PRACTITIONERS' GAPS AND REQUIREMENTS

2ND PUBLIC AVAILABLE ANNUAL REPORT FOR INDUSTRY AND ACADEMIA

PUBLIC VERSION

FOR CYCLOPES BY:
HOME OFFICE

This project has received funding from the European Union's Horizon 2020 - the Framework Programme for Coordination and Support Action (2014-2020) under grant agreement No. 101021669.

JUNE 2023

Table of Contents

CYCLOPES | Practitioners' gaps and requirements – 2nd Annual Report for Industry and Academia

Summary

CYCLOPES | Practitioners' gaps and requirements – 2nd Annual Report for Industry and Academia

This document contains the **3 publicly available reports** developed from CYCLOPES practitioners' workshops. These reports outline the priorities of law enforcement at an operational level, and the opportunities for development across the three topics covered by the workshops:

- **Automotive Digital Forensics**– organised on 20th–21st September 2022;
- **Cryptocurrency as a Facilitator for Cybercrime** – organised on 7th – 8th December 2022;
- **Investigations Involving Cloud Services** – organised on 22nd – 23rd February 2023.

Representatives of European law enforcement agencies participated in each of the workshops.

These reports are intended to act as a steer for industry and academia.

1. Automotive Digital Forensics

Vehicles are frequently involved in modern criminal activity, either as the subject of the criminal activity in the case of vehicle theft or as a facilitator for the crime, with transport surrounding a crime or being used as part of the commission of an offence such as getaway cars. Additionally, luxury cars are a typical commodity obtained with the spoils of criminal activity. As the number of sensors and computational capacity of vehicles continues to grow, the wealth of data they collect and share offers a significant opportunity for Law Enforcement.

Automotive digital forensics can be seen as securing/ acquiring digital data related to a vehicle that can be of relevance in a judicial investigation. It is a very broad subject that accumulates several different investigative disciplines and techniques.

The Automotive Digital Forensics workshop brought together expert practitioners from across 12 European countries to discuss LEA operational use and future requirements for digital forensics on vehicles.

1.1. Priorities of Law Enforcement in the field of Automotive Digital Forensics

Practitioners identified developing improved tools to access live vehicle data and introducing a standard for vehicle system architectures as the key priority areas for the Law Enforcement community. In addition, practitioners highlighted the priorities of developing a framework to facilitate manufacturer cooperation with Law Enforcement; establishing a centralised database of vehicle systems; improving links between LEAs and academic institutions; improved automated tools; an automotive digital forensics conference.

1.2. Opportunities for development within Automotive Digital Forensics

1. Improved tools to access live vehicle data

Improved tools for accessing live data from vehicles, preferably via remote connection (Bluetooth/ WiFi/ cellular). These tools must take into account safety considerations surrounding extracting live data, particularly from electric vehicles.

2. A framework for manufacturer cooperation with law enforcement

A framework outlining law enforcement expectations for vehicle manufacturers and legislated requirements surrounding data collection and data sharing.

3. Standardisation of system architectures and vehicle data ports

An international standard that homogenises system architectures and data ports in new vehicles.

4. A European vehicle system database

A centralised and maintained European database containing vehicle manufacturer, model, infotainment system and information surrounding system architecture.

5. LEA collaboration with academic institutions

Automotive Digital Forensics-themed internships and projects for students at universities and research institutes that are studying in fields relevant to digital forensics – coding in particular.

6. Improved automated tools for data extraction, analysis and visualisation

Automated tools to extract, analyse and visualise large amounts of digital data gathered in automotive digital forensics investigations. These tools must cover a broad range of vehicle models, and must be user friendly, able to effectively visualise data sets with good reporting and data-exporting functionality.

7. Automotive digital forensics conference

An annual conference to share updated automotive digital forensic tools and techniques and provide an opportunity for peer-to-peer networking for practitioners.

2. Cryptocurrency as a facilitator for Cybercrime

Criminals and Organised Crime Groups are increasing operational security by using end to end encrypted communication and anonymising their proceeds of crime with use of cryptocurrency. While the predominant criminal use of cryptocurrencies centre on money laundering, fraud and the online trade of illicit goods and services, criminal use of cruptocurrency has permeated every type of crime requiring the laundering of criminal assets. This represents a significant challenge for the law enforcement community.

Law enforcement agencies (LEAs) face an array of challenges that can broadly fall into three main categories: analysis of cryptocurrency flow; seizure of the cryptocurrencies; forensic examination of digital devices for the artifacts connected to the trade in cryptocurrencies.

The Investigations Involving Cryptocurrency workshop brought together expert practitioners from across 12 European countries to discuss LEA operational use and future requirements for cryptocurrency investigations.

2.1. Priorities of Law Enforcement in the field of Cryptocurrency

Practitioners suggested that developing comprehensive legal frameworks for crypto asset management is a key priority. Improved tools to trace cryptocurrency transactions that utilise obfuscation methods such as mixers were also highlighted.

In addition, practitioners highlighted the priorities of developing a framework to facilitate cooperation with Law Enforcement from Cryptocurrency exchanges and services; establishing a centralised repository to assist with cryptocurrency address attribution; improving links between LEAs and academic institutions; improved automated tools for standard cryptocurrency transactions.

2.2. Opportunities for development within investigations involving cryptocurrency

1. End to end Legal Framework for Crypto Asset Management

A comprehensive legal framework that describes crypto asset handling across a full criminal investigation, including procedures and legal basis for crypto asset seizure, holding, conversion and return.

2. EU level joint procurement group

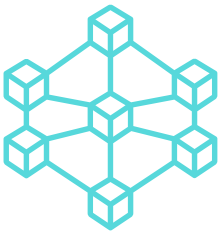
A centralised body or consortium of countries/ LEAs for identifying, assessing and purchasing crypto asset-specific tools. As well as procuring commercial tools, this group could promote 'in-house' innovation by providing a mechanism for trusted partners to share tools developed within their own agency.

3. Automated tools for analysis and reporting

User-friendly tools with an easily accessible user interface that can automate straightforward aspects of investigations and can present outputs in a format that is easy for non-specialist users such as a jury to understand.

3. Tools for tracing privacy coins

Tools for tracing transactions made using privacy coins, including Monero, Dash, Zcash etc. and for attributing wallets associated with illicit privacy coin transactions.



3. Tools to trace more complex cryptocurrency transactions

Tools to assist with the tracing of transactions that utilise obfuscation techniques such as the use of Mixing/Tumbling services or moving assets through different cryptocurrencies.

4. Improved job offers for cryptocurrency and cyber specialists

A review and rework of cyber and cryptocurrency specialist job descriptions that considers the competitive landscape for attracting and retaining people into these positions. To include consideration of leveraging factors beyond pay, including flexible working hours and location, fairer distribution of case work to avoid burnout, and opportunities for career development within law enforcement.

5. Crypto assets training for the Judiciary

Training or a framework for police and judiciary collaboration that covers basic understanding of key digital considerations and is regularly updated to keep pace with developments in technology and criminal Modus Operandi.

3. Investigations involving cloud services

The accessibility, flexibility and cost-effectiveness that cloud services offer make them hugely attractive to organisations, citizens and criminals. Their adoption has been further accelerated by the shift towards remote working, following the COVID-19 pandemic, with the migration to cloud services reducing the requirements for device storage and facilitating joint working. The development of cloud services has also led to the growth of devices such as Chromebooks, where very little information is locally stored, and virtual personal computer services such as Windows 365.

For LEAs, the cloud is both an investigative opportunity and a challenge: there is a wealth of data about crimes and suspects within the cloud, but also many challenges in terms of gaining access to critical information.

The Investigations Involving Cloud Services workshop brought together expert practitioners from across 12 European countries to discuss LEA operational use and future requirements for cloud services investigations.

3.1. Priorities of law enforcement in the field of cloud service investigations

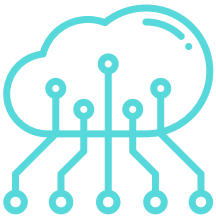
Practitioners suggested that there are a range of opportunities for increased automation that will reduce the administrative burden and dramatically speed up cloud services investigations, particularly surrounding triage of extracted cloud data.

In addition, practitioners highlighted the priorities of developing updated tools and methods for gaining access to Cloud Service accounts; developing faster processes for international cooperation; continual updating of legislation to keep pace with technological advancement; rewarding innovation that takes place within LEAs; providing an attractive training and development package to cyber specialists within Law Enforcement.

3.2. Opportunities for development within investigations involving Cloud Services

1. Automated tools for data triage

Automated tools capable of merging large datasets from multiple providers with varying proprietary formats and targeting key data of interest for investigations.



2. Tools to gain access to cloud service accounts

Tools and methods to identify user login credentials, and to by-pass passwords, biometrics and multi factor authentication.

3. Test environments and devices

Packages of test environments, datasets, sandboxes, and standalone devices that LEAs can use to test tools and validate results.

4. Review of the MLAT process

A review to determine opportunities for simplifying and expediting the MLAT process, including the introduction of time limits and making use of opportunities for automation.

5. Framework for updating legislation

A framework to facilitate adjusting existing legislation to take cyber considerations into account in far shorter cycles (2-3 months) than the current timeframe for introducing/ amending legislation (~3 years).

6. Training and development offer for law enforcement officers

Protected and prioritised time for training and development within LEA job offers for cyber specialists.

6. Police innovation awards

Competitions and awards for internal innovations such as tools and exploits that are developed in house by Law Enforcement practitioners.

CYCLOPES

JOIN THE CYCLOPES NETWORK

FOLLOW US

project-cyclopes

ProjectCyclopes

WEBSITE

https://cyclopes-project.eu

CONTACT

contact@cyclopes-project.eu

This project has received funding from the European Union's Horizon 2020 - the Framework Programme for Coordination and Support Action (2014-2020) under grant agreement No. 101021669.