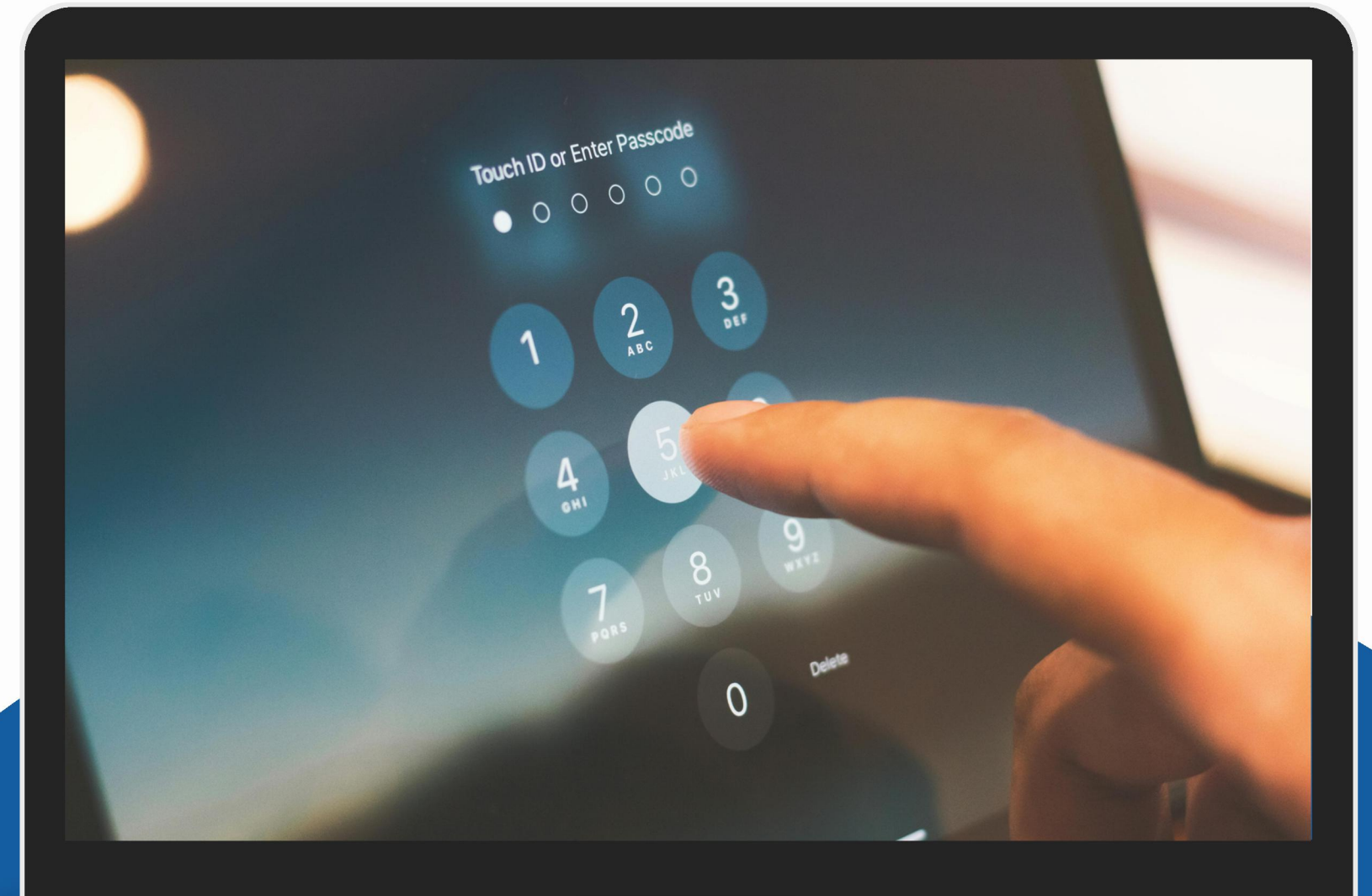


Advancing Mobile Forensic: A New Data Acquisition Method

By: กัทรรัตน์ หอมกระจ่าง
ธัญญ์พงษ์ อินทรสอน
สุธาวิณี ลิ้มสุวรรณ



Overview



Introduction: mobile forensic

- ระบบปฏิบัติการ
- ข้อมูลที่ได้จากอุปกรณ์สื่อสารเคลื่อนที่
- Software ที่ใช้ตรวจพิสูจน์

ภัทรรัตน์



การเก็บวัตถุพยาน

- collect and preserve

สุราวีณี



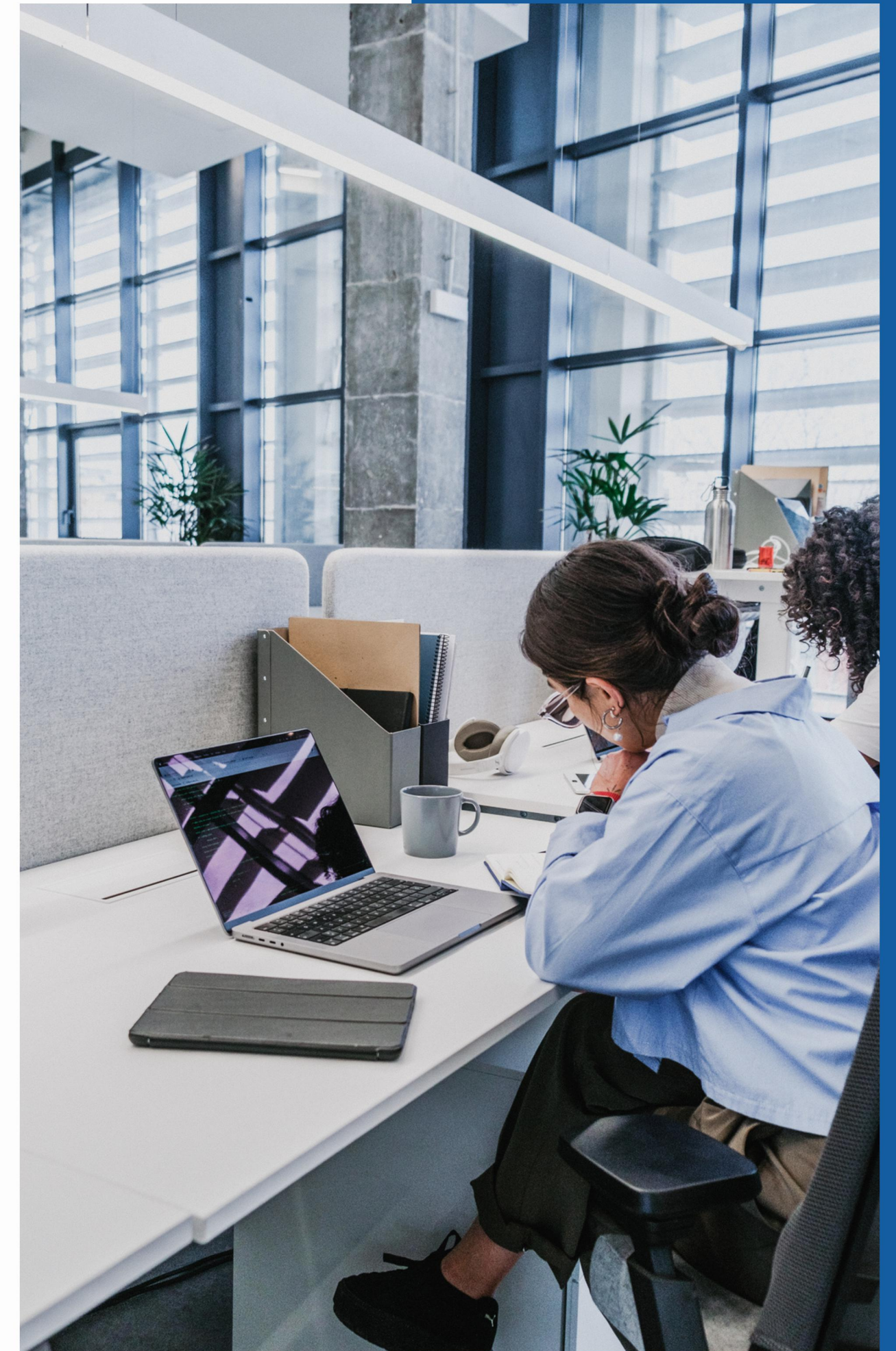
data acquisition คืออะไร
ปัญหาที่พบในปัจจุบัน
new method

ธัญญพงศ์



case study
ios
android

ธัญญพงศ์ สุราวีณี



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.

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



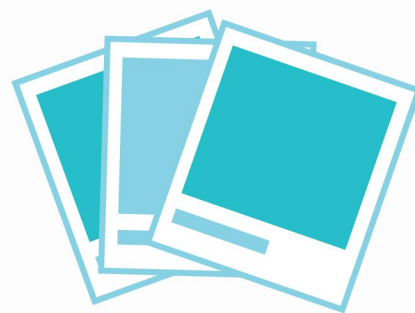
Location and
Movement Data

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



System and Device Data

Device configuration, software installations, and system events create



Media and Files

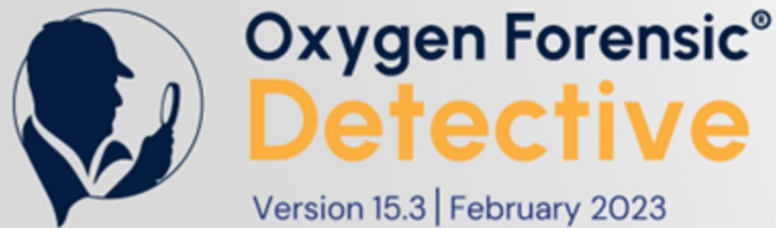
Digital Images and Videos, Audio Recording, Document and Files



Health and Lifestyle Data

health metrics, and daily routines

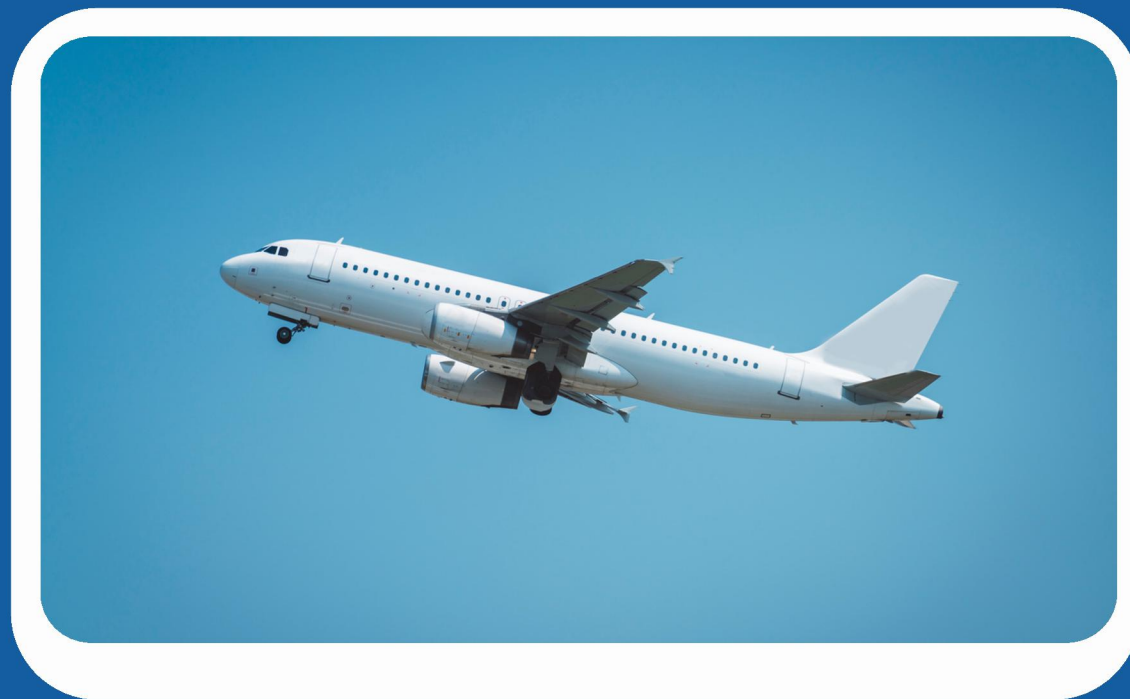
SOFTWARES



Evidence Collection and Preservation



Evidence Collection and Preservation



โหมดเครื่องบิน

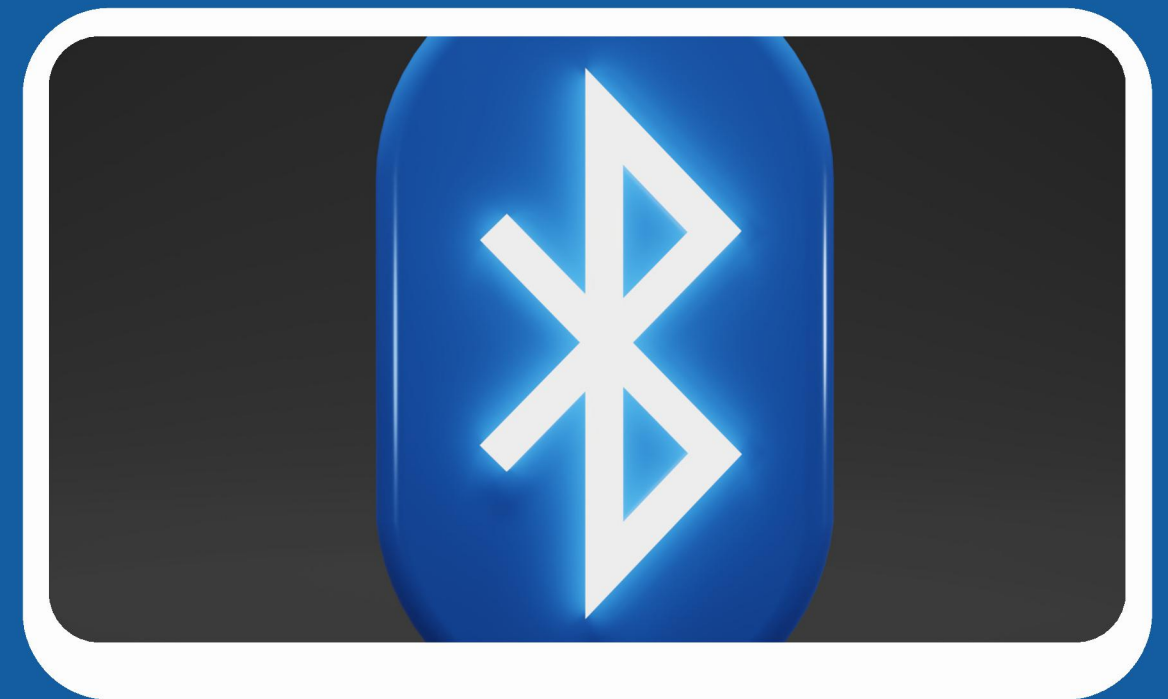
Flight mode

Airplane mode

Aeroplane mode



Wi-Fi

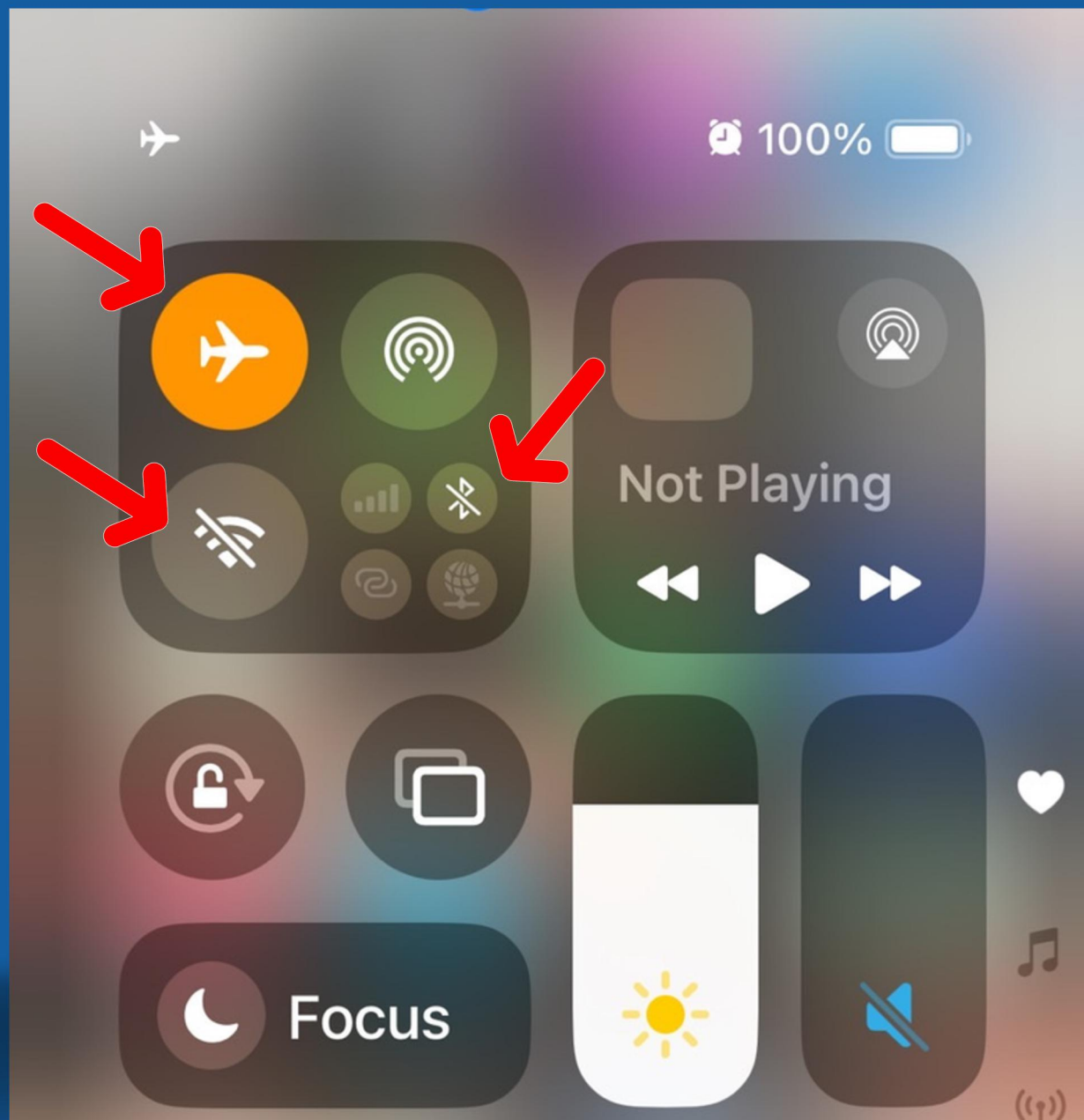


บลูทูธ

Bluetooth



Evidence Collection and Preservation



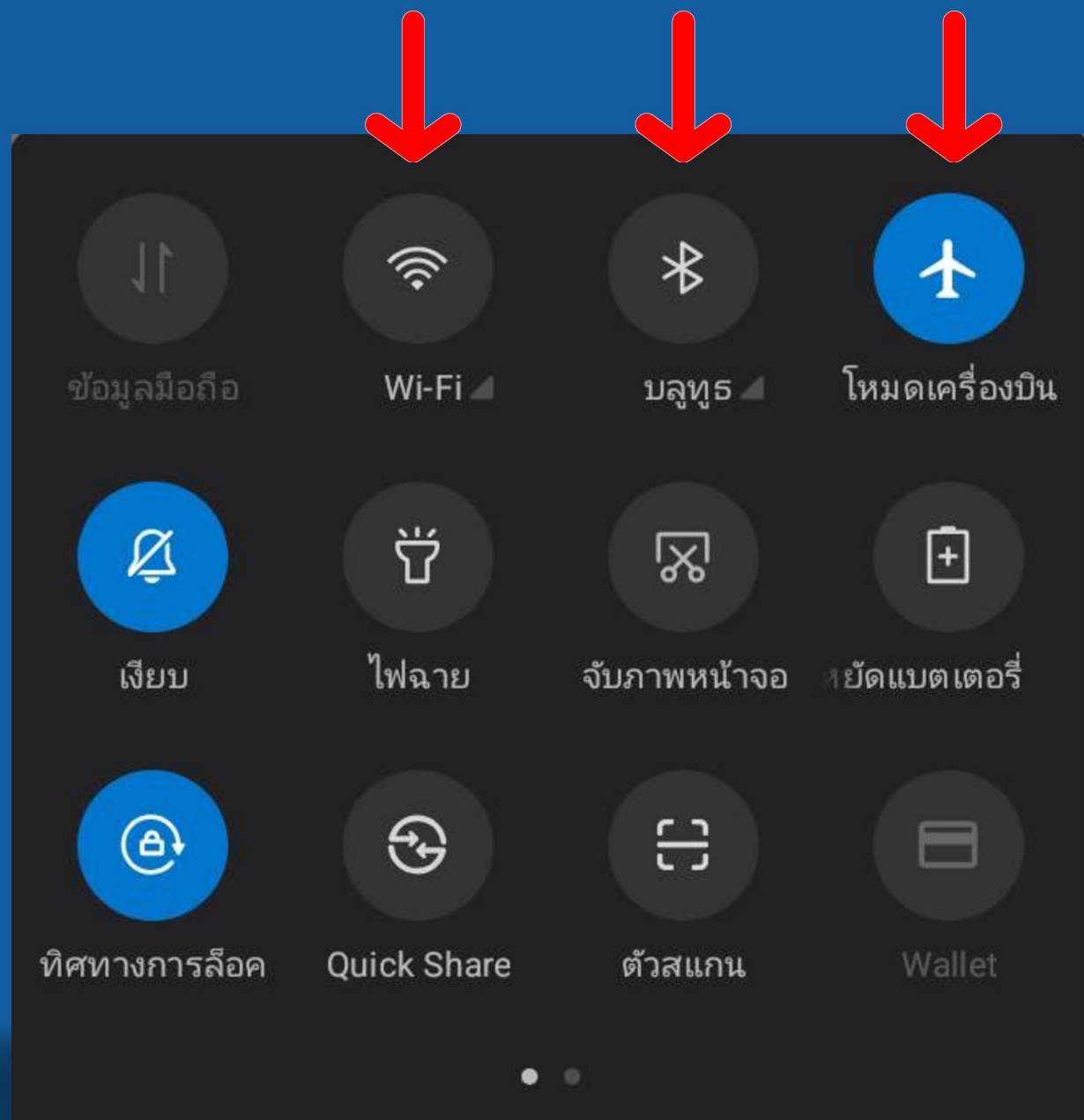
ศูนย์ควบคุม
(Control Center)



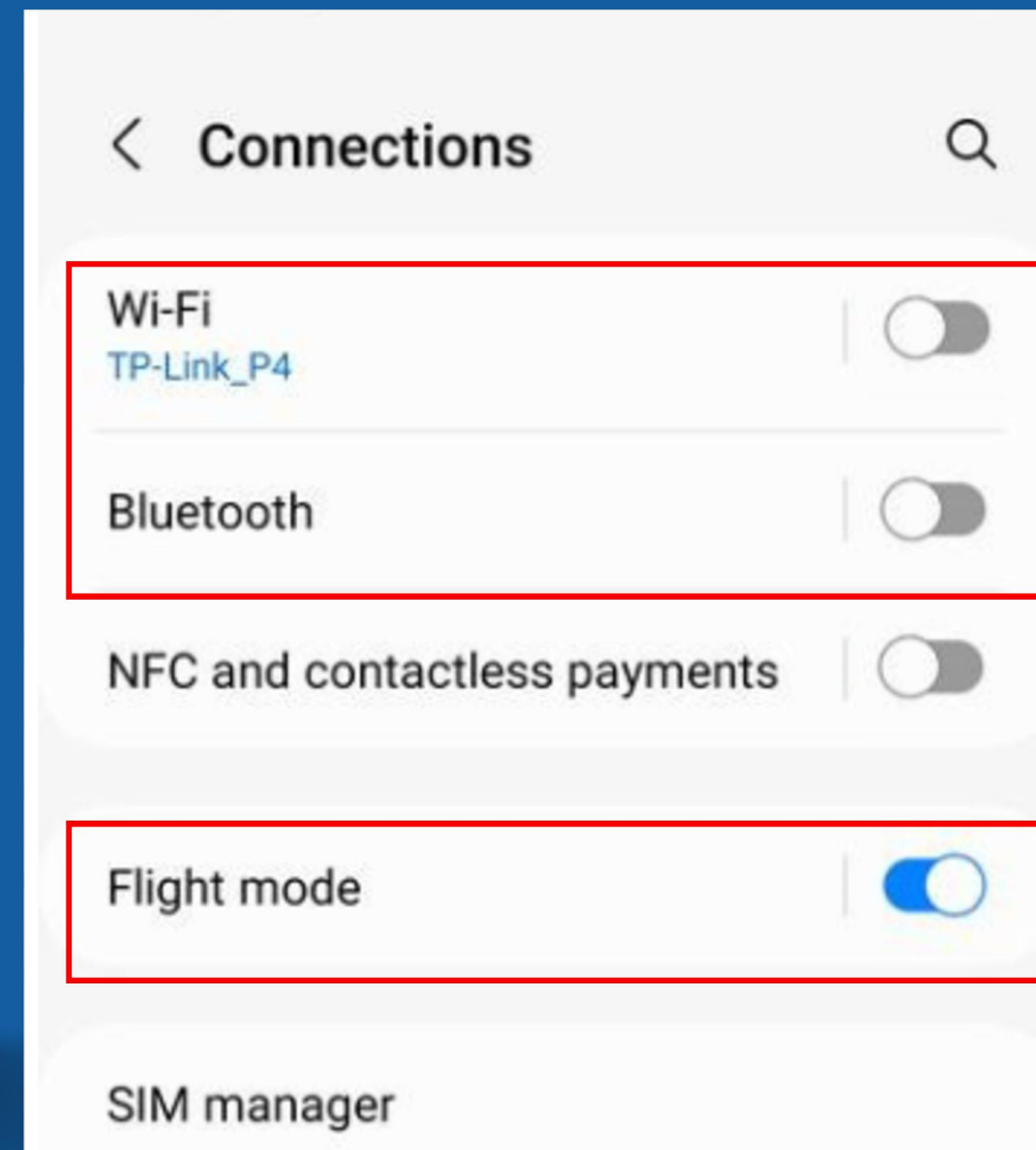
การตั้งค่า (Setting)



Evidence Collection and Preservation



แผงการตั้งค่าด่วน
(Quick Settings
panel)



การตั้งค่า (Setting)

Evidence Collection and Preservation



ชาร์จแบตเตอรี่



Evidence Collection and Preservation



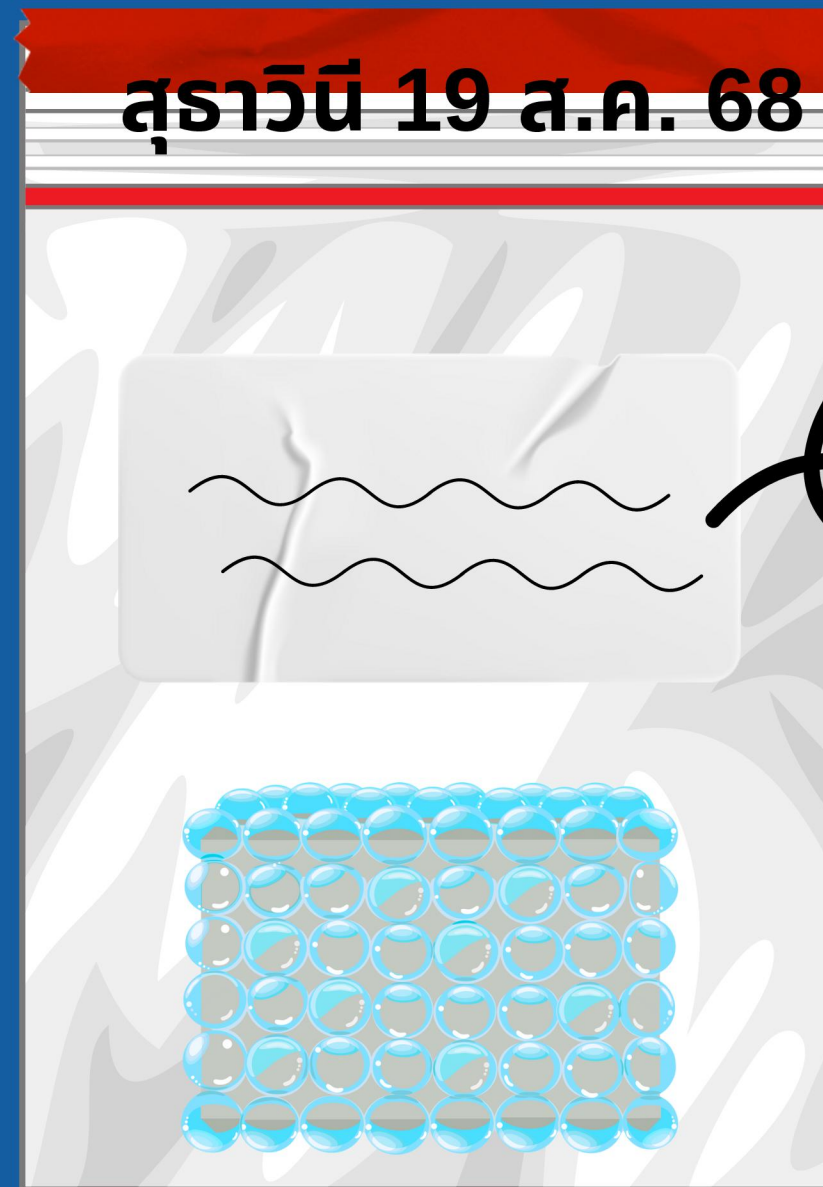
หีห่อ Faraday Bag

Evidence Collection and Preservation



หีบห่อ กรงฟาราเดย์แบบพอยล์อลูมิเนียม

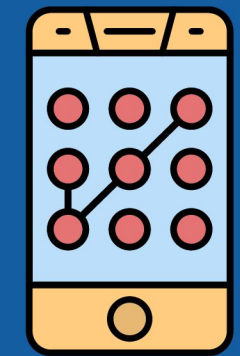
Evidence Collection and Preservation



ระบุ รายละเอียดวัตถุพยาน (สังเขป)
และรหัสการเข้าถึง



passcode



pattern

หีบห่อ



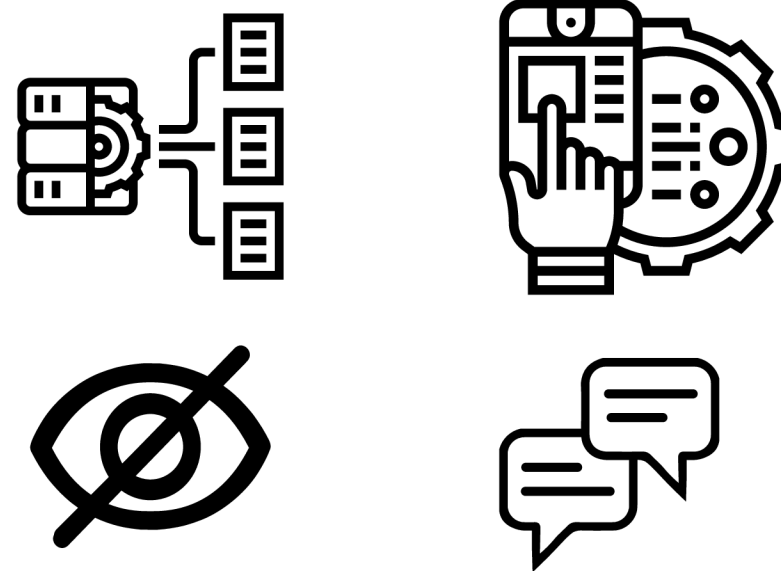
DATA ACQUISITION

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.

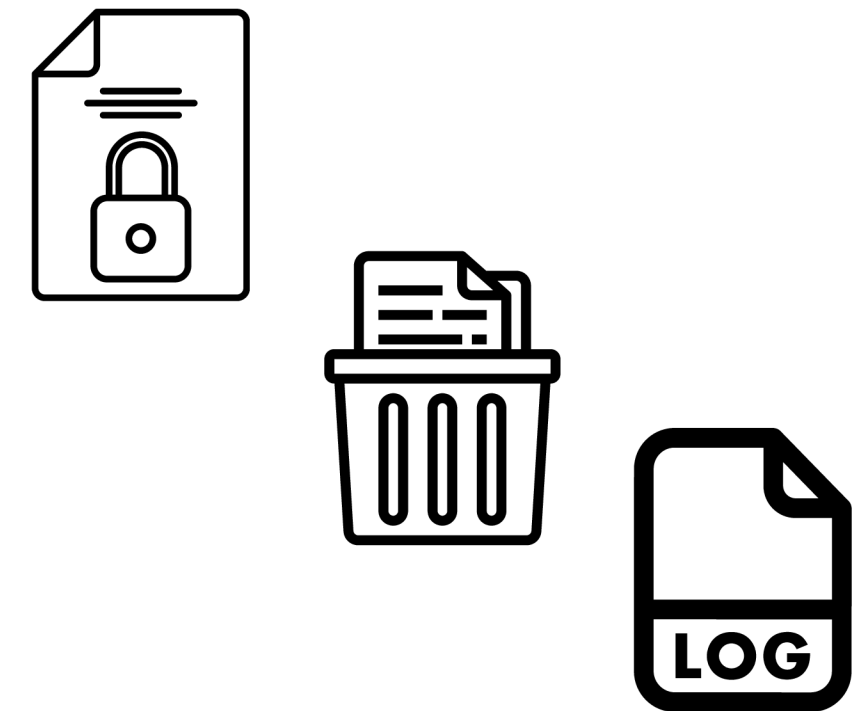
Data acquisition



**Logical
Acquisition**



**File System
Acquisition**



**Physical
Acquisition**



Data acquisition



Logical Acquisition

Logical

SMS

Contacts

Call logs

Media

App data

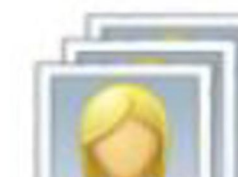


เป็นการเก็บข้อมูลที่ผู้ใช้สามารถมองเห็นได้ตามปกติ เช่น ไฟล์, โฟลเดอร์, รายชื่อติดต่อ, SMS, และข้อมูลแอปพลิเคชันบางส่วนที่อยู่ในฐานข้อมูล การทำ Logical Acquisition จะไม่เข้าถึงข้อมูลที่ถูกลบหรืออยู่ในพื้นที่ที่ระบบไม่อนุญาตให้เข้าถึงโดยตรง

Vendor API Can I have your SMS?

And your pictures as well?

Reply API



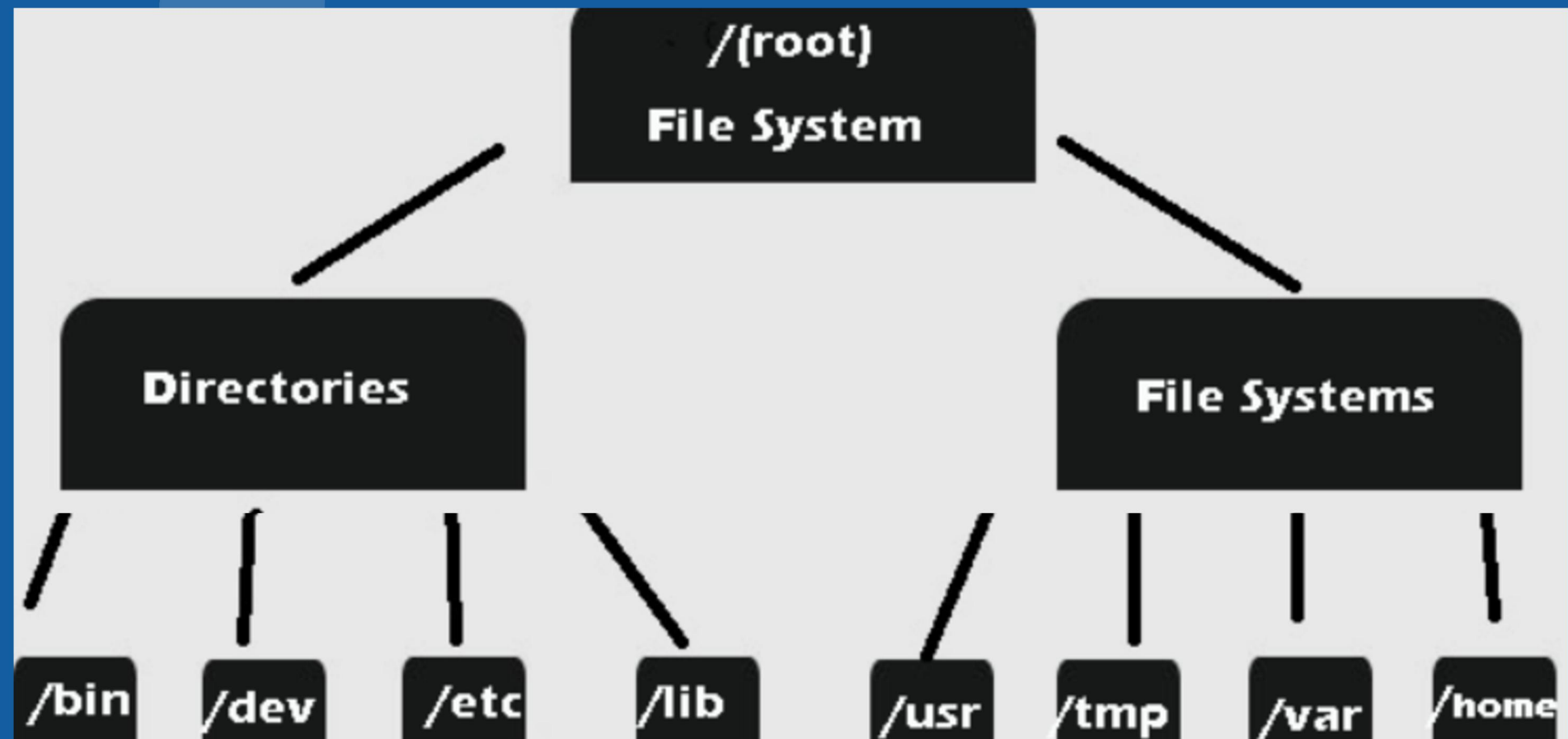
Data acquisition



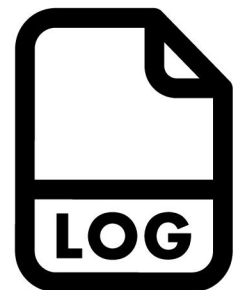
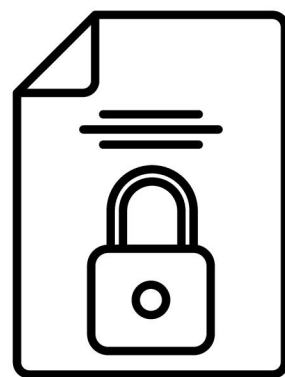
เป็นการเก็บข้อมูลที่ลึกกว่า Logical โดยจะเข้าถึงโครงสร้างระบบไฟล์ทั้งหมดของอุปกรณ์ ซึ่งรวมถึงไฟล์ของระบบและไฟล์ที่ถูกซ่อนไว้ แต่ยังไม่สามารถกู้คืนข้อมูลที่ถูกลบได้สมบูรณ์

File System Acquisition

- ### File System
- SMS
 - Contacts
 - Call logs
 - Media
 - App data
 - Files
 - Hidden Files



Data acquisition



Physical
Acquisition

Physical

SMS

Contacts

Call logs

Media

App data

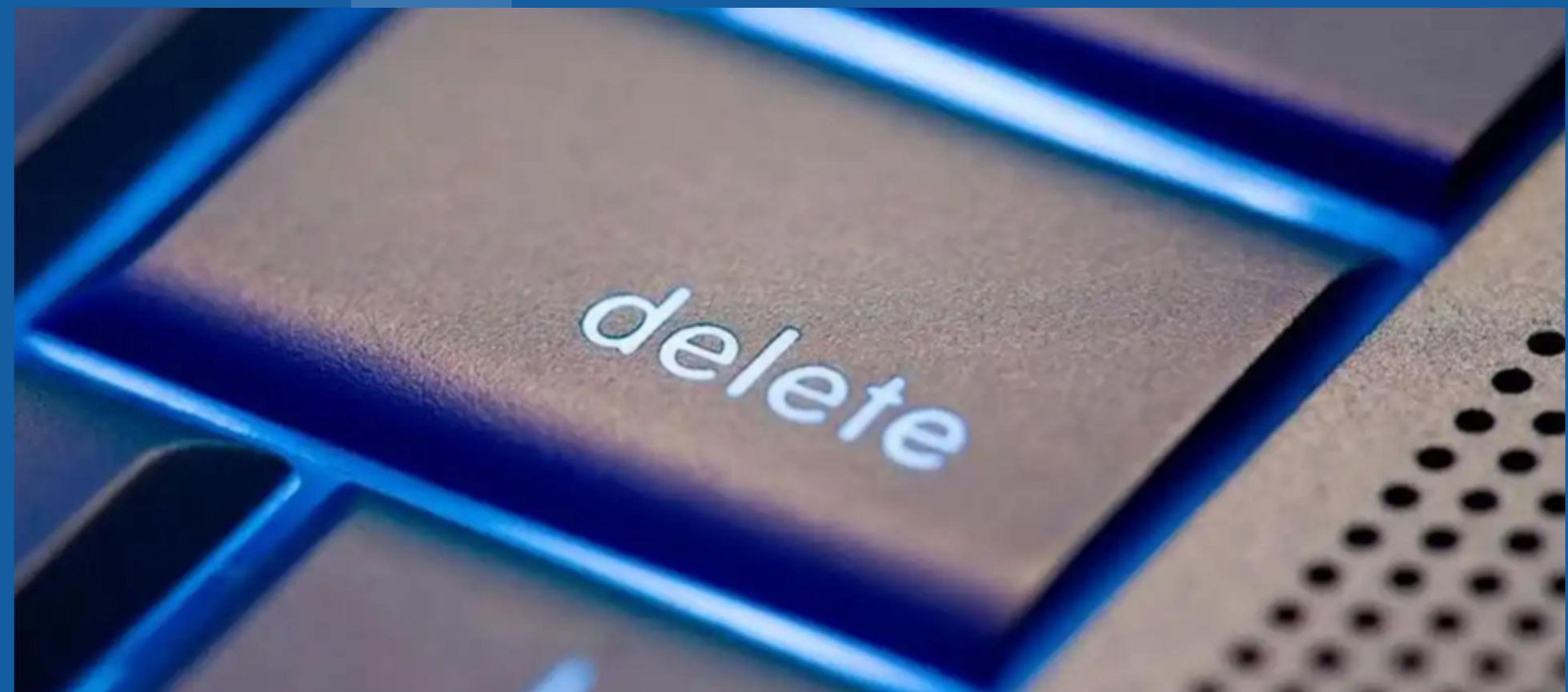
Files

Hidden Files

Deleted data



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



Data acquisition

ข้อจำกัด

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

Logical Acquisition

โดยทั่วไปไม่สามารถกู้คืนข้อมูลที่ถูกลบได้อย่างสมบูรณ์จากพื้นที่ Unallocated Space
ไม่สามารถเข้าถึงข้อมูลที่ถูกรหัสสูงสุด (เช่น Secure Enclave) ได้ทั้งหมดในอุปกรณ์รุ่นใหม่

File System Acquisition

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

Physical Acquisition



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

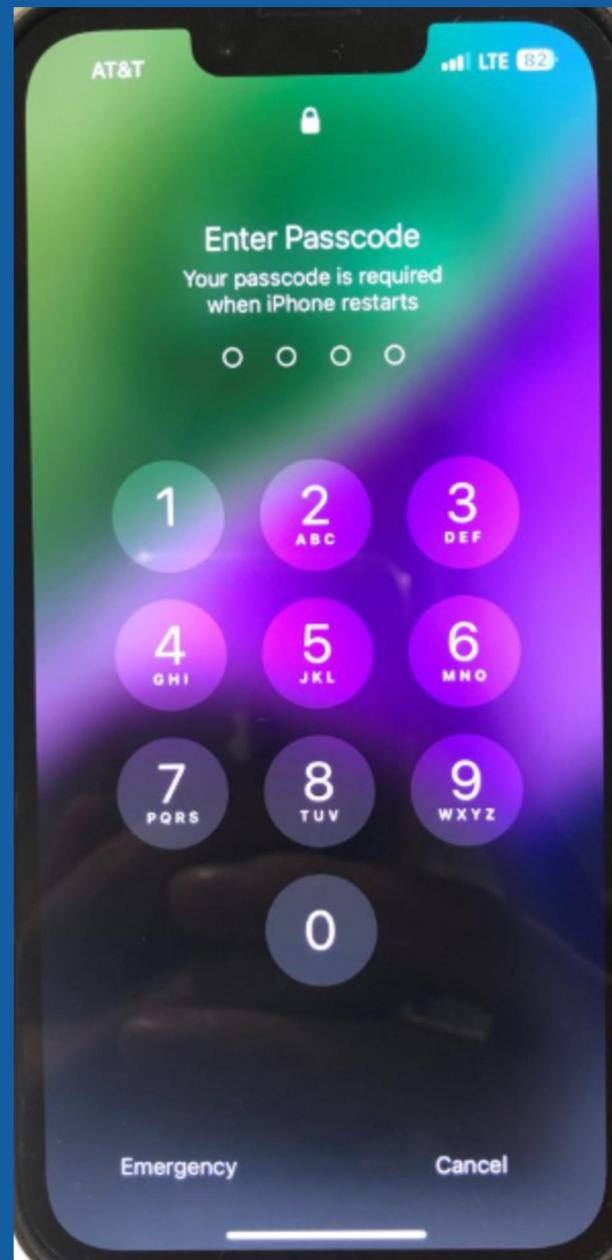
**Trusted Execution Environment
(TEE)**



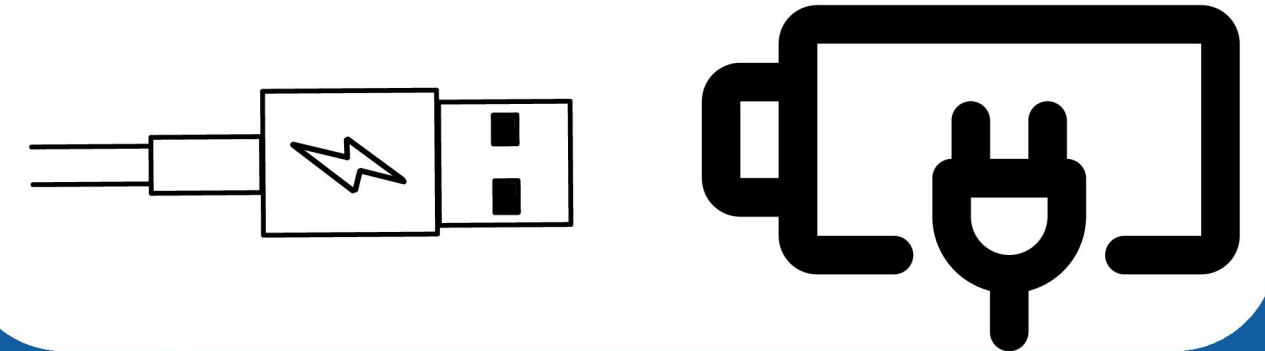
AFU & BFU

BFU (Before First Unlock)

สถานะที่มือถือถูกบูตแล้วแต่ยังไม่ป้อนรหัสผ่าน/ลายนิ้วมือหลังเปิดเครื่อง ข้อมูลส่วนใหญ่ยังถูกเข้ารหัสด้วยคีย์ระดับฮาร์ดแวร์ (Secure Enclave)



หากอุปกรณ์อยู่ในสถานะ AFU (ปลดล็อกอยู่) ควรเสียบสายชาร์จเพื่อรักษาพลังงานให้เพียงพอ ก่อนที่แบตเตอรี่จะหมดและเครื่องจะเข้าสู่สถานะ BFU



AFU (After First Unlock)

สถานะที่มือถือ ถูกปลดล็อกแล้วอย่างน้อย 1 ครั้ง ระบบปล่อยคีย์ถอดรหัสบางส่วนให้ซอฟต์แวร์ใช้งาน

Remote Wipe

Remote Wipe (การลบข้อมูลระยะไกล) คือ ฟังก์ชันที่อนุญาตให้ผู้ใช้หรือผู้ดูแลระบบลบข้อมูลทั้งหมดในอุปกรณ์แบบไร้สายผ่านเครือข่ายอินเทอร์เน็ตหรือเซลลูลาร์ มักใช้ในกรณีที่อุปกรณ์สูญหายหรือถูกขโมย เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต



Turbo Link / Cheetah

Turbo Link (ชื่อรหัสเดิม "Chetah") เป็นเทคนิคใหม่ที่พัฒนาเพื่อเร่งความเร็วการถอดรหัสข้อมูลบนอุปกรณ์มือถือ โดยเฉพาะในงาน Digital Forensics ช่วยลดเวลาการดึงข้อมูลจากวัน/ชั่วโมงเหลือเพียงนาที โดยอาศัยช่องโหว่หรือจุดอ่อนในระบบความปลอดภัยของอุปกรณ์

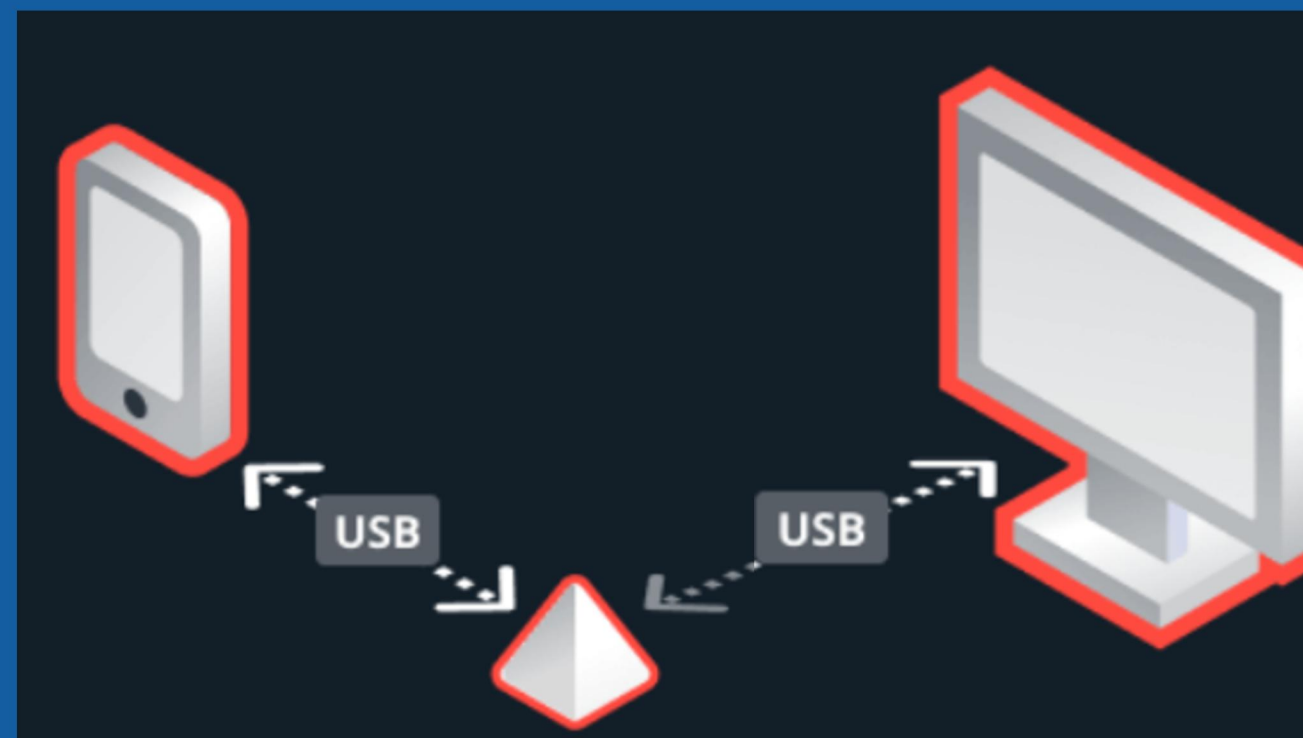


Turbo Link เป็นฮาร์ดแวร์ที่มีความสามารถในการใช้ช่องโหว่เฉพาะเพื่อเข้าถึงข้อมูลในระดับที่ลึกกว่าปกติ

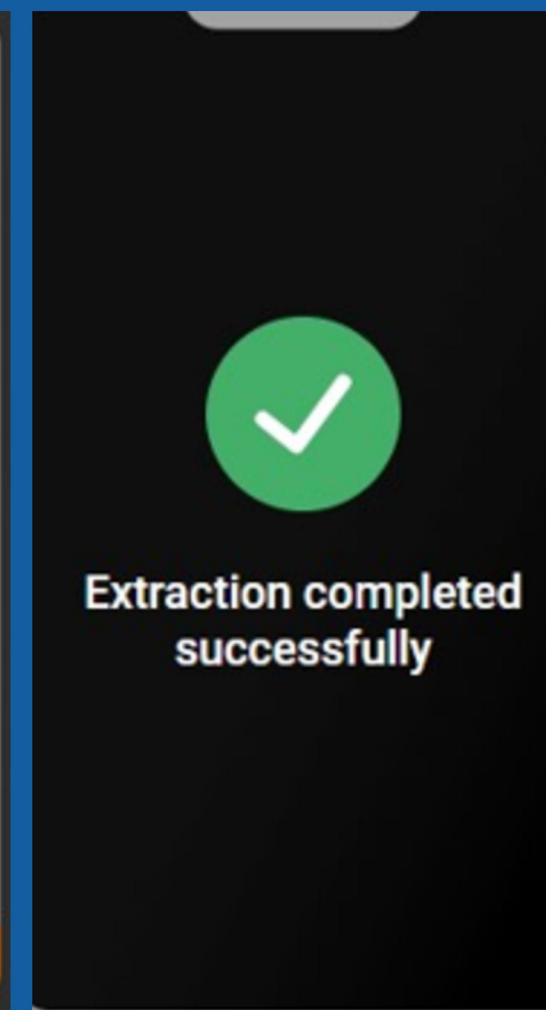
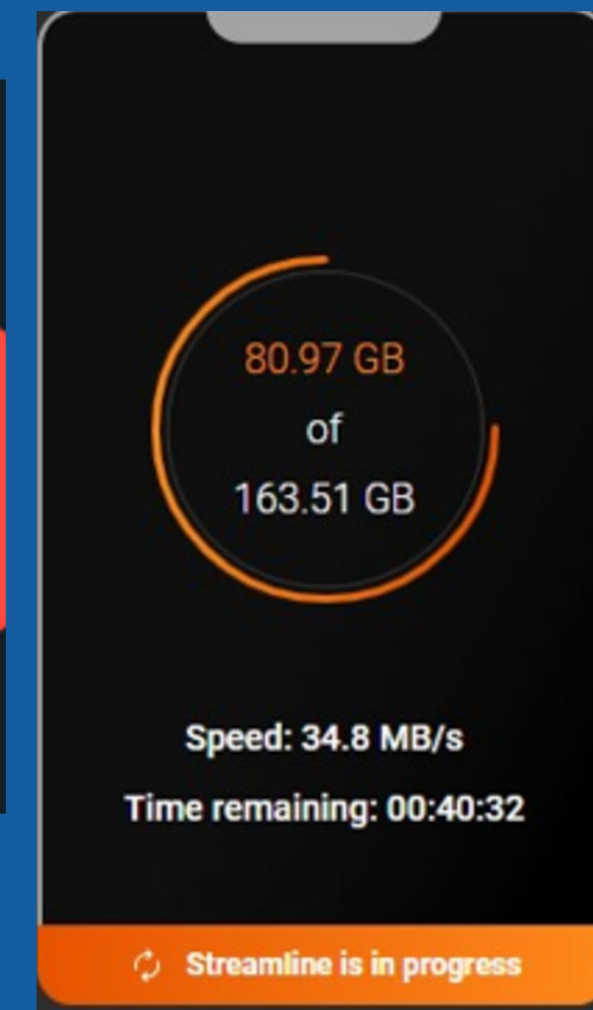
ใช้ประโยชน์จาก การเข้าถึงหน่วยความจำ (RAM) ขณะเครื่องเปิดอยู่ (AFU State) ดึง คีย์เข้ารหัสชั่วคราว ที่ระบบใช้อยู่แทน การ brute force ทั้งดิสก์

ใช้ได้เฉพาะผ่านช่องทางพิเศษ (เช่น Lightning Port ใน iPhone) เพื่อไม่ให้ระบบตรวจจับได้

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



⚠ Don't touch the device



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

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

< เกี่ยวกับโทรศัพท์

RAM
3.0GB

ROM
4.7GB (พื้นที่ที่ใช้งานได้) 16GB (พื้นที่ทั้งหมด)

หมายเลขบิวด์
F1fEX_11_160322

สถานะ

สถานะของการ์ด SIM1
หมายเลขโทรศัพท์ สัญญาณ ฯลฯ

สถานะซิม2
หมายเลขโทรศัพท์ สัญญาณ ฯลฯ

ข้อมูลทางกฎหมาย


เวอร์ชันเบสแบนด์
Q_V1_P14,Q_V1_P14


เวอร์ชันคอร์เนล
3.10.28-G201603221513


 maahalai.com
APP REVIEWER





< เพิ่มเติม


 คินการตั้งค่าจากโรงงาน


 การเข้าใช้งาน


 พิมพ์

 ตั้งเวลาเปิด/ปิดเครื่อง


 ชุดเครื่องมือซิมการ์ด

 **สำหรับนักพัฒนาซอฟต์แวร์**


 บริการหลังการขายของ OPPO


 การเชื่อมต่อ OTG




< สำหรับนักพัฒนาซอฟต์แวร์ 

รหัสผ่านการสำรองข้อมูลในเดสก์ท็อป
การสำรองข้อมูลเต็มรูปแบบในเดสก์ท็อปไม่ได้รับการป้องกันในขณะนี้


เปิดหน้าจอค้าง 
หน้าจอจะไม่เข้าสู่โหมดสลีปขณะชาร์จ

เปิดใช้บันทึก Bluetooth HCI snoop 
จับแพคเก็ต Bluetooth HCI ทั้งหมดไว้ในไฟล์เดียว

การปลดล็อก OEM 
อนุญาตการปลดล็อกคู่มือการโหลดแอป

สถิติการประมวลผล
สถิติทางเทคนิคที่เกี่ยวข้องกับกระบวนการทำงาน

การแก้ไขข้อบกพร่อง

การแก้ไขข้อบกพร่อง USB 
โหมดแก้ไขข้อบกพร่องเมื่อเชื่อมต่อ USB

ยกเลิกการให้สิทธิ์การแก้ปัญหา USB

โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

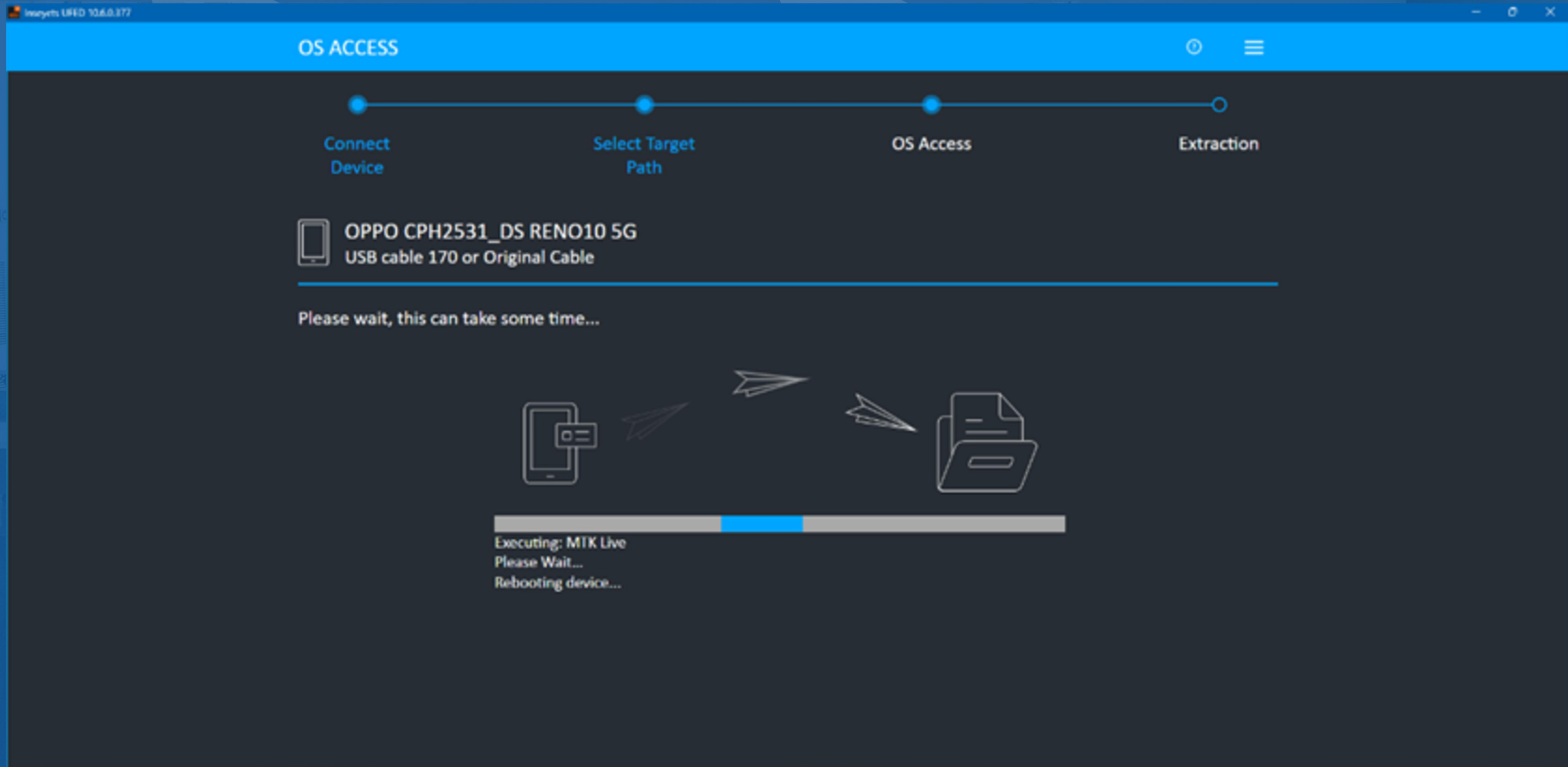
Inseyets UFED

The screenshot displays the Inseyets UFED software interface. At the top, the title bar reads "Inseyets UFED 10.6.0.377". The main interface features a blue header with the "Ins_{ts} UFED" logo and navigation icons. The central area is a dark grey grid of white tiles, each representing a different device type or tool:

- Mobile device**: A large light blue tile on the left with a smartphone icon.
- SIM card**: A white tile with a SIM card icon.
- Mass storage**: A white tile with a hard drive icon.
- UFED camera**: A white tile with a camera icon.
- Quick copy**: A white tile with an icon of two overlapping documents.
- Drone**: A white tile with a drone icon.
- Device tools**: A white tile at the bottom with a wrench and screwdriver icon.

At the bottom of the interface, there is a footer bar containing the version number "Version 10.6.0.377", a clock icon showing "8:58:58", and a calendar icon showing "21/7/2568".

โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G



Inseyets UFED 3 ครั้ง - Not Success


โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

Inseyets UFED 10.6.0.377


Ins_{ts} 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.



Android

Turbo Link

Abort



Samsung Galaxy Tab A7

Inseyets UFED 10.6.0.377

Insights UFED 9:12 21/7/2025 Resources 7,74,302

Android > Unlocked

Initializing...

Device status Quick view

Device	Model	Chipset
oppo	CPH2531	MT6877V/TTZA
OS version	Security patch level	Encryption type
15	2025-03-01	
Live encryption state		
—		

Extraction path

Available disk space: 197.96 GB free of 475.67 GB

Progress console

- 21/7/2025 9:10 - Downloading resource: And
- 21/7/2025 9:10 - Downloading resource: Mit
- 21/7/2025 9:11 - Preparing environment...
- 21/7/2025 9:11 - Connect a device to the cable now.
- 21/7/2025 9:11 - Device detected. Identifying... This could take up to 5 minutes.
- 21/7/2025 9:11 - Device detected: CPH2531
- 21/7/2025 9:11 - Attempting to connect to Cellebrite Agent. Waiting up to 4 minutes

Enter Passcode

If you know the passcode, enter it here. This will impact unlock-attempts on the device

.....

Abort No Passcode Next

Notify Me

Abort

โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

Inseyets UFED 10.6.0.377

Insights UFED 9:22 21/7/2025 Resources [7.74.302](#)

Android > **Unlocked**

Select an action

Device status Quick view

Device	Model	Chipset
oppo	CPH2531	MT6877V/TTZA
OS version	Security patch level	Encryption type
15	2025-03-01	File-based Encryption (...)
Live encryption state		
Hot (decrypted)		

Extraction path

Available disk space: 197.96 GB free of 475.67 GB

Progress console

```
21/7/2025 9:20 - Attempting to connect to Cellebrite Agent. Waiting up to 4 minutes
21/7/2025 9:20 - Cellebrite Agent initialized successfully
21/7/2025 9:21 - User 0 password change timestamp: 2024-01-26 11:55:43
21/7/2025 9:21 - User 0 password type: pin
21/7/2025 9:21 - Device bluetooth name: OPPO Reno10 5G
21/7/2025 9:21 - Found 1 IMEIs/MEIDs: 862211067244012
21/7/2025 9:21 - Users configured on the device: UID 0: Owner, Decrypted.
```

Access completed successfully

Notify Me

Finish Extraction Methods

โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

The screenshot displays the Cellebrite Ins_{ts} UFED interface. At the top, the title bar shows 'Inseyets UFED 10.6.0.377'. The main header includes the Ins_{ts} logo, the date '9:31 21/7/2025', and resource usage 'Resources 7.74.302'. The navigation path is 'Android > Unlocked'. The central section is titled 'File System Extraction' and features two tabs: 'Device status' (selected) and 'Quick view'. The 'Device status' tab contains a table with the following information:

Device	Model	Chipset
oppo	CPH2531	MT6877V/TTZA
OS version	Security patch level	Encryption type
15	2025-03-01	File-based Encryption (...)
Live encryption state		
Hot (decrypted)		

Below the table, the 'Extraction path' is shown as a redacted field. A green checkmark indicates 'Available disk space: 241.33 GB free of 475.67 GB'. The 'Progress console' shows a log of events:

- 21/7/2025 9:21 - Device bluetooth name: OPPO Reno10 5G
- 21/7/2025 9:21 - Found 1 IMEIs/MEIDs: 862211067244012
- 21/7/2025 9:21 - Users configured on the device: UID 0: Owner, Decrypted.
- 21/7/2568 9:27 - Extraction 1/1 - Full file system - Started
- 21/7/2025 9:27 - Performing File System Extraction
- 21/7/2025 9:27 - Connecting
- 21/7/2025 9:28 - Performing Full file system**

On the right side, a progress indicator shows '1.8 GB of 125.47 GB' extracted. Below this, it displays 'Speed: 21.6 MB/s' and 'Time remaining: 01:37:32'. A red button indicates 'Streamline is in progress' and a 'Notify Me' button is present. At the bottom right, there is a red 'Stop' button.

โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

InseYets UFED 10.6.0.377

15:25 21/7/2025 Resources 7.74.302

Android > Unlocked

File System Extraction

Device status Quick view

Device	Model	Chipset
oppo	CPH2531	MT6877V/TTZA
OS version	Security patch level	Encryption type
15	2025-03-01	
Live encryption state		
Hot (decrypted)		

Extraction path

Available disk space: 248.97 GB free of 475.67 GB

Progress console

- 21/7/2025 15:37 - On the use USB to pop-up the pop-up does not display "MTP"
- 21/7/2025 14:50 - Trying to get keys from user 0, package com.shopee.th
- 21/7/2025 15:18 - Key extraction completed successfully.
- 21/7/2025 15:18 - Extraction completed successfully
- 21/7/2025 15:25 - Please don't disconnect device from target side
- 21/7/2025 15:25 - Attempting to connect to Cellebrite Agent. Waiting up to 4 minutes

✓ **Streamline Status**

Extraction completed successfully and sent to InseYets Physical Analyzer.
Please check the case status in InseYets Physical Analyzer.

ok

✓

Extraction completed successfully

Notify Me


โทรศัพท์มือถือ ยี่ห้อ OPPO รุ่น Reno10 5G

ขนาดความจุ 125 GB



Extraction

- Inseeyets UFED >>> Not Success
- Inseeyets 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 Inseets Physical Analyzer | Version 10.5.0.1027

ins^ots_{PA} File View Tools Cloud Plug-ins Report Help

Search... Advanced Learning Hub

Extraction Summary (1) x

Dashboard View Data Details View Date Range Preliminary Device Report Generate Report

Extraction Name	Model name and specific...	Extraction Type	Extraction Start and End ...	Path	Image Hash
File System	OPPO OPPO Reno10 ...	FileSystem	21/7/2568 4:38:36(UT...		Hash data not available

Extraction Info

Extraction Name:	File System
Device Type:	Google Android Generic
Method Type:	FileSystem
Extraction start date/time:	21/7/2568 4:38:36(UTC+0)
Extraction ID:	e1cae3c7-361b-4edb-9d50-0a4...
Extraction decoding version:	15.0.0.2527
Extraction end date/time:	21/7/2568 8:25:14(UTC+0)
Extraction (UFD) file data integr...	Intact
Selected manufacturer:	OPPO
Preserved Extraction:	False
Machine name:	CIFS
Internal version:	10.6.0.377
Connection type:	Cable No. Original cable
Selected device name:	OPPO Reno10 5G
Unit identifier:	1640881852
Decoding start date/time:	21/7/2568 15:43:19
Extraction type:	File System [Android ADB]
UFED version:	10.6.0.377

Analyzed Data

- Application (58925)
- Calendar (1738) (1)
- Calls (369) (9)
- Contacts (6149)
- Finance & Purchase (2)
- Media (324719)
- Networks & Connections (170164) (26238)
- Search & Web (9495) (51)
- Social Media (181)
- Storage & Vaults (472)
- System & Logs (14419)
- User Accounts & Details (2459)

Data files

- All Files (10253)
- Applications (4)
- Archives (6)
- Configurations (6)
- Documents (654)
- Text (453)
- Uncategorized (9130)

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: j [REDACTED]

Locale Language: en_TH

Vendor: Apple

Chipset: A17

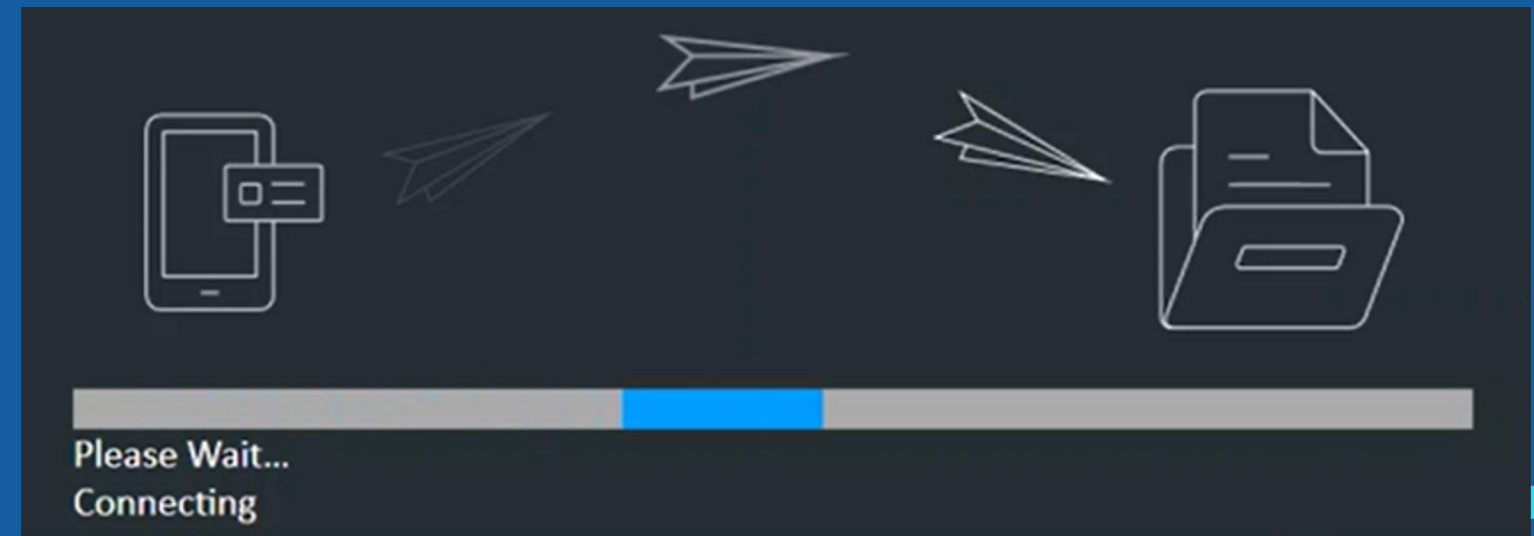
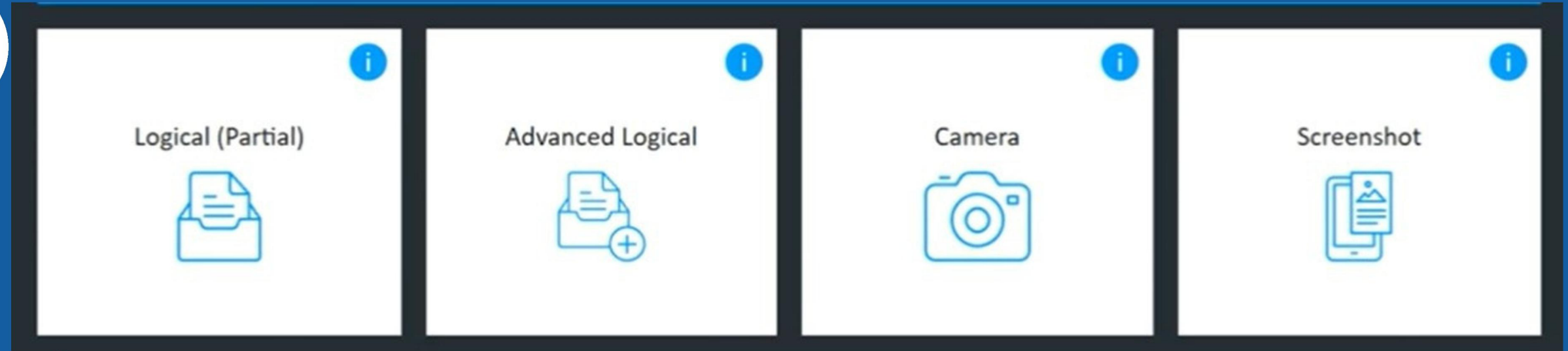
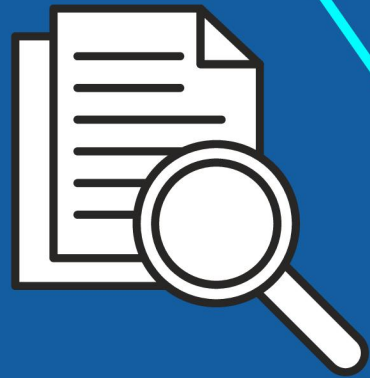
Encryption Type: FBE

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

IOS > **Locked**

iOS AFU Access method 4

Device status | Quick view


Device	Model	Chipset
Apple	iPhone 15 Pro	A17
OS version	Security patch level	Encryption type
18.4.1	—	FBE
Live encryption state		
—		

Extraction path

Available disk space: 224.83 GB free of 475.67 GB

Progress console

```
29/7/2025 12:18 - Stage 1: Preparing
29/7/2025 12:18 - Stage 2: Starting access
29/7/2025 12:32 - Stage 3: Initial access. This usually takes around 15 to 30 minutes.
29/7/2025 12:58 - Stage 4: Executing method. This usually takes around 30 to 60 minutes
29/7/2025 13:22 - Stage 5: Performing post execution actions
29/7/2025 13:26 - Stage 6: Deploying agent
29/7/2025 13:26 - Stage 7: Finished
```



Notify Me

Apple iPhone 15 Pro

iOS > Locked ?

iOS CLB mode

Device status Quick view

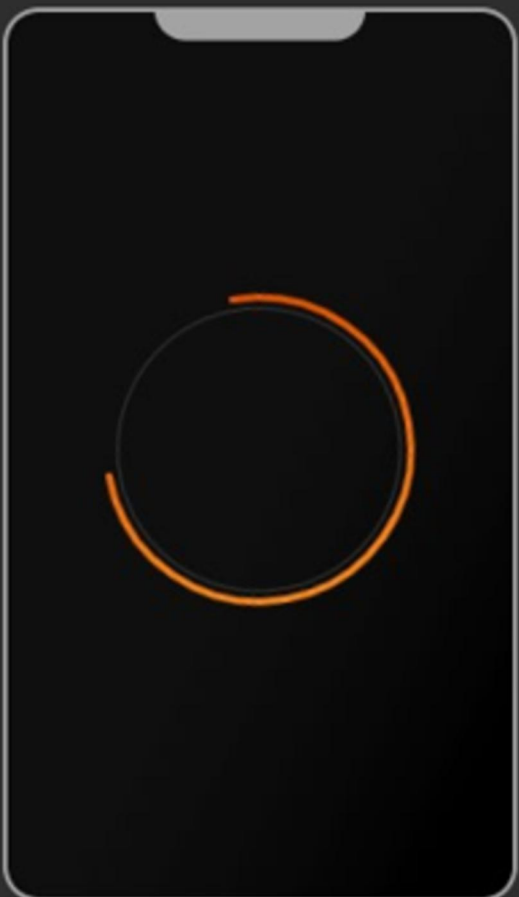
Device	Model	Chipset
Apple	iPhone 15 Pro	A17
OS version	Security patch level	Encryption type
18.4.1	—	FBE
Live encryption state		
—		

Extraction path

Available disk space: 224.83 GB free of 475.67 GB

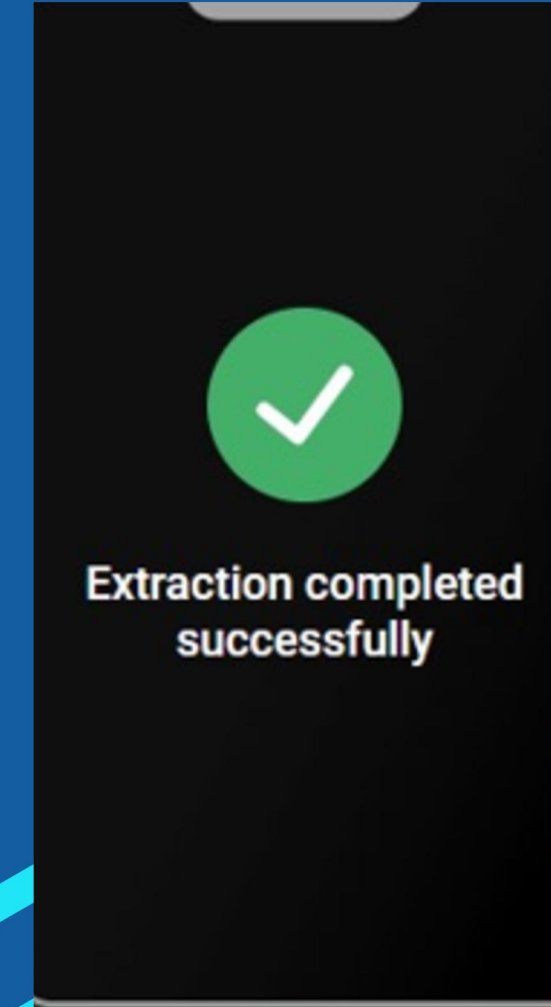
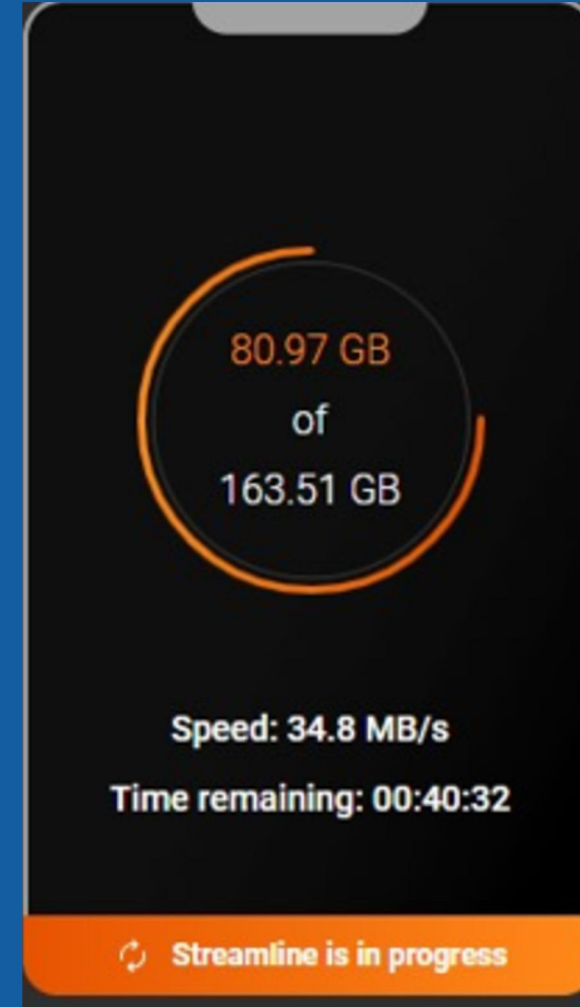
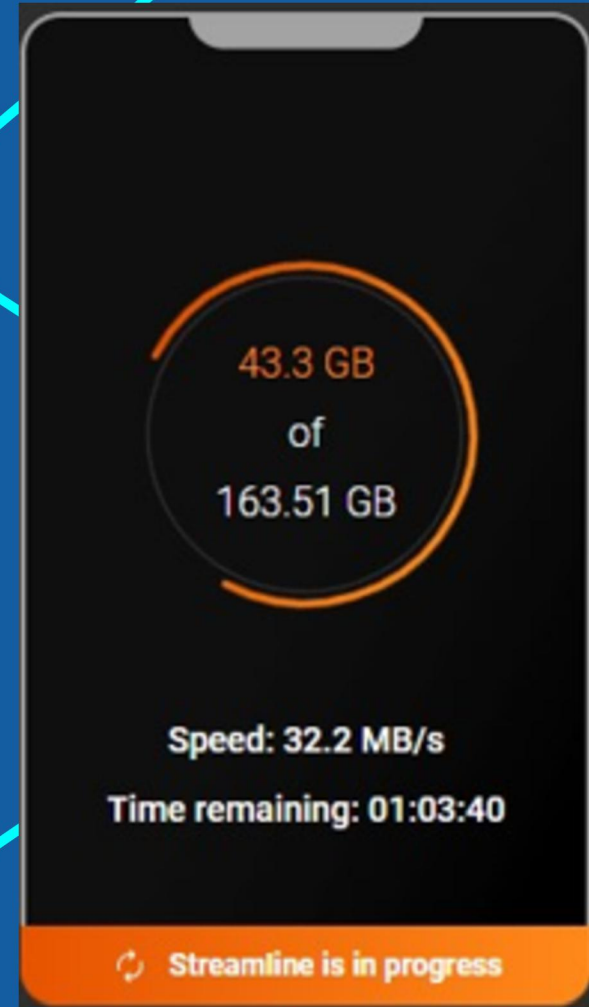
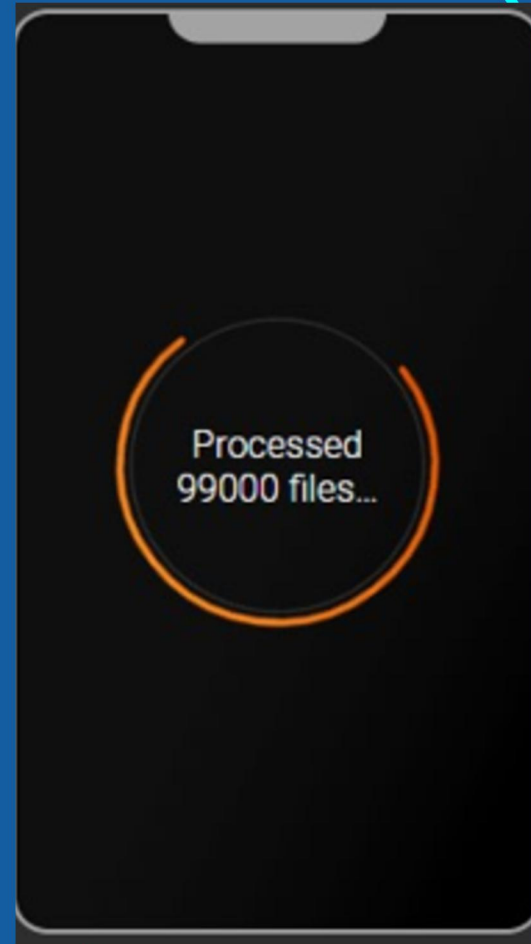
Progress console

```
29/7/2025 13:26 - Stage 6: Deploying agent
29/7/2025 13:26 - Stage 7: Finished
29/7/2025 13:27 - Time remaining until inactivity reboot: 71 hours and 59 minutes
29/7/2568 13:27 - Updating quick view data
29/7/2025 13:27 - Connecting
29/7/2025 13:27 - Connecting client
29/7/2025 13:27 - Reading Phone Info
```

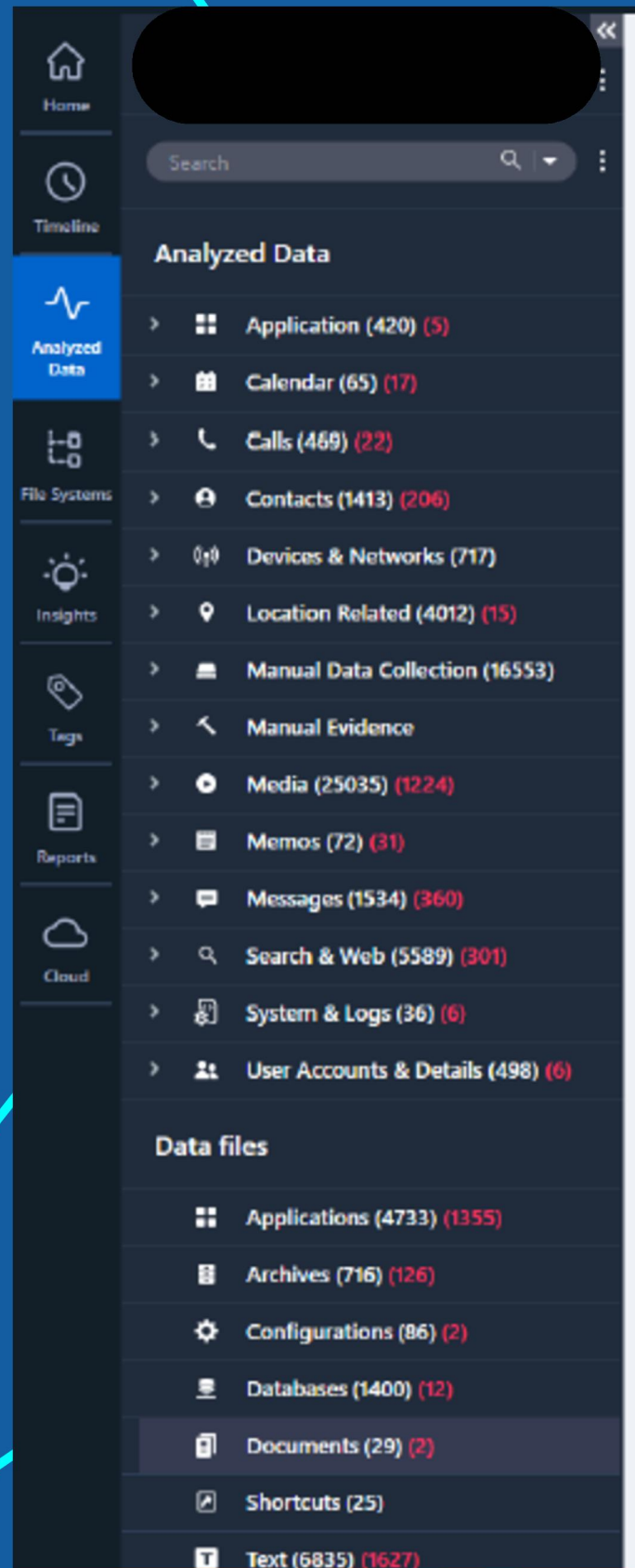


Notify Me

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 Number: [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



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

Thank you

