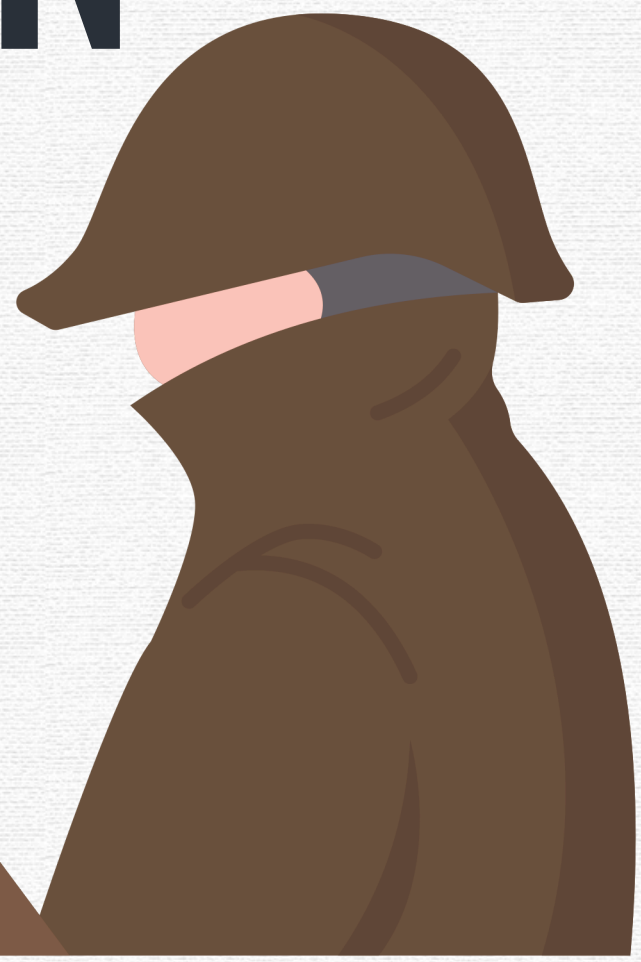
INFORMATION GATHERING



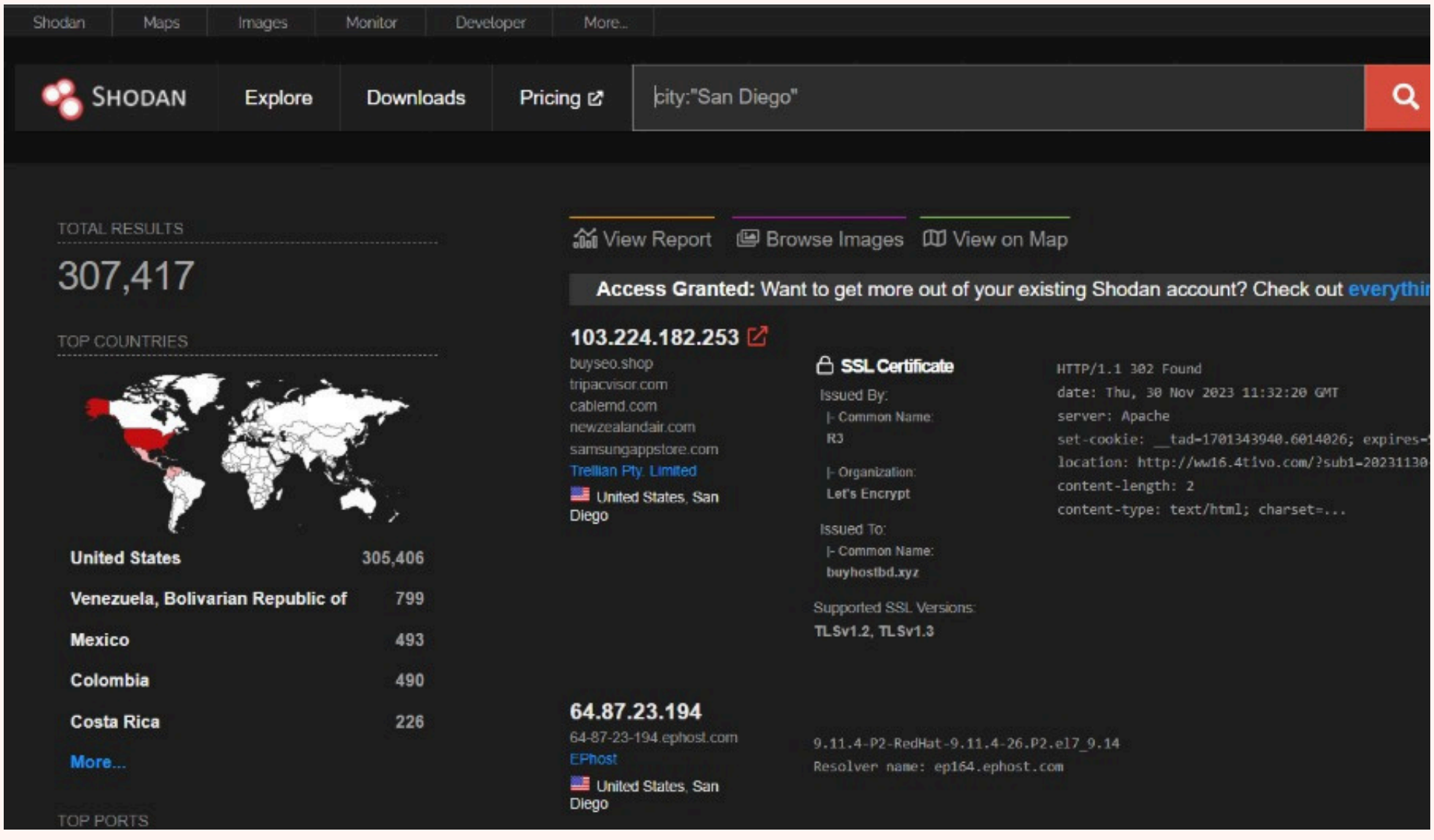
TOOLS

CODELIVLY
LEARN CYBERSECURITY

GOOGLE HACKING DATABASE

CODELIVLY
LEARN CYBERSECURITY

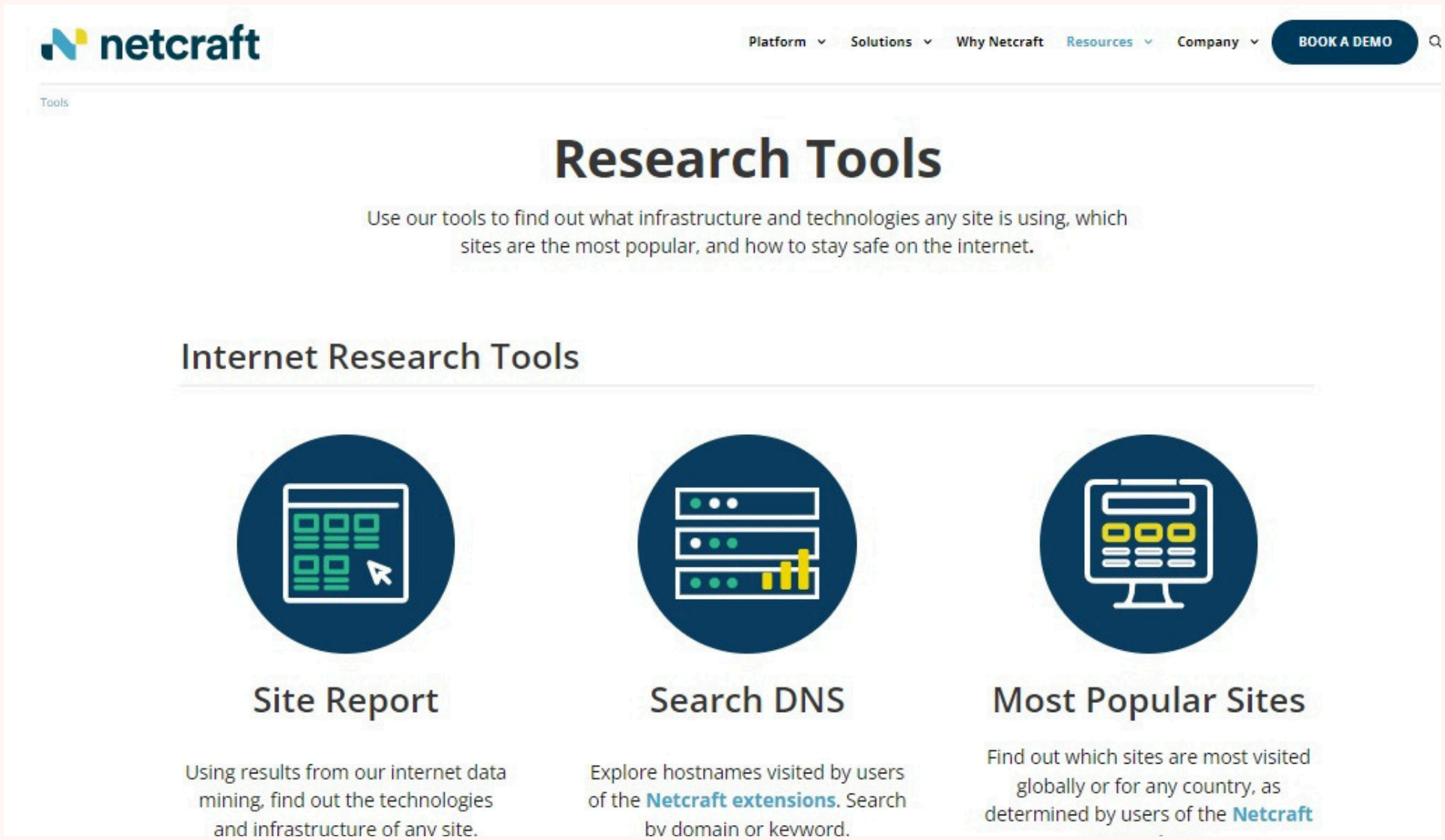
SHODAN.IO



CODELIVLY

LEARN CYBERSECURITY

NETCRAFT



CODELIVLY

LEARN CYBERSECURITY

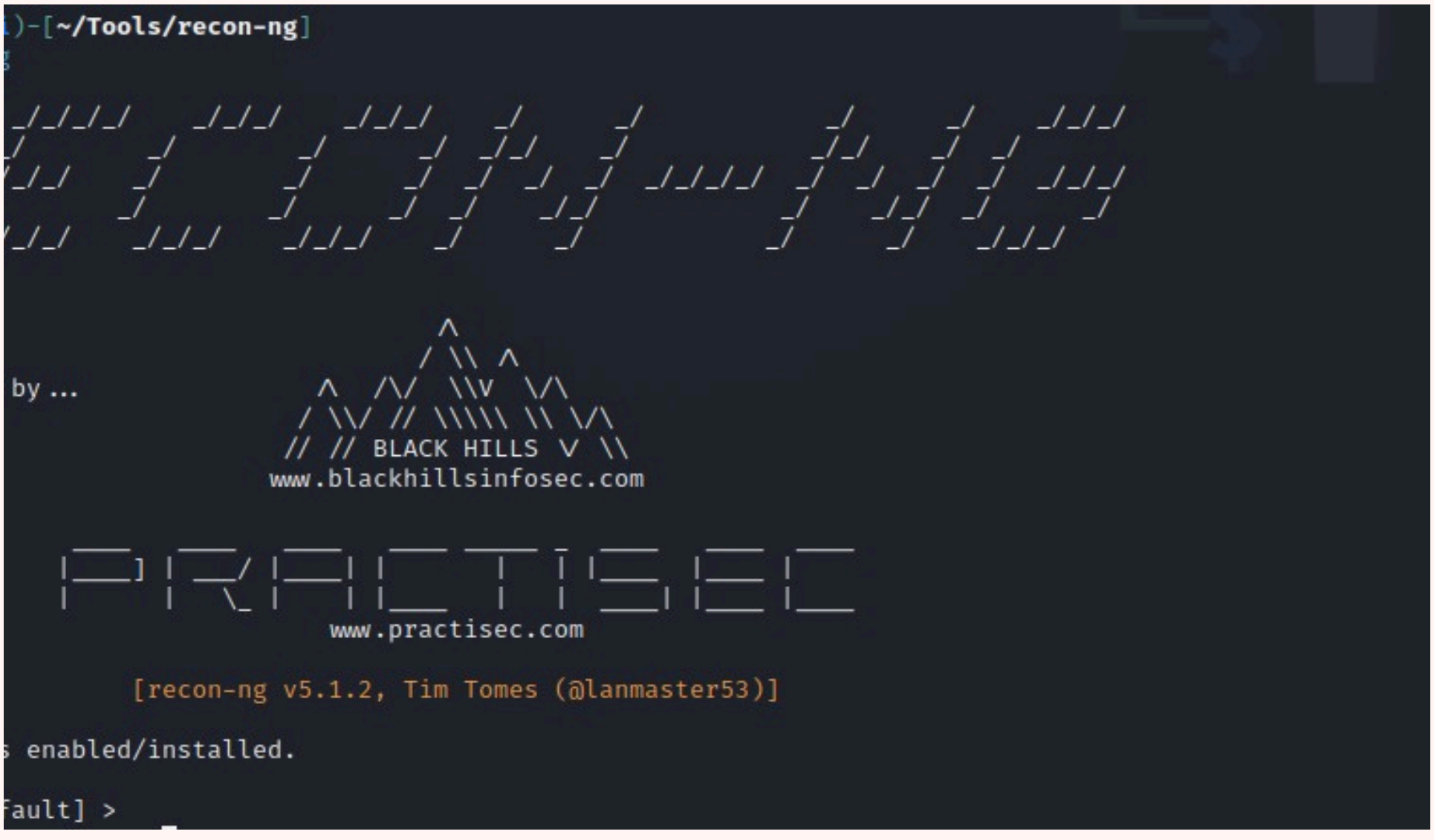
THE HARVESTER

```
┌──(root㉿kali)-[~]
└─# theHarvester -h
*******************************************************************
*                                                                 *
*  _   _                                            _             *
* | |_| |_ ___   /\  /\__ _ _ ____   _____  ___| |_ ___ _ __    *
* | __| _ \ / _ \ / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|   *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.4                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]] [-n] [-c] [-f FILEN

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

options:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -S START, --start START
                        Start with result number X, default=0.
  -p, --proxies         Use proxies for requests, enter proxies in proxies.yaml.
  -s, --shodan          Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output directory: --screenshot output_directory
  -v, --virtual-host    Verify host name via DNS resolution and search for virtual hosts.
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup.
  -t, --take-over       Check for takeovers.
  -r [DNS_RESOLVE], --dns-resolve [DNS_RESOLVE]
                        Perform DNS resolution on subdomains with a resolver list or passed in resolvers, default False.
  -n, --dns-lookup      Enable DNS server lookup, default False.
  -c, --dns-brute       Perform a DNS brute force on the domain.
  -f FILENAME, --filename FILENAME
                        Save the results to an XML and JSON file.
  -b SOURCE, --source SOURCE
                        anubis, baidu, bevigil, binaryedge, bing, bingapi, bufferoverun, brave, censys, certspotter, criminalip, crtsh, dnsdumpster, duckduck
                        onyphe, otx, pentesttools, projectdiscovery, rapiddns, rocketreach, securityTrails, sitedossier, subdomaincenter, subdomainfinderc99,
```

SHERLOCK

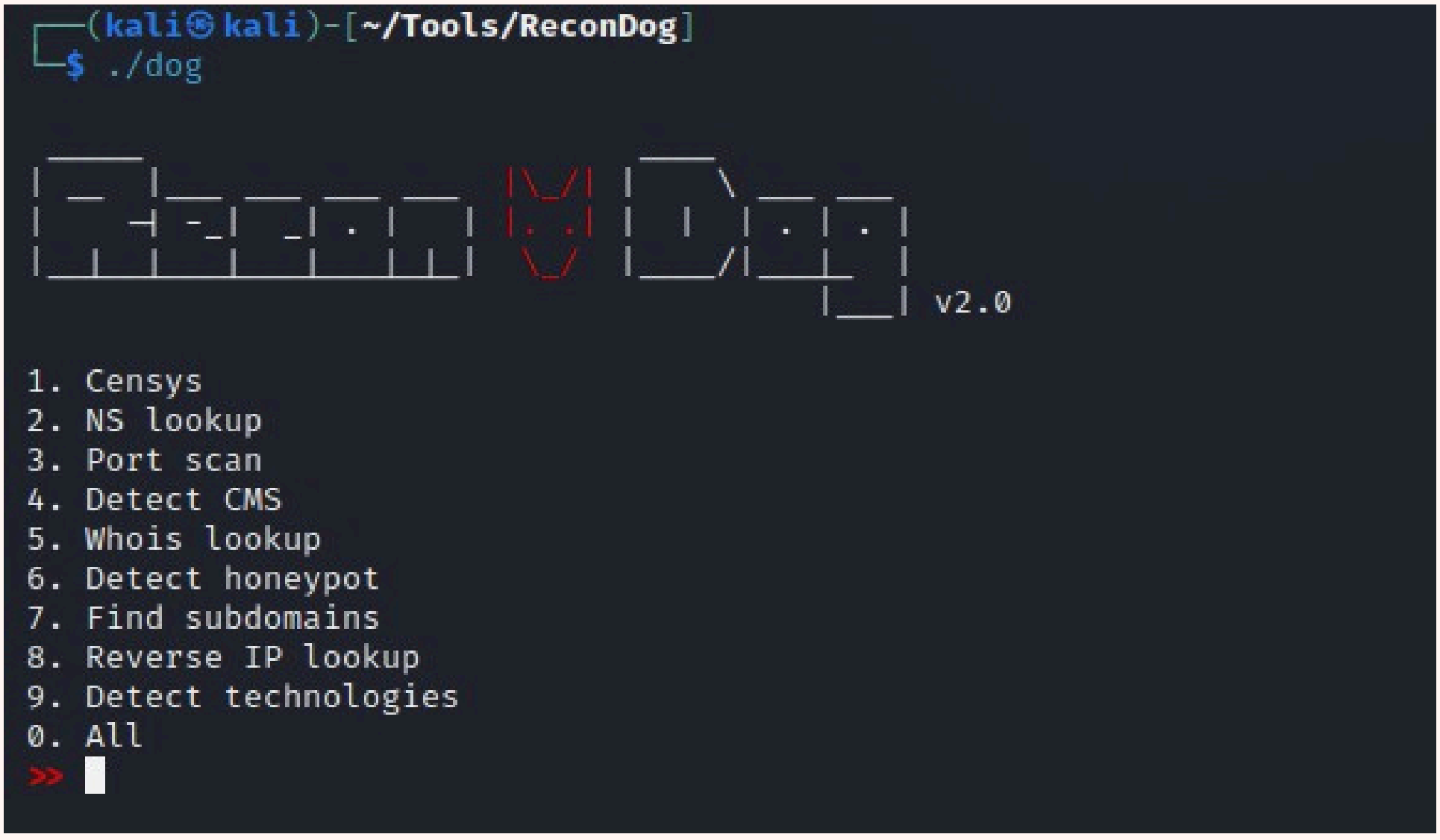
```
┌──(root㉿kali)-[~]
└─# sherlock venkatesh
[*] Checking username venkatesh on:

[+] 7Cups: https://www.7cups.com/@venkatesh
[+] 8tracks: https://8tracks.com/venkatesh
[+] 9GAG: https://www.9gag.com/u/venkatesh
[+] About.me: https://about.me/venkatesh
[+] Academia.edu: https://independent.academia.edu/venkatesh
[+] Airliners: https://www.airliners.net/user/venkatesh/profile/photos
[+] AllMyLinks: https://allmylinks.com/venkatesh
[+] Amino: https://aminoapps.com/u/venkatesh
[+] Anilist: https://anilist.co/user/venkatesh/
[+] Apple Developer: https://developer.apple.com/forums/profile/venkatesh
[+] Apple Discussions: https://discussions.apple.com/profile/venkatesh
[+] Archive.org: https://archive.org/details/@venkatesh
[+] Asciinema: https://asciinema.org/~venkatesh
[+] AskFM: https://ask.fm/venkatesh
[+] Audiojungle: https://audiojungle.net/user/venkatesh
```

RECON-NG



CODELIVLY
LEARN CYBERSECURITY

RECON-DOG



CODELIVLY
LEARN CYBERSECURITY

SUBLIST3R

CODELIVLY

LEARN CYBERSECURITY