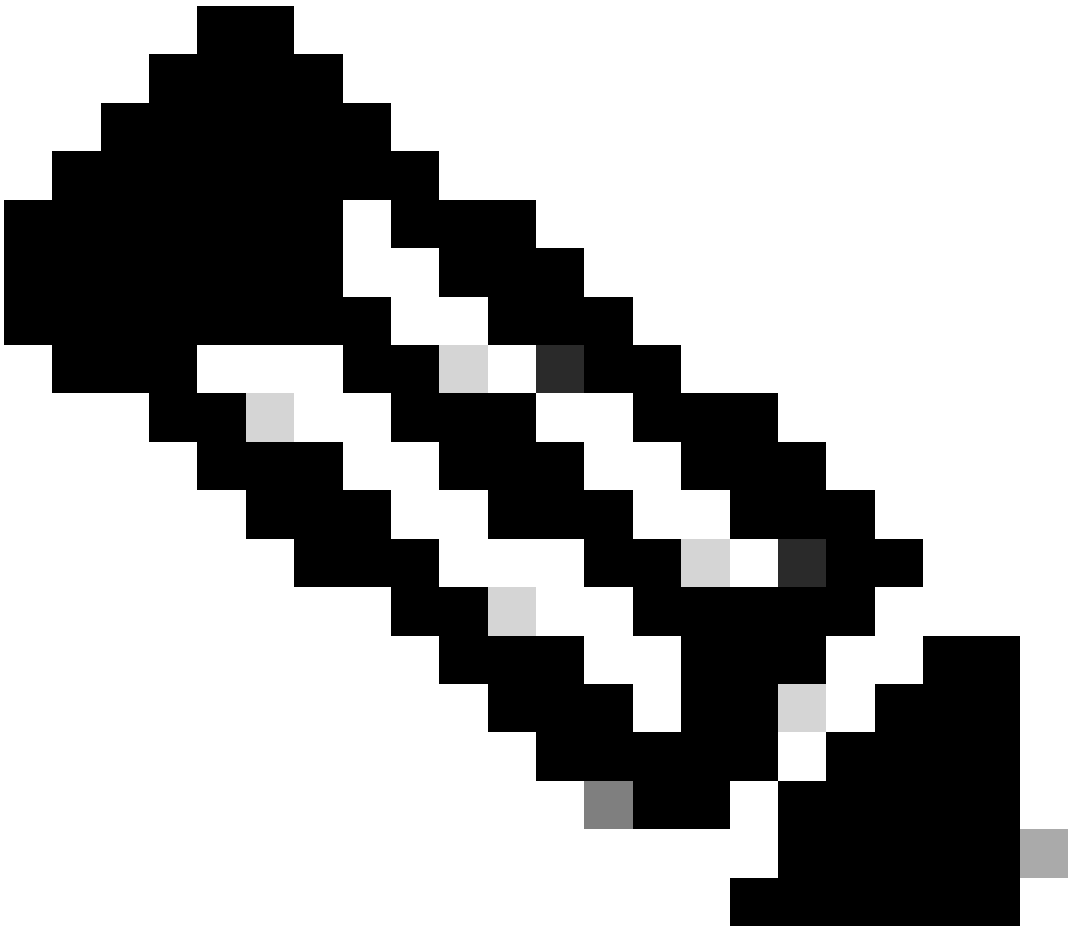
Raccolta dei log per il modulo XDR Forensics

Sommario

Introduzione

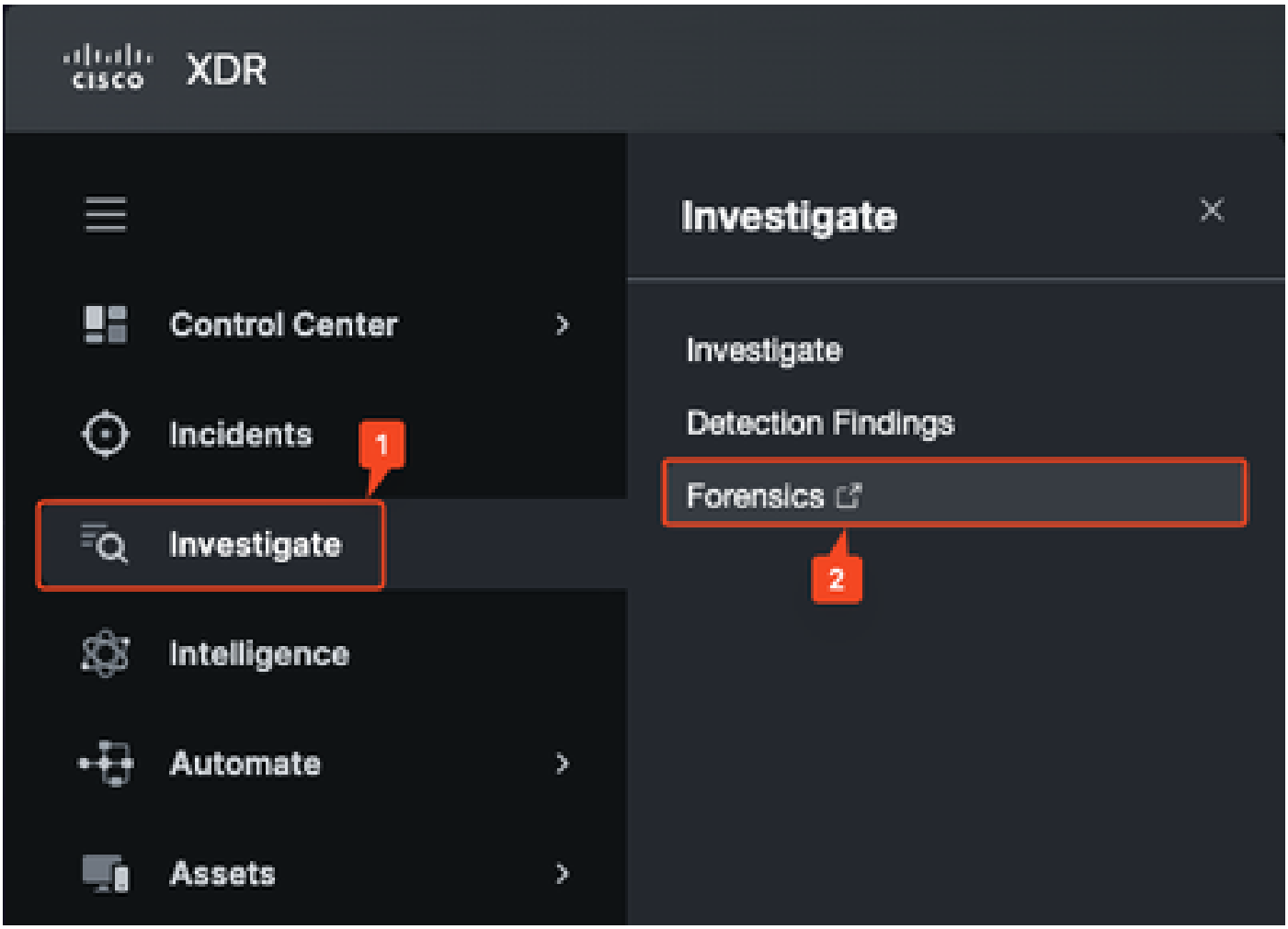
In questo documento viene descritto come recuperare in remoto i dati di diagnostica per risolvere i problemi relativi al modulo XDR Forensics nella relativa console.

Recupero dei log in remoto



Nota: Al momento, i log DART non contengono i log di XDR Forensics.

Passaggio 1. Aprire XDR e passare a Indaga > Console legale.



Passaggio 2. Verificare che il nome host dell'endpoint sia visibile nella pagina Asset passando alla pagina Asset. A tale scopo:

a) Aprire CMD sulla macchina in questione ed eseguire il comando hostname.

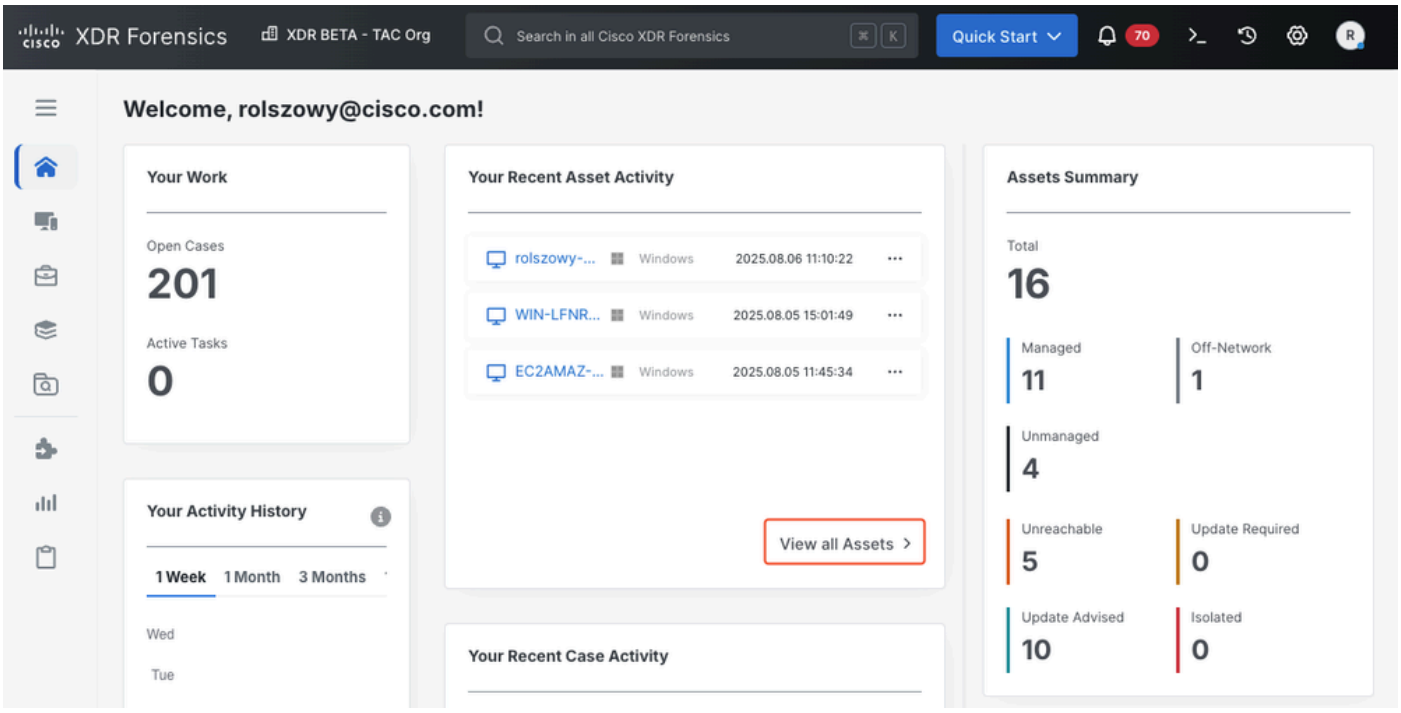
<#root>

```
C:\Users\Admin\
```

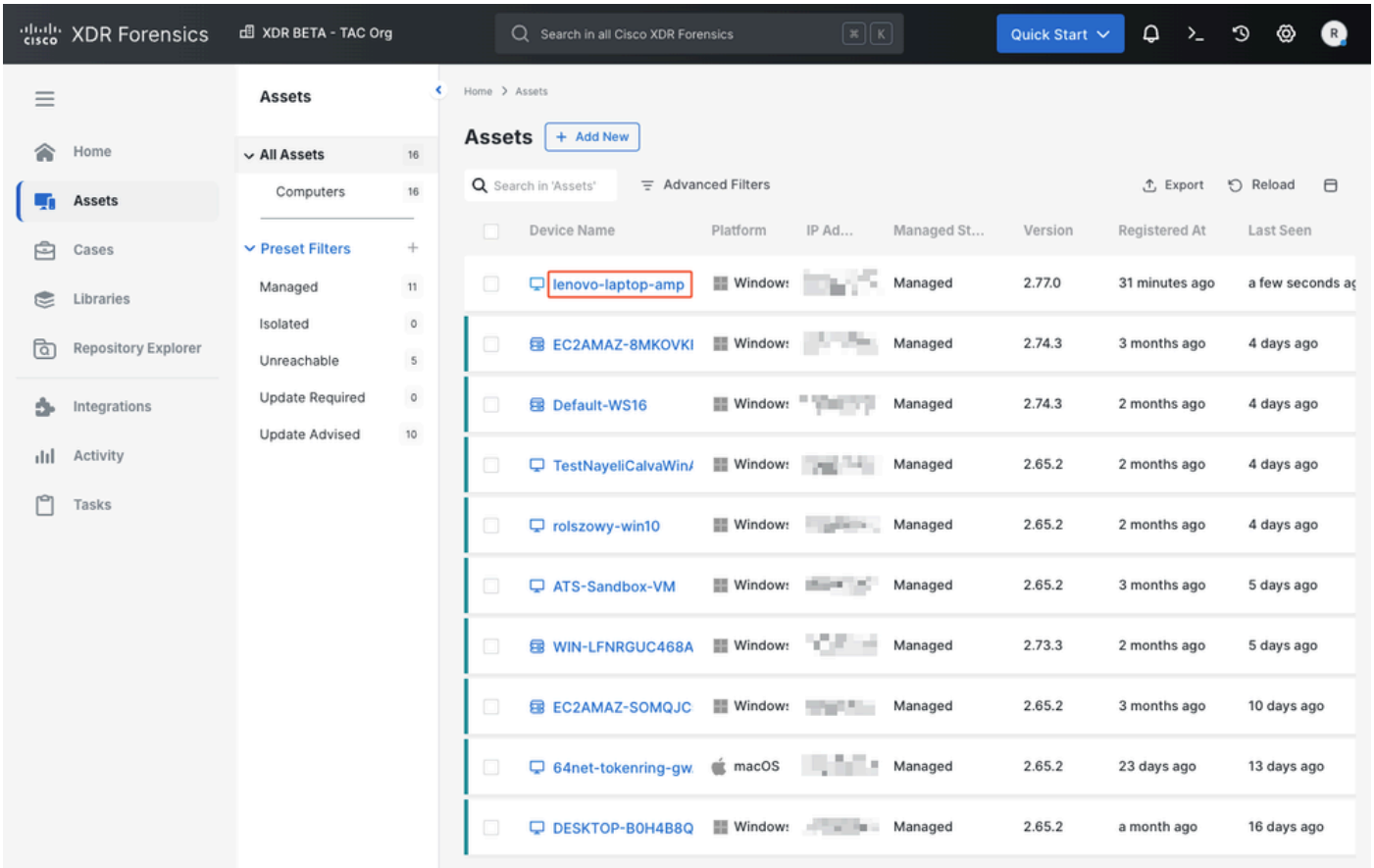
hostname

```
lenovo-laptop-amp
```

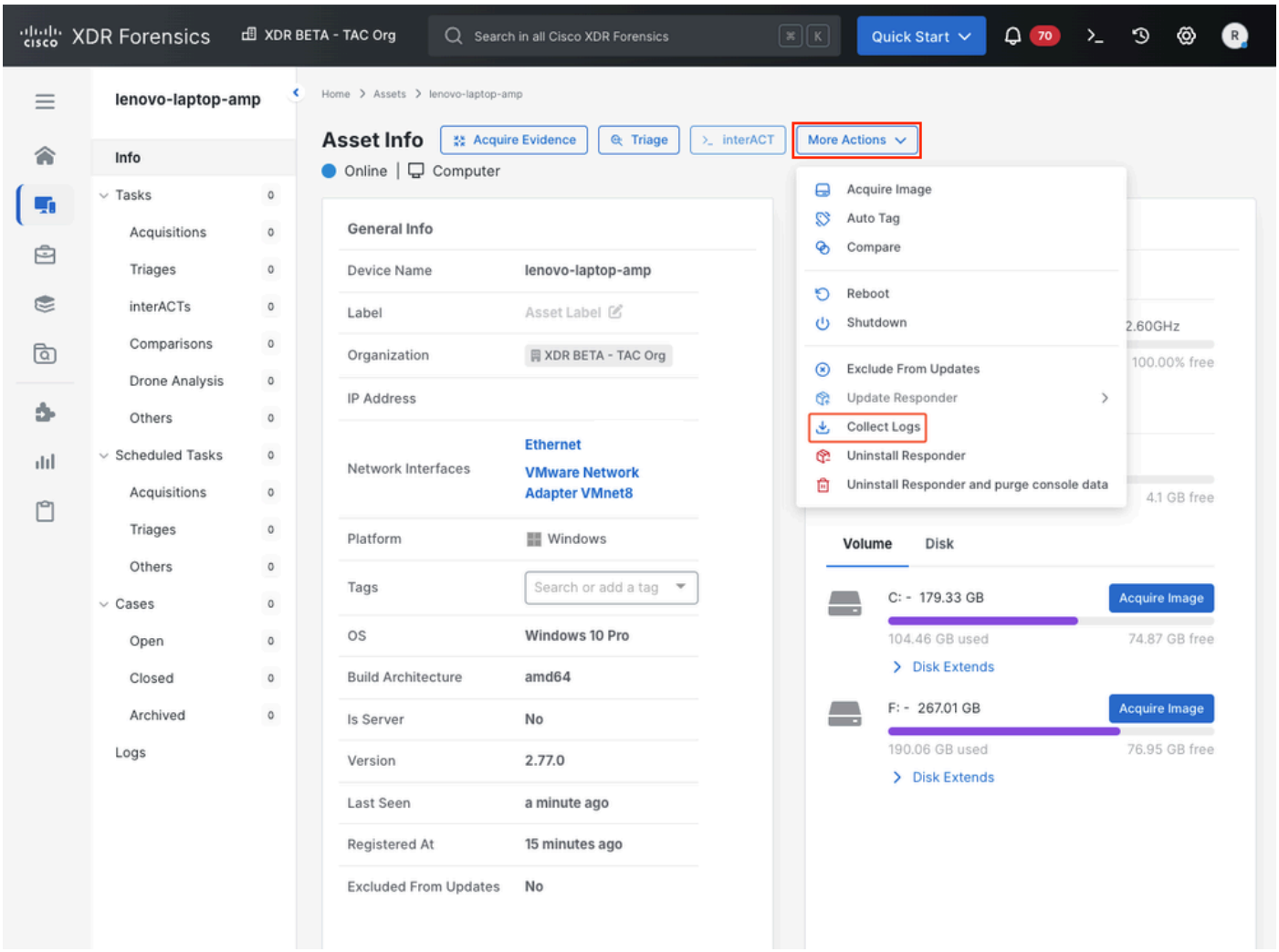
b) Nella pagina principale della console XDR Forensics fare clic su View all Assets (Visualizza tutti gli asset) (o utilizzare il menu Assets sulla sinistra).

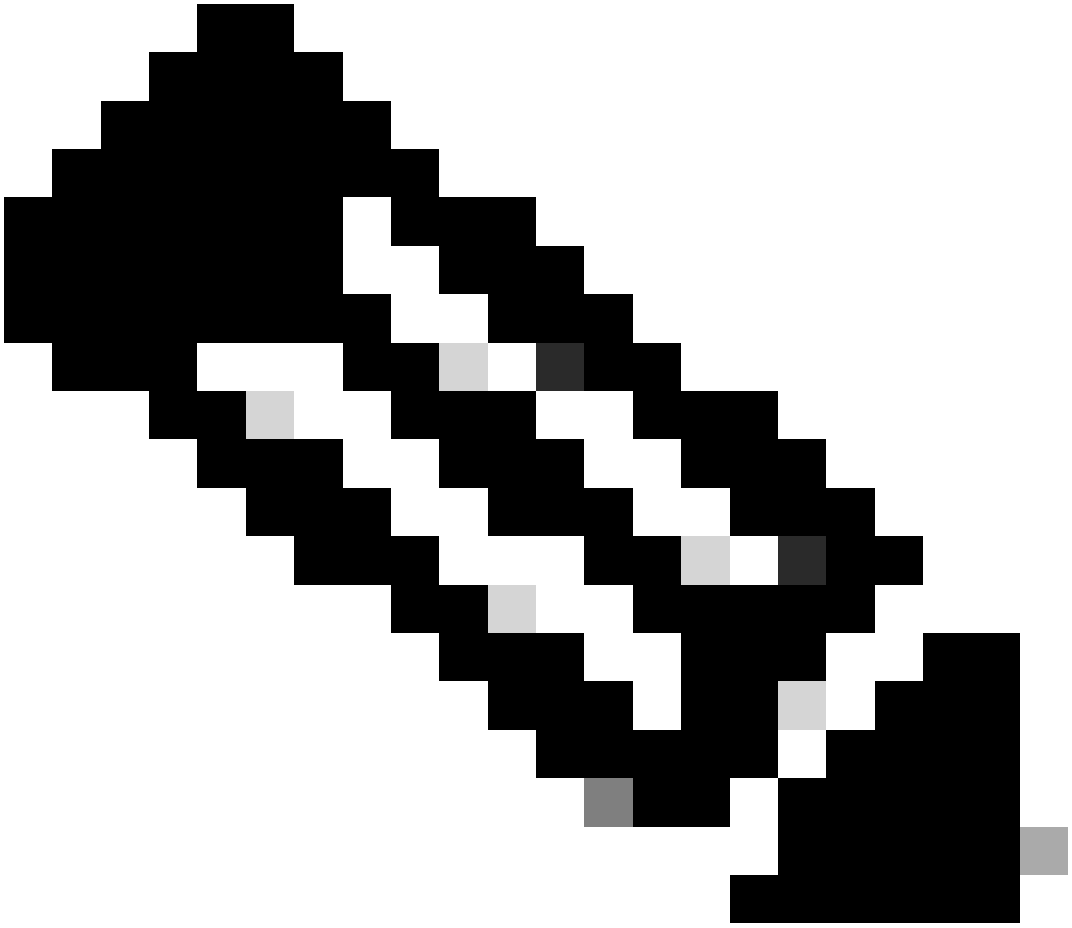


c) Localizzare l'endpoint nell'elenco e fare clic sul nome del dispositivo per immettere i dettagli.



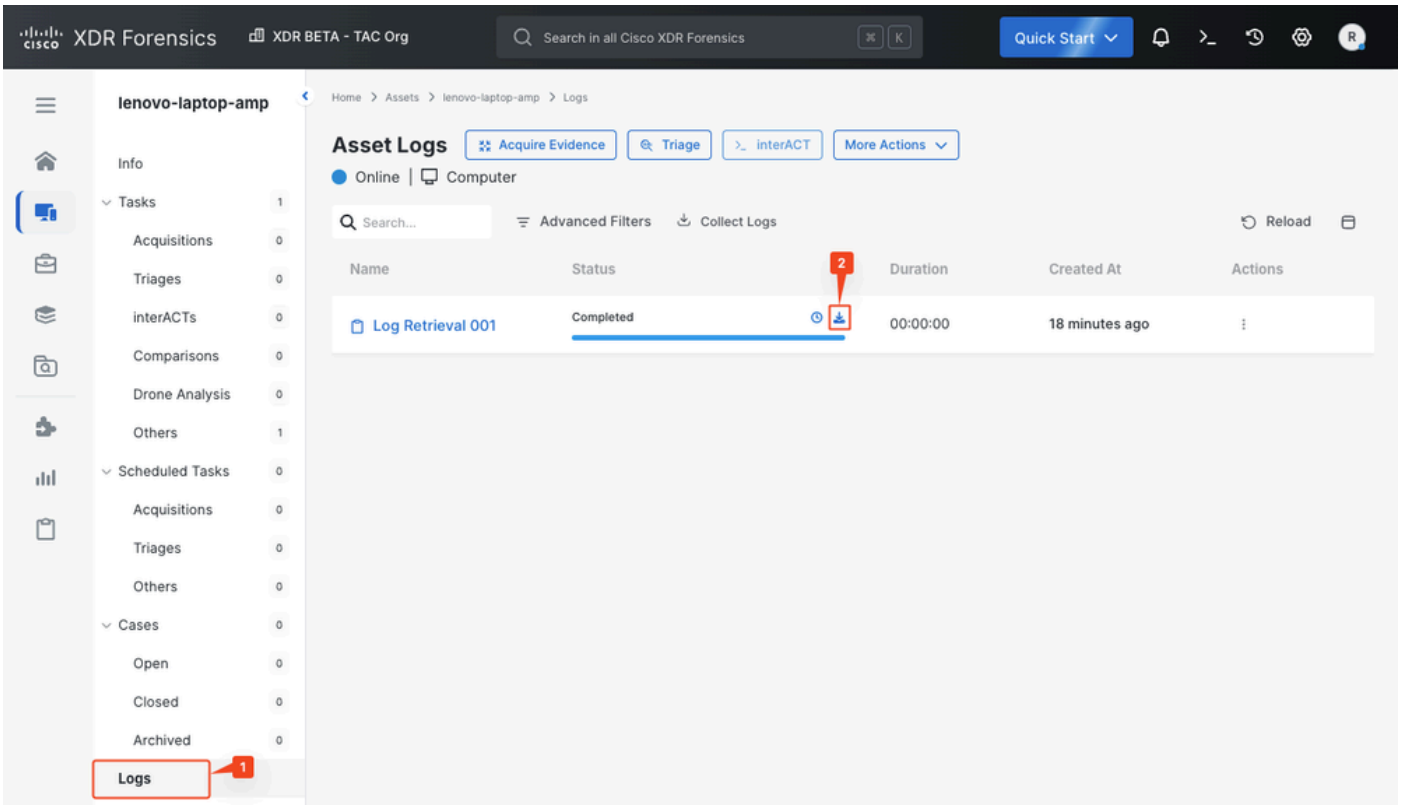
Passaggio 3. Nella pagina Informazioni asset, fare clic su Altre azioni > Raccogli log per avviare la raccolta di informazioni dall'endpoint.


XDR Forensics
XDR BETA - TAC Org
Search in all Cisco XDR Forensics
Quick Start
70
lenovo-laptop-amp
Info
Tasks 0
Acquisitions 0
Triages 0
interACTs 0
Comparisons 0
Drone Analysis 0
Others 0
Scheduled Tasks 0
Acquisitions 0
Triages 0
Others 0
Cases 0
Open 0
Closed 0
Archived 0
Logs
Home > Assets > lenovo-laptop-amp
Asset Info
Acquire Evidence
Triage
interACT
More Actions
Online | Computer
General Info
Device Name lenovo-laptop-amp
Label Asset Label
Organization XDR BETA - TAC Org
IP Address
Network Interfaces Ethernet
VMware Network Adapter VMnet8
Platform Windows
Tags Search or add a tag
OS Windows 10 Pro
Build Architecture amd64
Is Server No
Version 2.77.0
Last Seen a minute ago
Registered At 15 minutes ago
Excluded From Updates No
Acquire Image
Auto Tag
Compare
Reboot
Shutdown
Exclude From Updates
Update Responder
Collect Logs
Uninstall Responder
Uninstall Responder and purge console data
2.60GHz
100.00% free
4.1 GB free
Volume
Disk
C: - 179.33 GB
Acquire Image
104.46 GB used
74.87 GB free
Disk Extends
F: - 267.01 GB
Acquire Image
190.06 GB used
76.95 GB free
Disk Extends



Nota: Se la risorsa è in linea, occorrono alcuni secondi per completare l'operazione.

Passaggio 4. Andare alla sezione Log per verificare se i log sono già stati raccolti. Nella sezione Log asset, fare clic sull'icona per avviare il download dei log.

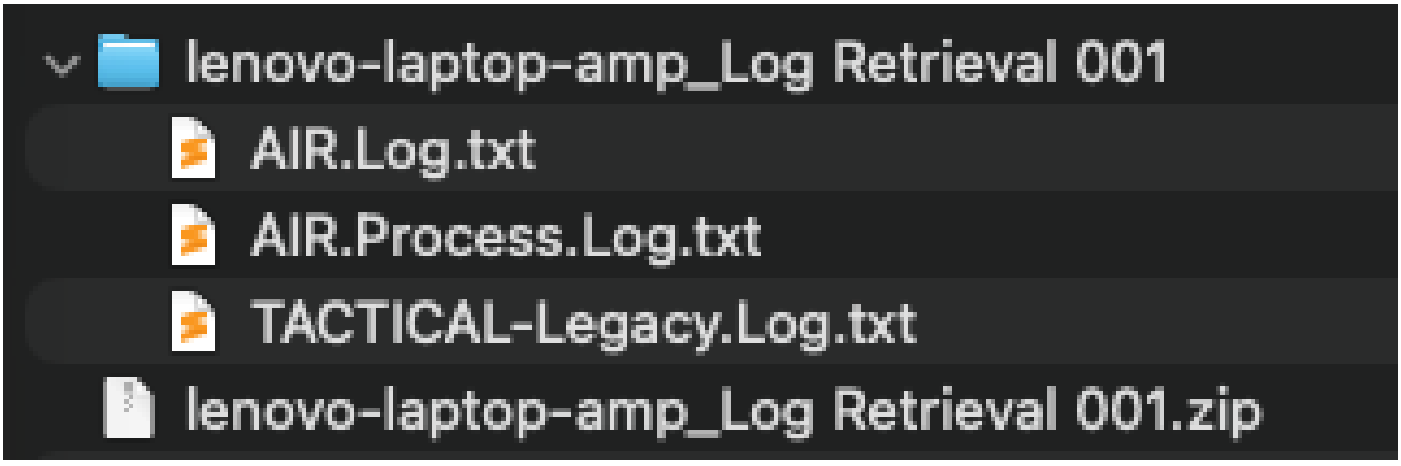


Passaggio 5. Il file *.zip acquisito contiene tre file necessari per la risoluzione dei problemi del modulo:

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).