

CRIME AS A SERVICE

MARKET & RESEARCH SCAN



2019-2020



Table of Contents

03

Introduction to the topic

11

Scenarios & Mind Mapping

12

Research Results

31

Market Solutions

52

About i-Lead & Conclusion

CRIME AS A SERVICE

One of the most growing trends in a cybercrime domain is the commercializing of cyber criminality so-called Crime-as-a-Service, in which the 'as-a-Service' part is based on business models from the legal corporate culture and incorporated in cybercriminal markets (underground economy). The aim is to provide easier access to digital means for the lesser skilled cybercriminal to achieve cybercrime. This lowering of the threshold may lead to an increase in the number of cybercrimes committed. The following figure shows an example of a CaaS.

On these flourishing 'underground' markets, a broad array of tools and services are offered. The cybercriminal can choose to purchase or rent entire packages, so-called 'toolkits', or to buy or rent parts of the toolkit. These toolkits can include malicious software, supporting infrastructure, stolen personal and financial data and the means to monetize criminal assets. The prices for these 'services' are completely out of proportion to the damage they can cause and can be paid by anyone who has a little bit of money and enough motivation for bad intentions. According to Europol, the thriving digital underground industry cost global economies an estimated USD 300+ billion per year in 2013, to an estimated USD 600 billion per year, according to last published report of McAfee.

'Investigating, targeting and disrupting cybercrimes associated with organized groups generating greatest harm and/or large criminal profits and cybercrime-as-a-service scheme', is described in Europol's programming document 2019 [2]. To investigate and disrupt these criminal activities, it is essential to understand what important (indispensable) enablers and actors are regarding CaaS schemes.

- Forums, websites and dark markets. The CaaS scheme is highly dependent on websites, forums, marketplaces and hubs where supply and demand meet. These are pre-eminently suitable places to buy/sell products and services, advertise, network, share experience and expertise.

- Actors:

- First level: administrators, experts (e.g. creators/code writers of malicious software).
- Second level: intermediaries, vendors, members.
- Third level: money mules.

- Supportive infrastructures. To stay under the radar from Law Enforcement, cybercriminals require infrastructure which provide a high level of anonymity and security. Hosting providers have a crucial role providing secure storage, especially Bullet-proof Hosting Services (BpHS). According to Europol, 'they are highly sought after in online marketplaces.' VPN and proxy services have an important part in providing anonymity to cybercriminals, as well as the TOR browser contribute in making it more difficult to trace.

As mentioned earlier, the CaaS scheme provides easier access to digital means for the lesser skilled cybercriminal to achieve cybercrime. This lowering the threshold can lead to an increase in the number of cybercrimes committed. At the same time, various services that anonymize criminal activities, such as BpHS, disrupt police investigations. As Europol describes the demand of these type of services is increasing, which in turn disrupts the investigations even more and making it more complex. The experts or code writers often stay off the LEA radar, because they outsource their criminal activities. Moreover, due to the diversity of the crimes involved, the organized criminal structure of CaaS and even more geographical diffusion of the crimes involved, investigations are very time consuming and difficult to solve.

CaaS PG workshop provided a great opportunity for LEA community:

- to identify the most common gaps, needs and challenges addressing CaaS crimes;
- to help in the decision making in the selection of the most promising technology areas to support and optimize investigation process;
- to identify areas that are the most targeted for innovations.

Five areas (technology, organizational, people, process and legal) that brings the biggest impact on the police performance have been selected by LEA practitioners. PG workshop report elaborates all areas in more detailed manner, highlights the biggest challenges and priorities for innovations and provides recommendations for the further improvements.



TECHNOLOGY

a) Encryption/decryption technologies:

CaaS workshop participants identified that majority of investigations involve the use of encryption intentionally to hide the data, communication evidences and criminal activities. Encrypted devices continue to be a big challenge for LEAs and the need for more decryption capabilities was repeatedly discussed by practitioners. Decryption is a time-consuming and expensive process and criminals frequently change the methods they use to protect communication. LEA shared priorities to address the issue:

- More tools to allow for dynamic interventions with more on-site capabilities that could allow more information to be obtained quickly;
- More cost-effective ways of dealing with decryption;
- The ability to decrypt in real-time.

b) Crypto-Currencies:

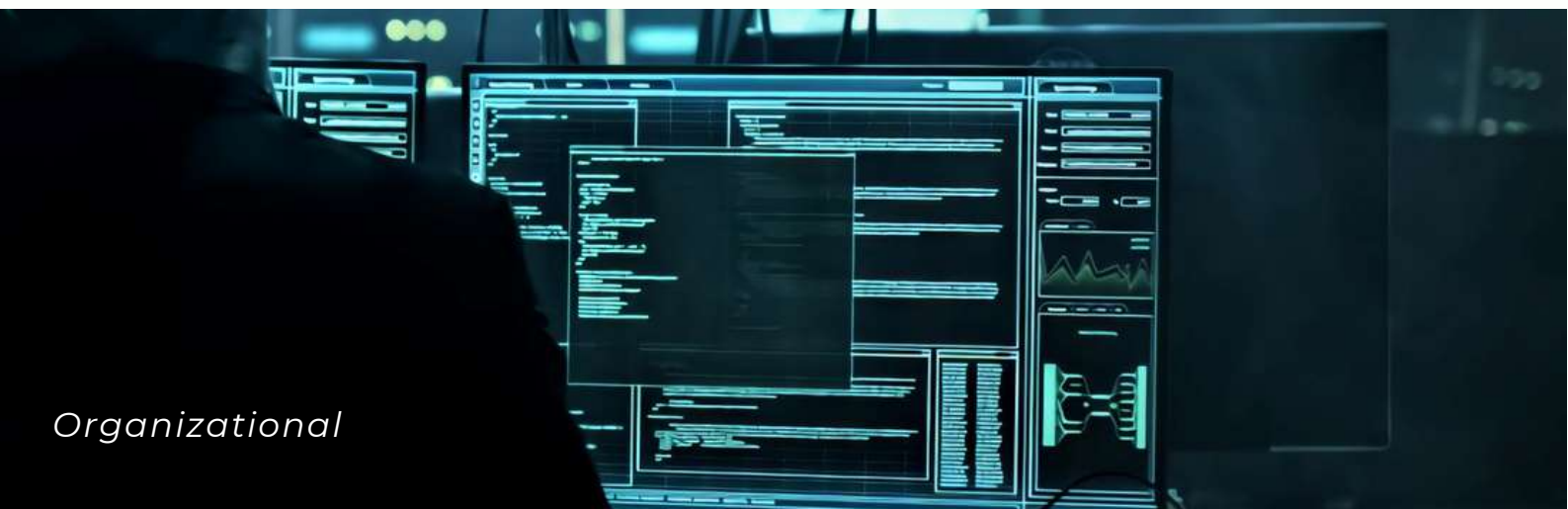
Crypto-currencies are widely exploited by cybercriminals and remains one of the key factors to perform criminal activities on the internet (e.g., rent or acquire packages of 'toolkits' to execute criminal activities and etc). Cybercrime investigations that involve crypto-currencies and blockchain analytics are growing rapidly therefore there is a huge demand for innovations to ensure that EU LEAs has relevant skills, tools and instruments to combat CaaS crimes.

c) Single tool to carry out all function:

Practitioners felt that there were currently a large number of tools available, many with a number of capabilities that weren't required. They agreed that they would like to see a number of these tools integrated into one tool that offered a broad range of capabilities. This tool should be straight forward to use for LEA's operational needs.

d) Secure data platform for experts:

A common requirement which arose during the practitioner presentations was the need for a platform where both operational and good working practices could be shared between LEAs. Some practitioners flagged that there was already the European Platform for Experts (EPE), however some users felt that it wasn't very intuitive and was difficult to use and access. Practitioners would also like a shared platform where a repository collection of useful open-source tools were available that could be easily accessed.



Organizational

ORGANIZATIONAL

a) Cooperation with Internet Service Provider (ISP):

Practitioners repeatedly expressed their frustration at the general lack of cooperation from Internet Service Providers (ISPs). When ISPs did comply with a request the timescale for a response was too slow. Discussions evolved as to whether European countries could collaboratively work together (possibly with the assistance of Europol) and exploit this greater scale to persuade ISPs to provide more assistance to LEAs in their criminal investigations.

b) International collaboration:

Arguably, the greatest problem faced by investigators is that cybercrimes, including CaaS crimes, are transnational. Often the criminals are in another country to the victim and it is problematic for LEAs to investigate or prosecute. There is a need to be greater cooperation at a political/judicial level between countries to combat these types of crimes. A common EU strategy would make it easier for LEAs to work together.

PEOPLE

a) Education for investigations:

Cybercrime is constantly evolving, and it is increasingly featuring in crimes being investigated by not just cybercrime specialist officers but also by crimes investigated by mainstream officers. As such, practitioners agreed that there is a need for continual training and education for all officers and technical staff – not just cybercrime investigators. Also, an LEA invest in new tools and technologies, however, often fail to train their officers on how to use them in the daily operations. As such these tools were often under-utilised. Practitioners would therefore like to see training as a matter of course for all new technologies introduced.

b) Multidisciplinary teams:

- OSINT
- Data analysis
- Financial investigations
- Cybercrime
- Malware analysis
- Mainstream officers to investigate aspects that didn't require a technical specialism

Cybercrimes are still often investigated in small, local teams where investigators try to perform a wide-ranging number of tasks. Practitioners felt that it is not practical for officers investigating cybercrimes to have all of the expertise required to investigate these types of crimes. A multidisciplinary team, where the unique expertise can be brought together, could be hugely beneficial. Practitioners agreed that preferably a team investigating cybercrimes would comprise of officers who had the following specialised skillsets:

```
Process
```

PROCESS

a) Interaction with private institutions:

As with ISPs, practitioners expressed their frustrations at the difficulty they often faced obtaining information from private institutions, particularly when the institution was located in another jurisdiction. Again, this often hinders a LEAs ability to investigate such crimes. As with ISPs, practitioners considered whether if countries worked collaboratively together, they could make use of this greater scale to persuade private institutions to provide more information to LEAs.

b) Improving intelligence/high situational awareness:

The subject of intelligence gathering was discussed and practitioners were of the same opinion that there were opportunities to improve the process. As stated previously, often many crimes can be linked to one organised crime gang.

Practitioners therefore stated that they needed the ability to easily and readily obtain information about the perpetrators and get 'the full picture'.

c) Improved workflow:

Practitioners agreed that the current workflow structure used by most LEAs is no longer suitable for investigating crimes with a cybercrime element due to the huge volume of data that can be accumulated during a digital investigation. To improve workflow practitioners suggested:

- the use of artificial intelligence to rapidly analyse the large quantities of data;
- a platform where practitioners can regularly share best and worst practices and share procedures;
- a move to victims being able to easily report crimes online;
- a standardized workflow across all LEAs for cybercrime.

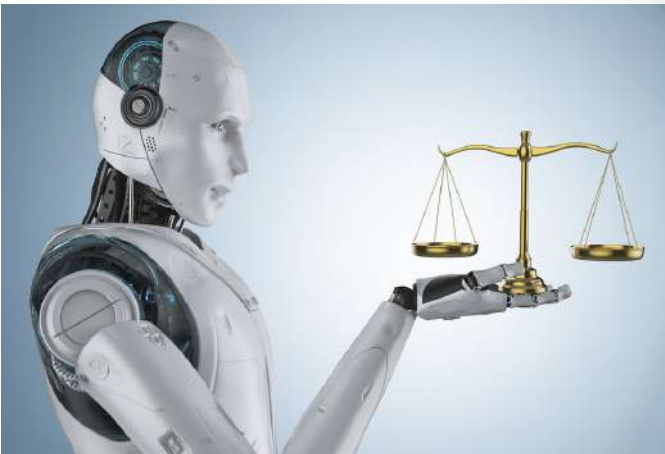


LEGAL

LEGAL

a) Jurisdiction:

As stated above, cybercrimes often span over several jurisdictions. As such, there needs to be a common strategy between countries. It was suggested that there should be a 'common jurisdiction in cybercrime'. Practitioners would like the ability to have fluent, open conversations with other countries and a secure international sharing platform, where intelligence relating to transnational crimes could be shared between LEAs quickly would assist with this.



b) Collaboration:

A key issue faced by a number of LEAs is the reluctance of companies to report cyber-attacks. It is thought that many companies are unwilling to do because:

- afraid to damage their reputation;
- concerns that customers could lose confidence in their ability to protect their information.

Whilst some countries have introduced legislation making it illegal not to report such an offence, other countries have not. Practitioners felt that consideration needed to be given as to how to encourage companies to engage with LEAs when they are a victim of an attack or a large number of cyber-attacks would continue to go unreported. Key to this it was agreed was giving companies the confidence that LEAs would work with them to protect their reputation.

SCENARIOS & MINDMAPPING

Majority of the challenges identified by security practitioners during PG workshop are equal in importance and brings a huge impact on police performance investigating CaaS crimes. Mind mapping session facilitated analysis and selection of the most promising technology areas that are targeted for innovations.


As a result of CaaS (Crime as a Service) mind-mapping session 3 priorities for technology areas were identified:

1. Encryption/ Decryption: encrypted devices are more frequently used by criminal, tools on site to improve the capabilities to decrypt communications, even the ability to decrypt in real time in the operations.
2. A single tool to carry out all functions, multifunctional tool. A unique tool to be used since the beginning of any investigation with full capabilities to carry out the whole investigations in a unique multifunctional platform.
3. Secure sharing platform for experts, to centralize information. To allow cross-border operations. Info exchanging in real time and also instant messaging between users.



RESEARCH RESULTS

Research solution according to the **first priority** - Encryption/ Decryption: encrypted devices are more frequently used by criminal, tools on site to improve the capabilities to decrypt communications, even the ability to decrypt in real time in the operations:

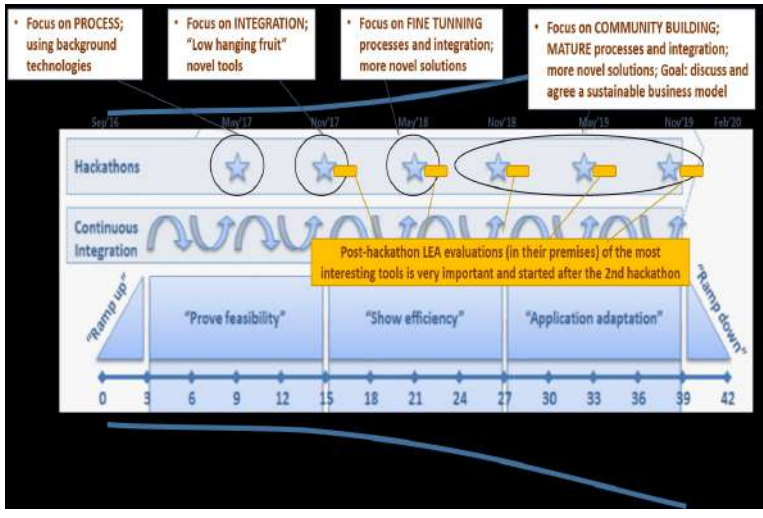
1	TITLE OF SOLUTION	
	CERBERUS	
DESCRIPTION & USE OF THE SOLUTION		
<p>The aim of the CERBERUS (Child Exploitation Response by Beating Encryption and Research to Unprotect Systems) project is to take control of the entire security chain through the development and implementation of a European decryption platform to block criminal groups including terrorists, political extremists, drug traffickers and perpetrators of sexual exploitation. New software and hardware to decrypt criminal information, that can be applied to any case. Hardware and software solutions can be used by any LEA for any case.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
<p>Constantly evolving, due to fast evolution of the encryption and decryption technologies.</p>		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	<p>CERBERUS is funded by EU's Internal Security Fund under agreement No. 822015.</p> <p>The project coordinated by <u>Forensic Research Institute of the French Gendarmerie</u>.</p> <p>Project details: https://cdn2.nextinpact.com/medias/cerb erus.pdf</p>	
	TECHNOLOGY READINESS LEVEL (1-9)	
	Unknown	

RESEARCH RESULTS

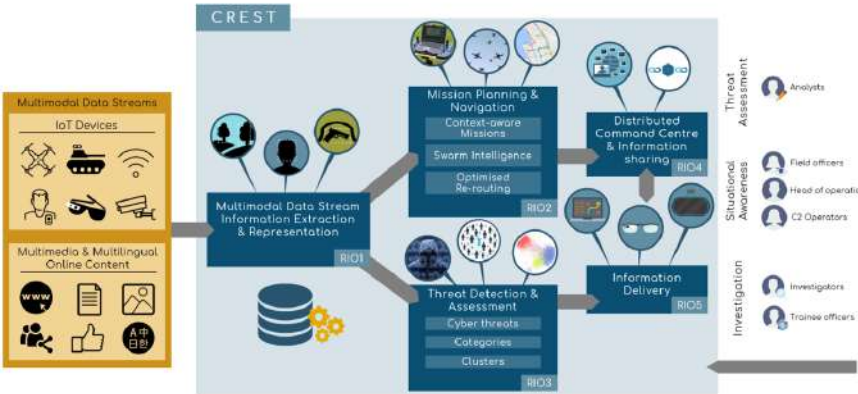
Research solutions according to the **second** priority - a single tool to carry out all functions, multifunctional tool. A unique tool to be used since the beginning of any investigation with full capabilities to carry out the whole investigations in a unique multifunctional platform:

TITLE OF SOLUTION	
2	RAMSES
	INTERNET FORENSIC PLATFORM FOR TRACKING THE MONEY FLOW OF FINANCIALLY-MOTIVATED MALWARE
DESCRIPTION & USE OF THE SOLUTION	
<p>The overall objective of RAMSES is to design and develop a holistic, intelligent, scalable and modular platform for Law Enforcement Agencies to facilitate digital Forensic Investigations. The system will extract, analyze, link and interpret information extracted from Internet related with financially-motivated malware. It focuses on 2 case studies: ransomware and banking.</p>	
TECHNOLOGICAL GAPS & CHALLENGES	
<p>Solution is applicable for RANSOMWARE AND BANKING TROJANS attacks.</p>	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
<p>The diagram is divided into three vertical sections representing different goals of the RAMSES project:</p> <ul style="list-style-type: none">GOAL 1: Methodology advancement<ul style="list-style-type: none">LEAs' proceduresEthical implicationsSocietal impactLegal complianceStakeholders engagementGuidelines & best practicesGOAL 2: RAMSES platform<ul style="list-style-type: none">Data privacy & securityAdvanced analyticsPredictive engineUser-oriented toolsInteroperabilityGOAL 3: Operational demonstration<ul style="list-style-type: none">Pilot projects (3 EU countries)Impact assessmentSocietal impact evaluationLEAs training <p>Below the text, there are three corresponding illustrations: a flowchart for Goal 1 involving stakeholders and LEAs, a screenshot of the RAMSES platform interface for Goal 2, and a map of Europe highlighting three pilot countries for Goal 3.</p>	<p>RAMSES project is funded from the EU H2020 Research and Innovation Programme under Grant Agreement No 700326. Consortium is led by <u>TREELOGIC</u>. https://ramses2020.eu/</p>
TECHNOLOGY READINESS LEVEL (1-9)	
7	


RESEARCH RESULTS

3	TITLE OF SOLUTION
	ASGARD - ANALYSIS SYSTEM FOR GATHERED RAW DATA
DESCRIPTION & USE OF THE SOLUTION	
<p>ASGARD aims to contribute to LEA Technological Autonomy, by building a sustainable, long-lasting community for law enforcement agencies (LEAs) and the R&D industry. This community will develop, maintain and evolve a best-of-class tool set for the extraction, fusion, exchange and analysis of Big Data, including cyber-offense data for forensic investigation.</p>	
TECHNOLOGICAL GAPS & CHALLENGES	
<p>Unclear how end-users can access the toolbox, what are certification options and how to join the user's community, no knowledge if it is still active and functioning.</p>	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
	<p>Asgard project has received funding from the EU H2020 Research and Innovation programme under Grant agreement No 700381. Consortium is led by <u>VICOMTECH</u>. https://asgard-project.eu/</p>
TECHNOLOGY READINESS LEVEL (1-9)	
5-6	

RESEARCH RESULTS

4	TITLE OF SOLUTION
	<p>CREST - FIGHTING CRIME AND TERRORISM WITH AN IOT-ENABLED AUTONOMOUS PLATFORM BASED ON AN ECOSYSTEM OF ADVANCED INTELLIGENCE, OPERATIONS, AND INVESTIGATION TECHNOLOGIES</p> <p>DESCRIPTION & USE OF THE SOLUTION</p> <p>CREST aims to equip LEAs with an advanced prediction, prevention, operation, and investigation platform by leveraging the IoT ecosystem, autonomous systems, and targeted technologies and building upon the concept of multidimensional integration and correlation of heterogeneous multimodal data streams (ranging from online content to IoT-enabled sensors) for:</p> <ul style="list-style-type: none"> • threat detection and assessment, • dynamic mission planning and adaptive navigation for improved surveillance based on autonomous systems, • distributed command and control of law enforcement missions, • sharing of information and exchange of digital evidence based on blockchain, and • delivery of pertinent information to different stakeholders in an interactive manner tailored to their needs. <p>CREST will also provide chain-of-custody, and path-to-court for digital evidence. Human factors and societal aspects will also be comprehensively addressed, while information packages for educating the wider public on identifying threats and protecting themselves will be prepared and distributed.</p> <p>TECHNOLOGICAL GAPS & CHALLENGES</p> <p>Ongoing project until 2023</p>
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
<p>Research and Innovation</p> 	<p>CREST project is funded by EU H2020 Research and Innovation programme under Grant agreement No 833464. Consortium is led by <u>SERVICIUL DE PROTECTIE SI PAZA</u>. https://project-crest.eu/</p> <p>TECHNOLOGY READINESS LEVEL (1-9)</p> <p>3-4</p>




RESEARCH RESULTS

TITLE OF SOLUTION	
5	TELLFINDER - A GLOBAL COUNTER-HUMAN TRAFFICKING PARTNER NETWORK, EMPOWERED BY DATA
DESCRIPTION & USE OF THE SOLUTION	
TellFinder technologies include a suite of tools for human trafficking investigators that uses emerging technologies to search deep-web content and discover hidden connections in data. TellFinder search engine is available to law enforcement for no cost	
TECHNOLOGICAL GAPS & CHALLENGES	
The Application is necessary to become a partner. TellFinder Tool for Counter Human Trafficking closes on December 10, 2021.	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
	TELLFINDER https://www.tellfinderalliance.com/
	TECHNOLOGY READINESS LEVEL (1-9)
	8

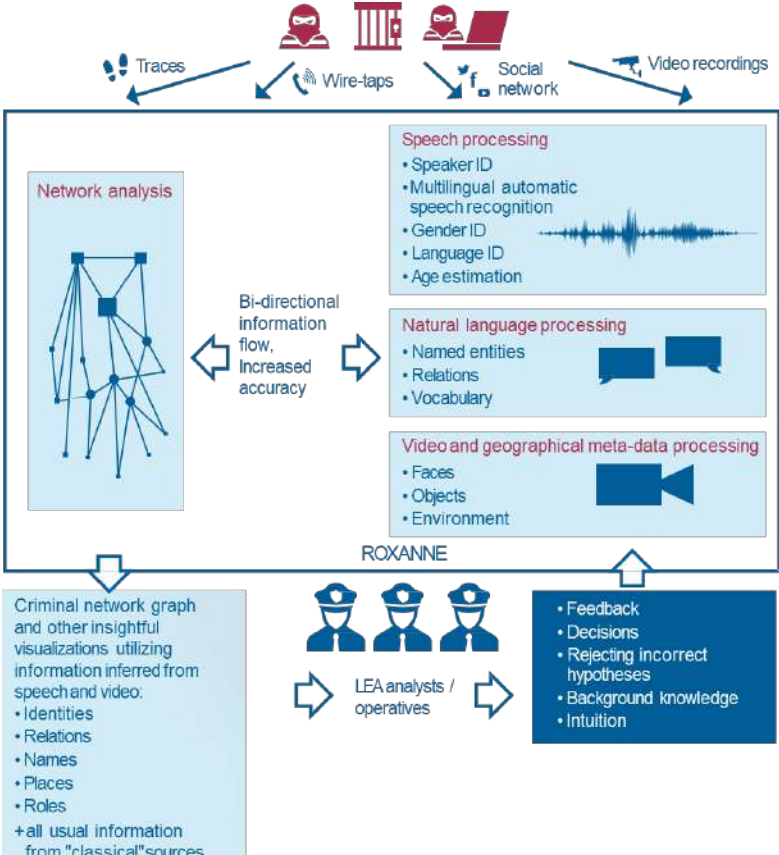
RESEARCH RESULTS

TITLE OF SOLUTION	
6	COPKIT
DESCRIPTION & USE OF THE SOLUTION	
The COPKIT project focuses on the problem of analysing, investigating, mitigating and preventing the use of new information and communication technologies by organised crime and terrorist groups. Develop a toolkit for knowledge production and exploitation in investigative and strategic analysis work to support the EW/EA paradigm	
TECHNOLOGICAL GAPS & CHALLENGES	
Solution is not yet available. Ongoing project until 2022	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
<div><p>Project concepts</p><p>Tool Categories</p></div>	<p>COPKIT project is funded by EU H2020 Research and Innovation programme under Grant agreement No 786687. COPKIT project consortium is coordinated by Isdefe. https://copkit.eu/</p>
TECHNOLOGY READINESS LEVEL (1-9)	
3	

RESEARCH RESULTS

TITLE OF SOLUTION	
7	TITANIUM - TOOLS FOR THE INVESTIGATION OF TRANSACTIONS IN UNDERGROUND MARKETS
DESCRIPTION & USE OF THE SOLUTION	
TITANIUM has researched, developed, and validated novel data-driven techniques and solutions designed to support Law Enforcement Agencies charged with investigating criminal or terrorist activities involving virtual currencies and/or underground markets in the darknet.	
TECHNOLOGICAL GAPS & CHALLENGES	
Not clear how LEA can benefit from the results of the project. Project sustainability plans are not well defined.	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
<div></div> <div>Monitoring trends in virtual currency and darknet market ecosystems</div>	Titanium project is funded by EU H2020 Research and Innovation programme under Grant agreement No 740558. Titanium consortium led by <u>Austrian Institute of Technology</u> . https://www.titanium-project.eu/
<div></div> <div>Analyzing transactions across different virtual currency ledgers</div>	
<div></div> <div>Generating court-proof evidence reports based on reproducible and legally compliant analytical procedures</div>	
TECHNOLOGY READINESS LEVEL (1-9)	
4	

RESEARCH RESULTS

8	TITLE OF SOLUTION
	ROXANNE - REAL TIME NETWORK, TEXT, AND SPEAKER ANALYTICS FOR COMBATING ORGANIZED CRIME
DESCRIPTION & USE OF THE SOLUTION	
<p>ROXANNE collaborates with Law Enforcement Agencies (LEAs), industry and researchers to develop new tools to speed up investigative processes and support LEA decision-making. The end-product will be an advanced technical platform which uses new tools to uncover and track organized criminal networks, underpinned by a strong legal framework.</p>	
TECHNOLOGICAL GAPS & CHALLENGES	
<p>Ongoing project until 2022 - no deliverables available as for Jan 2022.</p>	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
	<p>ROXANNE project is funded by EU H2020 Research and Innovation programme under Grant agreement No 833635.</p> <p>Project consortium led by <u>IDIAP</u>. https://roxanne-euproject.org/</p> <p>TECHNOLOGY READINESS LEVEL (1-9)</p> <p>3</p>




RESEARCH RESULTS

9	TITLE OF SOLUTION	
	CC-DRIVER	
DESCRIPTION & USE OF THE SOLUTION		
<p>The CC-DRIVER project seeks to understand the drivers of cybercriminality and researches methods to prevent, investigate and mitigate cybercriminal behaviour.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
<p>Ongoing project until 2022. Limited information available</p>		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
 <p>TOOLS FOR LAW ENFORCEMENT</p>  <p>POLICYMAKING TOOLKIT</p>  <p>VULNERABILITY ASSESSMENTS</p>	<p>CC-DRIVER project is funded by EU H2020 Research and Innovation programme under Grant agreement No 883543. The Project is Coordinated by <u>Trilateral Research</u>. https://www.ccdriver-h2020.com/</p>	
		TECHNOLOGY READINESS LEVEL (1-9)
		3


RESEARCH RESULTS

10	TITLE OF SOLUTION	
	NO MORE RANSOM	
DESCRIPTION & USE OF THE SOLUTION		
The “No More Ransom” website is an initiative by the National High-Tech Crime Unit of the Netherlands’ police, Europol’s European Cybercrime Centre, Kaspersky and McAfee with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.		
TECHNOLOGICAL GAPS & CHALLENGES		
At the moment, not every type of ransomware has a solution.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
N.A.	Dutch Police, http://www.nomoreransom.org/	
	TECHNOLOGY READINESS LEVEL (1-9)	
	8	

RESEARCH RESULTS

11	TITLE OF SOLUTION	
	FORMOBILE	
DESCRIPTION & USE OF THE SOLUTION		
<p>85% of the crime investigations include mobile data. Also 85% of all photos in Europe are taken with a smartphone. FORMOBILE is an H2020 project focused on creating a complete mobile forensic investigation chain as the standardized European method. FORMOBILE includes advanced tools and software for acquisition, recovery and analysis of the data, focused on criminals that use state of the art technology to evade detection.</p> <p>Methods are developed to cover forensic acquisition of data from mobile devices, plus the decoding and analysis of the data and the presentation of it.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
Focused on mobile devices.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
 <p>Rapid Retrieval of Digital Evidence</p> <p>Boosting first responders' abilities to trigger the investigation process</p>	<p>FORMOBILE project is funded by EU H2020 Research and Innovation programme under Grant agreement No 832800. The Project is Coordinated by <u>University of Mittweida</u>. https://formobile-project.eu/</p>	
 <p>Decoding Retrieved Data</p> <p>New techniques to access data, previously off-limits</p>		
 <p>Analysis & Validation</p> <p>Automatic & enriched data for more accurate and decisive evidence</p>	TECHNOLOGY READINESS LEVEL (1-9)	
3		

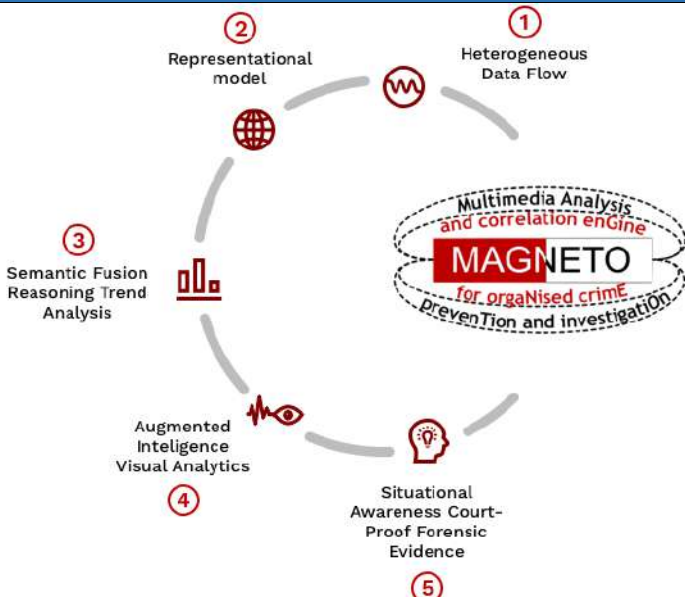
RESEARCH RESULTS

12	TITLE OF SOLUTION	
	WASTEFORCE	
DESCRIPTION & USE OF THE SOLUTION		
Within the Waste Force project a prototype of a forensic tool for data collection, retrieval and analysis is developed. This tool focuses on the use of data relevant within environmental crime and its connections to economic activities. This data can say something about the vulnerability of specific waste streams to criminal activities, the modus operandi and detection possibilities. The tool is focused on improving access to historic data that assist in casework and intelligence.		
TECHNOLOGICAL GAPS & CHALLENGES		
Environmental forensics is multidisciplinary and therefore tools vary per subject and region.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	The WasteForce project is funded by the EU's Internal Security Fund — Police (ISFP/2017/AG/ENV/821345). Consortium is led by IMPEL. https://www.wasteforceproject.eu/	
	TECHNOLOGY READINESS LEVEL (1-9)	
7		

RESEARCH RESULTS


13	TITLE OF SOLUTION	
	EXFILES	
DESCRIPTION & USE OF THE SOLUTION		
Within the “extract forensic information for LEAs from encrypted smartphones” (EXFILES) project new tools on data extraction on mobile devices are developed for LEA's. New tools are a combination of software, hardware and combined methods, including ethical and legal aspects. Improved holistic methods and techniques on forensic information extraction from modern encrypted smartphones used by criminals.		
TECHNOLOGICAL GAPS & CHALLENGES		
The project is still ongoing. The results (software toolbox for data extraction) can be tested only by the members of the project consortium . Knowledge distribution and tool deployment is planned on 2023.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
N.A.	The EXFILES project is funded from the EU H2020 research and innovation programme under grant agreement No. 883156. Consortium is led by <u>Technicon</u> . <u>https://exfiles.eu/</u>	
	TECHNOLOGY READINESS LEVEL (1-9)	
	4	

RESEARCH RESULTS

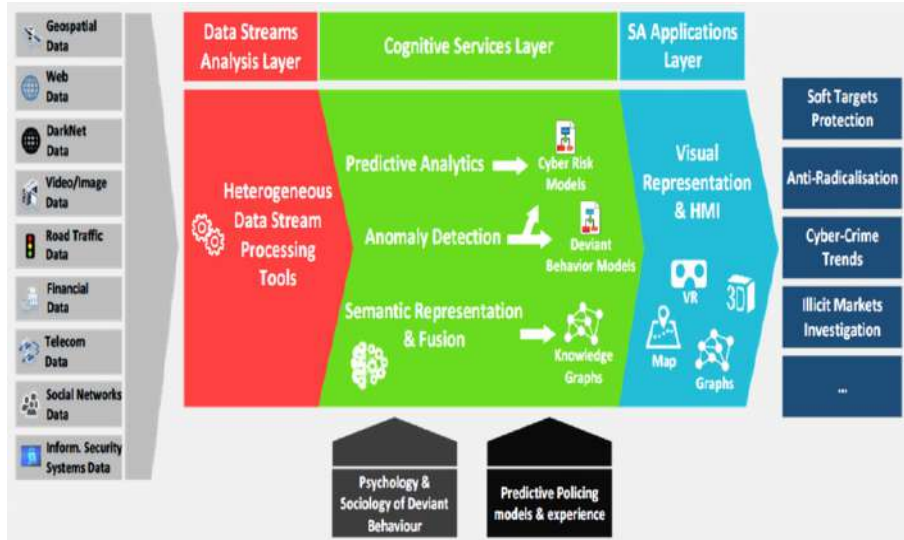
TITLE OF SOLUTION	
14	MAGNETO
DESCRIPTION & USE OF THE SOLUTION	
<p>MAGNETO innovates the both heterogeneous and big data capacity of LEAs for crime prevention and investigation. Magneto facilitates digital forensic investigations to collect information on the criminal case and suspects and provide evidence. Technologies solutions are focused on the more efficient processing of crime and terrorism data, that is useable as court-proof evidence. It includes an advanced correlation engine for automatic discovery of new relations within datasets, a representational model to represent knowledge in an open and standardized manner, an evidence collection platform to provide data mining, threat prediction, and augmented intelligence tools to increase SA. The results of the data processing are visually represented to represent accurate decision making, SA and evidence extraction that is court-proof.</p>	
TECHNOLOGICAL GAPS & CHALLENGES	
<p>The technology is not mature enough to be tested in operational environment</p>	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
	<p>MAGNETO project is funded from the EU's H2020 Research and Innovation Programme under Grant Agreement No. 786629. Consortium is led by ICCS. http://www.magneto-h2020.eu</p>
TECHNOLOGY READINESS LEVEL (1-9)	
4-5	

RESEARCH RESULTS

Research solutions according to the **third** priority - Secure sharing platform for experts, to centralize information. To allow cross-border operations. Info exchanging in real time and also instant messaging between users.

15	TITLE OF SOLUTION	
	INSPECTR - INTELLIGENCE NETWORK AND SECURE PLATFORM FOR EVIDENCE CORRELATION AND TRANSFER	
DESCRIPTION & USE OF THE SOLUTION		
<p>The principle objective of INSPECTr will be to develop a shared intelligent 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.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
<p>Ongoing project until 2022. Limited information available</p>		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	<p>INSPECTr project is funded by EU H2020 Research and Innovation programme under Grant agreement No 833276. The Project is Coordinated by University College Dublin, National University of Ireland. https://inspectr-project.eu/</p>	
	TECHNOLOGY READINESS LEVEL (1-9)	
	3	

RESEARCH RESULTS

16	TITLE OF SOLUTION	
PREVISION - PREDICTION AND VISUAL INTELLIGENCE FOR SECURITY INFORMATION		
DESCRIPTION & USE OF THE SOLUTION		
The overall strategy in the execution of the PREVISION project is based on an iterative development methodology, which involves frequent software releases being made available to the LEA and practitioners end-users for testing and evaluation, resulting in keeping them continuously in the production loop. The PREVISION Platform will be deployed in 10 different demonstrations, managed by the different LEAs and practitioners of the consortium.		
TECHNOLOGICAL GAPS & CHALLENGES		
Limited information available		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	PREVISION project is funded by EU H2020 Research and Innovation programme under Grant agreement No 833115. The Project is Coordinated by ICCS. http://www.prevision-h2020.eu/	
TECHNOLOGY READINESS LEVEL (1-9)		
	3	

RESEARCH RESULTS

Research solutions that could be assigned to the **second or third** priority:

TITLE OF SOLUTION	
17	ANITA - ADVANCED TOOLS FOR FIGHTING ONLINE ILLEGAL TRAFFICKING
DESCRIPTION & USE OF THE SOLUTION	
Investigation system for analysing heterogeneous (text, audio, video, image) online (Surface Web, Deep Web, DarkNet) and offline content for fighting illegal trafficking of drugs, counterfeit medicines, NPS and weapons and terrorism funding.	
TECHNOLOGICAL GAPS & CHALLENGES	
Model needs to be adapted to a particular use case	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
	ANITA is a project funded by the EC under the H2020 Research and Innovation program, Grant Agreement No 787061. Project Consortium is led by <u>ENGINEERING</u> Ingegneria Informatica S.p.A. www.anita-project.eu
	TECHNOLOGY READINESS LEVEL (1-9)
6	

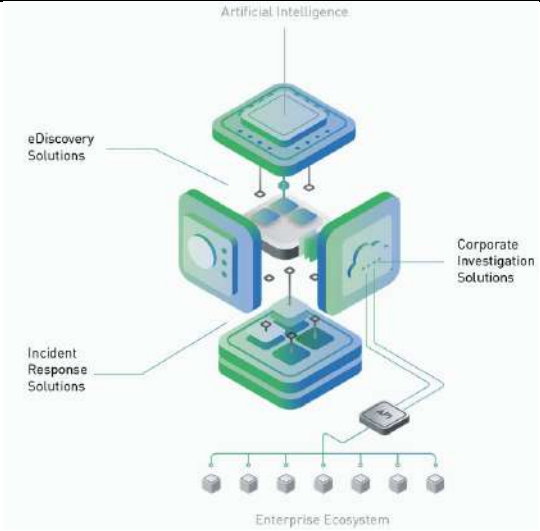
RESEARCH RESULTS

18	TITLE OF SOLUTION	
	CASE	
DESCRIPTION & USE OF THE SOLUTION		
<p>CASE stands for Cyber-investigation Analysis Standard Expression. The technology supports every context cyber-investigations. It is designed to support linked data and intelligent analysis. The representation is standard for chain of custody and chain of evidence.</p> <p>Cyber-investigation can be exchanged in a standardized form. It provides structure for intelligent analysis, system and tools are interoperable. Unsupported data structures can be imported using CASE and further process the data. Systems and tools are interoperable. Information can be transferred in CASE format between European countries and between government organizations in joint investigations.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
No gaps identified		
ILLUSTRATION		NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
<div><p>Cyber-Investigation Analysis Standard Expression</p><p>CASE roadmap to version 1.0 (Minimal Viable Product)</p><div><div>Community</div><div><div>organization</div><div>governance established ✓ bylaws established ✓ code of conduct established ✓ ontology committee established ✓ adoption committee established ✓ membership application process ✓</div><div>administration</div><div>Atlassian infrastructure setup ✓ Github repository organized ✓ code release process prepared ✓ CASE licensed under Apache 2.0 ✓</div><div>communication</div><div>caseontology.org website ✓ mailing lists setup ✓ workshops organized ✓</div><div>development practices</div><div>development and release procedures ✓ documentation style guides ✓ change request forms ✓</div></div><div><div>Ontology</div><div><div>clean up CASE ontology</div><div>CASE ontology normalized ✓ delineations between CASE and UCO established ✓ release CASE 0.2.0</div><div>identify MVP</div><div>identified MVP topics ✓ developed narratives for topics ✓ developed website gallery for narratives ✓</div><div>prepare MVP</div><div>CASE namespace defined ✓ demonstrate MVP narrative workflow identify MVP objects and properties define versioning scheme</div><div>develop MVP</div><div>map concepts to UCO constructs define MVP objects and properties release CASE version 1.0</div></div><div><div>Adoption & Documentation</div><div><div>document context</div><div>CASE & UCO domain descriptions ✓ CASE one-pager ✓ Adoption guide (draft) ✓ Mapping guide (draft) ✓</div><div>document MVP</div><div>documentation automatically generated ✓ document MVP object and property definitions JSON-LD examples / best practices F.A.Q. addressing CASE design fundamentals</div><div>support adoption</div><div>mapping examples ✓ reference implementations (beta) ✓ update Python verifier provide implementation examples transformation templating (e.g., Jinja) provide APIs</div></div></div><div></div><p>version 0.2 - July 2020</p></div></div></div>		<p>CASE Community https://caseontology.org/</p> <p>TECHNOLOGY READINESS LEVEL (1-9)</p> <p>7</p>


Three priorities:

1. Encryption/ Decryption: encrypted devices are more frequently used by criminal, tools on site to improve the capabilities to decrypt communications, even the ability to decrypt in real time in the operations
2. A single tool to carry out all functions, multifunctional tool. A unique tool to be used since the beginning of any investigation with full capabilities to carry out the whole investigations in a unique multifunctional platform.
3. Secure sharing platform for experts, to centralize information. To allow crossborder operations. Info exchanging in real time and also instant messaging between users.

Market solutions according to the **first** priority - Encryption/ Decryption: encrypted devices are more frequently used by criminal, tools on site to improve the capabilities to decrypt communications, even the ability to decrypt in real time in the operations:

1	TITLE OF SOLUTION CELEBRITE LAB SOLUTIONS
DESCRIPTION & USE OF THE SOLUTION	
<p>CELEBRITE offers several currently existing products on digital intelligence for law enforcement. To access (locked) devices, recover and extract data, obtain forensically-sound evidence from many sources and analyse several products are developed: A.o. the Cellebrite UFED (cloud) for accessing mobile and cloud-based data, Cellebrite Premium to access all iOS and high-end Android devices, and Macquisition for triage, data acquisition, collection and forensic imaging. Cellebrite offers advanced services and digital intelligence experts can also support gaining access to sensitive mobile evidence from several locked, encrypted or damaged devices. Also, training is available.</p>	
TECHNOLOGICAL GAPS & CHALLENGES	
<p>Not all device extraction is supported. Note: The Cellebrite Macquisition becomes the Cellebrite digital collector to support both Apple and Windows from Q1 2021.</p>	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
	<p>Cellebrite https://www.cellebrite.com/en/home/</p>
	TECHNOLOGY READINESS LEVEL (1-9)
 <p>The diagram illustrates the Enterprise Ecosystem. At the top is 'Artificial Intelligence'. Below it are three main components: 'eDiscovery Solutions', 'Incident Response Solutions', and 'Corporate Investigation Solutions'. These are connected to a central 'Enterprise Ecosystem' block at the bottom, which is further connected to a row of server icons representing the underlying infrastructure.</p>	<p>9</p>

MARKET SOLUTIONS

2	TITLE OF SOLUTION	
	SHODAN	
DESCRIPTION & USE OF THE SOLUTION		
<p>Shodan is a search engine for Internet-connected devices. For example, you can search Shodan for onions either by doing an SSL certificate search or search the full address of hidden service. Shodan can search the internet and specific domains for vulnerable devices. Used by hackers and professionals alike. Basic functionality is free. It can be used in a wide variety of use cases</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
<p>There is no available evidence that technology is secure enough to be used for LEA investigations.</p>		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	Shodan https://www.shodan.io/	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	


3	TITLE OF SOLUTION	
	HASHCAT	
DESCRIPTION & USE OF THE SOLUTION		
Hashcat is password recovery tool. It can be used to decrypt encrypted files. Free & open source. Very versatile tool (multi-os, multi-hash, multi-platform).		
TECHNOLOGICAL GAPS & CHALLENGES		
Not supported by a supplier - open source.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	Open source https://hashcat.net/hashcat/	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	

MARKET SOLUTIONS

4	TITLE OF SOLUTION	
	BRUTUS	
DESCRIPTION & USE OF THE SOLUTION		
<p>Brutus Password Cracker is a famous internet password cracking tool that may be used remotely. It claims to be the quickest and most versatile password cracking tool on the market. This programme is free and only works on Windows computers. It was first released in October of 2000.</p> <p>All in all, Brutus Password is a well-known Windows 10/8/7 password breaker. It is one of the most powerful and adaptable remote password crackers available. The nicest part of downloading Brutus password breaker is that it allows you to crack password hashes faster and more precisely.</p> <ul style="list-style-type: none">○ Windows 9x○ Windows NT○ All in all, Windows 2000○ Windows 7○ Windows 8○ More, Windows 10		
TECHNOLOGICAL GAPS & CHALLENGES		
Not supported by a supplier - open source.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	Open source https://github.com/LittleBigHack/Brutus-Password-Cracker	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	

MARKET SOLUTIONS

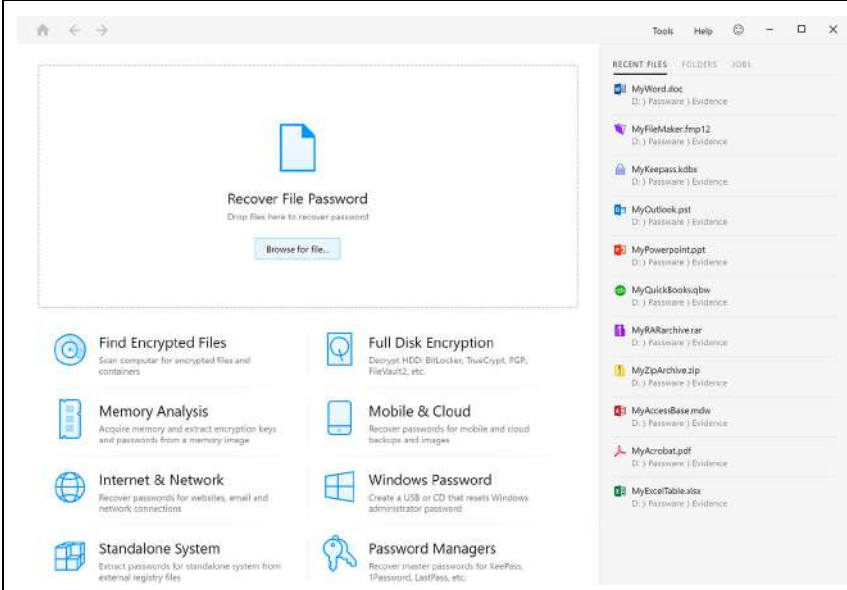
5	TITLE OF SOLUTION
	JOHN THE RIPPER
DESCRIPTION & USE OF THE SOLUTION	
Versatile password cracker. Its primary purpose is to detect weak Unix passwords. Besides several crypt (3) password hash types most commonly found on various Unix systems, supported out of the box are Windows LM hashes, plus lots of other hashes and ciphers in the community-enhanced version. John the Ripper is free and Open Source software, distributed primarily in source code form.	
TECHNOLOGICAL GAPS & CHALLENGES	
Not supported by a supplier - open source.	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
	Open source https://www.openwall.com/john/
	TECHNOLOGY READINESS LEVEL (1-9)
	9

6	TITLE OF SOLUTION	
	CRACKSTATION	
DESCRIPTION & USE OF THE SOLUTION		
<p>CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. Free & open source online tool to decrypt password hashes. Uses a huge library to apply a more intelligent brute force attack.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
<p>Can only be used for unsalted hashes.</p>		
ILLUSTRATION		NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
<div><div>Free Password Hash Cracker</div><div><div>Enter up to 20 non-salted hashes, one per line:</div><div><div></div><div><div><div>I'm not a robot</div><div></div></div><div>Crack Hashes</div></div></div></div><div><div>Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults</div><div>Download CrackStation's Wordlist</div></div></div>		<div><div>Open source</div><div>https://crackstation.net/</div></div>
		TECHNOLOGY READINESS LEVEL (1-9)
		9

7	TITLE OF SOLUTION	
	DIGITAL PASSWORD BOOK	
DESCRIPTION & USE OF THE SOLUTION		
<p>The digital password book of the NFI is used to decrypt information protected by a password. There are standard password books, based on what a password creation system enforces and applicable for different languages. When hard drives are present, these can contain relevant password information as well. The combination of this information and brute force may result in the algorithms finding the password. Access to data that can possible be used for evidence. Decryption can be done by the police, or in more complex cases by forensic experts from the NFI.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
<p>Digital protection methods are developed continuously, so the methods need to change too.</p>		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
N.A.	Netherlands Forensics Institute (NFI) https://www.forensischinstituut.nl/	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	

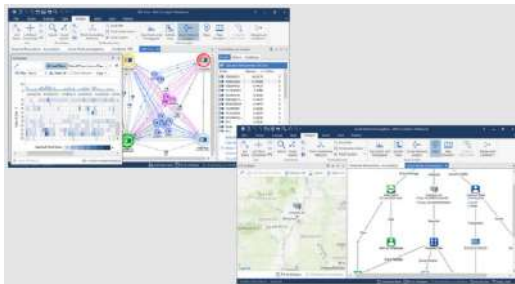
8	TITLE OF SOLUTION	
	PASSWARE KIT FORENSIC	
DESCRIPTION & USE OF THE SOLUTION		
<p>Passware Kit Forensic 2022 v1 discovers all password-protected items on a computer and decrypts them. The software recognizes 300+ file types and works in batch mode to recover their passwords. Many types of files are decrypted instantly, while other passwords are recovered through Dictionary and Brute-force methods using GPU acceleration and distributed computing (for Windows, Linux, and Amazon EC2). Available for Windows & Mac.</p> <ul style="list-style-type: none">• Support for Windows 11• Support for macOS Monterey• Password recovery for Acronis backups• List of passwords supported by the Known Passwords attack• LUKS2 decryption via memory analysis• Batch mode improvements• Passware dictionaries <p>Finding and recovering and decrypting of decrypted items on a variety of systems and cloud data. The passware forensic kit contains a starter guide, training, best practises and sample files to get started.</p> <p><u>Key Product Features:</u></p> <ul style="list-style-type: none">• Live memory analysis• Email notifications• Cross-platform Passware Kit Agents• Passware Bootable Memory Imager• Automatic updates• Hardware acceleration• Mobile forensics• Password recovery for 300+ file types• Encryption detection and analysis• Batch processing• Decryption of FDE• Password Exchange		
TECHNOLOGICAL GAPS & CHALLENGES		
No information available that technology is certified for LEA digital forensic investigations.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	

MARKET SOLUTIONS

	<p>Passware https://www.passware.com/</p>
	<p>TECHNOLOGY READINESS LEVEL (1-9)</p>
	<p>9</p>

MARKET SOLUTIONS

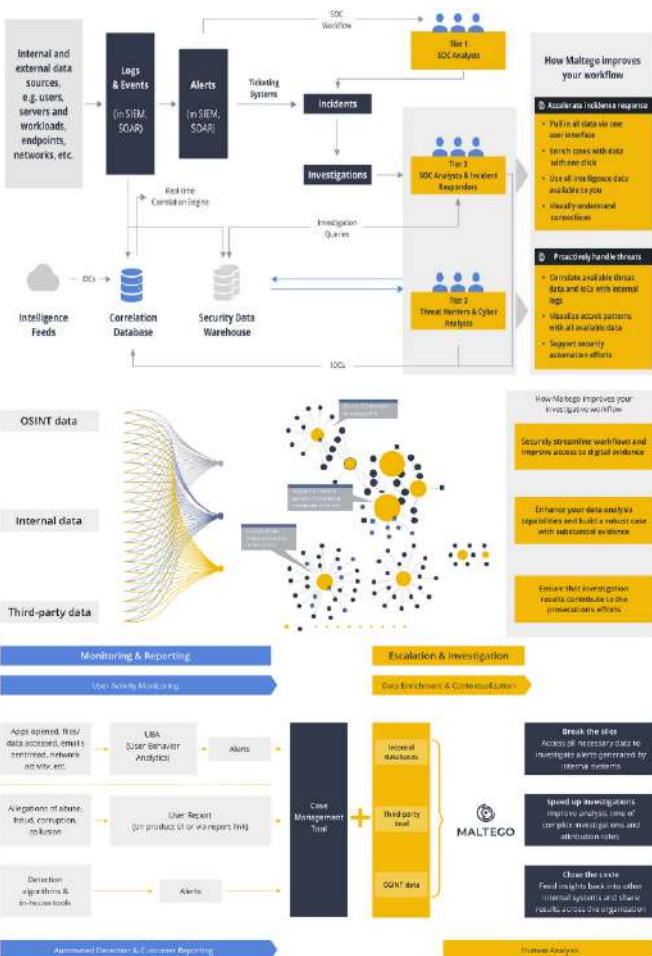
Market solutions according to the **second** priority - a single tool to carry out all functions, multifunctional tool. A unique tool to be used since the beginning of any investigation with full capabilities to carry out the whole investigations in a unique multifunctional platform:

9	TITLE OF SOLUTION	
	ANALYST NOTEBOOK	
DESCRIPTION & USE OF THE SOLUTION		
i2 Analyst's Notebook arms analysts with multidimensional visual analysis capabilities so they can quickly uncover hidden connections and patterns in data. Widely used by detective teams to analyse relationships within criminal cooperations. Can be connected to the digital domain as well.		
TECHNOLOGICAL GAPS & CHALLENGES		
More focused on the physical domain in relation to the digital domain.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	IBM https://www.ibm.com/products/i2-analysts-notebook	
	TECHNOLOGY READINESS LEVEL (1-9)	
		9

MARKET SOLUTIONS

10	TITLE OF SOLUTION	
	PALANTIR	
DESCRIPTION & USE OF THE SOLUTION		
Palantir's data management solution enables a common operating and intelligence picture in a live and collaborative platform, enabling defence intelligence teams to visualise and analyse geospatial data and plan missions in real time. A mobile application provides smartphone access to extend the platform's core capabilities into the field.		
TECHNOLOGICAL GAPS & CHALLENGES		
The Palantir platform requires regular updates, which typically occur every month. If the platform is blocked from being updated, it will be considered an 'unsupported' version, which Palantir will be unable to support. If a problem (i.e. security or bug issue) is discovered on an 'unsupported' version of the platform, the only course of action will be to upgrade the platform to the latest version.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
N.A.	Palantir https://www.palantir.com/solutions/law-enforcement/	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	

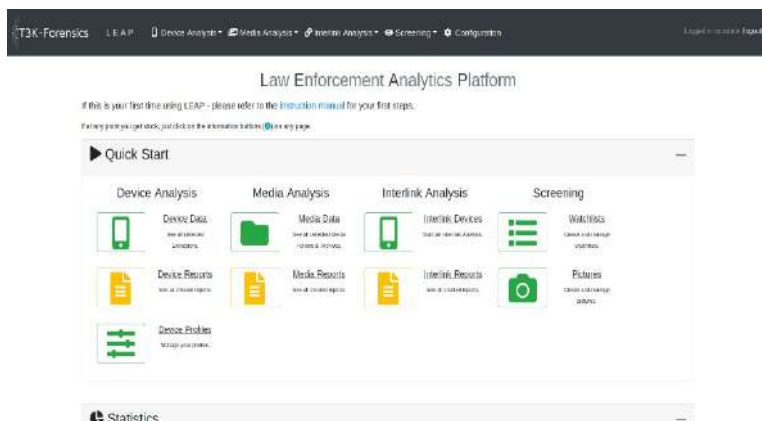
MARKET SOLUTIONS

11	TITLE OF SOLUTION MALTEGO
DESCRIPTION & USE OF THE SOLUTION	
<p>Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet.</p> <p>Promising open source intelligence (OSINT) and graphical link analysis tool for gathering and connecting information for investigative tasks. Integrate data from public sources (OSINT), commercial vendors, and internal sources via the Maltego Transform Hub. All data comes pre-packaged as Transforms ready to be used in investigations.</p>	
TECHNOLOGICAL GAPS & CHALLENGES	
Not clear how technology is accurate addressing niche languages.	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
 <p>The diagram illustrates the Maltego workflow, showing how data from various sources (Internal/external, OSINT, third-party) is processed through a Correlation Database and Security Data Warehouse to generate Alerts, Incidents, and Investigations. It also highlights how Maltego improves workflow by providing accurate evidence response and proactive threat hunting capabilities.</p>	<p>Maltego https://www.maltego.com/index.html</p>
	<p>TECHNOLOGY READINESS LEVEL (1-9)</p> <p>9</p>

TITLE OF SOLUTION	
12	CIPHERTRACE
DESCRIPTION & USE OF THE SOLUTION	
<p>CipherTrace is a provider of cryptocurrency anti-money laundering, blockchain forensics and threat intelligence solutions to businesses. CipherTrace uses pattern recognition, interactive visualization, a graph database, an advanced API and other technologies to de-anonymize cryptocurrency transactions.</p> <p>CipherTrace delivers comprehensive cryptocurrency intelligence. It includes the capability to trace more than 800 virtual assets, including BTC, BCH, ETH, ERC-20, Tether, and LTC tokens. Contains Automated Transaction Risk Scoring</p>	
TECHNOLOGICAL GAPS & CHALLENGES	
Technology is focused on business organizations	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
	<p>CipherTrace https://ciphertrace.com/</p>
	<p>TECHNOLOGY READINESS LEVEL (1-9)</p> <p>9</p>


13	TITLE OF SOLUTION	
	FORCLU (FORENSIC CLUSTERING)	
DESCRIPTION & USE OF THE SOLUTION		
<p>ForClu (forensic clustering) automatically arranges contents up to over 100.000 files into clusters. The applicable data is analysed with an artificial neural network, which are then divided into clusters (vehicles, vehicle type, etc.). With ForClu it is possible to generate specific filters that enhance search options. ForClu is a standalone toolkit. LEAP's workflow integration is planned, integration into currently existing forensic toolkits is being evaluated.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
<p>Tool is developed as a standalone, integration costs must be estimated.</p>		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	<p>T3K https://www.t3k.ai/en/ https://www.t3k.ai/forclu-en/</p>	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	

MARKET SOLUTIONS

14	TITLE OF SOLUTION	
	LEAP (LAW ENFORCEMENT ANALYTICS PLATFORM)	
DESCRIPTION & USE OF THE SOLUTION		
<p>The Law Enforcement Analytics Platform (LEAP) enables a quick analysis of data from smartphones and other sources. It provides insight and oversight in relevant data and risks that provides focus to the investigation. Identification of persons and incriminating material, including image, communication and interlink analysis, security watchlists and identity and location data. LEAP supports all major mobile forensic toolkits. It has an easy to use and fast analysis and contains an automated report function.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
<p>T3K-Forensics specializes in the extraction and in-depth analysis of Android and Apple devices</p>		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	<p>T3K https://www.t3k.ai/en/ https://www.t3k.ai/leap-en/</p>	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	

15	TITLE OF SOLUTION	
	MOBILE FORENSICS ECOSYSTEM	
DESCRIPTION & USE OF THE SOLUTION		
MSAB created the ecosystem of mobile forensics, in which there are three phases: extract, analyse and manage. This is a combination of all their separate products, platforms and services. Due to the range of their products, there is a tool available for the practitioner and situation; from operation onward. The most important sources of mobile data are supported: mobile devices, vehicles, cloud and IoT. And the chain of custody is ensured. Can be defined to the practitioners need in the particular situation. Also, training is available.		
TECHNOLOGICAL GAPS & CHALLENGES		
It takes knowledge on creating fitting solutions by matching the right MSAB technology.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
N/A	MSAB, https://www.msab.com/	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	

MARKET SOLUTIONS

16	TITLE OF SOLUTION	
	AXIOM	
DESCRIPTION & USE OF THE SOLUTION		
<p>With AXIOM digital evidence can be recovered from most sources (smartphones, clouds, IoT, images, etc.). All data can be analyzed in one case file. The latest version of Magnet AXIOM has GrayKey integration and further cloud and Mac support. The Magnet.AI module applies machine learning to search text-based and media content to identify crime related features. AXIOM's technologies can retrieve data from many sources, including Mac support. Data can be combined, analyzed with new features (e.g. Connections, Timeline), presented and easily reported. AXIOM provides training on the different aspects of the product.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
<p>Training to learn the full potential of the tool can be time consuming.</p>		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
<p>AXIOM Cyber Product Features</p> 	<p>Magnet Forensics https://www.magnetforensics.com/</p>	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	


MARKET SOLUTIONS

Market solutions according to the **third** priority - Secure sharing platform for experts, to centralize information. To allow cross-border operations. Info exchanging in real time and also instant messaging between users:

17	TITLE OF SOLUTION EUROPOL DECRYPTION PLATFORM
DESCRIPTION & USE OF THE SOLUTION <p>Europol and the European Commission's Joint Research Centre launched decryption platform. It will significantly increase Europol's capability to decrypt information lawfully obtained in criminal investigations.</p> <p>The platform is aimed at fighting organised crime and terrorism. The platform helps the police to investigate organised crime, terrorism, online child exploitation material and other serious crime. The European Cybercrime Centre within Europol operates the platform and supports the Member State investigations.</p>	
TECHNOLOGICAL GAPS & CHALLENGES <p>No gaps identified</p>	
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)
	<p>Europol & European Commission's Joint Research Centre https://www.europol.europa.eu</p>
	TECHNOLOGY READINESS LEVEL (1-9) <p>9</p>

18	TITLE OF SOLUTION	
	VISALLO	
DESCRIPTION & USE OF THE SOLUTION		
<p>Visallo helps intelligence analysts, law enforcement detectives, and fraud investigators produce more rigorous and defensible conclusions by helping them discover, visualize, and understand complex relationships hidden in massive amounts of data. It's an all-in-one suite of easy-to-use, web-based, visualization tools and machine learning data analysis algorithms.</p> <p>Helps Understand Complex Relationships Hidden in Data. Can be used with a multitude of file types. Access is secure and can be shared with other users.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
Technology more oriented for business organizations.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	Visallo https://www.visallo.com/	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	

MARKET SOLUTIONS

19	TITLE OF SOLUTION	
	IRIS	
DESCRIPTION & USE OF THE SOLUTION		
<p>IRIS is a scalable platform for automating online investigations. It contains a forensic investigation engine to combine data from open internet, social media, and the darknet.</p> <p>IRIS supports finding contact information of relevant persons or organisations, finding connections, but also in blacklist checks, risk analysis and darknet footprints. IRIS is designed according to data minimisation and contains no black box.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
Open source investigations.		
	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
	<p>WEB-IQ https://www.webiq.nl/</p>	
	TECHNOLOGY READINESS LEVEL (1-9)	
9		

20	TITLE OF SOLUTION	
	HANSKEN	
DESCRIPTION & USE OF THE SOLUTION		
<p>Hansken is a forensic search machine and data platform with software that can search efficiently through large quantities of data on different types of data carriers. The system processes a forensic copy so that it can be searched. There is the possibility to search on anything relevant, like words, characteristics, certain messages or photos from the same source. Researches can filter the tracks to a selection they want to manually look into.</p> <p>Improved investigative capacity and speed, improved investigative results on large quantities of data, increased innovation by (inter)national tool connection and extension, high quality and transparent reporting (including chains of evidence) and optimised organisational integration for easy cooperation. Case detectives can independently investigate digital data, which enables investigation speed. Forensic experts can focus on the deepening of traces.</p>		
TECHNOLOGICAL GAPS & CHALLENGES		
Continuously developing to adjust to new search needs.		
ILLUSTRATION	NAME OF ORGANISATION(S) OR PROJECT(S) OR DEVELOPER(S)	
N/A	Netherlands Forensics Institute (NFI) https://www.forensischinstituut.nl/	
	TECHNOLOGY READINESS LEVEL (1-9)	
	9	

ABOUT I-LEAD

i-LEAD's focus is on the incapability of groups of operational Law Enforcement Agencies (LEA) practitioners defining their needs for innovation. This will be done in a methodological way, also with the help of the research & industrial partners supplemented by a broad range of committed stakeholders. i-LEAD will build the capacity to monitor the security research and technology market in order to ensure a better matching and uptake of innovations by law enforcement agencies with the overarching aim to make it a sustainable Pan-European LEA network.

Earlier funded European research with a high technology readiness level as well as pipeline technologies will be closely monitored and assessed on its usefulness. Where possible, a strong dissemination towards the ENLETS and ENFSI members will take place to enable them to take up the actions from this research. i-LEAD will indicate priorities in five practitioner groups as well as aspects that needs (more) standardization and formulate recommendations how to incorporate these in procedures. As a final step, i-LEAD will make recommendations to LEA members on how to use Pre-Commercial Procurement (PCP) and Public Procurement of Innovation (PPI) instruments.



Authors:



Contributors:



This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SEC-2016-2017-1, under grant agreement no 740685.