



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

Methods 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 companies**, 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."

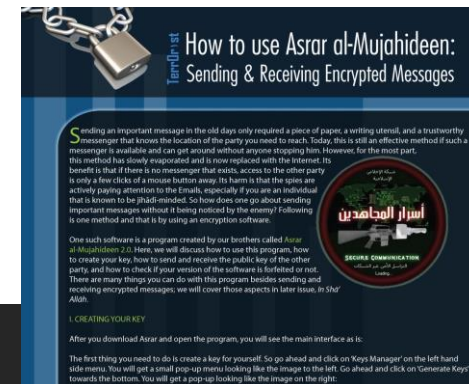
Proactive, preventive and other activities

Understanding the importance of multi-agency working groups and the tools 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 transit** 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.

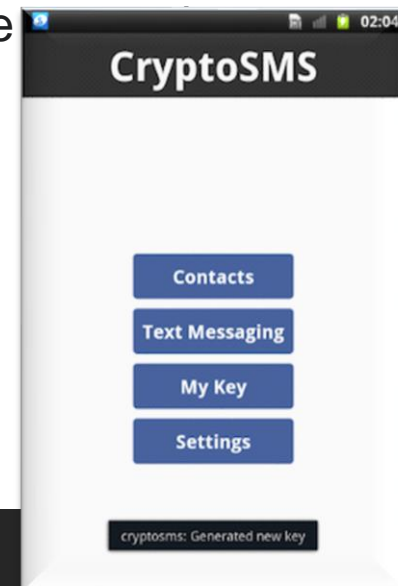
Green quest...



- **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

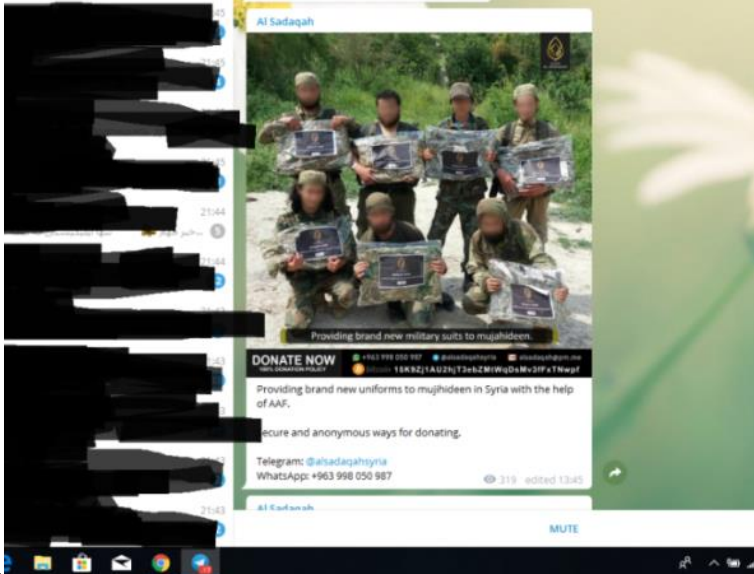
Al Sadaqah @AlSadaqah1 · Jan 19

If anyone has a Bitcoin ATM in your area or country, then you can send money to the mujahideen 100% anonymously with cash. It is really that simple. Look at coinatmradar.com for your nearest Bitcoin ATM. Inbox @alsadaqah11 for more help.



Bitcoin ATM Map – Find Bitcoin ATM, Online Rates
Find Bitcoin ATM locations easily with our Bitcoin ATM Map. For many Bitcoin machines online rates are available.

Al Sadaqah
298 members



Providing brand new military suits to mujahideen.

DONATE NOW +963 998 050 987 @alsadaqahsyria @alsadaqah.com
1E9XZ14U2N1T245CMWqD4Mz3F4T4W47

Providing brand new uniforms to mujahideen in Syria with the help of AAF.

Secure and anonymous ways for donating.

Telegram: @alsadaqahsyria
WhatsApp: +963 998 050 987

Al Sadaqah

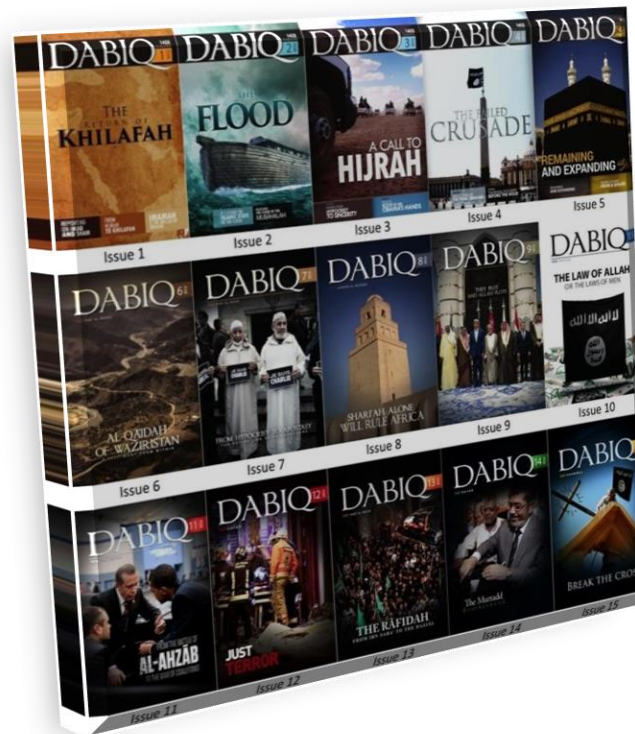
MUTE

ANITA H2020 experience

Advanced Tools for fighting online illegal trafficking

n° 787061

Funded by EU



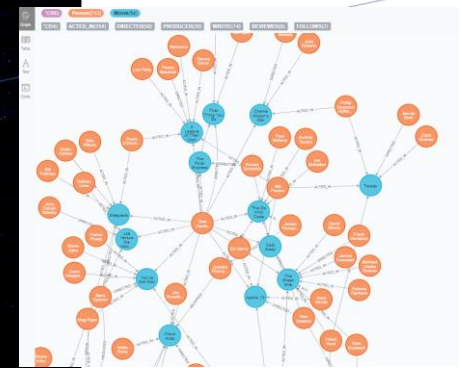
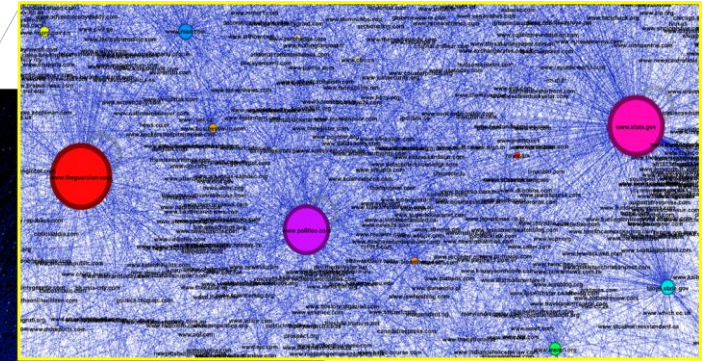
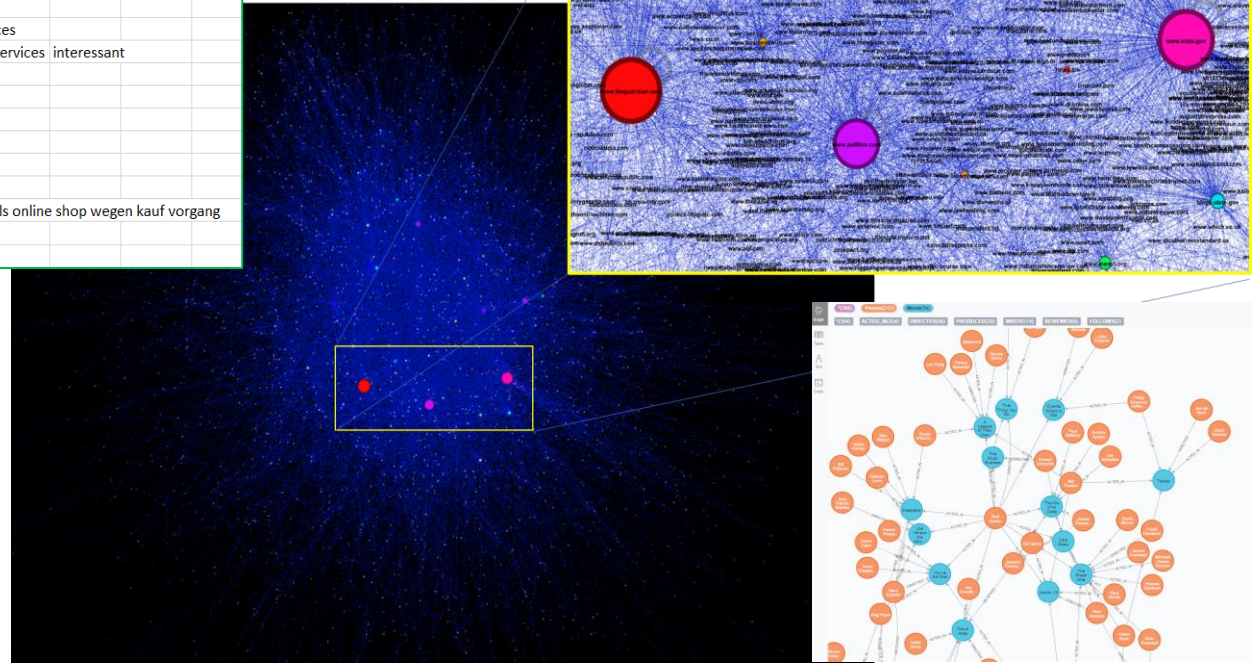
Basic input and results

Input: Search term



Results: crawling network

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 exachange 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:"			



Content acquisition 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 acquisition: Darknet source identification crawler

Black Market Crawler
Version 2020-12-01

Input Hidden Services Adress →

Select →

Statistics

Crawled: 169

Not yet crawled: 0

Crawling Results

https://facbookrjf3zolka.onion.ly/	25 Hits 3djgbyu5osi4na5	⋮
	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



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

SEARCH:

search for title, email, bitcoin addr or enter ".onion" domain for onion info. [G] means genuine, [F] means a fake clone site. domain status is alive, **problems** or **down**. showing 500 of 8940 results. [JS(2)]

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
uotddmqba25is5w.onion	[OFFICIAL & ORIGINAL] BITCOIN x200 SERVICE - *2021	5 min	now	now
fdecnrua6er2w42.onion	[OFFICIAL & ORIGINAL] BITCOIN x200 SERVICE - *2021	5 min	now	now
5mcr7le4bwjgwr.onion	Amazon Gift Cards	5 min	5 min	5 min
9kj27psdvjpuqki.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
3e7d3k4ozstlaj.onion	Black Shop	23 min	17 min	17 min
wx3eyw3mrsqjz7b.onion	[OFFICIAL & ORIGINAL] BITCOIN x200 SERVICE - *2021	23 min	5 min	5 min
zawkfmsvwx25azj.onion	Fast Money Accounts & Transfers	23 min	5 min	5 min
vdlhampecnuc3nwh.onion	Scam List of Tor	23 min	3 min	3 min
22leeimddld5ps7b.onion	netAuth	33 min	23 min	23 min
qjxglvbrgwrw5vd.onion	Raped Bitch - Real Rape Material	33 min	21 min	21 min
nw5xubjrmh24gd.onion	Porn Videos - XONIONS	42 min	35 min	35 min
3zchwmzeyqdecvd.onion	Default Web Site Page	42 min	23 min	23 min
twbkeadazo45w4r.onion	Horizon Store	55 min	49 min	49 min
nl4zcaru6rrvsh3.onion	Amazon Gift Cards	an hr	an hr	an hr

- **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 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

Statistics

START CRAWLING

Overall results: 823

Results per file type: N/A

Crawling Results

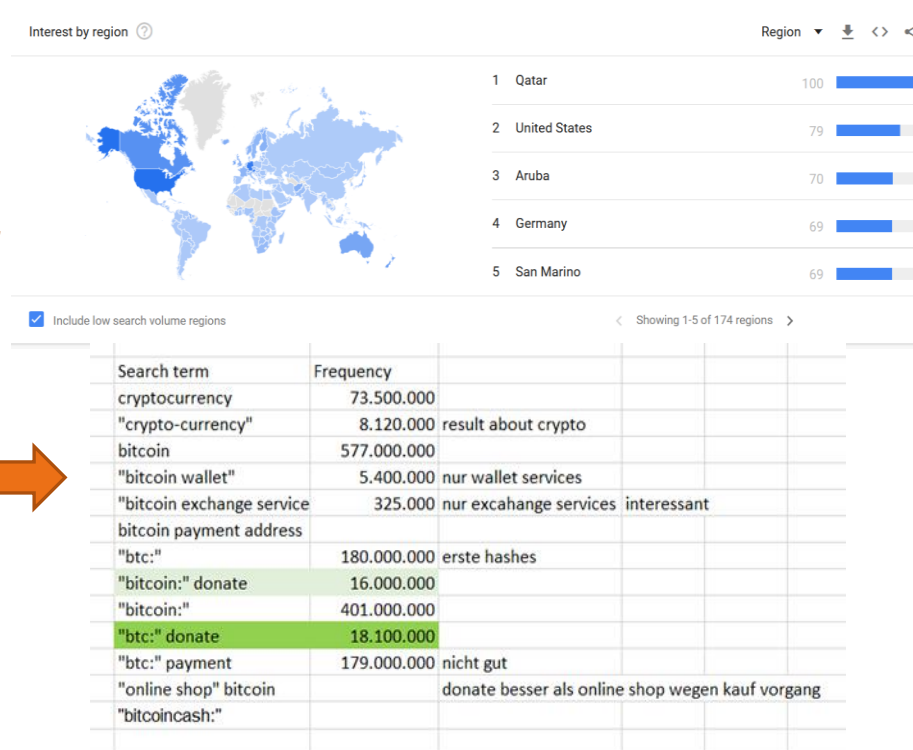
823 Hits http

823 Hits silkroadxjzvoyxh.onion

Start crawling and import data set

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



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

Data Filter

Choose markets to include:

- palmetto
- agartha
- berlusconi
- tochka
- cannazon
- silksroad3
- empiremarket
- darkmarket
- drugscenter
- drugsmedicine
- directdrugs
- cannahome
- apollon

Duplicates

12 duplicate names found

2 duplicate pgp's found

Select a value to investigate

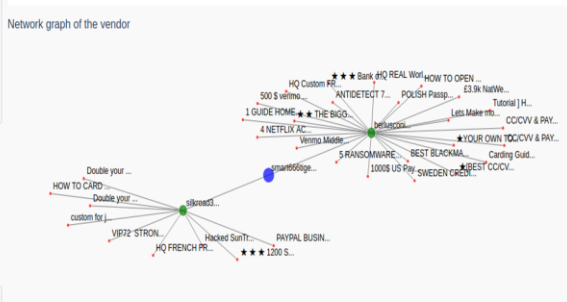
Name

PGP

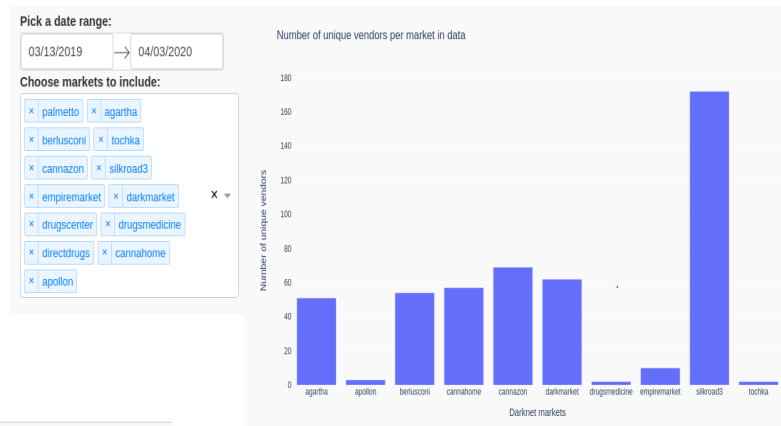
smart666iger

Show products

Network Tab



Descriptive Tab



Specific Tab

Search for vendor to select:

agartha Walgreens

Select a dump date: 2020-03-31

Textual information about vendor: Walgreens

Dump of 2020-03-31 used

Most recent dump of data : 2020-03-31

Score (between 0 and 1) : 0.99

Vendor since (around) : 2019-07-31 (Precision: month)

Vendor last login (around) : 2020-03-30 (Precision: day)

Sales by vendor : 500.0

PGP: -----BEGIN PGP PUBLIC KEY BLOCK-----Version: OpenPGP.js v3.0.9Comment: https://openpgpjs.org/sBNBF1vbJQBCADVprqrKTyZ0HNretDvlc3

Info on page: CONTACT US BEFORE PLACING YOUR ORDER FOR MORE INFORMATION THROUGH OURRefund policy 3 days WICKR IDwalgreenstore VERIFIED VENDOR FROM DREAM MARKET 4.7 AND WALL STREET 4.8 ACCOUNTS LOCKED AND MONEY STOLENWe do not use middle men to supply our product that way we can compete being one of the cheapest on all market places. We buy our product directly.Since coming onto the dark web in 2016 we have built a huge client base worldwide and continue to meet expectations and demands without fail.Our product, prices, service, experience and professionalism is without a doubt of the high

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

The screenshot displays the SYSTRAN modelStudio interface. The main area shows a neural network architecture diagram with a 'BACK TO TOP' button. The right sidebar contains a 'Model Summary' section with a dropdown menu open, showing options like 'Train From', 'Train From Scratch', 'Trans From', 'Compare Configs', and 'Download config'. Below this is a 'Model Configuration' section and a 'Test Sets' section with a table of test results.

<input checked="" type="checkbox"/>	Na...	Best ▾	Curre...	Δpare...	Δprev...	ΔGo... ▾
<input checked="" type="checkbox"/>	a...	68.53	60.43	1.23	-5.07	13.11
<input checked="" type="checkbox"/>	a...	50.65	38.39	0.27	-7.50	7.62

Model Studio 0.9.2 | SYSTRAN © 2019 All rights reserved

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.

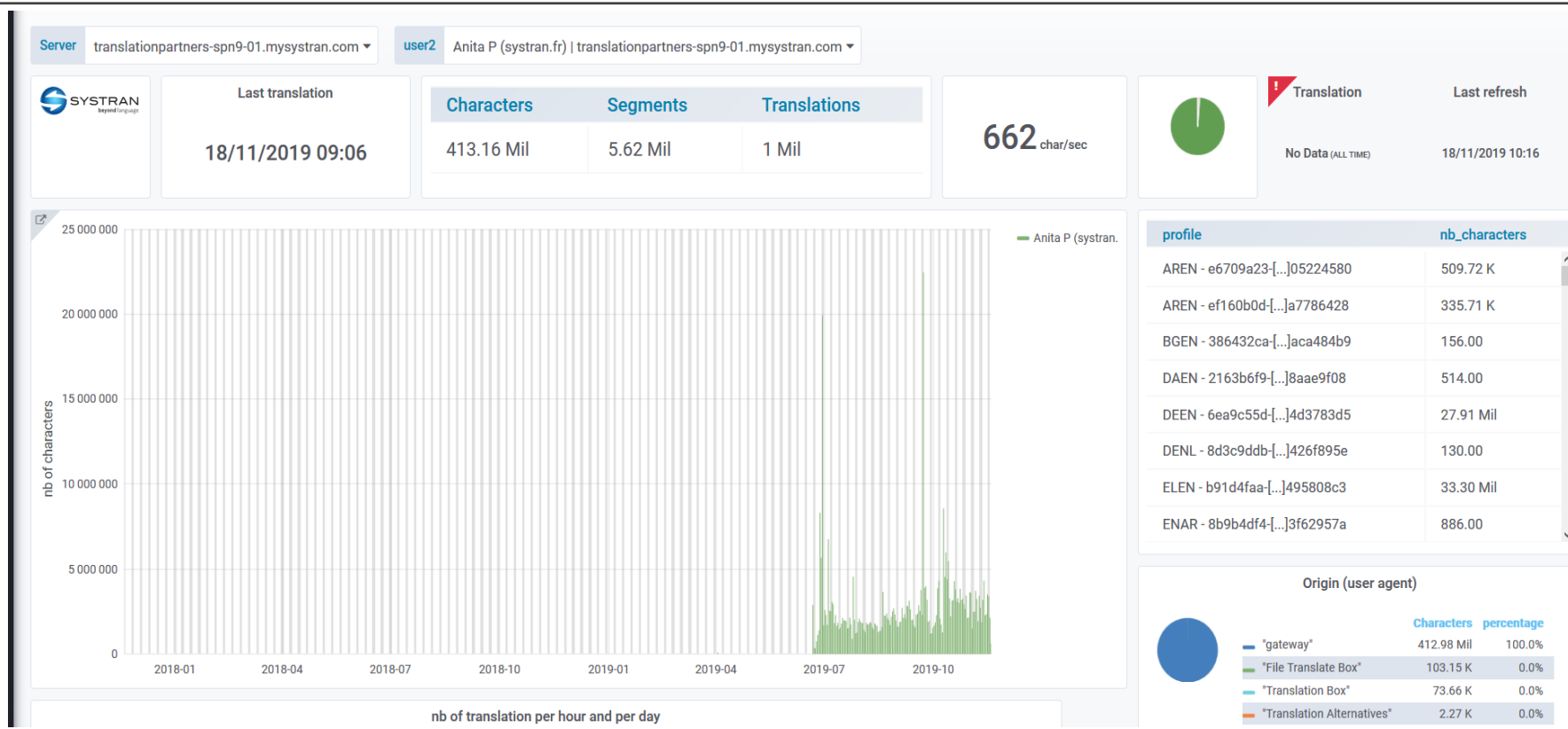
Extraction of overlaid text from images

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.

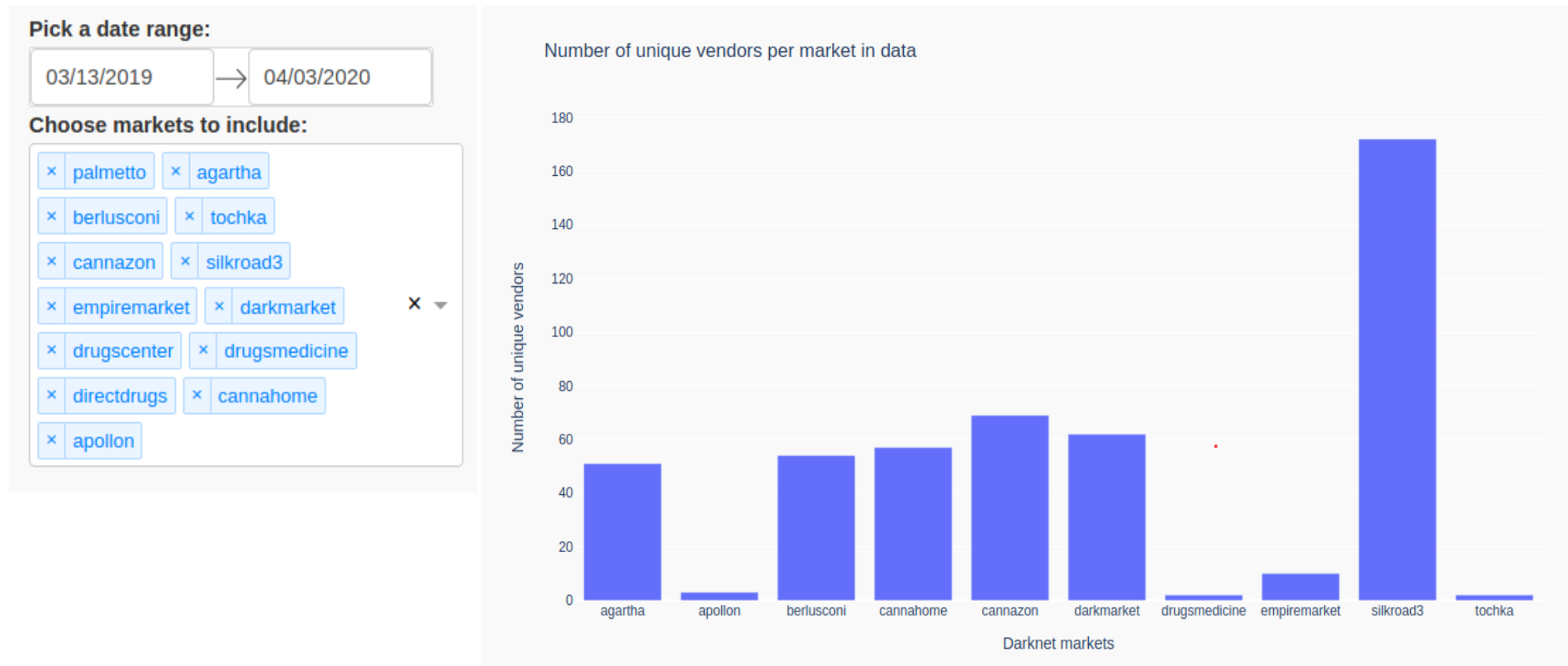
Progress made: A docker image has been delivered and currently it is under integration process. The image contains the Trend Analysis tool, the quality measures classifier, and all the related endpoints.

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:

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

Duplicates

12 duplicate names found

2 duplicate pgp's found

Select a value to investigate

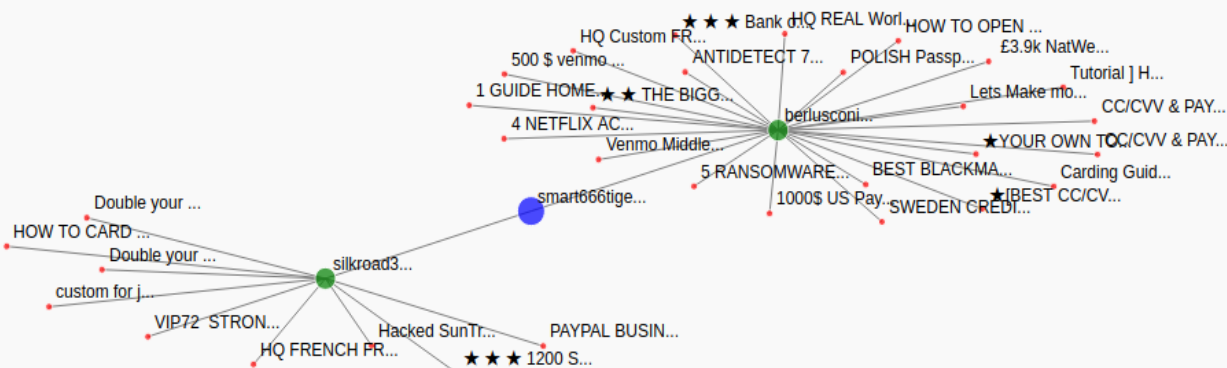
Name

PGP

smart666tiger x ▾

Show products

Network graph of the vendor



T6.5 Illegal trafficking trend analysis

Specific Tab

Search for vendor to select:

agartha x ▾ Walgreens x ▾

Select a dump date: 2020-03-31 x ▾

Textual information about vendor: Walgreens

Dump of 2020-03-31 used

Most recent dump of data : 2020-03-31

Score (between 0 and 1) : 0.99

Vendor since (around): 2019-07-31 *(Precision: month)*

Vendor last login (around) : 2020-03-30 *(Precision: day)*

Sales by vendor : 500.0

PGP:
-----BEGIN PGP PUBLIC KEY BLOCK-----Version: OpenPGP.js v3.0.9Comment: <https://openpgpjs.org>xsBNBF1vbjQBCADVprqrKTYrz0HNret0vlc3

Info on page:
CONTACT US BEFORE PLACING YOUR ORDER FOR MORE INFORMATION THROUGH OUR refund policy 3 days WICKR I'Dwalgreenstore VERIFIED VENDOR FROM DREAM MARKET 4.7 AND WALL STREET 4.8 ACCOUNTS LOCKED AND MONEY STOLEN!We do not use middle men to supply our product that way we can compete being one of the cheapest on all market places. We buy our product directly.Since coming onto the dark web in 2016 we have built a huge client base worldwide and continue to meet expectations and demands without fail.Our product, prices, service, experience and professionalism is without a doubt of the high

T6.6 Visual indexing

Leader: CERTH

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

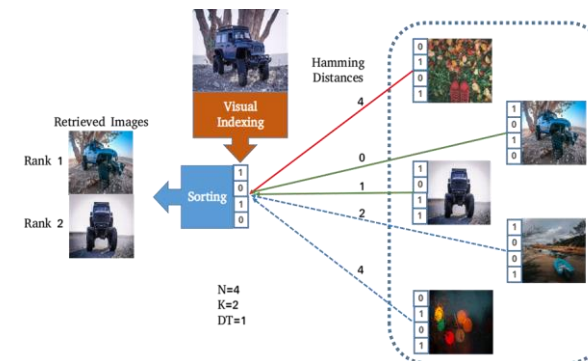
- Generate short length binary codes
- Use *Hamming* distance for comparison

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

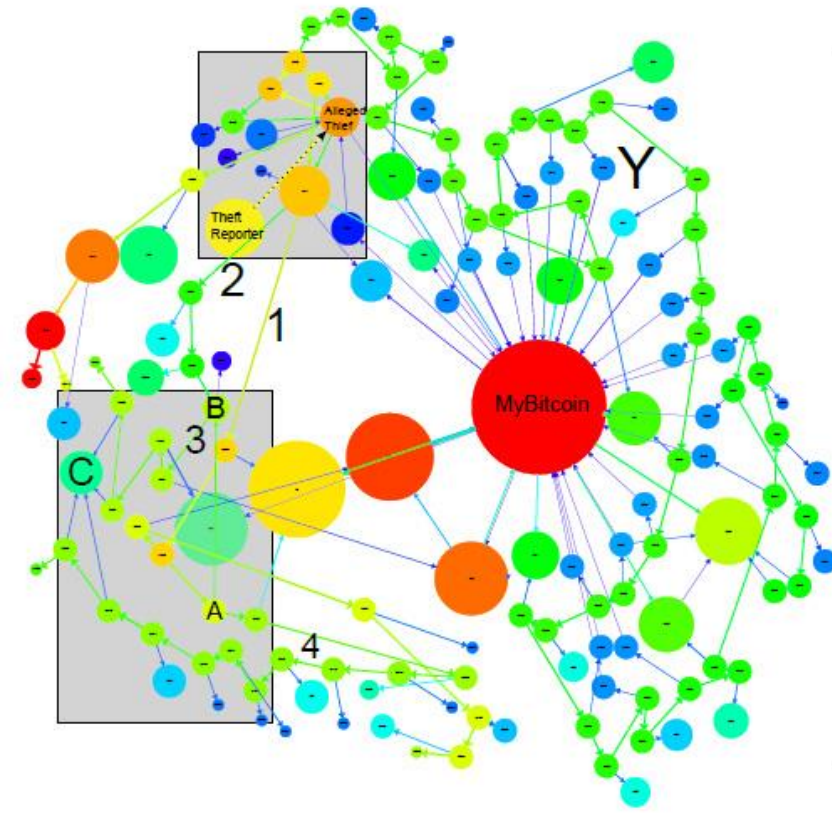
Platform capabilities

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

