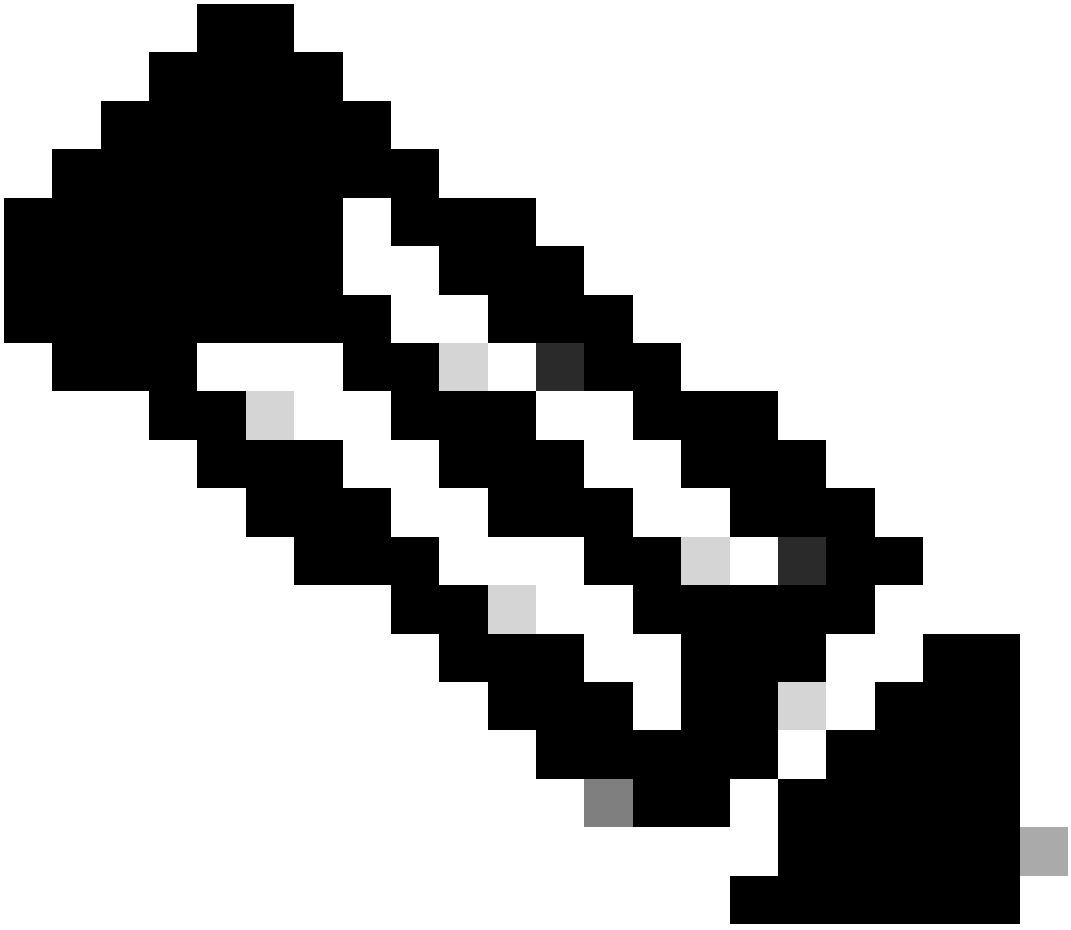
Collecter les journaux pour le module XDR Forensics

Table des matières

Introduction

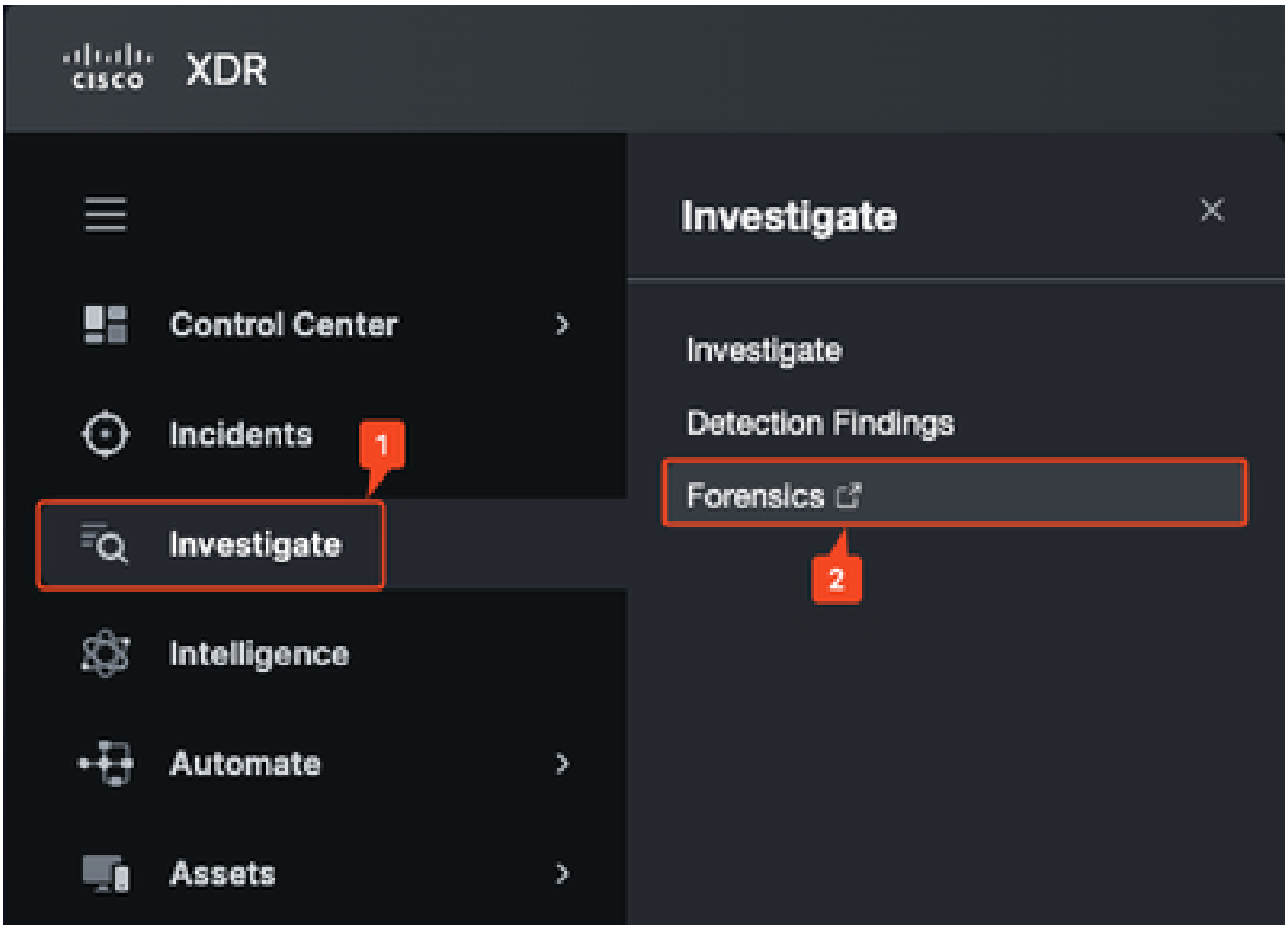
Ce document décrit comment récupérer à distance des données de diagnostic pour dépanner le module XDR Forensics dans sa console.

Récupération des journaux à distance



Remarque : Actuellement, les journaux DART ne contiennent pas de journaux XDR Forensics.

Étape 1. Ouvrez XDR et accédez à Investigate > Forensics console.



Étape 2 : vérifiez que le nom d'hôte du point de terminaison est visible sur la page Assets en accédant à la page Assets. Pour ce faire :

a) Ouvrez CMD sur la machine donnée et exécutez la commande hostname.

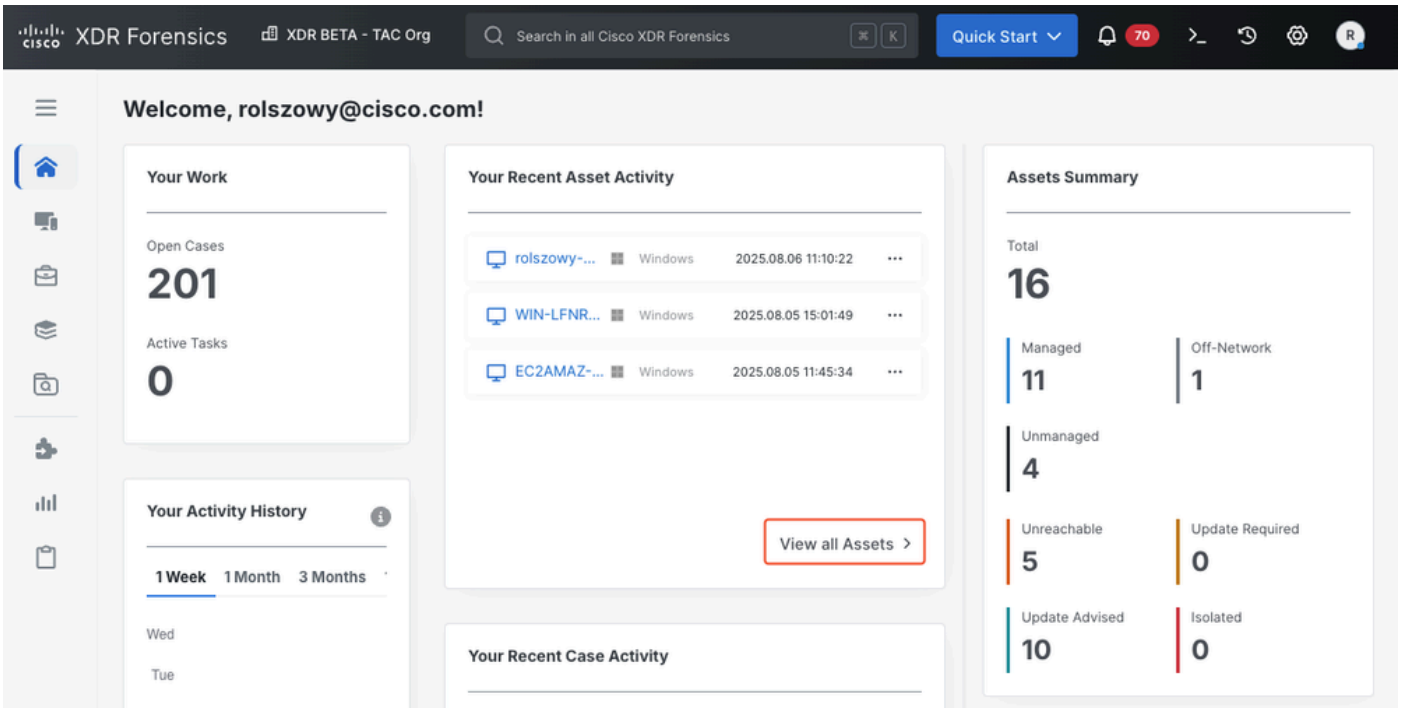
<#root>

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

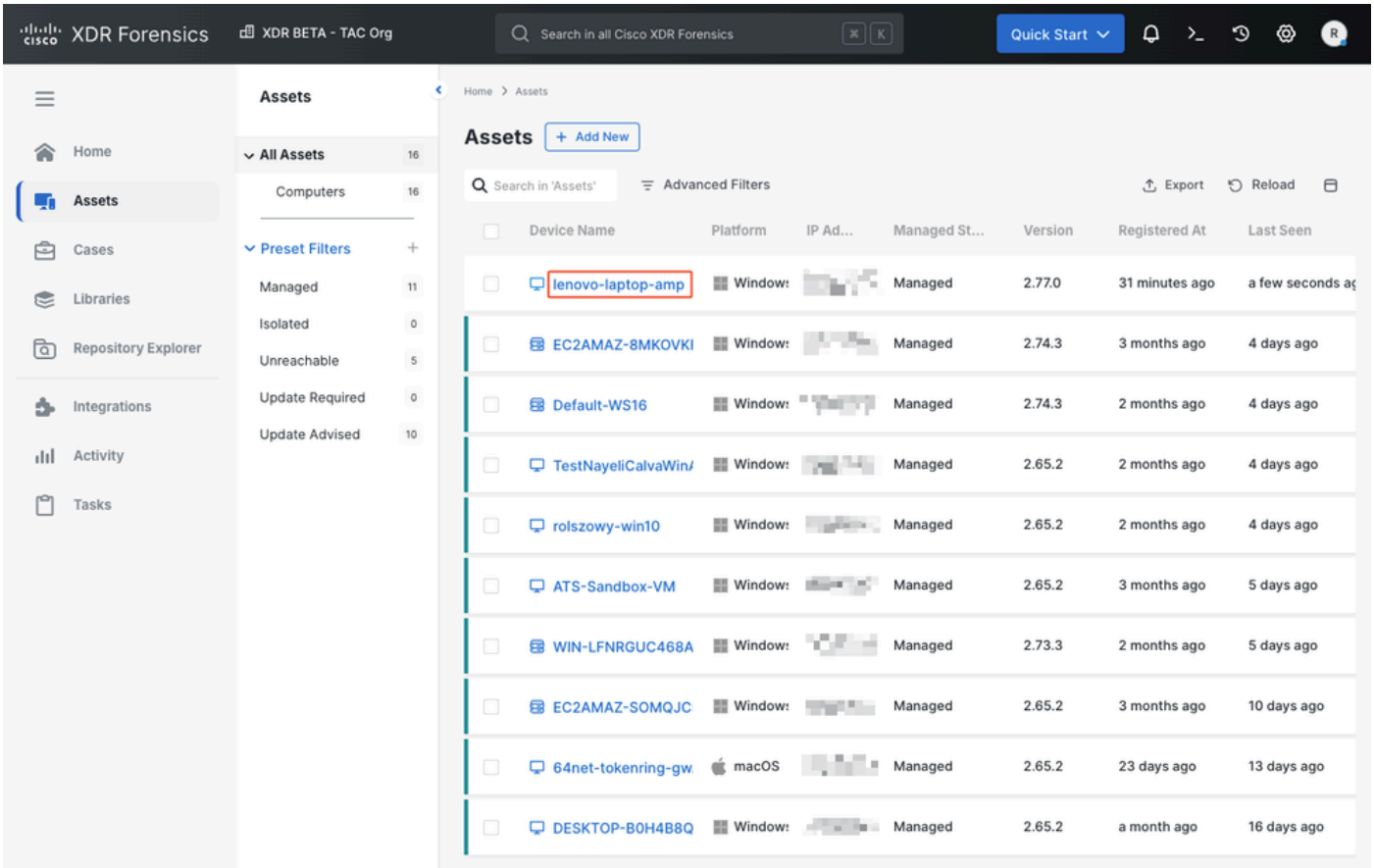
hostname

```
lenovo-laptop-amp
```

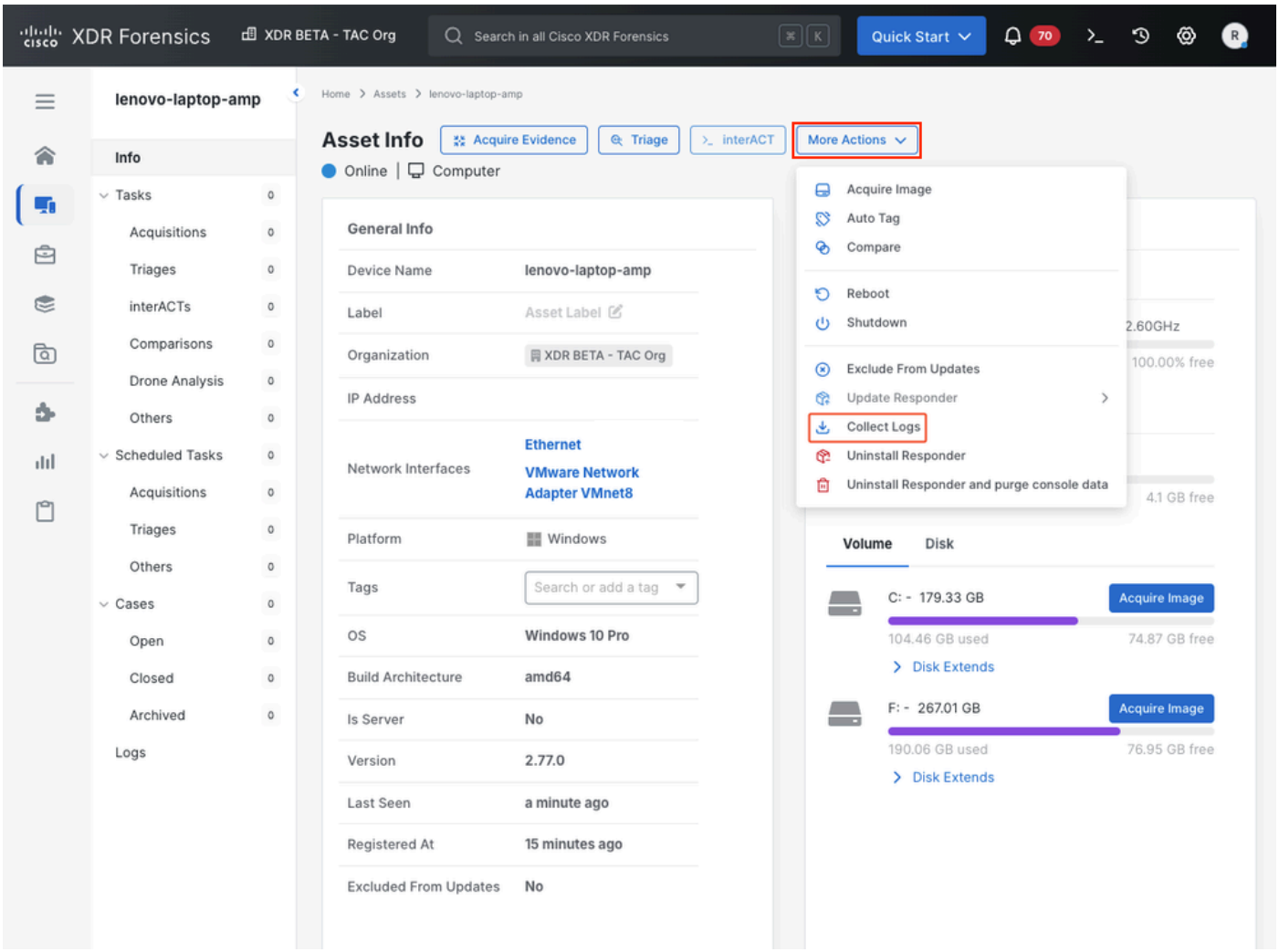
b) Dans la page principale de la console XDR Forensics, cliquez sur View all Assets (Afficher tous les actifs) (ou utilisez le menu Assets (Actifs) à gauche).

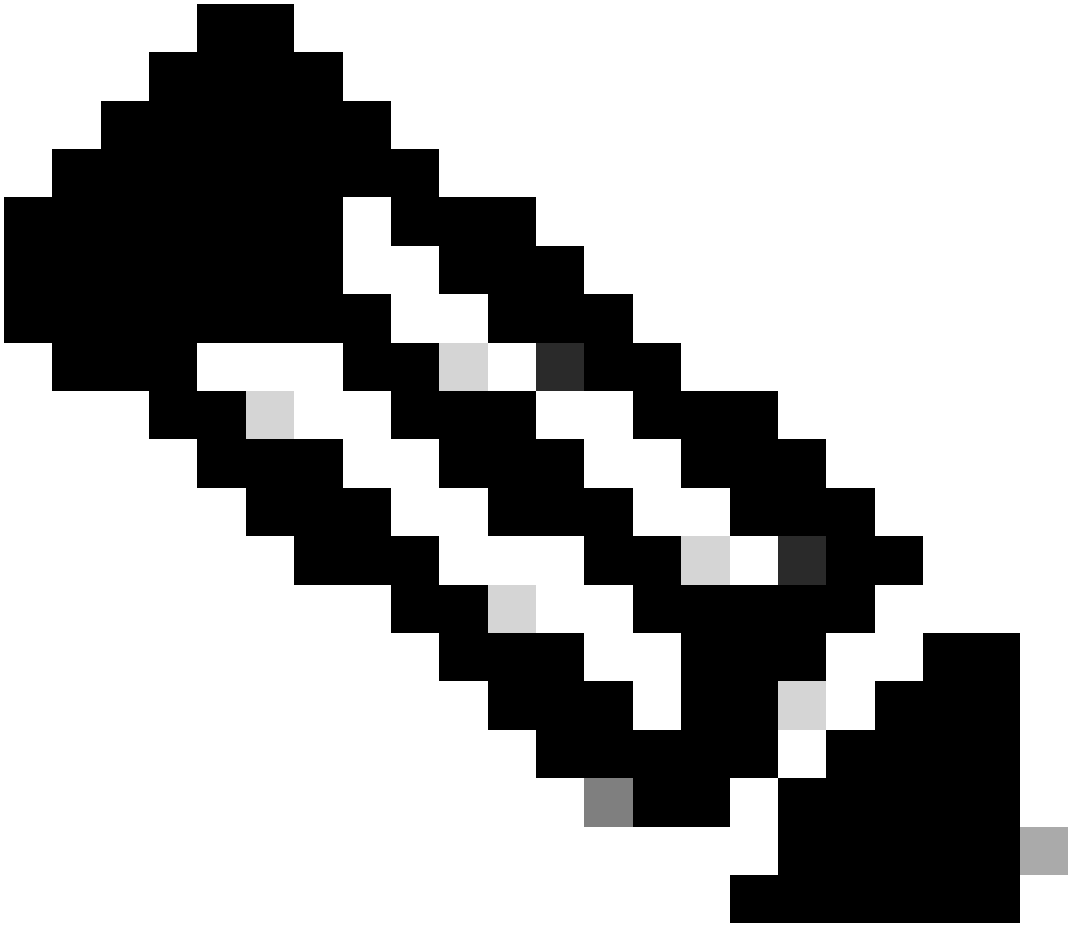


c) Localisez le terminal dans la liste et cliquez sur le nom du périphérique pour entrer ses détails.



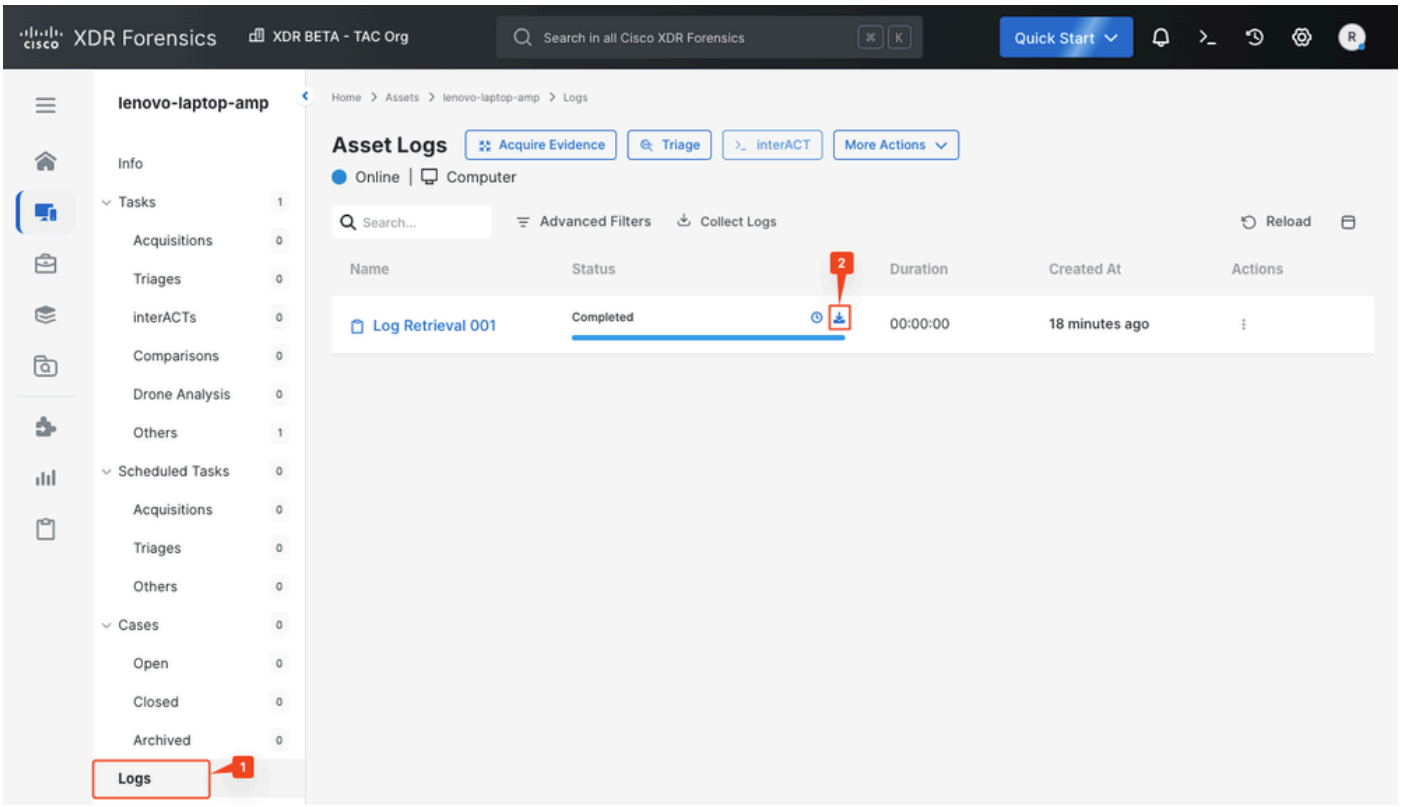
Étape 3. Dans la page Informations sur l'actif, cliquez sur Autres actions > Collecter les journaux pour commencer à collecter des informations à partir du point d'extrémité.


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



Remarque : Si la ressource est en ligne, cette opération prend quelques secondes.

Étape 4. Accédez à la section Journaux pour voir si les journaux ont déjà été collectés. Dans la section Journaux d'actifs, cliquez sur l'icône pour lancer le téléchargement des journaux.

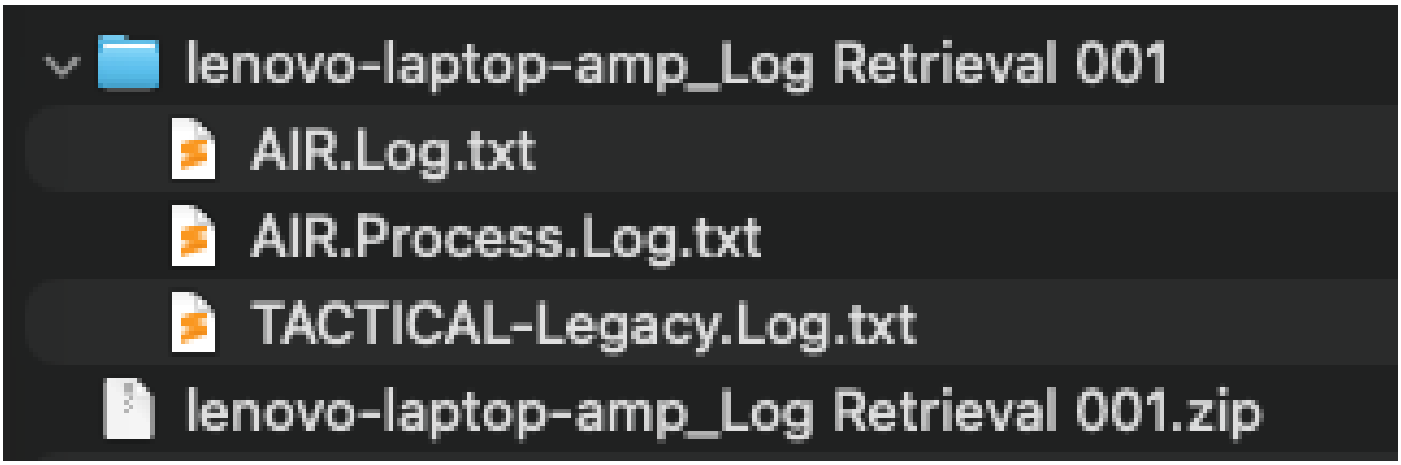


Étape 5. Le fichier *.zip acquis contient trois fichiers nécessaires au dépannage du module :

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.