SUNG KYUN KWAN UNIVERSITY

A Study on the Recovery of Damaged iPhone Hardware Exhibiting Panic Full Phenomena

Sunbum Song, Hongseok Yang, Eunji Lee, Sangeun Lee, Gibum Kim
Sungkyunkwan Univ.

Presenter : Eunji Lee

2025APAC
DFRWS

SUNG KYUN KWAN UNIVERSITY

CONTENTS

DFRWS

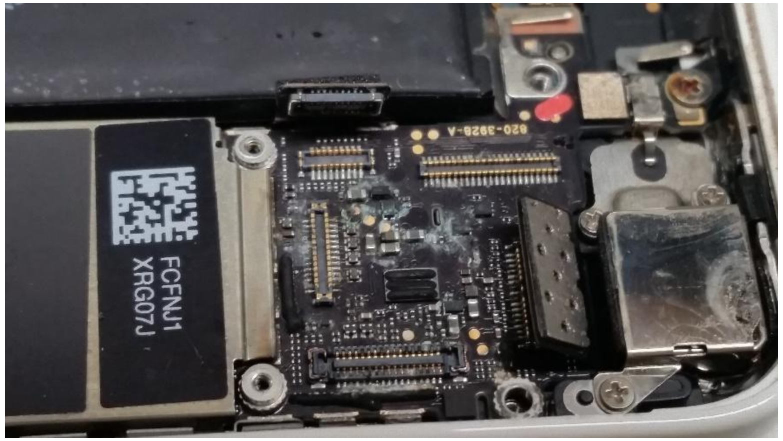
01

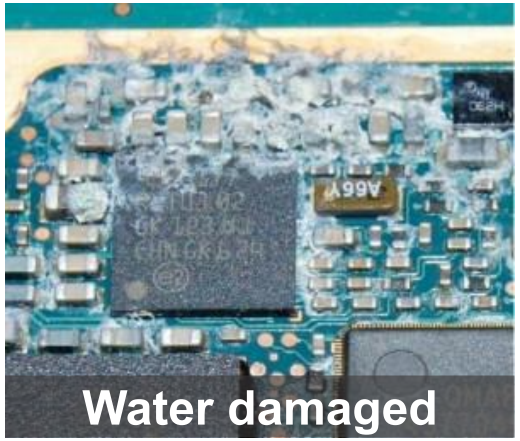
Introduction

SUNG KYUN KWAN UNIVERSITY

01 Research Background and Motivation

- **Challenges in Data Acquisition from Damaged iPhones**
  - Damaged devices frequently appear in forensic labs (water, impact, fire).
  - Traditional recovery:
    Chip-off → Remove flash memory and read data directly.
  - Modern smartphones use hardware-based encryption → chip-off is no longer sufficient.
  - Chip-transplantation = possible but high risk → High temperature exposure
    → Miniaturized APs → difficult and costly
  - Therefore, analysts increasingly focus on hardware repair and diagnostics to enable data recovery.

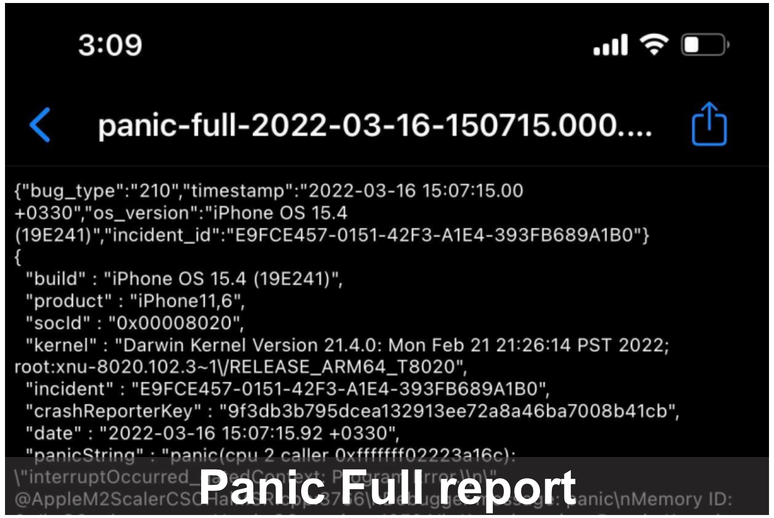




Water damaged

SUNG KYUN KWAN UNIVERSITY

- **Panic-Full Phenomenon in iPhones**
  - iPhones may enter a **continuous reboot loop, “panic-full”** when essential hardware modules are damaged.
  - Panic-full occurs even if AP and flash memory are intact.
  - Device logs contain “Panic Full” reports used for diagnosis and repair.
  - Public tools exist, but not from a forensic perspective.
  - Panic-full prevents forensic data acquisition → major obstacle.



Panic Full report

02 Research Motivation and Objectives

- **Research Gap** : Panic-full issues have not been addressed academically
- **Objective** : Develop a diagnostic and recovery methodology for iPhones in panic-full state.
- **Research Questions:**

  ✓ **RQ1: What modules are essential for normal data acquisition?**

  ✓ **RQ2: How can damaged modules be diagnosed?**

  ✓ **RQ3: Can module replacement resolve panic-full?**

  ✓ **RQ4: What methods can resolve unrecoverable panic-full cases?**

03 Contribution

- **Defines the minimum hardware combination required for data acquisition.**
- **Improves diagnostic reliability by validating public panic-full data.**
- **Proposes logic-board–level repair methods**
  (e.g., jumper connections, component replacement).
- **Suggests an improved recovery process before high-risk chip-transplantation.**
- **Scope: iPhones that can boot into panic-full** (not total board failure).

02

Background

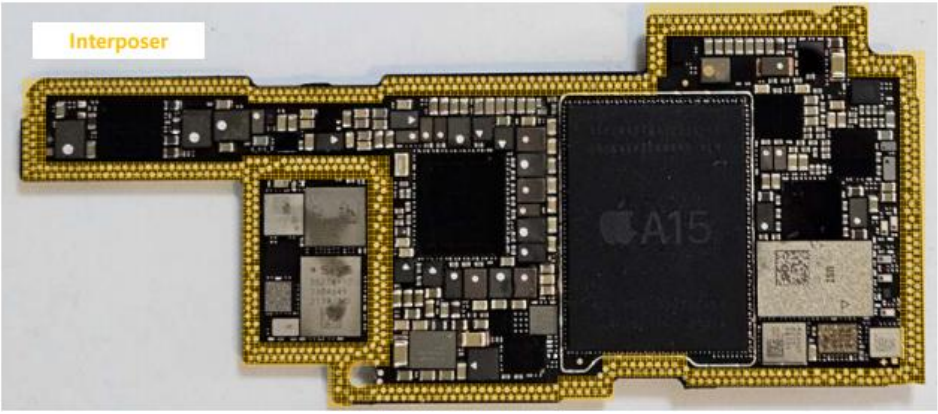
01 Structure of iPhone Logic Board

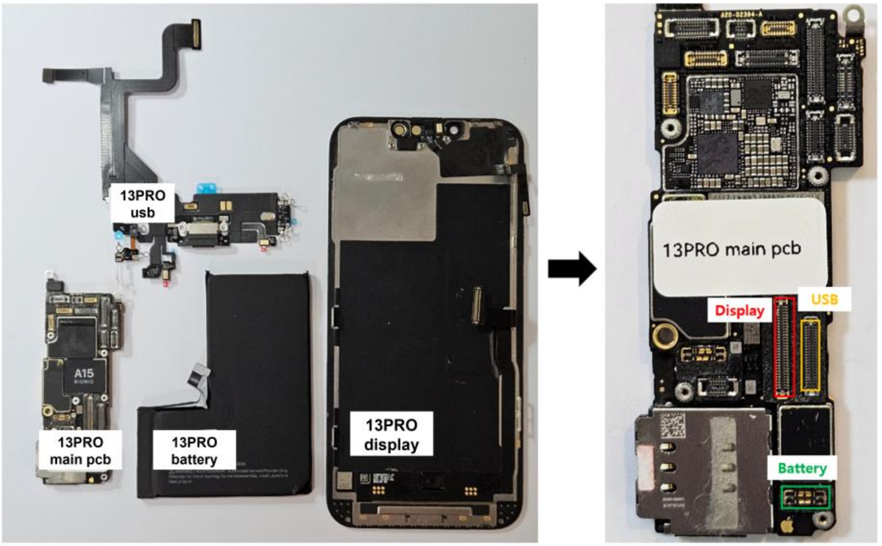
02 Diagnosis of Damaged Hardware

03 Hardware Recovery

01 Structure of iPhone Logic Board

- **Key Features**
  - Since iPhone X (2017), adopted stacked logic board design
    → Saved space and enabled integration of more components.
  - Logic board composed of two layers (upper & lower PCBs) → Connected through an interposer.
  - Microscopic edge contacts provide electrical connection between layers.
  - Connected modules use FPCB (Flexible Printed Circuit Board)
    → Thin, bendable, essential for compact internal structures.





02 Diagnosis of Damaged Hardware

- **Forensic analysts use various diagnostic techniques:**
  - Microscope inspections (Fukami & Nishimura, 2019)
  - Electrical tests (Kumar et al., 2021)
  - Infrared and X-ray analyses (Thomas-Brans et al., 2022)

  Among these, electrical testing using a multimeter is the most common.

- **Diode Mode**
  - ✓ Applies a small current and measures voltage drop.
  - ✓ Normal diode → Voltage drop one way, “OL” (Open Loop) the other.
  - ✓ Damaged diode → “OL” both ways (no current flow).
- **Continuity Mode**
  - ✓ Beep sound = circuit connected.
  - ✓ “OL” = broken circuit. (References: FLUKE, 2024; Geier, 2011)

03 Hardware Recovery

- **Two primary hardware recovery methods are used in digital forensics:**
  - Chip-off technique (Breeuwsma et al., 2007):
    - Physically removes the flash memory from a damaged device.
    - Reads data using a memory reader.
  - JTAG method (Blackman, 2015):
    - Extracts data via debugging ports even from **burned or shot** devices.
    - Proven effective across devices — e.g., Amazon Echo (Lorenz et al., 2023).

- **Modern devices employ hardware-level encryption for secure data protection:**
  - Bitlocker / Veracrypt / Apple’s Secure Enclave

- **Limitation : This make chip-off alone insufficient for data acquisition**

“Forensic focus has shifted to preventing further damage and repairing hardware”

03

Experiment

Insert Logo Here

SUNG KYUN KWAN UNIVERSITY

DFRWS

SUNGKYUNKWAN UNIVERSITY

- **Experimental Setup and Device Selection**
  - The experiments were conducted using **iPhone 11, 13 Pro, 14 Plus, 14 Pro, and 15 Pro** running various iOS versions.
  - **Supporting equipment**
    - **Board heater** – for separating stacked logic boards.
    - **Hot air gun** – for removing IC components.
    - **Soldering iron** – for jumper-wire connections and rework.

No	Device type	Manufacturer	Model	OS version	Misc.
1	Smartphone	Apple	iPhone 11	15	Stacked logic board
2	Smartphone	Apple	iPhone 13 Pro	16.4.1	Same as above
3	Smartphone	Apple	iPhone 14 Plus	17.4.1	Same as above
4	Smartphone	Apple	iPhone 14 Pro	18.3.2	Same as above
5	Smartphone	Apple	iPhone 15 Pro	17.2.1	Same as above
6	Board heater	AiXun	iHeater Pro	-	For board separation
7	Hot air gun	HAKO	FR-810B	-	For chip-off
8	Soldering iron	METCAL	MFR-1160	-	For jump re-soldering

01 Experimental Design

SUNG KYUN KWAN UNIVERSITY

● Experimental Scenarios

No	Scenario objectives	Summary of tests
1	Identify essential hardware module	Disconnected modules from the logic board and observe for panic-full be havior
2	Identify diagnostic information	For panic-full logs collected in Scenario 1, analyze and compare the log t o existing diagnostic methods
3	Resolve panic-full issue with replaceme nt of essential modules	Replace essential H/W modules with functioning modules from an identic al model and observe for panic-full behavior
4	Resolve panic-full issue with circuit-lev el repairs of logic board	Assume damage to the logic board module connectors, diagnose damag e using a multimeter, and identify circuit bypass routes
5	Determine necessity for logic board rea ssembly	Identify possibilities for not reassembling logic board after connecting es sential modules, and observe for panic-full behavior in due process

- **Scenario 1. Identify essential hardware module →** Module Disconnection Test
  - **Purpose** : To determine which modules trigger panic-full behavior when disconnected.
  - **Method**
    - Disassemble test devices.
    - Sequentially disconnect modules (USB, proximity sensor, etc.).
    - Observe system response (normal boot vs. panic-full).
  - **Observation**: Checked whether the device booted normally or entered panic-full mode.

device disassembly

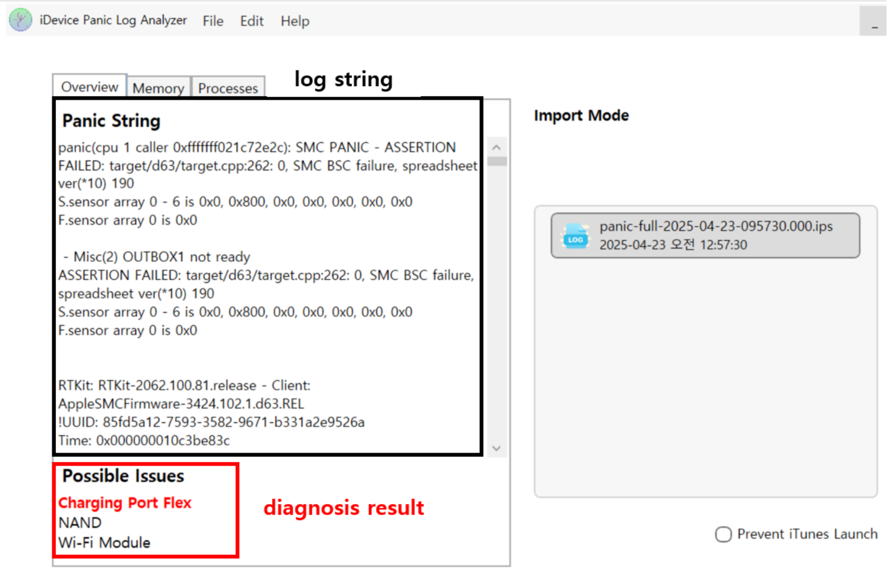
logic board connection

behavior observation

- **Scenario 1. Identify essential hardware module**
  - **Result**
    - Modules linked to panic-full events:
      - ✓ USB (Lightning)
      - ✓ Proximity sensor
      - ✓ Wireless charging
      - ✓ Power module
    - Required module combinations vary by iPhone model.

Model	USB module (Lightning or USB-C)	Proximity sensor	Wireless charging module	Power module
iPhone 11	Essential	Not essential	Not essential	Essential
iPhone 13 Pro	Essential	Not essential	Not essential	Not essential
iPhone 14 Plus	Essential	Essential	Essential	Not essential
iPhone 14 Pro	Essential	Essential	Not essential	Not essential
iPhone 15 Pro	Essential	Essential	Essential	Not essential

- **Scenario 2. Log and Error Correlation**
  - **Purpose** : Correlate panic-full logs and error codes with simulated damaged modules.
  - **Method** :
    Analyze logs collected in Scenario 1.
    Match error codes to specific module failures.
    Compare with public diagnostic data.

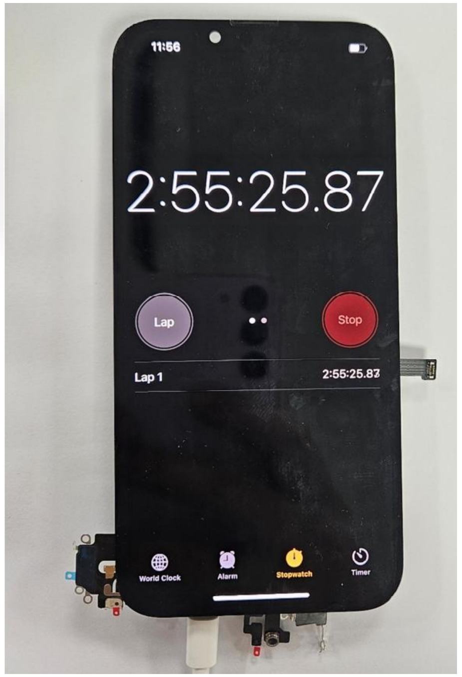


Result

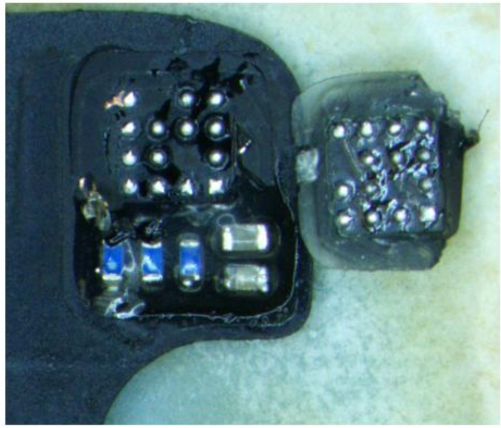
Model	Damaged module	Detection keyword (Test)	Tool results (Possible Issues)	Log keyword (repair.wiki)
11	USB	Prs0	Charging Port Flex Power Button Flex	Prs0 or Mic1
	Power button	mic2	Charging Port Flex Power Button Flex	Mic2
	USB+Power button	mic2, Prs0	Charging Port Flex Power Button Flex	-
13 Pro	USB	0x800	NAND Wi-Fi Module Crystal Interposer	0x800
14 Plus	USB	0x100000	NAND Crystal Interposer	0x100000
	proximity sensor	0x200000	NAND Crystal Interposer	0x200000
	USB + proximity sensor	0x300000	NAND Crystal Interposer	-
	wireless charging module	0x400000	NAND Crystal Interposer	0x400000
	USB + wireless charging module	0x500000	NAND Crystal Interposer	-
	wireless charging module + proximity sensor	0x600000	NAND Crystal Interposer	0x600000
	USB + wireless charging module + proximity sensor	0x700000	NAND Crystal Interposer	-
14 Pro	proximity sensor	0x80000	NAND Crystal Interposer	0x80000
	USB	0x40000	NAND Crystal Interposer	0x40000
	USB + proximity sensor	0xc0000	NAND Crystal Interposer	0xc0000
15 Pro	USB	0x100000	NAND	0x300000
	proximity sensor	0x200000	Proximity Sensor	0x200000
	USB + proximity sensor	0x300000	Charging Port Flex	-
	wireless charging module	0x400000	Wireless Charging Coil	0x400000
	USB + wireless charging module	0x500000	NAND	0x700000
	wireless charging module + proximity sensor	0x600000	Wireless Charging Coil + Proximity Sensor	0x600000
	USB + wireless charging module + proximity sensor	0x700000	Wireless Charging Coil + Charging Port Flex	-

SUNGKYUNKWAN UNIVERSITY

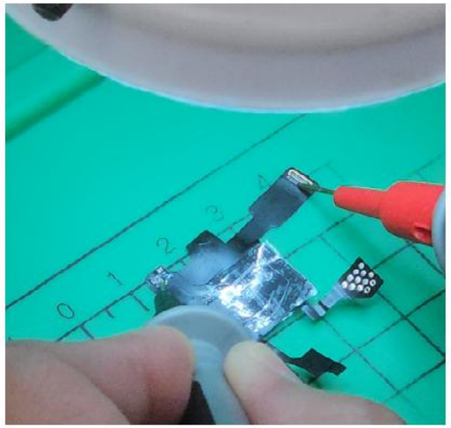
- **Scenario 3. Resolve panic-full issue with replacement of essential modules**
  - **Purpose**: Test data acquisition after replacing damaged modules.
  - **Procedure**: Replaced damaged components with functioning ones.
  - **Result**
    - Message displayed - “Unable to determine if your iPhone module is a genuine Apple part.”
    - However, No panic-full events or abnormal shutdowns occurred.
    - Data acquisition completed successfully.



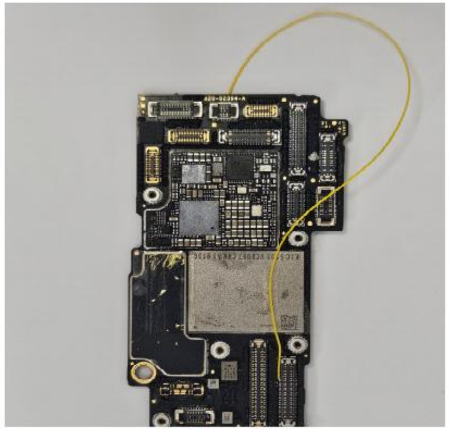
- **Scenario 4. Resolve panic-full with circuit-level repairs of logic board**
  - **Objective** : to identify a solution for cases where module replacement did not resolve the panic-full issue. Assume damage to the logic board connectors, diagnose damage using a multimeter, and identify circuit bypass routes
  - **Method** :
    - Removed individual components from the module using a hot air blower.
    - Checked if removal triggered panic-full behavior.
    - Identified critical components responsible for the malfunction.
    - Performed multimeter tests to trace electrical paths.
    - Reconnected paths and verified system stability.



core components finding (proximity sensor)



electric paths finding



new paths creation

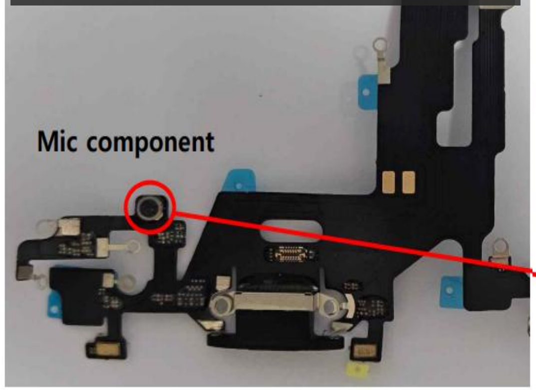
SUNG KYUN KWAN UNIVERSITY

- **Scenario 4. Resolve panic-full with circuit-level repairs of logic board**
  - Result 1 - USB Module

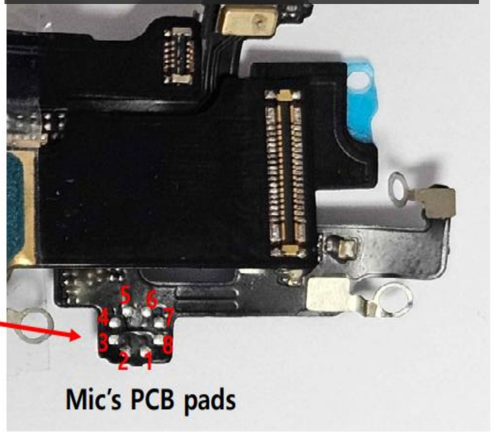
iPhone 11

- Removal of the **microphone component** in the USB module → panic-full event.
- Pads 4 and 7 on the PCB are electrically linked to **USB connector pins.**
- These pins connect to **capacitors**, a **filter**, and finally the **Power Management Unit (PMU)** .
- Disruption of this electrical path → panic-full event.

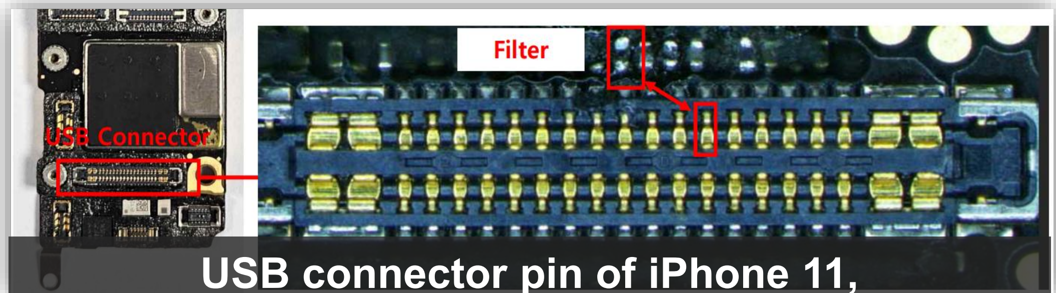
Microphone component of iPhone 11's USB module



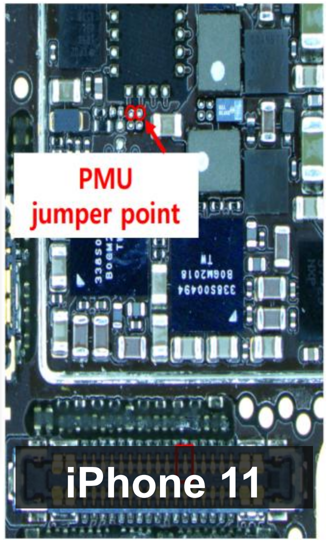
PCB pads after chip-off



Model	11	13 Pro	14 Pro	15 Pro
Error code	Prs0	0x800	0x1400000	0x1000000



USB connector pin of iPhone 11, electrical path to filter

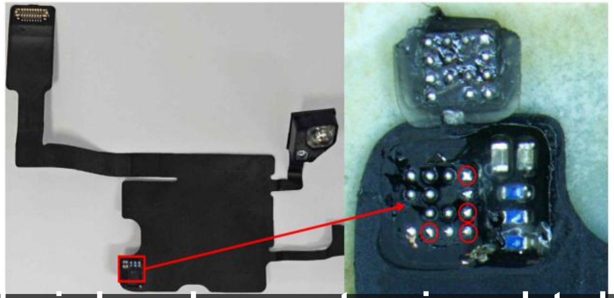


iPhone 11

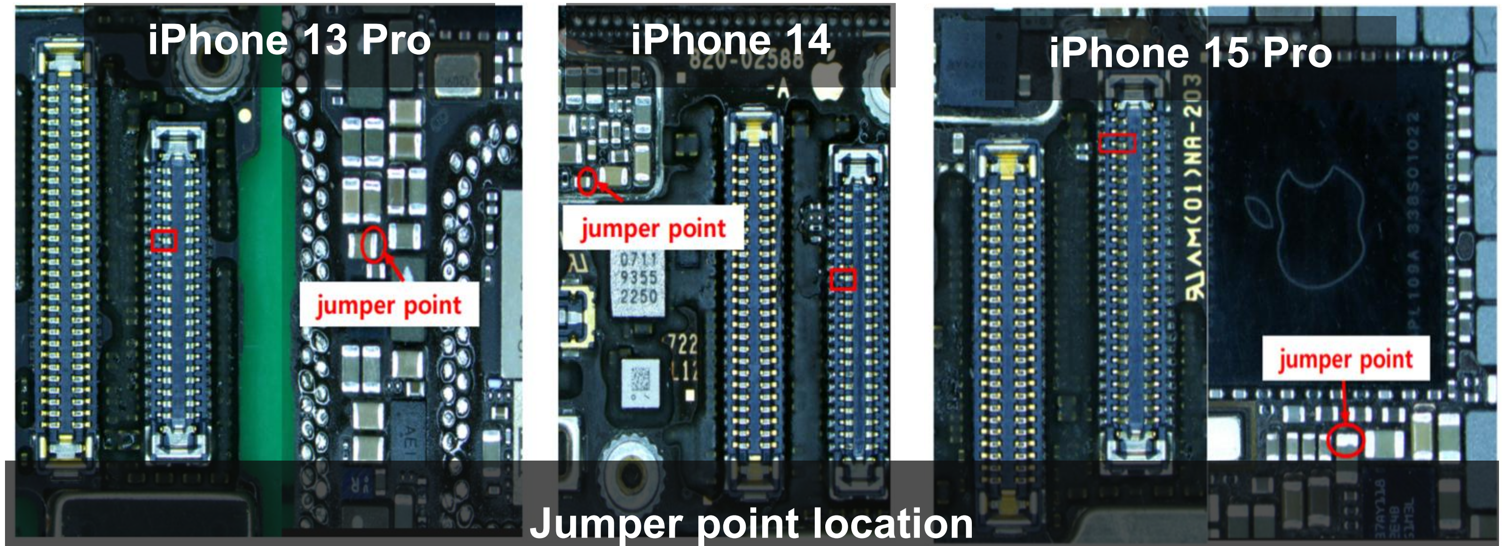
- **Scenario 4. Resolve panic-full with circuit-level repairs of logic board**
  - Result 1 - USB Module
    - Same issue confirmed in **iPhone 13 Pro / 14 Pro.**
    - **Diagnosis:** Diode-mode multimeter test identifies damaged filters.

iPhone Model	11	13 Pro	14 Pro	15 Pro
Diode expectation (Volt)	0.274	0.663	0.395	0.630

he path with **jumper-wire connection**



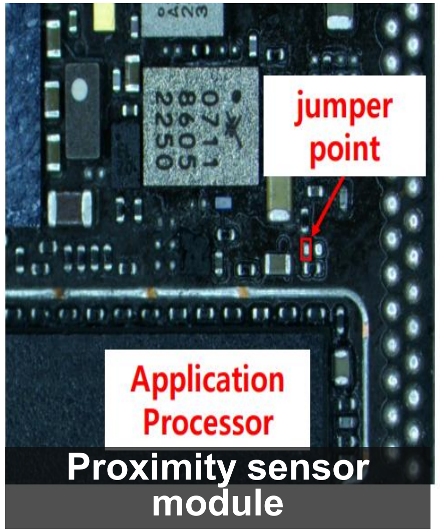
logic board connector pins related to the panic-full (In the USB Module)



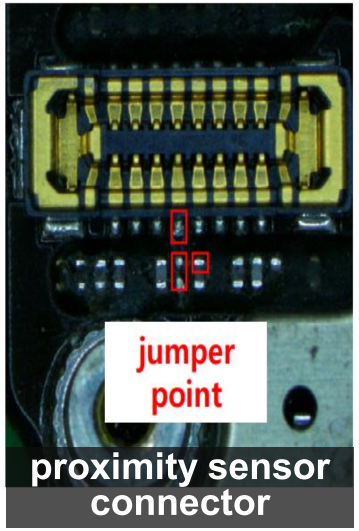
Jumper point location

Resolving a panic-full event by connecting jumper point

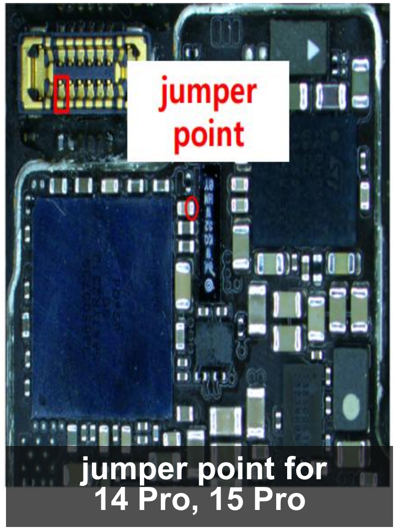
- **Scenario 4. Resolve panic-full with circuit-level repairs of logic board**
  - Result 2 - Proximity Sensor Module
    - Removing the IC component of the proximity sensor → panic-full event.
    - Error value in Panic String: 0x1800000.
    - Circuit path: Logic board connector → Proximity sensor → Ambient light sensor → Control IC.
    - Solution: connecting these jumper points to the terminal of the proximity sensor connector on *the logic board → Restores normal operation and allows forensic data acquisition.*



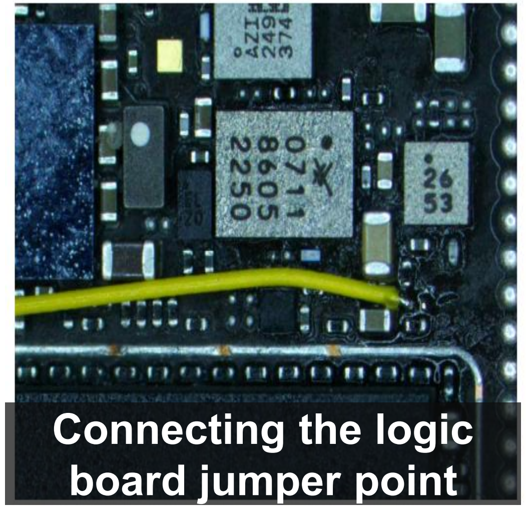
Proximity sensor module

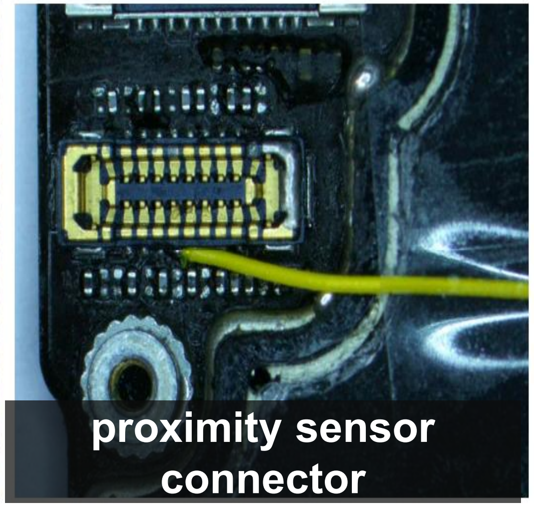


proximity sensor connector

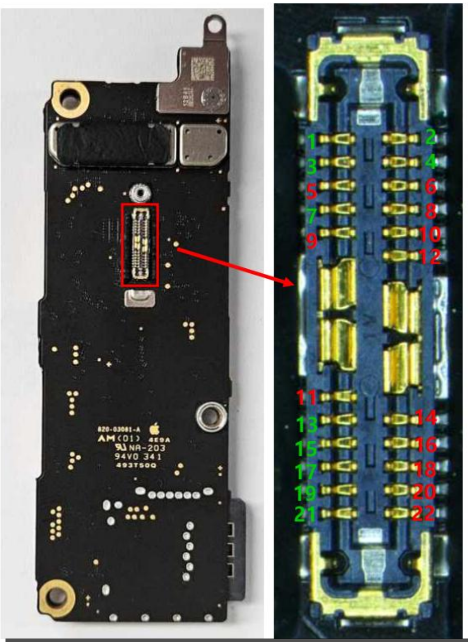


jumper point for 14 Pro, 15 Pro

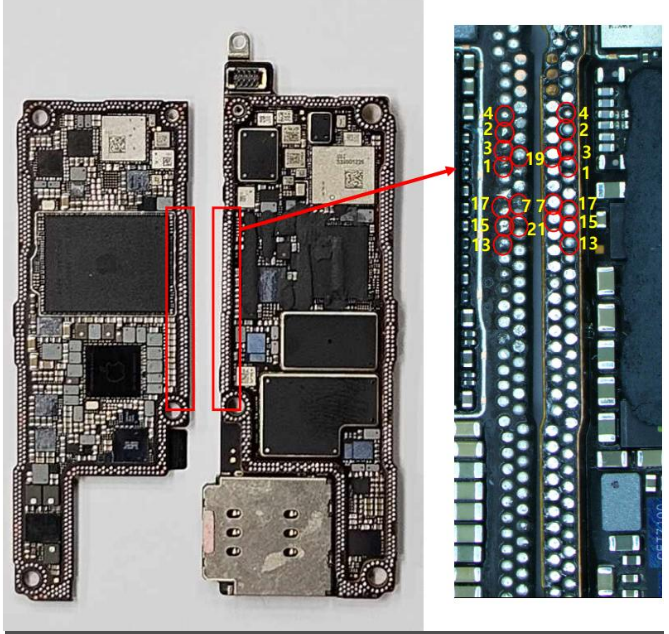

Connecting the logic board jumper point


proximity sensor connector

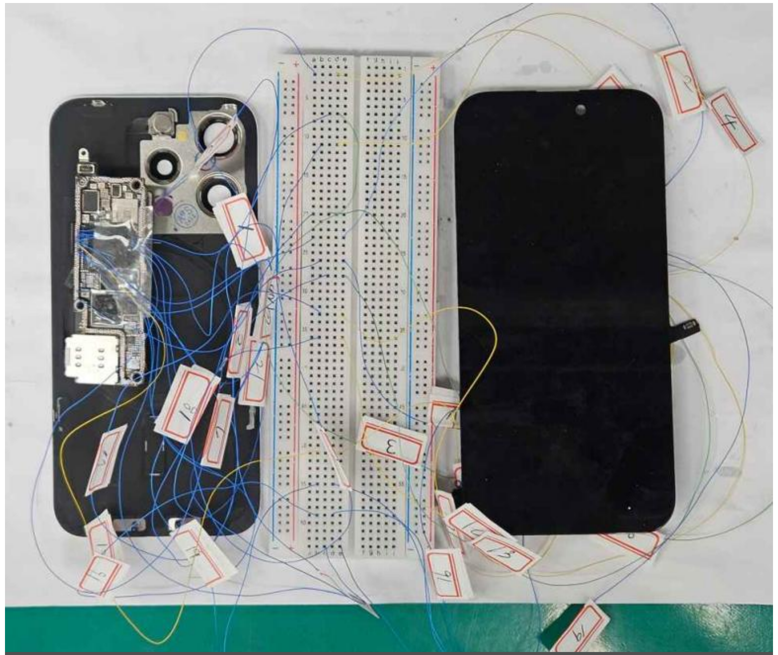
- **Scenario 4. Resolve panic-full with circuit-level repairs of logic board**
  - Result 3 – Wireless Charging Module
    - For the wireless charging module, jumper points are more complex.
    - Linking the connector and interposer with a breadboard also resolves the panic-full problem.



Wireless charging module connector



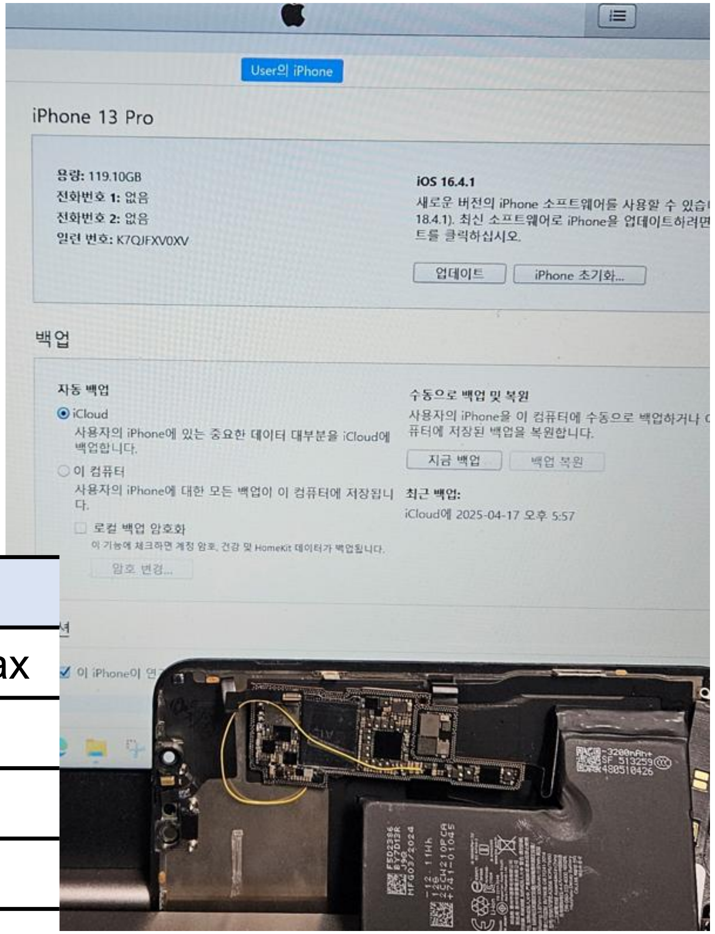
jumper point in the interposer for 15 Pro



Connecting the logic board interposer jumper point and wireless charging module connector of 15 Pro

Scenario 5. Determine necessity for logic board reassembly

- **Purpose:** Test whether reassembly of upper & lower logic-board parts is required after separation.
- **Findings:**
  - iPhone 15 / 15 Plus: Battery terminal + PMU supply power through the inter-board connection → Reassembly essential.
  - iPhone 15 Pro / Pro Max: Wireless-charging module located on lower board → Reassembly required.
  - Other models: Data acquisition possible without reassembly; only AP + essential module connectors needed.



Model(release)	Reassembly not required	Reassembly required
15 (2023)		15, 15 Plus, 15 Pro, 15 Pro Max
14 (2022)	14 Pro, 14 Pro Max	14, 14 Plus
13 (2021)	13, 13 Pro, 13 Pro Max, 13 Mini	
12 (2020)	12, 12 Pro, 12 Pro Max, 12 Mini	
11 (2019)	11 Pro, 11 Pro Max	11
X (2017 -2018)		X, XS, XS Max

SUNG KYUN KWAN UNIVERSITY

04

Conclusion

01 Key Findings and Proposed Recovery Procedure

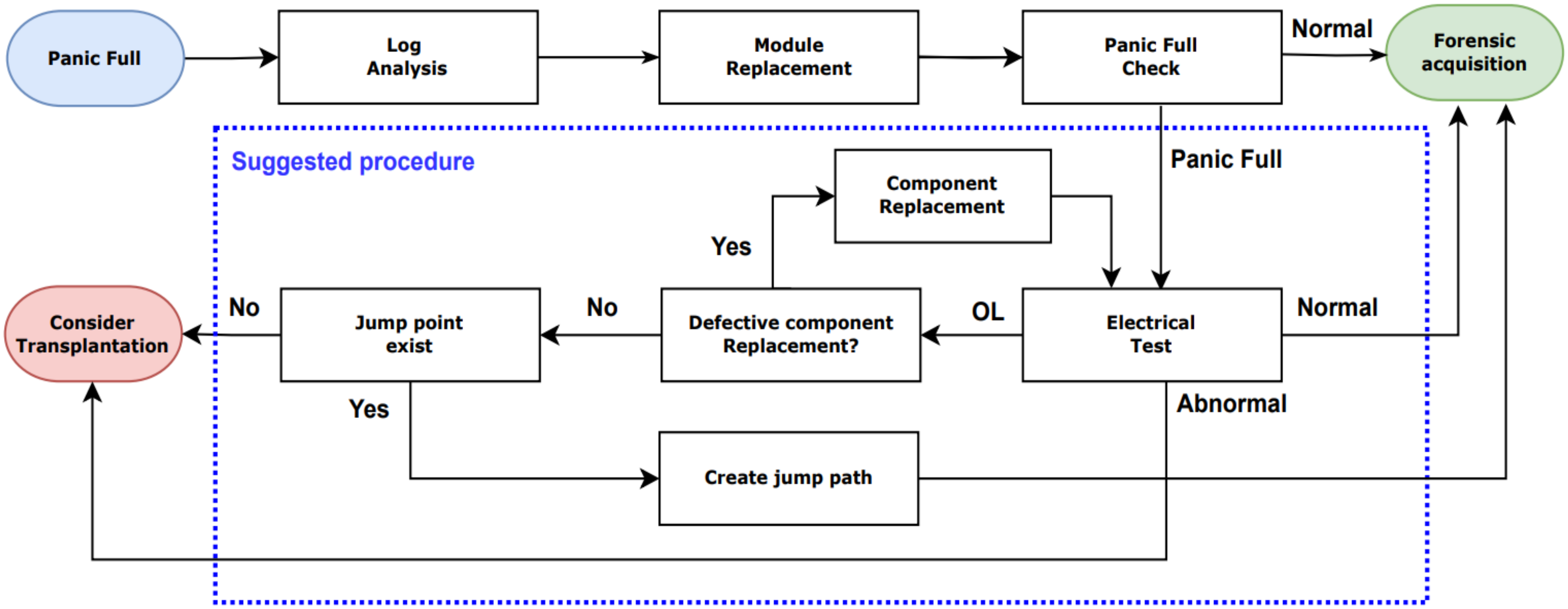
02 Additional Diagnostic – USB Communication Failure

03 Conclusion and Future Work

SUNG KYUN KWAN UNIVERSITY

1. Essential Modules

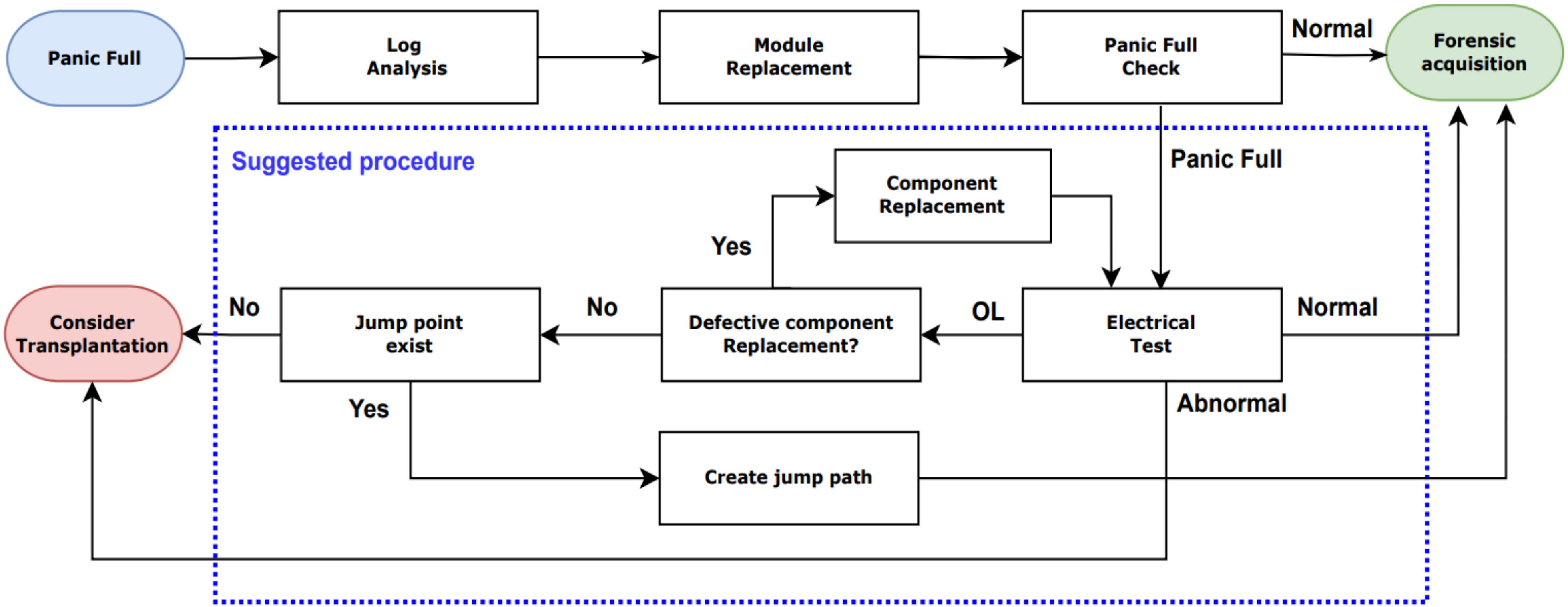
- Not all logic-board modules are required for data acquisition.
- Only certain modules (USB, Power, Proximity Sensor, Wireless Charging) are essential.
- Missing any of these triggers a panic-full event.
- Panic-full logs help identify malfunctioning modules (via Panic String error code).



SUNGKYUNKWAN UNIVERSITY

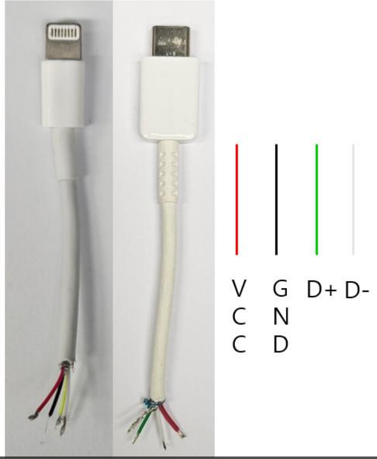
2. Damage Types and Solutions

- Tearing of FPCB modules → solved by **replacing the module**.
- Connector/filter damage on logic board → requires **circuit-level diagnosis** using a multimeter.
- If PCB pads intact → repair or **jumper-wire bypass** restores function.
- If pads or jumpers unavailable → apply **chip-transplantation** (AP + flash memory transfer).



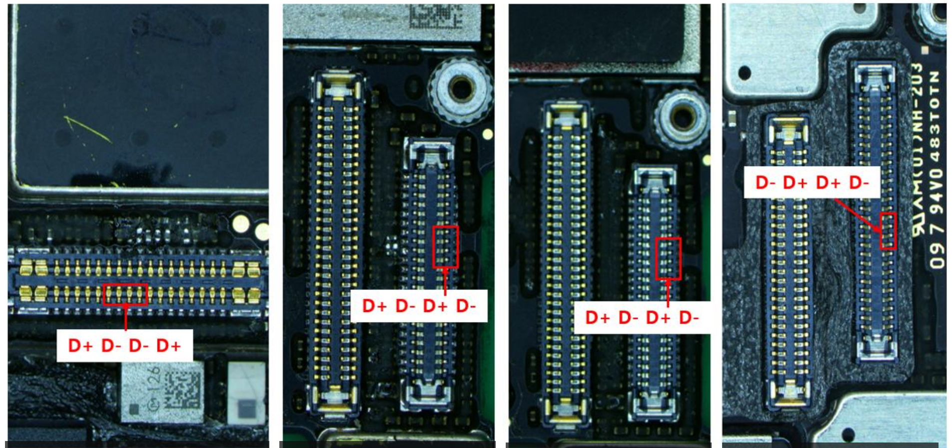
SUNGKYUNKWAN UNIVERSITY

- **When USB module damage prevents data communication:**
  - Perform **diode test** on USB connector pins.
  - **Normal condition:** multimeter readings match Table 9.
  - **Damage condition:** “OL” reading appears.
  - In case of “OL” inspect and, if needed, replace:
    - **USB connector**, and/or
    - **USB Switch IC**
      - ✓ iPhone 11 → U6300
      - ✓ iPhone 13 Pro / 14 Pro → U9300
      - ✓ iPhone 15 Pro → U9500



USB connector pin information

Model	D+ diode expectation (Volt)	D- diode expectatio n (Volt)
iPhone 11	0.656, 0.666	0.656, 0.664,
iPhone 13 Pro	0.4930, 0.508	0.486, 0.509
iPhone 14 Pro	0.577, 0.660	0.587, 0.661
iPhone 15 Pro	0.728, 0.720	0.725, 0.730



iPhone 11 | 13 Pro | 14 Pro | 15 Pro

Conclusion and Future Work

- **Novelty**
  - First study addressing *panic-full* issues on iPhones from a **digital forensic perspective.**
- **Contributions**
  - Identified that only a **subset of modules** (USB, power, proximity, wireless charging) trigger panic-full events.
  - Reconstructed panic-full phenomena and **collected diagnostic logs**.
  - Improved **reliability of forensic diagnostics** by comparing with public data.
  - Proposed a **model-specific list of essential modules** and clarified **when reassembly is required**.
  - Suggested **jumper-point and circuit-level repair methods** for damaged components.
  - Developed an **improved physical recovery procedure** for cost-effective forensic data extraction.
- **Limitations & Future Work**
  - Study focused only on hardware-related panic-full cases.
  - Future work: extend to **software-level failures** (firmware corruption, kernel crashes) and **broader device coverage**.

Q & A

Email : ssb16879@gmail.com

SUNG KYUN KWAN UNIVERSITY

Thank you for listening

2025APAC
DFRWS