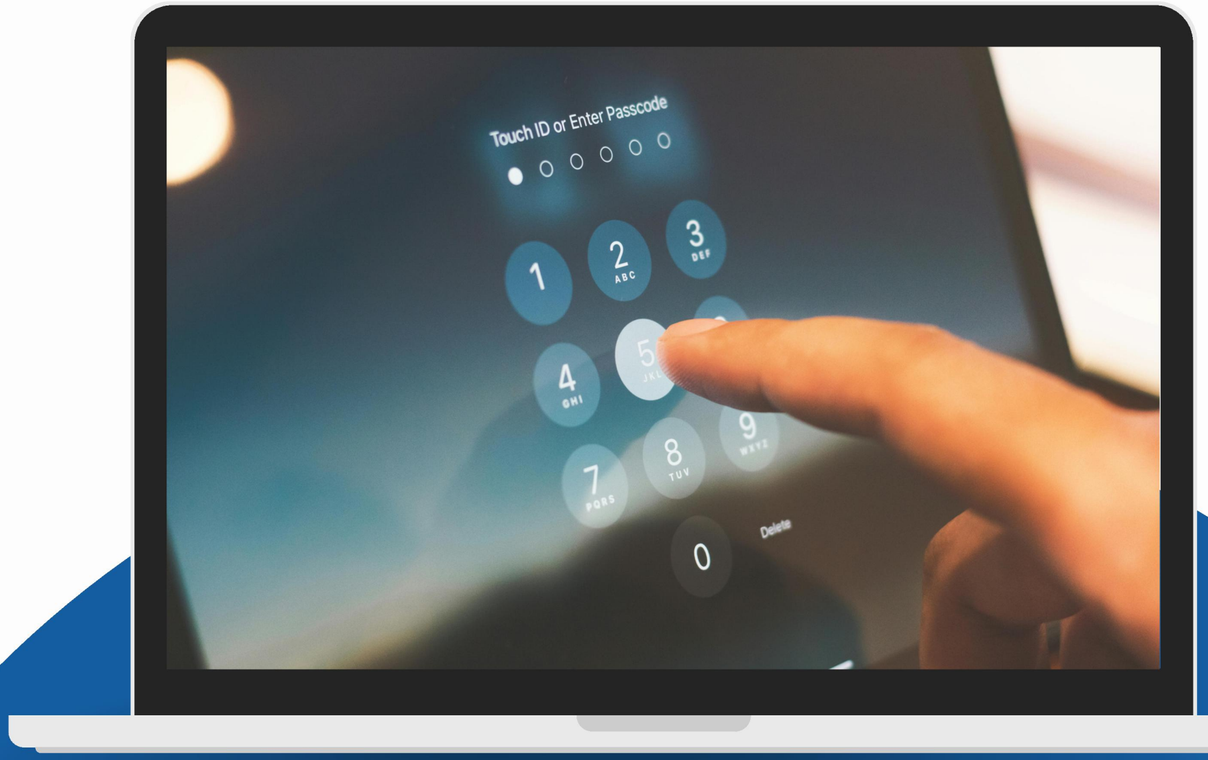
Advancing Mobile Forensic: A New Data Acquisition Method



By: ภัทรรัตน์ หอมกระจ่าง
ธัญญ์พงศ์ อินทรสอน
สุธาวินี ลิ้มสุวรรณ

กลุ่มตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ กองตรวจพิสูจน์ทางวิทยาศาสตร์

Overview

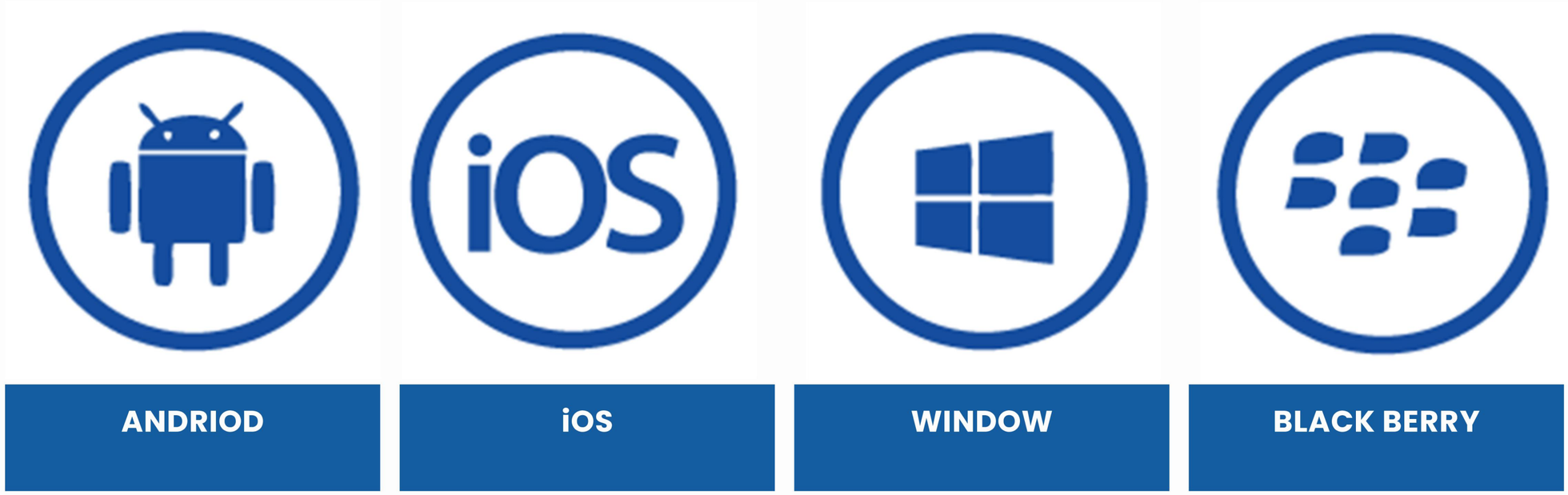
- Introduction: mobile forensic — ภัทรรัตน์
  - ระบบปฏิบัติการ
  - ข้อมูลที่ได้จากอุปกรณ์สื่อสารเคลื่อนที่
  - Software ที่ใช้ตรวจพิสูจน์
- การเก็บวัตถุพยาน — สุธาวินี
  - collect and preserve
- data acquisition คืออะไร — ธัญญ์พงศ์
  ปัญหาที่พบในปัจจุบัน
  new method
- case study — ธัญญ์พงศ์ สุธาวินี
  los
  android

MOBILE FORENSIC

Mobile device forensics has become essential in modern digital investigations, with smartphones and tablets containing critical evidence for both criminal and corporate cases. The fundamentals of mobile forensics, from evidence extraction and analysis to best practice considerations. Understanding how to properly collect and analyze mobile device evidence is crucial for successful forensic examinations.

https://www.forensicfocus.com/guides/mobile-forensics

Operating System



ANDRIOD	iOS	WINDOW	BLACK BERRY

The forensic examination of mobile devices can reveal a wealth of digital evidence crucial to investigations. Understanding the full scope and potential of this evidence is essential for conducting thorough examinations.

Communication Records

SMS/MMS, Chat Apps and Call Logs

Mobile App Data

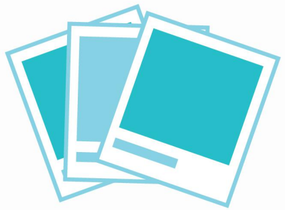
Web History, Social Media and User Activity

Location and Movement Data

GPS coordinates, cellular network , Wi-Fi and Bluetooth connection

System and Device Data

Device configuration, software installations, and system events create



Media and Files

Digital Images and Videos, Audio Recording, Document and Files

Health and Lifestyle Data

health metrics, and daily routines

SOFTWARES

Cellebrite Inseots

MAGNET AXIOM

Belkasoft
forensics made easier

Oxygen Forensic® Detective
Version 15.3 | February 2023

MSAB

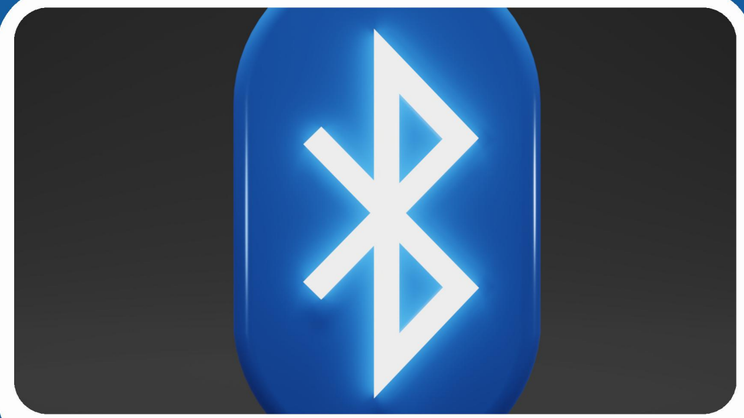
MOBILedit®

Evidence Collection and Preservation

Evidence Collection and Preservation

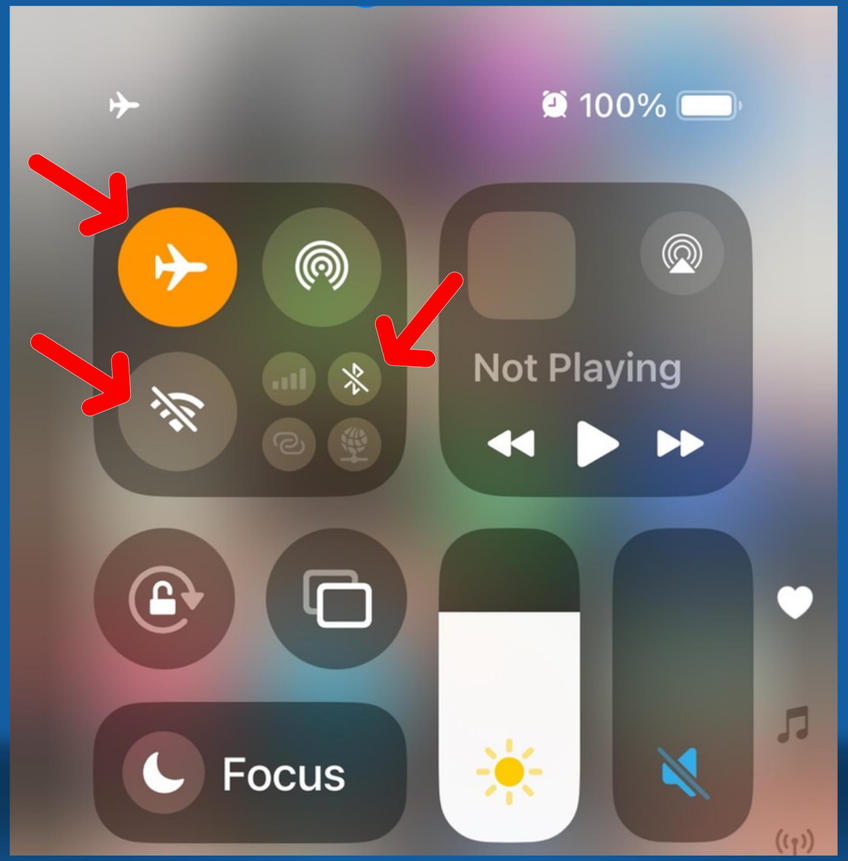
โหมดเครื่องบิน
Flight mode
Airplane mode
Aeroplane mode

Wi-Fi

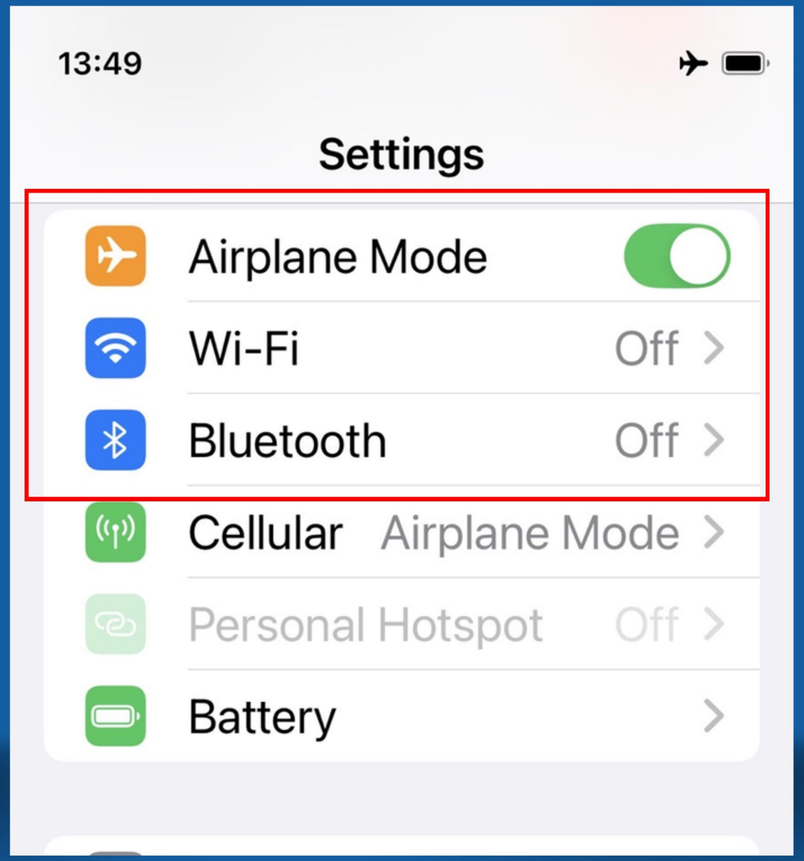


บลูทูธ
Bluetooth

Evidence Collection and Preservation

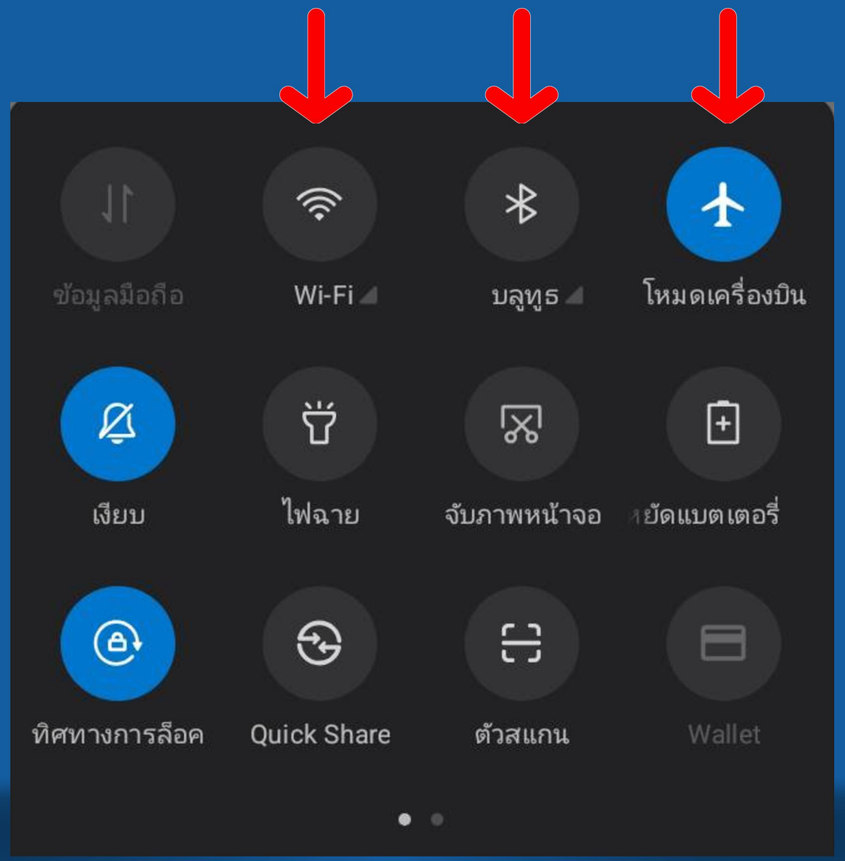


ศูนย์ควบคุม
(Control Center)

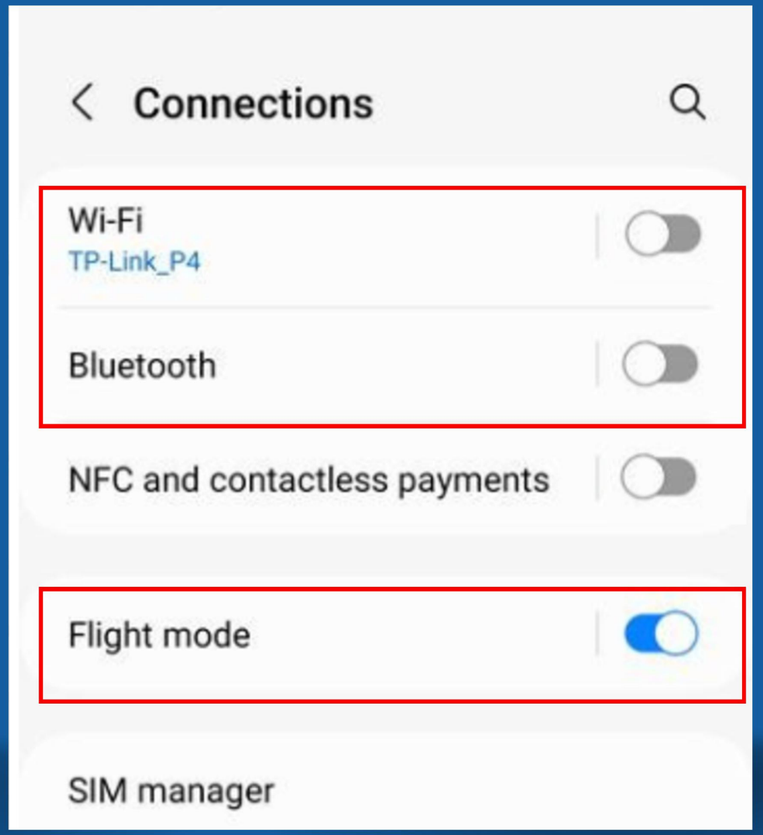


การตั้งค่า (Setting)

Evidence Collection and Preservation



แผงการตั้งค่าด่วน (Quick Settings panel)



การตั้งค่า (Setting)

Evidence Collection and Preservation

ชาร์จแบตเตอรี่

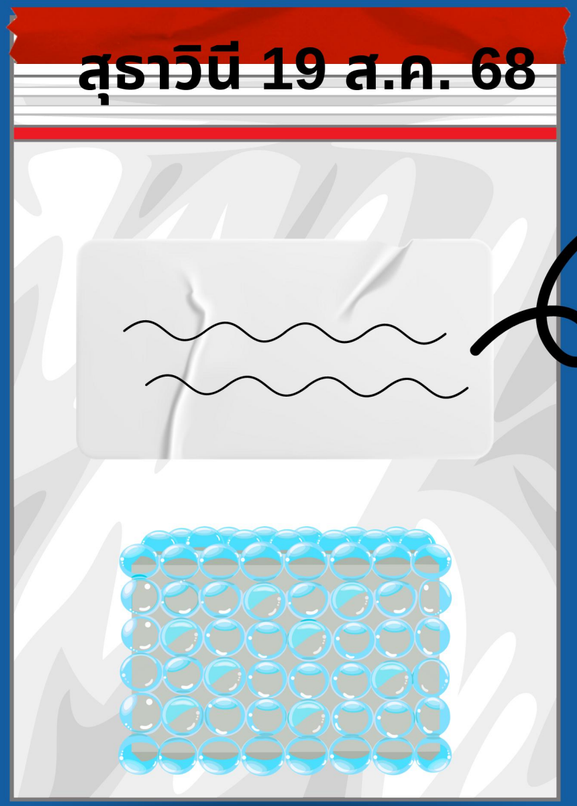
Evidence Collection and Preservation

หีบห่อ Faraday Bag

Evidence Collection and Preservation

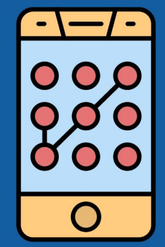
หีบห่อ กรงฟาราเดย์แบบฟอยล์อลูมิเนียม

Evidence Collection and Preservation



ระบุ รายละเอียดวัตถุพยาน (สังเขป)
และรหัสการเข้าถึง

passcode



pattern

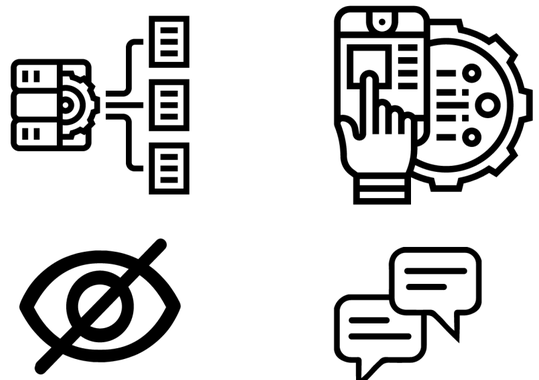
หีบห่อ

DATA ACQUISITION

In digital forensics, data acquisition is the critical process of creating an exact, bit-by-bit copy of digital evidence from electronic devices. The goal is to preserve the integrity and authenticity of the original data, ensuring it remains unaltered for legal admissibility. Specialized tools are used to prevent any modification to the source, making the forensic image a reliable duplicate for subsequent analysis and investigation.

Data acquisition

Logical Acquisition



File System Acquisition

Physical Acquisition

Data acquisition

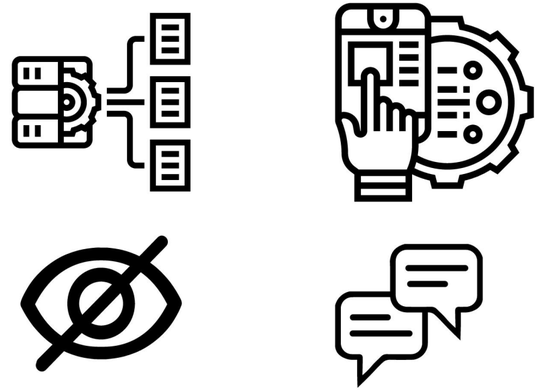
Logical Acquisition

Logical

- SMS
- Contacts
- Call logs
- Media
- App data

เป็นการเก็บข้อมูลที่ผู้ใช้สามารถมองเห็นได้ตามปกติ เช่น ไฟล์, โฟลเดอร์, รายชื่อติดต่อ, SMS, และข้อมูลแอปพลิเคชันบางส่วนที่อยู่ในฐานข้อมูล การทำ Logical Acquisition จะไม่เข้าถึงข้อมูลที่ถูกลบหรืออยู่ในพื้นที่ที่ระบบไม่อนุญาตให้เข้าถึงโดยตรง

Data acquisition

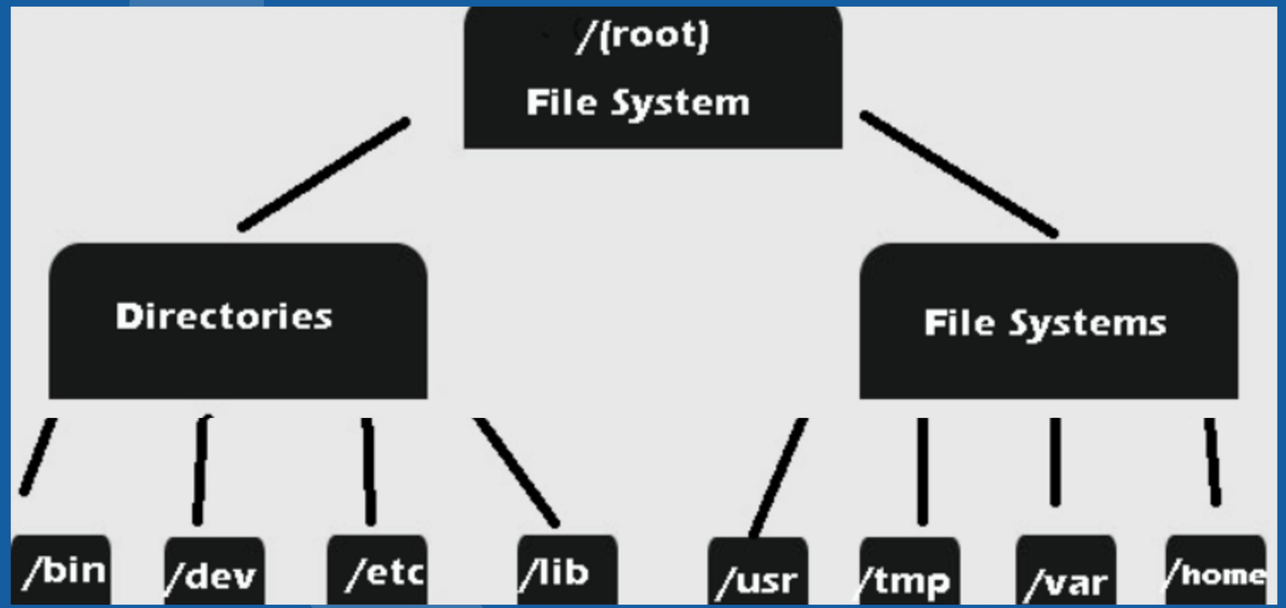


File System Acquisition

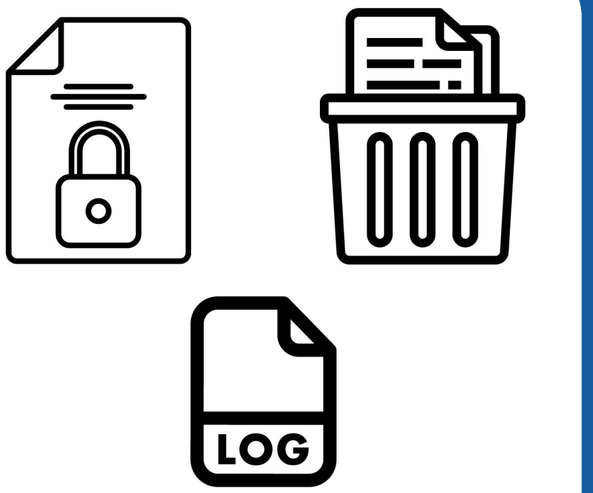
File System

- SMS
- Contacts
- Call logs
- Media
- App data
- Files
- Hidden Files

เป็นการเก็บข้อมูลที่ลึกกว่า Logical โดยจะเข้าถึงโครงสร้างระบบไฟล์ทั้งหมดของอุปกรณ์ ซึ่งรวมถึงไฟล์ของระบบและไฟล์ที่ถูกซ่อนไว้ แต่ยังไม่สามารถกู้คืนข้อมูลที่ถูกลบได้สมบูรณ์



Data acquisition



Physical Acquisition

Physical

- SMS
- Contacts
- Call logs
- Media
- App data
- Files
- Hidden Files
- Deleted data

เป็นการคัดลอกข้อมูลแบบ Bit-for-bit จากหน่วยความจำของอุปกรณ์โดยตรง ถือเป็นวิธีเข้าถึงข้อมูลได้มากที่สุด allocated และ unallocated space ที่ไม่สามารถเข้าถึงได้ด้วยวิธีอื่น

Data acquisition

ข้อจำกัด

Logical Acquisition

ไม่สามารถกู้คืนข้อมูลที่ถูกลบไปแล้วได้
ไม่สามารถเข้าถึงข้อมูลที่ถูกเข้ารหัสในระดับที่ลึกกว่า
ไม่ได้ข้อมูล Full File System
ไม่สามารถเข้าถึงพื้นที่ Unallocated Space (พื้นที่ที่ว่างแต่เคยมีข้อมูลอยู่)

File System Acquisition

โดยทั่วไปไม่สามารถกู้คืนข้อมูลที่ถูกลบได้อย่างสมบูรณ์จากพื้นที่ Unallocated Space
ไม่สามารถเข้าถึงข้อมูลที่ถูกเข้ารหัสสูงสุด (เช่น Secure Enclave) ได้ทั้งหมดในอุปกรณ์รุ่นใหม่

Physical Acquisition

ต้องใช้เครื่องมือเฉพาะและความเชี่ยวชาญสูง
อาจทำให้อุปกรณ์เสียหายถ้าใช้วิธีแบบ invasive เช่น chip-off
อุปกรณ์บางรุ่นมีการเข้ารหัสเต็มรูปแบบ (Full Disk Encryption) ทำให้ข้อมูลไม่สามารถอ่านได้หากไม่มี key

CHALLENGES IN MOBILE PHONE DATA ACQUISITION

Encryption

เป็นเทคโนโลยีการเข้ารหัสข้อมูลแบบทั้งดิสก์ โดยการเข้ารหัสข้อมูลทุกส่วนบนอุปกรณ์จัดเก็บข้อมูล ให้กลายเป็น ciphertext ที่ไม่สามารถอ่านได้โดยไม่มีคีย์ถอดรหัสที่ถูกต้อง เช่น PIN/รหัสผ่าน/ลายนิ้วมือ ตอนเข้าเครื่อง

Full Disk Encryption FDE

เป็นระบบการเข้ารหัสข้อมูลแบบแยกไฟล์หรือโฟลเดอร์ แทนการเข้ารหัสทั้งดิสก์ (FDE) โดยแต่ละไฟล์ถูกเข้ารหัสด้วยคีย์ที่ไม่เหมือนกัน ทำให้มีความยืดหยุ่นและความปลอดภัยสูงขึ้น
เช่น รหัสใน แอปธนาคาร หรือแอปสำคัญ รูปภาพ/วิดีโอใน Gallery ที่ล็อกด้วย App Lock

File Based Encryption FBE

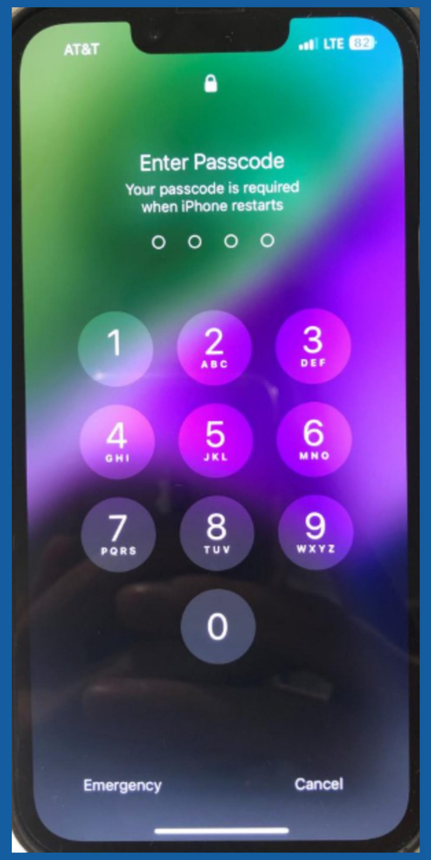
สภาพแวดล้อมที่ปลอดภัยและแยกออกจากระบบหลัก ออกแบบมาเพื่อประมวลผลข้อมูลสำคัญด้วยความปลอดภัยสูง โดยข้อมูลถูกป้องกันทั้งจากซอฟต์แวร์และฮาร์ดแวร์ แม้ระบบหลักถูกแฮกก็ไม่สามารถเข้าถึงได้ เช่น ระบบล็อกด้วยลายนิ้วมือ/Face ID การดูหนัง/ฟังเพลงแบบ DRM (เช่น Netflix, Disney+) Secure Enclave

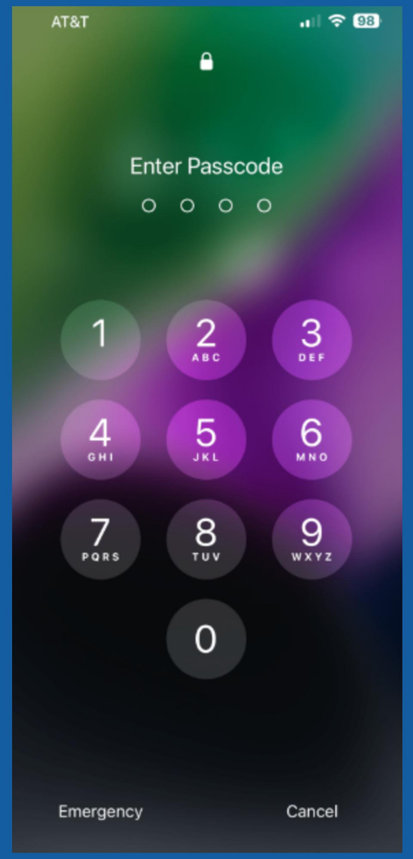
Trusted Execution Environment (TEE)

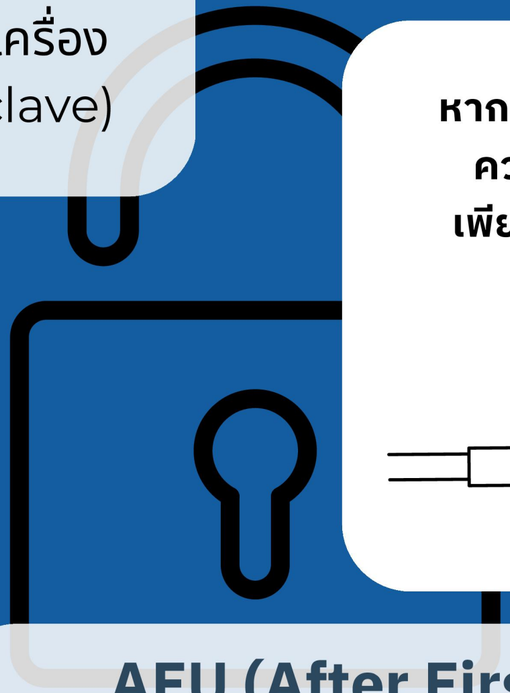
AFU & BFU

BFU (Before First Unlock)

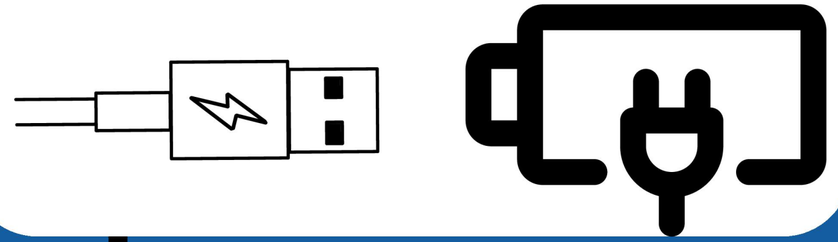
สถานะที่มือถือถูกบูตแล้วแต่ยังไม่ป้อนรหัสผ่าน/ลายนิ้วมือหลังเปิดเครื่อง ข้อมูลส่วนใหญ่ยังถูกเข้ารหัสด้วยคีย์ระดับฮาร์ดแวร์ (Secure Enclave)







หากอุปกรณ์อยู่ในสถานะ AFU (ปลดล็อกอยู่) ควรเสียบสายชาร์จเพื่อรักษาพลังงานให้เพียงพอ ก่อนที่แบตเตอรี่จะหมดและเครื่องจะเข้าสู่สถานะ BFU



AFU (After First Unlock)

สถานะที่มือถือ ถูกปลดล็อกแล้วอย่างน้อย 1 ครั้ง ระบบปล่อยคีย์ถอดรหัสบางส่วนให้ซอฟต์แวร์ใช้งาน

https://blogs.dsu.edu/digforce/2023/08/23/bfu-and-afu-lock-states/

Remote Wipe

Remote Wipe (การลบข้อมูลระยะไกล) คือ ฟีเจอร์ที่อนุญาตให้ผู้ใช้หรือผู้ดูแลระบบลบข้อมูลทั้งหมดในอุปกรณ์แบบไร้สายผ่านเครือข่ายอินเทอร์เน็ตหรือเซลลูลาร์ มักใช้ในกรณีที่อุปกรณ์สูญหายหรือถูกขโมย เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

Turbo Link / Cheetah

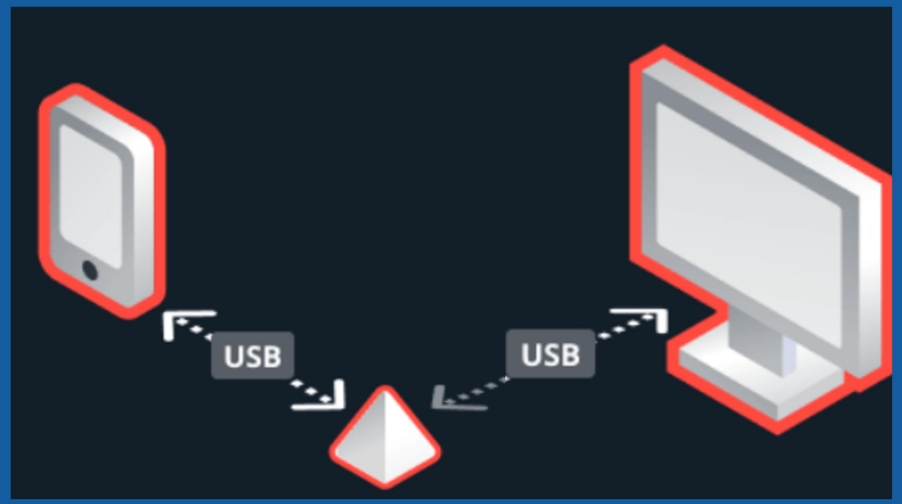
Turbo Link (ชื่อรหัสเดิม "Chetah")
เป็นเทคนิคใหม่ที่พัฒนาเพื่อ เร่งความเร็วการถอดรหัสข้อมูลบนอุปกรณ์มือถือ โดยเฉพาะในงานDigital Forensics ช่วยลดเวลาการดึงข้อมูลจากวัน/ชั่วโมงเหลือเพียงนาที โดยอาศัยช่องโหว่หรือจุดอ่อนในระบบความปลอดภัยของอุปกรณ์

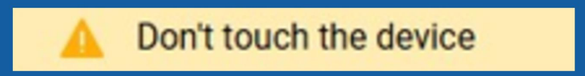
Turbo Link เป็นฮาร์ดแวร์ที่มีความสามารถในการใช้ช่องโหว่เฉพาะเพื่อเข้าถึงข้อมูลในระดับที่ลึกกว่าปกติ

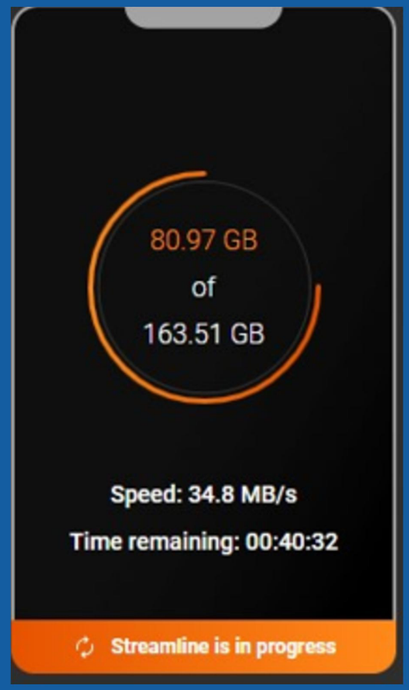
ใช้ประโยชน์จาก การเข้าถึงหน่วยความจำ (RAM) ขณะเครื่องเปิดอยู่ (AFU State) ดึง คีย์เข้ารหัสชั่วคราว ที่ระบบใช้อยู่แทนการ brute force ทั้งดิสก์

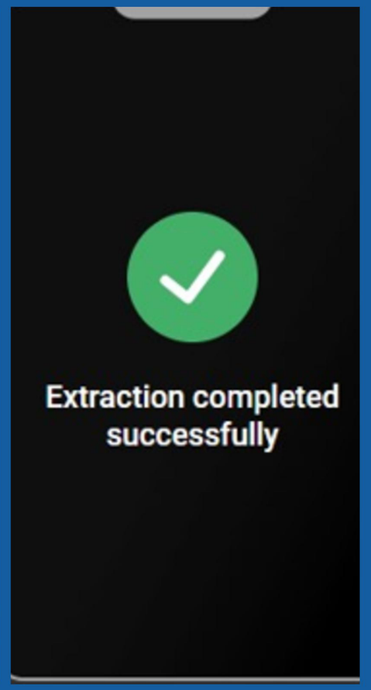
ใช้โค้ดเฉพาะผ่านช่องทางพิเศษ (เช่น Lightning Port ใน iPhone) เพื่อไม่ให้ระบบตรวจจับได้

ช่วยปลดล็อก (Unlock) อุปกรณ์บางรุ่น และดึงข้อมูลแบบ Full File System (FFS) ที่สมบูรณ์ แม้ในอุปกรณ์ที่ใช้มาตรการรักษาความปลอดภัยขั้นสูงอย่าง Secure Enclave









อาจไม่ได้ผลกับอุปกรณ์รุ่นใหม่ที่สุด (เช่น iPhone 15 ที่ปิดช่องโหว่แล้ว)
ต้องอยู่ในสถานะ AFU (After First Unlock)

https://cellebrite.com/en/cellebrite-inseyets-focus-hub/

CASE STUDY

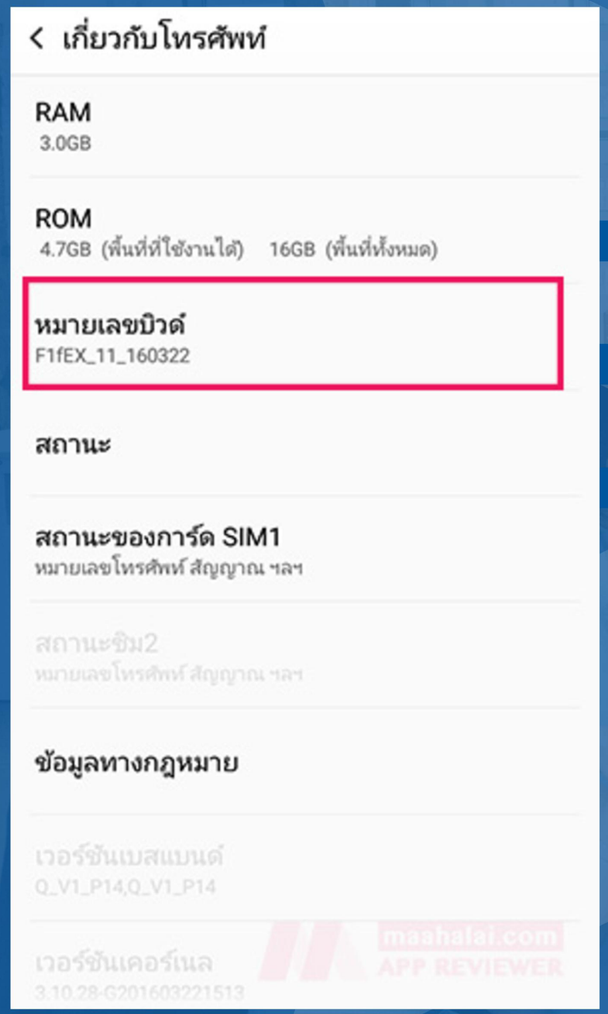
ios & android

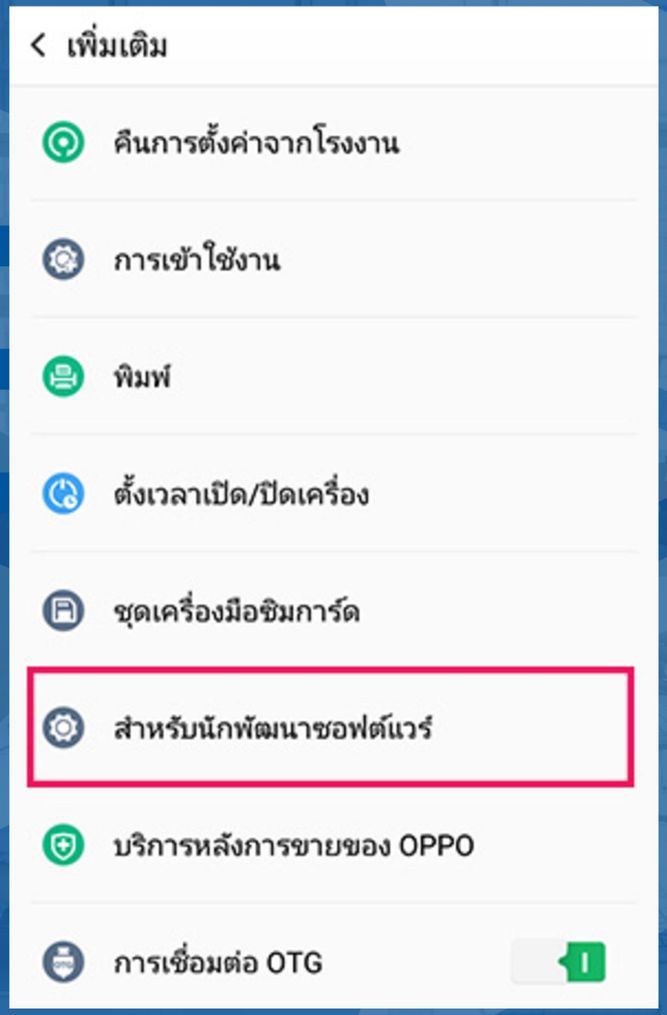
โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

ขนาดความจุ 125 GB

Vendor: OPPO
Marketing Model: OPPO Reno10 5G
OS: 15
Chipset: MT6877V/TTZA
Model: CPH2531
IMEIs: [redacted]

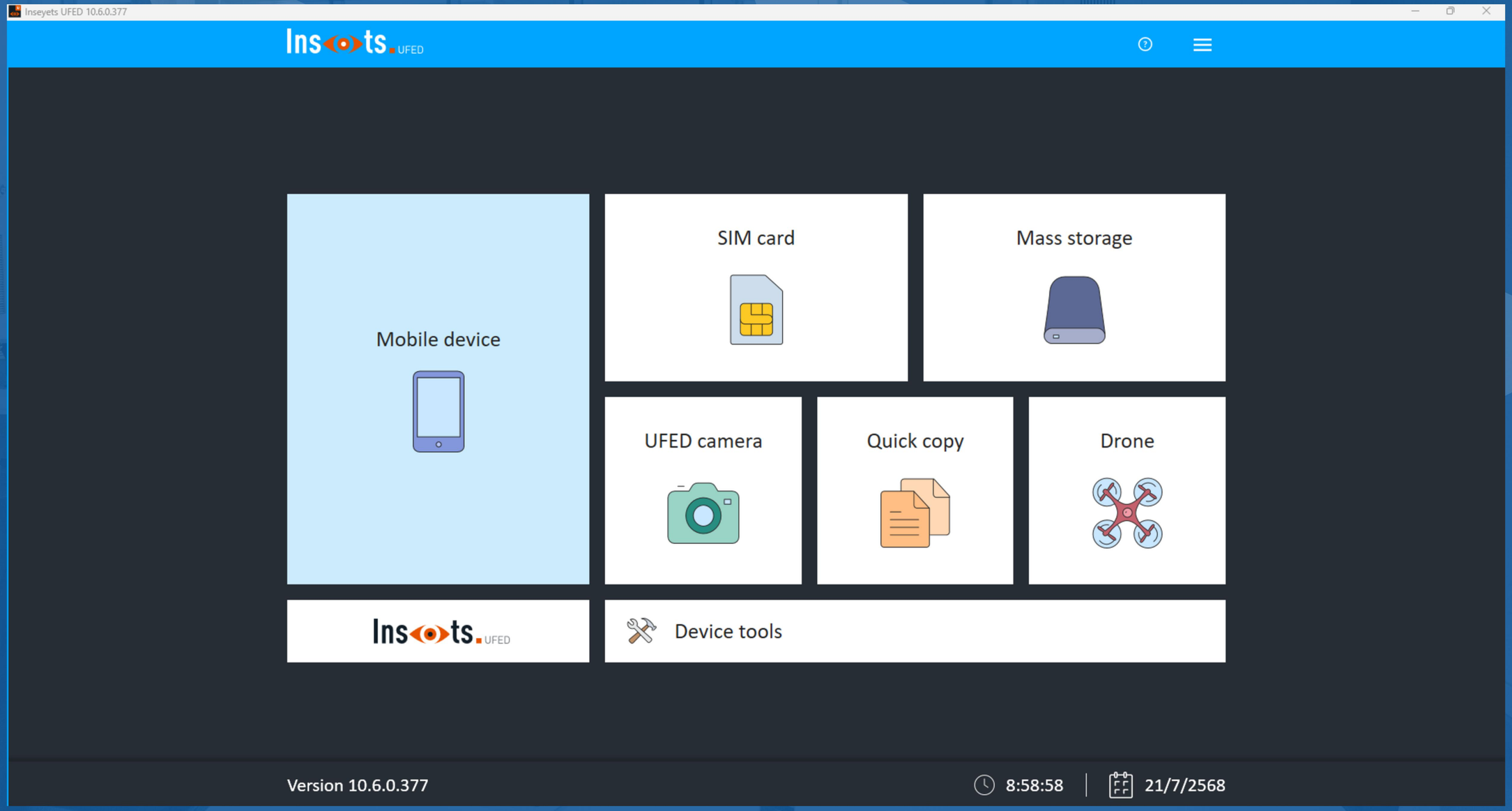
โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G



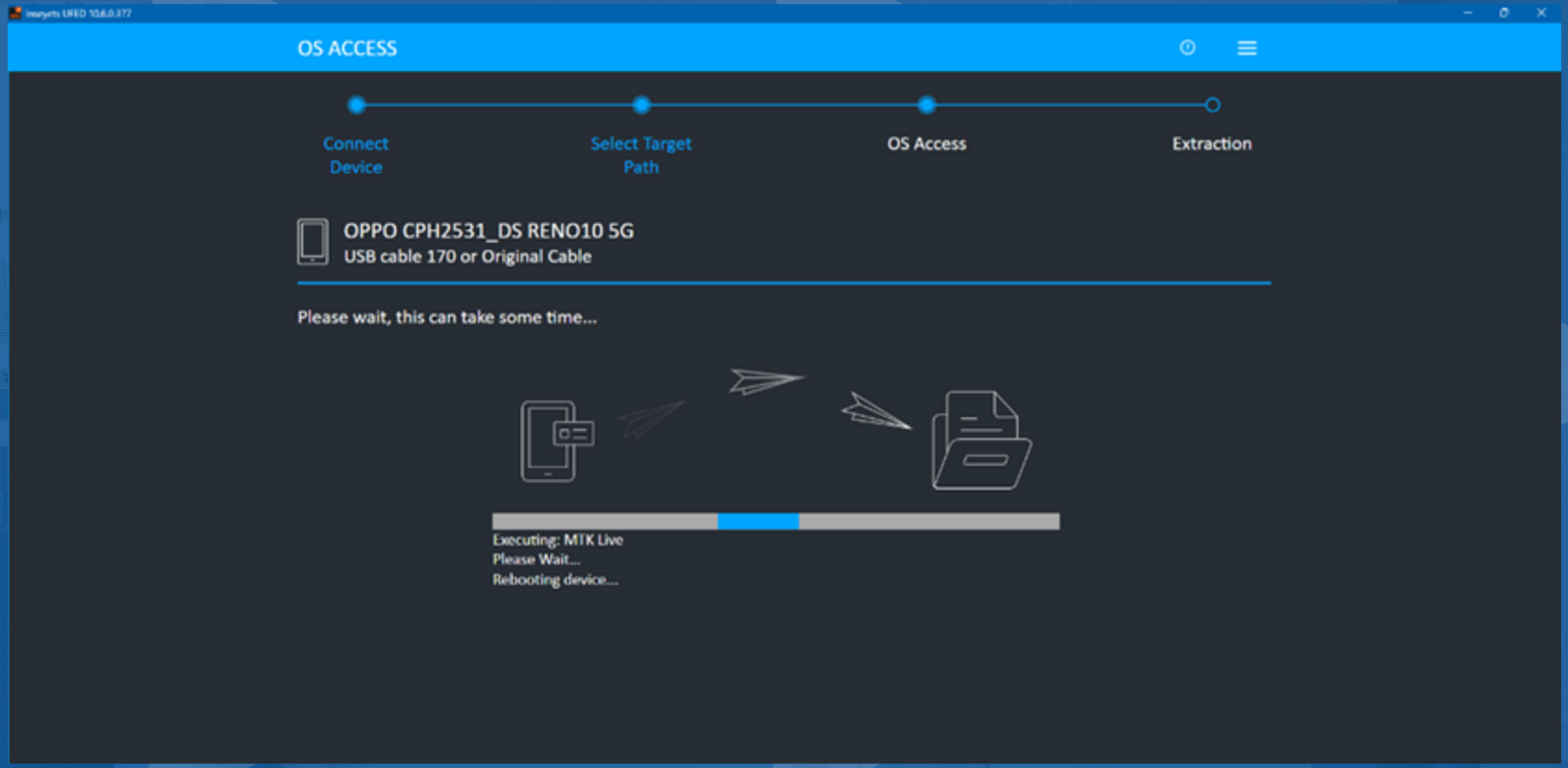


โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

Inseyets UFED



โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G



Inseyets UFED 3 ครั้ง - Not Success

โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

Cellebrite Inseyets

Inseyets UFED 10.6.0.377

Inseyets UFED

8:14 23/7/2025

Android > Unlocked

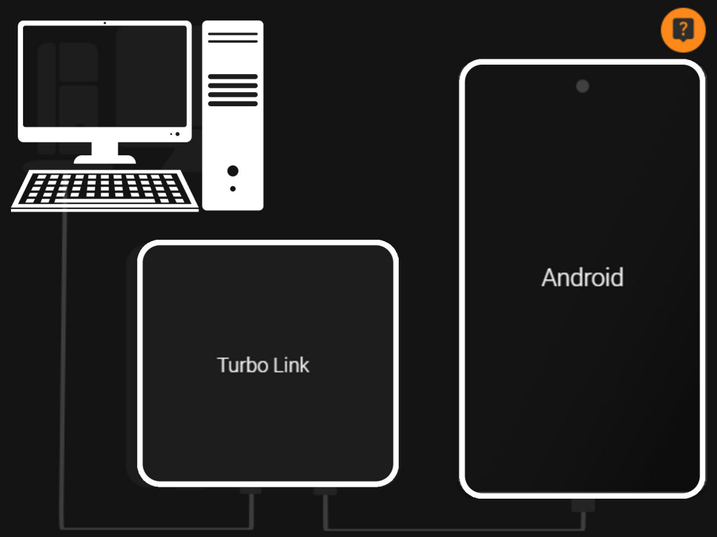
Preparation steps

01 Connect Turbo Link to computer.

02 Initializing the Turbo Link environment.

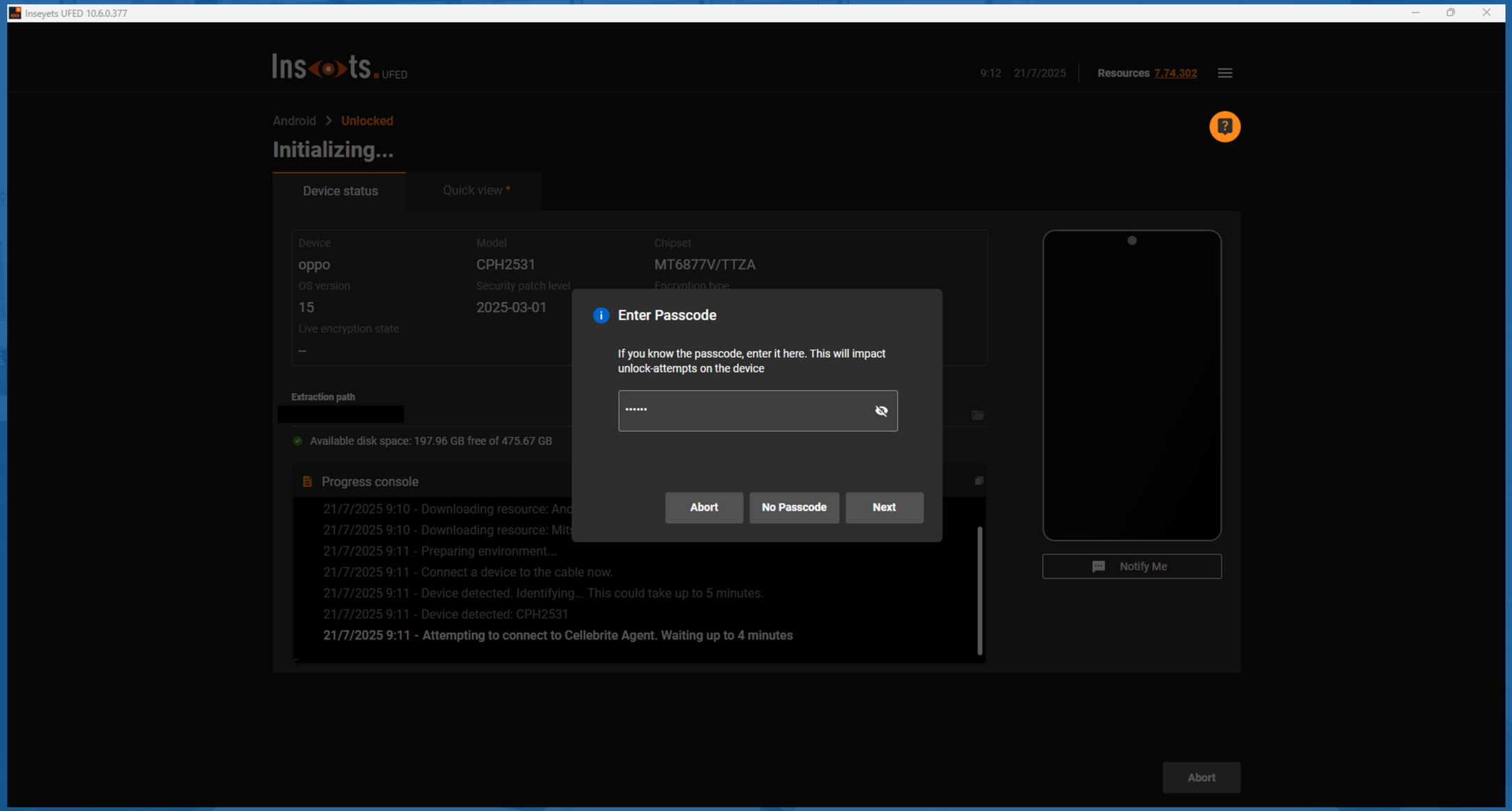
03 Connect device to Turbo Link.

Unlock the device.



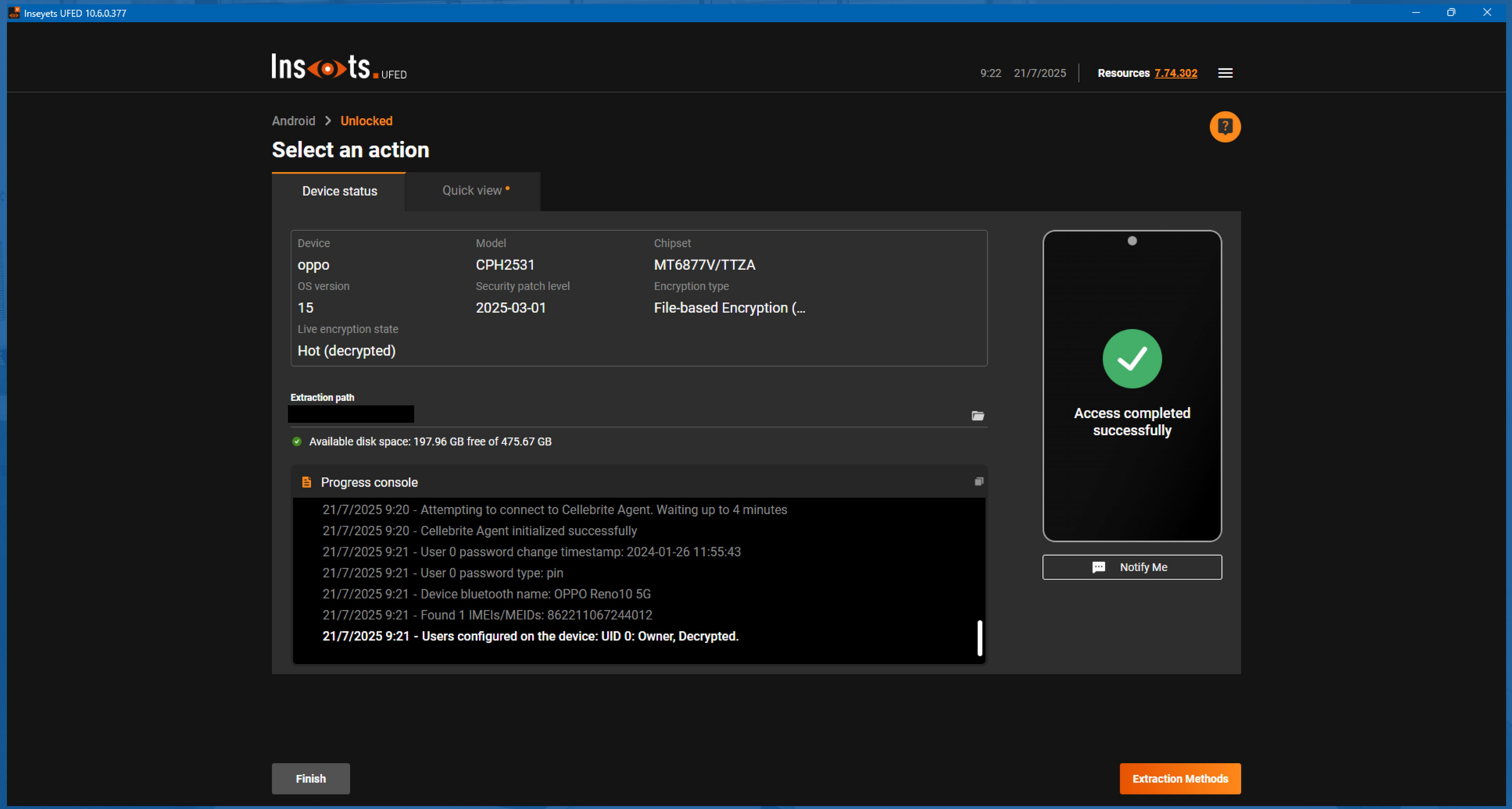
Abort

Samsung Galaxy Tab A7



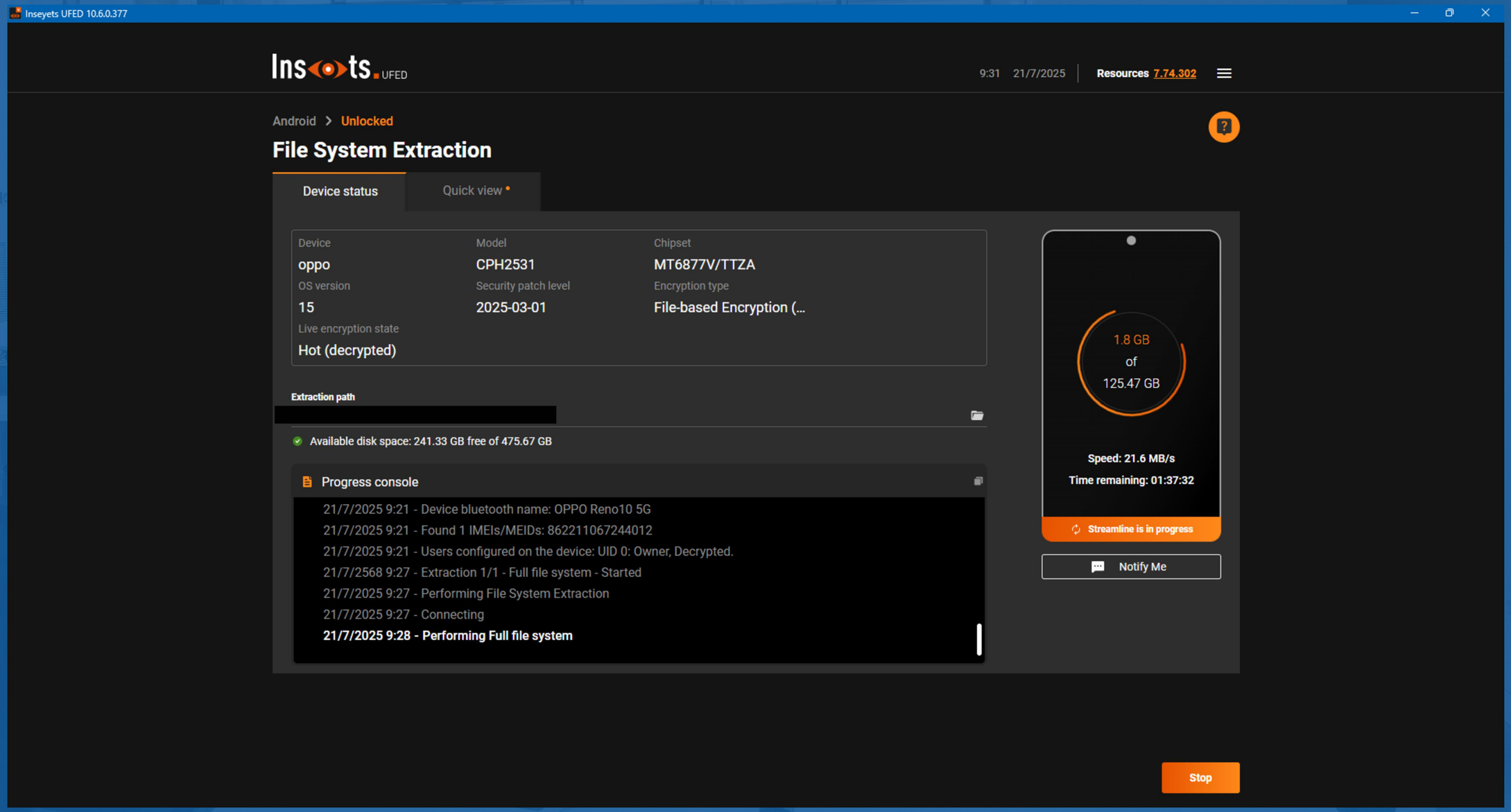
โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

Cellebrite Inseyets

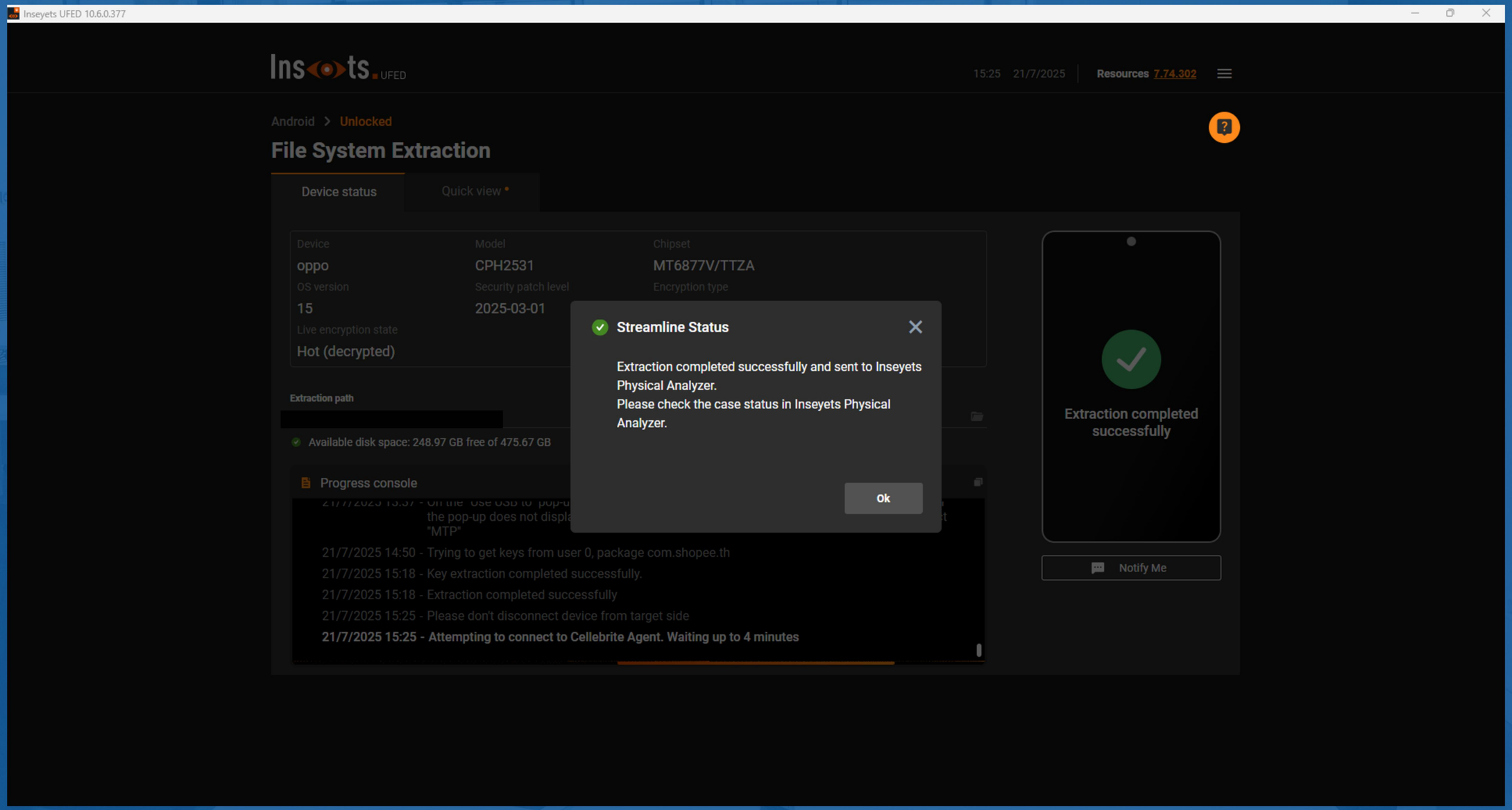


โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

Cellebrite Inseyets



โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G



โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

ขนาดความจุ 125 GB

Cellebrite Inseyets

Extraction

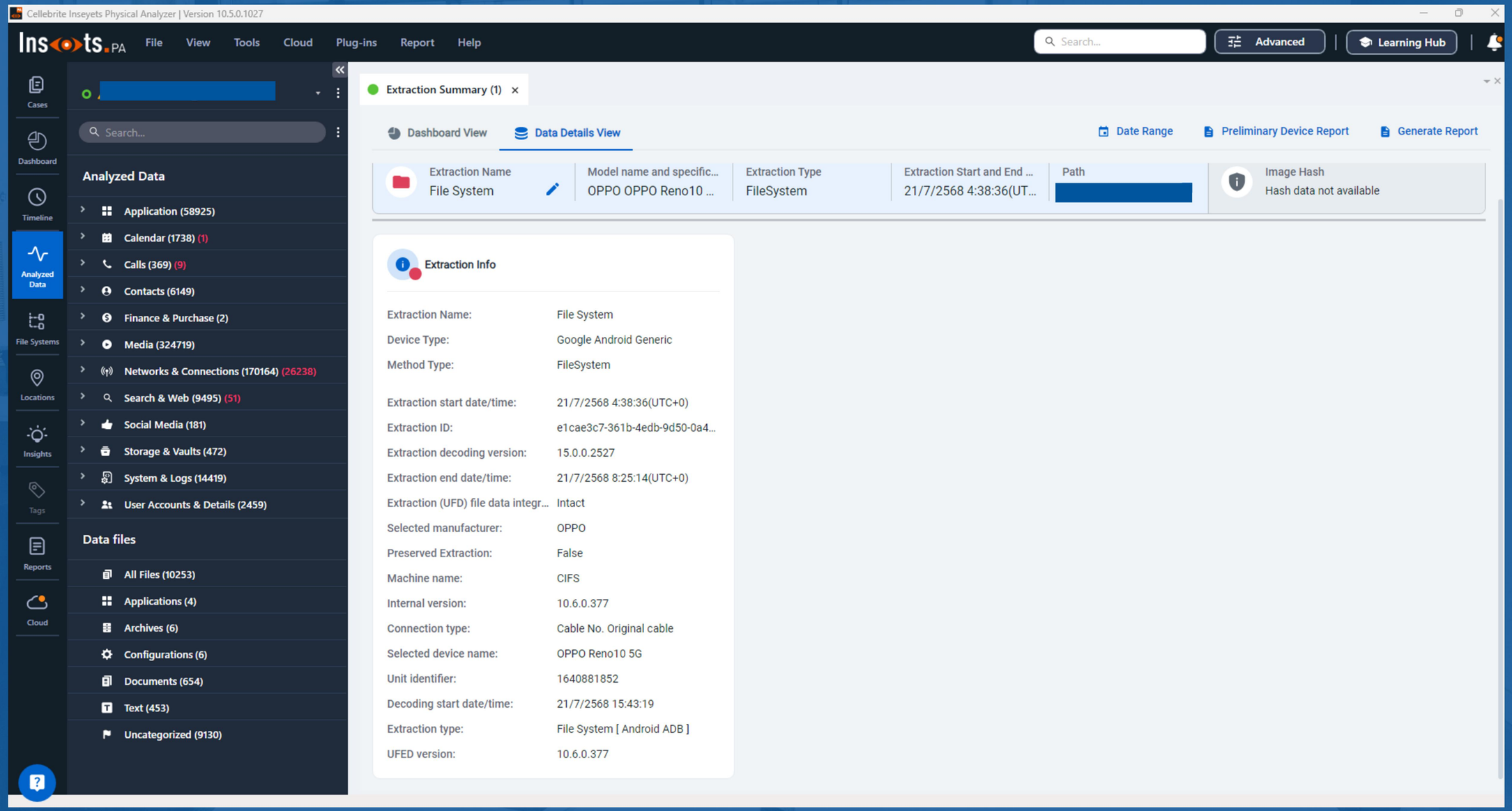
- Inseyets UFED ⟫ Not Success
- Inseyets UFED-Turbolink ⟫ Success

Extraction: Full file system | 2568-07-21 11:38:36

Extraction Type	File system
Extraction Method	Full file system
Extraction Status	Success
Extraction Start Time	2568-07-21 11:38:36
Extraction End Time	2568-07-21 15:25:14
Decryption Keys	True
File 1 Name	EXTRACTION_FFS.zip
File 1 SHA256	67384C0BFFB48590E40DB25BFFDFDFFCE0B8BC637D256F913B1D45D0579845F0

โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

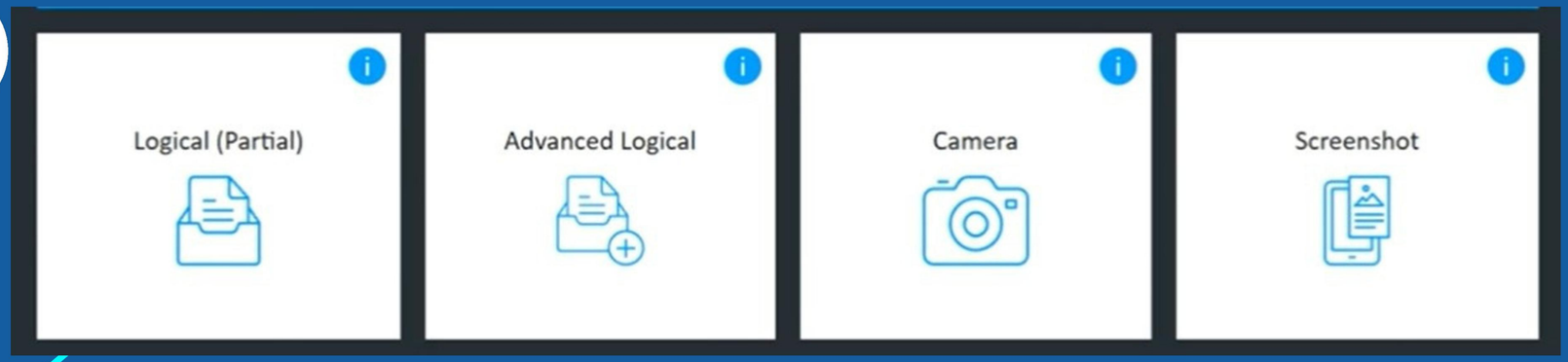
Cellebrite Ins◉ts



Apple iPhone 15 Pro

Marketing Model: iPhone 15 Pro
OS: 18.4.1
Model: D83AP
Ids:
352603483687138
352603483557505
IMSI: 520044009728279
Phone Number: 6683[redacted]
Device Name: [redacted]
Apple ID: [redacted]
Locale Language: en_TH
Vendor: Apple
Chipset: A17
Encryption Type: FBE
Device State: AFU
Live Encryption State: Hot
Bluetooth Name: [redacted]

Apple iPhone 15 Pro



Attention

Device: [redacted]
UDID: [redacted]
iOS: [redacted]
Backup: Encrypted

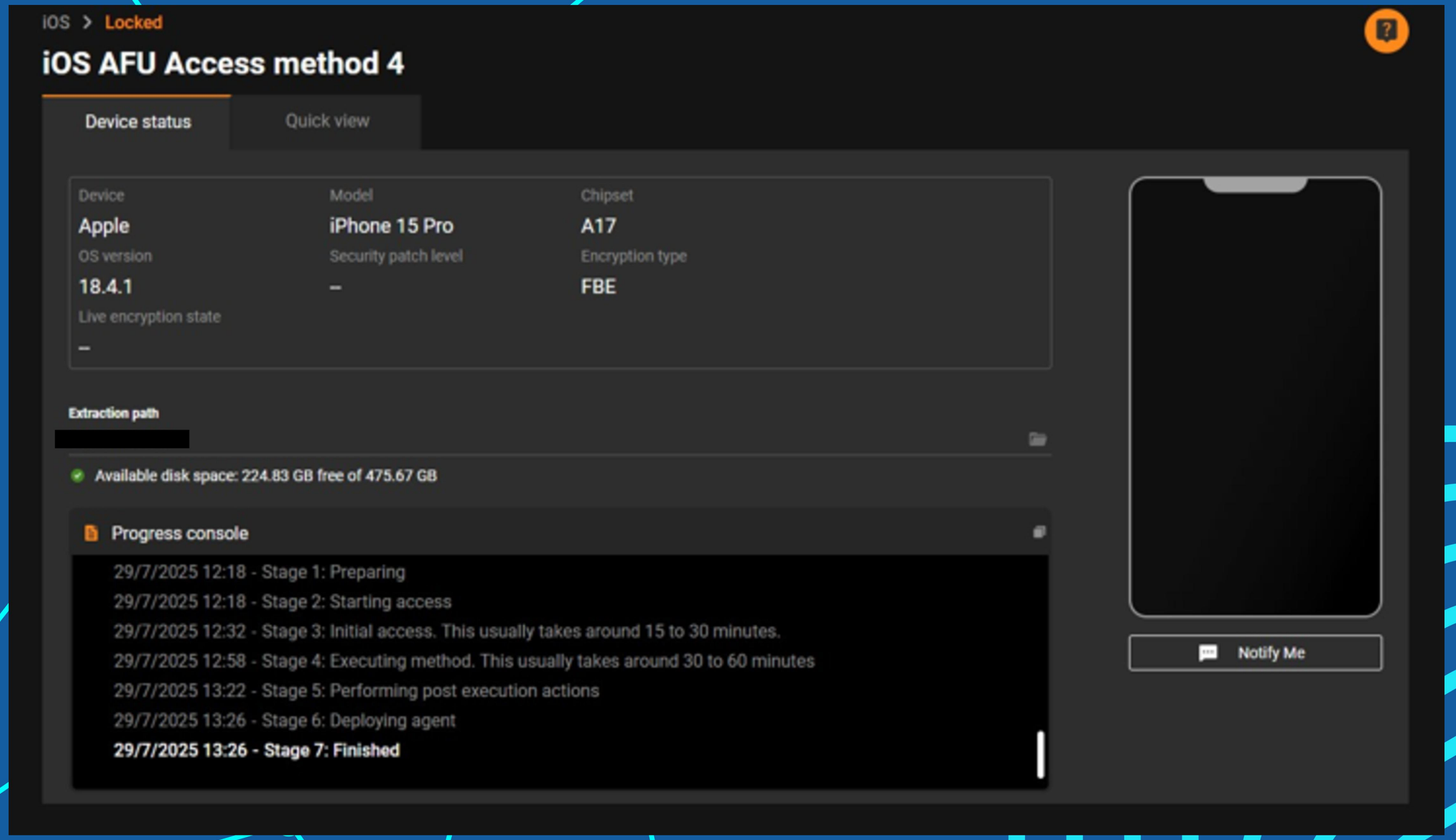
OK

Source Instructions

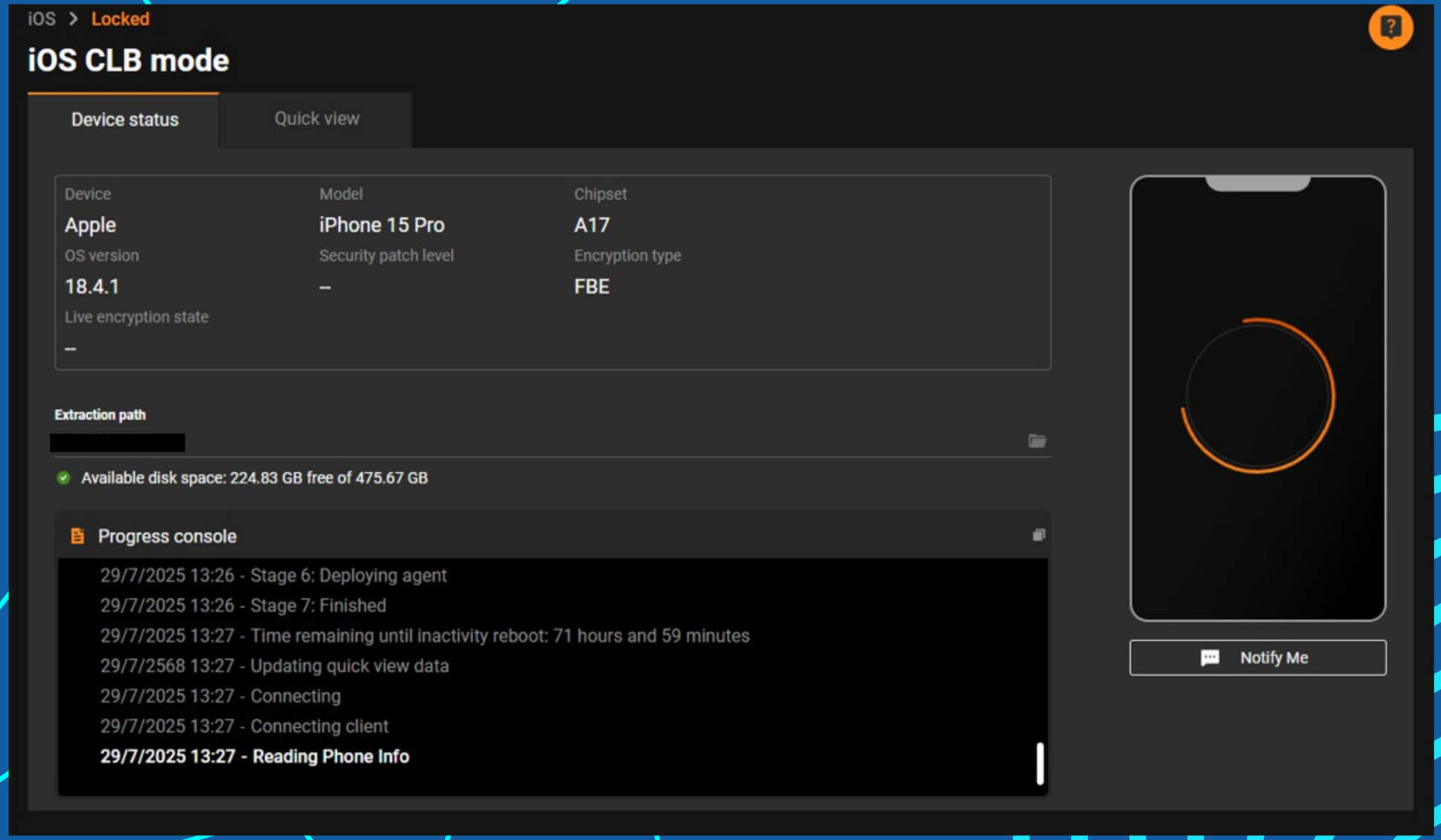
Unlock the mobile device. When the trust message appears, choose Trust.

Devices with iOS 11 or later may require you to enter the password to continue collecting data.

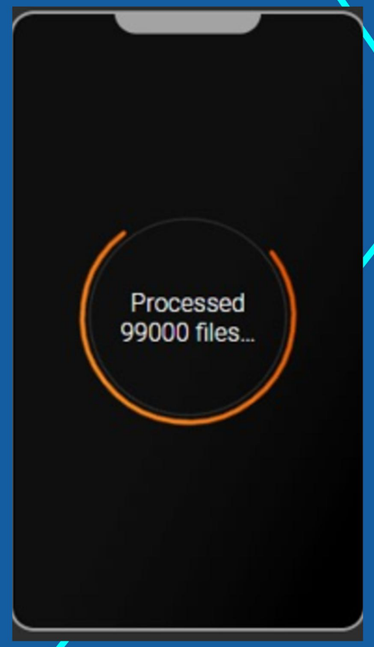
Apple iPhone 15 Pro

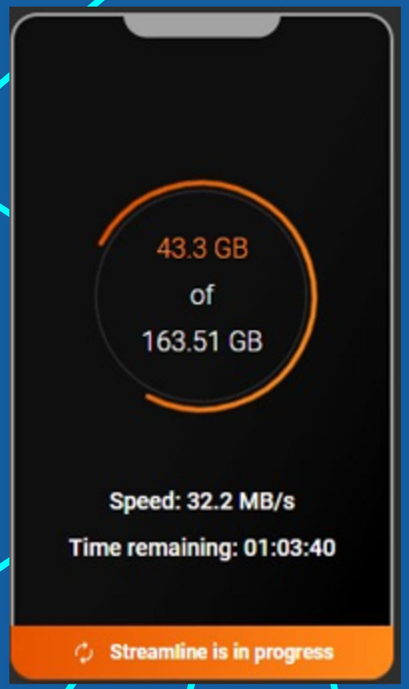


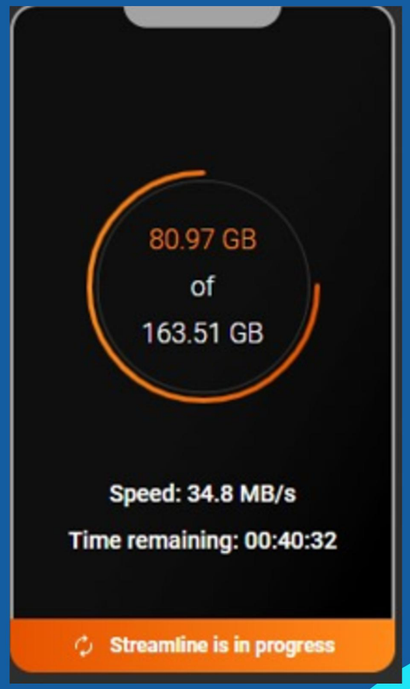
Apple iPhone 15 Pro

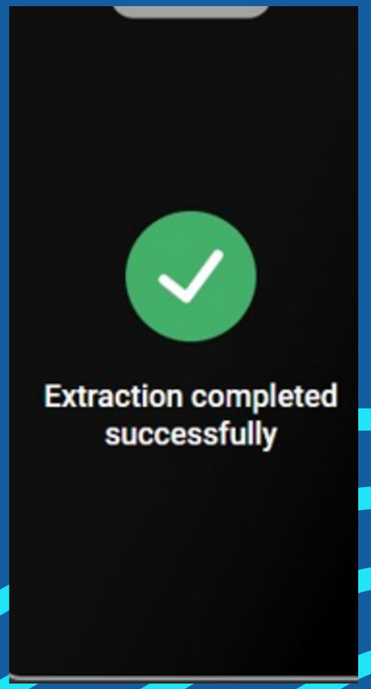


Apple iPhone 15 Pro

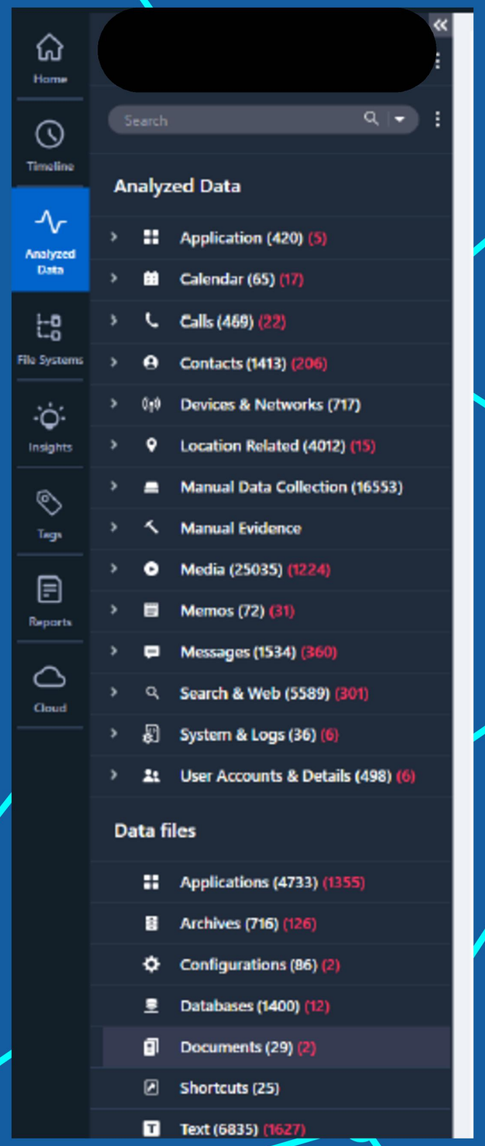








Apple iPhone 15 Pro



Device identifiers

Marketing Model: iPhone 15 Pro

OS: 18.4.1

Model: D83AP

Ids

- 352603483687138
- 352603483557505

IMSI: [redacted]

Phone Numb [redacted]

Device Name: [redacted]

Apple ID: [redacted]

Locale Language: en_TH

Vendor: Apple

Chipset: A17

Encryption Type: FBE

Device State: AFU

Live Encryption State: Hot

Bluetooth Name: [redacted]

Device user

Accounts

[redacted]

Usage details

Installed Apps

Date/Time: 2025-06-20 03:15:48.687039

Timezone: Asia/Bangkok (Asia/Bangkok)

Last Reboot Time: 2025-06-19 02:57:09

https://cellebrite.com/en/resources/guides

Thank you


LIVE
24
Mary Nara
Beautiful!
Mary Mick Donald
This place looks awesome!
Where is this?
Marsha Mello
Looks like heaven!
Sal Ami
Wonder-ful place. Lovely!
Write a comment...


LIVE
24
Mary Nara
Beautiful!
Mary Mick Donald
This place looks awesome!
Where is this?
Marsha Mello
Looks like heaven!
Sal Ami
Write a comment...


LIVE
24
Mary Nara
Mary Mick Donald
Marsha Mello
Sal Ami
Write a comment...