

# Esercizio di Pratica S11L1 -Esplorazione di Processi, Thread, Handle e Registro di Windows

## Sergio Falcone

### INTRODUZIONE

In questa parte, esplorerai i processi. I processi sono programmi o applicazioni in esecuzione. Esplorerai i processi utilizzando Process Explorer nella Suite SysInternals di Windows. Avvierai e osserverai anche un nuovo processo.

1. Esplorare un processo attivo (**Microsoft Edge**).

Il processo di Microsoft Edge può essere terminato in Process Explorer  
**Cosa è successo alla finestra del browser web quando il processo è stato terminato?**

2. Avviare un altro processo (**cmd.exe**)

Avviare un **ping** al prompt e osservare i cambiamenti sotto il processo cmd.exe.

**Cosa è successo durante il processo ping?**

3. Il processo figlio conhost.exe potrebbe essere sospetto. Selezionare **Check VirusTotal**.

4. Sul processo cmd.exe, selezionare **Kill Process**.

**Cosa è successo al processo figlio conhost.exe?**

5. Esplorazione di **Thread** e **Handle** (**chhost.exe**)

Esaminare i dettagli del thread.

**Che tipo di informazioni sono disponibili nella finestra Proprietà?**

Esplorare gli handle.

**A cosa puntano gli handle?**

6. Esplorazione del Registro di Windows

In **HKEY\_CURRENT\_USER**, individuare la chiave **EulaAccepted** e cambiare il valore 1 in 0

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

7. Aprire la cartella **SysInternalsSuite** > Aprire **procexp.exe**.  
 Quando apri Process Explorer, cosa vedi?

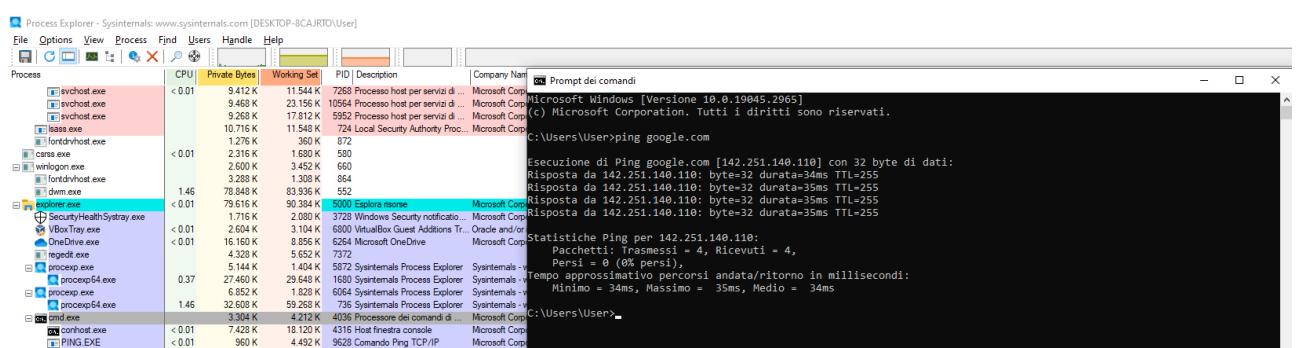
## ESECUZIONE

1. Estratto e avviato **Process Explorer(procexp.exe)** il quale mostra un elenco dei processi attualmente attivi, si è localizzato il processo del browser web trascinando l'icona **Find Window's Process**

msedge.exe	0.58	72.708 K	77.904 K	1084	Microsoft Edge	Microsoft Corporation
msedge.exe		2.288 K	1.352 K	7696	Microsoft Edge	Microsoft Corporation
msedge.exe		12.760 K	12.928 K	1160	Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	15.976 K	21.168 K	8560	Microsoft Edge	Microsoft Corporation
msedge.exe		8.828 K	4.420 K	9192	Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	58.088 K	72.432 K	4064	Microsoft Edge	Microsoft Corporation
msedge.exe		36.008 K	5.968 K	9944	Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	320.416 K	148.424 K	7120	Microsoft Edge	Microsoft Corporation
msedge.exe		9.112 K	4.912 K	6716	Microsoft Edge	Microsoft Corporation
msedge.exe		23.340 K	5.136 K	2424	Microsoft Edge	Microsoft Corporation

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

- Terminato il processo (**Kill Process**) la finestra del browser si è chiusa.
2. Si è avviato il Prompt dei Comandi (**cmd.exe**) e si è effettuato il **ping** verso [google.com](http://google.com) (**ping google.com**)



Cosa è successo durante il processo ping?

- Durante il processo di ping si è creato il processo temporaneo **PING.EXE**, il quale è sparito una volta terminato il processo di ping

3. Con il tasto destro su **conhost.exe** si è effettuato il check con **VirusTotal**

The screenshot shows the VirusTotal analysis interface. At the top left, there's a circular icon with a '0' and '/71'. Below it, a 'Community Score' button. In the center, a file analysis card for 'CONHOST.EXE' with the hash 'a26a1ff81a61281ffa55cb7778cc3fb0ff981704de49f75f1f18b283fba7a2'. It indicates 'No security vendors flagged this file as malicious'. Below the card are tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY' (with 15+ items). A green banner at the bottom encourages joining the community.

- Process Explorer calcola l'**hash** di **conhost.exe** e invia l'**hash** a **VirusTotal**, il browser mostra il report (0/70)

#### 4. Si seleziona Kill Process su cmd.exe

[Cosa è successo al processo figlio conhost.exe?](#)

- Entrambi i processi si sono illuminati e chiuso il processo **cmd.exe** si è chiuso anche il processo **conhost.exe**

#### 5. Vengono esaminati i dettagli del **thread**.

I thread sono le unità di esecuzione all'interno di un processo. Più thread possono appartenere allo stesso processo e condividono memoria e risorse, ma ciascun thread ha il proprio flusso di esecuzione e stack

The screenshot shows the Windows Task Manager. On the left, the 'Threads' tab of the 'conhost.exe:3864 Properties' dialog is open, displaying three threads with TID 6292, 11204, and 5648. On the right, a list of threads is shown in a grid view. The columns are CPU, Private Bytes, Working Set, PID, Description, and Comp. Notable threads include msedge.exe, explorer.exe, and cmd.exe. The 'explorer.exe' thread has a PID of 5000 and is described as '5000 Explora risorse'. The 'cmd.exe' thread has a PID of 9808 and is described as '9808 Processore dei comandi di ...'. The 'conhost.exe' thread has a PID of 3854 and is described as '3854 Host finestra console'.

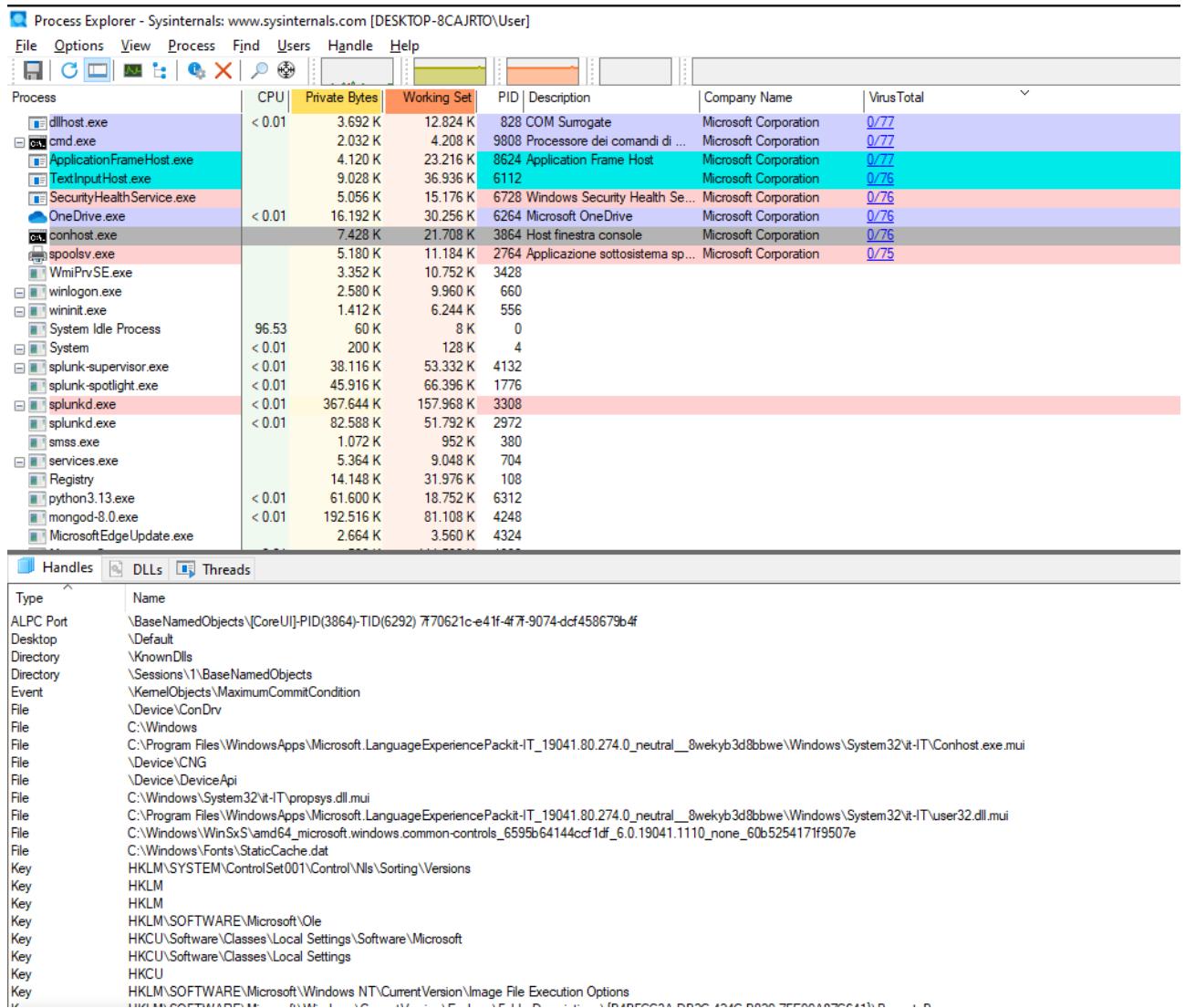
[Che tipo di informazioni sono disponibili nella finestra Proprietà?](#)

- Nella finestra delle Proprietà, nella sezione Threads sono disponibili Thread ID (TID) e Start Address, CPU cioè l'utilizzo di risorse e lo stato dei threads. Queste informazioni permettono di analizzare il

comportamento del processo, il carico di lavoro dei singoli thread e l’interazione con il sistema operativo.

Si esplorano gli Handles.

Un handle è un riferimento astratto creato dal sistema operativo per accedere a risorse interne e permette al processo di interagire con risorse senza conoscere direttamente gli indirizzi fisici o la struttura interna dell’oggetto.



The screenshot shows two windows from the Process Explorer tool. The top window is titled 'Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-8CAJRTO\User]' and displays a list of running processes. The columns include Process, CPU, Private Bytes, Working Set, PID, Description, Company Name, and Virus Total. The bottom window is titled 'Handles' and lists various handles categorized by type (ALPC Port, Desktop, Directory, Event, File, Key) and their corresponding names. The handles include system paths like '\BaseNamedObjects\{CoreUI}-PID(3864)-TID(6292)\70621c-e41f-4f79-9074-dcf458679b4' and registry keys like 'HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions'.

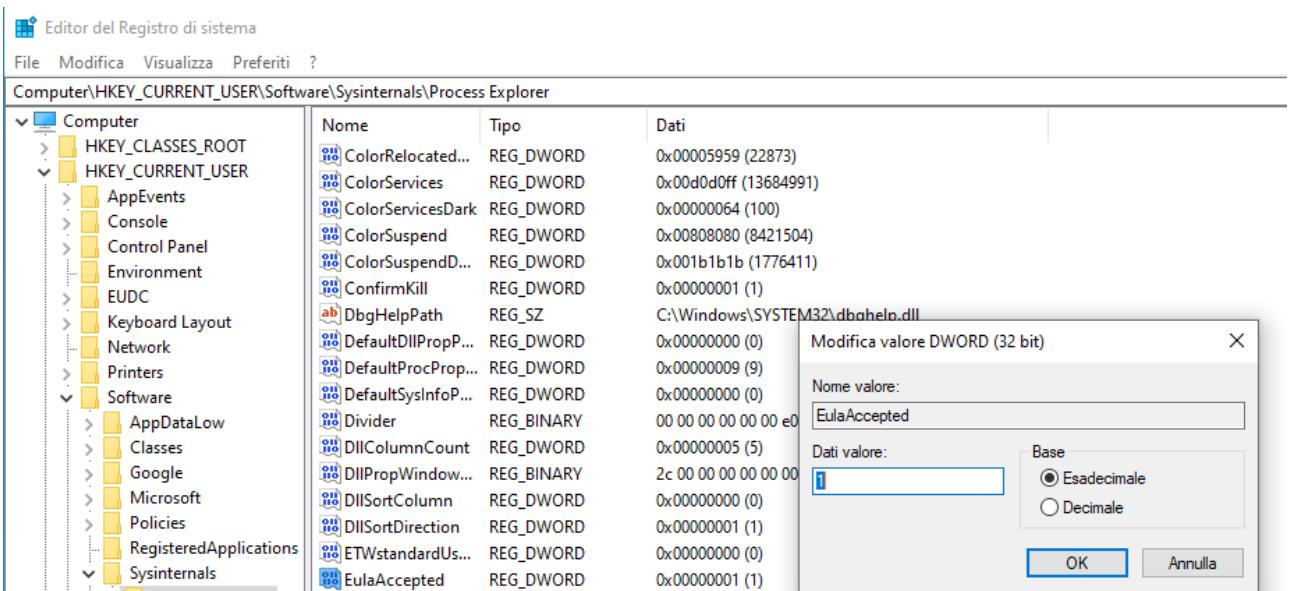
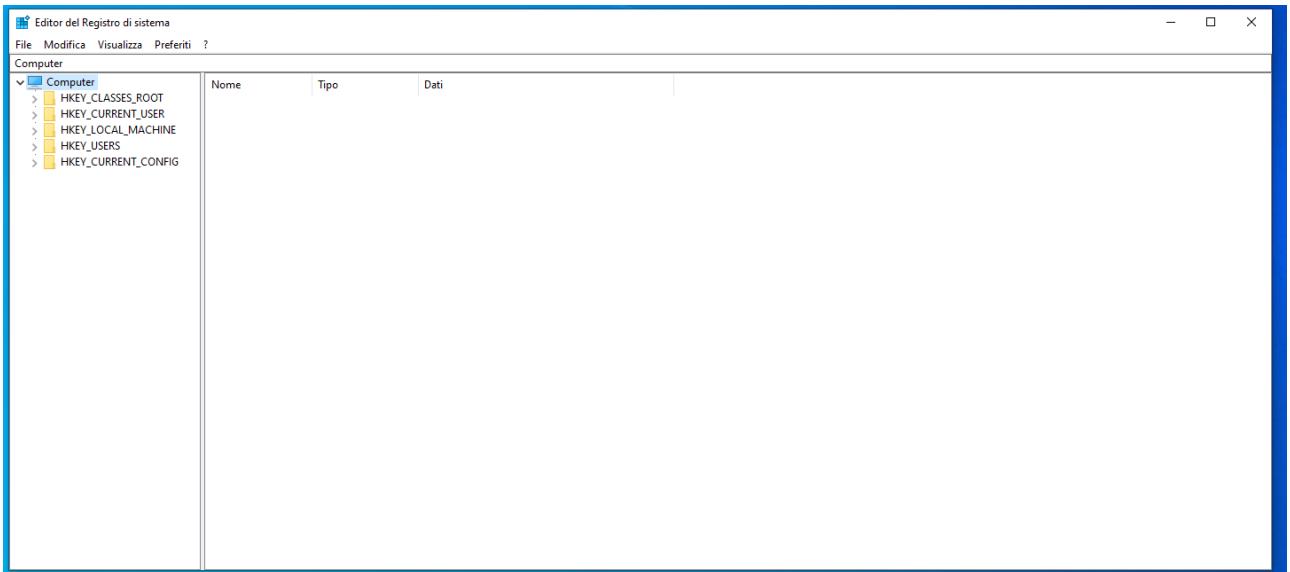
Type	Name
ALPC Port	\BaseNamedObjects\{CoreUI}-PID(3864)-TID(6292)\70621c-e41f-4f79-9074-dcf458679b4
Desktop	\Default
Directory	\KnownDlIs
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	C:\Program Files\Windows Apps\Microsoft.LanguageExperiencePackit-IT_19041.80.274.0_neutral__8wekyb3d8bbwe\Windows\System32\it-IT\Conhost.exe.mui
File	\Device\CNG
File	\Device\DeviceApi
File	C:\Windows\System32\it-IT\propsys.dll.mui
File	C:\Program Files\Windows Apps\Microsoft.LanguageExperiencePackit-IT_19041.80.274.0_neutral__8wekyb3d8bbwe\Windows\System32\it-IT\user32.dll.mui
File	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.1110_none_60b525417f9507e
File	C:\Windows\StaticCache.dat
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU\Software\Classes\Local Settings
Key	HKCU
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

### A cosa puntano gli handle?

- Gli Handle puntano a risorse gestite dal sistema operativo come file, chiavi di registro, sezioni di memoria e threads

## 6. Si accede al registro di Window attraverso Regedit.

In **HKEY\_CURRENT\_USER** si seleziona Process Explorer e si individua la chiave **EulaAccepted**



Il valore 1 indica che l'EULA è stato accettato dall'utente.

Si modifica il parametro da 1 a 0

EulaAccepted REG\_DWORD 0x00000000 (0)

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

- Il valore del registro nella colonna Data si modifica **da 0x00000000(1) a 0x000000000 (0)**

Quando apri Process Explorer, cosa vedi?

- Quando si riapre Process Explorer ricompare la sezione per accettare i termini di utilizzo.

