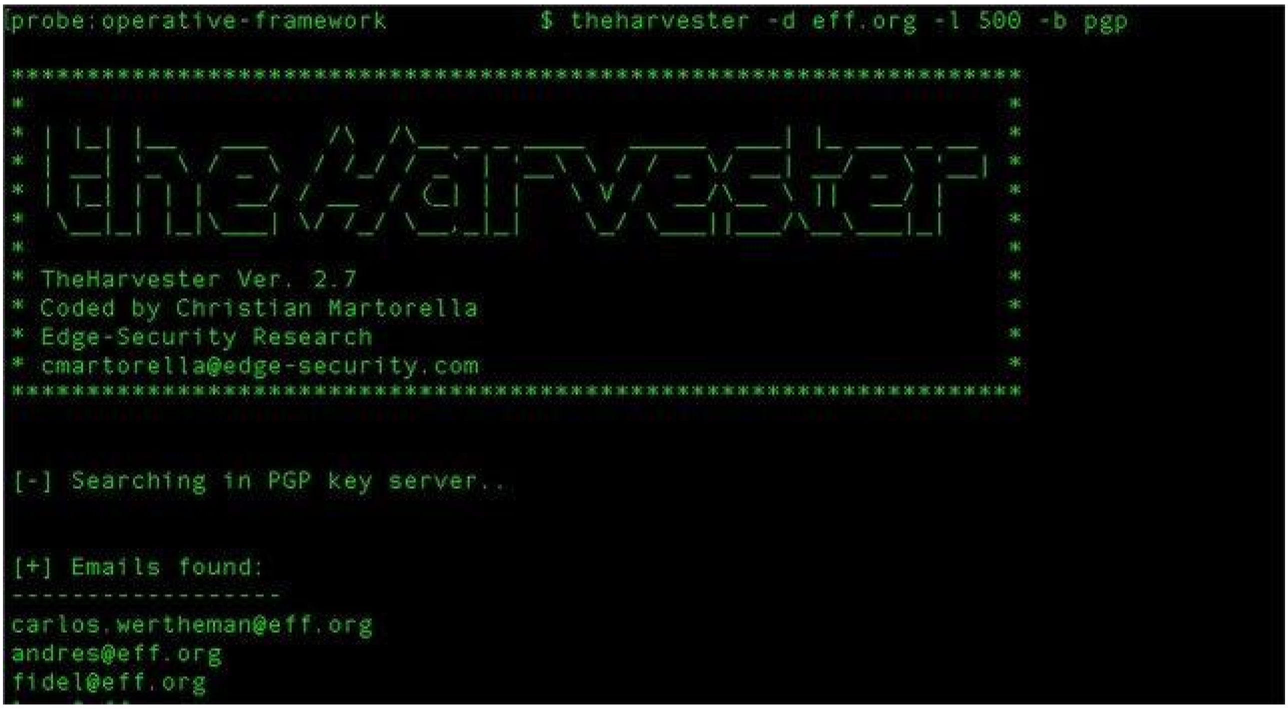
theHarvester is a tool for gathering e-mail accounts, subdomain names, virtual hosts, open ports/ banners, and employee names from different public sources (search engines, pgp key servers).



```
[probe:operative-framework        $ theharvester -d eff.org -l 500 -b pgp

*******************************************************************
*                                                                 *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in PGP key server..


[+] Emails found:
------------------
carlos.wertheman@eff.org
andres@eff.org
fidel@eff.org
```

Is a really simple tool, but very effective for the early stages of a penetration test or just to know the visibility of your company on the Internet.

theHarvester Information Gathering Sources

The sources supported are:

Passive theHarvester Methods

- **google:** google search engine
- **googleCSE:** google custom search engine
- **google-profiles:** google search engine, specific search for Google profiles
- **bing:** microsoft search engine
- **bingapi:** microsoft search engine, through the API (you need to add your Key)
- **dogpile:** Dogpile search engine
- **pgp:** pgp key server – mit.edu
- **linkedin:** google search engine, specific search for Linkedin users
- **vhost:** Bing virtual hosts search
- **twitter:** twitter accounts related to an specific domain (uses google search)
- **googleplus:** users that works in target company (uses google search)
- **yahoo:** Yahoo search engine

- **baidu:** Baidu search engine
- **shodan:** Shodan Computer search engine, will search for ports and banners

Active theHarvester Methods

- DNS brute force: this plugin will run a dictionary brute force enumeration
- DNS reverse lookup: reverse lookup of IPs discovered in order to find hostnames
- DNS TDL expansion: TLD dictionary brute force enumeration

How to use this harvester tool ?

```
  theharvester -d [domain name] -b [search engine name / all ][options]
[parameters]
```

Option's

- **-d:** Domain to search or company name.
- **-b:** Data source: baidu, bing, bingapi, dogpile, google, googleCSE, googleplus, google-profiles, linkedin, pgp, twitter, vhost, yahoo, all.
- **-s:** Start in result number X (default: 0).
- **-v:** Verify hostname via DNS resolution and also search for virtual hosts.
- **-f:** Save the results into an HTML and XML file (both).
- **-n:** Perform DNS reverse query on all ranges discovered.
- **-c:** Perform DNS brute force for the domain name.
- **-t:** Perform DNS TLD expansion discovery.
- **-e:** Use this DNS server.
- **-l:** Limit the number of results to work with (bing goes from 20 to 20 results, google 100 to 100, and pgp doesn't use this option).
- **-h:** Use SHODAN database to query discovered hosts.

Examples

- To list available options

```
theharvester
```

- To search emails

```
theHarvester.py -d wonderhowto.com -b all
```

- To search emails with a limit

```
theHarvester.py -d wonderhowto.com -b all -l 200
```

- To save the result into an html file

```
theharvester -d microsoft.com -b all -h myresults.html
```

- To search in PGP(Pretty Good Privacy) only

```
theharvester -d microsoft.com -b pgp
```