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 aims at covering this gap in the most inclusive manner possible. Work on what eventually became CASE began in 2015 and the project now involves over two dozen public organizations. 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, counter-terrorism, 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 that 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 E.U. and U.S. 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 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 where private or government tools desire integration with a pre-existing data model.