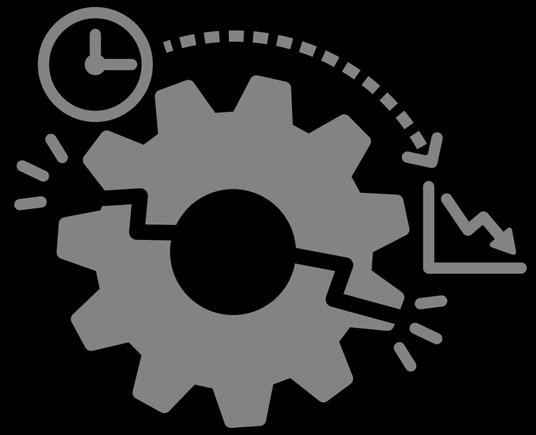
OSINT Techniques

Análise Forense de Sistemas Computacionais

Search

Search for open_source projects related to OSINT



Utilization

Installation usage and demonstrations of the previously mentioned tools

Analysis

Code and project analysis

Search

Find Various Tools

Mass repository collection

First Elimination

Tools that were deemed too complex or did not fit with the theme after a brief code examination.

Second Elimination

Tools that were installed but wouldn’t run due to deprication, paid APIs

Select Tools that are Correlated to Each Other.

Selection of the 3 best tools that correlate to each other

Projects Chosen

Sherlock

Cross-platform username searching tool

HOLEHE

Cross-platform Email searching tool

H8MAIL

Breach Hunting Tool

Fallen Projects

- Leaked
- PwnedOrNot
- Toutatis

Sherlock

- Cross-platform username searching tool
- Tracking digital footprint of a user
- Easy start/Low Effort

Demonstration

```
ricardo@Ricardo-Laptop:/mnt/c/Users/ricardo/Desktop/Uni/Forense/Proj/sherlock/sherlock$ python3 sherlock.py covelo13
[*] Checking username covelo13 on:

[+] Amino: https://aminoapps.com/u/covelo13
[+] Fiverr: https://www.fiverr.com/covelo13
[+] G2G: https://www.g2g.com/covelo13
[+] Lolchess: https://lolchess.gg/profile/na/covelo13
[+] Myspace: https://myspace.com/covelo13
[+] Twitch: https://www.twitch.tv/covelo13
[+] Twitter: https://twitter.com/covelo13
[+] Virgool: https://virgool.io/@covelo13
[+] Whonix Forum: https://forums.whonix.org/u/covelo13/summary
[+] metacritic: https://www.metacritic.com/user/covelo13

[*] Search completed with 10 results
```

Setbacks

- High error rate
- Doesn't account for minor changes
- Easily depricatable

Holele

- Cross-platform email searching tool
- Tracking digital footprint of a user
- Easy to use
- Checks 120 Services

Demonstration

$ Holehe telmobelasauce@gmail.com

```
*****************************
   telmobelasauce@gmail.com
*****************************
[x] about.me
[x] adobe.com
[+] amazon.com
[x] amocrm.com
[-] any.do
[-] archive.org
[-] armurerie-auxerre.com
[x] atlassian.com
[-] axonaut.com
[x] babeshows.co.uk
[x] badeggsonline.com
[x] bios-mods.com
[x] biotechnologyforums.com
[x] bitmoji.com
[x] blablacar.com
[x] blackworldforum.com
[x] blip.fm
[x] forum.blitzortung.org
[x] bluegrassrivals.com
[-] bodybuilding.com
[x] buymeacoffee.com
[x] discussion.cambridge-mt.com
[-] caringbridge.org
[x] chinaphonearena.com
[x] clashfarmer.com
[x] codecademy.com
[x] forum.codeigniter.com
[x] codepen.io
[-] coroflot.com
[x] cpaelites.com
[x] cpahero.com
[x] cracked.to
[x] crevado.com
[-] deliveroo.com
[x] demonforums.net
[-] devrant.com
[x] diigo.com
[-] discord.com
[-] docker.com
[-] dominos.fr
[-] ebay.com
[x] ello.co
[-] envato.com
[-] eventbrite.com
[-] evernote.com
[-] fanpop.com
[+] firefox.com
```

Demonstration

$ Holehe telmobelasauce@gmail.com –only-used

```
**************************************************
telmobelasauce@gmail.com
**************************************************
[+] firefox.com
[+] pinterest.com
[+] replit.com
[+] spotify.com
[+] twitter.com
```

Overview

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	✗
armurerieauxerre	armurerie-auxerre.com	register	✗
atlassian	atlassian.com	register	✗

Setbacks

- Rate Limit Applications low probability of finding accounts
- Necessary to find users email

H8mail

- Email OSINT and breach hunting tool
- Integrated with several OSINT breach and reconnaissance tools, like Hunter.io & Leak-Lookup.
- Identifier flexibility and loose matching pattern.
- URL resource and local file search capability.

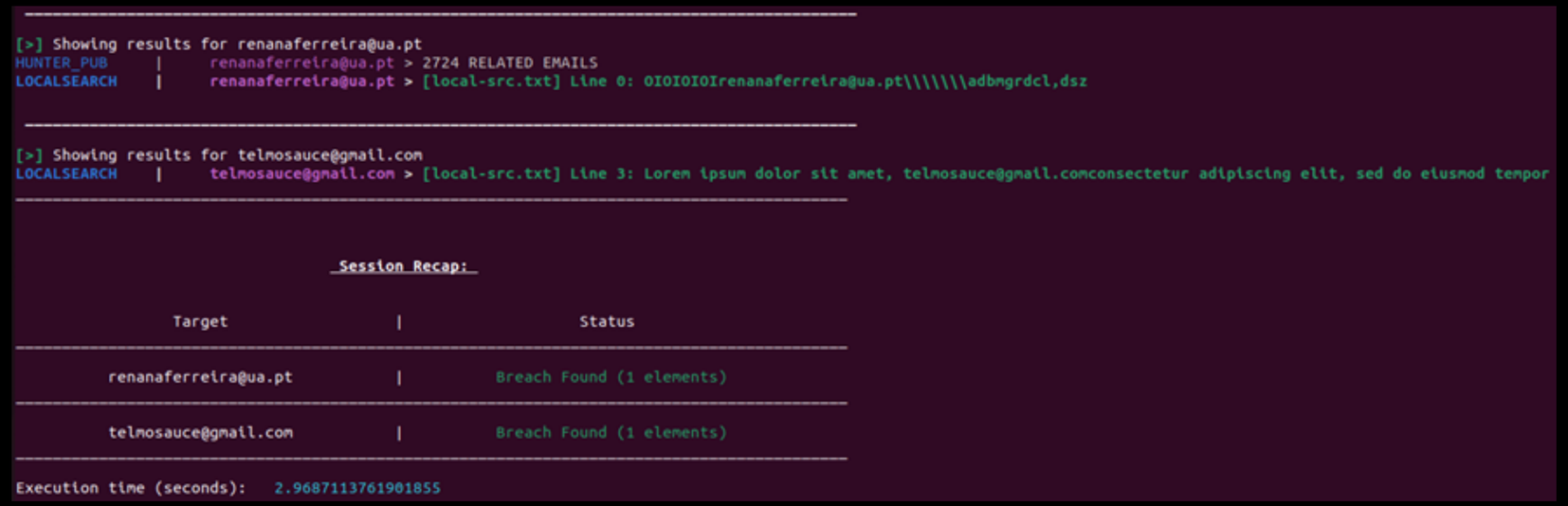
Demonstration

$ h8mail –t renanaferreira@hotmail.com –c h8mail_config.ini –o results1.csv

```
[>] h8mail is up to date
[~] Removing duplicates
[>] Targets:
[>] renanaferreira@hotmail.com
[>] scylla.so is up
[~] Target factory started for renanaferreira@hotmail.com
[~] [renanaferreira@hotmail.com]>[hunter.io public]
[>] Found 0 related emails for renanaferreira@hotmail.com using hunter.io (public)
[~] [renanaferreira@hotmail.com]>[leaklookup public]
[>] Found 4 entries for renanaferreira@hotmail.com using LeakLookup (public)
[~] [renanaferreira@hotmail.com]>[scylla.so]
[!] scylla.so error: renanaferreira@hotmail.com
Expecting value: line 2 column 1 (char 1)

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

[>] Showing results for renanaferreira@hotmail.com
LEAKLOOKUP_PUB |renanaferreira@hotmail.co > ccaa.com.br
LEAKLOOKUP_PUB |renanaferreira@hotmail.co > deezer.com
LEAKLOOKUP_PUB |renanaferreira@hotmail.co > descomplica.com.br
LEAKLOOKUP_PUB |renanaferreira@hotmail.co > mindjolt.com
------------------------------------------------------------------------------------------


                                  Session Recap:


                Target                  |                  Status
------------------------------------------------------------------------------------------
       renanaferreira@hotmail.com       |          Breach Found (4 elements)
------------------------------------------------------------------------------------------

Execution time (seconds):   4.291910886764526
```

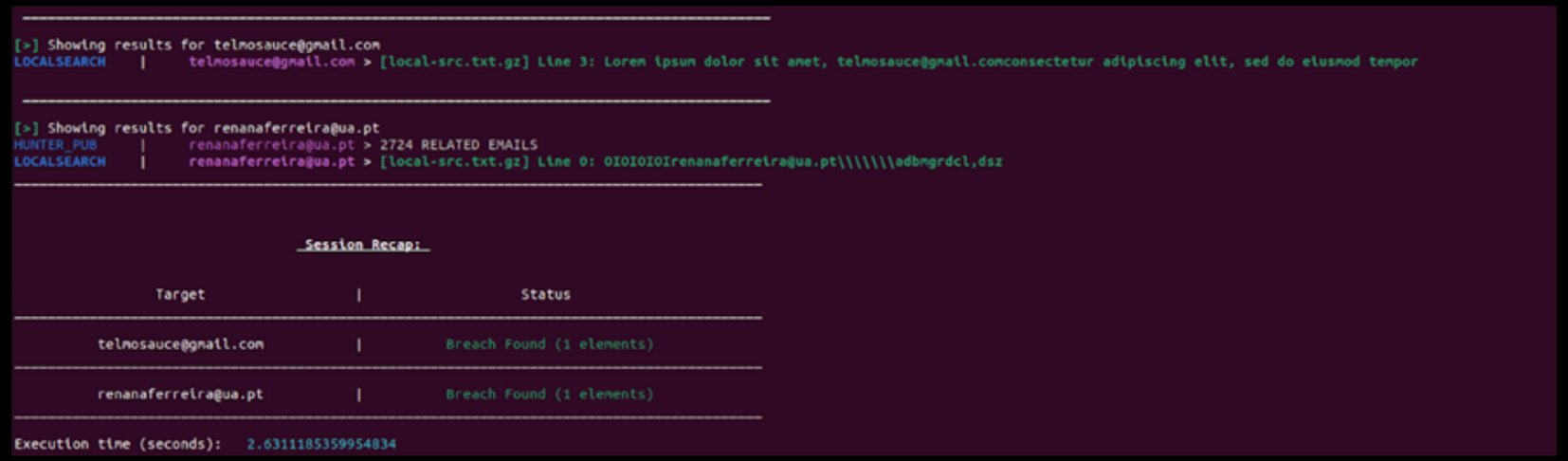
Demonstration

$ h8mail –t renanaferreira@ua.pt telmosauce@gmail.com –lb local–src.txt



Demonstration

$ h8mail –t renanaferreira@ua.pt telmosauce@gmail.com –gz local–src.txt.gz



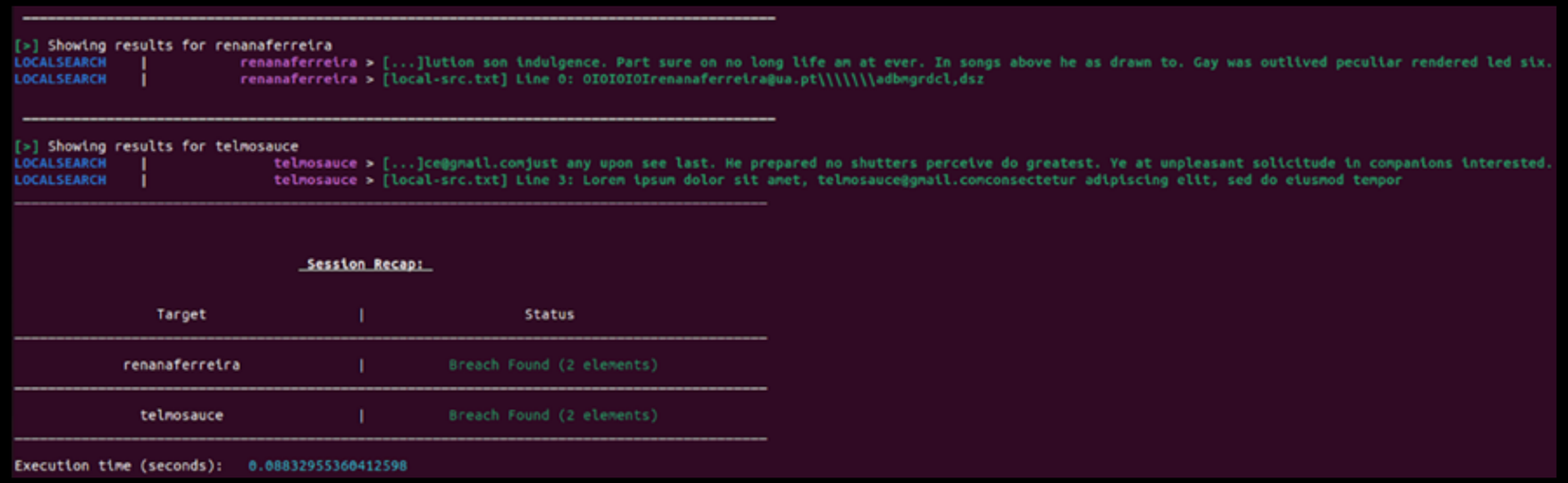
Demonstration

$ h8mail -t renanaferreira@ua.pt telmosauce@gmail.com -lb dir-local-search --debug

```
Traceback (most recent call last):
  File "/home/renan/anaconda3/bin/h8mail", line 8, in <module>
    sys.exit(main())
  File "/home/renan/anaconda3/lib/python3.9/site-packages/h8mail/utils/run.py", line 371, in main
    h8mail(user_args)
  File "/home/renan/anaconda3/lib/python3.9/site-packages/h8mail/utils/run.py", line 204, in h8mail
    breached_targets = local_to_targets(
  File "/home/renan/anaconda3/lib/python3.9/site-packages/h8mail/utils/localsearch.py", line 33, in local_to_targets
    c.debug_news(f"DEBUG: Found following content matching {t.target.target}")
AttributeError: 'str' object has no attribute 'target'
```

Demonstration

$ h8mail -t renanaferreira telmosauce -lb dir-local-search --skip-defaults --loose



Setbacks

- Major implementation errors, e.g. enabling debugging in local search.
- High error rate, including setting non-email token as an email.
- Not updated, e.g. legacy URLs to third-party OSINT tools.

Conclusion

- Efficient OSINT Tools.
- Although those tools have some limitations, improvements can turn them into highly effective and user-friendly OSINT searching and reconnaissance.

Conclusion

- Those tools can complement each other, with Sherlock and Holehe investigating a target social media presence and email address presence, respectively, and h8mail as a breach reconnaissance tool.
- For future work, those platforms must be able to analyse and filter its returned data, to decrease false positives and irrelevant information, taking this responsibility from their users.