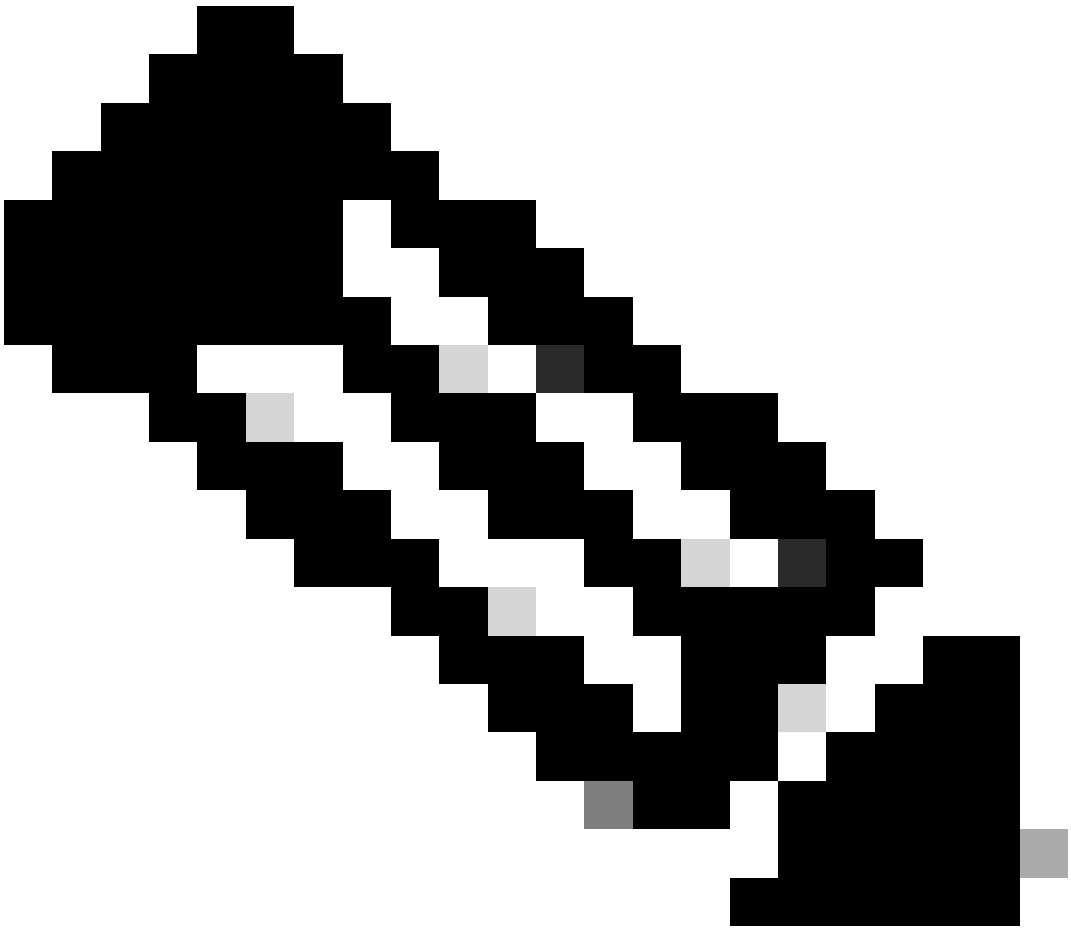
تجميع السجلات لوحدة XDR Forensics

المحتويات

المقدمة

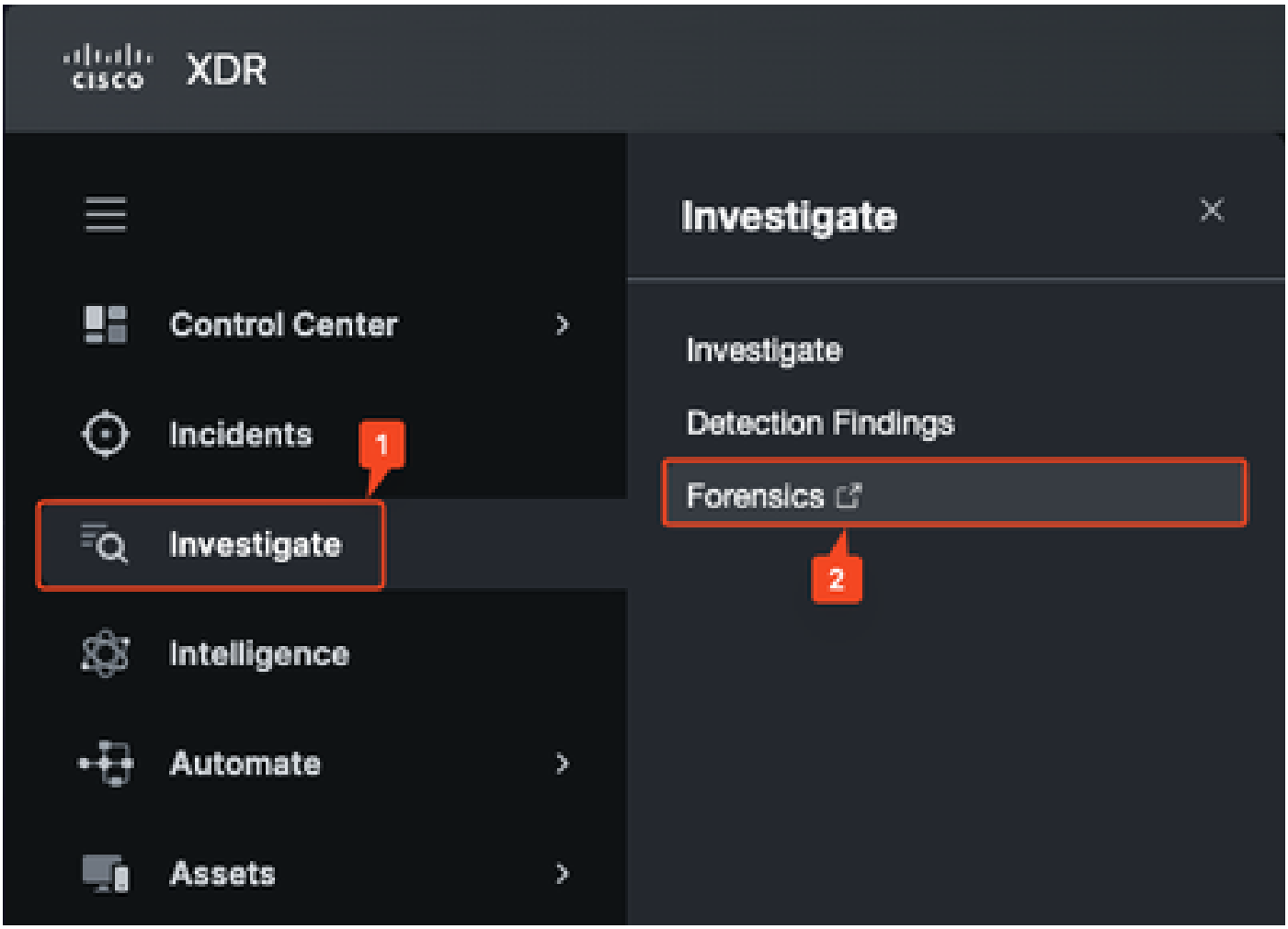
يوضح هذا المستند كيفية إحضار بيانات التشخيص عن بعد لاستكشاف أخطاء وحدة XDR Forensics النمطية وإصلاحها في وحدة التحكم الخاصة بها.

إحضار السجلات عن بعد



ملاحظة: حاليًا، لا تحتوي سجلات DART على سجلات XDR Forensic.

الخطوة 1. افتح XDR وانتقل إلى التحقيق > وحدة تحكم الأدلة الجنائية.



الخطوة 2. تأكد من ظهور اسم المضيف لنقطة النهاية على صفحة الأصول من خلال الانتقال إلى صفحة الأصول. للقيام بذلك:

أ) فتح CMD على الجهاز المحدد وتنفيذ الأمر hostname.

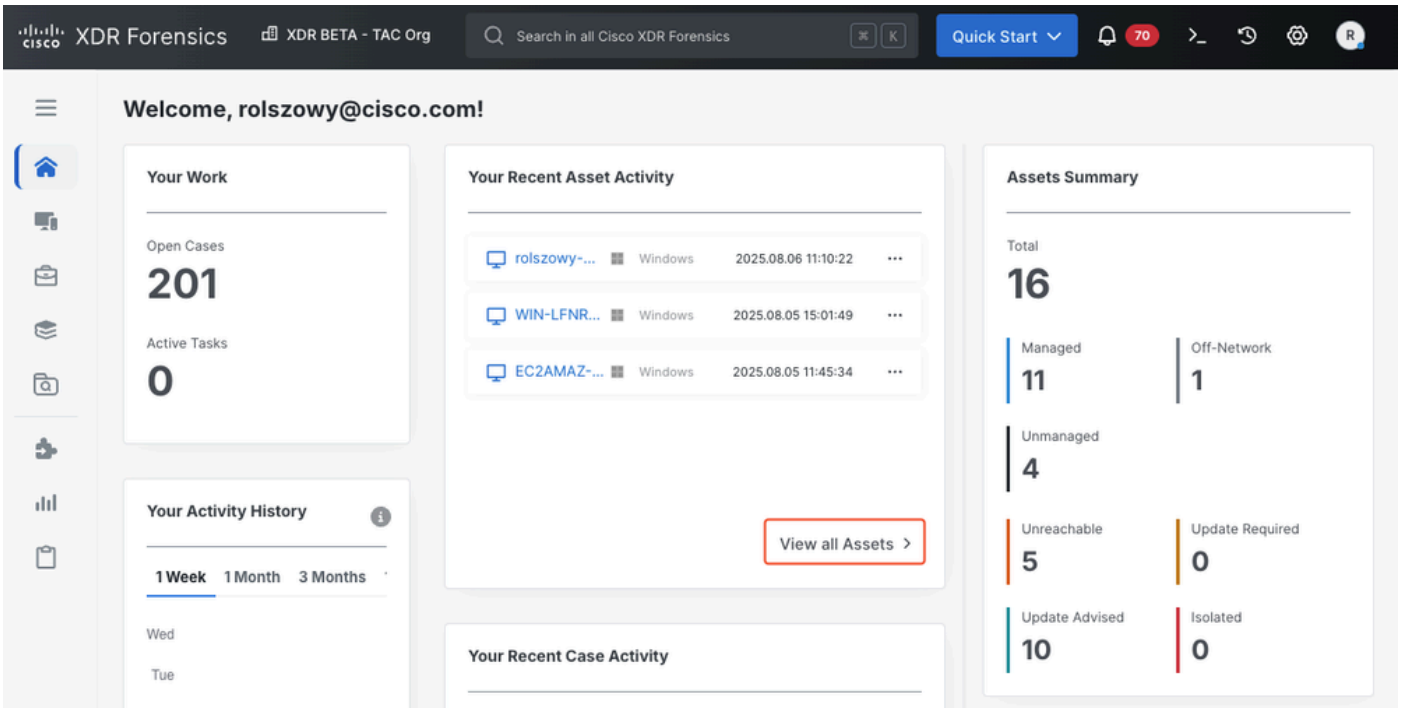
<#root>

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

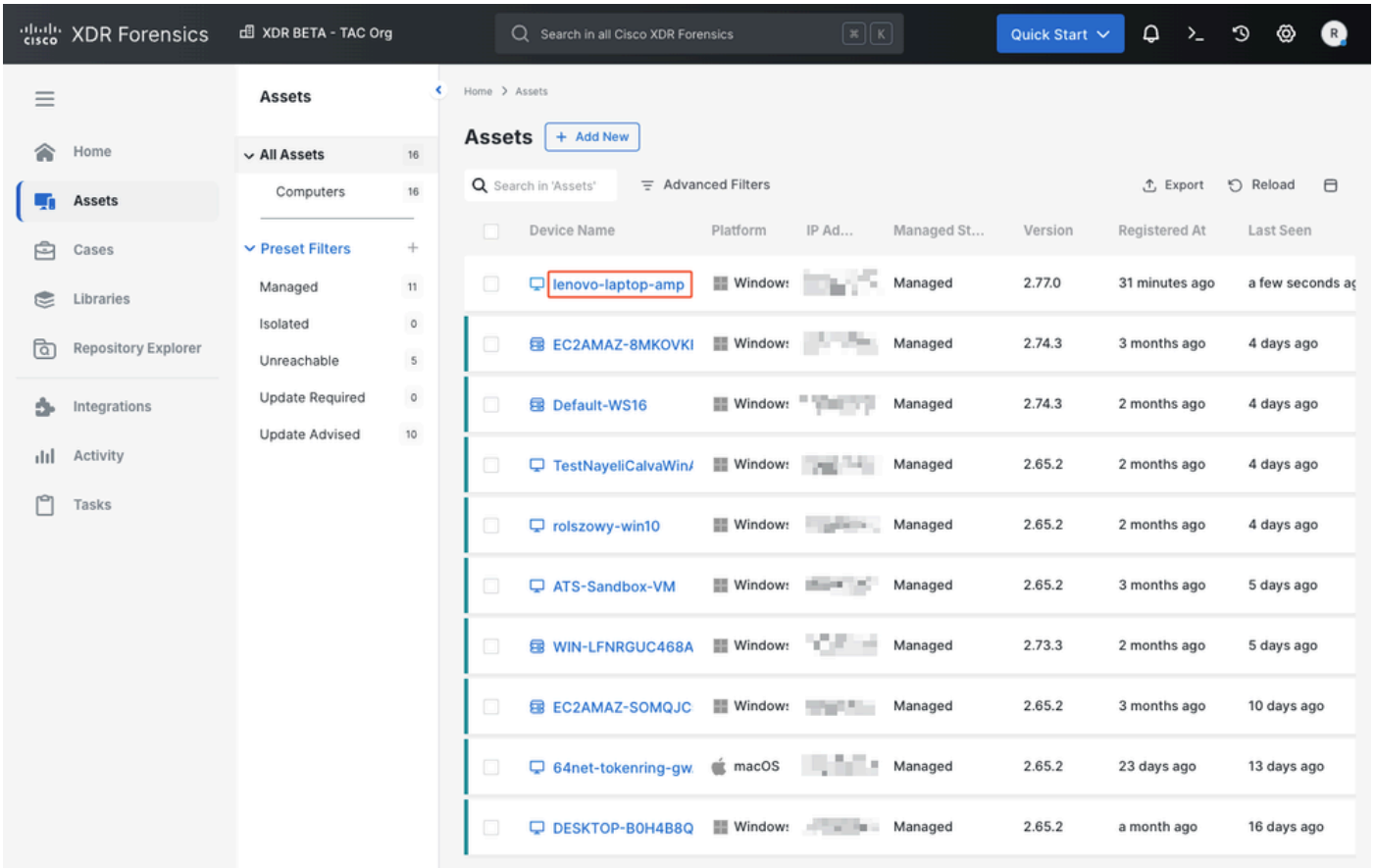
hostname

```
lenovo-laptop-amp
```

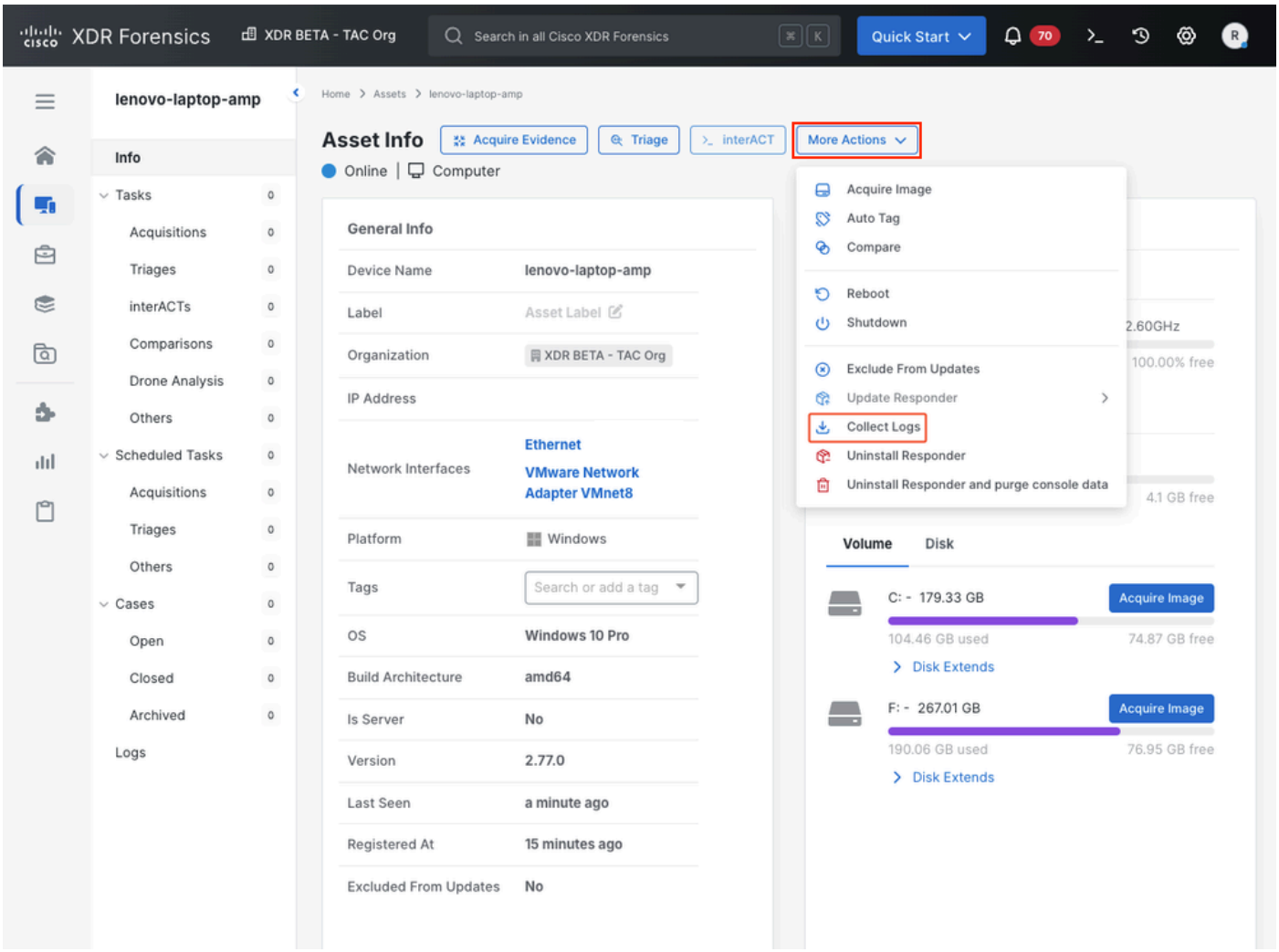
ب) في الصفحة الرئيسية لوحدة تحكم الأدلة الجنائية XDR، انقر فوق عرض جميع الأصول (أو استخدم قائمة الأصول على اليسار).

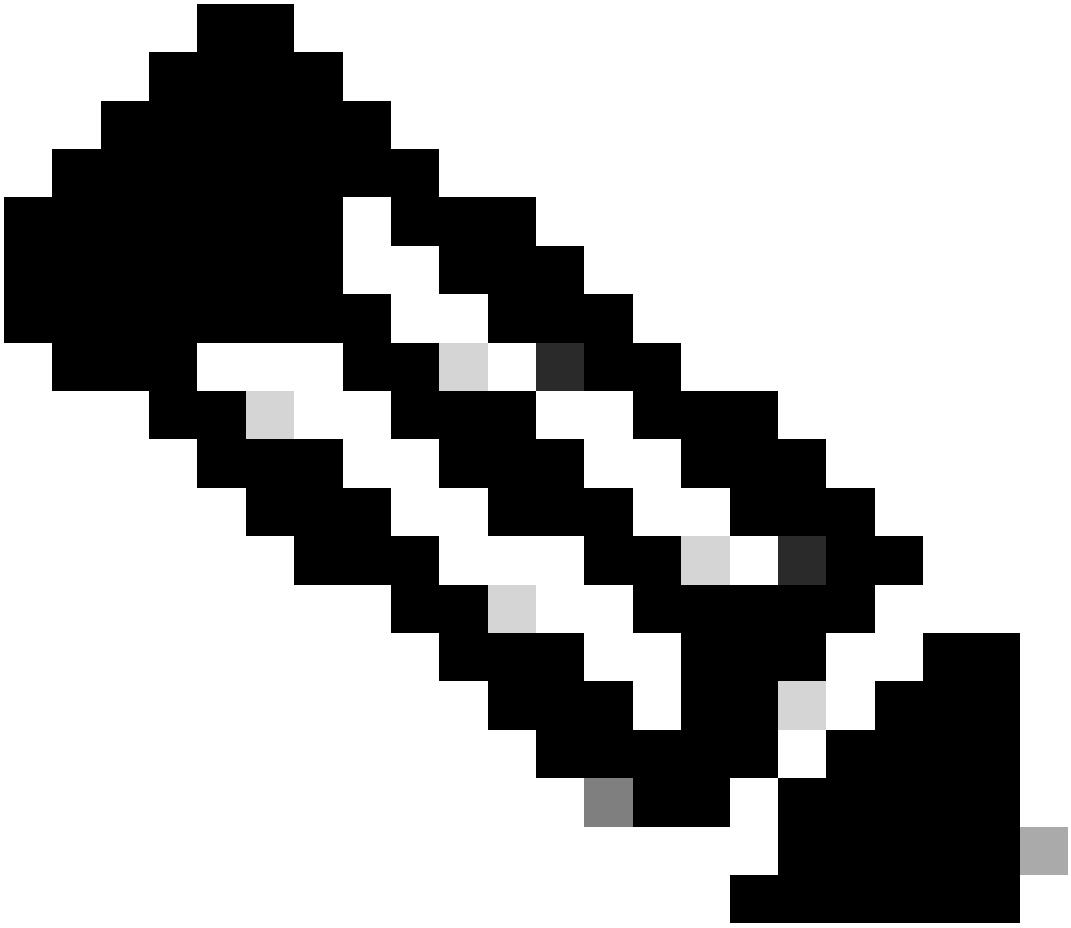


ج) قم بترجمة نقطة النهاية على القائمة وانقر على اسم الجهاز لإدخال تفاصيلها.



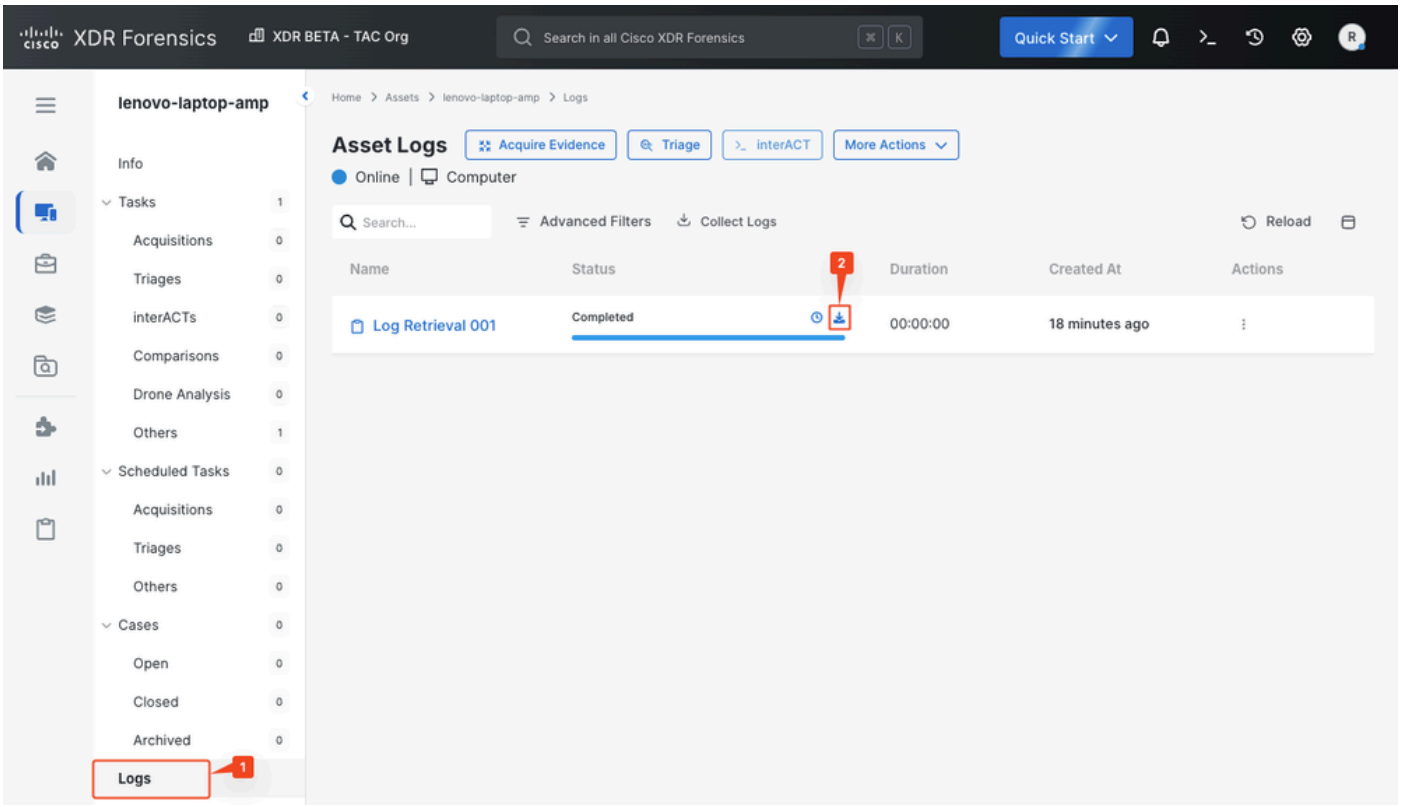
الخطوة 3. في صفحة معلومات الأصول، انقر فوق المزيد من الإجراءات >تجميع السجلات لبدء تجميع المعلومات من نقطة النهاية.


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



ملاحظة: إذا كان الأصل متصل بالإنترنت، يستغرق اكتماله بضع ثوان.

الخطوة 4. انتقل إلى قسم السجلات لمعرفة ما إذا كان قد تم تجميع السجلات بالفعل. في قسم سجلات الأصول، انقر فوق الرمز لبدء تنزيل السجلات.

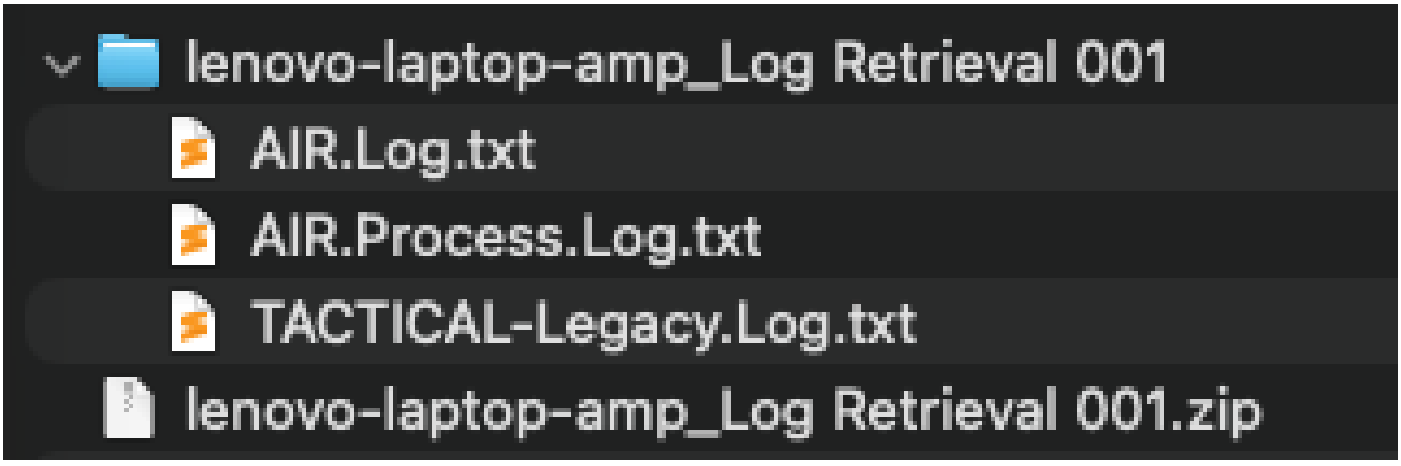


الخطوة 5. ملف Acquired *.zip يحتوي على ثلاثة ملفات مطلوبة لاستكشاف أخطاء الوحدة النمطية وإصلاحها:

- air.log.txt

- air.process.log.txt

- tactical-legacy.log.txt



حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).