AVALIAÇÃO DA ONTOLOGIA EXPERDF-ONTO PARA EXPERIMENTAÇÃO EM FORENSE DIGITAL POR MEIO DE CONSULTAS SPARQL

Ana Heloísa Bravin Mazur (PIBIC/CNPq/FA/UEM), Edson A. Oliveira Junior (Orientador). E-mail: edson@din.uem.br

Universidade Estadual de Maringá, Centro de Tecnologia, Maringá, PR

Área e subárea do conhecimento: Ciência da Computação, Sistemas de Informação

Palavras-chave: ontologias; forense digital; experimentação.

RESUMO

Este trabalho avaliou a ontologia *ExperDF-Onto,* desenvolvida para formalizar o processo de experimentação em forense digital. A avaliação foi conduzida por meio de consultas SPARQL para verificar sua usabilidade ontológica e sua capacidade de atender aos requisitos funcionais. Com base nos resultados, foram propostas melhorias e um protótipo para a segunda versão da ontologia. O trabalho conclui que a *ExperDF-Onto* é eficaz, mas sugere refinamentos para maximizar sua expressividade e aplicabilidade.

INTRODUÇÃO

A área de computação forense, ou forense digital, é uma adição recente à ciência forense, voltada à interpretação e análise de dados armazenados em dispositivos eletrônicos que tiveram parte em incidentes criminais. Devido a seu desenvolvimento recente, em comparação a outras áreas de pesquisa, a computação forense ainda não apresenta padronização em vários aspectos, em especial em métodos de pesquisa formais (MONTASARI; CARPENTER; HILL, 2019). Tendo como principal objetivo auxiliar o tribunal na elucidação de crimes, a confiabilidade das evidências obtidas na análise de um artefato digital é essencial para que estas sejam aceitas como provas. Como um instrumento de apoio para formalização do planejamento e da condução de experimentos em forense digital, Silva (2023) propõe a ontologia ExperDF-Onto, que tem como base o modelo conceitual proposto em OliveiraJr et al. (2020).

Avaliar e validar uma ontologia é essencial para garantir que ela cumpra seu propósito. Ontologias de domínio devem definir claramente o vocabulário especializado do domínio de interesse, de modo a possibilitar a interoperabilidade entre diferentes aplicações de software. Este trabalho tem como objetivo principal avaliar a ontologia ExperDF-Onto através do desenvolvimento de consultas na linguagem SPARQL, de modo a responder questões sobre sua usabilidade de uma perspectiva ontológica. Analisando as consultas desenvolvidas, foi possível chegar a conclusões sobre a utilidade da ontologia para cumprir o seu propósito. Além da avaliação, foram propostas algumas alterações e melhorias com o intuito de maximizar a expressividade semântica da ontologia.

MATERIAIS E MÉTODOS

A metodologia adotada neste trabalho foi estruturada para avaliar a ontologia *ExperDF-Onto* com foco em sua usabilidade e utilidade dentro do contexto da experimentação em forense digital. Com base na revisão de literatura realizada e nos requisitos funcionais da ontologia, foram definidas as questões de competência que a ontologia deve ser capaz de responder. Após a definição das questões de competência, foram desenvolvidas consultas em SPARQL para respondê-las. A linguagem SPARQL foi escolhida por ser a linguagem padrão para consulta a dados representados em RDF *(Resource Description Framework)* e OWL *(Ontology Web Language).* A etapa final consistiu na análise dos resultados obtidos a partir das consultas SPARQL. Sugestões para uma segunda versão da ontologia foram propostas, focando na melhoria da interoperabilidade e modularização da ontologia. Além disso, foi desenvolvido um protótipo para a nova versão da ontologia considerando os princípios da ontologia superior BFO (*Basic Formal Ontology)*.

RESULTADOS E DISCUSSÃO

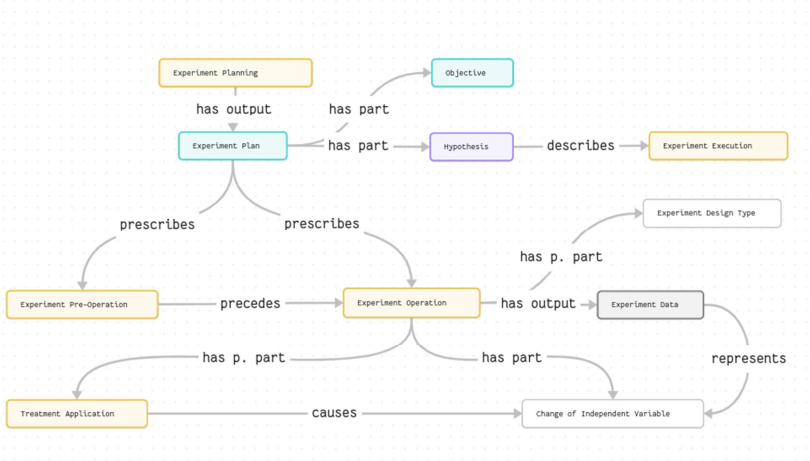
Uma das questões de competência formalizadas em SPARQL é apresentada na Figura 1. A consulta desta as relações entre as principais classes da ontologia, referentes as fases de um experimento. Nota-se que as classes são relacionadas por meio da relação *rdfs:subClassOf,* a relação de subsunção de classes. Um dos principais problemas encontrados na ontologia foi o uso dessa relação para substituir todas as relações presentes no modelo conceitual proposto em OliveiraJr et al. (2020).

```
SELECT?subClass WHERE {
      ?subClass rdfs:subClassOf owl:Thing.
      MINUS {
      # Remover subclasses indiretas
            ?subClass rdfs:subClassOf ?otherClass.
      FILTER(?otherClass != owl:Thing)
      FILTER(?otherClass != ?subClass)
      }
      FILTER(?subClass != owl:Thing)
}
```

Figura 1 – Questão de competência: quais são as fases de um experimento?

Partindo da avaliação realizada, foi desenvolvido um protótipo para a nova versão da ontologia. A nova versão tem como base a ontologia superior BFO, amplamente utilizada como uma ontologia de base em diversos projetos de ontologias de domínio em disciplinas científicas. Juntamente com BFO, foram utilizadas o conjunto de ontologias *Common Core* como ponto de partida para a especialização de classes. Para a modelagem dos conceitos referentes ao domínio da computação, foram consideradas ontologias existentes sobre o domínio para o reúso, como a ontologia C3O (*Common Cyber Ontology*) para o domínio de segurança da informação (DONOHUE et al., 2018). A Figura 2 apresenta um diagrama detalhando parte da ontologia desenvolvida, abrangendo o conceito de experimento. A ontologia desenvolvida descreve o processo de experimentação e oferece um vocabulário para os termos mais utilizados na área da computação, permitindo a representação de informações sobre experimentos envolvendo dispositivos digitais.

Figura 2 – Diagrama da ontologia com foco no conceito de experimento



CONCLUSÕES

Com a aplicação de consultas SPARQL foi possível identificar áreas que podem ser aprimoradas na ontologia *ExperDF-Onto*. Entre as sugestões de melhorias, destaca-

se a necessidade de maior detalhamento em certas classes e relações, bem como a inclusão de novos conceitos que possam enriquecer a descrição de experimentos. Além disso, a modularidade e a interoperabilidade da ontologia podem ser ampliados para facilitar sua integração com outras ontologias e sistemas utilizados na forense digital. O desenvolvimento de um protótipo para a segunda versão da *ExperDF-Onto* representa um avanço na direção dessas melhorias. As próximas etapas incluem a validação empírica das melhorias propostas e a exploração de novas aplicações da ontologia em cenários de investigação forense.

AGRADECIMENTOS

Ao Programa Institucional de Bolsas de Iniciação Científica (PIBIC/CNPq-FA-UEM) pela bolsa concedida à primeira autora. Edson A. Oliveira Junior agradece o apoio do CNPq (Processo 311503/2022-5).

REFERÊNCIAS

CASEY, E. **Handbook of Digital Forensics and Investigation.** USA: Academic Press, Inc., 2009.

DONOHUE, B. et al. A common core-based cyber ontology in support of cross-domain situational awareness. Em: **Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IX**. Orlando, United States: SPIE, 4 maio 2018.

OLIVEIRAJR, E.; ZORZO, A.; NEU, C. Towards a conceptual model for promoting digital forensics experiments. **Forensic Science International: Digital Investigation,** v. 35, p. 301014, 1 dez. 2020.

SILVA, T. J. **ExperDF-Onto: uma ontologia de apoio à experimentação controlada em forense digital.** 2023. 193 p. Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Maringá, Maringá – PR, 2023.

STUDER, R.; BENJAMINS, V. R.; FENSEL, D. Knowledge engineering: Principles and methods. **Data & Knowledge Engineering**, v. 25, n. 1, p. 161–197, 1 mar. 1998.