



# OSINT

## NSA surveillance for hipsters

# OSINT – Open Source Intelligence

- In this context:
  - Information that is available publicly or is not heavily restricted to only specific group of people
  - We will focus on the Internet and intelligence found there
- Techniques depends on target:
  - Human or a group of people
  - Organization
  - Website

# OPSEC – Operations Security

- Shameful wiki copy/paste:
  - **Operations security (OPSEC)** is a term originating in U.S. military jargon, as a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information

# Dorking – Google is your friend

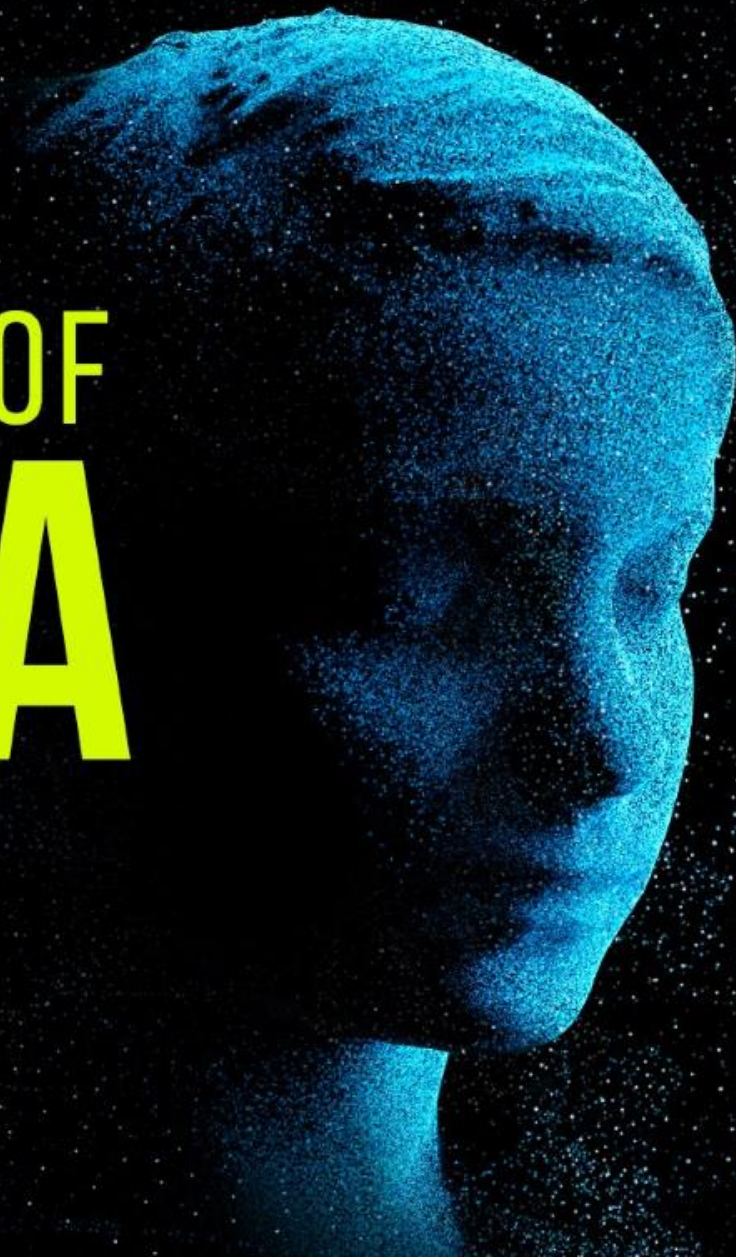
- Basic dorks that everyone knows but nobody uses them:
  - „site:“, „inurl:“
  - Reverse image search
- „site:“
  - Very helpful to narrow down search results to a particular site
  - Or to exclude them...

# „muni.cz“ site:pastebin.com

- <https://pastebin.com/i80uCT42>
  - LDAP debug logs
- <https://pastebin.com/JbKpYx9W>
  - [redacted] running sqlmap against „minotaur.fi.muni.cz“
  - ... and successfully found injection via parameter...
- <https://pastebin.com/4yvCgWg3>
  - CSIRT notification to some Croatia guys doing port scan on MUNI network
- ... + 99% of homeworks for PB162 (Java Introduction)
- What else? Try it ;)

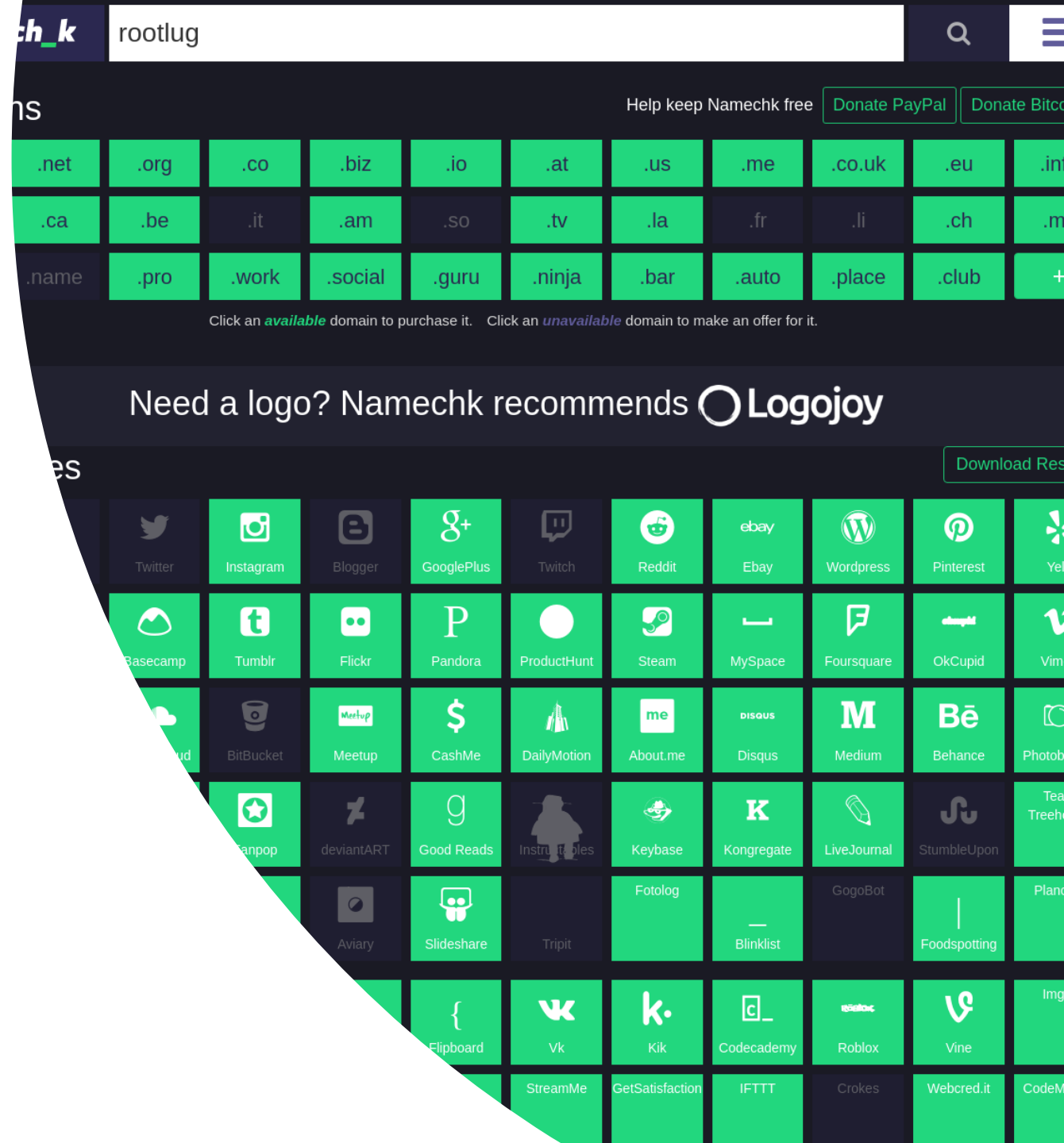


# THE HUMAN FACE OF **BIG DATA**



# Username checks

- namechk.com
- checkusernames.com



# Mailtester.com

## E-mail address verification

E-mail address

**xcarnog@fi.muni.cz**

Mail server found for domain:  
- relay.muni.cz (priority 50, ip address: 147.251.4.35)  
Mailserver identification:  
minas.ics.muni.cz ESMTP Sendmail 8.14.4/8.14.4/Debian-4+deb7u1; Wed, 1 Nov 2017 23:22:49 +0100; (No UCE/UBE) logging access from: mail.edustria.be(OK)-mail.edustria.be [185.159.220.230]  
E-mail address is valid


SMTP commands are your friends:


- VRFY
- EXPAND





# Reverse image search

- Google images: images.google.com
  - Just drag & drop a picture
- TinEye: tineye.com
  - Long time elite
  - Can track original location

 TinEye

 Upload or enter Image URL






JPEG, 140x139, 5.6 KB

**1 result**

Searched over **23.3 billion images** in 0.5 seconds.  
for: avatar.jpg

Best match ▼

Filter by domain/collection



JPEG, 128x128, 3.8 KB

[Compare Match](#)

**superuser.com**

Filename: [7dd6cb972d169a35532e95436e2a8347](#)

Found on: [questions/tagged/connection](#)  
Page crawled on Jul 29, 2014

Found on: [questions/tagged/ssh](#)  
Page crawled on Jul 26, 2014

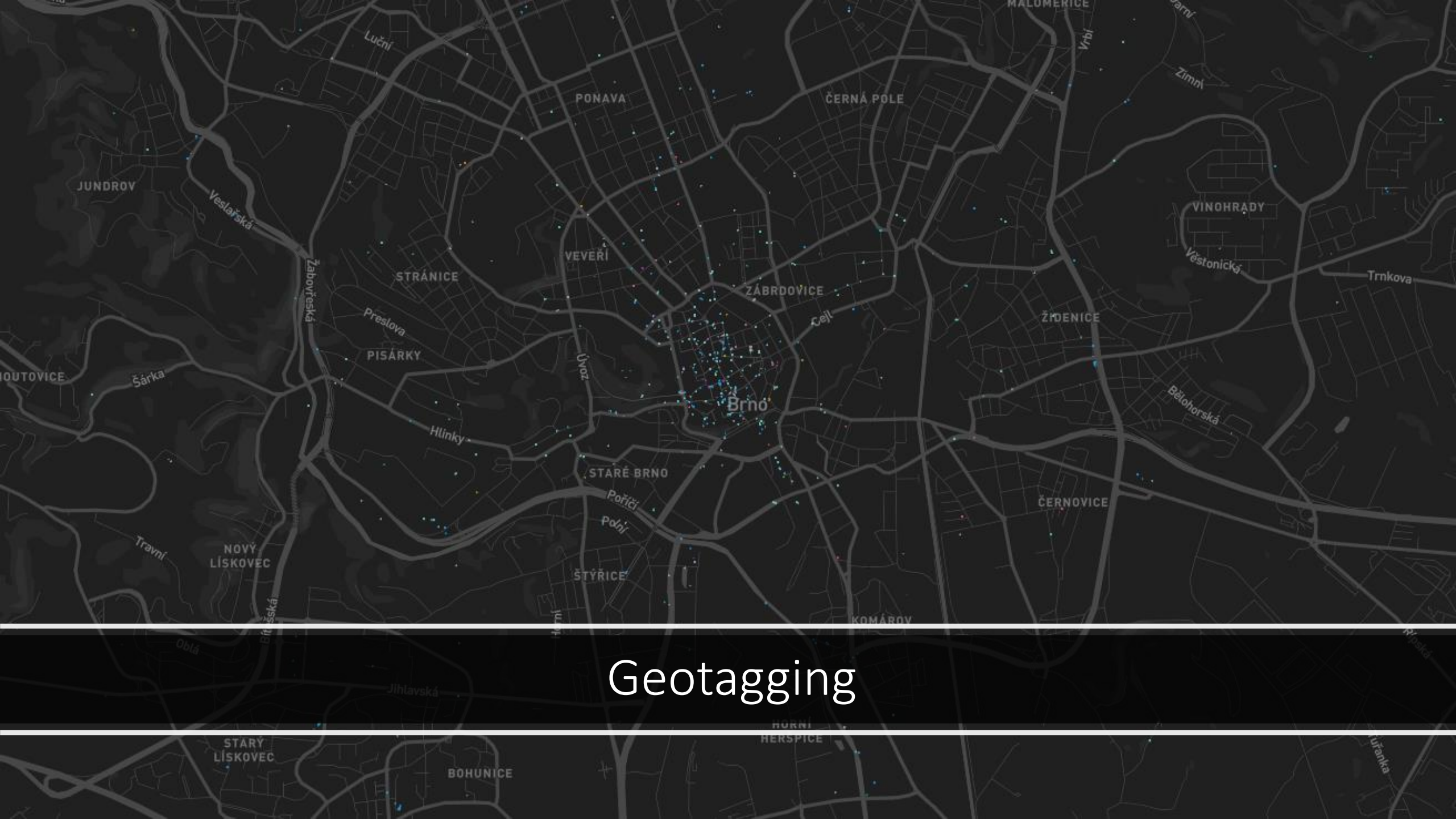
[view all 3 matches](#)

# Facebook – link picture to a profile

---

- [https://scontent-vie1-1.xx.fbcdn.net/v/t31.0-8/22291334\\_1812769128750995\\_4485931666373875347\\_o.jpg?oh=ecbfb7f4a79f21be8a116eb31a7b4559&oe=5A446272](https://scontent-vie1-1.xx.fbcdn.net/v/t31.0-8/22291334_1812769128750995_4485931666373875347_o.jpg?oh=ecbfb7f4a79f21be8a116eb31a7b4559&oe=5A446272)
- [facebook.com/1812769128750995](https://www.facebook.com/1812769128750995)





# Geotagging

# Twitter Geo-location

- Almost every mobile phone has a GPS
  - Most social networks attach GPS coordinate to the message
  - Some are publicly available
- Modern browsers have also basic geo location features
  - No built-in GPS so less accurate
  - Still accurate enough mostly to hundred few meters
- Tools:
  - <https://www.mapd.com/demos/tweetmap/>
  - Creepy (<https://twitter.com/creepy>)



# Geotagging

- Oops...

- [https://www.schneier.com/blog/archives/2015/06/us\\_identifies\\_a.html](https://www.schneier.com/blog/archives/2015/06/us_identifies_a.html)
- <https://www.techlicious.com/blog/isis-terrorist-selfie-bombing/>
- <https://twitter.com/davidthomson/status/559302457357258753>





# Image metadata

- Software : 7.0.6
- Lens Make : Apple
- Lens Model : iPhone 5s back camera 4.12mm f/2.2
- GPS Latitude Ref : North
- GPS Longitude Ref : East
- GPS Altitude Ref : Above Sea Level
- GPS Time Stamp : 18:32:17.18
- GPS Img Direction Ref : True North
- GPS Img Direction : 242.1097561
- GPS Altitude : 225.3 m Above Sea Level
- GPS Position : 49 deg 12' 24.19" N, 16 deg 37' 26.79" E
- Run Time Since Power Up : 10 days 23:12:22
- Create Date : 2014:04:23 20:32:38.378
- Date/Time Original : 2014:04:23 20:32:38.378

# Metadata on social networks

<http://www.embeddedmetadata.org/social-media-test-results.php>

Social Media site/system	Summary	Displays correctly?		Displays 4Cs?	Save As embedded?			Download embedded?		
<b>Dropbox</b> - <a href="http://www.dropbox.com">www.dropbox.com</a> Tested in late 2015	No embedded metadata shown. Embedded metadata only preserved in the downloaded image file but not in the SaveAs. Compared to 2013: also SaveAs files preserved metadata then = <b>decline</b>									
<b>Facebook</b> - <a href="http://www.facebook.com">www.facebook.com</a> Tested in late 2015	No embedded metadata shown. SaveAs file preserved Copyright Notice and Creator in IIM, anything else is stripped off. Surprise: 2 IIM fields contain data generated by Facebook. Compared to 2013: at least 2 fields in IIM survive now = <b>slight improvement</b>									
<b>Flickr FREE account</b> - <a href="http://www.flickr.com">www.flickr.com</a> Tested in late 2015	Some embedded metadata fields are shown, all correctly, but not all rights-relevant 4Cs. Embedded metadata is stripped off SaveAs files but preserved in downloaded files. Compared to 2013: <b>plus</b> = any downloaded file preserves metadata now; <b>minus</b> = even high resolution SaveAs file does not preserve it now.									
<b>Google Photo</b> - <a href="http://photos.google.com">photos.google.com</a> Tested in late 2015	Some embedded metadata fields are shown, all correctly, but not all rights-relevant 4Cs. SaveAs works only for downscaled files - only Exif metadata is preserved. Downloaded files preserved all metadata. Compared to 2013/Google+ photos: SaveAs file gets IIM and XMP metadata stripped off now = <b>decline</b>									
<b>Instagram</b> - <a href="http://instagram.com">instagram.com</a> Tested in late 2015	Tested using the Instagram iOS app v 6.4.1: No embedded metadata fields are shown. No retrieval of image files possible. Compared to 2013: then SaveAs was possible - with stripped off metadata.									
<b>LINKED IN 2015</b> - <a href="http://www.linkedin.com">www.linkedin.com</a> Tested in late 2015	No embedded metadata shown. Only embedded Exif fields are preserved in SaveAs files. Compared to 2013: not tested then.									
<b>Pinterest</b> - <a href="http://www.pinterest.com">www.pinterest.com</a> Tested in late 2015	No embedded metadata shown. Embedded metadata preserved in high resolution/original size images, but IIM and XMP metadata is stripped off in downscaled images. Compared to 2013: the loss of IIM and XMP metadata in downscaled images was not tested then.									
<b>Tumblr</b> - <a href="http://www.tumblr.com">www.tumblr.com</a> Tested in late 2015	No embedded metadata shown. Only the embedded Exif fields are preserved in the SaveAs image files, IIM and XMP metadata is stripped off. Compared to 2013: in SaveAs files all metadata were preserved then = <b>decline</b>									
<b>Twitter</b> - <a href="http://www.twitter.com">www.twitter.com</a> Tested in late 2015	No embedded embedded metadata shown. Only downscaled images are available for SaveAs and the metadata are stripped off such files. Compared to 2013: no change									

# pipl.com

- Search engine specifically created to aggregate social profiles
- Alternative with API access: fullcontact.com

intense.feel@gmail



intense.feel@gmail.com

Location (optional)



Martin Čarnogurský  
([intense.feel@gmail.com](mailto:intense.feel@gmail.com))

SPONSORED:

[Contact Info](#)

[Email Report](#)



CAREER:

IT Security Analyst & Developer at Honeywell Tech



EDUCATION:

Bachelor's degree from Masaryk University Brno,



PLACES:

Slovakia  
Brno, Czech Republic



Martin Čarnogurský, Brno, Czech Republic, Slovakia

[linkedin.com/in/martin-čarnogurský-4747834a](https://www.linkedin.com/in/martin-čarnogurský-4747834a)

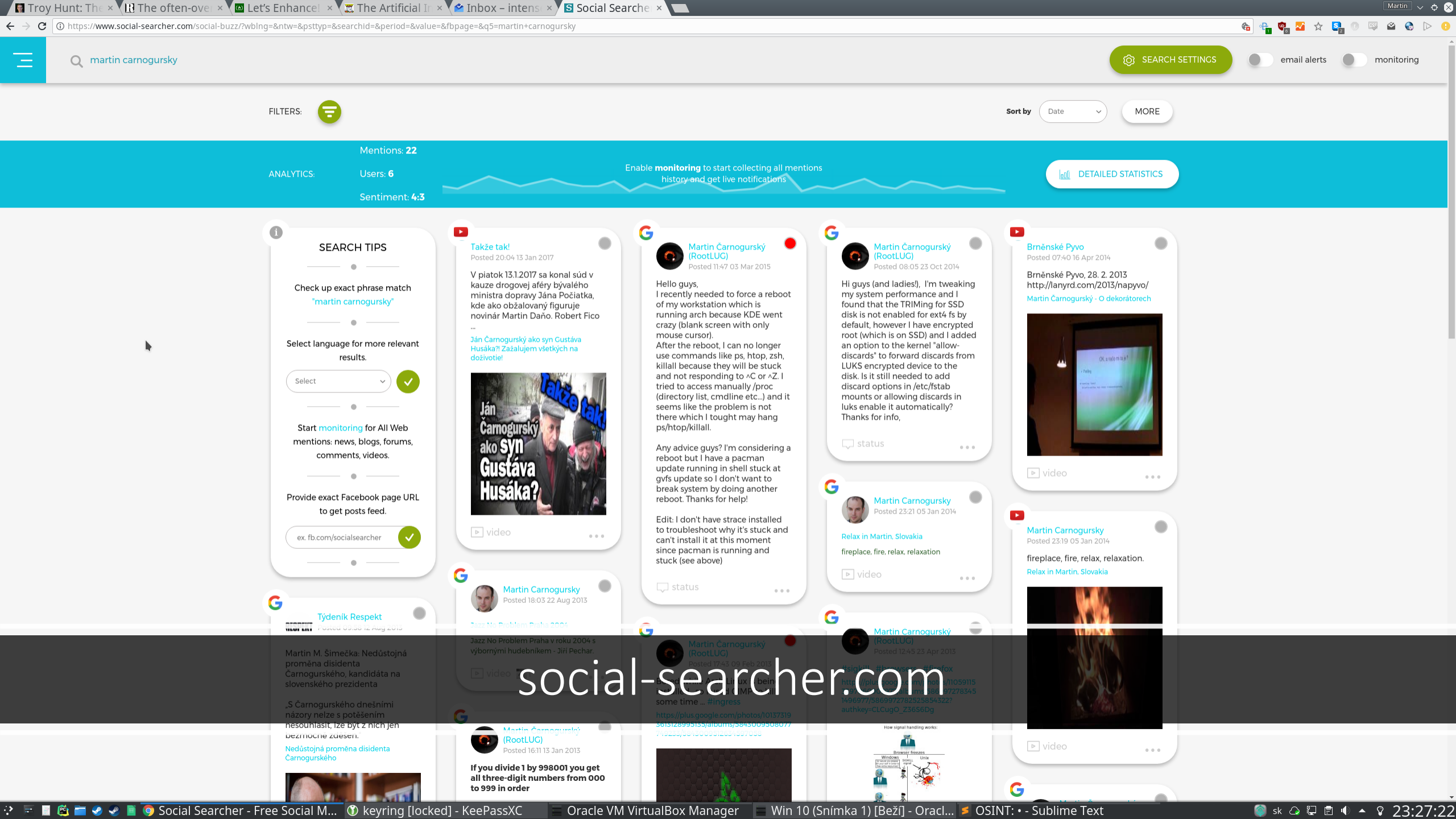
Professional Profile & Networking - LinkedIn



[intense.feel@gmail.com](mailto:intense.feel@gmail.com) - intense

[en.gravatar.com/7dd6cb972d169a35532e95436e2a8347](https://en.gravatar.com/7dd6cb972d169a35532e95436e2a8347)

Globally Recognized Avatars - Gravatar



# Schrödinger intel

- Information online is created and deleted
- When deleted – is it gone?
  - Retention policy
  - „Backups made by big brother“ / „3-letter agencies“
  - Someone in this world might still have a copy...
- TL;DR no OSINT?
- The Internet Archive project comes to our rescue!
  - Makes snapshots of online publicly accessible websites / documents
  - Some are made automatic, some manually requested



# Schrödinger intel – use case

---

- 1<sup>st</sup> October 2017 – Mass shooting in Las Vegas
- His wife had a facebook profile
  - Deleted by her (obviously...)
  - ... so is it gone?
- Nope <https://archive.is/kMdJb>



# Bypassing social media ACL

- Use mobile phones!
  - Android can be run inside emulator
- Still works for a huge number of social networks:
  - Signal, telegram, snapchat ...
  - Twitter accounts with „find by email“ disabled
  - Facebook phone number <-> profile pairing

# Have I been pwned?

- <https://haveibeenpwned.com/>
- Track publicly disclosed breaches
- Coinhive hacked:
  - [https://www.theregister.co.uk/2017/10/24/coin\\_hive\\_hacked\\_password\\_reuse/](https://www.theregister.co.uk/2017/10/24/coin_hive_hacked_password_reuse/)
- Password keyring ... anyone?



# ~~Linkedin~~ Leaked

Leaked

in

Stories About Data Leaks and Related Stuff

Home

About

Disclaimer

Abuse

phpMyAdmin SQL Dump

Posted by PasteMon on November 11th, 2016

149 voted

vote

Detected 1 occurrence(s) of '^~ phpMyAdmin SQL Dump':

```
-- phpMyAdmin SQL Dump
-- version 4.6.4
-- https://www.phpmyadmin.net/
--
-- 8Y8%NÑ, : localhost:8889
8'Ñ8888Ñ Ñ8%8·8'8°8%8,Ñ: 88%Ñ 11 2016 8³., 10:08
8'8µÑ8Ñ8,Ñ Ñ8µÑ88²8µÑ88°: 5.6.28
¹8µÑ8Ñ8,Ñ PHP: 7.0.10

\L_MODE = "NO_AUTO_VALUE_ON_ZERO";
\8_zone = "+00:00";

·°

~stebin.com/raw.php?i=CZRc09n1
```

PasteMon

Tags: [pastebin.com](#), [phpMyAdmin SQL Dump](#)

Comments Off on phpMyAdmin SQL Dump

with Interesting Data

11th, 2016

~qin|password|email|uid) \|':

~d\_date

Go

TOP-5 LEAKS

VISA Credit Card (424)

Simple Password (278)

MasterCard Credit Card (274)

Tracking Number (207)

Email Addresses List (203)

TAG CLOUD

Apache Configuration Directive API

Key Certificate Cisco Configuration

with Enabled Password Command Line

Password CVE Reference Default

Credentials Default Security Password

Dropbox Shared File E-mail

Headers Email/Password

Dump Email

Addresses List Exploit

Hacked Data Hacking

Notification HTTP POST

HTTP Proxies List IP Addresses

List Leaked Data MD5/SHA1

Hash MD5/SHA1 Hashes

MySQL Access Control MySQL

Connect Information

MySQL Table with

Email/Password Dump MySQL

Table with Interesting Data

MySQL Table with

Passwords MySQL URI Nmap

Scan Report Obfuscated





OSINT: Organizations



TOTAL RESULTS

3,943

TOP COUNTRIES

Czech Republic	3,943
----------------	-------

TOP SERVICES

SSH	730
HTTP	638
Portmap	557
HTTPS	426
NTP	397

TOP ORGANIZATIONS

Masarykova univerzita - Ustav vypocetni techniky	3,943
--	-------


TOP OPERATING SYSTEMS

Windows 7 or 8	22
Linux 3.x	17
Linux 2.6.x	10
Unix	5
Windows 8	3

TOP PRODUCTS

OpenSSH	505
---------	-----

RepearExplorer Galaxy

147.251.253.166  
cloud89b.cerit-sc.cz  
**Masarykova univerzita - Ustav vypocetni techniky**  
Added on 2017-11-01 22:04:55 GMT  
 Czech Republic, Brno  
[Details](#)

**SSL Certificate**

Issued By:  
|- Common Name: **TERENA SSL CA 3**  
|- Organization: **TERENA**  
Issued To:  
|- Common Name: **galaxy-elixir.cerit-sc.cz**  
|- Organization: **Masarykova univerzita**

**Supported SSL Versions**

TLsv1, TLsv1.1, TLsv1.2

**Diffie-Hellman Parameters**

**Fingerprint:** RFC3526/Oakley Group 14

HTTP/1.1 200 OK  
Date: Wed, 01 Nov 2017 22:04:55 GMT  
Server: Apache/2.4.10 (Debian)  
Last-Modified: Tue, 26 Sep 2017 08:38:20 GMT  
ETag: "1383-55a1398f0aa16"  
Accept-Ranges: bytes  
Content-Length: 4995  
Vary: Accept-Encoding  
Cache-Control: no-cache, no-store, must-revalidate  
Pragma: no-cache  
...

217.69.96.68

mimon1.ics.muni.cz  
**Masarykova univerzita - Ustav vypocetni techniky**  
Added on 2017-11-01 21:56:58 GMT  
 Czech Republic  
[Details](#)

SSH-2.0-OpenSSH\_5.3  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEA3oGWXsB9WzzNKAg2V6b9qYi1CyybYv+FCwv09ozCDk/CtNeL6nK+RyVhKUulfy57riAY4eggXsEw4M6l+maUWy8/iuuw7ycjS1drj3Zas96Af63/IGBN4V0Drxtxfny+tKhj2QMi3lriwddD8R5SgH2uJGgce/iIWSf3vN05tJbrZiYwSSwALeHEJubJ3Kq+JimJjmKqoJkeDPqRE21tBLp60A8gS66...

147.251.22.137

cjv-phabricator.muni.cz  
**Masarykova univerzita - Ustav vypocetni techniky**  
Added on 2017-11-01 21:55:43 GMT  
 Czech Republic, Brno  
[Details](#)

SSH-2.0-OpenSSH\_6.6.1p1 Ubuntu-2ubuntu2.8  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAADAQABAAQOC7h1OcVhUAGJn+D1GN/O59B2UM1wnYH35peZe6R73rB49BvZoQ/wn1yDRqVbAOZ01IMJruES8/3/JJ0B0S5Kumy9DD1y6X/Enwrp/r3vYLK0XJKJAeoeFvYokC5PphSjTRjf1Snq92GeheICxAw64DcOMBhe+3cg3mX/zy1I+MRUW06YV5wdx1qv18AbzqH5K1d1BC...

shodan.io

# Scans.io DNS set: 250G of (OSINT) porn

- [https://scans.io/study/sonar.fdns\\_v2](https://scans.io/study/sonar.fdns_v2)
- DNS ANY responses aggregated from full IPv4 scan and other sets
- Around 250G uncompressed
- JSON data per line
- Pro tip: use jq for advanced parsing/filtering

```
λ Hydra scansio → zcat 20170908-fdns.json.gz | head
{"timestamp":"1504976471","name":"reseauocoz.cluster007.ovh.net","type":"cname","value":"cluster007.ovh.net"}
{"timestamp":"1504937052","name":"ghs.googlehosted.com","type":"cname","value":"googlehosted.l.googleusercontent.com"}
{"timestamp":"1504925049","name":"isutility.web9.hubspot.com","type":"cname","value":"a1049.b.akamai.net"}
{"timestamp":"1504927264","name":"sendv54sxu8f12g.ihance.net","type":"a","value":"52.52.146.241"}
{"timestamp":"1504927264","name":"sendv54sxu8f12g.ihance.net","type":"a","value":"54.241.184.45"}
{"timestamp":"1504975181","name":"shops.myshopify.com","type":"cname","value":"shops.myshopify.com"}
{"timestamp":"1504976736","name":"www.triblocal.com.s3-website-us-east-1.amazonaws.com","type":"cname","value":"s3-website-us-east-1.amazonaws.com"}
{"timestamp":"1504920966","name":"*.2925.com.dycdn.com","type":"a","value":"121.201.116.57"}
{"timestamp":"1504870958","name":"*.2bask.com","type":"a","value":"176.31.246.156"}
{"timestamp":"1504974204","name":"*.5thlegdata.com","type":"a","value":"199.34.228.100"}
```

# Subdomain mapping

- MUNI.cz : **31225 domains!** (unfiltered)
- Tools:
  - Sublist3r
  - SDBF (Smart DNS brute forcer)
  - Massresolver / massdns
  - Scans.io FDNS dataset

# Certificate transparency project

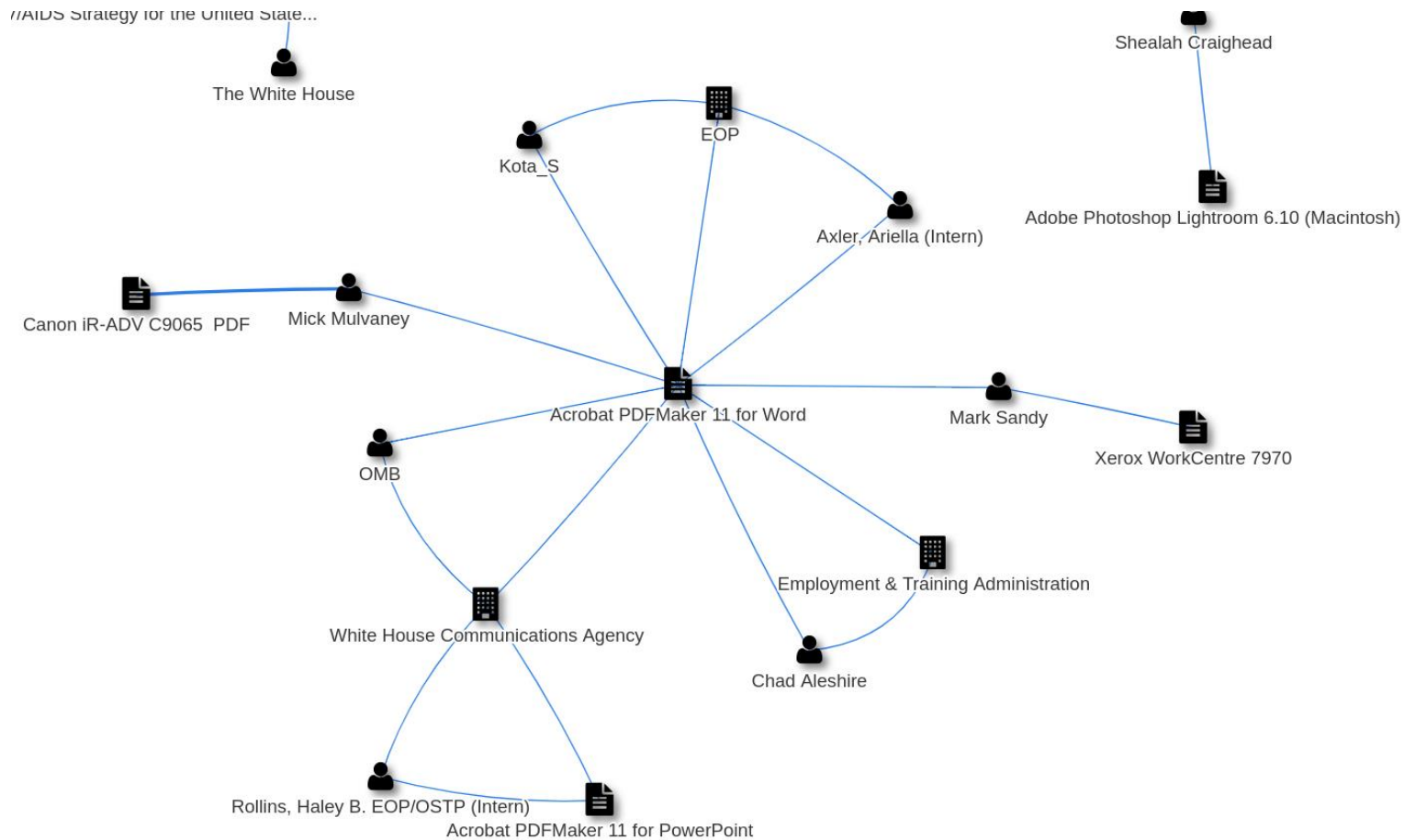
[illegible]

# Organizations: file search

- „filetype:“ dork
  - „site:whitehouse.gov filetype:pdf“
- Apart from content, file metadata is a very valuable intelligence
  - Software being used
  - Usernames
  - Emails
  - Internal file shares...
- More awesome reading: <https://blog.sweepatic.com/metadata-hackers-best-friend/>



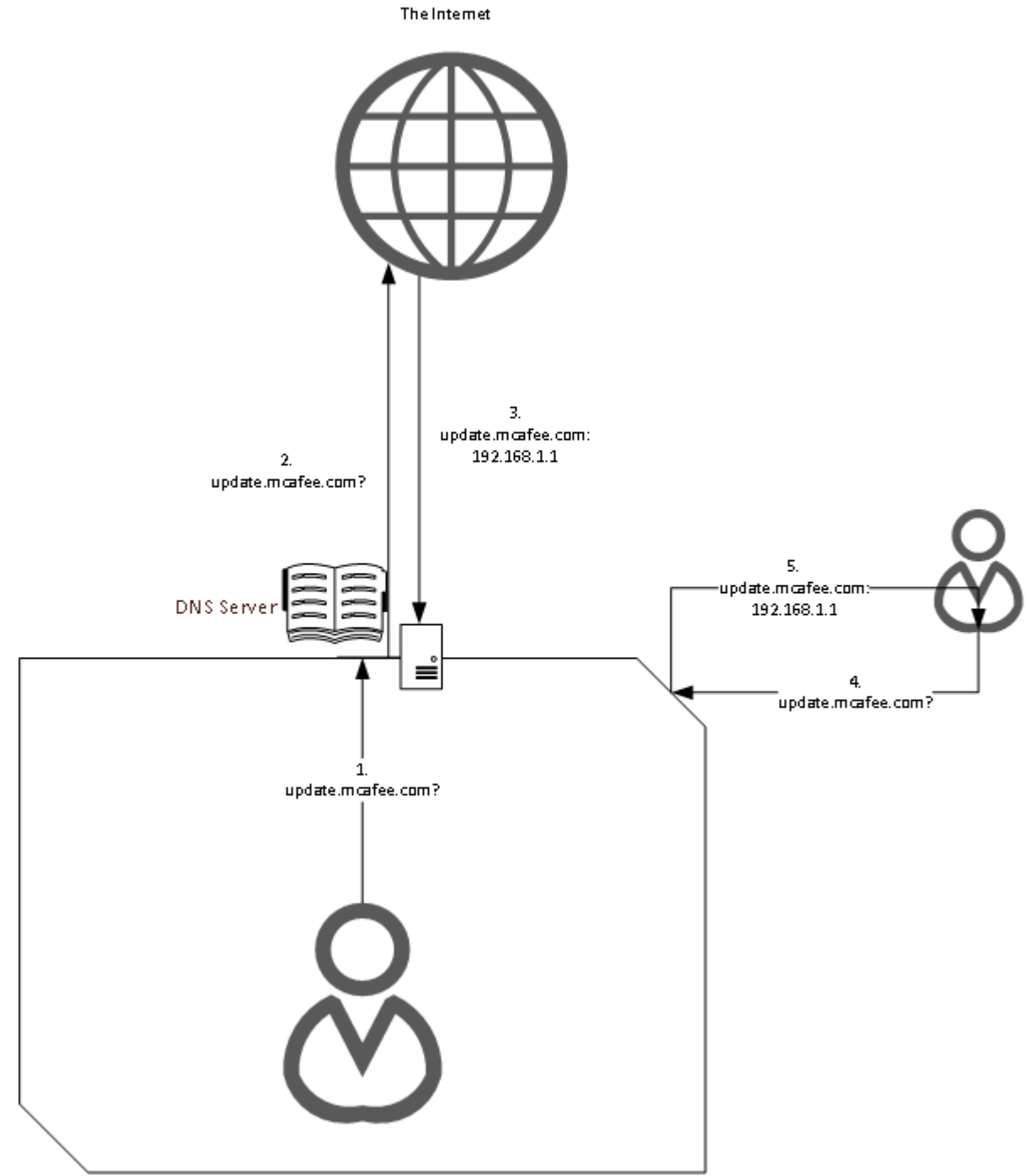
# Metadata analysis



CIA Director: „We kill people based on metadata“ <https://goo.gl/BqLMWb>

# DNS Cache snooping

- Abuse DNS cache leaks:
  - `nslookup -norecurse somedomain dns_server`
  - `dig @dns_server somedomain A +norecurse`



# Anti-OSINT: Welcome to the dark side

Delete	<p>Delete information</p> <ul style="list-style-type: none"><li>• Relative, can be sometimes recovered as shown earlier...</li></ul>
Understand	<p>Understand the process of collecting OSINT and break/manipulate it</p>
Create	<p>Create miss information</p>
Track	<p>Track OPSEC leaks</p>

# Anti-OSINT: Delete

- Self explanatory
  - Or restrict who have an access to your information
- Europe is your friend - **Right to be forgotten**
  - Request removal of your information
    - [https://www.google.com/webmasters/tools/legal-removal-request?complaint\\_type=rtbf](https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf)

# Anti-OSINT: Understand

- Workflow:
  - Take an information (for example e-mail) and reverse search to expand collected intel
  - Combine & repeat

## Solution?

- Don't use the same e-mail everywhere
  - WTF? Do I need new email for every website where I register?
  - Solution: e-mail proxies
    - Blur by Abine (<https://dnt.abine.com>)



# Anti-OSINT: Create

- Create conflicting information
  - Different birth dates
  - Different residencies
  - Information that lead to someone else

# Anti-OSINT: Track

- Force OPSEC leaks:
  - URL shorteners: can be used to track who opened the URL
  - Friend requests
  - Canary tokens
- Abusing big brother: Google adwords
  - Trigger Advertisement when someone search for you
  - Provides demographic information about triggers
  - Can be applied to other (social) advertisement networks

# Resources

## OPEN SOURCE INTELLIGENCE TECHNIQUES

RESOURCES FOR SEARCHING AND  
ANALYZING ONLINE INFORMATION

FIFTH EDITION



MICHAEL BAZZELL

- Grugq – OSINT & OPSEC guru
  - <https://medium.com/@thegrugq>
- Krypt3ia blog & twitter
  - <https://krypt3ia.wordpress.com/>
- Michael Bazzell
  - <https://inteltechniques.com/menu.html>

# Appendix: Tools

---

The screenshot displays the Maltego 3 software interface. On the left, a sidebar lists entity types under 'Infrastructure' (AS, DNS Name, Domain, IPv4 Address, Location, MX Record, NS Record, Netblock, Website) and 'Personal' (Email Address, Person, Phone Number, Phrase). The main workspace shows a central entity 'Chris Bohme' (a person) with arrows pointing to six other entities: Bianca Harck, Tanya Zandberg, Gisela Gips, Jo-Anne Steenkamp, Ruth Schwaiger, and Efrat Benai. Each entity is represented by a small profile picture. The top of the interface has tabs for 'Mining View', 'Dynamic View', 'Edge Weighted View', and 'Entity List'. On the right, there are four panels: 'Overview' showing a network graph, 'Detail View' showing the properties of 'Chris Bohme' (Type: Person, Full Name: Chris Bohme, First Names: Chris, Surname: Bohme, Image: http://www.facebook...), 'Property View' showing a table of properties, and 'Output - Transform Output \*' showing a log of a transform operation: 'Running transform To NS record [DNS] on 1 entities. Transform To NS record [DNS] returned with 5 entities.'



```

/ 2 / 44.439716 / 26.14863 / a1.booking.com / geocode /
/ 3 / 44.439716 / 26.14863 / b1.booking.com / geocode /
/ 4 / 44.439716 / 26.14863 / b2.booking.com / geocode /
/ 5 / 44.439716 / 26.14863 / c.booking.com / geocode /
/ 6 / 44.439716 / 26.14863 / cs.booking.com / geocode /
/ 7 / 44.439716 / 26.14863 / wiki.booking.com / geocode /
/ 8 / 44.439716 / 26.14863 / s1.booking.com / geocode /
/ 9 / 44.439716 / 26.14863 / ssl.booking.com / geocode /
/ 10 / 44.439716 / 26.14863 / u.booking.com / geocode /
/ 11 / 44.439716 / 26.14863 / v.booking.com / geocode /
/ 12 / 44.439716 / 26.14863 / w1.booking.com / geocode /
/ 13 / 44.439716 / 26.14863 / w2.booking.com / geocode /
/ 14 / 44.439716 / 26.14863 / w3.booking.com / geocode /
/ 15 / 44.439716 / 26.14863 / Strada Vatra Luminoasă 108, Bucharest, Romania / reverse_geocode /
+-----+

```

15 rows returned

```
[recon-ng][booking.com][reverse_geocode] > clear
```

```
Command: clear
```

```
[recon-ng][booking.com][reverse_geocode] > show hosts
```

rowid	host	ip_address	region	country	latitude	longitude	module
83	a1.booking.com	5.57.16.144	Slough, England	United Kingdom	51.5095	-0.59541	resolve
73	admin.booking.com	5.57.17.51	Amsterdam, Noord-Holland	Netherlands	52.374	4.88969	resolve
84	admin.c.booking.com	5.57.17.51	Amsterdam, Noord-Holland	Netherlands	52.374	4.88969	resolve
86	autodiscover.booking.com	5.57.20.145	Trumpington, England	United Kingdom	52.1721	0.11261	resolve
85	autodiscover.itspublic.booking.com	5.57.20.145	Trumpington, England	United Kingdom	52.1721	0.11261	resolve
87	b1.booking.com	5.57.18.140	Slough, England	United Kingdom	51.5095	-0.59541	resolve
88	b2.booking.com	5.57.18.141	Slough, England	United Kingdom	51.5095	-0.59541	resolve
78	barcelo.partner.booking.com	5.57.16.205	Slough, England	United Kingdom	51.5095	-0.59541	resolve
70	blog.booking.com	87.233.215.183	Amsterdam, Noord-Holland	Netherlands	52.374	4.88969	resolve
89	bob.booking.com	148.251.235.184	Nuremberg, Bayern	Germany	49.4478	11.0683	resolve
150	bookadmin.booking.com	5.57.16.143	Slough, England	United Kingdom	51.5095	-0.59541	reverse_res
80	bookingbutton.booking.com	5.57.16.143	Slough, England	United Kingdom	51.5095	-0.59541	resolve
90	bugs.booking.com	5.57.16.28	Slough, England	United Kingdom	51.5095	-0.59541	resolve
91	c.booking.com	5.57.16.220	Slough, England	United Kingdom	51.5095	-0.59541	resolve
120	client.perspagina.nl	54.229.233.23	Dublin, Dublin City	Ireland	53.344	-6.26719	resolve
121	client.perspagina.nl	176.34.142.255	Dublin, Dublin City	Ireland	53.344	-6.26719	resolve
118	client.presspage.com	176.34.142.255	Dublin, Dublin City	Ireland	53.344	-6.26719	resolve
119	client.presspage.com	54.229.233.23	Dublin, Dublin City	Ireland	53.344	-6.26719	resolve

# Recon-ng