eCrime2020— Symposium on Electronic Crime Research

LOCARD: Lawful evidence cOllecting and Continuity pIAtfoRm Development

Pablo López-Aguilar Beltrán: Head of IT & Cybersecurity

#UnitedInDiversity
Current Issues and Challenges on the Management of Digital Evidence

There are several disparities on how forensic reports are presented to different stakeholders among different jurisdictions.

- Budapest Convention
- EU Directives (e.g. 2014/41/EU – EIO)
- ISO Standards

eCrime2020 – Symposium on Electronic Crime Research
Standardizing the process used in the preparation and generation of digital forensic reports is a crucial step towards producing high quality reports to:

- Encourage digital forensic best practices.
- Facilitate sharing and admissibility of reports across jurisdictions.
EIO- LAPD: This project aims to “benefit all who are engaged in European cross-border crime investigation and judicial cooperation in criminal matters: judges, lawyers, public prosecutors, academics, police officers and others who are dealing with evidence gathering and investigation procedures on a daily basis.”

https://eio-lapd.eu/
Actions from the EU Commission

European Projects

Tool for the secure transmission of data, and foster:

- Exchange of information
- Cooperation

https://www.e-codex.eu/
Actions from the EU Commission

European Projects

Create an instrument with legal validity to carry out digital evidence exchanges related to EIO procedures through e-CODEX.

Provide people that deal with the legal and technological fields on EIO, digital evidence and e-CODEX.

Develop a case that serves as an example of how electronic evidence can be shared through e-CODEX.

https://evidence2e-codex.eu/
Actions from the EU Commission

European Projects

Reduce the gap between LEAs and the crime & terror organisations, giving them the tools and systems, to work with the latest devices.

A result of the project will be a European standard for the forensic investigation of mobile phones.

A dedicated training team will combine the best aspects of existing training courses available, into a new curriculum.

https://formobile-project.eu/

communication@formobile-project.eu
"Create a framework for the certification for European Cybercrime Investigators and Cybercrime European Prosecutors to establish the basis for the development of a group of professionals with the ability to deal properly with transnational problems of cybercrime."

https://www.ecteg.eu/running/gcc/
Actions from the EU Commission

Non-European Projects – Blockchain of Evidence (BoE)

“Website and smartphone app for secure evidence integrity from the minute it is collected. BoE enables transparency into the evidence collection process for everyone beginning at the point of origin.”

https://www.blockchainofevidence.org/
The LOCARD Project

Lawful evidence cOllecting & Continuity plAtfoRm Development

Toute action de l'homme, et a fortiori, l'action violente qu'est un crime, ne peut pas se dérouler sans laisser quelque marque.

Edmond Locard, La Police et Les Méthodes Scientifiques.

eCrime2020– Symposium on Electronic Crime Research
LOCARD presents the ultimate solution of accommodating independent users, jurisdictions, territories and global regulation, together with high security demands.

- 1st May 2019 – 30 April 2022
- 6,843,385.00€
- 19 partners
The LOCARD Project

Develop a standard based (among others) on the ISO 27000 series.

ISO/IEC 27037/2012
Provides guidelines [...] in facilitating the exchange of potential digital evidence between jurisdictions.

ISO/IEC 27042/2015
Provides guidance on the analysis and interpretation of digital evidence “...to guarantee continuity, validity, reproducibility, and repeatability.”

ISO/IEC 27043/2015
Provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence.

https://locard.eu/
The LOCARD Project

Permissioned Blockchain – Hyperledger Fabric

Secure and tamper-proof chain of custody and follow-up of cases.

Minimal data storage (e.g. hashes) to enhance performance and scalability.

Hyperledger channels provide private transactions between a subset of members, so that data from each case is properly managed.

https://locard.eu/
The LOCARD Project

Boundaries

1- Collection of the Digital Evidence

2- Identification and Analysis

3- Reporting of the Evidence

Research on Blockchain: Studying how to support scalability and efficiency through strong policy management and smart contracts.

Legal-Admissibility: Follows national / international standards, laws and methodologies for the chain of custody.
The LOCARD Project

High-Level Architecture

Entities may have different types of users with different level of clearance.

Users will be allowed to use LOCARD according to local and identity management policies.

Nodes represented inside the GREEN area correspond to blockchain nodes.

LEAD LEA: Assigned end user that will manage the crowdsourcing intelligence input cases, and will manage and distribute them accordingly between the rest of local end users or LEAs.
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intelligent crawler</strong></td>
<td>Collect digital evidences (malicious content) from the Internet.</td>
</tr>
<tr>
<td><strong>Investigator toolkit</strong></td>
<td>Offline forensic tools, so investigators can perform their usual data acquisition and analysis procedures.</td>
</tr>
<tr>
<td><strong>Blockchain manager</strong></td>
<td>Manage the LOCARD blockchain network and issue the smart contracts.</td>
</tr>
<tr>
<td><strong>Intelligence engine</strong></td>
<td>Process the LOCARD data to provide intelligence and extract correlations to ease criminal investigations.</td>
</tr>
<tr>
<td><strong>Communication engine</strong></td>
<td>Communication between end users so to request further details of a specific evidence, report or case.</td>
</tr>
<tr>
<td><strong>Deviant patterns repository</strong></td>
<td>Monitor social live streaming services and social media for deviant behaviours related to criminal activity.</td>
</tr>
<tr>
<td><strong>Reporting engine</strong></td>
<td>Collecting the data related to a specific case and creating an audit log of all the interactions related to it.</td>
</tr>
<tr>
<td><strong>UI/UX interface</strong></td>
<td>Front-end through which all modules are accessed.</td>
</tr>
</tbody>
</table>

Sources:
Network of Stakeholders

- Early access to technology and public results
- Demonstration of the platform during the project
- Customization of the platform following the given feedback
- Training and webinars

Law-Enforcement Agencies
Judicial Authorities
Scientific Community

https://locard.eu/
Lawful evidence cOllecting and Continuity plAtfoRm Development

Pablo López-Aguilar Beltrán
Head of IT & Cybersecurity
pablo.lopezaguilar@apwg.eu

"La paix et la prospérité ne peuvent être assurées que par l'union des hommes." - Jean Monnet

https://locard.eu  info@locard.eu
@LOCARD_EU

This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.