


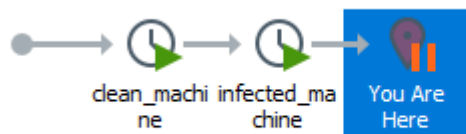
# lab 3

- rularea fisierului malitios

Name	Date modified	Type	Size
 CoronaVirus	5/23/2024 1:17 PM	Application	1,038 KB



- realizare snapshot dupa rulare pentru a pute verifica memoria



Name	Date modified	Type	Size
564d172f-6fc5-b362-bd32-3bbea1b86a38...	5/23/2024 11:27 PM	File folder	
caches	5/23/2024 10:01 PM	File folder	
windows.vmx.lck	5/23/2024 9:55 PM	File folder	
windows-disk1.vmdk.lck	5/23/2024 11:27 PM	File folder	
windows-disk1-000001.vmdk.lck	5/23/2024 11:27 PM	File folder	
windows-disk1-000002.vmdk.lck	5/23/2024 11:27 PM	File folder	
564d172f-6fc5-b362-bd32-3bbea1b86a38...	5/23/2024 11:27 PM	VMEM File	8,388,608 KB
vmware	5/23/2024 11:27 PM	Text Document	0 KB
vmware-0	5/23/2024 11:27 PM	Text Document	198 KB
vmware-1	5/23/2024 11:16 PM	Text Document	175 KB
vmware-2	5/23/2024 11:09 PM	Text Document	179 KB
windows.scoreboard	5/23/2024 11:27 PM	SCOREBOARD File	8 KB
windows	5/23/2024 11:27 PM	VMware snapshot ...	1 KB
windows	5/23/2024 11:27 PM	VMware virtual m...	4 KB
windows	5/23/2024 11:27 PM	VMware Team Me...	1 KB
windows-0.scoreboard	5/23/2024 11:16 PM	SCOREBOARD File	8 KB
windows-1.scoreboard	5/23/2024 11:09 PM	SCOREBOARD File	8 KB
windows-2.scoreboard	5/23/2024 11:03 PM	SCOREBOARD File	8 KB
windows-disk1.vmdk	5/23/2024 10:08 PM	VMDK File	43,102,336 ...
windows-disk1-000001.vmdk	5/23/2024 11:28 PM	VMDK File	78,336 KB
windows-disk1-000002.vmdk	5/23/2024 11:25 PM	VMDK File	11,423,936 ...
windows-file1	5/23/2024 11:27 PM	VMware Virtual M...	265 KB
windows-Snapshot1.vmem	5/23/2024 10:11 PM	VMEM File	8,388,608 KB
windows-Snapshot1	5/23/2024 10:11 PM	VMware virtual m...	4,226 KB
windows-Snapshot3.vmem	5/23/2024 11:27 PM	VMEM File	8,388,608 KB
windows-Snapshot3	5/23/2024 11:27 PM	VMware virtual m...	4,215 KB

- windows-Snapshot3.vmem - dump-ul de memorie al masinii virtuale
- windows-Snapshot3 - config pentru vmware

**python vol.py -f E:\vm\windows\windows-Snapshot3.vmem windows.pslist**

Executand aceasta comanda putem observa procesul CoronaVirus care este virusul executat pe masina

5396	6088	msedge.exe	0xba0812ac3080	14	-	1	False	2024-05-23 20:18:00.000000	N/A	Disabled
1824	812	svchost.exe	0xba0812b95080	3	-	1	False	2024-05-23 20:18:27.000000	N/A	Disabled
10056	976	CHXSmartScreen	0xba0812d80080	36	-	1	False	2024-05-23 20:18:44.000000	N/A	Disabled
2260	976	RuntimeBroker.	0xba0808f0d080	5	-	1	False	2024-05-23 20:18:48.000000	N/A	Disabled
6192	5956	CoronaVirus.exe	0xba0811ccf080	18	-	1	True	2024-05-23 20:19:01.000000	N/A	Disabled
9864	6192	cmd.exe	0xba0813c5a080	0	-	1	False	2024-05-23 20:19:13.000000	2024-05-23 20:20:08.000000	Disabled
6628	9864	mode.com	0xba08167d6080	0	-	1	False	2024-05-23 20:19:29.000000	2024-05-23 20:19:31.000000	Disabled
10748	9864	vssadmin.exe	0xba0814dcf080	0	-	1	False	2024-05-23 20:19:31.000000	2024-05-23 20:20:08.000000	Disabled
11216	812	svchost.exe	0xba0813e46080	6	-	0	False	2024-05-23 20:19:55.000000	N/A	Disabled
5368	2544	SearchProtocol	0xba0813989080	11	-	0	False	2024-05-23 20:24:28.000000	N/A	Disabled
11128	6192	cmd.exe	0xba0811af3080	0	-	1	False	2024-05-23 20:24:46.000000	2024-05-23 20:24:48.000000	Disabled
9396	11128	mode.com	0xba081221d080	0	-	1	False	2024-05-23 20:24:47.000000	2024-05-23 20:24:47.000000	Disabled
5972	2544	SearchFilterHo	0xba0808ddf080	7	-	0	False	2024-05-23 20:24:47.000000	N/A	Disabled
5824	11128	vssadmin.exe	0xba0811097080	0	-	1	False	2024-05-23 20:24:48.000000	2024-05-23 20:24:48.000000	Disabled
6432	812	VSSVC.exe	0xba0811d3a080	8	-	0	False	2024-05-23 20:24:48.000000	N/A	Disabled
4064	6192	mshta.exe	0xba0812a6a080	17	-	1	False	2024-05-23 20:24:48.000000	N/A	Disabled
2232	6192	mshta.exe	0xba08114ac080	18	-	1	False	2024-05-23 20:24:48.000000	N/A	Disabled
5948	976	backgroundTask	0xba08161d3080	9	-	1	False	2024-05-23 20:24:51.000000	N/A	Disabled
3360	976	RuntimeBroker.	0xba0813c1c080	8	-	1	False	2024-05-23 20:24:51.000000	N/A	Disabled

**python vol.py -f E:\vm\windows\windows-Snapshot3.vmem windows.cmdline**

Dupa ce am aflat procesul suspect din spate putem vizualiza ce comanda porneste acest proces

care foloseste **-a** care poate fi folosit pentru a porni anumite instructiuni

2260	RuntimeBroker.	C:\Windows\System32\RuntimeBroker.exe -Embedding
6192	CoronaVirus.exe	"C:\Users\User\Desktop\CoronaVirus.exe" -a
9864	cmd.exe	Required memory at 0xcace04c020 is not valid (process exited?)

**python .\vol.py -f E:\vm\windows\windows-Snapshot3.vmem windows.dlllist**

Folosit aceasta comanda vom putea vedea toate dll-urile incarcate in timpul realizarii

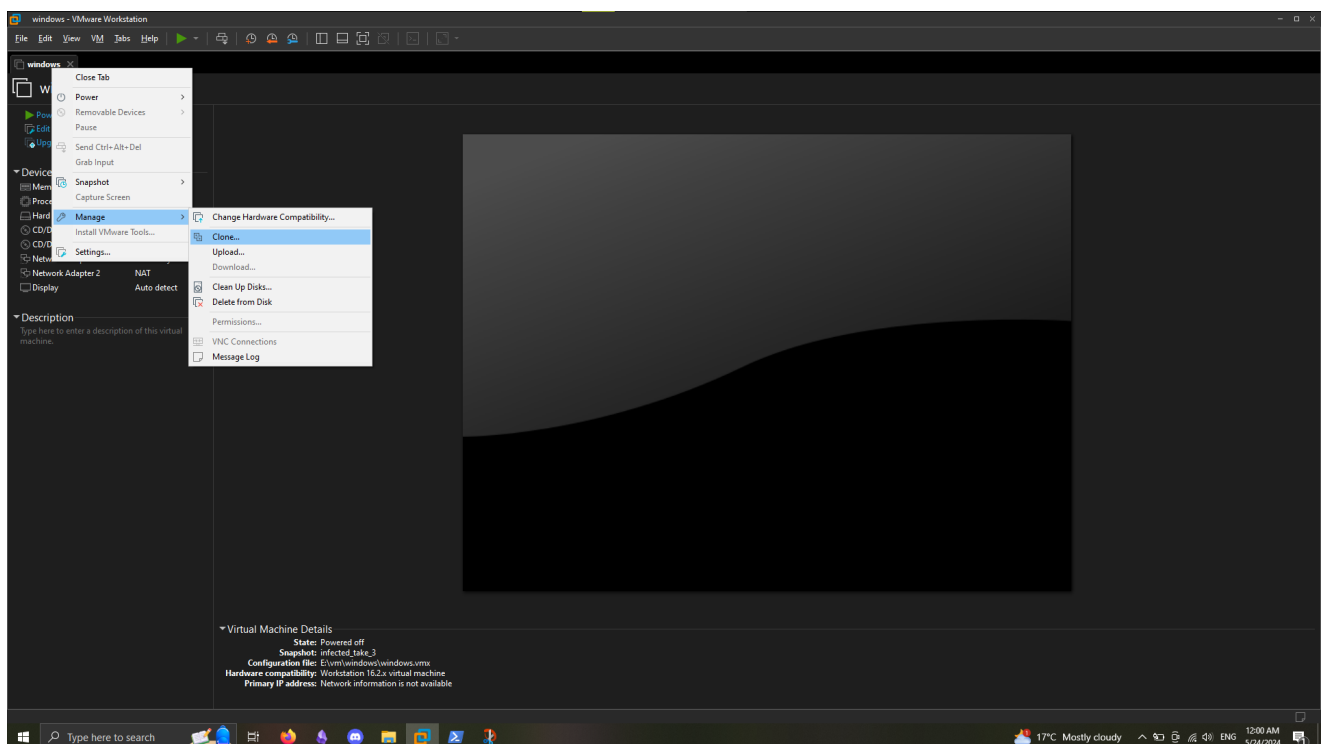
dumpului, analizand am observat si aici procesul CoronaVirus.exe care foloseste urmatoarele

DLL-uri:

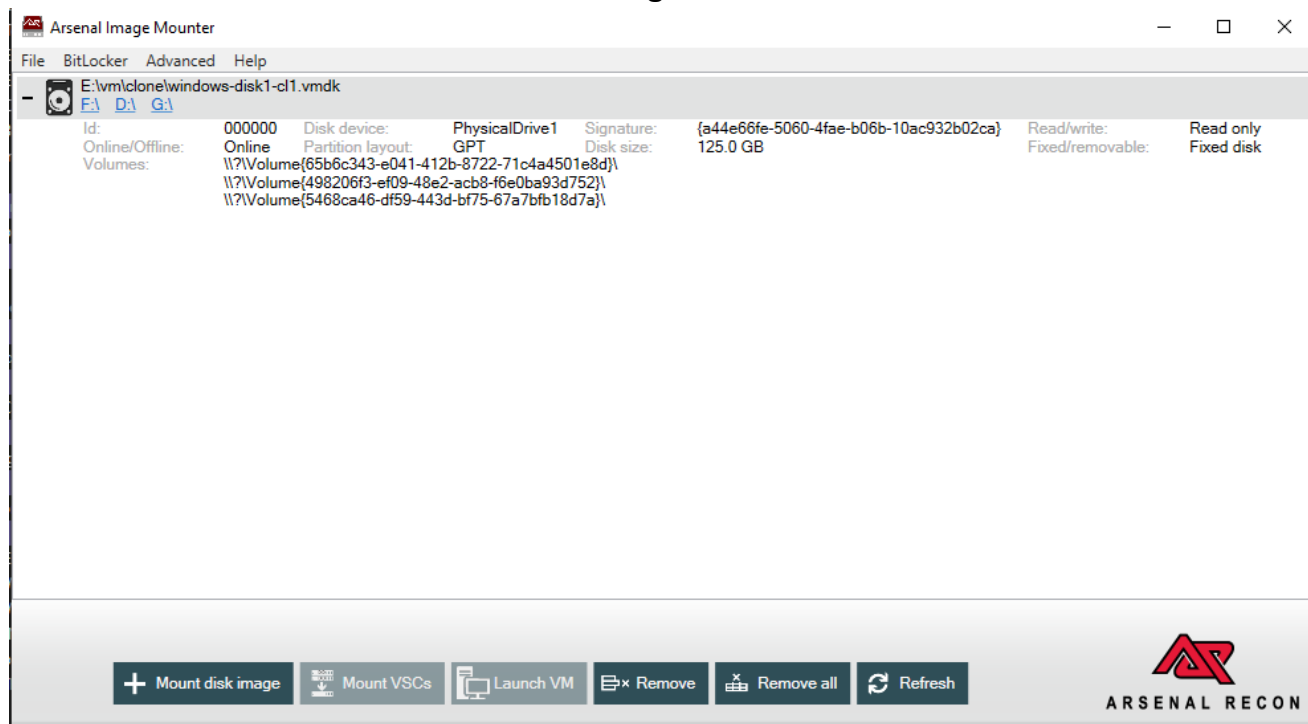
1. **ntdll.dll**: Este o componentă fundamentală a sistemului de operare Windows, furnizând funcționalități esențiale pentru gestionarea obiectelor, memoriei, proceselor și fișierelor.
2. **wow64.dll**: Este o componentă a subsistemului WoW64 (Windows-on-Windows 64-bit) care permite executarea aplicațiilor de 32 de biți pe un sistem de operare de 64 de biți. Acest modul este responsabil pentru gestionarea traducerii instrucțiunilor și gestionarea compatibilității între arhitecturile de 32 de biți și 64 de biți.
3. **wow64base.dll**: Face, de asemenea, parte din subsistemul WoW64 și oferă funcționalități de bază necesare pentru executarea aplicațiilor de 32 de biți pe un sistem de operare de 64 de biți.
4. **wow64win.dll**: Este parte a subsistemului WoW64 și furnizează suport pentru funcțiile Windows API pentru aplicațiile de 32 de biți care rulează pe un sistem de operare de 64 de biți.
5. **wow64con.dll**: Acest modul oferă suport pentru interacțiunea cu consola pentru aplicațiile de 32 de biți care rulează pe un sistem de operare de 64 de biți. Este responsabil pentru asigurarea compatibilității cu interfața text a sistemului de operare.

2260	RuntimeBroker.	0x7ffc47860000	0x28000	edputil.dll	C:\Windows\SYSTEM32\edputil.dll	2024-05-23 20:18:48.000000	Disabled	
6192	CoronaVirus.exe	0x480000	0x16f000	CoronaVirus.exe	C:\Users\User\Desktop\CoronaVirus.exe	2024-05-23 20:19:01.000000	Disabled	Disabled
6192	CoronaVirus.exe	0x7ffc55390000	0x216000	ntdll.dll	C:\Windows\SYSTEM32\ntdll.dll	2024-05-23 20:19:01.000000	Disabled	Disabled
6192	CoronaVirus.exe	0x7ffc54470000	0x57000	wow64.dll	C:\Windows\System32\wow64.dll	2024-05-23 20:19:01.000000	Disabled	Disabled
6192	CoronaVirus.exe	0x7ffc54460000	0x9000	wow64base.dll	C:\Windows\System32\wow64base.dll	2024-05-23 20:19:01.000000	Disabled	Disabled
6192	CoronaVirus.exe	0x7ffc544e0000	0x8b000	wow64win.dll	C:\Windows\System32\wow64win.dll	2024-05-23 20:19:01.000000	Disabled	Disabled
6192	CoronaVirus.exe	0x7ffc54630000	0x16000	wow64con.dll	C:\Windows\System32\wow64con.dll	2024-05-23 20:19:01.000000	Disabled	Disabled
6192	CoronaVirus.exe	0x77630000	0xa000	wow64cpu.dll	C:\Windows\System32\wow64cpu.dll	2024-05-23 20:19:01.000000	Disabled	Disabled

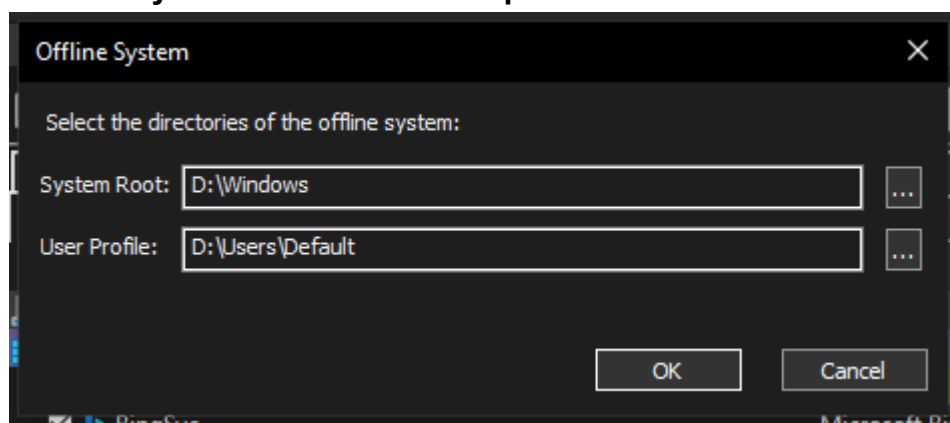
## Crearea unei clone



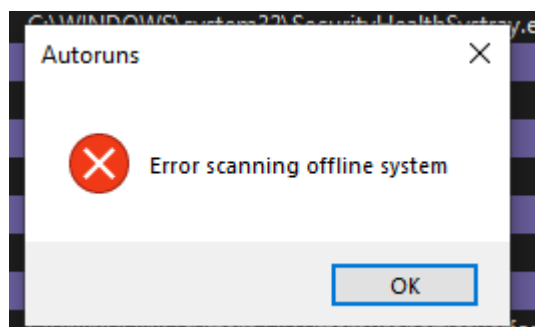
## Montarea sistemului offline in arsenal image mounter



## Setarea system root-ului si user profile in autoruns

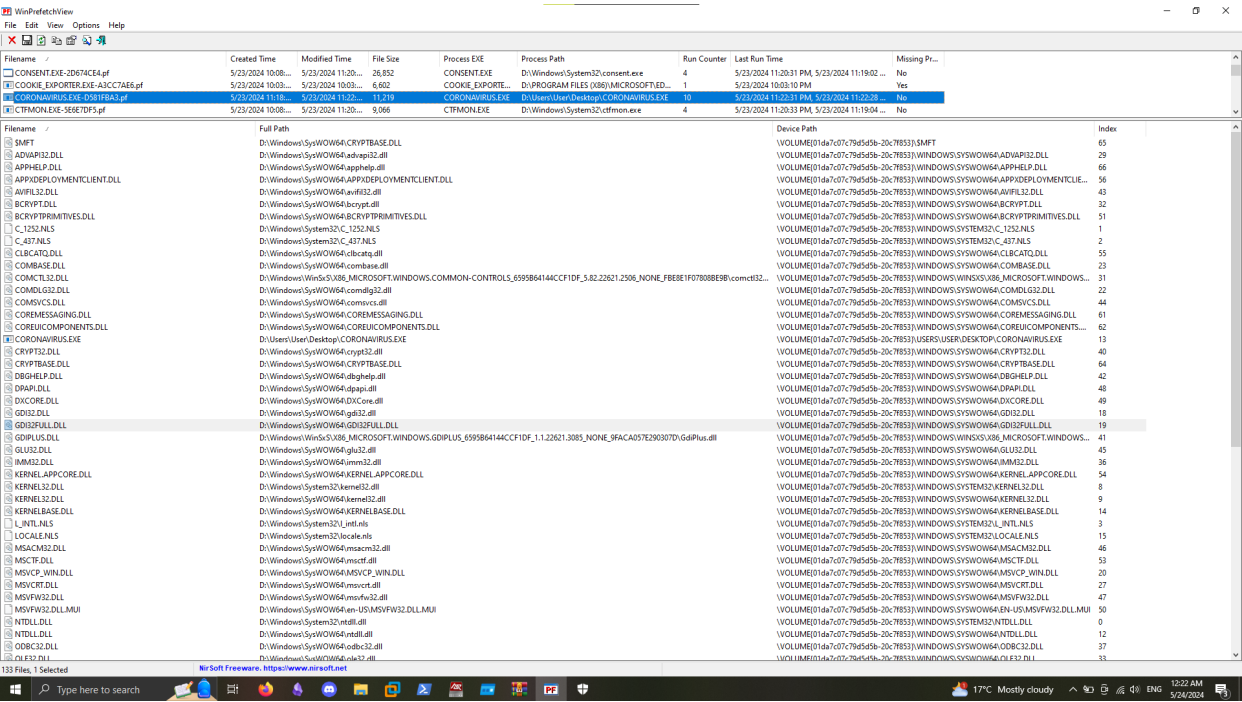


## Eroare la scanarea sistemului offline



- Utilizand WinPrefetchView am putut vedea folderul prefetch din sistemul infectat, astfel am vazut lista capturata la momentul realizarii clonei de dlluri folosita, e salvata intr-un

# fișier .txt in folder-ul PMRI de pe github



## Concluzie

Am inițiat o infecție pe sistemul de operare Windows folosind fișierul "CoronaVirus.exe". Am încercat să înțeleg cum funcționează acest virus și cum afectează sistemul folosind unelte precum Volatility pentru a face un snapshot al memoriei, Arsenal Image Mounter pentru a examina sistemul offline, Autoruns pentru a identifica setările sistemului și WinPrefetchView pentru a observa activitatea recentă a fișierelor și a aplicațiilor.

1. Am găsit un fișier executabil suspect numit "CoronaVirus.ex" în sistemul de operare Windows.
2. Am identificat și am analizat procesul asociat cu acest fișier, împreună cu comenzile pe care le rulează.
3. Am văzut că sistemul a încărcat unele componente importante și altele folosite pentru a permite rularea aplicațiilor mai vechi pe sistemul nou.
4. Am încercat să facem o copie a sistemului pentru investigații, dar am întâmpinat dificultăți.
5. Am folosit o unealtă numită WinPrefetchView pentru a vedea ce aplicații și fișiere au fost utilizate recent pe sistem.