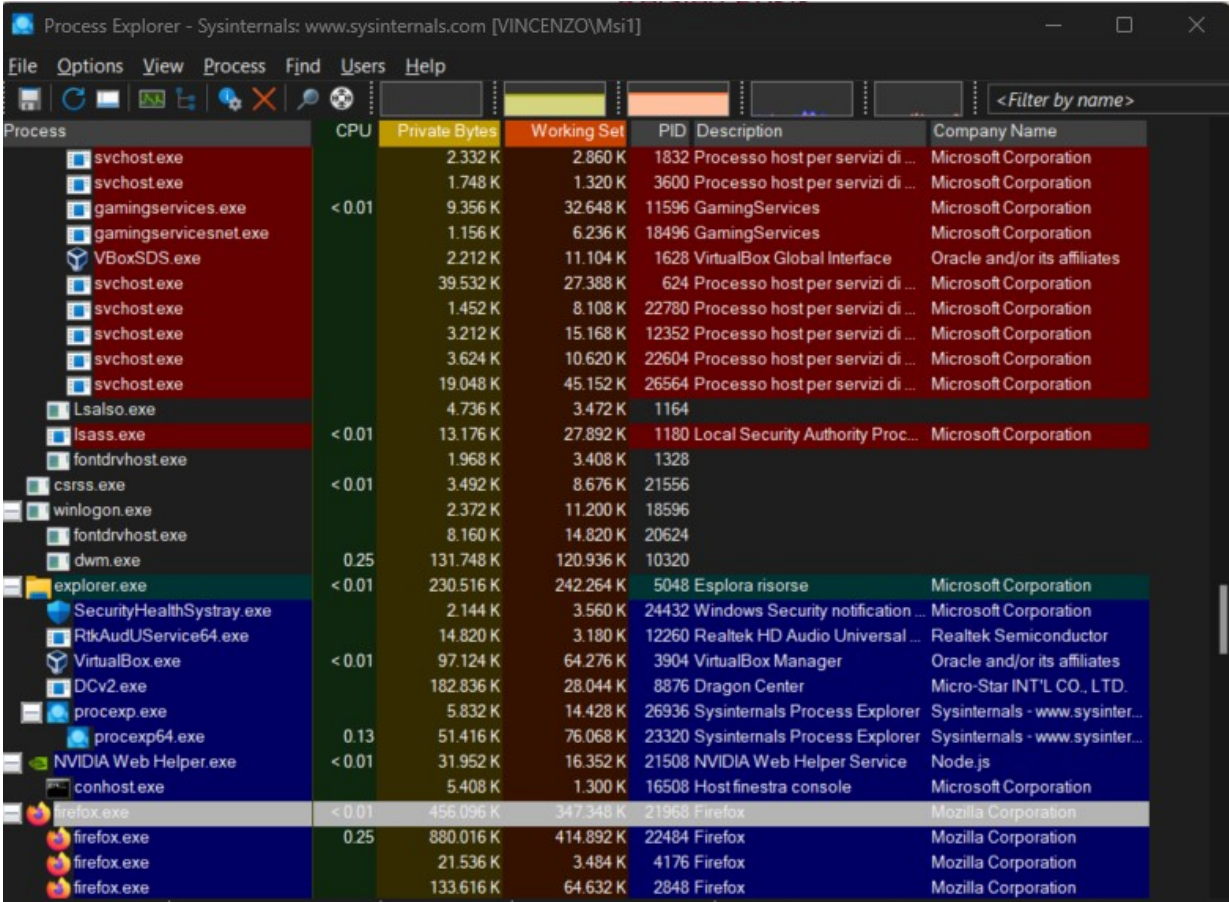


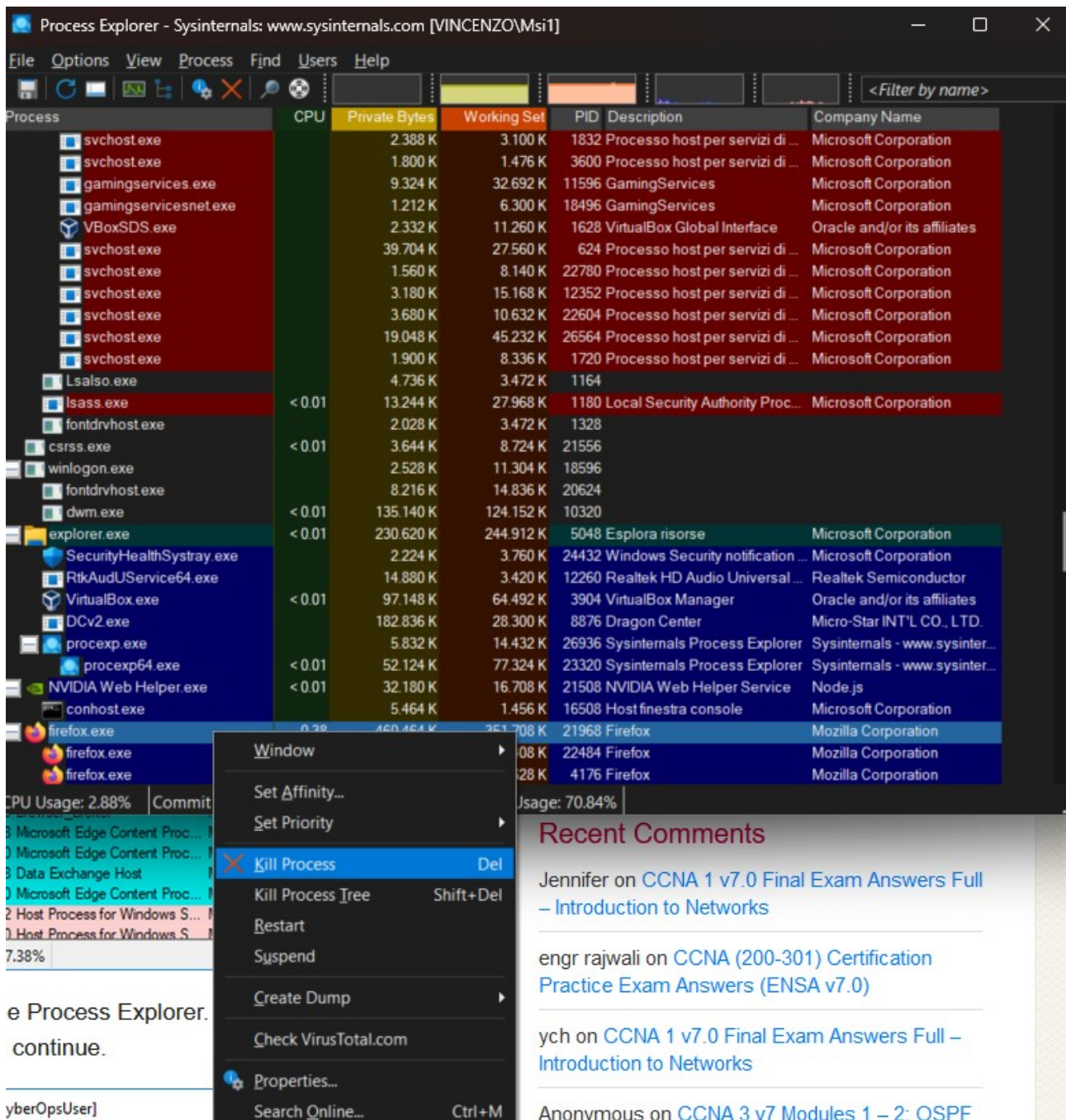
## Exploring Processes

1. Mi sposto nella cartella SysinternalsSuite dove ho estratto tutti i file
2. Faccio doppio click su procexp.exe e accetto l'accordo di licenza quando appare
3. Process Explorer mi mostra ora un elenco di tutti i processi attivi sul sistema
4. Per trovare il processo del browser, prendo l'icona "Find Window's Process" (quella con il mirino) e la trascino sulla finestra del mio browser aperto.



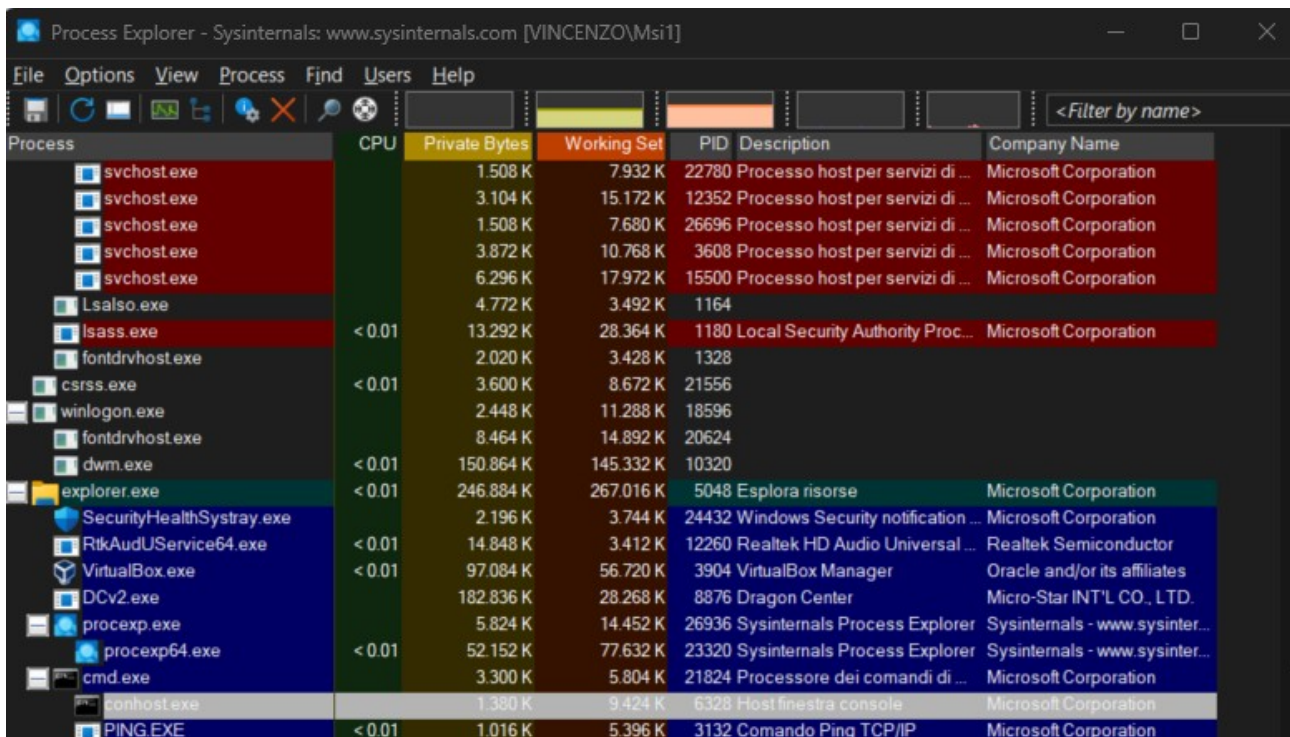
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		2.332 K	2.860 K	1832	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		1.748 K	1.320 K	3600	Processo host per servizi di ...	Microsoft Corporation
gamingservices.exe	< 0.01	9.356 K	32.648 K	11596	GamingServices	Microsoft Corporation
gamingservicesnet.exe		1.156 K	6.236 K	18496	GamingServices	Microsoft Corporation
VBoxSDS.exe		2.212 K	11.104 K	1628	VirtualBox Global Interface	Oracle and/or its affiliates
svchost.exe		39.532 K	27.388 K	624	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		1.452 K	8.108 K	22780	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		3.212 K	15.168 K	12352	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		3.624 K	10.620 K	22604	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		19.048 K	45.152 K	26564	Processo host per servizi di ...	Microsoft Corporation
Lsalso.exe		4.736 K	3.472 K	1164		
lsass.exe	< 0.01	13.176 K	27.892 K	1180	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1.968 K	3.408 K	1328		
csrss.exe	< 0.01	3.492 K	8.676 K	21556		
winlogon.exe		2.372 K	11.200 K	18596		
fontdrvhost.exe		8.160 K	14.820 K	20624		
dwm.exe	0.25	131.748 K	120.936 K	10320		
explorer.exe	< 0.01	230.516 K	242.264 K	5048	Esplora risorse	Microsoft Corporation
SecurityHealthSystray.exe		2.144 K	3.560 K	24432	Windows Security notification ...	Microsoft Corporation
RtkAudUService64.exe		14.820 K	3.180 K	12260	Realtek HD Audio Universal ...	Realtek Semiconductor
VirtualBox.exe	< 0.01	97.124 K	64.276 K	3904	VirtualBox Manager	Oracle and/or its affiliates
DCv2.exe		182.836 K	28.044 K	8876	Dragon Center	Micro-Star INT'L CO., LTD.
procexp.exe		5.832 K	14.428 K	26936	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.13	51.416 K	76.068 K	23320	Sysinternals Process Explorer	Sysinternals - www.sysinter...
NVIDIA Web Helper.exe	< 0.01	31.952 K	16.352 K	21508	NVIDIA Web Helper Service	Node.js
conhost.exe		5.408 K	1.300 K	16508	Host finestra console	Microsoft Corporation
firefox.exe	< 0.01	456.096 K	347.348 K	21968	Firefox	Mozilla Corporation
firefox.exe	0.25	880.016 K	414.892 K	22484	Firefox	Mozilla Corporation
firefox.exe		21.536 K	3.484 K	4176	Firefox	Mozilla Corporation
firefox.exe		133.616 K	64.632 K	2848	Firefox	Mozilla Corporation

5. Una volta identificato il processo di Mozilla Firefox in Process Explorer, faccio click destro su di esso
6. Dal menu che appare seleziono "Kill Process"
7. Mi appare una finestra di conferma, clicco "OK" per procedere con la terminazione del processo



Tutte le schede aperte di firefox si sono chiuse.

1. Apro il Prompt dei Comandi: vado su Start, cerco "Prompt dei Comandi" e lo seleziono
2. Trascino l'icona "Find Window's Process" di Process Explorer sulla finestra del Prompt dei Comandi
3. In Process Explorer vedo ora evidenziato il processo cmd.exe. Noto che:
  - Il suo processo padre è explorer.exe
  - Ha un processo figlio chiamato conhost.exe
4. Torno alla finestra del Prompt dei Comandi e digito il comando ping (per esempio "ping google.com") e osservo i cambiamenti che avvengono sotto il processo cmd.exe in Process Explorer



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		1.508 K	7.932 K	22780	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		3.104 K	15.172 K	12352	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		1.508 K	7.680 K	26696	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		3.872 K	10.768 K	3608	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		6.296 K	17.972 K	15500	Processo host per servizi di ...	Microsoft Corporation
lsass.exe	< 0.01	13.292 K	28.364 K	1180	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		2.020 K	3.428 K	1328		
csrss.exe	< 0.01	3.600 K	8.672 K	21556		
winlogon.exe		2.448 K	11.288 K	18596		
fontdrvhost.exe		8.464 K	14.892 K	20624		
dwm.exe	< 0.01	150.864 K	145.332 K	10320		
explorer.exe	< 0.01	246.884 K	267.016 K	5048	Esplora risorse	Microsoft Corporation
SecurityHealthSystray.exe		2.196 K	3.744 K	24432	Windows Security notification ...	Microsoft Corporation
RtkAudUService64.exe	< 0.01	14.848 K	3.412 K	12260	Realtek HD Audio Universal ...	Realtek Semiconductor
VirtualBox.exe	< 0.01	97.084 K	56.720 K	3904	VirtualBox Manager	Oracle and/or its affiliates
DCv2.exe		182.836 K	28.268 K	8876	Dragon Center	Micro-Star INT'L CO., LTD.
procexp.exe		5.824 K	14.452 K	26936	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	< 0.01	52.152 K	77.632 K	23320	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		3.300 K	5.804 K	21824	Processore dei comandi di ...	Microsoft Corporation
conhost.exe		1.380 K	9.424 K	6328	Host finestra console	Microsoft Corporation
PING.EXE	< 0.01	1.016 K	5.396 K	3132	Comando Ping TCP/IP	Microsoft Corporation



1. Analizzo la lista dei processi attivi e noto conhost.exe che potrebbe essere sospetto.

Per verificare:

- Faccio click destro su conhost.exe
- Seleziono "Check VirusTotal"
- Quando richiesto, clicco "Yes" per accettare i Termini di Servizio di VirusTotal
- Clicco "OK" nel prompt successivo

2. Infine:

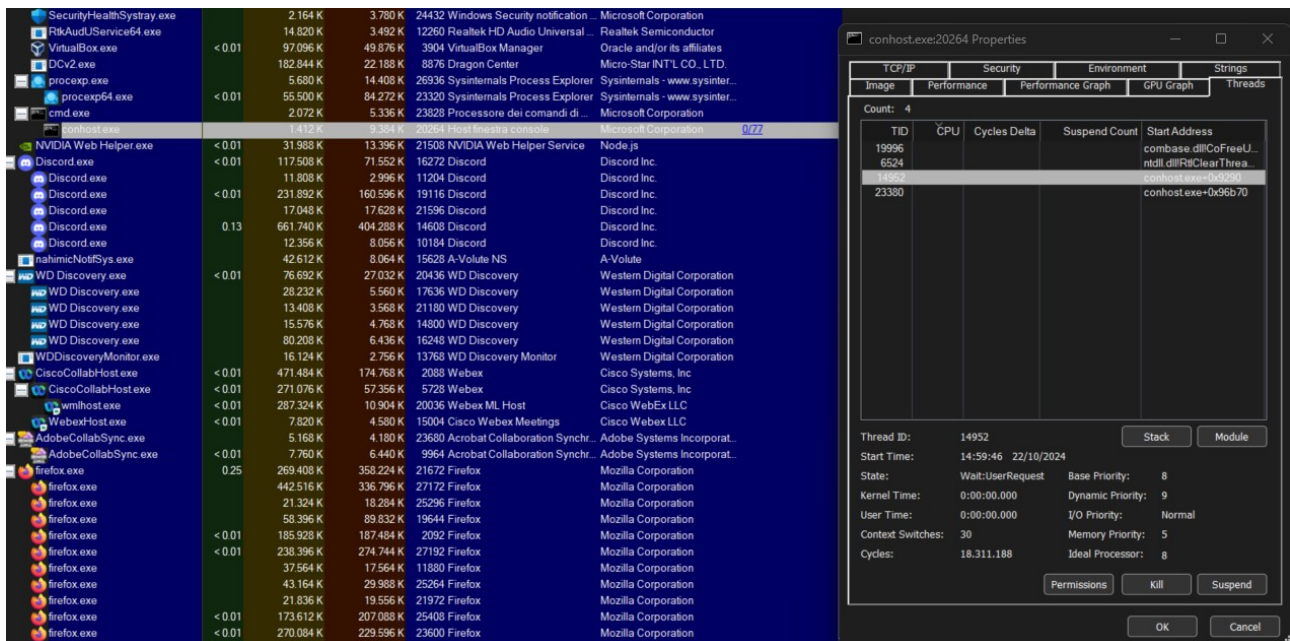
- Faccio click destro sul processo cmd.exe
- Seleziono "Kill Process" per terminarlo

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
svchost.exe		3.848 K	10.812 K	3608	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		3.416 K	14.876 K	20284	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		1.728 K	8.292 K	20144	Processo host per servizi di ...	Microsoft Corporation	
lsass.exe		4.816 K	3.684 K	1164			
lsass.exe	< 0.01	13.260 K	28.932 K	1180	Local Security Authority Proc...	Microsoft Corporation	
fontdrvhost.exe		1.992 K	3.412 K	1328			
csrss.exe	< 0.01	3.492 K	8.600 K	21556			
winlogon.exe		2.372 K	11.272 K	18596			
fontdrvhost.exe		8.436 K	14.876 K	20624			
dwm.exe	< 0.01	150.368 K	145.056 K	10320			
explorer.exe	< 0.01	251.432 K	275.416 K	5048	Esplora risorse	Microsoft Corporation	
SecurityHealthSystray.exe		2.228 K	3.808 K	24432	Windows Security notification ...	Microsoft Corporation	
RtkAudUService64.exe		14.820 K	3.396 K	12260	Realtek HD Audio Universal ...	Realtek Semiconductor	
VirtualBox.exe	< 0.01	97.088 K	56.724 K	3904	VirtualBox Manager	Oracle and/or its affiliates	
DCv2.exe		182.836 K	28.288 K	8876	Dragon Center	Micro-Star INT'L CO., LTD.	
procxp.exe		5.680 K	14.408 K	26936	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procxp64.exe	< 0.01	52.568 K	80.560 K	23320	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		3.152 K	5.708 K	21824	Processore dei comandi di ...	Microsoft Corporation	
conhost.exe		1.404 K	9.436 K	6328	Host finestra console	Microsoft Corporation	0/77

cmd.exe		2.120 K	5.692 K	21824	Processore dei comandi di ...	Microsoft Corporation	
conhost.exe		1.404 K	9.404 K	6328	Host finestra console	Microsoft Corporation	0/77
conhost.exe		1.404 K	9.404 K	5632			
conhost.exe		1.404 K	15.100 K	21508	NVIDIA Web Helper Service	Node.js	
conhost.exe		1.404 K	1.240 K	16508	Host finestra console	Microsoft Corporation	0/77
conhost.exe		1.404 K	70.300 K	16272	Discord	Discord Inc.	
conhost.exe		1.404 K	2.996 K	11204	Discord	Discord Inc.	
conhost.exe		1.404 K	155.552 K	19116	Discord	Discord Inc.	

## Exploring Threads and Handles

1. Apro un nuovo Prompt dei Comandi
2. In Process Explorer:
  - Faccio click destro su conhost.exe
  - Seleziono "Properties"
  - Vado nella scheda "Threads" per vedere i thread attivi del processo conhost.exe
  - Appare un avviso, clicco "OK" per continuare



1. In Process Explorer:
  - Vado nel menu "View"
  - Seleziono "Lower Pane View"
  - Clicco su "Handles"
2. Ora posso vedere nel pannello inferiore tutti gli handle (i riferimenti alle risorse) associati al processo conhost.exe, che possono includere:
  - File aperti
  - Chiavi di registro
  - Eventi di sistema
  - Altri oggetti di sistema a cui il processo ha accesso

The screenshot displays the Windows Task Manager interface, specifically the 'Processes' tab. The window title is 'Process Explorer - Sysinternals - www.sysinternals.com [VINCENZO\Msi1]'. The menu bar includes 'File', 'Options', 'View', 'Process', 'Find', 'Users', 'Handle', and 'Help'. The toolbar contains icons for various actions like refreshing, pausing, and searching.

The main table lists running processes with columns: Process, CPU, Private Bytes, Working Set, PID, Description, Company Name, and Virus Total. The processes are sorted by CPU usage. Key processes include svchost.exe, lsass.exe, explorer.exe, SecurityHealthSystray.exe, RtkAudUService64.exe, VirtualBox.exe, DCv2.exe, procexp.exe, cmd.exe, conhost.exe, NVIDIA Web Helper.exe, and several instances of Discord.exe. The bottom of the window shows the 'Handles' tab, displaying a list of system handles with columns for Type and Name.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Virus Total
svchost.exe		1.508 K	7.656 K	26696	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		1.672 K	8.312 K	20144	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		11.228 K	26.416 K	16944	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		3.036 K	14.932 K	14532	Processo host per servizi di ...	Microsoft Corporation	
lsass.exe	< 0.01	13.168 K	28.920 K	1180	Local Security Authority Proc...	Microsoft Corporation	
explorer.exe	< 0.01	360.228 K	375.600 K	5048	Esplora risorse	Microsoft Corporation	
SecurityHealthSystray.exe		2.196 K	3.796 K	24432	Windows Security notification ...	Microsoft Corporation	
RtkAudUService64.exe		14.848 K	3.512 K	12260	Realtek HD Audio Universal ...	Realtek Semiconductor	
VirtualBox.exe	< 0.01	97.152 K	50.024 K	3904	VirtualBox Manager	Oracle and/or its affiliates	
DCv2.exe		182.844 K	22.200 K	8876	Dragon Center	Micro-Star INT'L CO., LTD.	
procexp.exe		5.824 K	14.456 K	26936	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		3.116 K	5.352 K	23828	Processore dei comandi di ...	Microsoft Corporation	
conhost.exe		1.412 K	9.380 K	20264	Host finestra console	Microsoft Corporation	0/22
NVIDIA Web Helper.exe	< 0.01	32.136 K	13.324 K	21508	NVIDIA Web Helper Service	Node.js	
Discord.exe	< 0.01	117.504 K	71.620 K	16272	Discord	Discord Inc.	
Discord.exe		11.840 K	3.012 K	11204	Discord	Discord Inc.	
Discord.exe	< 0.01	230.744 K	159.356 K	19116	Discord	Discord Inc.	
Discord.exe		17.072 K	17.656 K	21596	Discord	Discord Inc.	
Discord.exe	1.68	656.860 K	395.824 K	14608	Discord	Discord Inc.	
Discord.exe		12.388 K	8.072 K	10184	Discord	Discord Inc.	
nahimicNotifSys.exe		42.660 K	8.100 K	15628	A-Volute NS	A-Volute	
WD Discovery.exe	< 0.01	76.768 K	27.304 K	20436	WD Discovery	Western Digital Corporation	
WD Discovery.exe		28.380 K	5.608 K	17636	WD Discovery	Western Digital Corporation	

Type	Name
ALPC Port	\RPC Control\OLE31727D1A3326DDD0BD6363BD78AD
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\3\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	\Device\KsecDD
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperience\PackIt-IT_22621.86.330.0_n...
File	\Device\CNG
File	\Device\NamedPipe\
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKCU
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU\Software\Classes\Local Settings
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom
Key	HKCR\PackagedCom\TreatAsClassIndex
Key	HKCR\PackagedCom\ClassIndex
Key	HKCU\Software\Classes\PackagedCom
Key	HKCU\Software\Classes\PackagedCom\Package
Key	HKCR\PackagedCom\Package
Key	HKCU\Software\Classes
Key	HKCU\Software\Classes
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack
Key	HKCR\PackagedCom\InterfaceIndex



Process Explorer - Sysinternals: www.sysinternals.com [VINCENZO\Msi1]							
File Options View Process Find Users DLL Help							
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Virus Total
svchost.exe		1.508 K	7.656 K	26696	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		1.672 K	8.312 K	20144	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		11.248 K	26.412 K	16944	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe		3.036 K	14.932 K	14532	Processo host per servizi di ...	Microsoft Corporation	
Lsalso.exe		4.808 K	3.692 K	1164			
lsass.exe	< 0.01	13.172 K	28.904 K	1180	Local Security Authority Proc...	Microsoft Corporation	
fontdrvhost.exe		2.020 K	3.424 K	1328			
csrss.exe	< 0.01	3.540 K	8.568 K	21556			
winlogon.exe		2.448 K	11.284 K	18596			
fontdrvhost.exe		7.452 K	11.248 K	20624			
dwm.exe	< 0.01	164.932 K	161.772 K	10320			
explorer.exe	< 0.01	358.256 K	373.940 K	5048	Esplora risorse	Microsoft Corporation	
SecurityHealthSystray.exe		2.196 K	3.796 K	24432	Windows Security notification ...	Microsoft Corporation	
RtkAudUService64.exe	< 0.01	14.848 K	3.512 K	12260	Realtek HD Audio Universal ...	Realtek Semiconductor	
VirtualBox.exe	< 0.01	97.064 K	49.980 K	3904	VirtualBox Manager	Oracle and/or its affiliates	
DCv2.exe		182.844 K	22.204 K	8876	Dragon Center	Micro-Star INT'L CO., LTD.	
proccxp.exe		5.824 K	14.456 K	26936	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
proccxp64.exe	0.12	61.096 K	89.944 K	23320	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
cmd.exe		3.116 K	5.352 K	23828	Processore dei comandi di ...	Microsoft Corporation	
conhost.exe		1.384 K	9.364 K	20264	Host finestra console	Microsoft Corporation	0/77
SnippingTool.exe	< 0.01	2.308 K	11.332 K	1380			
NVIDIA Web Helper.exe	< 0.01	32.136 K	13.160 K	21508	NVIDIA Web Helper Service	Node.js	
Discord.exe	< 0.01	117.604 K	71.696 K	16272	Discord	Discord Inc.	
Discord.exe	< 0.01	11.840 K	3.012 K	11204	Discord	Discord Inc.	
Discord.exe	< 0.01	231.164 K	159.932 K	19116	Discord	Discord Inc.	
Discord.exe	< 0.01	17.072 K	17.656 K	21596	Discord	Discord Inc.	
Discord.exe	< 0.01	666.732 K	407.172 K	14608	Discord	Discord Inc.	
Discord.exe	< 0.01	12.388 K	8.072 K	10184	Discord	Discord Inc.	
nahimicNotifSys.exe		42.652 K	8.100 K	15628	A-Volute NS	A-Volute	
WD Discovery.exe	< 0.01	76.764 K	26.656 K	20436	WD Discovery	Western Digital Corporation	
Handles DLLs Threads							
Name	Description	Company Name	Path				
advapi32.dll	API Windows 32 Base avanzato	Microsoft Corporation	C:\Windows\System32\advapi32.dll				
bcrypt.dll	Libreria primitiva di crittografia di W...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll				
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll				
C_1252.NLS			C:\Windows\System32\C_1252.NLS				
C_850.NLS			C:\Windows\System32\C_850.NLS				
C_850.NLS			C:\Windows\System32\C_850.NLS				
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll				
combase.dll	Microsoft COM per Windows	Microsoft Corporation	C:\Windows\System32\combase.dll				
conhost.exe	Host finestra console	Microsoft Corporation	C:\Windows\System32\conhost.exe				
Conhost.exe.mui	Host finestra console	Microsoft Corporation	C:\Program Files\WindowsApps\Microsoft.LanguageExperi...				
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll				
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32full.dll				
imm32.dll	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	C:\Windows\System32\imm32.dll				
kernel.appcore.dll	AppModel API Host	Microsoft Corporation	C:\Windows\System32\kernel.appcore.dll				
kernel32.dll	DLL client di Windows NT BASE API	Microsoft Corporation	C:\Windows\System32\kernel32.dll				
KernelBase.dll	DLL client di Windows NT BASE API	Microsoft Corporation	C:\Windows\System32\KernelBase.dll				
_intl.nls			C:\Windows\System32\_intl.nls				
_intl.nls			C:\Windows\System32\_intl.nls				
locale.nls			C:\Windows\System32\locale.nls				
msvcp_win.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\msvcp_win.dll				
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:\Windows\System32\msvcrt.dll				
ntdll.dll	DLL del livello NT	Microsoft Corporation	C:\Windows\System32\ntdll.dll				
oleaut32.dll	OLEAUT32 DLL	Microsoft Corporation	C:\Windows\System32\oleaut32.dll				
OpenConsoleProxy...			C:\ProgramData\Microsoft\Windows\AppRepository\Packa...				
rpcrt4.dll	Runtime RPC (Remote Procedure ...	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll				
sechost.dll	Host for SCM/SDDL/LSA Lookup A...	Microsoft Corporation	C:\Windows\System32\sechost.dll				
ucrtbase.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\ucrtbase.dll				
user32.dll	Multi-User Windows USER API Cli...	Microsoft Corporation	C:\Windows\System32\user32.dll				
win32u.dll	Win32u	Microsoft Corporation	C:\Windows\System32\win32u.dll				
Windows.StateRep...	Windows StateRepository API Core	Microsoft Corporation	C:\Windows\System32\Windows.StateRepositoryCore.dll				
CPU Usage: 0.87%		Commit Charge: 53.09%	Processes: 277	Physical Usage: 63.67%			

Process Explorer - Sysinternals: www.sysinternals.com [VINCENZO\msi1]

FileOptionsViewProcessFindUsersThreadHelp

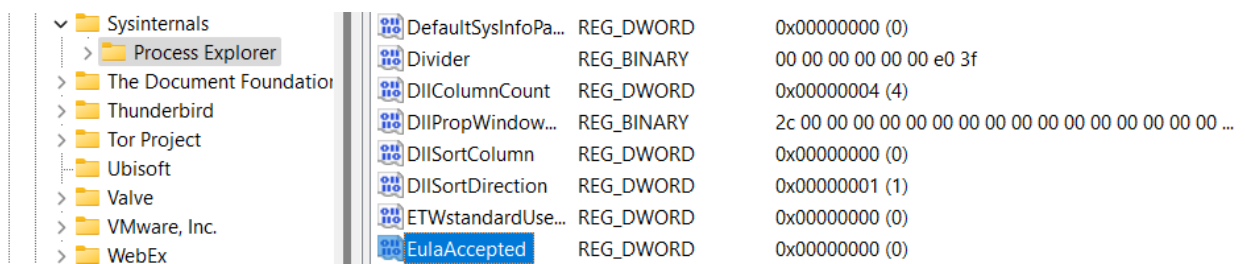
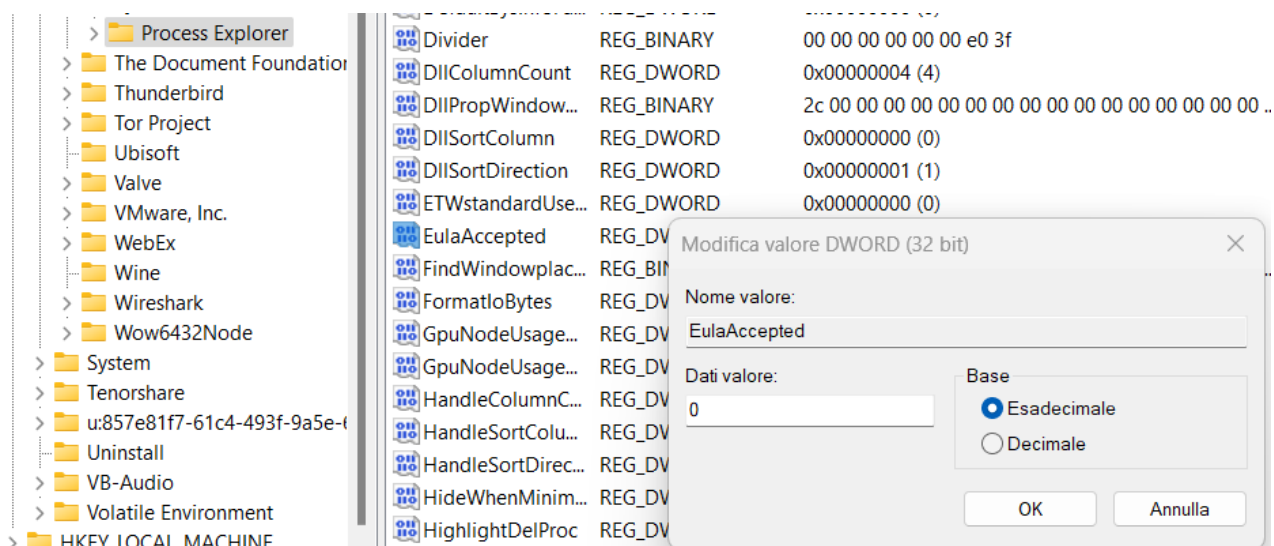
## Exploring Windows Registry

1. Vado su Start
2. Nella barra di ricerca digito "regedit"
3. Seleziono "Registry Editor" dai risultati
4. Quando appare il prompt UAC (User Account Control) che chiede il permesso di apportare modifiche al sistema, clicco "Yes"

A questo punto ho davanti l'Editor del Registry di Windows dove posso visualizzare e gestire le chiavi di registro del sistema.

1. Mi sposto nel percorso indicato:
  - HKEY\_CURRENT\_USER
  - Software
  - Sysinternals
  - Process Explorer
2. Cerco e trovo la chiave "EulaAccepted" che ha valore 0x00000001(1)
3. Faccio doppio click sulla chiave "EulaAccepted":
  - Vedo che il valore attuale è 1 (che indica che ho accettato l'EULA)
4. Modifico il valore:
  - Cambio l'1 in 0 (questo indica che l'EULA non è stata accettata)
  - Clicco "OK" per salvare la modifica





1. Vado nella cartella dove ho scaricato e estratto SysInternalsSuite
2. Faccio doppio click su procexp.exe

A questo punto, dato che ho impostato EulaAccepted a 0, Process Explorer dovrebbe mostrarmi nuovamente l'accordo di licenza (EULA) come se fosse la prima volta che lo apro, perché abbiamo "resettato" il suo stato di accettazione.

