Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

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

DFRWS USA 2025 - Selected Papers from the 25th Annual Digital Forensics Research Conference USA

Forensic recovery via chip-transplantation in samsung smartphones

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

[a] Sungkyunkwan University, Department of Forensic Science, 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:
Damaged device forensics
Chip-transplantation
eSE(embedded secure element)
Anti-forensic
Physical recovery

ABSTRACT

The advancement of mobile forensic technology has induced the increase of anti-forensic activities such as smartphone destruction, while prompting major manufacturers to strengthen their data encryption policies at the same time. Such changes resulted in forensic analysts having to perform 'Chip-transplantation' when extracting data from damaged smartphones. Chip-transplantation is a method referring to transplanting data storage and decryption modules from the original damaged device to a compatible device of same model. However, chip-transplantation consists of procedures such as chip-off which are risky in terms of data integrity, and require comprehensive understanding of the target device's hardware for a successful recovery. This study explores the improvements to chip-transplantation techniques that are compatible with Samsung's premium smartphone's AP and eSE modules. Experimental results indicate that for a successful data acquisition via Chip-Transplantation on Samsung smartphones, transplantation of the eSE module along with the AP and flash memory is required irrespective of user password settings. As there is a lack of research on the physical structure and PCB placement of the eSE, this study provides eSE's terminal information, PCB placement, and jump points to bypass damage to PCB pin terminals. Lastly, for cases where damage to AP or eSE modules is suspected prior to or after transplantation, this study suggests two less invasive and cost-effective diagnostic methods – smartphone log analysis during the boot process and current consumption pattern analysis – that can be used along with conventional continuity testing, thermal imaging, and X-ray analysis. As the adoption of dedicated encryption modules in smartphones grows with privacy protection schemes, this study will contribute to advancing the chip-transplantation success rate against ever-evolving hardware landscape.

1. Introduction

With the advancement of demand for mobile forensics and relevant technologies, anti-forensic activities, such as intentional damaging of smartphones by suspects in an attempt to conceal data, have also increased. Smartphone user data is stored in flash memory, and forensic analysts have conventionally used chip-off technique to extract data from damaged or waterlogged devices. Chip-off technique involves physically separating the memory chip from the damaged printed circuit board (PCB) and extracting the data using a specialized reader (Ayers et al., 2014; Breeuwsma et al., 2007) However, with the introduction of Android 10, Google has mandated file-based encryption (FBE) to enhance user data security (Google, 2024a), rendering conventional chip-off technique ineffective for data recovery. Consequently, forensic analysts are increasingly required to repair damaged devices or, if repair is not feasible, perform chip-transplantation. Chip-transplantation refers to methods of separating decryption modules of damaged devices and transplanting them on the PCB of an identical model (Heckmann et al., 2018). As the degree of module integration in smartphones increases, the complications for chip-transplantation also grow, along with the likelihood of failed data acquisition due to module damages incurred during the process. To improve the success rate of this technique, it is essential to identify hardware modules associated with data encryption, as well as accurately assess modules' conditions to minimize unnecessary physical impact during the procedure. A comprehensive understanding of the physical characteristics of the target device is also crucial. As of 2024, Samsung dominates approximately 23 % of the global smartphone market, and is the largest Android manufacturer by market share (Statcounter, 2024). Premium Samsung smartphone models differ from mid/low-range models in that their application processor (AP) and low-power double data rate (LPDDR) memory are configured in a Package-on-Package (PoP) structure. Additionally, since

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

https://doi.org/10.1016/j.fsidi.2025.301926

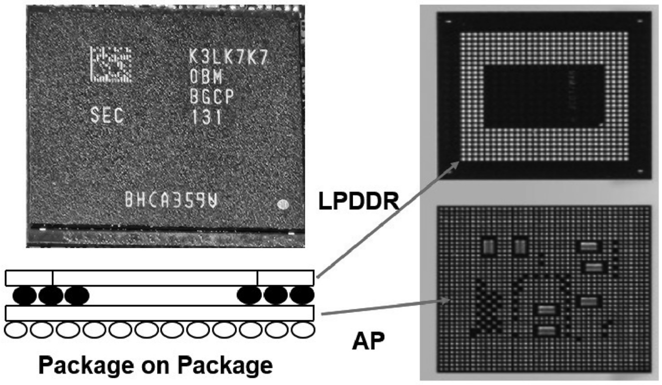


Fig. 1. Structure within package on package.

Galaxy S21 (SM-G991), Samsung introduced the embedded secure element (eSE), a dedicated encryption module, in its premium models.

This study examines potential improvements to existing physical recovery techniques, reflecting the hardware characteristics of recent Samsung premium smartphones. The findings confirm that successful data extraction via chip-transplantation requires the transplantation of the eSE module in addition to the AP and flash memory modules, regardless of user password settings. As there is a lack of prior research on the physical configuration and PCB placement of the eSE, this study provides information on the eSE terminals, and PCB placement, as well as the feasibility of creating jumper points to bypass damaged PCB pins. Lastly, this study proposes two cost-effective diagnostic methods—analyzing smartphone logs during the boot process and examining current consumption patterns—which can be adopted by forensic analysts who suspect damage to the AP or eSE modules during or after transplantation. Recent reinforcements in data privacy policies led to major Android manufacturers such as Google and Huawei adopting encryption modules similar to Samsung's eSE (Android Developers Blog, 2018; WIoT Group, 2024). This study aims to contribute to improving the success rate of chip-transplantation in response to the evolving hardware landscape.

2. Literature review

2.1. Background

PoP is a semiconductor packaging technology distinct from system on chip (SoC), which integrates system components into a single integrated circuit. As shown in Fig. 1, PoP involves stacking one package vertically on top of another. This method allows for the independent development and testing of each system component, reducing overall development time, optimizing space utilization, and improving electrical performance due to shorter interconnect distances between chips. PoP is widely employed in electronic devices such as smartphones.

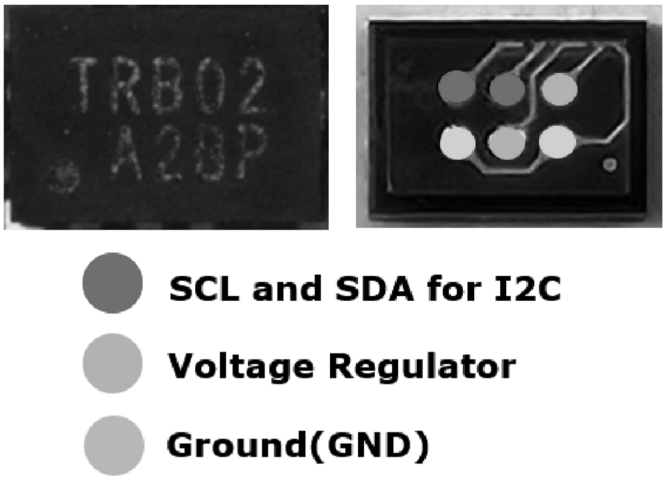
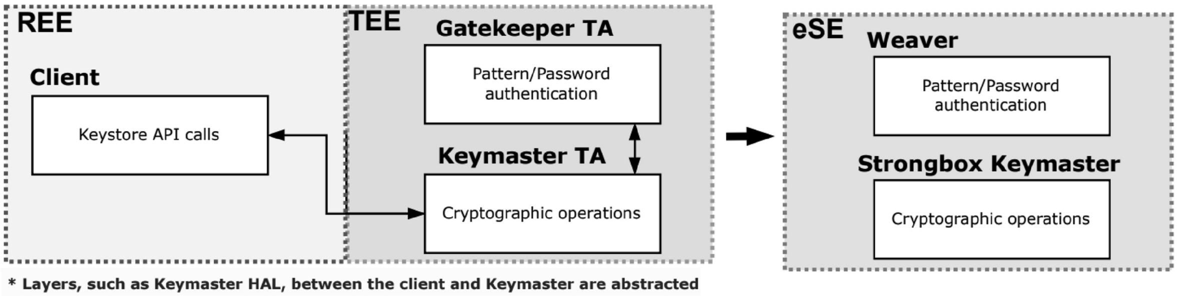


Fig. 3. Samsung eSE (S3K250AF) hardware information.

A trusted execution environment (TEE) is an isolated security region within a central processing unit (CPU), and operates as a sandbox environment which ensures the confidentiality and integrity of sensitive data and executable code (Intel, 2024). The exterior region of TEE, referred to as rich execution environment (REE), is where general operating systems and applications run. Within the TEE, there is a Trusted OS and trusted applications (TAs) that are isolated from REE. This isolation ensures that even if the REE OS is compromised through vulnerabilities, sensitive data within the TEE remains protected as external processes can not directly access TEE. TEE implementations are often supported by specialized hardware, with ARM's TrustZone being a prominent example (Li et al., 2019). Since version 5.0, Android has supported hardware-based encryption, such as TrustZone, and utilized it for encryption key generation and user authentication. Key TAs responsible for encryption tasks include Gatekeeper, which performs device password authentication and issues authentication tokens, and Keymaster, which implements Android Keystore. Keymaster is responsible for generating, encrypting, and decrypting keys using a hardware encryption engine. These applications operate within a TEE, ensuring the integrity and confidentiality of data from external interference (Google, 2024b). As shown in Fig. 2, Keymaster processes cryptographic tasks, including keystore API calls from the REE client and Gatekeeper authentication. Secure element (SE) is a tamper-resistant hardware (TRH) designed to securely execute applications and process encrypted data. SEs are categorized into detachable types, such as universal integrated circuit cards (UICCs), and embedded types, such as eSE. Android started to support eSE from version 9.0. In devices equipped with eSE, the conventional roles of Gatekeeper and Keymaster have been replaced by Weaver and StrongBox Keymaster that resides in a eSE (Google, 2024b; Mayrhofer et al., 2021; Bellom and Melotti, 2023). Fig. 3 shows the eSE module of the Samsung smartphone S3K250AF (Samsung, 2020). It is equipped with ARM's SecurCore SC000 and supports inter-integrated circuit (I2C) communication. The module consists of six



* Layers, such as Keymaster HAL, between the client and Keymaster are abstracted

Fig. 2. Hardware-based encryption module of Android: TEE and eSE.

pins: two pins for serial clock line (SCL) and serial data line (SDA) for I2C, two voltage regulator (VREG) pins, and two ground (GRD) pins.

To extract data from damaged mobile devices, forensic analysts conventionally rely on chip-off technique, which involves detaching storage media (e.g. flash memory) from the PCB and extracting data using a specialized reader. However, as previously mentioned, with the expansion of hardware-based encryption, the acquisition of user data without the support of decryption hardware (e.g. AP) has become impossible. Consequently, forensic analysts now repair damaged modules or, in cases where repair is not feasible, perform chip-transplantation of storage media and decryption-relevant modules.

2.2. Related work

Research on the forensic recovery of damaged digital devices has been actively conducted, with emphasis on diagnosis of damaged modules, chip-off techniques to separate functioning modules from PCBs, and transplantation methods to mount modules onto new PCB. As an early study on physical recovery, Sobey (2004) applied transplantation techniques to hard drive recovery. The method involved transferring non-volatile memory chips from damaged drives to functioning PCBs (donor PCBs) of the same model to attempt data recovery. Breeuwsma et al. (2007) studied data recovery of flash memory of mobile devices. The researchers explored the logical structure of data storage and its physical interfaces, and proposed techniques including utilization of Flasher Tools and joint test action group (JTAG) debug ports, chip-off methods via heating, as well as methods for file system analysis of the extracted data.

Subsequent research aimed to improve the reliability of invasive techniques like chip-off and transplantation of chips to a new PCB followed suit. Heckmann et al. (2016) utilized 42Sn/58Bi solder paste, which melts at 138 °C, for the reballing procedure, to reduce the risk of damage caused by high-temperature heat during the Chip-off/Chip-on process. Fukami et al. (2017) analyzed errors caused by charge leakage in NAND flash memory, demonstrating that high temperatures during heat-based chip-off significantly accelerated charge leakage, leading to increased errors by up to 259 times. To reduce such difficulties, the researchers proposed a ‘read-retry’(read reference voltage control) mechanism, which reduced error rates by 94.6 % and successfully recovered stored data. Heckmann et al. (2018) provided a novel recovery method through transplantation, involving the removal and resoldering of intact NAND memory, SoC, and encryption chips onto donor boards for rebooting. To address potential destruction caused by misalignment of PoP components during chip-off, the study introduced a new chip-off analysis method based on high-temperature thixotropic thermal conductive adhesives (HTTTCA) for bonding PoP packages. Fukami and Nishimura (2019) submerged multiple smartphones in water for 72 h, and examined the physical and electrical condition of the PCB. Water exposure led to metal corrosion, including electrochemical migration (ECM) and galvanic corrosion, and resulted in short circuits within the devices. To repair the damaged devices, the authors performed PCB cleaning and replacement of ICs where short circuits had occurred. Kumar et al. (2021) deliberately damaged a Samsung Galaxy Note 10+ and transplanted the motherboard to a new screen assembly, resulting in a successful recovery. Solodov and Solodov (2021) tackled the challenge of recovering data from burnt HDDs, where plastic debris had melted onto PCBs. For cases with minimal damage, they replaced the PCB with one from an identical model and transferred the ROM chip to the new PCB. This enabled successful access to the ROM chip and driver software within the service area. Thomas-Brans et al. (2022) proposed a combination of diagnostic methods for data extraction from damaged secure digital (SD) memory cards. The methods include non-invasive measures such as visual inspection, X-ray imaging, thermal imaging, as well as more invasive measures, such as multimeter scanning of microcontrollers and memory dies, infrared heat detection.They also suggested an improved forensic protocol to minimize additional damage during diagnosis.

Table 1
Hardware features of Samsung premium smartphones.

Year of Release	Model Name	eSE Adoption	PoP Package
2024	SM-F741N, SM-F956N, SM-S928N, SM-S926N, SM-S921N	Yes	Yes
2023	SM-F731N, SM-F946N, SM-S918N, SM-S916N, SM-S911N	Yes	Yes
2022	SM-F721N, SM-F936N, SM-S908N, SM-S906N, SM-S901N	Yes	Yes
2021	SM-F711N, SM-F926N, SM-G998N, SM-G996N, SM-G991N	Yes	Yes
2020	SM-N986N, SM-N981N, SM-G988N, SM-G986N, SM-G981N	No	Yes
2019	SM-G977N, SM-N971N, SM-N976N	No	Yes

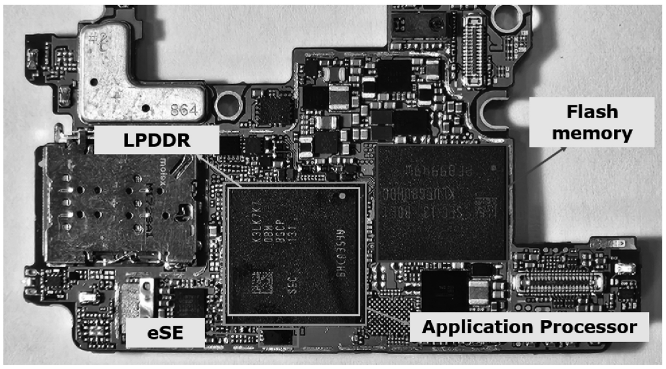


Fig. 4. Hardware elements of Samsung smartphone.

In addition, there have been many studies on the physical and software vulnerabilities of security hardware. Saβ et al. (2023) focused on voltage fault injection (VFI) attacks, particularly on how to bypass the security of ARM TrustZone-M. It introduces the μ-Glitch platform, which is the first VFI platform capable of injecting multiple, calibrated voltage faults using a single trigger signal. The paper demonstrates μ-Glitch successfully compromises TrustZone-M to access secure memory. Mahmod and Hicks (2024) studied on ‘SDRAM aging attack’ that typically involve stressing the SDRAM’s memory cells under conditions of high temperature and high voltage, aiming to increase bit errors and shorten the device’s lifespan. They used it to demonstrate reveals an AES key protected by TrustZone with up to 98 % accuracy. Navanesan et al. (2024) applied electromagnetic side-channel analysis (EM-SCA) to analyze encryption keys and operations by studying electromagnetic emissions. By training machine learning and deep learning models on the signals, the study achieved high accuracy in information extraction. However, performance significantly declined when tested on devices differing from the training set. Despite these limitations, the study demonstrated the potential for applying signal-based analysis across devices of the same model, suggesting possibilities for broader applications in forensic contexts. Alendal et al. (2018) analyzed Samsung’s secure boot and common criteria (CC) mode, and present methods to circumvent these security features for forensic data acquisition. CC mode is a security feature that enhances the security level of Samsung devices by restricting access to the firmware update mechanism. The authors analyzed Secure Boot and identified security vulnerabilities in CC mode and demonstrated how to exploit these vulnerabilities to enable data collection. Alendal et al. (2021) explored loopholes in eSE modules, by exploiting zero-day vulnerabilities through logical interfaces, demonstrating the potential for remote attacks and data acquisition. The findings highlighted risks that even in limited circumstances, attacks can be made with ease. Research on the security of smartphone encryption devices has also emerged, including studies

Table 2
Overview of experiment scenarios.

No.	Scenario	Summary
1	eSE Module Damage (Pattern Set)	Remove eSE module and verify operation with pattern lock.
2	eSE Module Damage (Pattern Unset)	Remove eSE module and verify operation without pattern lock.
3	eSE Module Replacement	Replace damaged eSE module with a new or existing module.
4	AP Damage (RAM Normal)	Verify operation with damaged AP and functional RAM.
5	RAM Damage (AP Normal)	Verify operation with damaged RAM and functional AP.
6	RAM Replacement	Replace damaged RAM and verify operation.

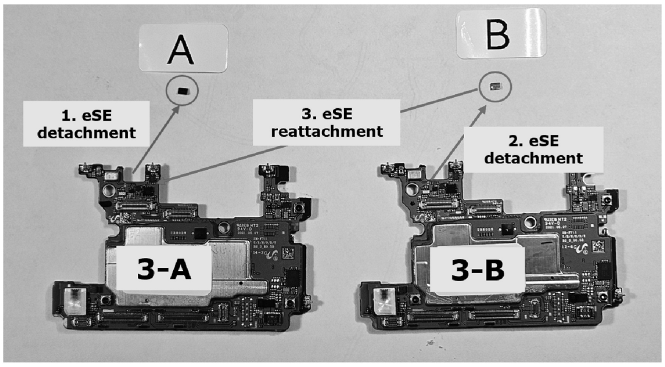


Fig. 5. Processes taken in Scenario 3.

based on their physical characteristics.

3. Experiment design

3.1. Objectives and design

This study aims to identify improvements to the chip-transplantation technique by taking into account the hardware characteristics of recent Samsung premium smartphones. Table 1 is the summary of the hardware features of premium Samsung smartphones released in South Korea between 2019 and 2024. As depicted in Fig. 4, Samsung's premium smartphones feature a PoP structure in which the AP and LPDDR memory are stacked. The eSE modules have also been adopted in models released since 2021. Reflecting the above hardware characteristics, this paper assumes physical damage to the device and AP/eSE modules due to intentional destruction or external impacts, and outlines 6 experimental scenarios as in Table 2.

Scenario 1 assumes that damage has been done to the smartphone's eSE module. The smartphone was first pattern-locked, and then its eSE module was removed from the PCB to simulate the damage. After supplying power, the smartphone was checked for normal operation and its diagnostic log data were collected. Scenario 2 assumes identical conditions as Scenario 1, except for the security setting conditions (no pattern lock).

Scenario 3 aims to determine whether a damaged eSE module can be replaced with eSE module from the same smartphone model for forensic recovery. As depicted Fig. 5, Two smartphones (3-A and 3-B) of the same model were prepared, both set with identical passwords, and the eSE module of 3-A was removed to simulate damage. Then, the eSE module of 3-B was detached and reattached to 3-A and the smartphone was tested for operation.

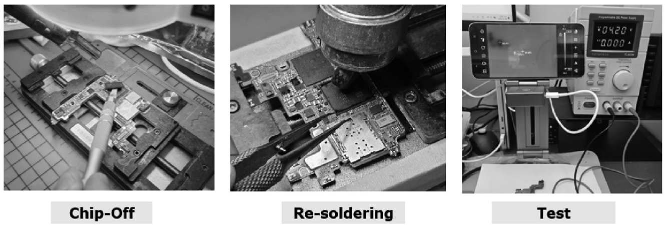


Fig. 6. Common process for test scenarios.

Scenarios 4 and 5 assume that damage has been done to the PoP-structured APs. Either the AP or RAM of the PoP structure can be subjected to damage. Scenario 4 assumes that damage has been done to AP, whereas Scenario 5 assumes that damage has been done to RAM. To simulate each condition, AP and RAM were first disassembled, and only AP (Scenario 4) or RAM (Scenario 5) was heated for damage. Then the AP and RAM were reassembled for testing.

In Scenario 6, damaged RAM of the PoP module from Scenario 5 was removed, and after verification of current, heat, and operation, a new non-damaged RAM was reassembled with the AP for testing.

This study did not cover the processing of flash memory, as prior research (Breeuwsma et al., 2007; Fukami et al., 2017) has already been made. Also power management integrated circuit (PMIC) damage due to waterlogging has been excluded from the scenario, since such damage is irrelevant to user data encryption despite its frequent occurrence.

3.2. Target devices and tools

Two Samsung smartphones equipped with eSE modules and PoP-packaged APs, Galaxy Z Flip3 (SM-F711N) and Galaxy S21 Ultra (SM-G998N), have been selected as the target devices. A hot air rework station to detach modules on PCB, a power supply to provide power to damaged PCBs, and a thermal imaging camera to monitor heat during operation as in Table 3.

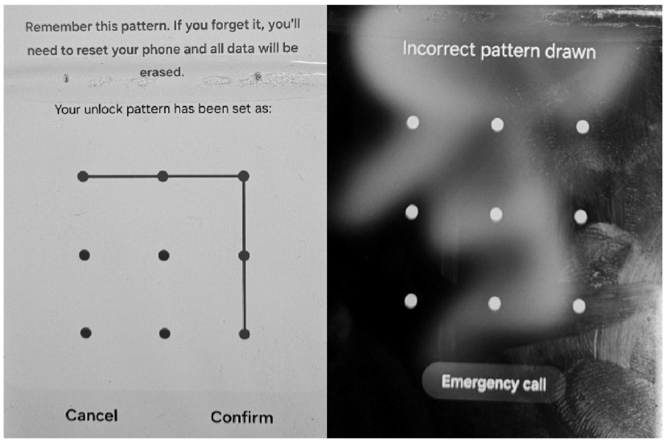
3.3. Experiment process

The following outlines general chip-transplantation process: (1) identification of modules to be transplanted (2) chip-off process to detach modules (3) cleaning up and reballing of detached modules (4) resoldering modules to a new PCB (5) verifying operation. Module detachment, reattachment, and testing after power application processes, as shown in Fig. 6 are identical in all scenarios of chip-transplantation.

For the detachment and reattachment of the modules, the hot air station was set to 360 °C with airflow. Power supply to the main PCB battery terminal was set at 4.2V DC. Current consumption was recorded every 0.5 s using the power supply's readings. If the PCB module is damaged, the USB connection is also disabled. As a result, accessing and

Table 3
Target devices and Tools (Software).

Type	Manufacturer	Model	OS Version	Quantity	Purpose
Smartphone	Samsung	SM-F711N	Android 14	3	eSE Scenario
Smartphone	Samsung	SM-G998N	Android 13	3	AP Scenario
Power supply	Toyotech	TL503N	–	1	PCB Current Measurement
Thermal Camera	MA ANT	RC-3	–	1	PCB Temperature Measurement
Hot Air Rework	HAKO	FR-810B	–	1	Chip-Off

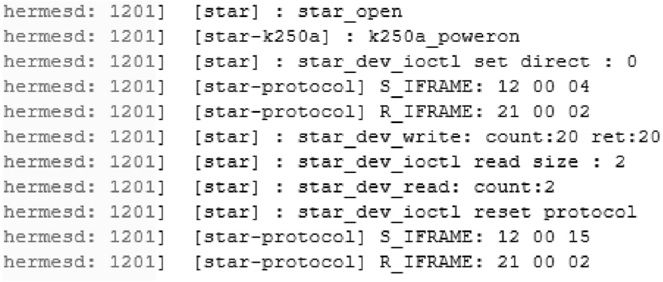


Remember this pattern. If you forget it, you'll need to reset your phone and all data will be erased.

Your unlock pattern has been set as:

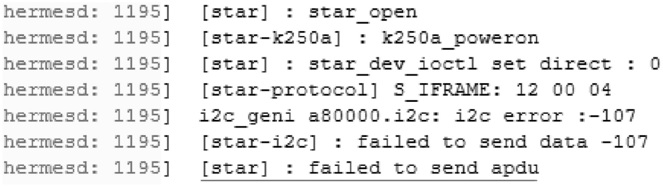
Incorrect pattern drawn

Fig. 7. Screen lock test of Scenario 1.



```
hermesd: 1201]  [star] : star_open
hermesd: 1201]  [star-k250a] : k250a_poweron
hermesd: 1201]  [star] : star_dev_ioctl set direct : 0
hermesd: 1201]  [star-protocol] S_IFRAME: 12 00 04
hermesd: 1201]  [star-protocol] R_IFRAME: 21 00 02
hermesd: 1201]  [star] : star_dev_write: count:20 ret:20
hermesd: 1201]  [star] : star_dev_ioctl read size : 2
hermesd: 1201]  [star] : star_dev_read: count:2
hermesd: 1201]  [star] : star_dev_ioctl reset protocol
hermesd: 1201]  [star-protocol] S_IFRAME: 12 00 15
hermesd: 1201]  [star-protocol] R_IFRAME: 21 00 02
```

Fig. 8. Result of diagnostic log analysis of a normal device.



```
hermesd: 1195]  [star] : star_open
hermesd: 1195]  [star-k250a] : k250a_poweron
hermesd: 1195]  [star] : star_dev_ioctl set direct : 0
hermesd: 1195]  [star-protocol] S_IFRAME: 12 00 04
hermesd: 1195]  i2c_geni a80000.i2c: i2c error :-107
hermesd: 1195]  [star-i2c] : failed to send data -107
hermesd: 1195]  [star] : failed to send apdu
```

Fig. 9. Result of diagnostic log analysis of Scenario 1.

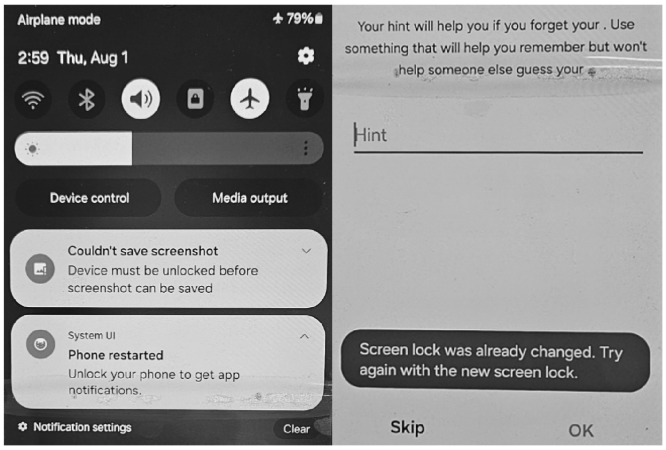
extracting stored data through the manufacturer's backup program is no longer possible. In such cases, Samsung Upload Client (Arsenij, 2023) was utilized to extract diagnostic logs from malfunctioning smartphones.

4. Results

4.1. eSE module damage

In Scenario 1 (simulated eSE module damage with pattern-locked condition), the smartphone successfully booted up to the lock screen. However, it was unable to unlock the device using the pre-configured pattern input. Additionally, no increase in delay time due to repeated pattern authentication attempts was observed as in Fig. 7. However, if the user exceeds the predefined limit for failed unlock attempts, the device becomes permanently locked.

To determine whether the defect of the eSE module could be diagnosed without any physical damage to the PCB, RAM dump logs were collected and analyzed using Samsung Upload Client. Alendal et al. (2021) shows that 'hermesd', an Android service process, communicates with '/dev/k250a', a logical device of eSE module, utilizing application protocol data unit (APDU). The key library of 'hermesd' related to this communication is 'libese-grdg.so'. To check for diagnostic logs depending on the eSE module damage, this research compared the state of 'hermesd' logs collected from a functioning smartphone to logs collected from Scenario 1–3.



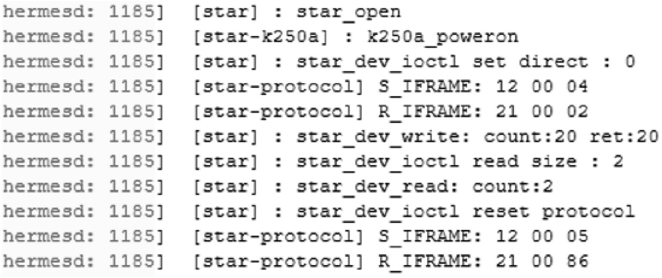
Couldn't save screenshot
Device must be unlocked before screenshot can be saved

System UI
Phone restarted
Unlock your phone to get app notifications.

Your hint will help you if you forget your . Use something that will help you remember but won't help someone else guess your

Screen lock was already changed. Try again with the new screen lock.

Fig. 10. Screen lock test of Scenario 2.



```
hermesd: 1185]  [star] : star_open
hermesd: 1185]  [star-k250a] : k250a_poweron
hermesd: 1185]  [star] : star_dev_ioctl set direct : 0
hermesd: 1185]  [star-protocol] S_IFRAME: 12 00 04
hermesd: 1185]  [star-protocol] R_IFRAME: 21 00 02
hermesd: 1185]  [star] : star_dev_write: count:20 ret:20
hermesd: 1185]  [star] : star_dev_ioctl read size : 2
hermesd: 1185]  [star] : star_dev_read: count:2
hermesd: 1185]  [star] : star_dev_ioctl reset protocol
hermesd: 1185]  [star-protocol] S_IFRAME: 12 00 05
hermesd: 1185]  [star-protocol] R_IFRAME: 21 00 86
```

Fig. 11. Result of diagnostic log analysis of Scenario 3.

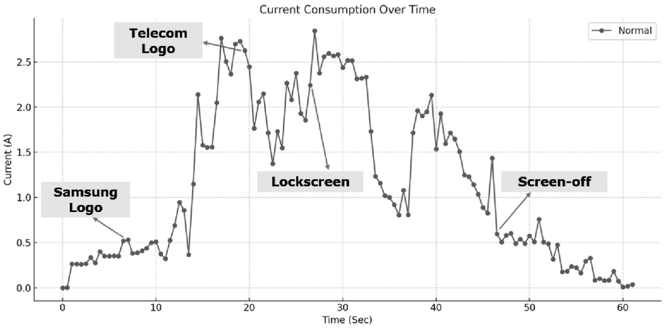


Fig. 12. Current consumption of a functioning PCB.

Among the data collected with Samsung Upload Client, 'ap_klog' has shown repeated occurrences of certain logs. Data from the functioning smartphone and and from Scenario 1 is shown in Figs. 8 and 9 respectively. As the eSE chip was removed from the PCB, it showed repeated '[star]: failed to send apdu' log, indicating a data communication error related to the eSE module.

In Scenario 2 (simulated eSE module damage without pattern-locked condition), the smartphone's screen displayed 'Phone is starting … ' message, yet no further operation was made afterwards. Unlike Scenario 1, the user could interact with the screen to access the 'Settings' menu and view device information and conditions. However, tasks related to saving data within the device, such as modifying screen lock and taking screenshots, were not doable, as shown in Fig. 10. The diagnostic logs of the device also revealed logs similar to those in Scenario 1.

The test results of Scenario 3 (simulated replacement of damaged eSE

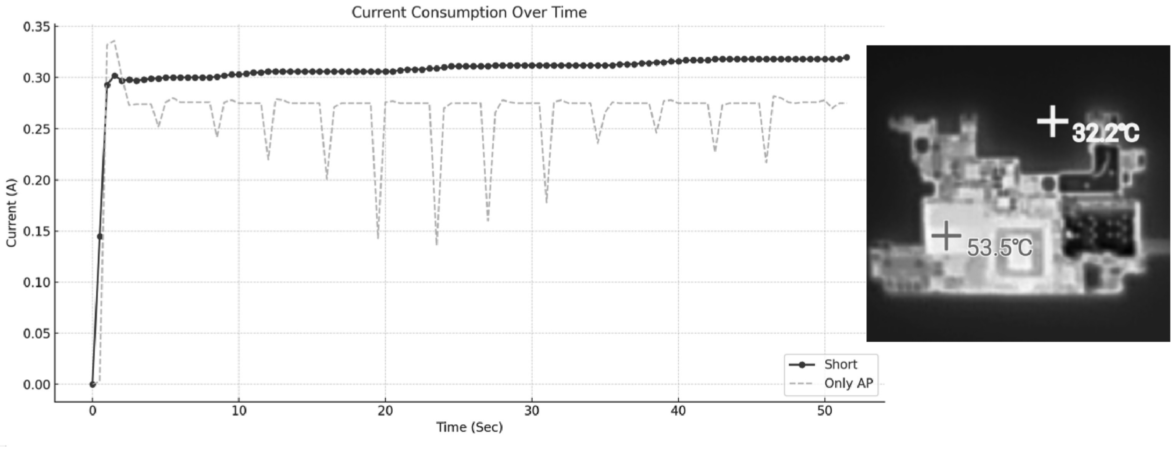
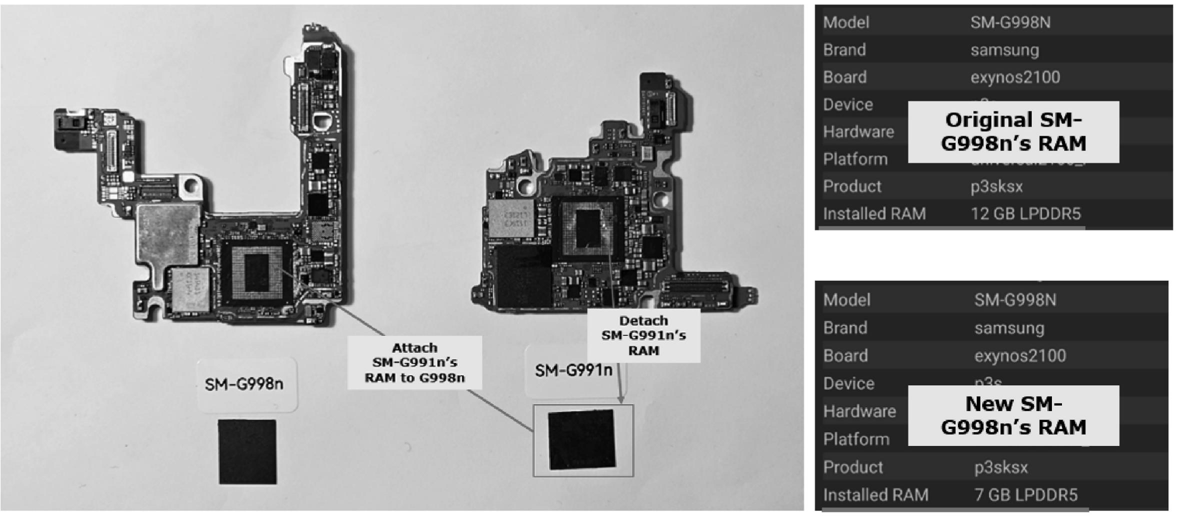


Fig. 13. Change in current consumption depending on defects and heat level.



Model	SM-G998N
Brand	samsung
Board	exynos2100
Device	
Hardware	
Platform	
Product	p3sksx
Installed RAM	12 GB LPDDR5

Model	SM-G998N
Brand	samsung
Board	exynos2100
Device	p3s
Hardware	
Platform	
Product	p3sksx
Installed RAM	7 GB LPDDR5

Fig. 14. Result of scenario 6 (reattach G991n's RAM to G998n's PCB).

module with new module) showed that although the damaged eSE module was replaced with an identical module, the pre-configured pattern lock did not unlock the screen. This has been also observed in Scenario 1. As depicted in Fig. 11, the eSE module performs normal APDU communications.

4.2. AP module damage

Fig. 12 indicates the current consumption of a functioning smartphone PCB. When power is supplied, the current consumption fluctuates between 0.2A and 2.7A, depending on the booting process. The test results for Scenario 4 (simulated AP damage) demonstrated that the current consumption stabilized within the range of 0.290A–0.318A, exhibiting a consistent waveform pattern (blue line). Thermal imaging reveals the highest temperature (53.5 °C) at the AP module as seen in Fig. 13.

Test results of Scenario 5, which used a damaged RAM module, show similar results to those of Scenario 4 (blue line), likely due to a circuit short in the AP. Test results of Scenario 6 show that when supplied with power after removing the damaged RAM from the PoP module, the AP attempts to operate but fails due to the absence of LPDDR memory. During this process the current consumption stabilizes at 0.27A, but constantly drops to below 0.25A (yellow line in Fig. 13). As the AP module is in operation, the thermal imaging shows identical results as Scenario 4. When damaged RAM is replaced with a new RAM, the target device's normal operation is confirmed as shown in Fig. 14.

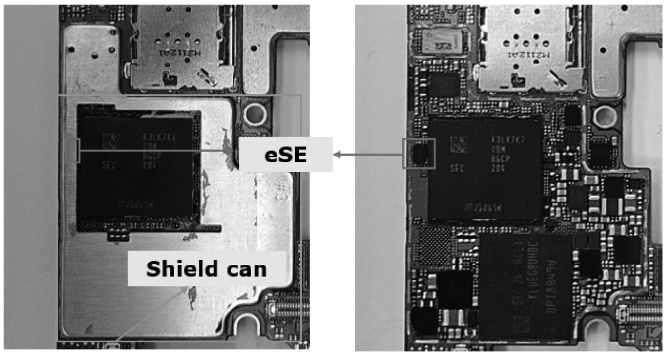


Fig. 15. eSE module placement (inside the shield can).

4.3. Information on eSE modules for physical recovery process

To increase the success rate of chip-transplantation, forensic analysts must familiarize themselves with the layout and structure of eSEs to minimize hardware damage during the process. As shown in Fig. 15, the eSE module in Samsung smartphones is located near the AP module and

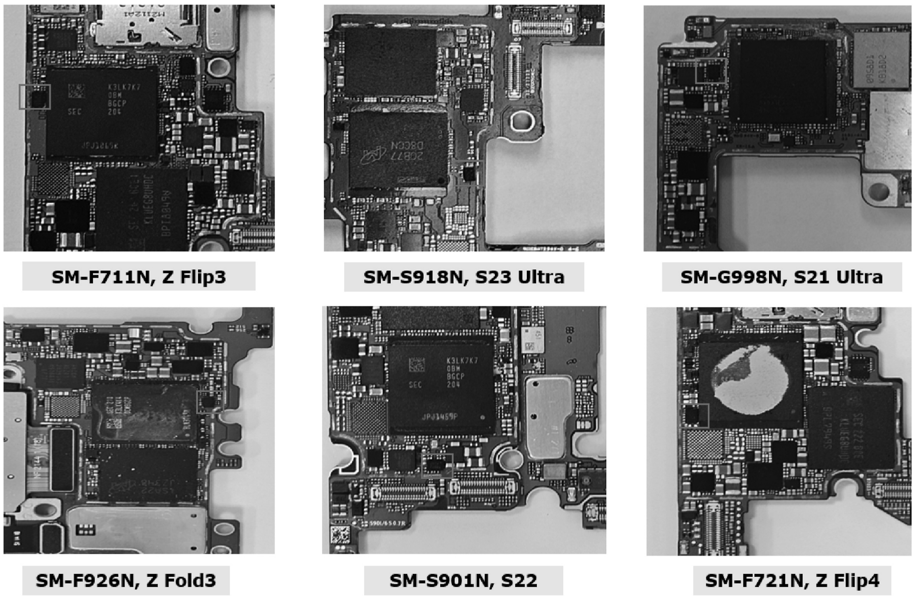


Fig. 16. eSE module placement in 6 Samsung smartphone models.

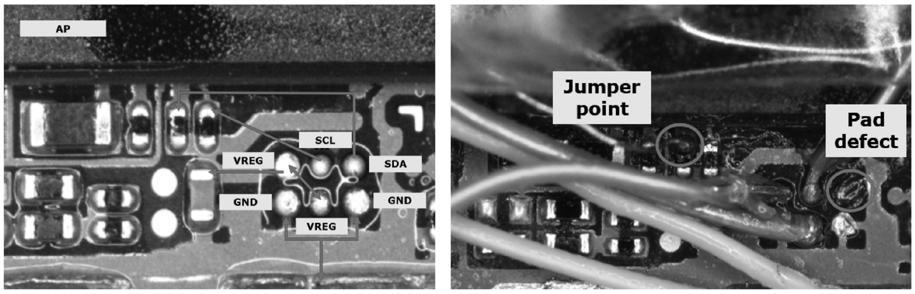


Fig. 17. Jumper points for damaged pins (left) and Reestablishing connection using a jumper point (right).

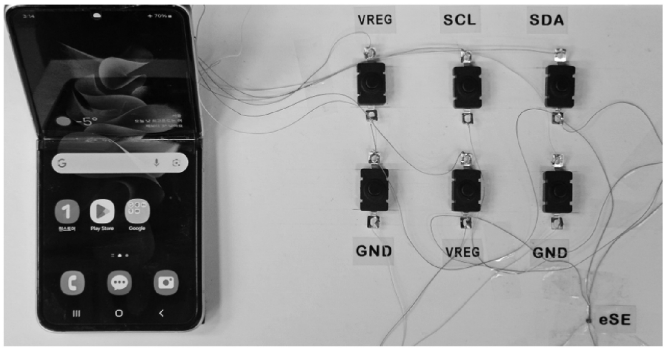


Fig. 18. eSE chip damage test.

is covered by a shield can, making identification difficult. During the physical recovery process, the ‘shield can’ should often be removed for a further process.

As the eSE module is located in the vicinity of the shield can, there is a high risk of eSE module detachment while removing the shield can. Fig. 16 provides the exact placement of eSE modules within the PCB of 6 Samsung smartphone models.

4.4. eSE pin information and strategies for damaged pins

The eSE pin information is shown in Fig. 3. The module consists of six pins: two pins for SCL and SDL for I2C, two VREG pins, and two GRD pins. Due to its size and placement, accidental damage to the lower pins and linked PCB pad can occur during the repair process. When the PCB pad linked to the eSE module is damaged, creating a bypass using the damaged PCB’s jumper point may reduce damage to hardware, compared to detaching the entire AP and Flash memory module to a new PCB. Fig. 17 shows the jumper points for each eSE pin. Reestablishing the connection between the eSE pins and the PCB restored the device functionality as in SM-F711N case.

As there are two VREG and GND pins each, this study tested for smartphone functionality depending on the damage level of each pin. As shown in Fig. 18, a switch was connected to each pin, allowing toggling during device operation. The results showed that the smartphone remained operational when one GND pin was damaged, but further damage in pins caused errors identical to that of Scenario 1.

4.5. Enhanced diagnostic procedures for AP and eSE modules

In previous studies (Fukami and Nishimura, 2019; Kumar et al., 2021; Thomas-Brans et al., 2022) on physical recovery, forensic analysts identified damaged modules using techniques such as short-circuit detection using multimeter, heat level detection using thermal imaging cameras, and X-ray analysis. However, each has certain limitations. Multimeter technique can only identify a broad area of potentially damaged modules. X-rays are costly and are insufficient in analyzing smartphones where modules are stacked. To identify soldering short circuits, the side view of the target device is required, which is difficult

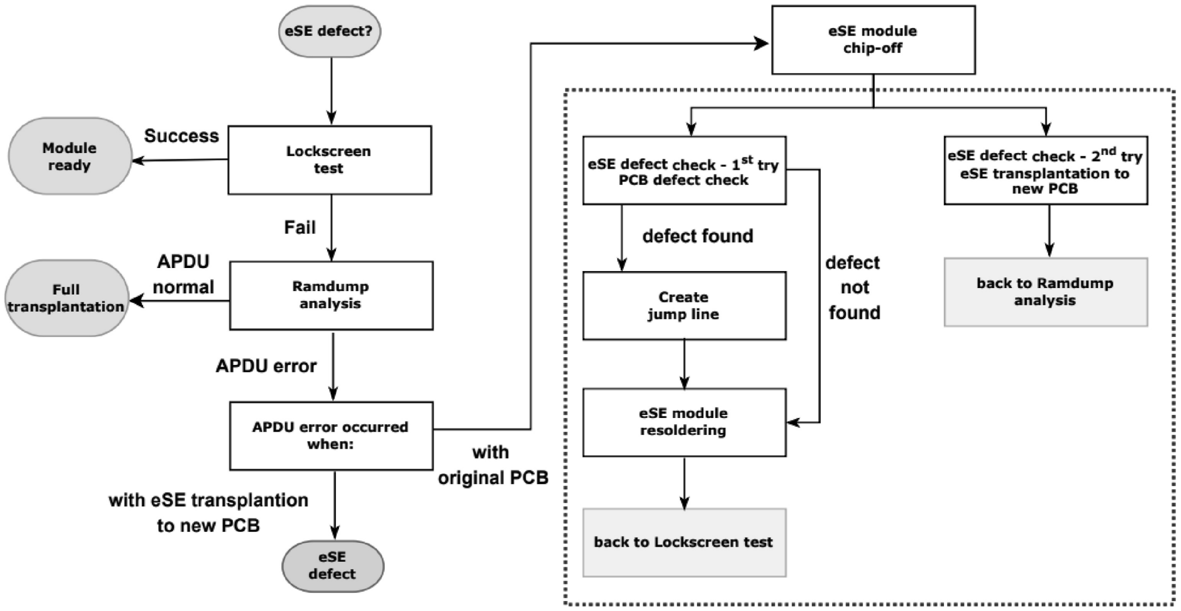


Fig. 19. Procedures to be taken when damage to the eSE module is suspected.

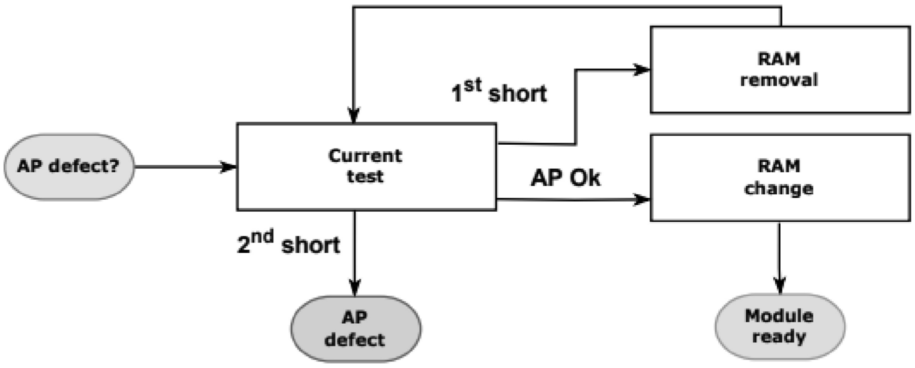


Fig. 20. Procedures to be taken when damage to the AP module is suspected.

when the target module remains mounted on the PCB. In physical recovery processes such as chip-transplantation, the removal and reattachment of modules—which carry a high risk of irreversible damage—should be minimized. Considering the physical characteristics of Samsung premium smartphones, this study proposes a novel diagnostic and physical recovery procedure that can complement existing methods. See Fig. 19.

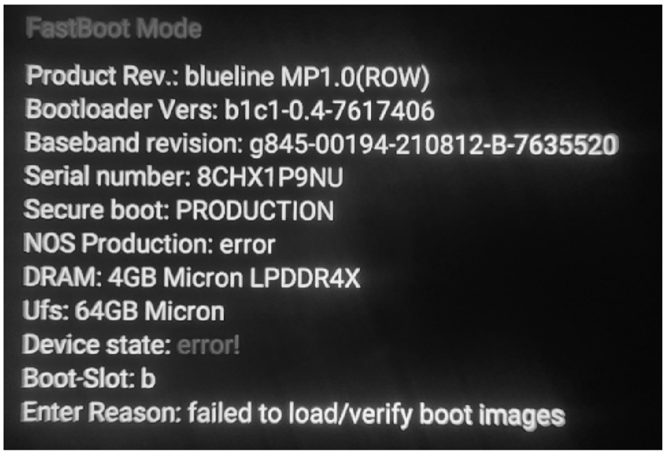
Based on the above findings, this study suggests the following diagnostic procedures for AP and eSE modules. First, if damage to the eSE module is suspected, apply power to the device and attempt to unlock the lock screen. If the device does not respond to user credentials or fails to display an error screen even when incorrect credentials are entered, it can be inferred that the issue lies with the eSE module itself or related PCB components. In such cases, diagnostic logs can be analyzed to verify whether the eSE module is defective. If a 'failed to send apdu' type error is identified in the diagnostic logs, consider performing eSE module chip-off to check for eSE chip defect. For the first attempt, inspecting the PCB for potential damage is recommended. If necessary, creating a jumper line to bypass damage is required. Then, resolder the module to the PCB and go back to the lock screen test. If the eSE defect issue persists despite these measures, transplant only the eSE module to a different PCB and analyze the diagnostic logs. If the transplanted eSE module functions well, transplant entire modules, including the AP, to a new PCB.

As shown in Fig. 20, if damage to the AP module is suspected, current consumption and thermal patterns after applying power to the device. For current patterns indicative of an AP short circuit, remove the RAM module and reanalyze the current pattern. If normal AP operation is confirmed, reattach a new RAM module from an identical model.

5. Discussion

This study aims to apply traditional forensic recovery techniques, such as chip transplanting, to Samsung's premium smartphones. Unlike devices in a previous paper Breeuwsma et al. (2007), most modern smartphones are equipped with dedicated hardware security modules, such as eSE, to encrypt stored data. However, there is a lack of research on eSE hardware information, as well as methods for diagnosing and addressing suspected physical damage to the module during the forensic recovery process. As a result, forensic analysts face challenges in identifying the cause of and providing the solutions for abnormal symptoms in Samsung smartphone acquisition, where screen unlock constantly fails despite correct input.

This study collected and analyzed the symptoms observed at the lock screen stage, when the eSE chip is damaged. Also, clues to identify eSE defects were gathered from the diagnostic logs of the smartphones. Combined findings allowed us to suggest a diagnostic procedure which will enable analysts to easily verify eSE damage while minimizing the



```
FastBoot Mode
Product Rev.: blueline MP1.0(ROW)
Bootloader Vers: b1c1-0.4-7617406
Baseband revision: g845-00194-210812-B-7635520
Serial number: 8CHX1P9NU
Secure boot: PRODUCTION
NOS Production: error
DRAM: 4GB Micron LPDDR4X
Ufs: 64GB Micron
Device state: error!
Boot-Slot: b
Enter Reason: failed to load/verify boot images
```

Fig. 21. Result of Google Pixel 3 experiment.

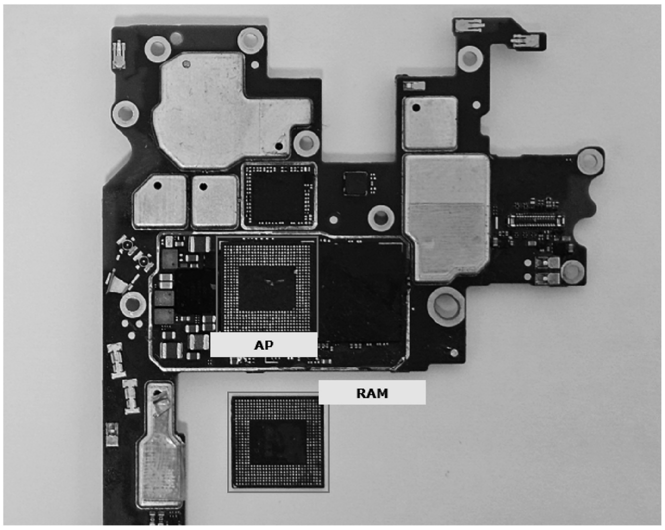


Fig. 22. Pixel 3 XL’s AP structure.

risk of physical damage during device disassembly. More specifically, to verify an eSE damage, this study discovered certain strings in diagnostic logs that are related to the eSE model name and I2C communication errors associated with the module (Scenario 1). Also, this study proposed a method to check eSE module functionality by replacing the eSE from the original smartphone to a new PCB and analyzing error messages related to Weaver (authentication component of eSE) in the collected ‘ap_klog’. As limited information is available on the diagnostic software of Samsung smartphones, this study derived its finding by comparing diagnostic logs collected from functioning devices and devices with damaged eSE modules. Further research involving other smartphone models is necessary to enhance the reliability of experimental results.

Recent smartphone manufacturers have begun integrating hardware security modules similar to eSE into their devices. For example, Google introduced the Titan M module in Pixel 3. To determine whether this diagnostic model can be applied to general hardware security models, we simulated Titan M module damage for experiment, yet as shown in Fig. 21, Pixel 3 failed to boot in the first place. This suggests that the diagnostic procedures suggested in this study are limited to Samsung smartphones.

As this study applied current consumption measurement techniques—traditionally used to detect short circuits in ICs during forensic recovery processes—to diagnose failures in PoP-based APs, it suggested that a simple removal of just the RAM module, rather than the entire AP chip itself, can be adopted to check for functionality when AP chip damage is suspected. This reduces the risk of device damage caused by high temperatures during chip-off processes. Furthermore, we confirmed that damaged RAM modules within APs could be replaced with identical RAM modules from the same model to resolve defect issues. As shown in Fig. 22, smartphone manufacturers such as Google Pixel adopt PoP-style APs. To determine whether this study’s RAM replacement technique can be applied to other smartphones with PoP-style APs, we performed the procedure on Pixel 3 XL. The model with replaced RAM functioned normally, indicating that this technique can be extended to devices provided by manufacturers other than Samsung.

6. Conclusion

This study empirically investigates novel methods for the chip-transplantation technique to enhance the success rate of physical recovery for damaged Samsung premium smartphones, considering their unique hardware characteristics. Through the research, it was confirmed that Samsung’s eSE module is a critical hardware component associated with user data encryption. Damage to this module affects the normal functioning of the smartphone and the data decryption process. The study identifies the physical placement of the eSE module, its pin configurations, and jumper points which can be utilized for creating bypasses. This information is crucial for forensic analysts who seek to minimize hardware damage during the chip-transplantation process. More importantly, beyond traditional diagnostic methods using multimeter, X-ray, and thermal camera, the study introduces diagnostic logs analysis and power consumption pattern analysis as new diagnostic techniques for identifying damaged modules. These approaches can help reduce forensic costs and better identify damaged modules. Lastly, a systematic, step-by-step protocol is developed to help analysts identify damage to the AP and eSE modules and evaluate recovery feasibility.

The findings of this study provide digital forensic professionals with insights into overcoming challenges during physical recovery processes of smartphones. For future research, we plan to explore methods to enhance the stability of the transplantation process following the chip-off extraction of key modules from physically damaged smartphones. This is expected to further improve forensic techniques for recovering data from damaged mobile devices.

Acknowledgment

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. RS-2024-00398745, Proof of evidence tampering and deployment of response technology in digital environment).

References

Alendal, G., Axelsson, S., Dyrkolbotn, G.O., 2021. Chip chop — smashing the mobile phone secure chip for fun and digital forensics. Forensic Sci. Int.: Digit. Invest. 37, 301191. https://doi.org/10.1016/j.fsidi.2021.301191. URL: https://www.sciencedirect.com/science/article/pii/S2666281721000998.

Alendal, G., Dyrkolbotn, G.O., Axelsson, S., 2018. Forensics acquisition — analysis and circumvention of samsung secure boot enforced common criteria mode. Digit. Invest. 24, S60–S67. https://doi.org/10.1016/j.diin.2018.01.008. URL: https://www.sciencedirect.com/science/article/pii/S1742287618300409.

Android Developers Blog, 2018. Building a titan: better security through a tiny chip. https://android-developers.googleblog.com/2018/10/building-titan-better-security-through.html. Viewed 20 January 2025.

Arsenij, T., 2023. Samsung upload mode dumper. https://github.com/m4drat/upload-mode-dumper. Viewed 20 January 2025.

Ayers, R., Brothers, S., Jansen, W., 2014. Guidelines on mobile device forensics. https://www.nist.gov/publications/guidelines-mobile-device-forensics. Viewed 20 January 2025.

Bellom, M.R., Melotti, D., 2023. Android data encryption in depth. https://blog.quarkslab.com/android-data-encryption-in-depth.html. Viewed 20 January 2025.

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

Fukami, A., Ghose, S., Luo, Y., Cai, Y., Mutlu, O., 2017. Improving the reliability of chip-off forensic analysis of NAND flash memory devices. Digit. Invest. 20, S1–S11.

Fukami, A., Nishimura, K., 2019. Forensic analysis of water damaged mobile devices. Digit. Invest. 29, S71–S79.

Google, 2024a. File-based encryption. https://source.android.com/docs/security/features/encryption/file-based. Viewed 20 January 2025.

Google, 2024b. Hardware-backed keystore. https://source.android.com/docs/security/features/keystore. Viewed 20 January 2025.

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.

Heckmann, T., Souvignet, T., Lepeer, S., Naccache, D., 2016. Low-temperature low-cost 58 bismuth – 42 tin alloy forensic chip re-balling and re-soldering. Digit. Invest. 19, 60–68. https://doi.org/10.1016/j.diin.2016.10.003. URL: https://www.sciencedirect.com/science/article/pii/S1742287616301001.

Intel, 2024. Trusted execution environments (tee). https://docs.trustauthority.intel.com/main/articles/concept-tees-overview.html. Viewed 20 January 2025.

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.

Li, W., Xia, Y., Chen, H., 2019. Research on arm trustzone. GetMobile: Mobile Comput. Commun. 22, 17–22.

Mahmod, J., Hicks, M., 2024. Untrustzone: systematic accelerated aging to expose on-chip secrets. In: IEEE Symposium on Security and Privacy, pp. 4107–4124.

Mayrhofer, R., Stoep, J.V., Brubaker, C., Kralevich, N., 2021. The android platform security model. ACM Transactions on Privacy and Security (TOPS) 24, 1–35.

Navanesan, L., Le-Khac, N.A., Oren, Y., Zoysa, K.D., Sayakkara, A.P., 2024. Cross-device portability of machine learning models in electromagnetic side-channel analysis for forensics. J. Univers. Comput. Sci. 30.

Samsung, 2020. Samsung introduces best-in-class data security chip solution for mobile devices. https://semiconductor.samsung.com/news-events/news/best-in-class-data-security-chip-solution-for-mobile. Viewed 20 January 2025.

Saß, X.M., Mitev, R., Sadeghi, A.R., 2023. Oops.! i glitched it again! how to multi-glitch the glitching-protections on ARM TrustZone-M. In: USENIX Security Symposium, vol. 32, pp. 6239–6256.

Sobey, C.H., 2004. Recovering Unrecoverable Data. A ChannelScience White Paper, pp. 15–16.

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.

Statcounter, 2024. Mobile vendor market share worldwide dec 2023 - dec 2024. https://gs.statcounter.com/vendor-market-share/mobile/worldwide/. Viewed 20 January 2025.

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.

WIoT Group, 2024. Nxp and xiaomi: the first to leverage android ready se. https://wiot-group.com/think/en/news/nxp-and-xiaomi-the-first-to-leverage-android-ready-se/. Viewed 20 January 2025.