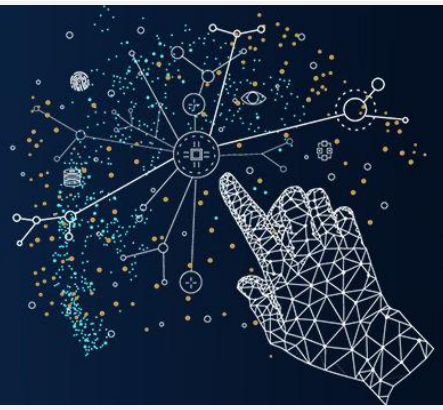
4iQ DELVE DEEP™

Investigate Adversaries. Stop future attacks. Take control.



IDHUNT™ ENTERPRISE

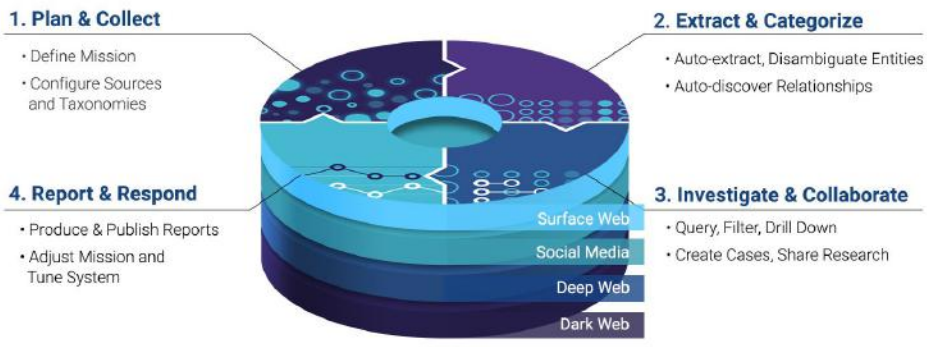
Powering Intel Units in the Public and Private Sector

SUMMARY

- Unmask bad actors.
- Collect & Fuse data from internal and external sources. Configure, schedule and manage thousands of collection policies.
- Automatic Entity Extraction and Enrichment.
- Dynamic Taxonomies.
- Automatic Linking & Powerful Analytics - Strong filtering, Network analysis, Maps and Geo-location, Time-series analysis etc.
- Dashboards, Reports & Alerts.
- Support different missions and Intel Units with granular access controls / permissions.
- Secure collaboration, Investigation case files, internal and cross Unit messaging, comprehensive Audit logs.
- Deploy software on-prem or in the cloud.

4iQ IDHunt™ Enterprise (unified OSINT and DARKINT) is a software platform that supports the full intelligence cycle. Depending on the mission, it allows investigators to figure out the real identity behind an action and what their motivations may be to help solve crimes, and predict and prevent future attacks and exploitations. With IDHunt Enterprise, intel units in private and public sectors can discover the real identity behind bad actors, configure collections, gather information and fuse data from across the surface, social, deep and dark web, internal file systems and 3rd party data sources in order to disrupt attacks.

At the core of **4iQ IDHunt™ Enterprise** information is stored in an actionable way so researchers can explore entities and relationships to gain insights on topics of investigations. As new information is gathered, you can configure the system to track, monitor and receive real-time alerts. The built-in search capabilities allow analysts to locate useful information based on hierarchies, synonyms, relatedness, natural language processing, fuzzy searches, proximity searches and boolean operators.



UNMASK BAD ACTORS

With **4iQ IDHunt™ Enterprise** intel operators and analysts can conduct targeted searches on suspect information, pivot on exposed data attributes returned from the **4iQ IDLake™** and cross reference open source datasets to uncover real identities.

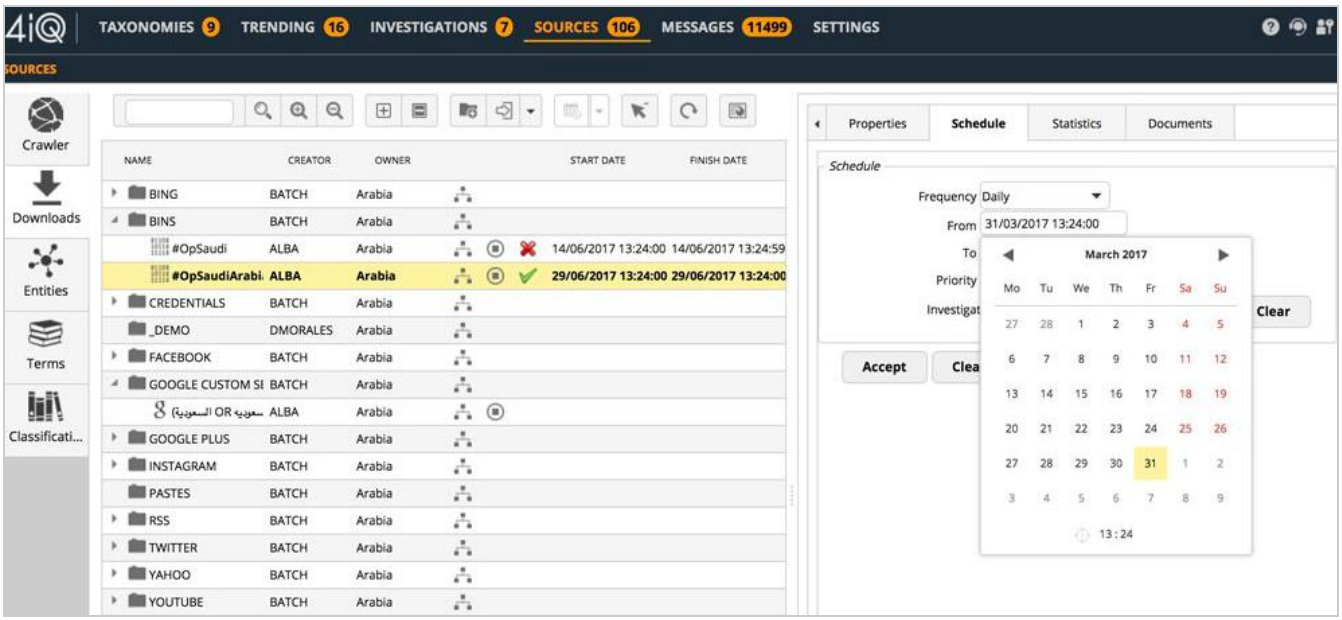
COLLECT & FUSE

4iQ IDHunt™ Enterprise can be configured to fuse external data sources with internal email, file system and other document sources. Data is stored using Apache-SOLR. The system comes with 40+ built-in connectors to sources including crawlers, search engines, social networks, niche websites, bins, dark web meta-search engines and more.

Extensive Portfolio of Built-In Connectors

GRANULAR CONTROL OVER THOUSANDS OF CRAWLING POLICIES

Depending on the mission, administrators or analysts with the right privileges can configure connectors, set up crawling policies, schedule and manage collection.



AUTOMATIC ENTITY EXTRACTION

4iQ IDHunt™ Enterprise automatically extracts entities including people, companies, organizations, places, things, events, topics, documents as well as custom objects.

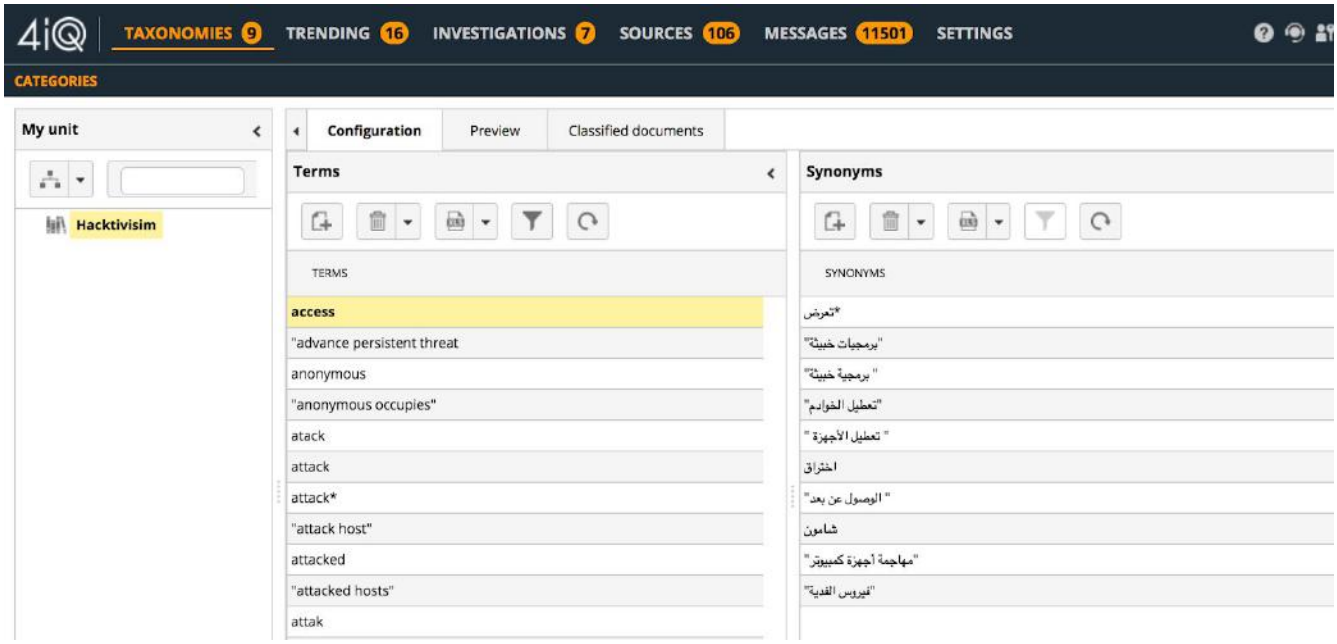
Multi-lingual support (UTF-8) with added support for 12 language pairs (Spanish, Portuguese, English, French…)

AUTOMATIC ENRICHMENT

Documents are processed with optical character recognition (OCR) and automatic text translation. Entities are enhanced with metadata extraction, url expansion, domain ranking, and content cleansing.

DYNAMIC TAXONOMIES

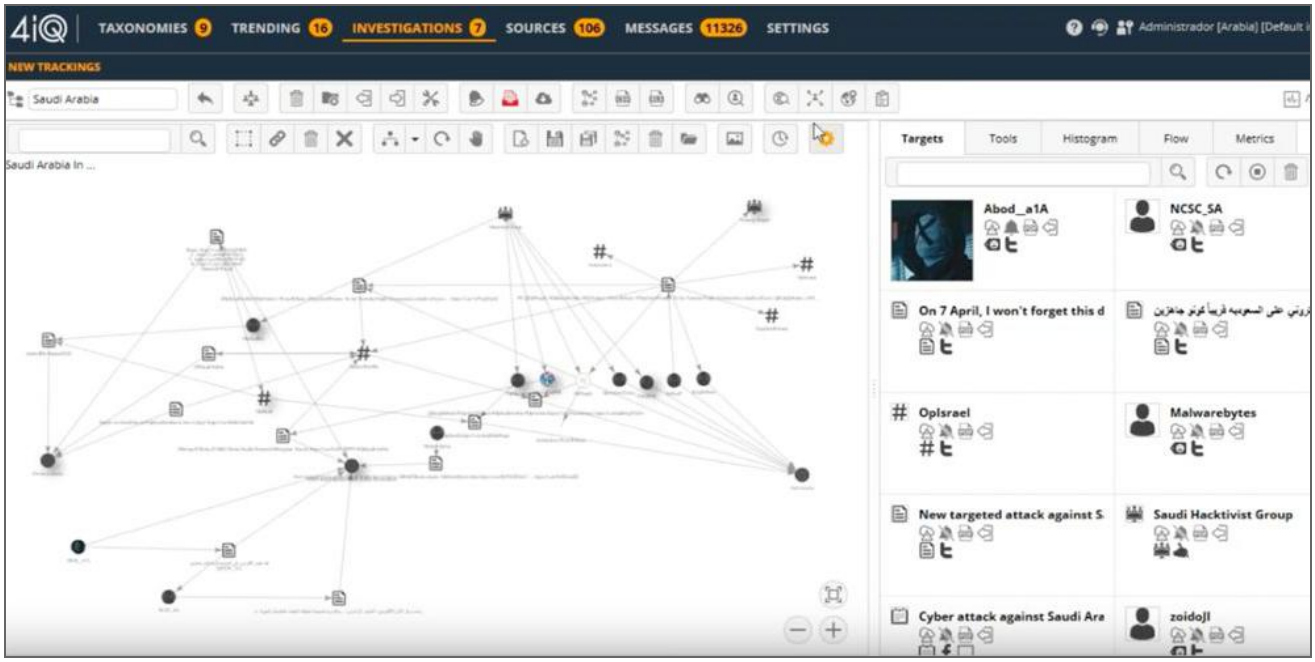
The system allows the creation of custom and dynamic taxonomies or knowledge trees tailored to the intelligence mission. Documents are automatically classified based on assets such as physical locations, buildings, railways, etc; keywords or terms, term groups and hierarchical categories.



AUTOMATIC LINKING & POWERFUL ANALYTICS

4iQ IDHunt™ Enterprise allows analysts to visualize relationships between entities and documents across time and space. Analysts can search across all data in the system at once, auto-expand entities to discover new relationships and surface previously hidden patterns.

Analysts can create investigation case files and selectively share insights with other teams. In addition, analysts can configure workflows to find filter, extract context, create associations, save documents and manage cases.



4iQ IDHunt™ Enterprise uses Apache-Lucene for search. It enables analysts to search based on hierarchies, synonyms, relatedness, natural language processing, fuzzy searches, proximity searches and boolean operators.

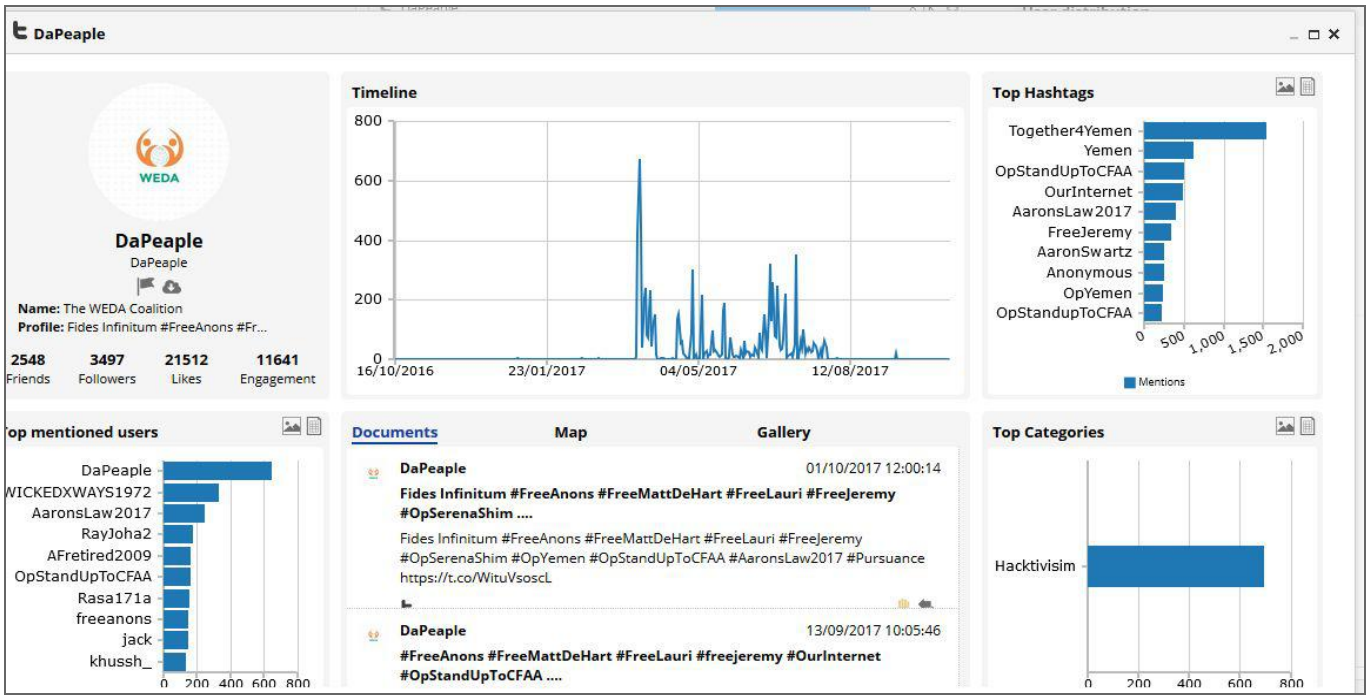
In addition, the system supports:

- Automated and ad-hoc queries with strong filtering capabilities across sources, entities, categories and terms.
- Easy drill down and correlation with network analysis.
- Document reviews with ratings and opinions.
- Time-series analysis.
- Maps (Google Earth, Google Maps) and geolocation (source metadata, source content, whois lookups).
- Dashboards with trends and statistics.

DASHBOARDS, REPORTS & ALERTS

Once the collected data has been analyzed, it can be presented to users in a variety of formats such as customized reports and visual graphs showing the relationships between entities.

A visual control panel shows current activities such as increasing or decreasing traffic patterns, trending topics, handles, hashtags, new activity on different websites, etc.



"Cyber APBs." Rules can be setup to perform automatic actions (translate, send internal/ external message, add to investigation folder) and generate alerts depending on the source, topic and content of documents.

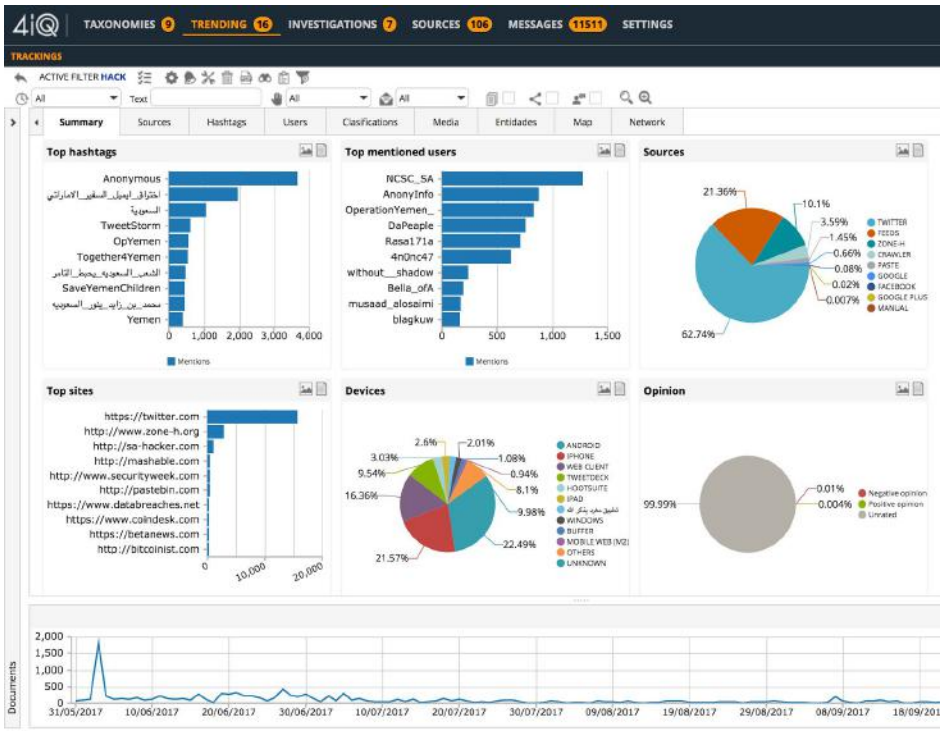
Alerts can be generated if there are significant variations in the volume of documents, if there are changes in source pages or browser or unusual user behavior. Alerts can also be sent to users who need notifications, but may not have access to restricted areas.

Custom Reports. Pre-defined and summary reports can be dynamically generated and exported to spreadsheets, XML, and JSON.

SECURE COLLABORATION

4iQ IDHunt™ Enterprise is a multi-tenant solution, supporting different missions and Intel units with:

- Granular access management of users, groups and units.
- Configuration management of proxies, user agents and credentials.
- Support for multiple case management, alert configuration and controlled sharing of information with cross-Unit and internal messaging.
- Comprehensive audit logs track login/logout, access to different modules, changes to permissions, opening of and changes to taxonomies, investigations, trackings, documents, tasks and processes.



FLEXIBLE DEPLOYMENT

4iQ IDHunt™ Enterprise can be deployed on-premise, in private clouds or managed by 4iQ in the public cloud. 4iQ provides support for system installation and configuration of connectors, taxonomies etc.

To learn more, go to www.4iq.com and connect with us:

@4iQ

4iqDelveDeep

Read our blog:

medium.com/4iqDelveDeep