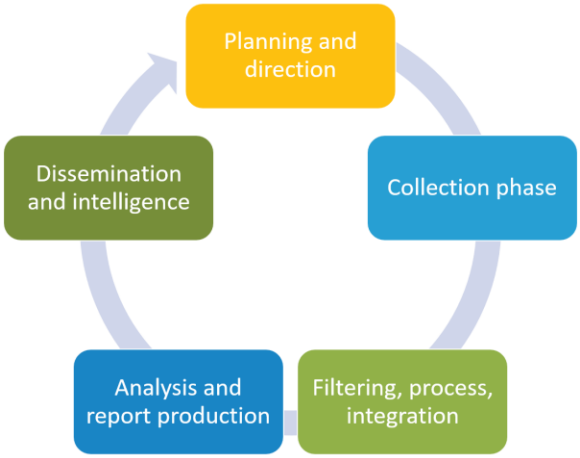
TMD's OSINT Solution

Crime today is becoming more sophisticated as criminals leverage advanced technologies and online solutions for illicit activities. As a result, investigations are becoming much more challenging to solve than ever before. TMD's proposed OSINT solutions helps investigations stay on top with capabilities to collect and analyze publicly available information. When a topic of interest, peace of information or an identifier is entered, massive data amount of publicly available information is automatically collected, generating a detailed view or report that includes information from all layers of the web: dark, deep and surface web.

This processed information than passed to investigation team to add its inputs and is returned to another round till the investigation team has enough insight to move to the interaction phase, covert or overt. The process of such investigation is described in the following image:



One can find many points of strenghts in TMD's proposed solution and, for example, identify the following uniquness and advantages over other systems:

SYSTEM ADMINISTRATION/USER MANAGEMENT

User management

The solution enables the administrator to create several workspaces (for different users and different groups) and assign different cases per workspace enabling full separation between the cases
Each workspace have its own virtual capsule, data cannot be moved from one capsule to other capsule protecting the analysts and preventing data leak
Administrator can define access right per user and per workspace, admin defines which workspace the user can access helping the organization have different clearance level for different analysts
The administrator can block and unblock at any time any of the users
The system supports two factor authentication and administrator is able to:

1 Connect the credentials to origination's security policy.
2 change user's passwords.

The administrator can manage the retention policy for each workspace.
The retention policy can be defined for a minimum of one year
The solution includes an integrated tool that allow the administrator to monitor all the activities performed by all users and to visualize the data in graphical way.

COLLECTION CAPABILITIES

General Avatars & Proxies Management

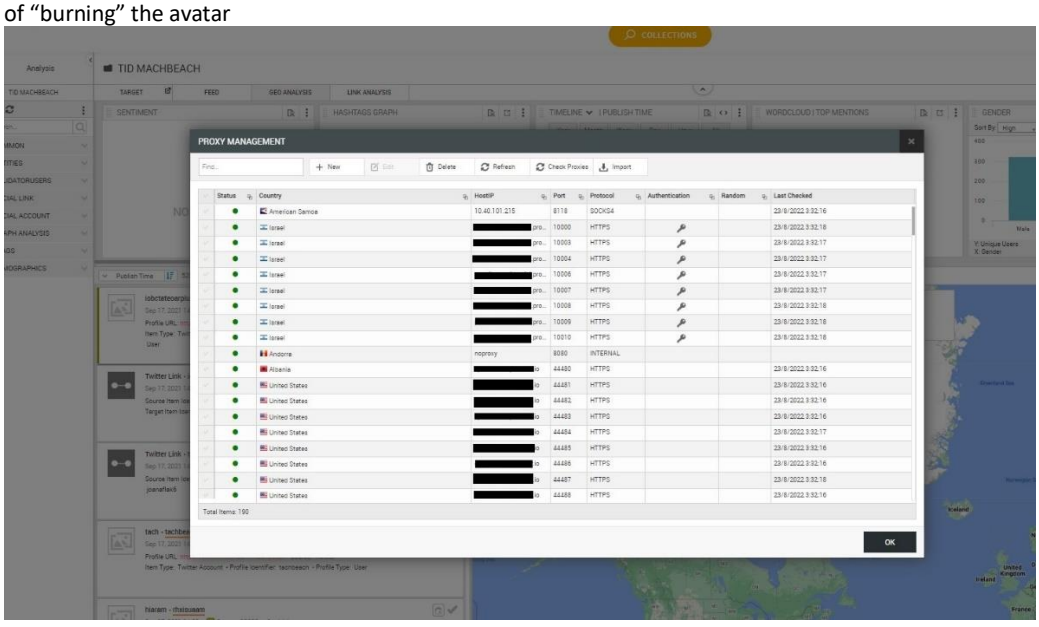
The solution includes a built-in automatic proxies inhibiter (minimum of 10 different global different providers), automatic proxy connector and management system

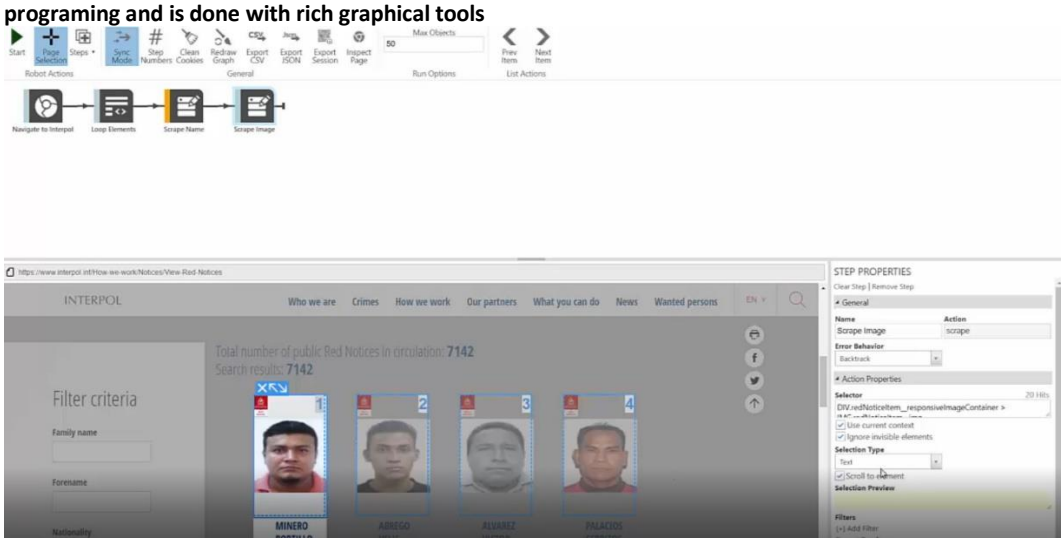
The solution offers a fully secured & anonymous collection process through an integrated avatars & proxies.
The administrator can import avatars credentials in a batch helping large organization manage its assets trough different platform
The administrator is able to import a batch of Proxies for the system

Each proxy can be assigned for a user / group of users. Access to the proxy is configured by asdmin to support

- HTTP
- HTTPS
- TOR

Each avatar could be assigned to a social network or case
The user can define a proxy for each avatar
The user is able to create its own virtual agents and define specific settings.
The user can define if the virtual agent (the avatar) is used through and API / or via login to a browser the risk of "burning" the avatar

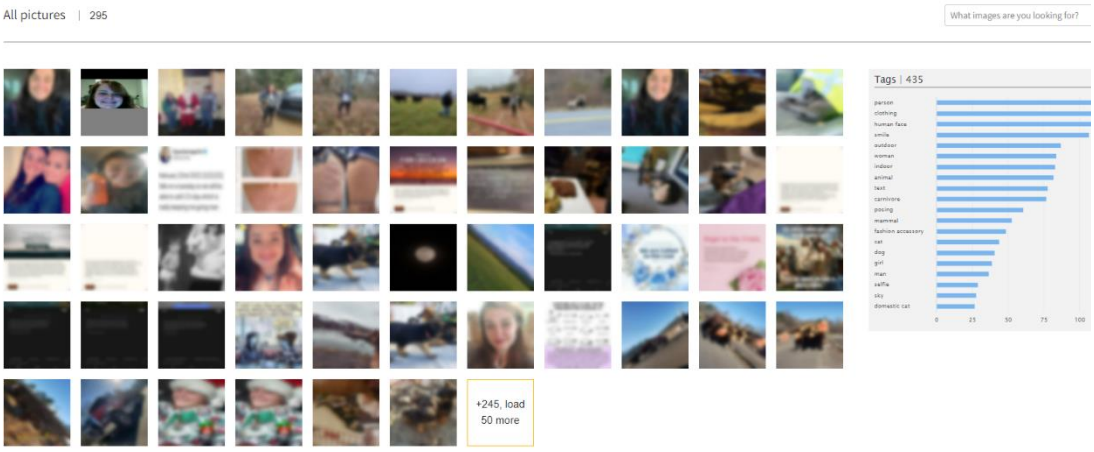


Collection scheduling	The system schedules and repeat a collection task according to the following recurrency: • Every week • Every day • Every hour • Every minute Or to Set the start date and end date
User's control of data collection	The user can assign for each collection task a specific virtual agent & proxy The user can schedule different search times (at least 5 different options) The user is able to write a description for each query helping the analysts with easy management of hundreds of tasks The user can run multiple queries in parallel The user is able to define to which case the query goes
Ease of harvesting and programing	The system includes a set of crawlers/robots that enable the data collection from the following open sources: • Open Web • Social Networks (such as: Facebook, Twitter, instagram, VK) • Darknet • Mobile applications (Telegram, Whatsapp and TikTok) **Development of new avatar / robotic proccess for data harvesting does not require knowladge of programing and is done with rich graphical tools** 
Retry mechanism	The system overcome virtual agent lockout and automatically dispatch at least three different virtual agents for a single query
Geo-fencing	The system enables to generate a query according to a specific geographic area and returning results from a specific area reducing the amount of information the analyst needs to handle
Social Media - Account Search	The system is enable to find different identity names based on keywords on the following networks: • Facebook • Twitter • Instagram
Minimum collection requirements for Facebook	Facebook identity • Feed (commenters, reactions) • Connections (even if the target has a closed friend's list) • About (income, pages) • Locations Facebook page • Feed (commenters, reactions) • Interactors page • About the page

	Facebook group • Feed (commenters, reactions) • Group members Facebook post • Commenters, • Followers reactions • Generic search - keywords
Minimum collection requirements for Twitter	• Identity • Followers • View information in a VLA display and allows you to link multiple Twitter accounts to find mutual friends. • Hashtags (and all accounts that use same Hashtag) • Mentioned accounts (View all accounts that remember the account name.) • **Retweets: Collected the accounts made by Retweets** • Enable a generic search by keywords
Minimum collection requirements for Instagram	• Identity • Followers • Feed • Hashtags • User location (Collect all the places mentioned in the Instagram account) • Followers (All subsequent accounts can be viewed and cross-counted on Instagram to see mutual friends) • Page location
Web Pages collection	• The system is able to choose and collect data from any normal website
Search engines	• Collect data from major search engines. The following are the minimum provided: Google, Bing, Yandex, Yahoo, Baidu
RSS	• RSS feed collection
Darknet	• **The system helps the user to create a generic keyword search on major search engines in the Darknet, including: Ahmia, Haystack, Not evil, Oculus, Tordex, Phobos, Torch, OnionLand, Pickle, Grams, Libera and others.**
Telegram	• **Ability to collect of a Telegram channel with a dedicated virtual agent**
Blockchain	**The solution enables a collection related to crypto currency/blockchain data including the following:** • **Wallet: String of letters representing an identifier connected to a specific coin. Also referred to as the *wallet address*.** • **Transactions: All transactions made *from* and *to* the analyzed wallet. In the world of blockchain transactions are named "Hash."** • **Classification: Label given to a specific wallet or group of wallets. E.g., terror financing, dark market** • **Entity and Entity Type: Name of the individual, object, or organization that may control the address.** • **Risk score: An algorithm generated risk rating, from 0 (high risk) to 100 (low risk), applicable to the searched address and/or transaction ID:**
New sources	**The system enables the user to easily create new robots/crawlers without supplier's assistance for sources that are not include with the solution such as: web sites, forums & blogs, darknet forums, social networks…) The solution should offer a friendly user interface and not requiring any code/sw development skills.**
ANALYSIS FATURES	
Entity extraction	The solution helps in automatic identification and extraction of various entity types. The following entities are mandatory: • Phone numbers, • Names, • Emails, • Organizations • Hashtags • Date & Time

	• Url • Crypto wallet number
	Entity dictionary **The user can define textual entities in any language, into hierarchical groups based on operational definitions.**
Visual Link Analysis (VLA)	The system displays in a graphical way the connections of a specific social network account. Easily filter the connections by the following criteria: • Workplace • Hometown • Education • Internal groups • Connection strength with the target • **Fake accounts** The system enables to collect data for the report directly from the VLA a connection (friend) data. The user can tag any account within the VLA
Timeline on a chart	Ability to: • Filter all results by years, months, weeks, days and hours • Switch the time display between bar chart and line chart • Manually set the date
Sentiment analysis	**Ability to see:** • **Sentiment - by negative, positive, or neutral** • **Filter results based on sentiment** • **Export the chart as an image and use it in a report within the system** • **Do that for more than 40 languages including the Indonesian Basah**
Influencers	Ability to display the most influential people as a list
Demographic information	Ability to filter results by: • Language • Generation • Gender
Hashtags analysis	The system must be able to display a Graphical analysis of the relationship of the main Hashtags and filter the results to see the most popular Hashtags
Geographic analysis on a map	Ability to: • See all results on a map • Filter at least three layers of information: 1. Display the places are mentioned in the text. 2. Display the places mentioned in metadata 3. Display the places mentioned by the users themselves • View the concentration of results and review each result separately Export the result
Main urls	Ability to: Present the main URLs, including social media and Darkweb
Main interactors , participants	Ability to: • **See the number of interactions for each account** • **Filter accounts together** • View account locations • View account ID
Main interactors of a web page or social network	Ability to: See which accounts are interacting on a Facebook page See the number of different interactions on the same page

Group analysis	Ability to • Display in a graphical way the interconnections of two or more accounts • Filter the connections and see which of the connections is related to more than one entity
Fake account detection	**The system is able to detect fake accounts in the following social networks:** • **Facebook,** • **Instagram** • **Twitter** **The system can filter the results by classification (Fake or Real accounts)** **The system allows the results to be exported** **The system supports manually override the classification of an account.**
Monitoring & Alerts	The system allows the users to create custom-made monitoring & alerts. Alerts generate emails indicating new content that has been collected and added to a subscribed investigation (saved query). The alerts are based on predefined filtering and analysis criteria. Examples are a monitored social network account posted content including the word "riot" or "terror attack"; new posts originating from a monitored area of interest, and more.
TARGET PROFILING	
General ease of use	**The solution offers the possibility to retrieve open-source information about a target and generate a report in a "one-click" operation, assisting novice analysts to get instant information (anyone who uses "google" search can operate the one-click feature**
Inputs	Inputs to be supported: • Phone number • Email • Name • Social Network ID (Facebook, Twitter and Instagram)
Outputs	The solution automatically generates a report that includes the following outputs: • Target picture • Target names • Target usernames • Target (additional) email(s) • Target (additional) phone numbers • Target location (on social networks) • Target social presence on the following social networks (Facebook, Twitter, Instagram…) • **Target connections on social networks <u>(even if the target has a closed friend's list)</u>** • Target media presence
Image analysis	Image analysis is processed on all target media pictures • Face detection- helps to compare target profile picture and social accounts profile pictures • Classification (types of cars, man, woman, goods) • OCR – helps to automatically extract additional information on top of the image metadata • Metadata extraction inclusive of location (if available)



VISUALIZATION & REPORT

Report	Ability to create report for each case and export any data in several formats: • JSON • PDF • I2 • CSV
Visualization	Ability to display the entire investigation flow in in map graphical display. The map should includes all investigation findings such as organizations, targets, connections, sites, events… This tool enables any user or user's hierarchy to understand the investigation flow. **The map should is interactive and enable the user to click on a node and access the raw data instantly**.