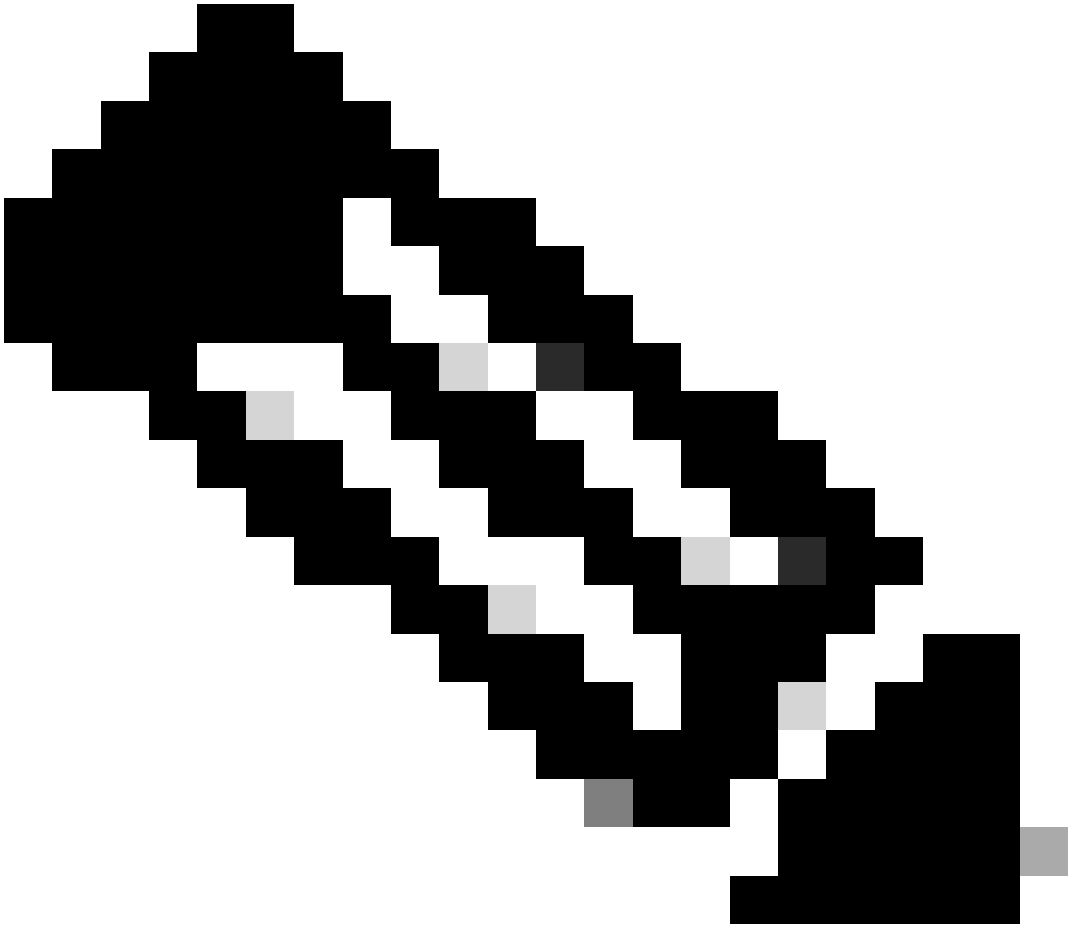
Recopilar registros para el módulo de diagnóstico XDR

Contenido

Introducción

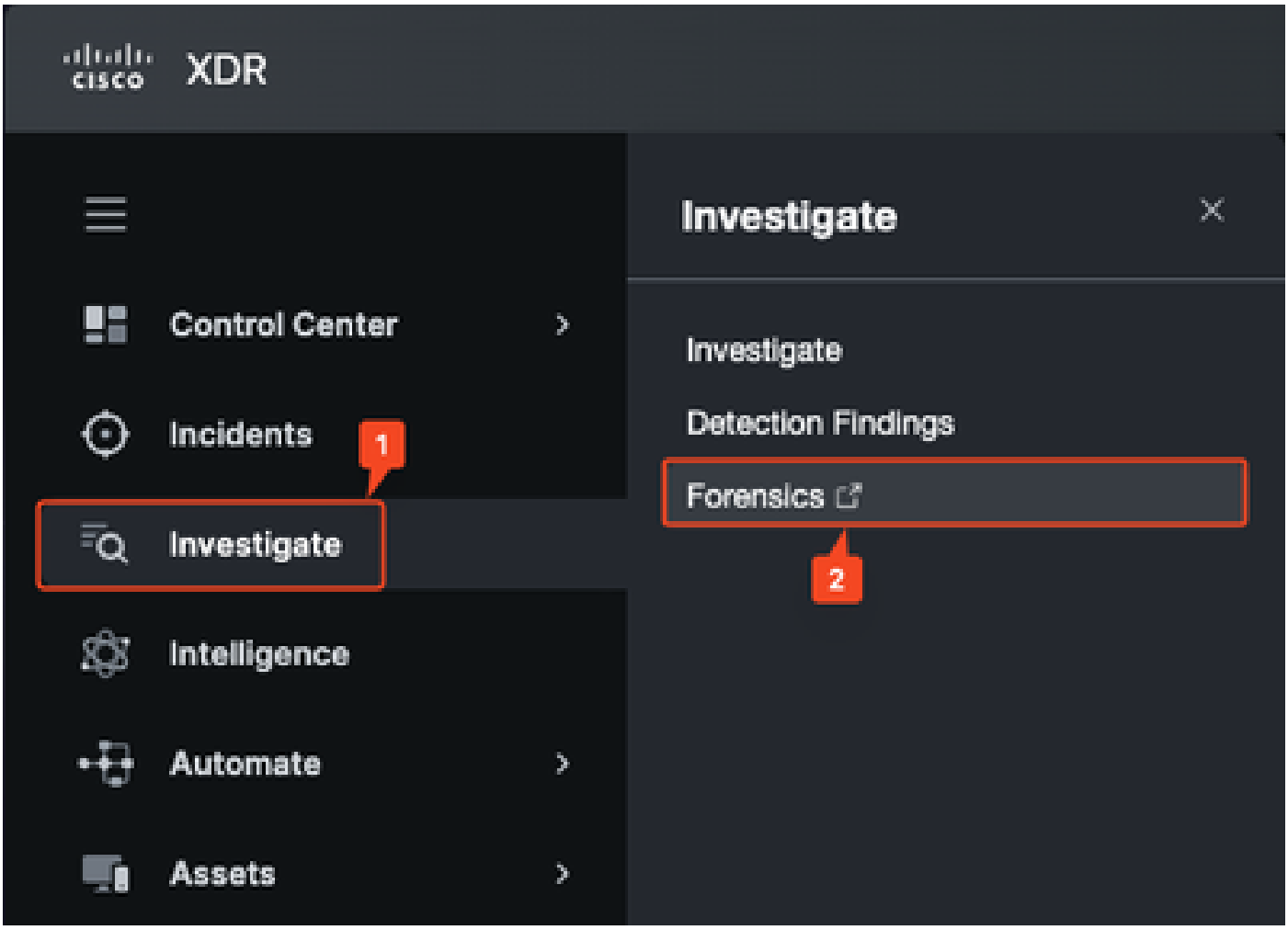
Este documento describe cómo obtener datos de diagnóstico de forma remota para resolver problemas del módulo XDR Forensics en su consola.

Obteniendo registros de forma remota



Nota: Actualmente, los registros de DART no contienen registros de diagnóstico de XDR.

Paso 1. Abra XDR y navegue hasta la consola de Investigate > Forensics.



Paso 2. Compruebe que el nombre de host del terminal está visible en la página Activos; para ello, acceda a la página Activos. Para llevar esto a cabo:

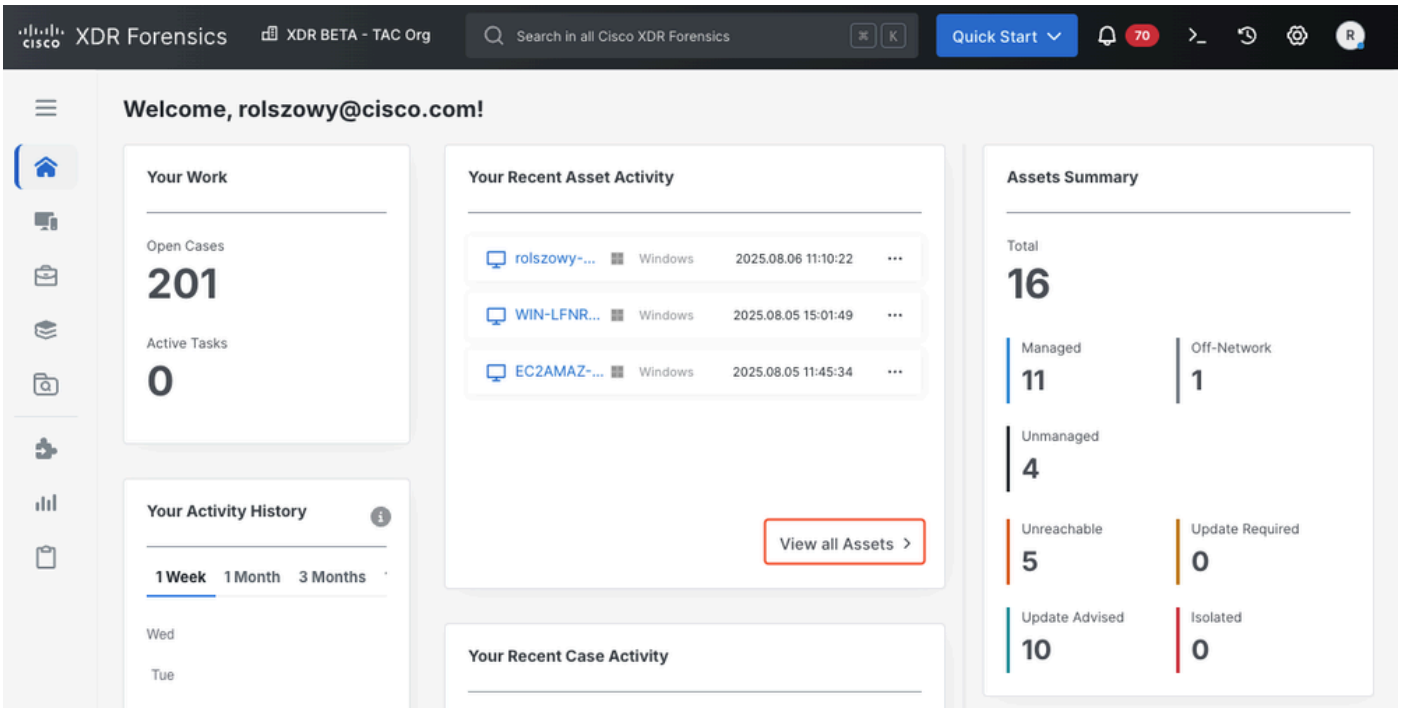
a) Abra CMD en la máquina dada y ejecute el comando hostname.

<#root>

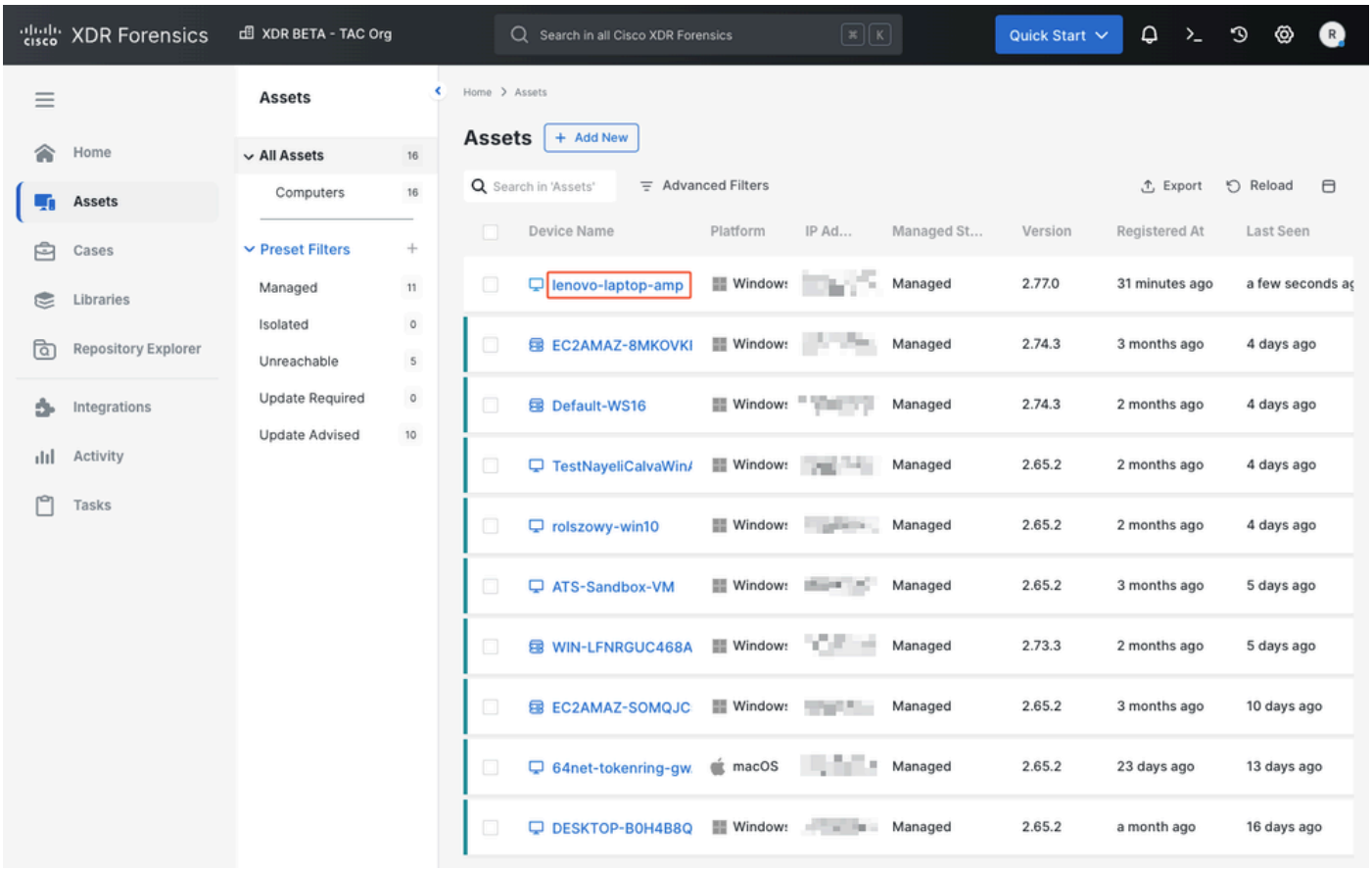
```
C:\Users\Admin\
hostname

lenovo-laptop-amp
```

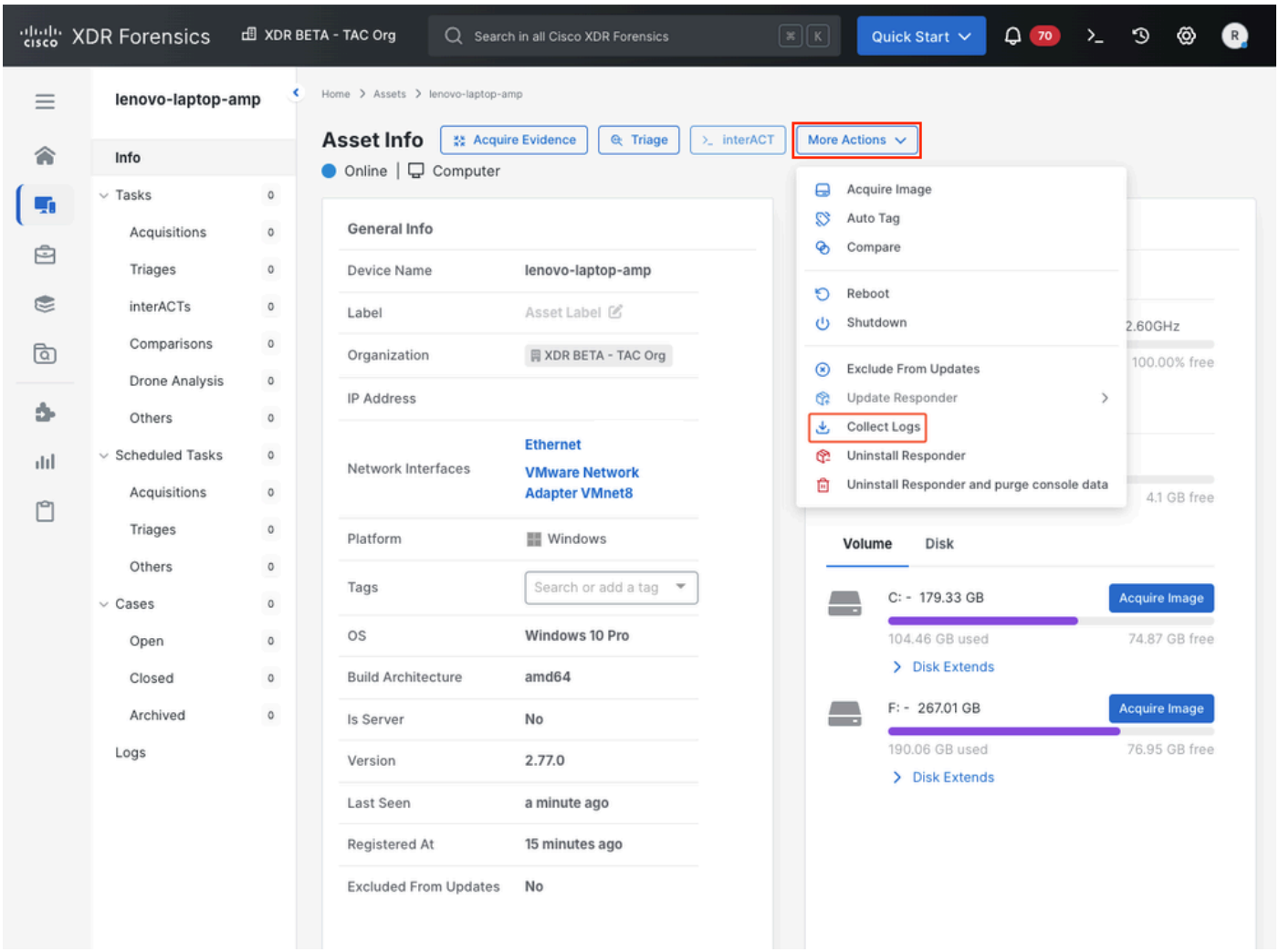
b) En la página principal de la consola de XDR Forensics, haga clic en Ver todos los recursos (o utilice el menú Activos a la izquierda).

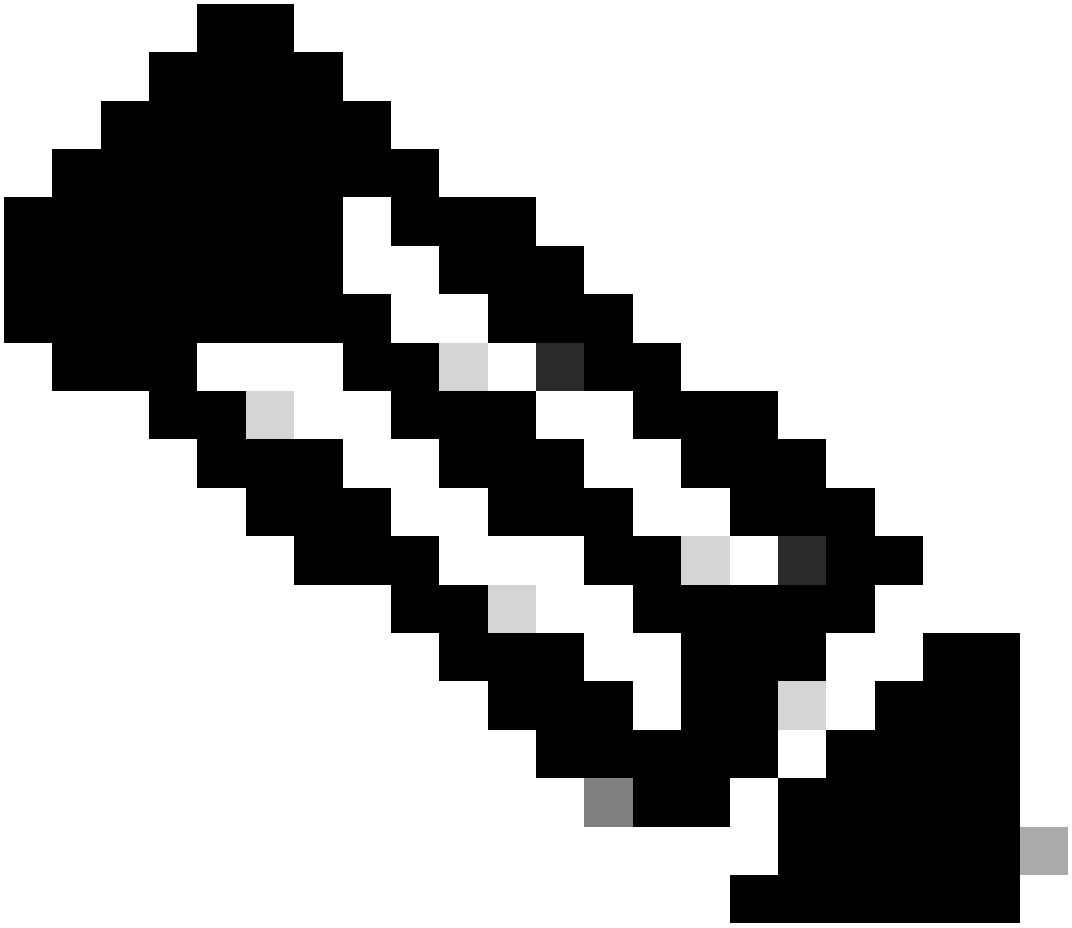


c) Localice el terminal de la lista y haga clic en el Nombre del dispositivo para introducir sus detalles.



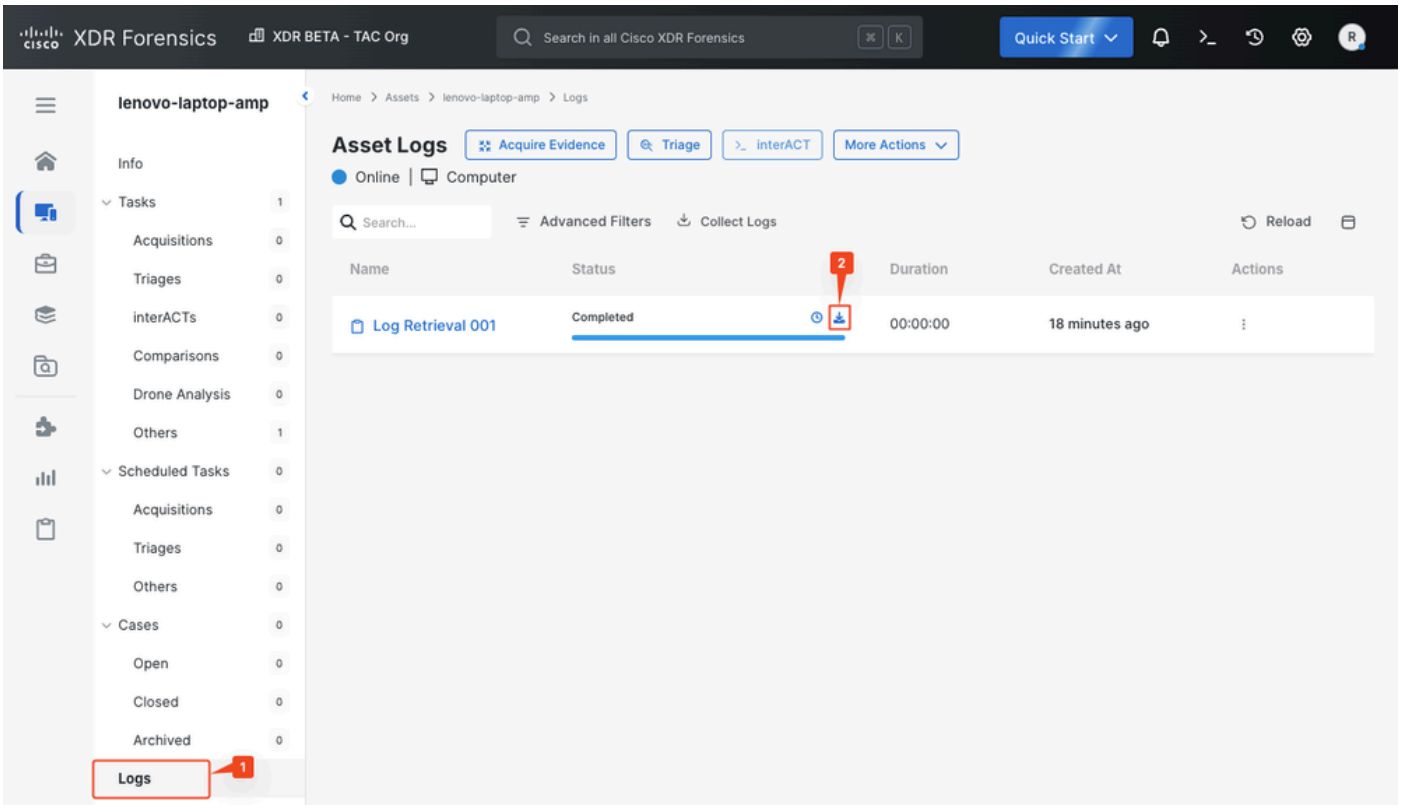
Paso 3. En la página Información de activo, haga clic en Más acciones > Recopilar registros para empezar a recopilar información del terminal.


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: Si el recurso está en línea, se tardará unos segundos en completarlo.

Paso 4. Vaya a la sección Registros para ver si los registros ya se han recopilado. En la sección Registros de activos, haga clic en el icono para iniciar la descarga de registros.

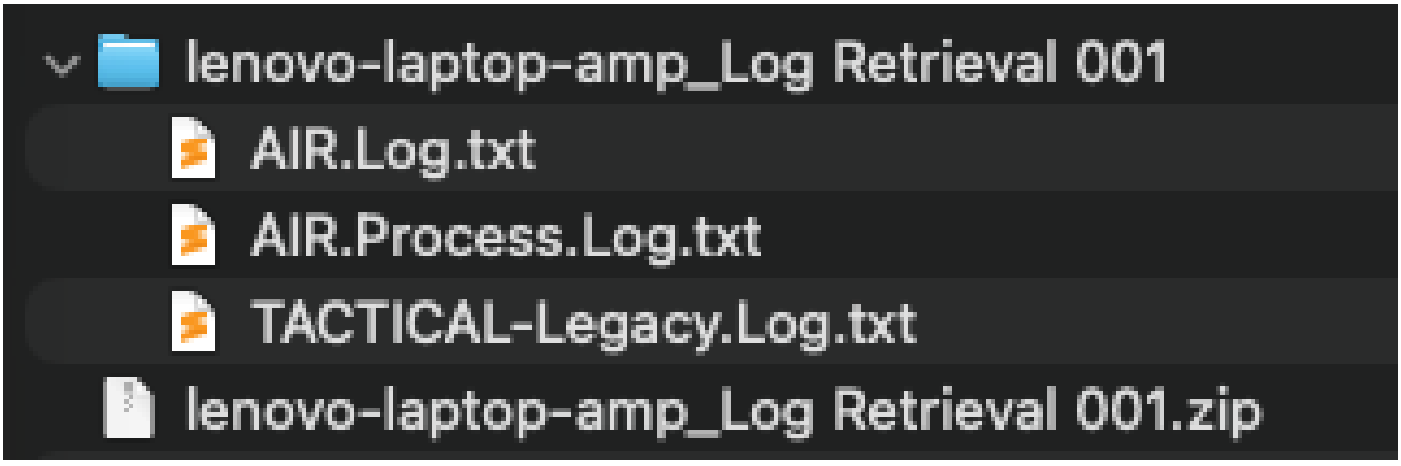


Paso 5. El archivo *.zip adquirido contiene tres archivos necesarios para resolver problemas del módulo:

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).