M. Meier, D. Reinhardt, S. Wendzel (Hrsg.): Sicherheit 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 55

A Semantic Framework for a better Understanding, Investigation and Prevention of Organized Financial Crime

Ronny Merkel[1], Christian Krätzer[1], Mario Hildebrandt[1],
Stefan Kiltz[1], Sven Kuhlmann[1], Jana Dittmann[1]

Abstract: Using semantic technology for data storage and exploration is an important issue in computer science, however barely applied to forensic investigations. In this paper, a conceptual framework is proposed for the detailed modeling of structured domain knowledge in the field of organized financial crime, with a special focus on sparse information (e.g. flows of money, data and know-how, exploited vulnerabilities and attackers motivation) and the proposition of a credibility measure (to rate the reliability of used information based on open source intelligence, expert surveys and captive interviews). In addition to the ontology-based, abstract domain knowledge model, the proposed framework consists of an explorative information discovery functionality, which can couple concrete, case-related data from different knowledge bases with the abstract domain knowledge, to assist experts in the investigation of crimes and the discovery of new relations between different pieces of evidence. The proposed framework is illustrated using the exemplary use case scenario of Point-of-Sale (POS) Skimming. Furthermore, its flexibility, scalability and a potential integration into current and emerging police standards is discussed.

Keywords: semantic modeling, organized financial crime, ontology, sparse information, credibility measure, explorative search

1 Introduction

Using semantic technologies is an important issue in computer science. Originating in linguistics and the philosophy of language, the modeling of meaning (semantics) is related to how we think (process information) and talk (express information), which can also be applied to digital data. With the idea of modeling semantics in the Web, Tim Berners-Lee has initiated a decade of research into this topic, utilizing semantic models for an increased accuracy, speed and flexibility of data processing [BHL01]. Exemplary use cases for semantic models include the fusion of information from different data storages, the extraction and structuring of information from unstructured data as well as the presentation of structured data for human processing, e.g. for an exploratory search.

In the scope of this paper, semantic technology is discussed from a forensic perspective. The idea of using semantics for forensic casework is not new and has been proposed in

[1] Workgroup on Multimedia & Security, Otto-von-Guericke University of Magdeburg, Universitaetsplatz 2, 39106 Magdeburg, {merkel, kraetzer, hildebrandt, kuhlmann, kiltz, dittmann}@ovgu.de

The work in this paper has been funded in part by the German Federal Ministry of Education and Research (BMBF), funding code 13N13473.

literature as well as in proprietary software tools. However, when looking at specific casework examples, it seems that these technologies are barely used in daily police work. The aim of this paper is therefore to propose a conceptual framework for modeling semantic information in the forensic context, exemplary illustrated using an organized financial crime use case. In particular, the contribution of this paper is as follows:

- A conceptual framework is proposed for modeling and usage of semantic information in forensic investigations, based on the exemplary field of organized financial crimes. The model includes a manually created ontology (representing structured, abstract domain knowledge), case-specific information (e.g. from concrete knowledge bases) and intermediate interfaces usable by forensic experts for abstract information modeling and explorative information discovery (views).

- When designing the framework, a specific focus is laid on three major issues. During the ontology creation, a specific focus is on the modeling of sparse information (e.g. money, data and know-how flows, vulnerabilities and motivation). A source-dependent credibility measure is proposed to assure the quality of the model (based on open source intelligence, expert surveys and captive interviews). Also, a forensic investigators view is designed to allow for explorative information discovery.

- The practical application of the scheme is illustrated using the example of Point-of-Sale (POS) Skimming from the domain of organized financial crimes. The procedure is demonstrated showing exemplary aspects of the ontology modeling, the explorative search of forensic experts as well as the knowledge base updating.

- Flexibility and scalability as well as a potential integration into contemporary police data exchange standards (such as FIDEX [Lot10] and XPolizei [Haa11]) are suggested and discussed, to provide easy extensibility of the framework.

The authors acknowledge the nature of this paper as work in progress. However, an early inclusion of the scientific community is regarded as a vital prerequisite to assure good scientific practice, especially in respect to the Daubert criteria for acceptability in court, such as scientific peer review, general acceptance and error rates [Dau13]. The remainder of this paper is structured as follows: section 2 gives a brief overview over relevant state of the art, followed by an introduction of the proposed framework in section 3. The three issues of major focus are discusses in section 4, section 5 illustrates the framework for a POS Skimming use case. Flexibility, scalability and integration into police standards are discussed in section 6. Future research is highlighted in section 7.

2 State of the Art

On a syntactical level, **taxonomies** can be considered as a form of hierarchical categorization of certain domain knowledge, often visualized in the form of a tree, e.g. for content management or information retrieval [Pfu12]. However, to also model complex

relations between different entities, computer scientists have adapted the concept of **ontologies** from Philosophy (the study of being and the existence of entities as well as their conditions and principles) [GI02]. Ontologies are used as a formal means of modeling semantic information of a certain knowledge domain in a structured and standardized way for computer communication, automatic inference, data representation and mining [GI02]. Today, semantic technologies are subject to broad research activities and a wide range of applications. The numerous protocols are summarized under the semantic web stack [W3C15].

In **forensic investigations**, machine-learning techniques are applied for detecting crime pattern, e.g. in [WRW+13]. Semantic models seem to be used in very selective cases only. Early semantic models were applied to synthesize alibis, e.g. by analyzing texts [Nis12]. A few examples of more recent approaches include proprietary software for police investigations (e.g. [Tex15] for semantic text mining, [Jac12] for searching structured and unstructured data as well as [Mar15] for tagging, searching and data integration). However, these are proprietary approaches and no information is openly available about their specific concepts, realization and performance. The possibilities of semantic technologies for police work and forensic investigations are partly discussed in [Liu12] and [HWS15]. A more comprehensive approach using semantic modeling with the help of an ontology is proposed in [ASB+14], based on structured and unstructured data from different police databases and freely available texts for the recognition of crime threats. It is regarded here as the first proposal for a practical realization of semantic approaches for forensic casework, allowing for data search, linking, exploration, modeling and visualization. However, the work is introduced on a very abstract level and only few specific details on the modeled components are given, e.g. the concrete entities of the underlying ontology. Especially the reliability of the (often automatically) extracted entities is unclear in the approach, which is described from a rather top level view. In comparison, the **here presented work** starts from a specific application scenario, especially focusing on sparse information and a credibility measure to assure the relevance and reliability of the extracted information. Scalability, flexibility and integration issues of the scheme are then discussed, making it a bottom up approach.

3 A Conceptual Framework for Semantic Information in Forensics

In forensic investigations, information is usually provided on different levels of abstractness: case-related information is usually concrete, such as the time and place of the crime, the damage caused or the number of people involved. Abstract information includes the experience of the forensic expert, such as typical modi operandi, places where traces can typically be found or common procedures of investigation. The expert has to combine these different levels to gain information. Using semantic modeling, the storage and processing of data from these different levels of abstractness can be facilitated through digital means, assisting the forensic expert in the investigation (Fig. 1). On the **abstract knowledge layer**, the overall experience of the forensic expert might be ex-

tended by information obtained from convicted criminals and open source intelligence and can be stored in the form of an ontology (left image). Such *ontology* (right image) contains no specific instances and represents the abstract domain knowledge of the application scenario, structured in a machine-readable form. It includes a hierarchical class structure with classes (e.g. 'attacker', 'vulnerability', 'attacking tool' or 'defense mechanism'), subclasses (e.g. 'human-based', 'technical' or 'organizational' 'vulnerabilities'), class attributes (e.g. 'credibility measure' providing reliability information, 'affected security aspects' like confidentiality / integrity or 'error rates' of an investigation method) and relations between different classes (e.g. a certain 'attacker' might use a certain 'attack tool', an 'attack' might exploit a certain 'vulnerability'). Two different types of ontologies are proposed in this work: a general *crime field ontology* to represent general domain knowledge as well as *additional ontologies*, representing sub-field specific knowledge to be integrated (e.g. knowledge about forensic traces found at a crime scene, like fingerprints or toolmarks). Additional ontologies can be integrated into the crime field ontology using hooks (e.g. a class 'trace' might be hooked up with an additional ontology 'fingerprints', which holds the domain knowledge of forensic fingerprint investigations). All ontologies are controlled using an *ontology manager* (*additional ontology manager* respectively). Such manager consists of a *user level* taking *request parameters* (e.g. creation / deletion of an ontology, reading global or local contexts represented by the relational neighborhood of a class, appending, renaming, deleting or moving of classes, change of attributes or relations). A requested operation is checked at the *system level* concerning its validity and then converted to appropriate read, write or delete commands, which are then applied to the specific ontology. Request parameters for reading, writing and deleting can be issued by the *ontology designer view*, used for manual update of the ontology (only option of gaining write access to the semantic domain model). Because the relationships between different entities of the ontology can be very complex and small changes might lead to a significant amount of remodeling of dependent relations (and might require updates of the database structure of the concrete knowledge layer), only an expert is allowed to manually perform this task.

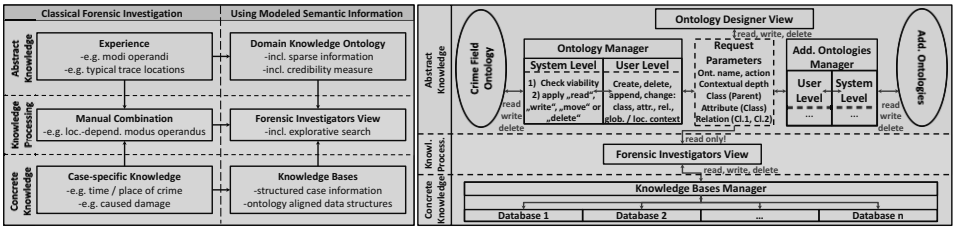

Fig. 1: Forensic abstraction layers: abstract knowledge (blue), knowledge processing (grey), concrete knowledge (green). Left: forensic investigations without and with the help of the proposed semantic modeling framework. Right: proposed interface structure.

On the **knowledge processing layer**, the *forensic investigators view* provides the main semantic functionality required for assisting the forensic expert in the investigation (left image). The investigator selects a relevant entity to explore (class of the crime field

ontology from a presented list view) as well as a contextual depth, which form the request parameters sent to the ontology managers of the respective ontologies. Only reading access is allowed to ensure the consistence of the abstract knowledge relations. The local (or global) context received by the forensic investigators view is forwarded to the *knowledge bases manager* in the form of a sub-ontology, where it is filled with all specific instances available in the *databases* for the classes provided and returned to the forensic investigators view (right image). Here it is displayed, showing the network of relations between the entities of the selected neighborhood as well as the associated instances (see also section 5). Thus, the investigator can explore important relations (e.g. which 'attack tool' has been used by a certain 'attacker'), potentially additional relations (e.g. other 'crimes' committed by the 'attacker') as well as all similar cases (e.g. all 'crimes' in which a certain 'attack tool' was used). Furthermore, the forensic expert can input new case-related information (specific instances of the selected local context), which can be directly stored in the corresponding databases of the knowledge bases manager. The forensic investigators view is depicted for a specific use case in section 5.

On the **concrete knowledge layer**, case-specific knowledge is usually available in the form of digital or physical files and folders in an unstructured form or in structured databases (left image). To allow for a reliable processing of this information, the *knowledge bases manager* needs to structure and store this data in respective databases (right image). Data might be structured automatically using certain data mining techniques (e.g. text mining). In the here presented scheme, a manual structuring of data is proposed for higher reliability. Data might furthermore be structured in two possible ways. In a **first general data structuring effort**, the global context of a complete ontology might be requested from the *ontology manager* of the *abstract knowledge level*. This is a read only access, but provides all class entities of an ontology. Based on these entities, database schema can be arranged in a way to store data using structures similar to the ontology, e.g. similarly named database keys. Specific case-related datasets then need to be manually entered by forensic experts according to the provided keys. In case of changes applied to the ontology via the *ontology designer view*, which have lead to structural changes in the data already stored in the database, database restructuring rules might have to be manually defined. In a **second general data structuring effort**, additional case information might be entered by the forensic expert during case analysis, using the *forensic investigators view*, which is sent to the knowledge bases manager and stored in respect to the corresponding database keys.

4 Sparse Information, Credibility & Explorative Search

In the scope of this paper, a special focus lies on the relevance and reliability of the designed ontology, to maximize the benefit for forensic investigations. To realize this goal, three main aspects are particularly considered. **Sparse information** is often not present to forensic investigators and therefore not included in the investigation. For example, the *flow of money* after a successful crime is often not known and even if a person is con-

victed, the whereabouts of the money are often undiscovered. If typical hideouts or techniques of money laundering can be acquired from additional sources (e.g. by interviewing convicts in prisons), this information might be useful to look for signs of specific hiding or laundering techniques. Therefore, sparse information is of great importance to the issue. In the scope of this paper, five specific types of sparse information are proposed (and first findings included in the ontology of the exemplary use case introduced in section 5). The *flow of money* describes typical money storing, laundering and spending behavior, which might help forensic investigators to direct their attention towards related activities. The *flow of (stolen) data* reflects on how criminals communicate, trust levels within an organization as well as techniques to convert stolen data into money. Such information seems vital for solving crimes. The *flow of know-how* indicates ways in which knowledge is acquired (e.g. from educational institutions, the internet or insider knowledge). Identifying sources of knowledge might help forensic investigations to narrow down the set of suspects in certain cases and seems very helpful for preventive applications. *Commonly exploited vulnerabilities* explicate preferably targeted weaknesses (e.g. organizational, human or technical). Such knowledge can be used especially in preventive work, but also to direct investigations. The *motivation of an attacker* illustrates reasons why criminal actions are conducted (e.g. personal gain, blackmail), which might be extracted successfully from captive interviews, providing valuable information towards the prevention of future crimes. To include such information into the modeling process, the combination of open source intelligence, expert knowledge and captive interviews seems very promising.

To measure the reliability of modeled semantic information, a **credibility measure** is proposed. The measure is stored in the form of ontology attributes (section 3), which are saved as a three-tuple for each class of the complete ontology:

$$\text{Credibility measure: } C(\text{OSINT},\text{ES},\text{CI}) \quad \{\text{OSINT}, \text{ES}, \text{CI}\} \in \mathbb{N}, 0 \leq \{\text{OSINT}, \text{ES}, \text{CI}\} \tag{1}$$

The tuple of formula (1) contains the amount of (independent) *open source intelligence sources* (OSINT), *surveyed experts* (ES) and *captives interviewed* (CI). Sources are considered independent if they are from different online sources, experts of different forensic departments or captives from different jails. It is acknowledged that such classification as well as the information provided by a human is subjective in a particular way. Objectivity is therefore aimed at by regarding only these entities as credible, which are acquired by a certain amount of different individuals, preferably from different origins (e.g. forensic experts vs. captives). An interesting aspect of future research can be seen in answering the question of how to deal with conflicting or opposing information from different sources. These cases should also be incorporated in a comprehensive credibility measure in the future.

An **explorative search view** is proposed as a main feature of the framework. Criminal investigators require the structured visualization of relevant entities and their relations and at the same time a reduction of irrelevant information. With keyword-based search engines, this goal seems not achievable. Displaying manual selected objects of interest and a flexible visualization of their affiliated objects, relations and available concrete

instances in varying depths seems a potential approach towards this challenge. Furthermore, the investigator has the option of storing additional case-related information during his analysis, which will be automatically saved by the knowledge bases manager. At the same time, the investigator is protected from accidental changes of the domain knowledge, because the ontology itself is write-protected.

5 Exemplary Use Case: Modeling Point-of-Sale (POS) Skimming

Point-of-Sale (POS) skimming is a well-suited example to visualize the different modeling steps of the proposed scheme. During such offense, a criminal gains access to a POS terminal (e.g. in a supermarket without cameras) at night, installs a hidden skimmer and escapes undetected. During normal operations of the supermarket, the magnetic stripe of credit or debit cards of customers is captured automatically by the skimmer, encrypted and sent to the criminals. The datasets are then decrypted by the technician of the criminal organization and stored onto fake cards used for shopping or funds withdrawal.

To **model the semantic domain knowledge** of such incident, several classes might be defined. For example, a 'criminal organization' might consist of different 'attackers', performing a certain 'offense' (e.g. POS skimming). They use specific 'attack tools' (e.g. skimmer), which exploit certain 'vulnerabilities' (in this case a lack of cameras in the supermarket or insufficient access restriction measures). The customers can be considered as 'attack target' and the attack causes a certain 'data flow' (stolen credit card data) and 'money flow' (stolen money). Earlier, a 'know-how flow' had taken place, transferring the crime-relevant knowledge to the criminal organization (e.g. from social engineering, or open source knowledge from universities or the internet). At some point, there might be a 'crime discovery' (e.g. reports of unauthorized withdrawals of funds). Forensic 'investigators' start applying 'investigative procedures' (e.g. tracing card data back to the supermarket, checking the POS terminals, etc.). The investigations can lead to certain 'consequences' (e.g. replacement of terminals, arrest of identified criminals) or additional 'defense mechanisms' (e.g. improved tamper protection of POS terminals, cameras inside the supermarket, better access restriction). For each of these classes, numerous subclasses might be modeled. For example, a 'money flow' might be further divided into the 'type of money' involved, its 'sender' and 'receiver' as well as the 'type of transfer'. In case of POS skimming, a 'money flow' might refer to type 'cash', transferred between a 'victim' and a 'criminal' via 'withdrawal'. A small section of the class structure is exemplary visualized in Fig. 2 (left) using the modeling language OWL2 [OWL12] and the open source toolkit NeOn [NeO14] (which can be considered as the ontology designer view in this example). Considering the credibility measure designed in section 4, each class of the hierarchy can only be considered as credible if a certain amount of sources specified in the *C(OSINT,ES,CI)* attribute of the class confirms its relevance for practical investigations. In Fig. 2 (left), the exemplary chosen transfer type of 'withdrawal' was reported by several websites, two of which are included here for illustration purposes [Gae13], [Kel15]. Furthermore, police authorities from two different countries

have confirmed in personal interviews the withdrawal of money using fake copies of skimmed credit or debit cards. The resulting credibility measure *C* would therefore take the form *C(2,2,0)*. The captive interviews are currently ongoing and are planned to further consolidate this credibility by increasing also the *CI* value of the tuple. Apart from modeling the hierarchical structure, the ontology also consists of several relations between the class entities. For example, a criminal organization 'consists' of attackers, which 'conduct' an offense, 'working with' a certain attack tool. Exemplary relations of the use case are visualized in Fig. 2 (right).

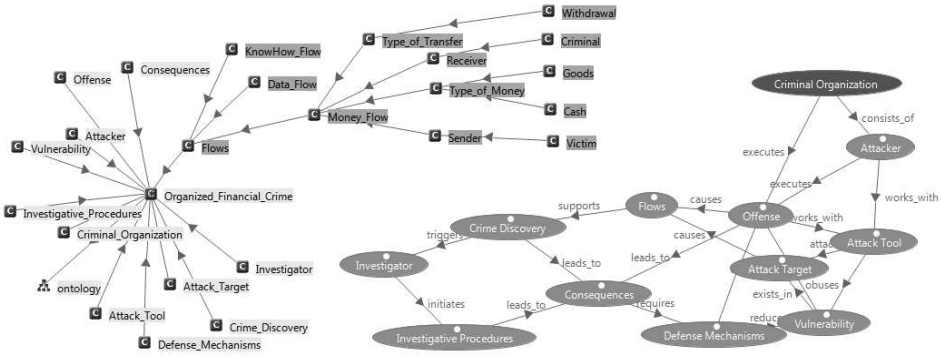

Fig. 2: Exemplary class hierarchy section for POS skimming (left) using the ontology designer view (here: NeOn toolkit [NeO14]). Exemplary visualization of selected relations (right).

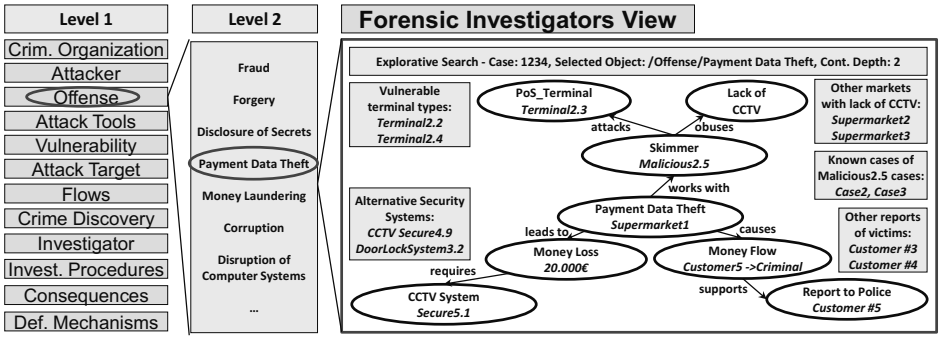

Fig. 3: Conceptual design of the forensic investigators view (POS skimming). Left: hierarchical ontology class structure from which investigated entity is chosen. Right: explorative search view.

To conduct an **explorative search** for the POS skimming scenario, the abstract ontology model is combined with concrete case information in the forensic investigators view, to assist the information extraction by an expert (Fig. 3). For that task, the class to be investigated is chosen from the hierarchical structure of the ontology (left part). In the given example, the type of 'offense' called 'Payment Data Theft' is investigated, which is located at the second hierarchy level of the ontology. The explorative investigation of the chosen class is conducted in the explorative search view (right part). A contextual dept of two is used, meaning that the neighborhood of two nodes from the 'Payment Data

Theft' is investigated in the scope of case '1234'. In this case, payment data has been stolen from 'Supermarket1'. The chosen neighborhood is sent to the knowledge base and the corresponding information of all available relevant cases is attached to the ontology classes in the form of instances. The expert can now explore these cases using the forensic investigators view. For example, he can analyze the specific skimming device applied ('Malicious2.5') and browse other cases in which the device has also been used. He could furthermore expose the terminals being (apart from 'Terminal2.3') also vulnerable to such attack (e.g. 'Terminal2.2', 'Terminal2.4') as well as supermarkets also lacking sufficient security mechanisms (e.g. 'Supermarket2', ' Supermarket3'). Regarding money loss, the expert could enquire alternative security systems to prevent this kind of attack in the future (e.g. 'CCTV Secure4.9', 'DoorLockSystem3.2') or browse other victims (e.g. 'Customer #3', 'Customer #4') for additional evidence. The view provides the information present in the knowledge base in a highly structured (semantical) way and includes only reliable (using the credibility measure) information, complemented by sparse information. It therefore exhibits the potential for a very comprehensive and resource-effective way of exploring a case and linking it to related information of other cases.

Within the different databases managed by the **knowledge bases manager**, the concrete case information of the POS skimming scenario is stored in a structured way. This means that the data is sorted according to the classes provided by the ontology. For investigating specific cases, the ontology should therefore be fixed and no changes should be applied to its structure. However, case-specific information can easily be added to the databases using the forensic investigators view. For example, if an expert has discovered that a currently analyzed skimmer is similar to 'Malicious2.5', the novel data stemming from this case (e.g. additional attacked terminals or exploited vulnerabilities) can be manually assigned to the forensic investigators view and will automatically be written to the appropriate databases by the knowledge bases manager. In case new semantic categories (ontology classes) need to be designed (e.g. as a consequence of changed modi operandi), the ontology has to be changed by an expert using the ontology designer view. If these changes create new classes, rules have to be provided for the knowledge bases manager to rearrange corresponding database keys and to map the stored entries accordingly.

A **practical validation** of the proposed scheme using large amounts of modeled entities and relations, also including specific measures of the scheme's contribution to the crime pattern extraction efforts of forensic practitioners in the field cannot be included into this paper, but remains an important issue for future work.

6 Flexibility, Scalability and Integration into Police Standards

In police work the investigation of organized crime requires a constant exchange of information across borders. This, however, is often impeded by the utilization of a multitude of commercial and incompatible software products and data formats in daily police

work. Thus, in many countries the predominant form of data exchange is via hardcopies. Especially in the context of organized crime this is slowing down case work due to the lack of a proper way of searching the documents or the possibility of applying data mining technologies to find similar patterns within the course of events. Hence, in various countries initiatives for standardized data exchange formats exist. Two examples are FIDEX [Lot10] which is relying on the National Information Exchange Model (NIEM [Nie15]) in the US and XPolizei [Haa11] as a XÖV standard in Germany. Especially regarding XPolizei, only a limited amount of information is publicly available. The XÖV standard defines process models, messages, semantic data type and code lists [BBH+13]. In contrast to that, NIEM primarily focuses on data exchange formats in the Information Exchange Package Documentation (IEPD) and a data model representing a dictionary of terms, definitions, formats and relationships [Nie15]. Thus, it primarily covers the messages and the semantic data types of the XÖV standard. The specific implementation of FIDEX defines two IEPDs: forensic case submission for the communication between forensic labs and police agencies and disposition reporting for communication with the court. Both approaches share XML as the used modeling language.

Toward the flexibility, scalability and integration into those standards no particular challenges arise since both formats specify how data should be transferred. The ontology itself can be easily integrated into the exchanged data because it utilizes XML data structures as well. However, with a growing amount of information within the ontology this might lead to an increased overhead of redundantly transmitted data. Thus, for the sake of scalability, very detailed knowledge can be outsourced into the additional ontologies (Fig. 1). It is furthermore reasonable to integrate versioning information within the ontology and to create an exchange policy for updated versions. This would only require including the version and specific items into the data exchange for a single case. With the matching ontology, the implications and relations between the items can be decoded locally. With respect to NIEM, this would also require two IEPDs, one for exchanging updated versions of the ontology (e.g. push or pull scenarios) and the exchange of the specific case work, which could be also integrated into the FIDEX Forensic Case Submission IEPD. In XÖV, different semantic data types can be defined for the exchange of ontologies. However, both approaches are limited to a national application because no global data exchange standards exist, yet. This is the primary requirement for implementing a flexible and efficient solution for a multi-national investigation of organized crime. Besides particular data standards, the compatibility of the legal requirements including data protection laws need to be considered.

7 Conclusion and Future Work

In this paper, a conceptual framework has been proposed to model structured domain knowledge from the field of organized financial crime using semantic technology, also including sparse information and a credibility measure based on open source intelligence, expert surveys and captive interviews. The framework has furthermore been ex-

tended by an explorative information discovery functionality, linking the modeled abstract domain knowledge to case-specific facts stored in knowledge bases and therefore allowing experts to explore available information in a comprehensive and efficient way. The framework has been illustrated using the exemplary use case of POS Skimming. Its flexibility, scalability and potential integration into current and emerging police standards have been discussed.

Future work should include the in-depth modeling of other modi operandi in organized financial crime, as well as a comprehensive amount of practically relevant entities and relations. Also, the possibilities of modeling time-related components should be investigated, e.g. using simulation tools. Furthermore, the inclusion of tools for mining unstructured data would enable the inclusion of additional, automatically extracted data. In this regard, also the credibility measure needs to be adapted, to allow for a reliability assessment of the extracted data and potentially opposing information from different sources. The model should be subject to a practical validation, to assess its specific contribution to forensic practitioners in finding crime patterns (including objective quality measures). Also, it might be of interest to analyze potential countermeasures of criminals towards the proposed scheme (e.g. deliberate variations of crime pattern) and the vulnerability of the approach towards such attacks. Overall, addressing these issues in future work might enable the suggested framework to be applied in practical investigative as well as preventive police work, including additional use case scenarios.

References

[BHL01] Berners-Lee, T.; Hendler, J.; Lassila, O.: The semantic web. Scientific American 284(5), pp. 28-37, 2001.

[Nis12] Nissan, E.: Computer Applications for Handling Legal Evidence, Police Investigation and Case Argumentation. Springer Science & Business Media, vol. 5, 2012.

[Tex15] Textron Systems: IMPACT. Available at: http://www.textronsystems.com/products/advanced-information/impact, last accessed: 17.11.2015.

[Mar15] MarkLogik: Semantics. Available at: http://www.marklogic.com/what-is-marklogic/features/semantics/, last accessed: 17.11.2015.

[Jac12] Jackson, R.: NZ Police deploy semantic search technology. Available at: http://www.computerworld.co.nz/article/490838/nz_police_deploy_semantic_search_technology/, last accessed: 17.11.2015.

[Liu12] Liu, J.: How can the Semantic Web help Law Enforcement? 2012. Available at: http://lib.post.ca.gov/lib-documents/CC/Class50/50-Liu.pdf, last accessed: 17.11.2015.

[HWS15] Hollywood, J.S.; Woods, D.; Silberglitt, R.; Jackson, B. A.: Using Future Internet Technologies to Strengthen Criminal Justice. 2015. Available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR900/RR928/RAND_RR928.appendix.pdf, last accessed: 17.11.2015.

[ASB+14] Adderley, R.; Seidler, P.; Badii, A.; Tiemann, M.; Neri, F.; Raffaelli, M.: Semantic mining and analysis of heterogeneous data for novel intelligence insights. Proceedings of The Fourth International Conference on Advances in Information Mining and Management, IARIA, pp. 36-40, 2014.

[Dau13] The Daubert Standard: Court Acceptance of Expert Testimony. Available at: http://www.forensicsciencesimplified.org/legal/daubert.html, last accessed: 23.11.2015.

[Pfu12] Pfuhl, M.: Taxonomien. Available at: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/daten-wissen/Wissensmanagement/Wissensmodellierung/Wissensreprasentation/Semantisches-Netz/Taxonomien, last accessed: 23.11.2015.

[Gi02] Gesellschaft für Informatik (GI): Ontologie(n). Available at: https://www.gi.de/index.php?id=647&tx_ttnews[tt_news]=57&cHash=fa4532c7f4dcda05664600a9738f3177, last accessed: 23.11.2015.

[W3C15] Berners-Lee, T.: W3C Architecture. Available at: http://www.w3.org/2000/Talks/1206-xml2k-tbl/slide10-0.html, last accessed: 23.11.2015.

[Lot10] Lothridge, K.: Forensic Information Data Exchange (FIDEX) – Final Project Report. 2010. Available at: https://www.nfstc.org/wp-content/files//FIDEX_Final-Project-Report_Final_v2_wcopyright.pdf, last accessed: 24.11.2015.

[Haa11] Voss-de Haan, P.: XPolizei - Aufbau eines einheitlichen Repository für polizeilich relevante Kerndatenobjekte. 2011. Available at: http://www.xoev.de/detail.php?gsid=bremen83.c.11268.de, last accessed: 24.11.2015.

[BBH+13] Büttner, F.; Bartels, U.; Hamann, L.; Hofrichter, O.; Kuhlmann, M.; Gogolla, M.; Rabe, L.; Steimke, F.; Rabenstein, Y.; Stosiek, A.: Model-driven standardization of public authority data interchange. Science of Computer Programming, vol. 89, part B, pp. 162-175, 2014.

[Nie15] NIEM: National Information Exchange Model. Available at: https://www.niem.gov, last accessed: 26.11.2015.

[NeO14] The NeOn Toolkit. Available at: http://neon-toolkit.org/wiki/Main_Page.html, last accessed: 07.12.2015.

[OWL12] W3C: OWL 2 Web Ontology Language Document Overview (Second Edition). Available at: http://www.w3.org/TR/owl2-overview/, last accessed: 07.12.2015.

[Gae13] Gäubote Herrenberger Zeitung: Banken sperren tausende EC-Karten. Available at: http://www.gaeubote.de/gb_10_110356796-24-_Banken-sperren-Tausende-EC-Karten-.html?GBID=766bfa500ab5af3ca062dc6e6df915d8, last accessed: 07.12.2015.

[Kel15] Kelly, N.: How White Card Fraud Works. Available at: http://www.sid.in-berlin.de/nedkelly-world/howwhitecardfraudworks.html, last accessed: 07.12.2015.

[WRW+13] Wang, T.; Rudin, C.; Wagner, D.; Sevieri, R.: Learning to detect patterns of crime. Machine Learning and Knowledge Discovery in Databases, pp. 515-530, Springer Berlin Heidelberg, 2013.