• Use a VPN (TOR) at all times when online.
• Search widely, back up and reinforce your findings
• Make a note/ take copies of ALL evidence collected at the time of identification (date):
  ➢ Screenprints
  ➢ Hyperlinks
  ➢ Website copies (Static/ video capture).
• Record EVERYTHING that you provide to websites (pseudonyms) for future reference and recall.
• Understand the market (language, terminology, options...)
• Lot of luck needed 🙂
• Consistency - Criminals adopt an identity and keep it!
• Confirm one identity – run checks on “username” elsewhere
• Where possible, also consider ‘alternative spellings’:
  ‘Bogdan123’
  ‘B0gdan123’
  ‘Bogdan_123’ ....
• Hide your IP address
• Change your IP address
• Mask your location
• Encrypt data transfers
• Access blocked websites
• Consider both current and historical registration domain records
• Applicable date ranges of these periods
• New leads - names, email addresses, telephone numbers, addresses
• Site options:
  Domain Tools (domaintools.com)
  Whoisology (whoisology.com)
  Domain History (domainhistory.net)
Terms and Conditions/ Disclaimer Pages

Interrogate for further information on:

- Contact details (including indication of geography)
- Affiliate companies
- Parent companies
- Phrasing used elsewhere online (compare and link)
Payment Methods

- Proceed through mock check-out process
- Use fake information to ‘analyse’
- Do not complete!
- Appropriate:
  - Check-out process
  - Account summary

---

United Kingdom

Securitatea contului

Parola
Enter password
Confr. parola
Confirm password

Detalii de plata

Total de plată azi: **€2.00EUR**

Alegeți metoda preferată de plată.

- **PayPal**
Search Engines on internet

Bing
Ask
AOL
Excite
Yahoo
Dogpile
Metacrawler
Gigablast
...
Search People

WebMii:
http://webmii.com

Pipl:
https://pipl.com/

Peoplesearch:
https://www.pplesearch.com
UK OSINT SOCIAL MEDIA SEARCH tool

http://www.uk-osint.net/facebook.html
Law Enforcement Online Requests

My Requests

<table>
<thead>
<tr>
<th>Case Number</th>
<th>Status</th>
<th>Account</th>
<th>Type</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>110551</td>
<td>New</td>
<td>Records</td>
<td>21 Stunden</td>
<td>7. Juni um 15:35</td>
</tr>
<tr>
<td>110554</td>
<td>New</td>
<td>Records</td>
<td>22 Stunden</td>
<td></td>
</tr>
<tr>
<td>104981</td>
<td>New</td>
<td>Records</td>
<td>7. Juni um 15:35</td>
<td></td>
</tr>
<tr>
<td>104888</td>
<td>New</td>
<td>Records</td>
<td>7. Juni um 15:21</td>
<td></td>
</tr>
</tbody>
</table>
Law Enforcement Online Requests

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent who is authorized to gather evidence in connection with an official investigation, you may request records from Facebook through this system.

☑ I am an authorized law enforcement agent and this is an official request

Request Access

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 3703 and 3711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the Law Enforcement Guidelines.
E-Mail Adresse, IP

Mobile number (if the account is new!)

https://www.facebook.com
Requestor Information

Records Request

Please complete all fields below and be sure to attach all relevant documentation. A U.S. search warrant, Mutual Legal Assistance Treaty (MLAT) or letter rogatory is generally required to compel disclosure of user content.

The Law Enforcement Response Team reviews each request separately and discloses account records solely in accordance with our terms of service and applicable law. Additional information can be found in the Facebook or Instagram Law Enforcement Guidelines.

Internal Case Reference Number:

Legal Process:
Nature of Case:
Legal Process Signed Date:
Request Date:

Konten:

Requesting Records Between:
Documents:

I am a law enforcement agent authorized to request account records and all the information I have provided is accurate.

Absenden
Geolocation

- Google maps (GPS) maps.google.com
- Maps (historical)
- Geolocation (IP address)
- https://www.iplocation.net
- http://www.infosniper.net
- https://www.openstreetmap.org
EMAIL

http://www.lettermelater.com
http://www.emkei.cz
http://www.anonymouse.com
http://www.yandex.com
# Email header analyzer

## Email Trace - Email Tracking - Result

At Tue, 19 Mar 2019 13:43:14 +0000, the email sender delivery@pnetiva.com sent you an email from the IP address 45.79.06.250 located in Fremont, California, United States.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Sender</td>
<td><a href="mailto:delivery@pnetiva.com">delivery@pnetiva.com</a></td>
</tr>
<tr>
<td>IP Address</td>
<td>45.79.06.250</td>
</tr>
<tr>
<td>IP Address Country</td>
<td>United States</td>
</tr>
<tr>
<td>IP Address State</td>
<td>California</td>
</tr>
<tr>
<td>IP Address City</td>
<td>Fremont</td>
</tr>
<tr>
<td>IP Address Postcode</td>
<td>94536</td>
</tr>
<tr>
<td>IP Address Latitude</td>
<td>37.5625</td>
</tr>
<tr>
<td>IP Address Longitude</td>
<td>-122.0004</td>
</tr>
<tr>
<td>ISP of this IP</td>
<td>Lincoln</td>
</tr>
<tr>
<td>Organization</td>
<td>Lincoln</td>
</tr>
<tr>
<td>Timezone</td>
<td>America/Los_Angeles</td>
</tr>
<tr>
<td>Local Time of this IP country</td>
<td>2019-03-19 09:32:45-07:00</td>
</tr>
</tbody>
</table>

![Map of the area around Fremont, California](image-url)
Google Images
images.Google.com

Bing
bing.com/images

Yandex (Russia)
images.yandex.com

Baidu (Chinese)
stu.baidu.com
Verexif (On-line Resource)
Removes Exif data from an image.
http://www.verexif.com/

Free OCR (On-line Resource)
Performs text recognition from an image with characters.
www.free-ocr.com

Onlineocr (On-line Resource)
Performs text recognition from an image or PDF and converts to Document (e.g. Doc, xls)
https://www.onlineocr.net/

FotoForensics (On-line Resource)
Returns metadata, and among other features, checks if an image has been manipulated.
http://fotoforensics.com/
**Stolencamerafinder (On-line Resource)**
By the image serial checks the origin of the camera, and search were are other photos taken by the camera.
http://www.stolencamerafinder.co.uk/

**Getghiro (Application)**
Application environment for forensic image analysis.
http://www.getghiro.org/
Display Video Frames

https://www.youtube.com/watch?v=K9qSsb_1iyA

http://i.ytimg.com/vi/K9qSsb_1iyA/0.jpg
http://i.ytimg.com/vi/K9qSsb_1iyA/1.jpg
http://i.ytimg.com/vi/K9qSsb_1iyA/2.jpg
http://i.ytimg.com/vi/K9qSsb_1iyA/3.jpg

Reverse Video

https://inteltechniques.com/menu.html

Metadata

https://citizenevidence.amnestyusa.org
Awesome OSINT

A curated list of amazingly awesome open source intelligence tools and resources. Open-source intelligence (OSINT) is intelligence collected from publicly available sources. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources).

Contents

- General Search
- Main National Search Engines
- Meta Search
- Specialty Search Engines
- Visual Search and Clustering Search Engines
- Similar Sites Search
- Document and Slides Search
- Pastebins
- Code Search
- Major Social Networks
- Real-Time Search, Social Media Search, and General Social Media Tools
- Social Media Tools
  - Twitter
  - Facebook
  - Google+
  - Instagram
  - Pinterest
  - Reddit
  - VKontakte
  - Tumblr
  - LinkedIn
- Blog Search
- Forums and Discussion Boards Search
https://inteltechniques.com/index.html
Thank you for your attention!

Bogdan CÎINARU
Tel.: +31611782482
bogdan.ciinaru@europol.europa.eu