A Forensic Approach on Data Retrieval from IC/eMMC of Damaged Windows Mobile Phone using Easy JTagPlus Box tool and Magnet Forensic Axiom

Bhushan Ghode¹, Akhlesh Kumar², Khevna Maniar³ and Dr. S. K. Jain⁴

¹- Forensic Professional, Cyber Forensic, Central Forensic Science Laboratory, DFSS, MHA, Govt. of India, Chandigarh, India
²- Assistant Director (Physics), Central Forensic Science Laboratory, DFSS, MHA, Govt. Of India, Chandigarh, India
³- Forensic Professional, Central Forensic Science Laboratory, DFSS, MHA, Govt. of India, Chandigarh, India
⁴- Director-cum –Chief Forensic Scientist, Central Forensic Science Laboratory, DFSS, MHA, Govt. Of India, Chandigarh, India

ABSTRACT

The digital world is dominated and ruled by the IOS and Android operating systems on mobile as well as tablet platforms. Together they share a whopping 99% (till 2021) of the share market. The Windows Phones (WP) are occupants of that less than 1% platform that they share with other subsidiary operating systems. Due to the lack of commercial popularity and production of such Windows devices, the process of data extraction and analysis of such devices is unique and challenging for forensic experts. The standard forensic data retrieving software and hardware do not support advanced requisition techniques except the direct extraction. Thus, in cases with locked WP devices, the software/ hardware is unable to support the device’s physical extraction or lock bypass facility. As observed in several digital cases, these portable devices contain details of an individual’s most private life including communications, contacts, browsing history, and location specifics at any given time. Although the operating systems of Microsoft and Windows mobile devices are similar in certain ways, specialized skill sets and tools are required while dealing with location, examination, and interpretation of the digital evidence on these systems. In this research paper, the authors are discussing the reliability and success of data extraction of a Windows mobile device from IC/eMMC using specialized hardware/software with the Windows device.

Keywords : Windows Phones, iOS, Android, chip-off, IC/eMMC using the Easy JTag Plus tool and Forensic Magnet Axiom software.
1. INTRODUCTION

Smartphones have become utterly common and users are dependent on them for doing an array of tasks like contacting people, messaging, reminders of appointments, making bookings, online surfing, etc. These tasks are all held by a series of codes and built-in algorithms that makes the tasks possible. The Locar’s Principle famously states that “with contact between two items, there will be an exchange of microscopic material.” This is befitting even for digital evidence. Thus, if smartphone users utilize the phones for their daily routine activities, microscopical evidence in the form of traces of activity logs, event logs, etc. are left in the smartphones. Moreover, whenever any data gets stored in the smartphone in the form of videos, pictures, audios, contacts, call logs, etc., a certain amount of information gets stored along with the main contents as deep-rooted information of the data in the device. These digital traces can guide forensic investigators in their investigations. The traces of these activities can be discovered through a myriad of forensic techniques and give forensic experts a better idea of user interaction with the device. This deeply buried data remains inconspicuously stored in the device and its retrieval can often provide as much if not more information than the particular content of the storage. Background applications data ranging from GPS location to app usage data would be completely pointless to an average user. Although, the obscure traces of the data can become extremely valuable to a digital analyst and a forensic expert.

The world of smartphones has been growing and developing since its conception. Nowadays, multiple OS is observed in smartphones. In the competitive world of mobile operating systems, Android has gained immense popularity. However, the Windows mobile developed by the Microsoft family is a shrouded family among the brands for smartphones and PDAs [1]. Nevertheless, the Microsoft family licenses the Windows Mobile Platform to various device manufacturers including NOKIA, HTC, Huawei, Gionee, Karbonn, LG, Lenovo, Micromax, and others. The Windows platform has offered five different OS to date since its creation which includes Windows CE, Windows Mobile, Windows Phone 7, Windows Phone 8.0/ 8.1 and the newly released Windows 10. This paper explores the functioning of Windows phones and showcases the data extraction from a damaged Windows device. To explore the functioning of a Windows phone, an important question is answered henceforth.

How Windows Phones Store Data?

Windows phones have three primary points of data storage, and often use a combination of any of the three. Like most modern smartphones, Windows Phones also use internal NAND flash memory chips to store data. Furthermore, Windows Phones also have a removable Secure Digital (SD) card slot for expanded memory capabilities. Most applications require some form of data storage for user preferences as well as for user-created data including local caches of data stored in a cloud application or web service. The NET Framework developers will be familiar with the data storage concepts discussed henceforth, as there are limited versions of the same storage technologies existing in the .NET Framework for many years. The differences between the storage APIs in the .NET Framework and the storage APIs provided in the Window Phone SDK are considerable and as explained here.

For starters, the Windows Phone security model limits storage available to third-party applications to an isolated storage sandbox. Each application is
 allotted its sandbox on the phone, isolated from all other applications and the operating system [2]. The application’s sandbox is separated into two folders, as shown in Figure 1. The first folder/sandbox, often referred to as AppData, contains the installed application files. The second folder/sandbox, called Isolated-Storage or isostore, stores files created or downloaded by the application [3].

**Windows Phone File System:**

The Windows Phone file systems are like Windows 7, Windows 8, and Windows 10. From the root directory, one can reach the files and folders which are available on the device [4]. The acquisition method used determines the amount of file system access that the expert has to the device. The details of physical partitions obtained from this case serve as a perfect example for the usual Windows File System directory [2]. The same has been discussed in the Results Section of this paper.

In this research paper, the authors are examining a case study where the victim was found dead in the hostel area of a well-known boarding organization. A hostel student had found the victim’s dead body. The student had then informed the housemaster. The housemaster in turn informed the principal. The entire incident was shocking as it was unprecedented and triggerless as far as the victim’s friends and teachers were concerned. Hence, this created a mysterious environment among all the students and teachers. The police were informed of the incident and called on the scene for further investigation. During the investigation, police recovered one mobile phone in the Victims’ belongings. Possession of a mobile device by students was against the school’s rules and therefore, it was incredible. The mobile phone was in broken and unbootable condition. Following the standard procedure, the mobile device was seized in the hopes of finding some links regarding the case. The authorities were hopeful of finding crucial evidence in the data from the mobile device. This device was hence sent to the Central Forensic Science Laboratory, Chandigarh.

Another question to answer is - **Why perform the Chip-Off Method?**

Even as the commercial tools are improving and making innovations at an impressive rate, unfortunately, the devices continue to evolve posing challenges for the examiners. The chip-off technique is a promising alternative means for data recovery of mobile phones that are damaged, broken, or locked due to which the standard procedures for extraction of data are not possible in such devices. This technique when utilized with other software is capable of extracting dump which can then be decoded further. Chip-Off and JTAG methods are advanced levels of data acquisition methods involving connecting the device’s Test Access Ports (TAPs) and processing the chip to gather the raw data from the chip [5]. Thus, it enables the examiners to extract full physical image from the devices which are not supported by the standard forensic tools.

Once the physical image of the device is retrieved, it was analyzed using the Magnet Forensic Axiom, Version- 4.6. Magnet Axiom is an investigation platform with an ability to recover, analyze, and report on data obtained from various digital devices-mobile, computer, and cloud sources in a single case file [6]. It has also been observed that Magnet Axiom has a higher acquisition capability index than Oxygen.
Forensics and WA Key/DB Extractor while handling EA artefacts [7].

II. METHOD

**Case Opening:** Generally, the case evidence is in sealed condition when received by the reporting scientist. The evidence is either delivered in person by a messenger or sent via post with the required documents regarding brief details of the case. Following that, the evidence is opened under a CCTV-recording, and images are also taken for reference. The same procedure was followed for the Microsoft device that was sent to the scientific officer for investigation. The parcel was opened and found an exhibit Microsoft (RM-1141) mobile device with a broken screen (Figure 2) and was appropriately marked the exhibit mobile device was shifted to the chip-off laboratory.

![Fig.2: The exhibit as received at the laboratory](image)

**Device Inspection:** The device had a broken screen and was unable to boot. The experts tried to charge it but the device didn’t show any indication of charging. A careful inspection was conducted of the device and found that a charging pinout was absent from the device. The charging pinout was soldered on the point and manual charging of the device was tried but was unable to boot. The circuit board was found in complete disarray (Figure 3). The motherboard and the other components were forensically repaired and replaced to enable extraction from a fully functioning device. However, the device was still unable to boot. Thus, the chip-off technique was a distinguished alternative that could be applied. The permission for the same was obtained from legal authorities for the device and then, the procedure for the chip-off was started.
The Chip-Off Technique:

The device was opened up and examined. The following steps were then followed for accomplishing the chip-off technique [8].

1) Chip Unsoldering: The chip unsoldering is an important part of chip-off technique and is required to be performed with utmost care as the chip should not be in the least bit overheated [9]. The unsoldering of the chip is essentially divided into two steps:
   i) Locating the NAND chip on the motherboard. (Figure 4)
   ii) Plucking the chip from its location. (Figure 5)

2) IC Cleaning: Once the chip was pulled from the motherboard successfully, it had to be cleaned off the adhesives attaching the chip to its motherboard. This process is completed by gum removers. First, a heat-based gum remover is applied to the chip which is then heated to allow the gum to move out with the adhesive while cleaning with a brush. Following this, a liquid gum remover is utilized to completely clean the connectors of the adhesive particles sticking to it. This
procedure is followed as many times as required to make the chip accessible for data extraction. The cleaning of the chip is several times followed by reballing of the chip [10] whenever the connection points necessitate changing all the soldered balls on the chip ball [11].

**Data retrieval:** All eMMC can work on a 1-bit bus. But if the authors use this feature for data extraction, it becomes time-consuming and impractical. So, the authors decided to utilize the same equipment as SD cards and adapters for chips. Here, the eMMC was connected with the appropriate adapter to the hardware-software Easy JTag Plus (Fig. 6), and the image/dump (.bin) file was exported (Fig.7 and Fig. 8). Further, the image/dump was processed and analyzed using Forensic Magnet Axiom 4.8 software.

**RESULT**

The physical image was able to provide access to several partitions that can be recovered from the data dump using the software Forensic Imager, Version 4.3. The authors were looking at a Windows Phone 10 device that contained 27 partitions, details as in the following screenshot (Fig. 9). Partitions 26 (Main OS)
and 27 (Data) contained the relevant data:

The Main OS partition in the preceding screenshot is the 26th partition, which contains the system data from the Windows Phone. As in all Windows devices, the system data contains artifacts relevant to investigations. In this example, partition 27 contains the User or Data partition. Depending on the device, the partition numbers may vary. In our example, the Data partition is shown in the following Figure 10 and Figure 11.
1. SMS Messages and Contact Data:
Data and Content associated with SMS messages and contact information were found within a file named store.vol. The store.vol file was located at Users\WPCOMMSERVICES\APPDATA\Local\Unistore\store.vol. The details are shown in Figure 12.

![Fig. 12: Location of Messages](image1)

2. Call History:
Call history data can currently be extracted from the Phone file. It's important to note that the file doesn't have an extension and is located at Users\WPCOMMSERVICES\APPDATA\Local\UserData. The details are shown in Figure 13.

![Fig. 13: Call History](image2)

3. Internet history:
Internet history can be extracted from the WebCacheV01.dat located at Users\DefApps\APPDATA\Local\Microsoft\Windows\WebCache. The details are shown in Figure 14.

![Fig. 14: Internet History](image3)

4. Windows Phone Registry & Other Files:
Windows Phone was found to contain versions of the expected registry hives commonly seen in other Windows operating systems, including NTUSER.dat, SAM, SECURITY, SOFTWARE, SYSTEM, and DEFAULT hives. Evidentiary data may also be in other various Windows artifact locations which are also common to PCs, including, pagefile, $LogFile, $MFT, and $USNjrnI. Sample data was provided to the developers of RegRipper and TriForce for development purposes. The details are shown in Figure 15.

![Fig. 15: Windows Phone Registry](image4)
The forensic dump of IC (Integrated Circuit)/Nand Flash Memory/Chip was exported using the hardware-software Easy Jtag Plus. The forensic dump was analyzed using the software Forensic Magnet Axiom, Version 4.8. Images, Audio, Video, Chats, call logs, browsing history, etc. were retrieved from the IC. All this retrieved exhibit data was exported and forwarded to the investigation agency while maintaining the chain of custody.

Figure 16 shown below shows the System Info of the mobile device obtained from the software Forensic Magnet Axiom, Version 4.8 and Figure 17 shows all the artifacts retrieved.

**DISCUSSION**

Acquiring data from IC/eMMC of the damaged windows phone is challenging as the other software i.e. UFED, MSAB XRY, MOBILedit Express Pro supports only logical extraction of most of the Windows devices, essentially in their unlocked state. Multiple tools, chip-off, JTAG, and other alternative
methods provide access to user data on Windows Phone devices. Often, it is observed find that Windows Phone devices require multiple extraction methods to acquire accessible data. The biggest challenge is getting access to the device to acquire the data. Due to the inconsiderable popularity of these phones, the developers of investigating hardware-software and investigators have less experience with these devices. The usual devices submitted and researched are iOS and/or Android mobile phones. Once the data retrieval is complete and the data available, all the extracted information can be analyzed by the examiner. As Windows Mobile devices become more prevalent, there is a growing need for forensic analysts who can acquire evidence from these devices, and examine their contents.

III. CONCLUSION

The case of foul-play in the victim’s death was essentially a tricky maneuver as all the suspects stemmed from a well-established school. Hence, the investigation had to be handled smartly, cleverly and expediently. The authors of this research paper strongly believe that following the chip-off procedure accurately accomplished the data retrieval from an otherwise obscure OS with ease and precision. The images, call logs, contacts, reminders, videos, etc. i.e., all the data extracted from the device proved to be the most conclusive and unequivocal evidence towards the suspect. Therefore, it proved to be a remarkable help to the officers on the case in catching the culprit. On the other hand, while observing the research perspective, the Windows OS is a unique and small-scale business that is slowly but steadily growing interest and popularity. In response to the same, the software developers are researching and focusing on developing more aid for an investigation into the Windows OS. Till the time comes when the developers have succeeded in determining the by-pass of locks and physical extractions from the Windows devices, it is essential that alternative methods may be utilized for the forensic examination and analysis.

IV. REFERENCES

[1]. "Digital Forensics for a Windows Phone," Gillware, Online]. Available: https://www.gillware.com/phone-data-recovery-services/windows-phone-forensics/. Accessed 1 September 2021.

[2]. "Windows Phone Digital Forensics I," Infosec, Online]. Available: https://resources.infosecinstitute.com/topic/windows-phone-digital-forensics/. Accessed 4 September 2021.

[3]. R. Tamma, O. Skulkin, H. Mahalik and S. Bommisetty, Practical Mobile Forensics, Third Edition ed., Birmingham: Packt Publishing, 2018.

[4]. C. Murphy, A. Leong, M. Gaffney, S. G. Punja, J. Gibb and B. McGarry, "Windows Phone 8 Forensic Artifacts," Sans, Giac Certifications, White Paper, 2021.

[5]. B. Elder, "Chip-Off and JTAG Analysis," 2008. Online]. Available: https://www.evidencemagazine.com/index.php?option=com_content&task=view&id=922. Accessed 05 September 2021.

[6]. "Recover & Analyze Your Evidence in One Case," Magnet Axiom, Online]. Available: https://www.magnetforensics.com/products/magnet-axiom/. Accessed 31 August 2021.

[7]. G. M. Zamroni and I. Riadi, "Mobile Forensic Tools Validation and Evaluation for Instant Messaging," International Journal on Advanced Science Engineering and Information Technology, vol. 10, no. 5, pp. 1860-1866, October 2020.

[8]. A. Kumar, B. Ghode and K. Maniar, "Data Extraction from Password Protection Mobile Phone by using Chip-off Method- A Forensic Case Study," International Journal of
Engineering Sciences & Research Technology, vol. 10, no. 3, pp. 28-37, March 2021.

[9]. I. Mikhaylov and O. Skulkin, "Chip-Off Technique in Mobile Forensics." Digital Forensics Corp, 2016. Online]. Available: https://www.digitalforensics.com/blog/chip-off-technique-in-mobile-forensics#content-anchor. Accessed 05 September 2021.

[10]. J. Farley, "Basic Overview of JTAG, ISP and Chip Off Extractions," Farley Forensics Digital Forensics Research & Development, 10 April 2019. Online]. Available: https://farleyforensics.com/2019/04/10/basic-overview-of-jtag-isp-chipoff-extractions/. Accessed 03 September 2021.

[11]. M. Tj, "Reballing- What it is and How to do it?,” Deskdecode, 10 September 2016. Online]. Available: https://www.deskdecode.com/reballing/. Accessed 29 August 2021.

Cite this article as:

Bhushan Ghode, Akhlesh Kumar, Khevna Maniar, 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), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 5, pp. 499-508, September-October 2021. Available at doi : https://doi.org/10.32628/IJSRST218568
Journal URL : https://ijsrst.com/IJSRST218568