

Guidelines for Vehicle Forensics in Law Enforcement

Degree programme : MAS Digital Forensics & Cyber Investigation

What route did the perpetrator take? Did they park near the scene of the crime? How many people were present when the crime was carried out? With whom did the perpetrator possibly have contact? Questions like these can be answered with forensic methods. But what does it take to do vehicle forensics? This thesis aims to answer these questions and to support police authorities in the implementation of vehicle forensics.

Context

In addition to traditional digital forensics, more and more other areas are emerging, such as IoT forensics or vehicle forensics. However, the diversity in the vehicle industry poses a great challenge for police authorities. In addition to knowledge about digital forensics, it also requires knowledge about car mechanics and electronics. Special tools, equipment, and maybe even a car lift are needed. A general overview or guideline describing where to start when doing vehicle forensics, what it takes and what needs to be considered is currently missing.

Goal

The aim of this master thesis is to create such a guideline for vehicle forensics for police departments. The guideline should cover topics such as the procedure, required equipment, acquisition of knowledge, available software and tools, but also possible contact persons and investigation approaches. It is intended to be an aid for police agencies that would like to introduce vehicle forensics at their facilities.

Methodology

In order to write the guideline as close to practice as possible, in addition to researching specialist literature, interviews and exchanges of experience with authorities that have been conducting vehicle forensics for a long time were the main focus. The interviews took place mostly on site and also to get a visual impression on the topic of vehicle forensics. The interviews took place with foreign authorities and companies like Europol, Trend Micro and the Netherlands Forensic Institute, as well as with domestic authorities like the Zurich Cantonal Police or the NCSC.

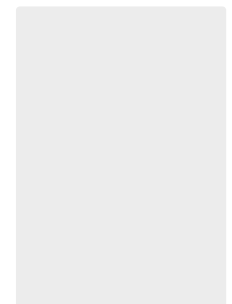
Result

The result of this master thesis is the „Guidelines for Vehicle Forensics in Law Enforcement“. The structure of the thesis is based on the „Harmonized

Digital Forensic Investigation Process“ by Aleksandar Valjarevic and Hein S. Venter from the University of Pretoria.

It describes the Identification Process, which shows how the acquisition of data is planned and what equipment is required. The Acquisitive Process describes the procedure at the location where the vehicle was found or at the scene of the crime. It describes what needs to be documented during the acquisition, what is volatile data, what are possible locations for digital evidence and what information (e.g. connected cell phones, POI from the navigation device, seat occupancy, etc.) can be found. Software such as Berla and its capabilities, as well as possible dangers when removing vehicle components and transporting vehicles, are explained.

The Investigative Process will highlight what tools are available to analyze the data. What challenges exist in terms of diversity in the vehicle market and what options are available to deal with this diversity. A hugely important issue with this topic is the sharing between police agencies. The Guideline also provides an overview of possible contacts with a lot of experience in the field of vehicle forensics.



Saskia Deborah Jessica Held