FINTER Experience of UCIPS

PROF. DR ZVONIMIR IVANOVIC

UCIPS SERBIA

UCIPS Serbia

P1	P2	P3	P4
Natrisk	IMPRESS	Narcomap	ANITA
Erasmus +	Erasmus +	with the financial support of the European Commission – Transnational initiatives to fight trafficking in drugs and firearms – DG Migrations and Home Affairs	Horizon 2020
Finished 2020	Finished 2020	Finished 2018	Finished 2021

Metdhos and techniques

Taken from theoretical to practical aspects

Interchange with MOI and others

ELC cyclus – to be at the edge

Feedback from both sides

Methods and techniques

1. multiple **smaller-value transfers** in an attempt to **bypass scrutiny**;
2. or they **may use people who have no criminal backgrounds to complete financial transactions to try to make fund transfers** harder to track. These transactions may also be disguised as donations to charities
3. often use any resource of money they can have access to in order to fund themselves. This can range from the **distribution of narcotics, black market oil, having businesses such as car dealerships, taxi companie**s, etc. ISIS is known to use black market oil distribution as a means of funding their terrorist activity.
4. Terrorist organizations **use propaganda in order to rally up financial support from those who follow them.**
5. They are also able to **find funds through criminal activity on the internet such as stealing online banking information** from people who are not correlated to these terrorist organizations.
6. Terrorist organizations also **use the front of being a charity to finance themselves**. Al- Qaeda is a known terrorist organization that has used the internet in order to finance their organization, as through this platform they are able to reach a wider audience

Methods and techniques

6. Bulk **cash smuggling and placement through cash-intensive businesses** is one typology.
7. They are now also moving monies **through the new online payment systems**.
8. They also use **trade linked schemes to launder monies**.
9. Nonetheless, **the older systems** have not given way. Terrorists also continue to move monies through MSBs/Hawalas, and through international ATM transactions.[19] Charities also continue to be used in countries where controls are not so stringent.
10. the Charlie Hebdo shooting in Paris, France in 2015, used transaction laundering to fund their activities.[20][21][22] Examples included reselling counterfeit goods and drugs.

    This chain of funding shows a clear correlation between transaction laundering and terrorism, using legitimate marketplaces to conduct illegal activity (in this case, selling counterfeit shoes) and then using the proceeds to launder money for terrorists."

Proactive, preventive and other activities

Understanding the **<u>importance of multi-agency working groups and the tools</u>** that can be used to identify, infiltrate, and dismantle organizations operating along the crime-terror nexus points.

Prevention

the notion of Know Your Customer (KYC)

The FATF Blacklist (the Non-Cooperative Countries or Territories list) mechanism was used to coerce countries to bring about change.

Green quest

considers **the following patterns of activity as indicators** of the collection and movement of funds that could be associated with terrorism financing:

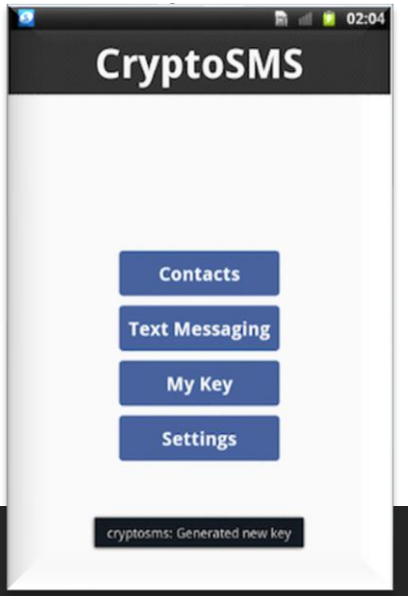
- **Account transactions that are inconsistent with past deposits or withdrawals** such as cash, cheques, wire transfers, etc.
- **Transactions involving a high volume of incoming or outgoing wire transfers, with no logical or apparent purpose that come from, go to, or transi**t through locations of concern, that is sanctioned countries, non-cooperative nations and sympathizer nations.
- **Unexplainable clearing or negotiation of third party cheques and their deposits** in foreign bank accounts.
- **Structuring at multiple branches or the same branch** with multiple activities.

Green quest…

- **Corporate layering, transfers between bank accounts of related entities or charities** for no apparent reasons.
- **Wire transfers by charitable organizations** to companies located in countries known to be bank or tax havens.
- **Lack of apparent fund raising** activity, for example a lack of small cheques or typical donations associated with charitable bank deposits.
- **Using multiple accounts to collect funds** that are then transferred to the same foreign beneficiaries
- **Transactions with no logical economic purpose**, that is, no link between the activity of the organization and other parties involved in the transaction.

Green quest

- **Overlapping corporate officers, bank signatories, or other identifiable similarities** associated with addresses, references and financial activities.
- **Cash debiting schemes in which deposits in the US correlate** directly with ATM withdrawals in countries of concern. Reverse transactions of this nature are also suspicious.
- **Issuing cheques, money orders or other financial instruments, often numbered sequentially**, to the same person or business, or to a person or business whose spelled similarly



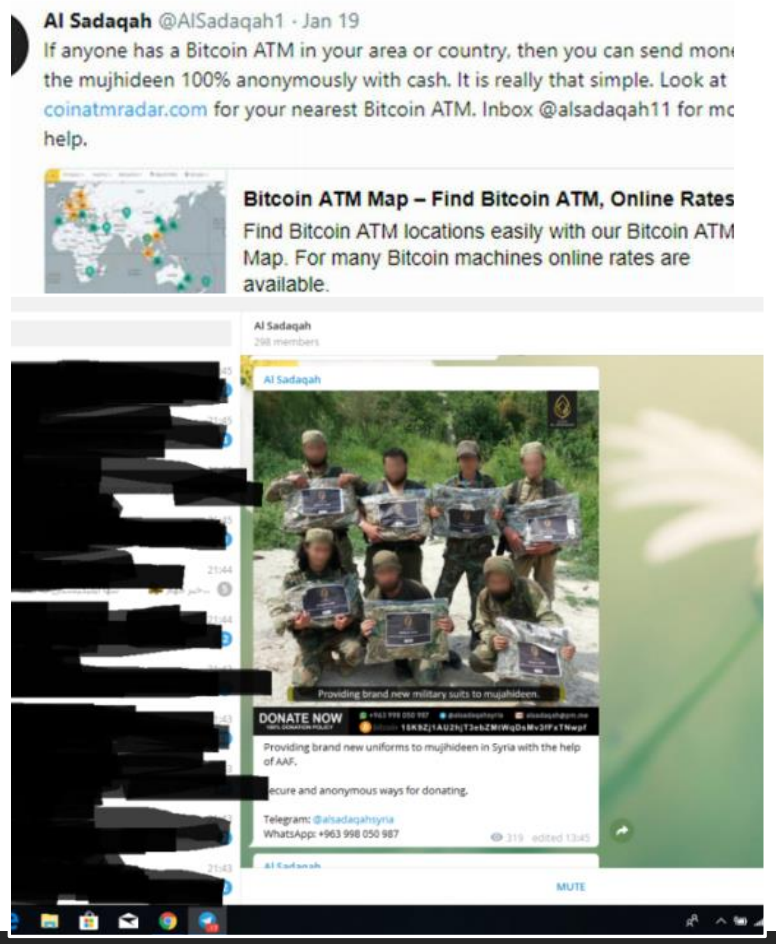
Actions

these activities must be examined in **context with other factors in order to determine a terrorism financing connection**. **Simple transactions** can be found to be suspect and money laundering derived from terrorism will typically involve instances in which simple operations had been performed (retail foreign exchange operations, international transfer of funds) **revealing links with other countries including FATF blacklisted countries**.

Some of the customers may have police records, particularly for trafficking in narcotics and weapons and may be linked with foreign terrorist groups. The funds may have moved through a state sponsor of terrorism or a country where there is a terrorism problem. A link with a Politically exposed person (PEP) may ultimately link up to a terrorism financing transaction. A charity may be a link in the transaction. Accounts (especially student) that only receive periodic deposits withdrawn via ATM over two months and are dormant at other periods could indicate that they are becoming active to prepare for an attack.

MOI RS

- Very inventive opponents
- Adaptable content and involved actors
- Infiltration
- Closed groups targeted
- Engaging specific individuals at right time and place

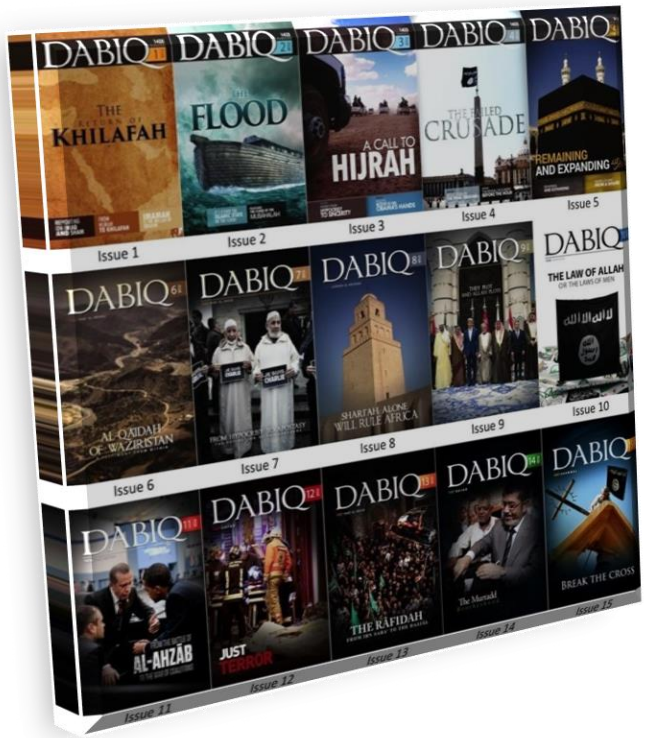


ANITA H2020 experience

Advanced Tools for fighting online illegal trafficking

n° 787061

Funded by EU

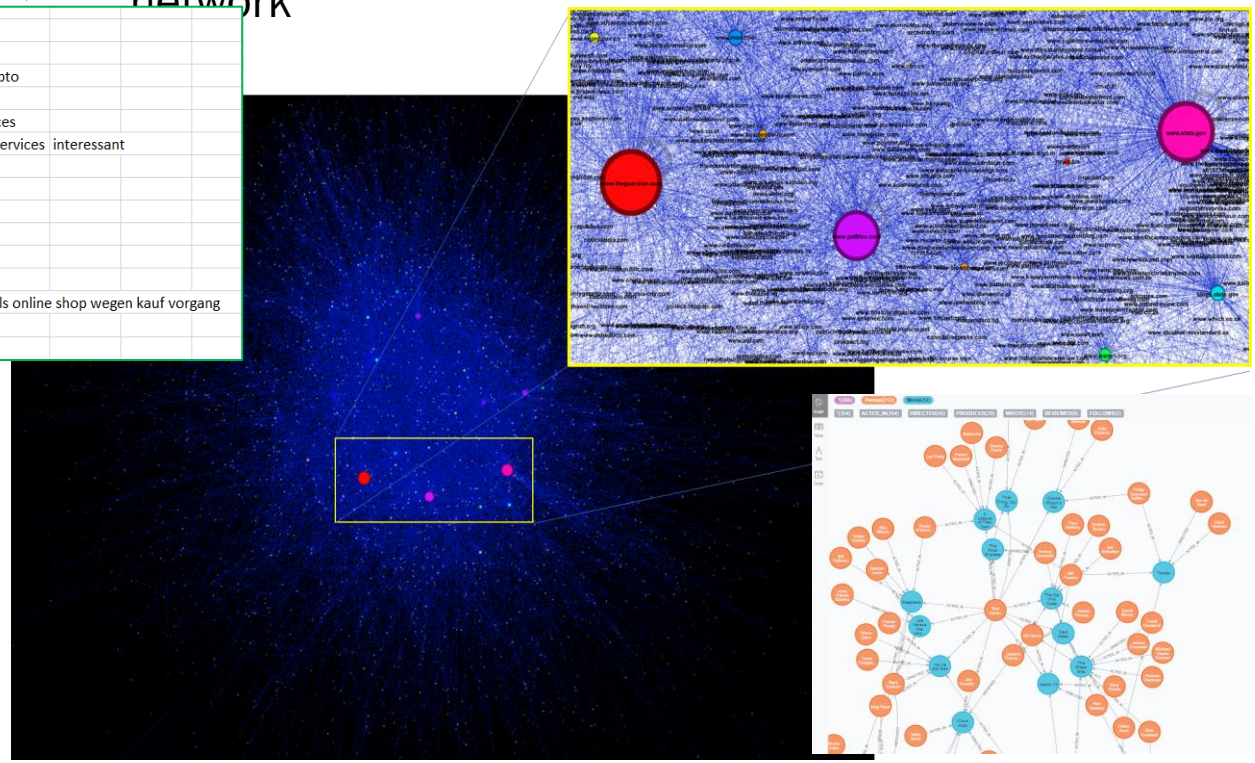


Basic input and results

Input: Search term

Search term	Frequency		
cryptocurrency	73.500.000		
"crypto-currency"	8.120.000	result about crypto	
bitcoin	577.000.000		
"bitcoin wallet"	5.400.000	nur wallet services	
"bitcoin exchange service	325.000	nur excahange services	interessant
bitcoin payment address			
"btc:"	180.000.000	erste hashes	
"bitcoin:" donate	16.000.000		
"bitcoin:"	401.000.000		
"btc:" donate	18.100.000		
"btc:" payment	179.000.000	nicht gut	
"online shop" bitcoin		donate besser als online shop wegen kauf vorgang	
"bitcoincash:"			

Results: crawling network



Content aquisition with Black market crawler

Module: **Black market crawler**

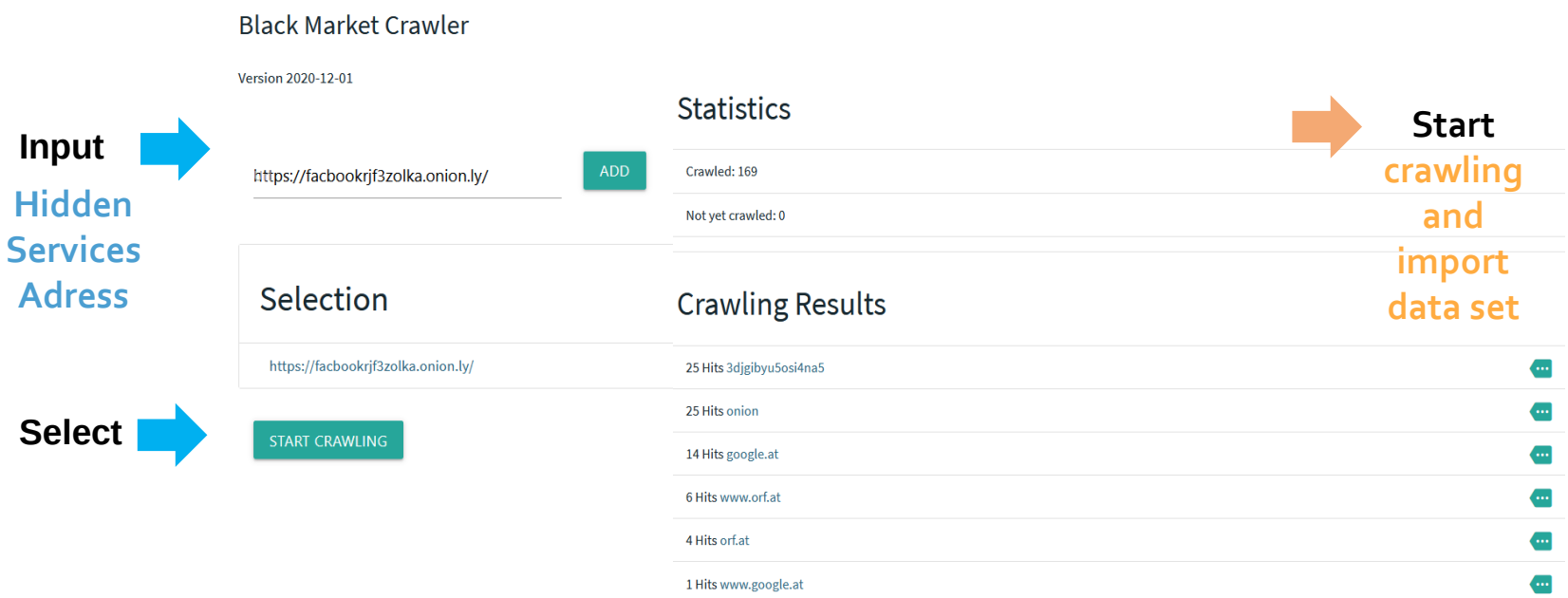
Functionality: Download deep web sites in the dark net (e.g. black markets)

Added value:

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

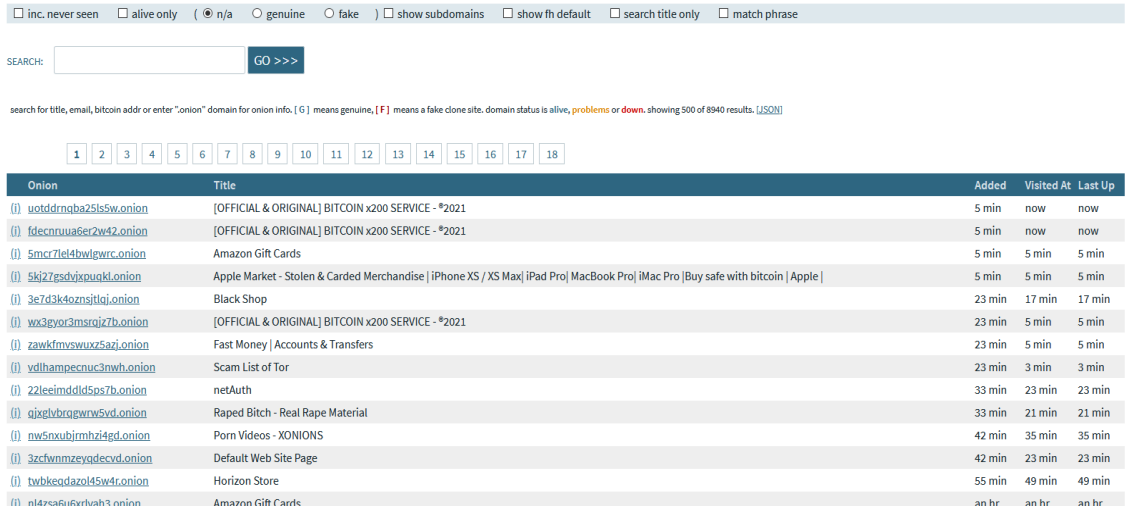
Contribution to ANITA use-cases: Black market content acquisition for ANITA usecases

Content aquisition: Darknet source identification crawler



How to find new and relevant onion links

- **Fast:** Using the dark net monitor



- **More precise:** Using the **source identification crawler** → Presented next

Content aquisition

Module: **Darknet source identification crawler**

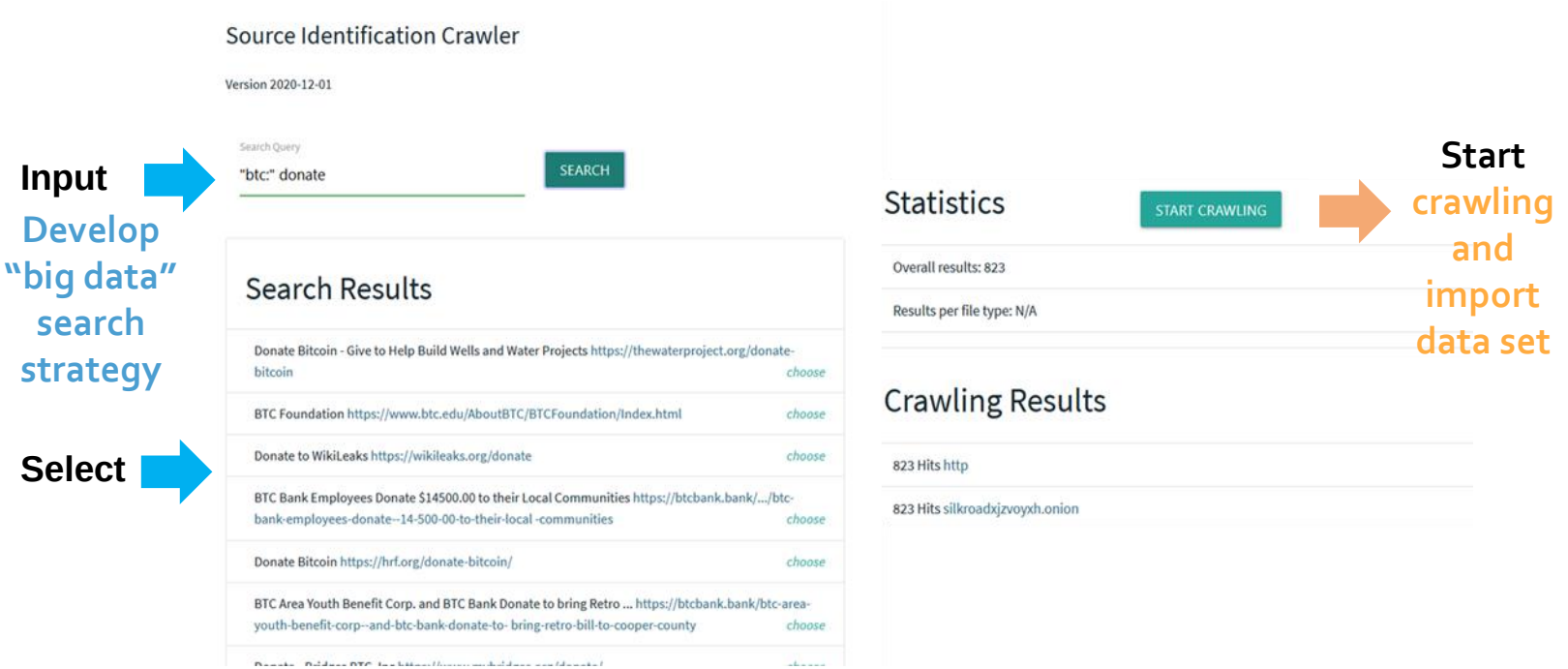
Functionality: Identify possible sources, marketplaces, communication channel across surface web, deep web or dark net

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)

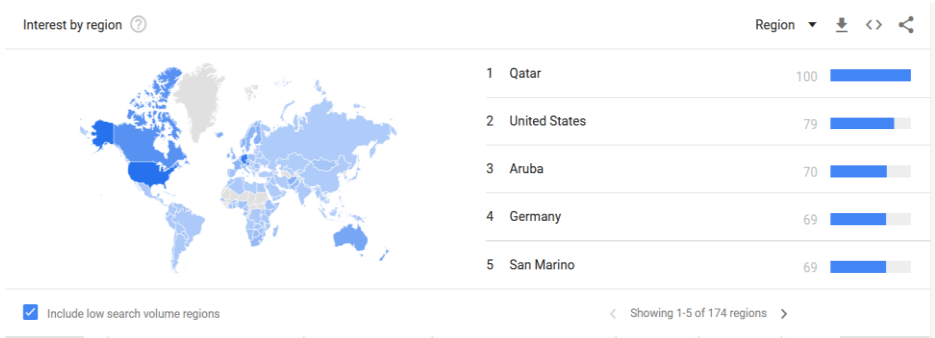
Contribution to ANITA use-cases: content acquisition for usecases

Content aquisition: Darknet source identification crawler



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 boarders and correlating geographic barriers
- Use search statistics
- **Use the best possible unique search strategy**



Search term	Frequency		
cryptocurrency	73.500.000		
"crypto-currency"	8.120.000	result about crypto	
bitcoin	577.000.000		
"bitcoin wallet"	5.400.000	nur wallet services	
"bitcoin exchange service	325.000	nur excahange services	interessant
bitcoin payment address			
"btc:"	180.000.000	erste hashes	
"bitcoin:" donate	16.000.000		
"bitcoin:"	401.000.000		
"btc:" donate	18.100.000		
"btc:" payment	179.000.000	nicht gut	
"online shop" bitcoin		donate besser als online shop wegen kauf vorgang	
"bitcoincash:"			

Trend Analysis

Module: Illegal trafficking trend analysis
Leader: TIU-JADS

Functionality: Provide a set of tools for detecting trends and analysing the incoming information with respect to illegal trafficking.

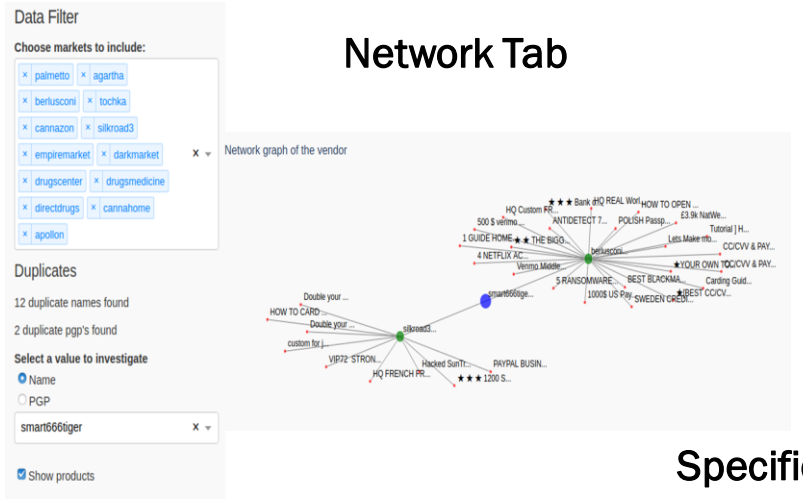
Added value:

- Generate **trends, analytics and actionable insights**
- Perform **quality measures on web pages**

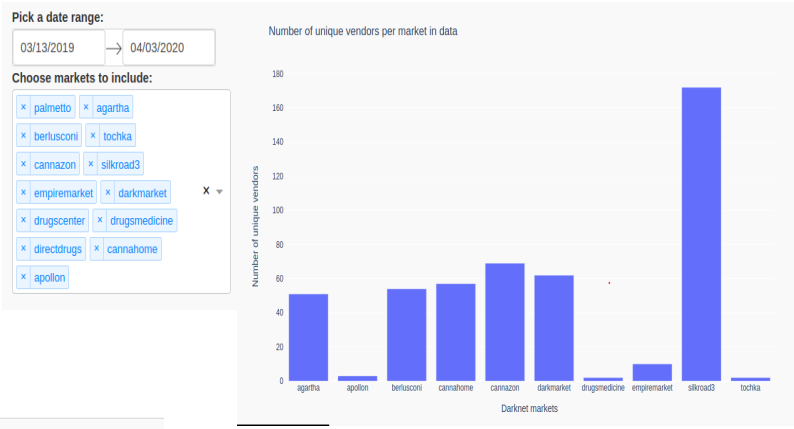
Contribution to ANITA use-cases: The Trend Analysis tool and the Quality measure approach cross all the use cases. The approaches are useful to extract insights from malicious webpages and web markets selling illicit goods

Trend Analysis

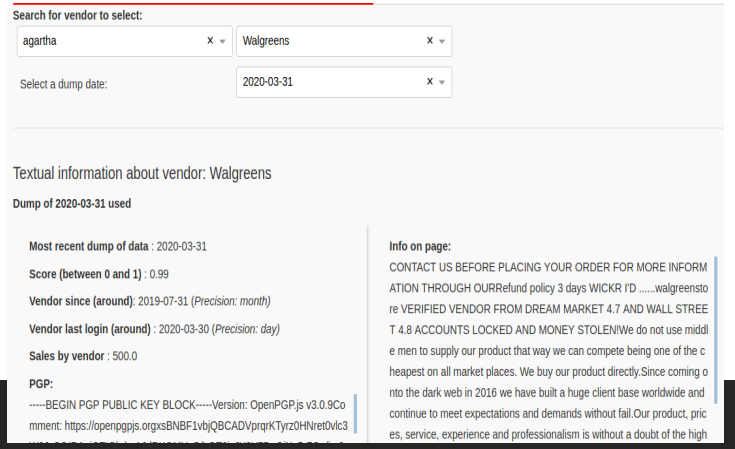
Network Tab



Descriptive Tab



Specific Tab



T6.3 Multilingual automated translation services

Leader: SYSTRAN

Aim: Support LEAs' linguistic needs, **translating in 56 languages** using SYSTRAN Pure Neural® technology

Progress made:

Open-Source Open NMT technology for both online and on-premise infrastructure per LEA's request

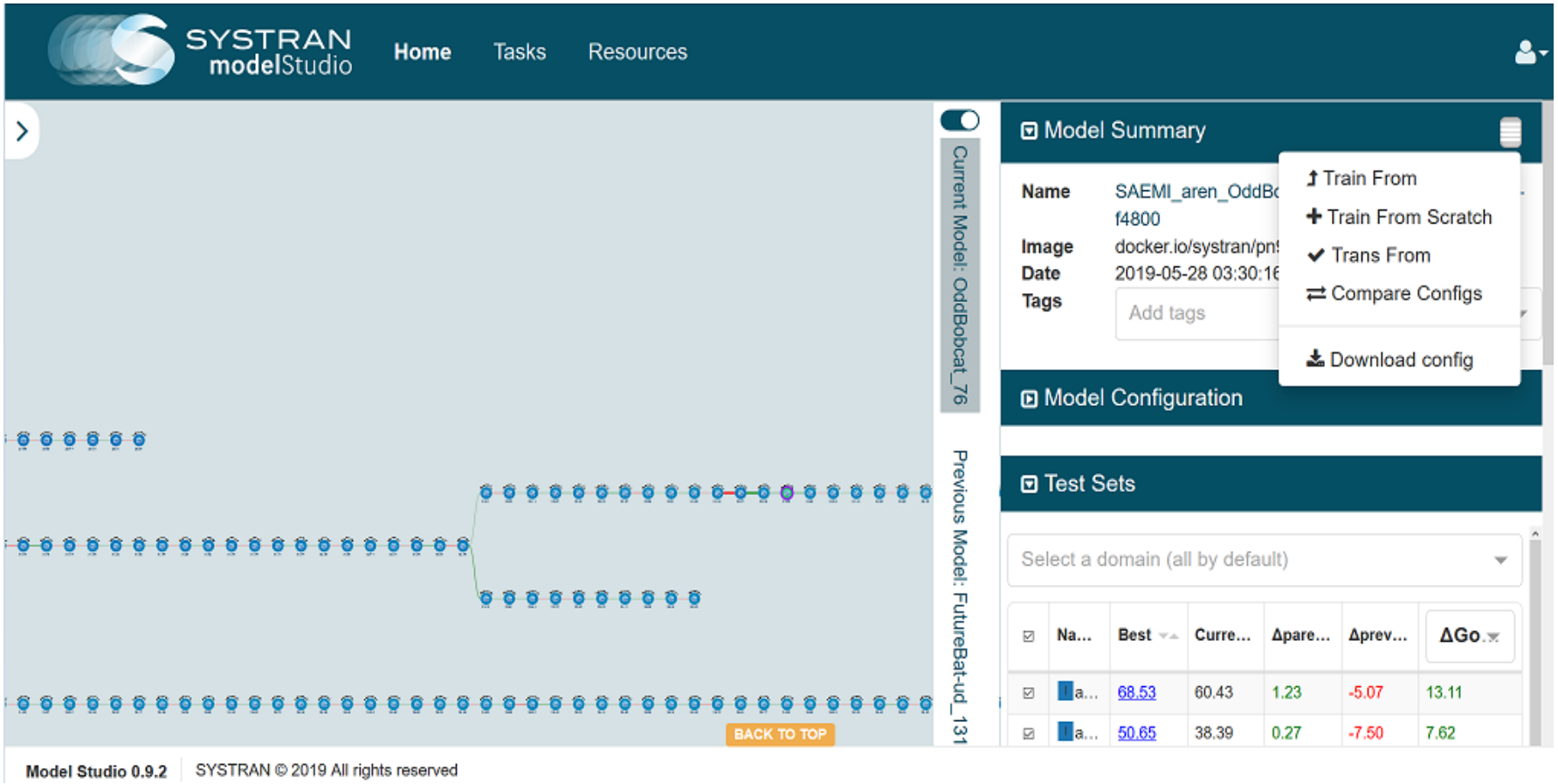
Major achievements:

Migration to TensorFlow Transformer-based framework for performance (>3x) and quality

Working module developed and integrated

T6.3 Multilingual automated translation service

Translate across **56** languages



T6.4 Multilingual speech to text services

Leader: SYSTRAN

Aim: Transparent for the user multi-modal **Speech to Text API** supporting the linguistic coverage in LEAs language combinations

Progress made:

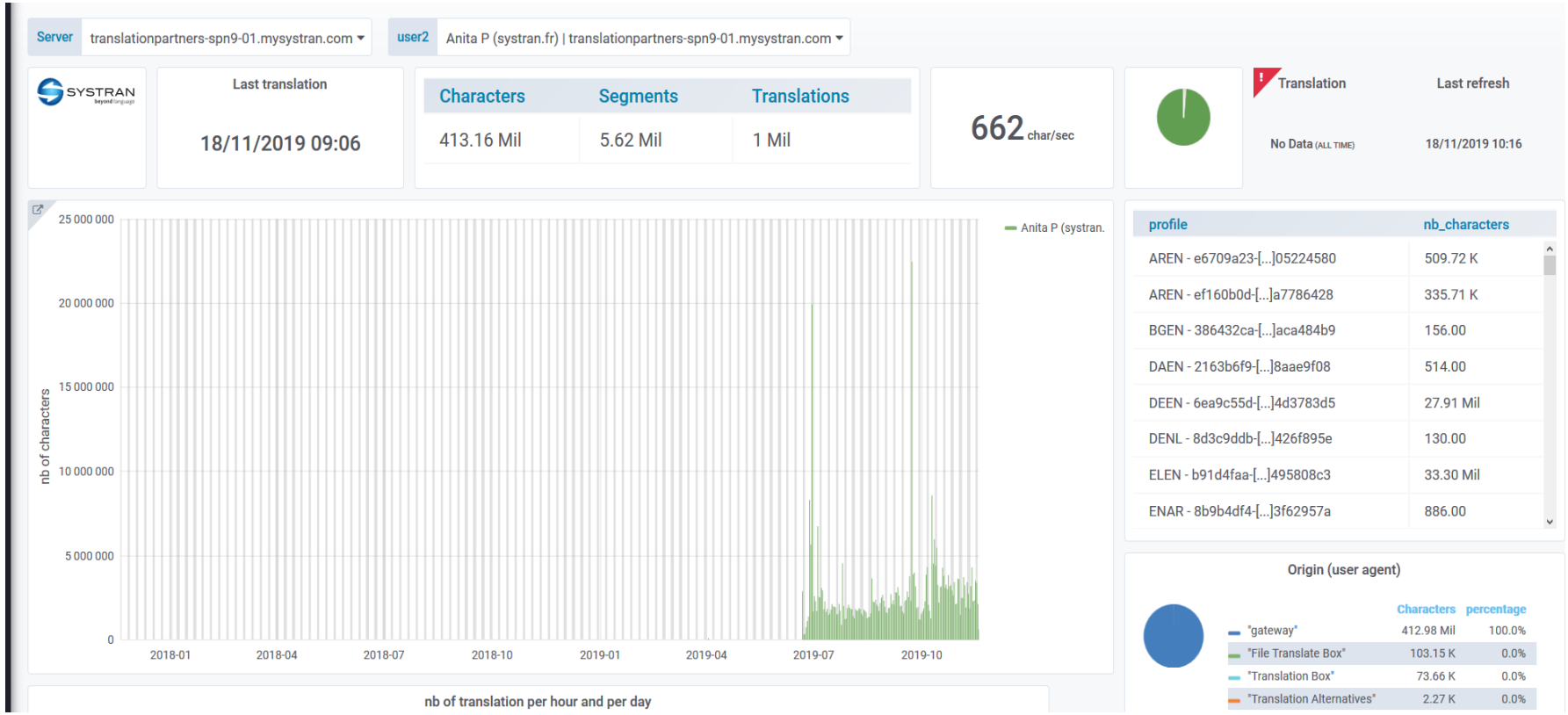
Open-Source Open NMT technology based S2T **API for transcription** and automatic normalization.

Extraction of overlaid text from images

Major achievements:

Multi-modal Multilingual Speech API developed and integrated to ANITA, coupled to TensorFlow Transformer-based framework for performance and quality

T6.4 Multilingual speech to text services



T6.5 Illegal trafficking trend analysis

Leader: TIU-JADS, Participants: CERTH

Aim: Provide a **trend analysis and webpage classification tool** to extract information related to a specific trend in buying/transaction habits in a dark web and to classify webpages in relationship to their risk level.

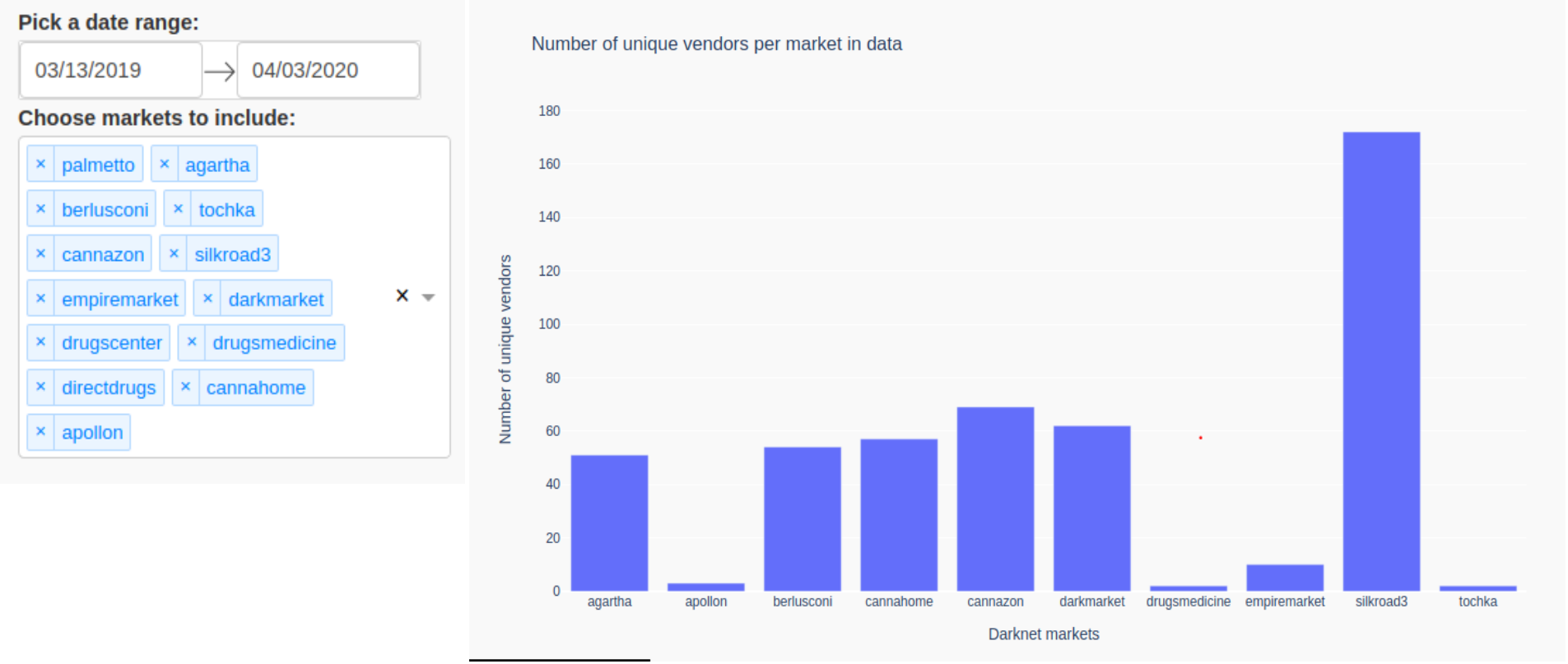
Progress made: A docker image has been delivered and currently it is under integration process. The image contains the Trend Analysis tool, the quality measures classifier, and all the related endpoints.

Major achievements:

- Creation of a machine learner that predicts **website legitimacy** based upon its appearance and software quality parameters
- Trend analysis tool to identify the **behavior of users** on dark web.
- Trend analysis tool to extract **info about vendors and products**.
- Creation of smart crawler to crawl data from the dark web.

T6.5 Illegal trafficking trend analysis

Descriptive Tab



T6.5 Illegal trafficking trend analysis

Network Tab

Data Filter

Choose markets to include:

palmetto, agartha, berlusconi, tochka, cannazon, silkroad3, empiremarket, darkmarket, drugscenter, drugsmedicine, directdrugs, cannahome, apollon

Duplicates

12 duplicate names found

2 duplicate pgp's found

Select a value to investigate

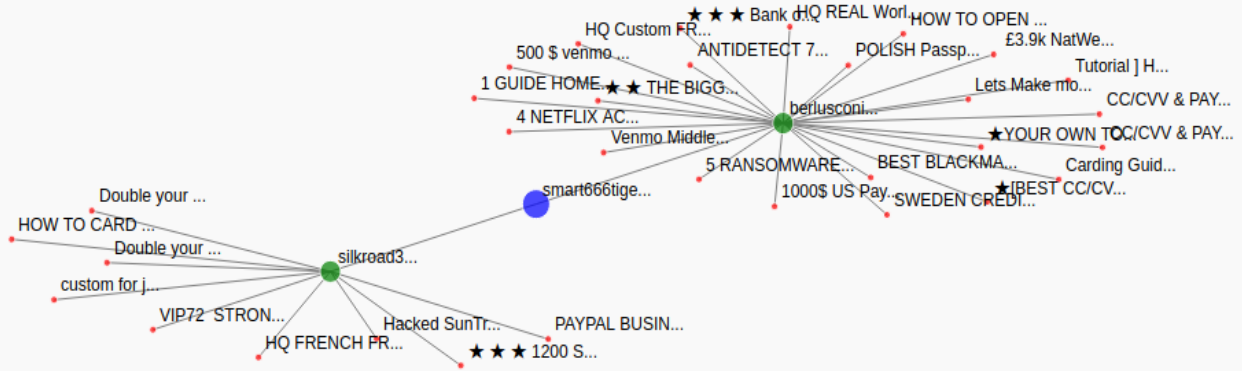
Name

PGP

smart666tiger

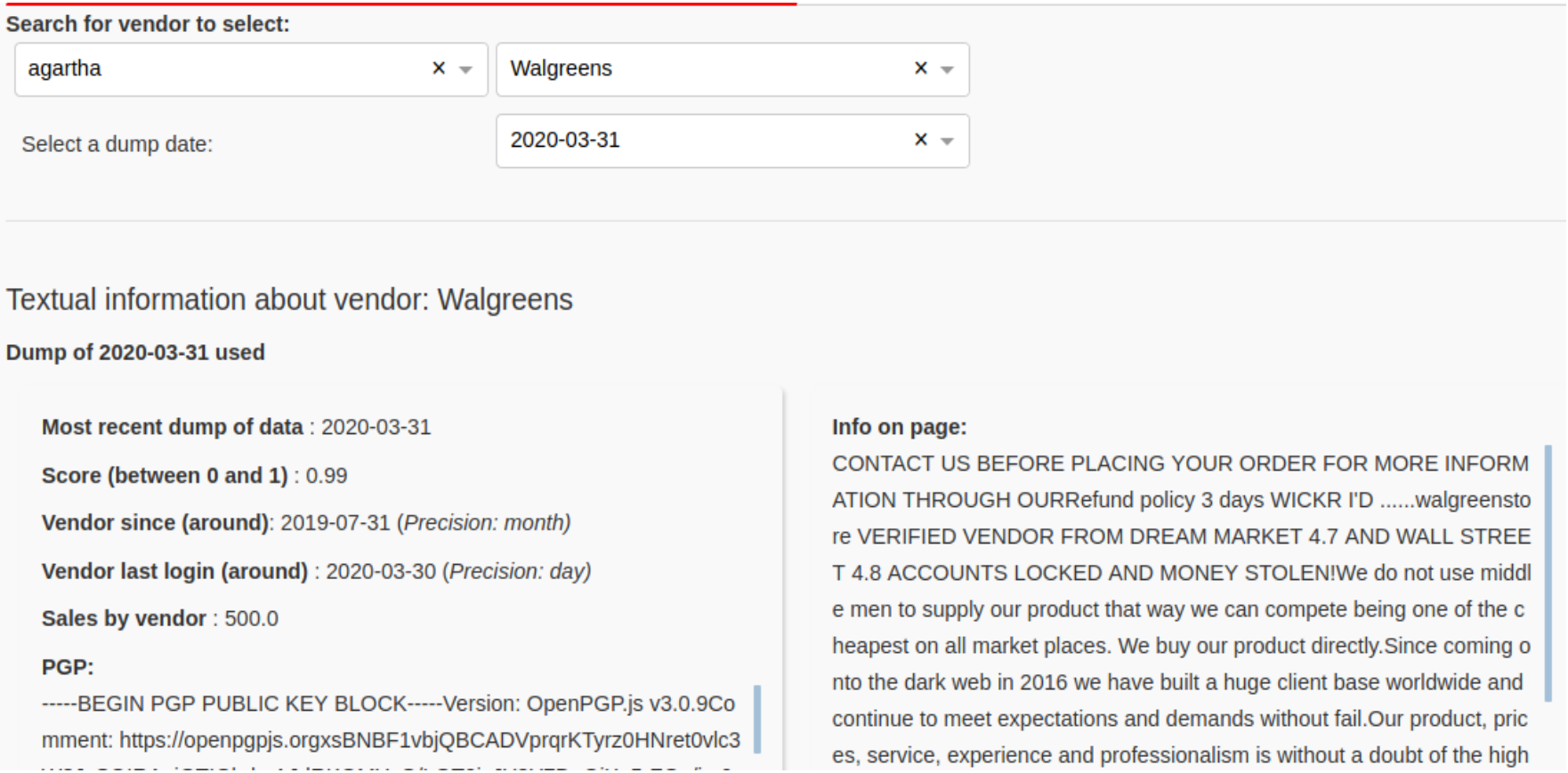
Show products

Network graph of the vendor



T6.5 Illegal trafficking trend analysis

Specific Tab



T6.6 Visual indexing

Leader: CERTH

Aim: Visual indexing task aims to generate a **compact representation of the visual content** in order to makes the similarity retrieval task efficient by:

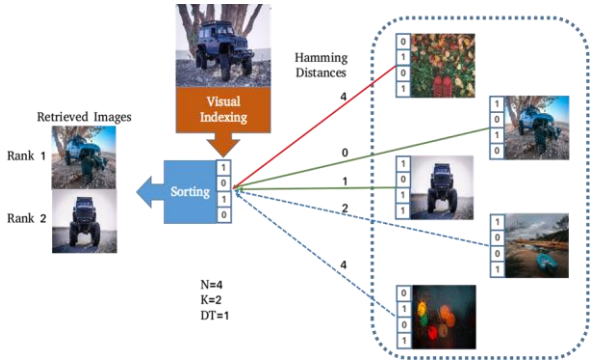
- Generate short length binary codes
- Use *Hamming* distance for comparison

Progress made:

- A **deep hashing** method was fine-tuned in order to represent images, with compact 48-bit hash codes. The delivered hash codes were used to retrieve similar images for a specific place
- The proposed method is **adapted on ANITA dataset** which provided by project partner AIT

Major achievements:

- Working demo is developed
- Evaluated in real data and on ANITA dataset



Recapitulation of tools

~~A set of sophisticated analytics tools has been developed in WP6 to offer the capability~~ to automatically manipulate, analyse, and semantically organize the vast amount of multi-modal content available from Surface/Deep Web, Dark Nets, Social media, and other sources. The tools are trained and evaluated on ANITA specific datasets.

Tools for **textual** analysis (T6.1, T6.3, T6.4)**:**

- Content characterization, Entity extraction, Authorship identification.
- Multilingual translation across 56 languages, Speech-to-text transcription

Tools for **visual** analysis (T6.2, T6.6)**:**

- Object, concept, event detection
- Content-based search, Approximate localization

Tools for illegal trafficking **trend** analysis (T6.5):

- Identification of suspicious webpages from their appearance and code
- Monitoring vendor and user framework to identify new and existing trends

Recapitulation of tools

Trend analysis

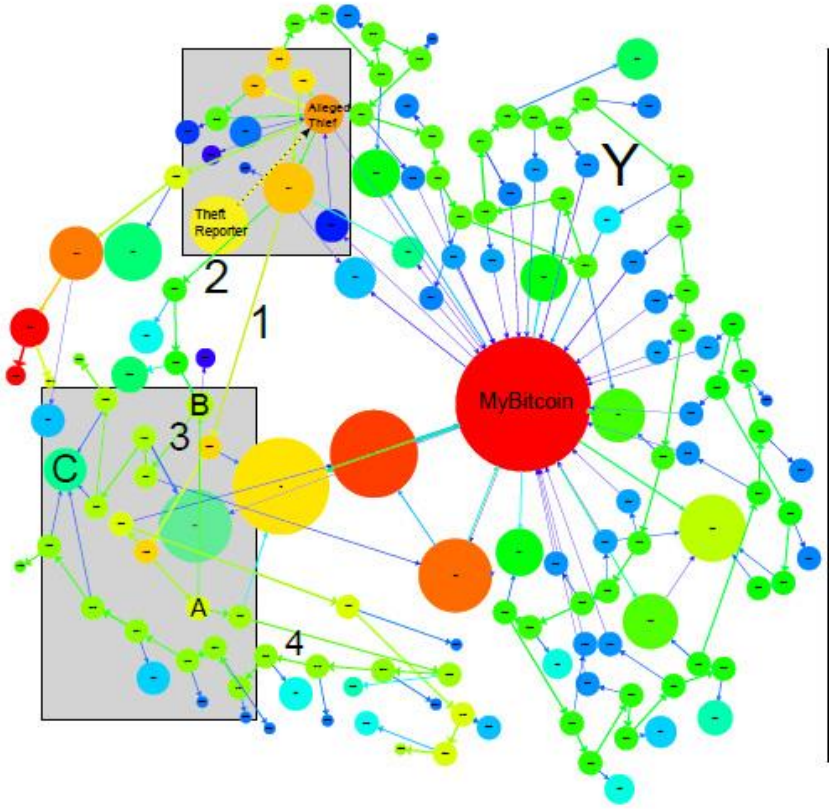
Platform capabilities

Scrappers of the darknet, deep web and clear web

Bitcoin analytics

Physical “field” activities

Results



Experience

Both lines included – practical and scientific

Inferring from personal and experience of others

Practical implementation and inferring – not very great

Issues with practical members hesitations

Political questions

Thank you for your attention

Prof. Dr Zvonimir Ivanovic

UCIPS Serbia

E-mail zvonimir.Ivanovic@kpu.edu.rs

tel:+381606146866