Ovaj projekat finansira Evropska unija

EU4JUSTICE

EXPERTISE FRANCE
Ovaj projekat implementira Expertise France

Kratki vodič za OSINT

Uvod

Ovaj kratki referentni vodič sadrži uvide za pretraživanje otvorenih izvora o kojima se raspravljalo tokom online radionica koje je organizirao projekt EU4Justice na temu *Osnove o OSINT-u* u aprilu i maju 2021. godine. Vodič je zamišljen da posluži kao brzi podsjetnik, a ne kao sveobuhvatni vodič.

Prije nego što započnete

- Provjerite razumijete li svoj pravni položaj i imate li potrebna ovlaštenja ukoliko želite i trebate pretraživati podatke iz otvorenih izvora za svoju istragu;
- Nikad nemojte koristiti lične račune (profile na društvenim mrežama) za pretraživanje koje se tiče vašeg posla;
- Budite svjesni tragova koje ostavljate prilikom pretraživanja;
- Budite svjesni ograničenja podataka iz otvorenih izvora i implikacija koje ti podaci mogu imati na valjanost vaših nalaza i prihvatljivost nalaza kao dokaza;
- Budite spremni odgovoriti na svako pitanje o metodologiji i korištenim alatima.

Pretraživači

Ono što pretražujete uvijek probajte naći na više pretraživača, npr. www.google.com, www.yandex.com , www.bing.com a možda i na nekim lokalnim. Kada upotrebljavate Google (ili drugi pretraživač):

- Ispravno unesite tražene pojmove koristeći prave ključne riječi;
- Koristite napredne opcije pretraživanja;
- Razmislite o Googleovim operatorima pretraživanja (Booleovi operatori) kako bi vaša pretraživanja bila što preciznija. Pregled operatora možete naći na: https://ahrefs.com/blog/google-advanced-search-operators/;
- Uvijek krenite s posljednje stranice rezultata i vraćajte se unatrag;
- Koristite dodatne ključne riječi koje su relevantne za vašu temu da biste otključali druge dijelove Googleovog indeksa. Za više informacija pogledajte https://www.blockint.nl/methods/how-less-is-more-advanced-google-searching/

Pretraživanje osoba

U istragama su podaci iz otvorenih izvora korisni kada tražimo ljude kako bismo utvrdili njihov pravi identitet ili njihove aktivnosti i veze. U nastavku je nekoliko ključnih savjeta koje treba imati na umu:

Muhameda Kantardžića 3/3, 71000 Sarajevo, Bosna i Hercegovina
www.eu4justice.ba info@eu4justice.ba +387 33 879 911 +387 33 879 916

- Kod pretraživanja na Facebooku, koristite opciju pretraživanja na samoj platformi ili koristite www.graph.tips/beta/
- Kod pretraživanja na LinkedInu, najbolja poveznica je: https://www.linkedin.com/search/results/people/?firstName=&origin=FACETED_SEARCH
- Kada pretražujete na Twitteru, koristite posebne Twitter operatore koje možete pronaći ovdje: https://developer.twitter.com/en/docs/twitter-api/v1/rules-and-filtering/search-operators , a razmislite i o tweetdeck.twitter.com;
- Posebno obratite pažnju na korisnička imena jer ona često govore nešto o korisniku;
- Ljudi često (iznova) koriste ista korisnička imena na više platformi društvenih mreža, kao i u svojim e-mail adresama. Stoga, provjerite korisničko ime, naprimjer, na *knowem.com, namevine.com ili whatsmyname.app* kako biste provjerili koristi li se isto korisničko ime na nekim drugim platformama. Pri tome, svakako provjerite radi li se zaista o istoj osobi;
- Pretražite TikTok-u putem https://www.osintcombine.com/tiktok-quick-search

Podaci koji su procurili u javnost

Svim većim platformama društvenih medija, ali i mnogim drugim kompanijama, dešavalo se da im korisnički podaci procure u javnost. To se dešavalo LinkedIn-u, Facebook-u, a nedavno i Clubhouse-u. Postoji niz internetskih stranica koje se mogu pretraživati kako bi se vidjelo je li procurilo neko korisničko ime ili e-adresa i koji su drugi podaci dostupni koji bi mogli biti zanimljivi za istragu. Stranice koje treba provjeriti su:

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

Regionalni registri kompanija

- Albanija - https://qkb.gov.al/search/search-in-trade-register/search-for-subject/
- Bosna i Hercegovina– https://bizreg.pravosudje.ba
- Bugarska - https://portal.registryagency.bg/CR/Reports/VerificationPersonOrg
- Hrvatska - https://sudreg.pravosudje.hr
- Kosovo - https://arbk.rks-gov.net/
- Makedonija - http://www.crm.org.mk/
- Crna Gora - http://www.pretraga.crps.me:8083/
- Rumunija - https://portal.onrc.ro/ONRCPortalWeb/ONRCPortal.portal
- Srbija - https://pretraga2.apr.gov.rs/unifiedentitysearch
- Slovenija - https://www.ajpes.si/prs/

Globalne baze podataka s podacima o kompanijama

- 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/
- Pregled registara EU – https://beta.e-justice.europa.eu/contentPresentation.do?clang=en&idTaxonomy=489
- Pregled registara - https://opencorporates.com/registers ili https://ebra.be/worldwide-registers/
- Pregled registara EU o stvarnim korisnicima - https://www.blockint.nl/kyc/ubo-registers-in-the-eu/

Metodologija pretraživanja

- Uvijek pođite od konkretnog pitanja na koje se može dobiti odgovor;
- Napravite plan na temelju onoga što je već poznato;
- Dokumentirajte ne samo nalaze, već i metapodatke i postupak koji ste slijedili;
- Koristite funkciju *Notepad* i tipku *'F5'* za brze bilješke prilikom pretraživanja;
- Koristite funkciju *Screenshot* u Firefoxu ili dodatak u Chromeu da biste tačno snimili ono što je bilo vidljivo, i koristite funkciju *pdf printing* da biste zadržali metapodatke;
- Razmislite o tome da internetske stranice spasite i u arhivi na archive.org;
- Razmislite o korištenju softvera umnih mapa za dokumentiranje svog procesa istraživanja, naprimjer https://www.xmind.net/
- Razmislite o korištenju Hunchly-a (alata koji se plaća), ako je pretraživanje otvorenih izvora zadaća koju radite puno radno vrijeme - vidi https://www.hunch.ly/

Direktoriji (pregledi izvora)

Mnogi stručnjaci koji se bave OSINT-om napravili su zbirke relevantnih izvora za sve vrste istraga. Iskoristite ih:

- 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

Geolokacija

Proces u 3 koraka do geolokacije ako Exif podaci ne otkrivaju lokaciju:

1) **Izdvojite** sve podatke s fotografije: opišite ono što vidite na fotografiji (npr. predmete, krajolik, strukture, vrijeme, klimu, vegetaciju, orijentaciju), provjerite i zabilježite metapodatke, zabilježite okolnosti i izvor fotografije;

2) **Pretraga**: Započnite s pretraživanjem obrnutih slika u različitim pretraživačima, koristite filtriranje ključnih riječi i boja na Googleu, potražite dijelove fotografije, potražite iste vrste objekata, upotrijebite druge izvore slika (npr. Instagram, Flickr, Imgur, LiveJournal)
3) **Provjera**: Kada pronađete vjerojatnu lokaciju, pokušajte dobiti najmanje 3 podatkovne tačke koje potvrđuju lokaciju (satelit, prikaz ulice, sadržaj koji su generirali korisnici)

Alati za geolociranje:

- 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

Proširenja

Proširenja ili ekstenzije su dodaci vašem internetskom pregledniku koji vam pomažu da učinkovitije izvršavate određene zadatke. U nastavku navodimo listu najčešće korištenih ekstenzija za rad s OSINT-om.

Funkcija	**Firefox**	**Chrome**
Screenshot [snimi zaslon]	Built-in	GoFullPage
Find EXIF information in images online or on your computer [Pronađi EXIF informacije na slikama na internetu ili na kompjuteru]	Exif Viewer	EXIF Viewer Pro
Download multiple links from a website [Preuzmi više poveznica s internetske stranice]	Simple mass downloader	Batch link downloader
Verification tool for video and images [Alat za provjeru slika i vodeozapisa]	*nije dostupno*	InVid WeVerify
Quickly scrape lists from webpages (such as followers) and export in csv [Brzo preuzmi s liste internetskih stranica (npr. Sljedbenike) i prenesi ih u csv. format]	*nije dostupno*	Instant Data Scraper

Obtain IP and domain information on the webpage you visit with one click [jednim klikom dohvati podatke o IP-u i domeni na web stranici koju posjetite]	IP Address and Domain Information	IP Address and Domain Information
Search the page in the Internet Archive or save it there. [Pretraži stranicu u arhivi interneta ili pohrani stranicu u arhivu]	Wayback Machine	Wayback Machine
Collapse all open tabs into one page [Prebaci sve otvorene tabulatore na jednu stranicu]	OneTab	OneTab
Reverse image search in multiple engines at once [istovremeno pretraži obrnute slike na više pretraživača]	RevEye Reverse Image Search	RevEye Reverse Image Search

Muhameda Kantardžića 3/3, 71000 Sarajevo, Bosna i Hercegovina
www.eu4justice.ba info@eu4justice.ba +387 33 879 911 +387 33 879 916