Scope

Describe traces from digital or physical resources to support cyber-investigations

RDF-oriented ontology:

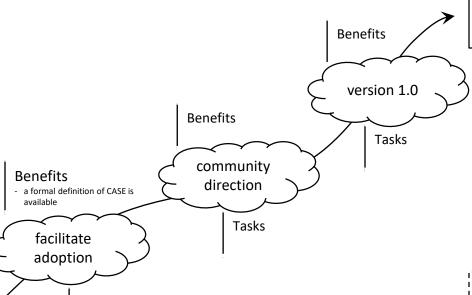
- release versioning
- trace descriptions
- ontology release version (mandatory)
- metadata using duck-typing
- data (included / referenced)
- provenance (chains of evidence and custody)
- marking / classification
- relationships between traces
- natural language glossary
- licensing

- application programming interfaces
- validators
- translators
- proof of concept implementations
- support tool-specific mappings
- licensing

CASE roadmap

Cyber-investigation Analysis Standard Expression

DRAFT - version 2018-04-12



Goals

All major tools provide a mechanism for importing and exporting CASE expressions.

CASE is actively used to:

- support investigations
 - evidence exchange
 - validate tools (based on ground truth available
 - as CASE expression)

Issues

- no end-users (investigators/prosecutors) involved
- not all major tool providers involved
- licensing not defined
- documentation is not easy to find

- release versioning not defined / available
- no mandatory version in CASE expressions
- no best practices, e.g.
- referencing / including data
- unsupported property bundles
- conflicting semantics, e.g.
- Contact vs. PhoneAccount

- no support for Java, C#
- no validator

Organization:

- no (issue-based) agenda for meetings
- no announcement mailing list
- GitHub fragmentation
- GitHub access control / ownership
- no wiki structure
- issue labeling
- CASE namespace not defined (URL)

Tasks

- define versioning and release plan
- define RDF distribution mechanism
- implement Python validator
- write implementer guide
- write contributor guide

Benefits Benefits organization on how to work on CASE is clear

organize

Tasks

- set up standard meeting agenda
- set up mailing list for announcements
- fix GitHub access control / ownership
- define and document labels for issues
- decide on CASE namespace / register URL

Organization

Online community

Regular (virtual) community meetings:

- ontology directions
- proposal/change decisions

Mailing list:

announcements

GitHub:

issue tracking

(draft) general documentation is available

Tasks

- defragment GitHub

- set up wiki structure

- write GitHub guide

document

- proposals (voting)
- versioning
- releases
- milestones
- snapshots (work in progress)
- recorded meetings
- meeting notes
- implementer guide
- contributor guide
- GitHub guide

Website:

- publications
- announcements
- mailing list subscriptions
- RDF releases