

Autopsy Support for CASE

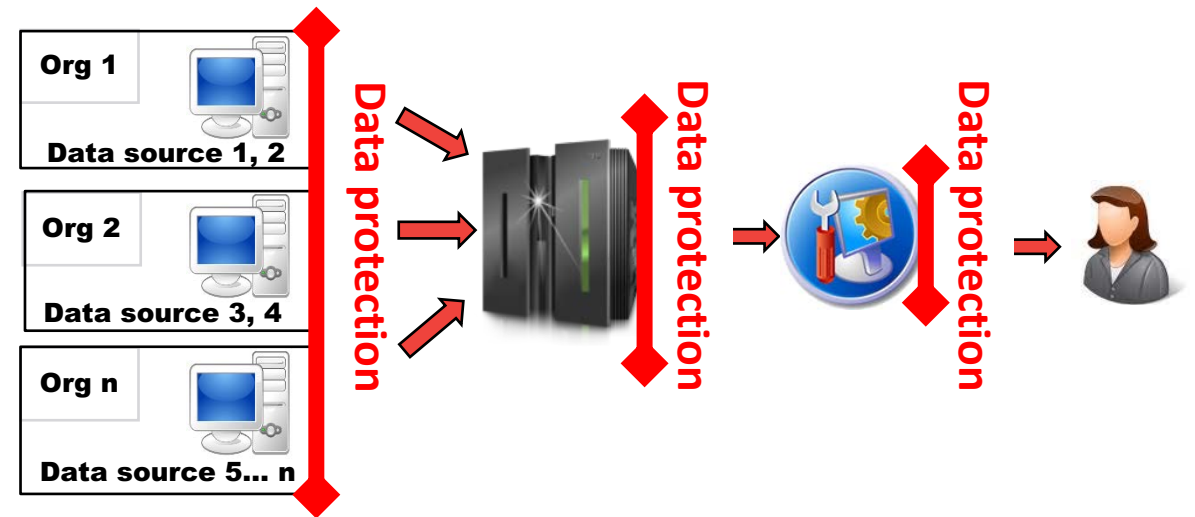
Eugene Livis – Basis Technology

Vik Harichandran – MITRE



Use Cases

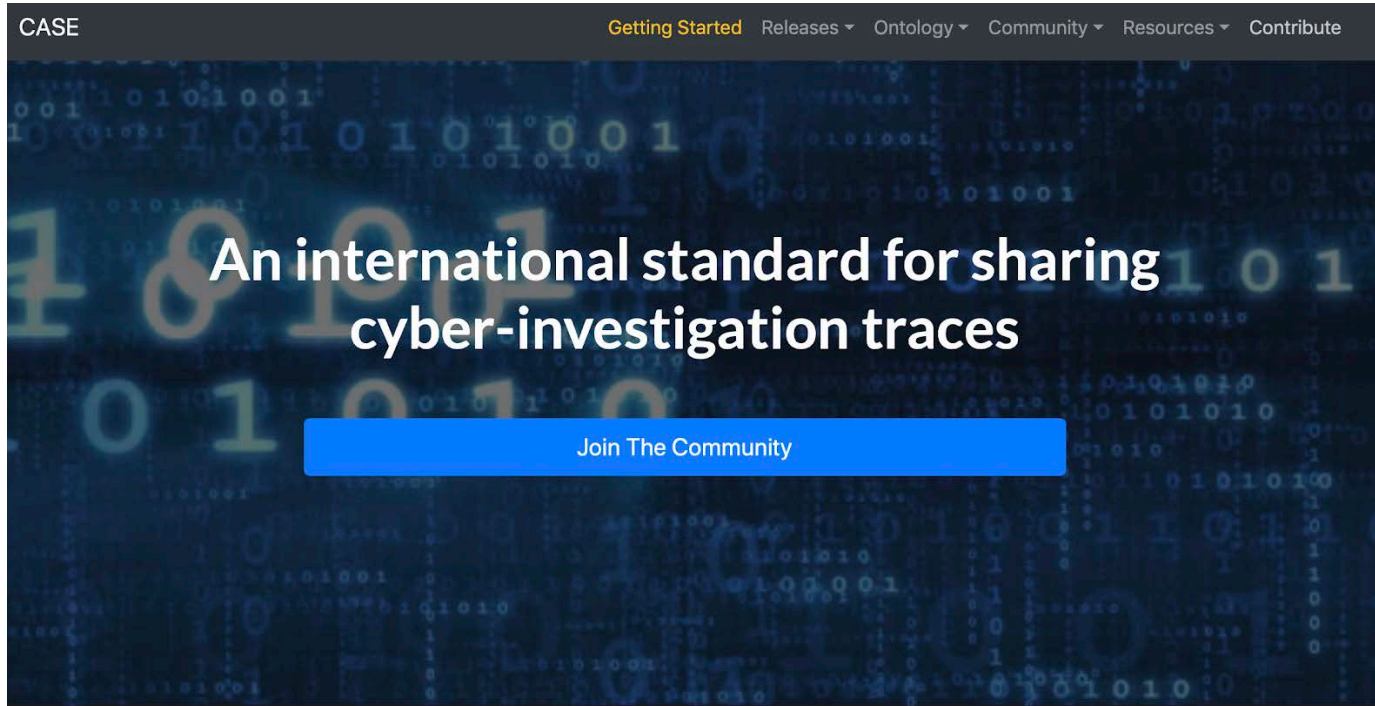
- Interoperability between digital investigation systems and tools.
- Maintain provenance at all phases of digital investigation lifecycle.
- Enhance tool testing and validation of results.
- Control access.
- Unsupported data structures.
- Allow intelligent analysis through **correlation and reasoning/inference**.



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.

<https://caseontology.org>




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

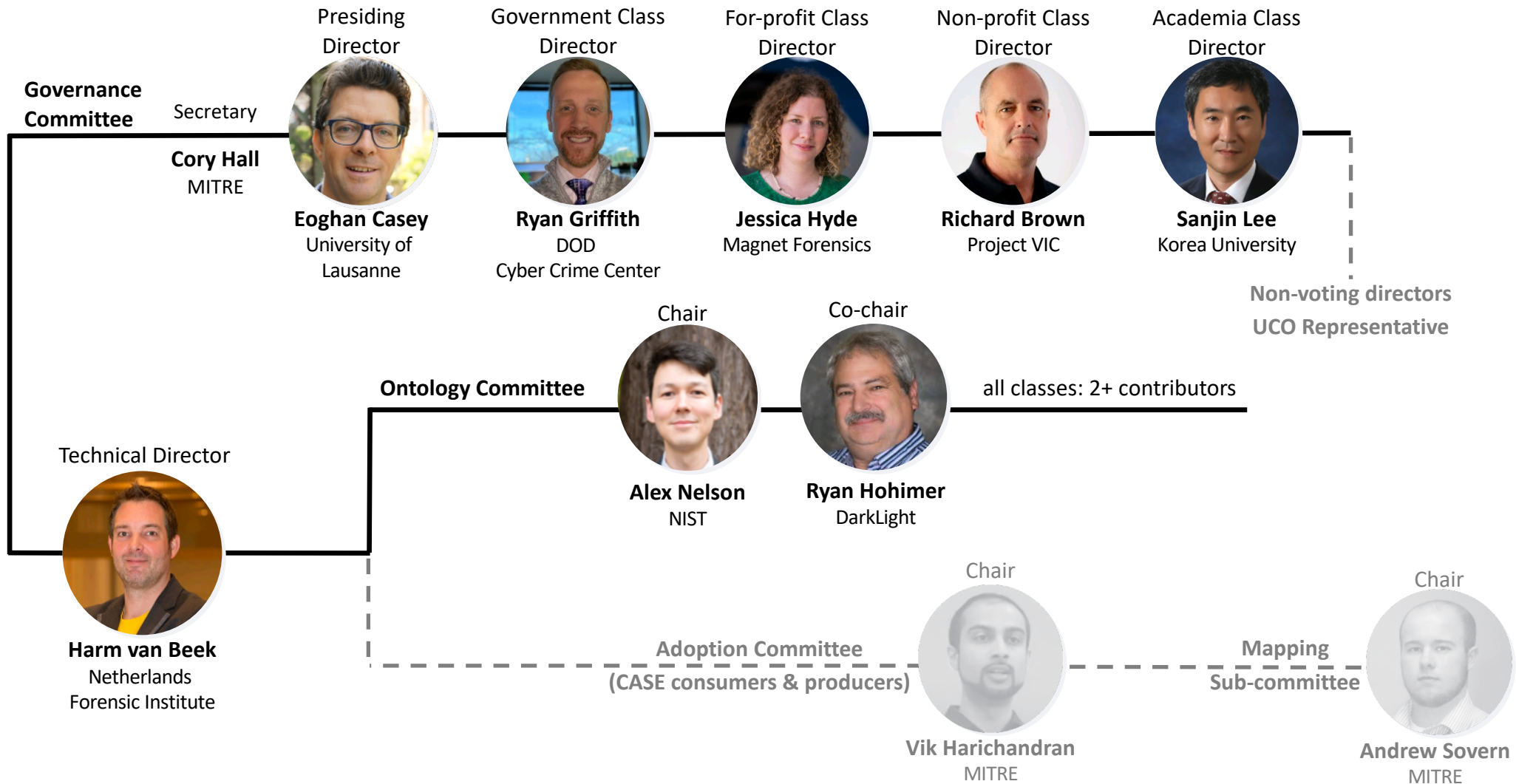
Get into the 1s and 0s right now.



Contribute

We are always looking for more contributors and adopters.

CASE Community Leadership



Class Representation is Key to Success

CASE
Governance
Committee

Presiding
Director

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

For-Profit Organization
Representative Director

Academia Organization
Representative Director

Government
Organization
Representative Director

Non-Profit Organization
Representative Director

Appoints Advisory
Committee



- Tool Vendor
- Practitioner
- Govt Contractor

Appoints Advisory
Committee



- Academic Org
- Independent R&D

Appoints Advisory
Committee



- National Govt
- Sub-national Govt
- International
- Law Enforcement

Appoints Advisory
Committee



- Separate Non-Profit

Organizational Representation

MITRE

Unil
UNIL | Université de Lausanne

Netherlands Forensic Institute
Ministry of Justice and Security



FireEye™
Next Generation Threat Protection

M
MAGNET
FORENSICS®

EVIDENCE2 / eCODEX
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

OXYGEN
FORENSICS
making good people to make the world safer

BASIS
TECHNOLOGY

MSAB

GUIDANCE
SOFTWARE

ocetic
Your Connection to ICT Research

IBM
i2
Accelerating Your Vision

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

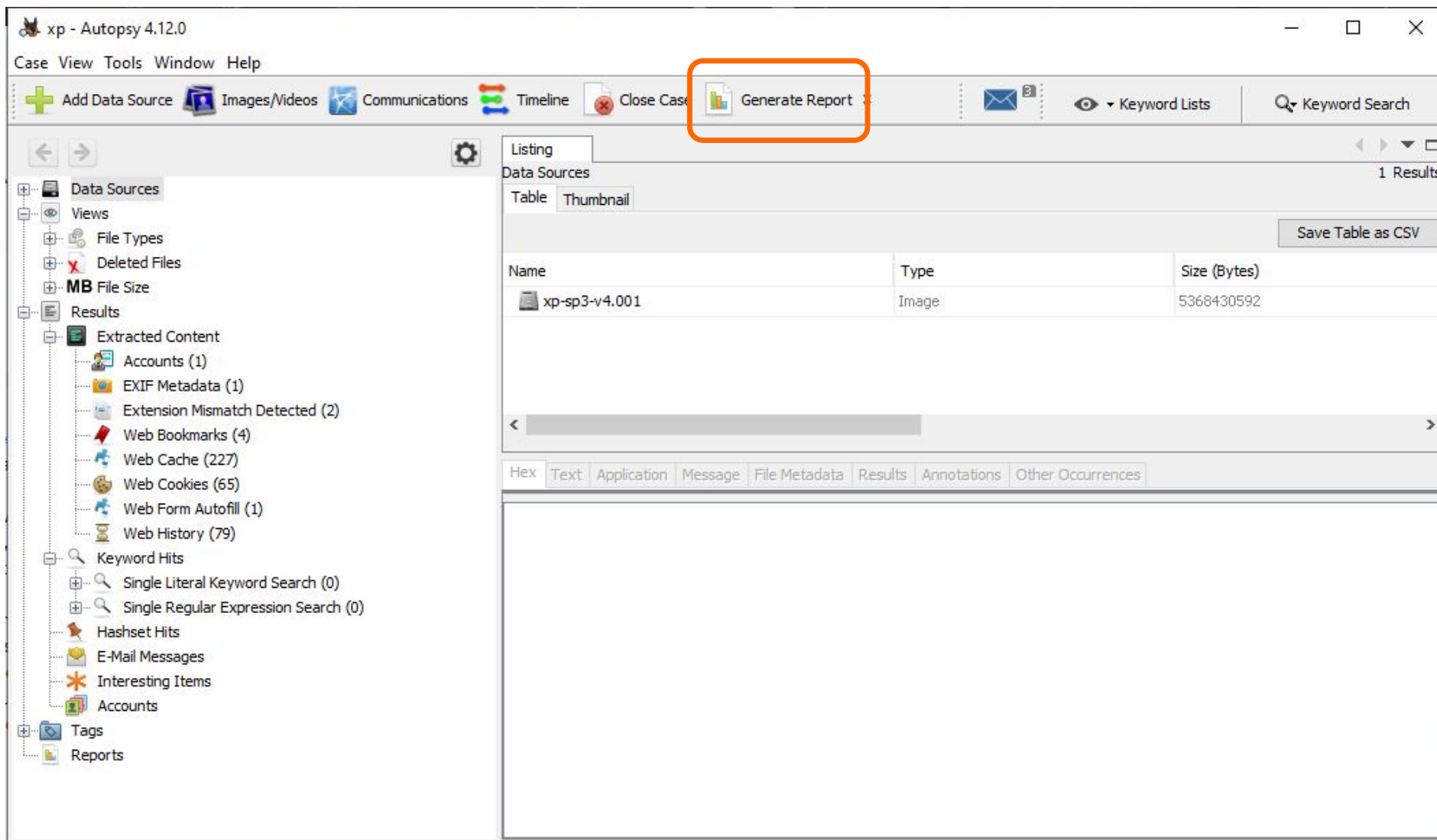
17

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

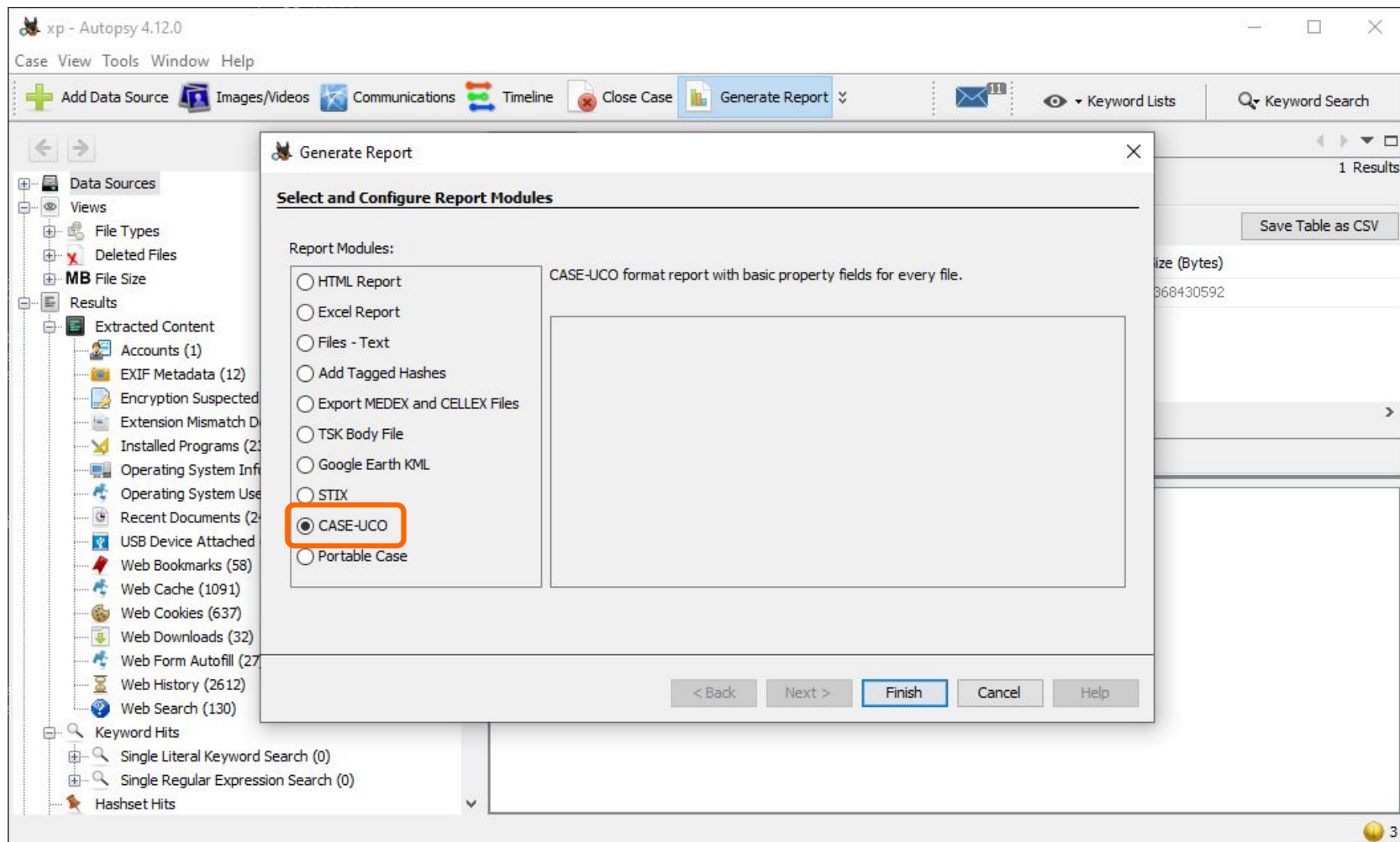
How To Generate a CASE Report



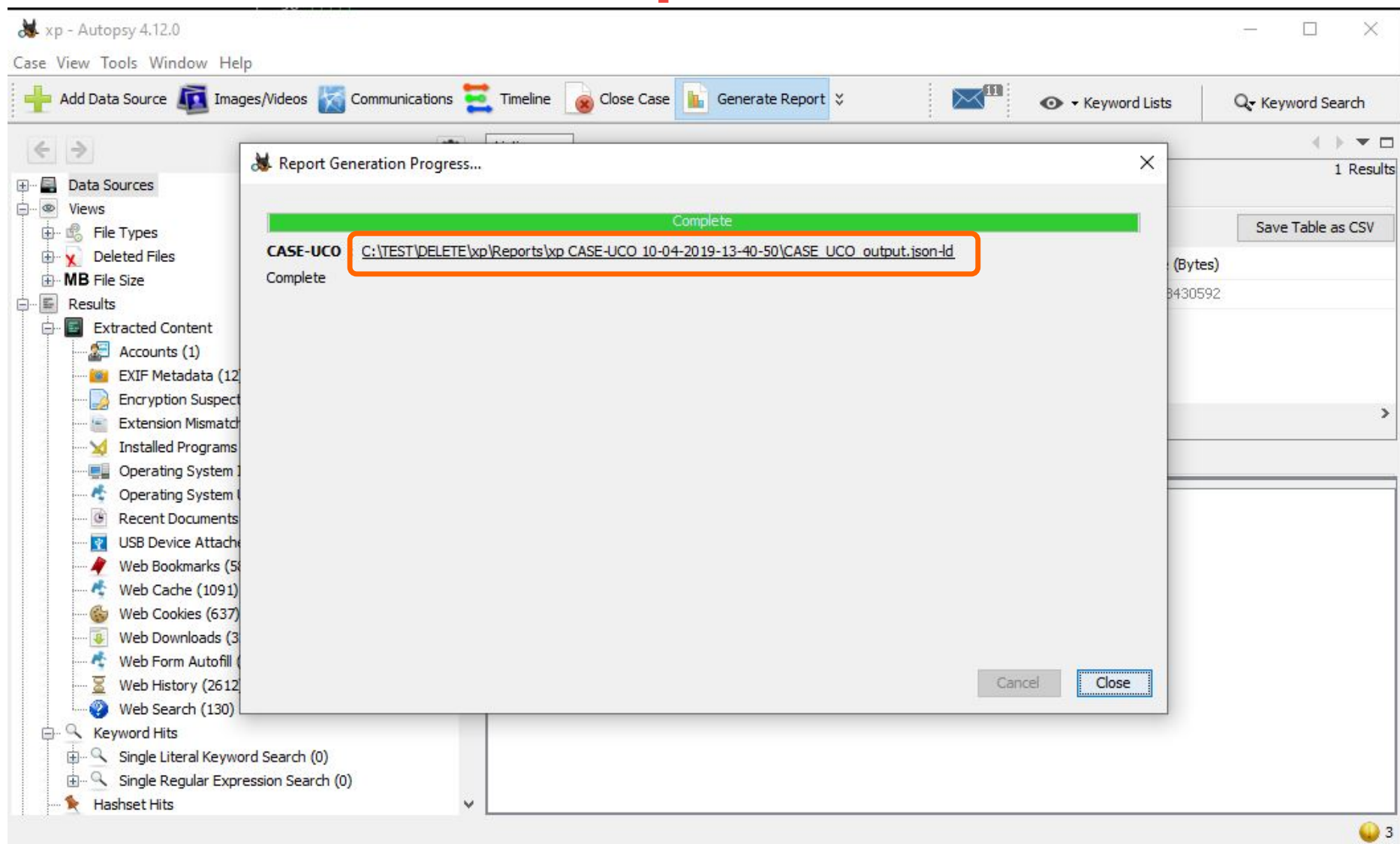
The screenshot shows the Autopsy 4.12.0 application window. The title bar reads 'xp - Autopsy 4.12.0'. The menu bar includes 'Case', 'View', 'Tools', 'Window', and 'Help'. The toolbar contains several icons, with the 'Generate Report' icon (a document with a green checkmark) highlighted by an orange rectangle. Other toolbar icons include 'Add Data Source', 'Images/Videos', 'Communications', 'Timeline', 'Close Case', 'Email', 'Keyword Lists', and 'Keyword Search'. The left sidebar shows a tree view of the case data, including 'Data Sources', 'Views', 'File Types', 'Deleted Files', 'MB File Size', 'Results', 'Extracted Content', 'Keyword Hits', 'Hashset Hits', 'E-Mail Messages', 'Interesting Items', 'Accounts', 'Tags', and 'Reports'. The main pane displays a 'Listing' of 'Data Sources' with 1 result. The table has columns for 'Name', 'Type', and 'Size (Bytes)'. The single entry is 'xp-sp3-v4.001' of type 'Image' with a size of 5368430592 bytes. A 'Save Table as CSV' button is visible in the top right of the table area. Below the table, there are tabs for 'Hex', 'Text', 'Application', 'Message', 'File Metadata', 'Results', 'Annotations', and 'Other Occurrences'.

Name	Type	Size (Bytes)
xp-sp3-v4.001	Image	5368430592

How To Generate a CASE Report



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.

```
CASE_UCO_output.json-ld - Notepad2-mod
File Edit View Settings ?
1 {
2   "@graph" : [ {
3     "@id" : "case-xp_20191004_132436",
4     "@type" : "Trace",
5     "propertyBundle" : [ {
6       "@type" : "File",
7       "filePath" : "C:/TEST/DELETE/xp/autopsy.db",
8       "isDirectory" : false
9     } ]
10   }, {
11     "@id" : "data-source-1",
12     "@type" : "Trace",
13     "propertyBundle" : [ {
14       "@type" : "File",
15       "filePath" : "C:/TEST/Inputs/xp-sp3-v4/xp-sp3-v4.001"
16     } ], {
17       "@type" : "ContentData",
18       "sizeInBytes" : "5368430592"
19     } ]
20   }, {
21     "@id" : "relationship-case-xp_20191004_132436",
22     "@type" : "Relationship",
23     "source" : "data-source-1",
24     "target" : "case-xp_20191004_132436",
25     "kindOfRelationship" : "contained-within",
26     "isDirectional" : true,
27     "propertyBundle" : [ {
28       "@type" : "PathRelation",
29       "path" : "C:/TEST/Inputs/xp-sp3-v4/xp-sp3-v4.001"
30     } ]
31   }, {
32     "@id" : "file-7",
33     "@type" : "Trace",
34     "propertyBundle" : [ {
35       "@type" : "File",
36       "createdTime" : "2012-01-20T17:09:03Z",
37       "accessedTime" : "2012-01-20T17:09:03Z",
38       "modifiedTime" : "2012-01-20T17:09:03Z",
39       "extension" : "",
40       "fileName" : "$AttrDef",
41       "filePath" : "/$AttrDef",
42       "isDirectory" : false,
43       "sizeInBytes" : "2560"
```

```
CASE_UCO_output.json-ld - Notepad2-mod
File Edit View Settings ?
8706 }, {
8707   "@id" : "file-449",
8708   "@type" : "Trace",
8709   "propertyBundle" : [ {
8710     "@type" : "File",
8711     "createdTime" : "2012-01-20T22:19:52Z",
8712     "accessedTime" : "2012-03-10T19:44:47Z",
8713     "modifiedTime" : "2012-01-20T22:19:52Z",
8714     "extension" : ".lnk",
8715     "fileName" : "Windows Messenger.lnk",
8716     "filePath" : "/Documents and Settings/All Users/Start Menu/Programs/Windows Messenger.lnk",
8717     "isDirectory" : false,
8718     "sizeInBytes" : "609"
8719   } ], {
8720     "@type" : "ContentData",
8721     "mimeType" : "application/octet-stream",
8722     "hash" : [ {
8723       "@type" : "Hash",
8724       "hashMethod" : "MD5",
8725       "hashValue" : "f2a5a0f56d833b19922fc05f92429e09"
8726     } ],
8727     "sizeInBytes" : "609"
8728   } ]
8729 }, {
8730   "@id" : "relationship-449",
8731   "@type" : "Relationship",
8732   "source" : "file-449",
8733   "target" : "data-source-1",
8734   "kindOfRelationship" : "contained-within",
8735   "isDirectional" : true,
8736   "propertyBundle" : [ {
8737     "@type" : "PathRelation",
8738     "path" : "/Documents and Settings/All Users/Start Menu/Programs/Windows Messenger.lnk"
8739   } ]
8740 }, {
8741   "@id" : "file-450",
8742   "@type" : "Trace",
8743   "propertyBundle" : [ {
8744     "@type" : "File",
8745     "createdTime" : "2012-01-20T22:19:52Z",
```


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

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.