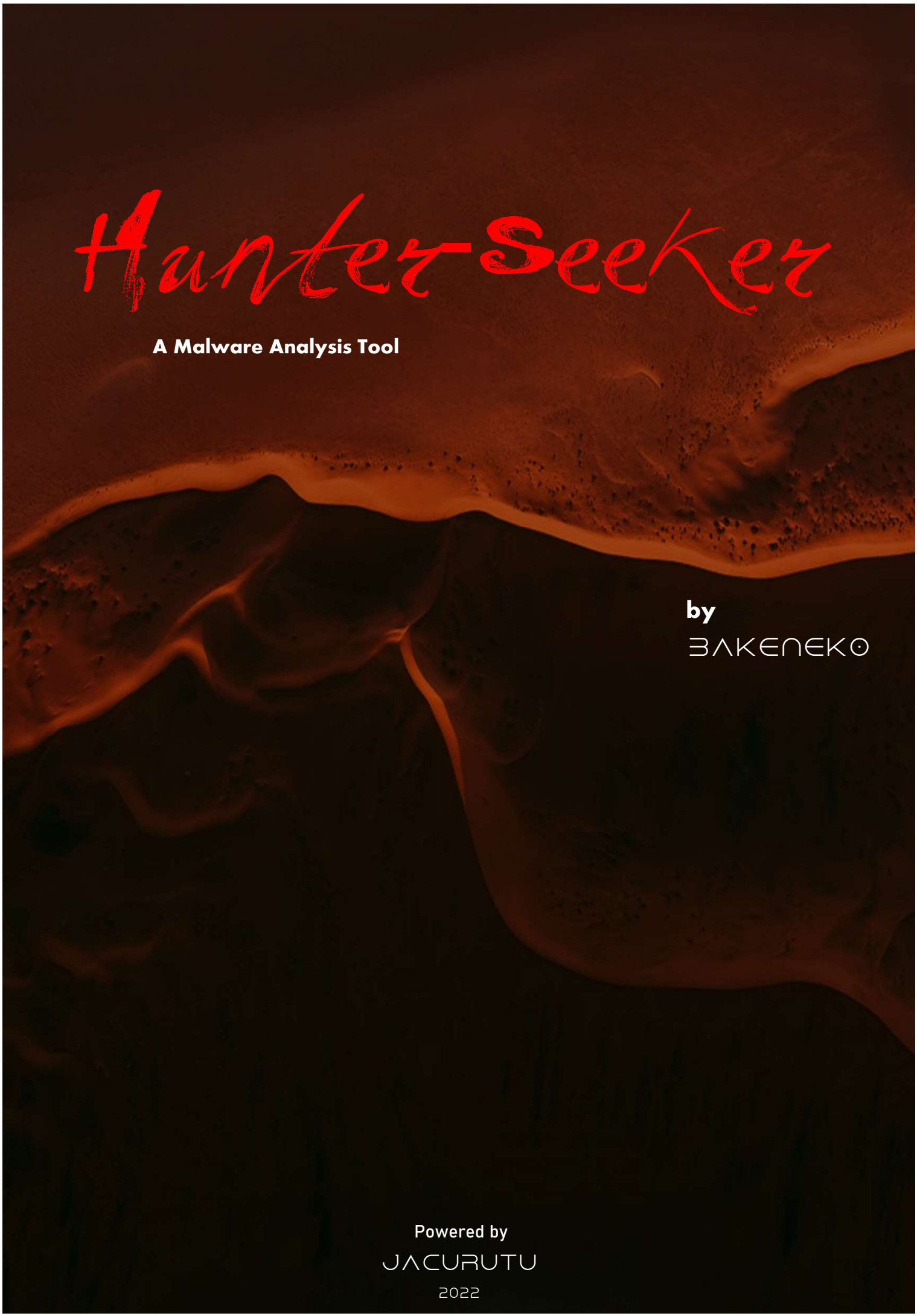
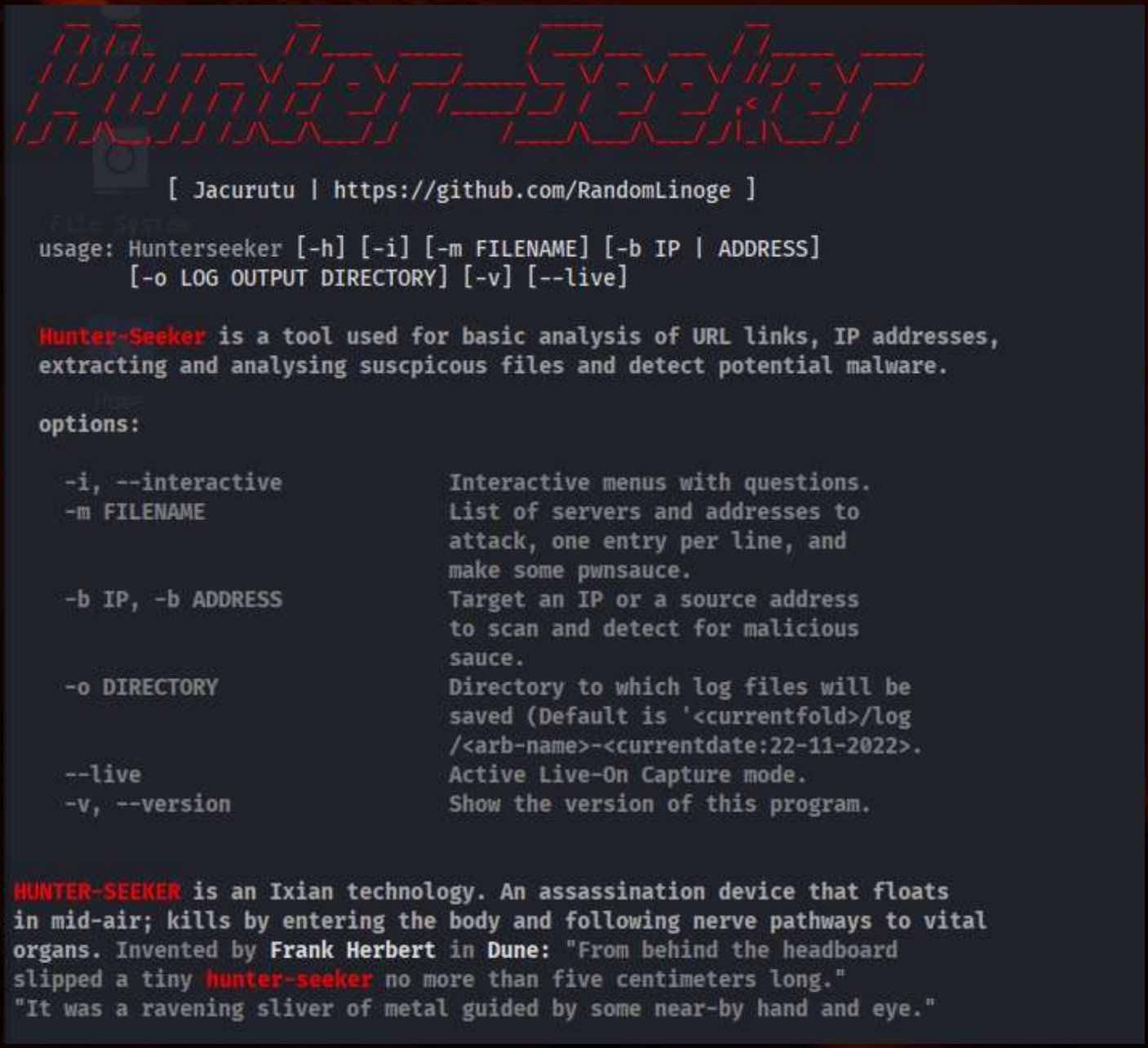

HunterSeeker
A Malware Analysis Tool
by
BAKENEKO
Powered by
JACURUTU
2022

HUNTER-SEEKER is an Ixian technology. An assassination device that floats in mid-air; kills by entering the body and following nerve pathways to vital organs.
Invented by **Frank Herbert** in **Dune**: "From behind the headboard slipped a tiny HUNTER-SEEKER no more than five centimeters long..."
"It was a ravening sliver of metal guided by some near-by hand and eye".

What is the Hunter-Seeker tool?

Hunter-Seeker is a tool used for basic analysis of URL links, IP addresses, and IoC links.
Extracting and analyzing suspicious files and detecting for potential malware.

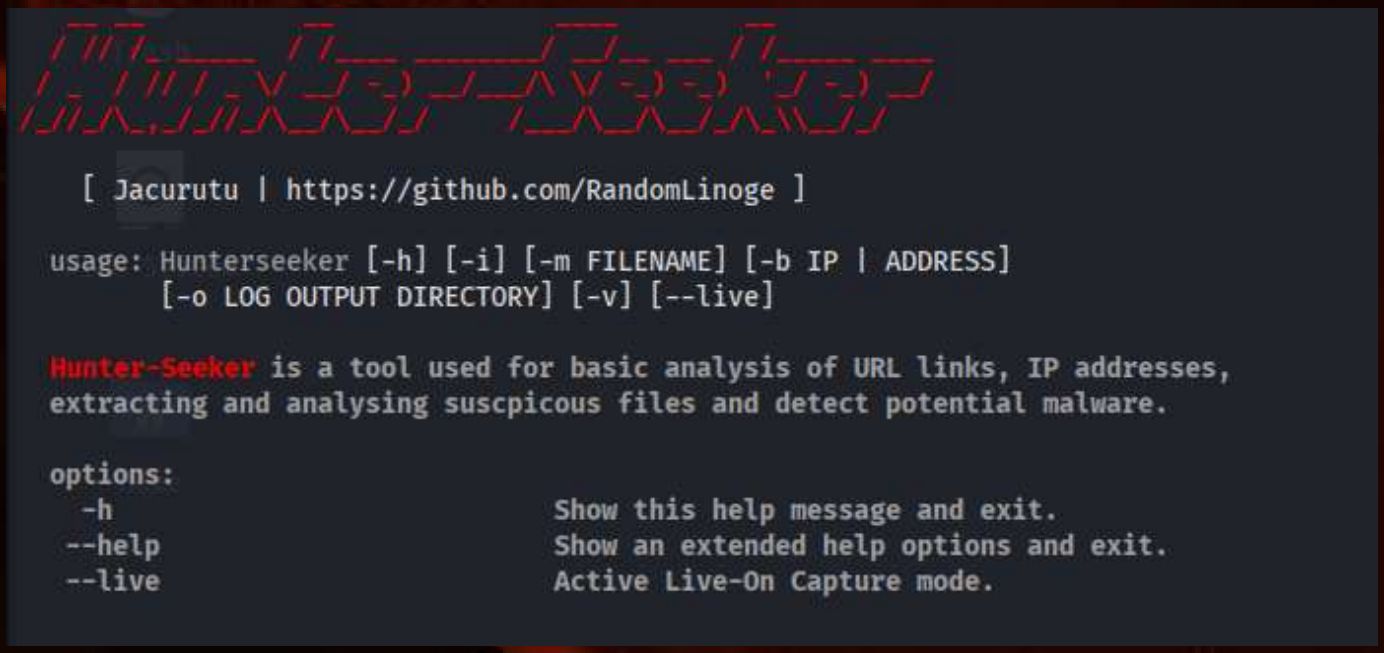


Full help information

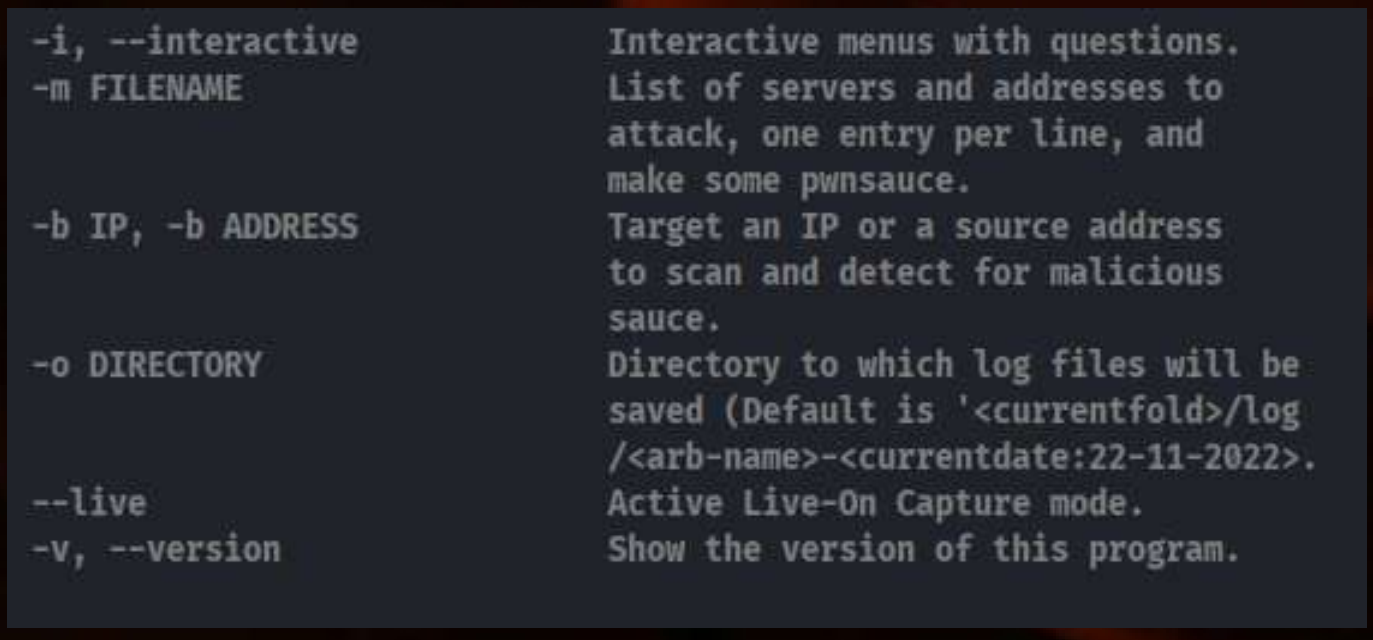
**Usage: ./Hunterseeker [-h | --help] [-I | --interactive]
[-m FILENAME] [-b IP | ADDRESS] [--live]
[-o LOG OUTPUT DIRECTORY] [-v | --version]**

Using "--help" will bring call the full help information

Using "-h" will bring call the short help information



Hunter-Seeker is available as a CLI-tool and also as a full menu interactive mode.



Using “--interactive” (or “-i” for short) will start the fully interactive mode that Hunter-Seeker is able to offer.

* Network Analysis allowing the user to analysis IP Addresses and URLs.
* File Analysis will allow the user to check hashes of files, and to scan A given file with multiple addresses and\or URLs for dangerous code.
* Live-On Mode will initialize a live capture of the network traffic and analysis all the connections made from the network IPs to outgoing domains.

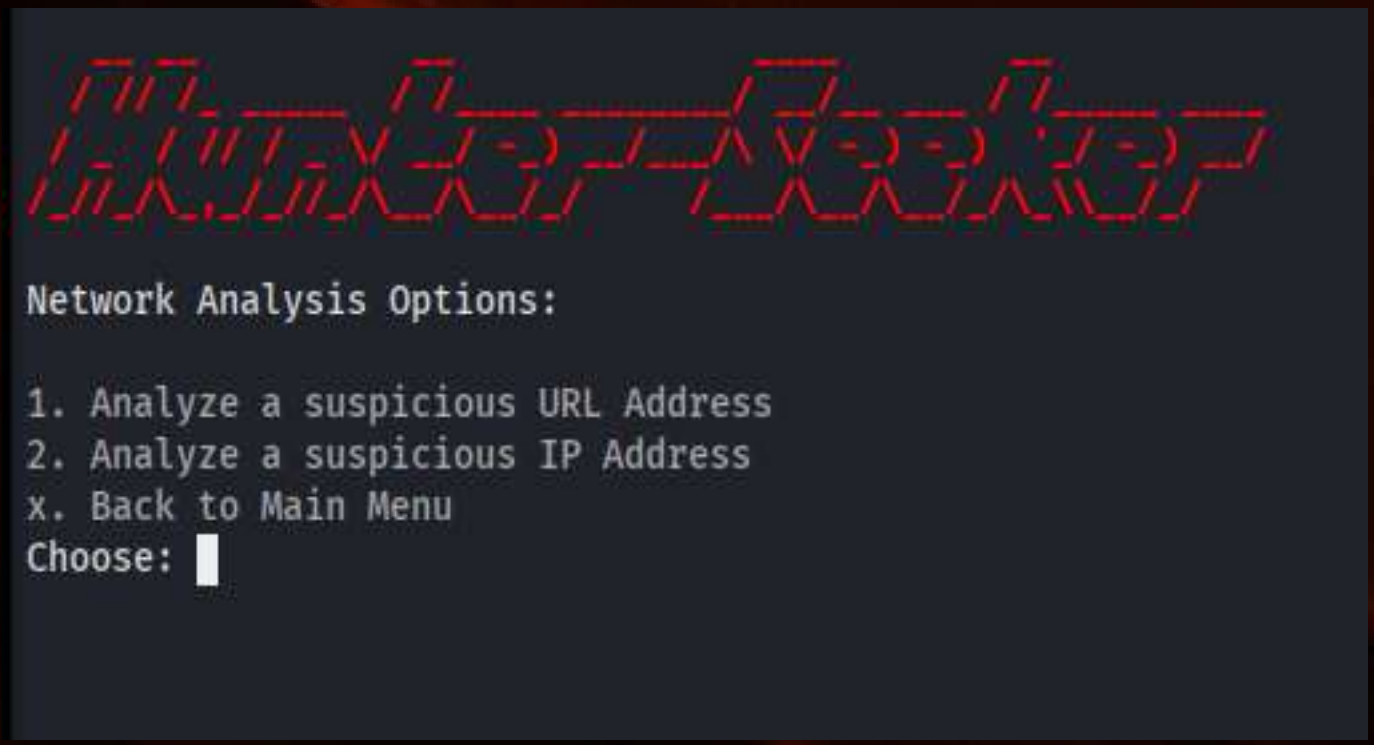
Using “--version” (or “-v” for short) will display the current version of the tool.

The Hunter-Seeker tool is connecting to the VirusTotal community, and will be checking wheter the user registered to an API to allow for a legitimate connection. If not, the user will be redirected to enter his API (in secret) and after affirmation, the tool will continue to the Network Analysis menu.

```
Checking for an existing VirusTotal API...

VirusTotal API found!
```

Network Analysis Menu



Choosing to analyze a URL Address will prompt the user to enter URL.

```
Enter an URL to analyze [example: www.google.com]: jb.cyberiumarena.com
Analyzing malicious activity in URL Address - jb.cyberiumarena.com
Log file saved - /[redacted]:/Scripts/Hunter/log/HuntSeek-MalURL-22-11-2022.log

--Total Votes--
Malicious:  0
```

After analyzing the given URL, the tool will output if any malicious data was found, and will save the detailed results in a log file. The log file directory default is in "/log/<filename>.log" and can be repurposed with assigning the "-o <directory" flag.

```
└─$ cat HuntSeek-MalURL-22-11-2022.log
- _id: "7f38497fdba55d14457727f4947066347f8fdc78cda986296d1b30d4373f48bc"
  _type: "url"
  categories:
  first_submission_date: 1623771463  # 2021-06-15 18:37:43 +0300 +03
  last_analysis_date: 1623771463  # 2021-06-15 18:37:43 +0300 +03
  last_analysis_results:
    ADMINUSLabs:
      category: "harmless"
      engine_name: "ADMINUSLabs"
      method: "blacklist"
      result: "clean"
    AICC (MONITORAPP):
      category: "harmless"
      engine_name: "AICC (MONITORAPP)"
      method: "blacklist"
      result: "clean"
    AlienVault:
      category: "harmless"
      engine_name: "AlienVault"
      method: "blacklist"
      result: "clean"
    Antiy-AVL:
      category: "harmless"
      engine_name: "Antiy-AVL"
      method: "blacklist"
      result: "clean"
    Armis:
      category: "harmless"
```

Choosing to analyze an IP Address will prompt the user will analyze and save the IP in a log file with details reports.

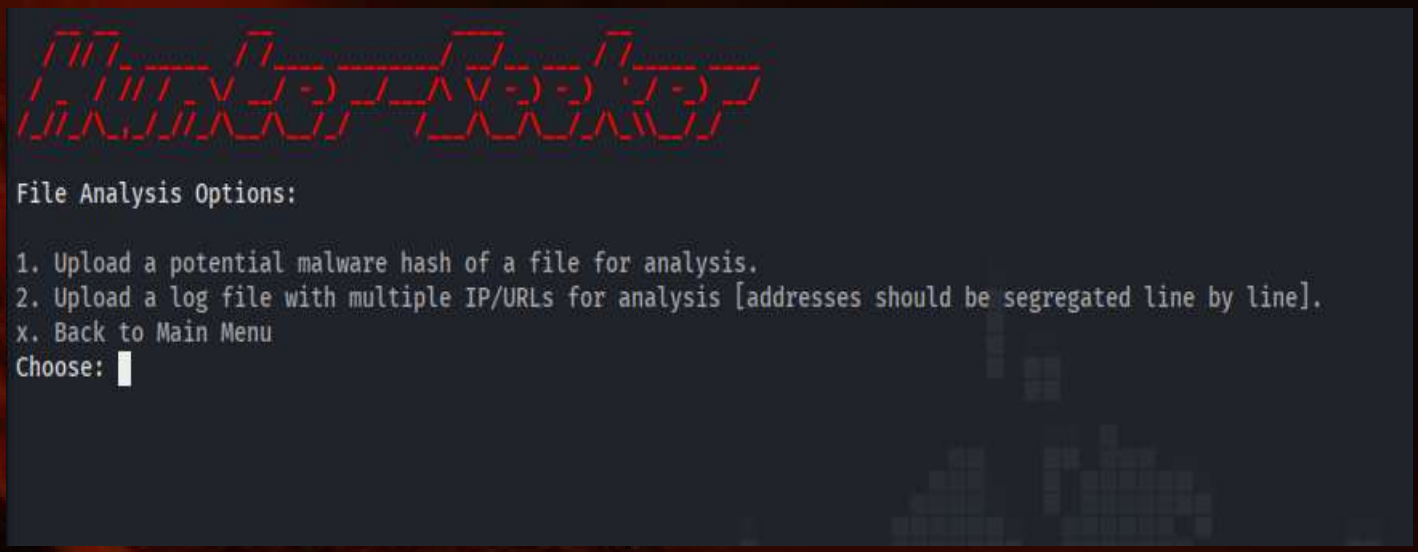
```
└─$ cat HuntSeek-MalIP-22-11-2022.log
- _id: "192.168.0.25"
  _type: "ip_address"
  last_analysis_date: 1669041945  # 2022-11-21 17:45:45 +0300 +03
  last_analysis_results:
    "0xSI_f33d":
      category: "undetected"
      engine_name: "0xSI_f33d"
      method: "blacklist"
      result: "unrated"
    ADMINUSLabs:
      category: "harmless"
      engine_name: "ADMINUSLabs"
      method: "blacklist"
      result: "clean"
    AICC (MONITORAPP):
      category: "harmless"
      engine_name: "AICC (MONITORAPP)"
      method: "blacklist"
      result: "clean"
    Abusix:
      category: "harmless"
      engine_name: "Abusix"
      method: "blacklist"
      result: "clean"
    Acronis:
```

Analyzing the given IP or URL is possible with assigning the flag "./HunterSeeker -b <IP | URL>". Afterwards, the tool will exit and not return to the menus available in the interactive mode.

```
Analyzing malicious activity in IP Address - 192.168.0.25
Log file saved - /home/Bakeneko/Documents/Scripts/Hunter/log/HuntSeek-MalIP-22-11-2022.log

--Total Votes--
Malicious:  0
```

File Analysis Menu



* User can upload a suspicious hash of a file, which will get scanned in VirusTotal and will produce a detailed report of information regarding the potential of malicious code found in given hash, including domains and IPs connected to it, information on the file and its variables, and community information updated by other users.
* The user is able to input a path of a text file stored locally with multiple addresses and domains and the tool will scan them one by one, and inform which of the given is malicious and how much votes it got from the VirusTotal community, and will save logs of more details in the log folder.

User can bind a file with the assigned flag “-m </filepath> from the Command-line without having to enter the interactive menus.

```
Analyzing malicious activity in the IoC file provided - top10-2.txt
 [ID: 111.63.3.214] -- [Malicious code found]:  0
 [ID: 113.125.90.46] -- [Malicious code found]:  0
 [ID: 113.78.109.174] -- [Malicious code found]:  0
 [ID: 114.215.81.200] -- [Malicious code found]:  0
 [ID: 115.206.50.179] -- [Malicious code found]:  0
 [ID: 115.238.58.162] -- [Malicious code found]:  0
 [ID: 116.236.208.206] -- [Malicious code found]:  0
 [ID: 116.236.21.34] -- [Malicious code found]:  0
 [ID: 116.236.220.74] -- [Malicious code found]:  0
 [ID: 118.123.105.89] -- [Malicious code found]:  0
 [ID: 120.132.35.111] -- [Malicious code found]:  0
 [ID: 120.48.131.222] -- [Malicious code found]:  0
 [ID: 123.177.19.13] -- [Malicious code found]:  2
 [ID: 138.99.216.223] -- [Malicious code found]:  0
```

When given a hash, file name is recognized, and in this example, the votes of the malicious dangers is up to 990!

```
Enter a file hash to analyze [example: 76cdb2bad9582d23c1f6f4d868218d6c]:
76cdb2bad9582d23c1f6f4d868218d6c

Analyzing file hash 76cdb2bad9582d23c1f6f4d868218d6c for malicious code.
Analyzing malicious activity in filename: "lprn_spotlightstory_015.zip"
Log file saved - /home/Bakeneko/Documents/Scripts/Hunter/log/HuntSeek-MalFile-22-11-2022.log

--Total Votes--
Malicious:  990
```

Partial details of given hash from the saved log file:

```
└─$ cat HuntSeek-MalFile-22-11-2022.log
- _id: "8739c76e681f900923b900c9df0ef75cf421d39cabb54650c4b9ad19b6a76d85"
  _type: "file"
  first_seen_itw_date: 1235525277  # 2009-02-25 04:27:57 +0300 +03
  first_submission_date: 1170892383  # 2007-02-08 02:53:03 +0300 +03
  known_distributors:
    data_sources:
    - "Microsoft Corporation"
    - "Google"
    - "National Software Reference Library (NSRL)"
    distributors:
    - "Microsoft"
    - "Google"
    - "MR-Software GbR"
    filenames:
    - "SpeechBr.pak"
    - "New Text Document.zip"
    - "lprn_spotlightstory_015.zip"
    - "MacmillanEducationAlturaDev-win32-x64-1.0.0.728.exe.zip"
    - "DDR_Asphalt_variety.zip"
    links:
    - "https://dl.google.com/dl/spotlight/test/lprn_spotlightstory/9/lprn_spotlightstory_015.zip"
    products:
    - "Dying Light"
    - "OMSI 2: Steam Edition"
  last_analysis_date: 1669083032  # 2022-11-22 05:10:32 +0300 +03
  last_analysis_results:
    ALYac:
      category: "undetected"
      engine_name: "ALYac"
```

```
    - "WINDOWS DIALUP.ZIP"
    - "kemsetup.ZIP"
    - "Data_Linux.zip"
    - "2003.zip"
    - "_6A271FB199E041FC82F4D282E68B01D6"
    products:
    - "Master Hacker Internet Terrorism (Core Publishing Inc.)"
    - "Read Rabbits Math Ages 6-9 (Smart Saver)"
    - "Neverwinter Nights Gold (Atari)"
    - "Limited Edition Print Workshop 2004 (ValuSoft)"
    - "Crysis (Electronic Arts Inc.)"
  reputation: -851
  sha1: "b04f3ee8f5e43fa3b162981b50bb72fe1acabb33"
  sha256: "8739c76e681f900923b900c9df0ef75cf421d39cabb54650c4b9ad19b6a76d85"
  size: 22
  ssdeep: "3:pjt/l:Nt"
  tags:
  - "nsrl"
  - "attachment"
  - "via-tor"
  - "known-distributor"
  - "trusted"
  - "software-collection"
  times_submitted: 221494
  tlsh: "TNULL"
  total_votes:
    harmless: 673
```

Log directory of saved log files:

```
┌──([redacted]/Hunter/log]
└─$ ls -la
total 104
drwxr-xr-x 2 root     root      4096 Nov 22 06:47 .
drwxr-xr-x 3 Bakeneko Bakeneko  4096 Nov 22 08:04 ..
-rw-r--r-- 1 root     root     14155 Nov 22 08:02 HuntSeek-LiveOn-22-11-2022.log
-rw-r--r-- 1 root     root     20038 Nov 22 05:43 HuntSeek-MalFile-22-11-2022.log
-rw-r--r-- 1 root     root     14497 Nov 22 05:42 HuntSeek-MalIP-22-11-2022.log
-rw-r--r-- 1 root     root     12640 Nov 22 06:44 HuntSeek-MalMultFiles-22-11-2022.log
-rw-r--r-- 1 root     root     25180 Nov 22 05:42 HuntSeek-MalURL-22-11-2022.log
```

User can change the default log folder and bind a different one Using the assigned flag of "-o <new folder name>". Unless assigned before the run of the script, the folder will remain the default.

```
┌──([redacted]/Hunter/newlogdir]
└─$ ls -la
total 16
drwxr-xr-x 2 root     root     4096 Nov 22 08:19 .
drwxr-xr-x 4 Bakeneko Bakeneko 4096 Nov 22 08:43 ..
-rw-r--r-- 1 root     root       24 Nov 22 08:31 HuntSeek-MalIP-22-11-2022.log
-rw-r--r-- 1 root     root       24 Nov 22 08:31 HuntSeek-MalURL-22-11-2022.log
```

Finally, the last option in the main menu, is the Live-On Capture mode. When break by any key, it will be saved into a detail report.

```
└─$ cat HuntSeek-LiveOn-22-11-2022.log
[Tuesday, Nov 22, 2022 05:47:00] --- [10.0.0.6] accessed [api.protonvpn.ch]
[Tuesday, Nov 22, 2022 05:47:00] --- [10.0.0.6] accessed [staticcdn.duckduckgo.com]
[Tuesday, Nov 22, 2022 05:47:00] --- [10.0.0.6] accessed [v10.events.data.microsoft.com]
[Tuesday, Nov 22, 2022 05:53:39] --- [10.0.0.6] accessed [ledger.bt.co]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [aefd.nelreports.net]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [amp-api.music.apple.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [duckduckgo.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [improving.duckduckgo.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [is1-ssl.mzstatic.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [is2-ssl.mzstatic.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [is3-ssl.mzstatic.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [is4-ssl.mzstatic.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [is5-ssl.mzstatic.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [links.duckduckgo.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [login.microsoftonline.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [mediaauth.apple.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [music.apple.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [qa.sockets.stackexchange.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [services.bingapis.com]
[Tuesday, Nov 22, 2022 05:57:34] --- [10.0.0.6] accessed [storage.live.com]
```

```
Log file saved - /[redacted]/Hunter/log/HuntSeek-LiveOn-22-11-2022.log

        Thank you for using Hunter-Seeker.
        Goodbye!
```


[Jacurutu | https://github.com/RandomLinoge]
JACURUTU
2022