Lab - Conducting OSINT Using CSI Linux Investigator

Overview

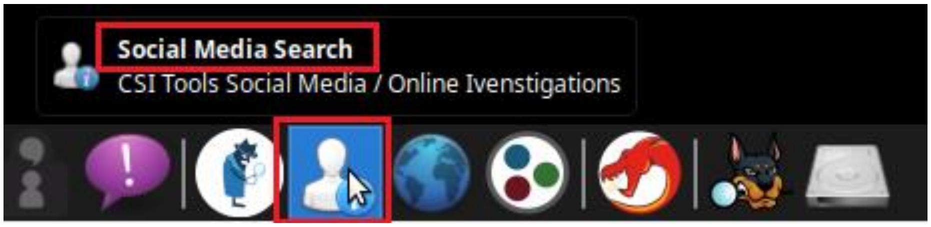
In this lab, we will see how we go about creating a case number and conducting an Open-source intelligence (OSINT) investigation. Open-source intelligence (OSINT) is data collected from publicly available sources used in an intelligence-gathering context. In the intelligence community, the term “open” refers to overt, publicly available sources (as opposed to covert or clandestine sources).

In this lab, we will be using the CSI Social Media Search Tool and Little Brother to perform a passive information scan about a person or company using information quickly pulled from a variety of Internet sources.

Begin the Lab!

Begin by logging on to your virtual install of CSI Linux Analyst. Ensure you have an Internet connection. Since this is a passive scan, we do not need to use the CSI Linux Gateway.

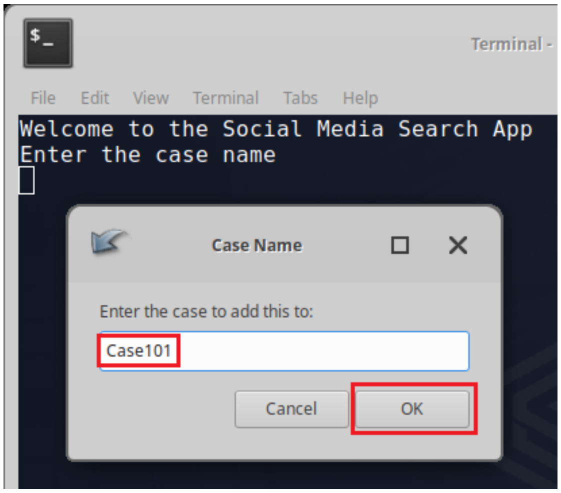
Once the desktop has loaded, from the bottom taskbar, left-click once to launch the Social Media search tool.



This tool is linked to the case folder located on your desktop, where all your cases or built and stored for easy organization and access.

Once the search Media tool is launched, you are prompted to create a case number. If you look inside the case folder shortcut located on your CSI Linux desktop, you will note the folder has only two subfolders. In some cases, the folder will be empty.

In the Case Name screen, type in a case name or number. For this exercise, I have named the case, Case101. Make sure there are no blank spaces in the title. Click OK.

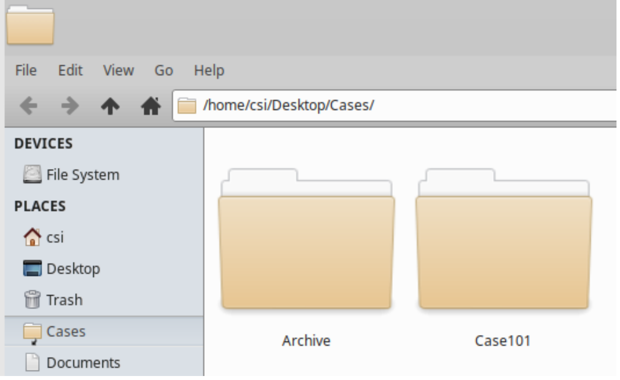


```
Welcome to the Social Media Search App
Enter the case name
```

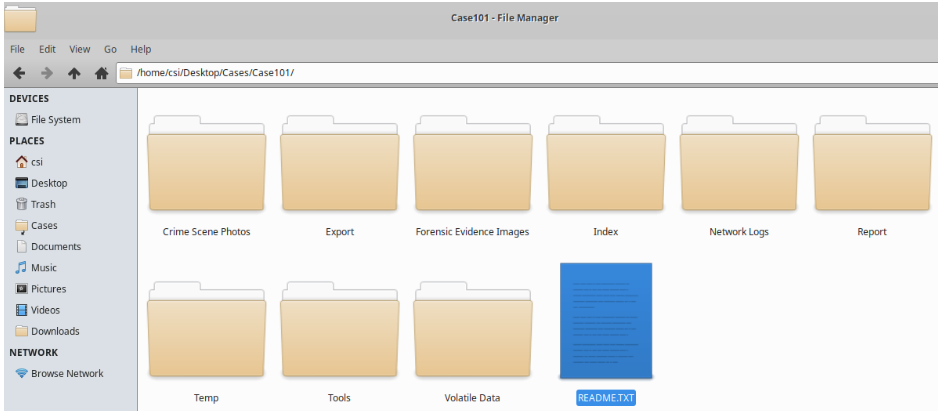
Enter the case to add this to:

Case101

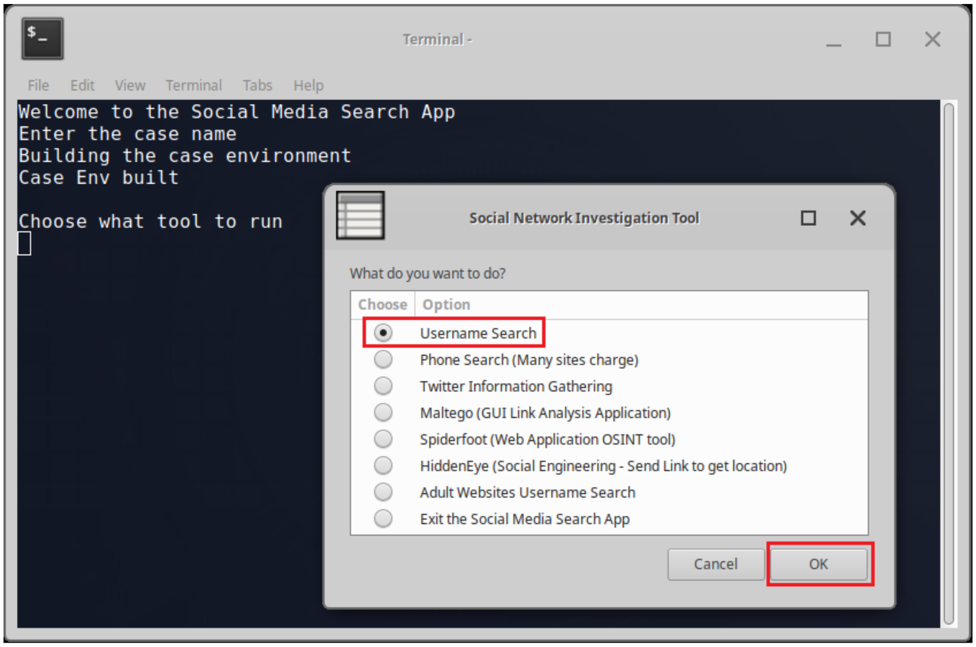
Now, if you open the Cases folder located on your desktop, you will see a new case folder has been built.



If you open the Case101 subfolder, you will see several additional subfolders all designed to help organize and manage your investigation. Feel free to reorganize and rename the folders as you see fit.



From our terminal, we have several search criteria to search with. In this example, we will accept the default to search for a username. Click OK to accept the default. You are free to search for any username you wish to use. In this example, I will conduct a media search using my username.

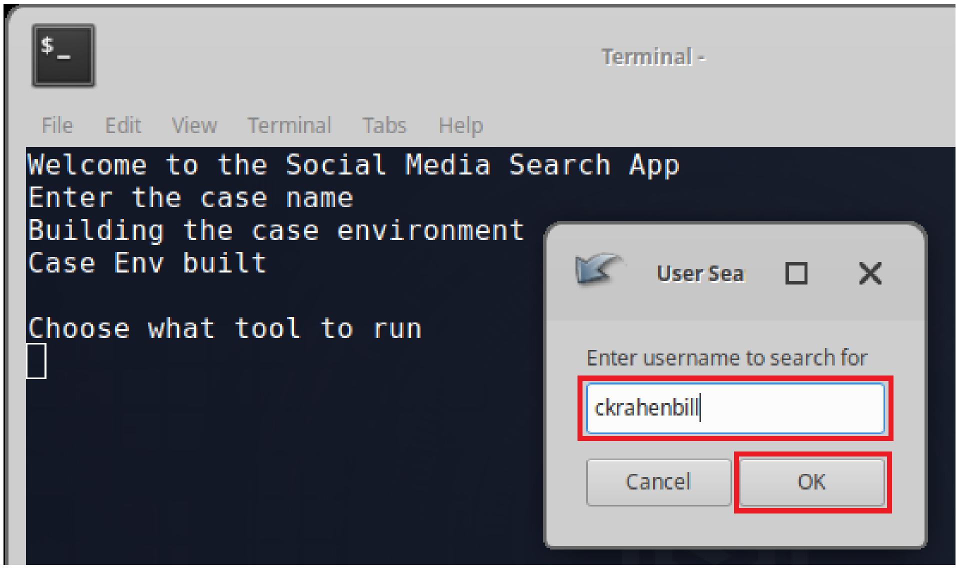

Terminal -
File Edit View Terminal Tabs Help
Social Network Investigation Tool
Cancel
OK

```
Welcome to the Social Media Search App
Enter the case name
Building the case environment
Case Env built

Choose what tool to run
```

What do you want to do?

Choose	Option
●	Username Search
○	Phone Search (Many sites charge)
○	Twitter Information Gathering
○	Maltego (GUI Link Analysis Application)
○	Spiderfoot (Web Application OSINT tool)
○	HiddenEye (Social Engineering - Send Link to get location)
○	Adult Websites Username Search
○	Exit the Social Media Search App

On the next screen, type in the username you wish to search for. Click OK.

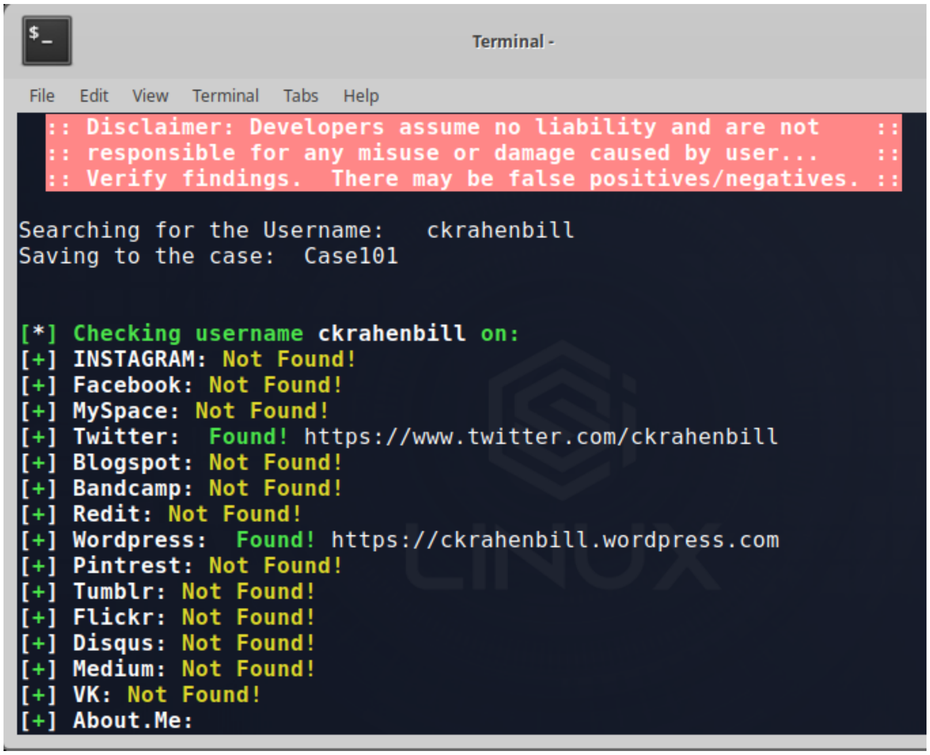


```
Welcome to the Social Media Search App
Enter the case name
Building the case environment
Case Env built

Choose what tool to run
```

Enter username to search for

ckrahenbill

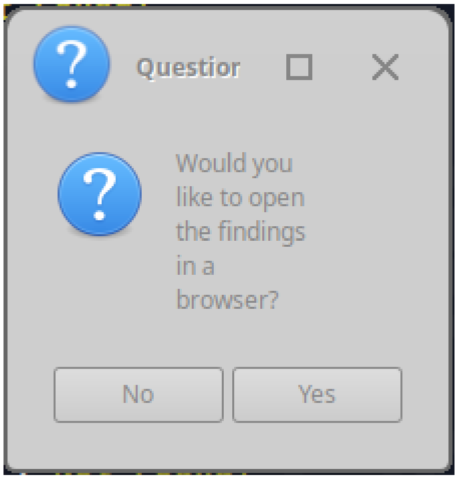
The search begins! Your results will vary. As you can see, I live a very social media-free life.



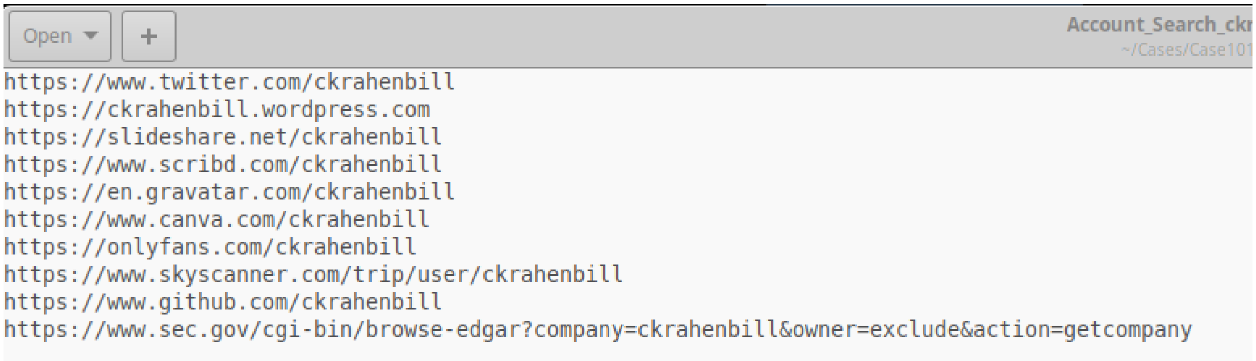
```
:: Disclaimer: Developers assume no liability and are not   ::
:: responsible for any misuse or damage caused by user...   ::
:: Verify findings.  There may be false positives/negatives. ::

Searching for the Username:   ckrahenbill
Saving to the case:  Case101

[*] Checking username ckrahenbill on:
[+] INSTAGRAM: Not Found!
[+] Facebook: Not Found!
[+] MySpace: Not Found!
[+] Twitter:  Found! https://www.twitter.com/ckrahenbill
[+] Blogspot: Not Found!
[+] Bandcamp: Not Found!
[+] Redit: Not Found!
[+] Wordpress:  Found! https://ckrahenbill.wordpress.com
[+] Pintrest: Not Found!
[+] Tumblr: Not Found!
[+] Flickr: Not Found!
[+] Disqus: Not Found!
[+] Medium: Not Found!
[+] VK: Not Found!
[+] About.Me:
```

Once the search completes, a browser will open, loading a large number of tabs. These search results are what you can use to verify or not the information as being accurate.

You Can have all the positive hits loaded into a browser, after which you can save the results as a text file to a subfolder inside your Case101folder. Over to the right of the taskbar is the save button.

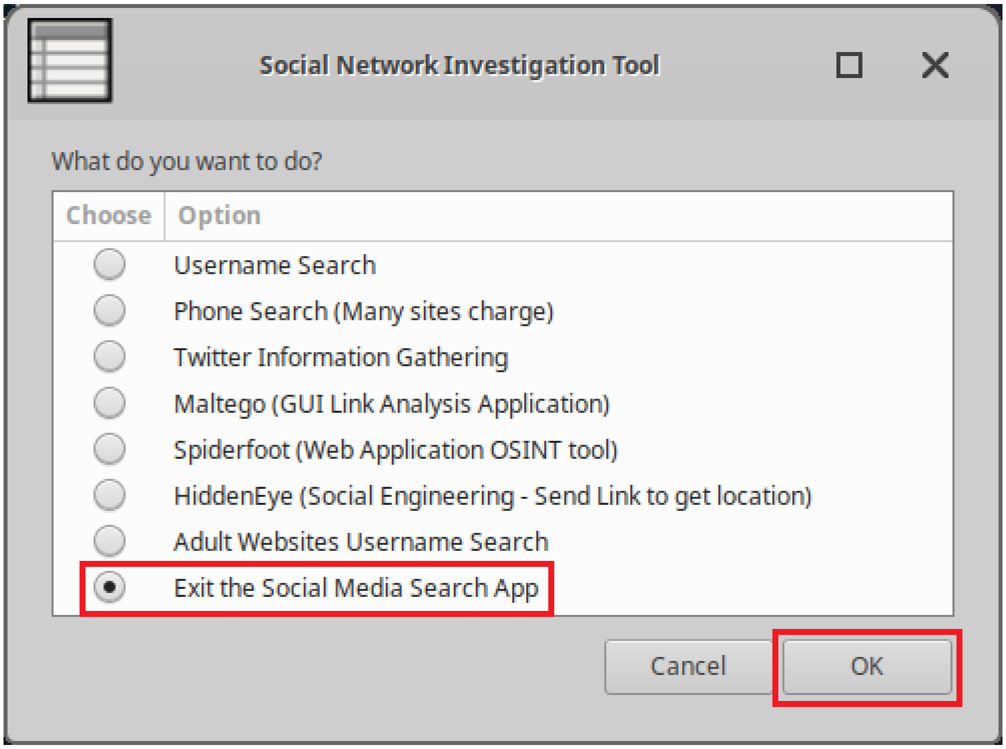


Would you like to open the findings in a browser?



```
https://www.twitter.com/ckrahenbill
https://ckrahenbill.wordpress.com
https://slideshare.net/ckrahenbill
https://www.scribd.com/ckrahenbill
https://en.gravatar.com/ckrahenbill
https://www.canva.com/ckrahenbill
https://onlyfans.com/ckrahenbill
https://www.skyscanner.com/trip/user/ckrahenbill
https://www.github.com/ckrahenbill
https://www.sec.gov/cgi-bin/browse-edgar?company=ckrahenbill&owner=exclude&action=getcompany
```

Once you’re satisfied with the results, you can exit the social media app.



What do you want to do?

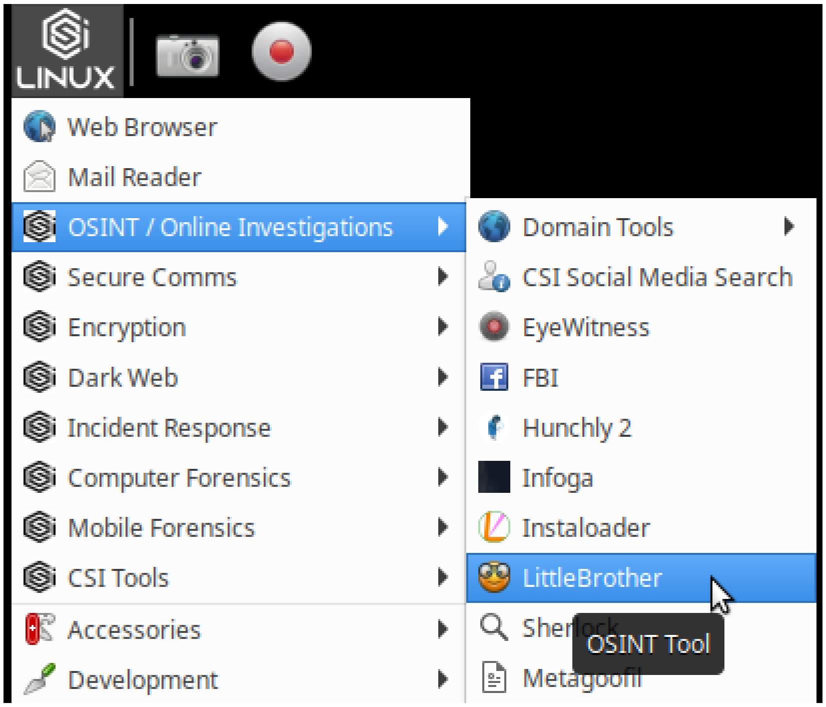
Choose	Option
○	Username Search
○	Phone Search (Many sites charge)
○	Twitter Information Gathering
○	Maltego (GUI Link Analysis Application)
○	Spiderfoot (Web Application OSINT tool)
○	HiddenEye (Social Engineering - Send Link to get location)
○	Adult Websites Username Search
●	Exit the Social Media Search App

OSINT Using Little Brother

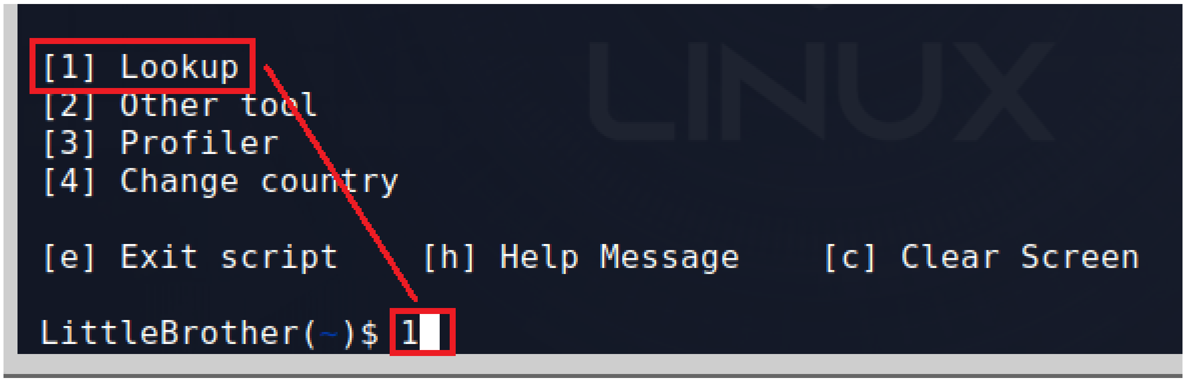
In this next lab, we will search for an individual using the OSINT information collection tool, Little Brother.

Little Brother is an information collection tool (OSINT) that aims to carry out research on a French, Swiss, Luxembourgish, or Belgian person, but it will do US/English background checks as well. It provides various modules that allow useful searches.

Open Applications and from the context menu, select OSINT / Online Investigations. From the next content menu, click on Little Brother. Wait for it to load up.

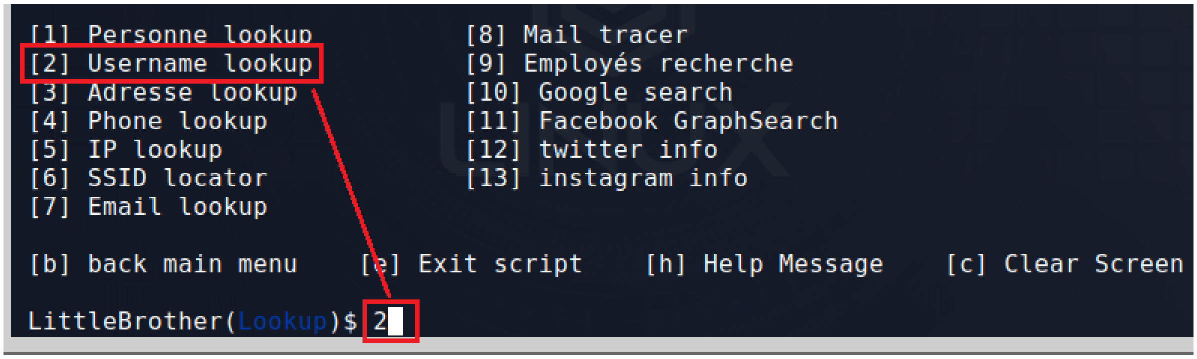


From the menu, select number 1 to conduct a lookup.



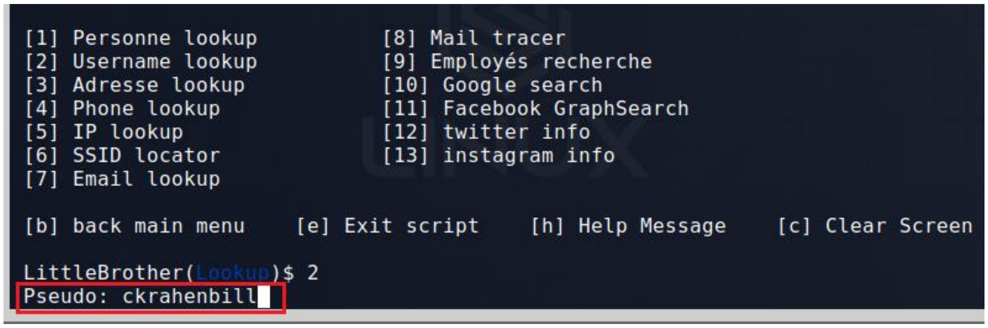
```
[1] Lookup
[2] Other tool
[3] Profiler
[4] Change country

[e] Exit script     [h] Help Message     [c] Clear Screen

LittleBrother(~)$ 1
```

On the next screen, select 2 for a username lookup. You’re free to conduct any of the available searches you choose.



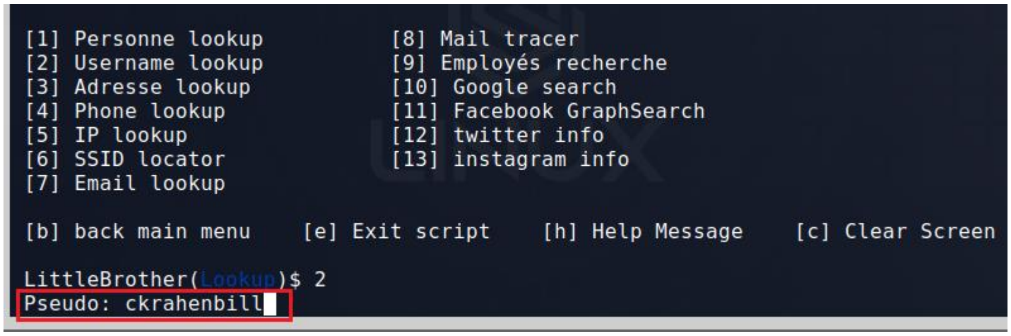
```
[1] Personne lookup            [8] Mail tracer
[2] Username lookup            [9] Employés recherche
[3] Adresse lookup             [10] Google search
[4] Phone lookup               [11] Facebook GraphSearch
[5] IP lookup                  [12] twitter info
[6] SSID locator               [13] instagram info
[7] Email lookup

[b] back main menu    [e] Exit script    [h] Help Message    [c] Clear Screen

LittleBrother(Lookup)$ 2
```

At the next prompt, type in the username. Use your username or the username of your friend or spouse. In this example, I'm using my username — press enter.



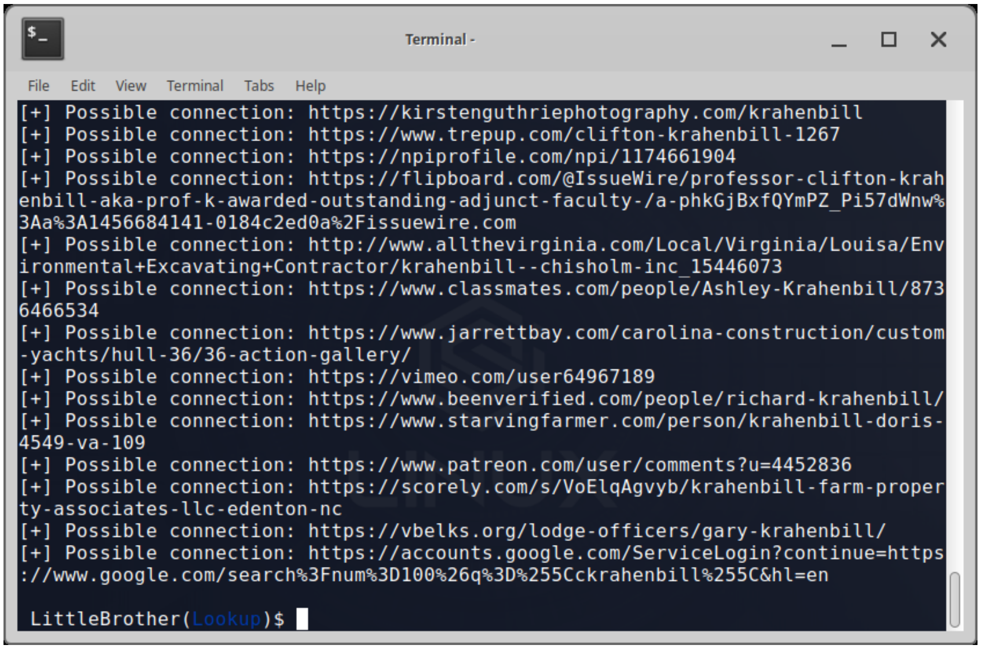
```
[1] Personne lookup            [8] Mail tracer
[2] Username lookup            [9] Employés recherche
[3] Adresse lookup             [10] Google search
[4] Phone lookup               [11] Facebook GraphSearch
[5] IP lookup                  [12] twitter info
[6] SSID locator               [13] instagram info
[7] Email lookup

[b] back main menu    [e] Exit script    [h] Help Message    [c] Clear Screen

LittleBrother(Lookup)$ 2
Pseudo: ckrahenbill
```

The search begins!



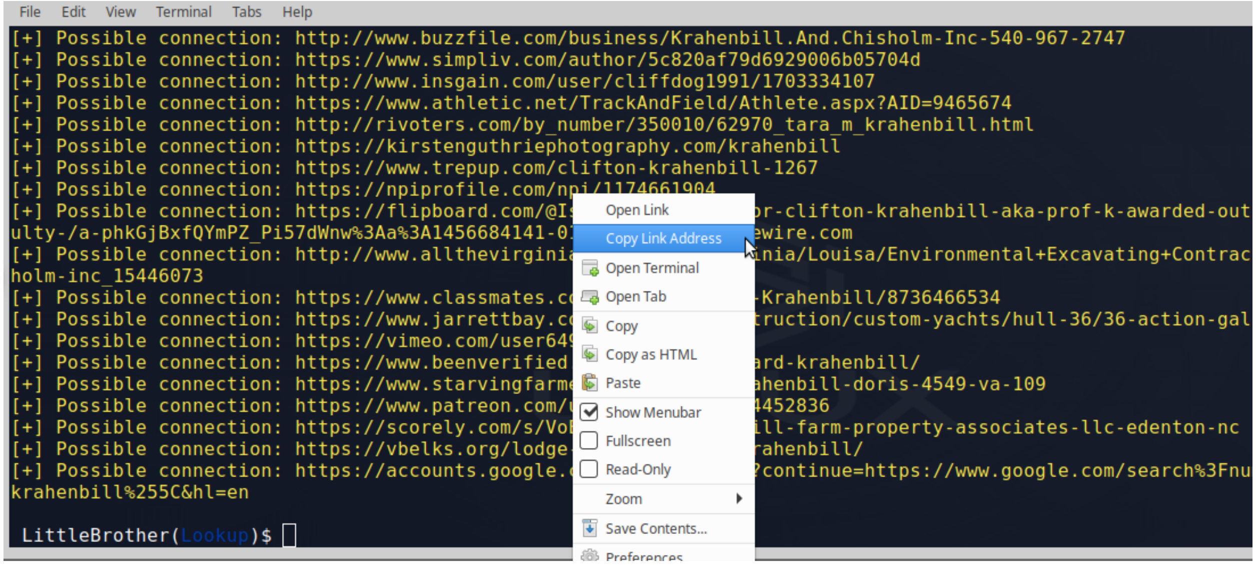
```
[1] Personne lookup            [8] Mail tracer
[2] Username lookup            [9] Employés recherche
[3] Adresse lookup             [10] Google search
[4] Phone lookup               [11] Facebook GraphSearch
[5] IP lookup                  [12] twitter info
[6] SSID locator               [13] instagram info
[7] Email lookup

[b] back main menu    [e] Exit script    [h] Help Message    [c] Clear Screen

LittleBrother(Lookup)$ 2
Pseudo: ckrahenbill
```

You can see that the search results are very extensive but not always accurate. Each of the entries is a hyperlink so you can visit the source to verify the information is valid or not.



```
[+] Possible connection: https://kirstenguthriephotography.com/krahenbill
[+] Possible connection: https://www.trepup.com/clifton-krahenbill-1267
[+] Possible connection: https://npiprofile.com/npi/1174661904
[+] Possible connection: https://flipboard.com/@IssueWire/professor-clifton-krah
enbill-aka-prof-k-awarded-outstanding-adjunct-faculty-/a-phkGjBxfQYmPZ_Pi57dWnw%
3Aa%3A1456684141-0184c2ed0a%2Fissuewire.com
[+] Possible connection: http://www.allthevirginia.com/Local/Virginia/Louisa/Env
ironmental+Excavating+Contractor/krahenbill--chisholm-inc_15446073
[+] Possible connection: https://www.classmates.com/people/Ashley-Krahenbill/873
6466534
[+] Possible connection: https://www.jarrettbay.com/carolina-construction/custom
-yachts/hull-36/36-action-gallery/
[+] Possible connection: https://vimeo.com/user64967189
[+] Possible connection: https://www.beenverified.com/people/richard-krahenbill/
[+] Possible connection: https://www.starvingfarmer.com/person/krahenbill-doris-
4549-va-109
[+] Possible connection: https://www.patreon.com/user/comments?u=4452836
[+] Possible connection: https://scorely.com/s/VoElqAgvyb/krahenbill-farm-proper
ty-associates-llc-edenton-nc
[+] Possible connection: https://vbelks.org/lodge-officers/gary-krahenbill/
[+] Possible connection: https://accounts.google.com/ServiceLogin?continue=https
://www.google.com/search%3Fnum%3D100%26q%3D%255Cckrahenbill%255C&hl=en

 LittleBrother(Lookup)$
```

You would need to go through the results line by line. You can select any or all links, right-click on any or all links and select to have it open in a browser or you can copy the links to a text file.



```
[+] Possible connection: http://www.buzzfile.com/business/Krahenbill.And.Chisholm-Inc-540-967-2747
[+] Possible connection: https://www.simpliv.com/author/5c820af79d6929006b05704d
[+] Possible connection: http://www.insgain.com/user/cliffdog1991/1703334107
[+] Possible connection: https://www.athletic.net/TrackAndField/Athlete.aspx?AID=9465674
[+] Possible connection: http://rivoters.com/by_number/350010/62970_tara_m_krahenbill.html
[+] Possible connection: https://kirstenguthriephotography.com/krahenbill
[+] Possible connection: https://www.trepup.com/clifton-krahenbill-1267
[+] Possible connection: https://npiprofile.com/npi/1174661904
[+] Possible connection: https://flipboard.com/@Is                or-clifton-krahenbill-aka-prof-k-awarded-out
ulty-/a-phkGjBxfQYmPZ_Pi57dWnw%3Aa%3A1456684141-01                ewire.com
[+] Possible connection: http://www.allthevirginia                inia/Louisa/Environmental+Excavating+Contrac
holm-inc_15446073
[+] Possible connection: https://www.classmates.co                -Krahenbill/8736466534
[+] Possible connection: https://www.jarrettbay.co                truction/custom-yachts/hull-36/36-action-gal
[+] Possible connection: https://vimeo.com/user649
[+] Possible connection: https://www.beenverified                 ard-krahenbill/
[+] Possible connection: https://www.starvingfarme                ahenbill-doris-4549-va-109
[+] Possible connection: https://www.patreon.com/u                4452836
[+] Possible connection: https://scorely.com/s/VoE                ill-farm-property-associates-llc-edenton-nc
[+] Possible connection: https://vbelks.org/lodge-                rahenbill/
[+] Possible connection: https://accounts.google.c                ?continue=https://www.google.com/search%3Fnu
krahenbill%255C&hl=en

 LittleBrother(Lookup)$
```

End of the lab!