Intention Recognition for Digital Forensics: A Formal Model

Yidnekachew Worku Kassa *, Joshua Isaac James , Elefelious Getachew Belay

Posted Date: 11 February 2025

doi: 10.20944/preprints202502.0764.v1

Keywords: Digital Forensics; Intention Recognition; Goal Recognition; plan recognition; cyberattack; cybercrime; model

 doi:10.20944/preprints202502.0764.v1

Article

Intention Recognition for Digital Forensics: A Formal Model

Yidnekachew Worku Kassa [1,*], Joshua Isaac James [2] and Elefelious Getachew Belay [1]

[1] School of Information Technology and Engineering, Addis Ababa Institute of Technology (AAiT), Addis Ababa University, Addis Ababa, Ethiopia
[2] DFIR Science LLC
* Correspondence: yidnekachew.worku@aau.edu.et or yidnekacheworku@gmail.com

Abstract: The rapid advancement of technology has been matched by a significant rise in cybercrime, posing substantial challenges for digital forensics investigators who must handle increasingly complex cases and navigate vast volumes of evidence. While current research on intent recognition has largely focused on cybersecurity measures for preventing attacks, there has been a noticeable gap in the integration of legal intent analysis with technical digital forensics. This paper addresses this gap by presenting an innovative model that combines legal and technical perspectives through a formal model. The model consists of three core components—Evidence Analysis, Intent Recognition, and a Criminal Repository—that systematically process digital evidence, reconstruct crime scenes, identify criminal intent, and offer recommendations for the conviction process. Using formal methods, the model rigorously defines key concepts such as crime, intent, and intent types, ensuring its robustness and reliability. By stimulating the model using phishing attack scenarios, we validate the model's capability, demonstrating its ability to identify various types of intent and manage complex cases. Looking forward, we suggest implementing the model by incorporating advanced AI approaches, particularly Agentic AI, or combining logic-based methods with explainable AI. This advancement would help address huge volume-related challenges of digital forensics and provide a powerful tool for modern investigative practices.

Keywords: digital forensics; intention recognition; goal recognition; plan recognition; cyberattack; cybercrime; model

1. Introduction

The exponential expansion of cyberspace, coupled with its inherent vulnerabilities and the challenges in raising awareness, has created an optimal environment for the proliferation of cybercrime [1,2]. Cybercrime encompasses not only attacks on cyber infrastructure but also the use of cyberspace to facilitate traditional crimes, as well as crimes that involve cyberspace in any capacity [3,4]. In the current digital era, the lines between traditional crime and cybercrime are increasingly blurred, as digital technology becomes more integrated with the physical world [4,5]. The surge in cybercrime is evident not only in the rising number of cases but also in the escalating volume and complexity of the data and technologies that must be scrutinized in each instance [1–3]. Digital forensics laboratories, tasked with the scientific investigation of cybercrimes, are currently inundated with cases, both in terms of case complexity as well as quantity and the sheer volume of data to be analyzed [6,7]. The digital investigation is now recognized as a significant big data challenge as without automation it is impossible to solve cases [8,9]. Various strategies have been proposed to manage the vast volumes of data encountered in digital forensics (DF), including data reduction techniques, data mining methodologies, triage procedures, and intelligence-driven approaches [10]. Each of these strategies offers a unique perspective on how to tackle the challenges posed by the ever-growing datasets in DF investigations.

 doi:10.20944/preprints202502.0764.v1

To address the challenge of managing large volumes of data in digital forensics, we propose a novel approach centered on Intention Recognition (IR). By discerning the underlying intentions, investigators can more effectively navigate the complexities of cyber investigations. Existing models for IR span various domains, primarily focusing on predicting goals and recognizing plans through the analysis of action sequences and state transitions. Some models employ Causal Networks to infer intent, while another leverages Path Analysis for similar purposes [11]. Further models incorporate advanced techniques such as Hidden Markov Models (HMM) [12], Deep Learning (DL) [13], and Long Short-Term Memory (LSTM) [14].

Despite the diversity of these models, they share a commonality: they are all predicated on a technical interpretation of IR, aimed at anticipating an attacker's objectives based on the subsequent actions and the current states. However, the aspect of intention as legally defined, considering the nuances of law and its implications, remains an unexplored territory in research. This gap presents an opportunity to develop a model that not only predicts technical behaviors but also aligns with legal definitions of intent, thereby bridging the divide between cyber forensics and legal aspects.

Legal doctrine categorizes intent, also known as mens rea, into four distinct types: purposeful, knowing, reckless, and negligent [15,16]. An individual is said to possess a purposeful intent when they consciously engage in actions that result in harm. Conversely, a knowing intent is ascribed to those who, while not actively seeking to cause harm, are aware that their actions have the potential to do so, thus representing a lesser degree of intent compared to purposeful intent. Recklessness is characterized by a disregard for a substantial and unjustifiable risk that a reasonable person would not ignore under similar circumstances. Lastly, negligent intent is attributed to individuals who fail to exercise the level of care that a reasonable person would consider prudent [15]. Each criminal act is evaluated against these gradations of intent, with the degree of culpability being largely contingent upon the level of intent demonstrated. This nuanced understanding of intent is crucial for the legal adjudication of crimes, as it directly influences the severity of charges and penalties imposed [15,17].

1.1. Paper Organization

This manuscript is structured into five comprehensive sections. The Introduction forms the first section, setting the stage for the ensuing discourse and establishing the context of the research. Section 2 delves into a critical examination of digital forensics and intention recognition, offering a synthesis of pertinent literature and existing methodologies. Section 3, discusses the methodology and approach we employed to develop the model. In Section 4, we formally define the important concepts in relation to DF and IR, laying the ground to the development of the model. Section 5, presents our innovative model for integrating IR within DF. This section not only elucidates the theoretical underpinnings of the model but also subjects it to validation through a series of scenarios. Section 6, the Discussion, is dedicated to a thorough analysis of the results obtained from the model's application on the scenarios. Here, we interpret the findings, drawing connections to the broader implications for the field of digital forensics. Finally, Section 7 encapsulates the Conclusion of our study, reflecting on the research outcomes and proposing trajectories for future inquiry. This conclusive part aims to provide closure to the current research while simultaneously opening avenues for subsequent scholarly exploration.

2. Literature Review

2.1. Digital Forensics

Digital forensics (DF) is a specialized field of forensic science that focuses on the recovery and investigation of digital technologies, often in connection with computer crime [18,19]. The practice involves the application of scientific principles and technological methods by considering legal requirements, to collect, analyze, and present data from digital sources [19,20]. It plays a crucial role in solving crimes that involve digital technologies, ensuring that digital evidence is handled in a legally admissible way.

 doi:10.20944/preprints202502.0764.v1

The essence of DF lies in its ability to establish the truth about digital events or activities. It applies a rigorous, scientific approach to the digital domain to uncover facts that can have real-world consequences, combining elements of law, computer science, and ethics [18,20,21]. It provides crucial evidence in legal proceedings, enhances cybersecurity, aids in incident response, ensures accountability, helps prevent future attacks, recovers data, contributes to cybersecurity intelligence, and builds trust in digital systems.

DF faces several challenges, including the overwhelming volume of data, strong encryption, data destruction, device diversity, cloud forensics, legal and ethical issues, tool efficacy, training and resources, rapid technological change, and the complexity of cases [6,21–24]. These challenges necessitate continuous development in the field, both technologically and in terms of expertise.

Various methodologies have been employed to address the challenges posed by the vast volume of data and the complexity of case analysis. In this study, we leverage the principles of intention recognition to develop a model for digital forensic investigation.

2.2. Intention Recognition

Intention recognition (IR) is a crucial concept in artificial intelligence, human-computer interaction, and psychology, aimed at understanding and predicting a person's goals based on their behavior, context, and communication [25–27]. It involves interpreting various cues to determine what a person intends to do. This concept is particularly important in areas like artificial intelligence (AI), human-computer interaction (HCI), and robotics, where understanding human intent is key for effective interaction or decision-making. [27–29].

In DF and cyber security, IR can be considered as identifying the plan or goal of the attacker or a criminal by analyzing the actions they perform or the observable behaviors they exhibit, and then inferring the specific plan they might be following to achieve those goals [11,25,30]. The problem of IR has been approached using a variety of AI methodologies, including logic-based approaches [31,32], classical machine learning [14,33], and deep learning methods [34,35] [30].

However, intention recognition faces several challenges. Ambiguity in human intentions can make accurate recognition difficult, as a single action might have multiple interpretations depending on the context [30,36]. Additionally, understanding intentions requires a thorough grasp of the surrounding context, which can be complex in dynamic or unfamiliar environments such as DF and Cybersecurity [30].

Since DF investigation is a highly sensitive task that requires meticulous attention to detail and a cautious approach, the application of intention recognition in this domain necessitates a deep understanding of the context as well as precise specification of the requirements. To effectively define and clarify these requirements, the use of formal methods presents an ideal solution, offering rigorous, structured approach to ensure accuracy and reliability in requirement specification process [37,38].

2.3. Formal Modeling

Modeling by utilizing formal methods is an approach in computer science and systems engineering that involves using mathematical techniques to create precise and unambiguous models of systems [37,39]. This method focuses on defining and analyzing system behavior through formal specifications and mathematical proofs, ensuring that systems are both reliable and efficient. Formal methods provide a rigorous framework for describing system properties and behaviors, which can be crucial for verifying correctness and consistency, especially in complex or critical systems [37,38]. In practical applications, formal methods are widely used in fields such as software engineering, aerospace, and telecommunications. For example, in software engineering, formal methods help in verifying that software programs meet their specifications and are free from critical errors [38–40].

To achieve effective modeling with formal methods, several techniques are used. These include formal specification languages, which provide a precise way to describe system or model requirements and behaviors, and theorem proving, which involves using mathematical proofs to verify that a system adheres to its specifications. Model checking is another technique that systematically explores all

 doi:10.20944/preprints202502.0764.v1

possible states of a system to ensure that it meets desired properties. These methods help in rigorously analyzing and validating system models to ensure their correctness [41,42].

There are various tools employed by formal methods to define and specify concepts, such as Temporal Logic, Z Notation, and Predicate Logic. In this work, we utilize Predicate Logic, a formal framework commonly used in mathematics, philosophy, and computer science to express statements and reason about relationships between objects. Predicate logic extends propositional logic by incorporating quantifiers and predicates, enabling more expressive statements that involve variables. In this system, predicates are functions that return true or false based on the values of their arguments, while quantifiers such as "for all" ($\forall$) and "there exists" ($\exists$) allow for generalizations over sets of objects. Predicate Logic provides a rigorous foundation for modeling and verifying system properties, making it an essential tool across various fields [37].

Despite their advantages, formal methods come with challenges. One major issue is the complexity and resource intensity of applying these methods, particularly for large or highly complex systems. Developing formal specifications and proofs can be time-consuming and requires specialized knowledge [43,44].

2.4. Related Works

Intention recognition plays a crucial role in various domains of cybercrime, including Advanced Persistent Threats (APT), mobile security, artificial intelligence (AI) security, network security, physical security (including video surveillance), and social media. The literature on this topic reveals a diverse range of approaches and methodologies tailored to each specific area of concern. For clarity, we categorize the related works into four main groups: the first category encompasses general domains such as APT, mobile, and AI security; the second focuses on network security; the third addresses physical security and video surveillance; and the fourth covers social media. Each category involves distinct techniques and challenges, reflecting the unique requirements and complexities associated with recognizing malicious intentions across these varied fields.

Ahmed et al. [45] propose a method for recognizing cyberattack intentions through similarity analysis, distinguishing between general intentions (such as availability, confidentiality, and integrity) and specific intentions (like DDoS attacks). Their approach, using the fuzzy min-max (FMM) neural network model, enhances the ability to anticipate attacks by filtering out similar cases. Tested on a subset of the page block dataset, the method demonstrates high accuracy and efficiency. Kim et al. [46] develop an Android application that uses an attack tree approach to detect attack intentions, operating through two phases: a pre-phase and a post-phase, which includes log collection, analysis, visualization, and alerting. This system effectively identifies smishing and backdoor attacks. Cheng et al. [47] tackle the challenge of understanding Advanced Persistent Threats (APTs) in Internet of Things (IoT) systems by introducing APTALCM, a framework that uses a similarity-based approach and an ontology to model APT attack scenarios. This framework includes modules for correlating alerts and logs, and it achieves a low false positive rate of 4.2% and a high true positive rate of 83.7%. Pang et al. [48] introduce AdviMind, a model for early detection of query-based adversarial attacks on deep neural networks (DNNs). It features three variants, including the Naive Intent Estimator, which provides baseline intent detection but lacks robustness. AdviMind achieves over 75% accuracy in detecting attack intents after observing fewer than three query batches and increases the query cost of adaptive attacks by over 60%.

Several network-related studies have explored intent recognition in cybercrime. Mirsky et al. [49] develop two metric-based algorithms, Plan Edit Distance (PED) and APC, for goal recognition in network security. PED measures the distance between observed sequences and optimal plans without requiring online planning, demonstrating superior performance in prediction accuracy, noise resistance, and processing times compared to traditional planner-based methods. Meanwhile, Chen et al. [50] propose an attack graph-based approach for identifying attacker intentions in network security. Their method effectively uncovers complex, multi-step attack intentions across various network environments. Li et al. [12] propose a method for recognizing multi-step attacks using a

 doi:10.20944/preprints202502.0764.v1

hidden Markov model (HMM) with probabilistic reasoning and temporal relationships to capture interrelated attack phases. They develop three models—HMM, HMM with Probabilistic Inference (HMM-PI), and HMM-PI with an updated Conditional Probability Table (HMM-PI-UCM)—and find the HMM-PI-UCM model to be the most effective, based on experiments with the LLDOS1.0 dataset.

Zhang et al. [32] introduce a technique for recognizing attack intentions by modeling attack-defense interactions as a strategic game and solving for game equilibria to compute attack probabilities. Validated through NetLogo simulations, their approach significantly enhances the accuracy of attack intention recognition. Shinde et al. [31] present a model based on the Interactive Partially Observable Markov Decision Process (I-POMDP) for identifying cyberattack intentions in a honeypot environment. This model shows improved accuracy and robustness in detecting attacker actions and intentions compared to traditional methods. Zhao et al. [51] propose HinAp, a framework that leverages heterogeneous attention networks and transductive learning to analyze intruder attack preferences. By integrating semantic information from meta-paths and meta-graphs, their model outperforms six other competing models. Kang et al. [52] introduce ActDetector, a framework designed to automatically detect attack activities from raw Network Intrusion Detection System (NIDS) alerts, thus reducing the workload for security analysts. ActDetector comprises an extractor, an embedder, and a classifier, and is evaluated using three datasets. It achieves an average of 94.8% precision, 95.0% recall, and 94.6% F1-score.

Some studies focus on advancements in physical security and video surveillance. Hsu et al. [53] developed a comprehensive method that integrates access control, surveillance, and host defense systems to detect malicious activity in physical environments. Their approach aggregates threat scores from these systems to generate effective alerts for identifying potential threats. Tang et al. [54] introduced a method for detecting attack intentions in power systems using Graph Convolutional Networks (GCNs). Their model, known as Attack Intention Detection for Power Systems Using Graph Convolutional Networks (AIGCN), operates in two main stages and achieves high precision rates of 97.34% and 98.25% on two datasets, significantly outperforming baseline methods and demonstrating its effectiveness and robustness.

Navalgund et al. [13] developed a real-time deep learning system for detecting criminal intentions from CCTV footage. Their system enhances crime prevention by integrating Faster R-CNN to identify weapons such as guns and knives and includes a text alert feature to notify authorities of potential threats. Martinez-Mascorro et al. [55] introduced a deep learning model utilizing 3D Convolutional Neural Networks (3D CNNs) for spatio-temporal analysis to identify shoplifting intentions from surveillance videos. Their model achieves a 75% accuracy rate, proving effective in the early detection of criminal intent. Bhugul et al. [34] developed a deep learning model designed for real-time detection of suspicious activities in private settings, such as bank robberies. Their system, which has been tested across various hardware platforms, detects firearms with an impressive 99.3% accuracy, surpassing existing methods like YOLO v3, v4, v5, and SVM.

On the other hand, several studies have concentrated on social media. Mendonça et al. [56] tackle the challenge of detecting criminal intentions in social media texts that are encoded with slang. They developed a framework that classifies such texts effectively. Tested on a dataset of 8.8 million tweets, their framework successfully identifies criminal intentions, contributing to cybercrime prevention by analyzing Portuguese social media slang. Abarna et al. [14] introduced an algorithm for detecting cyberharassment and intent in Instagram comments. By employing natural language processing (NLP) and a fast text model to analyze lexical meaning and word order, their algorithm demonstrates superior performance in precision, recall, and F1 score compared to existing methods, offering improved accuracy and lower error rates in detecting cyberharassment and its intent on social media platforms. Bokolo et al. [33] assessed five machine learning algorithms—logistic regression, ridge regression, SVM, Stochastic Gradient Descent (SGD), and random forests—for intent recognition on Twitter. Their analysis revealed that logistic regression achieved the highest accuracy at 92.87%,

 doi:10.20944/preprints202502.0764.v1

surpassing SVM (92.56%), random forests (92.39%), ridge regression (90.88%), and SGD (89.51%), establishing it as the most effective method for intent detection in social media contexts.

Pandey et al. [57] proposed a distributional semantic approach for detecting malicious intent in Twitter conversations about sexual assault. By developing a typology for malicious intent and using a convolutional neural network (CNN), their model—tested on messages collected over four months—outperformed several baseline models in detecting such intents. Tsinganos et al. [58] presented CSE-PersistenceBERT, a transfer learning model designed to detect the persistence of chat-based social engineering (CSE) attacks that exploit users' psychological vulnerabilities. This model helps alert users and administrators to potential threats. Additionally, Tsinganos et al. [35] proposed another deep learning model using dialogue state tracking to recognize CSE attack intentions. By creating an ontology and a dataset named SG-CSE, and adapting BERT-base into SG-CSE BERT, their approach shows promising results in detecting these attacks.

The literature on intention recognition can be categorized into three main approaches: logic-based, classical machine learning-based, and deep learning-based methodologies. These approaches span various application areas, including network security, Internet of Things (IoT) systems, Advanced Persistent Threats (APT), social media, visual surveillance, and AI security [30]. While much of the existing work focuses on enhancing technical aspects of cybersecurity and detecting social engineering attacks in social media contexts, there is a notable absence of research addressing criminal intent recognition from a legal perspective. This gap in the literature highlights the need for integrating legal frameworks with intention recognition systems, which is the primary focus of our research.

The growing application of intention recognition to identify various types of criminal activities marks a significant and encouraging trend in research. This progression not only demonstrates the potential of IR in crime analysis but also provides valuable guidance for extending its application to a wider range of crime types. By leveraging this concept, researchers and practitioners can explore new avenues to predict and analyze intentions associated with different forms of crime, contributing to improved prevention and enforcement strategies.

Additionally, the integration of diverse technologies—ranging from traditional machine learning and logic-based systems to advanced deep learning techniques and ontologies—highlights the adaptability and innovation in this area. This diversity not only enriches the research landscape but also offers extensive opportunities for developing our own model. By drawing from these various technological approaches, we can design a system that is robust, efficient, and tailored to the complexities of intention recognition.

However, a noticeable limitation in existing studies is their predominant focus on the technical aspects of IR. While technical precision is undoubtedly critical, most works lack a holistic perspective that considers the broader implications and contexts of intention, particularly in the legal domain. Our approach aims to bridge this gap by adopting a more holistic model that integrates IR within its broader legal sense. This enables us to address the multifaceted nature of intention, ensuring that our model aligns with legal principles and contributes meaningfully to both academic research and practical applications.

3. Method

The model development methodology is structured into three phases. In the concept development phase, the approach integrates essential concepts from law, computer science, and mathematics to establish a robust foundation for the model. The design phase follows, concentrating on the structuring of the model by defining its components and the interrelationships between them. Finally, in the testing phase, the model is tested using various scenarios to evaluate its practical applicability.

3.1. Concept Development

In the concept development phase, the approach involves integrating key concepts from law, computer science, and mathematics to establish a comprehensive foundation for the model. This entails integrating legal definitions of crime and intent with computational methods and mathematical rigor

 doi:10.20944/preprints202502.0764.v1

to create a unified model. The goal is to formally define critical concepts related to crime and intent using mathematical and logical formulations. This step ensures that the foundational theories and terminology are well-aligned and clearly articulated, providing a robust basis for further development of the model.

3.2. Designing the Model

The design phase focuses on structuring the model by defining its components and the relationships among them. This includes identifying and specifying the various elements that make up the model, such as suspects, crimes, evidence, and intentions, and determining how these components interact. This phase is crucial for defining theoretical concepts and the overall IR based DF model using formal method which can be understood by computers as well as it will be easy to simulate the model by using scenarios.

3.3. Testing the Model

In the final step, the model is simulated with different cases or scenarios to assess its practical applicability. This step helps identify any discrepancies or limitations in the model, allowing for adjustments and refinements to enhance its robustness and ensure it effectively meets the requirements of real-world applications.

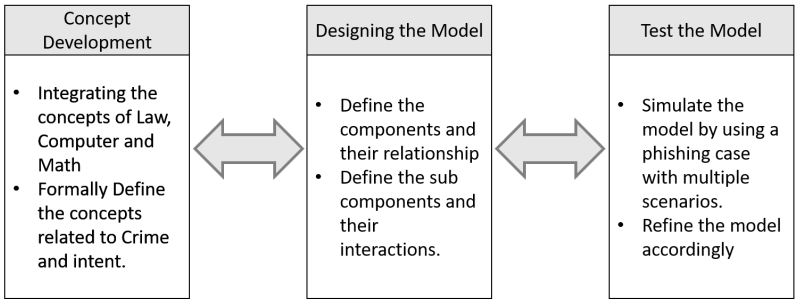


Figure 1. Model Development Approach.

4. Formal Definitions

This section takes the commonly accepted definitions of key concepts and transforms them into formal definitions that computers can process, using formal methods, specifically predicate logic. It provides formal representations for the terms "Crime," "Intent," each type of Intent, and "Intent Recognition," ensuring that these concepts are clearly defined in a way that can be understood and manipulated by computational systems.

4.1. Crime

Definition 4.1. *Crime is an action or omission that constitutes an offense and is punishable by law. [59–63]*

Definition 1: Crime is an action or omission that constitutes an offense and is punishable by law. [59–63]

This definition encompasses three essential elements: first, it identifies the specific action or omission attributed to the suspect; second, it recognizes that such actions or omissions are legally classified as offenses against individuals or society; and third, it stipulates that the offense is punishable under the law, commensurate with the degree of culpability. Thus, the concept of crime hinges on the simultaneous fulfillment of these three conditions.

Let

Sets:

- Let $\mathcal{C}$ = Set of all crimes.
- Set $\mathcal{A}$ = Set of all possible actions and inactions.
- Set $\mathcal{O}$ = Set of all offenses.

 doi:10.20944/preprints202502.0764.v1

- Set $\mathcal{P}$ = Set of all punishments.

Predicates:

- Constitutes(a, o): Specifies that Action (or Inaction) a constitutes an Offense o. This can be expressed as (1)

$$\exists o \in \mathcal{O} \mid \text{Action}(a) \wedge \text{Constitutes}(a, o) \tag{1}$$

- Punishable(o, p): Indicates that offense o is punishable by law with punishment p. This can be expressed as (2)

$$\exists p \in \mathcal{P} \mid \text{Offense}(o) \wedge \text{Punishable}(o, p) \tag{2}$$

- Crime: The definition of crime can be expressed as (3)

$$\forall c \text{Crime}(c) \Leftrightarrow \text{Action}(a) \wedge \text{Offense}(o) \wedge \text{Constitutes}(c, a) \wedge \text{Constitutes}(a, o) \wedge \text{Punishable}(o, p) \tag{3}$$

A crime constitutes of entity a that is either an action or omission, which in turn constitutes an offense o, and the offense is punishable by law with punishment p.

4.2. Criminal intent

Criminal intent, also termed mens rea, denotes the specific mental state or mindset that is legally requisite to substantiate a conviction for a criminal offense [15]. It encapsulates the defendant's state of mind at the time of committing the alleged criminal act, and it is crucial in determining culpability [15,64,65].

Criminal intent is a fundamental element that serves to differentiate between varying degrees of criminal responsibility based on the defendant's psychological disposition towards their conduct and its potential consequences [15,66,67].

To establish criminal intent, the prosecution must demonstrate that the defendant possessed a requisite level of mental awareness or purposefulness regarding their actions and the outcomes thereof. This mental state can vary across different crimes depending on the nature of the offense and the legal standards applicable [15,66]. According to the Modal Penal Code, criminal intent can be categorized as Purposely, Knowingly, Recklessly and Ignorantly [15]. the following are the formal definitions of Intent and Intent Types:

Definition 4.2. *A suspect has **Criminal Intent** when the evidence shows that the suspect commits a crime and the criminal action (or inaction) matches the elements required for the specific level of intent defined by the law [15]. Formally, continuing from the above:*

Let

- E: Set of all evidence,
- $I = \{I_p, I_k, I_r, I_i\}$: A finite set specifying the four levels of intention or mens rea, where:
  - I_p represents Purposely: Acting with the intention to achieve a specific result.
  - I_k represents Knowingly: Acting with awareness that a result is practically certain to follow.

 doi:10.20944/preprints202502.0764.v1

  - I_r represents Recklessly: Acting with disregard for a substantial and unjustifiable risk.
  - I_i represents Ignorantly: Acting without knowledge of the nature of the act or its consequences.
- S: Set of all suspects involved in the criminal activities.
- Commits(s, c, e): Specifies that the evidence e shows that the suspect s has committed the crime c.

  This can be expressed as (4)

$$\exists e \in E \mid \text{Suspect}(s) \land \text{Crime}(c) \land \text{Commits}(s, c, e) \tag{4}$$

- IsAdequate(e, l, i): Specifies that the evidence e adequately satisfies the expected elements by the law l for the intent level i. This can be expressed as (5)

$$\exists e \in E \mid \text{LawElements}(l) \land \text{IntentLevel}(i) \land \text{IsAdequate}(e, l, i) \tag{5}$$

- CriminalIntent(s, c, i): defines whether a suspect s has the criminal intent elements necessary for a crime c with intention i. For criminal intent to be established, the suspect must both commit the crime c and have the specific intention level i. Thus, criminal intent is true if and only if the evidence shows that the suspect has committed the crime and adequately satisfies the expected elements of the intention level i according to the law. This can be expressed as (6)

$$\begin{aligned} \forall s, c, i \ \text{CriminalIntent}(s, c, i) \Leftrightarrow \text{Suspect}(s) \land \text{Crime}(i) \land \\ \text{Intent}(i) \land \exists e, l \ \text{Evidence}(e) \land \text{LawElements}(l) \land \\ \text{Commits}(s, c, e) \land \text{IsAdequate}(e, l, i) \end{aligned} \tag{6}$$

- Alternatively:

$$\begin{aligned} \forall s, c, i \ \text{CriminalIntent}(s, c, i, l) \Leftrightarrow \text{Suspect}(s) \land \text{Crime}(i) \land \\ \text{Intent}(i) \land \text{LawElement}(l) \land \exists e \ \text{Evidence}(e) \\ \land \text{Commits}(s, c, e) \land \text{IsAdequate}(e, l, i) \end{aligned} \tag{7}$$

  This definition (7) is equivalent to the above definition, however, it gives us the flexibility to reuse it in defining each type of intent based on the relation to the required intent elements by the law.

4.3. Intent Types

The four types of intents can be formally defined as follows, continuing from above:

- Z: Set of all Outcomes.

1. Purposeful Intent:

 doi:10.20944/preprints202502.0764.v1

Definition 4.3. *A suspect exhibits purposeful intent if there exists a clear and deliberate goal to commit the crime, and their actions are aimed at achieving this goal [15].*

AimFor(s, z): Specifies that the suspect s aims for the outcome z. This can be expressed as (8)

$$\exists z \in Z \mid \text{Suspect}(s) \wedge \text{AimsFor}(s, z) \tag{8}$$

Purposely(s, c) : Specifies that the suspect s has purposefully aim for the outcome of Crime c. This can be expressed as (9)

$$\forall s, c \ \text{Purposely}(s, c) \Leftrightarrow \exists z \in Z \mid \text{CriminalIntent}(s, c, I_p, \text{AimsFor}(s, z)) \tag{9}$$

There must be specific goals or plans (e.g., to cause harm) and the suspect's actions must be supported by evidence that shows these actions are aimed at achieving these goals.

2. Knowing Intent:

Definition 4.4. *A suspect exhibits knowing intent if they are aware that their actions will likely contribute to the crime, even if they do not have the direct goal to commit the crime [15].*

AwareOf(s, z): Specifies that the suspect s is aware of the outcome z. This can be expressed as (10)

$$\exists z \in Z \mid \text{Suspect}(s) \wedge \text{AwareOf}(s, z) \tag{10}$$

Knowingly(s, c) : Specifies that suspect s is aware that their actions will almost certainly result in a specific outcome when committing crime c. This can be expressed as (11)

$$\forall s, c \ \text{Knowingly}(s, c) \Leftrightarrow \exists z \in Z \mid \text{CriminalIntent}(s, c, I_p, \text{AwareOf}(s, z)) \tag{11}$$

Evidence must show that the suspect was aware or should have been aware of the potential consequences of their actions, even if they did not intend to commit the crime.

3. Reckless Intent

Definition 4.5. *A suspect exhibits reckless intent if they consciously disregard a substantial risk that their actions will result in a crime [15].*

DisregardRisk(s, z): Specifies that the suspect s disregards a substantial risk of the outcome z. This can be expressed as (12)

$$\exists z \in Z \mid \text{Suspect}(s) \wedge \text{DisregardRisk}(s, z) \tag{12}$$

 doi:10.20944/preprints202502.0764.v1

Recklessly(s, c) : denotes that suspect s disregards a substantial and unjustifiable risk of causing a specific outcome when committing crime c. This can be expressed as (13)

$$\forall s, c \ \text{Recklessly}(s, c) \Leftrightarrow \exists z \in Z \mid \text{CriminalIntent}(s, c, I_p, \text{DisregardRisk}(s, z)) \quad (13)$$

There must be evidence that the suspect was aware of significant risks associated with their actions and acted despite these risks.

4. Ignorant Intent

Definition 4.6. *A suspect exhibits ignorant intent if they are unaware of the harmful nature of their actions and do not know that their actions could contribute to a crime [15].*

UnawareOf(s, z): Specifies that the suspect s is unaware of the outcome z. This can be expressed as (14)

$$\exists z \in Z \mid \text{Suspect}(s) \wedge \text{UnawareOf}(s, z) \quad (14)$$

Ignorantly(s, c) : denotes that suspect s is unaware of the nature of their actions or the possible consequences when committing crime c. This can be expressed as (15)

$$\forall s, c \ \text{Ignorantly}(s, c) \Leftrightarrow \exists z \in Z \mid \text{CriminalIntent}(s, c, I_p, \text{UnawareOf}(s, z)) \quad (15)$$

Evidence must show that the suspect was genuinely unaware of the harmful nature or potential criminal outcome of their actions.

One of the basic properties of these intent types is they are mutually exclusive that a suspect cannot be convicted of a crime in more than one intent level [15]. This property can formally be captured as (16)

$$\forall i \neq j \ (\neg(I_i \wedge I_j)) \quad (16)$$

specifying for all pairs of intents sequenced by i and j (where $i \neq j$), the intent levels I_i and I_j cannot both be true simultaneously. This is because the intents are somehow hierarchical in the sense that to prove a suspect is convinced of a crime at some higher level of intent (like purposely intent), the prosecutor needs more additional evidence than lower level intent (like knowingly intent).

5. The IR based Model

The IR based model is designed to enhance investigations by combining evidence processing and criminal intent recognition. As shown below, Figure 2, it comprises three main components: Evidence Analysis, Intention Recognition, and Crime Knowledge Base (CKB). The Evidence Analysis component filters and examines relevant evidence to support the investigation, transforming it into *action* formats. Intention Recognition analyzes this evidence to determine the suspect's level of intent, categorizing it as Purposely, Knowingly, Recklessly, Ignorantly, or None. Additionally, this component features a

 doi:10.20944/preprints202502.0764.v1

recommendation capability, which provides actionable suggestions for enhancing investigations by indicating the additional evidence needed or refining investigative approaches based on the analysis. The CKB serves as a critical reference, storing legal definitions, crime intent elements, crime intent patterns, and relevant data to guide the entire process. This integrated approach aids in assessing digital crime and optimizing investigation strategies.

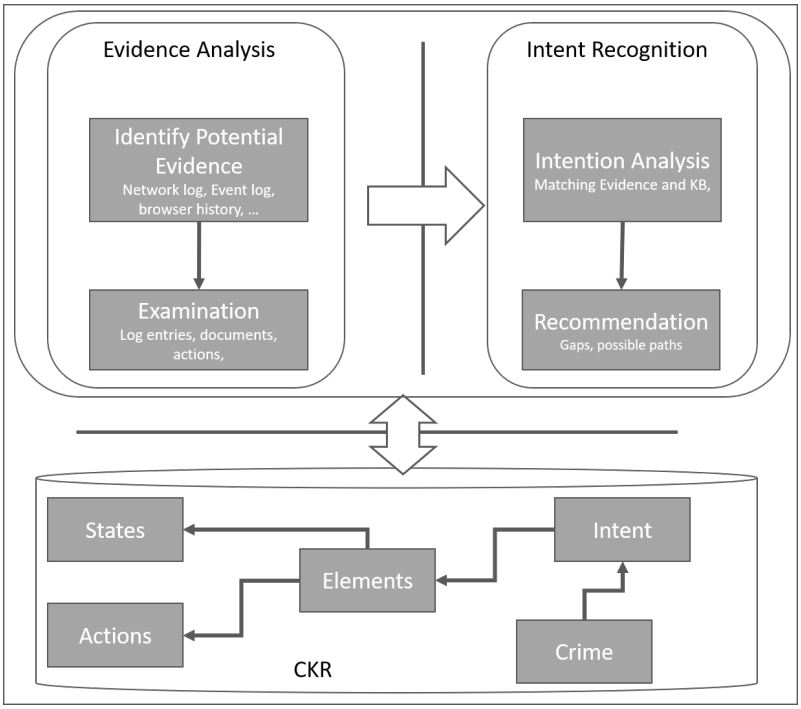


Figure 2. The Criminal Intention Recognition high-level model.

5.1. Evidence Analysis

The Evidence Analysis component is central to filtering and examining the digital evidence to ensure only the relevant data is processed in subsequent stages of the investigation. The component is divided into two sub-components: Identification of Potential Evidence and Examination of Evidence.

5.1.1. Identification of Potential Evidence

The task of this sub-component is to filter and select potential evidence related to a specific crime, considering the details of the criminal act. This involves pulling the list of relevant elements of the crime from the CKB and matching them against the overall digital evidence collected in relation to the suspect. The tasks of this sub component is highly related to the identification phase of the DF investigation phases [19]

For instance, to convict a suspect in a phishing attack, the court would generally require certain minimum elements to be fulfilled, although the specific requirements may depend on the legal system and the nature of the case. The minimum elements typically necessary to conclude the suspect is guilty at the level of "Purposely" intent are: Connection to the Suspect, Plan to Deceive, Transmission of Fraudulent Communications, and Loss (or Victim's Response). The details of these are discussed in the Scenario section

These four elements with the possible actions and state changes will be extracted from the CKB and this sub-component filters the evidence collected accordingly to identify the Potential Evidence.

 doi:10.20944/preprints202502.0764.v1

- Related(e,c,k): specifies that the evidence e is related to the crime c according to the crime knowledge repository k. This can be expressed as (17)

$$\exists e \quad \in \quad E \mid \text{Evidence}(e) \ \wedge \ \text{Crime}(c) \ \wedge \ \text{CKB}(k) \ \wedge \ \text{Related}(e, c, k) \quad (17)$$

- PotentialEvidence(p,c): denotes the set of potential evidence p, that is the subset of the overall evidence, which is filted by applying the crime knowledge base related to the crime c. This can be expressed as (18)

$$\forall p, c \ \text{PotentialEvididence}(p, c) \Leftrightarrow \exists e, k \mid \text{Evidence}(e) \wedge$$
$$p \in e \wedge \ \text{Crime}(c) \wedge \ \text{CKB}(k) \wedge \ \text{Related}(p, c, k) \quad (18)$$

5.1.2. Examiniation of Evidence

This sub-component's task is to thoroughly examine the filtered potential evidence and assess its relevance for supporting the case. The goal is to examine the potential evidence to identify the relevant entries from logs, histories, files or any other potential evidence categories and to convert these raw evidence into a common format that can be processed by the Intention Recognition component. The evidence is analyzed for actions and states indicative of the suspect's behavior. The tasks of this sub component are similar to the Examination phase of the DF invetigation [19]

- RelatedEntry(q, p, c, k): specifies that the entry q is recorded in the potential evidence p and it is related to crime c according to the knowledge base k. This can be expressed by (19)

$$\exists q \quad \in \quad Q, c, k \mid \text{PotentialEvididence}(p, c) \ \wedge \ \text{RelatedEntry}(q, p, c, k) \quad (19)$$

- Relevant(r): specifies that the evidence r is a relevant entry in the potential evidence for the crime c according to the crime knowledge repository k. This can be expressed by (20)

$$\forall r \ \text{Relevant}(r) \Leftrightarrow \exists r, p, c, k \mid \text{Crime}(c) \wedge$$
$$\text{CKB}(k) \wedge \ \text{RelatedEntry}(r, p, c, k) \quad (20)$$

5.2. Intent Recognition

The Intention Recognition component processes the evidence from the Evidence Analysis component and determines the suspect's criminal intention. This component consists of two sub-components: Intention Analysis and Recommendation.

5.2.1. Intention Analysis

The Intention Analysis sub-module is tasked with evaluating the suspect's involvement in various criminal activities based on the alignment of evidence with the knowledge base. This analysis involves assessing the extent of the suspect's engagement in multiple crimes, as well as determining the potential for the suspect to face charges reflecting a higher degree of intent within a single crime.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 February 2025 doi:10.20944/preprints202502.0764.v1

The sub-module systematically calculates the likelihood of different levels of criminal intent, thereby providing a nuanced understanding of the suspect's criminal engagement. To do so the component utilizes the output of the the Evidence Analysis component to contract the crime scene. The tasks of this component is highly related to the analysis phase of the DF investigation, however this component follows the intention recognition perspective [19].

- Match(r, k, c, i): specifies that each elements of the crime c at the intention level of i which are found in the Crime Knowledge Base k has a match in the relevant evidence r. This can be expressed by (21)

$$\exists r, k, c, i \mid \text{Relevant}(r) \wedge \text{CKB}(k) \wedge \text{Crime}(c) \wedge \text{Intention}(i) \wedge \text{Match}(r, k, c, i) \quad (21)$$

- Culpable(s,c,i,r,k): specifies that the Suspect s is culpable of the Crime c at an intention level of i, given the match of the Relevant evidence r and the CKB k. This can be expressed by (22)

$$\forall s, c, i \, \text{Culpable}(s, c, i, r, k) \Leftrightarrow \exists r, k \mid \text{Crime}(c) \wedge \text{Suspect}(s) \wedge \text{Intention}(i) \wedge \text{Relevant}(r) \wedge \text{CKB}(k) \wedge \text{Match}(r, k, c, i) \quad (22)$$

5.2.2. Recommendation

The Recommendation sub-module is responsible for guiding the investigation process by proposing optimal strategies based on the suspect's level of involvement. It evaluates the likelihood of uncovering additional evidence and suggests investigative pathways that align with the suspect's degree of engagement in the crime. This sub-module ensures that the investigative approach is both targeted and efficient, facilitating a thorough examination of the evidence and supporting the formulation of appropriate charges. The tasks of this sub component are mainly related to the reporting phase of the DF investigation, and this component emphasizes on the recommendations [19].

- NeededEvidence(d): specifies that from the elements of the crime c at the intention level of i which are found in the Crime Knowledge Base k, there are some elements d which are missing in the relevant evidence r. This can be expressed by (23)

$$\exists d \mid \text{Relevant}(r) \wedge \text{CKB}(d) \wedge \text{Crime}(c) \wedge \text{Intention}(i) \wedge \neg \text{Match}(r, d, c, i) \quad (23)$$

 doi:10.20944/preprints202502.0764.v1

- RelatedToOtherCrime(r): specifies that the Relevant evidence r is also related to other Crime c′ according to the CKB k. This can be expressed by (24)

$$\forall r, c' \ \text{RelatedToOtherCrime}(r, c') \Leftrightarrow \exists r \mid \text{Relevant}(r) \wedge \text{CKB}(k) \wedge \text{Crime}(c') \wedge \text{Related}(r, c', k) \quad (24)$$

5.3. Crime Knowledge Repository

The Knowledge Repository is a critical component that supports both the Evidence Analysis and Intention Recognition processes. It contains a comprehensive database of legal frameworks, crime definitions, instigator experiences, and digital forensics best practices, enabling effective analysis and interpretation of evidence. It provides the necessary information to identify and categorize evidence, as well as assist in determining the appropriate criminal intention level.

6. Scenario

To clarify how the model works, let us consider the following four scenarios of a single crime case, phising via email [68]. All the four levels of intention are mapped one-to-one to the scenarios. We try to capture the main phases of the model, the interaction among the components and the high-level data exchange during the processes.

1. Purposely
   - Context: An attacker (S1) designs a phishing email with a malicious link, aiming specifically at the company. The email is crafted to closely resemble legitimate communications from the company's trusted partners.
   - Specific Situation: The attacker sends the email to the finance officer, intending for it to be clicked and to initiate a DDoS attack on the company.
   - Action Taken: The attacker's goal is clear: to cause disruption or harm to the company's operations by tricking the finance officer into clicking the malicious link.
   - Categorization: The attacker's intent is categorized as "purposely" because the malicious email was sent with the specific objective of causing harm.

   For this level of culpability, the following crime elements are considered minimal requirements.
   - Connection to the Suspect: The court needs to establish that the suspect was indeed involved in the phishing attack. This can be done by showing evidence such as Network logs, email metadata, or records and transactions linking the suspect to the phishing activity [69,70]. (The necessary evidence are: Network logs, Email logs, Browser History)
   - Plan to Deceive: The court would need evidence showing that the suspect intentionally crafted a fraudulent communication to manipulate the victim into disclosing personal or financial information. This can be shown from the evidence by disclosing the phishing tools and techniques the attacker employed [68,69]. (The necessary evidence are: Network logs, Event logs, System Logs, Browser History, System files)
   - Transmission of Fraudulent Communications: The court would need proof that the suspect was responsible for sending the phishing communication—whether by email, phone, or other means. This can be shown through evidence such as email headers, phone logs, or IP address tracing [68,69]. (The necessary evidence are: Network log, email log, email content, phone log)
   - Loss (or Victim's Response): To prove that a phishing attack took place, it is generally necessary to show that the victim was deceived and suffered some form of harm, such as revealing sensitive information or losing money. Evidence such as victim testimony, transaction records, or documentation of identity theft can be used in establishing that

 doi:10.20944/preprints202502.0764.v1

the phishing attempt had a tangible impact [68,69]. (The necessary evidence are: Bank Transaction, Account History, reputation assessment, customer statistics)

The model will run the case as follows:

- Identification of Potential Evidence:
  - Input: The overall evidence collected in relation to the Suspect, S1.
  - Process: The sub component will filter the overall evidence by considering the evidence list for the specific crime, Phishing via email, from the Crime Knowledge Base.
  - Output: List of potential evidence extracted from the whole evidence. (Network log, Event log, Email log, Browser History, system files, Email Content, Phone log, Bank Transaction, Account History, Reputation Assessment, Customer statistics)
- Examination of Evidence:
  - Input: Potential evidence identified which is the output of previous (Identification of Potential Evidence) sub component.
  - Process: The sub component go through each potential evidence and identify the relevant entries in relation to the Suspect S1 and the phishing crime. Besides this sub component convert the entries to a common format used by the CKB using action and state template.
  - Output: List of Relevant entries in the form of actions and state documentation.
- Intention Analysis:
  - Input: List of Relevant entries in action and state format which is the output of the previous (Examination of Evidence) sub component.
  - Process: The sub component analyses the relevant entries with the expected evidence for the crime as documented in the CKB.
  - Output: The whole analysis as well as the entries and the expected evidence.
- Recommendation:
  - Input: The analysis, the entries and the expected evidence which are the output of the previous (Intention Analysis) sub component.
  - Process: The sub component analyzes: considering the available evidence what should be the conviction level, what evidence are needed to support or clarify the case, what other criminal activities are related to the evidence.
  - Output: List of recommendations.

2. Ignorance
   - Context: The company receives a phishing email that closely mimics previous legitimate communications and creates a sense of urgency.
   - Specific Situation: The finance officer, recognizing the email as urgent and similar to past legitimate messages, forwards it to the cyber security officer for validation. After not receiving a prompt response and due to the urgency conveyed in the email, the finance officer decides to click the link.
   - Action Taken: The finance officer clicks the link, assuming the email is legitimate, and is unaware of its malicious nature.
   - Categorization: The finance officer's action is categorized as "ignorance" because they acted under the mistaken belief that the email was legitimate, lacking awareness of its malicious intent.
3. Recklessly
   - Context: A phishing email, designed to appear legitimate, is sent to the company and is forwarded by the finance officer to the cyber security officer for validation.

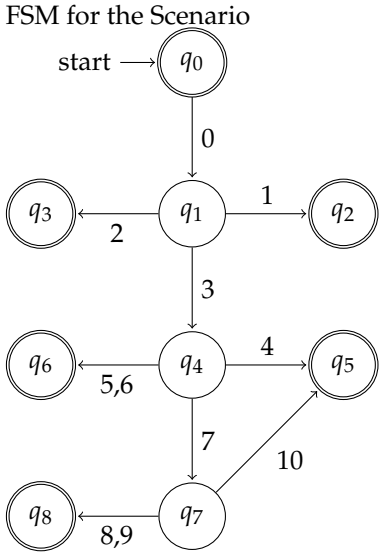
 doi:10.20944/preprints202502.0764.v1

- Specific Situation: The cyber security officer, overwhelmed by other urgent tasks, quickly responds to the finance officer's inquiry without thoroughly checking the link, indicating it is safe.
- Action Taken: The cyber security officer's hasty response, without proper verification of the link, demonstrates a disregard for the potential risks involved.
- Categorization: The cyber security officer's action is categorized as "recklessly" because they failed to exercise due diligence and responded in a manner that ignored the potential risks of the link.

4. Knowingly

- Context: A phishing email is received by the company, which closely resembles legitimate communications and contains a malicious link.
- Specific Situation: The finance officer forwards the email to the cyber security officer, requesting validation and indicating urgency. The cyber security officer, recognizing the link as malicious and knowing it could potentially lead to a DDoS attack, chooses not to respond to the finance officer's inquiry.
- Action Taken: The cyber security officer makes a deliberate decision to ignore the email, based on the belief that the company's security measures will mitigate any impact from the attack.
- Categorization: The cyber security officer's action is categorized as **knowingly** because they were aware of the threat and chose not to act, assuming the company's defenses would handle the risk.

FSM for the Scenario



Description:

1. States

- q_0: Attacker Sends Malicious Email and is guilty of "Purposefully" intent.
- q_1: Email Received by Finance Officer
- q_2: Finance officer is free from crime, (no criminal intent).
- q_3: Finance officer is guilty of "ignorantly" intent
- q_4: Finance Officer forwards the email to Cyber Security Officer for verification
- q_5: Cyber Security Officer is free from crime (no criminal intent).
- q_6: Cyber Security Officer is guilty of "recklessly" intent
- q_7: Email investigated by Cyber Security Officer
- q_8: Cyber Security Officer is guilty of "knowingly" intent

2. Transitions

 doi:10.20944/preprints202502.0764.v1

- 0: Attacker sends the email.
- 1: Finance officer ignores the email.
- 2: Finance officer clicks the malicious link inside the email, assuming it's legitimate.
- 3: Finance officer forwards the email to the Cyber Security Officer for validation.
- 4: Cyber Security Officer forbids the Finance Officer from clicking the malicious link.
- 5: Cyber Security Officer allows the Finance Officer to click the malicious link.
- 6: Cyber Security Officer ignores the email.
- 7: Cyber Security Officer analyzes the malicious link inside the email.
- 8: Cyber Security Officer allows the Finance Officer to click the malicious link, assuming the security measures are already in place to handle it.
- 9: Cyber Security Officer ignores the email, which is inaction despite knowing the threat.
- 10: Cyber Security Officer forbids the Finance Officer from clicking the malicious link.

7. Discussion

The evolution of forensic investigations heavily relies on sophisticated computational techniques to keep pace with the ever-expanding data landscape [6–8,71]. Without automated systems, the task of identifying pertinent information and piecing together a coherent narrative from the vast sea of digital artifacts would be insurmountable. The proposed model introduces a novel approach to addressing the challenge of managing vast volumes of digital evidence in forensics by focusing on intention recognition in a legal context. It systematically navigates through the evidence, identifying relevant information, reconstructing crime scenes, determining the nature of the crime, and assessing the suspect's intent. Operating autonomously around the clock with minimal human guidance, the model streamlines the forensic process and reduces the need for constant supervision. Additionally, it leverages both legal and technical expertise, as well as the experience of professionals, through a knowledge repository, CKB. This integration enhances the model's ability to provide valuable recommendations for the conviction process, including identifying additional evidence needed and suggesting further investigation into suspects' potential connections to other related crimes.

The model's design offers flexibility through its four autonomous sub-components, which are aligned with the NIST four-stage digital forensics framework. This alignment ensures that the model is easy to integrate into existing digital forensics practices, as it follows a well-established and widely recognized framework. Investigators can quickly adapt the model to their workflow, minimizing the learning curve and ensuring a smoother transition into its use. Furthermore, the autonomy of the sub-components enhances the model's versatility, as each component can be implemented using different technologies, making it adaptable to various digital forensics environments. This flexibility allows investigators to tailor the model to the specific tools, platforms, or software they currently utilize, ensuring compatibility with a wide range of technological setups.

The use of formal methods in developing the model brings several key benefits, starting with the accuracy and completeness of its specifications. As formal methods rely on mathematical expressions, it ensures that the model's definitions and specifications are precise and unambiguous. This rigorous approach contributes to a more correct and comprehensive representation of the processes involved in digital forensics. Additionally, by utilizing formal methods, the model allows for greater flexibility in the implementation of each of its four sub-components, as well as the orchestration among them. The mathematical foundation of the model facilitates a clear definition of how the components interact, providing a solid framework for their integration and operation in different environments. Beyond its specific application in digital forensics, the formal definitions presented here can be adapted and extended to other fields related to forensics. This makes the model not only a valuable tool for digital forensics but also a versatile framework that can contribute to the development of methods in other interdisciplinary areas.

To ensure the effectiveness and accuracy of the model, we employ scenarios that encompass all four intent types—Purposely, Knowingly, Recklessly, and Ignorantly. These scenarios are designed

 doi:10.20944/preprints202502.0764.v1

to simulate various criminal activities and provide a test of the model's capabilities. By applying the model to these scenarios, we assess its ability to correctly identify and differentiate between the different types of intent based on the evidence and context provided. It confirms that the model can accurately process and analyze complex data sets, effectively recognizing and categorizing the mental states of suspects as defined by legal standards.

While our proposed model demonstrates significant potential, it is not without its limitations. One key constraint is its heavy reliance on the knowledge base. The model's ability to perform effectively hinges on the accuracy, consistency, and comprehensiveness of the knowledge base. Any errors, inconsistencies, or inadequacies in the knowledge base can compromise the model's performance, leading to inaccurate or incomplete intention recognition. This reliance highlights the critical need for meticulous curation and maintenance of the knowledge base to ensure the model's reliability.

Another limitation lies in the scope of the model's applicability. While it has the flexibility to be extended to address other types of criminal activities, such as those involving strict liability, its current implementation is restricted to handling only the four types of intentions. This limited scope may reduce its immediate applicability to a broader range of legal contexts and criminal behaviors. Future iterations of the model would need to expand its capacity to address additional types of crimes and intentions to maximize its utility and effectiveness.

8. Conclusion and Future Work

In summary, our work addresses one of the pressing challenges faced by digital forensics investigators due to the overwhelming volume of evidence. By integrating concepts from law, computer science, and mathematics, we have developed a model that effectively navigates through vast amounts of digital data to identify relevant evidence, reconstruct crime scenes, and recognize suspect intent. The model's structure—comprising Evidence Analysis, Intent Recognition, and the Criminal Repository—ensures a comprehensive approach to forensic investigations, enhancing both accuracy and efficiency. Through the application of formal methods, we have rigorously defined key concepts such as crime and intent, ensuring that the model operates on a solid theoretical foundation. Simulating with scenarios has demonstrated the model's capability to accurately identify intent types and manage complex cases. Ultimately, our contributions bridge the gap between legal definitions and computational analysis, providing a valuable tool that addresses the volume challenge in digital forensics and significantly improves investigative effectiveness.

Looking ahead, we recommend implementing the model by incorporating AI utilizing its capabilities and effectiveness. Specifically, since the huge volume challenge better be solved with minimal human interaction, a self reliant AI model such as Agentic AI approach, that mimics agency, would be ideal [72,73]. This would enable the model to function as a self-reliant assistant, capable of autonomous action, decision-making, and goal pursuit. Ultimately, this would allow the model to provide well-informed recommendations for the investigation and conviction of the suspect.

Alternatively, implementing the model utilizing the hybrid approach that combines logic-based methodologies with explainable deep learning techniques could provide advantages. Integrating logic-based approaches ensures that the model retains its formal rigor and precise definitions, while the application of explainable deep learning can offer advanced pattern recognition and adaptive learning capabilities. This combination would enable the model to handle increasingly complex and dynamic data sets, improving its ability to identify subtle patterns and trends in evidence that may not be easily captured by traditional methods. Moreover, explainable AI can provide transparency in decision-making, allowing investigators to understand and trust the model's conclusions. By leveraging both these technologies, the model could evolve into a more robust and adaptive tool, further addressing the challenges of DF and supporting more nuanced and accurate investigative outcomes.

 doi:10.20944/preprints202502.0764.v1

References

1. Kuzior, A.; Tiutiunyk, I.; Zielińska, A.; Kelemen, R. Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies (2071-8330)* **2024**, *17*.
2. Sharma, V.; Manocha, T.; Garg, S.; Sharma, S.; Garg, A.; Sharma, R. Growth of Cyber-crimes in Society 4.0. In Proceedings of the 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), 2023, pp. 1–6. https://doi.org/10.1109/ICIPTM57143.2023.10118185.
3. Wall, D.S. *Cybercrime: The transformation of crime in the information age*; John Wiley & Sons, 2024.
4. Lusthaus, J. Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime? *Annual Review of Law and Social Science* **2024**, *20*, 369–385. https://doi.org/https://doi.org/10.1146/annurev-lawsocsci-041822-044042.
5. Biedron, S.R. Cybercrime in the Digital Age. Master's thesis, University of Oxford, 2024.
6. Fakhouri, H.N.; AlSharaiah, M.A.; Al hwaitat, A.k.; Alkalaileh, M.; Dweikat, F.F. Overview of Challenges Faced by Digital Forensic. In Proceedings of the 2024 2nd International Conference on Cyber Resilience (ICCR), 2024, pp. 1–8. https://doi.org/10.1109/ICCR61006.2024.10532850.
7. Alenezi, A.M. Digital forensics in the age of smart environments: A survey of recent advancements and challenges. *arXiv preprint arXiv:2305.09682* **2023**.
8. Dunsin, D.; Ghanem, M.C.; Ouazzane, K.; Vassilev, V. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation* **2024**, *48*, 301675. https://doi.org/https://doi.org/10.1016/j.fsidi.2023.301675.
9. Michelet, G.; Breitinger, F.; Horsman, G. Automation for digital forensics: Towards a definition for the community. *Forensic Science International* **2023**, *349*, 111769. https://doi.org/https://doi.org/10.1016/j.forsciint.2023.111769.
10. Quick, D.; Choo, K.K.R. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation* **2014**, *11*, 273–294. https://doi.org/10.1016/j.diin.2014.09.002.
11. Ahmed, A.A.; Ahlami, N.; Zaman, K. Attack Intention Recognition : A Review **2017**. *19*, 244–250. https://doi.org/10.6633/IJNS.201703.19(2).09.
12. Li, T.; Liu, Y.; Liu, Y.; Xiao, Y.; Nguyen, N.A. Attack plan recognition using hidden Markov and probabilistic inference. *Computers and Security* **2020**, *97*, 101974. https://doi.org/https://doi.org/10.1016/j.cose.2020.101974.
13. Navalgund, U.V.; K., P. Crime Intention Detection System Using Deep Learning. In Proceedings of the 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), dec 2018, pp. 1–6. https://doi.org/10.1109/ICCSDET.2018.8821168.
14. Abarna, S.; Sheeba, J.I.; Jayasrilakshmi, S.; Devaneyan, S.P. Identification of cyber harassment and intention of target users on social media platforms. *Engineering Applications of Artificial Intelligence* **2022**, *115*, 105283. https://doi.org/https://doi.org/10.1016/j.engappai.2022.105283.
15. Institute, A.L. *Model penal code : official draft and explanatory notes : complete text of model penal code as adopted at the 1962 annual meeting of the American Law Institute at Washington, D.C., May 24, 1962*; Philadelphia, Pa. : The Institute, 1985., 1985.
16. Jones, O.D.; Montague, R.; Yaffe, G. Detecting mens rea in the brain. *University of Pennsylvania Law Review* **2020**, *169*, 1–31.
17. Antill, G. Fitting the Model Penal Code into a ReasonsResponsiveness Picture of Culpability. *Yale Law Journal* **2022**, *131*, 1346–1384.
18. National, G.; Pillars, H. *Digital Forensics, Andre Arnes*; 2018; p. 373.
19. Kent, K.; Chevalier, S.; Grance, T.; Dang, H. Guide to Integrating Forensic Techniques into Incident Response. *The National Institute of Standards and Technology* **2006**.
20. Hassan, N.A. *Introduction: Understanding Digital Forensics*; 2019; pp. 1–33. https://doi.org/10.1007/978-1-4842-3838-7_1.
21. Holt, T.; Bossler, A.; Seigfried-Spellar, K. *Cybercrime and Digital Forensics*; Taylor and Francis, 2015. https://doi.org/10.4324/9781315777870.
22. Pandey, A.K.; Tripathi, A.K.; Kapil, G.; Singh, V.; Khan, M.W.; Agrawal, A.; Kumar, R.; Khan, R.A. Current Challenges of Digital Forensics in Cyber Security **2020**. pp. 31–46. https://doi.org/10.4018/978-1-7998-1558-7.ch003.

23. Montasari, R.; Hill, R.; Parkinson, S.; Peltola, P.; Hosseinian-Far, A.; Daneshkhah, A. Digital Forensics: Challenges and Opportunities for Future Studies. *International Journal of Organizational and Collective Intelligence* **2020**, *10*, 37–53. https://doi.org/10.4018/ijoci.2020040103.
24. Karie, N.M.; Venter, H.S. Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences* **2015**, *60*, 885–893. https://doi.org/10.1111/1556-4029.12809.
25. Sukthankar, G.; Geib, C.; Bui, H.H.; Pynadath, D.; Goldman, R.P. *Plan, activity, and intent recognition: Theory and practice*; Newnes, 2014.
26. Van-Horenbeke, F.A.; Peer, A. Activity, Plan, and Goal Recognition: A Review. *Frontiers in Robotics and AI* **2021**, *8*. https://doi.org/10.3389/frobt.2021.643010.
27. Han, T.A.; Pereira, L.M. State-of-the-art of intention recognition and its use in decision making. *AI Communications* **2013**, *26*, 237–246. https://doi.org/10.3233/AIC-130559.
28. Aarno, D.; Kragic, D. Motion intention recognition in robot assisted applications. *Robotics and Autonomous Systems* **2008**, *56*, 692–705. https://doi.org/https://doi.org/10.1016/j.robot.2007.11.005.
29. Qu, C.; Guo, Z.; Xia, S.; Zhu, L. Intention recognition of aerial target based on deep learning. *Evolutionary Intelligence* **2024**, *17*, 303–311. https://doi.org/10.1007/s12065-022-00728-9.
30. Kassa, Y.W.; James, J.I.; Belay, E.G. Cybercrime Intention Recognition: A Systematic Literature Review. *Information* **2024**, *15*. https://doi.org/10.3390/info15050263.
31. Shinde, A.; Doshi, P.; Setayeshfar, O. Cyber Attack Intent Recognition and Active Deception Using Factored Interactive POMDPs. In Proceedings of the Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems, Richland, SC, 2021; AAMAS '21, pp. 1200–1208.
32. Zhang, X.; Zhang, H.; Li, C.; Sun, P.; Liu, Z.; Wang, J. Network Attack Intention Recognition Based on Signaling Game Model and Netlogo Simulation. In Proceedings of the 2021 International Conference on Digital Society and Intelligent Systems (DSInS), 2021, pp. 162–166. https://doi.org/10.1109/DSInS54396.2021.9670583.
33. Bokolo, B.G.; Onyehanere, P.; Ogegbene-Ise, E.; Olufemi, I.; Tettey, J.N.A. Leveraging Machine Learning for Crime Intent Detection in Social Media Posts. In Proceedings of the AI-generated Content; Zhao, F.; Miao, D., Eds., Singapore, 2023; pp. 224–236.
34. Bhugul, A.M.; Gulhane, V.S. Novel Deep Neural Network for Suspicious Activity Detection and Classification. In Proceedings of the 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2023, pp. 1–7. https://doi.org/10.1109/SCEECS57921.2023.10063130.
35. Tsinganos, N.; Fouliras, P. Leveraging Dialogue State Tracking for Zero-Shot Chat-Based Social Engineering Attack Recognition **2023**.
36. Hamroun, M.; Gouider, M.S. A survey on intention analysis: successful approaches and open challenges. *Journal of Intelligent Information Systems* **2020**, *55*, 423–443. https://doi.org/10.1007/s10844-020-00604-x.
37. Bowen, J.P. Gerard O'Regan: Concise Guide to FormalMethods: Theory, Fundamentals and IndustryApplications. *Formal Aspects of Computing* **2020**, *32*, 147–148. https://doi.org/10.1007/s00165-020-00506-3.
38. Weyers, B.; Bowen, J.; Dix, A.; Editors, P.P. *Human–Computer Interaction Series The Handbook of Formal Methods in Human-Computer Interaction*; 2017.
39. ter Beek, M.H.; Chapman, R.; Cleaveland, R.; Garavel, H.; Gu, R.; ter Horst, I.; Keiren, J.J.A.; Lecomte, T.; Leuschel, M.; Rozier, K.Y.; et al. Formal Methods in Industry. *Form. Asp. Comput.* **2024**. https://doi.org/10.1145/3689374.
40. Larsen, K.; Legay, A.; Nolte, G.; Schlüter, M.; Stoelinga, M.; Steffen, B. Formal Methods Meet Machine Learning (F3ML). In Proceedings of the Leveraging Applications of Formal Methods, Verification and Validation. Adaptation and Learning; Margaria, T.; Steffen, B., Eds., Cham, 2022; pp. 393–405.
41. Seligman, E.; Schubert, T.; Kumar, M.V.A.K. *Formal verification: an essential toolkit for modern VLSI design*; Elsevier, 2023.
42. Woodcock, J.; Larsen, P.G.; Bicarregui, J.; Fitzgerald, J. Formal methods: Practice and experience. *ACM Comput. Surv.* **2009**, *41*. https://doi.org/10.1145/1592434.1592436.
43. Batra, M.; Malik, A.; Dave, M. Formal Methods: Benefits, Challenges and Future Direction. *Journal of Global Research in Computer Science* **2013**, *4*, 21–25.
44. Knight, J.C. Challenges in the utilization of formal methods. In Proceedings of the Formal Techniques in Real-Time and Fault-Tolerant Systems; Ravn, A.P.; Rischel, H., Eds., Berlin, Heidelberg, 1998; pp. 1–17.
45. Ahmed, A.A.; Mohammed, M.F. SAIRF: A similarity approach for attack intention recognition using fuzzy min-max neural network. *Journal of Computational Science* **2018**, *25*, 467–473. https://doi.org/https://doi.org/10.1016/j.jocs.2017.09.007.

46. Kim, D.; Shin, D.; Shin, D.; Kim, Y.H. Attack Detection Application with Attack Tree for Mobile System using Log Analysis. *Mobile Networks and Applications* **2019**, *24*, 184–192. https://doi.org/10.1007/s11036-018-1012-4.
47. Cheng, X.; Zhang, J.; Chen, B. Cyber Situation Comprehension for IoT Systems based on APT Alerts and Logs Correlation. *Sensors* **2019**, *19*. https://doi.org/10.3390/s19184045.
48. Pang, R.; Zhang, X.; Ji, S.; Luo, X.; Wang, T. AdvMind: Inferring Adversary Intent of Black-Box Attacks. In Proceedings of the Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, New York, NY, USA, 2020; KDD '20, pp. 1899–1907. https://doi.org/10.1145/3394486.3403241.
49. Mirsky, R.; Shalom, Y.; Majadly, A.; Gal, K.; Puzis, R.; Felner, A. New Goal Recognition Algorithms Using Attack Graphs. In Proceedings of the Cyber Security Cryptography and Machine Learning; Dolev, S.; Hendler, D.; Lodha, S.; Yung, M., Eds., Cham, 2019; pp. 260–278.
50. Chen, B.; Liu, Y.; Li, S.; Gao, X. Attack intent analysis method based on attack path graph. *ACM International Conference Proceeding Series* **2019**, pp. 97–102. https://doi.org/10.1145/3371676.3371680.
51. Zhao, J.; Liu, X.; Yan, Q.; Li, B.; Shao, M.; Peng, H.; Sun, L. Automatically predicting cyber attack preference with attributed heterogeneous attention networks and transductive learning. *Computers and Security* **2021**, *102*, 102152. https://doi.org/https://doi.org/10.1016/j.cose.2020.102152.
52. Kang, J.; Yang, H.; Zhang, Y.; Dai, Y.; Zhan, M.; Wang, W. ActDetector: A Sequence-based Framework for Network Attack Activity Detection. In Proceedings of the 2022 IEEE Symposium on Computers and Communications (ISCC), 2022, pp. 1–7. https://doi.org/10.1109/ISCC55528.2022.9912824.
53. Hsu, T.; Tang, C. Detection of Malicious Activities Using Machine Learning in Physical Environments. In Proceedings of the 2022 International Conference on Computational Science and Computational Intelligence (CSCI), Los Alamitos, CA, USA, dec 2022; pp. 1047–1052. https://doi.org/10.1109/CSCI58124.2022.00185.
54. Guang, K.; Guangming, T.; Xia, D.; Shuo, W.; Kun, W. A network security situation assessment method based on attack intention perception. In Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC), oct 2016, pp. 1138–1142. https://doi.org/10.1109/CompComm.2016.7924882.
55. Martínez-Mascorro, G.A.; Abreu-Pederzini, J.R.; Ortiz-Bayliss, J.C.; Garcia-Collantes, A.; Terashima-Marín, H. Criminal Intention Detection at Early Stages of Shoplifting Cases by Using 3D Convolutional Neural Networks. *Computation* **2021**, *9*. https://doi.org/10.3390/computation9020024.
56. de Mendonça, R.R.; de Brito, D.F.; de Franco Rosa, F.; dos Reis, J.C.; Bonacin, R. A framework for detecting intentions of criminal acts in social media: A case study on twitter. *Information (Switzerland)* **2020**, *11*, 1–40. https://doi.org/10.3390/info11030154.
57. Pandey, R.; Purohit, H.; Stabile, B.; Grant, A. Distributional Semantics Approach to Detect Intent in Twitter Conversations on Sexual Assaults. In Proceedings of the 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), 2018, pp. 270–277. https://doi.org/10.1109/WI.2018.00-80.
58. Tsinganos, N.; Fouliras, P.; Mavridis, I. Applying BERT for Early-Stage Recognition of Persistence in Chat-Based Social Engineering Attacks. *Applied Sciences* **2022**, *12*. https://doi.org/10.3390/app122312353.
59. Gill, A. What is Crime Mapping **2013**. *1*, 1–4.
60. Bell, S. crime, A Dictionary of Forensic Science, 2013. https://doi.org/10.1093/acref/9780199594009.013.0265.
61. Gooch, G.; Williams, M. crime, A Dictionary of Law Enforcement, 2015. https://doi.org/10.1093/acref/9780191758256.013.0805.
62. Dictionaries, O. crime, The Oxford Essential Dictionary of the U.S. Military, 2002. https://doi.org/10.1093/acref/9780199891580.013.2071.
63. Government of Ethiopia. Computer Crime Proclamation No.958/2016. *Negarit Gazeta* **2016**, p. 9104.
64. Gooch, G.; Williams, M. Intention, A Dictionary of Law Enforcement, 2015. https://doi.org/10.1093/acref/9780191758256.013.1671.
65. Law, J. intention, A Dictionary of Law (10 ed.), 2022. https://doi.org/10.1093/acref/9780192897497.013.2003.
66. Shahin, M. Criminal Intention and Motive in Criminal Law: A comparative approach. *Researchgate* **2021**. https://doi.org/10.13140/RG.2.2.21341.33766.
67. Coffey, G. Codifying the Meaning of 'Intention' in the Criminal Law. *Journal of Criminal Law* **2009**, *73*, 394–413. https://doi.org/10.1350/jcla.2009.73.5.590.
68. Rastenis, J.; Ramanauskaitė, S.; Janulevičius, J.; Čenys, A.; Slotkienė, A.; Pakrijauskas, K. E-mail-Based Phishing Attack Taxonomy. *Applied Sciences* **2020**, *10*. https://doi.org/10.3390/app10072363.

 doi:10.20944/preprints202502.0764.v1

69. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing Attacks : A Recent Comprehensive Study and a New Anatomy **2021**. *3*, 1–23. https://doi.org/10.3389/fcomp.2021.563060.
70. Leukfeldt, E.R. Cybercrime and social ties. *Trends in Organized Crime* **2014**, *17*, 231–249. https://doi.org/10.1007/s12117-014-9229-5.
71. *Knowledge and Information Edited by*.
72. Chawla, C.; Chatterjee, S.; Gadadinni, S.S.; Verma, P.; Banerjee, S. Agentic AI: The building blocks of sophisticated AI business applications. *Journal of AI, Robotics & Workplace Automation* **2024**, *3*, 1–15.
73. White, J. Building Living Software Systems with Generative and Agentic AI. *arXiv preprint arXiv:2408.01768* **2024**.