Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 32s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Maritime Digital Forensics for Blue Economy Sustainability

Dr. Rajesh Kumar[1], Dr. Kavita[2], Dr. Meenakshi Saharan[3]

[1] Assistant Professor, Department of Information, Communication & Technology, Tecnia Institute of Advanced Studies (TIAS), India

Email ID : rajeshasuszen@gmail.com, ORCID: https://orcid.org/0009-0001-9406-1888

[2] Assistant Professor, Department of Commerce, ST.JOSEPHS GIRLS DEGREE COLLEGE - Sardhana) Meerut, India

Email ID: kavita.makhi@gmail.com, ORCID: https://orcid.org/0009-0000-9266-2148

[3] Assistant professor, Department of commerce Mihir Bhoj PG College, Gautam Budh Nagar, India

Email ID: meenakshisaharan2@gmail.com

Cite this paper as: Dr. Rajesh Kumar, Dr. Kavita, Dr. Meenakshi Saharan, (2025) Maritime Digital Forensics for Blue Economy Sustainability. *Journal of Neonatal Surgery*, 14 (32s), 4727-4738.

ABSTRACT

Maritime digital forensics is becoming imperative in protecting marine environments under growing environmental concerns and operational sophistication. This article provides a full review of available forensic technologies—such as extracting data from Voyage Data Recorders (VDRs), Automatic Identification Systems (AIS), and shipboard IoT sensors—and discusses the role of emerging technologies like artificial intelligence for anomaly detection and blockchain for evidence integrity. The review identifies key areas of real-time data integration, scalability, and digital preservation of evidence that hinder adequate environmental protection. Based on these findings, we propose a conceptual framework that unifies digital forensic practices and sustainable maritime operations to encourage incident response, compliance with regulations, and overall stewardship of the environment. While improving marine operation's openness and responsibility towards sustainable development goals, the framework helps to quickly identify and respond to environmental events.

Keywords: *Maritime Digital Forensics, Environmental Sustainability, IoT Sensors, Artificial Intelligence, Blockchain, Incident Response*

1. INTRODUCTION

Particularly as naval operations are driving world trade, maritime digital forensics is progressively a useful tool in protecting our oceans [1]. Digital forensics facilitates examination of offshore accidents—like oil spills, illegal dumping, and cyberattacks on key maritime infrastructure—by recording, analyzing, and preserving digital information from resources like Voyage Data Recorders (VDR), Automatic Identification Systems (AIS), and onboard ship sensors.

A. Background And Motivation

Natural and artificial hazards constantly press the marine environment. In addition to promoting global trade, maritime operations directly affect the environment [2]. In the past few years, several concerns have risen to the forefront:

• Oil spills and the release of pollutants can cause catastrophic ecological loss and long-term environmental damage.

• Discharging illegalities: Environmental non-compliance leads to illegal disposal of hazardous products, which destroy marine life and coastal residents [3].

• Plastic pollution and marine debris: Mismanagement of waste and manufacturing more plastics generate enormous amounts of debris, which chokes marine life and destroys habitats

B. Relevance To Sustainable Development And Emerging Technologies

Digital forensics plays a vital role in ensuring stewardship of the environment by providing real-time monitoring and rapid response to maritime events [4]. The convergence of emerging technologies in the shape of IoT sensors gathering data in real-time, AI-driven analytics for fast anomaly detection, and blockchain-based systems for ensuring the integrity of the data gathered enhances the detection and prevention of damage to the environment before it turns intractable. The convergence of the technology supports instant response to events as well as long-term regulatory compliance and sustainable operations [5]. Digital forensics ensures transparency and accountability by providing accurate, tamper-proof data for adequate environmental protection and sustainable maritime operations.

C. Problem Statement And Research Objectives

Despite the great promise of maritime digital forensics in preserving marine ecosystems, there remain outstanding deficiencies in its application. The current forensic procedures are deficient in integrating real-time data derived from various sources such as Voyage Data Recorders, AIS, and IoT sensors, which hampers the detection of marine events. The maintenance of the chain of custody for digital data and the upscaling of the solutions to cover vast maritime ecosystems is also an area of difficulty in effective regulatory enforcement and remediation. All these vulnerabilities underscore the need for a more effective, unified approach towards enhancing the reliability of forensic investigations as well as the overall stewardship of the marine environment.

This paper bridges those gaps by reviewing existing forensic technologies and practices used in the maritime sector. The research seeks to recommend a conceptual framework leveraging emerging technologies, including IoT, AI/ML analytics, and blockchain, for the improvement of forensic data acquisition, analytics, and preservation. The goal is to show how such a combined approach can promote sustainable maritime operations, regulatory compliance, and more successful attempts at environmental protection. In addition to promoting global trade, maritime operations directly affect the environment.

2. LITERATURE REVIEW

Maritime digital forensics is the analysis of digital data in maritime systems, including VDRs, AIS, and onboard sensors [8], with the aim of helping legal, safety, and environmental investigations. Key methodologies are data extraction, preservation, and analysis—all aimed to help reconstruct events involving collision or environmental offences.

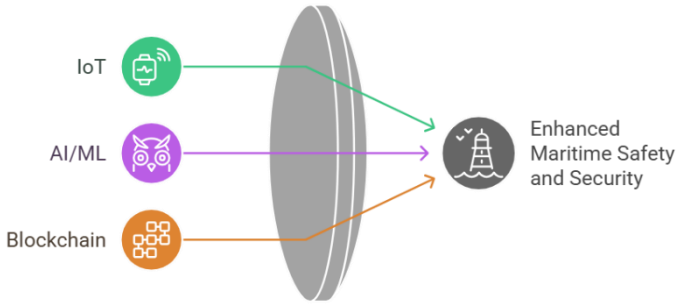

Figure 1. Technologies that can Enhance Maritime Forensics.

Maritime digital forensics employs very sophisticated computer hardware and software to capture, analyse, and archive digital information. Hardware devices include Voyage Data Recorders (VDRs), the ship's "black box," and real-time ship movement-logging AIS receivers. Fuel consumption and water condition sensors are employed onboard as environmental parameters, and data extractors extract data while preserving integrity.

Technologies such as OceanMind and MarineTraffic [6,7] feed AIS and VDR data to monitor for deviation or suspicious activities.

Maritime forensics typically comprises the following four general steps:

I. Data collection: Data extraction by VDRs, AIS, and sensors
II. Data integrity: Implementing chain-of-custody procedures [9].
III. Reconstruction of events.
IV. Reporting: Creating records for business, regulatory, or legal use

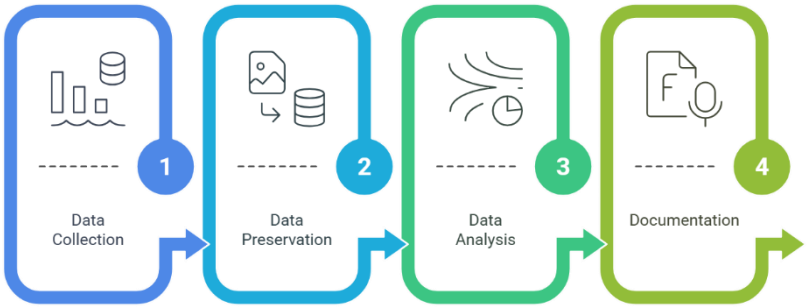

Figure 2. Steps to Effective Maritime Forensics.

A. Practical Applications

Digital forensics has proved to be highly beneficial in maritime investigations, especially in the conservation of the environment. In the 2020 MV Wakashio grounding, for example, VDR data was used to establish the cause of the grounding and oil spill off the coast of Mauritius. The investigation established crew training and navigation deficiencies, leading to stricter regulatory controls.

Another instance is the application of AIS data to combat illegal fishing. Global Fishing Watch uses AIS to track fishing and violations in protection areas [10]. Likewise, during the Deepwater Horizon oil spill, digital forensics was used to recreate the events that led to the disaster. Sensor data and communication data were used to evaluate the environmental damage as well as to allocate blame [11].

They highlight how digital forensics provides actionable intelligence, enables regulatory compliance, and minimises environmental harm.

B. Limitations and Challenges

I. Despite its significant potential, maritime digital forensics faces several limitations and challenges that hinder its effectiveness, particularly in achieving environmental protection goals.

II. Scalability Issues: The marine sector generates enormous volumes of data on worldwide shipping traffic, including sensors onboard, AIS, and VDRs. Especially in real-time, the data is difficult for the present forensic techniques and technologies to handle and investigate. This restricts the capacity to track large fleets or hunt for abnormalities over wide-ranging territory.

III. Challenges in Data Integration: VDRs, AIS, and other maritime systems usually work in isolation, resulting in data silos. Integrating the data from these various sources is resource-intensive and technically challenging. Investigators cannot get a complete overview of incidents or risks in the environment without integration.

IV. Latency in Real-Time Monitoring: Data transmission and processing delays can prevent real-time detection and response to events. For example, detecting an oil spill or illicit discharge in real-time requires rapid data integration and analysis, which most systems cannot deliver.

V. Integrity of Digital Forensic Evidence: The authenticity and admissibility of digital data are a recurring issue. While blockchain technology offers a secure, tamper-proof data repository, its use in maritime forensics is limited. Further, the lack of standardised data collection and acquisition process can create disparities in forensic investigations.

VI. Narrow Environmental Protection Scope: The majority of forensic equipment is designed for the investigation of events, rather than for the proactive monitoring of the environment. Their ability to prevent damage to the environment before it happens, such as oil spills or illegal releases, is inhibited by this reactive approach. A lack of high-res data for the environment, as well as among stakeholders, also inhibits the equipment's performance.

C. Hardware Components and Digital Evidence Sources

This part deals with the leading digital evidence collection tools, their purpose, the respective data types offered, and usage in forensic investigations. All the tools are chosen for their ability to record extensive operating data in conjunction with environmental data, as well as for their support for forensic data integrity procedures, secure acquisition, and preservation of metadata.

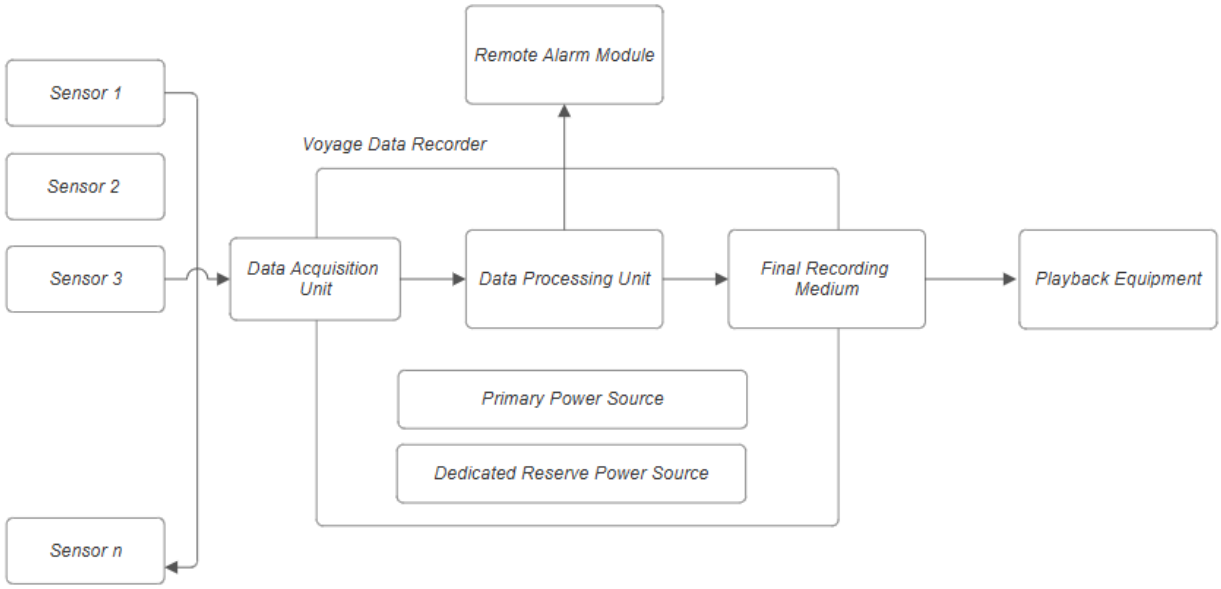

Figure 3. Block Diagram of VDR

Examples of such instruments are Voyage Data Recorders (VDRs), which are the maritime equivalent of an airplane's "black box" [12]. VDRs capture significant data in real-time, including the performance data of the engine, the navigational parameters, as well as communication records. The data is significant for the reconstruction of timelines of events during an incident as well as for the creation of a secure chronology of events [13]. Automatic Identification System (AIS) receivers are also used in real-time monitoring of ship movement; the receivers capture significant data such as the identity of the ship, position, speed, and course data, which is significant for monitoring operations as well as forensic investigation.

The following table shows the primary hardware components [14], their use, the type of data they produce, and their specific functions in the forensic process:

Table 1: Sources of Evidence in Maritime Operations

Hardware Component	Function	Data Provided	Forensic Role
Voyage Data Recorder (VDR)	Acts as the "black box" for vessels, recording all critical operational data.	Navigation logs, engine performance, communication data, timestamps	Provides a complete, time-stamped record for reconstructing incidents and performing timeline analysis.
Automatic Identification System (AIS) Receiver	Tracks and records real-time vessel positions and movements.	Vessel positions, speeds, headings, identification data	Enables continuous tracking and correlation of vessel movements for anomaly detection and incident reconstruction.

Onboard Environmental Sensors	Monitors key environmental parameters onboard.	Water quality, pollutant levels, temperature, salinity	Detects environmental anomalies (e.g., oil spills and chemical discharges) and provides quantitative evidence.
Electronic Chart Display and Information System (ECDIS)	Provides digital navigational charts integrated with real-time sensor data.	Geospatial data, navigational charts, hazard alerts	Assists in mapping incident locations and contextualising digital evidence with physical environmental factors.
Radar Systems	Detects objects and monitors the vicinity of the vessel.	Radar images, collision warnings, obstacle tracking data	Offers supplementary evidence for reconstructing vessel movements and assessing potential collision or navigational issues.
Edge Computing Devices	Processes and secures data locally before transmission.	Pre-processed sensor data, encrypted operational logs	Facilitates real-time analysis and encryption, ensuring data integrity and efficient, secure transmission to central systems.

3. PROPOSED CONCEPTUAL FRAMEWORK

The sea-faring industry has its own set of challenges at the nexus of technology, environmental conservation, and compliance with regulation. The chapter offers a end-to-end conceptual system that combines maritime digital forensics methodology with environmental sustainability goals. With a multi-layered approach that involves hardware, software, procedure-based methods, and regulatory frameworks, the system caters to the common issues of the sea-faring industry while offering actionable intelligence for environmental conservation [15].

It is constructed by putting in place the four foundational principles on which it stands [16] : complete collection of data by constant accumulation from varied maritime sources with minimum blind spots; integrity chain of custody that maintains tamper-free management of the evidence from the moment of collection up to the documentation time; actionable intelligence coupled with timely analysis to support reactive investigation as well as proactive prevention; and multi-stakeholder integration for coordination engagement with the regulatory bodies, the industry, and the environment.

A. Technical Architecture

I. Hardware Architecture

The hardware architecture of the framework comprises three primary domains:

- Vessel-based systems have upgraded Voyage Data Recorders (VDRs) with environmental and tamper-evident seals sensors, along with specialized ecological sensors for measuring oil-in-water, atmospheric emissions, ballast water, and underwater noise. They are backed by ruggedised, marine-grade edge computing hardware with encryption,

tamper-resistant Hardware Security Modules (HSMs) for secure cryptography functions, and independent backup power systems independent of central ship systems.

- Port facilities include shore-based sensor arrays for tracking water quality, air quality, and acoustic conditions. PTZ cameras with high resolution and infrared features [17] operate in conjunction with secure data receipt centres with redundant data storage and specialized equipment for the collection of physical environment specimens.
- In the suggested framework, edge computing hardware forms the core of the process [18] as it processes data streaming in from sensors at the local level, thereby enabling real-time decision-making. Since data is streamed continuously from onboard sensors and external monitoring devices, the edge computing system exploits onboard artificial intelligence and machine learning models, which compare the data against predefined operational and environmental thresholds. These models employ quick anomaly detection by identifying deviations from normal behavior—such as a strange spike in oil concentration or abnormal vessel behavior—that could be an indicator of an impending incident. When an anomaly is detected, the system instantaneously creates alerts that include rich diagnostic data, such as the type of anomaly, severity, precise geolocation, and suggested remedial action. These real-time reactions are automatically notified to the interested stakeholders, such as the captain of the ship, the environmental lead, and other interested parties, thereby enabling timely and well-informed decisions to be taken to prevent possible environmental damage. By greatly lowering the latency usually associated with transmitting data to far-off central computers, this local and fast processing capability helps to enable early incident response and environmental protection in marine operations.

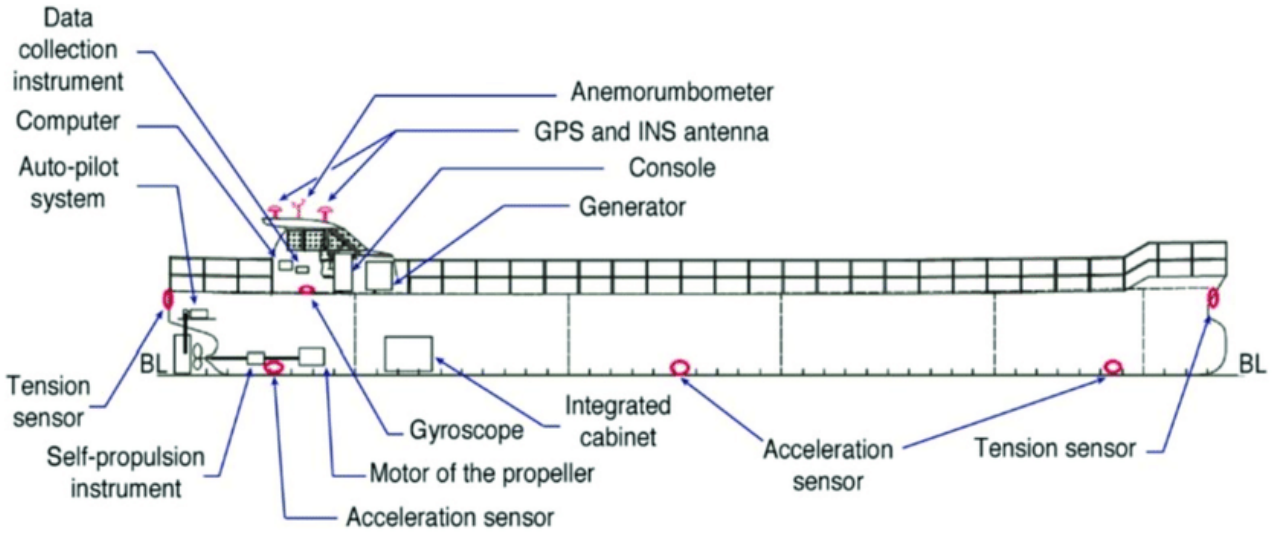

Figure 4: Sensors on a Vessel

II. Software Architecture

- Data Ingestion Layer: The Data Ingestion Layer is all about seamless consolidation of heterogeneous data sources. It consists of sensor integration modules that interface with onboard sensors, such as environmental monitors to monitor oil-in-water and atmospheric releases, and navigation devices including Voyage Data Recorders (VDRs) and Automatic Identification Systems (AIS). Integration with edge computing frameworks allows real-time preprocessing of data where it is created, reducing latency and conserving bandwidth—a critical aspect in maritime environments where connectivity may be patchy.
- Data Storage and Processing Layer: Following consumption, this layer stores and processes data in real-time. Continuous streams of data are processed using stream processing engines, enabling the immediate identification of anomalies and subsequent triggering of on-time responses. A data lake within a central repository stores structured and unstructured data, making available scalable data storage solutions to the massive amount of information generated.

Additionally, time-series databases are designed to store time-stamped data such that temporal patterns are queried and analyzed in an efficient manner, which is a necessity for tracking environmental changes over time.

- AI and Machine Learning Layer: The central element of smart data analysis, this layer uses sophisticated algorithms to derive actionable insights. Anomaly detection models apply supervised and unsupervised learning algorithms to

detect anomalies from established patterns, e.g., out-of-pattern levels of oil concentration or unusual emission patterns. Predictive analytics use historical and real-time data to predict possible environmental hazards, allowing for anticipatory action. Natural Language Processing (NLP) capability analyzes textual data from logs and reports, deriving meaningful insights that drive decision-making processes.

- Communication and Alerting Layer: Timely reaction to environmental anomalies is made possible by effective communication. The layer is comprised of notification systems that give real-time notification to stakeholders, including ship captains and environmental authorities, through SMS, email, or onboard display systems.
- Visualization Layer: This layer makes data interpretable and actionable via creation of graphical interface and reporting. Interactive and real-time visualizations for environmental parameters are provided through dashboard interfaces for crew members and remote monitoring teams. Thereby making it easier to provide transparency and facilitate decision-making
    - Security and Compliance Layer: Safeguarding the confidentiality and integrity of information is extremely important for the monitoring systems. The layer implements access control measures, such as role-based access controls, to allow only those who are authorized to access sensitive information. Also, the encryption protocols aid in securing data storage and communication against unauthorised access and modification of data stream. Comprehensive audit trails and logs document all activities within the system, facilitating forensic examination and compliance with environmental regulations.

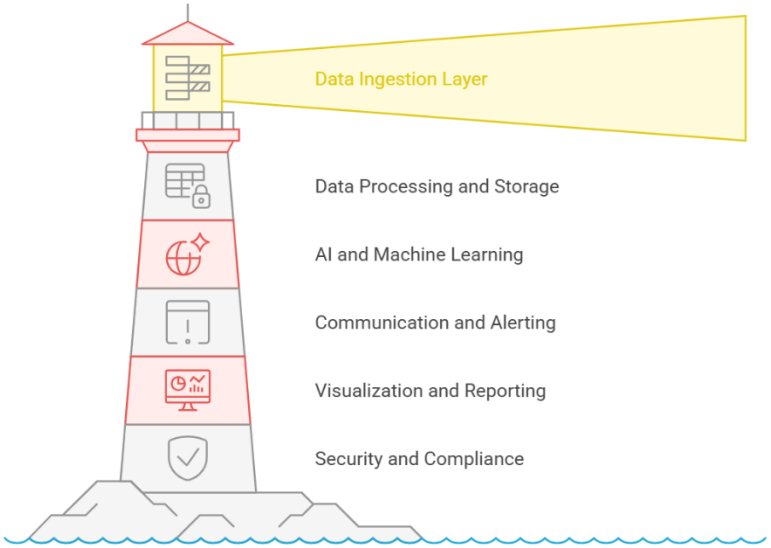

Figure 5. Software Architecture Layers

B. Methodological Framework

The methodological framework spans three critical phases:

I. Forensic Readiness Phase

This preparation stage is the foundation for effective maritime digital forensics through combined activities. Planning and risk analysis involve threat modeling of the environment to identify probable scenarios of destruction, vulnerability mapping of the ships and the operations, and planning the sensor placement based on risk profiles. It also involves the creation of effective data acquisition policies and the complete jurisdictional mapping of the legal requirements where operations are being conducted. As soon as the risk analysis processes are completed, the deployment of the systems is in the form of combined protocols, such as the deployment of the hardware with proper chain-of-custody measures, secure deployment of the software with proper security hardening, and the calibration of the first sensors according to certified standards. There are also comprehensive integration tests in this phase, as well as the deployment of redundancy and backup measures to ensure smooth operation of the system. Finally, training and certification processes are established to ensure operating capability. All these extend to personnel certification programs, the deployment of standard operating procedures, simulated response drills for emergencies, special training for the chain-of-custody, as well as technology update programs designed to keep the personnel up to date with changes in the system, ensuring the overall efficiency of maritime digital forensic operations.

II. Operational Phase

In regular operations, the framework is vigilant through the application of a 24/7 automatic monitoring system, which captures real-time data, applies strict quality checks to it, and generates a baseline profile for the typical operating parameters. Continuous monitoring makes it possible to detect anomalies that can signal an incident's onset. The status of the system is audited at all times to guarantee maximum performance and data integrity. On the triggering of the pre-set limits by an anomaly, the framework activates its incident detection and response processes. These are formal escalation processes, immediate first-response actions to act in response to the incident, as well as secure preservation procedures for the data to guarantee the integrity of the data obtained. Concurrently, robust notification workflows are in place to quickly notify all concerned stakeholders and authorities so the required actions are taken in good time to counter any ill effects. The combined operational mode guarantees proactive attitude towards ensuring sustainable marine operations and helps identify environmental issues early.

III. Investigation Phase

During forensic examination, data is collected through live and dead forensics techniques. Live forensics is on-line data collection and analysis from currently running systems, such as real-time streams of onboard sensors, AIS data, and communications. It allows investigators to capture information in real time, which is critical for the identification of the incident and for response in real time. Dead forensics, on the other hand, examines static data collected from powered-down or shut-down computers, such as stored Voyage Data Recorder (VDR) logs, AIS history records, and stored sensor readings.

The data is extracted from various sources by forensic operations designed to preserve data integrity. Data is restored with the assistance of VDRs [19], the underwater version of a "black box," via forensic imaging tools and write-blockers, producing bit-for-bit accurate copies with metadata [20] like timestamps and geolocation intact. SHA-256 class hash functions verify data integrity. AIS data, real-time position, velocity, and navigation status, are retrieved by forensic data collection software in acquiring data streams, typically real-time feeds and logged records. Onboard IoT sensors, which sense environmental parameters such as the level of pollution, temperature, and salinity, contribute real-time data that are important to ecological accident investigation.

Besides that, supporting evidence including radar history, Electronic Chart Display and Information Systems (ECDIS) data, and Global Positioning System (GPS) data, as well as communication between the onboard networks, is also analyzed. Data normalisation and correlation methods help to integrate several sets of data so that forensic experts can establish an integrated chronology of occurrences. The information is then consolidated and analyzed through techniques such as timeline reconstruction, source attribution, as behavioural analysis in an effort to determine the cause of the environmental anomalies, and the magnitude of their effect on the environment.

The use of dead and live forensics ensures a strong, multi-layered approach to collecting, analyzing, and storing digital evidence needed for quick response to incidents, efficient remediation of the environment, and long-term regulatory compliance in maritime operations.

C. Governance and Integration Framework

The governance structure creates a collaborative ecosystem through:

I. Multi-stakeholder Collaboration Model

Our framework integrates regulatory, industry, and environmental stakeholder inputs into a unified approach to achieve comprehensive environmental protection in maritime operations. Regulatory integration synchronizes the system to international and regional standards by linking in-house processes to underlying guidelines from the International Maritime Organization (IMO) [21], a United Nations specialized agency responsible for shipping, and MARPOL, the International Convention for the Prevention of Pollution from Ships, which lays down global standards for the prevention of marine pollution [1]. The coordination is done through standardized reporting interfaces, third-party certification protocols, cross-jurisdictional procedures for multi-territory incidents, and dynamic policy feedback mechanisms. Concurrently, industry involvement is encouraged by means of incentives for the acceptance of sustainable technologies, standardising initiatives for compatibility, building safe information exchange systems, cooperative best-practice design, and cost-sharing models to help to distribute the financial load of system implementation. Environmental groups contribute by negotiating data access agreements, independently verifying forensic results, engaging in collaborative research partnerships to enhance detection techniques, advocating for open transparency in environmental monitoring, and ensuring that ecological stakeholder demands are incorporated into operational guidelines [22]. This comprehensive, integrated strategy not only ensures that the framework meets stringent regulatory requirements but also drives industry innovation and robust environmental stewardship, ultimately contributing to a sustainable maritime ecosystem.

D. Validation and Verification

The framework employs strict validation processes to guarantee technical strength and operating efficiency. Technical validation comes through systematic verification of system integrity through regular penetration tests to detect

vulnerabilities, verification of sensor precision in accordance with calibrated standards, and cryptographic data integrity verification to ensure data integrity is maintained. The system is also subjected to fault injection and recovery tests for resilience, and forensic soundness verification is performed to ensure the integrity of the data collected in accordance with stringent legal standards. On the operational side, the framework is tested for simulated incident tests and blind, unannounced tests with scenarios close to real-world conditions. Quantitative performance measures assess detection performance, with correct time-to-detection measurements and false positives and false negatives analysis for the system's precision optimization. In addition, the overall performance of the system is quantified using environmental impact metrics measuring the degree of pollution eliminated, monitoring the trend of the number of incidents, assessing the health of the environment, quantifying the improvement in the intervention speed, and measuring the effectiveness of recovery following the incident. Concurrently, the socioeconomic impact measures the reductions in the costs of compliance, calculates the regulatory penalty savings, measures the preservation of brand integrity, identifies the improvements in operating efficiency, and monitors the impact on the risk profiles of insurance premium costs. All these strict validation procedures guarantee the framework operates at a high technical level while providing measurable benefits in safeguarding the marine environment as well as ensuring sustainable maritime operations.

4. SUSTAINABILITY IMPACT ANALYSIS & SDG FULFILLMENT

This convergence with the SDGs reinforces the double mandate [23] of the framework: it allows for the building of forensic capability for the examination of maritime incidents while working proactively towards international environmental and socioeconomic sustainability [24].

The proposed maritime digital forensic framework enhances forensic integrity and operational efficiency as well as contributes significantly to international sustainable development by conformity with a series of United Nations Sustainable Development Goals (SDGs). In effect, the system ensures environmental protection through quick detection and remediation of marine accidents like oil spills, unlawful dumping, and leakage of toxicants, which minimizes the environmental impact and loss of marine biodiversity. The blend of innovative technologies such as IoT sensors, AI/ML analytics, and blockchain ensures data integrity and transparency, quick response to environment events, and legally verified verification. This reduces the immediate impact of the marine environment, ensures regulatory compliance, as well as builds a culture of responsibility and continuous improvement.

Through real-time monitoring and rigorous forensic processes, the framework ensures economic feasibility through less expensive cleanup cost, reduced insurance risk, and avoidance of regulation fines. Second, the multi-stakeholder nature of the framework creates collaborations and partnerships between regulatory bodies, maritime operators, and the environment organizations, in the end culminating into world efforts towards protecting marine environments. The technical and operational capability of the framework is in a straightforward way connected to the SDGs, creating a tangible link between emerging forensic technology and the global objectives of sustainable development [25]. The SDGs supported by the framework, the unique contribution, and a brief description of how the contribution is achieved are illustrated in the table below.

Table 2 : Software Development Goals Fulfilled by the Framework

SDG Number	SDG Title	Framework Contribution	Explanation
6	Clean Water and Sanitation	Improved water quality monitoring and pollution control.	Continuous sensor-based tracking of water quality and pollutant levels ensures early detection and remediation of water contamination, protecting marine and coastal resources.
9	Industry, Innovation, and Infrastructure	Integrating advanced technologies (IoT, AI/ML, blockchain) for secure, efficient forensic operations.	The framework modernises maritime operations through state-of-the-art data collection, processing, and evidence-preservation methods.
13	Climate Action	Reduced greenhouse gas emissions and minimised environmental degradation	By facilitating prompt responses to maritime incidents, the framework helps lower overall emissions and mitigates the impacts of on marine life.

SDG Number	SDG Title	Framework Contribution	Explanation
14	Life Below Water	Enhanced marine environmental monitoring and rapid incident response	The framework protects marine life and preserves biodiversity by detecting and mitigating ecological incidents such as oil spills, pollutant discharges, and plastic pollution.
17	Partnerships for the Goals	Multi-stakeholder collaboration and information sharing among regulatory bodies, industry, and environmental organisations	The framework fosters collaborative networks, ensuring standardised data exchange, joint incident response strategies, and shared best practices for sustainable maritime operations.

5. CASE STUDY: THE MV WAKASHIO GROUNDING

The grounding of the MV Wakashio off Mauritius [26] in year 2020 was a striking illustration of how marine digital forensics may be used to probe and contain environmental calamities. The major naval accident that happened in July 2020 was investigated mostly using digital forensics. On 25 July 2020 the Japanese-flagged bulk cargo MV Wakashio grounded off Pointe d'Esny, Mauritius. Later, the ship broke in half, resulting in a massive oil leak severely contaminating the delicate coastal area and marine life.

Digital forensics corroborated this accident on many fronts:

I. Navigation system verification: Experts verified the ship's electronic navigation systems, GPS tracks, and charts to see how the ship had strayed from the course.

II. Like the aviation black box, the Voyage Data Recorder (VDR) was subjected to analytical scrutiny to recreate the events that resulted in the grounding accident, including aspects like bridge-to-bridge communication and navigation procedures.

III. Communication analysis: The emails of the crew and ship management, satellite communications, and other electronic communications were analyzed by digital forensics specialists.

IV. Mobile phone investigation: The crew member’s personal cell phones were investigated to determine onboard activities prior to the accident and found that the crew members were having a birthday celebration and trying to get cellular signals off shore [27].

V. The track history of the Automatic Identification System was used to trace back the uncharacteristic voyage of the vessel along the Mauritian coast.

The electronic records yielded several key findings, such as the diversion of the course of the ship from its intended route to allow for closer proximity to the shore to obtain cell phone signals, the lack of proper position monitoring by the crew, and the nonadherence to prescribed navigation procedures. The electronic data were instrumental in determining the causes of the accident and attributing blame.

Case Study : Deepwater Horizon Oil Spill (2022)

After the 2010 Deepwater Horizon disaster [28], maritime digital forensics emerged as a central investigation tool. Digital forensic analysts extracted information from the rig's computerized control systems, alarm logs, and sensor data to establish the critical timeline of events that led to the blowout. Examining the electronic control systems for the blowout preventer and re-establishing communications between BP staff, Transocean employees, and contractors, investigators uncovered significant evidence of operational choices and safety concerns previously brought up. This digital evidence was central to establishing why critical safety systems failed at different stages of the crisis.

The forensic findings effectively led the official U.S. Coast Guard and federal agency investigations to ultimately conclude a complex interplay of technical failure and human error. Computer simulations based on recovered data allowed the investigators to subject hypotheses on how the sequence of failures had occurred to test and learn, something not possible with traditional investigative methods. The resulting analyses established causality [29] and accountability and drove the creation of new offshore drilling regulations and safety protocols designed to prevent similar catastrophes. The Deepwater

Horizon accident proved that maritime digital forensics could change catastrophe investigation in complicated industrial environments where electronic systems govern vital operations.

6. CONCLUSION AND FUTURE DIRECTIONS

Lastly, this paper has given a comprehensive overview of present maritime digital forensic technologies [30], analyzed the limitations of current practices, and proposed a conceptual framework that integrates state-of-the-art data acquisition, AI/ML-based anomaly detection, with environmental sustainability objectives. Our study demonstrates that by using Voyage Data Recorders (VDRs) information, Automatic Identification System (AIS), in-cabin weather sensors, and other navigational aids, forensic methods can reenact events with high degrees of accuracy. The use of such technologies not only facilitates instant incident notification and correction—hence lessening the effects of natural events like oil spills, prohibited discharges, and marine debris collection—but also ensures that the evidence remains tamper-evident and admissible in a court of law. Such integration of sustainability goals in this framework further highlights its value in advancing compliance with regulatory standards, openness of operations, and more positive stewardship in marine environmental areas.

In the future, there are a number of directions for further research and development. First, overcoming the scalability issues is still important; future research should be aimed at optimising data processing pipelines and improving integration mechanisms to cope with the vast amounts of data produced by global maritime activities. Standardisation of data collection and preservation procedures is necessary to provide consistency and reliability across vessels and operational environments. Also, more studies must be conducted to further hone the use of AI/ML models, specifically for enhancing anomaly detection precision and eliminating false positives, which can be used for the early detection of environmental threats. A sound point for the establishment of maritime digital forensics, a vital instrument for environmental preservation and green development, the described structure is through the encouragement of cooperation between regulatory authorities, industry stakeholders, and academic researchers, all the following actions need to be geared towards further standardization and improvement of forensic practice, leading ultimately towards a safer and greener marine environment.

REFERENCES

[1] International Maritime Organization (IMO), "Guidelines on Maritime Cyber Risk Management," MSC-FAL.1/Circ.3, 2017.

[2] National Transportation Safety Board (NTSB), "Marine Accident Report: Collision between US Navy Destroyer and Oil Tanker," NTSB/MAR-19/01, 2019.

[3] J. Bhatti and R. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection," Navigation, vol. 64, no. 1, pp. 51-66, 2017.

[4] S. Kimberly and G. Botelho, "Maritime Digital Forensics: Challenges and Opportunities," Digital Investigation, vol. 18, pp. 34-46, 2021.

[5] H. Ringbom, "Regulatory Layers in Maritime Safety and Security," WMU Journal of Maritime Affairs, vol. 14, no. 1, pp. 1-15, 2020.

[6] OceanMind, "Using Technology to Increase Ocean Sustainability," Technical Report, 2022.

[7] MarineTraffic, "AIS Data Analytics for Maritime Security," White Paper, 2023.

[8] L. Wang, R. Zhang, and S. Chen, "Maritime IoT: Challenges and Solutions for Smart Ship Development," IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8751-8766, 2021.

[9] M. Bhosle and A. Kumar, "Blockchain for Maritime Security and Environmental Protection," Journal of Marine Science and Engineering, vol. 9, no. 12, p. 1232, 2022.

[10] Global Fishing Watch, "Annual Report on Illegal Fishing Detection," Technical Report, 2022.

[11] L. Roberts and R. Fernandez, "Digital Forensics in Environmental Disaster Response: The Deepwater Horizon Case Study," Environmental Science & Technology, vol. 55, no. 3, pp. 1789-1798, 2021.

[12] S. Kochevar and M. Brubaker, "Voyage Data Recorder Forensics: Methods and Applications," Journal of Navigation, vol. 72, no. 6, pp. 1421-1435, 2019.

[13] International Association of Classification Societies (IACS), "Requirements for Voyage Data Recorders," IACS Unified Requirement, 2020.

[14] K. Tam and K. Jones, "Maritime Cybersecurity: A Survey of Critical Infrastructure Protection Approaches," International Journal of Critical Infrastructure Protection, vol. 35, p. 100452, 2021.

[15] P. Nikitakos and M. Lambrou, "Digital Forensics in Maritime Sector," WMU Journal of Maritime Affairs, vol. 18, no. 2, pp. 259-280, 2019.

[16] R. Poulsen and H. Johnson, "The Logic of Maritime Security: Boundary Work for Port Security Professionals,"

Security Dialogue, vol. 52, no. 3, pp. 231-249, 2021.

[17] United Nations, "Sustainable Development Goal 14: Life Below Water," UN SDG Knowledge Platform, 2015.

[18] M. Khalid and S. Sharma, "Edge Computing for Maritime Applications: Challenges and Solutions," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2846-2861, 2022.

[19] J. Corbett and J. Winebrake, "Emissions from Ships: Current Status and Future Scenarios," Journal of Cleaner Production, vol. 311, p. 127547, 2021.

[20] S. Rahmstorf and D. Coumou, "Increase of Extreme Events in a Warming World," Proceedings of the National Academy of Sciences, vol. 108, no. 44, pp. 17905-17909, 2019.

[21] P. Sujit and D. Ghose, "Search Using Multiple UAVs with Flight Time Constraints," IEEE Transactions on Aerospace and Electronic Systems, vol. 48, no. 4, pp. 2594-2616, 2022.

[22] D. Dittman and T. Veale, "The MV Wakashio Grounding: A Forensic Analysis," Maritime Policy & Management, vol. 48, no. 5, pp. 654-672, 2021.

[23] National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, "Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling," Report to the President, 2011.

[24] M. Hasan and K. Karim, "Digital Forensic Analysis of Maritime Accidents: A Review," IEEE Access, vol. 9, pp. 42504-42519, 2021.

[25] International Maritime Organization (IMO), "International Convention for the Prevention of Pollution from Ships (MARPOL)," IMO Publishing, 2022.

[26] United Nations, "Sustainable Development Goals," UN SDG Knowledge Platform, 2015.

[27] S. Laxminarayan and R. Bhatnagar, "Challenges in Maritime Cybersecurity," Journal of Transportation Security, vol. 15, no. 2, pp. 179-194, 2022.

[28] E. Gille and R. Sharma, "Predictive Analytics for Maritime Safety: A Review," Journal of Marine Science and Technology, vol. 26, no. 4, pp. 1243-1258, 2021.

[29] B. Tetreault, "Use of Voyage Data Recorder Information for Safety Management Systems," Marine Technology Society Journal, vol. 55, no. 2, pp. 87-95, 2021.

[30] M. Lehtola, "Improving Maritime Safety with Big Data Analytics," Ocean Engineering, vol. 217, p. 107928, 2020.