INSPECTr Project

Intelligence Network & Secure Platform for Evidence Correlation and Transfer

Quarterly Newsletter: Fifth Edition

Edition: April 2022

Dear Colleagues,

Welcome to the INSPECTr project newsletter, a guide to our latest work and news.

INSPECTr Principal Objectives Brief Summary

Intelligence
Network &
Secure
Platform for
Evidence
Correlation and
Transfe**r**

To develop a shared intelligence platform and a novel process for gathering, analysing, prioritising, and presenting key data to help in the prediction, detection, and management of crime in support of multiple agencies at local, national, and international level. This data will originate from the outputs of free and commercial digital forensic tools complemented by online resource gathering. The final developed platform will be freely available to all Law Enforcement Agencies (LEAs).

INSPECTr Newsletter Fifth Edition

In this, our fifth edition, we will provide updates on our last quarter activities, information about meetings and events attended, our upcoming events, recent dissemination activities and a blog on the subject of the most recent Living Lab experimentation undertaken in the project.

BLOG

Introduction to INSPECTr Living Labs Experimentation

A network of LEA Living Labs was to be set up both organisationally and technically to specify requirements, experiment with and test the project outputs, and create the nucleus for the **sustainable use of the INSPECTr platform by LEAs throughout Europe**. Each LEA Living Lab was to provide an experimentation and a test-bench environment primarily and initially with mocked evidence from scenarios created by LEA partners to test the requirements, accuracy, and user acceptance of the platform. Use Case mocked but realistic evidence was then prepared by our Law

Enforcement project partners for experimentation and testing of the INSPECTr platform's functional and non-functional characteristics and have been developed to utilise the majority of the technological developments. Numerous forensic analysers and intelligence gathering tools are required to process both digital and non-digital items.

Early Milestones: An early milestone in the project was to define the common processes and baseline resources in LEA Living Labs to experiment towards producing a detailed requirements pipeline. This required comprehensively detailing the LEAs coordination and experimentation environment, each of the investigative tools used, and an in-depth analysis of a 3-stage questionnaire process completed with the support of our LEA partners. All of the efforts throughout this task were geared towards establishing a solid collaborative environment for LEAs. Based on LEA experimentation and feedback, the technical partners were able to extract the initial requirements and specifications for the forthcoming INSPECTr platform, which was being developed in parallel within the other relevant work packages. This process provided invaluable knowledge to inform the Consortium of what is expected of the INSPECTr platform, regarding its performance and functionalities that are most relevant to LEAs' investigative workflow.

Key Approaches: Using both structured and unstructured data as input, the developed platform will facilitate the ingestion and homogenisation of this data with increased levels of automatisation, allowing for interoperability between outputs from multiple data formats. Various knowledge discovery techniques will allow the investigator to visualise and bookmark important evidential material and export it to an investigative report. In addition to providing basic and advanced (cognitive) cross-correlation analysis with existing case data, this technique will aim to improve knowledge discovery across exhibit analysis within a case, between separate cases and ultimately, between inter-jurisdictional investigations. INSPECTr will deploy big data analytics, cognitive machine learning and blockchain approaches to significantly improve digital and forensics capabilities for pan-European Law Enforcement Agencies (LEAs).

Data Formatting: The appropriate formatting and structure of data has been an important consideration in the project from the outset, with the project ultimately opting for the open-source Cyber-investigation Analysis Standard Expression (CASE, https://caseontology.org) language. This is a community-developed ontology designed to serve as a standard for interchange, interoperability, and analysis of investigative information in a broad range of cyber-investigation domains. CASE provides a structured specification for representing information that is analysed and exchanged during investigations involving digital evidence. CASE also enables the merge of information from different data sources and forensic tool outputs to allow more comprehensive and cohesive analysis.

Gadgets: In INSPECTr our aim was always to be able to use our own tool outputs and develop a 'Toolbox' of data enrichment analysers, or as we call them, 'Gadgets' with the idea being that we would have free forensic tools and all of the outputs of these tools would be fed into the storage layers and accessible through the Case Management System.

Testing the Technology

Mocked use case development: 3-part scenarios scheduled to match the technology agenda

A challenge that presented early in the project was how can we test the technology while respecting **data privacy and GDPR**? The use of existing evidential data from historical cases for testing our platform would clearly contravene these. Therefore, the decision was taken early, to use mocked data for our experiments.

To replicate "real-life" investigations, our experienced law enforcement partners were tasked with developing three unique scenarios to be investigated, each with fake suspects and a rich history of communication across numerous sources of evidence. The evidence they created also reflects the volume of information that investigators see in real-life and the linkage between actors under investigation.

By using mocked evidence, our law enforcement partners can openly discuss issues with the platform with developers, while respecting ethical considerations. The use cases have been developed in three parts and address features of the platform as it develops. There are six phases of technology developments on the platform, so we wanted the LEAs to map the technology agenda to each part of their use case and get more technical as they develop.

Living Labs Phase 1 - April 2021

In April 2021, the INSPECTr technical partners demonstrated the features of the platform to law enforcement partners for the purposes of familiarisation and for gathering feedback on the developments to date.   A lot of services, which had so far been developed in isolation, were ready to be integrated in preparation for the next phase of development. It was essential to get the views and observations of our law enforcement partners prior to moving to this next stage and use their valuable feedback to guide the continued development of the platform technology.

Further Development of the INSPECTr Platform

Until this point, the INSPECTr project's primary focus had been on developing the platform rather than on a live environment but with the Living Labs, this was all set to change. The work carried out in the early parts of the project to understand the hardware, software and service requirements meant we had a good foundation for deployment. This initial planning phase meant that we had applicable hardware for the requirements mentioned above. We had several conditions in mind for the hardware planning phase, virtualisation capable hardware, easy expandability, and hardware uniformity; if we had an issue with one device, we would have the same issues with other devices. We also understood that asking partners to install multiple devices wasn't feasible and determined virtualisation as a critical aspect of our needs. Most infrastructure today is developed to be one device for many services. The hardware was selected with extendibility in mind and had an upgrade path available if the system needed more resources or if the project required more performance in future.

The above gives a brief overview of the hardware, but next comes the software and technologies aspect of the project. Virtualisation of services was the most important. Virtualisation allows us to have multiple services carrying out various functions; each node is a network in a box, providing all requirements for running a node on the INSPECTr network. To further segregate the hardware resources and separate them into parts that allow multiple services to work independently of one another, we used Docker. Docker allows more functionality than just segregation of resources, such as live updates of services, instead of requiring redeployment and shutting down systems to update. The platform's development process required such technologies, which became fundamental during the deployment process for the Living Labs.

So we have the technology and the hardware, but now came the question of how we would deploy it. There are numerous steps in the platform's deployment, but there was a degree of automation available due to having the same hardware in each case. We carried out the deployment with an automation framework that allowed us to deploy operating systems and software and set up each node as a replica of one another while not directly replicating. The strategy allowed us to deploy all living lab infrastructures within two days and have the Living labs up to date with the current rate of development pace. So, when developers need to update or modify code after deployment, changes made in the code management system (cms) are pushed to all Living Lab nodes. After a few minutes, these changes are live on all Living Lab nodes. Rather than waiting days for updates to software or, in the case of some commercial offerings, potentially months, these changes can be made much faster and with less downtime. More rapid deployment is not a silver bullet to software updates, but it gives allows the technical team to send code from developer to platform with fewer delays and minimal platform downtime.

Living Labs Phase 2 – March - April 2022

Phase 2 testing of the INSPECTr platform, using mocked evidence Use Cases, allowed our Law Enforcement partners (LEAs) to test our software in March and April 2022.

For this testing phase, formal feedback was gathered from our LEAs by means of a survey and informal feedback was gathered at a meeting of the Law Enforcement Steering Group following the completion of the testing phase. Feedback on the overall approach of the platform's development was positive, with our law enforcement partners clearly understanding the 'vision' of the INSPECTr platform and how it could be used and useful for investigative purposes. Overall, there was a good level of satisfaction with the ease of new case creation, which was found to be simple and intuitive, as well as the process of logging in, the widgets interface, and how to execute INSPECTr gadgets (but with a few issues still requiring more clarification on how to use them).

More detailed feedback was further provided by our LEA testers on individual elements of the platform where issues had arisen highlighting the need for further platform development and refinement in these areas. These elements included the following:

- some work and refinement on datatypes and gadget names needed, ensuring that the platform is more intuitive in the future
- numerous tasks should be grouped, to improve the usability of the interface. This will be addressed later in the project using workflow programming
- some minor adjustments to the data would be required, to simplify what will be a very intuitive analytic system.

LEA feedback on the issues of data security, data deletion, data sharing and exchange were expected issues as they are still currently in the development pipeline and were not expected to be ready for this testing stage. The main focus for this stage was to provide basic data processing and analysis. As a result, LEA participants provided very positive feedback on the way data can be ingested and processed and the visual reports (widgets) for each gadget.

Summary

This had been the first opportunity in the project to test the Use Cases in this much depth and it proved to be an extremely useful exercise and a great learning experience in terms of how the concerns of law enforcement can be addressed. The engagement of the INSPECTr law enforcement partners in developing the mocked evidence Use Cases, participating in the testing phase, and in providing feedback, has been invaluable. It has also been very encouraging from the technical side that the technical team were able to fix bugs and resolve issues raised during testing quite quickly. The issues raised during testing were tracked and categorised into headings of minor, major and critical. Only one critical type was recorded and that is the fact that evidence is not currently being segregated by case ID. This was a known factor prior to testing and is scheduled to receive remedial action before the next Living Lab. The technical team will also continue to work on the refinement of gadgets, widgets and dashboards and the way SIREN accesses the data, speeding that up and have greater linkage and better analytics overall. A more detailed demo will be prepared and provided to participating law enforcement partners ahead of the next Living Lab, Living Lab 3, which has been scheduled for 21st-23rd June 2022. This will be held in UCD, hosted by the INSPECTr Coordinator.

Further Opportunities for INSPECTr Dissemination and Cross-Project Learning and Collaboration

1. Europol Cyber Bits - Series: Tools:

This release from Europol in March 2022 included information about the INSPECTr project, its principal objective, information about the platform, and how FREETOOL outputs are being incorporated into the project with the benefit of this approach being that LEA can use the tools on a common platform. This dissemination opportunity provided an excellent channel for INSPECTr (and FREETOOL) as this release was received by 700 LE members.

2. 9th Annual Meeting of the Expert Group on Drugs Online held in the Council of Europe Headquarters, Strasbourg on 13th and 14th April 2022:

A member of the INSPECTr Project Coordinator team attended this meeting. Key discussion points of the meeting were:

- the close and effective cooperation with international bodies, the private sector, judiciary, and law enforcement in tackling the marketing and distribution of 'drugs online' is an ever-growing need.
- a multidisciplinary structure with professional cooperation with all partners is a key element to the success of this cooperation format.

The focus of the 2022 meeting was on online drug trafficking trends and modus operandi, tools for law enforcement cooperation, encryption technologies, instant messaging applications and case studies. The meeting brought together thirty-six experts from eighteen different countries and five international organisations. For the first time, Trinidad and Tobago participated as observer in meeting.

The INSPECTr presentation to the group focussed on the INSPECTr concept and basic architecture view and its principal objectives. The presentation was very well received with post presentation discussions taking place between LEAs.

Project Activities and Events between January 2022 – April 2022

- INSPECTr Monthly Project Meetings
- INSPECTr Weekly Technical Meetings
- INSPECTr LSG Monthly Meetings
- Ethics Work Package Monthly Meetings
- EARG Ethics Advisory and Review Group
- Living Labs Experimentation Phase 2

Meeting activities have continued throughout the first quarter of 2022:

- Monthly project meetings provide an overview of the activities undertaken in each work package.
- Weekly technical meetings provide a collaborative space for colleagues to discuss and demonstrate the evolving technical elements of the platform.
- Monthly meetings of the Law Enforcement Steering Group (LSG) ensure that the technical developments taking place in the platform remain aligned with the needs of law enforcement and continue to mirror the LEA investigative workflow.
- Ethics work package monthly meetings continue to be held in order to reinforce the project's Ethics-by-Design approach and allow time for deeper consideration and exploration of ethical issues that arise throughout the duration of the project.
- EARG - Ethics work package meetings are further supported by regular consultation taking place with the project Ethics Advisory and Review Group (EARG), a mandatory board established to offer relevant independent expertise on ethics issues.

Conferences, Workshops, and Future Events

INSPECTr Consortium Attendance at Conferences and Workshops

- SRE 2022 - Security Research Event
  1st-2nd March 2022 - CANCELLED
- 9th Annual Meeting of the Expert Group on Drugs Online, Council of Europe, Strasbourg
  13th – 14th April 2022

INSPECTr Consortium Attendance at Forthcoming Events

- Artificial Intelligence Hackathon
  Higher Institute of Electronics of Paris ISEP
  13th - 15th May 2022
- EAFS 2022 – Stockholm
  EAFS is a triannual conference on forensic science hosted by ENFSI (European Network of Forensic Science Institutes)
  30th May – 3rd June 2022
- CEPOL Research and Science Conference 2022 MRU, Vilnius: Preparing Law Enforcement for the Digital Age
  8th – 10th June 2022

Closing

We look forward to updating you further in August 2022 with our sixth edition of the INSPECTr Newsletter. In the interim, communications from our readers are welcome and if you wish to contact us or subscribe to our Newsletter you can e-mail us directly at inspectr@ucd.ie. Further information and updates can also be found on our project website https://inspectr-project.eu/.