

Analýza a bezpečnost DAT OSINT

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Cíl předmětu

- Digitální stopy
 - Analýza
 - Využití
 - Investigace
- Digitální stopy a bezpečnost
 - Prevence incidentů
 - Analýza incidentů

Něco základních pojmů

- Informace x data
- Bezpečnost
- Kyber prostor a jeho vlastnosti

Začneme OSINT

- Jak hackeři plánují své útoky?

- Jak si vybírají oběti?

OSINT – Open Source Intelligence

- Proč OSINT:

- Vytipování cíle útoku
 - Oběť nemůže zjistit, že OSINT probíhá
 - OSINT je nedílnou součástí bezpečnosti (na obou stranách)
-
- Součást téměř všech útoků
 - Provádí se v rámci penetračních testů a bezpečnostních outsourcingů
-
- Nedílná součást investigativní práce

OSINT – Open Source Intelligence

- **Neinvazivní získávání informací**

- Nic se neprolamuje
- Informace se získávají **legálně**
- Zveřejněná chráněná data
- Veřejná metadata

- **Otevřené zdroje (Open Sources)**

- Vše, co je na internetu přístupné
- Zahrnuje i zdroje na DeepWeb a DarkNet

Některé nástroje OSINT

- Vyhledávače – nejen google
- Rejstříky, databáze
- Webové archivy
- Sociální sítě a média
- Zpravodajské servery
- Chat, diskuse
- **Metadata**
- Analýza multimédií
- **ICT infrastruktura**

Interview ČT24 Speciál

PREMIERA: Středa 20. 5. na ČT24



- <https://www.ceskatelevize.cz/porady/10095426857-interview-ct24/220411033200002-interview-ct24-special/>

Digitální stopa

- Vše, co po sobě v kyber prostoru zanechám
- Stopa, kterou **neovlivním**
 - Veřejné rejstříky
 - Zpravodajství
 - Komunikace směrem ke mně
- Stopa, kterou **ovlivním**
 - Dobrovolná interakce
 - Způsob interakce

Digitální stopa – pozor, komu ji vytváříme



<https://www.facebook.com/>

Digitální identita

- Konzervativní x nekonzervativní digitální identita
- Identita pod kontrolou
- Identita bez kontroly

-

OSINT – Open Source Intelligence

- **Cesta z bodu A do B:**
 - Získávání informací
 - Analytika a vyhodnocení
 - Vytěžení

- **Cílem je:**
 - Osoba, organizace
 - ICT systém

Pečlivá mravenčí práce

– Google a spol.



vladimír lazecký



Vše

Obrázky

Mapy

Video

Zprávy

Více

Nastavení

Nástroje

Přibližný počet výsledků: 30 100 (0,32 s)

www.viavis.cz › o-nas ▾

O nás | VIAVIS | střežíme podstatné

Vladimír Lazecký. Generální ředitel, vladimir.lazecky@viavis.cz. Jsem spoluzakladatelem naší společnosti a jsem jejím ředitelem. Bezpečností se zabývám již ...

cz.linkedin.com › vladimir-lazecky-69a004108

Vladimír Lazecký - CEO - VIAVIS a.s. | LinkedIn

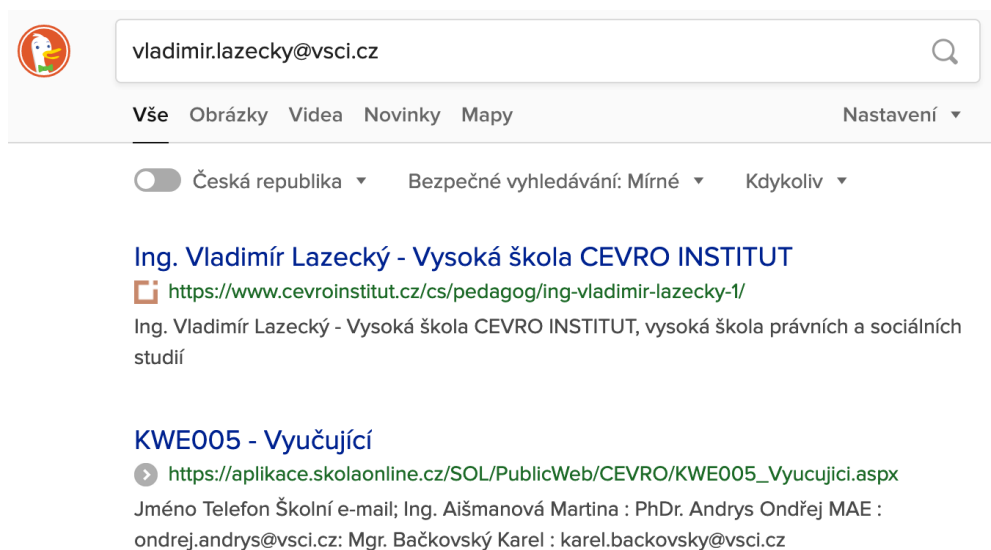
Vladimír Lazecký | Česká republika | CEO ve společnosti VIAVIS a.s. | 303 spojení | Zobrazit domovskou stránku, profil, aktivitu a články uživatele Vladimír.

Česká republika · CEO · VIAVIS a.s.

Hledání identit (identita x identifikátor)

Vladimír Lazecký

Generální ředitel, vladimir.lazecky@viavis.cz



Search interface showing results for the email address `vladimir.lazecky@vsci.cz`. The search bar contains the email address and a magnifying glass icon. Below the search bar are tabs for "Vše", "Obrázky", "Videa", "Novinky", "Mapy", and "Nastavení". The search results are filtered for "Česká republika" and "Bezpečné vyhledávání: Mírné".

Ing. Vladimír Lazecký - Vysoká škola CEVRO INSTITUT
<https://www.cevroinstitut.cz/cs/pedagog/ing-vladimir-lazecky-1/>
Ing. Vladimír Lazecký - Vysoká škola CEVRO INSTITUT, vysoká škola právních a sociálních studií

KWE005 - Vyučující
https://aplikace.skolaonline.cz/SOL/PublicWeb/CEVRO/KWE005_Vyucujici.aspx
Jméno Telefon Školní e-mail; Ing. Aišmanová Martina : PhDr. Andrys Ondřej MAE : ondrej.andrys@vsci.cz; Mgr. Bačkovský Karel : karel.backovsky@vsci.cz

Veřejná uložště

Datum : 02.04.2015

Diagnóza : D330 Nezhoubný novotvar- mozek supratentoriální

Další diagnózy :

Nález:

Pacientka sledován pro expanzi v pánvi a hyždi l. dx, subj mírná peogrese expanse

MR: nález s nepartnou objemovou progresí

D: Pacientka bude konsultována
bude sdělen distančně, děkuejem
Opouští ambulanci ve stabilizovan
Provedena edukace o medikací.
O indikaci ke zdravotnímu transpo
v delším časovém odstupu musí rozl
lékař pacienta na základě jeho akt

Lazecký.rar



<https://uloz.to/>

Veřejné rejstříky

- Registr smluv
- Katastr nemovitostí
- Obchodní rejstřík
- A další...

statnisprava.cz > Úřady v ČR > Rejstříky a registry

Rejstříky a registry

Rychlé hledání ve veřejném rejstříku

Obsahuje informace z obchodního rejstříku, rejstříku společenství vlastníků jednotek, rejstříku obecně prospěšných společností, rejstříku ústavů, nadačního a spolkového rejstříku.

Bydlení

- ▶ Katastr nemovitostí
Nahlížení do katastru nemovitostí.
- ▶ Registr sčítacích obvodů a budov
- ▶ Registr územní identifikace, adres a nemovitostí

Dotační programy

Žadatel - Obec	Kód podoblasti	Typ nemovitosti	Kombinace opatření	Kraj nemovitosti	Výše investiční podpory (Kč)	Výše podpory na projekt (Kč)	Dotační bonus (Kč)
Chrástřany	C11	RD	ne	Jihočeský	50 000	4 165	
Kunčice	C31	RD	ne	Olomoucký	55 000		
Valašské Klobouky	C31	RD	ne	Zlínský	55 000		
Trávník	C31	RD	ne	Zlínský	55 000		
Branka	C11	RD	ne	Moravskoslezský	95 000		
Kunovice	C31	RD	ne	Zlínský	55 000		
Prakšice	C31	RD	ano	Zlínský	55 000	5 000	20 000
Tichá	C31	RD	ne	Moravskoslezský	55 000		
Jeseník nad Odrou	C31	RD	ano	Moravskoslezský	55 000		0

file:///Users/vlada/Downloads/1582619376_31122019_ZU_prehled_prijemcu_po_dpory.pdf

Webové archivy

The screenshot shows the Wayback Machine interface for the URL <http://www.viavis.cz/kontakty/>. The interface includes a search bar with the URL, a 'Go' button, and a calendar navigation showing the date 13 Mar 2013. The main content area displays the VIAVIS logo and navigation menu. The page content is as follows:

[Domů](#) > [Kontakty](#)

Kontakty

Sídlo společnosti VIAVIS a.s. Obránců Míru 237/35 703 00 Ostrava Mapa	Kancelář PRAHA VIAVIS a.s. Nad Úpadem 63 140 00 Praha Mapa
--	---

Tel: +420 595 174 250 , E-mail: obchod@viavis.cz

<https://web.archive.org/web/20130313091149/http://www.viavis.cz/kontakty/>

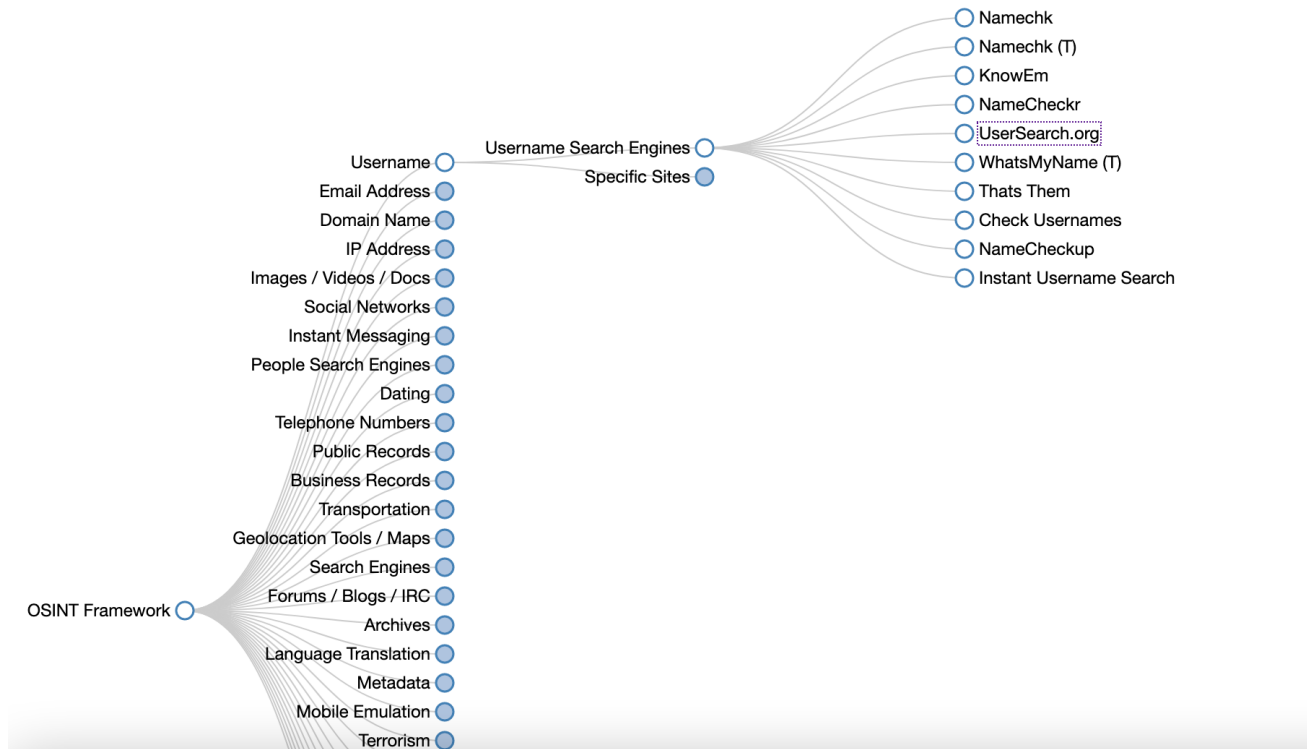
OSINT – Open Source Intelligence Tools

Top 14 OSINT tools as of 2021

OSINT stands for Open Source Intelligence. It refers to the practice of gathering data available from public sources.

<https://www.knowledgenile.com/blogs/top-osint-tools-2021/>

OSINT Framework



<https://osintframework.com/>

OSINT



Osoba

příjmení: jméno:

- Google Yahoo Seznam
 Google+ Lide Spoluzaci Facebook * LinkedIn * Twitter * Yasni V Kontakte
 Obchodní rejstřík RŽP Insolvenční rejstřík ARES Detail Zlaté stránky
Agregators: Carrot2 Dogpile Yippy PeekYou Pipl Yandex
 Zájmové osoby StB Archivní pomůcky bezpečnostních složek Cluuz Search Naši politici
 Interpol Wanted Interpol Missing FBI Wanted Panama Papers Cisko.info

Otevři osobu

[vybrat vše](#) [invertovat](#) [nic](#)

Firma

název: ičo: hint formát ČR 45274649

- Google Seznam Yahoo
 Obchodní rejstřík Insolvenční rejstřík ČSÚ Registr ekonomických subjektů ARES Detail ÚOOÚ
 podnikání - vizualizace vztahů
Agregators: Carrot2 Dogpile Yippy
 SPD a EKO daně Hoovers Tender Market Věstník e-tržiště Panama Papers Cisko.info Hlídač smluv
Registr smluv: publikující smluvní

<http://pejskove.net/>

OSINT – kde najít nástroje



OSINT Links for Investigators

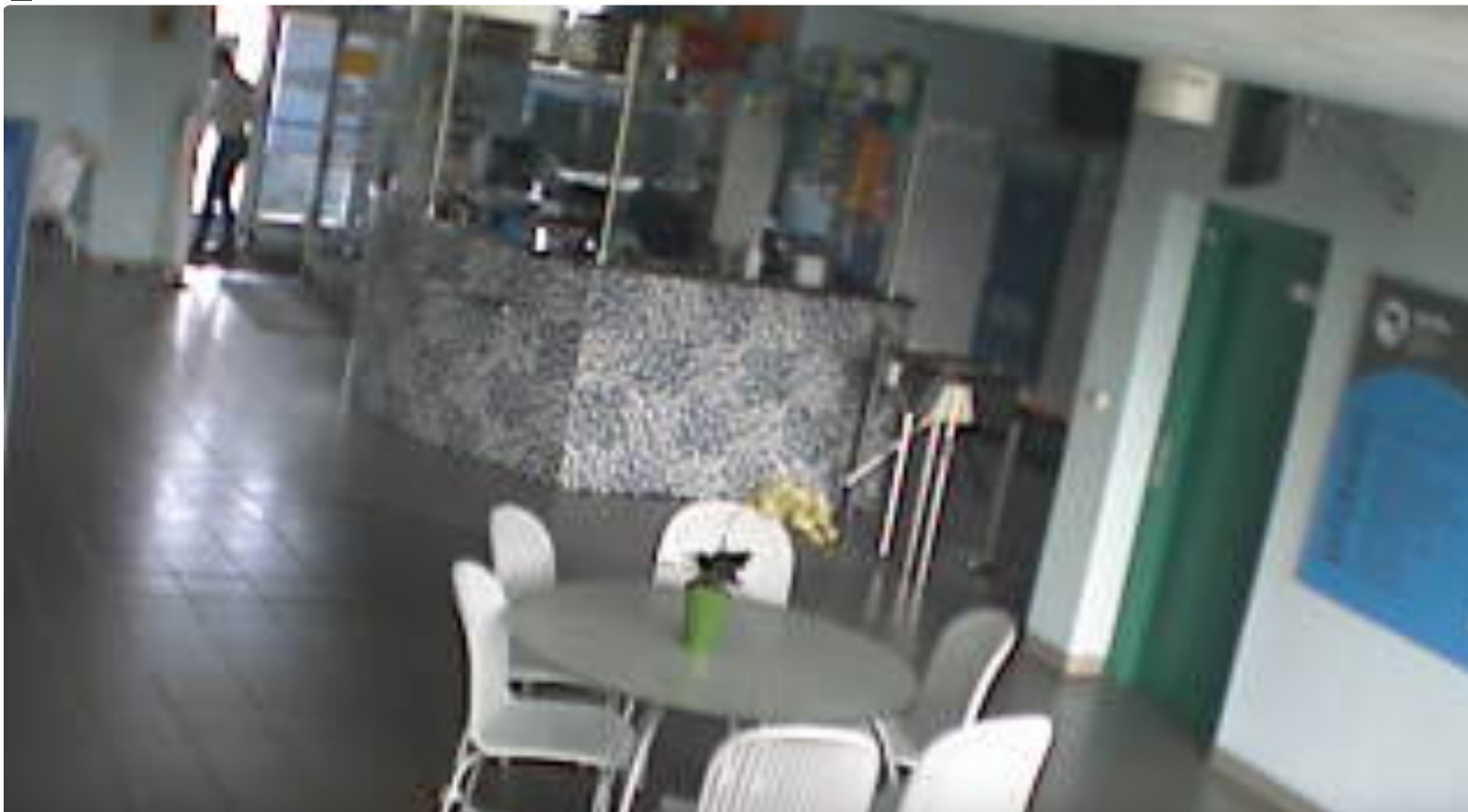
Updated for 2019

Use this interactive directory of OSINT links for background checks, investigative research and evidence gathering.

Save this handy OSINT directory onto your desktop to use as a starting point for your online investigative research. As you use the list, bookmark your favorite sites in your browser and save them into a folder for quick and easy access on your desktop, laptop or mobile device.

<https://i-sight.com/wp-content/uploads/2016/05/OSINT-Links-for-Investigators.pdf>

OSINT a kamerové systémy



<https://www.insecam.org/en/view/204260/>

Kamerové systémy

Track ID
2749898

Started from

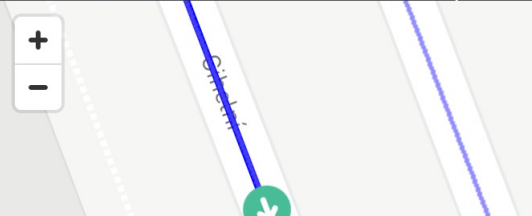

TRACK INFO

56 **1.37 km**
PHOTOS DISTANCE

560
POINTS

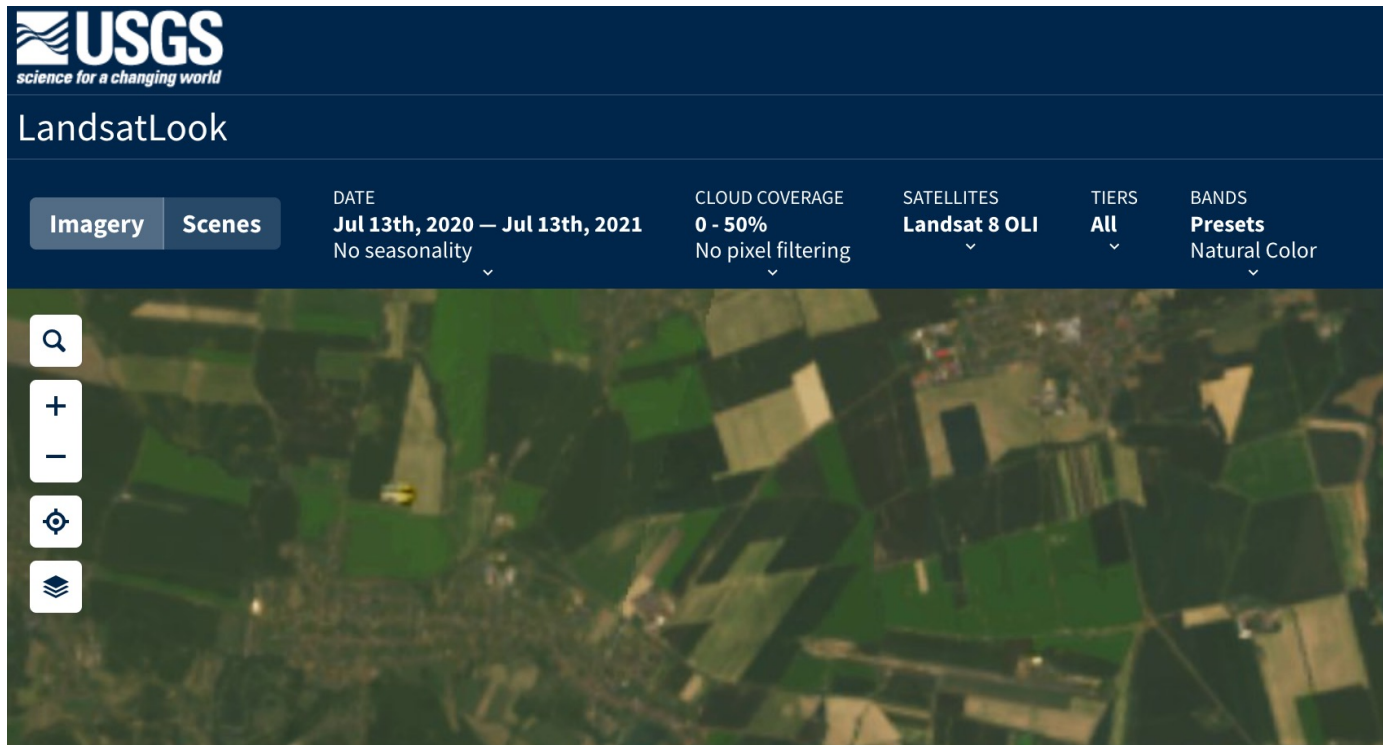
TRACK DETAILS

Contributed by: radim-ek
Recorded at: 19 June 2020 07:18
Coordinate: 49.8386344909668,



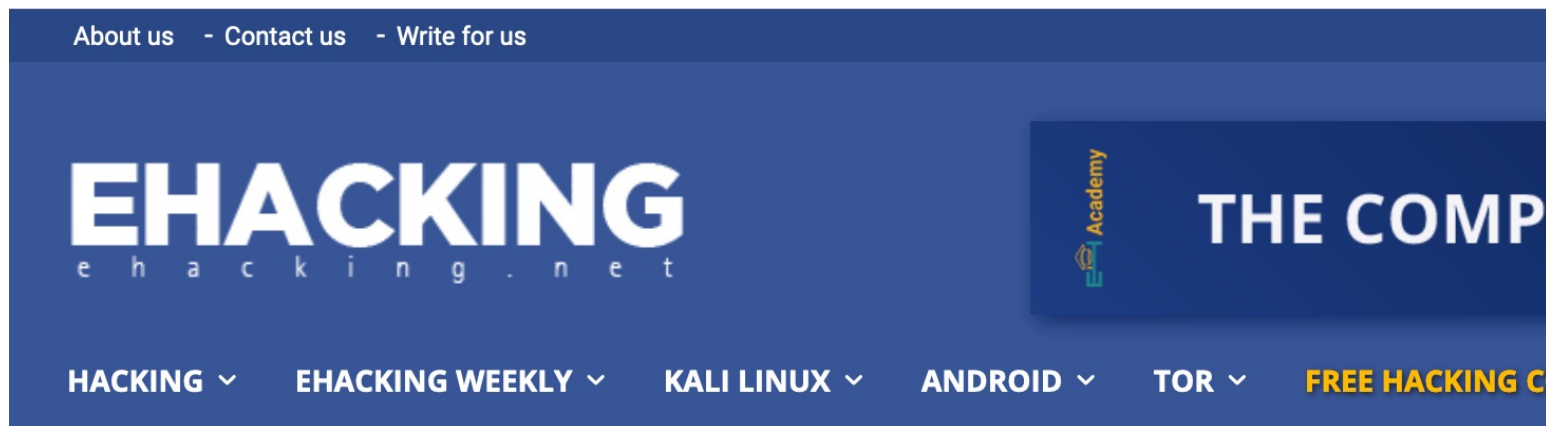
<https://kartaview.org/details/2749898/51/track-info>

Satelitní sledování – hledání změn



<https://landsatlook.usgs.gov/explore>

Telefonní číslo



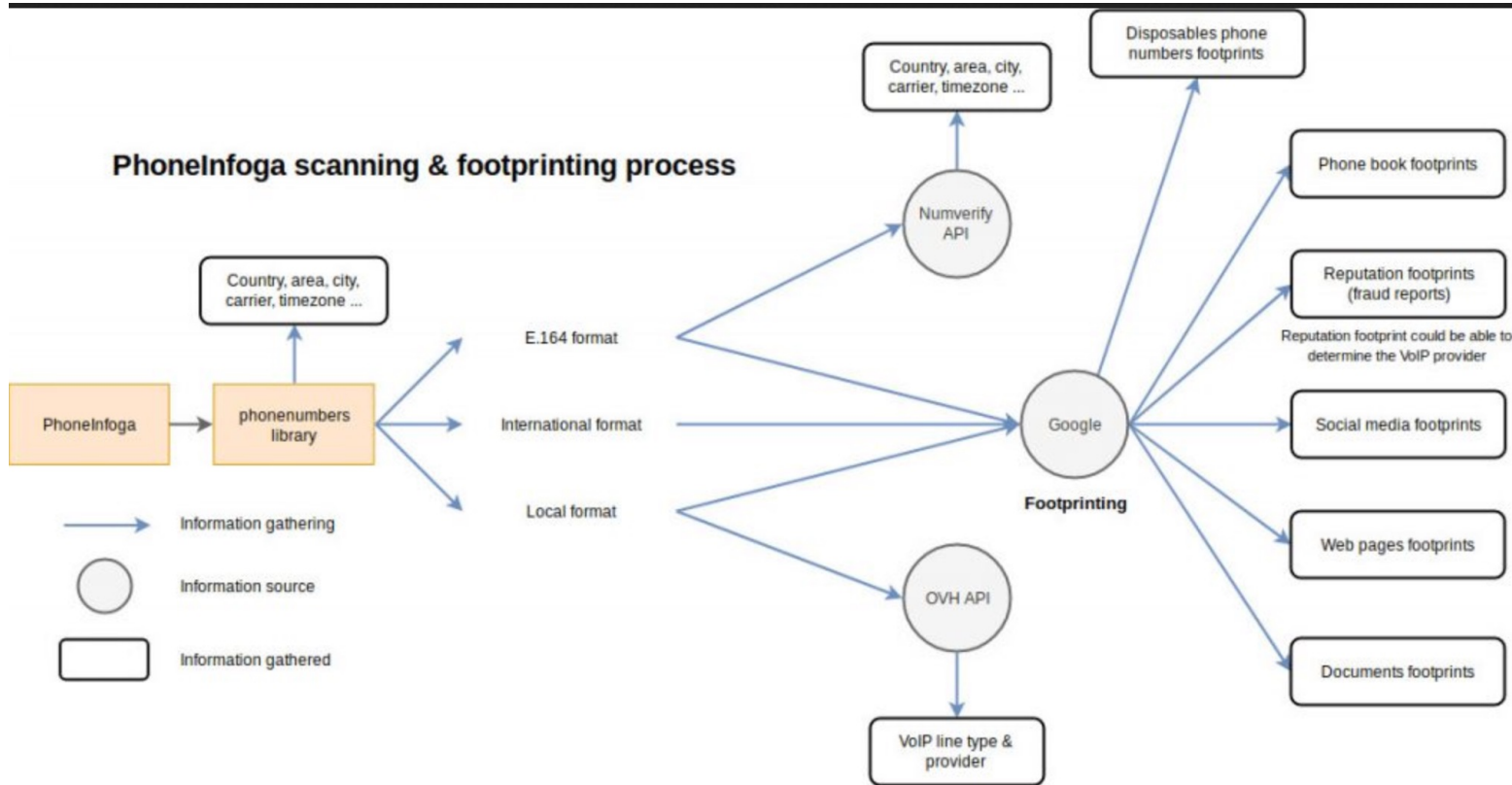
Home / Editorial / EH Academy / EH Security / EH Tools / Hacking / OSINT / OSINT tutorial to Find Information from a Phone

OSINT tutorial to Find Information from a Phone Number – PhoneInfoga Tool

 By **Irfan Shakeel** December 12, 2019

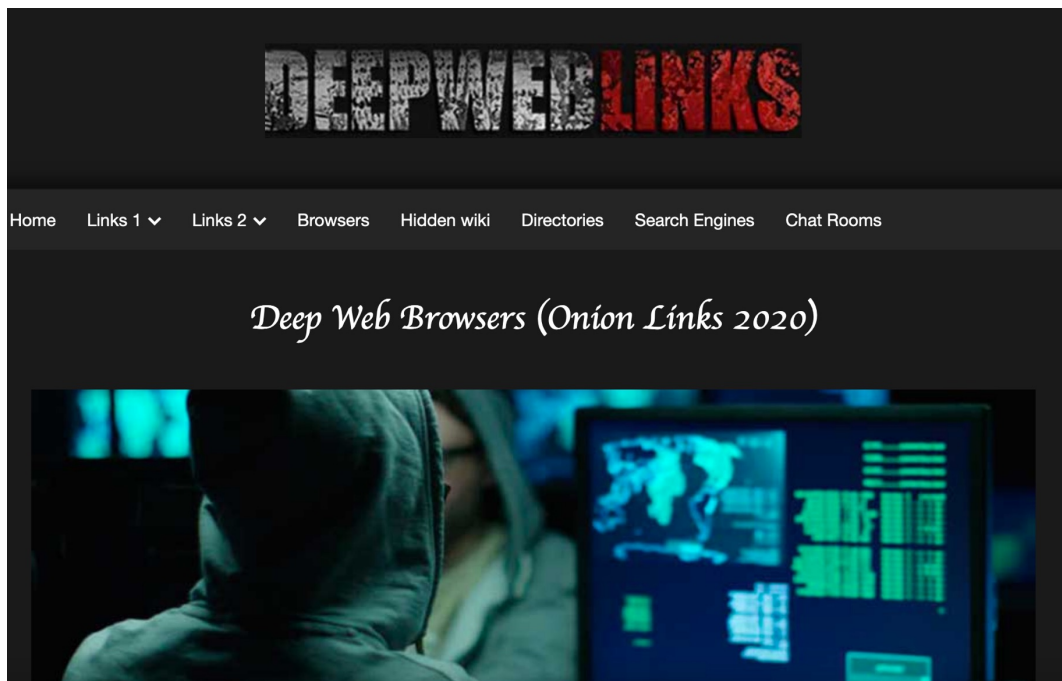
<https://www.ehacking.net/2019/12/osint-tutorial-phoneinfoga-phone-number-search.html>

Telefonní číslo



<https://www.ehacking.net/wp-content/uploads/2019/12/phoneinfogaosinttutorial-1024x517-1.jpg>

Webové služby – Deep a Dark NET



<https://deepweblinks.net/browsers/>

– NEDOPORUČUJI ZKOUŠET!!!!!! – JE NUTNO MÍT ZNALOST JAK NA TO

Vyhledávání obrázků - reverse image search



Search

Technology

Products

About

Upload

Paste or enter image URL



1 result

Searched over **48.3 billion images** in 0.7 seconds for: pic2.jpg

Sort by best match

Filter by website / collection



www.idnes.cz

wiki/obecne/institut-klinicke-a-experi... - First found on May 30, 2021

Filename: **WAS8a0c15_585768424703_5283124066723738229_o.jpg**
(230 x 129, 10 KB)


<https://tineye.com/>

Metadata obrázků, metadata souborů

Jeffrey's Image Metadata Viewer

URL:
or...
File: Soubor nevybrán.

Nejsm robot

 reCAPTCHA
Ochrana soukromí - Smluvní podmínky

This tool remains available so long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but a gift certificate (to: jfriedl@yahoo.com), or perhaps send me some good karma by doing something kind for a stranger.

If you have questions about this tool, please [see the FAQ](#).

Basic Image Information

Target file: pic3.jpg

Artist:	Ja [REDACTED]
File:	1,302 × 869 JPEG (1.1 megapixels) 189,896 bytes (185 kilobytes)
Color:	WARNING: No color-space metadata and no embedded color profile.



<http://exif.regex.info/exif.cgi>

Analýza tváře

Noldus

[APPLICATIONS](#)[PRODUCTS](#)[CUSTOMER STORIES](#)[ABOUT NOLDUS](#)[MYNOLDUS](#)

FaceReader Demonstration

Curious what emotions your own face shows? In this online demo the facial expression of a person is automatically extracted from a single picture. Additionally, FaceReader is capable of extracting some personal characteristics, like gender, facial hair, an age indication and whether a person is wearing glasses or not. This online demonstration lets you analyze images containing a face, by entering an URL or uploading a file.

[TRY NOW](#)[CONTACT US](#)

<https://www.noldus.com/facereader/facial-expression-analysis>

Analýza tváře

Visage Technologies

MALE, Age: 51

Anger
Disgust
Fear
Happiness
Sadness
Surprise
Neutral

Switch to Detector

Facial Features Tracker - High.cfg

DRAW OPTIONS:

- FEATURE POINTS
- IRIS RADIUS
- EARS
- GAZE
- FACE MODEL AXIS
- WIREFRAME
- TIGER MODEL
- GLOBAL TRACKING QUALITY
- FEATURE POINT QUALITY

FACE ANALYSIS:

- GENDER
- AGE
- EMOTIONS

FACE RECOGNITION:

- MATCH FACES
- FREEZE GALLERY

LOAD SAVE CLEAR

<https://www.visagetechologies.com/HTML5/latest/Samples/ShowcaseDemo/ShowcaseDemo.html>

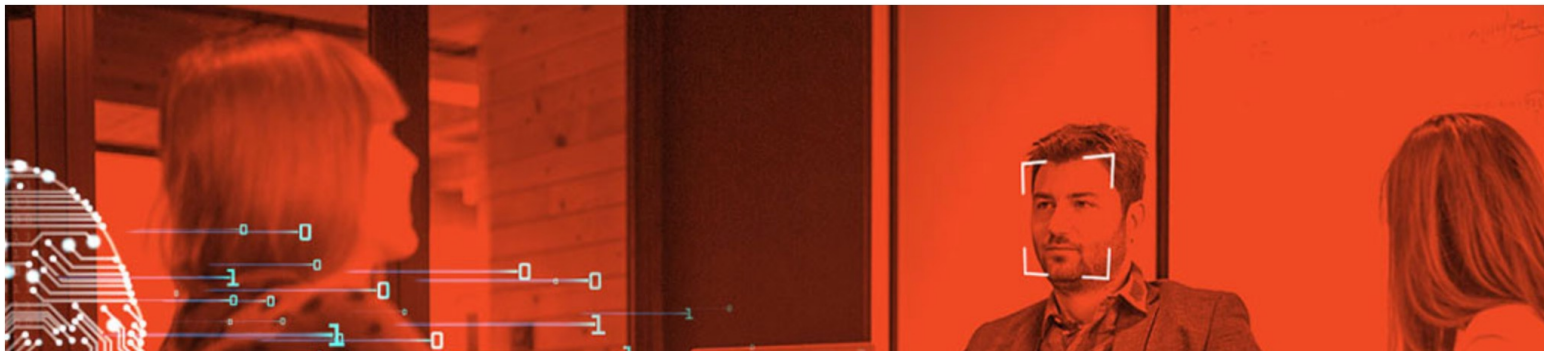
Analýza tváře a behaviorální analytika



COMPANY SOLUTIONS INDUSTRIES PARTNER PROGRAM BLOG

BioObserver

Advanced facial expression analysis for the study of human behavior in videos



<https://hertasecurity.com/advanced-solution-facial-expression-analysis/>

Zpravodajské agentury

- **OSINT** – veřejně dostupní zdroje
- **SIGINT** – zachycený přenos signálu a dat včetně metadat a odposlechů
- **IMINT** – obrazový materiál – drony, sledování, kamerové systémy
- **MASINT** – sledování významných příznaků (seizmické projevy...)

Zpravodajské agentury

VERINT

COVID-19

Products

Solutions

Services

Company

Partners

Careers



A graphic for a white paper featuring a hand interacting with a digital interface. The interface includes various icons: a shield with a checkmark, a padlock, a document with a checkmark, and a person icon. Text elements include 'INTRUSION DETECTED', 'DATA BREACH', and 'HACKING DE'. Percentages like 32%, 22%, 14%, and 56% are scattered around the icons.

White Paper: Proactive Intelligence for Effective Cyber Security

[Download +](#)



A graphic for a video featuring a person in a suit pointing at a large, glowing shield. The shield is surrounded by binary code (0s and 1s) and a circular digital interface. The text 'Verint National Cyber Defense' is visible.

Video: Verint National Cyber Defense

[Watch +](#)

<https://cis.verint.com/product/cyber-security/national-cyber-defense/>



Východiska

Co je pro oběť nejobtížnější?

Co mohu dělat?

Východiska snižování rizik – gramotnost a OSINT

- Zvýšení bezpečnostní gramotnosti
- OSINT na svou osobu, rodinu
- Odstranění nežádoucích dat
 - Využití zákonných práv
- **Minimalizace stop**



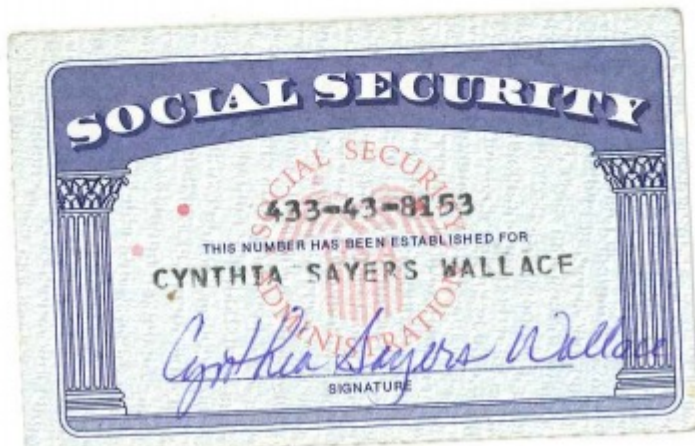
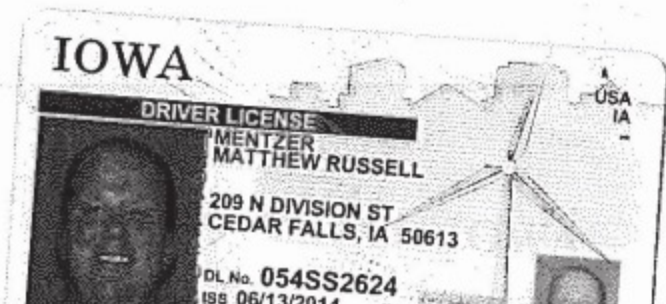
World Legal Information Institute

Free, independent and non-profit access to worldwide law

[\[Advanced Search\]](#) [\[LawCite\]](#) [\[Help\]](#)

[1834 databases](#) from 123 jurisdictions via [14 Legal Information Institutes](#)

CEO TAX, SOCIAL SECURITY NUMBER + DRIVER LICENSE



Ejercicio: 2018

	Debe	Haber	Saldo
NATURALES	5282,18	71860,84	-71860,84
	66.578,66		-66578,66
	71.860,84	71.860,84	

NATURALES	3585,94	51462,94	-51462,94
	47.877,00		-47877,00
	51.462,94	51.462,94	

27 69100010015 DETERIORAMIENTO TERRENOS I BIENES NATURA		51223,86	-51223,86
27 79100010015 REVERSION TERRENOS Y BIENES NATURALES	3566,57		-47657,29
29 Cierre contabilidad 2017	47.657,29		
06 ...	51.223,86	51.223,86	

ETERIORAMIENTO PARCELA (1296250CG7819N000002X)

27 69100010015 DETERIORAMIENTO TERRENOS I BIENES NATURA		51974,89	-51974,89
27 79100010015 REVERSION TERRENOS Y BIENES NATURALES	3547,22		-48427,67
29 Cierre contabilidad 2017	48.427,67		
06 ...	51.974,89	51.974,89	

ETERIORAMIENTO PARCELA (1296241CG7819N00000DX)

27 69100010015 DETERIORAMIENTO TERRENOS I BIENES NATURA		69967,28	-69967,28
27 79100010015 REVERSION TERRENOS Y BIENES NATURALES	5062,88		-64904,4
29 Cierre contabilidad 2017	64.904,40		
06 ...	69.967,28	69.967,28	

ETERIORAMIENTO PARCELA (1296243CG7819N00000IX)

27 69100010016 DETERIORAMIENTO TERRENOS I BIENES NATURA		73987,61	-73987,61
27 79100010016 REVERSION TERRENOS Y BIENES NATURALES			
38/xx			

Doporučení

- **Proč pravidelně provádět OSINT:**
 - Informace o průsaku informací
 - Úprava komunikovaných informací
 - Snižování rizik

- **Jak:**
 - Pravidelně

 - OSINT provádíme:
 - Jako součást bezpečnostního outsourcingu
 - Je součástí penetračních testů

Zadání samostatné práce – OSINT na osobu

- **Proveďte OSINT na dobrovolníka ...**
 - Zjistěte maximum informací
 - Proveďte vyhodnocení výsledků z hlediska použitelnosti pro útok
 - Navrhněte protiopatření
 - Připravte prezentaci
- **Prezentujte výsledky**

Máte nějaké dotazy?

Děkuji za pozornost a těším se příště

Vladimir.lazecky@viavis.cz