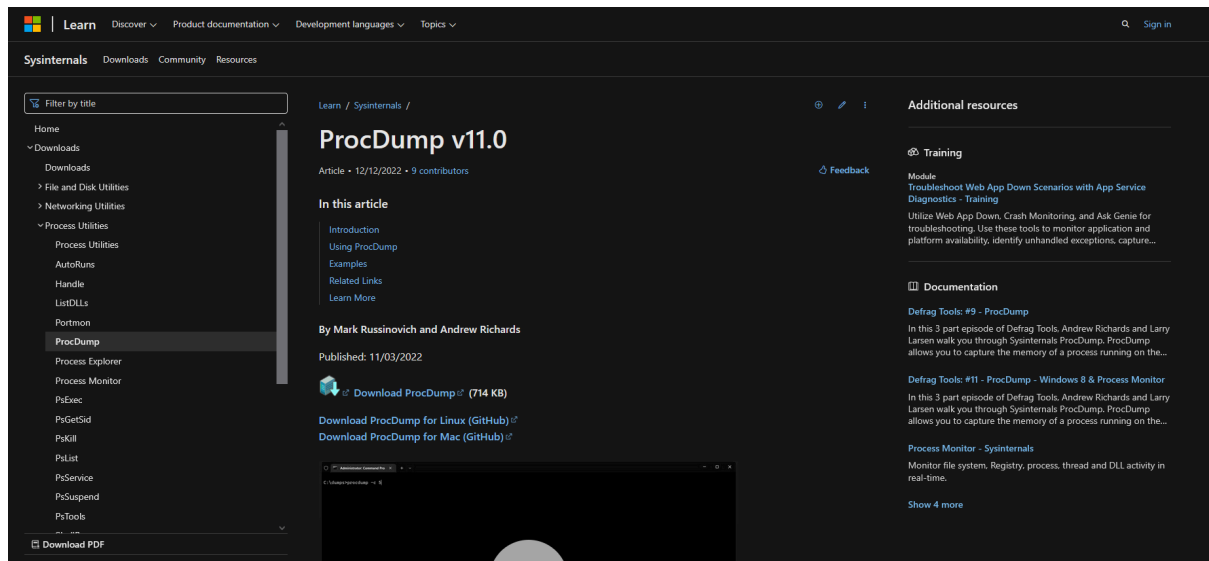
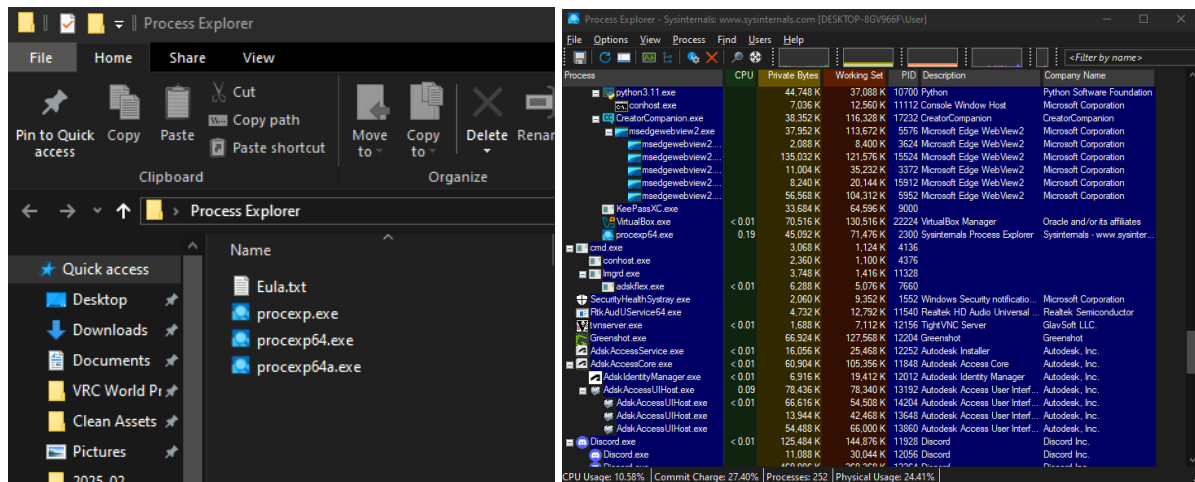


Consegna S11/L1


ho scaricato process explorer dal sito originale di microsoft



Successivamente l'ho estratto in una cartella a scelta e apro il file chiamato processxp.exe



Dopo averlo estratto ho aperto process explorer. process explorer ci permetterà di analizzare tutti i processi nel sistema. per selezionare una specifica applicazione dobbiamo

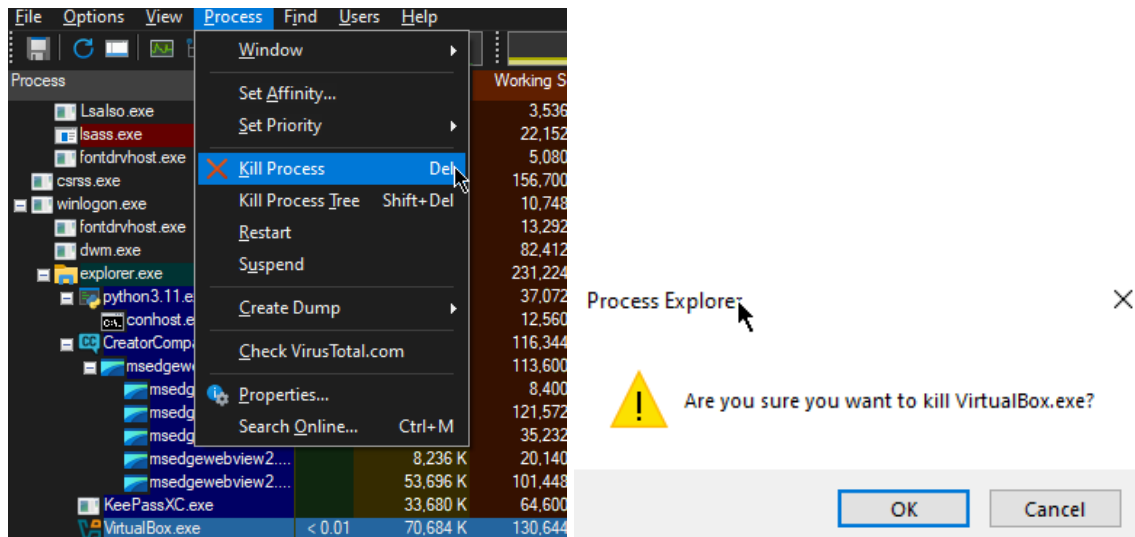
cliccare e tenere premuto il tasto destro questa icona  e rilasciare il tasto destro su un'applicazione a scelta se come forse stiamo cercando di muovere un file.



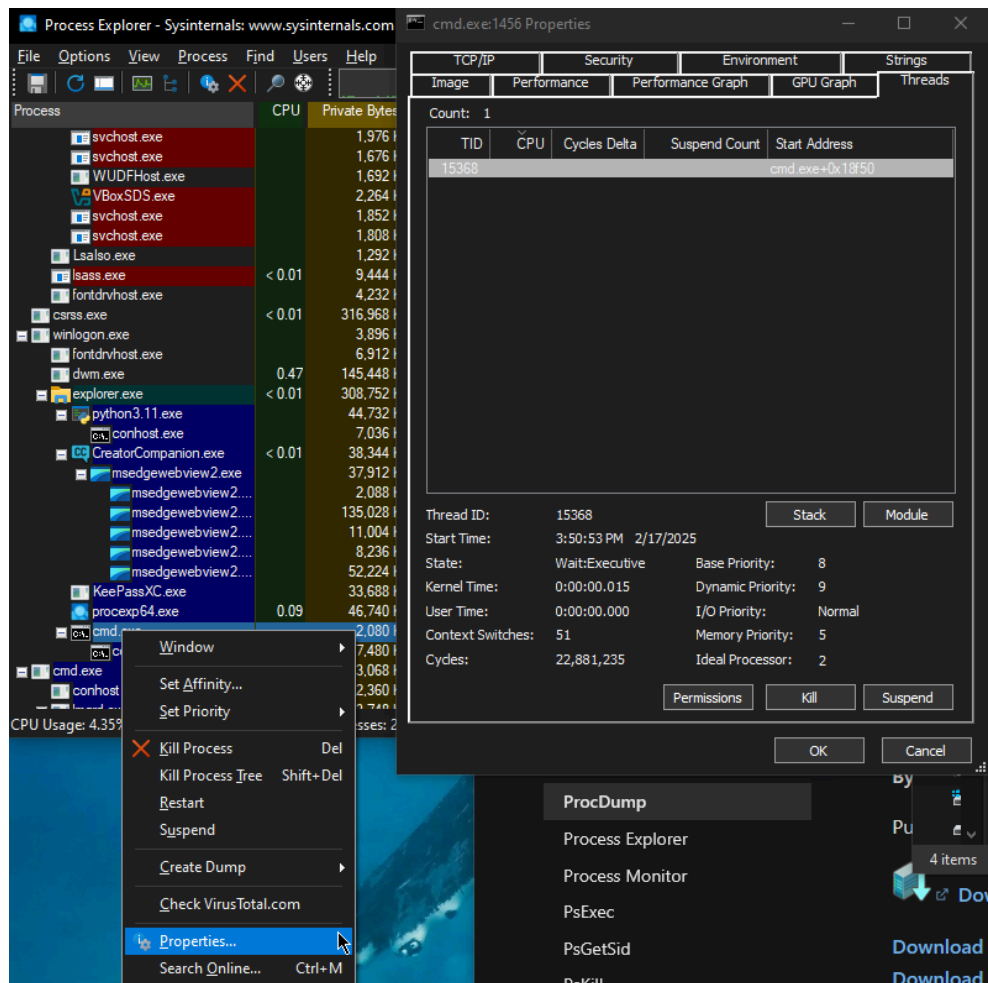
Dopo aver lasciato il click possiamo vedere che Process explorer ha selezionato l'applicazione che abbiamo scelto.

KeePassXC.exe		33,688 K	64,604 K	9000		
VirtualBox.exe	< 0.01	70,516 K	130,532 K	22224	VirtualBox Manager	Oracle and/or its affiliates
procexp64.exe	0.19	45,000 K	71,508 K	2300	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		3,068 K	1,124 K	4136		

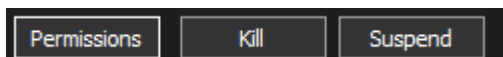
Per terminare il processo dobbiamo cliccare in alto su process e cliccare end process.



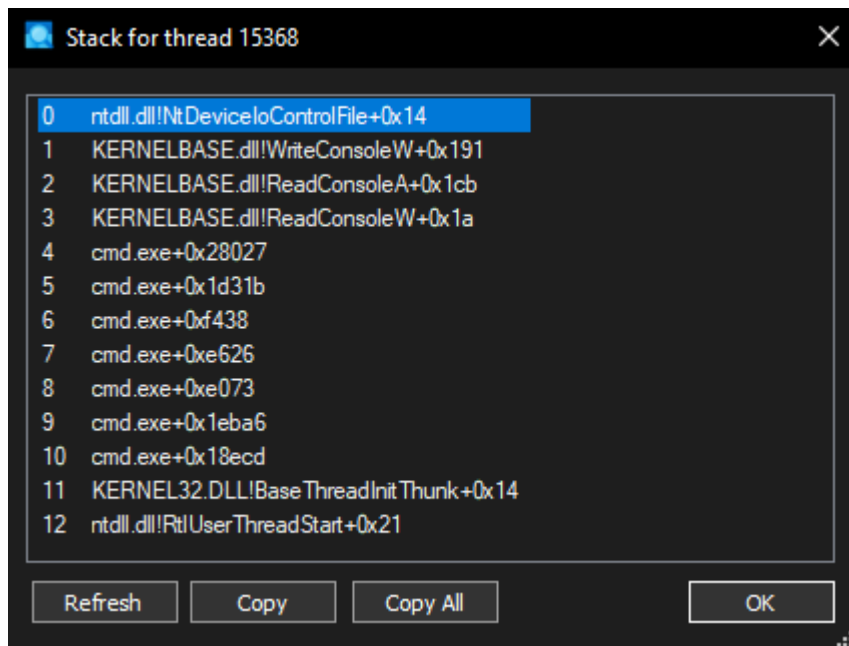
Per esplorare i thread dobbiamo aprire command prompt premendo **Win + R** e scrivendo cmd dopo di che dobbiamo andare su process explorer e selezionare la nostra finestra di cmd e cliccare con il tasto destro e cliccare proprietà successivamente dobbiamo cliccare su threads.



Come possiamo vedere possiamo vedere i permessi dell'applicazione o sospendere o terminarla completamente.



Cliccando sul risultato dove c'è TID possiamo vedere tutti i thread che utilizza il programma.



Funzioni dei thread

1. ntdll.dll!NtDeviceIoControlFile+0x14

Funzione di sistema a basso livello (parte del kernel di Windows NT) utilizzata per operazioni di I/O.

NtDeviceIoControlFile viene spesso usata per inviare comandi di controllo ai dispositivi.

2. KERNELBASE.dll!WriteConsoleW+0x191

WriteConsoleW scrive l'output nella console in formato Unicode.

3. KERNELBASE.dll!ReadConsoleA+0x1cb

ReadConsoleA legge l'input dalla console (versione ANSI).

4. KERNELBASE.dll!ReadConsoleW+0x1a

ReadConsoleW legge l'input dalla console (versione Unicode).

5. KERNEL32.DLL!BaseThreadInitThunk+0x14

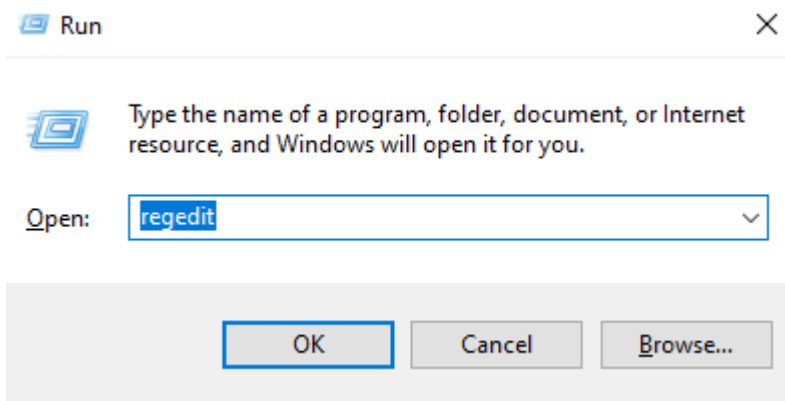
Funzione standard utilizzata all'avvio di un nuovo thread.

7. ntdll.dll!RtlUserThreadStart+0x21

Punto di ingresso per un nuovo thread in modalità utente.

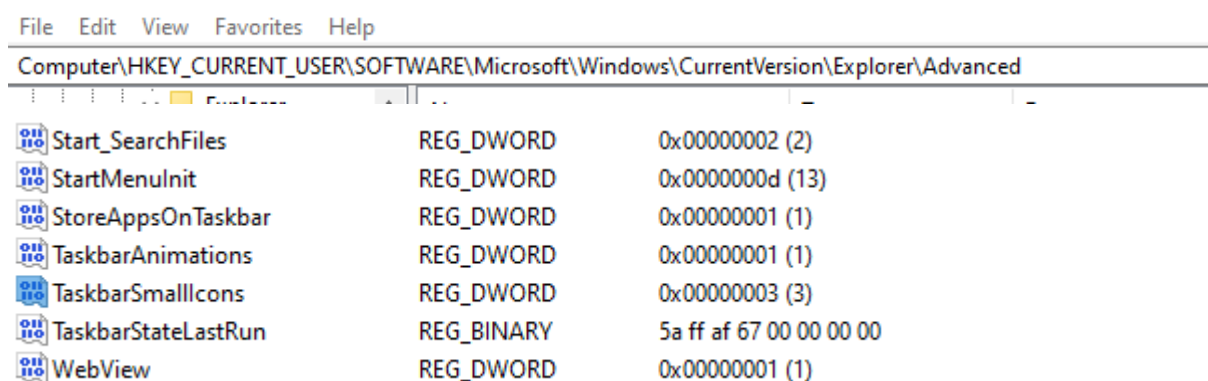
Modifica Windows con regedit

ho premuto WIN+ R scritto regedit

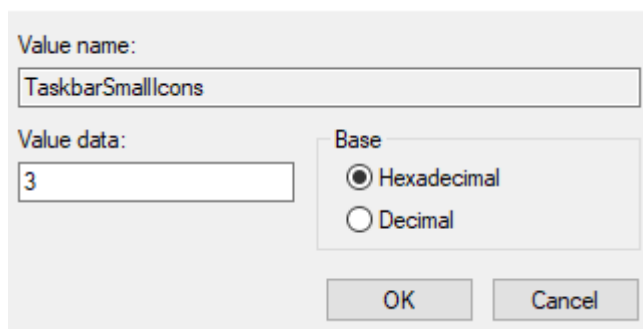


successivamente sono andato in questa path:

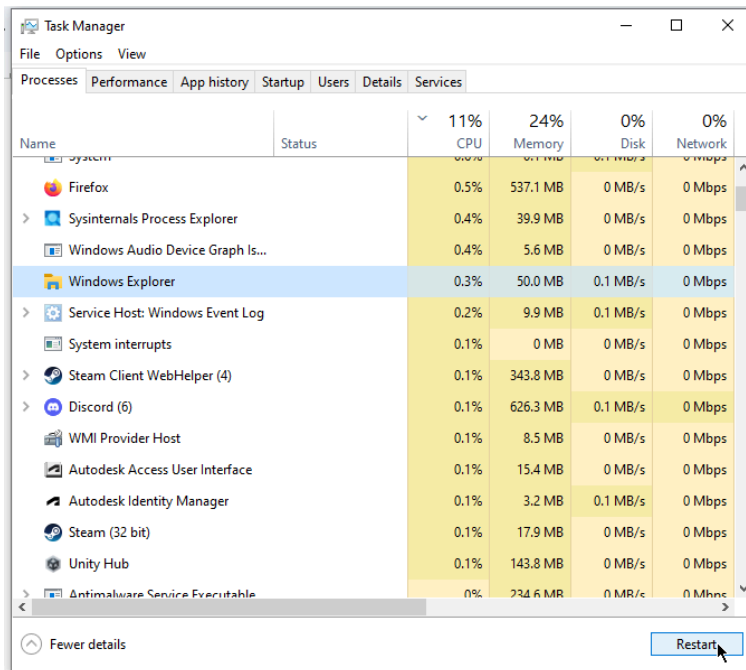
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced



Dopo aver navigato in quella path ho creato un file **DWORD 32bit** e l'ho nominato **TaskbarSmallIcons**. all'interno del file che ho creato gli ho assegnato il valore di **3** che andrà a modificare la dimensione delle icone nella taskbar.



Dopo aver cliccato ok dobbiamo aprire task manager e riavviare windows explorer



Come possiamo vedere dopo aver cliccato restart a windows explorer ha modificato la grandezza delle icone nella taskbar.

