Analysis of Data Tampering Possibilities and Attack Techniques for EDR Data[*†]

Suji Lee[1], Daul Jeon[1], Junsik Yoon[1], Samuel Woo[2], and Yousik Lee[1]

[1] Soonchunhyang University, Asan, Republic of Korea
{dltnwl0531, ekdnf0721, yjs20, yousik.lee}@sch.ac.kr
[2] Dankook University, Gyeonggi-do, Republic of Korea
samuelwoo@dankook.ac.kr

Abstract

The Event Data Recorder (EDR) records vehicle status and motion during traffic accidents, serving as critical data for accident reconstruction. This study analyzes potential threats to EDR data integrity and demonstrates data manipulation possibilities through ACU reset and direct memory access techniques. We propose a five-stage methodology for analyzing EDR data tampering and conduct experiments, contributing to automotive forensic methodologies.

Keywords: Event Data Recorder (EDR), Data tampering, Data integrity

1 Introduction

An Event Data Recorder (EDR) is a device designed to capture vehicle movement and status during specific events, such as traffic collisions. According to UN No. 160, EDRs are required to record all relevant data elements when predefined trigger conditions are satisfied [2]. The analysis of EDR data facilitates the identification of crash causes and supports efforts to improve vehicle safety. Farrugia et al. noted that EDR data becomes locked after airbag deployment, preventing ACU reuse [1]. However, read counters can be matched with MCU power supply counters to enable ACU reuse [3], allowing individuals to reset and reuse ACUs, raising data integrity concerns. Given that ACUs can be reset and reused, this study demonstrates that EDR data integrity can be compromised, enabling potential data manipulation. We propose a five-stage methodology and conduct direct manipulation experiments to provide concrete evidence of EDR vulnerabilities, contributing to enhanced automotive forensic methodologies.

2 Methodology

This study presents a systematic five-stage methodology for analyzing EDR data tampering possibilities.

Stage 1: We prepare crash-recorded and clean ACUs for comparative analysis to identify data structures and storage patterns.

Stage 2: We identify the ACU's physical properties, including storage medium type and access interfaces essential for data acquisition.

Stage 3: We focus on data extraction and adopt the chip-off method over diagnostic tools,

[*]This work was supported by the Technology development Program (00402427) funded by the Korea Planning & Evaluation of Industrial Technology (KEIT, Korea)

[†]Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-45, December 16-18, 2025, Sapporo, Japan.

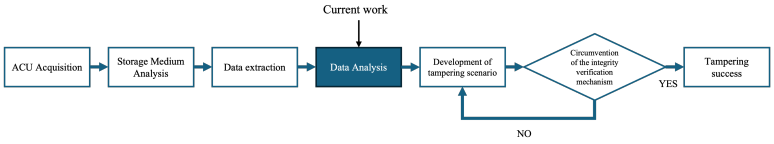


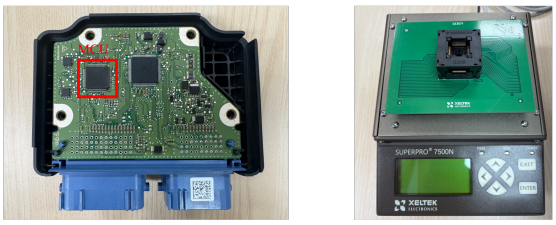
Figure 1: Overview of the research methodology

as it provides access regardless of vehicle condition and enables analysis from an attacker's perspective.

Stage 4: We conduct structural analysis by comparing crash and clean ACU data to identify EDR storage locations within memory.

Stage 5 (In Progress): We craft and write manipulated datasets into identified regions, requiring recalculation of integrity values such as CRC to ensure tampered data appears legitimate (Figure 1).

To validate this methodology, we used an ACU from a Hyundai Sonata (DN8) with SAK-TC233LP-16F200N MCUs and internal flash memory. After chip-off extraction, we utilized a SuperPro 7500N programmer to directly access and acquire data from the memory (Figure 2). Comparative analysis revealed that clean ACUs displayed 0xFF values while crash-recorded ACUs showed specific regions with collision information, enabling us to identify EDR storage locations. We have completed Stages 1-4 and confirmed the feasibility of both reading and writing to memory, indicating that data modification is technically possible. Currently, we are investigating integrity protection mechanisms for Stage 5.



(a) (b)

Figure 2: (a) Target ACU, (b) SuperPro 7500N

3 Results and Conclusion

This study demonstrates that EDR data integrity is vulnerable to ACU initialization and direct memory tampering. Through chip-off analysis, we identified memory structures and demonstrated manipulation feasibility. Results emphasize the necessity for enhanced integrity verification mechanisms and additional security measures, contributing to automotive forensic methodologies and highlighting needs for industry-wide EDR security improvements.

References

[1] R. Farrugia, C. Sammut, and K. P. Camilleri. Synchronization of event data recorder (EDR) data to data from the CAN bus and LabVIEW in emulated non-deployment and deployment laboratory experiments. In *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, pages 1–7, Rhodes, 2020. IEEE.

[2] United Nations Economic Commission for Europe. UN regulation no. 160 – uniform provisions concerning the approval of motor vehicles with regard to the event data recorder, 2021.

[3] YouTube. Airbag crash data reset. https://youtu.be/KzoKndbYgLo, n.d. accessed June 11, 2025.