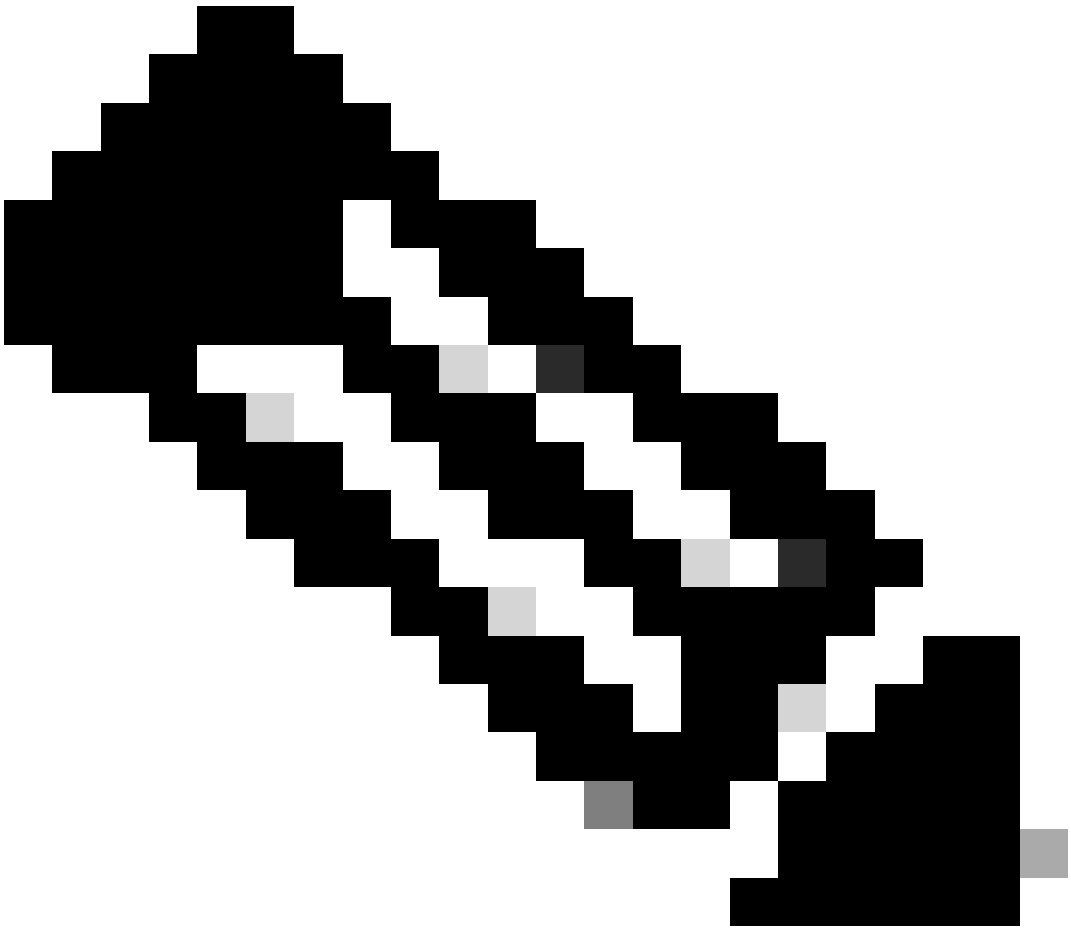
XDR調査モジュールのログの収集

内容

はじめに

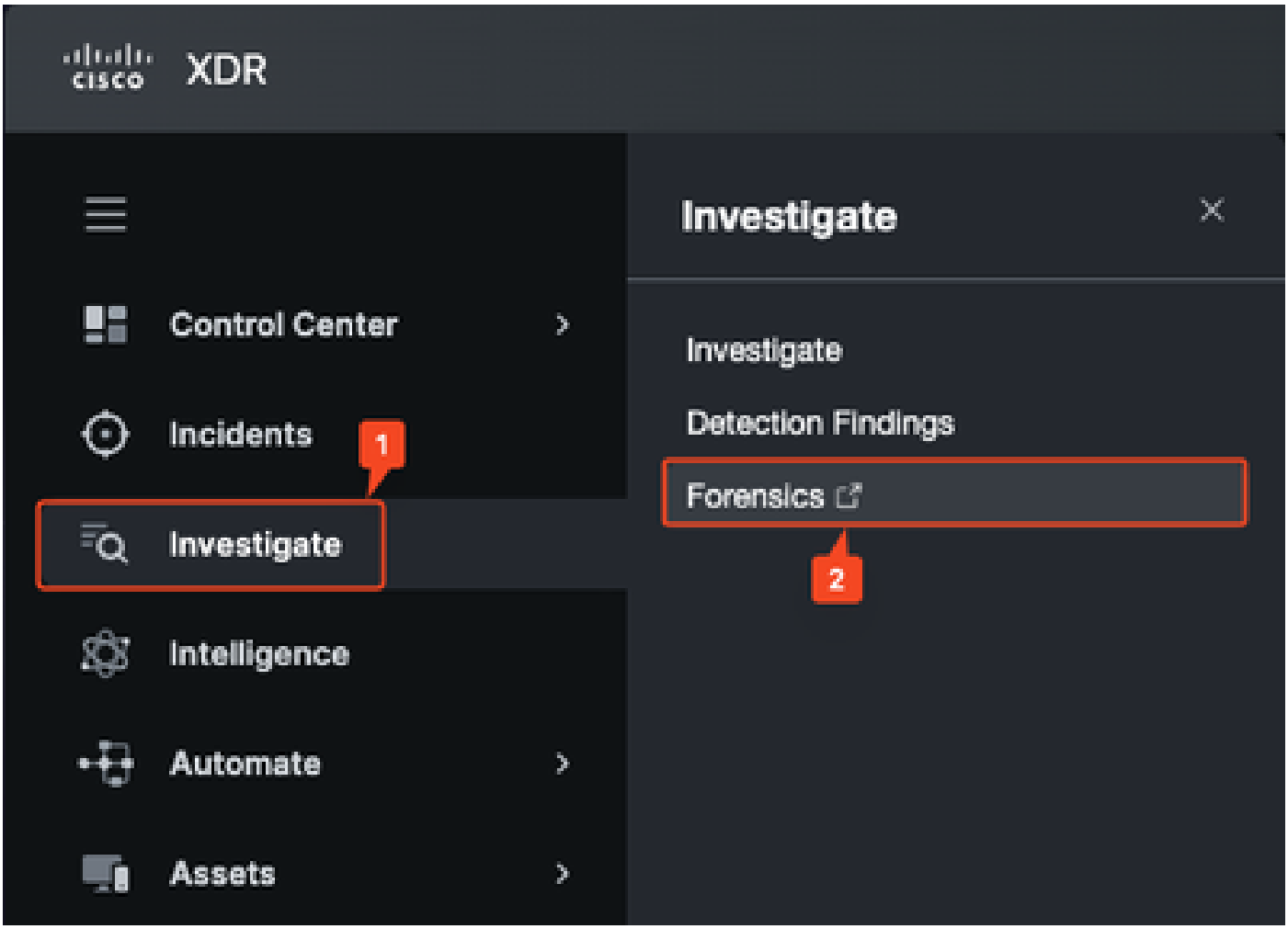
このドキュメントでは、コンソールでXDR調査モジュールをトラブルシューティングするために診断データをリモートで取得する方法について説明します。

リモートからのログのフェッチ



注：現在、DARTログにはXDR調査ログは含まれていません。

ステップ 1：XDRを開き、Investigate > Forensicsコンソールに移動します。



ステップ 2：Assetsページに移動して、エンドポイントのホスト名が「Assets」ページに表示されることを確認します。これを行うには、

a)指定されたマシン上でCMDを開き、hostnameコマンドを実行します。

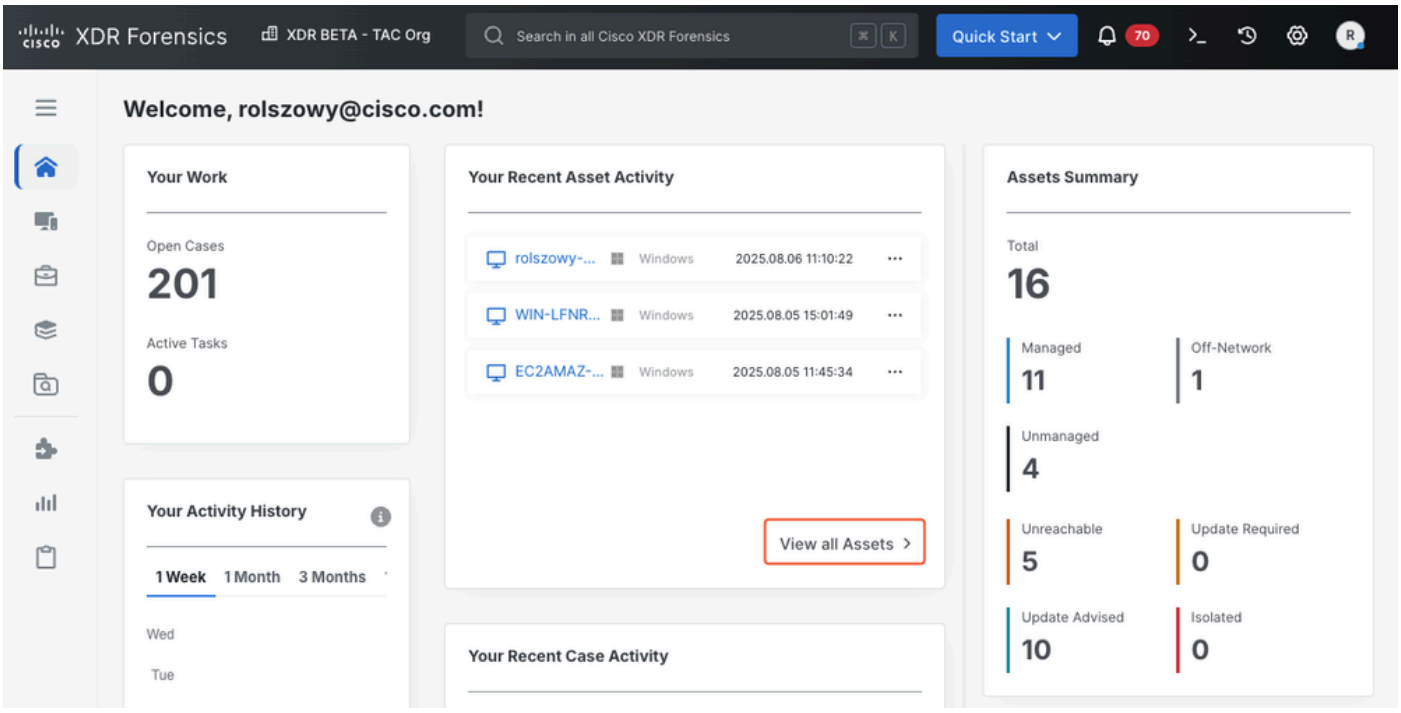
<#root>

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

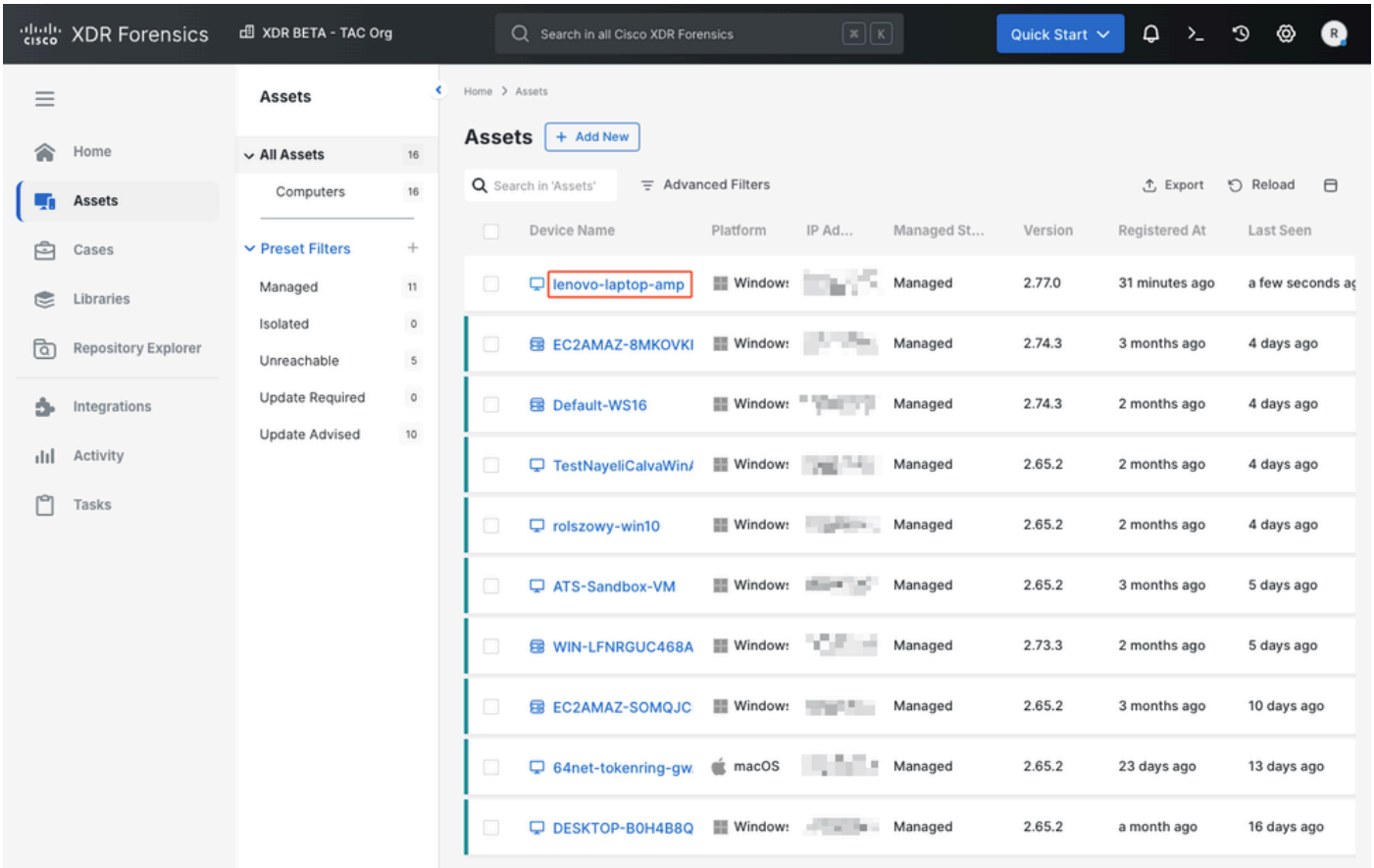
hostname

```
lenovo-laptop-amp
```

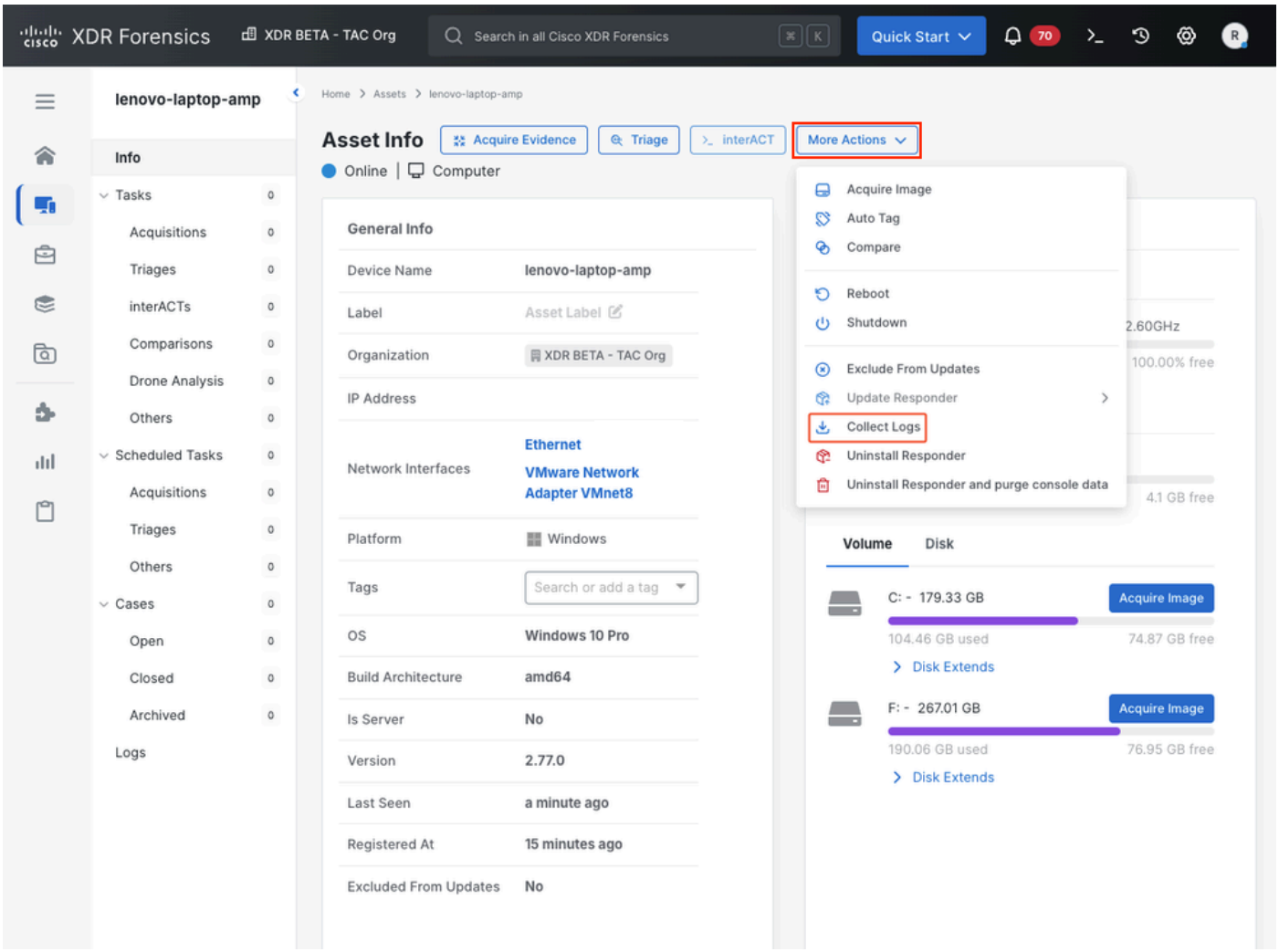
b) XDR Forensicsコンソールのメインページで、View all Assetsをクリックします(または、左側のAssetsメニューを使用)。

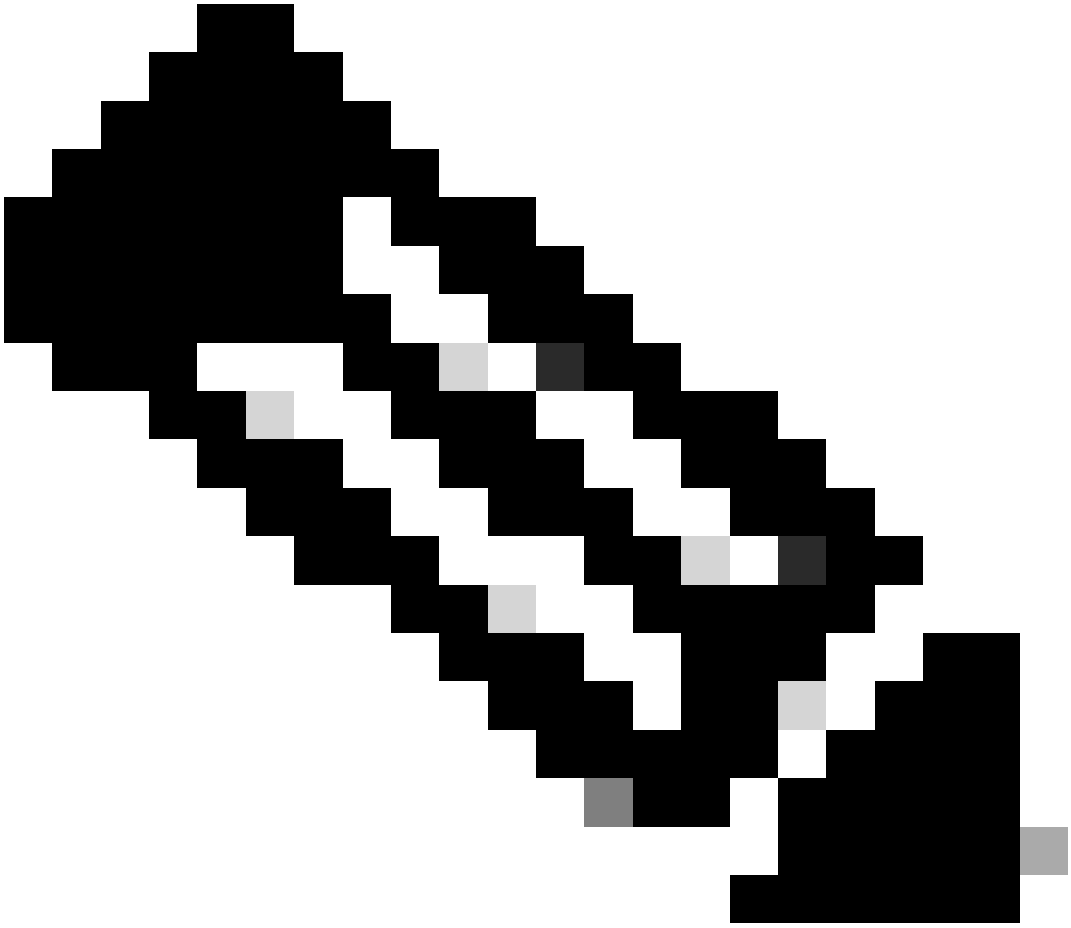


c)リスト上のエンドポイントをローカライズし、デバイス名をクリックして詳細を入力します。



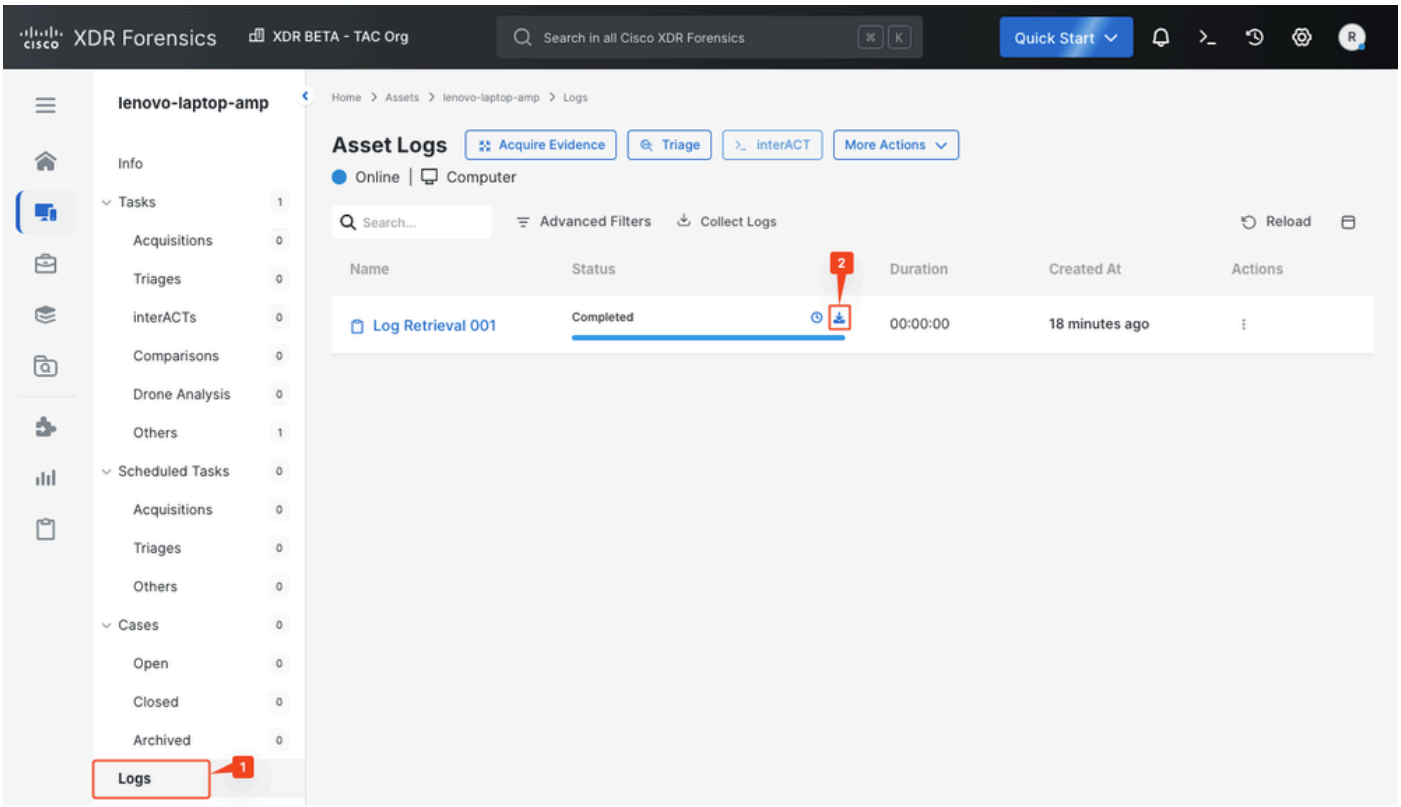
ステップ 3：Asset infoページで、More Actions > Collect Logsの順にクリックして、エンドポイントからの情報の収集を開始します。


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



注：アセットがオンラインの場合、完了までに数秒かかります。

ステップ 4：Logsセクションに移動し、ログがすでに収集されているかどうかを確認します。
Asset Logsセクションで、アイコンをクリックして、ログのダウンロードを開始します。

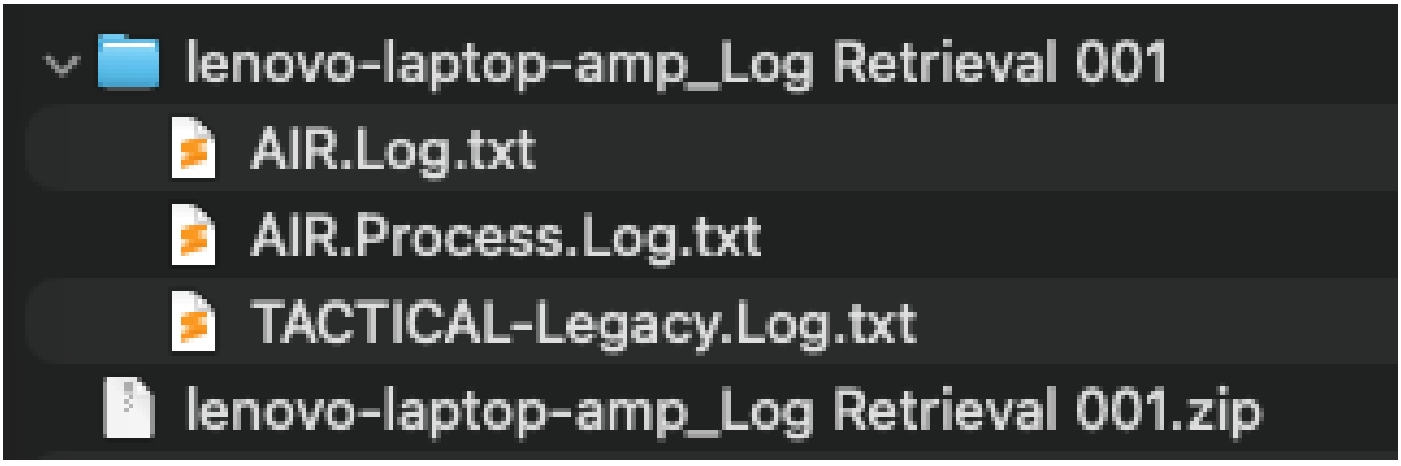


ステップ 5：取得した*.zipファイルには、モジュールのトラブルシューティングに必要な次の3つのファイルが含まれています。

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。