TOP of my free OSINT tools in 2023

By: Igor S. Bederov

@viehgroup

Note: This document is not created by a professional content writer so any mistake and error is a part of great design

Disclaimer

This document is generated by VIEH Group and if there is any contribution or or credit, it's mentioned on the first page. The information provided herein is for educational purposes only and does not constitute legal or professional advice. While we have made every effort to ensure the accuracy and reliability of the information presented, VIEH Group disclaims any warranties or representations, express or implied, regarding the completeness, accuracy, or usefulness of this document. Any reliance you place on the information contained in this document is strictly at your own risk. VIEH Group shall not be liable for any damages arising from the use of or reliance on this document. also we highly appreciate the source person for this document.

Happy reading !

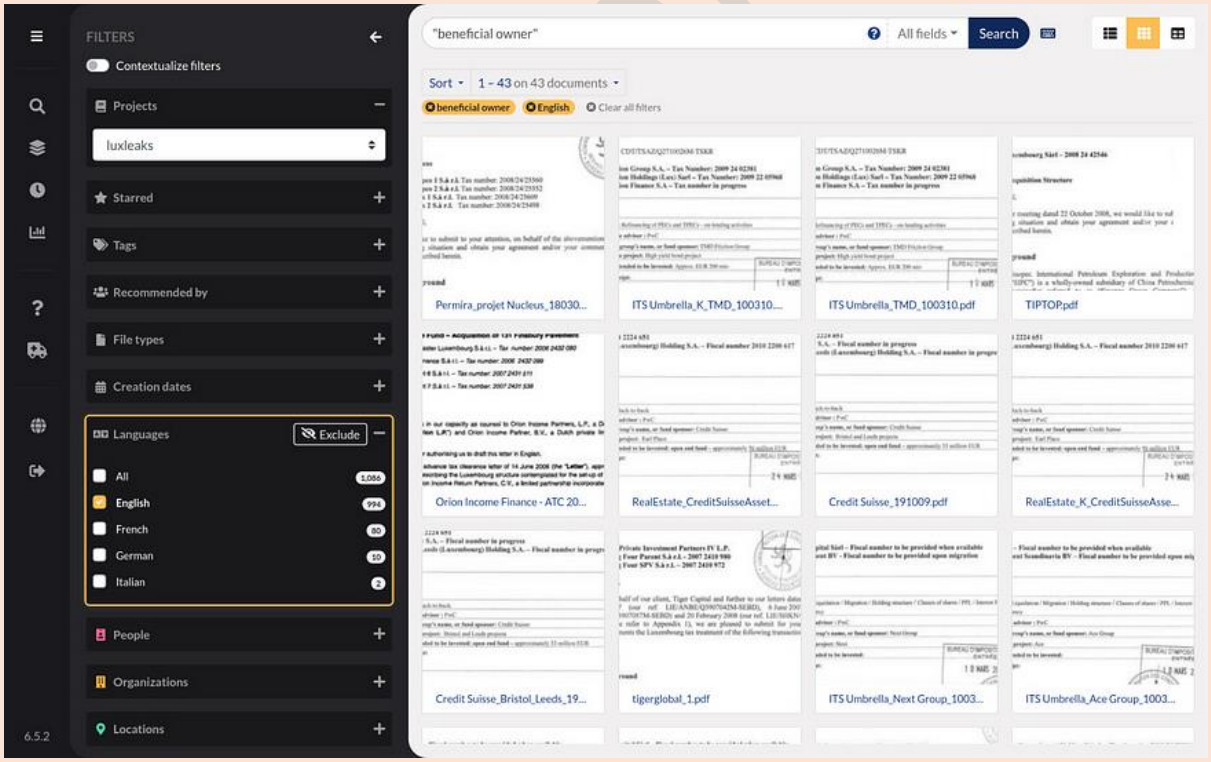
Content Credit: Igor S. Bederov

@viehgroup

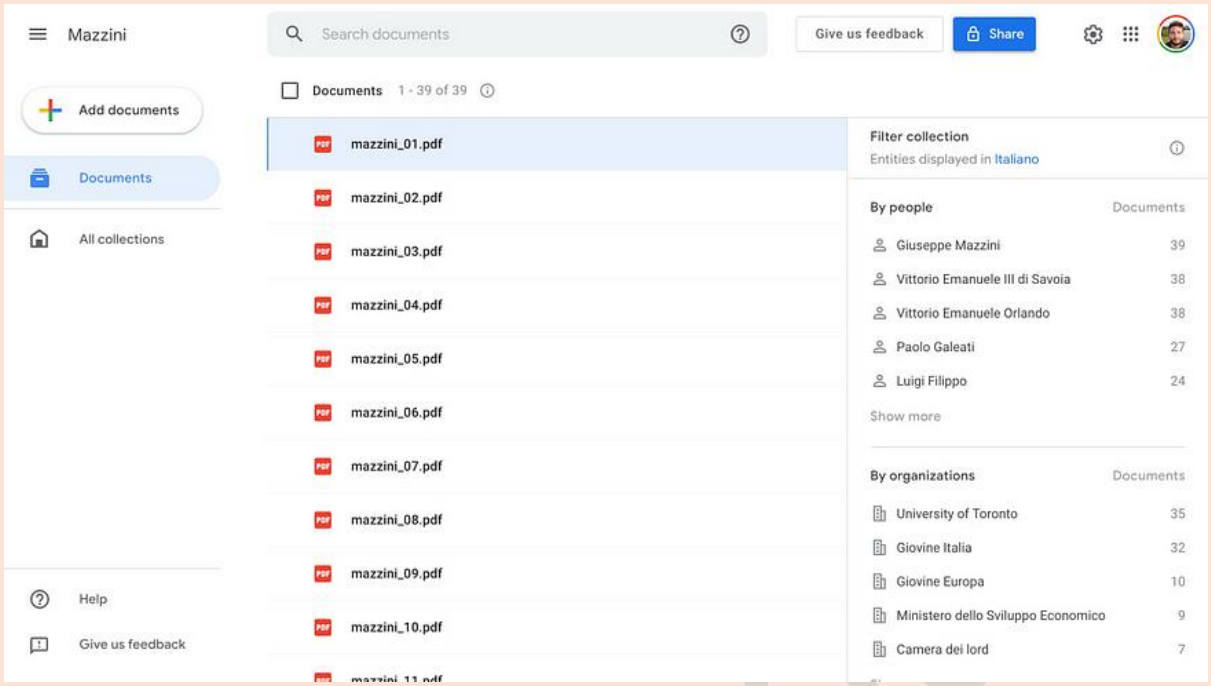
Introduction

In this article, we will look at the tools that are used every day in my work related to the investigation of crimes. Last year was tough but interesting. Some developments stopped working in Russia. Many, on the contrary, were created in our country. Including with my participation. So let's go!

Datashare and Pinpoint



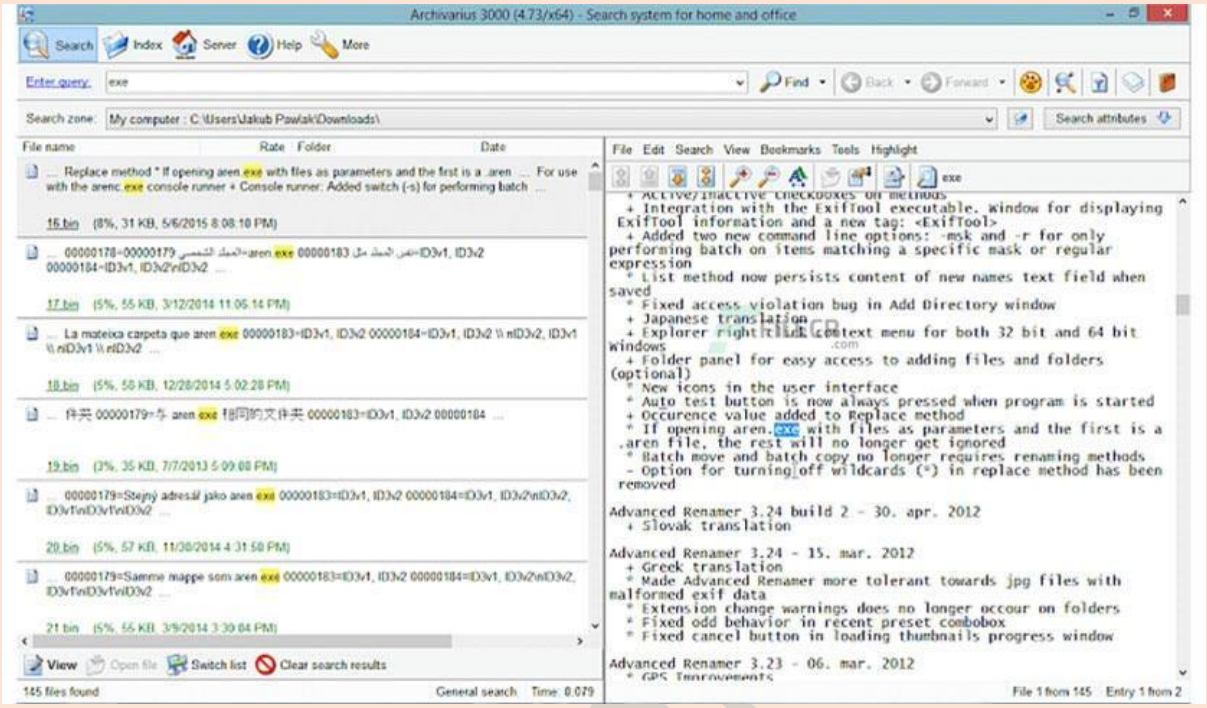
Datashare



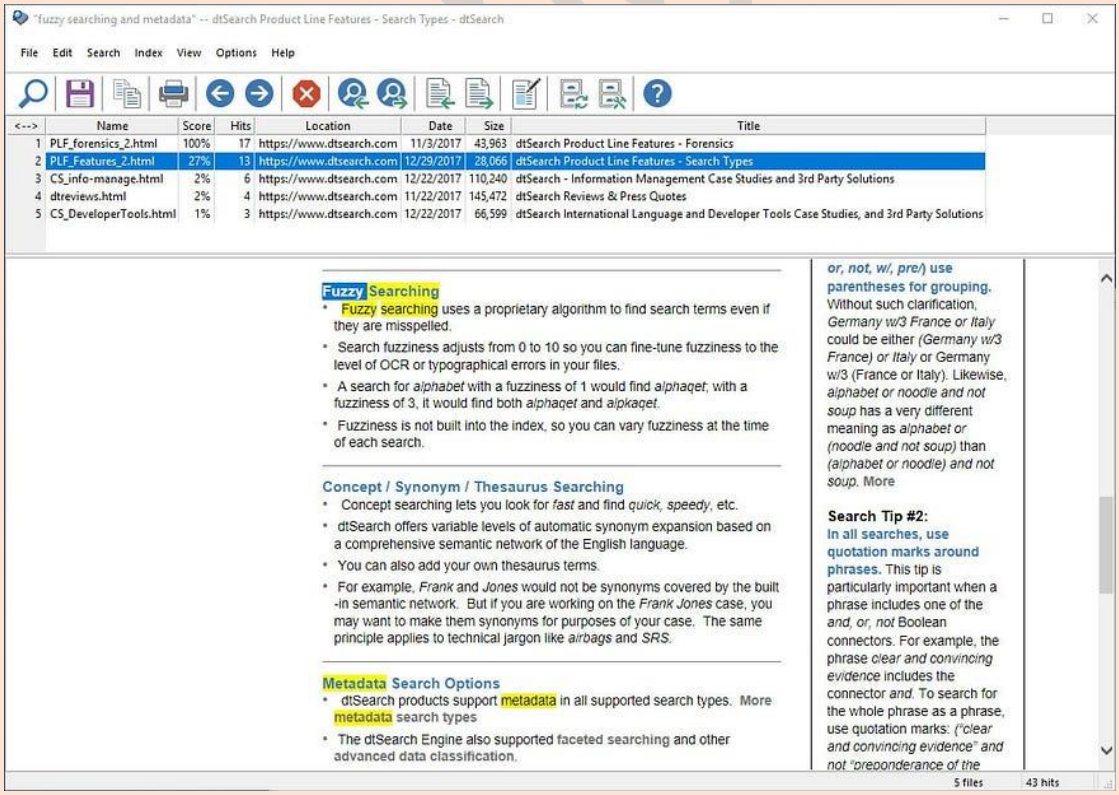
Pinpoint

Datashare and Pinpoint are for eDiscovery… The term is unfamiliar for Russia, so I'll explain it. eDiscovery is the process of identifying, collecting, validating, and analyzing digital evidence. If it is quite simple — the electronic material of the investigation. Compare, 10 volumes of a criminal case or a link to a similar case that can be shared online with external users, and it also has the ability to end-to-end analytics and search through materials. In other words, a must have for the execution of investigations.

Archivarius 3000 and DtSearch



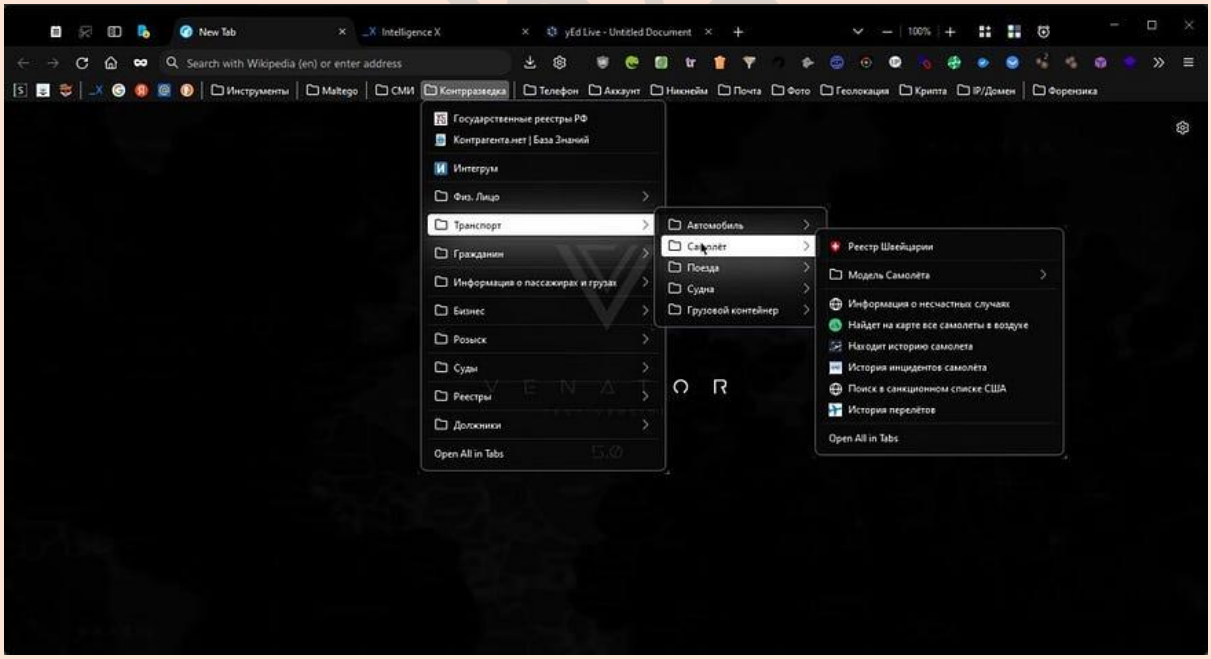
Archivarius 3000



DtSearch

Archivarius 3000 and DtSearch are designed to work with arrays of textual information. They are omnivorous, can read most types of files, and also extract entities from them (nicknames, email addresses, phone numbers, hyperlinks). Allows you to search for information in large amounts of information, including using extended search operators. They also have the functionality to search for information on partial data (for example, by email address or phone number, partially hidden by privacy settings).These two tools can also serve as a means to quickly create a non-relational database.

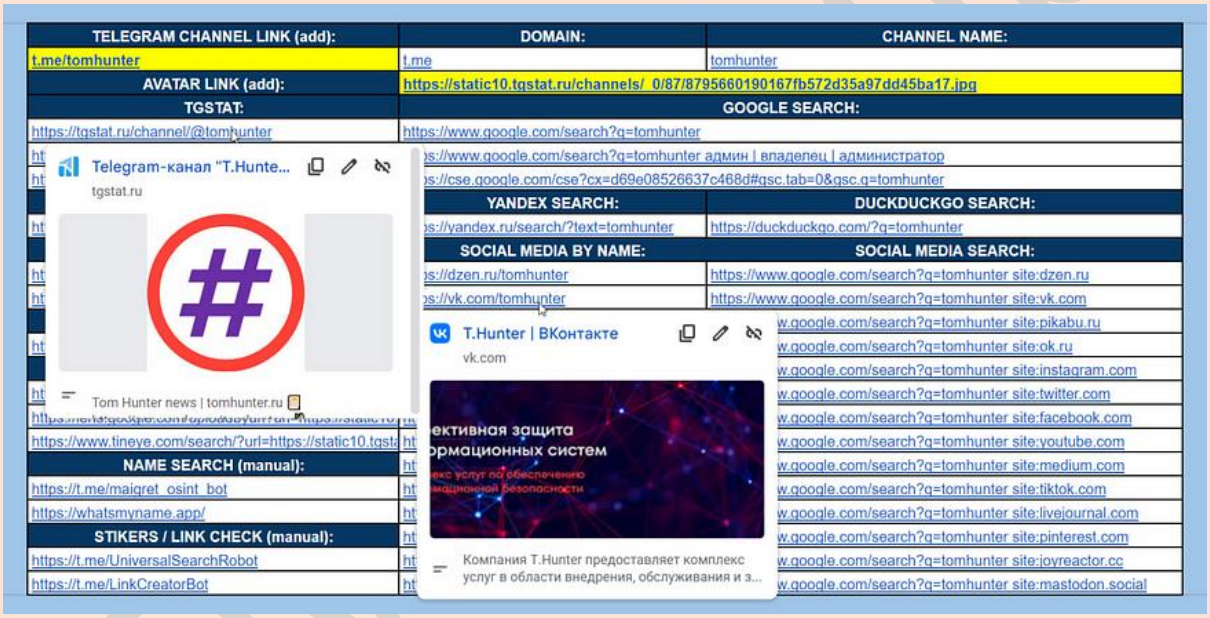
Venator



A multifunctional Venator OSINT browser based on Librewolf (it’s a fork of Firefox with an emphasis on privacy and security). The browser is focused on use in Eastern Europe, which distinguishes it from

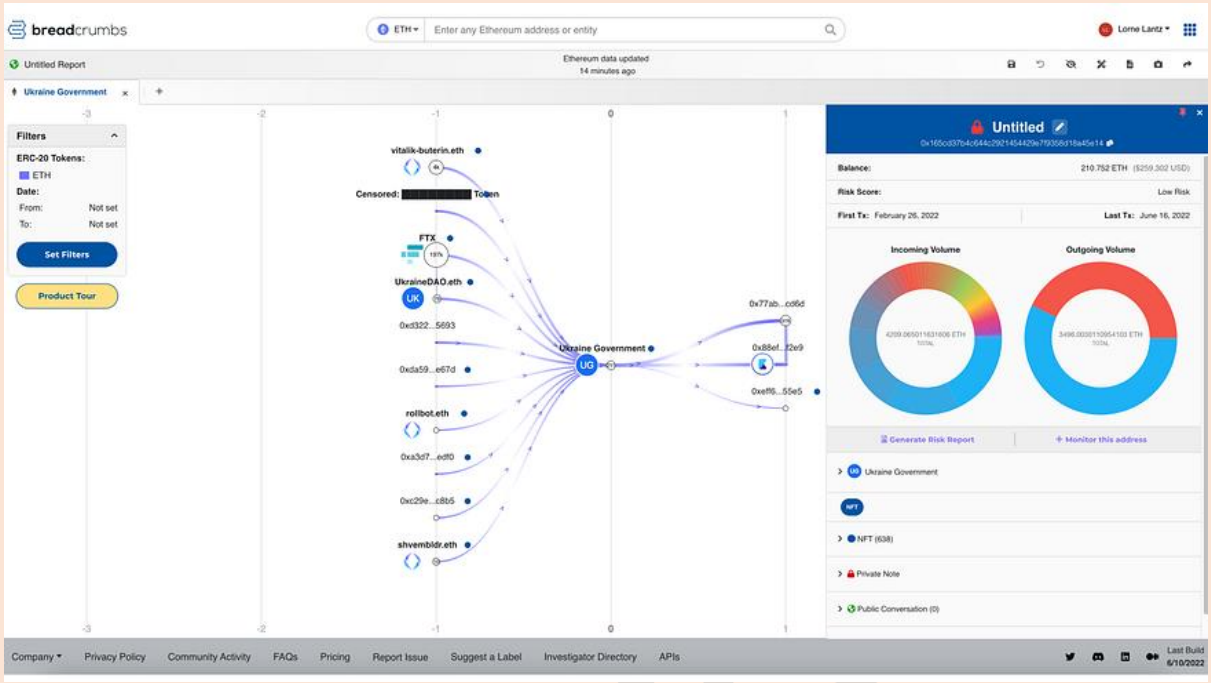
analogues such as Oryon, CSI and others. The browser interface includes additional panels for a quick transition to search engines, as well as to specialized OSINT resources divided by research topics (telephone, mail, nickname, website, etc.).

Spreadsheets

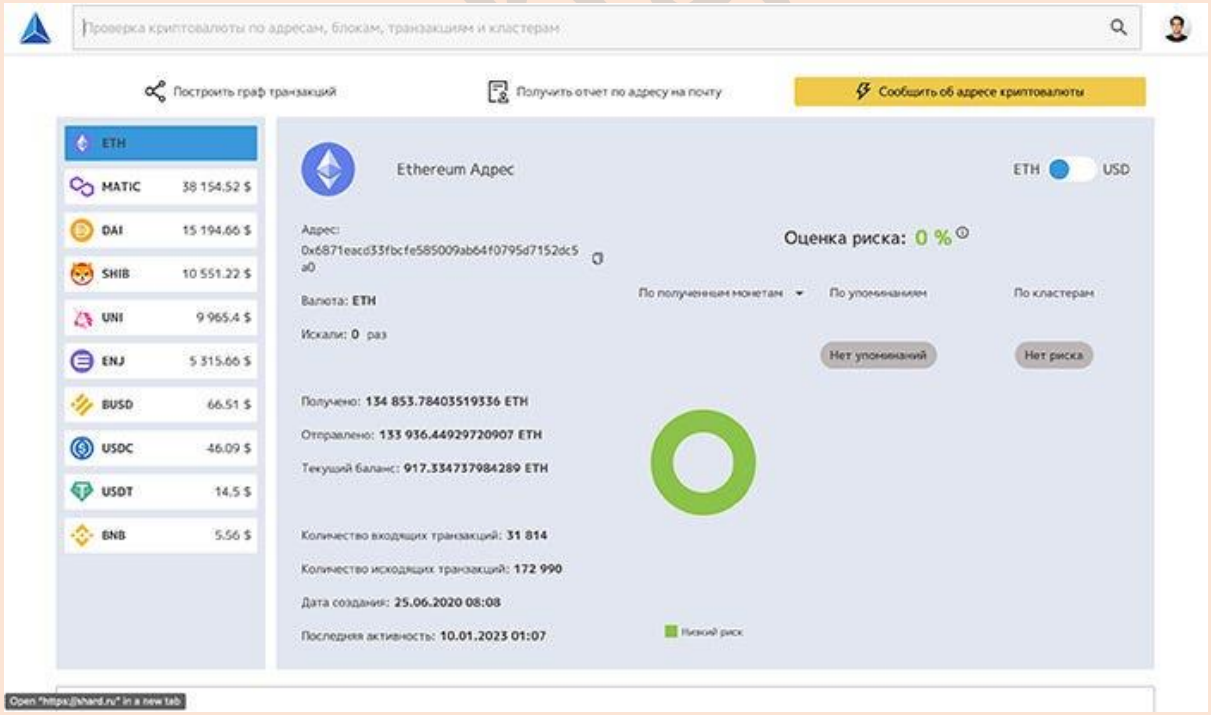


Don’t underestimate the power of Google Sheets. This is a universal tool that allows you to prototype almost any service in terms of collecting data from open sources. Leveraging the Google ecosystem, including dorks, makes Sheets a powerful OSINT tool. Based on it, I personally created a media monitoring system for key queries, a system for identifying Telegram channels, checking e-mail addresses and user nicknames.

Breadcrumbs and Shard



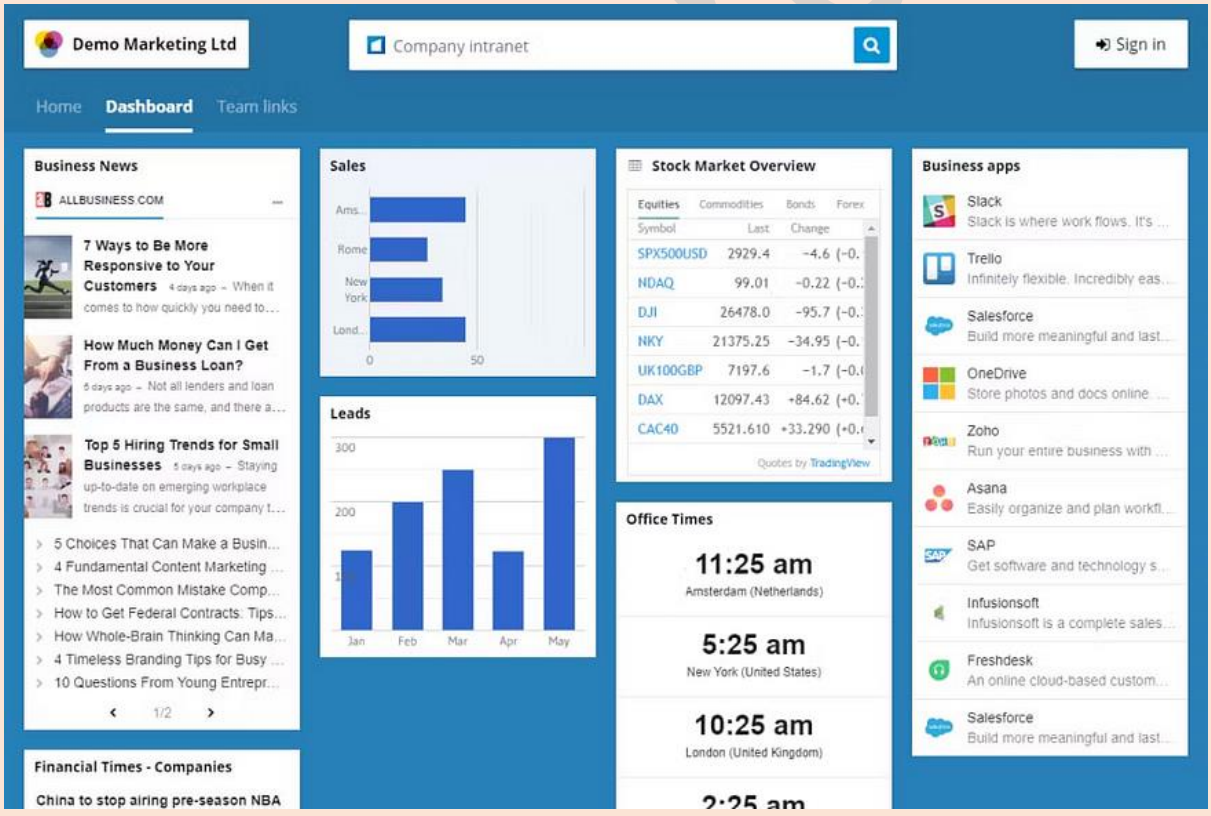
Breadcrumbs



Shard

Breadcrumbs is an analytical platform that allows you to explore the blockchain of individual cryptocurrencies, including functionality for conducting investigations, monitoring, tracking and sharing up-to-date information about blockchain transactions, as well as identifying individual crypto wallets. Closer to the middle of last year, a Russian analogue appeared on the market — the Shard service, which could be connected to at no extra charge.

Start

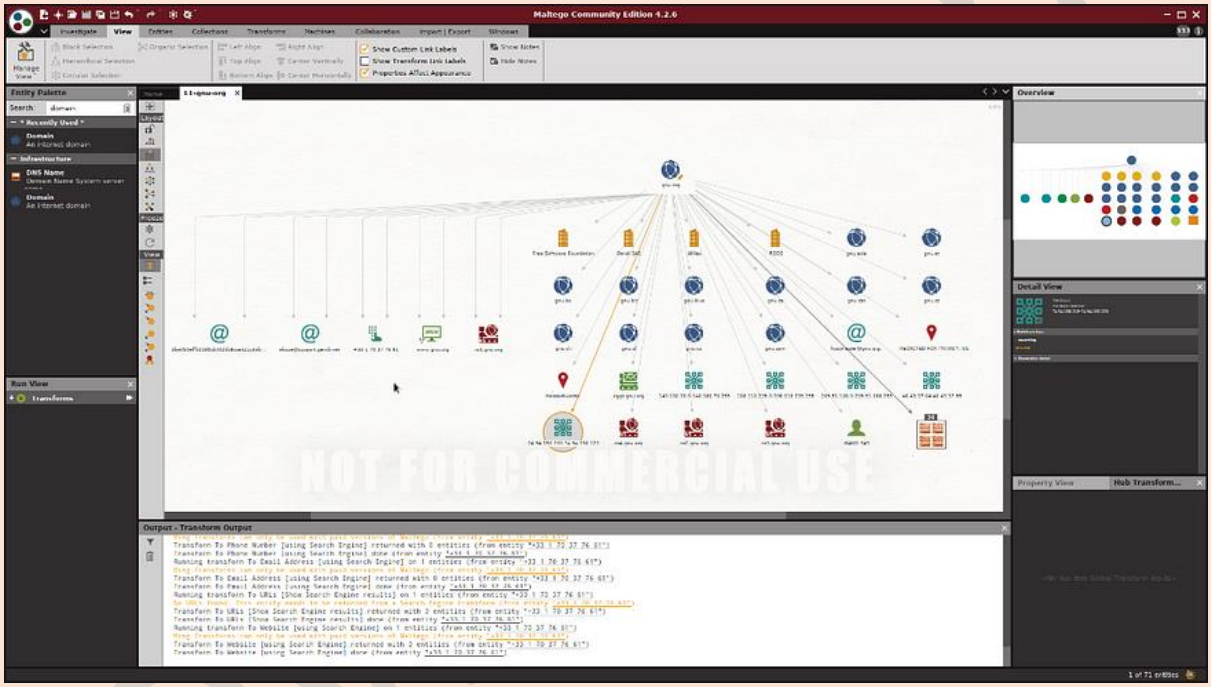


Start

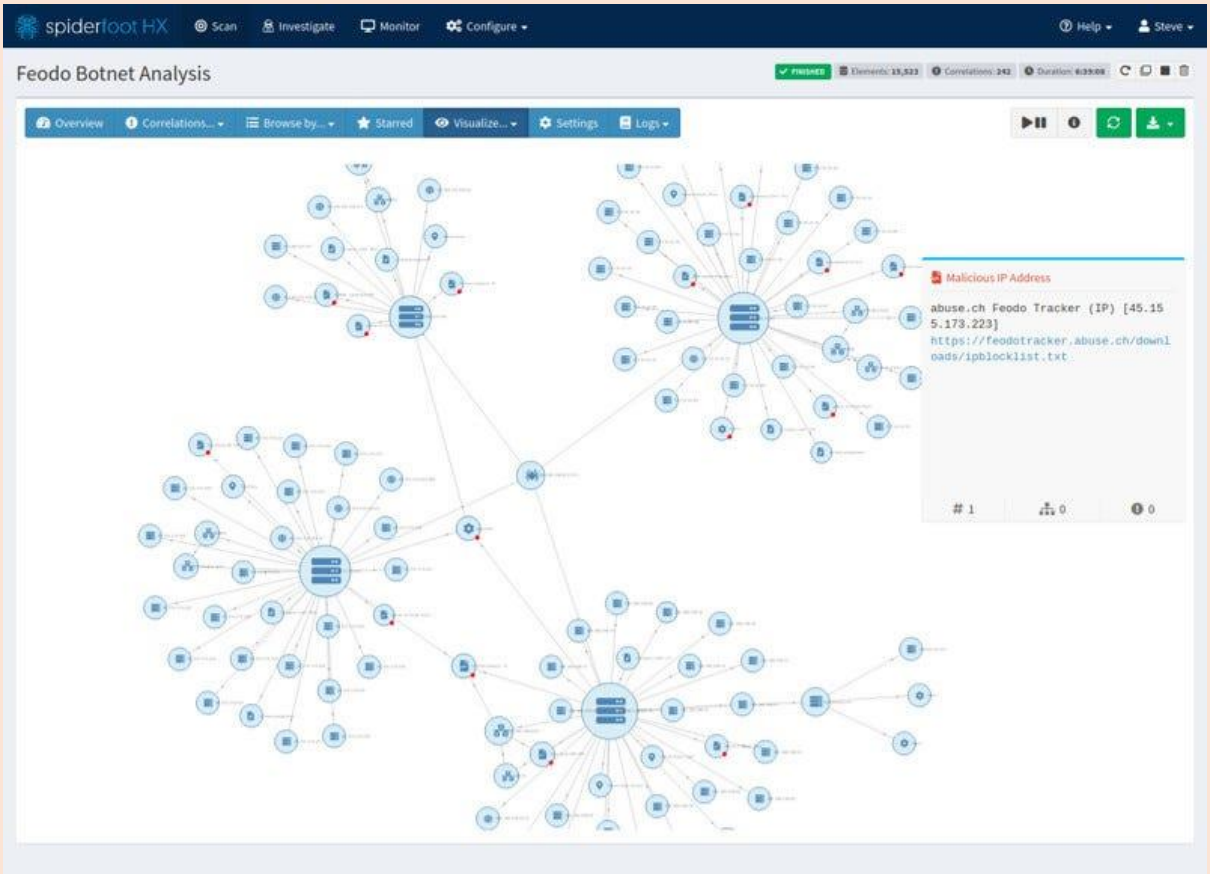
Start is a bookmark manager that is very popular with OSINT experts. In addition to its main task of being a collection of useful resources, the

service can perform the functions of a dashboard, be used to organize network monitoring for key queries, collect RSS feeds, and also be an effective honeypot (cyberdetective trap), since it allows tracking pixels to be placed on its pages.

Maltego and SpiderFoot



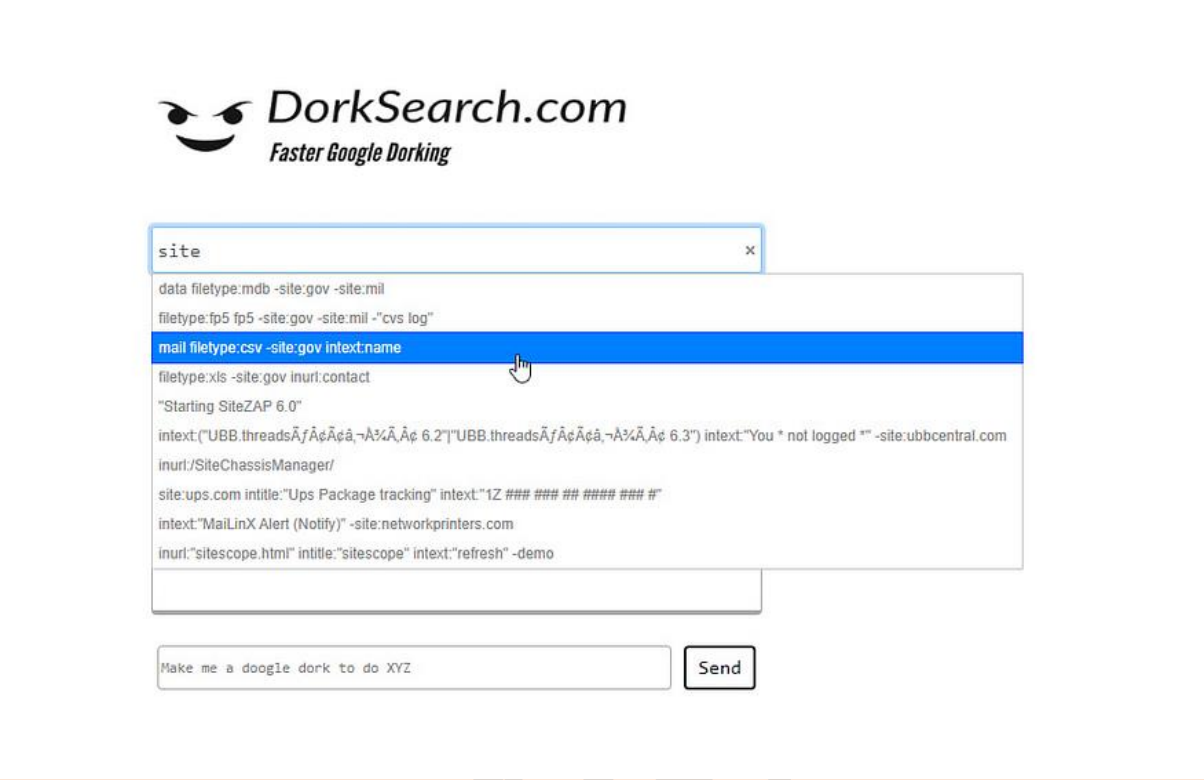
Maltego



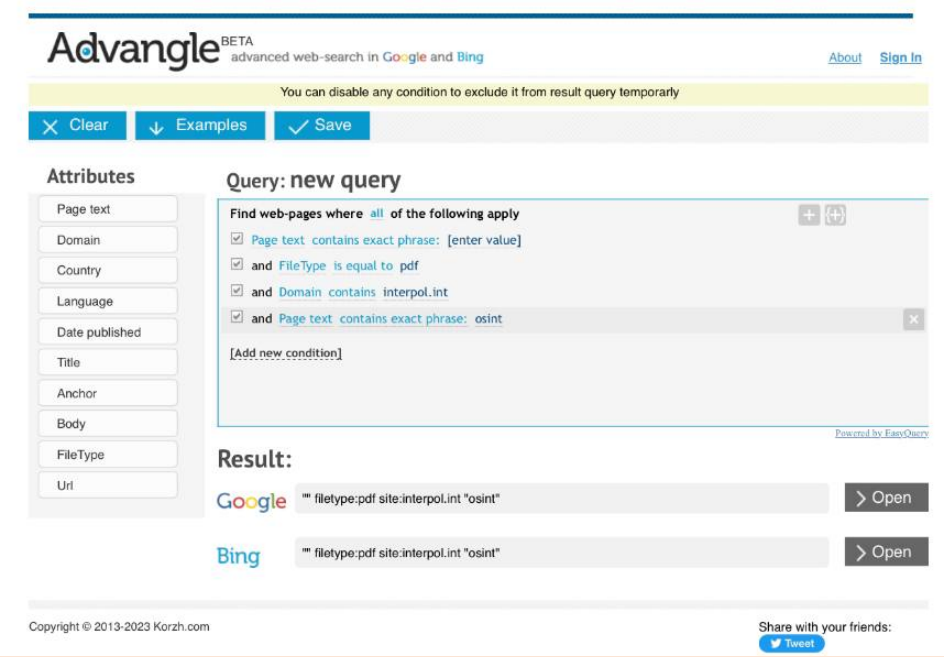
SpiderFoot

Maltego and SpiderFoot are entire software systems for OSINT, which may include other services (by API), as well as databases. Allow connection of own services and data. Despite some antediluvian interfaces (lack of file forensics, timelines and cartographic presentation of data), they allow you to build an investigation graph, as well as transfer it to other users. Depending on the filling of programs with external modules, they can conduct any kind of investigation.

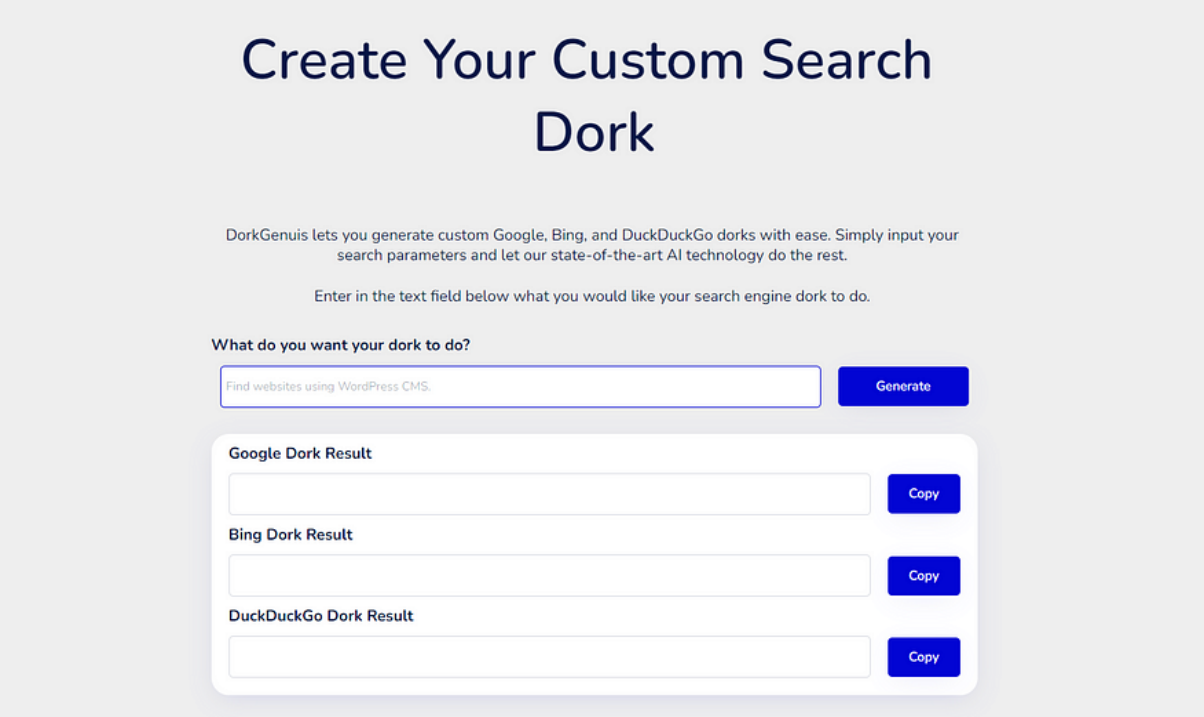
Dork Search, Advangle and DorkGenius



Dork Search



Advangle

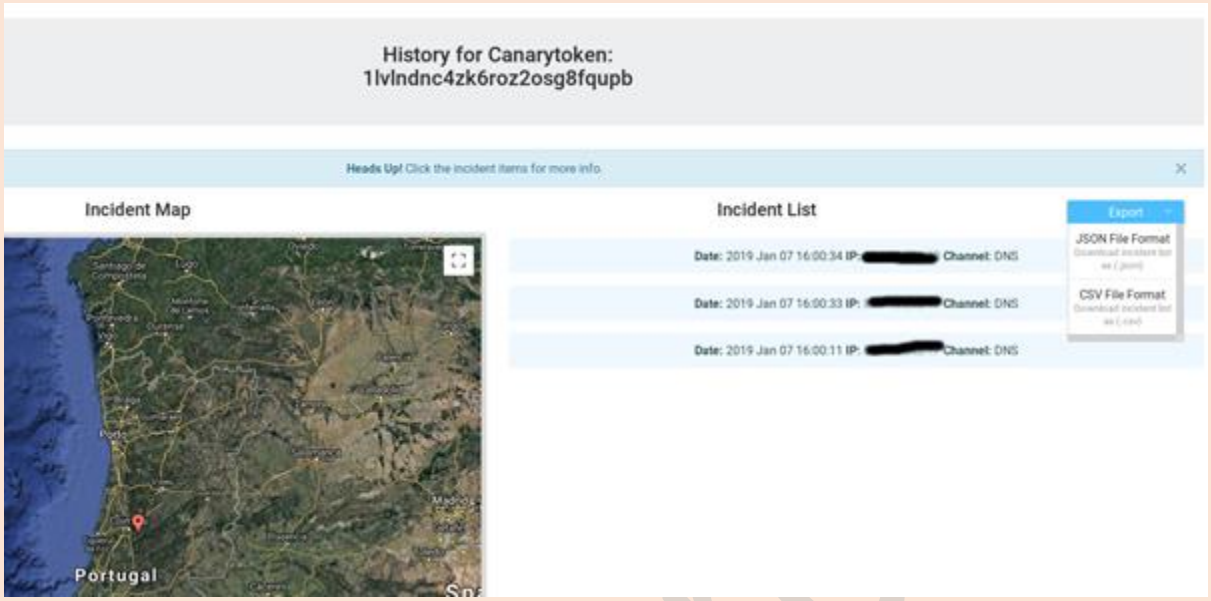


DorkGenius

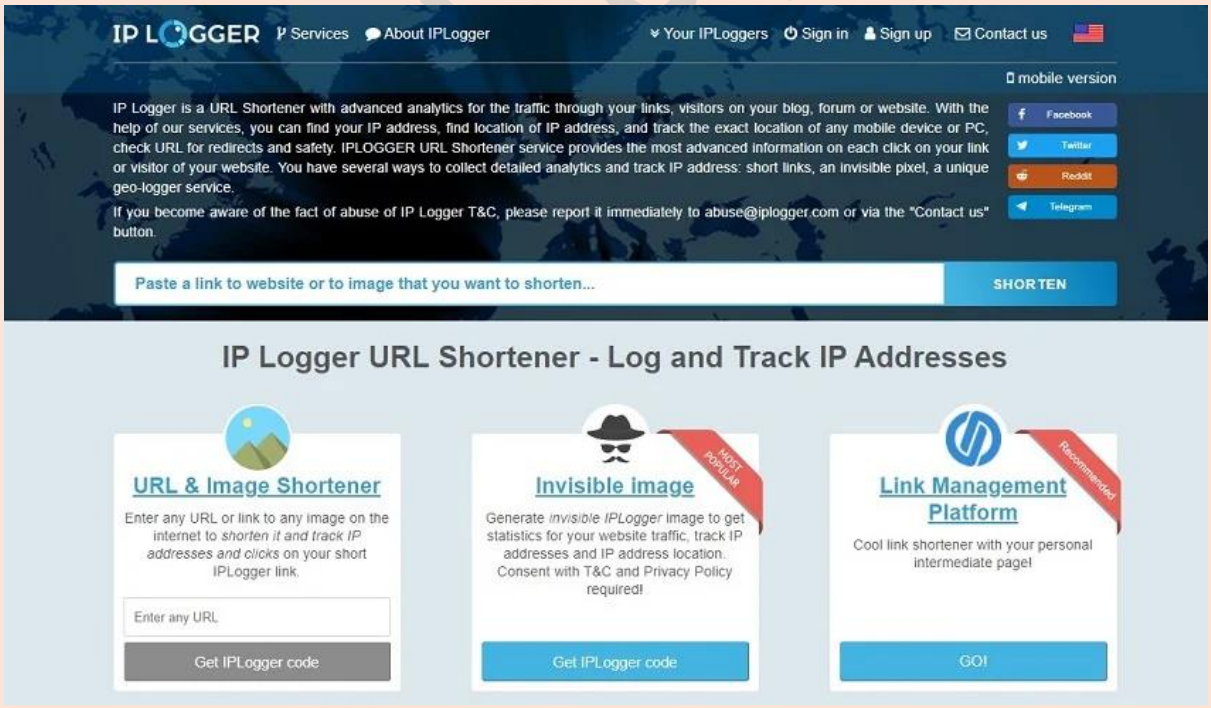
Dork Search is a tool for automating and suggesting advanced search operators (Google Dorks). It is useful not to delve into long manuals and select dorks by the “scientific poke method”. In 2023, I found an alternative service, Advangle, which turned out to be at least as good. Well, besides him, I advise you to try the DorkGenius service, which uses AI to create advanced search

queries for Google, Bing and DuckDuckGo. Now I use all three products in my work.

CanaryTokens and IP Logger



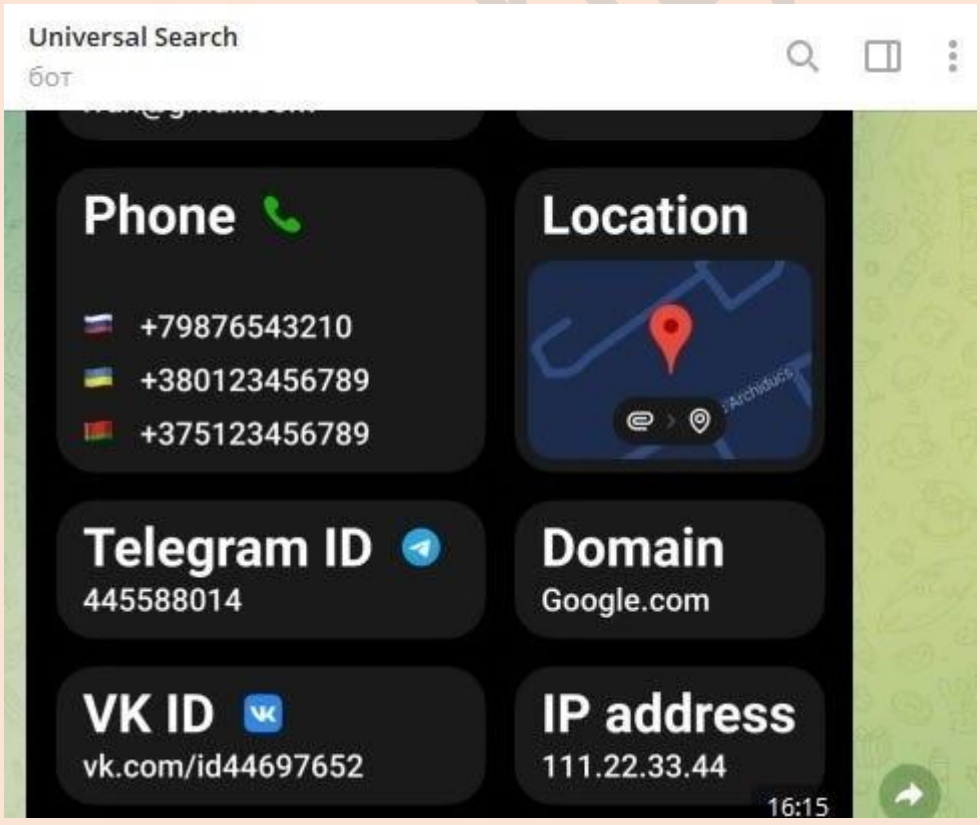
CanaryTokens



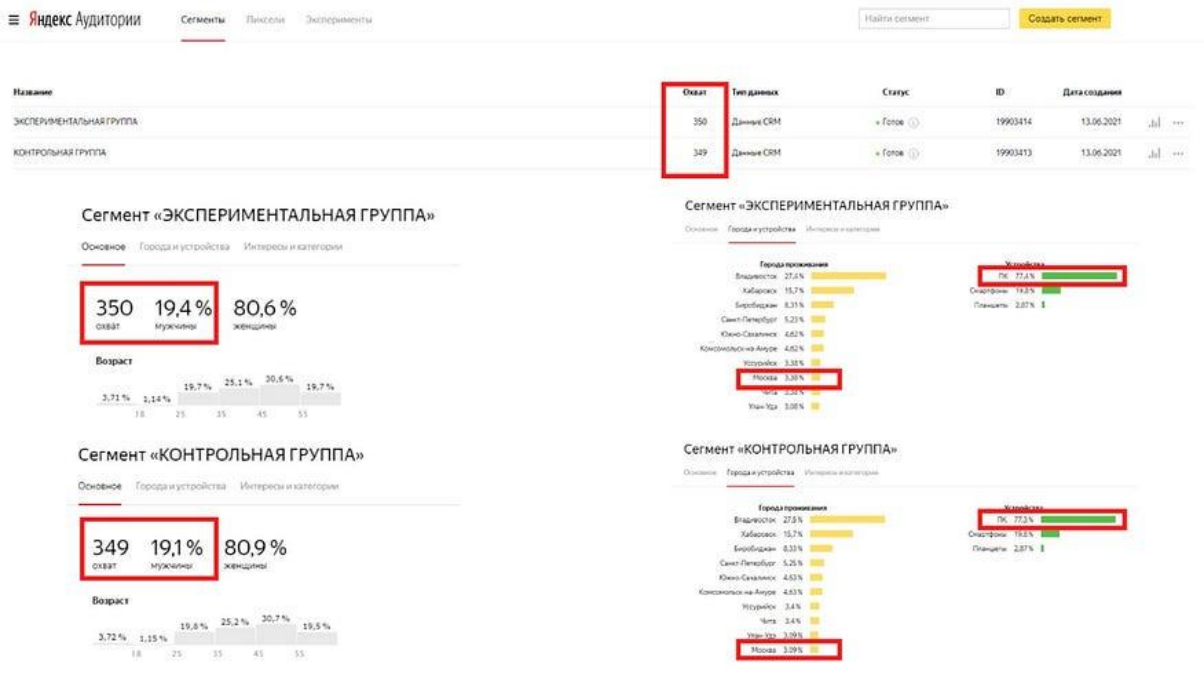
IP Logger

CanaryTokens and IP Logger are popular loggers, that is, services that allow you to get information about the connection and devices of Internet users. They are the basis for creating the simplest honeypots in the form of a hyperlink, an image, an email, a document, an invisible pixel, and even a credit card. Over the past year, both services have significantly added functionality. Now they allow the collection of a complete digital fingerprint of users, which increases the effectiveness of their use for the investigation of crimes, as well as in active OSINT events.

Universal Search and Yandex.Audience



Universal Search



Yandex.Audience

And finally, I also cannot fail to mention these tools in the selection. Universal Search collects and automates various OSINT methods. And it does it so well that young professionals using it in their work give the impression of experienced gurus. Yandex.Audience is a promising domestic tool for ADINT (advertising identifier intelligence). ADINT allows you to get a social graph and track movements by email address, phone number, MAC address, and identifiers of iOS and Android operating systems.

Thanks for reading

@viehgroup