

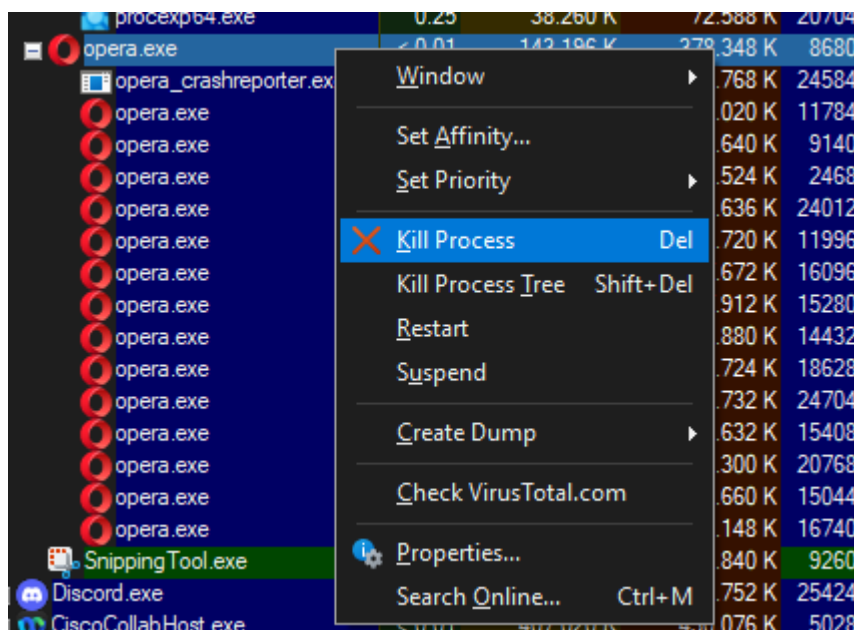
Esercizio L11S1

Parte 1

1. Kill processo attivo

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

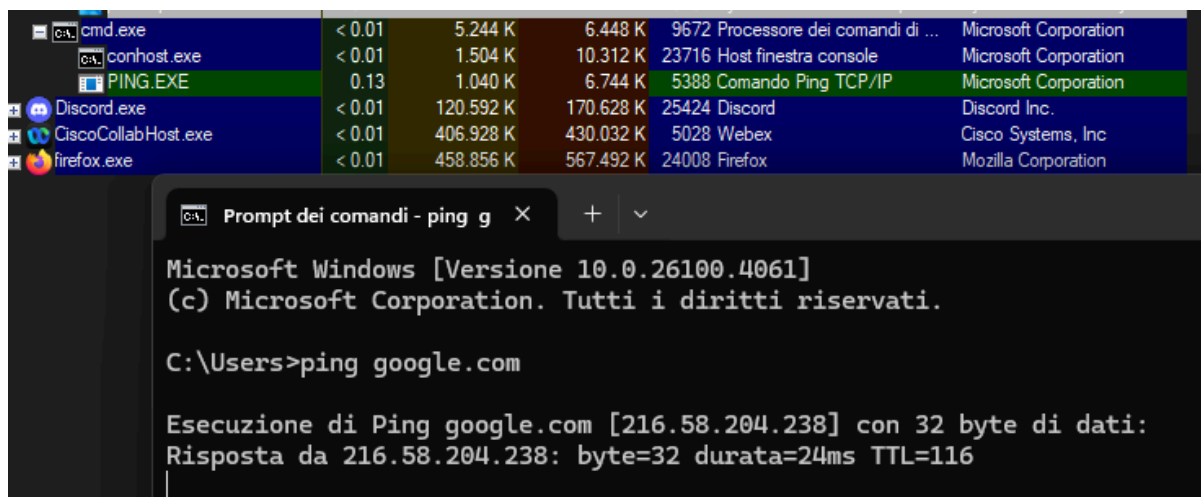
Selezionando "Kill Process" il processo selezionato verrà terminato dall'utente.



2. cmd

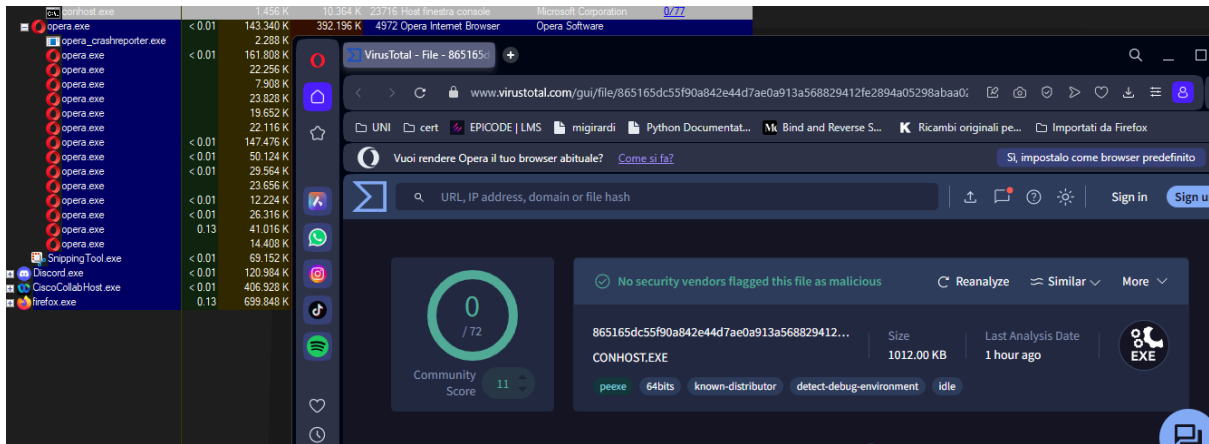
A. Cosa è successo durante il processo ping?

È apparso temporaneamente un nuovo processo figlio **PING.EXE** sotto **cmd.exe** durante l'esecuzione del comando.



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

Il processo figlio **conhost.exe** è stato terminato automaticamente insieme al processo genitore **cmd.exe**.



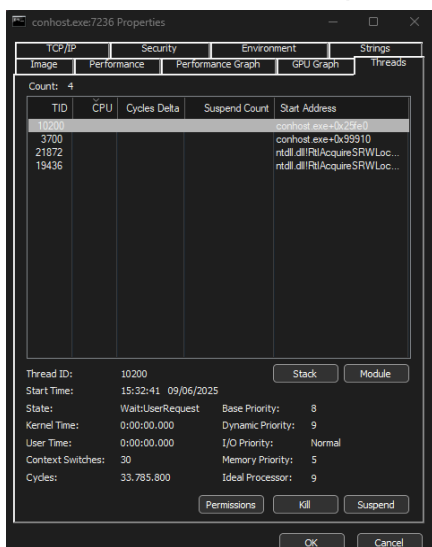
Parte 2

1. Esplorazione Threads e Handle

A. Che tipo di informazioni sono disponibili nella finestra Proprietà?

In questa schermata sono presenti:

- ID del Thread
- Start Time
- Stato del Thread
- Proprietà del Thread
- Proprietà dinamiche e memoria



B. Esaminare gli handle. A cosa puntano gli handle?

Gli Handle puntano a:

- Directory
- File
- Chiavi di registro
- Eventi
- Thread
- Processi
- Mutanti (Mutant)
- Semafori (Semaphore)

Handles		DLLs	Threads
Type	Name		
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\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	HKCR\PackagedCom\InterfaceIndex		
Mutant	\Sessions\14\BaseNamedObjects\SM0:7236:304:WinStaging_02		
Mutant	\Sessions\14\BaseNamedObjects\SM0:7236:120:WinError_03		
Section	\BaseNamedObjects__ComCatalogCache__		
Section	\BaseNamedObjects__ComCatalogCache__		
Semaphore	\Sessions\14\BaseNamedObjects\SM0:7236:304:WinStaging_02_p0		
Semaphore	\Sessions\14\BaseNamedObjects\SM0:7236:304:WinStaging_02_p0h		
Semaphore	\Sessions\14\BaseNamedObjects\SM0:7236:120:WinError_03_p0		
Semaphore	\Sessions\14\BaseNamedObjects\SM0:7236:120:WinError_03_p0h		
Thread	conhost.exe(7236): 3700		
Thread	conhost.exe(7236): 10200		
Thread	conhost.exe(7236): 10200		
WindowStation	\Sessions\14\Windows\WindowStations\WinSta0		
WindowStation	\Sessions\14\Windows\WindowStations\WinSta0		

2. Esplorazione del Registro Windows

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

Il valore di EulaAccepted impostato da 1 a 0

EulaAccepted REG_DWORD 0x00000001 (1)

Modifica valore DWORD (32 bit)

Nome valore:
EulaAccepted

Dati valore:
0

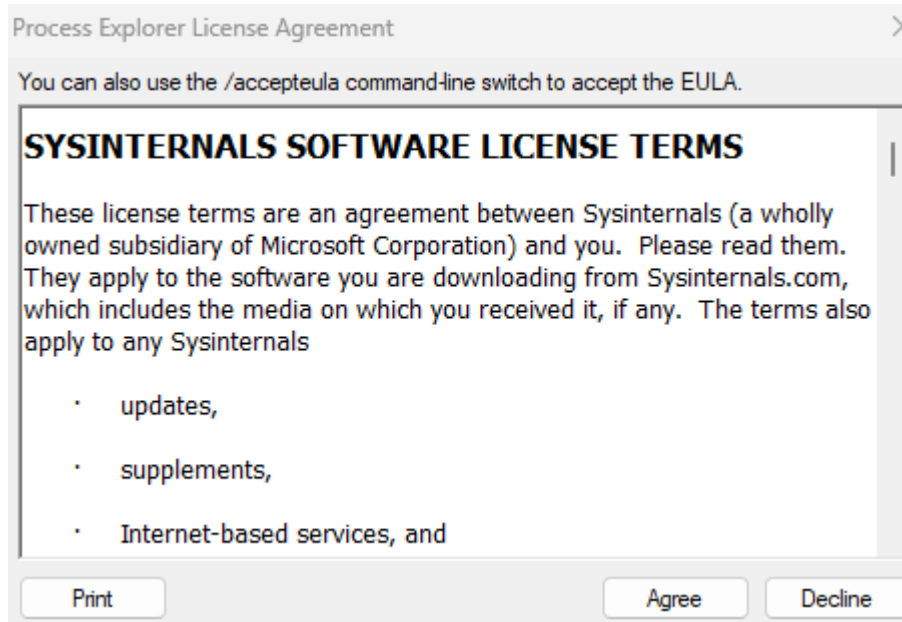
Base
☒ Esadecimale
☐ Decimale

OK Annulla

EulaAccepted REG_DWORD 0x00000000 (0)

B. Quando apri Process Explorer, cosa vedi?

Appare nuovamente la finestra dell'Accordo di Licenza (**EULA**) perché il valore nel registro è stato reimpostato a 0, indicando che l'**EULA** non è più considerato accettato.



3. Conclusioni

L'uso di Process Explorer ha rivelato la complessa gerarchia dei processi e la loro interdipendenza, mentre l'analisi di thread e handle ha mostrato come Windows gestisce l'esecuzione parallela e l'accesso alle risorse di sistema.

La modifica del registro ha dimostrato quanto sia centrale questo database nella configurazione del comportamento delle applicazioni, con effetti immediati e visibili.

L'esperienza di terminare processi e osservare le conseguenze sui processi figli ha evidenziato l'importanza di comprendere queste relazioni per una gestione sicura del sistema.