

Task 17 – Information Gathering Tools

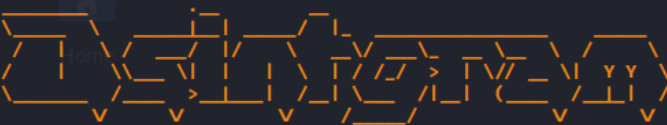
Name – Vishal Pathak

Osintgram – A osint tool for finding information regarding any social media accounts.

```
(venv) [root@kali] [~/Forensic/Osintgram]
#python3 main.py 2.vishal.3

Attempt to login...
ClientCookieExpiredError/ClientLoginRequiredError: Cookie expired at 1628592384

Logged as arthurleywin348. Target: 2.vishal.3 [8388764821] [PRIVATE PROFILE] [FOLLOWING]



Version 1.1 - Developed by Giuseppe Criscione

Type 'list' to show all allowed commands
Type 'FILE=y' to save results to files like '<target username>_<command>.txt (default is disabled)'
Type 'FILE=n' to disable saving to files'
Type 'JSON=y' to export results to a JSON files like '<target username>_<command>.json (default is disabled)'
Type 'JSON=n' to disable exporting to files'
Run a command: list
FILE=y/n      Enable/disable output in a '<target username>_<command>.txt' file'
JSON=y/n      Enable/disable export in a '<target username>_<command>.json' file'
addr          Get all registered addressed by target photos
cache         Clear cache of the tool
captions      Get target's photos captions
commentdata   Get a list of all the comments on the target's posts
comments      Get total comments of target's posts
followers     Get target followers
followings    Get users followed by target
fwersemail    Get email of target followers
fwingsemail   Get email of users followed by target
fwersnumber   Get phone number of target followers
fwingsnumber  Get phone number of users followed by target
hashtags      Get hashtags used by target
info          Get target info
likes         Get total likes of target's posts
mediatype     Get target's posts type (photo or video)
photodes      Get description of target's photos
photos        Download target's photos in output folder
propic        Download target's profile picture
stories       Download target's stories
tagged        Get list of users tagged by target
target        Set new target
wcommented    Get a list of user who commented target's photos
wtaged        Get a list of user who tagged target
Run a command: 
```

When you first run the open the tool you get something like this. You can see here that there are a lot of option to gather a good amount of info from the target by using our tool. Here our target is Instagram account 2.vishal.3.

Now, lets get started first we will try to find all the infos regarding his followers, likes, his profile pic and his other related infos, it infos would be in screenshot form below:

Followers

When you use the followers command it shows something like this

3196433424		sharmaji_jvs		Jay Sharma
4392420587		nikhil.nd0606		Nikhil Dudhuke
3511353307		varun._._.k		🇮🇦🇮🇦🇮🇦
7545089802		imyash0407		yash_with_u🌟❤
9385154231		kamalesh0002		(^_^)f♥ k🇮🇦🇮🇦🇮🇦lēsh ♥t(^_^)f
2116515213		its_jayjoshi0.07		Jay Joshi ♥
1370123046		a_skeptical_man		Amy
4643550602		gixhnu		JISHNU VENUGOPAL
2243745566		its_omkxrr		Omkar Kumbhar🤔
27139340859		quamir_ynsu		Qxamir-
3095342090		liferacer333		Hemanth Reddy
36992683506		college_onest		College O'Nest
31997696075		izhma_sh		CounterFieT🇧🇧
4565653291		jaipreeth		DoHackhaha ._. ._.
46405895687		nightman_hunter		
14514292632		ambient_photography8		tejas prajapati
31313743874		bug_xs		BUG XS CYBERSECURITY 🖥
48554704969		7h3_1nv1c7u5_		
12722184090		mr.innocent_1809		Patel Parth
44654952717		mari_karthik11		Marikarthik
9286740522		letsplandecors		LETSPLANDECORS NIKKI DESAI
26108355151		ghostclannft		
5675829341		anjali_22patel		anjali_22patel
5785941247		vyas8151		vyas janvi
49480571793		badass_marvel_fan		"I Can Do This All Day"
46503370145		eternal.dx		Eternal🔪🇸🇪
6834714493		_naina1603		Naina Sharma
44724503537		the_vitalityify		The Vitalityify
4211308331		vraj_1217		vraj_patel_12

Followings

11677203240	animetv_jp	AnimeTV チェーン
21076427	ryanbergara	Ryan Bergara
24763791351	wearewatcher	Watcher
14712485634	kid.killlua._	Kid.killlua
15065738242	nft.news2	Metaverse NFT Crypto
474567586	anime.quotes	Anime Quotes
8485873	dudeperfect	Dude Perfect
2075305619	carryminati	Ajey Nagar
7977071346	sciencelover212	Science Lover
4191557773	quanta_gramm	* Quantagramm *
259220806	9gag	9GAG: Go Fun The World
1337343	youtube	YouTube
2936697877	animeuproar	Anime Uproar
6778919690	sciensationist	Sciensationist: Science Media
16734470563	the_official_weeb	Anime Memes
1760411266	joshnissan	Joshua Nissan
46218147	igndotcom	IGN
366620103	crunchyroll	Crunchyroll
2296777006	brainheaters	Brainheaters™
3220219191	limisama	Call me Onii-chan
28250699851	_.blackclover	Black Clover
1517175094	fuyuki23	Fuyuki23
2321191491	toei_animation	Toei Animation
1173266158	ourvadodara	OUR VADODARA™
199393179	hbo	HBO
1975018120	therealjosephmorgan	Joseph Morgan
8006476055	anime_akai	ANIME POSTS ♥JOIN US↑↑
8473202876	theanimeclan	Anime Memes Videos
16659508468	anixarc	Animes & more!
1769476128	ferrari	Ferrari
12543425178	nft__calendar	NFT Calendar
7293953219	orjinallege	
2003919389	asusrog	ROG Global
1493354161	lifennoggin	Life Noggin
528817151	nasa	NASA
49337007536	virtuallytestingfoundation	Virtually Testing Foundation
207587378	netflix	Netflix US
2493037651	bhuvan.bam22	Bhuvan Bam
5675829341	anjali_22patel	anjali_22patel
700180961	typicalgamer	Typical Gamer
45053204010	weebplanet	Anime • Memes • Culture
28564188782	onepiecedestiny	One Piece • ワンピース
6393531713	vidyamohanajobs	Vidyamohana Jobs
184595688	rockstargames	Rockstar Games

Some commands like propic,likes,info are shown belows

```

wtagged Get a list of user who tagged target
Run a command: propic
Target propic saved in output folder
Run a command: likes
Searching for target total likes ...
203 likes in 10 posts
Run a command: infos
Unknown command
Run a command: info
[ID] 8388764821
[FULL NAME] Vishal Pathak
[BIOGRAPHY] When you have eliminated the impossible, whatever remains, however improbable
-Sherlock Holmes
[FOLLOWED] 140
[FOLLOW] 231
[BUSINESS ACCOUNT] False
[VERIFIED ACCOUNT] False
[HD PROFILE PIC] https://instagram.fstv8-2.fna.fbcdn.net/v/t51.2885-19/189285821_3809520
97LABVCyAlR03AsDiJGUyiIYnC4aQ6S-uJrJU6gDX0g6oe=621DD8FA&_nc_sid=e3b034

```

```

Run a command: photos
How many photos you want to download (default all): 10
Downloading 10 photos ...
Downloaded 10 photos
Woohoo! We downloaded 10 photos (saved in output folder)
Run a command: stories
Searching for target stories ...
Sorry! No results found :-(
mediatype
Searching for target captions ...
Checked 10 posts
Woohoo! We found 0 photos and 3 video posted by target
Run a command: fwingemails
Unknown command
Run a command: fwingemail
Unknown command
Run a command: fwingsemail
Searching for emails of users followed by target... this ca
Do you want to get all emails? y/n: n
5
Caught 2 followings email

```

This commands fwingemails shows the followings emails address if they are available to the person

```

Unknown Command
Run a command: fwingsemail
Searching for emails of users followed by target... this can take a few minutes
Do you want to get all emails? y/n: n
5
Caught 5 followings email

```

ID	Username	Full Name	Email
14503648261	__your_gallery__	Joshi Dhananjay	dhananjayjoshi1711@gmail.com
5451969785	dhruvamdave	Dhruvam Dave	dhruvamdave1105@gmail.com
2865754192	sarcastic_us	Sarcasm	marketing@digihoodmedia.com
27940149000	gravity.phy	Science	gravity.phy@gmail.com
4393916351	takealook_friends	TakeALook FRIENDS	takealook.videos@gmail.com

There are other commands also but this are one I found the most interesting one.

Tool- recon ng – it is a reconnaissance tool which searches for whatever infos is available for the target.

So when you first run the you need to add the modules in it. Here, there are various modules which can be used for gathering a information for any domain or a website with the appropriate tool and also we can make report on the same by using the report modules which are present in it.

```

[recon-ng][visnat][builtwith] > help

```

Commands (type [help|?] <topic>):

back	Exits the current context
dashboard	Displays a summary of activity
db	Interfaces with the workspace's database
exit	Exits the framework
goptions	Manages the global context options
help	Displays this menu
info	Shows details about the loaded module
input	Shows inputs based on the source option
keys	Manages third party resource credentials
modules	Interfaces with installed modules
options	Manages the current context options
pdb	Starts a Python Debugger session (dev only)
reload	Reloads the loaded module
run	Runs the loaded module
script	Records and executes command scripts
shell	Executes shell commands
show	Shows various framework items
spool	Spools output to a file

This are all the commands present in the tool and you can even see the use of them. Some of the important one are the workspaces,modules,marketplace key and run. This are the commands through which we can install a particular module and run it and if it needs api keys then we can enter the keys in it as well so that it can run the particular tool/modules.

Lets install a built with module for domain research. The installation is very simple , just goto the a workspace and run the marketplace search builtwith command and it will show all the tool names with builtwith commands.

```
[recon-ng][vishal] > marketplace search builtwith
[*] Searching module index for 'builtwith' ...

+-----+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+
| recon/domains-hosts/builtwith | 1.1 | installed | 2021-08-24 | | * |
+-----+-----+-----+-----+-----+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][vishal] > 
```

Then just run the marketplace install command and it will install. Now to run you need to add api keys by using the keys command. After that just write module load modulename and it will load. Next just run the module and it will search the hostname of the target. You can edit it by using source command to whatever your target is.

K = Requires keys. See info for details.

```
[recon-ng][vishal] > modules load recon/domains-hosts/builtwith  
[recon-ng][vishal][builtwith] > run
```

GRASPLE.COM

```
[*] Country: None  
[*] Email: hello@grasple.com  
[*] First_Name: None  
[*] Last_Name: None  
[*] Middle_Name: None  
[*] Notes: None  
[*] Phone: None  
[*] Region: None  
[*] Title: BuiltWith contact
```

```
[*]  
[*] Country: None  
[*] Email: support@grasple.com  
[*] First_Name: None  
[*] Last_Name: None  
[*] Middle_Name: None  
[*] Notes: None  
[*] Phone: None  
[*] Region: None  
[*] Title: BuiltWith contact
```

```
[*]  
[*] Country: None  
[*] Email: privacy@grasple.com  
[*] First_Name: None  
[*] Last_Name: None  
[*] Middle_Name: None  
[*] Notes: None  
[*] Phone: None  
[*] Region: None  
[*] Title: BuiltWith contact
```

```
[*]  
[*] Country: None  
[*] Host: app.grasple.com  
[*] Ip_Address: None  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None
```

Tool- Eagle Osint – it is a all in one tool where you find information regarding any sort of things like from a name to the his location even granted if we provide the correct information.

Now let try this tool.

When you first run the tool it shows something like this.


```

> choose: 1
> enter username: 2sabo3
Exception in thread Thread-48: | 66.2% FOUND: 14
Traceback (most recent call last):
  File "/usr/lib/python3.9/threading.py", line 973, in _bootstrap_inner
    self.run()
  File "/usr/lib/python3.9/threading.py", line 910, in run
    self._target(*self._args, **self._kwargs)
  File "/root/Forensic/E4GL30S1NT/E4GL30S1NT.py", line 145, in send_req
    if req.status_code == 200: color = g; userrecon_working += 1
UnboundLocalError: local variable 'req' referenced before assignment
71/71 | | 100.0% FOUND: 17

[404] 1/71 https://facebook.com/2sabo3
[404] 2/71 https://instagram.com/2sabo3
[200] 3/71 https://twitter.com/2sabo3
[404] 4/71 https://youtube.com/2sabo3
[404] 5/71 https://vimeo.com/2sabo3
[200] 6/71 https://github.com/2sabo3
[200] 7/71 https://pinterest.com/2sabo3
[404] 8/71 https://vk.com/2sabo3
[200] 9/71 https://plus.google.com/2sabo3
[404] 10/71 https://flickr.com/people/2sabo3
[404] 11/71 https://disqus.com/2sabo3
[404] 12/71 https://about.me/2sabo3
[404] 13/71 https://bitbucket.org/2sabo3
[404] 14/71 https://medium.com/@2sabo3
[404] 15/71 https://flipboard.com/@2sabo3
[404] 16/71 https://hackerone.com/2sabo3
[404] 17/71 https://keybase.io/2sabo3
[404] 18/71 https://buzzfeed.com/2sabo3
[200] 19/71 https://mixcloud.com/2sabo3
[404] 20/71 https://slideshare.net/2sabo3
[404] 21/71 https://soundcloud.com/2sabo3
[200] 22/71 https://badoo.com/en/2sabo3
[200] 23/71 https://imgur.com/user/2sabo3
[200] 24/71 https://open.spotify.com/user/2sabo3
[200] 25/71 https://pastebin.com/u/2sabo3
[404] 26/71 https://wattpad.com/user/2sabo3
[403] 27/71 https://canva.com/2sabo3
[404] 28/71 https://codecademy.com/2sabo3
[404] 29/71 https://last.fm/user/2sabo3
[404] 30/71 https://en.gravatar.com/2sabo3
[403] 31/71 https://creativemarket.com/2sabo3
[404] 32/71 https://blip.fm/2sabo3
[404] 33/71 https://ello.co/2sabo3
[200] 34/71 https://foursquare.com/2sabo3
[404] 35/71 https://angel.co/2sabo3
[404] 36/71 https://dribbble.com/2sabo3

```

As you can see it shows where this username is used and the status code which shows that its no longer used.

2 facedumper – gives facebook information about the target

3 maildumper – give you a list of mail with the name or anything you mention

```
11 RIPLookup      Reverse IP lookup
12 IPlocation     IP to location tracker
13 Bitly Bypass   Bypass all bitly urls
14 Github Lookup  Dump GitHub information
15 TempMail       Generate Temp Mail and Mail Box
00 Exit          bye bye ):

> choose: 3
> enter name: vishal

VALID 1/390 Status: valid Email: vishal@gmail.com
VALID 2/390 Status: valid Email: vishal@yahoo.com
VALID 3/390 Status: valid Email: vishal@aol.com
VALID 4/390 Status: valid Email: vishal@hotmail.com
UNKNOWN 5/390 Status: unknown Email: vishal@comcast.net
INVALID 6/390 Status: invalid Email: vishal@msn.com
VALID 7/390 Status: valid Email: vishal@live.com
UNKNOWN 8/390 Status: unknown Email: vishal@ymail.com
VALID 9/390 Status: valid Email: vishal@googlemail.com
UNKNOWN 10/390 Status: unknown Email: vishal@rocketmail.com
VALID 11/390 Status: valid Email: vishal@outlook.com
UNKNOWN 12/390 Status: unknown Email: vishal@rediffmail.com
INVALID 13/390 Status: invalid Email: vishal@cox.net
UNKNOWN 14/390 Status: unknown Email: vishal@att.net
UNKNOWN 15/390 Status: unknown Email: vishal@bellsouth.net
INVALID 16/390 Status: invalid Email: vishal@facebook.com
UNKNOWN 17/390 Status: unknown Email: vishal@earthlink.net
UNKNOWN 18/390 Status: unknown Email: vishal@sky.com
VALID 19/390 Status: valid Email: vishal@me.com
UNKNOWN 20/390 Status: unknown Email: vishal@optonline.net
UNKNOWN 21/390 Status: unknown Email: vishal@gmx.net
UNKNOWN 22/390 Status: unknown Email: vishal@mail.com
```

Here I have mentioned name vishal and it shows all the emails with that name.

4 godorker- gives info from the dorks . it similar to how you use google dork in google search but the output is shown here.

5 phoneinfo – give information from the phone number like place and etc.

```
> choose: 5
> enter number: 7778886062

- status : success
- phone : +917778886062
- phone_valid : True
- phone_type : mobile
- phone_region : India
- country : India
- country_code : IN
- country_prefix : 91
- international_number : +91 77788 8606
- local_number : 077788 86062
- e164 : +917778886062
- carrier : Telewings

DONE 7778886062
press enter for back to previous menu
```

6 dns lookup – gives you the domain system information of the domain you enter.

Example

```
13 Bitty Bypass Bypass all Bitty bits
14 Github Lookup Dump GitHub information
15 TempMail Generate Temp Mail and Mail Box
00 Exit bye bye :)

> choose: 6
> enter domain or IP: grasple.com

- A : 52.85.61.93
- A : 52.85.61.103
- A : 52.85.61.129
- A : 52.85.61.71
- AAAA : 2600:9000:2209:3400:14:3216:a940:93a1
- AAAA : 2600:9000:2209:c800:14:3216:a940:93a1
- AAAA : 2600:9000:2209:f400:14:3216:a940:93a1
- AAAA : 2600:9000:2209:b800:14:3216:a940:93a1
- AAAA : 2600:9000:2209:5c00:14:3216:a940:93a1
- AAAA : 2600:9000:2209:7000:14:3216:a940:93a1
- AAAA : 2600:9000:2209:7c00:14:3216:a940:93a1
- AAAA : 2600:9000:2209:ec00:14:3216:a940:93a1
- MX : 1 aspmx.l.google.com.
- MX : 10 aspmx2.googlemail.com.
- MX : 10 aspmx3.googlemail.com.
- MX : 5 alt1.aspmx.l.google.com.
- MX : 5 alt2.aspmx.l.google.com.
- NS : ns-1423.awsdns-49.org.
- NS : ns-146.awsdns-18.com.
- NS : ns-1686.awsdns-18.co.uk.
- NS : ns-672.awsdns-20.net.
- TXT : "atlassian-domain-verification=T0swCmj3dN6TwZML83dMavCSDr5N2B92dTcWw/z73LyTos3Zx247wXax41zqG2Of"
- TXT : "google-site-verification=DbBHq0HL9jm9YHUqA6UkIjgZkWL0sHnrA-5ikisd2ao"
- TXT : "v=spf1 include:_spf.google.com include:spf.mandrillapp.com include:servers.mcsv.net ~all"
- SOA : ns-1686.awsdns-18.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

press enter for back to previous menu
```

7 subnetwork – finds the subnet information of the target website.

```

14 Github Lookup   Dump GitHub information
15 TempMail        Generate Temp Mail and Mail Box
00 Exit            bye bye ):

> choose: 8
> enter domain or IP: grasple.com

- Address      = 2600:9000:233d:6400:14:3216:a940:93a1
- Network      = 2600:9000:233d:6400:14:3216:a940:93a1 / 128
- Netmask      = ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
- Wildcard Mask = ::
- Hosts Bits   = 1
- Max. Hosts   = 1 (2^1 - 1)
- Host Range   = { 2600:9000:233d:6400:14:3216:a940:93a1 - 2600:9000:233d:6400:14:3216:a940:93a1 }

press enter for back to previous menu █

```

Tool Links

<https://github.com/COMPL3XDEV/E4GL30S1NT>

<https://github.com/Datalux/Osintgram>

Recon ng is predownloaded in the kali linux or you can download using the

Sudo apt-get install recon-ng