A Generalized Approach to Automotive Forensics

By:
Kevin Klaus Gomez Buquerin, Christopher Corbett, and Hans-Joachim Hof

From the proceedings of
The Digital Forensic Research Conference
DFRWS EU 2021
March 29 - April 1, 2021

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment.
As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.
https://dfrws.org

DFRWS 2021 VIRTUAL EUROPE

A Generalized Approach to Automotive Forensics

KEVIN GOMEZ BUQUERIN

CHRISTOPHER CORBETT

HANS-JOACHIM HOF

30.03.2021

Motivation and Contribution

- New regulations, business and service models
- Increasing attack surface
- Attraction of security researchers and attackers

<u>Contributions</u>

- Presentation of stakeholders and scenarios for automotive forensics
- Presentation of available data classes of as well as their significance for forensic investigations
- Presentation, implementation, and evaluation of a general process to perform digital forensic investigations without additional extensions

Automotive Digital Forensics

- Utilization of digital forensic techniques and methods on automotive-related systems
- In-vehicle components, manufacturer IT, consumer electronics, and C2X
- Who, why, where, when, what, and how

<u>Stakeholders:</u>

- Insurer
- Legal Entity
- Manufacturer
- Supplier
- Customer/Car Owner

Automotive Digital Forensics

- Firmware
- Communication data
- User data
- Safety-related data
- Security-related data

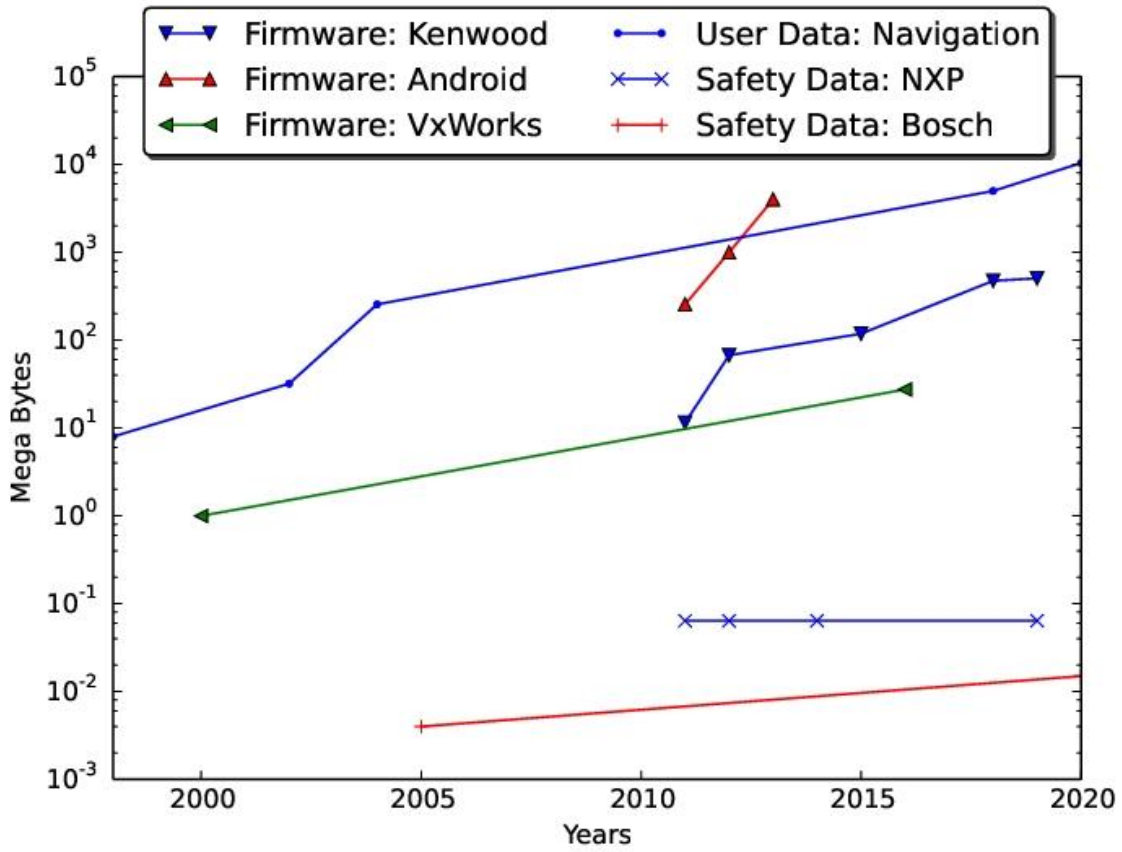

Figure 1: Growth of size for several examples of data found to be useful for automotive forensics.

Automotive Digital Forensics Process

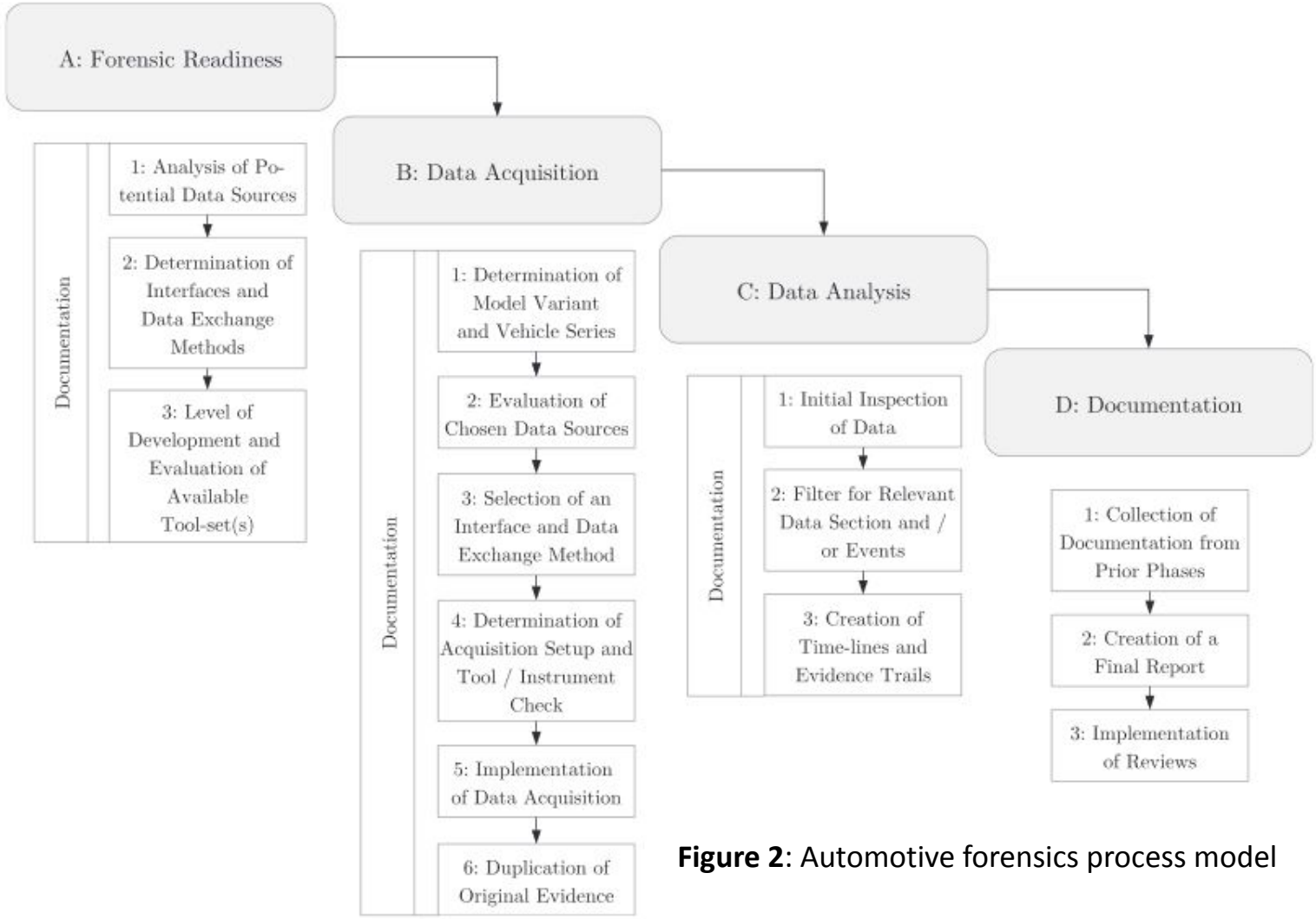

Figure 2: Automotive forensics process model

Implementation

- Scenario: Software or hardware manipulation
- Attacker model: OBD dongle installed in the vehicle
- Python framework implementing UDS and DoIP standards
- Network captures using Wireshark and LUA dissector

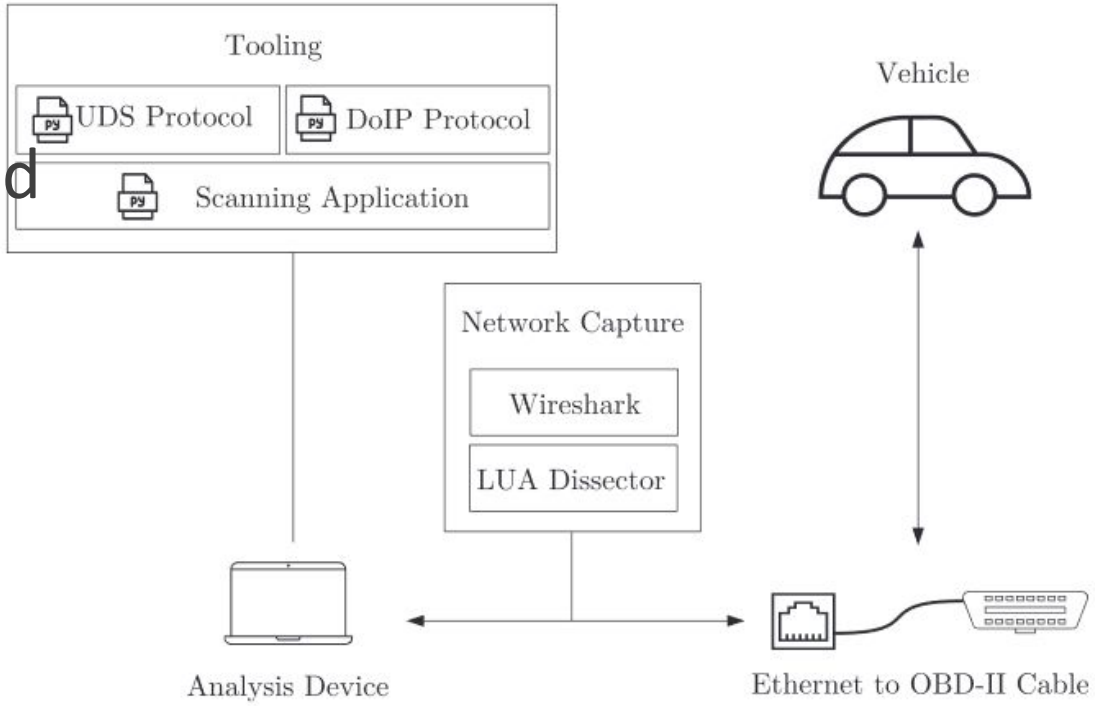

Figure 3: Data acquisition setup

Implementation

- Captured 3800 packets
- Filter for positive responses decrease to 245 packets
- Filter for manipulation-specific UDS data identifiers
- No software or hardware manipulation identified

UDS Data Identifier in Hexadecimal	Description
0xf180	bootSoftwareIdentificationDataIdentifier
0xf181	applicationSoftwareIdentificationDataIdentifier
0xf183	bootSoftwareFingerprintDataIdentifier
0xf184	applicationSoftwareFingerprintDataIdentifier
0xf198	repairShopCodeOrTesterSerialNumberDataIdentifier
0xf199	programmingDateDataIdentifier
0xf19a	calibrationRepairShopCodeOrCalibrationEquipmentSerialNumberDataIdentifier

Figure 4: UDS data identifier relevant for software or hardware manipulation

Evaluation

- Publicly available resource must be enriched with internal information or reverse engineering
- VIN, OBD, DoIP, and UDS are standardized
- Python framework is academic code and offers limited capabilities
- No tamper-proof storage in modern vehicles
- Cross-domain or cross-components effects were not viewed

Conclusion and Future Work

- Presented data classes relevant for forensic analysis
- Presented a generalized model for automotive forensic investigations
- Implemented model on a state-of-the-art vehicle

Future work

- Additional methods of forensic feature extraction for vehicles
- Solve stated gaps and evaluated solutions

DFRWS 2021 VIRTUAL EUROPE

Thank you for your attention!

(Automotive) Digital Forensics

https://www.soscisurvey.de/automotive-data-formats/

@kgbuquerin

www.kgbuquerin.com

extern.kevinklaus.gomezbuquerin@thi.de