CASE

Cyber-investigation Analysis Standard Expression

Community update

Harm van Beek

CASE Technical Director

March 2019

Outline

What is CASE?

CASE Ontology status

CASE Community status

Work in progress

Interested/involved organizations

CASE Resources

Cyber-investigation Analysis Standard Expression

CASE is a community-developed ontology to support:

- reporting of digital traces
- exchanging of digital traces
- tool validation (express ground truth)

in the context of:

- digital forensic science
- incident response
- counter-terrorism
- criminal justice
- forensic intelligence
- situational awareness

CASE

CASE Ontology status

Resource Description Framework (RDF in Turtle)

Natural Language Glossary

Example expressions

- Bulk Extractor Forensic Path (info)
- Call Log
- Device
- Email
- EXIF Data
- Files (info)
- Forensic Lifecycle
- Location
- Message
- Multipart File (info)
- Oresteia (info)
- Raw Data
- Reconstructed File (info)
- SMS and Contacts

Reference documents

- Representing Mobile Devices and SIM Cards
- Representing File and File System information
- Representing Recoverability of Unallocated Files
- Representing Accounts

Reference mappings

- Sleuthkit
- Cellebrite
- Bulk Extractor
- NSRL

Validators

- RDFDiff

Application Programming Interfaces

- Python API

CASE

CASE Community status

2015-03 Initial ideas presented (DI-12-1, 102-110)

2017-07 CASE introduction paper (DI-22, 14-45)

2018-04 workshop → first roadmap

2018-08 community formalization started:

- 2018-11 bylaws
- 2019-01 governance committee elected
- 2019-01 code of conduct
- 2019-02 ontology committee (charter)

Biweekly virtual meetings, approx. 1 hour:

- Governance committee
- Ontology committee

CASE Community Organization

Governance Committee

Presiding Director

Eoghan Casey
University of Lausanne

Government Class Director

Ryan Griffith
DOD Cyber Crime Center

For-profit Class Director

Jessica Hyde
Magnet Forensics

Non-profit Class Director

Richard Brown
Project VIC

Academic Class Director

Sanjin Lee
Korea University

coordinator
Cory Hall
MITRE

Ontology Committee

Chair

Alex Nelson
NIST

Co-chair

Ryan Hohimer
DarkLight

12 members

Technical Director

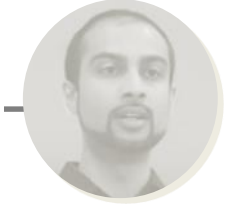
Harm van Beek
Netherlands Forensic Institute

Mapping Committee
(CASE producers)

Chair

Andrew Sovern
MITRE

Adoption Committee
(CASE consumers)

Chair

Vik Harichandran
MITRE

Work in progress

Organization

Mapping committee (charter)

Adoption committee (charter)

Privacy statement

Application form

Operations guideline

- Trello
- Github
- …

Ontology

Roadmap

Documentation

- W3C recommendation

License

- Apache 2

Ontology workshop

- May/June 2019

CASE

Interested/involved organizations

Questions?

CASE Community Website

`www.caseontology.org` *(coming soon)*

`sites.google.com/view/casework/`

organization – bylaws – code of conduct – meeting notes

documentation – roadmap – publications– use cases

CASE Ontology

`github.com/ucoProject/CASE/`

RDF – natural language glossary – open issues

CASE Organization*

`trello.com/caseworks`

work in progress – draft documentation – meeting agendas

CASE Development Forum*

`groups.google.com/d/forum/case-dev`

* Requires community membership

Harm van Beek, PhD
harm.van.beek@nfi.nl