

# Etikus Hackalés alapjai

## OSINT alapjai I.

Dr. Hidvégi Timót  
egyetemi docens, IT biztonsági szakértő

## *Tiltott adatszerzés és az információs rendszer elleni bűncselekmények*

- Büntető Törvénykönyv / 2012. évi C. törvény
  - információs rendszer: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége
- 375. §: Információs rendszer felhasználásával elkövetett csalás
- 386. §: Védelmet biztosító műszaki intézkedés kijátszása
- 422. §: Tiltott adatszerzés
- 423. §: Információs rendszer vagy adat megsértése
- 424. §: Információs rendszer védelmét biztosító technikai intézkedés kijátszása

[https://www.police.hu/sites/default/files/2012.\\_evi\\_c.\\_torveny.pdf](https://www.police.hu/sites/default/files/2012._evi_c._torveny.pdf)

- OSINT (Open Source INTelligence): Nyílt forrású hírszerzés
  - <http://ih.gov.hu/assets/frontend/videos/video.mp4>
- HUMINT (Human Intelligence)
  - Olyan személyek megkeresése, akik segítenek az információk megszerzésében.
- SIGINT (Signals Intelligence)
  - Technikai hírszerzés. Távközlési csatornák, adatátvitel figyelése. Informatikai támadásokkal megvalósuló hírszerzés.

■ Információk szerzése publikus forrásokból.

- Szövegek dokumentumokból, cikkekből, blogokról, stb
- Térképek, geolokalizációs adatok
- Képek, video, audio
- Közösségi média

■ Passzív hírszerzés

■ Nem érinti a célpontot

■ Nem mindig igazak a források.....



## *OSINT. Kik használják?*

- Kormányzat
  - Katonaság
    - Baráti és ellenséges
  - Rendőrség
  - Hírszerzők
  - Üzleti élet
  - Jogászok
- 
- Szinte mindenki.....





**SZÉCHENYI  
EGYETEM**  
UNIVERSITY OF GYŐR  
GÉPESZMÉRNÖKI, INFORMATIKAI  
ÉS VILLAMOSMÉRNÖKI KAR



CYBERSEC LAB

## Lehetőségek

- <https://twitter.com/michenriksen/status/953616091368099840>



## *Információk típusai*

- Üzleti információk
- Hálózati információk
- Személy/felhasználónév információk
- stb

### ■ Szervezeti információk

- Kik ők
- Mit csinálnak
- Kapcsolatok más vállalatokkal

### ■ Megjelenés

- Fizikai elhelyezkedés, méret, partnerek, nyilvántartások, szervezeti struktúra.
- Termékinformációk, szabadalmak
- Alkalmazott technológia, Alkalmazottak
- Álláslehetőségek
- Kapcsolatok
- Nyilvános dokumentumok metaadatai
- Szervezeti ábra



- Technológiák
- Távoli hozzáférés
  - VPN
  - Email
- Védekezés
  - hálózati
- Címzés
  - Flat network vs Szeparált

- Alkalmazotti információk
  - Kik ők, mit csinálnak
  - Szervezeti felépítés
  - Felhasználónév/jelszó
- Különböző helyeken található
  - Munkahely/szerep, korábbi munkahelyek
  - E-mail címek

### ■ Média

- Rádió, televízió, újságok

### ■ Internet

- Keresők
  - *Google, Yahoo, Bing, DuckDuckGo, Yandex, Shodan*
- Közösségi média
  - *Bemutakozás, fotók, ismerősök, like-ok*
- Vélemények, kommentek
- Különböző felületeken közös account-ok
- Geolokalizációs adatok
- Ingatlan információk (adás-vétel)
- Vallási csoportok, hobbiklub hírlevelek
- Élethelyzetek (születés, válás, stb)
- Kormányzati adatok, regisztrációk

## Hogyan kezdjük el?

- Titkosított, VPN kapcsolat
- Javasolt a virtuális gép alkalmazása
- Operációs rendszer kiválasztása
  - Linux? (pl.: Kali? Vagy van erre más OS?)
  - Windows 11 (ingyenes VM letöltése)
  - Android VM
    - <https://www.osboxes.org/android-x86/> <https://www.android-x86.org/>
- Fake profil létrehozása
  - (<https://www.fakepersongenerator.com/mastercard-generator>)
- Mivel készítsük el a riportot?
  - Pl.: cherrytree (<https://www.giuspen.com/cherrytree>)
- Böngésző user agent switch alkalmazása (Kell?)
  - <https://addons.mozilla.org/hu/firefox/addon/uaswitcher>



## Hogyan kezdjük el?

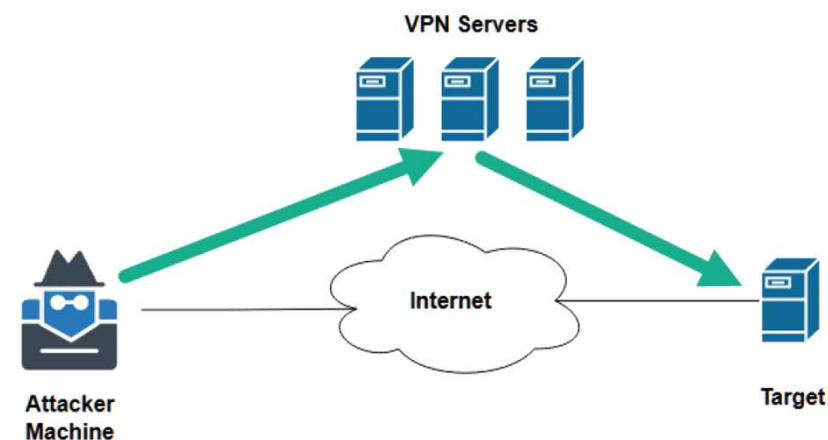
- ProtonVPN
  - <https://protonvpn.com/hu/free-vpn>
- Saját VPN szerver létrehozása?
- Fake profil létrehozása
  - <https://datafakegenerator.com/generator.php>
  - <https://www.elfqrin.com/fakeid.php>
  - <https://www.fakenamegenerator.com>
  - Kép létrehozása
    - <https://www.thispersondoesnotexist.com>
    - <https://www.morphthing.com>
  - Credit kártya
    - <https://privacy.com>
- Email létrehozása
  - <http://www.20minutemail.com>
  - <https://protonmail.com/hu/>
  - <https://tutanota.com/hu/>
  - <https://www.querrillamail.com>



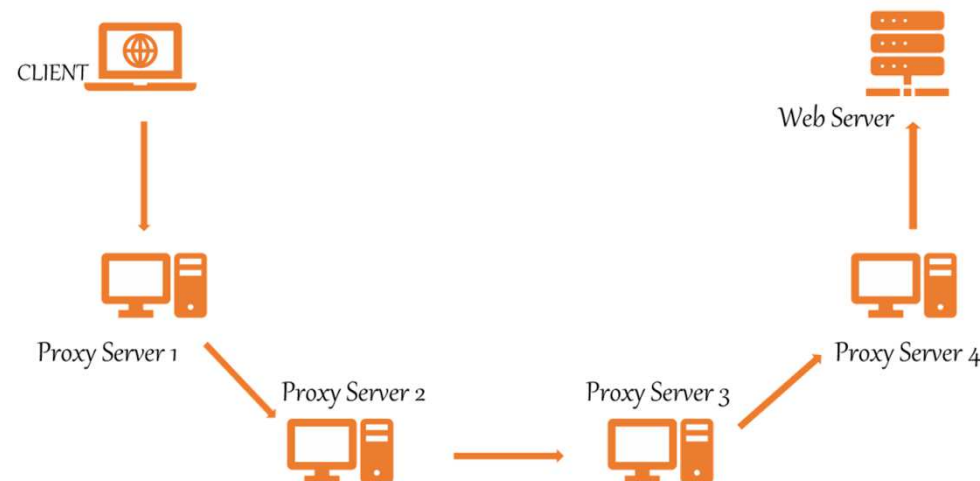
<https://web.archive.org/web/20190219025328/https://www.lyrn.ai/2018/12/26/a-style-based-generator-architecture-for-generative-adversarial-networks/>

- VPN (Virtual Private Network)
- Proxychains
- TOR (The Onion Router)

- A VPN-szolgáltató használata általában előfizetést igényel.
- A VPN szolgáltató nem vezessen naplót, és nem adja el a felhasználói adatokat harmadik félnek.
- A VPN-szolgáltató támogassa a VPN-kliensalkalmazás integrálását a használni kívánt operációs rendszerben.
- Különböző felhőszolgáltatók, például az Azure, az AWS használható a VPN-szolgáltatások beállításához.
- Fontos, hogy a Domain Name System (DNS) forgalma ne szivároogjon, mert ez elárulja a lokalizációs adatokat.
  - **Teszt:** DNS Leak Test ([www.dnsleaktest.com](https://www.dnsleaktest.com)) segítségével ellenőrizhető.

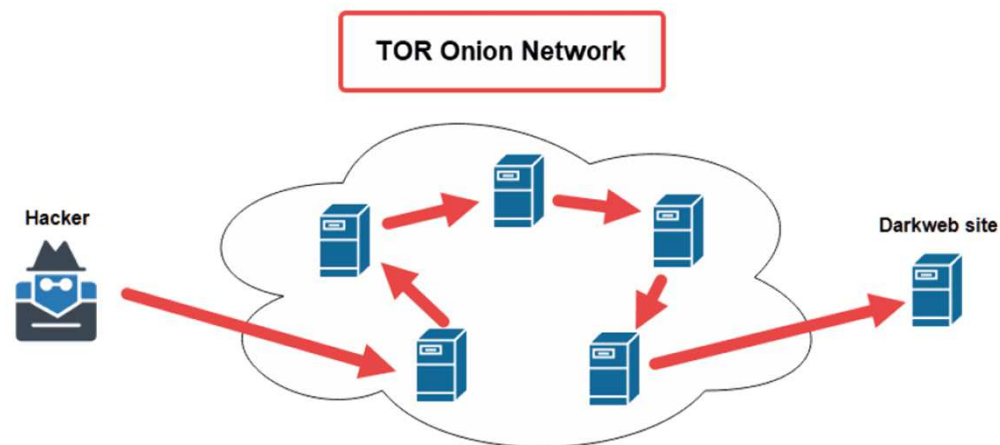


- A támadó rendszeréből érkező forgalom a proxyserver1-re megy, majd a proxyserver2-re, proxyserver3, és így tovább, amíg a láncban az utolsó szerver továbbítja a forgalmat a hálózaton vagy az interneten lévő tényleges célrendszerre.
- A proxychains használata nem titkosítja a forgalmat a VPN-ekhez képest, de anonimitást biztosít a hálózat számára. A valódi IP elrejtésre kerül.
- Ingyenes proxy szerverek listája:
  - <https://spys.one/en/>





- A TOR egy olyan szolgáltatás és speciális hálózat, amely lehetővé teszi a felhasználók számára az anonimitást az internetes böngészés és a dark webhez való hozzáférés során.
- A TOR egy hasonlít a proxy-láncre, de sokkal jobb és összetettebb. Titkosított a forgalom az egyes TOR-ok/csomópontok között, és sokkal többet tesz annak érdekében, hogy a célállomás soha ne tudja meg a személyazonosságot.



## *Miért használjunk VPN-t? Mit árul el a böngészőnk?*

### ■ Ezért.....

- <https://webkay.robinlinus.com>
- <http://whatsmyuseragent.org>
- <https://ipleak.net>
- <https://coveryourtracks.eff.org>

### Social Media

Facebook: logged in  
Google: logged in  
Flickr: logged in

#### Explanation:

See this post by [eatsfoobars](#)

#### Prevention:

To prevent your browser from leaking information about your social networks, logout, use [Private Browsing](#), or [NoScript](#).

Although those Vulnerabilities are [well known for several years](#), [none of the vulnerable companies wants to fix them](#).

### Hardware

#### CPU:

Win32, 8 Cores

#### GPU:

Vendor: Google Inc.  
Renderer: Google SwiftShader  
Display: 1536 x 864 - 24bits/pixel

#### Battery

Charging: not charging  
Battery Level: 88%  
Time remaining: 8.33h

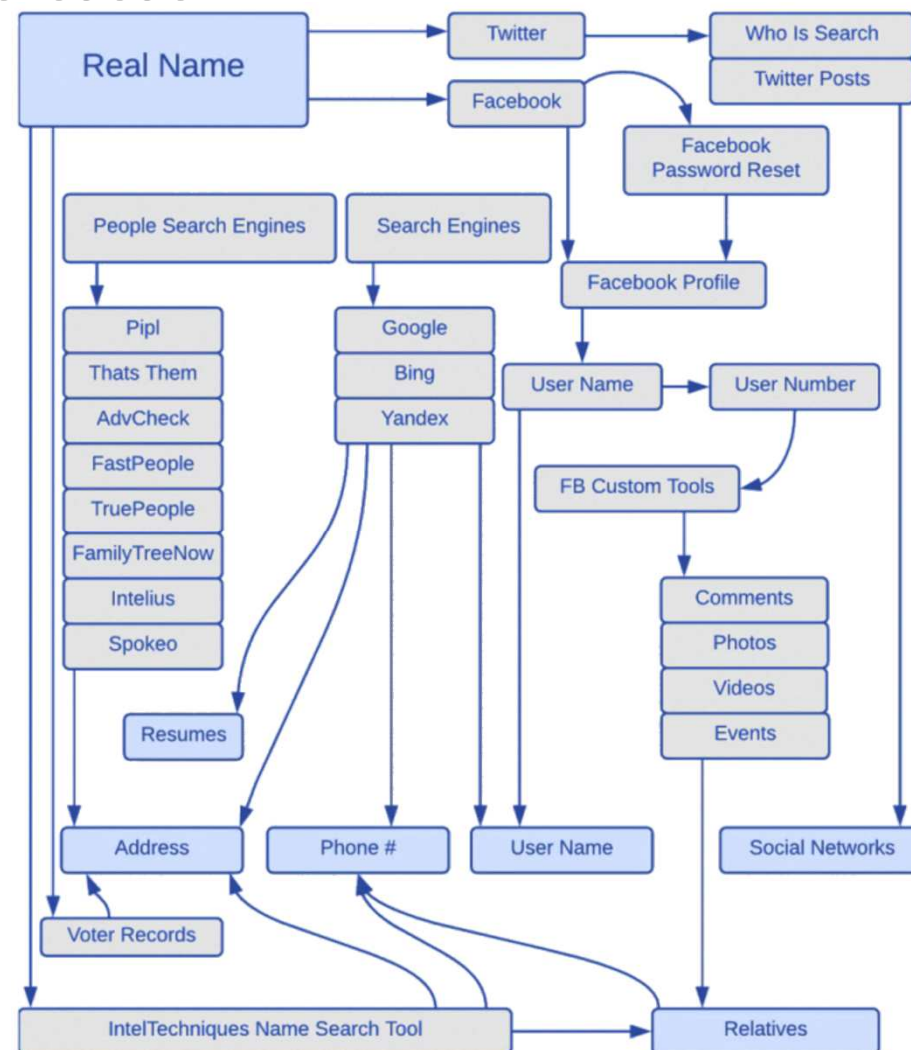
#### Prevention:

To prevent your browser from leaking device information use [NoScript](#).

## Személyek keresése

### ■ Személykereső és közösségi oldalak

- Számos ingyenes és nyilvánoselérhető oldalon kereshetők személyek.
- Személyes és szakmai információkat is kaphatók a célszemélyről.
  - *Facebook: az egyik legnépszerűbb közösségi oldal, könnyen kiadja a személyesinformációkat, például képeket, meglátogatott helyszíneket, érdeklődési köröket stb.*
  - *Linkedin: a szakmai közösségi platform, a célszemély hol dolgozott, valamint a szakmai képességeiről.*
  - *Ez az információs bázis igen hasznos lehet egy social engineering támadás felépítéséhez.*



## *Keresők (személy)*

- Facebook – <https://facebook.com>
- LinkedIn - <https://www.linkedin.com/>
- Hunter - <https://hunter.io/>
- Pastebin - <https://pastebin.com/>
- IntelTechniques - <https://inteltechniques.com>
- Recon-ng - <https://github.com> / repo-k
  - Telepítés: `sudo apt install recon-ng`
- Discover - <https://github.com/leebaird/discover>
- Egyéb
  - <https://www.whitepages.com>
  - <https://www.truepeoplesearch.com>
  - <https://www.fastpeoplesearch.com/>
  - <https://www.fastbackgroundcheck.com>
  - <https://www.peakyou.com/>
  - <https://www.spokeo.com/>
  - <https://webmii.com/>

### ■ Név

- <https://pipl.com>
- <https://radaris.com>
- <https://www.intelius.com>
- <https://www.spokeo.com>

### ■ Email

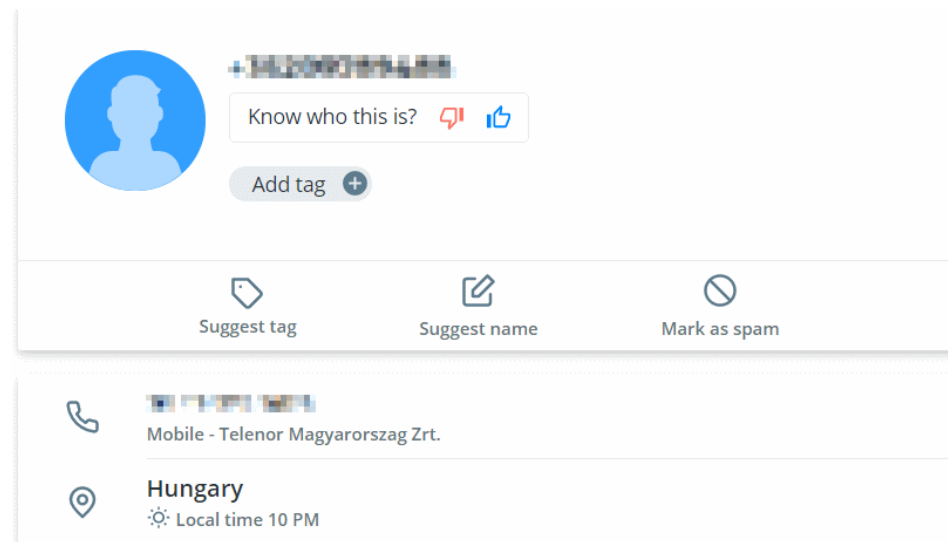
- <https://intelx.io>
- <https://haveibeenpwned.com>

### ■ Telefonszám

- <https://truecaller.com>
- <https://tools.epieos.com/phone.php>

### ■ Egyéb....

- <https://checkusernames.com>



- google.com

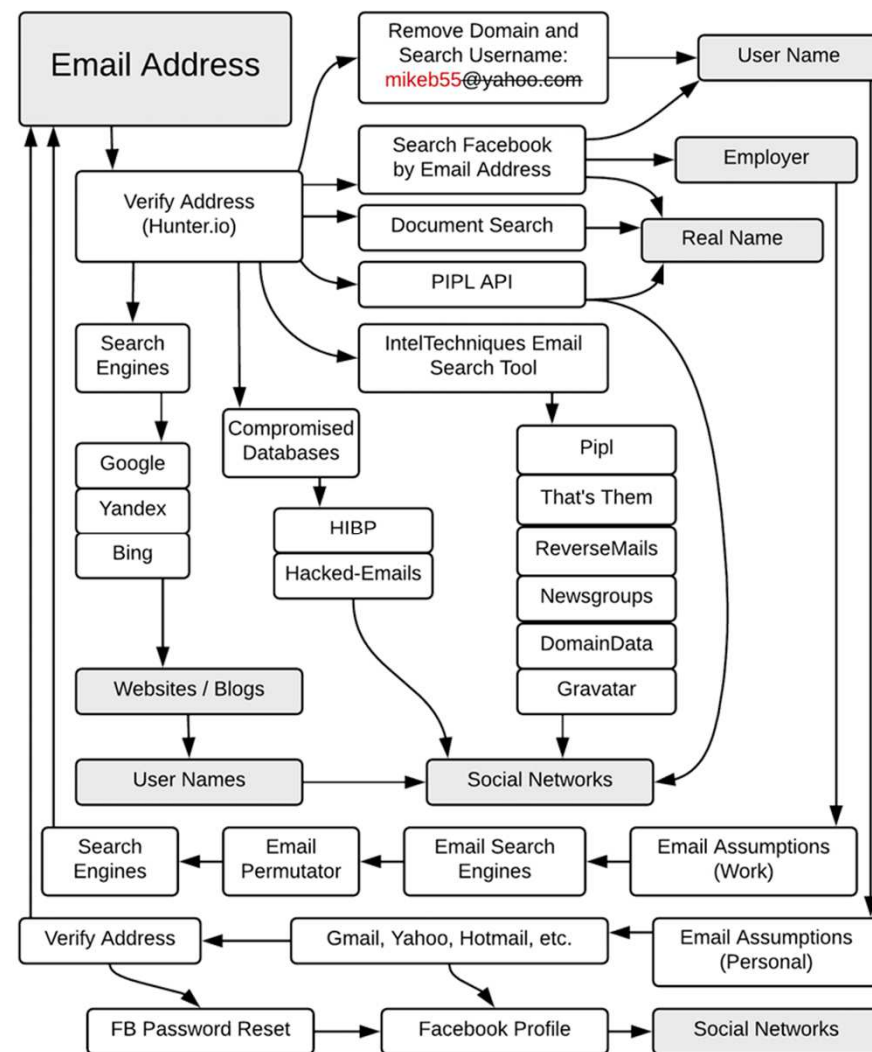
- [https://lens.google.com/search?ep=gsbubb&hl=hu&re=df&p=AbrfA8oF9lrkIDdF34QfWd-8Ubq8NNVTCbTtRKIcnOpOK6UL\\_YuxsPJH1Ju\\_cqHBtYNMkg4EiAnCwYVNrlCaeGCI9d2RLFWqGxCaWSF\\_OBt0CD9Xf\\_fbdLIRUbT-3u2BUR-HfWQYkR7rKx3pxg63Zv6oNB8d\\_WbtHa5p2FhIYhnQ1gbHu9MRjC7gmUJd1KVpJW8eDoRbL1MU9ceoJtA%3D%3D#Ins=W251bGwsbnVsbCxudWxsLG51bGwsbnVsbCxudWxsLG51bGwsIkVrY0tKR1F6TW1ReU5qRm1MV000TkRrdE5EWm1ZUzA0WkdNMExUYzBPREZtWm1FM00yTXIPQklmWXpReFMwcFJjREJ6VGpCV1dVUnpaM0puWDBNeFVEWjBRMnhGYWxsb2F3PT0iLG51bGwsbnVsbCxudWxsLG51bGwsbnVsbCxudWxsLG51bGwsWyJiOGIxMjRmNy1IMjNhLTQ0OTgtYTBIMC1iMWEyODkxNGY5MTIiXV0=](https://lens.google.com/search?ep=gsbubb&hl=hu&re=df&p=AbrfA8oF9lrkIDdF34QfWd-8Ubq8NNVTCbTtRKIcnOpOK6UL_YuxsPJH1Ju_cqHBtYNMkg4EiAnCwYVNrlCaeGCI9d2RLFWqGxCaWSF_OBt0CD9Xf_fbdLIRUbT-3u2BUR-HfWQYkR7rKx3pxg63Zv6oNB8d_WbtHa5p2FhIYhnQ1gbHu9MRjC7gmUJd1KVpJW8eDoRbL1MU9ceoJtA%3D%3D#Ins=W251bGwsbnVsbCxudWxsLG51bGwsbnVsbCxudWxsLG51bGwsIkVrY0tKR1F6TW1ReU5qRm1MV000TkRrdE5EWm1ZUzA0WkdNMExUYzBPREZtWm1FM00yTXIPQklmWXpReFMwcFJjREJ6VGpCV1dVUnpaM0puWDBNeFVEWjBRMnhGYWxsb2F3PT0iLG51bGwsbnVsbCxudWxsLG51bGwsbnVsbCxudWxsLG51bGwsWyJiOGIxMjRmNy1IMjNhLTQ0OTgtYTBIMC1iMWEyODkxNGY5MTIiXV0=)

- A tesztkép forrása (2024.11.12.)

- <https://uni.sze.hu>



## Email címek





## *Email címek*

- <https://tools.emailhippo.com/>
- <https://email-checker.net/>
- <https://www.voilanorbert.com/>
- <https://phonebook.cz/>
- <https://hunter.io>



- <https://namechk.com/>

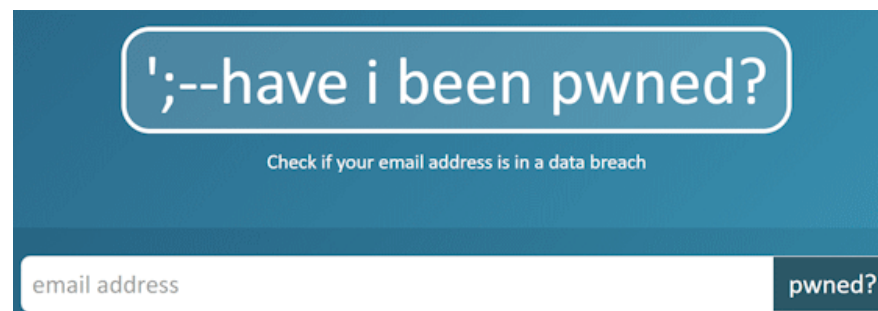


☐ Nem vagyok robot  
reCAPTCHA  
Adatvédelem - Általános Szerződési Feltételek

### Domains

cyberseclab.com	REGISTERED	cyberseclab.net	REGISTERED	cyberseclab.me	BUY
cyberseclab.org	REGISTERED	cyberseclab.us	BUY	cyberseclab.info	BUY
cyberseclab.la	BUY	cyberseclab.asia	BUY	cyberseclab.biz	BUY
cyberseclab.tv	BUY	cyberseclab.ws	BUY	cyberseclab.nyc	BUY
cyberseclab.okinawa	BUY	cyberseclab.online	BUY	cyberseclab.network	BUY
cyberseclab.ninja	BUY	cyberseclab.photo	REGISTERED	cyberseclab.photography	BUY

- <https://haveibeenpwned.com/>
- <https://leakcheck.io>
- <https://snusbase.com/>
- <https://dehashed.com>



';--have i been pwned?

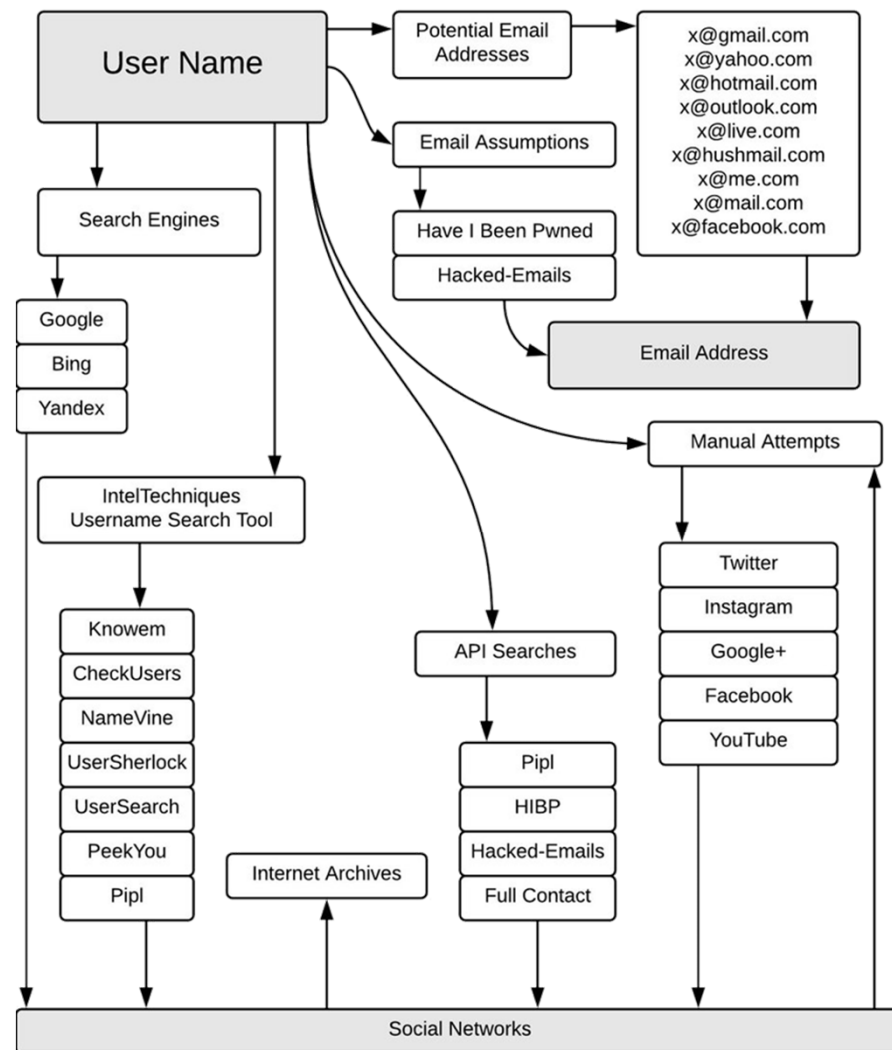
Check if your email address is in a data breach

email address

pwned?

## Felhasználói nevek

- userrecon
  - <https://github.com/wishihab/userrecon>
- <https://whatsmyname.app>

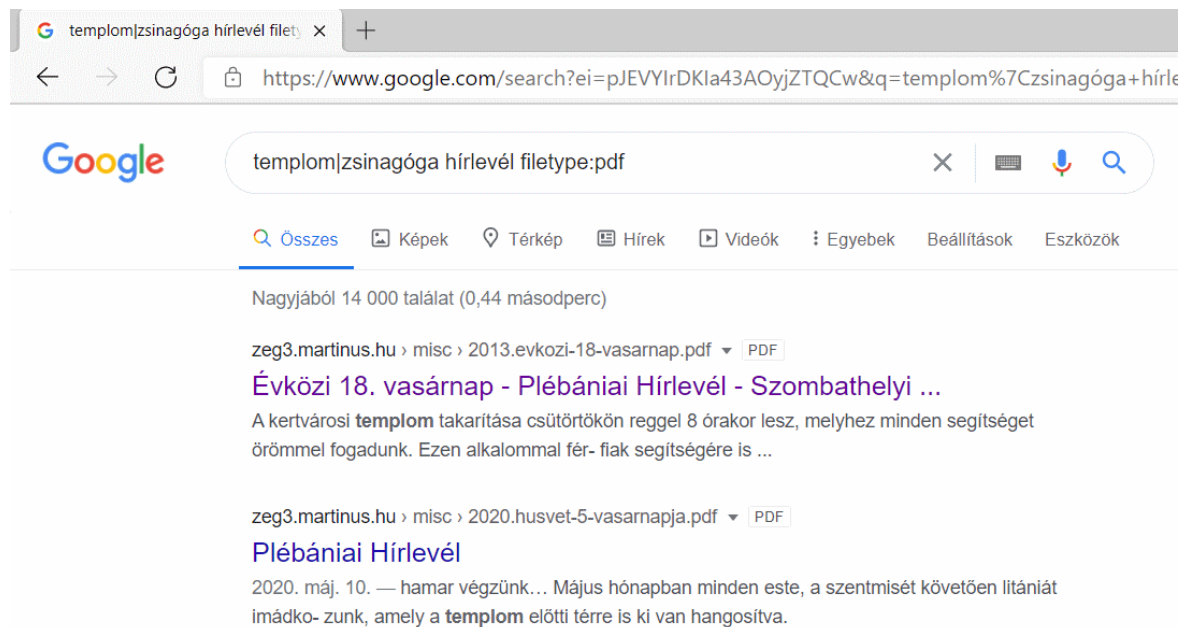


- recon-ng
- dmitry -s domainnév

```
(kali@kali)-[~]  
$ dmitry -s sze.hu  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
  
HostIP:193.224.131.121  
HostName:sze.hu  
  
Gathered Subdomain information for sze.hu  
_____  
Searching Google.com:80 ...  
HostName:uni.sze.hu  
HostIP:34.149.87.45  
HostName:alumni.sze.hu  
HostIP:195.228.36.185  
HostName:felveteli.sze.hu  
HostIP:193.224.131.121
```

- Shodan - <https://www.shodan.io/>
- Censys - <https://censys.io/>
- Find Subdomains - <https://findsubdomains.com/>
- HE BGP Toolkit - <https://bgp.he.net/>
- SPF Records - <https://mxtoolbox.com/spf.aspx>

- Nevek, címek, telefonszámok, email-ek
- Ki beteg?
- Közelgő események
- Életesemények ünneplése (Ki? Mikor?)
- Fotók



- Közhiteles céginformáció
  - <https://www.e-cegjegyzek.hu>
  
- „Panama iratok”
  - <https://offshoreleaks.icij.org/pages/database>

- Ha nem tag a közösségi médiában, akkor is:
  - Megjelenik egy fotón, arcfelismerő felismeri, Ismerősök megcímkézhetik

- Alkalmazások

- Lista
  - *Sherlock*
- LinkedIn
  - *InSpy*
- Twitter
  - *twint*
- Instagram
  - *Instalooter*
- Youtube
  - *hooktube*



**Gary Chavez** added a photo you might be in. ...

about a minute ago • 

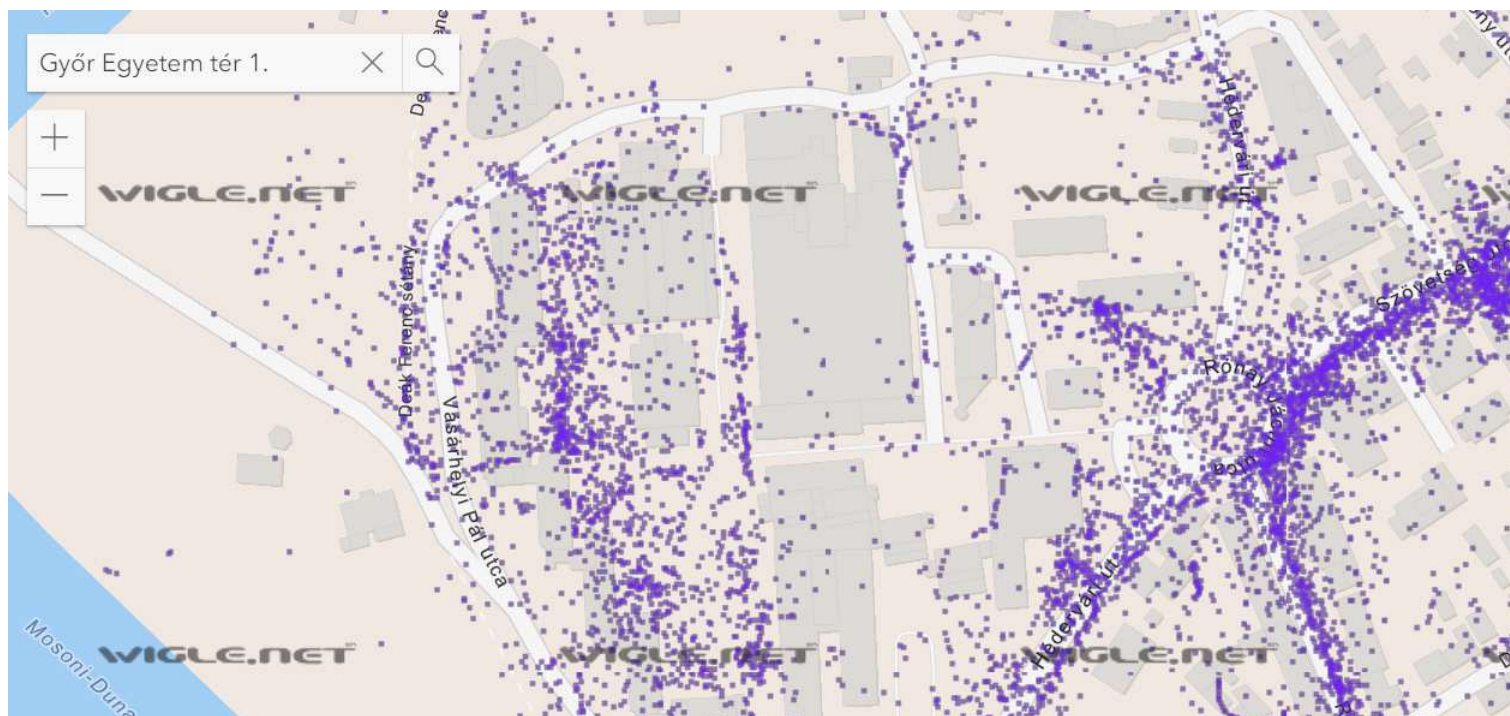


<https://techcrunch.com/2017/12/19/facebook-facial-recognition-photos/>



- Mi a UID? Hogyan tudom meg?
  - <https://lookup-id.com>, <https://www.facebook.com/profile.php?id=UID>
- Hogyan keresek postot, képet, stb?
  - <https://www.facebook.com/search/posts?q=elte>
  - <https://www.facebook.com/search/photos/?q=elte>
- Pattern készítés
  - <https://graph.tips/beta/>
- Keresés
  - <https://whopostedwhat.com>
- Videó letöltése
  - <https://fbdown.net>
- Általános
  - <https://fb-search.com>

- <https://wgle.net/>



- Web
  - <https://cyberseclab.eu>
- Facebook
  - <https://www.facebook.com/IndustrialandResearchLab>
- Github
  - <https://github.com/cyberseclabor>
- LinkedIn
  - <https://www.linkedin.com/company/industrial-and-research-lab-for-cybersecurity>



SZÉCHENYI  
EGYETEM  
UNIVERSITY OF GYŐR  
GÉPESZMÉRNÖKI, INFORMATIKAI  
ÉS VILLAMOSMÉRNÖKI KAR



CYBERSEC LAB

## *Industrial and Research Lab for Cybersecurity*

enumeration ISO21434 MiTM  
Artificial\_Intelligence network  
hacking education OT/ICS Android  
car spoofing S7 forensics CyberSecLab  
NIST800-82 training Purdue vehicle  
HMI modell opc-ua PLC  
OWASP pentest security NIS2 CAN  
cyber Python C# OSINT  
WiFi exploit linux AI OT nmap unit  
scada sniffing kali online  
modbus malware ethical  
SDR Machine\_Learning metasploit  
vulnerability head Pentesting  
Ethernet-IP