608, Length: 65,536	315
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 262,144, Length: 21,504	316
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	317
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 0, Length: 65,536, Priority: N...	318
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 65,536, Length: 65,536	319
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 131,072, Length: 65,536	320
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 196,608, Length: 65,536	321
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 262,144, Length: 65,536	322
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 327,680, Length: 65,536	323
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 393,216, Length: 65,536	324
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.dll	SUCCESS	Offset: 458,752, Length: 43,520	325
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	326
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 0, Length: 65,536, Priority: N...	327
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 65,536, Length: 54,272	328
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	329
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 0, Length: 65,536, Priority: N...	330
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 65,536, Length: 8,192	331
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	332
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 0, Length: 65,536, Priority: N...	333
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 65,536, Length: 49,152	334
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\winhttp.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	335
10:35...	1.EXE	3832	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\1.sys	SUCCESS	Offset: 0, Length: 4,096, I/O Flags: ...	336
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\1.sys	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	337
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\agentsvr.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	338
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\append.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	339
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\attrib.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	340
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\calc.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	341
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\chamap.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	342
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\cleanmgr.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	343
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\cmd.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	344
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\conf.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	345
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\conime.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	346
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\cscript.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	347
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\csrss.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	348
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\dialer.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	349
10:35...	1.sys	3964	WriteFile	C:\Users\Paul\Desktop\HoneyPot\HoneyPot\infectat\dhcpcsvc.exe	SUCCESS	Offset: 0, Length: 2,560, Priority: Nor...	350

INCHIDERE PRIN RESTAURAREA MASINII VIRTUALE LA VECHEA STARE



- Inchiderea oricărui experiment prin restaurarea masinii virtuale la vechea stare!

c.11.5

VIZUALIZAȚI EVENIMENTELE ‘POST DETONARE’



BCOMPARE – ANALIZA HONEYPOOT

COMPARAREA CONȚINUTULUI A DOUĂ FIȘIERE

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

The image shows two side-by-side windows of the Beyond Compare application, version 3.5.1, running on Windows 7. Both windows have the title "Windows 7 (TEST) [Cu NET] [Running] - Oracle VM VirtualBox". The left window is titled "agentsvr.exe <-> agentsvr.exe - Hex Compare - Beyond Compare" and shows the contents of "C:\...\Win32.Virut.A\Win32.Virut\DE INFECTAT\agentsvr.exe". The right window is also titled "agentsvr.exe <-> agentsvr.exe - Hex Compare - Beyond Compare" and shows the contents of "C:\...\Win32.Virut.A\Win32.Virut\CURAT\agentsvr.exe".

Annotations with red arrows and numbers point to specific areas:

- Annotation 1: Points to the first byte difference in the hex dump, which is highlighted in red. The value at address 00000018 is EE (highlighted in red) in the infected file and 40 in the clean file.
- Annotation 1': Points to the same byte difference in the ASCII dump, where the character '@' is highlighted in red in the infected file and a space character is shown in the clean file.
- Annotation 2: Points to the second byte difference in the hex dump, highlighted in red. The value at address 00000048 is 66 (highlighted in red) in the infected file and 41 in the clean file.
- Annotation 2': Points to the same byte difference in the ASCII dump, where the character '!' is highlighted in red in the infected file and a space character is shown in the clean file.
- Annotation 3: Points to the bottom of the left window's pane, indicating the end of the infected file.
- Annotation 4: Points to the bottom of the right window's pane, indicating the end of the clean file.

Two callout boxes provide additional context:

- A green callout box labeled "Coadă fisier neinfectat" points to the right window's pane.
- A green callout box labeled "Coadă fisier infectat" points to the left window's pane.

PROCESS MONITOR

ANALIZA UNUI MALWARE ÎNTR-O MAȘINĂ VIRTUALĂ (VM)

I. Activitatea Proceselor

- Crearea și terminarea proceselor.** Observați procesele create de malware. Anumite malware-uri pot lansa noi procese, fie pentru a executa sarcini specifice, fie pentru a se masca.
- Relațiile între procese.** Identificați dacă malware-ul creează procese copil sau dacă interacționează cu alte procese existente.

2. Modificări în Sistemul de Fișiere

- Crearea, modificarea și ștergerea fișierelor.** Fiți atenți la fișierele create sau modificate de malware, deoarece acestea pot indica activități precum extracția de date, instalarea de componente suplimentare sau încercări de persistență.
- Accesări suspecte de fișiere.** Monitorizați accesul la fișiere de configurare sau sistem, care ar putea sugera încercări de modificare a setărilor sistemului.

3. Modificări în Registri

- Crearea, modificarea și ștergerea cheilor de registru.** Malware-ul adesea modifică registrii pentru a asigura persistența, a modifica setările sistemului sau a dezactiva funcții de securitate.
- Acces la registri specifici.** Observați accesul la chei de registru ce controlează autorun, servicii, sau setări de rețea.

4. Activitatea de Rețea

- Conexiuni de rețea.** Monitorizați orice încercare de conexiune la adrese IP sau domenii externe, ceea ce poate indica comunicații cu un server de comandă și control (C&C) sau încercări de exfiltrare a datelor.
- Modificări ale setărilor de rețea.** Verificați dacă malware-ul modifică setările de rețea, cum ar fi proxy-uri sau DNS.

5. Hook-uri și DLL-uri Injectate

- Injectarea de cod.** Multe tipuri de malware injectează cod în alte procese pentru a executa operațiuni în mod ascuns sau pentru a obține drepturi de acces mai mari.
- Modificări ale DLL-urilor.** Atunci când un malware adaugă sau modifică DLL-uri, poate afecta funcționalitatea sistemului sau poate obține funcționalități suplimentare.

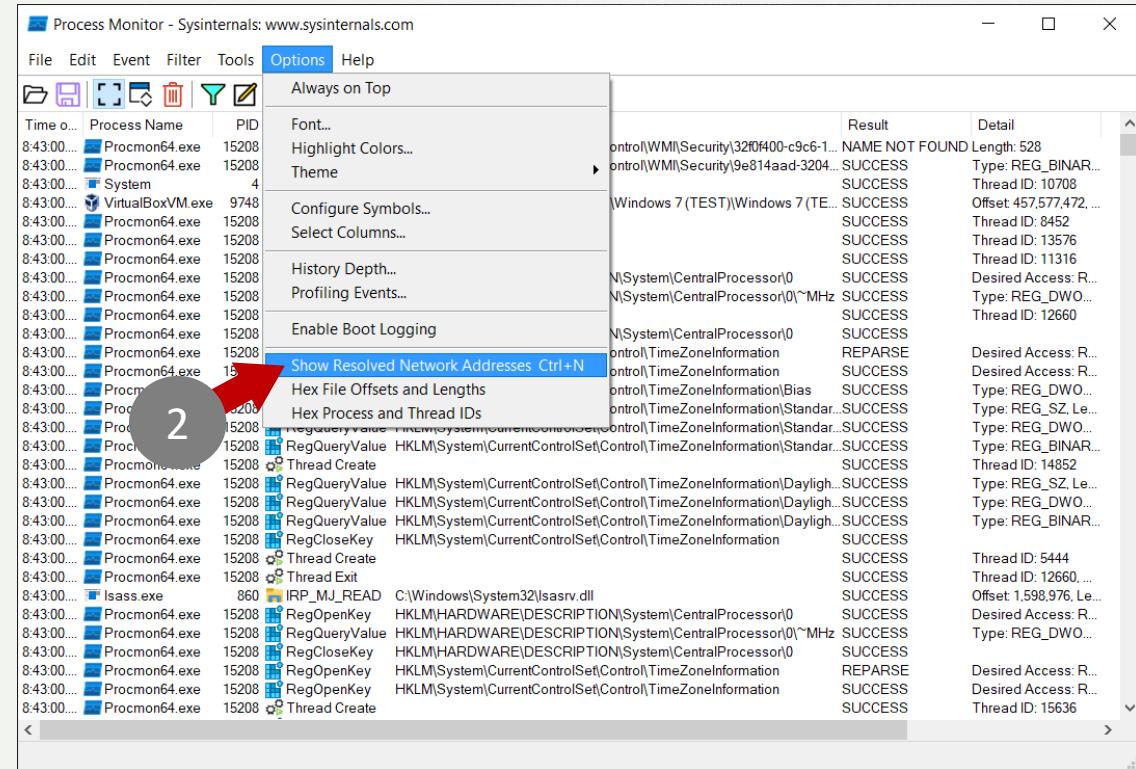
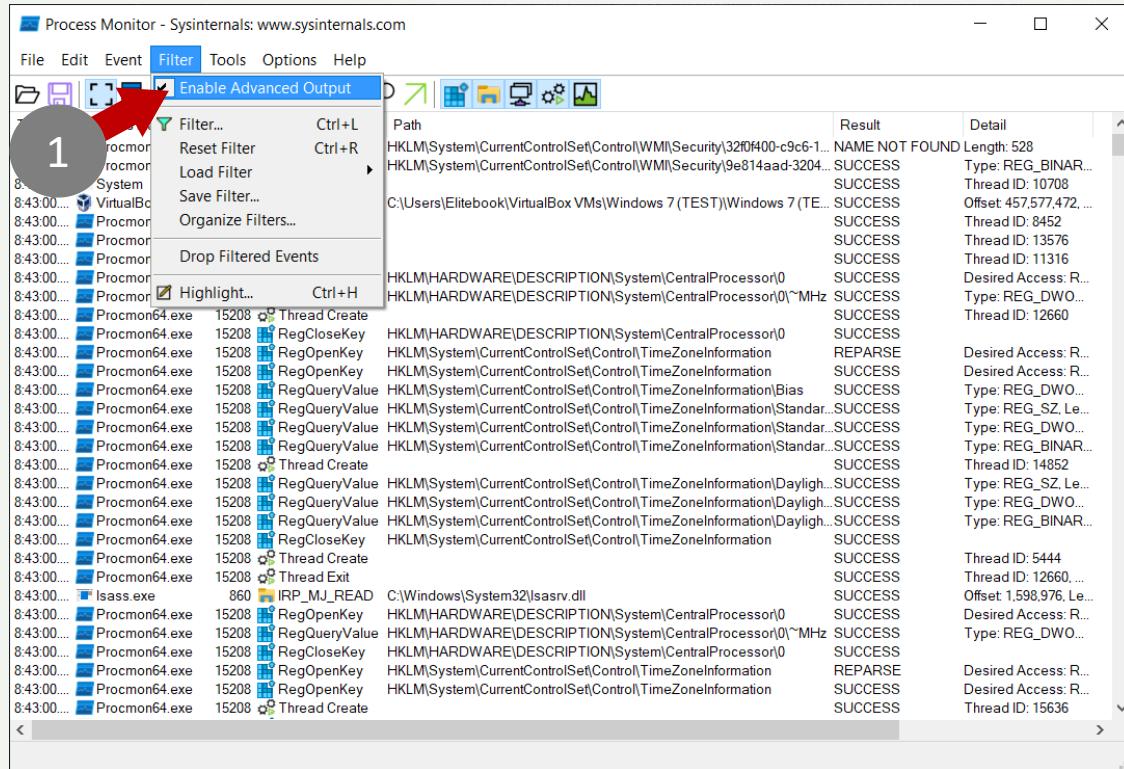
SFATURI GENERALE

PROCESS MONITOR

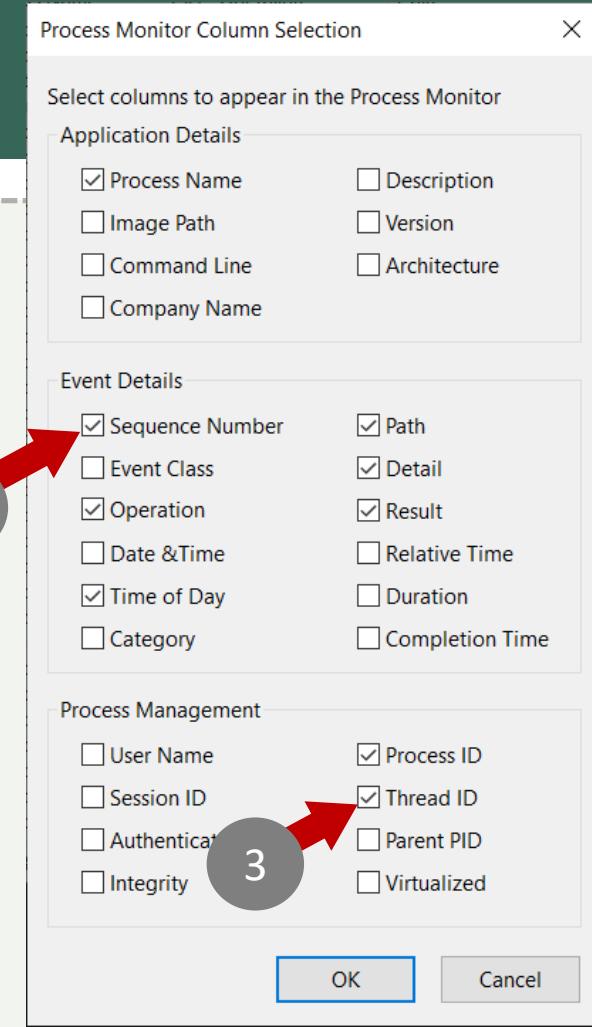
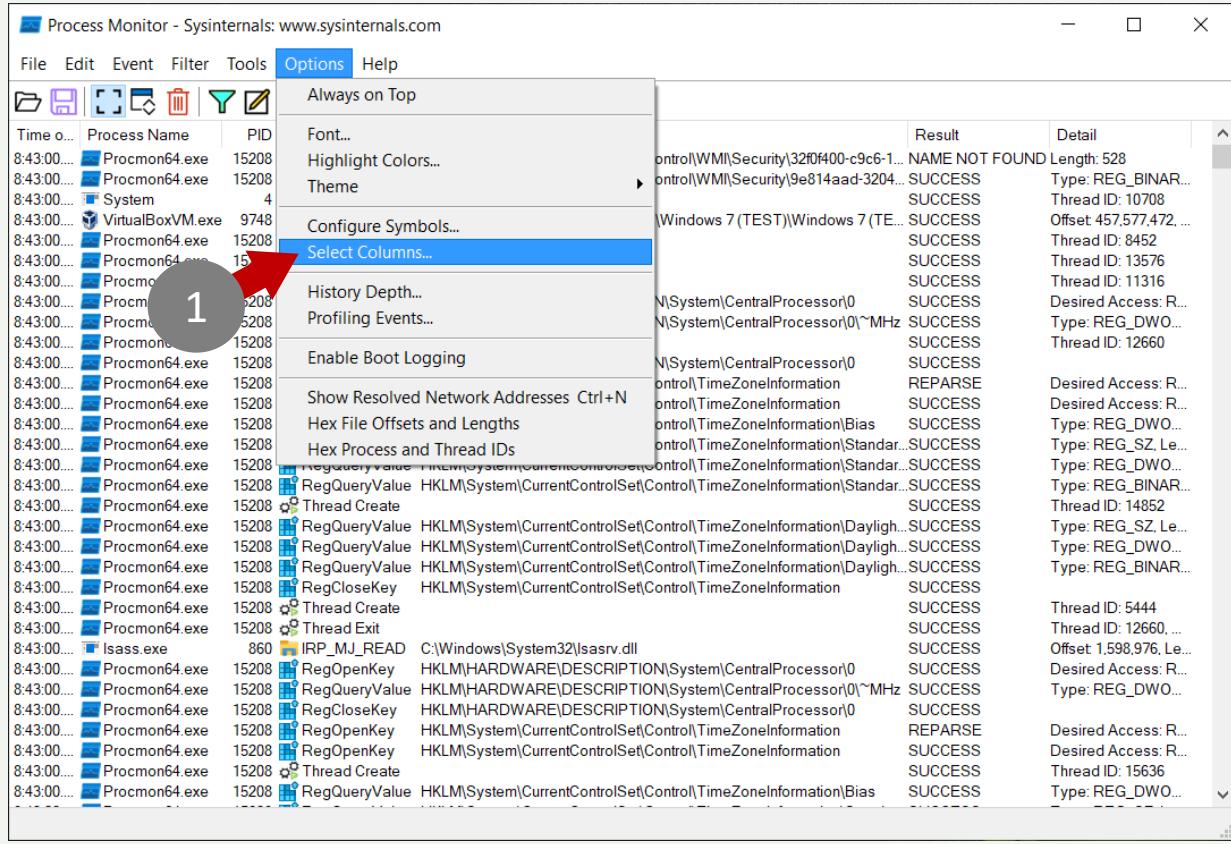
- **Filtrați și sortați datele.** Utilizați filtrele Process Monitor pentru a izola activitățile suspecte și a reduce zgomotul de fundal al activităților sistemului normal.
- **Exportați și salvați logurile.** Salvați logurile de monitorizare pentru analiză ulterioară și pentru a avea un punct de referință.
- **Utilizați snapshot-uri ale VM-ului.** Faceți snapshot-uri înainte și după detonarea malware-ului pentru a putea reveni rapid la o stare cunoscută și curată.
- **Folosiți alte unelte de analiză.** Complementați analiza cu alte unelte de securitate, cum ar fi antivirus, analizor de trafic de rețea, și unelte de analiză de malware pentru o imagine de ansamblu completă.

PROCESS MONITOR

SETUP PENTRU SALVAREA JURNALULUI (ORDINEA COLOANELOR)

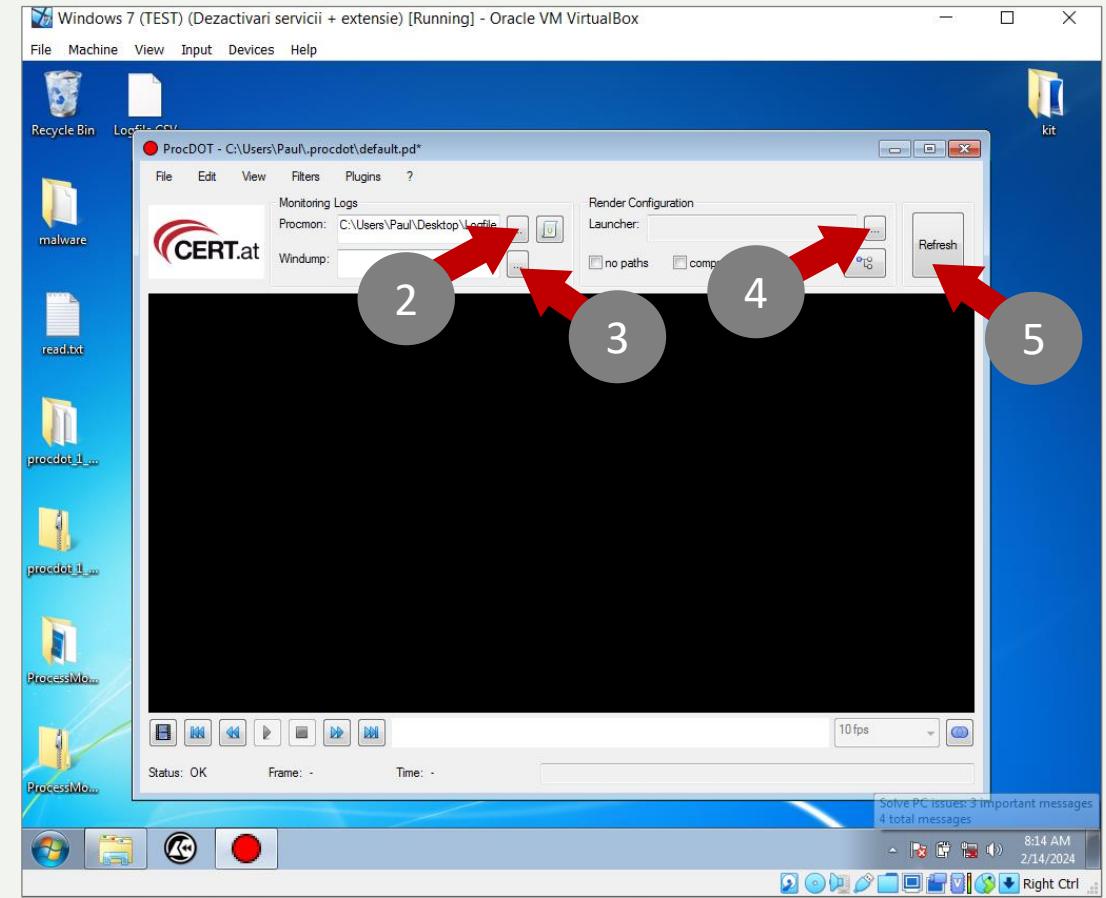
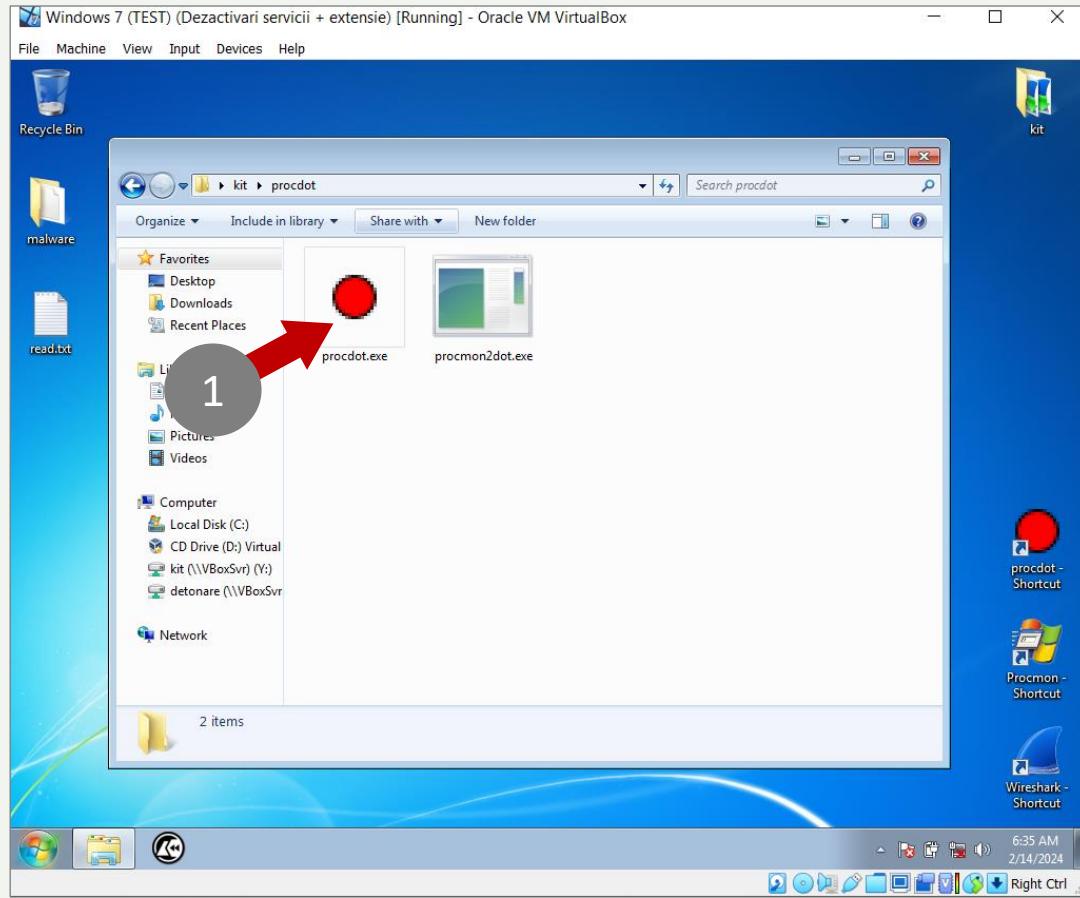


PROCESS MONITOR SETUP



PROCDOT

RULAREA ȘI UTILIZAREA JURNALELOR PROCMON ȘI WIRESHARK



PROCDOT

REZULTAT FINAL

Pornire rapidă în ProcDOT

=====

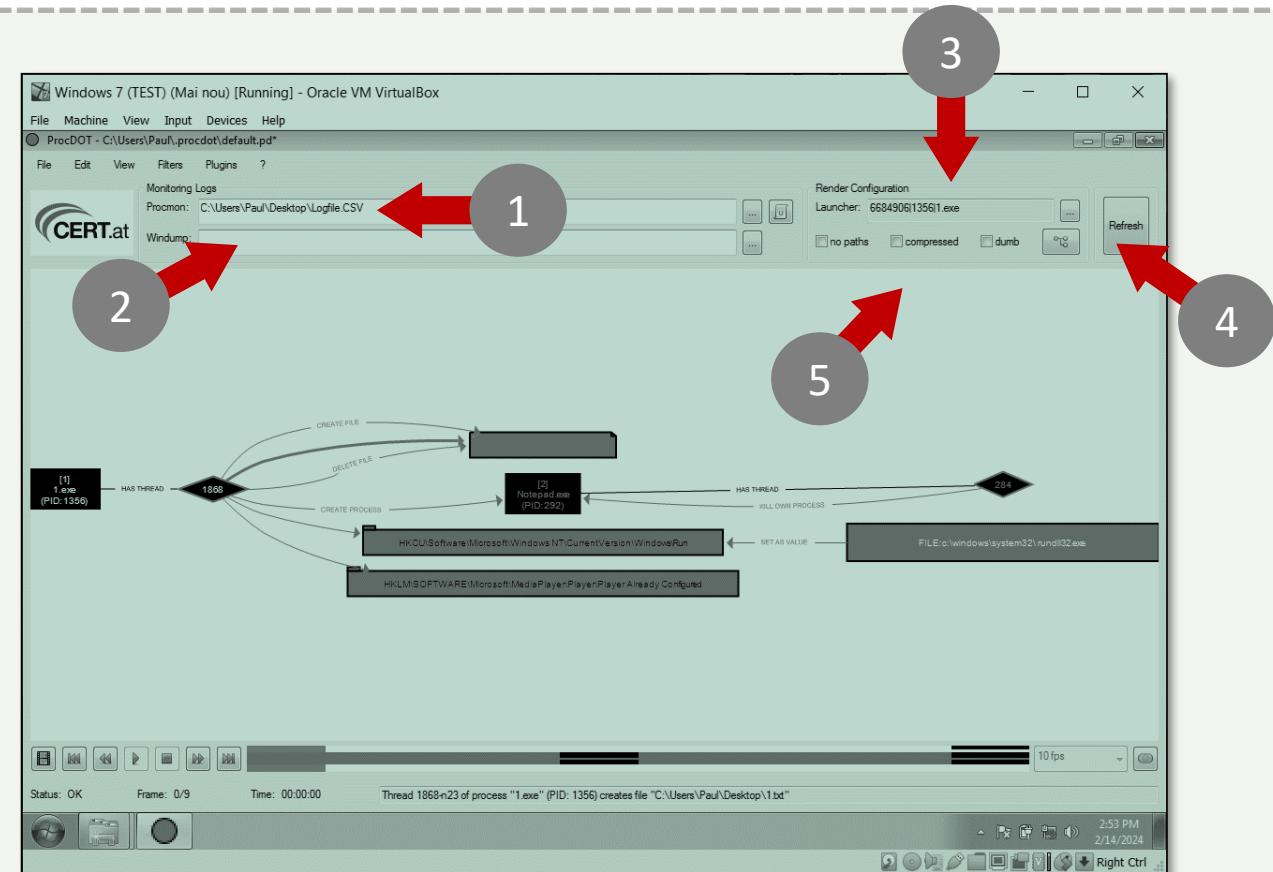
- 1) Selectați fișierele de jurnal (trist, dar adevărat, specificațiile pentru formatul de fișier nativ al Procmon (.PML) nu sunt disponibile (public). Prin urmare, trebuie să exportați fișierul dvs. .PML în .CSV, ceea ce se poate face cu ușurință prin „Salvare”.,, element de meniu din Procmon. Asigurați-vă că selectați „toate evenimentele”.)

- 2) Alegeți modul de reprezentare grafică (fără căi, comprimat)

- 3) Selectați primul proces relevant (malițios) (proces de lansare)

- 4) Faceți clic pe „Reîmprospătare”

dot.exe îl gasiți în graphviz



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>

