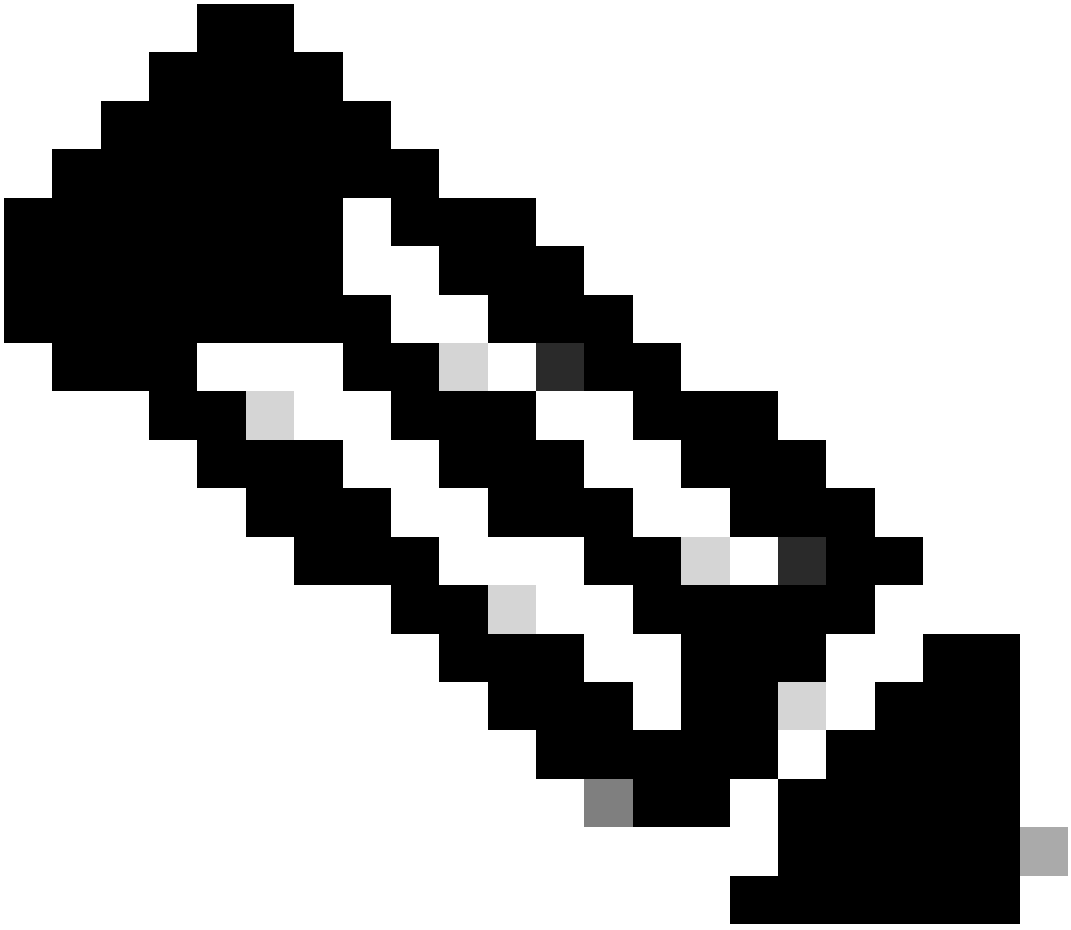
Sammeln von Protokollen für das XDR-Forensikmodul

Inhalt

Einleitung

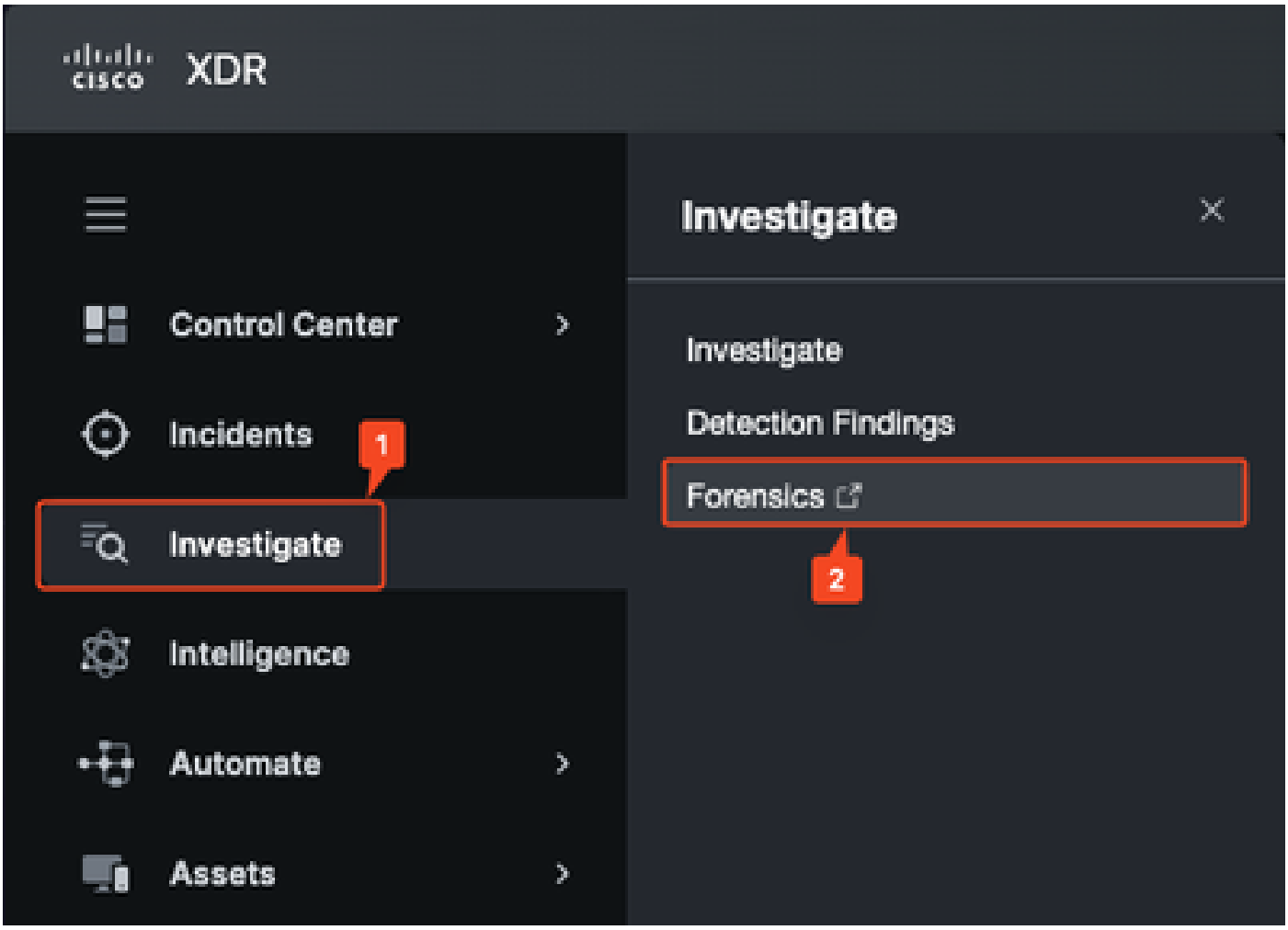
In diesem Dokument wird beschrieben, wie Sie Diagnosedaten remote abrufen können, um Probleme mit dem XDR-Forensikmodul in dessen Konsole zu beheben.

Remoteabruf von Protokollen



Anmerkung: Zurzeit enthalten DART-Protokolle keine XDR-Forensik-Protokolle.

Schritt 1: Öffnen Sie XDR, und navigieren Sie zu Investigate > Forensics console.



Schritt 2: Überprüfen Sie, ob der Hostname des Endpunkts auf der Seite "Ressourcen" angezeigt wird, indem Sie zur Seite "Ressourcen" navigieren. Gehen Sie dazu folgendermaßen vor:

a) Öffnen Sie CMD auf dem angegebenen Computer, und führen Sie den Befehl hostname aus.

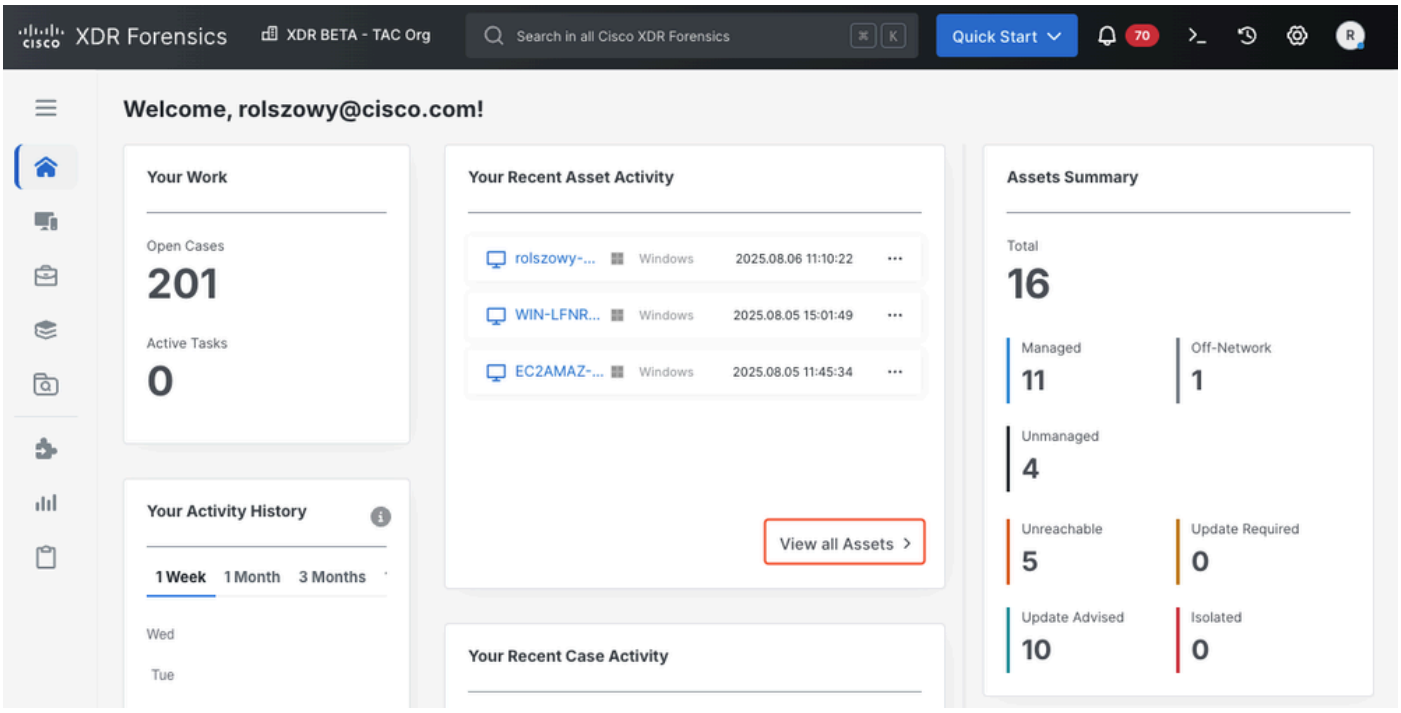
<#root>

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

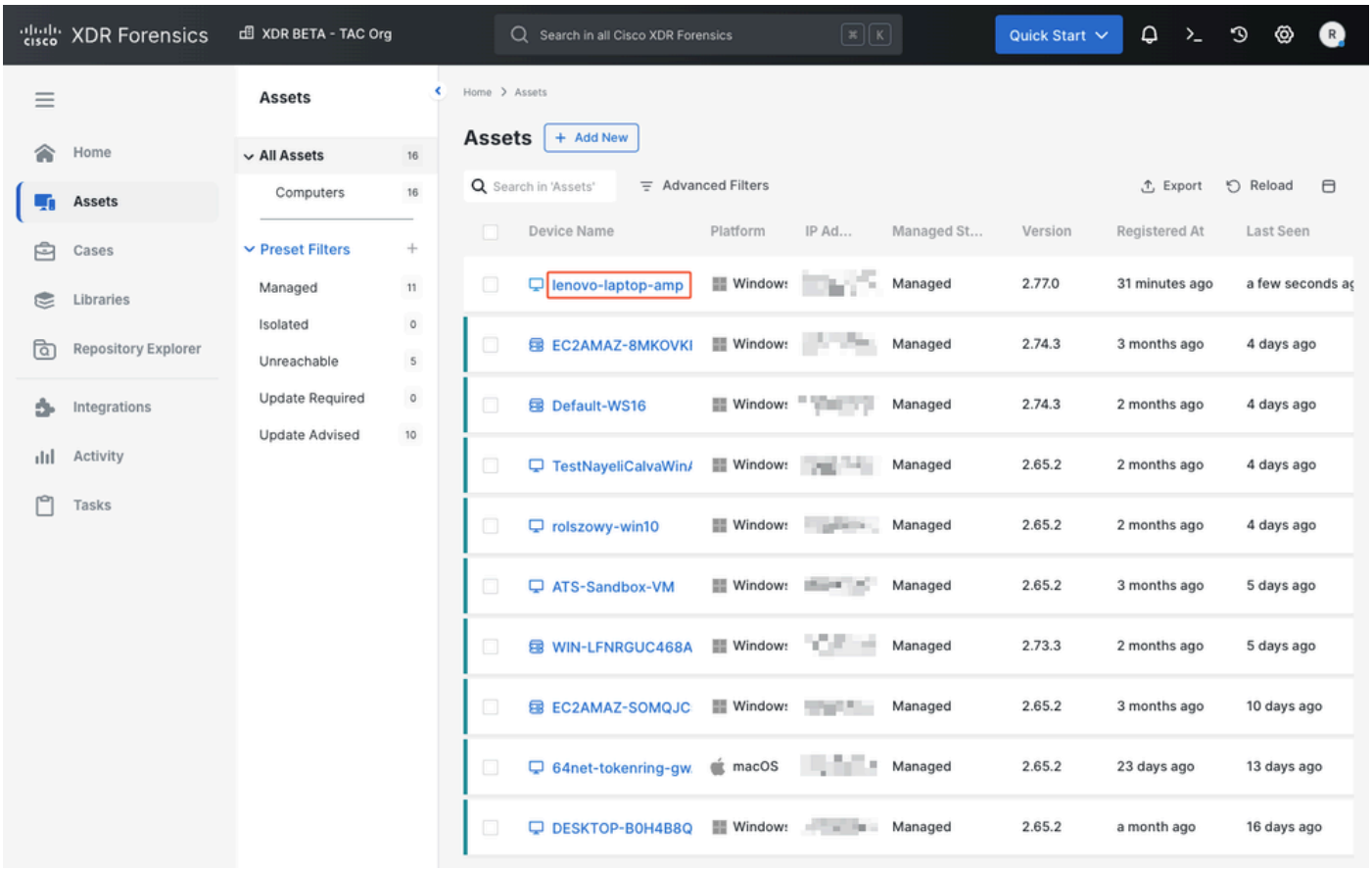
hostname

```
lenovo-laptop-amp
```

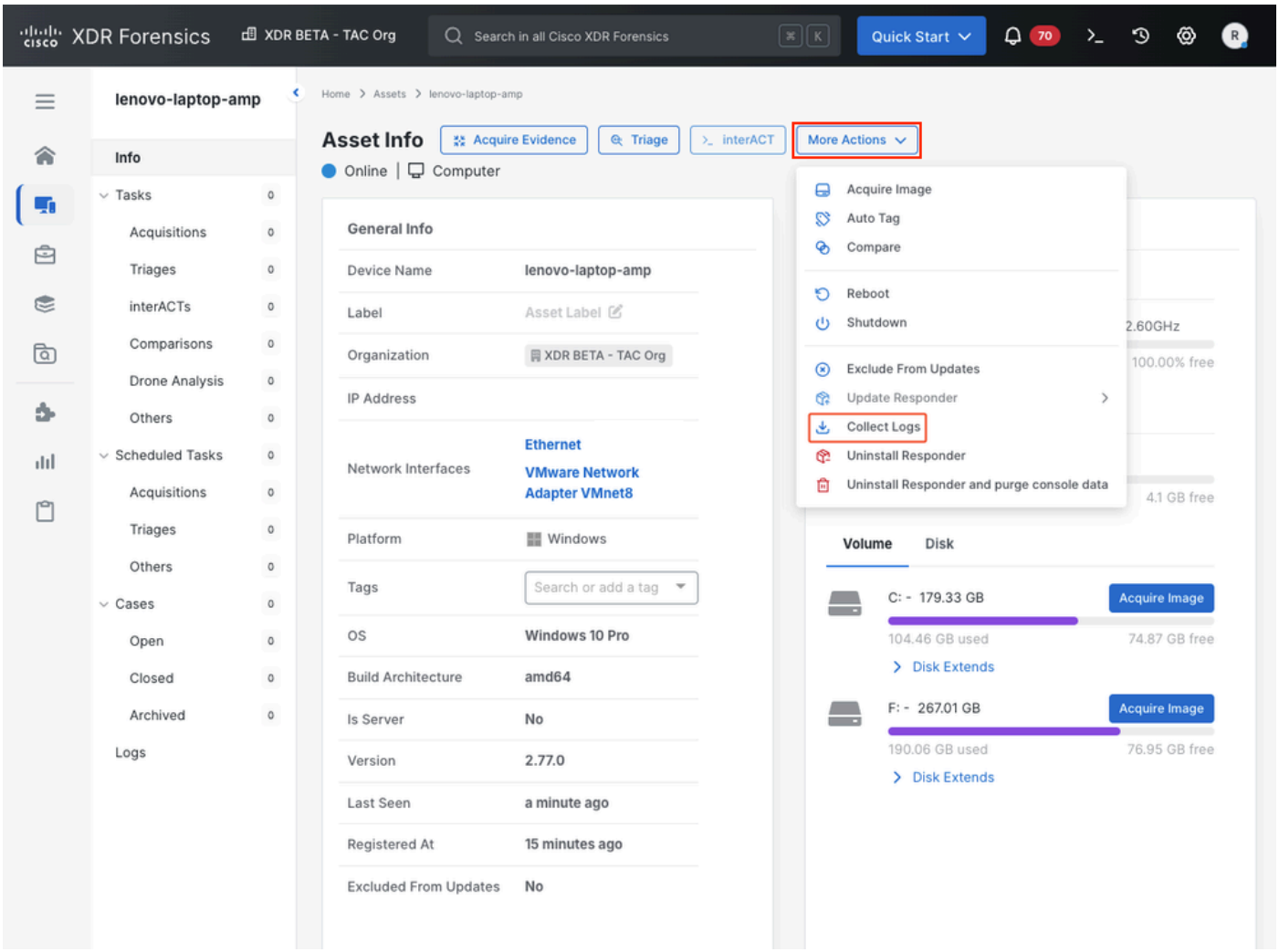
b) Klicken Sie auf der Hauptseite der XDR Forensics-Konsole auf Alle Ressourcen anzeigen (oder verwenden Sie links das Menü Ressourcen).

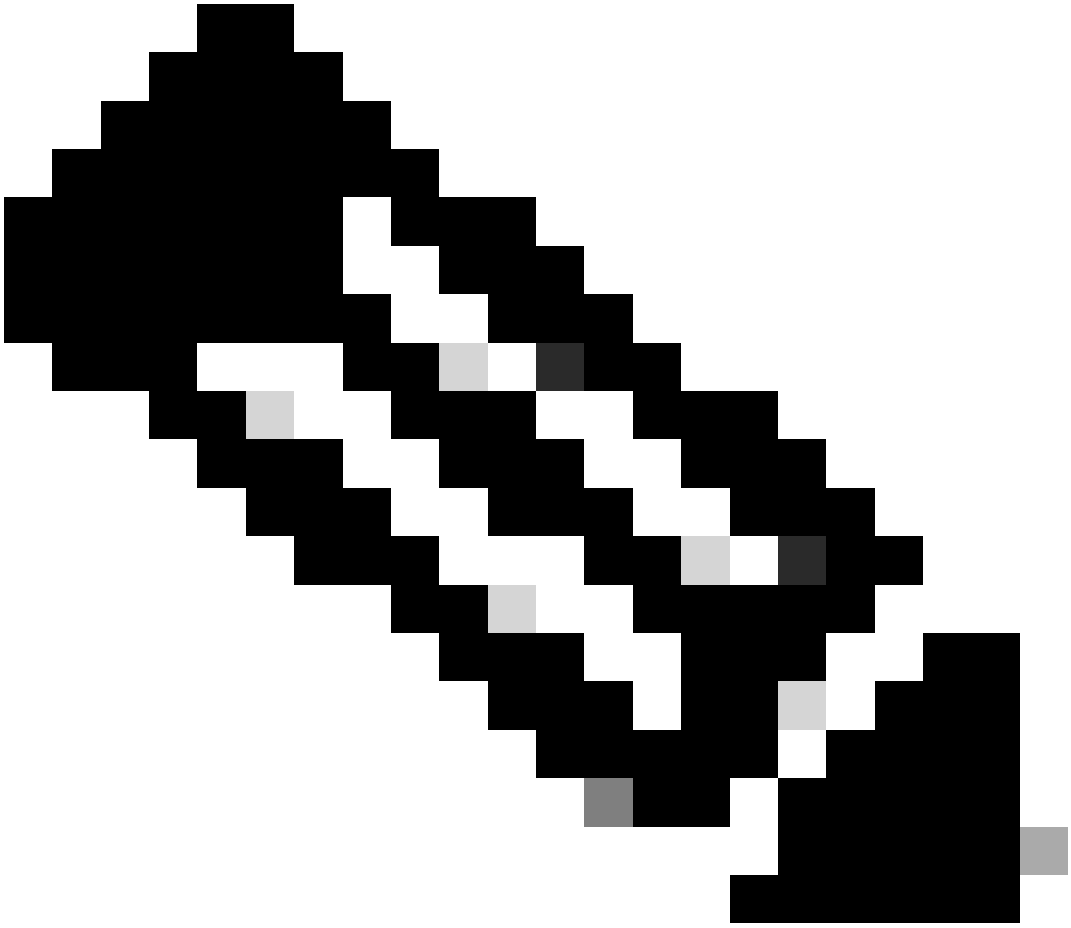


c) Lokalisieren Sie den Endpunkt in der Liste, und klicken Sie auf den Gerätenamen, um dessen Details einzugeben.



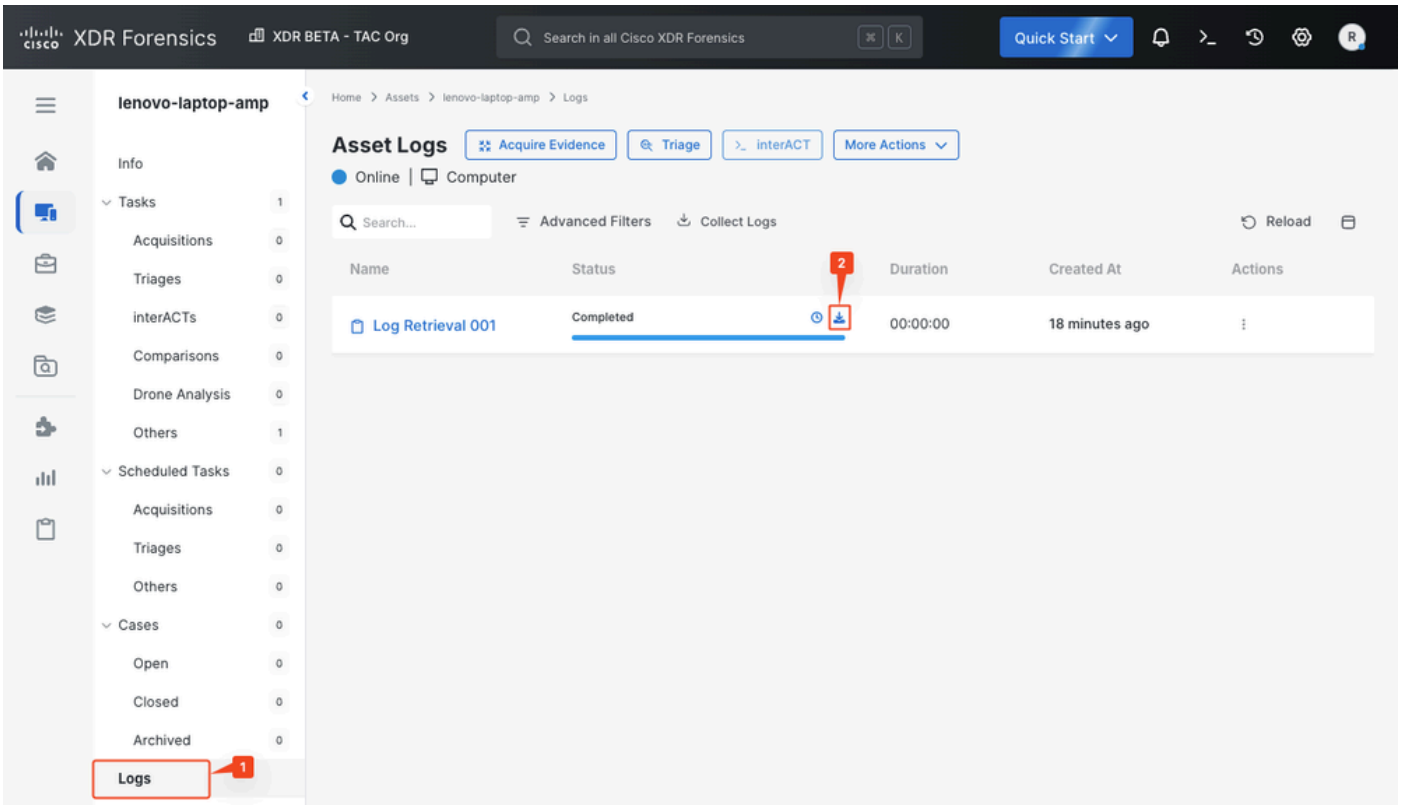
Schritt 3: Klicken Sie auf der Seite mit den Ressourceninformationen auf Weitere Aktionen > Protokolle sammeln, um Informationen vom Endpunkt zu sammeln.


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



Anmerkung: Wenn die Ressource online ist, dauert dies einige Sekunden.

Schritt 4. Gehen Sie zum Abschnitt Protokolle, um festzustellen, ob die Protokolle bereits erfasst wurden. Klicken Sie im Abschnitt Ressourcenprotokolle auf das Symbol, um den Protokolldownload zu starten.

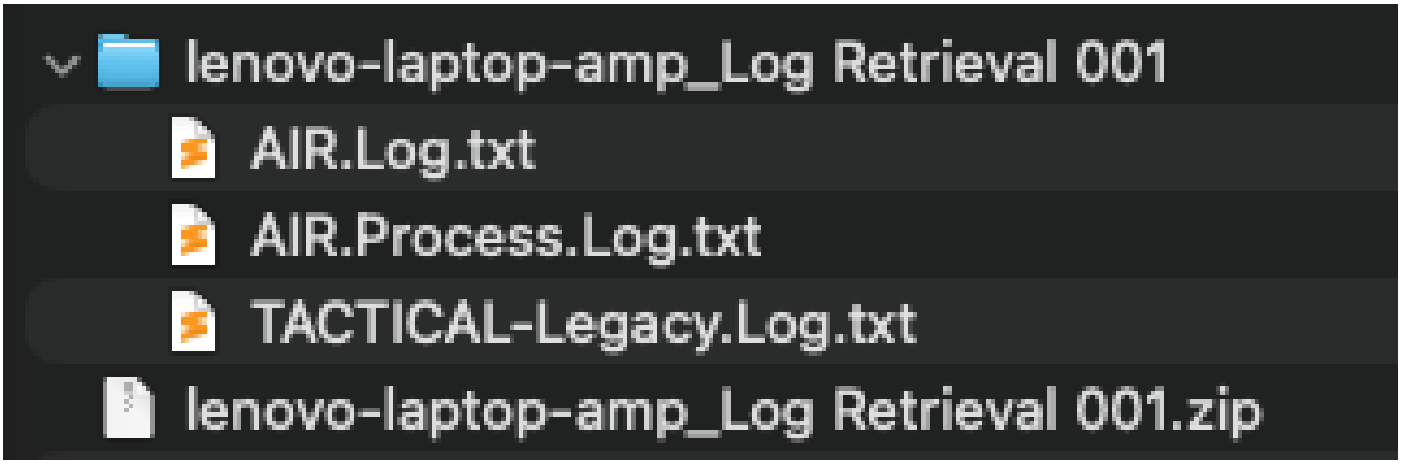


Schritt 5. Erworbene *.zip-Datei enthält drei Dateien, die für die Fehlerbehebung des Moduls erforderlich sind:

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.