CASE

(Cyber-investigation Analysis Standard Expression)

Workshop

DFRWS EU 2020 – 5 June 2020

Eoghan Casey

CASE Presiding Director /

University of Lausanne

Harm van Beek

CASE Technical Director /

Netherlands Forensic Institute (NFI)

Jessica Hyde

CASE Governance Committee/

Magnet Forensics

Ryan Griffith

CASE Governance Committee /

U.S. DoD Cyber Crime Center

CASE Workshop Agenda

Time (UK)	Time (NY)	Presentation Title	Presenters
1615-1630	1115-1130	CASE Vision and Roadmap	Harm van Beek, Technical Director
1630-1645	1130-1145	CASE Community Updates	Eoghan Casey, Presiding Director
1645-1655	1145-1200	CASE Ontology Status	Deborah L. Nichols, Ontology Committee
1700-1715	1200-1215	CASE Adoption Committee	Vik Harichandran, Adoption Committee Chair
1715-1730	1215-1230	*Break*	
1730-1750	1230-1250	Mapping Mobile Forensics Tools Output to the CASE Standard	Mattia Epifani & Fabrizio Turchi, CNR, Institute of Legal Informatics and Judicial Systems Claudia Meda, Reality Net Systems Solutions
1750-1810	1250-1310	Utilising the CASE Standard to View Bespoke File Systems	Gregory Webb, London Metropolitan Police (UK)
1810-1830	1310-1330	CASE Mapping Tutorial	Andrew Sovern, Mapping Working Group Leader
1830-1845	1330-1345	Discussion and CASE Online Resources	Ryan Griffith, Governance Committee Jessica Hyde, Governance Committee

CASE

Harm van Beek, CASE Technical Director / Netherlands Forensic Institute (NFI)

CASE VISION AND ROADMAP

CASE

Cyber-investigation Analysis Standard Expression

Harm van Beek

CASE Technical Director

5 June 2020

Cyber-investigation Analysis Standard Expression

CASE is a community-developed standard to support:

- reporting of digital traces
- exchanging of digital traces
- analysis 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

Outline

Why?

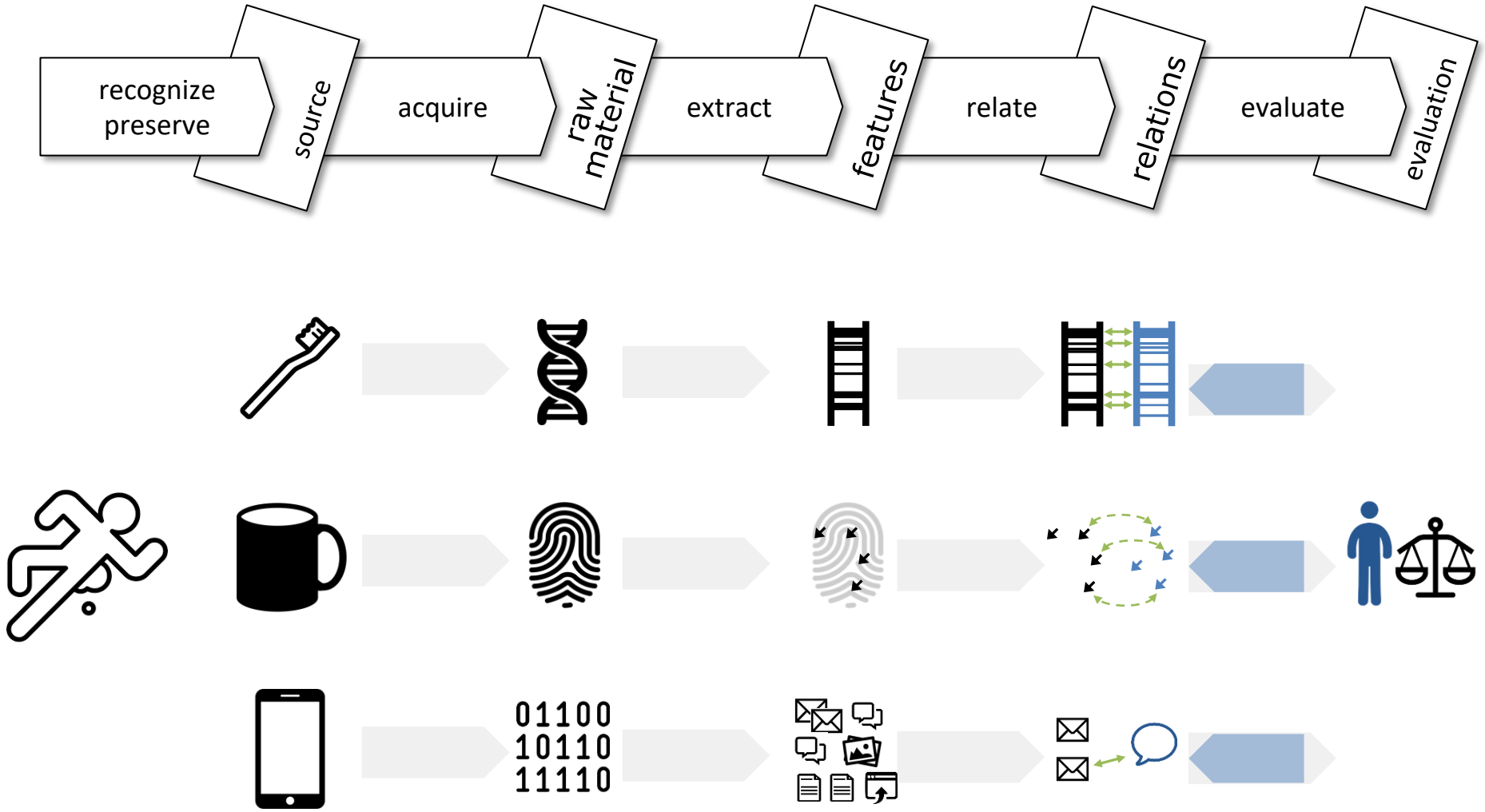
What?

How?

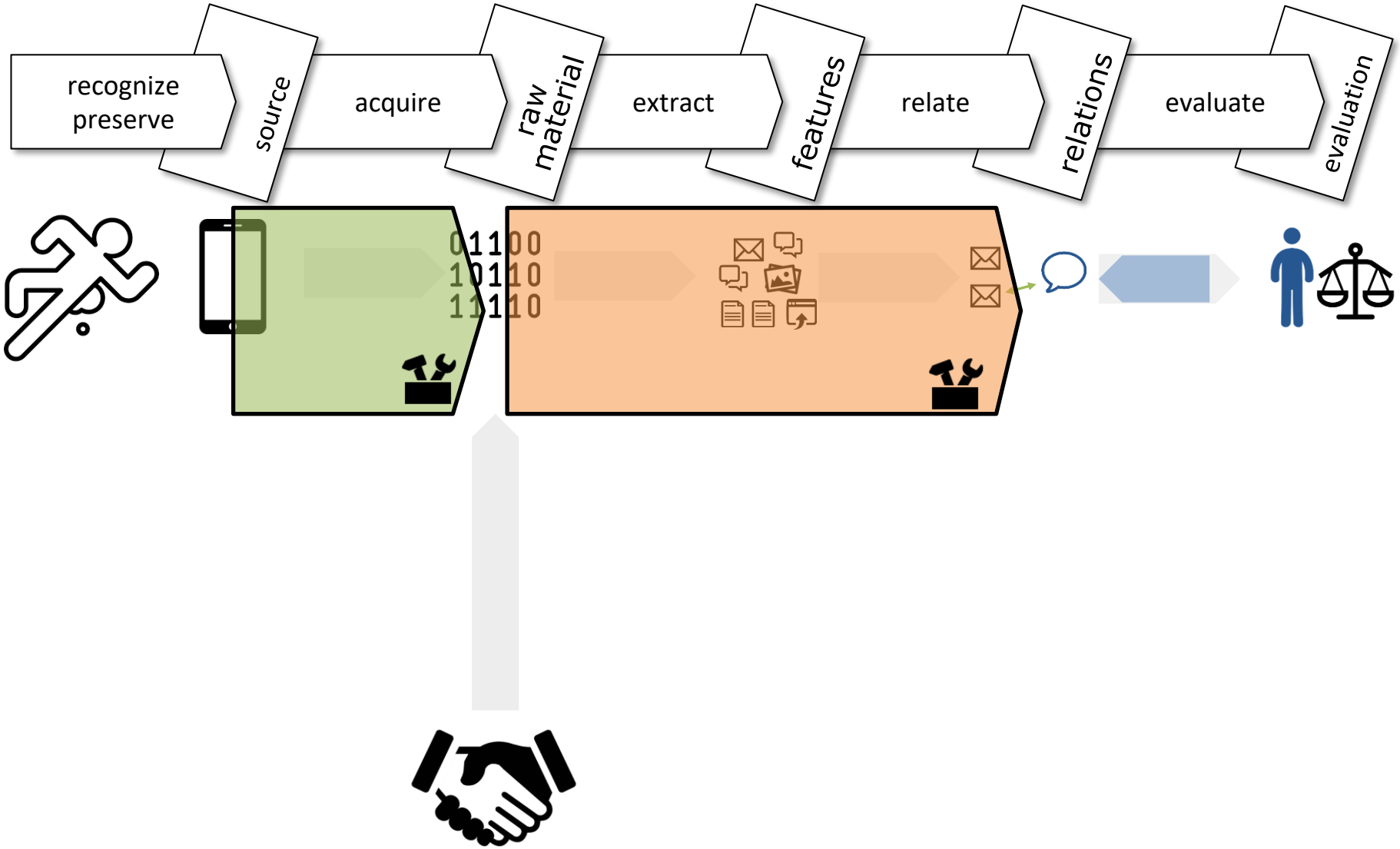
CASE

Cyber-investigation Analysis Standard Expression

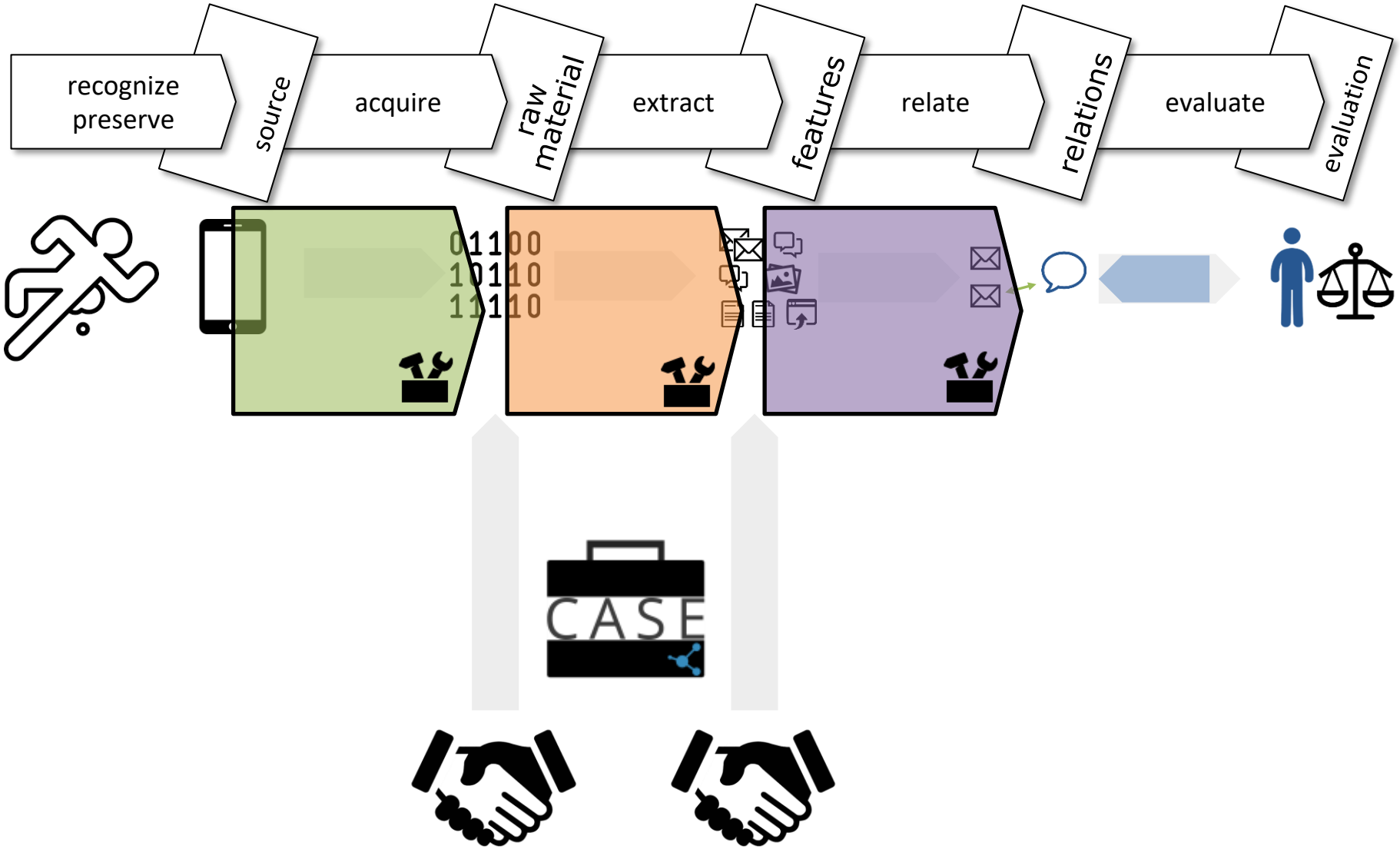
Why?



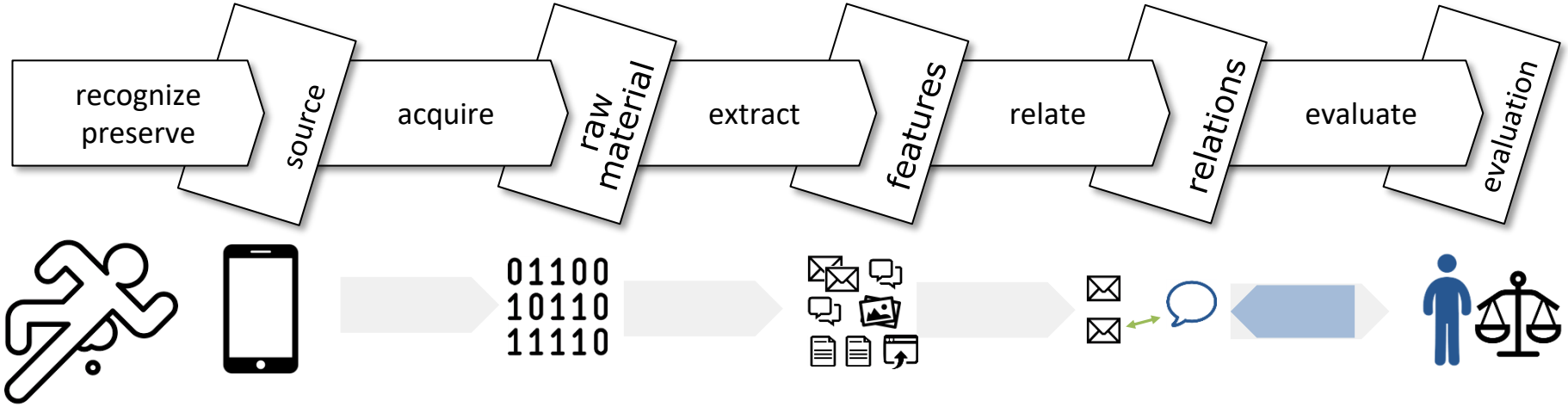
A forensic visual aid: traces versus knowledge - https://doi.org/10.1016/j.scijus.2018.08.006

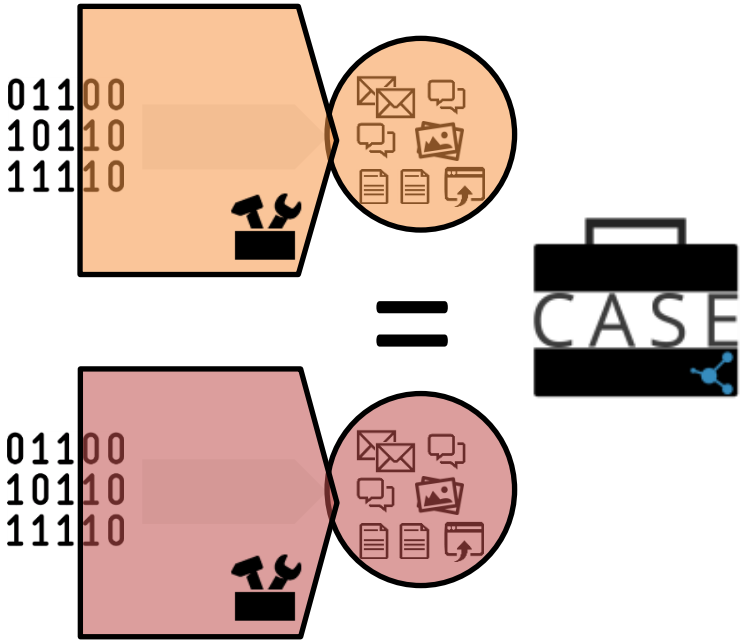


exchange intermediate results between tools

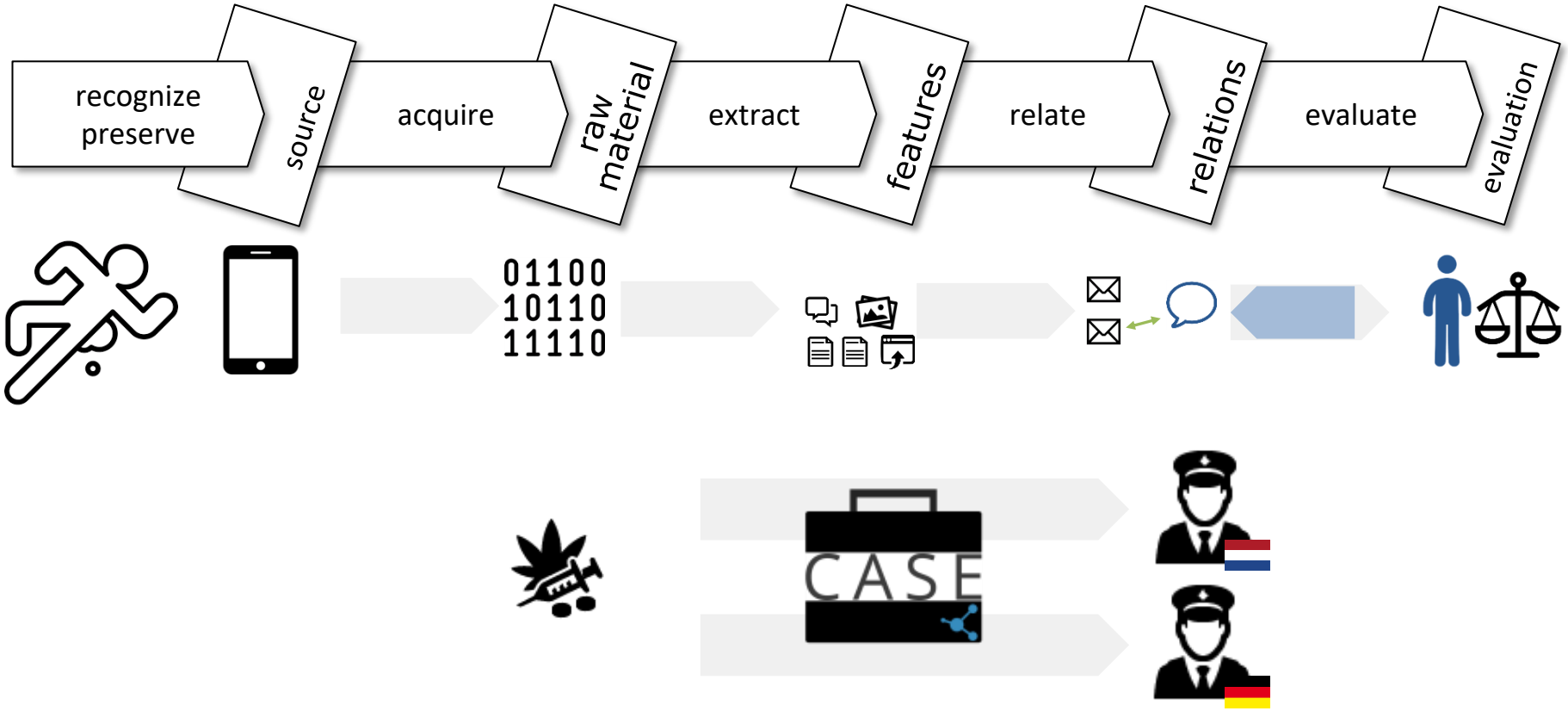


exchange intermediate results between tools





compare tool results



exchange results between organizations

CASE

Cyber-investigation Analysis Standard Expression

What?

"A strict and exhaustive schema

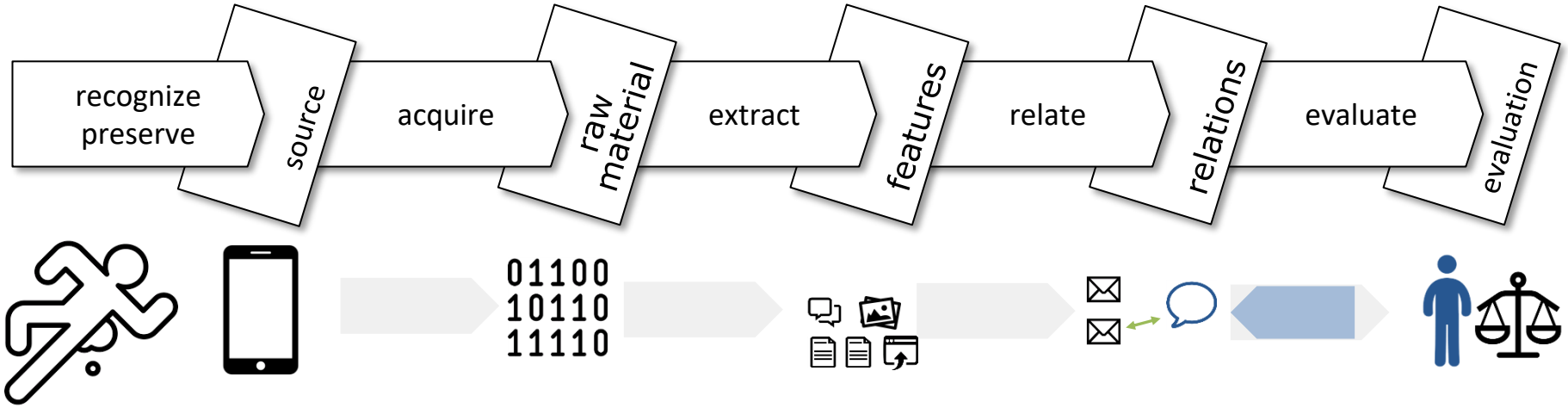
for a specific domain*,*

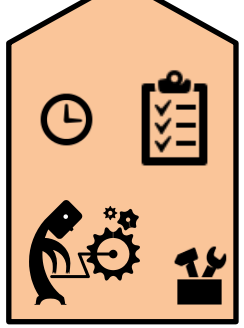
often in a hierarchical *structure,*

that defines the concepts *and their* relations*,*

as well as the rules *to which the concepts and relations must adhere within the domain."*

Becker, P., Linden, M. van der, Magrijn, H., & Sieverts, E. (2010). *Organiseer je informatie: Aan de slag met thesauri, taxonomieën, tags en topics.* Leidschendam: Biblion Uitgeverij.





metadata of the trace

reference to the source

from source to trace:

- how (tools, incl. versions/settings)
- who (user and role)
- when (date/time)
- why (forensic process)

CASE Concepts

Objects

- Traces
  - property bundles

Relationships

- embedded references
- external relationships

Annotations

Actions

- Action Lifecycles

Provenance

- Investigative Actions
  - Identity
  - Role
  - Tool
  - Location
  - Authorization
- Provenance Records

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

Proof-of-Concept Tool Integrations
- Plaso/log2timeline
- Volatility

CASE Roadmap to Version 1.0 (MVP)

Organization

development practices
internationalization of annotations
development and release procedures
documentation style guides
develop change request forms

administration setup
setup Atlassian infrastructure
organize Github repository
prepare code release

Ontology

identify MVP
map concepts to UCO constructs
identify MVP objects and properties
analyze requirements gap
prioritize concept development

clean up
multilingual documentation
upper-level object validation
define empty properties
normalize ontology

prepare MVP
define CASE namespace
define versioning scheme

develop MVP
develop MVP object and properties
release CASE version 1.0

Documentation

document context
CASE & UCO domain descriptions
CASE 1-pager

document examples
document examples including
- reference JSON-LD definition
- provenance

document MVP
document objects and properties
provide JSON-LD Context
definitions
cheat sheet
best practices

Community

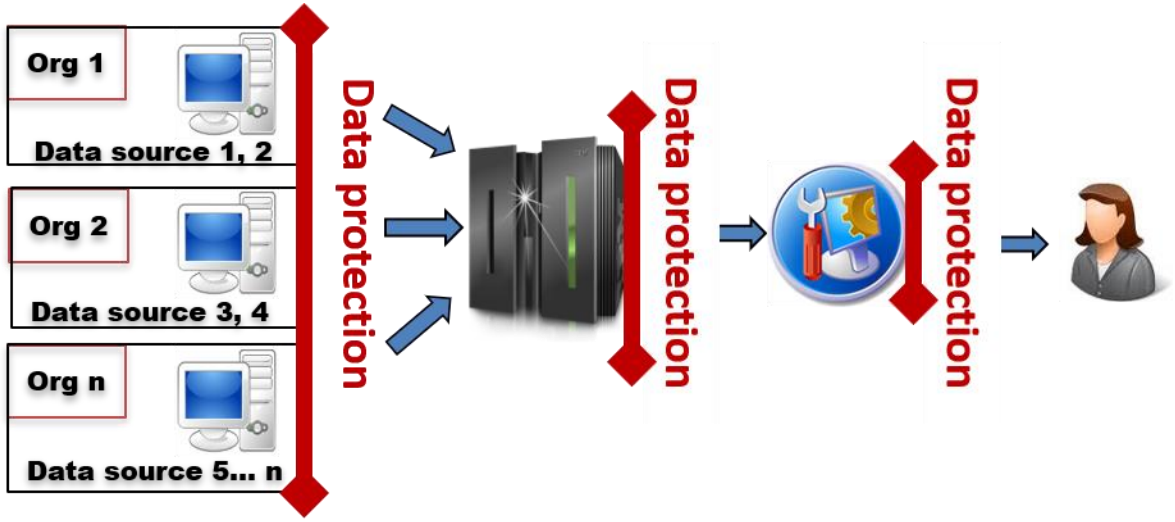
finalize community
establish Adoption committee

administration setup
setup Atlassian infrastructure
organize Github repository
prepare code release

Tools

Python tools
Update API generator
improve property cardinality support

Use Cases: Capabilities Supported by CASE



- Provide structure to support intelligent analysis
- Interoperability between systems and tools
- Maintain provenance at all phases of the cyber-investigation lifecycle
- Enhanced tool testing and validation of results
- Controlled access to privileged, proprietary, and personal information
- Capturing unsupported data structures

Eoghan Casey, CASE Presiding Director / University of Lausanne

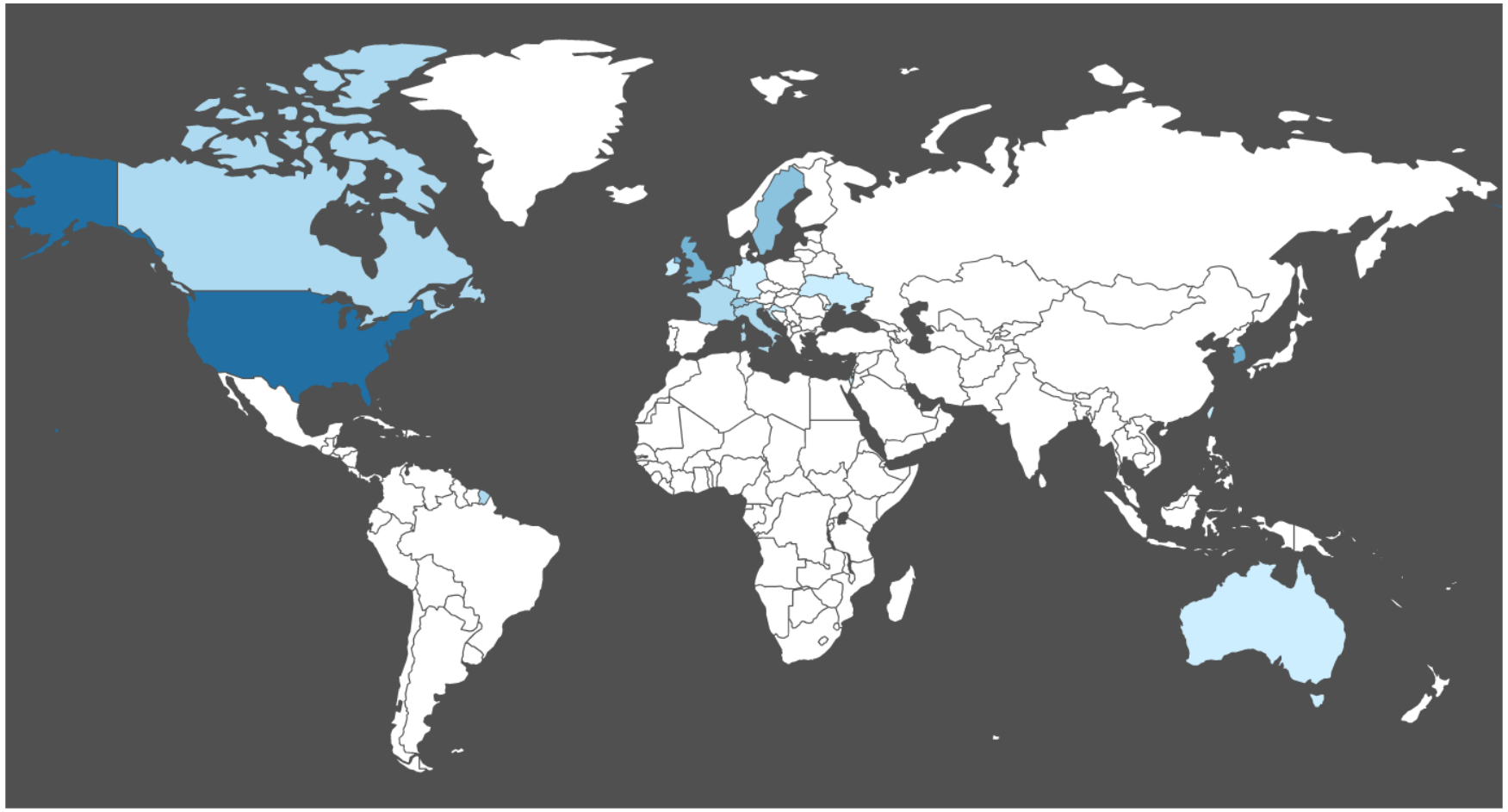
CASE COMMUNITY UPDATES

CASE

Cyber-investigation Analysis Standard Expression

Who?

The CASE Community is International



APPROVED MEMBERS

71

- 14 Non-profit
- 25 For-profit
- 16 Academia
- 16 Government/ Law Enforcement

ONTOLOGY COMMITTEE

48

COUNTRIES

17

Interested/Involved Organizations

MITRE

UNIL | Université de Lausanne

Netherlands Forensic Institute
Ministry of Justice and Security

DEPARTMENT OF DEFENSE CYBER CRIME CENTER

FireEye
Next Generation Threat Protection

MAGNET FORENSICS

UNIVERSITY OF NEW HAVEN CONNECTICUT 1920

KOREA UNIVERSITY 1905

EUROPOL
EC3 | European Cybercrime Centre

DARKLIGHT

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

OXYGEN FORENSICS

MOBILedit

cetic
Your Connection to ICT Research

IBM

i2

MSAB

BASIS TECHNOLOGY

GUIDANCE SOFTWARE

BlackBag TECHNOLOGIES

AUTOPSY DIGITAL FORENSICS

Cellebrite

VOLATILITY

EVIDENCE 2 / e-CODEX

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

NETRESEC

AccessData

nuix

CASE

And more:

- ADF Solutions
- Ajou University (Korea)
- Central
- CETIC
- CIB (Taiwan)
- CNR-IGSG
- DarkLight, Inc.
- Defense Commissary Agency (DeCA) (US)
- INTERPOL
- ITTIG (academia)
- King's College, London
- Lighthouse Global
- Longview Systems (CA)
- Marymount University
- Metropolitan Police, London
- Reality Net
- Sandia National Laboratory
- Schatz Forensics
- Semandex
- Synchrony
- Transforming Forensics (UK)
- University of Oxford
- University of Zagreb
- VM Group (IRL)
- ZITiS (Central Office for IT in the Security Sector) (Germany)

Community Organization and Leaders

2nd annual elections held Fall 2019.
Officers for CY 2020

Governance Committee

Secretary
Cory Hall
MITRE

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

Academia Class Director
Christopher Hargreaves
University of Oxford

Non-voting directors
UCO Representative

Technical Director

Harm van Beek
Netherlands
Forensic Institute

Ontology Committee

Chair

Alex Nelson
NIST

Assistant Chair

Ryan Hohimer
DarkLight

(All classes: 2+ contributors)

Adoption Committee
(CASE consumers & producers)

Chair

Vik Harichandran
MITRE

Compliance Working Group
Integration Working Group
Mapping Working Group
R & D Working Group

AC Assistant Chair & Mapping Group Lead

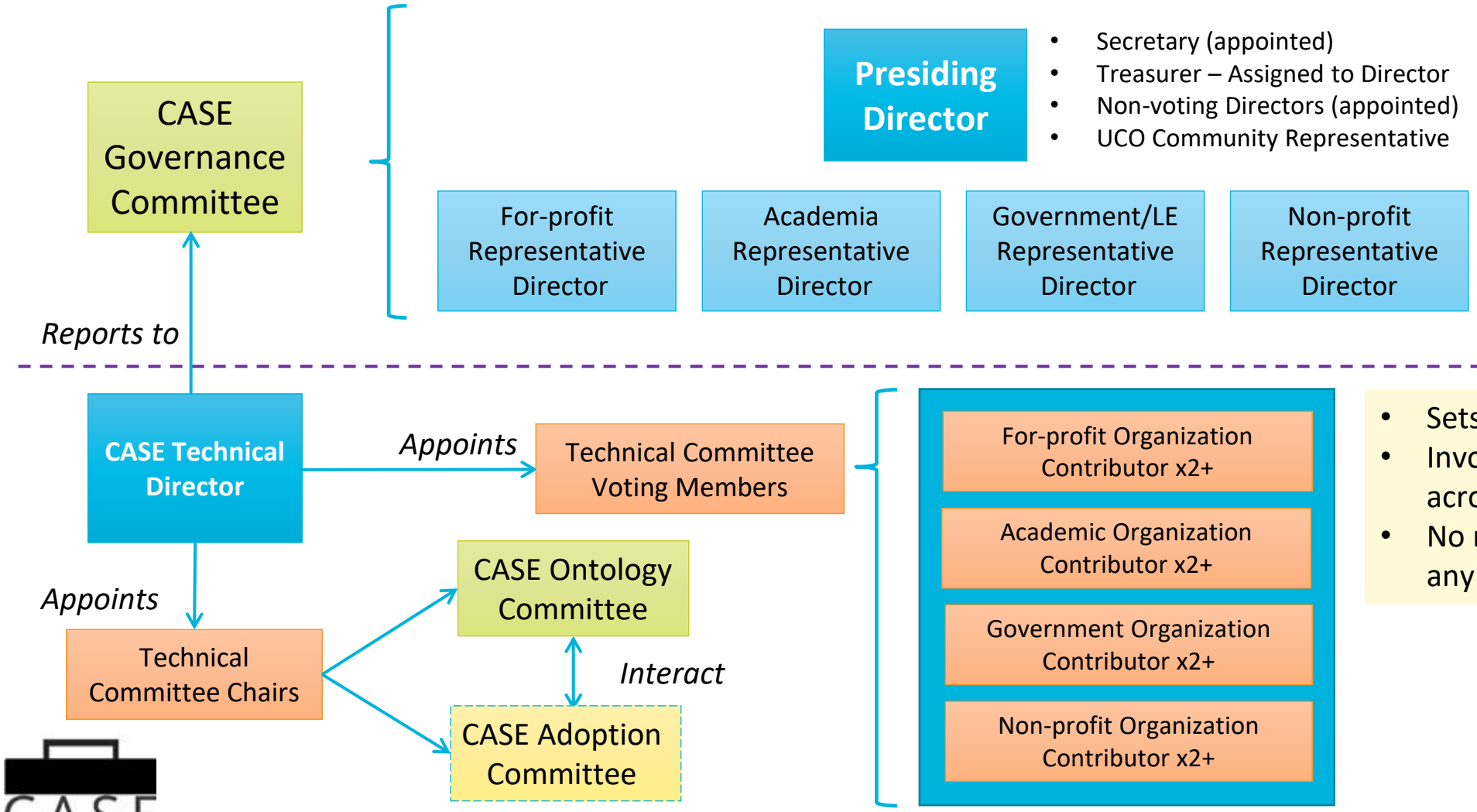
Andrew Sovern
MITRE

CASE

Cyber-investigation Analysis Standard Expression

How?

CASE Community Organization



- Focus on running the organization so the community can thrive
- Directors elected for one-year terms
- Charter new committees as necessary

- Sets technical direction for CASE
- Involves technical representatives across stakeholder communities
- No more than two appointees from any employer with voting rights

Class Representation is the Key to Success

Elected Directors appoint Advisory Committees for their class:

For-profit

- Tool Vendor
- Practitioner
- Government Contractor

Academia

- Academic Organizations
- Independent R&D Institutes

Non-profit

- Separate Non-profit

Government

- International
- National
- Sub-national
- Law Enforcement

CASE

CASE Community Membership

Online application via the CASE Community Website*

- **Active Members** are assigned to committees
  - Ontology Committee (modeling and formalization)
  - Adoption Committee (mapping and integration WGs)
- **Observer Members**
  - Receive updates from the community
  - Membership appropriate for organizational leaders and administrative staff
- **Organization Members**
  - For organizations that want to join the CASE Community (coming soon)
- Membership fee structure is in the works

* https://caseontology.org/contribute.html

CASE Community Timeline

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

2017-01 CASE v. 0.1.0 (prototype)

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

2018-04 Workshop → first Roadmap

2018-08 Community formalization started

2019-01 Organizational milestones: Officers elected; bylaws & code of conduct; Ontology Committee chartered; new website & new process workflows

2019-04 CASE Workshop at DFRWS EU 2019

2019-06 CASE Ontology Committee workshop (NIST) → updated Roadmap

2019-07 CASE Workshop at DFRWS USA 2019

2020-02 CASE in presentations at AAFS 2020

Community Resources

Community Website

www.caseontology.org

- organization
  - ✓ bylaws
  - ✓ code of conduct
  - ✓ meeting notes
- documentation
  - ✓ roadmap
  - ✓ publications
  - ✓ use cases
- online membership application

Organization*

case.atlassian.net/jira
case.atlassian.net/wiki

- meeting agendas
- works in progress
  - ✓ draft documentation
  - ✓ change proposals

CASE Ontology

github.com/casework/CASE

- RDF
  - ✓ natural language glossary
  - ✓ open issues
- documentation
  - ✓ guides

Development Forum*

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

Monthly TelCall meetings*

- Governance Committee
- Ontology Committee
- Adoption Committee (biweekly)

* Requires community membership

Deborah L. Nichols, CASE Ontology Committee / CASE Project Team, MITRE

CASE ONTOLOGY STATUS

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

CASE Ontology Status

5 June 2020

Deborah L. Nichols

CASE Ontology Committee / CASE Project Team, MITRE
DLNichols@mitre.org

CASE Ontology Activity since DFRWS EU 2019 (Oslo)

- Ontology Committee has grown to 48 active members
  - Monthly meetings and established workflow for ontology development
- Ontology Committee held an in-person working session (June 2019)
  - Identified MVP for CASE 1.0.0
  - To cover critical topics for digital evidence extraction and analysis
- CASE Workshop presented at DFRWS USA 2019 (July)
- Formalized cooperation agreement with UCO Community (Fall 2019)
- Work on MVP topics is ongoing, with planned intermediate release
- CASE 0.2.0 Release (AUG 2020)
  - Imports the Unified Cyber Ontology (UCO)
  - Includes concepts for representing investigations
  - Partial MVP topic coverage

Where We Started: CASE/UCO Prototype (CASE 0.1.0)

- Described in *Digital Investigations* 22 (2017) by E. Casey, *et al*.
- Included concepts (classes and properties) from two ontologies
  - UCO = Unified Cyber Ontology
    - Representing common kinds of objects in the cybersecurity domain
  - CASE = Cyber-investigation Analysis Standard Expression
    - Specifies investigative concepts (*e.g.*, authorization, evidence, provenance)
    - Applicable for digital forensics, incident response, criminal justice
    - Satisfies the needs of many use cases (via multi-typing ("duck-typing"))
- Used a single namespace: http://case.example.org/core#
- Encoded in OWL using Turtle (.ttl) syntax
  - Instance implementation in JSON-LD
  - Developed API and mappings conformant to the prototype

CASE Ontology Committee Work Session (June 2019)

- In-person Ontology Committee working session (Maryland, USA)
- Three-day event
  - CASE background for new members
  - Ontology tutorial
  - Discussion of CASE prototype and needed redesign (UCO import)
  - Identification of MVP (Minimum Viable Product) topics for CASE 1.0.0
- Established follow-up and workflow in monthly Ontology Committee meetings
  - Work is ongoing
- Next version of CASE (0.2.0) release: AUG 2020

New CASE Ontology Engineering

Work-in-progress by CASE Ontology Committee

- Establish the official CASE namespace DONE
- Separate CASE and UCO concepts into their respective namespaces DONE
- Process accumulated change requests for both ontologies ONGOING
  - Collaboration between CASE and UCO communities
- Migrate CASE API and mappings to CASE 1.0.0
  - Migration Guide will be published
- Update CASE examples & post to new GitHub repository DONE
  - Present examples on CASE Community website DONE
- Explore improved support for automated reasoning

CASE Imports the Unified Cyber Ontology (UCO)

- UCO Domain: Entity types applicable across all cybersecurity domains
- Release: UCO 0.3.0 (13 July 2019) *
  - https://github.com/ucoProject/UCO/releases/tag/v0.3.0
- baseURI: http://unifiedcyberontology.org
  - Example: Namespace for uco-core: http://unifiedcyberontology.org/ontology/uco/core#
- Managed by the UCO Community
  - Presiding Director: Sean Barnum (MITRE)
  - Technical Director: Ryan Hohimer (DarkLight)
- UCO GitHub: https://github.com/ucoProject/UCO

UCO 0.3.0 Metrics	
Axioms	4665
Log-ax	2166
Classes	220
O-Prop	137
D-Prop	511

* UCO 0.4.0 will be released JUNE 2020

CASE

MITRE

CASE Ontology

- CASE Domain: Concepts and terminology specific to digital investigation
- Ontology profile: OWL 2 DL (Description Logic)
- CASE 1.0.0 release planned for end-2020 (0.2.0 in AUG 2020)
- baseURI: http://caseontology.org
- Managed by the CASE Community
  - Presiding Director: Eoghan Casey (University of Lausanne)
  - Technical Director: Harm van Beek (Netherlands Forensic Institute)
  - Ontology Committee Chair: Alex Nelson ((U.S.) National Institute of Standards (NIST))
- Liaisons are appointed between the CASE and UCO ontology committees
- CASE GitHub: https://github.com/casework/CASE

Collaboration of CASE and UCO Communities

- CASE has a significant dependency on the Unified Cyber Ontology (UCO)
- CASE and UCO are working in cooperation
  - CASE and UCO have cross-representation on their Ontology Committees
  - New guidance document: *UCO and CASE Shared Development Practices*
- UCO current release: UCO 0.3.0 (13 JUL 2019)
  - About to be released: UCO 0.4.0 (JUN 2020)
- CASE current release: CASE 0.1.0 (13 JUL 2019)
  - Next release: CASE 0.2.0 (AUG 2020) – mappers are already working with the development branch of 0.2.0
  - CASE 1.0.0 planned for end-2020

CASE 1.0.0 – MVP Topics & Priority

- At June 2019 work sessions, CASE OC identified & prioritized topics to be covered by CASE version 1.0.0
- MVP topic workflow
  - *Topic narrative* is created by user(s) & reviewed by committee
  - *Concepts needed* to cover the topic are listed
  - *Ontology components* are identified in CASE+UCO or newly created (w/*IRIs*)
  - *Examples* using concepts are developed in JSON-LD & tested
- CASE Ontology Committee members work on MVP topics
- Concept-coverage for each topic may be in CASE or UCO, depending on scope
- New concept requests use appropriate ontology-development process
- Initial subset of MVP topics will be covered in CASE 0.2.0
- MVP process is also identifying post-1.0.0 topics

MVP Topics for CASE 1.0.0

Topics in priority order

1. Chain of Custody In Progress
2. Email Phishing In Progress
3. Messages
4. Pictures In Progress
5. Call Logs
6. Video
7. Audio Files
8. Documents
9. Database Files
10. Contacts
11. File System
12. Location
13. Installed Apps
14. Passwords, Tokens, Credentials
15. URLs / Browsing History In Progress
16. Network
17. Device Info

CASE

MITRE

MVP Topic 1: Chain of Custody – Narrative

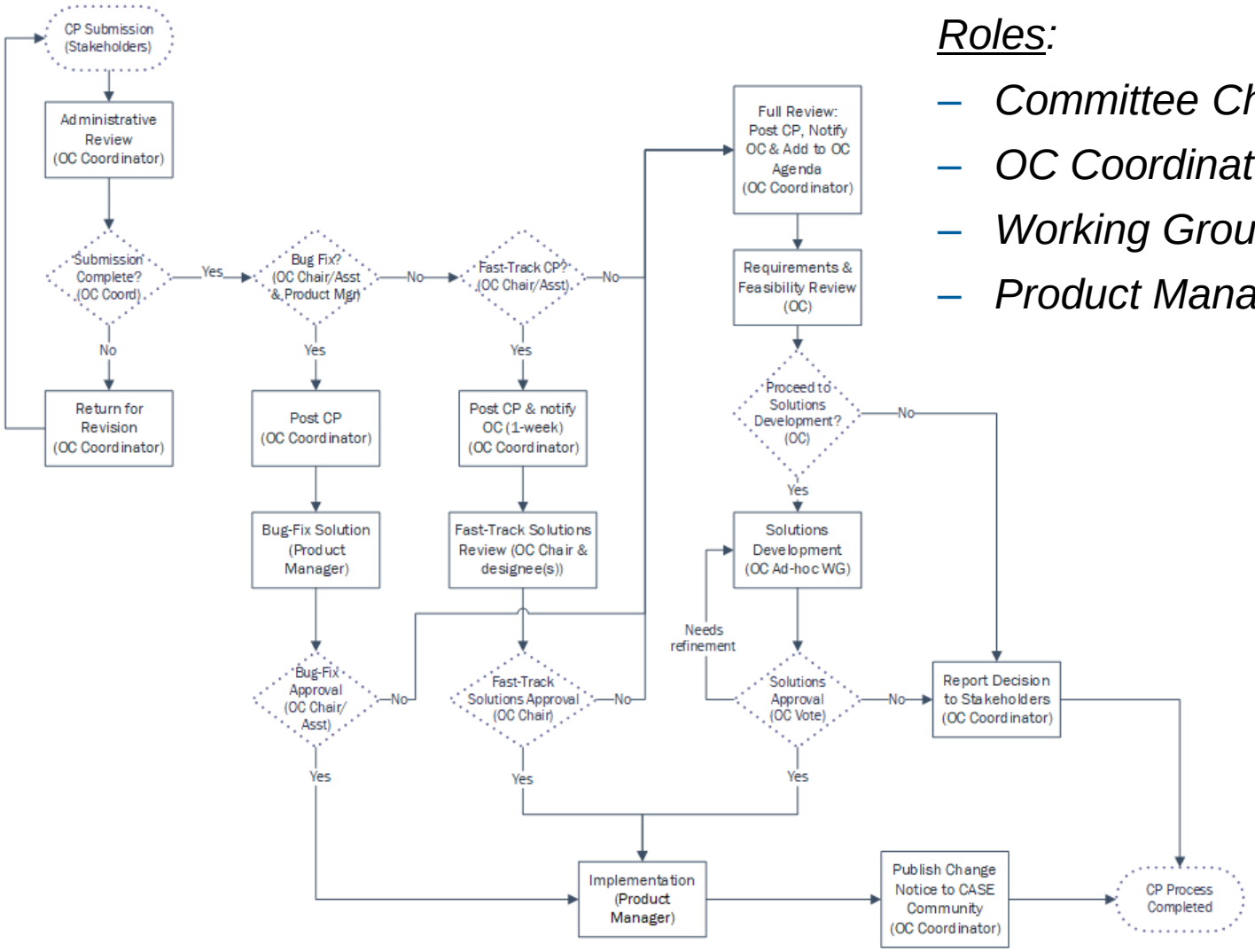
- Any investigation involving digital data must maintain chain of custody of the data to establish its authenticity and reliability.
  - Details about the data source, such as a computer or mobile device.
  - Details about the tools and transformations that led from acquired raw data to the resulting product.
- Provenance information tracks *who* processed digital evidence, *when*, *where*, *how*, and any *tool* and *method* used (with relevant *parameters*).
  - Includes the case name, evidence numbers, date/time seized, target system, evidence description, person who accessed the evidence, location of evidence, date/time when destroyed.
  - Also includes hash values of extracted digital information, including any associated malware, hash value for files/pages generated by malware, pieces of computer code, etc.

Chain of Custody Concepts – Existing or New

- ProvenanceRecord:
  - exhibitNumber
  - description - Annotation
  - object
  - priority NEW
- Action: NEW
  - [evidence] “received”, “verified”, “accepted”
  - startTime & endTime
  - performer
  - location
  - instrument (if applicable)
  - object
  - result
- Role
  - hasRelationship
- Identity:
  - SimpleName
    - givenName
    - familyName
  - Organization
- Location:
  - SimpleAddress
  - locality
  - postalCode
- Trace (UCO CyberItem)

New Concepts Feed into Ontology Development Process

- Development Requests (DR) & Change Proposals (CP)
- Requirements Review
- Collaboration with UCO
- 3-track CP Process
  - Bug fixes
  - Fast-track
  - Full formal review
- Technical Solutions
- Change Notifications



Roles:

- *Committee Chair*
- *OC Coordinator*
- *Working Groups*
- *Product Manager*

CASE Ontology Committee Manages Development

- The standing Committee responsible for the CASE Ontology, it acts as:
  - *Working group* for management and publication of the CASE Ontology
  - *Coordination body* for all CASE Ontology change requests
  - *Advisory group* to the CASE Technical Director
- Meets regularly (monthly & as-needed)
  - Conducts CASE requirements reviews and develops technical solutions
  - Coordinates & collaborates with the UCO Ontology Committee
- Provides expertise in ontology and/or data modeling in one or more cyber-investigation sub-domains
- Is responsible for CASE Ontology development
- Interacts with the CASE Adoption Committee to support adopters

Getting Involved

- Who: CASE Ontology Committee
- What: Ontology development processes
  - Use cases, requirements review, change requests & solutions development
- Where: Online meetings and occasionally in-person
- When: Monthly Ontology Committee meetings
  - Working groups may meet more frequently on special projects.
- Why: Promote a standard ontology to support data interoperability and automated reasoning for cyber-investigations
  - Bring your use cases to the community
  - Ensure your domain knowledge is represented in CASE
- How: Join us! https://caseontology.org/contribute.html

Vik Harichandran, CASE Adoption Committee Chair / CASE Project Team, MITRE

CASE ADOPTION COMMITTEE STATUS

CASE Adoption Committee

Vik Harichandran

CASE Adoption Committee Chair / CASE Project Team, MITRE

vharichandran@mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

MITRE Approved for public release under PRS 18-4297

Adoption Committee (AC)

- **CASE Adoption Committee established (March 2020)**
  - Mapping WG
  - Integration WG (consumers & producers)
  - Framework WG
- **AC responsibilities involve anything that supports the Ontology Committee in doing their job better, and for new adopters to more easily integrate CASE into their tools (i.e. software and mappings).**

Adoption Committee

(CASE consumers & producers)

Chair

Vik Harichandran
MITRE

Compliance Working Group

Integration Working Group

Mapping Working Group

R & D Working Group

AC Assistant Chair &
Mapping Group Lead

Andrew Sovern
MITRE

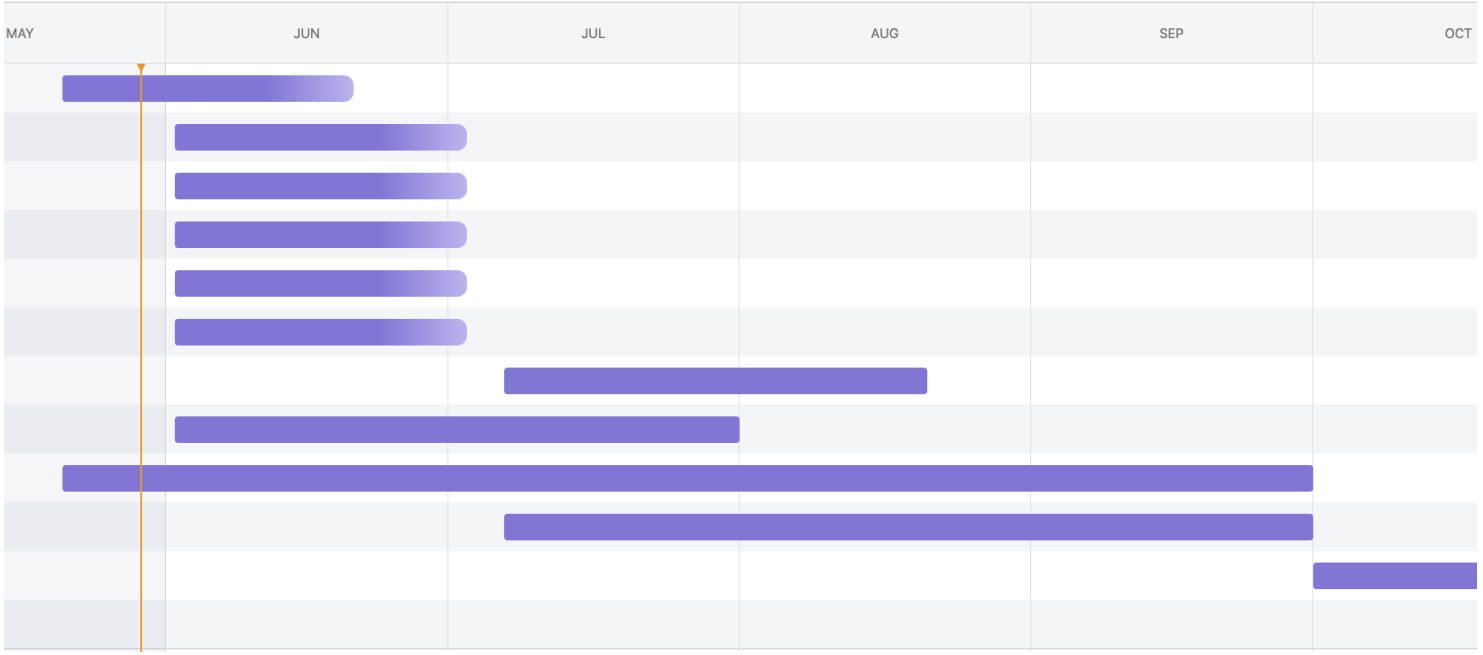
MITRE

Jira Tasks

- **MVP / current**
  - Python Verifier is our only verification at this point. It needs to be updated.
  - Mapping Guide will be published soon (if not already up by the date of this conference).
  - JSON-LD examples and implementation POCs need to be reviewed to assure alignment with MVP terminology and support.
- **Future**
  - SHACL and framing support
  - Packaging transformations into a single CASE “package” for download
  - Using CETIC’s ORS POC to support analytic view/example sandbox
  - Automate all the things! #DevOps #RobotsAreBetterThanHumans

Roadmap

Epic
0: Baseline & Policies
1: JSON-LD
2: CASE F.A.Q.
3: Adopters Welcome Guide (Google Drive -> Website)
4: Operations Guide (Google Drive)
5: Mapping Guide (Google Drive)
6: Adoption Guide (Google Drive -> Website)
7: Templating Transformations
8: Implementations
9: API Transformations
Post-MVP: Triplestores, Visualizations, & Correlation



Adoption Committee (AC)

Current membership consists of

- CETIC
- UK Met Police
- BlackBag Technologies (now subsidiary of Cellebrite)
- MITRE

Future membership

- Join the Framework or Integration WGs, and code the future of CASE !!!
- All adopters of CASE should have a representative in the Integration WG
- Create a plugin for your work so that it can be ingested into household names

→ CASE → GitHub Tool → CASE →

Break Now! After the Break: CASE Illustrative Examples

- Mapping Mobile Forensics Tools Output to the CASE Standard
  - Mattia Epifani, CNR, Institute of Legal Informatics and Judicial Systems
  - Claudia Meda, Reality Net System Solutions
  - Fabrizio Turchi, CNR, Institute of Legal Informatics and Judicial Systems
- Utilising the CASE Standard to View Bespoke File Systems
  - Gregory Webb, London Metropolitan Police, U.K.
- CASE Mapping Tutorial
  - Andrew Sovern, MITRE

CASE

15-MINUTE BREAK

Cyber-investigation Analysis Standard Expression (CASE)

ILLUSTRATIVE EXAMPLES

Mattia Epifani, CNR / Institute of Legal Informatics and Judicial Systems
Claudia Meda, Reality Net Systems Solutions
Fabrizio Turchi, CNR / Institute of Legal Informatics and Judicial Systems

MAPPING MOBILE FORENSICS TOOLS OUTPUT TO THE CASE STANDARD

ACTIVITIES, OBJECTIVES, OUTCOME

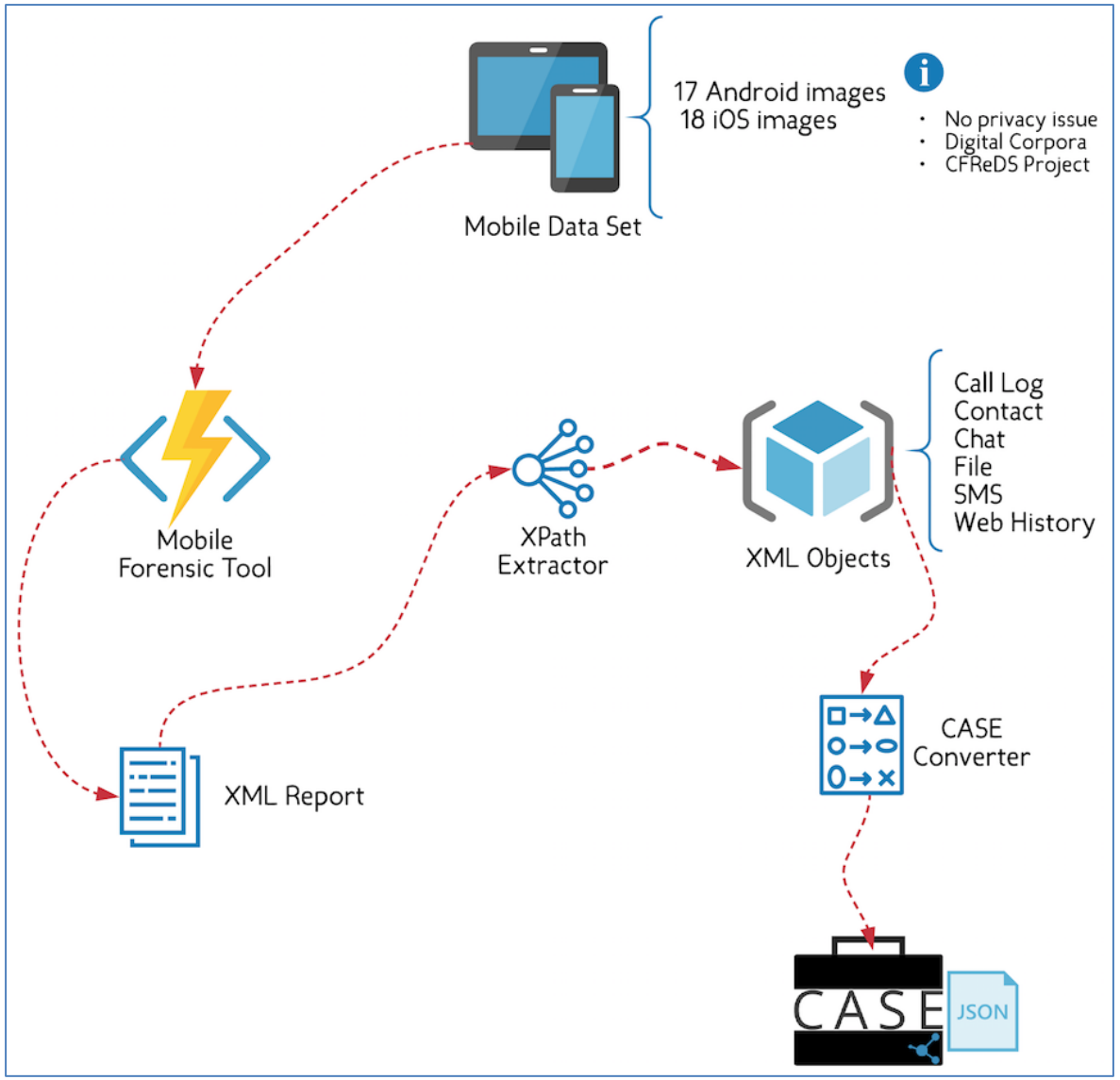
- **Activities**
  a. Parsing output of forensics tools to conform to standards
  b. Reference digital forensics domain model (CASE)

- **Objectives**
  a. Converting the output (XML Report) from the most popular forensic tools into CASE
  b. Extending/Improving the CASE model related to the information not covered yet

- **Outcome**
  a. Internal report on parser specification to convert Mobile Forensic Tools Output (XML) in CASE
  b. Light parsers only for demonstration purpose

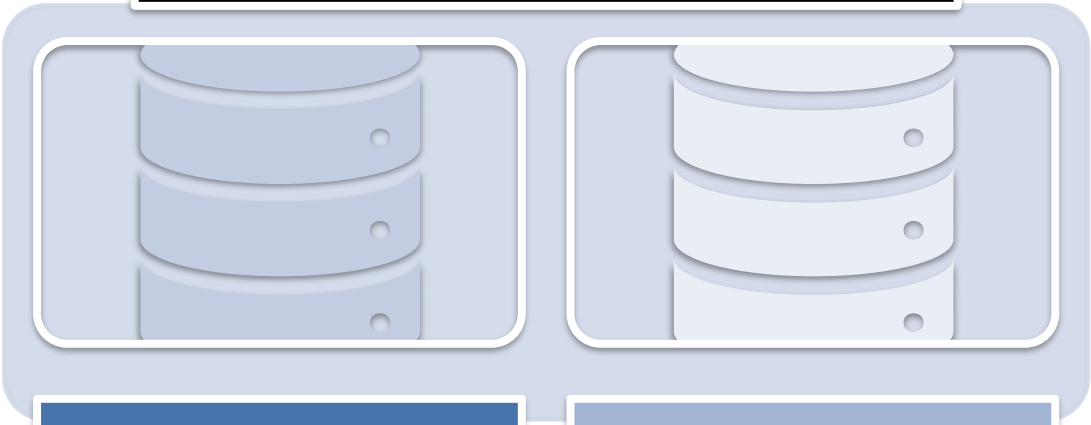
CASE

ACTIVITIES, OBJECTIVES, OUTCOME



DATASET

40 forensic acquisitions



19 android images

21 iOS images

DATASET

- **14** downloaded from **CFReDS Project**

- https://www.cfreds.nist.gov/mobile/

- **5** downloaded from **Josh Hickman / Digital Forensics Corpora**

- https://digitalcorpora.org/corpora/cell-phones/android-7
- https://digitalcorpora.org/corpora/cell-phones/android-8
- https://digitalcorpora.org/corpora/cell-phones/android-9

CASE

DATASET

- **17** iOS backups downloaded from **CFReDS project – Drones sections**

- https://www.cfreds.nist.gov/drone-images.html

- **1** iOS Physical image downloaded from CFReDS Project

- https://www.cfreds.nist.gov/mobile/cellebrite/index-images.htm

DATASET

android

ID	Dataset	Phone model	OS	Acquisition Method
01_HTC_Desire_626_Chip_Off	CFREDS	HTC Desire 626	6.0.1	Chip Off
02_HTC_Desire_S_Chip_Off	CFREDS	HTC Desire S	2.3.5	Chip Off
03_HTC_Desire_S_JTAG	CFREDS	HTC Desire S	2.3.5	JTAG
04_HTC_One_Mini_Chip_Off	CFREDS	HTC One Mini	4.4.2	Chip Off
05_HTC_One_Mini_JTAG	CFREDS	HTC One Mini	4.4.2	JTAG
06_HTC_One_XL_Chip_Off	CFREDS	HTC One XL	4.1.1	Chip Off
07_HTC_One_XL_JTAG	CFREDS	HTC One XL	4.1.1	JTAG
08_LG_K7_Chip_Off	CFREDS	LG K7	5.1.1	Chip Off
09_LG_E510_JTAG	CFREDS	LG Optimus	>= 2.3	JTAG
10_Moto_E_Chip_Off	CFREDS	Moto E	5.1	Chip Off
11_Samsung_S2_Chip_Off	CFREDS	Samsung S2	4.1.2	Chip Off
12_Samsung_S4_Chip_Off	CFREDS	Samsung S4	4.4.4	Chip Off
13_Samsung_S4_JTAG	CFREDS	Samsung S4	4.4.4	JTAG
14_ZTE_Z970_Chip_Off	CFREDS	ZTE Z970	4.4.4	Chip Off
15_LG_H790_UFED_NOUGAT	DigitalCorpora	LG H790	7.1.2	UFED 4PC
16_LG_H790_UFED_OREO	DigitalCorpora	LG H790	8.1	UFED 4PC
17_GOOGLE_PIXEL	DigitalCorpora	Google Pixel 3	9.0	UFED 4PC

CASE

DATASET iOS

ID	Dataset	Phone model	OS	Acquisition Method
DF061_DJI_PHANTOM_4	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF062_DJI_PHANTOM_4	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF063_DJI_PHANTOM_4	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF067_DJI_MAVIC_2_ZOOM	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF068_DJI_MAVIC_2_ZOOM	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF069_DJI_MAVIC_2_PRO	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF070_QYSEAE_FISH_P3	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF071_QYSEAE_FISH_P3	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF072_QYSEAE_FISH_P3	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF075_PARROT_BLUEGRASS	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF076_PARROT_BLUEGRASS	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF077_PARROT_ANAFI	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF078_PARROT_ANAFI	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF079_PARROT_ANAFI	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF080_MAVIC_2_ENTERPRISE	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF081_MAVIC_2_ENTERPRISE	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
DF082_MAVIC_2_ENTERPRISE	DRONEFOR	iPad Mini 4	11.4	IOS BACKUP
CFREDS_IPHONE_3GS	CFREDS	iPhone 3GS	4.3.1	IOS PHYSICAL

PROCESSING WITH MOBILE FORENSICS TOOLS

All the images were processed by using
4 mobile forensic tools

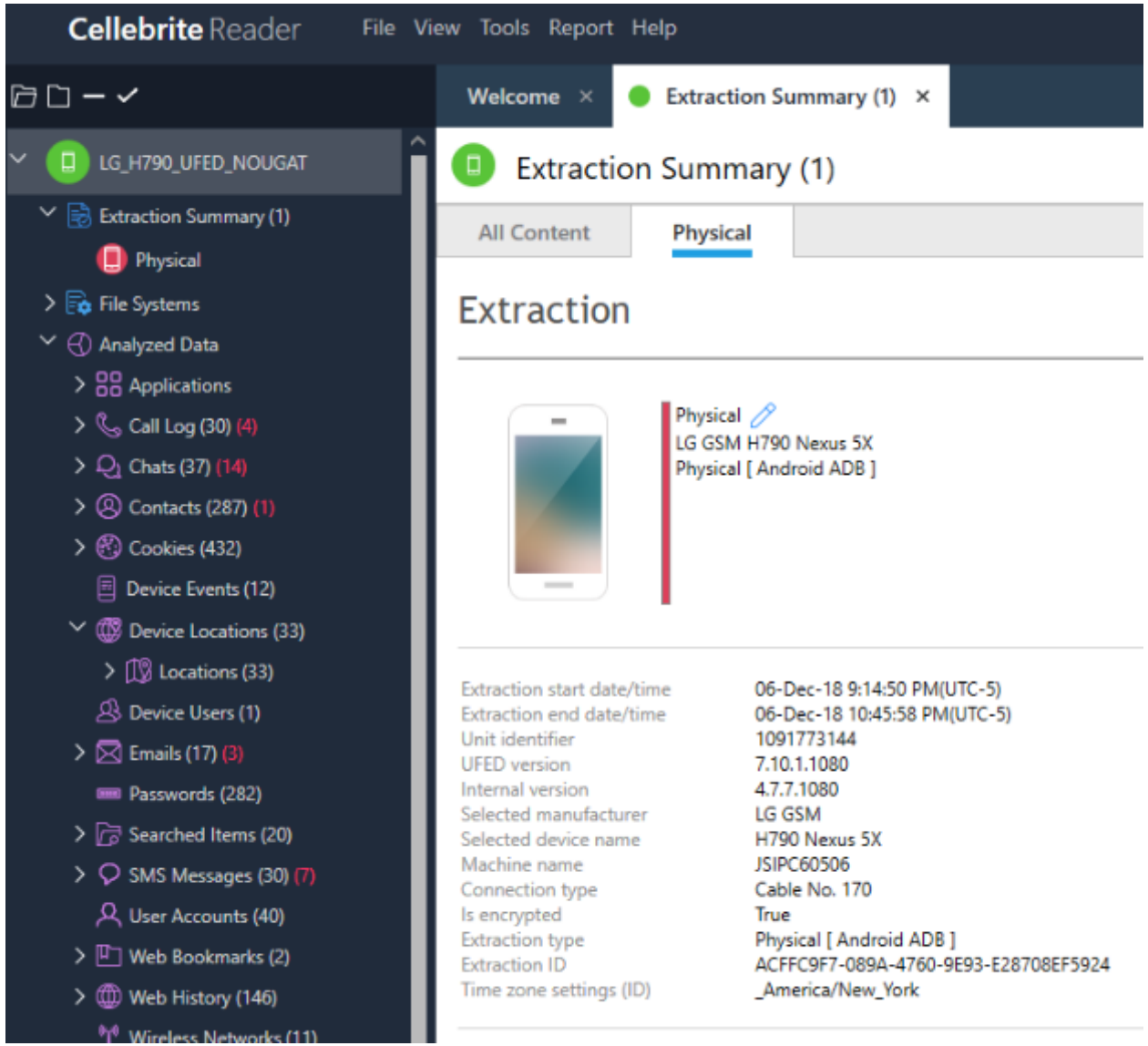
Software	**Version**
UFED Physical Analyzer	7.24.0.209
Oxygen Forensics Suite	12.0.0.151
Magnet AXIOM	3.8.0
MSAB XAMN	4.4.0

PROCESSING WITH MOBILE FORENSICS TOOLS

EXAMPLE

Cellebrite PA

Software	Version
UFED Physical Analyzer	7.24.0.209
IMAGE ID	
15_LG_H790_UFED_NOUGAT	



CASE

PROCESSING WITH MOBILE FORENSICS TOOLS

EXAMPLE

Cellebrite PA

Software	Version
UFED Physical Analyzer	7.24.0.209
IMAGE ID	
15_LG_H790_UFED_NOUGAT	

Device Info

Find:

General	
Android fingerprint	google/bullhead/bullhead:7.1.2/N2G47O/385...
Detected Phone Model	Nexus 5X
OS Version	7.1.2
Detected Phone Vendor	google
Android ID	4d2d47650ddb38e1
Bluetooth device name	Nexus 5X
Bluetooth device address	64:BC:0C:F5:D1:C9
Phone Activation Time	29-Nov-18 5:58:19 PM(UTC+0)
Time Zone	(UTC-05:00) New_York (America)
Location Services Enabled	True
ICCID	89014104279705559755
IMSI	310410970555975
Advertising Id	c692feb2-3361-45e4-8515-5a8da3a3eacd
Recovery Event	
1	1970-01-18T21:39:27.000-05:00
2	1970-05-25T10:11:34.000-04:00
3	1970-04-16T10:12:20.000-05:00
4	1969-12-31T18:23:03.000-05:00
5	1970-06-19T01:05:23.000-04:00
6	1970-07-18T04:41:19.000-04:00
7	1970-04-19T15:08:24.000-05:00
8	1970-04-16T22:42:34.000-05:00
9	1970-08-09T01:46:56.000-04:00
10	1970-02-27T00:32:41.000-05:00
11	1970-04-19T12:10:33.000-05:00
Tethering	
Hotspot password required	ce5047f6f1a2

CASE

PROCESSING WITH MOBILE FORENSICS TOOLS

EXAMPLE

Cellebrite PA

Software	Version
UFED Physical Analyzer	7.24.0.209
IMAGE ID	
15_LG_H790_UFED_NOUGAT	

Extraction start date/time	06-Dec-18 9:14:50 PM(UTC-5)
Extraction end date/time	06-Dec-18 10:45:58 PM(UTC-5)
Unit identifier	1091773144
UFED version	7.10.1.1080
Internal version	4.7.7.1080
Selected manufacturer	LG GSM
Selected device name	H790 Nexus 5X
Machine name	JSIPC60506
Connection type	Cable No. 170
Is encrypted	True
Extraction type	Physical [Android ADB]
Extraction ID	ACFFC9F7-089A-4760-9E93-E28708EF5924
Time zone settings (ID)	_America/New_York

CASE

PROCESSING WITH MOBILE FORENSICS TOOLS

EXAMPLE

Cellebrite PA

Software	Version
UFED Physical Analyzer	7.24.0.209
IMAGE ID	
15_LG_H790_UFED_NOUGAT	

Physical
LG GSM H790 Nexus 5X
Physical [Android ADB]

Extraction start date/time	06-Dec-18 9:14:50 PM(UTC-5)
Extraction end date/time	06-Dec-18 10:45:58 PM(UTC-5)
Unit identifier	1091773144
UFED version	7.10.1.1080
Internal version	4.7.7.1080
Selected manufacturer	LG GSM
Selected device name	H790 Nexus 5X
Machine name	JSIPC60506
Connection type	Cable No. 170
Is encrypted	True
Extraction type	Physical [Android ADB]
Extraction ID	ACFFC9F7-089A-4760-9E93-E28708EF5924
Time zone settings (ID)	_America/New_York

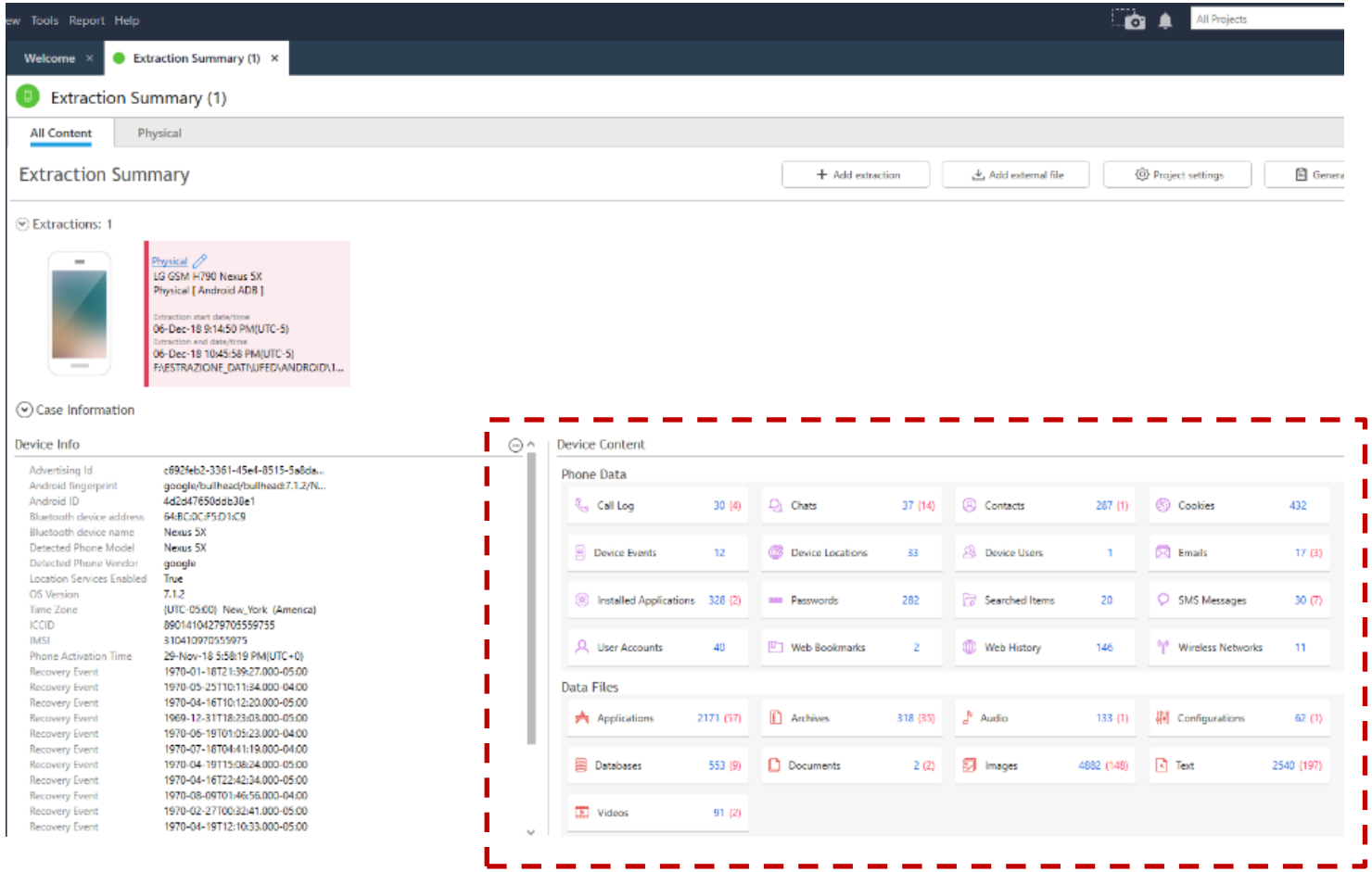
CASE

PROCESSING WITH MOBILE FORENSICS TOOLS

EXAMPLE

Cellebrite PA

Software	Version
UFED Physical Analyzer	7.24.0.209
IMAGE ID	
15_LG_H790_UFED_NOUGAT	



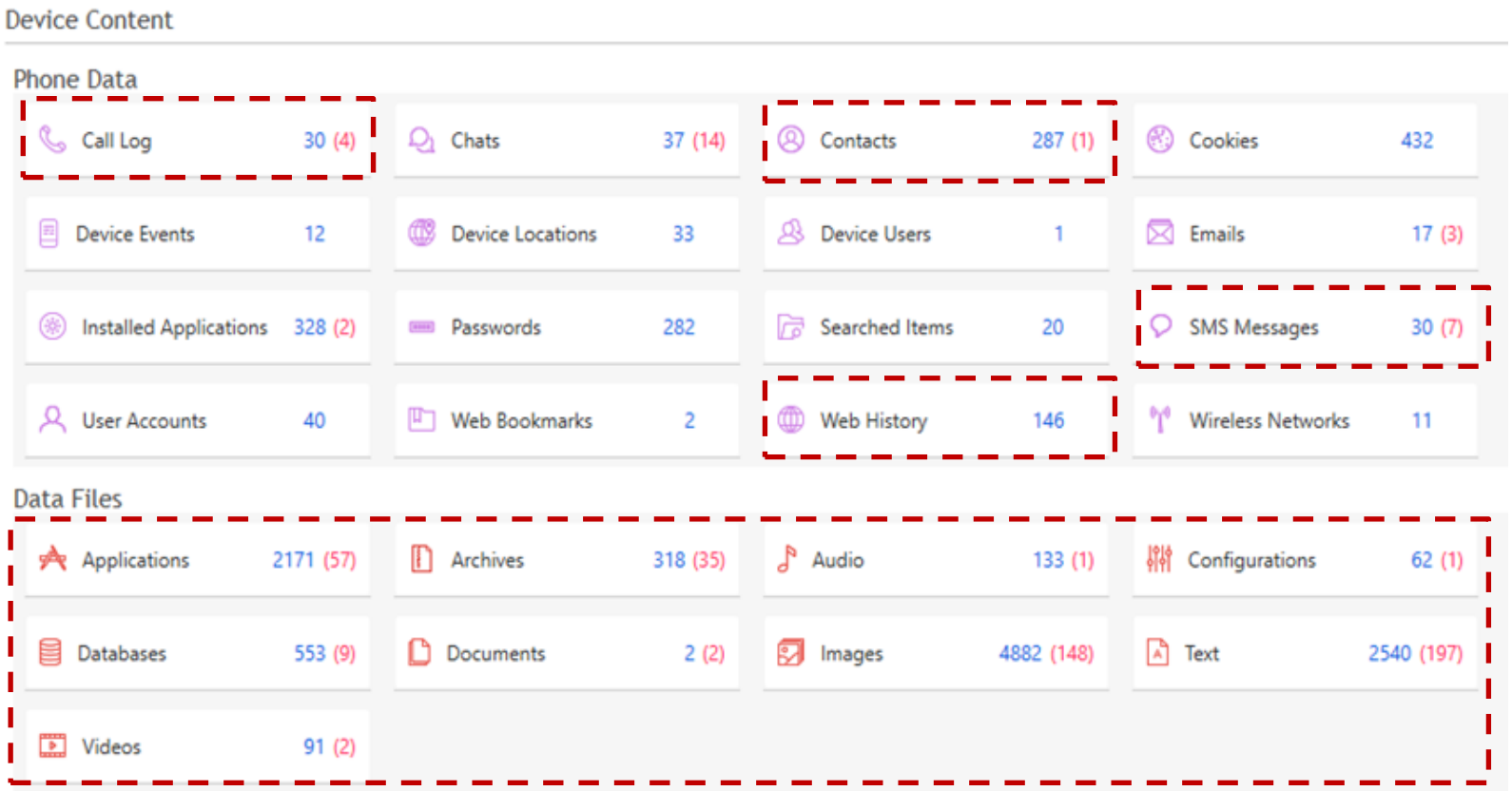
CASE

PROCESSING WITH MOBILE FORENSICS TOOLS

EXAMPLE

Cellebrite PA

Software	Version
UFED Physical Analyzer	7.24.0.209
IMAGE ID	
15_LG_H790_UFED_NOUGAT	



CASE

AFTER PROCESSING: THE EXTRACTION

Data extracted in **2 different formats:**

1) **XML Format** – based on the specific tool schema

2) **Proprietary Format** – available with specific reader provided by software company

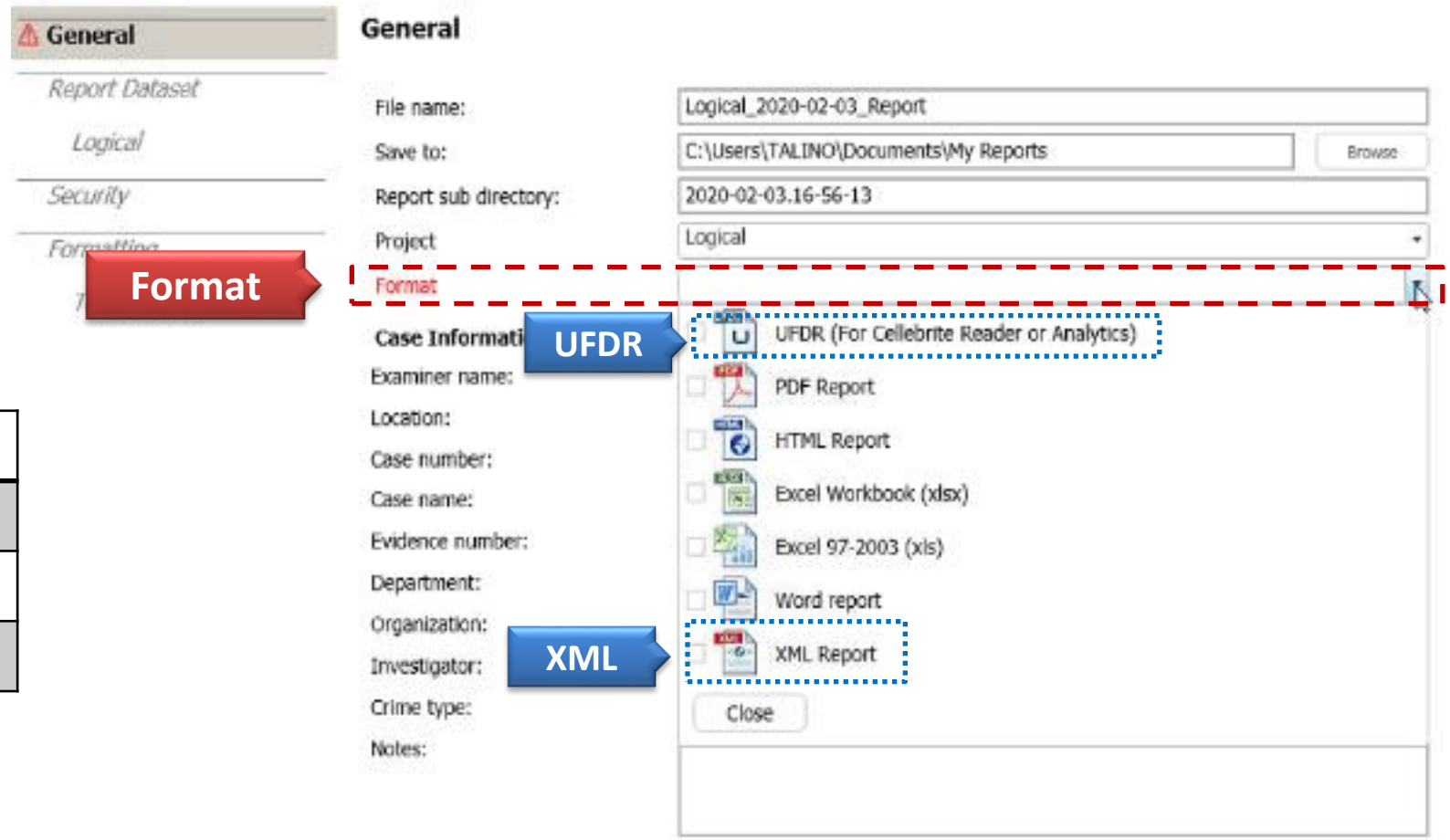
Software	Format	Viewer
UFED Physical Analyzer	UFDR	UFED Reader
Oxygen Forensics Suite	OFBX	Oxygen Viewer
Magnet AXIOM	MFDB	Magnet Examiner
MSAB XAMN	XRY	XAMN Portable

EXTRACTION

EXAMPLE

Cellebrite PA

Software	Version
UFED Physical Analyzer	7.24.0.209
IMAGE ID	
15_LG_H790_UFED_NOUGAT	



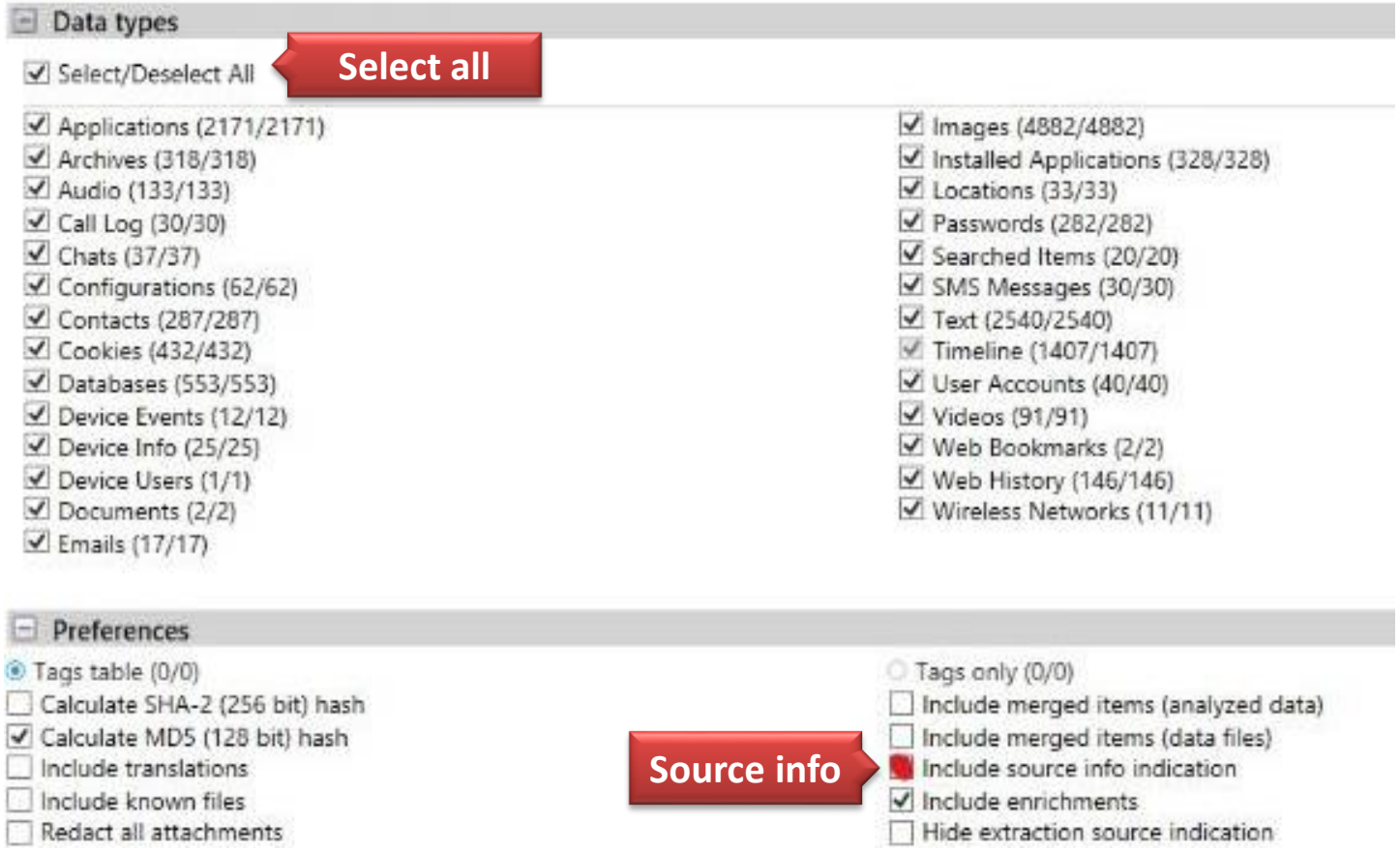
CASE

EXTRACTION

EXAMPLE

Cellebrite PA

Software	Version
UFED Physical Analyzer	7.24.0.209
IMAGE ID	
15_LG_H790_UFED_NOUGAT	



CASE

EXTRACTION

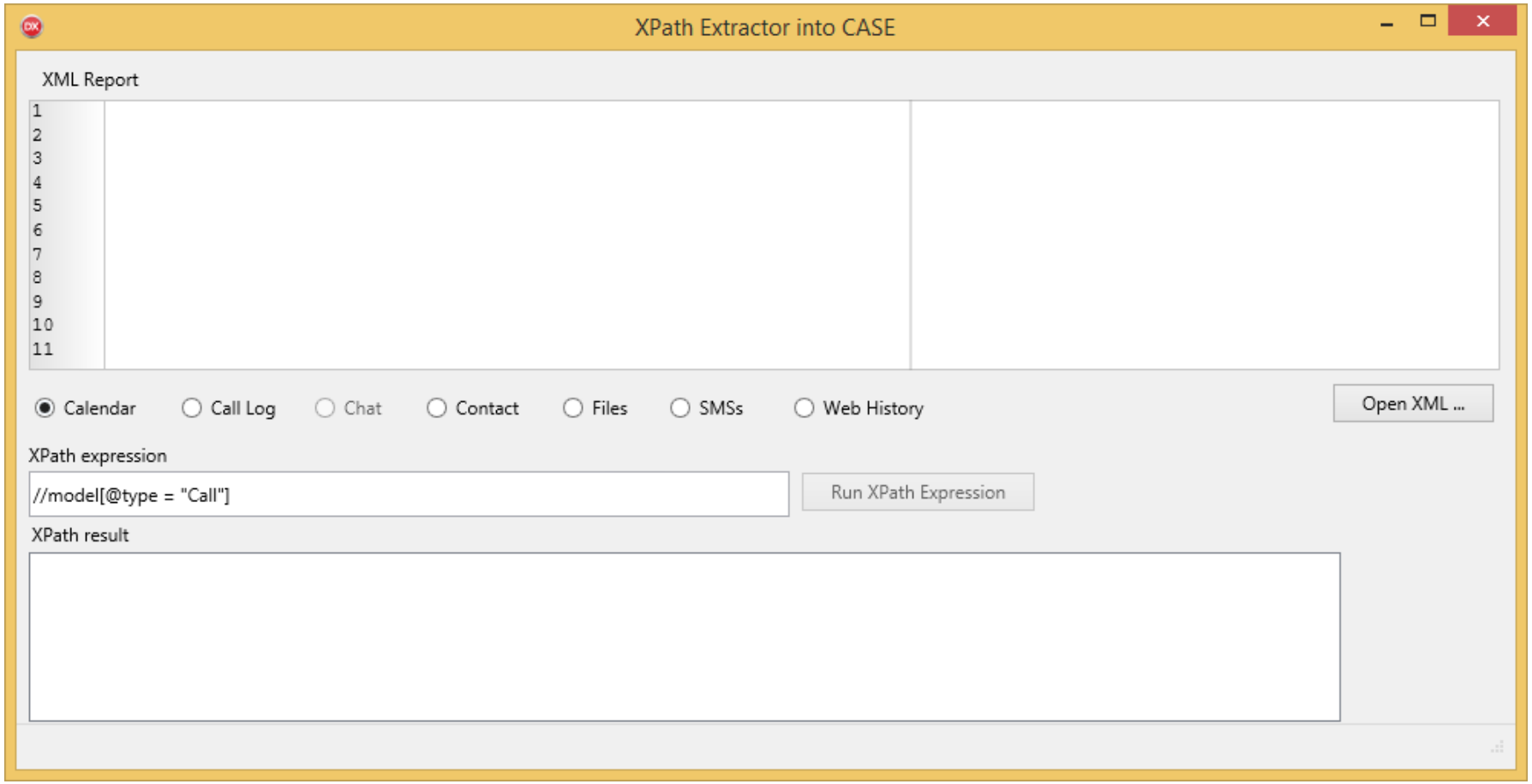

```
<?xml version="1.0" encoding="utf-8"?>
<project id="ce400713-d75d-4af9-a966-69468e675ff8" name="LG GSM_H790 Nexus 5X" reportVersion="5.6.1" licenseID="344390808" containsGarbage="False" extractionType="Physical" N
  <sourceExtractions>
    <extractionInfo id="0" name="Physical" isCustomName="False" type="Physical" deviceName="LG_H790" fullName="LG H790 Nexus 5X" index="0" IsPartialData="False" />
  </sourceExtractions>
  <caseInformation>
    <field name="Examiner name" isSystem="True" isRequired="True" fieldType="ExaminerName" multipleLines="False">M.E.</field>
  </caseInformation>
  <metadata section="Additional Fields">
    <item name="DeviceInfoCreationTime" systemtype="System.String"><![CDATA[25-11-2019 17:14:13]]></item>
    <item name="UFED_PA_Version" systemtype="System.String"><![CDATA[7.24.0.209]]></item>
  </metadata>
  <metadata section="Extraction Data">
    <item name="DeviceInfoExtractionStartDateTime" sourceExtraction="0" systemtype="System.String"><![CDATA[06-Dec-18 9:14:50 PM(UTC-5)]]></item>
    <item name="DeviceInfoExtractionEndDateTime" sourceExtraction="0" systemtype="System.String"><![CDATA[06-Dec-18 10:45:58 PM(UTC-5)]]></item>
    <item name="DeviceInfoUnitIdentifier" sourceExtraction="0" systemtype="System.String"><![CDATA[1091773144]]></item>
    <item name="DeviceInfoUnitVersion" sourceExtraction="0" systemtype="System.String"><![CDATA[7.10.1.1080]]></item>
    <item name="DeviceInfoInternalVersion" sourceExtraction="0" systemtype="System.String"><![CDATA[4.7.7.1080]]></item>
    <item name="DeviceInfoSelectedManufacturer" sourceExtraction="0" systemtype="System.String"><![CDATA[LG GSM]]></item>
    <item name="DeviceInfoSelectedDeviceName" sourceExtraction="0" systemtype="System.String"><![CDATA[H790 Nexus 5X]]></item>
    <item name="GlobalMachineName" sourceExtraction="0" systemtype="System.String"><![CDATA[JSIPC60506]]></item>
    <item name="DeviceInfoConnectionType" sourceExtraction="0" systemtype="System.String"><![CDATA[Cable No. 170]]></item>
    <item name="DeviceInfoIsEncrypted" sourceExtraction="0" systemtype="System.String"><![CDATA[GlobalTrue]]></item>
    <item name="DeviceInfoConnectionType" sourceExtraction="0" systemtype="System.String"><![CDATA[Physical [ Android ADB ]]]></item>
    <item name="DeviceInfoExtractionId" sourceExtraction="0" systemtype="System.String"><![CDATA[ACFFC9F7-089A-4760-9E93-E28708EF5924]]></item>
    <item name="DeviceInfoTimeSettings (ID)" systemtype="System.String"><![CDATA[_America/New_York]]></item>
    <item name="DeviceInfoDeviceInfo">
    <item id="[illegible]51-4acc-8b06-b875395bc96b" name="AndroidFingerprint" sourceExtraction="0" systemtype="System.String"><![CDATA[google/bullhead/bullhead:7.1.2/N2G47O/3
    <item id="[illegible]9b-407d-8788-2fdfba8b8933" name="DeviceInfoDetectedPhoneModel" sourceExtraction="0" systemtype="System.String"><![CDATA[Nexus 5X]]></item>
    <item id="6429a3e4-c77b-4236-9ffc-e4d32be46961" name="DeviceInfoOSVersion" sourceExtraction="0" systemtype="System.String"><![CDATA[7.1.2]]></item>
    <item id="[illegible]ba55-6d0eb1b8a54f" name="DeviceInfoDetectedPhoneVendor" sourceExtraction="0" systemtype="System.String"><![CDATA[google]]></item>
    <item id="[illegible]922c-0ada4b8c131c" name="DeviceInfoAndroidID" sourceExtraction="0" systemtype="System.String"><![CDATA[4d2d47650ddb38e1]]></item>
    <item id="[illegible]a4d8d0" name="DeviceInfoBluetoothDeviceName" sourceExtraction="0" systemtype="System.String"><![CDATA[Nexus 5X]]></item>
    <item id="[illegible]9eb3fe" name="DeviceInfoBluetoothDeviceAddress" sourceExtraction="0" systemtype="System.String"><![CDATA[64:BC:0C:F5:D1:C9]]></ite
    <item id="c2bec7f5-4d51-48[illegible]469a2d" name="Hotspot password required" group="Tethering" sourceExtraction="0" systemtype="System.String"><![CDATA[ce5047f6f1a2]]
    <item id="fdda21d5-e4f5-4d[illegible]0b4935" name="Phone Activation Time" sourceExtraction="0" systemtype="System.String"><![CDATA[29-Nov-18 5:58:19 PM(UTC+0)]]></item
    <item id="41c4fcb1-a295-45[illegible]277d85" name="DeviceInfoTimeZone" sourceExtraction="0" systemtype="System.String"><![CDATA[(UTC-05:00) New_York (America)]]></it
    <item id="4494c834-d756-4a[illegible]8f4b5a" name="DeviceInfoLocationServicesEnabled" sourceExtraction="0" systemtype="System.String"><![CDATA[True]]></item>
    <item id="845a46b4-738c-4117-8848-eca25667d3a7" name="ICCID" sourceExtraction="0" systemtype="System.String"><![CDATA[89014104279705559755]]></item>
    <item id="626b470a-7db9-4dd4-a989-bb027680875c" name="IMSI" sourceExtraction="0" systemtype="System.String"><![CDATA[310410970555975]]></item>
    <item id="cf0ea07b-a3e2-44c9-967f-388beea14ecb" name="Advertising Id" sourceExtraction="0" systemtype="System.String"><![CDATA[c692feb2-3361-45e4-8515-5a8da3a3eacd]]></it
    <item id="3f1087e7-d589-4d3e-af88-c594e69494e9" name="Recovery Event" sourceExtraction="0" systemtype="Utils.Types.TimeStamp">1970-01-18T21:39:27.000-05:00</item>
    <item id="9ed98b87-ba8b-4c92-8046-cd8060347e80" name="Recovery Event" sourceExtraction="0" systemtype="Utils.Types.TimeStamp">1970-05-25T10:11:34.000-04:00</item>
```


EXAMPLE
XML report

Cellebrite PA

CASE

XPATH EXTRACTOR



XPATH EXTRACTOR

XPath Extractor into CASE

XML Report

Lines: 465.368

```
<?xml version="1.0" encoding="utf-8"?>
<project id="ce400713-d75d-4af9-a966-69468e675ff8" name="LG GSM_H790 Nexus 5X" reportVersion="5.6.1" licenseID="344390808" c
  <sourceExtractions>
    <extractionInfo id="0" name="Physical" isCustomName="False" type="Physical" deviceName="LG_H790" fullName="LG H790 Nexus
  </sourceExtractions>
  <caseInformation>
    <field name="Examiner name" isSystem="True" isRequired="True" fieldType="ExaminerName" multipleLines="False">M.E.</field
  </caseInformation>
  <metadata section="Additional Fields">
    <item name="DeviceInfoCreationTime" systemtype="System.String"><![CDATA[25-11-2019 17:14:13]]></item>
```

Calendar | Call Log | Chat | Contact | Files | SMSs | Web History

Open XML ...

XPath expression

//model[@type="SMS"]

Run XPath Expression

XPath result

- SMS (30/7)
  - [1] 2dbc607d-b7d1-4db4-9740-b0763517912b - Intact
    - (FOLDER): Inbox
    - (BODY): Welcome to TracFone! Your number is: 9197580276, your Last Day of Service is 01/28/2019. For self-help options, text 'HELP' to 611611.
    - (STATUS): Read

Done! Extraction processing complete.

XPATH EXTRACTOR

DEMO

FUTURE STEPS

a. Developing XPath rules for Oxygen and Magnet

b. Extending the XPath Extractor to all the other forensic tools

c. Developing Light parsers only for demonstration purpose

d. Completing XML report conversion into CASE

e. Coordinating activities with other groups that are working on similar goals

f. Developing a converter tool for ISP data

g. Gathering CASE critical points (to be discussed with the Community)

CASE

Gregory Webb, London Metropolitan Police, UK / CASE Ontology Committee

UTILISING THE CASE STANDARD TO VIEW BESPOKE FILE SYSTEMS

Utilising the CASE Standard to View Bespoke File Systems

DFRWS EU 2020 (Oxford)

Author: Gregory Webb (Gregory.Webb@met.police.uk)

METROPOLITAN POLICE

NEW SCOTLAND YARD

Utilising the CASE Standard to View Bespoke File Systems

or alternatively

A Brief Introduction into some of the Capabilities of the CASE Standard.

METROPOLITAN POLICE

NEW SCOTLAND YARD

Talk Breakdown

- The Problem we Initially had.
- How we originally resolved it.
- A Brief Introduction to the CASE Standard.
- Using CASE to create a Universal FS Viewer.
- Current Limitations

METROPOLITAN POLICE

NEW SCOTLAND YARD

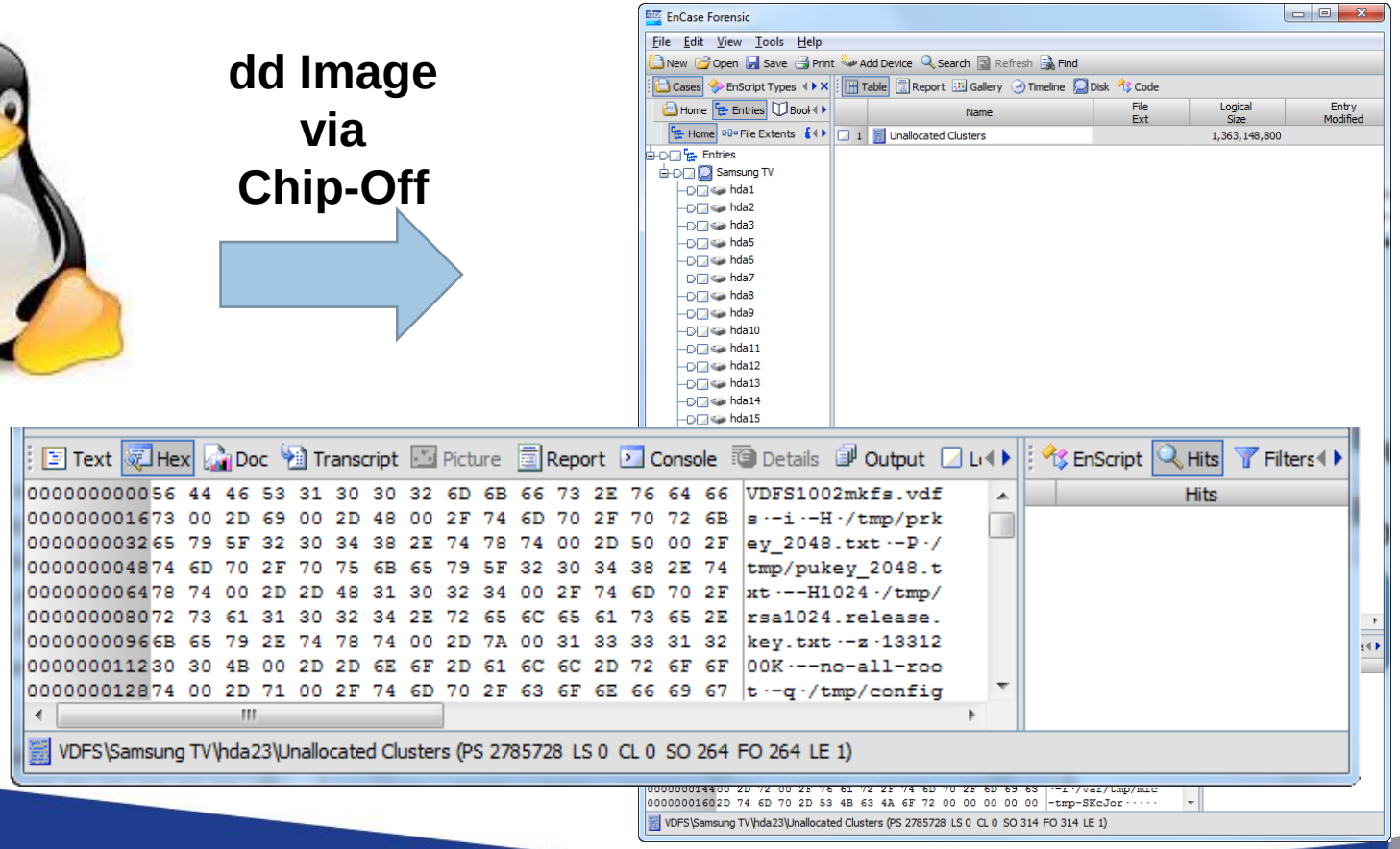
1. The Problem we Originally Had

METROPOLITAN POLICE

NEW SCOTLAND YARD

The Problem we Originally Had

dd Image via Chip-Off



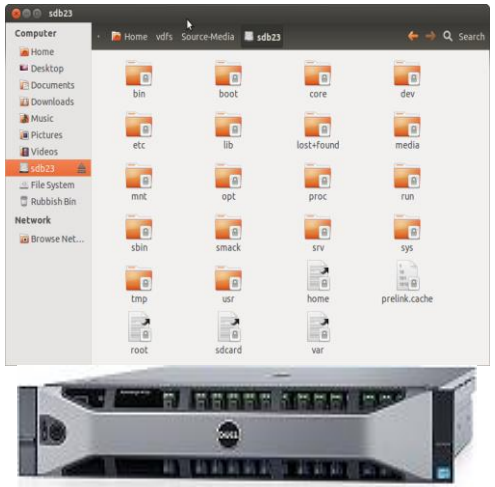
METROPOLITAN POLICE

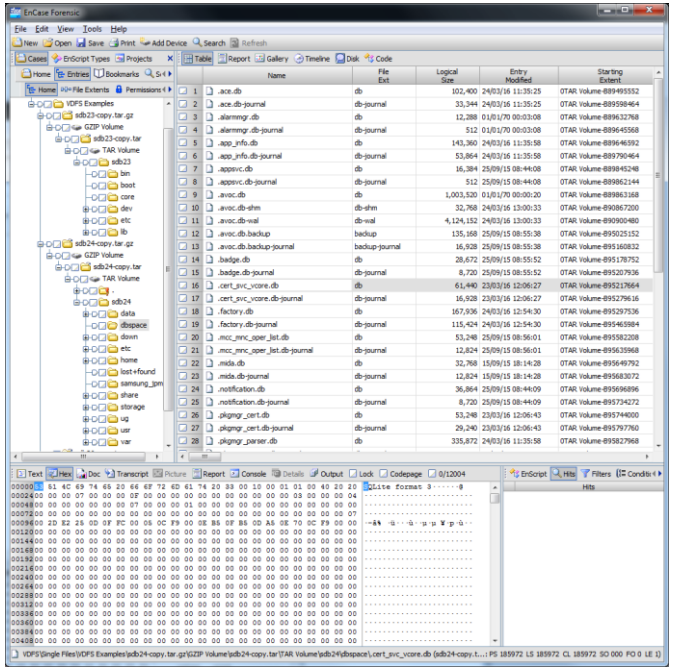
NEW SCOTLAND YARD

What we were seeking to Achieve

dd Image via Chip-Off

Ubuntu v?.?





Other Forensic Tools are Available

METROPOLITAN POLICE

NEW SCOTLAND YARD

2. How we originally Resolved It

METROPOLITAN POLICE

NEW SCOTLAND YARD

How we originally Resolved It

- Compile the Source Code into a Kernel Module.
- Mount the Disk Image in Linux.
- Export the Files to a ZIP File (no EWF L01 option).
- Import the ZIP file into a Forensic Tool.
- Analyse and Generate a Report.

Source Code Compilation Issues

- The Source Code may not be Available.
- The code may only compile in a specific Linux sub-version.
- Source Code may need to be modified to compile.
- The source code may only work for a specific version of the bespoke File System.

Exporting to Catalogue / ZIP File Issues

- File System data won’t natively be accessible.
- Some Inodes may have issues when being copied.
- Only a subset of the Available Data will be copied.
- Duplication of File data from Original Image.

General Limitations of the Method

- Difficult to Quality Control.
- It isn’t a Forensically Sound method.
- Knowledge of the File System remains Unknown.
- It relies on the Source Code being available.
- It requires a reasonable Knowledge of C and Linux Kernel Development.

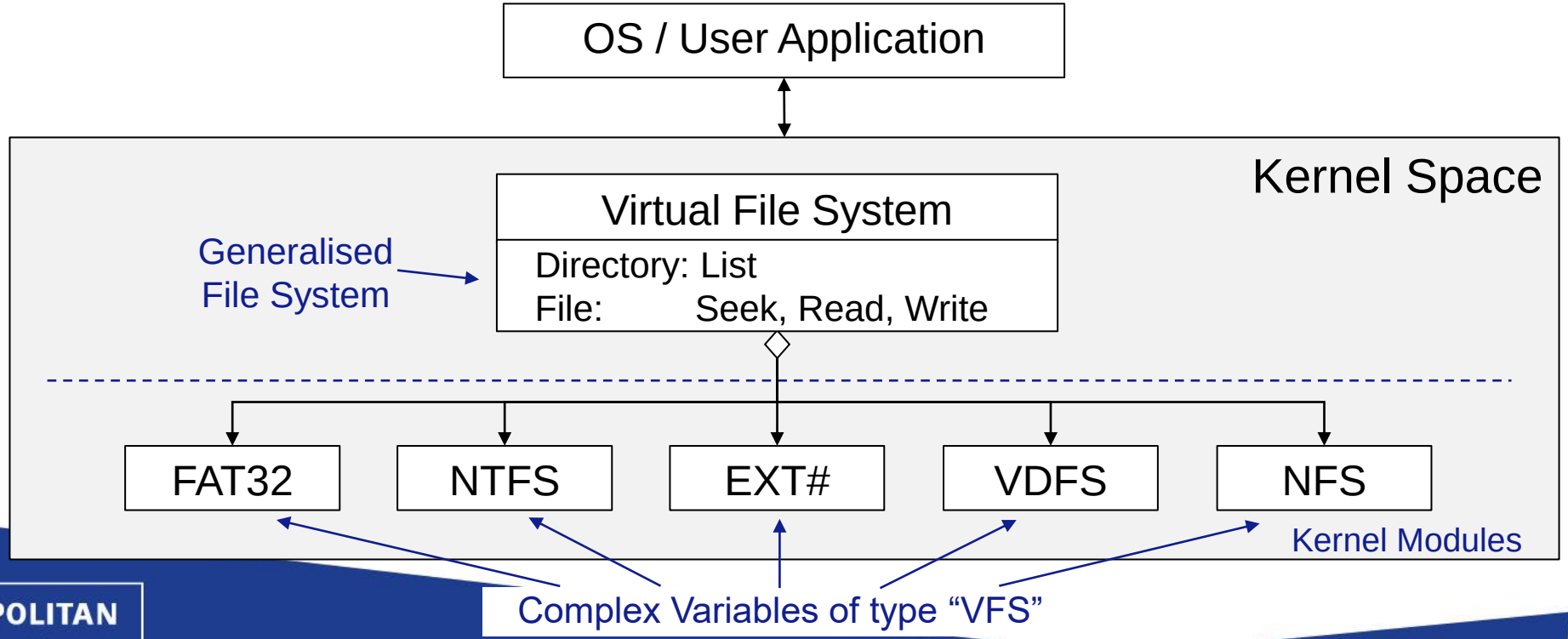
3. The Proof-of-Concept using VFS/CASE

METROPOLITAN POLICE

NEW SCOTLAND YARD

Linux Virtual File System (VFS)

A Simplified Overview of the Linux VFS



METROPOLITAN POLICE

NEW SCOTLAND YARD

Forensic Tool used for the PoC

The Free Forensic Tool “SleuthKit Autopsy” was used for the Proof-of-Concept for the following reasons:

- It doesn’t unfairly favour one commercial Forensic Tool provider.
- The Source Code is readily available, and well Documented.
- The SQLite database version is simple to analyse & update.
- The Ingestion Module can be coded natively in Java or Python.

Result: Viewing VDFS in Autopsy v4.13.0

Autopsy10_0_0_1-test01-VDFS - Autopsy 4.13.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Timeline | Close Case | Generate Report | Keyword Lists | Keyword Search

- Data Sources
  - VDFS-Test-Disk.E01
    - vol1 (Unallocated: 0-2047)
    - vol2 (Linux (0x83): 2048-1050623)
      - root (4)
        - $ystem (3)
        - Folder-Containing_Text_Files (1)
    - vol3 (Unallocated: 1050624-4188133)
- Views
- Results
- Tags
- Reports

Listing

/img_VDFS-Test-Disk.E01/vol_vol2/root — 4 Results

Table | Thumbnail | Save Table as CSV

Name	S	C	Size	Modified Time	Access Time	Created Time	Change Time	Flags(Dir)
$ystem			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	Allocated
Folder-Containing_Text_Files			0	2019-04-09 12:41:36 BST	2019-04-09 12:41:36 BST	0000-00-00 00:00:00	0000-00-00 00:00:00	Allocated
dummy.bin			120	2019-02-01 12:34:56 GMT	2019-02-01 12:34:56 GMT	2019-02-01 12:34:56 GMT	0000-00-00 00:00:00	Allocated
history.txt			4818	2017-10-09 14:02:29 BST	2017-11-03 11:22:56 GMT	2017-10-09 14:02:29 BST	0000-00-00 00:00:00	Allocated

Hex | Text | Application | Message | File Metadata | Results | Annotations | Other Occurrences

Page: 1 of 1 Page Go to Page: Jump to Offset 0 Launch in HxD

```
0x00000000: 20 20 20 20  31 20 20 73   75 64 6F 20  73 74 72 69       1  sudo stri
0x00000010: 70 20 2D 52  20 2E 6E 6F   74 65 2E 41  42 49 2D 74    p -R .note.ABI-t
0x00000020: 61 67 20 2F  75 73 72 2F   6C 69 62 2F  69 33 38 36    ag /usr/lib/i386
0x00000030: 2D 6C 69 6E  75 78 2D 67   6E 75 2F 6D  65 73 61 2F    -linux-gnu/mesa/
0x00000040: 6C 69 62 47  4C 2E 73 6F   2E 31 0A 20  20 20 20 32    libGL.so.1.    2
0x00000050: 20 20 73 75  64 6F 20 6C   64 63 6F 6E  66 69 67 0A      sudo ldconfig.
0x00000060: 20 20 20 20  33 20 20 50   61 73 73 77  6F 72 64 0A       3  Password.
0x00000070: 20 20 20 20  34 20 20 6C   73 20 2D 6C  72 61 69 6E       4  ls -lrain
0x00000080: 20 2F 6C 69  62 2F 6D 6F   64 75 6C 65  73 2F 33 2E     /lib/modules/3.
0x00000090: 38 2E 30 2D  32 39 2D 67   65 6E 65 72  69 63 0A 20    8.0-29-generic.
0x000000a0: 20 20 20 35  20 20 6C 73   20 2D 6C 72  61 69 6E 20       5  ls -lrain
0x000000b0: 2F 75 73 72  2F 73 72 63   0A 20 20 20  20 36 20 20    /usr/src.    6
```

METROPOLITAN POLICE

NEW SCOTLAND YARD

Example: File = history.txt

```
{
  "@type" : "File",
  "name" :        "history.txt",
  "path" :        "root\history.txt",
  "sizeInBytes" : 4818
          :
},
{
  "@type" : "ContentData",
  "sizeInBytes" : 4818,
  "hash" : [
    {
      "@type" : "Hash",
      "hashType" :  "MD5",
      "hashValue" : "0AB08EF7F109F6F3E0600CF3ADA541D4"
    }
  ], ...
},
```

CASE-LD output

Forensic Tool

```
"File\name"          = "history.txt",
"File\extension"     = "txt",
"File\path"          = "root\history.txt",
"File\isAllocated"   = true,
"File\sizeInBytes"   = 4818,
"File\createdTime"   = "2017-10-09T01:02:29.468335994Z",
"File\accessedTime"  = "2017-11-03T11:22:56.126680999Z",
"File\modifiedTime"  = "2017-10-09T01:02:29.468335994Z",
"ContentData\sizeInBytes" = 4818,
"ContentData\hash\MD5"    = "0AB08EF7F109F6F3E0600CF3ADA541D4"
"ExtInode\fileType"    = 2,
"ExtInode\flags"       = 0,
"ExtInode\inodeID"     = 9,
"ExtInode\permissions" = 33204,
"ExtInode\SGID"        = 1000,
"ExtInode\SUID"        = 1000
```

Key/Value pairs

METROPOLITAN POLICE

NEW SCOTLAND YARD

4. An Introduction to the CASE Standard

METROPOLITAN POLICE

NEW SCOTLAND YARD

An Introduction to the CASE Std. - 1

- So, What is CASE?

  Cyber-investigation Analysis Standard Expression

  https://caseontology.org

- OK. So, What is it?

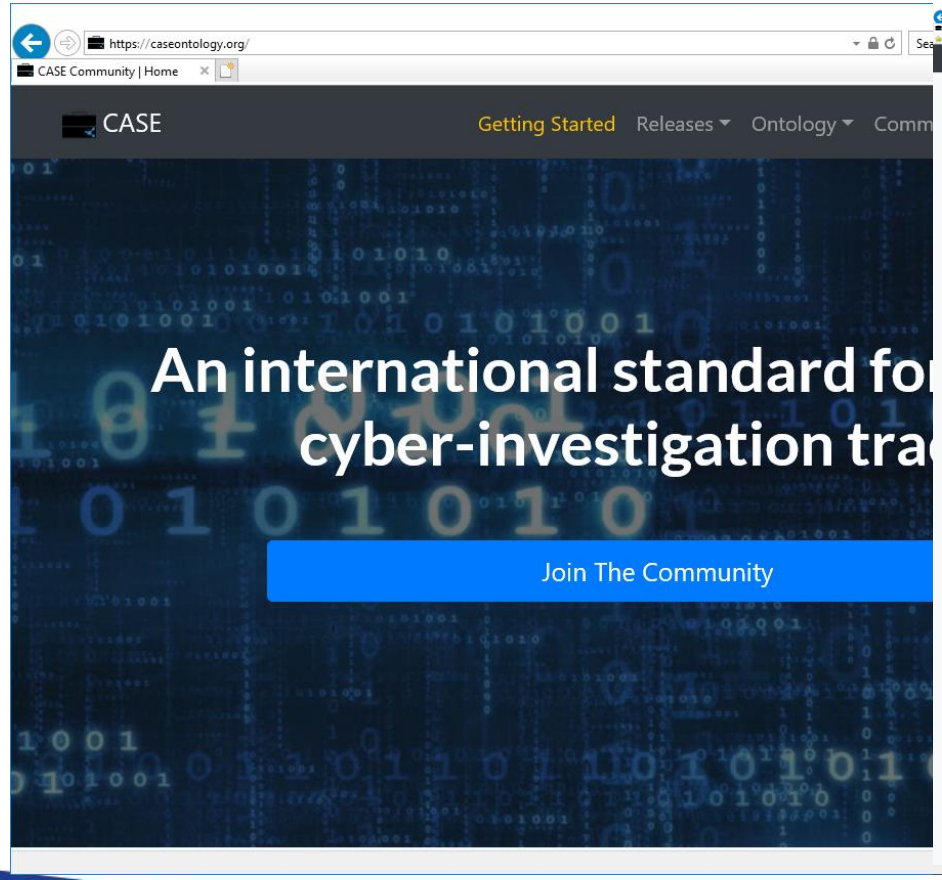
  Its primary design motivation is: **Interoperability**

  "*To advance the exchange of cyber-investigation information between tools and organisations*"

METROPOLITAN POLICE

NEW SCOTLAND YARD

CASE Website



Community Members page

METROPOLITAN POLICE

NEW SCOTLAND YARD

An Introduction to the CASE Std. - 2

- OK. So, What is it?

  It is a Digital Forensic Ontology based on the Unified Cyber Ontology (UCO)

  It is an Ontology standard, actively supported by Interpol / Europol, and Forensic Tool providers to facilitate the Exchange and further Analysis of Digital Investigation data utilising existing published W3C Semantic Web technologies as its foundations.

METROPOLITAN POLICE

NEW SCOTLAND YARD

An Introduction to the CASE Std. - 3

- In a Nutshell

  It enables results obtained by the examination process to be easily shared between forensic tools, and Case Management Systems, in a form that can be interpreted by both Humans and Automated Technologies, using standards based on existing W3C Web Linked-Data technologies.

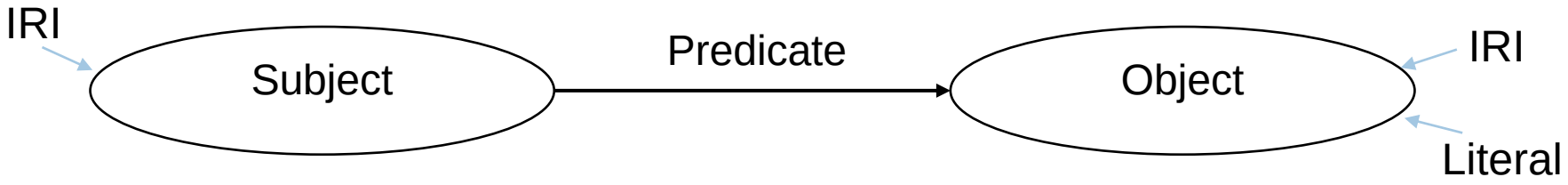
METROPOLITAN POLICE

NEW SCOTLAND YARD

An Introduction to the CASE Std. - 4

- How does it Work?

It utilises Triples of the form.



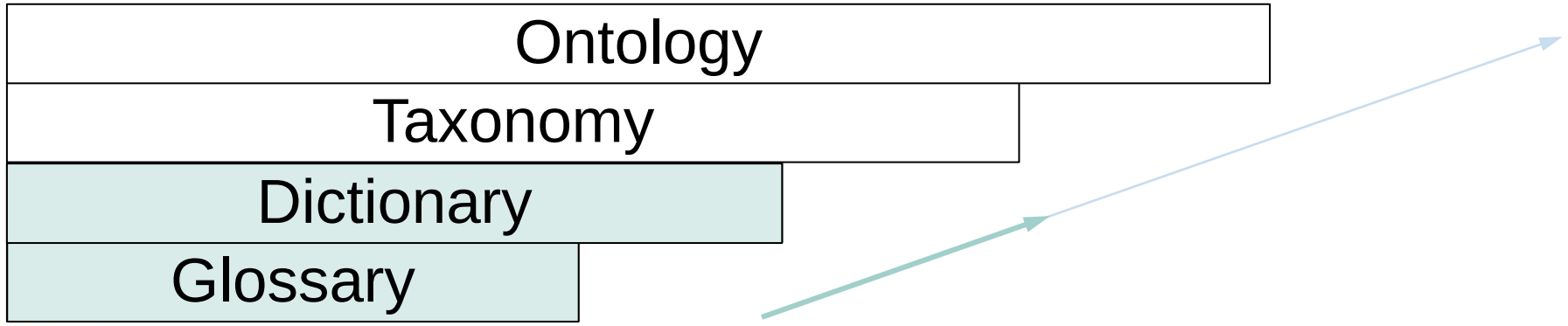
To express digital forensic information in a “Graph” based format that can easily be queried to extract, exchange and process stored data created from digital investigations.

METROPOLITAN POLICE

NEW SCOTLAND YARD

The CASE Ontology *Stack*

- The implementation utilises the CASE Glossary & Dictionary to characterise the elements required to describe a general File System; based on the Linux Virtual File System (VFS)



METROPOLITAN POLICE

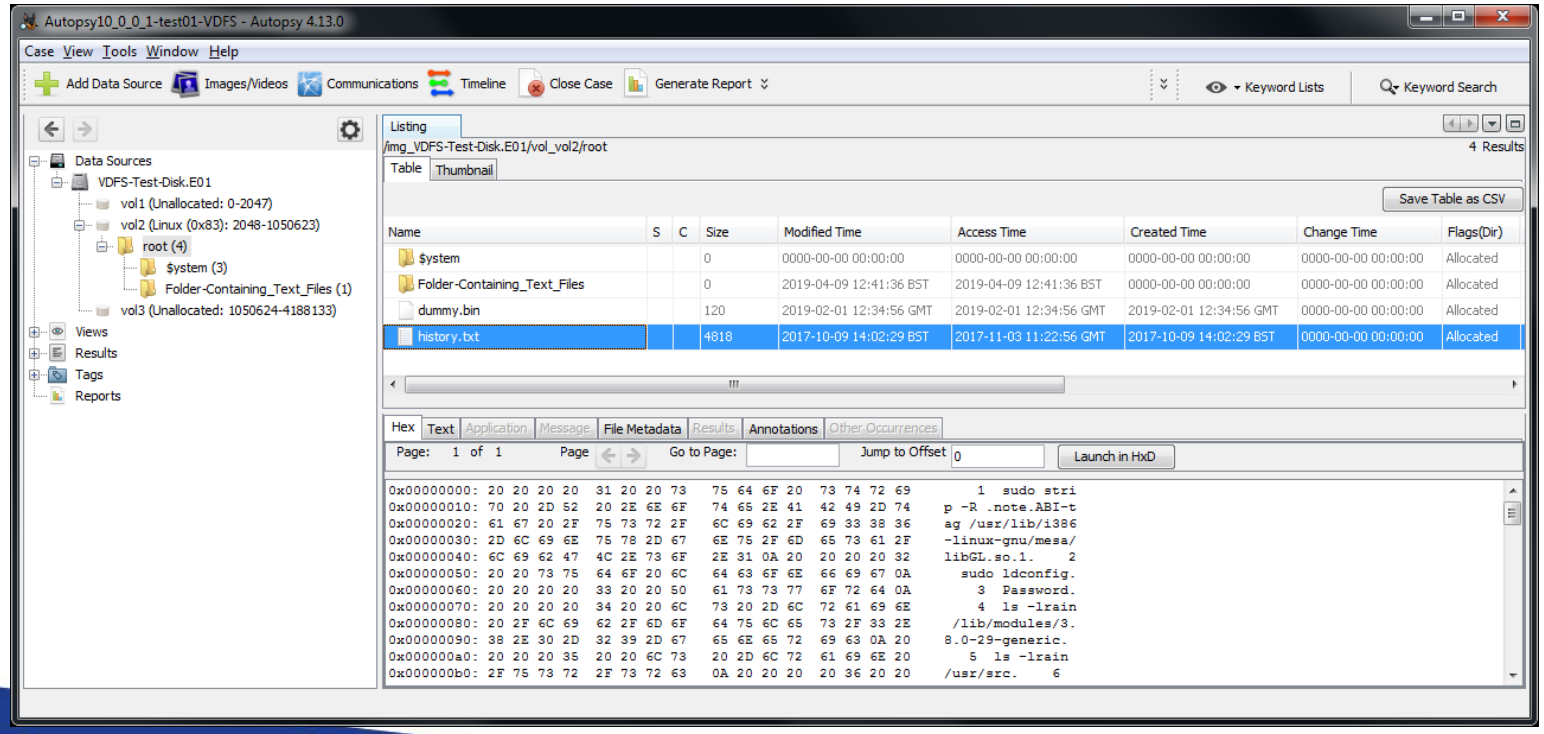
NEW SCOTLAND YARD

5. Using CASE to Create a Forensic Universal File System Viewer

METROPOLITAN POLICE

NEW SCOTLAND YARD

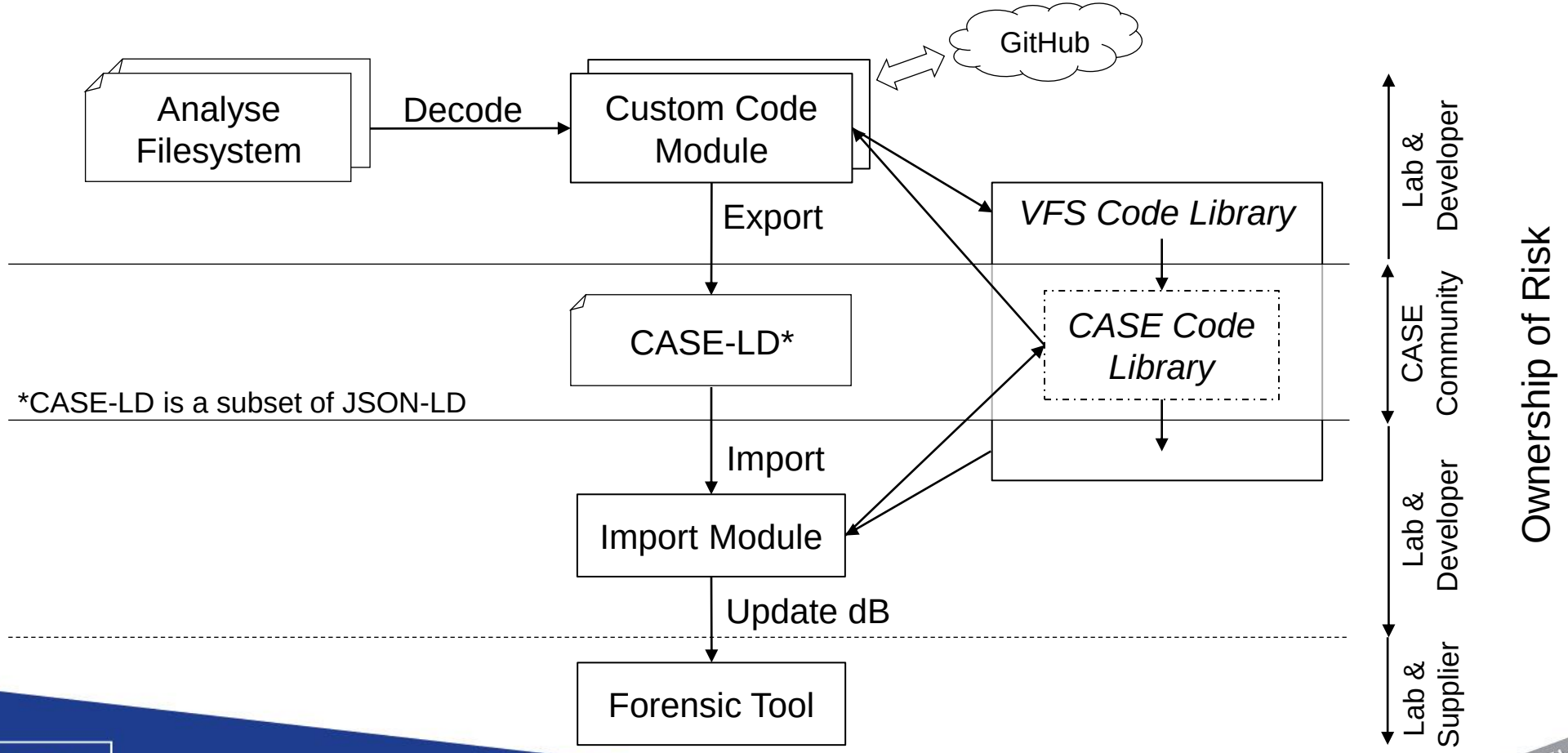
5. Using CASE to Create a Forensic Universal File System Viewer



METROPOLITAN POLICE

NEW SCOTLAND YARD

How the Concept Works



METROPOLITAN POLICE

NEW SCOTLAND YARD

6. The CASE-LD Structure

METROPOLITAN POLICE

NEW SCOTLAND YARD

The Basic CASE-LD Header Structures

```
{
  "@context": {
    "@vocab": "<CASE IRI core>#",
    "<prefix1>" : <Full IRI of prefix1>#,
    "<prefix2>" : <Full IRI of prefix2>#,
          :
    "<prefixP>" : <Full IRI of prefixP>#
  },
  "@graph": [
    { GraphItem1 },
    { GraphItem2 },
          :
    { GraphItemN }
  ]
}
```

METROPOLITAN POLICE

NEW SCOTLAND YARD

The Basic GraphItem Structure

```
GraphItem {
  "@id"   : "<graphitem-iri>",
  "@type" : "Trace" | "Relationship",
  // Required if "@type" : "Relationship" ---
  GraphItemRelationship {
    "source"             : "<source_IRI>",
    "target"             : "<target_IRI>",
    "kindOfRelationship" : "<relationship>",
    "isDirectional"      : true | false
  },
  // Required if "@type" : "Trace" ----------
  // Optional if "@type" : "Relationship"
  "hasPropertyBundle" : [
    { Facet1 }, { Facet2 }, ..., { FacetN }
  ]
}
```

Note: A Facet property may itself contain sub-Facets

METROPOLITAN POLICE

NEW SCOTLAND YARD

File Trace Example (with 3 Facets: File, ContentData, Hash)

```
{
   "@id" : "file-0073e2bd-eb74-4812-bd0d-18b3764126fb",
   "@type" : "Trace",
   "hasPropertyBundle" : [
      {
        "@type" : "File",
        "name" :        "history.txt",
        "path" :        "root\history.txt",
        "sizeInBytes" : 4818
             :
      },
      {
        "@type" : "ContentData",
        "sizeInBytes" : 4818,
        "hash" : [
          {
            "@type" : "Hash",
            "hashType" :  "MD5",
            "hashValue" : "0AB08EF7F109F6F3E0600CF3A
          }
        ], ...
      }
   ]
 }
```

CASE-LD output

```
"File\name"          = "history.txt",
"File\extension"     = "txt",
"File\path"          = "root\history.txt",
"File\isAllocated"   = true,
"File\sizeInBytes"   = 4818,
"File\createdTime"   = "2017-10-09T01:02:29.468335994Z",
"File\accessedTime"  = "2017-11-03T11:22:56.126680999Z",
"File\modifiedTime"  = "2017-10-09T01:02:29.468335994Z",
"ContentData\sizeInBytes" = 4818,
"ContentData\hash\MD5"    = "0AB08EF7F109F6F3E0600CF3ADA541D4"
"ExtInode\fileType"    = 2,
"ExtInode\flags"       = 0,
"ExtInode\inodeID"     = 9,
"ExtInode\permissions" = 33204,
"ExtInode\SGID"        = 1000,
"ExtInode\SUID"        = 1000
```

Key/Value pairs

METROPOLITAN POLICE

NEW SCOTLAND YARD

Demo

METROPOLITAN POLICE

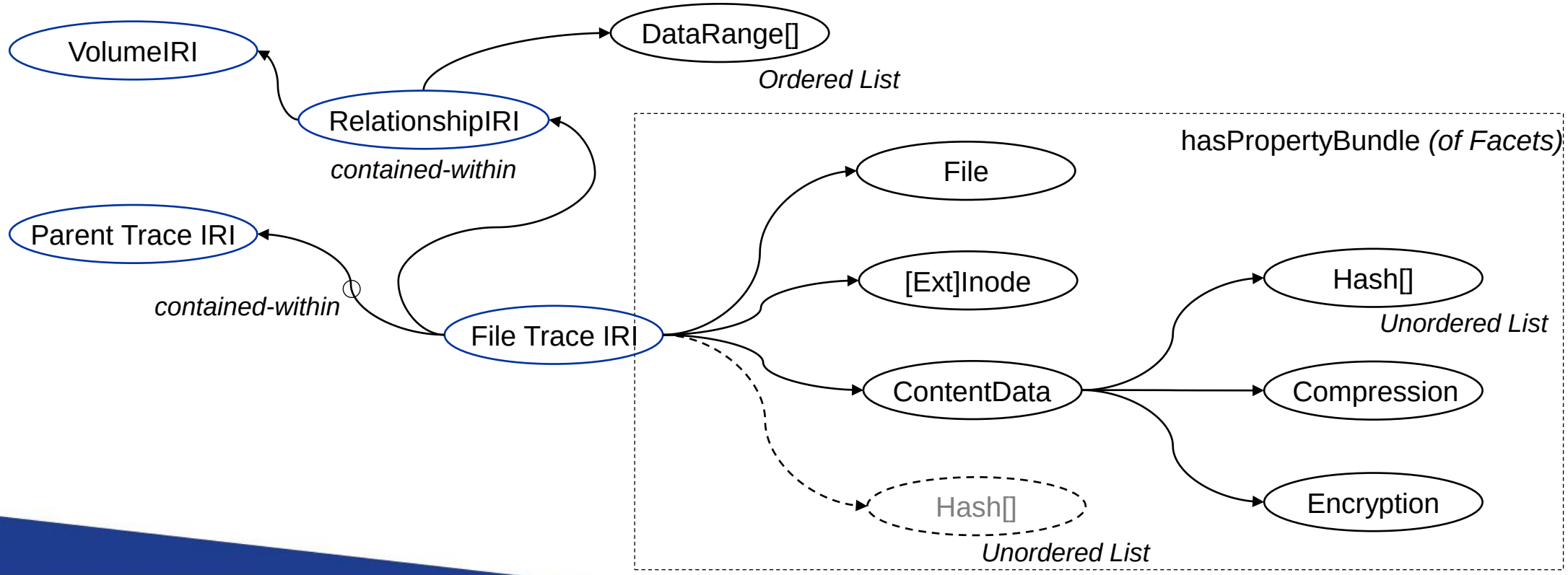
NEW SCOTLAND YARD

7. CASE Traces and Relationships

METROPOLITAN POLICE

NEW SCOTLAND YARD

CASE Compliant File Trace Overview



METROPOLITAN POLICE

NEW SCOTLAND YARD

CASE-LD Compliant File Trace

prefix ← → *uuid*

```
{
  "@id": "file-d4c533c0-9dd3-418d-97c6-9878c94ca1d2",
  "@type": "Trace",
  "hasPropertyBundle": [
    {
      "@type" : "File",
              :
    },
    {
      "@type" : "ExtInode",
              :
    },
    {
      "@type" : "ContentData",
              :
    }
  ]
}
```

Where:
Trace ID prefix matches primary Facet

METROPOLITAN POLICE

NEW SCOTLAND YARD

Decoded CASE-LD File Trace Structure

```
// Structure GraphItemHeader
{
  graphItemUUID = "file-d4c533c0-9dd3-418d-97c6-9878c94ca1d2",
  graphItemType = Trace,
  graphItemPB   = true
}
// Structure GraphItemProperties
{
  FacetNode[]  "<Facet>\<FacetNode propertyKey>" = "<FacetNode propertyValue>"
}
```

METROPOLITAN POLICE

NEW SCOTLAND YARD

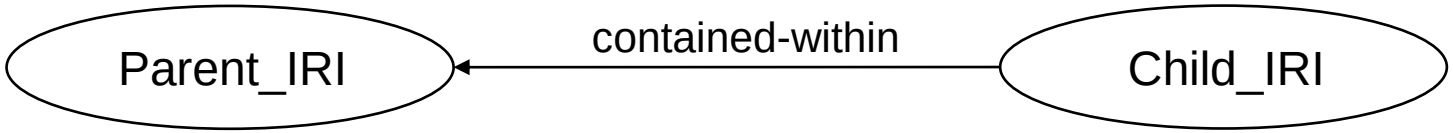
Decoded CASE-LD Relationship Structure

```
// Structure GraphItemHeader
{
  graphItemIRI  = "<relationship-iri>",
  graphItemType = RELATIONSHIP,
  graphItemPB   = false
}
// Structure GraphItemRelationship
{
  source                = "File_IRI",
  target                = "Parent_IRI",
  kindOfRelationship‟ = "contained-within",
  isDirectional‟      = true
}
// Structure GraphItemProperties (if graphItemPB == true)
{
  FacetNode[]  "<Facet>\<FacetNode propertyKey>" = "<FacetNode propertyValue>"
}
```

METROPOLITAN POLICE

NEW SCOTLAND YARD

CASE-LD Compliant Relationship

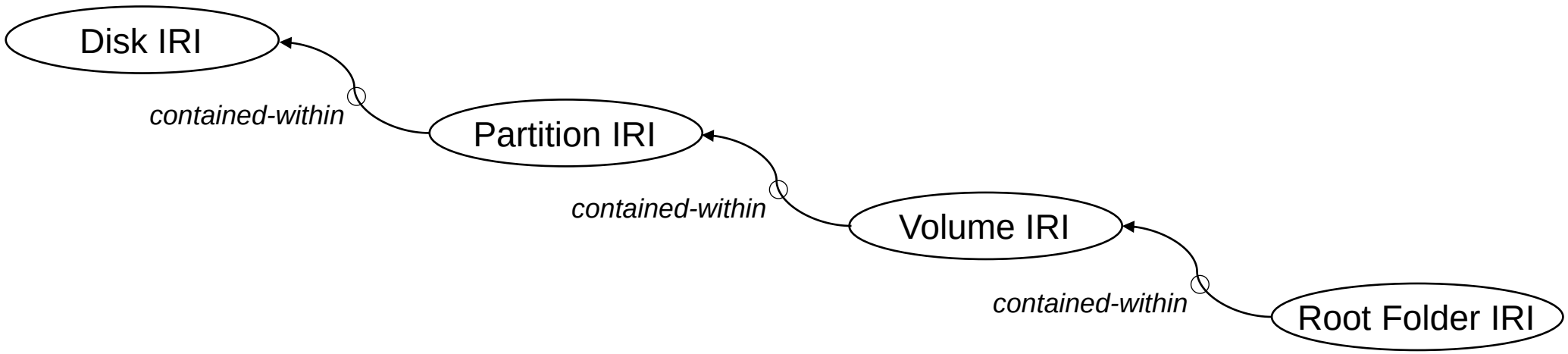



```
{
  "@id": "<relationship-IRI>",
  "@type": "Relationship",
  "source":              "File_IRI",
  "target":              "Parent_IRI",
  "KindOfRelationship": "contained-within",
  "isDirectional":       true
}
```

METROPOLITAN POLICE

NEW SCOTLAND YARD

CASE Disk to Root Relationships



METROPOLITAN POLICE

NEW SCOTLAND YARD

8. Current Limitations

METROPOLITAN POLICE

NEW SCOTLAND YARD

8. Current Limitations

- Customers don't know CASE support is available.
- So CASE Support isn't Requested by Customers.
- Suppliers focus on Customer Support Requests.
- Catch22, currently results in limited CASE Support.
- Waiting for official release of CASE MVP v1.0.

METROPOLITAN POLICE

NEW SCOTLAND YARD

Any Questions ?

METROPOLITAN POLICE

NEW SCOTLAND YARD

Thank You

METROPOLITAN POLICE

NEW SCOTLAND YARD

Andrew Sovern, Mapping Working Group Leader / CASE Project Team, MITRE

CASE MAPPING TUTORIAL

CASE Mapping Tutorial

Andrew Sovern

Mapping Working Group Leader /
CASE Project Team, MITRE
asovern@mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

What is mapping?

- **Connects items in a tool to the CASE ontology items**
- **Crucial step before implementing export/import capabilities into a tool**
  - Confirms the ontology has support for all attributes
  - If the above is not true, a Change Proposal can be used to add support

- **Requires an understanding of the tool and ontology**
- **Mappings need to be precise and descriptive**
  - Note what files and lines in code were referenced to do the mapping
  - Provide context and reasoning for each item
- Document how data is extracted and represented
  - Hierarchy in tool output will need to be represented in the ontology

MITRE

plaso/log2timeline

- Open-source Python-based log2timeline interface maintained on Github
- Designed to extract and aggregate timestamps from various files on a system
- Plaso is a timeline-based forensics framework that supports parsers, analysis plugins, and one-off scripts to automate workflows

https://github.com/log2timeline/plaso

Sample Mapping Demonstration

- **Map two Plaso modules to the draft CASE 0.2.0 ontology, which imports the UCO 0.3.0 ontology**
  - https://github.com/log2timeline/plaso

Example modules mapped:

- Android_calls
- Android_sms

Module Mapping - android_calls

call_type - direction/status

duration - call duration

timestamp - call start time

name - name of remote party

number - number of remote party

```
call_type = self._GetRowValue(query_hash, row, 'type')
call_type = self.CALL_TYPE.get(call_type, 'UNKNOWN')
duration = self._GetRowValue(query_hash, row, 'duration')
timestamp = self._GetRowValue(query_hash, row, 'date')

event_data = AndroidCallEventData()
event_data.call_type = call_type
event_data.duration = self._GetRowValue(query_hash, row, 'duration')
event_data.name = self._GetRowValue(query_hash, row, 'name')
event_data.number = self._GetRowValue(query_hash, row, 'number')
event_data.offset = self._GetRowValue(query_hash, row, 'id')
event_data.query = query
```

```
CALL_TYPE = {
    1: 'INCOMING',
    2: 'OUTGOING',
    3: 'MISSED'}
```

Module Mapping - android_calls (cont.)

Plaso	CASE & UCO	Notes
	uco-observable:PhoneCall	
call_type	uco-observable:callType	Determines if call is Incoming, Outgoing, or Missed
duration	uco-observable:duration	length of call
timestamp	uco-observable:startTime	Start time of call
name	uco-observable:contactName	Contact name
number	uco-observable:phoneNumber uco-observable:to/from	Remote participant number Depends on callType
	uco-observable:endTime	Result of timestamp + duration

Module Mapping - android_sms

address - phone number

body - msg text

offset - msg row ID

sms_read - Read status

sms_type - msg direction

timestamp - sent/received time

```
SMS_TYPE = {
    1: 'RECEIVED'
    2: 'SENT'}
SMS_READ = {
    0: 'UNREAD',
    1: 'READ'}
```

```
sms_read = self._GetRowValue(query_hash, row, 'read')
sms_type = self._GetRowValue(query_hash, row, 'type')

event_data = AndroidSMSEventData()
event_data.address = self._GetRowValue(query_hash, row, 'address')
event_data.body = self._GetRowValue(query_hash, row, 'body')
event_data.offset = self._GetRowValue(query_hash, row, 'id')
event_data.query = query
event_data.sms_read = self.SMS_READ.get(sms_read, 'UNKNOWN')
event_data.sms_type = self.SMS_TYPE.get(sms_type, 'UNKNOWN')

timestamp = self._GetRowValue(query_hash, row, 'date')
date_time = dfdatetime_java_time.JavaTime(timestamp=timestamp)
event = time_events.DateTimeValuesEvent(
    date_time, definitions.TIME_DESCRIPTION_CREATION)
parser_mediator.ProduceEventWithEventData(event, event_data)
```

CASE

MITRE

Module Mapping - android_sms (cont.)

Plaso	CASE	Notes
	uco-observable:Message	
address	uco-observable:to uco-observable:from	Uses sms_type to determine mapping
body	uco-observable:messageText	
offset	uco-observable:messageID	
sms_read	uco-observable:isRead	
sms_type	uco-observable:messageType	Sent or Received
timestamp	uco-observable:sentTime uco-observable:receivedTime	Depending on sms_type

Hotwash Tool Mapping

- **Where were the modules found?**
- **High level background of the data model**
  - Sometimes works better to scope modules (at a domain level) and find the specific properties that may be relevant to mapping
- **Any variables of interest?**
- **Any ontology items of interest?**
- **How can we make the plaso output CASE compliant?**

Jessica Hyde, CASE Governance Committee / Magnet Forensics
Ryan Griffith, CASE Governance Committee / U.S. DoD Cyber Crime Center

QUESTIONS AND DISCUSSION

Discussion

- Questions and comments?
- Topics of interest for future discussion?
  - There will be a CASE Workshop at DFRWS USA 2020 (virtual) in July

Wrap-up: CASE Online Resources and Contacts

- CASE Community Website: www.caseontology.org
- CASE GitHub: www.github.com/casework
- New members welcomed!
  - Apply online: https://caseontology.org/community/membership.html
  - FAQs, mailing lists, & more: https://caseontology.org/contribute.html
- PoCs:
  - General questions case@caseontology.org
  - Harm van Beek harm.van.beek@nfi.nl
  - Ryan Griffith Ryan.Griffith@dc3.mil
  - Vik Harichandran vharichandran@mitre.org
  - Deborah Nichols dlnichols@mitre.org

CASE