JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DATA EXTRACTION FROM LOCKED ANDROID MOBILE PHONES WITH JUMPER PIN POINT METHOD AS A SOLUTION - CASE STUDIES

Akhlesh Kumar*[1], Ayushi Dwivedi[2], Anuj Bhardwaj[3], Dr. S. K. Jain[4]
*[1] Assistant Director, Forensic Computer Division, Central Forensic Science Laboratory, Chandigarh, India
dohreakhlesh@gmail.com[1]
[2] Forensic Professional, Forensic Computer Division, Central Forensic Science Laboratory, Chandigarh, India
ayushidwivedi554@gmail.com[2]
[3] Forensic Professional, Forensic Computer Division, Central Forensic Science Laboratory, Chandigarh, India
bhardwaj20aj@gmail.com[3]
[4] Chief Forensic Scientist, Directorate of Forensic Science Services, Ministry of Home Affairs, New Delhi, India
cfs-dfss@nic.in

ABSTRACT

With the increase in cybercrime cases in recent times, the challenges have escalated immensely. The ongoing research has proved the need for advancement in digital forensics to combat digital crimes. Mobile Forensics has played an important role when it comes to Digital Forensics, ranging from minor offenses like petty theft, shoplifting and trespassing to more severe crimes like identity theft, hacking, murder, rape etc. In such crimes, one of the major challenges faced by investigating agencies is that the mobile phones are found in locked condition. Sometimes, the locked phones could not be bypassed using the routine mobile forensics tools. However, every technology has some limitations and drawbacks; hence, modern problems require new approaches and one of the approaches is the Jumper Pin Point method.

The present study will help the reader to know the challenges faced by mobile forensic experts in extracting data from password-protected mobile phones and how the Jumper Pin point method can help in solving the problem. In this study, two password-protected Android mobile phones (Vivo Y15 and Oppo A54) were initially analyzed using routine Mobile Forensic software, but they were unable to bypass the phone security. The chipsets of both phones were available on Passware Kit Mobile 2023. The two suggested methods of the tool to put the phone in boot ROM mode - button combination method and test point method were also not working. Finally, the jumper pinpoint method successfully put the mobile phones into boot ROM mode. The dump was created using Passware Kit Mobile 2023 and the report was generated using Magnet Axiom version 7.6.

Keywords: Jumper, Passware, Forensics, Law and Order, Jumper Pin Point Method, Mobile Forensics, Forensic Tools, Mobile Phones, Magnet Axiom, Passware Kit Mobile, MTK 6762 chipset, MTK 6765 chipset, MediaTek, Password Protected Phone, Locked Phone, Locked Android Phone, Vivo Y15, Oppo A54.

I. INTRODUCTION

Forensic data extraction of a mobile phone refers to the process of collecting and preserving digital evidence from a mobile device for investigative or legal purposes. This process involves extracting various types of data from the device, such as call logs, text messages, emails, photos, videos, app data, location information, and more. Forensic data extraction is commonly used in criminal investigations, litigations, and other scenarios where digital evidence is crucial.

Forensic data extraction must be conducted legally and in compliance with relevant laws and regulations. This

often requires obtaining proper authorization, such as a search warrant, court order, or the device owner's consent. Once seized the type and version of the mobile device (e.g., iPhone, Android phone) and its specific model must be identified, as different devices may require different extraction methods. The integrity of the evidence is maintained by creating a forensic copy of the device's storage (a forensic dump). This ensures that the original data remains unchanged during the extraction process. There are professional mobile forensic tools and software used to extract data from the mobile device. These tools may employ various techniques to access different types of data, such as logical extraction (accessing present data through the operating system) or physical extraction (accessing present and deleted data from the device's storage).

Depending on the device and circumstances, data extraction can be conducted via physical connections, wireless connections, or even remotely in some cases. There are different types of data, including call records, SMS and MMS, emails, social media data, geolocation information, internet browsing history, and more. The extraction process may involve accessing files, databases, and system logs.

Once the data is extracted, forensic experts analyze the collected information to uncover evidence relevant to the investigation. This may involve recovering deleted data, identifying patterns, and reconstructing timelines. Detailed documentation of the extraction process is crucial for maintaining the chain of custody and ensuring the admissibility of the evidence in court. This documentation includes information about the tools used, extraction methods, and any modifications made to the device. Also, maintaining a secure chain of custody is essential to demonstrate that the evidence was handled and preserved correctly throughout the investigation. After analysis a comprehensive forensic report is prepared, summarizing the findings and evidence collected during the extraction process. This report is frequently used in court cases.

Forensic data extraction is a specialized field that requires expertise and adherence to strict protocols and legal guidelines. It plays a critical role in modern investigations, helping law enforcement agencies, legal professionals, and cybersecurity experts uncover valuable digital evidence from mobile devices.

Jumper Pin Point

A jumper is a small conductor which acts as a bridge to open, close and even bypass a part of an electronic circuit. Jumper pins (points to be associated by the jumper) are organized in bunches called jumper blocks, each connecting with one set of contact points. It can be substituted with a Dual In-Line Package (DIP) switch (Figure 1). A jumper is sheathed in a nonconductive plastic block which prevents any possibility of a short circuit. Jumper pinpoint, also known as "jumper pins" or "jumper settings," are small connectors or pins on electronic devices, such as circuit boards or computer hardware components, that are used to configure or customize certain aspects of the device's operation. These pins are typically found on devices like motherboards, hard drives, and expansion cards. This type of pinpoint is found between the processor and the Embedded Multi-Media Card (eMMC). This place is covered with a metallic sheet. It is generally a tedious and laborious task for a Forensic expert to remove this sheet and identify the jumper pinpoint on the circuit.

Jumper pins are usually accompanied by a small plastic connector called a "jumper cap" or "jumper shunt." The jumper is placed on at least two pins which allow it to establish a connection and activate necessary instructions and a shunt is arranged on the pins that allows electric current to pass through the circuit points. By placing this cap or shunt onto specific jumper pins, you can change the way the device functions.

Figure 1. Dual In-Line Package (DIP) switch

Jumper pins are often used to set hardware parameters, such as clock speeds, voltage settings, or device IDs. Some devices have jumper pins to determine the boot order or to set the drive as the master or slave in the case of IDE drives. Jumper pins can also be used to enable or disable specific features or functions on a device. In some cases, jumper pins can be used to configure memory settings, especially on older computer motherboards or expansion cards. Jumper pins are often used to clear the CMOS (Complementary Metal-Oxide-Semiconductor) settings on a motherboard, which can reset the BIOS/UEFI settings to their default values.

Case Study I

As per the FIR filed by the mother of the victim, her daughter was studying in college and used to do a part-time job. It was alleged that three girls and one guy had

harassed the victim since college time and she was afraid that they would kill her. The mother was quite confident that her daughter had committed suicide after being bullied by the above-mentioned people. Two days later, she was found dead by falling off the roof of the same college.

The given case was brought to the Central Forensic Science Laboratory, Chandigarh for examination by the Forwarding Authorities report that at the scene of the incident, a deceased person's shattered Vivo Company cell phone was discovered.

The case was opened and it was found that the display of the phone was completely damaged (Figures 2 and 3). The exhibit was forensically repaired (Vivo Y15 Phone, chipset MTK 6762) and brought to working condition. However, it was in password-protected condition.

Figure 2. Front side of the exhibit-1

Figure 3. Rear side of the exhibit-1

The password was only known to the deceased and the forwarding authority/Investigating Officer was unable to provide the password. The password of the exhibit could not be bypassed using various mobile forensic tools and after a lot of trials, the data still could not be extracted. Many advanced procedures like the EDL method were unable to extract data as well.

Case Study II

As per the FIR lodged, the victim (son of the complainant) has committed suicide after being constantly harassed and threatened over the phone and in person by the accused for money. On the day of the incident accused came to the house of the victim to threaten him which led him to commit suicide by consuming aluminium phosphide.

In this case, the password-protected mobile phone of the victim (Oppo A54 Phone, chipset MTK MT 6765) with a damaged display was submitted to CFSL Chandigarh for data recovery (Figures 4 and 5). As neither any family member nor any friend/acquaintance knew the password of the deceased mobile phone, the investigating agency was unable to provide the password to CFSL Chandigarh.

Figure 4. Front side of the exhibit-2

Figure 5. Rear side of the exhibit-2

Similar to the previous case, the password of the exhibit could not be bypassed by performing n number of attempts with routine mobile forensic tools and advanced procedures like the EDL method. Therefore, the data could not be extracted from this exhibit too.

II. METHODS AND MATERIAL

The routine Mobile Forensic tools were ineffectual in the above cases. Initially, the display of the Vivo phone (Case 1) was forensically repaired and brought in working condition. The chipset of exhibit of case 1 was MTK 6762 and of case 2 was MT 6765 and the option to extract data from these specific chipsets was available in Passware Kit Mobile 2023. The challenge was that the mobiles were unable to go in Boot Rom mode. To solve

this issue, it was decided to work on a new approach. The new procedure was by Jumper Pin Point Method.

The mobile phones were opened following their service manual, and the PCB was removed. The area of eMMC and processor was accessed by removing the metallic cover. Thorough research on the internet helped in identifying CMD and DAT0 points after removing the cover (Figures 6 and 7). The test points in CLK were identified. Usually, "CLK" refers to the clock input/output or the clock signal. The clock signal, often denoted as CLK, is a crucial component in digital electronic systems, including chipsets, as it synchronizes the operation of various components within the system.

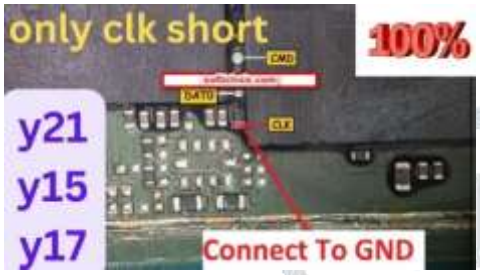

Figure 6. Test point on PCB of case 1

Figure 7. Test point on PCB of case 2

The test point was cleaned and a jumper wire was soldered on it. Mobile phones were re-assembled (Figures 8, 9 and 10).

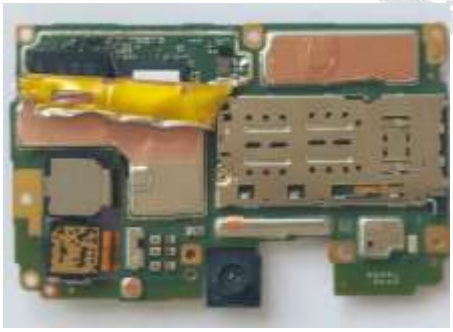

Figure 2.Connected Jumper pin point in case 1

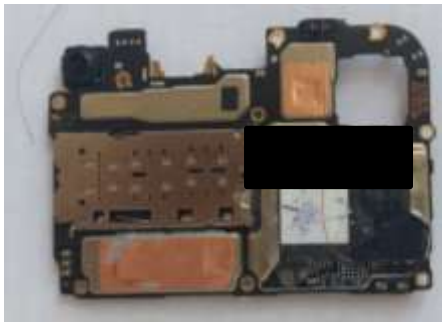

Figure 3.Connected Jumper pin point in case 2

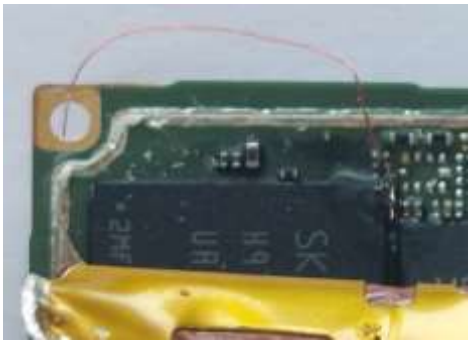

Figure 4. Soldered jumper to test point

The chipsets were selected on the Passware Kit Mobile 2023 tool in PC (Figure 11). The devices were put in Boot Rom mode by connecting the soldered Jumper wire to Ground H and while holding the wire in position the mobile was connected to the PC via USB (Figure 12).

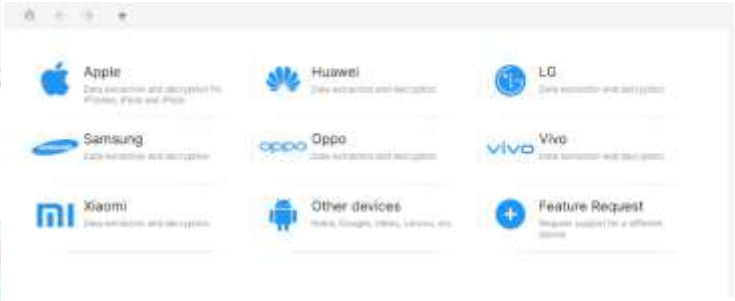

Figure 5.Home screen of Passware Kit Mobile 2023

Figure 6.Device entered Boot Rom mode after successful Jumper Pin Point Method

Once the devices entered into the Boot Rom mode successfully the tool asked to disconnect the test points and it automatically started making the dump of mobile phones. The dump was completely extracted, and analyzed using Magnet Axiom Process and Examine Version 7.5. The report relevant to the cases and the complete report of the data were generated through Magnet Axiom Process and Examine Version 7.5

III. RESULTS AND DISCUSSION

This technique requires a higher level of technical expertise because one should be aware of the PCB of

mobile phones, identify test points CMD, DATA0, and CLK on the PCB, and how to connect a jumper wire to the board.

The Passware Kit Mobile 2023, which was the key tool for this study, requires the mobile phone to be put in Boot Rom mode to break the password and extract the data. This Jumper Pinpoint method helps in putting the mobile in Boot Room mode when the other methods - button combination and test point methods fail. Therefore, even if the support for the mobile device/chipset is available on the tool and the examiner is unaware of this method, the case would be reported with no opinion as no data could be retrieved from the device. This method will help in all such cases where other tools are unable to break or bypass the password, and the examiner is unable to put the phone in Boot Rom Mode on Passware Kit Mobile 2023.

Once the connection has been made the dump created can be processed and analyzed in the usual way. The extracted data in the present study comprised media, documents, application usage, social networking, call logs, operating system data, emails, calendar, location, web-related and other possible information that could be retrieved from the device (Figures 13 and 14). This information aids in investigation and ensures timely response to criminal activity.

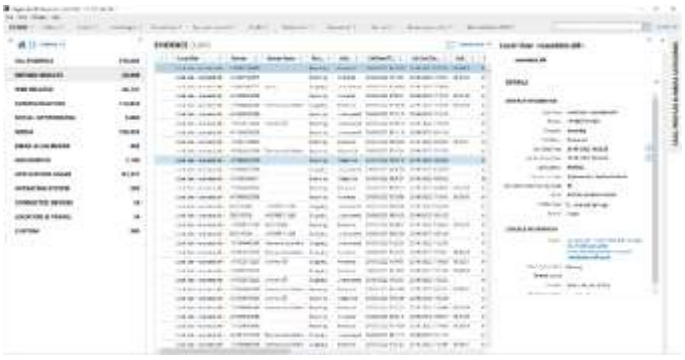

Figure 7. Data retrieved in case 1

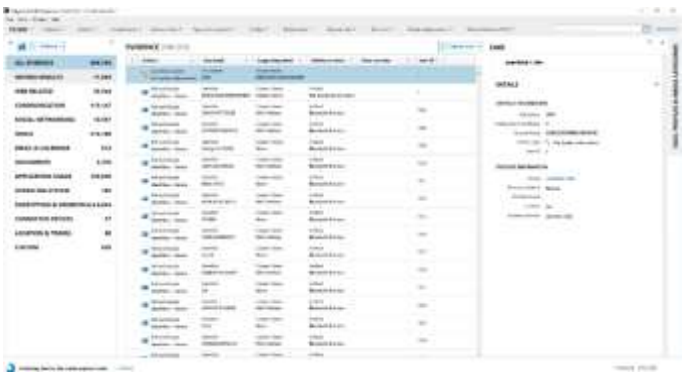

Figure 8.Data retrieved in case 2

Challenges

Extracting data from mobile phones can be challenging due to multiple reasons. Mobile devices, especially smartphones, are equipped with various security measures like PINs, passwords, biometrics and encryption. These safeguards are designed to protect user data, making it difficult for unauthorized parties to access the device's contents. Mobile phone manufacturers continuously enhance device security, leading to ever-evolving technologies and encryption methods. Breaking through these security measures requires constant research and development of new techniques and tools. Mobile devices run on different operating systems, such as Android, iOS, and others. Each OS has its own security mechanisms and file structures, requiring forensic experts to be proficient in multiple platforms. Mobile operating systems and apps are regularly updated, introducing new security features and closing vulnerabilities. Forensic techniques and equipment need to change to keep up with these advancements. Some devices have locked bootloaders, making it challenging to install custom recovery or forensic software to access the device's memory.

Modern smartphones often use hardware-based encryption to protect data stored on the device. Even if the device is physically accessed, the data may still be encrypted, necessitating the decryption of data to make it accessible. iCloud from Apple and Google Drive are examples of cloud-based services that are connected to mobile devices. Accessing data stored in these accounts often requires authentication, which may not be easily bypassed. Some mobile devices have secure hardware components, such as Apple's Secure Enclave, which store sensitive data like biometric information and encryption keys. Accessing this data is exceptionally challenging due to the high level of security. In cases of physical damage to a device, data extraction can be even more challenging, as there may be hardware issues or data corruption that complicates the process.

Mobile forensic investigations must adhere to legal and ethical standards. It is crucial to protect user privacy and data. Forensic experts must handle extracted data carefully, and there are legal and ethical considerations regarding what data can be accessed and used. Gaining unauthorized access to a device can result in legal consequences and may render the extracted data inadmissible in court. Due to these challenges, mobile forensic experts have to go through many time-consuming procedures by switching forensic tools for the specific model.One of the most occurring challenges in mobile forensics is when the password used for the lock screen is not provided by the forwarding authority as the owners of the mobile phone were deceased. In the following case studies, victims have committed suicide. Therefore, it was impossible to receive the password from the forwarding authority/case IO. Hence, a new technology was the need for the hour. In the present

study, two cases will be discussed in which a new method to bypass mobile passwords was used, where it was difficult or impossible to get the password from the investigating agency. The method we are going to discuss is Jumper Pin Point.

IV. CONCLUSION

The jumper pinpoint method is a technology that will play a crucial role in digital forensics. This technique will allow for the recovery of data from a wide range of devices and storage media, even if attempts have been made to delete or hide information and also if they are not supported in other Forensic Tools. This method recovers deleted data and performs physical extraction that helps forensic experts process and analyze large volumes of data more thoroughly, reducing investigation time. It is a cutting-edge method that can ensure the integrity of digital evidence, making it admissible in court and helping maintain the chain of custody. Given the prevalence of password-protected mobile devices, forensic experts need this method to extract and analyze data from password-protected smartphones and tablets by bypassing the security code.

In summary, technologies like jumper pinpoint methods are essential in digital forensics to keep pace with the evolving digital landscape, ensuring that investigators can effectively uncover and analyze evidence in a wide range of cases.

V. REFERENCES

[1] TechnicalRiyaz (2023). Vivo new security unlockTestpoint& CLK Y12 Y15 Y17 / pin pattern / latest 2023 @technicalmriyaz. YouTube. https://www.youtube.com/watch?v=Q_VHary_Ynw

[2] WorldMobilekpr (2023). OPPO A54 CPH2239 SCREEN FRP PIN PASSWORD PATERN UNLOCK CM2MT2 WITH TESTPOINT NEW SECURITY.YouTube.https://www.youtube.com/watch?v=PkifILcs7gU

[3] Jumper (computing) (2023) Wikipedia. Available at: https://en.wikipedia.org/wiki/Jumper_(computing) (Accessed: 17 October 2023).

[4] Akhlesh Kumar, Bhushan Ghode, KhevnaManiar, Dr. S. K. Jain, "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), ISSN : 2456-3307, Volume 7, Issue 3, pp.481-487, May-June-2021.

[5] Bhushan Ghode, Akhlesh Kumar, KhevnaManiar, Dr. S. K. Jain, " A Forensic Approach on Data Retrieval from IC/eMMC of Damaged Windows Mobile Phone using Easy JTagPlus Box tool and Magnet Forensic Axiom", International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X, Volume 8, Issue 5, pp.499-508, September-October-2021.

[6] Chang, Xu & Tang, Xin-hua& Wu, Jian. (2013). FORENSIC RESEARCH ON DATA RECOVERY OF ANDROID SMARTPHONE. 10.2991/iccsee.2013.299.

[7] Majid Goraya (2023). Small points Micro soldering techniques Tips & jumper wire use in mobile phone repairing Tutorial#7. YouTube. https://www.youtube.com/watch?v=x9k0qIB2O8k

[8] Tech Help & Guide (2023). what is jumper | how to use jumper wire. YouTube. https://www.youtube.com/watch?v=HmWxudhtJ_c

[9] Mcl. (2022, February 14). What are PCB test points: How to use PCB test points. mcl. https://www.mclpcb.com/blog/test-points-pcb/#:~:text=What%20Are%20Test%20Points%20on,of%20materials%2C%20sizes%20and%20colors.

[10] Mediatek test-point gallery – passware support. (n.d.). https://support.passware.com/hc/en-us/articles/7121135326999-MediaTek-test-point-gallery (Accessed: 19 October 2023).