# Semester Project – Milestone 2

# CSCI – 4321 -Computer Security

**Abigail Rodriguez Vazquez, Taja Hicks, Luis Morales**

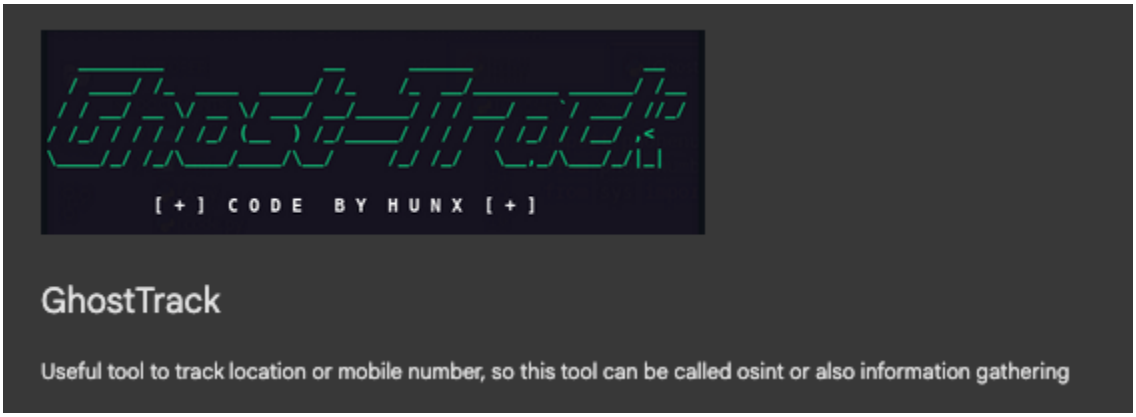
**October 25th, 2025**

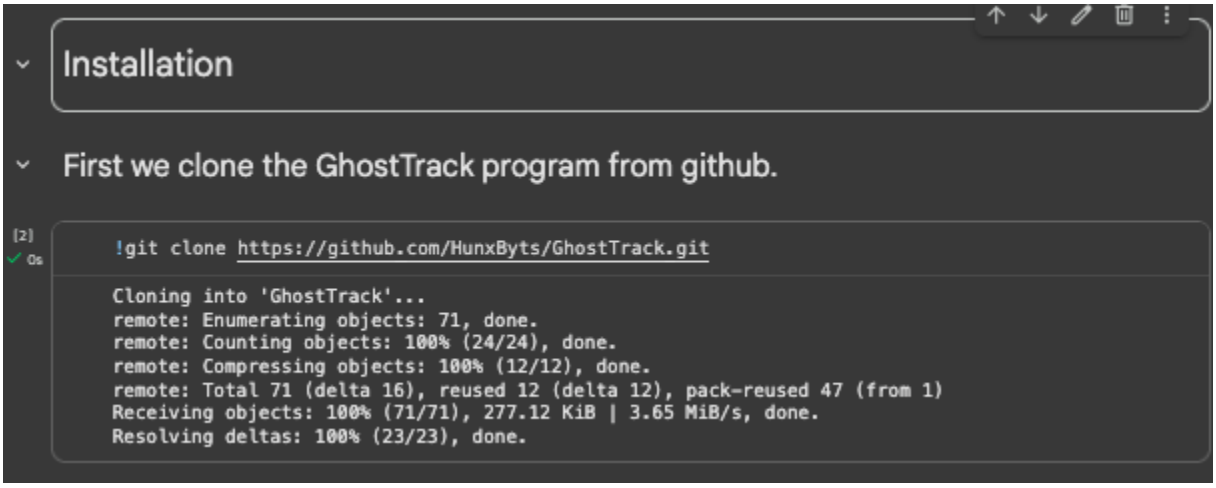
(1) Tools Comparison: (Must be completed in M2: 40%) Compare with at least two comparable tools and conduct a case study evaluation showing the following for the 3 tools:

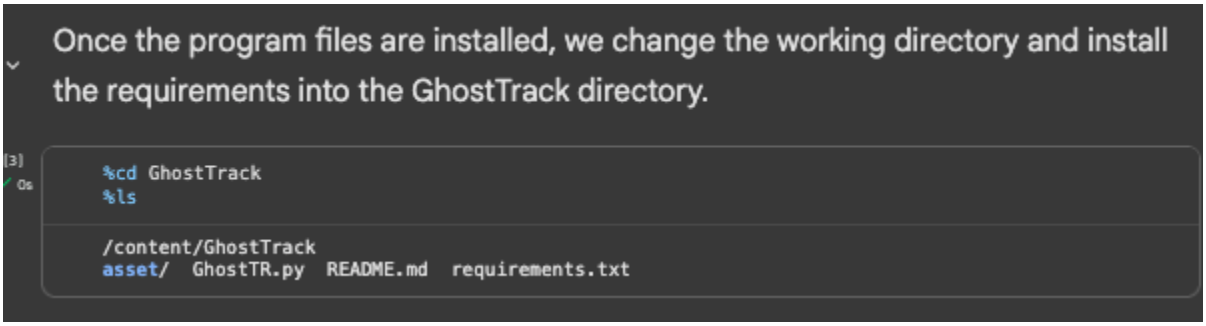
1.1 Sample demos of how each tool is used (practical part)

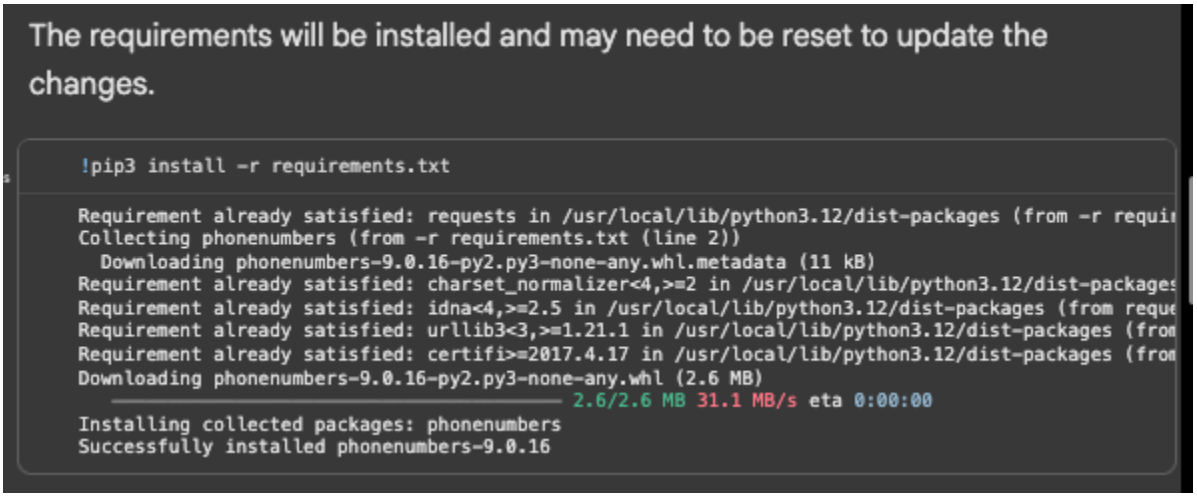
Sample Demo for Ghost Track

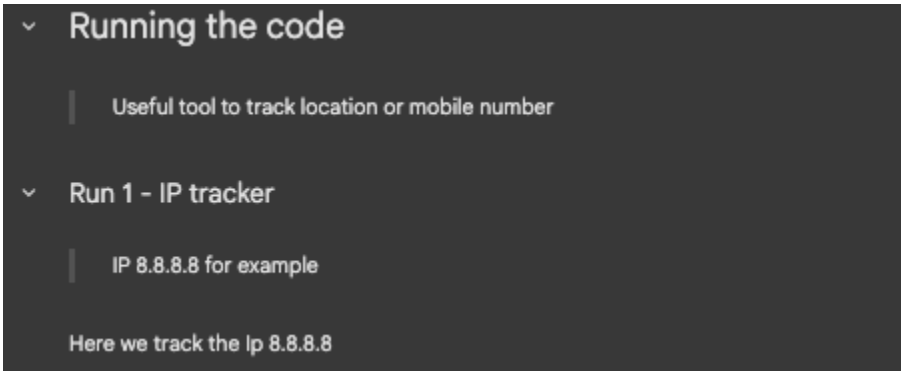
Link for Colab: [Ghost-Track Link]




The requirements will be installed and may need to be reset to update the changes.
!pip3 install -r requirements.txt
Requirement already satisfied: requests in /usr/local/lib/python3.12/dist-packages (from -r requi
Collecting phonenumbers (from -r requirements.txt (line 2))
Downloading phonenumbers-9.0.16-py2.py3-none-any.whl.metadata (11 kB)
Requirement already satisfied: charset_normalizer<4,>=2 in /usr/local/lib/python3.12/dist-packages
Requirement already satisfied: idna<4,>=2.5 in /usr/local/lib/python3.12/dist-packages (from reque
Requirement already satisfied: urllib3<3,>=1.21.1 in /usr/local/lib/python3.12/dist-packages (from
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.12/dist-packages (from
Downloading phonenumbers-9.0.16-py2.py3-none-any.whl (2.6 MB)
2.6/2.6 MB 31.1 MB/s eta 0:00:00
Installing collected packages: phonenumbers
Successfully installed phonenumbers-9.0.16


Running the code
Useful tool to track location or mobile number
Run 1 - IP tracker
IP 8.8.8.8 for example
Here we track the Ip 8.8.8.8


!python3 GhostTR.py
[ 2 ] Show Your IP
[ 3 ] Phone Number Tracker
[ 4 ] Username Tracker
[ 0 ] Exit
[ + ] Select Option : 1
H
GHOST - TRACKER - IP ADDRESS
@CODE BY HUNXBYTS
Enter IP target : 8.8.8.8
========== SHOW INFORMATION IP ADDRESS ==========
IP target : 8.8.8.8
Type IP : IPv4
Country : United States
Country Code : US
City : Mountain View
Continent : North America
Continent Code : NA
Region : California
Region Code : CA
Latitude : 37.3860517
Longitude : -122.0838511
Maps : https://www.google.com/maps/@37,-122,8z
EU : False
Postal : 94039
Calling Code : 1
Capital : Washington D.C.
Borders : CA,MX
Country Flag :
ASN : 15169
ORG : Google LLC
ISP : Google LLC
Domain : google.com
ID : America/Los_Angeles
ABBR : PDT
DST : True
Offset : -25200
UTC : -07:00
Current Time : 2025-10-21T11:56:39-07:00
[ + ] Press enter to continue

## Run 2 - Phone tracker

> Phones # +442083661177 for example

We use the example phone +442083661177 and it gives us information on it

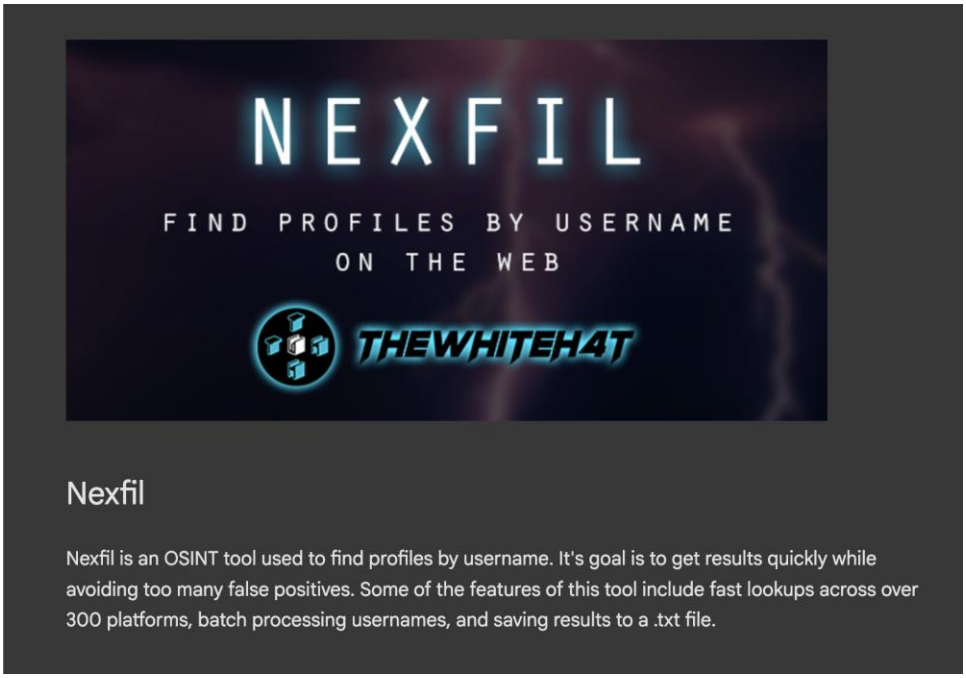
Run 3 - Username Tracker

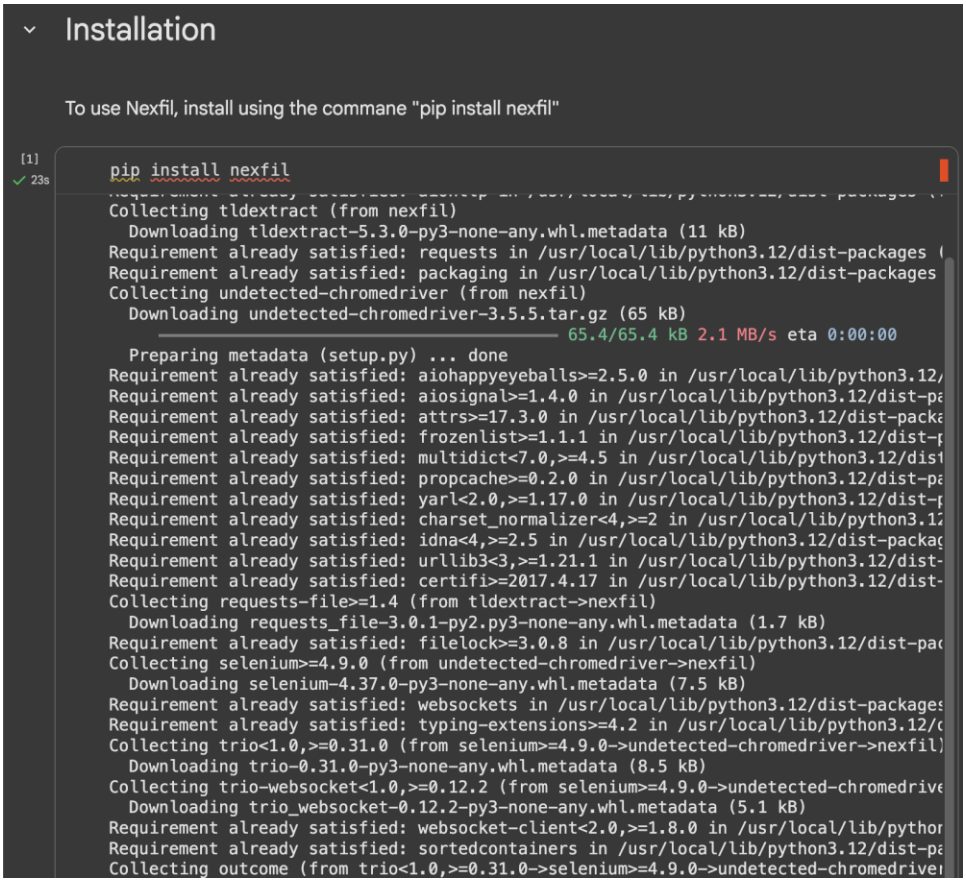
Using asep for example

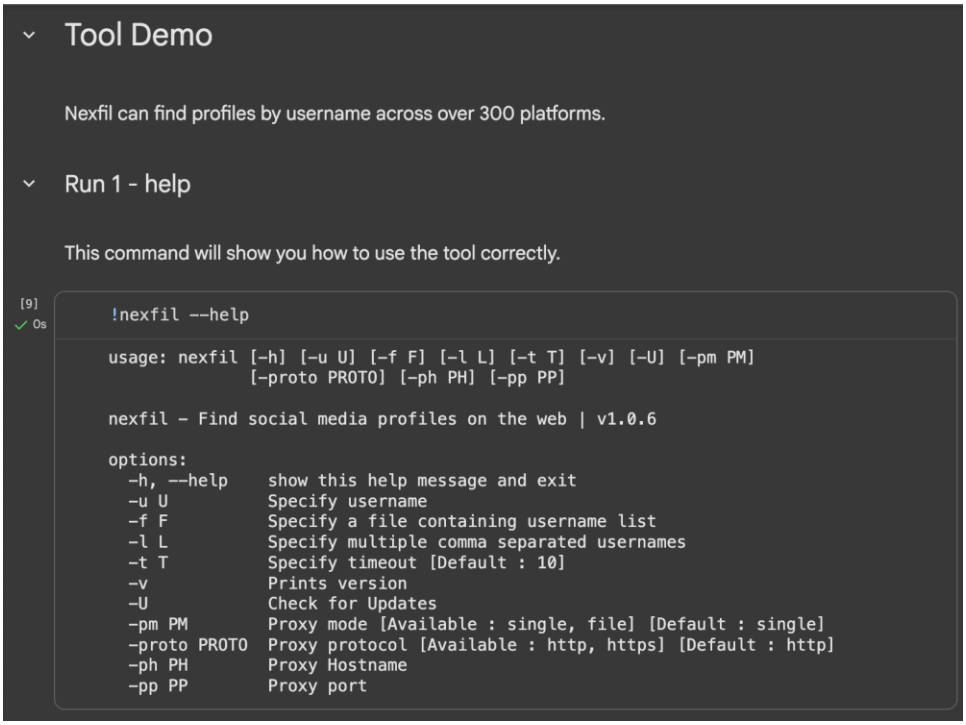
Here we use asep as an username and in return we get websites we are using with that username


Sample Demo for Nexfil

Link for Colab: Nexfil [7]

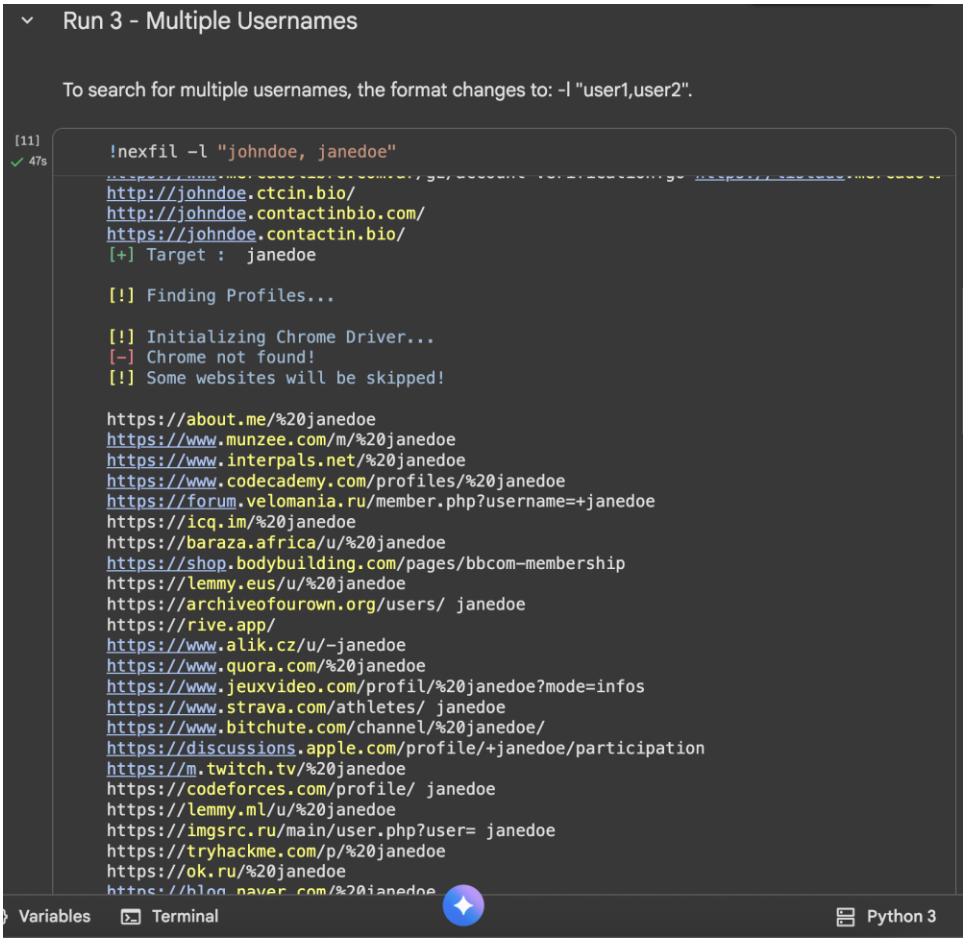

NEXFIL
FIND PROFILES BY USERNAME
ON THE WEB
THEWHITEH4T
Nexfil
Nexfil is an OSINT tool used to find profiles by username. It's goal is to get results quickly while avoiding too many false positives. Some of the features of this tool include fast lookups across over 300 platforms, batch processing usernames, and saving results to a .txt file.

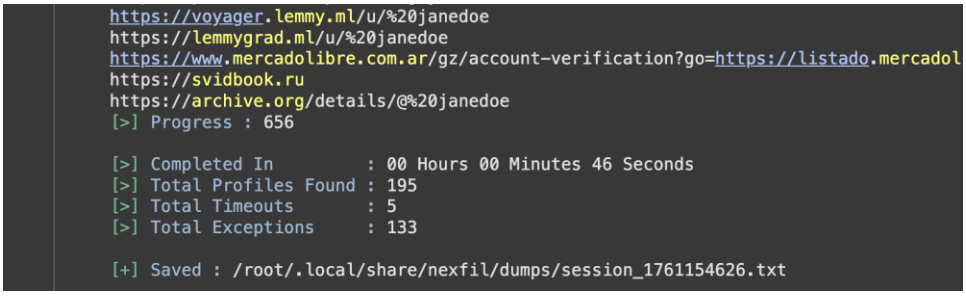

Installation
To use Nexfil, install using the commane "pip install nexfil"
[1]
23s
pip install nexfil
Collecting tldextract (from nexfil)
Downloading tldextract-5.3.0-py3-none-any.whl.metadata (11 kB)
Requirement already satisfied: requests in /usr/local/lib/python3.12/dist-packages
Requirement already satisfied: packaging in /usr/local/lib/python3.12/dist-packages
Collecting undetected-chromedriver (from nexfil)
Downloading undetected-chromedriver-3.5.5.tar.gz (65 kB)
65.4/65.4 kB 2.1 MB/s eta 0:00:00
Preparing metadata (setup.py) ... done
Requirement already satisfied: aiohappyeyeballs>=2.5.0 in /usr/local/lib/python3.12/
Requirement already satisfied: aiosignal>=1.4.0 in /usr/local/lib/python3.12/dist-pa
Requirement already satisfied: attrs>=17.3.0 in /usr/local/lib/python3.12/dist-packa
Requirement already satisfied: frozenlist>=1.1.1 in /usr/local/lib/python3.12/dist-p
Requirement already satisfied: multidict<7.0,>=4.5 in /usr/local/lib/python3.12/dist
Requirement already satisfied: propcache>=0.2.0 in /usr/local/lib/python3.12/dist-pa
Requirement already satisfied: yarl<2.0,>=1.17.0 in /usr/local/lib/python3.12/dist-p
Requirement already satisfied: charset_normalizer<4,>=2 in /usr/local/lib/python3.12
Requirement already satisfied: idna<4,>=2.5 in /usr/local/lib/python3.12/dist-packag
Requirement already satisfied: urllib3<3,>=1.21.1 in /usr/local/lib/python3.12/dist-
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.12/dist-
Collecting requests-file>=1.4 (from tldextract->nexfil)
Downloading requests_file-3.0.1-py2.py3-none-any.whl.metadata (1.7 kB)
Requirement already satisfied: filelock>=3.0.8 in /usr/local/lib/python3.12/dist-pac
Collecting selenium>=4.9.0 (from undetected-chromedriver->nexfil)
Downloading selenium-4.37.0-py3-none-any.whl.metadata (7.5 kB)
Requirement already satisfied: websockets in /usr/local/lib/python3.12/dist-packages
Requirement already satisfied: typing-extensions>=4.2 in /usr/local/lib/python3.12/d
Collecting trio<1.0,>=0.31.0 (from selenium>=4.9.0->undetected-chromedriver->nexfil)
Downloading trio-0.31.0-py3-none-any.whl.metadata (8.5 kB)
Collecting trio-websocket<1.0,>=0.12.2 (from selenium>=4.9.0->undetected-chromedrive
Downloading trio_websocket-0.12.2-py3-none-any.whl.metadata (5.1 kB)
Requirement already satisfied: websocket-client<2.0,>=1.8.0 in /usr/local/lib/python
Requirement already satisfied: sortedcontainers in /usr/local/lib/python3.12/dist-pa
Collecting outcome (from trio<1.0,>=0.31.0->selenium>=4.9.0->undetected-chromedriver

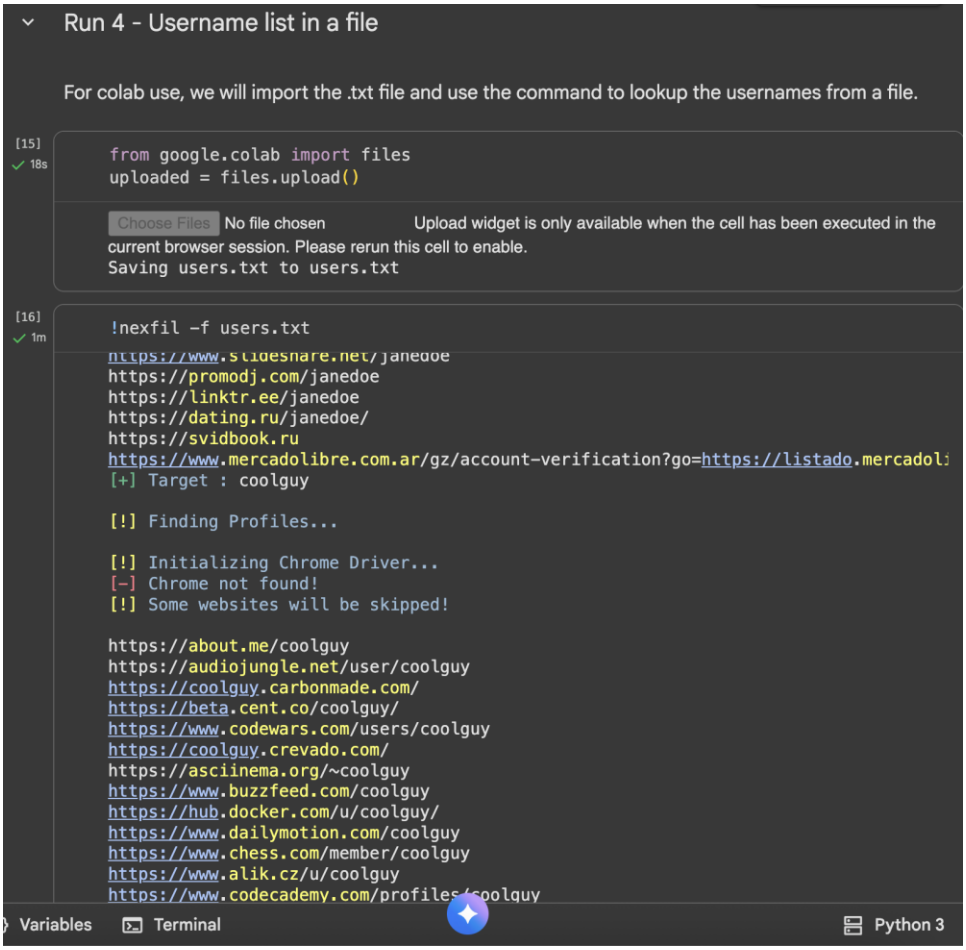

Tool Demo
Nexfil can find profiles by username across over 300 platforms.
Run 1 - help
This command will show you how to use the tool correctly.
[9]
0s
!nexfil --help
usage: nexfil [-h] [-u U] [-f F] [-l L] [-t T] [-v] [-U] [-pm PM]
[-proto PROTO] [-ph PH] [-pp PP]
nexfil - Find social media profiles on the web | v1.0.6
options:
-h, --help show this help message and exit
-u U Specify username
-f F Specify a file containing username list
-l L Specify multiple comma separated usernames
-t T Specify timeout [Default : 10]
-v Prints version
-U Check for Updates
-pm PM Proxy mode [Available : single, file] [Default : single]
-proto PROTO Proxy protocol [Available : http, https] [Default : http]
-ph PH Proxy Hostname
-pp PP Proxy port

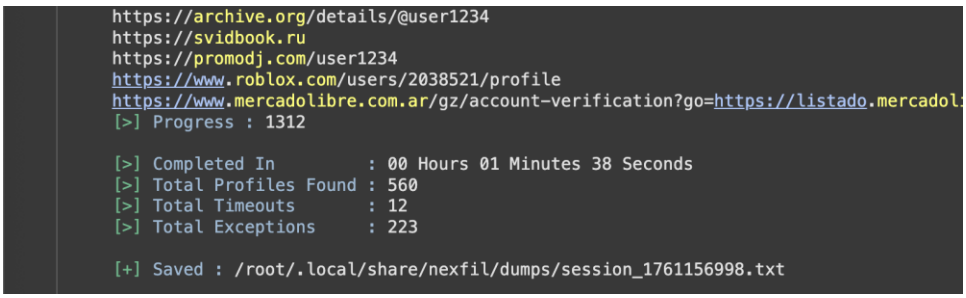

Run 2 - Single Username
[10]
27s
!nexfil -u johndoe
[+] Importing Modules...
[>] Created By : thewhiteh4t
|---> Twitter : https://twitter.com/thewhiteh4t
|---> Community : https://twc1rcle.com/
[>] Version : 1.0.6
[!] Loading URLs...
[+] 328 URLs Loaded!
[+] Timeout : 10 secs
[+] Target : johndoe
[!] Finding Profiles...
[!] Initializing Chrome Driver...
[-] Chrome not found!
[!] Some websites will be skipped!
https://about.me/johndoe
https://audiojungle.net/user/johndoe
https://www.buzzfeed.com/johndoe
https://archive.org/details/@johndoe
https://johndoe.carbonmade.com/
https://dev.to/johndoe
https://independent.academia.edu/johndoe
https://www.codewars.com/users/johndoe
https://beta.cent.co/johndoe/
https://asciinema.org/~johndoe
https://www.codecademy.com/profiles/johndoe
https://hub.docker.com/u/johndoe/
https://johndoe.crevado.com/
https://www.coroflot.com/johndoe
https://www.chess.com/member/johndoe
Variables
Terminal
Python 3


https://promodj.com/johndoe
https://johndoe.contactin.bio/
http://johndoe.contactinbio.com/
http://johndoe.ctcin.bio/
[>] Progress : 328
[>] Completed In : 00 Hours 00 Minutes 27 Seconds
[>] Total Profiles Found : 158
[>] Total Timeouts : 3
[>] Total Exceptions : 55
[+] Saved : /root/.local/share/nexfil/dumps/johndoe_1761154411.txt
As we can see, it gives a list of websites the username is found in and also gives an update at the end showind how long it took to complete, number of profiles found, total timeouts, and total exceptions. The results are also saved in a .txt file.


Run 3 - Multiple Usernames
To search for multiple usernames, the format changes to: -l "user1,user2".
[11]
47s
!nexfil -l "johndoe, janedoe"
http://johndoe.ctcin.bio/
http://johndoe.contactinbio.com/
https://johndoe.contactin.bio/
[+] Target : janedoe
[!] Finding Profiles...
[!] Initializing Chrome Driver...
[-] Chrome not found!
[!] Some websites will be skipped!
https://about.me/%20janedoe
https://www.munzee.com/m/%20janedoe
https://www.interpals.net/%20janedoe
https://www.codecademy.com/profiles/%20janedoe
https://forum.velomania.ru/member.php?username=+janedoe
https://icq.im/%20janedoe
https://baraza.africa/u/%20janedoe
https://shop.bodybuilding.com/pages/bbcom-membership
https://lemmy.eus/u/%20janedoe
https://archiveofourown.org/users/ janedoe
https://rive.app/
https://www.alik.cz/u/-janedoe
https://www.quora.com/%20janedoe
https://www.jeuxvideo.com/profil/%20janedoe?mode=infos
https://www.strava.com/athletes/ janedoe
https://www.bitchute.com/channel/%20janedoe/
https://discussions.apple.com/profile/+janedoe/participation
https://m.twitch.tv/%20janedoe
https://codeforces.com/profile/ janedoe
https://lemmy.ml/u/%20janedoe
https://imgsrc.ru/main/user.php?user= janedoe
https://tryhackme.com/p/%20janedoe
https://ok.ru/%20janedoe
Variables
Terminal
Python 3


https://voyager.lemmy.ml/u/%20janedoe
https://lemmygrad.ml/u/%20janedoe
https://www.mercadolibre.com.ar/gz/account-verification?go=https://listado.mercadol
https://svidbook.ru
https://archive.org/details/@%20janedoe
[>] Progress : 656
[>] Completed In : 00 Hours 00 Minutes 46 Seconds
[>] Total Profiles Found : 195
[>] Total Timeouts : 5
[>] Total Exceptions : 133
[+] Saved : /root/.local/share/nexfil/dumps/session_1761154626.txt




1.2 Strengths and weaknesses of each one of the three tools

Strengths for Blackbird

- Blackbird has a broader range of platforms, totaling 600.
- This provides a more in-depth look into the user, offering an analysis of the user's technical profile. As [1] mentions, this helps you understand more with less effort.
- It also includes polished PDF/CSV exports, making reading the information easy to read.

Weakness for Blackbird

- Although Blackbird has many advantages, it does not provide access to users' IP addresses or location. This information can be useful in some cases.
- It's also slower because of the number of results from queries

Strengths for Ghost-Track

- Ghost-track is very useful when it comes to tracking location or mobile numbers.
- Helping you gather information about a user, whether it be what country they live in or their capital.
- Ghost-track also tracks the username and checks what websites the user is on
- Also useful in physical threat scenarios

Weakness for Ghost-Track

- While Ghost-track also tracks username, there is a smaller range of platforms compared to the likes of Blackbird
- The information is good, but also very minimal.

Strengths for Nexfil

- Fast lookups that can be completed under 20 seconds
- Allows files containing usernames to be searched

Weakness for Nexfil

- Smaller range of platforms (over 300) when compared to Blackbird
- Limited to saving results to txt file only
- Limited features

## Literature Review

Open-Source Intelligence (OSINT) tools have become indispensable in cybersecurity, digital forensics, and ethical hacking. They automate the collection of publicly available data, enabling investigators to uncover digital footprints across social media, geolocation services, and online platforms. This review analyses the OSINT tool available on GitHub — Blackbird (Our Program), and places it in the context of broader academic and technical fields. We then compare their usage of Blackbird and other OSINT tools to our usage.

This paper [2] was written to undertake a study on how CITNT conducts activities to encourage citizens to participate in contributing to intelligence activities and decision-making processes. As it seems, the goal of this is more of a discussion on how we can integrate CITNT into our daily lives and government. In addition to exploring the benefits that would come from doing so. Another thing to note is that this research is primarily taking place in Finland, which means it is targeting a specific demographic. They do mention that some of the tools they utilize are Ukrainian Delta and Blackbird. From the article, it can be inferred that these tools are used to better understand and involve civilians in intelligence efforts, ultimately aiming to create a more informed and engaged public.

In our team's case, we had a completely different goal when it came to utilizing these tools. Our goals are to discuss possible computer security vulnerabilities, to uncover digital footprints, and to encourage safer online presence. We're attempting to answer queries about how we can better secure ourselves if we utilize various platforms with the same usernames. Some answers we found are integrating more secure login techniques, such as two-factor authentication. Our demographic is also broader than [2] since we are not really considering only one place.

Another paper we came across that used Blackbird was [3]. GoodFatR is a tool introduced in this article to collect threat reports and extract their Indicators of Compromise (IOCs). It appears that they deployed Blackbird to do an alternate validation, giving them user credentials tied to threats discovered by their tool. This takes a different approach because they created their own tool and just used Blackbird as supplementary support. The key tool for this research is Blackbird, which is used to identify potential computer security flaws. GoodFatR appears to be an effective tool to find indicators of compromise. We can investigate if it's possible to integrate certain features of this tool into our project and provide an IoC report on potential username input.

OSINT tools have many uses, and one of the uses we'll explore is its use in detecting and preventing organized crime. [4] is a paper that goes over organized crime and how those involved in it use information technology systems in their work. CAPER has six analysis modules, but the one this paper focuses on is the CAPER Facebook analysis submodule. This

paper also focuses on the interactions between users through posts and comments [4]. CAPER integrates many things such as text, images, or video to detect connections or patterns related to crime. It's on a much larger scale when compared to Blackbird. CAPER is used in this paper to analyze names, locations, organizations, and the relationships between them to create a user-friendly network graph [4].

Facebook is a social media platform used by many to post photos, videos, and information about things like daily life. There is a lot of information to be found on Facebook because of this including personal information such as name, relatives, friends, general location, and more. The CAPER Facebook module performs tasks including gathering information from Facebook pages, groups, events, and users [4]. Specific information can include the date the post was created, likes and comments on the post as well as mentions [4]. All of this data can be gathered and used for various purposes and in the case of the paper, used to detect and prevent organized crime. Blackbird is smaller scaled and performs fast checks for usernames with cyber security analysts being the main audience. The main audience for CAPER would include professional intelligence analysts and the police. We used blackbird and we are limited to a smaller number of features compared to CAPER.

Another paper we will explore is [8] and its use of the OSINT tool, Maltego. Maltego is an OSINT tool, like Blackbird but with a broader scope. Unlike Blackbird, Maltego uses interactive graphs for visualization, offers free and paid tiers for more results, features and more, and is popular in penetration testing. In [8], Maltego is used to conduct security testing and focuses on examining the website of X Company to collect information to be used to help test its security. The information on vulnerabilities found is used to give recommendations to X company so that its website can be more secure [8]. In the case of [8], Maltego was used to collect and analyze information for intelligence purposes compared to Blackbird which has features limited to username and email lookup across different sources. Because of the difference in features, Blackbird is limited to certain usage unlike Maltego.

InfoHound is an OSINT tool that reminded us that, every time something is published on the internet it gets indexed by many services [5]. InfoHound retrieves all publicly available information given a domain name. It will then help visualize which degree of exposure a web domain has on the internet. With the proliferation of users spread across public platforms, the need for tools that can efficiently collect, correlate, and analyze publicly available data has grown significantly. To this point, Blackbird, builds on the principles established by previous Open Source Intelligence (OSINT) applications. Offering both a modular and passive-first OSINT framework focused on identity resolution, account discovery, and analyst usability. Blackbird bridges gaps left by other tools by emphasizing identity enrichment and cross-platform account discovery. Instead of just listing emails or usernames, it tries to correlate them with actual profiles, services, and leaked credentials. This tactic shows a shift from simple enumeration towards actionable intelligence. By querying hundreds of platforms for the

presence of a given username, Blackbird can map digital identities across services. This feature allows for enhanced profiling, fraud detection, and adversary attributes(attacker's motivations, capabilities, and methods).

While Blackbird and similar tools have made a lot of progress, there is room for improvements. In the case of Blackbird relying on username matching alone, the potential for false positives is present. Connecting Blackbird to a visualization platform could potentially enhance its investigative uses [5]. Having a modular framework allows such enhancements and expansions on its utility. While also making it a strong candidate for further research and development in OSINT tooling. "The rapid development of CITINT processes and organizations places specific demands on legislative work and the definitions contained in international agreements" [9]. As non-state actors increasingly engage in intelligence gathering—often using sophisticated tools and platforms—the boundaries between civilian and combatant roles become blurred, challenging traditional legal frameworks.

(3) Contribution: (Must be started in M2: 20%) Make your own intuitive contribution to the original tool or code, this can take different forms:

Paper Topic: Privacy, Ethics & Human-Computer Interaction

Paper Outline Rough Draft:

- Abstract:
    - This paper presents the goal of presenting readers with a look into the dangers of utilizing the same usernames across multiple platforms as well as the possible threats OSINT can pose. Our team accomplishes this by conducting research on connected usernames/profiles and measuring how much information is gathered. This was all made possible with the OSINT tool Blackbird, as well as some other OSINT strategies.

- Introduction
    - Blackbird (about the tool)
        - OSINT tool developed by p1ngul1n0 that specializes in account enumeration.
        - Scans over 600 websites to identify specified usernames or email addresses helping investigators, ethical hackers, and researchers map digital footprints with minimal effort
        - Uses passive-first non-intrusive data collection to avoid alerting targets
        - Offers AI profiling based on the sites the targets are found
        - Modular framework makes it easier to extend searches to new platforms or create custom modules.
- Privacy Leakage
        - Privacy leakage occurs when information meant to remain confidential becomes accessible to unauthorized parties.
        - Blackbird works on publicly available data. while public in nature this information could be combined to expose behavioral patterns or private affiliations
        - As OSINT grows and becomes more automated, the risk of unintentional privacy violations grows.
- User Awareness & Ethical OSINT
- Conclusion
- References
- Possible example of how experiments may look like

    - Fraud prevention: In this hypothetical scenario, a ‘popular influencer’ attempts to scam their followers. The influencer uses Blackbird and the OSINT framework to gather information such as usernames and emails, analyze user behavior, and persuade followers to make purchases or click on suspicious links.
    - We will collect data and see how many scams are possible while utilizing the tools mentioned above.

SOURCES

[1] P. Carlesi, "Blackbird," GitHub. [Online]. Available: https://github.com/p1ngul1n0/blackbird.

[2] A. Franchino, S. V. W. Virdone, and F. De Marco, "Integrating Political Science and Artificial Intelligence: The Future of Political Analysis," *Frontiers in Political Science*, vol. 6, no. 1379789, 2024. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fpos.2024.1379789/full.

[3] J. Caballero, G. Gomez, S. Matic, G. Sánchez, and S. Sebastián, "GoodFATR: A Platform for Automated Threat Report Collection and IOC Extraction," *2022*. [Online]. Available: https://carlesi.vg/wp-content/uploads/2022/11/goodfatr.pdf.

[4] C. Aliprandi *et al.*, "CAPER: Crawling and analysing Facebook for intelligence purposes," *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*, Beijing, China, 2014, pp. 665–669, doi: 10.1109/ASONAM.2014.6921656.

[5] Xavier Marrugat Plaza, “InfoHound Tool – Improving OSINT open source CyberArsental for good,” 2023.[Online]. Available: https://openaccess.uoc.edu/items/9f1c6491-f7c2-4cda-b8a2-9ea7161ab83f

[6] p1ngul1n0, "Blackbird: An OSINT tool to search for accounts by username and email in social networks," GitHub repository, GitHub, Inc. [Online]. Available: https://github.com/p1ngul1n0/blackbird

[7] thewhiteh4t, “Nexfil: OSINT tool for finding profiles by username,” GitHub repository, GitHub, Inc. [Online]. Available: https://github.com/thewhiteh4t/nexfil

[8] I. P. A. E. Pratama and A. A. B. A. Wiradarma, “Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company),” *Int. J. Comput. Netw. Inf. Secur.* (IJCNIS), vol. 11, no. 7, pp. 8–12, Jul. 2019, doi: 10.5815/ijcnis.2019.07.02.

[9] Iikka Pietilä, Katleena Kortesuo, Ulla Pohjanen, Mikko Tuominen, “Kansalaisten tekemä CITINT ja sen vertautuminen valtiolliseen tiedusteluun,” [Online]. Available: https://www.researchgate.net/profile/Katleena_Kortesuo2/publication/383941320_Kansalaisten_tekema_CITINT_ja_sen_vertautuminen_valtiolliseen_tiedusteluun/links/66e15aca2390e50b2c7e9849/Kansalaisten-tekemae-CITINT-ja-sen-vertautuminen-valtiolliseen-tiedusteluun.pdf#page=51