

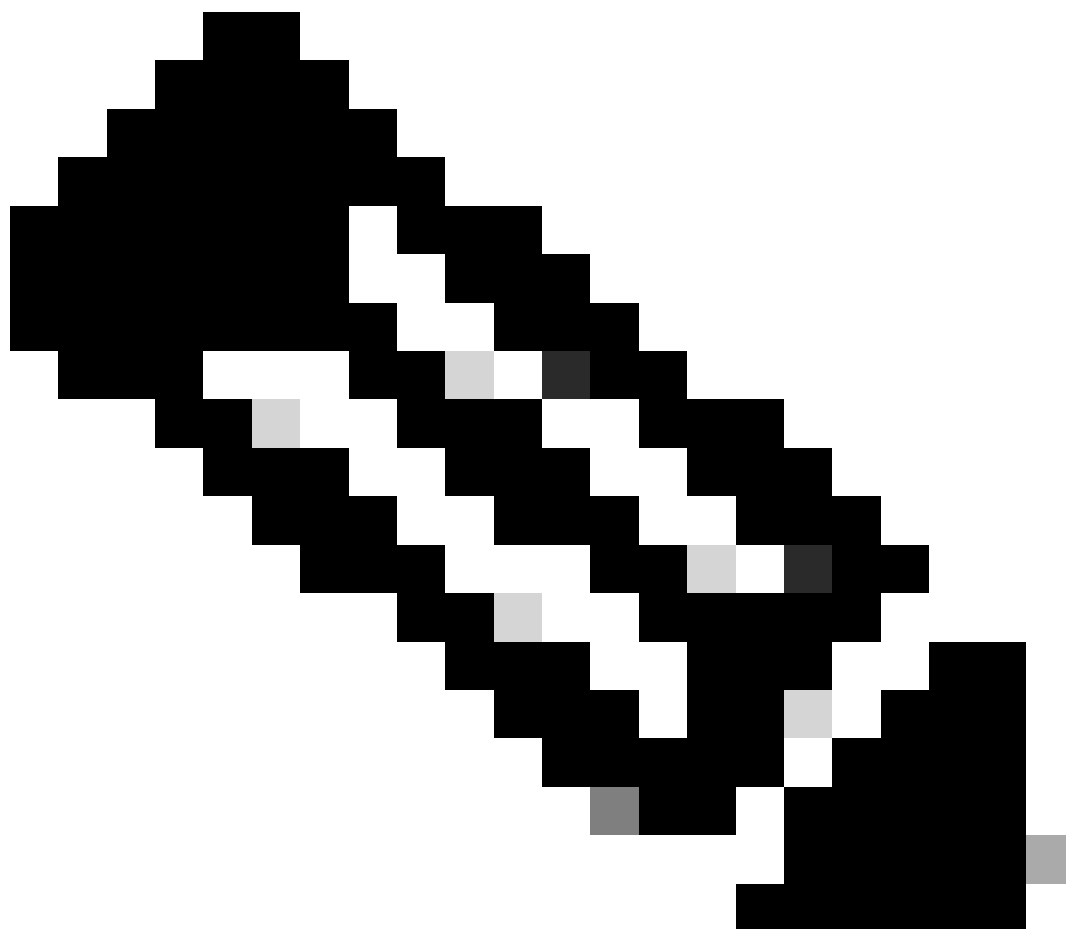
Logboeken verzamelen voor de XDR Forensics Module

Inhoud

Inleiding

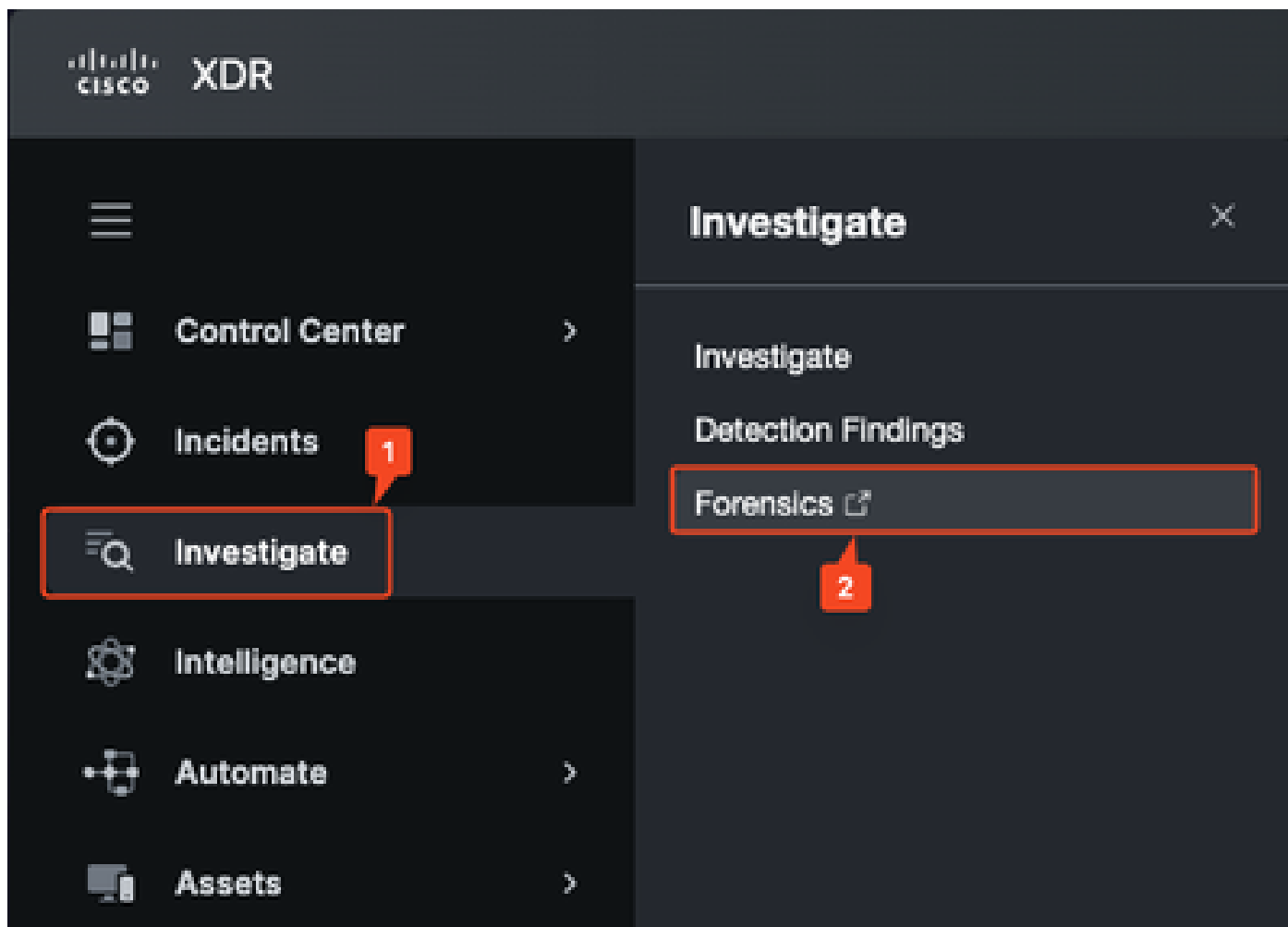
In dit document wordt beschreven hoe u op afstand diagnostische gegevens kunt ophalen om problemen met de XDR Forensics-module in de console op te lossen.

Logboeken op afstand ophalen



Opmerking: DART-logs bevatten momenteel geen XDR Forensics-logs.

Stap 1. Open XDR en navigeer naar Onderzoeken > Forensics-console.



Stap 2. Controleer of de hostnaam van het eindpunt zichtbaar is op de pagina Assets door naar de pagina Assets te gaan. Om dit te doen:

a) Open CMD op het gegeven systeem en voer de opdracht hostname uit.

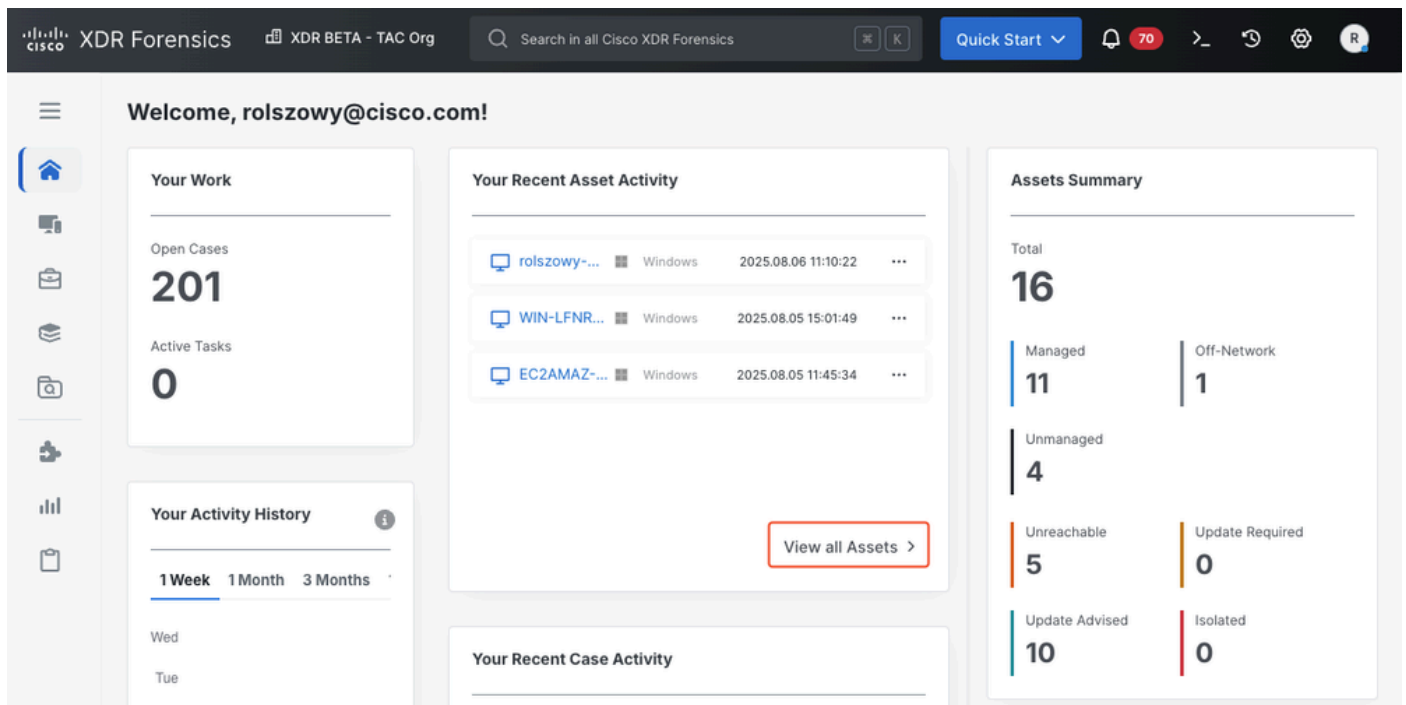
```
<#root>
```

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

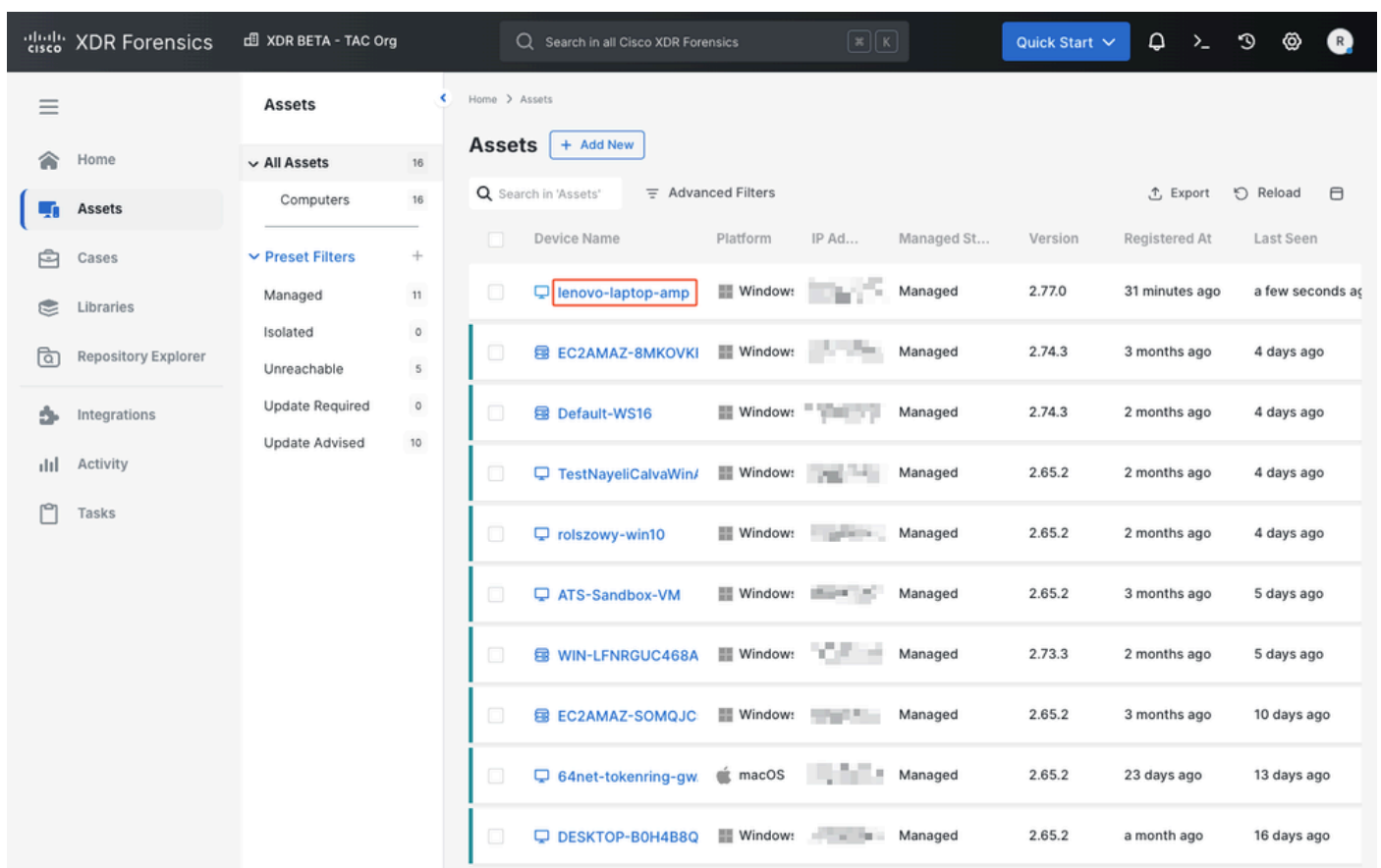
```
hostname
```

```
lenovo-laptop-amp
```

b) Klik op de hoofdpagina van de XDR Forensics-console op Alle elementen weergeven (of gebruik het menu Middelen aan de linkerkant).



c) Lokaliseer het eindpunt in de lijst en klik op de apparaatnaam om de details in te voeren.



Stap 3. Klik op de pagina met informatie over bedrijfsmiddelen op Meer acties > Logboeken verzamelen om informatie van het eindpunt te verzamelen.

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

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

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

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

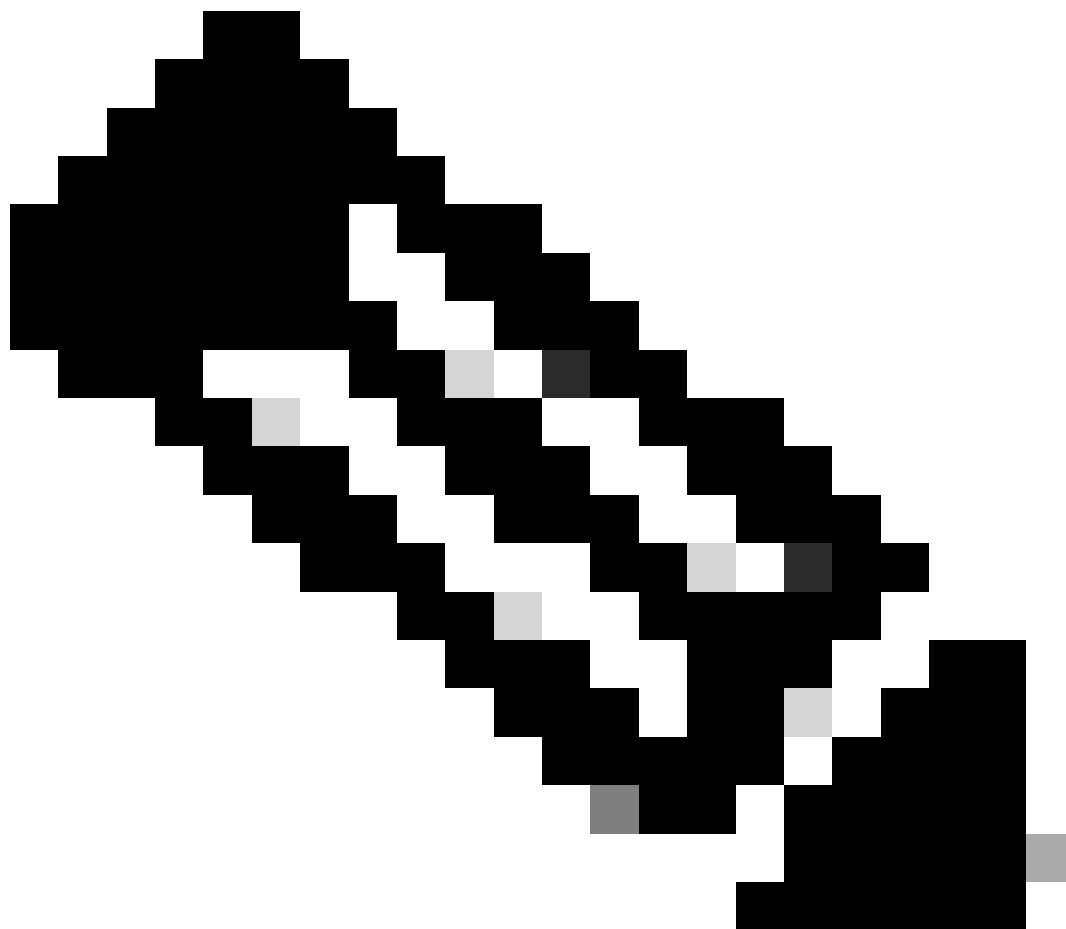
Acquire Image

F: - 267.01 GB

190.06 GB used

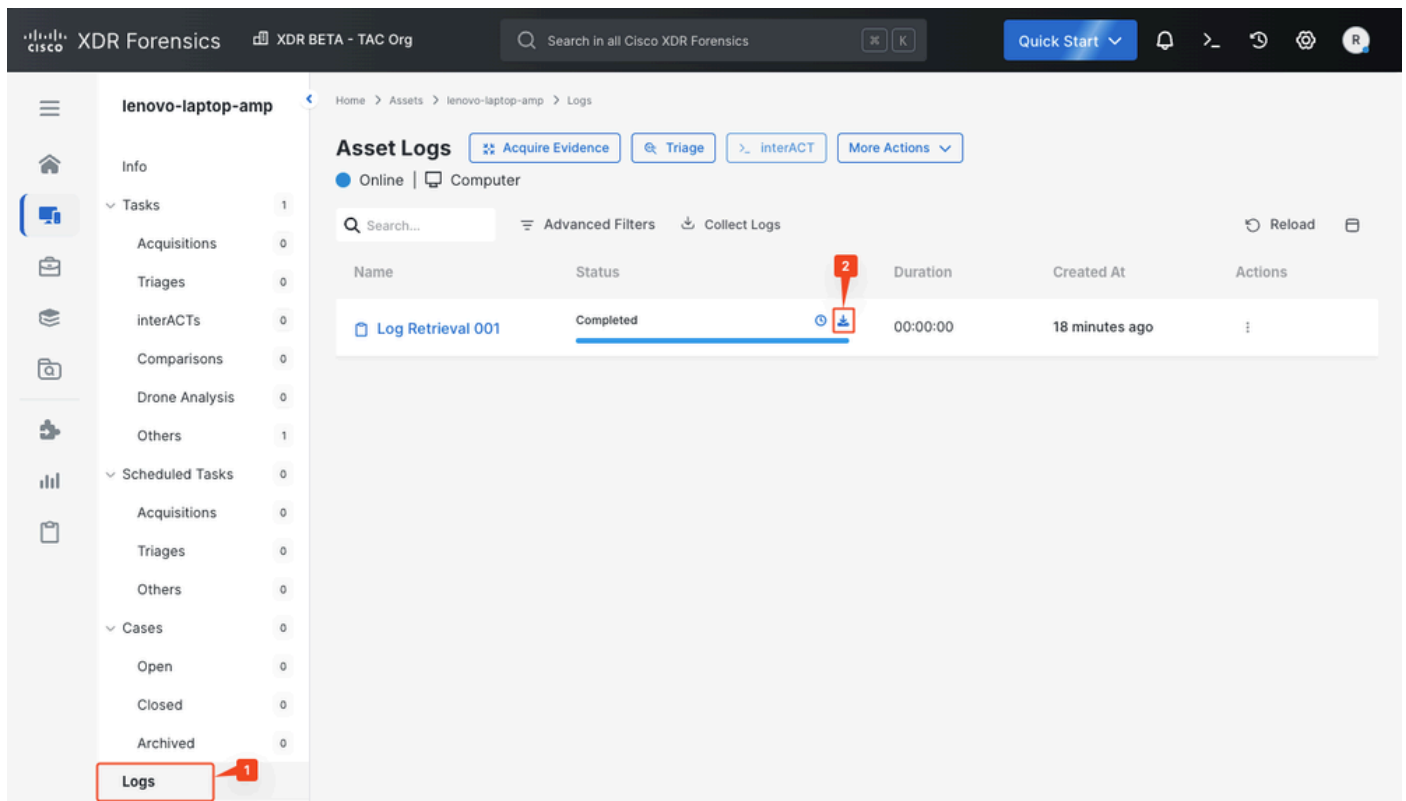
76.95 GB free

Acquire Image



Opmerking: als het actief online is, duurt het enkele seconden om dit te voltooien.

Stap 4. Ga naar de sectie Logs om te zien of er al logs zijn verzameld. Klik in het gedeelte Asset Logs op het pictogram om het downloaden van logs te starten.

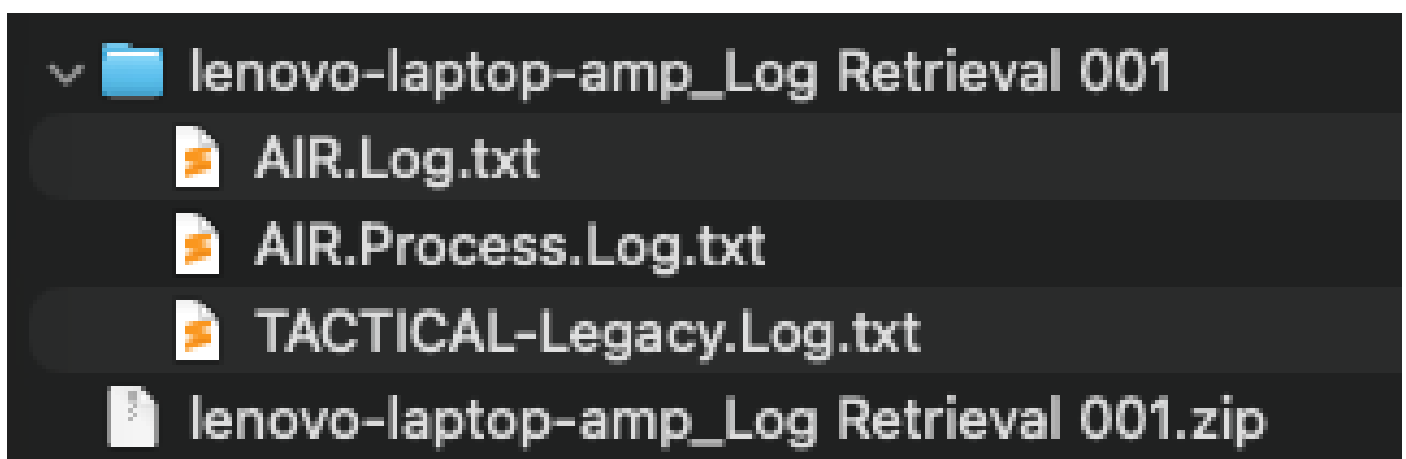


Stap 5. Verworven *.zip-bestand bevat drie bestanden die nodig zijn om problemen met de module op te lossen:

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.