Email intelligence

v 0.0.1

SPEAKER: **@soxoj**

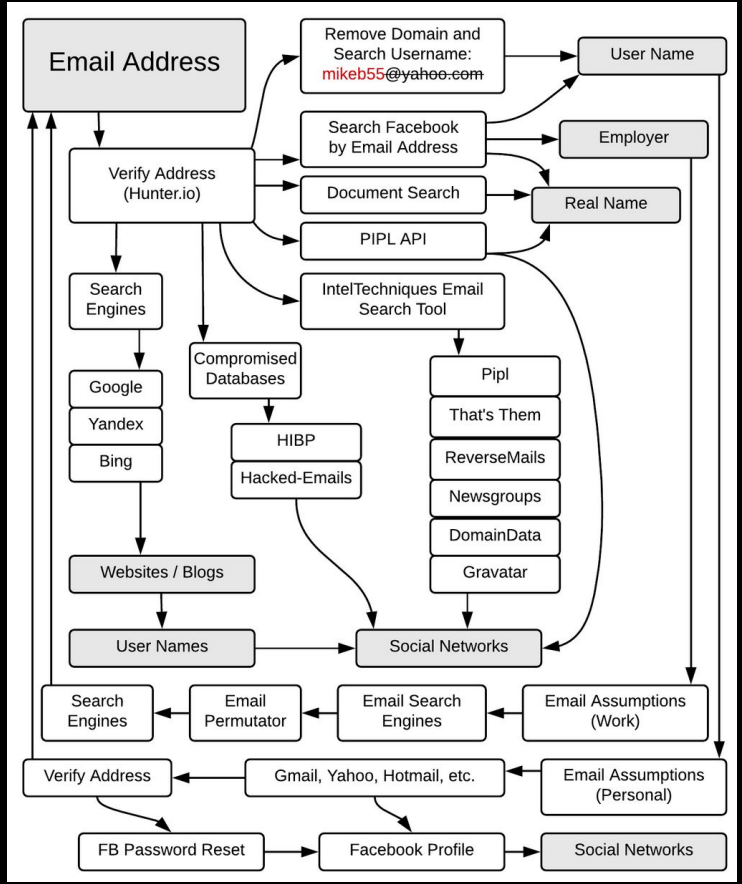
About me

Security engineer
Antifraud systems developer
OSINT enthusiast
DEFCON7495 speaker

Overview

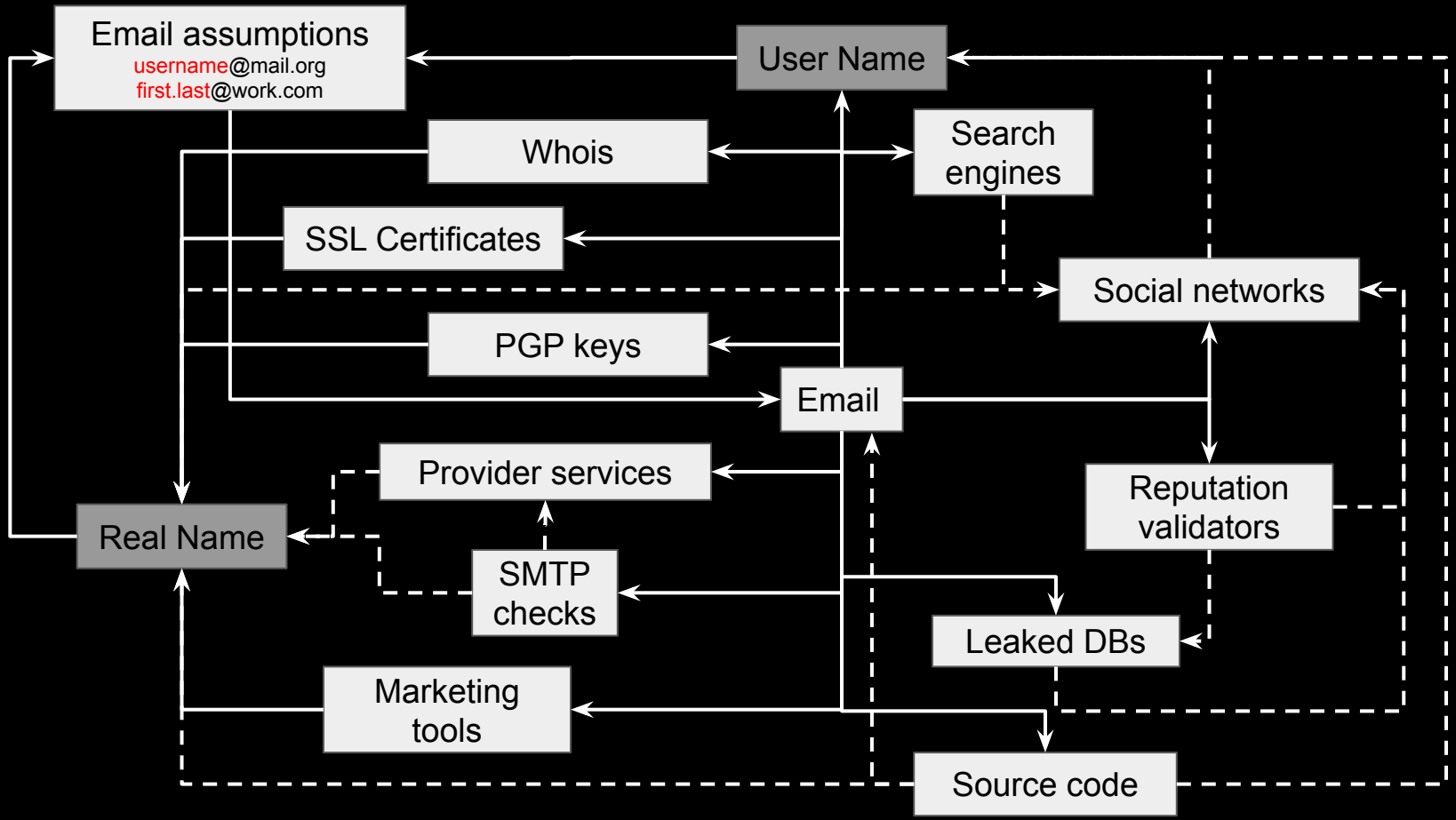
- Why are we talking about emails
- Email intelligence workflow
- Methods and services of emails checking
    - SMTP
    - Email providers and social networks
    - Whois, SSL certs, PGP keys
    - Source code
    - Email assumptions
    - Marketing & reputation tools
- Conclusions

Simplified workflow by Michael Bazzell



https://archive.is/hKP7d

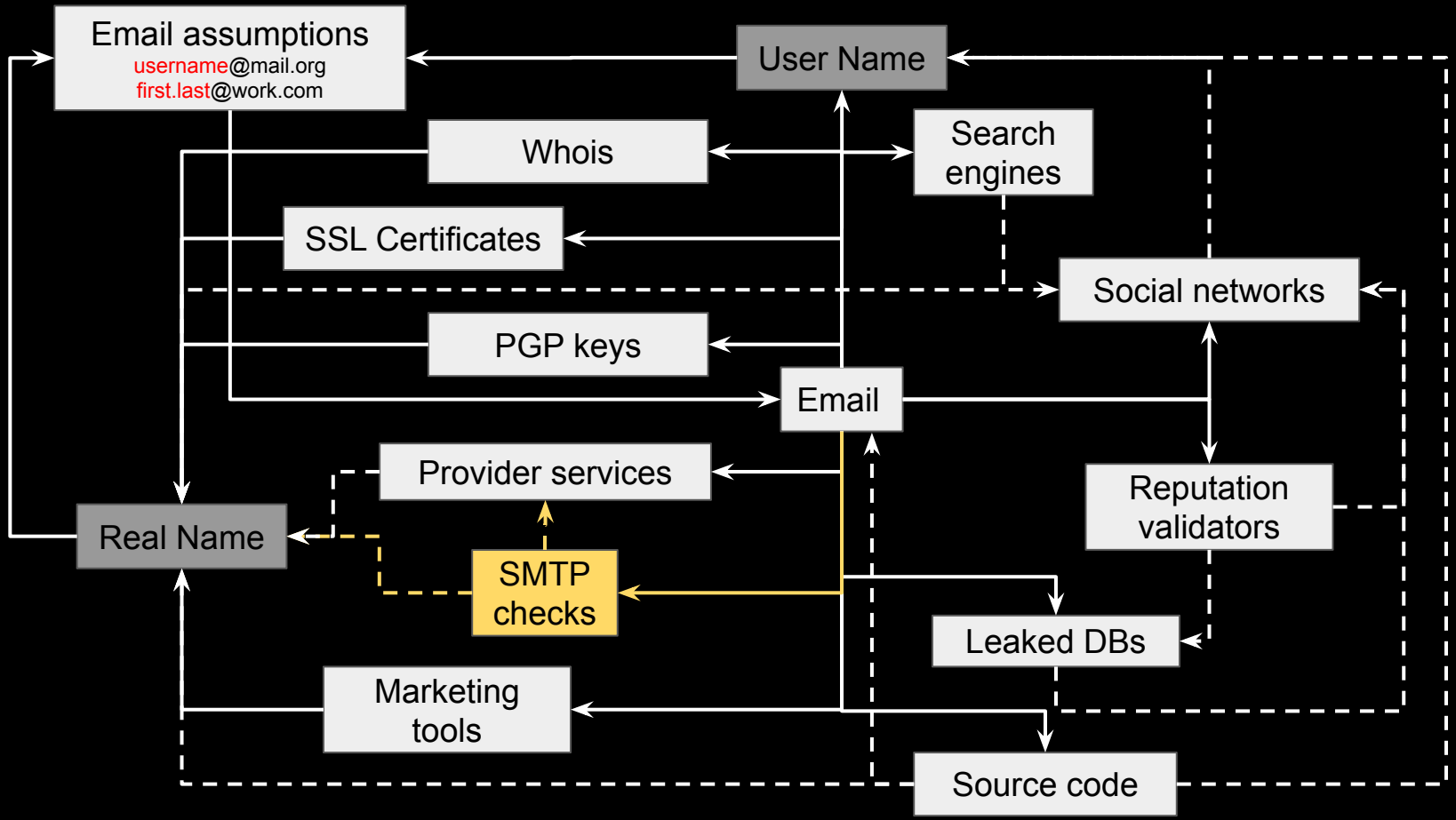
More real workflow by me



Simplified workflow

1. Validate email
2. Search information about owner
3. Gather all the relevant information, e.g. other emails
4. Exit if there is enough information
5. Repeat for the next email

Workflow overview: SMTP checks



SMTP checks

- VRFY - verify login, returns full name
- EXPN - verify and expand aliases / mailing lists
- RCPT - add recipient and check for its existence

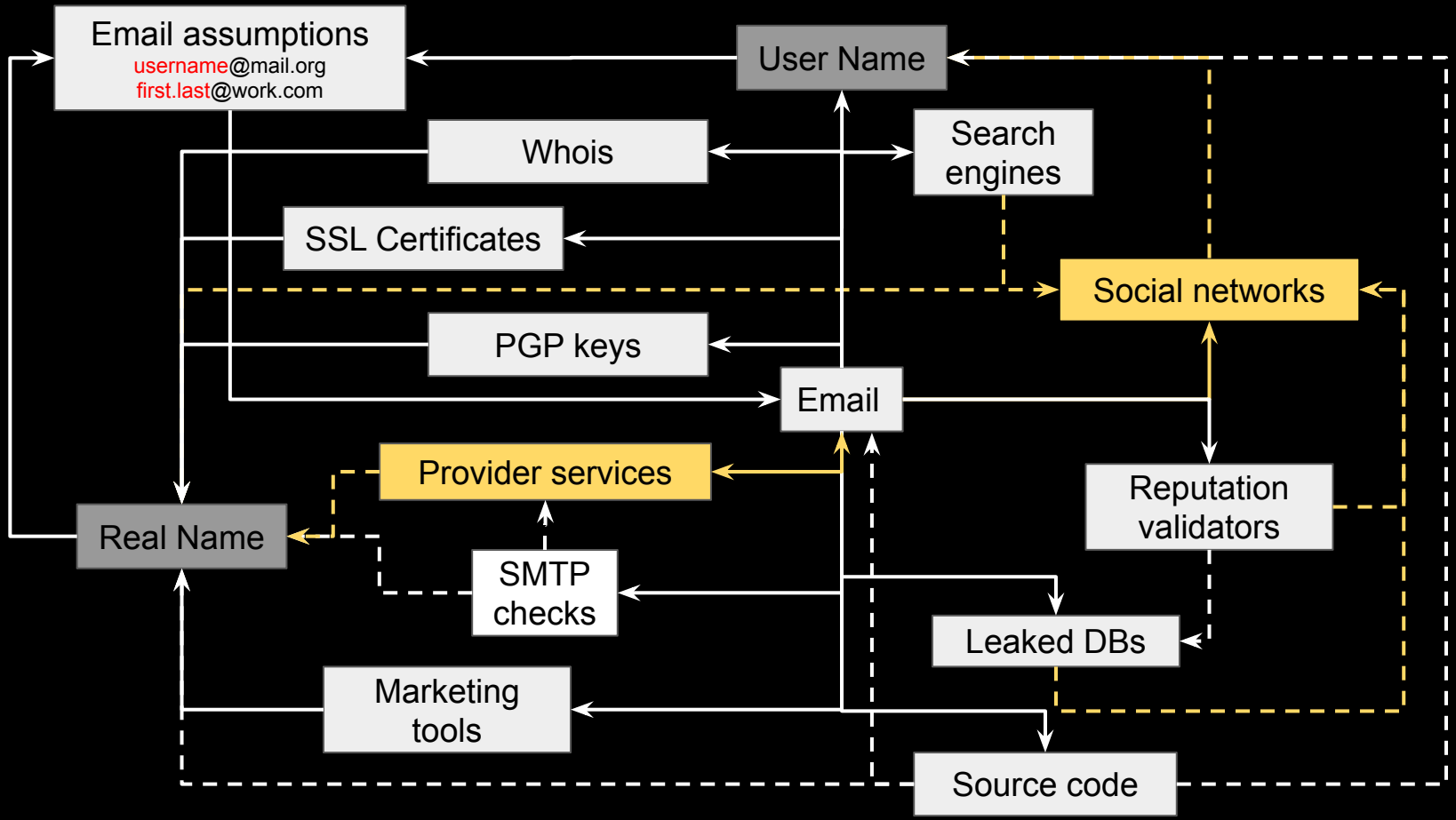
SMTP checks

- VRFY - verify login, returns full name
  old, enabled in some services only
- EXPN - verify and expand aliases / mailing lists
  old, disabled or unimplemented in most services
- RCPT - add recipient and check for its existence
  still working as a main part of protocol (gmail, yandex, etc.)

https://github.com/un33k/python-emailahoy
https://github.com/cytopia/smtp-user-enum

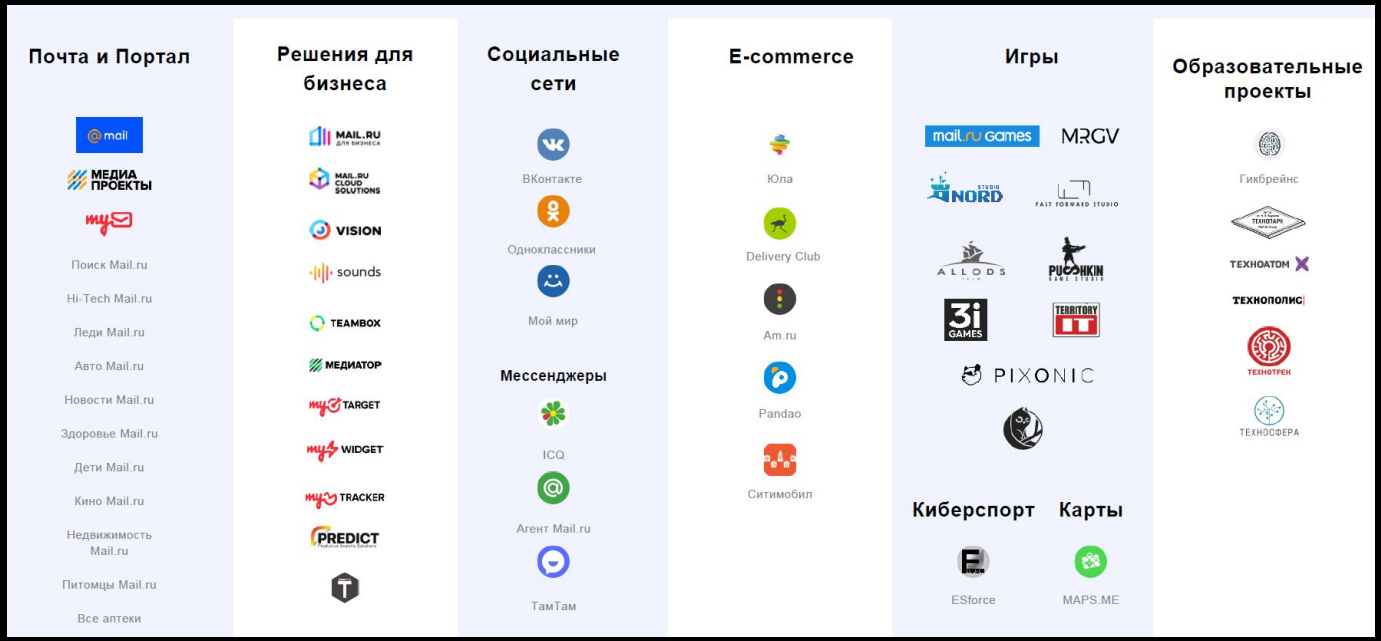
```
Connecting to mail.example.tld 25 ...
220 mail.example.tld ESMTP Sendmail 8.12.8/8.12.8; Wed, 22 Jan 2020 19:33:07 +0200
250 mail.example.tld Hello [10.0.0.1], pleased to meet you
Start enumerating users with VRFY mode ...
[----] admin              550 5.1.1 admin... User unknown
[----] OutOfBox           550 5.1.1 OutOfBox... User unknown
[SUCC] root               250 2.1.5 root <root@mail.example.tld>
[SUCC] adm                250 2.1.5 <adm@mail.example.tld>
[----] avahi-autoipd      550 5.1.1 avahi-autoipd... User unknown
[----] backup             550 5.1.1 backup... User unknown
[TEST] bin ...
```

Workflow overview: provider services and social networks



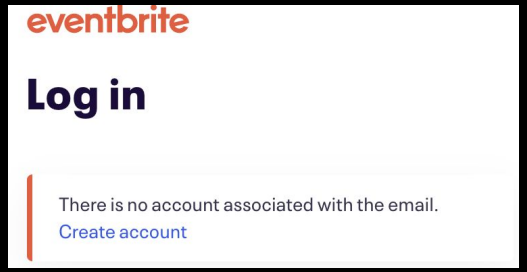
Provider services and social networks

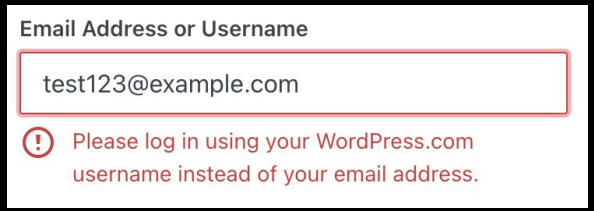
What's the difference?

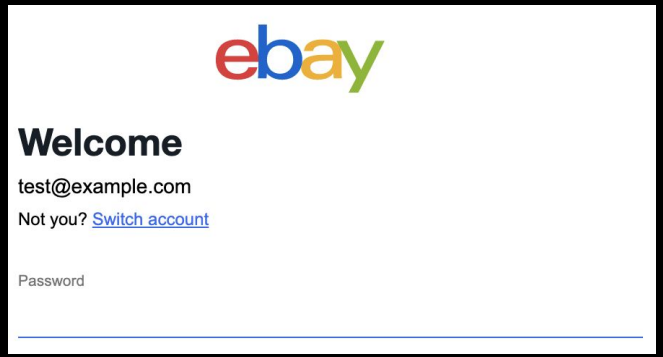


Provider services and social networks: authorization

Expectation:

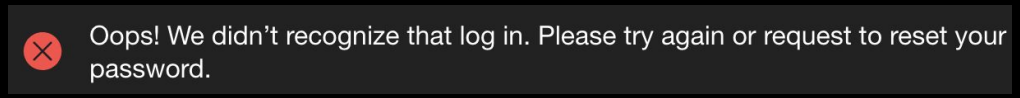


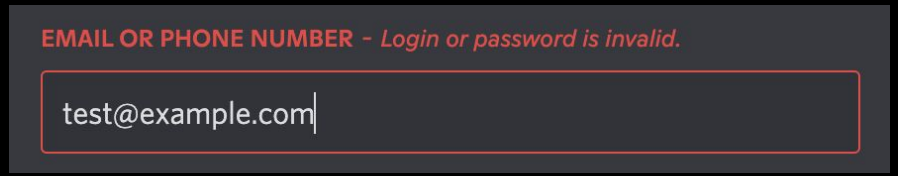


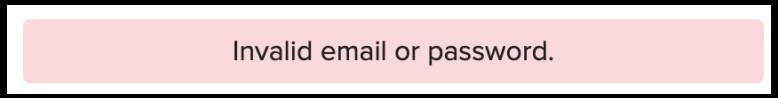


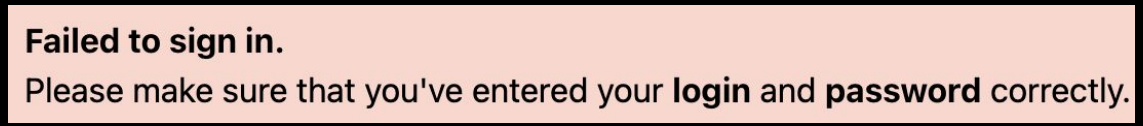
Provider services and social networks: authorization

Reality:

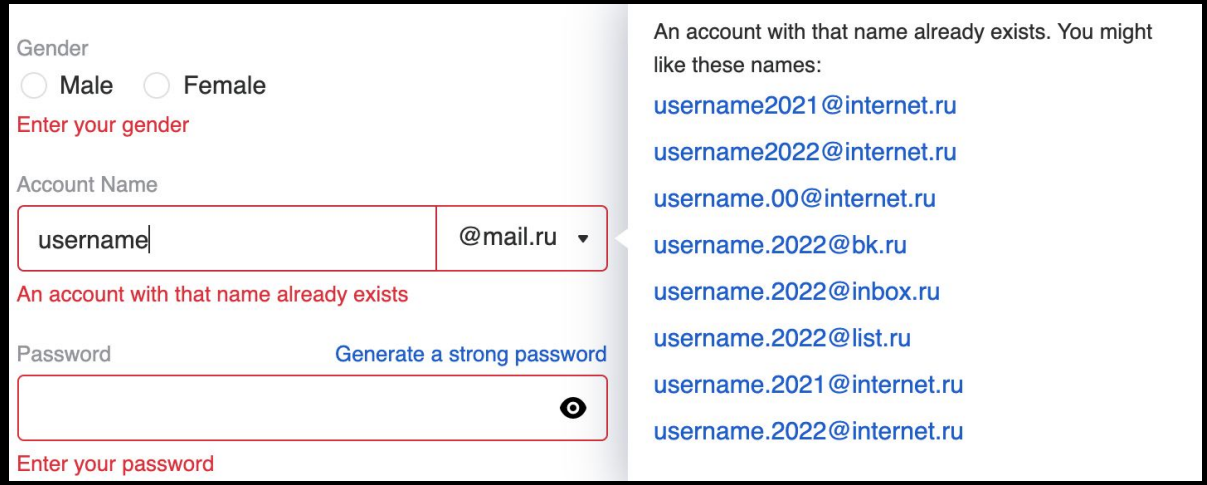


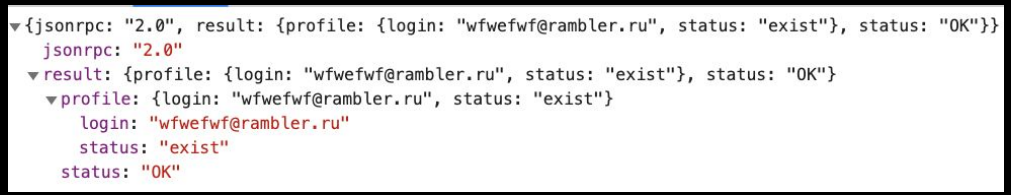




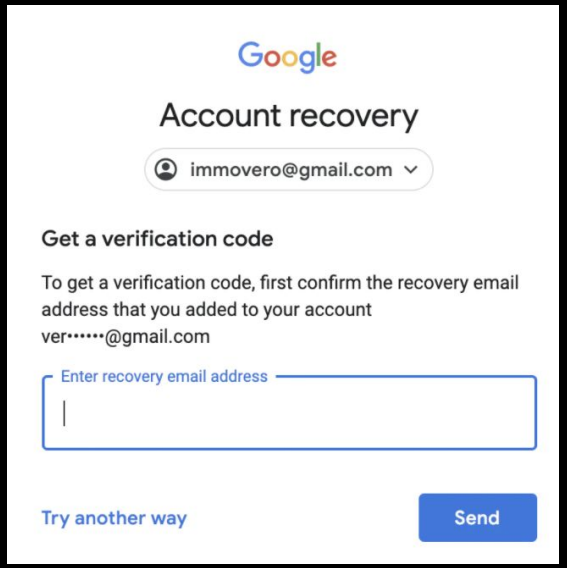


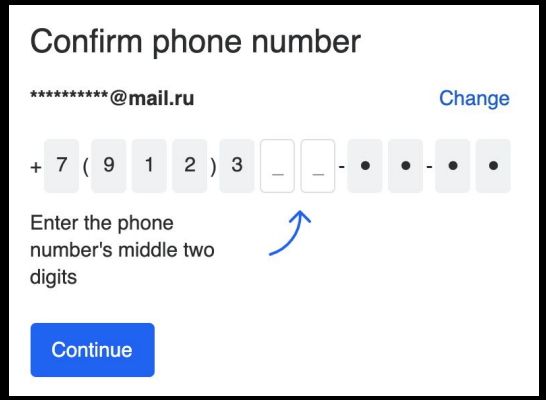
Provider services and social networks: registration

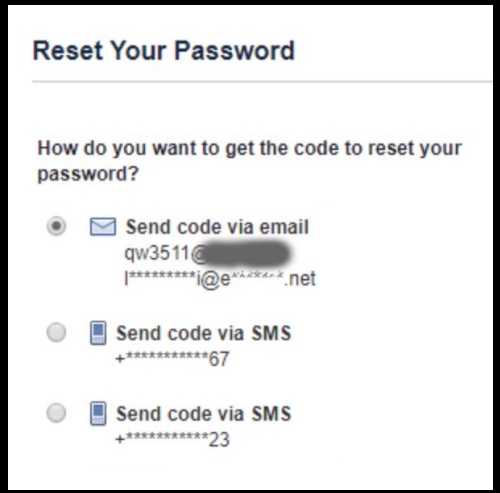




Provider services and social networks: access recovery







https://t.me/osint_mindset/62

Provider services and social networks: API

User needs first => Usable OSINT APIs

https://mail.google.com/mail/gxlu?email=<Google Email>

https://yandex.ru/collections/user/<Yandex Email Login>/

https://my.mail.ru/<Email domain>/<Email login>

https://filin.mail.ru/pic?email=<Mail.ru Email>

Provider services and social networks: API

Protonmail API: PGP key + fingerprint, uid, created_at

```
$ curl 'https://api.protonmail.ch/pks/lookup?op=get&search=soxoj@protonmail.com'
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: ProtonMail

xsBNBFmRzPgBCACmGORnj50UC6hZKVFaOxAsF1RxYs5433S0fZ/iOEQNfsyP
b5LGGqKU+r1pTsK3QrDviCIU5yQNEgpvu+u6Cki8XIDlKG3/1xo9mwQKAtSV
Wo4ECbjjNKPvosgw9/FQlRjcIWBRIN3suwH1/z+i7oEDZzW4yb0F5FCBXL0R
LTg1FaFt1tV1HKFIlMSf5LUw7+kMfsRH6kWMpeSC1aEm53W9JCflhyRw59Mm
xcN4hPO1URNeXoGKdt6Xixt7Kq9QSyQ0sIx2pekIVnN7eEOT3EO7gW3UZ7e4
```

```
$ curl 'https://api.protonmail.ch/pks/lookup?op=index&search=soxoj@protonmail.com'
info:1:1
pub:33251e162946a2e37331c07fbedadb627f2c2ca7:1:2048:1502727416::
uid:soxoj@protonmail.com <soxoj@protonmail.com>:1502727416::
```

https://github.com/pixelbubble/ProtOSINT

Provider services and social networks: tools

Holehe

- > 120 social networks
- Doesn’t notify the owner of email

Modules

Name	Domain	Method	Frequent Rate Limit
aboutme	about.me	register	✘
adobe	adobe.com	password recovery	✘
amazon	amazon.com	login	✘
amocrm	amocrm.com	register	✘
anydo	any.do	login	✓
archive	archive.org	register	✘

```
********************
   test@gmail.com
********************
[+] amazon.com
[+] any.do
[+] armurerie-auxerre.com
[+] bitmoji.com
[+] blip.fm
[+] bodybuilding.com
[+] buymeacoffee.com
[+] caringbridge.org
[+] codecademy.com
[+] coroflot.com
[+] cracked.to
[+] crevado.com
[+] deliveroo.com
[+] devrant.com
[+] diigo.com
```

Provider services and social networks: tools

Mailcat

- > 20 mail services, > 100 aliases
- Doesn’t notify the owner of email

Name	Domains	Method
Gmail	gmail.com	SMTP
Yandex	yandex.ru + 5 aliases	SMTP
Protonmail	protonmail.com + 2 aliases	API
iCloud	icloud.com, me.com, mac.com	Access recovery
tut.by	tut.by	SMTP/Registration
MailRu	mail.ru + 4 other domains	Registration
Rambler	rambler.ru + 5 other domains	Registration

```
# python3 mailcat.py username --tor -s
Tut.by:
*  username@tut.by
Yandex:
*  username@yandex.com
*  username@yandex.by
*  username@yandex.ua
*  username@ya.ru
*  username@yandex.ru
*  username@yandex.kz
Posteo:
*  username@posteo.net
*  ~50 aliases: https://posteo.de/en/help/which-
Zoho:
*  username@zohomail.com
Xmail:
*  username@xmail.net
Proton:
*  username@protonmail.com
*  username@protonmail.ch
*  username@pm.me
iCloud:
*  username@icloud.com
*  username@me.com
*  username@mac.com
```

Provider services and social networks: tools

GHunt

- Get info by email + document, YouTube, GAIA ID

- Extract real name, photo, YouTube channels, reviews, other usernames, calendar events, ...

```
# python3 ./ghunt.py email username@gmail.com

     .d8888b.  888    888                  888
    d88P  Y88b 888    888                  888
    888    888 888    888                  888
    888        8888888888 888  888 88888b.  888888
    888  88888 888    888 888  888 888 "88b 888
    888    888 888    888 888  888 888  888 888
    Y88b  d88P 888    888 Y88b 888 888  888 Y88b.
     "Y8888P88 888    888  "Y88888 888  888  "Y888

[+] 1 account found !

----------------------------

[-] Couldn't find name

[-] Default profile picture

Last profile edit : 2019/03/01 14:20:02 (UTC)

Email : username@gmail.com
Google ID : 105168534814143263578

Hangouts Bot : No

[-] Unable to fetch connected Google services.

Google Maps : https://www.google.com/maps/contrib/105168534814143263578/reviews
[-] No reviews

Google Calendar : https://calendar.google.com/calendar/u/0/embed?src=username@gmail.com
[-] No public Google Calendar.
```

Provider services and social networks: tools

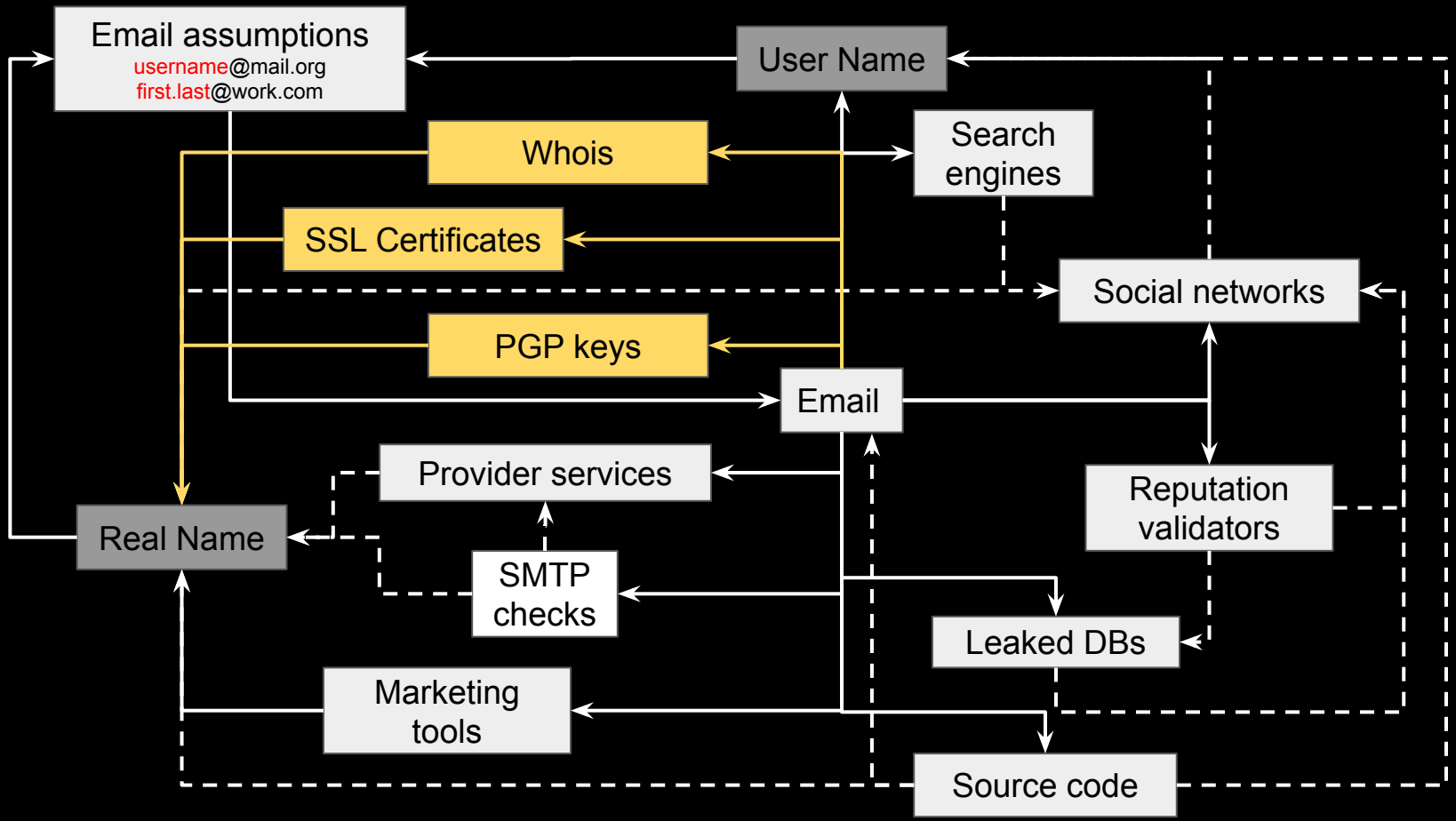
Other Google API tools

See also:

- https://tools.epieos.com/email.php
- https://t.me/UniversalSearchBot
- https://twitter.com/subfnSecurity/status/1255741950914727942


```
{
  "principal": [
    {
      "id": "users/10980222271073[redacted]",
      "user": {
        "gaiaId": "10980222271073[redacted]",
        "email": "[redacted]98@gmail.com",
        "lookupKeyEmail": "[redacted]13@mail.ru"
      }
    }
  ]
}
```

Workflow overview: sites and privacy

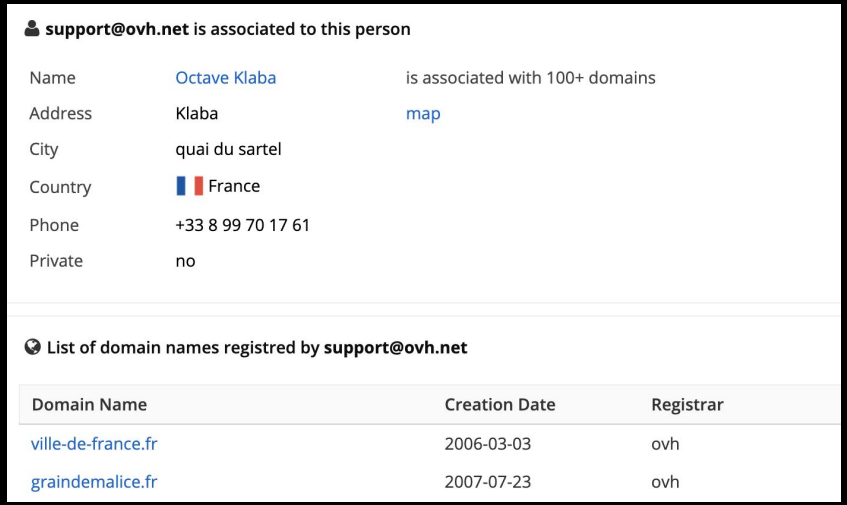


Domains, certificates, email encryption

Look for official email & name pairs

Examples:

- Search by domain registrant email: https://domainbigdata.com/
- Search by certificate identity email: https://crt.sh/?a=1
- Search by PGP keys owner email: https://pgp.mit.edu/

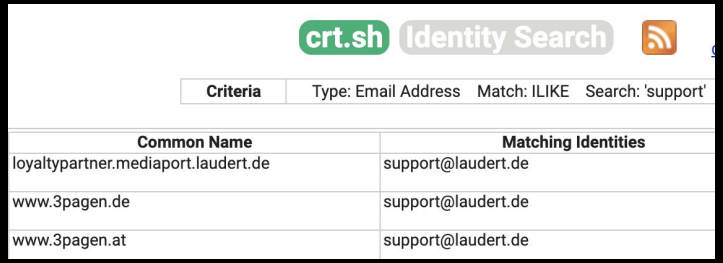


support@ovh.net is associated to this person

Name	Octave Klaba	is associated with 100+ domains
Address	Klaba	map
City	quai du sartel	
Country	France	
Phone	+33 8 99 70 17 61	
Private	no	

List of domain names registred by **support@ovh.net**

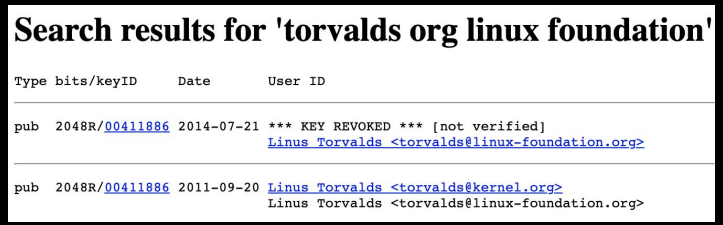
Domain Name	Creation Date	Registrar
ville-de-france.fr	2006-03-03	ovh
graindemalice.fr	2007-07-23	ovh



crt.sh Identity Search

Criteria	Type: Email Address	Match: ILIKE	Search: 'support'

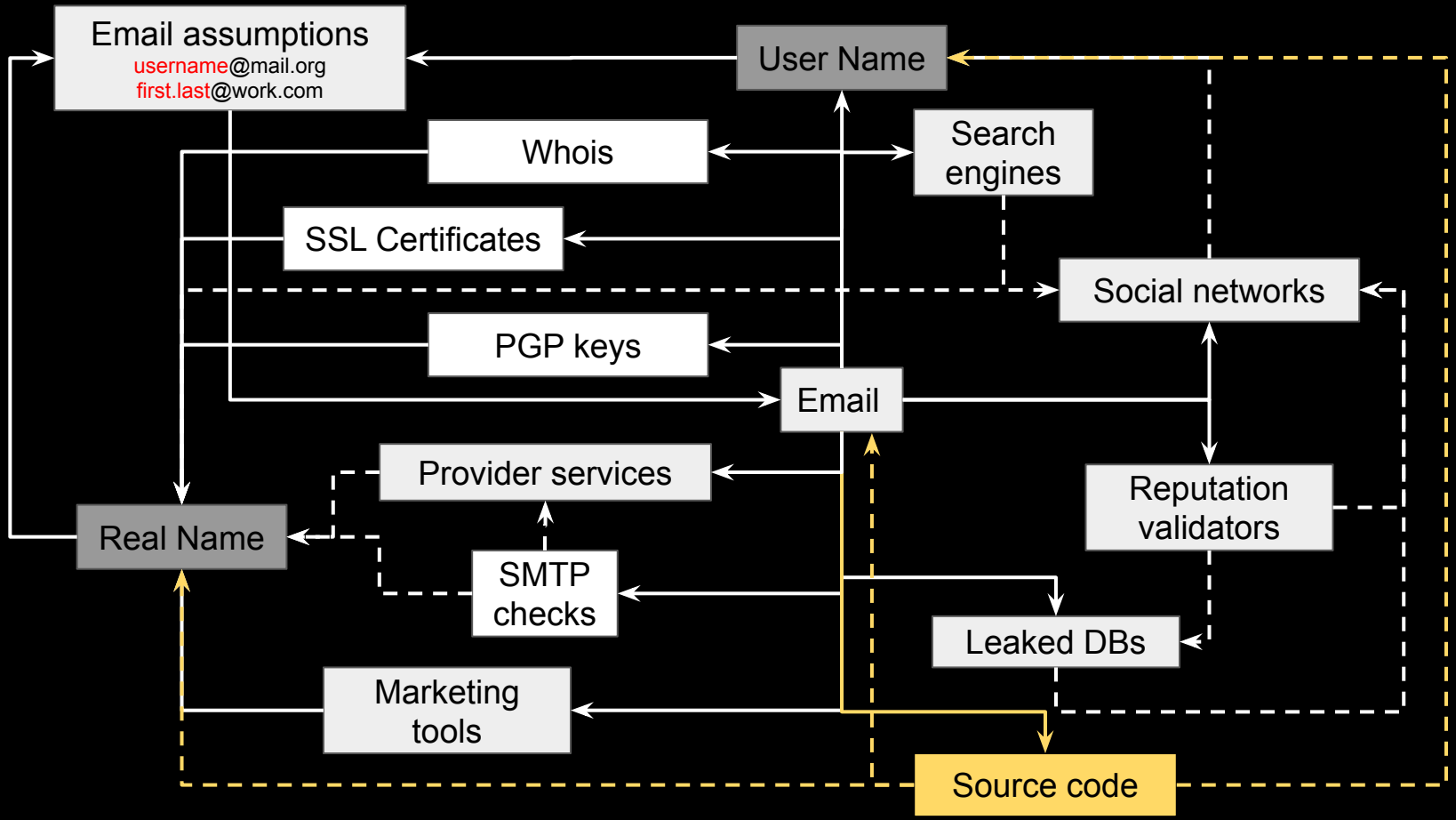
Common Name	Matching Identities
loyaltypartner.mediaport.laudert.de	support@laudert.de
www.3pagen.de	support@laudert.de
www.3pagen.at	support@laudert.de



Search results for 'torvalds org linux foundation'

```
Type bits/keyID     Date       User ID
pub  2048R/00411886 2014-07-21 *** KEY REVOKED *** [not verified]
                               Linus Torvalds <torvalds@linux-foundation.org>
pub  2048R/00411886 2011-09-20 Linus Torvalds <torvalds@kernel.org>
                               Linus Torvalds <torvalds@linux-foundation.org>
```

Workflow overview: source code



Source code

Look for emails where other emails come across

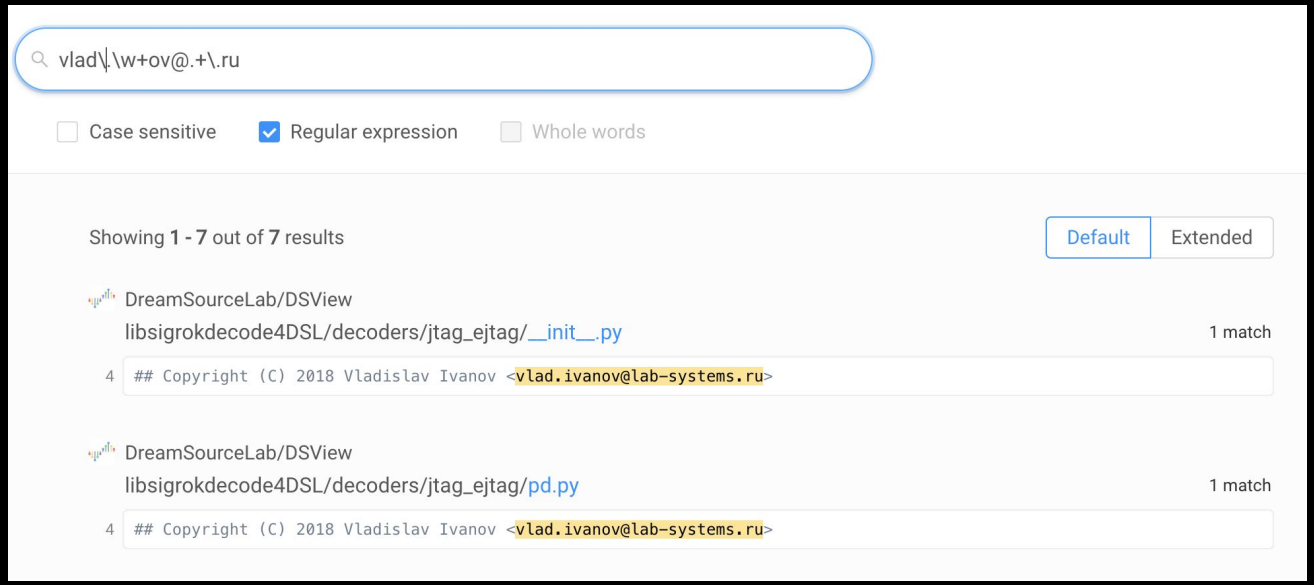
- People change emails and nicknames, but not a commit history
- People use work and personal email alternately
- People make mistakes

```
./gitcolombo.py -u https://github.com/facebook/folly

Matching info:
---------------
Aaryaman Sagar is the owner of emails:
                        aary@fb.com
                        aary@instagram.com

Tudor Bosman is the owner of emails:
                        tudor@rockset.com
                        tudor@rockset.io
                        tudorb@fb.com
```

https://telegra.ph/Gitcolombo---OSINT-v-GitHub-03-02
https://github.com/soxoj/gitcolombo

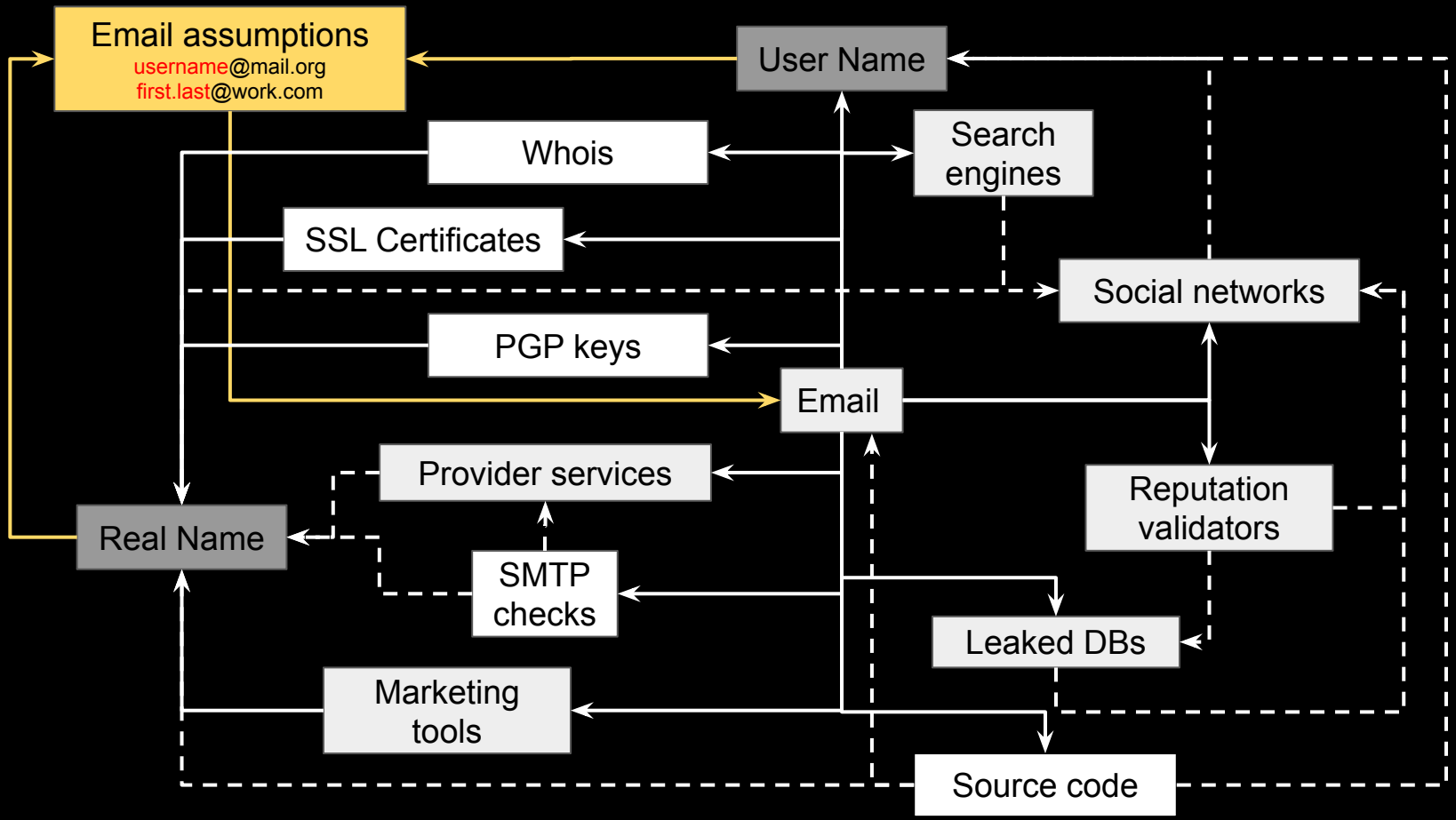
Source code

Don’t forget about special indexers like grep.app and archives, e.g. Google BigQuery GitHub Dataset



https://telegra.ph/Ishchem-po-email-v-GitHub-11-01

Workflow overview: email assumptions



Email assumptions

Suppose the target has several email addresses, work + personal at least

Email Permutator

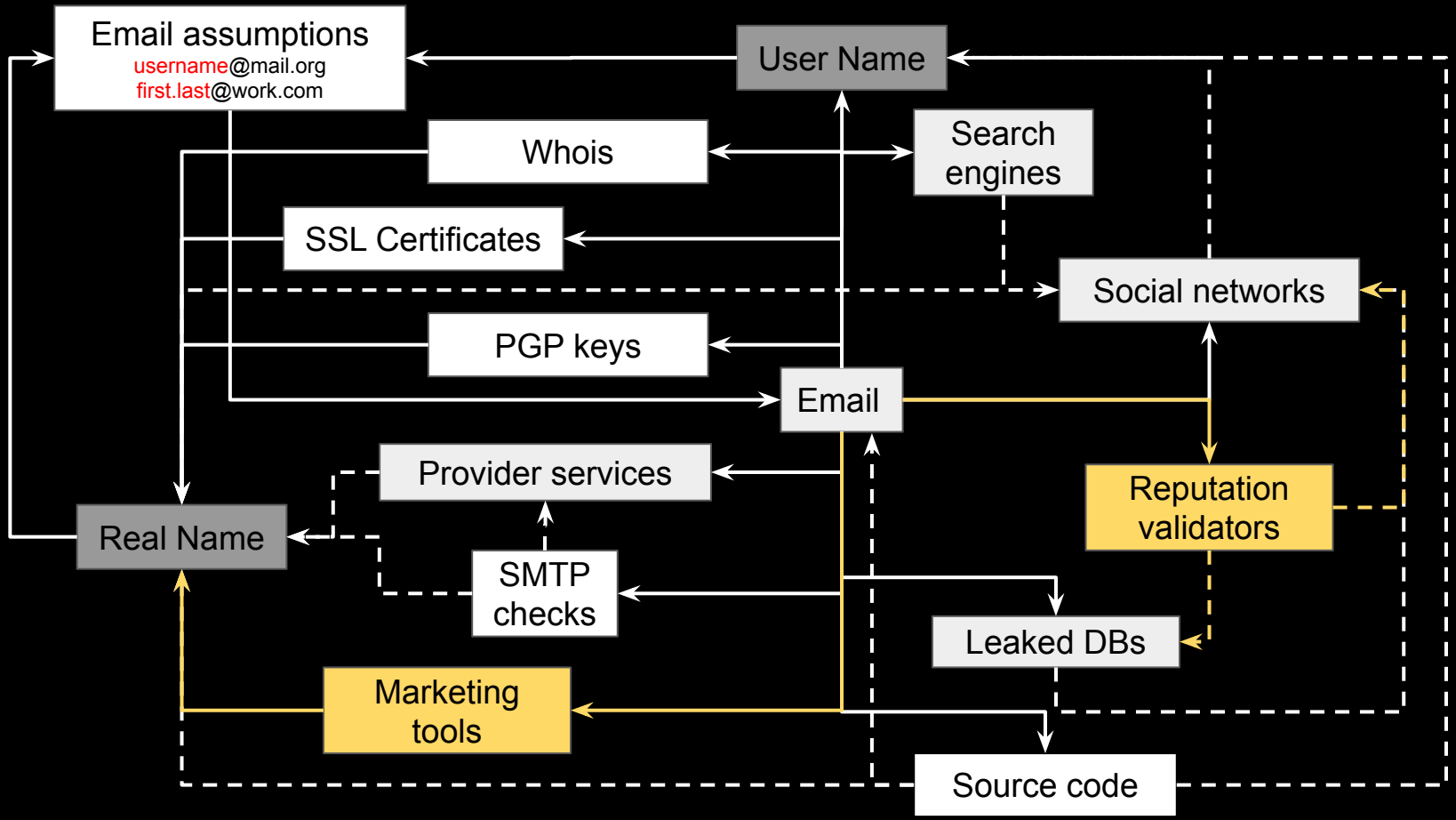
File Edit View Insert Format Data Tools Add-ons Help

100% View only

	A	B	D	E	F	G
1		**STEP 1: Fill in these details:**				**Step 2: Addresses appear down here:**
2		First Name: rob		Simple:	{fn}	rob@distilled.net
3		Middle Name:			{ln}	ousbey@distilled.net
4		Last Name: ousbey		Basics:	{fn}{ln}	robousbey@distilled.net
5		Domain: distilled.net			{fn}.{ln}	rob.ousbey@distilled.net
6					{fi}{ln}	rousbey@distilled.net
7					{fi}.{ln}	r.ousbey@distilled.net
8	NB: variables are:				{fn}{li}	robo@distilled.net
9	fn - firstname				{fn}.{li}	rob.o@distilled.net
10	fi - first initial				{fi}{li}	ro@distilled.net
11	mn - middle name				{fi}.{li}	r.o@distilled.net
12	mi - middle initial			Backwards:	{ln}{fn}	ousbeyrob@distilled.net
13	ln - lastname				{ln}.{fn}	ousbey.rob@distilled.net

https://t.me/cybred/299
https://github.com/c0rv4x/logins-generator

Workflow overview: email assumptions

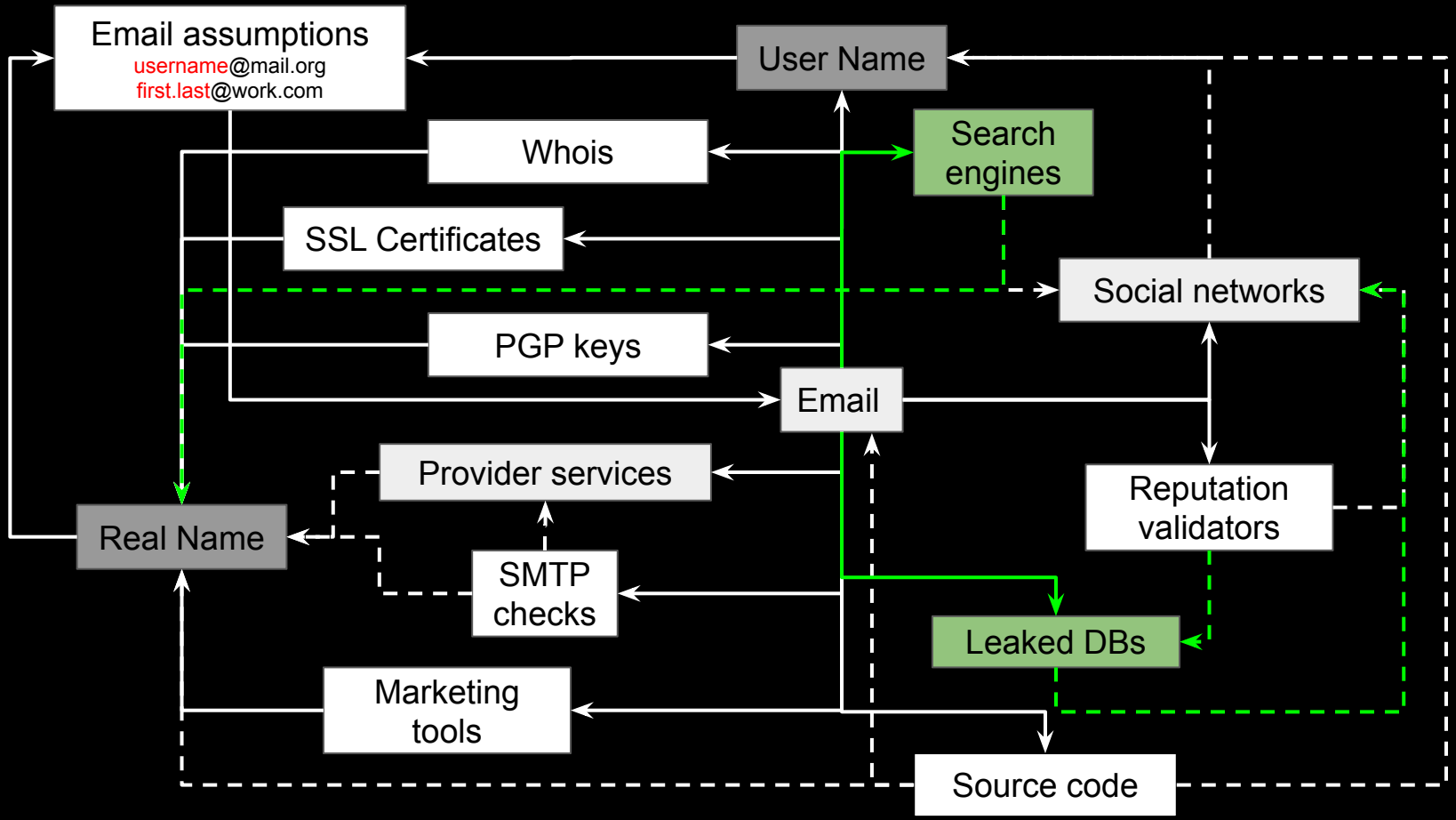


Marketing tools & reputation validators

Black-box validation services can be useful for fast and bulk checking

- HR, sourcing
- Sales
- Audience management
- Antifraud

Workflow overview: what we did't discuss



Conclusions

1. Methods are important, not specific tools
2. You should know internet landscape
3. Use info leaks from social services
4. Look for official email & name pairs
5. Look for emails where other emails come across
6. Don’t forget about special indexers and archives
7. Black-box validation services can be useful for fast and bulk checking

A large amount of tools:
https://github.com/HowToFind-bot/osint-tools/tree/master/Email

CHAOS CONSTRUCTIONS 2021

The End

https://t.me/soxoj
https://t.me/osint_mindset

THANKS. ANY QUESTIONS?