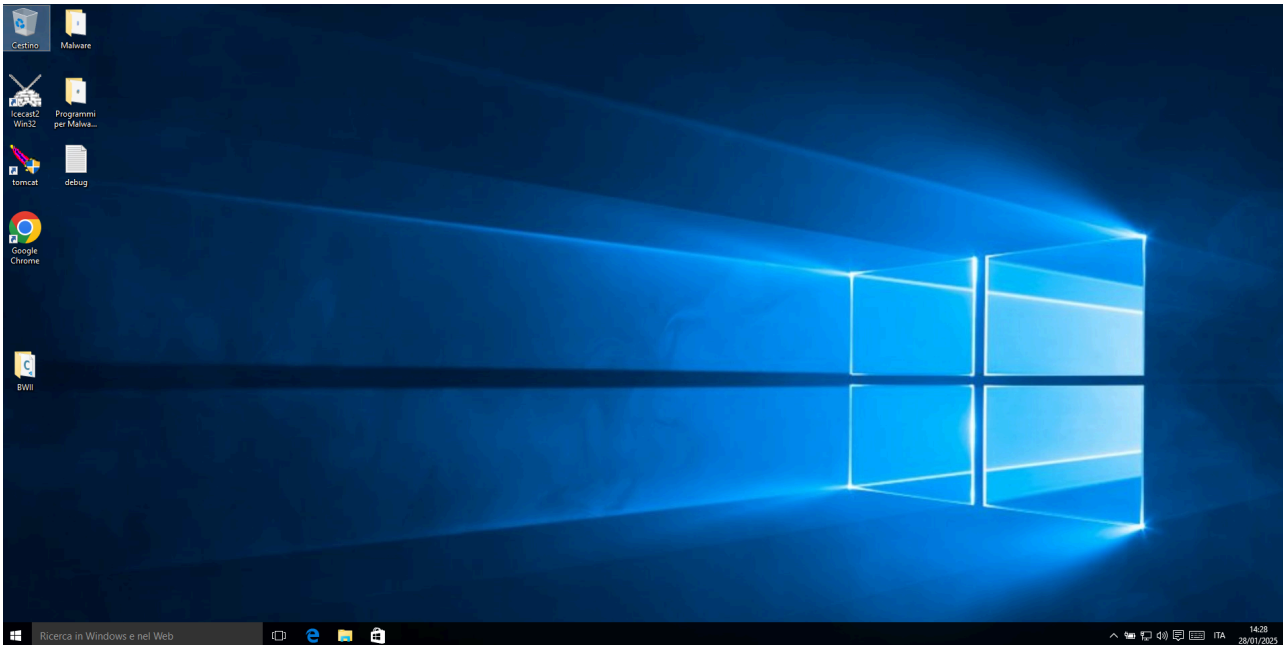
S11L2 - Esplorazione di Processi, Thread, Handle e Registro di Windows

Esplorazione di Processi, Thread, Handle e Registro di Windows

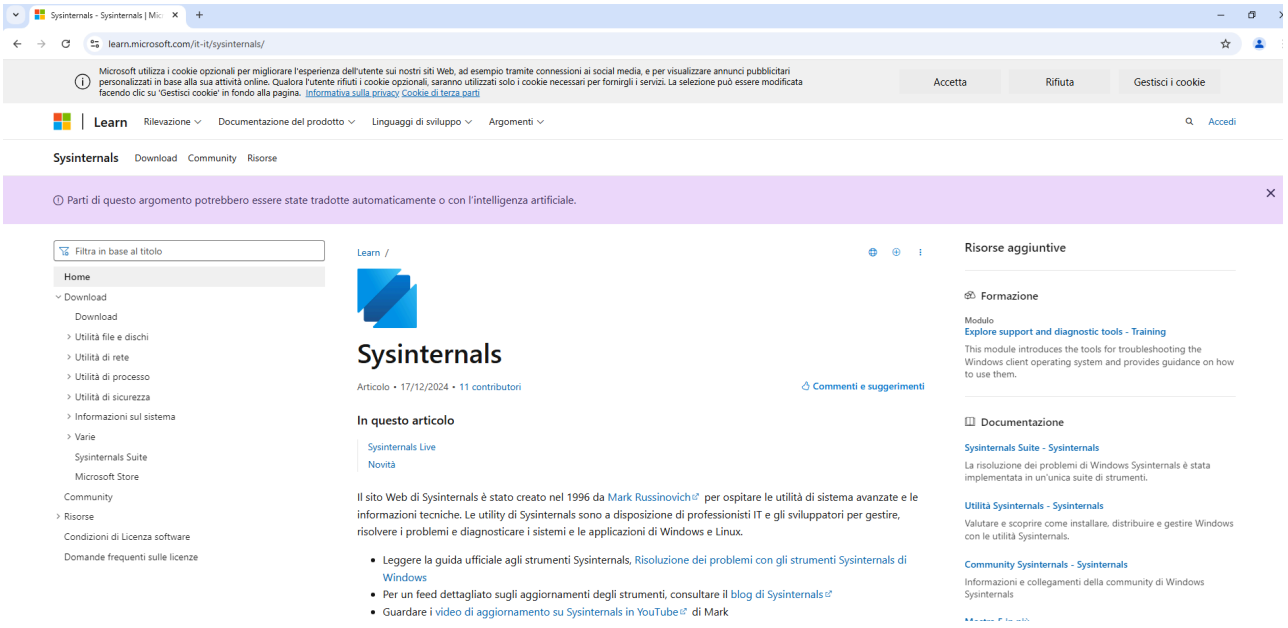
1. Esplorazione di Processi, Thread e Handle con Process Explorer

Passaggi:

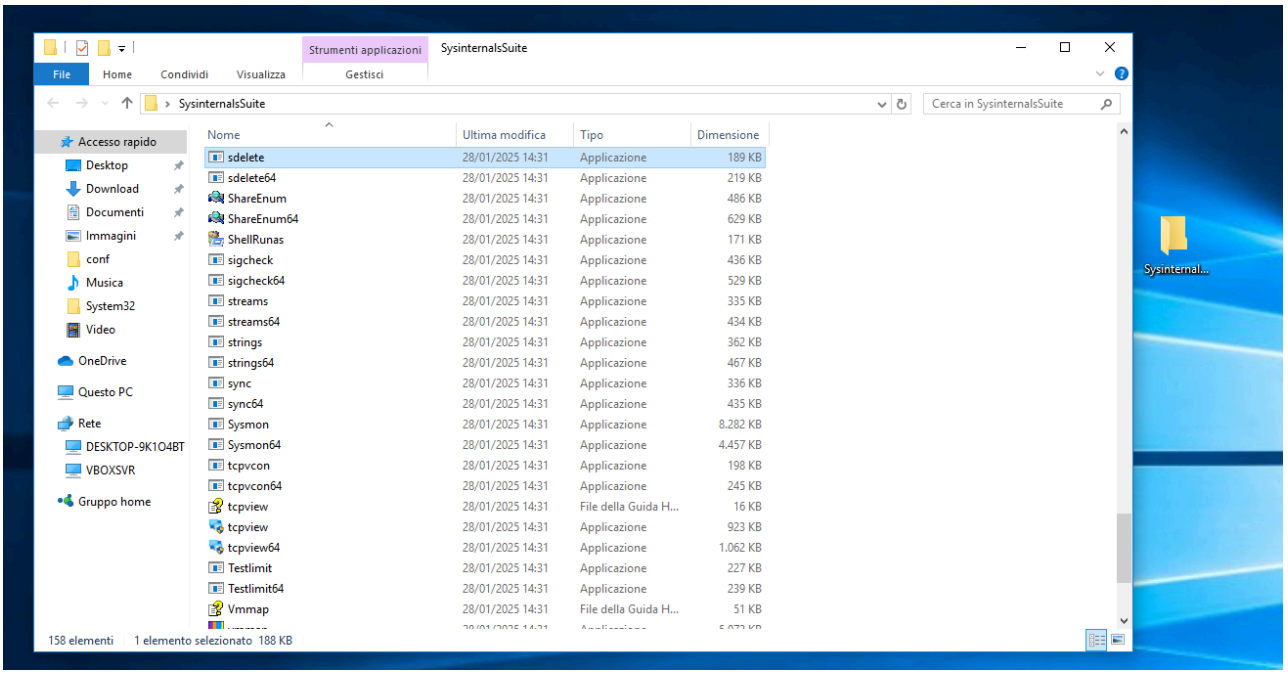
1. **Avvio di Process Explorer**:
   - Ho avviato la macchina virtuale Windows 10.



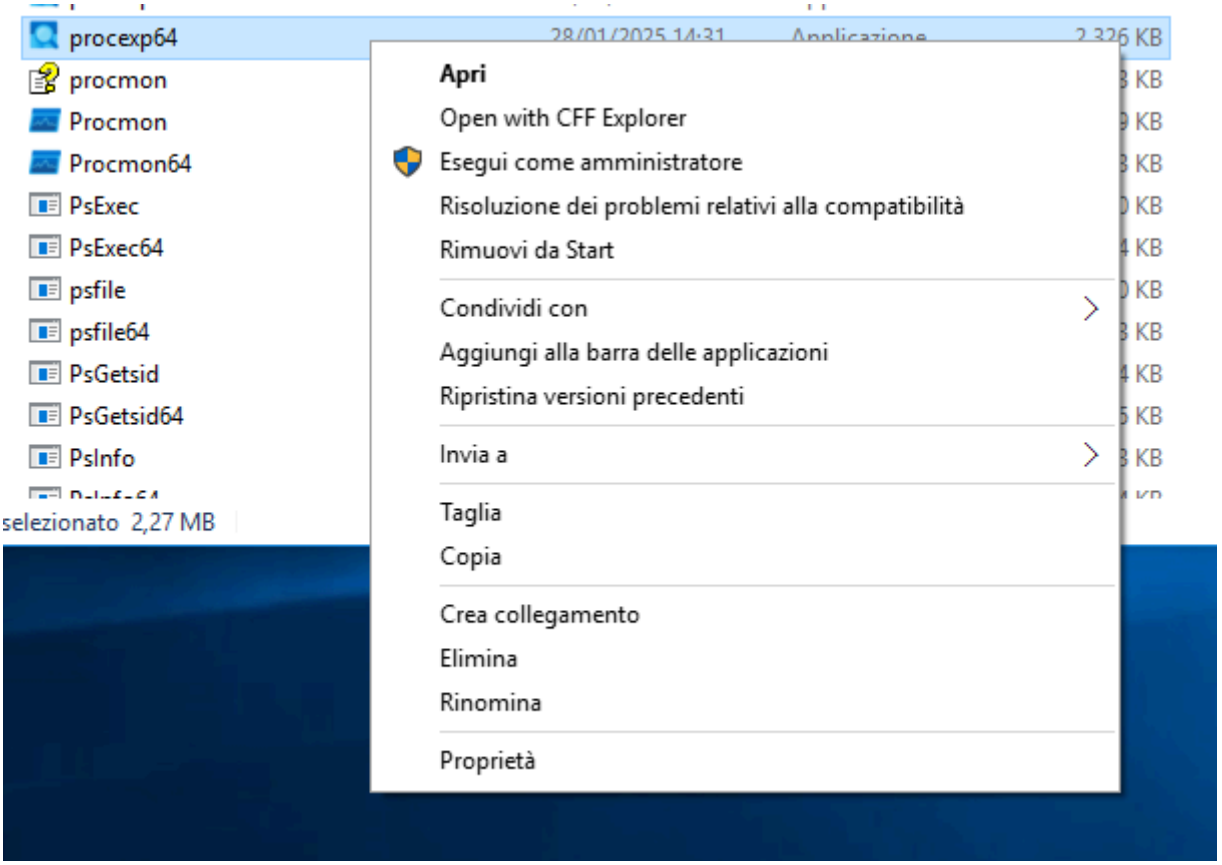
   - Ho scaricato la Sysinternals Suite (dato che non era già installata) da https://learn.microsoft.com/sysinternals.



- Ho estratto il file .zip

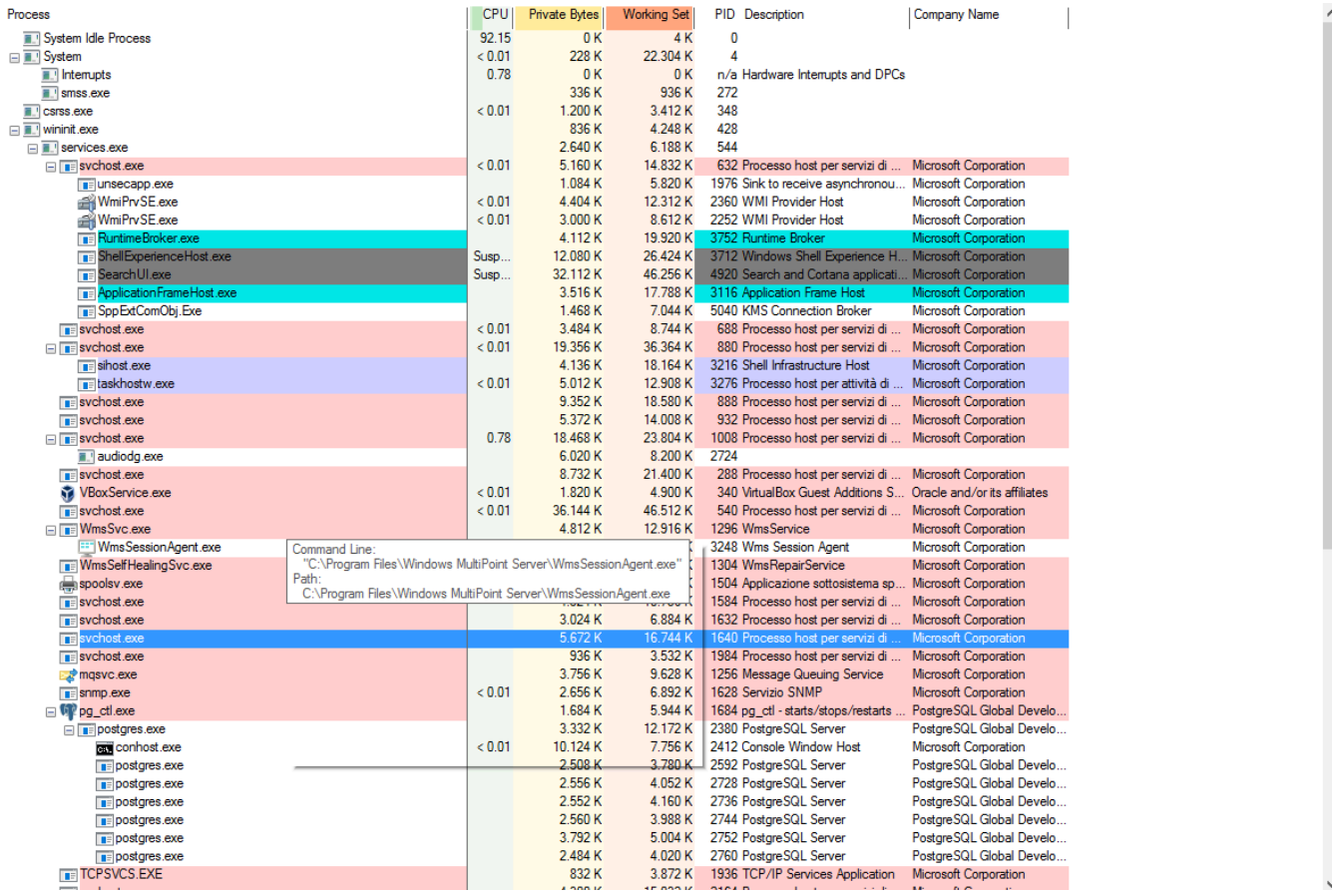


- Ho eseguito Process Explorer con privilegi di amministratore.

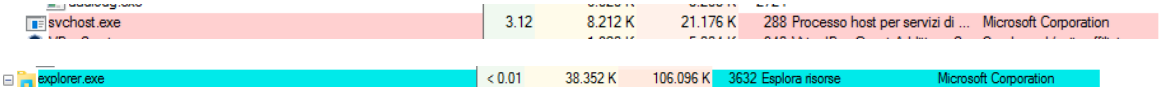


2. **Esplorazione dei Processi**:

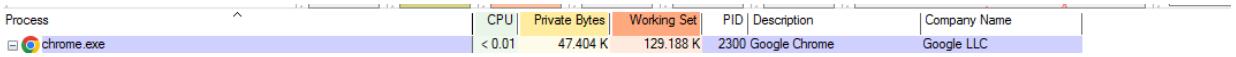
- Ho analizzato l'elenco dei processi attivi.



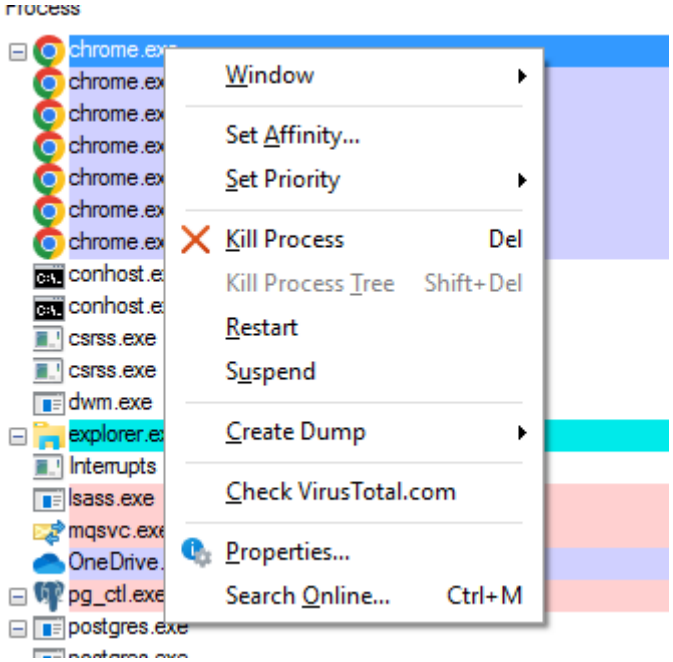
- Ho identificato i processi principali (ad esempio `explorer.exe`, `svchost.exe`).



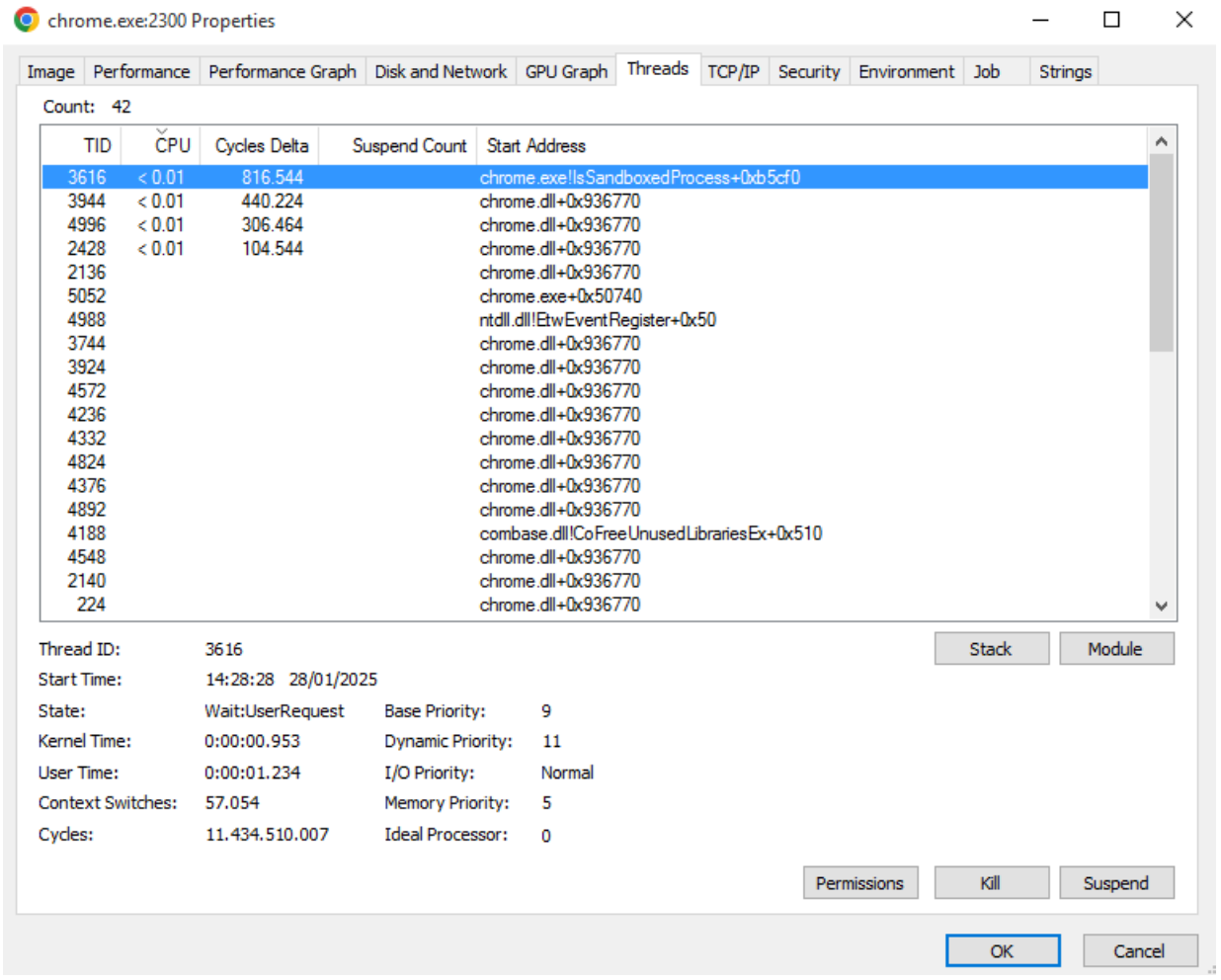
- Per ogni processo, ho osservato:
  - **PID (Process ID)**
  - Utilizzo della CPU e della memoria
  - Percorso eseguibile.



3. **Esplorazione dei Thread**:
   - Ho fatto clic destro su un processo (ad esempio `chrome.exe`, se aperto) e selezionato Properties.

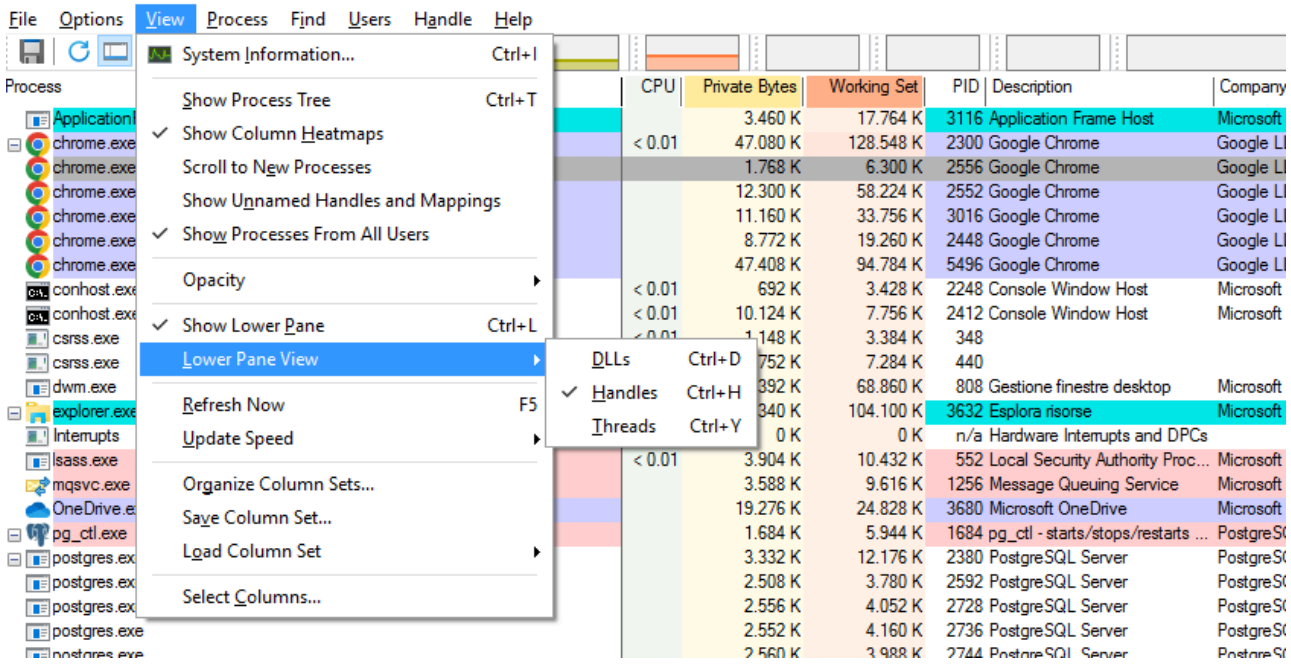


- Nella scheda **Threads**, ho:
  - Identificato i thread attivi.
  - Annotato il loro stato e i moduli associati.

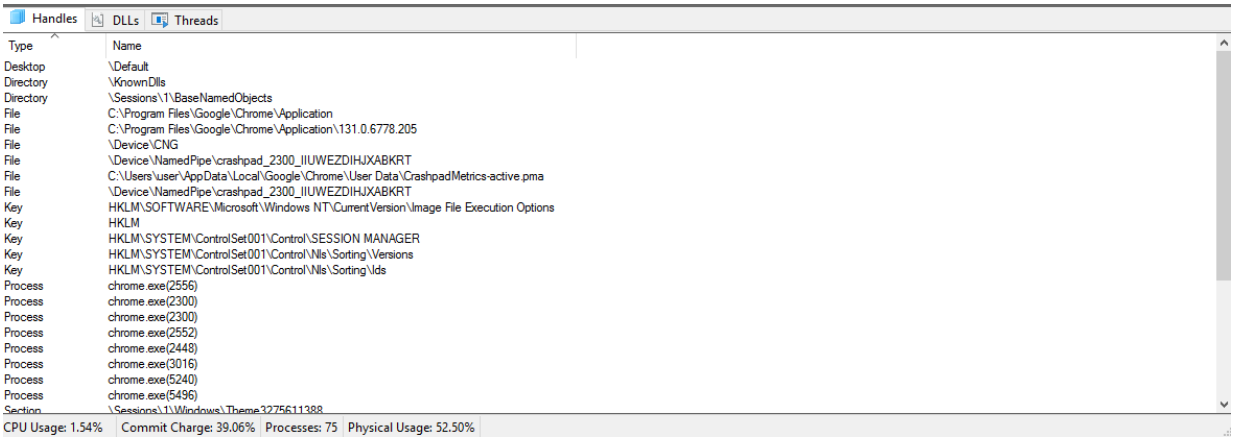


4. **Esplorazione degli Handle**:
   - Sono tornato su **Sysinternals Suite**.

- Nella scheda **View** ho abilitato la visualizzazione degli **Handles** da **Lower Pane View**



- Poi ho:
  - Identificato le risorse aperte (file, chiavi di registro, ecc.).
  - Notato eventuali handle sospetti o non necessari.

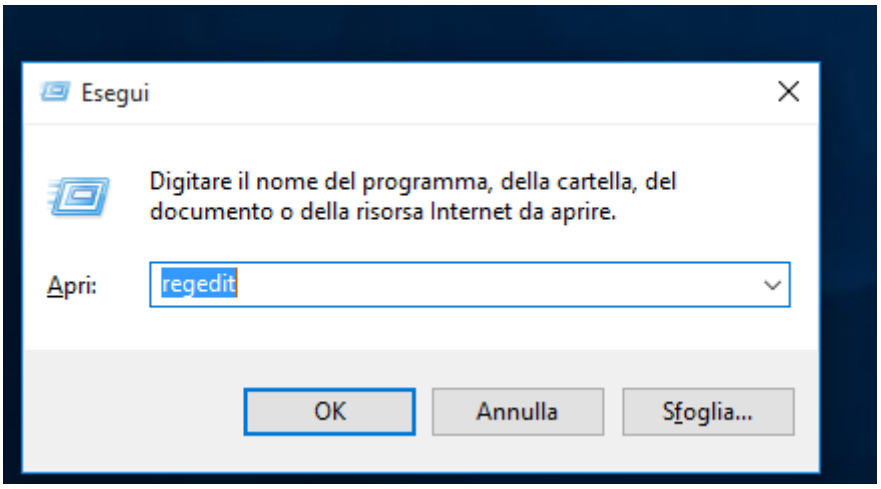


---

2. Modifica di un'Impostazione nel Registro di Windows

Passaggi:

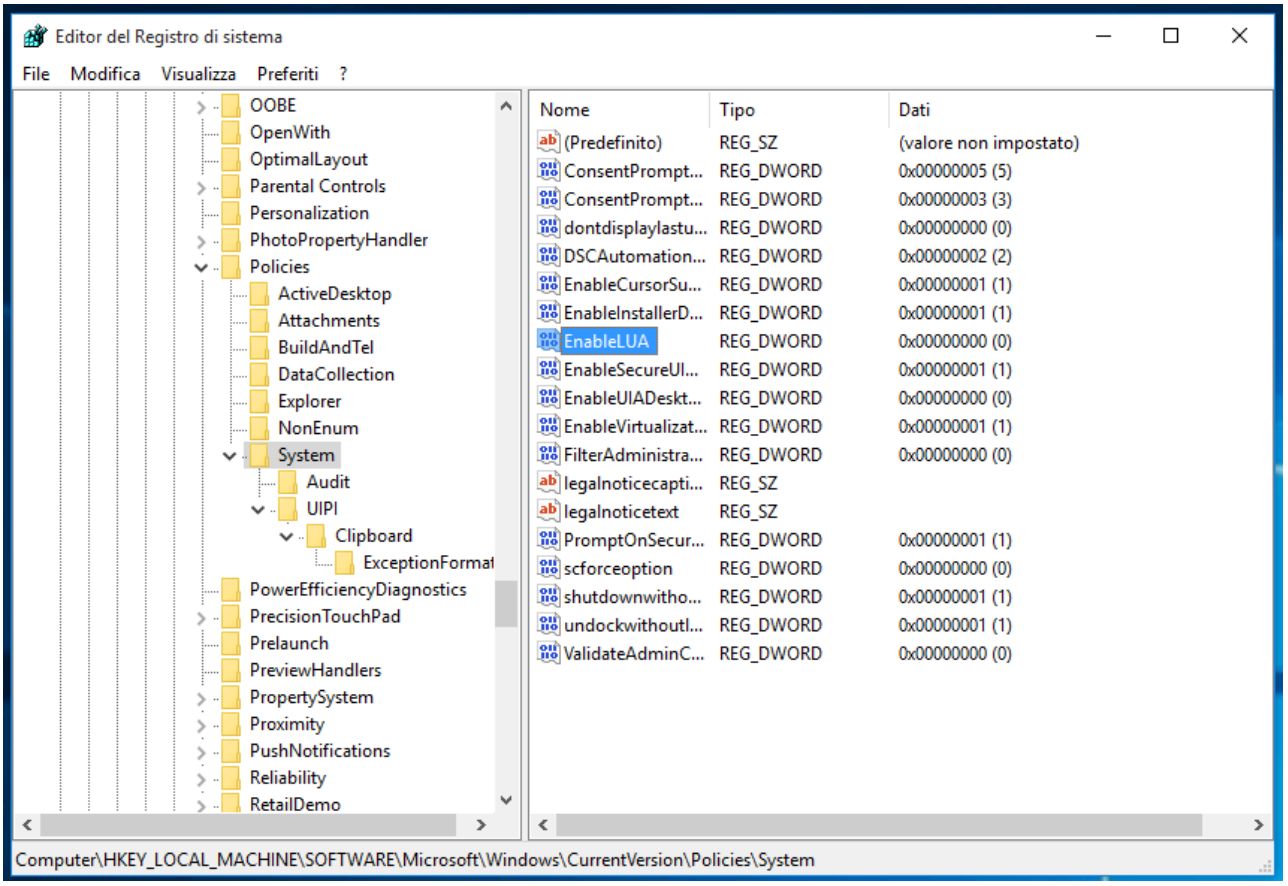
1. **Accesso al Registro di Windows**:
   - Nella macchina `Windows 10`, ho aperto il **Registry Editor** premendo `Win + R`, digitando `regedit` e premendo Invio.



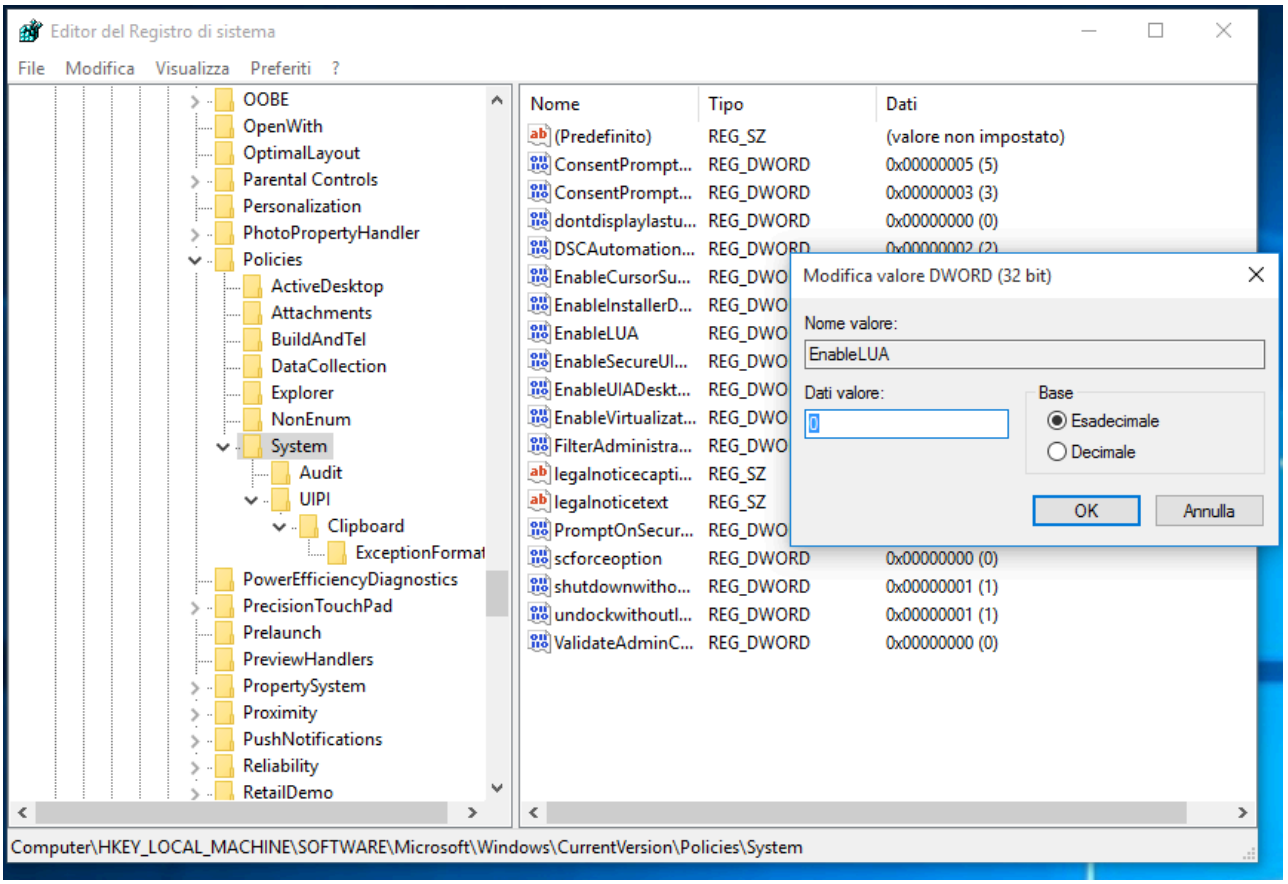
2. **Individuazione della Chiave da Modificare**:
   - Ho navigato fino alla chiave:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

3. **Modifica dell'Impostazione**:
   - Ho trovato il valore `EnableLUA` (controllando che esistesse).

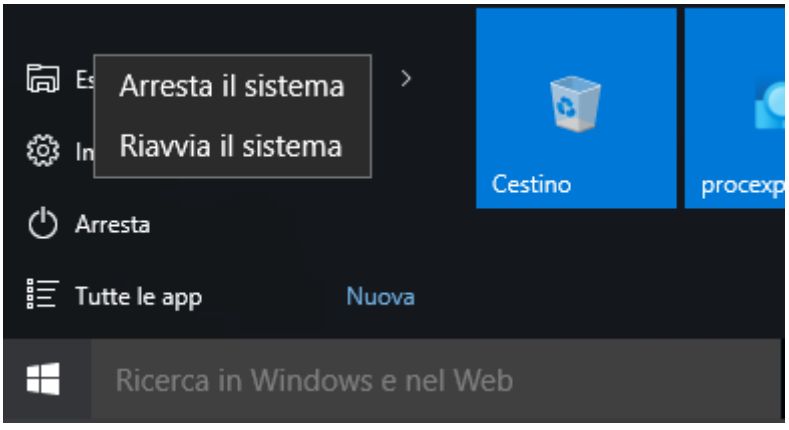


   - Ho modificato il valore da `1` (abilitato) a `0` (disabilitato) per disabilitare il Controllo dell'Account Utente (UAC).



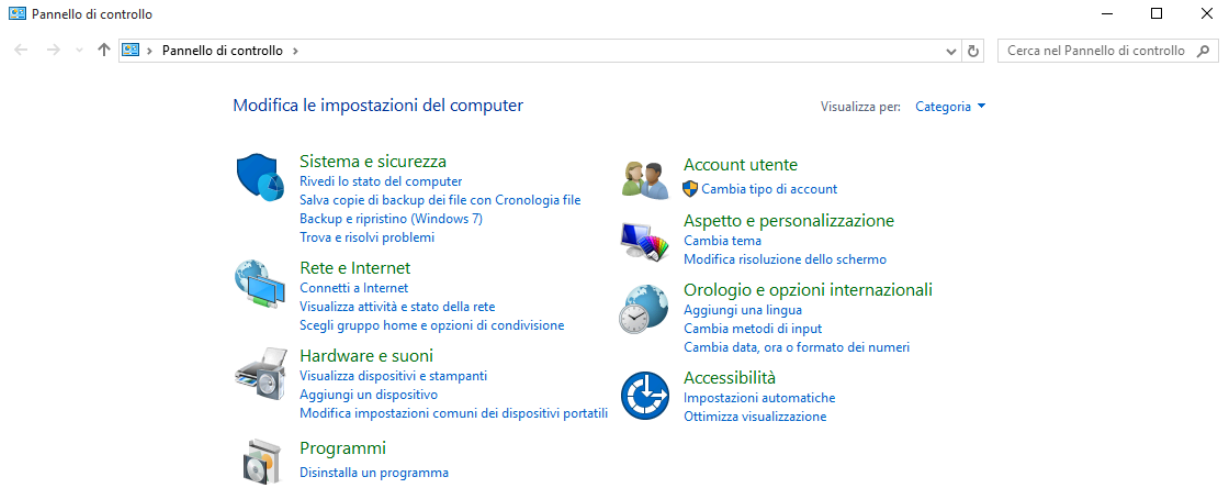
- Ho cliccato su OK per salvare la modifica.

4. **Verifica dell’Effetto della Modifica**:
   - Ho riavviato la macchina virtuale (se richiesto).

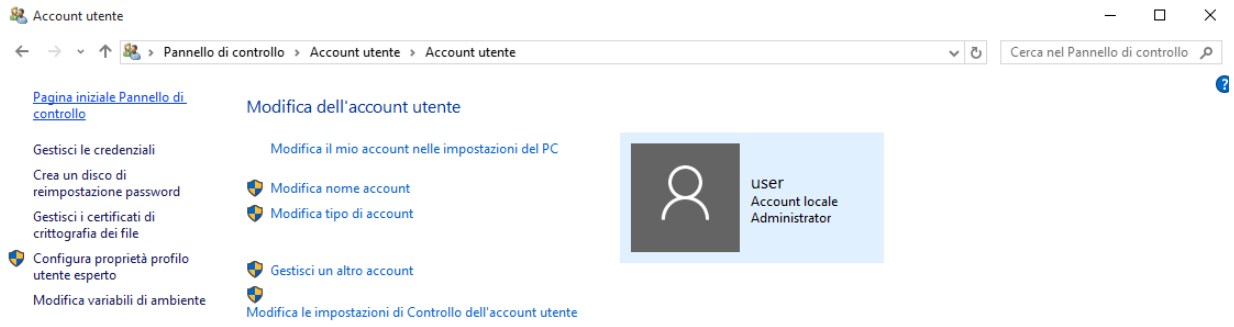


   - Ho verificato che l’UAC fosse stato disabilitato (nel Pannello di controllo).:

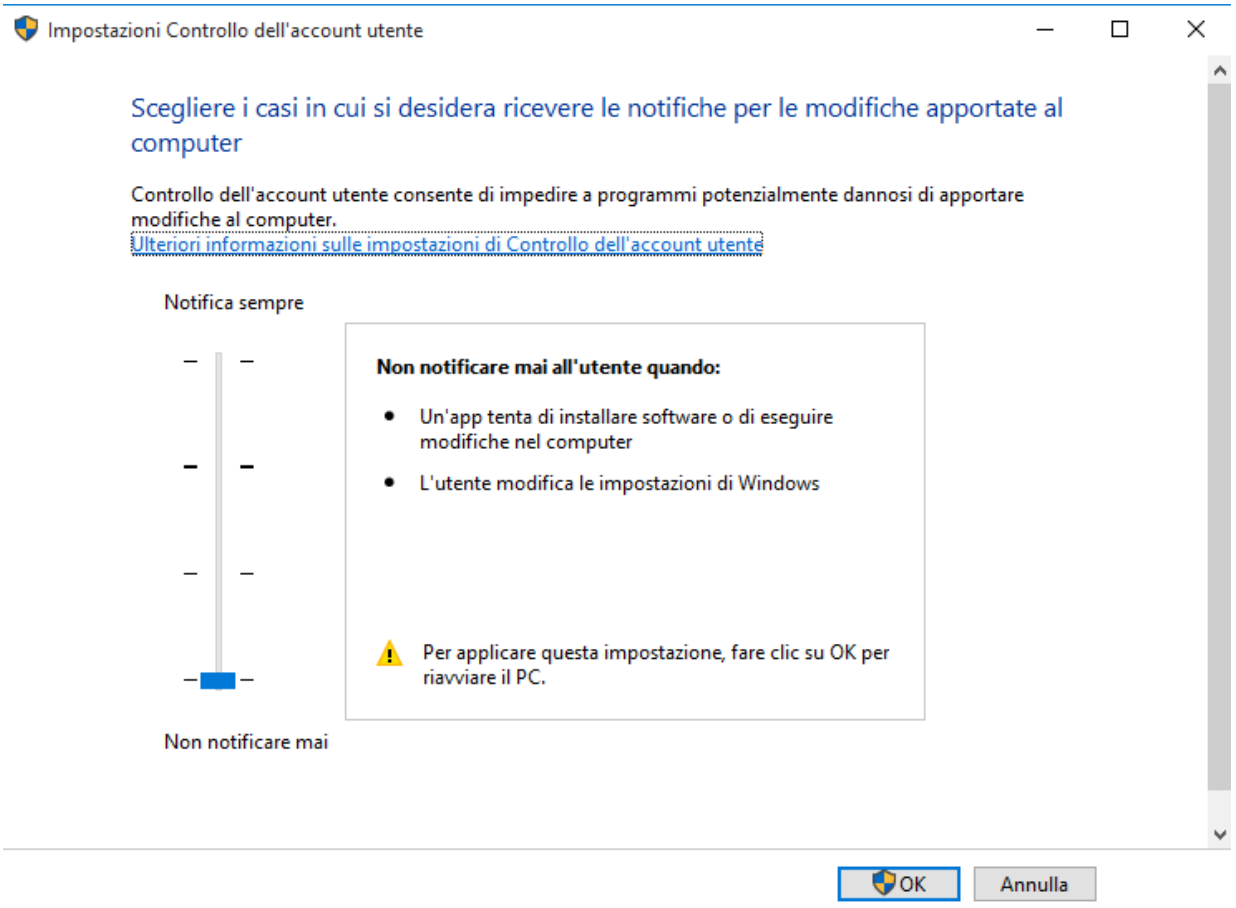
- Ho aperto il **Pannello di controllo**.



- Sono andata su **Account utente** > **Modifica le impostazioni di Controllo dell'account utente**.



- Ho verificato che la barra fosse completamente abbassata su **Non notificare mai**, confermando che l'UAC era disabilitato.



Nota: Al termine, ho ripristinato il valore originale (`1`) per motivi di sicurezza.