

Laboratori giorno 1 – Cisco CyberOps

In questo esercizio abbiamo svolto 3 attività:

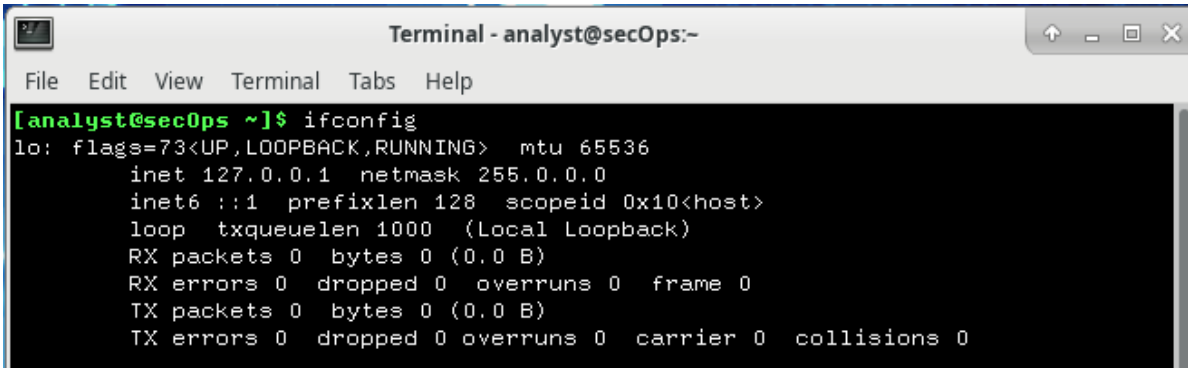
- Sistemato l'interfaccia di rete su una vecchia vm basata su arch
- Analizzato processi, threads e handles su Windows
- Cambiato un'impostazione di sistema tramite registro di sistema di Windows

VM Cyberops

Questa vm è basata su una vecchia versione di arch linux con desktop xfce.

La vm non riesce ad accedere ad internet. Di conseguenza procediamo con i primi controlli.

Con `ifconfig` notiamo che è presente solo l'interfaccia di loopback.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Con `ip addr` possiamo vedere tutte le interfacce di rete. Notiamo che c'è un'altra interfaccia di rete denominata `ens35` che però risulta spenta (`state DOWN`).

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
3: ens35: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000  
    link/ether 00:0c:29:8a:51:c4 brd ff:ff:ff:ff:ff:ff  
[analyst@secOps ~]$
```

In questa versione di linux, non troviamo le impostazioni GUI per la rete. Dobbiamo per forza cambiare le impostazioni da terminale.

Il file di configurazione della rete non si trova nella solita directory `/etc/network`, bensì nella directory `/etc/systemd/network`.

All'interno di questa directory c'è il file di configurazione `25-wired.network`, apriamolo con il comando `nano`.

Il nome dell'interfaccia di rete è errato. Inseriamo il nome dell'interfaccia di rete corretto (in questo caso `ens35`) e lasciamo come impostazione il `dhcp ipv4`.

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
GNU nano 2.9.5 /etc/systemd/network/25-wired.network  
[Match]  
Name=ens35  
  
[Network]  
DHCP=ipv4
```

Per ultima cosa dobbiamo abilitare l'interfaccia di rete. Abilitiamola con il comando `sudo ip link set ens35 up`.

Verifichiamo che l'interfaccia di rete sia attiva con il comando `ip addr`.

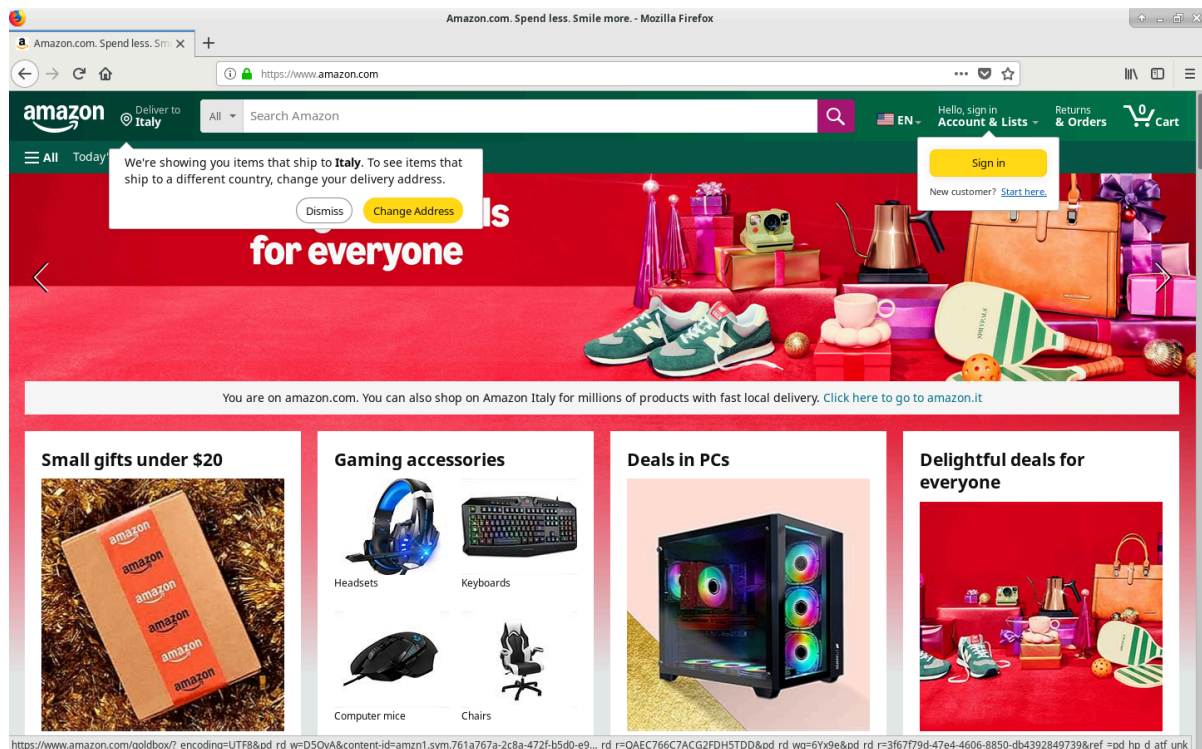
```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo ip link set ens35 up
[analyst@secOps ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
3: ens35: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:8a:51:c4 brd ff:ff:ff:ff:ff:ff
    inet6 fd00::20c:29ff:fe8a:51c4/64 scope global dynamic mngtmpaddr
        valid_lft 7198sec preferred_lft 3598sec
    inet6 fe80::20c:29ff:fe8a:51c4/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

Riavviamo la macchina con `sudo reboot`, dopodiché con `ifconfig` vediamo se l'interfaccia di rete è stata configurata con successo.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ ifconfig
ens35: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.24 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fd00::20c:29ff:fe8a:51c4 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::20c:29ff:fe8a:51c4 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:8a:51:c4 txqueuelen 1000 (Ethernet)
    RX packets 47 bytes 4153 (4.0 KiB)
    RX errors 0 dropped 38 overruns 0 frame 0
    TX packets 14 bytes 1720 (1.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[analyst@secOps ~]$
```

Facciamo la prova del nove caricando una pagina sul browser. Poi spegniamo la macchina con `sudo shutdown`.

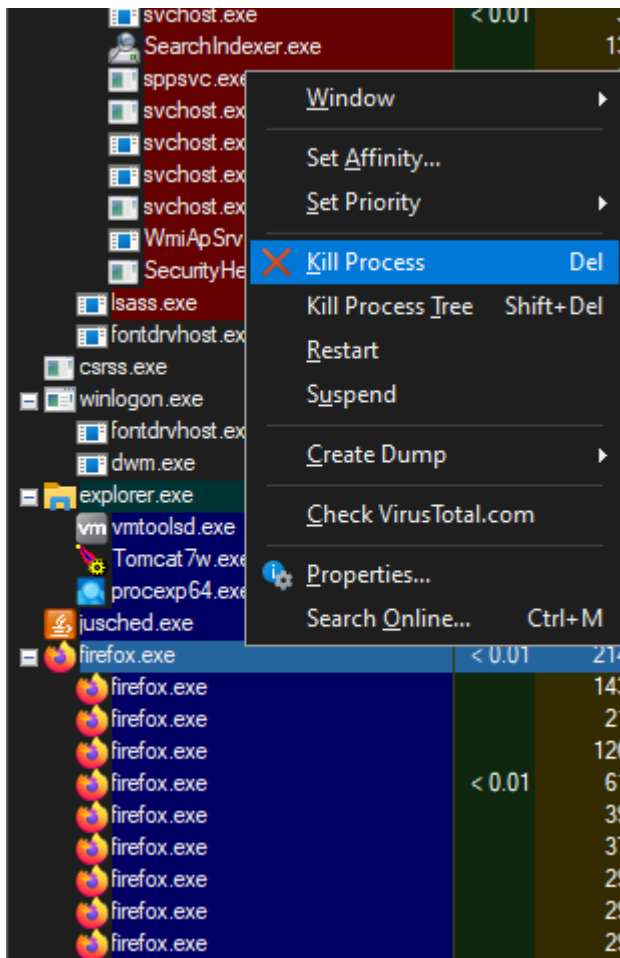


Process Explorer

Per prima cosa, apriamo un'applicazione da monitorare tramite process explorer. Apriamo ad esempio Firefox.

firefox.exe	< 0.01	235.296 K	316.972 K	492 Firefox	Mozilla Corporation
firefox.exe		143.440 K	52.684 K	5704 Firefox	Mozilla Corporation
firefox.exe		21.360 K	15.588 K	5316 Firefox	Mozilla Corporation
firefox.exe	< 0.01	110.124 K	122.448 K	4016 Firefox	Mozilla Corporation
firefox.exe	< 0.01	60.028 K	84.084 K	5364 Firefox	Mozilla Corporation
firefox.exe		39.412 K	20.304 K	5424 Firefox	Mozilla Corporation
firefox.exe		37.584 K	14.588 K	5500 Firefox	Mozilla Corporation
firefox.exe		29.468 K	29.796 K	5264 Firefox	Mozilla Corporation
firefox.exe		29.632 K	29.848 K	764 Firefox	Mozilla Corporation
firefox.exe		29.488 K	29.816 K	5468 Firefox	Mozilla Corporation

Tramite process explorer possiamo eseguire numerose azioni. Possiamo ad esempio terminare il processo.



Ora esploriamo i processi figli. Per praticità, apriamo il cmd ed eseguiamo un ping. Nel momento in cui eseguiamo il ping, verrà creato un processo figlio **PING.EXE**.

C:\cmd.exe	2.076 K	4.080 K	5632 Processore dei comandi di Windows	Microsoft Corporation
C:\conhost.exe	6.568 K	15.456 K	400 Host finestra console	Microsoft Corporation

svchost.exe	< 0.01	3.384 K	11.065 K	2436 Processore host per servizi di Windows	Microsoft Corporation
svchost.exe		7.120 K	34.044 K	3050 Processore host per servizi di Windows	Microsoft Corporation
svchost.exe		1.704 K	7.512 K	2808 Processore host per servizi di Windows	Microsoft Corporation
SearchIndexer.exe	< 0.01	3.540 K	21.212 K	3624 Processore host per servizi di Windows	Microsoft Corporation
sppsvc.exe		15.588 K	20.064 K	3848 Microsoft Windows Search Indexer	Microsoft Corporation
svchost.exe		8.800 K	18.044 K	940	
svchost.exe		4.208 K	17.020 K	3160	
svchost.exe		5.208 K	26.692 K	4536 Processore host per servizi di Windows	Microsoft Corporation
svchost.exe		1.800 K	8.112 K	5460 Processore host per servizi di Windows	Microsoft Corporation
svchost.exe		2.760 K	10.416 K	5820	
SecurityHealthService.exe		1.952 K	9.572 K	2168	
lsass.exe		5.852 K	17.068 K	624 Local Security Authority Process	Microsoft Corporation
fontdrvhost.exe		1.492 K	4.152 K	744 Usemode Font Driver Host	Microsoft Corporation
csrss.exe	< 0.01	6.924 K	25.952 K	472	
winlogon.exe		3.700 K	11.440 K	536 Applicazione Accesso a Windows	Microsoft Corporation
fontdrvhost.exe		3.468 K	8.200 K	752 Usemode Font Driver Host	Microsoft Corporation
dwm.exe	< 0.01	52.520 K	79.784 K	980 Gestione finestre desktop	Microsoft Corporation
explorer.exe	< 0.01	59.728 K	127.904 K	3424 Esplora risorse	Microsoft Corporation
vmtoolsd.exe	< 0.01	25.460 K	50.244 K	4584 VMware Tools Core Service	VMware, Inc.
Tomcat7w.exe	< 0.01	1.592 K	8.104 K	4664 Commons Daemon Service Manager	Apache Software Foundati...
cmd.exe	< 0.01	2.076 K	4.080 K	5632 Processore dei comandi di Windows	Microsoft Corporation
conhost.exe	< 0.01	6.540 K	15.776 K	1688 Host finestra console	Microsoft Corporation
PING.EXE	< 0.01	860 K	3.704 K	2352 Comando Ping TCP/IP	Microsoft Corporation

Amministratore: C:\Windows\system32\cmd.exe

Microsoft windows [Versione 10.0.19045.4651]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

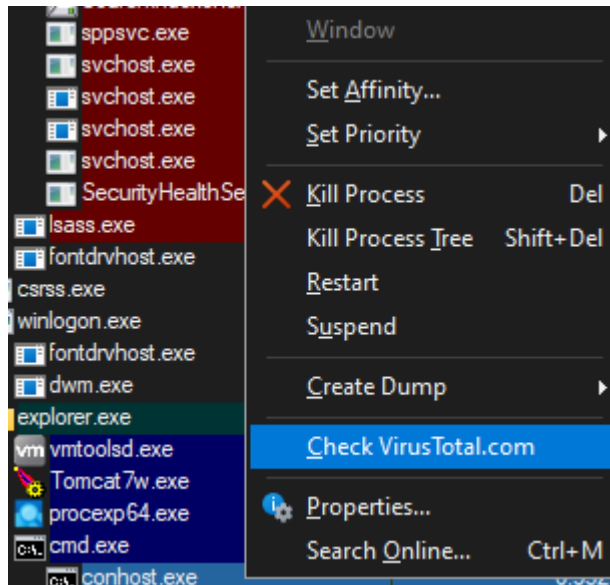
C:\Users\Admin>ping 192.168.1.1

Esecuzione di Ping 192.168.1.1 con 32 byte di dati:
Risposta da 192.168.1.1: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.1: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.1: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.1.1:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Users\Admin>

Process explorer ci permette anche di verificare se un processo è malevolo. Basta fare tasto destro sul processo interessato e clicchiamo su check VirusTotal.com



Process explorer calcolerà l'hash dell'eseguibile responsabile del processo e invierà l'hash a VirusTotal.

Dentro Process explorer possiamo visualizzare il risultato (0/76). Risulta quindi essere un processo innoquo.

firefox.exe	< 0.01	209.092 K	284.580 K	5308	Firefox	Mozilla Corporation	0/76
firefox.exe		126.216 K	50.360 K	5164	Firefox	Mozilla Corporation	0/76
firefox.exe		21.140 K	15.232 K	5652	Firefox	Mozilla Corporation	0/76
firefox.exe	< 0.01	69.808 K	90.332 K	4768	Firefox	Mozilla Corporation	0/76
firefox.exe		155.248 K	155.424 K	3260	Firefox	Mozilla Corporation	0/76
firefox.exe		37.452 K	14.032 K	5400	Firefox	Mozilla Corporation	0/76
firefox.exe		29.228 K	28.812 K	5424	Firefox	Mozilla Corporation	0/76
firefox.exe		29.172 K	28.700 K	4524	Firefox	Mozilla Corporation	0/76
firefox.exe		29.136 K	28.676 K	5616	Firefox	Mozilla Corporation	0/76

Se clicchiamo sul risultato (0/76) ci porterà sulla pagina di VirusTotal con il risultato della scansione.

0

/71

Community Score

4f6606e9a79f2c6f75bf34ce1bf54785713fbe077d37a80d4a9c951948628f19

firefox.exe

peek

signed

overlay

64bits

Size

656.06 KB

Last Analysis Date

44 minutes ago

EXE

Reanalyze

Similar

More

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	AliCloud	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
Bkav Pro	✓ Undetected	ClamAV	✓ Undetected

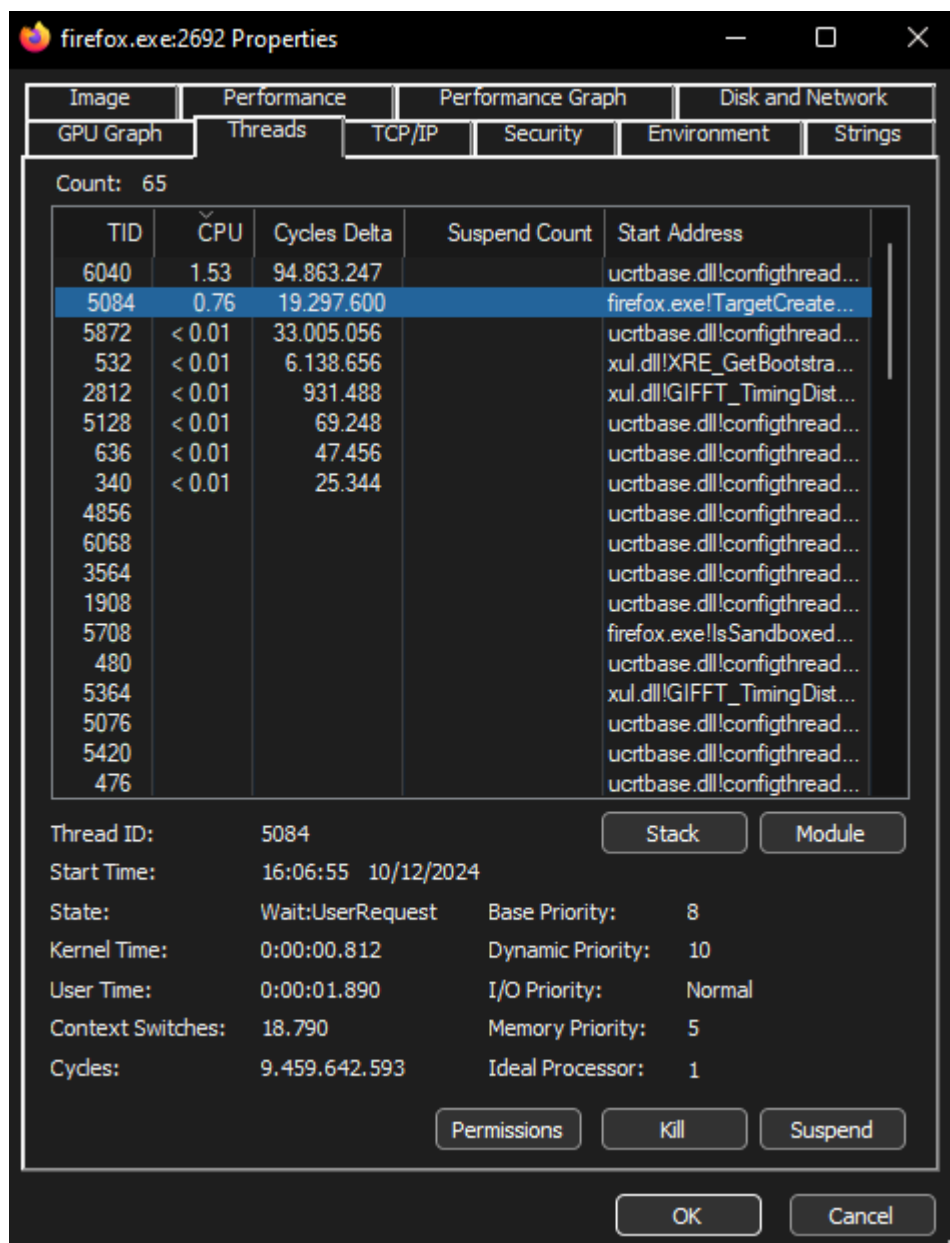
Ora vediamo i Threads. Sempre facendo tasto destro sul processo desiderato, apriamo le proprietà del processo ed entriamo nella scheda Threads.

Un **thread** è la più piccola unità di esecuzione di un programma all'interno di un sistema operativo. È un "filo" di attività che il processore può gestire separatamente, permettendo l'esecuzione parallela o concorrente di più compiti all'interno dello stesso processo.

Nella tabella sotto, sono riportati dettagli su ciascun thread, come il loro ID (TID), l'utilizzo della CPU, il ciclo di attività e l'indirizzo di avvio.

L'indirizzo di avvio, ad esempio, specifica la funzione o il modulo da cui è stato avviato il thread. Ad esempio, nel tuo caso, alcuni thread iniziano da **firefox.exe!...**, mentre altri iniziano da moduli come **ucrtbase.dll**.

Ogni thread è un'unità di esecuzione all'interno del processo Firefox, e possono essere responsabili di diverse operazioni, come il rendering delle pagine, la gestione delle estensioni o le operazioni di rete.



Ora invece vediamo gli handles. Per visualizzarli, clicchiamo su View > Lower Pane View > Handles.

Gli **handles** in Windows sono riferimenti o "puntatori" utilizzati dal sistema operativo per gestire risorse del sistema associate a un processo.

In pratica, un handle è una sorta di "chiave" che un processo usa per accedere e interagire con risorse come file, directory, dispositivi, oggetti di sincronizzazione, memoria condivisa e molto altro.

firefox.exe	< 0.01	164.576 K	251.600 K	2692 Firefox
firefox.exe		162.104 K	76.116 K	5556 Firefox
firefox.exe		21.160 K	15.540 K	4008 Firefox
firefox.exe	< 0.01	56.740 K	80.856 K	3644 Firefox
firefox.exe		85.360 K	98.104 K	4136 Firefox
firefox.exe		37.496 K	14.780 K	1804 Firefox
firefox.exe	< 0.01	193.308 K	219.580 K	5992 Firefox
firefox.exe		54.548 K	74.548 K	3888 Firefox
firefox.exe		29.308 K	28.832 K	6032 Firefox
firefox.exe		29.180 K	28.836 K	1916 Firefox
firefox.exe		29.364 K	28.964 K	4964 Firefox

Type	Name
ALPC Port	\BaseNamedObjects\{CoreUI}-PID(2692)-TID(5084) c3b986dc-edec-498e-9917-ba7878b1...
ALPC Port	\RPC Control\OLE03608B6E73119D1E06E22D4D926F
Desktop	\Default
Desktop	\sbox_altemate_desktop_0xA84
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
Event	\BaseNamedObjects\TermSrvReadyEvent
Event	\KernelObjects\LowMemoryCondition
File	C:\Program Files\Mozilla Firefox
File	C:\Program Files\Mozilla Firefox
File	\Device\KsecDD
File	\Device\KsecDD
File	\Device\CNG
File	C:\Users\Admin\AppData\Local\Mozilla\Firefox\SkeletonUILock-c388d246
File	C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\8cleb19.default-release\paren...
File	C:\Users\Admin\AppData\Local\Mozilla\Firefox\Profiles\8cleb19.default-release\startupCa...
File	C:\ProgramData\Mozilla-1de4eec8-1241-4177-a864-e594e8d1fb38\UpdateLock-308046B...
File	\Device\Nsi
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	C:\Users\Admin\AppData\Local\Mozilla\Firefox\Profiles\8cleb19.default-release\startupCa...

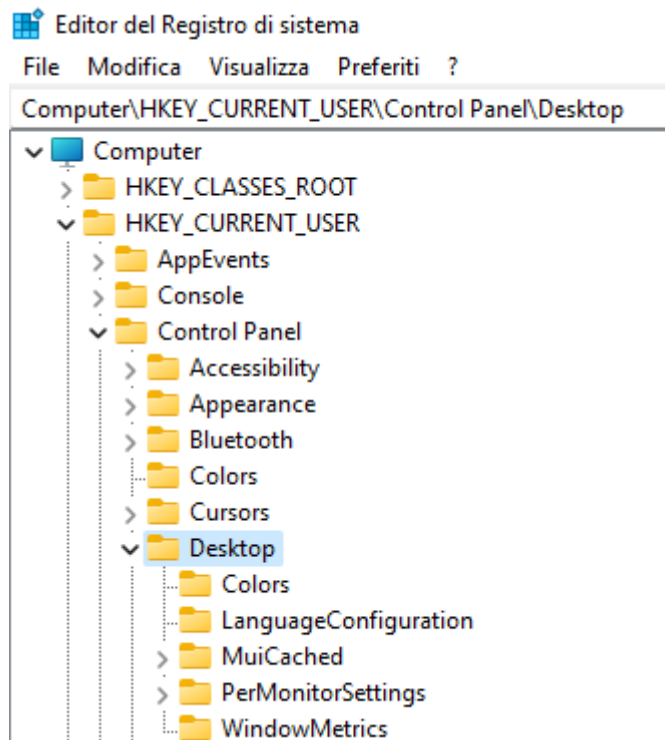
Registro di windows

Il **Registro di Windows** è un database gerarchico utilizzato dal sistema operativo Windows per archiviare configurazioni, impostazioni e informazioni su hardware, software, utenti e preferenze del sistema.

Ogni voce nel registro è organizzata in chiavi e sottochiavi, simili a una struttura di cartelle/sottocartelle/file, e contiene valori che definiscono parametri o impostazioni specifiche.

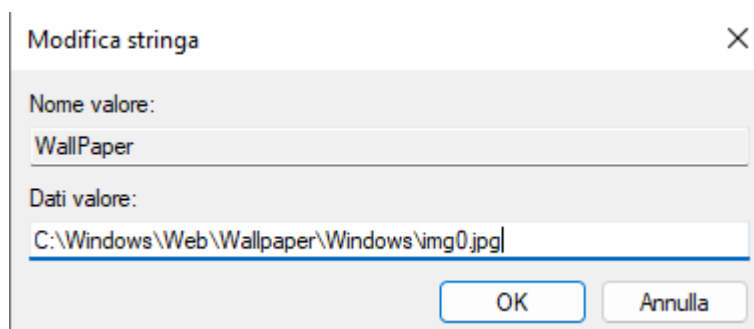
Proviamo ad esempio a cambiare lo sfondo del desktop tramite registro di sistema.

La chiave di registro che tiene memorizzato la posizione del file utilizzato come sfondo si trova in **HKEY_CURRENT_USER\Control Panel\Desktop**.

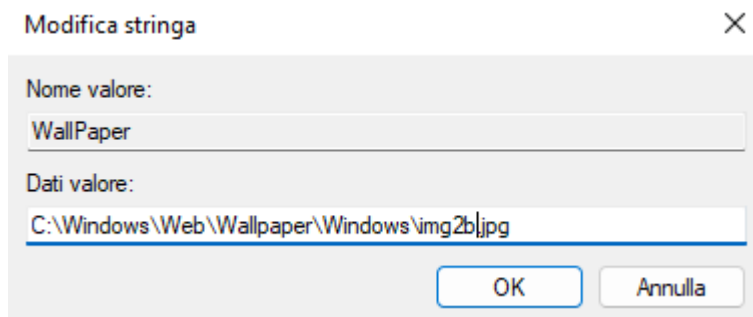
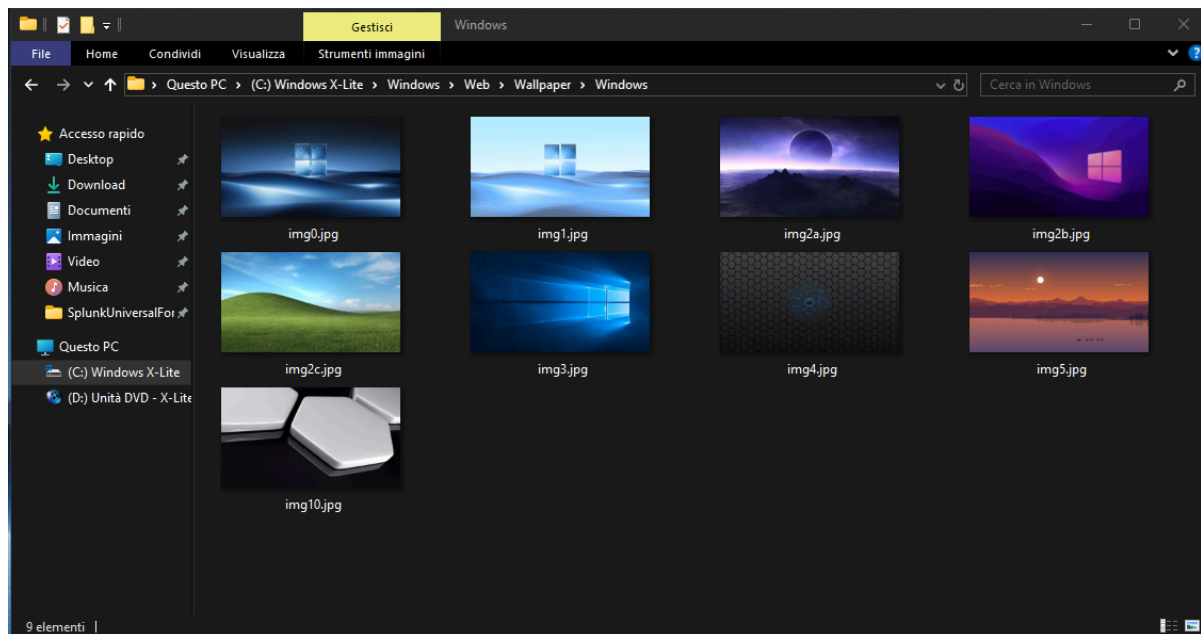


In questa cartella troveremo la chiave **WallPaper**.

UserPreferencesMask	REG_BINARY	90 12 03 80 10 00 00 00
WaitToKillAppTimeout	REG_SZ	2000
WallPaper	REG_SZ	C:\Windows\Web\Wallpaper\Windows\img0.jpg
WallpaperOriginX	REG_DWORD	0x00000000 (0)
WallpaperOriginY	REG_DWORD	0x00000000 (0)



In questo momento è impostato come sfondo `img0.img`. Impostiamo come sfondo `img2b.img` modificando la chiave di registro.



Clicchiamo su OK. Dobbiamo riavviare il computer prima di visualizzare le modifiche apportate. Prima di riavviare:



Dopo il riavvio:

