

INFORMATION GATHERING REPORT

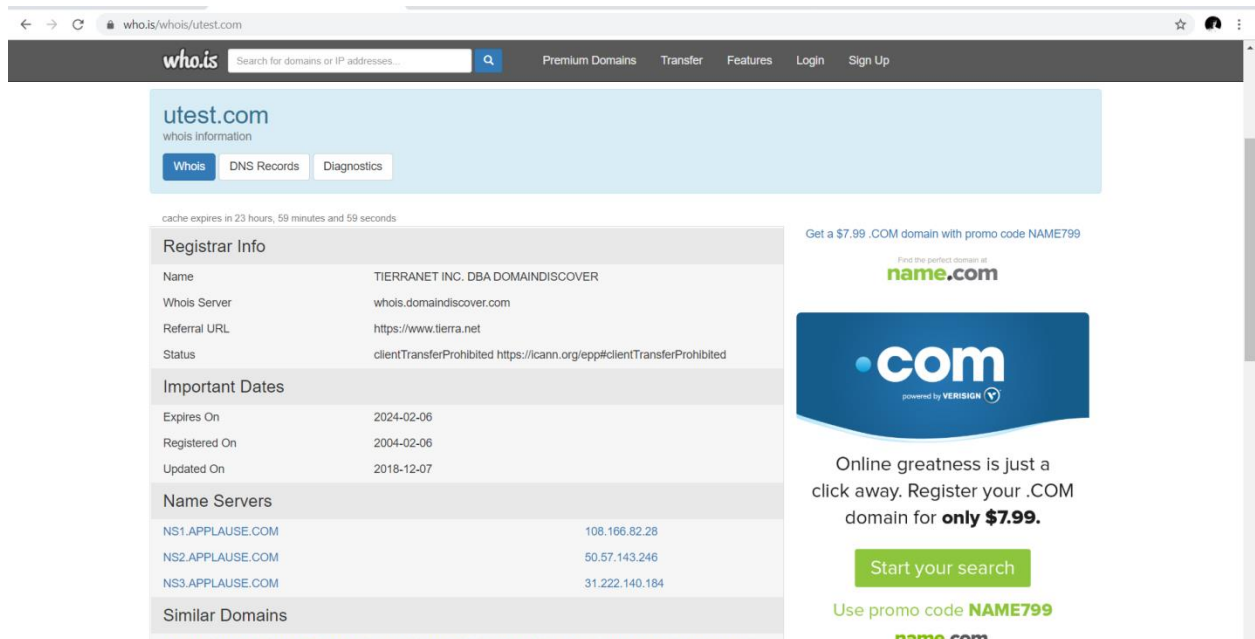
ON

“www.utest.com”

**Submitted to:
Ms. Tripti Misra
Assistant Professor(SS)
Department of Systemics**

**Student Name: OJASVI SINGH CHAUHAN
Roll No: R134218111
SAP ID: 500068394**

1. **Who.is** : It is a website by which we can perform searching on its whois database, look up domain and IP owner information, and we can check out dozens of other statistics. We can get all the data we need about a domain and everything associated with that domain anytime with a single search.



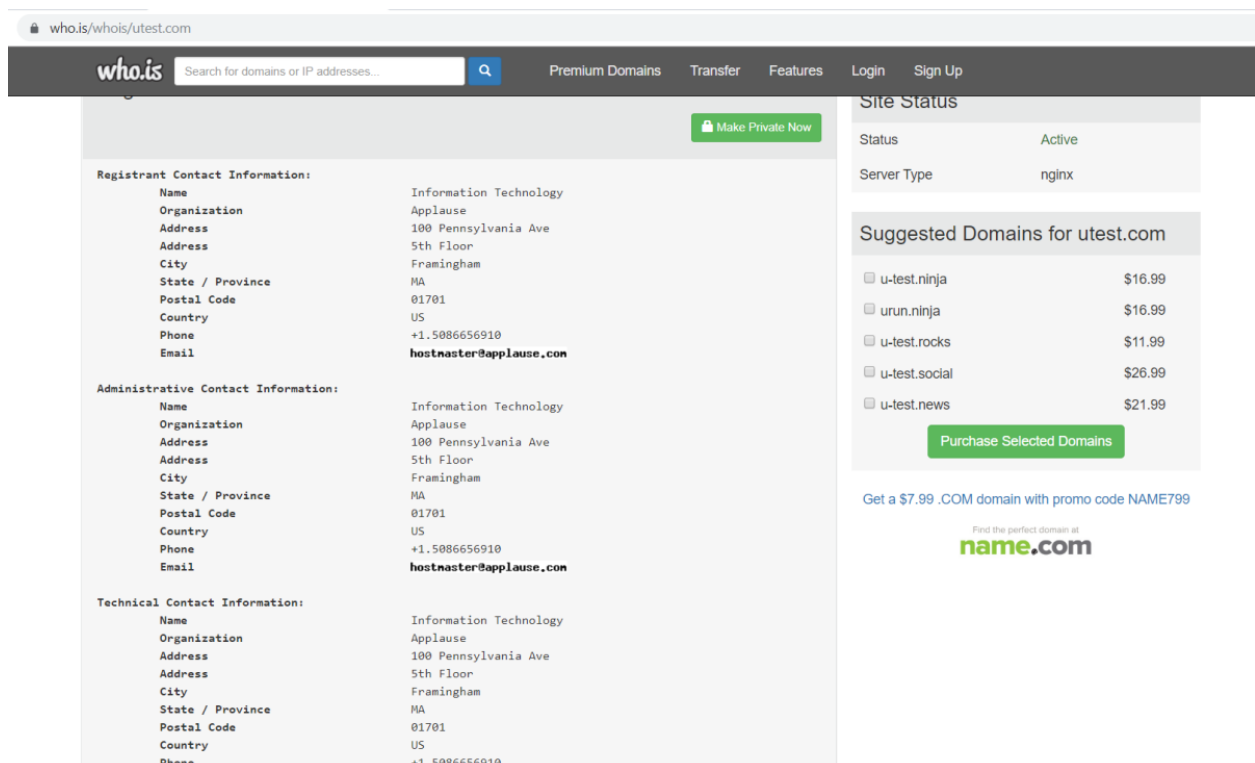
The screenshot shows the who.is website interface. The header includes the who.is logo, a search bar, and navigation links for Premium Domains, Transfer, Features, Login, and Sign Up. The main content area displays whois information for the domain **utest.com**. It includes tabs for Whois, DNS Records, and Diagnostics. The Registrar Info section shows details for TIERRANET INC. DBA DOMAINDISCOVER. The Important Dates section shows the domain expires on 2024-02-06. The Name Servers section lists three servers: NS1.APPLAUSE.COM, NS2.APPLAUSE.COM, and NS3.APPLAUSE.COM. The Similar Domains section is partially visible. On the right side, there is a promotional banner for name.com domains, offering a \$7.99 .COM domain with promo code NAME799.

Registrar Info	
Name	TIERRANET INC. DBA DOMAINDISCOVER
Whois Server	whois.domaindiscover.com
Referral URL	https://www.tierra.net
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates	
Expires On	2024-02-06
Registered On	2004-02-06
Updated On	2018-12-07

Name Servers	
NS1.APPLAUSE.COM	108.166.82.28
NS2.APPLAUSE.COM	50.57.143.246
NS3.APPLAUSE.COM	31.222.140.184

Similar Domains	
[Similar domains listed]	



The screenshot shows the who.is website interface with the contact information for the domain **utest.com**. The header is the same as the previous screenshot. The main content area displays three sections of contact information: Registrant Contact Information, Administrative Contact Information, and Technical Contact Information. All three sections list the same details for Information Technology, Applause, located at 100 Pennsylvania Ave, 5th Floor, Framingham, MA 01701, US. The phone number is +1.5086656910 and the email is hostmaster@applause.com. On the right side, there is a Site Status section showing the domain is Active and the server type is nginx. Below that is a Suggested Domains section for utest.com, listing various domain names and their prices. A green button labeled 'Purchase Selected Domains' is present. At the bottom, there is a promotional banner for name.com domains, offering a \$7.99 .COM domain with promo code NAME799.

Registrant Contact Information:	
Name	Information Technology
Organization	Applause
Address	100 Pennsylvania Ave
Address	5th Floor
City	Framingham
State / Province	MA
Postal Code	01701
Country	US
Phone	+1.5086656910
Email	hostmaster@applause.com

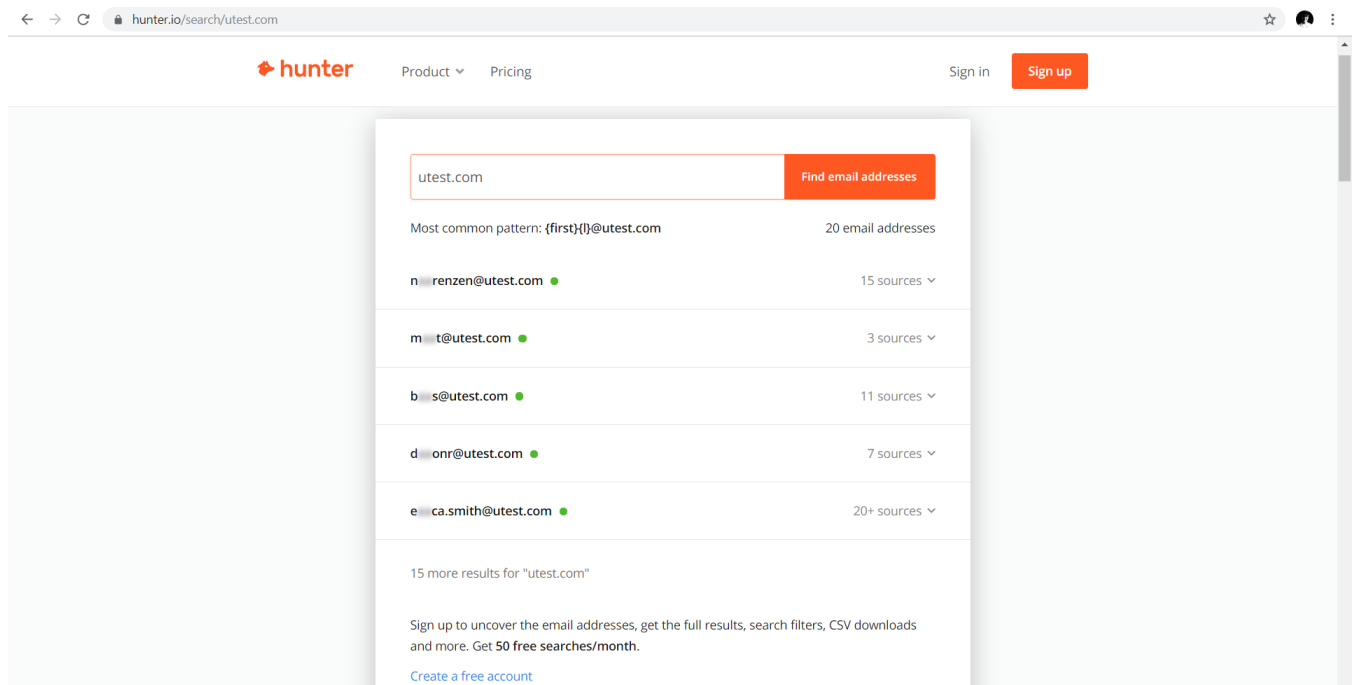
Administrative Contact Information:	
Name	Information Technology
Organization	Applause
Address	100 Pennsylvania Ave
Address	5th Floor
City	Framingham
State / Province	MA
Postal Code	01701
Country	US
Phone	+1.5086656910
Email	hostmaster@applause.com

Technical Contact Information:	
Name	Information Technology
Organization	Applause
Address	100 Pennsylvania Ave
Address	5th Floor
City	Framingham
State / Province	MA
Postal Code	01701
Country	US
Phone	+1.5086656910

Site Status	
Status	Active
Server Type	nginx

Suggested Domains for utest.com	
<input type="checkbox"/> u-test.ninja	\$16.99
<input type="checkbox"/> urun.ninja	\$16.99
<input type="checkbox"/> u-test.ocks	\$11.99
<input type="checkbox"/> u-test.social	\$26.99
<input type="checkbox"/> u-test.news	\$21.99

2. **Hunter.io** : We can get the email addresses behind any website. Its Domain Search lists all the people working in a company with their name and **email address** found on the web. With 200+ million email addresses indexed, effective search filters and scoring, it's the most powerful email-finding tool ever created.



3. **Snitch:** It is a tool which automates information gathering process for specified domain. Using build-in dork categories, this tool helps gather specified information domain which can be found using web search engines. It can be quite useful in early phases of pentest.

```
Applications ▾ Places ▾ Terminal ▾ Sun 8:30 PM
root@kali: ~/Desktop/snitch

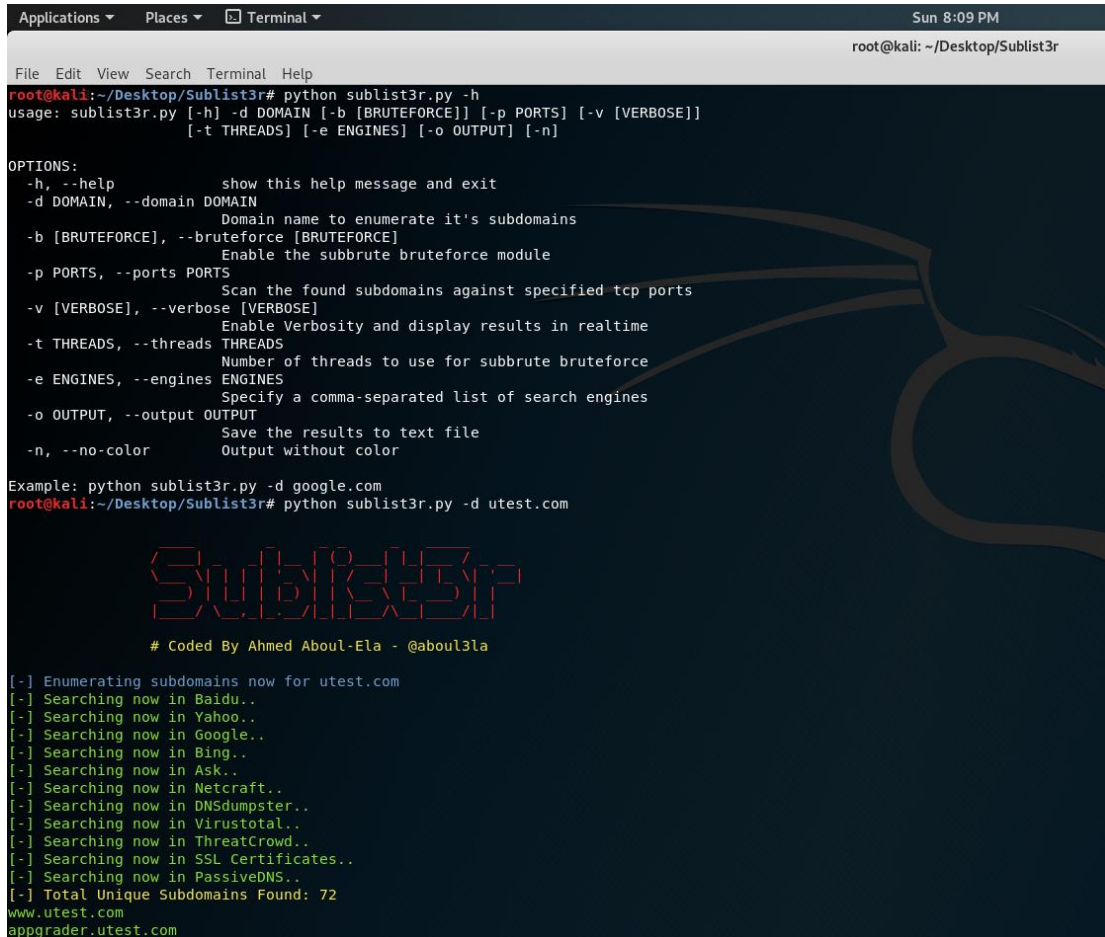
File Edit View Search Terminal Help
root@kali:~# cd Desktop/snitch
root@kali:~/Desktop/snitch# ls
README.md snitch.py
root@kali:~/Desktop/snitch# chmod a+rx snitch.py
root@kali:~/Desktop/snitch# ./snitch.py --help
Usage: snitch.py [options]

Options:
-h, --help            show this help message and exit
-U [url], --url=[url]  domain(s) or domain extension(s) separated by comma*
-D [type], --dork=[type] dork type(s) separated by comma*
-C [dork], --custom=[dork] custom dork*
-O [file], --output=[file] output file
-S [ip:port], --socks=[ip:port] socks5 proxy
-I [seconds], --interval=[seconds] interval between requests, 2s by default
-P [pages], --pages=[pages] pages to retrieve, 10 by default
-v                    turn on verbosity
root@kali:~/Desktop/snitch# ./snitch.py -D info --url=[utest.com]
[+] Target: [utest.com]

[+] Looking for information leaks

https://www.prestashop.com/forums/topic/292134-solved-error-on-upgrade-you-have-an-error-in-your-sql-syntax/
https://www.inmotionhosting.com/support/website/databases/error-1064/
https://community.mybb.com/thread-219215.html
https://community.talend.com/t5/Design-and-Development/You-have-an-error-in-your-SQL-syntax/td-p/10065
https://www.digitalocean.com/community/questions/you-have-an-error-in-your-sql-syntax-wpseo_sitemap_cache_data
https://confluence.atlassian.com/stashkb/can-t-connect-to-mysql-you-have-an-error-in-your-sql-syntax-658736090.html
https://moodle.org/mod/forum/discuss.php?d=183703
https://www.gavick.com/forums/194/1064-you-have-an-error-in-your-sql-syntax-23043
https://coderanch.com/t/610291/databases/mysql-jdbc-exceptions-jdbc-MySQLSyntaxErrorException
https://www.tutorialspoint.com/how-to-resolve-the-mysql-error-you-have-an-error-in-your-sql-syntax-check-the-manualthat-corre
http://www.asettembresivaascuola.it/index.php
https://www.codeproject.com/Questions/1208789/You-have-an-error-in-your-SQL-syntax-check-the-man
https://our.umbraco.com/forum/using-umbraco-and-getting-started/80900-petapoco-page-method-returning-you-have-an-error-in-you
https://support.zabbix.com/browse/ZBXNEXT-4662?page=com.atlassian.jira.plugin.system.issuetabpanels:all-tabpanel
https://community.powerbi.com/t5/Power-Query/MySQL-You-have-an-error-in-your-SQL-syntax-check-the-manual-that/td-p/765840
https://intellipaat.com/community/19811/1064-you-have-an-error-in-your-sql-syntax-python-mysql
https://github.com/gogs/gogs/issues/5602
https://forum.joomla.org/viewtopic.php?t=928785
https://dba.stackexchange.com/questions/123305/mysqlsyntaxerrorexception-you-have-an-error-in-your-sql-syntax
```

4. **Sublist3r** is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSDumpster and ReverseDNS.



```
Applications ▾ Places ▾ Terminal ▾ Sun 8:09 PM
root@kali: ~/Desktop/Sublist3r
File Edit View Search Terminal Help
root@kali:~/Desktop/Sublist3r# python sublist3r.py -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]]
                  [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color        Output without color

Example: python sublist3r.py -d google.com
root@kali:~/Desktop/Sublist3r# python sublist3r.py -d utest.com

          SUBLIST3R
          SUBBRUTE3R

          # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for utest.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 72
www.utest.com
appgrader.utest.com
```

- ```
Applications ▾ Places ▾ Terminal ▾ Sun 8:56 PM
root@kali: ~/Desktop/spiderfoot

File Edit View Search Terminal Help
root@kali:~# cd Desktop/spiderfoot
root@kali:~/Desktop/spiderfoot# ls
dicts dyn LICENSE modules README.md setup.py sfdb.py sflib.py sf.py sfscan.pyc sfwebui.pyc static THAN
Dockerfile lib LICENSE.tp py2exe requirements.txt sfcli.py sfdb.pyc sflib.pyc sfscan.py sfwebui.py spiderfoot.db test VERS
root@kali:~/Desktop/spiderfoot# ./sf.py
Attempting to verify database and update if necessary...
Starting web server at http://127.0.0.1:5001 ...

Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001

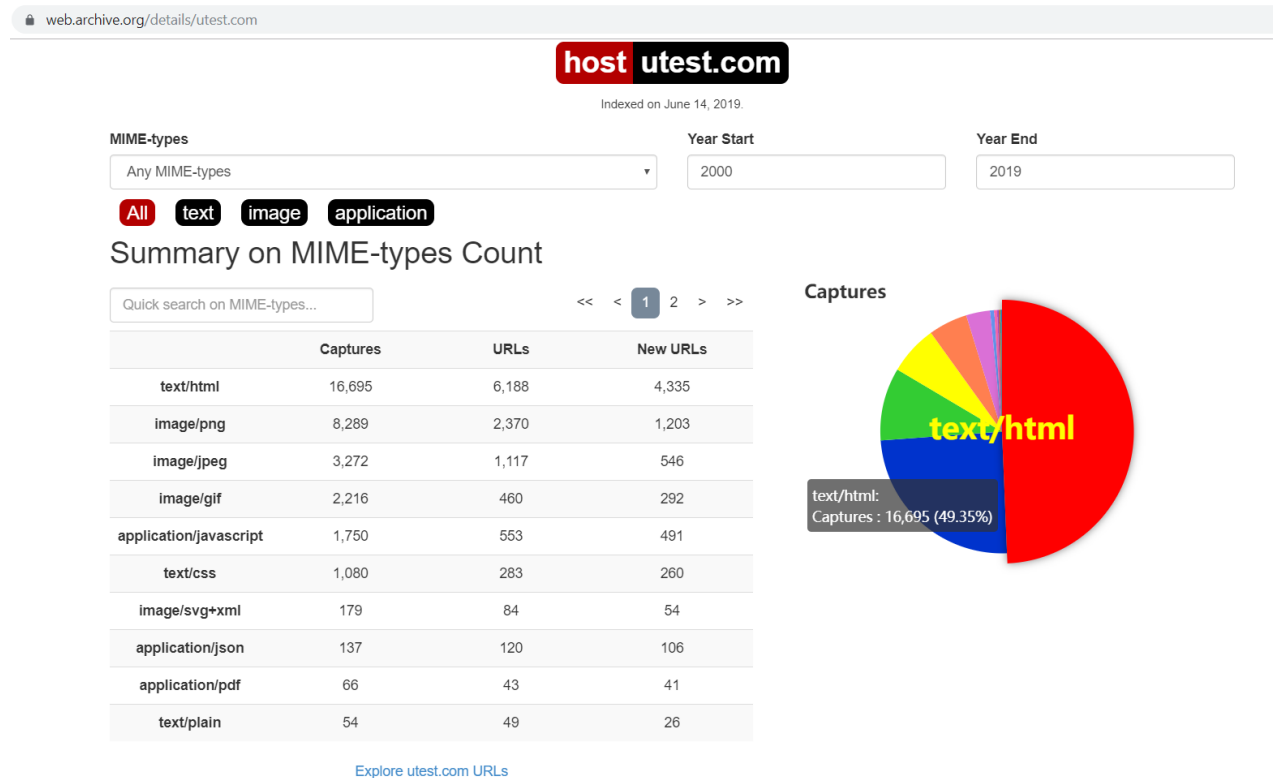
[15/Dec/2019:20:49:29] ENGINE Listening for SIGHUP.
[15/Dec/2019:20:49:29] ENGINE Listening for SIGTERM.
[15/Dec/2019:20:49:29] ENGINE Listening for SIGUSR1.
[15/Dec/2019:20:49:29] ENGINE Bus STARTING
[15/Dec/2019:20:49:29] ENGINE Serving on http://127.0.0.1:5001
[15/Dec/2019:20:49:29] ENGINE Bus STARTED
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET / HTTP/1.1" 200 16657 "" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET /static/css/bootstrap.min.css HTTP/1.1" 200 106006 "http://127.0.0.1:5001/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET /static/js/jquery.min.js HTTP/1.1" 200 88145 "http://127.0.0.1:5001/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET /static/css/spiderfoot.css HTTP/1.1" 200 596 "http://127.0.0.1:5001/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET /static/css/bootstrap-responsive.css HTTP/1.1" 200 22102 "http://127.0.0.1:5001/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET /static/js/spiderfoot.js HTTP/1.1" 200 2718 "http://127.0.0.1:5001/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET /static/js/viz.js HTTP/1.1" 200 13057 "http://127.0.0.1:5001/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET /static/js/jquery.tablesorter.min.js HTTP/1.1" 200 16520 "http://127.0.0.1:5001/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET /static/js/boostrap.min.js HTTP/1.1" 200 28631 "http://127.0.0.1:5001/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [15/Dec/2019:20:49:53] "GET /static/img/glyphicons-halflings.png HTTP/1.1" 200 12799 "http://127.0.0.1:5001/static/css/boostrap/60.0"
```





| Time                | Component             | Type  | Event                                                                                                                                                                               |
|---------------------|-----------------------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2019-12-15 20:52:06 | modules.sfp_binstring | INFO  | Fetched data: 6955 (https://www.utest.com/apple-touch-icon-114x114.png), took 2.45395302773s                                                                                        |
| 2019-12-15 20:52:05 | modules.sfp_binstring | INFO  | Fetching: https://www.utest.com/apple-touch-icon-114x114.png [user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0] [timeout: 30]             |
| 2019-12-15 20:52:04 | modules.sfp_binstring | INFO  | Fetching (HEAD only): https://www.utest.com/apple-touch-icon-114x114.png [user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0] [timeout: 30] |
| 2019-12-15 20:52:04 | modules.sfp_webserver | INFO  | Found web server: nginx (https://www.utest.com/)                                                                                                                                    |
| 2019-12-15 20:52:04 | SpiderFoot            | ERROR | You enabled sfp_spyonweb but did not set an API key!                                                                                                                                |
| 2019-12-15 20:52:04 | SpiderFoot            | ERROR | You enabled sfp_shodan but did not set an API key!                                                                                                                                  |
| 2019-12-15 20:52:04 | modules.sfp_pageinfo  | INFO  | Matched URL_JAVASCRIPT in content from https://www.utest.com/                                                                                                                       |
| 2019-12-15 20:52:04 | modules.sfp_spider    | INFO  | Fetched data: 4575 (https://www.utest.com/), took 3.31622099876s                                                                                                                    |
| 2019-12-15 20:52:02 | modules.sfp_spider    | INFO  | Fetching: https://www.utest.com/ [user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0] [timeout: 5]                                          |
| 2019-12-15 20:52:00 | modules.sfp_spider    | INFO  | Fetching (HEAD only): https://www.utest.com/ [user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0] [timeout: 5]                              |

6. **Wayback Machine** : The Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, they provide free access to researchers, historians, scholars, the print disabled, and the general public. Their mission is to provide Universal Access to All Knowledge.






7. **RBL Lookup:** It is a browser based RBL tool. It is used for discovering if an IP address is on any of the more popular real-time blackhole lists that is checked by the website. To perform a RBL lookup on a domain name, we just type directly into the RBL search box below.

← → ↻ [dnswatch.info/dns/rbl-lookup?host=utest.com&submit=RBL+Lookup](https://dnswatch.info/dns/rbl-lookup?host=utest.com&submit=RBL+Lookup)

---



Mailserver Hostname or IP


[utest.com](#)

RBL Lookup

[DNSWatch](#) > DNSBL/RBL Lookup

This test will check a mail server IP address against 121 DNS based Realtime Blackhole Lists (also known as [RBL](#), DNSBL or email blacklist). If your mail server has been blacklisted in one of the lists, your outgoing email might be considered as SPAM. If you don't know your mailserver's hostname, you can find it out by doing an [MX Lookup on your domain](#) (e.g. newslettertech.com). This is only for mail servers but you need to enter your outgoing mail servers here.

Checked 100.24.95.165 against **121**/121 RBLs.  
IP 100.24.95.165 is listed in **1** Realtime Blacklist(s).

| Blacklist Name  | Status                                                                             | Domain          | Description                             |
|-----------------|------------------------------------------------------------------------------------|-----------------|-----------------------------------------|
| Brazilian SPFBL |  | dnsbl.spfbl.net | Enforces rules like correct PTR records |

☐ Network Problem/Timeout   ☒ Listed in Blacklist