D6.10 Data analytics for LEAs (OTHER)

Lead Beneficiary:	PERFORMANCE TECHNOLOGIES ANONYMOS ETAIRIA PLIROFORIKIS (PT)
Dissemination Level:	PU
Date:	31/05/2024
GA Number:	101102641

The TRACY project has received funding from the DIGITAL 2022 programme under grant agreement No 101102641.

Project Information

Grant Agreement Number	101102641
Acronym	TRACY
Name	a big-data analyTics from base-stations Registrations And Cdrs e-evidence sYstem
Topic	DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI
Free keywords	Digital SME Support Actions
Start Date	01/06/2023
Duration	24 Months
Coordinator	Performance Technologies SA

Document Information

Work Package	WP6: Dissemination, Exploitation and EU Impact
Deliverable	D6.10 Data analytics for LEAs
Date	31/05/2024
Type	OTHER
Dissemination Level	Public (PU)
Lead Beneficiary	PT
Main Author(s)	Nikos Avgerinos (PT)
Contributors	Manolis Tsangaris (PT), Panagiotis Mertis (PT)
Document Reviewers	Konstantinos Filis (OTE)
Security Reviewer	George Kalpakidis (HPOL)
Ethics Reviewer	Kasia Kostka (TIMELEX)

Revision History

Version	Date	Author	Comments
0.1	27/05/2024	Nikos Avgerinos (PT)	Initial Structure and Content
0.2	28/05/2024	Nikos Avgerinos (PT)	Provided description per section
0.3	29/05/2024	Manolis Tsangaris (PT), Panagiotis Mertis (PT)	Final version ready for review
0.4	30/05/2024	Konstantinos Filis (OTE), Kasia Kostka (Timelex)	Review deliverable
0.5	30/05/2024	Nikos Avgerinos (PT)	Incorporated comments
0.6	30/05/2025	George Kalpakidis (HPOL)	Final review
1.0	31/05/2024	Nikos Avgerinos (PT)	Final version ready to submit

Disclaimer

Copyright

Abbreviations

EU	European Union
LEA	Law Enforcement Agency
NCD	Non-Content Data
PT	Performance Technologies
TRACY	a big-data analyTics from base-stations Registrations And Cdrs e-evidence sYstem

List of Figures

List of Tables

1 Table of Contents

Executive Summary

Include an one page project summary

Deliverable D6.10 “Data Analytics for LEAs” is one of the outputs of task T6.1 “Preparation and implementation of the Dissemination, communication and exploitation Plan”.

This report presents a quick summary of the Data Analytics for LEAs workshop organized by PT during M12 of the project in hybrid mode allowing both physical and remote presence. In total more than 50 representatives from 18 different competent authorities (Law enforcement and Public authorities) were registered to attend the event.

The agenda included four main aspects: a presentation for TRACY projects and a demo of the TRACY mini-platform for investigation based on NCD data, presentations from two companies experts in their domain; SAS presenting Visual Investigator and Chainalysis presenting crypto investigation solution, and finally a round table discussion where all participants had the opportunity to discuss current needs and challenges in data analytics domain.

2 Introduction

Brief Introduction

In the context of T6.1 “Preparation and implementation of the Dissemination, communication and exploitation Plan” certain dissemination activities are described. One of them is a workshop entitled “Data Analytics for LEAs” that was planned to take place on M12 of the project lifetime.

TRACY “Data Analytics for LEA” workshop was centered around two state-of‑the-art analytics platforms, that can be used to support the LEA investigations. As today’s crimes become more and more complex, data driven crime analysis becomes a necessity. On a different note, crime analysis needs to provide supporting evidence that can be used in the court of law, so it must be transparent, reliable, and explainable. With those motivations during the workshop two commercial platforms were presented ending with a roundtable discussion.

The first platform is SAS Visual Investigator, which transforms criminal investigations with advanced analytics, data integration, and visualization tools. By analyzing disparate data sources, it uncovers patterns and connections crucial for identifying and apprehending suspects. Its intuitive interface streamlines workflows, empowering law enforcement agencies to combat crime effectively and safeguard communities.

The second platform we present is Chainalysis, a leading blockchain analysis platform used for investigating and preventing cryptocurrency-related crime. It provides law enforcement, regulators, and businesses with tools to track and analyze cryptocurrency transactions, identifying illicit activities such as money laundering and fraud. Chainalysis helps ensure compliance with regulations and enhances trust in the digital asset ecosystem.

The last part of our workshop was a round table discussion on the role of Analytics Platforms in law enforcement investigations, especially as it relates to the previously described platforms. We will attempt to analyze and answer questions such as, how to best utilize those platforms to enhance the investigation process, what are the potential challenges (such as ethical and privacy considerations), or how to produce case studies to further realize values and challenges.

3 Workshop Information

The "Data analytics for LEAs" is part of the TRACY project Dissemination, Communication and Exploitation strategy being one of the at least four key dissemination activities included in the project plans.

The TRACY "Data Analytics for LEAs" workshop was centered around two state-of‑the-art analytics platforms, that can be used to support the LEA investigations. As today's crimes become more and more complex, data driven crime analysis becomes a necessity. On a different note, crime analysis needs to provide supporting evidence that can be used in the court of law, so it must be transparent, reliable, and explainable. With those motivations we organize a three-step workshop, presenting two platforms and ending with a roundtable discussion.

The first platform was SAS Visual Investigator, which transforms criminal investigations with advanced analytics, data integration, and visualization tools. By analyzing disparate data sources, it uncovers patterns and connections crucial for identifying and apprehending suspects. Its intuitive interface streamlines workflows, empowering law enforcement agencies to combat crime effectively and safeguard communities.

The second platform presented was Chainalysis, a leading blockchain analysis platform used for investigating and preventing cryptocurrency-related crime. It provides law enforcement, regulators, and businesses with tools to track and analyze cryptocurrency transactions, identifying illicit activities such as money laundering and fraud. Chainalysis helps ensure compliance with regulations and enhances trust in the digital asset ecosystem.

The last part of our workshop provided a round table discussion on the role of Analytics Platforms in law enforcement investigations, especially as it relates to the previously described platforms. We attempted to analyze and answer questions such as, how to best utilize those platforms to enhance the investigation process, what are the potential challenges (such as ethical and privacy considerations), or how to produce case studies to further realize values and challenges.

3.1 Workshop Agenda

Below is the agenda of the workshop, Table 1. It was hosted by Performance Technologies (PT) at its premises on the 24th of May 2024. The workshop started at around 09.00 CEST and lasted until 14.00 CEST.

Prior to the event an announcement has been uploaded to the project website, Figure 1. Both physical and remote access were considered for this event. The MS Teams link was sent to all colleagues that have registered via the TRACY project website, Figure 2.

Table 1 TRACY "Data Analytics for LEAs" workshop agenda

TRACY Data Analytics for LEAs Workshop – 24 May 2024 – Agenda – (09.00 CEST – 14.00 CEST)	
08.45 – 09.00	**Audience connection**
09.00 – 09.15	**Welcome message and introduction**
09.15 – 09.30	**TRACY Overview** • Brief introduction of the project
09.30 – 11.00	**SAS Visual Investigator** • Presentation • Demo
11.00 – 11.30	*Coffee break*
11.30 – 13.00	**Chainalysis – Crypto Currency Analytics** • Presentation • Demo
13.00 – 13.45	**Roundtable Discussion** • The role of Analytics Platforms for LEA incidents
13.45 – 14.00	**Wrap up and conclusions**

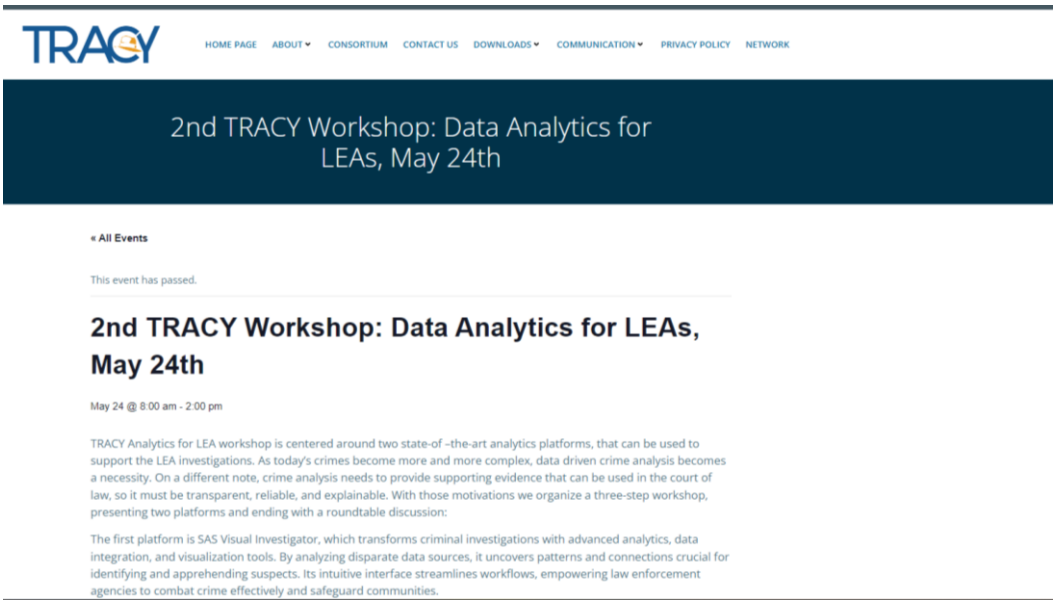


Figure 1 TRACY "Data Analytics for LEAs" workshop announcement on the project website

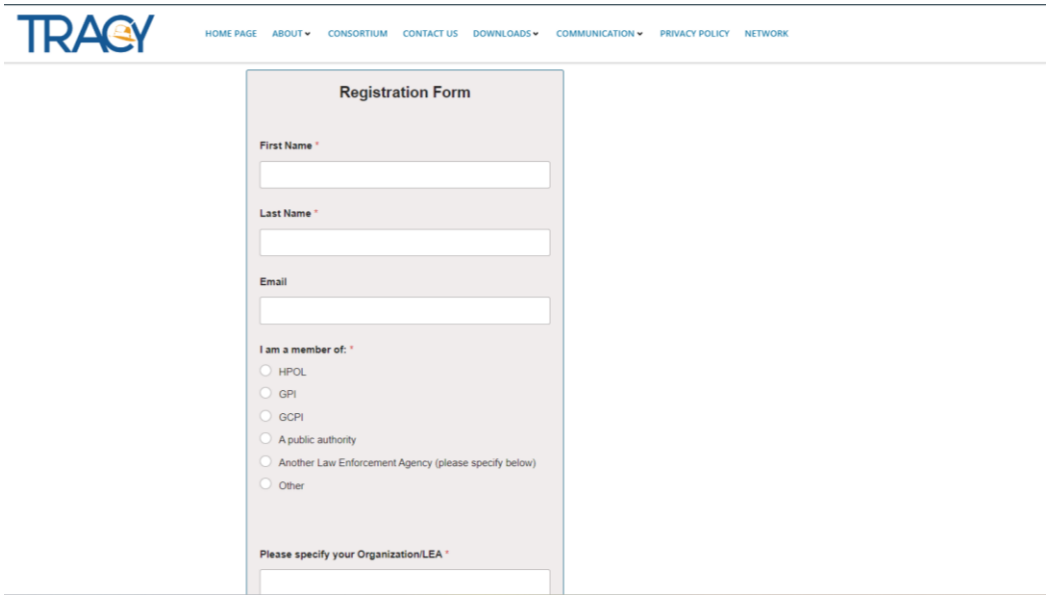


Figure 2 TRACY "Data Analytics for LEAs" workshop registration form on the project website

3.2 Workshop audience

The target groups of interest of the TRACY "Data Analytics for LEAs" workshop were a) Project internal stakeholders; mainly LEAs and b) Project external stakeholders; mainly LEAs and public authorities.

To maximise the outreach TRACY mobilised the network with other EU projects. In this sense the announcement was sent to several EU projects such as LAGO, POLIIICE, CYCLOPES, CYBERSPACE as well as to the TRACY Advisory Board Members.

Below is the full list of authorities that have attended the workshop.

Project internal stakeholders; mainly LEAs:

- HELLENIC POLICE (HPOL),
- INSPECTORATUL DE POLITIE JUDETEAN GALATI (GCPI) and
- INSPECTORATUL GENERAL AL POLITIEI (GPI).

Project external stakeholders; mainly LEAs and public authorities:

- Ministry of Internal Affairs of Georgia
- Police and Border Guard Board, Republic of Estonia
- ERTZAINTZA - BASQUE COUNTRY POLICE
- ACADEMY OF THE MINISTRY OF INTERNAL AFFAIRS OF GEORGIA
- Belgian Police PZ 5417 MC
- An Garda Síochána, Ireland
- Italian National Police
- District Prosecution Office, Albania

- Central Criminal Police Department of MIA of Georgia
- Gendarmerie, France
- NCC CZE, Directorate of Foreign Police Service, Police of the Czech Republic
- North Wales Police, United Kingdom
- State Police of Latvia
- Malta Police Force Cyber Crime Unit
- Zentrale Kriminalinspektion Oldenburg - Police Germany
- GNR, Portugal

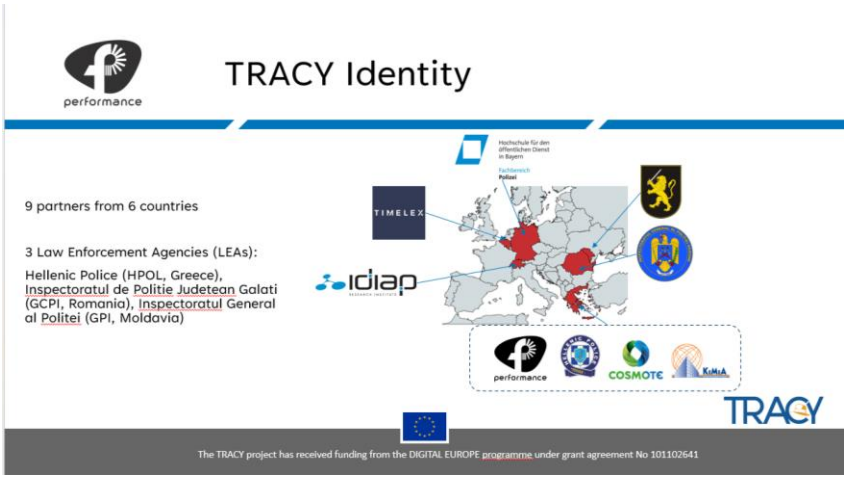
Below is the representation of the geographical spread of the stakeholders that attended the TRACY "Data Analytics for LEAs" workshop. The external stakeholders represented 15 different LEAs and Public Authorities across the European Union offering very satisfying visibility to the project activities. At the same time this shows the high interest of the relevant authorities to attend and be informed about such topics.

(a) (b)

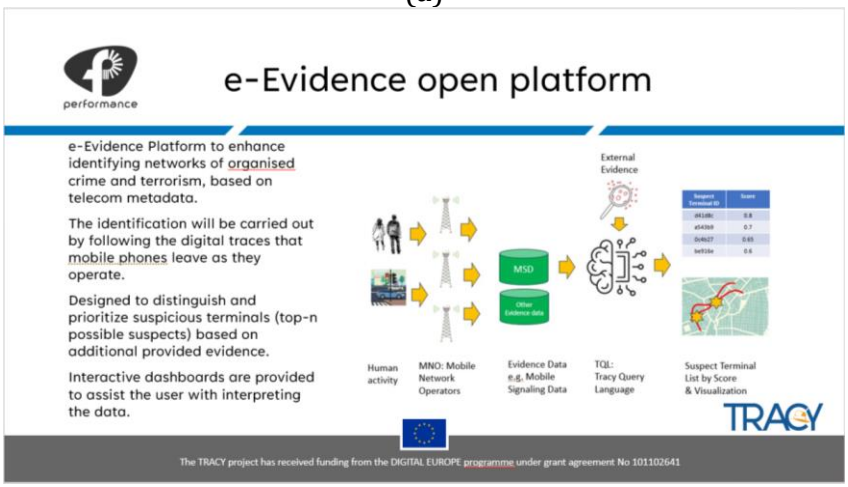
Figure 3 Geographical spread of stakeholders attending the workshop, a) project external and b) internal stakeholders.

3.3 Workshop material

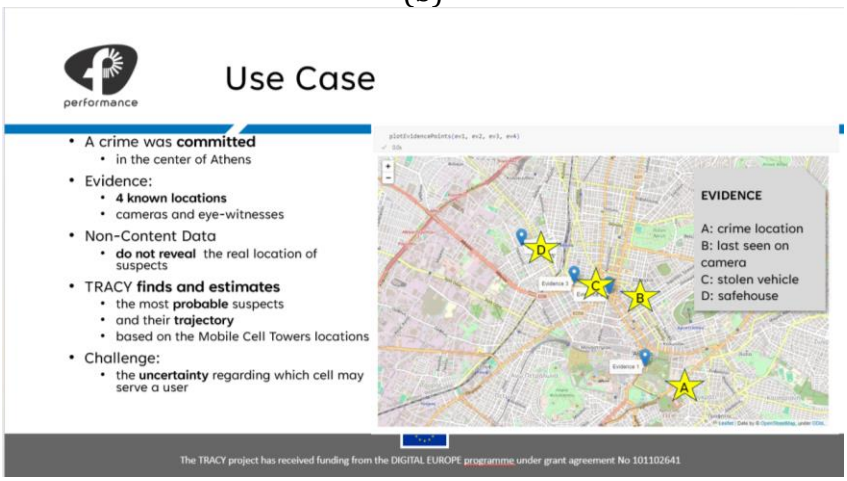
As indicated in the agenda the workshop had three main presentations. The first was for TRACY project activities presenting a general description of the project activities as planned. The presentation also highlighted the presence of the TRACY mini-platform available to TRACY project partners. PT did a quick presentation of the mini-platform showcasing synthetic NCD dataset handling while conducting an investigation of a realistic case. Below are some indicative images of the material included in this presentation, Figure 4.


TRACY Identity
performance
9 partners from 6 countries
3 Law Enforcement Agencies (LEAs):
Hellenic Police (HPOL, Greece),
Inspectoratul de Politie Judetean Galati (GCPI, Romania), Inspectoratul General al Politei (GPI, Moldavia)
TIMELEX
idiap
COSMOTE
TRACY
The TRACY project has received funding from the DIGITAL EUROPE programme under grant agreement No 101102641

(a)

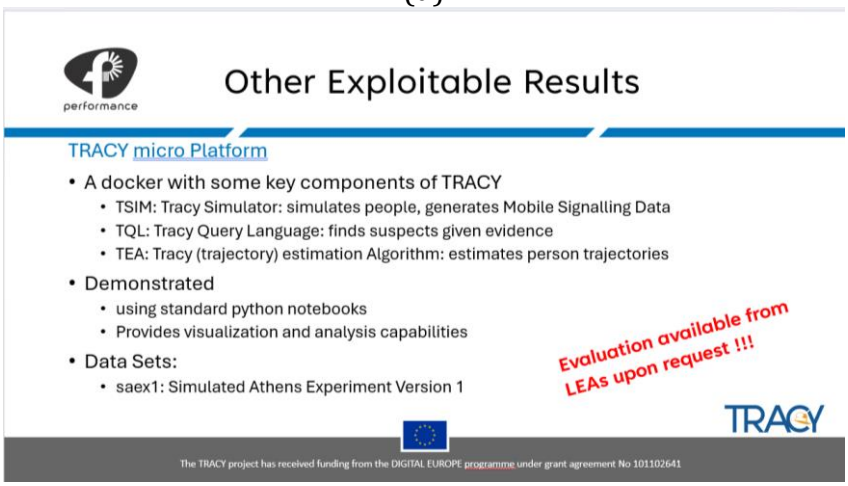

e-Evidence open platform
performance
e-Evidence Platform to enhance identifying networks of organised crime and terrorism, based on telecom metadata.
The identification will be carried out by following the digital traces that mobile phones leave as they operate.
Designed to distinguish and prioritize suspicious terminals (top-n possible suspects) based on additional provided evidence.
Interactive dashboards are provided to assist the user with interpreting the data.
External Evidence
MSD
Human activity
MNO: Mobile Network Operators
Evidence Data e.g. Mobile Signaling Data
TQL: Tracy Query Language
Suspect Terminal List by Score & Visualization
TRACY
The TRACY project has received funding from the DIGITAL EUROPE programme under grant agreement No 101102641

(b)


Use Case
performance
A crime was committed
in the center of Athens
Evidence:
4 known locations
cameras and eye-witnesses
Non-Content Data
do not reveal the real location of suspects
TRACY finds and estimates
the most probable suspects
and their trajectory
based on the Mobile Cell Towers locations
Challenge:
the uncertainty regarding which cell may serve a user
EVIDENCE
A: crime location
B: last seen on camera
C: stolen vehicle
D: safehouse
The TRACY project has received funding from the DIGITAL EUROPE programme under grant agreement No 101102641

(c)

(d)



(e)

Figure 4 TRACY presentation snapshots

The second presentation of the workshop was performed by Chainalysis. Organizations consistently choose Chainalysis to provide the most extensive and reliable real-world connections to on-chain data. Through robust crypto data collection and analysis, financial institutions, Web3 businesses, and government agencies gain the critical information necessary to make data-driven decisions that lead to positive outcomes such as solving cases faster, highlighting troublesome nation-state activity, and protecting their platforms by effectively managing risk.

Main solutions comprise:

- **CRYPTO INVESTIGATIONS**: Gain mission-critical intelligence to navigate crypto crime, ensure compliance, and advance the investigations. Operations are enriched with trusted, data-driven insights for swift, decisive action against crypto-related threats.
- **CRYPTO RISK**: Allows to keep pace with crypto's drive towards a secure, efficient, and compliant ecosystem. Adapt to evolving crypto risk, bolstering stakeholder platform's resilience against emerging illicit activity.

- **WEB3 GROWTH**: The web3 market offers significant opportunities for forward-thinking crypto businesses and consumer brands to become strategic leaders in this expanding ecosystem. Capitalize on this growth by building meaningful user relationships and strengthening the competitive edge, positioning the client at the forefront of an evolving industry.

When it comes to Crypto Investigations the main stakeholders of interest are Law Enforcement, Regulators, Tax Agencies, and Private Sector. For LEAs to effectively combat and prevent crypto crime with advanced analytics and intelligence focus areas include:

- Financial fraud detection
- Terrorism financing
- Identifying local and international fraud schemes
- Disrupting organized criminal networks such as CSAM and drug trafficking
- Preventing cyber extortion such as ransomware

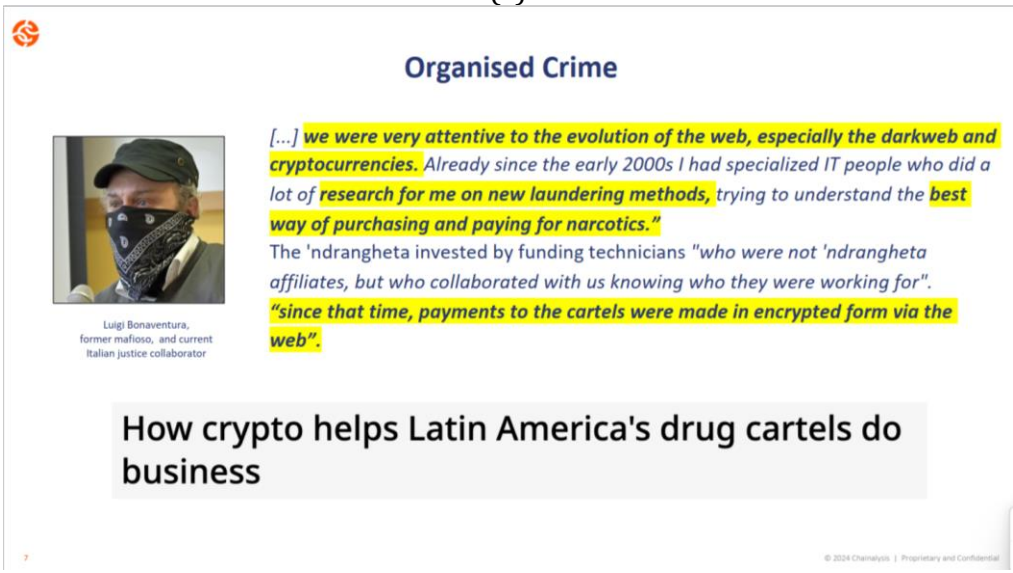
(a)


What do all these illicit activities have in common?
Ransomware
Darknet Markets
Terrorism Financing
Scams
Money Laundering
Child Abuse
Organized Crime
Drug trafficking

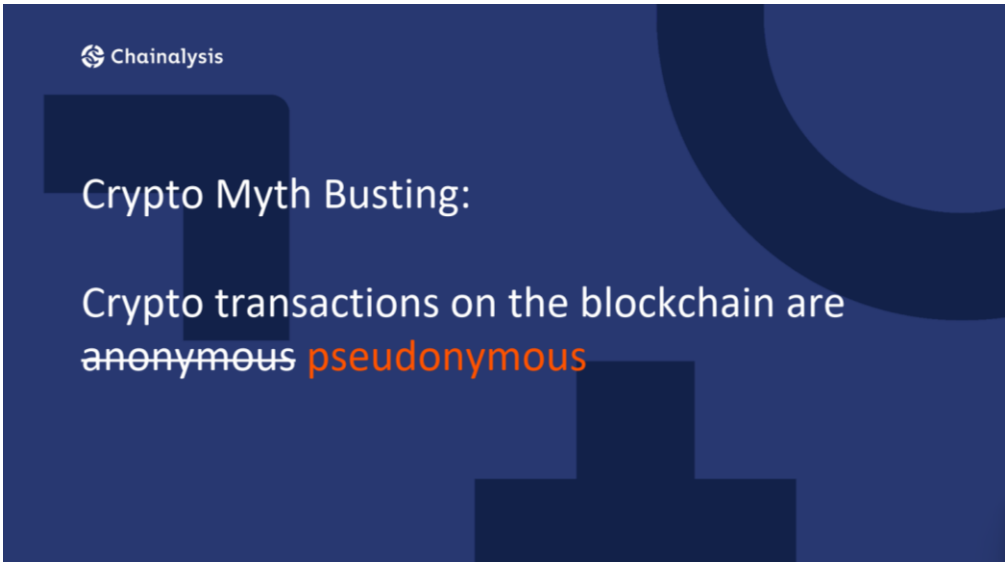
(b)


Ransomware
Cyber-hacking victims 'paid out record $1.1bn in ransoms last year'
Ransomware gangs targeted hospitals, schools and bodies such as BA and the BBC, Chainalysis finds
Total value received by ransomware attackers, 2019 - 2023
Ransomfeed

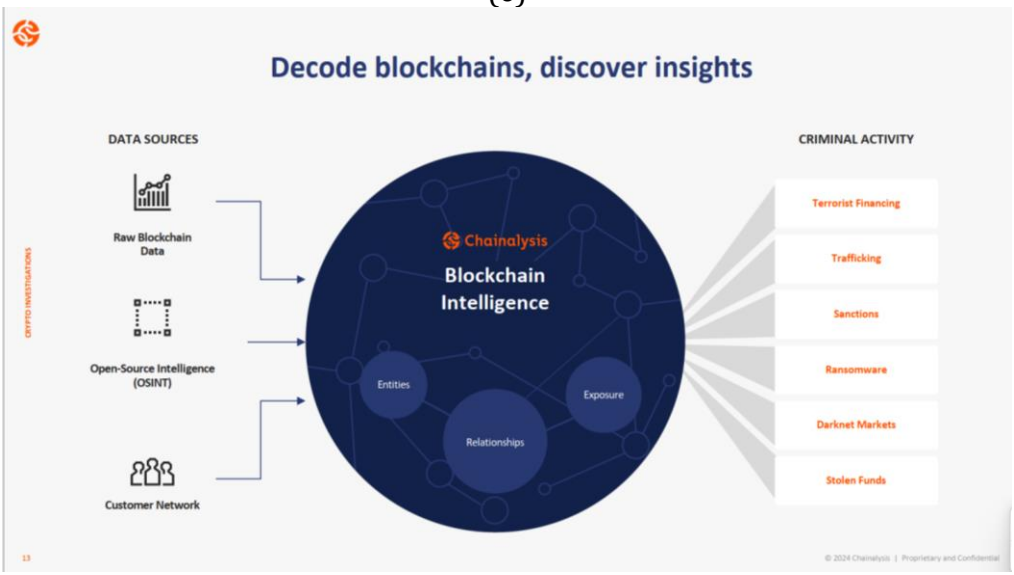
(c)


Organised Crime
Luigi Bonaventura, former mafioso, and current Italian justice collaborator
[...] we were very attentive to the evolution of the web, especially the darkweb and cryptocurrencies. Already since the early 2000s I had specialized IT people who did a lot of research for me on new laundering methods, trying to understand the best way of purchasing and paying for narcotics."
The 'ndrangheta invested by funding technicians "who were not 'ndrangheta affiliates, but who collaborated with us knowing who they were working for".
"since that time, payments to the cartels were made in encrypted form via the web".
How crypto helps Latin America's drug cartels do business

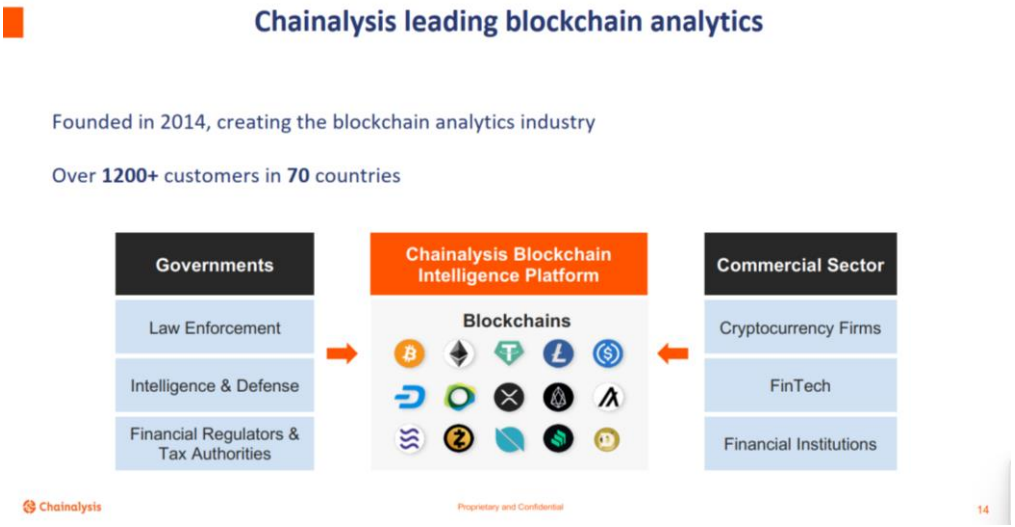
(d)


Chainalysis
Crypto Myth Busting:
Crypto transactions on the blockchain are
~~anonymous~~ pseudonymous

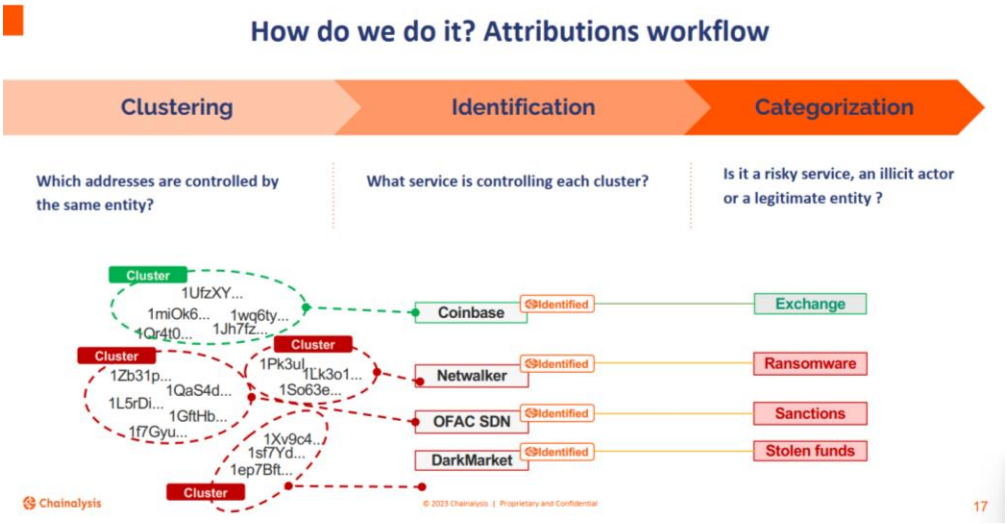
(e)


Decode blockchains, discover insights
DATA SOURCES
Raw Blockchain Data
Open-Source Intelligence (OSINT)
Customer Network
Chainalysis
Blockchain Intelligence
Entities
Exposure
Relationships
CRIMINAL ACTIVITY
Terrorist Financing
Trafficking
Sanctions
Ransomware
Darknet Markets
Stolen Funds

(f)


Chainalysis leading blockchain analytics
Founded in 2014, creating the blockchain analytics industry
Over 1200+ customers in 70 countries
Governments
Law Enforcement
Intelligence & Defense
Financial Regulators & Tax Authorities
Chainalysis Blockchain Intelligence Platform
Blockchains
Commercial Sector
Cryptocurrency Firms
FinTech
Financial Institutions
Chainalysis
14

(g)



(h)

Figure 5 Chainalysis presentation snapshots

The third presentation of the workshop was led by **SAS** presenting the **Visual Investigator** solution effectively addressing a wide range of intelligence analysis and investigation management needs in the cloud.

SAS Visual Investigator is a cloud-ready investigation and incident management solution that combines large, disparate, structured and unstructured data sources. Users can define, create, triage and manage alerts; perform detailed investigations; and customize the platform to meet their individual and organizational needs.

Dealing with mounting complexity, analysts and investigators need to boost their efficiency to make sense of the velocity of alerts and far-reaching networks. With SAS Visual Investigator, you can perform deep investigations to uncover hidden behaviors and activities, then share them across your organization for optimal team coordination.

SAS Visual Investigator is designed for banks and financial institutions looking for fraud and money laundering, national security and law enforcement organizations looking for terrorism and criminal activities, legal firms conducting discovery, and hospitals and public health organizations guarding against disease outbreaks.

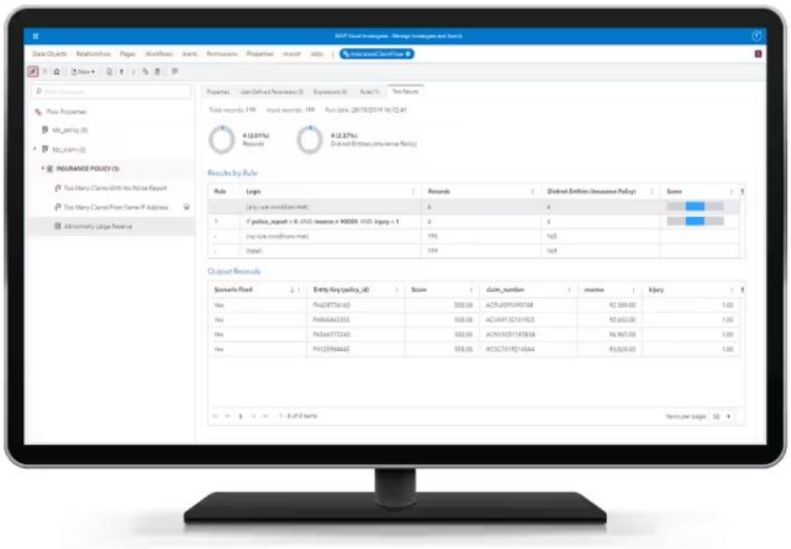
The SAS Visual Investigator capabilities include:

Adapt quickly to changing needs: Confront shifting tactics and emerging issues head-on. Our open, data-driven, hub-and-spoke approach gives you the agility to adapt to new trends and business problems, access new data sources and expand the solution's use across your business as needed. User-friendly administration and configuration tools – such as an interactive, drag-and-drop page builder – let you design and deploy new intelligence assets, and tailor the solution to each user's needs without requiring expensive customization.

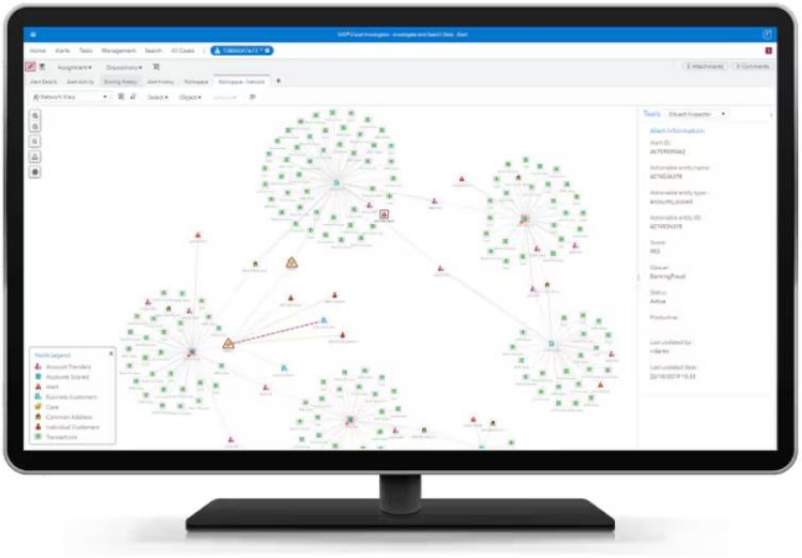
Expose hidden networks faster: An easy-to-use network viewer backed by powerful intelligence analytics lets you visualize and interactively explore entire social networks and their layout. You can expand or trim the network, explore communities and individual relationships, and expose obscured patterns and hidden connections. Interactive entity resolution capabilities deliver the most accurate picture of complex relationships. Entity analytics highlights potential areas of interest, showing entity closeness, betweenness and influence. You can see the complex network of relationships between people, places, things and events over time and across multiple dimensions.

Conduct more efficient, targeted investigations: A user-friendly interface empowers intelligence analysts and investigators to work more collaboratively and efficiently. Investigative workspaces provide interactive visualization and search capabilities for building, gathering, exploring, visualizing and manipulating data relevant to investigations and research. You can easily document findings by capturing views of search visualizations to narrate maps, timelines, networks and other content. Auditing information related to user activities is captured automatically by the system, and you can configure the level of detail captured to meet your compliance needs. In addition, you can design structured print templates that conform to regulatory requirements.

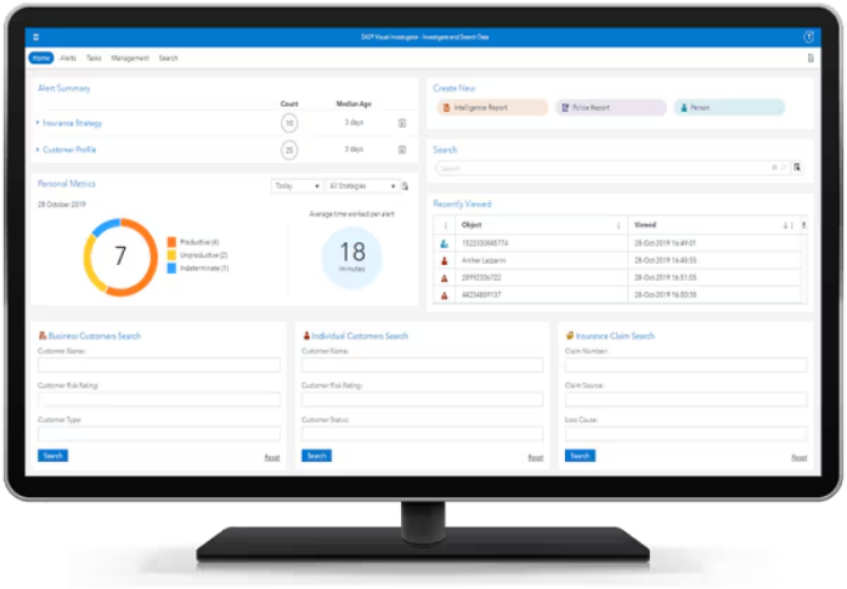
Turn insight into action. Fast: We've automated much of the data management, triage and workflow to empower users and increase efficiency. With an easy-to-use interface, users can import data, perform advanced searches, and apply temporal or geospatial methodologies to identify key patterns, connections, people and events hidden in complex data. Alerts are intelligently prioritized for expedient triage, investigation and disposition. And analysts and investigators are empowered to initiate cases for deeper investigation, as well as actively route or make decisions on events of interest as they occur, virtually eliminating information lag.



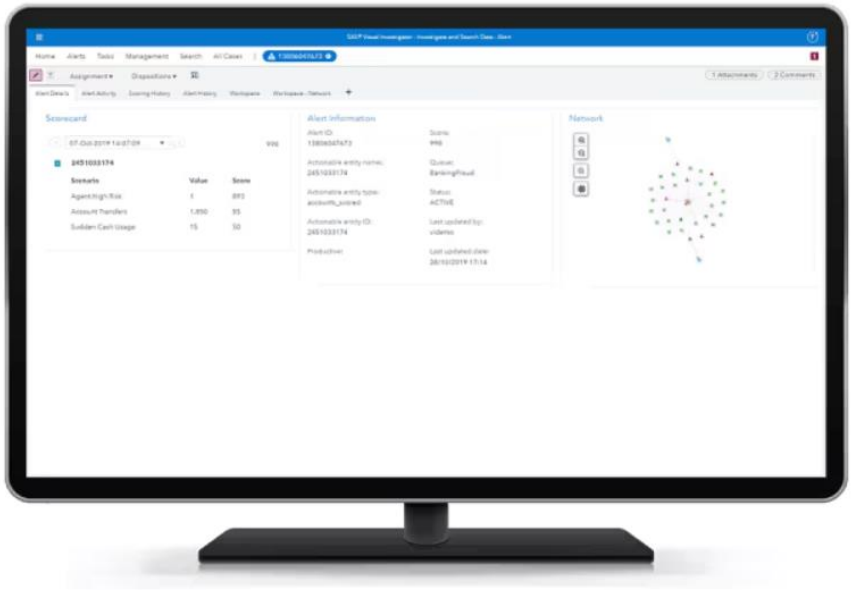
(a)



(b)



(c)



(d)

Figure 6 SAS presentation snapshots

4 Conclusion

Deliverable D6.10 is a summary report of the "Data Analytics for LEAs" workshop organised by PT in the context of task T6.1 "Preparation and implementation of the Dissemination, communication and exploitation Plan". In the context of T6.1 at least 4 meetings/workshops were included.

The main objective of this event was to give the opportunity to representatives from LEAs and other competent authorities to attend a workshop where modern tools in the domain of data analytics will be presented offering real life demonstrations covering operational needs based on the challenges that nowadays LEAs officers and investigators have to face.

The workshop succeeded to attract the attention of more that 20 representatives from 15 different competent authorities around EU apart from the TRACY partners. Top tier commercial solutions were presented to all participants describing features and capabilities as well as real life demos. This workshop was an opportunity to increase the visibility of TRACY around European authorities and increase the network of authorities that will later on follow TRACY project activities and could potentially be invited to other events positively contributing to the Dissemination and Communication aspects of the project.