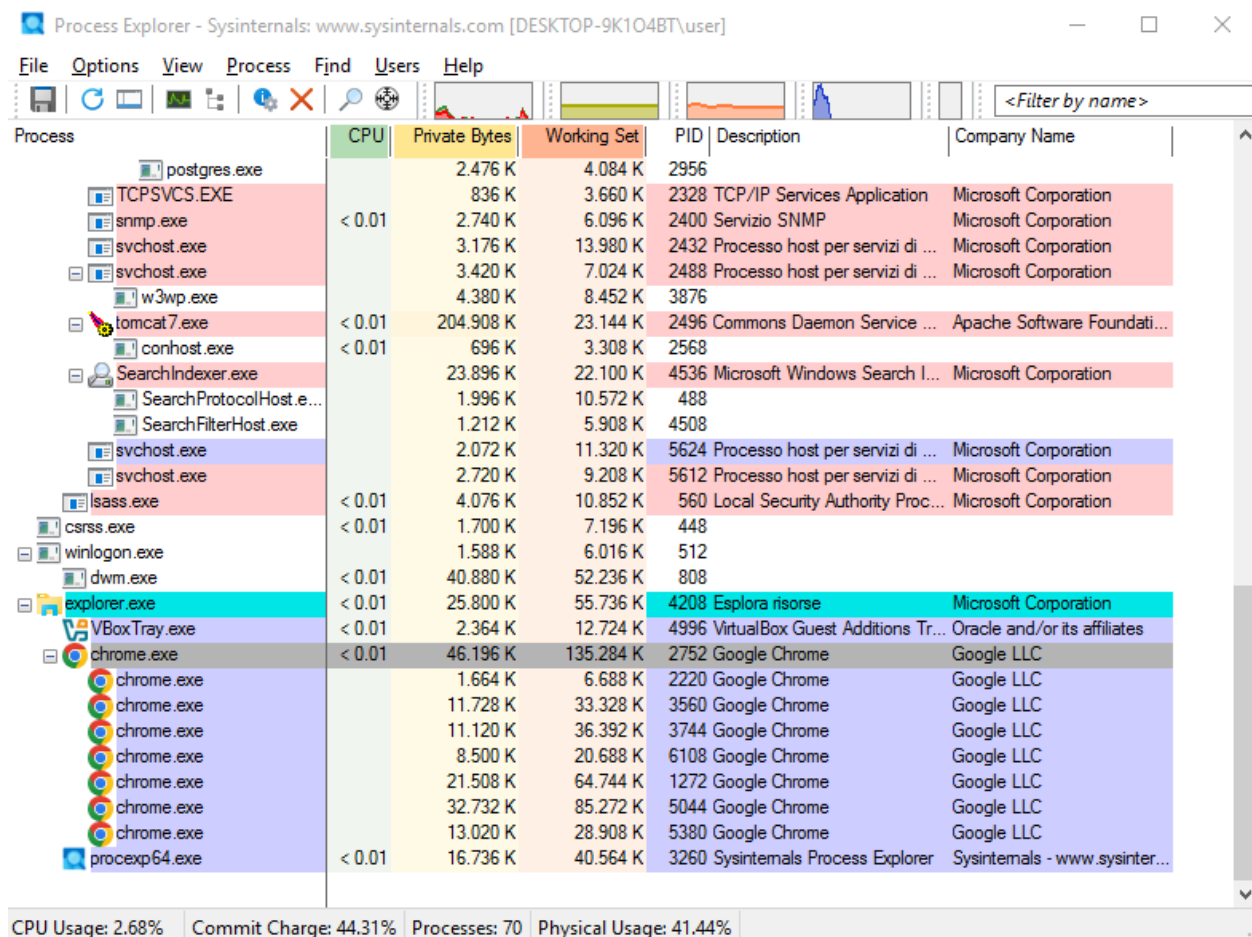


S11L1

Domanda: Cosa è successo alla finestra del browser web quando il processo è stato terminato?

Risposta: La finestra del browser si chiude immediatamente e scompare dallo schermo perché il processo che la gestiva è stato forzatamente interrotto.



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]

File Options View Process Find Users Help

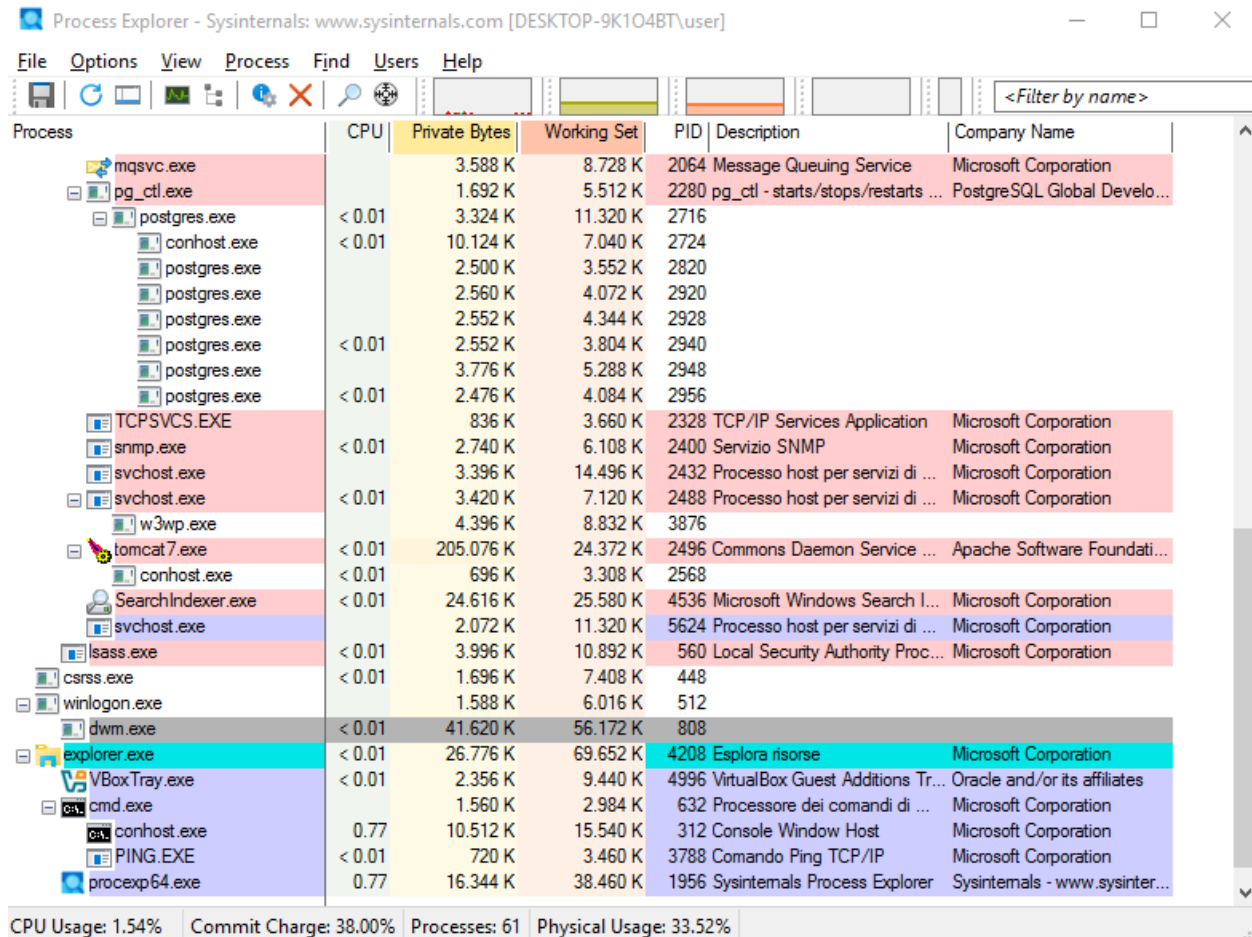
<Filter by name>

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|------------------------|--------|---------------|-------------|------|----------------------------------|--------------------------------|
| postgres.exe | | 2.476 K | 4.084 K | 2956 | | |
| TCPSSVC.SERVICE | | 836 K | 3.660 K | 2328 | TCP/IP Services Application | Microsoft Corporation |
| snmp.exe | < 0.01 | 2.740 K | 6.096 K | 2400 | Servizio SNMP | Microsoft Corporation |
| svchost.exe | | 3.176 K | 13.980 K | 2432 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | | 3.420 K | 7.024 K | 2488 | Processo host per servizi di ... | Microsoft Corporation |
| w3wp.exe | | 4.380 K | 8.452 K | 3876 | | |
| tomcat7.exe | < 0.01 | 204.908 K | 23.144 K | 2496 | Commons Daemon Service ... | Apache Software Foundati... |
| conhost.exe | < 0.01 | 696 K | 3.308 K | 2568 | | |
| SearchIndexer.exe | | 23.896 K | 22.100 K | 4536 | Microsoft Windows Search I... | Microsoft Corporation |
| SearchProtocolHost.exe | | 1.996 K | 10.572 K | 488 | | |
| SearchFilterHost.exe | | 1.212 K | 5.908 K | 4508 | | |
| svchost.exe | | 2.072 K | 11.320 K | 5624 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | | 2.720 K | 9.208 K | 5612 | Processo host per servizi di ... | Microsoft Corporation |
| lsass.exe | < 0.01 | 4.076 K | 10.852 K | 560 | Local Security Authority Proc... | Microsoft Corporation |
| csrss.exe | < 0.01 | 1.700 K | 7.196 K | 448 | | |
| winlogon.exe | | 1.588 K | 6.016 K | 512 | | |
| dwm.exe | < 0.01 | 40.880 K | 52.236 K | 808 | | |
| explorer.exe | < 0.01 | 25.800 K | 55.736 K | 4208 | Esplora risorse | Microsoft Corporation |
| VBBoxTray.exe | < 0.01 | 2.364 K | 12.724 K | 4996 | VirtualBox Guest Additions Tr... | Oracle and/or its affiliates |
| chrome.exe | < 0.01 | 46.196 K | 135.284 K | 2752 | Google Chrome | Google LLC |
| chrome.exe | | 1.664 K | 6.688 K | 2220 | Google Chrome | Google LLC |
| chrome.exe | | 11.728 K | 33.328 K | 3560 | Google Chrome | Google LLC |
| chrome.exe | | 11.120 K | 36.392 K | 3744 | Google Chrome | Google LLC |
| chrome.exe | | 8.500 K | 20.688 K | 6108 | Google Chrome | Google LLC |
| chrome.exe | | 21.508 K | 64.744 K | 1272 | Google Chrome | Google LLC |
| chrome.exe | | 32.732 K | 85.272 K | 5044 | Google Chrome | Google LLC |
| chrome.exe | | 13.020 K | 28.908 K | 5380 | Google Chrome | Google LLC |
| procexp64.exe | < 0.01 | 16.736 K | 40.564 K | 3260 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |

CPU Usage: 2.68% Commit Charge: 44.31% Processes: 70 Physical Usage: 41.44%

Domanda: Cosa è successo durante il processo ping?

Risposta: Sotto il processo **cmd.exe** in Process Explorer, dovresti veder apparire temporaneamente un nuovo processo figlio (**PING.EXE**) che scompare una volta terminata l'operazione.



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K104BT\user]

File Options View Process Find Users Help

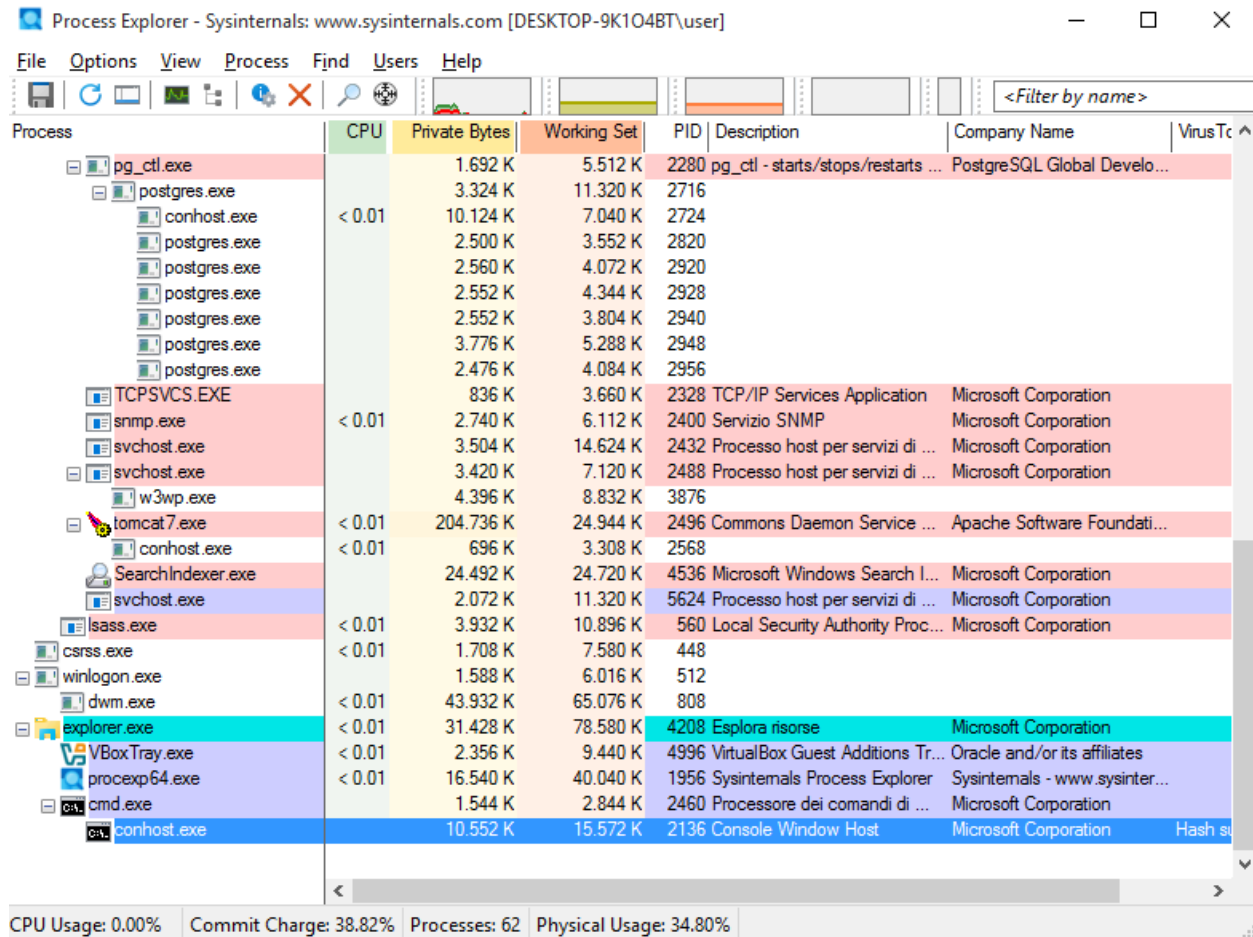
<Filter by name>

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|-------------------|--------|---------------|-------------|------|------------------------------------|--------------------------------|
| mqsvc.exe | | 3.588 K | 8.728 K | 2064 | Message Queuing Service | Microsoft Corporation |
| pg_ctl.exe | | 1.692 K | 5.512 K | 2280 | pg_ctl - starts/stops/restarts ... | PostgreSQL Global Develo... |
| postgres.exe | < 0.01 | 3.324 K | 11.320 K | 2716 | | |
| conhost.exe | < 0.01 | 10.124 K | 7.040 K | 2724 | | |
| postgres.exe | | 2.500 K | 3.552 K | 2820 | | |
| postgres.exe | | 2.560 K | 4.072 K | 2920 | | |
| postgres.exe | | 2.552 K | 4.344 K | 2928 | | |
| postgres.exe | < 0.01 | 2.552 K | 3.804 K | 2940 | | |
| postgres.exe | | 3.776 K | 5.288 K | 2948 | | |
| postgres.exe | < 0.01 | 2.476 K | 4.084 K | 2956 | | |
| TCPVCS.EXE | | 836 K | 3.660 K | 2328 | TCP/IP Services Application | Microsoft Corporation |
| snmp.exe | < 0.01 | 2.740 K | 6.108 K | 2400 | Servizio SNMP | Microsoft Corporation |
| svchost.exe | | 3.396 K | 14.496 K | 2432 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | < 0.01 | 3.420 K | 7.120 K | 2488 | Processo host per servizi di ... | Microsoft Corporation |
| w3wp.exe | | 4.396 K | 8.832 K | 3876 | | |
| tomcat7.exe | < 0.01 | 205.076 K | 24.372 K | 2496 | Commons Daemon Service ... | Apache Software Foundati... |
| conhost.exe | < 0.01 | 696 K | 3.308 K | 2568 | | |
| SearchIndexer.exe | < 0.01 | 24.616 K | 25.580 K | 4536 | Microsoft Windows Search I... | Microsoft Corporation |
| svchost.exe | | 2.072 K | 11.320 K | 5624 | Processo host per servizi di ... | Microsoft Corporation |
| lsass.exe | < 0.01 | 3.996 K | 10.892 K | 560 | Local Security Authority Proc... | Microsoft Corporation |
| csrss.exe | < 0.01 | 1.696 K | 7.408 K | 448 | | |
| winlogon.exe | | 1.588 K | 6.016 K | 512 | | |
| dwm.exe | < 0.01 | 41.620 K | 56.172 K | 808 | | |
| explorer.exe | < 0.01 | 26.776 K | 69.652 K | 4208 | Esplora risorse | Microsoft Corporation |
| VBoxTray.exe | < 0.01 | 2.356 K | 9.440 K | 4996 | VirtualBox Guest Additions Tr... | Oracle and/or its affiliates |
| cmd.exe | | 1.560 K | 2.984 K | 632 | Processore dei comandi di ... | Microsoft Corporation |
| conhost.exe | 0.77 | 10.512 K | 15.540 K | 312 | Console Window Host | Microsoft Corporation |
| PING.EXE | < 0.01 | 720 K | 3.460 K | 3788 | Comando Ping TCP/IP | Microsoft Corporation |
| procexp64.exe | 0.77 | 16.344 K | 38.460 K | 1956 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |

CPU Usage: 1.54% Commit Charge: 38.00% Processes: 61 Physical Usage: 33.52%

Domanda: Cosa è successo al processo figlio conhost.exe?

Risposta: Solitamente, quando si termina il processo padre (**cmd.exe**), anche il processo figlio strettamente dipendente come **conhost.exe** (che gestisce la finestra della console) viene terminato o si chiude immediatamente.



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-9K1O4BT\user]

File Options View Process Find Users Help

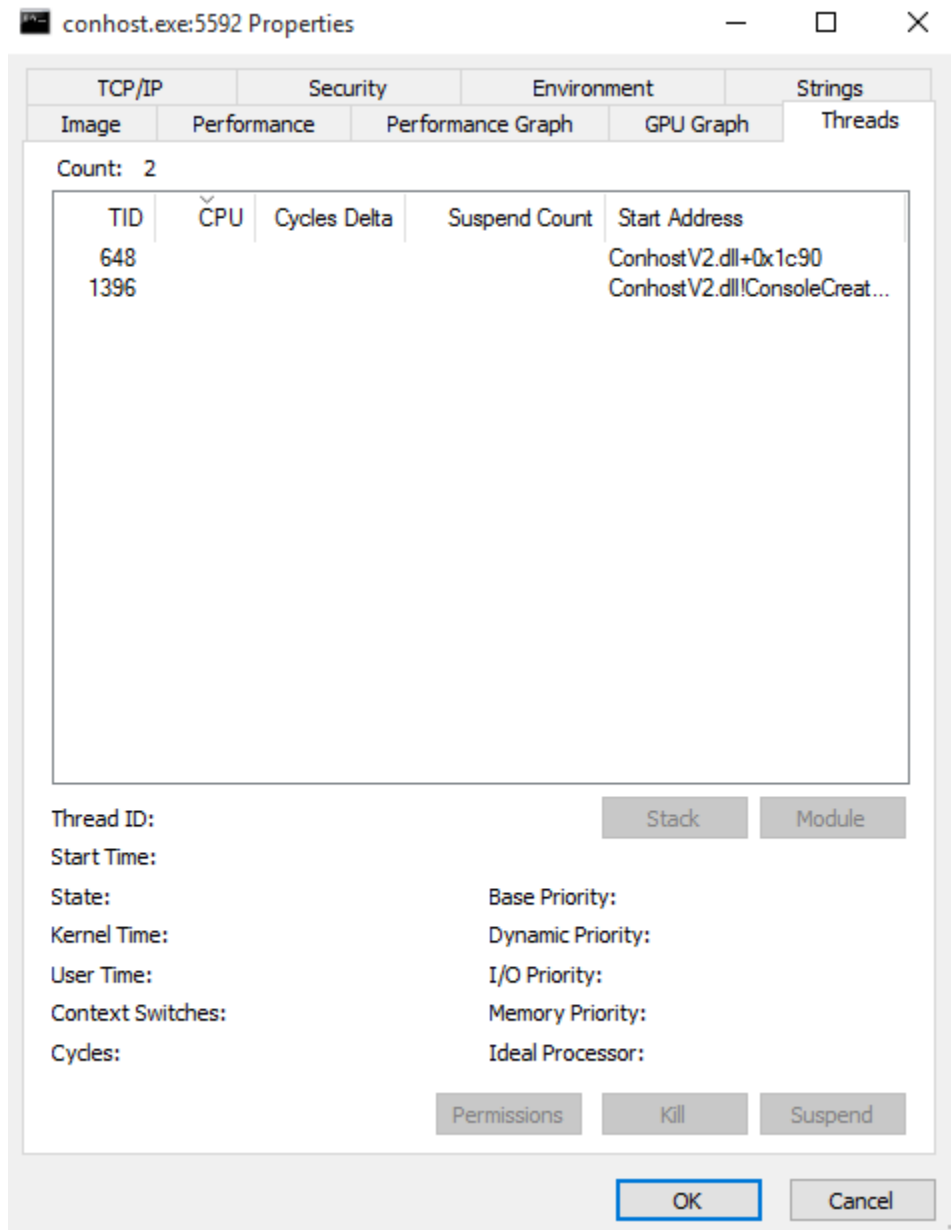
<Filter by name>

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name | VirusTc |
|-------------------|--------|---------------|-------------|------|------------------------------------|--------------------------------|---------|
| pg_ctl.exe | | 1.692 K | 5.512 K | 2280 | pg_ctl - starts/stops/restarts ... | PostgreSQL Global Develo... | |
| postgres.exe | | 3.324 K | 11.320 K | 2716 | | | |
| conhost.exe | < 0.01 | 10.124 K | 7.040 K | 2724 | | | |
| postgres.exe | | 2.500 K | 3.552 K | 2820 | | | |
| postgres.exe | | 2.560 K | 4.072 K | 2920 | | | |
| postgres.exe | | 2.552 K | 4.344 K | 2928 | | | |
| postgres.exe | | 2.552 K | 3.804 K | 2940 | | | |
| postgres.exe | | 3.776 K | 5.288 K | 2948 | | | |
| postgres.exe | | 2.476 K | 4.084 K | 2956 | | | |
| TCPVCS.EXE | | 836 K | 3.660 K | 2328 | TCP/IP Services Application | Microsoft Corporation | |
| snmp.exe | < 0.01 | 2.740 K | 6.112 K | 2400 | Servizio SNMP | Microsoft Corporation | |
| svchost.exe | | 3.504 K | 14.624 K | 2432 | Processo host per servizi di ... | Microsoft Corporation | |
| svchost.exe | | 3.420 K | 7.120 K | 2488 | Processo host per servizi di ... | Microsoft Corporation | |
| w3wp.exe | | 4.396 K | 8.832 K | 3876 | | | |
| tomcat7.exe | < 0.01 | 204.736 K | 24.944 K | 2496 | Commons Daemon Service ... | Apache Software Foundati... | |
| conhost.exe | < 0.01 | 696 K | 3.308 K | 2568 | | | |
| SearchIndexer.exe | | 24.492 K | 24.720 K | 4536 | Microsoft Windows Search I... | Microsoft Corporation | |
| svchost.exe | | 2.072 K | 11.320 K | 5624 | Processo host per servizi di ... | Microsoft Corporation | |
| lsass.exe | < 0.01 | 3.932 K | 10.896 K | 560 | Local Security Authority Proc... | Microsoft Corporation | |
| csrss.exe | < 0.01 | 1.708 K | 7.580 K | 448 | | | |
| winlogon.exe | | 1.588 K | 6.016 K | 512 | | | |
| dwm.exe | < 0.01 | 43.932 K | 65.076 K | 808 | | | |
| explorer.exe | < 0.01 | 31.428 K | 78.580 K | 4208 | Esplora risorse | Microsoft Corporation | |
| VBoxTray.exe | < 0.01 | 2.356 K | 9.440 K | 4996 | VirtualBox Guest Additions Tr... | Oracle and/or its affiliates | |
| procexp64.exe | < 0.01 | 16.540 K | 40.040 K | 1956 | Sysinternals Process Explorer | Sysinternals - www.sysinter... | |
| cmd.exe | | 1.544 K | 2.844 K | 2460 | Processore dei comandi di ... | Microsoft Corporation | |
| conhost.exe | | 10.552 K | 15.572 K | 2136 | Console Window Host | Microsoft Corporation | Hash su |

CPU Usage: 0.00% Commit Charge: 38.82% Processes: 62 Physical Usage: 34.80%

Domanda: Che tipo di informazioni sono disponibili nella finestra Proprietà?

Risposta: Puoi vedere l'ID del thread (TID), il tempo di CPU utilizzato (Kernel/User Time), lo stato, l'indirizzo di memoria di avvio (Start Address) e informazioni sullo stack.



Domanda: A cosa puntano gli handle?

Risposta: Gli handle puntano a risorse di sistema come **file** (percorsi su disco), **chiavi di registro**, **eventi**, **semafori**, **thread** e **directory**. Rappresentano le risorse che il processo sta "toccando" o utilizzando in quel momento.

The screenshot shows the Process Explorer window from Sysinternals. The top pane displays a list of processes. The bottom pane shows the 'Handles' tab for the selected process, w3wp.exe.

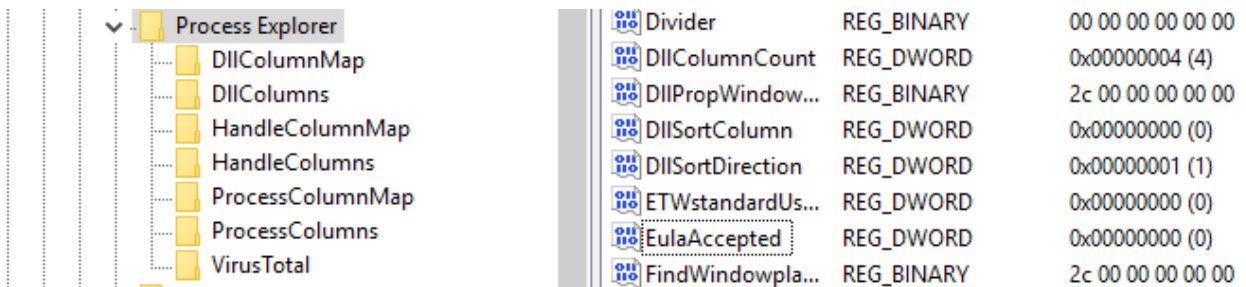
| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|--------------|--------|---------------|-------------|------|------------------------------------|-----------------------------|
| pg_ctl.exe | | 1.692 K | 5.512 K | 2280 | pg_ctl - starts/stops/restarts ... | PostgreSQL Global Develo... |
| postgres.exe | | 3.324 K | 11.320 K | 2716 | | |
| conhost.exe | < 0.01 | 10.124 K | 7.040 K | 2724 | | |
| postgres.exe | | 2.500 K | 3.552 K | 2820 | | |
| postgres.exe | | 2.560 K | 4.072 K | 2920 | | |
| postgres.exe | | 2.552 K | 4.344 K | 2928 | | |
| postgres.exe | | 2.552 K | 3.804 K | 2940 | | |
| postgres.exe | | 3.776 K | 5.288 K | 2948 | | |
| postgres.exe | | 2.476 K | 4.084 K | 2956 | | |
| TCPVCS.EXE | | 836 K | 3.660 K | 2328 | TCP/IP Services Application | Microsoft Corporation |
| snmp.exe | | 2.740 K | 6.116 K | 2400 | Servizio SNMP | Microsoft Corporation |
| svchost.exe | | 3.312 K | 14.528 K | 2432 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | | 3.420 K | 7.120 K | 2488 | Processo host per servizi di ... | Microsoft Corporation |
| w3wp.exe | | | | | | |

| Type | Name |
|-----------|--|
| Desktop | \Default |
| Directory | \KnownDlls |
| Directory | \Sessions\1\BaseNamedObjects |
| Event | \KernelObjects\MaximumCommitCondition |
| Event | \BaseNamedObjects\TermSrvReadyEvent |
| File | \Device\ConDrv |
| File | C:\Windows |
| File | \Device\CNG |
| File | C:\Windows\System32\it-IT\user32.dll.mui |
| File | C:\Windows\System32\it-IT\ConhostV2.dll.mui |
| File | C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.... |
| Key | HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions |
| Key | HKLM |

CPU Usage: 0.00% Commit Charge: 38.13% Processes: 60 Physical Usage: 33.97%

Domanda: Qual è il valore per questa chiave di registro nella colonna Dati (Data)?

Risposta: Ora il valore visualizzato è **0x00000000 (0)**.



Domanda: Quando apri Process Explorer, cosa vedi?

Risposta: Ti apparirà nuovamente la finestra pop-up con l'Accordo di Licenza (EULA). Questo accade perché abbiamo modificato il registro dicendo al programma che l'utente non ha ancora accettato la licenza.

