LOCARD: "Lawful evidence cOllecting and Continuity plAtfoRm Development"

Pablo López-Aguilar Beltrán[1]

[1] APWG European Union Foundation, Barcelona, Spain
pablo.lopezaguilar@apwg.eu

Abstract. Digital evidence is currently an integral part of criminal investigations, and not confined to pure cybercrime cases. Criminal behaviours like financial frauds, intellectual property theft, industrial espionage, and terrorist networks leverage the Internet and cyberspace. The very ubiquity of digital devices in modern society makes digital evidence extremely relevant for investigations about all kinds of criminal behaviour like murder, contraband activities, and people smuggling, to name a few.

Due to its nature, the use of digital evidence in a court of law has always been challenging. It is critical that it should be accompanied by a proper chain of custody, guaranteeing its source and integrity.

LOCARD aims to provide a holistic platform for chain of custody assurance along the forensic workflow, a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain. Each node of LOCARD will be able to independently set its own permission policies and to selectively share access to digital evidence with other nodes when deemed necessary and upon proper authorization through fine-grained policies. LOCARD's modularity will also allow diverse actors to tailor the platform to their specific needs and role in the digital forensic workflow, from preparation and readiness, to collection, to analysis and reporting.

Keywords: Forensics Sciences, Digital Evidence, Chain of Custody, Blockchain.

1 Introduction

The exponential increase in the volume of generated data together with the systems decentralisation open a wide window of opportunity in the field of cybercrime. This is one of the most important concerns of governments, societies and people, and it implies a high expense and risk for any society, weakens confidence in the Communication and Information Technologies and threatens international peace and stability.

In its fight against cybercrime, one of the most difficult challenges for the European Union is to homogenise the jurisdictions of the Member States. The procedure needed to obtain digital evidence, as well as its recognition in a court of justice, should follow a standardised procedure accepted by most countries within the Union. This procedure should guarantee the origin of the evidence and the integrity of the chain of custody.

Digital evidence is nowadays an integral part of criminal investigations and it is not only focussed on cybercrime specific cases, but also on determining criminal behaviour such as financial fraud, theft of intellectual property, industrial espionage and terrorist networks that constantly use the Internet and cyberspace. Given the ubiquity of digital devices, the correct management of digital evidence is extremely important.

LOCARD aims to develop a **holistic platform** aimed at ensuring the chain of custody throughout the flow of forensic analysis. It is a distributed and trusted platform that allows the storage of digital evidence metadata using **blockchain**.

Each node of LOCARD will independently establish its own permission policies and will selectively share access to digital evidence with other nodes (if necessary), and with the required authorisation. Thus, the developed platform will be modular since it will allow different agents to adapt the platform to their specific needs and their role in the digital forensic workflow, from preparation to compilation, analysis and reporting.

In addition, the platform will provide a collection resource module aimed at collecting citizens' information related to certain law violations, as well as a tracker to allow the detection and correlation of certain deviations based on behavioural patterns. It will also define a set of tools focused on investigators to allow them to collect digital evidence both online and offline.

All this will be managed through an identity management system that will **protect privacy** and allow access to evidence data, using a Trusted Execution Environment. The blockchain technology will not only guarantee the non-manipulation of information but its interoperability without requiring the services of third parties.

2 Project Description

LOCARD will provide a **collaborative** and **distributed** platform to automate the collection and documentation of every digital evidence. Its goal is to provide a holistic approach that aims to handle potential digital evidence to be able to present them in a court of law, alleviating many issues that face the current state of the art and practice. LOCARD will **increase trust** in the handling and processing of digital evidence, the management of chain of custody by providing transparency, using immutable storage to store the chain of custody and using end-to-end security through Trusted Environment Execution. More precisely, the mains objectives of the project are:

- Manage an immutable chain of custody of the digital evidence for every crime under investigation.
- Create the proper commitments per involved entity to handle the digital evidence accordingly.
- Allow for usage of live-streaming data as evidence.
- Allow victim organisations to monitor the progress of their digital investigation in real-time.

- Allow investigators to publish anonymised data that can be used to find correlations and identify campaigns.
- Provide investigators with online crawlers that will effectively detect deviant behaviour in online content.
- Provide investigators with offline tools that will assist them to collect multimedia evidence from media.
- Provide an infrastructure that could be used to store all digital evidence and handle their use in a court.
- Allow the international usage of digital evidence through ease to export and re-use of digital evidence in the corresponding format and automated filling of the forms/documents.
- Increase security of the platform by the integration of modules in a Trusted Execution Environment.
- Allow citizens report malicious online events.
- Allow investigators tag possible malicious activities/transactions etc, in data streams and receive notifications once alert criteria are met in processed data streams.

LOCARD will provide innovation and is going significantly beyond that state of the art in different key areas such as i) **mobile forensics** by exploring novel methods that would allow LEAs to unlock collected mobile devices for investigation that act as bottlenecks and prevent them from collecting necessary evidence, ii) **cloud forensics** by identifying emerging standards and technologies that would solve the most pressing problems fundamental, iii) **Copyright infringement** by providing end users with an “easy to use” dashboard where they will provide content in the form of free text, audio, multimedia etc and it will query the database to determine whether any of the cached apps is performing copyright infringement of this content, iv) **unification and standardization of digital forensics procedures** by introducing new documents completing the existing norms and v) **research on blockchain technology** by studying how to support scalability and efficiency for storing and sharing vast amounts of data with blockchain technologies.

3 Current Status

The project started last May and has a duration of three years. To date, the project accounts have been created on social networks as well as an initial version of the website [1] is already available under locard.eu domain.

The communication and dissemination strategy is being prepared and will be presented to the European Commission at the end of July. In addition, we are working on different key messages aimed at generating traction and interest to the different stakeholders.

Presentations of the project have been made at the EEMA Annual Conference 2019 [2] and at the Bucharest Symposium on Global Cybersecurity Awareness [3].

From a technical point of view, the development of the platform will begin once the functionality map has been developed aimed at meeting the needs of its main users.

4 Conclusions

LOCARD's research and toolbox will contribute to elevate the level of security across Europe by providing the different actors involved in judicial proceedings with comprehensive tools to assure timely collection and the integrity of digital evidence. LOCARD's identity management and blockchain elements will also support accountability of justice and citizens' trust. Moreover, the crowdsourcing platform will put citizens in the loop, allowing them to timely report incidents.

LOCARD will provide Law Enforcement Agencies an innovative platform to manage digital evidence continuity of evidence easily, as well as a way to support cooperation and exchange of information between different jurisdictions. This will facilitate criminal investigations as well as assure evidence integrity for presentation in a Court. The project will as well greatly benefit private organisations, especially those engaged in the providing of digital services and add an innovative set of services to any portfolio allowing security providers to easily integrate digital forensic into their offer.

5 Future work

From a dissemination point of view, four kind of dissemination activities have been considered and should be carried out targeting the different audience groups to generate awareness, understanding and adoption.

1. **Analyse the real needs of stakeholders**: for the creation of a network of stakeholders, we will identify interested actors and relevant stakeholders, considering potential LOCARD end-users from the public and private sectors. LOCARD will foster the creation of a network of European stakeholders from which it will collect their needs (for different stakeholders' perspectives) in terms of security requirements, threat intelligence, incidents, and significant use-cases in a structured manner. The stakeholder group will be involved in identifying their system criticalities and the security requirements still not satisfied by current platforms.
2. **Dissemination aimed at increasing awareness of LOCARD** (Awareness Dissemination): create awareness of the project and its goals through target audiences that do not require a detailed knowledge of the project achievements. The purpose of this action is to generate traction in target groups without a technical background. Tools such as the project website, social media channel and some events should be used for that purpose.
3. **Dissemination aimed at increased understanding of LOCARD** (Understanding Dissemination): dedicated to the direct beneficiaries of the project outcomes. These audiences should reach a deeper understanding of the project's work and goals.

4. **Dissemination for adoption** (Action Dissemination): this kind of dissemination is meant to involve target groups in the project activities and to promote the project's results for adoption, aiming to influence and change capability within their organizations through their skills, knowledge and understanding of the LOCARD results for achieving real change.

On the technical side, the development of the platform will be focused on four different use case scenarios (automated collection of digital evidence and case management, suspected presence of pedopornographic material, data exfiltration from an organization's database server and illegal streaming of unlicensed content) to build a long-term sustainable business model for the system, from an economical, commercial, and societal point of view.

References

1. LOCARD Homepage, https://locard.eu
2. EEMA Annual Conference Homepage, https://www.eema.org/event/eema-annual-conference-2019/
3. APWG.eu Symposium Homepage, https://apwg.eu/bucharest-global-cybersecurity-awareness-2019/