



Improving Information Sharing With the Cyber-investigation Analysis Standard Expression(CASE) and Unified Cyber Ontology (UCO)

By

Cory Hall and Vik Harichandran

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2019 USA

Portland, OR (July 15th - 19th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<https://dfrws.org>

Improving Information Sharing With the Cyber-investigation Analysis Standard Expression(CASE) and Unified Cyber Ontology (UCO)

Cory Hall

CASE Task Lead, MITRE

Vik Harichandran

CASE Developer, MITRE



Approved for public release under PRE 18-4297.

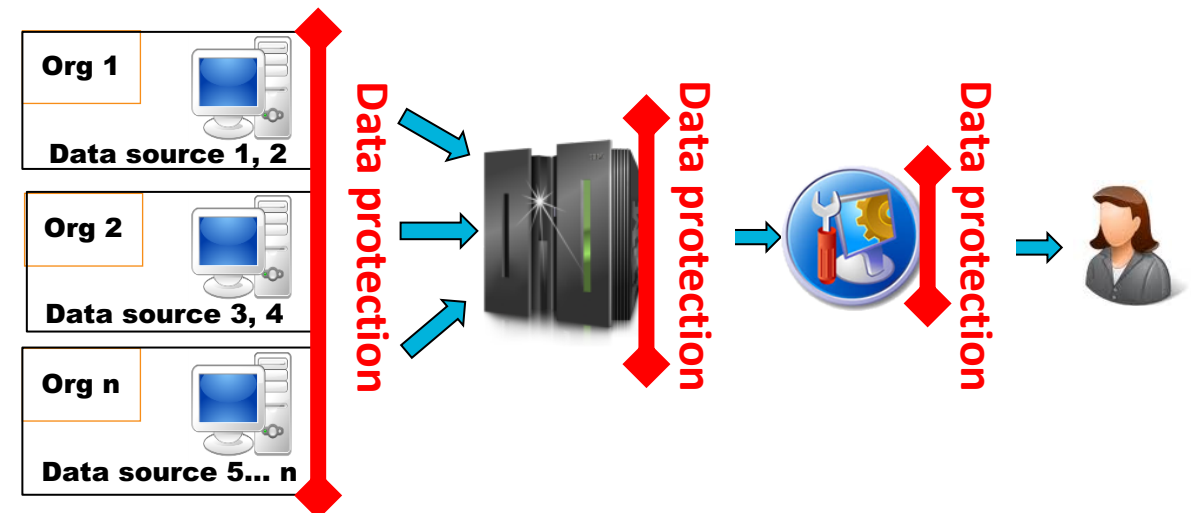
MITRE

Agenda

- **Introduction**
- **Use Cases**
- **UCO and CASE**
- **CASE Community Overview**
- **Resources**

Use Cases

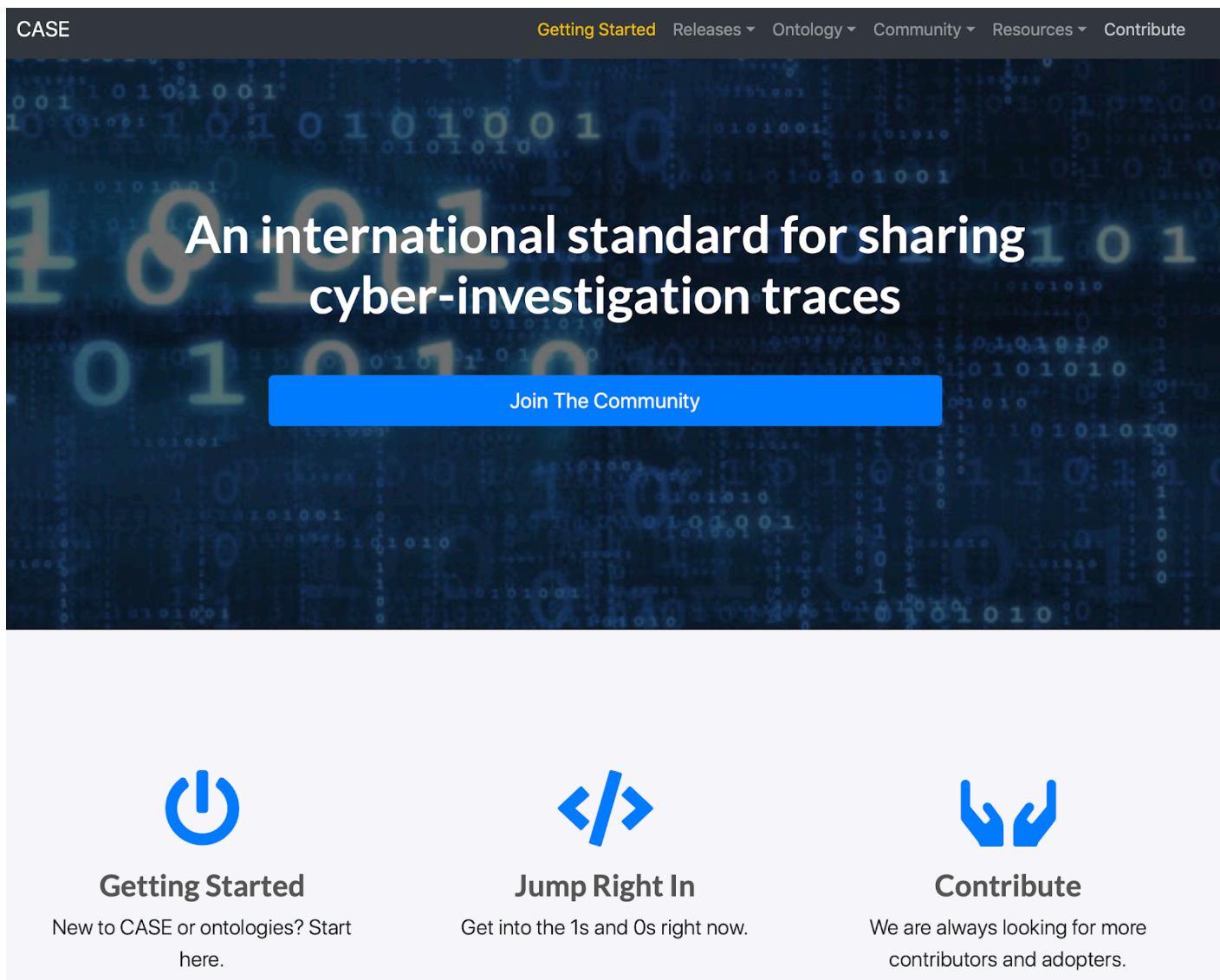
- Interoperability between digital investigation systems and tools.
- Maintain provenance at all phases of digital investigation lifecycle.
- Enhance tool testing and validation of results.
- Control access.
- Unsupported data structures.
- Allow intelligent analysis through correlation and reasoning/inference.



CASE/UCO

- **UCO = Unified Cyber Ontology:**
 - Declares the core concepts within the cyber domain.
 - UCO 0.3 released on 7/13/2019
- **CASE = Cyber-investigation Analysis Standard Expression:**
 - Derivative ontology that inherits UCO
 - Addresses digital investigation concepts in digital forensics, incident response, terrorism, and criminal justice investigations.
 - Examples: the process of a network breach, unique investigative process/mindset
 - Trying to achieve flexibility through multi-typing and custom property bundles.

<https://caseontology.org>




The screenshot shows the homepage of the CASE ontology website. The header is dark grey with the word 'CASE' on the left and navigation links 'Getting Started', 'Releases', 'Ontology', 'Community', 'Resources', and 'Contribute' on the right. The main banner has a dark blue background with binary code and the text 'An international standard for sharing cyber-investigation traces'. Below this is a blue button that says 'Join The Community'. The footer is light grey and contains three columns, each with an icon, a title, and a description.


CASE


Getting Started Releases Ontology Community Resources Contribute

An international standard for sharing
cyber-investigation traces

Join The Community

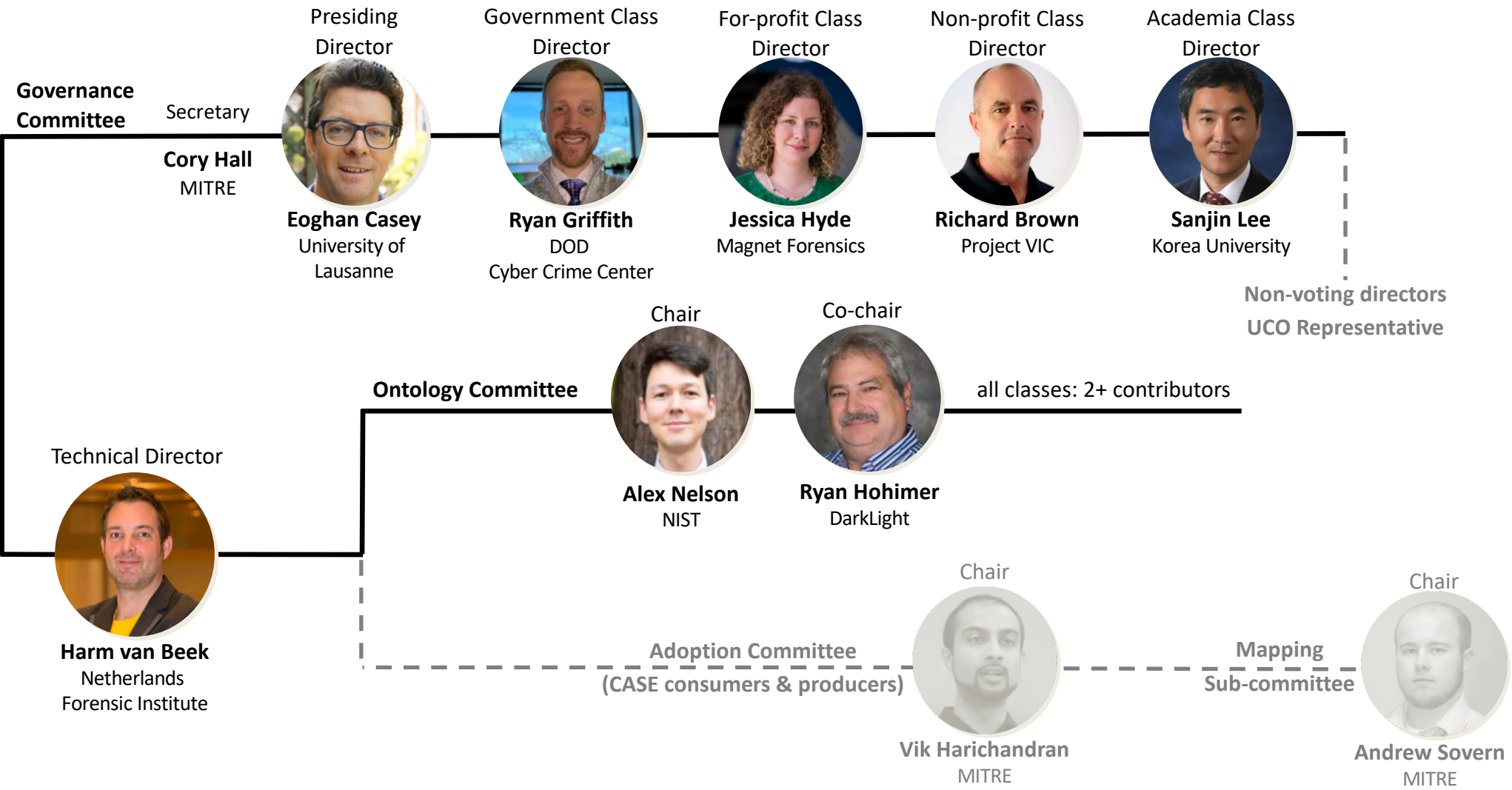

Getting Started
New to CASE or ontologies? Start here.


Jump Right In
Get into the 1s and 0s right now.

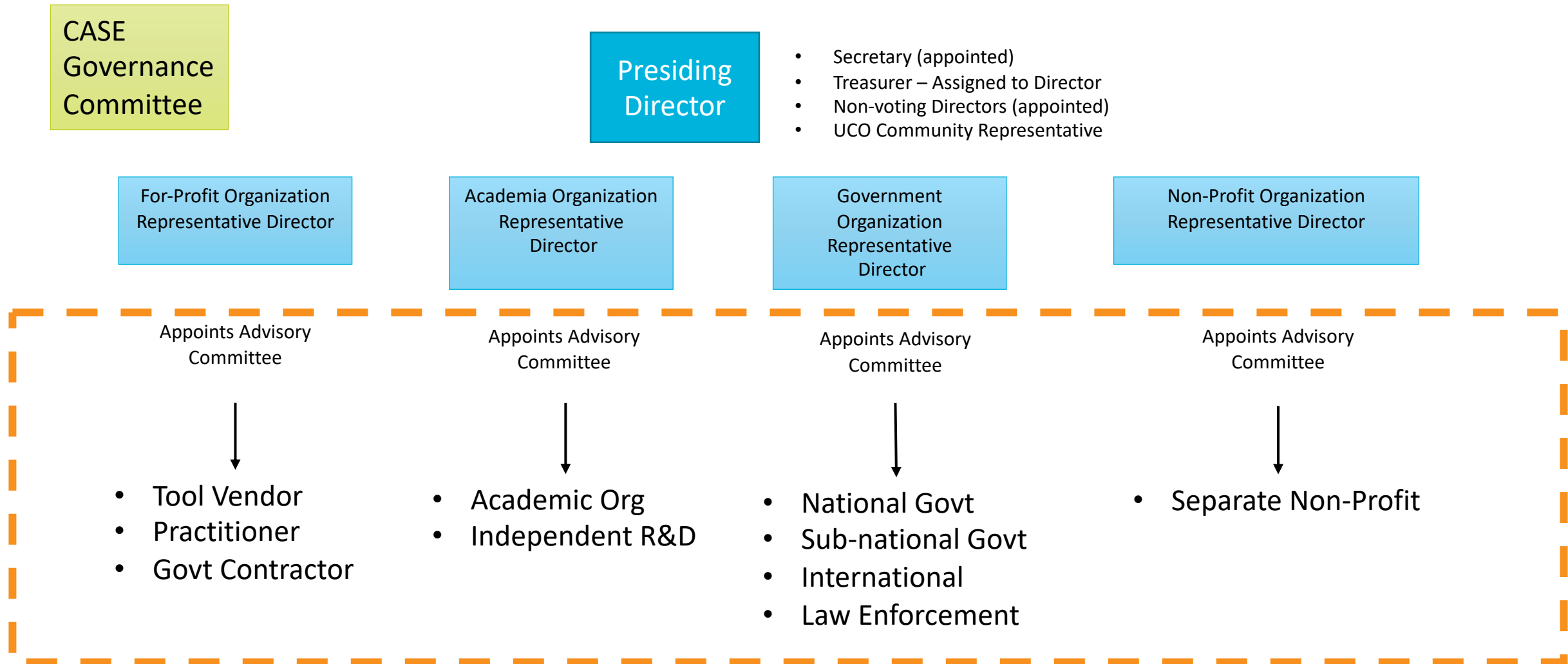

Contribute
We are always looking for more contributors and adopters.

The CASE Community

CASE Community Leadership



Class Representation is Key to Success



Organizational Representation

MITRE

Unil
UNIL | Université de Lausanne

 Netherlands Forensic Institute
Ministry of Justice and Security




Next Generation Threat Protection


MAGNET
FORENSICS®

 **EVIDENCE₂** / 
Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe




EUROPOL
EC3 | European Cybercrime Centre

DARK X **LIGHT**®


NCCOE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

MOBILedit


Your Connection to ICT Research


i2
Accelerating Your Vision


OXYGEN
FORENSICS
Helping good people to make the world safer


BASIS
TECHNOLOGY

MSAB

GUIDANCE
SOFTWARE




BlackBag
TECHNOLOGIES




AUTOPSY
DIGITAL FORENSICS


Cellebrite

VOLATILITY


NETRESEC


AccessData

nuix

Current Membership

COUNTRIES

9

APPROVED MEMBERS

26

- 7 Non-Profit
- 8 For-Profit
- 6 Academia
- 5 Gov/LE

ONTOLOGY COMMITTEE

17

CASE Community Membership

- **Visit the CASE Community website to apply for membership**
 - Active Members assigned to committee
 - Ontology
 - Adoption (coming soon)
 - Observer Member
 - Receive updates from the community
 - Membership for organization leaders and administrative staff that need visibility on CASE
 - Organization Member
 - For organizations that want to join the CASE Community (coming soon)
 - Membership fee structure is in the works

Questions?

- **CASE Community Website**
 - <https://caseontology.org>
- **Read Github Wiki:**
 - <https://github.com/ucoProject/CASE/wiki>
- **Reach out to us:**
 - clhall@mitre.org
 - vharichandran@mitre.org
- **Request private 1-on-1 consultation/direction from the CASE Community:**
 - cyberinvestigationexpress@gmail.com

MITRE

MITRE is a not-for-profit organization whose sole focus is to operate federally funded research and development centers, or FFRDCs. Independent and objective, we take on some of our nation's—and the world's—most critical challenges and provide innovative, practical solutions.

Learn and share more about MITRE, FFRDCs, and our unique value at www.mitre.org



LinkedIn

