Forensic Black Box Architecture for Digital Evidence Analysis

Daria Bulgakova
PhD in International Law, An advocate, Kryvyi Rih, Ukraine,
ORCID: https://orcid.org/0000-0002-8640-3622, e-mail: dariabulgakova@yahoo.com

Digital forensics faces challenges of consistently interpreting complex data. Therefore, technically possible alternative meanings need to be considered alongside the main research hypotheses when analysing digital traces. This becomes especially critical in cases involving missing or synthetic data, where the distinction between evidence-based conclusions and theoretical possibilities guarantees the integrity of forensic findings. To practically address the problem, the author proposes an architectural model of a "forensic black box" designed for forensic interpretations. This concept is consistent with Jeong Jong Chan's forensic black box for data validation, which integrates GPS, inertial navigation, OBD2, and visual data to detect and document events in a vehicle-based example, such as collisions. Consistent interpretation of sensor data in such systems relies heavily on the adequacy condition, which requires that two identical data instances do not produce different classifications. Applying this condition in forensic systems enhances logical consistency, supports reliable reconstruction of the incident, and supports the evidentiary value of digital findings in a legal context.

Keywords: *a technically possible alternative meanings; a forensic black box for data proof; data consistency; adequacy condition.*

Архітектура судово-аналітичної «чорної скриньки» під час дослідження цифрових доказів

Дар'я Булгакова

Цифрова криміналістика має проблему послідовної інтерпретації складних даних. Тому під час аналізу цифрових слідів потрібно зважати на технічно можливі альтернативні значення (поряд з основними дослідницькими гіпотезами). Це стає особливо критичним у випадках, пов'язаних із відсутніми або синтетичними даними, де розбіжності між підтвердженими доказами висновками й теоретичними можливостями гарантують цілісність результатів судової експертизи. Для того щоб практично розв'язати проблему, запропоновано архітектурну модель «криміналістичної чорної скриньки», призначену для судово-аналітичних інтерпретацій. Цю концепцію продемонстровано паралельно з ідеєю Jeong Jong Chan про криміналістичну чорну скриньку для підтвердження даних, яка об'єднує GPS, інерціальну навігацію, OBD2 і візуальні дані для виявлення та документування подій на прикладі із застосуванням транспортного засобу (зіткнення). Послідовне інтерпретування даних датчиків у таких системах значною мірою залежить від умови адекватності, яка потребує, щоб два ідентичні примірники даних не створювали різних класифікацій. Застосування цієї умови в системах судової експертизи посилить логічну послідовність, підтримає надійну реконструкцію інциденту й доказову цінність цифрових знахідок у правовому контексті.

Ключові слова: *технічно можливі альтернативні значення; криміналістична чорна скринька для підтвердження даних; узгодженість даних; умова адекватності.*

While traditional forensic sciences have established strong practices for interpreting and communicating findings, digital forensics still lacks development in this area. Due to complex systems and vast amounts of data, digital forensic practitioners must carefully interpret data traces to determine their meaning and value to an investigation. Beyond forming an initial hypothesis, they must also consider and communicate any technically possible alternative meanings of the evidence.

When considering the proposal of a technically possible alternative meanings (TPAMs) in relation to their primary investigative hypothesis regarding a data trace, it is suggested that the practitioner should consider conveying their position in one of six ways; No other possible explanation, a full trace possibility, a partial trace possibility, a documented technical possibility unsupported by available traces, a theoretical technical possibility, and finally, an unknown technical possibility [1, p. 693]. These six categories are proposed both in order to help a practitioner to clarify and express the objective evidence-base from which they have derived and offered a TPAM, whilst also helping those who are seeking to rely upon the practitioner's results to understand why a TPAM has been suggested [1].

These techniques are important. For example, in the case of missing data, synthetic data could fill up the gaps [2, p. 2126]. In such circumstances, indeed denoting between what is firmly backed by evidence and what is merely theoretically potential evolves integral to keeping the blamelessness of the forensic deductions. To improve the credibility and responsibility of digital forensic results, it is suggested a structured interpretive idea on a forensic black box that documents and clarifies the sense behind data renditions. This framework would serve as a diaphanous log of how digital specks were dissected, what direct suppositions were begun, what TPAMs were thought, and how closings were called. By systematically verifying both evidence-based and theoretical chances, predominantly in cases applying sketchy or synthetic data, this bar confirms that the decision-making approach stays reviewable, reproducible, and receptive to scrutiny by investigators, legal practitioners, and courts.

Likewise, the idea of Jeong Jong Chan relates to a forensic black box for data proof which performs position measurement while flying on a flight course, and continuously and periodically transmits location measurement information to provide proof of occurrences of accidents, accident prevention, and accidents [3]. The forensic black box for data proof comprises: an inertial navigation apparatus to use location and elevation information of a GPS receiver as measurements to assist in inertial navigation where errors are accumulated over time to reduce errors of location, speed, and posture information; a GPS receiver to acquire GPS information in real time; OBD2 to acquire data of transportation means; a proof data processing unit which is linked to the inertial navigation apparatus, the GPS receiver, and the OBD2, uses embedded collision analysis software to detect a collision, simultaneously recognizes an image acquired

by a camera unit, airway information acquired by the inertial navigation apparatus, and OBD2 data when a collision is detected to generate forensic proof data, and controls storage and transmission of the forensic proof data; and a proof data storage unit to store the forensic proof data generated by the proof data processing unit [3].

GPS, inertial navigation, OBD2, and cameras are deciphered into forensic finales such as placing a wreck or rebuilding a happening. And, rely upon need mainly on adequacy condition recreating for multiple data streams, likewise, location, speed, posture, vehicle diagnostics, and imagery. Significantly, it needs to constantly stay fused to generate forensic-proof data. At the same time, the proof data processing unit must unfailingly interpret similar sceneries of sensor assignments in the same way quite when determining occurrences like a clash. Hence, the adequacy condition, which remarks that *no two instances with identical attribute values should belong to different classes*, stresses consistency in classification [4, p. 46]. Is a lodestar that's equally compulsory in digital forensics. When a practitioner decrypts digital traces and assume TPAMs, they are virtually typing those traces founded on available evidence and context. It is similar to confirming a machine learning practicum set clings to the sufficiency state. If two similar data traces were solved differently without rationale, it would mirror inconsistency and potentially damage the credibility of the spotting.

Thus, the forensic black box helps enforce a forensic rendition of the adequacy prerequisite by demanding that riffs derived from identical or matching evidential traits be documented, justified, and logically invariant, particularly when TPAMs are evaluated. If the system violates the adequacy condition, then two nearly identical sensor scenarios could be interpreted differently, likewise, one as a collision and one as a non-event, which would compromise the integrity and legal reliability of the forensic evidence. Thus, the adequacy condition ought to only assure data consistency across comparable occasions and validate the variety of logic entrenched in the software, like for collision detection, to stem contradictory outcomes from the same or similar intake data patterns.

References

1. Horsman G. Considering "technically possible" alternative meanings for data traces found during a digital forensic examination. *Australian Journal of Forensic Sciences*. 2023. Vol. 55 (5). Pp. 689–698. DOI: 10.1080/00450618.2022.2071988 (date accessed: 28.03.2025).
2. Vries de K. You never fake alone. Creative AI in action. *Information, Communication & Society*. 2020. Vol. 23 (14). Pp. 2110–2127. DOI: 10.1080/1369118X.2020.1754877 (date accessed: 28.03.2025).
3. Jeong J. Ch. Proof of data forensic black box. Patent No. KR20190107881A. Application No.: KR20180029185 / Patentguru : web. 2019-09-23. URL: https://www.patentguru.com/assignee/jeong-jong-chan (date accessed: 28.03.2025).
4. Bramer M. Principles of Data Mining. 2nd ed. London : Springer, 2013. 344 p. DOI: 10.1007/978-1-4471-4884-5 (date accessed: 28.03.2025).