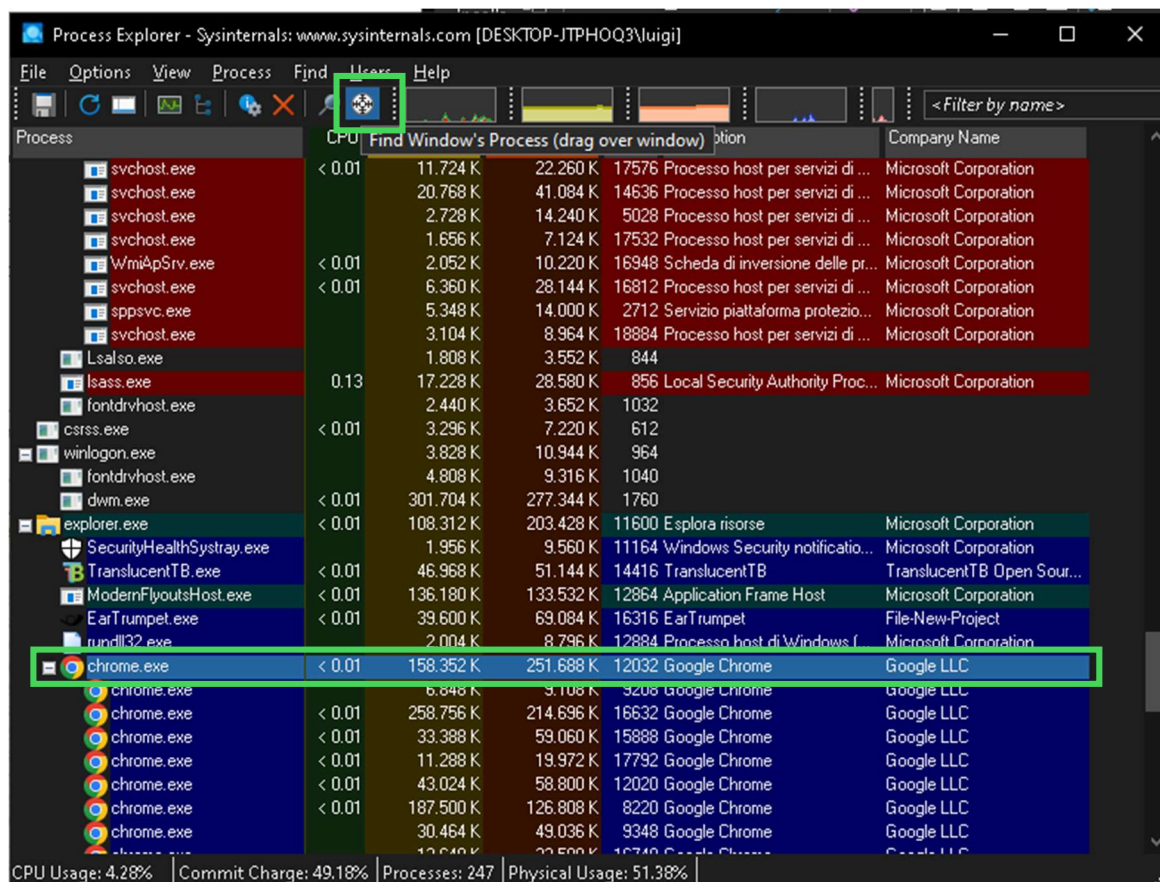
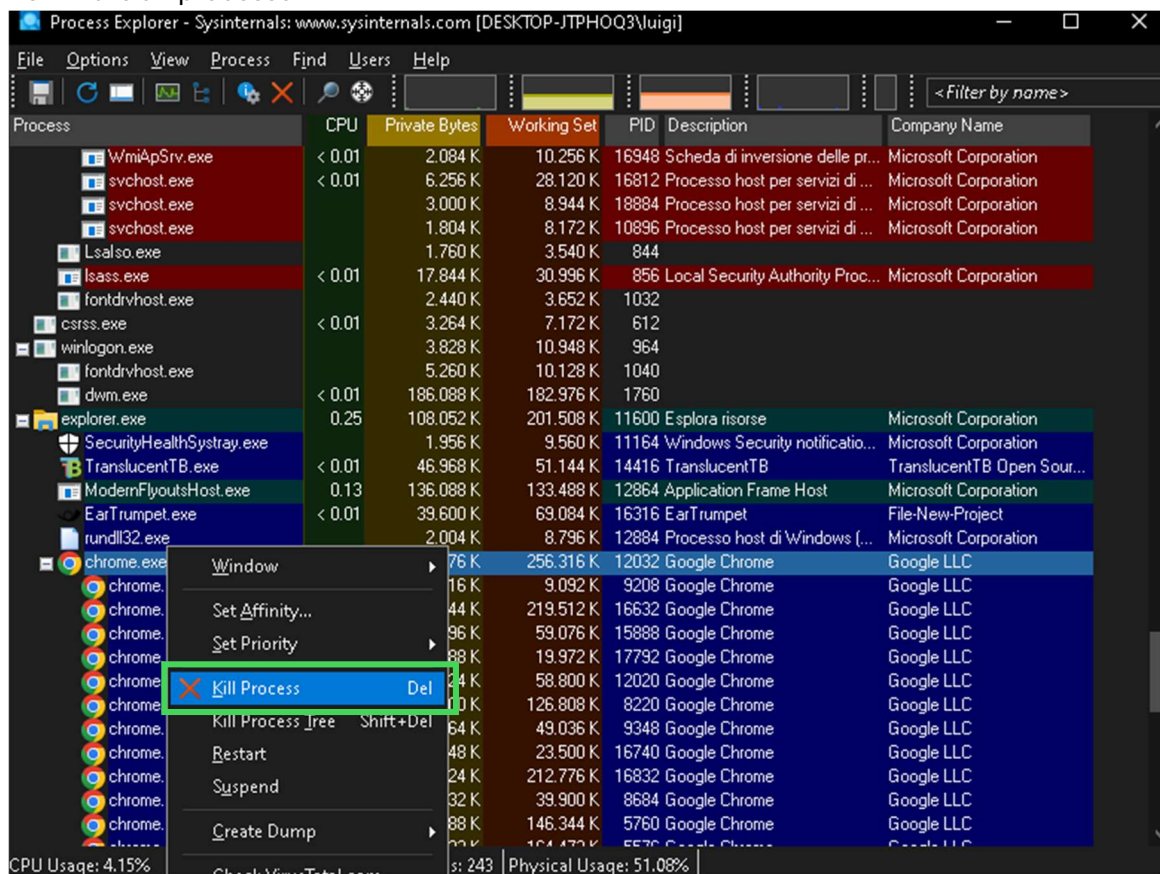


<https://itexamanswers.net/3-2-11-lab-exploring-processes-threads-handles-and-windows-registry-answers.html>



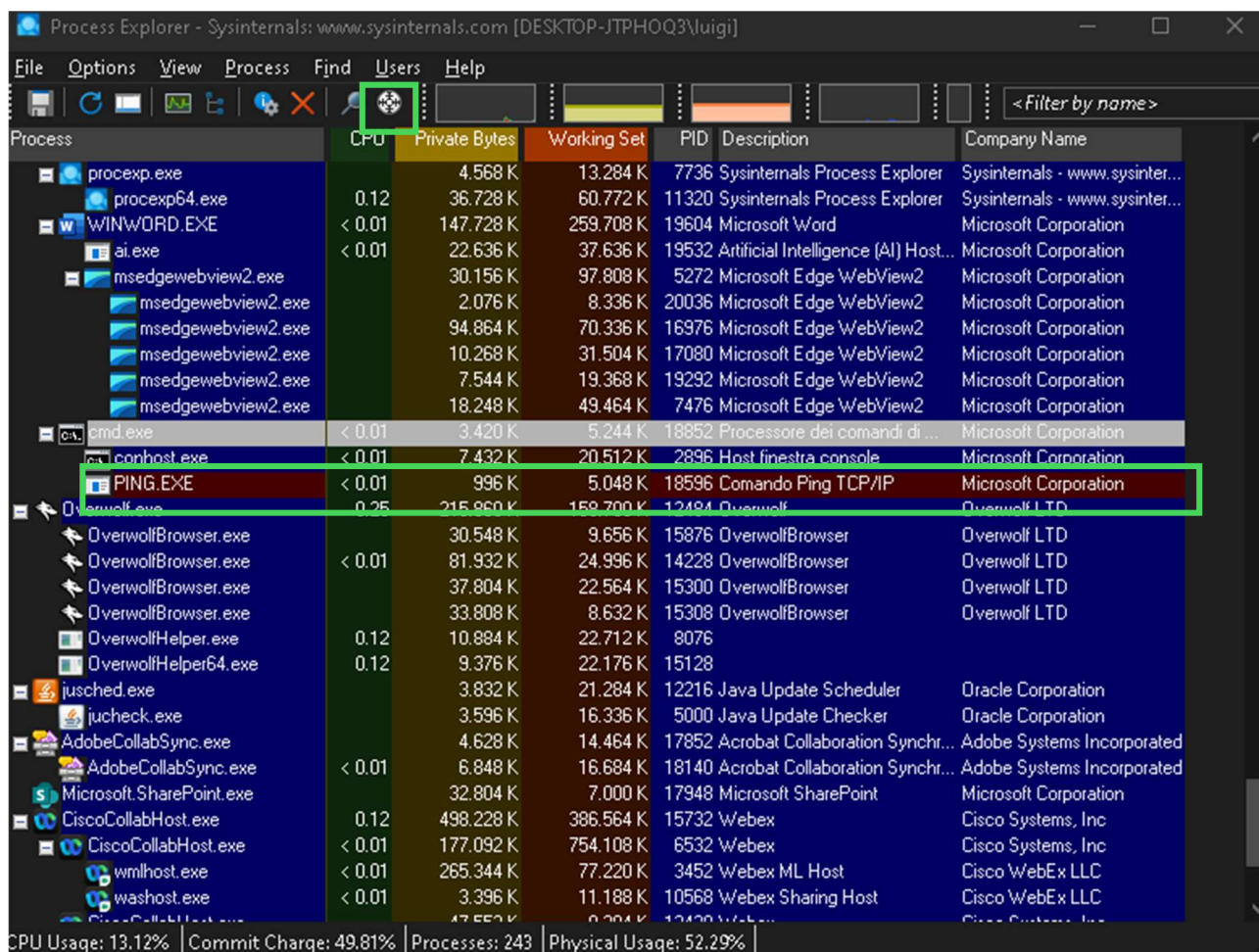
Per killare un processo:



Aperto il prompt dei comandi e trascinando il selettore di processi su di esso, comparirà il processo cmd.exe e se eseguiamo un ping, comparirà un processo figlio PING.exe

```
C:\Users\luigi>ping google.com

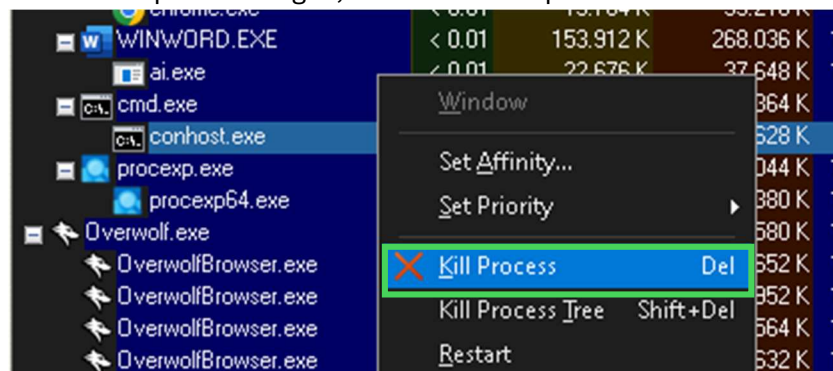
Esecuzione di Ping google.com [216.58.204.142] con 32 byte di dati:
Risposta da 216.58.204.142: byte=32 durata=28ms TTL=117
Risposta da 216.58.204.142: byte=32 durata=28ms TTL=117
Risposta da 216.58.204.142: byte=32 durata=28ms TTL=117
Risposta da 216.58.204.142: byte=32 durata=31ms TTL=117
```



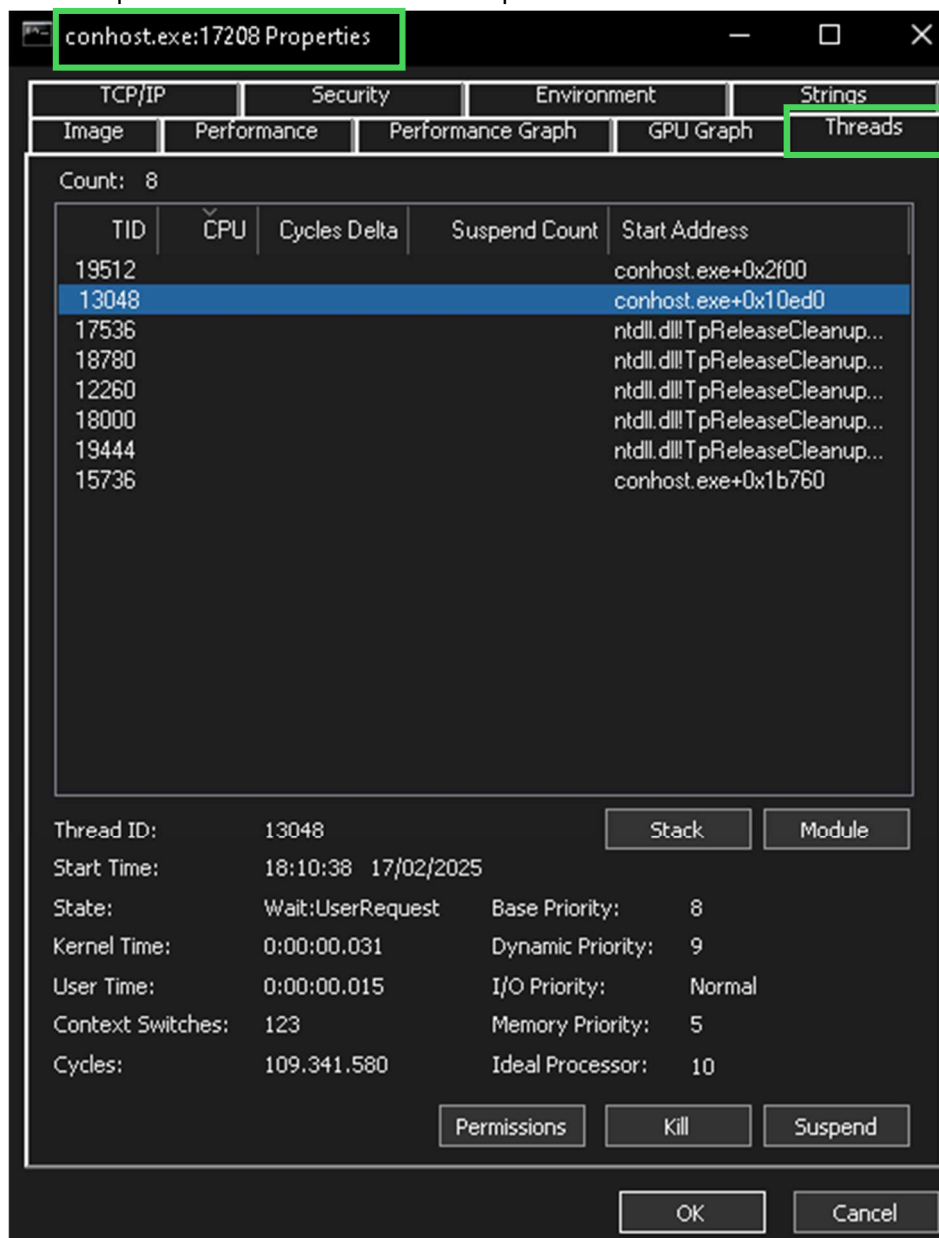
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
procexp.exe		4.568 K	13.284 K	7736	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.12	36.728 K	60.772 K	11320	Sysinternals Process Explorer	Sysinternals - www.sysinter...
WINWORD.EXE	< 0.01	147.728 K	259.708 K	19604	Microsoft Word	Microsoft Corporation
ai.exe	< 0.01	22.636 K	37.636 K	19532	Artificial Intelligence (AI) Host...	Microsoft Corporation
msedgewebview2.exe		30.156 K	97.808 K	5272	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2.076 K	8.336 K	20036	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		94.864 K	70.336 K	16976	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		10.268 K	31.504 K	17080	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		7.544 K	19.368 K	19292	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		18.248 K	49.464 K	7476	Microsoft Edge WebView2	Microsoft Corporation
cmd.exe	< 0.01	3.420 K	5.244 K	18852	Processore dei comandi di ...	Microsoft Corporation
conhost.exe	< 0.01	7.432 K	20.512 K	2896	Host finestra console	Microsoft Corporation
PING.EXE	< 0.01	996 K	5.048 K	18596	Comando Ping TCP/IP	Microsoft Corporation
Overwolf.exe	0.25	215.880 K	159.700 K	12484	Overwolf	Overwolf LTD
OverwolfBrowser.exe		30.548 K	9.656 K	15876	OverwolfBrowser	Overwolf LTD
OverwolfBrowser.exe	< 0.01	81.932 K	24.996 K	14228	OverwolfBrowser	Overwolf LTD
OverwolfBrowser.exe		37.804 K	22.564 K	15300	OverwolfBrowser	Overwolf LTD
OverwolfBrowser.exe		33.808 K	8.632 K	15308	OverwolfBrowser	Overwolf LTD
OverwolfHelper.exe	0.12	10.884 K	22.712 K	8076		
OverwolfHelper64.exe	0.12	9.376 K	22.176 K	15128		
jusched.exe		3.832 K	21.284 K	12216	Java Update Scheduler	Oracle Corporation
jucheck.exe		3.596 K	16.336 K	5000	Java Update Checker	Oracle Corporation
AdobeCollabSync.exe		4.628 K	14.464 K	17852	Acrobat Collaboration Synchr...	Adobe Systems Incorporated
AdobeCollabSync.exe	< 0.01	6.848 K	16.684 K	18140	Acrobat Collaboration Synchr...	Adobe Systems Incorporated
Microsoft.SharePoint.exe		32.804 K	7.000 K	17948	Microsoft SharePoint	Microsoft Corporation
CiscoCollabHost.exe	0.12	498.228 K	386.564 K	15732	Webex	Cisco Systems, Inc
CiscoCollabHost.exe	< 0.01	177.092 K	754.108 K	6532	Webex	Cisco Systems, Inc
wmlhost.exe	< 0.01	265.344 K	77.220 K	3452	Webex ML Host	Cisco WebEx LLC
washost.exe	< 0.01	3.396 K	11.188 K	10568	Webex Sharing Host	Cisco WebEx LLC

CPU Usage: 13.12% | Commit Charge: 49.81% | Processes: 243 | Physical Usage: 52.29%

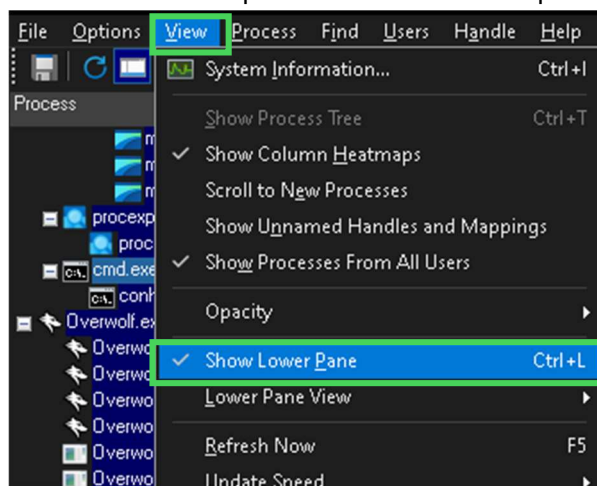
Se si killa il processo figlio, muore anche il padre:

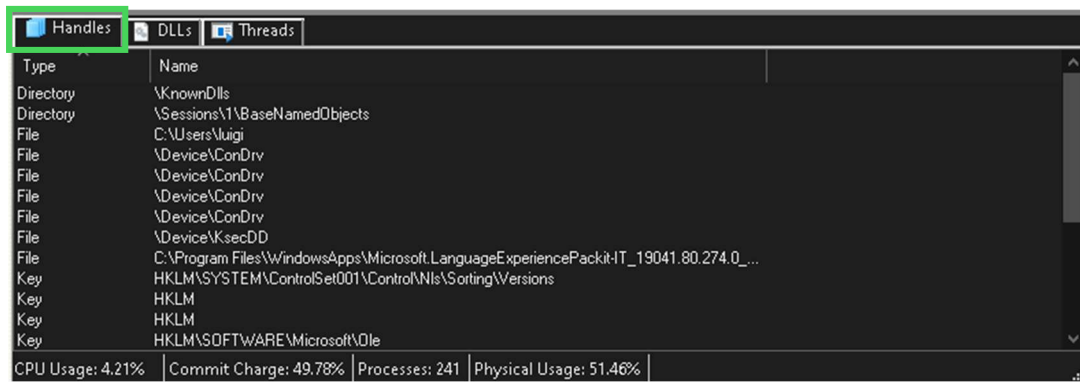


È anche possibile vedere i Thread di un processo cliccandoci col tasto destro e andando su proprietà:



È anche possibile gli handler che puntano a file, chiavi di registro e thread, andando nella finestra visualizza>mostra pannello inferiore e dal pannello inferiore basta andare nella sezione handles:





Type	Name
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
File	C:\Users\luigi
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\KsecDD
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePack\it-IT_19041.80.274.0_...
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\OLE

CPU Usage: 4.21% | Commit Charge: 49.78% | Processes: 241 | Physical Usage: 51.46%