ISSN: 2182-2069 / E-ISSN: 2182-2077

Adopting Computer Forensics Techniques to Investigate Cyber Incidents in Global Shipping Operations

Ramesh Balasubramanian[1*], and N. Anand[2]

[1*]Department of Nautical Science, AMET Institute of Science and Technology, Chengalpet, Tamil Nadu, India. rameshchitra2002@yahoo.co.in, https://orcid.org/0009-0009-5709-2739

[2]Department of GMDSS, AMET University, Kanathur, Tamil Nadu, India. anand.n@ametuniv.ac.in, https://orcid.org/0009-0008-9156-128X

Received: February 06, 2025; Revised: March 20, 2025; Accepted: April 30, 2025; Published: May 30, 2025

Abstract

Due to increasing reliance on information and communication technology (ICT), the global shipping industry which plays a pivotal role in international trade is growing more vulnerable to sophisticated cyber risks. GPS spoofing, onboard system hacking, and shipping company ransomware attacks are just a few of the many cyber incidents that put maritime operations at risk. More often than not, the industry lacks comprehensive and effective policies for incident investigation and response, integrating standardized frameworks suitable for maritime operations. This study focuses on global shipping operations, investigating the possible application of computer forensic methodologies as an organized framework for cyber incident investigation. Traditionally the realm of corporate and law enforcement sectors, computer forensics encompasses the identification, preservation, analysis, and presentation of digital evidence. Adapted for maritime settings, computer forensics provides immense aid in the investigation of cyberattacks, system compromise analysis, and post-attack evidence preservation for legal proceedings. The proposed framework incorporates computer forensic methods while taking into account the specifics of operational and IT/OT system integration in shipping, evidence collection challenges in high seas, and the need to control and account for those International Domain custody. The methodology consists of incident analysis: detection, digital evidence acquisition, forensic analysis, and structured reporting. Utilizing contemporary cyber incidents at sea and consulting with industry experts, the study illustrates how incorporating computer forensics into maritime cybersecurity frameworks can improve responsiveness, responsibility, and deterrence. These results suggest that the shipping industry must begin to consider forensics as part of their strategic planning in order to defend against increasingly sophisticated cyber-attacks.

Keywords: Computer Forensics, Cyber Incidents, Shipping Operations, Maritime Cybersecurity, Digital Evidence, Cybercrime Investigation, Global Shipping.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 409-422.
DOI: *10.58346/JISIS.2025.I2.029*

*Corresponding author: Department of Nautical Science, AMET Institute of Science and Technology, Chengalpet, Tamil Nadu, India.

1 Introduction

1.1 Defining Computer Forensics Within the Context of Global Shipping Activities

Computer forensics, or digital forensics, is the meticulous legal process of detecting, preserving, analyzing, and presenting data (Nelson et al., 2010). In global shipping operations, computer forensics relates to the cyber investigation of maritime systems, such as shipboard networks, port infrastructure, cargo control systems, and also maritime traffic communication systems. Unlike in the past when the shipping industry was dominated by manual activities and siloed systems, it is now supported by integrated digital systems like Electronic Chart Display and Information Systems (ECDIS), Automatic Identification Systems (AIS), and satellite-based tracking (Tam & Jones, 2018). These technologies have enhanced operational efficiency, but at the same time, increased opportunities for cybercriminals. In the context of maritime digital forensics, the focus is on gathering evidence from the shipborne ICT and Operational Technology (OT) environments post cyber incident (Guerra et al., 2024). Such evidence includes computer viruses located in navigational aids, unload access control system logs, and port site computer system network anomalies (Baldwin et al., 2020; Ismail & Khalil, 2025). Investigators face the additional challenge of conducting forensic examinations in severely constrained space environments under jurisdictional waters that complicate the collection of admissible evidence or data (Trisiana, 2024).

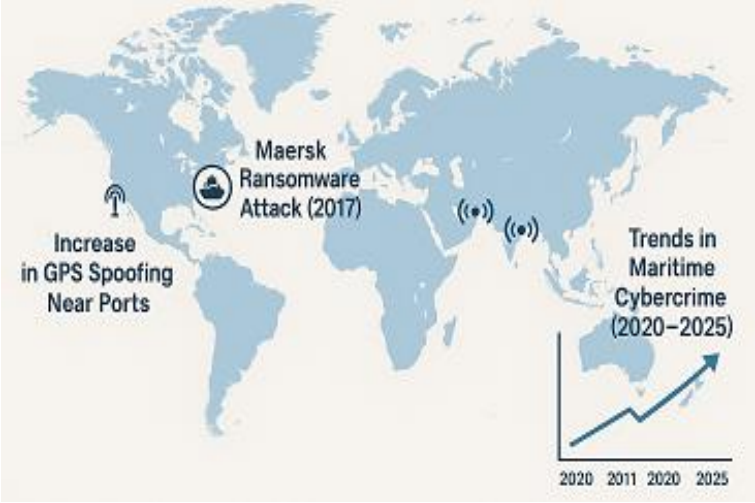

Figure 1(a): Global Shipping Cyber Threat Landscape

The figure 1(a) shows the development of cyber threats around the globe concerning maritime industries. Details in this figure also depicts the worrying events and trends regarding shipping related cyber threats. The ransomware attack on Maersk in 2017 which crippled a myriad of ports across the world marked an important event as it showcased how fragile cyber maritime infrastructures are to aggressive cyber warfare (Arvind & Nair, 2025). The figure is also marked with the rising occurrences of GPS spoofing in and around major ports in the US, China, and the Middle East which pose great risks to navigational and maritime safety. Exhibit in the right side of the map presents a line graph indicating the numbers of maritime cybercrime perpetrated from 2020 to 2025 which vividly denotes growing attacks on shipboard systems, port networks, and supply chain technologies. This figure brings forth the chronic underestimation and lack of attention that cyber threats in shipping receive, portraying the dire need of maritime operations to impose advanced cybersecurity policies.

1.2 Importance of Cyber Incident Investigation for Maritime Transportation

According to the International Maritime Organization, (2021), the shipping industry constitutes a fundamental pillar of the economy by enabling almost 90% of global trade in terms of volume. As technology continues to advance within the industry, the risk and scope of damage from cyberattacks increases significantly in financial, operational, and even environmental aspects (Radhi & Abdulahad, 2023). Maritime cyber warfare vulnerabilities were highlighted further in (Greenberg, 2020) where Maersk suffered a loss of over $300 million due to the ransomware attack's disruption of their global operations. The reasons supporting the need for cyber incident investigation in this sector are multifold: First, prompt and thorough mitigation of cyberattacks ensures malicious acts are discovered and contained or restricted from spreading (Kessler, 2022; Palash & Dhurvey, 2024). Forensic investigations also allow attack attribution functionality, which enables stakeholders to take legal or punitive action where necessary (Casey, 2011). Furthermore, digital forensics provides assistance towards an organization's root cause investigation functionality which enhances their ability to protect from future incidents (Jang-Jaccard & Nepal, 2014). Besides, the amount of regulatory scrutiny is growing. The amendments to the International Management Code for the Safe Operation of Ships and Hazardous Materials (ISM Code) are compulsory and cyber risk management is to be incorporated along with cyber forensic readiness which must be integrated within operational protocols (IMO, 2020). Inadequate compliance with these operational standards places shipping companies at operational and regulatory risks while endangering their reputation.

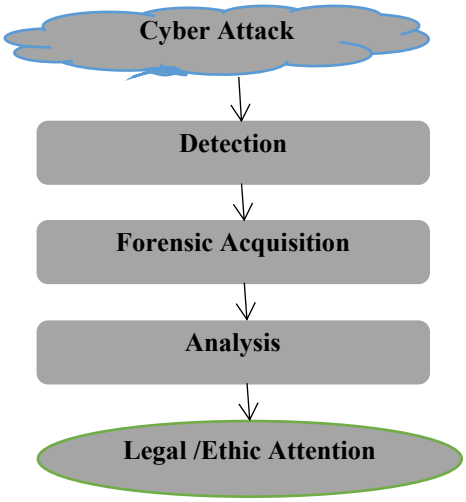

Figure 1(b): Role of Computer Forensics in Incident Response

Figure 1(b) highlights the importance of computer forensics in the incident response process within the realm of cybersecurity. Everything starts when a cyber attack happens, triggering the need for response. In the Detection phase, either suspicious activity or indicators of compromise are marked. Incidents result in Forensic Acquisition, where pertinent digital evidence is collected from the systems in question in a manner that maintains its integrity. Following this is Analysis, wherein the forensic data acquired is scrutinized to ascertain how the system was breached, the extent of the breach, and the possible attackers. This is then documented in the Reporting phase, where stakeholders are provided with adequate information together with insights and guidance. Lastly, the process ends in Legal and Ethical Action that involves possible sanctions, court action, or policy and infrastructural changes to avert a repeat scenario. This shows that computer forensics is more than just a set of technical exercises; it is an organized, strategic effort intended to encourage effective governance in light of cyber risks.

1.3 Research Queries Along with Objectives

This study emphasizes the central question considering the broadening spectrum of threats and the importance of shipping for the world economy:

1) To identify the specific features of cyber threats in maritime domain including both ship and port systems.
2) To investigate the scope and challenges of existing forensic technological approaches to the maritime domain.
3) To develop a model for forensic examination of cyber incidents for shipping operations.
4) To analyze the impact of international cooperation, enforcement of laws, and forensic preparedness on the level of maritime security.
5) To design proactive measures for maritime operators to enhance their capability for cyber incident response and forensic analysis.

By completing these goals, the research seeks to help develop and protect concepts in maritime security, providing valuable information to policy makers, shipping industry leaders, cyber defense specialists, and forensic experts.

2 Literature Review

2.1 The Global Shipping Industry Cyber Threat Overview

Adoption of modern technology in the shipping industry has enhanced efficiency but exposed it to sophisticated cyber threats. Modern ships are basically mobile data centers and are provided with systems like the Electronic Chart Display and Information System (ECDIS), Automatic Identification System (AIS), Integrated Bridge Systems (IBS), satellite based navigation and others that are prone to cyber theft (Tam & Jones, 2018; Soni et al., 2014). Other risks include ransom ware GPS spoofing, insider threats, and supply chain vulnerabilities (Prabhudeva & Hariharan, 2024). The BIMCO Cyber Security Guidelines of 2020 noted significant increases in cyber intrusions targeting vessels during voyage and port stays, with consequent interference to navigation systems, unauthorized cargo data access, and customs clearance hold-ups (Gopi Krishnan et al., 2020; BIMCO, 2020). Cybercriminals have illustrated the potential to remotely hijack or disable shipboard systems, resulting in vessels being off course and communication systems being inoperative (Di Renzo et al., 2020). A case in point is the hacking incident on COSCO Shipping Lines in 2018, which wrought havoc on the company's email infrastructure and port operations across the United States (McLaughlin, 2019; UNCTAD, 2021). In addition, the hybrid character of maritime cyber threats, which combine physical and digital axes, makes the impact especially serious by posing direct risks to people, marine ecosystems, and critical international economic trade (Chang et al., 2020).

2.2 Some Remarks on the Problems of Investigating Cyber Incidents in Shipping Operations

The shipping cyber incident is a mixture of technical, logistical, and legal difficulties. Perhaps one of the main barriers is the diversity of maritime systems. Most ships tend to operate proprietary equipment and software from multiple vendors which creates complications in standard forensic configurations (Bada & Nurse, 2020). Further, a vast number of onboard systems are legacy systems with poor logging practices and no forensic capabilities, thus, making the capture of post-incident evidence difficult (Berglund & Jacobsson, 2019). Investigations are complicated by jurisdictional problems, and ships are often mobile and cross borders frequently, operating under "flags of convenience," which raises legal

concerns surrounding ownership and responsibility, along with access to digital evidence. Most forensic personnel working in the maritime domain are not trained in digital forensics. This results in an incomplete or substandard investigation, which causes loss of volatile data, including RAM or system logs (Hosny & Liles, 2019). For the entire industry, a lack of uniform incident response procedures poses another challenge. Even though the International Maritime Organization (IMO) has developed guidelines to deal with cyber risks, adoption and enforcement tends to differ from one shipping company to another (IMO, 2020; Sindhu et al., 2021). These differences impact the effectiveness of coordinated response efforts which in turn, causes delays in cloud incident containment and forensic investigation.

2.3 Existing Computer Forensics Techniques and Tools

Computer forensics is defined as the application of scientific methods for collecting, preserving, and analyzing digital evidence. It includes disk cloning, memory examination, network forensics, and log file analysis (Nelson et al., 2010). Cyber forensic investigations focus on the use of different tools like EnCase, FTK (Forensic Toolkit), Autopsy, and Volatility (Azizova et al., 2024). These tools enable the reconstruction of deleted files, acquisition and analysis of system memory, user activity reconstruction, and tracing of unauthorized access (Carrier, 2018). Forensic tools have certain limitations in the context of maritime operations. For example, forensic imaging tools might not work with shipboard embedded systems and customized firmware (Kessler, 2022). Moreover, forensic investigation of shipping is a fast-response task because digital evidence on vessels is volatile. Cyber security readiness—where systems are set up beforehand to log important evidence—is becoming popular as an upward strategy to cybersecurity in maritime issues (Reyes et al., 2021). With live forensics and cloud-based forensics, some of the maritime constraints appear to be resolving. Live forensics allows evidence collection from active systems, making it possible to gather evidence without turning off systems in high-availability areas, such as shipping operations. Additionally, cloud-based incident response tools allow remote access to forensic data, which is critical while ships are in motion or docked in foreign jurisdictions. New collaborative approaches among port authorities, shipping companies and national cyber security centers are being developed with the aim to enhance forensic capabilities while ensuring uniform standards in cyber incident forensic investigations. Such approaches aim to access less restricted data and share intelligence, strong practices and training material, thus strengthening the global maritime cyber resilience.

3 Methodology

3.1 Selection of Case Studies from Global Shipping Companies

For my research, I focused on a few case studies from international shipping companies to demonstrate how different organizations manage cyber incidents and the role of computer forensics in their cybersecurity measures. The selection criteria focused on incidents that were particularly operationally and financially disruptive to the businesses. Selected case studies depict a range of evolving and sophisticated cyber threats such as ransomware attacks, data breaches, GPS spoofing, and even insider threats. This range of selected case studies enables the research to capture a significant number of cybersecurity issues within the shipping industry. Additionally, the cyber geography of the companies was analyzed as regions differ in their regulatory frameworks and practice of cybersecurity. This selection enables a comprehensive study on the application of forensics in cyber investigations by different companies, considering the regional response mechanisms, legal jurisdiction, and availability of forensic resources.

3.2 Methods of Collecting Information Pertaining to Cyber Incidents

This research's data collection method applies a documentary analysis technique that utilizes unrestricted internet interviews while incorporating some pre-existing incident reports. The initial phase of the research involves the collection of pertinent documents such as news articles and third-party analyses to construct a detailed trajectory of the cyber incidents in question. The documents contain important details about the nature of the attack, the company's initial response, and the investigative measures that were taken. Furthermore, semi-structured interviews will be conducted with a representative sample of maritime cybersecurity professionals, digital forensics practitioners, and relevant stakeholders to understand how forensics are applied to cyber incident investigations in the maritime domain. Their insights will inform what has been documented as best practices and challenges during the investigative processes. Where direct access to the forensic data is not possible, recourse will be made to, briefings, government reports, and academic publications which outline the specifics of the forensic investigations. Additionally, regulatory and organizational documents such as those of the International Maritime Organization (IMO) will be used to capture the maritime and forensic cybersecurity preparedness landscape in the industry.

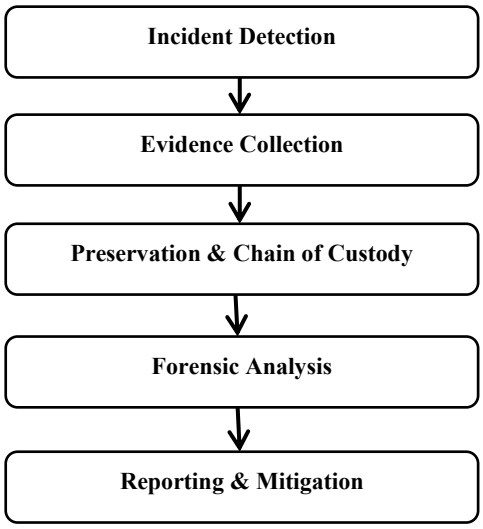

Figure 2: Computer Forensics Methodology Applied to Maritime Cyber Incidents

Figure 2 illustrates the stepwise methodological framework designed for the investigation of cyber incidents in the maritime domain using computer forensics. The process commences with Incident Detection, where atypical activities onboard maritime networks and systems are detected using security monitoring systems or reported by crew members. The discovered irregular activities trigger the action of Evidence Collection, which entails the systematic capturing of digital artifacts from onboard and shore-based systems, including but not limited to log files, communications, and snapshots of the system. This is followed by Preservation and Chain of Custody, where, for legal and investigative purposes, the evidence collected is documented accurately and maintained without interference. Focusing on the evidence, the fourth step, Forensic Analysis, provides a detailed technical scrutiny of the attack to determine the pathway, target systems, and ascertain whether sensitive data was exposed. Finally, the framework culminates in Reporting and Mitigation, where for the stakeholders, detailed reports are created with findings and further actions to avert future incidents are implemented. This figure underpins discipline that is legally defensible and highly technical, and speaks to the management of cyber threats in maritime environments.

3.3 Review of Computer Forensics Methods Utilized in Each Case Study

The techniques of analysis of computer forensics will form an integral part of this work. A computer forensic technique will be employed and analyzed for each case study. Specifically, the judicial approaches which pertain to the investigation of the cyber incidents will be analyzed. This broad analysis will include consideration of the methods of evidence capturing by means of disk imaging, network traffic capturing, memory forensics, and specialized forensic software applications. The study will investigate if the examined methods were appropriate considering the type of incident, and the maritime constraints of the case, which included "air-gapped" systems and frail access to digital evidences. An important component of the analysis will be the performance of forensic tools such as FTK, EnCase, and Autopsy that are used in digital forensics, and if they were modified or enhanced for the specific technological and operational context of shipping controllable environment Windows. The study will examine capturing forensic evidence from running systems without suspending operations, also termed live forensics, which is particularly relevant for the maritime realm because of the high cost of operational downtime. Moreover, the research will explore the techniques of attribution of attacks such as malware dissection and digital fingerprinting to establish how cyber investigators follow the trails of cybercriminals. Last, the study will focus on how the forensic data shaped the company's decisions, especially regarding enhancing cybersecurity and applying the strategies crafted to avert recurrence of such incidents.

4 Case Study Analysis

4.1 Investigation of Cyber Breaches in International Maritime Shipping

The increased sophistication of cyber breaches in international maritime shipping has made it more challenging to manage. Cyber shipping has emerged as a critical field in dire need of effective security measures due to cyber criminals increasingly setting their sights on shipping networks as they heavily depend on sophisticated interlinked systems of communication, navigation and logistics. A glaring illustration of this is the NotPetya ransomware attack lay siege to Maersk in 2017. This cyber incident alone resulted in the shutting down of the whole IT ecosystem of the organization which in turn stalled the shipping of containers, leading to operational losses of over 300 million dollars for Maersk. In 2018 a cyber attack on COSCO, a logistic giant resulted in the disruption of their system port operation across US and inhibited many ports across US from functioning. These assaults are sufficient to expose the maritime industry's potential risk to terroristic endeavors like ransomware, phishing, and doxing. Cyber shipping also severely impact the vessel's supply chain, operation system and client management interfaces. Exposing businesses that operate in this environment to severe operational disruptions and information like manifests, naval traffic data, financial details and many more can drastically harm the operational credibility of the organization. Furthermore, numerous cases highlighted vulnerabilities in the capacity of shipping firms to respond to cyber-attacks, particularly in terms of coordinating incident response communication across jurisdictions and with many relevant parties. Hence, analyzing such incidents is important for grasping the increasing complexities of cyber threats within the maritime sector, in addition to the need for advanced cyber defense systems and forensic investigative resources.

4.2 Use of Computer Forensics Tools in All Case Studies

For all reviewed cyber incidents, the use of computer forensics strategies helped in dealing with the aftermath of the attack, as well as recovering evidence for legal and operational proceedings. In Maersk's case, forensic specialists performed disk imaging and memory analysis for data preservation and

recovery. This allowed investigators to understand the propagation of NotPetya ransomware and its infection mechanisms on the company's IT infrastructure globally. Also, forensic analyses of system logs, network traffic, and malware samples with EnCase and FTK showed details of the attack and indicated how the attack was transmitted through the network and identified gaps in Maersk's cybersecurity infrastructure. In the same manner, COSCO experts were more concerned about the analyses of log files and network traffic for the detection of breach points and data extraction points for files, as well as evaluation of the data extraction level. Live forensics, which allowed for the collection of operational evidence without glaring disruptions to business activities, was key to evidence collection while maintaining business operations. In both scenarios, the use of forensics techniques, such as malware and file signature analysis, in addition to hash matching, proved indispensable in identifying the nature of the attack and the whereabouts of the cybercriminals. The use of cloud-based forensics tools also provided access to critical information, which allowed the investigators to continue their work regardless of the physical or logistical constraints created by the ships' locations and the company's worldwide presence. These techniques demonstrated the sophistication of cyber warfare in maritime domains and highlighted the need for pre-emptive forensics measures and investigative tools as part of maritime cybersecurity defenses.

Figure 3 depicts the insidious effects of different cyber incidents on shipping operations compared across three key metrics: operational disruption (in days), cost impact (in USD millions), and downtime (in hours). The NotPetya attack on Maersk remains the worst in terms of overall impact, costing the most and causing the greatest amount of downtime. The COSCO as well as ransomware attacks also incur considerable amounts of operational and financial losses albeit to a lesser extent than NotPetya. Data breaches, although still significant, are less disruptive and costly. This assists in understanding the need for appropriate cybersecurity in maritime operations. Figure 4 illustrates the various computer forensics techniques used in shipping operations with emphasis on scope of use, effectiveness, and time expended. Disk Imaging and Timeline Analysis are the most popular and successful techniques. However, less time is used by these techniques as compared to more time-consuming methods like Log Analysis. File Examination remains effective, but is used less often and is the least time-consuming. This indicates operational preference for investigative methods that yield the greatest results for forensic effectiveness while controlling time expenditure in maritime forensic investigation.

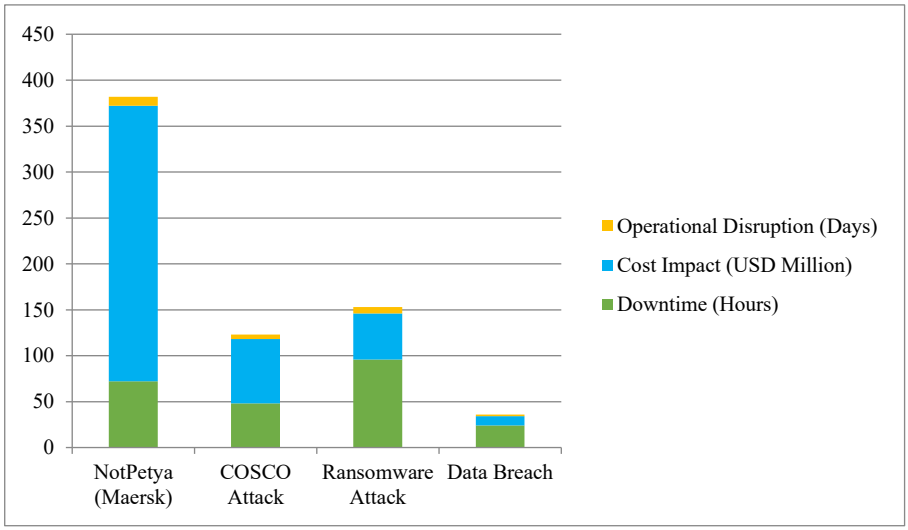

Figure 3: Cyber Incident Impact on Shipping Operations

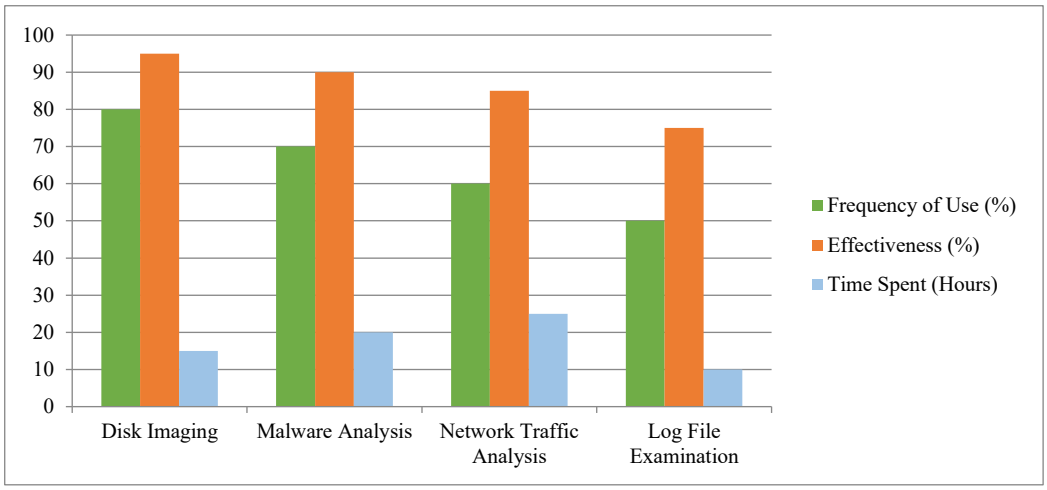

Figure 4: Application of Computer Forensics Techniques in Shipping Operations

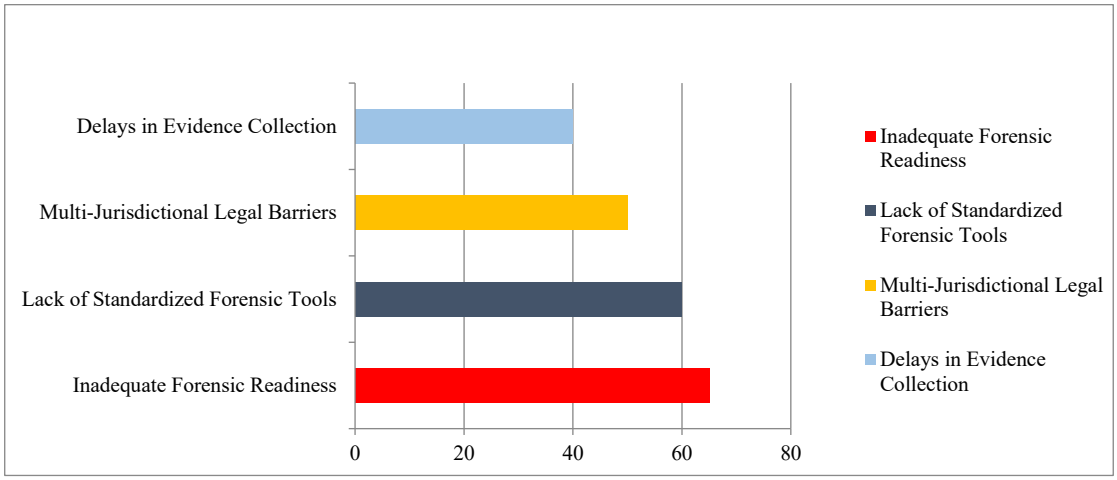

Figure 5: Key Challenges in Shipping Cyber Incident Investigations

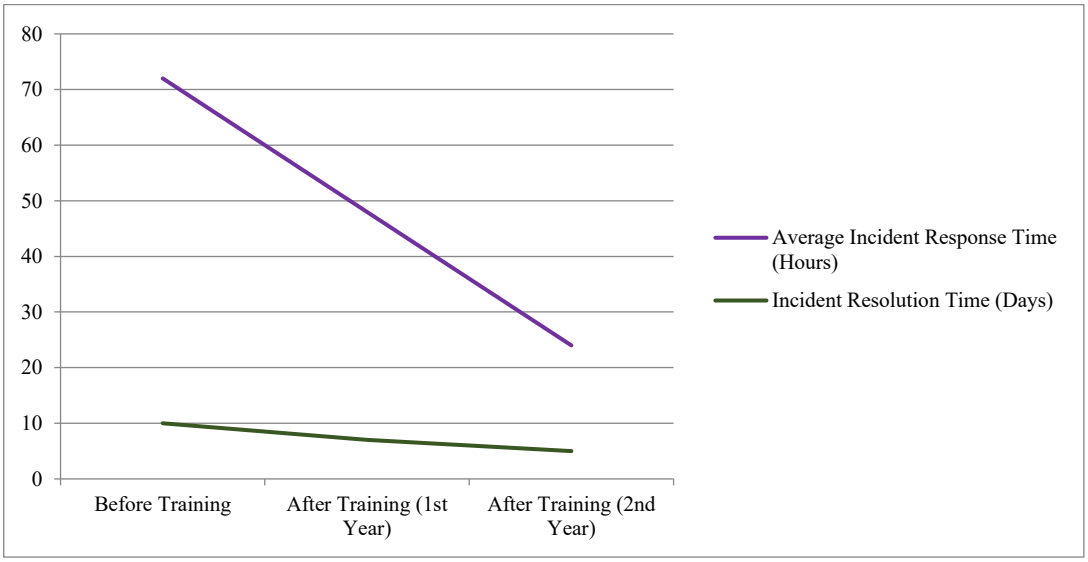

Figure 6: Impact of Cybersecurity Training on Incident Response Time

Figure 5 captures the other problems that pose challenges to the investigation of cyber incidents within the shipping industry. The most common remains poor forensic readiness followed by the absence of standard forensic tool sets. Staying within multiple jurisdictions creates legal holdups which can impede evidence gathering as well. These obstacles emphasize the need for better organization, uniformity, and collaboration at an international level to respond to and investigate maritime cyber incidents. As shown in Figure 6, the shipping industry has greatly benefitted from training courses on cybersecurity with regards to responding to incidents. The graph also illustrates the drastic drop in the mean response time (in hours), as well as the decline trend in the mean resolution time (in days) over two years following training implementation. Board maritime operations, it has been found that with sustained training on cybersecurity, the rate at which incidents are detected, dealt with, and resolved increases, enhanced efficiency, and effectiveness enable faster reaction, containment, and resolution of incidents.

4.3 Critical Reflections and Recommendations for the Analysis of Cyber Incidents Within Shipping Businesses

Through examining the cyber incidents in the shipping sector, one can take away lessons and best practices related to improving cyber threat investigative capabilities. Known as forensic readiness, the ability to investigate a crime scene and ascertain valuable evidence has to do with system designs with the capability to log important metadata needed when the systems undergo investigations. COSCO and Maersk cases show both companies were ill prepared because they lacked adequate data capturing and evidence gathering systems. Having forensic readiness enhances evidence preservation even when there are attacks. Another observation provided is the need for coordinated response with multiple parties involved. In view of both cases, communication gaps among distinct departments, vendors, and regulatory bodies stifled rapid responses, making important evidence irretrievable. As such, shipping firms should have comprehensive incident handling procedure checklists to engage relevant parties within the business and facilitate prompt information flow during cyber incidents. Also, the case studies show that investment on cybersecurity education and training for maritime personnel is crucial. In both scenarios, lack of cyber threat awareness among employees was a contributing factor which emphasizes the importance of further training to identify potential cyber threats and their responses. The study has also shed light on the importance of having a layered approach to security, where several measures of cybersecurity are applied vertically across all levels of operation, ranging from vessel systems to port operations. Ultimately, these monitoring capabilities should be integrated with continuous vulnerability management in order for shipping companies to pre-emptively defend against unwarranted access to security gaps. This will allow shipping companies to monitor, investigate, and respond effectively to cyber incidents, thus enhancing the overall posture of cyber security.

5 Discussion

5.1 Effects of Implementing Computer Forensics Methods on Global Maritime Transportation

The integration of computer forensics in global shipping can greatly enhance the investigation of cyber-related incidents. One of the primary effects is that it improves the general cybersecurity system of the shipping industry. Nowadays, computer threats are far more advanced, and shipping companies cannot depend on conventional security frameworks. Forensics includes the gathering, preservation, and analysis of evidence which aids in the thorough investigating computer breaches so that the violators will face the consequences. Forensics also helps enhance the incident response improvements through

preserving information as evidence. Companies are able to minimize disruption and data loss with the capture of information immediately after an attack. This can also advance the identification of security breaches leading to developing stronger defenses. Another very important effect of forensics is that it encourages collaboration from different sectors. It allows standardized forensic frameworks to be implemented in shipping so that companies together with regulatory and cybersecurity experts can address the threats better and enhance their measures for incident responsiveness. The implementation of forensics technology benchmarks trust pertaining to sensitive data and operational data among customers, stakeholders, and regulators as one of the prerequisites. Going beyond active protection measures, the adoption of such technologies further enables the global shipping system to dynamically adapt when facing new challenges. Ultimately, the application of computer forensic techniques within global shipping operations not only augments security, but also fortifies the industry against potential future cyber attacks.

5.2 The Issues and Constraints of Applying Computer Forensics in Cyber Investigations

Although it is clear that the implementation of computer forensic techniques offer benefits to global shipping activities, automation, and shipping technologies, there are still some hurdles and gaps that companies need to overcome. One of the foremost challenges is the intricate nature and variety of maritime systems. Custom developed software and hardware for ships pose a challenge for forensic investigators because proprietary software and hardware is developed by a multitude of vendors. This lack of standardization greatly hampers the use of universal forensics tools and techniques, requiring many to design specific tools and methods tailored to unique maritime technologies. The bespoke nature of forensic tools and techniques also prolongs the investigation process. Furthermore, one of the most pressing shipping company challenges is the lack of forensic readiness. The lack of ability to log, collect, and securely archive information programs on vessels and port operations actively results in the loss of important information that is needed to properly and effectively investigate cyber incidents. Preparation is very critical because without adequate preparation forensic grounded technologies and tools become futile and challenges like time constraints worsen the ability to investigate. Added to that, the ease with which vessels change their locations makes it more difficult to collect evidence because ships are frequently located in international waters or foreign seaports, and are subject to varying jurisdictions and legal systems. This results in problems concerning evidence ownership, data access, and compliance with jurisdictional regulations. Moreover, the budgetary constraints and resource limitations associated with having an in-house forensic team or purchasing forensic equipment may discourage some shipping companies from adopting holistic forensic approaches, particularly smaller ones. As a last point, the forensic strategies employed within the maritime sector may be limited due to the operations being time-critical. In particular, the need to maximize operational availability of the vessels complicates conducting detailed forensic examinations that may interrupt regular service, particularly when systems need to be analyzed in real time.

5.3 Shipping Sector Cybersecurity Solutions

To deal with the above issues, certain suggestions may be made. First, shipping firms need to implement measures that encourage active, persistent preparedness. For the shipping industry, this starts with the installation of special tools to aid in the capture and preservation of digital evidence throughout the industry. As noted previously, automated system loggers capable of monitoring vital components such as navigation, communication and cargo control systems are extremely useful. Hence, these companies will have the functional and tangible evidence necessary to enable them to conduct adequate investigations whenever there are instances of cyber incursion. Secondly, there is no uniform practice

of cyber security and forensic methodology standard throughout the sector. Such development and adoption of industry-specific guidelines on the measures to be taken when responding to incidents is useful in collecting information and in forensic evidence techniques streamlined investigative processes guided to further assist collaborative efforts around the globe. Regulatory bodies like the IMO need to enhance active participation in construction and steering shipping companies for compliant cyber incident response standards. Third, implement ongoing training and awareness campaigns to prepare shipping personnel to identify and respond to possible attacks (Malhotra & Iyer, 2024). Training on phishing, password management, and social engineering is equally important as it is human error that often leads to successful breaches. Forth, it is also helpful to encourage spending on advanced cybersecurity investments. A multi-layered security strategy involving the use of next-generation firewalls, intrusion detection systems, and endpoint protection must be put in place by shipping firms to meet ever-increasing cyber security challenges. In conclusion, companies need to form relationships with cybersecurity and digital forensic analysts to enable proper cyber incident investigations and rapid recovery from business disruptions. The relationships formed will aid forensic practitioners in formulating effective and operationally protective strategies in real-time response, thereby minimizing the time and resources lost during response to unanticipated financial constraints.

6 Conclusion

Global shipping has historically faced significant cyber threats and cyber-attacks, as evidenced by the case study analysis of global shipping cyber incidents. NotPetya's ransomware attack on Maersk and the COSCO breach amply illustrated the operational and financial consequences, not only to Maersk and COSCO, but also to other third party operators within the ecosystem. In averting cybersecurity threats, shipping companies suffer operational downtime, which incurs additional costs. Recovering lost data were the goals of employing various computer forensics techniques like disk imaging, malware analysis, and log file examination, which became essential in the investigation. Unfortunately, specialized forensic maritime technologies, archaeological forensic readiness, jurisdictional barriers, and a host of other forensic barriers exposed profound gaps within the investigative framework. Employing a range of forensic technologies and methodologies within the context of global shipping, which remains under researched, sets subdomains of computer forensics as new research landscapes. It has been shown that integrating forensic methodologies forces a rethink into shipping companies' cybersecurity governance policies, thereby reinforcing the need to develop operational frameworks that integrate maritime customs and forensics. Creating standards defined by the shipping industry's maritime culture and customs for forensic investigation, especially evidence creation and examination, becomes important into the investigation process. The addition of new forms of technology such as AI aimed towards incident monitoring can also be looked into as a way of advancing proactive measures designed to encourage forward thinking in incident detection. Also, solving the legal issues that come with multi-jurisdictional investigations, as well as increasing cybersecurity education among those working in the maritime field, are areas in need of more research. All these aspects will be critical in enhancing the defense and forensic strength of the shipping industry.

References

[1] Arvind, M., & Nair, A. (2025). Next-Generation Firewalls: Architecture and Effectiveness. In *Essentials in Cyber Defence* (pp. 35-55). Periodic Series in Multidisciplinary Studies.

[2] Azizova, F., Polvanova, M., Mamatov, A., Siddikova, S., Khasanova, N., Normamatova, P., Karshiev, A., & Zokirov, K. (2024). Evaluating the impact of communities-based fisheries education program on local communities attitudes towards sustainable fishing practices. *International Journal of Aquatic Research and Environmental Studies, 4*(S1), 71-76. https://doi.org/10.70102/IJARES/V4S1/12

[3] Bada, M., & Nurse, J. R. C. (2020). Developing cybersecurity education and awareness programmes for maritime sectors. *Journal of Cybersecurity, 6*(1), tyaa019.

[4] Baldwin, K., Goel, S., & Bhunia, S. (2020). Cybersecurity in maritime shipping: Challenges and solutions. *Journal of Maritime Affairs, 19*(3), 357–375. https://doi.org/10.1007/s13437-020-00200-5

[5] Berglund, M., & Jacobsson, A. (2019). Cybersecurity in the maritime industry: A systematic review. *Procedia Computer Science, 164,* 378–385.

[6] BIMCO. (2020). Industry Guidelines on Cyber Security Onboard Ships (4th ed.). https://www.bimco.org

[7] Carrier, B. (2018). *File system forensic analysis.* Addison-Wesley Professional.

[8] Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

[9] Chang, K. Y., Liu, L. M., & Lin, Y. C. (2020). Cybersecurity in smart shipping: Threats and countermeasures. *Marine Policy, 117,* 103894. https://doi.org/10.1016/j.marpol.2020.103894

[10] Di Renzo, B., Biondi, F., & Massacci, F. (2020). The cyber resilience of ships: A systematic review. *Computers & Security, 92,* 101752. https://doi.org/10.1016/j.cose.2020.101752

[11] Gopi Krishnan, V., Navaneetha Krishnan, T., Syed Karim, S., Yuvarajan, G., & Rama Priya, M. (2020). Cyber Security in Data Mining to Data Driven Security. *International Journal of Advances in Engineering and Emerging Technology, 11*(1), 71–76.

[12] Greenberg, A. (2020). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Anchor.

[13] Guerra, B. E. M., Ruiz, E. R. P., Barreto, J. V. A., Pérez, O. N. M., & Escobedo, F. (2024). Digital Marketing and Service Experience in a Peruvian Information Services Company. *Indian Journal of Information Sources and Services, 14*(3), 222–225. https://doi.org/10.51983/ijiss-2024.14.3.28

[14] Hosny, S., & Liles, S. (2019). Digital forensics in maritime security: Challenges and opportunities. *Journal of Digital Forensics, Security and Law, 14*(1), 1–14. https://doi.org/10.15394/jdfsl.2019.1531

[15] International Maritime Organization. (2020). Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3). https://www.imo.org

[16] International Maritime Organization. (2021). Shipping and World Trade: Facts and Figures. https://www.imo.org

[17] Ismail, K., & Khalil, N. H. (2025). Strategies and solutions in advanced control system engineering. *Innovative Reviews in Engineering and Science*, *2*(2), 25-32.

[18] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

[19] Kessler, G. C. (2022). *An introduction to computer forensics: Tools and techniques.* CRC Press.

[20] Malhotra, R., & Iyer, A. (2024). Developing an Effective Training System for Interventional Pulmonology Education through Digital Learning. *Global Journal of Medical Terminology Research and Informatics, 1*(1), 1-8.

[21] McLaughlin, M. (2019). Cyberattacks in maritime: The COSCO incident. *Maritime Executive, 17*(3), 14–18. https://www.maritime-executive.com

[22] Nelson, B., Phillips, A., Steuart, C., & Wilson, R. S. (2010). *Guide to computer forensics and investigations* (p. 720). Course Technology Cengage Learning.

[23] Palash, P. S., & Dhurvey, P. (2024). Analysis of Flyash Aggregate Behavior in Geopolymer Concrete Beams Using Method of Initial Functions (Mathematical Programming). *Archives for Technical Sciences, 2*(31), 168–174. https://doi.org/10.70102/afts.2024.1631.168
[24] Prabhudeva, T., & Hariharan, R. (2024). A Systematic Review and Meta-Analysis of Tuberculosis Patients: Perspectives of Pharmacists Towards Sustainability. *Clinical Journal for Medicine, Health and Pharmacy, 2*(4), 1-10.
[25] Radhi, A. E. J. A., & Abdulahad, A. F. (2023). Possibility of Reducing Risks of Audit Profession in Improving Audit Quality - A Case Study in the General Company for Electric Power Production / Southern Region. *International Academic Journal of Economics, 10*(2), 71–84. https://doi.org/10.9756/IAJE/V10I2/IAJE1008
[26] Reyes, J., Adiputra, Y., & Wibowo, A. (2021). Forensic readiness in maritime systems: A review and implementation roadmap. *International Journal of Cyber-Security and Digital Forensics, 10*(4), 297–306. https://doi.org/10.17781/P002511
[27] Sindhu, C. K., Sowmya, A. N., Haveela, B., & Kavya Nandini, G. (2021). Design of frequency reconfigurable microstrip antenna. *National Journal of Antennas and Propagation, 3*(1), 16–21.
[28] Soni, K., Kumar, U., & Dosodia, P. (2014). A Various Biometric application for authentication and identification. *International Journal of Communication and Computer Technologies (IJCCTS)*, *2*(1), 6-10.
[29] Tam, K., & Jones, K. (2018, June). Cyber-risk assessment for autonomous ships. In *2018 international conference on cyber security and protection of digital services (cyber security)* (pp. 1-8). IEEE. https://doi.org/10.1109/CyberSecPODS.2018.8560690
[30] Trisiana, A. (2024). A Sustainability-Driven Innovation and Management Policies through Technological Disruptions: Navigating Uncertainty in the Digital Era. *Global Perspectives in Management, 2*(1), 22-32.
[31] United Nations Conference on Trade and Development (UNCTAD). (2021). Review of Maritime Transport 2021. https://unctad.org/webflyer/review-maritime-transport-2021

Authors Biography

Capt. Ramesh Balasubramanian is a Master Mariner with 25 years of extensive sea-going experience in the deck department, having served on various dry fleet vessels. He holds academic qualifications from NIPM and HIMT and currently serves as an Associate Professor at AMET University. With a strong commitment to maritime education, he brings practical industry knowledge into the classroom, effectively preparing future marine professionals through structured training and real-world insights.

N. Anand started his sailing career with The Shipping Corporation of India as a Radio Officer and went on to sail for about 12 years with Univan Ship management, Hongkong and OMI Tankers, USA. He quit sailing in 2000 and took up a shore job with Southern Academy of Maritime Studies as Assistant Director. In 2005 he joined VELS UNIVERSITY as administrative officer of the maritime division. In 2007 he joined AMET UNIVERSITY and presently heads the GMDSS DEPARTMENT. He has published many research articles in marine related field in renowned international publishers.