This project is funded by the European Union

EU4JUSTICE

EXPERTISE FRANCE

This project is implemented by Expertise France

OSINT quick reference guide

Contents

Muhameda Kantardžića 3/3, 71000 Sarajevo, Bosnia and Herzegovina
www.eu4justice.ba info@eu4justice.ba +387 33 879 911 +387 33 879 916

Introduction

OSINT is an intelligence-gathering method used to collect and analyze publicly available information and data for investigative purposes. OSINT data sources encompass pretty much anything you can find on the internet, from an IP address to public governmental records.

OSINT techniques are practised by all sorts of investigators and analysts across a range of industries—cybersecurity operations analysts, law enforcement officers, fraud investigators, threat hunters, researchers, investigative journalists, and many more. The EU for justice project organized two pieces of training (April and May 2021) for project beneficiaries in Bosnia and Herzegovina on OSINT Essentials.

The training discussion was focused on:

- Search engines, people search;
- Methodology, public registers; and
- Data quality, geolocation.

The use of OSINT methodology for investigations can be applied without the immediate need for coercive measures which contributes to the proportionality and subsidiarity of investigations. Meanwhile, the amount of information available in open sources which can be leveraged for nearly every investigation is significant which will enhance the efficiency of the investigation and prosecution of organised crime and corruption cases.

This short reference guide contains the insights for research in open sources as discussed during the online rounds of the EU4Justice OSINT Essentials training. The guide is meant to be used as a quick *aide-memoire*, it is not a comprehensive guide.

The experts who shared their knowledge and experience were Mr Ludo Block and Mr Bert Jan Beneker.

Mr. Ludo Block who is an independent investigation and intelligence consultant and an associate partner at Grant Thornton Advisory in Slovenia. He started his career in 1987 in the Netherlands' police where he became a Detective Chief Inspector. From 1999 to 2004 he served in Moscow as the Netherlands' police liaison officer for Russia and surrounding countries. In 2004 he moved to the private sector and since has been conducting investigations and intelligence projects for corporates, international organizations, governments, and NGOs worldwide. Between 2010 and 2020 he was director of forensics at Grant Thornton in the Netherlands. He obtained a PhD at the Vrije Universiteit Amsterdam (2011) based on his research into the effects of EU Council policymaking on the actual practices of cross-border police cooperation in the EU.

Mr Bert Jan Beneker, who is a University of Amsterdam graduate (LL.M.) and has worked as a candidate civil-law notary for over 15 years, specializing in real estate transactions and corporate law. His clients included multinational corporations and high-net-worth individuals. In 2012 Bert Jan joined the Dutch police force as a real estate fraud and money laundering specialist. He has extensive experience in intelligence and investigations with a focus on complex money laundering schemes, AML/CFT regulation, data analytics and OSINT. He provides training and consultancy services to the law enforcement community and various stakeholders.

Muhameda Kantardžića 3/3, 71000 Sarajevo, Bosnia and Herzegovina
www.eu4justice.ba info@eu4justice.ba +387 33 879 911 +387 33 879 916

Before you start

- Make sure you understand your legal position and have the proper authorisations in place if and where needed to perform the OSINT work for your investigation;
- Never use personal (social media) accounts for work-related searches;
- Be aware of the traces you may leave when searching;
- Be aware of the limitations of data from open sources and the implications those may have for the validity of your findings and admissibility of the findings as evidence;
- Be prepared to answer any question about the methodology and tools used.

Search engines

Always try your searches on multiple search engines such as www.google.com, www.yandex.com, www.bing.com and perhaps a local one. When using Google (or another search engine):

- Make proper queries with the right keyword(s);
- Use the advanced search options;
- Think about the Google search operators to make your searches even more precise. See for an overview: https://ahrefs.com/blog/google-advanced-search-operators/;
- Start always on the last page of the results and work your way back;
- Use additional keywords which are relevant to your subject to unlock other parts of the Google index, see https://www.blockint.nl/methods/how-less-is-more-advanced-google-searching/

People searches

In investigations data from open sources is helpful when we are searching for people to either establish their true identity or to establish their activities and connections. Key tips to remember:

- For searches on Facebook either use the search options on the platform itself or use www.graph.tips/beta/
- For searching people on LinkedIn the best link is: https://www.linkedin.com/search/results/people/?firstName=&origin=FACETED_SEARCH
- When searching on Twitter make use of the special Twitter operators which can be found here: https://developer.twitter.com/en/docs/twitter-api/v1/rules-and-filtering/search-operators and also consider using tweetdeck.twitter.com;
- Take good note of usernames, often these reveal something about the user;
- People often (re)use their usernames on multiple social media platforms as well as in their email address. Therefore, check the username on for example knowem.com, namevine.com or whatsmyname.app to see on what other platforms the username is also used. Be sure to verify that it is the same person;
- Search in TikTok via https://www.osintcombine.com/tiktok-quick-search

Muhameda Kantardžića 3/3, 71000 Sarajevo, Bosnia and Herzegovina
www.eu4justice.ba info@eu4justice.ba +387 33 879 911 +387 33 879 916

Breach Data

All major social media platforms and many other companies had their user data leaked into the public. Examples are LinkedIn, Facebook and very recently Clubhouse. Several websites can be searched to see if a username or email address has been leaked and what other data is available that may be interesting for the investigation. Sites to check are:

- https://haveibeenpowned.com
- https://dehashed.com
- https://intelx.io
- https://leakpeek.com

Regional company registers

- Albania – https://qkb.gov.al/search/search-in-trade-register/search-for-subject/
- Bosnia and Herzegovina – https://bizreg.pravosudje.ba
- Bulgaria – https://portal.registryagency.bg/CR/Reports/VerificationPersonOrg
- Croatia – https://sudreg.pravosudje.hr
- Kosovo – https://arbk.rks-gov.net/
- Macedonia – http://www.crm.org.mk/
- Montenegro – http://www.pretraga.crps.me:8083/
- Romania – https://portal.onrc.ro/ONRCPortalWeb/ONRCPortal.portal
- Serbia – https://pretraga2.apr.gov.rs/unifiedentitysearch
- Slovenia – https://www.ajpes.si/prs/

Global databases with company data

- Open corporates – https://opencorporates.com/
- Dato Capital – https://en.datocapital.com/
- Cedar Rose – https://www.cedar-rose.com/
- Info Clipper – http://www.info-clipper.com/en/
- Dun and Bradstreet – https://www.dnb.com/
- Offshore Leaks – https://offshoreleaks.icij.org/
- EU overview of registers – https://beta.e-justice.europa.eu/contentPresentation.do?clang=en&idTaxonomy=489
- Overview of registers – https://opencorporates.com/registers or https://ebra.be/worldwide-registers/
- Overview of EU UBO registers – https://www.blockint.nl/kyc/ubo-registers-in-the-eu/

Research methodology

- Always start from a concrete answerable question;
- Make a plan based on what is already known;
- Document not only findings but also the metadata and process followed;
- Use Notepad and the ‘F5’ key for quick note-taking while researching;

Muhameda Kantardžića 3/3, 71000 Sarajevo, Bosnia and Herzegovina
www.eu4justice.ba info@eu4justice.ba +387 33 879 911 +387 33 879 916

- Use the screenshot function in Firefox or a plugin in Chrome to exactly capture what was visible, use pdf printing to retain the metadata;
- Consider saving webpages (also) on archive.org;
- Consider using mind map software for documenting your research process, like https://www.xmind.net/
- Consider using Hunchly (paid tool) if OSINT investigations are a full-time task – see https://www.hunch.ly/

Directories (source overviews)

Some OSINT experts have made collections of relevant sources for all kinds of investigations. Use these to your advantage:

- https://osintframework.com/
- https://start.me/p/ZME8nR/osint
- https://start.me/p/7kxyy2/osint-tools-curated-by-lorand-bodo
- https://start.me/p/rxeRqr/aml-toolbox
- https://technisette.com/p/home

Geolocation

3-step process to geolocation if the Exif data does not reveal the location:

1) Extract all data from the photo: describe what you see on the photo (e.g., objects, landscape, structures, weather, climate, vegetation, orientation), check and note meta-data, note the circumstances and source of the photo;
2) Search: start with reverse image searching in different search engines, use keyword and colour filtering in Google, search for parts of the photo, search for the same type of objects, use other image sources (e.g., Instagram, Flickr, Imgur, LiveJournal)
3) Verify: once a likely location has been found, try to obtain at least 3 data points that confirm the location (satellite, street view, user-generated content)

Tools for geolocation:

- http://exif.regex.info/exif.cgi
- images.google.com, yandex.ru/images, bing.com, tineye.com
- http://data.mashedworld.com/dualmaps/map.htm
- https://mapillary.com
- https://overpass-turbo.eu
- https://www.instantstreetview.com
- https://www.cellmapper.net

Extensions

Extensions are additions (addons) to your web browser which help you to efficiently perform certain tasks. Below we list a number of the often-used extensions for OSINT work.

Function	Firefox	Chrome
Screenshot	built-in	GoFullPage
Find EXIF information in images online or on your computer	Exif Viewer	EXIF Viewer Pro
Download multiple links from a website	Simple mass downloader	Batch link downloader
Verification tool for video and images	*not available*	InVid WeVerify
Quickly scrape lists from webpages (such as followers) and export in csv	*not available*	Instant Data Scraper
Obtain IP and domain information on the webpage you visit with one click	IP Address and Domain Information	IP Address and Domain Information
Search the page in the Internet Archive or save it there.	Wayback Machine	Wayback Machine
Collapse all open tabs into one page	OneTab	OneTab
Reverse image search in multiple engines at once	RevEye Reverse Image Search	RevEye Reverse Image Search

Muhameda Kantardžića 3/3, 71000 Sarajevo, Bosnia and Herzegovina
www.eu4justice.ba info@eu4justice.ba +387 33 879 911 +387 33 879 916