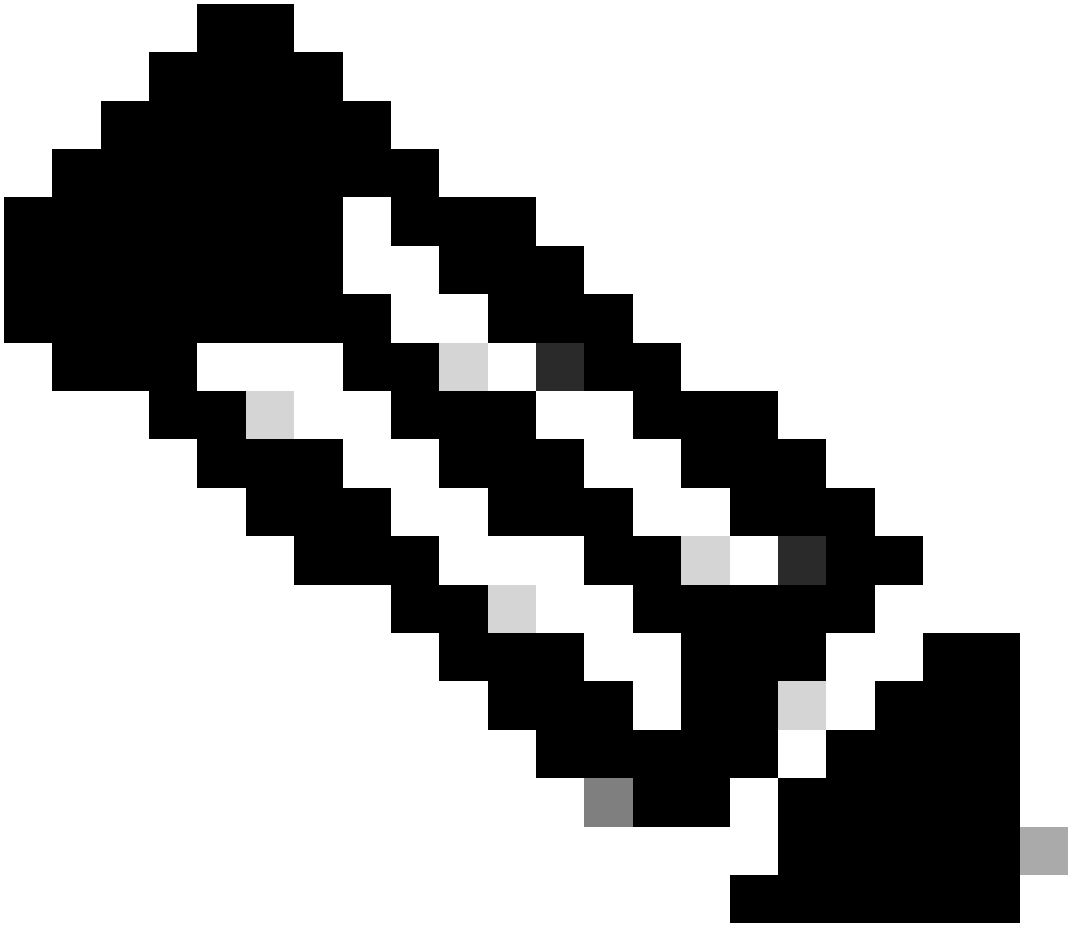
收集XDR调查分析模块的日志

目录

简介

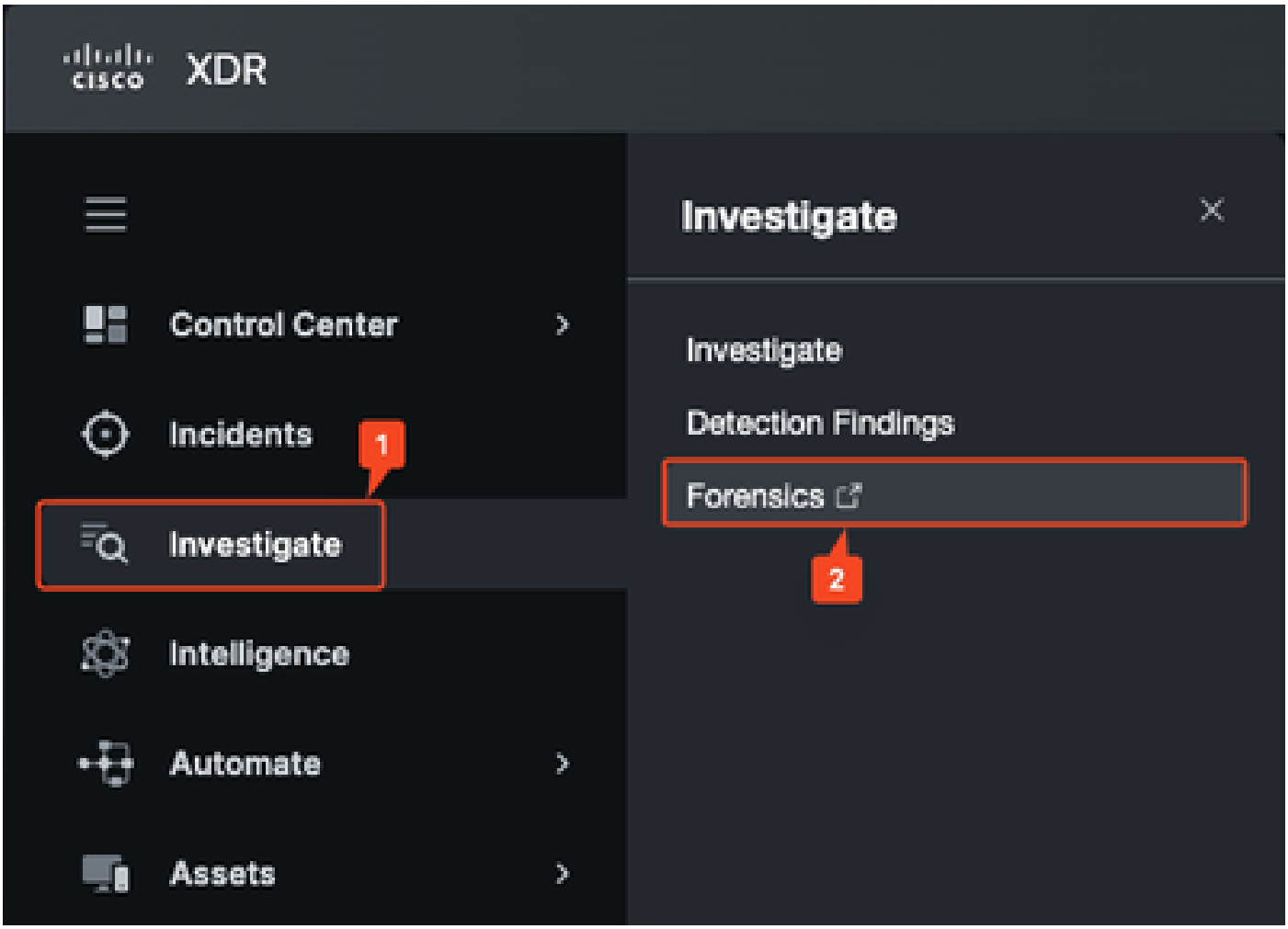
本文档介绍如何远程获取诊断数据以排除XDR调查分析模块在其控制台中的故障。

正在远程获取日志



注意：目前，DART日志不包含XDR调查分析日志。

步骤1.打开XDR并导航到调查>调查分析控制台。



第2步：导航到Assets页面，验证终端的主机名是否显示在Assets页面上。任务:

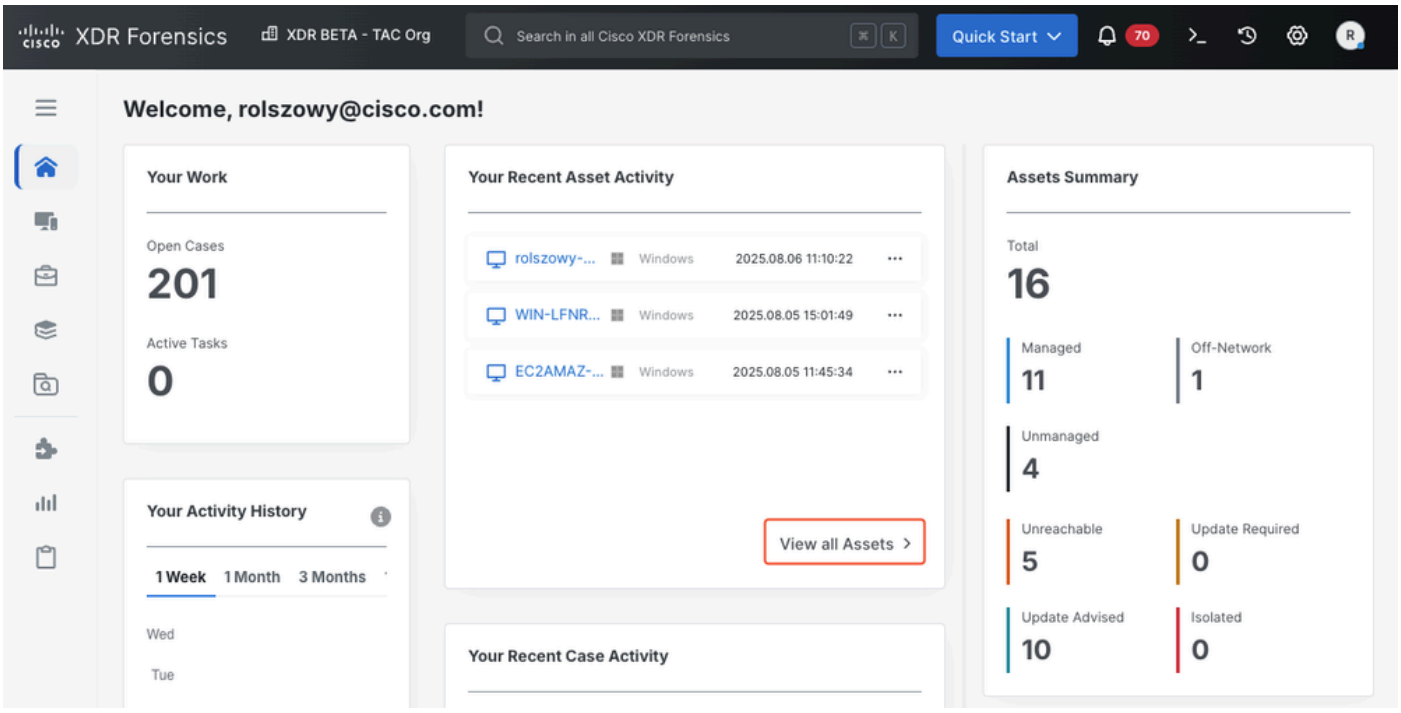
a)在给定计算机上打开CMD并执行hostname命令。

<#root>

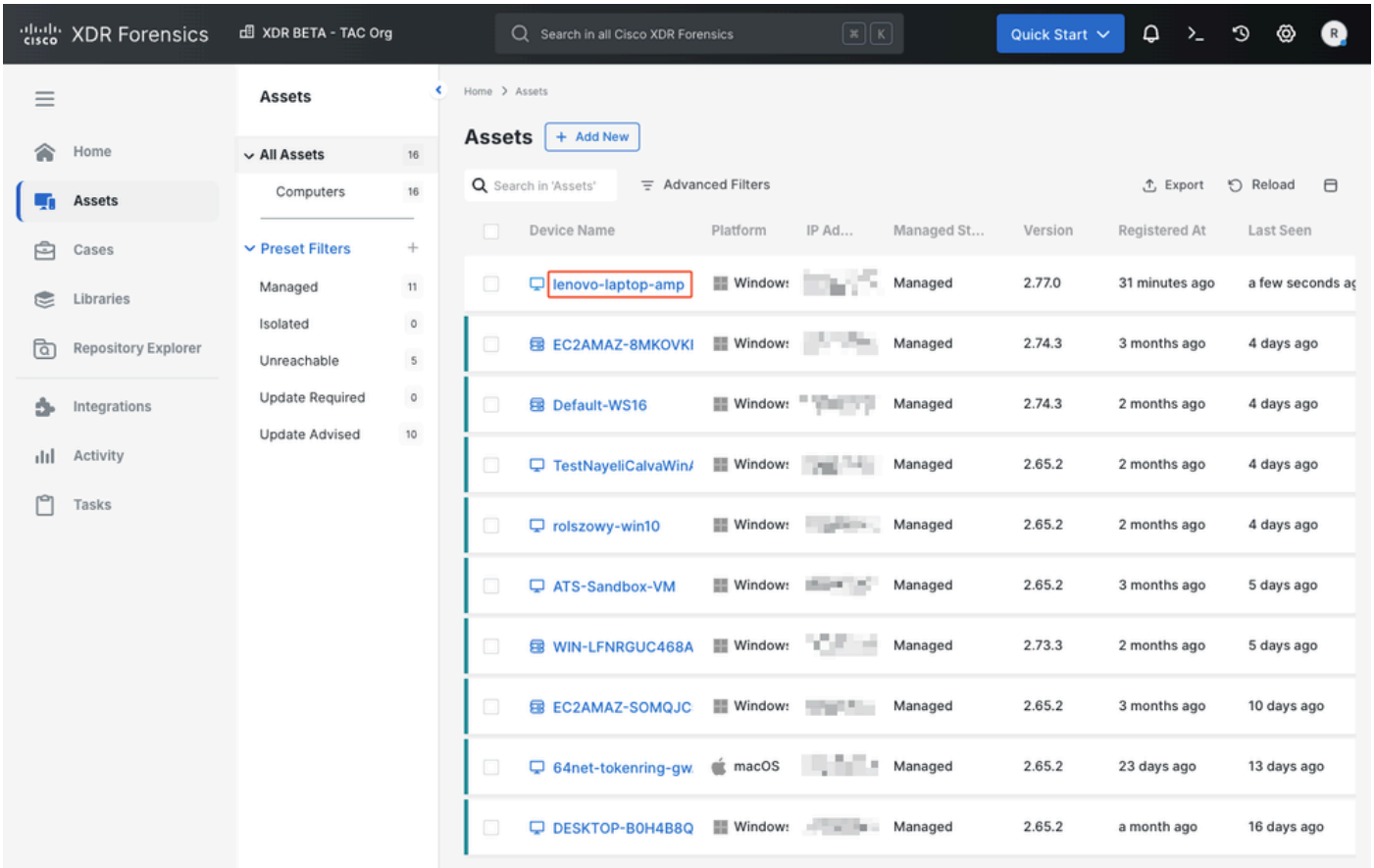
```
C:\Users\Admin\
hostname

lenovo-laptop-amp
```

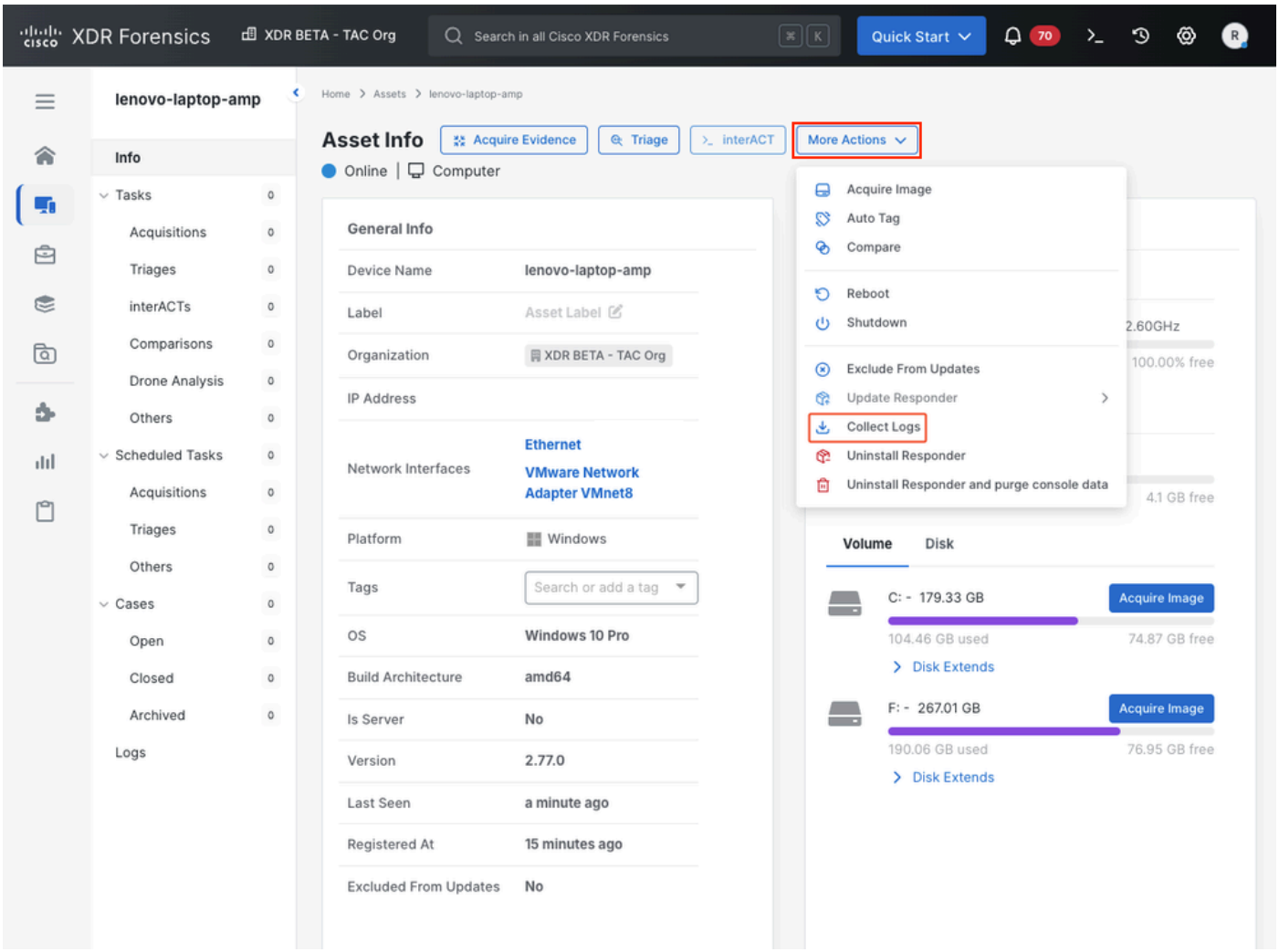
b)在XDR Forensics控制台主页中，单击View all Assets(或使用左侧的Assets菜单)。

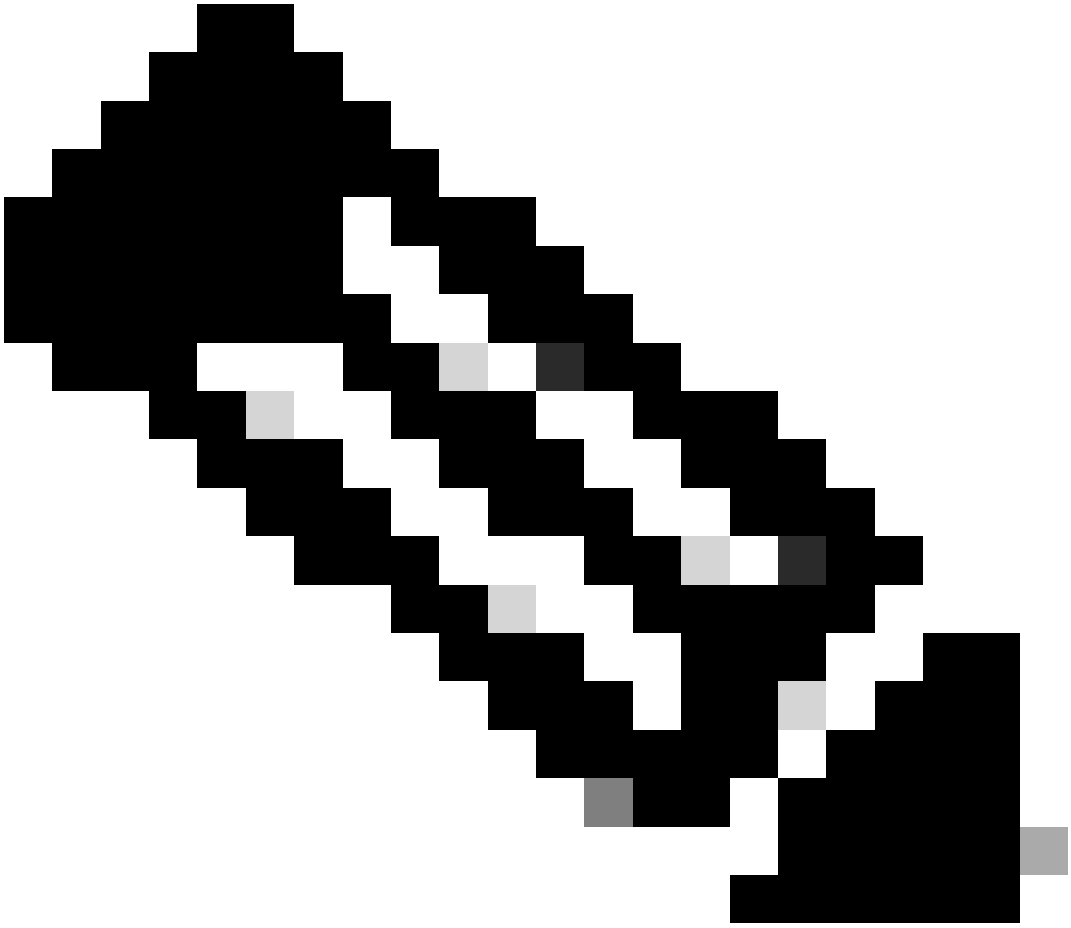


c)本地化列表上的终端，然后单击Device name输入其详细信息。



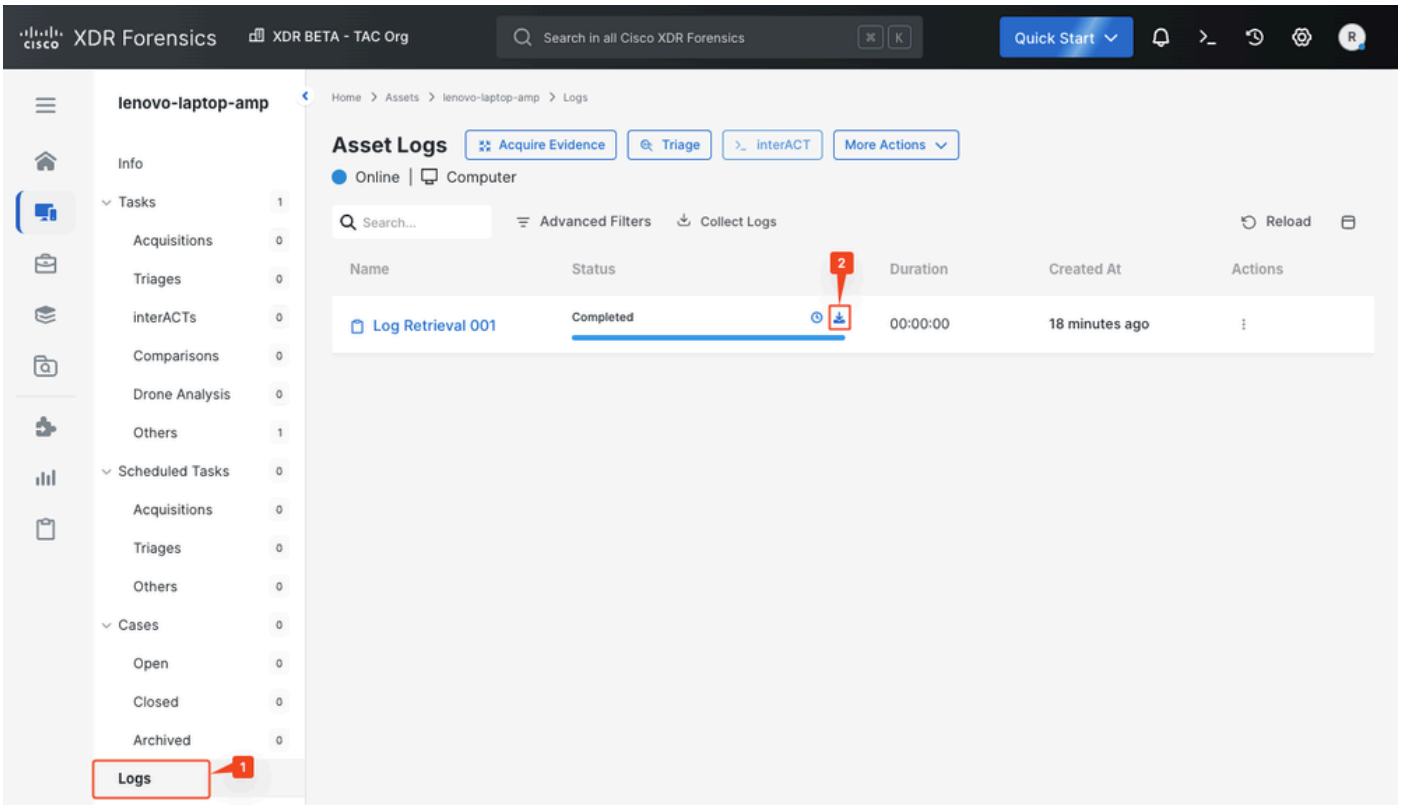
第3步：在Asset info页面中，点击More Actions > Collect Logs，开始从终端收集信息。


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



注意：如果资产处于联机状态，则需要几秒钟才能完成。

步骤4.转至日志部分以查看是否已收集日志。在资产日志部分，单击图标开始下载日志。

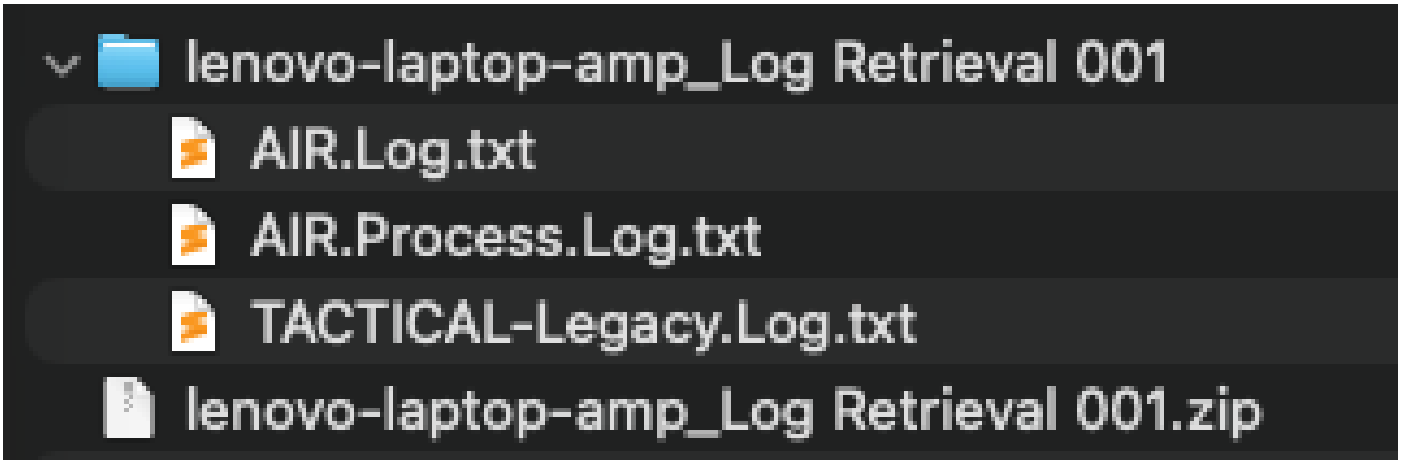


步骤5.获得的*.zip文件包含对模块进行故障排除所需的三个文件：

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。