

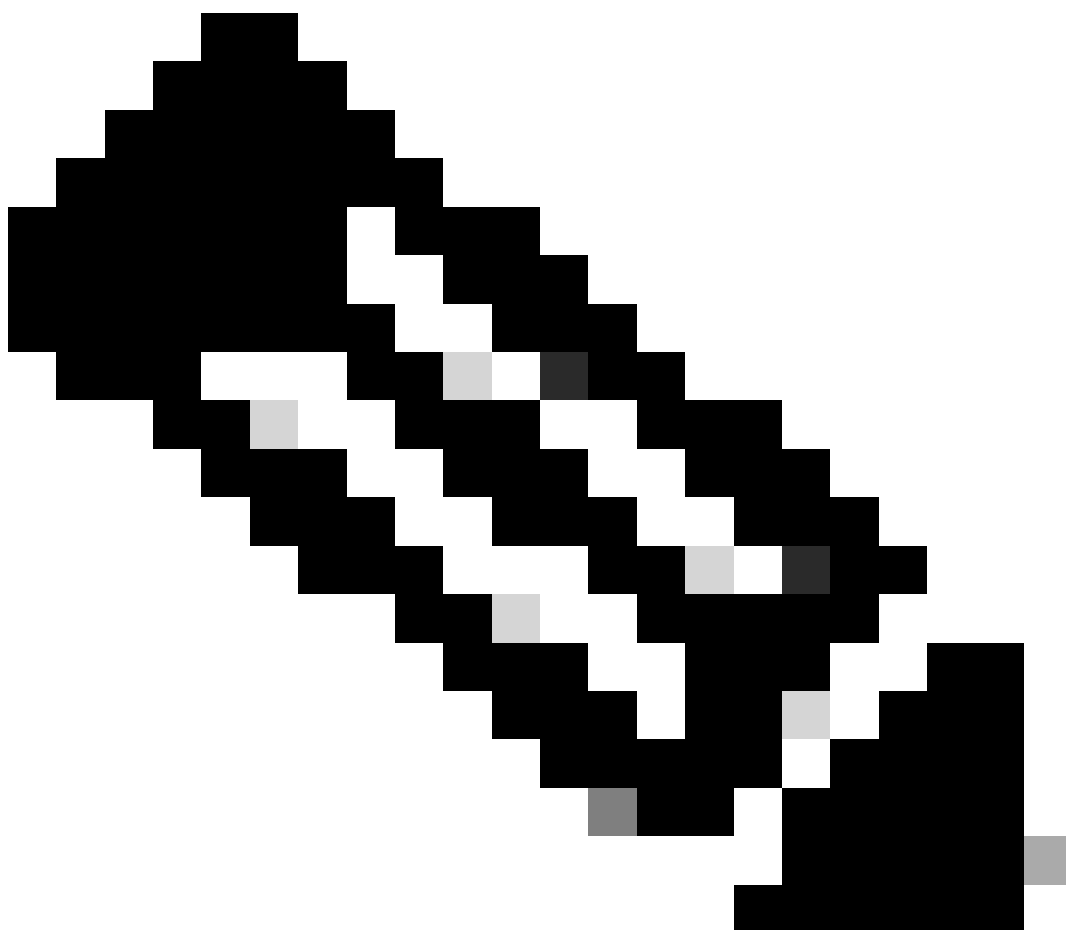
XDR Forensics ةدحول تالچسلا عي مچت

تايوتحملا

ةمدقملا

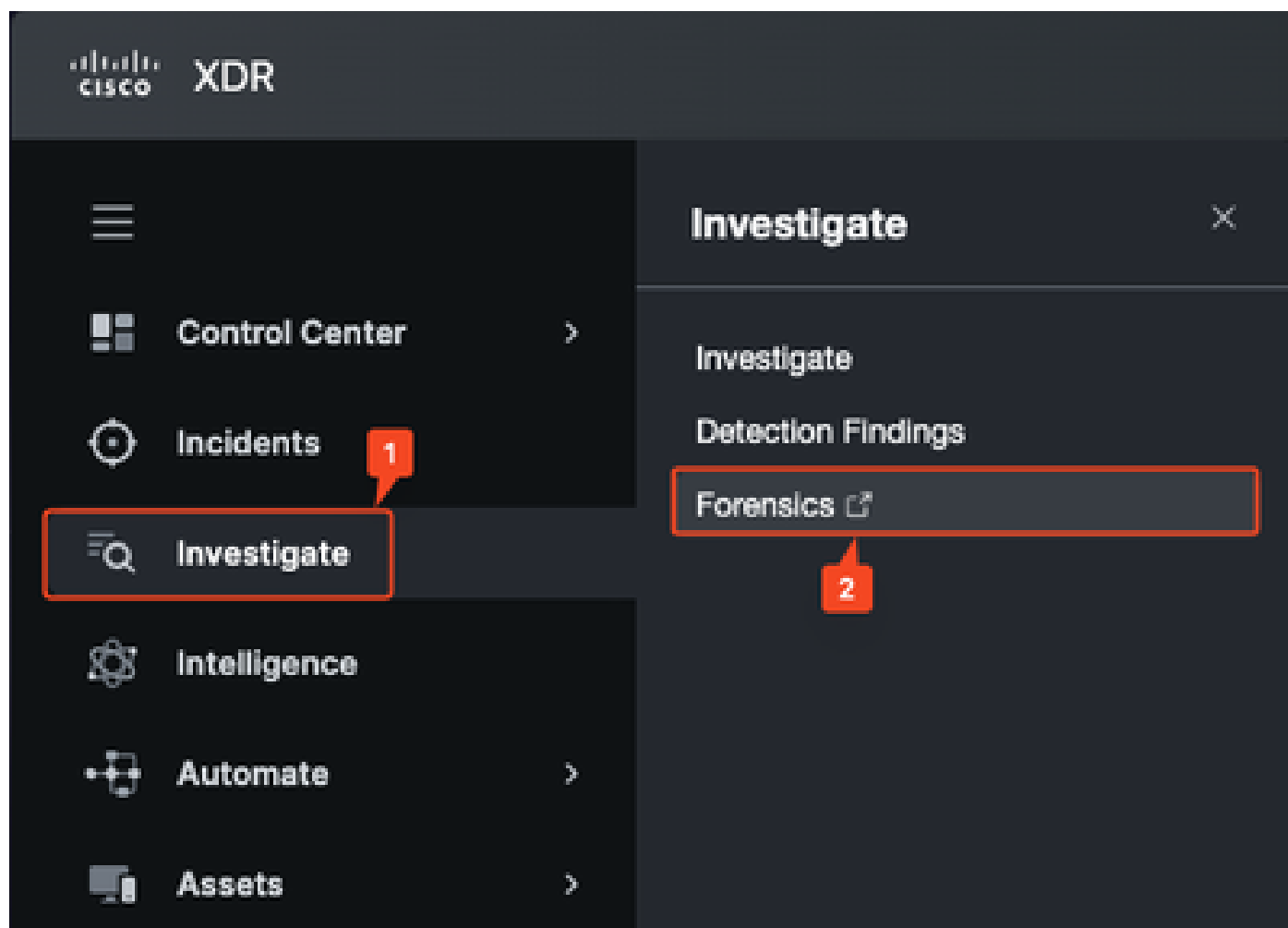
XDR ةدحو ءاطخأ فاشكتسال دع ب نع صيخشتل تانايب راضحإ ةيفيك دنتسملا اذه حضوي
اهب ةصاخلا مكحتلا ةدحو في اهالصال ةيظمنلا Forensics.

دع ب نع تالچسلا راضحإ



XDR Forensic تالچس ىلع DART تالچس يوتحت ال، ايلاح: ةظحالم

ةيئانجل ةلدأل مكحت ةدحو > قيقتلإلإ لقتنلإو XDR حتف 1. ةوطخل



لالخ نم لوصولأ ةحفص ىلع ةياهنلأ ةطقنل فيضملا مسا روهظ نم دكأت 2. ةوطخل
كلذب مايقلل. لوصولأ ةحفص ىلإ لاقتنلأ

أ) hostname رملأ ذيفنتو ددحمل زاهجل ىلع CMD حتف

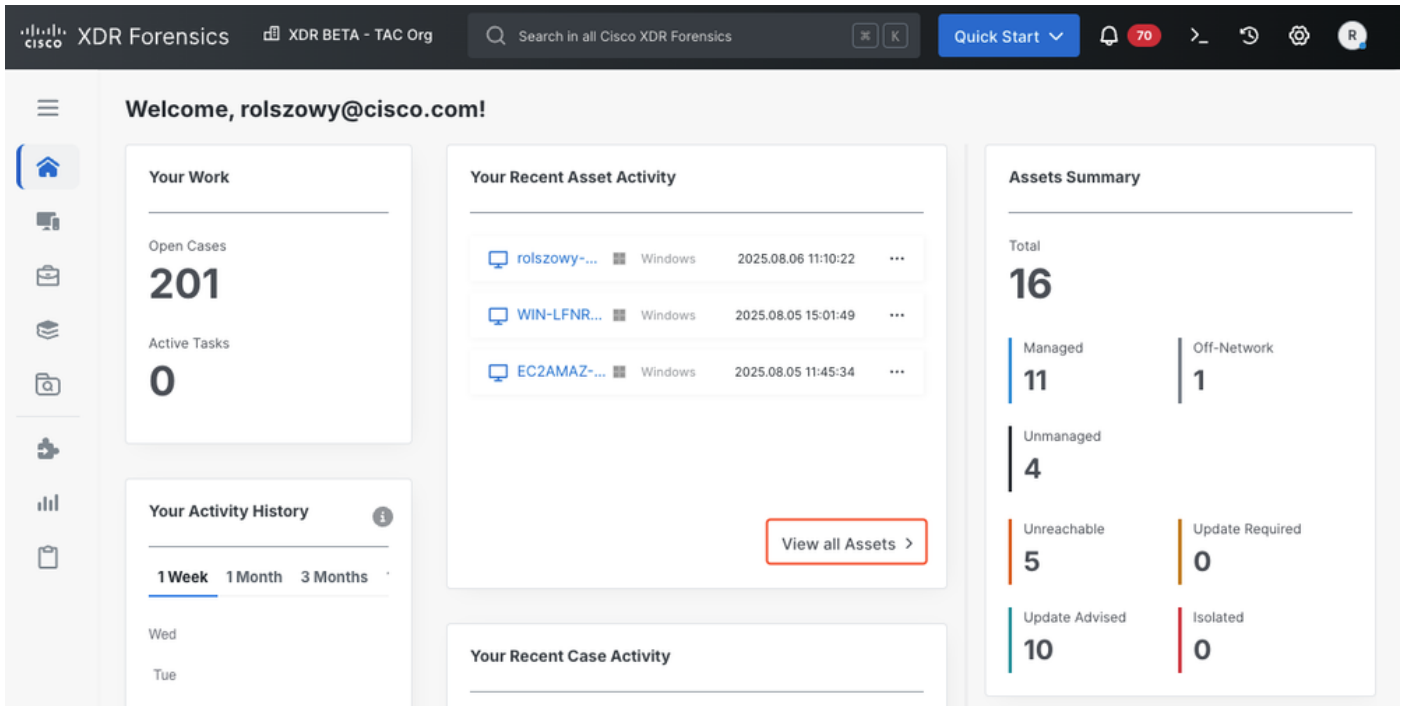
```
<#root>
```

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

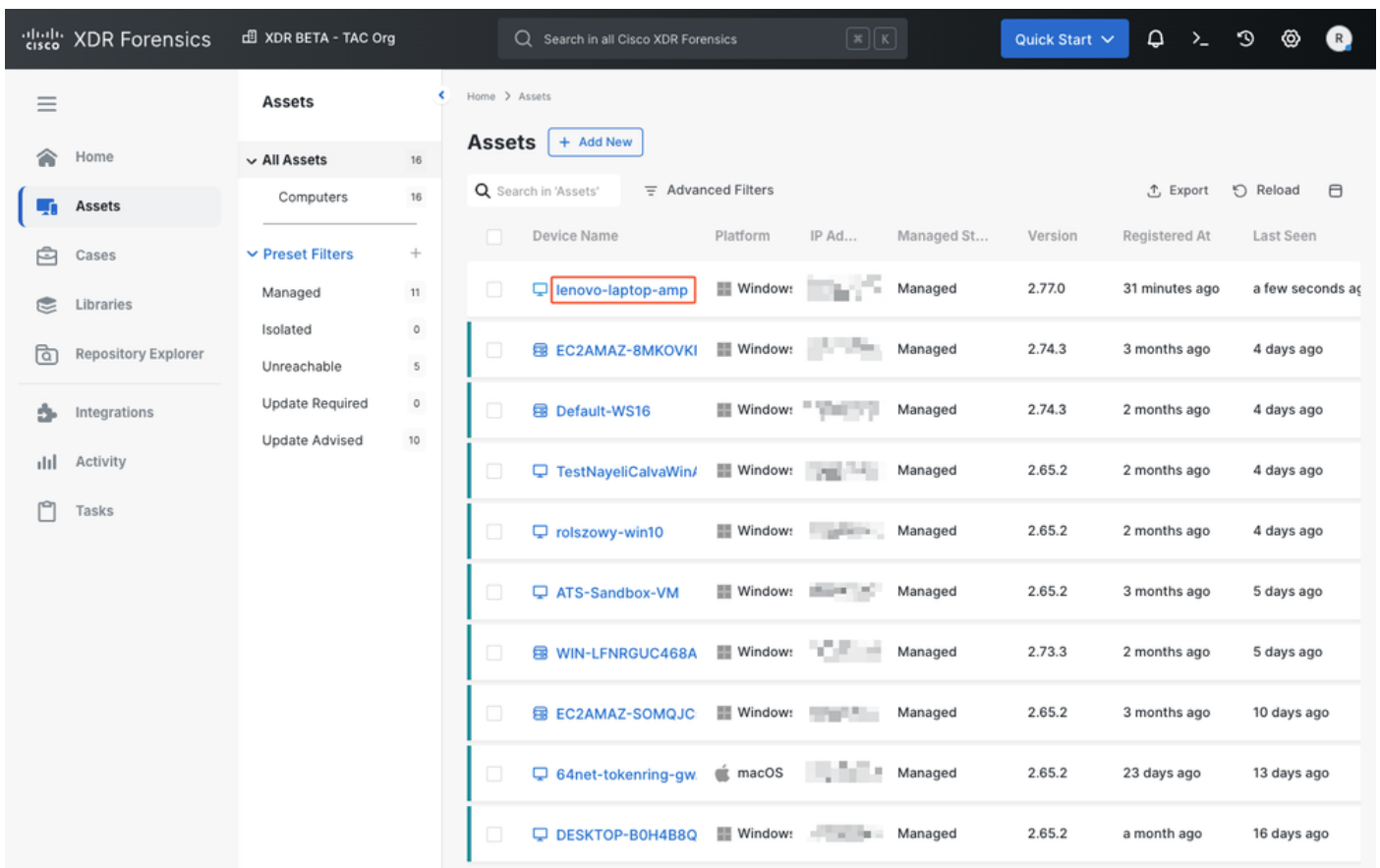
```
hostname
```

```
lenovo-laptop-amp
```

لوصولأ عيمج ضرع قوف رقنا، XDR ةيئانجل ةلدأل مكحت ةدحول ةيسيئرلأ ةحفصلأ يف ب)
(راسلأ ىلع لوصولأ ةمئاق مدختسأ وأ).



اهلي صافات لاخدا ل زاهج ل مسا يل ع ر ق ن و ا ة م ئ ا ق ل ا يل ع ة ي ا ه ن ل ا ة ط ق ن ة م ج ر ت ب م ق ج



تال ج س ل ا ع ي م ج ت > تاء ا ر ج ا ل ا ن م د ي ز م ل ا ق و ف ر ق ن ا ، ل و ص ا ل ا ت ا م و ل ع م ة ح ف ص ي ف 3. ة و ط خ ل ا ة ي ا ه ن ل ا ة ط ق ن ن م ت ا م و ل ع م ل ا ع ي م ج ت ا د ب ل

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

Info

Tasks

Acquisitions

Triages

interACTs

Comparisons

Drone Analysis

Others

Scheduled Tasks

Acquisitions

Triages

Others

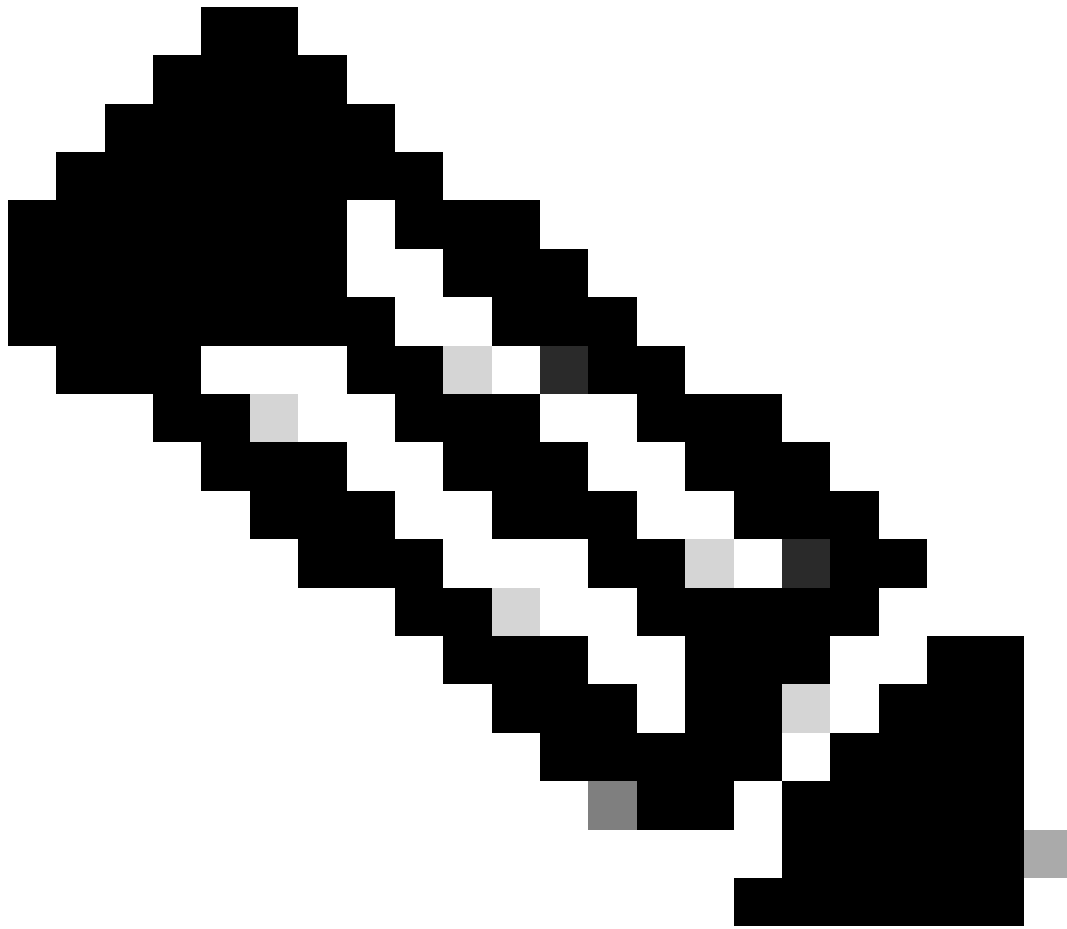
Cases

Open

Closed

Archived

Logs



ناوٲ عضب هلامتكا قرغتسي، تنرتن إلاب الصتم لصألا ناك اذا :ةظحالم

ف. لعفلاب تالچسلا عيمجت مت دق ناك اذا ام ةفرعمل تالچسلا مسق ىلإ لقتنا 4. ةوطخلا
تالچسلا ليزنت ادبل زمرلا قوف رقنا ،لوصألا تالچس مسق

The screenshot shows the Cisco XDR Forensics interface for an asset named 'lenovo-laptop-amp'. The left sidebar contains a navigation menu with categories like 'Info', 'Tasks', 'Acquisitions', 'Triages', 'interACTs', 'Comparisons', 'Drone Analysis', 'Others', 'Scheduled Tasks', 'Cases', and 'Logs'. The 'Logs' category is highlighted with a red box and a red '1' indicating it is the selected view. The main panel displays 'Asset Logs' for the selected asset, showing a table with columns: Name, Status, Duration, Created At, and Actions. A single log entry is visible: 'Log Retrieval 001' with a status of 'Completed', a duration of '00:00:00', and a creation time of '18 minutes ago'. A red box and a red '2' highlight the download icon in the 'Actions' column of this entry.

دحول اءاطخأ فاشكئسالةبولطم تافل م ةثالث لىل عيوتحي *.zip Acquired فلم 5 ةوطخل اءاحالصإو ةيطنلل:

- air.log.txt
- air.process.log.txt
- tactical-legacy.log.txt

The screenshot shows a file explorer window displaying the contents of a folder named 'lenovo-laptop-amp_Log Retrieval 001'. The folder contains four files: 'AIR.Log.txt', 'AIR.Process.Log.txt', 'TACTICAL-Legacy.Log.txt', and 'lenovo-laptop-amp_Log Retrieval 001.zip'.

ةمچرتل هذه لوح

ةللآل تاي نقتل نم ةومجم مادختساب دنتسمل اذه Cisco تمچرت
ملاعلا اناء عي مجي في ني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوكت نل ةللآل ةمچرت لصف اناء ظحال مچري. ةصاخلا مهتغلب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحا وه
ىل ائاد عوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلال يزيلچنل دنتسمل