FoRePlan: Supporting Digital Forensics Readiness Planning for Internet of Vehicles

CHRISTINA KATSINI, Industrial Systems Institute, Athena Research Centre, Greece
GEORGE E. RAPTIS, Industrial Systems Institute, Athena Research Centre, Greece
CHRISTOS ALEXAKOS, Industrial Systems Institute, Athena Research Centre, Greece
DIMITRIOS SERPANOS, University of Patras and Computer Technology Institute & Press "Diophantus", Greece

The massive amount of data collected by the connected and autonomous vehicles can be used as digital evidence for investigating cyber-attacks, identifying vulnerabilities and providing response and recovery solutions to increase the security in the Internet-of-Vehicles ecosystems. In this respect, the investigation of digital incidents, (e.g., cyber-attacks) requires setting appropriate digital forensics readiness plans for screening data and acquiring those that are more relevant to the incident. Aiming to support the process of creating and executing digital forensics readiness plans, in this paper, we present *FoRePlan*, which provides the security experts with means to prepare, manage, and execute customized digital forensics readiness plans tailored to the detected attacks in Internet-of-Vehicles ecosystems.

CCS Concepts: • **Security and privacy** → *Usability in security and privacy*; • **Applied computing** → **Computer forensics**; • **Software and its engineering** → *Designing software*;

Additional Key Words and Phrases: Cybersecurity, Digital Forensics Readiness, Plans, Internet of Vehicles (IoV)

ACM Reference Format:
Christina Katsini, George E. Raptis, Christos Alexakos, and Dimitrios Serpanos. 2021. FoRePlan: Supporting Digital Forensics Readiness Planning for Internet of Vehicles. *ACM Trans. Graph.* 37, 4, Article 111 (August 2021), 8 pages. https://doi.org/XX.XXXX/XXXXXXX.XXXXXXX

1 INTRODUCTION

Nowadays, rural and urban environments are transforming to smart contexts, with smart mobility being an important aspect. A fast growing sector of smart mobility is the use of connected and autonomous vehicles (CAVs). CAVs acquire, process, and analyze multifaceted data from the surrounding environment, and thus, they navigate with limited or even no human intervention. As a result, Internet-of-Vehicles (IoV) networks are built. IoV networks are dynamic ecosystems that include various types of communication, such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), and Vehicle-to-Pedestrian (V2P).

IoV is a challenging domain, because it features dynamic topological structures, huge network scalability, non-uniform distribution of components, complex granularities, and mobile limitations [16]. Focusing on CAVs, they are

Authors' addresses: Christina Katsini, Industrial Systems Institute, Athena Research Centre, Patras, Greece, katsini@isi.gr; George E. Raptis, Industrial Systems Institute, Athena Research Centre, Patras, Greece, graptis@isi.gr; Christos Alexakos, Industrial Systems Institute, Athena Research Centre, Patras, Greece, alexakos@isi.gr; Dimitrios Serpanos, University of Patras and Computer Technology Institute & Press "Diophantus", Patras, Greece, serpanos@isi.gr.

Manuscript submitted to ACM

vulnerable to attacks of diverse types (e.g., attacks on autonomous control systems, attacks on autonomous driving system components, attacks on vehicle-to-everything communications [5]). Their confrontation is critical, considering that such vulnerabilities can put human safety at risk and have a negative impact on the quality of life.

Towards this direction, nIoVe[1], which is a cybersecurity framework for the IoV ecosystem, enables the identification of risks associated with the IoV networks, the recognition of suspicious threat patterns, and the appropriate coordinated mitigation actions in order to pertain vehicle safety and security. Moreover, it supports the digital forensics readiness procedure, and thus, it ensures that necessary forensic information will be collected and used as a knowledge base for the cyber-attacks in CAVs and IoV ecosystems.

A vital part of this process is the development and execution of digital forensic readiness plans, which must be established proactively (i.e., before the occurrence of an attack or a suspicious activity) aiming to facilitate a cost-effective and efficient investigation [13] without interrupting the smooth operation of the IoV ecosystem. Therefore, it is important to provide the security experts with a tool that will enable them to create digital forensics readiness plans and support their execution to automate the data acquisition/preservation processes and speed up the investigation procedure. Towards this end, in this paper, we present the design of *FoRePlan* that supports the management of customized digital forensics readiness plans for IoV, which are executed when an intrusion has been detected.

The rest of the paper is organized as follows. We first provide background information, then, we review the related work, and identify the gap in the literature. Next, we present the design, implementation, and evaluation of *FoRePlan*. Finally, we provide a discussion about our approach, discuss the future steps, and conclude the paper.

2 BACKGROUND AND RELATED WORK

In this section, we discuss the nIoVe framework and the digital forensics readiness procedure, with a special focus on the planning.

2.1 nIoVe Framework

The nIoVe framework aims to implement a holistic cyber-security solution for IoV networks, with a primary focus on CAVs [18]. A core aspect is the real-time and post-incident investigation of the attack, aiming to identify the cause, the motives, and the characteristics of the attack, to fulfill legal requirements, to determine the cost of the attack and compliance with regulations, etc. Hence, the Attack Attribution and Digital Forensics Readiness Tool (AAFRT) has been developed to allow security experts to perform post-incident analysis of an incoming attack [1]. AAFRT supports two main functionalities:

- *Attack Attribution* [12], which attempts to identify indicators of compromise, aiming to help security experts to attribute the incoming attack to known threat actors by identifying common tactics, techniques, and procedures, with the use of machine learning approaches, and
- *Digital Forensics Readiness* [1], which attempts to automatically collect digital forensics relative data and to create a forensics investigation report with all the necessary information, while preserving the soundness and integrity of the acquired data and maintaining a valid chain of custody.

In IoV, a major challenge is the heterogeneity of the connected devices, which manage and share different types of information while communicating through diverse protocols. Therefore, customized digital forensics readiness plans should be prepared that would be selected and executed when specific attacks are detected. Such plans should enable the

[1]nIoVe is a EU-funded project that provides a novel adaptive cyber-security framework for IoV — website: https://www.niove.eu/

acquisition, preservation, and preliminary analysis of the attack-related data, so that not only the attack is confronted but also the vulnerability is communicated to the various IoV stakeholders to ensure that it is successfully remedied. Considering their importance, in the following sections we discuss the digital forensics readiness process, with a special focus on planning.

2.2 Digital Forensics Readiness for IoV

Digital forensics is an evolving domain, which can be defined as the coupling of computer/information systems knowledge with legal knowledge, aiming to analyze, in a legally acceptable manner, digital evidence that have been acquired, processed, and stored. Digital forensics are mainly used for investigations with legal or law enforcement issues, which are likely to end up in court. Hence, there is an emphasis on legal acceptability. Considering that digital evidence is volatile and can be lost or distorted, there is a need to manage (e.g., acquire, preserve) digital evidence ensuring that it will not be distorted or destroyed. Therefore, digital forensics readiness tools and techniques have been developed (e.g., [14, 15]) to acquire, preserve, and analyze evidence that can be used by an organization against other entities or to defend their assets.

Focusing on the IoV ecosystem, the conventional forensics are not suitable, due to the mobility of the IoV entities, the distributed nature of the infrastructure, and the massive amount of the potential evidence that can be generated from such a complex ecosystem [7]. Nilsson and Larson [9] provided a list of requirements for detection, data collection, and event reconstruction for in-vehicle networks. Hossain et al. [3] introduced *Trust-IoV*, a forensic investigation framework for IoVs. Trust-IoV consists of two services: i) Forensics Gateway, which in embedded in the IoV entities and is responsible for logging all incoming and outgoing interactions, and ii) IoV-Forensic Service, which is responsible for storing the data and provides read-only access to the evidence. Apart from interaction data, data from infotainment systems also store information relevant to forensics investigation [6]. Feng et al. [2] introduced a model for collecting and preserving incident data from automated vehicles. They raised the issue of the easiness of altering evidential data in vehicular forensics and they proposed the use of hashing and encryption for ensuring data integrity.

2.3 Forensics Readiness Planning

An core part of forensics readiness is the process of *planning*. According to Valjarevic and Venter [17] and ISO/IEC 27043:2015, planning can be identified in various sub-processes such as planning incident detection (i.e., the plan is prepared by defining the actions that must be performed when an incident is detected) and implementing incident detection (i.e., the plan for a specific incident is executed upon the detection of that incident). Therefore, we could say that planning consists of three main sub-processes: preparation of the plan, selection of the appropriate plan when an incoming attack is detected, and execution of the plan.

While planning is considered a key to forensic success [10], a few works deal with digital forensics readiness planning: Pooe and Labuschagne [11] used cognitive approaches for digital forensic readiness planning, Luthfi and Prayudi [8] included incident response planning as part of a digital forensics readiness scheme for recommendation of evidence preservation, Kebande and Venter [4] included planning as part of their comparative analysis of digital forensic readiness models. Considering the importance of planning the digital forensics readiness procedure and given the importance of acquiring the required data from a complex IoV ecosystem on time and without the risk of overwhelming the network with requests of massive volume of data transfers, in this paper, we present *FoRePlan*, which is a tool that supports the digital forensics readiness planning for IoV by providing the security experts with means to prepare, manage, and execute customized plans tailored to the characteristics of the detected attacks.

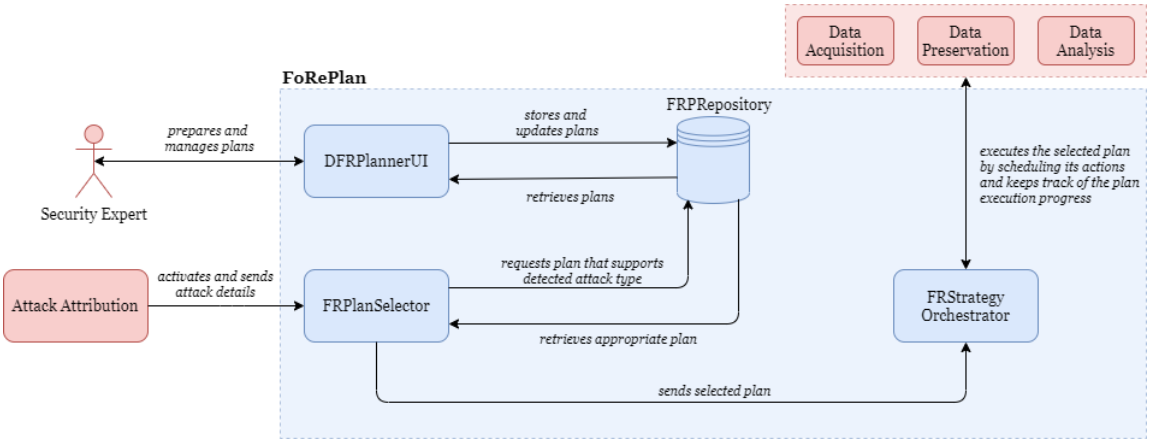

Fig. 1. Conceptual architectural model of *FoRePlan*.

3 FOREPLAN

3.1 Design

FoRePlan aims to support the digital forensics readiness planning for IoV environments. The support is active during the preparation, selection, and execution of the plans. These activities are supported by three different sub-components of *FoRePlan*: i) *FRPlannerUI* is used for the preparation of the plans; ii) *FRPlanSelector* is used for the selection of the appropriate plan when an incoming attack is detected; iii) *FRStrategyOrchestrator* is used for the execution of the selected plan. To ensure the functionality of *FoRePlan*, *FRPRepository* is used, which is a repository that stores the digital forensics plans for diverse attack types. Figure 1 depicts the conceptual architecture of *FoRePlan*. The next sections discuss the aforementioned components.

FRPlannerUI. This component aims to enable the security expert to prepare and manage digital forensics readiness plans. It features a graphical user interface (GUI), allowing them to create, view, update, and delete plans. Through the GUI, the security expert can schedule specific actions to be executed when an attack is taking place in the IoV system. *FoRePlan* supports a wide range of attacks including Denial-of-Service on the CAN bus, alteration of camera stream both in-vehicle and outside of vehicle, GNSS or RTK/NTRIP spoofing, GNSS or RTK/NTRIP jamming, Jamming of V2X signals, Spoofing of V2X signals, malware detection, Man-in-the-Middle, and sensor false reading. The actions that must be scheduled include the acquisition and preservation of different types of evidence, such as vehicle log data, malware file, memory dump, vehicle network analysis, sensor raw data, and vehicle route. The security expert must also select the IoV component that will provide the requested data. The source components include CAN bus, on-vehicle camera, GNSS, lidar, network, on-board unit (OBU), road-side unit (RSU), sensor, supervision center, and in-vehicle computer. Moreover, the security expert has the option to apply sequential, parallel, or mixed scheduling for the selected plan actions. Besides the scheduling, the security expert chooses a name for the plan and sets it as active or inactive. The digital forensics plans are stored in *FRPRepository*.

FRPRepository. It is a repository that keeps the digital forensics plans for diverse attack types. As discussed in the previous section, each plan is characterized by the supported attack type, its status, a series of actions and commands

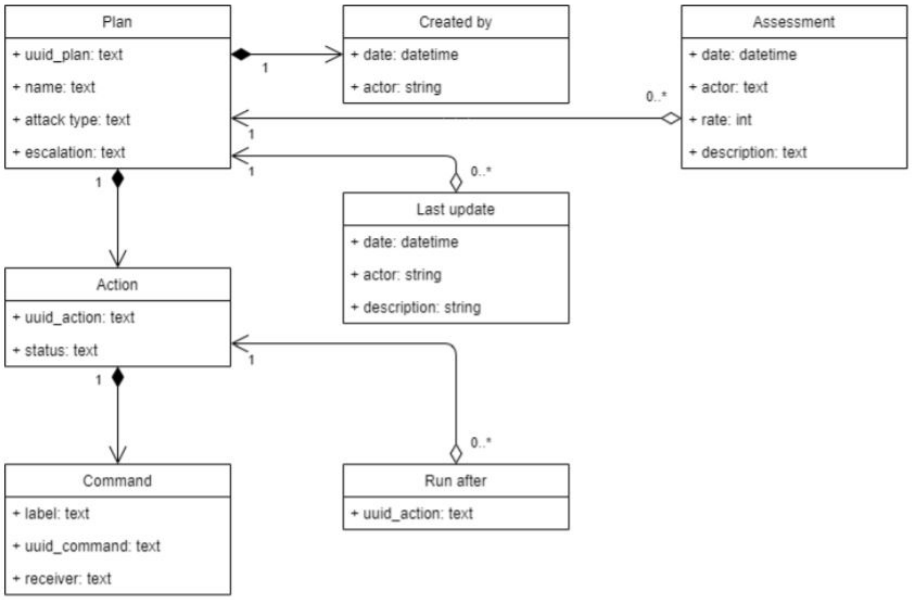

Fig. 2. The data model of the forensics readiness plan.

that are scheduled to take place sequentially, in parallel, or using a combination of them and target a specific component of the IoV ecosystem. Moreover, to have a clearer picture on the plans, information about the security expert who created and/or updated each plan is stored along with information about the date and time of any adjustment actions made. After an attack is identified and a plan is executed (we will discuss it next), *FoRePlan* provides the security experts with the opportunity to assess the plan (i.e., how effective the plan was for the specific forensics readiness process); this information is also stored to the repository. Figure 2 depicts the data model for the plans stored in *FRPRepository*.

FRPlanSelector. This component initiates when an attack is detected and attributed in the IoV system. It is responsible for selecting the appropriate digital forensics readiness plan. In particular, it receives the detected attack profile as input and then, based on the attack, it retrieves the most suitable plan from *FRPRepository*. In case that a plan matches the attributes of the detected attack, then it is retrieved and it is sent to *FRStrategyOrchestrator* to be executed. *FRPlanSelector* also forwards system-specific metadata (e.g., vehicle id, sensor id) to specify the IoV components for which the plan will be executed.

FRStrategyOrchestrator. This component initiates after a digital forensics readiness plan is selected. It is responsible for the proper execution of the selected plan. To achieve this, the data acquisition, preservation, and analysis actions targeted to the corresponding IoV providers are scheduled carefully aiming to ensure the minimization of the cost of response, recovery, and investigation without interrupting the normal operation of the IoV ecosystem. Various types of communication (e.g., requests) are made with other IoV components during the execution of the selected plan. Moreover, this component is responsible for keeping track of the progress of the requests sent to or received from external components and the required actions.

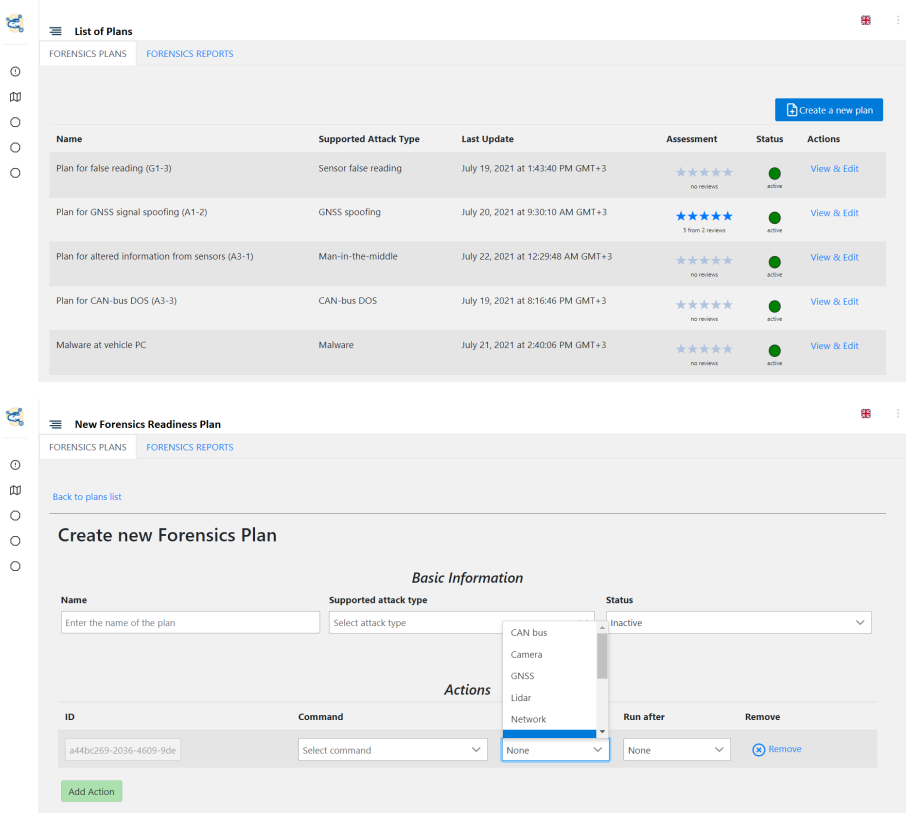

Fig. 3. The security expert can view all the available forensics readiness plans (top) and can prepare new plans for specific attack types (bottom).

We should note that the actions performed throughout the digital forensics readiness planning procedure are tracked. In particular, throughout *FoRePlan* processes, a MISP-based threat intelligence platform updates the current event with information (e.g., objects, relationships) about the planning procedure (e.g., which plan is selected, plan performance). This would allow the analysis, extraction, and sharing of information with other IoV systems and speed up future investigations and mitigation activities.

3.2 Implementation

To implement *FoRePlan*, a wide range of technologies were used: `Angular` was used for the development of the web-based GUI of *FRPlannerUI*; *FRPRepository* is based on `MongoDB`; `Flask` was used as the core web framework; `RabbitMQ` was used as the message-broker for the communication between the components; `Celery` was used to schedule the required plan actions sequentially or in-parallel; `Python` was used as the main programming language for most of the processes implemented in *FoRePlan*. Figure 3 depicts two screenshots of the implementation of the *FRPlannerUI* component of *FoRePlan*.

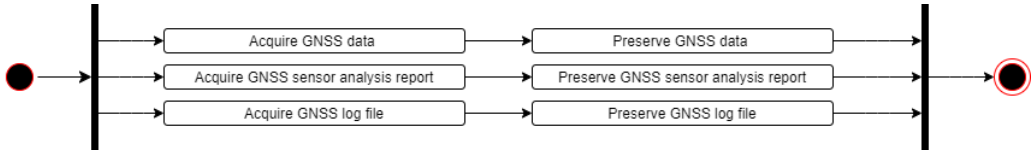

Fig. 4. The plan for the acquisition and preservation of data when GNSS signal spoofing is detected.

3.3 Performance Evaluation

To evaluate the performance of *FoRePlan*, a testbed was executed in the deployed infrastructure. In this testbed, the performance was evaluated in terms of task completion and time of executing the *FoRePlan* operations. This was achieved by measuring the time taken for each message to be consumed by each component and the time taken for the processes that were performed in each component. For the evaluation, a series of ten experiments were performed. In all experiments, the plans were retrieved and executed successfully with no issues noticed. The mean time for *FRPlanSelector* performance was $6ms$ and for *FRStrategyOrchestrator* it was $41ms$. *FRPlanSelector* was activated in $2ms$, *FRStrategyOrchestrator* in $2ms$, and the processes followed were activated in $1ms$. We experimented with various scenarios, such as GNSS signal spoofing (Figure 4), sensor false reading, vehicle camera stream alteration, and denial of service on CAN bus, with *FoRePlan* having a high performance.

4 DISCUSSION

In this paper, we presented the design, implementation, and performance evaluation of *FoRePlan*, a tool that aims to support the digital forensics readiness planning within IoV ecosystems when a threat (e.g., cyber-attack) is detected. *FoRePlan* is part of a larger cyber-security solution of the nIoVe framework. Its contribution is two-fold: i) from a legal perspective, the plans that are prepared, selected, and executed ensure that the data acquired and preserved are forensically sound and that they validate and reconstruct an incident so that it can be presented at court, and ii) from a technological perspective, the selection and execution of the plans are completed transparently, with no human intervention, and in real time, enabling the IoV system to respond effectively and instantly to an incoming attack. The success of the digital forensics readiness is highly dependent on the timing, which is a crucial parameter for safety and security critical systems, such as the ones developed for IoV. Minimization of the timings leads to higher performance of response, recovery, and investigation processes, aiming both to return the under-attack IoV system to a previous safe, stable, and functional state and to ensure a sound digital forensics readiness process.

As a final remark, we should note that *FoRePlan* incorporates a human-centered philosophy, as it engages security experts to prepare and manage digital forensics readiness plans that will be selected and executed when an attack is detected. Through *FoRePlan*, the security experts can adjust any plan to meet the unique requirements of each threat identified in IoV, such as attack type, action to take place (e.g., preserve data), type of data (e.g., GNSS data), and source of the data (e.g., in-vehicle camera). Moreover, the security experts can assess the plan after the investigation (e.g., assess whether the identified evidence was suitable), aiming to review how well the plan fitted to a specific attack type and to improve the forensics readiness process in the future. In this paper, we evaluated the performance of *FoRePlan* and ensured that it performed well transparently with minimum timing cost. As a direct future step, we aim to evaluate the use of the *FRPLannerUI* component of *FoRePlan* from security experts though a user study.

5 CONCLUSION

In this paper we presented *FoRePlan*, a tool for creating and automatically selecting and executing digital forensics readiness plans for an IoV ecosystem. We presented its design, implementation, and performance evaluation. *FoRePlan* provides the security experts with means to prepare, manage, and execute customized digital forensics readiness plans tailored to the detected attacks in Internet-of-Vehicles ecosystems.

ACKNOWLEDGMENTS

We acknowledge support of this work by the European Union (EU) Horizon 2020 research and innovation programme nIoVe: A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles under grant agreement No 833742.

REFERENCES

[1] Christos Alexakos, Christina Katsini, Konstantinos Votis, Antonios Lalas, D. Tzovaras, and Dimitrions Serpanos. 2021. Enabling Digital Forensics Readiness for Internet of Vehicles. *Transportation Research Procedia* 52 (2021), 339–346. https://doi.org/10.1016/j.trpro.2021.01.040 23rd EURO Working Group on Transportation Meeting, EWGT 2020, 16-18 September 2020, Paphos, Cyprus.

[2] X. Feng, E. S. Dawam, and S. Amin. 2017. A New Digital Forensics Model of Smart City Automated Vehicles. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 274–279.

[3] Md Mahmud Hossain, Ragib Hasan, and Shams Zawoad. 2017. Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV).. In *ICIOT*. 25–32.

[4] Victor Rigworo Kebande and Hein S. Venter. 2019. A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. 1, 6 (June 2019). https://doi.org/10.1002/wfs2.1350

[5] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, and Huy Kang Kim. 2021. Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense. *Computers & Security* 103 (2021), 102–150. https://doi.org/10.1016/j.cose.2020.102150

[6] Jesse Lacroix, Khalil El-Khatib, and Rajen Akalu. 2016. Vehicular Digital Forensics: What Does My Vehicle Know About Me?. In *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications* (Malta, Malta) *(DIVANet '16)*. Association for Computing Machinery, New York, NY, USA, 59–66. https://doi.org/10.1145/2989275.2989282

[7] Nhien-An Le-Khac, Daniel Jacobs, John Nijhoff, Karsten Bertens, and Kim-Kwang Raymond Choo. 2020. Smart vehicle forensics: Challenges and case study. *Future Generation Computer Systems* 109 (2020), 500 – 510. https://doi.org/10.1016/j.future.2018.05.081

[8] Ahmad Luthfi and Yudi Prayudi. 2015. Process Model of Digital Forensics Readiness Scheme (DFRS) as a Recommendation of Digital Evidence Preservation. IEEE. https://doi.org/10.1109/cybersec.2015.31

[9] Dennis K Nilsson and Ulf E Larson. 2009. Conducting forensic investigations of cyber attacks on automobile in-vehicle networks. *International Journal of Digital Crime and Forensics (IJDCF)* 1, 2 (2009), 28–41.

[10] Mark Pollitt. 2016. The key to forensic success: examination planning is a key determinant of efficient and effective digital forensics. Elsevier, 27–43. https://doi.org/10.1016/b978-0-12-804526-8.00002-2

[11] Antonio Pooe and Les Labuschagne. 2013. Cognitive Approaches for Digital Forensic Readiness Planning. Springer Berlin Heidelberg, 53–66. https://doi.org/10.1007/978-3-642-41148-9_4

[12] George E. Raptis, Christina Katsini, and Christos Alexakos. 2021. Towards Automated Matching of Cyber Threat Intelligence Reports based on Cluster Analysis in an Internet-of-Vehicles Environment. IEEE. https://doi.org/10.1109/csr51186.2021.9527983

[13] Robert Rowlingson et al. 2004. A ten step process for forensic readiness. *International Journal of Digital Evidence* 2, 3 (2004), 1–28.

[14] Nikolaos Serketzis, Vasilios Katos, Christos Ilioudis, Dimitrios Baltatzis, and George J. Pangalos. 2019. Actionable threat intelligence for digital forensics readiness. 27, 2 (June 2019), 273–291. https://doi.org/10.1108/ics-09-2018-0110

[15] Andrii Shalaginov, Asif Iqbal, and Johannes Olegård. 2020. IoT Digital Forensics Readiness in the Edge: A Roadmap for Acquiring Digital Evidences from Intelligent Smart Applications. Springer International Publishing, 1–17. https://doi.org/10.1007/978-3-030-59824-2_1

[16] Yunchuan Sun, Lei Wu, Shizhong Wu, Shoupeng Li, Tao Zhang, Li Zhang, Junfeng Xu, Yongping Xiong, and Xuegang Cui. 2016. Attacks and Countermeasures in the Internet of Vehicles. *Annals of Telecommunications* 72, 5-6 (Nov. 2016), 283–295. https://doi.org/10.1007/s12243-016-0551-6

[17] Aleksandar Valjarevic and Hein S. Venter. 2015. A Comprehensive and Harmonized Digital Forensic Investigation Process Model. 60, 6 (Aug. 2015), 1467–1483. https://doi.org/10.1111/1556-4029.12823

[18] Angeliki Zacharaki, Ioannis Paliokas, Konstantinos Votis, Christos Alexakos, Dimitrios Serpanos, and Dimitrios Tzovaras. 2019. Complex Engineering Systems as an Enabler for Security in Internet of Vehicles: The nIoVe Approach. In *2019 First International Conference on Societal Automation (SA)*. IEEE, 1–8. https://doi.org/10.1109/SA47457.2019.8938044