Examination of defective mobile devices – a case study

second lieutenant Marcin Napiórkowski[1]
ORCID 0009-0009-3499-000X

1 Forensic Laboratory of the Provincial Police Headquarters in Szczecin, marcin.napiorkowski@sc.policja.gov.pl

Abstract

This article is devoted to the issue of examination of mobile devices damaged by water. Nowadays, these devices are with us almost all the time and gather a lot of information, making them a valuable and often irreplaceable source of factual evidence. Read-out data can have a very important role during criminal proceedings and it should not be too difficult for a skilled computer forensic investigator to retrieve data from a functioning and unlocked device. Slightly more work is required to extract data from devices that have been damaged, e.g. intentionally or as a result of an accident.

Keywords: Computer forensics, computer forensics research, data recovery, mobile devices

Introduction

The examination of mobile devices (phones and tablets) in police forensic laboratories, from the expert's point of view, often focuses on the selection of an appropriate data acquisition method. Its reading in logical mode is often limited and insufficient, the goal is to acquire a physical image of the memory, which makes it possible to reconstruct even more data, e.g. deleted data or data from system areas. The data obtained in this way is interpreted in accordance with the commissioning party's request for an appropriate report. Manufacturers of mobile devices, obviously having a number of financial, social media, messaging, etc. applications on their phones and tablets, take care to protect the data of their users and apply increasingly effective security measures. This is why accessing the information contained on a device is becoming increasingly difficult. It is no secret that modern devices store data using encryption algorithms, and their complexity makes it very time-consuming or practically impossible to break through the security measures. Another obstacle is the size of the device's memory space, as applications store increasingly more data and multimedia content is stored in high resolutions. It is common nowadays to examine devices with 512GB of memory. Such devices take a long time to acquire and analyse. The real challenge arises when the examined device is damaged or not fully operational. The case described below demonstrates the application of the test method to an Apple phone and tablet.

Case description

Two devices were submitted to the IT testing laboratory of the Forensic Laboratory of the Provincial Police Headquarters in Szczecin to be examined i.e. an iPhone 6S phone made by Apple and an iPad 2 tablet of the same brand. Moreover, the commissioning part reported that the devices in question had been discovered at the bottom of the Oder River, where they had been submerged for approximately six months. It is commendable that the evidence was secured in paper packaging, which allowed some of the humidity to escape. The request of examination indicated that the objects revealed had been sent in connection with a suspected homicide and belonged to the victim. The request included standard questions regarding the reading of image and video files, text and multimedia messages and instant messaging. The examination

began by unpacking the material (Fig. 1 and 2), photographically recording their physical condition (Fig. 3-8), cleaning them of loose debris and drying them at room temperature in an airy and dry room. The drying process began by disassembling the devices (Fig. 9), disconnecting the batteries and removing the key components, the motherboard containing the memory media.

Fig. 1. collective packaging of the evidence.
Source: own resources

Fig. 2. Individual packaging of the evidence.
Source: own resources

Fig. 3. Tablet, front view.
Source: own resources

Fig. 4. Tablet, rear view.
Source: own resources

Fig. 5. Tablet, view from the 30-pin connector.
Source: own resources

Fig. 6. Phone, front view.
Source: own resources

Fig. 7. Phone, rear view.
Source: own resources

Fig. 8. Phone, view from the Lightning-type connector.
Source: own resources

A bulge in the screen on the iPad 2 device is noticeable (Fig. 5), caused by a change in battery volume. This is not unusual among faulty lithium-ion cells; it happens as a result of a build-up of gases in the sealed battery pack. This happens, for example, as a result of over-discharge or damage to the controller monitoring the battery status. There were also shielding elements on the motherboards of the devices in the form of special adhesive labels and metal covers that could hinder the drying process, so these were removed (Fig. 10). Loose debris was removed from both device motherboards using a soft brush, a 2% solution of ultrasonic cleaner (Tech-Sonic) and distilled water. The next step could be to thoroughly clean the system in an ultrasonic cleaner, but the Forensic Laboratory of the Provincial Police Headquarters in Szczecin does not have the facilities to accommodate such a large device. A hot air flask with a temperature setting of 100°C and a distance of about 20cm from the system was used for re-drying. In addition, compressed air was used to remove humidity that may have accumulated underneath the large area systems. This method should be used very carefully due to the risk of detachment and loss of damaged components. Visually, no damage was revealed. The main power line was then identified on the motherboard of the iPad 2, where no short circuit to ground was found. An identical device was obtained from the Communications and IT Department of the Provincial Police Headquarters in Szczecin, in which the motherboard was replaced with the one removed from the evidence device. The tablet did not start up despite being powered up. When a switched-off Apple phone or tablet is connected to a power source, it automatically starts up. For this reason, a thorough inspection of the motherboard was carried out using a microscope and, for example, only the connector area (J2201) showed the destructive effects of water, with oxidation of the pathway at the contact points between the tin and the copper field. It is possible to bridge the connections thanks to diagrams of the motherboard available on the Internet. Another method of fixing this defect is to scrape the protective mask off the surface of the pathway and extend it. Due to the lack of a precision soldering iron at the Forensic Laboratory of the Provincial Police Headquarters in Szczecin, this defect cannot be fixed, the attempt to read the data failed.

Fig. 9. View of the inside of the phone.
Source: own resources

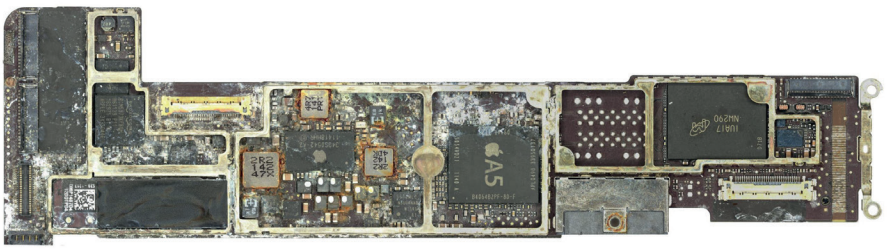

Fig. 10. View of the dismounted tablet motherboard.
Source: own resources

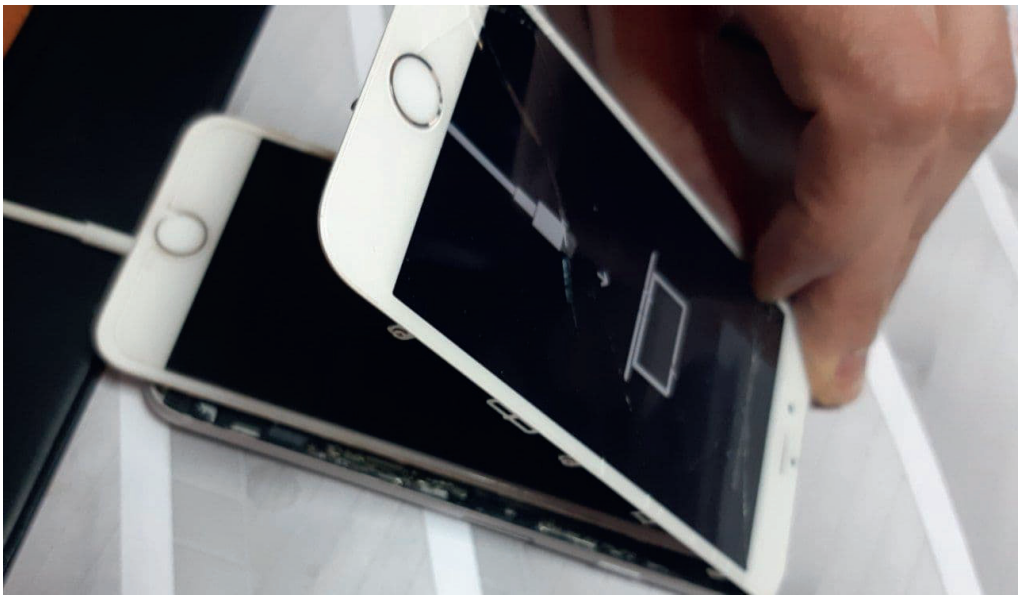

Fig. 11. The iPhone during start-up.
Source: own resources

The examination of the iPhone motherboard followed the same procedure as that used for the iPad. Shielding elements were removed, and loose debris was removed with a soft brush and solution. An ultrasonic cleaner with a solution of the concentration as above was used for the purpose of thoroughly cleaning the motherboard, the operating time was set at three minutes. Visually, no damage was revealed. The main power line was identified on the motherboard, where no short circuit to ground was found. The Communications and IT Department of the Provincial Police Headquarters in Szczecin could not supply an identical device, so the so-called donor was obtained from external sources, but with a faulty button under the Home Button screen. The motherboard was replaced with the one removed from the evidence device, connected to power and the phone booted up. At this stage the problem I mentioned in the introduction occurred, the phone prompted for a user PIN code, which is unknown. The data on the phone is secured against unauthorised access by a six-digit PIN, which results in 1,000,000 possible combinations. The iPhone 6S features the Apple 9 processor, which is susceptible to a dictionary attack that can be performed using specialised software in the DFU (Device Firmware Upgrade) mode. Putting the phone into DFU mode requires the use of physical buttons, the side buttons and the Home Button below the screen (which in the replacement device is defective). The design of the phone's front panel is made up of three basic components, i.e. the display, the digitizer (the component responsible for detecting touch on the screen) and the Home Button. Each of these is connected to the motherboard via a separate cable with a plug, so it is possible to use the Home Button located on the evidence screen (Fig. 11). In this configuration, the phone was put into DFU mode and the procedure for breaking the security measure applied was initiated. This activity took place on the phone at a rate of approximately six passwords per minute. After only 17 hours, the correct PIN was revealed, allowing data extraction in FFS (Full File System) and Checkm8 modes.

Conclusions

Despite the examination steps applied, the device's memory content was not read. The local lab does not have the technical means to repair the device. The iPhone's memory revealed content in the form of text and multimedia messages, correspondence using Facebook Messenger, Grindr, iMessages, Instagram, WhatsApp, as well as audio and video files.