# Effects of parental controls in the context of Digital Forensics

Degree programme: MAS Digital Forensics & Cyber Investigation

This study examines the influence of parental control functionalities for child accounts on devices such as mobile phones (Android, iPhones) and Windows 11 devices. To investigate this topic, multiple test devices equipped with test accounts were prepared. These devices were imaged using advanced digital forensic imaging tools and subsequently analysed. The study identifies the challenges associated with parental control functions and assesses potential alternative solutions.

## Context

The psychological impact of parental controls has been extensively examined. However, in circumstances where a digital forensic professional is presented with a child's device featuring active parental control functions, the standard imaging and analytical procedures may be hindered. For instance, attempting to image a mobile phone secured with a known PIN and in which the option to enable Developer Mode is unavailable due to child restrictions. This study examines the impact of parental control functions on the digital forensic examination process and explores methods to address these challenges in a forensically sound manner.

## Goal

The objective of this study is to determine whether certain circumstances within the digital forensic imaging process hinder a digital forensic investigation when parental control functions are enabled on a child's device. Furthermore, the study examines the potential impact of these parental control features on the analysis of the imaged content. In conclusion, the study guides digital forensic professionals on managing these restrictions and offers recommendations for handling devices with active parental controls in their professional environment.

## Methodology

The study involves the creation of multiple test devices and accounts for Android (Google accounts), iPhones (Apple accounts), and Windows 11 devices (Microsoft accounts). These devices are configured with child accounts and parental control features activated. For each device, test images are captured both with and without enabled parental controls, utilising various imaging methods such as After First Unlock (AFU), Before First Unlock (BFU), and PIN extractions, conducted in a manner that is digitally forensically sound. The identified issues were documented, and several recommendations were provided for each problem identified. Additionally, after image acquisition, the images were subjected to content analysis. Comparisons were made between the devices used by parents and those used by children, with the differences systematically listed.

## Result

It has been observed that particular challenges arise with activated parental controls during the process of forensic imaging. In the case of iPhones, no restrictions were identified during the study involving the tested devices and accounts. For Android smartphones, AFU and BFU procedures are feasible and recommended for these devices. In the case of an image using the PIN, enabling Developer Mode isn't possible. Regarding Windows 11 devices, imaging performed with the device powered off (cold state) does not produce any impact; however, during live forensic investigations (powered on), some restrictions are encountered because the child account lacks administrative privileges. Furthermore, without administrative rights, it is not possible to retrieve the BitLocker key for cold images. No impact has been observed about the content under analysis.

Selina Märchy