OPEN ACCESS Freely available online

ISSN: 2090-2697
Journal of
Forensic Biomechanics

Perspective

Brief Note on Mobile Forensics

Yuri Robeck*

Department of Legal Medicine and Forensic Sciences, University of Porto, Porto, Portugal

DESCRIPTION

Mobile forensics is a branch of digital forensics that deals with the acquisition and analysis of mobile devices to obtain the digital evidence under investigation. In particular, mobile forensics deals with evidence of recovery from mobile devices such as smartphones and tablets. Now that people rely on mobile devices to send, receive, and retrieve data, it's not surprising that these devices hold a vast amount of evidence that can be applied to investigators. Mobile devices can provide all sorts of important data, from call logs and text messages to web search history and location data that show where the device owner was at a particular point in time.

MOBILE FORENSIC RESEARCH PROCESS

Seizures

When a mobile device is trapped, it is usually necessary to isolate the mobile device from the network so that incoming data does not overwrite old data. It can then be shipped in a Faraday cage or a special Faraday bag. The confiscated device can also clone airplane mode (Wi-Fi is turned off) or SIM card, depending on the situation. Ideally, the device should be acquired awake and unlocked and always on. Note that for locked devices, the PIN code is protected by the 5th Amendment, but fingerprints may not be protected.

Data Acquisition

Data acquisition is the process of collecting information from mobile devices and related media. This process reduces the possibility of data loss due to damage during storage and transportation or battery drain. Mobile device identification is required at the start of the forensic investigation. Data collection from mobile devices can be done in two ways.

Physical Acquisition: Physical Acquisition is also known as a physical memory dump. This is a technique for capturing all data from a mobile device's flash memory chip. Forensic tools can collect all the rest of the deleted data, including deleted call logs, contacts, media files, GPS locations, passwords, and more. The received data is initially in raw format and cannot be read. Later, some methods are applied to convert the unread data into a readable format.

Logical Acquisition: Logical Acquisition is a bit-by-bit copy of the data from the directories and files that are preset on the file system partition. It is also known as logical extraction. This is a technique to extract files and folders from your mobile phone without deleting the data. However, certain data such as photos, call history, text messages, calendars, videos, etc. Make a copy of the file using a software tool.

Digital evidences that can be extracted from mobile devices are: Call Detail Recording (CDR), Global Positioning System (GPS), app data, SMS, photos and videos (gallery), and contacts.

TOOLS AND TECHNIQUES

Mobile devices are usually connected to workstation using the JTAG or cable connection used for physical extraction and Bluetooth or Cable Connection are used in logical extraction cables or connectors. Forensic specialists or forensic analysts must understand the several types of forensic tools. The classification offers a framework for forensic analysts to compare the acquisition techniques used by different forensic tools to capture data. Tools used in manual extraction are project a phone, EDEC eclipse. Tools used in logical and physical extraction are XRY, oxygen forensic suite, lantern, cellebrite UFED. Tools used in hex dump are XACT, pandora`s box. Tools used in chip-off are iseasamo phone opening tool, FEITA digital inspection station, chip epoxy glue remover.

FUTURE

Mobile forensics is a rapidly evolving field-one that needs to keep pace with the innovations of the tech industry at large. The market share of certain hardware as well as certain operating systems can fluctuate significantly over a short time span,

Correspondence to: Yuri Robeck, Department of Legal Medicine and Forensic Sciences, University of Porto, Porto, Portugal, E-mail: robeckyuri@gmail.com

Received: 04-Jan-2022, Manuscript No. jfb-22-388; **Editor assigned:** 05-Jan-2022, Pre QC No. jfb-22-388 (PQ); **Reviewed:** 13-Jan-2022, QC No. jfb-22-388; **Revised:** 20-Jan-2022, Manuscript No. jfb-22-388 (R); **Published:** 26-Jan-2022, DOI: 10.35248/2090-2697.22.13.388.

Citation: Robeck Y (2022) Brief Note on Mobile Forensics. J. Forensic Biomech. 13:388.

changing the tools and procedures that mobile forensics need to use in order to acquire and analyze a smartphone`s data. Additional security measures, such as two factor authentication on cloud stored data and an increasing level of base layer encryption, add further layers of complexity. A new generation of analytical toolkits and overlapping legislation within the jurisdiction requires expert training for today's mobile forensic investigators. However, mobile forensics isn't just about catching criminals. The learning curve for mobile forensics may be high, but so are the stakes. Truth and justice can be done at earliest.