information

Article

Interoperability-Enhanced Knowledge Management in Law Enforcement: An Integrated Data-Driven Forensic Ontological Approach to Crime Scene Analysis

Alexandros Z. Spyropoulos [1,2,*], Charalampos Bratsas [3], Georgios C. Makris [4], Emmanouel Garoufallou [2] and Vassilis Tsiantos [1]

[1] Department of Physics, School of Science, Kavala's Campus, International Hellenic University (IHU), GR-57001 Thessaloniki, Greece; tsianto@physics.ihu.gr
[2] Department of Library Science, Archives and Information Systems, School of Social Sciences, Alexander's Campus, International Hellenic University (IHU), GR-57400 Thessaloniki, Greece; mgarou@ihu.gr
[3] Department of Information and Electronic Engineering, Alexander's Campus, International Hellenic University (IHU), GR-57400 Thessaloniki, Greece; cbratsas@iee.ihu.gr
[4] Inter-Faculty Master Program on Networks and Complexity, Aristotle University of Thessaloniki (AUTH), GR-54124 Thessaloniki, Greece; geomak@auth.gr
* Correspondence: daspyro@physics.ihu.gr

Abstract: Nowadays, more and more **sciences** are **involved** in strengthening the work of **law enforcement authorities**. Scientific documentation is evidence highly respected by the courts in administering justice. As the involvement of science in **solving crimes increases**, so does **human subjectivism**, which often leads to wrong conclusions and, consequently, to bad judgments. From the above arises the need to **create a single information system** that will be fed with **scientific evidence** such as fingerprints, genetic material, digital data, forensic photographs, information from the forensic report, etc., and also **investigative data** such as information from witnesses' statements, the apology of the accused, etc., from **various crime** scenes that will **be able**, through formal **reasoning procedure**, to conclude **possible perpetrators**. The present study examines a proposal for developing an information system that can be a basis for creating a **forensic ontology**—***a semantic representation of the crime scene***—through descriptive logic in the owl semantic language. The **Interoperability**-Enhanced information system to be developed could **assist law enforcement authorities** in **solving crimes**. At the same time, it would promote closer **cooperation** between **academia**, **civil society**, and **state institutions** by fostering a culture of engagement for the common good.

Keywords: knowledge management; law enforcement; interoperability; forensic ontology; crime scene analysis; semantic representation; criminal investigation; information systems; descriptive logic; digital forensics

check for updates

Citation: Spyropoulos, A.Z.; Bratsas, C.; Makris, G.C.; Garoufallou, E.; Tsiantos, V. Interoperability-Enhanced Knowledge Management in Law Enforcement: An Integrated Data-Driven Forensic Ontological Approach to Crime Scene Analysis. *Information* **2023**, *14*, 607. https://doi.org/10.3390/info14110607

Academic Editors: Mohamed Hedi Karray, Linda Elmhadhbi, Arkopaul Sarkar and Antonio De Nicola

Received: 29 September 2023
Revised: 31 October 2023
Accepted: 2 November 2023
Published: 9 November 2023

1. Introduction

The interplay between science and law enforcement has gained unprecedented attention in recent years. The infusion of scientific methodologies into investigative processes has not merely enhanced traditional methods but fundamentally transformed the landscape of crime-solving, elevating it from mere gut intuition to *evidence-based reasoning*. This approach is rooted in the scientific method, systematically employing data and empirical evidence to inform every phase of the investigation [1–3]. Advanced technologies such as DNA profiling, digital forensics, and computational simulations have not only increased the precision in evidence gathering but also expanded the definition and scope of what qualifies as "evidence" in judicial settings [4–7]. The ascendancy of this scientific, evidence-based reasoning carries considerable weight in judicial settings, often tipping the scales in favor of more conclusive, fact-based judgments. Such evidence is often subjected to rigorous standards of validation and reliability, adding a layer of objectivity to legal

proceedings that was previously unattainable through anecdotal or circumstantial evidence alone [8,9].

Yet, the fusion of science into the criminal justice system is not without its caveats. While science offers empirical methods and objective data, the human elements involved in its application introduce the potential for subjectivity and bias [1,7,9,10]. For instance, the interpretation of forensic results, the selective use of scientific tests, or even how data is collected and preserved can be influenced by human judgment. This human subjectivity, although often unintentional, can compromise the integrity of judicial decisions [2,4,5,7,10]. The risk is magnified when considering that scientific evidence is frequently viewed as incontrovertible [9]. Therefore, any lapse in objective application or interpretation of this evidence can have far-reaching implications, possibly leading to miscarriages of justice [3,6,7,11–13].

In light of these complexities, there is an escalating need for a robust framework that seamlessly integrates scientific evidence with *traditional investigative data*, which includes elements like police reports, eye-witness accounts, and physical evidence, while minimizing human subjectivity. The framework should be capable of synthesizing diverse types of data—from forensic reports and biological samples to witness testimonies and *digital footprints*—into a cohesive and interpretable format [3,5,8,9]. The key feature of our proposed model is its focus on "*interoperability-enhanced*" systems. This ensures seamless communication and data exchange between various services involved in criminal investigations such as law enforcement agencies, judicial bodies, forensic medical services, and criminology labs. By marrying advanced scientific methods with traditional data, we aim to create a comprehensive picture of the criminal scenario that is both nuanced and impartial. Against this backdrop, the present study aims to introduce an information system that employs *forensic ontology* and *data-driven approaches*—defined as the utilization of algorithmic to analyze and interpret data—to offer a more nuanced and impartial methodology for crime scene analysis [1–3,9,10].

The primary objective of this study is to present an interoperability-enhanced information system that integrates various types of scientific evidence and investigative data to aid in crime scene analysis [14–16]. This endeavor aims to resolve law enforcement agencies' multifaceted challenges in synthesizing large volumes of disparate data. By *centralized repository*, we mean a single, secure database where multiple forms of evidence and data can be stored and accessed conveniently. The envisioned system is designed to be such a centralized repository where information from biological samples like DNA and fingerprints to digital artifacts and eyewitness accounts can be cohesively stored and analyzed [17–20]. This amalgamation of varied data sources into a unified platform allows for a more comprehensive understanding of crime scenes, enhancing the quality of investigations and judicial proceedings [20–22]. The system's capability to correlate seemingly unrelated information through advanced algorithms can illuminate new investigative pathways, turning the centralized repository into not just a storage unit, but a dynamic tool for deeper crime analysis, enriching the context and narratives constructed around criminal events [16,17,20,23].

A secondary objective is to utilize *forensic ontology* as the backbone for organizing and interpreting this complex, multi-dimensional data [17–19,23]. In general terms, an ontology is a formal representation of knowledge within a specific domain, involving a set of terms and the relationships between them. Forensic ontology, specifically, is a set of structured terms, definitions, and relationships tailored to capture the complexities of the forensic domain. By adopting a structured semantic framework, the system will be able to not only store data, but also understand and interpret the relationships between different sets of information [17,23]. Forensic ontology acts as the scaffold for complex decision-making, enabling the system to sift through the intricacies of large-scale data. This is pivotal for enabling a formal reasoning process that can autonomously generate insights, identify patterns, and suggest likely hypotheses or conclusions based on the available evidence. Leveraging forensic ontology in this manner serves as a mechanism

for automated reasoning. In a realm where human subjectivity can significantly sway judgments, incorporating a machine-assisted reasoning process serves as a counterbalance, adding an additional layer of *impartiality and rigor*—defined as unbiased judgment and strict adherence to methodological standards—to the investigative process [14,15,18,23].

Lastly, the study aims to foster collaboration and engagement among *stakeholders*, who are the individuals or groups with a vested interest in the outcomes of the research, including academia, civil society, and state institutions. The research is anticipated to instigate a culture of collective responsibility and mutual trust by creating an efficient, transparent, and accountable system [20,21]. This is particularly significant in the current socio-political climate, where skepticism towards law enforcement practices is not uncommon. A scientifically robust system, which invites scrutiny and input from all stakeholders, methodologically sound and openly verifiable, can bridge the gap between the public and law enforcement agencies and open avenues for academic research and policy development [14,18,19].

This study proposes developing and evaluating an interoperability-enhanced information system for crime scene analysis. While the domain of knowledge management is expansive and encompasses many systems, including databases, decision support systems, and expert systems, this research narrowly concentrates on leveraging forensic ontology to integrate scientific evidence and investigative data. The system aims to serve as a centralized hub for law enforcement agencies, providing a holistic view of the crime scene by amalgamating various forms of data. Thus, the implications of this research are principally targeted at law enforcement agencies involved in investigative work, aiming to refine their methodologies by incorporating data-driven insights [24–29].

However, it is imperative to acknowledge the inherent limitations that accompany the scope of this study. While the proposed system aims to minimize human subjectivity by employing *machine-assisted reasoning*, which uses computational algorithms to aid in the analysis and interpretation of data, thereby reducing the likelihood of biased or subjective judgments, it is only partially devoid of human influence, particularly in data collection and input stages. Additionally, the focus on forensic ontology means that the study does not delve into other potentially useful knowledge management frameworks or methodologies. The utilization of machine-assisted reasoning specifically targets the reduction of human error and bias in the decision-making process, especially during the evaluation of complex multi-faceted evidence. This limitation is especially relevant in rapidly evolving technological advancements, which might offer alternative or complementary data integration and analysis approaches [12,13,26,30,31]. Therefore, the findings should be interpreted cautiously, acknowledging that they represent one of many possible avenues for enhancing investigative work.

Furthermore, although the study aims for broad applicability, it is conditioned by the availability of resources in terms of data and computational capabilities. The analysis assumes a foundational level of technological infrastructure and expertise within law enforcement agencies, which may not be universally applicable. Consequently, the implementation and effectiveness of the proposed system could vary significantly across different jurisdictions or organizations, depending on their technological readiness and adaptability. This could limit the generalizability of the study's findings and recommendations, making it essential for future research to explore these aspects in greater detail.

2. Literature Review

Forensic science has undergone significant advancements, evolving from rudimentary methods to the highly sophisticated technologies of today [32,33]. Early forensic practices were primarily based on observational skills and basic scientific principles. For instance, fingerprinting, one of the oldest forensic techniques, began as a simple yet effective way of identifying individuals based on the unique patterns found on their fingertips [34,35]. Initially, these fingerprint records were manually compared, a laborious process often leading to errors [32,33,36–39]. With the advent of computer technology, automated fingerprint

identification systems (AFIS) were developed, revolutionizing the speed and accuracy of fingerprint analysis. These computerized systems represented a significant leap forward, streamlining the identification process and allowing for the storage and quick retrieval of millions of fingerprint records [34,35,40].

Over the years, the introduction of DNA technology marked another milestone in forensic science. Unlike fingerprinting, which serves primarily as a means of identification, DNA analysis can provide additional information, such as familial relationships and genetic predispositions [40]. The complexity and sensitivity of DNA techniques, including Polymerase Chain Reaction (PCR), a method that amplifies tiny segments of DNA for easier analysis, and Short Tandem Repeat (STR) analysis, a technique that examines specific regions (or loci) within DNA to identify individuals, have granted investigators the ability to extract valuable information from the most minute biological samples This technological leap has profoundly impacted solving crimes, often enabling convictions in cases that would otherwise remain unsolved. The application of DNA technology is not confined to violent crimes alone; it has proven instrumental in a range of topics, from paternity disputes to wildlife poaching [35,40].

However, as forensic science has advanced, it has become increasingly specialized, requiring a deep understanding of various scientific disciplines such as chemistry, biology, and computer science [33,36]. For example, digital forensics is a relatively new subfield that deals with extracting and interpreting data from electronic devices, and it demands a different skill set than traditional forensic methods. With the surge in cybercrimes, expertise in digital forensics is becoming indispensable for modern law enforcement agencies. Despite the complexity and the need for specialization, the advancements in forensic science have indisputably enriched the toolkit available to law enforcement, contributing substantially to both solving crimes and securing convictions [34,36,40].

Despite the advancements in forensic science and technology, the current state of knowledge management systems within law enforcement agencies leaves much to be desired [41–43]. One of the most glaring issues is the existence of *information silos*, which are isolated pockets of data stored in disparate systems that don't communicate with each other. Various departments or units within a law enforcement agency may use different systems for storing and managing data, often with little or no interoperability [41,44,45]. For instance, the cybercrime unit might have its specialized database for digital evidence, while the homicide department may use another platform for DNA and ballistics data [36,42,43,46]. Such compartmentalization hampers the ability to cross-reference information, leading to inefficiencies and increasing the risk of oversight and errors [41,42,47]. A singular case may require integrating multiple types of evidence, and the absence of a centralized knowledge repository poses a substantial challenge in achieving this seamlessly [43,46,48].

The impact of these siloed systems is particularly acute in time-sensitive investigations, where every moment lost can affect the outcome of a case [41,42]. A lack of immediate access to relevant information can delay decision-making, compromise the quality of investigative work, and even jeopardize the safety of law enforcement personnel and public safety [45]. Additionally, these fragmented systems often result in duplicated efforts, as different units may unknowingly work on related aspects of a case without sharing crucial information. This wastes valuable resources and increases the likelihood of conflicting or contradictory evidence, which could weaken a lawsuit in court [41,44,45].

Moreover, current knowledge management systems' *data integrity*, which involves maintaining the accuracy and consistency of data over its entire lifecycle, and security issues must be addressed. Ensuring information authenticity, confidentiality, and availability becomes daunting with data's increasing complexity and volume [47,48]. Data breaches, unauthorized access, and tampering risk are ever-present, and these vulnerabilities can have severe legal and ethical repercussions. Data integrity is particularly critical in forensic science because it ensures that the data remains unaltered from its original state and can therefore be trusted. The admissibility of evidence in court hinges on the chain of

custody and the verification of its authenticity [42]. The current state of fragmented and unprotected systems exacerbates these challenges, reinforcing the need for a robust, centralized, and secure knowledge management system to meet modern law enforcement's demands [41,45,48].

Ontology plays a pivotal role in shaping the architecture of modern data management systems, particularly in contexts that require the integration of diverse and complex data sets [49,50]. At its core, ontology is a structured framework that defines the relationships between various entities and concepts within a particular domain. For example, in a forensic context, ontology could define the relationships between a suspect, a crime scene, and different types of evidence, such as DNA samples or digital data [36,51,52]. This structured approach facilitates more than just data storage; it allows for effective data retrieval and the ability to draw meaningful conclusions from complex, interconnected information [51–56]. The utility of ontology extends to creating semantic networks, which allow for the representation of complex relationships that are machine-readable and intuitively understandable for human operators [57].

Ontology's structured framework is not just a theoretical construct; it has practical implications that can significantly enhance the efficiency and effectiveness of law enforcement operations. The application of ontology in data management enables advanced querying capabilities, making it possible to ask complex questions that span multiple data sets and types [53,57,58]. For instance, investigators could query the relationship between a DNA sample found at one crime scene and digital evidence from another, all within the same ontological framework [36,42,49]. This is particularly useful in cases involving serial crimes or organized criminal networks, where the ability to link seemingly unrelated pieces of information can be crucial for solving issues. Moreover, the ontological structure supports formal reasoning algorithms, which can autonomously generate insights and identify previously unnoticed patterns or connections, thereby aiding investigators in hypothesis generation and validation [57–59].

However, the implementation of ontology in data management presents challenges [53]. Designing an ontological framework that is comprehensive and flexible enough to adapt to the evolving nature of criminal activities requires a deep understanding of the domain and expertise in ontology design principles. Furthermore, the effectiveness of an ontology-based system is highly dependent on the quality and completeness of the data it contains [51,52]. Incomplete or inaccurate data can lead to misleading or false conclusions, and therefore, the data input process must be rigorously controlled and validated. Despite these challenges, the benefits of incorporating ontology in data management systems, especially in the complex and dynamic field of law enforcement, are substantial, offering a pathway to more informed and objective decision-making [49,57,58].

3. Methodology

The present study proposes developing a prototype forensic ontology as the primary artifact to fulfill the research objectives. The development followed a systematic *design science research methodology* (Design Science Research Methodology), particularly suited for creating innovative artifacts to solve complex problems. The research began with a problem identification stage involving an extensive literature review and interviews with domain experts in law enforcement and forensic science [60–63]. This initial phase helped define the prototype's scope and limitations, ensuring that it addresses the most pressing challenges in current knowledge management systems while being adaptable to the evolving landscape of forensic science. The design process then proceeded through iterative cycles of development, testing, and refinement, involving academic researchers and practitioners in the field to validate the practicality and efficacy of the system [64–66].

The prototype's design incorporated key components such as data sources, a data integration layer, and a logical inference engine. The ontological framework was built using semantic OWL language and descriptive logic, facilitating complex querying and formal reasoning [67–69]. Given that the study focuses on crime scene analysis, the ontology was

populated with entities and relationships most relevant to this context, such as types of evidence, crime scenes, suspects, and investigative actions. The prototype was designed to be highly modular, allowing for future expansions or modifications, such as adding additional data types or integrating more advanced reasoning algorithms. A case study was then conducted to evaluate the prototype, using both simulated and real-world scenarios to assess its ability to integrate diverse data sets and generate meaningful insights.

Semantic Web Ontology Language (OWL) and descriptive logic were the primary tools used to develop the forensic ontology in this research [69–71]. The choice of these tools was motivated by their ability to represent complex relationships in a machine-readable format while enabling sophisticated querying and formal reasoning [63,67,68,72,73]. OWL is a W3C standard language designed explicitly for ontology modeling and is widely supported by various ontology editors and reasoning engines [71]. It provides a robust set of constructs for defining classes, properties, and constraints, making it an ideal choice for creating a comprehensive and intricate ontological framework. On the other hand, descriptive logic serves as the underlying formalism that guides the structure and semantics of the ontology [74,75]. It provides the inference rules and allows for validating the relationships defined in the ontology, thereby ensuring logical consistency and coherence [67–69].

In addition to OWL and descriptive logic, several software platforms were utilized to develop and evaluate the forensic ontology [73]. Protégé, an open-source ontology editor, created and modified the ontology, providing a user-friendly interface for managing complex relationships and rules [76]. Furthermore, the Pellet Reasoning Engine was integrated into the system for the logical reasoning component [74,76]. This engine performs automated reasoning tasks based on the OWL constructs and descriptive logic rules, fulfilling the system's requirement for a formal reasoning process [73]. The overall architecture was supported by a relational database backend for data storage, and the front end was developed using standard web technologies like HTML, CSS, and JavaScript, ensuring that the system is scalable and accessible [71,76].

3.1. Technological Readiness of Law Enforcement Agencies

Addressing the technological readiness of diverse law enforcement agencies is critical for the successful implementation of the proposed forensic ontological system. This subsection aims to delineate the varying levels of technological sophistication among these agencies and propose solutions for less tech-savvy bodies, as well as address concerns about the heavy reliance on Semantic OWL and descriptive logic.

To cater to the needs of less tech-savvy law enforcement agencies, several strategies were considered. First, the ontological system was designed to be modular and scalable, allowing for incremental adoption based on the agency's technological readiness. Agencies can start with basic functionalities and gradually add more sophisticated modules as they become more comfortable with the system.

Second, development of a user-friendly interface is proposed, complete with training modules and support documentation. This aims to lower the barrier to entry and facilitate easier system adoption. Third, partnerships with governmental and non-governmental organizations were sought to provide additional training and financial resources for system implementation. These partnerships aim to bridge the technological gap and ensure that all agencies, irrespective of their current capabilities, can benefit from the system.

Lastly, the system architecture was designed to be compatible with existing legacy systems [59,77–80]. This is to ensure that even agencies with outdated technologies can integrate the proposed system without requiring a complete overhaul of their existing infrastructures.

In addition to technological readiness, the system's reliance on Semantic OWL and descriptive logic warrants consideration. The usage of these technologies enables a more robust and formal representation of forensic data, but it also introduces challenges, especially when discrepancies in data occur. To address this, the system incorporates adaptability measures, such as data validation algorithms that can detect and rectify inconsistencies in

the input data. Furthermore, the system has built-in mechanisms for handling uncertain or ambiguous information, thereby ensuring the integrity and reliability of the reasoning process.

In summary, by taking into account the diverse technological readiness and semantic adaptability requirements of law enforcement agencies, the proposed system adopts a flexible, user-centric approach to encourage widespread adoption, thereby enhancing the collective capability of these agencies in forensic investigations.

3.2. Comparison with Alternative Approaches

In an evolving landscape where data-driven methodologies are increasingly being integrated into law enforcement systems, alternative approaches have been scrutinized. Methods such as relational databases, keyword-based searches, and rule-based expert systems have previously been employed [56,59,77–80].

The choice of an ontology-based approach over these alternative methods was driven by its inherent capabilities for semantic representation and formal reasoning [81–84]. Unlike relational databases that struggle with semantic ambiguities, the ontology approach captures complex relationships and enables intricate queries. Moreover, while keyword-based searches offer a simpler method for data retrieval, they fall short in creating semantic connections between data entities [85–88]. Rule-based expert systems, although effective for specific tasks, lack the flexibility to adapt to the diverse and dynamic nature of crime scene investigations.

Therefore, an ontology-based approach, especially when combined with descriptive logic and OWL, presents a more comprehensive and adaptive framework capable of addressing the multifaceted nature of forensic investigations.

3.3. Criteria for Selecting OWL over Other Methods

The selection of OWL for the creation of the legal ontology was made after careful evaluation of alternative options. Semantic richness is offered by OWL, a feature scarcely found in relational databases or XML schemas. While relational databases excel in managing structured data, they struggle to represent complex, hierarchical, or intricate relationships [29,56].

Furthermore, supported formal reasoning was another contributing factor to the choice of OWL. Unlike languages such as RDF Schema, which are limited in their inferencing capabilities, OWL is based on description logic and allows for more advanced analyses.

In addition, the advantage of wide support and tooling was afforded by OWL, being a W3C standard. In contrast to customized solutions or less popular languages, this offers a foundation for future expansion and collaboration.

Finally, scalability was a critical issue that was addressed. Traditional databases may require significant revisions when new data or functions are added, whereas OWL is designed in a way that makes it easier to manage large and dynamically increasing datasets.

In this manner, the selection of OWL was found to be most apt, aligning fully with the multidimensional requirements and objectives of the legal ontological system.

4. Conceptual Framework

The conceptual framework for this study leverages the principles of ontology to create a semantic representation of crime scenes to enable a more sophisticated and nuanced analysis of evidence and data. In this context, the term "semantic representation" refers to a structured model that not only stores data but also understands and interprets the relationships between different types of information, such as DNA samples, digital evidence, and witness testimonies [82,89,90]. The framework can represent complex hierarchies and dependencies among these diverse data types by adopting ontology. For instance, a DNA sample could be linked to multiple crime scenes related to various suspects, witnesses, and other forms of evidence like digital footprints or surveillance footage [42,82,89,90].

The ontological structure allows for this intricate web of relationships to be mapped out logically and consistently, thereby enriching the depth of the analysis and facilitating more effective investigative strategies [70,71,76,82,90,91].

Forensic ontology is the backbone of the proposed information system, providing the rules and constructs governing how data is stored, retrieved, and analyzed. In addition to serving as a repository for multi-modal data, ontology plays an active role in the reasoning process [92–94]. By incorporating descriptive logic rules into the ontology, the system can conduct formal reasoning to generate new insights or hypotheses based on the existing data. For example, suppose a new DNA sample is entered into the system. In that case, the ontology-based reasoning engine can automatically identify potential matches or discrepancies with existing records, thereby aiding investigators in drawing timely and accurate conclusions. This proactive role of the ontology extends the system's utility beyond mere data storage, making it an invaluable tool for both reactive and proactive investigative processes [91,92,95,96].

Descriptive logic serves as the formalism that underpins the ontological structure, employed to define the relationships between different sets of data and facilitate more effective reasoning within the system [97–100]. In essence, descriptive logic provides a set of rules and constructs that guide the interpretation of the ontology, ensuring that it adheres to a coherent and logically consistent framework. For example, descriptive logic can define the conditions under which a particular piece of evidence, such as a DNA sample, can be considered a match or a mismatch with another example in the database [98,99,101]. These rules are not mere static guidelines but dynamic constructs enabling the system to perform automated reasoning. By applying these rules, the system can make inferences, validate hypotheses, and generate new questions or lines of investigation that may not have been immediately apparent to human investigators [99,100].

Integrating descriptive logic into the forensic ontology enhances the system's ability to manage complex, multi-faceted data sets. It provides the mechanism for complex querying and extracting nuanced insights from the accumulated data [101–104]. For instance, investigators could input a complex query asking whether any DNA samples from unsolved cases match the profiles of newly entered suspects. The descriptive logic rules would guide the reasoning engine in interpreting this query, navigating through the ontological relationships to provide a comprehensive and logically sound answer [102,103]. This way, descriptive logic elevates the system's capabilities from mere data storage and retrieval to more dynamic knowledge management. It provides actionable insights that can significantly aid law enforcement agencies' investigative processes [98,101].

The Semantic Web Ontology Language (OWL) plays a critical role in the conceptual framework, serving as the language that actualizes the ontology and descriptive logic into a functional system [71,76,105–107]. Semantic OWL language enables the system to understand and interpret complex relationships between various data points, converting raw data into actionable knowledge [108–111]. OWL's rich vocabulary and expressive power make it possible to define intricate relationships and constraints within the ontological structure. For example, OWL can specify that a "fingerprint match" can only occur if a crime scene and a fingerprint from a database share specific predefined characteristics. This level of detail is vital for ensuring the accuracy and reliability of the reasoning process, and it adds a layer of rigor to the system's analytical capabilities [108,112,113].

Moreover, OWL's semantic capabilities extend beyond just defining relationships; they also facilitate the integration of disparate data types into a cohesive whole. Given that crime scene analysis often involves a plethora of data, including biological samples, digital evidence, and eyewitness accounts, the ability to semantically link these diverse data points is invaluable [105,108,111]. The OWL language provides the tools to create such semantic bridges, allowing for harmonizing data that might initially seem unrelated. This capability is handy for investigators who must compile fragmented or incomplete information to form a coherent picture of a crime scene. By employing OWL as the semantic foundation of the system, the framework ensures that it can adapt to the complexities and nuances

inherent in forensic investigations, thereby fulfilling its aim of providing a comprehensive, reliable, and dynamic tool for law enforcement agencies [71,108,112,113].

Integration of Knowledge Management Tools

The integration of Knowledge Management Tools significantly amplifies the capabilities of the existing conceptual framework. Firstly, these tools build upon the existing ontology to offer a more sophisticated layer of abstraction for data representation. Specifically, the incorporation of taxonomies, classifications, and metadata enhances the semantic depth of the data, thereby streamlining the search, retrieval, and interpretation processes [97,105,107,114,115].

This enriched ontology serves as a foundation for the next logical extension: augmented reasoning capabilities. Knowledge Management Tools introduce advanced machine learning algorithms, supplementing the existing ontology-based reasoning mechanisms. These algorithms enable a greater array of analytical processes, making the system more versatile in conducting seamless and efficient analyses [83,91,95].

Furthermore, data integration is markedly improved through the use of these tools. Advanced mapping techniques and data transformation processes are employed to harmonize disparate data types, such as text, images, and geospatial data, into a unified ontology. This enhanced integration adds versatility to the system, making it capable of accommodating and interpreting a broader range of information types.

Another vital contribution of Knowledge Management Tools is their impact on the system's query capabilities. They bring added flexibility to the existing descriptive logic rules, thereby facilitating the processing of complex, multi-variable, and conditional queries. This adaptability enables more nuanced data extraction and reporting, enriching the overall utility of the system [74,97,116–118].

In conclusion, the utility of the Knowledge Management Tools extends beyond mere data management. They also have a profound impact on the investigative strategies of law enforcement agencies. By incorporating real-time analytics and predictive modeling, these tools pave the way for more dynamic and proactive policing strategies. Hence, they fulfill the system's overarching objective of serving as a comprehensive resource for law enforcement, not only by enhancing data storage and retrieval but also by significantly influencing proactive investigative methodologies.

5. Ontology Development

In the domain of knowledge engineering, the significance of ontologies as a means for structuring and formalizing domain-specific knowledge must be balanced. Protege, a free, open-source ontology editor developed by the Stanford Center for Biomedical Informatics Research, is a critical tool widely employed for this purpose. Within this software environment, the creation, manipulation, and sharing of ontologies are facilitated, offering researchers a robust platform for academic and industrial applications [76,88,119,120].

One of the foundational components in the development of an ontology is the concept of "classes", which categorize entities within the domain of interest. A class is a blueprint for objects with common attributes or relations. Subclasses represent entities that inherit the characteristics of their parent classes but may possess additional features or links that distinguish them. For instance, in a medical ontology, the class "Disease" might have subclasses like "Infectious Disease" and "Genetic Disorder", each with its own set of attributes and relationships [120–122].

Another integral aspect of ontology development involves using "object properties", which define the relationships between different classes. Object properties specify how instances of one type can be related to models of another, thus capturing the complexity and interconnectedness of domain-specific entities. For example, an object property could specify that a "Patient" is related to a "Disease" through a "hasDiagnosis" relationship, enabling the formalization of intricate domain knowledge [88,119].

The concept of "data properties" further refines the granularity of ontologies by associating instances of classes with literal values. Unlike object properties, which link cases of different types, data properties connect models to data values such as strings, numbers, or dates. In a healthcare ontology, for example, a data property might specify that a "Patient" has an "age" that is an integer or a "name" that is a string [88,119].

In summary, the development of an ontology involves a series of structured steps and relies heavily on the understanding and formalization of classes, subclasses, object properties, and data properties. Protege serves as a comprehensive tool that enables this intricate process, offering a variety of features that assist in developing, testing, and deploying robust ontologies. Complex domains can be modeled with high precision through the judicious use of these ontology components, facilitating advanced applications in areas ranging from artificial intelligence and semantic web technologies to industry-specific solutions [88,119–122].

In ontology development for the Semantic Web, the role of "individuals" or "instances" emerges as a critical aspect of semantic representation. Individuals are specific occurrences of classes, serving as the concrete data points that populate the ontological structure. In essence, individuals are to classes what data entries are to database schemas. They embody the real-world entities the ontology aims to describe, enabling the transition from abstract, domain-specific knowledge to actionable insights. In the Protege environment, individuals are explicitly defined and managed through a dedicated interface, offering a seamless method for populating ontological classes. When formulated in OWL (Web Ontology Language), individuals are associated with object and data properties, inheriting the relational and attribute-based characteristics defined at the class level. Including individuals enhances an ontology's expressivity and utility, allowing for a more nuanced capture of domain knowledge and facilitating complex reasoning tasks [120].

Based on the above, a rigorously defined framework for ontology development emerges. Specifically, the process encompasses four phases: 1. *Needs assessment and analysis*, 2. *Design*, 3. *Development*, and 4. *Evaluation and adaptation* [Figure 1].

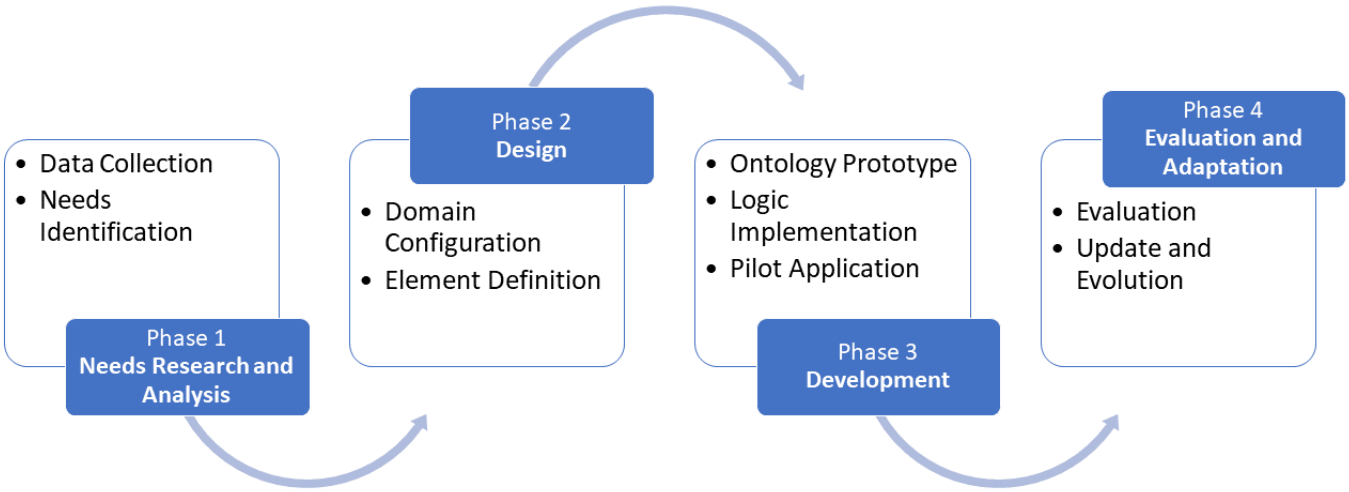

Figure 1. Four Phases of Forensic Ontology Development.

In Detail:

- Phase 1: Needs Research and Analysis
  - o Data Collection: All available data from various sources, such as types of crimes, investigation procedures, types of evidence, and data, are collected.
  - o Needs Identification: The needs of the involved entities (police, judicial system, public) are understood.
- Phase 2: Design

- Domain Configuration: The primary domains of the ontology (e.g., Identities, Criminal Actions, Investigative Procedures, Adjudication) are defined.
- Element Definition: The classes, properties, and data properties to be included are defined.

- Phase 3: Development
  - Ontology Prototype: A prototype is created using tools such as Protege, with OWL as the language.
  - Logic Implementation: Descriptive logic is incorporated for functions such as reasoning, classification, and other query operations.
  - Pilot Application: The ontology is tested in real or hypothetical cases to validate its effectiveness and accuracy.
- Phase 4: Evaluation and Adaptation
  - Evaluation: Feedback is collected from the involved entities and necessary modifications are made.
  - Update and Evolution: The ontology is improved and updated in accordance with new technologies and data.

In the developed proposal ontology context, three key tables serve as pivotal reference points that encapsulate the various elements and their interrelations. Table 1 outlines the Classes and Subclasses, providing a hierarchical view of the entities and their specialized forms within the domain. Each class and subclass are accompanied by a description elucidating its specific role and attributes. Table 2 focuses on Object Properties, detailing the relationships between different types. This table specifies each object property's domain, range, and characteristics, comprehensively mapping how entities interact within the ontology. Table 3, on the other hand, is devoted to Data Properties, listing the properties that link class instances to literal values. This table elucidates each data property's domain, range, and characteristics, enabling a finer granularity in representing domain-specific information. Collectively, these tables serve as the backbone of the ontology, offering a structured and detailed overview that is indispensable for both development and subsequent applications.

Table 1. Enumerates the foundational 'Classes' and 'Subclasses' of the proposed Forensic Ontology, providing a brief 'Description' for each. It serves as a guide for understanding and implementing the ontology.

Classes	Subclasses	Description
CrimeScene	CrimeUnderInvestigation	The specific offense or offenses currently being looked into.
	VictimFound	The individual or individuals who have been directly affected by the crime and are present at the scene.
	TopographicDiagram	A schematic representation of the crime scene's layout.
	FingerprintCollection	The gathering of fingerprint evidence from the crime scene.
	DNACollection	The collection of biological material for DNA analysis.
	ForensicPhotography	The process of taking photographs of the crime scene and evidence.
	AutopsyReport	A medical report detailing the cause and circumstances of a death.
	SeizureOfObject	The act of lawfully confiscating an object for evidence.
	VideoFootageCollection	Gathering video recordings related to the crime.
JudicialActions	WitnessTestimony(Civilian)	Statements given by non-law enforcement witnesses.
	WitnessTestimony(Police)	Statements given by law enforcement officers.
	Defendant'sStatement	The statement or defense presented by the person accused of the crime.
ForensicMedicalReport	CrimeVictim	The individual or individuals directly affected by the crime.
	VictimExamined	The process of medically examining the victim for evidence and information.
	CauseOfDeath	Medical reasons explaining the victim's death.
	LethalWeapon	The object or method used to carry out the killing.

Table 1. *Cont.*

Classes	Subclasses	Description
MobilePhoneData	ModeOfCommunication	The type of communication used (e.g., SMS, call).
	DurationOfCommunication	The length of the communication event.
	DateOfCommunication	The date when the communication took place.
	TimeOfCommunication	The specific time when the communication occurred.
	ActivatedMobileTower	The cellular tower facilitated the communication.
	IP_OfCommunication	The IP address used during the communication.
Humans	Witnesses	Individuals who have relevant information but are not directly involved in the crime.
	Victims	Individuals who have been directly affected by the crime.
SurveillanceData	CCTV_Footage	Video captured from closed-circuit television cameras.
	AudioRecordings	Recorded audio that may be used as evidence.
LegalDocuments	SearchWarrants	Legal documents authorizing the search of premises.
	ArrestWarrants	Legal documents authorizing the arrest of an individual.
InvestigationTeam	LeadInvestigator	The person in charge of guiding the investigation.
	SupportingStaff	Additional staff aiding in various aspects of the investigation.
CaseStatus	Open	The case is currently under investigation.
	Closed	The case has been resolved or dismissed.
	PendingReview	Awaiting further action or analysis.

From Tables 1–3, a Preliminary Forensic Ontology can be constructed for the purpose of experimenting with some basic functionalities, such as querying using descriptive logic. This preliminary Forensic Ontology is submitted as Supplementary Material. The development of a comprehensive Forensic Ontology necessitates the interface between various stakeholders, such as law enforcement agencies, forensic medical services, the prosecution office, and the university.

Once developed, the ontology could be visually represented as shown in Figure 2.

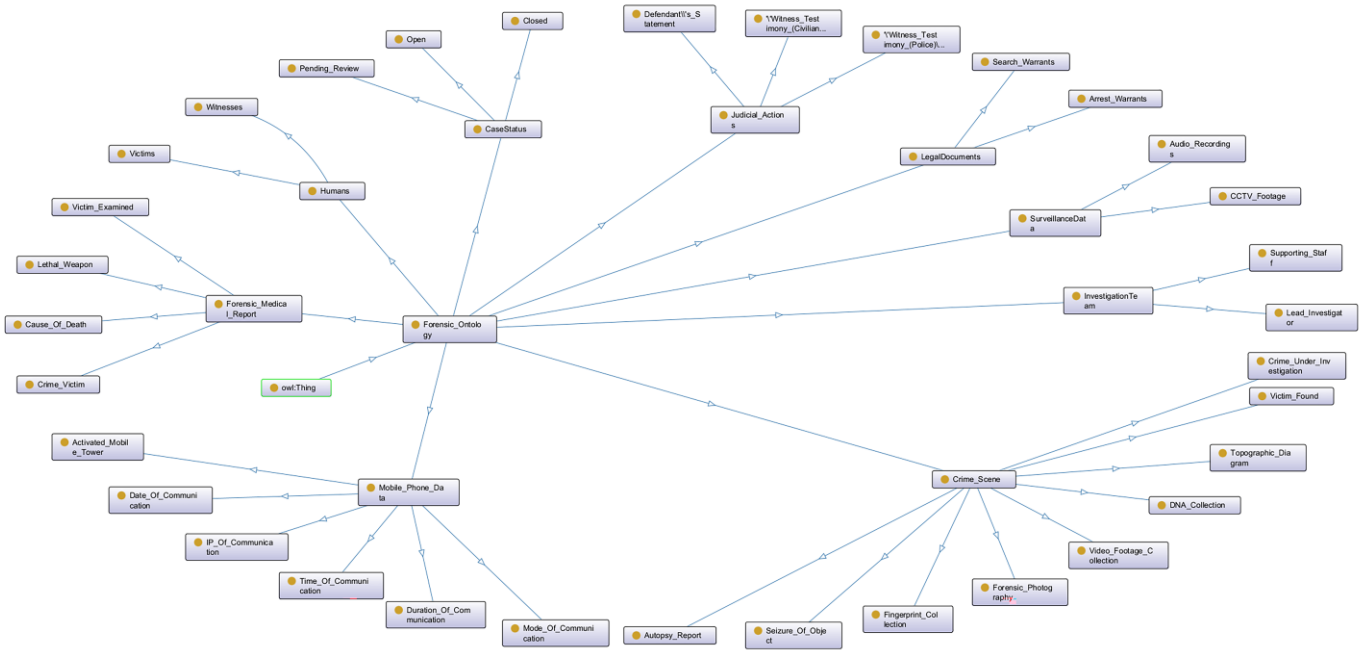

Figure 2. Provides a visual representation of the proposed Forensic Ontology, featuring its Classes and Subclasses as outlined in Table 1. The figure serves to graphically elucidate the hierarchical relationships and structural complexity inherent to the ontology.

Table 2. Delineates the Object Properties crucial to the Forensic Ontology. Each property is characterized by its 'Domain', 'Range', and specific 'Characteristics', alongside a brief 'Description' that clarifies its role in linking various forensic entities and processes.

Property	Domain	Range	Characteristics	Description
hasCrimeUnderInvestigation	CrimeScene	CrimeUnderInvestigation	Symmetric	Links a crime scene to the specific offenses being investigated.
hasVictim	CrimeScene	VictimFound	Symmetric	Links a crime scene to the victims found.
hasTopographicDiagram	CrimeScene	TopographicDiagram	Functional	Links a crime scene to its topographic layout.
hasFingerprint	CrimeScene	FingerprintCollection	Symmetric	Links a crime scene to collected fingerprints.
hasDNA	CrimeScene	DNACollection	Symmetric	Links a crime scene to collected DNA samples.
hasPhotographicEvidence	CrimeScene	ForensicPhotography	Functional	Links a crime scene to forensic photographs.
hasAutopsyReport	CrimeScene	AutopsyReport	Functional	Links a crime scene or victim to an autopsy report.
hasSeizedObject	CrimeScene	SeizureOfObject	Symmetric	Links a crime scene to objects that have been seized as evidence.
hasVideoFootage	CrimeScene	VideoFootageCollection	Symmetric	Links a crime scene to collected video footage.
hasCivilianWitnessStatement	JudicialActions	WitnessTestimony(Civilian)	Symmetric	Links judicial actions to statements given by civilian witnesses.
hasPoliceWitnessStatement	JudicialActions	WitnessTestimony(Police)	Symmetric	Links judicial actions to statements given by police officers.
hasDefendantStatement	JudicialActions	Defendant'sStatement	Functional	Links judicial actions to the statement made by the defendant.
examinesVictim	ForensicMedicalReport	VictimExamined	Functional	Links a forensic medical report to the examination of the victim.
identifiesCauseOfDeath	ForensicMedicalReport	CauseOfDeath	Functional	Links a forensic medical report to the cause of death.
identifiesLethalWeapon	ForensicMedicalReport	LethalWeapon	Functional	Links a forensic medical report to the weapon or method that caused death.
usesCommunicationMode	MobilePhoneData	ModeOfCommunication	Symmetric	Links mobile phone data to the method of communication used.
hasCommunicationDuration	MobilePhoneData	DurationOfCommunication	Functional	Links mobile phone data to the duration of the communication.
hasCommunicationDate	MobilePhoneData	DateOfCommunication	Functional	Links mobile phone data to the date of the communication.
hasCommunicationTime	MobilePhoneData	TimeOfCommunication	Functional	Links mobile phone data to the time of the communication.
activatesMobileTower	MobilePhoneData	ActivatedMobile Tower	Symmetric	Links mobile phone data to the mobile tower that facilitated the communication.
usesIP	MobilePhoneData	IP_OfCommunication	Functional	Links mobile phone data to the IP address used during the communication.
involvesWitness	Humans	Witnesses	Symmetric	Links a case or judicial action to individuals who are witnesses.
involvesVictim	Humans	Victims	Symmetric	Links a case or judicial action to individuals who are victims.
involvesCCTV	SurveillanceData	CCTV_Footage	Symmetric	Links surveillance data to CCTV footage.
involvesAudioRecording	SurveillanceData	AudioRecordings	Symmetric	Links surveillance data to audio recordings.
involvesSearchWarrant	LegalDocuments	SearchWarrants	Functional	Links legal documents to search warrants.
involvesArrestWarrant	LegalDocuments	ArrestWarrants	Functional	Links legal documents to arrest warrants.
hasLeadInvestigator	InvestigationTeam	LeadInvestigator	Functional	Links an investigation team to its lead investigator.
hasSupportingStaff	InvestigationTeam	SupportingStaff	Symmetric	Links an investigation team to its supporting staff.
hasCaseStatus	JudicialActions	CaseStatus	Functional	Links an investigation to its current status (open, closed, pending review).

Table 3. Outlines the Data Properties essential to the Forensic Ontology. These properties are classified by their 'Domain', 'Range', and specific 'Characteristics', accompanied by a succinct 'Description' that explicates the property's role in capturing quantifiable or textual information within the forensic context.

Data Property	Domain	Range	Characteristics	Description
crimeReportedDate	CrimeScene	xsd:date	Functional	The date when the crime was reported.
crimeOccurredTime	CrimeScene	xsd:time	Functional	The time when the crime occurred.
numberOfVictims	VictimFound	xsd:integer	Functional	The number of victims found at the crime scene.
fingerprintCount	FingerprintCollection	xsd:integer	Functional	The number of fingerprints collected.
DNASequencesCollected	DANN_Collection	xsd:integer	Functional	The number of DNA sequences or samples collected.
autopsyDate	AutopsyReport	xsd:date	Functional	The date when the autopsy was performed.
seizedObjectCount	SeizureOfObject	xsd:integer	Functional	The number of objects seized.
videoFootageDuration	VideoFootageCollection	xsd:duration	Functional	The duration of the video footage collected.
civilianWitnessCount	JudicialActions	xsd:integer	Functional	The number of civilian witnesses.
policeWitnessCount	JudicialActions	xsd:integer	Functional	The number of police witnesses.
defendantName	Defendant'sStatement	xsd:string	Functional	The name of the defendant.
victimMedicalReportDate	VictimExamined	xsd:date	Functional	The date when the medical examination of the victim took place.
causeOfDeath	CauseOfDeath	xsd:string	Functional	The medical reason for the victim's death.
lethalWeaponType	LethalWeapon	xsd:string	Functional	The type of weapon or method that caused death.
communicationMode	ModeOfCommunication	xsd:string	Functional	The method of communication used (e.g., SMS, call).
communicationDuration	DurationOfCommunication	xsd:duration	Functional	The duration of the communication.
communicationDate	DateOfCommunication	xsd:date	Functional	The date of the communication.
communicationTime	TimeOfCommunication	xsd:time	Functional	The specific time when the communication occurred.
mobileTowerLocation	ActivatedMobileTower	xsd:string	Functional	The location of the activated mobile tower.
IPAddress	IP_OfCommunication	xsd:string	Functional	The IP address used for the communication.
witnessStatement	Witnesses	xsd:string	Functional	The statement provided by the witness.
victimStatement	Victims	xsd:string	Functional	The statement or account provided by the victim.
CCTVFootageLocation	CCTV_Footage	xsd:string	Functional	The location where the CCTV footage was captured.
audioRecordingDuration	AudioRecordings	xsd:duration	Functional	The duration of the audio recording.
searchWarrantIssuedDate	SearchWarrants	xsd:date	Functional	The date when the search warrant was issued.
arrestWarrantIssuedDate	ArrestWarrants	xsd:date	Functional	The date when the arrest warrant was issued.
leadInvestigatorName	LeadInvestigator	xsd:string	Functional	The name of the lead investigator.
supportingStaffCount	SupportingStaff	xsd:integer	Functional	The number of supporting staff involved in the investigation.
caseStatus	CaseStatus	xsd:string	Functional	The current status of the case (e.g., Open, Closed, Pending Review).

5.1. Description Logic

Description Logic (DL) serves as a formal framework for representing the conceptual structure of domains in a semantically rigorous manner [83,123–126]. Utilized primarily in ontology modeling and artificial intelligence, it aims to provide a set of constructors to define complex concepts based on simpler ones. In the realm of ontology development, DL is often employed to enable automated reasoning over concepts and relationships, thereby allowing for the validation of the structural and semantic integrity of the model. This capability underpins its widespread application in ontology-based systems, facilitating tasks such as knowledge extraction, consistency checking, and inferencing [126–130].

The logical operators in Description Logic hold particular significance for their role in shaping the semantics of the ontology. Standard constructors include existential quantification ($\exists$), universal quantification ($\forall$), conjunction ($\cap$), and negation ($\neg$), among others [129–132]. These operators allow for the expression of intricate relationships and constraints among ontology elements. For instance, in this discussed Forensic Ontology, the class "Crime Scene" and its subclass "Victim Found" could be represented as:

$$CrimeScene \sqsubseteq \exists hasVictim.VictimFoundCrimeScene \sqsubseteq \exists hasVictim.VictimFound,$$

indicating that a Crime Scene necessarily involves the existence of a Victim Found. Similarly, the object property "hasCrimeUnderInvestigation" linking "Crime Scene" to "Crime Under Investigation" can be described as:

$$hasCrimeUnderInvestigation : CrimeScene \rightarrow CrimeUnderInvestigationhasCrimeUnderInvestigation : CrimeScene \rightarrow CrimeUnderInvestigation.$$

Data properties, as mentioned in the context of the same Forensic Ontology, associate individuals from the domain of a class with data values. For example, the data property "crimeReportedDate" attached to the "Crime Scene" class can be written as:

$$crimeReportedDate : CrimeScene \rightarrow xsd : datecrimeReportedDate : CrimeScene \rightarrow xsd : date,$$

Indicating that each instance of a Crime Scene is associated with a date value. This formalization using Description Logic provides a mathematical foundation for the ontology and enables the application of automated reasoning tools for ontology verification and query answering. Thus, the transition from tabular representations to Description Logic enhances the ontology's operational effectiveness and semantic clarity [132–135].

5.2. Reasoning on Forensic Ontology

Reasoning in ontologies and the Semantic Web pertains to the formal inference process by which new knowledge is derived from existing data and relationships. In essence, ontologies serve as a structured framework for organizing and categorizing information, thereby enabling sophisticated forms of logical reasoning [58,74,82,91]. Within this framework, various reasoning techniques, such as deductive, inductive, and abductive reasoning, can infer new facts or validate existing ones. The Semantic Web, an extension of the World Wide Web, is built upon these ontologies and employs reasoning to link and integrate disparate data sources. Using descriptive logic and formal reasoning procedures, the Semantic Web seeks to transform the Internet into a more intelligent and intuitive environment where automated reasoning is carried out to facilitate information retrieval and decision-making processes [71,76,124–127].

Applying reasoning in forensic analysis through ontologies offers manifold pivotal advantages for law enforcement agencies [81,100,136]. First and foremost, ontological sense enhances the accuracy and reliability of crime scene investigations by systematically correlating multiple types of evidence and data points. This is particularly beneficial for

complex cases that involve a vast array of interconnected elements such as DNA samples, fingerprints, and witness statements [74,84,97,137]. Additionally, ontological reasoning promotes the objectivity and impartiality of forensic analysis by reducing human error and subjectivity. A more nuanced and holistic understanding of the crime scene is achieved by formalizing the relationships between different classes and subclasses of evidence and incorporating them into a single, unified system. This, in turn, enhances the quality of evidence presented in court and aids in administering justice [124–127].

Using reasoning and reasoners by law enforcement personnel addresses several critical challenges in criminal investigations. For instance, the issue of data silos, where information is stored in disparate, unconnected databases, is mitigated through the integration and semantic linking of data [136,138]. This speeds up the investigative process and ensures that every critical piece of evidence is noticed. Furthermore, reasoning enables predicting and identifying criminal patterns, thereby aiding in proactive policing and preventing future crimes. Automated reasoners can sift through large volumes of data to identify inconsistencies or contradictions in witness statements, evidence, or the internal logic of the case itself. This capability is invaluable for validating an investigation's integrity and flagging potential miscarriages of justice. Hence, reasoning and reasoners are vital tools for enhancing law enforcement operations' effectiveness, integrity, and reliability [82,91,95,129,139].

6. Scenario Example

We now focus on a hypothetical crime scene scenario to demonstrate the practical applications of forensic ontology and reasoning in criminal investigations. In this simulation, five different crime scenes involving murder are presented. While each set is unique, certain common elements, such as fingerprints and DNA samples, are observed across multiple locations. Witness statements have been gathered, describing individuals related to the crimes. These crime scenes are located within geographically relevant areas, providing an intricate web of information that can be unraveled through ontological reasoning to identify the perpetrator.

Script

Five crime scenes are distributed across a city, each bearing striking similarities to one another:

- Crime Scene 1: A body was found in an alley with fingerprints on a discarded weapon nearby.
- Crime Scene 2: A victim was discovered in an abandoned warehouse, and DNA samples were collected from a cloth next to the body.
- Crime Scene 3: A body was found in a park, and fingerprints were collected from a park bench.
- Crime Scene 4: A victim in a car parked in a garage, DNA samples on the steering wheel.
- Crime Scene 5: A body was discovered in a motel room, with fingerprints on the doorknob.

Witness statements from various scenes describe a person seen loitering in the vicinity wearing a red jacket. The same DNA and fingerprint patterns are found in scenes 1, 3, and 5.

All elements from the Script are incorporated as Individuals in the Forensic Ontology according to Table 4, so that the Forensic Ontology can provide us with information by formulating suitable queries.

Descriptive Logic to Identify the Perpetrator

- $hasFingerprint(CS1, FP1) \cap hasFingerprint(CS3, FP3) \cap hasFingerprint(CS5, FP5)$
- $hasDNA(CS2, DNA2) \cap hasDNA(CS4, DNA4)$
- $involvesWitness(CS1, W1) \cap involvesWitness(CS2, W2) \cap \ldots$
- $hasCaseStatus(CS1, Open) \cap hasCaseStatus(CS2, Open) \cap \ldots$

Using reasoning, it can be inferred that the same fingerprints found in scenes 1, 3, and 5 indicate a typical perpetrator. Furthermore, the witness descriptions of an individual in a red jacket across multiple locations corroborate this connection. Therefore, reasoning and forensic ontology can be employed to logically deduce that these crimes are the work of a single individual, at this moment identified as the 'Perpetrator'.

Table 4. Lists the Individual Instances within key Classes of the Forensic Ontology, offering specific 'Description' for each set of instances. These instances serve as real-world examples or case-specific data points within the ontology framework.

Classes	Individual Instances	Description
Crime Scene	CS1, CS2, CS3, CS4, CS5	The five different crime scenes.
Fingerprint	FP1, FP3, FP5	Fingerprints found at scenes 1, 3, and 5.
DNA	DNA2, DNA4	DNA samples found at scenes 2 and 4.
Witnesses	W1, W2, W3, W4, W5	Witnesses from each crime scene.
Humans	Perpetrator	The individual responsible for the crimes.
Case Status	Open	The case is currently under investigation.

In summary, the significance of forensic ontology and reasoning is reaffirmed through this exercise. Such methodologies allow for the systematic analysis of complex and multifaceted crime scenes, thereby enhancing the efficacy and reliability of criminal investigations.

7. Discussion and Conclusions

The far-reaching implications of the proposed interoperability-enhanced, data-driven forensic ontological system for law enforcement cannot be overstated. By amalgamating various types of evidence and data in a centralized platform, the system confers unprecedented analytical depth and precision for crime scene investigations. Incorporating reasoning techniques further empowers this framework, allowing for the extraction of nuanced insights that would otherwise remain elusive. This fortifies law enforcement agencies' investigatory capabilities and significantly elevates the standard of evidence presented in judicial settings, thereby contributing to more accurate and just outcomes.

Specific Analysis of Findings: In the hypothetical scenario explored within the manuscript, the system's ability to integrate multiple forms of evidence such as fingerprints, DNA samples, and witness accounts contributes uniquely to identifying the perpetrator. Each form of evidence enhances the reliability and validity of the findings, effectively reducing uncertainties and blind spots in the investigation.

Moreover, this system's impact extends well beyond law enforcement, offering fertile ground for academic exploration and societal collaboration. The multidisciplinary nature of the framework opens new avenues for scholarly research into semantic technology, data analytics, and forensic science. Concurrently, the system encourages broader societal engagement by integrating diverse stakeholders, including academia, government institutions, and civil society, into a unified effort to bolster public safety and justice. This collaborative ethos enriches the investigative process and engenders a culture of shared responsibility for societal well-being.

Evaluation of Data Collection Techniques: Our methods for data collection and analysis have proven to be effective but are not without limitations. For example, the speed at which data can be processed may be hindered by the sheer volume of data or the complexity of the algorithms employed.

The study unequivocally demonstrates the efficacy and viability of integrating an ontological approach into forensic analyses of crime scenes. The hypothetical scenario explored within the manuscript substantiates the utility and practicality of the proposed system, particularly its ability to derive coherent and logical inferences from complex, multi-faceted data sets. Thus, the system is a robust, scientifically rigorous tool that can

materially aid in the resolution of complex criminal cases, thereby enhancing the integrity and effectiveness of law enforcement endeavors.

Critique and Limitations: It is worth noting that our system is not a panacea. While it does offer a streamlined and efficient approach to crime scene analysis, there are computational and ethical considerations that warrant attention. For instance, the use of machine learning algorithms may raise questions about fairness and bias, especially when training data are not fully representative.

Looking ahead, it becomes evident that the system will require continual updates and refinements to remain aligned with forensic science and data technology advances. To this end, future research efforts should be directed toward forging partnerships with government agencies. Such collaborations are invaluable for tailoring the system to law enforcement agencies' evolving and specific needs, thereby facilitating the development of a pioneering forensic ontology that can further amplify the already commendable efforts in criminal investigations.

Recommendations for Future Research: With the insights gained from the current study, future work should focus on refining the ontological structures and expanding the types of data that can be integrated. Moreover, longitudinal studies could be beneficial in further validating the system's effectiveness over time.

The Iterative Feedback Loop

Critical to the developmental process of the proposed forensic ontology was the iterative feedback loop, which encompassed a cycle of development, validation, and refinement. The loop began with a design phase where components were formulated based on previous research [59,77–80]. Upon the incorporation of these feedback insights, the prototype underwent further development.

Test results demonstrated a progressive improvement in the system's ability to integrate diverse datasets and generate meaningful insights. Moreover, the feedback loop facilitated the timely discovery and rectification of flaws, thereby enhancing the system's robustness and reliability.

By focusing on continuous improvement through iterative feedback, the design science research methodology employed ensures the evolution of a prototype that is both academically rigorous and practically effective.

8. Challenges and Practical Deployment

The development and deployment of the proposed forensic ontological system in law enforcement pose a range of practical challenges. One paramount concern is the issue of data privacy and security. Given that the system aims to integrate a wide array of data types, including potentially sensitive personal information, robust security measures such as encryption protocols and strict access controls are imperative. These measures not only ensure data privacy but also prevent unauthorized manipulation or disclosure of the integrated data.

Additionally, the challenge of interoperability and data integration looms large. To function optimally, the system needs to amalgamate data from diverse sources, which necessitates seamless integration between disparate systems. This calls for standardized data formats and protocols, and possibly the development of middleware solutions capable of translating between different data formats or structures.

Resource constraints represent another obstacle, particularly given the varying levels of technological sophistication among law enforcement agencies. The system must be designed to operate efficiently even on less powerful hardware, necessitating optimizations to reduce computational complexity or storage requirements.

Legal and ethical considerations also warrant attention. The advanced capabilities of the system, especially in crime scene analysis, could raise questions about the admissibility of generated evidence in legal settings. Hence, the design phase must consider

existing legislation and regulations, with consultations from legal experts advised to ensure compliance.

Scalability and modularity are integral design features aimed at making the system adaptable. However, these very features present challenges in practical implementation. Rigorous testing is essential to ensure that new components or software updates do not compromise the system's overall integrity.

User training and adoption are crucial for the successful deployment of the system. Comprehensive training programs, adaptable to the varied levels of technological familiarity among law enforcement agencies, should be developed to acclimatize personnel to the system's functionalities.

Lastly, the potential for future partnerships and collaborations with government agencies and academic institutions cannot be overlooked. Such alliances are instrumental for the system's ongoing development and refinement, offering additional perspectives, financial support, and technological expertise.

In summary, while the proposed system promises significant advantages for law enforcement, these advantages come with a set of complex challenges that must be judiciously addressed. Acknowledging these challenges upfront and designing the system with adaptability and scalability in mind significantly increases the likelihood of successful implementation and broader adoption.

Supplementary Materials: The following supporting information can be downloaded at https://www.mdpi.com/article/10.3390/info14110607/s1, Supplementary Materials: S1 Preliminary Forensic Ontology.

Author Contributions: Conceptualization, A.Z.S.; methodology, A.Z.S. and C.B.; software, A.Z.S.; writing—original draft preparation, A.Z.S.; writing—review and editing, A.Z.S. and G.C.M.; visualization, A.Z.S.; supervision, E.G. and V.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dong, Y.; Pan, W.D. A Survey on Compression Domain Image and Video Data Processing and Analysis Techniques. *Information* **2023**, *14*, 184. [CrossRef]
2. Hou, M.; Hu, X.; Cai, J.; Han, X.; Yuan, S. An Integrated Graph Model for Spatial–Temporal Urban Crime Prediction Based on Attention Mechanism. *ISPRS Int. J. Geo-Inf.* **2022**, *11*, 294. [CrossRef]
3. Louge, T.; Karray, M.H.; Archimède, B. Using Adaptive Logics for Expression of Context and Interoperability in DL Ontologies. *Information* **2022**, *13*, 139. [CrossRef]
4. Tchouanguem Djuedja, J.F.; Abanda, F.H.; Kamsu-Foguem, B.; Pauwels, P.; Magniont, C.; Karray, M.H. An Integrated Linked Building Data System: AEC Industry Case. *Adv. Eng. Softw.* **2021**, *152*, 102930. [CrossRef]
5. Andronie, M.; Lăzăroiu, G.; Iatagan, M.; Hurloiu, I.; Ștefănescu, R.; Dijmărescu, A.; Dijmărescu, I. Big Data Management Algorithms, Deep Learning-Based Object Detection Technologies, and Geospatial Simulation and Sensor Fusion Tools in the Internet of Robotic Things. *ISPRS Int. J. Geo-Inf.* **2023**, *12*, 35. [CrossRef]
6. Trizzino, A.; Messina, P.; Sciarra, F.M.; Zerbo, S.; Argo, A.; Scardina, G.A. Palatal Rugae as a Discriminating Factor in Determining Sex: A New Method Applicable in Forensic Odontology? *Dent. J.* **2023**, *11*, 204. [CrossRef]
7. Shahbazi, Z.; Byun, Y.-C. NLP-Based Digital Forensic Analysis for Online Social Network Based on System Security. *Int. J. Environ. Res. Public. Health* **2022**, *19*, 7027. [CrossRef] [PubMed]
8. Khatri, S.; Al-Sulbi, K.; Attaallah, A.; Ansari, M.T.J.; Agrawal, A.; Kumar, R. Enhancing Healthcare Management during COVID-19: A Patient-Centric Architectural Framework Enabled by Hyperledger Fabric Blockchain. *Information* **2023**, *14*, 425. [CrossRef]
9. Shamim, T. Forensic Odontology. *J. Coll. Physicians Surg. Pak.* **2012**, *22*, 240–245. [PubMed]
10. Senn, D.R.; Weems, R.A. *Manual of Forensic Odontology*; CRC Press: Boca Raton, FL, USA, 2013; ISBN 1-4398-5133-6.
11. Rai, B.; Kaur, J.; Rai, B.; Kaur, J. Forensic Odontology: History, Scope, and Limitations. In *Evidence-Based Forensic Dentistry*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 1–7.
12. De Nicola, A.; Vicoli, G.; Villani, M.L. Gamified Software to Support the Design of Business Innovation. *Information* **2018**, *9*, 324. [CrossRef]

13. Teixeira, A.; Azevedo, A.; Pérez-Mongiovi, D.; Caldas, I.M.; Costa-Rodrigues, J. Involving Forensic Students in Integrative Learning—A Project Proposal. *Forensic Sci.* **2023**, *3*, 69–79. [CrossRef]
14. Perdana, A.P.; Ostermann, F.O. A Citizen Science Approach for Collecting Toponyms. *ISPRS Int. J. Geo-Inf.* **2018**, *7*, 222. [CrossRef]
15. Mesejo, P.; Martos, R.; Ibáñez, Ó.; Novo, J.; Ortega, M. A Survey on Artificial Intelligence Techniques for Biomedical Image Analysis in Skeleton-Based Forensic Human Identification. *Appl. Sci.* **2020**, *10*, 4703. [CrossRef]
16. Amdouni, E.; Sarkar, A.; Jonquet, C.; Karray, M.H. IndustryPortal: A Common Repository for FAIR Ontologies in Industry 4.0. In Proceedings of the 22nd International Semantic Web Conference (ISWC)—Demo & Poster, Athens, Greece, 6–10 November 2023.
17. Dunsmore, K.P.; Devidas, M.; Linda, S.B.; Borowitz, M.J.; Winick, N.; Hunger, S.P.; Carroll, W.L.; Camitta, B.M. Pilot Study of Nelarabine in Combination with Intensive Chemotherapy in High-Risk T-Cell Acute Lymphoblastic Leukemia: A Report from the Children's Oncology Group. *J. Clin. Oncol.* **2012**, *30*, 2753–2759. [CrossRef]
18. Wangke, H. The Management of Kutai National Park through the Multi Stakeholder Partnership. In Proceedings of the 1st International Conference on Administrative Science, Policy and Governance Studies (ICAS-PGS 2017) and the 2nd International Conference on Business Administration and Policy (ICBAP 2017), Jakarta, Indonesia, 30–31 October 2017; Atlantis Press: Dordrecht, The Netherlands, 2017; pp. 343–352.
19. Korro Bañuelos, J.; Rodríguez Miranda, Á.; Valle-Melón, J.M.; Zornoza-Indart, A.; Castellano-Román, M.; Angulo-Fornos, R.; Pinto-Puerto, F.; Acosta Ibáñez, P.; Ferreira-Lopes, P. The Role of Information Management for the Sustainable Conservation of Cultural Heritage. *Sustainability* **2021**, *13*, 4325. [CrossRef]
20. Cihon, P.; Schuett, J.; Baum, S.D. Corporate Governance of Artificial Intelligence in the Public Interest. *Information* **2021**, *12*, 275. [CrossRef]
21. Klie, J.-C. INCEpTION: Interactive Machine-Assisted Annotation. *DESIRES* **2018**, 105.
22. Syme, D. *Machine Assisted Reasoning About Standard ML Using HOL*; Citeseer: University Park, PA, USA, 1992.
23. Spyropoulos, A.Z.; Bratsas, C.; Makris, G.C.; Ioannidis, E.; Tsiantos, V.; Antoniou, I. Entropy and Network Centralities as Intelligent Tools for the Investigation of Terrorist Organizations. *Entropy* **2021**, *23*, 1334. [CrossRef]
24. Resende de Mendonça, R.; Felix de Brito, D.; 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* **2020**, *11*, 154. [CrossRef]
25. Villani, M.L.; De Nicola, A.; Bouma, H.; van Rooijen, A.; Räsänen, P.; Peltola, J.; Toivonen, S.; Guarneri, M.; Stifini, C.; De Dominicis, L. A Modular Architecture of Command-and-Control Software in Multi-Sensor Systems Devoted to Public Security. *Information* **2023**, *14*, 162. [CrossRef]
26. Bouma, H.; Villani, M.L.; van Rooijen, A.; Räsänen, P.; Peltola, J.; Toivonen, S.; De Nicola, A.; Guarneri, M.; Stifini, C.; De Dominicis, L. An Integrated Fusion Engine for Early Threat Detection Demonstrated in Public-Space Trials. *Sensors* **2023**, *23*, 440. [CrossRef] [PubMed]
27. Antoniou, P.E.; Chondrokostas, E.; Bratsas, C.; Filippidis, P.-M.; Bamidis, P.D. A Medical Ontology Informed User Experience Taxonomy to Support Co-Creative Workflows for Authoring Mixed Reality Medical Education Spaces. In Proceedings of the 2021 7th International Conference of the Immersive Learning Research Network (iLRN), Eureka, CA, USA, 17 May–10 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–9.
28. Lange, C.; Ion, P.; Dimou, A.; Bratsas, C.; Sperber, W.; Kohlhase, M.; Antoniou, I. Bringing Mathematics to the Web of Data: The Case of the Mathematics Subject Classification. In Proceedings of the The Semantic Web: Research and Applications: 9th Extended Semantic Web Conference, ESWC 2012, Heraklion, Crete, Greece, 27–31 May 2012; Proceedings 9. Springer: Berlin/Heidelberg, Germany, 2012; pp. 763–777.
29. Bratsas, C.; Filippidis, P.-M.; Karampatakis, S.; Ioannidis, L. Developing a Scientific Knowledge Graph through Conceptual Linking of Academic Classifications. In Proceedings of the 2018 13th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP), Zaragoza, Spain, 6–7 September 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 113–118.
30. Kavitha, B.; Einstein, A.; Sivapathasundharam, B.; Saraswathi, T. Limitations in Forensic Odontology. *J. Forensic Dent. Sci.* **2009**, *1*, 8. [CrossRef]
31. Arbaaeen, A.; Shah, A. Ontology-Based Approach to Semantically Enhanced Question Answering for Closed Domain: A Review. *Information* **2021**, *12*, 200. [CrossRef]
32. Thompson, W.C.; Vuille, J.; Taroni, F.; Bidermann, A. After Uniqueness: The Evolution of Forensic Science Opinions. *Judicature* **2018**, *102*, 18.
33. Irons, A.; Lallie, H.S. Digital Forensics to Intelligent Forensics. *Future Internet* **2014**, *6*, 584–596. [CrossRef]
34. Górka, K.; Mazur, M. The Current Status of Forensic Anthropology in Poland-Assessment of the Discipline. *Forensic Sci.* **2021**, *1*, 102–115. [CrossRef]
35. Peterson, J.L.; Leggett, A.S. The Evolution of Forensic Science: Progress amid the Pitfalls. *Stetson Rev.* **2006**, *36*, 621.
36. Balachander, N.; Babu, N.A.; Jimson, S.; Priyadharsini, C.; Masthan, K.M.K. Evolution of Forensic Odontology: An Overview. *J. Pharm. Bioallied Sci.* **2015**, *7*, S176.
37. Bratsas, C.; Koutkias, V.; Kaimakamis, E.; Bamidis, P.D.; Pangalos, G.I.; Maglaveras, N. KnowBaSICS-M: An Ontology-Based System for Semantic Management of Medical Problems and Computerised Algorithmic Solutions. *Comput. Methods Programs Biomed.* **2007**, *88*, 39–51. [CrossRef] [PubMed]
38. Konstantinidis, S.T.; Ioannidis, L.; Spachos, D.; Bratsas, C.; Bamidis, P.D. mEducator 3.0: Combining Semantic and Social Web Approaches in Sharing and Retrieving Medical Education Resources. In Proceedings of the 2012 Seventh International Workshop

on Semantic and Social Media Adaptation and Personalization, Luxembourg, 3–4 December 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 42–47.
39. Bratsas, C.; Koutkias, V.; Kaimakamis, E.; Bamidis, P.; Maglaveras, N. Ontology-Based Vector Space Model and Fuzzy Query Expansion to Retrieve Knowledge on Medical Computational Problem Solutions. In Proceedings of the 2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Lyon, France, 22–26 August 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 3794–3797.
40. Miranda Lopez, E.; Moon, S.Y.; Park, J.H. Scenario-Based Digital Forensics Challenges in Cloud Computing. *Symmetry* **2016**, *8*, 107. [CrossRef]
41. Singh, M.; Fuenmayor, E.; Hinchy, E.P.; Qiao, Y.; Murray, N.; Devine, D. Digital Twin: Origin to Future. *Appl. Syst. Innov.* **2021**, *4*, 36. [CrossRef]
42. Li, Z.; Chen, H.; Yan, W. Exploring Spatial Distribution of Urban Park Service Areas in Shanghai Based on Travel Time Estimation: A Method Combining Multi-Source Data. *ISPRS Int. J. Geo-Inf.* **2021**, *10*, 608. [CrossRef]
43. Schriegel, S.; Kobzan, T.; Jasperneite, J. Investigation on a Distributed SDN Control Plane Architecture for Heterogeneous Time Sensitive Networks. In Proceedings of the 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), Imperia, Italy, 13–15 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–10.
44. Magro, M.J. A Review of Social Media Use in E-Government. *Adm. Sci.* **2012**, *2*, 148–161. [CrossRef]
45. Fattahi, S.; Ura, S.; Noor-E-Alam, M. Decision-Making Using Big Data Relevant to Sustainable Development Goals (SDGs). *Big Data Cogn. Comput.* **2022**, *6*, 64. [CrossRef]
46. Ping, Y.; Zhan, Y.; Lu, K.; Wang, B. Public Data Integrity Verification Scheme for Secure Cloud Storage. *Information* **2020**, *11*, 409. [CrossRef]
47. Tosca, N.J.; Agee, C.B.; Cockell, C.S.; Glavin, D.P.; Hutzler, A.; Marty, B.; McCubbin, F.M.; Regberg, A.B.; Velbel, M.A.; Kminek, G. *Time-Sensitive Aspects of Mars Sample Return (MSR) Science*; Mary Ann Liebert, Inc.: Larchmont, NY, USA, 2022; ISBN 1531-1074.
48. Iacobas, S.; Ede, N.; Iacobas, D.A. The Gene Master Regulators (GMR) Approach Provides Legitimate Targets for Personalized, Time-Sensitive Cancer Gene Therapy. *Genes* **2019**, *10*, 560. [CrossRef] [PubMed]
49. Chaves-Fraga, D.; Corcho, O.; Yedro, F.; Moreno, R.; Olías, J.; De La Azuela, A. Systematic Construction of Knowledge Graphs for Research-Performing Organizations. *Information* **2022**, *13*, 562. [CrossRef]
50. Daraio, C.; Lenzerini, M.; Leporelli, C.; Naggar, P.; Bonaccorsi, A.; Bartolucci, A. The Advantages of an Ontology-Based Data Management Approach: Openness, Interoperability and Data Quality. *Scientometrics* **2016**, *108*, 441–455. [CrossRef]
51. Chui, K.T.; Gupta, B.B.; Liu, J.; Arya, V.; Nedjah, N.; Almomani, A.; Chaurasia, P. A Survey of Internet of Things and Cyber-Physical Systems: Standards, Algorithms, Applications, Security, Challenges, and Future Directions. *Information* **2023**, *14*, 388. [CrossRef]
52. Elmhadhbi, L.; Karray, M.-H.; Archimède, B.; Otte, J.N.; Smith, B. An Ontological Approach to Enhancing Information Sharing in Disaster Response. *Information* **2021**, *12*, 432. [CrossRef]
53. Wang, W.M.; Göpfert, T.; Stark, R. Data Management in Collaborative Interdisciplinary Research Projects—Conclusions from the Digitalization of Research in Sustainable Manufacturing. *ISPRS Int. J. Geo-Inf.* **2016**, *5*, 41. [CrossRef]
54. Bratsas, C.; Bamidis, P.; Dimou, A.; Antoniou, I.; Ioannidis, L. Semantic CMS and Wikis as Platforms for Linked Learning. 2nd Int. In Proceedings of the Workshop on Learning and Education with the Web of Data (LiLe2012)–24th Int. World Wide Web Conference, Lyon, France, 17 April 2012.
55. Filippidis, P.-M.; Karampatakis, S.; Koupidis, K.; Ioannidis, L.; Bratsas, C. The Code Lists Case: Identifying and Linking the Key Parts of Fiscal Datasets. In Proceedings of the 2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP), Thessaloniki, Greece, 20–21 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 165–170.
56. Bratsas, C.; Chondrokostas, E.; Koupidis, K.; Antoniou, I. The Use of National Strategic Reference Framework Data in Knowledge Graphs and Data Mining to Identify Red Flags. *Data* **2021**, *6*, 2. [CrossRef]
57. Spyropoulos, A.Z.; Kissoudi, N.; Samalis, A.; Makris, G.C. Representation in the Semantic Web of the Structure and Functions of a Police Department in Greece. *Int. J. Eng. Sci. Invent. IJESI* **2020**, *9*, 1–6. [CrossRef]
58. Spyropoulos, A.Z.; Kornilakis, A.; Makris, G.C.; Bratsas, C.; Tsiantos, V.; Antoniou, I. Semantic Representation of the Intersection of Criminal Law & Civil Tort. *Data* **2022**, *7*, 176. [CrossRef]
59. Bratsas, C.; Quaresma, P.; Pangalos, G.; Maglaveras, N. Using Ontologies to Build a Knowledge Base of Cardiology Problems and Algorithms. In Proceedings of the Computers in Cardiology, Chicago, IL, USA, 19–22 September 2004; IEEE: Piscataway, NJ, USA, 2004; pp. 609–612.
60. Spyropoulos, A.Z.; Bratsas, C.; Makris, G.C.; Ioannidis, E.; Tsiantos, V.; Antoniou, I. Investigation of Terrorist Organizations Using Intelligent Tools: A Dynamic Network Analysis with Weighted Links. *Mathematics* **2022**, *10*, 1092. [CrossRef]
61. Montasari, R.; Carpenter, V.; Hill, R. A Road Map for Digital Forensics Research: A Novel Approach for Establishing the Design Science Research Process in Digital Forensics. *Int. J. Electron. Secur. Digit. Forensics* **2019**, *11*, 194–224. [CrossRef]
62. Alhussan, A.A.; Al-Dhaqm, A.; Yafooz, W.M.S.; Emara, A.-H.M.; Bin Abd Razak, S.; Khafaga, D.S. A Unified Forensic Model Applicable to the Database Forensics Field. *Electronics* **2022**, *11*, 1347. [CrossRef]
63. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information* **2017**, *8*, 44. [CrossRef]

64. Ding, K.; Meng, F.; Liu, Y.; Xu, N.; Chen, W. Perceptual Hashing Based Forensics Scheme for the Integrity Authentication of High Resolution Remote Sensing Image. *Information* **2018**, *9*, 229. [CrossRef]
65. Al-Dhaqm, A.; Ikuesan, R.A.; Kebande, V.R.; Razak, S.; Ghabban, F.M. Research Challenges and Opportunities in Drone Forensics Models. *Electronics* **2021**, *10*, 1519. [CrossRef]
66. Shi, X. The Semantics of Web Services: An Examination in GIScience Applications. *ISPRS Int. J. Geo-Inf.* **2013**, *2*, 888–907. [CrossRef]
67. Liu, T.; Yan, D.; Wang, R.; Yan, N.; Chen, G. Identification of Fake Stereo Audio Using SVM and CNN. *Information* **2021**, *12*, 263. [CrossRef]
68. Kalogianni, E.; Dimopoulou, E.; Quak, W.; Germann, M.; Jenni, L.; Van Oosterom, P. INTERLIS Language for Modelling Legal 3D Spaces and Physical 3D Objects by Including Formalized Implementable Constraints and Meaningful Code Lists. *ISPRS Int. J. Geo-Inf.* **2017**, *6*, 319. [CrossRef]
69. Armstrong, C.; Armstrong, H. Modeling Forensic Evidence Systems Using Design Science. In Proceedings of the Human Benefit through the Diffusion of Information Systems Design Science Research, Perth, Australia, 30 March–1 April 2010; Pries-Heje, J., Venable, J., Bunker, D., Russo, N.L., DeGross, J.I., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 282–300.
70. Spyropoulos, A.Z.; Ioannidis, E.; Antoniou, I. Interoperability and Targeted Attacks on Terrorist Organizations Using Intelligent Tools from Network Science. *Information* **2023**, *14*, 580. [CrossRef]
71. OWL—Semantic Web Standards. Available online: https://www.w3.org/OWL/ (accessed on 25 September 2023).
72. Kondylakis, H.; Nikolaos, A.; Dimitra, P.; Anastasios, K.; Emmanouel, K.; Kyriakos, K.; Iraklis, S.; Stylianos, K.; Papadakis, N. Delta: A Modular Ontology Evaluation System. *Information* **2021**, *12*, 301. [CrossRef]
73. Husáková, M.; Bureš, V. Formal Ontologies in Information Systems Development: A Systematic Review. *Information* **2020**, *11*, 66. [CrossRef]
74. Singh, S.; Karwayun, R. A Comparative Study of Inference Engines. In Proceedings of the 2010 Seventh International Conference on Information Technology, Washington, DC, USA, 12–14 April 2010; New Generations: San Jose, CA, USA; pp. 53–57.
75. Al-Thawadi, M.; Sallabi, F.; Awad, M.; Shuaib, K.; Naqvi, M.R.; Ben Elhadj, H. A-SHIP: Ontology-Based Adaptive Sustainable Healthcare Insurance Policy. *Sustainability* **2022**, *14*, 1917. [CrossRef]
76. Protégé. Available online: https://protege.stanford.edu/ (accessed on 25 September 2023).
77. Atinga, E.M. Police E-Readiness Assessment: A Case Study of Five Kenyan Police Stations. Ph.D. Thesis, University of Nairobi, Nairobi, Kenya, 2016.
78. Justice, C. *High-Priority Information Technology Needs for Law Enforcement*; Rand Corporation: Santa Monica, CA, USA, 2015.
79. Kyser, G.; Keegan, M.; Musa, S.A.; National Defense Univ Washington Dc Inst for National Strategic Studies. Applying Law Enforcement Technology to Counterinsurgency Operations. *Jt. Force Q.* **2007**, *46*, 32.
80. Hendrix, J.A.; Taniguchi, T.; Strom, K.J.; Aagaard, B.; Johnson, N. Strategic Policing Philosophy and the Acquisition of Technology: Findings from a Nationally Representative Survey of Law Enforcement. *Polic. Soc.* **2017**, *29*, 727–743. [CrossRef]
81. Pearl, J. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*; Elsevier: Amsterdam, The Netherlands, 2014; ISBN 978-0-08-051489-5.
82. Amato, F.; Castiglione, A.; Cozzolino, G.; Narducci, F. A Semantic-Based Methodology for Digital Forensics Analysis. *J. Parallel Distrib. Comput.* **2020**, *138*, 172–177. [CrossRef]
83. Li, W.; Zhou, X.; Wu, S. An Integrated Software Framework to Support Semantic Modeling and Reasoning of Spatiotemporal Change of Geographical Objects: A Use Case of Land Use and Land Cover Change Study. *ISPRS Int. J. Geo-Inf.* **2016**, *5*, 179. [CrossRef]
84. Katsumi, M.; Grüninger, M. Automated Reasoning Support for Ontology Development. In Proceedings of the Knowledge Discovery, Knowledge Engineering and Knowledge Management, Madeira, Portugal, 6–8 October 2009; Fred, A., Dietz, J.L.G., Liu, K., Filipe, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 208–225.
85. Khan, M.; Khan, M.N.A. Exploring Query Optimization Techniques in Relational Databases. *Int. J. Database Theory Appl.* **2013**, *6*, 11–20.
86. Lown, C.; Sierra, T.; Boyer, J. How Users Search the Library from a Single Search Box. *Coll. Res. Libr.* **2017**, *74*, 227–241. [CrossRef]
87. Setlur, V.; Kanyuka, A.; Srinivasan, A. Olio: A Semantic Search Interface for Data Repositories. *arXiv* **2023**, arXiv:2307.16396.
88. Stolic, P.; Milosevic, D.; Stevic, Z.; Radovanovic, I. Ontology Development for Creating Identical Software Environments to Improve Learning Outcomes in Higher Education Institutions. *Electronics* **2023**, *12*, 3057. [CrossRef]
89. Arbaaeen, A.; Shah, A. A Knowledge-Based Sense Disambiguation Method to Semantically Enhanced NL Question for Restricted Domain. *Information* **2021**, *12*, 452. [CrossRef]
90. Mancinelli, E.; Li, J.-B.; Lis, A.; Salcuni, S. Adolescents' Attachment to Parents and Reactive–Proactive Aggression: The Mediating Role of Alexithymia. *Int. J. Environ. Res. Public. Health* **2021**, *18*, 13363. [CrossRef] [PubMed]
91. Sikos, L.F. AI in Digital Forensics: Ontology Engineering for Cybercrime Investigations. *WIREs Forensic Sci.* **2021**, *3*, e1394. [CrossRef]
92. Gamallo, P.; Garcia, M. Editorial for the Special Issue on "Natural Language Processing and Text Mining". *Information* **2019**, *10*, 279. [CrossRef]
93. Claro, D.B.; Souza, M.; Castellã Xavier, C.; Oliveira, L. Multilingual Open Information Extraction: Challenges and Opportunities. *Information* **2019**, *10*, 228. [CrossRef]

94. Dosis, S.; Homem, I.; Popov, O. Semantic Representation and Integration of Digital Evidence. *Procedia Comput. Sci.* **2013**, *22*, 1266–1275. [CrossRef]
95. Bhandari, S.; Jusas, V. An Ontology Based on the Timeline of Log2timeline and Psort Using Abstraction Approach in Digital Forensics. *Symmetry* **2020**, *12*, 642. [CrossRef]
96. Wu, Y.; Wang, X.; Zhang, T. Crime Scene Shoeprint Retrieval Using Hybrid Features and Neighboring Images. *Information* **2019**, *10*, 45. [CrossRef]
97. Chang, L.; Lin, F.; Shi, Z. A Dynamic Description Logic for Representation and Reasoning About Actions. In Proceedings of the Knowledge Science, Engineering and Management, Melbourne, Australia, 28–30 November 2007; Zhang, Z., Siekmann, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; pp. 115–127.
98. Astarita, V.; Giofrè, V.P.; Mirabelli, G.; Solina, V. A Review of Blockchain-Based Systems in Transportation. *Information* **2020**, *11*, 21. [CrossRef]
99. Galici, R.; Ordile, L.; Marchesi, M.; Pinna, A.; Tonelli, R. Applying the ETL Process to Blockchain Data. Prospect and Findings. *Information* **2020**, *11*, 204. [CrossRef]
100. Meyer, J.-J.C. Dynamic Logic for Reasoning About Actions and Agents. In *Logic-Based Artificial Intelligence*; Minker, J., Ed.; The Springer International Series in Engineering and Computer Science; Springer US: Boston, MA, USA, 2000; pp. 281–311, ISBN 978-1-4615-1567-8.
101. Cai, S.; Goh, M.; de Souza, R.; Li, G. Knowledge Sharing in Collaborative Supply Chains: Twin Effects of Trust and Power. *Int. J. Prod. Res.* **2013**, *51*, 2060–2076. [CrossRef]
102. Carter, J.G.; Grommon, E. Officer Perceptions of the Impact of Mobile Broadband Technology on Police Operations. *Polic. Soc.* **2017**, *27*, 847–864. [CrossRef]
103. Zhao, C.; Heilili, N.; Liu, S.; Lin, Z. Representation and Reasoning on RBAC: A Description Logic Approach. In Proceedings of the Theoretical Aspects of Computing–ICTAC, Hanoi, Vietnam, 17–21 October 2005; Van Hung, D., Wirsing, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; pp. 381–393.
104. Segerberg, A.; Bennett, W.L. Social Media and the Organization of Collective Action: Using Twitter to Explore the Ecologies of Two Climate Change Protests. *Commun. Rev.* **2011**, *14*, 197–215. [CrossRef]
105. Munkhondya, H.; Ikuesan, A.R.; Venter, H.S. A Case for a Dynamic Approach to Digital Forensic Readiness in an SDN Platform. In Proceedings of the International Conference on Cyber Warfare and Security, Norfolk, VA, USA, 12–13 March 2020; Academic Conferences International Limited: Reading, UK, 2020; p. 584-XVIII.
106. Stadlinger, J.; Dewald, A. A Forensic Email Analysis Tool Using Dynamic Visualization. *J. Digit. Forensics, Secur. Law* **2017**, *12*, 6. [CrossRef]
107. Esheiba, L.; Elgammal, A.; Helal, I.M.A.; El-Sharkawi, M.E. A Hybrid Knowledge-Based Recommender for Product-Service Systems Mass Customization. *Information* **2021**, *12*, 296. [CrossRef]
108. Cao, L.; Zhao, Y.; Zhang, H.; Luo, D.; Zhang, C.; Park, E.K. Flexible Frameworks for Actionable Knowledge Discovery. *IEEE Trans. Knowl. Data Eng.* **2010**, *22*, 1299–1312. [CrossRef]
109. Ronzhin, S.; Folmer, E.; Maria, P.; Brattinga, M.; Beek, W.; Lemmens, R.; van't Veer, R. Kadaster Knowledge Graph: Beyond the Fifth Star of Open Data. *Information* **2019**, *10*, 310. [CrossRef]
110. Bernasconi, E.; Ceriani, M.; Di Pierro, D.; Ferilli, S.; Redavid, D. Linked Data Interfaces: A Survey. *Information* **2023**, *14*, 483. [CrossRef]
111. Wolff, J.G. The SP Theory of Intelligence: Benefits and Applications. *Information* **2014**, *5*, 1–27. [CrossRef]
112. Agosto, E.; Ajmar, A.; Boccardo, P.; Giulio Tonolo, F.; Lingua, A. Crime Scene Reconstruction Using a Fully Geomatic Approach. *Sensors* **2008**, *8*, 6280–6302. [CrossRef]
113. Wu, Y.; Dong, X.; Shi, G.; Zhang, X.; Chen, C. Crime Scene Shoeprint Image Retrieval: A Review. *Electronics* **2022**, *11*, 2487. [CrossRef]
114. Silega, N.; Varén, E.; Varén, A.; Rogozov, Y.I.; Lapshin, V.S.; Alekseevich, S.A. Exploiting an Ontological Model to Study COVID-19 Contagion Chains in Sustainable Smart Cities. *Information* **2022**, *13*, 40. [CrossRef]
115. Megaw, E.D. Factors Affecting Visual Inspection Accuracy. *Appl. Ergon.* **1979**, *10*, 27–32. [CrossRef]
116. Cuesta, Á.; Barrero, D.F.; R-Moreno, M.D. A Descriptive Analysis of Twitter Activity in Spanish around Boston Terror Attacks. In Proceedings of the Computational Collective Intelligence. Technologies and Applications: 5th International Conference, ICCCI 2013, Craiova, Romania, 11–13 September 2013; Proceedings 5. Springer: Berlin/Heidelberg, Germany, 2013; pp. 631–640.
117. Greenberg, J.; Garoufallou, E. Change and a Future for Metadata. In Proceedings of the Metadata and Semantics Research, Thessaloniki, Greece, 19–22 November 2013; Garoufallou, E., Greenberg, J., Eds.; Springer International Publishing: Cham, Switzerland, 2013; pp. 1–5.
118. Belkin, N.J. Cognitive Models and Information Transfer. *Soc. Sci. Inf. Stud.* **1984**, *4*, 111–129. [CrossRef]
119. Wang, Y.; Jiang, T.; Liu, J.; Li, X.; Liang, C. Hierarchical Instance Recognition of Individual Roadside Trees in Environmentally Complex Urban Areas from UAV Laser Scanning Point Clouds. *ISPRS Int. J. Geo-Inf.* **2020**, *9*, 595. [CrossRef]
120. Noy, N.; Crubezy, M.; Fergerson, R.; Knublauch, H.; Tu, S.; Vendetti, J.; Musen, M. Protégé-2000: An Open-Source Ontology-Development and Knowledge-Acquisition Environment. *AMIA Annu. Symp. Proc.* **2003**, *2003*, 953. [PubMed]

121. Tudorache, T.; Noy, N.F.; Tu, S.; Musen, M.A. Supporting Collaborative Ontology Development in Protégé. In Proceedings of the The Semantic Web—ISWC, Karlsruhe, Germany, 26–30 October 2008; Sheth, A., Staab, S., Dean, M., Paolucci, M., Maynard, D., Finin, T., Thirunarayan, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 17–32.
122. Schekotihin, K.; Rodler, P.; Schmid, W.; Horridge, M.; Tudorache, T. *Test-Driven Ontology Development in Protégé*; ICBO: Paris, France, 2018.
123. Qiu, D.; Jiang, H.; Chen, S. Fuzzy Information Retrieval Based on Continuous Bag-of-Words Model. *Symmetry* **2020**, *12*, 225. [CrossRef]
124. Hjørland, B. Information Retrieval and Knowledge Organization: A Perspective from the Philosophy of Science. *Information* **2021**, *12*, 135. [CrossRef]
125. Nuninger, L.; Verhagen, P.; Libourel, T.; Opitz, R.; Rodier, X.; Laplaige, C.; Fruchart, C.; Leturcq, S.; Levoguer, N. Linking Theories, Past Practices, and Archaeological Remains of Movement through Ontological Reasoning. *Information* **2020**, *11*, 338. [CrossRef]
126. Möller, R.; Neumann, B. Ontology-Based Reasoning Techniques for Multimedia Interpretation and Retrieval. In *Semantic Multimedia and Ontologies: Theory and Applications*; Kompatsiaris, Y., Hobson, P., Eds.; Springer: London, UK, 2008; pp. 55–98. ISBN 978-1-84800-076-6.
127. Suntisrivaraporn, B. *Polynomial-Time Reasoning Support for Design and Maintenance of Large-Scale Biomedical Ontologies*; Dresden University of Technology: Dresden, Germany, 2023.
128. Wagenpfeil, S.; Mc Kevitt, P.; Hemmje, M. Towards Automated Semantic Explainability of Multimedia Feature Graphs. *Information* **2021**, *12*, 502. [CrossRef]
129. Saad, S.; Traore, I. Method Ontology for Intelligent Network Forensics Analysis. In Proceedings of the 2010 Eighth International Conference on Privacy, Security and Trust, Ottawa, ON, Canada, 17–19 August 2010; pp. 7–14.
130. Bakillah, M.; Liang, S.H.L.; Zipf, A.; Arsanjani, J.J. Semantic Interoperability of Sensor Data with Volunteered Geographic Information: A Unified Model. *ISPRS Int. J. Geo-Inf.* **2013**, *2*, 766–796. [CrossRef]
131. Hoss, A.M.; Carver, D.L. Weaving Ontologies to Support Digital Forensic Analysis. In Proceedings of the 2009 IEEE International Conference on Intelligence and Security Informatics, Richardson, TX, USA, 8–11 June 2009; pp. 203–205.
132. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. An Advanced Abnormal Behavior Detection Engine Embedding Autoencoders for the Investigation of Financial Transactions. *Information* **2021**, *12*, 34. [CrossRef]
133. Alruwaili, F.F. CustodyBlock: A Distributed Chain of Custody Evidence Framework. *Information* **2021**, *12*, 88. [CrossRef]
134. Karagiannis, C.; Vergidis, K. Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information* **2021**, *12*, 181. [CrossRef]
135. Ahmed, S.; Gentili, M.; Sierra-Sosa, D.; Elmaghraby, A.S. Multi-Layer Data Integration Technique for Combining Heterogeneous Crime Data. *Inf. Process. Manag.* **2022**, *59*, 102879. [CrossRef]
136. Prakken, H.; Sartor, G. Law and Logic: A Review from an Argumentation Perspective. *Artif. Intell.* **2015**, *227*, 214–245. [CrossRef]
137. Zhang, H.; Zhang, Z.; Zhou, L.; Wu, S. Case-Based Reasoning for Hidden Property Analysis of Judgment Debtors. *Mathematics* **2021**, *9*, 1559. [CrossRef]
138. Van Engers, T.; Boer, A.; Breuker, J.; Valente, A.; Winkels, R. Ontologies in the Legal Domain. In *Digital Government: E-Government Research, Case Studies, and Implementation*; Chen, H., Brandt, L., Gregg, V., Traunmüller, R., Dawes, S., Hovy, E., Macintosh, A., Larson, C.A., Eds.; Integrated Series in Information Systems; Springer: Boston, MA, USA, 2008; pp. 233–261, ISBN 978-0-387-71611-4.
139. Method Ontology for Intelligent Network Forensics Analysis. Available online: https://ieeexplore.ieee.org/abstract/document/5593235/?casa_token=IulCK1eicu4AAAAA:hIP7LoXx7f7TTGLikzePubwzGE3MSjWFMkKuyaUbuGbX5_kXeaiT4yeFYA-Cn1ML-h-9Yjk (accessed on 25 September 2023).