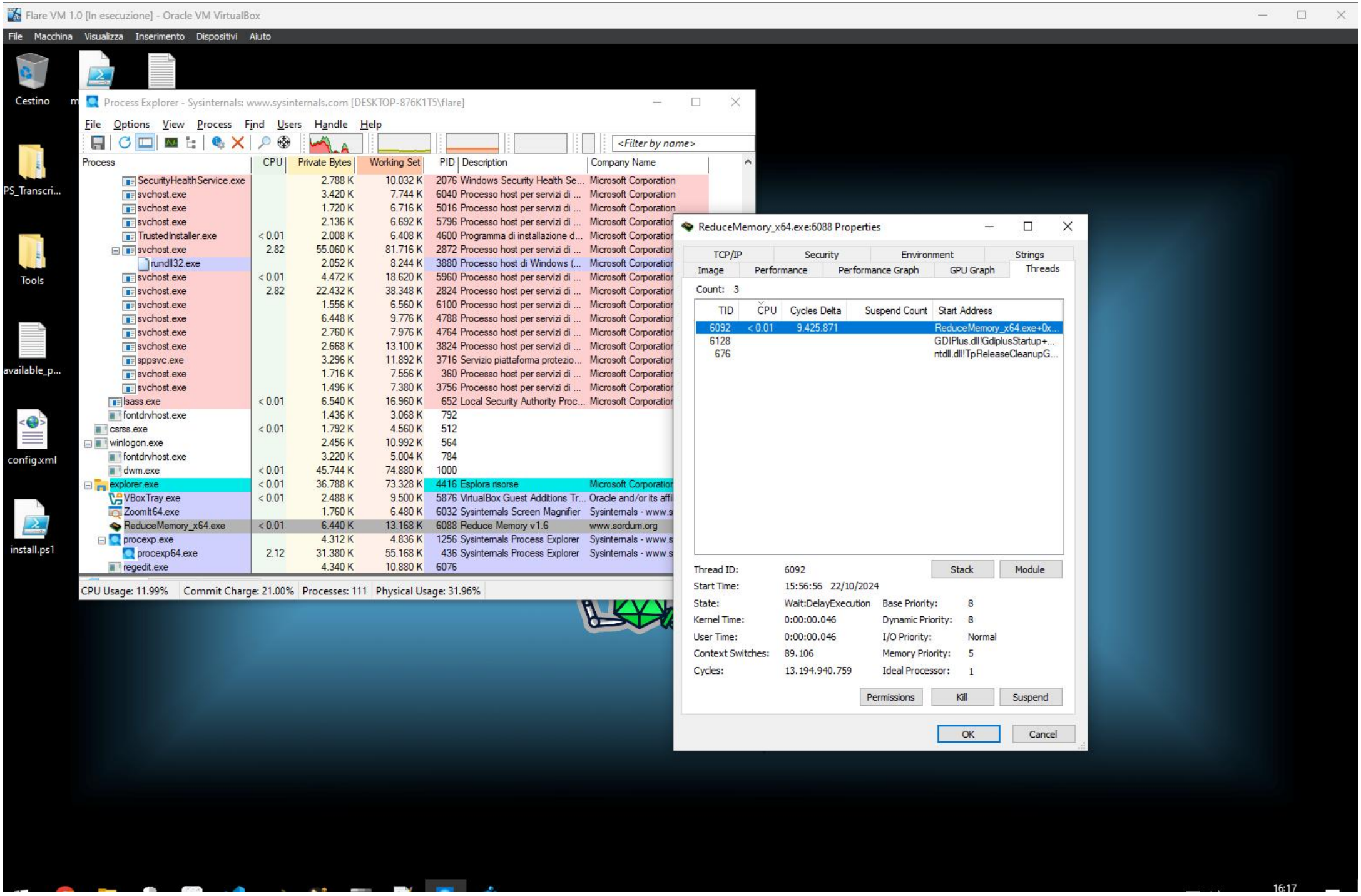
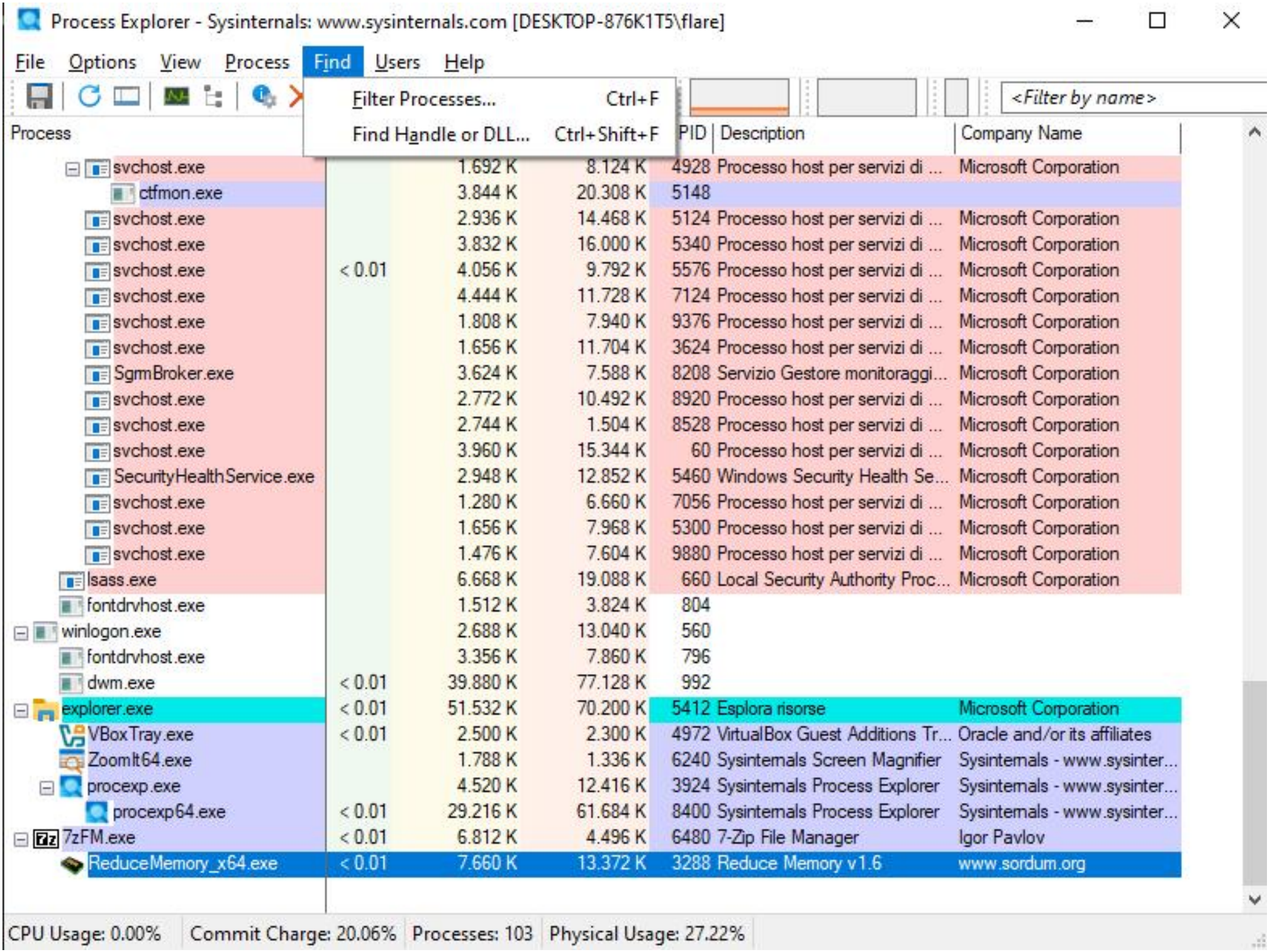
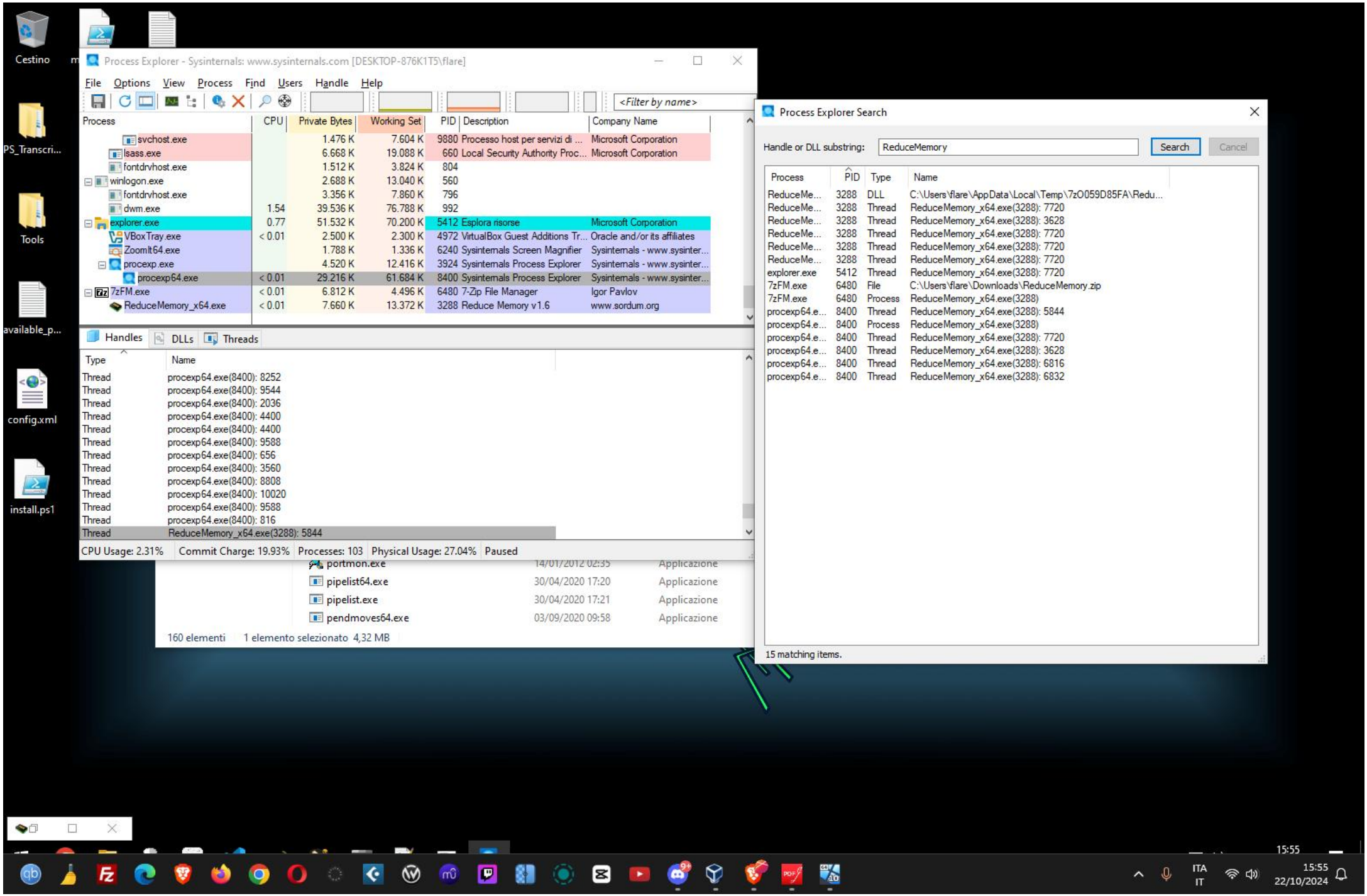
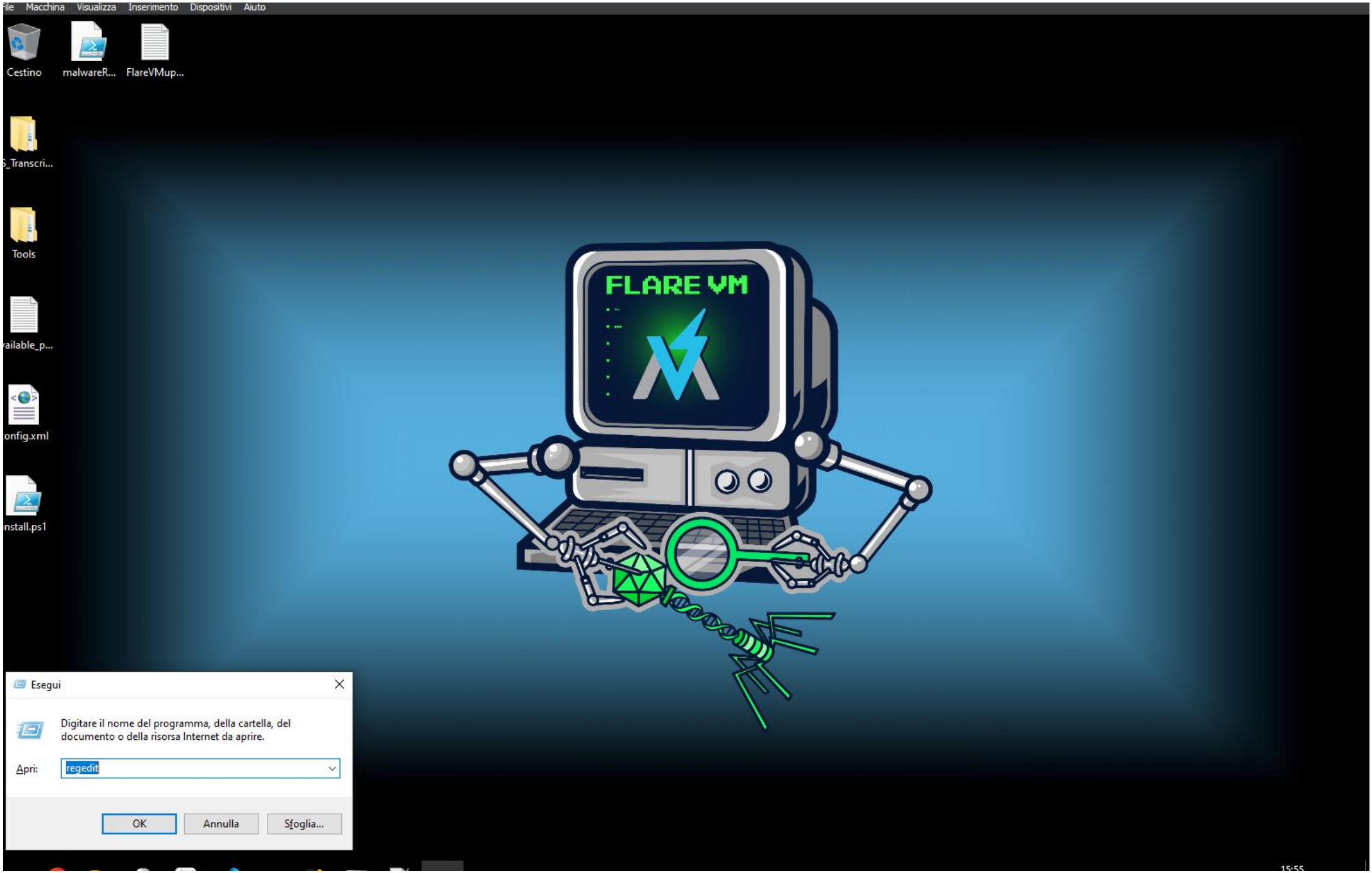
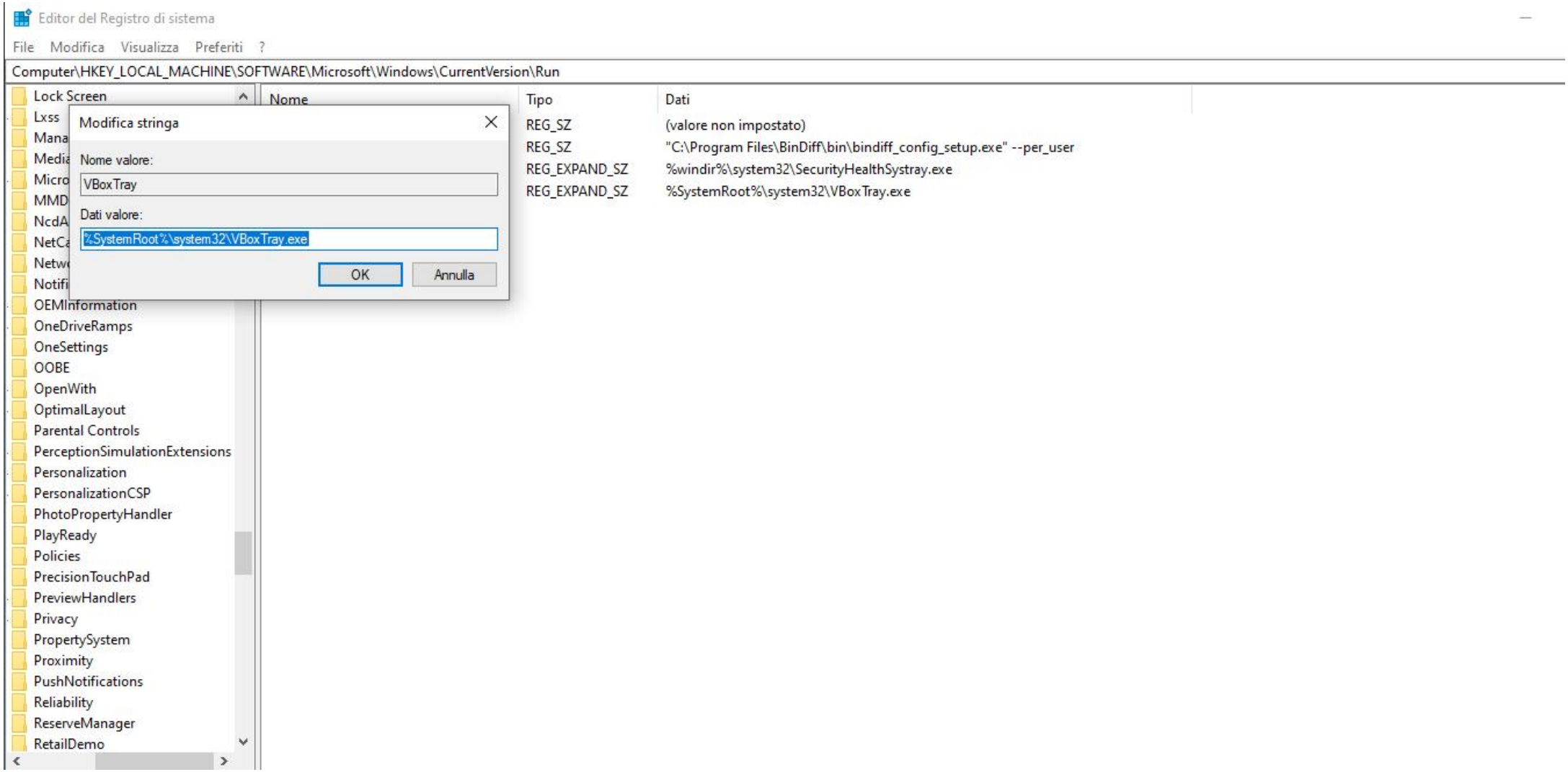
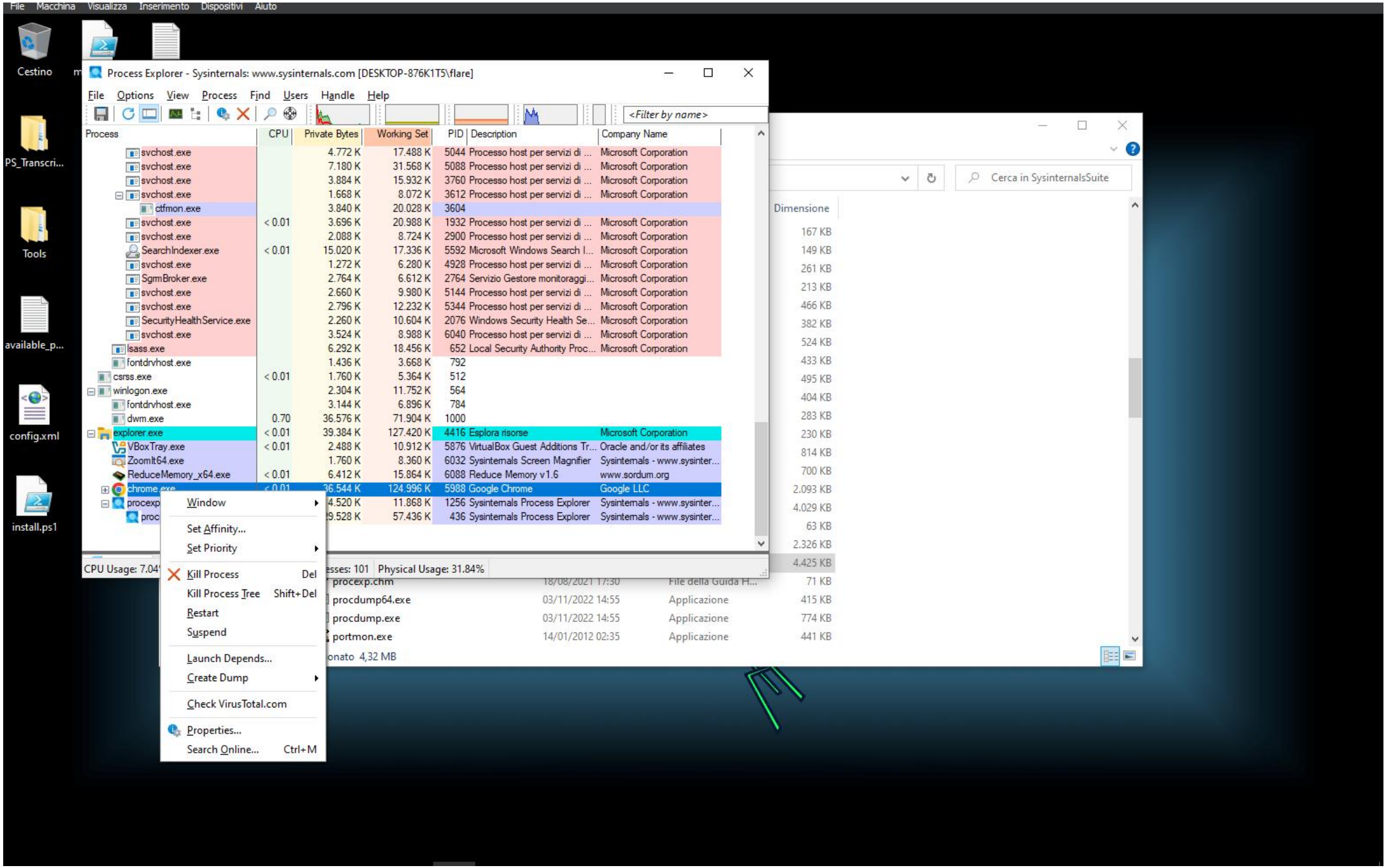

Flare VM 1.0 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
PS_Transcri...
Tools
available_p...
config.xml
install.ps1
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-876K1T5\flare]
File Options View Process Find Users Handle Help
<Filter by name>
Process CPU Private Bytes Working Set PID Description Company Name
SecurityHealthService.exe 2.788 K 10.032 K 2076 Windows Security Health Se... Microsoft Corporation
svchost.exe 3.420 K 7.744 K 6040 Processo host per servizi di ... Microsoft Corporation
svchost.exe 1.720 K 6.716 K 5016 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.136 K 6.692 K 5796 Processo host per servizi di ... Microsoft Corporation
TrustedInstaller.exe < 0.01 2.008 K 6.408 K 4600 Programma di installazione d... Microsoft Corporation
svchost.exe 2.82 55.060 K 81.716 K 2872 Processo host per servizi di ... Microsoft Corporation
rundll32.exe 2.052 K 8.244 K 3880 Processo host di Windows (... Microsoft Corporation
svchost.exe < 0.01 4.472 K 18.620 K 5960 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.82 22.432 K 38.348 K 2824 Processo host per servizi di ... Microsoft Corporation
svchost.exe 1.556 K 6.560 K 6100 Processo host per servizi di ... Microsoft Corporation
svchost.exe 6.448 K 9.776 K 4788 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.760 K 7.976 K 4764 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.668 K 13.100 K 3824 Processo host per servizi di ... Microsoft Corporation
sppsvc.exe 3.296 K 11.892 K 3716 Servizio piattaforma protezio... Microsoft Corporation
svchost.exe 1.716 K 7.556 K 360 Processo host per servizi di ... Microsoft Corporation
svchost.exe 1.496 K 7.380 K 3756 Processo host per servizi di ... Microsoft Corporation
lsass.exe < 0.01 6.540 K 16.960 K 652 Local Security Authority Proc... Microsoft Corporation
fontdrvhost.exe 1.436 K 3.068 K 792
csrss.exe < 0.01 1.792 K 4.560 K 512
winlogon.exe 2.456 K 10.992 K 564
fontdrvhost.exe 3.220 K 5.004 K 784
dwm.exe < 0.01 45.744 K 74.880 K 1000
explorer.exe < 0.01 36.788 K 73.328 K 4416 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.488 K 9.500 K 5876 VirtualBox Guest Additions Tr... Oracle and/or its affi
ZoomIt64.exe 1.760 K 6.480 K 6032 Sysinternals Screen Magnifier Sysinternals - www.s
ReduceMemory_x64.exe < 0.01 6.440 K 13.168 K 6088 Reduce Memory v1.6 www.sordum.org
procexp.exe 4.312 K 4.836 K 1256 Sysinternals Process Explorer Sysinternals - www.s
procexp64.exe 2.12 31.380 K 55.168 K 436 Sysinternals Process Explorer Sysinternals - www.s
regedit.exe 4.340 K 10.880 K 6076
CPU Usage: 11.99% Commit Charge: 21.00% Processes: 111 Physical Usage: 31.96%
ReduceMemory_x64.exe:6088 Properties
TCP/IP Security Environment Strings
Image Performance Performance Graph GPU Graph Threads
Count: 3
TID CPU Cycles Delta Suspend Count Start Address
6092 < 0.01 9.425.871 ReduceMemory_x64.exe+0x...
6128 GDIPlus.dll!GdiplusStartup+...
676 ntdll.dll!TpReleaseCleanupG...
Thread ID: 6092
Start Time: 15:56:56 22/10/2024
State: Wait:DelayExecution
Kernel Time: 0:00:00.046
User Time: 0:00:00.046
Context Switches: 89.106
Cycles: 13.194.940.759
Base Priority: 8
Dynamic Priority: 8
I/O Priority: Normal
Memory Priority: 5
Ideal Processor: 1
Stack
Module
Permissions
Kill
Suspend
OK
Cancel
16:17

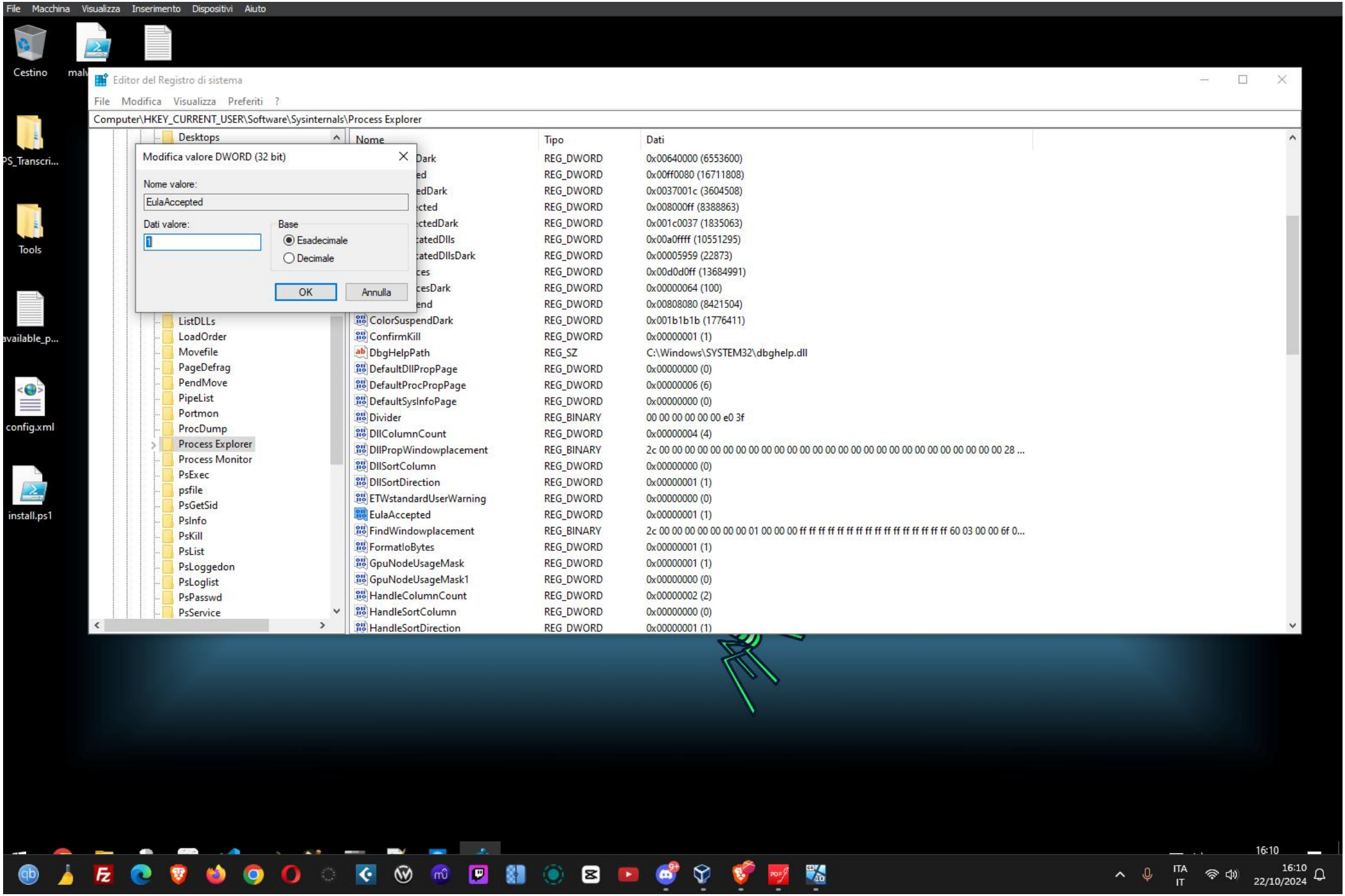

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-876K1T5\flare]
File Options View Process Find Users Help
Filter Processes... Ctrl+F
Find Handle or DLL... Ctrl+Shift+F
<Filter by name>
Process PID Description Company Name
svchost.exe 1.692 K 8.124 K 4928 Processo host per servizi di ... Microsoft Corporation
ctfmon.exe 3.844 K 20.308 K 5148
svchost.exe 2.936 K 14.468 K 5124 Processo host per servizi di ... Microsoft Corporation
svchost.exe 3.832 K 16.000 K 5340 Processo host per servizi di ... Microsoft Corporation
svchost.exe < 0.01 4.056 K 9.792 K 5576 Processo host per servizi di ... Microsoft Corporation
svchost.exe 4.444 K 11.728 K 7124 Processo host per servizi di ... Microsoft Corporation
svchost.exe 1.808 K 7.940 K 9376 Processo host per servizi di ... Microsoft Corporation
svchost.exe 1.656 K 11.704 K 3624 Processo host per servizi di ... Microsoft Corporation
SgrmBroker.exe 3.624 K 7.588 K 8208 Servizio Gestore monitoraggi... Microsoft Corporation
svchost.exe 2.772 K 10.492 K 8920 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.744 K 1.504 K 8528 Processo host per servizi di ... Microsoft Corporation
svchost.exe 3.960 K 15.344 K 60 Processo host per servizi di ... Microsoft Corporation
SecurityHealthService.exe 2.948 K 12.852 K 5460 Windows Security Health Se... Microsoft Corporation
svchost.exe 1.280 K 6.660 K 7056 Processo host per servizi di ... Microsoft Corporation
svchost.exe 1.656 K 7.968 K 5300 Processo host per servizi di ... Microsoft Corporation
svchost.exe 1.476 K 7.604 K 9880 Processo host per servizi di ... Microsoft Corporation
lsass.exe 6.668 K 19.088 K 660 Local Security Authority Proc... Microsoft Corporation
fontdrvhost.exe 1.512 K 3.824 K 804
winlogon.exe 2.688 K 13.040 K 560
fontdrvhost.exe 3.356 K 7.860 K 796
dwm.exe < 0.01 39.880 K 77.128 K 992
explorer.exe < 0.01 51.532 K 70.200 K 5412 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.500 K 2.300 K 4972 VirtualBox Guest Additions Tr... Oracle and/or its affiliates
ZoomIt64.exe 1.788 K 1.336 K 6240 Sysinternals Screen Magnifier Sysinternals - www.sysinter...
procexp.exe 4.520 K 12.416 K 3924 Sysinternals Process Explorer Sysinternals - www.sysinter...
procexp64.exe < 0.01 29.216 K 61.684 K 8400 Sysinternals Process Explorer Sysinternals - www.sysinter...
7zFM.exe < 0.01 6.812 K 4.496 K 6480 7-Zip File Manager Igor Pavlov
ReduceMemory_x64.exe < 0.01 7.660 K 13.372 K 3288 Reduce Memory v1.6 www.sordum.org
CPU Usage: 0.00% Commit Charge: 20.06% Processes: 103 Physical Usage: 27.22%

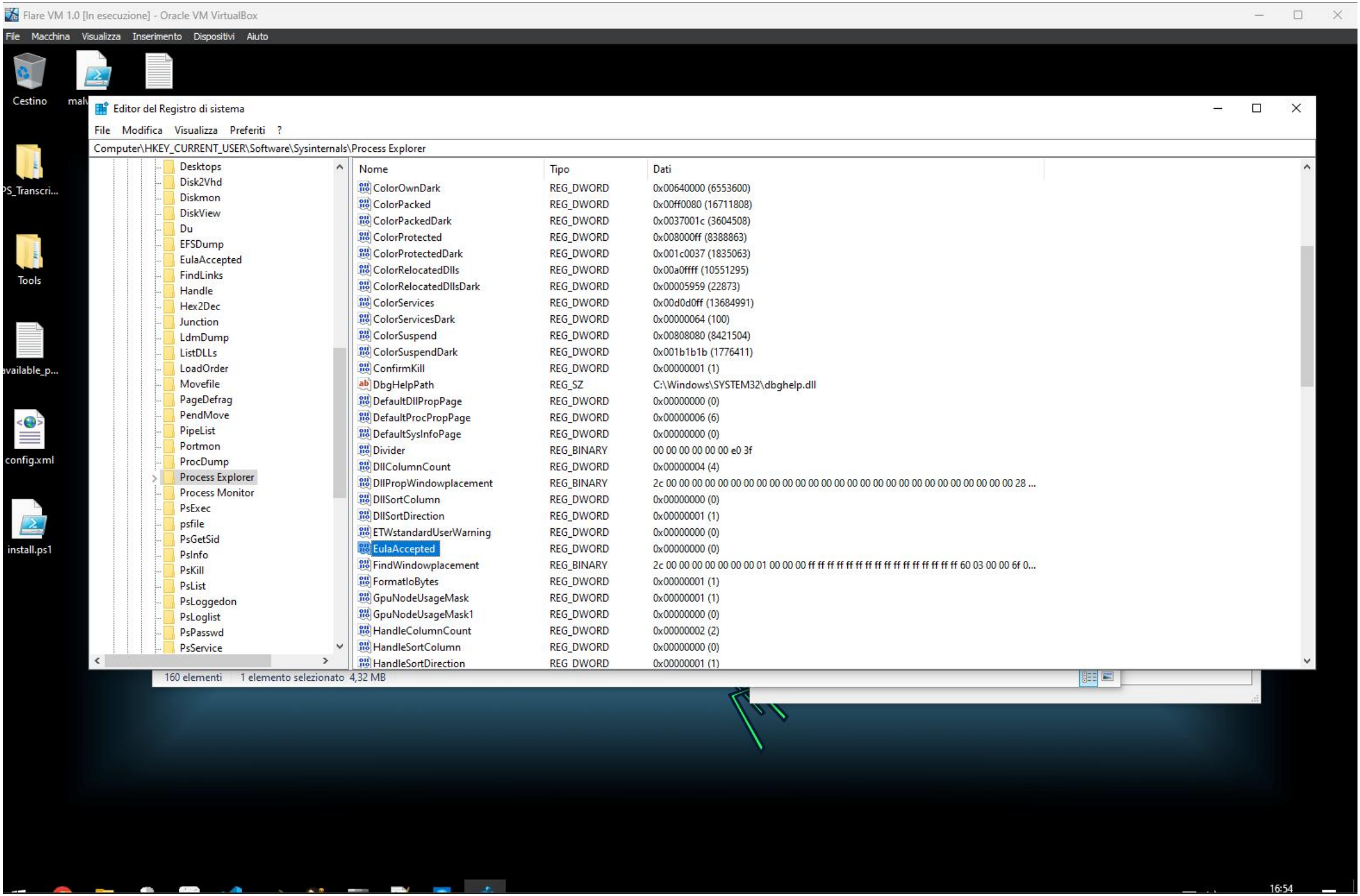

Cestino
PS_Transcri...
Tools
available_p...
config.xml
install.ps1
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-876K1T5\flare]
File Options View Process Find Users Handle Help
<Filter by name>
Process CPU Private Bytes Working Set PID Description Company Name
svchost.exe 1.476 K 7.604 K 9880 Processo host per servizi di ... Microsoft Corporation
lsass.exe 6.668 K 19.088 K 660 Local Security Authority Proc... Microsoft Corporation
fontdrvhost.exe 1.512 K 3.824 K 804
winlogon.exe 2.688 K 13.040 K 560
fontdrvhost.exe 3.356 K 7.860 K 796
dwm.exe 1.54 39.536 K 76.788 K 992
explorer.exe 0.77 51.532 K 70.200 K 5412 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.500 K 2.300 K 4972 VirtualBox Guest Additions Tr... Oracle and/or its affiliates
ZoomIt64.exe 1.788 K 1.336 K 6240 Sysinternals Screen Magnifier Sysinternals - www.sysinter...
procexp.exe 4.520 K 12.416 K 3924 Sysinternals Process Explorer Sysinternals - www.sysinter...
procexp64.exe < 0.01 29.216 K 61.684 K 8400 Sysinternals Process Explorer Sysinternals - www.sysinter...
7zFM.exe < 0.01 6.812 K 4.496 K 6480 7-Zip File Manager Igor Pavlov
ReduceMemory_x64.exe < 0.01 7.660 K 13.372 K 3288 Reduce Memory v1.6 www.sordum.org
Handles DLLs Threads
Type Name
Thread procexp64.exe(8400): 8252
Thread procexp64.exe(8400): 9544
Thread procexp64.exe(8400): 2036
Thread procexp64.exe(8400): 4400
Thread procexp64.exe(8400): 4400
Thread procexp64.exe(8400): 9588
Thread procexp64.exe(8400): 656
Thread procexp64.exe(8400): 3560
Thread procexp64.exe(8400): 8808
Thread procexp64.exe(8400): 10020
Thread procexp64.exe(8400): 9588
Thread procexp64.exe(8400): 816
Thread ReduceMemory_x64.exe(3288): 5844
CPU Usage: 2.31% Commit Charge: 19.93% Processes: 103 Physical Usage: 27.04% Paused
portmon.exe 14/01/2012 02:35 Applicazione
pipelist64.exe 30/04/2020 17:20 Applicazione
pipelist.exe 30/04/2020 17:21 Applicazione
pendmoves64.exe 03/09/2020 09:58 Applicazione
160 elementi 1 elemento selezionato 4,32 MB
Process Explorer Search
Handle or DLL substring: ReduceMemory
Search
Cancel
Process PID Type Name
ReduceMe... 3288 DLL C:\Users\flare\AppData\Local\Temp\7zO059D85FA\Redu...
ReduceMe... 3288 Thread ReduceMemory_x64.exe(3288): 7720
ReduceMe... 3288 Thread ReduceMemory_x64.exe(3288): 3628
ReduceMe... 3288 Thread ReduceMemory_x64.exe(3288): 7720
ReduceMe... 3288 Thread ReduceMemory_x64.exe(3288): 7720
ReduceMe... 3288 Thread ReduceMemory_x64.exe(3288): 7720
explorer.exe 5412 Thread ReduceMemory_x64.exe(3288): 7720
7zFM.exe 6480 File C:\Users\flare\Downloads\ReduceMemory.zip
7zFM.exe 6480 Process ReduceMemory_x64.exe(3288)
procexp64.e... 8400 Thread ReduceMemory_x64.exe(3288): 5844
procexp64.e... 8400 Process ReduceMemory_x64.exe(3288)
procexp64.e... 8400 Thread ReduceMemory_x64.exe(3288): 7720
procexp64.e... 8400 Thread ReduceMemory_x64.exe(3288): 3628
procexp64.e... 8400 Thread ReduceMemory_x64.exe(3288): 6816
procexp64.e... 8400 Thread ReduceMemory_x64.exe(3288): 6832
15 matching items.
ITA IT
15:55 22/10/2024


File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
malwareR...
FlareVMup...
_Transcri...
Tools
ailable_p...
onfig.xml
nstall.ps1
FLARE VM
Esegui
Digitare il nome del programma, della cartella, del documento o della risorsa Internet da aprire.
Apri:
regedit
OK
Annulla
Sfoglia...
15:55


Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Lock Screen
Lxss
Mana
Media
Micro
MMD
NcdA
NetCa
Netwo
Notifi
OEMInformation
OneDriveRamps
OneSettings
OOBE
OpenWith
OptimalLayout
Parental Controls
PerceptionSimulationExtensions
Personalization
PersonalizationCSP
PhotoPropertyHandler
PlayReady
Policies
PrecisionTouchPad
PreviewHandlers
Privacy
PropertySystem
Proximity
PushNotifications
Reliability
ReserveManager
RetailDemo
Modifica stringa
Nome valore:
VBoxTray
Dati valore:
%SystemRoot%\system32\VBoxTray.exe
OK
Annulla
Nome
Tipo
Dati
REG_SZ
(valore non impostato)
REG_SZ
"C:\Program Files\BinDiff\bin\bindiff_config_setup.exe" --per_user
REG_EXPAND_SZ
%windir%\system32\SecurityHealthSystray.exe
REG_EXPAND_SZ
%SystemRoot%\system32\VBoxTray.exe


File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
PS_Transcri...
Tools
available_p...
config.xml
install.ps1
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-876K1T5\flare]
File Options View Process Find Users Handle Help
<Filter by name>
Process CPU Private Bytes Working Set PID Description Company Name
svchost.exe 4.772 K 17.488 K 5044 Processo host per servizi di ... Microsoft Corporation
svchost.exe 7.180 K 31.568 K 5088 Processo host per servizi di ... Microsoft Corporation
svchost.exe 3.884 K 15.932 K 3760 Processo host per servizi di ... Microsoft Corporation
svchost.exe 1.668 K 8.072 K 3612 Processo host per servizi di ... Microsoft Corporation
ctfmon.exe 3.840 K 20.028 K 3604
svchost.exe < 0.01 3.696 K 20.988 K 1932 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.088 K 8.724 K 2900 Processo host per servizi di ... Microsoft Corporation
SearchIndexer.exe < 0.01 15.020 K 17.336 K 5592 Microsoft Windows Search I... Microsoft Corporation
svchost.exe 1.272 K 6.280 K 4928 Processo host per servizi di ... Microsoft Corporation
SgrmBroker.exe 2.764 K 6.612 K 2764 Servizio Gestore monitoraggi... Microsoft Corporation
svchost.exe 2.660 K 9.980 K 5144 Processo host per servizi di ... Microsoft Corporation
svchost.exe 2.796 K 12.232 K 5344 Processo host per servizi di ... Microsoft Corporation
SecurityHealthService.exe 2.260 K 10.604 K 2076 Windows Security Health Se... Microsoft Corporation
svchost.exe 3.524 K 8.988 K 6040 Processo host per servizi di ... Microsoft Corporation
lsass.exe 6.292 K 18.456 K 652 Local Security Authority Proc... Microsoft Corporation
fontdrvhost.exe 1.436 K 3.668 K 792
csrss.exe < 0.01 1.760 K 5.364 K 512
winlogon.exe 2.304 K 11.752 K 564
fontdrvhost.exe 3.144 K 6.896 K 784
dwm.exe 0.70 36.576 K 71.904 K 1000
explorer.exe < 0.01 39.384 K 127.420 K 4416 Esplora risorse Microsoft Corporation
VBoxTray.exe < 0.01 2.488 K 10.912 K 5876 VirtualBox Guest Additions Tr... Oracle and/or its affiliates
ZoomIt64.exe 1.760 K 8.360 K 6032 Sysinternals Screen Magnifier Sysinternals - www.sysinter...
ReduceMemory_x64.exe < 0.01 6.412 K 15.864 K 6088 Reduce Memory v1.6 www.sordum.org
chrome.exe < 0.01 36.544 K 124.996 K 5988 Google Chrome Google LLC
procexp 4.520 K 11.868 K 1256 Sysinternals Process Explorer Sysinternals - www.sysinter...
proc 9.528 K 57.436 K 436 Sysinternals Process Explorer Sysinternals - www.sysinter...
CPU Usage: 7.04
esses: 101 Physical Usage: 31.84%
Window
Set Affinity...
Set Priority
Kill Process Del
Kill Process Tree Shift+Del
Restart
Suspend
Launch Depends...
Create Dump
Check VirusTotal.com
Properties...
Search Online... Ctrl+M
Cerca in SysinternalsSuite
Dimensione
167 KB
149 KB
261 KB
213 KB
466 KB
382 KB
524 KB
433 KB
495 KB
404 KB
283 KB
230 KB
814 KB
700 KB
2.093 KB
4.029 KB
63 KB
2.326 KB
4.425 KB
procexp.chm 18/08/2021 17:30 File della Guida H... 71 KB
procdump64.exe 03/11/2022 14:55 Applicazione 415 KB
procdump.exe 03/11/2022 14:55 Applicazione 774 KB
portmon.exe 14/01/2012 02:35 Applicazione 441 KB
onato 4,32 MB


File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
Computer\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer
Modifica valore DWORD (32 bit)
Nome valore:
EulaAccepted
Dati valore:
1
Base
Esadecimale
Decimale
OK
Annulla
Desktops
ListDLLs
LoadOrder
Movefile
PageDefrag
PendMove
PipeList
Portmon
ProcDump
Process Explorer
Process Monitor
PsExec
psfile
PsGetSid
PsInfo
PsKill
PsList
PsLoggedon
PsLoglist
PsPasswd
PsService
Nome
Tipo
Dati
ColorSuspendDark REG_DWORD 0x001b1b1b (1776411)
ConfirmKill REG_DWORD 0x00000001 (1)
DbgHelpPath REG_SZ C:\Windows\SYSTEM32\dbghelp.dll
DefaultDllPropPage REG_DWORD 0x00000000 (0)
DefaultProcPropPage REG_DWORD 0x00000006 (6)
DefaultSysInfoPage REG_DWORD 0x00000000 (0)
Divider REG_BINARY 00 00 00 00 00 00 e0 3f
DllColumnCount REG_DWORD 0x00000004 (4)
DllPropWindowplacement REG_BINARY 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 ...
DllSortColumn REG_DWORD 0x00000000 (0)
DllSortDirection REG_DWORD 0x00000001 (1)
ETWstandardUserWarning REG_DWORD 0x00000000 (0)
EulaAccepted REG_DWORD 0x00000001 (1)
FindWindowplacement REG_BINARY 2c 00 00 00 00 00 00 00 01 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 60 03 00 00 6f 0...
FormatIoBytes REG_DWORD 0x00000001 (1)
GpuNodeUsageMask REG_DWORD 0x00000001 (1)
GpuNodeUsageMask1 REG_DWORD 0x00000000 (0)
HandleColumnCount REG_DWORD 0x00000002 (2)
HandleSortColumn REG_DWORD 0x00000000 (0)
HandleSortDirection REG_DWORD 0x00000001 (1)
ITA IT
16:10 22/10/2024


Flare VM 1.0 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
malv
PS_Transcri...
Tools
available_p...
config.xml
install.ps1
Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
Computer\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer
Desktops
Disk2Vhd
Diskmon
DiskView
Du
EFSDump
EulaAccepted
FindLinks
Handle
Hex2Dec
Junction
LdmDump
ListDLLs
LoadOrder
Movefile
PageDefrag
PendMove
PipeList
Portmon
ProcDump
Process Explorer
Process Monitor
PsExec
psfile
PsGetSid
PsInfo
PsKill
PsList
PsLoggedon
PsLoglist
PsPasswd
PsService
Nome Tipo Dati
ColorOwnDark REG_DWORD 0x00640000 (6553600)
ColorPacked REG_DWORD 0x00ff0080 (16711808)
ColorPackedDark REG_DWORD 0x0037001c (3604508)
ColorProtected REG_DWORD 0x008000ff (8388863)
ColorProtectedDark REG_DWORD 0x001c0037 (1835063)
ColorRelocatedDlls REG_DWORD 0x00a0ffff (10551295)
ColorRelocatedDllsDark REG_DWORD 0x00005959 (22873)
ColorServices REG_DWORD 0x00d0d0ff (13684991)
ColorServicesDark REG_DWORD 0x00000064 (100)
ColorSuspend REG_DWORD 0x00808080 (8421504)
ColorSuspendDark REG_DWORD 0x001b1b1b (1776411)
ConfirmKill REG_DWORD 0x00000001 (1)
DbgHelpPath REG_SZ C:\Windows\SYSTEM32\dbghelp.dll
DefaultDllPropPage REG_DWORD 0x00000000 (0)
DefaultProcPropPage REG_DWORD 0x00000006 (6)
DefaultSysInfoPage REG_DWORD 0x00000000 (0)
Divider REG_BINARY 00 00 00 00 00 00 e0 3f
DllColumnCount REG_DWORD 0x00000004 (4)
DllPropWindowplacement REG_BINARY 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 ...
DllSortColumn REG_DWORD 0x00000000 (0)
DllSortDirection REG_DWORD 0x00000001 (1)
ETWstandardUserWarning REG_DWORD 0x00000000 (0)
EulaAccepted REG_DWORD 0x00000000 (0)
FindWindowplacement REG_BINARY 2c 00 00 00 00 00 00 00 01 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 60 03 00 00 6f 0...
FormatIoBytes REG_DWORD 0x00000001 (1)
GpuNodeUsageMask REG_DWORD 0x00000001 (1)
GpuNodeUsageMask1 REG_DWORD 0x00000000 (0)
HandleColumnCount REG_DWORD 0x00000002 (2)
HandleSortColumn REG_DWORD 0x00000000 (0)
HandleSortDirection REG_DWORD 0x00000001 (1)
160 elementi 1 elemento selezionato 4,32 MB
16:54