Forensic case studies - extraction of deleted data from smashed/damaged android mobile phone through replacement of PCB (Printed Circuit Board) in other mobile of same model.

Akhlesh Kumar*[1], Anuj Bhardwaj[2], Ayushi Dwivedi[3], Damini Thakur[4], Dr. S. K. Jain[5]
*[1] *Assistant Director, Forensic Computer Division, Central Forensic Science Laboratory, Chandigarh, India*
[2,3,4] *Forensic Professional, Forensic Computer Division, Central Forensic Science Laboratory, Chandigarh, India*
[5] *Chief Forensic Scientist, Directorate of Forensic Science Services, Ministry of Home Affairs, New Delhi, India*

Abstract: **With the evolution of technology, the method of committing crimes is also evolving, it has shifted from physical to digital space. Forensic investigators have considerable obstacles when recovering data from broken cell phones. The recovery procedure is more difficult due to different kinds of damage, such as physical shock, water exposure, and encryption. Since broken mobile devices require functional components to unlock or access data, existing forensic technologies may not work with them. Therefore, advanced knowledge, skills and tools are necessary to overcome this limitation. The fact that cell phones are password-locked is one of the biggest problems for the investigating agencies. Therefore, new methods are required to solve this issue. Removal of PCB (Printed Circuit Board) from a damaged device and transferring it to a new body of the same model is one such approach.**

In the present study, two damaged mobile phones: Redmi 9 (whole body broken with a hammer) and Vivo Y91i (broken into multiple parts) were studied. Initially, the PCB of both mobile phones were removed and transferred to corresponding working mobile phones of the same models. The support for the chipsets to unlock both devices was present in the Passware Kit Mobile 2024 software. The mobile phones were put in boot ROM mode and a physical dump was created. Further, the dump was decrypted and analysed using the Magnet Axiom 7.8 version.

Keywords: **PCB, Printed Circuit Board, Damaged Mobile Phone, Android Mobile Phone, Android, Passware Kit Mobile, Magnet Axiom, Forensic Science, Cyber Forensic, Deleted Data Retrieval, Boot ROM Mode, Redmi 9, Vivo Y91i, Mobile Forensics**

I. INTRODUCTION

At present, digital data is an essential aspect of investigation. Mobile forensics is a critical field in digital investigations, but it comes with its own set of challenges, especially when it comes to data extraction. Existing forensic tools often fail with damaged devices, as they require functional components to unlock or access data. Devices that are physically damaged or inoperable pose additional challenges for data extraction. Forensic experts may need specialized equipment or techniques to recover data from such devices.

The proper chain of custody and documentation of the extraction procedure helps in the adequate admissibility of the evidence in court. While seizing the mobile phone from the crime scene, the investigating officer must document the exact specifications of the mobile phone such as the exact model of the seized mobile phone, the type and version of the operating system running on the mobile phone and if possible the lock screen password along with the date and time displayed on the mobile phone at the time of seizure.

The forensic dump of the device is created so that the integrity of the exhibit can be maintained. Various internationally certified forensic software for data extraction are available. Different extraction methods such as Logical extraction, File System extraction and Physical extraction are present. However, depending on the chipsets and model of the mobile phone data (i.e. call logs, chats, contacts, user accounts, device info, instant messages, emails, documents, web history, audio,

images and videos) is extracted accordingly. After the examination and analysis of the dump created, a comprehensive report is prepared involving a complete data report and case-related relevant reports by the forensic expert.

Mobile forensics can be particularly challenging when devices are physically damaged. Accessing data from phones with shattered or unresponsive screens can be difficult. Touch input may not work, and data access may require specialized tools. Phones exposed to water can suffer from internal circuit damage, making direct access to the device's memory and storage difficult or impossible without professional tools. Phones damaged due to accidents (fire, crushing, etc.) may have broken chips or storage components, which makes recovering data a complex process requiring advanced techniques. Damaged devices might result in corrupted or fragmented data, making it difficult to piece together evidence accurately. Mishandling damaged devices can cause further data loss, so special care is needed during extraction. A damaged device that will not power on can hinder direct access to its storage components. The forensic expert might need to bypass the device's power system, using chip-off or JTAG techniques to extract data, but this requires expertise and specialized equipment. Physical damage can also corrupt the storage media of the mobile phone. This means that even if the data can be accessed, portions of it might be irrecoverable or need reconstruction.

Security features such as biometrics, PIN codes, and pattern locks might be difficult to bypass if the device cannot function. Forensic tools can sometimes break through security, but with damage, this becomes much more difficult. Many modern smartphones have built-in encryption for both internal storage and SD cards. When the phone is damaged, especially if the device does not power on, breaking through encryption to recover data can be nearly impossible without the proper passcodes or forensic expertise. There is no one specific solution for damaged mobile devices, and each case might require different forensic methods.

Extracting and decrypting physical data from damaged mobile phones presents significant technical challenges. If the phone doesn't power on, physical data extraction methods like USB connection, Android Debug Bridge (ADB), or regular forensic tools can't be used. The phone needs to be repaired, or more invasive techniques such as chip-off or JTAG methods must be applied. However, there are a few limitations when it comes to advanced or invasive techniques depending on the features of the exhibit mobile phones, therefore forensic repairing and replacement wherever possible should be applied to retrieve the data from damaged mobile phones.

CASE STUDY I

In this case, the forwarding authority brought the case to the Central Forensic Science Laboratory Chandigarh for examination in which one Redmi 9 mobile phone was seized from the accused, who allegedly used it for extortion. The seizure memo stated that the accused purposely broke the mobile phone to eliminate all the digital evidence from it. The phone was found in completely broken and bent condition (Figures 1 and 2). The chipset of the mobile phone was Mediatek MTK 6765 Helio G35.

Figure 1. Front side of the exhibit-1

Figure 2. Rear side of the exhibit-1

CASE STUDY II

In this case, the forwarding authority brought the case to the Central Forensic Science Laboratory Chandigarh for examination in which the accused allegedly recorded the screen in his Vivo Y91i mobile phone while the said phone was displaying some obscene videos of the victim and threatened to make them public. According to the seizure memo, the accused allegedly tried to remove all digital evidence from the vivo Y91i phone by intentionally breaking it (Figures 3 and 4). The chipset of the mobile phone was MTK 6762 Helio P22.

Figure 3. Front side of the exhibit-2

Figure 4. Rear side of the exhibit-2

II. METHODS AND MATERIAL

In the aforementioned cases, the standard mobile extraction methods were ineffective. As both the exhibits were not in working order they needed to be opened and checked if any repair or replacement of parts is required. An authorization letter from the forwarding authority for the repair/replacement of parts of the mobile phone for retrieval of data was also submitted with other case-receiving documents. Therefore, both the exhibit mobile phones were opened/dismantled along with the videography of the same. In both cases, the PCB (Printed Circuit Board) was found intact and after testing the PCBs, they were found in working order. To bring mobile phones in working condition the PCBs of broken mobile phones were removed and the same were transferred to another body of the same model i.e. Redmi 9 and Vivo Y91i (Figure 5). After giving DC power supply in the PCB of both the exhibits, the charging symbols appeared and Mobile phones were brought in working condition forensically. After fully charging the first mobile phone i.e. Redmi 9 it was found password protected (unspecified characters) (Figure 6). The other mobile phone was not protected by any password or pattern.

Figure 5. PCB transferred

Figure 6. Password protected mobile phone

Passware Kit Mobile Beta 2024 (Figure 7*)* was used to identify the password and to extract the data from Xiaomi Redmi 9 as support to unlock the devices with Mediatek MTK 6765 chipset present on the software.

The mobile phone was brought into boot ROM mode by pressing both the volume up and down

buttons while connecting it to the forensic workstation with Passware Kit Mobile Beta 2024 installed using a USB cable. The password was identified using the brute force method and after processing, the password of the mobile phone was identified and the unprotected physical dump was created as a .dar file. The .dar file along with keystore_decryption.dig key was decrypted using the forensic software Magnet Axiom 8.2 version.

Passware Kit Mobile Beta 2024 was also used to create the physical dump of the Vivo Y91i mobile phone as support to create a physical dump from the devices with MTK 6762 Helio P22 chipset was present on the software. The dump in the form of a .dar file along with keystore_decryption.dig key was decrypted using the forensic software Magnet Axiom 8.2 version.

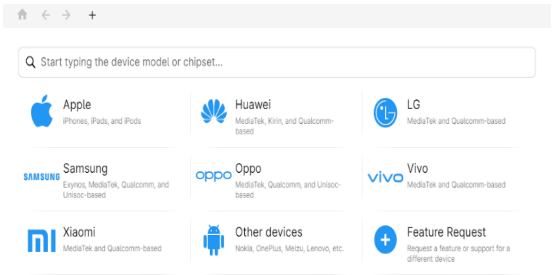

Figure 7. Home Screen of Passware Kit Mobile Beta 2024

III. RESULTS AND DISCUSSION

The PCB transfer method demonstrated success in extracting data from both the physically damaged mobile phones as the damage was isolated to non-essential components like the display, battery, or external ports.

The decrypted data of both mobile phones resulted in web-related, communication, social media, media, email and calendar, documents, additional sources, peer-to-peer, application usage, operating system, encryption and credentials, connected devices, location and travel, and custom including deleted files (Figure 8). Further, the case-related relevant reports and the complete reports were generated using Magnet Axiom 8.2 version.

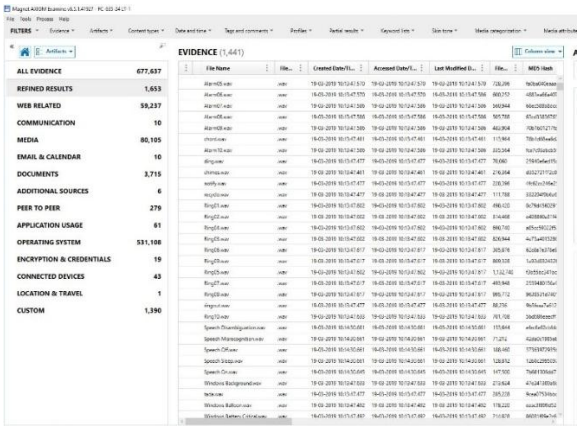

Figure 8. Decrypted data on Magnet Axiom

Challenges and Limitations of PCB Transfer Method:

One of the key challenges in the PCB transfer method is finding the exact Mobile phone as the PCBs vary widely in terms of design, layout, and components and some mobile phone models may not always be available, especially older or rare devices. The PCB transfer process requires high levels of precision and expertise. Specialized tools and expert knowledge are needed to carry out the transfer.

Decryption after PCB Transfer:

Data encryption still poses a challenge, even after successfully booting the device via the test mobile phone containing the exhibit PCB. Encrypted files or full-disk encryption must be bypassed using traditional forensic decryption methods. Depending on the security setup (PIN, password, biometrics), decrypting the device may still require access to the original credentials. Without them, brute-forcing or exploiting vulnerabilities (such as a known flaw in the encryption system) may be the only way forward. Some devices might require external authentication (such as cloud-based verification) to unlock the phone, adding another layer of difficulty for forensic investigators.

IV. CONCLUSION

In conclusion, PCB transfer is a valuable technique for forensic investigators, especially when paired with other forensic tools to complete the decryption process. However, its practical application is constrained by the specific conditions of the damaged device and the resources available for the forensic investigation.

Using PCB (Printed Circuit Board) transfer as a solution for extracting and decrypting physical data from damaged mobile phones is a promising technique. The PCB transfer method allows the phone to boot up with its original configuration. However, if the device is locked or secured with full-disk encryption or file-based encryption, forensic experts still need to overcome encryption hurdles. But the advantage is that once the phone is operational, regular forensic tools can be used for decryption. In cases where the transfer is successful, data integrity is maintained. Since the method preserves the original memory and processor, the risk of further data corruption is minimized. This method also preserves the integrity of essential components such as the eMMC or UFS storage chips, as well as the CPU, which are crucial for data decryption.

V. REFERENCES

[1] Bhardwaj, A., & Kaushik, K. (Eds.). (2024). Cyber Forensics and Investigation on Smart Devices. BENTHAM SCIENCE PUBLISHERS.

[2] Alatawi, H., Alenazi, K., Alshehri, S., Alshamakhi, S., Mustafa, M., & Aljaedi, A. (2020). Mobile Forensics: A Review. In 2020 International Conference on Computing and Information Technology (ICCIT-1441) (pp. 1–6). 2020 International Conference on Computing and Information Technology (ICCIT-1441). IEEE.

[3] Da Costa, A. M., De Sa, A. O., & Machado, R. C. S. (2022). Data Acquisition and extraction on mobile devices-A Review. In 2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT) (pp. 294–299). 2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT). IEEE. https://doi.org/10.1109/metroind4.0iot54413.2022.9831724

[4] Rajinder Singh Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 2(Version 1), February 2014, pp.519-521

[5] E. Casey, (ed.) Handbook of Digital Forensics and Investigation, Academic Press, 2010.

[6] Larson S. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Journal of Digital Forensics, Security and Law. 2014.

[7] Passware kit mobile - bypass or recover pin locks and passcodes, perform extraction of data from locked or encrypted mobile devices. Passware. (n.d.). https://www.passware.com/kit-mobile/

[8] Magnet axiom cyber. Magnet Forensics. https://www.magnetforensics.com/products/magnet-axiom-cyber/

[9] CFSL Chandigarh's Working Procedure Manual of Cell Phone Forensics CFSL/CHD/WPM/CPF Chandigarh issue no. 01, Issue date: 27.05.2022.

[10] Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of Mobile Device Forensics. In Digital Investigation (Vol. 10, Issue 4, pp. 323–349). Elsevier BV. https://doi.org/10.1016/j.diin.2013.10.003