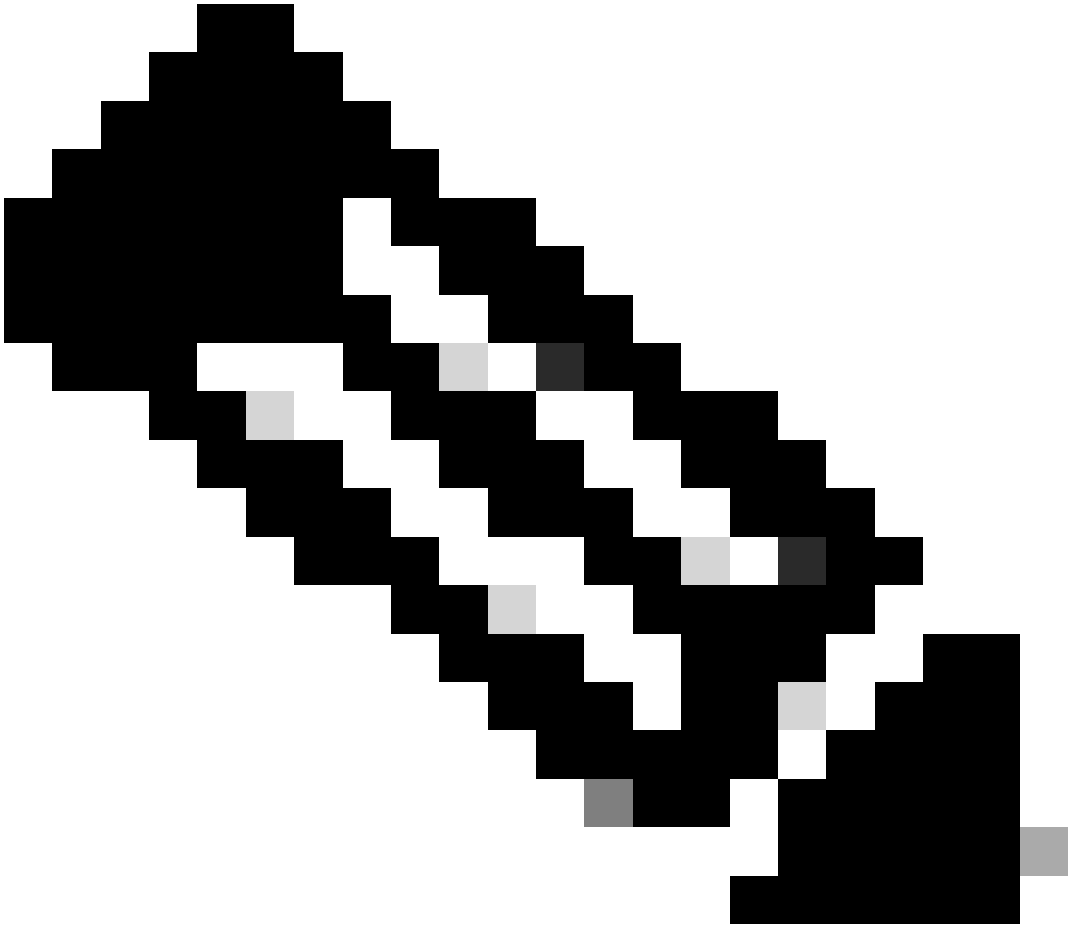
XDR 포렌식 모듈에 대한 로그 수집

목차

소개

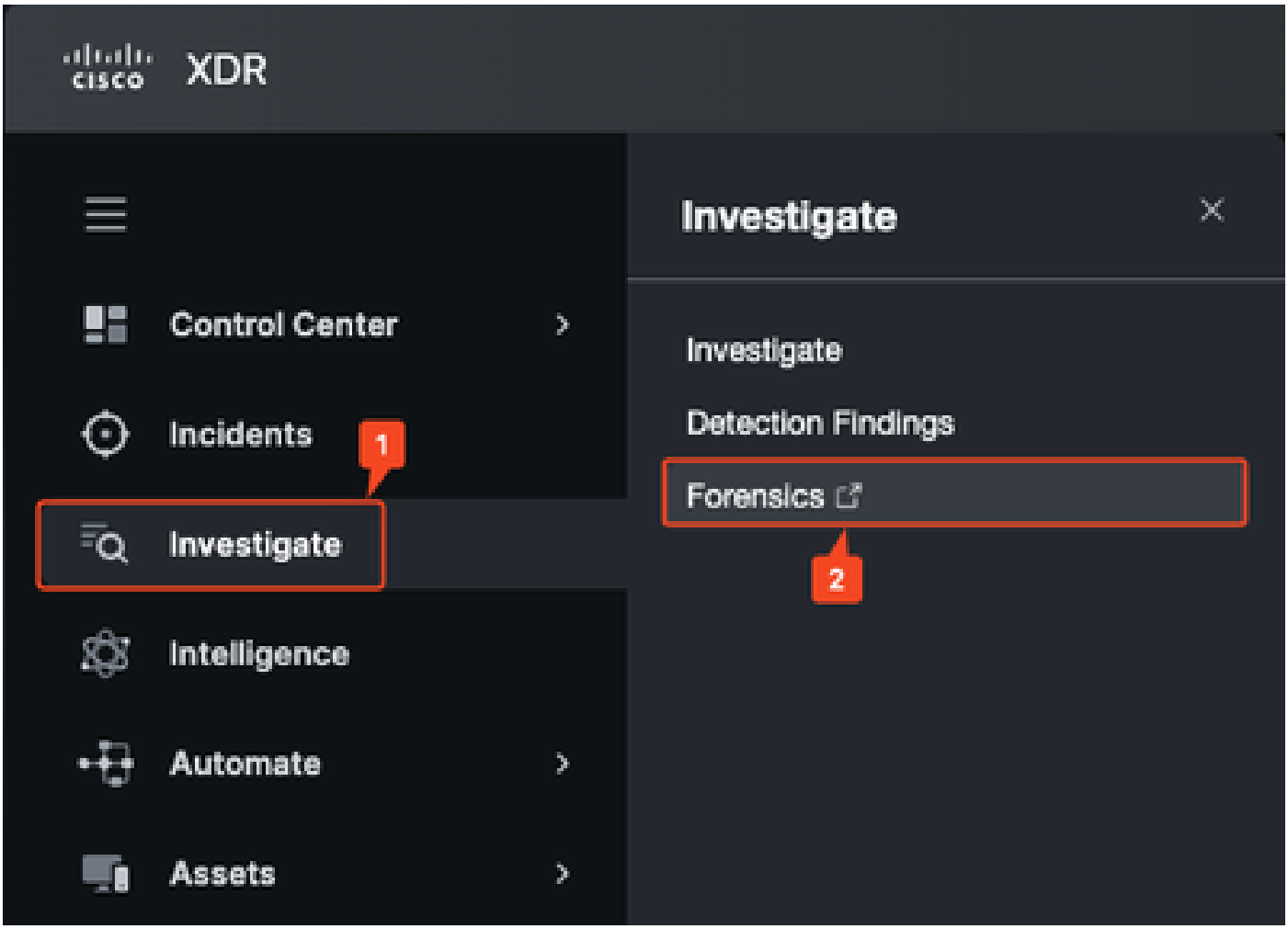
이 문서에서는 콘솔에서 XDR 포렌식 모듈의 문제를 해결하기 위해 진단 데이터를 원격으로 가져오는 방법에 대해 설명합니다.

원격으로 로그 가져오기



참고: 현재 DART 로그에는 XDR 포렌식 로그가 포함되어 있지 않습니다.

1단계. XDR을 열고 Investigate > Forensics console로 이동합니다.



2단계. Assets(자산) 페이지로 이동하여 엔드포인트의 호스트 이름이 Assets(자산) 페이지에 표시되는지 확인합니다. 이렇게 하려면 다음을 수행합니다.

a) 지정된 시스템에서 CMD를 열고 hostname 명령을 실행합니다.

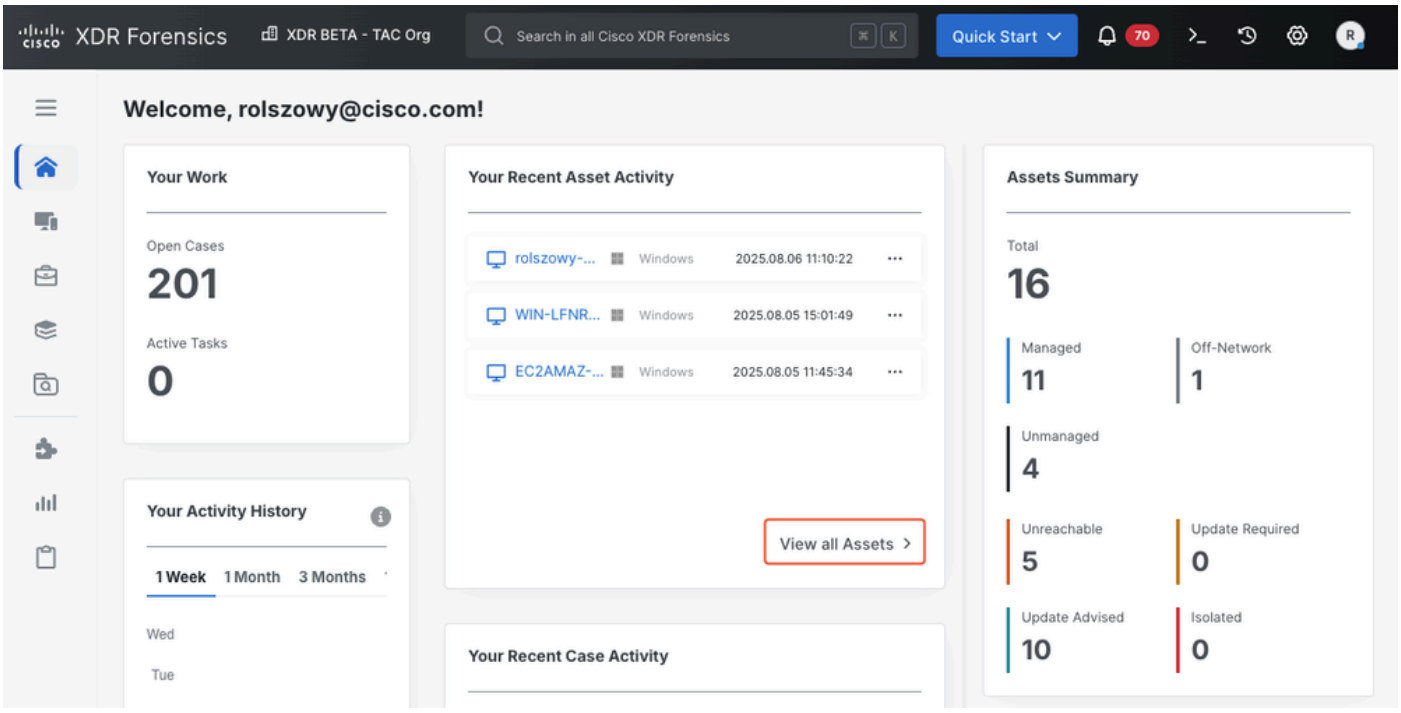
<#root>

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

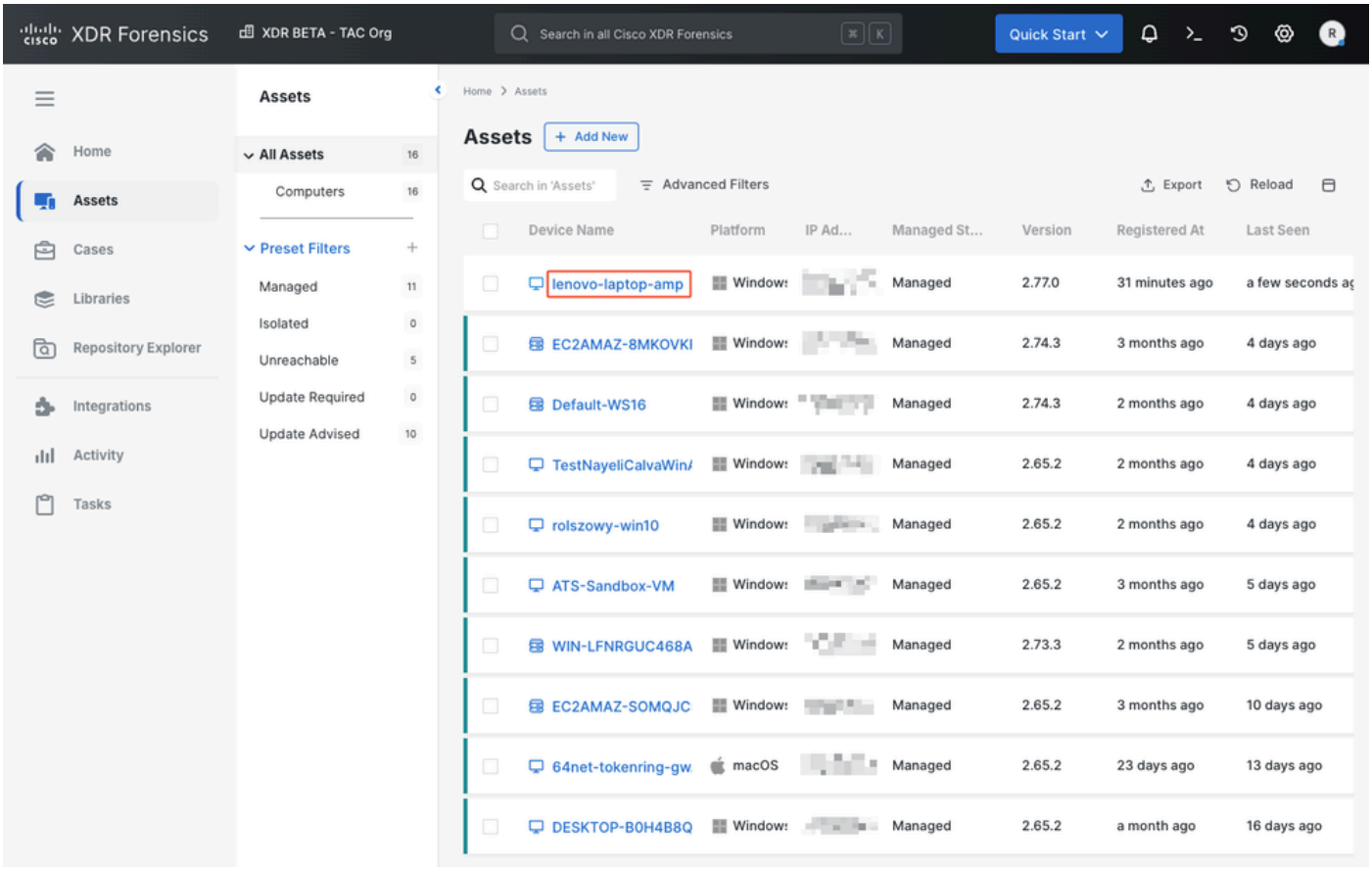
hostname

```
lenovo-laptop-amp
```

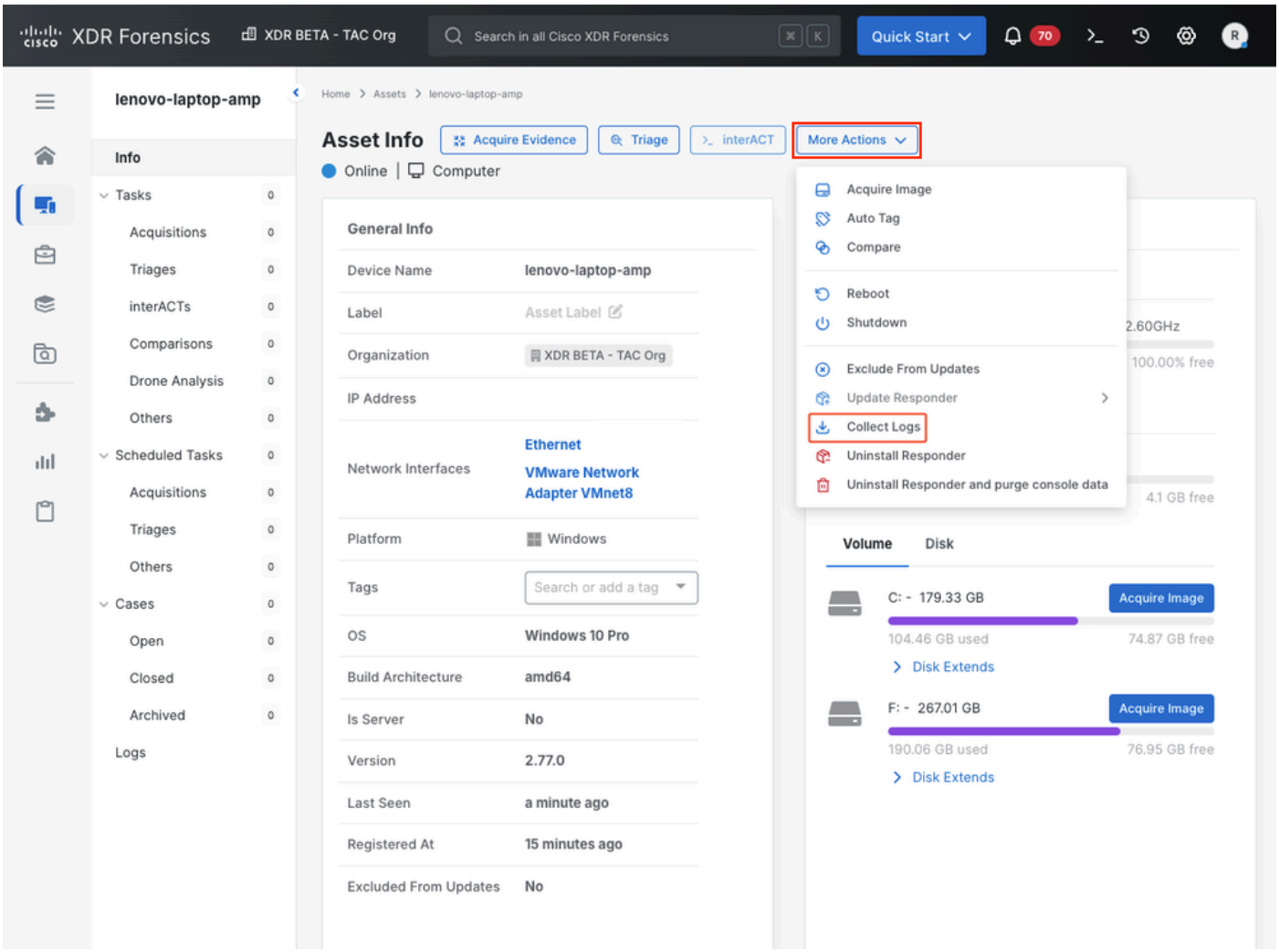
b) XDR Forensics 콘솔 기본 페이지에서 모든 자산 보기(또는 왼쪽의 자산 메뉴 사용)를 클릭합니다.

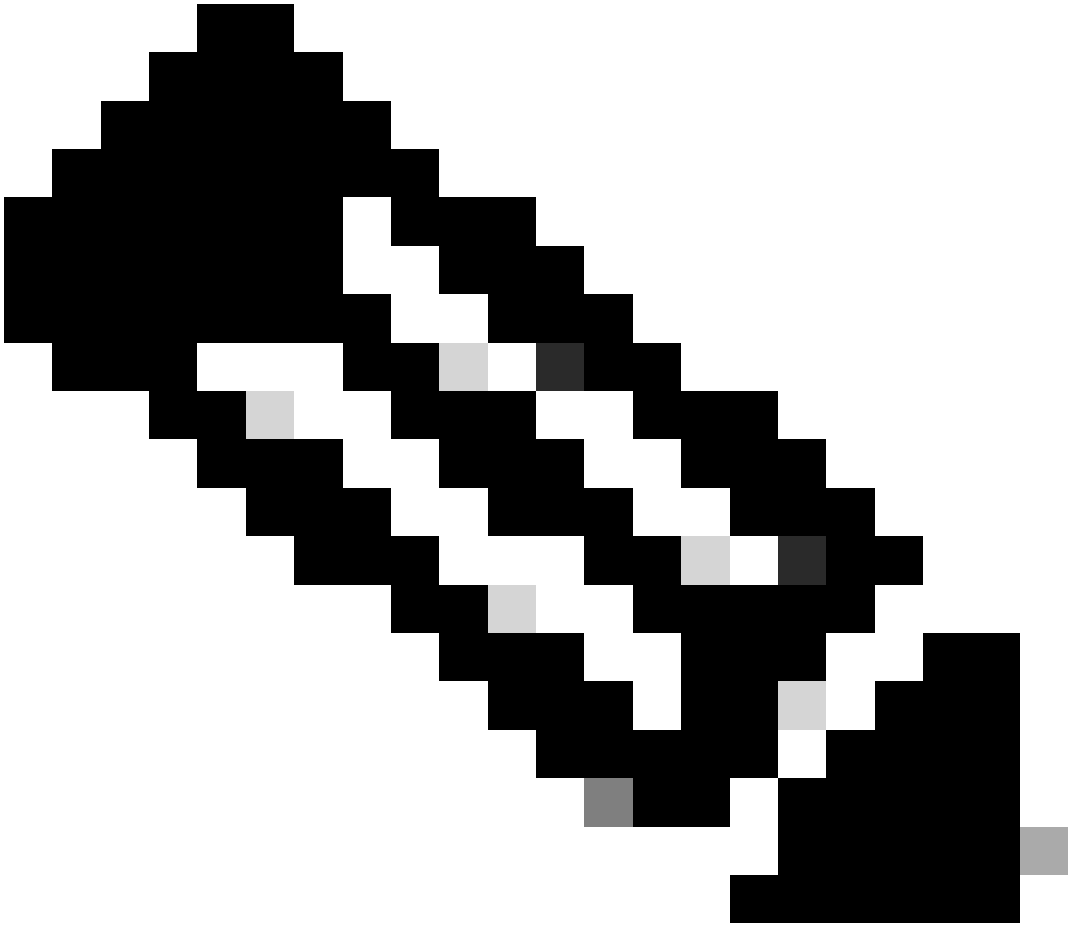


c) 목록에서 엔드포인트를 현지화하고 디바이스 이름을 클릭하여 세부 정보를 입력합니다.



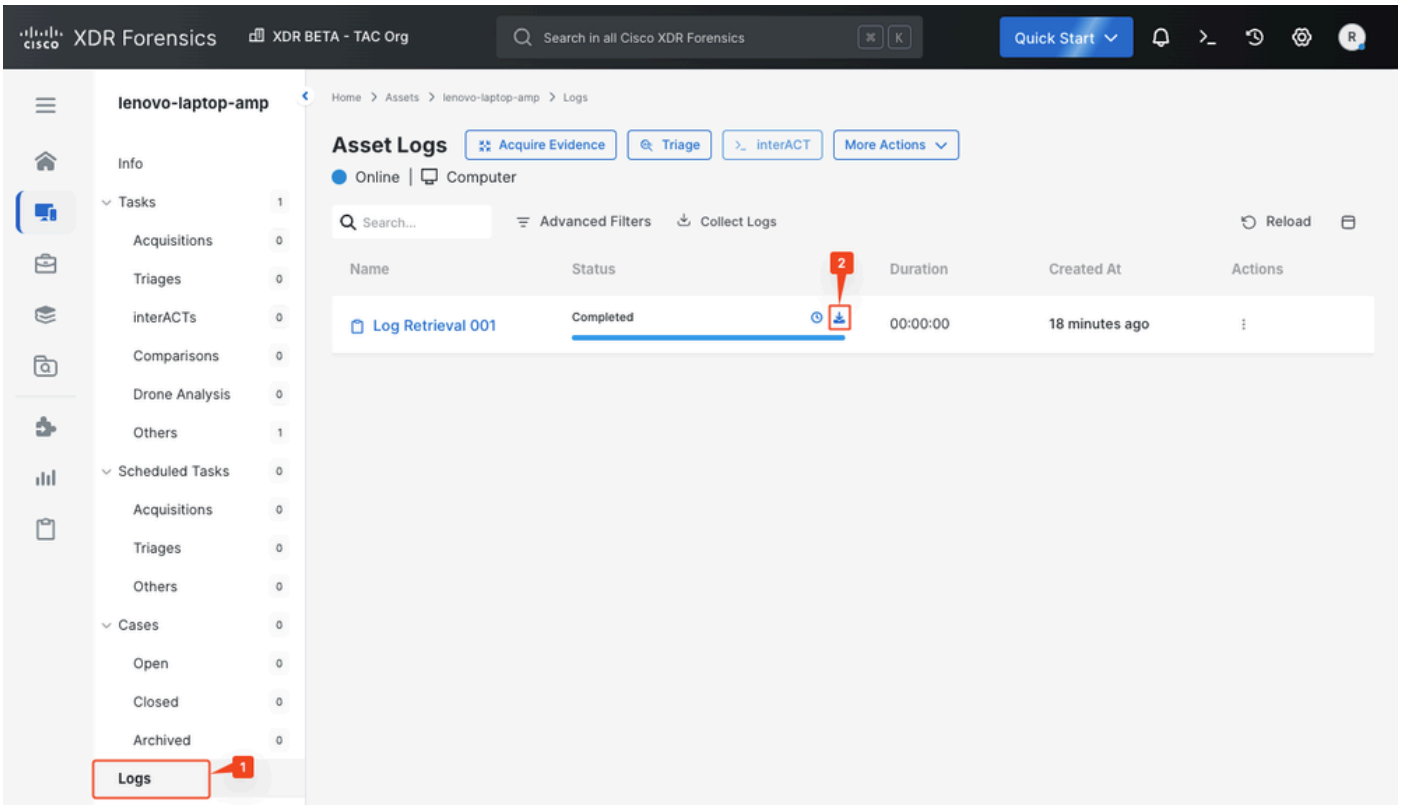
3단계. Asset info(자산 정보) 페이지에서 More Actions(추가 작업) > Collect Logs(로그 수집)를 클릭하여 엔드포인트에서 정보 수집을 시작합니다.


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



참고: 자산이 온라인 상태인 경우 완료하는 데 몇 초가 걸립니다.

4단계. 로그 섹션으로 이동하여 로그가 이미 수집되었는지 확인합니다. [자산 로그] 섹션에서 아이콘을 눌러 로그 다운로드를 시작합니다.

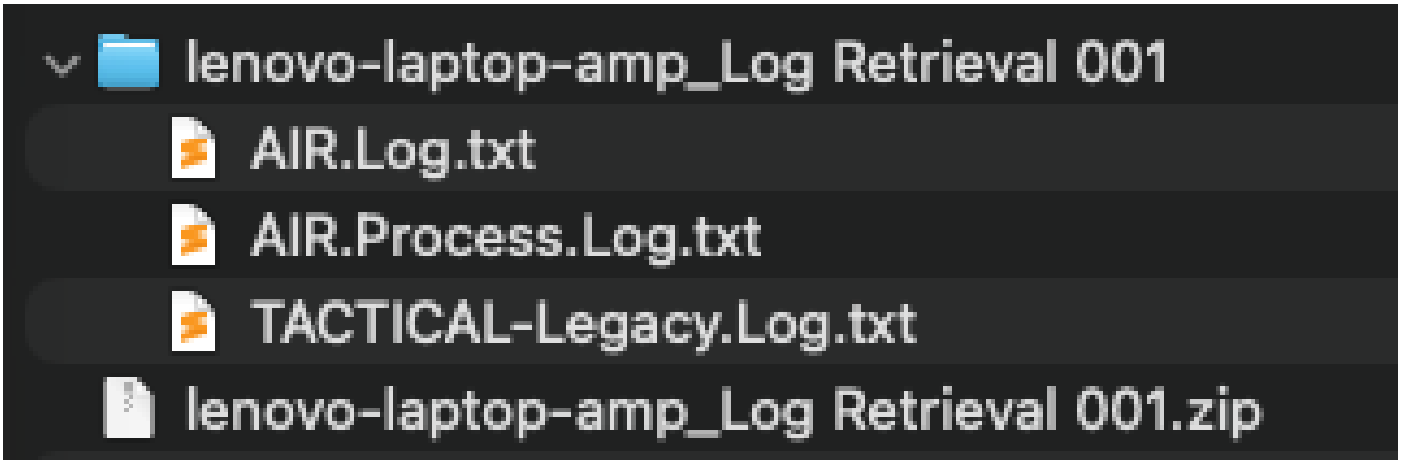


5단계. 취득한 *.zip 파일에는 모듈 트러블슈팅에 필요한 세 개의 파일이 들어 있습니다.

-AIR.Log.txt

-AIR.Process.Log.txt

-TACTICAL-Legacy.Log.txt



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.