A Potential Digital Evidence Classification Model for 5G NFV Environments Using Supervised Machine Learning Algorithms

Sheunesu Makura, Lucas Blanc and Hein Venter
University of Pretoria, South Africa

makura.sm@up.ac.za
u21436135@tuks.co.za
hventer@up.ac.za

Abstract: The adoption of fifth-generation (5G) mobile networks has increased significantly due to enhanced bandwidth, reduced latency, and support for heterogeneous services. Key enabling technologies such as Network Function Virtualisation (NFV) and network slicing introduce flexibility and scalability but also expand the attack surface for cyber threats. These threats complicate digital forensic investigations, particularly the identification and classification of Potential Digital Evidence (PDE) in dynamic virtualised environments. This paper proposes a machine learning-based classification model for PDE in 5G NFV environments to support digital forensic readiness (DFR). The model integrates digital evidence collection, preservation, and storage processes with supervised machine learning algorithms to automatically classify forensic artefacts. A Random Forest classifier was evaluated using a combined dataset consisting of CIC-IDS 2017 traffic and real 5G packet captures. Experimental results demonstrate high classification performance, achieving a weighted precision of 0.97, recall of 0.93, and F1-score of 0.95. Feature importance analysis further highlights key traffic characteristics relevant to forensic investigations. The proposed model enhances forensic readiness by enabling automated identification and categorisation of relevant evidence, reducing manual effort and improving investigation timeliness in 5G NFV environments.

Keywords: 5G networks, Network function virtualisation (NFV), Machine Learning, Potential digital evidence, Digital forensic investigation

1. Introduction

Mobile networks have experienced rapid growth over the past decade, driven by increasing demand for high-speed connectivity, low latency, and support for diverse digital services (Hassan, Yau and Wu 2019). Fifth generation (5G) networks introduce advanced capabilities through technologies such as Network Function Virtualisation (NFV) and network slicing, enabling flexible and scalable network deployments (Barakabitze et al. 2020). However, these technologies also introduce new security challenges by increasing system complexity and expanding the attack surface available to cyber adversaries (Madi et al. 2021).

The dynamic and distributed nature of NFV environments further complicates digital forensic investigations, as Potential Digital Evidence (PDE), including network traffic records, system logs, configuration files, and user activity traces, may be dispersed across virtualised components with limited persistence. PDE refers to any form of digital data that may prove potentially useful to a digital forensic investigation (Gogolin 2021). Consequently, identifying, collecting, and classifying forensic artefacts in real time remains a significant challenge for investigators, particularly in highly virtualised 5G infrastructures (Makura and Venter 2024).

Digital Forensic Readiness (DFR) seeks to maximise the availability and usability of digital evidence while minimising investigation costs and response time through proactive preparation mechanisms (Tan 2001). Although prior research has proposed DFR frameworks for 5G environments, limited work has focused on the automated classification of forensic artefacts using machine learning techniques. Addressing this gap, this paper proposes a supervised machine learning-based model for classifying PDE in 5G NFV environments. The model integrates DFR processes with automated classification to support timely and accurate digital forensic investigations. A Random Forest (RF) classifier is evaluated using a hybrid dataset comprising public intrusion detection data and real 5G network traffic.

The research problem addressed in this paper arises from the virtualised and transient nature of 5G NFV infrastructures, which makes manual identification and classification of forensic evidence difficult, time-consuming, and error-prone (Madi et al. 2021). To overcome these limitations, there is a need for automated mechanisms capable of classifying PDE in real time to support DFR and incident response.

The objectives of this study are fourfold: (i) to develop a machine learning-based model for classifying PDE in 5G NFV environments; (ii) to evaluate the performance of supervised learning algorithms for forensic artefact classification; (iii) to analyse feature importance in order to identify forensic-relevant network characteristics; and (iv) to demonstrate how automated classification can support DFR and reporting.

The key contributions of this paper are:

- A machine learning-based PDE classification model integrated with DFR processes for 5G NFV environments.
- An empirical evaluation using hybrid datasets, combining CIC-IDS 2017 intrusion data with real 5G packet captures.
- Feature importance analysis for forensic relevance, identifying network characteristics useful for forensic investigations.

The remainder of this paper is organised as follows. Section 2 presents background and related work on 5G NFV security and DFR. Section 3 describes the research methodology and machine learning model development. Section 4 presents experimental results. Section 5 discusses findings and limitations. Section 6 concludes the paper and outlines future research directions.

2. Background and Related Works

The evolution of 5G networks has significantly enhanced communication capabilities through high bandwidth, low latency, and support for diverse services. These advancements are enabled by technologies such as Network Function Virtualisation (NFV) and network slicing, which provide scalability and flexibility but also introduce increased complexity and expanded attack surfaces. As a result, forensic investigations in 5G environments become more challenging, particularly due to the distributed and transient nature of digital evidence. Ensuring DFR through proactive evidence collection, preservation, and classification is therefore critical. While international standards provide general guidance for digital investigations, they do not fully address the challenges of virtualised 5G NFV environments. At the same time, machine learning has shown strong potential in cybersecurity, particularly for intrusion detection, but its application to forensic artefact classification remains limited. This section reviews the foundations of 5G and NFV, associated security and forensic challenges, and the role of machine learning in supporting DFR, before positioning the proposed work within existing literature.

2.1 5G Networks and Network Function Virtualisation

5G Networks represent a significant evolution in cellular communication, providing enhanced data rates, ultra-low latency, and support for massive device connectivity. These capabilities enable emerging applications such as the Internet of Things (IoT), autonomous systems, and real-time analytics (Hassan, Yau and Wu 2019).

A key architectural shift in 5G is the adoption of NFV which replaces dedicated hardware appliances with software-based Virtual Network Functions (VNFs) running on commodity hardware (Yi et al. 2018). NFV improves scalability and flexibility while reducing deployment costs. Furthermore, 5G networks employ network slicing to create multiple logical networks over shared physical infrastructure, each optimised for specific service requirements (Barakabitze et al. 2020). Despite these advantages, virtualisation introduces additional complexity and expands the attack surface, creating new challenges for cybersecurity and digital forensic investigations.

2.2 Security Challenges in 5G NFV Environments

The integration of NFV and network slicing in 5G infrastructures introduces several security risks. The virtualisation layer creates opportunities for hypervisor attacks, compromised VNFs, and cross-slice interference (Madi et al. 2021). Additionally, distributed architectures increase exposure to denial-of-service attacks, malware propagation, and insider threats (Wichary et al. 2022).

Location-shift attacks, where VNFs migrate across physical hosts, further complicate monitoring and forensic tracking of malicious activities (Yi et al. 2018). These challenges necessitate advanced detection and forensic mechanisms capable of operating in highly dynamic environments.

2.3 Digital Forensics and Digital Forensic Readiness

Digital forensics (DF) focuses on the identification, acquisition, preservation, analysis, and presentation of digital evidence following a security incident (Gogolin, 2021). This process is typically reactive, meaning evidence is collected after systems may have been altered or compromised. Digital Forensic Readiness (DFR), in contrast, adopts a proactive approach by ensuring that relevant evidence is systematically collected,

preserved, and readily available before incidents occur (Tan, 2001). Rather than replacing DF, DFR enhances the efficiency, reliability, and evidentiary value of investigations.

This distinction is particularly important in 5G NFV environments, where virtualised network functions are dynamic and distributed, and digital artefacts may be short-lived. In such contexts, reactive approaches increase the risk of evidence loss, while DFR enables continuous evidence collection and organisation to support effective post-incident analysis. ISO/IEC 27043 provides a structured framework for DFR through defined readiness processes, including planning, implementation, and assessment (Valjarević and Venter, 2016; ISO/IEC, 2015). Supporting standards such as ISO/IEC 27037 and ISO/IEC 27041 address evidence handling and investigative procedures (Ajijola, Zavarsky and Ruhl, 2014; ISO/IEC, 2012; ISO/IEC, 2016). However, these standards do not explicitly address the complexities of 5G NFV environments.

This research builds on these standards by applying DFR principles within a 5G NFV context and integrating machine learning-based classification. The proposed model aligns with ISO/IEC 27043 to ensure that automated classification of Potential Digital Evidence is both technically effective and forensically sound. standards.

2.4 Investigation Challenges in 5G NFV Environments

Forensic investigations in NFV-based 5G networks face several technical and operational challenges. Evidence sources are distributed across cloud-based infrastructure, edge devices, and virtualised network components, leading to difficulties in evidence acquisition and correlation. High-speed traffic volumes further exceed the processing capabilities of traditional forensic tools (Madi et al. 2021). Cross-domain investigations involving multiple service providers and administrative domains introduce legal and jurisdictional complexities. Moreover, the dynamic lifecycle of virtual machines and containers results in transient evidence that may be lost if not captured proactively.

2.5 Machine Learning for Cybersecurity and Digital Forensics

Machine learning techniques have been widely applied in intrusion detection, anomaly detection, and cyber threat classification. Supervised learning models such as Logistic Regression, Support Vector Machines, Random Forests, and Neural Networks have demonstrated effectiveness in detecting network attacks (Moham, Sugunaraj and Ranganathan 2022).

RF classifiers are particularly suited for tabular network traffic data due to their robustness, resistance to overfitting, and interpretability. Deep learning models such as Multilayer Perceptrons (MLP) can capture complex non-linear patterns but often require large datasets and computational resources.

However, existing research has largely focused on intrusion detection rather than forensic artefact classification. Limited work has explored how machine learning can support DFR by automatically identifying and categorising PDE in virtualised network environments.

2.6 Related Work

Research on machine learning for cybersecurity in 5G and virtualised network environments has grown significantly, with most studies focusing on intrusion detection, anomaly detection, and traffic classification. Supervised learning approaches, in particular, have demonstrated strong performance in identifying malicious activities within complex and high-throughput network infrastructures.

Several studies have evaluated the effectiveness of supervised machine learning algorithms, including RF, SVM, and LR in 5G network contexts. For example, Mohan et al. (2022) investigated multiple supervised learning techniques for cybersecurity in 5G networks and reported that ensemble-based models such as RF consistently achieve high detection accuracy. Their findings highlight the suitability of RF for handling high-dimensional network traffic data and complex attack patterns.

Similarly, Ferrag et al. (2022) explored machine learning-based intrusion detection approaches for Software-Defined Networking (SDN) and Network Function Virtualisation (NFV)-enabled 5G environments. Their work demonstrates that supervised classifiers are effective in detecting distributed and sophisticated attacks in next-generation network architectures. In another study, Krishnan and Salim (2018) applied supervised learning techniques to classify malicious traffic in virtualised infrastructures, showing improved detection performance compared to traditional rule-based systems.

Across these studies, RF has emerged as a widely adopted technique due to its robustness, resistance to overfitting, and ability to model non-linear relationships in heterogeneous data. Its ensemble structure allows it to perform well in environments characterised by noisy, high-dimensional, and mixed-type features conditions typical of 5G NFV networks. Furthermore, RF provides intrinsic feature importance measures, which enhance interpretability and are particularly valuable in cybersecurity applications.

However, despite the demonstrated success of machine learning techniques in intrusion detection, existing research predominantly focuses on real-time attack detection and prevention, with limited attention given to DF requirements. Specifically, issues such as evidence preservation, DFR, evidentiary traceability, and post-incident investigation support are not extensively addressed. As a result, there remains a clear gap between machine learning-based detection systems and the needs of DF investigations.

Makura and Venter (2024) proposed a DFR model tailored for 5G NFV environments, emphasising proactive evidence collection and preservation. While this work provides an important conceptual foundation, it does not incorporate automated classification of forensic artefacts or empirical evaluation using machine learning techniques.

This study builds upon and extends prior work by integrating supervised machine learning specifically RF classification into a DFR framework. Unlike existing approaches that prioritise threat detection, the proposed model focuses on the classification of PDE to support forensic investigation processes. By aligning machine learning outputs with ISO/IEC 27043 readiness principles, this research bridges the gap between cybersecurity monitoring and DF investigation, enabling automated, interpretable, and forensically relevant evidence classification in 5G NFV environments.

Table 1 summarises key related studies and highlights the distinction between intrusion detection-focused approaches and the forensic readiness-oriented contribution of this work.

Table 1: Summary of related work on supervised machine learning in 5G and virtualised network environments

Study	Environment	Machine Learning Approach	Primary Focus	Forensic Readiness Support
Mohan, Sugunaraj and Ranganathan (2022)	5G networks	Supervised ML (RF, SVM, LR)	Intrusion detection	No
Ferrag et al. (2022)	5G / SDN / NFV	Supervised ML classifiers	Attack detection and prevention	No
Krishnan & Salim (2018)	SDN/NFV networks	Supervised ML	Malicious traffic classification	No
Makura and Venter (2024)	5G NFV	Conceptual forensic framework	Digital forensic readiness	Partial (no ML evaluation)
This study	5G NFV	Supervised ML (Random Forest)	Potential Digital Evidence classification	Yes (ISO/IEC 27043-aligned)

3. Methodology

To address the challenges of classifying PDE in complex 5G NFV environments, this study employs a structured quantitative experimental methodology. The approach is designed to ensure both scientific rigor and practical relevance by combining synthetic intrusion detection data with real-world 5G network traffic. The methodology encompasses several interconnected phases: research design, dataset acquisition, preprocessing, feature engineering, model development, and experimental evaluation. Each phase is carefully aligned with the overarching goal of enhancing DFR through automated evidence classification. By integrating supervised machine learning techniques with forensic processes, the methodology not only evaluates algorithmic performance but also demonstrates how automated classification can be embedded into forensic workflows to support timely investigation, reporting, and incident response.

3.1 Research Design

This study adopts a quantitative experimental research design to develop and evaluate a machine learning-based model for classifying PDE in 5G NFV environments. The methodology consists of data acquisition, preprocessing, feature engineering, model training, and performance evaluation. The proposed model aims to support DFR by automating the identification and classification of forensic artefacts.

3.2 Dataset Description

Two datasets were used in this study:

1. **CIC-IDS 2017 Dataset:** A publicly available intrusion detection dataset containing benign and malicious network traffic, widely used for cybersecurity research (Canadian Institute for Cybersecurity 2017). The dataset includes multiple attack categories such as denial-of-service, brute force, infiltration, and web-based attacks.
2. **Real 5G Network Traffic and Logs:** Packet captures and system logs collected from a simulated 5G test environment. These logs contain network events, system messages, and traffic metadata relevant for forensic analysis.

The combination of synthetic and real-world data enhances the ecological validity of the proposed model. Although the dataset includes real 5G packet captures and logs, these were collected within a controlled testbed environment designed to emulate key characteristics of operational 5G networks, rather than from a live production network.

3.3 Data Preprocessing

The datasets were preprocessed to ensure consistency and suitability for machine learning analysis. Preprocessing steps included:

- Removal of duplicate and incomplete records
- Handling missing values through imputation
- Normalisation and scaling of numerical features
- Label encoding of categorical variables

For textual 5G network logs, preprocessing included tokenisation, stop-word removal, and term frequency inverse document frequency (TF-IDF) vectorisation to transform unstructured log text into numerical feature vectors suitable for classification.

3.4 Feature Engineering

Feature engineering was conducted to extract relevant attributes for forensic classification. Network traffic features included flow duration, packet counts, byte rates, protocol types, and flag statistics. Log-based textual features were represented using TF-IDF vectors to capture semantic patterns associated with attack events and system anomalies. Feature selection techniques were applied to reduce dimensionality and remove redundant features, improving model performance and computational efficiency.

3.5 Machine Learning Model Development

Several supervised machine learning algorithms were evaluated, including LR, SVM, MLP, and RF classifiers. RF was selected as the primary model due to several characteristics that make it particularly suitable for 5G NFV forensic environments.

First, RF performs well on high-dimensional and heterogeneous data, which is essential in this study where both structured network traffic features and unstructured log-derived features are combined. Second, RF is robust to noise and overfitting, which is important in dynamic 5G environments where traffic patterns may vary significantly. Third, RF provides intrinsic feature importance measures, enabling interpretability and supporting forensic requirements such as evidentiary traceability and justification of analytical decisions.

Furthermore, ensemble-based methods such as RF have demonstrated strong performance in prior cybersecurity studies, particularly in intrusion detection and traffic classification tasks within 5G and virtualised environments. These characteristics motivated the selection of RF as the primary model for PDE classification in this study.

3.6 Experimental Setup

The dataset was divided into training and testing subsets using an 80/20 split. Cross-validation was performed to reduce bias and ensure generalisability of results. Model performance was evaluated using precision, recall, F1-score, and accuracy metrics. Feature importance analysis was conducted to identify attributes most relevant for forensic investigations, providing insights into evidence prioritisation.

3.7 Forensic Readiness Integration

The proposed classification model was integrated into a DFR workflow, including evidence collection, preservation, storage, and reporting processes. Classified forensic artefacts were automatically summarised to support investigation documentation and incident response.

4. Experimental Results

This section presents the outcomes of the experimental evaluation conducted to assess the effectiveness of supervised machine learning models in classifying PDE within 5G NFV environments. The results highlight both the comparative performance of baseline algorithms and the superior capabilities of the RF classifier, which consistently achieved the highest precision, recall, F1-score, and accuracy across diverse attack categories and benign traffic. Beyond raw performance metrics, the experiments also provide insights into the forensic relevance of specific network and log-based features, demonstrating how automated classification can prioritise critical attributes for investigation. The findings not only validate the robustness of the proposed model but also underscore its practical implications for DFR, showing how machine learning can reduce manual effort, accelerate evidence triage, and strengthen incident response in dynamic and distributed 5G infrastructures.

4.1 Model Performance Evaluation

The performance of the supervised machine learning models was evaluated using precision, recall, F1-score, and accuracy. LR, SVM, MLP, and RF classifiers were implemented and compared.

Table 2 summarises the classification performance of the evaluated models. RF achieved the highest overall performance across all metrics, indicating its suitability for forensic artefact classification in 5G NFV environments.

Table 2: Performance comparison of machine learning models

Model	Precision	Recall	F1-score	Accuracy
Logistic Regression	0.06	0.04	0.05	0.08
Support Vector Machine	0.25	0.20	0.22	0.26
Multilayer Perceptron	0.90	0.86	0.88	0.89
Random Forest	0.97	0.93	0.95	0.94

4.2 Random Forest Classification Results

The RF classifier achieved a weighted precision of 0.97, recall of 0.93, and F1-score of 0.95, outperforming all baseline models. These results demonstrate the model's ability to accurately classify PDE associated with different 5G related cyberattack types and benign traffic.

Figure 1 presents the confusion matrix for the RF model, illustrating classification accuracy across attack categories and benign traffic classes.

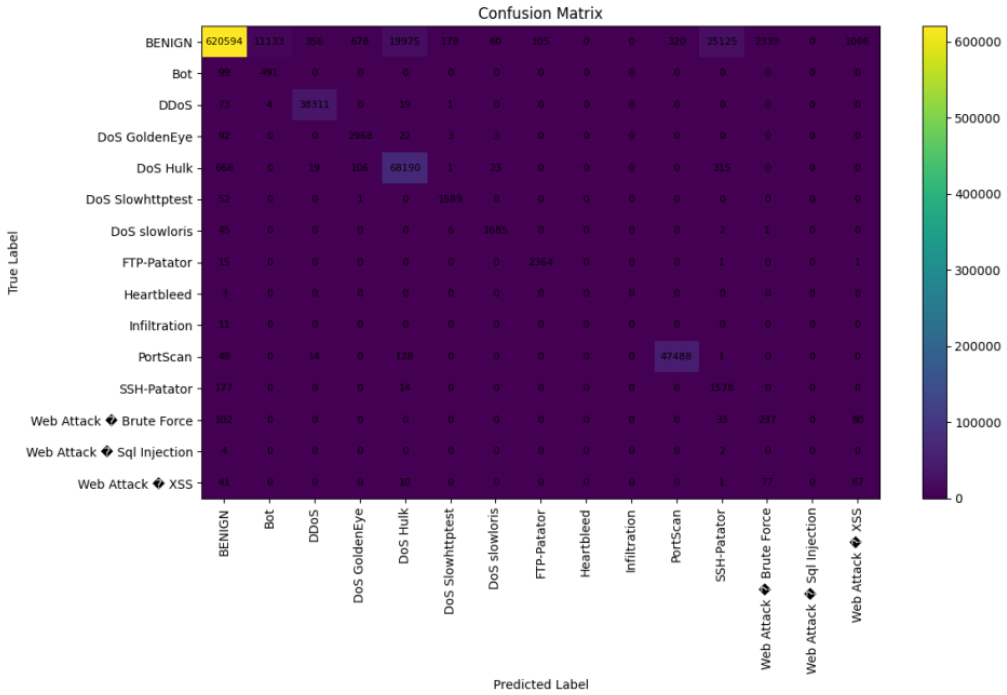

Figure 1: Confusion matrix for Random Forest classifier

4.3 Comparative Analysis with Baseline Models

LR and SVM demonstrated moderate classification performance but exhibited reduced recall for minority attack classes. The MLP model captured non-linear patterns but showed higher variance and training complexity compared to RF.

The superior performance of RF can be attributed to its ensemble-based decision trees, which effectively handle heterogeneous network traffic and log-based features while reducing overfitting.

Figure 2 illustrates the comparative F1-scores of the evaluated models.

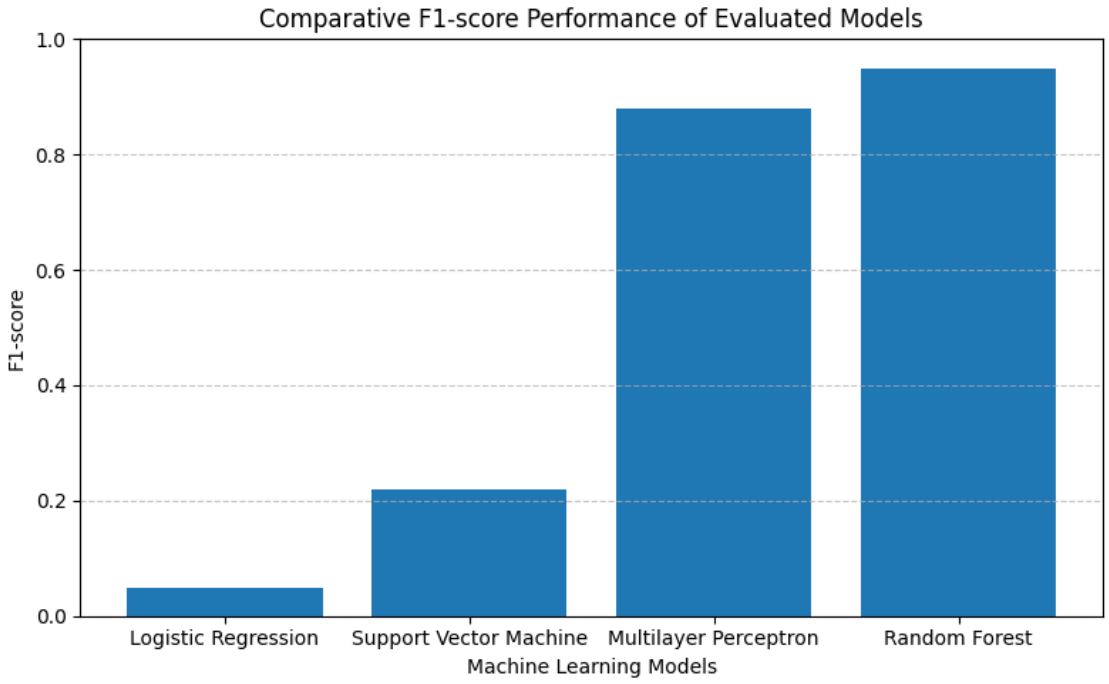

Figure 2: Comparative performance of machine learning models

4.4 Feature Importance Analysis

To enhance forensic interpretability and support evidentiary analysis, feature importance analysis was conducted using the RF classifier. RF models provide intrinsic feature importance scores based on the contribution of each feature to the ensemble decision process.

Figure 3 illustrates the top-ranked features influencing classification outcomes. Highly weighted features included network flow characteristics such as packet size variance, flow duration, byte rates, and protocol-related attributes. These features are commonly associated with abnormal traffic patterns and are particularly relevant for distinguishing between benign and malicious network activity in high-speed 5G environments.

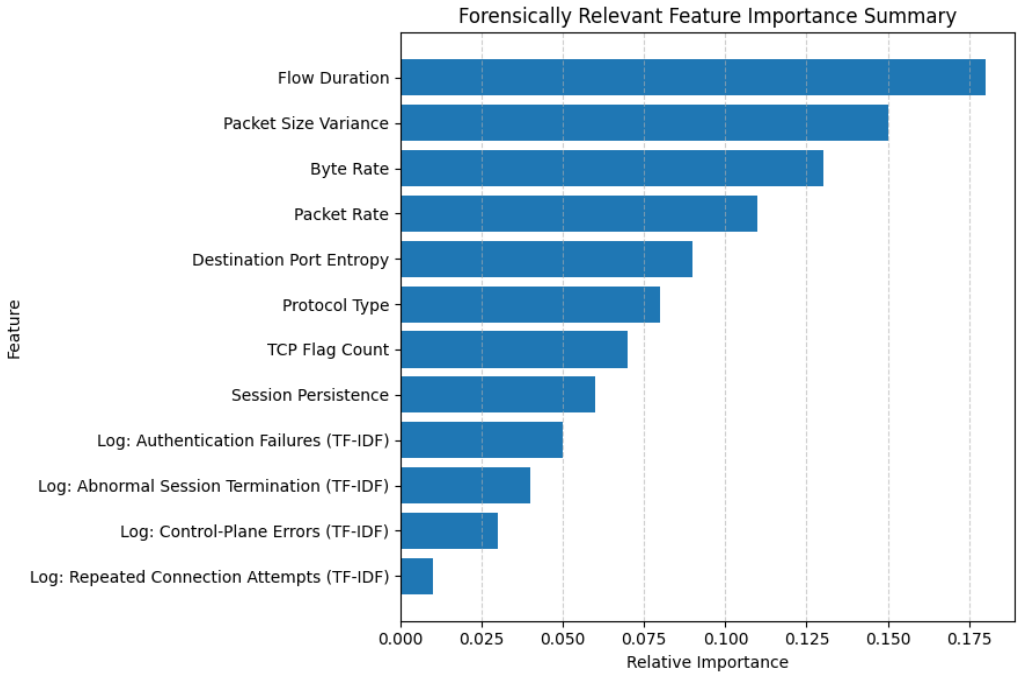

Figure 3: Summary of forensically relevant features frequently identified as influential during Random Forest model evaluation for PDE classification in a 5G NFV environment

In addition to traffic-based features, several log-derived features represented using TF-IDF vectorisation were identified as significant contributors. These features capture semantic patterns in 5G network and system logs, such as authentication failures, session terminations, and abnormal control-plane events. Their prominence highlights the importance of integrating both structured network metrics and unstructured log data when classifying PDE.

From a DFR perspective, the identification of salient features supports evidence prioritisation and investigative decision-making. By highlighting attributes most indicative of malicious activity, investigators can focus on high-value artefacts during post-incident analysis. This aligns with the interpretability and traceability principles emphasised in ISO/IEC 27043 readiness processes. The feature importance summary presented reflects the most consistently influential attributes observed during model evaluation, rather than a single extracted importance vector, and is intended to support forensic interpretability rather than precise model introspection.

4.5 Implications for Digital Forensic Readiness

The experimental results demonstrate that machine learning-based classification can significantly enhance DFR by automating the identification and categorisation of PDE. Automated classification reduces manual triage effort and accelerates forensic investigations, particularly in dynamic 5G NFV environments where evidence is transient and distributed.

5. Results and Discussion

This section discusses the experimental findings and critically evaluates the proposed machine learning-based classification model in the context of DFR for 5G NFV environments.

5.1 Discussion of Results

The experimental results demonstrate that supervised machine learning techniques can effectively support the classification of PDE in virtualised 5G NFV environments. Among the evaluated models, the RF classifier consistently outperformed LR, SVM, and the MLP across all evaluation metrics.

The superior performance of RF can be attributed to its ensemble-based structure, which enables the model to capture complex, non-linear relationships across heterogeneous feature sets. This is particularly relevant in 5G NFV environments, where evidence sources include both structured network traffic metrics and unstructured log-based artefacts.

While the MLP achieved competitive performance on frequently occurring attack classes, its effectiveness diminished when class support was limited. In contrast, RF maintained stable performance across both dominant and minority attack categories, making it more suitable for DFR scenarios where consistent detection and classification are critical.

5.2 Digital Forensic Readiness and Evidentiary Value

A key contribution of this research is the integration of machine learning-based classification with DFR principles. Rather than focusing solely on intrusion detection, the proposed model emphasises the identification and categorisation of PDE suitable for forensic investigation.

Feature importance analysis further enhances forensic applicability by identifying attributes most relevant to evidentiary interpretation, such as packet size variance, flow duration, and log-derived indicators. These insights support prioritisation of evidence during investigations and improve the interpretability of automated decisions.

The automated generation of structured forensic reports demonstrates how detection outputs can be transformed into actionable evidential artefacts. This capability reduces manual overhead, supports timely incident response, and aligns with forensic standards that emphasise traceability and documentation.

5.3 Strengths of the Proposed Approach

5.3.1 Multi-source evidence integration

The combination of publicly available intrusion detection data with real 5G network traffic and logs improves the generalisability of the proposed model. By learning from both synthetic and real-world sources, the system better reflects the diversity of data encountered in operational environments.

5.3.2 Interpretability and explainability

Unlike deep learning approaches that operate as black boxes, the Random Forest classifier provides interpretable decision structures through feature importance measures. This transparency is particularly valuable in forensic contexts, where investigators must justify conclusions and evidence handling decisions.

5.3.3 Alignment with forensic standards

The proposed workflow aligns with established DFR standards by supporting systematic evidence collection, preservation, analysis, and reporting. Although not explicitly standard-compliant, the model complements existing frameworks and enhances their applicability in 5G NFV contexts.

5.4 Limitations and Threats to Validity

Despite promising results, several limitations must be acknowledged. First, although the dataset was enhanced using real 5G traffic and logs, the experimental environment was based on a controlled laboratory testbed rather than a live operator network. Consequently, certain operational characteristics, such as dynamic network slicing policies and large-scale mobility patterns, were not fully captured.

Second, publicly available intrusion datasets such as CIC-IDS 2017 do not represent the full spectrum of contemporary or emerging 5G-specific attack vectors. As a result, some attack classes may be underrepresented, potentially affecting generalisability.

Third, while standard evaluation metrics provide useful performance insights, additional operational metrics such as detection latency, resource consumption, and scalability were outside the scope of this study. These factors are particularly relevant in high-throughput 5G environments and should be addressed in future work.

5.5 Implications for Cybersecurity and Cyber Warfare

From a cybersecurity and cyber warfare perspective, the findings indicate that automated forensic artefact classification can enhance situational awareness and post-incident analysis in complex network infrastructures. In high-tempo environments where attacks may be persistent, distributed, and multi-vector, the ability to rapidly identify and categorise evidence supports both tactical response and strategic assessment. The proposed approach contributes toward bridging the gap between detection systems and forensic investigation capabilities, enabling organisations to move beyond reactive defence toward proactive forensic preparedness.

6. Conclusion and Future Work

This paper presented a machine learning-based model for classifying PDE in 5G NFV environments and thereby attain DFR in 5G NFV environments. By integrating supervised machine learning with DFR processes, the proposed approach addresses the challenges posed by dynamic, virtualised network infrastructures such as 5G. Experimental results demonstrated that the Random Forest classifier outperformed baseline models, achieving a weighted F1-score of 0.95 while providing superior interpretability. The ability to identify and prioritise forensic-relevant features, combined with automated report generation, supports efficient evidence handling and post-incident investigation. The findings confirm that machine learning-based classification can play a valuable role in enabling DFR within 5G NFV environments by reducing manual effort, enhancing evidentiary clarity, and supporting timely incident response.

While this study incorporated real 5G traffic within a controlled testbed to approximate operational conditions, future research will extend the proposed model to fully deployed 5G core environments (e.g., Open5GS-based infrastructures) to validate performance under true operational conditions, including live network slicing, large-scale user mobility, and production-level traffic variability. Expanding the dataset to incorporate additional attack types and contemporary threat scenarios will further improve generalisability. Future work will also investigate the use of explainable artificial intelligence techniques, such as SHAP and LIME, to enhance transparency and strengthen the evidentiary value of automated classifications. Additional performance metrics, including detection latency, throughput, and resource utilisation, will be explored to assess real-world feasibility.

Acknowledgements

Acknowledgement and funding Support: The authors acknowledge the support received through the Network Security Call grant from the South African National Research Network (SANReN), which contributed to the research activities underlying this work. The support is gratefully acknowledged.

Ethics Declaration: This research did not involve human participants, personal data, or animal subjects. All network traffic and log data were collected from publicly available datasets and controlled laboratory test environments. Ethical clearance was therefore not required for this study.

AI Declaration: AI tools, including ChatGPT, were used to assist with language refinement, structural editing, and clarity improvement of the manuscript. All research design, data collection, experiments, analysis, and results are the original work of the authors.

References

Ajijola, A., Zavarsky, P. and Ruhl, R. (2014) 'A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev. 1:2014 and ISO/IEC 27037:2012', *Proceedings of the World Congress on Internet Security (WorldCIS)*, pp. 66–73. DOI: https://doi.org/10.1109/WorldCIS.2014.7028169

Barakabitze, A.A., Ahmad, A., Mijumbi, R. and Hines, A. (2020) '5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges', *Computer Networks*, 167, 106984. DOI: https://doi.org/10.1016/j.comnet.2019.106984 .

Canadian Institute for Cybersecurity (2017) *CIC-IDS2017 Intrusion Detection Evaluation Dataset*. Canadian Institute for Cybersecurity, University of New Brunswick. Available at: https://www.unb.ca/cic/datasets/ids-2017.html (Accessed: 29 December 2025).

Ferrag, M.A., Maglaras, L., Janicke, H. and Smith, R. (2019) 'Deep learning techniques for cyber security intrusion detection: A detailed analysis', *Computer Networks*, 207, 108879. DOI: https://doi.org/10.14236/ewic/icscsr19.16 .

Gogolin, G. (2021) *Digital forensics explained*. 2nd Edition. Boca Raton, FL: CRC Press. DOI: https://doi.org/10.1201/9781003049357

Hassan, N., Yau, K.-L.A. and Wu, C. (2019) 'Edge computing in 5G: A review', *IEEE Access*, 7, pp. 127276–127289. DOI : https://doi.org/10.1109/ACCESS.2019.2938534

ISO/IEC (2012) *ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. Geneva: International Organization for Standardization.

ISO/IEC (2015) *ISO/IEC 27043:2015 — Information technology — Security techniques — Incident investigation principles and processes*. Geneva: International Organization for Standardization.

ISO/IEC (2016) *ISO/IEC 27041:2016 — Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative methods*. Geneva: International Organization for Standardization.

Makura, S. and Venter, H. (2024) 'Towards the development of a digital forensic readiness model for 5G NFV environments', *Proceedings of the IST-Africa Conference*, pp. 1–12. DOI: https://doi.org/10.23919/IST-Africa63983.2024.10569788

Madi, T., Alameddine, H.A., Pourzandi, M. and Boukhtouta, A. (2021) 'NFV security survey in 5G networks: A three-dimensional threat taxonomy', *Computer Networks*, 197, 108288. DOI: https://doi.org/10.1016/j.comnet.2021.108288

Mohan, J.P., Sugunaraj, N. and Ranganathan, P. (2022) 'Cyber security threats for 5G networks', *Proceedings of the IEEE International Conference on Electro Information Technology (eIT)*, pp. 446–454. DOI: https://doi.org/10.1109/eIT53891.2022.9813965 .

Krishnan, N. and Salim, A., 2018, July. Machine learning based intrusion detection for virtualized infrastructures. In *2018 International CET Conference on Control, Communication, and Computing (IC4)* (pp. 366-371). IEEE. DOI: https://doi.org/10.1109/CETIC4.2018.8530912

Tan, J. (2001) 'Forensic readiness', *Stake Journal*, 1(1), pp. 1–8.

Valjarević, A., Venter, H. and Petrović, R. (2016) 'ISO/IEC 27043:2015—role and application', *Proceedings of the 24th Telecommunications Forum (TELFOR)*, pp. 1–4. DOI: https://doi.org/10.1109/TELFOR.2016.7818718

Wichary, T., Batalla, J.M., Mavromoustakis, C.X., Żurek, J. and Mastorakis, G. (2022) 'Network slicing security controls and assurance for verticals', *Electronics*, 11(2), 222. DOI: https://doi.org/10.3390/electronics11020222

Yi, B., Wang, X., Li, K. and Huang, M. (2018) 'A comprehensive survey of network function virtualization', *Computer Networks*, 133, pp. 212–262. DOI: https://doi.org/10.1016/j.comnet.2018.01.021

Zhang, P. and Martonosi, M. (2012) *What is mobile computing?* Hershey, PA: IGI Global.