Autopsy Support for CASE

Eugene Livis – Basis Technology
Vik Harichandran – MITRE
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.
An international standard for sharing cyber-investigation traces

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.
Class Representation is Key to Success

CASE Governance Committee

For-Profit Organization Representative Director
Appoints Advisory Committee
- Tool Vendor
- Practitioner
- Govt Contractor

Academia Organization Representative Director
Appoints Advisory Committee
- Academic Org
- Independent R&D

Government Organization Representative Director
Appoints Advisory Committee
- National Govt
- Sub-national Govt
- International
- Law Enforcement

Non-Profit Organization Representative Director
Appoints Advisory Committee
- Separate Non-Profit

Presiding Director
- Secretary (appointed)
- Treasurer – Assigned to Director
- Non-voting Directors (appointed)
- UCO Community Representative

Appoints Advisory Committee
- Tool Vendor
- Practitioner
- Govt Contractor
- Academic Org
- Independent R&D
- National Govt
- Sub-national Govt
- International
- Law Enforcement
- Separate Non-Profit
## Current Membership

<table>
<thead>
<tr>
<th>COUNTRIES</th>
<th>APPROVED MEMBERS</th>
<th>ONTOLOGY COMMITTEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>26</td>
<td>17</td>
</tr>
<tr>
<td>7 Non-Profit</td>
<td>8 For-Profit</td>
<td>6 Academia</td>
</tr>
<tr>
<td>5 Gov/LE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
How To Generate a CASE Report
How To Generate a CASE Report

![Image of Autopsy software interface showing the Generate Report module with CASE-UCO selected]

- Select the CASE-UCO module for generating a report with basic property fields for every file.
How To Generate a CASE Report
Sample Autopsy CASE Output

Autopsy CASE Report
Contains:
- Autopsy case and data source info.
- Manifest of all files in the case.
  - Includes extracted archive files, unallocated space, etc.
  - Includes files from all data sources contained in the case (can be multiple data sources).
- Currently only files get saved in the CASE report. Artifacts are not getting saved.
Questions?

Basis (Brian Carrier):
  brianc@basistech.com

MITRE (Vik Harichandran):
  vharichandran@mitre.org

CASE Community Website:
  https://caseontology.org

Github Organization:
  https://github.com/casework
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

Approved for public release under PRE 18-4297.