A study on the recovery of damaged iPhone hardware exhibiting panic full phenomena

By:
Sunbum Song, Hongseok Yang, Eunji Lee, Sangeun Lee, Gibum Kim

From the proceedings of
The Digital Forensic Research Conference
DFRWS APAC 2025
Nov 10-12, 2025

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment.
As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.
https://dfrws.org

Forensic Science International: Digital Investigation 54 (2025) 301980

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS APAC 2025 - Selected Papers from the 5th Annual Digital Forensics Research Conference APAC

A study on the recovery of damaged iPhone hardware exhibiting panic full phenomena

Sunbum Song [a,b,1], Hongseok Yang [a,b,1], Eunji Lee [a], Sangeun Lee [a,b], Gibum Kim [a,*]

[a] Sungkyunkwan University, Department of Forensic Science, Digital Forensics, 25-2 Sungkyunkwan-ro, Jongno-gu, Seoul, 03063, Republic of Korea
[b] Korean National Police Agency, Digital Forensic Center, 97, Tongil-ro, Seodaemun-gu, Seoul, 03739, Republic of Korea

ARTICLE INFO

Keywords:
Panic full bypass
Physical recovery
iPhone reboot
Mobile forensics
iPhone diagnosis

ABSTRACT

To acquire data stored on damaged devices, forensic analysts have conventionally removed the flash memory from the device and directly extracted the data from it. This process, often called 'chip-off' technique, has faced difficulties in application as data encryption technologies are being widely adopted. Except for rare instances where highly advanced chip transplantation is necessary, analysts generally attempt to repair the damaged modules as much as possible. When critical modules in an iPhone are damaged, the device experiences a phenomenon known as panic-full, in which the device repeatedly reboots, preventing analysts from acquiring data within. This research reviews the previously disclosed causes and analysis methods of panic-full through experiments. Furthermore, for cases where module replacement does not resolve the panic-full status, this paper provides diagnosis methods to detect damages to logic boards and as well as jumper point information. Lastly, based on above findings, an improved physical recovery process for iPhones in panic-full status is suggested. This study has been conducted on limited models of iPhone models, yet with Apple's unified hardware ecosystem, the findings and methodologies suggested in this paper can be easily extended to other models.

1. Introduction

Digital devices such as smartphones and laptops often arrive at forensic laboratories damaged due to various reasons, including water immersion, physical impact, and fire. Traditionally, in order to acquire data stored on such damaged devices, analysts identify and repair damaged components such as integrated chip (IC), similar to the procedures taken at official service centers. In cases where repair is not feasible, analysts employ methods such as the chip-off technique, which involves physically removing components that contains data—such as flash memory—from the device in order to directly extract the data (Blackman, 2015). Since smartphones contain personal information such as photos, call logs, and messages, Apple Inc. introduced device data encryption starting with the iPhone 3 GS in 2009, and Android followed suit with version 3.0 in 2011 (Schuetz, 2014; Zobnin, 2015). With device encryption in place, techniques that directly extract data from storage media, such as the aforementioned chip-off, have become increasingly impractical. Alternatively, the chip-transplantation technique, which involves removing both the flash memory and the additional module responsible for data encryption and transplanting them onto a functioning board of the same model, can be considered. However, during the process of detaching modules from the original board and remounting them onto a new board, the evidence is exposed to high temperatures multiple times, increasing the risk of data degradation. Also, the miniaturization of the Application Processor (AP) makes it difficult to guarantee the success of the procedure. For these reasons, chip-transplantation is regarded as the last resort for analysts (Heckmann et al., 2018). Instead, techniques aimed at preventing further damage to the device upon arrival at the forensic laboratory, diagnosing abnormal or malfunctioning modules, and restoring their functionality are increasingly preferred (Vishnoi and Sapra, 2024; Kumar et al., 2021). Unlike Android devices, iPhones may enter a state of continuous rebooting — known as "panic-full" — when one or more essential modules connected to the logic board (main PCB) are damaged (Wiki, 2023b). Panic-full occurs even when critical components on the logic board, such as the Application Processor (AP) and flash memory, are functioning normally. Since data acquisition often takes several hours, it is not feasible to perform proper forensic data extraction on a device experiencing panic-full. To address the panic-full phenomenon, conventional device repair approaches reference the "Panic Full" logs

* Corresponding author.
E-mail addresses: ssb16879@gmail.com (S. Song), jamemanionda@naver.com (E. Lee), freekgb02@gmail.com (G. Kim).
[1] First author, Authors contributed equally.

https://doi.org/10.1016/j.fsidi.2025.301980

Available online 3 November 2025
2666-2817/© 2025 The Author(s). Published by Elsevier Ltd on behalf of DFRWS. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

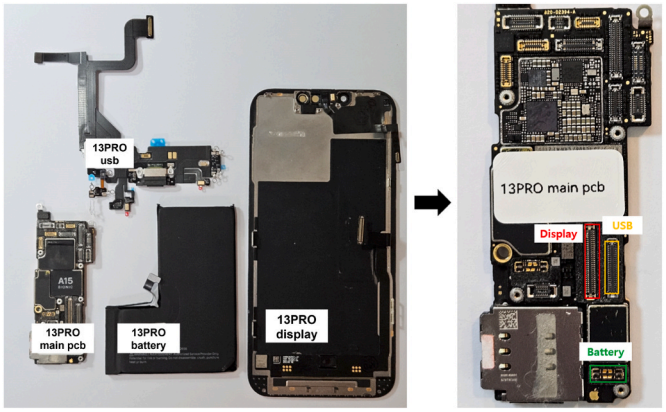

Fig. 1. Logicboard and modules of iPhone 13.

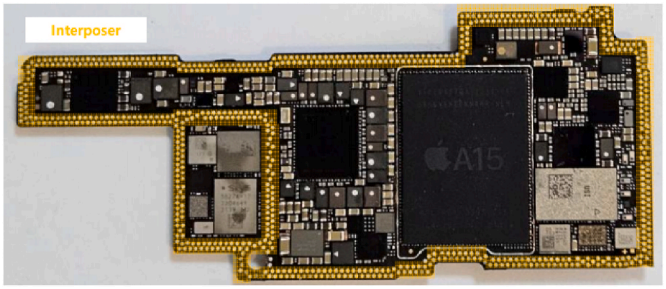

Fig. 2. Interposer of logic board.

Table 1
User occupancy by iPhone model (Scientiamobile, 2024).

model	iPhone 11	iPhone 13	iPhone 12	iPhone 14 Pro	iPhone 14	iPhone 13 Pro
occupancy	4.47 %	3.25 %	2.22 %	1.89 %	1.64 %	1.62 %

retained on the iPhone to diagnose the issue and replace suspected damaged modules. Diagnostic programs and relevant information for these procedures are publicly accessible online. However, there are cases where the panic-full phenomenon cannot be resolved through these procedures. In such cases, particularly when the analysis is about critical evidence, analysts have had to consider applying the highly advanced chip-transplantation technique. Despite the significance of these challenges, panic-full states remain largely unexplored from a digital forensic perspective in academic literature. To address this research gap, this study aims to address the following research questions (RQ) in data acquisition from iPhones experiencing panic-full:

RQ1: What are the essential hardware modules required for data acquisition from an iPhone in a state where the panic-full phenomenon does not occur?
RQ2: What are the symptoms and diagnostic methods when essential hardware modules are damaged?
RQ3: Can a simple replacement of damaged modules resolve the issue?
RQ4: If simple module replacement does not resolve the panic-full phenomenon, are there additional diagnostic and resolution methods?

With respect to answering the above RQs, this study presents the following contributions.

Table 2
Test devices and software.

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

Table 3
Test Scenarios objective and summary.

No	Scenario objectives	Summary of tests
1	Identify essential hardware module	Disconnected modules from the logic board and observe for panic-full behavior
2	Identify diagnostic information	For panic-full logs collected in Scenario 1, analyze and compare the log to existing diagnostic methods
3	Resolve panic-full issue with replacement of essential modules	Replace essential H/W modules with functioning modules from an identical model and observe for panic-full behavior
4	Resolve panic-full issue with circuit-level repairs of logic board	Assume damage to the logic board module connectors, diagnose damage using a multimeter, and identify circuit bypass routes
5	Determine necessity for logic board reassembly	Identify possibilities for not reassembling logic board after connecting essential modules, and observe for panic-full behavior in due process

Fig. 3. Procedures taken for Scenario 1.

- The objective of general device repair, which aims to enable users to fully operate all functions of the device, differs from that of forensic recovery, which seeks to restore only the minimum functions necessary for internal data acquisition. This study presents the specific combination of hardware modules required for data acquisition from a forensic recovery perspective, focusing on iPhone models that are currently widely used.
- Tools and methods for identifying the faulty components via Panic Full log analysis are publicly available online. This study improves the reliability of such diagnostic approaches by comparing the information available online with experimental results derived from scenario-based testing.

Table 4
Modules per test 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

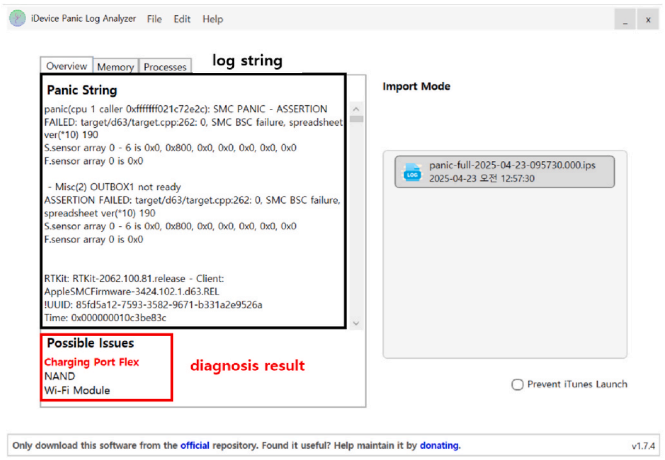

Fig. 4. iDevice Panic Log Analyzer.

- While panic-full phenomena can generally be resolved by replacing the defective module, damage resulting from events such as water immersion may affect the logic board itself, rendering simple module replacement ineffective. In such cases, forensic analysts may consider the chip-transplantation technique. As chip-transplantation is often the last resort, this study proposes a new diagnostic and repair approach to identify damage to logic board connectors and surrounding components, as well as to construct circuit bypass routes that can be utilized to mitigate further evidence degradation while resolving the panic-full condition.
- By integrating the above methods, this paper presents an improved physical recovery process for iPhones exhibiting panic-full phenomenon.

The scope of this study is limited to iPhones that exhibit the panic-full phenomenon after booting, and does not include devices that fail to reach the normal boot stage due to issues such as short circuits in the logic board.

The remainder of this paper is organized as follows. Section 2 discusses the background and related work. Section 3 describes the experimental scenarios and devices used. Section 4 presents the experimental results and improved solutions, and Sections 5 covers the conclusion and discussion, respectively.

2. Background and related work

2.1. Hardware structure of the iPhone

In general, smartphones are structured around a mainboard that integrates the AP, flash memory for data storage, and wireless communication modules, with peripheral components such as the camera, battery, and display connected to it. In the case of iPhones, as shown in

Table 5
Comparison of panic-full log per module damage.

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	–

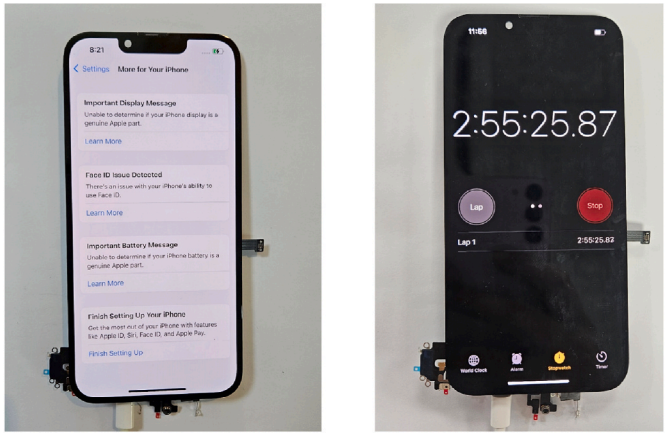

Fig. 5. Test results of Scenario 3 (13 Pro).

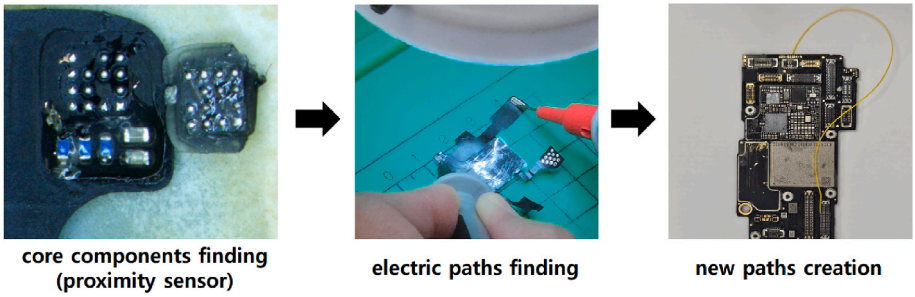

Fig. 6. Testing methodology of Scenario 4.

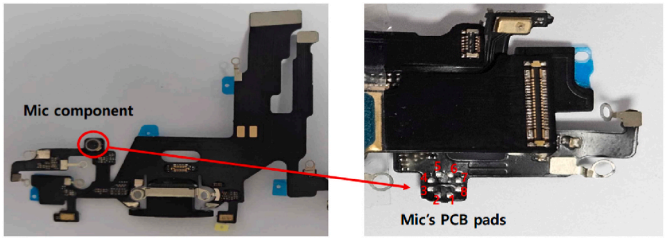

Fig. 7. (Left) Microphone component of iPhone 11's USB module/(right) PCB pads after chip-off.

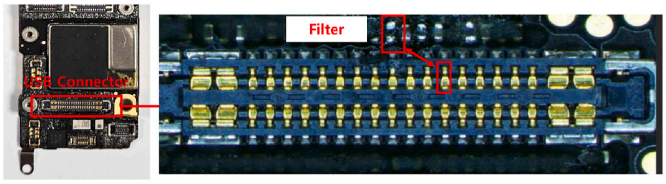

Fig. 8. USB connector pin of iPhone 11, and electrical path to filter.

Fig. 1, various hardware modules are connected to a central logic board. Beginning with the iPhone X, released in 2017, Apple adopted a stacked logic board design—transitioning from a single-layer structure—in order to conserve internal space and accommodate a greater number of components (PCMAG, 2017; IFIXIT, 2017).

The logic board features a stacked structure composed of an upper and lower layer, which are connected via an interposer. The interposer, as shown in Fig. 2, electrically links the upper and lower PCBs through a series of fine contact points located along the edges of the board. Modules connected to the logic board typically utilize a Flexible Printed Circuit Board (FPCB) structure. FPCB is an electronic component consisting of printed circuits on a flexible substrate. Its thin and bendable nature makes them essential for the compact and complex internal architecture of smartphones.

2.2. Diagnosis of damaged hardware

Digital devices such as smartphones integrate various components—including Integrated Circuits (ICs) such as the AP, flash memory, and the Power Management Integrated Circuit (PMIC), as well as resistors—onto a single board. Damage to any of these components can disrupt the normal operation of the device. To identify faulty modules, forensic analysts employ diagnostic techniques such as microscope inspections (Fukami and Nishimura, 2019), electrical tests (Kumar et al., 2021), infrared analysis, and X-ray-based inspection methods (Thomas-Brans et al., 2022). Among these, one of the most commonly employed techniques is electrical test utilizing multi-meter. The following are frequently used modes. In a diode mode, the tester applies a small current through the test leads and measures the voltage drop

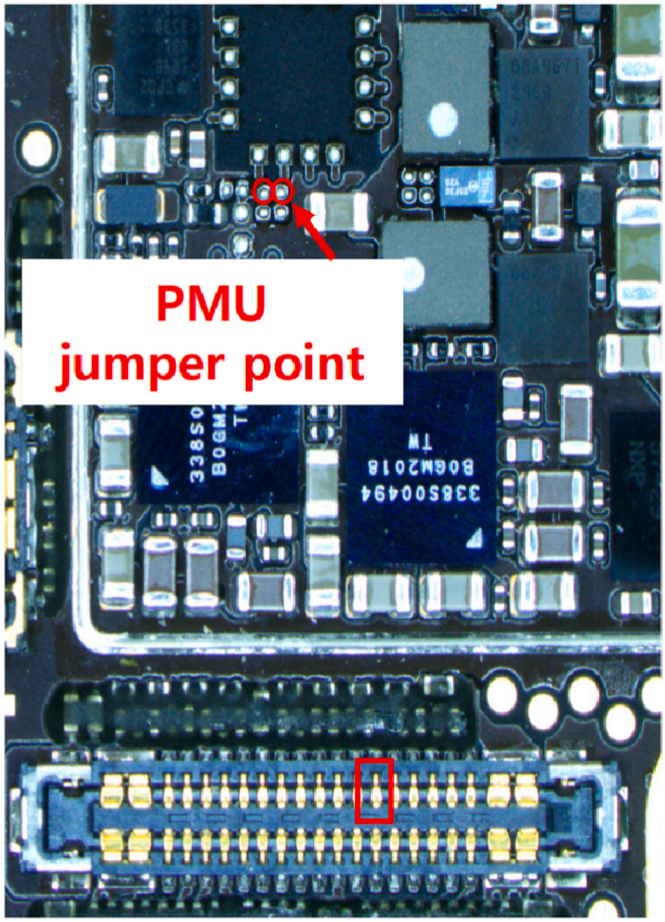

Fig. 9. PMU Jumper point of iPhone 11.

Table 6
Error codes for USB module path disruption.

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

Table 7
Multimeter diode expectation by model.

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

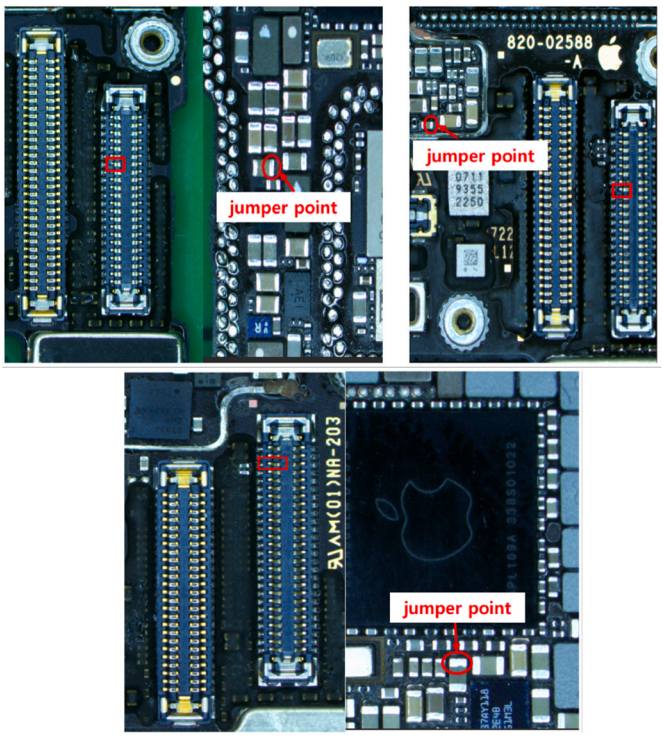

Fig. 10. Jumper point locations of iPhone 13 Pro (left), iPhone 14 (center), iPhone 15 Pro (right).

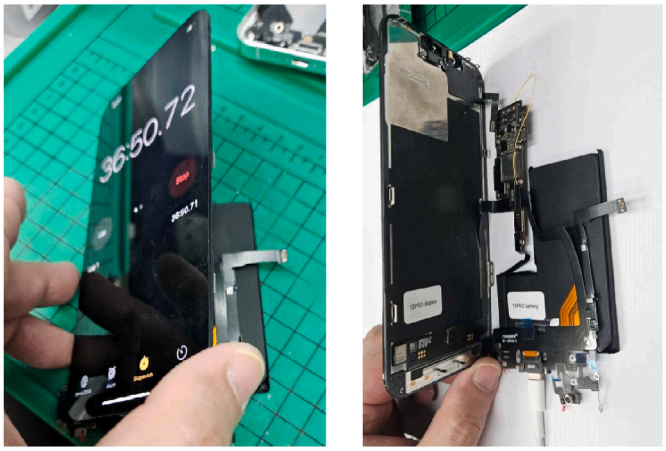

Fig. 11. Resolving a panic-full event by connecting jumper point.

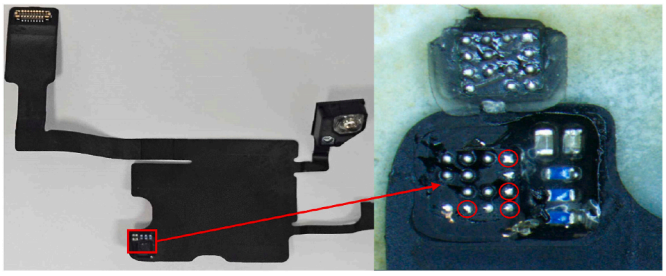

Fig. 12. Removal of the proximity sensor module in iPhone 14 Pro.

across a diode. A functional diode typically shows a voltage drop in one direction and "Open Loop" (OL) in the reverse direction, indicating no current flow. A damaged diode, on the other hand, may display OL in both directions, signifying a failure to conduct current. When the circuit is connected, the multimeter usually emits a beep indicating continuity and if the circuit is broken, OL is displayed (FLUKE, 2024; Geier, 2011).

2.3. Hardware recovery from a digital forensics perspective

Physical damage to digital devices can occur due to impact, water immersion, or intentional destruction. Such damage interferes with digital forensic procedures, especially the process of data acquisition. In response to these challenges, forensic analysts have conducted various studies to overcome hardware damage. Breeuwsma et al. (2007) proposed the chip-off technique, which involves physically removing the flash memory from a damaged device (e.g. smartphone), and acquiring the stored data using a memory reader. Blackman (2015) presented several case studies in which data was successfully extracted from smartphones damaged by gunshots or fire using techniques such as Joint Test Action Group (JTAG) and chip-off. Similarly, Lorenz et al. (2023) demonstrated the application of the chip-off method in extracting data from Amazon Echo devices, highlighting its adaptability across a range of digital hardware.

However, with the demand for secure user data management growing, data stored on digital devices is now commonly encrypted using technologies such as bitlocker (Paolomatarazzo and Vinaypamnani-msft, 2025) and veracrypt (Veracrypt, 2016). In particular, the introduction and spread of dedicated hardware for encryption, such as Apple's Secure Enclave (Apple, b), has made it virtually impossible to acquire data solely by accessing the flash memory via chip-off technique. In response to these changes, forensic analysts have been focusing on techniques that either prevent further damage to the device or identify and repair damaged hardware components to enable successful data acquisition (Fukami and Nishimura, 2019; Kumar et al., 2021; Breeuwsma et al., 2007; Solodov and Solodov, 2021). When the extent of the damage renders repair unfeasible, but both the flash memory and data encryption modules remain functional, analysts may consider the chip-transplantation technique. which involves transplanting of the relevant modules onto a functioning mainboard of the same device model.

Nonetheless, the use of chip-transplantation techniques repeatedly exposes the device to high temperatures, increasing the risk of evidence degradation. Also, the process requires highly skilled micro-level reballing steps, making it impractical for routine application to every single device submitted as evidence.

2.4. iOS log forensics

Recent forensic research into Apple's iOS logs has primarily focused on 'Sysdiagnose' and 'knowledgeC.db'. iOS provides Sysdiagnose logs which contain crash reports and various diagnostic data to assist in resolving issues that occur during system operation. Epifani et al. (2019) conducted a study on the collection and structure of Sysdiagnose logs in iOS, publishing a Python script capable of analyzing 13 distinct types of Sysdiagnose logs, including OS and network data. Sysdiagnose utilizes the Apple Unified Log (AUL) format, and research has been made on its structure. Edwards (2017) analyzed AUL-format logs and proposed forensic methods for extracting user-related artifacts such as login activity and Time Machine backup history by using iOS built-in system commands. Holcomb (2022), through a structural analysis of AUL, developed a Python script to analyze logs without relying on system commands. KnowledgeC.db is a system database found in iOS versions 11 through 16. This database enables forensic analysts to examine user activity, such as application usage and website visit history (Belkasoft, 2002). Sarah Edwards demonstrated that knowledgeC.db retains detailed information on application usage and history for approximately

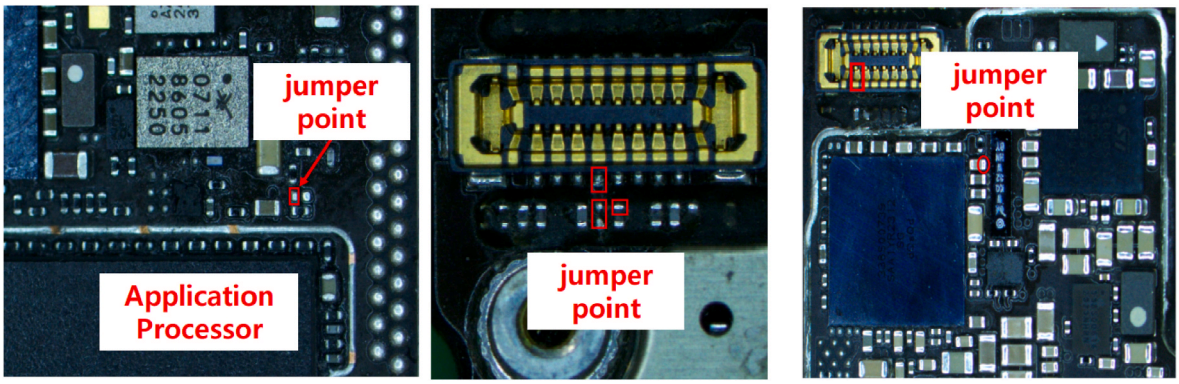

Fig. 13. Proximity sensor module (left) and proximity sensor connector (center) jumper point for iPhone 14 Pro, iPhone 15 Pro (right).

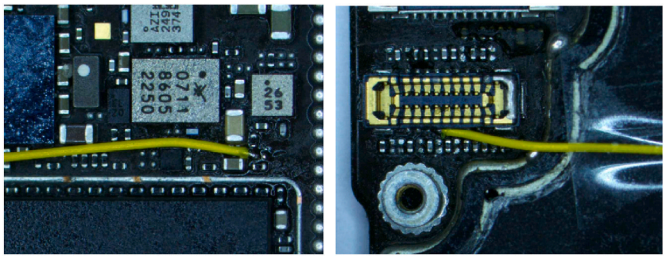

Fig. 14. Connecting the logic board jumper point (left) and proximity sensor connector (right) of iPhone 14 Pro.

four weeks (Edwards, 2018b, 2018a). Whiffin further analyzed the artifacts in knowledgeC.db and developed the ArtEX tool, which allows analysis of not only knowledgeC.db but also other iOS databases such as sms.db and history.db (Whiffin, 2019, 2023).

Finally, iOS records diagnostic data in 'Crash Logs' whenever applications terminate unexpectedly. These logs allow analysts to identify which applications were active at specific period of time. In particular, when the iOS kernel experiences a critical error, the system logs detailed hardware and memory information in 'Kernel Panic Logs', after which the device automatically reboots. These logs are stored in files whose names begin with 'panic-full', and are commonly referred to as panic-full logs (8ksecresearch, 2021). For rooted iPhones, panic-full logs can be accessed at the file path/private/var/mobile/Library/Logs/CrashReporter. On non-rooted devices, they can be viewed via the Settings → Privacy → Analytics menu on the iPhone (Apple, a). Additionally, these logs can be extracted using tools such as idevicecrashreport of the (Libimobiledevice, 2020). The panic-full logs are stored in plain text format and contain detailed information about memory status and processes. By examining the 'Panic String' field, analysts can identify the cause of the panic and related diagnostic codes. When physical damage occurs to an iPhone, it is common for the device to enter a panic-full state, characterized by repeated reboot cycles (Aimon). From a device repair-oriented perspective, tools and publicly available resources to analyze panic-full logs exist to support the diagnosis of hardware failures as well as to guide corresponding repair techniques (iDevice Panic Log Analyzer, 2020; IFIXIT, 2024; Wiki, 2023a).

3. Experimental design

3.1. Experimental subjects and equipment

To develop appropriate experimental scenarios, we selected the experimental subjects as follows. Among all iPhone models released from the initial iPhone in 2007 up to the iPhone 16e, we identified the models with the highest user share in the first half of 2024. As shown in Table 1, the iPhone 11 had the highest market share at 4.47 %, followed by the iPhone 13 at 3.25 %, and the iPhone 12 at 2.22 % (Scientiamobile, 2024). In addition to the aforementioned statistics, we also considered the availability and economic feasibility of various iPhone models, and selected the test devices as shown in Table 2. Next, to carry out procedures such as the separation of stacked logic boards, removal of IC components mounted on the PCB, and jumper wire

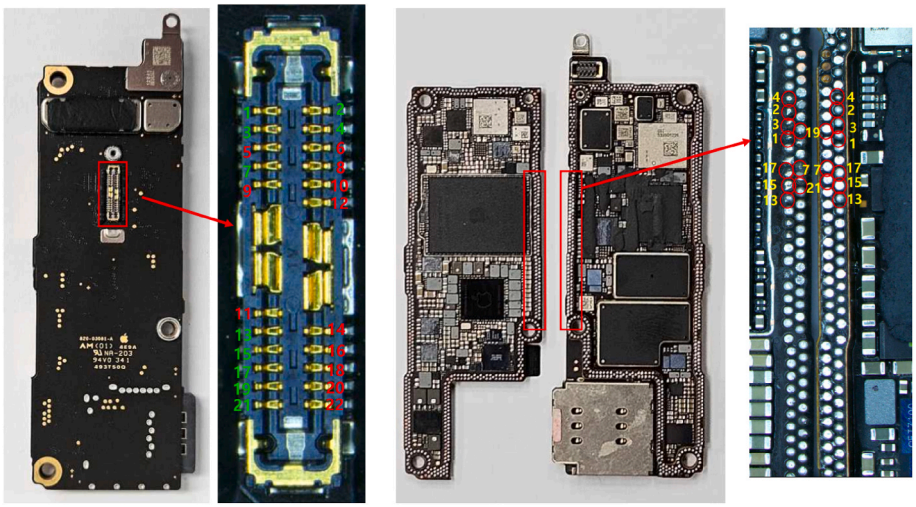

Fig. 15. Wireless charging module connector (left) and jumper point in the interposer for iPhone 15 Pro (right).

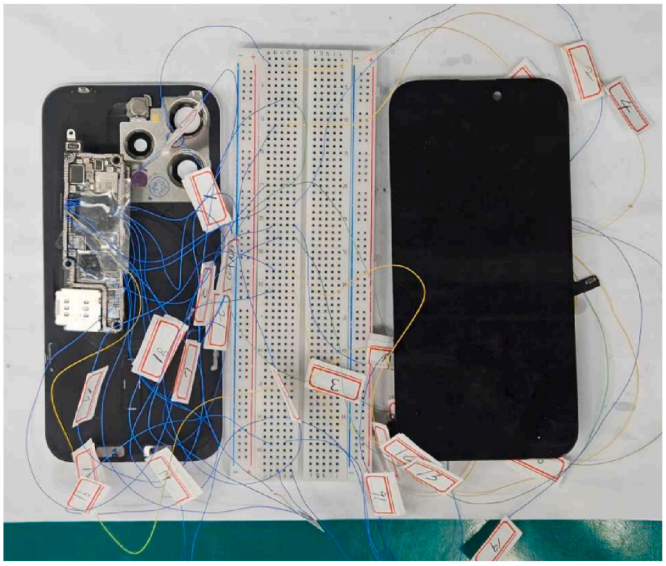

Fig. 16. Connecting the logic board interposer jumper point and wireless charging module connector of iPhone 15 Pro.

Fig. 17. Scenario 5 Results if iPhone 13 Pro.

Table 8
Necessity for reassembly of logic board after separation.

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

connections, we used equipment including a board heater, a hot air gun, and a soldering iron, as listed in Table 2.

3.2. Experimental scenario

To address the research questions, we designed a total of five experimental scenarios, as summarized in Table 3. Scenario 1 focuses on identifying the essential hardware modules required for forensic data acquisition from an iPhone. To simulate hardware failures, we disassembled the test devices and sequentially disconnected modules connected to the logic board — such as USB connectors and proximity sensors — then observed whether the device booted normally or exhibited panic-full behavior. The objective of Scenario 1 is to determine the minimal combination of modules that must be connected to the logic board to prevent the occurrence of a panic-full status. For each device exhibiting panic-full, the panic-full logs are collected. These logs are then used in Scenario 2, which aims to identify diagnostic information that can be used to determine which module has failed. Currently, a number of tools and resources for analyzing panic-full logs are publicly available online. Among them, this paper compares the results of the analysis provided by the Repair.wiki website (Wiki, 2023a) and the iDevice Panic Log Analyzer tool (iDevice Panic Log Analyzer, 2020) with the logs collected during the experiment, to verify the reliability of the existing log-based diagnostic methods. Scenario 3 involves the replacement of the damaged module. Once a faulty module is identified, the forensic analyst may consider transplanting a functioning module from an identical device model to the damaged model. In this scenario, we replaced the damaged module to evaluate whether the panic-full issue is resolved and to identify any other errors that may occur during the data acquisition process. Scenario 4 addresses damage to the logic board module connectors. If replacing a faulty module in Scenario 3 does not resolve the panic-full issue, the forensic analyst may further diagnose damage to the logic board itself. Using a multimeter, the analyst examines areas such as individual modules and the connectors on the logic board. To simulate damage, the ICs attached to the modules were removed and the device was observed for the occurrence of panic-full behavior. Scenario 4 seeks to determine whether panic-full behavior that was unresolved by simple module replacement (Scenario 3) can be mitigated through circuit-level repairs prior to considering chip-transplantation process, which involves removing and relocating the AP and flash memory. Lastly, Scenario 5 focuses on the structural characteristics of the latest iPhone models, which adopt a stacked logic board design. During hardware recovery, the forensic analyst often has to separate the top and bottom layers of the logic board. Reassembling the split PCBs involves a technically demanding re-balling process. Therefore, Scenario 5 investigates whether it is absolutely necessary to reassemble the logic board during the forensic data acquisition process.

4. Experimental results

4.1. Results by scenario

In Scenario 1, we examined whether the device booted normally or triggered a panic-full behavior by sequentially disconnecting individual module connectors from the logic board, as shown in Fig. 3.

As shown in Table 4, the essential modules related to panic-full behavior include USB (lightning), proximity sensor, wireless charging, and power modules. Furthermore, the required combination of modules varies depending on the iPhone model. In the case of the iPhone 14 Plus, it was confirmed that all three modules — USB, proximity sensor, and wireless charging module — must be connected to the logic board. If any of these modules are not attached, the device triggers a panic-full event and reboots after approximately 50–150 s, rendering data acquisition infeasible.

When a panic-full event occurred in Scenario 1, the corresponding panic-full logs were collected. In Scenario 2 these logs and error codes were associated with the (simulated) damaged modules. Subsequently, as shown in Fig. 4, the results were compared with the result analysis publicly available online. The comparative precision of the diagnostics is summarized in Table 5.

In Scenario 3, when we replaced damaged modules with functioning ones on all test devices, an error message ("Unable to determine if your iPhone module is a genuine Apple part"') appeared after booting, as shown in Fig. 5. However, the device did not experience abnormal shutdowns, such as panic-full events, and subsequent data acquisition

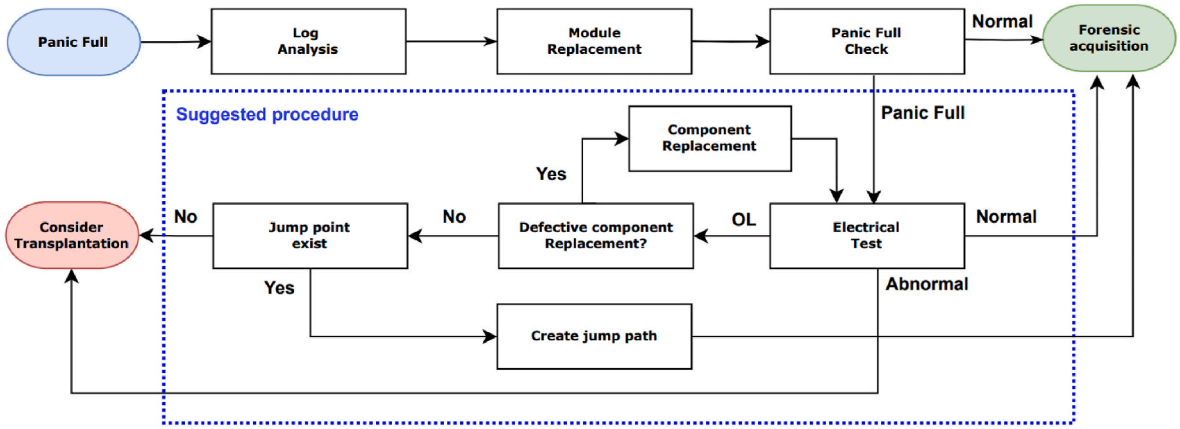

Fig. 18. Improved iPhone physical recovery procedure.

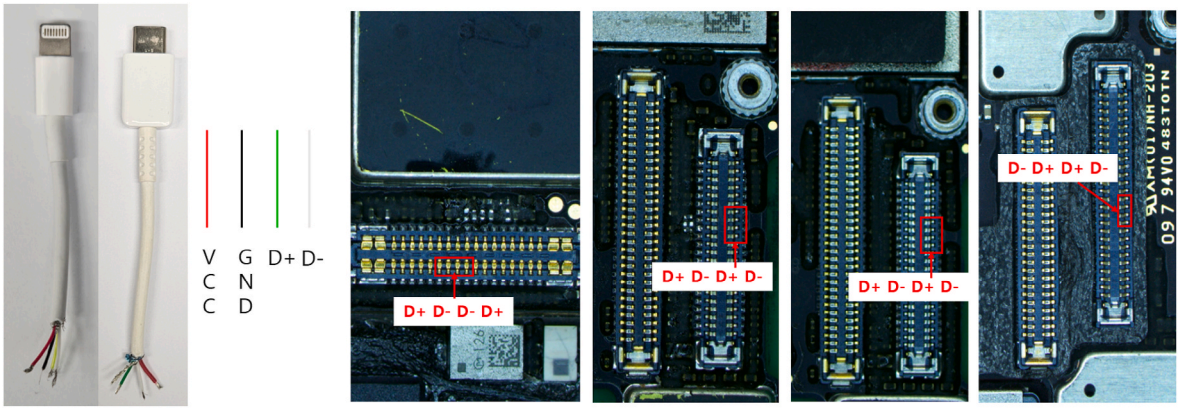

Fig. 19. USB connector pin information for iPhone 11, 13 Pro, 14 Pro, 15 Pro.

Table 9
Multimeter diode expectation for connector terminal by model.

Model	D+ diode expectation (Volt)	D- diode expectation (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

was performed successfully.

In Scenario 4, we sought to identify a solution for cases where module replacement did not resolve the panic-full issue. The specific testing methodology is depicted in Fig. 6. To determine whether individual components within a module could trigger a panic-full event, we removed key components using a hot air blower and then checked whether the device operated normally. If a malfunction occurred, the component was considered critical to the panic-full issue. Subsequently, we conducted electronic tests using a multimeter to identify electrical paths between the critical component, the logic board connector, and the core components. If such electrical paths were identified, we reconnected them and then verified whether the panic-full issue had been resolved.

In the case of the USB module, as shown in Fig. 7, the removal of the microphone component triggered a panic-full event. The PCB connected to the microphone component has a total of eight pads, as illustrated on the right side of Fig. 7, among which pads 4 and 7 are electrically connected to the USB connector pins on the logic board, as shown in Fig. 8. These USB connector pins on the logic board are also electrically connected to the capacitors and the filter located on the upper side of the connector. Ultimately, this electrical path leads to the Power Management Unit (PMU), as depicted in Fig. 9. The disruption of this electrical path leads to a panic-full event.

In other iPhone models (13 Pro, 14 Pro), a panic-full event was also triggered when the path linking the microphone component, filter, and PMU was disrupted. The corresponding error codes extracted from the panic-full logs in the above cases are summarized in Table 6.

In relation to panic-full events caused by USB module defects, the diode mode test of a multimeter is an efficient method for diagnosing damage to components, for example the filter located along the relevant circuit path. When components function normally, the multimeter results are typically similar to those shown in Table 7, whereas in the case of damage, an OL is displayed.

If damage to a component located along the logic board circuit path is confirmed, it is generally possible to either repair the component or identify a jumper point to bypass the damaged path, and then connect it using thin copper wires. This study explored the latter approach and confirmed that even if a component is damaged, the panic-full issue can be resolved as long as the associated PCB pads remain intact. The relevant jumper points were identified, as shown in Fig. 10. Generally, the connector and jumper points are located on the same surface of the PCB. However, in the case of the iPhone 13 Pro, the jumper point is located on the opposite side of the PCB from the USB connector.

As shown in Fig. 11, if a component located along the circuit path related to the USB module on the logic board is damaged, a panic-full event can be resolved by directly connecting the jumper points with a thin copper wire.

In the case of the proximity sensor module, it was confirmed that a panic-full event occurred when the IC component of the sensor module

on the iPhone 14 Pro was removed, as shown in Fig. 12. As in the USB module, the logic board connector pins related to the panic-full issue are indicated on the right side of Fig. 12. When the proximity sensor module is damaged, the error value in the Panic String is 0x1800000.

The circuit path related to the panic-full event of the proximity sensor module consists of the logic board connector, the proximity sensor, the ambient light sensor, and the sensor control IC. As with the USB module, in cases where a component within the electric path associated with the panic-full issue is damaged, the jumper point connection provides a solution to the issue. The relevant jumper point is depicted in Fig. 13. As shown in Fig. 14, connecting these jumper points to the terminal of the proximity sensor connector on the logic board can resolve the issue and allow the forensic acquisition to proceed.

Jumper points for the wireless charging module is relatively more complicated than that of the proximity sensor module. In the case of the iPhone 15 Pro, as shown in Fig. 15, jumper points are located on the interposer of the logic board and on the connector of the wireless charging module. As shown in Fig. 16, linking the connector and the interposer using a breadboard, can resolve the panic-full issue.

In Scenario 5, the necessity for reassembly of the upper and lower parts of the logic board after separation was tested. The results indicated that for iPhone 15 and 15 Plus, the battery terminal and PMU are designed to supply power through the connection between the upper and lower parts of the logic board, making it essential to reassemble the separated PCBs. Also in the case of iPhone 15 Pro and Pro Max, the wireless charging module is located in the lower part of the board, making reassembly a prerequisite for data acquisition. In other cases, it was confirmed that the acquisition of data is possible without reassembling, which means only the PCB connected to the AP and the essential module connectors is sufficient for data extraction. Fig. 17 shows the result of Scenario 5 and Table 8 outlines the necessity for the reassembly of the logic board after separation per model.

4.2. Improved iPhone hardware recovery procedure

Based on the experimental results, the following findings were identified. Not all modules connected to the logic board are required for proper data acquisition. Depending on the iPhone model, only certain modules — such as the USB, power button, proximity sensor, or wireless charging module — are essential. If these essential modules are not connected, a panic-full event is triggered after booting. In this case, forensic analysts can collect the panic-full log and analyze the error code within the Panic String field to identify the malfunctioning module. Tearing is a common result of impact damage to FPCB-based modules. In such cases, replacing the damaged module with a functioning module of the same model typically resolves the panic-full issue. However, if damage such as water immersion affects components on the logic board such as connectors or filters, replacing the module alone does not resolve the panic-full status. In such cases, analysts can use a multimeter to diagnose the components within the circuit path between the faulty module and the logic board. If the components on the logic board are damaged but the PCB pads or associated circuits remain intact, the panic-full issue can be resolved either by replacing the damaged component or by bridging the damaged circuit with an alternative path. However, if the PCB pads of the component are also damaged or if no accessible jumper points are available on the logic board, the panic-full issue cannot be resolved through these methods. In such situations, the analyst may consider chip-transplantation as a last resort, transferring critical components such as the AP and flash memory to a new logic board to retrieve the data within. Based on the above results, Fig. 18 proposes an improved iPhone physical recovery procedure to address panic-full errors.

Additionally, it was found that in cases where the USB module is damaged and data communication is not possible, a diode test of the USB connector pins on the logic board (as shown in Fig. 19) can help distinguish whether the problem lies with the connector or/and the USB switch IC. When both the connector and the USB switch IC are functioning normally, the multimeter results are typically similar to those shown in Table 9, while in the case of damage to either of the components, an OL reading is displayed. In the case of an OL, the connector and the USB Switch IC (designated as U6300 in iPhone 11, and U9300 in iPhone 13 Pro and 14 Pro, U9500 in iPhone 15 Pro) should be respectively inspected before replacement.

5. Conclusion

Although there are numerous tools and resources available for repairing iPhones in relation to panic-full issues, no prior research has addressed their causes and solutions from a digital forensic perspective. This study presents the first digital forensic-focused diagnostic and recovery methodology to address panic-full issue on iPhone for data extraction. The experimental findings reveal that not all modules connected to the logic board are related to a panic-full event and that there is a common subset of essential modules that consistently trigger the issue. Based on this discovery, this study reconstructed panic-full phenomena resulting from iPhone hardware damage and collected related logs. By comparing the experimental findings to the publicly available data, the reliability of the diagnostic information accessible by forensic analysts has been improved. From a digital forensic perspective, this research aimed to determine the minimal hardware combination necessary for data acquisition, which is the ultimate objective of hardware recovery. It provides a list of essential modules required for proper operation per model and highlights cases in which reassembly of the stacked logic boards after separation is not necessary. This paper went beyond simple replacement of damaged modules and sought solutions for damage to connectors and critical components on the logic board, which are commonly found in actual forensic cases. Specifically, for USB and proximity sensor modules, this paper identified the circuit paths and components responsible for triggering panic-full conditions. Furthermore, jumper points that can be used to create bypass paths were suggested for practical usage. Based on these insights, this study proposed an improved physical recovery process for iPhones experiencing panic-full issue. This allows forensic practitioners to pursue cost-effective recovery options before considering high-risk and technically demanding procedures such as chip transplantation. This study did not cover all existing iPhone models and focused solely on hardware damage related to panic-full phenomena. Nevertheless, unlike the Android ecosystem — where a wide variety of hardware manufacturers exist — iPhones operate within a unified hardware ecosystem. Therefore, the findings of this study, along with the proposed diagnostic methodology for hardware damage, can be readily extended to other iPhone models. Future work may broaden this research to encompass a wider variety of devices and explore panic-full cases caused by software-level failures, such as firmware corruption or kernel crashes.

References

8ksecresearch, 2021. Analyzing ios kernel panic logs. https://8ksec.io/analyzing-kernel-panic-ios.

Aimon, U.. How to fix “your iphone was restarted because of a problem”. https://www.macobserver.com/tips/fix-your-iphone-was-restarted-because-of-a-problem.

Apple, b. Protecting keys with the secure enclave. https://developer.apple.com/documentation/security/protecting-keys-with-the-secure-enclave.

Apple, a. Acquiring crash reports and diagnostic logs. https://developer.apple.com/documentation/xcode/acquiring-crash-reports-and-diagnostic-logs.

Belkasoft, 2002. Knowledgec database forensics: a comprehensive guide. https://belkasoft.com/knowledgec-database-forensics-with-belkasoft.

Blackman, D., 2015. Mobile Device Damage and the Challenges to the Modern Investigator. SRI Security Research Institute, Edith Cowan University, Perth, Western.

Breeuwsma, M., De Jongh, M., Klaver, C., Van Der Knijff, R., Roeloffs, M., 2007. Forensic data recovery from flash memory. Small Scale Digital Device Forensics Journal 1, 1–17.

Edwards, S., 2017. Logs unite! forensic analysis of apple unified logs. https://github.com/mac4n6/Presentations/blob/master/LogsUnite!-ForensicAnalysisofAppleUnifiedLogs/LogsUnite.pdf.

Edwards, S., 2018a. Knowledge is power ii – a day in the life of my iphone using knowledgec.db. https://www.mac4n6.com/blog/2018/9/12/knowledge-is-pow.
Edwards, S., 2018b. Knowledge is power! using the macos/ios knowledgec.db database to determine precise user and application usage. http://www.mac4n6.com/blog/2018/8/5/knowledge-is-power-using-the-knowledgecdb-database-on-macos-and-ios-to-determine-precise-user-and-application-usage.
Epifani, M., Leong, A., Mahalik, H., 2019. Using apple bug reporting for forensic purposes. www.for585.com/sysdiagnose.
FLUKE, 2024. How to test diodes with a digital multimeter. https://www.fluke.com/en/learn/blog/digital-multimeters/how-to-test-diodes.
Fukami, A., Nishimura, K., 2019. Forensic analysis of water damaged mobile devices. Digit. Invest. 29, S71–S79.
Geier, M.J., 2011. How to Diagnose and Fix Everything Electronic. McGraw-Hill/TAB Electronics.
Heckmann, T., Markantonakis, K., Naccache, D., Souvignet, T., 2018. Forensic smartphone analysis using adhesives: transplantation of package on package components. Digit. Invest. 26, 29–39.
Holcomb, A., 2022. Reviewing macos unified logs. https://www.mandiant.com/resources/blog/reviewing-macos-unified-logs.
iDevice Panic Log Analyzer, 2020. Idevice panic log analyzer. https://github.com/waynebonc/iDeviceLogAnalyzer-public.
IFIXIT, 2017. iphone x teardown. https://www.ifixit.com/Teardown/iPhone+X+Teardown/98975.
IFIXIT, 2024. Iphone kernel panics. https://www.ifixit.com/Wiki/iPhone_Kernel_Panics.
Kumar, A., Ghode, B., Maniar, K., Jain, S.K., 2021. Forensic analysis of broken and damaged mobile phone - a crime case study. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) 7, 481–487.
Libimobiledevice, 2020. Libimobiledevice 1.3.0. https://libimobiledevice.org/.
Lorenz, S., Stinehour, S., Chennamaneni, A., Subhani, A.B., Torre, D., 2023. Iot forensic analysis: a family of experiments with amazon echo devices. Forensic Sci. Int.: Digit. Invest. 45, 301541.
Paolomatarazzo, Novosadkry, Vinaypamnani-msft, 2025. Bitlocker overview. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker.
PCMAG, 2017. Apple's iphone x packs in a super dense logic board. https://www.pcmag.com/news/apples-iphone-x-packs-in-a-super-dense-logic-board.
Schuetz, D., 2014. A (Not So) Quick Primer on Ios Encryption.
Scientiamobile, 2024. Mobile overview report Jan - july 2024. https://scientiamobile.com/movr-mobile-overview-report/.
Solodov, D., Solodov, I., 2021. Data recovery in a case of fire-damaged hard disk drives and solid-state drives. Forensic Sci. Int.: Report 3, 100199.
Thomas-Brans, F., Heckmann, T., Markantonakis, K., Sauveron, D., 2022. New diagnostic forensic protocol for damaged secure digital memory cards. IEEE Access 10, 33742–33757.
Veracrypt, 2016. What does veracrypt bring to you? https://www.veracrypt.fr/en/Home.html.
Vishnoi, A., Sapra, V., 2024. Data recovery from water-damaged android phones. In: Cyber Forensics and Investigation on Smart Devices. Bentham Science Publishers, pp. 92–117.
Whiffin, I., 2019. Knowledgec (and friends). https://www.doubleblak.com/blogPost.php?k=knowledgec.
Whiffin, I., 2023. Knowledgec complete(ish). https://www.doubleblak.com/blogPost.php?k=knowledgec2.
Wiki, R., 2023a. How to fix an iphone 14 pro that randomly restarts. https://repair.wiki/w/How_To_Fix_an_iPhone_14_Pro_That_Randomly_Restarts.
Wiki, R., 2023b. How to troubleshoot and fix iphone random restarts using panic logs. https://repair.wiki/w/How_to_Troubleshoot_And_Fix_iPhone_Random_Restarts_Using_Panic_Logs.
Zobnin, E., 2015. Android privacy: a brief history from version 1.0 to 11. https://hackmag.com/mobile/android-privacy-history.