

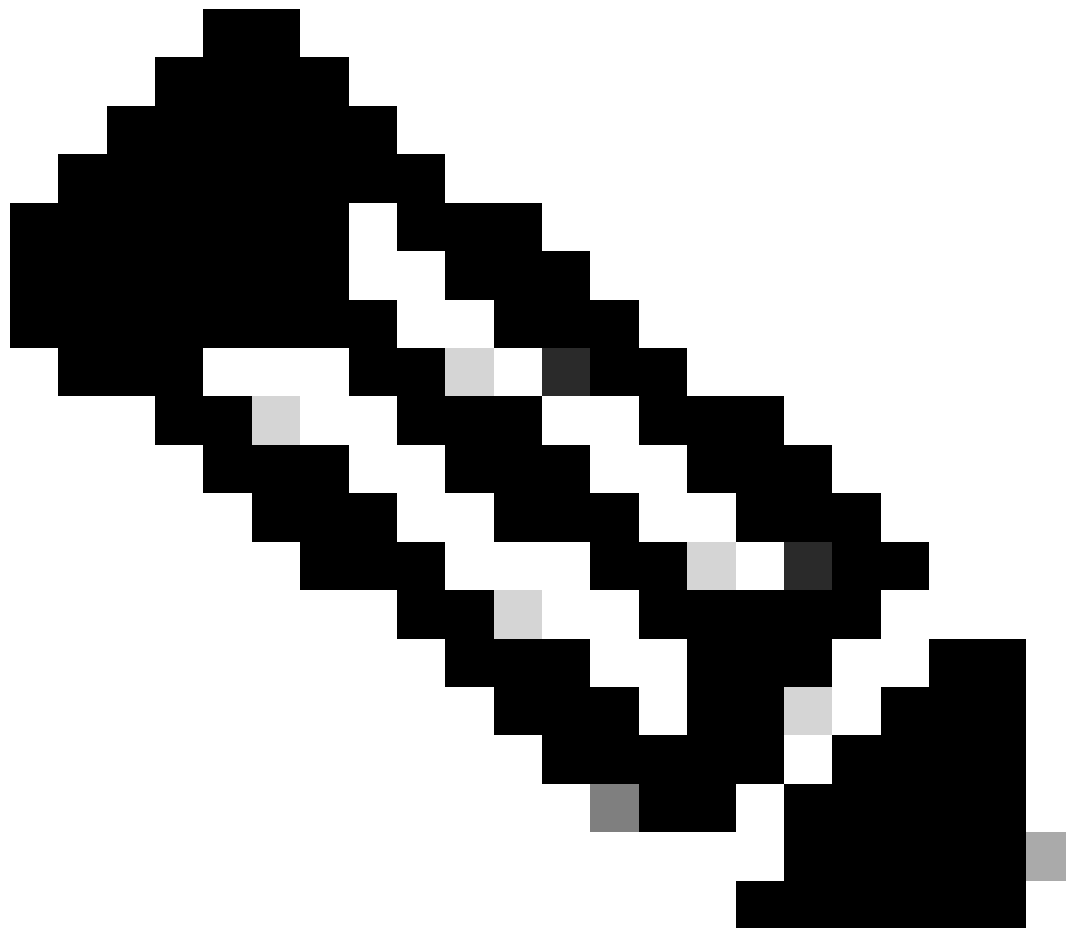
Collect Logs for the XDR Forensics Module

Contents

Introduction

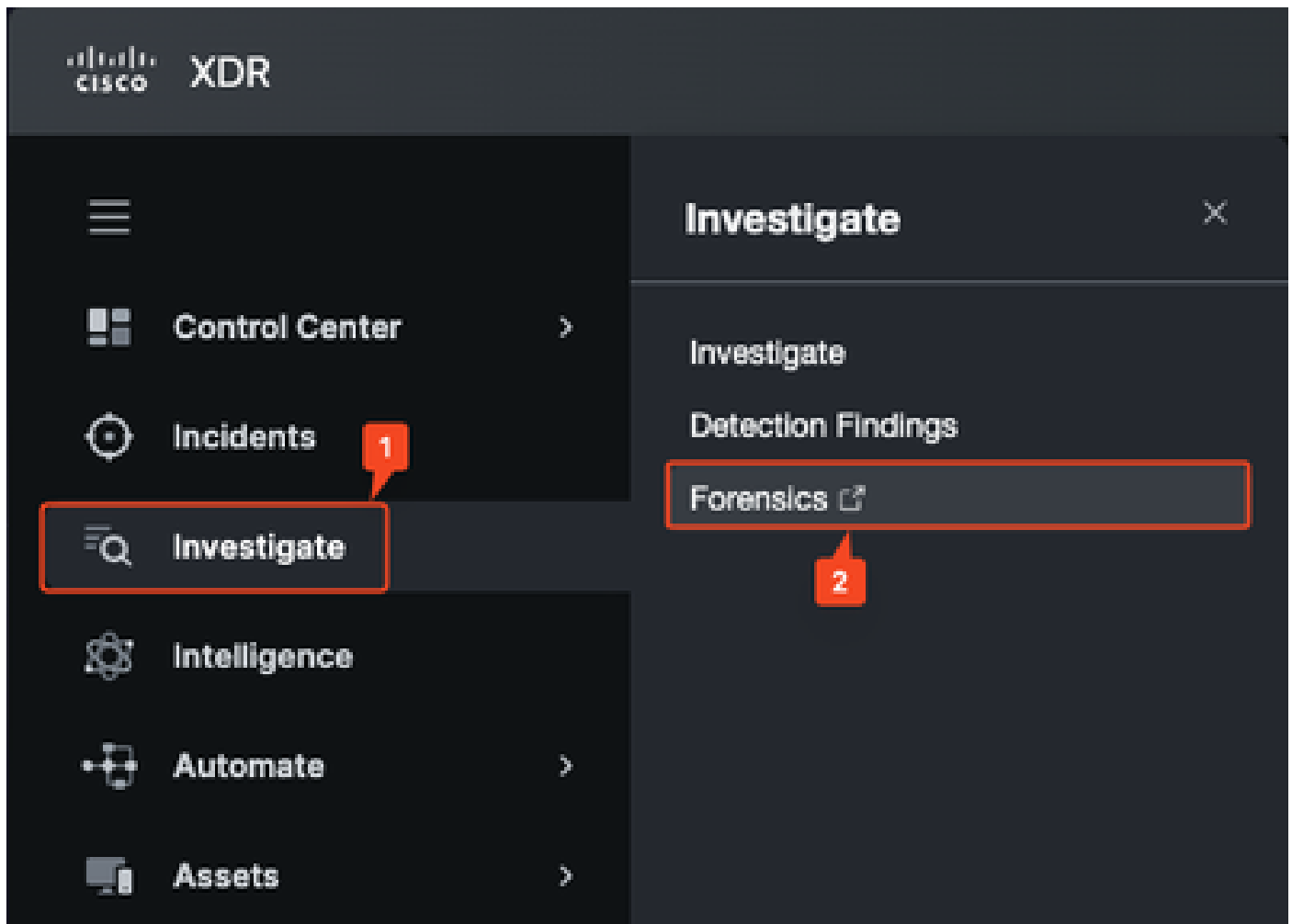
This document describes how to remotely fetch diagnostic data to troubleshoot the XDR Forensics module in its console.

Fetching logs remotely



Note: Currently, DART logs do not contain XDR Forensics logs.

Step 1. Open XDR and navigate to **Investigate > Forensics** console.



Step 2. Verify the hostname of the endpoint is visible on the Assets page by navigating to **Assets** page. To do this:

a) Open CMD on the given machine and execute **hostname** command.

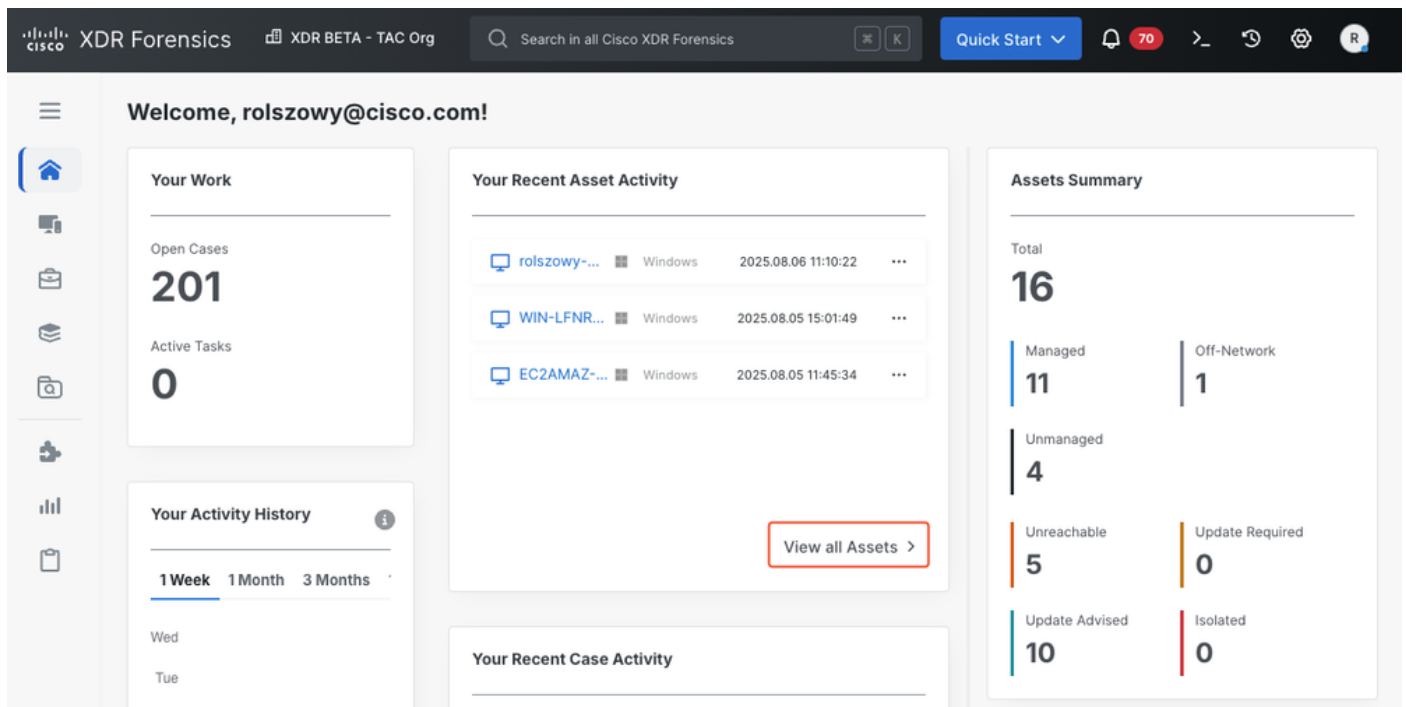
```
<#root>
```

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

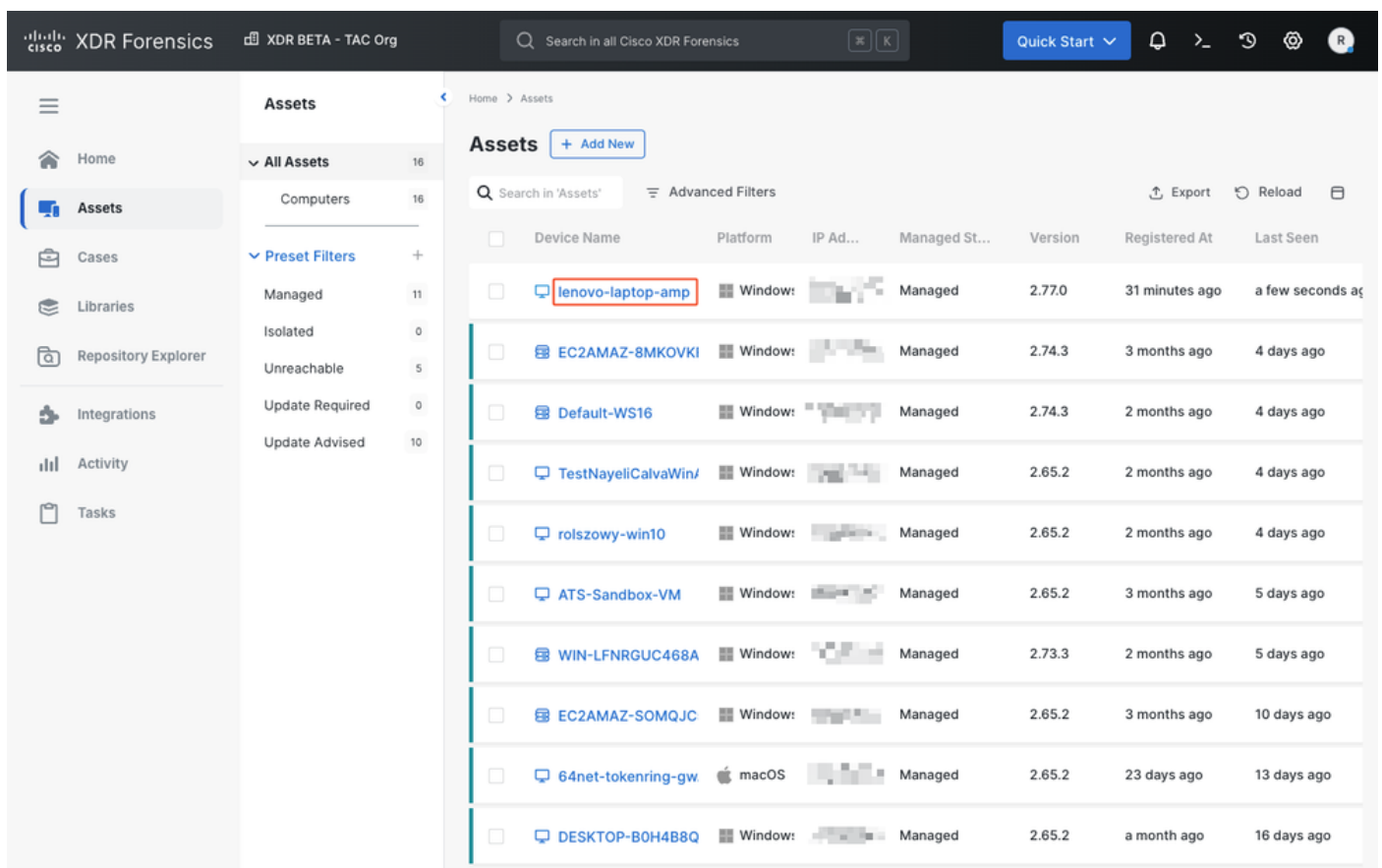
```
hostname
```

```
lenovo-laptop-amp
```

b) In **XDR Forensics** console main page click **View all Assets** (or use **Assets** menu on the left).



c) Localize the endpoint on the list and click the **Device name** to enter its details.



Step 3. In the Asset info page, click **More Actions > Collect Logs** to start gathering information from the endpoint.

lenovo-laptop-amp

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

Info

Tasks

Acquisitions

Triages

interACTs

Comparisons

Drone Analysis

Others

Scheduled Tasks

Acquisitions

Triages

Others

Cases

Open

Closed

Archived

Logs

Acquire Image

Auto Tag

Compare

Reboot

Shutdown

Exclude From Updates

Update Responder

Collect Logs

Uninstall Responder

Uninstall Responder and purge console data

Volume

Disk

C: - 179.33 GB

104.46 GB used

74.87 GB free

Acquire Image

F: - 267.01 GB

190.06 GB used

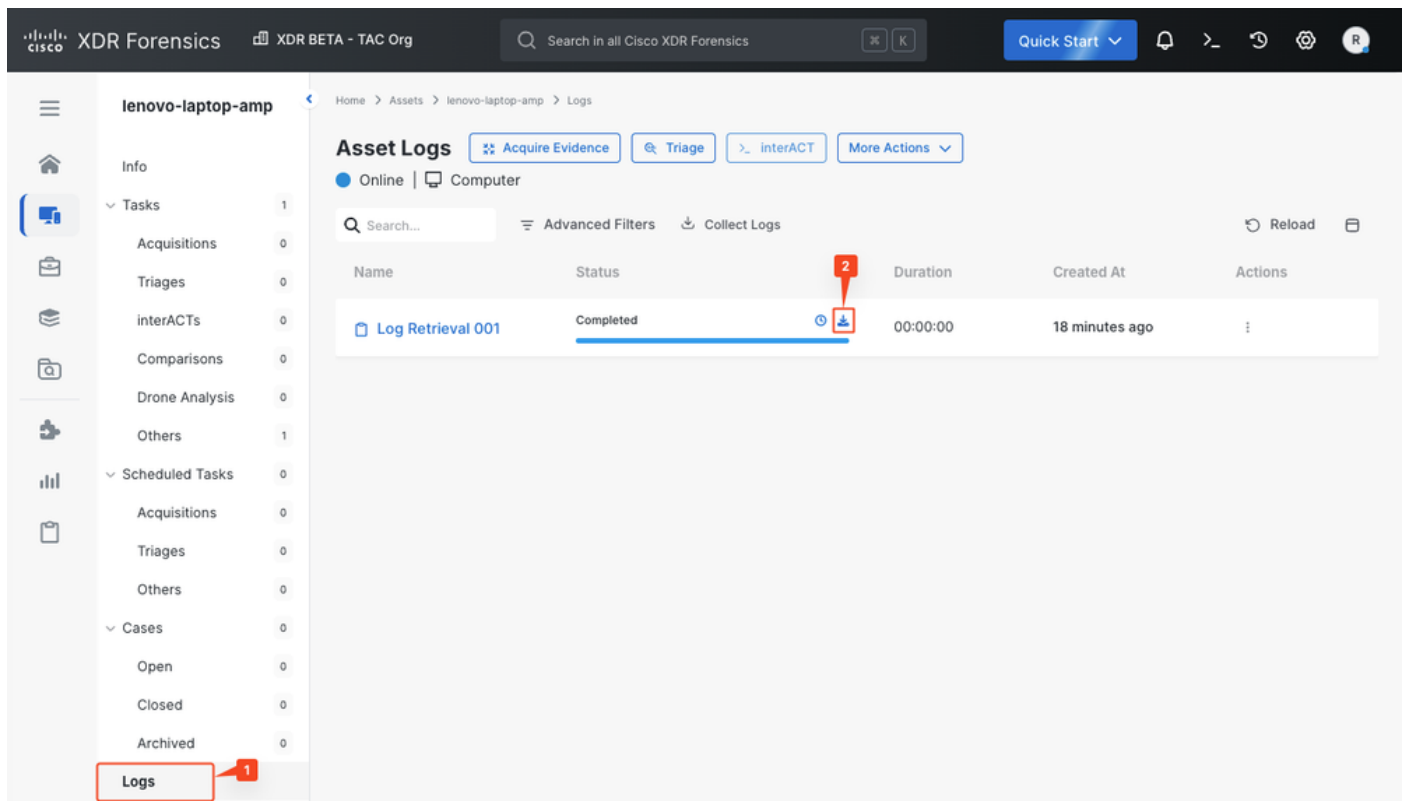
76.95 GB free

Acquire Image



Note: If the asset is online, this takes a few seconds to complete.

Step 4. Go to **Logs** section to see if logs has been gathered already. In **Asset Logs** section, click the **icon** to start logs download.



Step 5. Acquired *.zip file contains three files required to troubleshoot the module:

- AIR.Log.txt
- AIR.Process.Log.txt
- TACTICAL-Legacy.Log.txt

