**ZHAW - MAS Informatik**

**MAS Thesis**

**Controlled communication of seized mobile devices in the IT Forensics Unit of Zurich Metropolitan Police**

A controlled network environment that completely blocks the data communication of seized mobile phones and only allows essential communication through whitelisting.

Alexander Wüst

Kronenwis 19

8864 Reichenburg

**Abgabe** [1]

**Betreuer:in** Peter Heinrich

**Abstract**

Dies ist ein Platzhalter-Text. Dies ist ein Platzhalter-Text. Dies ist ein Platzhalter-Text. Dies ist ein Platzhalter-Text. Dies ist ein Platzhalter-Text. Dies ist ein Platzhalter-Text. Dies ist ein Platzhalter-Text. Dies ist ein Platzhalter-Text.

**Table of Contents**

[1. Introduction 1](#_Toc197590663)

[1.1. Preface 1](#_Toc197590664)

[2. Background 2](#_Toc197590665)

[3. Implementation 2](#_Toc197590666)

[4. Analysis / Results 2](#_Toc197590667)

[5. Discussion / ConclusionReferences 2](#_Toc197590668)

[Appendix 4](#_Toc197590669)

[Declaration of Originality 5](#_Toc197590670)

# Introduction

## Preface

Electronic evidence plays a central role in today's criminal prosecution. Almost no criminal proceedings can do without the analysis of digital data - be it data from mobile phones, computers, IoT devices, cloud data and many other data sources. Digital forensics plays a crucial role in this: IT forensic experts prepare the seized devices according to forensic standards to ensure that the data collected can be used in court.

It's important does the collected devices are completely isolated from data networks after seizing them to maintain data integrity. If this is not possible due to security settings, the Zurich Metropolitan Police use a Faraday room[[1]](#footnote-1). This prevents data communication from the mobile phone and data on the device from being changed. As soon as a mobile phone is reconnected to the internet it will updating apps and synchronising data, such as cloud services, messages and other application data and this of course will trigger write processes on the data storage. Also, there is the risk of a remote deletion of the device which needs to be avoided.

A fundamental principle of forensic work is the reproducibility of the results. Once write operations occur on the data storage, this reproducibility can no longer be guaranteed. So it would be clear, establishing a network connection or even simply powering on a device seems not to be a option and needs to be avoided.

However, best practices at the Metropolitan Police Zurich have shown that powering on a device is necessary to verify whether the data acquired by the forensic hardware and software has been processed correctly. A defined protocol is followed to check for any apps or entries that may not have been parsed correctly – In fact there are often problems during parsing in practice. Especially apps just known in Switzerland like “Twint” are not parsed automaticly.

Without powering on the device, still in Airplane mode, it is not possible to detect parsing errors. For example, when no WhatsApp messages are shown at all or to idenfify if any media files such as photos are missing. In recent years, when physical access to a device was possible, like with a known or brute-forced[[2]](#footnote-2) passcode, it has proven useful to use this access to validate the acquisition and ensure no data was lost or misinterpreted during the process. The decribed procedure, although it also causes write operations, but it is considered as essential to ensure a good and complete data acquisition.

It is more and more common that not everything that is accessible on the device is actually saved on the device. Common examples are images and videos that are stored directly on provider servers (cloud). When manuel reviewing chat conversations trough a police investigator, it can happen that the content of chats clearly goes in one direction, but the images and videos taken are missing because they are no longer or have never been stored locally on the device. For example, an image that could be identified as an offence or a prohibited media file containing violence or even child pornography may be missing from the device and because that it will not allow any clear conclusions. Or the communication seems to be clear but the pictures are harmless? So it is important to give during a search the best possible picture. But how to gain these extra information without getting the device online? The best way is to access the data directly with a cloud acquisition method. For this method the service needs to be supported and a valid token needs to be extracted from the device. Sometimes even that method is not possible due to different reasons. Then it will normaly give a consultation between the public prosecutor, the police officer who is in charge for the case and the forensic examiner. One of the biggest problems is the possibility of a remote deletion when taking the device online. As the acquiring trough forensic hard- and software took already place it will still possible to have the original copy of the state of the device when it was seized.

Actually there is no easy solution that makes it possible to take a device online in a controlled environment without risking the remote deletion of data and at the same time only allowing the really necessary connections to the Internet. This MAS thesis aims to close this gap.

## Goal of the work

Reference to use cases…

## What the work contains and what it will not contain scope

# Background

## Evolution of Firewalls

### Existing Firewalls

### Comparison of firewalls like pfSense, OPNSense just iptables/nftables or also commercial ones like Fortinet or Palo Alto.

## Remote wipe

### Apple iOS

### Google Android

# Implementation

# Analysis / Results

# Discussion / ConclusionReferences

Mohler, M. (2008). *Der Faradaysche Käfig*. https://lp.uni-goettingen.de/get/text/833

# Appendix

Hier sind die in der Arbeit referenzierten Anhänge aufzuführen.

# Declaration of Originality

Bitte Wortlaut aus «Merkblatt Erstellung Abschlussarbeit in CAS, DAS und MAS» übernehmen.

1. Faraday room or Faraday cage, which prevents communication from or into the room. A great and quite simple setup was made by the University of Gottingen (Mohler, 2008). [↑](#footnote-ref-1)
2. Brute force refers to methods that systematically attempt all possible passcode combinations. [↑](#footnote-ref-2)