The H2020 ANITA platform: generating knowledge about crime through user-centred innovative tools

[*]Full/Regular Research Paper for CSCI-ISCW

Valentina Mazzonello
Research and Innovation Division
Engineering Ingegneria Informatica S.p.A.
Palermo, Italy
valentina.mazzonello@eng.it

Ernesto La Mattina
Research and Innovation Division
Engineering Ingegneria Informatica S.p.A.
Palermo, Italy
ernesto.lamattina@eng.it

Roberto Acquaviva
Research and Innovation Division
Engineering Ingegneria Informatica S.p.A.
Palermo, Italy
roberto.acquaviva@eng.it

Gianluca Cinà
Research and Innovation Division
Engineering Ingegneria Informatica S.p.A.
Palermo, Italy
gianluca.cina@eng.it

Marialuna De Tommaso
Research and Innovation Division
Engineering Ingegneria Informatica S.p.A.
Napoli, Italy
marialuna.detommaso@eng.it

Youssef Bouali
Research and Innovation Division
Engineering Ingegneria Informatica S.p.A.
Lecce, Italy
youssef.bouali@eng.it

Barbara Pirillo
Research and Innovation Division
Engineering Ingegneria Informatica S.p.A.
Palermo, Italy
barbara.pirillo@eng.it

Simone Simoncini
Research and Innovation Division
Engineering Ingegneria Informatica S.p.A.
Palermo, Italy
simone.simoncini@eng.it

Abstract: This paper illustrates a novel user-centred and secure investigation platform to discover relevant data sources disseminated on the Web (including the Dark Web) and to analyse, enrich and correlate them to support knowledge-generation and investigations on illegal trafficking activities. The platform was designed and implemented in the context of the Horizon 2020 project ANITA (https://www.anita-project.eu/) to effectively support Law Enforcement Agencies in better understanding and investigating the online illegal trafficking framework and further improve their capacity to analyse complex criminal scenarios and big amount of relevant data. The paper illustrates the ANITA platform capabilities through some of the 'horizontal criminal scenarios' defined by the Project to explore connections between illegal trafficking activities concerning different goods. These 'scenarios' refer to cases of the same vendor distributing both firearms and synthetic drugs on the same or in different crypto markets, the same profiles found to be active on both some Dark Web crypto markets and Surface platforms or terrorist attacks performed with firearms bought on the Dark Web.

Keywords — Online illegal trafficking, Black markets on Dark Web, Big Data Analytics, Knowledge generation, User feedback

I. INTRODUCTION

Over the recent years, online illegal trafficking activities have hugely elaborated and expanded. The illegal trade of drugs and firearms represents a serious international threat that involves countless unscrupulous criminal networks. The production, trafficking and distribution of illegal drugs and firearms are even more interrelated and key enablers for other criminal activities and violent acts, including terrorist attacks [1].

Law Enforcement Agencies (LEAs) have been invested both on new technologies and in training activities to equip officers and practitioners with the necessary tools and professional skills for fighting the rapid increasing of the illegal trafficking phenomenon. To efficiently understand the organisational structure, the criminal behaviours and dynamics and their interconnections and interactions, it is of vital importance to collect and analyse all relevant online available clues in near real-time and to correlate them with closed-source information provided by the LEAs, in order to identify hidden relationships, recurrent strategies and emerging patterns in support of illegal activities. Among the most emblematic and widespread aspects of online illegal trafficking are the cases of counterfeit/falsified medicines, drugs, and Novel Psychoactive Substances (NPS), weapons and firearms, and terrorism funding.

Surface Web, Deep Web and Dark Nets can be regarded as key crime-facilitators in this context [2]. They offer new opportunities to the organised criminal groups, assisting them in: a) cooperating in a more effective, efficient, anonymous and secure way, although dislocated in diverse countries (e.g., through the usage of P2P or Tor networks); b) to manage criminal activities, with anonymous online payments, through crypto-currencies (e.g., Bitcoin); and c) to enlarge the crime-as-a-service activities and the related black markets (e.g., Tochka, Agartha market [3]) in the Dark Web.

Scope of this article is to present the H2020 ANITA Project's platform, which aims to provide LEAs with an integrated platform equipped with tools and services to detect, investigate and mitigate online illegal trafficking activities, especially in black markets, through the automated monitoring of Surface and Dark Web source, analysis and correlation of acquired information, and generation of new knowledge to propose to end users to support investigative activities, while maintaining the chain of custody on acquired contents throughout their journey in the platform, from their acquisition to their export.

Based on ontological inference and reasoning mechanisms, the process of knowledge generation and management starts from acquired information and is conducted through a continuous interaction with the user, which is the final recipient of such knowledge. Indeed, generated knowledge is proposed to the user under the form of "suggestions", which the user can validate or not. If the user validates the proposed suggestion, it becomes validated knowledge, that can be further reused by the platform to generate and propose new suggestions to the user.

For this reason, ANITA platform can be considered knowledge-centred and user-oriented and the quality level of the knowledge produced depends on the continuous interaction between the user's contribution and the platform capabilities.

The rest of the paper is organized as follow: Section II provides an overview of state-of-the-art frameworks and platforms currently used to support LEAs activities in combating online illegal activities. Then, the ANITA platform is illustrated in Section III. Operational scenarios in which ANITA has been tested to support LEAs are depicted in Section IV. Conclusions are reported in Section V.

II. State-of-art frameworks and tools against online illegal activities

Criminal networks apply constantly changing operational models related to online illicit trafficking to get in contact with victims, anonymise their identities, promote their products on online markets, share information both in clear (videos, handbooks, etc.) and encrypted (e.g., PGP-encrypted emails) way, and manage fake social profiles to get financing. These criminal phenomena increase the exigency of solutions that enable LEAs and security organisations to fight them in the most rapid and accurate way. Some research approaches are emerging for the identification of suspected web sites and markets in the Dark web [4][5], sometimes linked with Surface web sites to gain more visibility and attract more sellers [6]. However, the maturity level is usually low, most of them only proofs on concept, and need additional refinements to be used in operational environments.

More comprehensive platforms have been also built and are continuously updated and revised according to these needs. Such solutions usually comprehend one or more applications dedicated to information collection, curation and exploration.

Paterva Maltego [7] is a software for open-source intelligence and forensics, discovery of data from open sources, and visualisation of information in a graph format, suitable for link analysis and data mining. The focus of the application is analysing real-world relationships between people, groups, websites, domains, networks, internet infrastructure, and affiliations with online services exploiting open-source intelligence (OSINT) techniques (DNS records, whois records, search engines, social networks, various online APIs). Maltego does not provide integrated features for multimedia analysis, crawling on Deep web and Dark nets, visual analytics.

IBM i2 Intelligence Analysis Portfolio [8] consists in a suite of products for intelligence and investigative operations, like managing information on people, groups, companies, websites, vehicles, etc., and their relationships through graph visualization, generating alerts whenever an item changes, creating customised charts, and performing data mining. However, it does not support source crawling and monitoring, nor multimedia analysis and chain of custody.

Palantir Technologies [9] offers a general-purpose suite of software tools for integrating, visualising and analysing information; some applications in the law enforcement have been built by means of this suite. It does not offer integrated tools for online information acquisition, or video analysis.

SAS Intelligence and Investigation Management [10] provides data management, advanced analytics and operational solutions for gathering and managing intelligence, conducting complex investigations, and improving investigative processes and workflows. It does not include monitoring capabilities and multimedia analysis.

Additional software solutions, more or less similar to the previous ones, are also available in the market of investigation management. However, all these solutions, due to their commercial nature (and then born to be acquired by a broader set of customers), can address generic tasks related to intelligence and investigative activities, without providing relevant support in specific contexts, like for instance illicit trafficking domain. ANITA platform aims to be complementary, focusing on real-time analysis of OSINT as well as deep and dark web sources, providing an integrated platform to LEAs and potential stakeholders. Additionally, ANITA focuses specifically on monitoring, analysing, and detecting dangerous activity considering knowledge of the illegal trafficking domain with all its peculiarities, and therefore respond the requirements of LEAs in this field. Furthermore, its multimodal analysis capability that includes cryptocurrency transactions allows a complete and precise investigative reconstruction usable for prosecution purposes thanks to a lawful chain of custody.

III. ANITA platform

ANITA stands for Advanced tools for fighting oNline Illegal TrAfficking and aims to provide Law Enforcement Agencies with an integrated platform equipped with tools to boost investigative work to combat illicit trafficking activities. The project has received funding from the European Union's Horizon 2020 programme[1] and focuses on three main use cases related to drugs, weapons, and terrorism financing, and are used to validate the capabilities and potentialities of the platform.

ANITA provides officers with a set of interactive applications to support them in the discovery of illegal trafficking activities conducted online, specifically for searching and monitoring over time online sources of interest (both on Surface and Dark web), extracting information from multimedia (documents, videos, images and audio files) contents through advanced and context-oriented analysis tools, generating new knowledge under the form of *suggestions* to propose to users, based on previously collected information and fresh analysis results, visualizing and exploring analytics on current events and

[1] The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n° 787061 and topic SEC-12-FCT-2016-2017 (*Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism*).

trends. It assumes the continuous interaction with users, that is responsible for seeing and validating the proposed suggestions. Once validated, the suggestions become available knowledge to be reused to generate further suggestions (Fig. 1).

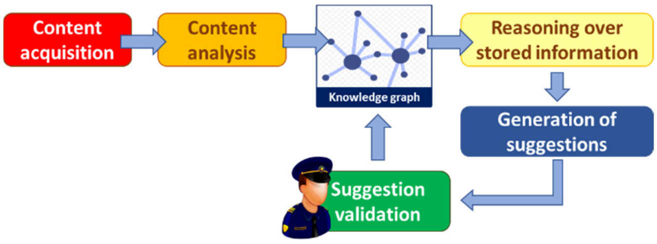


Fig. 1: Knowledge validation process

The platform is case-oriented: users can operate inside dedicated workspaces, which can be assigned with specific permissions. Access to the acquired information is provided in a user-friendly and meaningful way through graph-oriented visualization and exploration patterns (Fig. 2). Finally, users can share and use information externally to the platform by exporting collected data and the related chain of custody, under the form of documental report (for prosecution purposes) or machine-readable package (to be read by external software systems or other ANITA installations).

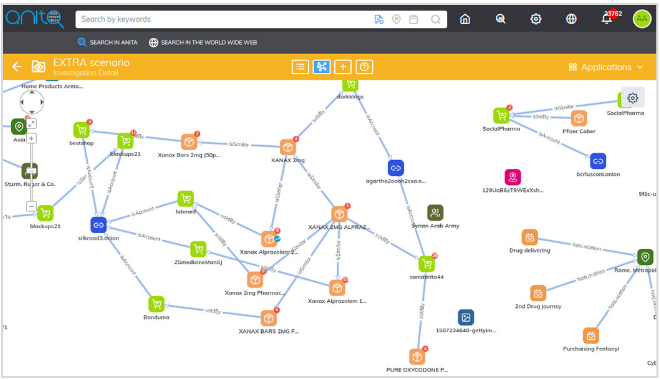


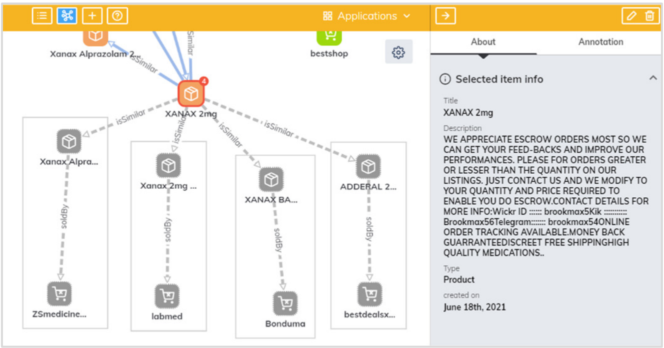
Fig. 2: ANITA platform overview

Multiple tasks running in background can be started to monitor online sources. These monitoring processes leverage on embedded crawlers able to download and reconstruct the navigability of crawled sites, enabling users to browse offline those sites. Contents can also be searched online as well as uploaded by users inside the platform.

Data acquisition is performed by SONAR (Source iNtegration And monitoring fRamework), which is a framework designed and developed by Engineering Ingegneria Informatica SpA that consists in several crawlers/scrapers integrated as third-party services and managed by a single node (the *SONAR core*) in order to separate the crawlers' layer. This way, each crawler can have its specific custom crawling process for a specific source, and it can even be developed and coded with different languages. The advantage of this layer separation is the possibility to add or remove crawlers on the fly, creating, in fact, a plug-n-play framework. Moreover, a strong benefit of the framework is the implementation of unified data models for requests and data collected, making it a middleware between the ANITA platform and the internet. Whenever a user performs a search or a source monitoring request in ANITA, the platform contacts the SONAR core with the same request data model, then the core routes the request to crawlers that can fulfil it. Data collected by crawlers are very heterogeneous since they come from different internet sources (e.g., forums, social media, blogs, Dark web pages), and they can be retrieved in different ways (e.g., traditional scraping, API, third party services), so each crawler performs an homogeneity process, mapping the collected data in a single and unified data model as general as possible to describe data coming from most of the internet sources. Search and monitoring are the two possible requests allowed: the former is a simple "one-shot" search task, while the latter represents a search over time, very useful when users want to track a specific source and all its changes by collecting different versions of the monitored source. Moreover, SONAR has a granular management of tasks with the opportunity to edit, delete, suspend, resume, and check running tasks.

Once acquired, contents are automatically analysed by integrated tools able to extract information on vendors, products, locations, organizations, and other items of interest (like phone numbers, crypto addresses, email addresses, pills, medicines, rifles, guns, laboratories, 3D printers, but also stylometric writeprints over anonymous texts).

Extracted information is then correlated to that already stored inside the platform: result of these correlations consists in a *knowledge graph*, which supports users in connecting-the-dots about a case. The process of knowledge enrichment, useful to reconstruct criminal activities, consists in the exploitation of reasoning mechanisms applied to the information stored in the knowledge graph for the generation of *suggestions* that are proposed to the user and that can open new avenues for the resolution of the case. A *suggestion* is a "virtual" sub-graph that connects entities already present in the knowledge graph (Fig. 3).



Selected item info

Title
XANAX 2mg

Description
WE APPRECIATE ESCROW ORDERS MOST SO WE CAN GET YOUR FEED-BACKS AND IMPROVE OUR PERFORMANCES. PLEASE FOR ORDERS GREATER OR LESSER THAN THE QUANTITY ON OUR LISTINGS. JUST CONTACT US AND WE MODIFY TO YOUR QUANTITY AND PRICE REQUIRED TO ENABLE YOU DO ESCROW.CONTACT DETAILS FOR MORE INFO:Wickr ID :::::: brookmax5Kik :::::::::: Brookmax56Telegram::::::: brookmax54ONLINE ORDER TRACKING AVAILABLE.MONEY BACK GUARRANTEEDISCREET FREE SHIPPINGHIGH QUALITY MEDICATIONS..

Type
Product

created on
June 18th, 2021

Fig. 3: Suggestions generated for a product sold on a dark market

Such a sub-graph is virtual because it is not (yet) part of the investigation, it does not represent real knowledge and needs to be validated by the user before being added to the knowledge graph. Since it is a sub-graph, a suggestion consists of one or more relationships and nodes: the simplest form of a suggestion is a single relationship, linking two nodes in the knowledge graph. Produced suggestions are proposed as grey parts of the knowledge graph, waiting for users to validate them. A user can decide to validate or not a suggestion, as well as to leave it as is in the knowledge graph and decide on it later. This is because in an investigation the collection of the required information to validate a suggestion could come at different time frames.

Suggestions are produced on the basis of a) similarity metrics between nodes, b) matches between information stored in the knowledge graph and crawled contents, c) ontological inference and topological patterns identified on the basis of how nodes are interlinked between them. For the latter case, a dedicated ontology has been realised, focused on illegal trafficking domain and events of interest. The ontology includes entities managed inside the knowledge graph (Fig. 4). For *Event* and *Object* concepts, specific categories have been included to characterize illegal trafficking domain. Events can be categorized as *Browsing*, *Delivery*, *Manufacturing*, *Messaging*, *Posting*, *Purchasing*, *Selling*, *Sending* and *Transaction*: those types of events can potentially be part of broader illegal trafficking activities. Objects can be instead categorised as *Services* or *TradedGoods*. *Service* concept refers to intangible services that are sold in black markets (hacking services, frauds, etc.), while *TradedGood* concept refers to physical objects, like drugs, weapons, and precursors. Precursors are intended as materials used in the illegal manufacturing of drugs or explosives and have been selected as stated in the European Regulation on drug precursors [11] and on the marketing and use of explosives precursors [12] currently in force.

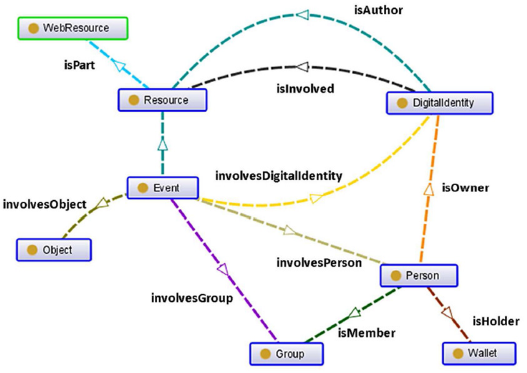
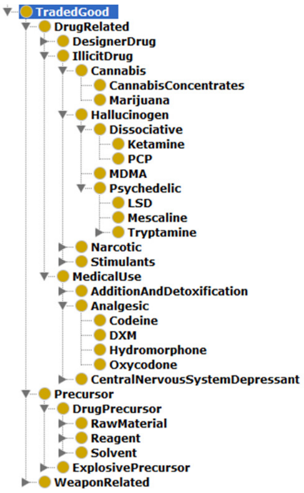


Fig. 4: ANITA knowledge graph ontology

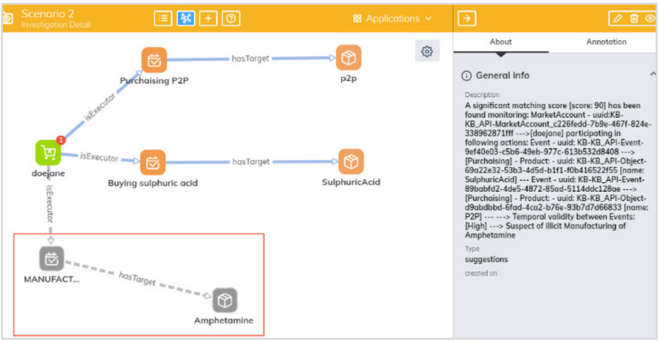
Starting from this ontology, it was possible to set ontological rules to identify patterns of events and entities in the knowledge graph and derive more complex illegal trafficking-related activities from them. A *knowledge pattern* (KP) is the topological definition of a sub-graph in the knowledge graph that can be relevant to the domain of application. Generally, a sub-graph contains more information than the sum of single entities that compose it, since it also involves the relationships (with types and metadata) existing among these entities. This makes KPs suitable to represent complex information that exists among one or more entities and that would not be represented with the same level of accuracy by considering each single entity at time.



- TradedGood
  - DrugRelated
    - DesignerDrug
    - IllicitDrug
      - Cannabis
        - CannabisConcentrates
        - Marijuana
      - Hallucinogen
        - Dissociative
          - Ketamine
          - PCP
        - MDMA
        - Psychedelic
          - LSD
          - Mescaline
          - Tryptamine
      - Narcotic
      - Stimulants
    - MedicalUse
      - AdditionAndDetoxification
      - Analgesic
        - Codeine
        - DXM
        - Hydromorphone
        - Oxycodone
      - CentralNervousSystemDepressant
  - Precursor
    - DrugPrecursor
      - RawMaterial
      - Reagent
      - Solvent
    - ExplosivePrecursor
  - WeaponRelated

Fig. 5: Part of ANITA ontology

By defining domain-oriented KPs and including a set of rules based on the temporal, spatial and causal relationships between events, it has been possible to recognize high-level illegal activities starting from low-level information about resources, people, digital identities, groups, organizations, objects, events and their relationships (Fig. 6).



General info

Description

A significant matching score [score: 90] has been found monitoring: MarketAccount - uuid:KB-KB_API-MarketAccount_c226fedd-7b9e-467f-824e-338962871fff --->[doejane] participating in following actions: Event - uuid: KB-KB_API-Event-9ef40e03-c5b6-49eb-977c-613b532d8408 ---> [Purchaising] - Product: - uuid: KB-KB_API-Object-69a22e32-53b3-4d5d-b1f1-f0b416522f55 [name: SulphuricAcid] --- Event - uuid: KB-KB_API-Event-89babfd2-4de5-4872-85ad-5114ddc128ae ---> [Purchaising] - Product: - uuid: KB-KB_API-Object-d9abdbbd-6fad-4ca2-b76e-93b7d7d66833 [name: P2P] --- ---> Temporal validity between Events: [High] ---> Suspect of illicit Manufacturing of Amphetamine

Type

suggestions

created on

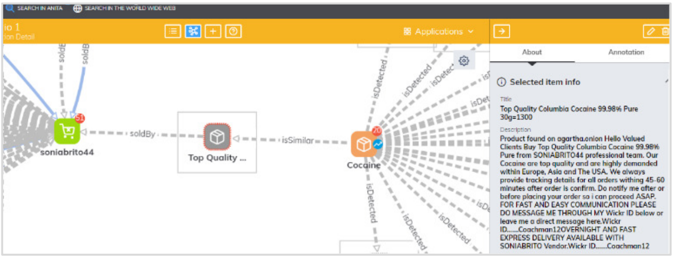
Fig. 6: Recognition of high-level activities

KPs that represent complex illegal activities have then a well-known topology. Starting from knowledge of these expected KP topologies, it is also possible to identify incomplete KPs. Incomplete patterns can be useful to alert users about potential suspicious activities that can occur and to suggest users which kind of missing information to look for to complete a pattern. In the former case, users can prevent that an illicit activity occurs. In the latter case, in case of successful pattern completion, users can verify that an illegal activity has really occurred. This way, the process can guide not only in "recognizing", but also in "tracking" emerging illegal activities. Once the user validates a suggestion, nodes and relationships belonging to that suggestion are stored in the knowledge graph, ready to be exploited for further tasks. That way, both the user and the platform take advantages from this iterative and interactive approach: the user receives support from the platform in discovering hidden links and considering additional investigative pathways and strategies, while the platform benefits from user validation feedback to minimize the risk of false positives presence, thus maintaining only high-quality information in the knowledge graph.

IV. Operational Scenarios

ANITA platform has been tested by users during two pilot sessions planned for the project. Two realistic scenarios were prepared which combine the project use cases: drugs trafficking, weapons trafficking, and terrorist funding. The scenarios include actors that are active both in Dark web markets and on the Surface web. The collection of information, their analysis and understanding - with the support of ANITA - can provide useful insights for both monitoring and investigative purposes. The added value is represented by the capacity to connect-the-dots, experiment with different paths of analysis and validate diverse hypothesis, through a user-centred approach.

The first scenario focuses on a man, arrested because in possess of cocaine bought on a specific black market. Police want to know more on who is behind this illegal business. First steps that are performed by a user through ANITA is starting a monitoring task on the monitored market and uploading the suspicious emails found in the laptop of the arrested man. ANITA starts retrieving contents from the selected market, as well as analysing uploaded emails, from which information is extracted, added in the knowledge graph, and compared to that collected from Agartha market. A match between an email address and a vendor nickname is found and proposed to the user as suggestion, as well as the same vendor and the cocaine product (Fig. 7). Through the continuous interaction between the system, through the generation of suggestions, and the user, through the validation of proposed suggestion, it is found that the vendor has also left traces on Reddit, as well as on Surface web sites, where other email addresses are found, leading to the hypothesis that a criminal network, instead of single individual, could be behind the selling of cocaine (and possibly other illegal products).



Selected item info

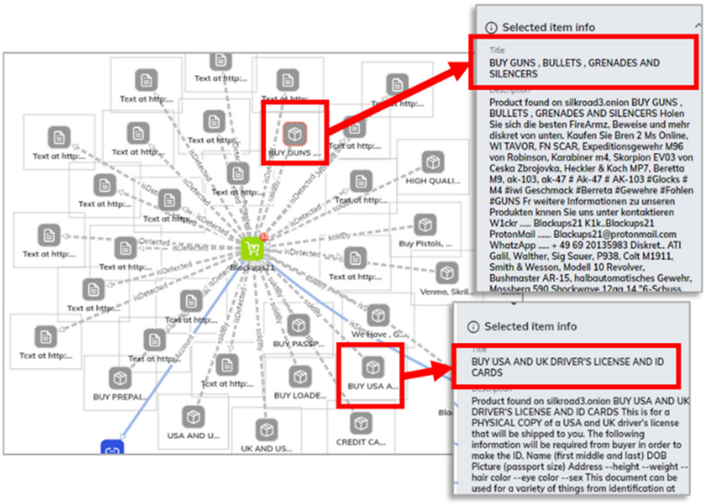
Title
Top Quality Columbia Cocaine 99.98% Pure 30g=1300

Description
Product found on agartha.onion Hello Valued Clients Buy Top Quality Columbia Cocaine 99.98% Pure from SONIABRITO44 professional team. Our Cocaine are top quality and are highly demanded within Europe, Asia and The USA. We always provide tracking details for all orders withing 45-60 minutes after order is confirm. Do notify me after or before placing your order so i can proceed ASAP. FOR FAST AND EASY COMMUNICATION PLEASE DO MESSAGE ME THROUGH MY Wickr ID below or leave me a direct message here.Wickr ID.......Coachman12OVERNIGHT AND FAST EXPRESS DELIVERY AVAILABLE WITH SONIABRITO Vendor.Wickr ID.......Coachman12

Fig. 7: Suggestions proposed by the platform for the first scenario

The second scenario is about a person stopped by police during a daily roadblock. Police found a rifle inside his car. During the interrogation, the car driver admitted having bought the rifle on Darkmarket. The police want to gather more information – and possibly evidence – about vendors selling this type of rifle, so to better assess if the business is done legally or not. From the monitoring of Darkmarket, a vendor is found to sell the same rifle found in the car, but also other kinds of weapons, fake identity cards, drive licences and credit cards (Fig. 8).

Then, the user starts searching through ANITA more information on the vendor, finding that two web markets on the Surface web are active, registered under two different aliases (one of them equal to the vendor nickname), but with "About us" page with identical description and with one equal phone number (multiple numbers are present in the Contact page of both markets). Then, it is found that one of the other phone numbers is referring to a Pinterest account collecting pins related to identity cards of different nationality. This leads the user to the hypothesis that the vendor could be linked to other types of illegal activities and continue to investigate on that with the support of ANITA.



Selected item info

Title
BUY GUNS , BULLETS , GRENADES AND SILENCERS

Description
Product found on silkroad3.onion BUY GUNS , BULLETS , GRENADES AND SILENCERS Holen Sie sich die besten FireArmz, Beweise und mehr diskret von unten. Kaufen Sie Bren 2 Ms Online, WI TAVOR, FN SCAR, Expeditionsgewehr M96 von Robinson, Karabiner m4, Skorpion EV03 von Ceska Zbrojovka, Heckler & Koch MP7, Beretta M9, ak-103, ak-47 # Ak-47 # AK-103 #Glocks # M4 #iwi Geschmack #Berreta #Gewehre #Fohlen #GUNS Fr weitere Informationen zu unseren Produkten knnen Sie uns unter kontaktieren W1ckr ...... Blackups21 K1k..Blackups21 ProtonMail .... Blackups21@protonmail.com WhatzApp ..... + 49 69 20135983 Diskret.. ATI Galil, Walther, Sig Sauer, P938, Colt M1911, Smith & Wesson, Modell 10 Revolver, Bushmaster AR-15, halbautomatisches Gewehr, Mossberg 590 Shockwave 12ga 14 "6-Schuss

Selected item info

Title
BUY USA AND UK DRIVER'S LICENSE AND ID CARDS

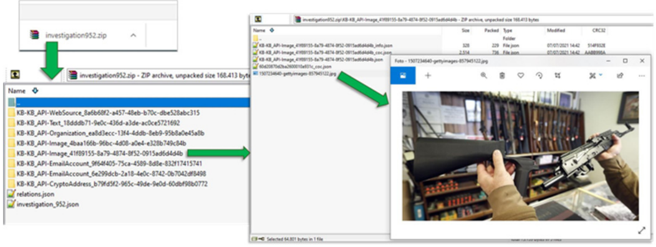
Description
Product found on silkroad3.onion BUY USA AND UK DRIVER'S LICENSE AND ID CARDS This is for a PHYSICAL COPY of a USA and UK driver's license that will be shipped to you. The following information will be required from buyer in order to make the ID. Name (first middle and last) DOB Picture (passport size) Address --height --weight --hair color --eye color --sex This document can be used for a variety of things from identification at

Fig. 8: Products suggested by the platform for the second scenario

ANITA enables to demonstrate in court the entire investigative reconstruction thanks to its own lawful chain of custody and evidence (CoC/CoE). The need of embedding a CoC/CoE mechanism into ANITA system originates from the danger that stored data could be accessed and manipulated in unauthorised and malicious way to compromise current investigations.

Data stored into the ANITA system by the CoC/CoE can be divided in two main categories: multimedia resources and metadata generated manually or added after validation of analysis results. Chain of evidence consists in the calculation of a digital mark that uniquely identifies a resource every time it is modified. Its hash value is continuously recalculated and compared to the known one, to verify its integrity. Whenever a hash value of a resource does not correspond to that computed at acquisition time, this means that the resource has been corrupted in unauthorized way. Integrity of resources forensically marked in this way can be proved and ensured through comparison of hash values. Instead, chain of custody must be maintained for both resources and metadata. Chain of custody refers to mechanisms for logging activities that have been performed by a user or the system over stored information. Chain of custody, together with chain of evidence in case of resources, enables the forensic reuse of information stored into ANITA system.

Functionalities to handle the evidence export have been realised to allow users to export information of the investigative reconstruction. The output of the export services consists in an archive package containing metadata of the investigation to which the entities being exported belong, metadata of those entities, potential relationships among them tracked into ANITA, and the chain of custody (Fig. 9).



investigation952.zip

investigation952.zip - ZIP archive, unpacked size 168.413 bytes

Name

KB-KB_API-WebSource_8a6b68f2-a457-48eb-b70c-dbe528abc315
KB-KB_API-Text_18dddb71-9e0c-436d-a3de-ac0ce5721692
KB-KB_API-Organization_ea8d3ecc-13f4-4ddb-8eb9-95b8a0e45a8b
KB-KB_API-Image_4baa166b-96bc-4d08-a0e4-e328b749c84b
KB-KB_API-Image_41f89155-8a79-4874-8f52-0915ad6d4d4b
KB-KB_API-EmailAccount_9f64f405-75ca-4589-8d8e-832f17415741
KB-KB_API-EmailAccount_6e299dcb-2a18-4e0c-8742-0b7042df8498
KB-KB_API-CryptoAddress_b79fd5f2-965c-49de-9e0d-60dbf98b0772
relations.json
investigation_952.json

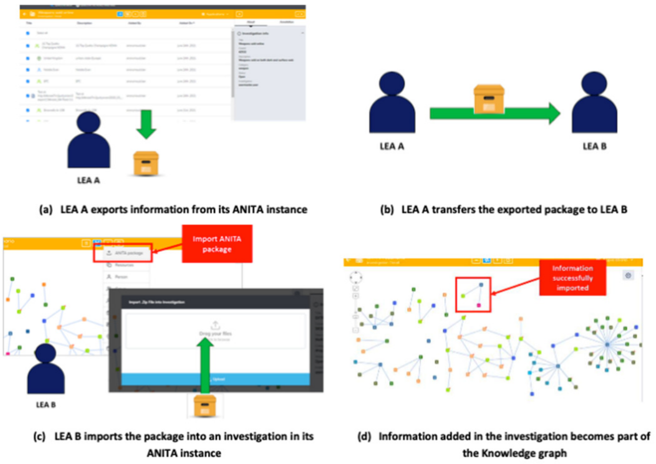
Selected 64.801 bytes in 1 file

Fig. 9: Export of investigative reconstruction package

The ANITA export package format was realised according to the two assumptions:

- any LEA could have its own ANITA instance running on their premises, most likely running within a secured networking infrastructure directly managed by the IT team of that LEA;
- because of different legislations and procedures in force into any nation, it would be advisable that the sharing of information is managed at organizational level: organisations could agree through signed documents the sharing of information.

Due to these assumptions, the solution adopted to enable information sharing capabilities between two physically separated ANITA instances was to include in the system complementary export and import services to be used by end users whenever needed (Fig. 10).



(a) LEA A exports information from its ANITA instance

(b) LEA A transfers the exported package to LEA B

(c) LEA B imports the package into an investigation in its ANITA instance

(d) Information added in the investigation becomes part of the Knowledge graph

Fig. 10: Export and import functionalities to support information sharing between LEAs

V. Conclusions

ANITA platform has been realized to support LEAs' activities in combating illegal trafficking activities, as well as related crimes with different nature but somehow linked. Through a knowledge-based and user-centred approach, it was shown how the users and the platform itself can benefit from each other in investigative cases. Their continuous interaction enables to connect-the-dots in faster and higher-quality way, while always keeping in the loop the human factor in the validation of suggestions proposed by the platform.

Acknowledgments

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n° 787061 and topic SEC-12-FCT-2016-2017 (Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism).
The support is gratefully acknowledged.

References

[1] EU SOTCA 2021 – European Union Serious and Organised Crime Threat Assessment - QL-09-21-093-EN-C / ISBN :978-92-95220-23-2 / DOI: 10.2813/02362

[2] M. Faizan and R. A. Khan, "Exploring and analyzing the dark web: A new alchemy," First Monday, vol. 24, no. 5, pp. 1–20, 2019.

[3] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in Proc. 22nd Int. World Wide Web Conf., Brazil: Rio de Janeiro, pp. 213–224, 2013.

[4] Alyami H., Faizan M., Alosaimi W., Alharbi A., Pandey A. K., Ansari Md T. J., Agrawal A., Khan R. A., "An Ensemble Approach to Identify Firearm Listing on Tor Hidden-Services". Comput. Syst. Sci. Eng. 38(2): 141-149, 2021.

[5] Rawat R., Rajawat A.S., Mahor V., Shaw R.N., Ghosh A., "Dark Web-Onion Hidden Service Discovery and Crawling for Profiling Morphing, Unstructured Crime and Vulnerabilities Prediction". In: Innovations in Electrical and Electronic Engineering pp. 717-734, Springer, Singapore, 2021. https://doi.org/10.1007/978-981-16-0749-3_57

[6] A. T. Zulkarnine, R. Frank, B. Monk, J. Mitchell and G. Davies, "Surfacing collaborated networks in dark web to find illicit and criminal content," 2016 IEEE Conference on Intelligence and Security Informatics (ISI), pp. 109-114, 2016. doi: 10.1109/ISI.2016.7745452

[7] Paterva Maltego. Available at: https://www.maltego.com/

[8] IBM i2 Intelligence Analysis Portfolio. Available at: https://www.ibm.com/products/i2-enterprise-insight-analysis

[9] Palantir Intelligence Technologies. Available at: https://www.palantir.com/offerings/intelligence/

[10] SAS Intelligence and Investigation Management. Available at: https://www.sas.com/it_it/software/intelligence-investigation-management.html

[11] Regulation (EC) No 273/2004 of the European Parliament and of the Council of 11 February 2004 on drug precursors. Available at: https://eur-lex.europa.eu/eli/reg/2004/273/2021-01-13

[12] Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013. Available at: https://eur-lex.europa.eu/eli/reg/2019/1148/2019-07-11