C3 Improving Information Sharing With the Cyber-Investigation Analysis Standard Expression/Unified Cyber Ontology (CASE/UCO)

Vikram Harichandran, MS, Fairfax, VA 22031; Cory Hall, MS, The MITRE Corporation, Severn, MD 21144*

Learning Overview: After attending this presentation, attendees will have a deeper understanding of what an ontology is, why adoption of the CASE standard is different from other specifications, why it will massively improve information sharing, and where the proper resources are for their organization to get involved in development or adoption.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by demonstrating how CASE can be adopted and integrated to better share information, also allowing those involved to help shape the ontology to cover gaps.

As the cybersecurity domain has grown, the amount of increasingly varied information needing to be shared has increased. There is now a greater need to validate, normalize, combine, and correlate investigative data between different countries, domains, organizations, teams, individuals, classification levels, and tools; the status quo is insufficient.

CASE is an international open-source and community-developed ontology/specification language that seeks to cover this gap in the most inclusive manner possible.[1] Work on what eventually became CASE began in 2015, and the project now involves more than two dozen public organizations.[2,3] It derives from UCO and is thus formally cited as CASE/UCO. UCO is intended to allow compatibility between CASE and other preexisting ontologies/schemas. However, unlike prior domain-specific specifications like Structured Threat Information Expression (STIX) and Digital Forensics Analysis eXpression (DFAX), CASE attempts to bring domains together, including incident response, counterterrorism, criminal justice, forensics, intelligence, and situational awareness. This will enable better workflow efficiencies in laboratories, cross-correlation between investigations under different jurisdictions, potentially on the same malicious actors, and a more aware view of criminal patterns.

The CASE team facilitates integration of subdomain knowledge from its global academic, private sector, and government community members; the ontology retains a core focus on tracking provenance and casework metadata (e.g., people who performed an action using a specific tool). Linked-data in the form of Resource Description Framework (RDF) graphs are used to export all data as JSON-LD (JSON for Linked-Data), which can be stored for transit, archiving, or tool ingestion. This past year, the MITRE Corporation has assisted in improving documentation and the supporting framework, while both European Union and United States governments have begun discussing a mandate for widespread adoption. The Github repositories (https://github.com/ucoProject) provide proof-of-concept mappings and implementations into forensics tools and outline the details of using the Application Programming Interfaces (API) in different ways. Additionally, exploration tools are available for the Terse RDF Triple Language (Turtle) format that the ontology is specified in. As the ontology evolves, it will encompass perspectives from community popular votes. However, custom and private schemas may still be supported for cases in which private or government tools desire integration with a preexisting data model.

This presentation will include a technical overview and example implementations of CASE, including a glance at the Python API and other resources.

Reference(s):

1. Casey, E., Barnum S., et al. Advancing Coordinated Cyber-Investigations and Tool Interoperability Using a Community Developed Specification Language. *Digital Investigation.* 22(2017): 14-45, https://doi.org/10.1016/j.diin.2017.08.002.
2. Harichandran, V., Walnycky, D., et al. CuFA: A More Formal Definition for Digital Forensic Artifacts. *Digital Investigation.* 18(2016), S125-S137, https://doi.org/10.1016/j.diin.2016.04.005.
3. CASE official website. https://sites.google.com/view/casework/home.

Information Sharing, Ontology, Standards

*Presenting Author