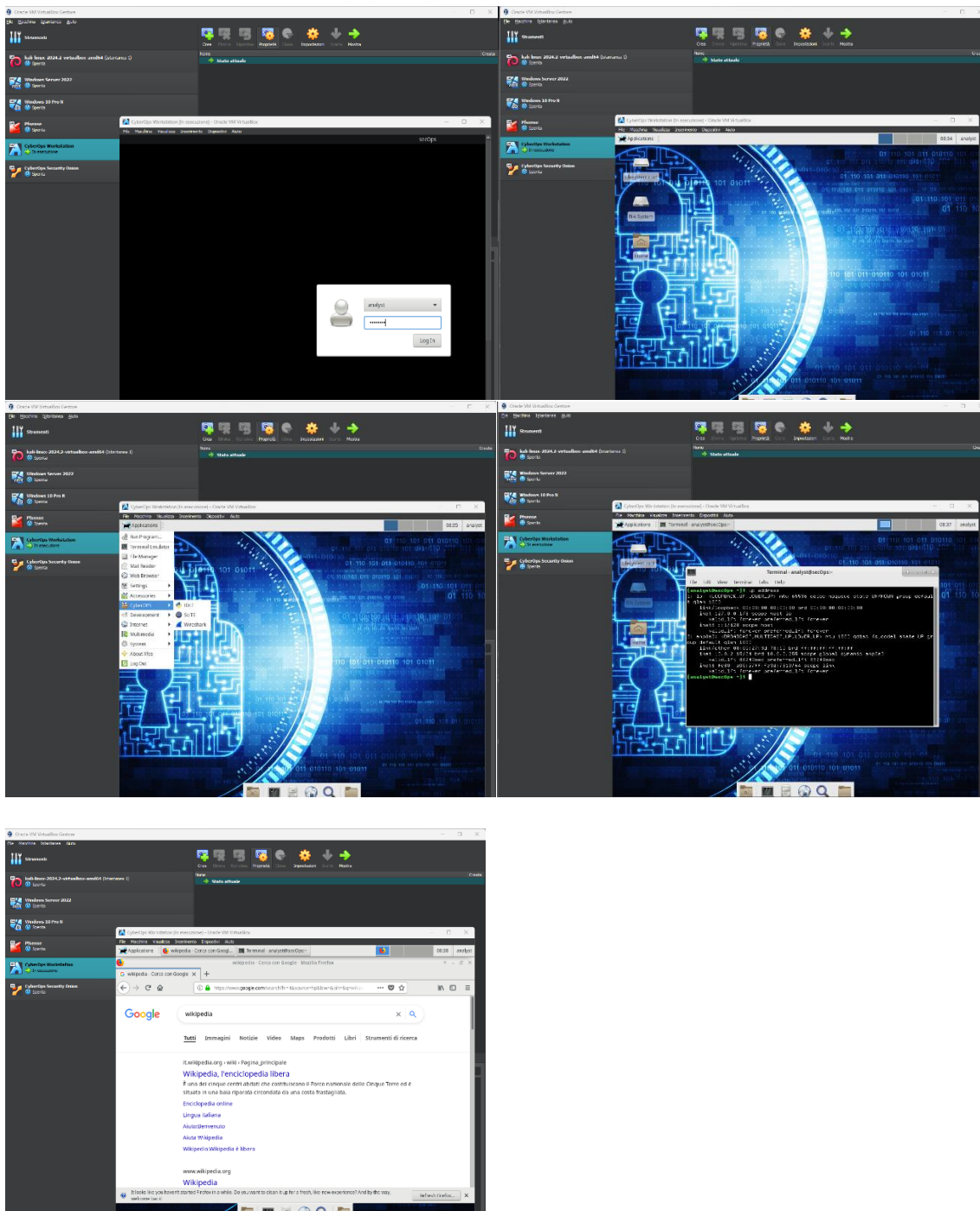


Relazione sulle Attività Svolte

1. Installazione delle Macchine Virtuali

La prima fase del laboratorio ha riguardato l'installazione delle macchine virtuali necessarie per il completamento delle attività. Abbiamo seguito le istruzioni riportate in consegna per installare e configurare correttamente la **CyberOps Workstation** e la **CyberOps Security Onion**.

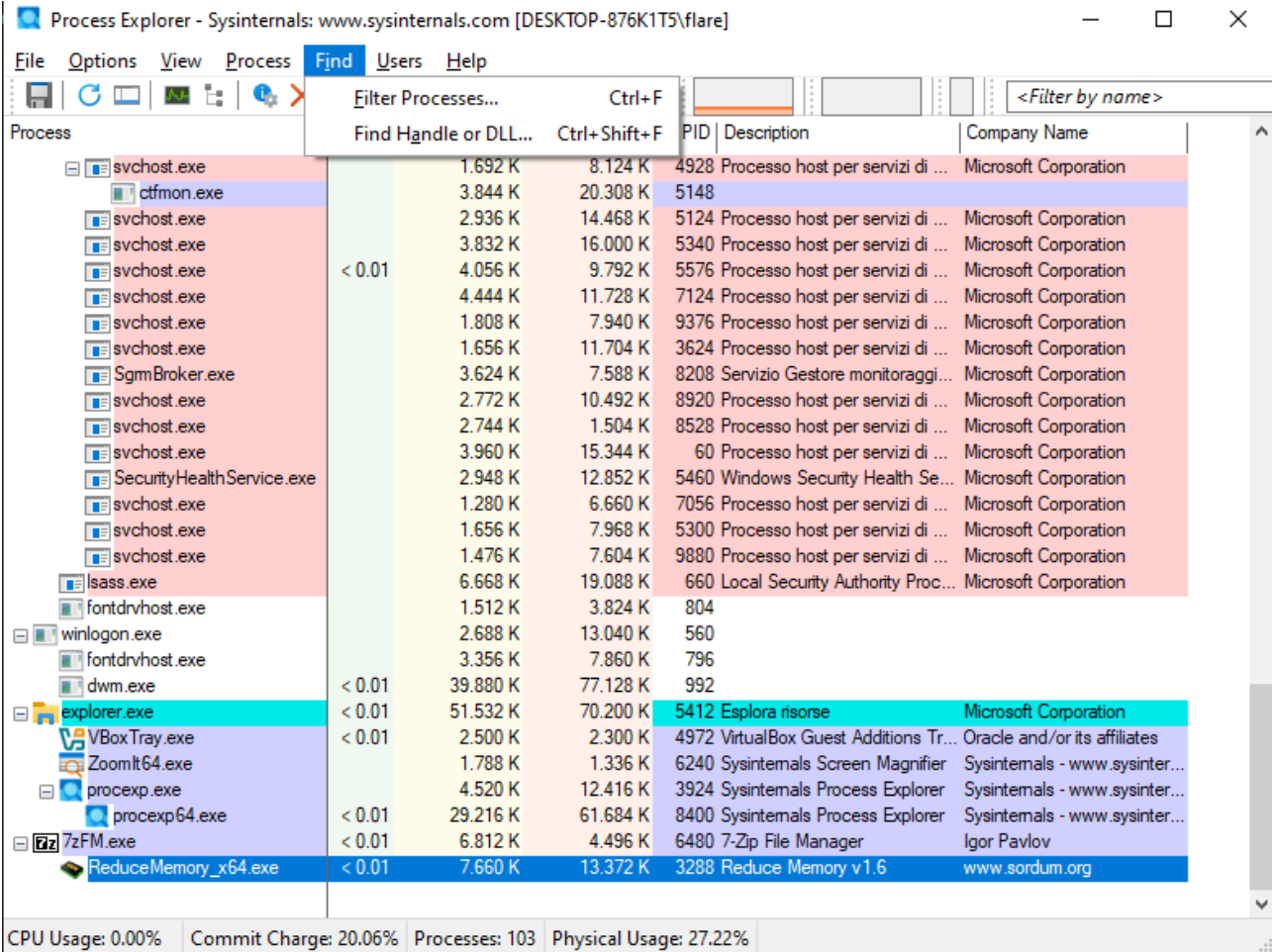
1. **CyberOps Workstation:** Abbiamo scaricato l'OVA (Open Virtualization Archive) del sistema operativo e l'abbiamo importato nel nostro hypervisor. Dopo l'importazione, la macchina è stata configurata in NAT seguendo i parametri indicati nella guida.



2. **CyberOps Security Onion:** Successivamente, abbiamo installato anche questa macchina virtuale utilizzando una procedura simile, configurandola per l'analisi e il monitoraggio della sicurezza.

2. Esplorazione di Processi, Thread, Handle e Registro di Windows

Nella seconda fase del laboratorio, ci siamo concentrati sull'esplorazione di alcuni aspetti interni di un sistema Windows tramite l'utilizzo di strumenti avanzati come **Process Explorer** e il **Registro di Windows**.

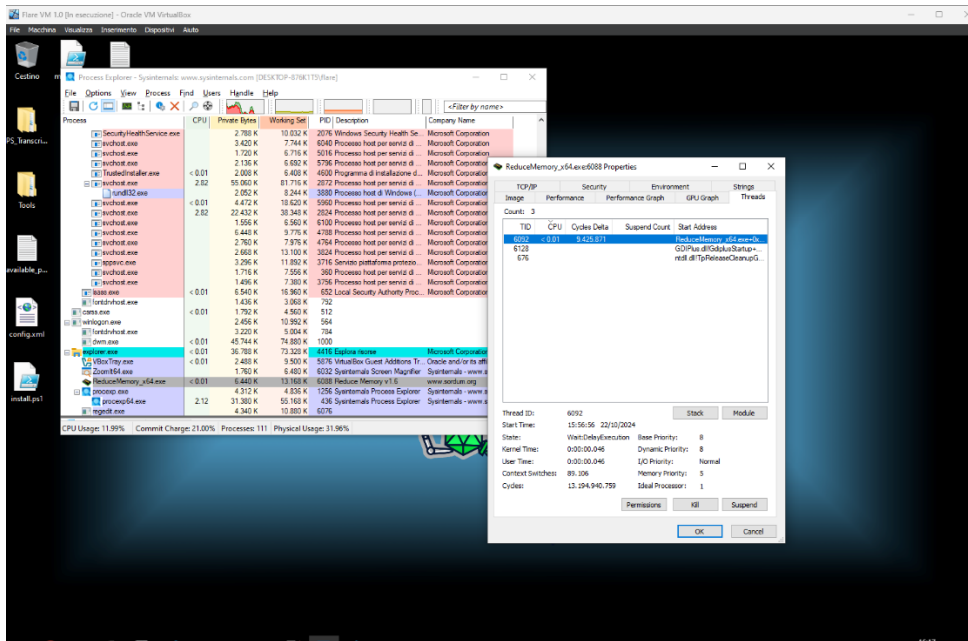


| Process | PID | Description | Company Name |
|---------------------------|------|----------------------------------|--------------------------------|
| svchost.exe | 4928 | Processo host per servizi di ... | Microsoft Corporation |
| ctfmon.exe | 5148 | | |
| svchost.exe | 5124 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | 5340 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | 5576 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | 7124 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | 9376 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | 3624 | Processo host per servizi di ... | Microsoft Corporation |
| SgmBroker.exe | 8208 | Servizio Gestore monitoraggi... | Microsoft Corporation |
| svchost.exe | 8920 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | 8528 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | 60 | Processo host per servizi di ... | Microsoft Corporation |
| SecurityHealthService.exe | 5460 | Windows Security Health Se... | Microsoft Corporation |
| svchost.exe | 7056 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | 5300 | Processo host per servizi di ... | Microsoft Corporation |
| svchost.exe | 9880 | Processo host per servizi di ... | Microsoft Corporation |
| lsass.exe | 660 | Local Security Authority Proc... | Microsoft Corporation |
| fontdrvhost.exe | 804 | | |
| winlogon.exe | 560 | | |
| fontdrvhost.exe | 796 | | |
| dwm.exe | 992 | | |
| explorer.exe | 5412 | Esplora risorse | Microsoft Corporation |
| VBoxTray.exe | 4972 | VirtualBox Guest Additions Tr... | Oracle and/or its affiliates |
| ZoomIt64.exe | 6240 | Sysinternals Screen Magnifier | Sysinternals - www.sysinter... |
| procexp.exe | 3924 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| procexp64.exe | 8400 | Sysinternals Process Explorer | Sysinternals - www.sysinter... |
| 7zFM.exe | 6480 | 7-Zip File Manager | Igor Pavlov |
| ReduceMemory_x64.exe | 3288 | Reduce Memory v1.6 | www.sordum.org |

CPU Usage: 0.00% Commit Charge: 20.06% Processes: 103 Physical Usage: 27.22%

Obiettivi del laboratorio

- Esplorare i processi, i thread e gli handle utilizzando **Process Explorer** della Sysinternals Suite.



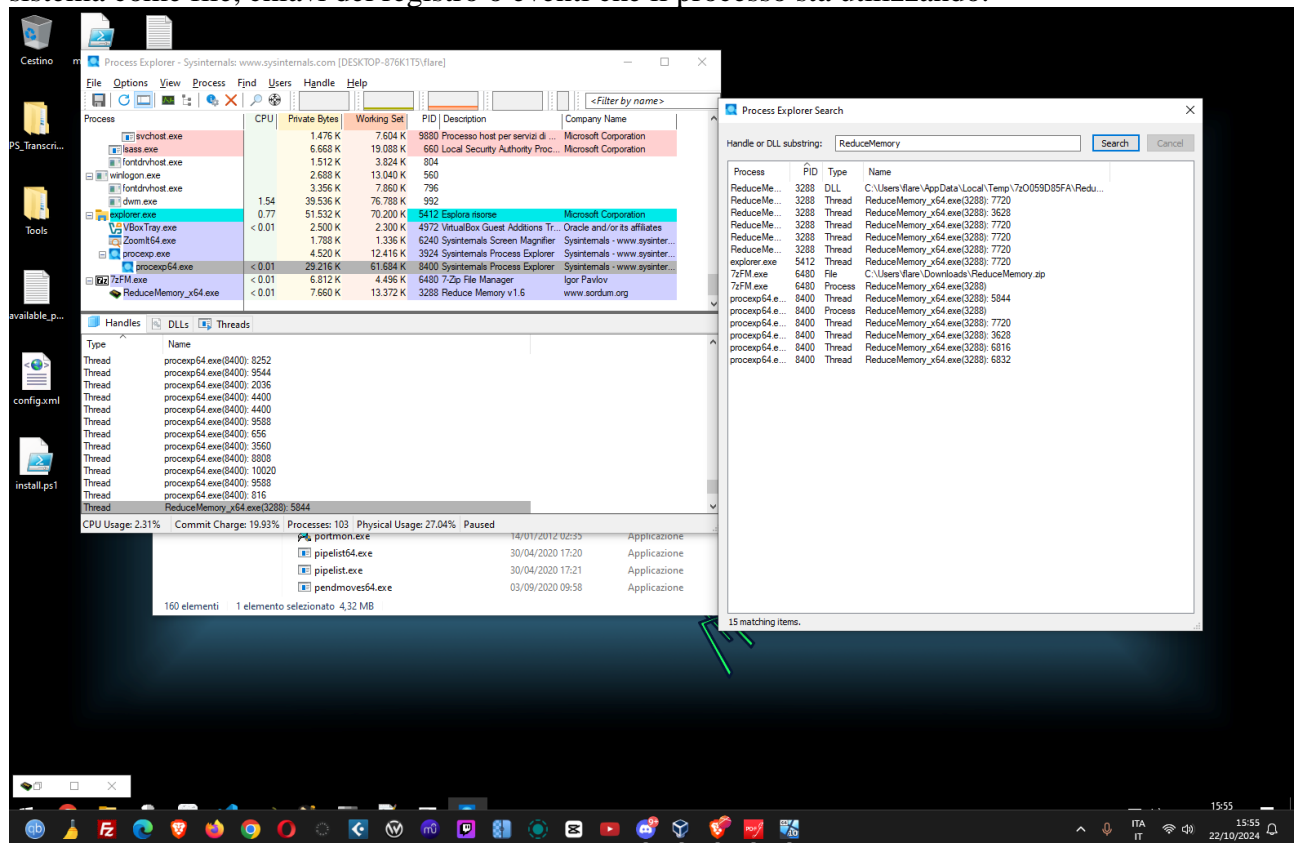
- Modificare un'impostazione tramite il **Registro di Windows**.

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

Process Explorer è uno strumento avanzato della Sysinternals Suite che consente di esaminare in dettaglio i processi in esecuzione su un sistema Windows. Durante questa fase, abbiamo:

- **Identificato i processi** attivi, visualizzando informazioni dettagliate come l'uso della CPU e della memoria.
- **Analizzato i thread** associati a ciascun processo, comprendendo come essi vengono gestiti dal sistema operativo.

- **Esaminato gli handle** aperti da ciascun processo. Gli handle sono riferimenti a risorse di sistema come file, chiavi del registro o eventi che il processo sta utilizzando.

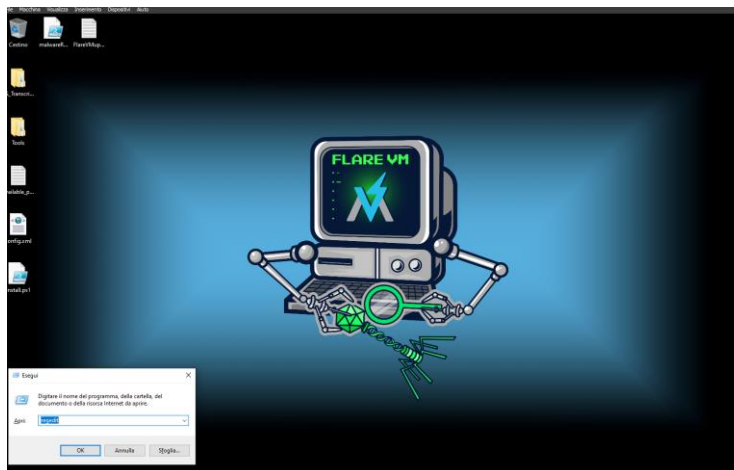


Abbiamo imparato come **Process Explorer** possa essere utilizzato per individuare potenziali minacce, come malware nascosti sotto processi legittimi o utilizzi anomali delle risorse.

2.2. Modifica di un'impostazione nel Registro di Windows

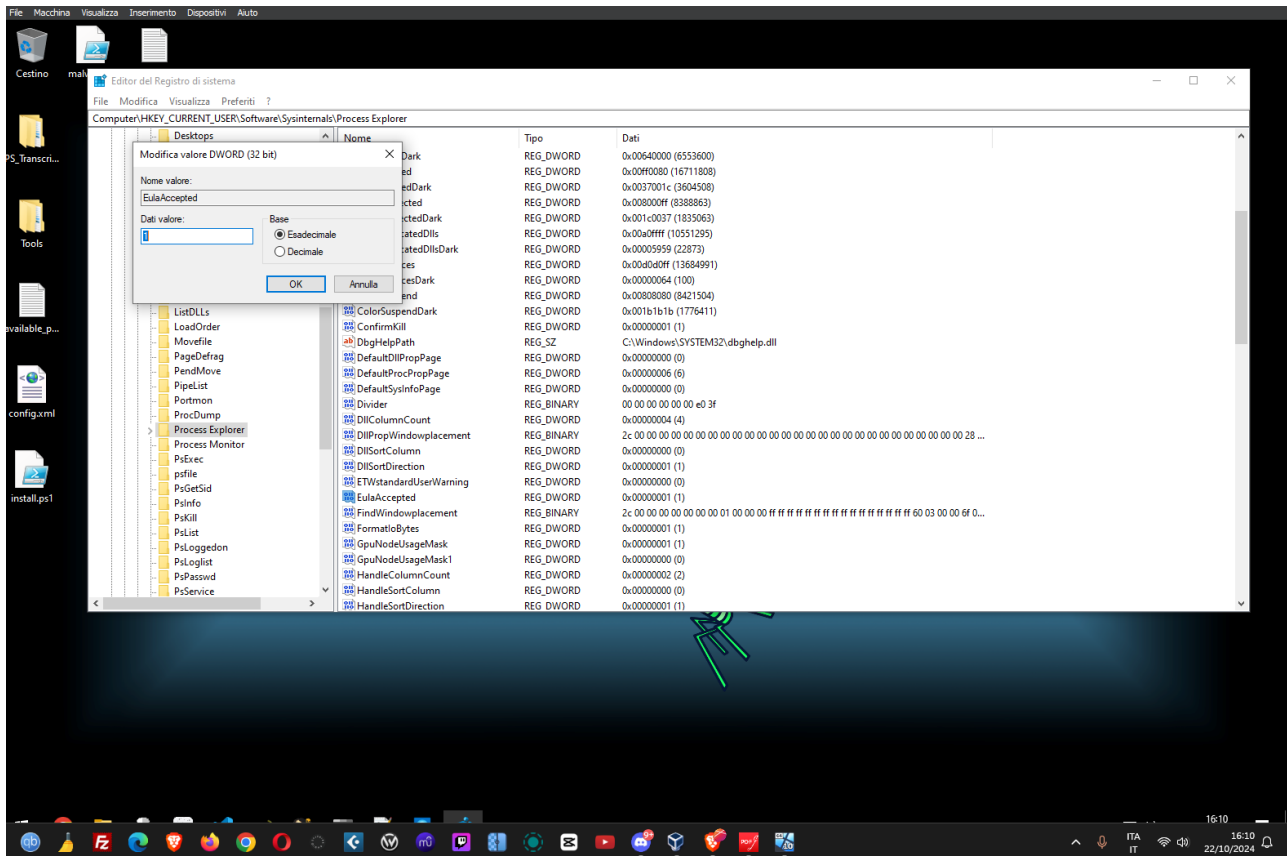
Il **Registro di Windows** è una base di dati gerarchica che memorizza le configurazioni e le impostazioni di sistema. In questo laboratorio, abbiamo:

- Navigato attraverso il Registro di Windows utilizzando l'editor regedit.



- Modificato un'impostazione specifica all'interno del registro per personalizzare il comportamento del sistema.

Quindi siamo andati su **HKEY_CURRENT_USER > Software > Sisinterni > Process Explorer**, individuato la chiave **EulaAccepted** e lo abbiamo modificato da 0x0000001 a 0x0000000



L'attività ci ha permesso di comprendere meglio come le impostazioni a basso livello del sistema operativo possano essere manipolate per cambiare il funzionamento di Windows, un aspetto importante sia per l'analisi forense che per la risoluzione dei problemi.

Conclusioni

Questo laboratorio ci ha permesso di acquisire competenze pratiche sia nell'utilizzo di strumenti avanzati di analisi come **Process Explorer**, sia nella modifica di configurazioni critiche attraverso il **Registro di Windows**. Queste attività sono fondamentali per chi opera nel campo della sicurezza informatica, poiché permettono di monitorare e risolvere problemi legati alla gestione di processi e risorse del sistema, oltre a fornire strumenti utili per l'analisi forense in caso di incidenti di sicurezza.