CASE roadmap

Cyber-investigation Analysis Standard Expression

version: 2018-09-19

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

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

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

General:
- no end-users (investigators/prosecutors) involved
- not all major tool providers involved
- No flyer/one-pager available

Ontology:
- 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

Tools:
- no support for Java, C#, and JSON-LD languages
- no validator

Events:
- mapping and implementation workshop
- vendor customer feedback (survey as well)
- ontology conference/workshop

Global meetings:
- no (issue-based) agenda for meetings (add to governance model)
- update on website

Add to Governance Model:
- declare mailing lists (announcements)
- declare establishing dates for roadmap review
- declare create a nonprofit or organization to hold URL namespace
- declare governance/licensing documentation
- declare periodic review of major milestones (assigned to Github)
- declare global meeting agenda

facilitate adoption 12/2018

Benefits
- Preparation for starting a community is finished

Tasks
- define versioning and release plan
- define RDF distribution mechanism
- write first versions of guides
- pre-schedule monthly dev calls
- pre-schedule quarterly roadmap calls
- define default agendas for calls
- plan conference/workshop

community direction 03/2019

Benefits
- the community is actively working on version 1.0

Tasks
- invite potential community members
- distribute one-pager and guides

version 1.0 01/2020

Benefits
- First stable version is available

Tasks
- define minimal requirements
- verify if all requirements are met
- release version 1.0
- communicate press release

organization

Benefits
1. organization on how to work on CASE is clear
2. governance structure is clear and set up

Tasks
1. set up mailing list for announcements
1. schedule roadmap call every 3 months (mid-month)
2. Design and document governance model
2. approach and nominate candidates
2. Elect committees' members

administation

Benefits
- centralized and simple workflow
- licencing is clear and set up

Tasks
- decide on CASE namespace / register URL
- write one-pager
- write GitHub use
- write versioning guidelines
- define and document labels for ontology issues

Organization

Online community

Governance structure
- ontology & governance committees
- election protocol
- election protocol
- licensing

Regular (virtual) community meetings:
- ontology directions
- proposal/change decisions

Mailing list:
- announcements (same as website)

GitHub:
- issue tracking, bugs, proposals
- continue updating guides
- versioning
  - releases
  - milestones
  - snapshots (work in progress)

Website (Community Portal):
- announcements tab (same as mailing list)
- recorded meetings tab (hosting platform?)
- publications tab
- contact tab (mailing list subscriptions)
- release tab (RDF ontology releases)