



ADVANCED TOOLS FOR FIGHTING
ONLINE ILLEGAL TRAFFICKING

ANITA PLATFORM HANDBOOK

Edited by

Ivana Bodrožić, PhD, Assistant professor of Criminal law

Milan Srećković

Vladimir Aksentijević

Published by

University of Criminal Investigation and Police Studies, Belgrade

ISBN 978-86-7020-467-6

BELGRADE, 2021.

FOREWORD

The main purpose of writing this manual is to support the implementation of training within the Anita project, as well as to facilitate the process of mastering the necessary skills for members of law enforcement agencies.

As the Anita project is primarily intended to strengthen the capacity of law enforcement services, through the process of their continuous training, such a manual should serve as a basis and reference point for the acquisition and implementation of knowledge and skills in practice.

The manual was created as a textbook of materials used in the first pilot training, in which the trainers presented the necessary knowledge and skills in the shortest but at the same time most transparent way.

The manual is systematized in relation to several criteria:

1. according to the criterion of generality, from general information to specific data;
2. according to the temporal, i.e. chronological criterion, in relation to the temporal dimension of the author's presentation, i.e. trenbera, and
3. according to the criterion of the type of media used, on the PowerPoint presentation materials and video material, which is available to each participant in the training, with the code and credentials.

The manual is divided into several sections, which follow the dynamics and structure of the training, but also contains general remarks about the Project and the platform, its content, expected opportunities, and scope in combating illegal online trade.

It is to be expected that it will serve as a basis and a reference point for further training, determined primarily by the dynamics and content of changes in the training process itself.

LIST OF CONTENT

Foreword.....	2
Instead of Introduction – Short Review of the ANITA project from the program "Horizon 2020"	4
1. General Overview – Consortium, Goal, and Objectives	6
2. Content Aquisition	19
3. Case Studies	27
4. Simulated example of an horizontal scenario.....	36
5. ANITA Graph entity legend	64
Conclusion.....	66

INSTEAD OF INTRODUCTION – SHORT REVIEW OF THE ANITA PROJECT FROM THE PROGRAM "HORIZON 2020"

In January 2014 the European Union adopted a new concept and program for financing science and technological development called "Horizon 2020", which consists of three pillars - excellence in science, leadership in industry, and society. Within this area of research, the ANITA project was launched in May 2018, led by a consortium of 17 partners from 11 countries with the main goal of the development and creation of a state-of-the-art, science-based, and user-oriented research platform to overcome the challenges banned. Online store, which provides tools for creating databases, blockchain analysis, analysis of large amounts of data, modeling knowledge and exploitation of such modeling, incorporation of cognitive function in analysis, and providing user-oriented intelligence applications.

One of the members of the consortium is the University of Criminal Investigation and Police Studies, as the youngest state university in the Republic of Serbia and a leading institution in the field of higher education, training, and specialist training of future and current police officers and members of other law enforcement services (law enforcement agencies). Within the division of project responsibilities, the so-called work packages, the University is in charge of transmitting and disseminating project results, training, and education. Work package 11, which is assigned to the University, includes the development of mechanisms and tools for dissemination of results, the establishment of a community of stakeholders of project participants so that, in the context of knowledge and skills, they can benefit from the experience gained on the project, as well as identifying best practices, developing adequate curricula and preparing training for the development of a strategy and plan for the exploitation of project results.

As a general project task, ANITA studies, creates, and develops: 1) innovative blockchain technologies for network and cryptocurrency analysis, 2) sophisticated analytical tools for large amounts of data for automated extraction and analysis, 3) sophisticated methodologies for making, modeling, reasoning, processing and storing knowledge in forms understandable to the human race and 4) user, adaptive and modeling framework that allows the collection, analysis, translation and explanation, imitation and integration of human cognitive information and user-oriented intelligence applications, equipped with control panels for research, reconstruction and identification of special temporal and causal correlations among the events of illegal trade.

It is planned that the listed tasks will be accomplished by applying various approaches, such as a multidisciplinary one that provides an online investigation system of illegal online trade (online trafficking). It is an automatic, wide-ranging, user-oriented cognitive system for

efficient detection of illegal online trade activities that enables: gathering knowledge and information for the domain of application applications and their use for training new members of the police; anonymous identification of new relevant content while maintaining a balance between speed and accuracy; high level of downloading and storing in a secure repository; assessment and evaluation of the importance of web source research and blockchain analysis, to reveal links and evidence of illegal transactions.

Project beneficiaries have played a key role in this from the very beginning by helping to identify and prioritize the required functionalities, participate and provide support in design and evaluation by demonstrating the application of the system and contributing to defining training activities and organizing workshops on which will analyze and evaluate the results of the project.

All mentioned activities, framework, goals, methodology, and evaluation are established following ethical principles and relevant national and international legislation, as well as with the laws of the European Union, including the Charter of Fundamental Rights of the European Union and the European Convention on human rights.

All of the above was transferred to the preliminary training system, which was held in the form of pilot training and which contains practical aspects of the application of the Anita platform in everyday police work.

Like any training program, pilot training has supporting material in the form of manuals, which should serve to facilitate the process of mastering the knowledge and skills presented in the training.

1. GENERAL OVERVIEW – CONSORTIUM, GOAL, AND OBJECTIVES

by Ernesto La Mattina

The first presentation material is intended for the distribution of basic data on the project, consortium, objectives as well as the use of a case study to support law enforcement services in detecting and reconstructing the illegal trade chain in specific areas.

The project started on May 1, 2018, with the planned completion date of October 31, 2021.

It was written for the call of the European Commission within the Horizon 2020 project, and is being implemented under the number H2020-SEC-12-FCT-2017, also under the title Technologies for prevention, investigation, and mitigation in the context of fight crime and terrorism.

The priority goal is to design and develop the platform, through cooperation with law enforcement services, which will aim to identify relevant data sources disseminated via the Web, including Darknets, as well as analyze and expand the scope of knowledge and to link existing data with the existing corpus. Knowledge of police officers, in order to support and improve the investigation of illegal trade.

The project involves 11 countries, 17 partners, one of which is from the area of Industry, two SMEs, two NPOs, as well as 6 law enforcement services.

In addition to the basic data that training participants must have, the most important part of the presentation material of the first part of the training is the enumeration and knowledge of the goals.

They are categorized as:

- improvement and strengthening of analytical services in the investigation process for Surface Web and Darknet,

- expanding the scope and domain of existing knowledge of police officers from the personnel to the automated level, in order to collect, design, distribute and increase the efficiency and ability to reason,
- understanding the phenomenon of illegal trade and its causes, in order to develop and support effective countermeasures and activities to build appropriate policies and decision-making,
- enabling the verification of tools by the law enforcement services of the consortium members, in order to check them in practical circumstances,
- providing efficient Big Data analytical services, law enforcement services,
- gathering of human resources within the operational analytical group,
- Distribution of TRL6 / TRL7 applications to combat illegal trade and other criminal activities
- and finally ensuring the compliance of the entire application, its application, and model with social, ethical, legal, and other requirements, as well as requirements that protect the right to privacy.

ANITA Consortium

ANITA

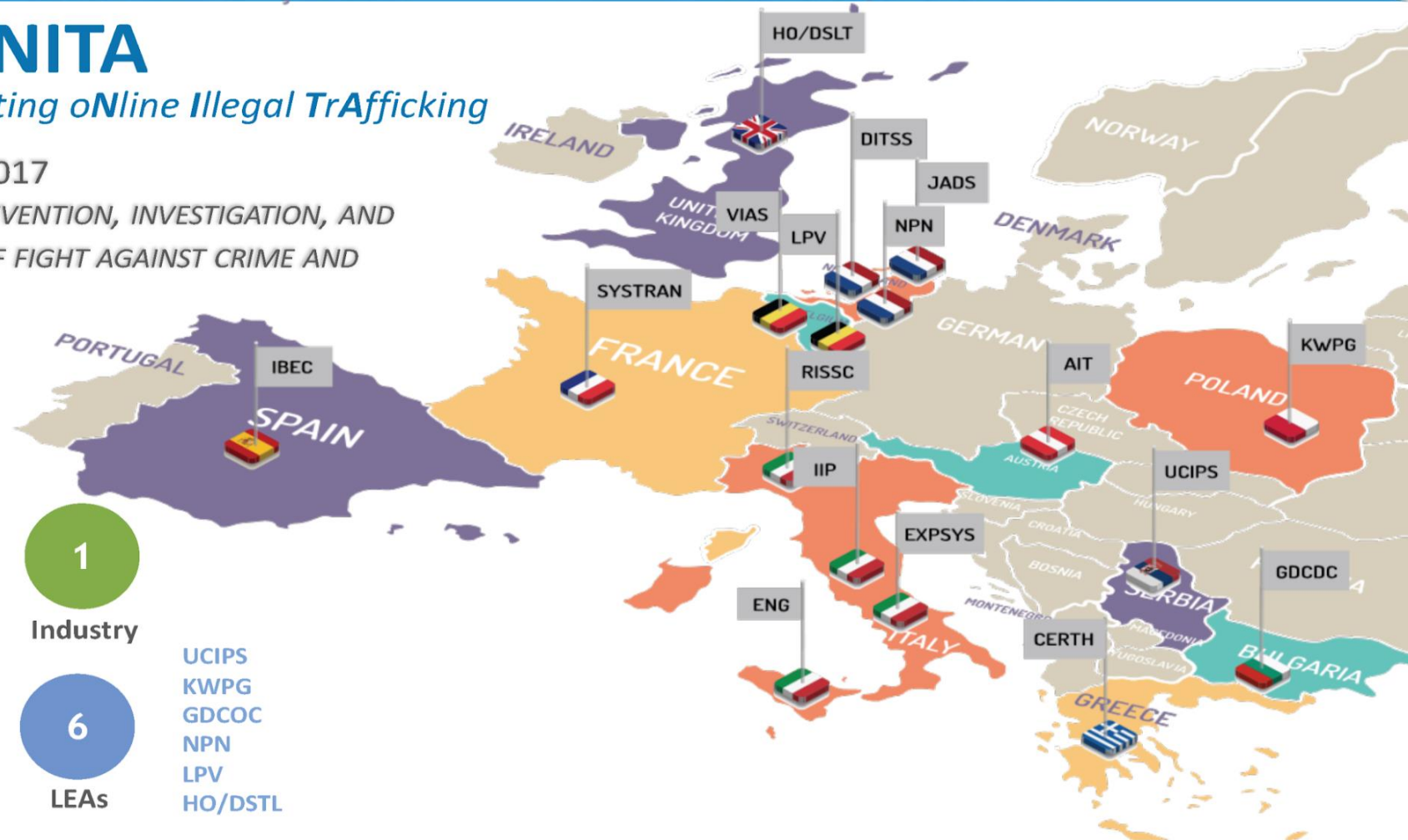
Advanced tools for fighting oNline Illegal TrAfficking

CALL: H2020-SEC-12-FCT-2017

TOPIC: TECHNOLOGIES FOR PREVENTION, INVESTIGATION, AND MITIGATION IN THE CONTEXT OF FIGHT AGAINST CRIME AND TERRORISM

START: 1 MAY 2018

END: 31 OCTOBER 2021



17

Partners

11

Countries

1

Industry

2

SMEs

2

NPOs

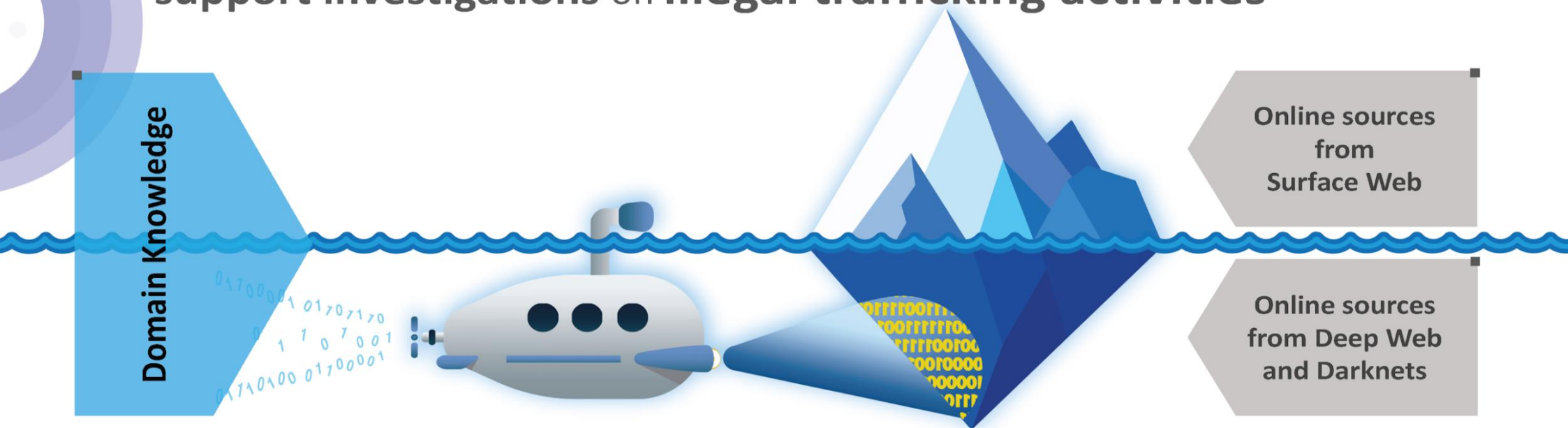
6

LEAs

UCIPS
KWPBG
GDCOC
NPN
LPV
HO/DSLTL

ANITA Goal

ANITA aims to collaborate with Law Enforcement Agencies to design and develop a **novel user-centered investigation platform** to discover relevant data sources disseminated on the Web (including Darknets) and analyse, enrich and correlate them with the pre-existing officers knowledge to support investigations on **illegal trafficking activities**



ANITA Objectives

- 1** To enhance investigation analytics services for Surface Web and Darknets
- 2** To provide LEAs with accurate and efficient Big Data analytics services
- 3** Automated domain knowledge collection, modelling, sharing and reasoning capabilities
- 4** Integration of the human expert in the investigative analysis loop
- 5** Understanding the phenomenon and its route causes and supporting efficient counter measures and policy making acts
- 6** Delivering TRL6/TRL7 applications for fighting illegal trafficking and criminal activities
- 7** Deploying tools at consortium LEAs' premises for evaluation in real operational environments
- 8** Ensuring adherence to social, ethical, privacy and legal requirements

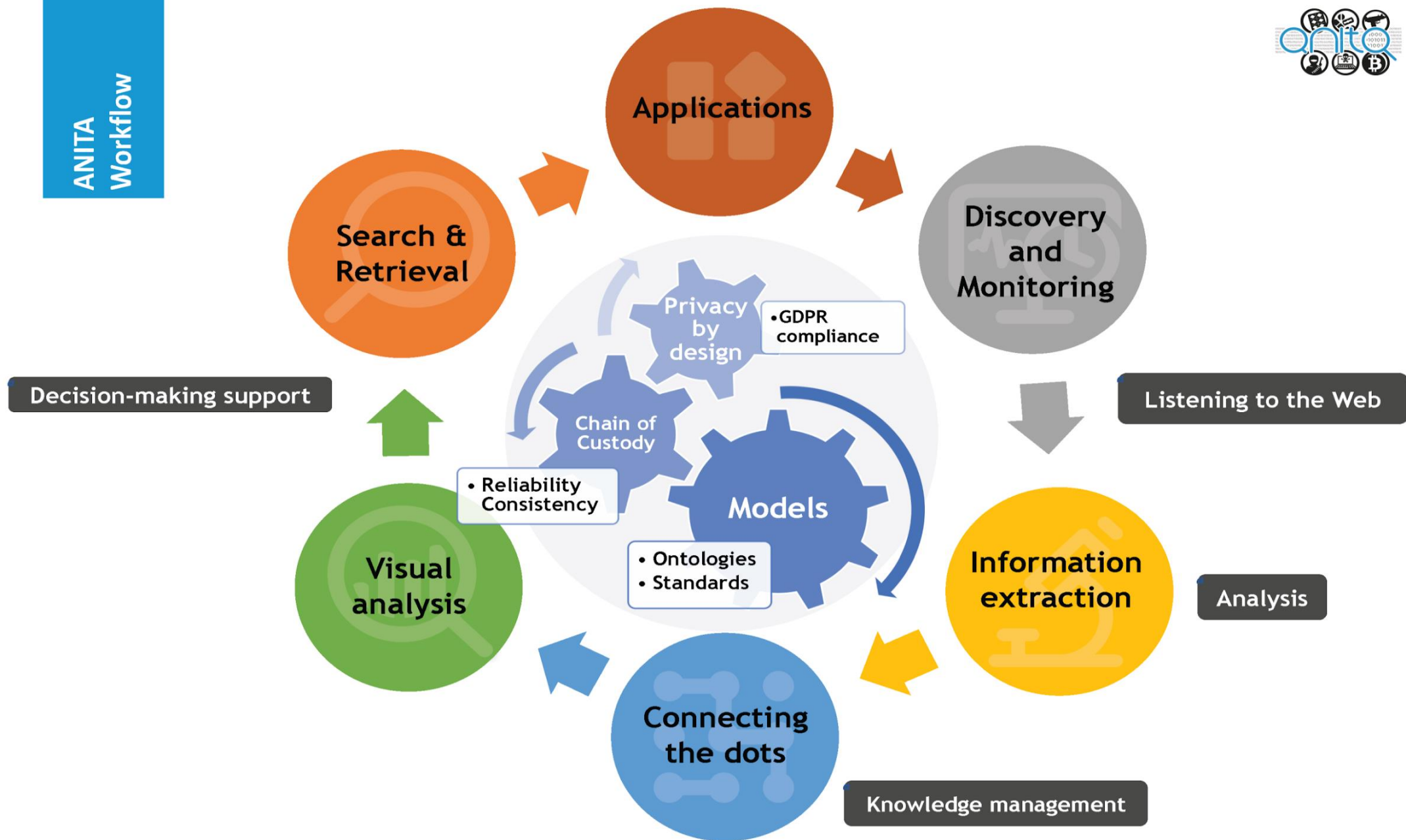
Use cases

Supporting LEAs investigations to **discover** and **reconstruct the illegal trafficking chain** in specific areas

NPS, Drugs and Counterfeit medicines

Weapons and firearms

Trafficking related to terrorist activities and funding



Listening to the web: Discovering and monitoring

The collage displays several key features of the onit platform:

- Investigation Detail View:** Shows a sidebar with navigation options (Investigation folders, Financial transactions, Monitoring, Deep Crawling, Data copy requests, Pinned sources) and a main panel with investigation information (Title, Case ID, Description, Category, Open status, Investigators).
- Product Listings:** Displays a grid of products with images, titles, and prices. Examples include 'Digital Goods', 'Carded Items', 'Services', 'Software & Malware', and 'Hosting & Security'.
- Investigation Table:** A table listing investigations with columns for ID, Title, Created On, and Owner. It includes entries like 'Investigation Title', 'Investigation 4', 'Drugs traffic case', 'Drug ring 3', 'Drug ring 2', and 'Drug ring'.
- Product Detail View:** Shows a detailed view of a product listing, including a 'Downloaded Pages' section, a 'Vendors' section, and a 'Products' section with a list of items and their prices.
- Word Cloud:** A large, stylized word cloud in the center, representing the 'List of words sorted by total term frequency'.

Big Data Analysis and Analytics



Named entity recognition



Topic extraction



Classification Clustering



Summarization



Emotions recognition



Stylometric Analysis



Image and Video analytics



Multilingual automatic translation



Speech to Text

XYlogaLft8Y.mp4
Video Detail Detail

Applications

ORIGINAL RESOURCE SPEECH TO TEXT TEXT SUMMARIZATION TEXT CLASSIFICATION STYLOMETRIC ANALYSIS

Language Detected: ar

Transcription:

وهذا واحد من الإرهابيين الذين خصموا لعمليات زرع الفكر التكفيري ، فبات وحدا في صورة إسماعيل عدنان أحمد بالرغم من وين جاي من إرسل مبعوث من عند مارتن ذو يشغل أن جهة الصورة ... تكون الفهم معكم عثمان ذو قاتل الجيش السوري المجموعة الباقية التي معه ... حبيب أنت فلا تمكني عن التليفزيون السوري هذا التليفزيون السوري ونحن الجيش السوري وعناصر الجيش السوري التليفزيون السوري مل أنت بين الجيش السوري ... لا ما بين ... أرسلنا أنت أياك ممر التحقيق معكم هذا على الحرية ... العلم يشغل ... أنت العلم ما بأعرفه بين أوره عدد دم على أيدع جيت لي عندما ثقب بوز عليه ... صدر بني انشوا المعصرة مينة

Translation:

This is one of the terrorists who was subjected to the operations of planting takfiri thought. He became a monster in the image of Adnan Ahmed, although where is he coming from, sending an envoy from Martin, what is his job, is that Jabhat Al-Nusra ... be with you, because what did the Syrian army kill the rest of the group with you ... OK, are you now talking about the Syrian television, this is the Syrian TV, we are the Syrian army and the Syrian TV, are you between the Syrian army ... no between ... we sent you answer egypt, the investigation with you is flexible ... the teacher is working ... You know what I don't know, but his father has blood on his followers, you came to me when

anite Search by keywords

SEARCH IN ANITA SEARCH IN THE WORLD WIDE WEB

weapons.jpg
Image Detail Detail

Applications

ORIGINAL RESOURCE OBJECT DETECTION VISUAL INDEXING (LOCATION-BASED) CONCEPT DETECTION

categories matching
Rifles

Category	Accuracy
Rifles	95%
Rifles	61%

View B.B.

Article2.txt
Text Detail Detail

Applications

TRANSLATION STYLOMETRIC ANALYSIS TEXT SUMMARIZATION TEXT CLASSIFICATION ENTITY RECOGNITION

14 CONCEPT 6 LOCATION 3 ORGANIZATION 4 PERSON ALL

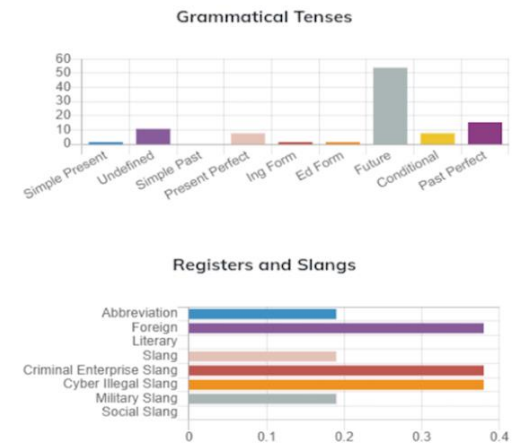
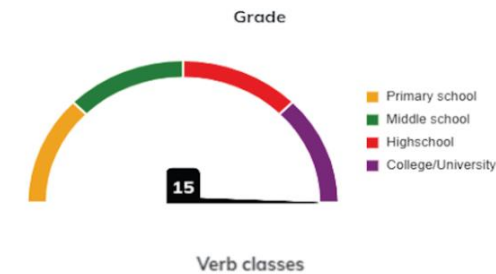
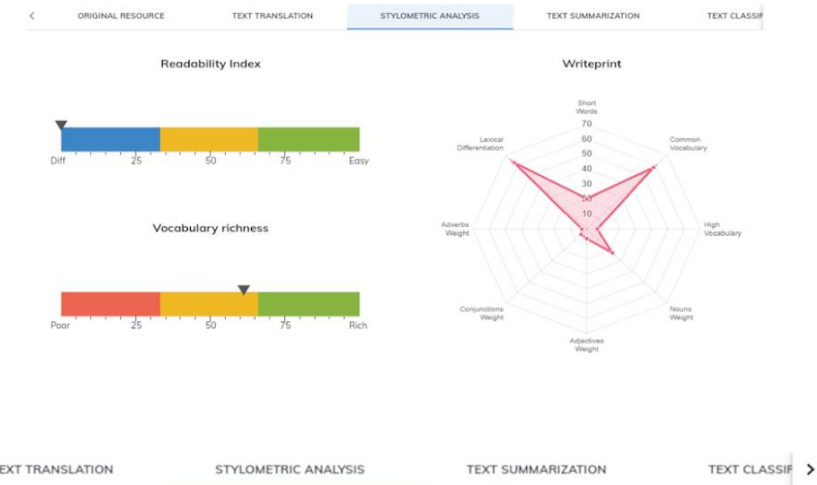
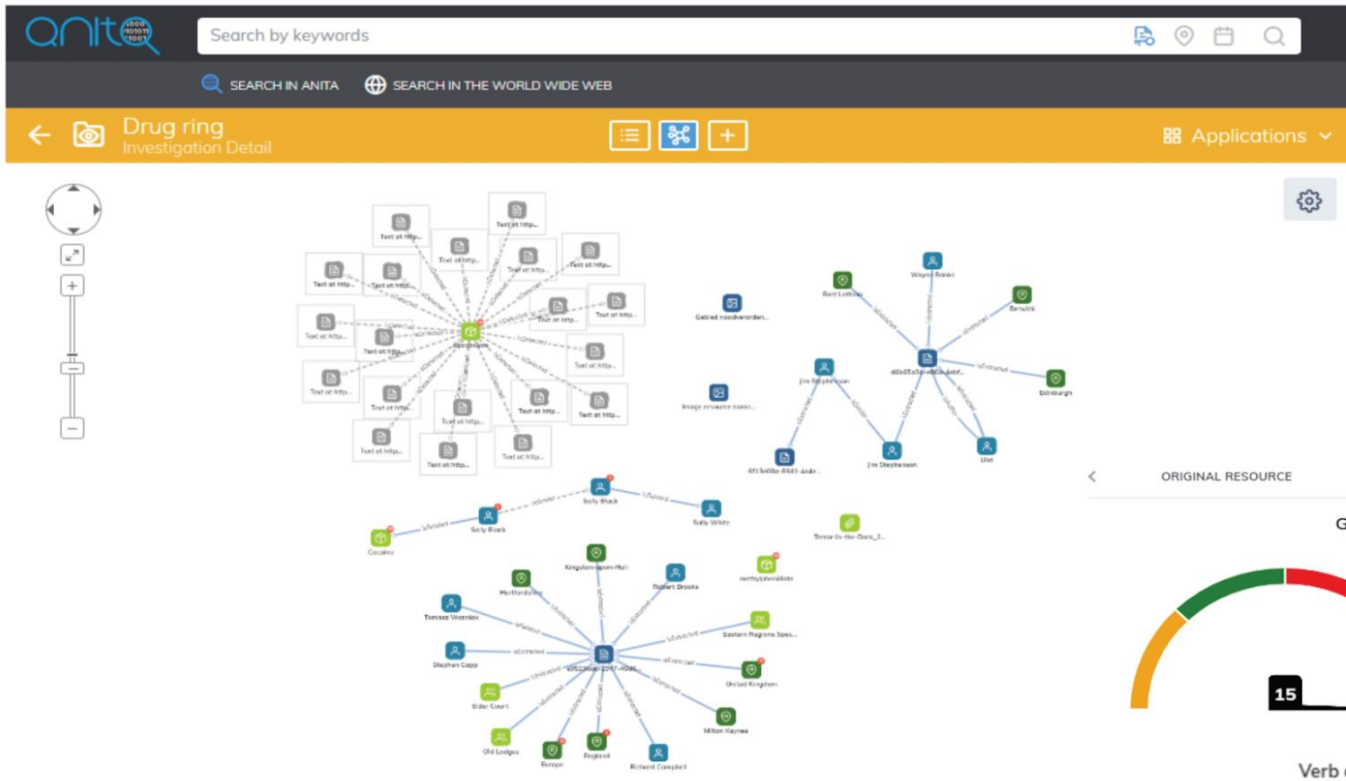
Name	Type	Matches
Milton Keyr	Location	1
England	Location	1
Robert Brooks	Person	1
Eastern Re	Location	1
Hertfordshi	Location	1
United King	Location	1

The leader of a 58m drug smuggling ring was jailed after his own dashcam recorded cocaine and heroin being distributed from a Hertfordshire farm. Robert Brooks was sentenced to 21 years in prison for importing Class A drug. It was the largest ever drugs conspiracy investigated by the region's police and has been documented on Channel 4's 24 Hours in Police Custody. An officer said "it would have been a lot harder" to convict Robert Brooks without the footage. The officer for the Eastern Regions Special Operations Unit, who is remaining anonymous, said Robert Brooks "s complacency, stupidity and lack of attention to detail" meant his dashcam recorded drugs being collected from his business unit on Little Samuels Farm in Hunsdon. Robert Brooks "m still quite shocked Robert Brooks was stupid enough to have it in his car and have it recording when someone picked up the commodity," Robert Brooks said. Robert Brooks, 51, of Elder Court, Hertford, pleaded guilty to conspiracy to fraudulently evade the prohibition on the importation of Class A drug and possession of criminal property, and was jailed in September. Robert Brooks was described as the managing director of the English end of the operation that was connected to Europe and further afield, prosecutors said. Leader of 58m drug smuggling ring jailed Three jailed for roles in 58m drug smuggling ring Gang jailed for 65m illegal steroid operation In August 2019 officers from the Eastern Regions Special Operations






Knowledge Generation and Reasoning



Tools and Applications for Law Enforcement Agencies



Main results of the second Period

-  **Final version of System Architecture defined**
-  **Pilot plans prepared and replanned**
-  **Analysis tools and ANITA platform validated in Lab**
-  **First training session organised**
-  **Plan for public demonstration and dissemination of the results within EU LEAs Community**

Advisory Board

- Policia Judiciaria, Portugal
- Turin Local Police, Italy
- Security Science Center of Óbuda University, Hungary
- Métropole Nice Côte d'Azur, France
- Directorate General Logistics, Romania
- Landeskriminalamt Baden-Württemberg, Germany
- Policia Municipal de Madrid, Spain
- Metropolitan Police, London
- Police of the Czech Republic

Future actions

-  **To continue training activities**
-  **To perform pilots and evaluation (2 rounds)**
-  **To organise public demonstrations**
-  **To deploy system in LEAs premises for evaluation in operational environment**

2. CONTENT AQUISITION

by Joachim Klerx

The second part of the training is about collecting the content available within Darknet, i.e. the sequence of necessary steps that lead to the identification of sources on the Darknet through a meta-search engine developed within the Anita platform.

Mentioned in the context of functionality implies the identification of potential data sources, markets, communication channels through regular Web services, Deep web, and darknet with emphasis on the fact that this is evidence that by its legal nature and application potential is original, not derivative, in one a broader sense of usability in the process of forensic evidence.

The next segment of training is aimed at developing big data search strategies to model the intelligence approach in identifying potentially suspicious habits, as well as visualizing and filtering all objects that are the subject of analysis, which includes text, audio, and video content, people, organizations and other unique identifiers.

In order to develop a search strategy, the following can be singled out as basic parameters or references:

1. specific ways of thinking in the information environment,
2. use of search engines for different observation and understanding of the information environment,
3. use of advanced search tools,
4. the use of operational analytics of prevailing trends, to identify and overcome geographical and linguistic barriers.

Content aquisition

Module: **Black market crawler**

Functionality: Download deep web sites in the dark net (e.g. black markets)

Added value:

- Full court prove documentation of hidden services (including files, pictures and streaming videos)
- Untraceable investigations with improve processing speed

Contribution to ANITA use-cases: Black market content acquisition for ANITA usecases

Content acquisition: Darknet source identification crawler

Input →

Hidden Services Address

Select →

Black Market Crawler

Version 2020-12-01

ADD

Selection

<https://facebookrjf3zolka.onion.ly/>

START CRAWLING

Statistics

Crawled: 169
Not yet crawled: 0

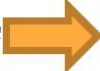
Crawling Results

25 Hits 3djgibyu5osi4na5	⋮
25 Hits onion	⋮
14 Hits google.at	⋮
6 Hits www.orf.at	⋮
4 Hits orf.at	⋮
1 Hits www.google.at	⋮

→

Start crawling and import data set

How to find new and relevant onion links

- **Fast:** Using the  dark net monitor
- **More precise:** Using the source identification crawler

☐ inc. never seen
 ☐ alive only
 ☒ n/a
 ☐ genuine
 ☐ fake
 ☐ show subdomains
 ☐ show fh default
 ☐ search title only
 ☐ match phrase

SFARC: (X) >>>

search for title, email, bitcoin addr or enter "onion" domain for onion info. [G] means genuine, [F] means a fake clone site, comain status is alive, **problems** or **down**, showing 500 of 8910 results: [\[25/48\]](#)

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18

Onion	Title	Added	Visited At	Last Up
uutdujmcu25b5w.onion	[OFFICIAL & ORIGINAL] BITCOIN x200 SERVICE - *2021	5 min	now	now
tdecnrua6e2w42.onion	[OFFICIAL & ORIGINAL] BITCOIN x200 SERVICE - *2021	5 min	now	now
5mcr7et4lwjgw.onion	Amazon Gift Cards	5 min	5 min	5 min
5kj27sdyjspuqkl.onion	Apple Market: Stolen & Carded Merchandise iPhone XS / XS Max iPad Pro MacBook Pro iMac Pro Buy safe with bitcoin Apple	5 min	5 min	5 min
3e7d3k4oqnsj.lqj.onion	Black Shop	23 min	17 min	17 min
vq3gyor3msrqjz7b.onion	[OFFICIAL & ORIGINAL] BITCOIN x200 SERVICE - *2021	23 min	5 min	5 min
aankfrwswux5a4j.onion	Fast Money Accounts & Transfers	23 min	5 min	5 min
vdlhampcncuc3nwh.onion	Scam List of Tor	23 min	3 min	3 min
22leeimddld5as7b.onion	netAuth	33 min	23 min	23 min
qixglvbrcgwrwsvd.onion	Raped Bitch: Real Rape Material	33 min	21 min	21 min
nw5nuxbjmh4gd.onion	Porn Videos - XONIONS	42 min	35 min	35 min
3zcdwnmzeycdcdvd.onion	Default Web Site Page	42 min	23 min	23 min
tubkengdsol45w4r.onion	Horizon Store	55 min	49 min	49 min
nltzabaisvrvah3.onion	Amazon Gift Cards	an hr	an hr	an hr

Content aquisition

Module: **Darknet source identification crawler**

Functionality: Identify possible sources, marketplaces, communication channel across surface web, deep web or dark net

Added value:

- Crawling results are not biased by search engines (no black listing of criminal activities)
- Full court prove documentation (including files, pictures and streaming videos)

Contribution to ANITA use-cases: content acquisition for usecases

Content acquisition: Darknet source identification crawler

Input →

Develop "big data" search strategy

Select →

Source Identification Crawler

Version 2020-12-01

Search Query: "btc:" donate SEARCH

Search Results	
Donate Bitcoin - Give to Help Build Wells and Water Projects https://thewaterproject.org/donate-bitcoin	choose
BTC Foundation https://www.btc.edu/AboutBTC/BTCFoundation/Index.html	choose
Donate to WikiLeaks https://wikileaks.org/donate	choose
BTC Bank Employees Donate \$14500.00 to their Local Communities https://btcbank.bank/.../btc-bank-employees-donate-14-500-00-to-their-local-communities	choose
Donate Bitcoin https://hrf.org/donate-bitcoin/	choose
BTC Area Youth Benefit Corp. and BTC Bank Donate to bring Retro ... https://btcbank.bank/btc-area-youth-benefit-corp--and-btc-bank-donate-to-bring-retro-bill-to-cooper-county	choose

Start crawling and import data set →

Statistics START CRAWLING

Overall results: 823

Results per file type: N/A

Crawling Results

823 Hits http

823 Hits silkroadxjzvoyxh.onion

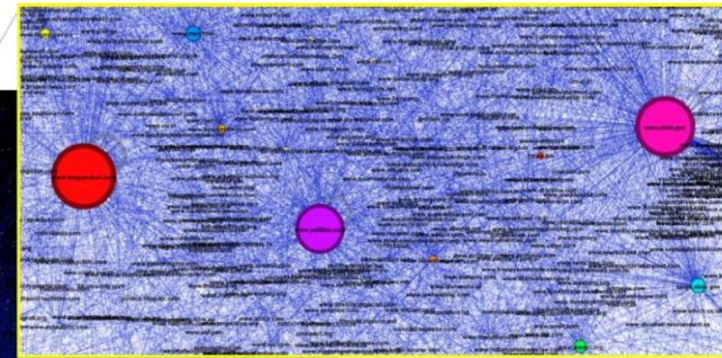
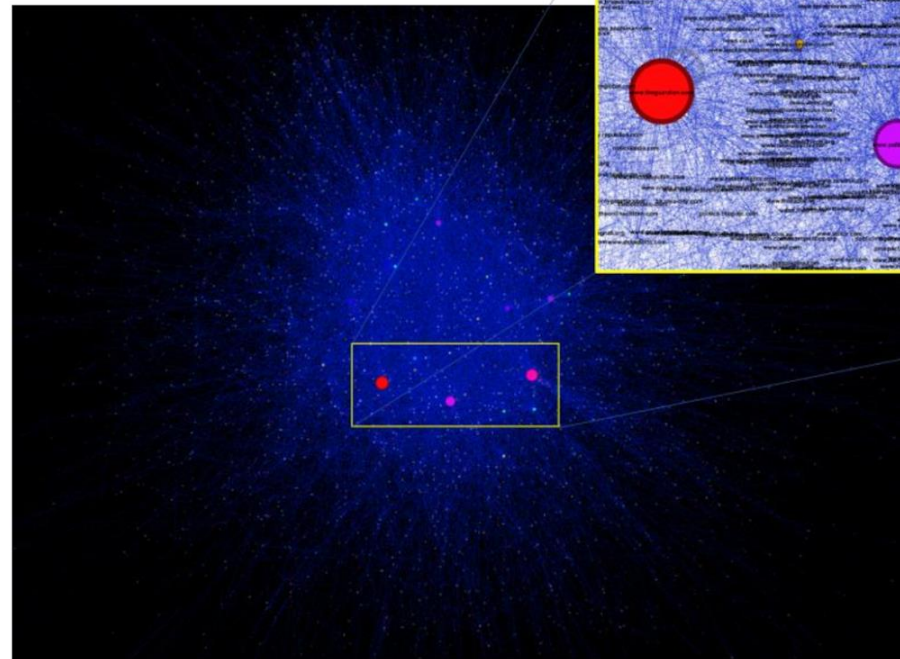
Content acquisition: Results

Intelligence
approach to identify
suspect patterns

Visualisations and
filter of all
knowledge objects,
including:

- Text, Audio Video
- Persons
- Organisations
- Other unique identifiers

Qanon source network

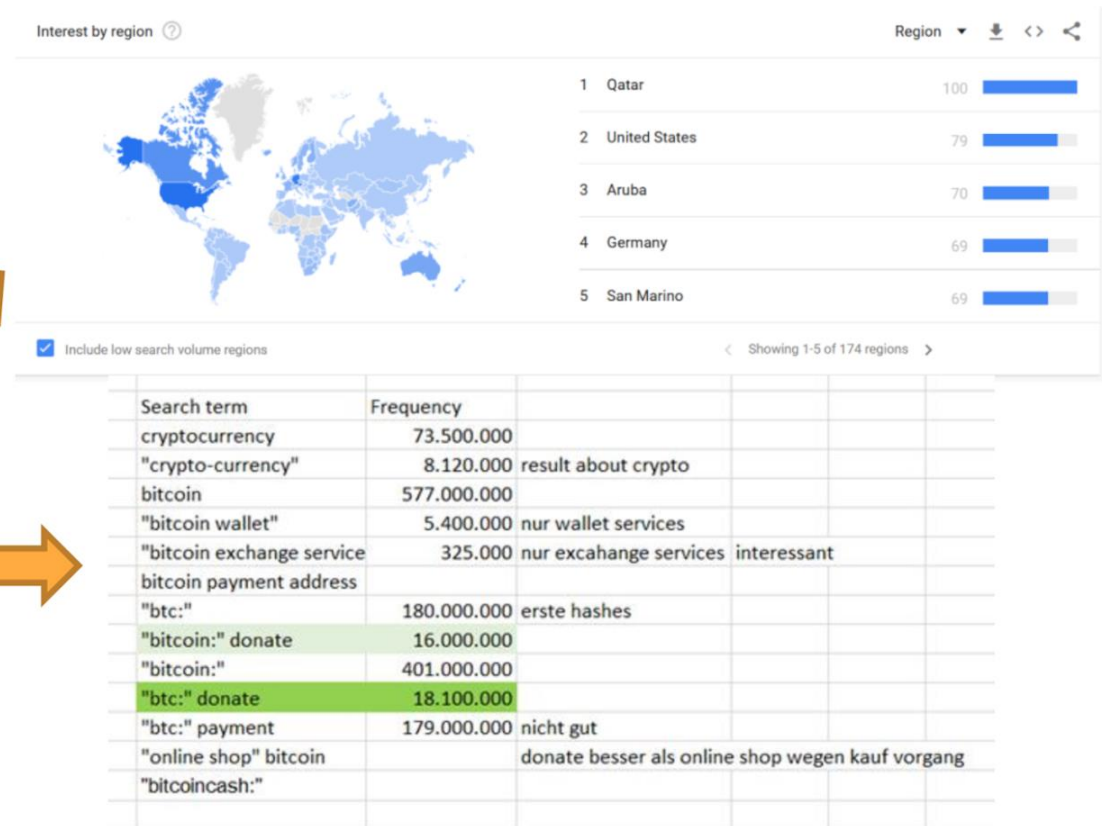


Browsing and filtering



How to develop a crawling strategy

- Think in “information spaces”
- Use Google, Yandex and Baidu for different views on the information spaces
- Use advanced search attributes
- Use “trend analytics” to identify language borders and correlating geographic barriers
- Use search statistics
- **Use the best possible unique search strategy**



3. CASE STUDIES

by Valentina Scioneri

The material under the working title establishing the interdependence between narcotics and drugs, weapons and firearms presents the content of criminological analysis, drug, and arms trafficking, which aims to clarify the connection and impact of criminal activities on the Dark web markets, the term criminal offense as a service, within which the hypothesis of the potential relationship of this type of crime with organized crime is confirmed.

The characteristics of the human factor as a supplier are determined, through data on nicknames, behind which can be found a whole group of people, acting around the world to meet the needs of consumers, types of offered and sold goods or services, number of listings, listing content, as and the country of origin and destination of the goods or services.

The conclusion is that continuous brainstorming with partners is a key component of efficiency, and testing the quality and scope of the analyzed and presented approach is enabled through the platform.



ANITA USE CASES

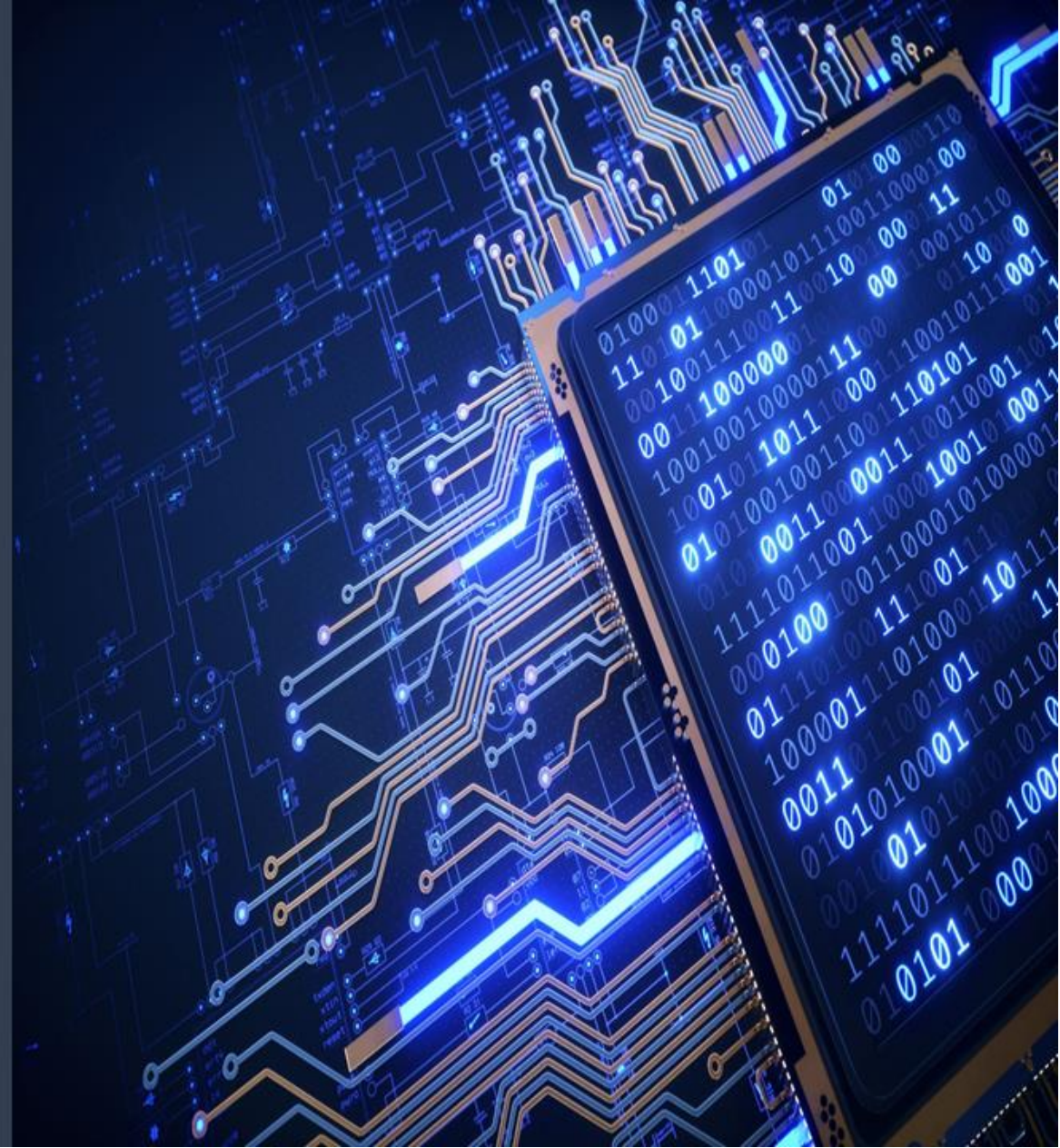
HORIZONTAL SCENARIOS

A case study of interdependencies between:

01. DRUGS, NPS AND MEDICINES

02. WEAPONS AND FIREARMS

in the Dark web



Criminological approach



01

Drugs / Weapons trafficking

Assessing the intersections of criminal activities in the Dark web markets

02

Vendors

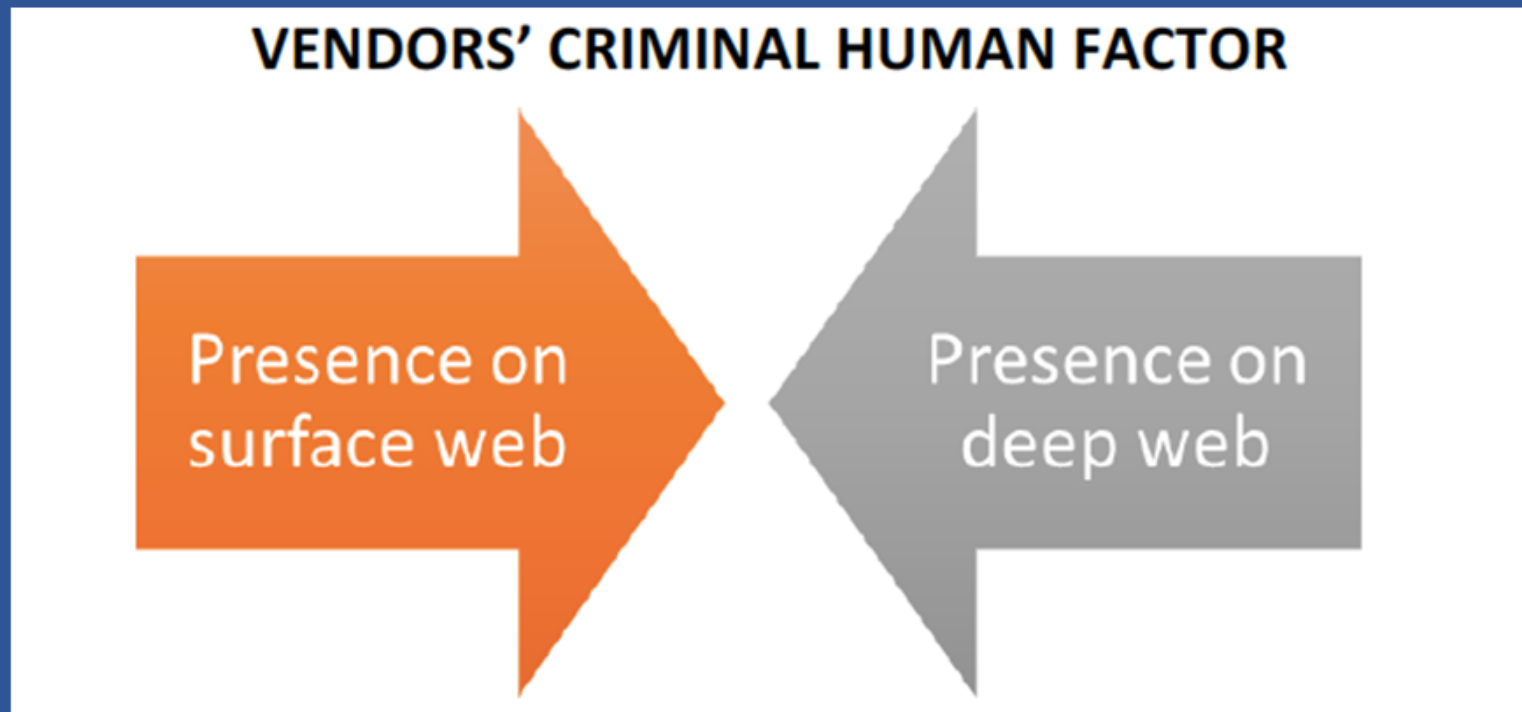
Understanding their modus operandi

03

Crime-as-a-service

Exploring the hypothesis of customized crime VS organized criminal network

INVESTIGATE INTERDEPENDENCIES BETWEEN:



QUALITATIVE EXERCISE AIMED AT CROSSCHECKING DIFFERENT SOURCES TO EXTRAPOLATE RELEVANT INFORMATION ON THE HUMAN FACTORS OF WEAPONS' AND DRUGS' SELLERS OPERATING ON THE DARKWEB, AND POSSIBLE RELATIONS TO OTHER ILLICIT TRAFFICKING



Information assessed

- Vendors' nicknames
- Categories of products sold
- N° of listings
- Listings' contents
- Origin/Destination countries



4 vendors identified
apparently selling
both drugs and
weapons on the
same or on different
markets

Case study - vendor 1



Pistols
Ammunitions
Long-range gun

Benzodiazepines
Opioids
Psychedelic/
dissociative hallucinogens
Stimulants

- 01 **Digital trafficking routes:**
DRUGS – origin: unspecified / destination: worldwide
WEAPONS – origin: worldwide / destination: China – USA
- 02 **Products/Listings:**
Limited n° of drug listings (35) and variety of substances sold → promotion on market to gain visibility (peculiarity of Tochka: Dark net community offering services)
On Berlusconi market, vendor 1 is apparently selling also counterfeit money
- 03 **Modus operandi:**
Presence on several markets and wide portfolio of products offered

behind the nickname there might be a network of people engaged in different criminal activities, operating worldwide and meeting different customers' needs

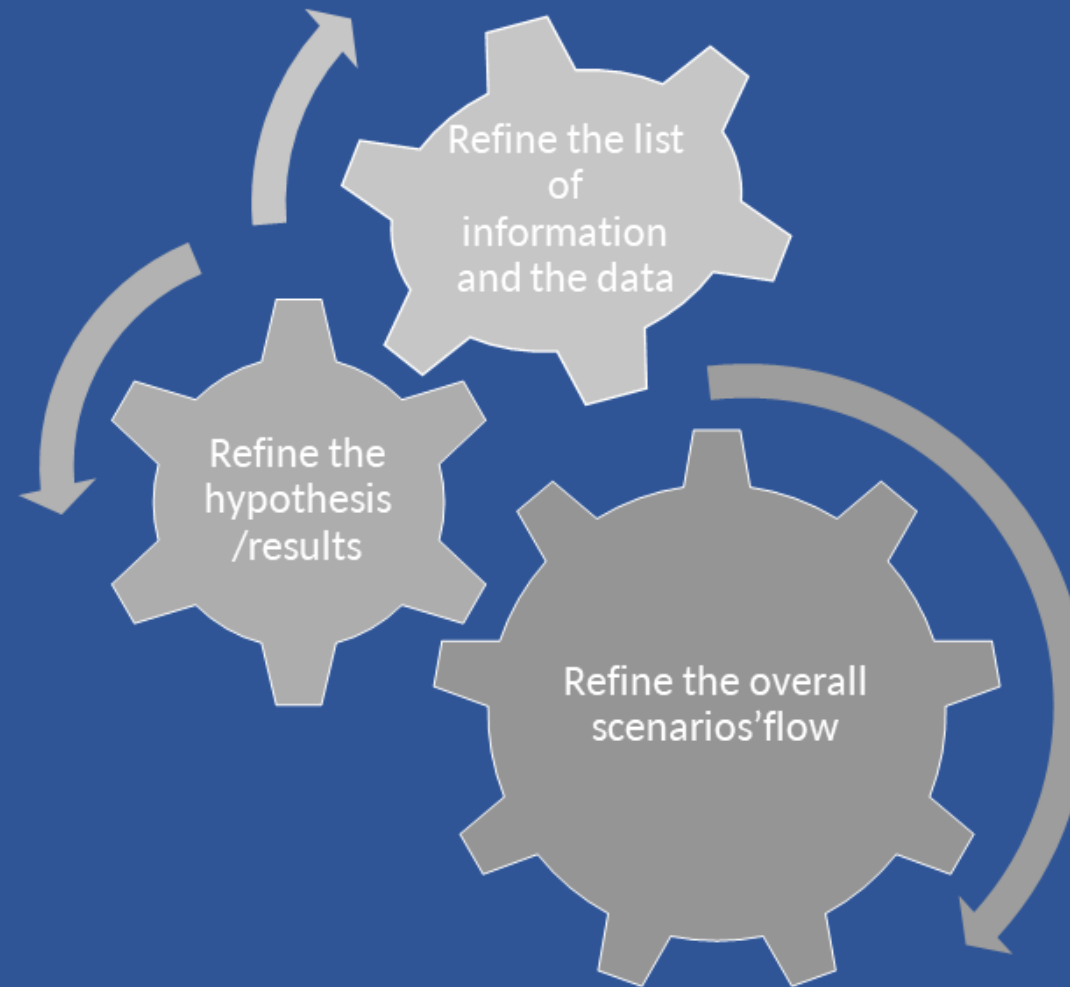
the exercise showed how cross-checking information on vendors both on the dark web and surface web may provide

Information on their identities

Information on their illicit activities

In conjunction with verifications on additional elements, this approach is intended to support investigators not only in following each vendor's activities or money flows, but also assessing networks of connected actors.

Next steps: to continue brainstorm with partners and test the approach through the use of the integrated platform



4. SIMULATED EXAMPLE OF AN HORIZONTAL SCENARIO

by RISCC

A presentation called “Simulated example of a horizontal scenario” describes a situation in which a narcotics supplier is active on both the Surface Web and the Dark Web Cryptomarket.

The focus is on understanding and collecting data, which has probative value in relation to his criminal activities, through the support of the Anita platform, which provides insight into both the surveillance process and the evidentiary process.

The added value is reflected in the so-called capacity to connect key concepts and points, to reduce and experiment with different paths, and to confirm different hypotheses.

Description of the analysed case: the national law enforcement service arrested a person named Jim, suspected of drug trafficking.

E-mail correspondence with a supplier called soniabrito44, which is active in the Agarthia market, was found on his computer.

Inspectors want to gather information and possible evidence about this supplier, to better understand and later prove his role in the commission of the crime, as well as the manner of its commission.

In the presentation:

1. Step 1 -open an investigation
2. Step 2 - uploading documents,

3. Step 3 - automatic data analysis and finally highlighting the human factor in accessing and confirming the process of automated data collection and learning, because Anita system is a knowledge-oriented and high-quality database, whose development depends on the interaction between user contributions and system capacity.
4. Step 4 involves entering new data
5. Step 5 - Advanced automation analysis of the same.
6. Step 6 involves access to new entries in the system, followed by
7. Step 7 relating to further research
8. Step 8 refers to the use of blockchain data.
9. Step 9, should imply progress in thinking and reasoning, which is called thinking "outside the box".

This use case is a simulated example of an **horizontal scenario** where a **drug vendor** is active both in a **Dark web cryptomarket** and on the **Surface web**

Understanding and collecting information/evidence about his activities - 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, to experiment different paths of analysis and validate diverse hypothesis

Use case description

a national LEA has just arrested a person – “Jim” - suspected of buying drugs online. In his pc, the e-mails exchanged with a vendor [soniabruto44] were found. This vendor is active on **Agartha market**

The investigator wants to gather more information – and possibly evidence – about this vendor, so to better assess his role and modus operandi

STEP 1 – opening of the investigation

The image illustrates the first step of opening an investigation in a system. It shows a multi-step process for creating a new investigation:

- Step 1: General Info** - The user enters details such as ID (12345), Title (Horizontal scenario), Category (drug), and Description (Horizontal scenario). A red arrow points from the 'Next >' button to the next step.
- Step 2: Add Investigators** - The user adds investigators to the investigation. A red arrow points from the 'Next >' button to the next step.
- Step 3: Upload Resources** - The user uploads resources to the investigation. A red arrow points from the 'Next >' button to the next step.

The final view shows the 'Horizontal scenario' investigation detail, displaying a graph with nodes and edges. The nodes are 'Jim Stephenson' and '0bdc5929-3d2d-417...'. The edge is labeled 'isExtracted'.

DOWNLOADED PAGES

VENDORS

PRODUCTS

VENDORS

VENDOR INFO

Name

williamsharry464

Walgreens

USA_PUSHER

USA_PLUG

Threebeard12

swizzbeats

soniabrto44

sixxzeros

Agartha is monitored by ANITA. The vendor is available in the list

LISTINGS:★ The

t but the quality is

method, please indicate

contact us before you

d/solution.There is

imals. ★ When should

days

worldwide...Please provide me your address this way:★ FIRST AND

LAST NAME★ ADDRESS + STREET★ POSTAL ZIP CODE + CITY★

COUNTRY (DON'T FORGET THIS ONE)*DOWNLOAD THE APP

WICKR AND ADD US ASAP FOR FAST CONVERSATION.Wickr....

harrysalesRefunds:50% RESHIP for non arrival if you make a new

order of the same amount.This way you get what you paid for and

we can compromise our lost with the profit of the new order.

FEEDBACK (VENDOR SELECTED)

message	deals	score	user	date
100% legit vendor.Very honest guy.	0	5 of 5	b****e	172800.0
Thank you so much bro. You are the best.I recommend Admins to place vendors like you on a ranking bar based on buyers recommendation.	1 - 10 deals	5 of 5	s****l	1555200.0
The best so far that i have ever seen on the darknet. Buy from them with 100% assurance.	1 - 10 deals	5 of 5	s****l	1555200.0
Trusted vendor.Deal with him without any doubt.	1 - 10 deals	5 of 5	s****l	1468800.0
Order from there and you will enjoy fast delivery. Thank you guys so much.	1 - 10 deals	5 of 5	s****l	1468800.0
Very reliable. Thank you so much.	1 - 10 deals	5 of 5	s****l	1382400.0

STEP 2 – upload of documents

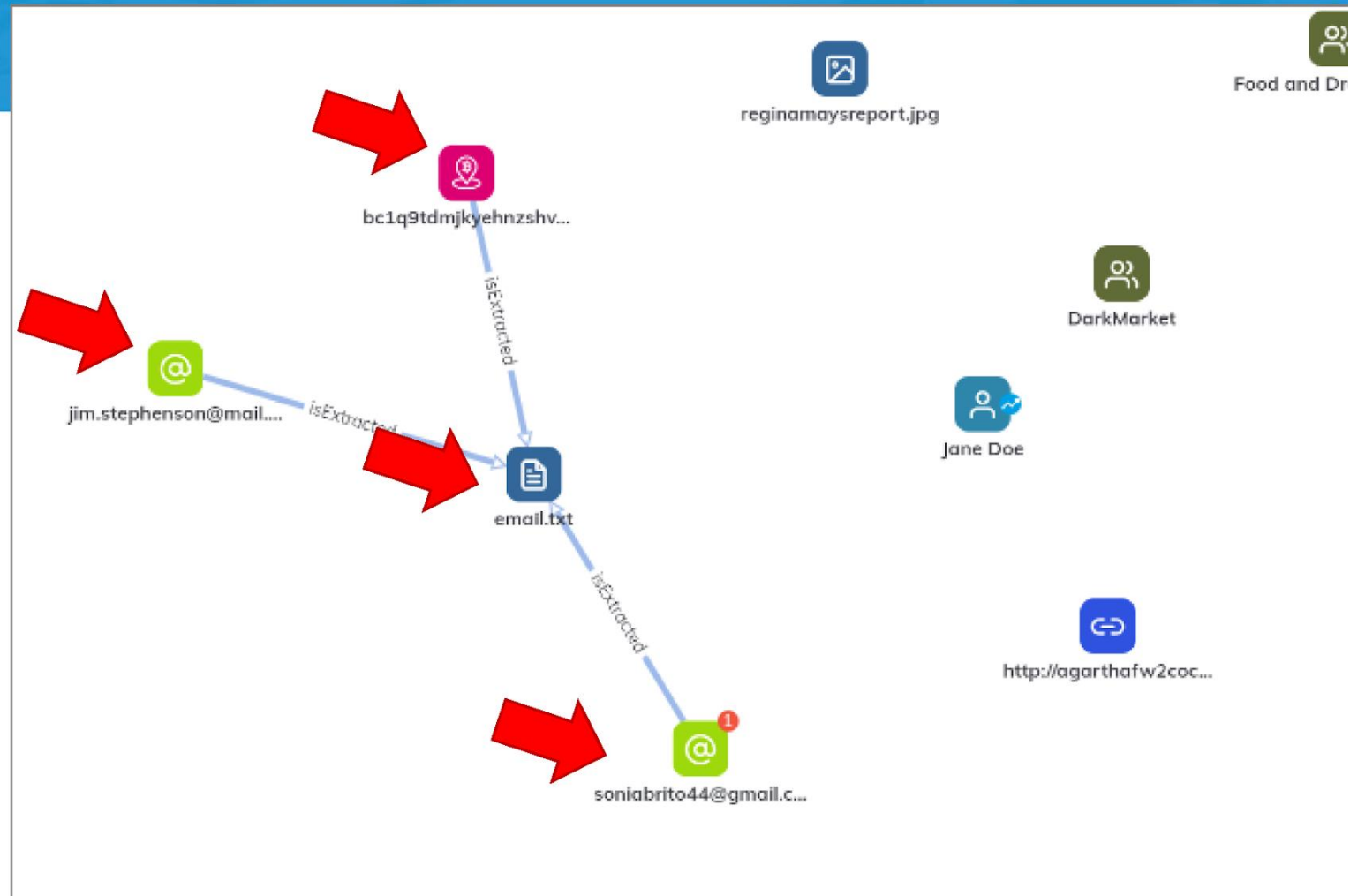
A text file containing one of the e-mails retrieved in the pc is uploaded into the platform

The screenshot illustrates the process of uploading a document to the onit platform. It is divided into three main sections:

- Top Section:** Shows the 'Investigation Title' header and a sidebar menu. The 'Resources' option is highlighted with a red box, and a red arrow points from it towards the upload dialog.
- Bottom-Left Section:** Displays the 'Import File into Investigation' dialog box. It shows a file named 'email.txt' with a size of 1.57 KB and a status of 'pending'. A green progress bar is visible, and an 'Upload' button is at the bottom.
- Bottom-Right Section:** Shows the main investigation interface. A red box highlights the 'email.txt' file icon, which has been successfully uploaded. Other icons for 'reginamaysreport.jpg', 'http://agarthafw2coc...', 'Brigham', and 'DarkMarket' are also visible.

STEP 3 – automatic analysis

ANITA extracts the entities and inserts them into the graph (together with the relationships that link them to the textual resource from which they were extracted)



STEP 3 – automatic analysis

Entities extracted:

1. e-mail address (of the arrested person)
2. Crypto address

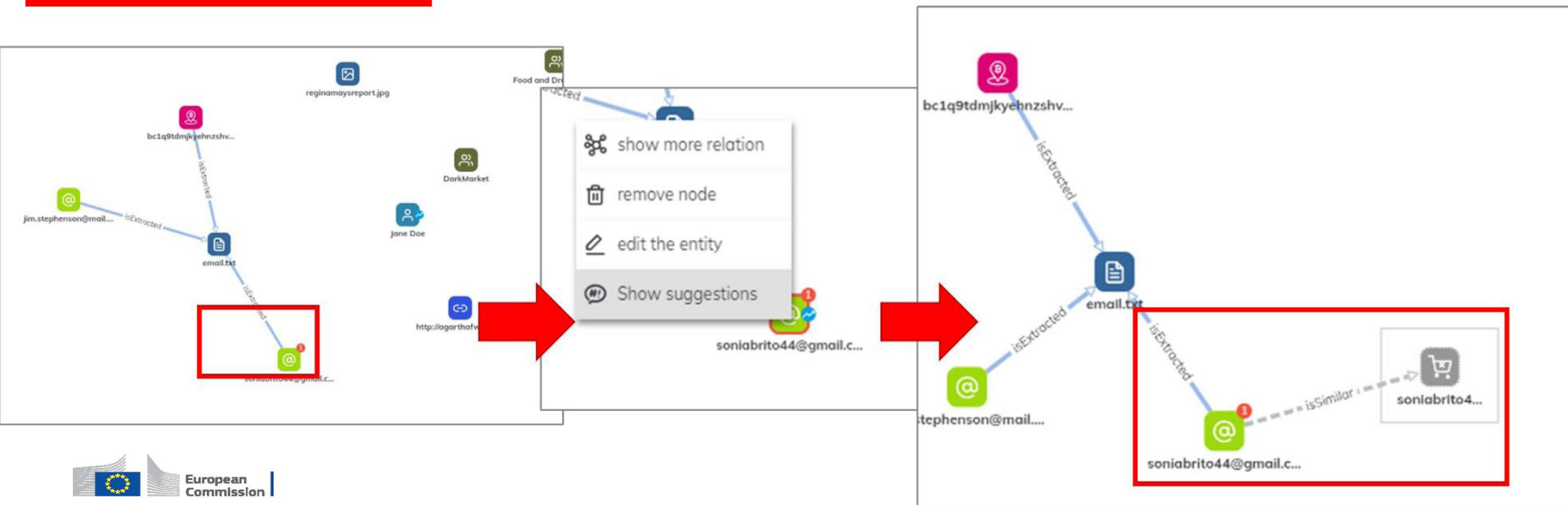


The mechanisms that operate in the background for the discovery of hidden relationships find that the e-mail address "soniabrito44@gmail.com" is very similar to one of the vendors previously extracted from the Agarth market

Consequently, the suggestion of the alleged relationship is proposed to the user in the form of a red badge

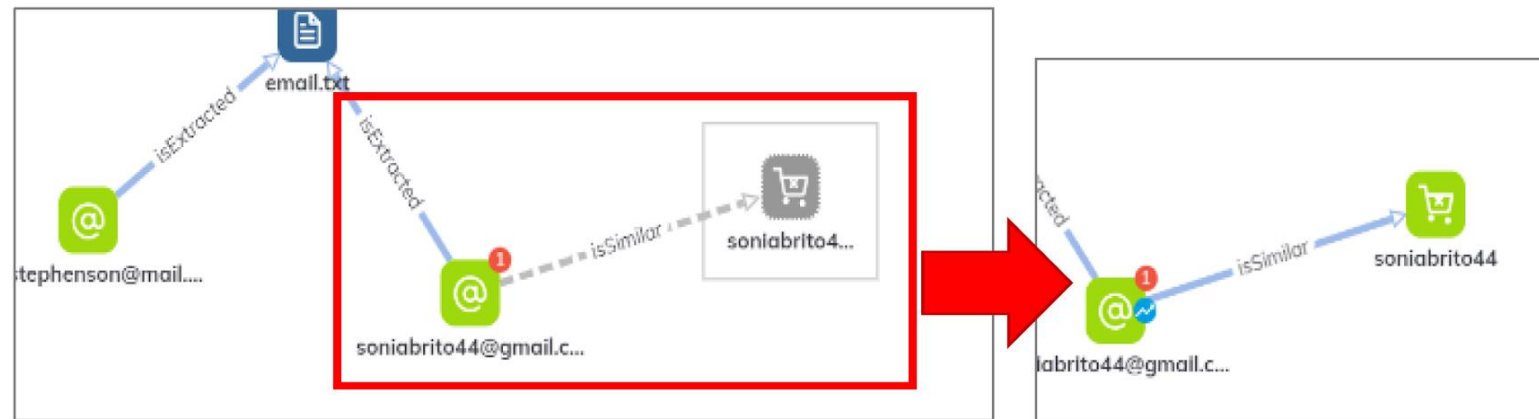


the user can then
expand the
relationships and
explore the
suggestion



Key role of the “human factor” in assessing and validating the automatic learning process

IF the user accepts the suggestion, the suggestion becomes knowledge that is part of the investigative graph



Key role of the “human factor” in assessing and validating the learning process

The inclusion in the graph allows the mechanisms in the background to find further information



Key role of the “human factor” in assessing and validating the learning process

SO, in our case, ANITA finds pages in the Agarthia market where the vendor is also present



The ANITA system is **knowledge centered** and the quality level of the knowledge base developed depends on the continuous interaction between the user's contribution and the system capacities

STEP 4 – adding new details ...

The investigator knows that the person arrested bought fentanyl from the vendor

This information is added into ANITA

Create or edit a Object Entity

Entity Type: Product

Product Name: Fentanyl

Category: Narcotic

Save

Create or edit a Event

Name: Buying Fentanyl

Description: Event with category Purchasing

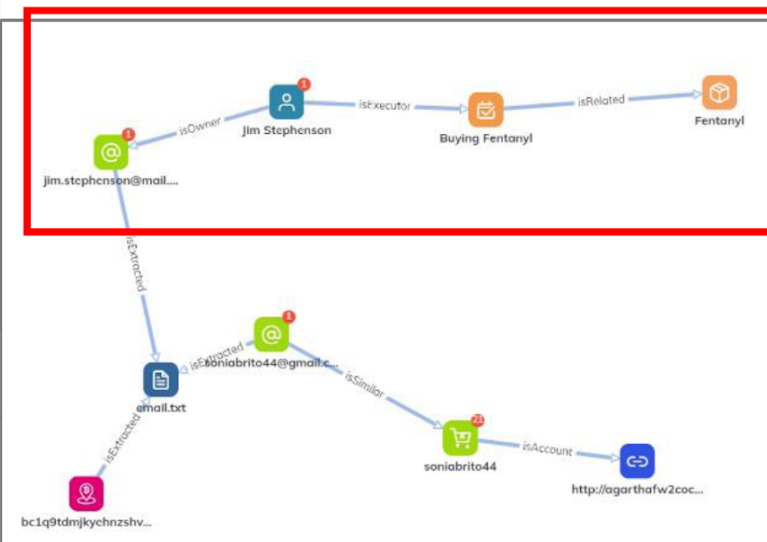
Range Date: [] []

Location: search by location

Categories: category

Purchasing x

Save

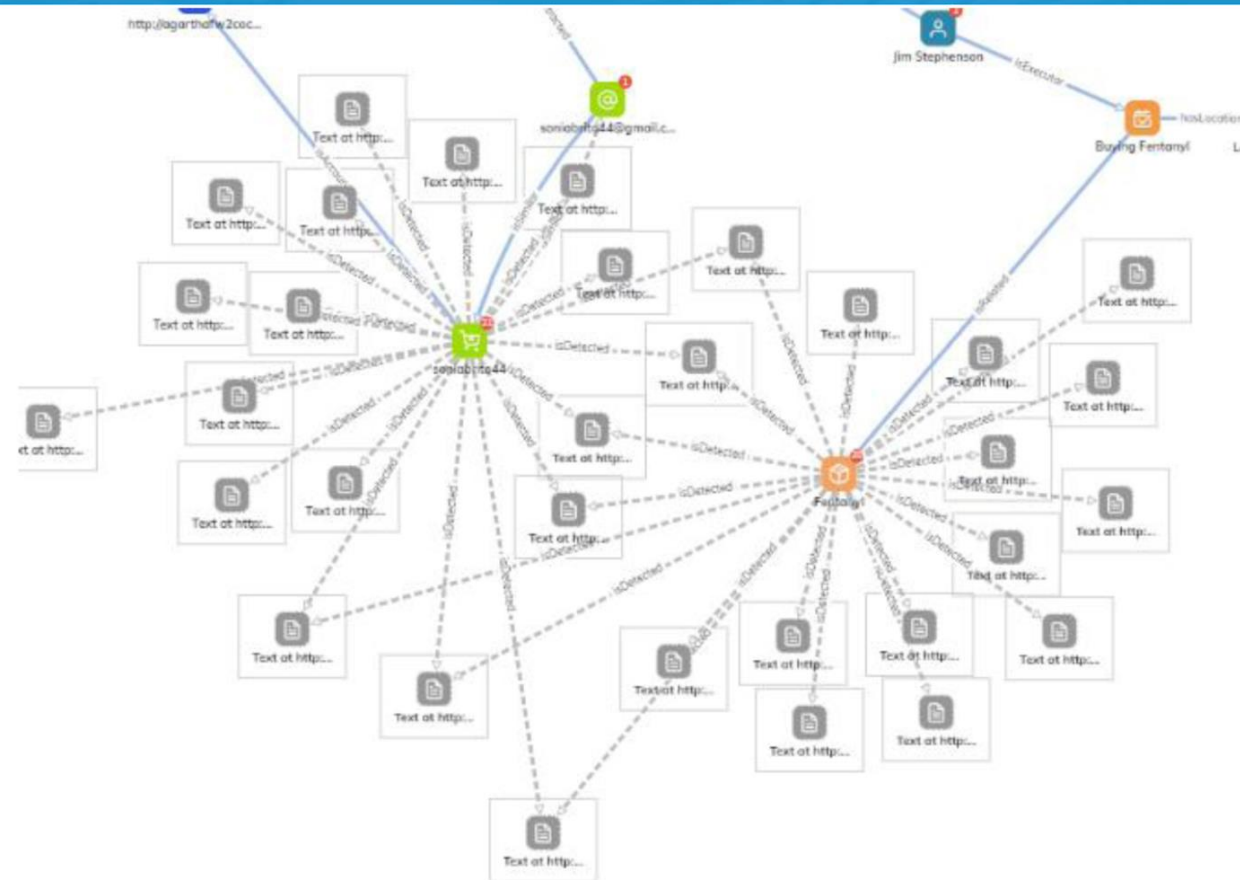


STEP 5 – improved automatic analysis

**ANITA in the background
discovers new relationships
and proposes them to the
user**

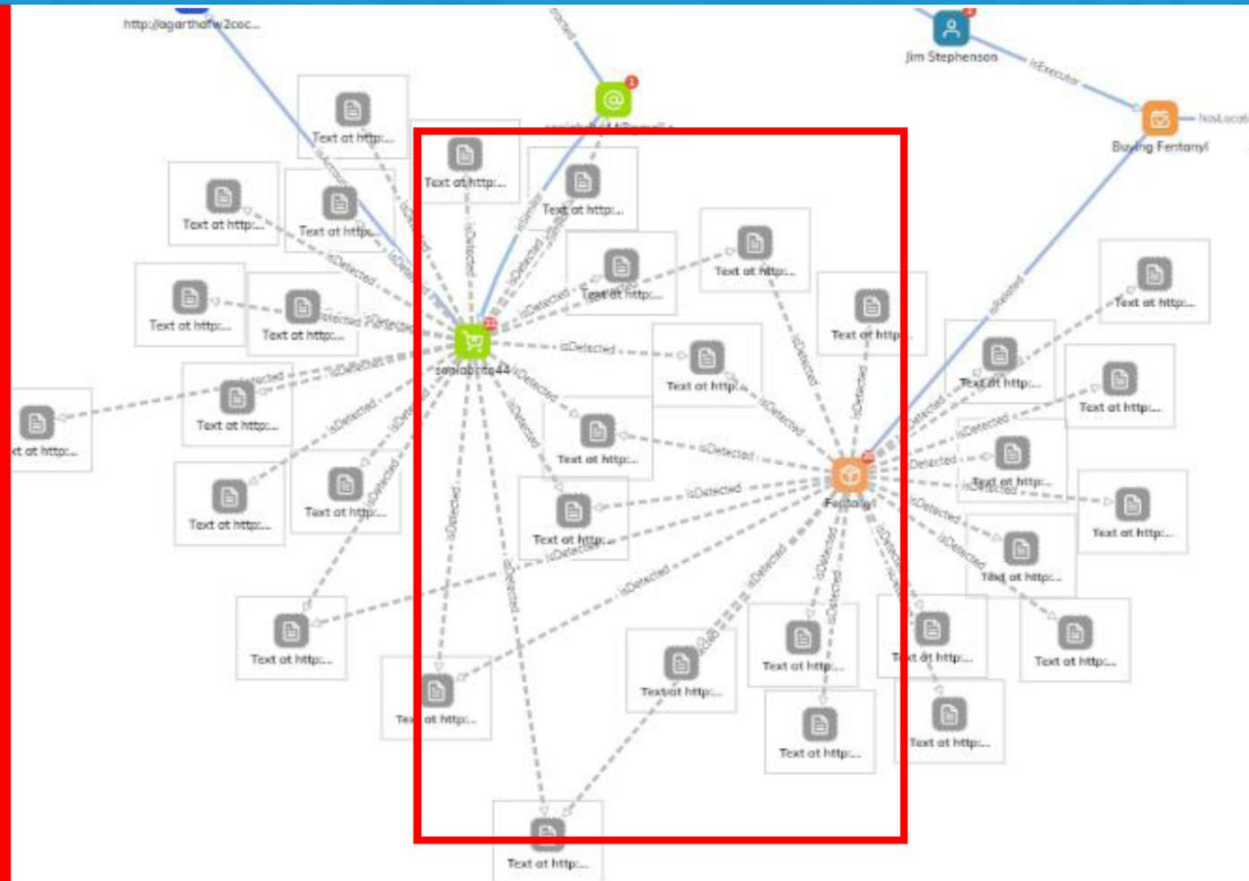
STEP 5 – improved automatic analysis

In our case,
fentanyl is present
on Agarth



STEP 6 – assessing new inputs from the system

The officer can decide to cross-check this suggestion with the information retrieved for the vendor under investigation (soniabritto44)

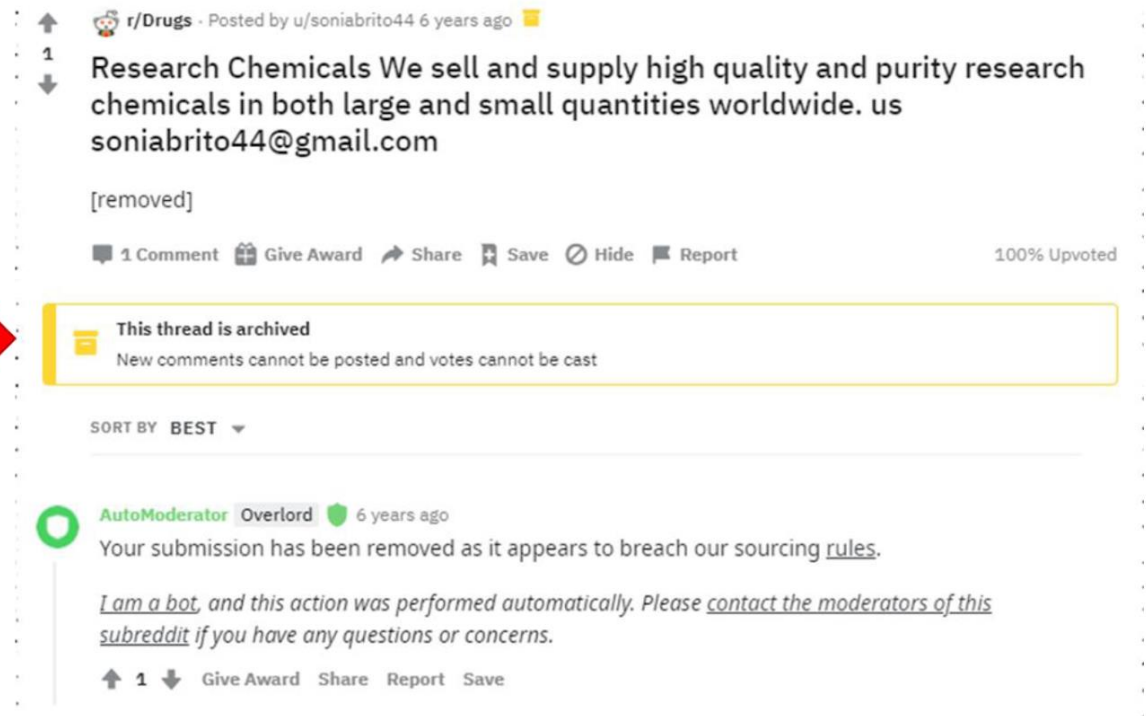
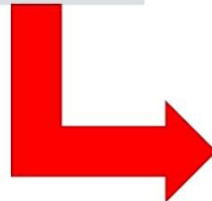


INPUT
soniabritto44
could be
actually
involved in the
sale of fentanyl

STEP 7 – additional research / 1

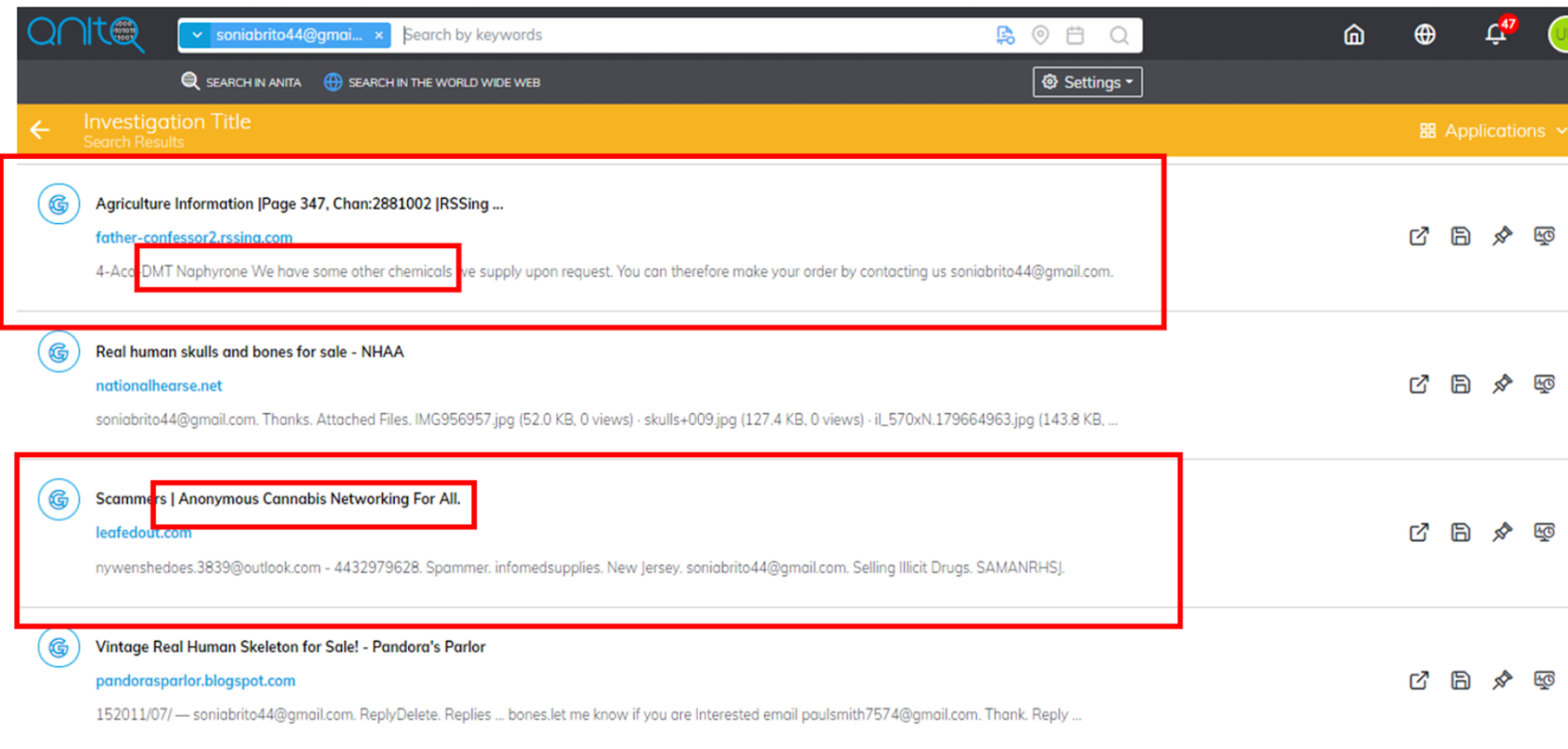


By conducting an online search, the investigator discovers that the “soniabrito44” account is present on REDDIT, also confirming ownership of the soniabrito44@gmail.com email address



STEP 7 – additional research / 2

In addition, looking for the e-mail address soniabrito44@gmail.com online, the investigator discovers some suspicious web pages



The screenshot shows the Anito search interface with the following results:

- Investigation Title** Search Results
- Agriculture Information** [Page 347, Chan:2881002] RSSing ...
[father-confessor2.rssing.com](#)
 4-Aceto DMT Naphyrone We have some other chemicals we supply upon request. You can therefore make your order by contacting us soniabrito44@gmail.com.
- Real human skulls and bones for sale - NHAA**
[nationalhearse.net](#)
 soniabrito44@gmail.com. Thanks. Attached Files. IMG956957.jpg (52.0 KB, 0 views) · skulls+009.jpg (127.4 KB, 0 views) · il_570xN.179664963.jpg (143.8 KB, ...)
- Scammers | Anonymous Cannabis Networking For All.**
[leafedout.com](#)
 nywenshedoes.3839@outlook.com - 4432979628. Spammer. infomedsupplies. New Jersey. soniabrito44@gmail.com. Selling Illicit Drugs. SAMANRHSJ.
- Vintage Real Human Skeleton for Sale! - Pandora's Parlor**
[pandorasparlor.blogspot.com](#)
 152011/07/ — soniabrito44@gmail.com. ReplyDelete. Replies ... bones.let me know if you are Interested email paulsmith7574@gmail.com. Thank. Reply ...

Options for the investigator, who can:

1. keep the resource found in the investigative graph
2. keep the web source(s) for later monitoring
3. start monitoring it immediately

Investigation Title
Search Results

Agriculture Information (Page 347, Chan2881002 [RSSing ...]
father-confessor2rssing.com
4-Aco-DMT Naphyrone We have some other chemicals we supply upon request. You can therefore make your order by contacting us sonibrito44@gmail.com.

Real human skulls and bones for sale - NHAA
nationalhvarse.net
sonibrito44@gmail.com. Thanks. Attached Files: IMG956957.jpg (52.0 KB, 0 views) skulls+009.jpg (127.4 KB, 0 views) -iL570xN179664963.jpg (143.8 KB, ...)

Scammers | Anonymous Cannabis Networking For All.
leafedout.com
nywenshedoes.3839@outlook.com - 4432979628. Spammer. infomedsupplies. New Jersey. sonibrito44@gmail.com. Selling illicit Drugs. SAMANR+GJ.

Vintage Real Human Skeleton for Sale! - Pandora's Parlor
pandorasparlor.blogspot.com
152011/07 --- sonibrito44@gmail.com. ReplyDelete. Replies ... bones let me know if you are interested email paulsmith7574@gmail.com. Thank. Reply ...

leafedout.com/scammers?page=653

HOME ABOUT ADVERTISE NEWS JOBS Sign Up For Free

The Scammers List

Be careful of any request to send payment in advance via Gift Cards, Paypal, Zelle, Bitcoins, MoneyGram, Western Union and in overseas money request and check the Vendor and Consumer Reviews and information such as time the profile has been active. Vendors with contact information on their profiles are possible scammers. Avoid them!
(If you want to dispute you being on this page please email support@leafedout.com)

Search Search Add New Scammer

Showing 9781 - 9795 of 10216

Scammer Alias	Region	Known Contact Info
michealobi	-	regan8263@gmail.com - 12092601968
linkinsama	Multiple Locations	linkinsama@outlook.com - 8622315992
USplug22	Fresno, CA	riccharles46@gmail.com - 12092601968
temuxoty	New york	ez772@boun.cr - 3159495476
getproperde	-	nywenshedoes.3839@outlook.com - 4432979628
infomedsupplies	New Jersey	sonibrito44@gmail.com

Example – how to keep the resource found in the investigative graph

In this case, the investigator keeps the resource found in the investigative graph. Additional email addresses are found by analyzing the resource and are added to the graph.

Horizontal scenario
Search Results

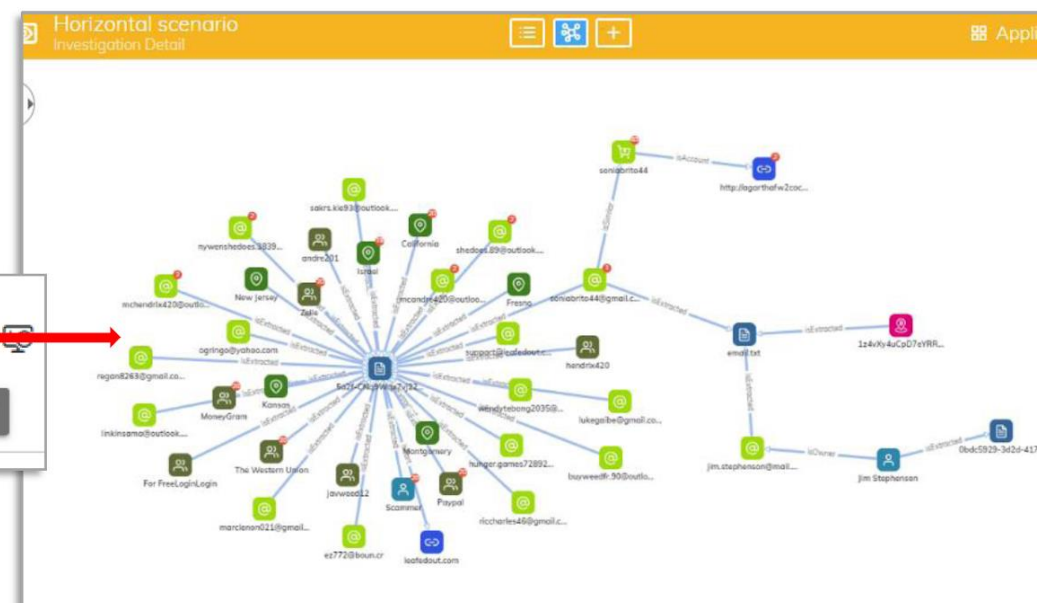
78567177 sonibrito44@gmail.com

Skulls and Bones
skullandbone.tumblr.com
102018/01/ — If you are interested, you can contact her at this mail address: sonibrito44@gmail.com. I'm sure she is available to ask all of your request and ...

Scammers | Anonymous Cannabis Networking For All.
leafedout.com
nywenshede3839@outlook.com - 4432979628. Spammer, informedsupplies. New Jersey sonibrito44@gmail.com, selling illicit Drugs. SAMANRHS).

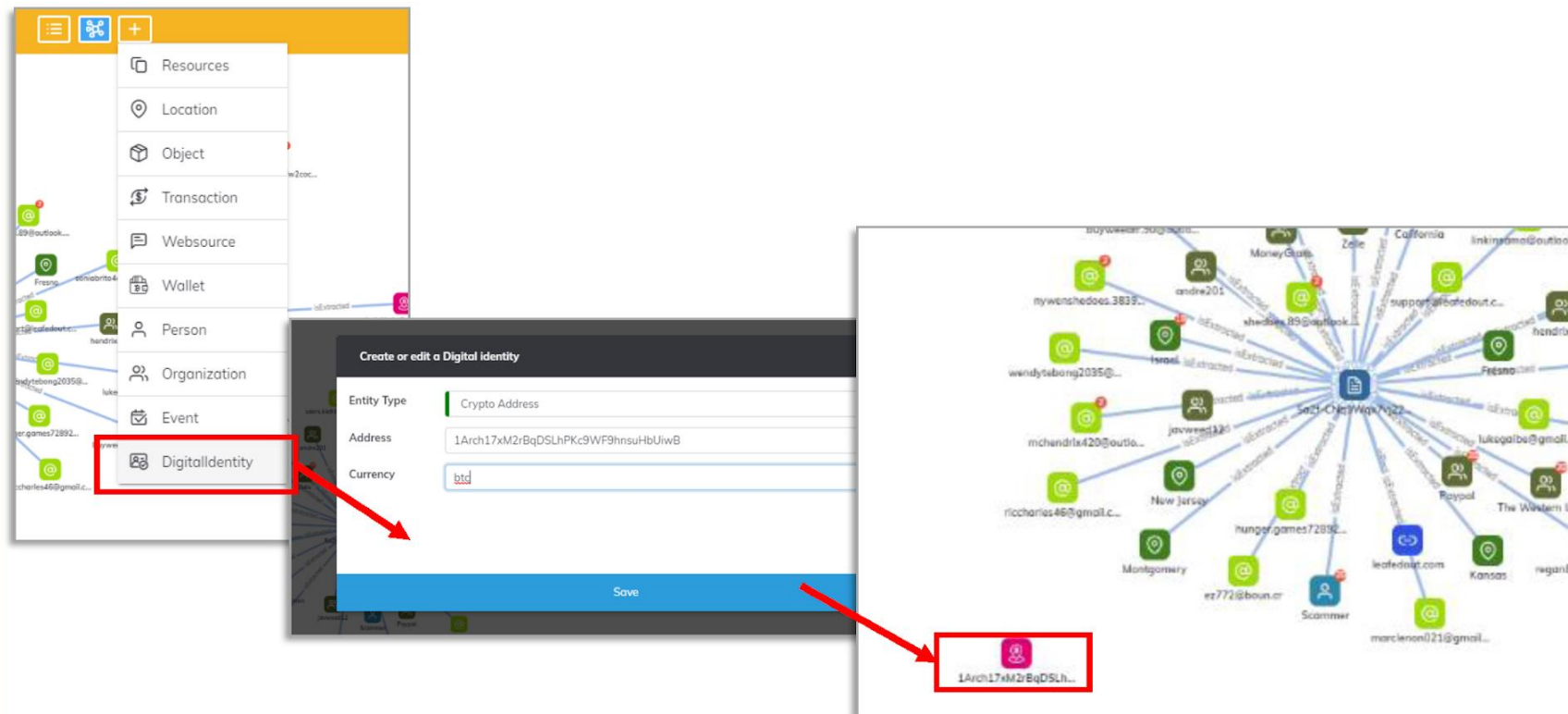
Best Christmas Present Ever - Chris Rahn
chrisrahnart.blogspot.com
sonibrito44@gmail.com. Reply ... zockdekenzo@gmail.com. I'm sure she is ... bones.let me know if you are Interested email hellershari@gmail.com. Thank.

Source is Downloaded



STEP 8 – exploiting information from the blockchain / 1

Since the police can get access to the seized pc, information about cryptoaddress **1Arch17xM2rBqDSLhPKc9WF9hnsuHbUiwB** used by Jim can be added to the graph



STEP 8 – exploiting information from the blockchain / 2

Information of a cryptoaddress can be navigated within the blockchain

Selected item info

Name
1Arch17xM2rBqDSLhPKc9WF9hnsuHbUiwB

Description
1Arch17xM2rBqDSLhPKc9WF9hnsuHbUiwB

Type

1Arch17xM2rBqDSLhPKc9WF9hnsuHbUiwB
Cryptoaddress Detail

TRANSACTIONS	TAGS	RECEIVED	SENT
Hash value	Executed on	Amount	
73b774772737f61f6d90535713f68039...	Jan 2, 2018, 4:58:14 PM	-0.20102028 BTC	+
0e889d017cc74d11613e0b3c6a642c0...	Dec 22, 2017, 8:21:21 PM	0.20102028 BTC	+
79e9609dad138ea34585fb27b9eafd0...	Oct 16, 2016, 9:28:06 PM	-0.73817486 BTC	+
55dcd93433d383f91e6b91bffe7435ba...	Jun 28, 2016, 11:43:54 PM	0.0098 BTC	+
78c2fe77f431d0c936b3a3e76f6c65ecb...	Jun 28, 2016, 11:43:54 PM	0.0045232 BTC	+
1c8feadb9911e33903d116872353fc2...	Jun 14, 2016, 9:32:29 PM	-0.22763201 BTC	+
276abd22637717d9055dc599c158693...	Jan 19, 2016, 12:01:29 AM	-0.00527612 BTC	+
5c75dc95b7d281f4bd20f361ccc5b830...	Jan 12, 2016, 2:28:13 PM	0.02403886 BTC	+
8f6ebf6430406609c8b149466c30a083...	Jan 12, 2016, 12:25:39 PM	-0.0801 BTC	+

Last Usage
Jan 2, 2018, 4:58:14 PM

Total Received
2.05512784 BTC

Total Spent
2.05512784 BTC

Final Balance
0 BTC

STEP 8 – exploiting information from the blockchain / 3

In this case, a transaction is found and it is possible to have input and output addresses already present in the investigation graph

1Arch17xM2rBqDSLhPKc9WF9hnsuHbUiwB Cryptaddress Detail			
TRANSACTIONS		TAGS	RECEIVED SENT
Hash value	Executed on		Amount
73b774772737f61f6d90535713f68039...	Jan 2, 2018, 4:58:14 PM		-0.20102028 BTC

73b774772737f61f6d90535713f68039b085... Transaction Detail		Applications	+
INPUTS		TRANSACTION	
Address	Value		
1Arch17xM2rBqDSLhPKc9WF9hnsuHbUiwB	0.20102028 BTC	✓	

73b774772737f61f6d90535713f68039b085... Transaction Detail		Applications	+
INPUTS		TRANSACTION	
Address	Value		
18DwZtUcusYVH5Ly3sdPxfvuZVCn6TdEB	0.20012566 BTC	✓	

STEP 8 – exploiting information from the blockchain / 3

The investigator can decide to import the transaction in the investigation graph

The screenshot displays the Onit application interface. At the top, a transaction detail view for ID 73b774772737f61f6d90535713f68039b085... is shown. It includes a table with the following data:

Address	Value
18Dw2tUcusYVH5Ly3sdPxfuZiVn6TdEB	0.20012566 BTC

A red box highlights a '+' icon in the top right corner of the transaction detail view. Below this, a modal dialog asks: "Are you sure you want to add this transaction to your investigation?". A red arrow points from the '+' icon to this dialog. The dialog has a green "Yes" button, which is also highlighted with a red box. A red arrow points from the "Yes" button to the investigation graph below. The graph, titled "Horizontal scenario Investigation Detail", shows a complex network of nodes and edges. A red box highlights a specific node in the graph, which is connected to the transaction ID 73b774772737f61f6d90535713f68039b085....












STEP 9 – thinking “out of the boxes”








For example, for the same account under investigation, the investigator could also:

1. assess the inputs of ANITA about *Glocks*, thus checking if the same account is involved not only in drug trafficking but also in firearms trafficking
2. further explore the inputs of ANITA about the crypto address retrieved in the e-mail already uploaded
3. search for additional information about email addresses found online in the same web page containing the suspected email address, to discover if there is a criminal network behind this illicit activity

5. ANITA GRAPH ENTITY LEGEND

It essentially represents the legend of the symbols used on the platform, to denote different entities.

Symbol	Entity	Description
	Audio	Audio resource
	Image	Image resource
	Text	Text resource
	Video	Video resource
	Location	Location with information about address and coordinates
	Product	Generic object of interest for the investigation
	Vehicle	For transporting people and/or goods
	PC	Object of interest involved in activities
	Smartphone	Object of interest involved in activities
	Transaction	A financial transaction involving crypto currency exchange (like bitcoins) between two or more crypto addresses
	Web source	URL of a generic web site (like markets, forums, etc.)
	Wallet	Digital wallet that can contain one or more crypto addresses
	Person	Set of information representing people
	Organization	Set of information representing organizations
	Event	Set of information representing an event
	Email account	Type of digital identity

	Social account	Type of digital identity acting in social media
	Forum account	Type of digital identity acting in online fora
	Market account	Type of digital identity acting in online markets
	IP address	Type of digital identity
	Phone number	Type of digital identity
	Crypto address	Type of digital identity that can be involved in financial transactions and that can be part of a wallet
	Suggestion	<p>When an entity has grey background, it means that the entity is not part of the investigation graph but is "suggested" as relevant for the investigation.</p> <p>It is proposed to the user, which can later accept or discard the suggestion.</p> <p>Accepting a suggestion implies that the entity effectively becomes part of the investigation graph (and the icon will be updated accordingly).</p>

VIDEO AVAIBLE AT ANITA MOODLE PLAFORM

CONCLUSION

The manual for the use of the Anita platform was written by members of the research team of the University of Criminal Investigation and Police Studies, who themselves underwent training and the first pilot training.

From the point of view of the need to present the materials, they tried to include everything presented in the content of the manual, and from the point of view of the trained persons, they systematize the mentioned materials so that they fully threaten and depict the training process itself.

The basis of the idea of making the manual was that it represents a written form of materials used in the training, to be a kind of reminder and a basis for learning and improving existing knowledge and skills.

As the training process changes, as new content is added, the manual itself will be in a continuous process of development, and this dynamism and adaptability should be an accompanying part of every development process of training.

The authors have no illusions that the text could not have been conceived differently, but they are open to all kinds of suggestions, proposals, and criticisms, which would lead to the textbook being improved or further developed.

With the hope that the mentioned text will be of use to all who will receive and use it,

Authors