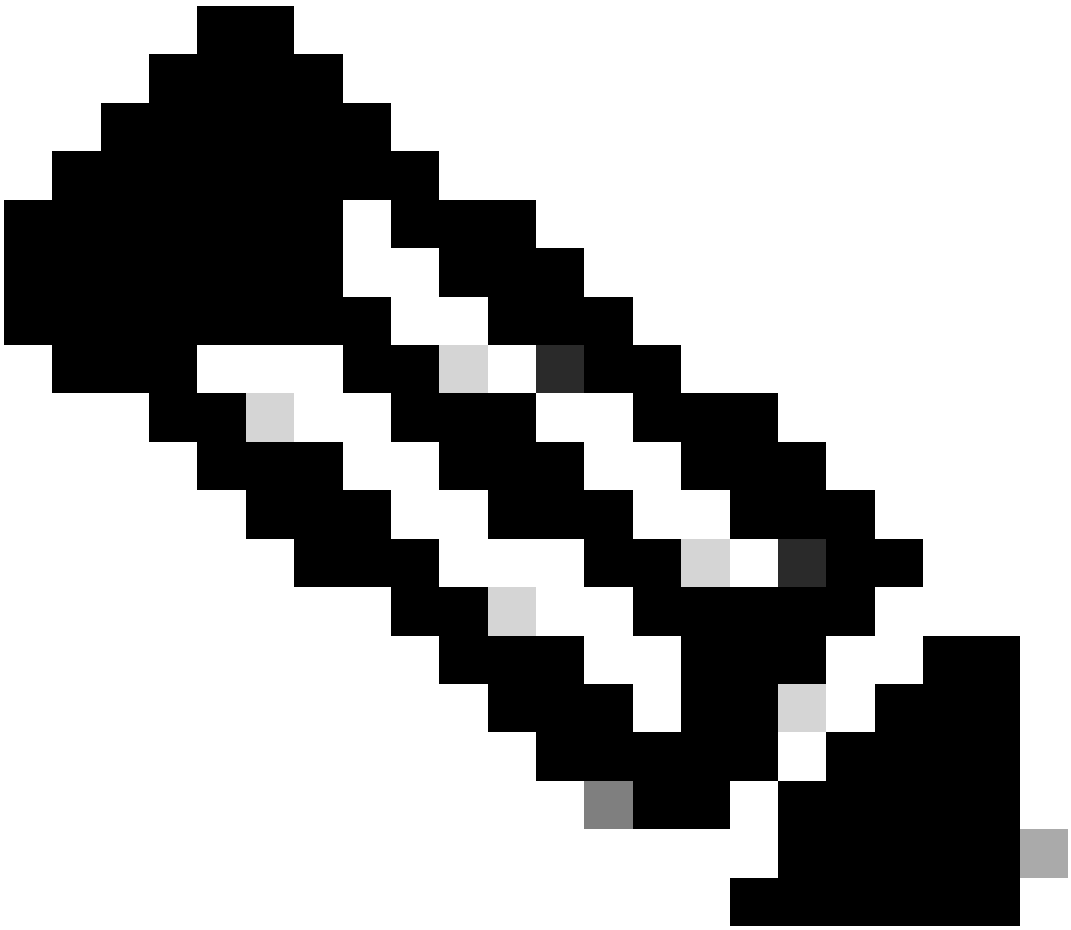
Coletar Logs para o Módulo Forensics XDR

Contents

Introdução

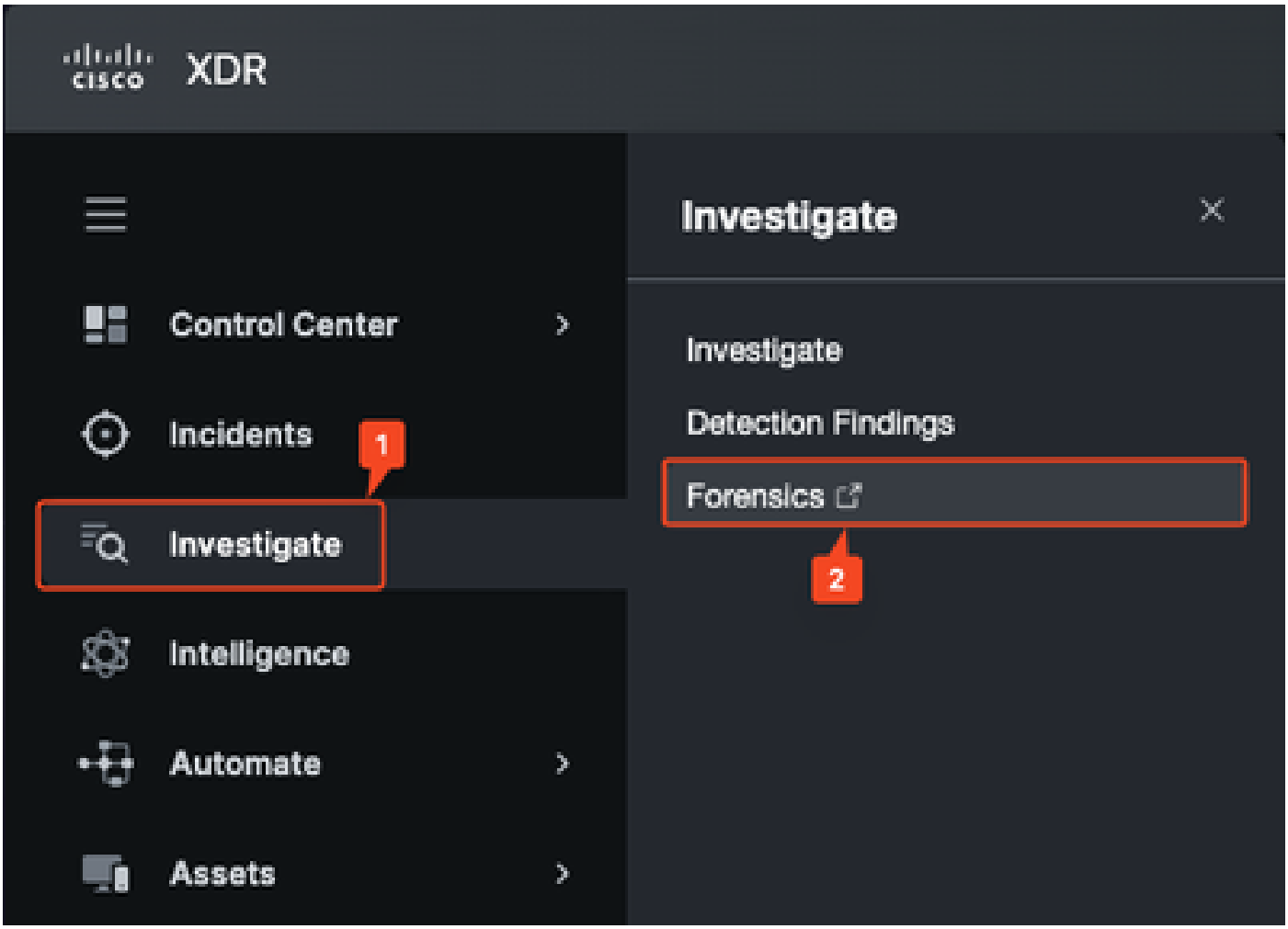
Este documento descreve como buscar dados de diagnóstico remotamente para solucionar problemas do módulo XDR Forensics em seu console.

Buscando logs remotamente



Note: Atualmente, os logs do DART não contêm logs do XDR Forensics.

Etapa 1. Abra o XDR e navegue até o console Investigar > Forensics.



Etapa 2. Verifique se o nome de host do ponto final está visível na página Ativos navegando até a página Ativos. Para fazer isso:

a) Abra o CMD na máquina especificada e execute o comando hostname.

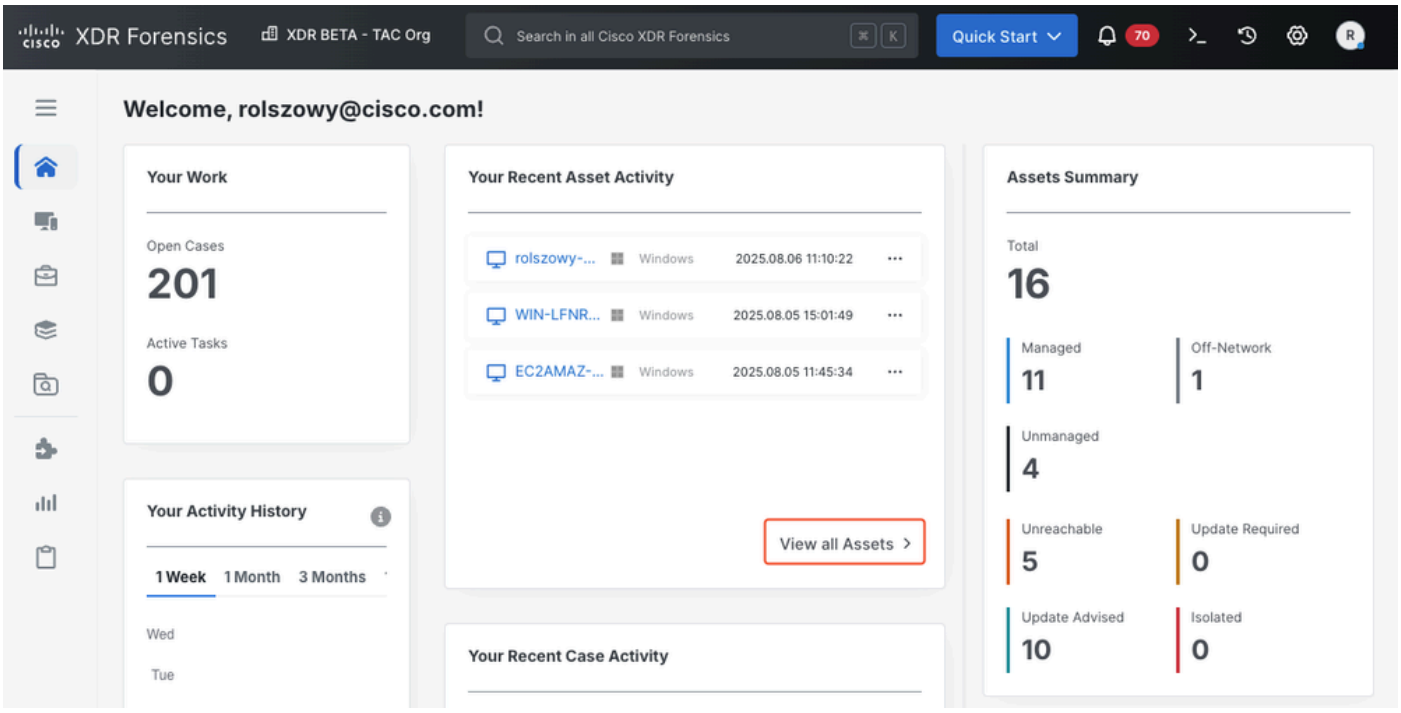
<#root>

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

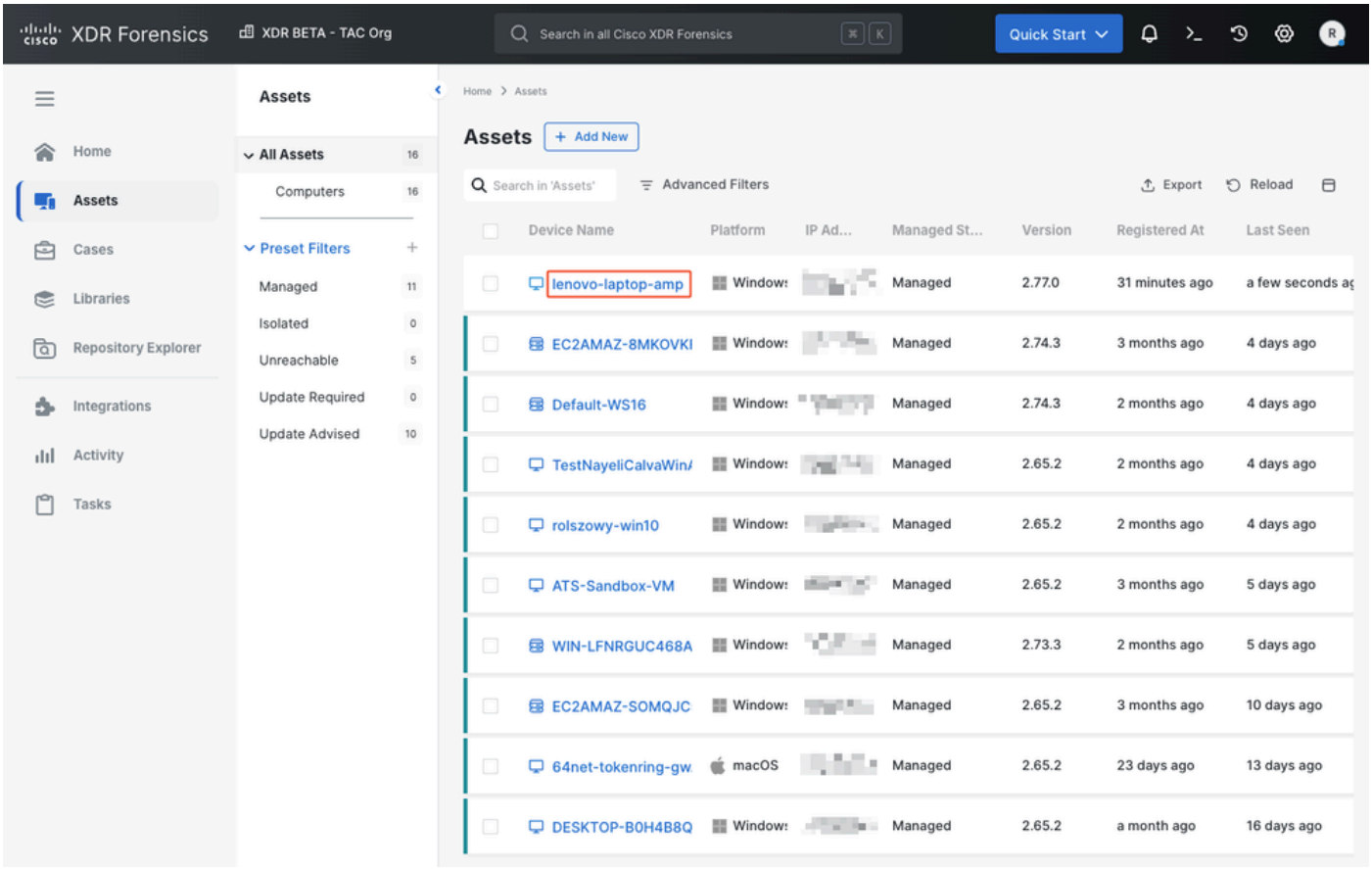
hostname

```
lenovo-laptop-amp
```

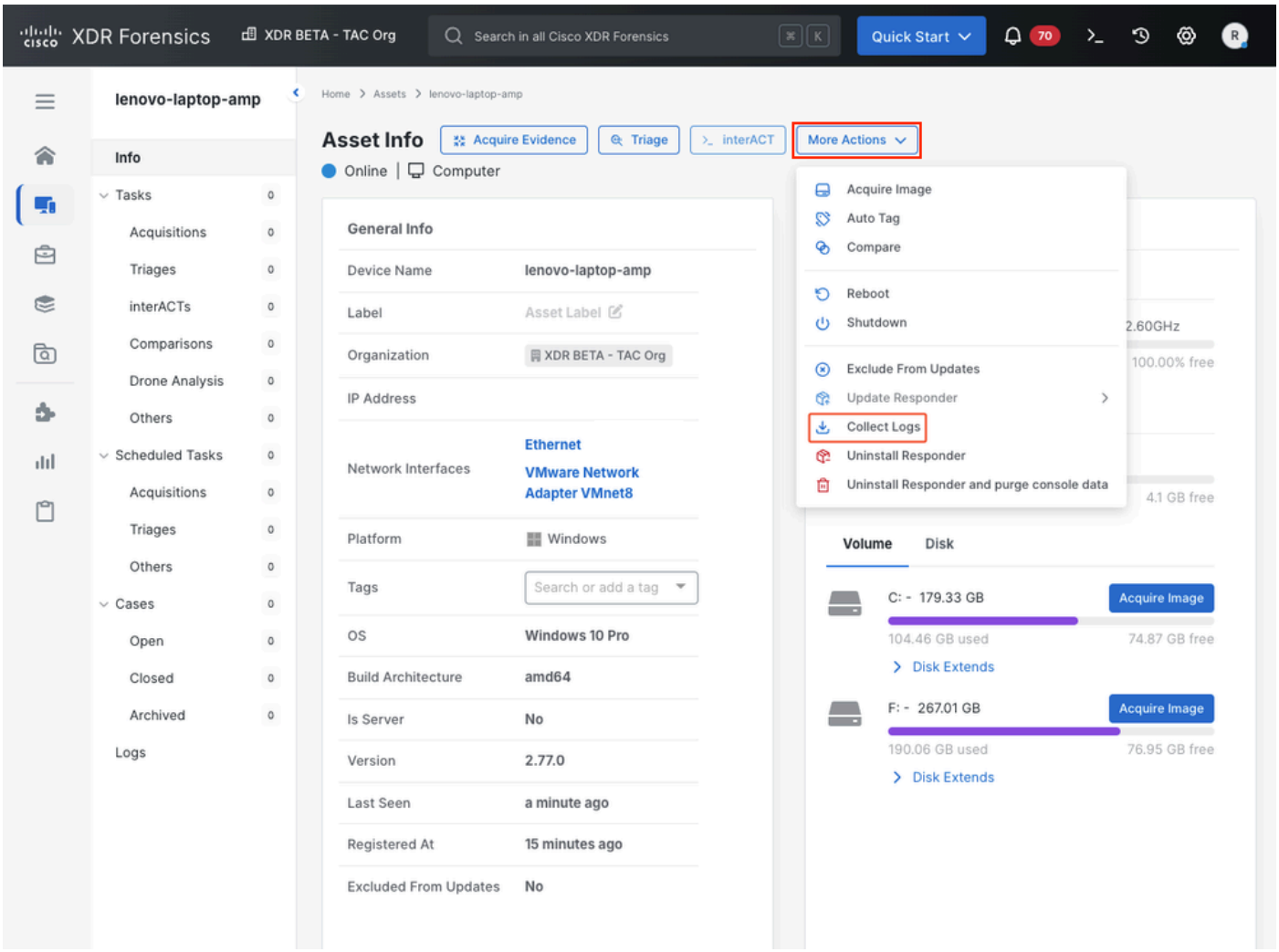
b) Na página principal do console do XDR Forensics, clique em View all Assets (ou use o menu Assets à esquerda).

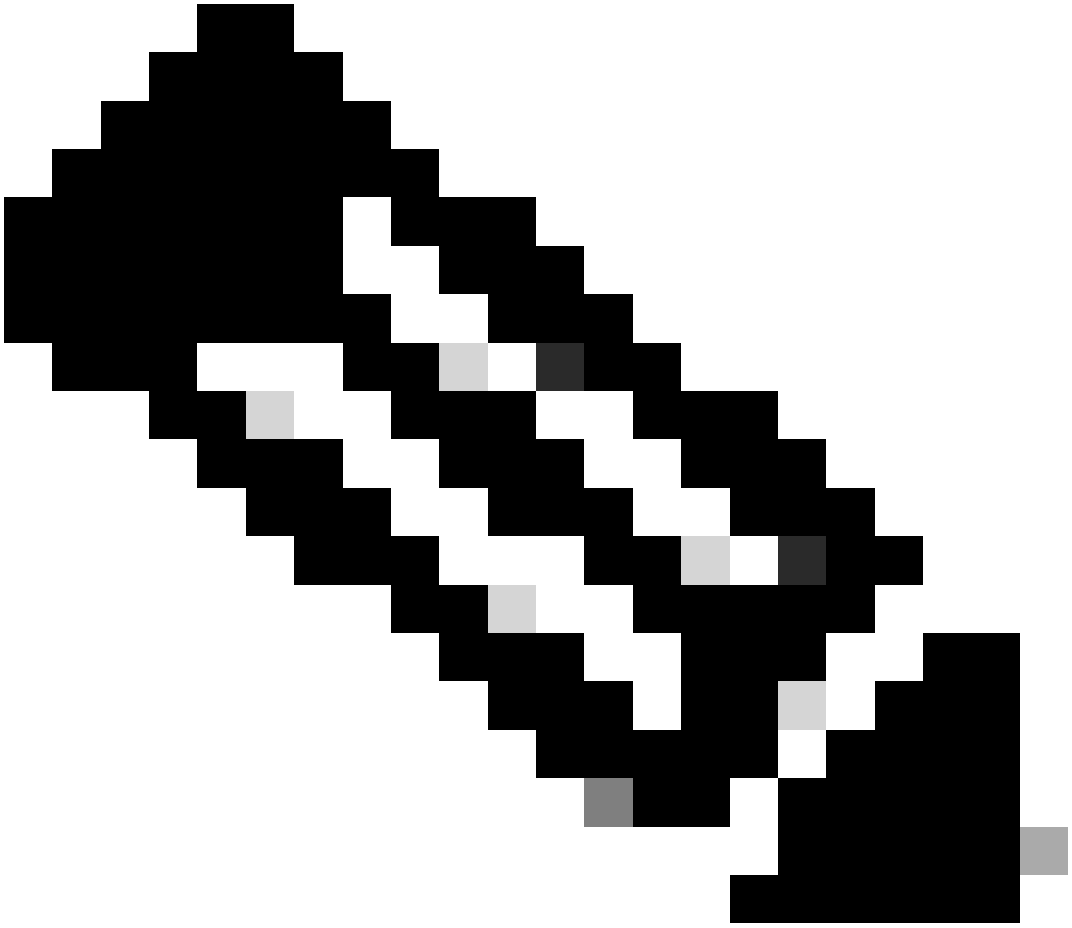


c) Localize o endpoint na lista e clique no Nome do dispositivo para inserir seus detalhes.



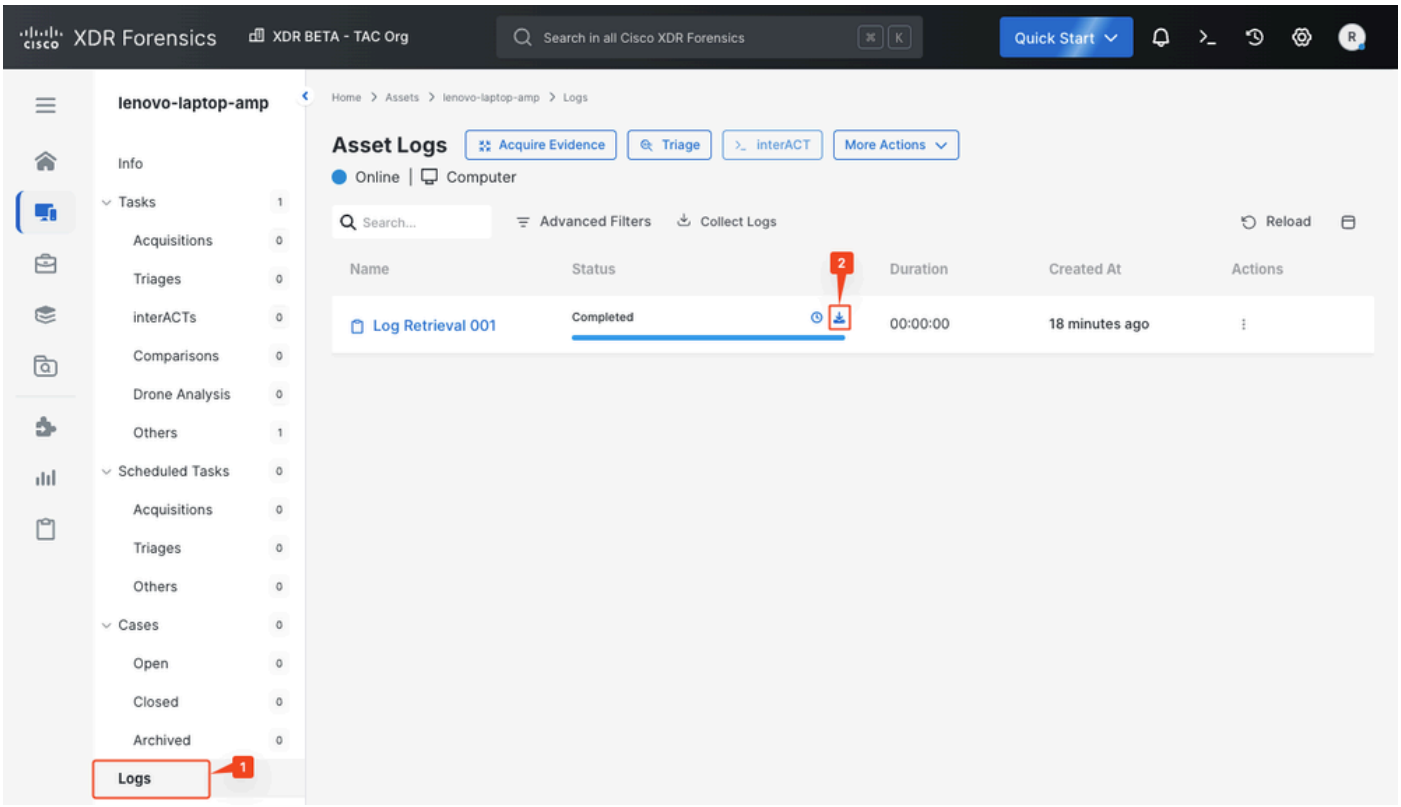
Etapa 3. Na página Informações do ativo, clique em Mais ações > Coletar logs para iniciar a coleta de informações do ponto final.


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



Note: Se o ativo estiver on-line, isso levará alguns segundos para ser concluído.

Etapa 4. Vá até a seção Logs para ver se os logs já foram coletados. Na seção Logs de ativos, clique no ícone para iniciar o download dos logs.

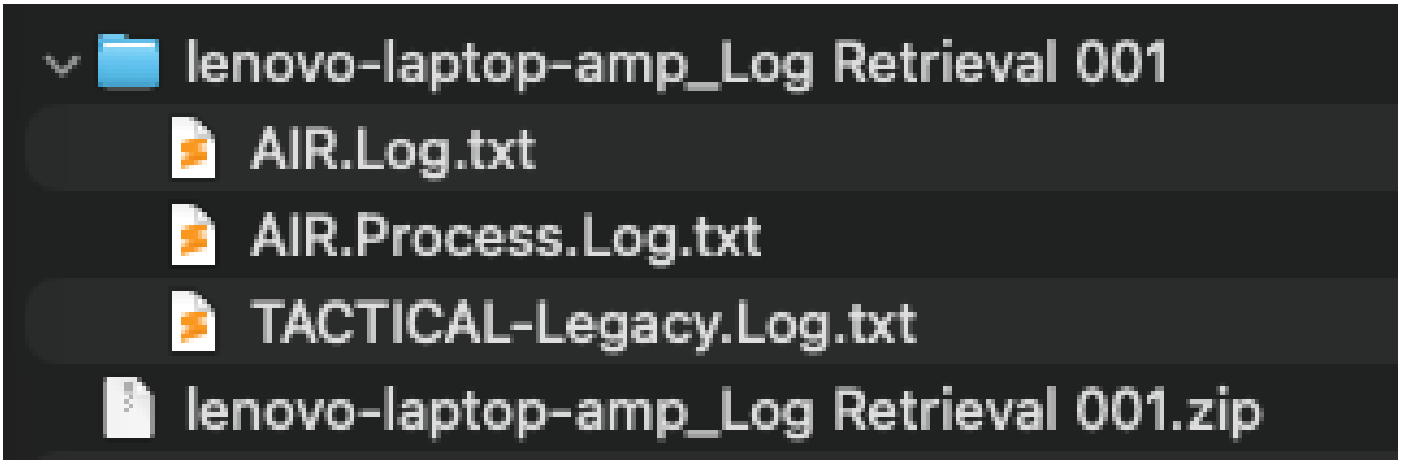


Etapa 5. O arquivo *.zip adquirido contém três arquivos necessários para solucionar problemas do módulo:

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.